INFORMATICA, 2006, Vol. 17, No. 4, 577–586

Cryptanalysis and Improvement of Practical Convertible Authenticated Encryption Schemes Using Self-Certified Public Keys

Zuhua SHAO
Department of Computer and Electronic Engineering
Zhejiang University of Science and Technology
No. 85, XueYuan Road, Hangzhou, Zhejiang, P.R. of China, 310012
e-mail: zhshao_98@yahoo.com

Received: March 2006

Abstract. A convertible authenticated encryption scheme allows a specified recipient to recover and verify a message simultaneously. Moreover the recipient can prove the dishonesty of the sender to any third party if the sender repudiates her signature later. Recently, Lv *et al.* (2005) showed that the Wu *et al.*'s (1999) and the Huang *et al.*'s (2003) convertible authenticated encryption schemes cannot provide the semantic security of encrypted messages. Then they proposed a practical convertible authenticated encryption scheme using self-certified public keys, and extended it to one with message linkages when the signed message is large. In this paper, we show that the verifier can recover messages if given many triples of message, signature and ciphertext in the Lv *et al.*'s basic convertible authenticated encryption scheme. Finally we propose a new improvement to these schemes to overcome this weakness and to improve its efficiency.

Key words: public key cryptology, authenticated encryption scheme, self-certified public key, message linkages.

1. Introduction

Convertible Authenticated Encryption. A digital signature is analogous to an ordinary hand-written signature, which is an evidence of possession of an electronic document. A digital signature scheme allows a signer to generate a value on a message m, which depends on m and on the signer's public key and private key in such a way that anyone can check validity just by using the public key. Moreover, using digital signatures with message recovery introduced by Nyberg and Rueppel (1994) is more important for many small message applications, the aim of which is to enable a signer to send a signature for a message to a verifier. After receiving the signature, the verifier can recover and verify the message from the signature. Later, Horster *et al.* (1994) proposed an authenticated encryption scheme modified from the Nyberg–Rueppel scheme. In an authenticated encryption scheme, the signer may generate the signature for a message and then send it to a specified recipient, and only the specified recipient can recover and verify the message. Therefore, the authenticated encryption scheme can be regarded as the combination of data encryption schemes and digital signature schemes. In comparison with the straightforward approach employing an encryption scheme and a signature scheme for a message separately, the authenticated encryption scheme requires smaller bandwidth of data communications for achieving privacy, integrity and authentication. Afterwards, many similar schemes have been proposed (Hwang *et al.*, 1996; Lee and Chang, 1997; Wu *et al.*, 1999; Tseng *et al.*, 2003; Chen, 2004; Hwang and Liu, 2005).

Because no one except the specified recipient can be convinced of the signer's signature in an authenticated encryption scheme, so if the signer repudiates her signature later, the recipient cannot prove the dishonesty of the signer to any verifier without releasing his secret. To overcome this weakness, Araki *et al.* (1999) proposed a convertible limited verifier scheme to enable the recipient to convert the signature to an ordinary one so that any verifier can verify its validity. But it needs the cooperation of the signer when the recipient converts the signature, which is obviously a weakness if the signer is unwilling to cooperate.

Later, Wu and Hsu (2002) proposed a new convertible authenticated encryption scheme. The recipient can easily produce the ordinary signature without the cooperation of the signer, and if the signer wants to repudiate her signature, he can reveal the converted signature and then any verifier can prove the dishonesty of the signer. Unfortunately, Huang and Chang (2003) showed that the Wu *et al.*'s scheme does not consider the problem that once an intruder knows the message then he can also easily convert a signature into an ordinary one and claim that the signature is sent to him. Finally, they proposed a new convertible authenticated encryption scheme to solve this problem.

On the other hand, if the signed message is large, the message must be divided into a sequence of small message blocks and each message block can be encrypted and signed as a signature block individually. But this approach has a weakness that an intruder can reorder or partially delete blocks so that the recipient cannot realize this. Recently, Lv *et al.* (2005) showed that neither the Wu *et al.*'s scheme nor the Huang *et al.*'s scheme can provide semantic security for messages. That is, any adversary can determine whether his guessed message is the actual message signed by the original signer after he gets a valid signature. Furthermore, the Huang *et al.*'s scheme has another weakness: once an adversary gets a valid signature on a specific message, then he can recover another message if he gets its corresponding signature.

Then Lv *et al.* proposed a new convertible authenticated encryption scheme using self-certified public keys (Girault, 1991), and extended it to one with message linkages when the signed message is large. Each scheme provides semantic security of messages, i.e., after getting a valid signature, any adversary cannot determine whether his guessed message is the actual message.

In this paper, we show that the Lv *et al.*'s scheme cannot provide confidentiality either since the verifier can recover messages if given many triples of messages, signature and ciphertexts in the basic convertible authenticated encryption scheme. Finally we propose a new improvement to overcome these weaknesses and to improve its efficiency.

2. Brief Review of the Basic Convertible Authenticated Encryption Scheme

The basic scheme of Lv *et al.* consists of the following five phases: system initialization, signature generation, signature recovery and verification, conversion and recipient proof.

System Initialization

The trusted authority, TA, chooses two large and distinct primes p and q, and computes $n = pq$, where $p = 2p^* + 1,\ q = 2q^* + 1$ and $p^*,\ q^*$ are two large primes. Then, TA selects a generator g in Z_n, where g has an order of $p^*\, q^*$, and a public one-way hash function $H(\cdot)$. TA publishes n, g and $H(\cdot)$ to all users and keeps (p^*, q^*, p, q) secret. When a user, Alice say, intends to join the system, she first chooses a secret key x_a and computes $Y_a = g^{x_a}$ mod n. Then she sends Y_a and her identity ID_a to TA. After receiving them, TA computes $y_a = (Y_a - ID_a)^{(H(ID_a))^{-1}}$mod n as Alice's public key. Alice can check the validity of y_a by checking the equation $y_a^{H(ID_a)} + ID_a = Y_a$ mod n. Every participant in this cryptosystem must register in the same way.

Signature Generation

To sign a message $M \in \mathrm{Z}_n$ to a recipient Bob, Alice does the following:

Step 1: Alice, who knows the identity ID_b and the public key y_b corresponding to the secret key x_b of a recipient, Bob, randomly selects an integer x, and computes

$$\begin{aligned} r &= M(y_b^{H(ID_b)} + ID_b)^{-x} \bmod n, \\ v &= g^{x(y_b^{H(ID_b)} + ID_b)^{x_a}} \bmod n, \\ c &= H(M, v, g^x), \\ s &= x - cx_a. \end{aligned} \tag{1}$$

Step 2: Alice sends the tuple (c, r, s) to the recipient Bob.

Message Recovery and Verification

After receiving the tuple (c, r, s), the recipient Bob computes

$$\begin{aligned} Y_a &= y_a^{H(ID_a)} + ID_a \bmod n, \\ M &= r(g^s Y_a^c)^{x_b} \bmod n, \\ v &= (g^s Y_a^c)^{Y_a^{x_b}} \bmod n. \end{aligned}$$

Then, Bob checks if the following equation holds:

$$c = H(M, v, g^s Y_a^c). \tag{2}$$

If it holds, then he is convinced that the signature is a valid signature from Alice. Rejects, otherwise.

Conversion

If the signer Alice wants to repudiate her signature later, the recipient Bob can prove Alice's dishonesty to any verifier by revealing the message M and the parameter v for a given (c, s). Any verifier can check Alice's dishonesty by Eq. 2. Only if it holds does the verifier accept the signature generated by Alice. If Bob does not reveal v, any verifier cannot check the validity of the message even though he gets the message M and the corresponding signature (c, r, s).

Recipient Proof

If Bob wants to prove to any verifier Tom that he is the real recipient, they can do as follows:

Step 1: Bob first sends the message M, the parameter v and the signature (c, s) to Tom.

Step 2: After determining Bob's identity, Tom computes

$$Y_a = y_a^{H(ID_a)} + ID_a \bmod n,$$

and then checks if Eq. 2 holds. If it holds, then he continues the following steps. Otherwise, terminates the protocol.

Step 3: Tom selects a random integer k, computes

$$K = (g^s Y_a^c)^k \bmod n$$

and then sends K to Bob;

Step 4: After receiving K, Bob computes $Z = K^{Y{a^{x_b}}}$ mod n, and returns it to Tom.

Step 5: Tom computes $Z = v^k$ mod n, and checks if $Z = Z^*$ holds. If it holds, then he is convinced that the signature is sent to Bob.

3. Confidentiality of the Lv *et al.*'s Scheme

Lv *et al.* claimed that their scheme can provide the semantic security of messages. However, we find that their claim is not right. Before the attack description, we first point some problems in their scheme. We think that they are typos.

3.1. *Typos*

In Signature Generation, Alice randomly selects an integer x, and computes

$$\begin{aligned} r &= M(y_b^{H(ID_b)} + ID_b)^{-x} \bmod n, \\ v &= g^{x(y_b^{H(ID_b)} + ID_b)^{x_a}} \bmod n, \\ c &= H(M, v, g^x), \\ s &= x - cx_a. \end{aligned} \tag{1}$$

In Message Recovery and Verification

After receiving the tuple (c, r, s), the recipient Bob, computes

$$Y_a = y_a^{H(ID_a)} + ID_a \bmod n,$$

$$M = r(g^s Y_a^c)^{x_b} \bmod n,$$
$$v' = (g^s Y_a^c)^{Y_a^{x_b}} \bmod n.$$

Then, Bob checks if the following equation holds:

$$c = H(M, v', g^s Y_a^c). \tag{2}$$

To make Bob to accept the signature, it should have the equation

$$H\big(M, g^{x(y_b^{H(ID_b)}+ID_b)^{x_a}} \bmod n, g^x\big) = H\big(M, (g^s Y_a^c)^{Y_a^{x_b}} \bmod n, g^s Y_a^c\big).$$

It means that $g^{x(y_b^{H(ID_b)}+ID_b)^{x_a}} \bmod n = (g^s Y_a^c)^{Y_a^{x_a}} \bmod n$ and $g^x = g^s Y_a^c$, which imply that $(y_b^{H(ID_b)} + ID_b)^{x_a} = Y_a^{x_b} \bmod p^* q^*$ and $g^x = g^s Y_a^c \bmod n$.

To obtain consistency, it should be

$$v = g^{x((y_b^{H(ID_b)}+ID_b)^{x_a} \bmod n)} \bmod n,$$
$$v' = (g^s Y_a^c)^{(Y_a^{x_b} \bmod n)} \bmod n,$$
$$c = H(M, v, g^x \bmod n), \tag{1}$$
$$c' = H(M, v', g^s Y_a^c \bmod n). \tag{2}$$

Besides, the equation $Z = K^{Y a^{x_b}} \bmod n$ should be $Z = K^{(Y a^{x_b} \bmod n)} \bmod n$.

Furthermore, notice that the equation $s = x - c x_a$. To keep the private key x_a secret, x should be lager enough. Otherwise from $s = x \bmod c$, an adversary would obtain $s = (s \bmod c) + tc - c x_a$ for a unknown integer t. If t is not large, the adversary can guess t off-linely, then derives the private key x_a of the signer Alice.

Though we think that these errors are typos, the following weakness is fatal to the Lv *et al.*'s scheme.

3.2. *Confidentiality*

Lv *et al.* showed that the Huang *et al.*'s scheme is insecure since if the adversary has gotten a valid signature on one message, he would recover other messages from corresponding signature.

However, there is a similar weakness in the Lv *et al.*'s scheme.

Suppose that an adversary, for example any verifier Tom, has gotten some valid signatures on messages $(M_i, c_i, r_i, s_i),\ i = 1, 2, \ldots, k$. Hence, the adversary would obtain the equations

$$M_i = r_i (g^{s_i} Y_a^{c_i})^{x_b} \bmod n,$$
$$(Y_a^{x_b})^{c_i} = M_i / (r_i Y_b^{s_i}) \bmod n.$$

Now if the adversary gets another valid signature (c, r, s) on a message M, he can recover the message M as long as c is a multiple of GCD($c_1, c_2, \ldots, c_k$). Because the probability that two random integers are relatively prime is at least 0.6, it is likely that the adversary can find integers $t_1, t_2, \ldots, t_k$ such that $c = t_1c_1 + t_2c_2 + \ldots + t_kc_k$. Then he can compute

$$(Y_a^{x_b})^c = \prod_{i=1}^{k} \big(M_i/(r_iY_b^{s_i})\big)^{t_i} \bmod n.$$

Finally, he would obtain $M = r(Y_b^sY_a^{x_b})^c \bmod n$.

Hence, the Basic Convertible Authenticated Encryption Scheme of the Lv *et al.*'s scheme is insecure.

To withstand this attack, the equation

$$M = r(g^sY_a^c)^{x_b} \bmod n$$

should be replaced by

$$M = rH\big((g^sY_a^c)^{x_b} \bmod n\big) \bmod n.$$

However, since the order p^*q^* of the generator g is unknown except for TA, the exponents in this equation are long, which would take more time to compute. Meanwhile, TA knows the factors p and q of the modulo n. Then if p and q are not very large, TA can evaluate the discrete logarithms $Y_a = g^u \bmod p$ and $Y_a = g^v \bmod q$. Hence $x_a = u \bmod 2p^*$ and $x_a = v \bmod 2q^*$. Finally, TA can obtain the private key x_a by using Chinese Remainder Theorem. Hence, p and q should be large enough to make discrete logarithms in Z_p and Z_q hard.

Therefore, the Lv *et al.*'s scheme is not efficient.

4. Our Efficient Convertible Authenticated Encryption Schemes Using Self-Certified Public Keys

System Initialization

The trusted authority, TA, chooses four large and distinct primes q, p, p_1 and q_1, and computes $n = p_1q_1$, where $p < n, q|(p-1), p_1$ and q_1 are safe primes. Then, TA selects a generator g of order q in Z_p^*, and three public one-way hash functions $H(\cdot)$: $\{0,1\}^* \to Z_q, F(\cdot), G(\cdot)$: $Z_p \to Z_p$. TA publishes $n, g, p, q, F(\cdot), G(\cdot)$ and $H(\cdot)$ to all users and keeps (p_1, q_1) secret. When a user, Alice say, intends to join the system, she first chooses a private key $x_a \in Z_q^*$ and computes $Y_a = g^{x_a} \bmod p$. Then she sends Y_a and her identity ID_a to TA. After receiving them, TA computes $y_a = (Y_a - ID_a)^{(H(ID_a))^{-1}} \bmod n$ as Alice's public key. Alice can check the validity of y_a by verifying the equation $y_a^{H(ID_a)} + ID_a = Y_a \bmod n$. Every participant in this cryptosystem must register in the same way.

Signature Generation

To sign a message $M \in Z_p$ to a recipient Bob, Alice does the following:

Step 1: Alice, who knows the identity ID_b and the public key y_b corresponding to the private key x_b of a recipient, Bob, randomly selects two integers $t \in Z_q^*$ and $\sigma \in Z_p^*$, and computes

$$\begin{aligned}
&r = g^t \bmod p,\\
&e = H(M, \sigma, r),\\
&s = t - ex_a \bmod q,\\
&v = F\Big(\big((y_b^{H(ID_b)} + ID_b) \bmod n\big)^t \bmod p\Big) \oplus \sigma,\\
&c = G(\sigma) \oplus M,
\end{aligned}$$

where the symbol $\oplus$ denotes exclusive-or operation.

Step 2: Alice sends the tuple (c, v, e, s) to the recipient Bob.

Notice that if M is large, $c = E_{G(\sigma)}(M)$, where E is a one-time security symmetric encryption scheme (see (Fujisaki and Okamoto, 1999)).

Message Recovery and Verification

After receiving the tuple (c, v, e, s), the recipient Bob, computes

$$\begin{aligned}
&Y_a = y_a^{H(ID_a)} + ID_a \bmod n,\\
&r = g^s Y_a^e \bmod p,\\
&\sigma = v \oplus F(r^{x_b} \bmod p),\\
&M = c \oplus G(\sigma).
\end{aligned}$$

Then, Bob checks if the following equation holds:

$$e = H(M, \sigma, r). \tag{3}$$

If it holds, then he is convinced that the signature is a valid signature from Alice. Otherwise, rejects.

Conversion

If the signer Alice wants to repudiate her signature later, the recipient Bob can prove Alice's dishonesty to any verifier by revealing the parameter σ for a given (c, v, e, s). Any verifier can check Alice's dishonesty by the equation

$$e = H\big(c \oplus G(\sigma), \sigma, g^s (y_a^{H(ID_a)} + ID_a \bmod n)^e \bmod p\big).$$

Only if it holds does the verifier accept the signature generated by Alice. If Bob does not reveal σ, any verifier cannot check the validity of the message even though he gets the message M and the corresponding signature (c, v, e, s).

5. Security and Performance

In this section, we only give a heuristic security discussion of the new improvement for the sake of brevity.

The security property of the new improvement depends on those of a signature scheme, an encryption scheme and self-certified public key scheme.

The verification equations of the signature scheme is the equation

$$e = H\big(c \oplus G(\sigma), \sigma, g^s(y_a^{H(ID_a)} + ID_a \bmod n)^e \bmod p\big).$$

Hence this is a variant of the verification equation of the Schnorr signature scheme (Schnorr, 1991) that is proven secure against an adaptively chosen-message attack under the difficulty of discrete logarithms in random oracle models (Pointcheval and Stern, 2000).

In the encryption scheme, we adapt the technique of secure integration of asymmetric and symmetric encryption schemes proposed by Fujisaki and Okmoto (1999) to achieve the chosen ciphertext security. Here, an ElGamal encryption scheme (ElGamal, 1985) is employed only for distributing a session key of a symmetric encryption scheme for message encryption. Fujisaki and Okmoto showed that the security of this hybrid encryption scheme depends only on those of the asymmetric and symmetric encryption primitives and the following property of the asymmetric encryption primitive – given an appropriate message space, for any message in the space, the variants of the encryption occur in a large *enough* number, provided the coins are chosen uniformly from the coin space of the encryption scheme.

The security of the self-certified public keys comes from the RSA assumption (Rivest *et al.*, 1978).

Compared with the Lv *et al.*'s scheme, our scheme is more efficient in terms of communication and computation costs. The bit size of modulo n in the Lv *et al.*'s scheme is double of those in our scheme. The bit size of s in the Lv *et al.*'s scheme is larger than those of e plus s in our scheme. Meanwhile, the bit size of exponents in the Lv *et al.*'s scheme is double of those of modulo n, which is larger than those of modulo q in our scheme.

6. Conclusions

We have first showed that the verifier can recover messages if given many triples of message, signature and ciphertext in the basic convertible authenticated encryption scheme proposed by Lv *et al.*

Finally, we propose new improvements to the Lv *et al.*'s schemes to overcome these weaknesses. We heuristically show that the public key encryption scheme is chosen ciphertext secure in the random oracle model under the difficulty of Diffie–Hellman problem and the signature scheme is secure against an adaptively chosen-message attack in the random oracle model.

By using a new way to use Girault's self-certified public key, our improvement is more efficient than the convertible authenticated encryption scheme of Lv *et al.* Hence our improvement is more practical.

Our further work is to give a formal security model and provide a formal security proof to the new improvements.

Acknowledgements

This material is based upon work funded by Zhejiang Provincial Natural Science Foundation of China under Grant No. Y104201.

The author wishes to thank the anonymous referees for their very useful comments and suggestions.

References

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

Chen, B.-H. (2004). Improvement of authenticated encryption schemes with message linkages for message flows. *Computers & Electrical Engineering*, **30**, 465–469.

ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Tran.*, IT-31, 469–472.

Fujisaki, E., and T. Okamoto (1999). Secure integration of asymmetric and symmetric encryption schemes. In *Advances in Cryptology – CRYPTO'99*, vol. 1666 of LNCS, Springer-Verlag, Berlin. pp. 537–554.

Girault, M. (1991). Self-certified public keys. In *Advance in Cryptology-EUROCRYPT'91*, *LNCS 547*, Springer-Verlag, Berlin. pp. 491–497.

Horster, P., M. Michels and H. Petersen (1994). Authenticated encryption schemes with low communication costs. *Electronics Letters*, **30**(15), 1212–1213.

Huang, H., and C. Chang (2003). An efficient convertible authenticated encryption scheme and its variant. In *Proc. of ICICS2003 – Fifth International Conference on Information and Communications Security*, *LNCS 2836*, Springer-Verlag. pp. 382–392.

Hwang, M.-S., and C.-Y. Liu (2005). Authenticated encryption schemes: Current status and key issues. *International Journal of Network Security*, **1**(2), 61–73.

Hwang, S.-J., C.-C. Chang and W.-P. Yang (1996). Authenticated encryption schemes with message linkages. *Inform. Process Lett.*, **58**(4), 189–194.

Lee, W.-B., and C.-C. Chang (1997). Authenticated encryption schemes with message linkage between message blocks. *Inform. Process Lett.*, **63**(5), 247–250.

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

Nyberg, K., and A.R. Rueppel (1994). Message recovery for signature schemes based on the discrete logarithm problem. In *Advances in Cryptology – Eurocrypt'94*, *LNCS 950*, Springer, Berlin. pp. 175–190.

Pointcheval, D., and J. Stern (2000). Security arguments for digital signatures and blind signatures. *J. Cryptology*, **13**(3), 361–396.

Rivest, R.L., A. Shamir and L. Adelman (1978). A method for obtain digital signatures and public-key cryptosystem. *Commun. ACM*, **21**(2), 120–126.

Schnorr, C.P. (1991). Efficient signature generation by smart cards. *Journal of Cryptology*, **3**(3), 161–174.

Tseng, Y.-M., J.-K. Jan and H.-Y Chien (2003). Authenticated encryption schemes with message linkages for message flows. *Computers & Electrical Engineering*, **29**(1), 101–109.

Wu, T., and C. Hsu (2002). Convertible authenticated encryption scheme. *The Journal of Systems and Software*, **62**, 205–209.

Wu, T.-S., T.-C. Wu and W.-H. He (1999). Authenticated encryption schemes with double message linkage. In *Proceedings of Ninth National Conference on Information Security*, Taiwan, ROC. pp. 303–308.

Z. Shao received BS degree in mathematics and MS in algebra from the Northeastern Normal University, People's Republic of China in 1976 and 1981 respectively. His current research interests are cryptography and financial data security.

Praktinių konvertuojamo autentikuoto kodavimo schemų, naudojančių pasiliudijančius atvirus raktus, kriptoanalizė ir pagerinimas

Zuhua SHAO

Konvertuojamo autentikuoto kodavimo schemos leidžia nurodytam gavėjui ir atstatyti, ir patikrinti pranešimą. Be to, gavėjas gali įrodyti trečiajai šaliai siuntėjo nesąžiningumą, jei siuntėjas vėliau išsižada savo parašo. Neseniai Lv ir kiti parodė, kad Wu ir kitų bei Huang ir kitų konvertuojamo autentikuoto kodavimo schemos negali užtikrinti semantinio užkoduotų pranešimų saugumo. Todėl jie pasiūlė praktinio konvertuojamo autentikuoto kodavimo schemą, panaudojančią pasiliudijančius atvirus raktus, ir išplėtė ją situacijai, kai pasirašyti pranešimai yra dideli. Šiame straipsnyje mes parodome, kad tikrintojas gali atstatyti pranešimus, jei turi daug Lv ir kitų konvertuojamo autentikuoto kodavimo schemos pranešimo, parašo ir kodo trejetų. Vėliau mes pasiūlome naują šių schemų pagerinimą, įveikiantį šį trūkumą ir pagerinantį jo efektyvumą.