LETTER *Special Section on Information and Communication System Security*

An Improved Authenticated Encryption Scheme*

Fagen LI[†,††,†††a)], ***Member***, **Jiang DENG**[†], ***Nonmember***, ***and*** **Tsuyoshi TAKAGI**[†††], ***Member***

SUMMARY Authenticated encryption schemes are very useful for private and authenticated communication. In 2010, Rasslan and Youssef showed that the Hwang et al.'s authenticated encryption scheme is not secure by presenting a message forgery attack. However, Rasslan and Youssef did not give how to solve the security issue. In this letter, we give an improvement of the Hwang et al.'s scheme. The improved scheme not only solves the security issue of the original scheme, but also maintains its efficiency.

key words: *authenticated encryption, unforgeability, confidentiality, non-repudiation*

1. Introduction

Two important services of public key cryptography are privacy and authentication. Public key encryption schemes aim at providing confidentiality whereas digital signature schemes must provide authentication and non-repudiation. Nowadays, many practical cryptographic applications require those distinct goals to be simultaneously achieved, such as electronic commerce and mobile communication. Authenticated encryption schemes are designed to satisfy such requirements. An authenticated encryption scheme allows a signer to generate an authenticated ciphertext such that only the designated receiver can decrypt the signed message and verify the corresponding signature. A good authenticated encryption scheme should satisfy unforgeability, confidentiality and non-repudiation.

In an authenticated encryption scheme, if a message is large, we need divide the message into a sequence of message blocks and each message block is encrypted and signed as a signature block individually. However, such method will need more computation and communication costs. To reduce the computation and communication costs, a notion called authenticated encryption with message linkages was proposed. In 2003, Tseng, Jan and Chien [1] proposed two authenticated encryption schemes with message linkages. In 2006, Hwang et al. [2] showed that the Tseng-Jan-Chien schemes suffered from message flows destroyed by an adversary but the receiver is unconscious of the wrong flaws. That is, the Tseng-Jan-Chien schemes do not satisfy the unforgeability and non-repudiation. In addition, Hwang et al. gave an improvement of the Tseng-Jan-Chien schemes. Unfortunately, in 2010, Rasslan and Youssef [3] showed that the Hwang et al.'s authenticated encryption scheme is also not secure by presenting a message forgery attack. That is, the Hwang et al.'s scheme also does not satisfy the unforgeability and non-repudiation. However, Rasslan and Youssef did not give how to solve the security issue. In this letter, we give an improvement of the Hwang et al.'s scheme. The improved scheme not only solves the security issue of the original scheme, but also maintains its efficiency.

2. An Improved Scheme

Let p be a large prime, q be a large prime factor of $p-1$, g be a generator with order q in Z_p and $h(\cdot)$ be a one-way hash function. The signer U_a has a private key $x_a \in Z_q^*$ and a corresponding public key $y_a = g^{x_a} \bmod p$. The receiver U_b has a private key $x_b \in Z_q^*$ and a corresponding public key $y_b = g^{x_b} \bmod p$. The improved scheme consists of three phases: the signature generation phase, the message recovery phase and the conversion phase.

Signature generation phase: To generate a signature for a large message M (the message M is made up of the sequence $\{M_1, M_2, \ldots, M_n\}$, where $M_i \in Z_p$) and send it to U_b, U_a performs the following steps.

1. Choose a random integer $k \in Z_q^*$.
2. Set $r_0 = 0$.
3. Compute $t = g^k \bmod p$.
4. Compute $s = k + x_a h(M, t) \bmod q$.
5. Compute $r_i = M_i \oplus h(r_{i-1} \oplus y_b^k)$ for $i = 1, 2, \ldots, n$. Here $\oplus$ denotes the exclusive or operator.
6. Compute $v = s \oplus h(y_b^k)$.
7. Send $(t, r_1, r_2, \ldots, r_n, v)$ to U_b.

Message recovery phase: After receiving the $(t, r_1, r_2, \ldots, r_n, v)$, U_b performs the following steps.

1. Compute $M_i = r_i \oplus h(r_{i-1} \oplus t^{x_b})$ for $i = 1, 2, \ldots, n$ and $r_0 = 0$.

Manuscript received February 1, 2011.

Manuscript revised April 23, 2011.

[†] The authors are with the School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China.

[††] The author is with the State Key Laboratory of Information Security, Graduate School of Chinese Academy of Sciences, Beijing 100049, China.

[†††] The authors are with the Faculty of Mathematics, Kyushu University, Fukuoka-shi, 819–0395 Japan.

[*] This work is supported by the National Natural Science Foundation of China (Grant Nos. 60803133, 60873233, 61073176, 61003230, and 61003232), the State Key Laboratory of Information Security, and the Fundamental Research Funds for the Central Universities.

a) E-mail: fagenli@uestc.edu.cn

DOI: 10.1587/transinf.E94.D.2171

Table 1 Security and performance comparison.

schemes	security			computation cost		communication cost
	uf	co	nr	signature generation	message recovery	
[1]	no	yes	no	$T_e + (n+1)T_m + (n+1)T_h$	$3T_e + (n+1)T_m + nT_i + (n+1)T_h$	$n\lvert p\rvert + \lvert q\rvert + \lvert h\rvert$
[2]	no	yes	no	$2T_e + T_m + (n+1)T_h$	$3T_e + T_m + nT_i + (n+1)T_h$	$(n+1)\lvert p\rvert + \lvert q\rvert$
ours	yes	yes	yes	$2T_e + T_m + (n+2)T_h$	$3T_e + T_m + (n+2)T_h$	$(n+1)\lvert p\rvert + \lvert q\rvert$

2. Recover the signature element $s = v \oplus h(t^{x_b})$.
3. Check if the following equation holds:

$$g^s = t y_a^{h(M,t)} \bmod p \qquad (1)$$

If the above equation holds, the signature is valid. Otherwise, U_b should reject it.

Conversion phase: U_b publishes the converted signature (t, s) for the message M. With this converted signature, anyone can verify its validity by checking Eq. (1).

Our modification has two points: (1) Schnorr signature scheme is used to resist the attack in [3]; (2) the signature element s is encrypted to achieve the confidentiality.

3. Analysis of the Improved Scheme

The main security leak of Hwang et al.'s scheme [2] is that they use an insecure signature verification equation. Our improved scheme eliminates this leak by using standard Schnorr's signature verification equation [4].

For the unforgeability, we use Schnorr signature scheme [4] to generate (t, s), i.e., $t = g^k \bmod p$ and $s = k + x_a h(M, t) \bmod q$. Schnorr's signature scheme has been proved to be secure against an adaptively chosen message attack in the random oracle model under the computational Diffie-Hellman assumption [5]. Therefore, without the private key x_a of U_a, any attacker cannot make up a valid (t, s) that pass the verification of Eq. (1).

For the confidentiality, anyone cannot extract the message M from the ciphertext $(t, r_1, r_2, \ldots, r_n, v)$ except the receiver U_b. To extract the message M, the attacker has to obtain the session key $h(r_{i-1} \oplus t^{x_b})$. Since h is a secure hash function, the attacker has to obtain $r_{i-1} \oplus t^{x_b}$. However, the attacker cannot obtain $r_{i-1} \oplus t^{x_b}$ from $t = g^k \bmod p$ and y_b. In the improved scheme, $t = g^k \bmod p$ and $r_i = M_i \oplus h(r_{i-1} \oplus y_b^k)$ are actually a hashed ElGamal ciphertext. From [6], we know that the hashed ElGamal encryption satisfies the semantic security under the decisional Diffie-Hellman assumption. So the improved scheme satisfies the confidentiality.

For the non-repudiation, anyone can verify that (t, s) is a standard Schnorr signature if the receiver U_b releases the triple (M, t, s). So, a trusted third party can easily settle potential dispute between the U_a and the U_b by checking if Eq. (1) holds.

We compare the security and performance of the improved scheme with those of the Tseng-Jan-Chien scheme [1] and Hwang et al.'s scheme [2] in Table 1. For convenience, the following notation is used to analyze the performance evaluation of the improved schemes: T_e is the time for executing a modular exponentiation operation; T_m is the time for executing a modular multiplication operation; T_i is the time for executing a modular inverse operation; T_h is the time for executing a one-way hash function; $|x|$ is the bit-length of an integer x. The computational cost of executing the modular addition, modular subtraction and exclusive or operations are neglected because they are much smaller than T_e, T_m, T_i and T_h. The uf, co and nr in the "security" column refer to unforgeability, confidentiality and non-repudiation, respectively.

From Table 1, we know that both Tseng-Jan-Chien scheme [1] and Hwang et al.'s scheme [2] do not satisfy the unforgeability and non-repudiation. Our scheme satisfy the unforgeability, confidentiality and non-repudiation. The Hwang et al.'s scheme and improved scheme are more efficient than the Tseng-Jan-Chien scheme. As compared with the Hwang et al.'s scheme, the improved scheme needs more one hash function operation in the signature generation phase and one hash function operation in the message recovery phase. However, the improved scheme saves the n modular inverse operations in the message recovery phase. So the improved scheme maintains the efficiency of the Hwang et al.'s scheme.

4. Conclusion

In this letter, we give an improvement of the Hwang et al.'s authenticated encryption scheme. The improved scheme not only solves the security issue of the original scheme, but also maintains its efficiency.

References

[1] Y.M. Tseng, J.K. Jan, and H.Y. Chien, "Authenticated encryption schemes with message linkages for message flows," Computers and Electrical Engineering, vol.29, no.1, pp.101–109, 2003.

[2] M.S. Hwang, J.W. Lo, S.Y. Hsiao, and Y.P. Chu, "Improvement of authenticated encryption schemes with message linkages for message flows," IEICE Trans. Inf. & Syst., vol.E89-D, no.4, pp.1575–1577, April 2006.

[3] M. Rasslan and A. Youssef, "Cryptanalysis of Hwang-Lo-Hsiao-Chu authenticated encryption schemes," IEICE Trans. Inf. & Syst., vol.E93-D, no.5, pp.1301–1302, May 2010.

[4] C.P. Schnorr, "Efficient signature generation by smart cards," J. Cryptol., vol.4, no.3, pp.161–174, 1991.

[5] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," J. Cryptol., vol.13, no.3, pp.361–396, 2000.

[6] V. Shoup, "Sequences of games: A tool for taming complexity in security proofs," Cryptology ePrint Archive: Report 2004/332, http://eprint.iacr.org/2004/332.