Applications of Structure-Preserving Cryptography and Pairing-Based NIZK Proofs

Benoît Libert

Ecole Normale Supérieure de Lyon

Applications of Structure-Preserving Cryptography and Pairing-Based NIZK Proofs

Benoît LIBERT

Chercheur

Mémoire d'habilitation à diriger des recherches

Présenté le 29 mai 2015 après avis des rapporteurs :

Charanjit JUTLA, Researcher, IBM Research (USA)
Eike KILTZ, Professor, Ruhr University of Bochum (Germany)
David POINTCHEVAL, Directeur de recherche, CNRS, École Normale Supérieure

Examinateurs :

Dario CATALANO, Professor, Università di Catania (Italy)
Guillaume HANROT, Professeur, Ecole Normale Supérieure de Lyon
Pascal PAILLIER, CEO and Senior Security Expert at CryptoExperts, Paris
David POINTCHEVAL, Directeur de recherche, CNRS, École Normale Supérieure
Brigitte VALLÉE, Directrice de recherche, CNRS, Université de Caen

Contents

Introduction

This document presents some of the results I obtained in the recent years in the area of cryptography.

My current and past researches were devoted to the design of efficient and provably secure public-key cryptographic schemes. These days, when it comes to proposing a new cryptosystem, it is (fortunately) a common practice to provide strong evidence of its security by means of a rigorous security proof. To this end, one should first formally define what it means for the specific cryptographic primitive to be secure. Then, a common approach consists in giving a reduction showing that, in the sense of the considered security definition, any efficient adversary (i.e., with polynomial running time in the security parameter) breaking the system with non-negligible probability would imply a polynomial algorithm solving a hard problem (such as factoring large integers, computing discrete logarithms, etc). The conjectured intractability of the problem in polynomial time thus implies the non-existence of polynomial adversaries. In some cases, security proofs may take place in the random oracle model [32], which is an idealized model of computation where hash functions are modeled as oracles controled by the reduction. This notably implies that, whenver the adversary wants to know the hash value of any input string, it has to ask an oracle for it and thus reveal to the reduction which hash values it decides to compute. The random oracle methodology has been subject to criticism as there are examples (see, e.g., [72]) of cryptographic schemes that have no secure instantiation with a real hash function although they do have a security proof in the random oracle model. For this reason, a security proof in the standard model (i.e., without random oracles) may be preferrable, especially when it comes at a reasonable cost. The results presented in this habilitation thesis do not rely on random oracles and thus stand in the standard model of computation.

My contributions fit within several sub-areas of public-key cryptography. In order to describe the global context of my research, these sub-areas will briefly outlined in the following pages. In this habiliation thesis, however, I will focus on the topics of anonymity-related cryptographic protocols and homomorphic cryptography, which are discussed in sections 0.5 and 0.7 of this introduction.

0.1 Identity-Based Encryption

My PhD thesis presented new applications of bilinear maps over groups where the discrete logarithm problem is presumably hard. These tools found many applications such as identity-based encryption (IBE) [236, 45], where any human-readable identifier (e.g., an email address) can serve as a public key so as to eliminate the need for digital certificates and simplify key management. The most important contribution [27] of my PhD thesis was

to describe the most efficient identity-based cryptosystem combining the functionalities of signature and encryption. This research was carried out in collaboration with Paulo Barreto and Noel McCullagh.

Part of my post-doctoral research was also related to identity-based encryption. In collaboration with Damien Vergnaud, we described an improved technique [186] allowing to decrease the required amount of trust in authorities (that have to generate users' private keys and are obviously able to decrypt all ciphertexts) in IBE schemes as initially suggested by Goyal [130]. We showed [186] an efficient way to prevent dishonest authorities from re-distributing copies of users' private keys without being detected. Our technique allows tracing obfuscated decryption devices (based on their input-output behavior) that illegally decrypt users' communications back to their source. The advantage of our construction is to provide a much better efficiency than previous constructions [130, 131] enabling black-box traceability. In collaboration with Nuttapong Attrapadung, we also described [22] the first identity-based broadcast encryption scheme — where the sender can encrypt messages for several identities -– that simultaneously provides adaptive security and constant-size ciphertexts, regardless of the number of receivers. This result was published at the Public-Key Cryptography 2010 conference. Together with Nuttapong Attrapadung and Elie de Panafieu (who was an internship student of mine during the summer 2009), we also described several constructions [24, 21] of attribute-based encryption (ABE) schemes featuring short ciphertexts. In short, ABE schemes are a generalization of identity-based encryption where ciphertexts are labeled with sets of descriptive attributes whereas users' private keys encode a complex access formula specifying which ciphertexts users are entitled to decrypt. The ABE primitive is motivated by fine-grained access control over encrypted data. For example, they make it possible to selectively share one's data in cloud storage systems. Our contribution [24, 21] was to describe the first truly expressive solutions where the size of the ciphertext does not depend on the number of associated attributes.

0.2 Key-Evolving Cryptography

Between 2006 and 2009, in collaboration with Moti Yung, I explored techniques allowing to confine the effect of private key exposures – caused by hackers rather than actual cryptanalysis – within a certain time interval. With the growing use of mobile devices, it has become much easier to break into users' computer than defeating cryptosystems by solving hard problems. One way to address this concern is to update private keys at discrete time periods (without changing the public key) in such a way that the security of past periods is preserved after a key exposure. This property is termed "forward security". Our main result [181] was a generic technique allowing a computer to automatically handle key updates (without any human intervention) in forward-secure signatures where private keys are shielded by a second factor, such as a password. Most previous key-evolving signatures were not compatible with this kind of additional password-based key protection since, in straightforward implementations, users had to enter their password at each update operation, which was impractical in case of frequent updates. Our results [181, 182] consisted of generic ways allowing an untrusted computing environment to update an encrypted version of the user's private key, in such a way that passwords only come into play to sign messages.

0.3 Cryptographic Schemes with Delegation

In 2008, in collaboration with Damien Vergnaud, we studied [184] key delegation techniques that find applications in the secure forwarding of encrypted emails or in distributed file systems. As initially suggested by Blaze, Bleumer and Strauss [35], a proxy re-encryption system (PRE) is an encryption scheme where a delegator A can provide a proxy with a re-encryption key allowing to translate ciphertexts initially encrypted for A into ciphertexts encrypted for a delegatee B. The proxy should be able to do so without seeing underlying plaintexts or any user's private key. Our contribution [184] was to describe the first unidirectional PRE system (where the proxy can translate from A to B without being also able to translate from B to A) that can be proven secure against chosen-ciphertext attacks, where the adversary has access to a decryption oracle. Later on, we addressed similar problems in the context of signature schemes [183], where a proxy should be able to translate B's signatures into signatures bearing A's name. In 2005, Ateniese and Hohenberger showed how cryptographic bilinear maps can be used to design unidirectional proxy re-signatures (PRS), which are useful for the inter-domain conversion of digital certificates. They left open the problem of constructing unidirectional PRS schemes where signatures can be translated in sequence (from A to B first, then from B to C and so on). We provided the first step [183] towards efficiently solving this problem suggested for the first time by Blaze, Bleumer and Strauss in 1998 [35].

0.4 Distributed Cryptography

Threshold cryptography [96, 98] aims at avoiding single points of failure by splitting private keys into n shares, each one of which is given to a different server, in such a way that at least t of these shares should be combined to recover the original private key. This implies that at least t servers should contribute to private key operations (namely, the decryption procedure in a public-key encryption scheme and the signing process in digital signatures). A threshold primitive is said robust if a malicious adversary who corrupts at most $t-1$ servers cannot prevent the honest majority (which exists when $n \geq 2t-1$) from successfully completing their operations. Threshold cryptographic schemes have been mostly analyzed in the scenario of static corruptions, where the adversary has to choose which servers he wants to corrupt before the generation of the public key. Unfortunately, adaptive adversaries (who can choose whom to corrupt at any time, based on their complete view) turn out to be harder to deal with. In the context of robust threshold public-key encryption systems with chosen-ciphertext security (i.e., that resist adversaries equipped with a decryption oracle), most adaptively secure solutions have a relatively complex decryption protocol, where some interaction is required among decryption servers. In collaboration with Moti Yung, we proposed the first fully non-interactive robust threshold cryptosystems that provide chosen-ciphertext security against adaptive adversaries in the standard model. In 2011, we first described a scheme [189] based on specific number theoretic assumptions. In 2012, we provided a more general framework [191] for constructing such threshold cryptosystems and gave several instantiations with a better efficiency than our initial realization.

0.5 Anonymity-Related Cryptographic Primitives

Between 2009 and 2014, I also worked on privacy-enhancing cryptographic mechanisms such as those allowing users to accountably hide in a crowd. Group signatures[1], as introduced by Chaum and Van Heyst [85], allow registered members of a group to anonymously sign messages in the name of the entire group. If necessary, an authority is able to identify the signer using some secret information. This primitive finds applications in trusted computing platforms or in electronic auction systems. It is well-known how to construct efficient group signatures in the random oracle model [15] and in the standard model [55, 56, 134]. Traceable signatures [155] extend group signatures in that the group manager can additionally reveal a user-specific trapdoor allowing to publicly trace all signatures issued by a given member suspected of illegal activity. Hence, misbehaving users' signatures can be traced without requiring the opening authority to open all signatures, which would harm the privacy of honest users. In a joint work with Moti Yung [187, 190], we constructed the first efficient traceable signature scheme that does not appeal to the random oracle model.

In the area of group signatures, I also paid attention to the revocation problem, which consists in efficiently disabling the anonymous signing capability of expelled group members and only these members. Together with Damien Vergnaud [185], we proposed a first solution in the standard model in 2009. Unfortunately, this approach has the disadvantage of incurring a verification cost linear in the number of revocations. In collaboration with Moti Yung and Thomas Peters [180, 179], we subsequently showed how to avoid this limitation. Specifically, we described a new revocation mechanism which is borrowed from the literature on broadcast encryption. This approach is well-suited to group signatures in the standard model. Its main advantage over many existing solutions is that unrevoked group members do not need to update their private keys when other members are revoked. At the same time, the verification cost and the size of signatures are constant (where "constant" means that it only depends on the security parameter and not on the number of revocations or the maximal number group members). Our initial scheme improves upon a comparable mechanism (published by Nakanishi *et al.* [202]) in that it completely avoids linear complexities in the maximal cardinality of the group: the complexity is at most poly-logarithmic in all metrics. Subsequently, we further showed how to additionally obtain constant-size private keys without degrading the efficiency in other metrics.

Group encryption [156] is the encryption analogue of group signatures. Namely, a sender should be able to encrypt a message for some anonymous member of a group while appending to the ciphertext a proof that the latter is well-formed and intended for some certified group member. The primitive finds applications in the asynchronous transfer of credentials between peer devices or the verifiable encryption of keys to anonymous trusted parties. The first scheme, proposed by Kiayias, Tsiounis and Yung in 2007 [156], requires interactive conversations (at least if one is willing to avoid the random oracle model) between the sender and the proof verifier. The need for interaction is a limitation since it requires senders to be online at the same time as verifiers and to remember the random numbers that were used to encrypt all ciphertexts. In collaboration with Julien Cathalo and Moti Yung [81], we showed the first truly non-interactive scheme (i.e., no interaction is ever needed between the sender and the verifier) with a security proof in the standard model. In the same article on non-interactive group encryption [81], we described one of the first realizations (actually, the first

[1] Note that, here, the term "group" refers to a population for users rather than an algebraic structure.

practical one with a security proof under non-interactive number theoretic assumptions) of a primitive initially suggested by Groth [133] and that was subsequently called "structure-preserving signature" in the literature [4, 6]. Structure-preserving signatures are signature schemes where messages and public keys only consist of elements of an abelian group over which a bilinear map is efficiently computable. They have many applications in privacy-preserving protocols because they are fully compatible with the Groth-Sahai non-interactive proof systems [138]. The reason is that Groth-Sahai proofs can only serve as proofs of knowledge – in the sense that a knowledge extractor can recover the witnesses from any valid proof – when the witnesses are elements of an abelian group over which a bilinear map is efficiently computable. The useful property of structure-preserving signatures is that they precisely allow signing elements of bilinear groups without destroying their algebraic structure (in particular, without first hashing them). For example, this allows one to efficiently prove knowledge of a hidden message-signature pair, as typically done in group signature schemes. More efficient structure-preserving signatures appeared in the literature later on [4, 6, 2, 3].

In the context of group signatures, I also considered alternatives to factoring and discrete-logarithm-based solutions. In collaboration with Fabien Laguillaumie, Adeline Langlois and Damien Stehlé [166], we proposed the first group signature based on lattice hardness assumptions with logarithmic signature size in the cardinality of the group. In earlier lattice-based constructions [129, 69], the signature length was linear in the maximal number of group members.

0.6 Commitment Schemes with Special Properties

A commitment scheme is the digital analogue of a safe or a sealed envelope. Namely, whatever is in the envelope remains secret until the opening of that envelope. At the same time, the sender is bound to a unique message and cannot change his mind about the content when the envelope is sealed. Commitment schemes are a fundamental cryptographic primitive (often used in auction protocols, for example) which comes into play when it comes to force a party to choose a value without directly revealing it. Zero-knowledge sets (ZKS) [199] allow a prover to commit to a set of values S so as to be able to subsequently (and non-interactively) prove statements such as « element x belongs to the set S » or « element y does not belong to S » without revealing anything else, not even the overall cardinality of the set S. In collaboration with Moti Yung, we described [188] a ZKS protocol where proofs of membership and non-membership can both be short (less than 2 kB in implementations using suitable parameters). We thus improved upon previous ZKS schemes (and notably the construction of Catalano, Fiore and Messina [76]), where only proofs of non-membership can be made compact. So far, our construction remains the most efficient ZKS system in terms of communication complexity. In comparison with the first proposal of Micali, Rabin and Kilian [199], proofs are compressed to 13 % of their original length. In addition, we showed how to provide our scheme with certain non-malleability properties. Namely, we can prevent dishonest provers from correlating their hidden set to those of honest provers and still generating convincing proofs. In the same paper [188], as an intermediate result, we also proposed the first commitment scheme that allows committing to vectors of messages in such a way that the commitment – which has constant size – can be selectively opened with respect to one coordinate of the vector without revealing the content of other

coordinates and with an opening of constant size (here, "constant" means independent of the dimension of the vector). As a second contribution to the area of commitment schemes, in collaboration with Marc Fischlin and Mark Manulis, we described [108] new constructions of universally composable commitments [71]. These are commitment schemes that, as required by Canetti's universal composition framework [70], provably remain secure in arbitrary environments, when composed with any other protocol. Universally composable (UC) commitments provide very strong security guarantees, including non-malleability, but they are notoriously very hard to construct (some setup assumption, like a common reference string generated by some trusted party, is inevitable, as shown by Canetti and Fischlin [71]). Yet, our new constructions feature a previously unique combination of efficiency and security properties. Namely, they are the first adaptively secure UC commitments where: (1) The sender can commit to multiple bits at once (so that n-bit strings can be committed to using $O(k+n)$ bits instead of $O(kn)$, where k is the security parameter); (2) The common reference string can be re-used across multiple commitments (and not only once as in certain constructions); (3) The commitment and opening phases both consist of a single message from the sender to the receiver.

0.7 Homomorphic Cryptography

Homomorphic signatures were first suggested by Desmedt [97] and formally defined by Johnson *et al.* [148]. They can be seen as the signature counterpart of homomorphic public-key encryption in that they allow a signer to authenticate messages in such a way that anyone can publicly derive a signature on certain functions of previously signed messages. In linearly homomorphic signatures [48], for example, the signer can authenticate vectors using his private key. Later on, anyone will be able to compute a signature on any linear combination of the signed vectors. As another example, homomorphic subset signatures [148, 11] make it possible for the signer to sign a set of values so that it will be possible to publicly derive a signature on a subset of the original set. Homomorphic signatures notably find applications in proofs of storage [13, 16] or proofs of correct computation [47, 46, 11] in cloud computing systems: when a client wants to outsource large datasets on a remote storage server, he can ask the latter to perform computations on his data. If the original dataset is signed by the client using a homomorphic signature scheme, the server will be able to authenticate the result of his computation, by publicly deriving a signature on the result of the carried out operation. For example, a linearly homomorphic scheme allows one to authenticate sums, averages or Fourier transforms on outsourced data: by verifying the signature derived by the server, the client will be convinced that the server properly archived his dataset and correctly computed the requested statistics. Certain applications need homomorphic signatures that satisfy certain privacy properties requiring derived signatures to be perfectly indistinguishable from original signatures. In proofs of correct computation, one may want the derived signature to hide all partial information about the original dataset: only the mean or the average should become public. If homomorphic subset signatures are used by an administration to authenticate e-ID cards, the latter privacy notion guarantees that the card holder will be able to prove that he is above 18 years old (by deriving a signature on the "date of birth" field of his ID card) without revealing his exact place of birth or any other private information. In collaboration with Nuttapong Attrapadung and Thomas Peters, we suggested stronger definitions of information-theoretic privacy for homomorphic

signatures. In [25, 26], we also described the first constructions of homomorphic subset signatures and linearly homomorphic signatures that satisfy our strongest privacy notion in the standard model. We also described the most efficient (notably in terms of signature size) linearly homomorphic signature with a security proof under standard assumptions in the standard model. At PKC 2013, we also designed a homomorphic quotable signature scheme – where a signature on a string allows publicly computing a signature on any substring of the original string – satisfying the strongest privacy property while retaining signatures of optimal size.

In 2013, in collaboration with Marc Joye, Moti Yung and Thomas Peters [177], we showed a somewhat surprising application of linearly homomorphic signatures in the construction of non-interactive non-malleable commitments [101, 102] in the common reference string model. The goal of non-malleable commitments is to enforce the independence among distinct parties' committed values. To our knowledge, there was previously no efficient construction of non-interactive non-malleable commitment where a short commitment string allows committing to a vector while remaining able to efficiently prove properties about committed coordinates (which precludes the trivial solution consisting in committing to hashed vectors). In [177], we showed that any linearly homomorphic signature that fits a certain template – as is the case of all known constructions based on bilinear maps – can be turned into a primitive called non-interactive simulation-sound trapdoor commitment [116, 195] which, in turn, implies non-interactive non-malleable commitments in the sense of a definition used by Damgård and Groth [94]. Our construction yields constant-size commitments to vectors which preserve the ability to prove statements about committed vectors in a zero-knowledge manner (using interaction or not). In the same paper [177], we also considered linearly homomorphic signature schemes that are also structure-preserving. Namely, they make it possible to sign vectors of group elements of unknown discrete logarithms. We described efficient constructions of linearly homomorphic structure-preserving signatures (LHSPS) and used them to generically build non-malleable commitments to group elements. These were the first examples of non-malleable commitments allowing to prove knowledge of an opening using the Groth-Sahai techniques [138]. Later on [178], we also used linearly homomorphic structure-preserving signatures to build quasi-adaptive non-interactive zero-knowledge (QA-NIZK) proof systems, as defined by Jutla and Roy [151], with constant-size proofs. Specifically, our construction [178] allows proving that a vector of group elements $\mathbf{v} \in \mathbb{G}^n$ belongs to a linear subspace spanned by $t < n$ independent vectors of group elements $\mathbf{v}_1, \ldots, \mathbf{v}_t \in \mathbb{G}^n$. The novelty of our proof system – which is actually an argument system since only polynomially bounded adversaries are unable to prove false statements – is to provide constant-size proofs (typically made of 2 or 3 group elements), regardless of the dimension of the subspace. In addition, we showed how our QA-NIZK proof system can be endowed with a property called simulation-soundness [231], which basically prevents a probabilistic polynomial-time (PPT) adversary from proving false statements, even after having seen simulated proofs for possibly false statements. As an application, we described [178] more efficient non-interactive threshold cryptosystems that are both chosen-ciphertext-secure and secure against adaptive corruptions.

0.8 Organization

In the upcoming chapters, this thesis will give an overview of my results on the applications of structure-preserving cryptography. Chapter 1 will provide some background material which will ease the reading of subsequent chapters. Chapter 2 will describe my results on the design of group encryption [81] and revocable group signatures [180, 179], which are amongst my most important results on privacy-enhancing cryptographic protocols based on structure-preserving cryptography. Chapter 3 will finally present my constructions [178] of structure-preserving signatures with additive homomorphic properties and explain their applications in the design of non-interactive non-malleable primitives. These include non-malleable commitments, space-efficient simulation-sound QA-NIZK argument systems and chosen-ciphertext-secure public-key encryption.

List of Publications

Articles marked with [⋆] are the articles presented in this manuscript.
The articles below can be downloaded at `http://perso.ens-lyon.fr/benoit.libert/`.

Refereed Journals

[J1] Benoît Libert, Jean-Jacques Quisquater and Moti Yung. *Key Evolution Systems in Untrusted Update Environments* , extended version of [15], in *ACM Transactions on Information and System Security (ACM-TISSEC)*, December 2010, volume 13(4), Article 37.

[J2] Benoît Libert and Damien Vergnaud. *Unidirectional Chosen-Ciphertext Secure Proxy Re-Encryption*, extended version of [17], in IEEE Transactions on Information Theory, March 2011, volume 57(3), pp. 1786–1802.

[J3] Benoît Libert and Moti Yung. *Efficient Traceable Signatures in the Standard Model* , extended version of [22], in Theoretical Computer Science, March 2011, volume 412(12-14), pp. 1220–1242.

[J4] Benoît Libert and Damien Vergnaud. *Towards Practical Black-Box Accountable Authority IBE*: *Weak Black-Box Traceability with Short Ciphertexts and Private Keys* , extended version of [20], in IEEE Transactions on Information Theory, October 2011, volume 57(10), pp. 7189-7204.

[J5] Nuttapong Attrapadung and Benoît Libert. *Functional Encryption for Public-Attribute Inner Product*: *Achieving Constant-Size Ciphertexts with Adaptive Security or Support for Negation*, extended version of [27], in Journal of Mathematical Cryptology, October 2011, vol. 5(2), pp. 115-158.

[J6] Nuttapong Attrapadung, Javier Herranz, Fabien Laguillaumie, Benoît Libert, Elie De Panafieu and Carla Ràfols. *Attribute-Based Encryption Schemes with Constant-Size Ciphertexts*. Includes an extended version of [30], in Theoretical Computer Science, March 2012, vol. 422, pp. 15-38, 2012.

[J7] Benoît Libert and Moti Yung. *Adaptively Secure Non-Interactive Threshold Cryptosystems*, extended version of [32], in Theoretical Computer Science, March 2013, Vol. 478, pp. 76–100.

Papers in international conferences with scientific committee and proceedings

[1] Benoît Libert & Jean-Jacques Quisquater. *New identity based signcryption schemes from pairings*, in *IEEE Information Theory Workshop (ITW) 2003*, (J. Boutros ed.), IEEE, 2003, p. 155-158.

[2] Benoît Libert & Jean-Jacques Quisquater. *Efficient Revocation and Threshold Pairing Based Cryptosystems*, in *22nd Symposium on Principles of Distributed Computing (PODC 2003)*, (S. Rajsbaum ed.), ACM Press, 2003, p. 163-171.

[3] Benoît Libert & Jean-Jacques Quisquater. *Identity Based Undeniable Signatures*, in *Topics in Cryptology -* CT-RSA *2004* (T. Okamoto, ed.), Lect. Notes Comput. Sci., vol. 2964, Springer, 2004, p. 112-125.

[4] Benoît Libert & Jean-Jacques Quisquater. *Efficient Signcryption with Key Privacy from Gap Diffie-Hellman Groups*, in *Public Key Cryptography (*PKC*) 2004* (F. Bao, ed.), Lect. Notes Comput. Sci., vol. 2947, Springer, 2004, p. 187-200.

[5] Julien Cathalo, Benoît Libert & Jean-Jacques Quisquater. *Cryptanalysis of a Verifiably Committed Signature Scheme based on GPS and RSA*, in *Information Security Conference (*ISC*) 2004* (K. Zhang & Y. Zheng, ed.), Lect. Notes Comput. Sci., vol. 3225, Springer, 2004, p. 52–60.

[6] Benoît Libert & Jean-Jacques Quisquater. *Improved Signcryption from q-Diffie-Hellman Problems*, in *Fourth Conference on Security in Communication Networks, SCN 2004* (C. Blundo & S. Cimato, eds.), Lect. Notes Comput. Sci., vol. 3352, Springer, 2005, p. 220–234.

[7] Benoît Libert & Jean-Jacques Quisquater. *Identity Based Encryption without Redundancy*, in *Applied Cryptography and Network Security (*ACNS*) 2005* (J. Ioannidis, A. Keromytis & M. Yung eds.), Lect. Notes Comput. Sci., vol. 3531, Springer, 2005, p. 285-300.

[8] Paulo Barreto, Benoît Libert, Noel McCullagh & Jean-Jacques Quisquater. *Efficient and Provably-Secure Identity-Based Signatures and Signcryption from Bilinear Maps*, in *Advances in Cryptology -* ASIACRYPT *2005*, (B. Roy ed.), Lect. Notes Comput. Sci., vol. 3788, Springer, 2005, p. 515-532.

[9] Julien Cathalo, Benoît Libert & Jean-Jacques Quisquater. *Efficient and Non-interactive Timed-Release Encryption*, in *Information and Communications Security, 7th International Conference, ICICS 2005* (J. Lopez, W. Mao, S. Qing & G. Wang eds.), Lect. Notes Comput. Sci., vol. 3783, Springer, 2004, p. 291-303.

[10] Benoît Libert & Jean-Jacques Quisquater. *On Constructing Certificateless Cryptosystems from Identity Based Encryption*, in *Public Key Cryptography (PKC) 2006* (M. Yung ed.), Lect. Notes Comput. Sci., vol. 3958, Springer, 2007, p. 474-490.

[11] Fabien Laguillaumie, Benoît Libert & Jean-Jacques Quisquater. *Universal Designated Verifier Signatures Without Random Oracles or Non-Black Box Assumptions*, in *Security and Cryptography for Networks (SCN) 2006*, (R. De Prisco & M. Yung eds.), Lect. Notes Comput. Sci., vol. 4116, Springer, 2007, p. 63–77.

[12] Benoît Libert, Jean-Jacques Quisquater & Moti Yung. *Efficient Intrusion-Resilient Signatures Without Random Oracles*, in *2nd International Conference on Information Security and Cryptology (Inscrypt 2006)*, Lect. Notes Comput. Sci., vol. 4318, Springer, 2006, p. 27–41.

[13] Benoît Libert, Jean-Jacques Quisquater & Moti Yung. *Parallel Key-Insulated Public Key Encryption Without Random Oracles*, in *Public Key Cryptography (PKC) 2007* (T. Okamoto & X. Wang eds.), Lect. Notes Comput. Sci., vol. 4450, Springer, 2007, p. 298–314.

[14] Benoît Libert & Jean-Jacques Quisquater. *Practical Time Capsule Signatures in the Standard Model from Bilinear Maps*, in *1st International Conference on Pairing-based Cryptography* – PAIRING *2007*, (T. Takagi & T. Okamoto eds.), Lect. Notes Comput. Sci., vol. 4575, Springer, 2007, p. 23-38.

[15] Benoît Libert, Jean-Jacques Quisquater & Moti Yung. *Forward-secure signatures in untrusted update environments*: *efficient and generic constructions*, in *14th ACM Conference on Computer and Communications Security (ACM-CCS) 2007* (S. De Capitani di Vimercati & P. Syverson eds.), ACM Press, 2007, p. 266–275.

[16] Alexander W. Dent, Benoît Libert & Kenneth G. Paterson. *Certificateless Encryption Schemes Strongly Secure in the Standard Model*, in *Public Key Cryptography (PKC) 2008* (R. Cramer ed.), Lect. Notes Comput. Sci., vol. 4939, Springer, 2008, p. 344-359.

[17] Benoît Libert & Damien Vergnaud. *Unidirectional Chosen-Ciphertext Secure Proxy Re-Encryption*, in *Public Key Cryptography (PKC) 2008* (R. Cramer ed.), Lect. Notes Comput. Sci., vol. 4939, Springer, 2008, p. 360-379.

[18] Benoît Libert & Damien Vergnaud. *Tracing Malicious Proxies in Proxy Re-Encryption*, in *2nd International Conference on Pairing-Based Cryptography (Pairing 2008)*, (S. Galbraith & K. Paterson eds.), Lect. Notes Comput. Sci., vol. 5209, Springer, 2008, p. 332-353.

[19] Benoît Libert & Damien Vergnaud. *Multi-Use Unidirectional Proxy Re-Signatures*, in *15th ACM Conference on Computer and Communications Security (ACM-CCS) 2008* (P. Syverson & S. Jha eds.), ACM Press, 2008, p. 511-520.

[20] Benoît Libert & Damien Vergnaud. *Towards Black-Box Accountable Authority IBE with Short Ciphertexts and Private Keys*, in *Public Key Cryptography (PKC) 2009*, (G. Tsudik & S. Jarecki eds.), Lect. Notes Comput. Sci., vol. 5443, Springer, 2009, p. 235-255.

[21] Benoît Libert & Damien Vergnaud. *Adaptive-ID Secure Revocable Identity-Based Encryption*, in *Topics in Cryptology* - CT-RSA *2009*, (M. Fischlin ed.), Lect. Notes Comput. Sci., vol. 5473, Springer, 2008, p. 1–15.

[22] Benoît Libert & Moti Yung. *Efficient Traceable Signatures in the Standard Model*, in *3rd International Conference on Pairing-Based Cryptography* - PAIRING *2009* (H. Shacham & B. Waters eds.), Lect. Notes Comput. Sci., vol. 5671, Springer, 2009, p. 187–205.

*[23] Julien Cathalo, Benoît Libert & Moti Yung. *Group Encryption*: *Non-Interactive Realization in the Standard Model*, in *Advances in Cryptology* - ASIACRYPT *2009* (M. Matsui ed.), Lect. Notes Comput. Sci., vol. 5912, Springer, 2009, p. 179–196.

[24] Benoît Libert & Damien Vergnaud. *Group Signatures with Verifier-Local Revocation and Backward Unlinkability in the Standard Model*, in *8th International Conference on Cryptology and Network Security (CANS 2009)*, (J. Garay & A . Miyaji eds.), Lect. Notes Comput. Sci., vol. 5888, Springer, 2009, p. 498–517.

[25] Benoît Libert & Moti Yung. *Concise Mercurial Vector Commitments and Independent Zero-Knowledge Sets with Short Proofs*, in *7th Theory of Cryptography Conference* - TCC *2010* (D. Micciancio ed.), Lect. Notes Comput. Sci., vol. 5978, Springer, 2010, p. 499–517.

[26] Benoît Libert & Moti Yung. *Dynamic Fully Forward-Secure Group Signatures*, in *5th ACM Symposium on Information, Computer and Communications Security (AsiaCCS) 2010* (D. Basin ed.), ACM Press, 2010, p. 70–81.

[27] Nuttapong Attrapadung & Benoît Libert. *Functional Encryption for Inner Product*: *Achieving Constant-Size Ciphertexts with Adaptive Security or Support for Negation*, in *Public Key Cryptography (PKC) 2010* (P. Nguyen & D. Pointcheval eds.), Lect. Notes Comput. Sci., vol. 6056, Springer, 2010, p. 384–402.

[28] David Galindo, Benoît Libert, Marc Fischlin, Georg Fuchsbauer, Anja Lehmann, Mark Manulis & Dominique Schröder. *Public-Key Encryption with Non-Interactive Opening*: *New Constructions and Stronger Definitions*, in *Africacrypt 2010* (D. Bernstein & T. Lange eds.), Lect. Notes Comput. Sci., vol. 6055, Springer, 2010, p. 333–350.

[29] Benoît Libert & Moti Yung. *Efficient Completely Non-Malleable Public Key Encryption*, in *37th International Colloquium on Automata, Languages and Programming (ICALP) 2010 - Track A (Algorithms, Complexity and Games)* (P. Spirakis ed.), Lect. Notes Comput. Sci., vol. 6198 , Springer, 2010, p. 127–139.

[30] Nuttapong Attrapadung & Benoît Libert. *Homomorphic Network Coding Signatures in the Standard Model*, in *Public Key Cryptography (PKC) 2011* (D. Catalano, N. Fazio, R. Gennaro & A. Nicolosi eds.), Lect. Notes Comput. Sci., vol. 6571, Springer, 2011, p. 17–34.

[31] Nuttapong Attrapadung, Benoît Libert & Elie de Panafieu. *Expressive Key-Policy Attribute-Based Encryption with Constant-Size Ciphertexts*, in *Public Key Cryptography (PKC) 2011*, (D. Catalano, N. Fazio, R. Gennaro & A. Nicolosi eds.), Lect. Notes Comput. Sci., vol. 6571, Springer, 2011, p. 90–108.

[32] Benoît Libert & Moti Yung. *Adaptively Secure Non-Interactive Threshold Cryptosystems*, in *38th International Colloquium on Automata, Languages and Programming (ICALP) 2011 - Track C (Models, Algorithms and Information Management)* (M. Henzinger, L. Aceto & J. Sgall eds.), Lect. Notes Comput. Sci., vol. 6756, Springer, p. 588–600, 2011.

[33] Brett Hemenway, Benoît Libert, Rafail Ostrovsky & Damien Vergnaud. *Lossy Encryption*: *Constructions from General Assumptions and Efficient Selective Opening Chosen Ciphertext Security*, in *Advances in Cryptology* - ASIACRYPT *2011* (D.-H. Lee & X. Wang eds.), Lect. Notes Comput. Sci., vol. 7073, Springer, p. 70–88, 2011.

[34] Marc Fischlin, Benoît Libert & Mark Manulis. *Non-Interactive and Re-Usable Universally Composable String Commitments with Adaptive Security*, in *Advances in Cryptology* - ASIACRYPT *2011* (D.-H. Lee & X. Wang eds.), Lect. Notes Comput. Sci., vol. 7073, p. 468–485, Springer, 2011.

[35] Malika Izabachène, Benoît Libert & Damien Vergnaud. *Block-Wise P-Signatures and Non-Interactive Anonymous Credentials with Efficient Attributes*, in *IMA International Conference on Cryptography and Coding* (IMACC) *2011* (L. Chen ed.), Lect. Notes Comput. Sci., vol. 7089, p. 431–450, Springer, 2011.

[36] Javier Herranz, Fabien Laguillaumie, Benoît Libert & Carla Ràfols. *Short Attribute-Based Signatures for Threshold Predicates*, in *Topics in Cryptology* - CT-RSA *2012* (O. Dunkelman ed.), Lect. Notes Comput. Sci., vol. 7178, p. 51–67, Springer, 2012.

[37] Benoît Libert & Moti Yung. *Non-Interactive CCA-Secure Threshold Cryptosystems with Adaptive Security*: *New Framework and Constructions*, in *9th Theory of Cryptography Conference (TCC 2012)* (R. Cramer ed.), Lect. Notes Comput. Sci., vol. 7194, p. 75–93, Springer, 2012.

*[38] Benoît Libert, Thomas Peters & Moti Yung. *Scalable Group Signatures with Revocation*, in *Advances in Cryptology* - EUROCRYPT *2012* (D. Pointcheval & T. Johansson eds.), Lect. Notes Comput. Sci., vol. 7237, p. 609–627, Springer, 2012.

[39] Benoît Libert, Kenneth G. Paterson & Elizabeth A. Quaglia. *Anonymous Broadcast Encryption*: *Adaptive Security and Efficient Constructions in the Standard Model*, in *Public Key Cryptography (PKC) 2012* (M. Fischlin, J. Buchmann & M. Manulis eds.), Lect. Notes Comput. Sci., vol. 7293, p. 206–224, Springer, 2012.

[40] Malika Izabachène & Benoît Libert. *Divisible E-Cash in the Standard Model*, in *5th International Conference on Pairing-Based Cryptography* - PAIRING *2012* (M. Abdalla & T. Lange eds.), Lect. Notes Comput. Sci. vol. 7708, p. 314–332, Springer, 2012.

*[41] Benoît Libert, Thomas Peters & Moti Yung. *Group Signatures with Almost-for-free Revocation*, in *Advances in Cryptology* - CRYPTO *2012* (R. Safavi-Naini & R. Canetti eds.), Lect. Notes Comput. Sci. vol. 7417, p. 571-589, Springer, 2012.

[42] Nuttapong Attrapadung, Benoît Libert & Thomas Peters. *Computing on Authenticated Data*: *New Privacy Definitions and Constructions*, in *Advances in Cryptology* - ASIACRYPT *2012* (X. Wang & K. Sako eds.), Lect. Notes Comput. Sci. vol. 7658, p. 367-385, Springer, 2012.

[43] Pooya Farshim, Benoît Libert, Kenneth G. Paterson & Elizabeth Quaglia. *Robust Encryption, Revisited*, in PUBLIC KEY CRYPTOGRAPHY *(PKC) 2013* (K. Kurosawa ed.), Lect. Notes Comput. Sci. vol. 7778, p. 352-368, Springer, 2013.

[44] Nuttapong Attrapadung, Benoît Libert & Thomas Peters. *Efficient Completely Context Hiding Quotable and Linearly Homomorphic Signatures*, in PUBLIC KEY CRYPTOGRAPHY *(PKC) 2013,* (K. Kurosawa ed.), Lect. Notes Comput. Sci. vol. 7778, p. 386-404, Springer, 2013.

[45] Marc Joye & Benoît Libert. *A Scalable Scheme for Privacy-Preserving Aggregation of Time-Series Data*, in FINANCIAL CRYPTOGRAPHY AND DATA SECURITY *(FC) 2013* (A. Sadeghi ed.), Lect. Notes Comput. Sci. vol. 7859, p. 111-125, Springer, 2013.

[46] Marc Joye & Benoît Libert. *Efficient Cryptosystems from 2^k-th Power Residue Symbols*, in *Advances in Cryptology* - EUROCRYPT *2013* (T. Johansson & P. Nguyen eds.), Lect. Notes Comput. Sci. vol. 7881, p. 76-92, Springer, 2013.

*[47] Benoît Libert, Thomas Peters, Marc Joye & Moti Yung. *Linearly Homomorphic Structure-Preserving Signatures and their Applications*, in *Advances in Cryptology* - CRYPTO *2013* (R. Canetti & J. Garay eds.), Lect. Notes Comput. Sci. vol. 8043, p. 289-307, Springer, 2013.

[48] Fabien Laguillaumie, Adeline Langlois, Benoît Libert & Damien Stehlé. *Lattice-Based Group Signatures with Logarithmic Signature Size*, in *Advances in Cryptology* - ASIACRYPT *2013* (K. Sako & P. Sarkar eds.), Lect. Notes Comput. Sci. vol. 8270, p. 41-61, Springer, 2013.

[49] Benoît Libert & Marc Joye. *Group Signatures with Message-Dependent Opening in the Standard Model*, in *Topics in Cryptology* - CT-RSA *2014* (J. Benaloh ed.), Lect. Notes Comput. Sci. vol. 8366, p. 286-306, Springer, 2014.

[50] Alex Escala, Javier Herranz, Benoît Libert & Carla Ràfols. *Identity-Based Lossy Trapdoor Functions*: *New Definition, Hierarchical Extensions, and Implications*, in *Public Key Cryptography (*PKC*) 2014* (H. Krawczyk ed.), Lect. Notes Comput. Sci. vol. 8383, p. 239-256, Springer, 2014.

[51] Benoît Libert, Moti Yung, Marc Joye & Thomas Peters. *Traceable Group Encryption*, in *Public Key Cryptography (*PKC*) 2014* (H. Krawczyk ed.), Lect. Notes Comput. Sci. vol. 8383, p. 592-610, Springer, 2014.

*[52] Benoît Libert, Thomas Peters, Marc Joye & Moti Yung. *Non-Malleability from Malleability*: *Simulation-Sound Quasi-Adaptive NIZK Proofs and CCA2-Secure Encryption from Homomorphic Signatures*, in *Advances in Cryptology* - EUROCRYPT *2014* (P. Nguyen & E. Oswald eds.), Lect. Notes Comput. Sci. vol. 8441, p. 514-532, Springer, 2014.

[53] Benoît Libert, Marc Joye & Moti Yung. *Born and Raised Distributively*: *Fully Distributed Non-Interactive Adaptively-Secure Threshold Signatures with Short Shares*, in *33rd Symposium on Principles of Distributed Computing (PODC 2014)*, (S. Dolev ed.), p. 303-312, ACM Press, 2014.

[54] Benoît Libert, Marc Joye, Moti Yung and Thomas Peters. *Concise Multi-Challenge CCA-Secure Encryption and Signatures with Almost Tight Security*. In *Advances in Cryptology* - ASIACRYPT *2014* (P. Sarkar & T. Iwata eds.), Lect. Notes Comput. Sci. series, Springer, 2014.

CHAPTER 1

Background

This chapter briefly recalls several notions and definitions that are related to non-interactive zero-knowledge proofs and structure-preserving cryptography. These reminders will make it easier to explain the results of subsequent chapters.

1.1 Bilinear Maps and Hardness Assumptions

Definition 1 (Bilinear Groups). *A bilinear group system is a tuple* $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, g_1, g_2)$ *where* $\mathbb{G}_1$, $\mathbb{G}_2$ *and* $\mathbb{G}_T$ *are cyclic abelian groups of prime order* $p > 2^\lambda$, *where* $\lambda \in \mathbb{N}$ *is a security parameter, generated respectively by* $g_1 \in \mathbb{G}_1$, $g_2 \in \mathbb{G}_2$ *and* $e(g_1, g_2) \in \mathbb{G}_T$. *If* $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ *is a non-degenerated bilinear form, for all* $X \in \mathbb{G}_1$, *for all* $Y \in \mathbb{G}_2$, *for all* $a, b \in \mathbb{Z}_p$,

$$e(X^a, Y^b) = e(X, Y)^{ab}. \tag{1.1}$$

For a security parameter λ, *it is assumed that bilinear groups are efficiently samplable so that* $p > 2^\lambda$. *Mainly, there are three types of elliptic-curve instantiations [115]:*

Type I: *where* $\mathbb{G}_1 = \mathbb{G}_2$ *and* $g_1 = g_2$. *We usually refer to Type-I instances as* symmetric pairings. *We denote by* $(p, \mathbb{G}, \mathbb{G}_T, e, g) \leftarrow \Lambda(\lambda)$ *the generation of this setting.*

Type II: *where* $\mathbb{G}_1 \neq \mathbb{G}_2$ *and an efficient isomorphism* $\psi : \mathbb{G}_2 \to \mathbb{G}_1$ *is available but none is efficiently computable from* $\mathbb{G}_1$ *to* $\mathbb{G}_2$.

Type III: *where* $\mathbb{G}_1 \neq \mathbb{G}_2$ *but no efficient isomorphism between* $\mathbb{G}_1$ *and* $\mathbb{G}_2$ *is efficiently computable in either direction.*

Type III elliptic curves have the most efficient instantiations and admit a smaller representation of $\mathbb{G}_1$-elements than those of $\mathbb{G}_2$-elements. At a same bit-security level, $\mathbb{G}$-elements of Type I elliptic curves have an intermediate size relatively to Type III curves. In the following chapters we will often use Type I groups in order to keep the description of systems as simple as possible. We will, however, mention extensions to Type II or Type III pairings whenever they are possible.

1.1.1 Algorithmic Assumptions

All the schemes proposed in the thesis have their security based on one or several of the following assumptions. To simplify their descriptions we will say "a problem is hard in a group $\mathbb{G}$" for "a problem is hard relatively to the generation of $\mathbb{G}$", which means that the

probability to efficiently solve the problem is negligible in the security parameter λ where the random coins are taken over the distribution of the λ-bit length instance of the problem and the distribution that generates the group $\mathbb{G}$ whose cardinality is at least 2^λ. In symmetric bilinear groups, the latter distribution is that of $\Lambda(\lambda)$ such that $(p, \mathbb{G}, \mathbb{G}_T, e, g) \leftarrow \Lambda(\lambda)$.

As a warm-up, we start with the weakest assumption of the thesis. Breaking this assumption means breaking all the other ones since the underlying problem is the hardest to solve. For a set S, $s \xleftarrow{\$} S$ means that s is equally-likely sampled from S.

Assumption 1 (DLOG). *The* **Discrete Logarithm** *(DLOG) problem in a cyclic group $(p, \mathbb{G}, g)$, is to compute $a \in \mathbb{Z}_p$ such that $h = g^a$ for some $h \xleftarrow{\$} \mathbb{G}$. The* **Discrete Logarithm Assumption** *asserts that the DLOG problem is hard in $\mathbb{G}$.*

Assumption 2 (CDH). *In a cyclic group $\mathbb{G} = \langle g \rangle$ of order p, the* **Computational Diffie-Hellman** *(CDH) problem is, given $(g, g^a, g^b) \in \mathbb{G}^3$, for some $a, b \xleftarrow{\$} \mathbb{Z}_p^*$, to compute $g^{ab} \in \mathbb{G}$. The* **Computational Diffie-Hellman Assumption** *posits the intractability of the CDH problem in the group $\mathbb{G}$.*

In some cases, reductions from the hardness of CDH may be difficult to obtain. In such situations, the following assumption is sometimes convenient to use.

Assumption 3 (Flex-CDH [163]). *The* ***Flexible Diffie-Hellman Assumption*** *(Flex-CDH) in $\mathbb{G}$ asserts the hardness of finding a non-trivial triple $(g^\mu, g^{a \cdot \mu}, g^{ab \cdot \mu}) \in (\mathbb{G} \backslash \{1_\mathbb{G}\})^3$, for some non-zero $\mu \in \mathbb{Z}_p^*$, given $(g, g^a, g^b) \xleftarrow{\$} \mathbb{G}$.*

When it comes to proving indistinguishability-based security, the hardness of decisional problems often come in handy. A well-known decisional assumption is the difficulty of the Decision Diffie-Hellman DDH problem which amounts to recognizing the solution of a CDH instance.

Assumption 4 (DDH). *In a cyclic group $\mathbb{G} = \langle g \rangle$ of order p, the* **Decision Diffie-Hellman** *(DDH) problem, is to distinguish the distributions (g, g^a, g^b, g^{ab}) and (g, g^a, g^b, g^c), with $a, b \xleftarrow{\$} \mathbb{Z}_p$, $c \xleftarrow{\$} \mathbb{Z}_p$. The* **Decision Diffie-Hellman Assumption** *posits that DDH is hard in $\mathbb{G}$. The DDH assumption holds in $\mathbb{G}$ if, for any PPT distinguisher $\mathcal{A}$, it holds that*

$$\mathbf{Adv}_{\mathcal{A}}^{\mathrm{DDH}}(\lambda) = \Big| \Pr[\mathcal{A}(g, g^a, g^b, g^{ab}) = 1 \mid a, b \xleftarrow{R} \mathbb{Z}_p] - \Pr[\mathcal{A}(g, g^a, g^b, g^c) = 1 \mid a, b, c \xleftarrow{R} \mathbb{Z}_p] \Big| \in \mathsf{negl}(\lambda),$$

where the probabilities are taken over all coin tosses.

In symmetric bilinear groups $(p, \mathbb{G}, \mathbb{G}_T, e, g) \leftarrow \Lambda(\lambda)$, the DDH assumption does not hold. Indeed, given $(g, h, f, T) \in \mathbb{G}^4$, deciding whether $T = f^{\log_g(h)}$ can be done efficient by checking whether $e(g, T) = e(h, f)$.

On the other hand, the DDH assumption is believed [234] to hold in $\mathbb{G}_1$ for asymmetric bilinear groups $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, g_1, g_2)$ of Type II since there is no apparent way to invert the isomorphism $\psi : \mathbb{G}_2 \to \mathbb{G}_1$. In Type III configurations $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, g_1, g_2)$ (where no isomorphism is efficiently computable in either direction between $\mathbb{G}_1$ and $\mathbb{G}_2$), the DDH assumption is believed to hold in both $\mathbb{G}_1$ and $\mathbb{G}_2$. The simultaneous intractability of DDH

in $\mathbb{G}_1$ and $\mathbb{G}_2$ for Type III pairings is called Symmetric eXternal Diffie-Hellman assumption (SXDH) [234].

In symmetric pairings, the hardness of the DLIN problem appears as a reasonable assumption to rely on.

Assumption 5 (DLIN [44]). *In a cyclic group $\mathbb{G} = \langle g \rangle$ of order p, the* **Decision Linear** *(DLIN) problem is to distinguish the distributions $(g^a, g^b, g^{ac}, g^{bd}, g^{c+d})$ and $(g^a, g^b, g^{ac}, g^{bd}, g^z)$, with $a, b, c, d \xleftarrow{\$} \mathbb{Z}_p$, $z \xleftarrow{\$} \mathbb{Z}_p$. The* **Decision Linear Assumption** *is the intractability of DLIN for any PPT distinguisher $\mathcal{D}$. The advantage of a distinguisher is defined analogously to the DDH case.*

Equivalently, for random group elements $g, h, f \leftarrow \mathbb{G}^3$, the DLIN assumption is the hardness of deciding whether an given triple $(f^c, h^d, Z) \in \mathbb{G}^3$, for unknown $(c, d) \in \mathbb{Z}_p^2$, satisfies $(f^c, h^d, Z) \in \mathsf{span}\langle (f, 1, g), (1, h, g) \rangle$ (i.e., $Z = g^{c+d}$), where span stands for the linear span of two or more vectors.

Assumption 6 (DP [4]). *In asymmetric bilinear groups $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, g_1, g_2)$, the* ***Double Pairing*** *(DP) problem is, given $g_z, g_r \xleftarrow{\$} \mathbb{G}_1$, to find a non-trivial $(z, r) \in (\mathbb{G}_2 \backslash \{1_{\mathbb{G}_2}\})^2$ satisfying $1_{\mathbb{G}_T} = e(g_z, z) \cdot e(g_r, r)$. The* **Double Pairing Assumption** *asserts that the DBP problem is hard in $\mathbb{G}$.*

It is easy to see that the DP assumption is implied by the DDH assumption in $\mathbb{G}_1$. Given a DDH instance $(g_z, g_r, g_z^\theta, g_r^{\theta'})$, for any non-trivial pair $(z, r) \in \mathbb{G}_2^2$ satisfying the equality $e(g_z, z) \cdot e(g_r, r) = 1_{\mathbb{G}_T}$, we have $\theta = \theta'$ if and only if $e(g_z^\theta, z) \cdot e(g_r^{\theta'}, r) = 1_{\mathbb{G}_T}$.

In symmetric pairings, the DP and DDH problems are both easy. However, the DP assumption has an analogue, which we introduced in [81], that seems to hold in Type I pairings. This assumption is called Simultaneous Double Pairing (SDP) and, as shown in [81], it is implied by DLIN.

Assumption 7 (SDP [81]). *The* ***Simultaneous Double Pairing Problem*** *(SDP) in a symmetric bilinear group $(p, \mathbb{G}, \mathbb{G}_T, e, g) \leftarrow \Lambda(\lambda)$ is, given $g_z, g_r, h_z, h_u \xleftarrow{\$} \mathbb{G}^4$, to find $(z, r, u) \in \mathbb{G}^3$ satisfying the equalities*

$$1_{\mathbb{G}_T} = e(g_z, z) \cdot e(g_r, r), \qquad 1_{\mathbb{G}_T} = e(h_z, z) \cdot e(h_u, u). \tag{1.2}$$

The **Simultaneous Double Pairing Assumption** *is the hardness of the SDP problem.*

The assumption can be generalized to asymmetric pairing configurations $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$. If g_z, g_r, h_z, h_u are in $\mathbb{G}_1$ (resp. $\mathbb{G}_2$), finding a non-trivial $(z, r, u) \in \mathbb{G}_2^3$ (resp. $(z, r, u) \in \mathbb{G}_1^3$) such that (resp. $e(z, g_z) \cdot e(r, g_r) = e(z, h_z) \cdot e(u, h_u) = 1_{\mathbb{G}_T}$) is at least as hard as breaking the DLIN assumption in $\mathbb{G}_1$ (resp. $\mathbb{G}_2$).

In the symmetric setting, the connection between SDP and DLIN was observed [81] by noticing that, given a DLIN instance $(g_r, h_u, g, g_r^{\theta_1}, h_u^{\theta_2}, T)$ where either $T = g^{\theta_1 + \theta_2}$ or $T \in_R \mathbb{G}$, for any triple $(z, r, u) \in \mathbb{G}$ such that $e(g_r^{\theta_1}, z) \cdot e(g_r, r) = e(h_u^{\theta_2}, z) \cdot e(h_u, u) = 1_{\mathbb{G}_T}$, we have the equivalence

$$T = g^{\theta_1 + \theta_2} \quad \Leftrightarrow \quad e(T, z) \cdot e(g, r \cdot u) = 1_{\mathbb{G}_T}.$$

The DLIN assumption can be generalized as the problem of deciding whether $K + 1$ vectors of dimension $K + 1$ are linearly independent.

Assumption 8 (*K*-LIN [235, 143]). *In a cyclic group* $\mathbb{G} = \langle g \rangle$ *of order* p*, the* K**-Linear** *(K-LIN) problem is to distinguish the distributions*

$$\{(g_1^{a_1}, g_2^{a_2}, \ldots, g_K^{a_K}, g^{\sum_{i=1}^{K} a_i}) \mid g_1, \ldots, g_K \xleftarrow{\$} \mathbb{G},\ a_1, \ldots, a_K \xleftarrow{\$} \mathbb{Z}_p\}$$

and

$$\{(g_1^{a_1}, g_2^{a_2}, \ldots, g_K^{a_K}, g^{z}) \mid g_1, \ldots, g_K \xleftarrow{\$} \mathbb{G},\ a_1, \ldots, a_K, z \xleftarrow{\$} \mathbb{Z}_p\}.$$

The K-linear assumption is the infeasibility of K-LIN for any PPT algorithm.

The DDH and DLIN assumptions can be seen as special cases of the K-LIN assumption for $K = 1$ and $K = 2$, respectively. The difficulty of the problem is believed to increase with the dimension K. In the generic group model, it was shown [235, 143] that, for each $K > 1$, the K-linear problem remains hard in the presence of an oracle solving $(K-1)$-linear instances.

The SDP assumption as a similar generalization, which is implied by the K-linear assumption in the same way as SDP is implied by DLIN.

Assumption 9. *The* **Simultaneous** K**-wise Pairing** *(K-SDP) problem is, given a random tuple*

$$(g_{1,z}, \ldots, g_{K,z}, g_{1,r}, \ldots, g_{K,r}) \in_R \mathbb{G}^{2K},$$

to find a non-trivial vector $(z, r_1, \ldots, r_K) \in \mathbb{G}^{K+1}$ *such that*

$$e(g_{j,z}, z) \cdot e(g_{j,r}, r_j) = 1_{\mathbb{G}_T} \qquad j \in \{1, \ldots, K\} \tag{1.3}$$

and $z \neq 1_{\mathbb{G}}$.

Given a K-linear instance $(g_{1,r}, \ldots, g_{k,r}, g_{1,r}^{a_1}, \ldots, g_{K,r}^{a_K}, \eta) \in \mathbb{G}^{2K+1}$, for any non-trivial tuple $(z, r_1, \ldots, r_K)$ satisfying $e(g_{j,r}^{a_j}, z) \cdot e(g_{j,r}, r_j) = 1_{\mathbb{G}_T}$ for each $j \in \{1, \ldots, k\}$, we have

$$\eta = g^{\sum_{j=1}^{K} a_j} \qquad \Leftrightarrow \qquad e(g, \prod_{j=1}^{K} r_j) \cdot e(z, \eta) = 1_{\mathbb{G}_T}.$$

Hence, any algorithm solving K-SDP with non-negligible probability implies a K-linear distinguisher.

All the above assumptions can be classified in the category of *simple* assumptions [249]. By "simple assumption", we mean an assumption which is simultaneously falsifiable[1] [206] and with a description made of a constant number of group elements. In particular, the number of input elements does not depend on the number of queries made by the adversary or any feature (such as the maximal number of users in a system) of a specific cryptographic scheme. Simple assumptions are usually deemed more reliable than so-called q-type assumptions, which are parametrized and variable-length assumptions.

In some applications, more efficient schemes may be obtained by relying on a family of q-type assumptions. While these assumptions are usually falsifiable, the number of group elements in a problem instance depends on a parameter q determined by the cryptographic system (e.g., the maximal number of members in a group of users) or the power of adversary (via the number of queries). The strength of the assumption thus depends on the desired scalability of the considered protocol or the resources made available to the adversary. However, the assumptions described in this section all resist generic adversaries [237].

[1] Namely, it should be possible to publicize a problem instance as a challenge and efficiently check the correctness of any candidate solution to this challenge.

q-type assumptions We also rely on assumptions that can be seen as non-interactive variants of "one-more" problems, where the goal of the problem solver is to find a new solution given q initial solutions. However, a difference between q-type problems and one-more problems is that, in in the former, the solver is given q inputs at once at the beginning instead of dynamically interacting with an oracle. Still, the length and the strength of the assumption are determined by a parameter q, which usually depends on the scalability of the system or the power of the adversary. For example, in the first use of the q-Strong Diffie-Hellman assumption [41], q was the number of signing queries made by the adversary.

Assumption 10 (q-SDH [41])**.** *The q-**Strong Diffie-Hellman problem** (q-SDH) in a group $(p, \mathbb{G}, g)$ is, given $(g, g^a, \ldots, g^{(a^q)})$, for some $a \xleftarrow{\$} \mathbb{Z}_p$, to find a pair $(g^{1/(a+s)}, s) \in \mathbb{G} \times \mathbb{Z}_p$. The q-**Strong Diffie-Hellman Assumption** asserts the hardness of the q-SDH problem.*

In [56], Boyen and Waters considered the following variant of the q-SDH assumption.

Assumption 11 ([56])**.** *The q-**Hidden Strong Diffie-Hellman problem** (q-HSDH) in $\mathbb{G}$ consists in, given $(g, \Omega = g^\omega, u) \xleftarrow{\$} \mathbb{G}^3$ and triples $\{(g^{1/(\omega+s_i)}, g^{c_i}, u^{c_i})\}_{i=1}^q$ with $c_1, \ldots, c_q \xleftarrow{\$} \mathbb{Z}_p$, finding another triple $(g^{1/(\omega+c)}, g^c, u^c)$ such that $c \neq c_i$ for $i = 1, \ldots, q$.*

While stronger than the q-SDH assumption, the q-HSDH assumption was shown [56] to hold in generic bilinear groups.

The following assumption has been used to prove the security of a constant-size structure-preserving signature [4, 6] scheme that allows signing vectors of group elements. It will also serve as a building block for some of our constructions in the forthcoming chapters.

Assumption 12 (q-SFP [6])**.** *The q-**Simultaneous Flexible Pairing Problem** (q-SFP) in a symmetric bilinear group $(p, \mathbb{G}, \mathbb{G}_T, e, g)$ is, given $g_z, h_z, g_r, h_r, a, \tilde{a}, b, \tilde{b} \in \mathbb{G}$ and $q \in \mathsf{poly}(\lambda)$ tuples $(z_j, r_j, s_j, t_j, u_j, v_j, w_j) \in \mathbb{G}^7$ such that*

$$\begin{aligned} e(a, \tilde{a}) &= e(g_z, z_j) \cdot e(g_r, r_j) \cdot e(s_j, t_j) \\ e(b, \tilde{b}) &= e(h_z, z_j) \cdot e(h_r, u_j) \cdot e(v_j, w_j), \end{aligned} \tag{1.4}$$

*to find a new tuple $(z^\star, r^\star, s^\star, t^\star, u^\star, v^\star, w^\star) \in \mathbb{G}^7$ satisfying relation (1.4) and such that $z^\star \neq 1_\mathbb{G}$ and $z^\star \neq z_j$ for $j \in \{1, \ldots, q\}$. The q-**Simultaneous Flexible Pairing** assumption states that the q-SFP problem is intractable in $\mathbb{G}$.*

Assumption 13 (q-DHE [49])**.** *The q-**Diffie-Hellman Exponent Problem** (q-DHE) in a cyclic group $(p, \mathbb{G}, g)$ is, given $(g, g_1, \ldots, g_q, g_{q+2}, \ldots, g_{2q}) \in \mathbb{G}^{2q}$ such that $g_i = g^{(\alpha^i)}$ for each i and where $\alpha \xleftarrow{\$} \mathbb{Z}_p^*$, to compute the missing element $g_{q+1} = g^{(\alpha^{q+1})}$. The hardness of the q-DHE problem is referred to as the q-**Diffie-Hellman Exponent** assumption in $\mathbb{G}$.*

The latter assumption and the q-SDH assumption are somewhat incomparable. On one hand, the q-DHE assumption is stronger as the adversary is given more input elements for the same parameter q. On the other hand, unlike the q-SDH problem, any instance of the q-DHE problem has only one possible answer.

As observed in [66], the q-DHE problem is not easier than the q-Bilinear Diffie-Hellman Exponent (q-BDHE) problem defined by Boneh, Gentry and Waters [49], which is to compute

$e(g,h)^{(\alpha^{q+1})}$ on input of the same values and the additional element $h \in \mathbb{G}$. The generic hardness of q-DHE thus follows from the generic security of the family of assumptions analyzed by Boneh, Boyen and Goh [43].

We also appeal to a stronger variant of Assumption 13, which was defined in [145], where its generic hardness was proved. While the Flex-CDH assumption relaxes the resolution of the CDH problem, the following assumption relaxes the q-DHE problem in a similar way.

Assumption 14 (q-Flex-DHE)**.** *In a cyclic group $\mathbb{G} = \langle g \rangle$ of prime order p, the* **Flexible q-Diffie-Hellman Exponent** *(q-FlexDHE) problem is, given $(g, g_1, \ldots, g_q, g_{q+2}, \ldots, g_{2q}) \in \mathbb{G}^{2q}$ where $g_i = g^{(\alpha^i)}$ for each i and with $\alpha \xleftarrow{\$} \mathbb{Z}_p^*$, to find a triple $(g^\mu, g_{q+1}^\mu, g_{2q}^\mu) \in (\mathbb{G}\backslash\{1_\mathbb{G}\})^3$, for some non-zero $\mu \in \mathbb{Z}_p^*$ and where $g_{q+1} = g^{(\alpha^{q+1})}$. The* **Flexible q-Diffie-Hellman Exponent** *assumption is the hardness of the q-FlexDHE problem for any PPT adversary.*

1.2 Non-Interactive Zero-Knowledge and Witness Indistinguishable Proofs

Zero-knowledge proofs [127, 126] allow a prover to convince a verifier that a given statement x belongs to some specific language $\mathcal{L}$ without revealing anything beyond the fact that $x \in \mathcal{L}$. In a proof system for an NP language, the prover uses an additional private input w, called the *witness*, which allows *efficiently* generating a convincing proof. This witness is generally hard-to-compute for the verifier since, otherwise, the latter could get convinced without any help from the prover.

1.2.1 Definition and Security Notions

Let $\mathcal{V}$ be a set whose elements are efficiently recognizable. A family of relations $\mathcal{R}$ defines a hard-to-invert NP language $\mathcal{L} \subsetneq \mathcal{V}$ if, for a security parameter λ, given the description of a relation $R \leftarrow \mathcal{R}(\lambda)$, there exists an efficient algorithm for sampling a pair (x, w), made of a statement x and a witness w, such that $R(x, w) = 1$. Moreover, given only the statement $x \in \mathcal{L} := \{x \in \mathcal{V} \,|\, \exists w : R(x, w) = 1\}$, it is computationally hard to compute a witness w such that $R(x, w) = 1$.

A language $\mathcal{L} \subset \mathcal{V}$ is said *hard-to-decide* if no PPT algorithm can distinguish random elements of $\mathcal{L}$ from random elements of $\mathcal{V}\backslash\mathcal{L}$. When speaking of a *hard language*, we mean a language which is hard-to-decide. For example, for fixed generators $(g, h) \in \mathbb{G}^2$ in a cyclic group $\mathbb{G}$, the Diffie-Hellman relation $R((g_1, g_2), w) := \big((g_1, g_2) = (g^w, h^w)\big)$ defines a hard-to-decide language in $\mathcal{V} = \mathbb{G}^2$ as long as the DDH assumption holds in $\mathbb{G}$.

Proving a statement $x \in \mathcal{L}$ can be done by demonstrating the existence of w such that that $R(x, w) = 1$. Also, the relation R can be defined so as to take as input a set of public parameters $\mathsf{pp} \leftarrow \mathsf{Setup}(\lambda)$, so that R is generated as $R \leftarrow \mathcal{R}(\mathsf{pp})$ rather than simply from the security parameter.

In non-interactive zero-knowledge proof systems, there is no online conversation between the prover and the verifier: each proof consists of a single message from the former to the latter. In addition to common public parameters pp, the prover and the verifier both take as input a common reference string crs which can be seen as another set of public parameters generated by a trusted party. In some cases, the public parameters pp can be part of the common reference string crs but it will be useful to separate them.

Definition 2 (NIZK Proofs [38, 37])**.** *A non-interactive zero-knowledge (NIZK) proof system* $\Pi_{\mathcal{P}}$ *for a family of hard relations* $\mathcal{R}$ *is a tuple of algorithms* $(\mathsf{Setup}_{\mathcal{P}}, \mathsf{CRS\text{-}Gen}_{\mathcal{P}}, \mathsf{Prove}, \mathsf{Verify}_{\mathcal{P}})$.

Setup$_{\mathcal{P}}(1^{\lambda})$*: from the security parameter* λ*, generates the public parameters* pp *of the proof system;*

CRS-Gen$_{\mathcal{P}}(\mathsf{pp})$*: takes in* pp *and outputs the common reference string* crs *that are public elements helping performing a proof for* $R \leftarrow \mathcal{R}(\mathsf{pp})$

Prove(crs, x, w)*: computes a proof* π *for* x *using the public* crs *and the private witness* w*.*

Verify$_{\mathcal{P}}(\mathsf{crs}, x, \pi)$*: returns either* 1 *or* 0 *if* π *is a valid proof associated to the language* L_R*.*

A NIZK proof system $\Pi_{\mathcal{P}}$ *has the following properties:*

Perfect Completeness: *for any PPT adversary* $\mathcal{A}_1$*,*

$$\Pr[\mathsf{pp} \leftarrow \mathsf{Setup}_{\mathcal{P}}(\lambda);\ \mathsf{crs} \leftarrow \mathsf{CRS\text{-}Gen}_{\mathcal{P}}(\mathsf{pp});\ (x, w) \leftarrow \mathcal{A}_1(\mathsf{crs});\ \pi \leftarrow \mathsf{Prove}(\mathsf{crs}, x, w) : \mathsf{Verify}(\mathsf{crs}, x, \pi) = 0 \ \wedge\ R(x, w) = 1] = 0,$$

Computational Soundness: *for any PPT adversary* $\mathcal{A}_2$*,*

$$\Pr[\mathsf{pp} \leftarrow \mathsf{Setup}_{\mathcal{P}}(\lambda);\ \mathsf{crs} \leftarrow \mathsf{CRS\text{-}Gen}_{\mathcal{P}}(\mathsf{pp});\ (x, \pi) \leftarrow \mathcal{A}_2(\mathsf{crs}) : \mathsf{Verify}_P(\mathsf{crs}, x, \pi) = 1 \ \wedge\ (\nexists w : R(x, w) = 1)] \in \mathsf{negl}(\lambda),$$

The notion of **statistical** *soundness is obtained by allowing* $\mathcal{A}_2$ *to be a computationally unbounded adversary. Non-interactive proof systems where the soundness property is only guaranteed in the computational sense are often called* **arguments***.*

Zero-Knowledge: *there exists a PPT simulator* $(\mathsf{S}_1, \mathsf{S}_2)$ *such that, for any PPT adversary* $\mathcal{A}_3$*,*

$$\Pr[\mathsf{pp} \leftarrow \mathsf{Setup}_{\mathcal{P}}(\lambda);\ (\mathsf{crs}, \tau) \leftarrow \mathsf{S}_1(\mathsf{pp}) : \mathcal{A}_3^{\mathsf{S}_2(\mathsf{crs}, \tau, ., .)}(\mathsf{crs}) = 1] \approx \Pr[\mathsf{pp} \leftarrow \mathsf{Setup}_{\mathcal{P}}(\lambda);\ \mathsf{crs} \leftarrow \mathsf{CRS\text{-}Gen}_{\mathcal{P}}(\mathsf{pp}) : \mathcal{A}_3^{\mathcal{P}(\mathsf{crs}, ., .)}(\mathsf{crs}) = 1],$$

- $\mathcal{P}(\mathsf{crs}, ., .)$ *emulates the actual prover. It takes as input a pair* (x, w) *and outputs a proof* π *if* $(x, w) \in R$*. Otherwise, it outputs* $\perp$*,*
- $\mathsf{S}_2(\mathsf{crs}, \tau, ., .)$ *is an oracle that takes as input* (x, w) *and outputs a simulated proof* $\pi \leftarrow \mathsf{S}_2(\mathsf{crs}, \tau, x)$ *if* $(x, w) \in R$ *and* $\perp$ *if* $(x, w) \notin R$*. Importantly,* π *is computed without using the witness* w *if* $(x, w) \in R$*.*

In some cases, the public parameters are generated at the same time as the CRS crs by the **CRS-Gen**$_{\mathcal{P}}$ algorithm. The above definition allows them to be generated separately in order to capture Quasi-Adaptive NIZK proofs, which will be discussed later on.

The above definition of the zero-knowledge (ZK) property is computational since $\mathcal{A}_3$ is restricted to be efficient. By removing this restriction and allowing for an all powerful $\mathcal{A}_3$, we can capture statistical or perfect ZK if the distributions are statistically close or perfectly indistinguishable, respectively.

Intuitively, the zero-knowledge property captures that, for any $x \in \mathcal{L}$, the only information revealed by an honestly generated proof π is the same as a simulated proof that

is generated without using w. Hence, the verifier learns nothing beyond the truth of the proven statement $x \in \mathcal{L}$. In particular, no information about the witness w is revealed. In many applications, a weaker notion called *witness-indistinguishability* suffices. It requires that, when a given statement $x \in \mathcal{L}$ admits at least two distinct witnesses w_0, w_1 such that $R(x, w_0) = R(x, w_1) = 1$, the distribution of a proof π for x does not depend on which witness is used to compute π. However, π may not be computable by an efficient simulator $(\mathsf{S}_1, \mathsf{S}_2)$ as in the zero-knowledge property.

Definition 3 (Witness Indistinguishability)**.** *A non-interactive proof system* $\Pi_{\mathcal{P}} = (\mathsf{Setup}_{\mathcal{P}}, \mathsf{CRS\text{-}Gen}_{\mathcal{P}}, \mathsf{Prove}, \mathsf{Verify}_{\mathcal{P}})$ *for a hard language* $\mathcal{L}$ *is witness-indistinguishable (NIWI) if, for any PPT adversary* $(\mathcal{A}_4, \mathcal{A}_5)$*, for any* $\mathsf{pp} \leftarrow \mathsf{Setup}_{\mathcal{P}}(\lambda)$ *and* $\mathsf{crs} \leftarrow \mathsf{CRS\text{-}Gen}_{\mathcal{P}}(\mathsf{pp})$*,*

$$\begin{aligned}\Pr[(x, w_0, w_1, \mathsf{st}) \leftarrow \mathcal{A}_4(\mathsf{crs}); \pi \leftarrow \mathsf{Prove}(\mathsf{crs}, x, w_0) : \mathcal{A}_5(\pi, \mathsf{st}) = 1] \\ \approx \quad \Pr[(x, w_0, w_1, \mathsf{st}) \leftarrow \mathcal{A}_4(\mathsf{crs}); \pi \leftarrow \mathsf{Prove}(\mathsf{crs}, x, w_1) : \mathcal{A}_5(\pi, \mathsf{st}) = 1],\end{aligned}$$

where $(x, w_0), (x, w_1) \in R$*.*

For hard languages that admit efficient an zero-knowledge simulator, the latter can always use its simulation trapdoor to compute proof for true statements without knowing the witnesses. The trapdoor can also be used for computing proofs for false statements, *i. e.*proofs that satisfy the verification test although $x \notin \mathcal{L}$. This property is a very useful theoretic tool for building chosen-ciphertext-secure cryptosystems, for example based on the Naor-Yung/Sahai [208, 231] paradigm. The ability to simulate proofs for false statements should be used with caution as observing such fake proofs may help the adversary prove false statements by itself. The notion of simulation-soundness, as introduced by Sahai [231] captures that seeing a polynomial number of fake proofs should not break the soundness property.

Definition 4 (Simulation-Soundness [231])**.** *A non-interactive proof system* $\Pi_{\mathcal{P}} = (\mathsf{Setup}_{\mathcal{P}}, \mathsf{CRS\text{-}Gen}_{\mathcal{P}}, \mathsf{Prove}, \mathsf{Verify}_{\mathcal{P}})$ *for a hard language* $\mathcal{L}$ *is simulation-sound if there exists a PPT simulator* $(\mathsf{S}_1, \mathsf{S}_2)$ *such that, for any PPT adversary* $\mathcal{A}_6$*,*

$$\begin{aligned}\Pr[\mathsf{pp} \leftarrow \mathsf{Setup}_{\mathcal{P}}(\lambda);\ (\mathsf{crs}, \tau) \leftarrow \mathsf{S}_1(\mathsf{pp}); (x, \pi) \leftarrow \mathcal{A}_6^{\mathsf{S}_2(\mathsf{crs}, \tau, ., .)}(\mathsf{crs}) : \\ \mathsf{Verify}_P(\mathsf{crs}, x, \pi) = 1 \ \wedge \ \neg(\exists w : R(x, w) = 1) \ \wedge \ (x, \pi) \notin Q] \in \mathsf{negl}(\lambda)\end{aligned}$$

where the adversary is granted access to an oracle $\mathsf{S}_2(\mathsf{crs}, \tau, .)$ *that takes as input a statement* x *(where* x *may be outside* $\mathcal{L}$*) and outputs a simulated proof* $\pi \leftarrow \mathsf{S}_2(\mathsf{crs}, \tau, x)$ *before setting* $Q := Q \cup \{(x, \pi)\}$*, which is initially empty.*

The proof system is said *unbounded* simulation-sound if it provides simulation-soundness against adversaries which are allowed to invoke the oracle $\mathsf{S}_2(\mathsf{crs}, \tau, .)$ an *a priori* unbounded (but polynomial) number of times. In the strictly weaker notion of *one-time* simulation-soundness, the adversary is restricted to query $\mathsf{S}_2(\mathsf{crs}, \tau, .)$ only once.

Note that, since proofs for false statements do exist in simulation-sound proof systems, the soundness property can only hold in the computational sense.

1.3 Groth-Sahai Proof Systems

In their seminal paper published in 2008, Groth and Sahai gave efficient non-interactive witness indistinguishable proof systems allowing to efficiently prove algebraic statements in groups with a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. Their techniques build on earlier ideas suggested by Groth, Ostrovsky and Sahai [137, 136] in that they rely on homomorphic commitments that can be either perfectly hiding or perfectly binding depending on how the commitment key is generated. A difference with [137, 136], however, is that the Groth-Sahai methods directly demonstrate the validity of algebraic statements without proving the satisfiability of a circuit. While this restricts the range of provable languages, it allows for a much better efficiency as it avoids the need for an expensive NP reduction.

In Groth-Sahai proofs, the statements to be proved involve witnesses that can be either exponents in $\mathbb{Z}_p$ or group elements in $\mathbb{G}_1$ or $\mathbb{G}_2$. One caveat is that these NIWI proofs can only be used as proofs of knowledge when the witnesses are all group elements.

The Groth-Sahai (GS) proof systems can be instantiated using the K-linear assumption for any $K > 0$. In their instantiation based on the DLIN assumption (with $K = 2$) in symmetric pairing configurations (i.e., with $\mathbb{G}_1 = \mathbb{G}_2$), the Groth-Sahai (GS) proof systems [138] use a common reference string (CRS) consisting of three vectors $\mathbf{g_1}, \mathbf{g_2}, \mathbf{g_3} \in \mathbb{G}^3$, where $\mathbf{g_1} = (g_1, 1, g)$, $\mathbf{g_2} = (1, g_2, g)$ for some $g_1, g_2 \in \mathbb{G}$. In order to commit to a group element $X \in \mathbb{G}$, the prover computes $\mathbf{C} = (1, 1, X) \cdot \mathbf{g_1}^r \cdot \mathbf{g_2}^s \cdot \mathbf{g_3}^t$ with $r, s, t \xleftarrow{\$} \mathbb{Z}_p$. When the proof system is configured to provide perfectly sound proofs, $\mathbf{g_3}$ is set as $\mathbf{g_3} = \mathbf{g_1}^{\xi_1} \cdot \mathbf{g_2}^{\xi_2}$ with $\xi_1, \xi_2 \xleftarrow{\$} \mathbb{Z}_p$. In this case, commitments can be written as

$$\mathbf{C} = (g_1^{r+\xi_1 t}, g_2^{s+\xi_2 t}, X \cdot g^{r+s+t(\xi_1+\xi_2)}),$$

so that they can be interpreted as Boneh-Boyen-Shacham (BBS) ciphertexts. Moreover, the committed $X \in \mathbb{G}$ can be recovered by running the BBS decryption algorithm using the private key $(\alpha_1, \alpha_2) = (\log_g(g_1), \log_g(g_2))$. When the CRS is set up to give perfectly witness indistinguishable (WI) proofs, $\mathbf{g_1}, \mathbf{g_2}$ and $\mathbf{g_3}$ are linearly independent vectors, so that $\mathbf{C}$ is a perfectly hiding commitment to $X \in \mathbb{G}$: a typical choice is $\mathbf{g_3} = \mathbf{g_1}^{\xi_1} \cdot \mathbf{g_2}^{\xi_2} \cdot (1, 1, g)^{-1}$. Under the DLIN assumption, the two distributions of CRS are computationally indistinguishable.

To commit to an exponent $x \in \mathbb{Z}_p$, the prover computes $\mathbf{C} = \boldsymbol{\varphi}^x \cdot \mathbf{g_1}^r \cdot \mathbf{g_2}^s$, with $r, s \xleftarrow{\$} \mathbb{Z}_p$, using a CRS containing $\boldsymbol{\varphi}, \mathbf{g_1}, \mathbf{g_2}$. In the perfect soundness setting $\boldsymbol{\varphi}, \mathbf{g_1}, \mathbf{g_2}$ are linearly independent (typically $\boldsymbol{\varphi} = \mathbf{g_3} \cdot (1, 1, g)$ where $\mathbf{g_3} = \mathbf{g_1}^{\xi_1} \cdot \mathbf{g_2}^{\xi_2}$) whereas, in the perfect WI setting, choosing $\boldsymbol{\varphi} = \mathbf{g_1}^{\xi_1} \cdot \mathbf{g_2}^{\xi_2}$ yields perfectly hiding commitments since $\mathbf{C}$ is statistically independent of x.

To prove that committed variables satisfy a set of relations, the GS techniques replace variables by the corresponding commitments in each relation. The entire proof consists of one commitment per variable and one proof element (made of a constant number of elements) per relation.

Efficient NIWI proofs are available for pairing-product relations, which are equations of the type

$$\prod_{i=1}^{n} e(\mathcal{A}_i, \mathcal{X}_i) \cdot \prod_{i=1}^{n} \cdot \prod_{j=1}^{n} e(\mathcal{X}_i, \mathcal{X}_j)^{a_{ij}} = t_T, \tag{1.5}$$

for constants $t_T \in \mathbb{G}_T$, $\mathcal{A}_1, \ldots, \mathcal{A}_n \in \mathbb{G}$, $a_{ij} \in \mathbb{Z}_p$, for $i, j \in \{1, \ldots, n\}$, and variables $\mathcal{X}_1, \ldots, \mathcal{X}_n \in \mathbb{G}$. Efficient proofs also exist for multi-exponentiation equations, which are of the

form

$$\prod_{i=1}^{m} \mathcal{A}_i^{y_i} \cdot \prod_{j=1}^{n} \mathcal{X}_j^{b_j} \cdot \prod_{i=1}^{m} \cdot \prod_{j=1}^{n} \mathcal{X}_j^{y_i \gamma_{ij}} = T,$$

for constants $T, \mathcal{A}_1, \ldots, \mathcal{A}_m \in \mathbb{G}$, $b_1, \ldots, b_n \in \mathbb{Z}_p$ and $\gamma_{ij} \in \mathbb{Z}_p$, for $i \in \{1, \ldots, m\}$, $j \in \{1, \ldots, n\}$ and variables $\mathcal{X}_1, \ldots, \mathcal{X}_n \in \mathbb{G}$, $y_1, \ldots, y_m \in \mathbb{Z}_p$.

Multi-exponentiation equations always admit non-interactive zero-knowledge (NIZK) proofs at no additional cost. On a perfectly witness indistinguishable CRS, a trapdoor (such as the hidden exponents $(\xi_1, \xi_2) \in \mathbb{Z}_p^2$ when $\mathbf{g_3} = \mathbf{g_1}^{\xi_1} \cdot \mathbf{g_2}^{\xi_2} \cdot (1, 1, g)^{-1}$) makes it possible to simulate proofs without knowing witnesses and simulated proofs are perfectly indistinguishable from real proofs. As for pairing-product equations, zero-knowledge proofs are often possible – this is usually the case when the right-hand-side member t_T of (1.5) is a product of pairings involving known group elements – but the number of group elements per proof may not be constant anymore. Here, when using such NIZK simulators, we just introduce a constant number of extra group elements in the proofs.

In both cases, proofs for quadratic equations cost 9 group elements. Linear pairing-product equations (when $a_{ij} = 0$ for all i, j) take 3 group elements each. Linear multi-exponentiation equations of the type $\prod_{j=1}^{n} \mathcal{X}_j^{b_j} = T$ (resp. $\prod_{i=1}^{m} \mathcal{A}_i^{y_i} = T$) demand 3 (resp. 2) group elements.

Groth-Sahai proofs can also be instantiated under the SXDH assumption. This instantiation uses prime order groups and a common reference string containing two vectors $\mathbf{f_1}, \mathbf{f_2} \in \mathbb{G}^2$, where $\mathbf{f_1} = (g, f_1)$, $\mathbf{f_2} = (h, f_2)$, for some $g, h, f_1, f_2 \in \mathbb{G}$. To commit to a group element $X \in \mathbb{G}$, the prover chooses $r, s \xleftarrow{\$} \mathbb{Z}_p$ and computes $\mathbf{C} = (1, X) \cdot \mathbf{f_1}^r \cdot \mathbf{f_2}^s$. On a perfectly sound common reference string, we have $\mathbf{f_2} = \mathbf{f_1}^{\xi}$, for some $\xi \in \mathbb{Z}_p$. Commitments $\mathbf{C} = (g^{r+\xi s}, f_1^{r+\xi s} \cdot X)$ are extractable as their distribution coincides with that of an Elgamal ciphertexts [103] and the committed X can be extracted using $\beta = \log_g(f_1)$. In the witness indistinguishability (WI) setting, the vector $\mathbf{f_2}$ is chosen so that $(\mathbf{f_1}, \mathbf{f_2})$ are linearly independent vectors and $\mathbf{C}$ is a perfectly hiding commitment. Under the DDH assumption in $\mathbb{G}$, the two kinds of CRS can be exchanged for one another without the adversary noticing.

To convince the verifier that committed variables satisfy a set of relations, the prover computes one commitment per variable and one proof element per equation.

In pairing-product equations, proving a linear equation of the form

$$\prod_{i=1}^{n} e(\mathcal{X}_i, \mathcal{A}_i) = t_T, \tag{1.6}$$

where $\mathcal{X}_1, \ldots, \mathcal{X}_n \in \mathbb{G}$ and $\mathcal{A}_1, \ldots, \mathcal{A}_n \in \hat{\mathbb{G}}$, costs two elements of $\hat{\mathbb{G}}$. If variables are in $\hat{\mathbb{G}}$, proofs must live in $\mathbb{G}^2$ instead of $\hat{\mathbb{G}}^2$. Quadratic equations are somewhat more expensive to prove and they main contain elements of both $\mathbb{G}$ and $\hat{\mathbb{G}}$. Multi-exponentiation equations have similar proof sizes.

In [28], Belenkiy *et al.* showed that Groth-Sahai proofs are perfectly randomizable. Given commitments $\{\mathbf{C}_{\mathcal{X}_i}\}_{i=1}^n$ and a NIWI proof $\boldsymbol{\pi}_{\text{PPE}}$ that committed $\{\mathcal{X}\}_{i=1}^n$ satisfy (1.5), anyone can publicly compute re-randomized commitments $\{\mathbf{C}_{\mathcal{X}_i'}\}_{i=1}^n$ and a re-randomized proof $\boldsymbol{\pi}'_{\text{PPE}}$ of the same statement. Moreover, $\{\mathbf{C}_{\mathcal{X}_i'}\}_{i=1}^n$ and π'_{PPE} are distributed as freshly generated commitments and proof.

Groth-Sahai proofs are also malleable [83] in that it is often possible to publicly modify a proof π of a given statement x and turn it into a proof π' of another statement x' which is related to x. This malleability property – which appears unique to GS proofs – can be a useful property in certain situations. For example, Belenkiy *et al.* used it to construct delegatable anonymous credentials [28]. More recently, Chase *et al.* [83] took advantage of the malleability of Groth-Sahai proofs to build homomorphic encryption schemes satisfying a relaxed form of chosen-ciphertext security [222], efficient non-interactive proofs for shuffles and elections systems [83, 84].

In the design of non-malleable protocols like chosen-ciphertext-secure public-key encryption, however, this malleability property is usually undesirable. Groth [133] showed an elegant technique, inspired by earlier ideas due to Lindell [192], for tweaking Groth-Sahai proofs and obtain unbounded simulation-soundness. The upcoming chapters will present more efficient methods for obtaining one-time and unbounded simulation-sound variants of Groth-Sahai proofs.

1.4 Quasi-Adaptive NIZK Proofs

While much more efficient than general NIZK proofs, the GS techniques remain more expensive than non-interactive proofs obtained from the Fiat-Shamir heuristic [107] in the random oracle model [32]: for example, proving that t variables satisfy a system of n linear equations demands $\Theta(t+n)$ group elements where Σ-protocols allow for $\Theta(t)$-size proofs.

For languages consisting of linear subspaces of a vector space, Jutla and Roy [151] showed how to significantly improve upon the GS paradigm in the *quasi-adaptive* setting. In quasi-adaptive NIZK proofs (QA-NIZK) for a class of languages $\{\mathcal{L}_\rho\}$ parametrized by ρ, the common reference string (CRS) is allowed to depend on the particular language $\mathcal{L}_\rho$ of which membership must be proved. At the same time, a single simulator should be effective for the whole class of languages $\{\mathcal{L}_\rho\}$. As pointed out in [151], QA-NIZK proofs are sufficient for many applications of Groth-Sahai proofs. In this setting, Jutla and Roy [151] gave very efficient QA-NIZK proofs of membership in linear subspaces. If $\mathbf{A} \in \mathbb{Z}_p^{t\times n}$ is a matrix or rank $t < n$, in order to prove membership of $\mathcal{L} = \{\mathbf{v} \in \mathbb{G}^n \mid \exists \mathbf{x} \in \mathbb{Z}_p^t \text{ s.t. } \mathbf{v} = g^{\mathbf{x}\cdot\mathbf{A}}\}$, the Jutla-Roy proofs only take $O(n-t)$ group elements – instead of $\Theta(n+t)$ in [138] – at the expense of settling for computational soundness.

Quasi-Adaptive NIZK (QA-NIZK) proofs are NIZK proofs where the CRS is allowed to depend on the specific language for which proofs have to be generated. The CRS is divided into a fixed part Γ, produced by an algorithm $\mathbb{K}_0$, and a language-dependent part ψ. However, there should be a single simulator for the entire class of languages.

Let λ be a security parameter. For public parameters Γ produced by $\mathbb{K}_0$, let $\mathcal{D}_\Gamma$ be a probability distribution over a collection of relations $\mathcal{R} = \{R_\rho\}$ parametrized by a string ρ with an associated language $\mathcal{L}_\rho = \{x \mid \exists w : R_\rho(x,w) = 1\}$.

We consider proof systems where the prover and the verifier both take a label $|\mathsf{b}|$ as additional input. For example, this label can be the message-carrying part of an Elgamal-like encryption. Formally, a tuple of algorithms $(\mathbb{K}_0, \mathbb{K}_1, \mathsf{P}, \mathsf{V})$ is a QA-NIZK proof system for $\mathcal{R}$ if there exists a PPT simulator $(\mathsf{S}_1, \mathsf{S}_2)$ such that, for any PPT adversaries $\mathcal{A}_1, \mathcal{A}_2$ and $\mathcal{A}_3$, we have the following properties:

Quasi-Adaptive Completeness:

$$\Pr[\Gamma \leftarrow \mathbb{K}_0(\lambda);\ \rho \leftarrow D_\Gamma;\ \psi \leftarrow \mathbb{K}_1(\Gamma,\rho);\\ (x,w,\mathsf{lbl}) \leftarrow \mathcal{A}_1(\Gamma,\psi,\rho);\ \pi \leftarrow \mathsf{P}(\psi,x,w,\mathsf{lbl}) : \mathsf{V}(\psi,x,\pi,\mathsf{lbl}) = 1 \text{ if } R_\rho(x,w) = 1] = 1.$$

Quasi-Adaptive Soundness:

$$\Pr[\Gamma \leftarrow \mathbb{K}_0(\lambda);\ \rho \leftarrow D_\Gamma;\ \psi \leftarrow \mathbb{K}_1(\Gamma,\rho);\ (x,\pi,\mathsf{lbl}) \leftarrow \mathcal{A}_2(\Gamma,\psi,\rho) :\\ \mathsf{V}(\psi,x,\pi,\mathsf{lbl}) = 1 \ \wedge\ \neg(\exists w : R_\rho(x,w) = 1)] \in \mathsf{negl}(\lambda).$$

Quasi-Adaptive Zero-Knowledge:

$$\Pr[\Gamma \leftarrow \mathbb{K}_0(\lambda);\ \rho \leftarrow D_\Gamma;\ \psi \leftarrow \mathbb{K}_1(\Gamma,\rho)\ :\ \mathcal{A}_3^{\mathsf{P}(\psi,\cdot,\cdot)}(\Gamma,\psi,\rho) = 1]\\ \approx \Pr[\Gamma \leftarrow \mathbb{K}_0(\lambda);\ \rho \leftarrow D_\Gamma;\ (\psi,\tau_{sim}) \leftarrow \mathsf{S}_1(\Gamma,\rho)\ :\ \mathcal{A}_3^{\mathsf{S}(\psi,\tau_{sim},\cdot,\cdot,\cdot)}(\Gamma,\psi,\rho) = 1],$$

where

- $\mathsf{P}(\psi,.,.,.)$ emulates the actual prover. It takes as input (x,w) and lbl and outputs a proof π if $(x,w) \in R_\rho$. Otherwise, it outputs $\perp$.
- $\mathsf{S}(\psi,\tau_{sim},.,.,.)$ is an oracle that takes as input (x,w) and lbl. It outputs a simulated proof $\mathsf{S}_2(\psi,\tau_{sim},x,\mathsf{lbl})$ if $(x,w) \in R_\rho$ and $\perp$ if $(x,w) \notin R_\rho$.

We assume that the CRS ψ contains an encoding of ρ, which is thus available to V. The definition of Quasi-Adaptive Zero-Knowledge requires a single simulator for the entire family of relations $\mathcal{R}$.

It is often useful to have a property called *simulation-soundness*, which requires that the adversary be unable to prove false statements even after having seen simulated proofs for possibly false statements.

Unbounded Simulation-Soundness: For any PPT adversary $\mathcal{A}_4$, it holds that

$$\Pr[\Gamma \leftarrow \mathbb{K}_0(\lambda);\ \rho \leftarrow D_\Gamma;\ (\psi,\tau_{sim}) \leftarrow \mathsf{S}_1(\Gamma,\rho);\ (x,\pi,\mathsf{lbl}) \leftarrow \mathcal{A}_4^{\mathsf{S}_2(\psi,\tau_{sim},\cdot,\cdot)}(\Gamma,\psi,\rho)\ :\\ \mathsf{V}(\psi,x,\pi,\mathsf{lbl}) = 1 \ \wedge\ \neg(\exists w : R_\rho(x,w) = 1) \ \wedge\ (x,\pi,\mathsf{lbl}) \notin Q] \in \mathsf{negl}(\lambda),$$

where the adversary is allowed unbounded access to an oracle $\mathsf{S}_2(\psi,\tau,.,.)$ that takes as input statement-label pairs (x,lbl) (where x may be outside $\mathcal{L}_\rho$) and outputs simulated proofs $\pi \leftarrow \mathsf{S}_2(\psi,\tau_{sim},x,\mathsf{lbl})$ before updating the set $Q = Q \cup \{(x,\pi,\mathsf{lbl})\}$, which is initially empty.

In the weaker notion of one-time simulation-soundness, only one query to the S_2 oracle is allowed.

In some applications, one may settle for a weaker notion, called *relative soundness* by Jutla and Roy [150], which allows for more efficient proofs, especially in the single-theorem case. Informally, relatively sound proof systems involve both a public verifier *and* a private verification algorithm, which has access to a trapdoor. For hard languages, the two verifiers should almost always agree on any adversarially-created proof. Moreover, the private

verifier should not accept a non-trivial proof for a false statement, even if the adversary has already seen proofs for false statements.

A labeled single-theorem relatively sound QA-NIZK proof system is comprised of a quasi-adaptive labeled proof system $(\mathbb{K}_0, \mathbb{K}_1, \mathsf{P}, \mathsf{V})$ along with an efficient private verifier W and an efficient simulator $(\mathsf{S}_1, \mathsf{S}_2)$. Moreover, the following properties should hold for any PPT adversaries $(\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3, \mathcal{A}_4)$.

Quasi Adaptive Relative Single-Theorem Zero-Knowledge:

$$\begin{aligned}\Pr[\Gamma \leftarrow \mathbb{K}_0(\lambda);\ \rho \leftarrow D_\Gamma;\ \psi \leftarrow \mathbb{K}_1(\Gamma,\rho);\ (x,w,\mathsf{lbl},s) \leftarrow \mathcal{A}_1^{\mathsf{V}(\psi,\cdot,\cdot)}(\Gamma,\psi,\rho);\\ \pi \leftarrow \mathsf{P}(\psi,\rho,x,w,\mathsf{lbl}) : \mathcal{A}_2^{\mathsf{V}(\psi,\cdot,\cdot)}(\pi,s)=1]\\ \approx \Pr[\Gamma \leftarrow \mathbb{K}_0(\lambda);\ \rho \leftarrow D_\Gamma;\ (\psi,\tau) \leftarrow \mathsf{S}_1(\Gamma,\rho);\ (x,w,\mathsf{lbl},s) \leftarrow \mathcal{A}_1^{\mathsf{W}(\psi,\tau,\cdot,\cdot)}(\Gamma,\psi,\rho);\\ \pi \leftarrow \mathsf{S}_2(\psi,\rho,\tau,x,\mathsf{lbl}) : \mathcal{A}_2^{\mathsf{W}(\psi,\tau,\cdot,\cdot)}(\pi,s)=1],\end{aligned}$$

Here, $\mathcal{A}_1$ is restricted to choosing (x,w) such that $R_\rho(x,w)=1$.

Quasi Adaptive Relative Single-Theorem Simulation-Soundness:

$$\begin{aligned}\Pr[\Gamma \leftarrow \mathbb{K}_0(\lambda);\ \rho \leftarrow D_\Gamma;\ (\psi,\tau) \leftarrow \mathsf{S}_1(\Gamma,\rho);\ (x,\mathsf{lbl},s) \leftarrow \mathcal{A}_3^{\mathsf{W}(\psi,\tau,\cdot,\cdot)}(\Gamma,\psi,\rho);\\ \pi \leftarrow \mathsf{S}_2(\psi,\rho,\tau,x,\mathsf{lbl}) : (x',\mathsf{lbl}',\pi') \leftarrow \mathcal{A}_4^{\mathsf{W}(\psi,\tau,\cdot,\cdot)}(s,\pi) :\\ (x,\pi,\mathsf{lbl}) \neq (x',\pi',\mathsf{lbl}') \wedge\ \nexists w' \text{ s.t. } R_\rho(x',w')=1 \wedge \mathsf{W}(\psi,\tau,x',\mathsf{lbl}',\pi')=1] \in \mathsf{negl}(\lambda)\end{aligned}$$

Note that the definition of relative simulation-soundness does not require the adversary to provide a witness but the definition of single-theorem zero-knowledge does.

1.5 Structure-Preserving Cryptography

Many anonymity-related cryptographic protocols (e.g., [81, 6, 4, 112, 5, 2]) build on Groth-Sahai proofs in order to prove security in the standard model of computation. In order to guarantee the extractability of witnesses for proofs generated on a perfectly sound CRS, it is convenient to have signature schemes which allow one to sign elements of bilinear groups while maintaining the feasibility of conveniently proving that a committed signature is valid for a committed message.

Signature schemes where messages only consist of group elements appeared for the first time as ingredients of Groth's construction [133] of group signatures in the standard model. The scheme of [133] was mostly a proof of concept, with signatures consisting of thousands of group elements. More efficient solutions were described by Fuchsbauer [112] and, independently, in a paper of mine [81]. While the scheme of [112] is somewhat more efficient, it only allows signing messages with a particular structure (typically, Diffie-Hellman tuples). The construction of Cathalo, Yung and myself [81] does not have this restriction but its disadvantage resides in the linear length $O(n)$ of signatures if $\mathbb{G}^n$ is the message space. Abe, Haralambiev and Ohkubo [6, 4] – who introduced the "structure-preserving" terminology – subsequently showed how to sign messages of n group elements at once using $O(1)$-size signatures. Lower bounds on the size of structure-preserving signatures were given in [5] while

Abe *et al.* [5] provided evidence that optimally short SPS necessarily rely on interactive assumptions. As an ingredient for their tightly secure cryptosystems, Hofheinz and Jager [142] gave constructions based on the Decision Linear assumption [44] while similar results were independently achieved in [63, 82]. Quite recently, Abe *et al.* [2, 3] obtained constant-size signatures without sacrificing the security guarantees offered by security proofs under simple assumptions.

In the context of symmetric pairings, the description below assumes public parameters $\mathsf{pp} = \big((\mathbb{G}, \mathbb{G}_T),\ g\big)$ consisting of bilinear groups $(\mathbb{G}, \mathbb{G}_T)$ of prime order $p > 2^\lambda$, where $\lambda \in \mathbb{N}$ and a generator $g \in \mathbb{G}$.

Keygen(pp, n)**:** given an upper bound $n \in \mathbb{N}$ on the number of group elements per signed message, choose generators $G_r, H_r \xleftarrow{\$} \mathbb{G}$. Pick $\gamma_z, \delta_z \xleftarrow{\$} \mathbb{Z}_p$ and $\gamma_i, \delta_i \xleftarrow{\$} \mathbb{Z}_p$, for $i = 1$ to n. Then, compute $G_z = G_r^{\gamma_z}$, $H_z = H_r^{\delta_z}$ and $G_i = G_r^{\gamma_i}$, $H_i = H_r^{\delta_i}$ for each $i \in \{1, \ldots, n\}$. Finally, choose $\alpha_a, \alpha_b \xleftarrow{\$} \mathbb{Z}_p$ and define $A = e(G_r, g^{\alpha_a})$ and $B = e(H_r, g^{\alpha_b})$. The public key is defined to be

$$pk = \big(G_r,\ H_r,\ G_z,\ H_z,\ \{G_i, H_i\}_{i=1}^n,\ A,\ B\big) \in \mathbb{G}^{2n+4} \times \mathbb{G}_T^2$$

while the private key is $sk = \big(\alpha_a, \alpha_b, \gamma_z, \delta_z, \{\gamma_i, \delta_i\}_{i=1}^n\big)$.

Sign$(sk, (M_1, \ldots, M_n))$**:** to sign $(M_1, \ldots, M_n) \in \mathbb{G}^n$ using $sk = (\alpha_a, \alpha_b, \gamma_z, \delta_z, \{\gamma_i, \delta_i\}_{i=1}^n)$, choose $\zeta, \rho_a, \rho_b, \omega_a, \omega_b \xleftarrow{\$} \mathbb{Z}_p$ and compute $\theta_1 = g^\zeta$ as well as

$$\theta_2 = g^{\rho_a - \gamma_z \zeta} \cdot \prod_{i=1}^n M_i^{-\gamma_i}, \qquad \theta_3 = G_r^{\omega_a}, \qquad \theta_4 = g^{(\alpha_a - \rho_a)/\omega_a},$$

$$\theta_5 = g^{\rho_b - \delta_z \zeta} \cdot \prod_{i=1}^n M_i^{-\delta_i}, \qquad \theta_6 = H_r^{\omega_b}, \qquad \theta_7 = g^{(\alpha_b - \rho_b)/\omega_b},$$

The signature consists of $\sigma = (\theta_1, \theta_2, \theta_3, \theta_4, \theta_5, \theta_6, \theta_7)$.

Verify$(pk, \sigma, (M_1, \ldots, M_n))$**:** parse σ as $(\theta_1, \theta_2, \theta_3, \theta_4, \theta_5, \theta_6, \theta_7) \in \mathbb{G}^7$ and return 1 iff these equalities hold:

$$\begin{aligned} A &= e(G_z, \theta_1) \cdot e(G_r, \theta_2) \cdot e(\theta_3, \theta_4) \cdot \prod_{i=1}^n e(G_i, M_i), \\ B &= e(H_z, \theta_1) \cdot e(H_r, \theta_5) \cdot e(\theta_6, \theta_7) \cdot \prod_{i=1}^n e(H_i, M_i). \end{aligned}$$

The scheme was proved [6, 4] existentially unforgeable under chosen-message attacks under the q-SFP assumption, where q is the number of signing queries.

As shown in [6, 4], Signatures components $\{\theta_i\}_{i=2}^7$ can be publicly randomized to obtain a different signature $\{\theta_i'\}_{i=1}^7 \leftarrow \mathsf{ReRand}(pk, \sigma)$ on $(M_1, \ldots, M_n)$. After randomization, we have $\theta_1' = \theta_1$ whereas other signature components $\{\theta_i'\}_{i=2}^7$ are uniformly distributed among the values satisfying the relations

$$\begin{aligned} e(G_r, \theta_2') \cdot e(\theta_3', \theta_4') &= e(G_r, \theta_2) \cdot e(\theta_3, \theta_4) \\ e(H_r, \theta_5') \cdot e(\theta_6', \theta_7') &= e(H_r, \theta_5) \cdot e(\theta_6, \theta_7). \end{aligned}$$

Moreover, $\{\theta'_i\}_{i\in\{3,4,6,7\}}$ are statistically independent of the message and the rest of the signature. This implies that, in privacy-preserving protocols, re-randomized $\{\theta'_i\}_{i\in\{3,4,6,7\}}$ can safely appear in clear as long as $(M_1, \ldots, M_n)$ and $\{\theta'_i\}_{i\in\{1,2,5\}}$ are given in committed form.

In [5], Abe, Groth, Haralambiev and Ohkubo described shorter structure-preserving signatures based on interactive assumptions (or, alternatively, in the generic group model [237]). In the forthcoming chapters, we only rest on non-interactive and falsifiable assumptions, so that the above scheme will be preferred to those of [5].

In [2, 3], Abe *et al.* described constant-size structure-preserving signatures based on the standard DLIN assumption. While these constructions allow for the modular design of many privacy-enhancing protocols (e.g., group signatures) based on simple assumptions, they are somewhat less efficient than the original AHO signature [6]. While several of our results build on the latter system (as they were published before [2, 3]), they can often be modified by using the DLIN-based structure-preserving signatures of [2, 3] so as to avoid non-standard q-type assumption.

Regarding primitives beyond signature schemes, Camenisch *et al.* [65] showed a structure-preserving variant of the Cramer-Shoup cryptosystem [88] and used it to implement oblivious third parties [64]. Groth [135] described length-reducing trapdoor commitments (*i. e.*, where the commitment is shorter than the committed message) to group elements whereas [7] showed the impossibility of realizing such commitments when the commitment string lives in the same group as the message. Sakai *et al.* [233] recently suggested to use structure-preserving identity-based encryption [236] systems to restrict the power of the opening authority in group signatures.

CHAPTER 2

Applications of Structure-Preserving Cryptography and NIZK Proofs to Privacy-Enhancing Primitives

This chapter presents two applications of structure-preserving cryptography and Groth-Sahai proofs in the setting of privacy-preserving protocols where users can retain anonymity while taking certain actions within a group they belong to.

The first application is the design of a non-interactive group encryption system [156], where anyone can encrypt a message for a certified but anonymous member of a group of users. At the same time, the sender can convince anyone that a ciphertext is a valid encryption intended for some group member which an authority can identify if necessary.

The second application deals with the revocation problem in group signatures. Group signatures [85] are signatures schemes where group users can sign messages while hiding their identify within a group of members. Again, in order to deter abuses of the system, an authority is capable of identifying the author of any signature.

In this chapter, although group signatures are an older primitive than group encryption, our result on group encryption will be presented first since it makes use of our realization of structure-preserving signatures [81], which is less efficient than the one of Abe *et al.* [6] that we use in our revocable group signatures [180, 179].

2.1 Non-Interactive Group Encryption

Introduced by Kiayias, Tsiounis and Yung [156], group encryption (GE) is the encryption analogue of group signatures [85]. The latter primitives allow a group member to sign messages in the name of a group without revealing his identity. In a similar spirit, GE systems aim to hide the identity of a ciphertext's recipient and still guarantee that he belongs to a population of registered members in a group administered by a group manager (GM). A sender can generate an anonymous encryption of some plaintext m intended for a receiver holding a public key that was certified by the GM (message security and receiver anonymity being both in the CCA2 sense). The ciphertext is prepared while leaving an opening authority (OA) the ability to "open" the ciphertext (analogously to the opening operation in group signatures) and uncover the receiver's name. At the same time, the sender should be able to convince a verifier that: (1) The ciphertext is a valid encryption under the public key of some group member holding a valid certificate; (2) If necessary, the opening authority will be able to find out who the receiver is; (3) The plaintext is a witness satisfying some public relation.

MOTIVATIONS. As a natural use case, group encryption allows a firewall to block all encrypted emails attempting to enter a network unless they are generated for some certified organization member and they carry a proof of malware-freeness. Group encryption also enables oblivious retriever storage mechanisms in the cloud. Namely, when encrypting datasets on a remote storage server, the sender can convince this server that the data is intended for some legitimate certified user (who paid a subscription for storing his data) without disclosing the latter's identity. The GE primitive was also motivated by various privacy applications such as anonymous trusted third parties. Many cryptographic protocols such as fair exchange, fair encryption or escrow encryption, involve trusted third parties that remain offline most of the time and are only involved to resolve problems. Group encryption allows one to verifiably encrypt some message to such a trusted third party while hiding his identity among a set of possible trustees. For instance, a user can encrypt a key (e.g., in an "international key escrow system") to his own national trusted representative without letting the ciphertext reveal the latter's identity, which could leak information on the user's citizenship. At the same time, everyone can be convinced that the ciphertext is heading for an authorized trustee.

Group encryption also finds applications in ubiquitous computing, where anonymous credentials must be transferred between peer devices belonging to the same group. Asynchronous transfers may require to involve an untrusted storage server to temporarily store encrypted credentials. In such a situation, GE schemes may be used to simultaneously guarantee that (1) the server retains properly encrypted valid credentials that it cannot read; (2) credentials have a legitimate anonymous retriever; (3) if necessary, an authority will be able to determine who the retriever is.

By combining cascaded group encryptions using multiple trustees and according to a sequence of identity discoveries and transfers, one can also implement group signatures where signers can flexibly specify how a set of trustees should operate to open their signatures.

PRIOR WORKS. Kiayias, Tsiounis and Yung (KTY) [156] formalized the concept of group encryption and gave a suitable security modeling. They presented a modular design of GE system and proved that, beyond zero-knowledge proofs, anonymous public key encryption schemes with CCA2 security, digital signatures, and equivocal commitments are necessary to realize the primitive. They also showed how to efficiently instantiate their general construction using Paillier's cryptosystem [216]. While efficient, their scheme is not a single message encryption, since it requires the sender to interact with the verifier in a Σ-protocol to convince him that the aforementioned properties are satisfied. Interaction can be removed using the Fiat-Shamir paradigm [107] (and thus the random oracle model [32]), but only heuristic arguments [128] (see also [72]) are then possible in terms of security.

Independently, Qin *et al.* [224] considered a closely related primitive with non-interactive proofs and short ciphertexts. However, they avoid interaction by employing a random oracle and also rely on strong interactive assumptions. As we can see, none of these schemes is a truly non-interactive encryption scheme without the random oracle idealization.

OUR CONTRIBUTION. As already noted in various contexts such as anonymous credentials [29], rounds of interaction are expensive and even impossible at times as, in some applications, proofs should be verifiable by third parties that are not present when provers are available. In the setting of group encryption, this last concern is even more constraining as it requires the sender, who may be required to repeat proofs with many verifiers, to maintain a

state and remember the random coins that he uses to encrypt *every* single ciphertext. In the frequent situation where many encryptions have to be generated using independent random coins, this becomes a definite bottleneck.

Together with Julien Cathalo and Moti Yung [81], we solved the above problems and described the first realization of fully non-interactive group encryption with CCA2-security and anonymity in the standard model. In our scheme, senders do not need to maintain a state: thanks to the Groth-Sahai [138] non-interactive proof systems, the proof of a ciphertext can be generated once-and-for-all at the same time as the ciphertext itself. Furthermore, using suitable parameters and for a comparable security level, we can also shorten ciphertexts by a factor of 2 in comparison with the KTY scheme. As far as communication goes, the size of proofs allows decreasing by more than 75% the number of transmitted bits between the sender and the verifier.

Since our goal is to avoid interaction, we also design a joining protocol (*i.e.*, a protocol whereby the user effectively becomes a group member and gets his public key certified by the GM) which requires the smallest amount of interaction: as in the Kiayias-Yung group signature [157], only two messages have to be exchanged between the GM and the user and the latter need not to prove anything about his public key. In particular, rewinding is not necessary in security proofs and the join protocol can be safely executed in a concurrent environment, when many users want to register at the same time. The join protocol uses a non-interactive public key certification scheme where discrete-logarithm-type public keys can be signed as if they were ordinary messages (and without knowing the matching private key) while leaving the ability to efficiently prove knowledge of the certificate/public key using the Groth-Sahai techniques. To certify users without having to rewind[1] in security proofs, the KTY scheme uses groups of hidden order (and more precisely, Camenisch-Lysyanskaya signatures [68]). In public order groups, to the best of our knowledge, our construction is the first certification method that does not require any form of proof of knowledge of private keys. We believe it to be of independent interest as it can be used to construct group signatures (in the standard model) where the joining mechanism tolerates concurrency in the model of [157] without demanding more than two moves of interaction.

2.1.1 Model and Security Notions

Syntax. Group encryption schemes involve a sender, a verifier, a group manager (GM) that manages the group of receivers and an opening authority (OA) which is able to uncover the identity of ciphertext receivers. A GE system is formally specified by the description of a relation $\mathcal{R}$ as well as a collection $\mathsf{GE} = \big(\mathsf{SETUP}, \mathsf{JOIN}, \langle \mathcal{G}_r, \mathcal{R}, \mathsf{sample}_{\mathcal{R}} \rangle, \mathsf{ENC}, \mathsf{DEC}, \mathsf{OPEN}, \langle \mathcal{P}, \mathcal{V} \rangle\big)$ of algorithms or protocols. Among these, SETUP is a set of initialization procedures that all take (explicitly or implicitly) a security parameter λ as input. They can be split into one that generates a set of public parameters params (a common reference string), one for the GM and another one for the OA. We call them $\mathsf{SETUP}_{\mathsf{init}}(\lambda)$, $\mathsf{SETUP}_{\mathsf{GM}}(\mathsf{params})$ and $\mathsf{SETUP}_{\mathsf{OA}}(\mathsf{params})$, respectively. The latter two procedures are used to produce key pairs $(\mathsf{pk}_{\mathsf{GM}}, \mathsf{sk}_{\mathsf{GM}})$, $(\mathsf{pk}_{\mathsf{OA}}, \mathsf{sk}_{\mathsf{OA}})$ for the GM and the OA. In the following, params is incorporated in the inputs of all algorithms although we sometimes omit to explicitly write it.

$\mathsf{JOIN} = (\mathsf{J}_{\mathsf{user}}, \mathsf{J}_{\mathsf{GM}})$ is an interactive protocol between the GM and the prospective user.

[1] Although the simulator does not need to rewind proofs of knowledge in [156], users still have to interactively prove the validity of their public key.

As in [157], we will restrict this protocol to have minimal interaction and consist of only two messages: the first one is the user's public key pk sent by $\mathsf{J}_{\mathsf{user}}$ to J_{GM} and the latter's response is a certificate $\mathsf{cert}_{\mathsf{pk}}$ for pk that makes the user's group membership effective. We do not require the user to prove knowledge of his private key sk or anything else about it. In our construction, valid keys will be publicly recognizable and users do not need to prove their validity. After the execution of JOIN, the GM stores the public key pk and its certificate $\mathsf{cert}_{\mathsf{pk}}$ in a public directory database.

Algorithm sample allows sampling pairs $(x, w) \in \mathcal{R}$ (made of a public value x and a witness w) using keys $(\mathsf{pk}_{\mathcal{R}}, \mathsf{sk}_{\mathcal{R}})$ produced by $\mathcal{G}_r$. Depending on the relation, $\mathsf{sk}_{\mathcal{R}}$ may be the empty string (as will be the case in our scheme). The testing procedure $\mathcal{R}(x, w)$ returns 1 whenever $(x, w) \in \mathcal{R}$. To encrypt a witness w such that $(x, w) \in \mathcal{R}$ for some public x, the sender fetches the pair $(\mathsf{pk}, \mathsf{cert}_{\mathsf{pk}})$ from database and runs the randomized encryption algorithm. The latter takes as input w, a label L, the receiver's pair $(\mathsf{pk}, \mathsf{cert}_{\mathsf{pk}})$ as well as public keys $\mathsf{pk}_{\mathsf{GM}}$ and $\mathsf{pk}_{\mathsf{OA}}$. Its output is a ciphertext $\psi \leftarrow \mathsf{ENC}(\mathsf{pk}_{\mathsf{GM}}, \mathsf{pk}_{\mathsf{OA}}, \mathsf{pk}, \mathsf{cert}_{\mathsf{pk}}, w, L)$. On input of the same elements, the certificate $\mathsf{cert}_{\mathsf{pk}}$, the ciphertext ψ and the random coins $coins_{\psi}$ that were used to produce it, the non-interactive algorithm P generates a proof π_{ψ} that there exists a certified receiver whose public key was registered in database and that is able to decrypt ψ and obtain a witness w such that $(x, w) \in \mathcal{R}$. The verification algorithm V takes as input ψ, $\mathsf{pk}_{\mathsf{GM}}$, $\mathsf{pk}_{\mathsf{OA}}$, π_{ψ} and the description of $\mathcal{R}$ and outputs 0 or 1. Given ψ, L and the receiver's private key sk, the output of DEC is either a witness w such that $(x, w) \in \mathcal{R}$ or a rejection symbol $\perp$. Finally, OPEN takes as input a ciphertext/label pair (ψ, L) and the OA's secret key $\mathsf{sk}_{\mathsf{OA}}$ and returns a receiver's public key pk.

Security notions. The security model of Kiayias, Tsiounis and Yung [156] considers three notions called message security, anonymity and soundness. The first one captures the CCA2-security of messages encrypted under the receiver's public key, even if the adversary controls both the group manager and the opening authority. The notion of anonymity subsumes the anonymity of group encryption ciphertexts (in particular, the inability to tell apart encryptions of ciphertexts encrypted under pk_0 from those encrypted under pk_1), even given access to an opening oracle (run on behalf of the opening authority) and decryption oracles for both pk_0 and pk_1. The notion of soundness captures the security of the group manager against malicious encryptors colluding with a dishonest opening authority. In short, no malicious sender (even with the help of a corrupted opening authority) can create a valid proof for a ciphertext whose receiver cannot be traced to a certified group member. Detailed definitions are given in [156, 81]

2.1.2 Building Blocks: Structure-Preserving Commitments and Signatures

Our structure-preserving signature uses a trapdoor commitment to group elements as an important ingredient to dispense with proofs of knowledge of users' private keys.

A Strictly Structure-Preserving Trapdoor Commitment

We need a trapdoor commitment scheme that allows committing to elements of a group $\mathbb{G}$ where bilinear map arguments are taken. The scheme has to be structure-preserving in the strict sense in that commitments will have to be themselves elements of $\mathbb{G}$, which prevents us from using Groth's scheme [135] where commitments live in the range $\mathbb{G}_T$ of the pairing.

Such commitments can be obtained using the perfectly hiding Groth-Sahai commitment based on the linear assumption recalled in section 1.3. This commitment scheme uses a common reference string describing a prime order group $\mathbb{G}$ and a generator $f \in \mathbb{G}$. The commitment key consists of vectors $(\mathbf{f_1}, \mathbf{f_2}, \mathbf{f_3})$ chosen as $\mathbf{f_1} = (f_1, 1, f)$, $\mathbf{f_2} = (1, f_2, f)$ and $\mathbf{f_3} = \mathbf{f_1}^{\xi_1} \cdot \mathbf{f_2}^{\xi_2} \cdot (1, 1, f)^{\xi_3}$, with $f_1, f_2 \xleftarrow{\$} \mathbb{G}$, $\xi_1, \xi_2, \xi_3 \xleftarrow{\$} \mathbb{Z}_p^*$. To commit to a group element $X \in \mathbb{G}$, the sender picks $\phi_1, \phi_2, \phi_3 \xleftarrow{\$} \mathbb{Z}_p^*$ and sets $\mathbf{C}_X = (1, 1, X) \cdot \mathbf{f_1}^{\phi_1} \cdot \mathbf{f_2}^{\phi_2} \cdot \mathbf{f_3}^{\phi_3}$, which, if $\mathbf{f_3}$ is parsed as $(f_{3,1}, f_{3,2}, f_{3,3})$, can be written $\mathbf{C}_X = (f_1^{\phi_1} \cdot f_{3,1}^{\phi_3}, f_2^{\phi_2} \cdot f_{3,2}^{\phi_3}, X \cdot f^{\phi_1+\phi_2} \cdot f_{3,3}^{\phi_3})$. Due to the use of GS proofs, commitment openings need to only consist of group elements (and no scalar). To open $\mathbf{C}_X = (C_1, C_2, C_3)$, the sender reveals $(D_1, D_2, D_3) = (f^{\phi_1}, f^{\phi_2}, f^{\phi_3})$ and X. The receiver is convinced that the committed value was X by checking that

$$\begin{cases} e(C_1, f) = e(f_1, D_1) \cdot e(f_{3,1}, D_3) \\ e(C_2, f) = e(f_2, D_2) \cdot e(f_{3,2}, D_3) \\ e(C_3, f) = e(X \cdot D_1 \cdot D_2, f) \cdot e(f_{3,3}, D_3). \end{cases}$$

If a cheating committer can produce distinct openings of $\mathbf{C}_X$, we can solve a SDP instance $(g_1, g_2, g_{1,c}, g_{2,d})$. Namely, the commitment key is set as $(f_1, f_2, f_{3,1}, f_{3,2}) = (g_1, g_2, g_{1,c}, g_{2,d})$ and $f, f_{3,3}$ are chosen at random. When the adversary outputs openings $(X, (D_1, D_2, D_3))$ and $(X', (D_1', D_2', D_3'))$, these openings must simultaneously satisfy the equalities

$$e(f_1, D_1/D_1') = e(f_{3,1}, D_3'/D_3), \qquad e(f_2, D_2/D_2') = e(f_{3,2}, D_3'/D_3)$$

and $e((XD_1D_2)/(X'D_1'D_2'), f) = e(f_{3,3}, D_3'/D_3)$. A solution to the SDP instance is obtained as $(u, v, w) = (D_1/D_1', D_2/D_2', D_3'/D_3)$, which is a non-trivial triple as long as $X' \neq X$.

We also observe that, using the trapdoor (ξ_1, ξ_2, ξ_3), the receiver can equivocate commitments. Given a commitment $\mathbf{C}_X$ and its opening $(X, (D_1, D_2, D_3))$, one can trapdoor open $\mathbf{C}_X$ to any other $X' \in \mathbb{G}$ (and without knowing $\log_g(X')$) by computing

$$D_1' = D_1 \cdot (X'/X)^{\xi_1/\xi_3}, \qquad D_2' = D_2 \cdot (X'/X)^{\xi_2/\xi_3}, \qquad D_3' = (X/X')^{1/\xi_3} \cdot D_3.$$

Unlike Groth's trapdoor commitment to group elements [135], the above construction is not length-reducing in that the commitment string is longer than the message. In *strictly* structure-preserving commitments (i.e., where the commitment lives in the source group $\mathbb{G}$ instead of the target group $\mathbb{G}_T$), however, Abe, Haralambiev and Ohkubo showed [7] that this is inevitable. A slightly more efficient construction of strictly structure-preserving trapdoor commitment was given in [7].

A Structure-Preserving Signature Scheme

In [81], we first described a structure-preserving signature scheme in order to certify public keys for the DLIN-based variant [235, 143] of the Cramer-Shoup cryptosystem [88, 90]. These keys should be signed while retaining algebraic properties that make it possible to prove knowledge of a public key and its corresponding certificate in an efficient way. In particular, signing hashed public keys is proscribed as it would destroy their algebraic structure. In the interactive setting, several papers (e.g., [39, 134]) described efficient interactive protocols where a public key is jointly generated by a user and a certification authority in such a way that the user eventually obtains a certified public key and no one else learns the

underlying private key. In our construction, we aim at minimizing the amount of interaction and let users generate their public key entirely on their own before requesting their certification. Ideally, we would like to be able to sign public keys without even requiring users to prove knowledge of their private key and, in particular, without having to first rewind a proof of knowledge so as to extract the user's private key in the security proof. This is where structure-preserving signatures come in handy.

In the description, we assume common public parameters cp consisting of bilinear groups $(\mathbb{G}, \mathbb{G}_T)$ of prime order $p > 2^\lambda$, for a security parameter λ, and a generator $g \xleftarrow{\$} \mathbb{G}$. We also assume that certified public keys always consist of a fixed number n of group elements (*i.e.*, $\mathcal{PK} = \mathbb{G}^n$).

The scheme borrows from the Boyen-Waters group signature [56] in the use of the Hidden Strong Diffie-Hellman assumption. A simplified version of this scheme involves a signer that holds a public key $PK = (\Omega = g^\omega, A = (g,g)^\alpha, u, u_0, u_1 = g^{\beta_1}, \ldots, u_n = g^{\beta_n})$, for private elements $SK = (\omega, \alpha, \beta_1, \ldots, \beta_n)$, where n denotes the number of groups elements that certified public keys consist of. To certify a public key $\mathsf{pk} = (X_1 = g^{x_1}, \ldots, X_n = g^{x_n})$, the signer chooses an exponent $c_{\mathcal{ID}} \xleftarrow{\$} \mathbb{Z}_p^*$ and computes $S_1 = (g^\alpha)^{1/(\omega + c_{\mathcal{ID}})}$, $S_2 = g^{c_{\mathcal{ID}}}$, $S_3 = u^{c_{\mathcal{ID}}}$, $S_4 = (u_0 \cdot \prod_{i=1}^n X_i^{\beta_i})^{c_{\mathcal{ID}}}$ and $S_5 = (S_{5,1}, \ldots, S_{5,n}) = (X_1^{c_{\mathcal{ID}}}, \ldots, X_n^{c_{\mathcal{ID}}})$. Verification then checks whether $e(S_1, \Omega \cdot S_2) = A$ and $e(S_2, u) = e(g, S_3)$ as in [56]. It must also be checked that $e(S_4, g) = e(u_0, S_2) \cdot \prod_{i=1}^n e(u_i, S_{5,i})$ and $e(S_{5,i}, g) = e(X_i, S_2)$ for $i = 1, \ldots, n$.

The security of this simplified scheme can only be proven if, when answering certification queries, the simulator can control the private keys $(x_1, \ldots, x_n)$ and force them to be random values of its choice. To allow the simulator to sign arbitrary public keys without knowing the private keys, we modify the scheme so that the signer rather signs commitments (calculated using our structure-preserving trapdoor commitment) to public key elements $X_1, \ldots, X_n$. In the security proof, the simulator first generates a signature on n fake commitments $\mathbf{C}_i = (C_{i,1}, C_{i,2}, C_{i,3})$ that are all generated in such a way that it knows $\log_g(C_{i,j})$ for $i = 1, \ldots, n$ and $j = 1, 2, 3$. Using the trapdoor of the commitment scheme, it can then open $\mathbf{C}_i$ to any arbitrary $X_i \in \mathbb{G}$ without knowing $\log_g(X_i)$.

This use of the trapdoor commitment is reminiscent of a technique (notably used in [89]) to construct signature schemes in the standard model using chameleon hash functions [162]: the simulator first signs messages of its choice using a basic signature scheme and then "equivocates" the chameleon hashes to make them correspond to adversarially-chosen messages.

Keygen(pp, n)**:** given common public parameters $\mathsf{pp} = \{g, \mathbb{G}, \mathbb{G}_T\}$, select $u, u_0 \xleftarrow{\$} \mathbb{G}$ as well as $\alpha, \omega \xleftarrow{\$} \mathbb{Z}_p^*$ and set $A = e(g,g)^\alpha$, $\Omega = g^\omega$. Then, pick $\beta_{i,1}, \beta_{i,2}, \beta_{i,3} \xleftarrow{\$} \mathbb{Z}_p^*$ and define

$$\overline{u}_i = (u_{i,1}, u_{i,2}, u_{i,3}) = (g^{\beta_{i,1}}, g^{\beta_{i,2}}, g^{\beta_{i,3}})$$

for $i = 1, \ldots, n$. Choose $f, f_1, f_2, f_{3,1}, f_{3,2}, f_{3,3} \xleftarrow{\$} \mathbb{G}$ that define a commitment key consisting of vectors $\mathbf{f_1} = (f_1, 1, f)$, $\mathbf{f_2} = (1, f_2, f)$ and $\mathbf{f_3} = (f_{3,1}, f_{3,2}, f_{3,3})$. Define the private key to be $SK = \big(\alpha, \omega, \{\overline{\beta}_i = (\beta_{i,1}, \beta_{i,2}, \beta_{i,3})\}_{i=1,\ldots,n}\big)$ and the public key as

$$PK \;=\; \Big(\mathbf{f} = (\mathbf{f_1}, \mathbf{f_2}, \mathbf{f_3}),\; A = e(g,g)^\alpha,\; \Omega = g^\omega,\; u,\; u_0,\; \{\overline{u}_i\}_{i=1,\ldots,n}\Big).$$

Sign(pp, SK, M)**:** parse SK as $\big(\alpha, \omega, \{\overline{\beta}_i\}_{i=1,\ldots,n}\big)$, M as $(X_1, \ldots, X_n)$ and do the following.

1. For each $i \in \{1, \ldots, n\}$, pick $\phi_{i,1}, \phi_{i,2}, \phi_{i,3} \xleftarrow{\$} \mathbb{Z}_p^*$ and compute a commitment

$$C_i = (C_{i,1}, C_{i,2}, C_{i,3}) = (f_1^{\phi_{i,1}} \cdot f_{3,1}^{\phi_{i,3}},\ f_2^{\phi_{i,2}} \cdot f_{3,2}^{\phi_{i,3}},\ X_i \cdot f^{\phi_{i,1}+\phi_{i,2}} \cdot f_{3,3}^{\phi_{i,3}})$$

   and the matching de-commitment $(D_{i,1}, D_{i,2}, D_{i,3}) = (f^{\phi_{i,1}}, f^{\phi_{i,2}}, f^{\phi_{i,3}})$.

2. Choose $c_{\mathcal{ID}} \xleftarrow{\$} \mathbb{Z}_p^*$ and compute $S_1 = (g^{\alpha})^{1/(\omega + c_{\mathcal{ID}})}$, $S_2 = g^{c_{\mathcal{ID}}}$, $S_3 = u^{c_{\mathcal{ID}}}$ as well as

$$S_4 = \Big(u_0 \cdot \prod_{i=1}^{n} (C_{i,1}^{\beta_{i,1}} \cdot C_{i,2}^{\beta_{i,2}} \cdot C_{i,3}^{\beta_{i,3}})\Big)^{c_{\mathcal{ID}}}$$
$$S_5 = \{(S_{5,i,1}, S_{5,i,2}, S_{5,i,3})\}_{i=1,\ldots,n} = \{(C_{i,1}^{c_{\mathcal{ID}}}, C_{i,2}^{c_{\mathcal{ID}}}, C_{i,3}^{c_{\mathcal{ID}}})\}_{i=1,\ldots,n}$$

Return $\mathsf{cert}_M = \Big(\{(C_{i,1}, C_{i,2}, C_{i,3}), (D_{i,1}, D_{i,2}, D_{i,3})\}_{i=1,\ldots,n}, S_1, S_2, S_3, S_4, S_5\Big)$.

Verify$(\mathsf{pp}, PK, M, \mathsf{cert}_M)$**:** parse M as $(X_1, \ldots, X_n)$ and cert_M as above. Return 1 if, for indices $i = 1, \ldots, n$, it holds that $X_i \in \mathbb{G}$ and

$$e(C_{i,1}, f) = e(f_1, D_{i,1}) \cdot e(f_{3,1}, D_{i,3}) \quad (2.1)$$
$$e(C_{i,2}, f) = e(f_2, D_{i,2}) \cdot e(f_{3,2}, D_{i,3}) \quad (2.2)$$
$$e(C_{i,3}, f) = e(X_i \cdot D_{i,1} \cdot D_{i,2}, f) \cdot e(f_{3,3}, D_{i,3}), \quad (2.3)$$

and if the following checks are also satisfied. Otherwise, return 0.

$$e(S_1, \Omega \cdot S_2) = A \quad (2.4)$$
$$e(S_2, u) = e(g, S_3) \quad (2.5)$$
$$e(S_4, g) = e(u_0, S_2) \cdot \prod_{i=1}^{n} \big(e(u_{i,1}, S_{5,i,1}) \cdot e(u_{i,2}, S_{5,i,2}) \cdot e(u_{i,3}, S_{5,i,3})\big), \quad (2.6)$$
$$e(S_{5,i,j}, g) = e(C_{i,j}, S_2) \qquad \text{for } i = 1, \ldots, n,\ j = 1, 2, 3 \quad (2.7)$$

A signature on $(X_1, \ldots, X_n) \in \mathbb{G}^n$ is comprised of $9n + 4$ group elements. Subsequently to our work, Abe *et al.* [6, 4] showed how to sign messages in $\mathbb{G}^n$ using $O(1)$ group elements.

We note that the scheme is not structure-preserving in the strict sense since the public key component $A = e(g, g)^a$ lives in the group $\mathbb{G}_T$. However, everything goes through if $A = e(g, g)^a$ is replaced by a pair of public group elements $(A_1, A_2) \in \mathbb{G}^2$ such that $e(A_1, A_2) = e(g, g)^a$.

Regarding the security of the scheme, the following theorem is proved in [81].

Theorem 1 ([81])**.** *The scheme is secure under chosen-message attacks if the HSDH, FlexDH and SDP problems are all hard in* $\mathbb{G}$.

The scheme can also be used to construct non-frameable group signatures that are secure in the concurrent join model of [157] without resorting to random oracles. To the best of our knowledge, before 2009, the Kiayias-Yung construction [157] was the only scalable group signature where joining supports concurrency at both ends while requiring the smallest amount of interaction. In the standard model, our signature scheme thus provided the

first[2] way to achieve the same result. In this case, we have $n = 1$ (since prospective group members only need to certify one group element if non-frameability is ensured by signing messages using Boneh-Boyen signatures [42] in the same way as in Groth's group signature [134]) so that membership certificates comprise 13 group elements and their shape is fully compatible with GS proofs.

2.1.3 A Group Encryption Scheme with Non-Interactive Proofs

In [81], we built a non-interactive GE scheme for the Diffie-Hellman relation $\mathcal{R} = \{(X, Y), W\}$ where $e(g, W) = e(X, Y)$, for which the keys are $\mathsf{pk}_{\mathcal{R}} = \{\mathbb{G}, \mathbb{G}_T, g\}$ and $\mathsf{sk}_{\mathcal{R}} = \varepsilon$. While our example is for the Diffie-Hellman relation, it can be easily generalized to any relation that can be expressed in terms of pairing-product equations for which NIZK proofs are available.

The construction slightly departs from the modular design of [156] in that commitments to the receiver's public key and certificate are part of the proof (instead of the ciphertext), which simplifies the proof of message-security. The security of the scheme eventually relies on the HSDH, FlexDH and DLIN assumptions. All security proofs are available in the full version of [81].

The group manager uses a key pair for our structure-preserving signature of Section 2.1.2 to sign public keys of the DLIN-based version [143, 235] of the Cramer-Shoup cryptosystem [88]. In the latter system, if we assume public generators g_1, g_2, g that are parts of public parameters, each receiver's public key is made of $n = 6$ group elements

$$\begin{array}{rclll} X_1 & = & g_1^{x_1} g^{x} & X_3 = g_1^{x_3} g^{y} & X_5 = g_1^{x_5} g^{z} \\ X_2 & = & g_2^{x_2} g^{x} & X_4 = g_2^{x_4} g^{y} & X_6 = g_2^{x_6} g^{z}. \end{array}$$

To encrypt a plaintext $m \in \mathbb{G}$ under the label[3] L (see [238] for a definition of encryption schemes with labels), the sender picks $r, s \xleftarrow{\$} \mathbb{Z}_p^*$ and computes

$$\psi_{\mathsf{CS}} = \big(U_1, U_2, U_3, U_4, U_5\big) = \Big(g_1^r,\ g_2^s,\ g^{r+s},\ m \cdot X_5^r X_6^s,\ (X_1 X_3^{\alpha})^r \cdot (X_2 X_4^{\alpha})^s\Big),$$

where $\alpha = H(U_1, U_2, U_3, U_4, L) \in \mathbb{Z}_p^*$ is a collision-resistant hash[4]. Given (ψ_{CS}, L), the receiver computes α. He returns $\perp$ if $U_5 \neq U_1^{x_1+\alpha x_3} U_2^{x_2+\alpha x_4} U_3^{x+\alpha y}$ and $m = U_4/(U_1^{x_5} U_2^{x_6} U_3^{z})$ otherwise.

Our GE scheme goes as follows.

$\mathsf{SETUP}_{\mathsf{init}}(\lambda)$: choose bilinear groups $(\mathbb{G}, \mathbb{G}_T)$ of order $p > 2^{\lambda}$, $g \xleftarrow{\$} \mathbb{G}$ and $g_1 = g^{\alpha_1}, g_2 = g^{\alpha_2}$ with $\alpha_1, \alpha_2 \xleftarrow{\$} \mathbb{Z}_p^*$. Define $\mathbf{g_1} = (g_1, 1, g)$, $\mathbf{g_2} = (1, g_2, g)$ and $\mathbf{g_3} = \mathbf{g_1}^{\xi_1} \cdot \mathbf{g_2}^{\xi_2}$ with

[2] Non-frameable group signatures described in [95, 54] achieve concurrent security by having the prospective user generate an extractable commitment to some secret exponent (which the simulator can extract without rewinding using the trapdoor of the commitment) and prove that the committed value is the discrete log. of a public value. In the standard model, this technique requires interaction and the proof should be simulatable in zero-knowledge when proving security against framing attacks. Another technique [113] requires users to prove knowledge of their secret exponent using Groth-Sahai non-interactive proofs. It is nevertheless space-demanding as each bit of committed exponent requires its own extractable GS commitment.

[3] A label is basically a set of public data that is bound to the ciphertext in a non-malleable manner.

[4] The proof of CCA2-security [88, 235] only requires a universal one-way hash function (UOWHF) [207] but collision-resistance is required when the scheme uses labels.

$\xi_1, \xi_2 \xleftarrow{\$} \mathbb{Z}_p^*$, which form a CRS $\mathbf{g} = (\mathbf{g_1}, \mathbf{g_2}, \mathbf{g_3})$ for the perfect soundness setting. Select a strongly unforgeable (as defined in [12]) one time signature scheme $\Sigma = (\mathcal{G}, \mathcal{S}, \mathcal{V})$ and a random member $H : \{0,1\}^* \to \mathbb{Z}_p$ of a collision-resistant hash family. Public parameters consists of $\mathsf{param} = \{\lambda, \mathbb{G}, \mathbb{G}_T, g, \mathbf{g}, \Sigma, H\}$.

$\mathsf{SETUP}_{\mathsf{GM}}(\mathsf{params})$: runs the setup algorithm of the certification scheme described in section 2.1.2 with $n = 6$. The obtained public key consists of

$$\mathsf{pk}_{\mathsf{GM}} = \Big(\mathbf{f},\ A = e(g,g)^{\alpha},\ \Omega = g^{\omega},\ u,\ u_0,\ \{\overline{u}_i\}_{i=1,\ldots,6}\Big)$$

and the matching private key is $\mathsf{sk}_{\mathsf{GM}} = \big(\alpha, \omega, \{\overline{\beta}_i = (\beta_{i,1}, \beta_{i,2}, \beta_{i,3})\}_{i=1,\ldots,6}\big)$.

$\mathsf{SETUP}_{\mathsf{OA}}(\mathsf{params})$: generates $\mathsf{pk}_{\mathsf{OA}} = (Y_1, Y_2, Y_3, Y_4) = (g^{y_1}, g^{y_2}, g^{y_3}, g^{y_4})$, as a public key for Kiltz's tag-based encryption (TBE) scheme [160], and the corresponding private key as $\mathsf{sk}_{\mathsf{OA}} = (y_1, y_2, y_3, y_4)$.

JOIN: the user sends a linear Cramer-Shoup public key $\mathsf{pk} = (X_1, \ldots, X_6) \in \mathbb{G}^6$ to the GM and obtains a certificate

$$\mathsf{cert}_{\mathsf{pk}} = \big(\{(C_{i,1}, C_{i,2}, C_{i,3}), (D_{i,1}, D_{i,2}, D_{i,3})\}_{i=1,\ldots,6}, S_1, S_2, S_3, S_4, S_5\big).$$

$\mathsf{ENC}(\mathsf{pk}_{\mathsf{GM}}, \mathsf{pk}_{\mathsf{OA}}, \mathsf{pk}, \mathsf{cert}_{\mathsf{pk}}, W, L)$: to encrypt $W \in \mathbb{G}$ such that $((X,Y), W) \in \mathcal{R}$ (for public elements $X, Y \in \mathbb{G}$), parse $\mathsf{pk}_{\mathsf{GM}}$, $\mathsf{pk}_{\mathsf{OA}}$ and pk as above and do the following.

1. Generate a one-time signature key pair $(\mathsf{SK}, \mathsf{VK}) \leftarrow \mathcal{G}(\lambda)$.
2. Choose $r, s \xleftarrow{\$} \mathbb{Z}_p^*$ and compute a linear CS encryption of W, the result of which is denoted by ψ_{CS}, under the label $L_1 = L||\mathsf{VK}$ (and using the collision-resistant hash function specified by params).
3. For $i = 1, \ldots, 6$, choose $w_{i,1}, w_{i,2} \xleftarrow{\$} \mathbb{Z}_p^*$ and encrypt X_i under $\mathsf{pk}_{\mathsf{OA}}$ using Kiltz's TBE scheme [160] with the tag VK. Let
$$\psi_{\mathsf{K}_i} = (Y_1^{w_{i,1}}, Y_2^{w_{i,2}}, (g^{\mathsf{VK}} Y_3)^{w_{i,1}}, (g^{\mathsf{VK}} Y_4)^{w_{i,2}}, X_i \cdot g^{w_{i,1}+w_{i,2}})$$
be the ciphertexts.
4. Set the GE ciphertext ψ as $\psi = \mathsf{VK}||\psi_{\mathsf{CS}}||\psi_{\mathsf{K}_1}||\cdots||\psi_{\mathsf{K}_6}||\sigma$ where σ is a one-time signature obtained as $\sigma = \mathcal{S}(\mathsf{sk}, (\psi_{\mathsf{CS}}||\psi_{\mathsf{K}_1}||\cdots||\psi_{\mathsf{K}_6}||L))$.

Return (ψ, L) and $coins_{\psi}$ consist of $\{(w_{i,1}, w_{i,2})\}_{i=1,\ldots,6}$, (r,s). If the one-time signature of [133] is used, VK and σ take 3 and 2 group elements, respectively, so that ψ comprises 40 group elements.

$\mathcal{P}(\mathsf{pk}_{\mathsf{GM}}, \mathsf{pk}_{\mathsf{OA}}, \mathsf{pk}, \mathsf{cert}_{\mathsf{pk}}, (X,Y), W, \psi, L, coins_{\psi})$: parse $\mathsf{pk}_{\mathsf{GM}}$, $\mathsf{pk}_{\mathsf{OA}}$, pk and ψ as above. Conduct the following steps.

1. Generate commitments (as explained in section 1.3) to the $9n + 4 = 58$ group elements that $\mathsf{cert}_{\mathsf{pk}}$ consists of. The resulting overall commitment $com_{\mathsf{cert}_{\mathsf{pk}}}$ contains 184 group elements.

2. Generate GS commitments to the public key elements $\mathsf{pk} = (X_1, \ldots, X_6)$ and obtain the set $com_{\mathsf{pk}} = \{com_{X_i}\}_{i=1,\ldots,6}$, which consists of 18 group elements.
3. Generate a proof $\pi_{\mathsf{cert}_{\mathsf{pk}}}$ that $com_{\mathsf{cert}_{\mathsf{pk}}}$ is a commitment to a valid certificate for the public key contained in com_{pk}. For each $i = 1, \ldots, 6$, relations (2.1)-(2.3) cost 9 elements to prove (and thus 54 elements altogether). The quadratic equation (2.4) takes 9 elements and linear ones (2.5)-(2.6) both require 3 elements. Finally, (2.7) is a set of 18 linear equations which demand 54 elements altogether. The whole proof $\pi_{\mathsf{cert}_{\mathsf{pk}}}$ thus takes 123 group elements.
4. For $i = 1, \ldots, 6$, generate a NIZK proof $\pi_{eq\text{-}key,i}$ that com_{X_i} (which is part of com_{pk}) and ψ_{K_i} are encryptions of the same X_i. If ψ_{K_i} comprises

$$(V_{i,1}, V_{i,2}, V_{i,5}) = (Y_1^{w_{i,1}}, Y_2^{w_{i,2}}, X_i \cdot g^{w_{i,1}+w_{i,2}})$$

and com_{X_i} is parsed as $(c_{X_{i1}}, c_{X_{i2}}, c_{X_{i3}}) = (g_1^{\theta_{i1}} \cdot g_{3,1}^{\theta_{i3}},\ g_2^{\theta_{i2}} \cdot g_{3,2}^{\theta_{i3}},\ X_i \cdot g^{\theta_{i1}+\theta_{i2}} \cdot g_{3,3}^{\theta_{i3}})$, where $w_{i,1}, w_{i,2} \in coins_\psi$, $\theta_{i1}, \theta_{i2}, \theta_{i3} \in \mathbb{Z}_p^*$ and $\mathbf{g_3} = (g_{3,1}, g_{3,2}, g_{3,3})$, this amounts to prove knowledge of values $w_{i,1}, w_{i,2}, \theta_{i1}, \theta_{i2}, \theta_{i3} \in \mathbb{Z}_p^*$ such that

$$\Big(\frac{V_{i,1}}{c_{X_{i1}}}, \frac{V_{i,2}}{c_{X_{i2}}}, \frac{V_{i,3}}{c_{X_{i3}}}\Big) = \big(Y_1^{w_{i,1}} \cdot g_1^{-\theta_{i1}} \cdot g_{3,1}^{-\theta_{i3}},\ Y_2^{w_{i,2}} \cdot g_2^{-\theta_{i2}} \cdot g_{3,2}^{-\theta_{i3}},\ g^{w_{i,1}+w_{i,2}-\theta_{i1}-\theta_{i2}} \cdot g_{3,3}^{-\theta_{i3}}\big).$$

Committing to the encryption exponents $w_{i,1}, w_{i,2}, \theta_{i1}, \theta_{i2}, \theta_{i3}$ introduces 90 group elements whereas the above relations only require two elements each. Overall, proof elements $\pi_{eq\text{-}key,1}, \ldots, \pi_{eq\text{-}key,6}$ incur 126 elements.
5. Generate a NIZK proof $\pi_{val\text{-}enc}$ that $\psi_{\mathsf{CS}} = (U_1, U_2, U_3, U_4, U_5)$ is a valid CS encryption. This requires to commit to underlying encryption exponents $r, s \in coins_\psi$ and prove that $U_1 = g_1^r$, $U_2 = g_2^s$, $U_3 = g^{r+s}$ (which only takes 3 times 2 elements as base elements are public) and $U_5 = (X_1 X_3^\alpha)^r \cdot (X_2 X_4^\alpha)^s$ (which takes 9 elements since base elements are themselves variables). Including commitments com_r and com_s to exponents r and s, $\pi_{val\text{-}enc}$ demands 21 group elements overall.
6. Generate a NIZK proof $\pi_{\mathcal{R}}$ that the ciphertext ψ_{CS} encrypts a group element $W \in \mathbb{G}$ such that $((X, Y), W) \in \mathcal{R}$. To this end, generate a commitment

$$com_W = (c_{W,1}, c_{W,2}, c_{W,3}) = (g_1^{\theta_1} \cdot g_{3,1}^{\theta_3},\ g_2^{\theta_2} \cdot g_{3,2}^{\theta_3},\ W \cdot g^{\theta_1+\theta_2} \cdot g_{3,3}^{\theta_3})$$

and prove that the underlying W is the same as the one for which $U_4 = W \cdot X_5^r \cdot X_6^s$ in ψ_{CS}. In other words, prove knowledge of exponents $r, s, \theta_1, \theta_2, \theta_3$ such that

$$\Big(\frac{U_1}{c_{W,1}}, \frac{U_2}{c_{W,2}}, \frac{U_4}{c_{W,3}}\Big) = \big(g_1^{r-\theta_1} \cdot g_{3,1}^{-\theta_3},\ g_2^{s-\theta_2} \cdot g_{3,2}^{-\theta_3},\ g^{-\theta_1-\theta_2} \cdot g_{3,3}^{-\theta_3} \cdot X_5^r \cdot X_6^s\big). \quad (2.8)$$

Commitments to r, s are already part of $\pi_{val\text{-}enc}$. Committing to $\theta_1, \theta_2, \theta_3$ takes 9 elements. Proving the first two relations of (2.8) requires 4 elements whereas the third one is quadratic and its proof is 9 elements. Proving the linear pairing-product relation $e(g, W) = e(X, Y)$ in NIZK[5] demands 9 elements. Since $\pi_{\mathcal{R}}$ includes com_W, it entails a total of 34 elements.

[5]It requires to introduce an auxiliary variable $\mathcal{X}$ and prove that $e(g, \mathcal{W}) = e(\mathcal{X}, Y)$ and $\mathcal{X} = X$, for variables $\mathcal{W}, \mathcal{X}$ and constants g, X, Y. The two proofs take 3 elements each and 3 elements are needed to commit to $\mathcal{X}$.

The entire proof $\pi_\psi = com_{\mathsf{cert_{pk}}}||com_{\mathsf{pk}}||\pi_{\mathsf{cert_{pk}}}||\pi_{eq\text{-}key,1}||\cdots||\pi_{eq\text{-}key,6}||\pi_{val\text{-}enc}||\pi_{\mathcal{R}}$ eventually takes 516 elements.

$\mathcal{V}(\mathsf{params}, \psi, L, \pi_\psi, \mathsf{pk_{GM}}, \mathsf{pk_{OA}})$: parse $\mathsf{pk_{GM}}$, $\mathsf{pk_{OA}}$, pk, ψ and π_ψ as above. Return 1 if and only if $\mathcal{V}(\mathsf{VK}, \sigma, (\psi_{\mathsf{CS}}||\psi_{\mathsf{K}_1}||\cdots||\psi_{\mathsf{K}_6}||L)) = 1$, all proofs verify and if $\psi_{\mathsf{K}_1}, \ldots, \psi_{\mathsf{K}_6}$ are all valid tag-based encryptions w.r.t. the tag VK.

$\mathsf{DEC}(\mathsf{sk}, \psi, L)$: parse the ciphertext ψ as $\mathsf{VK}||\psi_{\mathsf{CS}}||\psi_{\mathsf{K}_1}||\cdots||\psi_{\mathsf{K}_6}||\sigma$. Return $\perp$ in the event that $\mathcal{V}(\mathsf{VK}, \sigma, (\psi_{\mathsf{CS}}||\psi_{\mathsf{K}_1}||\cdots||\psi_{\mathsf{K}_6}||L)) = 0$. Otherwise, use sk to decrypt (ψ_{CS}, L).

$\mathsf{OPEN}(\mathsf{sk_{OA}}, \psi, L)$: parse ψ as $\mathsf{VK}||\psi_{\mathsf{CS}}||\psi_{\mathsf{K}_1}||\cdots||\psi_{\mathsf{K}_6}||\sigma$. Return $\perp$ if $\psi_{\mathsf{K}_1}, \ldots, \psi_{\mathsf{K}_6}$ are not all valid TBE ciphertexts w.r.t. the tag VK or if $\mathcal{V}(\mathsf{VK}, \sigma, (\psi_{\mathsf{CS}}||\psi_{\mathsf{K}_1}||\cdots||\psi_{\mathsf{K}_6}||L)) = 0$. Otherwise, decrypt $\psi_{\mathsf{K}_1}, \ldots, \psi_{\mathsf{K}_6}$ using $\mathsf{sk_{OA}}$ and return the resulting $\mathsf{pk} = (X_1, \ldots, X_6)$.

The following security result was proved in [81].

Theorem 2 ([81]). *The above group encryption system provides message privacy, anonymity and soundness assuming that H is a collision-resistant hash function and that the HSDH, FlexDH, and DLIN problems are all hard in $\mathbb{G}$.*

From an efficiency standpoint, the length of ciphertexts is about 4.5 kB in an implementation using symmetric pairings with a 512-bit group order. Moreover, our proofs only require 32.250 kB. This is significantly cheaper than in the original GE scheme [156] where, for 1024-bit RSA moduli, interactive proofs reach a communication cost of 70 kB to achieve a 2^{-50} knowledge error.

Of course, the above construction can be made significantly more efficient if our structure-preserving signature is replaced by the construction of Abe *et al.* [6], which was recalled in Section 1.5. In [176], we used the latter SPS system to build a group encryption scheme where, as in traceable signatures [155], the tracing authority can release a user-specific trapdoor that allows tracing all ciphertexts encrypted for a given user.

2.2 Group Signatures with Efficient Revocation in the Standard Model

Group signatures are a central cryptographic primitive, suggested by Chaum and van Heyst [85], which allows members of a population of users managed by some authority to sign messages in the name of the group while hiding their identity. At the same time, a tracing authority is capable of identifying the signer if necessary. A crucial problem is the revocation of the anonymous signing capability of users when they are banned from or intentionally leave the group.

2.2.1 Related Work

GROUP SIGNATURES. The first efficient and provably coalition-resistant group signature dates back to the work of Ateniese, Camenisch, Joye and Tsudik [15]. By the time their scheme appeared, the security of the primitive was not appropriately formalized yet. Suitable security definitions remained lacking until the work of Bellare, Micciancio and Warinschi [31] (BMW) who captured all the requirements of group signatures in three properties.

In (a variant of) this model, Boneh, Boyen and Shacham [44] obtained very short signatures using the random oracle methodology [32].

The BMW model assumes static groups where no new member can be introduced after the setup phase. The setting of dynamically changing groups was analyzed later on by Bellare-Shi-Zhang [33] and, independently, by Kiayias and Yung [158]. In the models of [33, 158], constructions featuring relatively short signatures were proposed in [210, 95]. A construction in the standard model was also suggested by Ateniese *et al.* [14] under interactive assumptions. At the same time, Boyen and Waters gave a different solution [55] without random oracles using more standard assumptions. By improving upon their own scheme, they managed [56] to obtain signatures of constant size. Their constructions [55, 56] were both presented in the BMW model [31] and provide anonymity in the absence of signature opening oracle. In the dynamic model [33], Groth [133] showed a system in the standard model with $O(1)$-size signatures but, due to very large hidden constants, his scheme was mostly a feasibility result. Later on, Groth came up with an efficient realization [134] (and signatures of about 50 group elements) with the strongest anonymity level.

REVOCATION. As in ordinary PKIs, where certificate revocation is a critical issue, membership revocation is a complex problem that has been extensively studied [57, 17, 68, 52] in the last decade. Generating a new group public key and distributing new signing keys to unrevoked members is a simple solution. In large groups, it is impractical to update the public key and provide members with new keys after they joined the group. Bresson and Stern suggested a different approach [57] consisting of having the signer prove that his membership certificate does not belong to a list of revoked certificates. Unfortunately, the length of signatures grows with the number of revoked members. In forward-secure group signatures, Song [240] chose a different way to handle revocation but verification takes linear time in the number of excluded users.

Camenisch and Lysyanskaya [68] proposed an elegant method using accumulators[6] [34]. Their technique, also used in [243, 66], allows revoking members while keeping $O(1)$ costs for signing and verifying. The downside of this approach is its history-dependence: it requires users to follow the dynamic evolution of the group and keep track of all changes: each revocation incurs a modification of the accumulator value, so that unrevoked users have to upgrade their membership certificate before signing new messages. In the worst case, this may require up to $O(r)$ exponentiations, if r is the number of revoked users.

Another drawback of accumulator-based approaches is their limited applicability in the standard model. Indeed, for compatibility reasons with the central tool of Groth-Sahai proofs, pairing-based accumulators are the only suitable candidates. However, in known pairing-based accumulators [209, 66], public keys have linear size in the maximal number of accumulations, which would result in linear-size group public keys in immediate implementations. To address this concern in delegatable anonymous credentials, Acar and Nguyen [8] chose to sacrifice the constant size of proofs of non-membership but, in group signatures, this would prevent signatures from having constant size. Boneh, Boyen and Shacham [44] managed to avoid linear dependencies in a revocation mechanism along the lines of [68]. Unfortunately, their technique does not seem to readily interact[7] with Groth-Sahai proofs

[6] An accumulator is a kind of "hash" function mapping a set of values to a short, constant-size string while allowing to efficiently prove that a specific value was accumulated.

[7] In [44], signing keys consist of pairs $(g^{1/(\omega+s)}, s) \in \mathbb{G} \times \mathbb{Z}_p$, where $\omega \in \mathbb{Z}_p$ is the secret key of the group manager, and the revocation method relies on the availability of the exponent $s \in \mathbb{Z}_p$. In the standard model,

[138] so as to work in the standard model. Moreover, like the Camenisch-Lysyanskaya technique [68], the Boneh-Boyen-Shacham method may require up to $O(r)$ exponentiations to update unrevoked users' private keys if r is the cardinality of the processed revocation list.

In [58], Brickell considered the notion of *verifier-local revocation* group signatures, for which formal definitions were given by Boneh and Shacham [52] and other extensions were proposed in [203, 251, 185]. In this approach, revocation messages are only sent to verifiers and the signing algorithm is completely independent of the number of revocations. Verifiers take as additional input a revocation list (RL), maintained by the group manager, and have to perform a revocation test for each RL entry in order to be convinced that signatures were not issued by a revoked member (a similar revocation mechanism is used in [59]). The verification cost is thus inevitably linear in the number of expelled users.

In 2009, Nakanishi, Fuji, Hira and Funabiki [202] came up with a revocable group signature with constant complexities for signing/verifying. At the same time, group members never have to update their keys. On the other hand, their proposal suffers from linear-size group public keys in the maximal number N of users, although a variant reduces the group public key size to $O(N^{1/2})$.

In anonymous credentials, Tsang *et al.* [241, 242] showed how to prevent users from anonymously authenticating themselves without compromising their anonymity or involving a trusted third party. Their schemes either rely on accumulators (which may be problematic in our setting) or have linear proving complexity in the number of revocations. Camenisch, Kohlweiss and Soriente [67] dealt with revocations in anonymous credentials by periodically updating users credentials in which a specific attribute indicates a validity period. In group signatures, their technique would place an important burden on the group manager who would have to generate updates for each unrevoked individual credential.

2.2.2 Our Results

For various reasons, none of the previously mentioned constructions conveniently supports large groups, especially if we restrict ourselves to constructions without random oracles.

Together with Moti Yung and Thomas Peters [180], we described a novel revocation mechanism, borrowed from the literature on broadcast encryption, which is truly scalable and well-suited to constructions in the standard model. Using the Subset Cover framework of Naor, Naor and Lotspiech [205] (NNL), we provided two distinct constructions [180, 179] of history-independent revocable group signatures in the standard model. Our technique [180] blends well with structure-preserving signatures and Groth-Sahai proofs.

Constructions with polylog-size private keys

As in the NNL Subset Cover framework [205], our first revocable group signature assigns each group member to a leaf of a binary tree and, at any time, the set $\{1, \ldots, N\} \backslash \mathcal{R}$ of unrevoked group members is partitioned into a collection $S_1, \ldots, S_m$ of disjoint subsets of leaves, for some $m \in \mathbb{N}$. Each unrevoked member should belong to exactly one subset S_i in the cover of authorized leafs determined by the group manager. In order to sign a message, an authorized member thus has to demonstrate that he is not revoked by proving his membership of one of the subsets S_i without revealing which one. In its best tradeoff, our first

the Groth-Sahai techniques would require to turn the membership certificates into triples $(g^{1/(\omega+s)}, g^s, u^s)$, for some $u \in \mathbb{G}$ (as in [56]), which is not compatible with the revocation mechanism.

construction [180] builds on the public-key variant, due to Dodis and Fazio [99], of the Subset Difference (SD) method [205], where unrevoked group members $\{1, \ldots, N\} \setminus \mathcal{R} = \bigcup_{i=1}^{m} S_i$ are partitioned into a collection of $m = O(|\mathcal{R}|)$ subsets, each of which is the difference between two sub-trees.

Like the Dodis-Fazio construction [99], our first group signature builds on hierarchical identity-based encryption (HIBE) and uses the property that, in the broadcast encryption system of [99], each ciphertext can be seen as a collection of $m = O(|\mathcal{R}|)$ HIBE ciphertexts (one for each subset S_i of the partition), which is turned into a revocation list. In short, our group signature can be seen as having authorized group members prove that they are not revoked by showing their ability to decrypt a HIBE ciphertext contained in the revocation list. Of course, for anonymity purposes, the signer should not reveal which HIBE ciphertext he is able to decrypt since it would leak information on his position in the tree. For this reason, the relevant entry of the revocation list only appears in committed form in the group signature. In order to prove that he is using a legal entry of the revocation list, the user generates a set membership proof [61] and proves knowledge of a signature from the group manager on the committed RL entry. It is worth noting that RLs are *not* part of the group public key: verifiers only need to know the number of the latest revocation epoch and they should not bother to read RLs entirely.

This method features constant signature size and verification time, $O(\log N)$-size group public keys, revocation lists of size $O(r)$ (as in standard PKIs and group signatures with verifier-local revocation) and membership certificates of size $O(\log^3 N)$. In a different trade-off of the same high-level construction, we can reduce the private key size to $O(\log N)$ using the Complete Subtree method [205]. In this case, however, revocation lists are inflated by a factor of $O(\log N/r)$. While the Layered Subset Difference method [140] allows for noticeable improvements, the constructions of [180] still suffer from relatively large membership certificates. We remark, however, that some logarithmic dependency is expected when basing revocation on a tree-like NNL methodology.

For groups of N members, our first constructions thus feature constant-size signatures and verification time at the cost of membership certificates of size $O(\log^3 N)$ (or $O(\log^{2.5} N)$ using the Layered Subset Difference method). In many applications, this can become rather expensive even for moderately large groups: for example, using the Subset Difference method with $N = 1000 \approx 2^{10}$, users may have to privately store thousands of group elements. In order to be competitive with other group signatures in the standard model such as [134] and still be able to revoke members while keeping them "stateless", it is desirable to avoid this storage complexity.

Constructions with Short Private Keys

In our second main construction of revocable group signature [179], we managed to get rid of the polylogarithmic complexity in the private key size and obtained constant-size membership certificates while retaining the same complexities in other metrics. This improvement was achieved at the expense of relying on a somewhat stronger (but still falsifiable) hardness assumption in the security proofs.

Our improved construction [179] also builds on the NNL Subset Cover framework [205] to partition the subset of authorized users using the Subset Difference method. However, instead of relying on a broadcast encryption system, it leverages the properties of a special kind of commitment schemes introduced by Moti Yung and myself in 2010 [188]. These com-

mitments yield private keys of *constant* size without degrading other performance criteria. This may sound somewhat surprising since, in the SD method, (poly)logarithmic complexities inherently seem inevitable in several metrics. Indeed, in the context of broadcast encryption [205], it requires private keys of size $O(\log^2 N)$ (and even $O(\log^3 N)$ in the public key setting [99] if the result of Boneh-Boyen-Goh [43] is used). Here, we reduce this overhead to a constant while the only dependency on N is a $O(\log N)$-size group public key.

Instead of relying on hierarchical identity-based encryption [45, 144, 123] as in the public-key variant [99] of NNL, our improved construction employs *concise* vector commitment schemes [188, 75], where each commitment can be opened w.r.t. individual coordinates in a space-efficient manner (namely, the size of a coordinate-wise opening does not depend on the length of the vector). These vector commitments interact nicely with the specific shape of subsets – as differences between two subtrees – in the SD method. Using them, we compactly encode as a vector the path from the user's leaf to the root. To provide evidence of their inclusion in one of the SD subsets, group members successively prove the equality and the inequality between two coordinates of their vector (i.e., two nodes of the path from their leaf to the root) and specific node labels indicated by an appropriate entry of the revocation list. This is where the position-wise openability of concise commitments is very handy.

The use of concise commitments allows making the most of the Subset Cover approach [180] by reducing the size of membership certificates to a small constant: at the cost of lengthening signatures by a small constant factor (roughly 1.5), we obtain membership certificates consisting of only 9 group elements and a small integer. For $N = 1000$, users' private keys are thus compressed by a multiplicative factor of several hundreds and this can only become more dramatic for larger groups. At the same time, our main scheme retains all the useful properties of [180]: like the construction of Nakanishi *et al.* [202], it does not require users to update their membership certificates at any time but, unlike [202], our group public key size is $O(\log N)$. Like the SD-based construction of [180], our improved system uses revocation lists of size $O(r)$, which is on par with Certificate Revocation Lists (CRLs) of standard PKIs.

Eventually, we thus obtain revocable group signatures that become competitive with the regular CRL approach in PKIs: signature generation and verification have constant cost, signatures and membership certificates being of $O(1)$-size while revocation lists have size $O(r)$. It is conceivable that our improved revocation technique can find applications beyond group signatures.

2.2.3 Definition of Group Signatures with Revocation

We consider group signature schemes that have their lifetime divided into revocation periods at the beginning of which group managers update their revocation lists. The syntax and the security model are built on those defined by Kiayias and Yung [158]. Like the Bellare-Shi-Zhang model [33], the Kiayias-Yung (KY) model assumes an interactive *join* protocol whereby a prospective user becomes a group member by interacting with the group manager. This protocol provides the user with a membership certificate and a membership secret.

Syntax. We denote by $N \in \mathsf{poly}(\lambda)$ the maximal number of group members. At the beginning of each revocation period t, the group manager publicizes an up-to-date revocation list RL_t and we denote by $\mathcal{R}_t \subset \{1, \ldots, N\}$ the corresponding set of revoked users (we assume that $\mathcal{R}_t$ is part of RL_t). A revocable group signature (R-GS) scheme consists of the following algorithms or protocols.

Setup(λ, N)**:** given a security parameter $\lambda \in \mathbb{N}$ and a maximal number of group members $N \in \mathbb{N}$, this algorithm (which is run by a trusted party) generates a group public key $\mathcal{Y}$, the group manager's private key $\mathcal{S}_{\mathsf{GM}}$ and the opening authority's private key $\mathcal{S}_{\mathsf{OA}}$. Keys $\mathcal{S}_{\mathsf{GM}}$ and $\mathcal{S}_{\mathsf{OA}}$ are given to the appropriate authority while $\mathcal{Y}$ is publicized. The algorithm also initializes a public state St comprising a set data structure $St_{\mathsf{users}} = \emptyset$ and a string data structure $St_{\mathsf{trans}} = \epsilon$, which are initially empty.

Join: is an interactive protocol between the group manager GM and a user $\mathcal{U}_i$ who becomes a group member. The protocol involves two interactive Turing machines $\mathsf{J}_{\mathsf{user}}$ and J_{GM} that both take $\mathcal{Y}$ as input. The execution ends with user $\mathcal{U}_i$ obtaining a membership secret sec_i, that no one else knows, and a membership certificate cert_i. If the protocol is successful, the GM updates the public state St by setting $St_{\mathsf{users}} := St_{\mathsf{users}} \cup \{i\}$ as well as $St_{\mathsf{trans}} := St_{\mathsf{trans}} || \langle i, \mathsf{transcript}_i \rangle$.

Revoke: is a (possibly randomized) algorithm allowing the GM to generate an updated revocation list RL_t for the new revocation period t. It takes as input a public key $\mathcal{Y}$ and a set $\mathcal{R}_t \subset St_{\mathsf{users}}$ that identifies the users to be revoked. It outputs an updated revocation list RL_t for period t.

Sign: given a revocation period t with its revocation list RL_t, a membership certificate cert_i, a membership secret sec_i and a message M, this algorithm outputs $\perp$ if $i \in \mathcal{R}_t$ and a signature σ otherwise.

Verify: given a signature σ, a revocation period t, the corresponding revocation list RL_t, a message M and a group public key $\mathcal{Y}$, this algorithm returns either 0 or 1.

Open: takes as input a message M, a valid signature σ w.r.t. $\mathcal{Y}$ for the indicated revocation period t, the opening authority's private key $\mathcal{S}_{\mathsf{OA}}$ and the public state St. It outputs $i \in St_{\mathsf{users}} \cup \{\perp\}$, which is the identity of a group member or a symbol indicating an opening failure.

In our extension of the Kiayias-Yung model [158], a R-GS scheme must satisfy three security notions.

The first one is called *security against misidentification attacks*. It requires that, even if the adversary can introduce and revoke users at will, it cannot produce a signature that traces outside the set of unrevoked adversarially-controlled users. As in ordinary group signatures, the notion of *security against framing attacks* captures that under no circumstances should an honest user be held accountable for messages that he did not sign, even if the whole system conspired against him. Finally, the notion of *anonymity* is also defined by granting the adversary access to a signature opening oracle as in the models of [33, 158].

These security properties are formalized using experiments which are described in the articles in appendices. In short, they can be outlined as follows.

In a misidentification attack, the adversary can corrupt the opening authority. Moreover, he can also introduce malicious users in the group and revoke users at any time. His purpose is to come up with a signature $\sigma^\star$ that verifies w.r.t. $RL_{t^\star}$, where $t^\star$ denotes the current revocation period. He is deemed successful if the produced signature $\sigma^\star$ does not open to any unrevoked adversarially-controlled. The definition extends the usual definition [158] in that $\mathcal{A}$ also wins if his forgery $\sigma^\star$ verifies w.r.t. $RL_{t^\star}$ but opens to an adversarially-controlled user that *was* revoked during the revocation period $t^\star$.

Framing attacks consider the situation where the entire system, including the group manager and the opening authority, is colluding against some honest user. The adversary can corrupt the group manager as well as the opening authority. He is also allowed to introduce honest group members, observe the system while these users sign messages and create dummy users. In addition, before the possible corruption of the group manager, the adversary can revoke group members at any time. As a potentially corrupted group manager, $\mathcal{A}$ is allowed to come up with his own revocation list $RL_{t^\star}$ at the end of the game. We assume that anyone can publicly verify that $RL_{t^\star}$ is correctly formed so that the adversary does not come up with an ill-formed revocation list.

The notion of anonymity is formalized by means of a game involving a two-stage adversary. The first stage allows the adversary $\mathcal{A}$ to open arbitrary signatures by probing a signature opening oracle. When this stage ends, $\mathcal{A}$ chooses a message-period pair $(M^\star, t^\star)$ as well as two pairs $(\mathsf{sec}_0^\star, \mathsf{cert}_0^\star)$, $(\mathsf{sec}_1^\star, \mathsf{cert}_1^\star)$, consisting of a valid membership certificate and a corresponding membership secret. Then, the challenger flips a coin $d \leftarrow \{0,1\}$ and computes a challenge signature $\sigma^\star$ using $(\mathsf{sec}_d^\star, \mathsf{cert}_d^\star)$. The adversary is given $\sigma^\star$ with the task of eventually guessing the bit $d \in \{0,1\}$. Before doing so, he/she is allowed further oracle queries throughout the second stage, called guess stage, but is restricted not to query the opening oracle for $(M^\star, \sigma^\star, t^\star)$.

2.2.4 Our Construction with Short Private Keys

Our construction [179] with short private keys relies on concise vector commitment schemes, where commitments can be opened with a short de-commitment string for each individual coordinate. Such commitments based on ideas from [49, 66] were described by Libert and Yung [188] and, under weaker assumptions, by Catalano and Fiore [75]. In [188], the commitment key is $ck = (g, g_1, \ldots, g_\ell, g_{\ell+2}, \ldots, g_{2\ell}) \in \mathbb{G}^{2\ell}$, where $g_i = g^{(\alpha^i)}$ for each i. The trapdoor of the commitment is $g_{\ell+1}$, which does not appear in ck. To commit to a vector $(m_1, \ldots, m_\ell)$, the committer picks $r \xleftarrow{\$} \mathbb{Z}_p$ and computes $C = g^r \cdot \prod_{\kappa=1}^{\ell} g_{\ell+1-\kappa}^{m_\kappa}$. A single group element $W_i = g_i^r \cdot \prod_{\kappa=1,\kappa\neq i}^{\ell} g_{\ell+1-\kappa+i}^{m_\kappa}$ provides evidence that m_i is the i-th component of the vector as it satisfies the relation $e(g_i, C) = e(g, W_i) \cdot e(g_1, g_\ell)^{m_i}$. The infeasibility of opening a commitment to two distinct messages for some coordinate i relies on the ℓ-DHE assumption. For our purposes, we only rely on the position-wise binding property of vector commitments and do not need them to be hiding. The randomizer r will thus be removed from of C.

Intuition

The number of users is assumed to be $N = 2^{\ell-1} \in \mathsf{poly}(\lambda)$, for some integer ℓ, so that each group member is assigned to a leaf of the tree. Each node is assigned a unique identifier. For simplicity, the root is identified by $\mathcal{ID}(\epsilon) = 1$ and, for each other node x, we define the identifier $\mathcal{ID}(x) \in \{1, \ldots, 2N-1\}$ to be $\mathcal{ID}(x) = 2 \cdot \mathcal{ID}(\mathsf{parent}(x)) + b$, where $\mathsf{parent}(x)$ denotes x's father in the tree and $b = 0$ (resp. $b = 1$) if x is the left (resp. right) child of its father. The root of the tree is assigned the identifier $\mathcal{ID}(\epsilon) = 1$.

At the beginning of each revocation period t, the GM generates an up-to-date revocation list RL_t containing one entry for each generic subset $S_{k_1,u_1}, \ldots, S_{k_m,u_m}$ produced by the Subset Difference method. These subsets are encoded in such a way that unrevoked users

can anonymously prove their membership of one of them. Our technique allows doing this using a proof of *constant* size.

The intuition is as follows. In the generation of RL_t, for each $i \in \{1, \ldots, m\}$, if x_{k_i} (resp. x_{u_i}) denotes the primary (resp. secondary) root of S_{k_i,u_i}, the GM encodes S_{k_i,u_i} as a vector of group elements R_i that determines the levels of nodes x_{k_i} and x_{u_i} in the tree (which are called ϕ_i and ψ_i hereafter) and the identifiers $\mathcal{ID}(x_{k_i})$ and $\mathcal{ID}(x_{u_i})$. Then, the resulting vector R_i is authenticated by means of a structure-preserving signature Θ_i, which is included in RL_t and will be used in a set membership proof.

During the join protocol, users obtain from the GM a structure-preserving signature on a compact encoding C_v – which is computed as a concise commitment to a vector of node identifiers $(I_1, \ldots, I_\ell)$ – of the path $(I_1, \ldots, I_\ell)$ between their leaf v and the root ϵ. This path is encoded as a single group element.

The group manager uses two key pairs for the AHO structure-preserving signature. The first one is used during the join protocol to bind a group element X chosen by the user, who knows $x = \log_g(X)$, to the path from the user's leaf v to the root ϵ.

In order to anonymously prove his/her non-revocation, a group member $\mathcal{U}_i$ uses RL_t to determine the generic subset S_{k_l,u_l}, with $l \in \{1, \ldots, m\}$, where his/her leaf v_i lies. He/she commits to the corresponding vector of group elements R_l that encodes the node identifiers $\mathcal{ID}(x_{k_l})$ and $\mathcal{ID}(x_{u_l})$ of the primary and secondary roots of S_{k_l,u_l} at levels ϕ_l and ψ_l, respectively. If $(I_1, \ldots, I_\ell)$ identifies the path from his/her leaf v_i to ϵ, the unrevoked member $\mathcal{U}_i$ generates a membership proof for the subset S_{k_l,u_l} by proving that $\mathcal{ID}(x_{k_l}) = I_{\phi_l}$ and $\mathcal{ID}(x_{u_l}) \neq I_{\psi_l}$ (in other words, that x_{k_l} is an ancestor of v_i and x_{u_l} is not). To succinctly prove these statements, $\mathcal{U}_i$ uses the properties of the LY concise vector commitment scheme[8]. Finally, in order to convince the verifier that he used a legal element of RL_t, $\mathcal{U}_i$ follows the technique of [61] and proves knowledge of a signature Θ_l on the committed vector of group elements R_l. By doing so, $\mathcal{U}_i$ thus provides evidence that his/her leaf v_i is a member of some authorized subset S_{k_l,u_l} without revealing $l \in \{1, \ldots, m\}$.

In order to obtain the strongest flavor of anonymity (*i.e.*, where the adversary has access to a signature opening oracle), the scheme uses Kiltz's tag-based encryption scheme as in Groth's construction [134] exactly as we did in the previous construction. In non-frameability concerns, the group member $\mathcal{U}_i$ also generates a weak Boneh-Boyen signature (which yields a fully secure signature when combined with a one-time signature) using $x = \log_g(X)$, where $X \in \mathbb{G}$ is a group element certified by the GM and bound to the path $(I_1, \ldots, I_\ell)$ during the join protocol.

Description

As in standard security models for group signatures, we assume that, before joining the group, user $\mathcal{U}_i$ chooses a long term key pair $(\mathsf{usk}[i], \mathsf{upk}[i])$ and registers it in some PKI.

Setup(λ, N)**:** given a security parameter $\lambda \in \mathbb{N}$ and the number of users $N = 2^{\ell-1}$,

1. Choose bilinear groups $(\mathbb{G}, \mathbb{G}_T)$ of prime order $p > 2^\lambda$, with $g \leftarrow \mathbb{G}$.
2. Define $n_0 = 2$ and $n_1 = 5$. Generates key pairs $(sk^{(0)}_{\mathsf{AHO}}, pk^{(0)}_{\mathsf{AHO}})$ and $(sk^{(1)}_{\mathsf{AHO}}, pk^{(1)}_{\mathsf{AHO}})$ for the AHO signature in order to sign messages of n_0 and n_1 group elements,

[8] Note that no randomness is needed here since we do not rely on the hiding property of the commitment.

respectively. These key pairs are

$$pk_{\mathsf{AHO}}^{(d)} = \Big(G_r^{(d)}, H_r^{(d)}, G_z^{(d)} = G_r^{\gamma_z^{(d)}}, H_z^{(d)} = H_r^{\delta_z^{(d)}}, \\ \{G_i^{(d)} = G_r^{\gamma_i^{(d)}}, H_i^{(d)} = H_r^{\delta_i^{(d)}}\}_{i=1}^{n_d}, A^{(d)}, B^{(d)}\Big)$$

and $sk_{\mathsf{AHO}}^{(d)} = \big(\alpha_a^{(d)}, \alpha_b^{(d)}, \gamma_z^{(d)}, \delta_z^{(d)}, \{\gamma_i^{(d)}, \delta_i^{(d)}\}_{i=1}^{n_d}\big)$, where $d \in \{0,1\}$. These will be used to sign messages consisting of 2 and 5 group elements, respectively.

3. Generate a public key $ck = (g_1, \ldots, g_\ell, g_{\ell+2}, \ldots, g_{2\ell}) \in \mathbb{G}^{2\ell-1}$ for ℓ-dimension vectors of the LY concise vector commitment scheme. The trapdoor $g_{\ell+1}$ is not needed and can be discarded.
4. As a Groth-Sahai CRS for the NIWI proof system, select three vectors $\mathbf{f} = (\mathbf{f_1}, \mathbf{f_2}, \mathbf{f_3})$ such that $\mathbf{f_1} = (f_1, 1, g) \in \mathbb{G}^3$, $\mathbf{f_2} = (1, f_2, g) \in \mathbb{G}^3$, and $\mathbf{f_3} = \mathbf{f_1}^{\xi_1} \cdot \mathbf{f_2}^{\xi_2}$, where $f_1 = g^{\beta_1}, f_2 = g^{\beta_2}$ in $\mathbb{G}$ and random $\beta_1, \beta_2, \xi_1, \xi_2 \leftarrow \mathbb{Z}_p^*$. We also define the vector $\boldsymbol{\varphi} = \mathbf{f_3} \cdot (1, 1, g)$.
5. Choose random $(U, V) \leftarrow \mathbb{G}^2$ that, together with generators $f_1, f_2, g \in \mathbb{G}$, will form a public encryption key.
6. Select a strongly unforgeable one-time signature $\Sigma = (\mathcal{G}, \mathcal{S}, \mathcal{V})$.
7. Sets $\mathcal{S}_{\mathsf{GM}} := \big(sk_{\mathsf{AHO}}^{(0)}, sk_{\mathsf{AHO}}^{(1)}\big)$, $\mathcal{S}_{\mathsf{OA}} := (\beta_1, \beta_2)$ as authorities' private keys and the group public key is

$$\mathcal{Y} := \Big(g,\ pk_{\mathsf{AHO}}^{(0)},\ pk_{\mathsf{AHO}}^{(1)},\ ck,\ \mathbf{f},\ \boldsymbol{\varphi},\ (U, V),\ \Sigma\Big).$$

Join$^{(\mathrm{GM},\mathcal{U}_i)}$**:** the GM and the prospective user $\mathcal{U}_i$ run the following protocol:

1. $\mathcal{U}_i$ draws $x \leftarrow \mathbb{Z}_p$ at random and computes $X = g^x$ which is sent to the GM. If $X \in \mathbb{G}$ already appears in some entry $\mathsf{transcript}_j$ of the database St_{trans}, $\mathsf{J_{GM}}$ halts and returns $\perp$ to $\mathcal{U}_i$.
2. The GM assigns to the user $\mathcal{U}_i$ an available leaf v of identifier $\mathcal{ID}(v)$ in the tree T. Let $x_1, \ldots, x_\ell$ be the path from the chosen leaf $x_\ell = v$ to the root $x_1 = \epsilon$ of T. Let also $(I_1, \ldots, I_\ell) = (\mathcal{ID}(x_1), \ldots, \mathcal{ID}(x_\ell))$ be the corresponding vector of identifiers (with $I_1 = 1$ and $I_\ell = \mathcal{ID}(v) \in \{N, \ldots, 2N-1\}$). Then, the GM does the following.
   (a) Compute a compact encoding $C_v = \prod_{\kappa=1}^{\ell} g_{\ell+1-\kappa}^{I_\kappa} = g_\ell^{I_1} \cdots g_1^{I_\ell}$ of $(I_1, \ldots, I_\ell)$.
   (b) Using $sk_{\mathsf{AHO}}^{(0)}$, generate an AHO signature $\sigma_v = (\theta_{v,1}, \ldots, \theta_{v,7})$ on the pair $(X, C_v) \in \mathbb{G}^2$ so as to bind C_v to the value X that identifies $\mathcal{U}_i$.
3. The GM sends $\mathcal{ID}(v) \in \{N, \ldots, 2N-1\}$ and C_v to $\mathcal{U}_i$ that halts if $\mathcal{ID}(v) \notin \{N, \ldots, 2N-1\}$ or if C_v is found incorrect. Otherwise, $\mathcal{U}_i$ sends an ordinary digital signature $sig_i = \mathrm{Sign}_{\mathsf{usk}[i]}\big(X||(I_1, \ldots, I_\ell)\big)$ to the GM.
4. The GM checks that $\mathrm{Verify}_{\mathsf{upk}[i]}\big((X||(I_1, \ldots, I_\ell)), sig_i\big) = 1$. If not, the GM aborts. Otherwise, it returns the structure-preserving signature σ_v to the user $\mathcal{U}_i$ and stores $\mathsf{transcript}_i = (X, \mathcal{ID}(v), C_v, \sigma_v, sig_i)$ in the database St_{trans}.

5. The user $\mathcal{U}_i$ defines his membership certificate cert_i as

$$\mathsf{cert}_i = \big(\mathcal{ID}(v), X, C_v, \sigma_v\big) \in \{N, \ldots, 2N-1\} \times \mathbb{G}^9,$$

where X will serve as the tag identifying $\mathcal{U}_i$. The membership secret sec_i is defined as $\mathsf{sec}_i = x \in \mathbb{Z}_p$.

Revoke$(\mathcal{Y}, \mathcal{S}_{\mathsf{GM}}, t, \mathcal{R}_t)$**:** Parse $\mathcal{S}_{\mathsf{GM}}$ as $\S_{\mathsf{GM}} := \big(sk^{(0)}_{\mathsf{AHO}}, sk^{(1)}_{\mathsf{AHO}}\big)$ and do the following.

1. Using the covering algorithm of the SD method, find a cover of the unrevoked user set $\{1, \ldots, N\} \backslash \mathcal{R}_t$ as the union of disjoint subsets of the form $S_{k_1,u_1}, \ldots, S_{k_m,u_m}$, with $m \leq 2 \cdot |\mathcal{R}_t| - 1$.
2. For $i = 1$ to m, do the following.
   (a) Consider S_{k_i,u_i} as the difference between sub-trees rooted at an internal node x_{k_i} and one of its descendants x_{u_i}. Lets $\phi_i, \psi_i \in \{1, \ldots, \ell\}$ be the depths of x_{k_i} and x_{u_i}, respectively, in T assuming that the root ϵ is at depth 1. Encode S_{k_i,u_i} as a vector $\big(g_{\phi_i}, g_1^{\mathcal{ID}(x_{k_i})}, g_{\psi_i}, g^{\mathcal{ID}(x_{u_i})}\big)$.
   (b) In order to authenticate S_{k_i,u_i} and bind it to the revocation period t, use $sk^{(1)}_{\mathsf{AHO}}$ to generate a structure-preserving signature $\Theta_i = (\Theta_{i,1}, \ldots, \Theta_{i,7}) \in \mathbb{G}^7$ on the message $R_i = \Big(g^t, g_{\phi_i}, g_1^{\mathcal{ID}(x_{k_i})}, g_{\psi_i}, g^{\mathcal{ID}(x_{u_i})}\Big) \in \mathbb{G}^5$, where the period number t is interpreted as an element of $\mathbb{Z}_p$.

Returns the revocation data

$$RL_t = \Big(t,\ \mathcal{R}_t,\ \big\{\phi_i,\ \psi_i,\ \mathcal{ID}(x_{k_i}),\ \mathcal{ID}(x_{u_i}),\ \Theta_i = (\Theta_{i,1}, \ldots, \Theta_{i,7})\big\}_{i=1}^{m}\Big). \tag{2.9}$$

Sign$(\mathcal{Y}, t, RL_t, \mathsf{cert}_i, \mathsf{sec}_i, M)$**:** returns $\perp$ if $i \in \mathcal{R}_t$. Otherwise, to sign $M \in \{0,1\}^*$, generates a one-time signature key pair $(\mathsf{sk}, \mathsf{VK}) \leftarrow \mathcal{G}(\lambda)$. Parse the membership certificate cert_i as $\mathsf{cert}_i = \big(\mathcal{ID}(v_i), X, C_{v_i}, \sigma_{v_i}\big) \in \{N, \ldots, 2N-1\} \times \mathbb{G}^9$ and sec_i as $x \in \mathbb{Z}_p$. Let $\epsilon = x_1, \ldots, x_\ell = v_i$ denote the path connecting v_i to the root ϵ of T and let $(I_1, \ldots, I_\ell) = (\mathcal{ID}(x_1), \ldots, \mathcal{ID}(x_\ell))$ be the vector of node identifiers. First, $\mathcal{U}_i$ generates a commitment $com_{C_{v_i}}$ to the encoding C_{v_i} of the path $(I_1, \ldots, I_\ell)$ from v_i to the root. Then, he does the following.

1. Using RL_t, find the set S_{k_l,u_l}, with $l \in \{1, \ldots, m\}$, that contains the leaf v_i identified by $\mathcal{ID}(v_i)$. Let x_{k_l} and x_{u_l} denote the primary and secondary roots of S_{k_l,u_l} at depths ϕ_l and ψ_l, respectively. Since x_{k_l} is an ancestor of v_i but x_{u_l} is not, it must be the case that $I_{\phi_l} = \mathcal{ID}(x_{k_l})$ and $I_{\psi_l} \neq \mathcal{ID}(x_{u_l})$.
2. In order to prove that v_i belongs to S_{k_l,u_l} without leaking l, re-randomize the l-th AHO signature Θ_l contained in RL_t as $\{\Theta'_{l,i}\}_{i=1}^{7} \leftarrow \mathsf{ReRand}(pk^{(1)}_{\mathsf{AHO}}, \Theta_l)$. Then, commit to the l-th revocation message

$$R_l = (R_{l,1}, \ldots, R_{l,5}) = \big(g^t, g_{\phi_l}, g_1^{\mathcal{ID}(x_{k_l})}, g_{\psi_l}, g^{\mathcal{ID}(x_{u_l})}\big) \tag{2.10}$$

and its signature $\Theta'_l = (\Theta'_{l,1}, \ldots, \Theta'_{l,7})$ by computing Groth-Sahai commitments $\{com_{R_{l,\tau}}\}_{\tau=2}^{5}$ and $\{com_{\Theta'_{l,j}}\}_{j\in\{1,2,5\}}$ to $\{R_{l,\tau}\}_{\tau=2}^{5}$ and $\{\Theta'_{l,j}\}_{j\in\{1,2,5\}}$ respectively.

(a) To prove that $I_{\phi_l} = \mathcal{ID}(x_{k_l})$, compute $W_{\phi_l} = \prod_{\kappa=1,\ \kappa\neq\phi_l}^{\ell} g_{\ell+1-\kappa+\phi_l}^{I_\kappa}$ that satisfies the equality $e(g_{\phi_l}, C_{v_i}) = e(g_1, g_\ell)^{I_{\phi_l}} \cdot e(g, W_{\phi_l})$. Then, generate a Groth-Sahai commitment $com_{W_{\phi_l}}$ to W_{ϕ_l}. Compute a NIWI proof that committed variables $(R_{l,2}, R_{l,3}, C_{v_i}, W_{\phi_l})$ satisfy

$$e(R_{l,2}, C_{v_i}) \quad = \quad e(R_{l,3}, g_\ell) \cdot e(g, W_{\phi_l}). \tag{2.11}$$

We denote by $\pi_{eq} \in \mathbb{G}^9$ the proof for the quadratic equation (2.11).

(b) To prove that $I_{\psi_l} \neq \mathcal{ID}(x_{u_l})$, compute $W_{\psi_l} = \prod_{\kappa=1,\ \kappa\neq\psi_l}^{\ell} g_{\ell+1-\kappa+\psi_l}^{I_\kappa}$ that satisfies $e(g_{\psi_l}, C_{v_i}) = e(g_1, g_\ell)^{I_{\psi_l}} \cdot e(g, W_{\psi_l})$. Then, compute a Groth-Sahai commitment $com_{W_{\psi_l}}$ to W_{ψ_l} as well as commitments com_{Γ_l} and $\{com_{\Psi_{l,\tau}}\}_{\tau\in\{0,1,2\ell\}}$ to the group elements

$$(\Gamma_l, \Psi_{l,0}, \Psi_{l,1}, \Psi_{l,2\ell}) = \big(g^{1/(I_{\psi_l} - \mathcal{ID}(x_{u_l}))}, g^{I_{\psi_l}}, g_1^{I_{\psi_l}}, g_{2\ell}^{I_{\psi_l}}\big).$$

The next step is to generate a NIWI proof that the committed group elements $(R_{l,4}, R_{l,5}, C_{v_i}, \Gamma_l, \Psi_{l,0}, \Psi_{l,1}, \Psi_{l,2\ell})$ satisfy

$$e(R_{l,4}, C_{v_i}) = e(\Psi_{l,1}, g_\ell) \cdot e(g, W_{\psi_l}), \tag{2.12}$$
$$e(\Psi_{l,0}/R_{l,5}, \Gamma_l) = e(g, g), \tag{2.13}$$
$$e(\Psi_{l,1}, g) = e(g_1, \Psi_{l,0}), \tag{2.14}$$
$$e(\Psi_{l,2\ell}, g) = e(g_{2\ell}, \Psi_{l,0}). \tag{2.15}$$

We denote this NIWI proof by $\pi_{neq} = (\pi_{neq,1}, \pi_{neq,2}, \pi_{neq,3}, \pi_{neq,4})$. Since the first two equations (2.12) and (2.13) are quadratic, $\pi_{neq,1}$ and $\pi_{neq,2}$ consist of 9 elements each. The last two equations (2.14) and (2.15) are linear and both cost 3 elements to prove.

3. Provide evidence that the tuple R_l of (2.10) is a certified revocation message for period t: namely, compute a NIWI proof π_{R_l} that committed message elements $\{R_{l,\tau}\}_{\tau=2}^{5}$ and signature components $\{\Theta'_{l,j}\}_{j\in\{1,2,5\}}$ satisfy the equations

$$\begin{aligned} A^{(1)} \cdot e(\Theta'_{l,3},\Theta'_{l,4})^{-1} \cdot e(G_1^{(1)}, g^t)^{-1} &= e(G_z^{(1)}, \Theta'_{l,1}) \cdot e(G_r^{(1)}, \Theta'_{l,2}) \cdot \prod_{\tau=2}^{5} e(G_\tau^{(1)}, R_{l,\tau}), \\ B^{(1)} \cdot e(\Theta'_{l,6},\Theta'_{l,7})^{-1} \cdot e(H_1^{(1)}, g^t)^{-1} &= e(H_z^{(1)}, \Theta'_{l,1}) \cdot e(H_r^{(1)}, \Theta'_{l,5}) \cdot \prod_{\tau=2}^{5} e(H_\tau^{(1)}, R_{l,\tau}). \end{aligned} \tag{2.16}$$

Since $\{\Theta'_{l,j}\}_{j\in\{3,4,6,7\}}$ are constants, equations (2.16) are both linear and thus require 3 elements each. Hence, π_{R_l} takes 6 elements altogether.

4. Let $\sigma_{v_i} = (\theta_{v_i,1}, \ldots, \theta_{v_i,7})$ be the AHO signature on (X, C_{v_i}). Re-randomize σ_{v_i} as $\{\theta'_{v_i,j}\}_{j=1}^{7} \leftarrow \mathsf{ReRand}(pk_{\mathsf{AHO}}^{(0)}, \sigma_{v_i})$ and generate commitments $\{com_{\theta'_{v_i,j}}\}_{j\in\{1,2,5\}}$ to $\{\theta'_{v_i,j}\}_{j\in\{1,2,5\}}$ as well as a commitment com_X to X. Then, generate a NIWI proof $\pi_{\sigma_{v_i}}$ that committed variables satisfy the verification equations

$$\begin{aligned} A^{(0)} \cdot e(\theta'_{l,3}, \theta'_{l,4})^{-1} &= e(G_z^{(0)}, \theta'_{l,1}) \cdot e(G_r^{(0)}, \theta'_{l,2}) \cdot e(G_1^{(0)}, X) \cdot e(G_2^{(0)}, C_{v_i}), \\ B^{(0)} \cdot e(\theta'_{l,6}, \theta'_{l,7})^{-1} &= e(H_z^{(0)}, \theta_{l,1}) \cdot e(H_r^{(0)}, \theta'_{l,5}) \cdot e(H_1^{(0)}, X) \cdot e(H_2^{(0)}, C_{v_i}). \end{aligned}$$

Since these equations are linear, $\pi_{\sigma_{v_i}}$ requires 6 group elements.

5. Using VK as a tag, compute a tag-based encryption [160] of X by drawing random exponents $z_1, z_2 \leftarrow \mathbb{Z}_p$ at random and setting

$$(\mathrm{Y}_1, \mathrm{Y}_2, \mathrm{Y}_3, \mathrm{Y}_4, \mathrm{Y}_5) = \big(f_1^{z_1}, f_2^{z_2}, X \cdot g^{z_1+z_2}, (g^{\mathsf{VK}} \cdot U)^{z_1}, (g^{\mathsf{VK}} \cdot V)^{z_2}\big).$$

6. Generate a NIZK proof that $com_X = (1, 1, X) \cdot \mathbf{f_1}^{w_{X,1}} \cdot \mathbf{f_2}^{w_{X,2}} \cdot \mathbf{f_3}^{w_{X,3}}$ and $(\mathrm{Y}_1, \mathrm{Y}_2, \mathrm{Y}_3)$ are BBS encryptions of the same value X. If we write $\mathbf{f_3} = (f_{3,1}, f_{3,2}, f_{3,3})$, the commitment com_X can be written as $(f_1^{w_{X,1}} \cdot f_{3,1}^{w_{X,3}}, f_2^{w_{X,2}} \cdot f_{3,2}^{w_{X,3}}, X \cdot g^{w_{X,1}+w_{X,2}} \cdot f_{3,3}^{w_{X,3}})$, so that we have

$$com_X \cdot (\mathrm{Y}_1, \mathrm{Y}_2, \mathrm{Y}_3)^{-1} = \big(f_1^{\chi_1} \cdot f_{3,1}^{\chi_3},\ f_2^{\chi_2} \cdot f_{3,2}^{\chi_3},\ g^{\chi_1+\chi_2} \cdot f_{3,3}^{\chi_3}\big) \tag{2.17}$$

with $\chi_1 = w_{X,1} - z_1$, $\chi_2 = w_{X,2} - z_2$, $\chi_3 = w_{X,3}$. Compute commitments to $\{\chi_j\}_{j=1}^3$ as $com_{\chi_j} = \boldsymbol{\varphi}^{\chi_j} \cdot \mathbf{f_1}^{w_{\chi_j,1}} \cdot \mathbf{f_2}^{w_{\chi_j,2}}$, with $w_{\chi_j,1}, w_{\chi_j,2} \xleftarrow{\$} \mathbb{Z}_p$ for $j \in \{1, 2, 3\}$ and generate proofs $\{\pi_{eq\text{-}com,j}\}_{j=1}^3$ that χ_1, χ_2, χ_3 satisfy the three linear relations (2.17). These latter proofs $\{\pi_{eq\text{-}com,j}\}_{j=1}^3$ cost 2 elements each.

7. Compute a Boneh-Boyen signature $\sigma_{\mathsf{VK}} = g^{1/(x+\mathsf{VK})}$ on VK and a commitment $com_{\sigma_{\mathsf{VK}}}$ to σ_{VK}. Then, generate a NIWI proof $\pi_{\sigma_{\mathsf{VK}}} = (\boldsymbol{\pi}_{\sigma_{\mathsf{VK}},1}, \boldsymbol{\pi}_{\sigma_{\mathsf{VK}},2}, \boldsymbol{\pi}_{\sigma_{\mathsf{VK}},3}) \in \mathbb{G}^9$ that the committed variables $(\sigma_{\mathsf{VK}}, X) \in \mathbb{G}^2$ satisfy $e(\sigma_{\mathsf{VK}}, X \cdot g^{\mathsf{VK}}) = e(g, g)$.
8. Compute a one-time signature $\sigma_{ots} = \mathcal{S}(\mathsf{sk}, (M, RL_t, \mathrm{Y}_1, \mathrm{Y}_2, \mathrm{Y}_3, \mathrm{Y}_4, \mathrm{Y}_5, \Omega, \mathbf{com}, \mathbf{\Pi}))$ where $\Omega = \{\Theta'_{l,i}, \theta'_{l,i}\}_{i\in\{3,4,6,7\}}$ and

$$\begin{aligned}\mathbf{com} &= \big(com_{C_{v_i}}, com_X, \{com_{R_{l,\tau}}\}_{\tau=2}^5, com_{W_{\phi_l}}, com_{W_{\psi_l}}, com_{\Gamma_l}, \{com_{\Psi_{l,\tau}}\}_{\tau\in\{0,1,2\ell\}},\\ &\qquad \{com_{\Theta'_{l,j}}\}_{j\in\{1,2,5\}}, \{com_{\theta'_{l,j}}\}_{j\in\{1,2,5\}}, \{com_{\chi_j}\}_{j=1}^3, com_{\sigma_{\mathsf{VK}}}\big),\\ \mathbf{\Pi} &= \big(\pi_{eq}, \pi_{neq}, \pi_{R_l}, \pi_{\sigma_{v_i}}, \{\pi_{eq\text{-}com,j}\}_{j=1}^3, \pi_{\sigma_{\mathsf{VK}}}\big).\end{aligned}$$

Return the signature

$$\sigma = \big(\mathsf{VK}, \mathrm{Y}_1, \mathrm{Y}_2, \mathrm{Y}_3, \mathrm{Y}_4, \mathrm{Y}_5, \Omega, \mathbf{com}, \mathbf{\Pi}, \sigma_{ots}\big). \tag{2.18}$$

Verify$(\sigma, M, t, RL_t, \mathcal{Y})$**:** parse σ as in (2.18). If $(\mathrm{Y}_1, \mathrm{Y}_2, \mathrm{Y}_3, \mathrm{Y}_4, \mathrm{Y}_5)$ is not a well-formed tag-based encryption (that is, if $e(\mathrm{Y}_1, g^{\mathsf{VK}} \cdot U) \neq e(f_1, \mathrm{Y}_4)$ or $e(\mathrm{Y}_2, g^{\mathsf{VK}} \cdot V) \neq e(f_2, \mathrm{Y}_5)$) or if $\mathcal{V}(\mathsf{VK}, (M, RL_t, \mathrm{Y}_1, \mathrm{Y}_2, \mathrm{Y}_3, \mathrm{Y}_4, \mathrm{Y}_5, \Omega, \mathbf{com}, \mathbf{\Pi}), \sigma_{ots}) = 0$, return 0. Then, return 1 if all proofs properly verify. Otherwise, return 0.

Open$(M, t, RL_t, \sigma, \mathcal{S}_{\mathsf{OA}}, \mathcal{Y}, St)$**:** parse σ as above and return $\perp$ if $\mathsf{Verify}(\sigma, M, t, RL_t, \mathcal{Y}) = 0$. Otherwise, given $\mathcal{S}_{\mathsf{OA}} = (\beta_1, \beta_2)$, compute $\tilde{X} = \mathrm{Y}_3 \cdot \mathrm{Y}_1^{-1/\beta_1} \cdot \mathrm{Y}_2^{-1/\beta_2}$. In the database St_{trans}, find a record $\langle i, \mathsf{transcript}_i = (X_i, \mathcal{ID}(v_i), C_{v_i}, \sigma_{v_i}, sig_i)\rangle$ such that $X_i = \tilde{X}$. If no such record exists in St_{trans}, returns $\perp$. Otherwise, return i.

At first glance, the variable $\Psi_{l,2\ell}$ and the proof of the second equality (2.14) may seem unnecessary in step 2.b of the signing algorithm. However, this element plays a crucial role when it comes to proving the security under the ℓ-FlexDHE assumption. Indeed, the proof of security against misidentification attacks ceases to go through if we remove $\Psi_{l,2\ell}$ and its corresponding proof.

Efficiency

As far as efficiency goes, each entry of RL_t contains 7 group elements and two node identifiers of $O(\log N)$ bits each. If $\lambda_{\mathbb{G}}$ is the bitlength of a group element, we have $\log N \ll \lambda_{\mathbb{G}}/2$ (since $\lambda \leq \lambda_{\mathbb{G}}$ and N is polynomial), so that the number of bits of RL_t is bounded by $2 \cdot |\mathcal{R}_t| \cdot (7 \cdot \lambda_{\mathbb{G}} + 2\log N + 2\log\log N) < 2 \cdot |\mathcal{R}_t| \cdot (9\lambda_{\mathbb{G}})$ bits. The size of RL_t is thus bounded by that of $18 \cdot |\mathcal{R}_t|$ group elements.

Unlike our first scalable construction [180], group members only need to store 9 group elements in their membership certificate. As far as the size of signature goes, **com** and $\mathbf{\Pi}$ require 66 and 60 group elements, respectively. If the one-time signature of [133] is used, VK and σ_{ots} consist of 3 elements of $\mathbb{G}$ and 2 elements of $\mathbb{Z}_p$, respectively. The global size σ amounts to that of 144 group elements, which is about 50% longer than [180]. In comparison with [134] (which does not natively support revocation), signatures are only longer by a factor of 3. At the 128-bit security level, each group element should have a 512-bit representation and a signature takes 9 kB.

Verifying signatures takes time $O(1)$. The signer has to compute $2\ell = O(\log N)$ exponentiations to obtain W_{ϕ_l} and W_{ψ_l} at the beginning of each period. Note that these exponentiations involve short exponents of $O(\log N)$ bits each. Hence, computing W_{ϕ_l} and W_{ψ_l} requires $O(\log^2 N)$ multiplications in $\mathbb{G}$. For this reason, since $\log^2 N \ll \lambda$ (as long as $N \ll 2^{\lambda^{1/2}}$), this cost is dominated by that of a single exponentiation in $\mathbb{G}$.

Security

The security of the scheme relies on the same assumptions as in our first revocable group signature [180] (namely, the q-SFP, q-SDH and DLIN assumptions) and the ℓ-FlexDHE assumption. While we need an addition non-standard assumption, we only need the ℓ-FlexDHE assumption to hold for small values of the parameter $\ell = \log N$, where N is the maximal number of users.

In the article [179, Appendix C], we suggest a variant of the scheme where the ℓ-FlexDHE assumption is replaced by an assumption of constant size, introduced by Laguillaumie *et al.* [167], at the expense of increasing the group public key size from $O(\log N)$ to $O(\log^2 N)$. This is achieved by replacing the concise vector commitment of Libert and Yung [188] by the one of Catalano and Fiore [75], which relies on the CDH assumption instead of the ℓ-DHE assumption but has a longer commitment key. By applying the results of Abe *et al.* [2] to our modified scheme [179, Appendix C], it is further possible to construct a revocable group signature with $O(\log^2 N)$-size group public keys which only relies on simple assumptions in the standard model.

In a follow-up work, Attrapadung *et al.* [20] used a different mechanism from the broadcast encryption literature – due to Attrapadung, Libert and de Panafieu [24, 21] – to achieve an efficiency tradeoff which is exactly dual to ours. While we obtain membership certificates and revocation lists made of $O(1)$ and $O(r)$ group elements, respectively, Attrapadung *et al.* [20] perform the other way around with $O(1)$-size revocation lists and $O(R)$-size membership certificates, where R is an upper bound on the number of revoked users. However, the maximal number R of revoked users must be fixed in advance even if it is much smaller than the total number of users N. Similar results were obtained by Nakanishi and Funabiki [204].

2.3 Conclusion

This chapter presented two important applications of structure-preserving cryptographic primitives in the design of anonymity-related cryptographic mechanisms. One of our contributions was the first reasonably efficient construction [81] – which was proposed at the same time as (and independently of) Fuchsbauer's automorphic signatures [112] – of the primitive, initially introduced by Groth [133], that was subsequently named "structure-preserving signature" by Abe *et al.* [6, 4]. This construction allowed us to obtain the first fully non-interactive group encryption system in the standard model and also immediately implied the first group signatures with concurrent join in the standard model [157]. Together with other techniques (such as the NNL framework [205] and our construction of concise vector commitments [188]), the optimized SPS scheme of Abe *et al.* [6] also enabled the design of a new revocation mechanism for group signature schemes in the standard model.

Structure-preserving signatures were also used in other results of mine [176, 173] on privacy-preserving primitives which are not discussed in this manuscript. In collaboration with Marc Joye, Moti Yung and Thomas Peters, we built on the Abe *et al.* [6] system to construct a group encryption scheme [176] with refined tracing capabilities similar to those of traceable signatures [155]: specifically, the opening authority can disclose a user-specific trapdoor that makes it possible to trace all ciphertexts encrypted for a given suspicious user without affecting the privacy of well-behaved users. Together with Marc Joye, we also designed a partially structure-preserving identity-based encryption (IBE) scheme [173] – where "partially" means that identities are still encoded as bitstrings (rather than group elements) but encrypted messages live in the source group $\mathbb{G}$ of the bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ instead of the target group $\mathbb{G}_T$ as in most IBE schemes in the standard model [248] – and used it to construct the first efficient standard model realization of group signatures with message-dependent opening (GS-MDO) [233]. In short GS-MDO schemes, as introduced by Sakai *et al.* [233], are group signatures where the opening authority can only open signatures for which a separate authority has released a message specific trapdoor. Sakai *et al.* [233] showed that GS-MDO implies identity-based encryption, which raised the intuition that realizing GS-MDO schemes in the standard model requires a structure-preserving IBE. In [173], we showed that a partially structure-preserving IBE suffices for this purpose and we built a GS-MDO scheme with logarithmic signature size in the standard model.

CHAPTER 3

Constructions of Non-Malleable Primitives from Structure-Preserving Cryptography

In the last three years, a large body of work has analyzed the feasibility and the efficiency of structure-preserving signatures (SPS) [133, 81, 112, 6, 4, 5, 63, 82, 142, 2, 3], public-key encryption [65] and commitments schemes [135, 7].

In this chapter, we consider applications of structure-preserving signatures in the design of non-malleable protocols such as non-interactive non-malleable commitments or chosen-ciphertext-secure public-key encryption. Paradoxically, this is achieved by first considering structure-preserving signatures which are intentionally made malleable. We consider SPS schemes with linearly homomorphic properties and argue that such primitives have many applications, even independently of Groth-Sahai proofs.

3.0.1 Linearly Homomorphic Structure-Preserving Signatures

The concept of homomorphic signatures can be traced back to Desmedt [97] while proper definitions remained lacking until the work of Johnson *et al.* [148]. Since then, constructions have appeared for various kinds of homomorphisms (see [11] and references therein).

Linearly Homomorphic Schemes. Linearly homomorphic signatures are an important class of homomorphic signatures for arithmetic functions, whose study was initiated by Boneh, Freeman, Katz and Waters [48]. While initially motivated by applications to network coding [48], they are also useful in proofs of storage [13, 16] or in verifiable computation mechanisms, when it comes to authenticate servers' computations on outsourced data (see, *e.g.*, [11]). The recent years, much attention was given to the notion and a variety of constructions [120, 23, 47, 46, 77, 78, 111, 25, 26] based on various assumptions have been studied.

Structure-Preserving Signatures Made Homomorphic. In collaboration with Thomas Peters, Marc Joye and Moti Yung [177], we put forth the notion of linearly homomorphic structure-preserving signatures (LHSPS). While structure-preserving signatures and linearly homomorphic signatures have both been studied before, simultaneously combining the homomorphic and structure-preserving properties turns out to be useful and non-trivial. As we will see in this chapter, such a combination has unexpected applications that are not known to be possible with only one of these two properties individually. In particular, we describe

applications of LHSPS schemes *beyond* their compatibility with the Groth-Sahai techniques. These signature schemes function exactly like ordinary homomorphic signatures with the additional restriction that signatures and messages only consist of (vectors of) group elements whose discrete logarithms may not be available. We describe three constructions and prove their security under well-established assumptions in bilinear groups.

Our first scheme's starting point is the one-time (regular) SPS scheme of Abe *et al.* [6]. By removing certain public key components, we obtain the desired linear homomorphism, and prove the security using information-theoretic arguments as in [6]. The key observation here is that, as long as the adversary does not output a signature on a linear combination of previously signed vectors, it will be unable to sign its target vector in the same way as the reduction would, because certain private key components will remain perfectly hidden.

Our initial scheme inherits the one-time restriction of the scheme in [6] in that only one linear subspace can be safely signed with a given public key. Nevertheless, we can extend it to build a full linearly homomorphic SPS system. To this end, we suitably combine our first scheme with Waters signatures [248]. Here, Waters signatures are used as a resting ground for fresh random exponents which are introduced in each signed vector and help us refresh the state of the system and apply each time the same argument as in the one-time scheme. We also present techniques to turn the scheme into a fully randomizable one, where a derived signature has the same distribution as a directly signed message.

3.0.2 Applications

Verifiable computation on encrypted data. First, we show that the primitive enables verifiable computation mechanisms on encrypted data.[1] Specifically, it allows a client to store encrypted files on an untrusted remote server. While the dataset is encrypted using an additively homomorphic encryption scheme, the server is able to blindly compute linear functions on the original data and provide the client with a short homomorphically derived signature vouching for the correctness of the computation. This is achieved by having the client sign each ciphertext using a homomorphic SPS scheme and handing the resulting signatures to the server at the beginning. After this initial phase, the client only needs to store a short piece of information, no matter how large the file is. Still, he remains able to authenticate linear functions on his data and the whole process is completely non-interactive.

Non-malleable commitments to group elements. As a more surprising application, we show that LHSPS schemes generically yield non-malleable [102] trapdoor commitments to group elements. We actually construct a simulation-sound trapdoor commitment [116] — a primitive known (by [116, 195]) to imply re-usable non-malleable commitments with respect to opening [94] — from any linearly homomorphic SPS satisfying a relatively mild condition. To our knowledge, we thus obtain the first constant-size trapdoor commitments to group elements providing re-usable non-malleability with respect to opening. Previous non-interactive commitments to group elements were either malleable [138, 135] or inherently length-increasing [108]: if we disregard the trivial solution consisting of hashing the message first (which is not an option when we want to allow for efficient proofs of knowl-

[1] Our goals are very different from those of [119], where verifiable computation on homomorphically encrypted data is also considered. We do not seek to outsource computation but rather save the client from storing large datasets.

edge of an opening), no general technique has been known, to date, for committing to many group elements at once using a short commitment string.

In the structure-preserving case, our transformation is purely generic as it applies to a template which any linearly homomorphic SPS necessarily satisfies in symmetric bilinear groups. We also generalize the construction so as to build simulation-sound trapdoor commitments to vectors from any pairing-based (non-structure-preserving) linearly homomorphic signature. In this case, the conversion is only semi-generic as it imposes conditions which are only met by pairing-based systems for the time being: essentially, we need the underlying signature scheme to operate over groups of finite, public order. While only partially generic, this construction of non-malleable commitments from linearly homomorphic signatures is somewhat unexpected considering that the terms "non-malleability" and "homomorphism" are antagonistic, and thus may be considered incompatible.

Constant-Size Quasi-Adaptive NIZK Proofs for Linear Subspaces. Our LHSPS schemes also allowed us [178] to construct constant-size QA-NIZK arguments of linear subspace membership. Given a $t \times n$ matrix of group elements of rank $t < n$, the QA-NIZK proofs of Jutla and Roy [151] save $\Omega(t)$ group elements compared to Groth-Sahai. In [178], we gave QA-NIZK arguments for proving the same statement using a *constant* number group elements, regardless of the number of equations or the number of variables. Our one-time LHSPS system immediately gives QA-NIZK arguments of linear subspace membership comprised of only 3 group elements under the DLIN assumption (and 2 group elements under the SXDH assumption). While our constant-size QA-NIZK arguments are malleable in their simplest version, they readily extend – at minimal cost – to provide a form of one-time simulation-soundness defined by Jutla and Roy [150]. Moreover, we describe a construction of *unbounded* simulation-sound QA-NIZK argument based on our randomizable LHSPS system. Unlike previous unbounded simulation-sound Groth-Sahai-based proofs, our construction does not involve quadratic pairing product equations and does not rely on a chosen-ciphertext-secure encryption scheme.

Our constant-size QA-NIZK argument systems allowed us [178] to design new and improved CCA2-secure encryption schemes. In particular, we could significantly optimize the adaptively secure non-interactive threshold versions of the Cramer-Shoup cryptosystem given by Libert and Yung [191]. We also built an efficient CCA2-secure keyed-homomorphic encryption scheme. Keyed-homomorphic encryption is a primitive, suggested by Emura *et al.*[104], which allows reconciling homomorphism and IND-CCA2 security. The idea of Emura *et al.*[104] is that homomorphic operations can only be carried out using a dedicated evaluation key. A keyed homomorphic scheme should be designed so as to be chosen-ciphertext-secure against any adversary that is withheld access to the evaluation key. At the same time, the evaluation key does not enable decryption and IND-CCA1 security should be preserved even if this evaluation key is made available to the adversary. The keyed homomorphic constructions of Emura *et al.*[104] are only known to satisfy a relaxed definition of security where the adversary is only given access to a restricted homomorphic evaluation oracle. Using our unbounded simulation-sound QA-NIZK proofs, we were able [178] to build a keyed homomorphic encryption scheme satisfying the strongest definition of chosen-ciphertext security given in [104]. At the same time, our construction enables threshold decryption, as shown in [178], which is a useful capability in many applications of homomorphic encryption. Our results were recently improved by Jutla and Roy [153, 152]

who gave even shorter QA-NIZK proofs [153] of linear subspace membership and improved unbounded simulation-sound constructions [152].

3.1 Linearly Homomorphic Structure-Preserving Signatures

3.1.1 Definitions for Linearly Homomorphic Signatures

Let $(\mathbb{G}, \mathbb{G}_T)$ be a configuration of (multiplicatively written) groups of prime order p over which a bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is efficiently computable.

We consider linearly homomorphic signatures for which the message space $\mathcal{M}$ consists of pairs $\mathcal{M} := \mathcal{T} \times \mathbb{G}^n$, for some $n \in \mathbb{N}$, where $\mathcal{T}$ is a tag space. We remark that, in the applications considered in this paper, tags do not need to be group elements. We thus allow them to be arbitrary strings.

Definition 5. *A linearly homomorphic structure-preserving signature (LHSPS) over $(\mathbb{G}, \mathbb{G}_T)$ is a tuple of efficient algorithms $\Sigma = (\mathsf{Keygen}, \mathsf{Sign}, \mathsf{SignDerive}, \mathsf{Verify})$ for which the message space is $\mathcal{M} := \mathcal{T} \times \mathbb{G}^n$, for some $n \in \mathsf{poly}(\lambda)$ and some set $\mathcal{T}$, and such that:*

$\mathsf{Keygen}(\lambda, n)$: *is a randomized algorithm that takes in a security parameter $\lambda \in \mathbb{N}$ and an integer $n \in \mathsf{poly}(\lambda)$ denoting the dimension of vectors to be signed. It outputs a key pair (pk, sk) and the description of a tag (i.e., a file identifier) space $\mathcal{T}$.*

$\mathsf{Sign}(\mathsf{sk}, \tau, \mathbf{M})$: *is a possibly probabilistic algorithm that takes in a private key sk, a file identifier $\tau \in \mathcal{T}$ and a vector $\mathbf{M} \in \mathbb{G}^n$. It outputs a signature $\sigma \in \mathbb{G}^{n_s}$, for some $n_s \in \mathsf{poly}(\lambda)$ determined by pk.*

$\mathsf{SignDerive}(\mathsf{pk}, \tau, \{(\omega_i, \sigma^{(i)})\}_{i=1}^{\ell})$: *is a (possibly probabilistic) signature derivation algorithm. It takes as input a public key pk, a file identifier τ as well as ℓ pairs $(\omega_i, \sigma^{(i)})$, each of which consists of a weight $\omega_i \in \mathbb{Z}_p$ and a signature $\sigma^{(i)} \in \mathbb{G}^{n_s}$. The output is a signature $\sigma \in \mathbb{G}^{n_s}$ on the vector $\mathbf{M} = \prod_{i=1}^{\ell} \mathbf{M}_i^{\omega_i}$, where $\sigma^{(i)}$ is a signature on $\mathbf{M}_i$.*

$\mathsf{Verify}(\mathsf{pk}, \tau, \mathbf{M}, \sigma)$: *is a deterministic algorithm that takes in a public key pk, a file identifier $\tau \in \mathcal{T}$, a signature σ and a vector $\mathbf{M}$. It outputs 1 if σ is deemed valid and 0 otherwise.*

Correctness is expressed by imposing that, for all security parameters $\lambda \in \mathbb{N}$, all integers $n \in \mathsf{poly}(\lambda)$ and all triples $(\mathsf{pk}, \mathsf{sk}, \mathcal{T}) \leftarrow \mathsf{Keygen}(\lambda, n)$, the following holds:

1. For all identifiers $\tau \in \mathcal{T}$ and all n-vectors $\mathbf{M} \in \mathbb{G}^n$, if $\sigma = \mathsf{Sign}(\mathsf{sk}, \tau, \mathbf{M})$, then we have $\mathsf{Verify}(\mathsf{pk}, \tau, \mathbf{M}, \sigma) = 1$.

2. For all identifiers $\tau \in \mathcal{T}$, any $\ell > 0$ and any set of triples $\{(\omega_i, \sigma^{(i)}, \mathbf{M}_i)\}_{i=1}^{\ell}$, if we have $\mathsf{Verify}(\mathsf{pk}, \tau, \mathbf{M}_i, \sigma^{(i)}) = 1$ for each $i \in \{1, \ldots, \ell\}$, then

$$\mathsf{Verify}\big(\mathsf{pk}, \tau, \prod_{i=1}^{\ell} \mathbf{M}_i^{\omega_i}, \mathsf{SignDerive}(\mathsf{pk}, \tau, \{(\omega_i, \sigma^{(i)})\}_{i=1}^{\ell})\big) = 1.$$

In our constructions, n_s will be a constant which does not depend on the dimension n of signed vectors. This will play a crucial role in certain application like short quasi-adaptive NIZK proofs of linear subspace membership.

Security. At first, the very name of the primitive may sound almost self-contradictory when it comes to formally define its security. Indeed, the security of a linearly homomorphic scheme [48] notably requires that it be infeasible to publicly compute a signature on a vector outside the linear span of originally signed vectors. The problem is that, when vector entries live in a discrete-logarithm hard group, deciding whether several vectors are independent or not is believed to be a hard problem. Yet, this will not prevent us from applying new techniques and constructing schemes with security proofs under simple assumptions. In the security proof of our first construction, the reduction will be able to detect when the adversary has won using the private key of the system.

In linearly homomorphic signatures, we use the same definition of unforgeability as in [25]. This definition implies security in the stronger model used by Freeman [111] since the adversary can interleave signing queries for individual vectors belonging to distinct subspaces. Moreover, file identifiers can be chosen by the adversary (which strengthens the definition of [48]) and are not assumed to be random. As a result, a file identifier can be a low-entropy, easy-to-remember string such as the name of the dataset's owner.

Definition 6. *A linearly homomorphic SPS scheme* $\Sigma = (\mathsf{Keygen}, \mathsf{Sign}, \mathsf{SignDerive}, \mathsf{Verify})$ *is secure if no PPT adversary has non-negligible advantage in the game below:*

1. *The adversary* $\mathcal{A}$ *chooses an integer* $n \in \mathbb{N}$ *and sends it to the challenger who runs* $\mathsf{Keygen}(\lambda, n)$ *and obtains* $(\mathsf{pk}, \mathsf{sk})$ *before sending* pk *to* $\mathcal{A}$.

2. *On polynomially-many occasions,* $\mathcal{A}$ *can interleave the following kinds of queries.*

   - *Signing queries:* $\mathcal{A}$ *chooses a tag* $\tau \in \mathcal{T}$ *and a vector* $\mathbf{M} \in \mathbb{G}^n$. *The challenger picks a handle* h *and computes* $\sigma \leftarrow \mathsf{Sign}(sk, \tau, \mathbf{M})$. *It stores* $(\mathsf{h}, (\tau, \mathbf{M}), \sigma)$ *in a table* T *and returns* h.
   - *Derivation queries:* $\mathcal{A}$ *chooses a vector of handles* $\mathsf{h} = (\mathsf{h}_1, \ldots, \mathsf{h}_k)$ *and a set of coefficients* $\{\omega_i\}_{i=1}^k$. *The challenger retrieves the tuples* $\{(\mathsf{h}_i, (\tau_i, \mathbf{M}_i), \sigma^{(i)})\}_{i=1}^k$ *from* T *and returns* $\perp$ *if one of these does not exist or if there exists* $i \in \{1, \ldots, k\}$ *such that* $\tau_i \neq \tau$. *Otherwise, it computes the linear combination* $\mathbf{M} = \prod_{i=1}^k \mathbf{M}_i^{\omega_i}$ *and runs* $\sigma' \leftarrow \mathsf{SignDerive}\big(\mathsf{pk}, \tau, \{(\omega_i, \sigma^{(i)})\}_{i=1}^k\big)$. *It also chooses a handle* h', *stores* $(\mathsf{h}', (\tau, \mathbf{M}), \sigma')$ *in* T *and returns* h' *to* $\mathcal{A}$.
   - *Reveal queries:* $\mathcal{A}$ *chooses a handle* h. *If no tuple of the form* $(\mathsf{h}, (\tau, \mathbf{M}), \sigma')$ *exists in* T, *the challenger returns* $\perp$. *Otherwise, it returns* σ' *to* $\mathcal{A}$ *and adds* $((\tau, \mathbf{M}), \sigma')$ *to the set* Q.

3. $\mathcal{A}$ *outputs an identifier* $\tau^\star$, *a signature* $\sigma^\star$ *and a vector* $\mathbf{M}^\star \in \mathbb{G}^n$. *The adversary* $\mathcal{A}$ *wins if* $\mathsf{Verify}(\mathsf{pk}, \tau^\star, \mathbf{M}^\star, \sigma^\star) = 1$ *and one of the conditions below is satisfied:*

   - *(Type I):* $\tau^\star \neq \tau_i$ *for any entry* $(\tau_i, .)$ *in* Q *and* $\mathbf{M}^\star \neq (1_\mathbb{G}, \ldots, 1_\mathbb{G})$.
   - *(Type II):* $\tau^\star = \tau_i$ *for* $k_i > 0$ *entries* $(\tau_i, .)$ *in* Q *and* $\mathbf{M}^\star \notin V_i$, *where* V_i *denotes the subspace spanned by all vectors* $\mathbf{M}_1, \ldots, \mathbf{M}_{k_i}$ *for which an entry of the form* $(\tau^\star, \mathbf{M}_j)$, *with* $j \in \{1, \ldots, k_i\}$, *appears in* Q.

$\mathcal{A}$'s advantage is its probability of success taken over all coin tosses.

In our first scheme, we will consider a weaker notion of *one-time* security. In this notion, the adversary is limited to obtain signatures for only *one* linear subspace. In this case, there

is no need for file identifiers and we assume that all vectors are assigned the identifier $\tau = \varepsilon$.

In the following, the adversary will be said *independent* if

- For any given tag τ, it is restricted to only query signatures on linearly independent vectors.
- Each vector is only queried at most once.

Non-independent adversaries are not subject to the above restrictions. It will be necessary to consider these adversaries in our construction of non-malleable commitments. Nevertheless, security against independent adversaries suffices for many applications —including encrypted cloud storage— since the signer can always append unit vectors to each newly signed vector.

At first, one may wonder how Definition 6 can be satisfied at all given that the challenger may not have an efficient way to check whether the adversary is successful. Indeed, in cryptographically useful discrete-logarithm-hard groups $\mathbb{G}$, deciding whether vectors $\{\mathbf{M}_i\}_i$ of $\mathbb{G}^n$ are linearly dependent is believed to be difficult when $n > 2$. However, it may be possible using some trapdoor information embedded in pk, especially if the adversary additionally outputs signatures on $\{\mathbf{M}_i\}_i$.

In some applications, it makes sense to consider a weaker attack model where a Type II adversary is only deemed successful if it outputs a convincing proof that its target vector $\mathbf{M}^\star$ is indeed independent of the vectors that were signed for the tag $\tau^\star$. The proof can be either a NIZK proof or, alternatively, a vector in the kernel of the matrix whose rows are the vectors that were signed for $\tau^\star$. We call such an adversary a *targeting* adversary.

3.2 Constructions of Linearly Homomorphic Structure-Preserving Signatures

As a warm-up, we begin by describing a one-time homomorphic signature, where a given public key allows signing only *one* linear subspace.

3.2.1 A One-Time Linearly Homomorphic Construction

The construction is based on a one-time structure-preserving signature described by Abe *et al.* [6, Appendix C.1] and the observation that this system can be made homomorphic by removing certain public key components.

In the description hereunder, since only one linear subspace can be signed for each public key, no file identifier τ is used. We thus set τ to be the empty string ε in all algorithms.

Keygen(λ, n): given a security parameter λ and the dimension $n \in \mathbb{N}$ of the subspace to be signed, choose bilinear group $(\mathbb{G}, \mathbb{G}_T)$ of prime order $p > 2^\lambda$. Then, choose generators $h, g_z, g_r, h_z \xleftarrow{\$} \mathbb{G}$. Pick $\chi_i, \gamma_i, \delta_i \xleftarrow{\$} \mathbb{Z}_p$, for $i = 1$ to n. Then, for each $i \in \{1, \ldots, n\}$, compute $g_i = g_z^{\chi_i} g_r^{\gamma_i}$, $h_i = h_z^{\chi_i} h^{\delta_i}$. The private key is $\mathsf{sk} = \{\chi_i, \gamma_i, \delta_i\}_{i=1}^n$ while the public key is defined to be

$$\mathsf{pk} = \left(g_z,\ h_r,\ h_z,\ h,\ \{g_i, h_i\}_{i=1}^n\right) \in \mathbb{G}^{2n+4}.$$

Sign($\mathsf{sk}, \tau, (M_1, \ldots, M_n)$): to sign a vector $(M_1, \ldots, M_n) \in \mathbb{G}^n$ associated with the identifier $\tau = \varepsilon$ using $sk = \{\chi_i, \gamma_i, \delta_i\}_{i=1}^n$, compute the signature consists of $\sigma = (z, r, u) \in \mathbb{G}^3$, where

$$z = \prod_{i=1}^{n} M_i^{-\chi_i}, \qquad r = \prod_{i=1}^{n} M_i^{-\gamma_i}, \qquad u = \prod_{i=1}^{n} M_i^{-\delta_i}.$$

SignDerive($\mathsf{pk}, \tau, \{(\omega_i, \sigma^{(i)})\}_{i=1}^{\ell}$): given the public key pk, a file identifier $\tau = \varepsilon$ and ℓ tuples $(\omega_i, \sigma^{(i)})$, parse each $\sigma^{(i)}$ as $\sigma^{(i)} = (z_i, r_i, u_i) \in \mathbb{G}^3$ for $i = 1$ to ℓ. Compute and return the derived signature $\sigma = (z, r, u) = \left(\prod_{i=1}^{\ell} z_i^{\omega_i}, \prod_{i=1}^{\ell} r_i^{\omega_i}, \prod_{i=1}^{\ell} u_i^{\omega_i}\right)$.

Verify($\mathsf{pk}, \sigma, \tau, (M_1, \ldots, M_n)$): given a signature $\sigma = (z, r, u) \in \mathbb{G}^3$, a vector $(M_1, \ldots, M_n)$ and a file identifier $\tau = \varepsilon$, return 1 iff $(M_1, \ldots, M_n) \neq (1_{\mathbb{G}}, \ldots, 1_{\mathbb{G}})$ and (z, r, u) satisfy

$$1_{\mathbb{G}_T} = e(g_z, z) \cdot e(g_r, r) \cdot \prod_{i=1}^{n} e(g_i, M_i), \qquad 1_{\mathbb{G}_T} = e(h_z, z) \cdot e(h, u) \cdot \prod_{i=1}^{n} e(h_i, M_i). \tag{3.1}$$

The security proof relies on the fact that, while the signing algorithm is deterministic, signatures are not unique as each vector has an exponential number of valid signatures. However, the reduction can compute exactly one signature for each vector. At the same time, an adversary has no information about which specific signature the legitimate signer would compute on a vector outside the span of already signed vectors. Moreover, by obtaining two distinct signatures on a given vector, the reduction can readily solve a given instance of the SDP problem [81].

Theorem 3 ([177]). *The scheme is unforgeable if the SDP assumption holds in* $(\mathbb{G}, \mathbb{G}_T)$.

The scheme can be modified so as to work in asymmetric pairing configurations and the Double Pairing assumption.

One particularity of this scheme is that, even if the private key is available, it remains difficult to find two distinct signatures on the same vector if the SDP assumption holds: by dividing out the two signatures, one obtains the solution of an SDP instance (g_z, g_r, h_z, h_u) contained in the public key.

3.2.2 A Full-Fledged Linearly Homomorphic SPS Scheme

Our one-time construction can be upgraded to obtain a scheme allowing to sign an arbitrary number of linear subspaces. Here, each file identifier τ consists of a L-bit string. The construction builds on the observation that, in the scheme of Section 3.2.1, signatures (z, r, u) could be re-randomized by computing $(z \cdot g_r^{\theta}, r \cdot g_z^{-\theta}, u \cdot h_z^{-\log_h(g_r)\cdot\theta})$, with $\theta \xleftarrow{\$} \mathbb{Z}_p$, if $h_z^{-\log_h(g_r)}$ were available. Since publicizing $h_z^{-\log_h(g_r)}$ would render the scheme insecure, our idea is to use Waters signatures as a support for introducing extra randomizers in the exponent.

In the scheme, the u component of each signature can be seen as an aggregation of the one-time construction with a Waters signature $(h_z^{\log_h(g_r)} \cdot H_{\mathbb{G}}(\tau)^{-\rho}, h^{\rho})$ [248] on the tag τ.

Keygen(λ, n): given a security parameter λ and the dimension $n \in \mathbb{N}$ of the subspace to be signed, choose bilinear group $(\mathbb{G}, \mathbb{G}_T)$ of prime order $p > 2^{\lambda}$. Then, conduct the following steps.

1. Choose $h \xleftarrow{\$} \mathbb{G}$ and $\alpha_z, \alpha_r, \beta_z \xleftarrow{\$} \mathbb{Z}_p$. Define $g_z = h^{\alpha_z}$, $g_r = h^{\alpha_r}$ and $h_z = h^{\beta_z}$.
2. For $i = 1$ to n, pick $\chi_i, \gamma_i, \delta_i \xleftarrow{\$} \mathbb{Z}_p$ and compute $g_i = g_z^{\chi_i} g_r^{\gamma_i}$, $h_i = h_z^{\chi_i} h^{\delta_i}$.
3. Choose a random vector $\overline{\mathbf{w}} = (w_0, w_1, \ldots, w_L) \xleftarrow{\$} \mathbb{G}^{L+1}$ and define a hash function $H_{\mathbb{G}} : \{0,1\}^L \to \mathbb{G}$ which maps the L-bit string $\tau = \tau[1] \ldots \tau[L] \in \{0,1\}^L$ to $H_{\mathbb{G}}(\tau) = w_0 \cdot \prod_{k=1}^{L} w_k^{\tau[k]}$.

The private key is $\mathsf{sk} = \left(h_z^{\alpha_r},\ \{\chi_i, \gamma_i, \delta_i\}_{i=1}^n\right)$ while the public key consists of

$$\mathsf{pk} = \left(g_z,\ g_r,\ h_z,\ h,\ \{g_i, h_i\}_{i=1}^n,\ \overline{\mathbf{w}}\right) \in \mathbb{G}^{2n+4} \times \mathbb{G}^{L+1}.$$

Sign$(\mathsf{sk}, \tau, (M_1, \ldots, M_n))$: to sign $(M_1, \ldots, M_n) \in \mathbb{G}^n$ w.r.t. the file identifier τ using the private key $sk = \left(h_z^{\alpha_r},\ \{\chi_i, \gamma_i, \delta_i\}_{i=1}^n\right)$, choose $\theta, \rho \xleftarrow{\$} \mathbb{Z}_p$ and output $\sigma = (z, r, u, v)$, where

$$\begin{aligned} z &= g_r^{\theta} \cdot \prod_{i=1}^{n} M_i^{-\chi_i} & r &= g_z^{-\theta} \cdot \prod_{i=1}^{n} M_i^{-\gamma_i} \\ u &= (h_z^{\alpha_r})^{-\theta} \cdot \prod_{i=1}^{n} M_i^{-\delta_i} \cdot H_{\mathbb{G}}(\tau)^{-\rho} & v &= h^{\rho} \end{aligned}$$

SignDerive$(\mathsf{pk}, \tau, \{(\omega_i, \sigma^{(i)})\}_{i=1}^{\ell})$: given pk, a file identifier τ and ℓ tuples $(\omega_i, \sigma^{(i)})$, parse $\sigma^{(i)}$ as $\sigma^{(i)} = (z_i, r_i, u_i, v_i) \in \mathbb{G}^4$ for $i = 1$ to ℓ. Then, choose $\rho' \xleftarrow{\$} \mathbb{Z}_p$ and compute and return $\sigma = (z, r, u, v)$, where $z = \prod_{i=1}^{\ell} z_i^{\omega_i}$, $r = \prod_{i=1}^{\ell} r_i^{\omega_i}$, $u = \prod_{i=1}^{\ell} u_i^{\omega_i} \cdot H_{\mathbb{G}}(\tau)^{-\rho'}$ and $v = \prod_{i=1}^{\ell} v_i^{\omega_i} \cdot h^{\rho'}$.

Verify$(\mathsf{pk}, \sigma, \tau, (M_1, \ldots, M_n))$: given $\sigma = (z, r, u, v) \in \mathbb{G}^4$, a file identifier τ and $(M_1, \ldots, M_n)$, return 1 if and only if $(M_1, \ldots, M_n) \neq (1_{\mathbb{G}}, \ldots, 1_{\mathbb{G}})$ and (z, r, u, v) satisfy

$$\begin{aligned} 1_{\mathbb{G}_T} &= e(g_z, z) \cdot e(g_r, r) \cdot \prod_{i=1}^{n} e(g_i, M_i), \qquad (3.2) \\ 1_{\mathbb{G}_T} &= e(h_z, z) \cdot e(h, u) \cdot e(H_{\mathbb{G}}(\tau), v) \cdot \prod_{i=1}^{n} e(h_i, M_i). \end{aligned}$$

The security of the scheme against *non-independent* Type I adversaries is proved under the SDP assumption. In the case of Type II forgeries, we need to assume the adversary to be independent because, at some point, the simulator is only able to compute a signature for a unique value[2] of θ.

Theorem 4 ([177]). *The scheme is unforgeable against independent adversaries if the SDP assumption holds in $(\mathbb{G}, \mathbb{G}_T)$. Moreover, the scheme is secure against non-independent Type I adversaries.*

Since the signature component u cannot be publicly randomized, the scheme does not have fully randomizable signatures. In Section 3.2.3, we describe a fully randomizable variant. In applications like non-malleable commitments to group elements, the above scheme is sufficient however.

[2]Note that this is not a problem since the signer can derive θ as a pseudorandom function of τ and $(M_1, \ldots, M_n)$ to make sure that a given vector is always signed using the same θ.

3.2.3 A Fully Randomizable Construction

We show that our scheme of Section 3.2.2 can be modified so as to become *strongly* context-hiding in the sense of [11, 25]. Namely, signatures produced by the SignDerive algorithm should be statistically indistinguishable from signatures freshly generated by Sign, even when the original signatures are given.

The difficulty is that, in the scheme of Section 3.2.2, we cannot re-randomize the underlying θ without knowing $h_z^{\alpha_r}$. To address this problem, it is tempting to include in each signature a randomization component of the form $(h_z^{\alpha_r} \cdot H_{\mathbb{G}}(\tau)^{-\zeta}, h^{\zeta})$, for some $\zeta \in \mathbb{Z}_p$, which can be seen as a signature on the vector $(1_{\mathbb{G}}, \ldots, 1_{\mathbb{G}})$. Unfortunately, the security proof ceases to go through as the reduction finds itself unable to generate a well-formed pair $(h_z^{\alpha_r} \cdot H_{\mathbb{G}}(\tau)^{-\zeta}, h^{\zeta})$ at some step of its interaction with the adversary. Our solution actually consists in committing to the signature components that cannot be re-randomized and provide evidence that committed group elements satisfy the verification equations. This is achieved using Groth-Sahai non-interactive arguments on a perfectly NIWI Groth-Sahai CRS, as in the linearly homomorphic construction of Attrapadung *et al.* [26]. A slight difference with [26], however, is that signature components $(H_{\mathbb{G}}(\tau)^{-\rho}, h^{-\rho})$ are no longer used and replaced by the technique of Malkin *et al.* [196], which yields slightly shorter signatures.

In the following notations, for each $h \in \mathbb{G}$ and any vector $\mathbf{g} = (g_1, g_2, g_3) \in \mathbb{G}^3$, we denote by $E(h, \mathbf{g})$ the vector $(e(h, g_1), e(h, g_2), e(h, g_3)) \in \mathbb{G}_T^3$.

Keygen(λ, n): given a security parameter λ and the dimension $n \in \mathbb{N}$ of the subspace to be signed, choose bilinear group $(\mathbb{G}, \mathbb{G}_T)$ of order $p > 2^{\lambda}$. Then, do the following.

1. Choose $h \xleftarrow{\$} \mathbb{G}$ and $\alpha_z, \alpha_r, \beta_z \xleftarrow{\$} \mathbb{Z}_p$. Define $g_z = h^{\alpha_z}$, $g_r = h^{\alpha_r}$ and $h_z = h^{\beta_z}$.
2. For $i = 1$ to n, pick $\chi_i, \gamma_i, \delta_i \xleftarrow{\$} \mathbb{Z}_p$ and compute $g_i = g_z^{\chi_i} \cdot g_r^{\gamma_i}$, $h_i = h_z^{\chi_i} \cdot h^{\delta_i}$.
3. Generate $L + 1$ Groth-Sahai CRSes by choosing $f_1, f_2 \xleftarrow{\$} \mathbb{G}$ and defining vectors $\mathbf{f_1} = (f_1, 1, g) \in \mathbb{G}^3$, $\mathbf{f_2} = (1, f_2, g) \in \mathbb{G}^3$ and $\mathbf{f}_{3,i} \xleftarrow{\$} \mathbb{G}^3$, for each $i \in \{0, \ldots, L\}$.

The private key is $\mathsf{sk} = \left(h_z^{\alpha_r},\ \{\chi_i, \gamma_i, \delta_i\}_{i=1}^n\right)$ while the public key consists of

$$\mathsf{pk} = \Big(g_z,\ g_r,\ h_z,\ h,\ \{g_i, h_i\}_{i=1}^n,\ \mathbf{f} = \left(\mathbf{f}_1, \mathbf{f}_2, \{\mathbf{f}_{3,i}\}_{i=0}^L\right)\Big).$$

Sign$(\mathsf{sk}, \tau, (M_1, \ldots, M_n))$: to sign a vector $(M_1, \ldots, M_n) \in \mathbb{G}^n$ using $\mathsf{sk} = \left(h_z^{\alpha_r},\ \{\chi_i, \gamma_i, \delta_i\}_{i=1}^n\right)$ with the file identifier τ, conduct the following steps.

1. Choose $\theta \xleftarrow{\$} \mathbb{Z}_p$ and compute

$$z = g_r^{\theta} \cdot \prod_{i=1}^{n} M_i^{-\chi_i} \qquad r = g_z^{-\theta} \cdot \prod_{i=1}^{n} M_i^{-\gamma_i} \qquad u = h_z^{-\theta \cdot \alpha_r} \cdot \prod_{i=1}^{n} M_i^{-\delta_i}$$

2. Using the bits $\tau[1] \ldots \tau[L]$ of $\tau \in \{0,1\}^L$, define the vector $\mathbf{f}_\tau = \mathbf{f}_{3,0} \cdot \prod_{i=1}^{L} \mathbf{f}_{3,i}^{\tau[i]}$ so as to assemble a Groth-Sahai CRS $\mathbf{f}_\tau = (\mathbf{f}_1, \mathbf{f}_2, \mathbf{f}_\tau)$.

3. Using $\mathbf{f}_\tau$, compute Groth-Sahai commitments

$$\begin{aligned}\mathbf{C}_z &= (1_\mathbb{G}, 1_\mathbb{G}, z) \cdot \mathbf{f_1}^{\nu_{z,1}} \cdot \mathbf{f_2}^{\nu_{z,2}} \cdot \mathbf{f}_\tau^{\nu_{z,3}},\\ \mathbf{C}_r &= (1_\mathbb{G}, 1_\mathbb{G}, r) \cdot \mathbf{f_1}^{\nu_{r,1}} \cdot \mathbf{f_2}^{\nu_{r,2}} \cdot \mathbf{f}_\tau^{\nu_{r,3}},\\ \mathbf{C}_u &= (1_\mathbb{G}, 1_\mathbb{G}, u) \cdot \mathbf{f_1}^{\nu_{u,1}} \cdot \mathbf{f_2}^{\nu_{u,2}} \cdot \mathbf{f}_\tau^{\nu_{u,3}}\end{aligned}$$

to z, r and u, respectively. Then, generate NIWI proofs $\boldsymbol{\pi}_1 = (\pi_{1,1}, \pi_{1,2}, \pi_{1,3}) \in \mathbb{G}^3$ and $\boldsymbol{\pi}_2 = (\pi_{2,1}, \pi_{2,2}, \pi_{2,3}) \in \mathbb{G}^3$ that (z, r, u) satisfy the pairing-product equations $1_{\mathbb{G}_T} = e(g_z, z) \cdot e(g_r, r) \cdot \prod_{i=1}^n e(g_i, M_i)$ and $1_{\mathbb{G}_T} = e(h_z, z) \cdot e(h, u) \cdot \prod_{i=1}^n e(h_i, M_i)$. These proofs are obtained as

$$\begin{aligned}\boldsymbol{\pi}_1 &= (\pi_{1,1}, \pi_{1,2}, \pi_{1,3}) = \big(g_z^{-\nu_{z,1}} \cdot g_r^{-\nu_{r,1}},\ g_z^{-\nu_{z,2}} \cdot g_r^{-\nu_{r,2}},\ g_z^{-\nu_{z,3}} \cdot g_r^{-\nu_{r,3}}\big)\\ \boldsymbol{\pi}_2 &= (\pi_{2,1}, \pi_{2,2}, \pi_{2,3}) = \big(h_z^{-\nu_{z,1}} \cdot h^{-\nu_{u,1}},\ h_z^{-\nu_{z,2}} \cdot h^{-\nu_{u,2}},\ h_z^{-\nu_{z,3}} \cdot h^{-\nu_{u,3}}\big)\end{aligned}$$

and satisfy the verification equations

$$\prod_{i=1}^n E\big(g_i, (1_\mathbb{G}, 1_\mathbb{G}, M_i)\big)^{-1} = E\big(g_z, \mathbf{C}_z\big) \cdot E\big(g_r, \mathbf{C}_r\big) \cdot E(\pi_{1,1}, \mathbf{f}_1) \cdot E(\pi_{1,2}, \mathbf{f}_2) \cdot E(\pi_{1,3}, \mathbf{f}_\tau) \tag{3.3}$$

$$\prod_{i=1}^n E\big(h_i, (1_\mathbb{G}, 1_\mathbb{G}, M_i)\big)^{-1} = E\big(h_z, \mathbf{C}_z\big) \cdot E\big(h, \mathbf{C}_u\big) \cdot E(\pi_{2,1}, \mathbf{f}_1) \cdot E(\pi_{2,2}, \mathbf{f}_2) \cdot E(\pi_{2,3}, \mathbf{f}_\tau).$$

The signature consists of

$$\sigma = (\mathbf{C}_z, \mathbf{C}_r, \mathbf{C}_u, \boldsymbol{\pi}_1, \boldsymbol{\pi}_2) \in \mathbb{G}^{15}. \tag{3.4}$$

SignDerive(pk, τ, $\{(\omega_i, \sigma^{(i)})\}_{i=1}^\ell$): given pk, a file identifier τ and ℓ tuples $(\omega_i, \sigma^{(i)})$, parse each signature $\sigma^{(i)}$ as a tuple of the form $\sigma^{(i)} = (\mathbf{C}_{z,i}, \mathbf{C}_{r,i}, \mathbf{C}_{u,i}, \boldsymbol{\pi}_{1,i}, \boldsymbol{\pi}_{2,i}) \in \mathbb{G}^{15}$ for $i = 1$ to ℓ. Otherwise, the derivation process proceeds in two steps.

1. Compute

$$\begin{aligned}\mathbf{C}_z &= \prod_{i=1}^\ell \mathbf{C}_{z,i}^{\omega_i} \qquad \mathbf{C}_r = \prod_{i=1}^\ell \mathbf{C}_{r,i}^{\omega_i} \qquad \mathbf{C}_u = \prod_{i=1}^\ell \mathbf{C}_{u,i}^{\omega_i}\\ \boldsymbol{\pi}_1 &= \prod_{i=1}^\ell \boldsymbol{\pi}_{1,i}^{\omega_i} \qquad \boldsymbol{\pi}_2 = \prod_{i=1}^\ell \boldsymbol{\pi}_{2,i}^{\omega_i}\end{aligned}$$

2. Re-randomize the above commitments and proofs using their homomorphic property and return the re-randomized version $\sigma = (\mathbf{C}_z, \mathbf{C}_r, \mathbf{C}_u, \boldsymbol{\pi}_1, \boldsymbol{\pi}_2)$.

Verify(pk, σ, τ, $(M_1, \ldots, M_n)$): given a pair $(\tau, (M_1, \ldots, M_n))$ and a purported signature σ parse the latter as $(\mathbf{C}_z, \mathbf{C}_r, \mathbf{C}_u, \boldsymbol{\pi}_1, \boldsymbol{\pi}_2)$. Then, return 1 if and only if it holds that $(M_1, \ldots, M_n) \neq (1_\mathbb{G}, \ldots, 1_\mathbb{G})$ and equations (3.3) are satisfied.

We believe this construction to be of interest even if we disregard its structure-preserving property. Indeed, if we compare it with the only known completely context-hiding linearly homomorphic signature in the standard model [26], its signatures are shorter by one group

element. Moreover, we can prove the security under the sole DLIN assumption whereas the scheme of [26] requires an additional assumption.

The scheme is clearly completely context hiding because signatures only consist of perfectly randomizable commitments and NIWI arguments.

As for the unforgeability of the scheme, the proof of the following theorem is along the lines of [196, Theorem 5]. However, we can only prove unforgeability in a weaker sense as we need to assume that the adversary is targeting. Namely, in the case of Type II attacks, the adversary must also output a proof that it actually broke the security of the scheme and that its vector $\mathbf{M}^\star = (M_1^\star, \ldots, M_n^\star) \in \mathbb{G}^n$ is indeed independent of the vectors for which it obtained signatures for the target tag $\tau^\star$.

If $\{\mathbf{M}_i = (M_{i,1}, \ldots, M_{i,n})\}_{i=1}^m$ denote the linearly independent vectors that were signed for $\tau^\star$, the adversary could simply output a vector $\mathbf{W} = (W_1, \ldots, W_n) \in \mathbb{G}^n$ such that $\prod_{j=1}^n e(M_j^\star, W_j) \neq 1_{\mathbb{G}_T}$ and $\prod_{j=1}^n e(M_{i,j}, W_j) = 1_{\mathbb{G}_T}$ for each $i \in \{1, \ldots, m\}$. The latter test guarantees that the adversary's output is a non-trivial Type II forgery.

Theorem 5 ([177]). *The above scheme provides unforgeability against independent targeting adversaries if the DLIN assumption holds in* $\mathbb{G}$.

3.2.4 Application to Verifiable Computation on Encrypted Data

Linearly homomorphic schemes are known (see, *e. g.*, [11]) to provide verifiable computation mechanisms for outsourced data. Suppose that a user has a dataset consisting of n samples $s_1, \ldots, s_n \in \mathbb{Z}_p$. The dataset can be encoded as vectors $\mathbf{v}_i = (\mathbf{e}_i | s_i) \in \mathbb{Z}_p^{n+1}$, where $\mathbf{e}_i \in \mathbb{Z}_p^n$ denotes the i-th unit vector for each $i \in \{1, \ldots, n\}$. The user then assigns a file identifier τ to $\{\mathbf{v}_i\}_{i=1}^n$, computes signatures $\sigma_i \leftarrow \mathsf{Sign}(\mathsf{sk}, \tau, \mathbf{v}_i)$ on the resulting vectors and stores $\{(\mathbf{v}_i, \sigma_i)\}_{i=1}^n$ at the server. When requested, the server can then evaluate a sum $s = \sum_{i=1}^n s_i$ and provide evidence that the latter computation is correct by deriving a signature on the vector $(1, 1, \ldots, 1, s) \in \mathbb{Z}_p^{n+1}$. Unless the server is able to forge a signature for a vector outside the span of $\{\mathbf{v}_i\}_{i=1}^n$, it is unable to fool the user. The above method readily extends to authenticate weighted sums or Fourier transforms.

One disadvantage of the above method is that it requires the server to retain the dataset $\{s_i\}_{i=1}^n$ in the clear. Using LHSPS schemes, the user can apply the above technique on encrypted samples using the Boneh-Boyen-Shacham (BBS) cryptosystem [44].

The BBS cryptosystem involves a public key $(g, \tilde{g}, f = g^x, h = g^y) \in_R \mathbb{G}^4$, where $(x, y) \in \mathbb{Z}_p^2$ is the private key. The user (or anyone else knowing his public key) can first encrypt his samples $\{s_i\}_{i=1}^n$ by computing BBS encryptions $(C_{1,i}, C_{2,i}, C_{3,i}) = (f^{r_i}, h^{t_i}, \tilde{g}^{s_i} \cdot g^{r_i+t_i})$, with $r_i, t_i \xleftarrow{\$} \mathbb{Z}_p$, for each $i \in \{1, \ldots, n\}$. If the user holds a LHSPS key pair for vectors of dimension $n+3$, he can generate n signatures on vectors $((C_{1,i}, C_{2,i}, C_{3,i}) | \mathbf{E}_i) \in \mathbb{G}^{n+3}$, where $\mathbf{E}_i = (1_{\mathbb{G}}, \ldots, 1_{\mathbb{G}}, g, 1_{\mathbb{G}}, \ldots, 1_{\mathbb{G}}) = g^{\mathbf{e}_i}$ for each $i \in \{1, \ldots, n\}$, using the scheme of Section 3.2.2. The vectors $\{((C_{1,i}, C_{2,i}, C_{3,i}) | \mathbf{E}_i)\}_{i=1}^n$ and their signatures $\{(z_i, r_i, u_i, v_i)\}_{i=1}^n$ are then archived in the cloud in such a way that the server can publicly derive a signature on the vector $\left(f^{\sum_i r_i}, h^{\sum_i t_i}, \tilde{g}^{\sum_i s_i} \cdot g^{\sum_i (r_i+t_i)}, g, g, \ldots, g\right) \in \mathbb{G}^{n+3}$ in order to convince the client that the encrypted sum was correctly computed. Using his private key (x, y), the client can then retrieve the sum $\sum_i s_i$ as long as it remains in a sufficiently small range.

The interest of the above solution lies in that the client can dispense with the need for storing the $O(n)$-size public key of his linearly homomorphic signature. Indeed, he can simply retain the random seed that was used to generate pk and re-compute private key

elements $\{(\chi_i, \gamma_i, \delta_i)\}_{i=1}^n$ whenever he wants to verify the server's response. In this case, the verification equations (3.2) become

$$1_{\mathbb{G}_T} = e(g_z, z \cdot \prod_{i=1}^{n} M_i^{\chi_i}) \cdot e(g_r, r \cdot \prod_{i=1}^{n} M_i^{\gamma_i}) = e(h_z, z \cdot \prod_{i=1}^{n} M_i^{\chi_i}) \cdot e(h, u \cdot \prod_{i=1}^{n} M_i^{\delta_i}) \cdot e(H_{\mathbb{G}}(\tau), v),$$

so that the client only has to compute $O(1)$ pairings. Moreover, the client does not have to determine an upper bound on the size of his dataset when generating his public key. Initially, he only needs to generate $\{(g_j, h_j)\}_{j=1}^3$. When the i-th ciphertext $(C_{1,i}, C_{2,i}, C_{3,i})$ has to be stored, the client derives $(\chi_{i+3}, \gamma_{i+3}, \delta_{i+3})$ and (g_{i+3}, h_{i+3}) by applying a PRF to the index i. This will be sufficient to sign vectors of the form $((C_{1,i}, C_{2,i}, C_{3,i})|\mathbf{E}_i)$.

Complete and security models for "verifiable computation on encrypted data" are beyond the scope of this work. Here, they would naturally combine the properties of secure homomorphic encryption and authenticated computing. It should be intuitively clear that a malicious server cannot trick a client into accepting an incorrect result (i.e., one which differs from the actual defined linear function it is supposed to compute over the defined signed ciphertext inputs) without defeating the security of the underlying homomorphic signature.

3.3 Non-Malleable Trapdoor Commitments to Group Elements from Linearly Homomorphic Structure-Preserving Signatures

This section shows that, under a certain mild condition (fulfilled by our constructions), LH-SPS imply length-reducing non-malleable structure-preserving commitments to vectors of group elements.

As a result, we obtain the first length-reducing non-malleable structure-preserving trapdoor commitment. Our scheme is not *strictly*[3] structure-preserving (according to the terminology of [7]) because the commitment string lives in $\mathbb{G}_T$ rather than $\mathbb{G}$. Still, openings only consist of elements in $\mathbb{G}$, which makes it possible to generate efficient NIWI proofs that committed group elements satisfy certain properties. To our knowledge, the only known non-malleable commitment schemes whose openings only consist of group elements were described by Fischlin *et al.* [108]. However, these constructions cannot be length-reducing as they achieve universal composability [70, 71].

Our schemes are obtained by first constructing simulation-sound trapdoor commitments (SSTC) [116, 195] to group elements. SSTC schemes were first suggested by Garay, MacKenzie and Yang [116] as a tool for constructing universally composable zero-knowledge proofs [70]. MacKenzie and Yang subsequently gave a simplified security definition which suffices to provide non-malleability with respect to opening in the sense of the definition of re-usable non-malleable commitments [94].

In a SSTC, each commitment is labeled with a tag. The definition of [195] requires that, even if the adversary can see equivocations of commitments to possibly distinct messages for several tags $tag_1, \ldots, tag_q$, it will not be able to break the binding property for a new tag $tag \notin \{tag_1, \ldots, tag_q\}$.

[3] We recall that strictly structure-preserving commitments cannot be length-reducing, as shown by Abe *et al.* [7], so that our scheme is essentially the best we can hope for if we aim at short commitment stings.

Definition 7 ([195]). *A simulation-sound trapdoor commitment (SSTC)* $(\mathsf{Setup}, \mathsf{Com}, \mathsf{FakeCom}, \mathsf{FakeOpen}, \mathsf{Verify})$ *is a tuple where* $(\mathsf{Setup}, \mathsf{Com}, \mathsf{Verify})$ *forms a non-interactive commitment scheme and* $(\mathsf{FakeCom}, \mathsf{FakeOpen})$ *are PPT algorithms with the following properties*

Trapdoor: *for any tag and any message* Msg*, the following distributions are computationally indistinguishable:*

$$D_{fake} := \{(pk, tk) \leftarrow \mathsf{Setup}(\lambda);\ (\widetilde{\mathsf{com}}, \mathsf{aux}) \leftarrow \mathsf{FakeCom}(pk, tk, tag);\ \widetilde{\mathsf{dec}} \leftarrow \mathsf{FakeOpen}(\mathsf{aux}, tk, \widetilde{\mathsf{com}}, \mathsf{Msg}) : (pk, tag, \mathsf{Msg}, \widetilde{\mathsf{com}}, \widetilde{\mathsf{dec}})\}$$

$$D_{real} := \{(pk, tk) \leftarrow \mathsf{Setup}(\lambda);\ (\mathsf{com}, \mathsf{dec}) \leftarrow \mathsf{Com}(pk, tag, \mathsf{Msg}) : (pk, tag, \mathsf{Msg}, \mathsf{com}, \mathsf{dec})\}$$

Simulation-sound binding: *for any PPT adversary* $\mathcal{A}$*, the following probability is negligible*

$$\Pr[(pk, tk) \leftarrow \mathsf{Setup}(\lambda);\ (\mathsf{com}, tag, \mathsf{Msg}_1, \mathsf{Msg}_2, \mathsf{dec}_1, \mathsf{dec}_2) \leftarrow \mathcal{A}^{\mathcal{O}_{tk,pk}}(pk) : \mathsf{Msg}_1 \neq \mathsf{Msg}_2 \wedge \mathsf{Verify}(pk, tag, \mathsf{Msg}_1, \mathsf{com}, \mathsf{dec}_1) = \mathsf{Verify}(pk, tag, \mathsf{Msg}_2, \mathsf{com}, \mathsf{dec}_2) = 1 \wedge tag \notin Q],$$

where $\mathcal{O}_{tk,pk}$ *is an oracle that maintains an initially empty set* Q *and operates as follows:*

- *On input* (commit, tag)*, it runs* $(\widetilde{\mathsf{com}}, \mathsf{aux}) \leftarrow \mathsf{FakeCom}(pk, tk, tag)$*, stores the triple* $(\widetilde{\mathsf{com}}, tag, \mathsf{aux})$*, returns* $\widetilde{\mathsf{com}}$*.*
- *On input* $(\mathsf{decommit}, \widetilde{\mathsf{com}}, \mathsf{Msg})$*: if a tuple* $(\widetilde{\mathsf{com}}, tag, \mathsf{aux})$ *was previously stored, it computes* $\widetilde{\mathsf{dec}} \leftarrow \mathsf{FakeOpen}(\mathsf{aux}, tk, tag, \widetilde{\mathsf{com}}, \mathsf{Msg})$*, adds* tag *in* Q *and returns* $\widetilde{\mathsf{dec}}$*. Otherwise,* $\mathcal{O}_{tk,pk}$ *returns* $\perp$*.*

While our SSTC to group elements will be proved secure in the above sense, a *non-adaptive* flavor of simulation-sound binding security is sufficient for the construction of non-malleable commitments. Indeed, Gennaro used [118] such a relaxed notion to achieve non-malleability from similar-looking multi-trapdoor commitments. In the non-adaptive notion, the adversary has to choose the set of tags $tag_1, \ldots, tag_\ell$ for which it wants to query the $\mathcal{O}_{tk,pk}$ oracle before seeing the public key pk.

3.3.1 Template of Linearly Homomorphic SPS Scheme

We first remark that *any* constant-size linearly homomorphic structure-preserving signature necessarily complies with the template below. Indeed, in order to have a linear homomorphism, each verification equation necessarily computes a product of pairings which should equal $1_{\mathbb{G}_T}$ in a valid signature. In each pairing of the product, one of the arguments must be a message or signature component while the second argument is either part of the public key or an encoding of the file identifier.

For simplicity, the template is described in terms of symmetric pairings but generalizations to asymmetric configurations are possible.

Keygen(λ, n): given λ and the dimension $n \in \mathbb{N}$ of the vectors to be signed, choose constants n_z, n_v, m. Among these, n_z and n_v will determine the signature length while

m will be the number of verification equations. Then, choose $\{F_{j,\mu}\}_{j\in\{1,\ldots,m\},\mu\in\{1,\ldots,n_z\}}$, $\{G_{j,i}\}_{i\in\{1,\ldots,n\},\ j\in\{j,\ldots,m\}}$ in the group $\mathbb{G}$. The public key is

$$\mathsf{pk} = \left(\{F_{j,\mu}\}_{j\in\{1,\ldots,m\},\mu\in\{1,\ldots,n_z\}}, \{G_{j,i}\}_{i\in\{1,\ldots,n\},\ j\in\{j,\ldots,m\}}\right)$$

while sk consists of information about the representation of public elements w.r.t. specific bases.

Sign$(\mathsf{sk}, \tau, (M_1, \ldots, M_n))$: Outputs a tuple $\sigma = \left(Z_1, \ldots, Z_{n_z}, V_1, \ldots, V_{n_v}\right) \in \mathbb{G}^{n_z+n_v}$.

SignDerive$(\mathsf{pk}, \tau, \{(\omega_i, \sigma^{(i)})\}_{i=1}^{\ell})$: parses each $\sigma^{(i)}$ as $\left(Z_1^{(i)}, \ldots, Z_{n_z}^{(i)}, V_1^{(i)}, \ldots, V_{n_v}^{(i)}\right)$ and computes

$$Z_\mu = \prod_{i=1}^{\ell} {Z_\mu^{(i)}}^{\omega_i} \qquad V_\nu = \prod_{i=1}^{\ell} {V_\nu^{(i)}}^{\omega_i} \qquad \mu \in \{1, \ldots, n_z\},\ \nu \in \{1, \ldots, n_v\}.$$

After a possible extra re-randomization step, it outputs $\left(Z_1, \ldots, Z_{n_z}, V_1, \ldots, V_{n_v}\right)$.

Verify$(\mathsf{pk}, \sigma, \tau, (M_1, \ldots, M_n))$: given a signature $\sigma = \left(Z_1, \ldots, Z_{n_z}, V_1, \ldots, V_{n_v}\right) \in \mathbb{G}^{n_z+n_v}$, a tag τ and $(M_1, \ldots, M_n)$, return 0 if $(M_1, \ldots, M_n) = (1_{\mathbb{G}}, \ldots, 1_{\mathbb{G}})$. Otherwise, do the following.

1. For each $j \in \{1, \ldots, m\}$ and $\nu \in \{1, \ldots, n_v\}$, compute one-to-one[4] encodings $T_{j,\nu} \in \mathbb{G}$ of the tag τ as a group element.
2. Return 1 if and only if $c_j = 1_{\mathbb{G}_T}$ for $j = 1$ to m, where

$$c_j = \prod_{\mu=1}^{n_z} e(F_{j,\mu}, Z_\mu) \cdot \prod_{\nu=1}^{n_v} e(T_{j,\nu}, V_\nu) \cdot \prod_{i=1}^{n} e(G_{j,i}, M_i) \qquad j \in \{1, \ldots, m\}. \quad (3.5)$$

In the following, we say that a linearly homomorphic SPS is *regular* if, for each file identifier τ, any non-trivial vector $(M_1, \ldots, M_n) \neq (1_{\mathbb{G}}, \ldots, 1_{\mathbb{G}})$ has a valid signature.

3.3.2 Construction of Simulation-Sound Structure-Preserving Trapdoor Commitments

Let $\Pi^{\mathsf{SPS}} = (\mathsf{Keygen}, \mathsf{Sign}, \mathsf{SignDerive}, \mathsf{Verify})$ be a linearly homomorphic SPS. We construct a simulation-sound trapdoor commitment as follows.

SSTC.Setup(λ, n): given the desired dimension $n \in \mathbb{N}$ of committed vectors, choose public parameters pp for the linearly homomorphic SPS scheme. Then, run $\Pi^{\mathsf{SPS}}.\mathsf{Keygen}(\lambda, n)$ to obtain a public key $\mathsf{pk} = \left(\{F_{j,\mu}\}_{j\in\{1,\ldots,m\},\mu\in\{1,\ldots,n_z\}}, \{G_{j,i}\}_{i\in\{1,\ldots,n\},\ j\in\{j,\ldots,m\}}\right)$, for some constants n_z, n_v, m, and a sk. The commitment key is $pk = \mathsf{pk}$ and the trapdoor tk consists of sk. Note that the public key defines a signature space $\mathbb{G}^{n_z+n_v}$, for constants n_z and n_v.

[4] This condition can be relaxed to have collision-resistant deterministic encodings. Here, we assume injectivity for simplicity.

SSTC.Com$(pk, tag, (M_1, \ldots, M_n))$: to commit to $(M_1, \ldots, M_n) \in \mathbb{G}^n$ with respect to the tag $tag = \tau$, choose $(Z_1, \ldots, Z_{n_z}, V_1, \ldots, V_{n_v}) \xleftarrow{\$} \mathbb{G}^{n_z+n_v}$ in the signature space. Then, run step 1 of the verification algorithm and evaluate the right-hand-side member of (3.5). Namely, compute

$$c_j = \prod_{\mu=1}^{n_z} e(F_{j,\mu}, Z_\mu) \cdot \prod_{\nu=1}^{n_v} e(T_{j,\nu}, V_\nu) \cdot \prod_{i=1}^{n} e(G_{j,i}, M_i) \qquad j \in \{1, \ldots, m\} \tag{3.6}$$

where $\{T_{j,\nu}\}_{j,\nu}$ form an injective encoding of $tag = \tau$ as a set of group elements. The commitment string is defined to be $\mathsf{com} = (c_1, \ldots, c_m)$ whereas the decommitment consists of $\mathsf{dec} = (Z_1, \ldots, Z_{n_z}, V_1, \ldots, V_{n_v})$.

SSTC.FakeCom(pk, tk, tag): proceeds like SSTC.Com with $(\hat{M}_1, \ldots, \hat{M}_n) \xleftarrow{\$} \mathbb{G}^n$. If $(\hat{\mathsf{com}}, \hat{\mathsf{dec}})$ denotes the resulting pair, the algorithm outputs $\widetilde{\mathsf{com}} = \hat{\mathsf{com}}$ and the auxiliary information aux, which consists of the pair $\mathsf{aux} = ((\hat{M}_1, \ldots, \hat{M}_n), \hat{\mathsf{dec}})$ for $tag = \tau$.

SSTC.FakeOpen$(\mathsf{aux}, tk, tag, \widetilde{\mathsf{com}}, (M_1, \ldots, M_n))$: the algorithm parses $\widetilde{com}$ as $(\tilde{c}_1, \ldots, \tilde{c}_m)$ and aux as $\big((\hat{M}_1, \ldots, \hat{M}_n), (\hat{Z}_1, \ldots, \hat{Z}_{n_z}, \hat{V}_1, \ldots, \hat{V}_{n_v})\big)$. It first generates a homomorphic signature on $(M_1/\hat{M}_1, \ldots, M_n/\hat{M}_n)$ for the tag $tag = \tau$. Namely, using $tk = \mathsf{sk}$, compute $\sigma' = (Z'_1, \ldots, Z'_{n_z}, V'_1, \ldots, V'_{n_v}) \leftarrow \Pi^{\mathsf{SPS}}.\mathsf{Sign}\big(\mathsf{sk}, \tau, (M_1/\hat{M}_n, \ldots, M_n/\hat{M}_n)\big)$. Since σ' is a valid signature and $\mathsf{aux} = \big((\hat{M}_1, \ldots, \hat{M}_n), (\hat{Z}_1, \ldots, \hat{Z}_{n_z}, \hat{V}_1, \ldots, \hat{V}_{n_v})\big)$ satisfies

$$\tilde{c}_j = \prod_{\mu=1}^{n_z} e(F_{j,\mu}, \hat{Z}_\mu) \cdot \prod_{\nu=1}^{n_v} e(T_{j,\nu}, \hat{V}_\nu) \cdot \prod_{i=1}^{n} e(G_{j,i}, \hat{M}_i) \qquad j \in \{1, \ldots, m\}, \tag{3.7}$$

the algorithm can run $(\tilde{Z}_1, \ldots, \tilde{Z}_{n_z}, \tilde{V}_1, \ldots, \tilde{V}_{n_v}) \leftarrow \mathsf{SignDerive}(\mathsf{pk}, \tau, \{(1, \sigma'), (1, \hat{\sigma})\})$, where $\hat{\sigma} = (\hat{Z}_1, \ldots, \hat{Z}_{n_z}, \hat{V}_1, \ldots, \hat{V}_{n_v})$, and output $\widetilde{\mathsf{dec}} = (\tilde{Z}_1, \ldots, \tilde{Z}_{n_z}, \tilde{V}_1, \ldots, \tilde{V}_{n_v})$ which is a valid de-commitment to the vector $(M_1, \ldots, M_n)$ with respect to $tag = \tau$.

SSTC.Verify$(pk, tag, (M_1, \ldots, M_n), \mathsf{com}, \mathsf{dec})$: parse com as $(c_1, \ldots, c_m) \in \mathbb{G}_T^m$ and the de-commitment dec as $(Z_1, \ldots, Z_{n_z}, V_1, \ldots, V_{n_v}) \in \mathbb{G}^{n_z+n_v}$ (if these values do not parse properly, return 0). Then, compute a one-to-one encoding $\{T_{j,\nu}\}_{j,\nu}$ of $tag = \tau$. Return 1 if relations (3.6) hold and 0 otherwise.

In the full version of [177], we generalize the above construction so as to build simulation-sound trapdoor commitment to vectors from any linearly homomorphic signature that fits a certain template. This template captures essentially all known pairing-based constructions, including LHSPS schemes. As a result, we obtain a modular construction of constant-size non-malleable commitment to vectors which preserves the feasibility of efficiently proving properties about committed values. In particular, our generalized construction can be instantiated using the CDH-based (non-structure-preserving) linearly homomorphic signature of Attrapadung, Libert and Peters [25]. Unlike the CDH-based simulation-sound commitment of Fujisaki [114], our realization is non-interactive and allows committing to vectors with a constant-size commitment string. Unlike the solution consisting in committing to a short string obtained by hashing the vector, our solution allows the sender to prove properties (using Σ protocols or Groth-Sahai proofs) about committed vectors in an efficient way.

For vectors of dimension $n = 1$, we obtain a simplification of existing multi-trapdoor (or

identity-based) trapdoor commitments [100, 214] based on Waters signatures. Our generalized construction of simulation-sound commitments [177] can also be instantiated under the Strong Diffie-Hellman assumption using the homomorphic signature of Catalano *et al.* [78]. For vectors of dimension 1, the obtained non-malleable commitment is a variant of the one of [118, Section 4.2].

Theorem 6 ([177]). *Assuming that the underlying linearly homomorphic SPS is regular and secure against non-independent Type I adversaries, the above construction is a simulation-sound trapdoor commitment to group elements.*

A standard technique (see, e.g., [116, 118]) to build a re-usable and non-interactive non-malleable commitment (assuming a CRS) from a SSTC scheme is as follows. To commit to Msg, the sender generates a key-pair $(\mathsf{VK}, \mathsf{SK})$ for a one-time signature and generates $(\mathsf{com}, \mathsf{dec}) \leftarrow \mathsf{SSTC.Commit}(pk, \mathsf{VK}, \mathsf{MSg})$ using VK as a tag. The non-malleable commitment string is the pair $(\mathsf{com}, \mathsf{VK})$ and the opening is given by (dec, σ), where σ is a one-time signature on com, so that the receiver additionally checks the validity of σ. This construction is known to provide independence [93, 121] and thus non-malleability with respect to opening, as proved in [93, 121].

In our setting, we cannot compute σ as a signature of com, as it consists of $\mathbb{G}_T$ elements. However, we can rather sign the pair $(\mathsf{Msg}, \mathsf{dec})$ — whose components live in $\mathbb{G}$ — as long as it uniquely determines com. To this end, we can use the one-time structure-preserving of [6, Appendix C.1] since it allows signing messages of arbitrary length using a constant-size one-time public key. Like our scheme of Section 3.2.2, it relies on the SDP assumption and thus yields a non-malleable commitment based on this sole assumption. Alternatively, we can move σ in the commitment string (which thus consists of $(\mathsf{com}, \mathsf{VK}, \sigma)$), in which case the one-time signature does not need to be structure-preserving but it has to be strongly unforgeable (as can be observed from the definition of independent commitments [93]) while the standard notion of unforgeability suffices in the former case.

3.4 (Constant-Size) Simulation-Sound Quasi-Adaptive NIZK Arguments from LHSPS Schemes

Earlier sections showed that structure-preserving signatures with additive homomorphic properties have unexpected applications in the design of non-malleable structure-preserving commitments. In this section, we extend their range of applications and demonstrate that they can surprisingly be used (albeit non-generically) in the design of simulation-sound quasi-adaptive NIZK (QA-NIZK) proofs and chosen-ciphertext-secure cryptosystems.

Concretely, our one-time LHSPS scheme of Section 3.2.1 already allows showing membership of a $t \times n$ linear subspace (of rank $t < n$) using only 3 group elements under the SDP assumption. Moreover, we show how to extend this construction to get unbounded simulation-soundness while retaining *constant-size* proofs. The length of a proof does not depend on the number of equations or the number of variables, but only on the underlying assumption. Like those of [151], our proofs are computationally sound under standard assumptions. Somewhat surprisingly, they are even asymptotically shorter than random-oracle-based proofs derived from Σ-protocols.

Under the DLIN assumption, we obtain QA-NIZK arguments consisting of 15 group elements and a one-time signature with its verification key. As it turns out, it is also the first

unbounded simulation-sound proof system that does not involve quadratic pairing product equations or a CCA2-secure encryption scheme. Efficiency comparisons show that we only need 20 group elements per proof where the best USS extension [62] of Groth-Sahai costs $6t + 2n + 52$ group elements. Under the k-linear assumption, the proof length becomes $O(k^2)$ and thus avoids any dependency on the subspace dimension.

For applications, like CCA2 security [208, 231], where only one-time simulation-soundness is needed, we further optimize our proof system and obtain a relatively simulation-sound QA-NIZK proof system, as defined in [150], with constant-size proofs. Under the DLIN assumption (resp. the k-linear assumption), we achieve relative simulation-soundness with only 4 (resp. $k + 2$) group elements!

As the first application of USS proofs, we construct a chosen-ciphertext-secure keyed-homomorphic encryption scheme with threshold decryption. Keyed-homomorphic encryption is a primitive, suggested by Emura *et al.* [104], where homomorphic ciphertext manipulations are only possible to a party holding a devoted evaluation key SK_h which, by itself, does not enable decryption. The scheme should provide IND-CCA2 security when the evaluation key is unavailable to the adversary and remain IND-CCA1 secure when SK_h is exposed. Other approaches to reconcile homomorphism and non-malleability were taken in [221, 222, 223, 51, 83] but they inevitably satisfy weaker security notions than adaptive chosen-ciphertext security [226]. The results of [104] showed that CCA2-security does not rule out homomorphicity when the capability to compute over encrypted data is restricted.

Emura *et al.* [104] gave realizations of CCA2-secure keyed-homomorphic schemes based on hash proof systems [90]. However, these do not readily enable threshold decryption – as would be desirable in voting protocols – since valid ciphertexts are not publicly recognizable, which makes it harder to prove CCA security in the threshold setting. Moreover, these solutions are not known to satisfy the strongest security definition of [104]. The reason is that this definition seemingly requires a form of unbounded simulation-soundness. Our QA-NIZK proofs fulfill this requirement and provide an efficient CCA2-secure threshold keyed-homomorphic system where ciphertexts are 65% shorter than in instantiations of the same high-level idea using previous simulation-sound proofs.

Using our relatively simulation-sound QA-NIZK proofs, we then build adaptively secure non-interactive threshold cryptosystems with CCA2 security and improved efficiency. The constructions of Libert and Yung [191] were improved by Escala *et al.* [105]. So far, the most efficient solution is obtained from the Jutla-Roy results [150, 151] via relatively sound proofs [150]. Using our relatively sound QA-NIZK proof system, we shorten ciphertexts by $\Theta(k)$ elements under the k-linear assumption.

3.4.1 Construction with Unbounded Simulation-Soundness

In the following, vectors are considered as row vectors. If $\mathbf{A} \in \mathbb{Z}_p^{t\times n}$ is a matrix, we denote by $g^{\mathbf{A}} \in \mathbb{G}^{t\times n}$ the matrix obtained by exponentiating g using the entries of $\mathbf{A}$.

We consider public parameters $\Gamma = (\mathbb{G}, \mathbb{G}_T, g)$ consisting of bilinear groups $(\mathbb{G}, \mathbb{G}_T)$ with a generator $g \in \mathbb{G}$. Like [151], we will consider languages $\mathcal{L}_\rho = \{g^{\mathbf{x}\cdot\mathbf{A}} \in \mathbb{G}^n \mid \mathbf{x} \in \mathbb{Z}_p^t\}$ that are parametrized by $\rho = g^{\mathbf{A}} \in \mathbb{G}^{t\times n}$, where $\mathbf{A} \in \mathbb{Z}_q^{t\times n}$ is a $t \times n$ matrix of rank $t < n$.

As in [151], we assume that the distribution $\mathcal{D}_\Gamma$ is efficiently samplable: there exists a PPT algorithm which outputs a pair $(\rho, \mathbf{A})$ describing a relation R_ρ and its associated language $\mathcal{L}_\rho$ according to $\mathcal{D}_\Gamma$. One example of such a distribution is obtained by picking a uniform matrix $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_p^{t\times n}$ – which has full rank with overwhelming probability – and setting $\rho = g^{\mathbf{A}}$.

Our construction builds on the homomorphic signature recalled in Section 3.2.3. Specifically, the language-dependent CRS ψ contains one-time linearly homomorphic signatures on the rows of the matrix $\rho \in \mathbb{G}^{t\times n}$. For each vector $\mathbf{v} \in \mathcal{L}_\rho$, the prover can use the witness $\mathbf{x} \in \mathbb{Z}_p^t$ to derive and prove knowledge of a one-time homomorphic signature (z, r, u) on $\mathbf{v}$. This signature (z, r, u) is already a QA-NIZK proof of membership but it does not provide simulation-soundness. To acquire this property, we follow [196] and generate a NIWI proof of knowledge of (z, r, u) for a Groth-Sahai CRS that depends on the verification key of an ordinary one-time signature. The latter's private key is used to sign the NIWI proof so as to prevent unwanted proof manipulations. Using the private key of the homomorphic one-time signature as a trapdoor, the simulator is also able to create proofs for vectors $\mathbf{v} \notin \mathcal{L}_\rho$. Due to the use of perfectly NIWI proofs, these fake proofs do not leak any more information about the simulation key than the CRS does. At the same time, the CRS can be prepared so that, with non-negligible probability, it becomes perfectly binding on an adversarially-generated proof, which allows extracting a non-trivial signature on a vector $\mathbf{v} \notin \mathcal{L}_\rho$.

Like [151], our QA-NIZK proof system $(\mathbb{K}_0, \mathbb{K}_1, \mathsf{P}, \mathsf{V})$ is a split CRS construction in that $\mathbb{K}_1$ can be divided into two algorithms $(\mathbb{K}_{10}, \mathbb{K}_{11})$. The first one $\mathbb{K}_{10}$ outputs some state information s and a first CRS $\mathbf{CRS}_2$ which is only used by the verifier and does not depend on the language $\mathcal{L}_\rho$. The second part $\mathbb{K}_{11}$ of $\mathbb{K}_1$ inputs the state information s and the output of Γ of $\mathbb{K}_0$ and outputs $\mathbf{CRS}_1$ which is only used by the prover.

$\mathbb{K}_0(\lambda)$**:** choose symmetric bilinear groups $(\mathbb{G}, \mathbb{G}_T)$ of prime order $p > 2^\lambda$ with $g \xleftarrow{\$} \mathbb{G}$. Then, output $\Gamma = (\mathbb{G}, \mathbb{G}_T, g)$

The dimensions (t, n) of the matrix $\mathbf{A} \in \mathbb{Z}_p^{t\times n}$ can be either fixed or part of the language, so that t, n can be given as input to the CRS generation algorithm $\mathbb{K}_1$.

$\mathbb{K}_1(\Gamma, \rho)$**:** parse Γ as $(\mathbb{G}, \mathbb{G}_T, g)$ and ρ as a matrix $\rho = \big(G_{i,j}\big)_{1\le i\le t,\, 1\le j\le n} \in \mathbb{G}^{t\times n}$.

1. Generate a key pair $(\mathsf{pk}_{hsps}, \mathsf{sk}_{hsps})$ for the randomizable LHSPS of Section 3.2.3 to sign vectors of $\mathbb{G}^n$. Namely, choose $g_z, g_r, h_z, h_u \xleftarrow{\$} \mathbb{G}$ and do the following.
   a. For $i = 1$ to n, pick $\chi_i, \gamma_i, \delta_i \xleftarrow{\$} \mathbb{Z}_p$ and compute $g_i = g_z{}^{\chi_i} g_r{}^{\gamma_i}$ and $h_i = h_z{}^{\chi_i} h_u{}^{\delta_i}$.
   b. Generate $L + 1$ Groth-Sahai common reference strings, for some $L \in \mathsf{poly}(\lambda)$. To this end, choose $f_1, f_2 \xleftarrow{\$} \mathbb{G}$ and define the vectors $\mathbf{f}_1 = (f_1, 1, g) \in \mathbb{G}^3$, $\mathbf{f}_2 = (1, f_2, g) \in \mathbb{G}^3$. Then, pick $\mathbf{f}_{3,i} \xleftarrow{\$} \mathbb{G}^3$ for $i = 0$ to L.

   Let $\mathsf{sk}_{hsps} = \{(\chi_i, \gamma_i, \delta_i)\}_{i=1}^n$ be the private key and the matching public key is

$$\mathsf{pk}_{hsps} \;=\; \Big(g_z,\ g_r,\ h_z,\ h_u,\ \{(g_i, h_i)\}_{i=1}^n,\ \mathbf{f} = \big(\mathbf{f}_1, \mathbf{f}_2, \{\mathbf{f}_{3,i}\}_{i=0}^L\big) \Big).$$

2. Use sk_{hsps} to generate one-time linearly homomorphic signatures $\{(z_i, r_i, u_i)\}_{i=1}^t$ on the vectors $(G_{i1}, \ldots, G_{in}) \in \mathbb{G}^n$ that form the rows of ρ. These are obtained as

$$(z_i, r_i, u_i) \;=\; \Big(\prod_{j=1}^n G_{i,j}^{-\chi_j},\ \prod_{j=1}^n G_{i,j}^{-\gamma_j},\ \prod_{j=1}^n G_{i,j}^{-\delta_j}\Big) \qquad\qquad \forall i \in \{1, \ldots, t\}.$$

3. Choose a strongly unforgeable one-time signature $\Sigma = (\mathcal{G}, \mathcal{S}, \mathcal{V})$ with verification keys consisting of L-bit strings.

4. The CRS $\psi = (\mathbf{CRS}_1, \mathbf{CRS}_2)$ consists of two parts which are defined as

$$\mathbf{CRS}_1 = \Big(\rho,\ \mathsf{pk}_{hsps},\ \{(z_i, r_i, u_i)\}_{i=1}^{t},\ \Sigma\Big), \qquad \mathbf{CRS}_2 = \Big(\mathsf{pk}_{hsps},\ \Sigma\Big),$$

while the simulation trapdoor τ_{sim} is $\mathsf{sk}_{hsps} = \{(\chi_i, \gamma_i, \delta_i)\}_{i=1}^{n}$.

$\mathsf{P}(\Gamma, \psi, \mathbf{v}, x, \mathsf{lbl})$**:** given a vector $\mathbf{v} \in \mathbb{G}^n$ and a witness $\mathbf{x} = (x_1, \ldots, x_t) \in \mathbb{Z}_p^t$ such that $\mathbf{v} = g^{\mathbf{x}\cdot\mathbf{A}}$, generate a one-time signature key pair $(\mathsf{VK}, \mathsf{SK}) \leftarrow \mathcal{G}(\lambda)$ and do the following.

1. Using $\{(z_j, r_j, u_j)\}_{j=1}^{t}$, derive a one-time linearly homomorphic signature (z, r, u) on $\mathbf{v}$. Namely, compute $z = \prod_{i=1}^{t} z_i^{x_i}$, $r = \prod_{i=1}^{t} r_i^{x_i}$ and $u = \prod_{i=1}^{t} u_i^{x_i}$.
2. Using $\mathsf{VK} = \mathsf{VK}[1] \ldots \mathsf{VK}[L] \in \{0,1\}^L$, define the vector $\mathbf{f}_{\mathsf{VK}} = \mathbf{f}_{3,0} \cdot \prod_{i=1}^{L} \mathbf{f}_{3,i}^{\mathsf{VK}[i]}$ and assemble a Groth-Sahai CRS $\mathbf{f}_{\mathsf{VK}} = (\mathbf{f}_1, \mathbf{f}_2, \mathbf{f}_{\mathsf{VK}})$. Using $\mathbf{f}_{\mathsf{VK}}$, generate commitments $\mathbf{C}_z$, $\mathbf{C}_r$, $\mathbf{C}_u$ to the components of $(z, r, u) \in \mathbb{G}^3$ along with NIWI proofs $(\boldsymbol{\pi}_1, \boldsymbol{\pi}_2)$ that $\mathbf{v}$ and (z, r, u) satisfy (3.1). Let $(\mathbf{C}_z, \mathbf{C}_r, \mathbf{C}_u, \boldsymbol{\pi}_1, \boldsymbol{\pi}_2) \in \mathbb{G}^{15}$ be the resulting commitments and proofs.
3. Generate $\sigma = \mathcal{S}(\mathsf{SK}, (\mathbf{v}, \mathbf{C}_z, \mathbf{C}_r, \mathbf{C}_u, \boldsymbol{\pi}_1, \boldsymbol{\pi}_2, \mathsf{lbl}))$ and output

$$\pi = (\mathsf{VK}, \mathbf{C}_z, \mathbf{C}_r, \mathbf{C}_u, \boldsymbol{\pi}_1, \boldsymbol{\pi}_2, \sigma) \tag{3.8}$$

$\mathsf{V}(\Gamma, \psi, \mathbf{v}, \pi, \mathsf{lbl})$**:** parse π as per (3.8) and $\mathbf{v}$ as $(v_1, \ldots, v_n) \in \mathbb{G}^n$. Return 1 if and only if

(i) $\mathcal{V}(\mathsf{VK}, (\mathbf{v}, \mathbf{C}_z, \mathbf{C}_r, \mathbf{C}_u, \boldsymbol{\pi}_1, \boldsymbol{\pi}_2, \mathsf{lbl}), \sigma) = 1$;

(ii) $(\mathbf{C}_z, \mathbf{C}_r, \mathbf{C}_u, \boldsymbol{\pi}_1, \boldsymbol{\pi}_2)$ forms a valid NIWI proof for the CRS $\mathbf{f}_{\mathsf{VK}} = (\mathbf{f}_1, \mathbf{f}_2, \mathbf{f}_{\mathsf{VK}})$, so that $\boldsymbol{\pi}_1 = (\pi_{1,1}, \pi_{1,2}, \pi_{1,3})$ and $\boldsymbol{\pi}_2 = (\pi_{2,1}, \pi_{2,2}, \pi_{2,3})$ satisfy

$$\prod_{i=1}^{n} E\big(g_i, (1_{\mathbb{G}}, 1_{\mathbb{G}}, v_i)\big)^{-1} = E\big(g_z, \mathbf{C}_z\big) \cdot E\big(g_r, \mathbf{C}_r\big) \cdot E(\pi_{1,1}, \mathbf{f}_1) \cdot E(\pi_{1,2}, \mathbf{f}_2) \cdot E(\pi_{1,3}, \mathbf{f}_{\mathsf{VK}})$$

$$\prod_{i=1}^{n} E\big(h_i, (1_{\mathbb{G}}, 1_{\mathbb{G}}, v_i)\big)^{-1} = E\big(h_z, \mathbf{C}_z\big) \cdot E\big(h, \mathbf{C}_u\big) \cdot E(\pi_{2,1}, \mathbf{f}_1) \cdot E(\pi_{2,2}, \mathbf{f}_2) \cdot E(\pi_{2,3}, \mathbf{f}_{\mathsf{VK}}).$$

To simulate a proof for a given vector $\mathbf{v} \in \mathbb{G}^n$, the simulator uses $\tau_{sim} = \mathsf{sk}_{hsps}$ to generate a fresh one-time homomorphic signature on $\mathbf{v} \in \mathbb{G}^n$ and proceeds as in steps 2-3 of P.

The proof π only consists of 15 group elements and a one-time pair (VK, σ). Remarkably, its length does not depend on the number of equations n or the number of variables t. In comparison, Groth-Sahai proofs already require $3t + 2n$ group elements in their basic form and become even more expensive when it comes to achieve unbounded simulation-soundness. The Jutla-Roy techniques [151] reduce the proof length to $2(n - t)$ elements – which only competes with our proofs when $t \approx n$ – but it is unclear how to extend them to get unbounded simulation-soundness without affecting their efficiency. Our CRS consists of $O(t + n + L)$ group elements against $O(t(n - t))$ in [151]. More detailed comparisons are given in Section 3.4.3 between proof systems based on the DLIN assumption.

Interestingly, the above scheme even outperforms Fiat-Shamir-like proofs derived from Σ-protocols which would give $\Theta(t)$-size proofs here. The construction readily extends to rely on the k-linear assumption for $k > 2$. In this case, the proof comprises $(k + 1)(2k + 1)$ elements and its size thus only depends on k, as detailed in the full version of [178].

Moreover, the verification algorithm only involves *linear* pairing product equations whereas all known unbounded simulation-sound extensions of Groth-Sahai proofs require either quadratic equations or a linearization step involving extra variables.

We finally remark that, if we give up the simulation-soundness property, the proof length drops to $k+1$ group elements under the k-linear assumption.

Theorem 7 ([178]). *The scheme is an unbounded simulation-sound QA-NIZK proof system if the DLIN assumption holds in* $\mathbb{G}$ *and* Σ *is strongly unforgeable.*

The above construction is not tightly secure as the gap between the simulation-soundness adversary's advantage and the probability to break the DLIN assumption depends on the number of simulated proofs obtained by the adversary. For applications like tight CCA2 security [142], it would be interesting to modify the proof system to obtain tight security.

3.4.2 Construction with (Single-Theorem) Relative Soundness

In applications where single-theorem relatively sound NIZK proofs suffice, we can further improve the efficiency. Under the k-linear assumption, the proof length reduces from $O(k^2)$ elements to $O(k)$ elements. Under the DLIN assumption, each proof fits within 4 elements and only costs $2n+6$ pairings to verify. In comparison, the verifier needs $2(n-t)(t+2)$ pairing evaluations in [151].

As in [150], we achieve relative soundness using smooth projective hash functions [90]. To this end, we need to encode the matrix $\rho \in \mathbb{G}^{t\times n}$ as a $2t \times (2n+1)$ matrix.

$\mathbb{K}_0(\lambda)$**:** choose symmetric bilinear groups $(\mathbb{G}, \mathbb{G}_T)$ of prime order $p > 2^\lambda$ with $g \xleftarrow{\$} \mathbb{G}$. Then, output $\Gamma = (\mathbb{G}, \mathbb{G}_T, g)$.

Again, the dimensions of $\mathbf{A} \in \mathbb{Z}_p^{t\times n}$ can be either fixed or part of $\mathcal{L}_\rho$, so that t, n can be given as input to the CRS generation algorithm $\mathbb{K}_1$.

$\mathbb{K}_1(\Gamma, \rho)$**:** parse Γ as $(\mathbb{G}, \mathbb{G}_T, g)$ and ρ as $\rho = \big(G_{ij}\big)_{1\leq i\leq t,\, 1\leq j\leq n} \in \mathbb{G}^{t\times n}$ and do the following.

1. Choose two n-vectors $\mathbf{d} = (d_1, \ldots, d_n) \xleftarrow{\$} \mathbb{Z}_p^n$ and $\mathbf{e} = (e_1, \ldots, e_n) \xleftarrow{\$} \mathbb{Z}_p^n$ in order to define $\mathbf{W} = (W_1, \ldots, W_t) = g^{\mathbf{A}\cdot\mathbf{d}^\top} \in \mathbb{G}^t$ and $\mathbf{Y} = (Y_1, \ldots, Y_t) = g^{\mathbf{A}\cdot\mathbf{e}^\top} \in \mathbb{G}^t$. These will be used to define a projective hash function.
2. Generate a key pair $(\mathsf{pk}_{ots}, \mathsf{sk}_{ots})$ for the one-time linearly homomorphic signature of Section 3.2.1 in order to sign vectors in $\mathbb{G}^{2n+1}$. Let the public key be
$$\mathsf{pk}_{ots} = \big((\mathbb{G}, \mathbb{G}_T), g_z, g_r, h_z, h_u, \{(g_i, h_i)\}_{i=1}^{2n+1}\big)$$
and let $\mathsf{sk}_{ots} = \{(\chi_i, \gamma_i, \delta_i)\}_{i=1}^{2n+1}$ be the corresponding private key.
3. Use sk_{ots} to generate one-time homomorphic signatures $\{(z_i, r_i, u_i)\}_{i=1}^{2t}$ on the vectors below, which are obtained from the rows of the matrix $\rho = \big(G_{i,j}\big)_{1\leq i\leq t,\, 1\leq j\leq n}$.
$$\begin{aligned} \mathbf{H}_{2i-1} &= (G_{i,1}, \ldots, G_{i,n}, Y_i, 1, \ldots, 1) \in \mathbb{G}^{2n+1} && i \in \{1, \ldots, t\} \\ \mathbf{H}_{2i} &= (1, \ldots, 1, W_i, G_{i,1}, \ldots, G_{i,n}) \in \mathbb{G}^{2n+1} \end{aligned}$$
4. Choose a collision-resistant hash function $H : \{0,1\}^* \to \mathbb{Z}_p$.

5. The CRS ψ consists of a first part $\mathbf{CRS}_1$ that is only used by the prover and a second part $\mathbf{CRS}_2$ which is only used by the verifier. These are defined as

$$\mathbf{CRS}_1 = \Big(\rho,\ \mathsf{pk}_{ots},\ \mathbf{W},\ \mathbf{Y},\ \{(z_i, r_i, u_i)\}_{i=1}^{2t},\ H\Big), \qquad \mathbf{CRS}_2 = \Big(\mathsf{pk}_{ots},\ \mathbf{W},\ \mathbf{Y},\ H\Big).$$

The simulation trapdoor τ_{sim} is sk_{ots} and the private verification trapdoor consists of $\tau_v = \{\mathbf{d}, \mathbf{e}\}$.

$\mathsf{P}(\Gamma, \psi, \mathbf{v}, x, \mathsf{lbl})$**:** given a candidate vector $\mathbf{v} \in \mathbb{G}^n$, a witness $\mathbf{x} = (x_1, \ldots, x_t) \in \mathbb{Z}_p^t$ such that $\mathbf{v} = g^{\mathbf{x}\cdot\mathbf{A}}$ and a label lbl, compute $\alpha = H(\rho, \mathbf{v}, \mathsf{lbl}) \in \mathbb{Z}_p$. Using $\{(z_i, r_i, u_i)\}_{i=1}^{2t}$, derive a one-time homomorphic signature (z, r, u) on $\tilde{\mathbf{v}} = \big(v_1, \ldots, v_n, \pi_0, v_1^{\alpha}, \ldots, v_n^{\alpha}\big) \in \mathbb{G}^{2n+1}$, where $\pi_0 = \prod_{i=1}^{t}(W_i^{\alpha} Y_i)^{x_i}$. Namely, compute and output $\pi = (z, r, u, \pi_0) \in \mathbb{G}^4$, where

$$z = \prod_{i=1}^{t}(z_{2i-1} \cdot z_{2i}^{\alpha})^{x_i}, \quad r = \prod_{i=1}^{t}(r_{2i-1} \cdot r_{2i}^{\alpha})^{x_i}, \quad u = \prod_{i=1}^{t}(u_{2i-1} \cdot u_{2i}^{\alpha})^{x_i}, \quad \pi_0 = \prod_{i=1}^{t}(W_i^{\alpha} Y_i)^{x_i}$$

$\mathsf{V}(\Gamma, \psi, \mathbf{v}, \pi, \mathsf{lbl})$**:** parse the vector $\mathbf{v}$ as $(v_1, \ldots, v_n) \in \mathbb{G}^n$ and π as $(z, r, u, \pi_0) \in \mathbb{G}^4$. Compute $\alpha = H(\rho, \mathbf{v}, \mathsf{lbl})$ and return 1 if and only if the triple (z, r, u) is a valid signature on the vector $\tilde{\mathbf{v}} = (v_1, \ldots, v_n, \pi_0, v_1^{\alpha}, \ldots, v_n^{\alpha}) \in \mathbb{G}^{2n+1}$. Namely, it should satisfy the equalities

$$\begin{aligned} 1_{\mathbb{G}_T} &= e(g_z, z) \cdot e(g_r, r) \cdot \prod_{i=1}^{n} e(g_i \cdot g_{i+n+1}^{\alpha}, v_i) \cdot e(g_{n+1}, \pi_0) \\ 1_{\mathbb{G}_T} &= e(h_z, z) \cdot e(h_u, u) \cdot \prod_{i=1}^{n} e(h_i \cdot h_{i+n+1}^{\alpha}, v_i) \cdot e(h_{n+1}, \pi_0). \end{aligned} \tag{3.9}$$

$\mathsf{W}(\Gamma, \psi, \tau_v, \mathbf{v}, \pi, \mathsf{lbl})$**:** given a vector $\mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{G}^n$, parse π as $(z, r, u, \pi_0) \in \mathbb{G}^4$ and τ_v as $\{\mathbf{d}, \mathbf{e}\}$, with $\mathbf{d} = (d_1, \ldots, d_n) \in \mathbb{Z}_p^n$ and $\mathbf{e} = (e_1, \ldots, e_n) \in \mathbb{Z}_p^n$. Compute $\alpha = H(\rho, \mathbf{v}, \mathsf{lbl}) \in \mathbb{Z}_p$ and return 0 if the public verification test V fails. Otherwise, return 1 if $\pi_0 = \prod_{j=1}^{n} v_j^{e_j + \alpha d_j}$ and 0 otherwise.

We note that, while the proving algorithm is deterministic, each statement has many valid proofs. However, finding two valid proofs for the same statement is computationally hard, as we proved in [178].

The scheme readily extends to rest on the k-linear assumption with $k > 2$. In this case, the proof requires $k + 2$ group elements – whereas combining the techniques of [150, 151] demands $k(n + 1 - t)$ elements per proof – and a CRS of size $O(k(n + t))$. Subsequently to our work [178], Jutla and Roy [153] and Abdalla, Ben Hamouda and Pointcheval [1] gave different constructions of one-time relatively-sound or simulation-sound QA-NIZK proofs made of only 3 group elements under the DLIN assumption.

Theorem 8 ([178])**.** *The above proof system is a relatively sound QA-NIZK proof system if the SDP assumption holds in* $(\mathbb{G}, \mathbb{G}_T)$ *and if* H *is a collision-resistant hash function.*

As an application, we showed in the full version of [178] how the DLIN-based version [235] of the Cramer-Shoup cryptosystem [88, 90] can be made publicly verifiable (meaning that well-formed ciphertext are recognizable given only the public key) by introducing only three group elements in the ciphertext. In the threshold setting, the resulting system

can be distributed – without interaction during the decryption process – and proved secure against adaptive corruptions. As a result, we obtained [178] a new adaptively secure CCA2-secure *non-interactive* threshold cryptosystem based on the DLIN assumption with ciphertexts comprised of only 8 group elements. In comparison with the best previous variants [150, 151] of Cramer-Shoup with publicly verifiable ciphertexts, we thus spare one group element per ciphertext. If we compare our construction [178, Appendix I] with the first adaptively secure non-interactive threshold version of Cramer-Shoup [189], we shorten ciphertexts by 60%. The recent results of Jutla and Roy [153] yield further optimizations, which allow for ciphertexts made of 7 group elements under the DLIN assumptions (and even 5 group elements under the SXDH assumption).

Under the k-linear assumption, the scheme provides ciphertexts that are $\Theta(k)$ group elements shorter than in previous such constructions.

3.4.3 Comparisons

This section compares the various NIZK proofs of linear subspace membership based on the DLIN assumption. Comparisons are given in terms of CRS size, proof size and the number of pairing evaluations for the verifier.

In the table, we consider our basic proof system (without any form of simulation-soundness, where each proof is a one-time linearly homomorphic signature (z, r, u)), its unbounded simulation-sound variant and the relatively simulation-sound variant of Section 3.4.2. We compare these with the original Groth-Sahai proofs, their most efficient unbounded simulation-sound extensions due to Camenisch *et al.* [62] and the Jutla-Roy techniques [151, 153] with and without relative soundness.

Table 3.1: Comparison between proof systems for linear subspaces

Proof systems	CRS size$^{\diamondsuit}$ *	Proof length$^{\diamondsuit}$	# of pairings† at verification
Groth-Sahai [138]	6	$3t + 2n$	$3n(t+3)$
Jutla-Roy [151]	$4t(n-t)+3$	$2(n-t)$	2(n-t)(t+2)
Jutla-Roy RSS [151] + [150]	$4t(n+1-t)+3$	$2(n+1-t)+1$	$2(n+1-t)(t+2)$
Groth-Sahai USS [62]	18	$6t + 2n + 52^{\ddagger}$	$O(tn)$
Our basic QA-NIZK proofs	$2n + 3t + 4$	3	$2n + 4$
Our RSS QA-NIZK proofs	$4n + 8t + 6$	4	$2n + 6$
Our USS QA-NIZK proofs	$2n + 3t + 3L + 10$	$20^{\ddagger}$	$2n + 30$
Jutla-Roy [153]	$O(t+n)$	2	$2n + 4$
Jutla-Roy RSS [151] + [153]	$O(t+n)$	3	$2n + 4$
Abdalla *et al.*, one-time SS [1]	$O(t+n)$	3	$2n + 4$

n: number of equations; t: number of variables; L: length of a hashed one-time verification key

$\diamondsuit$ These sizes are measured in terms of number of group elements.
$*$ The description $\rho \in \mathrm{G}^{t \times n}$ of the language is not counted as being part of the CRS here.
† The table does not consider optimizations using randomized batch verification techniques here.
‡ We consider instantiations using Groth's one-time signature [133], where verification keys and signatures consist of 3 group elements and two elements of $\mathbb{Z}_p$, respectively.

As can be observed in the table, our constructions all yield constant-size arguments. Moreover, the number of pairing evaluations is always independent of the number of variables t, which substantially fastens the verification process when $t \approx n/2$. The last three rows of the table consider the results that were subsequent to ours, including the implications of the techniques of Jutla and Roy [153] who independently proposed a different construction of constant-size QA-NIZK proofs of linear subspace membership. While their construction of [153] does not provide simulation-soundness, it can be combined with earlier results [150] so as to obtain a (one-time) relatively sound proof system with only 3 group elements per proof. It is unclear how to extend it into an unbounded simulation-sound proof system and the same holds for the construction of [1].

We also note that randomized batch verification techniques can be used to drastically reduce the number of pairing computations. In our USS system, for example, the number of pairings drops to $n + 18$ if the two verification equations are processed together and further optimizations are possible.

Our common reference strings always fit within $O(t + n)$ group elements (with another $O(L)$ elements in the USS variant) and thus provide significant savings w.r.t. [151] when $t \approx n/2$.

3.5 Conclusion

We gave new and somewhat unexpected applications of structure-preserving signatures in the construction of non-malleable cryptographic primitives like non-interactive non-malleable commitments, simulation-sound QA-NIZK proofs and chosen-ciphertext-secure public-key encryption. Paradoxically, these applications were made possible by first rendering structure-preserving signatures homomorphic (and thus malleable).

Beyond their applications to non-malleability, our LHSPS primitive is powerful enough to provide very simple realizations of constant-size QA-NIZK proofs of linear subspace membership. In fact, it is not hard to see that any one-time LHSPS system can be generically used to build such a QA-NIZK proof system. Moreover, the specific algebraic properties of our constructions made it possible to tweak them so as to obtain unbounded simulation-soundness without sacrificing the constant proof size. Via the technique of Malkin *et al.* [196], it is actually possible to combine the Groth-Sahai NIZK proofs with any LHSPS systems so as to build an USS QA-NIZK argument of subspace membership: the QA-NIZK proof can consist of a NIZK proof of knowledge of a linearly homomorphic signature. However, due to the use of Groth-Sahai NIZK proofs for pairing product equations, the resulting QA-NIZK proofs would not necessarily be of constant size. The constant proof length of our construction stems from the specific structure of the scheme which, via suitable information theoretic arguments in the security proof, allows us to only require NIWI (rather than NIZK) proofs of knowledge for pairing product equations.

Our constant-size QA-NIZK arguments recently allowed us [175] to improve upon the results of Chen and Wee [86], who gave signature schemes with almost tight security – meaning that the security loss only depends on the security parameter and not on the number of signing queries made by the adversary – under the K-linear assumption. Under the DLIN assumption, our construction allows reducing the signature length from 8 to 6 group elements. Our signature scheme [175] crucially relies on the fact that the size of proofs does not depend of the dimension of the considered subspace. It can be generalized to use any QA-NIZK ar-

gument of linear subspace membership. Hence, if the improved Jutla-Roy construction [153] is plugged into the high-level construction of [175], the signature length reduces to 5 group elements under the DLIN assumption and 3 elements under the SXDH assumption. The QA-NIZK proofs of [153] thus provide our construction with as short signatures as those of Blazy, Kiltz and Pan [36] with the benefit of shorter private keys.

Finally, together with Marc Joye and Moti Yung [174], we used our LHSPS systems to design (albeit in a non-generic manner) fully distributed non-interactive adaptively secure threshold signatures with round-optimal key generation. We expect our LHSPS primitive to find other applications in the future. For example, Catalano, Marcedone and Puglisi [79] recently used them to devise linearly homomorphic signatures which can operate in online/offline mode [106], by allowing expensive public-key operations to take place before the data to be signed is available.

Conclusion and Perspectives

Summary of Results

This manuscript highlighted the importance of structure-preserving cryptographic primitives and pairing-based non-interactive proof systems. Several applications were described with a focus on privacy-enhancing cryptographic techniques, like group encryption and group signatures, and non-malleable non-interactive primitives which include non-malleable commitments, simulation-sound QA-NIZK arguments of linear subspace membership and CCA2-secure encryption schemes.

Our contributions in the context of anonymity-related cryptography included the first efficient realization of the structure-preserving signature primitive suggested for the first time by Groth [133] in 2006. As an application of the more efficient SPS schemes proposed by Abe *et al.* [6, 4], we gave a novel and efficient solution to the venerable problem of conveniently revoking users in group signatures. Our most efficient revocable group signature [179] suitably combines structure-preserving signatures with other ingredients like the NNL Subset Cover [205] framework for broadcast encryption and the concise vector commitment scheme proposed by Moti Yung and myself in 2010 [188].

Surprisingly, the applications of structure-preserving signatures to non-malleability were made possible by first tweaking certain existing SPS schemes [6] so as to obtain linearly homomorphic (and thus malleable) structure-preserving signatures. Our construction of non-interactive non-malleable commitment to group elements is completely generic and can be based on any LHSPS realization. In their basic version (i.e., without the simulation-soundness property), our QA-NIZK arguments can also generically rely on any LHSPS scheme. In order to achieve unbounded simulation-soundness, our construction is no longer generic since its security proof relies on information-theoretic arguments which are specific to our concrete homomorphic LHSPS system.

Our results showed that structure-preserving signatures with homomorphic properties are a powerful primitive with unexpected applications. In a recent result [175], we also used them to design a more efficient variant of the Chen-Wee [86] signatures with a nearly tight security proof under the DLIN assumption (a similar result was independently obtained by Blazy *et al.* [36]). By applying techniques suggested in [192, 133, 3], we also obtained a more efficient construction of CCA2-secure public-key encryption scheme in the multi-challenge, multi-user setting[5] [30, 142]. In comparison with the best known construction with tight

[5] As shown in [30], the multi-user, multi-challenge CCA2 security of a cryptosystem is implied by its security in the single-user, single-challenge setting. However, the reduction is linearly affected by the number of users and the number of challenge ciphertexts per user. Tight multi-user, multi-challenge CCA2 security is thus generally non-trivial to prove.

multi-challenge CCA2 security [3], our technique reduces the ciphertext length from 398 to 69 group elements under the DLIN assumption. Together with Marc Joye and Moti Yung [174], we further used our specific one-time LHSPS scheme of Section 3.2.1 to build fully distributed non-interactive adaptively secure threshold signatures. We provide two optimally-resilient constructions – namely, one in the random oracle model and a slightly less efficient one in the standard model – with a one-round distributed key generation protocol in the erasure-free setting (meaning that the servers are not assumed to reliably erase all intermediate computation results in order to ensure security). To our knowledge, our constructions are the first non-interactive adaptively secure threshold signatures to simultaneously feature all these useful properties.

Directions for Future Work

Attribute-Based Encryption from QA-NIZK Proofs

We believe that other applications of linearly homomorphic structure-preserving signatures have not been explored yet. For example, they allowed us devise an ordinary digital signature scheme with a nearly tight reduction from a simple assumption in the standard model [175]. While, at first glance, this signature scheme appears amenable to constructing an identity-based encryption system (via the standard technique, notably used in [36], of randomizing the verification algorithm), we did not manage to formally prove it. In fact, while Jutla and Roy managed to construct a fully secure IBE system from their QA-NIZK arguments [151, Appendix H] via the dual system paradigm [249], we have not been able to build an IBE from our LHSPS schemes yet. One of my future objectives will be to fill this gap and further extend the realm of applications of the LHSPS primitive.

More generally, it will be interesting to determine the exact extent to which QA-NIZK proofs can be used to implement the dual system encryption paradigm [249, 171]. Jutla and Roy [151] used them in a non-generic way to build a very efficient IBE scheme with full security (as opposed to selective security [40]) under the SXDH assumption in prime order groups. Related results were obtained by Blazy *et al.* [36] via a more generic approach. However, both articles [151, 36] focus on the (hierarchical) IBE setting and it is unclear how to apply their techniques to get full security in attribute-based encryption [232, 132]. One of my upcoming goals will be to obtain a framework for building fully secure[6] attribute-based encryption schemes (in prime order groups) from QA-NIZK proofs by extending the dual system encryption method [249] in the same way as in [169, 215]. Ideally, the new framework should use QA-NIZK proofs so as to translate the techniques of Attrapadung [19] from composite order groups to prime order groups. This should notably provide us with fully secure unbounded attribute-based encryption systems for large universes [172, 228] and online/offline efficiency in prime order groups. Finally, extensions of the framework will be considered in order to use QA-NIZK proofs so as to build attribute-hiding functional encryption schemes (like inner product encryption [154]. In summary, my hope is to use QA-NIZK proofs in order to improve upon existing frameworks [170, 215, 87] for building fully secure IBE and related primitives [50] in prime order groups.

[6] Full security, as opposed to selective security [40], refers to the strongest security notion where the aversary can choose the attribute set of the challenge ciphertext in the challenge phase.

Better Constructions of Functional Encryption from Different Assumptions

In recent years, a renewed attention has been paid to lattice-based cryptography. Breakthrough results [122] showed how to safely implement efficient lattice-based signatures and identity-based encryption. It is even possible [74, 9] to construct hierarchical identity-based encryption (HIBE) schemes [123]. Despite certain improvements [10], currently available lattice-based HIBE schemes still have ciphertexts and private keys whose lengths depend on the depth of the hierarchy. The reason is that the latter always affects the dimension of underlying lattices in a way or another. In contrast, the world of bilinear maps allows HIBE schemes [43] with ciphertexts of constant size: their length only depends on the security parameter and not on the number of levels in the hierarchy or the depth of the receiver.

In the setting of an ongoing project on functional encryption, I am planning to investigate whether the aforementioned overhead is inherent to lattice-based cryptography. Should the answer be negative, I hope for a lattice-based analogue of [43] and aim at designing HIBE schemes with constant-size ciphertexts. This achievement would notably imply lattice-based forward-secure public-key encryption schemes with ciphertexts of constant (i.e, independent of the number of time periods) size and also open the way to lattice-based broadcast encryption with short ciphertexts. This would solve yet another challenging open problem as, for the time being, all broadcast encryption systems with short ciphertexts and private keys rely on ad hoc assumptions. In particular, we do not have a realization based on the standard learning-with-errors (LWE) assumption [227], let alone with adaptive security [124].

Another limitation of all known adaptively-secure lattice-based HIBE schemes [74, 9, 10] is that hierarchies are restricted to have a constant and small number of levels: indeed, a polynomial number of levels would translate into a non-polynomial reduction (and thus fail to provide any security guarantee) as the security bound exponentially declines with the number of levels. In order to sidestep the latter limitation, I thus hope to adapt suitable techniques from pairing-based cryptography [249] in the setting of lattices and obtain HIBE schemes supporting a polynomial number of levels with a polynomial reduction in their security proof. Ideally, I would like to obtain a fully secure lattice-based HIBE scheme (in the standard model) where the number of levels in the hierarchy does not need to be fixed when the system is set up. While such HIBE systems exist under discrete-logarithm-related assumptions [172], they remain elusive in the lattice world so far. It would also be interesting to extend those results so as to obtain full security in generalizations of (H)IBE such as attribute-based and functional encryption [50]. For the time being, we do not have a fully secure attribute-based encryption scheme based on standard lattice assumptions.

Efficient QA-NIZK Proofs for Lattice Problems

The quasi-adaptive setting [151] made it possible to improve upon the efficiency of existing NIZK proof systems in the standard model [151, 153, 178] for the specific language of linear subspaces in vector spaces spanned by vectors of group elements. An interesting open question is whether QA-NIZK proofs can be more efficiently obtained than regular NIZK proofs for specific problems involving lattices.

For example, given a random matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ defined over a prime modulus q and where $m = O(n \log q)$, it would be interesting to have QA-NIZK proofs for the LWE language $\mathcal{L} = \{\mathbf{v} \in \mathbb{Z}_q^m \mid \mathbf{v} = \mathbf{A} \cdot \mathbf{s} + \mathbf{e},\ \mathbf{s} \in \mathbb{Z}_q^n\}$, where $\mathbf{e} \in \mathbb{Z}^m$ is a small-norm noise vector. This problem can be seen as a "subspace closeness" problem rather than a subspace

membership problem: instead of putting the entries of $\mathbf{A}$ and $\mathbf{v}$ in the exponent, one adds a noise to the entries of $\mathbf{v}$. Unfortunately, our techniques of building QA-NIZK proofs from homomorphic signatures (described in Section 3.4) do not seem to carry over here. In particular, it seems difficult to apply them to the Boneh-Freeman linearly homomorphic signatures [47, 46]. The main difficulty is seemingly to guarantee the NIZK property while handling vectors of integers rather than vectors of group elements.

Solving this problem would help fill important gaps in lattice-based cryptography since, even in the random oracle model, efficient non-interactive zero-knowledge proof systems are only available for specific languages [200, 194, 146, 193, 141] so far. In the standard model, the best constructions we are aware of are those of Peikert and Vaikuntanathan [218], which are not known to apply to the LWE language. In the future, I am thus hoping to take steps towards filling this gap.

Bibliography

[1] M. Abdalla, F. Ben Hamouda, and D. Pointcheval. Disjunctions for hash proof systems: New constructions and applications. *Cryptology ePrint Archive: Report 2014/483*, 2014.

[2] M. Abe, M. Chase, B. David, M. Kohlweiss, R. Nishimaki, and M. Ohkubo. Constant-size structure-preserving signatures: Generic constructions and simple assumptions. In Wang and Sako [247], pages 4–24.

[3] M. Abe, B. David, M. Kohlweiss, R. Nishimaki, and M. Ohkubo. Tagged one-time signatures: Tight security and optimal tag size. In Kurosawa and Hanaoka [165], pages 312–331.

[4] M. Abe, G. Fuchsbauer, J. Groth, K. Haralambiev, and M Ohkubo. Structure-preserving signatures and commitments to group elements. In Tal Rabin, editor, *Advances in Cryptology - CRYPTO 2010*, volume 6223 of *LNCS*, pages 209–236. Springer, 2010.

[5] M. Abe, J. Groth, K. Haralambiev, and M. Ohkubo. Optimal structure-preserving signatures in asymmetric bilinear groups. In Phillip Rogaway, editor, *CRYPTO*, volume 6841 of *Lecture Notes in Computer Science*, pages 649–666. Springer, 2011.

[6] M. Abe, K. Haralambiev, and M. Ohkubo. Signing on elements in bilinear groups for modular protocol design. *IACR Cryptology ePrint Archive*, 2010:133, 2010.

[7] M. Abe, K. Haralambiev, and M. Ohkubo. Group to group commitments do not shrink. In Pointcheval and Johansson [220], pages 301–317.

[8] T. Acar and L. Nguyen. Revocation for delegatable anonymous credentials. In Catalano et al. [80], pages 423–440.

[9] S. Agrawal, D. Boneh, and X. Boyen. Efficient lattice (H)IBE in the standard model. In *EUROCRYPT*, pages 553–572, 2010.

[10] S. Agrawal, D. Boneh, and X. Boyen. Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE. In *CRYPTO*, 2010.

[11] J. Ahn, D. Boneh, J. Camenisch, S. Hohenberger, A. Shelat, and B. Waters. Computing on authenticated data. In Cramer [92], pages 1–20.

[12] J. An, Y. Dodis, and T. Rabin. On the security of join signature and encryption. In Knudsen [161], pages 83–107.

[13] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song. Provable data possession at untrusted stores. In Ning et al. [212], pages 598–609.

[14] G. Ateniese, J. Camenisch, S. Hohenberger, and B. de Medeiros. Practical group signatures without random oracles. *IACR Cryptology ePrint Archive*, 2005:385, 2005.

[15] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik. A practical and provably secure coalition-resistant group signature scheme. In *CRYPTO'00*, pages 255–270, 2000.

[16] G. Ateniese, S. Kamara, and J. Katz. Proofs of storage from homomorphic identification protocols. In Matsui [197], pages 319–333.

[17] G. Ateniese, D. Song, and G. Tsudik. Quasi-efficient revocation in group signatures. In *Financial Cryptography*, pages 183–197, 2002.

[18] Vijayalakshmi Atluri, Birgit Pfitzmann, and Patrick Drew McDaniel, editors. *Proceedings of the 11th ACM Conference on Computer and Communications Security, CCS 2004, Washington, DC, USA, October 25-29, 2004*. ACM, 2004.

[19] N. Attrapadung. Dual system encryption via doubly selective security: Framework, fully secure functional encryption for regular languages, and more. In Nguyen and Oswald [211], pages 557–577.

[20] N. Attrapadung, K. Emura, G. Hanaoka, and Y. Sakai. A revocable group signature scheme from identity-based revocation techniques: Achieving constant-size revocation list. In *Applied Cryptography and Network Security (ACNS'14)*, pages 419–437, 2014.

[21] N. Attrapadung, F. Laguillaumie, J. Herranz, B. Libert, E. de Panafieu, and C. Ràfols. Attribute-based encryption schemes with constant-size ciphertexts. *Theoretical Computer Science*, (422):15–38, 2012.

[22] N. Attrapadung and B. Libert. Functional encryption for inner product: Achieving constant-size ciphertexts with adaptive security or support for negation. In *Public Key Cryptography*, pages 384–402, 2010.

[23] N. Attrapadung and B. Libert. Homomorphic network coding signatures in the standard model. In Catalano et al. [80], pages 17–34.

[24] N. Attrapadung, B. Libert, and E. de Panafieu. Expressive key policy attribute-based encryption with constant-size ciphertexts. In *Public Key Cryptography*, pages 90–108, 2011.

[25] N. Attrapadung, B. Libert, and T. Peters. Computing on authenticated data: New privacy definitions and constructions. In Wang and Sako [247], pages 367–385.

[26] N. Attrapadung, B. Libert, and T. Peters. Efficient completely context-hiding quotable and linearly homomorphic signatures. In Kurosawa and Hanaoka [165], pages 386–404.

[27] P. Barreto, B. Libert, N. McCullagh, and J.-J. Quisquater. Efficient and provably secure identity-based signatures and signcryption from bilinear maps. In *ASIACRYPT*, pages 515–532, 2005.

[28] M. Belenkiy, J. Camenisch, M. Chase, M. Kohlweiss, A. Lysyanskaya, and H. Shacham. Randomizable proofs and delegatable anonymous credentials. In Halevi [139], pages 108–125.

[29] M. Belenkiy, M. Chase, M. Kohlweiss, and A. Lysyanskaya. P-signatures and noninteractive anonymous credentials. In Ran Canetti, editor, *TCC*, volume 4948 of *Lecture Notes in Computer Science*, pages 356–374. Springer, 2008.

[30] M. Bellare, A. Boldyreva, and S. Micali. Public-key encryption in a multi-user setting: Security proofs and improvements. In *EUROCRYPT*, pages 259–274, 2000.

[31] M. Bellare, D. Micciancio, and B. Warinschi. Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions. In *EUROCRYPT 2003*, volume 2656 of *LNCS*, pages 614–629. Springer, 2003.

[32] M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In Dorothy E. Denning, Raymond Pyle, Ravi Ganesan, Ravi S. Sandhu, and Victoria Ashby, editors, *ACM Conference on Computer and Communications Security*, pages 62–73. ACM, 1993.

[33] M. Bellare, H. Shi, and C. Zhang. Foundations of group signatures: The case of dynamic groups. In *CT-RSA 2005*, volume 3376 of *LNCS*, pages 136–153. Springer, 2005.

[34] J. Benaloh and M. de Mare. One-way accumulators: A decentralized alternative to digital sinatures (extended abstract). In *EUROCRYPT*, pages 274–285, 1993.

[35] M. Blaze, G. Bleumer, and M. Strauss. Divertible protocols and atomic proxy cryptography. In *EUROCRYPT*, pages 127–144, 1998.

[36] O. Blazy, E. Kiltz, and J. Pan. (hierarchical) identity-based encryption from affine message authentication. In *CRYPTO*, 2014.

[37] M. Blum, A. de Santis, S. Micali, and G. Persiano. Noninteractive zero-knowledge. *SIAM J. Comput.*, 20(6):1084–1118, 1991.

[38] M. Blum, P. Feldman, and S. Micali. Non-interactive zero-knowledge and its applications (extended abstract). In *STOC*, pages 103–112. ACM, 1988.

[39] A. Boldyreva, M. Fischlin, A. Palacio, and B. Warinschi. A closer look at PKI: Security and efficiency. In Catalano et al. [80], pages 458–475.

[40] D. Boneh and X. Boyen. Efficient selective-ID secure identity-based encryption without random oracles. In Cachin and Camenisch [60], pages 223–238.

[41] D. Boneh and X. Boyen. Short signatures without random oracles. In Cachin and Camenisch [60], pages 56–73.

[42] D. Boneh and X. Boyen. Short signatures without random oracles and the SDH assumption in bilinear groups. *J. Cryptology*, 21(2):149–177, 2008.

[43] D. Boneh, X. Boyen, and E. Goh. Hierarchical identity based encryption with constant size ciphertext. In Cramer [91], pages 440–456.

[44] D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In Franklin [110], pages 41–55.

[45] D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. In Kilian [159], pages 213–229.

[46] D. Boneh and D. Freeman. Homomorphic signatures for polynomial functions. In Paterson [217], pages 149–168.

[47] D. Boneh and D. Freeman. Linearly homomorphic signatures over binary fields and new tools for lattice-based signatures. In Catalano et al. [80], pages 1–16.

[48] D. Boneh, D. Freeman, J. Katz, and B. Waters. Signing a linear subspace: Signature schemes for network coding. In Jarecki and Tsudik [147], pages 68–87.

[49] D. Boneh, C. Gentry, and B. Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In Victor Shoup, editor, *CRYPTO*, volume 3621 of *Lecture Notes in Computer Science*, pages 258–275. Springer, 2005.

[50] D. Boneh, A. Sahai, and B. Waters. Functional encryption: Definitions and challenges. In *TCC*, pages 253–273, 2011.

[51] D. Boneh, G. Segev, and B. Waters. Targeted malleability: homomorphic encryption for restricted computations. In Shafi Goldwasser, editor, *ITCS*, pages 350–366. ACM, 2012.

[52] D. Boneh and H. Shacham. Group signatures with verifier-local revocation. In Atluri et al. [18], pages 168–177.

[53] Dan Boneh, editor. *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, volume 2729 of *Lecture Notes in Computer Science*. Springer, 2003.

[54] X. Boyen and C. Delerablée. Expressive subgroup signatures. In *SCN*, pages 185–200, 2008.

[55] X. Boyen and B. Waters. Compact group signatures without random oracles. In Vaudenay [244], pages 427–444.

[56] X. Boyen and B. Waters. Full-domain subgroup hiding and constant-size group signatures. In *PKC 2007*, volume 4450 of *LNCS*, pages 1–15. Springer, 2007.

[57] E. Bresson and J. Stern. Efficient revocation in group signatures. In *Public Key Cryptography*, pages 190–206, 2001.

[58] E. Brickell. An efficient protocol for anonymously providing assurance of the container of the private key. In *Submission to the Trusted Computing Group*, 2003.

[59] E. Brickell, J. Camenisch, and L. Chen. Direct anonymous attestation. In Atluri et al. [18], pages 132–145.

[60] Christian Cachin and Jan Camenisch, editors. *Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004, Proceedings*, volume 3027 of *Lecture Notes in Computer Science*. Springer, 2004.

[61] J. Camenisch, R. Chaabouni, and A. shelat. Efficient protocols for set membership and range proofs. In Pieprzyk [219], pages 234–252.

[62] J. Camenisch, N. Chandran, and V. Shoup. A public key encryption scheme secure against key dependent chosen plaintext and adaptive chosen ciphertext attacks. In Joux [149], pages 351–368.

[63] J. Camenisch, M. Dubovitskaya, and K. Haralambiev. Efficient structure-preserving signature scheme from standard assumptions. In *SCN*, pages 76–94, 2012.

[64] J. Camenisch, T. Groß, and T. Heydt-Benjamin. Rethinking accountable privacy supporting services: extended abstract. In *Digital Identity Management*, pages 1–8, 2008.

[65] J. Camenisch, K. Haralambiev, M. Kohlweiss, J. Lapon, and V. Naessens. Structure preserving CCA secure encryption and applications. In Lee and Wang [168], pages 89–106.

[66] J. Camenisch, M. Kohlweiss, and C. Soriente. An accumulator based on bilinear maps and efficient revocation for anonymous credentials. In Jarecki and Tsudik [147], pages 481–500.

[67] J. Camenisch, M. Kohlweiss, and C. Soriente. Solving revocation with efficient update of anonymous credentials. In *SCN*, pages 454–471, 2010.

[68] J. Camenisch and A. Lysyanskaya. Dynamic accumulators and application to efficient revocation of anonymous credentials. In Yung [250], pages 61–76.

[69] J. Camenisch, G. Neven, and M. Rückert. Fully anonymous attribute tokens from lattices. In *SCN*, pages 57–75, 2012.

[70] R. Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *FOCS*, pages 136–145. IEEE Computer Society, 2001.

[71] R. Canetti and M. Fischlin. Universally composable commitments. In Kilian [159], pages 19–40.

[72] R. Canetti, O. Goldreich, and S. Halevi. The random oracle methodology, revisited (preliminary version). In Vitter [245], pages 209–218.

[73] Ran Canetti and Juan A. Garay, editors. *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part II*, volume 8043 of *Lecture Notes in Computer Science*. Springer, 2013.

[74] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert. Bonsai trees, or how to delegate a lattice basis. In Gilbert [125].

[75] D. Catalano and D. Fiore. Vector commitments and their applications. In Kurosawa and Hanaoka [165], pages 55–72.

[76] D. Catalano, D. Fiore, and M. Messina. Zero-knowledge sets with short proofs. In Smart [239], pages 433–450.

[77] D. Catalano, D. Fiore, and B. Warinschi. Adaptive pseudo-free groups and applications. In Paterson [217], pages 207–223.

[78] D. Catalano, D. Fiore, and B. Warinschi. Efficient network coding signatures in the standard model. In Fischlin et al. [109], pages 680–696.

[79] D. Catalano, A Marcedone, and O. Puglisi. Authenticating computation on groups: New homomorphic primitives and applications. In *ASIACRYPT (2)*, pages 193–212, 2014.

[80] Dario Catalano, Nelly Fazio, Rosario Gennaro, and Antonio Nicolosi, editors. *Public Key Cryptography - PKC 2011 - 14th International Conference on Practice and Theory in Public Key Cryptography, Taormina, Italy, March 6-9, 2011. Proceedings*, volume 6571 of *Lecture Notes in Computer Science*. Springer, 2011.

[81] J. Cathalo, B. Libert, and M. Yung. Group encryption: Non-interactive realization in the standard model. In Matsui [197], pages 179–196.

[82] M. Chase and M. Kohlweiss. A new hash-and-sign approach and structure-preserving signatures from dlin. In *SCN*, pages 131–148, 2012.

[83] M. Chase, M. Kohlweiss, A. Lysyanskaya, and S. Meiklejohn. Malleable proof systems and applications. In Pointcheval and Johansson [220], pages 281–300.

[84] M. Chase, M. Kohlweiss, A. Lysyanskaya, and S. Meiklejohn. Verifiable elections that scale for free. In Pointcheval and Johansson [220], pages 479–496.

[85] D. Chaum and E. van Heyst. Group signatures. In *EUROCRYPT*, pages 257–265, 1991.

[86] J. Chen and H. Wee. Fully, (almost) tightly secure IBE from standard assumptions. In Canetti and Garay [73], pages 435–460.

[87] J. Chen and H. Wee. Dual system groups and its applications — compact HIBE and more. Cryptology ePrint Archive: Report 2014/265, April 2014.

[88] R. Cramer and V. Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In Hugo Krawczyk, editor, *CRYPTO*, volume 1462 of *Lecture Notes in Computer Science*, pages 13–25. Springer, 1998.

[89] R. Cramer and V. Shoup. Signature schemes based on the strong rsa assumption. In *ACM-CCS*, pages 46–51, 1999.

[90] R. Cramer and V. Shoup. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In Knudsen [161], pages 45–64.

[91] Ronald Cramer, editor. *Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings*, volume 3494 of *Lecture Notes in Computer Science*. Springer, 2005.

[92] Ronald Cramer, editor. *Theory of Cryptography - 9th Theory of Cryptography Conference, TCC 2012, Taormina, Sicily, Italy, March 19-21, 2012. Proceedings*, volume 7194 of *Lecture Notes in Computer Science*. Springer, 2012.

[93] G. Di Crescenzo, Y. Ishai, and R. Ostrovsky. Non-interactive and non-malleable commitment. In Vitter [245], pages 141–150.

[94] I. Damgård and J. Groth. Non-interactive and reusable non-malleable commitment schemes. In Lawrence L. Larmore and Michel X. Goemans, editors, *STOC*, pages 426–437. ACM, 2003.

[95] C. Delerablée and D. Pointcheval. Dynamic fully anonymous short group signatures. In *VIETCRYPT*, pages 193–210, 2006.

[96] Y. Desmedt. Society and group oriented cryptography: A new concept. In Carl Pomerance, editor, *CRYPTO*, volume 293 of *Lecture Notes in Computer Science*, pages 120–127. Springer, 1987.

[97] Y. Desmedt. Computer security by redefining what a computer is. In *NSPW*, pages 160–166, 1993.

[98] Y. Desmedt and Y. Frankel. Threshold cryptosystems. In Gilles Brassard, editor, *CRYPTO*, volume 435 of *Lecture Notes in Computer Science*, pages 307–315. Springer, 1989.

[99] Y. Dodis and N. Fazio. Public key broadcast encryption for stateless receivers. In Joan Feigenbaum, editor, *Digital Rights Management Workshop*, volume 2696 of *Lecture Notes in Computer Science*, pages 61–80. Springer, 2002.

[100] Y. Dodis, V. Shoup, and S. Walfish. Efficient constructions of composable commitments and zero-knowledge proofs. In Wagner [246], pages 515–535.

[101] D. Dolev, C. Dwork, and M. Naor. Non-malleable cryptography (extended abstract). In Cris Koutsougeras and Jeffrey Scott Vitter, editors, *STOC*, pages 542–552. ACM, 1991.

[102] D. Dolev, C. Dwork, and M. Naor. Non-malleable cryptography. *SIAM Journal on Computing*, 30(2):391–437, 2000.

[103] T. ElGamal. A public-key cryptosystem and a signature scheme based on discrete logarithms. In *CRYPTO*, pages 10–18, 1984.

[104] K. Emura, G. Hanaoka, G. Ohtake, T. Matsuda, and S. Yamada. Chosen ciphertext secure keyed-homomorphic public-key encryption. In Kurosawa and Hanaoka [165], pages 32–50.

[105] A. Escala, G. Herold, E. Kiltz, C. Ràfols, and J. L. Villar. An algebraic framework for diffie-hellman assumptions. In Canetti and Garay [73], pages 129–147.

[106] S. Even, O. Goldreich, and S. Micali. On-line/off-line digital schemes. In *CRYPTO*, pages 263–275, 1989.

[107] A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In Andrew M. Odlyzko, editor, *CRYPTO*, volume 263 of *Lecture Notes in Computer Science*, pages 186–194. Springer, 1986.

[108] M. Fischlin, B. Libert, and M. Manulis. Non-interactive and re-usable universally composable string commitments with adaptive security. In Lee and Wang [168], pages 468–485.

[109] Marc Fischlin, Johannes Buchmann, and Mark Manulis, editors. *Public Key Cryptography - PKC 2012 - 15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, May 21-23, 2012. Proceedings*, volume 7293 of *Lecture Notes in Computer Science*. Springer, 2012.

[110] Matthew K. Franklin, editor. *Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings*, volume 3152 of *Lecture Notes in Computer Science*. Springer, 2004.

[111] D. Freeman. Improved security for linearly homomorphic signatures: A generic framework. In Fischlin et al. [109], pages 697–714.

[112] G. Fuchsbauer. Automorphic signatures in bilinear groups and an application to round-optimal blind signatures. *IACR Cryptology ePrint Archive*, 2009:320, 2009.

[113] G. Fuchsbauer and D. Pointcheval. Encrypting proofs on pairings and its application to anonymity for signatures. In *Pairing 2009*, pages 132–149, 2009.

[114] E. Fujisaki. New constructions of efficient simulation-sound commitments using encryption and their applications. In Orr Dunkelman, editor, *CT-RSA*, volume 7178 of *Lecture Notes in Computer Science*, pages 136–155. Springer, 2012.

[115] S. D. Galbraith, K. G. Paterson, and N. P. Smart. Pairings for cryptographers. *Discrete Appl. Math.*, 156(16), September 2008.

[116] J. Garay, P. MacKenzie, and K. Yang. Strengthening zero-knowledge protocols using signatures. In Eli Biham, editor, *EUROCRYPT*, volume 2656 of *Lecture Notes in Computer Science*, pages 177–194. Springer, 2003.

[117] Juan A. Garay, Atsuko Miyaji, and Akira Otsuka, editors. *Cryptology and Network Security, 8th International Conference, CANS 2009, Kanazawa, Japan, December 12-14, 2009. Proceedings*, volume 5888 of *Lecture Notes in Computer Science*. Springer, 2009.

[118] R. Gennaro. Multi-trapdoor commitments and their applications to proofs of knowledge secure under concurrent man-in-the-middle attacks. In Franklin [110], pages 220–236.

[119] R. Gennaro, C. Gentry, and B. Parno. Non-interactive verifiable computing: Outsourcing computation to untrusted workers. In Rabin [225], pages 465–482.

[120] R. Gennaro, J. Katz, H. Krawczyk, and T. Rabin. Secure network coding over the integers. In Phong Q. Nguyen and David Pointcheval, editors, *Public Key Cryptography*, volume 6056 of *Lecture Notes in Computer Science*, pages 142–160. Springer, 2010.

[121] R. Gennaro and S. Micali. Independent zero-knowledge sets. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *ICALP (2)*, volume 4052 of *Lecture Notes in Computer Science*, pages 34–45. Springer, 2006.

[122] C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *STOC*, pages 197–206, 2008. Full version available at `http://eprint.iacr.org/2007/432.pdf`.

[123] C. Gentry and A. Silverberg. Hierarchical ID-based cryptography. In Yuliang Zheng, editor, *ASIACRYPT*, volume 2501 of *Lecture Notes in Computer Science*, pages 548–566. Springer, 2002.

[124] C. Gentry and B. Waters. Adaptive security in broadcast encryption systems (with short ciphertexts). In Joux [149], pages 171–188.

[125] Henri Gilbert, editor. *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30 - June 3, 2010. Proceedings*, volume 6110 of *Lecture Notes in Computer Science*. Springer, 2010.

[126] O. Goldreich, S. Micali, and A. Wigderson. Proofs that yield nothing but their validity and a methodology of cryptographic protocol design. In *FOCS*, pages 174–187, 1986.

[127] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof systems. In *STOC*, pages 291–304, 1985.

[128] S. Goldwasser and Y. Tauman. On the (in)security of the Fiat-Shamir paradigm. In *FOCS*, pages 102–113, 2003.

[129] S. Dov Gordon, J. Katz, and V . Vaikuntanathan. A group signature scheme from lattice assumptions. In Masayuki Abe, editor, *ASIACRYPT*, volume 6477 of *Lecture Notes in Computer Science*, pages 395–412. Springer, 2010.

[130] V. Goyal. Reducing trust in the PKG in identity-based cryptosystems. In *CRYPTO*, pages 430–447, 2007.

[131] V. Goyal, S. Lu, A. Sahai, and B. Waters. Black-box accountable authority identity-based encryption. In Ning et al. [213], pages 427–436.

[132] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In Ferng-Ching Lin, Der-Tsai Lee, Bao-Shuh Paul Lin, Shiuhpyng Shieh, and Sushil Jajodia, editors, *ACM Conference on Computer and Communications Security*, pages 195–203. ACM, 2006.

[133] J. Groth. Simulation-sound NIZK proofs for a practical language and constant size group signatures. In Xuejia Lai and Kefei Chen, editors, *ASIACRYPT*, volume 4284 of *Lecture Notes in Computer Science*, pages 444–459. Springer, 2006.

[134] J. Groth. Fully anonymous group signatures without random oracles. In Kurosawa [164], pages 164–180.

[135] J. Groth. Homomorphic trapdoor commitments to group elements. *IACR Cryptology ePrint Archive*, 2009:7, 2009.

[136] J. Groth, R. Ostrovsky, and A. Sahai. Non-interactive Zaps and new techniques for NIZK. In Vaudenay [244], pages 97–111.

[137] J. Groth, R. Ostrovsky, and A. Sahai. Perfect non-interactive zero knowledge for NP. In Vaudenay [244], pages 339–358.

[138] J. Groth and A. Sahai. Efficient non-interactive proof systems for bilinear groups. In Smart [239], pages 415–432.

[139] Shai Halevi, editor. *Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings*, volume 5677 of *Lecture Notes in Computer Science*. Springer, 2009.

[140] D. Halevy and A. Shamir. The LSD broadcast encryption scheme. In Yung [250], pages 47–60.

[141] F. Ben Hamouda, J. Camenisch, S. Krenn, V. Lyubashevsky, and G. Neven. Better zero-knowledge proofs for lattice encryption and their application to group signatures. In *ASIACRYPT (1)*, pages 551–572, 2014.

[142] D. Hofheinz and T. Jager. Tightly secure signatures and public-key encryption. In Safavi-Naini and Canetti [230], pages 590–607.

[143] D. Hofheinz and E. Kiltz. Secure hybrid encryption from weakened key encapsulation. In *CRYPTO*, pages 553–571, 2007.

[144] J. Horwitz and B. Lynn. Toward hierarchical identity-based encryption. In Knudsen [161], pages 466–481.

[145] M. Izabachène, B. Libert, and D. Vergnaud. Block-wise p-signatures and non-interactive anonymous credentials with efficient attributes. In Liqun Chen, editor, *IMA Int. Conf.*, volume 7089 of *Lecture Notes in Computer Science*, pages 431–450. Springer, 2011.

[146] A. Jain, S. Krenn, K. Pietrzak, and A. Tentes. Commitments and efficient zero-knowledge proofs from learning parity with noise. In *ASIACRYPT*, pages 663–680, 2012.

[147] Stanislaw Jarecki and Gene Tsudik, editors. *Public Key Cryptography - PKC 2009, 12th International Conference on Practice and Theory in Public Key Cryptography, Irvine, CA, USA, March 18-20, 2009. Proceedings*, volume 5443 of *Lecture Notes in Computer Science*. Springer, 2009.

[148] R. Johnson, D. Molnar, D. Song, and D. Wagner. Homomorphic signature schemes. In Bart Preneel, editor, *CT-RSA*, volume 2271 of *Lecture Notes in Computer Science*, pages 244–262. Springer, 2002.

[149] Antoine Joux, editor. *Advances in Cryptology - EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, 2009. Proceedings*, volume 5479 of *Lecture Notes in Computer Science*. Springer, 2009.

[150] C. Jutla and A. Roy. Relatively-sound NIZKs and password-based key-exchange. In Fischlin et al. [109], pages 485–503.

[151] C. Jutla and A. Roy. Shorter quasi-adaptive NIZK proofs for linear subspaces. In Kazue Sako and Palash Sarkar, editors, *ASIACRYPT (1)*, volume 8269 of *Lecture Notes in Computer Science*, pages 1–20. Springer, 2013.

[152] C. Jutla and A. Roy. Dual-system simulation-soundness with applications to UC-PAKE and more. *Cryptology ePrint Archive: Report 2014/805*, 2014.

[153] C. Jutla and A. Roy. Switching lemma for bilinear tests and constant-size NIZK proofs for linear subspaces. In *CRYPTO (2)*, pages 295–312, 2014.

[154] J. Katz, A. Sahai, and B. Waters. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In Smart [239], pages 146–162.

[155] A. Kiayias, Y. Tsiounis, and M. Yung. Traceable signatures. In Cachin and Camenisch [60], pages 571–589.

[156] A. Kiayias, Y. Tsiounis, and M. Yung. Group encryption. In Kurosawa [164], pages 181–199.

[157] A. Kiayias and M. Yung. Group signatures with efficient concurrent join. In Cramer [91], pages 198–214.

[158] A. Kiayias and M. Yung. Secure scalable group signature with dynamic joins and separable authorities. *IJSN*, 1(1/2):24–45, 2006.

[159] Joe Kilian, editor. *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings*, volume 2139 of *Lecture Notes in Computer Science*. Springer, 2001.

[160] E. Kiltz. Chosen-ciphertext security from tag-based encryption. In *TCC'06*, volume 3876 of *LNCS*, pages 581–600. Springer, 2006.

[161] Lars R. Knudsen, editor. *Advances in Cryptology - EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, April 28 - May 2, 2002, Proceedings*, volume 2332 of *Lecture Notes in Computer Science*. Springer, 2002.

[162] H. Krawczyk and T. Rabin. Chameleon signatures. In *NDSS*, 2000.

[163] S. Kunz-Jacques and D. Pointcheval. About the security of MTI/C0 and MQV. In Roberto De Prisco and Moti Yung, editors, *SCN*, volume 4116 of *Lecture Notes in Computer Science*, pages 156–172. Springer, 2006.

[164] Kaoru Kurosawa, editor. *Advances in Cryptology - ASIACRYPT 2007, 13th International Conference on the Theory and Application of Cryptology and Information Security, Kuching, Malaysia, December 2-6, 2007, Proceedings*, volume 4833 of *Lecture Notes in Computer Science*. Springer, 2007.

[165] Kaoru Kurosawa and Goichiro Hanaoka, editors. *Public-Key Cryptography - PKC 2013 - 16th International Conference on Practice and Theory in Public-Key Cryptography, Nara, Japan, February 26 - March 1, 2013. Proceedings*, volume 7778 of *Lecture Notes in Computer Science*. Springer, 2013.

[166] F. Laguillaumie, A. Langlois, B. Libert, and D. Stehlé. Lattice-based group signatures with logarithmic signature size. In *ASIACRYPT*, pages 41–61, 2013.

[167] F. Laguillaumie, P. Paillier, and D. Vergnaud. Universally convertible directed signatures. In Roy [229], pages 682–701.

[168] Dong Hoon Lee and Xiaoyun Wang, editors. *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, volume 7073 of *Lecture Notes in Computer Science*. Springer, 2011.

[169] A. Lewko. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In Gilbert [125], pages 62–91.

[170] A. Lewko. Tools for simulating features of composite order bilinear groups in the prime order setting. In Pointcheval and Johansson [220], pages 318–335.

[171] A. Lewko and B. Waters. New techniques for dual system encryption and fully secure HIBE with short ciphertexts. In Micciancio [201], pages 455–479.

[172] A. Lewko and B. Waters. Unbounded HIBE and attribute-based encryption. In Paterson [217], pages 547–567.

[173] B. Libert and M. Joye. Group signatures with message-dependent opening in the standard model. In *CT-RSA*, pages 286–306, 2014.

[174] B. Libert, M. Joye, and M. Yung. Born and raised distributed: Fully distributed non-interactive adaptively secure threshold signatures with short shares. In *PODC*, pages 303–312. ACM Press, 2014.

[175] B. Libert, M. Joye, M. Yung, and T. Peters. Concise multi-challenge CCA-secure encryption and signatures with almost tight security. In *ASIACRYPT (2)*, pages 1–21, 2014.

[176] B. Libert, M. Joye, M. Yung, and T. Peters. Traceable group encryption. In Canetti and Garay [73], pages 592–610.

[177] B. Libert, T. Peters, M. Joye, and M. Yung. Linearly homomorphic structure-preserving signatures and their applications. In Canetti and Garay [73], pages 289–307.

[178] B. Libert, T. Peters, M. Joye, and M. Yung. Non-malleability from malleability: Simulation-sound quasi-adaptive NIZK proofs and CCA2-secure encryption from homomorphic signatures. In Nguyen and Oswald [211].

[179] B. Libert, T. Peters, and M. Yung. Group signatures with almost-for-free revocation. In Safavi-Naini and Canetti [230], pages 571–589.

[180] B. Libert, T. Peters, and M. Yung. Scalable group signatures with revocation. In Pointcheval and Johansson [220], pages 609–627.

[181] B. Libert, J.-J. Quisquater, and M. Yung. Foward-secure signatures in untrusted update environments: Efficient and generic constructions. In Ning et al. [212], pages 511–520.

[182] B. Libert, J.-J. Quisquater, and M. Yung. Key evolution systems in untrusted update environments. *ACM Transactions on Information and Systems Security*, 13(4), 2010.

[183] B. Libert and D. Vergnaud. Multi-use unidirectional proxy re-signatures. In Ning et al. [213], pages 511–520.

[184] B. Libert and D. Vergnaud. Unidirectional chosen-ciphertext-secure proxy re-encryption. In Ronald Cramer, editor, *PKC*, volume 4939 of *Lecture Notes in Computer Science*, pages 360–379. Springer, 2008.

[185] B. Libert and D. Vergnaud. Group signatures with verifier-local revocation and backward unlinkability in the standard model. In Garay et al. [117], pages 498–517.

[186] B. Libert and D. Vergnaud. Towards black-box accountable authority IBE with short ciphertexts and private keys. In Garay et al. [117], pages 235–255.

[187] B. Libert and M. Yung. Efficient traceable signatures in the standard model. In *Pairing*, pages 187–205, 2009.

[188] B. Libert and M. Yung. Concise mercurial vector commitments and independent zero-knowledge sets with short proofs. In Micciancio [201], pages 499–517.

[189] B. Libert and M. Yung. Adaptively secure forward-secure non-interactive threshold cryptosystems. In Chuankun Wu, Moti Yung, and Dongdai Lin, editors, *Inscrypt*, volume 7537 of *Lecture Notes in Computer Science*, pages 1–21. Springer, 2011.

[190] B. Libert and M. Yung. Efficient traceable signatures in the standard model. *Theoretical Computer Science*, 412(12-14):1220–1242, 2011.

[191] B. Libert and M. Yung. Non-interactive CCA-secure threshold cryptosystems with adaptive security: New framework and constructions. In Cramer [92], pages 75–93.

[192] Y. Lindell. A simple construction of CCA2-secure public-key encryption under general assumptions. In Menezes [198], pages 241–254.

[193] S. Ling, K. Nguyen, D. Stehlé, and H. Wang. Improved zero-knowledge proofs of knowledge for the isis problem, and applications. In *Public Key Cryptography*, pages 107–124, 2013.

[194] V. Lyubashevsky. Lattice-based identification schemes secure under active attacks. In *PKC*, pages 162–179, 2014.

[195] P. MacKenzie and K. Yang. On simulation-sound trapdoor commitments. In Cachin and Camenisch [60], pages 382–400.

[196] T. Malkin, I. Teranishi, Y. Vahlis, and M. Yung. Signatures resilient to continual leakage on memory and computation. In Yuval Ishai, editor, *TCC*, volume 6597 of *Lecture Notes in Computer Science*, pages 89–106. Springer, 2011.

[197] Mitsuru Matsui, editor. *Advances in Cryptology - ASIACRYPT 2009, 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, December 6-10, 2009. Proceedings*, volume 5912 of *Lecture Notes in Computer Science*. Springer, 2009.

[198] Alfred Menezes, editor. *Advances in Cryptology - CRYPTO 2007, 27th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2007, Proceedings*, volume 4622 of *Lecture Notes in Computer Science*. Springer, 2007.

[199] S. Micali, M. Rabin, and J. Kilian. Zero-knowledge sets. In *FOCS*, pages 80–91, 2003.

[200] D. Micciancio and S. Vadhan. Statistical zero-knowledge proofs with efficient provers: Lattice problems and more. In *CRYPTO*, pages 282–298, 2003.

[201] Daniele Micciancio, editor. *Theory of Cryptography, 7th Theory of Cryptography Conference, TCC 2010, Zurich, Switzerland, February 9-11, 2010. Proceedings*, volume 5978 of *Lecture Notes in Computer Science*. Springer, 2010.

[202] T. Nakanishi, H. Fujii, Y. Hira, and N. Funabiki. Revocable group signature schemes with constant costs for signing and verifying. In Jarecki and Tsudik [147], pages 463–480.

[203] T. Nakanishi and N. Funabiki. Verifier-local revocation group signature schemes with backward unlinkability from bilinear maps. In Roy [229], pages 533–548.

[204] T. Nakanishi and N. Funabiki. Revocable group signatures with compact revocation list using accumulators. In *ICISC*, pages 435–451, 2013.

[205] D. Naor, M. Naor, and J. Lotspiech. Revocation and tracing schemes for stateless receivers. In Kilian [159], pages 41–62.

[206] M. Naor. On cryptographic assumptions and challenges. In Boneh [53], pages 96–109.

[207] M. Naor and M. Yung. Universal one-way hash functions and their cryptographic applications. In *STOC*, pages 33–43, 1989.

[208] M. Naor and M. Yung. Public-key cryptosystems provably secure against chosen ciphertext attacks. In Harriet Ortiz, editor, *STOC*, pages 427–437. ACM, 1990.

[209] L. Nguyen. Accumulators from bilinear pairings and applications. In Alfred Menezes, editor, *CT-RSA*, volume 3376 of *Lecture Notes in Computer Science*, pages 275–292. Springer, 2005.

[210] L. Nguyen and R. Safavi-Naini. Efficient and provably secure trapdoor-free group signature schemes from bilinear pairings. In Pil Joong Lee, editor, *ASIACRYPT*, volume 3329 of *Lecture Notes in Computer Science*, pages 372–386. Springer, 2004.

[211] Phong Q. Nguyen and Elisabeth Oswald, editors. *Advances in Cryptology - EUROCRYPT 2014, 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*, Lecture Notes in Computer Science. Springer, 2014.

[212] Peng Ning, Sabrina De Capitani di Vimercati, and Paul F. Syverson, editors. *Proceedings of the 2007 ACM Conference on Computer and Communications Security, CCS 2007, Alexandria, Virginia, USA, October 28-31, 2007*. ACM, 2007.

[213] Peng Ning, Paul F. Syverson, and Somesh Jha, editors. *Proceedings of the 2008 ACM Conference on Computer and Communications Security, CCS 2008, Alexandria, Virginia, USA, October 27-31, 2008*. ACM, 2008.

[214] R. Nishimaki, E. Fujisaki, and K. Tanaka. A multi-trapdoor commitment scheme from the RSA assumption. In *ACISP*, pages 182–199, 2010.

[215] T. Okamoto and K. Takashima. Fully secure functional encryption with general relations from the decisional linear assumption. In Rabin [225], pages 191–208.

[216] P. Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *EUROCRYPT'99*, LNCS, pages 223–238. Springer, 1999.

[217] Kenneth G. Paterson, editor. *Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings*, volume 6632 of *Lecture Notes in Computer Science*. Springer, 2011.

[218] C. Peikert and V. Vaikuntanathan. Noninteractive statistical zero-knowledge proofs for lattice problems. In *CRYPTO*, pages 536–553. Springer, 2008.

[219] Josef Pieprzyk, editor. *Advances in Cryptology - ASIACRYPT 2008, 14th International Conference on the Theory and Application of Cryptology and Information Security, Melbourne, Australia, December 7-11, 2008. Proceedings*, volume 5350 of *Lecture Notes in Computer Science*. Springer, 2008.

[220] David Pointcheval and Thomas Johansson, editors. *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*, volume 7237 of *Lecture Notes in Computer Science*. Springer, 2012.

[221] M. Prabhakaran and M. Rosulek. Rerandomizable RCCA encryption. In Menezes [198], pages 517–534.

[222] M. Prabhakaran and M. Rosulek. Homomorphic encryption with CCA security. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *ICALP (2)*, volume 5126 of *Lecture Notes in Computer Science*, pages 667–678. Springer, 2008.

[223] M. Prabhakaran and M. Rosulek. Towards robust computation on encrypted data. In Pieprzyk [219], pages 216–233.

[224] B. Qin, Q. Wu, W. Susilo, Y. Mu, and Y. Wang. Publicly verifiable privacy-preserving group decryption. In *Inscrypt*, LNCS, pages 72–83. Springer, 2008.

[225] Tal Rabin, editor. *Advances in Cryptology - CRYPTO 2010, 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings*, volume 6223 of *Lecture Notes in Computer Science*. Springer, 2010.

[226] C. Rackoff and D. Simon. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In Joan Feigenbaum, editor, *CRYPTO*, volume 576 of *Lecture Notes in Computer Science*, pages 433–444. Springer, 1991.

[227] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In *STOC*, pages 84–93, 2005.

[228] Y. Rouselakis and B. Waters. Practical constructions and new proof methods for large universe attribute-based encryption. In Ahmad-Reza Sadeghi, Virgil D. Gligor, and Moti Yung, editors, *ACM Conference on Computer and Communications Security*, pages 463–474. ACM, 2013.

[229] Bimal K. Roy, editor. *Advances in Cryptology - ASIACRYPT 2005, 11th International Conference on the Theory and Application of Cryptology and Information Security, Chennai, India, December 4-8, 2005, Proceedings*, volume 3788 of *Lecture Notes in Computer Science*. Springer, 2005.

[230] Reihaneh Safavi-Naini and Ran Canetti, editors. *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, volume 7417 of *Lecture Notes in Computer Science*. Springer, 2012.

[231] A. Sahai. Non-malleable non-interactive zero knowledge and adaptive chosen-ciphertext security. In *FOCS*, pages 543–553. IEEE Computer Society, 1999.

[232] A. Sahai and B. Waters. Fuzzy identity-based encryption. In Cramer [91], pages 457–473.

[233] Y. Sakai, K. Emura, G. Hanaoka, Y. Kawai, T. Matsuda, and K. Omote. Group signatures with message-dependent opening. In *Pairing*, pages 270–294, 2012.

[234] M. Scott. Authenticated ID-based key exchange and remote log-in with simple token and pin number. Technical report, Cryptology ePrint Archive: Report 2002/164, 2002.

[235] H. Shacham. A cramer-shoup encryption scheme from the linear assumption and from progressively weaker linear variants. *IACR Cryptology ePrint Archive*, page 74, 2007.

[236] A. Shamir. Identity-based cryptosystems and signature schemes. In *CRYPTO*, pages 47–53, 1984.

[237] V. Shoup. Lower bounds for discrete logarithms and related problems. In *EUROCRYPT*, pages 256–266, 1997.

[238] V. Shoup. A proposal for an ISO standard for public key encryption (version 2.1). Manuscript, December 2001.

[239] Nigel P. Smart, editor. *Advances in Cryptology - EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008. Proceedings*, volume 4965 of *Lecture Notes in Computer Science*. Springer, 2008.

[240] D. Song. Practical forward secure group signature schemes. In *ACM Conference on Computer and Communications Security*, pages 225–234, 2001.

[241] P. Tsang, M. Ho Au, A. Kapadia, and S. Smith. Blacklistable anonymous credentials: blocking misbehaving users without ttps. In Ning et al. [212], pages 72–81.

[242] P. Tsang, M. Ho Au, A. Kapadia, and S. Smith. Perea: towards practical ttp-free revocation in anonymous authentication. In Ning et al. [213], pages 333–344.

[243] G. Tsudik and S. Xu. Accumulating composites and improved group signing. In Chi-Sung Laih, editor, *ASIACRYPT*, volume 2894 of *Lecture Notes in Computer Science*, pages 269–286. Springer, 2003.

[244] Serge Vaudenay, editor. *Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings*, volume 4004 of *Lecture Notes in Computer Science*. Springer, 2006.

[245] Jeffrey Scott Vitter, editor. *Proceedings of the Thirtieth Annual ACM Symposium on the Theory of Computing, Dallas, Texas, USA, May 23-26, 1998*. ACM, 1998.

[246] David Wagner, editor. *Advances in Cryptology - CRYPTO 2008, 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008. Proceedings*, volume 5157 of *Lecture Notes in Computer Science*. Springer, 2008.

[247] Xiaoyun Wang and Kazue Sako, editors. *Advances in Cryptology - ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings*, volume 7658 of *Lecture Notes in Computer Science*. Springer, 2012.

[248] B. Waters. Efficient identity-based encryption without random oracles. In Cramer [91], pages 114–127.

[249] B. Waters. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In Halevi [139], pages 619–636.

[250] Moti Yung, editor. *Advances in Cryptology - CRYPTO 2002, 22nd Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 2002, Proceedings*, volume 2442 of *Lecture Notes in Computer Science*. Springer, 2002.

[251] S. Zhou and D. Lin. Shorter verifier-local revocation group signatures from bilinear maps. In *CANS*, pages 126–143, 2006.

Résumé

Ce mémoire s'intéresse aux primitives cryptographiques qui préservent la structure algébrique, ainsi qu'à leur utilisation dans la conception de preuves non-interactives sans divulgation de connaissance (de l'anglais "zero-knowledge") et de primitives protégeant la vie privée. En 2008, Groth et Sahai ont montré comment rendre ces systèmes de preuve efficaces dans des groupes abéliens munis de formes bilinéaires. Toutefois, l'utilisation de ces techniques nécessite de manipuler des objets qui vivent dans des groupes abéliens cycliques. On a donc besoin de signer des messages sans affecter leur structure algébrique (en particulier, sans les hacher) de façon à pouvoir prouver efficacement des propriétés à propos de messages signés secrets. La première partie du mémoire décrit un schéma de signature préservant la structure qui a été la première réalisation efficace de la primitive sous des hypothèses algorithmiques ayant fait l'objet d'études préalables. Les mêmes outils sont ensuite utilisés dans la conception d'un nouveau mécanisme de révocation pour les signatures de groupe, qui permettent à des membres d'une population de signer des messages au nom de celle-ci tout en cachant leur identité. La seconde partie étudie les applications des signatures préservant la structure dotées de propriétés homomorphes. Nous montrons comment les utiliser dans la construction de cryptosystèmes non-malléables. Au moyen de signatures homomorphes qui gardent la structure, nous construisons ainsi des systèmes de mise sous scellé et des preuves "zero-knowledge" non-malléables, ainsi que des systèmes de chiffrement résistant aux attaques à chiffrés choisis.

Abstract

This habilitation thesis deals with cryptographic primitives that preserve the algebraic structure of underlying objects (messages, keys, etc) and their applications to the design of non-interactive zero-knowledge proofs and privacy-enhancing cryptographic primitives. In 2008, Groth and Sahai showed how to make these proof systems relatively efficient in abelian groups endowed with a bilinear map. These techniques, however, require to work with lower-level primitives where handled objects all live in a cyclic abelian group. Among other things, we need to sign messages without destroying their algebraic structure (in particular, without hashing them first) so as to be able to efficiently prove properties about hidden signed messages. The first part of this thesis describes a structure-preserving signature scheme which was the first efficient realization under previously studied algorithmic assumptions. These tools are also utilized in the design of a novel revocation mechanism for group signatures, which allow users to anonymously sign messages on behalf of a population they belong to. The second part of this thesis considers structure-preserving signatures endowed with homomorphic properties. We show how to use them in the design of non-malleable cryptographic primitives. Using linearly homomorphic structure-preserving signatures, we notably obtain non-malleable commitments to group elements and non-interactive zero-knowledge proofs, as well as public-key encryption schemes that resist chosen-ciphertext attacks.