A New Approach for Biometric Template Storage and Remote Authentication

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 propose a new remote biometric based authentication scheme, which is designed for distributed systems with a central database for the storage of the biometric data. For our scheme, we consider the recently introduced security notions of Identity and Transaction privacy and present a different storage mechanism for biometrics resulting in a reduced database storage cost. Besides, the components of the system do not need to store any biometric template in cleartext or in encrypted form, which affects the social acceptance of the system positively. Finally, we compare our results with existing schemes satisfying the current security notions and achieve improved computational complexity.

Keywords: Remote authentication, Biometric template security, Identity privacy, Distributed systems.

1 Introduction

Biometric-based identification provides unforgeable authentication without requiring the user to store any secret identification data or remember long passwords. Biometric information is unique, unforgettable, non-transferable and it could be easily integrated with password-based and/or token-based authentication techniques. As each authentication technique has its weaknesses, a multi-factor authentication scheme with the correct design and security model results in a reliable system.

Currently, the secrecy of biometric data is viewed with skepticism since it is very easy to obtain biological information such as fingerprint, iris or face data through fingerprint marking or using a camcorder. However, biometrics is a sensitive information, thus it should not be easy to obtain the biometric data by compromising the server, where the biometrics of each user is often associated with his personal information. This also affects the social accpetence of the biometric systems especially when biometric data are stored in a central database which can be vulnerable to internal or external attackers.

Biometric authentication could be categorized broadly as remote server or client end authentication, where in the first case, the remote server stores the

M. Tistarelli and M.S. Nixon (Eds.): ICB 2009, LNCS 5558, pp. 909–918, 2009.

reference biometric data and performs the matching. In a typical biometric based remote authentication scheme, the user registers his identity information and biometrics to the server end that stores this information either in cleartext or in encrypted form. When the user wants to authenticate himself, the user provides a fresh biometric, which is compared to the previously stored biometric information after decryption or in the encryption domain by exploiting the homomorphic properties of the underlying encryption scheme.

The security and privacy protection of remote biometric-based authentication systems is enhanced by implementing distributed biometric systems, where the goal is to detach the biometric data storage from the service provider and to guarantee the notions of user privacy and database privacy, which have been recently introduced as a new security model for biometric authentication. Current systems implementing this approach provide provable security in this new model, but they are not suitable for weak computational devices such as smart cards and RFID's, since the user has to encrypt at each authentication request his fresh biometric information using public key encryption. Moreover, the employment of homomorphic encryption schemes and Private Information Retrieval (PIR) systems results in high communication and computational costs. Consequently, one has to design a secure and efficient remote biometric authentication scheme for a distributed system, where the service provider, the database and the client end with a smart card collaborate during the authentication process.

1.1 Related Work

Remote biometric-based authentication systems could be classified based on the employment of cryptographic encryption schemes or lightweight computational primitives. The systems described in [1,2,3,4,5] combine homomorphic encryption techniques with biometrics in a distributed environment. Specifically, the user U registers its biometric template in cleartext or in encrypted form at the database DB. Besides, U registers his personal information and the index of the database storage location of his biometrics at the service provider SP. To authenticate himself, U encrypts his biometrics using a homomorphic encryption scheme and sends this to SP, which retrieves the index of U to be used in a PIR protocol between SP and DB. In [1,5], an independent verification unit is additionally required for the matching operation and the final decision. In [1], the biometric template is stored as a plaintext and a user sends the encryption of each singe bit using Goldwasser-Micali scheme resulting in a high transmission and computation cost. Also, the relationship between the user's identity and his biometrics is kept private by employing a PIR with the communication cost linear in the size N of the database. Besides, protocols using Paillier Public Key System are described in [5,6], where the authors of [5] present an attack against the scheme of [1] that reveals the user's biometric data to SP. Furthermore, the scheme of [1] is improved in terms of communication cost by combining a PIR, a secure sketch and a homomorphic encryption scheme [3,4,2].

For the second case that consider biometric data as a secret information, a biometric authentication system for weak computational devices is presented [7], which requires the use of a fixed permutation stored by the server and the client. Additionally, a number of secret values are stored in the client's smart card, whose loss results in the compromise of the biometric template by evasedropping on the communication channel [1]. Moreover, in [8] efficient biometric authentication schemes for mobile devices are presented, where as opposed to [7], a reference biometric template should be stored on the mobile device. Similarly, other systems are designed using error-correction procedures [9,10,11,12,13,14,15,16]. In [17], the author describes a brute force attack that extracts both the secret and the biometric template from the fuzzy vault [15] with $O(10^{17})$ binary operations and thus he suggests the use of strong cryptographic techniques for a secure biometric authentication.

Finally, a combination of the two approaches is presented in [18], where a multi-factor biometric authentication system is described using a public key pair that is generated by combining a secret key and a biometric based key. The system requires the selection of a representative template that is fixed to one pattern and a Public Key Infrasturacture (PKI) for the public key certificates. However, the template should be stored in the user's smart card and a correct matching on card will activate the keys to be used in the authentication.

1.2 Motivation and Contributions

The privacy protection and the secure storage of the biometric templates are the main concerns for the biometric-based authentication schemes. As it is noted in [4], privacy protection not only means the attackers inability to compromise the biometric template but also the protection of the sensitive relationship between the identity and the biometric information of the user. To achieve this property, we separate the storage of personal identity information from the storage of biometrics using the distributed structure of [3,4,2], which is composed of the user U_i, the sensor client SC, the service provider SP and the database DB. Here, SC, SP and DB are independent of each other and the latter two are assumed to be malicious whereas the sensor client is always honest. This way, SP cannot obtain the biometrics of the user and can have business agreements with different parties that make the sensor client available to users at different locations. Also, DB could function as a trusted storage for different SP's.

Since SC captures the biometric data and performs the feature extraction, this component could be installed as a Trusted Biometric Reader as in [19]. Alternatively, a special smartcard biometric reader [7] could be used to capture biometrics and perform the necessary computations for session key generation and AES, which would provide the highest security for the user since no transfer of biometric data will take place between the user's smart card and SC. However, as it is noted in [20], the computational cost for feature extraction is very high compared to AES and Elliptic Curve Digital Signature (ECDS) computation on a smart card. Thus, we only require a smart card that implements AES and an efficient Identity based encryption (IBE) system such as the Boneh/Franklin scheme [21] to perform a short session key generation using the stored private key. This way, the session keys could be constructed in an anonymous, authenticated and efficient way. Specifically, an IBE scheme is called as anonymous if the ciphertext does not reveal the identity of the recipient [22]. Besides, the users should not store any biometric data in their smart cards as relying only on tamper proofness is not a wise assumption [7]. Even if the smart card is lost or stolen, the compromise of the secret values and keys should not reveal the biometrics since the revocation of these values is possible as opposed to biometric data. Finally, we aim to design an efficient system that minimizes the costs of storage, encryption and communication. For this purpose, we propose a different approach for the storage of the biometrics in the database and describe a new remote biometric-based authentication system.

2 Preliminaries and Definitions

Our system consists of four independent entities: A human user U_i with identity ID_i, the sensor client SC with ID_{SC}, the service provider SP with ID_{SP} and the database SB with ID_{DB}. Similar to existing authentication schemes, our system is composed of two phases: the registration and the verification phase, which have the following workflow.

1. In the registration phase, the human user U_i presents its biometrics to SC, which captures the raw biometric data and extracts the feature vector $B_i = (\mu_1, ..., \mu_n)$. Next, U_i registers each feature at a randomly selected storage location in DB and registers his personalized username ID_i at SP. Here, the size of the database is denoted as N and the dimension of the feature vector is denoted as n.
2. In the verification phase, the user U_i presents its biometrics to SC, which computes the feature set B'_i. Using cryptographic techniques, SP communicates with U_i and DB and decides based on a distance metric and a predefined threshold to accept or to reject U_i. In our scheme, we will consider set overlap as the distance metric [23,24], where the value d represents the error tolerance in terms of minimal set overlap.

2.1 Assumptions on the System

- Liveliness Assumption: This is an indispensable assumption 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_i, SC, SP and DB should be encrypted using standard protocols. Specifically, the session key generation should be performed in an anonymous and authenticated way.
- Collusion Assumption: Due to the distributed system structure, we assume that DB and SP are malicious but they do not collude. Additionally, the sensor client is always honest.

2.2 Security Requirements

Identity Privacy: Informally, this notion guarantees the privacy of the sensitive relationship between the user identity and its biometrics against a malicious service provider or a malicious database even in case of multiple registrations of the same user with different personalized usernames. Briefly, it means that the service provider or the database (or an attacker that has compromised one of them) cannot recover the biometric template of the user [4].

Transaction Privacy: Informally, transaction anonymity means that a malicious database cannot learn anything about the personal identity of the user for any authentication request made to the service provider.

The formal definitions of the security notions could be found in [2,4,1,3].

3 A New Biometric Authentication Scheme

In this section, we present a new remote biometric-based authentication scheme using a different approach for storing the biometric features resulting in a secure and more efficient protocol compared to the existing protocols. For this purpose, we use Boneh/Franklin IBE [21] scheme to encrypt a random session key for AES and an efficient PIR protocol [25] which allows SP to retrieve an item from the DB without revealing which item SP is retrieving. Due to page limitations, the reader is referred to [21,27,25] for a detailed discussion of IBE and PIR.

3.1 Registration Phase

The registration phase consists of the following initialization of the components.

1. The four components of the system, namely, U_i, SC, SP and DB are initialized by the Private Key Generator (PKG) of the IBE system with the private keys $d_i, d_{SC}, d_{SP}, d_{DB}$, respectively.
2. The user U_i presents its biometrics to the sensor client which extracts the feature set $B_i = (\mu_1, ..., \mu_n)$ of the user. Here, each of the features of arbitrary length can be hashed using some collision-resistant hash function [24] or mapped to an element of a finite field [23].
3. The user picks some random indexes $i_k \in Z$ where $1 \leq k \leq n$ and registers each feature at the locations i_k of the database.

   Remark 1. If the location of the database is already occupied by another feature, then the user selects another random index for the feature. Also, if some of the features of the user are already stored in the database, then the database returns the indexes of the common features. Thus, common features are not stored more than once, which decreases the total storage cost of the database.

4. The user U_i registers its personalized username at the service provider and stores the index list $Index_i = (i_1, ..., i_n)$ in his smart card.

3.2 Verification Phase

The verification phase has the following workflow.

1. U_i inserts his smart card into the terminal of SC and presents its biometrics. SC performs feature extraction to compute the feature set B'_i. U_i and SC agree on a session key using Boneh-Franklin IBE [21] scheme and SC encrypts the feature set using AES. To provide non-malleability, SC also signs the hash of the feature set B'_i using an efficient identity based signature scheme based on bilinear pairings [26]. Finally, SC communicates with the smart card of U_i by sending the $E(B'_i) = Enc_{AES}(B'_i)||Sign(H(B'_i))$, where H is a cryptographic hash function.
2. U_i decrypts the first part of $E(B'_i)$ using the session key to obtain the feature set $B'_i = (\mu'_1, ..., \mu'_n)$ and verifies the signature.
3. U_i makes an authentication request to SP and both entities agree on a short session key using IBE. U_i sends the encryption of the index list as $E_k = Enc_{AES}(i_k)||H(Enc_{AES}(i_k), H(i_k))$ for $1 \leq k \leq n$.
4. SP decrypts each E_k and obtains the $Index_i$ of U_i.
5. For $1 \leq t \leq N$, DB randomly selects r_t and computes $E^1_t = r_t \oplus \mu_t$ and $E^2_t = H(r_t \oplus \mu_t, H(r_t))$.
6. SP runs a PIR protocol [25] to obtain each masked feature and the corresponding hash value of $Index_i$ from the database. Next, SP stores the hash values in the set S_1 to be used later in the matching stage.
7. For $1 \leq l \leq n$, SP computes $E_l = Enc_{AES}(M_l, Sign(H(M_l)) = Enc_{AES}(r_l \oplus \mu_l), Sign(H(r_l \oplus \mu_l))$ and sends each E_l to U_i.
8. For $1 \leq l \leq n$, U_i decrypts each E_l using the session key and computes $r'_l = M_l \oplus \mu'_l$. Lastly, U_i sends each $R_l = Enc_{AES}(H(r'_l))$ to SP.
9. SP decrypts each R_l and computes $H(M_l, H(r'_l))) = H(r_l \oplus \mu_l, H(r_l \oplus \mu_l \oplus \mu'_l))$, which are then stored in the set S_2. Finally, using the threshold d, SP checks $|S_1 \cap S_2| \geq d$. If this condition is satisfied, then the user is authenticated, otherwise rejected.

4 Analysis of the Protocol

In the first part, we evaluate the major security criteria that should be satisfied in a biometric authentication system

- Identity-biometric template relation: At the registration phase, a user selects a random number for each feature of his biometrics and each feature is stored as a separate entry using the randomly selected index. Hence, even if the database is compromised, the attacker would not be able to find an index that points to a biometric template stored as cleartext or encrypted. This also provides security against the database since it only stores a randomly ordered pool of features from different users, where each feature is hashed using a specific cryptographic hash function before it is stored in the database. Besides, when the same user registers at the service provider using different personalized (pseudorandom) usernames, than the service provider is not even aware of this situation since it does not store any index number corresponding to the database storage location as opposed to [2,4,5,1].

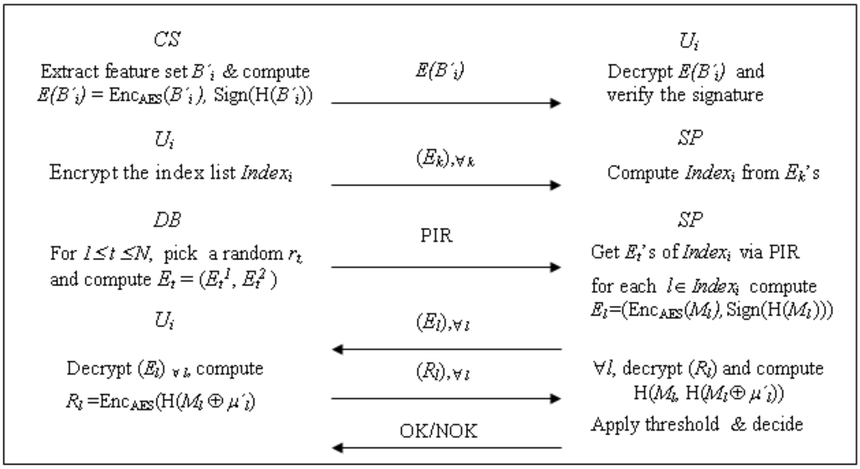
CS
Extract feature set B'_i & compute
$E(B'_i)$ = Enc$_{AES}$(B'_i), Sign(H(B'_i))
$E(B'_i)$
U_i
Decrypt $E(B'_i)$ and
verify the signature
U_i
Encrypt the index list $Index_i$
$(E_k),\forall k$
SP
Compute $Index_i$ from E_k's
DB
For $1 \le t \le N$, pick a random r_t
and compute $E_t = (E_t^1, E_t^2)$
PIR
SP
Get E_t's of $Index_i$ via PIR
for each $l \in Index_i$ compute
E_l=(Enc$_{AES}$(M_l), Sign(H(M_l)))
U_i
$(E_l),\forall l$
Decrypt (E_l) $\forall l$, compute
R_l =Enc$_{AES}$(H($M_l \oplus \mu'_i$))
$(R_l),\forall l$
$\forall l$, decrypt (R_l) and compute
H(M_l, H($M_l \oplus \mu'_i$))
Apply threshold & decide
OK/NOK

Fig. 1. Verification phase of the new Protocol

- No single point of failure: In order to impersonate a user, the attacker needs to obtain both the biometrics and the smart card that stores the private key and the index list of the user.
- Loss of the secret does not compromise the template: The user has to store only a private key and some index numbers in the smart card instead of storing his biometric template and the compromise of these values do not reveal the biometric information in any step of the authentication. When the user's smart card is lost or stolen, then the user can obtain a new secret key from PKG and the index list by reregistering to the database. However, most of the user's features are already stored in DB, so DB only returns the corresponding index list after the user presents his feature vector.
- No replay attack possible: At each authentication request, the database xores each feature in the database with a new random number and sends these values to the service provider. Also, the service provider and the user agrees on a different session key for each application and the authentication requires the collaboration of each party. So, it is not possible to send replayed data.
- No need for PKI: Our scheme uses an efficient Anonymous Identity Based Encryption (IBE) scheme such as Boneh/Franklin IBE [21] for the generation of a short session key, hence, an eavesdropper (or a malicious database) on the communication channel cannot discover the identity of the user since the ciphertext does not reveal anything about the identity of the recipient (and the sender for authenticated Boneh/Franklin scheme [27]) of the ciphertext [22]. This is a vital point in the privacy of the user identity in a biometric authentication system, however, in many schemes, this property is not considered. Also, our design does not require a PKI and public key certificates as in [18].
- Encryption of the channel: The communication channel between the components of the system is encrypted, hence eavesdropping on the channel is prevented.

In addition, our new design has the following advantages in terms of computation and storage costs.

– Efficient memory storage: Since each feature is stored as a separate entry in the database, there could be common features belonging to different users. Thus, during registration phase, the database could check for this situation and could return the index of the previously stored feature. This way, the size of the registered feature set and the total storage in the database could be smaller. Besides, since no biometric template is stored as an entry, there is no need to apply a public key encryption scheme such as ElGamal to store the biometric data as encrypted, where the ciphertext size is twice the plaintext size as in [4,2]. Finally, the choice of the system parameters of [3,1] result in a constraint on the size of the database, whereas our design is also suitable for a large scale central database that stores biometric data.
– Lower computational cost: In [3,1], the database performs $O(N)$ exponentiations modulo q^2 [3] and modulo q [1], where q is an RSA modulus with $|q|$=2048 bits. Similarly, the schemes of [4,2] require $O(N)$ exponentiations in group G, on which the ElGamal public key scheme is defined. The computational cost of our scheme is dominated by the $O(N)$ random number selections and $O(N)$ hash computations in order to encrypt each feature stored in the database using one time pad. Except for the session key generations, we use symmetric key encryption and lightweight cryptographic primitives, hence, our scheme is suitable for energy constrained devices. In the following table, we summarize various remote biometric-based authentication schemes that satisfy the security model described in section 2.

Table 1. Comparison of various biometric authentication systems

Scheme	Communication Cost	Computation Cost	Storage Cost*
System 1 [1]	$O(N)$	M exponentiations + $(MN)/2$ multiplications	M bits
System 2 [3]	$O(\log^2(N))$	$O(N)$ exponentiations	128 Kbytes
System 3 [4]	$O(k+2M)$	$O(N)$ exponentiations	$2M$ bits
System 4 [2]	$O(k+2M)$	$O(N)$ exponentiations	$2M$ bits
Our System	$O(n(k+\|\mu\|))$	$O(N)$ random number selections + $O(N)$ Hash computations	$\|\mu\|$

*At each entry of the database
Abbreviations: N=total number of entries in the database; n=dimension of the feature vector of a user; M= size of the biometric template; $|\mu|$=size of a feature; $k \geq \log(N)$

5 Conclusion

In this paper, we presented a new design for a remote biometric based authentication protocol, where the entities of the system are independent of each other. The system follows the state-of-the-art security model for biometric authentication systems with an improved computational complexity. Besides, a different storage mechanism for the biometric data is introduced, which could be of independent interest for the biometrics and information security community. In addition to the increased efficiency in the database storage, this approach also affects the social acceptance of biometric systems operating with central databases positively since the compromise of the database (namely, a random pool of features) would not help any attacker in the recovery of a user's template, which could otherwise only be guaranteed by storing the biometrics as encrypted. Finally, an open problem is to decrease the communication cost of the distributed biometric authentication systems, which is caused by the use of PIR systems.

Acknowledgement

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

References

1. 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)
2. 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)
3. 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)
4. 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)
5. 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)
6. Schoenmakers, B., Tuyls, P.: Efficient binary conversion for paillier encrypted values. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 522–537. Springer, Heidelberg (2006)
7. Atallah, M.J., Frikken, K.B., Goodrich, M.T., Tamassia, R.: Secure biometric authentication for weak computational devices. In: Patrick, A.S., Yung, M. (eds.) FC 2005. LNCS, vol. 3570, pp. 357–371. Springer, Heidelberg (2005)
8. Yoon, E.J., Yoo, K.Y.: A secure chaotic hash-based biometric remote user authentication scheme using mobile devices. In: Chang, K.C.-C., Wang, W., Chen, L., Ellis, C.A., Hsu, C.-H., Tsoi, A.C., Wang, H. (eds.) APWeb/WAIM 2007. LNCS, vol. 4537, pp. 612–623. Springer, Heidelberg (2007)
9. Boyen, X., Dodis, Y., Katz, J., Ostrovsky, R., Smith, A.: Secure remote authentication using biometric data. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 147–163. Springer, Heidelberg (2005)

10. Crescenzo, G.D., Graveman, R.F., Ge, R., Arce, G.R.: Approximate message authentication and biometric entity authentication. In: Patrick, A.S., Yung, M. (eds.) FC 2005. LNCS, vol. 3570, pp. 240–254. Springer, Heidelberg (2005)
11. Dodis, Y., Reyzin, L., Smith, A.: Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 523–540. Springer, Heidelberg (2004)
12. Juels, A., Sudan, M.: A fuzzy vault scheme. Des. Codes Cryptography 38(2), 237–257 (2006)
13. Juels, A., Wattenberg, M.: A fuzzy commitment scheme. In: ACM Conference on Computer and Communications Security, pp. 28–36. ACM, New York (1999)
14. Tuyls, P., Goseling, J.: Capacity and examples of template-protecting biometric authentication systems. In: Maltoni, D., Jain, A.K. (eds.) BioAW 2004. LNCS, vol. 3087, pp. 158–170. Springer, Heidelberg (2004)
15. Uludag, U., Pankanti, S., Jain, A.K.: Fuzzy vault for fingerprints. In: Kanade, T., Jain, A., Ratha, N.K. (eds.) AVBPA 2005. LNCS, vol. 3546, pp. 310–319. Springer, Heidelberg (2005)
16. Uludag, U., Jain, A.: Securing fingerprint template: Fuzzy vault with helper data. In: Computer Vision and Pattern Recognition Workshop. IEEE Computer Society, Los Alamitos (2006)
17. Mihailescu, P.: The fuzzy vault for fingerprints is vulnerable to brute force attack. CoRR abs/0708.2974 (2007)
18. Itakura, Y., Tsujii, S.: Proposal on a multifactor biometric authentication method based on cryptosystem keys containing biometric signatures. Int. J. Inf. Sec. 4(4), 288–296 (2005)
19. Salaiwarakul, A., Ryan, M.D.: Verification of integrity and secrecy properties of a biometric authentication protocol. In: Chen, L., Mu, Y., Susilo, W. (eds.) ISPEC 2008. LNCS, vol. 4991, pp. 1–13. Springer, Heidelberg (2008)
20. Park, B., Moon, D., Chung, Y., Park, J.W.: Impact of embedding scenarios on the smart card-based fingerprint verification. In: Lee, J.K., Yi, O., Yung, M. (eds.) WISA 2006. LNCS, vol. 4298, pp. 110–120. Springer, Heidelberg (2007)
21. Boneh, D., Franklin, M.K.: Identity-based encryption from the weil pairing. SIAM J. Comput. 32(3), 586–615 (2003)
22. Boneh, D., Gentry, C., Hamburg, M.: Space-efficient identity based encryptionwithout pairings. In: FOCS 2007: Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science, pp. 647–657. IEEE Computer Society, Los Alamitos (2007)
23. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005)
24. Baek, J., Susilo, W., Zhou, J.: New constructions of fuzzy identity-based encryption. In: ASIACCS 2007, pp. 368–370. ACM, New York (2007)
25. Gentry, C., Ramzan, Z.: Single-database private information retrieval with constant communication rate. In: Caires, L., Italiano, G.F., Monteiro, L., Palamidessi, C., Yung, M. (eds.) ICALP 2005. LNCS, vol. 3580, pp. 803–815. Springer, Heidelberg (2005)
26. Bellare, M., Namprempre, C., Neven, G.: Security proofs for identity-based identification and signature schemes. In: Cachin, C., Camenisch, J. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 268–286. Springer, Heidelberg (2004)
27. Pan, J., Cai, L., Shen, X.: Promoting Identity-Based Key Management in Wireless Ad Hoc Networks. In: Xiao, Y., Shen, X., Du, D. (eds.) Wireless/Mobile Network Security - Signals and Communication Technology, pp. 83–102. Springer, Heidelberg (2007)