A Robust Convertible Multi-Authenticated Encryption Scheme with One-Way Hash Function

Chung-Fu Lu, Chien-Lung Hsu, Han-Yu Lin, and Chien-Hui Su

***Abstract*—A convertible multi-authenticated encryption (CMAE) scheme allows a group of signers to cooperatively produce a valid authenticated encryption signature and still preserves the characteristic of convertible authenticated encryption (CAE) schemes. In 2008, Tsai proposed a CMAE scheme based on the intractability of one-way hash functions and discrete logarithms. However, we find that Tsai's scheme cannot provide the semantic security of the message and the computational efficiency of this scheme is rather high. In this paper, we propose a secure CMAE scheme, in which it enhances the semantic security of the message to overcome the defect in Tsai's scheme. Moreover, by compared with Tsai's scheme, the performance of the proposed scheme is more efficient than Tsai's in term of computational complexity.**

***Index Terms*—Semantic security, authenticated encryption, one-way hash function.**

I. Introduction

Elaborating on the Nyberg-Rueppel message recovery signature scheme [1], Horster *et al.*, proposed an authenticated encryption (AE) scheme [2]. An AE scheme allows one signer to generate an authenticated ciphertext such that only a designated recipient has the ability to decrypt the signed message and verify its corresponding signature. That is to say, AE schemes achieve the security requirements of confidentiality, integrity, authenticity, and non-repudiation. So far, a number of AE schemes and variations have been proposed [3]-[16].

In AE schemes, only a designated verifier is able to recover the signed message and then verify the validity of corresponding signatures. In case of a later dispute over repudiation, it is necessary to either reveal the verifier's private key or perform a zero-knowledge protocol for convincing any third party of the signer's dishonesty. In 1998, Araki *et al.* [5] proposed a convertible limited verifier signature scheme without revealing the designated verifier's private key or performing the zero-knowledge protocol. Their scheme can be recognized as a new type of AE scheme and called the convertible authenticated encryption (CAE) scheme.

In 2008, Wu *et al.*, [9] elaborated on the merits of the CAE and the multisignature schemes to propose a convertible multi-authenticated encryption (CMAE) scheme for group-oriented applications based on the computational Diffie-Hellman problem (CDHP). Their scheme allows a group of signers to cooperatively produce a valid authenticated encryption signature and still preserves the characteristic of CAE schemes. The signed message is recovered from a given signature and the validity of the recovered message along with its corresponding signature can be verified by checking the message redundancy embedded in the message. That is, the security of Wu *et al.*'s scheme is primarily based on the adopted message redundancy generation algorithm. Recently, Tsai [10] proposed a new CMAE scheme with one-way hash function. His scheme outperforms Wu *et al.*, one in terms of computational efficiency.

The security of Tsai's scheme is based on the one-way hash function and solving the discrete logarithm problem, which are believed infeasible to solve in polynomial time. However, we will show that the scheme cannot provide the semantic security of the message. In this paper, we gave a further improvement to provide the semantic security. Our improvement makes it more efficient in computation and communication.

II. Review of Tsai's Scheme

The Tsai's scheme manipulated over GF (p), is comprised of three phases: 1) Signature encryption phase, 2) Message recovery and verification phase, and () Signature conversion phases. Before reviewing of the Tsai's scheme, all necessary parameters are described as follows:

p, q: large primes, such that $q|(p\text{-}1)$,
g: a generator of order q over GF(p),
$h()$: a public one way hash function,
$\oplus$: the bit-wise exclusive-or operation,
U_i: denote a user.

Each U_i owns the private key $x_i \in_R Z_q^*$ and public key $y_i = g^{x_i} \bmod p$ which is publicly accessible. Each phase of Tsai's scheme is described as follows.

A. Signature Encryption (SE) Phase

Without loss of generality, let $SG = \{U_1, U_2, ..., U_n\}$ be the signing group and signers $U_i \in SG$ want to send U_v a message M, where $1 \le M \le p-1$. For signing the message M, each $U_i \in SG$ performs the following steps:

Step 1: U_i chooses a random number $w_i \in Z_q^*$ to compute and broadcasts r_i to $U_j \in SG \setminus \{U_i\}$.

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

Step 2: By all received r_j's from $U_j \in SG \setminus \{U_i\}$ and r_i, U_i

Manuscript received January 9, 2014; revised April 10, 2014.

Chung-Fu Lu, Chien-Lung Hsu, Chien-Hui Su are with Department of Information Management, Chihlee Institute of Technology, No. 313, Sec.1, Wunhua Rd., Banciao District, New Taipei City, Taiwan (e-mail: peter61@mail.chihlee.edu.tw, clhsu@mail.cgu.edu.tw, lucy30812@gmail.com).

Han-Yu Lin is with National Taiwan Ocean University, Department of Computer Science and Engineering, 2 Pei-Ning Road, Keelung, Taiwan (e-mail: lin.hanyu@msa.hinet.net).

DOI: 10.7763/IJFCC.2014.V3.318

computes and then sends s_i to the $U_j \in SG \setminus \{U_i\}$

$$R = M\big(\prod_{U_j \in SG} r_j\big) \bmod p\,, \tag{2}$$

$$K = h(R, M) \bmod p\ , \tag{3}$$

$$s_i = x_i K + w_i \bmod q \tag{4}$$

Step 3: Upon receiving s_j from $U_j \in SG \setminus \{U_i\}$, U_i verifies

$$g^{s_j} = y_j^K r_j \bmod p\,. \tag{5}$$

If Eq. (4) holds, proceed to Step 4; otherwise U_i requests $U_j \in SG \setminus \{U_i\}$ to resend s_j.

Step 4: When all $\{r_j, s_j\}$'s are collected and verified, the clerk U_k who can be any signer in *SG*, chooses $d \in_R Z_q$ to compute

$$S = \sum_{U_j \in SG} s_j \bmod q\,, \tag{6}$$

$$C_1 = g^d \bmod p\,, \tag{7}$$

$$C_2 = R \oplus (y_v^d \bmod p)\,, \tag{8}$$

Note that y_v is the public key of the designated recipient U_v.

Step 5: The clerk U_k sends $\{S, C_1, C_2, K\}$ to the designated recipient U_v.

Tsai's scheme is a distributed scheme and, hence, anyone in *SG* can act as the clerk to collect and verify all individual signatures, and combines them into $\{S, C_1, C_2, K\}$ for the designated recipient U_v. It means that each individual signers can produce the same signature $\{S, C_1, C_2, K\}$. If the clerk dishonestly performs his tasks, the validity of the combined $\{S, C_1, C_2, K\}$ will be detected by other signers.

B. Message Recovery and Verification (MRV) Phase

Upon receiving $\{S, C_1, C_2, K\}$ from the clerk U_k, the designated recipient U_v can perform as following three steps: Step1: The designated recipient U_v computes

$$R = C_2 \oplus C_1^{x_v} \bmod p\,. \tag{9}$$

Step 2: The recipient U_v recovers the message *M* by computing

$$M = R(g^{-s})\big(\prod_{U_i \in SG} y_i\big)^K \bmod p\,\cdot \tag{10}$$

Step 3: The recipient U_v verifies

$$K = h(R, M)\,. \tag{11}$$

$$K = h(M(g^{-s}(\prod_{U_i \in SG} y_i)^K)^{-1} \bmod p, M)\,\cdot \tag{12}$$

If Eq. (11) holds, the signature is accepted; otherwise it is refused.

C. Signature Conversion (SC) Phase

If dispute on repudiation, the recipient U_v can release the $\{S, K\}$ for the message *M*. With this converted signature, anyone can validate its validity by computing

D. Weakness of Tsai's Scheme

Suppose an adversary gets a valid $\{K, S, y_i\,; i = 1, 2, ..., n\}$, he can check whether his guessed message *M** satisfies Eq. (12). If it holds, then he gets the actual message. So Tsai's scheme cannot provide the semantic security of the message. Tsai's scheme cannot provide the semantic security of the message.

III. Our Improved Scheme

Semantic security is of very importance to an authenticated encryption scheme for practical communications. Otherwise, if the possible messages are limited, then an adversary can eventually determine which message the signer signs by checking which satisfies the verification equalities. Tsai's scheme cannot provide the semantic security of the message. To provide the semantic security, the authors propose an improved scheme. Furthermore, our improvement is more efficient in term of computational efforts. Each phases of our improved scheme are described as follows.

A. Signature Encryption (SE) Phase

The system model and parameters are defined as those in Section II. For signing the message *M*, each $U_i \in SG$ performs the following steps:

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

$$r_i = g^{w_i} \bmod p \tag{13}$$

And broadcasts r_i to $U_j \in SG \setminus \{U_i\}$.

Step 2: By all received r_j's from $U_j \in SG \setminus \{U_i\}$ and r_i, U_i computes

$$R = M \oplus \big(\prod_{U_j \in SG} r_j\big) \bmod p\,, \tag{14}$$

$$K = h\big(\prod_{U_j \in SG} r_j, M\big) \bmod p\,, \tag{15}$$

$$s_i = x_i K + w_i \bmod q\ , \tag{16}$$

And then sends s_i to the $U_j \in SG \setminus \{U_i\}$.

Step 3: Upon receiving s_j from $U_j \in SG \setminus \{U_i\}$, U_i verifies

$$g^{s_j} \overset{?}{=} y_j^K r_j \bmod p\,. \tag{17}$$

If Eq. (4) holds, proceed to Step 4; otherwise U_i requests $U_j \in SG \setminus \{U_i\}$ to resend s_j.

Step 4: When all $\{r_j, s_j\}$'s are collected and verified, the clerk U_k who can be any signer in *SG*, chooses $d \in_R Z_q$ to compute

$$S = \sum_{U_j \in SG} s_j \bmod q\,, \tag{18}$$

$$C_1 = g^d \bmod p\,, \tag{19}$$

$$C_2 = R \oplus (y_v^d \bmod p)\,, \tag{20}$$

$$Q = K \oplus (y_v^d \bmod p)\,. \tag{21}$$

Note that y_v is the public key of the designated recipient U_v.

Step 5: The clerk U_k sends $\{S, C_1, C_2, Q\}$ to the recipient U_v.

B. Message Recovery and Verification (MRV) Phase

Upon receiving $\{S, C_1, C_2, Q\}$ from the clerk U_k, the designated recipient U_v can perform as following three steps:

Step 1: The designated recipient U_v computes

$$R = C_2 \oplus C_1^{x_v} \bmod p, \tag{22}$$

$$K = Q \oplus C_1^{x_v} \bmod p. \tag{23}$$

Step 2: The recipient U_v recovers the message M by computing

$$M = R \oplus (g^S (\prod_{U_j \in SG} y_j)^{-K} \bmod p) \cdot \tag{24}$$

Step 3: The recipient U_v verifies

$$K = h((g^S (\prod_{U_j \in SG} y_j)^{-K} \bmod p), M). \tag{25}$$

If Eq. (25) holds, the signature is accepted; otherwise it is refused.

C. Signature Conversion (SC) Phase

If dispute on repudiation, the recipient U_v can release the $\{S, K\}$ for the message M. With this converted signature, anyone can validate its validity by Eq. (25).

IV. Analysis of the Improved Scheme

Security analysis and computational complexity analysis of our improved scheme are given below.

A. Security Analysis

The security of the proposed scheme is based on well-known cryptographic assumptions: solving the discrete logarithm problem (DLP) [17] and the intractability of reversing the one-way hash function (OWHF) [18]. In the following, we discuss some possible attacks against the proposed scheme and show that the proposed scheme is secure under the protection of the DLP and OWHF assumptions.

1) Can the attacker reveal the secret key x_i of the signer $U_i \in SG$ or the secret key x_V of the designated recipient U_V from all public information?

With the authenticated encryption signature $\{S, C_1, C_{2,l}, Q\}$, s_i and r_i, the attacker cannot derive the signer's secret key x_i from Eq. (16), since the equation contains two unknown variables x_i and w_i, and w_i is protected under the DLP assumptions. Similarly, the attacker cannot reveal verifier's secret key x_V from Eq.(22) and Eq.(23), since x_V here is protected under the DLP assumptions.

2) Can the attacker forge an authenticated encryption signature?

To forge a signature for satisfying Eq. (24), the attacker must know the all random numbers w_i's and U_i's private key x_i. However, it will not be workable since all w_i's and x_i are protected under the DLP assumption. The attacker cannot get them, because w_i and x_i are only hold by the signer $U_i \in SG$. Thus, it is impossible for any attacker to forge the digital multi-signature of the message M.

3) Can the attacker forge a converted signature?

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 cannot get them, because the w_i and 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 cannot get the w_i and x_i, because the w_i and 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.

4) Can the attacker recover the message from the authenticated encryption signature?

With the authenticated encryption signature $\{S, C_1, C_{2,l}, Q\}$, the attacker cannot derive the message M from Eq. (25) since the K is protected under the DLP assumption. In addition, the x_V is only hold by the signer U_V. The attacker cannot derive the R from Eq. (22). Thus, it is impossible for an attacker to recover the message M from the Eq. (24) successfully.

TABLE I: Comparisons of Computational Complexities

Phases		Our proposed scheme	Tsai's scheme [2]
SE	Time complexities	$nT_H + (3n)T_{EXP}$ $+ (n^2+n-1)T_{MUL}$	$nT_H + (3n)T_{EXP}$ $+ (n^2+2n-1)T_{MUL}$
	Rough Estimation	$(n^2+725n-1)T_{MUL}$	$(n^2+726n-1)T_{MUL}$
MRV	Time complexities	$T_H + (n+1)T_{MUL}$ $+ 3T_{EXP} + T_{INV}$	$T_H + (n+1)T_{MUL}$ $+ 3T_{EXP} + T_{INV}$
	Rough Estimation	$(n+734)T_{MUL}$	$(n+735)T_{MUL}$
SC	Time complexities	$T_H + nT_{MUL}$ $+ 2T_{EXP} + T_{INV}$	$T_H + (n+1)T_{MUL}$ $+ 2T_{EXP} + T_{INV}$
	Rough Estimation	$(n+494)T_{MUL}$	$(n+495)T_{MUL}$
Total	Time complexities	$(n+2)T_H + 2T_{INV}$ $+ (n^2+3n-1)T_{MUL}$ $+ (3n+5)T_{EXP}$	$(n+2)T_H + 2T_{INV}$ $+ (n^2+4n+1)T_{MUL}$ $+ (3n+5)T_{EXP}$
	Rough Estimation	$(n^2+727n+1227)T_{MUL}$	$(n^2+728n+1229)T_{MUL}$

5) Can the attacker verify the signature before converted?

It requires the message M to perform the signature verification of Eq. (25). From the discussion (4), the attacker cannot obtain the message M before the signature is converted. Hence he cannot verify the signature.

B. Computational Complexity Analysis

We denote the following notations to facilitate the performance evaluation:

T_{MUL}: time for performing a modular multiplication computation,

T_{EXP}: time for performing a modular exponentiation computation,

T_H: time for performing a one-way hash function computation,

T_{INV}: time for performing a modular inversion computation.

The time for performing the modular addition and the exclusive OR (XOR) operation are ignored, since they are relatively smaller than those for performing other operations. From [19], [20], the time complexities can be respectively regarded as $T_{EXP} \approx 240\ T_{MUL}$, $T_{INV} \approx 10\ T_{MUL}$, and $T_H \approx 4\ T_{MUL}$. The performance evaluations of the two schemes are described as Table I. Thus, we conclude that the proposed scheme is more efficient than Tsai's in term of computational complexity.

V. Conclusion

Semantic security is of very importance to an authenticated encryption scheme for practical communications. This article has shown that Tsai's scheme cannot provide the semantic security of the message. To provide the semantic security, the authors propose a secure CMAE scheme based on the intractability of one-way hash functions and discrete logarithms. Furthermore, our improvement is more efficient in term of computational complexity.

Acknowledgment

We would like to thank anonymous referees for their valuable suggestions. We thank Healthy Aging Research Center (HARC) of Chang Gung University for excellent technical assistance. This work was supported in part by the Healthy Aging Research Center Grant CMRPD1B0331, in part by the Chang Gung Memorial Hospital Grant CMRPD3D0041, and in part by National Science Council under the grant NSC 100-2628-H-182-001-MY3.

References

[1] K. Nyberg and R. A. Ruppel, "Message recovery for signature scheme based on the discrete logarithm problem," *Advance in Cryptology – Eurocrypt'94*, Springer, Berlin, 1994, pp. 175-190.

[2] P. Horster, M. Michels, and H. Petersen, "Authenticated encryption schemes with low communication costs," *Electron. Lett.*, vol. 30, no. 15, pp. 1212-1213, July, 1994.

[3] W. B. Lee and C. C. Chang, "Authenticated encryption schemes without using a one way function," *Electron. Lett.*, vol. 31, no.19, pp.1656-1657, September, 1995.

[4] W. B. Lee and C. C. Chang, "Authenticated encryption schemes with linkage between message blocks," *Inf. Process. Lett.*, vol. 63, no. 5, pp. 247-250, September, 1997.

[5] S. Araki, S. Uehara, and K. Imamura, "Convertible limited verifier signature based on Horster's authenticated encryption," in *Proc. 1998 Symposium on Cryptography and Information Security*, 1998, pp. 32-36.

[6] T. S. Wu and C. L. Hsu, "Convertible authenticated encryption scheme," *J. Syst. Softw.*, vol. 62, no. 3, pp. 205-209, June, 2002.

[7] H.Y. Chien, "Convertible authenticated encryption scheme without using conventional one-way function," *Inform.*, vol. 14, no. 4, pp. 445-454, 2003.

[8] J. Zhang and Y. Wang, "On the security of a convertible authenticated encryption," *Appl. Math. Comput*, vol. 169, no. 2, pp. 1063-1069, 2005.

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

[10] J. L. Tsai, "Convertible multi-authenticated encryption scheme with one-way hash function," *Comput. Commun*, vol. 32, no. 5, pp. 783-786, March, 2009.

[11] J. L. Tsai, T. S. Wu, H.Y Lin, and J. E. Lee, "Efficient convertible multi-authenticated encryption scheme without message redundancy or one-way hash function," *Int. J. Innov. Comp. Inf. Control*, vol. 6, no. 9, pp. 3843-3852, September, 2010.

[12] J. H. Zhang, X. Liu, and C.L. Liu, "Security Analysis of a Convertible Multiauthenticated Encryption Scheme," *Adv. Mater. Res.*, vol. 159, pp. 111-115, December, 2010.

[13] C. L. Hsu and H. Y. Lin, "New identity-based key-insulated convertible multi-authenticated encryption scheme," *J. Netw. Comput. Appl.*, vol. 34, no. 5, pp. 1724-1731, September, 2011.

[14] H. Y. Lin, C. L. Hsu, and S. K. Huang, "Improved convertible authenticated encryption scheme with provable security," *Inf. Process. Lett.*, vol. 111, no. 13, July, pp. 661-666, 2011.

[15] T. S. Wu, Y. S. Chen, H. Y. Lin, and T. K. Chang, "Authenticated encryption scheme based on paillier system with verifiable public keys," *Commun. Comput. Secur.*, vol. 1, pp. 1-5, 2012.

[16] C. F. Lu, C. L. Hsu, and H. Y. Lin, "Provably convertible multi-authenticated encryption scheme for generalized group communications," *Inf. Sci.*, vol. 199, pp. 154-166, September, 2012.

[17] B. Schneier, *Applied Cryptography Protocols Algorithms and Source Code in C*, second Ed., John Wiley and Sons: New York, 1996.

[18] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644-654, January, 1976.

[19] N. Koblitz, A. Menezes, and S. Vanstone, "The state of elliptic curve cryptography," *Des. Codes Crypto,* vol. 19, no. 2-3, March, 173-193, 2000.

[20] S. Contini, A. K. Lenstra, and R. Steinfeld, "VSH, an Efficient and Provable Collision-Resistant Hash Function," *Advances in Cryptology – EUROCRYPT 2006*, Saint Petersburg, Russia, 2006, pp. 165-182.

Chung-Fu Lu received the B.S. and M.S. degree in electrical engineering from National Taiwan University of Science and Technology in 1991 and 1993 respectively. He is currently a Ph.D student in the Department of Information Management, National Taiwan University of Science and Technology. He is also a lecturer of the Taipei College of Maritime Technology. His research interests are in the areas of cryptography, computer networks and network security.

Chien-Lung Hsu received a B.S. degree in business administration, an M.S. degree in information management, and a Ph.D. degree in information management from the National Taiwan University of Science and Technology, Taiwan in 1995, 1997, and 2002, respectively. He was an assistant professor and an associate professor in the Department of Information Management, Chang Gung University (CGU), Taiwan from 2004 to 2007 and from 2007 to 2011, respectively. Currently, he is a professor in the Department of Information Management, Chang Gung University since 2011. He is also the leader of the Ubiquitous Security and Applications Lab, the director of Chinese Cryptology Information Security Association (CCISA, Taiwan), the chair of Education Promotion Committee of CCISA, the member of Academia-Industry Cooperation Committee of CCISA, the chair of Program of RFID Applications in Logistics Supply Chain Management of CGU, the chair of program of information security with medical applications of CGU, the director of Division of Instructional Support of Computer Center of CGU, the researcher of Healthy Aging Research Center (HARC) of CGU, the researcher of Elder Industry Development and Research Center (EIDRC) of CGU, and the senior researcher of Taiwan Information Security Center (TWISC). His current research includes cryptography, information security, wireless sensor network, mobile commerce, digital forensics, vehicular system security, healthcare system and user acceptance, smart home system, and etc.

Han-Yu Lin received BA degree in economics from the Fu-Jen University, Taiwan in 2001, his MS degree in information management from the Huafan University, Taiwan in 2003, and his Ph.D. degree in computer science and engineering from the National Chiao Tung University, Taiwan in 2010. He has been an assistant professor in the Department of Computer Science and Engineering of National Taiwan Ocean University since August 2012. His research interests include cryptology, network security, digital forensics, cloud computing security and e-commerce security.

Chien-Hui Su received a bachelor's degree from National Taipei University of Nursing and Health Sciences in 2009; She received her master's degree in information management from Chang Gung University in 2011. Now she is a Ph.D. student in graduate institute of business and management from Chang Gung University in 2014, respectively. Her research interests include information security, information systems, cryptography, mobile commerce, and health care.