ISBN 978-981-11-0008-6
Proceedings of 2016 6th International Workshop on Computer Science and Engineering (WCSE 2016)
Tokyo, Japan, 17-19 June, 2016, pp. 355-358
doi: 10.18178/wcse.2016.06.056

A New Convertible Authenticated Encryption Scheme Based on Bilinear Square Diffie-Hellman Problem

Han-Yu Lin [+]

Department of Computer Science and Engineering, National Taiwan Ocean University, Taiwan

Abstract. Convertible authenticated encryption (CAE) scheme is a cryptographic scheme which has been found numerous practical applications like on-line credit card transactions, confidential contract signing and the protection of digital evidence, etc. In this paper, we propose a new CAE scheme based on the bilinear square Diffie-Hellman problem. The proposed scheme is proved secure against adaptive chosen-plaintext attacks (CPA2) and adaptive chosen-message attacks (CMA) in the random oracle mode. Compared with previous schemes, ours not only provides better functionalities, but also has provable security.

Keywords: convertible, authenticated encryption, digital signature, bilinear pairings, random oracle

1. Introduction

In 1994, Horster *et al*. [1] introduced an authenticated encryption (AE) scheme simultaneously combining the functions of digital signature and public key encryption. That is, the requirements of authenticity and confidentiality [2] are both satisfied. In such a scheme, a signer can produce an authenticated ciphertext while only a designated recipient having the corresponding private key can decrypt it and verify the embedded signature. Yet, when a designated recipient encounters the situation of later repudiation, he cannot convince anyone of signer's dishonesty. To deal with the dispute, in 1999, Araki *et al*. [3] addressed a variant providing an additional arbitration mechanism. However, Zhang and Kim [4] pointed out that Araki *et al*.'s scheme cannot withstand a universal forgery attack.

In 2002, Wu and Hsu [5] came up with a convertible authenticated encryption (CAE) scheme allowing the designated recipient to solely announce a converted signature. The next year, Huang and Chang [6] proposed another enhanced variant. Nevertheless, Lv *et al.* [7] showed that neither the Wu-Hsu nor the Huang-Chang schemes achieve the security requirement of confidentiality. In 2009, Lee *et al*. [8] further introduced the ElGamal-based CAE scheme. In 2012, Lu *et al*. [9] introduced a convertible multi-authenticated encryption scheme for generalized group communications. In 2014, an RSA-based CAE scheme [10] is also addressed. In this paper, we propose a new CAE scheme from bilinear pairing cryptosystems. The proposed scheme is proved secure in the random oracle model.

2. The Proposed Scheme

In this section, we present our proposed scheme from bilinear pairings. The used notations are stated as Table 1. The proposed CAE scheme consists of the following algorithms:

Setup(1^k)**:** On input a security parameter k, the Setup algorithm selects two groups $(\boldsymbol{G}_1, +)$ and $(\boldsymbol{G}_2, \times)$ of the same prime order q. Let P be a generator of order q over $\boldsymbol{G}_1$, e: $\boldsymbol{G}_1 \times \boldsymbol{G}_1 \rightarrow \boldsymbol{G}_2$ a bilinear pairing and h_1: $\{0, 1\}^k \times \boldsymbol{G}_1 \rightarrow Z_q$, h_2: $\boldsymbol{G}_1 \times \boldsymbol{G}_1 \times \boldsymbol{G}_2 \rightarrow \{0, 1\}^k$ and h_3: $\boldsymbol{G}_1 \rightarrow \boldsymbol{G}_1$ collision resistant hash functions. The algorithm outputs public parameters $params = \{\boldsymbol{G}_1, \boldsymbol{G}_2, q, P, e, h_1, h_2, h_3\}$.

[+] Corresponding author. Tel.: +886-2-2462-2192 ext 6656; fax: +886-2-2462-3249.
E-mail address: hanyu@mail.ntou.edu.tw.

Reg_U(i)**:** On input an index i, the Reg_U algorithm chooses a private key $x_i \in Z_q$, computes the public key $Y_i = x_iP$ and then further generates the public key certificate $Cert_i$ by the X.509 standard [11].

TABLE I: THE USED NOTATIONS

$(\boldsymbol{G}_1, +)$	Additive group of prime order q
$(\boldsymbol{G}_2, \times)$	Multiplicative group of prime order q
Z_q^*	multiplicative group of integers modulo q
$x \in Z_q^*$	element x in set Z_q^*
$x \leftarrow Z_q^*$	sampling element x uniformly in set Z_q^*
$\lvert x \rvert$	bit-length of integer x, also absolute value of x
$\oplus$	logical operation XOR
$\Pr[E]$	probability of event E occurring

Sign_M(m, x_s, Y_v)**:** On input a message m, the public key Y_v of the designated recipient and the private key x_s of signer, the algorithm chooses $t \in Z_q^*$ to compute $R = tP$, $\sigma = (x_s + h_1(m, R))^{-1}R$, $W = h_3(tY_v)$, $Z = e(x_sY_v, W)$, $r = m \oplus h_2(R, \sigma, Z)$ and then outputs the authenticated ciphertext $\delta = (R, \sigma, r)$.

Verify_AEC(δ, x_v, Y_s)**:** On input an authenticated ciphertext $\delta = (R, \sigma, r)$, the private key x_v of designated recipient and the public key Y_s of signer, the algorithm first computes $W = h_3(x_vR)$ and $Z = e(x_vY_s, W)$ to recover the message m as $m = r \oplus h_2(R, \sigma, Z)$ and then checks the redundancy embedded in m. The algorithm further verifies the signature by checking whether $e(\sigma, Y_s + h_1(m, R)P) = e(R, P)$. If it holds, the message m and its converted signature $\Omega = (R, \sigma)$ is outputted; else, the error symbol $\perp$ is returned as a result. We prove that the equality works correctly. From the left-hand side of it, we have $e(\sigma, Y_s + h_1(m, R)P) = e((x_s + h_1(m, R))^{-1}R, Y_s + h_1(m, R)P) = e((x_s + h_1(m, R))^{-1}R, (h_1(m, R) + x_s)P) = e(R, P)$ which leads to the right-hand side of it.

3. Security Proof and Comparison

In this section, we first state the underlying security assumption and prove the security of our scheme.

Bilinear Square Diffie-Hellman Problem; BSDHP: Given an instance $(P, A, B) \in \boldsymbol{G}_1$ where P is a generator, $A = aP$ and $B = bP$ for some $a, b \in Z_q^*$, compute $e(P, P)^{a^2b} \in \boldsymbol{G}_2$.

Bilinear Square Diffie-Hellman (BSDH) Assumption: For every probabilistic polynomial-time algorithm $\mathcal{A}$, every positive polynomial $Q(\cdot)$ and all sufficiently large k, $\mathcal{A}$ can solve the BSDHP with the advantage at most $1/Q(k)$, i.e., $\Pr[\mathcal{A}(P, aP, bP) = e(P, P)^{a^2b}; a, b \leftarrow Z_q^*, P, aP, bP \leftarrow \boldsymbol{G}_1] \le 1/Q(k)$. The probability is taken over the uniformly and independently chosen instance and over the random choices of $\mathcal{A}$.

Theorem 1. (Proof of Confidentiality) The proposed CAE scheme is secure against adaptive chosen-plaintext attacks (CPA2) in the random oracle model if there exists no probabilistic polynomial-time adversary that can break the BSDHP with non-negligible advantage.

Proof: Suppose that a probabilistic polynomial-time (PPT) adversary $\mathcal{A}$ can break our scheme with non-negligible advantage ε under the adaptive chosen-plaintext attack after marking at most q_{h_i} h_i (for i = 1 to 3), q_{Reg_U} Reg_U and q_{Sign_M} Sign_M queries. Then we can construct another algorithm $\mathcal{B}$ to obtain $e(P, P)^{a^2b}$ by taking the (P, aP, bP)-BSDHP instance as inputs. In this proof, $\mathcal{B}$ simulates a challenger to $\mathcal{A}$.

Setup: $\mathcal{B}$ runs the Setup(1^k) algorithm and sends public parameters $params = \{\boldsymbol{G}_1, \boldsymbol{G}_2, q, P, e\}$ to $\mathcal{A}$.

Phase 1: $\mathcal{A}$ issues the following kinds of queries adaptively:

- $h_1(m, R)$ *oracle:* $\mathcal{B}$ chooses $v_1 \in_R Z_q$, adds the entry (m, R, v_1) into h_1-list and returns v_1 as a result.
- $h_2(R, \sigma, Z)$ *oracle:* $\mathcal{B}$ first searches the h_2-list for an matched entry; else, $\mathcal{B}$ seeks the form $(R, \sigma, \text{NULL}, v_2)$ and then replaces NULL with Z. Otherwise, $\mathcal{B}$ chooses $v_2 \in_R \{0, 1\}^k$, adds the entry (R, σ, Z, v_2) into h_2-list and returns v_2 as a result.
- $h_3(tY_v)$ *oracle:* $\mathcal{B}$ chooses $v_3 \in_R \boldsymbol{G}_1$ and adds the entry (tY_v, v_3) into h_3-list. Finally, $\mathcal{B}$ returns v_3 as a result.

- *Reg_U query* $\langle i \rangle$*:* If $i = IDs$, $\mathcal{B}$ returns ($Y_s = aP$, $Cert_s$). If $i = IDv$, $\mathcal{B}$ returs ($Y_v = bP$, $Cert_v$). Otherwise, $\mathcal{B}$ runs Reg_U$\langle i \rangle$ and then returns (Y_i, $Cert_i$) to $\mathcal{A}$.
- *Sign_M query* $\langle m, Y_i, Y_j \rangle$*:* If $Y_i \neq aP$, $\mathcal{B}$ returns Sign_M(m, x_i, Y_j). When $Y_i = aP$, $\mathcal{B}$ chooses t, $v_1 \in_R Z_q$ and $v_2 \in_R \{0, 1\}^k$, computes $\sigma = dP$, $r = m \oplus v_2$ and $R = d(aP) + v_1 dP$, adds the entry (m, R, v_1) into h_1-list and the entry (R, σ, NULL, v_2) into h_2-list. Then the ciphertext $\delta = (R, \sigma, r)$ is returned to $\mathcal{A}$.

Challenge: $\mathcal{A}$ generates two messages, m_0 and m_1, of the same length. $\mathcal{B}$ flips a coin $\lambda \leftarrow \{0, 1\}$ and chooses t, $v_1 \in_R Z_q$, $\sigma^* \in_R \boldsymbol{G}_1$ and $v_2 \in_R \{0, 1\}^k$, computes $r^* = m_\lambda \oplus v_2$ and $R^* = tP$ and adds the entry ($t(bP)$, aP) into h_3-list and the entry (R^*, σ^*, NULL, v_2) into h_2-list. The ciphertext $\delta^* = (R^*, \sigma^*, r^*)$ is then delivered to $\mathcal{A}$ as a target challenge. $\mathcal{A}$ can make new queries as those stated in Phase 1.

Output: Finally, $\mathcal{B}$ randomly chooses an entry of h_2-list and outputs Z as a correct answer to the BSDHP.

Analysis of the game: To win the game with a non-negligible advantage, $\mathcal{A}$ might attempt to decrypt the ciphertext $\delta^* = (R^*, \sigma^*, r^*)$ and recover m_λ. Since $\mathcal{B}$ sets $h_3(tY_v) = h_3(x_v R^*) = aP$ and implicitly defines $h_2(R^*, \sigma^*, Z^*) = v_2$ where $Z^* = e(x_v Y_s, W) = e(P, P)^{a^2b}$, $\mathcal{B}$ has a non-negligible advantage to solve the BSDHP on condition that $\mathcal{A}$ makes an $h_2(R^*, \sigma^*, Z^*)$ oracle query in phase 2. The probability that $\mathcal{A}$ guesses the correct random value without asking an h_2 oracle is not greater than 2^{-k}, i.e., the probability that Z^* is in the h_2-list is not less than $(\varepsilon - 2^{-k})$. Since $\mathcal{B}$ randomly chooses an entry from the h_2-list and outputs Z as the answer, we have $\Pr[Z = Z^*] = {q_{h_2}}^{-1}$. Consequently, $\mathcal{B}$ can solve the BSDHP with a non-negligible advantage $({q_{h_2}}^{-1})(\varepsilon - 2^{-k})$ in polynomial-time.

Theorem 2. (Proof of Unforgeability) The proposed CAE scheme is secure against existential forgery on adaptive chosen-message attacks (CMA) in the random oracle model if there exists no probabilistic polynomial-time adversary that can break the BSDHP with non-negligible advantage.

Proof: Suppose that a PPT adversary $\mathcal{A}$ can break the proposed scheme with non-negligible advantage ε under the adaptive chosen-message attack after making at most q_{h_i} h_i (for $i = 1$ to 3), q_{Reg_U} Reg_U and q_{Sign_M} Sign_M queries. Then we can construct another algorithm $\mathcal{B}$ to obtain $e(P, P)^{a^2b}$ by taking the (P, aP, bP)-BSDHP instance as inputs. In this proof, $\mathcal{B}$ simulates a challenger to $\mathcal{A}$.

Setup: $\mathcal{B}$ runs the Setup(1^k) algorithm and sends public parameters $params = \{\boldsymbol{G}_1, \boldsymbol{G}_2, q, P, e\}$ to $\mathcal{A}$.

Phase 1: $\mathcal{A}$ adaptively makes new queries as those defined in Theorem 1. Note that in the j-th $h_3(tY_v)$ oracle query where $j \leq q_{h_3}$, $\mathcal{B}$ directly returns $W_j = aP$.

Forgery: $\mathcal{A}$ outputs a forged authenticated ciphertext $\delta^* = (R^*, \sigma^*, r^*)$ for some m^*.

Output: Finally, $\mathcal{B}$ randomly chooses an entry of h_2-list and outputs Z as a correct answer to the BSDHP.

Analysis of the game: If $\mathcal{A}$ computes Z^* with the j-th result of $h_3(tY_v)$ oracle query, i.e., $Z^* = e(x_s Y_v, W_j) = e(x_s Y_v, aP) = e(P, P)^{a^2b}$ and the forged authenticated ciphertext $\delta^* = (R^*, \sigma^*, r^*)$ is valid, the value Z^* should be kept in some entry of the h_2-list when $\mathcal{A}$ makes an $h_2(R^*, \sigma^*, Z^*)$ oracle query. The probability that $\mathcal{A}$ guesses the correct random value without asking an h_2 oracle is not greater than 2^{-k}, i.e., the probability that Z^* is in the h_2-list is not less than $(\varepsilon - 2^{-k})$. Since $\mathcal{B}$ has set the j-th $h_3(tY_v)$ oracle query to be aP and randomly outputs Z from some entry of the h_2-list as the answer, we obtain $\Pr[Z = Z^*] = 1/q_{h_2}$ and $\Pr[W = W_j] = 1/q_{h_3}$. Therefore, the advantage to solve the BSDHP is $(\varepsilon - 2^{-k})(q_{h_2} q_{h_3})^{-1}$.

We compare the proposed scheme with some previous ones including AUI [3], Sek [12] and WH [5] schemes. Detailed comparisons in terms of functionalities and security are demonstrated as Table 2.

4. Conclusions

CAE schemes have played an important role in e-commerce and the protection of digital evidence, etc. In the literature, we proposed a new CAE scheme based on the bilinear square Diffie-Hellman problem. Unlike previous works which only provide heuristic security proofs, we formally prove that the proposed scheme is secure in the random oracle mode. When a later dispute occurs, the designated recipient can solely reveal the converted signature to convince any third party of the signer's dishonesty. Also, we still preserve the merit that the signature conversion process takes no extra efforts. With better functionalities and the provable security, we claim that the proposed scheme has crucial benefits to practical applications.

TABLE II: COMPARISONS OF THE PROPOSED AND PREVIOUS SCHEMES

Item & Scheme	AUI	Sek	WH	Ours
Non-interactive conversion process	√	√	√	√
Unforgeability/Non-repudiation/No conversion cost	×	×	√	√
Confidentiality & Forward secrecy	√	√	×	√
Provable security	×	×	×	√

5. Acknowledgements

This work was supported in part by the Ministry of Science and Technology of Republic of China under the contract number MOST 104-2221-E-019-018.

6. References

[1] P. Horster, M. Michel and H. Peterson, "Authenticated encryption schemes with low communication costs," *Electronics letters*, 1994, **30** (15): 1212-1213.

[2] W. Stallings, Cryptography and Network Security: Principles and Practices, 4th Ed., Pearson, 2005.

[3] S. Araki, S. Uehara and K. Imamura, "The limited verifier signature and its application," *IEICE Transactions on Fundamentals*, 1999, **E82-A** (1): 63-68.

[4] F. Zhang and K. Kim, "A universal forgery on Araki *et al.*'s convertible limited verifier signature scheme," *IEICE Transactions on Fundamentals*, 2003, **E86-A** (2): 515-516.

[5] T. S. Wu and C. L. Hsu, "Convertible authenticated encryption scheme," *The Journal of Systems and Software*, 2002, **62** (3): 205-209.

[6] H. F. Huang and C. C. Chang, "An efficient convertible authenticated encryption scheme and its variant," *Proceedings of the 5th International Conference on Information and Communications Security (ICICS2003)*, Springer-Verlag, Berlin, 2003, pp. 382-392.

[7] J. Lv, X. Wang and K. Kim, "Practical convertible authenticated encryption schemes using self-certified public keys," *Applied Mathematics and Computation*, 2005, **169** (2): 1285-1297.

[8] C. C. Lee, M. S. Hwang and S. F. Tzeng, "A new convertible authenticated encryption scheme based on the ElGamal cryptosystem," *International Journal of Foundations of Computer Science*, 2009, **20** (2): 351-359.

[9] C. F. Lu, C. L. Hsu and H. Y. Lin, "Provably convertible multi-authenticated encryption scheme for generalized group communications," *Information Sciences*, 2012, **199** (15): 154-166.

[10] T. S. Wu and H. Y. Lin, "Provably secure proxy convertible authenticated encryption scheme based on RSA," *Information Sciences*, 2014, **278** (10): 577-587.

[11] ISO/IEC 9594-8, Information technology – open systems interconnection – the directory: public-key and attribute certificate frameworks, International Organization for Standardization, 2001.

[12] M. R. Sekhar, "Signatures scheme with message recovery and its applications," *International Journal of Computer Mathematics*, 2004, **81** (3): 285-289.