Applied Mathematics & Information Sciences
An International Journal

@ 2012 NSP
Natural Sciences Publishing Cor.

A Novel Biometric Signcryption Scheme that Is Identity-based and Group-oriented

Mingwen Wang[1,2] and Dongming Tang[1]
[1]*Information Research Institute, Southwest Jiaotong University, Chengdu 610031, P.R. China*
[2]*Information Center, Dongfang Boiler Group Co. Ltd, Zigong 643000, P.R. China*
Email: wangmw@home.swjtu.edu.cn

Received: 11 Mar. 2012; Revised 25 Jul. 2012; Accepted 06 Aug. 2012

Abstract: The signcryption scheme plays an important role in the applications which need privacy and authentication simultaneously. In order to get high efficiency in one-to-many communication environment and simplify the management of keys, a novel biometric signcryption scheme, identity-based and group-oriented, is proposed in this paper. In the scheme, the sender signcrypts the message and broadcasts it, but only the members of the receiver group can unsigncrypt the cipher text correctly. The implement of the scheme does not need bilinear pairing computation and modular exponentiation computation, hence it is very efficient. The analysis results show that the scheme is secure.

Keywords: Cryptography, signcryption, biometric, group-oriented.

1 Introduction

Privacy is a fundamental goal in network communication and usually achieved by encryption schemes. In point-to-point communication, one encrypts the message and sends it to the other one by one, however this model is not fit for the one-to-many communication applications because of its low efficiency especially for a large receiver group. In order to solve above problem in one-to-many communication environment, Fiat and Naor proposed broadcast encryption scheme [1], in which the message can be encrypted once by the sender and be decrypted only by the authenticated receiver.

Authentication is another fundamental goal in network communication environment. The traditional approach to ensure privacy and authentication simultaneously is signature-then-encryption. It has lower efficiency than signcryption scheme [2] which fulfils both the functions of digital signature and encryption simultaneously.

In order to reduce the system complexity and the cost for establishing and managing the public key in pubic key infrastructure, Shamir [3] proposed the concept of identity based cryptography in which users identifier information such as email or IP addresses instead of digital certificates can be used as public key for encryption or signature verification. The first identity-based encryption scheme was proposed by Boneh and Franklin [4] in 2001 and the first fuzzy identity based encryption scheme was proposed by Sahai and Waters [5] in 2005.

Identity-based group-oriented signcryption scheme is important in the network applications which need to maintain privacy and authentication of the message simultaneously in one-to-many communication environment. The first Identity-based group-oriented signcryption scheme was proposed by Duan et al [6] in 2007, however it has a low efficiency. To overcome the problem, some more efficient schemes were proposed later [7, 8].

We note that the combination of biometric identity and cryptography is a hot research area in recent years. Some biometric based signcryption schemes have been proposed, such as a biometric identify-based signcryption scheme proposed by Li et al [9] and a biometric signcryption scheme proposed by Zhang et al [10]. However, to the best of our knowledge there has not a biometric identity-based group-oriented signcryption scheme. Moreover, most of the previous identity-based signcryption scheme need bilinear pairing computations, so the efficiency of the schemes was relatively low. Initiated by Liu et al's signcryption scheme without bilinear pairing [11], we proposed a biometric identity-based group-oriented signcryption scheme in this paper. The scheme is efficient and can provide privacy and authentication at the same time.

2 Preliminaries

2.1 Fuzzy Extractor Method

Cryptography traditionally relies on uniformly distributed and precisely reproducible random strings for its secrets. Since the biometric data, such as fingerprint, is not precisely the same each time it is measured, it is hard to generate keys directly by biometric data. Dodis et al proposed a scheme [12] to illustrate how to turn biometric information to cryptographic keys. In their scheme, a primitive termed fuzzy extractor is proposed to extract a uniformly random string U from biometric information b in a noise-tolerant way.[13] Suppose the input biometric data be b', if b' is close enough to b, the string U can be reproduced exactly. To assist in reproducing U from b', the fuzzy extractor outputs a nonsecret string V. It is important to note that U remains secret even if given V. Three metrics was used in the construction of fuzzy extractor:

1. Hamming Distance: the number of symbol positions that differ between b and b'.

2. Set Difference: size of the symmetric difference of two input sets between b and b'.

3. Edit Distance: the number of insertions and deletions needed to convert b' into b.

Hamming Distance is the main metric and the other two are auxiliary.

The definition of fuzzy extractor is as follow:

Let M be a matrix with finite dimensions and a distance function is defined as: $M \times M \to Z^*$. Let the length of output string U be l and the minimum noise-tolerant distance be t. An $(M, m, l, t, \varepsilon)$-fuzzy extractor is a pair of randomized procedures, Gen and Rep with the following properties:

1. The generation procedure Gen on input $b \in M$ outputs an extracted string $U \in \{0,1\}^l$ and a helper string $V \in \{0,1\}^*$.

2. The reproduction procedure Rep takes an element $b' \in M$ and a bit string $V \in \{0,1\}^*$ as inputs. The correctness property of fuzzy extractors guarantees that if $dis(b,b') \le t$ and U, V were generated by $(U,V) \leftarrow Gen(b)$, then $Rep(b',V) = U$. If $dis(b,b') > t$, then no guarantee is provided about the output of Rep.

3. The security property guarantees that for any distribution b on M of min-entropy m, the string U is nearly uniform even for those who observe.

By the fuzzy extractor, one can extract some randomness U from b and then successfully reproduce U from any string b' that is close to b. The reproduction uses the helper string V produced during the initial extraction; yet V need not remain secret, because U looks truly random even given V.

2.2 Formal Model of Biometric Identity-based Group-oriented Signcryption

Refer to the model of identity-based group-oriented signcryption proposed in [8], we define the formal model of biometric identity-based group-oriented signcryption scheme as follows. A generic biometric identity-based group-oriented signcryption scheme consists of the following four algorithms.

1. Setup: is a probabilistic polynomial-time (PPT) algorithm run by a PKG that takes as input 1^k and outputs a master secret key msk and public parameters $params$. Here k is a security parameter.

2. Extract: is a key generation algorithm run by a PKG that takes as input the master secret key msk, the receiver group identity G_{ID} and the biometric data b_i of group member u_i, and outputs the corresponding private key S_{ID_i}. Here identity ID_i is computed from b_i.

3. Signcrypt: is a PPT algorithm that takes as input a plaintext message m, the public parameters $params$, the receiver group identity G_{ID}, the sender's biometric data b_s and private key S_{ID_s}, and outputs a cipher text

$$\sigma \leftarrow Signcrypt(m, G_{ID}, b_s, S_{ID_s})$$

The sender broadcasts the cipher text to the receiver group through the public channel.

4. Unsigncrypt: is a deterministic algorithm that takes as input a cipher text σ, the public parameters $params$, the receiver's private key S_{ID_r}, and outputs the original message m or the symbol $\perp$ if σ is an invalid cipher text.

There exists the consistency constraint that for the member belongs to the receiver group, if

$$\sigma \leftarrow Signcrypt(m, G_{ID}, b_s, S_{ID_s})$$

then

$$m = Unsigncrypt(\sigma, S_{ID_r}, G_{ID}) .$$

3 The Proposed Scheme

3.1 Setup

Given a security parameter k, two big prime numbers p and q are generated, where $q \mid p-1$. The PKG chooses a cyclic group G on ellipse curve and a generator P with order q. The PKG selects secure hash functions: $H_1 : \{0,1\}^* \times G \to Z_q^*$, $H_2 : \{0,1\}^* \to Z_q^*$, $H_3 : G \to \{0,1\}^*$. The PKG chooses a master secret key $z \in Z_q^*$ randomly and computes $y = zP$. The PKG publishes $(p, q, P, y, H_1, H_2, H_3)$ and keeps the master secret key z secret.

3.2 Extract

On obtaining the user's biometric data b_i, the PKG computes $Gen(b_i) \to (U_i, v_i)$ and lets U_i be the user's identity ID_i. The PKG chooses randomly $c_i \in Z_q^*$ and computes $r_i = c_i H_2(ID_i)$, $R_i = r_i P$, $D_i = r_i + zH_1(G_{ID}, y)$. The PKG sends D_i to user ID_i as his/her private key over a secure channel. The corresponding public key is R_i.

The user ID_i can verify his/her private key by the equation $R_i + H_1(G_{ID}, y)y = D_i P$.

3.3 Signcrypt

The user A input his/her biometric information $b_A^{'}$ to reproduce U_A by $Rep(b_A^{'}, v_A) \to U_A$, where v_A is the public helper information. U_A is the user A's identity ID_A.

For the message m, the user A chooses $a \in Z_q^*$ randomly and computes $T_A = aP$, $h_1 = H_1(G_{ID}, y)$, $h = H_2(T_A \| ID_A \| m)$, $s = a/(D_A + h)$, $V_A = ah_1 yP$, $C = H_3(V_A) \oplus (m)$. In the end, the user A computes the cipher text $\sigma = (h, s, C)$ and sends it to the receiver group G_{ID}.

3.4 Unsigncrypt

Without loss of generality, we assume the member's identity binding to the receiver group G_{ID} is $ID_{B_i} (i = 1, \cdots, n)$, where n is the number of members of the group.

For accepted cipher text σ, the group member B_i reproduce ID_A by $Rep(b_A^{'}, v_A) \to U_A$ and computes:

$$h_1^{'} = H_1(G_{ID}, y)$$

$$V_B = s(D_B P - R_B)(R_A + h_1^{'} y + hP),$$

unsigncrypt the message by $m = C \oplus H_3(V_B)$.

If the equation $H_2(s(R_A + h_1^{'} y + hP) \| ID_A \| m) = h$ holds, the user B_i accepts the message m.

The correctness of the signature can be verified by the third party. Received (h, s, m) and the user A's biometric data $b_A^{'}$, the third party firstly reproduces ID_A by $Rep(b_A^{'}, v_A) \to U_A$, then checks

$$H_2(s(R_A + h_1^{'} y + hP) \| ID_A \| m) \overset{?}{=} h$$

If it holds, we can conclude that the message was signed by the user A.

4 Security and Complexity

4.1 Security Analysis

According to the discussion above, we know the signcryption message is broadcasted to the receiver group by the sender and can only be unsigncrypted by the members in the receiver group. In the following we will discuss the security of the scheme in three aspects and prove that possible attacks cannot break the scheme.

Theorem 1 Correctness. If all the members follow the protocol, the correct signcryption message σ can surely be generated. In another word, the equality $m = C \oplus H_3(V_B)$ and $H_2(s(R_A + h_1^{'} y + hP) \| ID_A \| m) = h$ holds.

Proof. The correctness of the scheme consists of two parts, one is the authentication of the signature, the other is the correctness of the message.

Firstly, we have

$$\begin{aligned} s(R_A + h_1^{'}y + hP) &= (a/(D_A + h))(r_A P + h_1^{'}zP + hP) \\ &= (a/(D_A + h))(D_A + h)P \\ &= aP \\ &= T_A \end{aligned}$$

So that $H_2(s(R_A + h_1^{'}y + hP) \| ID_A \| m) = h$ holds.

Secondly, the correctness of the message can be concluded as follows:

$$\begin{aligned} m &= H_3(V_B) \oplus C \\ &= H_3(s(D_B P - R_B)(R_A + h_1^{'}y + hP) \oplus C \\ &= H_3(aP(D_B P - R_B)) \oplus C \\ &= H_3(aP(r_B P + zH_1(G_{ID}, y)P - R_B)) \oplus C \\ &= H_3(aPzH_1(G_{ID}, y)P) \oplus C \\ &= H_3(ayh_1 P) \oplus C \\ &= H_3(V_A) \oplus H_3(V_A) \oplus (m) \\ &= m \end{aligned}$$

Theorem 2 Confidentiality. Only the members in the receiver group can decrypt the cipher text σ and recover the original message m.

Proof. In theorem 1, we have proved that a group member can surely recover the original message m, here we try to prove any person outside the group can not recover the message m.

Assume a PPT adversary ADV, he wants to decrypt cipher text σ and recover the original message m. All the information for ADV is the system public parameters $(p, q, P, y, H_1, H_2, H_3)$, the member's public key R_i, and the cipher text $\sigma = (h, s, C)$. In order to recover m, the possible way is to solve the equations $h = H_2(T_A \| ID_A \| m)$ and $C = H_3(V_A) \oplus (m)$. Suppose H_2 is a strong-collision one-way function, m can not be solved from the equation $h = H_2(T_A \| ID_A \| m)$. Hence, the adversary ADV need to work out V_A. Note that $V_A = ah_1 yP$, where $a \in Z_q^*$ is a random value and is secret to the adversary, so that V_A can not be worked out by ADV. On the other hand, the authenticated receiver B calculate V_A by $V_B = s(D_B P - R_B)(R_A + h_1^{'}y + hP)$ and $m = C \oplus H_3(V_B)$. Because D_B is the private key of the user B and $D_B = r_B + zH_1(G_{ID}, y) = c_B H_2(ID_B) + zH_1(G_{ID}, y)$, where c_B (r_B) is secret value to ADV over Z_q^*, it is hard for the adversary to work out V_B.

In summary, none except the member of the receiver group can decrypt the cipher text.

Theorem 3 Unforgeability. For the message m, the probability for a PPT adversary to output a cipher text $\sigma^* = (h^*, s^*, C^*)$ which can be accepted by the group member is negligible small.

Proof. The receiver accepts the cipher text only if the equation $H_2(s^*(R_A + h_1^{'}y + hP) \| ID_A \| m) = h$ holds. In another word, the equation $s^*(R_A + h_1^{'}y + hP) = T_A^*$ must hold.

Because we have

$$\begin{aligned} s^*(R_A + h_1^{'}y + hP) &= (a/(D_A^* + h))(r_A P + h_1^{'}y + hP) \\ &= (a/(D_A^* + h))(D_A + h)P \quad , \\ &= aP(D_A + h)/(D_A^* + h) \end{aligned}$$

and $D_A \in Z_q^*$, the probability satisfying the equation $s^*(R_A + h_1^{'}y + hP) = aP$ is no more than n/q for a receiver group with n members. For $n << q$, that is to say, it is hard for a PPT adversary to forge a signcryption message.

4.2 Complexity Analysis

Let P, P_E, P_M and P_C denote the elapse time of one bilinear paring, one modular exponentiation, one modular multiplication and one modular inverse respectively. Suppose the number of the members of the receiver group be n, let $|x|$ denote the length of the integer x. We analysis the complexity of the scheme from three aspects: the length of the signcryption message, computational complexity in the signcryption phase and unsigncryption phase respectively.

We compare our proposed scheme with the previous identity-based group-oriented signcryption scheme in the paper [6], [7] and [8].

Table.1. Complexity Contrast Results

scheme	Complexity Analysis		
	Length of cipher text	*Computation time in signcryption*	*Computation time in unsigncryption*
scheme [6]	$(n+2)\|G\| + \|m\| + \|ID\|$	$P + (n+4)P_E + (n+2)P_M$	$4P + P_C + P_M$
scheme [7]	$(n+2)\|G\| + \|G_T\| + \|m\|$	$P + (n+4)P_M$	$3P + P_C + 3P_M$
scheme [8]	$2\|G\| + 2\|G_T\| + \|Z_p^*\|$	$2P + 5P_M + 3P_E + P_C$	$2P + 7P_M + 4P_E$

scheme	Complexity Analysis		
	Length of cipher text	*Computation time in signcryption*	*Computation time in unsigncryption*
our scheme	$2\lvert G\rvert+\lvert m\rvert$	$5P_M+P_C$	$5P_M$

From table 1 we can get:

1. The length of cipher text of our proposed scheme is independent with the number of the members in the receiver group comparing to the schemes in [6] and [7]. Compared with the scheme in [8], the length of cipher text of our scheme is linear to the length of the message m, hence it is very fit for the short message applications. Contrast results show the length of cipher text of our scheme is relatively short comparing to the previous schemes.

2. The computation time in signcryption phase in our scheme is independent with the number of the members in the receiver group comparing to the schemes in [6] and [7]. Moreover, because the heavily time-consuming bilinear paring computation is not need in our scheme, our scheme is more efficient than the schemes [6–8] in signcryption phase.

3. Because the bilinear pairing computation is not need in our scheme and the computation time of P_M is nearly 20 times of the computation time of P, the computation time in unsigncryption phase in our scheme is more efficient than the schemes [6–8].

From above we can conclude that our scheme is more efficient than the previous schemes.

5 Conclusion

Identity-based and group-oriented signcryption scheme is important in the network applications which need to maintain privacy and authentication of the message simultaneously in one-to-many communication environment. A biometric identity-based and group-oriented signcryption scheme is proposed in this paper. The signcrypted message can be generated by a group identity and be broadcasted. Only the members in the receiver group can unsigncrypt the signcrypted message. The correctness, confidentiality and unforgeability of the scheme have been proved. Unlike most of the previous identity-based and group-oriented signcryption schemes, it does not need bilinear pairing computation and modular exponentiation computation, and the complex analysis results show that the proposed scheme is more efficient than most of the previous schemes.

Acknowledgements

This work was supported in part by National Science Foundation for Post-doctoral Scientists of China under Grant No. 20110491736, the National Natural Science Foundation of China under Grant No. 61100118, the Fundamental Research Funds for the Central Universities under No. SWJTU11BR090. The work was also partially funded by Dongfang Boiler Group Corporation. The author is grateful to the anonymous referee for a careful checking of the details and for helpful comments that improved this paper.

References

[1] A. Fiat and M. Naor. Broadcast encryption, Advances in cryptology-CRYPTO 1993. Lecture Notes in Computer Science 773, Berlin, Springer-Verlag, 480–491(1994).

[2] Y. Zheng, Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption), Advances in Cryptology, CRYPTO'97, Lecture Notes in Computer Science 1294, Springer-Verlag, 165–179(1997).

[3] A. Shamir, Identity-based Cryptosystems and Signature Schemes, Proceedings of CRYPTO'84, Lecture Notes in Computer Science 196, Springer-Verlag, 47–53(1984).

[4] D. Boneh and M. Franklin, Identity-Based Encryption from the Weil Pairing, Proceedings of CRYPTO 2001, Lecture Notes in Computer Science 2139, Springer-Verlag, 213–229 (2001).

[5] A. Sahai and B. Waters, Fuzzy identity-based encryption, in: Advances in Cryptology, EUROCRYPT 2005, in: Lecture Notes in Computer Science 3494, Springer-Verlag, 457–473(2005).

[6] S. Duan and Z. Cao. Efficient and provably secure multi-receiver identity-based signcryption. ACISP 2006[C]. Lecture Notes in Computer Science 4058, Berlin, Springer-Verlag, 195–206(2006).

[7] Y. Yu, B. Yang and X. Huang et al. Efficient identity-based signcryption scheme for multiple receivers. ATC 2007. Lecture Notes in Computer Science 4610, Berlin, Springer-Verlag, 13–21(2007

[8] B. Zhang and Q. Xu. Identity-based group-oriented signcryption scheme, Journal on Communications,

30(11A) , 23–28(2009).

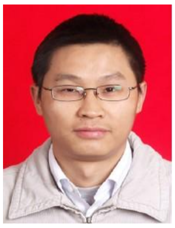
[9] F. Li and M. Khan, A biometric identity-based signcryption scheme, Future Generation Computer Systems, 2010.11.004, 1–5(2010).

[10] M.W. Zhang, B. Yang and T. Takagi, et al. Fuzzy biometric signcryption scheme with bilinear pairings in the standard model. PAISI 2010, Lecture Notes in Computer Science 6122, 77–87 (2010).

[11] W.H. Liu, C.X. Xu. Certificateless signcryption scheme without bilinear pairing. Journal of Software, 22(8), 1918–1926 (2011).

[12] Y. Dodis, L. Reyzin and A. Smith, Fuzzy extractors: how to generate strong keys from biometrics and other noisy data, in: Advances in Cryptology, EUROCRYPT 2004, in: Lecture Notes in Computer Science 3027, Springer-Verlag, 523–540 (2004).

Mingwen Wang received his B.S. degree from Zhejiang University, Hangzhou, PR China in 1994, M.S. degree and Ph.D. degree from University of Electronic Science and Technology of China, Chengdu, PR China in 2003 and 2007 respectively. he was a postdoctoral fellow in Southwest Jiaotong University, Chengdu, China From 2010. He is now an assistant research fellow in Information Research Institute of Southwest Jiaotong University, Chengdu, PR China. His recent research interests include cryptography and network security. He has published more than 20 papers in the international journals and conferences.



Dongming Tang received his M.S. degree from Guizhou University, Guiyang, PR China in 2006, Ph.D. degree from University of Electronic Science and Technology of China, Chengdu, PR China in 2010. He is now an assistant research fellow in Information Research Institute of Southwest Jiaotong University, Chengdu, PR China. His research interests include algorithms, big data processing, bioinformatics.