Applied Mathematical Sciences, Vol. 2, 2008, no. 5, 249 - 254

A Novel (t,n) Threshold Convertible Authenticated Encryption Scheme

Han-Yu Lin and Yi-Shiung Yeh

Department of Computer Science
National Chiao Tung University
Hsinchu, 300, Taiwan, Republic of China
hanyu.cs94g@nctu.edu.tw

Abstract

Authenticated encryption schemes allow the signer to generate an authenticated ciphertext such that only the designated recipient has the ability to recover the message and verify its corresponding signature. It can be seen that authenticated encryption schemes are applicable to lots of E-Commerce applications like credit card transactions, since these schemes simultaneously fulfill the security requirements of integrity, authenticity, confidentiality and non-repudiation. For more extended applications, an alternative designed for multi-user setting is necessary. In this paper, we propose a novel group-oriented authenticated encryption scheme called the (t, n) threshold convertible authenticated encryption (TCAE) scheme. The (t, n)-TCAE scheme can allow any t or more of n signers cooperatively to produce a valid authenticated ciphertext on behalf of the original group while less than or equal to $t - 1$ can not. Further, when the case of a later dispute over repudiation occurs, the designated recipient has the ability to convert the signature into an ordinary one for convincing anyone of the signers' dishonesty.

Keywords: convertible authenticated encryption, group-oriented, threshold, discrete logarithms

1. Introduction

In 1976, Diffie and Hellman [2] introduced the first public key system based on the discrete logarithm problem (DLP) [2, 6]. Each one in the system owns a private key and its corresponding public key. It is computationally infeasible to derive the private key from its public one based on the security assumption of the DLP. With the two keys, one can perform either the public key encryption or digital signature schemes [3, 8]. As for the applications which require both functions, authenticated encryption schemes first proposed by Horster *et al.* [4] in 1994 are applicable, since such schemes simultaneously satisfy the security requirements of integrity [9], confidentiality [5], authenticity [1,9] and non-repudiation [7]. A significant property of the authenticated encryption scheme is that it allows a signer to generate an authenticated ciphertext such that only the designated recipient has the ability to recover the message and verify its corresponding signature. Yet, a later dispute that the signer disclaims having generated a signature might occur. To eliminate the weakness, in 2002, Wu and Hsu [11] proposed a convertible authenticated encryption (CAE) scheme which equipped the designated recipient with the ability to convert the signature into an ordinary one for protecting his rights or benefits.

With the rapid development of E-Commerce, group-oriented applications are getting more and more important. Those previously proposed cryptographic schemes designed for one-to-one user setting are not able to deal with the complex situation under a mode of multi-user setting. In this paper, therefore, we will elaborate on the merits of convertible authenticated encryption schemes to propose a group-oriented (t, n)-TCAE scheme as a better alternative for the applications requiring simultaneously fulfill before-mentioned security requirements. The proposed (t, n)-TCAE scheme can enable any t or more of n signers cooperatively to produce a valid authenticated ciphertext on behalf of the original group while less than or equal to $t - 1$ can not. The generated authenticated ciphertext can only be recovered and verified by the designated recipient. Further, when the case of a later dispute over repudiation occurs, the designated recipient has the ability to convert the signature into an ordinary one for convincing anyone of the signers' dishonesty.

2. (t, n)-TCAE Scheme Based on Discrete Logarithms

In this section, we propose the novel (t, n)-TCAE scheme over a finite field. The proposed scheme can be divided into three stages: signature generation, message recovery and signature verification, and signature conversion stages. There is also a system authority (SA) who is responsible for initializing the system and helping users with the generation of their key pairs. Initially, the SA chooses the following necessary parameters:

p, q : two large primes satisfying that $q \mid (p - 1)$;
g : a generator of order q over GF(p);
$h(\cdot)$: a secure one-way hash function which accepts input of any length and generates a fixed length output;
G : $= \{u_1, u_2, \ldots, u_n\}$, the group of n users;
d : the group G's private key $d \in Z_q^*$;
y_D : the group G's public key computed as

$$g^d \bmod p; \tag{1}$$

$f(x)$: $= d + d_1x + \ldots + d_{t-1}x^{t-1}$, a $t - 1$ degree polynomial where d_i's $\in Z_q$;

All the above parameters are made public except for the group G's private key d and the $t - 1$ degree polynomial $f(x)$. Then the SA distributes each user u_i's private key as $x_i = f(i)$, for $i = 1$ to n, via a secure channel. The corresponding public key of each user u_i with respect to x_i is computed as $y_i = g^{x_i}$ mod p. Details of each stage are described below:

***Signature generation stage*:** Without loss of generality, let $SG = \{u_1, u_2, \ldots, u_t\}$ be the signing group. For signing the message m (with redundancy embedded) on behalf of the original group G, each $u_i \in SG$ first computes the Lagrange coefficient [10] c_i and other parameters as follows:

$$c_i = \prod_{u_j \in SG\backslash\{u_i\}} j/(j-i) \mod q, \tag{2}$$

$$e_i = c_i \cdot x_i \mod q, \tag{3}$$

$$v_{ij} = e_i(h(y_j^{c_i} \bmod p))^{-1} \bmod p,\ u_j \in SG\backslash\{u_i\}, \tag{4}$$

$$t_i = h(e_i, h(g^{c_i} \bmod p)) \bmod q, \tag{5}$$

$$\sigma_i = c_i - x_i t_i \bmod q. \tag{6}$$

Then (v_{ij}, t_i, σ_i) is sent to $u_j \in SG\backslash\{u_i\}$. Upon receiving all (v_{ji}, t_j, σ_j)'s, $u_j \in SG\backslash\{u_i\}$, each $u_i \in SG$ further computes

$$e_j = h((g^{\sigma_j} y_j^{t_j})^{x_i} \bmod p) v_{ji} \bmod q,\ u_j \in SG\backslash\{u_i\}, \tag{7}$$

and checks whether Eq. (8) holds or not.

$$t_j = h(e_j, h(g^{\sigma_j} y_j^{t_j} \bmod p)) \bmod q,\ u_j \in SG\backslash\{u_i\}. \tag{8}$$

If the above equality holds, $u_i \in SG$ proceeds to compute $(\delta, d, C, s_1, s_2, s_3)$ as follows; else, (v_{ij}, t_i, σ_i) is requested to be sent again.

$$\delta = \sum_{u_j \in SG} \sigma_j \bmod q, \tag{9}$$

$$d = \sum_{u_j \in SG} e_j \bmod q, \tag{10}$$

$$C = y_v^{\delta} \bmod p, \tag{11}$$

$$s_1 = mh(C)^{-1} \bmod p, \tag{12}$$

where y_v is the public key of the designated recipient.

$$s_2 = h(m, h(g^{\delta} \bmod p), C) \bmod q, \tag{13}$$

$$s_3 = \delta - ds_2 \bmod q. \tag{14}$$

Here, the authenticated ciphertext for the message m is (s_1, s_2, s_3), which is then sent to the verifier u_v.

***Message recovery and signature verification stage*:** After receiving the signature,

u_v first computes C as Eq. (15) and recovers the message m with its embedded redundancy by Eq. (16).

$$C = (g^{s_3} y_D{}^{s_2})^{x_v} \bmod p, \tag{15}$$

$$m = h(C)s_1 \bmod p. \tag{16}$$

u_v finally verifies the signature (s_1, s_2, s_3) by checking Eq. (17):

$$s_2 = h(m, h(g^{s_3} y_D{}^{s_2} \bmod p), C) \bmod q. \tag{17}$$

If it holds, u_v is convinced that the signature is valid. The correctness of Eqs. (16) and (17) can be assured as the proofs of Theorems 1 and 2, respectively.

Theorem 1. The designated recipient u_v can recover the message m with its embedded redundancy with Eq. (16).

Proof: From the right-hand side of Eq. (16), we have

$$\begin{aligned}
& h(C)s_1 && \\
&= h((g^{s_3} y_D{}^{s_2})^{x_v} \bmod p)s_1 && \text{(by Eq. (15))} \\
&= h(g^{\delta - ds_2 + ds_2})^{x_v} \bmod p)s_1 && \text{(by Eqs. (14) and (1))} \\
&= h(y_v{}^{\delta} \bmod p)m(h(y_v{}^{\delta} \bmod p))^{-1} && \text{(by Eqs. (11) and (12))} \\
&= m \pmod p &&
\end{aligned}$$

which equals to the left-hand side of Eq. (16).

Q.E.D.

Theorem 2. The signature verification equation Eq. (17) works correctly.

Proof: From the right-hand side of Eq. (17), we have

$$\begin{aligned}
& h(m, h(g^{s_3} y_D{}^{s_2} \bmod p), C) && \\
&= h(m, h(g^{\delta - ds_2 + ds_2} \bmod p), C) && \text{(by Eqs. (14) and (1))} \\
&= h(m, h(g^{\delta} \bmod p), C) && \\
&= s_2 \pmod q && \text{(by Eq. (13))}
\end{aligned}$$

which equals to the left-hand side of Eq. (17).

Q.E.D.

Signature conversion stage: In case of a later dispute over repudiation, the recipient u_v can just release the recovered message m along with its converted signature (s_2, s_3). Consequently, anyone can perform Eq. (17) to realize the dishonesty of the signers.

3. Security Considerations

In this section, we will discuss some security considerations of the proposed scheme. The mathematical assumptions of our proposed scheme are the discrete logarithm problem (DLP) and the one-way hash function (OHF) [2, 6]. We analyze the security considerations from three perspectives: confidentiality, unforgeability and non-repudiation.

Confidentiality: An attacker cannot successfully retrieve the user u_i's private key x_i unless he has the ability to invert the DLP or reconstruct the $t - 1$ degree polynomial $f(x)$. To recover the message m by Eq. (16), an attacker has to retrieve the common key between the group G and u_v first. However, he cannot successfully plot the attack under the protection of the DLP and the OHF.

Unforgeability: It is computationally infeasible for an attacker to forge a valid public key under the security assumptions of the DLP. Forging a valid authenticated ciphertext (s_1', s_2', s_3') on an arbitrarily chosen message m', an attacker may first randomly choose (s_2', s_3') and then arbitrarily choose δ to derive s_1' satisfying Eq. (12). However, the randomly chosen (s_2', s_3') cannot pass the test of Eq. (17). Moreover, based on the secret polynomial $f(x)$, he cannot derive the group G's private key d to forge a valid authenticated ciphertext either. On the contrary, if the attacker attempts to forge a valid converted signature (s_2', s_3'), he may first choose a random message m' and then compute (s_2', s_3') satisfying Eq. (17). Unfortunately, he cannot make it under the protection of the DLP and the OHF. Similarly, choosing (s_2', s_3') first to compute a specific m' for satisfying Eq. (17) is not workable.

Non-repudiation: The authenticated ciphertext (s_1, s_2, s_3) generated by the signing group SG can only be verified by the designated recipient u_v. In case of a later dispute, the designated recipient u_v can announce the converted signature (s_2, s_3) with the recovered message m to convince anyone that the signature is indeed generated by the signing group SG. According to the analyses of the confidentiality of the user u_i's private key and the unforgeability of the authenticated ciphertext, any attacker cannot forge a valid signature without knowing the group private key d. Therefore, the signing group SG cannot deny their signatures.

From above discussions, it can be seen that our proposed scheme is secure against well-known active attacks based on the assumptions of DLP and OHF.

4. Conclusions

In this paper, we have proposed a novel (t, n)-TCAE scheme based on discrete logarithms. A significant characteristic of its design is the multi-user setting which can provide crucial benefits to those group-oriented applications requiring simultaneously satisfy the security requirements of integrity, authenticity, confidentiality and no-repudiation. We also demonstrated the correctness of the proposed scheme and analyzed its security against some well-known active attacks. In addition, when the case of a later dispute over repudiation occurs, the designated recipient has the ability to convert the signature into an ordinary one for convincing anyone of the signers' dishonesty.

References

[1] B.F. Cooper, M. Bawa, N. Daswani, S. Marti, H. Garcia-Molina, Authenticity and availability in PIPE networks, Future Generation Computer Systems 21 (3) (2005) 391-400.

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

[3] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory IT-31 (4) (1985) 469-472.

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

[5] F. Hou, Z. Wang, Y. Tang, Z. Liu, Protecting integrity and confidentiality for data communication, Proceedings of Ninth International Symposium on Computers and Communications (ISCC) 1 (28) (2004) 357-362.

[6] A. Menezes, P. Oorschot, S. Vanstone, Handbook of applied cryptography, CRC Press, Inc., 1997.

[7] B. Meng, S. Wang, Q. Xiong, A fair non-repudiation protocol, The 7th International Conference on Computer Supported Cooperative Work in Design, 2002, pp. 68-73.

[8] R. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM 21 (2) (1978) 120-126.

[9] W. Stallings, Cryptography and network security: principles and practices, 3rd. Ed., Prentice Hall, 2002.

[10] B. Wendroff, Theoretical Numerical Analysis, Academic Press Inc., 1996.

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

Received: July 17, 2007