Computer Communications 32 (2009) 783–786

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Convertible multi-authenticated encryption scheme with one-way hash function

Jia-Lun Tsai *

Department of E-Learning, National Chiao Tung University, No. 1001, Ta Hsueh Road, Hsinchu 300, Taiwan, ROC

ARTICLE INFO

Article history:
Received 15 August 2008
Accepted 12 December 2008
Available online 24 December 2008

Keywords:
Multi-authenticated encryption scheme
One-way hash function
Discrete logarithms

ABSTRACT

To send the message to the recipient securely, authenticated encryption schemes were proposed. In 2008, Wu et al. [T.S. Wu, C.L. Hsu, K.Y. Tsai, H.Y. Lin, T.C. Wu, Convertible multi-authenticated encryption scheme, Information Sciences 178 (1) 256–263.] first proposed a convertible multi-authenticated encryption scheme based on discrete logarithms. However, the author finds that the computational complexity of this scheme is rather high and the message redundancy is used. To improve the computational efficiency and remove the message redundancy, the author proposes a new convertible multi-authenticated encryption scheme based on the intractability of one-way hash functions and discrete logarithms. As for efficiency, the computation cost of the proposed scheme is smaller than Wu et al.'s scheme.

1. Introduction

Authenticated encryption scheme is important issue of the network security. It ensure that the message was sent to a specified recipient securely via the insecure network environment. In general, it must achieve the confidentiality, the authenticity, and the non-repudiation properties [1–7]. In 1994, Horster et al. [1] proposed an authenticated encryption by using one-way hash function, which modified Nyberg and Ruppel's message recovery signature [2]. Since then, some similar schemes have been proposed [8–21].

In 1999, Araki et al. [8] proposed a convertible limited verifier scheme to enable the recipient to convert the message and verify the signature. However, this scheme might be unworkable if the signer is unwilling to cooperate. In 2002, Wu et al. [18] found this weakness and then proposed a convertible authenticated encryption scheme. The scheme has the following advantages: (1) The recipient easily prove the ordinary signature without the cooperation of the signer. (2) If the signer wants to repudiate his signature, he can reveal the converted signature and then any verifier can prove the dishonesty of the signer. Unfortunately, in 2003, Huang and Chang [12] found that Wu et al.'s scheme has a weakness. This weakness is that if an adversary knows the message, then he can easily convert a signature into an ordinary one. To overcome this weakness, they also proposed a new convertible authenticated encryption scheme. Letter, Chien [10] also proposed a new convertible authenticated encryption scheme. Unfortunately, in 2005, Zhang and Wang [20] found that Chen's scheme have not unforgeability and non-repudiation. Then, they also proposed an improvement of Chen's scheme.

These convertible authenticated encryption schemes have a weakness. Their schemes can not work, when the signers are more than one. In order to improve this weakness, in 2008, Wu et al. [22] propose a convertible multi-authenticated encryption scheme. The proposed scheme is used to deliver a message which is chosen and signed by multi-signer. The generated authenticated message of the proposed scheme is independent of the number of total participating signers, so it is very suitable for multi-signers.

In this paper, the author finds that the computational complexity of Wu et al.'s scheme [22] is rather high and message redundancy is used. To improve the computational efficiency and remove the message redundancy, the authors integrates convertible authenticated encryption schemes and multisignature schemes [23,24] into a new convertible multi-authenticated encryption scheme with one-way hash function. The security of this proposed multi-authenticated encryption scheme is based on one-way hash function and discrete logarithms, and the message redundancy is not used in the proposed scheme. In additions, the total computational cost of our proposed scheme is also lower than Wu et al.'s scheme. Hence, this proposed scheme is better than Wu et al.'s scheme.

The rest of this paper is organized as follows. Section 2 reviews Wu et al.'s multi-authenticated encryption scheme. In the subsequent two sections, we describe and evaluate our proposed scheme, respectively. Finally, conclusions are given in Section 5.

2. Review of Wu et al.'s scheme

The scheme of Wu et al., manipulated over GF(p), can be divided into three phases: the signature encryption, the message recovery

* Tel.: +886 3 3685557; fax: +886 3 3654872.
E-mail address: crousekimo@yahoo.com.tw

0140-3664/$ - see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2008.12.009

and the signature-conversion phases. Before reviewing of the Wu et al.'s scheme, all necessary parameters are described as follows:

p, q: large primes, such that $q|(p-1)$
g: a generator of order q over GF(p)
U_i: denote a user

Each U_i owns a private key $x_i \in Z_q$ and a corresponding public key $y_i = g^{x_i} \bmod p$ which is publicly accessible. Each phase of Wu et al.'s scheme is described as follows.

2.1. The signature-encryption phase

Without loss of generality, let $SG = \{U_1, U_2, \ldots, U_n\}$ be the signing group. For signing the message M (with redundancy embedded), each $U_i \in SG$ performs the following steps:

Step 1: U_i first chooses $w_i \in Z_q^*$ to compute

$$r_i = g^{w_i} \bmod p \quad (1)$$

and then broadcasts r_i to $U_j \in SG \setminus \{U_i\}$.
Step 2: U_i computes

$$R = M\left(\prod_{U_j \in SG} r_j^{r_j}\right) \bmod p \quad (2)$$

$$s_i = w_i r_i + x_i R \bmod q \quad (3)$$

and sends s_i to $U_j \in SG \setminus \{U_i\}$.
Step 3: U_k verifies

$$g^{s_j} = r_j^{r_j} y_j^R (\bmod p) \quad (4)$$

If the above equality holds, proceed to the next step; else, s_j is requested to be sent again.
Step 4: When all (r_j, s_j)'s are collected and verified, the clerk U_k, who can be any signer in SG, randomly chooses $d \in Z_q$ to compute

$$S = \sum_{U_j \in SG} s_j \bmod q \quad (5)$$

$$C_1 = g^d \bmod p \quad (6)$$

$$C_2 = R \oplus (y_v^d \bmod p) \quad (7)$$

Note that y_v is the public key of the designated recipient U_v.
Step 5: The clerk U_k send (C_1, C_2, S) to the recipient U_v.

2.2. The message-recovery phase

Upon receiving (C_1, C_2, S), the recipient U_v performs the following two steps:

Step 1: Compute

$$R = C_2 \oplus C_1^{x_v} \bmod p \quad (8)$$

Step 2: Recover the message M by computing

$$M = R\left(g^{-S}\left(\prod_{U_j \in SG} y_j\right)^R\right) \bmod p \quad (9)$$

If the redundancy embedded in the message M is correct, U_v accepts the signature; otherwise U_v rejects it.

2.3. The signature-conversion phase

In case of a later dispute on repudiation, U_v can just release (R, S) for the message M, such that anyone can validate the signature with Eq. (9).

3. The proposed scheme

In this section, the author shows the proposed multi-authenticated encryption scheme. The proposed encryption scheme can be divided into three phases: the signature-encryption phase, the message-recovery and the signature-conversion phase. Let $h()$ be a public one way hash function and every U_i has the private key x_i and public key $y_i = g^{x_i} \bmod p$ which can be publicly accessible. Before executing signature-encryption phase, we need to determine a clerk U_k in advance, who is randomly chosen among all the signers of the group. Each phases of our proposed multi-authenticated encryption scheme are described as follows.

3.1. The signature-encryption phase

Without loss of generality, assume that signers $U_i \in SG$ want to send U_v a message M, where $1 \leqslant M \leqslant p-1$. Let $SG = \{U_1, U_2, \ldots, U_n\}$ be the signing group. For signing the message M (with redundancy embedded), each $U_i \in SG$ performs the following steps:

Step 1: U_i first chooses a random number $w_i \in Z_q^*$ to compute

$$r_i = g^{w_i} \bmod p \quad (10)$$

And then broadcasts r_i to $U_j \in SG \setminus \{U_i\}$.
Step 2: Upon receiving r_j from $U_j \in SG \setminus \{U_i\}, U_i$ computes

$$R = M\left(\prod_{U_j \in SG} r_j\right) \bmod p \quad (11)$$

$$K = h(R, M) \bmod p \quad (12)$$

$$s_i = x_i K + w_i \bmod q \quad (13)$$

and sends s_i to the clerk U_k, who can be any signer $U_k \in SG$.
Step 3: After receiving (r_i, s_i) from $U_j \in SG \setminus \{U_i\}$, the clerk U_k verifies.

$$g^{s_j} ? = (y_i)^K * r_i \bmod p \quad (14)$$

If they are equal, proceed to the next step; else, s_j is requested to be sent again.
Step 4: When all (r_j, s_j) are collected, the clerk U_k chooses an random number $d \in Z_q$ to compute

$$S = \sum_{U_j \in SG} s_j \bmod q \quad (15)$$

$$C_1 = g^d \bmod p \quad (16)$$

$$C_2 = R \oplus (y_v^d \bmod p) \quad (17)$$

Note that y_v is the public key of the designated recipient.
Step 5: Then, this clerk U_k sends (C_1, C_2, S, K) to the recipient U_v.

3.2. The message-recovery phase

Upon receiving (C_1, C_2, S, K) from the clerk U_k, the recipient U_v can perform as following four steps:

Step 1: The recipient U_v computes

$$R = C_2 \oplus (C_1^{x_v})^{-1} \bmod p \quad (18)$$

Step 2: Recover the message M by computing

$$M = R(g^{-S})\left(\prod_{Ui\in SG}(y_i)\right)^K \bmod p \tag{19}$$

Step 3: Uses SG's public key $y_j \in SG, M, K$ and S to compute and verify

$$K? = h(R, M) \tag{20}$$

Theorem 1. *The $U_j \in SG \setminus \{U_i\}$ verifies s_i by Eq. (14).*

Proof.

$$g^{s_i}$$
$$= g^{x_i K + w_i \bmod q}$$
$$\because g^{x_i} = y_i \text{ and } g^{w_i} = r_i$$
$$= (y_i)^K * r_i \bmod p \quad \square$$

Theorem 2. *The recipient U_v uses public key $y_j \in SG, K$ and S to compute and verify by Eq. (21).*

Proof.

$$R(g^{-S})\left(\prod_{Ui\in SG}(y_i)\right)^K$$
$$\because R = M\left(\prod_{U_j\in SG} r_j\right) \bmod p, \quad s_i = x_i K + w_i \bmod q$$
$$= \left(M\left(\prod_{U_i\in SG} r_i\right)\right)\left(g^{-\left(\sum_{U_i\in SG} x_i K + w_i\right)}\right)\left(\prod_{U_i\in SG}(y_i)^K\right) = M \qquad \square$$

3.3. The signature-conversion phase

If dispute on repudiation, the recipient U_v can release the (S, K) for the message M. Anyone can use the conform its validity by computing

$$K? = h\left(M\left((g^{-S})\left(\prod_{Ui\in SG}(y_i)\right)^K\right)^{-1} \bmod p, M\right) \tag{21}$$

4. Security analysis and performance of proposed encryption scheme

4.1. Security analysis

Suppose that all communication is under the control of the adversary. That is, this adversary can read the message produced by the parties, and modified the messages before they reach their destination. The security of this proposed scheme is based on the one-way hash function and solving the discrete logarithm problem, which are believed infeasible to solve in polynomial time. They are described as follows:

Assumption 1. Intractability of reversing a one-way hash function [7]: It is computationally infeasible to derive x from a given hashed value $h(x)$, or to find two different values x, x' such that $h(x) = h(x')$.

Assumption 2. Discrete Logarithms problem [25]: for given$y \in Z_p$, it is computationally infeasible to derive x such that $y = g^x \bmod p$.

We shall consider some possible attacks against the proposed scheme, and then prove that the proposed scheme can withstand these possible attacks.

(1) Can the adversary reveal the U_i's private keys x_i from all public informations.
Assume that an adversary want to derive the U_i's private ket x_i from the U_i's public key $y_i = g^{x_i} \bmod p$. It is as difficult as solving the discrete algorithm problems. From the signature $s_i = x_i K + w_i \bmod q$, this adversary also can not do it successfully, because $s_i = x_i K + w_i \bmod q$ has two unknown variables x_i and w_i.

(2) Can the adversary forge the digital multi-signature of the message M?The multi-signature $\left(S = \sum_{U_j\in SG} s_j \bmod p = \sum_{U_i\in SG} x_i h(R, M) + w_i \bmod p, K\right)$ of the message is generated by U_i's private key x_i, random number w_i, the message M and R. If an adversary wants to forge a converted multi-signature (S, K) of the message M, this adversary must find the digital multi-signature which satisfies the following equation:

$$\left(\prod_{Ui\in SG}(y_i)\right)^{h(R,M)} * K? = g^S \tag{22}$$

From above equation, we can find that s_j consists of random number w_i, U_i's private key x_i and $h(R, M)$. Therefore, if an adversary wants to forge a signature (S, K) of the message M, this adversary must know the random number w_i, U_i's private key x_i, the message M and R. Assume that this adversary is an outsider. He can not get them, because the random number w_i and the U_i's private key x_i are only hold by the signer U_i, and R is the authenticated message for the message M. Assume that this adversary is an insider. He can not get the random number w_i and U_i's private key x_i, because the random number w_i and the U_i's private key x_i are only hold by U_i. Thus, it is impossible for any adversary to forge the digital multi-signature of the message M.

(3) Can the adversary recover the message M from the signature s_j or S?
In our proposed scheme, it is impossible for an adversary to recover the message M from the signature s_j or S successfully. The message M is encrypted by one-way hash function and protected by the private key x_i and the random number w_i. Because of the difficulty of solving the one-way hash function, it is computationally infeasible to derive the message M from a given hashed value $h(R, M)$. In addition, the private key x_i and the random number w_i are only hold by the signer $U_i \in SG$. Hence, in our proposed scheme, any adversary can not recover the message from the signature s_j or S.

(4) Can this scheme resist against the clerk attack? [26].
Assume that an adversary, say signer 1, is the clerk in our proposed scheme. This adversary wish his partner $2, 3, \ldots, n$ to sign any message M' chosen by him. His partners abnegate it, but they approve to sign the eligible message M with him. Thus, every signer U_i selects his random number $w_i \in Z_q^*$ and computes $r_i = g^{w_i} \bmod p$. Then, they broadcast r_i to every signer. Because one-way hash function and the U_i's private key x_i, it is difficult for this adversary to compute r_i and w_i which can eliminate the message M and replace it with the message M'. Check the following equation:

$$s_i = x_i h(R, M) + w_i \bmod q, \quad \text{where } R$$
$$= M\left(\prod_{U_j\in SG} r_j\right) \bmod p \tag{23}$$

Table 1
Total performance evaluation of Wu et al.'s scheme and our proposed scheme.

Phases	Our scheme	Wu et al.'s scheme
Signature-encryption phase (for all signers and the clerk)	$(n)T_h + (n^2 + n + 1)T_m + (3n)T_e$	$(2n^2 + 3n)T_m + (3n^2 + 2n + 2)T_e$
Message-recovery phase	$1T_h + (n + 2)T_m + 2T_e$	$(n + 1)T_m + 3T_e$
Signature-conversion phase	0	0
Total	$(n + 1)T_h + (n^2 + 2n + 3)T_m + (3n + 2)T_e$	$(2n^2 + 4n + 1)T_m + (3n^2 + 2n + 5)T_e$

T_m: the time for performing a modular multiplication computation.
T_e: the time for performing a modular exponentiation computation
T_h: the time for performing a one-way hash function computation.

r_i can not replace the message M with the message M', because the message M is directly encrypted with one-way hash function and protected by the U_i's private key x_i and the U_i's chosen random number w_i.

4.2. Performance evaluation

In this section, we compare the performance evaluation of our proposed scheme with the one proposed by Wu et al. From showing our scheme and Wu et al.'s scheme, we can find that the total computation cost of multi-authenticated encryption scheme increases with the number of signers, because multi-authenticated encryption scheme allows a designated recipient to recover and verify an authenticated message which is signed by multiple signers. Hence, we consider the performance comparisons not only in terms of the computational complexity of each phases but also in terms of the computational complexity required for all signers and the clerk in signature-encryption phase, for the recipient in message-recovery phase, and for the recipient in signature-conversion phase. The performance evaluation of Wu et al.'s scheme and our scheme are described as Table 1.

The time for performing the modular addition and the exclusive OR (XOR) operation is ignored because they are negligible as compared to the others. The total computation cost of our proposed scheme is $(n+1)T_h + (n^2 + 2n + 3)T_m + (3n + 2)T_e$, and the total computation cost of Wu et al.'s scheme is $(2n^2 + 4n + 1)T_m + (3n^2 + 2n + 5)T_e$. Traditionally, the time for performing a modular exponentiation computation is slower than time for performing a modular multiplication computation and time for performing a one-way hash function computation ($1T_e \approx 600T_h$) [25,27,28], so it could be easily checked that the total computational cost of our proposed scheme is lower than Wu et al.'s scheme.

5. Conclusions

In this paper, a new convertible multi-authenticated encryption scheme with one-way hash function has been proposed. The security of this proposed scheme is based on one-way hash function and discrete algorithms. As for efficiency, the computation cost of the proposed scheme is smaller than Wu et al.'s scheme. This scheme not only allows a group of singers to cooperatively produce a valid authenticated message, but also only the specific recipient can recover the message and verify by the signature. Besides, for avoiding the abuse of the signature, the proposed scheme provides ability to convert the signature into an ordinary one that can be verified by anyone.

References

[1] P. Horster, M. Michels, H. Petersen, Meta Signature Schemes Giving Message Recovery Based on the Discrete Logarithm Problem, Advances in Cryptology - ASIACRYPT '94, Springer-Verlag, 1994. 82–92.
[2] K. Nyberg, R.A. Ruppel, Message Recovery for Signature Schemes Based on the Discrete Logarithm Problem, Advances in Cryptology - EUROCRYPT'94, Springer-Verlag, 1994. May, 182–193.
[3] Y. Zheng, Digital Signcryption or How to Achieve Cost (Signature & Encryption) Cost (Signature) + Cost (Encryption), Advances in Cryptology - CRYPTO'97, Springer-Verlag, 1997. 165–179.
[4] H. Petersen, M. Michels, Cryptanalysis and improvement of signcryption schemes, IEE Proceedings-Computer Digital Techniques 145 (2) (1998) 149–151.
[5] W.B. Lee, C.C. Chang, Authenticated encryption scheme without using one-way hash function, Electronics Letter 31 (19) (1995) 1656–1657.
[6] M.K. Lee, D.K. Kim, K. Park, An authenticated encryption scheme with public verifiability, in: Japan-Korea Joint Workshop on Algorithms and Computation (WAAC2000), 2000, 49–56.
[7] W. Diffie, M. Hellman, New directions in cryptography, IEEE Transactions on Information Theory IT 22 (6) (1976) 644–654.
[8] S. Araki, S. Uehara, K. Imamura, The limited verifier signature and its application, IEICE Transactions on Fundamentals E82-A (1) (1999) 63–68.
[9] F. Bao, R.H. Deng, A signcryption scheme with signature directly verifiable by public key, Proceedings of the PKC'98-Public Key Cryptography LNCS 1431, Springer-Verlag, Berlin, 1998. 55–59.
[10] H.Y. Chien, Convertible authenticated encryption scheme without using conventional one-way function, Informatica 14 (4) (2003) 1–9.
[11] Y. Dodis, J.H. An, Concealment and Its Applications to Authenticated Encryption, Advance in Cryptology - EUROCRYPT'03, Springer-Verlag, 2003. 312–329.
[12] H.F. Huang, C.C. Chang, An efficient convertible authenticated encryption scheme and its variant, in: Proceedings of ICICS2003-Fifth International conference on Information and Communications Security, LNCS 2836, Springer-Verlag, Berlin, 2003, 382–392.
[13] C.L. Hsu, T.C. Wu, Authenticated encryption schemes with (t, n) shared verification, IEE Proceedings of the Computer and Digital Technology 145 (2) (1998) 117–120.
[14] W.B. Lee, C.C. Chang, Authenticated encryption schemes with linkage between message blocks, Information Processing Letters 63 (5) (1997) 247–250.
[15] J. Lv, X. Wang, K. Kim, Practical convertible authenticated encryption schemes using self-certified public keys, Applied Mathematics and Computation 169 (2) (2005) 1285–1297.
[16] A. Menezes, P. Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997.
[17] Y.M. Tseng, J.K. Jan, H.Y. Chien, Digital signature with message recovery using self-certified public keys and its variants, Applied Mathematics and Computation 136 (2–3) (2003) 203–214.
[18] T.S. Wu, C.L. Hsu, Convertible authenticated encryption scheme, Journal of Systems and Software 62 (3) (2002) 205–209.
[19] F. Zhang, K. Kim, A universal forgery of Araki et al.'s convertible limited verifier signature scheme, IEICE Transactions on fundamentals E86-A6 (2) (2003) 515–516.
[20] J. Zhang, Y. Wang, On the security of a convertible authenticated encryption, Applied Mathematics and Computation 169 (22) (2005) 1063–1069.
[21] Y. Zheng, Signcryption and its applications in efficient public key solutions, in: Proceedings of the ISW'97-Information Security Workshop, LNCS 1396, 1997, 291–312.
[22] T.S. Wu, C.L. Hsu, K.Y. Tsai, H.Y. Lin, T.C. Wu, Convertible multi-authenticated encryption scheme, Information Sciences 178 (1) (2008) 256–263.
[23] S. Rahul, R.C. Hansdah, A multisignature scheme for implementating safe delivery rule in group communication systems. in: International Workshop on Distributed Computing (IWDC04), LNCS 3326, Springer-Verlag, pp. 231–239, 2004.
[24] M.L. Das, A. Saxena, V. Gulati. Cryptanalysis and improvement of a multisignature scheme. in: IWDC 2005, LNCS 3741, Springer-Verlag, pp. 398–403, 2005.
[25] B. Schneier, Applied Cryptography Protocols Algorithms and Source Code in C, second ed., John Wiley and Sons Inc., New York USA, 1996. pp.15.
[26] C.C. Chang, J.J. Leu, P.C. Hwang, W.B. Lee, A scheme for obtaining a message from the digital multisignature, in: International Workshop on Practice and Theory Public Key Cryptography, Springer-Verlag, Berlin, 1998, pp. 154–163.
[27] B. Schneier, Applied Cryptology, second ed., Wiley, New York, 1996.
[28] T.F. Cheng, J.S. Lee, C.C. Chang, Security enhancement of an IC-card-based remote login mechanism, Computer Networks 51 (2007) 2280–2287.