International Journal of Foundations of Computer Science
Vol. 20, No. 2 (2009) 351–359
© World Scientific Publishing Company

World Scientific
www.worldscientific.com

A NEW CONVERTIBLE AUTHENTICATED ENCRYPTION SCHEME BASED ON THE ELGAMAL CRYPTOSYSTEM

CHENG-CHI LEE
Department of Information & Communication Engineering, Asia University
No. 500, Lioufeng Raod, Wufeng Shiang, Taichung, Taiwan, R.O.C.
cclee@asia.edu.tw

MIN-SHIANG HWANG
Department of Management Information System
National Chung Hsing University
250 Kuo Kuang Road, 402 Taichung, Taiwan, R.O.C.
Correspondence: mshwang@nchu.edu.tw

SHIANG-FENG TZENG
Department of Information Management
Chaoyang University of Technology
168 Gifeng E. Rd., Wufeng, Taichung County, Taiwan 413, R.O.C.
ShiangFeng@ms67.url.com.tw

Received 27 August 2008
Accepted 18 December 2008
Communicated by Arto Salomaa

A convertible authenticated encryption scheme allows a designated receiver to retrieve an authenticated ciphertext and convert the authenticated ciphertext into an ordinary signature. The receiver can prove the dishonesty of the sender to anyone if the sender repudiates his/her signature. Recently, many researchers have proposed convertible authenticated encryption schemes based on cryptological algorithms. In this paper, the authors shall present a new convertible authenticated encryption scheme based on the ElGamal cryptosystem. The proposed scheme is more efficient than Wu-Hsu's scheme in terms of computational complexity.

Keywords: Authenticated encryption scheme; cryptography; digital signature; discrete logarithms; ElGamal cryptosystem.

1991 Mathematics Subject Classification: 22E46, 53C35, 57S20

1. Introduction

In 1993, Nyberg and Rueppel [12, 13] were the first to propose a digital signature scheme with message recovery based on discrete logarithms. To reduce the communication cost of Nyberg and Rueppel's schemes, Horster et al. [5] proposed an authenticated encryption scheme, and there have actually been quite a lot of efficient authenticated encryption schemes [1, 4, 7, 8, 9, 10, 14, 19] presented since then. In their schemes, the signer could produce a signature for a message and then send it to a specified receiver. After receiving the signature, only the receiver could recover and verify the message.

Consider the condition of a later dispute; e.g., the signer denies having signed a signature. It could be required to reveal the message along with its signature for verifying. To protect the receiver's welfare in case of a later dispute, we should further enable the receiver to convert the signature into its ordinary form that can be verified by anyone.

In 1999, Araki et al. [1] presented a convertible limited verifier signature scheme. However, the conversion of the signature demands the signer to release one more parameter. It could be infeasible if the signer is unwilling to cooperate. Recently, Wu and Hsu [18] presented a convertible authenticated encryption scheme. In the scheme, when the signer repudiates the signature, the receiver can prove the dishonesty of the signer by revealing an ordinary signature that can be verified by anyone without the cooperation of the signer. Lv et al. [11] proposed a practical convertible authenticated encryption scheme using self-certified public keys. They showed that Wu and Hsu's scheme cannot provide the semantic security of the message. An attacker can get the actual message even if the message is encrypted. The computational load of Lv et al.'s scheme is the same as the Wu and Hsu's scheme. Chien [2] proposed a convertible authenticated encryption scheme without using conventional one-way function. However, Zhang et al. [20] showed that Chien's scheme have forgeability and repudiation. Tzeng et al. [16] proposed a new convertible authenticated encryption scheme with message linkages. Not only can the scheme deliver a large message but the scheme is also to convert the signature into an ordinary one. Wu et al. [17] proposed a convertible multi-authenticated encryption scheme. It allows the signature is cooperatively produced by a group of signers instead of a single signer. It is suitable for multiparty environments.

In this paper, we shall present a new convertible authenticated encryption scheme based on the ElGamal cryptosystem. The proposed scheme is more efficient than Wu-Hsu's scheme in terms of computational complexity. In the next section, related works will be given. Then, in Section 3, our proposed scheme will be released. The security and performance analysis of the proposed scheme will be discussed in Section 4. Finally, the conclusion will be given in Section 5.

2. Related Works

2.1. *The Wu-Hsu scheme*

There are three phases in Wu and Hsu's scheme: the signature generation phase, the message recovery phase, and the conversion phase [18]. Initially, the system parameters are defined as follows. Let p be a large prime, q be a large prime factor of $p - 1$, g be a generator with order q in $GF(p)$, and let $h(\cdot)$ be a one-way hash function. Each user U_i owns a private key $x_i \in Z_q^*$ and calculates the corresponding public key $y_i = g^{x_i} \bmod p$. Let U_A be the signer and U_B be the receiver. The scheme as illustrated in Figure 1, works as follows.

Signature Generation Phase:
Assume that U_A wants to deliver a message M to U_B. U_A fulfills the following process to create the signature. U_A first selects an integer $k \in Z_q^*$ and calculates

$$\begin{cases} r_1 = M(h(y_B^k \bmod p))^{-1} \bmod p, \\ r_2 = h(M, h(g^k \bmod p)) \bmod q, \\ s \ \ = k - x_A r_2 \bmod q. \end{cases}$$

U_A sends the signature $(r_1,\, r_2,\, s)$ to U_B.

Message Recovery Phase:
After receiving the signature $(r_1,\, r_2,\, s)$, U_B can recover the message

$$M = h((g^s y_A^{r_2})^{x_B} \bmod p) r_1 \bmod p,$$

and verify the signature

$$r_2 =?\ h(M, h(g^s y_A^{r_2} \bmod p)) \bmod q. \tag{1}$$

If the result is positive, the signature is valid.

Conversion Phase:
If U_A repudiates the signature, U_B can confirm the dishonesty of the signer by revealing the converted signature $(r_2,\, s)$ for the message M. With this converted signature, anyone can confirm its validity by checking it against Equation (1).

U_A		U_B
chooses an integer $k \in Z_q^*$		
$r_1 = M(h(y_B^k \bmod p))^{-1} \bmod p$		
$r_2 = h(M, h(g^k \bmod p)) \bmod q$		
$s = k - x_A r_2 \bmod q$		
	$\xrightarrow{(r_1, r_2, s)}$	
		$M = h((g^s y_A^{r_2})^{x_B} \bmod p) r_1 \bmod p$
		$r_2 = h(M, h(g^s y_A^{r_2} \bmod p)) \bmod q$

Fig. 1. The Wu-Hsu scheme.

2.2. *ElGamal cryptosystem*

The parameters of ElGamal cryptosystem [3, 6, 15] are composed by public information p, g, a public key y and a secret key x, where p is a large prime, g is generated from $\mathrm{GF}(p)$, x is a random number less than p, and y is computed by $y = g^x \bmod p$.

Assume that Alice wants to send the ciphertext (r, c) to Bob. The sender, Alice, need to encrypt the plaintext M using Bob's public key y. First, Alice generates a random number, k, less than p. Next, Alice computes r and c as follows.

$$\begin{aligned} r &= g^k \bmod p, \\ c &= My^k \bmod p. \end{aligned}$$

Whenever Bob receives (r, c) from Alice, he can decrypt the plaintext M using his secure key x as follows.

$$\begin{aligned} M &= c(r^x)^{-1} \bmod p, \\ &= My^k(r^x)^{-1} \bmod p, \\ &= Mg^{xk}(r^x)^{-1} \bmod p, \\ &= Mg^{xk}(g^{xk})^{-1} \bmod p, \\ &= Mg^{xk}(g^{-xk}) \bmod p, \\ &= M \bmod p. \end{aligned}$$

3. Our Proposed Scheme

In this section, we shall propose a new convertible authenticated encryption scheme based on the ElGamal cryptosystem [3, 6, 15]. The proposed scheme is also composed of three phases: the signature generation phase, the message recovery phase, and the conversion phase. The system initialization is the same as that of the scheme reviewed in the preceding Section 2.1, and the details of the phases will be given in the following paragraphs and illustrated in Figure 2.

Signature Generation Phase:

Without loss of generality, assume that U_A wants to generate a signature for a message M and send it to U_B. The signature generating procedure is as follows. U_A chooses a random integer $k \in Z_q^*$. Then, U_A computes the signature (c, r, s) for message M where

$$\begin{aligned} r &= g^k \bmod p, && (2) \\ c &= M(y_B^{(k+x_A)})^{-1} \bmod p, && (3) \\ s &= k + x_A h(M, r) \bmod q. && (4) \end{aligned}$$

Finally, U_A delivers the signature (c, r, s) to U_B.

Message Recovery Phase:
After receiving the signature (c, r, s), U_B can recover the message M by using her/his private key x_B as follows:

$$M = c(ry_A)^{x_B} \bmod p. \tag{5}$$

The recovered message M must be verified by checking the validity of the following equality:

$$g^s = ry_A^{h(M,r)} \bmod p. \tag{6}$$

If the equation holds, the signature is valid.

Conversion Phase:
This phase is similar to that in the preceding section. U_B can display the converted signature (r, s) for the message M. With this converted signature, anyone can confirm its validity by checking Equation (6).

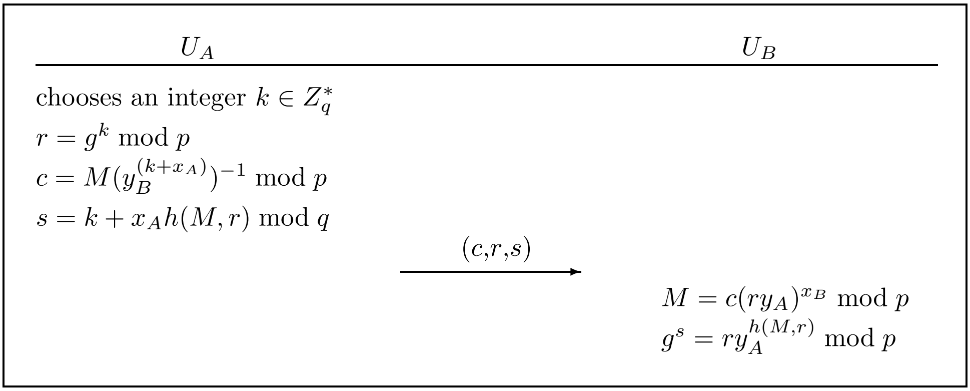
U_A
U_B
chooses an integer $k \in Z_q^*$
$r = g^k \bmod p$
$c = M(y_B^{(k+x_A)})^{-1} \bmod p$
$s = k + x_A h(M,r) \bmod q$
$\xrightarrow{(c,r,s)}$
$M = c(ry_A)^{x_B} \bmod p$
$g^s = ry_A^{h(M,r)} \bmod p$

Fig. 2. The proposed scheme.

In the following, we shall prove that the proposed scheme can work correctly. In the message recovery phase, the receiver U_B can recover the message by following Equation (5). According to Equation (5), we have

$$\begin{aligned}
&c(ry_A)^{x_B} \\
&= M(y_B^{(k+x_A)})^{-1}(ry_A)^{x_B}) \\
&= M(g^{(x_B k + x_A x_B)})^{-1} g^{(x_B k + x_A x_B)} \\
&= M.
\end{aligned}$$

4. Security and Performance Analysis

First, to demonstrate the security of our scheme, we shall analyze some possible ways in which an opponent may attempt to attack it. We shall prove that the proposed scheme can successfully withstand those possible attacks.

Attack 1: An opponent attempts to derive the user's private key x_i from all the public information available.

Analysis of attack 1: Assume that the opponent wants to derive U_A's private key x_A from the corresponding public key $y_A = g^{x_A} \bmod p$. It is as difficult as to break discrete logarithms [3, 6, 15] to obtain U_A's private key x_A. From the signature, it seems difficult to the opponent to derive U_A's private key x_A through Equation (4), since the equation has two unknown variables k and x_A, and k is also under the protection of discrete logarithms.

Attack 2: An opponent attempts to forge some message of an authenticated encryption signature.

Analysis of attack 2: To construct a signature to satisfy Equation (5), the opponent should know the common key y_{AB} $(= y_A^{x_B} = y_B^{x_A})$ between U_A and U_B in the first place. As with Attack 1, she/he will have to face the difficult problem.

Attack 3: An opponent tries to forge a converted signature to pass Equation (6).

Analysis of attack 3: From Equation (6), given s, it is difficult to determine r because of the difficulty of solving the one-way hash function and the discrete logarithms. Similarly, given r, it is also infeasible to determine s such that Equation (6) holds.

Attack 4: An opponent attempts to recover the message M from the authenticated encryption signature.

Analysis of attack 4: From Equation (5), the message M can be recovered by one who has the private key x_A or x_B. Similar to Attack 1, it is as difficult as to break discrete logarithms to obtain the user's private key.

Attack 5: An opponent tries to verify the signature before converting.

Analysis of attack 5: To perform the signature verification in Equation (6), the opponent needs the message M. Similar to Attack 4, she/he cannot obtain or recover the message M. Therefore, she/he cannot verify the signature.

Attack 6: An opponent gets a valid (c, r, s), he/she tries to check whether his/her guessed message M^* satisfies Equation (3) and Equation (4) [11].

Analysis of attack 6: To perform the guessed message in Equation (3) and Equation (4), the opponent must know the k and x_A. However, these values are private and secure. Therefore, the opponent cannot use this attack to obtain the message.

Then, let's see how our proposed scheme and Wu and Hsu's scheme compare in terms of communication cost and computational complexity. The performance evaluation notations are defined as follows:

Table 1. The Comparison between the Wu-Hsu scheme and the proposed Scheme.

	The Wu-Hsu Scheme	The Proposed Scheme
Length of original signature	$\|p\| + 2\|q\|$	$2\|p\| + \|q\|$
Length of converted signature	$2\|q\|$	$\|p\| + \|q\|$
Computation cost for signature generation	$2T_{exp} + 2T_m + T_{inv} + 3T_h$	$2T_{exp} + 2T_m + T_{inv} + T_h$
Computation cost for message recovery	$3T_{exp} + 2T_m + 3T_h$	$3T_{exp} + 3T_m + T_h$
Computation cost for verifying converted signature	$2T_{exp} + T_m + 2T_h$	$2T_{exp} + T_m + T_h$

- T_{exp}: the time for a modular exponential computation
- T_m: the time for a modular multiplication computation
- T_{inv}: the time for a modular inverse computation
- T_h: the time for a one way hash function $f(\cdot)$ computation
- $|x|$: the bit-length of an integer x.

We ignore the computation times of modular addition operations and modular subtraction operations. The comparison results are given in Table 1. The transmitted size of a signature (r_1, r_2, s) is $|p| + 2|q|$ in Wu-Hsu's scheme, while the size of a signature (c, r, s) is $2|p| + |q|$ in the proposed scheme. Through the conversion phase, the length of a converted signature (r_2, s) is $2|q|$ in the Wu-Hsu scheme, while the length of a converted signature (r, s) is $|p| + |q|$ in our proposed scheme.

In the signature generation phase of the proposed scheme, the computational complexity that the signer requires is T_{exp} for Equation (2), $T_{exp} + T_m + T_{inv}$ for Equation (3) and $T_m + T_h$ for Equation (4). Then, the total computational complexity of the signature generation phase adds up to be $2T_{exp} + 2T_m + T_{inv} + T_h$. However, the Wu-Hsu scheme requires $2T_{exp} + 2T_m + T_{inv} + 3T_h$. It is obvious that the proposed scheme is more efficient than the Wu-Hsu scheme in this phase.

In the message recovery phase of the proposed scheme, the computational complexity required includes $T_{exp} + 2T_m$ for Equation (5) and $2T_{exp} + T_m + T_h$ for Equation (6). The total computational complexity of the message recovery phase is $3T_{exp} + 3T_m + T_h$. However, the total computational complexity the Wu-Hsu scheme requires in the same phase is $3T_{exp} + 2T_m + 3T_h$.

Anyone in the proposed scheme requires $2T_{exp} + T_m + T_h$ in the conversion phase. However, the computational complexity of the Wu-Hsu scheme in the same phase is $2T_{exp} + T_m + 2T_h$. It is obvious that the proposed scheme is more efficient than the Wu-Hsu scheme in this phase. Through the comparison, we conclude that the proposed scheme outperforms Wu and Hsu's scheme in computational complexities of the signature generation phase and the conversion phase.

5. Conclusion

In this article, we have proposed a new convertible authenticated encryption scheme based on the ElGamal cryptosystem. The concepts of data encryption and digital signature are integrated. Furthermore, for avoiding the abuse of the signature, the proposed scheme supports the ability to convert the signature into an ordinary form that can be verified by anyone. Besides, the conversion does not require the cooperation of the signer, and the proposed scheme provides perfect protection for the receiver. Some possible attacks have been considered, and none of them can successfully break the proposed scheme. Furthermore, we have also demonstrated that the computational complexity of the signature generation and the checking converted signature of the proposed scheme are more desirable than that of Wu and Hsu's scheme.

Acknowledgments

This work was supported in part by the Taiwan Information Security Center (TWISC) and the National Science Council under the grants NSC95-2218-E-001-001, NSC95- 2218-E-011-015 and NSC97-2218-E-468-010.

References

[1] Shunsuke Araki, Satoshi Uehara, and Kyoki Imamura, "The limited verifier signature and its application," *IEICE Transactions on Fundamentals*, vol. E82-A, no. 1, pp. 63–68, 1999.

[2] H. Y. Chien, "Convertible authenticated encryption scheme without using conventional one-way function," *Informatica*, vol. 14, no. 4, pp. 1–9, 2003.

[3] T. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. IT-31, pp. 469–472, July 1985.

[4] L. Hernandez Encinas, A. Martin del Rey, and J. Munoz Masque, "A weakness in authenticated encryption schemes based on Tseng et al.'s schemes ," *International Journal of Network Security*, vol. 2, no. 2, pp. 157–159, 2008.

[5] P. Horster, M. Michels, and H. Petersen, "Authenticated encryption schemes with low communication costs," *Electronics Letters*, vol. 30, no. 15, p. 1212, 1994.

[6] Min-Shiang Hwang, Chin-Chen Chang, and Kuo-Feng Hwang, "An ElGamal-like cryptosystem for enciphering large messages," *IEEE Transactions on Knowledge and Data Engineering*, vol. 14, no. 2, pp. 445–446, 2002.

[7] Min-Shiang Hwang and Chi-Yu Liu, "Authenticated encryption schemes: current status and key issues ," *International Journal of Network Security*, vol. 1, no. 2, pp. 61–73, 2005.

[8] Shin-Jia Hwang, Chin-Chen Chang, and Wei-Pang Yang, "Authenticated encryption schemes with message lingage," *Information Processing Letters*, vol. 58, no. 4, pp. 189–194, 1996.

[9] Wei-Bin Lee and Chin-Chen Chang, "Authenticated encryption schemes without using a one way function," *Electronics Letters*, vol. 31, no. 19, pp. 1656–1657, 1995.

[10] Wei-Bin Lee and Chin-Chen Chang, "Authenticated encryption schemes with linkage between message blocks," *Information Processing Letters*, vol. 63, no. 5, pp. 247–250, 1997.

[11] J. Lv, X. Wang, and K. Kim, "Practical convertible authenticated encryption schemes using self-certified public keys," *Applied Mathematics and Computation*, vol. 169, no. 2, pp. 1285–1297, 2005.

[12] K. Nyberg and R. A. Rueppel, "A new signature scheme based on the DSA giving message recovery," in *1st ACM Conference on Computer and Communications Security*, pp. 58–61, Fairfax, Virginia, Nov. 1993.

[13] K. Nyberg and R. A. Rueppel, "Message recovery for signature schemes based on the discrete logarithm," in *Advances in Cryptology, EUROCRYPT'94*, pp. 175–190, 1994.

[14] K. Nyberg and R. A. Rueppel, "Message recovery for signature schemes based on the discrete logarithm," *Designs, Codes and Cryptography*, vol. 7, no. 1-2, pp. 61–81, 1996.

[15] Michal Sramka, "Cryptanalysis of the cryptosystem based on DLP $\gamma = \alpha^a\beta^b$," *International Journal of Network Security*, vol. 6, no. 1, pp. 80–81, 2008.

[16] S. F. Tzeng, Y. L. Tang, and M. S. Hwang, "A new convertible authenticated encryption scheme with message linkages," *Computers and Electrical Engineering*, vol. 33, no. 2, pp. 133–138, 2007.

[17] T. S. Wu, C. L. Hsu, K. Y. Tsai, H. Y. Lin, and T. C. Wu, "Convertible multi-authenticated encryption scheme," *Information Sciences*, vol. 178, no. 1, pp. 256–263, 2008.

[18] Tzong-Sun Wu and Chien-Lung Hsu, "Convertible authenticated encyption scheme," *The Journal of Systems and Software*, vol. 62, no. 3, pp. 205–209, 2002.

[19] Tzong-Sun Wu, Tzong-Chen Wu, and Wei-Hua He, "Authenticated encrption schemes with double message linkage," in *Proceeding of* 9^{th} *National Conference on Information Security, R.O.C.*, pp. 303–308, 1999.

[20] J. Zhang and Y. Wang, "On the security of a convertible authenticated encryption," *Applied Mathematics and Computation*, vol. 169, no. 2, pp. 1063–1069, 2005.