A Novel Convertible Authenticated Encryption Scheme based on RSA Assumption

R. Arshad¹ and N.Ikram¹

¹Department of Computer Science, National University of Science and Technology, Pakistan
raziarhad@hotmail.com, nassar@nust.edu.pk

Abstract: An authenticated encryption allows the specific recipient to verify the authenticity while recovering the message. To protect the recipient’s interest in case of a later dispute, a convertible authenticated encryption scheme allows the specific recipient to retrieve an authenticated cipher text and convert the authenticated ciphertext into an ordinary signature so that it becomes publicly verifiable. In this paper, we propose a novel and secure convertible authenticated encryption scheme based on RSA assumption. The proposed scheme allows the specific recipient to convert the authenticated ciphertext into an ordinary signature without extra computation efforts or communication overheads. To analyze the security of our proposed scheme, we use the techniques from provable security.

Keywords: Authenticated encryption, discrete logarithm, security, RSA.

1. Introduction

In 1976, Diffie and Hellman [1] proposed the first public key cryptosystem based on discrete logarithm problem. The public key cryptosystem has been widely applied to many fields. The encryption and signatures are the main functions of public key cryptosystem. The former ensures confidentiality while the latter ensures authenticity and non-repudiation. Yet, some applications, such as the credit card transactions have to simultaneously fulfill the above properties.Authenticated encryption schemes are designed to satisfy such requirements. It allows a signer to generate an authenticated ciphertext and then send it to a specific recipient; only the specific recipient decrypts the signed message and verifies the corresponding signature. Therefore, the authenticated encryption scheme can be regarded as the combination of digital signature scheme and data encryption scheme. In 1994, Nyberg and Rueppel [3] introduced the digital signatures scheme with message recovery. Later, Horster et al. [4] proposed an authenticated encryption scheme modified from the Nyberg–Rueppel scheme. In comparison with the straightforward approach of employing an encryption scheme and a signature scheme on a message separately, the authenticated encryption scheme requires smaller bandwidth of data communications for achieving authentication, confidentiality and non-repudiation. Afterwards, many similar schemes have been proposed [11]-[17].

In authenticated encryption scheme, only the specific recipient can be convinced of the signer’s signature, so if the signer repudiates his/her signature later, the specific recipient cannot prove the dishonesty of the signer to any verifier without releasing his/her secret. To overcome this weakness, in 1999, Araki et al. [5] proposed a convertible limited verifier scheme in which a specific recipient converts the signature into an ordinary one so that any verifier can verify its validity but when the specific recipient converts the signature, he/she needs the cooperation of the signer. In case of an unwilling signer, this is not realizable. Later, in 2002, Wu and Hsu [6] proposed a new convertible authentication encryption scheme. The specific recipient can easily produce the ordinary signature without the help of the signer, and if the signer wants to repudiate his/her signature, he/she can reveal the converted signature and then any verifier can prove the dishonesty of the signer. Unfortunately, in 2003, Huang and Chang [7] showed that the Hsu et al.’s scheme does not consider the problem that once an intruder knows the desired message, then he/she can also convert a signature easily into an ordinary signature and claim that the signature is sent to him. Finally, they proposed a new convertible authenticated encryption scheme to solve this problem.

In 2005, Lv et al. [8] showed that neither the Hsu et al.’s scheme nor the Huang et al.’s scheme can provide semantic security for messages. That is, after getting a valid signature, any adversary can determine whether his/her guessed message is the actual message signed by the original signer. Then, Lv et al. proposed a new convertible authenticated encryption scheme using self-certified public keys and extended it to one with message linkages when the signed message is large. Each scheme provides semantic security of messages. Lv et al.’s scheme cannot provide confidentiality either since the verifier can recover messages if given many triples of messages, signatures and ciphertext in the basic convertible authenticated encryption scheme. In 2008, Wu et al. [9] elaborated the merits of convertible authenticated encryption and multi-signature schemes [10] to propose a convertible multi-authenticated encryption scheme. Nevertheless, these schemes are primarily based on the Discrete Logarithm Problem (DLP) [1] or the Elliptic Curve Discrete Logarithm Problem (ECDLP) [18] and not applicable to RSA-based cryptosystems [2].

In order to find the solution of confidential transactions of RSA-based cryptosystems, we propose a novel and secure convertible authenticated encryption scheme based on RSA assumption in which a signer can generate an authenticated ciphertext and only the specific recipient has the ability to verify it. The proposed convertible authenticated encryption scheme is efficient because it is not necessary to establish a
2. Preliminaries

Before introducing our proposed convertible authenticated encryption scheme, in this section, we first briefly review the RSA problem [2].

2.1 RSA Problem

Let \( n = pq \) be the product of two large primes \( p \) and \( q \), \( e, d \) be the two integers such that \( ed \equiv 1 \pmod{\phi(n)} \), where \( \phi(n) = (p-1)(q-1) \) is Euler-phi function.

Given \( n, e, y \in \mathbb{Z}_n^* \), compute the modular \( e^h \) root \( x \) of \( y \) such that \( x^e \equiv y \pmod{n} \). We define by \( \text{Succ}_{\text{RSA}}^n(A) \) the success probability of an algorithm \( A \) in solving the RSA problem as
\[
\text{Succ}_{\text{RSA}}^n(A) = \Pr[A(n, e, y = x^e \pmod{n}) = x \in \mathbb{Z}_n^*]
\]
We say that \( \text{RSA} \) assumption holds if \( \text{Succ}_{\text{RSA}}^n(A) \) is negligible for any probabilistic polynomial time adversary \( A \).

3. Proposed Convertible Authenticated Encryption Scheme

In this section, we propose a novel and secure convertible authentication encryption scheme based on RSA assumption. In our proposed scheme, there are two participants: a signer \( S \) and a specific recipient \( R \). Each is a probabilistic Turing machine that runs in polynomial time in the security parameter.

Our proposed scheme can be divided into four phases: the key generation, the authenticated ciphertext generation, the message recovery and signature verification, and the signature conversion phases. Details of each phase are listed below.

The key generation phase

In key generation phase, each user chooses two large primes \( p \) and \( q \) of similar size, and computes \( n = pq \). Next, each user chooses an integer \( e \) relatively prime to \( \phi(n) \) 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 \( l \).

The authenticated ciphertext generation phase

For signing the message \( M \), \( S \) chooses an integer \( k \in \mathbb{Z}_{\phi(n)}^* \) and computes
\[
\begin{align*}
v &= (Mk)^{\phi(n)} \pmod{n_R} \\
w &= (k)^{\phi(n)} \pmod{n_R} \\
s &= (h(M,k))^{d_s} \pmod{n_S}
\end{align*}
\]
and then delivers the authenticated ciphertext \((v, w, s)\) to \( R \).

Note that \( l \) is a pre-defined security parameter to determine the output length of hash function.

The message recovery and signature verification phase

Upon receiving the ciphertext \((v, w, s)\), \( R \) uses his/her private key \( d_R \) to compute
\[
k = (w)^{d_s} \pmod{n_R}
\]
He then recovers the message \( M \) as
\[
M = v^{d_S}k^{-1} \pmod{n_R}
\]
and checks the redundancy embedded in \( M \). \( R \) can further verify \((v, w, s)\), by checking
\[
s^{d_S} = h(M, k) \pmod{n_S}
\]

The signature conversion phase

Since the parameter \( k \) is obtained during the verification of the authenticated ciphertext, the recipient can reveal easily the converted signature \((s, k)\) 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 Analysis

In this section, we first prove that the security of our proposed convertible authenticated encryption scheme is computationally related to RSA assumption. We demonstrate that the proposed convertible authenticated encryption 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 convertible authenticated encryption scheme is correct if the signer can generate a valid authenticated ciphertext and the specific recipient only is capable of decrypting and verifying it. We prove the correctness of our proposed scheme as Theorems 1 and 2.

**Theorem 1:** The specific recipient \( R \) can correctly recover the message \( M \) with embedded redundancy by Eq. (5).

**Proof:** From the right-hand side of Eq. (5), we have
\[
\begin{align*}
v^{d_s}k^{-1} & \pmod{n_R} \\
& = ((Mk)^{\phi(n)})^{d_s}k^{-1} \pmod{n_R}
\end{align*}
\]
A Novel Convertible Authenticated Encryption Scheme based on RSA Assumption

Theorem 2: The specific recipient R can correctly verify the signature (s, k) with Eq. (6).

Proof: From the right-hand side of Eq. (6), we have
\[ h(M, k) = h(M, k)^{k_{\text{sig}}} = s^{\alpha}(\mod n_{\text{s}}) \]
this leads to the left-hand side of Eq. (6).

Theorem 3: The proposed convertible authenticated encryption scheme is secure against adaptive chosen ciphertext attacks in the random oracle model if there exists no probabilistic polynomial-time algorithm B that can (t, \epsilon) break the RSA problem, where
\[ \epsilon \geq \frac{1}{q_h}(1 - q_{\text{sig}}- q_{\text{ver}}2^{-\lambda}) \epsilon' \]  \hspace{1cm} (7)
\[ t < t' + t_r(q_h + q_{\text{sig}} + q_{\text{ver}}) \]  \hspace{1cm} (8)

Proof: Suppose that \( \text{Adv} (= \text{Pr}[t' = t], \text{Adv}) \) is playing in a real Turing machine that breaks the proposed convertible authenticated encryption scheme with the given ciphertext attack, where \( t' \) denotes the running time, \( q_{\text{h}} \) the times of \( h \)-oracle queries, \( q_{\text{sig}} \) the times of authenticated ciphertext oracle queries, \( q_{\text{ver}} \) the times of signature verification oracle queries and \( \epsilon' \) the probability that \( \text{Adv} \) succeeds. We will take \( \text{Adv} \) as a subroutine to construct a \((t, \epsilon)\) algorithm \( B \) that solves the RSA problem with respect to the designated recipient’s key pair in time \( t \) with the probability \( \epsilon \). The algorithm \( B \) is said to \((t, \epsilon)\) break the RSA problem. Let \( R \) be the specific recipient with the key pair \((n_\text{R}, eR)\) and \((pR, qR, dR)\). The objective of \( B \) is to obtain \( \alpha = \beta^{dR}(\mod n_\text{R}) \) by taking \((n_\text{R}, eR)\) and \( b \in \mathbb{Z}^{*}_{n_{\text{R}}} \) as inputs. In this proof, \( B \) simulates a challenger to \( \text{Adv} \) in the following game.

Game phase 1: \( \text{Adv} \) issues the following kinds of queries adaptively:

- \( h \)-oracle query: When \( \text{Adv} \) issues a \( h \)-oracle query of \( h(M, k) \), \( B \) first randomly chooses \( c \in \mathbb{Z}^{*}_{n_{\text{R}}} \), and computes \( u = c^{\alpha}(\mod n_{\text{R}}) \). Then \( B \) keeps \((M, k, c, u)\) in a hash oracle query table and returns \( u \) as a result.
- Authenticated-ciphertext-oracle query: When \( \text{Adv} \) issues a ciphertext query \((v, w, s)\), \( B \) searches the hash oracle query table of \((M, k, c, u)\)’s. If one of them satisfies \( s = c \) and \((M, k, c, u)\), \( B \) outputs \( \alpha \). Otherwise, \( \text{Adv} \) wins this game. 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 \( \text{Adv} \) guesses correctly, i.e., \( t' = t \) it has to compute \( \alpha = w^{\beta}(\mod n_{\text{R}}) \) and query \( h(M, \alpha) \) for checking whether \( s^{\alpha} = b^{\alpha}(\mod n_{\text{R}}) \) holds or not. Then an entry \((M, \alpha, c_i, u_i)\) should be recorded in the hash oracle query table for some \( c_i \) and \( u_i \). It can be seen that the distribution of the probabilistic Turing machine \( \text{Adv} \)’s view in the simulation is identical to that \( \text{Adv} \) is playing in a real convertible authenticated encryption scheme except the failure of signature-verification-oracle queries for some valid authenticated ciphertexts. Since there are at most \( q_{\text{ver}} \) queries, the probability of rejecting a valid authenticated ciphertext is not greater than \( q_{\text{ver}} 2^{-\lambda} \). In addition, \( \text{Adv} \) makes at most \( q_{\text{ver}} \) queries.
signature-verification oracle queries and \( B \) randomly chooses \( k \) from one of at most total \( q_h \) entries in the hash oracle query table. We can express the probability \( \varepsilon \) as
\[
\varepsilon \geq \left( \frac{1}{q_h} \right) (1 - q_{\text{ver}} q_h^{-1}) \varepsilon' \quad \text{which implies Eq. (7)}.
\]
The running time \( t \) of \( B \) is that of all oracle queries along with that of the probabilistic Turing machine \( \mathcal{A} \). Consequently, we obtain
\[
t < t' + t_e(q_h + q_{\text{sig}} + q_{\text{ver}}) \quad \text{which implies Eq. (8)}.
\]

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 (EF-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 \( t_e \) be the average running time of one oracle-query in the following proof.

**Theorem 4:** The proposed convertible authenticated encryption 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 \((t, \varepsilon)\) break the RSA problem, where
\[
\varepsilon \geq \left( \frac{1}{q_h} \right) \varepsilon' \quad \text{(9)}
\]
\[
t < t' + t_e(q_h + q_{\text{sig}}) \quad \text{(10)}
\]

**Proof:** Suppose that \( \mathcal{A} \) is a probabilistic Turing machine 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, \( q_{\text{sig}} \) the times of authenticated-ciphertext-oracle queries and \( \varepsilon' \) the probability that \( \mathcal{A} \) succeeds. We will take \( \mathcal{A} \) as a subroutine to construct a \((t, \varepsilon)\) algorithm \( B \) that solves the RSA problem with respect to the signer’s key pair in time \( t \) with the probability \( \varepsilon \). Let \( S \) be the signer with the key pair \((n_S, e_S)\) and \((p_S, q_S, d_S)\). The objective of \( B \) is to derive \( \alpha(= b^{d_S} \mod n_S) \) by taking \((n_S, e_S)\) and \( b \in Z_n \) as inputs. In this proof, \( B \) simulates a challenger to \( \mathcal{A} \) in the following game.

**Game phase 1:** \( \mathcal{A} \) 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 \( \mathcal{A} \) to forge a signature.

**Game phase 2:** \( \mathcal{A} \) issues new queries as those stated in game phase 1. It is not allowed to make an authenticated ciphertext oracle query for the target challenge \( M^* \). When \( \mathcal{A} \) issues a \( h \)– oracle query of \( h(M,k) \) with \( M = M^* \) for the first time, \( B \) directly outputs \( b \). Otherwise, \( B \) follows the same procedures as stated in game phase 1.

**Response of forgery:** \( \mathcal{A} \) outputs a valid authenticated ciphertext \((v, w, s)\) for \( M^* \) with the probability \( \varepsilon' \).

**Output:** \( B \) outputs \( s \) as the solution to \( b^{d_S} \mod n_S \). 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 \( s = \alpha(\mod n_S) \), and then \( B \) has successfully computed \( \alpha(= b^{d_S} \mod n_S) \). It can be seen that the distribution of the probabilistic Turing machine \( \mathcal{A} \)’s view in the simulation is identical to that \( \mathcal{A} \) is playing in a real convertible authenticated encryption scheme. Besides, \( B \) has answered one of total \( q_h \) \( h \)-oracles \( \mathcal{A} \) queried with the value \( b \) which will lead to the forged authenticated ciphertext \((v, w, s)\) with \( s = \alpha(\mod n_S) \). Consequently, the success probability \( \varepsilon \) to solve the RSA problem for \( B \) can be further expressed as \( \varepsilon \geq \left( \frac{1}{q_h} \right) \varepsilon' \) which implies Eq. (9). The running time \( t \) of \( B \) is that of all oracle queries along with that of the probabilistic Turing machine \( \mathcal{A} \). Therefore, we can express it as \( t < t' + t_e(q_h + q_{\text{sig}}) \) which implies Eq. (10).

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

**Corollary 1:** The proposed convertible authenticated encryption scheme satisfies the security requirement of non-repudiation.

**4.2. Performance comparison**

For the 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 Table 1.

In order to obtain fair comparison results, we assume that only one signer is involved and responsible for generating the authenticated ciphertext. We compare the proposed scheme with some previous works including the Wu-Hsu’s scheme [6], Lv et al.’s [8], Araki et al.’s scheme [5] and Huang et al.’s [7]. Detailed comparisons in terms of security and functionalities are demonstrated as Table 2. To the best of our knowledge, the proposed scheme is the first provable secure convertible authenticated encryption scheme based on RSA assumption.
In this paper, we have proposed a novel and secure convertible authenticated encryption scheme based on RSA assumption as a solution to confidential transactions of RSA-based cryptosystems. The proposed scheme allows the signer to produce an authenticated ciphertext and the specific recipient only can recover the message and verifies the signature for ensuring the confidentiality. The specific recipient also reveals the ordinary signature for the public verification. It can be seen that the signature conversion process is rather simple and efficient, that is, the conversion process takes no extra computation efforts or communication overheads. Moreover, we analyze the security of our proposed scheme by using the techniques from provable security.

5. Conclusions

In this paper, we have proposed a novel and secure convertible authenticated encryption scheme based on RSA assumption as a solution to confidential transactions of RSA-based cryptosystems. The proposed scheme allows the signer to produce an authenticated ciphertext and the specific recipient only can recover the message and verifies the signature for ensuring the confidentiality. The specific recipient also reveals the ordinary signature for the public verification. It can be seen that the signature conversion process is rather simple and efficient, that is, the conversion process takes no extra computation efforts or communication overheads. Moreover, we analyze the security of our proposed scheme by using the techniques from provable security.

References


Author Biographies

R. Arshad graduated in Mathematics and Computer Science from Quaid-i-Azam University, Islamabad, Pakistan and International Islamic University, Islamabad, Pakistan in 2001 and 2004 respectively. He received his M.Sc. in Information Security from Sichuan University, Chengdu, China in 2007. He is currently research associate at National University of Sciences and Technology (NUST), Pakistan. His current research interests include network security and cryptography.

N. Ikram graduated in Electrical Engineering from NED, Karachi, Pakistan in 1987. He received his M.Sc. in Military Electronics and Systems Engineering from Royal Military College of Sciences, Shrivenham, Cranfield University, UK in 1995 and PhD in information Security from Bradford University, UK in 1999. He is currently Professor at National University of Sciences and Technology (NUST), Pakistan. His current research interests include network security and cryptography.