Neyire Deniz Sarier (2009). Biometric Identity Based Signature Revisited. In *Public Key Infrastructures, Services and Applications*, Fabio Martinelli & Bart Preneel, editors, volume 6391 of *Lecture Notes in Computer Science*, 271–285. Springer-Verlag. ISBN 978-3-642-16441-5. ISSN 0302-9743. URL https://dx.doi.org/10.1007/978-3-642-16441-5_18.

Biometric Identity Based Signature Revisited

Neyire Deniz Sarier

Bonn-Aachen International Center for Information Technology
Computer Security Group
Dahlmannstr. 2, D-53113 Bonn Germany,
denizsarier@yahoo.com

Abstract. In this paper, we describe a new biometric Identity Based Signature (IBS) scheme based on the Sakai Kasahara Key Construction and prove its security in the framework of a stronger security model compared to exisiting adversarial models. Besides, we present a new type of a denial of service (DoS) attack and evaluate existing biometric IBS schemes in this context. Based on the recently defined privacy notions, we show that our scheme achieves weak signer-attribute privacy and the security is reduced to the k-DHI computational problem in the ROM with an efficient reduction. Finally, our scheme is compared to other error tolerant signature schemes and shown to be much more efficient in terms of its each phase.

Keywords: Biometrics, fuzzy IBS, t-ABS, Unforgeability.

1 Introduction

In Eurocrypt'05, Sahai and Waters proposed a new Identity Based Encryption (IBE) system called fuzzy IBE that uses biometric attributes as the identity instead of an arbitrary string like an email address. This new system combines the advantages of IBE with those of biometric identities, where IBE avoids the need for an online Public Key Infrastructure (PKI), which is the most inefficient and costly part of Public Key Encryption (PKE). Fuzzy IBE could be used in an ad-hoc setting where the users are unprepared, namely without having any public key or even predefined e-mail addresses. Instead, the signer could present his biometrics to the verifier, who can check the signature for validity using the biometric identity of the signer. Besides, the use of biometric identities in the framework of IBE simplifies the process of key generation at the Private Key Generator (PKG). Since biometric information is unique, unforgettable and non-transferable, the user only needs to provide his biometrics at the PKG under the supervision of a well-trained operator to avoid biometric forgery and to obtain his private key instead of presenting special documents and credentials to convince the PKG about his identity. It should be noted that biometrics is assumed as public information, hence the compromise of the biometrics does not affect the security of the system. This point of view is also accepted in the biometrics community, where the raw biometric data is assumed as public data whereas

the revocable biometric template that is stored in a central database or on a smartcard for biometric authentication is considered as private data. The signature analogue of fuzzy IBE is introduced in [21], where a provably secure fuzzy Identity Based Signature (IBS) scheme is described. Since the error tolerance property is satisfied, fuzzy IBS of [21] is applicable for biometric identities and it shares the same advantages of fuzzy IBE.

The private key components of a fuzzy system are generated by combining the values of a unique polynomial on each feature of the biometrics with the master secret key ms of PKG. However, due to the noisy nature of biometrics, a fuzzy system allows for error tolerance in the decryption stage for fuzzy IBE (or in the verification stage for fuzzy IBS). Particularly, a signature constructed using the biometrics ID could be verified by the receiver using a set of publicly computable values corresponding to the identity ID', provided that ID and ID' are within a certain distance of each other. Moreover, fuzzy IBS could be considered in the context of Attribute Based Signature (ABS), which allows the signer to generate a signature using the attributes she possess.

Another approach for incorporating biometrics into IBS is presented in [5], where the error tolerance is provided by a different identity structure compared to fuzzy IBS, namely by integrating a fuzzy extractor into the IBS scheme. This way, both the signer and verifier operate with the same public key, which is required for standard cryptographic schemes.

1.1 Related Work

The first fuzzy IBE scheme is described by Sahai and Waters in [13] and the security is reduced to the MBDH problem in the standard model, where the size of the public parameters is linear in the number of the attributes of the system or the number of attributes (or features) of a user. More efficient fuzzy IBE and biometric IBE schemes are achieved with short public parameter size by employing the random oracle model (ROM) [12, 1, 9, 15].

Burnett et al [5] described the first biometric IBS scheme called BIO-IBS, where they used the biometric information as the identity and construct the public key (namely the identity) of the signer using a fuzzy extractor [8], which is then used in the modified SOK-IBS scheme [3]. Despite the fuzzy extraction process, the scheme is very efficient compared to fuzzy IBS of [21], which is the signature analogue of fuzzy IBE. However BIO-IBS is not secure against a new type of Denial of Service (DoS) attack that we are going to present in the next section.

Besides, the fuzzy IBS scheme of [21] is provably secure in the standard model, where the scheme is based on the Sahai-Waters construction [13] and the two level hierarchical signature of Boyen and Waters [20] and its security is reduced to the computational DH problem. However, the scheme is very inefficient due to the $d(n+4)$ exponentiations and the $d+2$ bilinear pairing computations during the verification process, where d is the error tolerance parameter of the scheme and n is the size of the feature (i.e. attribute) set of each user. Recently, a threshold ABS (t-ABS) scheme [16] with the same key generation phase as of fuzzy IBS and

with threshold attribute based verification is designed, which suffers from the same disadvantages described for the fuzzy IBS. Due to the threshold verification, t-ABS can also be implemented as a biometric IBS scheme as opposed to other ABS schemes [11, 10, 18], which are proven secure in the ROM or generic group model. Thus, there is a need to devise an efficient and provably secure signature scheme with error-tolerance property in order to integrate biometric data.

1.2 Our Contribution

In this paper, we present a new biometric IBS scheme that is more efficient compared to the fuzzy IBS of [21] and the t-ABS scheme of [16] when implemented for biometric identities. Moreover, our scheme could function as a fuzzy IBS or threshold ABS (t-ABS) scheme and it is immune against a new type of a DoS attack that we are going to introduce. The new scheme is based on the Sakai Kasahara Key Construction [14] and the security is reduced to the k-DHI computational problem in the ROM with a different proof compared to [7, 6, 2]. The verification phase of the new scheme requires d exponentiations in group $\mathbb{G}$ and d pairing computations instead of $d(n+4)$ exponentiations and $d+2$ pairings as in [21, 16] and achieves much shorter public parameter size, private key and signature sizes compared to [21, 16]. Also, we have a structurally simpler key generation algorithm compared to [21, 16], where the number of exponentiations in the group $\mathbb{G}$ is reduced from $n(n+4)$ as in [21, 16] to n and the cost of signing is half of the existing schemes. Finally, we do not require a MapToPoint hash function as opposed to the modified t-ABS scheme, which is obtained by replacing the computationally expensive T function in t-ABS of [16] with a MapToPoint hash function as described in [12]. The details of the modified t-ABS scheme and the security reduction of our new scheme in the framework of a stronger adversarial model is presented in the Appendix.

1.3 Outline of the Paper

In section 2, we will state the necessary definitions and security model for fuzzy IBS. In section 3, we present a new type of DoS attack and evaluate existing biometric IBS schemes with respect to this attack. Next, we describe our scheme and prove its security. Finally, we compare our scheme to related schemes that are provably secure and conclude our proposals in section 5.

2 Definitions and Building Blocks

In order to introduce the new biometric IBS scheme, at first, we review the definitions and required computational primitives. Given a set S, $x \xleftarrow{R} S$ defines the assignment of a uniformly distributed random element from the set S to the variable x. Biometric identities will be element subsets of some universe, U, of size $|U|$, where each element is associated with a unique integer in $\mathbb{Z}_p^*$ as in [1, 13]. The function $\epsilon(k)$ is defined as negligible if for any constant c, there

exists $k_0 \in \mathbb{N}$ with $k > k_0$ such that $\epsilon < (1/k)^c$. Finally, we define the Lagrange coefficient $\Delta_{\mu_i,S}$ for $\mu_i \in \mathbb{Z}_p$ and a set S of elements in $\mathbb{Z}_p$ as

$$\Delta_{\mu_i,S}(x) = \prod_{\mu_j \in S, \mu_j \neq \mu_i} \frac{x - \mu_j}{\mu_i - \mu_j}$$

Bilinear Pairing: Let $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{F}$ be multiplicative groups of prime order p and let g_1, g_2 be generator of $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively. ψ is an isomorphism from $\mathbb{G}_2$ to $\mathbb{G}_1$ with $\psi(g_2) = g_1$ and $1_{\mathbb{G}_1}, 1_{\mathbb{F}}$ denote the identity elements of $\mathbb{G}_1$ and $\mathbb{F}$, respectively. A bilinear pairing is denoted by $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{F}$ if the following two conditions hold.

1. $\forall\ (u, v) \in \mathbb{G}_1 \times \mathbb{G}_2$ and $\forall\ (a, b) \in \mathbb{Z}$ we have $\hat{e}(u^a, v^b) = \hat{e}(u, v)^{ab}$
2. If $\hat{e}(u, v) = 1_{\mathbb{F}}\ \forall v \in \mathbb{G}_2$, then $u = 1_{\mathbb{G}_1}$, namely the pairing is non-degenerate.

The security of our scheme is reduced to the well-exploited complexity assumption (k-DHI), which is stated as follows.

DH Inversion ((k-DHI) [7]: For $k \in \mathbb{N}$, and $x \xleftarrow{R} \mathbb{Z}_p^*$, $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{F}$, given $(g_1, g_2, g_2^x, g_2^{x^2}, ..., g_2^{x^k})$, computing $g_1^{(1/x)}$ is hard.

2.1 Fuzzy Identity Based Signature

In [21], the generic fuzzy IBS scheme is defined as follows. The same definition applies for t-ABS [16], if the identity consists of a set of attributes.

- **Setup**(1^{k_0}): Given a security parameter k_0, the PKG generates the master secret key ms and the public parameters of the system.
- **Key Generation**: Given a user's identity $ID = \{\mu_1, ..., \mu_n\}$ and the master secret key ms, the PKG returns the corresponding private key D^{ID}. Here, n denotes the size of the set ID.
- **Sign**: A probabilistic algorithm that takes as input the private key D^{ID} associated to the identity ID, public parameters and a message $m \in M$ and outputs the signature σ.
- **Verify**: A deterministic algorithm that given an identity ID' such that $|ID \cap ID'| \geq d$, the signature σ together with the corresponding message m and the public parameters, returns a bit b. Here $b = 1$ means that σ is valid and d denotes the error tolerance parameter of the scheme.

Correctness: A fuzzy IBS scheme has to satisfy the correctness property, i.e., a signature generated by a signer with identity ID must pass the verification test for any ID' if $|ID \cap ID'| \geq d$.

2.2 Signer-Attribute Privacy

In [16], privacy of the signer is guaranteed with an additional algorithm for converting the t-ABS scheme to another signature scheme that is verifiable against the set of signer attributes that are known to the verifier, namely ID' in our setting. This way, the converted signature reveals only the d attributes of ID that are common with ID' chosen by the signer at the time of conversion. This property is defined as weak signer-attribute privacy and it is achieved by the following algorithms for our setting.

- **Convert**: Given the public parameters of the fuzzy IBS, a message signature pair (m, σ), and an identity ID', the signer generates a converted signature $\tilde{\sigma}$ on the message.
- **CvtVerify**: An algorithm that given an identity ID', a message converted-signature pair $(m, \tilde{\sigma})$ and the public parameters, returns a bit b. Here $b = 1$ means that $\tilde{\sigma}$ is a valid converted signature by a signer who has at least d of the attributes in ID', namely $|ID \cap ID'| \geq d$.

In addition, the authors of [16] define the full signer-attribute privacy, which guarantees that the verifier learns nothing more than the fact that $|ID \cap ID'| \geq d$ by combining the converted signature with an interactive verification protocol, which is a zero knowledge proof of knowledge of a valid converted signature with respect to the public inputs. For our scheme, we only consider the weak privacy level.

2.3 Security Model

A fuzzy IBS scheme is selectively unforgable under adaptive chosen message and given identity attacks (SUF-FIBS-CMA) if no probabilistic polynomial time (PPT) adversary has a non-negligable advantage in the game between a challenger and the adversary as follows [21, 16].

- **Phase 1**: The adversary A declares the challenge identity $ID^* = \{\mu_1^*, ..., \mu_n^*\}$.
- **Phase 2**: The challenger runs the Setup algorithm and returns the system parameters to A.
- **Phase 3**: A issues private key queries for any identity ID' such that $|ID' \cap ID^*| < d$. The adversary issues signature queries for any identity.
- **Phase 4**: A outputs a forgery (ID^*, m^*, σ^*), where A does not make a signature query on (m^*, σ^*) for ID^*.

The success of the adversary A is defined as

$$\mathrm{Succ}_A^{SUF-FIBS-CMA} = Pr[Verify(ID^*, m^*, \sigma^*)] = 1$$

For our scheme, we can consider a stronger notion of security, namely existential unforgability against chosen message and identity attacks (EUF-FIBS-CMA), since given a selectively unforgable scheme, one can construct an existentially unforgable scheme by hashing each component of the identity ID with

the hash function H, where H is assumed to be a random oracle. By the employment of the ROM, this stronger notion is achieved with a better reduction cost compared to proofs in the standard model.

Collusion Resistance: It is important to note that the above definition of unforgeability guarantees collusion resistance since users with common biometric features cannot collude to generate a signature that is not generable by one of the colluders.

Remark 1. The security reduction of our scheme allows the adversary A to have as much power as possible by providing A with private key components of any identity ID' including the case of $|ID' \cap ID^*| > d$ except for the component $\mu^* \in ID^*$. Thus, our security model is stronger than the (SUF-FIBS-CMA) model of [21, 16] and the details of this model is presented in Appendix B.

3 A New Attack on BIO-IBS

The first biometric IBS scheme is introduced in [5], where a fuzzy extractor is used to obtain a unique string ID via error correction codes from the biometrics b of the user in such a way that an error tolerance t is allowed. In other words, the same string ID is obtained even if the fuzzy extractor is applied on a different b' such that $dis(b, b') < t$. Here, $dis()$ is the distance metric used to measure the variation in the biometric reading and t is the error tolerance parameter. In particular, the authors of [5] describe a concrete fuzzy extractor using a $[n, k, 2t+1]$ BCH error correction code, Hamming Distance metric and a one-way hash function $H : \{0,1\}^n \rightarrow \{0,1\}^l$. Specifically,

- The **Gen** function takes the biometrics b as input and returns $ID = H(b)$ and public parameter $PAR = b \oplus C_e(ID)$, where C_e is a one-to-one encoding function. This function is called during the key generation phase of BIO-IBS.
- The **Rep** function takes a biometric b' and PAR as input and computes $ID' = C_d(b' \oplus PAR) = C_d(b \oplus b' \oplus C_e(ID))$. $ID = ID'$ if and only if $\mathbf{dis}(b, b') \leq t$. Here C_d is the decoding function that corrects the errors upto the threshold t. This function is called during the verification phase of BIO-IBS.

BIO-IBS scheme of [5] requires the public storage of the value PAR, which is the information needed for error-tolerant reconstruction of the biometric identity string ID and subsequent fuzzy extraction. Since the verification is performed by combining the biometrics b' with the public value PAR of the signer, the presence of an active adversary who maliciously alters the public string PAR leads the verifier to use a wrong public key for the verification due to a different identity string computed by the fuzzy extractor. By the malicious modification of the public value PAR, an adversary cannot gain any secret information but the signature cannot be verified despite being valid. We define this type of DoS attack as Denial of Verification (DoV) attack. Since BIO-IBS is essentially an IBS scheme, no PKI is employed to publish certificates that binds the public value PAR to the signer as in PKE.

The first idea to prevent a DoV attack is using a robust fuzzy extractor, which is resilient to modification of the public value PAR [4], which is also proposed in [5] to prevent a legitimate signer from tampering with PAR in order to later disavow the signature. However, the robust fuzzy sketches/fuzzy extractors described in [4] assumes the biometrics as secret data and replaces the value PAR with $PAR^* = \langle PAR, H(b, PAR)\rangle$, where H is a hash function [4]. Since the adversary knows the biometric data b, he can easily modify the value PAR^* by computing a valid hash value, hence, the verifier cannot detect the modification of the public value.

Another solution is for the verifier to store PAR himself rather than obtain it from the server or the public store, but this defeats the purpose of biometric IBS, where the user does not need to store any additional cryptographic information [4].

However, since the identity ID of our scheme and fuzzy IBS of [21, 16] consists of only the biometric features of the signer, i.e. the schemes do not integrate a fuzzy extractor in order to generate a unique identity string of the signer to be used in a signature scheme, there is no usage of the value PAR necessary for the reconstruction of the unique signer identity. Instead, we allow for a certain amount of error-tolerance in the signer identities ID and ID' that are measured at different times and use the set overlap as the distance metric, where the threshold t represents the error tolerance in terms of minimal set overlap of ID and ID'. Hence, fuzzy IBS of [21, 16] and our scheme are immune against the Denial of Verification attack. It should be noted that DoV attack is a generic attack applicable to any biometric IBE/IBS scheme, where the authenticity of PAR is not provided.

4 A New Efficient Biometric IBS Scheme

The first idea for an efficient biometric IBS Scheme is to modify the t-ABS scheme of [16] by replacing T with a hash function used as a random oracle, which will reduce computational overhead in the key generation and verification algorithms dramatically. The same approach was used in [12] to obtain an efficient Attribute Based Encryption (ABE) scheme.

Since a new random polynomial is chosen for each private key, the modified t-ABS is secure against collusion attacks. The $n + 1$ exponentiations needed to solve T in [16, 21] have been replaced with a single MapToPoint hash and signatures can contain a variable number of attributes, rather than be required to contain n as in [16, 21]. Verification can be optimized to reduce the number of bilinear map operations by bringing the Lagrange coefficients in [12]. This optimization reduces the number of bilinear map operations from $3d$ to $d + 2$ at the expense of increasing the number of exponentiations from d to $3d$, thus the overall speed of verification is improved. The details of this scheme is presented in Appendix A.

However, as it is noted in [2, 19], it is difficult to find groups $\mathbb{G}_2$ as the range of the MapToPoint hash function and to define an efficient isomorphism

$\psi : \mathbb{G}_2 \rightarrow \mathbb{G}_1$ at the same time. Thus, our new biometric IBS scheme uses the Sakai Kasahara Key Construction [14] for the generation of the private keys. This way, the problems stated above for the modified t-ABS are prevented and better performance is obtained due to the use of an ordinary hash function instead of MapToPoint hash function, which is called n times for the key generation and verification algorithms respectively. Besides, the total number of exponentiations and bilinear pairings required for the remaining phases are also reduced. Finally, the size of the public parameters and the signature is also much shorter compared to the fuzzy IBS scheme of [21, 16]. The details of the new scheme is presented as follows.

- **Setup**(1^{k_0}): Given a security parameter k_0, the parameters of the scheme are generated as below.

  1. Generate three cyclic groups $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{F}$ of prime order $p > 2^{k_0}$ and a bilinear pairing $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{F}$. Pick a random generator $g_1 \in \mathbb{G}_1$ and $g_2 \in \mathbb{G}_2$ such that $\psi(g_2) = g_1$.
  2. Pick random $x, y \in \mathbb{Z}_p^*$, compute $P_{pub} = g_2^x \in \mathbb{G}_2$ and $\kappa = \hat{e}(g_1, g_2)^y$.
  3. Pick two cryptographic hash functions $H_1 : \mathbb{Z}_p^* \rightarrow \mathbb{Z}_p^*$ and $H_2 : \{0,1\}^{k_1} \times \mathbb{F} \rightarrow \mathbb{Z}_p^*$.

  The message space is $M = \{0,1\}^{k_1}$. The master public key is $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{F}, \psi, \hat{e}, g_1, g_2, P_{pub}, \kappa, H_1, H_2)$ and the master secret key is $ms = x, y$.

- **Key Generation**: First, the set of biometric attributes $ID = \{\mu_1, ..., \mu_n\}$ of the signer are obtained from the raw biometric information as in [1, 13, 15]. Next, the PKG picks a random polynomial $q(\cdot)$ of degree $d-1$ over $\mathbb{Z}_p$ such that $q(0) = y$ and returns $D_i^{ID} = g_1^{\frac{q(\mu_i)}{t_i}}$ for each $\mu_i \in ID$. Here $t_i = x + H_1(\mu_i)$.

- **Sign**: Given a message $m \in M$ and D^{ID}, the following steps are performed.

  1. Pick a random $z \in \mathbb{Z}_p^*$ and compute $h = H_2(m, \kappa^z) = H_2(m, r)$
  2. $\sigma_i = (D_i^{ID})^{z+h}$ for each $\mu_i \in ID$.

  The signature on the message m for identity ID is $\sigma = (\Sigma, h)$, where $\Sigma = \{\sigma_i : \mu_i \in ID\}$.

- **Verify**: Given σ, m and ID', choose an arbitrary set $S \subseteq ID \cap ID'$ such that $|S| = d$ and check $h = H_2(m, r')$ by computing

$$
\begin{aligned}
r' &= \Big[\prod_{\mu_i \in S} \hat{e}(\sigma_i, P_{pub} \cdot g_2^{H_1(\mu_i)})^{\Delta_{\mu_i,S}(0)}) \Big] \kappa^{-h} \\
&= \Big[\prod_{\mu_i \in S} \hat{e}((D_i^{ID})^{z+h}, g_2^{t_i})^{\Delta_{\mu_i,S}(0)}) \Big] \kappa^{-h} \\
&= \Big[\prod_{\mu_i \in S} \hat{e}(g_1^{q(\mu_i)(z+h)}, g_2)^{\Delta_{\mu_i,S}(0)}) \Big] \kappa^{-h} \\
&= \hat{e}(g_1^{y(z+h)}, g_2) \kappa^{-h} \\
&= \kappa^z
\end{aligned}
$$

Here, the polynomial $q(\cdot)$ of degree $d-1$ is interpolated using d points by polynomial interpolation in the exponents using Shamir's secret sharing method [17].

Theorem 1. *Suppose the hash functions H_1, H_2 are random oracles and there exists an adaptively chosen message and given identity attacker A that produces a forgery by making q_1, q_2 random oracle queries, and q_s signature queries. Then there exists an algorithm B that solves the k-DHI problem.*

Proof. See appendix B.

4.1 Weak Signer-Attribute Privacy

In [16], the verifier is able to identify which d common attributes are used in the generation of the converted signature, since $ID' \setminus S$ components of the converted signature are publicly simulatable. If only weak signer-attribute privacy is considered, more efficient **Convert** and **CvtVerify** algorithms could be designed by removing the bilinear pairings and exponentiations computed for the *dummy* components, namely $ID' \setminus S$. For applications that require full signer-attribute privacy, the modified t-ABS scheme could be a suitable choice as it is much more efficient compared to t-ABS of [16].

- **Convert**: On input the public parameters of the fuzzy IBS, the message signature pair (m, σ), and the identity ID', the signer selects $S \subseteq ID \cap ID'$ such that $|S| = d$ and sets $\forall \mu_i \in S$, $\tilde{\sigma}_i = \sigma_i$. Next, $\forall \mu_i \in ID' \setminus S$, the signer sets $\tilde{\sigma}_i = \perp$ and returns the verifier $(m, \tilde{\sigma})$.
- **CvtVerify**: Given an identity ID', a message converted-signature pair $(m, \tilde{\sigma})$ and the public parameters, the verifier can easily identify the d common attributes and verifies the signature as before.

5 Efficiency Discussions and Comparison

In this section, we compare different fuzzy IBS and ABS schemes applicable for biometric identities. For simplicity of the comparison, ψ is taken as the identity

map (i.e. $\mathbb{G}_1 = \mathbb{G}_2 = \mathbb{G}$) and the computational cost for multiplication in $\mathbb{G}$ is omitted. All the computations are performed according to the optimization introduced in [12], where the dominant operations are considered as bilinear pairings followed by exponentiations. The abbreviations used in the following table denote the following: $|B|$ is the bit-length of an element in set (or group) B; n is the number of features in ID; T_e is the computation time for a single exponentiation in $\mathbb{G}$; T'_e is the computation time for a single exponentiation in $\mathbb{F}$; T_H is the computation time for a MapToPoint hash function; T_i is the computation time for a single inverse operation in $\mathbb{Z}_p$; T_p is the computation time for a single pairing operation; T'_i the computation time for a single inverse operation in $\mathbb{F}$; d is the error tolerance parameter; k_1 the size of the message; k_2 output size of the H_2 hash function.

Fig. 1. Comparison of error tolerant IBS schemes

	fuzzy IBS [21]	t-ABS [16]	Modified t-ABS	Our Scheme
Size of public parameters	$(n+k_1+4)\|\mathbb{G}\|+\|\mathbb{F}\|$	$(n+5)\|\mathbb{G}\|$	$4\|\mathbb{G}\|$	$2\|\mathbb{G}\|+\|\mathbb{F}\|$
Size of D^{ID}	$2n\|\mathbb{G}\|$	$2n\|\mathbb{G}\|$	$2n\|\mathbb{G}\|$	$n\|\mathbb{G}\|$
Size of σ	$3n\|\mathbb{G}\|$	$3n\|\mathbb{G}\|$	$3n\|\mathbb{G}\|$	$n\|\mathbb{G}\|+k_2$
Cost of Key Generation	$n(n+4)T_e$	$n(n+4)T_e$	$n(3T_e+T_H)$	$n(T_i+T_e)$
Cost of Sign	$(k_1+2n)T_e$	$2nT_e$	$2nT_e$	$nT_e+T'_e$
Cost of Verify	$d((n+4)T_e+T_p)$ $k_1T_e+2T_p$	$d((n+4)T_e+T_p)$ $2T_p+2T'_i$	$d(3T_e+T_p+T_H)$ $2T_p+2T'_i$	$d(T_p+T_e)$ $+T'_e$
Security Model	Standard Model	Standard Model	ROM	ROM

6 Conclusion

In this paper, we review the existing signature schemes applicable for biometric identities and propose a more efficient biometric IBS scheme by employing the Sakai Kasahara Key Construction. In addition, our scheme could function as a practical threshold ABS scheme with the claim that the new scheme is faster than all known pairing-based IBS methods for fuzzy identities similar to the claim in [2]. Considering the security of our scheme in the ROM, we achieve a better reduction cost compared to the reviewed signature schemes since the security penalty can be reduced to the maximum number of oracle queries the adversary can make. Besides, examining the full signer-attribute privacy for fuzzy IBS and our scheme could be an interesting future work since the user may use

his biometrics in other applications such as biometric encryption or authentication systems, where the latter assumes the privacy of the identity-biometrics relationship rather than the secrecy of the biometrics of the user. Finally, an open problem is to prove the security of our scheme in the standard model.

Acknowledgement

The author is grateful to her supervisor Prof. Dr. Joachim von zur Gathen for his valuable support, encouragement and guidance.

References

1. Joonsang Baek, Willy Susilo, and Jianying Zhou. New Constructions of Fuzzy Identity Based Encryption. In *ACM Symposium on Information, Computer and Communications Security - ASIACCS'07*, pages 368–370. ACM, 2007.
2. Paulo S. L. M. Barreto, Benoît Libert, Noel McCullagh, and Jean-Jacques Quisquater. Efficient and Provably-Secure Identity-Based Signatures and Signcryption from Bilinear Maps. In Bimal K. Roy, editor, *Advances in Cryptology - ASIACRYPT'05*, volume 3788 of *LNCS*, pages 515–532. Springer, 2005.
3. Mihir Bellare, Chanathip Namprempre, and Gregory Neven. Security Proofs for Identity Based Identification and Signature Schemes. In *Advances in Cryptology - EUROCRYPT'04*, volume 3027 of *LNCS*, pages 268–286. Springer, 2004.
4. Xavier Boyen, Yevgeniy Dodis, Jonathan Katz, Rafail Ostrovsky, and Adam Smith. Secure remote authentication using biometric data. In Ronald Cramer, editor, *Advances in Cryptology - EUROCRYPT'05*, volume 3494 of *LNCS*, pages 147–163. Springer, 2005.
5. Andrew Burnett, Fergus Byrne, Tom Dowling, and Adam Duffy. A Biometric Identity Based Signature Scheme. *International Journal of Network Security*, 5(3):317–326, 2007.
6. L. Chen, Z. Cheng, J. Malone-Lee, and N. Smart. Efficient ID-KEM based on the Sakai Kasahara Key Construction. *IEE Proceedings Information Security*, 153(1):19–26, 2006.
7. Liqun Chen and Zhaohui Cheng. Security Proof of Sakai Kasahara's Identity-Based Encryption Scheme. In *Cryptography and Coding, IMA Int. Conf.*, volume 3796 of *LNCS*, pages 442–459. Springer, 2005.
8. Yevgeniy Dodis, Leonid Reyzin, and Adam Smith. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. In *Advances in Cryptology - EUROCRYPT'04*, volume 3027 of *LNCS*, pages 523–540. Springer, 2004.
9. Jun Furukawa, Nuttapong Attrapadung, Ryuichi Sakai, and Goichiro Hanaoka. A Fuzzy ID-Based Encryption Efficient When Error Rate Is Low. In Dipanwita Roy Chowdhury, Vincent Rijmen, and Abhijit Das, editors, *Progress in Cryptology - INDOCRYPT'08*, volume 5365 of *LNCS*, pages 116–129. Springer, 2008.
10. Dalia Khader. Attribute Based Group Signatures. Cryptology ePrint Archive, Report 2007/159, 2007. http://eprint.iacr.org/.
11. Hemanta Maji, Manoj Prabhakaran, and Mike Rosulek. Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance. Cryptology ePrint Archive, Report 2008/328, 2008. http://eprint.iacr.org/.

12. Matthew Pirretti, Patrick Traynor, Patrick McDaniel, and Brent Waters. Secure Attribute Based Systems. In *ACM Conference on Computer and Communications Security*, pages 99–112. ACM, 2006.
13. Amit Sahai and Brent Waters. Fuzzy Identity Based Encryption. In *Advances in Cryptology - EUROCRYPT'05*, volume 3494 of *LNCS*, pages 457–473. Springer, 2005.
14. Ryuichi Sakai and Masao Kasahara. Id based cryptosystems with pairing on elliptic curve. Cryptology ePrint Archive, Report 2003/054, 2003. http://eprint.iacr.org/.
15. Neyire Deniz Sarier. A New Biometric Identity Based Encryption Scheme. In *The 2008 International Symposium on Trusted Computing - TrustCom 2008*, pages 2061–2066. IEEE Computer Society, 2008.
16. Siamak F Shahandashti and Reihaneh Safavi-Naini. Threshold Attribute-Based Signatures and Their Application to Anonymous Credential Systems. In Bart Preneel, editor, *Progress in Cryptology - AFRICACRYPT'09*, volume 5580 of *LNCS*, pages 198–216. Springer, 2009.
17. Adi Shamir. How to Share a Secret. *Commun. ACM*, 22(11):612–613, 1979.
18. Guo Shanqing and Zeng Yingpei. Attribute-based Signature Scheme. In *International Conference on Information Security and Assurance - ISA'08*. IEEE Computer Society, 2008.
19. Nigel P. Smart and Frederik Vercauteren. On computable isomorphisms in efficient asymmetric pairing-based systems. *Discrete Appl. Math.*, 155(4):538–547, 2007.
20. Brent Waters. Efficient Identity-Based Encryption Without Random Oracles. In Ronald Cramer, editor, *Advances in Cryptology - EUROCRYPT'05*, volume 3494 of *LNCS*, pages 114–127. Springer, 2005.
21. Piyi Yang, Zhenfu Cao, and Xiaolei Dong. Fuzzy Identity Based Signature. Cryptology ePrint Archive, Report 2008/002, 2008. http://eprint.iacr.org/.

Appendix A

The modified t-ABS scheme consists of the following phases.

- **Setup**(1^{k_0}): Given a security parameter k_0, the parameters of the scheme are generated as follows.
  1. Generate two cyclic groups $\mathbb{G}$ and $\mathbb{F}$ of prime order $p > 2^{k_0}$ and a bilinear pairing $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{F}$. Pick a random generator $g \in \mathbb{G}$.
  2. Pick randomly $y \in \mathbb{Z}_p^*$ and $h, g_2 \in \mathbb{G}$ and compute $g_1 = g^y$.

  The public parameters are (g, g_1, g_2, h) and the master secret key is y.
- **Key Generation**: Let $H : \{0,1\}^* \rightarrow \mathbb{Z}_p$ be a collision resistant hash function and let $T : \mathbb{Z}_p \rightarrow \mathbb{G}$ be a MapToPoint hash function modeled as a random oracle. Let Γ be the set defined as $\Gamma = \bigcup_{\mu \in ID} H(\mu)$. A new random degree $d-1$ polynomial $q(\cdot)$ over $\mathbb{Z}_p$ is selected such that $q(0) = y$ and $\forall i \in \Gamma$, a random r_i is chosen and $D_i^{ID} = (g^{q(\mu_i)} T(\mu_i)^{r_i}, g^{r_i})$ for each $\mu_i \in ID$
- **Sign**: Given a message $m \in M$ and D^{ID}, the following steps are performed.
  1. Pick a random $s_i \in \mathbb{Z}_p$ for $i \in [1, n]$
  2. Compute $\sigma_{1i} = g^{q(\mu_i)} T(\mu_i)^{r_i} (g_1^m \cdot h)^{s_i}$, $\sigma_{2i} = g^{r_i}$, $\sigma_{3i} = g^{s_i}$ for each $i \in [1, n]$.

The signature on the message m for identity ID is $\sigma = (\sigma_{1i}, \sigma_{2i}, \sigma_{3i})$ for $i \in [1, n]$.

– **Verify**: Given σ, m and ID', choose an arbitrary set $S \subseteq ID \cap ID'$ such that $|S| = d$ and check

$$\hat{e}(g_2, g_1) = \prod_{\mu_i \in S} \left(\frac{\hat{e}(\sigma_{1i}, g)}{\hat{e}(T(\mu_i), \sigma_{2i})\hat{e}(g_1^m \cdot h, \sigma_{3i})}\right)^{\Delta_{\mu_i, S}(0)}$$

The modifed t-ABS scheme satisfies both weak signer-attribute and full signer-attribute privacy if the additional protocols for signature conversion and interactive verification are applied. The reader is referred to [16] for the details of this application.

Appendix B: Proof of Theorem 1

Proof. Assume that a polynomial time attacker A produces a forgery, then using A, we show that one can construct an attacker B solving the k-DHI problem.

Suppose that B is given the k-DHI problem $(g_1, g_2, g_2^x, g_2^{x^2}, ..., g_2^{x^k})$, B will compute $g_1^{1/x}$ using A as follows.

– ***Phase 1***: A declares the challenge identity $ID^* = \{\mu_1, ...\mu_n\}$.

– ***Phase 2***: B picks a random feature $\mu^* \in ID^*$ and simulates the public parameters for A as follows.

1. B selects $h_0, ..., h_{k-1} \in \mathbb{Z}_p^*$ and sets $f(z) = \prod_{j=1}^{k-1}(z + h_j)$, which could be written as $f(z) = \sum_{j=0}^{k-1} c_j z^j$. The constant term c_0 is non-zero because $h_j \neq 0$ and c_j are computable from h_j. Here, h_0 denotes the hash value of the challenge attribute $\mu^* \in ID^*$, where μ^* is picked at random by B.

2. B computes $p_2 = \prod_{j=0}^{k-1}(g_2^{x^j})^{c_j} = g_2^{f(x)} \in \mathbb{G}_2$ and $p_1 = \psi(p_2) = g_1^{f(x)} \in \mathbb{G}_1$. Next, $p_2^x = g_2^{xf(x)} = \prod_{j=0}^{k-1}(g_2^{x^{j+1}})^{c_j}$ and $p_1^x = \psi(p_2^x)$. The public key is fixed as $P_{pub} \in \mathbb{G}_2 = p_2^{x-h_0}$. If $p_2 = 1$, then $x = -h_j$ for some j, then k-DHI problem could be solved directly [6].

3. B computes $f_j(z) = \frac{f(z)}{z+h_j} = \sum_{v=0}^{k-2} d_{j,v} z^v$ for $1 \leq j < k$ and $p_1^{1/(x+h_j)} = g_1^{f_j(x)} = \prod_{v=0}^{k-2} \psi((g_2^{x^v}))^{d_{j,v}}$.
4. Besides, we compute the following entity, which leads to a different proof compared to [6, 7, 2]. Namely, $p_1^{x/(x+h_j)} = g_1^{xf_j(x)} = \prod_{v=0}^{k-2} \psi((g_2^{x^{v+1}}))^{d_{j,v}}$. This way, the signature queries can be simulated for any identity chosen by A.

B picks a random $y \in \mathbb{Z}_p^*$ to compute $\kappa = \hat{e}(p_1, p_2)^y$ and returns A the public parameters $(p_1, p_2, \hat{e}, \psi, \mathbb{G}_1, \mathbb{G}_2, \mathbb{F}, \psi, P_{pub}, \kappa, H_1, H_2, d)$, where $d \in \mathbb{Z}^+$ and H_1, H_2 are random oracles controlled by B as follows.

H_1**-queries**: For a query on μ_i,

1. If $\mu_i \in ID^*$ and $\mu_i = \mu^*$,return h_0 and add $\langle \mu^*, h_0, \perp \rangle$ to H_1List.
2. Else return $h_i + h_0$, add the tuple $\langle \mu_i, h_i + h_0, p_1^{1/(x+h_i)} \rangle$ to H_1List.

Key extraction queries: Upon receiving a query for $|ID \cap ID^*| < d$, for every $\mu_i \neq \mu^* \in ID$, run the H_1-oracle simulator and obtain $\langle \mu_i, h_i + h_0, p_1^{1/(x+h_i)} \rangle$ from H_1List. Pick a random $d-1$ degree polynomial $q(\cdot)$ such that $q(0) = y$ and return $D_{\mu_i} = p_1^{q(\mu_i)/(x+h_i)}$ for each $\mu_i \in ID$.

Remark 2. The security model is stronger than the model of fuzzy IBS since the adversary has access to private key components of any ID including the case of $|ID \cap ID^*| \geq d$, as opposed to the security model of [21, 16]. In particular, a random $d-1$ degree polynomial $q(\cdot)$ such that $q(0) = y$ is picked for the first query on ID such that $|ID \cap ID^*| \geq d$, and A is given the private key components $D_{\mu_i} = p_1^{q(\mu_i)/(x+h_i)}$ except for the case when $\mu_i = \mu^*$. Further queries on any identity ID' such that $|ID' \cap ID^*| \geq d$ are answered using the same polynomial $q(\cdot)$ without affecting the previously computed shares by computing $D_{\mu_i'} = p_1^{q(\mu_i')/(x+H_1(\mu_i'))}$ for each $\mu_i' \in ID'$ due to the extensibility property of the Shamir's threshold secret sharing scheme. The only exception is for the component μ^*, since the simulator B does not know the corresponding private key $p_1^{q(\mu^*)/x}$.

Signature queries: For a query on a message-identity pair (m, ID),

1. If $|ID \cap ID^*| \geq d$ and $\mu^* \in ID$, B picks randomly $a, h \in \mathbb{Z}_p^*$, computes $r = \hat{e}(p_1^{ax} \cdot p_1^{-h}, p_2)^y = \hat{e}(p_1^{ax-h}, p_2)^y$ and backpatches to define the value $H_2(m, r)$ as h. Next, B obtains the corresponding private key components by simulating the key extraction oracle on ID and computes $\sigma_i = p_1^{axq(\mu_i)/(x+h_i)}$ for each $\mu_i \neq \mu^*$. For the feature $\mu_i = \mu^*$, he computes $\sigma_{\mu^*} = p_1^{aq(\mu^*)}$. Lastly, B returns $\sigma = (\Sigma, h)$ to A, where $\Sigma = (\sigma_i : \mu_i \in ID)$.
2. Else if $|ID \cap ID^*| < d$ and $\mu^* \in ID$, step 1 is repeated.
3. Else, B picks randomly $z, h \in \mathbb{Z}_p^*$, computes $r = \hat{e}(p_1^z, p_2)^y$ and backpatches to define $H_2(m, r)$ as h. Finally, B obtains the corresponding private key components by simulating the key extraction oracle and returns $(D_{\mu_i}^{ID})^{z+h}$ for each $\mu_i \in ID$.

B aborts in the unlikely event that $H_2(m, r)$ is already defined.

Remark 3. The simulation of the signature queries on any ID with $\mu^* \in ID$ is correct since given (σ, m), A chooses an arbitrary set $\mu^* \in S \subseteq ID$ such that $|S| = d$ and checks $h = H_2(m, r)$ by computing

$$
\begin{aligned}
r &= \big[\prod_{\mu_i \in S} \hat{e}(\sigma_i, P_{pub} \cdot p_2^{H_1(\mu_i)})^{\Delta_{\mu_i,S}(0)}) \big] \kappa^{-h} \\
&= \big[(\prod_{\mu^* \neq \mu_i \in S} \hat{e}(p_1^{axq(\mu_i)/(x+h_i)}, p_2^{x-h_0} \cdot p_2^{H_1(\mu_i)}) \cdot \hat{e}(\sigma_{\mu^*}, p_2^{x-h_0} \cdot p_2^{H_1(\mu^*)}))^{\Delta_{\mu_i,S}(0)}) \big] \kappa^{-h} \\
&= \big[(\prod_{\mu^* \neq \mu_i \in S} \hat{e}(p_1^{axq(\mu_i)/(x+h_i)}, p_2^{x-h_0} \cdot p_2^{h_i+h_0}) \cdot \hat{e}(\sigma_{\mu^*}, p_2^{x-h_0} \cdot p_2^{h_0}))^{\Delta_{\mu_i,S}(0)}) \big] \kappa^{-h} \\
&= \big[(\prod_{\mu^* \neq \mu_i \in S} \hat{e}(p_1^{axq(\mu_i)/(x+h_i)}, p_2^{x+h_i}) \cdot \hat{e}(p_1^{aq(\mu^*)}, p_2^{x}))^{\Delta_{\mu_i,S}(0)}) \big] \kappa^{-h} \\
&= \big[(\prod_{\mu^* \neq \mu_i \in S} \hat{e}(p_1^{axq(\mu_i)}, p_2) \cdot \hat{e}(p_1^{aq(\mu^*)}, p_2^{x}))^{\Delta_{\mu_i,S}(0)}) \big] \kappa^{-h} \\
&= \big[(\prod_{\mu_i \in S} \hat{e}(p_1^{axq(\mu_i)}, p_2))^{\Delta_{\mu_i,S}(0)}) \big] \kappa^{-h} \\
&= \hat{e}(p_1^{axy}, p_2) \hat{e}(p_1, p_2)^{-hy} \\
&= \hat{e}(p_1^{ax-h}, p_2)^{y}
\end{aligned}
$$

After the queries to the random oracles, the adversary has to forge a signature (m, r, σ) on the exact challenge identity $ID^* = (\mu_1, .., \mu^*, ..\mu_n)$. Next, the forking lemma is applied on (m, r, h, Σ). If the triples (r, h, Σ) can be simulated without knowing the private key components of ID^*, then there exists a Turing machine B' that replays a sufficient number of times on the input (P_{pub}, ID^*) to obtain two valid signatures (m^*, r, h', Σ') and (m^*, r, h'', Σ'') such that $h' \neq h''$ for the same message m^* and commitment r. If both forgeries satisfy the verification equation for all the sets $S \subseteq ID^*$ such that $|S| = d$ and $\mu^* \in S$, namely,

$$
\begin{aligned}
r &= \big[\prod_{\mu_i \in S} (\hat{e}(\sigma_i', P_{pub} \cdot p_2^{H_1(\mu_i)})^{\Delta_{\mu_i,S}(0)}) \big] \kappa^{-h'} \\
&= \big[\prod_{\mu_i \in S} (\hat{e}(\sigma_i'', P_{pub} \cdot p_2^{H_1(\mu_i)})^{\Delta_{\mu_i,S}(0)}) \big] \kappa^{-h''}
\end{aligned}
$$

By verifying all the possible combinations for the set S, B is assured that each partial signature σ_i' and σ_i'' is valid. Since each private key component of $\mu_i \neq \mu^* \in ID^*$ is known by B (also by A), the solution to the k-DHI problem could only be obtained from the forgeries associated to $\mu^* \in ID^*$, namely $\sigma_{\mu^*}', \sigma_{\mu^*}''$.

Then, the computations are performed as in [2],

$$
\begin{aligned}
&\hat{e}(\sigma_{\mu^*}', P_{pub} \cdot p_2^{H_1(\mu^*)}) \hat{e}(p_1, p_2)^{-h'} = \hat{e}(\sigma_{\mu^*}'', P_{pub} \cdot p_2^{H_1(\mu^*)}) \hat{e}(p_1, p_2)^{-h''} \\
&\Rightarrow \hat{e}(\sigma_{\mu^*}', p_2^x) \hat{e}(p_1, p_2)^{-h'} = \hat{e}(\sigma_{\mu^*}'', p_2^x) \hat{e}(p_1, p_2)^{-h''} \\
&\Rightarrow \hat{e}(\sigma_{\mu^*}'/\sigma_{\mu^*}'', p_2^x)^{(h'-h'')^{-1}} = \hat{e}(p_1, p_2)
\end{aligned}
$$

Similar to the proof in [2], we set $T = p_1^{q(\mu^*)/x} = (\sigma'_{\mu^*}/\sigma''_{\mu^*})^{(h'-h'')^{-1}}$.

The solution to the k-DHI problem, $g_1^{1/x}$ is obtained by outputting $(T^{1/q(\mu^*)}/\prod_{j=1}^{k-1}\psi(g_2^{x^{j-1}})^{c_j})^{1/c_0}$ since

$$T^{1/q(\mu^*)} = p_1^{1/x} = \psi(p_2)^{1/x} = \prod_{j=0}^{k-1}(\psi(g_2^{x^{j-1}}))^{c_j} = \psi(g_2)^{c_0/x} \cdot \prod_{j=1}^{k-1}\psi(g_2^{x^{j-1}})^{c_j}$$

.

Remark 4. Since A already knows the private keys for each feature of the challenge identity ID^* except for the feature $\mu^* \in ID^*$, A only has to forge the partial signature σ_{μ^*} corresponding to μ^* of ID^*.