Group-Oriented Convertible Authenticated Encryption Scheme with (t, n) Shared Verification

Han-Yu Lin[1,*], Tzong-Sun Wu[2], Ting-Yu Huang[1] and Tzu-Chiang Lin[1]
(林韓禹　吳宗杉　黃定宇　林子強)
[1] Department of Computer Science
National Chiao Tung University
Hsinchu, 300, Taiwan
[2] Department of Computer Science and Engineering
National Taiwan Ocean University
Keelung, 202, Taiwan
[*] hanyu.cs94g@nctu.edu.tw

Abstract

Conventional authenticated encryption (AE) schemes put emphasis on the one-to-one setting, which allow one signer to produce an authenticated ciphertext such that only the designated recipient can recover the message and verify its corresponding signature. To meet the need of diversified applications which require simultaneously fulfilling the security requirements of integrity, authenticity, confidentiality and non-repudiation, this paper presents a group-oriented convertible authenticated encryption (CAE) scheme with (*t*, *n*) shared verification. Designed mainly for the multi-user setting, the proposed scheme enables one signer to send a confidential message along with the signature to the designated group of *n* recipients. Any *t* or more of *n* designated recipients can cooperatively recover the message and verify its signature while less than or equal to $t - 1$ can not. Moreover, in case of a later dispute over repudiation, the designated group of recipients has the ability to convert the signature into an ordinary one for convincing anyone of the signer's dishonesty.

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

摘要

傳統鑑別加密方法著重於一對一的設置，其允許一位簽署者產生鑑別加密訊息，此訊息只有該特定接收者能回復原始訊息並驗證其簽章。爲滿足更多樣化，且同時達到完整性、鑑別性、機密性與不可否認性等安全性要求的運用需求，本論文提出一(*t*, *n*)共享驗證之群體導向可轉換鑑別加密方法。以多人設置為主要設計考量，本方法允許一位簽署者傳送秘密訊息與其簽章給一群由 *n* 位特定接收者所組成的群體。此群體中任意 *t* 位或以上的特定接收者即可共同回復原始訊息並驗證簽章，而 $t-1$ 位或更少則無法完成。此外，當發生事後否認的爭議時，該特定接收群體亦具備將此簽章轉換成一般簽章的能力，可使任意第三者信服簽署者的不誠實行為。

關鍵詞：群體導向、可轉換鑑別加密、門檻式、離散對數。

1. Introduction

The public key encryption and digital signature schemes [4, 11] are two vital functions of the public key cryptosystem which was first introduced by Diffie and Hellman [3] in 1976. Based on the intractability of solving the discrete logarithm problem (DLP) [3, 9], the public key system equips each user a self-chosen private key and the corresponding public key stored in the public key directory which is accessible to anyone. It is computationally infeasible for any malicious adversary to derive the private key from its known public one. When communicating over an insecure channel like the Internet, a sender can deliver a message encrypted with the receiver's public key to the destination such that only the intended receiver can decrypt the ciphertext with his own private key and then read the message. On the contrary, the digital signature for the message is produced with the sender's private key and is publicly verifiable with the sender's public key. It can be seen that the public key encryption fulfills the security requirements of confidentiality [6] while digital signature schemes satisfy those of integrity [12], authenticity [2, 12] and non-repudiation [10].

As to simultaneously fulfilling the above four security requirements, a flat-out way would be the conventional two-step approach [13], i.e., first sign then encrypt. However, the approach is inefficient since the cost is equal to the sum of both. To obtain better efficiency, an authenticated encryption (AE) scheme was proposed by Horster *et al*. [5] in 1994. AE schemes enable 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. Yet, a later dispute that the signer repudiates his signatures might occur. To eliminate the drawback, in 1999, Araki *et al*. [1] proposed a convertible limited verifier signature scheme which provided the signature conversion mechanism to deal with the dispute over repudiation. In 2002, Wu and Hsu [15] further proposed a convertible authenticated encryption (CAE) scheme in which the signature conversion process was rather simple and could be solely done by the designated recipient. Lv *et al*. [8] also proposed a more secure and practical CAE scheme in 2005.

With the diversified development of E-Commerce, group-oriented applications have played an important role in the modern society. To facilitate those gradually important group-oriented applications which require simultaneously satisfying all the before-mentioned security requirements, this paper elaborates on the merits of conventional CAE schemes to propose a group-oriented CAE scheme with (t, n) shared verification. The proposed scheme enables one signer to generate an authenticated ciphertext such that any t or more of n designated recipients can cooperatively recover the message and verify the signature while less than or equal to $t - 1$ can not. Further, when the case of a later dispute over repudiation occurs, the designated group of recipients has the ability to convert the signature into an ordinary one for convincing anyone of the signers' dishonesty.

The rest of this paper is organized as follows. Section 2 presents the group-oriented CAE scheme with (t, n) shared verification. The security considerations of our proposed scheme and comparisons with other previous works are given in Section 3. Finally, we make some conclusions with respect to the significance of the proposed scheme in Section 4.

2. The Proposed Scheme Based on Discrete Logarithms

In this section, we introduce the group-oriented CAE scheme with (t, n) shared verification over a finite field. The proposed scheme is divided into three stages: the signature generation, the message recovery and signature verification, and the signature conversion stages. Initially, a trusted system authority (SA) will choose the following necessary parameters and help each user with the generation of his key pair:

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

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

$f(x)$: $= d + d_1 x + \ldots + d_{t-1} x^{t-1}$, a $t-1$ degree polynomial where d_i's $\in Z_q$;

Note that the group G's private key d and the $t-1$ degree polynomial $f(x)$ are kept secret while others are made public. Each user u_i's private key is derived by the SA as $x_i = f(i)$, for $i = 1$ to n, and then distributed to u_i via a secure channel. The corresponding public key of u_i with respect to x_i is computed as $y_i = g^{x_i} \bmod p$. Details of each stage are described as follows:

***The signature generation stage*:** For signing the message m with redundancy embedded, the signer u_a first chooses an integer $k \in Z_q^*$ and then computes

$$C = y_D{}^k \bmod p, \tag{2}$$

$$s_1 = mh(C)^{-1} \bmod p, \tag{3}$$

$$s_2 = h(m, h(g^k \bmod p), C) \bmod q, \tag{4}$$

$$s_3 = k - x_a s_2 \bmod q. \tag{5}$$

Here, the authenticated ciphertext for the message m is (s_1, s_2, s_3) which is then sent to the group G of designated recipients.

***The message recovery and signature verification stage*:** Without loss of generality, let $VG = \{u_1, u_2, \ldots, u_t\}$ be the verifying group of t designated recipients who will cooperatively recover the message m and verify its signature on behalf of the original group G. Upon receiving the signature, each $u_i \in VG$ first computes the Lagrange coefficient [14] c_i and some other parameters as follows:

$$c_i = \prod_{u_j \in VG \setminus \{u_i\}} j/(j-i) \mod q, \tag{6}$$

$$e_i = c_i \cdot x_i \bmod q, \tag{7}$$

$$v_{ij} = e_i (h(y_j{}^{c_i} \bmod p))^{-1} \bmod p,\ u_j \in VG \setminus \{u_i\}, \tag{8}$$

$$t_i = h(e_i, h(g^{c_i} \bmod p)) \bmod q, \tag{9}$$

$$\sigma_i = c_i - x_i t_i \bmod q. \tag{10}$$

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

$$e_j = h((g^{\sigma_j} y_j{}^{t_j})^{x_i} \bmod p) v_{ji} \bmod q,\ u_j \in VG \setminus \{u_i\}, \tag{11}$$

and checks whether Eq. (12) holds or not.

$$t_j = h(e_j, h(g^{\sigma_j} y_j{}^{t_j} \bmod p)) \bmod q,\ u_j \in VG \setminus \{u_i\}. \tag{12}$$

If the above equality holds, $u_i \in VG$ computes C' and recovers the message as Eqs. (13) and (14); else, (v_{ij}, t_i, σ_i) is requested to be sent again.

$$C' = \prod_{u_j \in VG} (g^{s_3} {y_a}^{s_2})^{e_j} \bmod p, \quad (13)$$

$$m = h(C')s_1 \bmod p. \quad (14)$$

$u_i \in VG$ finally verifies the signature (s_1, s_2, s_3) by checking Eq. (15):

$$s_2 = h(m, h(g^{s_3} {y_a}^{s_2} \bmod p), C') \bmod q. \quad (15)$$

If it holds, $u_i \in VG$ is convinced that the signature is valid. The correctness of Eqs. (14) and (15) can be assured as the proofs of Theorems 1 and 2, respectively.

Theorem 1. $u_i \in VG$ can recover the message m with its embedded redundancy by Eq. (14).

Proof: From the right-hand side of Eq. (14), we have

$$\begin{aligned} & h(C')s_1 \\ &= h(\prod_{u_j \in VG} (g^{s_3} {y_a}^{s_2})^{e_j})s_1 && \text{(by Eq. (13))} \\ &= h(\prod_{u_j \in VG} (g^{k - x_a s_2} g^{x_a s_2})^{e_j})s_1 && \text{(by Eq. (5))} \\ &= h(\prod_{u_j \in VG} (g^k)^{c_j x_j}) m(h({y_D}^k \bmod p))^{-1} \\ & && \text{(by Eqs. (3) and (7))} \\ &= h(g^{kd}) m(h({y_D}^k \bmod p))^{-1} \\ & && \text{(by Lagrange Interpolation [14])} \\ &= h({y_D}^k) m(h({y_D}^k \bmod p))^{-1} && \text{(by Eq. (1))} \\ &= m \pmod p \end{aligned}$$

which equals to the left-hand side of Eq. (14).

Q.E.D.

Theorem 2. $u_i \in VG$ can verify the signature by checking Eq. (15).

Proof: From the right-hand side of Eq. (15), we have

$$\begin{aligned} & h(m, h(g^{s_3} {y_a}^{s_2} \bmod p), C') \\ &= h(m, h(g^{k - x_a s_2} g^{x_a s_2} \bmod p), C') && \text{(by Eq. (5))} \\ &= h(m, h(g^k \bmod p), C') \\ &= s_2 \pmod q && \text{(by Eq. (4))} \end{aligned}$$

which equals to the left-hand side of Eq. (15).

Q.E.D.

The signature conversion stage: In case of a later dispute over repudiation, the designated group VG can convince anyone that the resulted signature is u_a's signature indeed by revealing the recovered message m and its converted signature (s_2, s_3). With the help of Eq. (15), anyone can realize the signer's dishonesty.

3. Security Considerations and Comparisons

In this section, we will discuss some security considerations of the proposed scheme followed by the comparisons with several previous works.

3.1. Security Considerations

The subsection talks about some security considerations of the proposed scheme. The security assumptions of our proposed scheme are the discrete logarithm problem (DLP) and the one-way hash function (OHF) [3, 9]. The definition of DLP is briefly restated below: Let p be a large prime, g a generator, and α a random integer. It is computationally infeasible to derive α from known (g, $g^{\alpha} \bmod p$). In the following, we analyze the security considerations in terms of confidentiality, unforgeability and non-repudiation.

Confidentiality

Consider the attack that a malicious adversary attempts to derive the user u_i's private key x_i from the corresponding known public key y_i directly. However, he will face the difficulty in solving the DLP and fail to make it. As to computing the private key x_i from the $t - 1$ degree polynomial $f(x)$, he has to know the secret polynomial $f(x)$ first by reconstructing it. Unfortunately, the secret polynomial $f(x)$ can only be cooperatively reconstructed by any t or more of n legitimate users. Thus, any adversary can not successfully derive u_i's private key x_i under the protection of the DLP and the secret polynomial $f(x)$.

If the attacker tries to recover the message m by Eq. (14), he will make it unless he can retrieve the common key between the group G and u_a first. However, he cannot successfully plot the attack under the protection of the DLP and the OHF.

Unforgeability

The unforgeability of each u_i's public key is based on the security assumption of the DLP. If an attacker attempts to forge a valid authenticated ciphertext (s_1', s_2', s_3') on his arbitrarily chosen message m', he has to derive s_1' fulfilling Eq. (14) by first randomly choosing (s_2', s_3', e_j's). Yet, the randomly chosen (s_2', s_3') cannot pass the test of Eq. (15). Further, it is computationally infeasible to derive the signer u_a's private key x_a for forging a valid authenticated ciphertext based on the intractability of solving the DLP and the secret polynomial $f(x)$. As to forging a valid converted signature (s_2', s_3'), an attacker has to compute (s_2', s_3') satisfying Eq. (15) by first choosing a random message m'. Unfortunately, he will face the difficulty in inverting the DLP and the OHF, and vice versa.

Non-repudiation

The authenticated ciphertext (s_1, s_2, s_3) produced by the signer u_a can only be verified by the group *VG* of *t* designated recipients instead of anyone else for the purpose of confidentiality. When the case of a later dispute over repudiation occurs, the designated group *VG* can convince anyone of the signer u_a's dishonesty by simply announcing the converted signature (s_2, s_3) with the recovered message *m*. Consequently, anyone can perform the signature verification equation Eq. (15) to arbitrate the dispute. According to the above analyses of the confidentiality of the user u_i's private key and the unforgeability of the authenticated ciphertext, any malicious adversary cannot successfully forge a valid authenticated ciphertext without knowing the signer u_a's private key x_a. Hence, the signer u_a cannot deny his signatures.

From the above security discussions in terms of confidentiality, unforgeability and non-repudiation, it can be seen that our proposed scheme is secure against known active attacks on condition that the security assumptions of the DLP and the OHF are intractable.

3.2. Comparisons

We compare the proposed scheme (LWHH for short) with several previously proposed ones including the Hsu-Wu scheme (HW for short) [7], Araki *et al.*'s scheme (AUI for short) [1] and Lv *et al.*'s scheme (LWK for short) [8] in terms of some cryptographic properties. The comparisons are shown as Table 1.

Table 1. Comparisons among previous works and the proposed scheme

Schemes / Properties	LWHH	HW	AUI	LWK
Multi-user setting	O	O	×	×
Convertible signature	O	×	O	O
No extra conversion cost	O	×	×	O

4. Conclusions

In this paper, we have proposed a group-oriented CAE scheme with (*t*, *n*) shared verification for facilitating the gradually wide applications which has to simultaneously satisfy the security requirements of integrity, authenticity, confidentiality and non-repudiation. Instead of the conventional one-to-one setting, the proposed scheme enables one signer to generate an authenticated ciphertext such that any *t* or more of *n* recipients can cooperatively recover the message and verify the corresponding signature while less than or equal to $t - 1$ can not. In case of a later dispute over repudiation, the designated group has the ability to convert the signature into an ordinary one for convincing anyone of the signer's dishonesty. In addition, we also proved the correctness of the proposed scheme and analyzed its security against known active attacks.

References

[1] S. Araki, S. Uehara and K. Imamura, "The limited verifier signature and its application," IEICE Transactions on Fundamentals, Vol. E82-A, No. 1, pp. 63-68, 1999.

[2] B. F. Cooper, M. Bawa, N. Daswani, S. Marti and H. Garcia-Molina, "Authenticity and availability in PIPE networks," Future Generation Computer Systems, Vol. 21, No. 3, pp. 391-400, 2005.

[3] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, Vol. IT-22, No. 6, pp. 644-654, 1976.

[4] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Transactions on Information Theory, Vol. IT-31, No. 4, pp. 469-472, 1985.

[5] P. Horster, M. Michel and H. Peterson, "Authenticated encryption schemes with low communication costs," Electronics letters, Vol. 30, No. 15, pp. 1212-1213, 1994.

[6] F. Hou, Z. Wang, Y. Tang and Z. Liu, "Protecting integrity and confidentiality for data communication," Proceedings of Ninth International Symposium on Computers and Communications (ISCC), Vol. 1, No. 28, pp. 357-362, 2004.

[7] C. L. Hsu and T. C. Wu, "Authenticated encryption scheme with (t, n) shared verification," IEE Proceedings Computers and Digital Techniques, Vol. 145, No. 2, pp. 117-120, March 1998.

[8] J. Lv, X. Wang and K. Kim, "Practical convertible authenticated encryption schemes using self-certified public keys," Applied Mathematics and Computation, Vol. 169, No. 2, pp. 1285-1297, 2005.

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

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

[11] R. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, Vol. 21, No. 2, pp. 120-126, 1978.

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

[13] VISA and MasterCard Inc., Secure Electronic Transaction (SET) Specification, Version 1.0, 1997.
[14] B. Wendroff, Theoretical Numerical Analysis, Academic Press Inc., 1996.
[15] T. S. Wu and C. L. Hsu, “Convertible authenticated encryption scheme,” The Journal of Systems and Software, Vol. 62, No. 3, pp. 205-209, 2002.