Security Notions of Biometric Remote Authentication Revisited

Neyire Deniz Sarier

B-IT, Cosec
Dahlmannstr. 2, D-53113 Bonn Germany
denizsarier@yahoo.com

Abstract. In this paper, we describe a new biometric-based remote authentication (BRA) system by combining distributed biometric authentication and cancelable biometrics. The motivation of this construction is based on our new attacks against the BRA schemes designed according to the security model of Bringer et al. Specifically, we prove that identity privacy cannot be achieved for the schemes in this model, if biometrics is assumed as public data and a publicly stored sketch is employed for improved accuracy. Besides, a statistical attack is shown that is effective even if the sketch is stored as encrypted. To prevent statistical attacks, we propose a weaker notion of identity privacy, where the adversary has limited power. Next, we design a BRA protocol in cancelable biometric setting, which is also applicable for biometrics represented as a set of features. For this setting, we define a stronger security notion, which is guaranteed for the BRA schemes that are vulnerable to our attacks if they are implemented in cancelable biometric setting.

Keywords: Security Notions, Biometric-based Remote Authentication, Identity Privacy, Secure Sketch, Cancelable Biometrics.

1 Introduction

Biometric-based authentication systems can be classified as remote or local authentication, where the former system authenticates a user over a network by performing the matching of his transmitted fresh biometrics to his stored biometric data at the remote server. A special type of biometric-based remote authentication (BRA) system and a new security model is introduced by Bringer et al. in ACISP'07, where security against insider attacks is considered. In this model, the server-side functionalities are performed in a distributed fashion using a detached biometric database and non-colluding system components. Basically, this system is composed of three entities, the authentication server $\mathcal{AS}$, the sensor $\mathcal{S}$ capturing the biometrics and the detached biometric database $\mathcal{DB}$. $\mathcal{AS}$ only stores the identity information of the users and provides the communication between $\mathcal{S}$ and $\mathcal{DB}$. Besides, $\mathcal{AS}$ does not have access to the reference biometrics that is stored as encrypted using homomorphic encryption, thus all the computations performed by $\mathcal{AS}$, $\mathcal{S}$ and $\mathcal{DB}$ stay in the encrypted domain. This leads to

C. Meadows and C. Fernández-Gago (Eds.): STM 2011, LNCS 7170, pp. 72–89, 2012.

a new security notion called identity privacy that guarantees the privacy of the link between the identity (name) and the biometrics of the user although biometrics is assumed as public data. The intuition of this notion is that a malicious $\mathcal{AS}$ that generates two templates for a user, cannot identify from the protocol runs, which of the two biometric templates is registered to the $\mathcal{DB}$ as encrypted with probability significantly better than that of random guessing. Moreover, $\mathcal{AS}$ performs the matching after a Private Information Retrieval (PIR) protocol that prevents a curious $\mathcal{DB}$ from tracking the user that authenticates to the system. Thus, transaction anonymity against a (malicious) database is satisfied which is the second notion for biometric remote authentication.

1.1 Related Work

Existing distributed biometric remote authentication schemes differ from each other based on the homomorphic encryption scheme chosen, incorporation of a secure sketch scheme, the biometric storage mechanism and whether an additional security factor is required as in the case of multi-factor biometric authentication. The distributed biometric remote authentication schemes that are designed according to the security model of Bringer et al. [2,4,16,13] combine homomorphic encryption, secure sketches and Private Information Retrieval (PIR) to achieve the security notions of identity privacy and transaction anonymity. The first biometric system in this model [3] employs Goldwasser-Micali encryption and a special PIR in order to compare two binary biometric strings in encrypted domain using hamming distance. Next, the systems of [4,16] require a secure sketch scheme to error-correct the biometric string such as an 2048 bits Iris code and use ElGamal encryption for equality testing [7] together with an efficient PIR scheme. Similarly, the work of [2] combines a secure sketch, Goldwasser-Micali and Paillier encryption in Lipmaa's PIR protocol to prevent the attacks against the scheme in [3]. Besides, in [13], elliptic curve ElGamal and a PIR scheme is employed together with a special secure sketch scheme applicable to an ordered biometric feature set. Another work that assumes biometrics as a set of features [1] provides a secure biometric identification scheme using a Support Vector Machine and Paillier encryption by adapting the security notions for biometric features (usually an k-tuple of numbers). A survey of these systems is given in [12]. Recently, [15] presents a survey of attacks against the schemes of [3,1] and some other biometric schemes. No attacks are known for the schemes presented in [2,4,16], which require the use of secure sketches. Except for the works of [1,13,11,14], the biometrics is assumed as a binary string such as an 2048 bits iris code, whereas the general representation of biometrics is a set of features that can be either ordered such as face, voice, iris, handwritten signatures or unordered such as fingerprint minutia.

1.2 Motivation and Contributions

The contributions of our paper is twofold. First, we consider the biometric remote authentication (BRA) schemes that require a fuzzy sketch scheme for improved

accuracy. We analyze the security based on the model of Bringer et al., where we prove that if biometrics is assumed as public data and the fuzzy sketch required for error-correction is stored publicly, the notion of identity privacy against a malicious authentication server $\mathcal{AS}$ can never be satisfied. Basically, this notion guarantees the secrecy of identity-biometrics relation through a security game between the (malicious) $\mathcal{AS}$ and a simulator (i.e. challenger) $\mathcal{C}$. If $\mathcal{AS}$ can correctly distinguish the registered reference template $\sim$that is one of the two templates output by $\mathcal{AS}\sim$ by listening to the protocol runs, $\mathcal{AS}$ wins this game, thus breaks the scheme in the sense of identity privacy.

In identity privacy game, the malicious $\mathcal{AS}$ has to output two biometric templates describing the user U. Since the definition of this notion does not restrict $\mathcal{AS}$ on how he chooses the two biometric templates, $\mathcal{AS}$ can output a pair of templates (b_1, b_2) for U, where the distance between the two templates is either $\mathsf{dis}(b_1, b_2) < t$ or $\mathsf{dis}(b_1, b_2) > t$. Here, t is the error correction threshold of the secure sketch scheme that is used to correct the errors given a similar biometrics and a public helper data PAR. For the two cases, we prove separately that the adversary can easily compute the exact biometric template that is registered by the challenger $\mathcal{C}$ of the game using the helper data PAR of the secure sketch that is publicly available. Thus, the schemes of [4,16] and any biometric remote authentication scheme that assumes biometrics and the required secure sketch as public data are vulnerable to this attack and cannot satisfy identity privacy. Although the scheme of [2] stores the helper data PAR as encrypted, we propose a statistical attack to break identity privacy, where the adversary uses the (known) distribution of U's biometrics and outputs the two templates (b_1, b_2) for U in a special way. To our knowledge, no concrete attack has been presented against the sketch-based schemes of [2,4,16].

Thus, we observe that the security model of Bringer et al. does not consider the attacks that reveal the cleartext of the stored reference biometrics with the help of the public sketch. Besides, if the sketch is stored secretly, then identity privacy game should be modified so that there is a restriction on the templates generated by the adversary $\mathcal{AS}$ to prevent $\mathcal{AS}$ breaking the notion with statistical attacks. Thus, we describe a new notion called Weak-Identity privacy that does not allow the adversary to generate the possible templates for a particular user, instead the templates are given to him by the challenger. Under this new notion, the scheme of [2] is resistant against our statistical attacks.

Secondly, we discuss alternative solutions to guarantee the security of BRA schemes requiring public sketches. The trivial solution for the schemes [4,16] is to store the sketch PAR secretly, namely, in the tamper-proof smartcard of the user. This will result in a two-factor authentication scheme, thus, the system is not anymore a pure biometric-based authentication scheme. Besides, if these systems are implemented for biometrics that are represented as a set of features, this solution still does not cover brute-force attacks for biometrics with a small feature space. We note that current provably secure schemes are only defined for biometrics represented as a fixed length binary string such as an 2048 bits

long Iris code except for the schemes of [13,1] that assume biometrics as a set of features, i.e. k-tuple of integers.

As a first solution, we describe a new BRA protocol where we combine cancelable biometrics and distributed remote authentication. Briefly, cancelable biometrics perform a distortion of the biometric image or features before matching. The variability in the distortion parameters provides the cancelable nature of the scheme. Distortion (i.e masking) is performed either using a one-way transformation or a high entropy randomness that is stored in the user's smart card to be used later for authentication in the transformed space. Our protocol is applicable for biometrics represented as a set of features and resistant against brute-force attacks if the feature space is small. Next, we define a stronger notion as 'Identity privacy for cancelable biometrics', where breaking this notion implies breaking the underlying encryption scheme in the sense of indistinguishability. The schemes of [4,16] that are vulnerable to our attack are secure in cancelable biometric setting based on this new notion.

Finally, we employ the detached biometric storage in distributed biometric authentication systems, which is not considered in current cancelable biometric systems and in their security analysis. Thus, a trusted biometric database can serve different service providers due to its distributed structure. Besides, a major difference of our model to existing schemes of Bringer et al. [3,2,4,16] is the use of bilinear pairings, which allows the $\mathcal{AS}$ to compute the final authentication decision without any decryption operation. Thus, $\mathcal{AS}$ does not need to store a secret key, whose leakage endangers the system's security drastically.

2 Preliminaries

In order to analyze the differences between existing biometric remote authentication systems, we briefly define the necessary components of the biometric remote authentication systems designed according to the model of Bringer et al.

Definition 1. *A function $\epsilon(k) : \mathbb{N} \rightarrow \mathbb{R}$ is defined as negligible if for any constant c, there exists $k_0 \in N$ with $k > k_0$ such that $\epsilon < (1/k)^c$.*

Definition 2. *A Private Information Retrieval (PIR) protocol allows a party to retrieve the i-th bit (more generally, the i-th item) from the $\mathcal{DB}$ consisting of m bits while keeping the value i private.*

2.1 Architecture of the System

The system structure for biometric-based remote authentication schemes designed according to the security model of Bringer et al. consists of four components. Here, the user U and the sensor S denote the client side and the remaining components denote the server-side of the system.

-*Human user U*, which uses his biometrics to authenticate himself to an authentication server. The user may possess a smart card for storing additional data

such as error correcting information or user specific data other than biometrics if a multi-factor authentication scheme is designed.
-*Sensor client* $\mathcal{S}$, which captures the raw biometric data and extracts a biometric template, and communicates with the authentication server by performing cryptographic operations such as public key encryption. We also assume a liveness link between the sensor and the server-side components, to provide confidence that the biometric data received on the server-side is from a living person.
-*Authentication server* $\mathcal{AS}$, which deals with human user's authentication request by communicating with the user and organizing the entire server-side procedure. The data stored at the $\mathcal{AS}$ consists of a list $\mathcal{L}$= $\{ID_1, ..., ID_N\}$ of user identities $ID_l \in \{0,1\}^*$. The index of the user in this list will be $j \in \{1, ..., N\}$. In a successful authentication the $\mathcal{AS}$ will obviously learn the user's identity, which means that it should learn nothing about the biometric data being submitted.
-*Database* $\mathcal{DB}$, which stores biometric information for users either in cleartext or as in encrypted form. Since the $\mathcal{DB}$ is aware of privileged biometric data, it should learn nothing about the user's identity, or even be able to correlate or trace authentication runs from a given (unknown) user.

A biometric authentication system consists of the two following phases:

- *Enrollment phase*: The user U registers his reference biometrics at the database $\mathcal{DB}$ and his personalized username ID at the authentication server $\mathcal{AS}$. The user may have multiple registrations at the same $\mathcal{AS}$ under different usernames.
- *Verification phase*: The user U issues an authentication request to the authentication server $\mathcal{AS}$ through the sensor client $\mathcal{S}$. $\mathcal{AS}$ decides based on U's biometrics with help from the database $\mathcal{DB}$.

2.2 Secure Sketches

Let $\mathcal{H}$ be a metric space with distance function dis. A secure sketch scheme allows recovery of a hidden value $w \in \mathcal{H}$ from any value $w' \in \mathcal{H}$ close to this hidden value with the help of some public value PAR, which does not leak too much information about w. A $(\mathcal{H}, m, m', t)$- sketch is a pair of functions (SS,Rec):

-The sketching function SS takes $w \in \mathcal{H}$ as input and returns the public parameter PAR in $\{0,1\}^*$ such that for all random variables W over $\mathcal{H}$ with min-entropy $\mathbf{H}_\infty(W) \geq m$, the conditional min-entropy is $\bar{\mathbf{H}}_\infty(W|\mathsf{SS}(W)) \geq m'$.

-The Rec function takes a vector w' and PAR as input and computes w if and only if $\mathsf{dis}(b, b') \leq t$ for any $\mathsf{PAR} = \mathsf{SS}(w)$.

The fuzzy sketch for iris biometrics based on the code-offset construction is used in the biometric authentication schemes of [2,16]. Let C be an $(n, k, 2t+1)$ binary linear error correcting code in Hamming space. Let $\mathsf{PAR} = c \oplus b$, where c is a random codeword in C. From the corrupted codeword $c' = \mathsf{PAR} \oplus b' = c \oplus (b \oplus b')$, one can recover c if the hamming distance $\mathsf{dis}_\mathcal{H}$ between b and b' is $\mathsf{dis}_\mathcal{H}(b, b') < t$. An important requirement for such a scheme is that the value PAR should not reveal too much information about the biometric template b.

2.3 Cancelable Biometrics

The idea of cancelable biometrics is to transform biometric data with an irreversible transformation and to perform the matching directly on the transformed data allowing the use of existing feature extraction and matching algorithms. Formally, given two biometric data w and w', the matching score will be computed directly on transformed data by $m(f(w), f(w'))$, where m denotes the similarity measure and f be a transformation that does not degrade the matching performances too much. The three properties of f are: (1) w and $f(w)$ do not match together; (2) For two different transformations f_1 and f_2, $f_1(w)$ and $f_2(w)$ do not match together; (3) A pre-image of $f(w)$ is hard to compute.

Besides, [10,8,5] proposes another method for cancelable biometrics, where the biometric information is masked by a random number, and then, the masked information is stored in the server as a template. The random number used for masking is needed to have a certain level of entropy, and to be stored in a smart card carried by authorized user. Biometric information presented at the authentication phase is also masked by the same random number, and compared with the template (i.e. biometric information masked by the random number) [10]. This way, biometric data stored at the server is protected through this transformation and biometrics can be updated by changing the transformation function or the randomness. This system also prevents the user's traceability across different biometric databases. Example systems employing a high entropy randomness stored in a smart card for cancelable biometrics are given in [8,5,10]. Even if the (masked) templates are compromised, no biometric information will leak out. Also, in this method, no information except for the random number is stored in a smart card, which is assumed as a tamper proof smart card.

2.4 ElGamal Encryption Scheme

- Setup: An authority chooses and publishes a cyclic group $\mathbb{G}$ of prime order q together with a generator g of the group. Also, ElGamal encryption can be implemented on an elliptic curve.
- Keygen: Each user chooses the private key $x \leftarrow \mathbb{Z}_q$ and publishes the corresponding public key $y = g^x$.
- $\mathsf{Encrypt}$: To encrypt a message $m \in \mathbb{G}$, one randomly selects $r \leftarrow \mathbb{Z}_q$ and computes $(u, v) = (g^r, y^r m)$. The ciphertext is $c = (u, v) \in C$.
- $\mathsf{Decrypt}$: To decrypt $c = (u, v)$, one computes $m = vu^{-x}$.

ElGamal cryptosystem [7] is one-way secure based on the CDH problem, IND-CPA secure based on the DDH problem and OW-PCA secure if the GDH problem is hard. In many practical protocols $\mathbb{G}$ would be the group of multiples of a point P on an elliptic curve defined over a finite field.

The multiplicative homomorphic property is that $\mathsf{Enc}(a) \times \mathsf{Enc}(b) = \mathsf{Enc}(a \times b)$. ElGamal encryption can also be additively homomorphic if we generate the ciphertext $c = \mathsf{Enc}_{pk}(m) = (g^r, pk^r g^m)$ instead of $c = (g^r, pk^r m)$. Thus, $\mathsf{Enc}(a) \times \mathsf{Enc}(b) = \mathsf{Enc}(a + b)$.

3 Security Model

The security model of the biometric remote authentication systems designed according to the model of Bringer et al. [3,4,2,16,13,1] have the following properties. Firstly, sensor client $\mathcal{S}$ and authentication server $\mathcal{AS}$ are assumed to be independent components. In [16], this is considered to be an appropriate assumption in the remote authentication environment, where human users access $\mathcal{AS}$ through different $\mathcal{S}$'s, which are not owned by $\mathcal{AS}$ but have a business agreement with it. Additionally, we have the following properties.

-Liveliness Assumption: This is an indispensable assumption on $\mathcal{S}$ for any biometric system as it guarantees with high probability that the biometrics is coming from a live human user.
-Security link Assumption: To provide the confidentiality and integrity of sensitive information, the communication channel between U, $\mathcal{S}$, $\mathcal{AS}$ and $\mathcal{DB}$ should be encrypted using standard protocols.
-Collusion Assumption: Due to the distributed system structure, we assume that U, $\mathcal{DB}$ and $\mathcal{AS}$ are malicious but they do not collude. Also, $\mathcal{S}$ is always honest.

3.1 Identity Privacy

The security notions for biometric remote authentication are introduced in [3] and further analyzed in [2,4,16,1]. Informally, this notion guarantees the privacy of the sensitive relationship between the user identity and its biometrics against a malicious authentication server $\mathcal{AS}$ even in case of multiple registrations of the same user with different personalized usernames. Briefly, it means that the authentication server or the database (or an attacker that has compromised one of them) cannot recover the biometric template of the user [3,16]. Here, l denotes the security parameter of the protocol and the symbol $\emptyset$ means that there is no explicit output (besides the state information) for the adversary.

Given an adversary $\mathcal{A}$ running against the biometric authentication scheme and a challenger $\mathcal{C}$ that simulates the registration phase of the scheme, we consider the following game between $\mathcal{A}$ and $\mathcal{C}$.

Experiment $Exp_{\mathcal{A}}(l)$
For $(i, ID_i, b_i^0, b_i^1, (ID_j, b_j)_{\{j \neq i\}}) \leftarrow \mathcal{A}(1^l)$
$b_i^\beta \xleftarrow{R} \{b_i^0, b_i^1\}$
$b_i = b_i^\beta$
$\emptyset \leftarrow Enrollment((ID_j, b_j)_j)$
$\beta' \leftarrow \mathcal{A}(Challenger; Verification)$
if $\beta' = \beta$ return 1 else return 0

A biometric authentication scheme satisfies the notion of Identity Privacy if

$$Adv_{\mathcal{A}}(l) = Pr[Exp_{\mathcal{A}} = 1|\beta = 1] - Pr[Exp_{\mathcal{A}} = 1|\beta = 0] \quad (1)$$

is negligible. Here, the adversary $\mathcal{A}$ generates the authentication data for the users U_j $(j \neq i)$ together with two biometric (binary) templates b_i^0, b_i^1 for an

additional user U_i in the system. The challenger $\mathcal{C}$ picks at random biometrics $b_i = b_i^{\beta}$ of U_i and simulates the enrollment phase by registering the encryption of the biometrics of each user in the system at the $\mathcal{DB}$. After running the verification protocol polynomially many times, $\mathcal{A}$ outputs a guess for the biometrics of U_i that $\mathcal{C}$ has chosen. The intuition of this notion is that a malicious authentication server, who knows that the registered biometric template is one of the two templates that he has generated, cannot identify the random choice β of the challenger from listening to the protocol runs with probability significantly better than that of random guessing.

A second notion is defined as transaction anonymity, which means that a malicious database cannot learn anything about the personal identity of the user for any authentication request made to the authentication server [3,16]. This notion is based on the security of the PIR protocol (i.e. user privacy of the PIR) instead of the secrecy of the identity-biometrics relation.

4 Schemes Based on Secure Sketches

In [2], [4] and [16], the authors present distributed biometric remote authentication schemes requiring secure sketches. The main difference of these biometric systems is the integration of a secure sketch scheme for error correcting a biometric (binary) string such as an 2048 bits Iris code and the use of homomorphic encryption. This way, there is no need for a similarity metric (i.e. hamming distance) for the final decision, instead the system is used for equality testing. Here, each biometric string is stored at the $\mathcal{DB}$ as encrypted with the public key pk of the $\mathcal{AS}$ as opposed to the scheme of [3], where each biometrics is stored in clear.

The first scheme of [4] and the scheme of [16] are based on ElGamal encryption, where $\mathcal{AS}$ generates an ElGamal key pair (pk, sk) during the setup phase of the protocol with $pk = y = g^x$ and $sk = x$.

In the enrollment phase, the user U registers at the $\mathcal{DB}$ by sending $R = (R^1, R^2) = \mathsf{Enc}(g^b, pk) = (g^r, y^r g^b)$, namely the ElGamal encryption of its biometrics b to $\mathcal{DB}$ and the parameter PAR is publicly available for reconstruction of the same biometrics b using the secure sketch scheme. The user U also registers his pseudorandom identifier ID at the $\mathcal{AS}$. Verification phase is as follows:

- $\mathcal{S}$ sends U's identity ID to the $\mathcal{AS}$ and the error-corrected and encrypted fresh biometrics $X = (X^1, X^2) = \mathsf{Enc}(g^{b'}, pk)$ to the $\mathcal{DB}$ using the PAR for error-correction and ElGamal encryption.
- For each entry $j \in [1, N]$, $\mathcal{DB}$ selects random $r_j, r'_j \in \mathbb{Z}_q$ and computes $C_j = ((g^{r'_j}(X^1(R_j^1)^{-1})^{r_j}, (y^{r'_j}(X^2(R_j^2)^{-1})^{r_j})) = (g^{r'_j}(g^r(R_j^1)^{-1})^{r_j}, y^{r'_j}(y^r g^{b'}(R_j^2)^{-1})^{r_j})$, where R_j, $j \in [1; N]$ is the ElGamal encryption of each user U_j's biometrics stored in the $\mathcal{DB}$ during enrollment.
- Finally, $\mathcal{AS}$ runs an efficient PIR protocol to obtain the value C corresponding to the user U from the $\mathcal{DB}$ and decrypts it using his secret key sk.
  If $\mathsf{Dec}(C)$=1, $\mathcal{AS}$ authenticates U, else rejects.

Secondly, [2] uses Goldwasser-Micali encryption and a different PIR scheme for storing biometrics as encrypted sketches, which we summarize as below.

In the enrollment phase, the user U registers at the $\mathcal{DB}$ by sending $R = (R^1, R^2) = \mathsf{Enc}(\mathsf{PAR}, pk)$ and $H(c)$, namely the encryption of its biometric sketch $\mathsf{PAR} = c \oplus b$ using Goldwasser-Micali encryption scheme and the hash of the codeword c, i.e. $H(c)$ to $\mathcal{DB}$, where the parameter PAR is not publicly available as in [4,16]. The user also registers his pseudorandom identifier ID and $H(c)$ at the $\mathcal{AS}$. For authentication, the following steps are performed.

- $\mathcal{S}$ sends the user identity ID to the $\mathcal{AS}$ and the encryption of the fresh biometrics $X = (X^1, X^2) = \mathsf{Enc}(b', pk)$ using Goldwasser-Micali encryption.
- $\mathcal{S}$ integrates the encrypted biometrics of the user into the PIR request that is sent to the $\mathcal{DB}$, which returns the encryption of $c \oplus b' \oplus b$ and the encryption of $H(c)$ to the $\mathcal{AS}$.
- Finally, $\mathcal{AS}$ decrypts the values with the help of the hardware security model that stores the secret keys of the system and obtains $c' = c \oplus b' \oplus b$ and $H(c)$. If $\mathsf{dis}(b, b') < t$, then $\mathcal{AS}$ is able to decode c' and obtains a codeword c''. Next, it checks $H(c) = H(c'')$ to accept/reject the authentication request of U.

As one can notice from the first step of the authentication phase of [4] and [2], the sensor client $\mathcal{S}$ communicates with the $\mathcal{DB}$ to send the fresh encryption of the biometrics, which could be impractical. In practice, there might be only very few organizations that can be trusted by human users to store their biometric information though they may want to use their biometrics for the authentication purpose at many authentication servers. Therefore, in [16], the authors suggest a scenario like that of Single Sign-On systems, where biometric information for all authentication servers are centrally stored and managed. Thus, human users access the authentication server through sensor clients, which are not owned by the authentication server but have a business agreement with the authentication server. Hence, the sensor does not need to communicate with the $\mathcal{DB}$ during the verification phase as in [4,2], instead $\mathcal{S}$ only communicates with the $\mathcal{AS}$. Considering this fact, [16] presents a slightly modified version of the first scheme of [4] by simplifying the randomization step of the $\mathcal{DB}$.

5 A New Attack

Considering the security model for identity privacy as described in section 3.1, we first assume that the adversary produces two biometric templates (b_i^0, b_i^1) for the target user U_i with ID_i such that $\mathsf{dis}(b_i^0, b_i^1) < t$, where t is the error correction threshold of the secure sketch scheme. We call this first attack as $Atk1_{\mathcal{A}}$, which successfully distinguishes the template that was registered for the challenge user ID_i using the public helper data PAR_i, which is the output of the secure sketch in order to be used to error correct the biometrics.

For the attack $Atk1_{\mathcal{A}}$, the adversary can easily distinguish which template was chosen by the challenger to be registered for U_i by looking at the output of the decoding function of the secure sketch. If he correctly guessed the template

Attack $Atk1_{\mathcal{A}}$	Attack $Atk2_{\mathcal{A}}$
For $(i, ID_i, b_i^0, b_i^1, (ID_j, b_j)_{\{j \neq i\}}) \leftarrow \mathcal{A}(1^l)$.	For $(i, ID_i, b_i^0, b_i^1, (ID_j, b_j)_{\{j \neq i\}}) \leftarrow \mathcal{A}(1^l)$
$b_i^\beta \xleftarrow{R} \{b_i^0, b_i^1\}$	$b_i^\beta \xleftarrow{R} \{b_i^0, b_i^1\}$
$b_i = b_i^\beta$	$b_i = b_i^\beta$
$\emptyset \leftarrow Enrollment((ID_j, b_j)_j)$	$\emptyset \leftarrow Enrollment((ID_j, b_j)_j)$
Use public data of ID_i: $\mathsf{PAR}_i = c \oplus b_i^\beta$	Use public data of ID_i: $\mathsf{PAR}_i = c \oplus b_i^\beta$
Compute $b_i^1 \oplus \mathsf{PAR}_i = c'$	Compute $b_i^1 \oplus \mathsf{PAR}_i = c'$
If $\mathsf{Decode}(c') = c'$	If $\mathsf{Decode}(c') = \perp$
Return $\beta = 1$	Return $\beta = 0$
Else if $\mathsf{Decode}(c') = b_i^0 \oplus \mathsf{PAR}_i$	Else If $\mathsf{Decode}(c') = b_i^1 \oplus \mathsf{PAR}_i$
Return $\beta = 0$	Return $\beta = 1$

b_i^1, then the computation of $b_i^1 \oplus \mathsf{PAR}_i$ will result in a correct codeword, which does not need to be error corrected. Otherwise, he returns $\beta = 0$.

The second case we consider is that the adversary produces two biometric templates (b_i^0, b_i^1) for the target user ID_i with $\mathsf{dis}(b_i^0, b_i^1) > t$, which we call as $Atk2_{\mathcal{A}}$. We note that this pair of templates still describe the same user U_i, since the variation of the biometrics can be larger then the error-correction capacity of the secure sketch. Our attack successfully distinguishes the template that was registered for the challenge user ID_i using the public helper data PAR_i. The difference to the previous attack is that, if b_i^1 is not the template that was registered by the challenger $\mathcal{C}$, then, since the distance between the two templates (b_i^0, b_i^1) is above the error-correction capacity, the decoding procedure will not work. Thus, the registered template is b_i^0, and $\mathcal{A}$ returns $\beta = 0$.

The reason that the public data PAR of the secure sketch scheme helps the adversary in the identity privacy game is due to the fact that for secure sketch construction the standard notions of security do not fit. The statement "PAR leaks no information about the biometric template b" is normally formalized by requiring that b and PAR be almost statistically independent. Even the analogue requirement for computationally bounded adversaries, semantic security, is impossible here: if Eve knows that b is one of two similar strings (b_1, b_2), then she can compute b from PAR and b_1. The difficulty, then, is that the standard definitions of security require secrecy even when Eve knows a lot about b, which is in contrast to the security of sketches, where Eve is sufficiently uncertain about b, since biometrics is assumed as secret data. In [6], it is shown that secure sketches can only guarantee entropic security, which assumes that the adversary is sufficiently uncertain about the user's biometrics, which implies that secure sketches can never guarantee the notion of indistinguishability for computationally bounded adversaries. Thus, the schemes of [4,16] and any biometric remote authentication scheme that assumes biometrics and the required secure sketch as public data are vulnerable to this attack and cannot satisfy identity privacy.

As opposed to the schemes of [4,16], the scheme of [2] stores the sketch as encrypted in the $\mathcal{DB}$. Thus, a malicious $\mathcal{AS}$ has only access to different corrupted codewords $c'_{ik} = \mathsf{PAR}_i \oplus b'_{ik}$, where b'_{ik} is the fresh biometrics of the user U_i at the k^{th} authentication run. However, this data can also help the malicious $\mathcal{AS}$

when playing the identity privacy game, since there is no restriction on the two templates the adversary generates for the challenge user U_i. Assume that the adversary knows that biometrics of U_i behave according to some distribution, and has determined the mean of this distribution after taking enough samples; a well-motivated adversary can take more measurements, and thus determine the mean more accurately. Let the adversary set one of the two templates he generates in the game as equal to the mean value of this distribution, i.e. $b_i^0 = \mu$ and the second template he has to output equal to the value that is the maximum (allowable) distance to the mean, i.e. $b_i^1 = \mu + \delta$, where 2δ denotes the variability of the biometrics of U_i with identity ID_i, namely the range of U_i's biometrics. Enough number of samples $\{b_{ir}^S\}_{1<r<M}$ of U_i's biometric data b_i allows the adversary to compute this range information. Since the malicious $\mathcal{AS}$ performs the decoding of the corrupted codeword c_i' for user U_i and obtains the correct codeword c_i that was used in $\mathsf{PAR}_i = c_i \oplus b_i^\beta$, $\mathcal{AS}$ has access to c_{ik}''s for $1 < k < M$ obtained at the k^{th} authentication run of U_i and the unique codeword c_i after decoding each corrupted codeword c_{ik}'. The attack is denoted by $Atk3_{\mathcal{A}}^*$.

Attack $Atk3_{\mathcal{A}}^*$

For $(i, ID_i, b_i^0, b_i^1, (ID_j, b_j)_{\{j \neq i\}}) \leftarrow \mathcal{A}(1^l)$ s.t. $b_i^0 = \mu$ and $b_i^1 = \mu + \delta$
$b_i^\beta \xleftarrow{R} \{b_i^0, b_i^1\}$
$b_i = b_i^\beta$
$\emptyset \leftarrow Enrollment((ID_j, b_j)_j)$
At the k^{th} authentication run of ID_i ,where $1 < k < M$
    Obtain the data of ID_i, $\mathsf{PAR}_i \oplus b_{ik}' = c_i \oplus b_i^\beta \oplus b_{ik}' = c_{ik}'$
    If $\mathsf{Decode}(c_{ik}') = c_i$, store $e_{ik} = c_{ik}' \oplus c_i$.
Compute $a = Mean(HW(e_{ik}))$, $b = Mean(HW(b_{ir}^S \oplus b_i^0))$ and $c = Mean(HW(b_{ir}^S \oplus b_i^1))$
If $a \approx b$ return $\beta = 0$, else if $a \approx c$ return $\beta = 1$

The intuition of this attack is that by setting one of the templates to the mean of the distribution of U_i's biometrics, and the other template to the maximum value of its range, listening to enough protocol runs of U_i allows the adversary to distinguish which template was registered using a statistical attack on the errors. Since the hamming weight HW of the error $e_{ik} = b_i^\beta \oplus b_{ik}'$ when $b_i^\beta = b_i^0$ will be significantly less than the hamming weight of the error when $b_i^\beta = b_i^1$, we can apply various statistical analysis methods by comparing the errors obtained from the authentication runs of U_i to the simulated errors based on the distribution of the U_i's biometrics and determine the value of β.

An alternative way to analyze the error and determine the value of β could be described by the following algorithm. Similar to the attack $Atk3_{\mathcal{A}}^*$, in this attack we expect that the majority of the fresh templates presented to the sensor to be concentrated around the mean template b_i^0 of user U_i. Thus, computing an intermediate value b_i^2 can help us to determine the value of β. The exact value of b_i^2 could be set based on the distribution of the biometrics and other experiments.

Thus, the condition on the two templates generated by $\mathcal{A}$ must be specified in a concrete way to avoid such statistical attacks. However, with this current

Attack $Atk3^{**}_{\mathcal{A}}$

For $(i, ID_i, b_i^0, b_i^1, (ID_j, b_j)_{\{j\neq i\}}) \leftarrow \mathcal{A}(1^l)$ s.t. $b_i^0 = \mu$ and $b_i^1 = \mu + \delta$
$b_i^\beta \xleftarrow{R} \{b_i^0, b_i^1\}$
$b_i = b_i^\beta$
$\emptyset \leftarrow Enrollment((ID_j, b_j)_j)$
Compute $b_i^2 \approx \mu + \delta/2$
At the k^{th} authentication run of ID_i ,where $1 < k < M$
    Obtain the data of ID_i, $\mathsf{PAR}_i \oplus b'_{ik} = c_i \oplus b_i^\beta \oplus b'_{ik} = c'_{ik}$
    If $\mathsf{Decode}(c'_{ik}) = c_i$, store $e_{ik} = c'_{ik} \oplus c_i$.
Compute $a = Mean(HW(e_{ik})$, $b = (HW(b_i^2 \oplus b_i^0))$
If $a < b$ return $\beta = 0$, else return $\beta = 1$

definition of identity privacy, this is not possible since the generation of the two templates is controlled by the adversary. Thus, one should modify the identity privacy notion to avoid statistical attacks. One possible solution is adapting a weaker security notion of public key encryption to our setting. This weaker notion is called as Weak-Indistinguishability where the adversary cannot select challenge plaintexts (m_0, m_1), instead the challenger computes (m_0, m_1) and returns them to the adversary [17]. The same idea could be applied to identity privacy notion, where the two possible templates for U_i are computed by the challenger using the biometric template space BtSp associated to the user U_i. Then, one of the two templates presented by the challenger to the adversary is registered to the database. If the two templates $\{b_i^0, b_i^1\}$ are chosen close to each other, then we may refer to the notion of *Indistinguishability of Errors*, which prevents an insider adversary to obtain some information about the reference template of U_i based on the errors he collects.
Thus, Weak-Identity Privacy is defined as follows:

Experiment $Exp_{\mathcal{A}}(l)$
For $(i, ID_i, (ID_j, b_j)_{\{j\neq i\}}) \leftarrow \mathcal{A}(1^l)$
$\{b_i^0, b_i^1\} \leftarrow \mathsf{BtSp}(U_i)$
$b_i^\beta \xleftarrow{R} \{b_i^0, b_i^1\}$
$b_i = b_i^\beta$
$\emptyset \leftarrow Enrollment((ID_j, b_j)_j)$
$\beta' \leftarrow \mathcal{A}(Challenger; Verification)$
if $\beta' = \beta$ return 1 else return 0

A biometric authentication scheme satisfies Weak-Identity Privacy if equation (1) is negligible. Under this weaker notion, [2] is secure against statistical attacks. The security analysis based on this weaker notion is identical to the analysis presented in [2].

6 Preventing the Attacks

As we show in the previous section, for each different scheme, we have a different attack based on the properties/architecture of the system. For statistical

attacks against schemes with encrypted sketches, we suggest to evaluate the security of the scheme based on our new notion called Weak-Identity privacy. Other sketch-based schemes used for equality testing can be made resistant against our attacks through the following solutions. The first solution is to store the sketch PAR secretly for the schemes of [4,16], for instance in the tamper-proof smartcard of the user. This will result in a multi-factor authentication scheme, thus, the system is not anymore a pure biometric based authentication scheme. Still, this solution does not cover a brute-force attack if these systems are employed for biometrics that can be represented as a set of features with a small feature space. Since encryption of each feature is performed individually, an insider adversary can try different feature sets to obtain some information on the stored template of the user from the authentication result. For a large feature space, he can mount an attack similar to the statistical attack of the previous section. Specifically, if the biometrics is represented as an ordered set of features as in face biometrics, the adversary can generate the two templates in such a way that the first template includes some particularly chosen features, whereas the second template does not. By observing the matching/non-matching of these particular features, the malicious server can distinguish which template is registered by the challenger. It is cancelable biometrics that can prevent this attack, if the stored template is somehow distorted, where the distortion parameters are unknown to the insider adversary. Specifically, if we define identity privacy in a different setting, then biometric remote authentication schemes assuming biometrics as public data can achieve Identity privacy if they are combined with cancelable biometrics. The cancelable biometrics system we use requires a high entropy randomness that is stored in the user's smart card to be used later for authentication in the transformed space. This way, biometric data stored at the server is protected through this transformation and biometrics can be updated by changing the transformation function or the randomness. This system also prevents the user's traceability across different biometric databases, even if the (distorted) biometric templates are stored in clear. Example systems employing a high entropy randomness stored in a smart card for cancelable biometrics are given in [8,5,10].

Our proposed design is a multi-factor solution that requires each user to possess a smartcard to store some high entropy randomness that will be hashed with the biometrics before the encryption (and storage in the $\mathcal{DB}$). So the same randomness is used during verification by hashing it with the fresh biometrics and after that, the encryption of the result is transmitted to the server side for matching. If a secure sketch is applied, then first biometrics are corrected with the help of PAR, then the randomness is hashed with the corrected biometrics and encryption is performed afterwards. Also, our proposal allows for the integration of a secure sketch without endangering the security of the scheme, since the value PAR is only stored in the tamper-proof smart card of the user. This way, the secrecy of the relationship between the identity and the stored (distorted) biometrics of the user is maintained based on the privacy of the randomness used in the distortion of the biometrics, which is stored in the tamper-proof

smartcard of the user. This solution guarantees the two security notions even if we employ a secure sketch and biometrics with small feature space. Finally, we use a cryptographic hash function for the computation of the distorted biometrics, thus, statistical attacks are not possible as even one bit of change of the input of the hash function leads to a complete different hash value.

6.1 A New Protocol

In this section, we describe an example scheme that achieves weak-identity privacy for biometrics represented as an ordered set of features and (standard) identity privacy for biometrics represented as a binary string. The new scheme is defined in cancelable biometrics setting, where we assume biometrics as public data but the randomness used in the distortion of the biometric features is kept as secret. We assume biometrics as an ordered set of features such as face, iris, voice, handwritten signatures [9], however, the system also works for biometrics defined as a binary string such as an 2048-bit Iris code. The matching of the fresh biometrics and the stored template is performed as in [13] with the help of bilinear pairings, where the authentication server $\mathcal{AS}$ does not need a secret key for its operations. This is an important difference to the existing schemes [4,16,2], which store the biometrics as encrypted with the public key of the $\mathcal{AS}$. Thus, if the secret key of the $\mathcal{AS}$ is leaked, then each user in the system has to re-register in the best case scenario, i.e. before the compromise of the $\mathcal{DB}$, whereas the compromise of the $\mathcal{AS}$ does not affect the security of our system as $\mathcal{AS}$ does not need its secret key for its computations due to the use of bilinear pairings, hence, does not store any secret key. Finally, we assume the general representation of biometrics, where a biometric template B_e consists of k features, i.e. $B_e = \{w_i\}_{1 \leq i \leq k}$. A possible attack for this type of biometrics occurs when the feature space is small. A malicious $\mathcal{AS}$ may compare the encryption of different features to the authentication data and using pairings, he decides whether he correctly guessed the feature. Since we concatenate a different random string to each feature, based on the secrecy of these distortion values applied to each feature, the adversary cannot launch this brute-force attack. In our scheme, we use the same architecture of [16] as summarized in section 4, which does not require a detached verification unit $\mathcal{VU}$ and the sensor does not communicate with the biometric database as in many real-life applications.

Enrollment Phase

- $\mathcal{S}$ generates his key pair $(pk_{\mathcal{S}}, sk_{\mathcal{S}})$ and publishes the two keys. In addition, $\mathcal{AS}$ is given an elliptic curve ElGamal public key $pk_{\mathcal{AS}} = g^y$ without the associated secret key, for instance, a trusted third party can generate this public key. Finally, a cryptographic hash function $H : \{0,1\}^* \rightarrow \mathbb{G}$ and a bilinear pairing $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{F}$ are required.
- The user U generates his personalized username ID and registers it at the $\mathcal{AS}$, computes his distorted biometrics by picking at random $r_i \in \mathbb{Z}_q$ for $i \in [1; k]$ to compute $H(w_i, r_i)$ and registers his distorted biometric features as

$R_i = (R_i^1, R_i^2) = (g^{r_i}, g^{yr_i} H(w_i, r_i))$ for $i \in [1;k]$ at the $\mathcal{DB}$. The distortion numbers $\{r_1, ..., r_k\}$ are stored at the tamper-proof smartcard of U.

Remark 1. To further increase the accuracy, a secure sketch for ordered biometrics can be used, whose public parameter PAR is only stored in the tamperproof smartcard of the user together with the distortion numbers, thus PAR is not publicly available as in the schemes of [4,16,2]. This is required to guarantee the identity privacy notion if a secure sketch is employed.

Verification Phase

- $\mathcal{S}$ sends the user U's identity ID and the encrypted fresh biometrics for $i \in [1;k]$, $X_i = (X_i^1, X_i^2) = \mathsf{Enc}(H(w_i', r_i), pk_{\mathcal{AS}}) = (g^{x_i}, g^{yx_i} H(w_i', r_i))$ to the $\mathcal{AS}$ using ElGamal encryption and the distortion values r_i's stored in the smartcard. $\mathcal{S}$ sends his signature σ on $X = \{X_i : i \in [1;k]\}$ to $\mathcal{AS}$.
- $\mathcal{AS}$ verifies the signature of $\mathcal{S}$ and communicates with the $\mathcal{DB}$.
- $\mathcal{DB}$ computes for each entry $j \in [1, N]$ the rerandomization of R_{ji},where R_{ji} is the encryption of the i^{th} feature of the j^{th} user's distorted biometrics. For instance, the rerandomization for U's biometric template is computed as $C_i = (C_i^1, C_i^2) = (g^{\beta_i} R_i^1, g^{y\beta_i} R_i^2) = (g^{\beta_i + r_i}, g^{y\beta_i + yr_i} H(w_i, r_i))$ for $i \in [1;k]$.
- $\mathcal{AS}$ first retrieves the index for ID and runs an efficient PIR protocol to obtain the user U's rerandomized biometrics denoted as C_i for each feature of U. Next, $\mathcal{AS}$ selects a random $s_i \in \mathbb{Z}_q$ and computes for each biometric feature of U, $Z_i = (X_i \oslash C_i)^{s_i}$, where, for any integer x and two ElGamal ciphertexts (c_1, c_2) and (c_3, c_4), the operator $\oslash$ is defined as follows: $((c_1, c_2) \oslash (c_3, c_4))^x = ((\frac{c_1}{c_3})^x, (\frac{c_2}{c_4})^x)$. Thus, for the matching features, we obtain $Z_i = (Z_i^1, Z_i^2) = ((g^{x_i} \cdot (g^{\beta_i + r_i})^{-1})^{s_i}, (g^{yx_i} \cdot (g^{y\beta_i + yr_i})^{-1})^{s_i})$.
  Finally, $\mathcal{AS}$ finds the total number of matched features using bilinear pairings. Here, $\mathcal{AS}$ obtains $\hat{e}(pk_{\mathcal{AS}}, Z_i^1) = \hat{e}(g, Z_i^2)$ for the matching features by computing in total $2k$ bilinear pairings. If the number of Z_i's satisfying this equation is above the threshold, $\mathcal{AS}$ authenticates U, else rejects.

Lemma 1. *The proposed scheme achieves identity privacy against the $\mathcal{AS}$, based on the Gap DH problem and the tamper-proofness of the user smartcard.*

Lemma 2. *The proposed scheme achieves transaction anonymity against a malicious $\mathcal{DB}$, based on the security (user privacy) of the PIR protocol.*

Due to the page limitations, the proofs will be presented in the full version of this paper.

6.2 Identity Privacy for Cancelable Biometrics: A New Notion

Our first solution presented in the previous section guarantees identity privacy due to the one-wayness property of the cancelable biometrics and the secrecy of the helper data PAR. Thus, in order to distinguish one of the biometric templates, the adversary playing the identity privacy game as described in [3] has

to break the one-wayness of the cancelable biometrics, where one-wayness is a weaker security notion than indistinguishability. To overcome this limitation, we define the following notion, where breaking this new notion implies breaking the underlying encryption scheme in the sense of indistinguishability, which is a stronger security notion.

Given an adversary $\mathcal{A}$ running against the biometric authentication scheme and a challenger $\mathcal{C}$ that simulates the registration phase of the scheme, we consider the following game between $\mathcal{A}$ and $\mathcal{C}$.

Experiment $Exp_A(l)$
For $((ID_j, b_j, r_j, PAR_j)_{\{j \neq e\}}) \leftarrow \mathcal{A}(1^l)$
$(e \neq j, ID_e, b_e, r_e^0, r_e^1, PAR_e) \leftarrow \mathcal{A}(1^l)$
$r_e^\beta \overset{R}{\leftarrow} \{r_e^0, r_e^1\}$
$r_e \leftarrow r_e^\beta$
$\emptyset \leftarrow Enrollment^*(Distortion(b_j, r_j)_j)$
$\beta' \leftarrow \mathcal{A}(Challenger; Verification)$
if $\beta' = \beta$ return 1 else return 0

A biometric authentication scheme satisfies the notion of "Identity Privacy for Cancelable Biometrics" if equation (1) is negligible. Here, the adversary $\mathcal{A}$ generates the authentication data for $N-1$ users together with the reference biometrics b_j, the secure sketch PAR, and two different distortion parameters for an additional user U_e. $\mathcal{C}$ picks at random a distorion parameter $r_e = r_e^\beta$. Next, the chosen distortion parameter is applied to the reference biometric template and the enrollment phase is completed. The difference of our notion to the Bringer et al.'s identity privacy notion [3,2,16] is that the $\mathcal{C}$ does not need to choose randomly one of the two similar biometrics generated by the adversary $\mathcal{A}$, since with the public value PAR, the error-corrected template can be easily computed and a unique reference template b_e is obtained. Thus, $\mathcal{C}$ only needs to apply the random distortion r_j^β to this reference template b_j and then register the encryption of this distorted biometrics in the $Enrollment^*$ phase. This application could be performed as in the protocol described in section 6.1, by simply picking at random $r_e^1, r_e^2 \in \mathbb{Z}_q$ as input to the hash function. After running the verification protocol, $\mathcal{A}$ outputs a guess for the distortion parameter that $\mathcal{C}$ has chosen. One can easily show that the schemes of [4,16] achieve identity privacy for cancelable biometrics against a malicious $\mathcal{AS}$, based on the semantic security of the ElGamal encryption although the sketch PAR is public. The proof is identical to the proofs presented in [4,16] for biometrics represented as a fixed length binary string. If biometrics is represented as a set of features, a set of randomly picked distortion parameters is applied instead of a single parameter.

7 Comparison

In this section, we present an overview of the protocols designed according to the model of Bringer et al. We compare the schemes based on the security notions they achieve and whether the schemes are still secure even if the secret key of the verification unit in [3,1] or the secret key of the authentication server in [16,4] is

leaked, where this key is required for the matching stage and the final decision. In our scheme the authentication server does not know his secret key and uses bilinear pairings for the matching in the encrypted domain, thus, our scheme is resistant against this attack. $^{+}$ denotes the first biometric scheme.

Table 1. Comparison of distributed biometric remote authentication schemes

Scheme	Identity Privacy	Transaction Anonymity	Security against Key Compromise	Current Attacks
Sys. 1 [3]	No	No	No	Attack of [15]
Sys. 2 [1]	Yes	Yes	No	Attack of [15]
Sys.$^{+}$3 [4]	No	Yes	No	$Atk1_{\mathcal{A}}, Atk2_{\mathcal{A}}$
Sys. 4 [2]	No	Yes	No	$Atk3^{*}_{\mathcal{A}}, Atk3^{**}_{\mathcal{A}}$
Sys. 5 [16]	No	Yes	No	$Atk1_{\mathcal{A}}, Atk2_{\mathcal{A}}$
New Sys.	Yes	Yes	Yes	-

8 Conclusion

In this paper, we present three new attacks that reveal the reference biometric template of the user to the malicious server. The first type of attack applies to any system that assumes biometrics and the sketch as public data since a secure sketch can only guarantee a weak level of security. However, if the sketch is stored secretly, i.e. in a tamper-proof smartcard, then the systems are secure for biometrics represented as a fixed length binary string. The second type of attack is a statistical attack, which works even if the sketch is stored as encrypted at the database. Consequently, the security of pure biometric remote authentication schemes is questionable if they are evaluated in the framework of a realistic and strong security model. Thus, we suggest that BRA systems should be implemented as a two-factor authentication system, which employs a tamper-proof smartcard for storing additional data as the second factor. Besides, the current systems are not suitable for other biometric traits that are represented as an ordered/unordered feature set, whereas our new protocol for cancelable biometric setting is both secure against the three types of attacks and resistant for attacks as a result of different representations of biometrics. Finally, if identity privacy is redefined in cancelable biometric setting, the schemes vulnerable to the first type of attack are secure for public sketches.

Acknowledgement. This work was supported in part by the B-IT Research School within the NRW (North Rhine-Westphalia) Research Schools of Excellence. The author is grateful to her supervisor Prof. Dr. Joachim von zur Gathen for his valuable support, encouragement and guidance. Also, the author is grateful to Prof. Michael Huth and the reviewers of STM for their valuable comments.

References

1. Barbosa, M., Brouard, T., Cauchie, S., de Sousa, S.M.: Secure Biometric Authentication with Improved Accuracy. In: Mu, Y., Susilo, W., Seberry, J. (eds.) ACISP 2008. LNCS, vol. 5107, pp. 21–36. Springer, Heidelberg (2008)

2. Bringer, J., Chabanne, H.: An Authentication Protocol with Encrypted Biometric Data. In: Vaudenay, S. (ed.) AFRICACRYPT 2008. LNCS, vol. 5023, pp. 109–124. Springer, Heidelberg (2008)
3. Bringer, J., Chabanne, H., Izabachène, M., Pointcheval, D., Tang, Q., Zimmer, S.: An Application of the Goldwasser-micali Cryptosystem to Biometric Authentication. In: Pieprzyk, J., Ghodosi, H., Dawson, E. (eds.) ACISP 2007. LNCS, vol. 4586, pp. 96–106. Springer, Heidelberg (2007)
4. Bringer, J., Chabanne, H., Pointcheval, D., Tang, Q.: Extended Private Information Retrieval and its Application in Biometrics Authentications. In: Bao, F., Ling, S., Okamoto, T., Wang, H., Xing, C. (eds.) CANS 2007. LNCS, vol. 4856, pp. 175–193. Springer, Heidelberg (2007)
5. Cambier, J., von Seelen, U.C., Moore, R., Scott, I., Braithwaite, M., Daugman, J.: Application specific biometric templates. In: IEEE Workshop on Automatic Identification Advanced Technologies, pp. 167–171. IEEE (2002)
6. Dodis, Y., Smith, A.: Correcting errors without leaking partial information. In: STOC 2005, pp. 654–663. ACM (2005)
7. El Gamal, T.: A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 10–18. Springer, Heidelberg (1985)
8. Hirata, S., Takahashi, K.: Cancelable Biometrics with Perfect Secrecy for Correlation-Based Matching. In: Tistarelli, M., Nixon, M.S. (eds.) ICB 2009. LNCS, vol. 5558, pp. 868–878. Springer, Heidelberg (2009)
9. Li, Q., Sutcu, Y., Memon, N.D.: Secure Sketch for Biometric Templates. In: Lai, X., Chen, K. (eds.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 99–113. Springer, Heidelberg (2006)
10. Sakashita, T., Shibata, Y., Yamamoto, T., Takahashi, K., Ogata, W., Kikuchi, H., Nishigaki, M.: A Proposal of Efficient Remote Biometric Authentication Protocol. In: Takagi, T., Mambo, M. (eds.) IWSEC 2009. LNCS, vol. 5824, pp. 212–227. Springer, Heidelberg (2009)
11. Sarier, N.D.: A New Approach for Biometric Template Storage and Remote Authentication. In: Tistarelli, M., Nixon, M.S. (eds.) ICB 2009. LNCS, vol. 5558, pp. 909–918. Springer, Heidelberg (2009)
12. Sarier, N.D.: A survey of distributed biometric authentication systems. In: BIOSIG 2009. LNI, vol. 155, pp. 43–55. GI (2009)
13. Sarier, N.D.: Improving the accuracy and storage cost in biometric remote authentication schemes. J. Network and Computer Applications 33(3), 268–274 (2010)
14. Sarier, N.D.: Practical Multi-factor Biometric Remote Authentication. In: BTAS 2010, pp. 1–6. IEEE (2010)
15. Simoens, K., Bringer, J., Chabanne, H., Seys, S.: Analysis of biometric authentication protocols in the blackbox model. CoRR, abs/1101.2569 (2011)
16. Tang, Q., Bringer, J., Chabanne, H., Pointcheval, D.: A Formal Study of the Privacy Concerns in Biometric-Based Remote Authentication Schemes. In: Chen, L., Mu, Y., Susilo, W. (eds.) ISPEC 2008. LNCS, vol. 4991, pp. 56–70. Springer, Heidelberg (2008)
17. Yang, G., Tan, C.H., Huang, Q., Wong, D.S.: Probabilistic Public Key Encryption with Equality Test. In: Pieprzyk, J. (ed.) CT-RSA 2010. LNCS, vol. 5985, pp. 119–131. Springer, Heidelberg (2010)