Secure Convertible Authenticated Encryption Scheme Based on RSA

Tzong-Sun Wu
Department of Computer Science and Engineering, National Taiwan Ocean University, Keelung, 202, Taiwan
E-mail: ibox456@gmail.com

Han-Yu Lin
Department of Computer Science, National Chiao Tung University, Hsinchu, 300, Taiwan
E-mail: hanyu.cs94g@nctu.edu.tw

Keywords: authenticated encryption, digital signature, conversion, RSA

Received: November 24, 2008

A convertible authenticated encryption (CAE) scheme is a better way to simultaneously provide cryptographic schemes with the properties of confidentiality, authenticity and non-repudiation. The authors propose a RSA based secure CAE scheme which is different from previously proposed ones based on the discrete logarithms or elliptic curve discrete logarithms. The proposed scheme has the nice arbitration mechanism allowing the designated recipient to convert the authenticated ciphertext into an ordinary signature without any extra computation efforts or communication overheads for the public arbitration. Additionally, the security requirement of confidentiality against adaptive chosen ciphertext attacks (IND-CCA2) and that of unforgeability against existential forgery on adaptive chosen-message attacks (EU-CMA2) are proved in the random oracle model.

Povzetek: Predlagana shema se uporablja za sprotne zaupne transakcije.

1. Introduction

Since Diffie and Hellman [3] proposed the first public key system based on the discrete logarithms, the public key system has been widely applied to many fields. The encryption and the digital signature are two fundamental functions of public key systems. The former ensures the confidentiality while the latter ensures the authenticity and non-repudiation. Yet, some applications, such as the credit card transactions have to simultaneously fulfill the above properties. In 1994, Horster *et al*. [7] proposed an authenticated encryption (AE) scheme to realize the concept of providing digital signature schemes with the confidentiality. An AE scheme allows the signer to produce an authenticated ciphertext such that only the designated recipient has the ability to recover the message and verify its signature. It can be seen that the requirement of confidentiality is achieved in an AE scheme. In addition, it is not necessary to establish a session key between the signer and the designated recipient in advance. However, a later dispute over repudiation might occur, since the authenticated ciphertext is not publicly verifiable. To deal with the problem, in 1999, Araki *et al*. [1] proposed a convertible limited verifier signature scheme with a signature conversion mechanism. To complete the signature conversion process, the signer has to release an extra parameter, which is considered unworkable if the signer refuses to cooperate with. Besides, the computation cost of the conversion is rather high. In 2002, Wu and Hsu [16] proposed a convertible authenticated encryption (CAE) scheme with the efficient signature conversion process. In their scheme, the converted signature is just embedded in the authenticated ciphertext. Therefore, the designated recipient can solely reveal the converted signature in case of a later repudiation. Because the converted signature is derived during the verification process of the authenticated ciphertext, the signature conversion takes no additional computation cost or communication overhead. Since then, several CAE variants were proposed. In 2005, Chen and Jan [2] proposed CAE schemes using self-certified public key system. Later, Peng *et al*. [14] proposed a publicly verifiable authenticated encryption scheme with message linkages for transmitting a large message. Lv *et al*. [11] further proposed practical CAE schemes using self-certified public keys. Next, Wu *et al*. [17] proposed generalized CAE schemes based on elliptic curves [10, 13] for facilitating gradually popular applications like mobile phones and PDAs. In 2008, Wu *et al.* [18] elaborated the merits of CAE and multi-signature schemes [4-6, 8] to propose a convertible multi-authenticated encryption (CMAE) scheme. Nevertheless, these schemes are primarily based on the discrete logarithm problem (DLP) [3] or the elliptic curve discrete logarithm problem (ECDLP) [12] and not applicable to RSA-based systems [15].

1.1. Our Results

In this paper, the authors focus on the solution to confidential transactions of RSA-based systems and propose a secure CAE scheme based on RSA. The signer can generate an authenticated ciphertext and only the designated recipient has the ability to verify it. The proposed scheme is efficient because it is not necessary to establish a session key in advance. The arbitration mechanism enables the recipient to reveal the ordinary signature for the public verification without extra costs, since the converted signature is obtained during the verification process of the authenticated ciphertext. Moreover, the security requirement of confidentiality against adaptive chosen ciphertext attacks (IND-CCA2) and that of unforgeability against existential forgery on adaptive chosen-message attacks (EU-CMA2) are proved in the random oracle model.

2. Preliminaries

In this section, we first define involved parties of a CAE scheme and then review the security notions with respect to RSA cryptosystems [15].

2.1. Involved Parties

A CAE scheme has two involved parties: a signer and a designated recipient. 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 ciphertext. Finally, the designated recipient decrypts the ciphertext and verifies the signature.

2.2. Security Notions

***Definition 1 (RSA Problem)*:**

Let $N = pq$ where p and q are two large primes, e an integer satisfying that $gcd(e, (p - 1)(q - 1)) = 1$ and d an integer such that $ed = 1 \bmod (p - 1)(q - 1)$. Given $c \equiv m^e \pmod N$ as the input, output the integer m satisfying $m \equiv c^d \pmod N$.

***Definition 2 (RSA Assumption)*:**

Let $\boldsymbol{G}$ be the RSA key generator which takes the security parameter 1^k as its input and outputs (N, e, d, p, q). Given a RSA instance (N, e, c), the advantage for any probabilistic polynomial-time (PPT) adversary A, every positive polynomial $P(\cdot)$ and all sufficiently large k to solve the RSA problem is at most $1/P(k)$, i.e.,

$$\Pr[A(N, e, c) = m, c \leftarrow m^e \bmod N, m \leftarrow Z_N, (N, e, d, p, q) \leftarrow \boldsymbol{G}] \le 1/P(k).$$

3. Proposed CAE Scheme Based on RSA

In this section, we propose a CAE scheme based on RSA. The proposed scheme can be divided into three phases: the authenticated ciphertext generation, the message recovery and signature verification, and the signature conversion phases. Initially, each user chooses two large primes p, q, and computes $N = pq$. Next, each user chooses an integer e relatively prime to $(p - 1)(q - 1)$ and computes d satisfying $ed \equiv 1 \pmod{\phi(N)}$ where $\phi(N)$ is the Euler function of N. Here, (N, e) and (p, q, d) are the public and the private keys of each user, respectively. Let h be a secure one-way hash function which accepts two variable-length inputs and generates a fixed-length output of size l. Details of each phase are described below:

***The authenticated ciphertext generation phase*:** For signing the message M, the signer U_S chooses an integer $c \in \{0, 1\}^l$ and computes

$$r = Mc^c \bmod N_V, \quad (1)$$

$$t = c^{e_V} \bmod N_V, \quad (2)$$

$$s = (h(M, c))^{d_S} \bmod N_S, \quad (3)$$

and then deliveries the authenticated ciphertext (s, r, t) to the designated recipient U_V. Note that l is a predefined security parameter to determine the output length of hash function.

***The message recovery and signature verification phase*:** Upon receiving the ciphertext (s, r, t), U_V first computes

$$c = t^{d_V} \bmod N_V. \quad (4)$$

He then recovers the message M as

$$M = rc^{-c} \bmod N_V, \quad (5)$$

and checks the redundancy embedded in M. U_V can further verify (s, r, t) by checking

$$s^{e_S} = h(M, c) \bmod N_S. \quad (6)$$

***The signature conversion phase*:** Since the parameter c is obtained during the verification of the authenticated ciphertext, the recipient can easily reveal the converted signature (s, c) along with the message M in case of a later repudiation. One can see that the conversion process is efficient for that it will not incur extra computation costs or communication overheads. Anyone can perform Eq. (6) to verify the correctness of the converted signature.

4. Security Proof

In this section, we first prove that the security of our proposed scheme is computationally related to RSA. We demonstrate that the proposed CAE scheme is correct and achieves the security requirements of confidentiality, unforgeability and non-repudiation. Then we evaluate the performance of our scheme and compare it with some previous works.

4.1. Security Proof

Correctness. A CAE scheme is correct if the signer can generate a valid authenticated ciphertext and only the designated recipient is capable of decrypting and verifying it. We prove the correctness of our proposed scheme as Theorems 1 and 2.

Theorem 1. *The designated recipient U_v can correctly recover the message M with embedded redundancy by Eq. (5).*

Proof: From the right-hand side of Eq. (5), we have

$$
\begin{aligned}
& rc^{-c} \\
&= (Mc^{c})c^{-c} && \text{(by Eq. (1))} \\
&= M \pmod{N_v}
\end{aligned}
$$

which leads to the left-hand side of Eq. (5).

Q.E.D.

Theorem 2. *The designated recipient U_v can correctly verify the signature (s, c) with Eq. (6).*

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

$$
\begin{aligned}
& h(M,c) \\
&= h(M,c)^{d_s \cdot e_s} \\
&= s^{e_s} \pmod{N_s} && \text{(by Eq. (3))}
\end{aligned}
$$

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

Q.E.D.

Message Confidentiality. A CAE scheme satisfies the security requirement of message confidentiality if the resulted authenticated ciphertext is computationally indistinguishable even with respect to two candidate plaintexts. We prove that the proposed scheme achieves the IND-CCA2 security as Theorem 3. The proof idea is a security reduction from the RSA problem to the adaptive chosen ciphertext attacks against our proposed scheme in the random oracle model. Let t_λ be the average running time of one oracle-query in the following proof.

Theorem 3. *The proposed CAE scheme is $(t', q_h, q_{\mathrm{sig}}, q_{\mathrm{ver}}, \varepsilon')$-secure against adaptive chosen ciphertext attacks in the random oracle model if there exists no probabilistic polynomial-time algorithm B that can (t, ε)-break the RSA problem, where*

$$\varepsilon \geq (1/q_h)(1 - q_{\mathrm{ver}}q_h 2^{-l})\varepsilon', \tag{7}$$

$$t < t' + t_\lambda(q_h + q_{\mathrm{sig}} + q_{\mathrm{ver}}). \tag{8}$$

Proof: Suppose that A is a $(t', q_h, q_{\mathrm{sig}}, q_{\mathrm{ver}}, \varepsilon')$-PPTM that breaks the proposed CAE scheme with the chosen ciphertext attack, where t' denotes the running time, q_h the times of h-oracle queries, q_{sig} the times of authenticated ciphertext oracle queries, q_{ver} the times of signature verification oracle queries and ε' the probability that A succeeds. We will take A as a subroutine to construct a (t, ε)-algorithm B that solves the RSA problem with respect to the designated recipient's key pair in time t with the probability ε. The algorithm B is said to (t, ε)-break the RSA problem. Let U_v be the designated recipient with the key par (N_v, e_v) and (p_v, q_v, d_v). The objective of B is to obtain α ($\equiv b^{d_v} \pmod{N_v}$) by taking (N_v, e_v) and $b \in Z_{N_v}$ as inputs. In this proof, B simulates a challenger to A in the following game.

Phase 1: A issues the following kinds of queries adaptively:

–h-oracle query: When A issues a h-oracle query of $h(M, c)$, B first randomly chooses $a \in \{0, 1\}^l$, and computes $u \equiv a^{e_s} \pmod{N_s}$. B then keeps (M, c, a, u) in a hash oracle query table and returns u as a result.

– Authenticated-ciphertext-oracle query: When A issues a authenticated ciphertext oracle query of a message M, B randomly chooses $c \in \{0, 1\}^l$ to compute

$$r = Mc^{c} \bmod N_v,$$

$$t = c^{e_v} \bmod N_v.$$

B then checks whether $h(M, c)$ has been queried in the hash oracle query table. If it has not, B randomly chooses $a \in \{0, 1\}^l$ to compute $u \equiv a^{e_s} \pmod{N_s}$, writes (M, c, a, u) into the hash oracle query table and sets $s = a \bmod N_s$; else, B finds the corresponding a and sets $s = a \bmod N_s$. Finally, B returns the ciphertext (s, r, t) as the result of authenticated-ciphertext-oracle query for M.

– Signature-verification-oracle query: When A submits an authenticated ciphertext $\delta = (s, r, t)$, B searches the hash oracle query table of (M, c, a, u)'s. If one of them satisfies $s = a$ and $M = rc^{-c} \bmod N_v$, B outputs M. Otherwise, the □ symbol is returned as a result to signal that the authenticated ciphertext is invalid.

Challenge: The PPTM A generates two messages, M_0 and M_1, of the same length. The challenger B flips a coin $\lambda \leftarrow \{0, 1\}$ and generates an authenticated ciphertext $\delta^* = (s^*, r^*, t^*)$ where $t^* = b \pmod{N_v}$ and (s^*, r^*) are randomly selected strings from some appropriate space.

Phase 2: A issues new queries as those stated in Phase 1. It is not allowed to make a signature-verification-oracle query for the target challenge δ^*.

Guess: A outputs a bit λ' as the result. If $\lambda' = \lambda$, A wins this game. We define A's advantage as $Adv(A) = \Pr[\lambda' = \lambda] - 1/2$.

Output: Finally, B randomly picks c from an entry (M, c, a, u) of the hash oracle query table and outputs it as the solution to $b^{d_v} \pmod{N_v}$. The probability of outputting a correct answer and the running time are bounded by the inequalities of Eqs. (7) and (8).

Analysis of the game: If A guesses correctly, i.e., $\lambda' = \lambda$, it has to compute

$$\alpha = t^{d_v} \bmod N_v,$$

and query $h(M_\lambda, \alpha)$ for checking whether

$$s^{*e_s} = h(M_\lambda, \alpha) \bmod N_s$$

holds or not. Then an entry $(M_\lambda, \alpha, a_i, u_i)$ should be recorded in the hash oracle query table for some a_i and u_i. It can be seen that the distribution of the PPTM A's view in the simulation is identical to that A is playing in a real CAE scheme except the failure of signature-verification-oracle queries for some valid authenticated ciphertexts. Since there are at most q_h queries, the probability of rejecting a valid authenticated ciphertext is not greater than $q_h 2^{-l}$. In addition, A makes at most q_{ver} signautre-verification-oracle queries and β randomly chooses c from one of at most total q_h entries in the hash oracle query table. We can express the probability ε as $\varepsilon \geq (1/q_h)(1 - q_{\text{ver}} q_h 2^{-l})\varepsilon'$ which implies Eq. (7). The running time t of B is that of all oracle queries along with that of the PPTM A. Consequently, we obtain $t < t' + t_\lambda(q_h + q_{\text{sig}} + q_{\text{ver}})$ which implies Eq. (8).

Q.E.D.

Unforgeability. A signature scheme fulfills the security requirement of unforgeability if it is secure against adaptive chosen-message attacks. The security of unforgeability against existential forgery on adaptive chosen-message attacks (EU-CMA2) is proved in the random oracle model as Theorem 4. The proof concept of Theorem 4 is a security reduction from the RSA problem to the existential forgery attack against our proposed scheme in the random oracle model. Let t_λ be the average running time of one oracle-query in the following proof.

Theorem 4. *The proposed CAE scheme is* $(t', q_h, q_{\text{sig}}, \varepsilon')$*-secure against existential forgery on adaptive chosen-message attack in the Random Oracle model if there exists no polynomial-time algorithm* B *that can* (t, ε)*-break the RSA problem, where*

$$\varepsilon \geq (1/q_h)\varepsilon', \tag{9}$$

$$t < t' + t_\lambda(q_h + q_{\text{sig}}). \tag{10}$$

Proof: Suppose that A is a PPTM that can $(t', q_h, q_{\text{sig}}, \varepsilon')$-break the proposed scheme with the existential forgery attack, where t' denotes the running time, q_h the times of h-oracle queries, q_{sig} the times of authenticated-ciphertext-oracle queries and ε' the probability that A succeeds. We will take A as a subroutine to construct a (t, ε)-algorithm B that solves the RSA problem with respect to the signer's key pair in time t with the probability ε. Let U_s be the signer with the key par (N_s, e_s) and (p_s, q_s, d_s). The objective of B is to derive α ($\equiv b^{d_s} (\text{mod} N_s)$) by taking (N_s, e_s) and $b \in Z_{N_s}$ as inputs. In this proof, B simulates a challenger to A in the following game.

Phase 1: A issues h-oracle and authenticated-ciphertext-oracle queries as those defined in Theorem 3 adaptively.

Challenge: The challenger B randomly chooses a message M^* for A to forge a signature.

Phase 2: A issues new queries as those stated in Phase 1. It is not allowed to make an authenticated ciphertext oracle query for the target challenge M^*. When A issues a h-oracle query of $h(M, c)$ with $M = M^*$ for the first time, B directly outputs b. Otherwise, B follows the same procedures as stated in Phase 1.

Response of forgery: A outputs a valid authenticated ciphertext (s, r, t) for M^* with the probability ε'.

Output: B outputs s as the solution to $b^{d_s} (\text{mod} N_s)$. The probability of outputting a correct answer and the running time are bounded by the inequalities of Eqs. (9) and (10).

Analysis of the game: Consider the case when $s \equiv \alpha$ (mod N_s), and then B has successfully computed α ($\equiv b^{d_s} (\text{mod} N_s)$). It can be seen that the distribution of the PPTM A's view in the simulation is identical to that A is playing in a real CAE scheme. Besides, B has answered one of total q_h h-oracles A queried with the value b which will lead to the forged authenticated ciphertext (s, r, t) with $s \equiv \alpha$ (mod N_s). Consequently, the success probability ε to solve the RSA problem for B can be further expressed as $\varepsilon \geq (1/q_h)\varepsilon'$ which implies Eq. (9). The running time t of B is that of all oracle queries along with that of the PPTM A. Therefore, we can express it as $t < t' + t_\lambda(q_h + q_{\text{sig}})$ which implies Eq. (10).

Q.E.D.

According to Theorem 4, the proposed scheme is secure against existential forgery attacks. That is, the signature key can not be forged and the signer can not repudiate having generated his signatures. Hence, we obtain the following corollary.

Corollary 1. *The proposed CAE scheme satisfies the security requirement of non-repudiation.*

4.2. Performance and Comparison

For facilitating the reader with the following performance evaluation, we first define some used notations:

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

T_e: the time for performing a modular exponentiation computation;

T_m: the time for performing a modular multiplication computation;

T_i: the time for performing a modular inverse computation;

Note that the time for performing modular addition and modular subtraction is ignored because it is negligible as compared to those of performing other computations. The detailed evaluation of our proposed scheme in terms of computational costs is shown as Tables 1.

Phase	Computational costs
Authenticated ciphertext generation	$3T_e + T_m + T_h$
Message recovery and signature verification	$3T_e + T_m + T_i + T_h$
Signature conversion	0

Table 1: Performance evaluation of proposed scheme.

We compare the proposed scheme with some previous works including the Wu-Hsu scheme [16] (WH for short), Lv *et al.*'s [11] (LWK for short), Araki *et al.*'s scheme [1] (AUI for short) and Huang *et al.*'s [9] (HLL for short). Detailed comparisons in terms of the security and functionalities are demonstrated as Table 2. To the best of our knowledge, the proposed scheme is the first provably secure one based on RSA assumption.

Scheme Item	WH	LWK	AUI	HLL (2)	Ours
No conversion cost	O	O	×	O	O
Security assumption	DLP	DLP	DLP	RSA	RSA
Confidentiality	N.A.	-	-	N.A.	IND-CCA2
Unforgeability	- (1)	-	N.A.	N.A.	EU-CMA2

Table 2: Comparisons of proposed and other schemes.

Remarks: (1) It is unknown that what security level with respect to the evaluated item the scheme can achieve, since it provides no formal proofs.

(2). To obtain fair comparison results, we assume that only one signer is involved and responsible for generating the authenticated ciphertext.

5. Conclusions

In this paper, the authors proposed a secure CAE scheme based on RSA as a solution to confidential transactions of RSA-based systems. The proposed scheme allows the signer to produce an authenticated ciphertext and only the designated recipient can recover the message and verify the signature for ensuring the confidentiality. The arbitration mechanism provides the designated recipient with the ability to solely reveal the ordinary signature for the public verification. It can be seen that the signature conversion process is rather simple and efficient for that the converted signature is obtained during the verification process of the authenticated ciphertext. That is, the conversion process takes no extra computation efforts or communication overheads. Moreover, the security requirement of confidentiality against adaptive chosen ciphertext attacks (IND-CCA2) and that of unforgeability against existential forgery on adaptive chosen-message attacks (EU-CMA2) are proved in the random oracle model.

References

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

[2] 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*, 2005, **39**(3): 90-96.

[3] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, 1976, **IT-22**(6): 644-654.

[4] L. Harn, "Group-oriented (t, n) threshold digital signature scheme and digital multisignature," *IEE Proceedings - Computers and Digital Techniques*, 1994, **141**(5): 307-313.

[5] L. Harn and T. Kiesler, "New scheme for digital multisignature," *Electronics Letters*, 1989, **25**(15): 1002-1003.

[6] L. Harn, C.Y. Lin and T.C. Wu, "Structured multisignature algorithms," *IEE Proceedings - Computers and Digital Techniques*, 2004, **151**(3): 231-234.

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

[8] C.L. Hsu, T.S. Wu and T.C. Wu, "New nonrepudiable threshold proxy signature scheme with known signers," *The Journal of Systems and Software*, 2001, 58(2): 119-124.

[9] C.H. Huang, C.Y. Lee, C.H. Lin, C.C. Chang and K.L. Chen, "Authenticated encryption schemes with message linkage for threshold signatures," *Proceedings of the IEEE 19th International Conference on Advanced Information Networking and Applications*, Vol. 2, 2005, pp. 261-264.

[10] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, 1987, **48**(177): 203-209.

[11] 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.

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

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

[14] 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 Third International Conference on Networking and Mobile Computing*, ICCNMC, Zhangjiajie, China, 2005, pp. 1271-1276.

[15] R. Rivest, A. Shamir and L. Adleman, "A method

for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, 1978, **21**(2): 120-126.

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

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

[18] T.S. Wu, C.L. Hsu, K.Y. Tsai, H.Y. Lin and T.C. Wu, "Convertible multi-authenticated encryption scheme," *Information Sciences*, 2008, **178**(1): 256-263.