Bilinear Pairings Based Convertible Authenticated Encryption Scheme with Provable Recipient

Han-Yu Lin[a] and Tzong-Sun Wu[b]
[a] *Department of Computer Science*
National Chiao Tung University, Taiwan
hanyu.cs94g@nctu.edu.tw
[b] *Department of Computer Science and Engineering*
National Taiwan Ocean University, Taiwan
ilan543@gmail.com

Abstract-*Convertible authenticated encryption (CAE) schemes are important cryptographic techniques which are applicable to many confidential business applications such as the contract signing and the credit card transactions. In case of a later dispute over repudiation, CAE schemes provide an arbitration mechanism for the public verification. Yet, previous proposed CAE schemes are primarily based on the discrete logarithm problem or the factorization problem and can not allow the designated recipient to prove himself as the real recipient. In this paper, we propose a bilinear pairings based efficient CAE scheme with provable recipient. The proposed scheme not only enables the designated recipient to prove that he is the real recipient if needed, but also has a nice signature conversion mechanism which can be solely done by the designated recipient without any extra computation or communication cost.*

Keywords: authenticated encryption, conversion, bilinear pairings, public key encryption.

1. Introduction

With the rapid development of electronic commerce (eCommerce), the security of on-line transactions has received the great attention. Generally speaking, cryptographic techniques can be adopted to protect the communication content over the Internet. In 1967, Diffie and Hellman [6] proposed the first public key cryptosystem based on the discrete logarithm problem (DLP) [6, 18]. In the system, each user owns a self-chosen private key and then further computes the corresponding public key. The former is kept secret and stored by the user himself while the latter is made public and maintained in the public key directory which is accessible to anyone else. It is computationally infeasible to derive any user's private key from his public one.

With these two keys, one can perform the public key encryption and the digital signature scheme [7, 16]. The public key encryption satisfies the requirement of confidentiality [10] while the digital signature scheme satisfies those of integrity [18], authenticity [18] and non-repudiation [18]. One can see that some business activities such as the contract signing and the credit card transactions require that all the above properties simultaneously be fulfilled. Although one can use the so-called two-step approach [19], i.e., sign-then-encrypt, to achieve the purpose, this approach is inefficient for that the total cost is equal to the sum of both.

To obtain a better performance, in 1994, Horster *et al*. [9] proposed an authenticated encryption (AE) scheme combining the functions of public key encryption and the digital signature scheme. In an AE scheme, the signer can generate an authenticated ciphertext such that only the designated recipient is capable of decrypting the ciphertext and verifying the signature. As compared with the two-step approach, an AE scheme greatly reduces the computational complexities. Yet, AE schemes have a potential drawback in dealing with a later repudiation dispute, since only the designated recipient can verify the signer's signature instead of anyone else. Consequently, it is even difficult for an arbitrator to judge who is lying. To overcome the problem, in 1999, Araki *et al*. [1] proposed a convertible limited verifier signature scheme which allows the designated recipient to convert the ciphertext into an ordinary signature. However, the conversion process requires the signer's corporation and will increase the additional computation cost. If the signer is unwilling to cooperate with, the conversion process is unworkable.

In 2002, Wu and Hsu [20] proposed a convertible authenticated encryption (CAE) scheme in which the signature conversion can be solely done by the designated recipient and takes no extra computation or communication cost. Since then, lots of researchers [5, 12, 15, 21-23] have devoted themselves to the enhancement of CAE schemes. Nevertheless, these schemes are primarily based on the DLP or the factorization problem [16].

Recently, a so-called bilinear pairings cryptosystem from elliptic curves [11, 13, 14] has been found various applications [2-4, 8, 17, 24] in cryptography. In this paper, we address a solution to confidential transactions of pairings-based systems and propose an efficient CAE scheme based on bilinear pairings. Preserving the merits of traditional CAE schemes based on DLP, the proposed one further equips the designated recipient with the ability to prove that he is the real recipient if needed. A significant advantage of our scheme is that the signature conversion process takes no additional computation efforts or communication overheads, because the converted signature will be derived during the signature verification phase. Moreover, it is not necessary for the designated recipient to reveal his private key for the public arbitration. We also demonstrate that the proposed CAE scheme is correct and fulfills the requirements of confidentiality, unforgeability, non-repudiation and semantic security.

The rest of this paper is organized as follows. Section 2 states some preliminaries. We present the proposed scheme in Section 3. The security analyses and the efficiency evaluation are discussed in Sections 4. Finally, a conclusion with respect to the proposed scheme is given in Section 5.

2. Preliminaries

In this section, we first define involved parties of a CAE scheme and then review some security definitions with respect to the proposed scheme.

2.1 Involved Parties

A CAE scheme has two involved parties: a signer and a designated recipient (or verifier). Each is a polynomial-time-bounded probabilistic Turing machine (PPTM). The signer will generate an authenticated ciphertext and deliver it to the designated recipient. Yet, a dishonest signer might repudiate his generated signatures. Finally, the designated recipient decrypts the ciphertext and verifies the signer's signature.

2.2 Security Notions

Let $(\boldsymbol{G}_1, +)$ and $(\boldsymbol{G}_2, \times)$ denote groups of the same prime order q. Assume that e: $\boldsymbol{G}_1 \times \boldsymbol{G}_1 \rightarrow \boldsymbol{G}_2$ is a bilinear map satisfying the following properties:

(i) ***Bilinearity***:

$e(P_1 + P_2, Q) = e(P_1, Q)e(P_2, Q)$;

$e(P, Q_1 + Q_2) = e(P, Q_1)e(P, Q_2)$;

$e(aP, bQ) = e(P, Q)^{ab}$ for $P, Q \in \boldsymbol{G}_1$ and $a, b \in Z_q^*$.

(ii) ***Non-degeneracy***:

If P is a generator of $\boldsymbol{G}_1$, then $e(P, P)$ is a generator of $\boldsymbol{G}_2$.

(iii) ***Computability***:

Given $P, Q \in \boldsymbol{G}_1$, the value of $e(P, Q)$ can be efficiently computed by a polynomial-time algorithm.

Definition 1 (Bilinear Diffie-Hellman problem)

Given an BDH instance $(P, A, B, C) \in \boldsymbol{G}_1$ where $A = aP$, $B = bP$ and $C = cP$ for some $(a, b, c) \in Z_q^*$, compute $e(P, P)^{abc} \in \boldsymbol{G}_2$.

Definition 2 (Bilinear Diffie-Hellman assumption)

For every probabilistic polynomial-time algorithm $\mathcal{A}$, every positive polynomial $Q(\cdot)$ and all sufficiently large k, the algorithm $\mathcal{A}$ can solve the BDH problem with an advantage at most $\frac{1}{Q(k)}$, i.e.,

$$\Pr[\mathcal{A}(P, aP, bP, cP) = e(P, P)^{abc},\ (a, b, c) \leftarrow Z_q^*,\ (P, aP, bP, cP) \leftarrow \boldsymbol{G}_1] \leq \frac{1}{Q(k)}.$$

The probability is taken over the uniformly and independently $P \in \boldsymbol{G}_1$ and $(a, b, c) \in Z_q^*$ and over the random choices of $\mathcal{A}$.

Definition 3 (Elliptic curve discrete logarithm problem; ECDLP)

Let P be a generator of prime order q of $\boldsymbol{G}_1$. The elliptic curve discrete logarithm problem is, given an instance (P, Y) for some $Y \in \boldsymbol{G}_1$, to derive $x \in Z_q^*$ such that $Y = xP$.

Definition 4 (Elliptic curve discrete logarithm assumption)

For every probabilistic polynomial-time algorithm $\mathcal{A}$, every positive polynomial $Q(\cdot)$ and all sufficiently large k, the algorithm $\mathcal{A}$ can solve the ECDLP with an advantage at most $\frac{1}{Q(k)}$, i.e.,

$$\Pr[\mathcal{A}(P, xP) = x, x \leftarrow Z_q^*, P \leftarrow \boldsymbol{G}_1] \leq \frac{1}{Q(k)}.$$

The probability is taken over the uniformly and independently $P \in \boldsymbol{G}_1$ and $x \in Z_q^*$ and over the random choices of $\mathcal{A}$.

3. The Proposed Scheme

The proposed CAE scheme can be divided into four phases: the signature generation, the signature verification, the signature conversion and the recipient proof phases. Initially, the system determines the following public information:

q:	a large prime;
$\boldsymbol{G}_1$, $\boldsymbol{G}_2$:	two groups of the same order q;
P:	a generator of order q over $\boldsymbol{G}_1$;
e:	a bilinear pairing, e: $\boldsymbol{G}_1 \rightarrow \boldsymbol{G}_2$;
h_1:	a one-way hash function, h_1: $\{0, 1\}^* \times \boldsymbol{G}_1 \rightarrow Z_q^*$;
h_2:	a one-way hash function, h_1: $\boldsymbol{G}_1 \rightarrow Z_q^*$;

Each user U_i chooses his private key $x_i \in Z_q^*$ and computes the corresponding public key as $Y_i = x_iP$. Details of each phase are described below:

***The signature generation phase*:** Let U_a be the signer and U_b the designated recipient. For signing the message m, U_a chooses an integer $r \in Z_q^*$ and computes

$$R = rP, \tag{1}$$

$$S = (rx_a^{-1} + h_1(m, R))P, \tag{2}$$

$$K = rY_b, \tag{3}$$

$$t = h_2(R)^{-1}m \bmod q, \tag{4}$$

and then deliveries the authenticated ciphertext (S, K, t) to U_b.

***The signature verification phase*:** Upon receiving the ciphertext (S, K, t), U_b first computes

$$R = x_b^{-1}K. \tag{5}$$

He then recovers the message m as

$$m = th_2(R), \tag{6}$$

and checks the redundancy embedded in m. U_b can further verify the signature by checking

$$e(S, Y_a) = e(R + h_1(m, R)Y_a, P). \tag{7}$$

***The signature conversion phase*:** In case of a latter dispute over repudiation, U_b can just release the message m along with its converted signature (S, R). Then any third party can perform Eq. (7) to realize the signer's dishonesty. It can be seen that the parameter R is derived during the signature verification process. Consequently, the signature conversion takes no additional computation efforts or communication overheads. Besides, it is not necessary for the designated recipient to reveal his private key.

***The recipient proof phase*:** For convincing someone, say, U_c, that U_b is the real recipient, he can perform the following interactive steps with U_c:

Step 1 U_b sends the ciphertext (S, K, t), the converted signature (S, R) and the original message m to U_c.

Step 2 U_c first checks the converted signature's validity with Eq. (7). If it holds, U_c proceeds to the next step; otherwise, the protocol is terminated.

Step 3 U_c randomly chooses an integer d to compute $E = dK$ and then transmits E to U_b.

Step 4 Upon receiving E, U_b computes $W = x_b^{-1}E$ and returns it to U_c.

Step 5 U_c computes $W' = dR$ and checks whether $W = W'$. If it holds, U_c is convinced that U_b is the real recipient.

4. Security Analyses and Efficiency

In this section, we first analyze the security of our proposed scheme and then evaluate its efficiency.

4.1 Security Analyses

We demonstrate that the proposed CAE scheme is correct and achieves the security requirements of confidentiality, unforgeability and non-repudiation.

Correctness. A CAE scheme is correct if the signer can generate a valid authenticated ciphertext and only the designated recipient is capable of decrypting the ciphertext and verifying the recovered signature when all involved parties follow the steps of the scheme. We prove the correctness of our proposed scheme as Theorems 1 and 2.

Theorem 1. *The designated recipient U_b can correctly recover the message m with embedded redundancy by Eq. (6).*

Proof: From the right-hand side of Eq. (6), we have

$$\begin{aligned} & th_2(R) \\ &= th_2(x_b^{-1}K) && \text{(by Eq. (5))} \\ &= th_2(x_b^{-1}rY_b) && \text{(by Eq. (3))} \\ &= th_2(x_b^{-1}r\, x_bP) \\ &= th_2(rP) \\ &= th_2(R) && \text{(by Eq. (1))} \\ &= m && \text{(by Eq. (4))} \end{aligned}$$

which leads to the left-hand side of Eq. (6).

Q.E.D.

Theorem 2. *The designated recipient U_b can correctly verify the signature with Eq. (7).*

Proof: From the right-hand side of Eq. (7), we have

$$\begin{aligned} & e(R + h_1(m, R)Y_a, P) \\ &= e(rP + h_1(m, R)Y_a, P) && \text{(by Eq. (1))} \\ &= e(rP + h_1(m, R)x_aP, P) \\ &= e((r + h_1(m, R)x_a)P, P) \\ &= e(x_a(rx_a^{-1} + h_1(m, R))P, P) \\ &= e((rx_a^{-1} + h_1(m, R))P, x_aP) \\ &= e(S, Y_a) && \text{(by Eq. (2))} \end{aligned}$$

which leads to the left-hand side of Eq. (7).

Q.E.D.

Confidentiality

(i). ***The confidentiality of the user U_i's private key:*** To successfully derive the user U_i's private key x_i from its corresponding public key, an attacker must has the ability to solve the ECDLP which is computationally infeasible. If the attacker attempts to compute the signer's private key from Eq. (2), he has to know the secret integer r first. Even though he has the knowledge of r, he still faces the intractability of ECDLP. Hence, the confidentiality of the user U_i's private key x_i is assured under the protection of ECDLP.

(ii). ***The confidentiality of the original message:*** To recover the message m, any attacker has to obtain the parameter R first. However, computing R with Eq. (5) requires the designated recipient's private key x_b which is computationally infeasible to obtain according the above analyses. We further consider the requirement of semantic security. A CAE scheme is said to satisfy the requirement of semantic security if the generated authenticated ciphertext is computationally indistinguishable with respect to even two candidate messages. It can be seen that to guess a correct candidate message for a given ciphertext from Eq. (7), any attacker still requires an additional parameter R to complete the process. Yet, we have known that the parameter R can only be derived by the designated recipient. Therefore, any attacker has the advantage of guessing the correct one with no more than 1/2, i.e., the generated authenticated ciphertext is computationally indistinguishable. We conclude that the proposed CAE scheme satisfies the requirement of semantic security and thus the confidentiality of the message is achieved.

Unforgeability

(i) ***The unforgeability of the authenticated ciphertext:*** To forge a valid authenticated ciphertext (S', K', t') on an arbitrarily chosen message m', an attacker may first randomly choose r' to compute R', K' and t' with Eqs. (1), (3) and (4), respectively. Then he attempts to derive S' fulfilling Eq. (7). However, he will face the intractability of BDHP and fail to make it. In addition, based on the difficulty of ECDLP, he cannot obtain the signer's private key to forge a valid authenticated ciphertext either.

(ii) ***The unforgeability of the converted signature:*** To forge a valid converted signature (S', R') on an arbitrarily chosen message m', an attacker may first randomly choose S' and then compute R' satisfying Eq. (7). Unfortunately, he cannot make it unless he has the ability to compute the BDHP and invert the one-way hash function. On the contrary, if he randomly chooses R' to derive S' passing the test of Eq. (7), the intractable situation remains the same. Hence, the proposed CAE scheme is secure against existential forgery attack on arbitrarily chosen messages.

Non-repudiation

The proposed CAE scheme allows the signer

U_a to generate an authenticated ciphertext (S, K, t) which can only be decrypted and verified by the designated recipient U_b. When the case of a later repudiation occurs, U_b can just reveal the converted signature (S, R) and the original message m for the public arbitration. According to the analyses of the confidentiality of the user U_i's private key and the unforgeability of the converted signature, any attacker cannot forge a valid signature without knowing the signer's private key x_a. Therefore, the signer U_a cannot deny his generated signatures.

From the above discussions, it can be seen that the proposed CAE scheme is secure against known active attacks even under the semantic security based on the hardness of ECDLP and BDHP.

4.2 Efficiency

Since the proposed scheme is totally different from previous CAE ones based on the DLP or the factorization problem, we only evaluate the efficiency of our scheme in terms of the computational complexities. For facilitating the following evaluation, we first define some necessary notations below.

T_{EA}: the time for performing a modular addition computation over an elliptic curve;

T_{EM}: the time for performing a modular multiplication computation over an elliptic curve;

T_I: the time for performing a modular inverse computation;

T_M: the time for performing a modular multiplication computation;

T_H: the time for performing a one-way hash function;

T_B: the time for performing a bilinear paring computation;

Note that the time for performing the modular addition operation is ignored because they are negligible as compared to computing time of performing others. The detailed evaluation is demonstrated as Table 1.

5. Conclusions

In this paper, we have proposed a bilinear pairings based efficient CAE scheme with provable recipient. In our proposed scheme, the signature conversion can be solely performed by the designated recipient without extra computation efforts or communication overheads, because the converted signature will be derived during the signature verification phase. It is not necessary for the designated recipient to reveal his private key for the public arbitration in case of a later dispute over repudiation. Also, the proposed scheme provides the designated recipient with the ability to prove himself as the real recipient if needed. Moreover, we have demonstrated that the proposed CAE scheme fulfills the requirements of confidentiality, unforgeability, non-repudiation and semantic security.

Table 1. Performance evaluation of the proposed CAE scheme.

Item Phase	**Computational Complexities**
Signature generation	$2T_H + 2T_I + 2T_M + 3T_{EM}$
Signature verification	$2T_H + T_I + T_M + 2T_{EM} + T_{EA} + 2T_B$
Signature conversion	0
Recipient proof	$T_H + T_I + 4T_{EM} + T_{EA} + 2T_B$

References

[1] S. Araki, S. Uehara and K. Imamura, "The limited verifier signature and its application," *IEICE Transactions on Fundamentals*, Vol. E82-A, No. 1, pp. 63-68, 1999.

[2] P.S.L.M. Barreto, H.Y. Kim, B. Lynn and M. Scott, "Efficient algorithms for pairing-based cryptosystems," *Advances in Cryptology – CRYPTO 2002*, Springer-Verlag, pp. 354-368, 2002.

[3] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," *Advances in Cryptology – CRYPTO 2001*, Springer-Verlag, pp. 213-229, 2001.

[4] D. Boneh, B. Lynn and H. Shacham, "Short signature from the Weil pairing," *Advances in Cryptology – ASIACRYPT 2001*, Springer-Verlag, pp. 514-532, 2001.

[5] Y.H. Chen and J.K. Jan, "Enhancement of digital signature with message recovery using self-certified public keys and its variants," *ACM SIGOPS Operating Systems Review*, Vol. 39, No. 3, pp. 90-96, 2005.

[6] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, Vol. IT-22, No. 6, pp. 644-654, 1976.

[7] T. ElGamal, "A public key cryptosystem and a

signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, Vol. IT-31, No. 4, pp. 469-472, 1985.

[8] C. Gentry and A. Silverberg, "Hierarchical id-based cryptography," *Advances in Cryptology – ASIACRYPT 2002*, Springer-Verlag, pp. 548-566, 2002.

[9] P. Horster, M. Michel and H. Peterson, "Authenticated encryption schemes with low communication costs," *Electronics letters*, Vol. 30, No. 15, pp. 1212-1213, 1994.

[10] F. Hou, Z. Wang, Y. Tang and Z. Liu, "Protecting integrity and confidentiality for data communication," *Proceedings of 9th International Symposium on Computers and Communications (ISCC)*, Vol. 1, No. 28, pp. 357-362, 2004.

[11] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, Vol. 48, No. 177, pp. 203-209, 1987.

[12] 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.

[13] A. Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publishers, 1993.

[14] V. Miller, "Use of elliptic curves in cryptography," *Advances in Cryptology, CRYPTO'85*, Springer-Verlag, pp. 417-426, 1985.

[15] Y.Q. Peng, S.Y. Xie, Y.F. Chen, R. Deng and L.X. Peng, "A publicly verifiable authenticated encryption scheme with message linkages," *Proceedings of the 3rd International Conference on Networking and Mobile Computing*, ICCNMC, Zhangjiajie, China, pp. 1271-1276, 2005.

[16] R. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, Vol. 21, No. 2, pp. 120-126, 1978.

[17] N.P. Smart, "Identity-based authenticated key agreement protocols based on Weil Pairings," *Electronics Letters*, Vol. 13, No. 38, pp. 630-632, 2002.

[18] W. Stallings, *Cryptography and Network Security: Principles and Practices*, 4th. Ed., Prentice Hall, 2005.

[19] VISA and MasterCard Inc., *Secure Electronic Transaction (SET) Specification*, Version 1.0, 1997.

[20] T.S. Wu and C.L. Hsu, "Convertible authenticated encryption scheme," *The Journal of Systems and Software*, Vol. 62, No. 3, pp. 205-209, 2002.

[21] T.S. Wu, C.L. Hsu and H.Y. Lin, "Efficient convertible authenticated encryption schemes for smart card applications in network environments," *The 9th World Multi-Conference on Systemics, Cybernetics and Informatics, WMSCI2005*, Orlando, Florida, U.S.A., July 2005.

[22] 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.

[23] T.S. Wu, H.Y. Lin and W.Y. Chang, "Improved Threshold Authenticated Encryption Scheme Based on the Factorization Problem," *2006 International Conference of Digital Technology and Innovation Management*, Taipei, Taiwan, pp. 1699-1709, April 2006.

[24] F. Zhang, and K. Kim, "ID-based blind signature and ring signature from pairings," *Advances in Cryptology – ASIACRYPT 2002*, Springer-Verlag, pp. 533-547, 2002.