HAL
open science

An Application of the Boneh and Shacham Group Signature Scheme to Biometric Authentication

Julien Bringer, Hervé Chabanne, David Pointcheval, Sébastien Zimmer

To cite this version:

Julien Bringer, Hervé Chabanne, David Pointcheval, Sébastien Zimmer. An Application of the Boneh and Shacham Group Signature Scheme to Biometric Authentication. The 3rd International Workshop on Security (IWSEC '08), 2008, Kagawa, Japon, Japan. pp.219–230. inria-00419151

HAL Id: inria-00419151

https://inria.hal.science/inria-00419151v1

Submitted on 22 Sep 2009

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.

This extended abstract appeared in
Proceedings of the 3rd International Workshop on Security (IWSEC '08)
November 25–27, 2008, Kagawa, Japan – K. Matsuura and E. Fujisaki Eds. Springer-Verlag, LNCS 5312, pages 219–230.

An Application of the Boneh and Shacham Group Signature Scheme to Biometric Authentication*

Julien Bringer[1], Hervé Chabanne[1], David Pointcheval[2], and Sébastien Zimmer[2]

[1] Sagem Sécurité
[2] École Normale Supérieure

Abstract We introduce a new way for generating strong keys from biometric data. Contrary to popular belief, this leads us to biometric keys which are easy to obtain and renew. Our solution is based on two-factor authentication: a low-cost card and a biometric trait are involved.
Following the Boneh and Shacham group signature construction, we introduce a new biometric-based remote authentication scheme. Surprisingly, for ordinary uses no interactions with a biometric database are needed in this scheme. As a side effect of our proposal, privacy of users is easily obtained while it can possibly be removed, for instance under legal warrant.

Keywords. Biometric Data, Privacy, Group Signature.

1 Introduction

Authentication is a central problem in cryptography and many cryptographic tools have been created to established authenticated channels. Since these cryptographic tools are often difficult to attack, an adversary may prefer concentrate her efforts on a weaker part of the authentication process. This is the goal of social engineering attacks which focus on the user mistakes to discover his password. There is no cryptographic solution against this type of attacks, one has to deploy external security protections. However, a way to strengthen the security level of authentication procedures is to combine several authentication means in such a way that, to impersonate an honest user, the adversary is compelled to break *all* the authentication factors.

Traditionally, three possible human authentication factors are distinguished (even if a forth one has already been introduced [5]):

- what I *know* (as a password),
- what I *have* (as a card),
- who I *am* (as a biometric trait).

All the combinations can be used, however in this paper we focus on a two-factor authentication using a low-cost card ("what I have"), such as a plastic card, and a biometric trait ("who I am").

Biometric authentication, the "who I am" part of the tryptic, has less to do with cryptographic techniques. This is mainly due to the fact that biometric data involved during the authentication must be considered as public data if a high security level is required. Indeed, they are easy to obtain by an adversary: for example a fingerprint can be recovered from any object that have just been touched and an image of an iris scan can be taken with a good camera. This rises two main problems.

Firstly, since an adversary can recover biometric data, no secrecy is used during the biometric authentication procedure. Therefore, what prevents the adversary to

* Work partially supported by french ANR RNRT project BACH.

© Springer-Verlag 2008.

use some (public) biometric templates to impersonate an honest user? Biometrics are valuable for authentication only if one can check that the biometric template used during authentication comes directly from a real living person and not from a fake. Both technical and cryptographic solutions exist to guarantee integrity of biometric data (authenticated channel, supervision of the biometric acquisition by a trusted human, acquisition of several biometrics at the same time, tamper proof resistance of the sensor, ...). The assumption that the biometric template comes directly from a real person is called the *liveness assumption*. The liveness assumption while mandatory for biometric systems is ensured by technical means beyond the scope of this paper and not described here.

Secondly, since the (public) biometric data is unequivocally linked to a person, if some information about the biometric data is leaked during the protocol, then the identity of the user involved in the authentication could be revealed. To protect the privacy of the users, authentication should stay anonymous and the biometric data involved should stay private. Our work thus focuses on the integration of biometric data into cryptographic protocols to respect the privacy of their participants.

1.1 Our Solution

In this paper we propose a two-factor biometric authentication protocol. As no processing power is needed on the side of the user except from the sensor, one can imagine to simply write the reference biometric template on a plastic card. The contribution of this paper is two-fold: first, we propose a simple way to generate strong biometric secret keys, and second, we integrate it in a new authentication protocol which guarantees client anonymity and some other nice features described below.

The protocol presented in this paper is the consequence of a basic observation: the biometric measures are prone to a large amount errors which cannot reasonably be predicted. In other words, the global error between two measures has a high entropy, therefore, even knowing the distribution of the biometrics, an adversary cannot guess the exact value of a biometric template with a good precision.

Traditionally, the errors are seen as an obstacle but, with this remark in mind, one can try to take benefits of these errors to introduce a secret in the biometric part of the authentication protocol, secret which does not exist without it. If the reference biometric template is acquired privately, then its exact value cannot be guessed by an adversary. We propose to hash this template to generate a secret key. More precisely, the reference biometric template is stored in the plastic card and it is compared with a fresh biometric template by the sensor. The matching is made on the client side and if this new template comes from the same biometric trait as the reference template, then the reference template is hashed to regenerate the secret key. The latter is used to authenticate the user to the server.

Another simple solution would be to hide the reference biometric template and any random secret key on a card. However, it requires additional infrastructure to bind the template and the key together (e.g. a PKI). Indeed, without any link between these elements, an adversary can read the key in the card, replace the reference biometric template by one of her own and then she is able to authenticate to the server with the same secret key. In other words, the security relies only on the card and not also on the biometric data. Whereas, our solution makes profit of the properties of the biometrics

which link unequivocally the secret key and the biometric data, we guarantee a secure two factor authentication.

Besides, to complete the authentication protocol, we propose to use the Boneh and Shacham group signature scheme [2]. This scheme has several nice features that can be used in our context. First of all, it allows to guarantee the anonymity of the client towards the server. This is the main property that one want to preserve. Moreover, it allows to revoke compromised keys by generating a Revocation List: compromised keys are revoked and added to the list, so that the server can check online if an adversary tries to use one of the compromised keys to authenticate. Since the only secret is the error and not the biometric data, to generate a new secret key one only has to acquire a new reference biometric template from the same biometric trait. Finally, if the entity which generates the keys, the Card Issuer, is allowed to securely store for every user the reference biometric template, then under legal warrant it can reveal to whom some secret key belongs.

1.2 Related Works

In order to integrate biometrics into cryptographic protocols, it is often proposed to replace traditional matching algorithms by error-correction techniques [3,4,6,7,8,9,10,11,12,17,18,19] and to use Secure Sketches [9] instead of traditional template generators. The main problem with these techniques comes from the use of decoding algorithms instead of classical matching algorithms. This doing, performances are degraded. Moreover, for some kind of biometrics, as for instance for the worldwide deployed fingerprints' minutiae, theoretical solutions have recently been proposed [14] but effective coding solutions – which achieve performances comparable with existing matching based solutions – are still to be found.

1.3 Organization of this Paper

In Section 2, we explain the principles of our solution. In Section 3, we give statistical evidence on biometric data to justify our work. In Section 4, we introduce a new protocol for secure remote biometric authentication with our solution. Finally, we conclude in Section 5.

2 Our Procedure in a Nutshell

Let B denotes a biometric trait. We write:

- $b, b', \ldots \leftarrow B$ for different acquisitions of the same biometric trait B,
- $b \sim b'$ indicates that a matching algorithm will consider b and b' as belonging to the same biometric source B.

During enrollment phase: A biometric trait is acquired: $b \leftarrow B$. This particular acquisition is treated as confidential (see justification in Section 3.2). A copy of b is kept by his owner on a plastic card. Let x denote $x = H(b)$, a cryptographic hash of b.

The main idea here is that whereas the trait B is considered as public, it is not the case of one acquisition b.

During verification phase: A user comes with his card containing the biometric reference b. The same biometric trait is acquired: $b' \leftarrow B$. If $b \sim b'$, a remote cryptographic proof of knowledge of x is made in order to validate the verification.

It means we first run a biometric matching for a local authentication and thereafter we can authorize the use of $x = H(b)$ for a remote authentication.

3 Some Elements on Volatility of Biometric Acquisitions

3.1 An Example

We give an example based on the iris biometrics to illustrate the variations occurring between two acquisitions of the same biometric trait. Iris is often considered as the easiest biometric technology to integrate into cryptographic protocols as it encodes biometric trait as binary vectors and as the matching is made by computing a simple Hamming distance (see below).

What we say for iris is also true for other kind of biometric data. But often in these cases, as for instance for the minutiae matching of fingerprints, we do not even know how to handle them efficiently as binary vectors.

We report some results on a public iris database. This is called the Iris Challenge Evaluation (ICE) database and is used to evaluate matching algorithms [13,15]. It contains 2953 images from 244 different eyes. For each picture, we compute a 256 bytes information vector I together with a 256 bytes mask vector M. The mask vector indicates for each bit whether or not some information is available in I (due to eyelid, eyelashes, reflections, some bits may be missing, ...). The matching of two iris b_1 and b_2 represented as I_1, I_2 with masks M_1, M_2 is done by computing their relative Hamming distance, i.e. the Hamming distance computed over the portion of the information vectors not erased by masks:

$$\mu(b_1, b_2) = \frac{||(I_1 \oplus I_2) \cap M_1 \cap M_2||}{||M_1 \cap M_2||} \tag{1}$$

This leads to the following distributions of matching scores (cf. Fig. 1) where we observe a large number of errors to handle. For instance, if we accept to wrongly reject at most 5 % of the users, we then have to deal with at least 29 % of errors, i.e. up to $\mu(b_1, b_2) = 0.29$. An additional difficulty comes from the number of bits where no information is available which varies from 512 to 1977.

3.2 How Can Volatility Help us To Secure x?

Let $b_i \leftarrow B$, $i = 1, \ldots, l$ be different acquisitions of the same biometric trait. As it is indicated in the introduction, we consider that an adversary may have access to some of these b_i.

Below we explain how different can be two biometric captures of the same biometric trait.

Suppose we are dealing with binary vectors of length n and that any two matching data $b \sim b'$ have more than ϵn differences, then to retrieve b from the knowledge of b' there is at least $\binom{n}{\epsilon n}$ possibilities which correspond to switch the value of ϵn

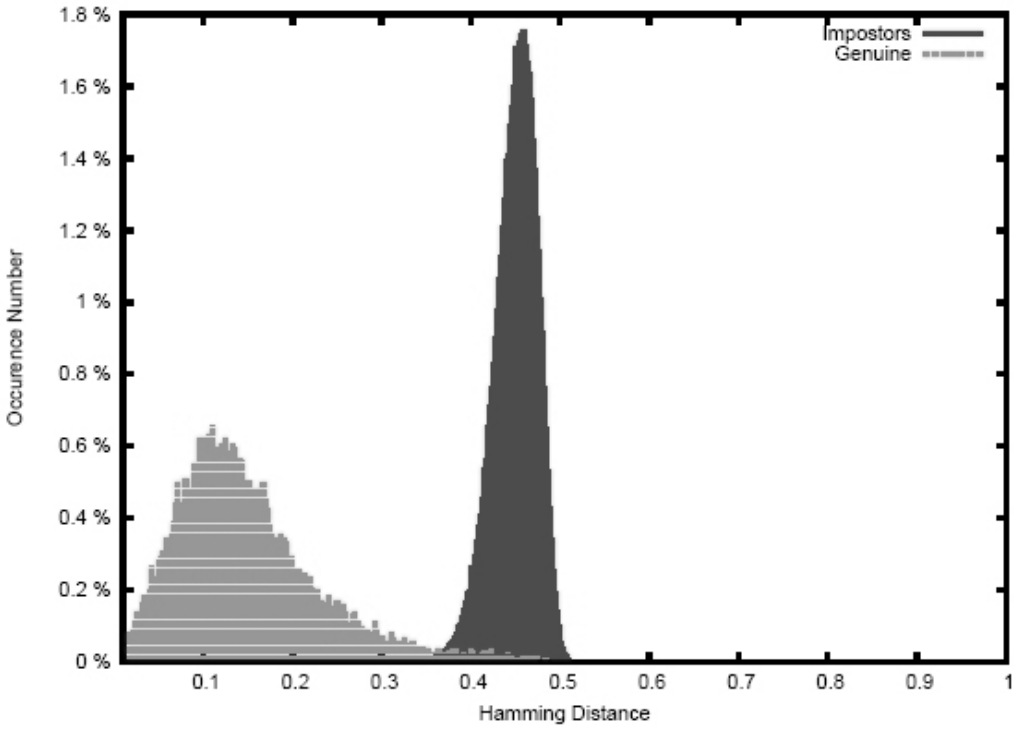

Figure 1. Inter-eyes and intra-eye distributions

coordinates of b' (we assume for the moment errors to be uniform and independent random bits). More precisely an adversary has to search among the vectors of the Hamming spheres $S(b', r)$ of center b' and radius $r \geq r_0$, starting with $r_0 = \epsilon n$.

For instance, for the ICE iris database introduced in the previous section 3.1, we have $n = 2048$ and the distance, computed as in (1) only on the non-erased positions, varies from 44 to 658, amongst the 26874 possible comparisons with two non-equal matching data. This means that without taking masks into consideration, the " closest " b_i differs from b in 44 bits, i.e. $\epsilon \approx 2.15\%$. Thereafter an adversary must switch at least 44 coordinates of b_i to recover b, this leads to $\binom{2048}{44} \approx 2^{302}$ possibilities. Moreover, the masks are also different between two biometric measures, so he will have to correct their differences. Let M_b, M_{b_i} the masks of b and b_i, even if he knows M_b, he will need to choose a value in $\{0, 1\}$ for each erased position of b_i which was not erased for b, i.e. in $\overline{M_{b_i}} - (\overline{M_b} \cap \overline{M_{b_i}})$. The overall number of possibilities is

$$\binom{||M_b \cap M_{b_i}||}{\mu(b, b_i) \times ||M_b \cap M_{b_i}||} \times 2^{||\overline{M_{b_i}} - (\overline{M_b} \cap \overline{M_{b_i}})||}.$$

In the previous example it leads to about 2^{539} possibilities as the number of common non-erased positions is 1056 and the number of differences between the masks is 280. For all the database, the minimum is around 2^{500}. So, in practice even for errors not "uniformly" random[1], the number of possibilities might stay very large.

In practice an adversary may try to reduce the complexity of recovering b by collecting several different b_i. In general, it would remain hard to recover b whereas

[1] Which seems more realistic however the entropy of errors between two biometric captures is very hard to estimate.

for situations where variability is not sufficient we can embed additional random bits under the erased coordinates of b (at least 512 positions for the ICE database). This allows to rely on a random data while it stays transparent for the biometric matching (cf. eq. (1)).

4 An Application to Secure Remote Biometric Authentication

4.1 Introduction

In our system for biometric-based authentication schemes, we consider four types of components.

- Human user $\mathcal{H}$, who uses his biometric data to authenticate himself to a service provider.
- Sensor client $\mathcal{S}$, which extracts human user's biometric trait using some biometric sensor and communicates with the service provider.
- Service provider $\mathcal{P}$, who deals with human user's authentication request, granting access or not.
- Card Issuer $\mathcal{I}$, who holds two master secrets: γ which is needed to derive keys in the scheme (see below and next Section 4.2) and λ which is the private key only used in case of legal warrant, with Λ the corresponding public key (see Section 4.3).

Remark 1 *In our system, we make a separation between everyday interactions where user $\mathcal{H}$ deals with his service provider $\mathcal{P}$ and exceptional procedures. For daily authentications, our proposal provides privacy for $\mathcal{H}$. However, in case of legal warrant, Card Issuer $\mathcal{I}$ has the capability – by using his cryptographic keys – to retrieve who is authenticating himself (cf. Section 4.3).*

The authentication link we want to establish is the following:

Human user $\leftrightarrow$	his biometric trait
$\leftrightarrow$	his biometric key (cf. Section 2): x
$\leftrightarrow$	his private key in the system (cf. below): (x, A)

Hereafter, the x's we have introduced before serves as part of a private key for a group signature [2]. A group signature scheme enables a member of a group to anonymously sign a message on behalf of the group (here, the users who has subscribed to $\mathcal{P}$). A is derived from x by the Card Issuer $\mathcal{I}$ under his master secret γ. The pair (x, A) forms the private key of $\mathcal{H}$ in this system. Details are given in the next section. At this point, we only need to know that (x, A) verifies an algebraic relation:

$$A^{x+\gamma} = g_1 \tag{2}$$

where g_1 is a public parameter. The cryptographic part of the authentication consists in convincing $\mathcal{P}$ that $\mathcal{H}$ holds a private key verifying such a relation.

Keeping notations from previous sections, we have:

Enrollment phase at Card Issuer's facilities: A biometric trait is acquired for user $\mathcal{H}$: $b \leftarrow B$. The Card Issuer $\mathcal{I}$ computes A with the help of γ. A plastic card $\mathcal{C}$ containing (b, A) is issued by $\mathcal{I}$ for $\mathcal{H}$. The Card Issuer keeps b in a database $\mathcal{DB}$ of his own.

Remark 2 *Following a standard trick of the biometric world, it is also possible to envisage that $\mathcal{DB}$ is used during enrollment phase to ensure that none user registers twice.*

During verification phase:

1. A sensor $\mathcal{S}$ takes "fresh" biometric trait b' of a user $\mathcal{H}$. $\mathcal{S}$ verifies the liveness of b'.
2. A match of b' against the b stored in the plastic card $\mathcal{C}$ is performed.
3. In case of success, a proof of knowledge of the private key (x, A) is made by signing a challenge sent by the service provider $\mathcal{P}$ following the Boneh and Shacham scheme [2] which is described in the next Section.

4.2 The Boneh-Shacham Group Signature Scheme

System parameters:

- $\mathbb{G}_1$ is a multiplicative cyclic group of prime order p.
- $\mathbb{G}_2$ is a multiplicative group whose order is some power of p.
- ψ is a homomorphism from $\mathbb{G}_2$ to $\mathbb{G}_1$.
- g_2 is an order-p element of $\mathbb{G}_2$ and g_1 is a generator of $\mathbb{G}_1$ such that $\psi(g_2) = g_1$.
- $\mathbb{G}_T$ is a multiplicative cyclic group of prime order p.
- $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ is a bilinear non-degenerate map.
- H is a hash function from $\{0,1\}^*$ to $\mathbb{Z}_p$ and H_0 is another hash function mapping $\{0,1\}^*$ to $\mathbb{G}_2^2$.

Some other elements:

- group public key: $gpk = (g_1, g_2, w)$ where $w = g_2^\gamma$ for some secret $\gamma \in \mathbb{Z}_p$.
- private key: a pair (x, A), where $A \in \mathbb{G}_1$ and $x \in \mathbb{Z}_p$ verifying (2), i.e. $e(A, wg_2^x) = e(g_1, g_2)$. Given x, A must be computed by the owner of γ.

We are now ready to recall the principles of the signature from [2]. We here consider that the verifier sends a challenge M to be signed by the prover.

Signature of M. The prover obtains generators

$$(\hat{u}, \hat{v}) = H_0(gpk, M, r) \in \mathbb{G}_2^2 \tag{3}$$

with a random $r \in \mathbb{Z}_p$. He computes their images $u = \psi(\hat{u}), v = \psi(\hat{v})$. He then selects a random $\alpha \in \mathbb{Z}_p$ and computes:

- $T_1 = u^\alpha$, $T_2 = Av^\alpha$
- $\delta = x\alpha$

From random r_α, r_x, r_δ in $\mathbb{Z}_p$, he computes helper values:

– $R_1 = u^{r_\alpha}$, $R_2 = e(T_2, g_2)^{r_x}.e(v, w)^{-r_\alpha}.e(v, g_2)^{-r_\delta}$, $R_3 = T_1^{r_x}.u^{-r_\delta}$

Let $c = H(gpk, M, r, T_1, T_2, R_1, R_2, R_3) \in \mathbb{Z}_p$. The prover computes:

– $s_\alpha = r_\alpha + c\alpha$, $s_x = r_x + cx$, $s_\delta = r_\delta + c\delta$.

He sends to the verifier the signature of M: $\sigma = (r, c, T_1, T_2, s_\alpha, s_x, s_\delta)$.

Verification. The verifier recovers $(\hat{u}, \hat{v})$ from (3) and their images u, v in $\mathbb{G}_1$. He computes the helper data as:

$\tilde{R}_1 = u^{s_\alpha}/T_1^c$

$\tilde{R}_2 = e(T_2, g_2)^{s_x}.e(v, w)^{-s_\alpha}.e(v, g_2)^{-s_\delta}.(e(T_2, w)/e(g_1, g_2))^c$

$\tilde{R}_3 = T_1^{s_x}.u^{-s_\delta}$

He checks whether $c = H(gpk, M, r, T_1, T_2, \tilde{R}_1, \tilde{R}_2, \tilde{R}_3)$ and accepts the signature accordingly.

4.3 Implementation Issues

Sensors $\mathcal{S}$ and liveness detection. The sensor has to acquire biometric traits and to verify that these traits are coming from "living persons". This liveness link must be maintained throughout the authentication. For achieving this, we propose that only trusted sensors are allowed to communicate with the service provider $\mathcal{P}$. This is a quite usual assumption[2] where we assume that the system follows the protocol honestly. In practice, we proceed as follows:

1. $\mathcal{P}$ sends the challenge M to sensor $\mathcal{S}$.
2. $\mathcal{S}$ gets the "fresh" biometric trait b' and reads (b, A) from the card.
3. $\mathcal{S}$ checks whether $b' \sim b$, and in this case computes $x = H(b)$.
4. $\mathcal{S}$ computes the signature σ of M under (x, A).
5. The sensor $\mathcal{S}$ encrypts b' – with a semantically secure encryption scheme – under the key Λ of the Card Issuer $\mathcal{I}$. It then signs this encrypted value together with σ to obtain a signature Σ and sends both σ and Σ to $\mathcal{P}$.
6. $\mathcal{P}$ verifies the signature Σ. This doing, $\mathcal{P}$ insures itself that the signature σ and the encryption of b' can be trusted, as computed by a trusted sensor. The latter is important as the value could be requested under legal warrant. Finally $\mathcal{P}$ checks the signature σ of M to accept the authentication or not.

Remark 3 *To enforce b secrecy, one can think to use Match On Card (MOC) [16]. With this technology, new traits $b' \leftarrow B$ are acquired by a sensor but the matching is made inside the card $\mathcal{C}$ which has to decide whether $b \sim b'$. This way, the confidentiality of b also relies on inherent protections of smartcards against physical threats. Moreover, b does not go out of the card. In this case, $\mathcal{C}$ performs directly the signature of challenges on behalf of the group as previously described in Section 4.2.*

[2] It could require to deal with protected sensors – e.g. via tamper proof hardware.

Privacy. Privacy for the signature scheme of the Boneh and Shacham relies on the following problem:

Decision Linear Problem in $\mathbb{G}$*:* Given $u, v, h, u^{a_1}, v^{a_2}, h^{a_3} \in \mathbb{G}$ as input, output yes if $a_1 + a_2 = a_3$ and no otherwise.

It is proved in [2] that, in the Random Oracle model and assuming the Decision Linear Problem holds in the group $\mathbb{G}_2$, a group member can tell whether he generated a particular signature σ but if he didn't, he learns nothing else about the origin of σ. This property is known as selfless-anonymity.

Hence, the biometric authentication becomes anonymous against the service provider $\mathcal{P}$ and any external eavesdropper.

Revocation. The scheme of Boneh and Shacham has another interesting property: a Revocation List (RL) constituted with the second parts – the A's – of the private keys of revoked users can be established. A verifier in possession of this list (RL) can then determine whether he is interacting with a revoked prover or not.

In our system, the Revocation List (RL) is held by the Service Provider $\mathcal{P}$. To check whether a user belongs to this list (RL), $\mathcal{P}$ verifies that A is encoded in (T_1, T_2) which happens when $e(T_2/A, \hat{u}) = e(T_1, \hat{v})$.

More precisely, when a user $\mathcal{H}$ has a problem with his plastic card – for instance, if he looses it – he has to go to the Card Issuer $\mathcal{I}$ to declare the event. $\mathcal{I}$ then sends the corresponding A to $\mathcal{P}$ for being added to the Revocation List (RL). Enrolled data can then easily be renewed. The same holds if part of the system, e.g. $\mathcal{P}$, detects a malicious behavior: he can alert $\mathcal{I}$ in order to add a key into RL.

Legal Warrant and database $\mathcal{DB}$ of the Card Issuer. Under legal warrant, the service provider $\mathcal{P}$ can forward the encryption of b' to the Card Issuer $\mathcal{I}$ who can decrypt it to check to who this biometric trait is corresponding in his database $\mathcal{DB}$. The database $\mathcal{DB}$ can also be used to check the coherence of b' with the underlying biometric key x coming with σ.

Note that for ordinary uses, no information has to be sent to $\mathcal{I}$: $\mathcal{P}$ decides by itself if the authentication is a success or not. The database $\mathcal{DB}$ is in fact optional and can be avoided if the property above is not required.

Remark 4

1. *As explained in [2], the scheme of Boneh and Shacham also achieves traceability, i.e. an adversary cannot forge a signature σ without being able to trace him back to one of the users in the coalition which has served to generate σ. This means a user's key is strongly binded to the enrolled biometric data. See [2] for further details.*
2. *Boneh, Boyen and Shacham propose in [1] an extension of the previous protocol which is zero-knowledge. This extension does not share the same properties, in particular the revocation capability of the scheme we used. This is why we do not choose this extension. Nevertheless, note that in [1], the subject of the simultaneous revocation of many keys – for instance, at the end of a cryptoperiod – is studied. This mechanism can also be employed here.*

5 Conclusion

Taking to our advantage the very nature of biometrics, i.e. their volatility and their need to interact with trusted sensors, we present a simple but effective way of considering biometric data for remote authentication. Our procedure does not depend on the kind of underlying biometric information as we can take back traditional matching algorithms.

We combine our idea with a group signature scheme due to Boneh and Shacham [2] to obtain an effective protocol for remote biometric authentication with anonymity features.

Acknowledgment

The authors wish to thank Julien Stern for helpful comments on the scheme. This work has been partially supported by European Commission through ECRYPT.

References

1. D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In M. K. Franklin, editor, *CRYPTO*, volume 3152 of *Lecture Notes in Computer Science*, pages 41–55. Springer, 2004.
2. D. Boneh and H. Shacham. Group signatures with verifier-local revocation. In V. Atluri, B. Pfitzmann, and P. D. McDaniel, editors, *ACM Conference on Computer and Communications Security*, pages 168–177. ACM, 2004.
3. X. Boyen. Reusable cryptographic fuzzy extractors. In V. Atluri, B. Pfitzmann, and P. D. McDaniel, editors, *CCS '04: Proceedings of the 11th ACM conference on Computer and communications security*, pages 82–91. ACM Press, 2004.
4. X. Boyen, Y. Dodis, J. Katz, R. Ostrovsky, and A. Smith. Secure remote authentication using biometric data. In R. Cramer, editor, *Advances in Cryptology — EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 147–163. Springer, 2005.
5. J. G. Brainard, A. Juels, R. L. Rivest, M. Szydlo, and M. Yung. Fourth-factor authentication: somebody you know. In *ACM Conference on Computer and Communications Security*, pages 168–178, 2006.
6. J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, and G. Zémor. Optimal iris fuzzy sketches. In *IEEE First International Conference on Biometrics: Theory, Applications and Systems, BTAS'07*, 2007.
7. G. D. Crescenzo, R. Graveman, R. Ge, and G. Arce. Approximate message authentication and biometric entity authentication. In A. S. Patrick and M. Yung, editors, *Financial Cryptography and Data Security, 9th International Conference*, volume 3570 of *Lecture Notes in Computer Science*, pages 240–254. Springer, 2005.
8. Y. Dodis, J. Katz, L. Reyzin, and A. Smith. Robust fuzzy extractors and authenticated key agreement from close secrets. In C. Dwork, editor, *Advances in Cryptology — CRYPTO 2006*, volume 4117 of *Lecture Notes in Computer Science*, pages 232–250. Springer, 2006.
9. Y. Dodis, L. Reyzin, and A. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In C. Cachin and J. Camenisch, editors, *Advances in Cryptology — EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 523–540. Springer, 2004.
10. A. Juels and M. Sudan. A fuzzy vault scheme. *Design Codes and Cryptography*, 38(2):237–257, 2006.
11. A. Juels and M. Wattenberg. A fuzzy commitment scheme. In *ACM Conference on Computer and Communications Security*, pages 28–36, 1999.
12. J. M. G. Linnartz and P. Tuyls. New shielding functions to enhance privacy and prevent misuse of biometric templates. In J. Kittler and M. S. Nixon, editors, *Audio-and Video-Based Biometrie Person Authentication, 4th International Conference*, volume 2688 of *Lecture Notes in Computer Science*, pages 393–402. Springer, 2003.

13. X. Liu, K. W. Bowyer, and P. J. Flynn. Iris Recognition and Verification Experiments with Improved Segmentation Method. In *Fourth IEEE Workshop on Automatic Identification Advanced Technologies (AutoID), 17-18 October 2005, Buffalo, New York*, 2005.
14. K. Nandakumar, A. K. Jain, and S. Pankanti. Fingerprint-based fuzzy vault: Implementation and performance. *IEEE Transactions on Information Forensics and Security*, 2008.
15. National Institute of Standards and Technology (NIST). Iris Challenge Evaluation. `http://iris.nist.gov/ICE`, 2005.
16. National Institute of Standards and Technology (NIST). The minutiae interoperability exchange test. `http://fingerprint.nist.gov/minex/`.
17. P. Tuyls, A. H. M. Akkermans, T. A. M. Kevenaar, G. Jan Schrijen, A. M. Bazen, and R. N. J. Veldhuis. Practical biometric authentication with template protection. In T. Kanade, A. K. Jain, and N. K. Ratha, editors, *Audio- and Video-Based Biometric Person Authentication, 5th International Conference*, volume 3546 of *Lecture Notes in Computer Science*, pages 436–446. Springer, 2005.
18. P. Tuyls and J. Goseling. Capacity and examples of template-protecting biometric authentication systems. In *ECCV Workshop BioAW*, pages 158–170, 2004.
19. P. Tuyls, E. Verbitskiy, J. Goseling, and D. Denteneer. Privacy protecting biometric authentication systems: an overview. In *EUSIPCO 2004*, 2004.