



HAL
open science

Relativistic zero-knowledge protocol for NP over the internet unconditionally secure against quantum adversaries

André Chailloux, Yann Barsamian

► **To cite this version:**

André Chailloux, Yann Barsamian. Relativistic zero-knowledge protocol for NP over the internet unconditionally secure against quantum adversaries. 2023. hal-04320923

HAL Id: hal-04320923

<https://inria.hal.science/hal-04320923>

Preprint submitted on 4 Dec 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

Relativistic zero-knowledge protocol for NP over the internet unconditionally secure against quantum adversaries

André Chailloux* and Yann Barsamian†
Inria de Paris, EPI COSMIQ

Relativistic cryptography is a proposal for achieving unconditional security that exploits the fact that no information carrier can travel faster than the speed of light. It is based on space-time constraints but doesn't require quantum hardware. Nevertheless, it was unclear whether this proposal is realistic or not. Recently, Alikhani *et al.* [ABC⁺21] performed an implementation of a relativistic zero-knowledge for NP. Their implemented scheme shows the feasibility of relativistic cryptography but it is only secure against classical adversaries. In this work, we present a new relativistic protocol for NP which is secure against quantum adversaries and which is efficient enough so that it can be implemented on everyday laptops and internet connections. We use Stern's zero-knowledge scheme for the Syndrome Decoding problem, which was used before in post-quantum cryptography. The main technical contribution is a generalization of the consecutive measurement framework of [CL17] to prove the security of our scheme against quantum adversaries, and we perform an implementation that demonstrates the feasibility and efficiency of our proposed scheme.

I. INTRODUCTION

a. Context. There is a strong conceptual and practical appeal for building cryptographic schemes which have unconditional security meaning that they cannot be attacked by any classical or quantum computer, even with unlimited computing power. Quantum Key Distribution [BB84] is a prime example of this, and a huge amount of work has been done to understand its security and perform efficient implementations. Relativistic cryptography is another proposal for achieving unconditional security that exploits the no superluminal signaling (NSS) principle. NSS states that no information carrier can travel faster than the speed of light. The interest of relativistic cryptography is that it can perform coin flipping and bit commitment protocols with unconditional security which is known to be impossible even using quantum information [May97, LC97], so relativistic cryptography and quantum cryptography complete each other well for protocols with unconditional security. In order to perform protocols in relativistic cryptography, there has to be some strict space-time constraints between the different agents performing the protocol but they can be done without quantum hardware. The goal of this work is to show the practicality of relativistic cryptography by presenting a new relativistic zero-knowledge protocol for NP and demonstrating its feasibility in real-life conditions, on standard laptops using a standard internet connection. This is the first time a protocol for relativistic cryptography is implemented in this setting and shows these are much simpler to perform than what we could have expected.

b. Relativistic cryptography. The idea of using the NSS principle for cryptographic protocols started in a work by Kent [Ken99] as a way to physically enforce a

no-communication constraint between different agents (a similar idea already existed in multi-prover interactive proofs[BGKW88], but without any explicit implementation proposal). The original goal of Kent was to bypass the no-go theorems for quantum bit-commitment, and there has been many proposals for unconditionally secure relativistic bit commitment[Ken11, Ken12, KTHW13]. The original idea of [BGKW88] was also revisited by Crépeau *et al.* in [CSST11]. Based on this work, Lunghi *et al.* devised a relativistic bit commitment protocol involving only four agents, two for Alice and two for Bob [LKB⁺15] - hereafter called the \mathbb{F}_Q relativistic bit commitment. Their protocol is secure against quantum adversaries and a multi-round variant, with longer duration time, was shown to be secure against classical adversaries [LKB⁺15, CCL15, FF15]. While these protocols only seemed of theoretical interest at first, recent implementations have convincingly demonstrated that the required timing and location constraints can be efficiently enforced. In [VMH⁺16], the authors performed a 24-hour-long bit commitment with the pairs of agents standing 8km apart.

c. Relativistic zero-knowledge protocols for NP-complete problems. One important application of commitment schemes is zero-knowledge protocols. It was first observed in [CL17] that one can use the single round \mathbb{F}_Q relativistic bit commitment scheme to construct a relativistic zero-knowledge protocol for the Hamiltonian cycle problem, which is NP-complete with unconditional security even against entangled adversaries. The communication cost of this protocol however becomes quickly prohibitive and the necessary space-time constraints can't be ensured. A more recent proposal [CMS⁺20] constructs a variation over the standard 3 coloring zero-knowledge protocol. They manage to drastically reduce the communication at each round. However, the number of repetitions required is quite large to obtain classical security and is prohibitively too large to obtain security against quantum adversaries. This proposal (the variant secure

* andre.chailloux@inria.fr

† yann@barsamian.fr

	#Bytes/Round	#Repetitions	# Provers	Quantum Sec
[CL17]	1.89 MB	100	2	✓
[ABC ⁺ 21]	2 B	10 ⁶	2	×
[ABC ⁺ 21]	2 B	10 ¹⁹	3	✓
This work	17.03 KB	340	2	✓

TABLE I: Parameters for different zero-knowledge proposals for 100 security bits (see Appendix A for more details).

against classical adversaries) was recently implemented using some dedicated hardware [ABC⁺21].

In this letter, we present a new proposal for relativistic zero-knowledge for NP based on the Syndrome Decoding problem. This is an NP-complete problem which is also believed to be hard against quantum computer for random instances. We will use here Stern’s zero-knowledge scheme [Ste93] which was used before for post-quantum signature schemes with the \mathbb{F}_Q relativistic string commitment. This protocol will have a moderate amount of communication, but also a small amount of rounds to decrease the soundness error. A comparison between the different schemes is presented in Table I.

Our main technical contribution is to prove the security of this protocol against quantum adversaries. In order to do so, we relate its security to an entangled game and prove a lower bound on this game using a new quantum learning lemma on consecutive quantum measurements, in the similar vein of [CL17]. We then implement the key steps of this protocol and show it is efficient enough so that the space-time constraints can be satisfied using standard computers and a standard internet connection. The only specific hardware we require are synchronized clocks.

II. PRELIMINARIES

a. The relativistic \mathbb{F}_Q string commitment. We recall here the relativistic \mathbb{F}_Q string commitment that we will use in our relativistic zero-knowledge protocol. We consider a prover \mathcal{P} that wants to commit a string $z \in \mathbb{F}_P$ to a verifier \mathcal{V} . Both parties, have agents respectively $\mathcal{P}_1, \mathcal{P}_2$ and $\mathcal{V}_1, \mathcal{V}_2$. $\mathcal{P}_1, \mathcal{V}_1$ are at a certain spatial location and $\mathcal{P}_2, \mathcal{V}_2$ at a different spatial location, at a distance D from the first one. The committed string is in \mathbb{F}_P and we also consider a set $\mathbb{F}_Q \supseteq \mathbb{F}_P$, where Q is a parameter of the commitment scheme. The protocol (when followed by honest players) consists of 3 phases: preparation, commit, and reveal. The string commitment protocol goes as follows.

1. *Preparation phase:* $\mathcal{P}_1, \mathcal{P}_2$ (resp. $\mathcal{V}_1, \mathcal{V}_2$) share a random number $a \in \mathbb{F}_Q$ (resp. $b \in \mathbb{F}_Q$).
2. *Commit phase:* \mathcal{V}_1 sends b to \mathcal{P}_1 , who immediately returns $y = a + z * b$ where $z \in \mathbb{F}_P$ is the committed

string. We map $z \in \mathbb{F}_P$ as an element of \mathbb{F}_Q , since $\mathbb{F}_P \subseteq \mathbb{F}_Q$, the operations $+$ and $*$ used are those of \mathbb{F}_Q .

3. *Reveal phase:* \mathcal{P}_2 reveals the values of z and a to \mathcal{V}_2 who checks that $y = a + z * b$.

This protocol has the following timing properties: let τ_1 the time when \mathcal{V}_1 sends b and τ_2 the time when \mathcal{V}_2 receives (z, a) . If $\tau_2 - \tau_1 < D/c$ where c is the speed of light then the NSS principle ensures that the message (z, a) is independent of b . The following security properties were proven in [LKB⁺15]:

- It is *perfectly hiding*: the verifiers don’t have any information about z after the commit phase.
- It is *binding*: informally, the provers can change their mind about z after the commit phase only with vanishingly small probability.

b. The syndrome decoding problem. The Hamming weight $|\mathbf{v}|_H$ of a binary vector is the number of 1 coordinates of this vector.

Problem 1 (Syndrome Decoding - SD(n, k, w)).

- Instance: a matrix $\mathbf{H} \in \{0, 1\}^{(n-k) \times n}$, a column vector $\mathbf{s} \in \{0, 1\}^{n-k}$,
- Goal: output a column vector $\mathbf{e} \in \{0, 1\}^n$ such that $\mathbf{H}\mathbf{e} = \mathbf{s}$ and $|\mathbf{e}|_H = w$.

The Syndrome Decoding problem is NP-complete and also believed to be hard on random instances even against quantum computers. It is the canonical hard problem for code-based cryptography. In order to construct a zero-knowledge protocol for this scheme, we first have to split the instances of our problem into Yes instances and No instances. For the SD(n, k, w) problem, Yes instances are the pairs (\mathbf{H}, \mathbf{s}) such that a solution (*i.e.* a vector $\mathbf{e} \in \{0, 1\}^n$ st. $\mathbf{H}\mathbf{e} = \mathbf{s}$ and $|\mathbf{e}|_H = w$) exists. No instances are the pairs (\mathbf{H}, \mathbf{s}) where no such solution exists.

III. OUR PROPOSAL FOR RELATIVISTIC ZERO-KNOWLEDGE FOR NP

A. Brief definition of a zero-knowledge scheme

In a zero-knowledge protocol between a prover \mathcal{P} and verifier \mathcal{V} , they are given an instance of a computational problem which is either a Yes or a No instance. \mathcal{P} wants to convince \mathcal{V} that they are in a Yes instance but he doesn’t want to reveal any other information to \mathcal{V} . Zero-knowledge protocols have many applications in cryptography, for example for identification schemes. If we start from a Yes instance and both players are honest then \mathcal{V} should be convinced and always accept (*Completeness*). If \mathcal{P} is honest then \mathcal{V} shouldn’t learn anything more from its interaction with \mathcal{P} than the fact that they have a Yes instance (*Zero-knowledge*). If we start from a No instance

and for any cheating prover \mathcal{P} , \mathcal{V} should reject with high probability (*Soundness*). The honest prover could in theory be computationally unbounded, but in our case, we only require a polynomial time prover, which additionally knows a solution to the problem for Yes instances. We give him this solution in an Auxiliary input. However, cheating provers stay computationally unbounded.

B. Description of our 1-round relativistic zero-knowledge protocol for NP

We combine the \mathbb{F}_Q relativistic string commitment and Stern's 1-round zero-knowledge protocol for SD in order to get our 1-round relativistic zero-knowledge protocol for SD. Again, \mathcal{P} and \mathcal{V} are split into 2 agents $\mathcal{P}_1, \mathcal{P}_2$ and $\mathcal{V}_1, \mathcal{V}_2$. In the honest case, we require $\mathcal{V}_1, \mathcal{V}_2$ to be at some distance D . We present this protocol in Figure 1. This description is self-contained but we discuss more in length this protocol as well as Stern's original zero-knowledge protocol in Appendix B, which can be a good start for those not familiar with the scheme. The timing constraints ensure that for each $i \in \{1, 2\}$, the message sent by \mathcal{P}_i is independent of the message sent from \mathcal{V}_j to \mathcal{P}_j for $j \neq i$.

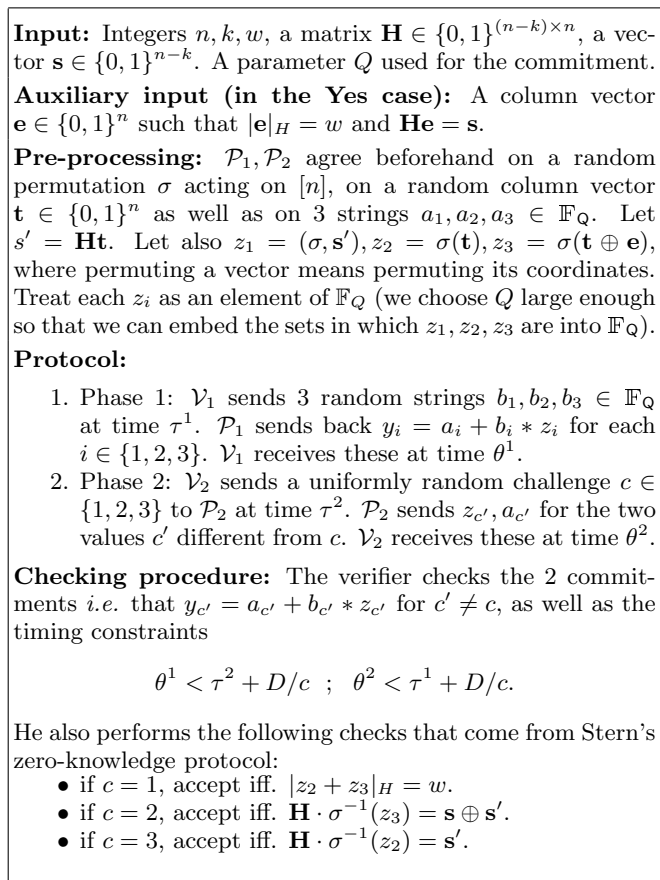


FIG. 1: 1-round Relativistic zero-knowledge protocol for SD using the \mathbb{F}_Q commitment scheme.

We prove the security of this scheme. Completeness and the zero-knowledge property follow quite directly from the security of Stern's signature scheme and of the \mathbb{F}_Q commitment scheme. The main technical contribution of this work is to bound the soundness of this protocol. We prove the following:

Theorem 1. *This protocol has perfect completeness, perfect zero-knowledge and has soundness $\frac{2}{3} + \left(\frac{n!2^{4n}}{Q}\right)^{1/4}$ if the space-time constraints are satisfied.*

This means that for No instances, an all powerful cheating prover can convince the verifier wp. at most $\frac{2}{3} + \left(\frac{n!2^{4n}}{Q}\right)^{1/4}$. By taking $Q = 10^{12}n!2^{4n}$, the soundness becomes $\frac{2}{3} + 0.001$. This seems like a very large Q but recall that sending an element of \mathbb{F}_Q requires $\log_2(Q)$ and performing additions and multiplications in a field of this size is still very efficient. We give the full proof of this Theorem in Appendix C.

IV. FULL PROTOCOL AND IMPLEMENTATION

Our full loss-tolerant relativistic zero-knowledge protocol for NP is described in Figure 2. We repeat our 1-round protocol R times sequentially and allow for a λ fraction of rounds where the space-time constraints are not satisfied, for eg. because of losses in the signal. We extend our security proof to this full protocol in Appendix D.

a. Timing constraints. We added an extra parameter T_{shift} that will make the space-time constraints easier to satisfy. For round i , let $T_i^{\text{Phase1}} = \theta_i^1 - \tau_i^1$ and $T_i^{\text{Phase2}} = \theta_i^2 - \tau_i^2$. In phase 1, \mathcal{V}_1 sends 3 strings in \mathbb{F}_Q , \mathcal{P}_1 does a computation and sends back 3 strings in \mathbb{F}_Q . In phase 2, \mathcal{V}_2 sends a challenge in $\{1, 2, 3\}$ and gets back 2 messages in \mathbb{F}_Q . This explains why phase 1 is longer than phase 2. The timing constraints become for each i :

$$\theta_i^1 < \tau_i^2 + D/c \quad \Rightarrow \quad T_i^{\text{Phase1}} - T_{\text{Shift}} < D/c \quad (1)$$

$$\theta_i^2 < \tau_i^1 + D/c \quad \Rightarrow \quad T_i^{\text{Phase2}} + T_{\text{Shift}} < D/c \quad (2)$$

Here, we see why we use T_{Shift} . Since the 2 phases take different times, the first constraint would be harder to achieve than the second one with $T_{\text{Shift}} = 0$. By taking T_{Shift} to be an estimate of $\frac{1}{2}(T_i^{\text{Phase1}} - T_i^{\text{Phase2}})$ for an average i , we make the two constraints essentially equally hard to satisfy.

b. Our two scenarios. We perform a demonstration of this full scheme using only regular laptops as well as standard network links (ethernet or wifi). We run the experiment in 2 different scenarios.

1. \mathcal{V}_1 and \mathcal{P}_1 are in the same room and are connected through a direct ethernet cable. \mathcal{V}_2 and \mathcal{P}_2 are in a different location but also connected through an ethernet cable. The distance between \mathcal{V}_1 and \mathcal{V}_2 is about 400km

Parameters: (n,k,w) for the SD problem. A parameter Q for the commitment used. A parameter D gives the distance between the 2 verifiers, and a time parameter Δ_T to delimit the time of a round, a time parameter T_{Shift} to determine the time shift between the 2 phases of the protocol. A number of rounds R and an allowed fraction of losses λ .

1. The 2 provers and verifiers agree together on an initial time T_1 on which they start the protocol.
2. For i from 1 to R : run the 1-round relativistic ZK protocol with the \mathbb{F}_Q commitment scheme. \mathcal{V}_1 sends his first message at time $\tau_i^1 = T_1 + (i - 1) * \Delta_T$, and \mathcal{V}_2 sends his first message at time $\tau_i^2 = T_1 + (i - 1) * \Delta_T + T_{\text{Shift}}$. Let θ_i^1 the time at which \mathcal{V}_1 receives the message from \mathcal{P}_1 and θ_i^2 the time at which \mathcal{V}_2 receives the message from \mathcal{P}_2 .
3. At the end of the protocol, the verifiers check the space-time constraints for each i from 1 to R , *i.e.* check that $\theta_i^1 < \tau_i^2 + D/c$ and $\theta_i^2 < \tau_i^1 + D/c$. Let F be the number of rounds where these space-time constraints are not satisfied.
4. The verifiers accept if they accept each iteration of the zero-knowledge protocol when the space-time constraints were satisfied and if $F \leq \lceil \lambda R \rceil$.

FIG. 2: Full loss-tolerant relativistic zero-knowledge protocol for NP

2. \mathcal{V}_1 and \mathcal{P}_1 (resp. $\mathcal{V}_2, \mathcal{P}_2$) are in different cities and communicate through the usual internet. For each i , $\mathcal{V}_i, \mathcal{P}_i$ are about 400km away. We put $\mathcal{V}_1, \mathcal{V}_2$ at distance about 9000km.

These scenarios are illustrated by the following, with examples of cities for which these constraints are satisfied, see Figure 3.

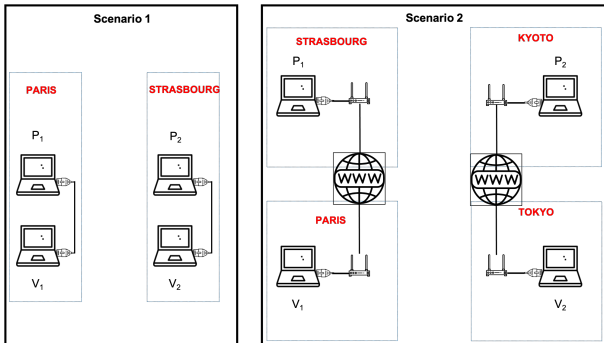


FIG. 3: Scenarios that we consider for which we demonstrate the feasibility of our full relativistic zero-knowledge protocol for NP.

c. Specific implementation parameters. Our main protocol that achieves 100 bits of quantum security has the following parameters that appear in the two scenar-

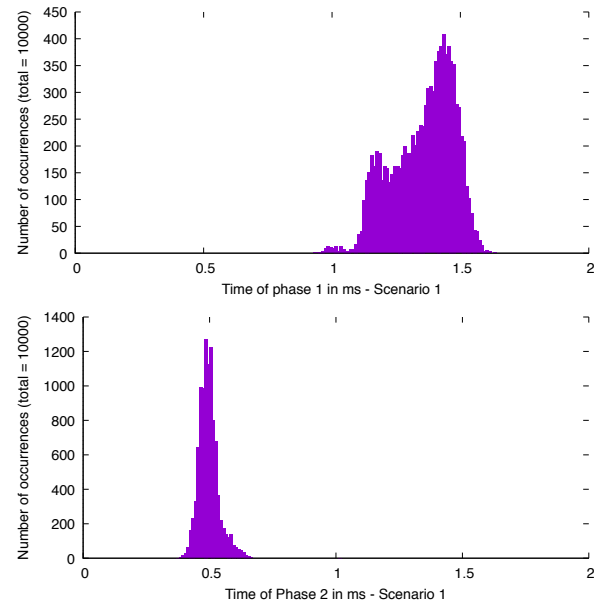


FIG. 4: T^{Phase1} and T^{Phase2} for Scenario 1 with 10000 rounds, times are aggregated in intervals of size 0.01ms.

ios.

$$n = 1704, k = 769, w = 216$$

$$R = 340, F = 22, Q = 2^{23209} - 1, \omega^*(G_{\text{Stern}}^{\text{rel}}) \leq \frac{2}{3} + 2^{-138}$$

Let D be the distance between \mathcal{V}_1 and \mathcal{V}_2 and let D' be the distance between $\mathcal{V}_1, \mathcal{P}_1$ (and also between $\mathcal{V}_2, \mathcal{P}_2$). Depending on our scenario, we have the following parameters; where $c \approx 299.8 \text{ km/sec}$ is the speed of light in vacuum.

1. Scenario 1: $D = 400 \text{ km}$, $D' = 10 \text{ m}$, $D/c \approx 1.33 \text{ ms}$, $\Delta_T = 2 \text{ ms}$, $T_{\text{shift}} = 0.5 \text{ ms}$. With these parameters, the space-time constraints are satisfied for $T_i^{\text{Phase1}} < 1.83 \text{ ms}$ and $T_i^{\text{Phase2}} < 0.83 \text{ ms}$.
2. Scenario 2: $D = 9000 \text{ km}$, $D' = 400 \text{ km}$, $D/c \approx 30 \text{ ms}$, $\Delta_T = 40 \text{ ms}$, $T_{\text{shift}} = 2.5 \text{ ms}$. With these parameters, the space-time constraints are satisfied for $T_i^{\text{Phase1}} < 32.5 \text{ ms}$ and $T_i^{\text{Phase2}} < 27.5 \text{ ms}$.

We show in Figures 4 and 5 the real running times of the different phases.

In order to prove soundness, the probability that a cheating prover succeeds in the No case is bounded by $P^*(R, F)$. If we use Equation D1 from Appendix D with $\omega^*(G_{\text{Stern}}^{\text{rel}}) \leq \frac{2}{3} + 2^{-138}$ and $\lambda = \frac{22}{340}$, we obtain $P^*(R, F) \leq 2^{-103}$. For the completeness error, we estimate the probability that the space-time constraint is not satisfied with $p_{\text{loss}} \leq \frac{1}{1000}$, which is larger than what we actually observe. With this estimate, if we define $CE(R, F, p_{\text{loss}})$ the probability of failure in the honest case, we obtain from Equation D2 that $CE(R, F, p_{\text{loss}}) \leq 2^{-102}$. We therefore get the following results, valid for the 2 scenarios:

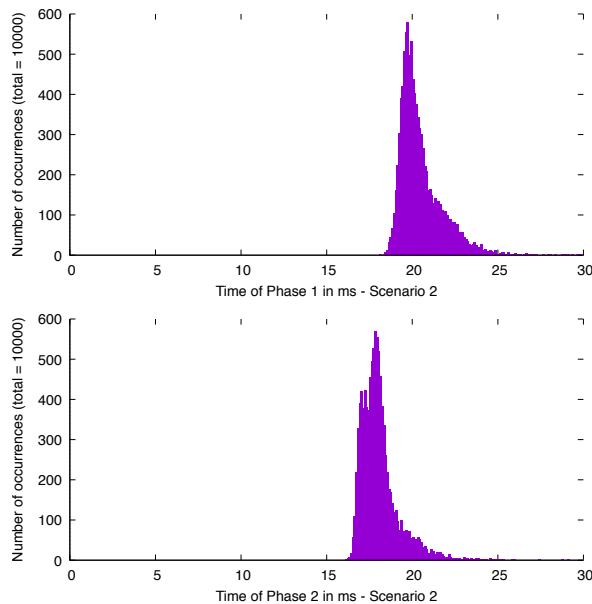


FIG. 5: T^{Phase1} and T^{Phase2} for Scenario 2 with 10000 rounds, times are aggregated in intervals of size 0.1ms .

Theorem 2. *In our experiments, the probability that the verifier rejects an honest run of the protocol is 2^{-102} (Completeness error), the soundness is 2^{-103} and it is perfect zero-knowledge.*

We performed the benchmarks with our working laptops and desktops both in Paris and Strasbourg. In

this first scenario, we actually connected two desktops from the same local network of our research group. In the second scenario, we performed a communication between our local laptop in Paris and a distant desktop in Strasbourg, which is 400km away. We use this setup both for analyzing the running time of our protocol between $\mathcal{P}_1, \mathcal{V}_1$ and $\mathcal{P}_2, \mathcal{V}_2$ in the 2 scenarios. While we didn't perform a fully integrated implementation into a larger cryptographic protocol, the results we obtain show the feasibility and practicality of our relativistic scheme. Also, it is quite flexible on the locations of the verifiers, as shows by our 2 scenarios and we don't use dedicated hardware for the communication and the computation so one could have even more flexibility with better hardware but again, our goal was to show that this protocol can be implemented without specific hardware. Experimental hardwares are Intel Xeon E5-2650 v3 @2.3 GHz (Haswell) and Intel Core i5-6300U CPU @2.4 GHz (Skylake). Our C code does not use parallelism, and was compiled using the GNU C Compiler 7.5.0, and the GNU Multiple Precision Arithmetic Library (<https://gmplib.org/>) to perform arithmetic operations in \mathbb{F}_Q (with $Q = 2^{23 \cdot 209} - 1$ in our example).

We also did experiments for other values of n to show to what extent n can be increased before the space-time constraints are not verified anymore. We present our data with increased n in Appendix E and if one requires a larger security, it is always possible to make $\mathcal{V}_1, \mathcal{V}_2$ farther away or to use better hardware.

Acknowledgments. AC and YB were supported by ANR DEREK <ANR-16-CE39-0001-01>.

-
- [ABC⁺21] Pouriya Alikhani, Nicolas Brunner, Claude Crépeau, Sébastien Designolle, Raphaël Houlmann, Weixu Shi, and Hugo Zbinden. Experimental relativistic zero-knowledge proofs. *Nature* 599, 47-50, 2021.
- [BB84] Bennett and Brassard. Quantum cryptography: Public key distribution and coin tossing. in Proc. Of IEEE Inter. Conf. on Computer Systems and Signal Processing, Bangalore, Karnataka, (Institute of Electrical and Electronics Engineers, New York, 1984.
- [BGKW88] Michael Ben-Or, Shafi Goldwasser, Joe Kilian, and Avi Wigderson. Multi-prover interactive proofs: How to remove intractability assumptions. In *STOC*, 1988.
- [Bjö14] Andreas Björklund. Determinant sums for undirected hamiltonicity. 43(1):280-299, 2014.
- [CCL15] Kaushik Chakraborty, André Chailloux, and Anthony Leverrier. Arbitrarily long relativistic bit commitment. *arXiv preprint arXiv:1507.00239*, 2015.
- [CL17] André Chailloux and Anthony Leverrier. Relativistic (or 2-prover 1-round) zero-knowledge protocol for np secure against quantum adversaries. In *EUROCRYPT'17*, pages 369-396, 2017.
- [CMS⁺20] Claude Crépeau, Arnaud Y. Massenet, Louis Salvail, Lucas Shigeru Stinchcombe, and Nan Yang. Practical Relativistic Zero-Knowledge for NP. In *ITC'20*, volume 163 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 4:1-4:18, 2020.
- [CSST11] Claude Crépeau, Louis Salvail, Jean-Raymond Simard, and Alain Tapp. Two provers in isolation. In *Advances in Cryptology-ASIACRYPT 2011*, pages 407-430. Springer, 2011.
- [FF15] Serge Fehr and Max Fillinger. On the composition of two-prover commitments, and applications to multi-round relativistic commitments. *arXiv preprint arXiv:1507.00240v1*, 2015.
- [Ken99] Adrian Kent. Unconditionally secure bit commitment. *Phys. Rev. Lett.*, 83:1447-1450, Aug 1999.
- [Ken11] Adrian Kent. Unconditionally secure bit commitment with flying qudits. *New Journal of Physics*, 13(11):113015, 2011.
- [Ken12] Adrian Kent. Unconditionally secure bit commitment by transmitting measurement outcomes. *Phys. Rev. Lett.*, 109:130501, Sep 2012.
- [KT17] Ghazal Kachigar and Jean-Pierre Tillich. Quantum information set decoding algorithms. In Tanja Lange and Tsuyoshi Takagi, editors, *Post-Quantum Cryptography*, pages 69-89, Cham, 2017. Springer International Publishing.
- [KTHW13] Jed Kaniewski, Marco Tomamichel, Esther Hanggi, and Stephanie Wehner. Secure bit commitment

- from relativistic constraints. *Information Theory, IEEE Transactions on*, 59(7):4687–4699, 2013.
- [LC97] Hoi-Kwong Lo and H. F. Chau. Is quantum bit commitment really possible? *Phys. Rev. Lett.*, 78(17):3410–3413, Apr 1997.
- [LKB⁺15] T. Lunghi, J. Kaniewski, F. Bussi eres, R. Houlmann, M. Tomamichel, S. Wehner, and H. Zbinden. Practical relativistic bit commitment. *Phys. Rev. Lett.*, 115:030502, Jul 2015.
- [May97] Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.*, 78(17):3414–3417, Apr 1997.
- [Mer90] N. David Mermin. Simple unified form for the major no-hidden-variables theorems. *Phys. Rev. Lett.*, 65:3373–3376, Dec 1990.
- [NC00] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, New York, NY, USA, 2000.
- [Per90] Asher Peres. Incompatible results of quantum measurements. *Physics Letters A*, 151(3-4):107–108, 1990.
- [Ste93] Jacques Stern. A new identification scheme based on syndrome decoding. In Douglas R. Stinson, editor, *Advances in Cryptology — CRYPTO’ 93*, pages 13–21, Berlin, Heidelberg, 1993. Springer Berlin Heidelberg.
- [VMH⁺16] Ephanielle Verbanis, Anthony Martin, Rapha el Houlmann, Gianluca Boso, F elix Bussi eres, and Hugo Zbinden. 24-hour relativistic bit commitment. *Phys. Rev. Lett.*, 117:140506, Sep 2016.

Appendix A: Comparison between the different existing schemes

The authors of [ABC⁺21] use parameters for which they have 100 bits of security. This means both the underlying NP-instance should require time 2^{100} to solve using the best quantum algorithms and the soundness should be 2^{-100} . We will use this benchmarking for comparing the different schemes.

- For [CL17]. The best algorithm for Hamiltonian cycle on a graph G with n vertices runs in time $O(1.657^n)$ [Bjö14] so we need $n \geq 138$ in order to achieve 100 bits of security. The best running time is actually performed by a classical algorithm, we don't know a better quantum algorithm for this problem. This protocol requires to commit each bit of the upper triangle of the adjacency matrix of G using the relativistic \mathbb{F}_Q bit commitment scheme with $Q > 10000n!$ (to have soundness close to $1/2$) so each round of communication requires at least $2 * \frac{n(n-1)}{2} \log_2(10000 * Q)$ bits of communication. $\frac{n(n-1)}{2}$ is the number of bits in the upper triangle of the adjacency matrix. The factor 2 comes from the fact that the verifier first sends $\frac{n(n-1)}{2}$ elements of \mathbb{F}_Q and then the prover sends back $\frac{n(n-1)}{2}$ elements of \mathbb{F}_Q . For $n = 138$, this gives a communication of $1.51 \cdot 10^7$ bits which is approximately 1.89 MBytes. In order to achieve soundness of 2^{-100} , we use 100 rounds since each round has soundness $\frac{1}{2}$.
- The protocol of [CMS⁺20] and its implementation in [ABC⁺21] uses a graph G with 588 vertices and 1097 edges. The communication is essentially sending an edge which is of size less than 2 bytes. In order to achieve a soundness of 2^{-100} , the number of repetition they use is 10^6 . These parameters achieve classical security. If we wanted to achieve quantum security, [ABC⁺21] claims that this would require $(21 * |E|)^4 * 100$ which is more than 10^{19} , as well as a third prover/verifier pair.
- The best quantum algorithm for random instances of the syndrome decoding problem requires time at least $2^{0.05869n}$ [KT17] for $k \approx 0.4514n$ and $w \approx 0.1268n$. Our protocol uses $n = 1704, k = 769, w = 216$ in order to have 100 bits of security. At each round, we have to commit to 3 strings of \mathbb{F}_Q which means the communication at each round is $6 \log_2(Q)$. We can prove security of our scheme by taking $Q = 10^{12} n! 2^{4n}$, so the communication is $6 \log_2(Q) = 136177$ bits which is equal to 17.03 KB. The number of rounds we take is 340, which allows our protocol to be loss tolerant.

Appendix B: Stern's zero-knowledge protocol for the syndrome decoding problem

We now describe Stern's zero-knowledge protocol [Ste93] for the Syndrome Decoding problem. It uses a commitment scheme that we don't explicit here.

Stern's single round zero-knowledge protocol for SD.

Input: Integers k, w , a matrix $\mathbf{H} \stackrel{\$}{\leftarrow} \{0, 1\}^{(n-k) \times n}$, a column vector (called the syndrome) $\mathbf{s} \in \{0, 1\}^{n-k}$.

Auxiliary input: A column vector $\mathbf{e} \in \{0, 1\}^n$ such that $|\mathbf{e}|_H = w$ and $\mathbf{H}\mathbf{e} = \mathbf{s}$.

Protocol:

1. The prover picks a random permutation σ acting on $[n]$ and a random column vector $\mathbf{t} \in \{0, 1\}^n$. Let $\mathbf{s}' = \mathbf{H}\mathbf{t}$, $z_1 = (\sigma||\mathbf{s}')$, $z_2 = \sigma(\mathbf{t})$, $z_3 = \sigma(\mathbf{t} \oplus \mathbf{e})$, where permuting a vector means permuting its coordinates. He commits to z_1, z_2 and z_3 separately and sends these commitments y_1, y_2, y_3 .
2. The verifier sends a uniformly random challenge $c \in \{1, 2, 3\}$.
3. The prover opens $z_{c'}$ for the two values c' different from c .
4. The verifier checks the validity of the 2 commitments and also performs the following checks:
 - if $c = 1$, accept iff. $|z_2 + z_3|_H = w$.
 - if $c = 2$, accept iff. $\mathbf{H} \cdot \sigma^{-1}(z_3) = \mathbf{s} \oplus \mathbf{s}'$.
 - if $c = 3$, accept iff. $\mathbf{H} \cdot \sigma^{-1}(z_2) = \mathbf{s}'$.

This protocol was shown to be secure in [Ste93]. We reproduce here the main aspects of this proof.

a. Completeness The protocol has perfect completeness. Indeed, in the honest case:

1. $|z_2 + z_3|_H = |\sigma(\mathbf{t}) \oplus \sigma(\mathbf{t} \oplus \mathbf{e})|_H = |\sigma(\mathbf{e})|_H = w$.
2. $\mathbf{H} \cdot \sigma^{-1}(\sigma(\mathbf{t} \oplus \mathbf{e})) = \mathbf{H}\mathbf{t} \oplus \mathbf{H}\mathbf{e} = \mathbf{s} \oplus \mathbf{s}'$.
3. $\mathbf{H} \cdot \sigma^{-1}(\sigma(\mathbf{t})) = \mathbf{H}\mathbf{t} = \mathbf{s}'$.

b. Soundness We are in the NO case, so there are no vectors \mathbf{e} such that $|\mathbf{e}|_H = w$ and $\mathbf{H}\mathbf{e} = \mathbf{s}$. We will prove a proposition which is closely related to the soundness (more precisely the 3-special soundness) of the scheme.

Proposition 1. *In the NO case, assume the prover manages to successfully answer the 3 challenges at the same time for the same first message, then he is able to successfully produce 2 different openings for the same commitment.*

Proof. We will prove this proposition by contradiction. We are in the NO case, and assume the prover successfully answers the 3 challenges from the same first message $M_1 = y_1, y_2, y_3$. Assume by contradiction that for each challenge, he uses the same openings for the commitment y_1, y_2, y_3 , which we call $z_1 = (\sigma||\mathbf{s}')$, z_2, z_3 . Let

$\mathbf{e}_0 = \sigma^{-1}(z_2) \oplus \sigma^{-1}(z_3) = \sigma^{-1}(z_2 \oplus z_3)$. Since the prover successfully answers challenge 1, we have $|z_2 \oplus z_3|_H = w$ hence $|\mathbf{e}_0|_H = w$. Moreover, since he successfully answers challenges 2 and 3, we have

$$\mathbf{H}\mathbf{e}_0 = \mathbf{H}(\sigma^{-1}(z_2) + \sigma^{-1}(z_3)) = \mathbf{s} \oplus \mathbf{s}' \oplus \mathbf{s}' = \mathbf{s}.$$

Since we are in the NO case, such an \mathbf{e}_0 doesn't exist, hence the contradiction. \square

This means that a cheating prover can cheat with probability at most $\frac{2}{3}$ unless he is able to break the binding property of the commitment scheme.

c. Zero-knowledge The protocol is known to be zero-knowledge if the commitment scheme is hiding, we sketch the proof here. The verifier doesn't get any information from the commitments from the hiding property of the commitment scheme. If the verifier sends the challenge $c = 1$, he receives $\sigma(\mathbf{t})$ and $\sigma(\mathbf{t} + \mathbf{e})$ from which he cannot recover any information because σ is unknown. For the challenge $c = 2$, he receives $\sigma, \mathbf{s}', \sigma(\mathbf{t} + \mathbf{e})$ hence he can recover $\mathbf{t} + \mathbf{e}$. However, since \mathbf{t} is unknown, this looks like a random vector. For the challenge $c = 3$ he receives $\sigma, \mathbf{s}', \sigma(\mathbf{t})$, which are random elements independent of \mathbf{e} .

Appendix C: Proof of the security of our 1 round relativistic zero-knowledge protocol

The goal of this section is to prove the security of our 1-round relativistic zero-knowledge for NP presented in Figure 1.

a. Completeness. Completeness follows directly from the completeness of Stern's single round, and from the fact that the \mathbb{F}_Q string commitment has perfect completeness.

b. Zero-knowledge. Stern's signature scheme is perfectly zero-knowledge if the commitment scheme is perfectly hiding, which is the case of the \mathbb{F}_Q string commitment. Therefore, the protocol is perfectly zero-knowledge. This zero-knowledge property is also preserved when the scheme is repeated sequentially.

c. Soundness. Proving soundness against quantum adversaries, is the main technical challenge of this work. We start from a NO instance meaning that there is no solution to the SD problem and we consider an all powerful cheating prover that wants to convince the verifier such a solution exists.

In all generality, \mathcal{P}_1 and \mathcal{P}_2 can share an entangled state $|\Phi\rangle$. Then \mathcal{P}_1 receives $B = b_1, b_2, b_3$ from \mathcal{V}_1 and \mathcal{P}_2 receives $c \in \{1, 2, 3\}$ from \mathcal{V}_2 . They output respectively $Y = y_1, y_2, y_3$ and $ZA = \{(z_{c'}, a_{c'})\}_{c' \neq c}$. The verifiers then come together and perform the verification step. We assume the timing constraints are verified which ensures that \mathcal{P}_1 has no information about *chall* before sending his

message Y and \mathcal{P}_2 has no information about B_1, B_2, B_3 before sending his message ZA .

Any strategy from the provers can be directly related to the strategy for the following 2-player game where the 2 provers play the role of these 2 players and the verifiers play the role of the referee (*i.e.* they send the random questions to the provers and check the validity of their outputs). This game, that we call $G_{\text{Stern}}^{\text{rel}}$, is defined as follows:

2-player game $G_{\text{Stern}}^{\text{rel}}$

- Alice receives $B = b_1, b_2, b_3 \in_R \mathbb{F}_Q$. Bob receives $c \in_R \{1, 2, 3\}$.
- Alice outputs $Y = y_1, y_2, y_3 \in \mathbb{F}_Q$ and Bob outputs $AZ = \{(a_{c'}, z_{c'})\}_{c' \neq c}$ where each $a_i \in \mathbb{F}_Q$.
- Each z_i is an element of \mathbb{F}_Q but we interpret z_1 as an element (σ, \mathbf{s}') of $S_1 = P_n \times \{0, 1\}^n$. Similarly, we interpret z_2, z_3 as vectors in $\{0, 1\}^n$ using a mapping that we detail after the description of the game. If this mapping fails, the game is lost. Otherwise, we first check the constraint $y_{c'} = a_{c'} + z_{c'} * b_{c'}$ for $c' \neq c$. We then check:
 1. if $c = 1$, we also require $|z_2 + z_3|_H = w$.
 2. if $c = 2$, we also require $\mathbf{H} \cdot \sigma^{-1}(z_3) = \mathbf{s} \oplus \mathbf{s}'$.
 3. if $c = 3$, we also require $\mathbf{H} \cdot \sigma^{-1}(z_2) = \mathbf{s}'$.

The “+” and “*” operations we use are the one in $\mathbb{F}_Q = \{\bar{0}, \dots, \overline{Q-1}\}$ where \bar{i} is the i^{th} element of \mathbb{F}_Q . We do our mapping as follows: If $z_1 \in \{\bar{0}, \dots, \overline{S_1-1}\}$, then we map z_1 to the z_1^{th} element of S_1 , otherwise, we say that the mapping fails. We do the same thing for z_2, z_3 , if they are in $\{\bar{0}, \dots, \overline{2^n-1}\}$ then we can map them to binary vectors, otherwise, we say that the mapping fails. In order for this mapping to be well defined, we must take Q large enough, more precisely $Q \geq |S_1|$ and $Q \geq 2^n$.

What is the optimal cheating strategy we can expect for this game? There are some strategies that can win Stern's single round zero-knowledge protocol with probability $\frac{2}{3}$ [Ste93] from which we can directly derive strategies for this game with 2 classical players that win wp. $\frac{2}{3}$. This means we have strategies for which the players win for 2 possible challenges for Bob but not for the third one.

So what we want to show is that there is no strategy for which the players will win for the 3 challenges received by Bob. What we know from Proposition 1 is that they can't give answers for the 3 challenges simultaneously but this doesn't mean they can't answer each challenge separately. This behavior can appear when we consider entangled strategies. For example in magic square game [Mer90, Per90], Alice and Bob can't answer all questions at the same time — because all the constraints of the magic square game lead to a contradiction. However, the

entangled value of the game is still 1.

Our main contribution is to bound the entangled value of $G_{\text{Stern}}^{\text{rel}}$. As Q increases, the entangled value converges to $\frac{2}{3}$ which is optimal. We prove the following theorem

Theorem 3.

$$\omega^*(G_{\text{Stern}}^{\text{rel}}) \leq \frac{2}{3} + \left(\frac{n!2^{4n}}{Q}\right)^{1/4}.$$

From this theorem, our result on the soundness of our 1-round relativistic scheme will follow immediately. In the next section, we will prove the bound in $\omega^*(G_{\text{Stern}}^{\text{rel}})$.

1. Bounding the value of the game

We can now prove our lower bound on the entangled value of $G_{\text{Stern}}^{\text{rel}}$.

Proof of the lower bound of the game. Let any $\delta > 0$ and consider a finite dimensional projective strategy for Alice and Bob that wins the game $G_{\text{Stern}}^{\text{rel}}$ wp. $\omega^*(G_{\text{Stern}}^{\text{rel}}) - \delta$.

Let $P^B = \{P_Y^B\}$ and $Q^c = \{Q_A^c\}$ be respectively Alice's and Bob's projective measurements for their respective inputs $B = b_1, b_2, b_3$ and c . Alice's output is $Y = y_1, y_2, y_3$ and Bob's output AZ corresponds to the 2 pairs $(a_{c'}, z_{c'})$ for $c' \neq c$, starting with the one with smallest index. Let $|\psi\rangle$ be the quantum state they share.

Fix an input/output pair BY for Alice and let σ^{BY} be the state held by Bob, conditioned on this pair. For each $c \in \{1, 2, 3\}$, let $W_c = \{AZ : V(Y, AZ, B, c) = 1\}$ be the set of winning outputs for Bob where $V(Y, AZ, B, c)$ is the function that outputs 1 if the game is won on inputs/outputs $(B, c)/(Y, AZ)$, and outputs 0 otherwise.

A necessary condition of validity (for a fixed BY), is that $y_i = a_i + b_i * z_i$ for the z_i revealed so for each z_i , there is a unique valid a_i which is $y_i - b_i * z_i$. For $c = 1$, Bob outputs a_2, z_2, a_3, z_3 . A necessary condition is that z_2, z_3 can each be mapped into the set of binary vectors. Since there is a 1 to 1 correspondence between z_i and a_i , we have $|W_1| \leq 2^{2n}$. For $c = 2$, Bob outputs a_1, z_1, a_3, z_3 . A necessary condition is that z_1 can be mapped to an element (π, \mathbf{s}') where π is a permutation on $[n]$ and $\mathbf{s}' \in \{0, 1\}^n$ and z_3 has to be mapped to a binary vector, which implies $|W_2| \leq 2^n n! \cdot 2^n = 2^{2n} n!$. A similar reasoning for $c = 3$ gives $|W_3| \leq 2^{2n} n!$.

For each $c \in \{1, 2, 3\}$, let $Q_W^c = \sum_{AZ \in W_c} Q_{AZ}^c$ the projector on the winning outputs for Bob on input c (for the fixed input/output pair BX of Alice). Let V^{BX} be the probability that Alice and Bob win the game for this input. We have

$$V^{BX} = \frac{1}{3} \sum_{c \in \{1, 2, 3\}} \text{tr}(Q_W^c \sigma^{BX}).$$

and also $\mathbb{E}_{BX}[V^{BX}] = \omega^*(G_{\text{Stern}}^{\text{rel}}) - \delta$. We now consider the following quantum strategy for Bob that will make him succeed on the 3 challenges: wp. $\frac{1}{2}$, run Q^1 to get

output AZ_1 , then on the resulting state, run Q^2 to get output AZ_2 and on the resulting state, run Q^3 to get output AZ_3 . Wp. $\frac{1}{2}$, do the same thing but swap the order of Q^1 and Q^2 . Let E^{BX} be the probability of success of this strategy. We can write

$$E^{BX} = \frac{1}{2} \left(\sum_{\substack{AZ_1 \in W_1 \\ AZ_2 \in W_2 \\ AZ_3 \in W_3}} \text{tr}(Q_{AZ_3}^3 Q_{AZ_2}^2 Q_{AZ_1}^1 \sigma^{BX} Q_{AZ_1}^1 Q_{AZ_2}^2) + \text{tr}(Q_{AZ_3}^3 Q_{AZ_1}^1 Q_{AZ_2}^2 \sigma^{BX} Q_{AZ_2}^2 Q_{AZ_1}^1) \right)$$

Notice that for any 3 projectors, P_1, P_2, P_3 , we have $\text{tr}(P_3 P_2 P_1 \sigma P_1 P_2 P_3) = \text{tr}(P_3^2 P_2 P_1 \sigma P_1 P_2) = \text{tr}(P_3 P_2 P_1 \sigma P_1 P_2)$ hence the expression E^{BX} .

In order to conclude, we use the 2 following equations, which will be proven in upcoming proposition. The first one

$$\mathbb{E}_{BX}[E^{BX}] = \frac{1}{Q}, \quad (\text{C1})$$

claims that our strategy will succeed in answering valid outputs A_1, A_2, A_3 for the 3 challenges wp. at most $\frac{1}{Q}$. In high level, this is a direct consequence of Proposition 1 and of the binding property of the \mathbb{F}_Q -relativistic commitment scheme, but we prove this claim from scratch. We then relate E_{BX} and V_{BX} using a generic proposition on projectors

$$E^{BX} \geq \frac{9(V^{BX} - \frac{2}{3})^4}{2|W_1||W_2|}. \quad (\text{C2})$$

Proving this inequality is actually where we had most of the technical difficulty. In order to prove this statement, we generalized the approach of [CL17] to 3 measurements and showed that if you can win for the 3 challenges at the same time wp. at most $\frac{1}{Q}$ then a quantum adversary can win at most wp. $\frac{2}{3} + \varepsilon$ where ε is vanishingly small for Q large enough.

We first conclude and then go on proving Equations C1 and C2. To conclude our proof, we have from Equation C2 that

$$E^{BX} \geq \frac{9(V^{BX} - \frac{2}{3})^4}{2 \cdot 2^{4n} n!}.$$

By taking the expectation on each side, we obtain

$$\frac{1}{Q} = \mathbb{E}_{BX}[E^{BX}] \geq \mathbb{E}_{BX}\left[\frac{9(V^{BX} - \frac{2}{3})^4}{2 \cdot 2^{4n} n!}\right] \geq \frac{9(\omega^*(G_{\text{Stern}}^{\text{rel}}) - \delta - \frac{2}{3})^4}{2 \cdot 2^{4n} n!}$$

where we used the convexity of the function $x \mapsto x^4 - \frac{2}{3}$. Since this holds for any $\delta > 0$, we take $\delta \rightarrow 0$ and have

$$\frac{1}{Q} \geq \frac{9(\omega^*(G_{\text{Stern}}^{\text{rel}}) - \frac{2}{3})^4}{2 \cdot 2^{4n} n!}.$$

□

We now prove our two equations. We first prove the following

Lemma 1 (Equation C1). *In the NO case, the probability that Bob successfully outputs 3 valid couples (AZ_1, AZ_2, AZ_3) , on average on BY is at most $\frac{1}{Q}$.*

Proof. Fix an input/output BY with $B = b_1, b_2, b_3$ and $Y = y_1, y_2, y_3$. Assume by contradiction that Bob can output 3 valid couples AZ_1, AZ_2, AZ_3 with $AZ_c = (a_{c'_1}^c, z_{c'_1}^c), (a_{c'_2}^c, z_{c'_2}^c)$ for the 2 different values $c'_1, c'_2 \neq c$. Assume by contradiction that $z_1^2 = z_1^3 = z_1, z_2^1 = z_2^3 = z_2, z_3^1 = z_3^2 = z_3$. We map z_1 to a pair (σ, σ') , z_2, z_3 to vectors $\in \{0, 1\}^n$. Passing the 3 winning conditions implies that

$$\mathbf{H}\sigma^{-1}(z_2 + z_3) = \mathbf{s} \quad \text{and} \quad |\sigma^{-1}(z_2 + z_3)| = w.$$

This implies that $\sigma^{-1}(z_2 + z_3)$ is a solution to the syndrome decoding problem but since we are in the NO case, such a solution doesn't exist hence the contradiction.

This means there exists $c' \in \{1, 2, 3\}$ st. $z_{c'_1}^{c'} \neq z_{c'_2}^{c'}$ for the two values $c_1, c_2 \neq c'$. Because these are valid answers, this means we have

$$\begin{aligned} z_{c'_1}^{c_1} * b_{c'} &= y_{c'} - a_{c'_1}^{c_1} \\ z_{c'_2}^{c_2} * b_{c'} &= y_{c'} - a_{c'_2}^{c_2} \end{aligned}$$

From which we get

$$b_{c'} = (a_{c'_2}^{c_2} - a_{c'_1}^{c_1}) / (z_{c'_1}^{c_1} - z_{c'_2}^{c_2}).$$

where $/$ is the division in \mathbb{F}_Q . From there, this means Bob can guess $b_{c'}$ but from non-signaling, Bob should have no information about $b_{c'}$. Moreover, notice that Bob knows which c' to take, it is the index where $z_{c'_1}^{c_1} \neq z_{c'_2}^{c_2}$. Since $b_{c'}$ is a random element from \mathbb{F}_Q , we conclude that Bob can guess this value wp. $\frac{1}{Q}$ which concludes the proof. \square

The next section is devoted to the proof of the second equation.

2. Proof of Equation C2

We prove the following

Proposition 2. *Consider 3 projectors P_1, P_2, P_3 such that for each $i \in \{1, 2, 3\}$, we can write $P_i = \sum_{s_i=1}^{S_i} P_i^{s_i}$ where for each i , the $\{P_i^{s_i}\}$ are orthogonal projectors meaning that $P_i^s P_i^{s'} = \delta_{s,s'} P_i^s$. Let σ be any quantum state. Let $V = \sum_i \text{tr}(P_i \sigma)$ and*

$$\begin{aligned} E &= \frac{1}{2} \left(\sum_{s_3=1}^{S_3} \sum_{s_2=1}^{S_2} \sum_{s_1=1}^{S_1} \text{tr}(P_3^{s_3} P_2^{s_2} P_1^{s_1} \sigma (P_1^{s_1}) (P_2^{s_2})) + \right. \\ &\quad \left. \sum_{s_3=1}^{S_3} \sum_{s_2=1}^{S_2} \sum_{s_1=1}^{S_1} \text{tr}(P_3^{s_3} P_1^{s_1} P_2^{s_2} \sigma (P_2^{s_2}) (P_1^{s_1})) \right). \end{aligned}$$

We have $E \geq \frac{9(V - \frac{2}{3})^4}{2S_1 S_2}$.

In order to prove our proposition, we first need the following trigonometric lemma.

Lemma 2. $\forall \alpha_1, \alpha_2 \in [0, \pi/2[$ st. $\cos^2(\alpha_1) + \cos^2(\alpha_2) > 1$, if we define $c_1 = \cos(\alpha_1), c_2 = \cos(\alpha_2), s_1 = \sin(\alpha_1), s_2 = \sin(\alpha_2)$, we have

$$\min_{y \in [-s_1, s_1]} \left\{ \frac{c_2^2 (c_1 c_2 + y s_2)^2}{(c_1 c_2 + y s_2)^2 + s_1^2 - y^2} \right\} \geq c_1^2 + c_2^2 - 1.$$

Proof. Let $t_1 = \tan(\alpha_1)$ and $t_2 = \tan(\alpha_2)$. Since $c_1^2 + c_2^2 > 1$, we have $\alpha_1 + \alpha_2 < \pi/2$ and $t_1 t_2 < 1$. Let also

$$T(y) = (c_1 c_2 + y s_2)^2 \quad ; \quad U(y) = s_1^2 - y^2.$$

Our goal is hence to minimize the function

$$f(y) = \frac{c_2^2 T(y)}{T(y) + U(y)} \quad \text{for } y \in [-s_1, s_1].$$

We write

$$\begin{aligned} f'(y) &= \frac{c_2^2 T'(y) (T(y) + U(y)) - c_2^2 T(y) (T'(y) + U'(y))}{(T(y) + U(y))^2} \\ &= \frac{c_2^2 (T'(y) U(y) - T(y) U'(y))}{(T(y) + U(y))^2} \end{aligned}$$

and

$$\begin{aligned} Z_0 &= T'(y) U(y) - T(y) U'(y) \\ &= (2y s_2^2 + 2c_1 c_2 s_2)(s_1^2 - y^2) - (y^2 s_2^2 + 2y c_1 c_2 s_2 + c_1^2 c_2^2)(-2y) \\ &= 2y^2 (c_1 c_2 s_2) + 2y (s_1^2 s_2^2 + c_1^2 c_2^2) + 2c_1 c_2 s_1^2 s_2 \\ &= 2c_1 c_2 s_2 \left(y + \frac{s_1^2 s_2}{c_1 c_2} \right) \left(y + \frac{c_1 c_2}{s_2} \right) \end{aligned}$$

This implies the equation $f'(y) = 0$ has 2 solutions $y_0 = -\frac{s_1^2 s_2}{c_1 c_2} = -s_1 t_1 t_2$ and $y_1 = -\frac{c_1 c_2}{s_2} = -\frac{s_1}{t_1 t_2}$. Notice that only y_0 lies in the interval $[-s_1, s_1]$ since $t_1 t_2 < 1$.

We now write $f(-s_1) = f(s_1) = c_2^2$ and

$$T(y_0) = \frac{1}{c_1^2 c_2^2} (c_1^2 c_2^2 - s_1^2 s_2^2)^2$$

$$U(y_0) = \frac{s_1^2}{c_1^2 c_2^2} (c_1^2 c_2^2 - s_1^2 s_2^2)$$

which implies

$$\begin{aligned} f(y_0) &= \frac{c_2^2 (c_1^2 c_2^2 - s_1^2 s_2^2)}{(c_1^2 c_2^2 - s_1^2 s_2^2) + s_1^2} \\ &= c_2^2 - s_1^2 \quad \text{using } (c_1^2 c_2^2 - s_1^2 s_2^2) = c_2^2 - s_1^2 \\ &= c_1^2 + c_2^2 - 1 \end{aligned}$$

In order to conclude, we write

$$f(-s_1) = c_2^2 ; f(s_1) = c_2^2 ; f(y_0) = c_1^2 + c_2^2 - 1 \leq f(s_1).$$

Since y_0 is the unique point in $[-s_1, s_1]$ such that $f'(y_0) = 0$ we can conclude that

$$\min_{y \in [-s_1, s_1]} \{f(y)\} = f(y_0) = c_1^2 + c_2^2 - 1.$$

\square

We now prove our proposition for the special case $S_1, S_2 = 1$ and for a pure state $|\Omega\rangle$ instead of σ .

Proposition 3. *Let $|\Omega\rangle$ be a quantum state. Let P_1, P_2, P_3 be projectors. Let $V = \frac{1}{3} \|P_i|\Omega\rangle\|^2 = \frac{2}{3} + \varepsilon$ with $\varepsilon \geq 0$ and $E = \frac{1}{2} (\|P_3P_2P_1|\Omega\rangle\|^2 + \|P_3P_1P_2|\Omega\rangle\|^2)$. We have $E \geq \frac{9\varepsilon^4}{2}$.*

Proof. Let $|\phi_i\rangle = \frac{P_i|\Omega\rangle}{\|P_i|\Omega\rangle\|}$. We write

$$|\Omega\rangle = \cos(\alpha_i)|\phi_i\rangle + \sin(\alpha_i)|\phi_i^\perp\rangle \quad \text{for } i \in \{1, 2, 3\}. \quad (\text{C3})$$

This means

$$V = \frac{1}{3} (\cos^2(\alpha_1) + \cos^2(\alpha_2) + \cos^2(\alpha_3)).$$

We write

$$|\phi_2\rangle = \cos(\alpha_2)|\Omega\rangle + \sin(\alpha_2)|B\rangle \quad (\text{C4})$$

for some pure state $|B\rangle \perp |\Omega\rangle$ and

$$|\phi_1\rangle = \cos(\alpha_1)|\Omega\rangle + x|A\rangle + y|B\rangle \quad (\text{C5})$$

for some pure state $|A\rangle \perp |B\rangle$ and $|A\rangle \perp |\Omega\rangle$. This means we have

$$\cos^2(\alpha_1) + |x|^2 + |y|^2 = 1. \quad (\text{C6})$$

We also write

$$P_2 = |\phi_2\rangle\langle\phi_2| + P'_2 \quad \text{with } P'_2|\phi_2\rangle = \mathbf{0}. \quad (\text{C7})$$

We have

$$\begin{aligned} |W\rangle &= P_2P_1(|\Omega\rangle) = \cos(\alpha_1)(P_2|\phi_1\rangle) \\ &= \cos(\alpha_1)\langle\phi_1|\phi_2\rangle|\phi_2\rangle + \cos(\alpha_1)P'_2|\phi_1\rangle \end{aligned} \quad (\text{C8})$$

Notice that $P_2|\Omega\rangle = \cos(\alpha_2)|\phi_2\rangle = |\phi_2\rangle\langle\phi_2| \cdot |\Omega\rangle$ hence $P'_2|\Omega\rangle = \mathbf{0}$. This implies that $P'_2|B\rangle = \mathbf{0}$ and

$$P'_2|\phi_1\rangle = P'_2(x|A\rangle) = z|A'\rangle \quad (\text{C9})$$

for some $|A'\rangle$ orthogonal to $|\Omega\rangle$ and $|B\rangle$ and $|z| \leq |x|$. So we rewrite

$$\begin{aligned} \frac{1}{\cos(\alpha_1)}|W\rangle &= \langle\phi_1|\phi_2\rangle|\phi_2\rangle + P'_2|\phi_1\rangle \\ &= (\cos\alpha_1 \cos(\alpha_2) + \sin(\alpha_2)y)|\phi_2\rangle + z|A'\rangle \end{aligned} \quad (\text{C10})$$

Let $u = (\cos\alpha_1 \cos(\alpha_2) + \sin(\alpha_2)y)$ so that

$$|W\rangle = \cos(\alpha_1)u|\phi_2\rangle + \cos(\alpha_1)z|A'\rangle \quad (\text{C11})$$

The norm of $|W\rangle$ is therefore

$$\|W\rangle\| = |\cos(\alpha_1)|\sqrt{|u|^2 + |z|^2}.$$

Let $|\widetilde{W}\rangle = |W\rangle / \|W\rangle\|$. From Equation C11, we have

$$\begin{aligned} |\langle\Omega|\widetilde{W}\rangle|^2 &= \left(\frac{|\cos(\alpha_2)\cos(\alpha_1)u|}{\|W\rangle\|}\right)^2 = \frac{\cos^2(\alpha_2)u^2}{u^2 + z^2} \\ &\geq \frac{\cos^2(\alpha_2)u^2}{u^2 + (1 - \cos^2(\alpha_1) - y^2)}. \end{aligned}$$

Using lemma 2, we obtain $|\langle\Omega|\widetilde{W}\rangle|^2 \geq \cos^2(\alpha_1) + \cos^2(\alpha_2) - 1$. We hence write $|\langle\Omega|\widetilde{W}\rangle|^2 = \cos^2(\beta)$ for some $\beta \leq \alpha_1 + \alpha_2$. In order to conclude, we define $Angle(|\psi\rangle, |\phi\rangle) = \arccos(|\langle\psi|\phi\rangle|)$. The angle function is a distance measure [NC00]. We will use several times the trigonometric inequality $\cos(\rho + \theta) \geq \cos^2(\rho) + \cos^2(\theta) - 1$ for any ρ, θ with $\rho + \theta \leq \pi/2$ and we can hence write

$$\begin{aligned} \|P_3|\widetilde{W}\rangle\|^2 &\geq |\langle\phi_3|\widetilde{W}\rangle|^2 \\ &= \cos^2\left(\text{Angle}\left(|\phi_3\rangle, |\widetilde{W}\rangle\right)\right) \\ &\geq \cos^2\left(\text{Angle}\left(|\phi_3\rangle, |\Omega\rangle\right) + \text{Angle}\left(|\Omega\rangle, |\widetilde{W}\rangle\right)\right) \\ &\geq \cos^2(\alpha_3 + \beta) \\ &\geq (\cos^2(\alpha_3) + \cos^2(\beta) - 1)^2 \\ &= (\cos^2(\alpha_1) + \cos^2(\alpha_2) + \cos^2(\alpha_3) - 2)^2 = \varepsilon^2 \end{aligned}$$

From there, we can conclude

$$\begin{aligned} \|P_3P_2P_1|\Omega\rangle\|^2 &= \|P_3|W\rangle\|^2 = \|P_3|\widetilde{W}\rangle\|^2 \|W\|^2 \\ &\geq \varepsilon^2 \|P_2P_1|\Omega\rangle\|^2 \end{aligned}$$

In order to conclude, we use $|y| \leq \sin(\alpha_1)$ (Equation C6) which gives $|u| \geq \cos(\alpha_1 + \alpha_2)$, and

$$\|P_2P_1|\Omega\rangle\|^2 = \|W\|^2 \geq \cos^2(\alpha_1) \cos^2(\alpha_1 + \alpha_2).$$

which gives

$$\|P_3P_2P_1|\Omega\rangle\|^2 \geq \varepsilon^2 \cos^2(\alpha_1) \cos^2(\alpha_1 + \alpha_2) \quad (\text{C12})$$

Similarly, we have

$$\begin{aligned} \|P_3P_1P_2|\Omega\rangle\|^2 &= \varepsilon^2 \|P_1P_2|\Omega\rangle\|^2 \|P_3|\widetilde{W}\rangle\|^2 \\ &\geq \varepsilon^2 \cos^2(\alpha_2) \cos^2(\alpha_1 + \alpha_2) \end{aligned} \quad (\text{C13})$$

$$\begin{aligned} \frac{1}{2} \left(\|P_3P_2P_1|\Omega\rangle\|^2 + \|P_3P_1P_2|\Omega\rangle\|^2 \right) &\geq \\ &\frac{\varepsilon^2}{2} (\cos^2(\alpha_1) + \cos^2(\alpha_2)) \cos^2(\alpha_1 + \alpha_2) \end{aligned}$$

Now, since $\cos^2(\alpha_1) + \cos^2(\alpha_2) \geq 1 + 3\varepsilon$ (from $V \geq \frac{2}{3} + \varepsilon$), we have $\cos^2(\alpha_1) + \cos^2(\alpha_2) \geq 1$ and $\cos^2(\alpha_1 + \alpha_2) \geq (\cos^2(\alpha_1) + \cos^2(\alpha_2) - 1)^2 = (3\varepsilon)^2$, from which we conclude

$$\frac{1}{2} \left(\|P_3P_2P_1|\Omega\rangle\|^2 + \|P_3P_1P_2|\Omega\rangle\|^2 \right) \geq \frac{9\varepsilon^4}{2}.$$

□

We proved our main proposition for $S_1, S_2 = 1$. From there, we can directly go to the general case in similar way than in [CL17]. We need the following statement

Lemma 3 (Proposition 4 from [CL17]). *Let a projector $P = \sum_{i=1}^m P_i$ where $\{P_i\}_{i \in [m]}$ are orthogonal projectors. For any pure state $|\psi\rangle$, we have*

$$\sum_{i=1}^m P_i |\psi\rangle \langle \psi| P_i \geq \frac{1}{m} P |\psi\rangle \langle \psi| P.$$

With this lemma, we can prove our main proposition.

Proof of Proposition 2. First, in order to use Proposition 3, we need to work on pure states similarly as in [CL17]. Assume σ is a quantum mixed state in some Hilbert space \mathcal{B} and the projectors P_i^s act on \mathcal{B} . We add an extra Hilbert space \mathcal{E} . We consider a purification $|\Omega\rangle$ of σ in $\mathcal{B}\mathcal{E}$ and define $\tilde{P}_i = P_i \otimes I_E$, $\tilde{P}_i^s = P_i^s \otimes I_E$, $\tilde{V} = \sum_i \text{tr}(\tilde{P}_i |\Omega\rangle)$ and

$$\tilde{E} = \frac{1}{2} (\tilde{E}_1 + \tilde{E}_2)$$

with

$$\begin{aligned} \tilde{E}_1 &= \left(\sum_{s_3=1}^{S_3} \sum_{s_2=1}^{S_2} \sum_{s_1=1}^{S_1} \text{tr} \left(\tilde{P}_3^{s_3} \tilde{P}_2^{s_2} \tilde{P}_1^{s_1} |\Omega\rangle \langle \Omega| \left(\tilde{P}_1^{s_1} \right) \left(\tilde{P}_2^{s_2} \right) \right) \right) \\ \tilde{E}_2 &= \sum_{s_3=1}^{S_3} \sum_{s_2=1}^{S_2} \sum_{s_1=1}^{S_1} \text{tr} \left(\tilde{P}_3^{s_3} \tilde{P}_1^{s_1} \tilde{P}_2^{s_2} |\Omega\rangle \langle \Omega| \left(\tilde{P}_2^{s_2} \right) \left(\tilde{P}_1^{s_1} \right) \right). \end{aligned}$$

One can easily check that $\tilde{V} = V$ and $\tilde{E} = E$. Now, using Lemma 3 twice, we have

$$\begin{aligned} \tilde{E}_1 &\geq \frac{1}{S_1} \sum_{s_3=1}^{S_3} \sum_{s_2=1}^{S_2} \text{tr} \left(\tilde{P}_3^{s_3} \tilde{P}_2^{s_2} \tilde{P}_1 |\Omega\rangle \langle \Omega| \tilde{P}_1 \left(\tilde{P}_2^{s_2} \right) \right) \\ &\geq \frac{1}{S_1 S_2} \sum_{s_3=1}^{S_3} \text{tr} \left(\tilde{P}_3^{s_3} \tilde{P}_2 \tilde{P}_1 |\Omega\rangle \langle \Omega| \tilde{P}_1 \tilde{P}_2 \right) \\ &= \frac{1}{S_1 S_2} \text{tr}(\tilde{P}_3 \tilde{P}_2 \tilde{P}_1 |\Omega\rangle \langle \Omega| \tilde{P}_1 \tilde{P}_2) \end{aligned}$$

Similarly, we can prove

$$\tilde{E}_2 \geq \frac{1}{S_1 S_2} \text{tr}(\tilde{P}_3 \tilde{P}_1 \tilde{P}_2 |\Omega\rangle \langle \Omega| \tilde{P}_2 \tilde{P}_1).$$

In order to conclude, we use Proposition 3 which directly gives us the desired result. \square

Appendix D: Security proof of the full scheme and loss-tolerance

1. Analysis of loss tolerance

We consider the R round protocol where we allow at most F aborts and let $\lambda = \frac{F}{R}$. An adversary can of course

use this allowed number of losses to cheat in the protocol. We consider cheating provers and assume here that the hardware is perfect, which can only help the cheating provers. At the first round, the provers can perform a strategy that aborts with probability λ^* and for which they win the game with probability p^* conditioned on not aborting. The probability $P^*(R, F)$ of cheating is therefore

$$P^*(R, F) = \lambda^* P_1 + (1 - \lambda^*) p^* P_2.$$

where P_1 is the probability that the provers win on the $R - 1$ remaining rounds and they have $F - 1$ aborts left, and P_2 is the probability that the provers win on the $R - 1$ remaining rounds and they have F aborts left. While computing P_1 and P_2 is hard, notice that $P_2 \geq P_1$. Moreover, $(1 - \lambda^*) p^* \leq \omega^*(G_{\text{Stern}}^{\text{rel}})$ and $p^* \leq 1$, so $(1 - \lambda^*) p^* \leq \min\{\omega^*(G_{\text{Stern}}^{\text{rel}}), 1 - \lambda^*\}$. We now distinguish 2 cases

- If $\lambda^* \in [0, 1 - \omega^*(G_{\text{Stern}}^{\text{rel}})]$, $P^* \leq \lambda^* P_1 + \omega^*(G_{\text{Stern}}^{\text{rel}}) P_2$ and this right hand side is increasing in λ^* .
- If $\lambda^* \in [1 - \omega^*(G_{\text{Stern}}^{\text{rel}}), 1]$, $P^* \leq \lambda^* P_1 + (1 - \lambda^*) P_2 = P_2 + \lambda^*(P_1 - P_2)$ and this right hand side is decreasing in λ^* since $P_2 \geq P_1$.

This shows that the best strategy for the prover is to take at the first round $\lambda^* = 1 - \omega^*(G_{\text{Stern}}^{\text{rel}})$. Notice that the above reasoning is independent on the number of remaining rounds or the number of allowed aborts. This means the same argument can be applied to each round. From there, we have that the provers optimal strategy at each round is to perform a strategy that aborts wp. $\lambda^* = 1 - \omega^*(G_{\text{Stern}}^{\text{rel}})$. In this case, we potentially have $p^* = 1$ so the provers will win all the games where they don't abort but they will most probably abort too often, for well chosen parameters. Let $P_{\text{losses}}^*(R, F)$ be the probability that the provers perform less than F aborts with this strategy. We use the following Chernoff bound

Proposition 4 (Additive Chernoff bound). *Suppose X_1, \dots, X_n are independent random variables taking value in $\{0, 1\}$. Let X denote their sum, $p = \mathbb{E}[X_1]$ and $\varepsilon > 0$. We have*

$$\begin{aligned} \Pr[X \geq pn + \varepsilon n] &\leq 2^{n((p+\varepsilon) \log_2(\frac{p}{p+\varepsilon}) + (1-p-\varepsilon) \log_2(\frac{1-p-\varepsilon}{1-p}))}, \\ \Pr[X \leq pn - \varepsilon n] &\leq 2^{n((p-\varepsilon) \log_2(\frac{p}{p-\varepsilon}) + (1-p+\varepsilon) \log_2(\frac{1-p}{1-p+\varepsilon}))}. \end{aligned}$$

In our case, the strategy of the provers outputs ‘Abort’ wp. λ^* and they succeed in cheating if there are at most $F = \lambda R$ aborts. We use the above Chernoff bound (second equation) with $n = R$, $p = \lambda^* = 1 - \omega^*(G_{\text{Stern}}^{\text{rel}})$, $\varepsilon = \lambda^* - \lambda$ which bounds the probability that there are less than $F = \lambda n$ aborts, and we write

$$\begin{aligned} P^*(R, F) &\leq 2^R \left(\lambda \log_2 \left(\frac{\lambda^*}{\lambda} \right) + (1 - \lambda) \log_2 \left(\frac{1 - \lambda^*}{1 - \lambda} \right) \right) \\ &= 2^R \left(\lambda \log_2 \left(\frac{1 - \omega^*(G_{\text{Stern}}^{\text{rel}})}{\lambda} \right) + (1 - \lambda) \log_2 \left(\frac{\omega^*(G_{\text{Stern}}^{\text{rel}})}{1 - \lambda} \right) \right) \end{aligned} \quad (\text{D1})$$

2. Analysis of the completeness error

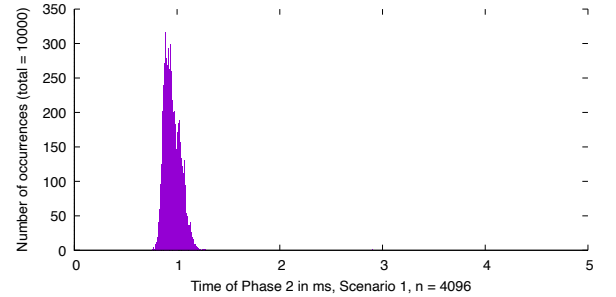
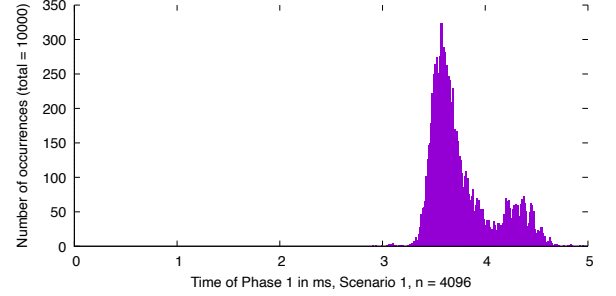
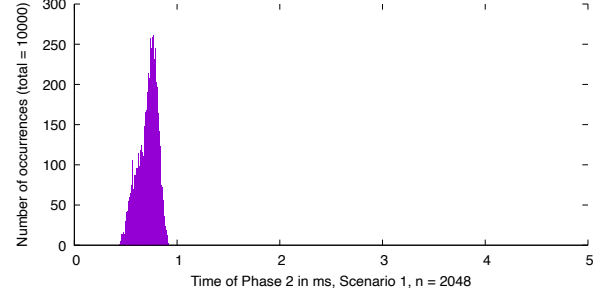
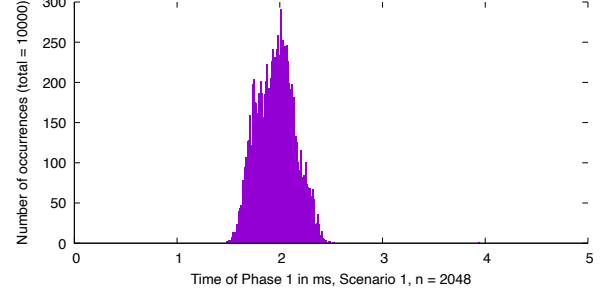
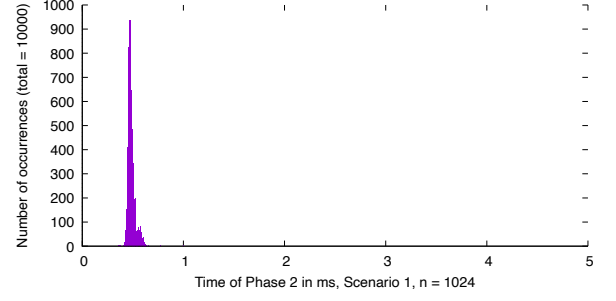
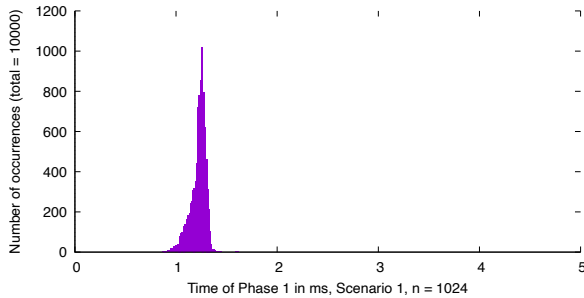
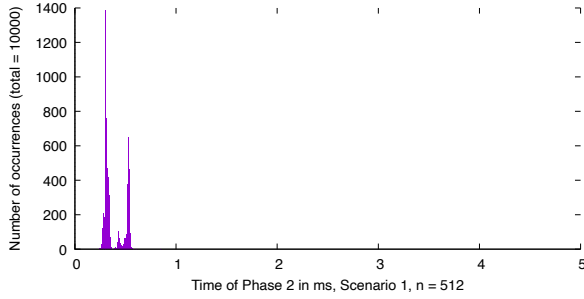
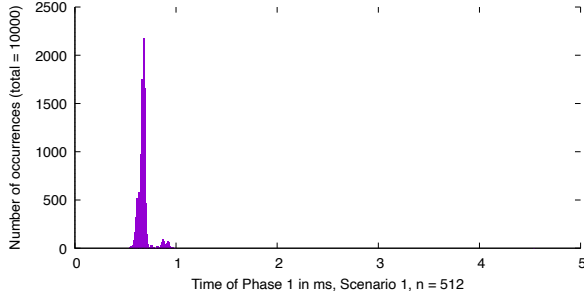
We can also use the above Chernoff bound to bound the completeness error, *i.e.* the probability that the protocol aborts when all players are honest. We allow up to F aborts and assume we have parameters for which the signal doesn't arrive in time with some probability p_{loss} . Let $CE(R, F, p_{\text{loss}})$ denote the completeness error and $\lambda = \frac{F}{R}$. Using again the Chernoff bound (first equation) with $R = n, p = p_{\text{loss}}, \varepsilon = \lambda - p_{\text{loss}}$, we have

$$CE(R, F, p_{\text{loss}}) \leq 2^{R(\lambda \log_2(\frac{p_{\text{loss}}}{\lambda}) + (1-\lambda) \log_2(\frac{1-p_{\text{loss}}}{1-\lambda}))}. \quad (\text{D2})$$

Appendix E: Other parameters

The plots we present in the main text correspond to $n = 1704$ which allows us to have 100 bits of security. We present here the plots for other values of n , for our 2 scenarios, to present the scaling of our scheme.

a. First scenario, different values of n .



b. *Second scenario, different values of n .*

