Available online at www.sciencedirect.com
ScienceDirect
Computers and Electrical Engineering xxx (2006) xxx–xxx
Computers and Electrical Engineering
www.elsevier.com/locate/compeleceng

A new convertible authenticated encryption scheme with message linkages

Shiang-Feng Tzeng [a], Yuan-Liang Tang [a], Min-Shiang Hwang [b,*]

[a] *Department of Information Management, Chaoyang University of Technology, 168 Gifeng E. Road, Wufeng, Taichung County 413, Taiwan, ROC*
[b] *Department of Management Information Systems, National Chung Hsing University, 250 Kuo Kuang Road, Taichung 402, Taiwan, ROC*

Received 21 January 2003; received in revised form 5 February 2006; accepted 24 February 2006

Abstract

In this article, we present an authenticated encryption scheme with message linkages used to deliver a large message. To protect the receiver's benefit, the receiver can easily convert the signature into an ordinary one that can be verified by anyone. Several feasible attacks will be discussed, and the security analysis will prove that none of them can successfully break the proposed scheme.

Keywords: Authenticated encryption scheme; Discrete logarithms; Digital signature; Message recovery

1. Introduction

Nyberg and Rueppel [11,12] were the first to propose the idea of a digital signature scheme with message recovery based on the discrete logarithm problem. To reduce the communication cost of Nyberg and Rueppel's schemes, Horster et al. [5] presented an authenticated encryption scheme, and there have actually been quite a number of efficient authenticated encryption schemes [1–3,7,8,10,13,16] proposed since then. In their schemes, the signer could generate a signature for a message and then send it to a specified receiver. After receiving the signature, only the receiver could recover and verify the message.

Recently, Tseng et al. [14] have proposed two efficient authenticated encryption schemes with message linkages. One is a basic scheme that is superior to all previously proposed schemes in terms of computation and communication cost. The other is a generalized scheme which allows the receiver to recover the message after receiving the partial signature blocks.

* Corresponding author. Fax: +886 4 22857173.
E-mail address: mshwang@nchu.edu.tw (M.-S. Hwang).

0045-7906/$ - see front matter © 2006 Elsevier Ltd. All rights reserved.
doi:10.1016/j.compeleceng.2006.02.005

Further, consider the condition of a later dispute; e.g., the signer denies having signed a signature. It could be required to reveal the message along with its signature for verifying. To protect the receiver's benefit in case of a later dispute, we should further enable the recipient to convert the signature into an ordinary one that can be verified by anyone. Araki et al. [2] presented a convertible limited verifier signature scheme. However, the conversion of the signature demands the signer to release one more parameter. It could be unworkable if the signer is unwilling to cooperate. Wu and Hsu [15] presented a convertible authenticated encryption scheme. In the scheme, when the signer repudiates the signature, the receiver can prove the dishonesty of the signer by revealing an ordinary signature that can be verified by anyone without the cooperation of the signer.

In the next section, we shall propose a convertible authenticated encryption scheme with message linkages. Not only can the proposed scheme deliver a large message but the scheme is also to convert the signature into an ordinary one. Then Section 3 will present the security analysis and performance evaluation of the proposed scheme. Finally, some concluding remarks will be in the last section.

2. The proposed scheme

In this section, we shall present a convertible authenticated encryption scheme with message linkages based on Tseng et al.'s basic scheme [14]. In the proposed scheme, the signature only needs be recovered and verified by the specified receiver in the normal procedure. Later, if the signer repudiates the signature, the receiver can reveal the converted signature for verifying. The proposed scheme consists of four phases: the system initialization phase, the signature generation phase, the message recovery phase, and the conversion phase as follows. The flow chart of the signature generation phase and message recovery phase is illustrated in Fig. 1.

2.1. System initialization phase

The system parameters are defined as follows. Let p be a large prime, q be a large prime factor of $p-1$, g be a generator with order q in $GF(p)$, and let $h(\cdot)$ be a one-way hash function. Each user U_i owns a private

Alice (U_a)

make $r_0 = 0$

select a random integer $k \in GF(q)$

$r_i = M_i \cdot h(r_{i-1} \oplus y_b^k) \bmod p$

$r = h(r_1||r_2||\cdots||r_n)$

$R = h(M, r, h(g^k \bmod p)) \bmod q$

$S = k - Rx_a \bmod q$

$\xrightarrow{(R, S, r, r_1, r_2, \cdots, r_n)}$

Bob (U_b)

$r' = h(r_1||r_2||\cdots||r_n)$

confirm $r' \stackrel{?}{=} r$

$M_i = r_i \cdot h(r_{i-1} \oplus (g^S y_a^R)^{x_b})^{-1} \bmod p$

$R \stackrel{?}{=} h(M, r, h((g^S y_a^R \bmod p)) \bmod q$

Fig. 1. Convertible authenticated encryption scheme with message linkages.

Please cite this article as: Shiang-Feng Tzeng et al., A new convertible authenticated encryption scheme ..., Computers and Electrical Engineering (2006), doi:10.1016/j.compeleceng.2006.02.005

key $x_i \in Z_q^*$ and calculates the corresponding public key $y_i = g^{x_i} \bmod p$. Let U_a be the signer and U_b be the receiver.

2.2. Signature generation phase

Without loss of generality, assume that the signer U_a wants to deliver a large message M to the specified receiver U_b. Suppose that the message M is composed of the sequence $\{M_1, M_2, \ldots, M_n\}$, where $M_i \in GF(p)$. Then, U_a performs the following steps to create the signature blocks for the message M.

1. Let $r_0 = 0$ and select a random integer $k \in GF(q)$.
2. Calculate $r_i = M_i \cdot h(r_{i-1} \oplus y_b^k) \bmod p$ for $i = 1, 2, \ldots, n$, where "$\oplus$" denotes the exclusive operator.
3. Calculate $r = h(r_1 \| r_2 \| \ldots \| r_n)$, where "$\|$" denotes the concatenation operator.
4. Calculate $R = h(M, r, h(g^k \bmod p)) \bmod q$.
5. Calculate

$$S = k - Rx_a \bmod q. \tag{1}$$

U_a delivers the signature blocks $(R, S, r, r_1, r_2, \ldots, r_n)$ to U_b via a public channel. Note that r_i is used as a linking parameter between the ith and $(i+1)$th message block.

2.3. Message recovery phase

After receiving the signature blocks $(R, S, r, r_1, r_2, \ldots, r_n)$, U_b can recover the message blocks $\{M_1, M_2, \ldots, M_n\}$ by following the steps below:

1. Calculate $r' = h(r_1 \| r_2 \| \cdots \| r_n)$ and confirm that $r' \stackrel{?}{=} r$ is true.
2. Recover the message blocks $\{M_1, M_2, \ldots, M_n\}$ as follows:

$$M_i = r_i \cdot h(r_{i-1} \oplus (g^S y_a^R)^{x_b})^{-1} \bmod p, \tag{2}$$

   for $i = 1, 2, \ldots, n$ and $r_0 = 0$.
3. Verify the signature with the following equality:

$$R \stackrel{?}{=} h(M, r, h(g^S y_a^R \bmod p)) \bmod q. \tag{3}$$

   If the equation does, the signature is valid.

2.4. Conversion phase

If U_a repudiates the signature, U_b can confirm the dishonesty of the signer by revealing the converted signature (R, S, r) for the message M. With this converted signature, anyone can conform its validity using Eq. (3).

Now, we shall prove that the proposed scheme can work correctly by checking the following theorems:

Theorem 2.1. *In the message recovery phase, the receiver U_b can recover the message using Eq. (2).*

Proof 1. According to Eq. (2), we have

Please cite this article as: Shiang-Feng Tzeng et al., A new convertible authenticated encryption scheme ..., Computers and Electrical Engineering (2006), doi:10.1016/j.compeleceng.2006.02.005

$$
\begin{aligned}
& r_i \cdot f(r_{i-1} \oplus (g^S y_a^R)^{x_b})^{-1}, \\
& \quad = r_i \cdot f(r_{i-1} \oplus (g^{k-Rx_a} y_a^R)^{x_b})^{-1}, \\
& \quad = r_i \cdot f(r_{i-1} \oplus (g^k y_a^{-R} y_a^R)^{x_b})^{-1}, \\
& \quad = r_i \cdot f(r_{i-1} \oplus (g^k)^{x_b})^{-1}, \\
& \quad = r_i \cdot f(r_{i-1} \oplus y_b^k)^{-1}, \\
& \quad = M_i \bmod p. \qquad \square
\end{aligned}
$$

Theorem 2.2. *In the conversion phase, the converted signature can be verified by Eq. (3).*

Proof 2. According to Eq. (3), we have

$$
\begin{aligned}
& h(M, r, h(g^S y_a^R \bmod p)), \\
& \quad = h(M, r, h(g^{k-Rx_a} y_a^R \bmod p)), \\
& \quad = h(M, r, h(g^k y_a^{-R} y_a^R \bmod p)), \\
& \quad = h(M, r, h(g^k \bmod p)), \\
& \quad = R \bmod q. \qquad \square
\end{aligned}
$$

3. Discussions

3.1. Security analysis

Our convertible authenticated encryption scheme is as secure as a digital signature scheme. The security of the proposed scheme is based on the difficulty of breaking a one-way hash function [9] and discrete logarithms [4,6]. In this section, we shall consider some possible attacks against the proposed scheme. We shall prove that the proposed scheme can successfully withstand those possible attacks.

Attack 1: An adversary attempts to derive the user's private key x_i from all public information available.

Analysis of attack 1: Assume that the adversary wants to derive U_a's private key x_a from the corresponding public key $y_a = g^{x_a} \bmod p$. It is as difficult as breaking the discrete logarithms to obtain U_a's private key x_a. From the signature, the adversary cannot derive U_a's private key x_a through Eq. (1), since the equation has two unknown variables x_a and k, and k is also based on the one-way hash function and the discrete logarithms.

Attack 2: An adversary knows one message block M_i and tries to obtain the common key $y_{ab} (= y_a^{x_b})$ or the other message blocks.

Analysis of attack 2: The adversary can calculate $h(r_{i-1} \oplus y_b^k) = M_i^{-1} \cdot r_i \bmod p$. Assume she/he can derive y_b^k, which means y_{ab} can be obtained from $y_b^k = (g^S y_a^R)^{x_b} \bmod p$. However, y_b^k is difficult to solve under the one-way hash function. Due to the value of y_b^k, the adversary cannot also derive the other message blocks through Eq. (2).

Attack 3: An adversary attempts to forge the blocks of an authenticated encryption signature.

Analysis of attack 3: To construct a signature to satisfy satisfying Eq. (2), the adversary should first know the common key y_{ab} between U_a and U_b. As with Attack 2, she/he will have to face the difficult problem.

Attack 4: An adversary tries to forge a converted signature to pass Eq. (3).

Analysis of attack 4: From Eq. (3), given S, it is difficult to determine r and R because of the difficulty of solving the one-way hash function and the discrete logarithms. Similarly, given r and R, it is also infeasible to determine S such that Eq. (3) holds.

Attack 5: An adversary attempts to recover the message M_i from the authenticated encryption signature.

Please cite this article as: Shiang-Feng Tzeng et al., A new convertible authenticated encryption scheme ..., Computers and Electrical Engineering (2006), doi:10.1016/j.compeleceng.2006.02.005

Analysis of attack 5: From Eq. (2), the message M_i can be recovered by one who has the private key x_a or x_b. Similar to Attack 1, it is as difficult as breaking the discrete logarithms to obtain the user's private key.

Attack 6: An adversary tries to verify the signature before converting.

Analysis of attack 6: To perform the signature verification in Eq. (3), the adversary needs the message M. Similar to Attack 5, she/he cannot obtain or recover the message M_i. Therefore, she/he cannot verify the signature.

Attack 7: An adversary attempts to reorder, modify, delete or replicate the message blocks.

Analysis of attack 7: If any signature block is recorded, modified, deleted or replicated, then the signature $R = h(M,r,h(g^k \bmod p)) \bmod q$ and $S = k - Rx_a \bmod q$ must be changed as well. Thus, those signature blocks cannot pass the verification equations because the relationship $r = h(r_1\|r_2\| \cdots \|r_n)$ will no longer exist. Therefore, the receiver will detect the changes.

3.2. Performance evaluation

In the following, the performance evaluation of the proposed scheme is discussed. We shall express the computational complexity and communication cost of the proposed scheme. We denote the performance evaluation notations as follows: $T_{\exp}$ is the time for a modular exponentiation computation; T_{mul} is the time for a modular multiplication computation; T_{inv} is the time for a modular inverse computation; T_h is the time for a one-way hash function $h(\cdot)$ computation; $|x|$ is the bit-length of an integer x. The computational complexities of executing the exclusive and subtraction operations are neglected.

Assume there is a large message to deliver. The message is divided into n message blocks. In the convertible authenticated encryption scheme with message linkages, the set of signature blocks is $(R, S, r, r_1, r_2, \cdots, r_n)$. Therefore, the signer requires $2T_{\exp} + (n+1)T_{\mathrm{mul}} + (n+3)T_h$ to generate the message blocks, while verifying and retrieving the message blocks requires $3T_{\exp} + (n+1)T_{\mathrm{mul}} + nT_{\mathrm{inv}} + (n+3)T_h$. Finally, the communication cost in the proposed scheme is $n|p| + 2|q| + |h|$.

4. Conclusion

In this article, a novel convertible authenticated encryption scheme with message linkages have been proposed. For avoiding the abuse of the signature, the proposed scheme provides the ability to convert the signature into an ordinary one that can be verified by anyone. Besides, the conversion does not require the cooperation of the signer. The proposed scheme provides protection for the receiver. Some possible attacks have been considered, and none of them can successfully break the proposed scheme. Again, our scheme can be used on the Tseng et al.'s generalized scheme for message flows [14]. The receiver can recover the message blocks and use them before the receiving of the entire signature.

Acknowledgement

This research was partially supported by the National Science Council, Taiwan, ROC, under Contract No.: NSC91-2213-E-324-003.

References

[1] Abdel-Hafez Ahmed, Miri A, Orozco-Barbosa Louis. Authenticated group key agreement protocols for ad hoc wireless networks. Int J Network Secur 2007;4(1):90–8.

[2] Araki Shunsuke, Uehara Satoshi, Imamura Kyoki. The limited verifier signature and its application. IEICE Trans Fundament 1999;E82-A(1):63–8.

[3] Choo KKR. Revisit of mccullagh-barreto two-party id-based authenticated key agreement protocols. Int J Network Secur 2005;1(3):154–60.

[4] ElGamal T. A public-key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans Informat Theory (IT-31) 1985:469–72.

[5] Horster P, Michels M, Petersen H. Authenticated encryption schemes with low communication costs. Electronics Lett 1994;30(15):1212.

[6] Hwang MS, Chang TY. Threshold signatures current status and key issues. Int J Network Secur 2005;1(3):123–37.
[7] Hwang Shin-Jia, Chang Chin-Chen, Yang Wei-Pang. Authenticated encryption schemes with message lingage. Informat Process Lett 1996;58(4):189–94.
[8] Lee Wei-Bin, Chang Chin-Chen. Authenticated encryption schemes with linkage between message blocks. Informat Process Lett 1997;63(5):247–50.
[9] Mangipudi KV, Katti RS. A hash-based strong password authentication protocol with user anonymity. Int J Network Secur 2006;2(3):205–9.
[10] Mangipudi KV, Katti RS, Fu H. Authentication and key agreement protocols preserving anonymity. Int J Network Secur 2006;3(3): 259–70.
[11] Nyberg K, Rueppel RA, A new signature scheme based on the DSA giving message recovery, In: 1st ACM Conference on Computer and Communications Security, Fairfax, Virginia, 1993, pp. 58–61.
[12] Nyberg K, Rueppel RA. Message recovery for signature schemes based on the discrete logarithm, in advances in cryptology. EUROCRYPT'94 1994:175–90.
[13] Nyberg K, Rueppel RA. Message recovery for signature schemes based on the discrete logarithm. Des Codes Cryptogr 1996; 7(1-2):61–81.
[14] Tseng Yuh-Min, Jan Jinn-Ke, Chien Hung-Yu. Authenticated encryption schemes with message linkages for message flows. Comput Electrical Eng 2003;29(1):101–9.
[15] Wu Tzong-Sun, Hsu Chien-Lung. Convertible authenticated encyption scheme. J Sys Software 2002;62(3):205–9.
[16] Yoon EJ, Yoo KY. On the security of signature scheme with message recovery and its application. Int J Network Secur 2006;3(2):151–4.

Shiang-Feng Tzeng received the B.S. and M.S. degree in Information Management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, Republic of China, in 2001 and in 2003. He is currently pursuing his Ph.D. degree in Information Management from CYUT. His current research interests include applied cryptography and data security. His current research interests include cryptography, information security, and network security.

Yuan-Liang Tang obtained his Ph.D. in Computer Engineering from the Pennsylvania State University in the United States. He is currently an associate professor of department of Information Management at Chaoyang University of Technology in Taiwan. His research interests include information hiding, digital watermarking, image processing, computer vision, and information systems.

Min-Shiang Hwang received the B.S. in Electronic Engineering from the National Taipei Institute of Technology, Taipei, Taiwan, ROC, in 1980; the M.S. in Industrial Engineering from the National Tsing Hua University, Taiwan, in 1988; and a Ph.D. in Computer and Information Science from the National Chiao Tung University, Taiwan, in 1995. He also studied Applied Mathematics at the National Cheng Kung University, Taiwan, from 1984 to 1986. Dr. Hwang passed the National Higher Examination in field "Electronic Engineer" in 1988. He also passed the National Telecommunication Special Examination in field "Information Engineering", qualified as advanced technician the first class in 1990. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications, ROC. He was also the chairman of the Department of Information Management, Chaoyang University of Technology (CYUT), Taiwan, during 1999–2002. He was a professor and chairman of the Graduate Institute of Networking and Communications, CYUT, during 2002–2003. He obtained the 1997, 1998, 1999, 2000, and 2001 Outstanding Research Award of National Science Council of the Republic of China. He is currently a professor and chairman of the department of Management Information Systems, National Chung Hsing University, Taiwan, ROC. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include electronic commerce, database and data security, cryptography, image compression, and mobile computing. Dr. Hwang has published over 100 articles on the above research fields in international journals.