New Efficient Identity-Based Key-Insulated Multisignature Scheme

Han-Yu Lin, Tzong-Sun Wu, Ming-Lun Lee, and Chi-Kuang Yeh

***Abstract*—We propose a new efficient identity-based key-insulted multisignature scheme for facilitating group-oriented applications and mitigating the impact of key exposure. Integrated with identity-based systems, the proposed scheme adopts explicitly verifiable public keys without additional certificate. Each user can also periodically update his private key while the public one remains unchanged. In the proposed scheme, a valid key-insulted multisignature must be cooperatively generated by all signers. Our scheme has the properties of unbounded time periods and random-access key-updates. We also demonstrate that our scheme has better efficiency as compared with previous works and formally prove its security of unforgeability against existential forgery under adaptive chosen-message attacks (EF-CMA) in the random oracle model.**

***Index Terms*—Identity-based, key-insulted, multi-signature, key exposure, bilinear pairing.**

I. INTRODUCTION

In 1976, Diffie and Hellman [1] introduced the public key cryptosystem in which each user first chooses a private key and then computes the corresponding public one. The former is kept secret while the latter is stored in a public directory and accessible to anyone. Two fundamental functions of the public key systems are encryption and digital signature. Encryption protects confidentiality [2] and digital signature ensures integrity, authenticity and non-repudiation [3]. So far, lots of digital signature variants have been proposed, which include multi-signatures [4]–[7], proxy signatures [8], [9], designated verifier signatures [10], [11], etc. Since the public keys are open, a malicious adversary can plot the well-known substitution attack to replace someone's public key with a fake one. To withstand the attack, one should first verify the corresponding public key certificate for obtained public keys. However, some extra communication and computation costs would incur due to the transmission and verification of public key certificates.

In 1984, Shamir [12] introduced the first identity-based system in which each user's public key is straightly his identification information such as name, address and so on. Consequently, the public key can be explicitly verified without accompanying a corresponding public key certificate. In such a system, a system authority (SA) is responsible for issuing everyone's private keys. When a private key is accidentally compromised, all encrypted ciphertexts protected by the private key will no longer be confidential.

To deal with the key exposure problem, Dodis *et al.* [13], [14] proposed the so-called key-insulted cryptosystems in which every user can periodically update his short-term private key for performing all kinds of cryptographic mechanisms such as encryptions and digital signatures [15]–[17]. Each user also owns a physically-secure but computation limited device called base or helper which stores a long-term private key. The helper assists each user with the short-term private key update procedure. It thus can be seen that an adversary having the knowledge of someone's private key associated with the time period i cannot decrypt any message of different time periods. Combining with identity-based systems and pairing-based systems, in 2005, Hanaoka *et al.* [18] addressed the first identity-based key-insulted encryption (IB-KIE) and its applications based on bilinear pairings. The next year, Zhou *et al.* [19] presented an identity-based key-insulated signature (IB-KIS) scheme. Both of Hanaoka *et al.*'s and Zhou *et al.*'s schemes are proved secure in the random oracle model.

Further consider the security of helper which stores the long-term private key, Hanaoka *et al.* [20] utilized two independent helps to construct a so-called parallel KIE. The two helpers are adopted alternatively to assist with the short-term private key update procedure. In 2008, Weng *et al.* [21] further came up with an identity-based (k, n) threshold KIE scheme in which n helpers are adopted. When a user attempts to update his short-term private key, at least k helpers are sufficient to perform the key-update procedure while less than or equal to $k - 1$ cannot.

Recently, Wu *et al.* [22] proposed an IB-KIS scheme with batch verification from pairings. The key-update procedure of their scheme is efficient as compared with previous works. They also introduced a new application for their proposed scheme, called full delegation proxy signature scheme with time restriction. For facilitating group-oriented applications and mitigate the impact of key exposure problems, in this paper, we incorporate the key-update procedure of Wu *et al.*'s scheme to propose a new identity-based key-insulted multi-signature (IB-KIMS) scheme with provable security.

II. PROPOSED IB-KIMS SCHEME

We adopt the key update mechanism in Wu *et al.*'s [22] scheme to further construct our IB-KIMS scheme from pairings. Details of each phases are described below:

–Setup: Taking as input 1^k, the private key generation

Manuscript received November 13, 2012; revised January 8, 2013. This work was supported in part by the National Science Council of Republic of China under the contract number NSC 101-2218-E-019-005.

H. Y. Lin, T. S. Wu and C. K. Yeh are with the Department of Computer Science and Engineering, National Taiwan Ocean University, Taiwan (e-mail: hanyu@mail.ntou.edu.tw).

DOI: 10.7763/IJMLC.2013.V3.284

center (PKG) chooses a master secret key $s \in_R Z_q$ along with a master helper key $w \in_R Z_q$, and then computes the corresponding public keys $P_{TA} = sP$ and $P_{HK} = wP$, respectively. The master helper key w is sent to the helper via a secure channel. The PKG also selects two groups ($\boldsymbol{G}_1$, +) and ($\boldsymbol{G}_2$, ×) of the same prime order q where $|q| = k$. Let P be a generator of order q over $\boldsymbol{G}_1$, e: $\boldsymbol{G}_1 \times \boldsymbol{G}_1 \rightarrow \boldsymbol{G}_2$ a bilinear pairing, H: $\{0, 1\}^k \rightarrow \boldsymbol{G}_1$ and F: $\{0, 1\}^k \times Z_q \times \boldsymbol{G}_1 \times \boldsymbol{G}_2 \rightarrow Z_q$ collision resistant hash functions. The PKG announces public parameters $params = \{P_{TA}, P_{HK}, \boldsymbol{G}_1, \boldsymbol{G}_2, q, P, e, H, F\}$.

–KeyExtract (KE): Without loss of generality, let $A = \{A_1, A_2, \ldots, A_n\}$ be a group of n signers. Given an identity, say ID_{A_j} of the user A_j, the PKG computes the initial private key as

$$S_{A_j,\ 0} = sH(ID_{A_j}) + wH(ID_{A_j},\ 0), \quad (1)$$

and then returns it to A_j via a secure channel. The corresponding public key is computed as $\sigma_{A_j} = e(P_{TA}, H(ID_{A_j}))$.

– KeyUpdate (KU): Given an identity ID_{A_j} and a time period $i \in \{1, \ldots, N\}$, the helper first generates a helper key as

$$HK_{A_j,\ i} = w[H(ID_{A_j},\ i) - H(ID_{A_j},\ i - 1)] \quad (2)$$

and then Alice can update her private key by computing

$$S_{A_j,\ i} = S_{A_j,\ i-1} + HK_{A_j,\ i}.$$

The values $(S_{A_j, i-1}, HK_{A_j, i})$ are deleted subsequently.

– Multi-Signature-Generation (MSG): At the time period $i \in \{1, \ldots, N\}$, to sign a message M, each signer A_j first chooses $r_j \in_R Z_q$ and then computes

$$R_j = r_j P, \quad (4)$$

$$d_{A_j} = \sigma_{A_j}{}^{r_j} \cdot e(P_{HK},\ r_j H(ID_{A_j},\ i)), \quad (5)$$

and sends (R_j, d_{A_j}) to the clerk who can be any signer of the group A. Upon receiving all (R_j, d_{A_j})'s, the clerk computes

$$R = \sum\nolimits_{j=1}^{n} R_j\ , \quad (6)$$

$$d_A = \prod\nolimits_{j=1}^{n} d_{A_j}\ , \quad (7)$$

and then returns (R, d_A) to each A_j. After receing it, each A_j computes

$$Q_j = (r_j + F(i,\ M,\ R,\ d_A))S_{A_j,\ i} \quad (8)$$

which is then delivered to the clerk. When all Q_j's are received, the clerk comptues

$$Q = \sum\nolimits_{j=1}^{n} Q_j\ , \quad (9)$$

The key-insulated multi-signature for M is $\delta = (i, R, Q, d_A)$. Anyone can verify it by checking if

$$e(P, Q) = d_A \cdot [\prod\nolimits_{j=1}^{n} \sigma_{A_j} \; e(P_{HK}, \sum\nolimits_{j=1}^{n} H(ID_{A_j}, i))]^{F(i, M, R, d_A)}. \quad (10)$$

We demonstrate the correctness of Eq. (10). From the left-hand side of Eq. (10), we have

$$\begin{aligned}
& e(P, Q) \\
&= e(P, \sum\nolimits_{j=1}^{n} (r_j + F(i, M, R, d_A))S_{A_j, i}) \qquad \text{(by Eqs. (8) and (9))} \\
&= e(P, \sum\nolimits_{j=1}^{n} (r_j + F(i, M, R, d_A))(sH(ID_{A_j}) + wH(ID_{A_j}, i))) \qquad \text{(by Eq. (1))} \\
&= e(P, \sum\nolimits_{j=1}^{n} (r_j + F(i, M, R, d_A))(sH(ID_{A_j}))) \; e(P, \sum\nolimits_{j=1}^{n} (r_j + F(i, M, R, d_A))(wH(ID_{A_j}, i))) \\
&= e(P, \sum\nolimits_{j=1}^{n} r_j sH(ID_{A_j}))e(P, F(i, M, R, d_A) \sum\nolimits_{j=1}^{n} (sH(ID_{A_j})))e(P, \sum\nolimits_{j=1}^{n} r_j wH(ID_{A_j}, i)) \; e(P, F(i, M, R, d_A) \sum\nolimits_{j=1}^{n} (wH(ID_{A_j}, i))) \\
&= \prod\nolimits_{j=1}^{n} \sigma_{A_j}{}^{r_j} \cdot \sigma_{A_j}{}^{F(i, M, R, d_A)} \; e(P_{HK}, \sum\nolimits_{j=1}^{n} r_j H(ID_{A_j}, i))e(P_{HK}, F(i, M, R, d_A) \sum\nolimits_{j=1}^{n} H(ID_{A_j}, i)) \\
&= \prod\nolimits_{j=1}^{n} d_{A_j} \cdot \sigma_{A_j}{}^{F(i, M, R, d_A)} e(P_{HK}, F(i, M, R, d_A) \sum\nolimits_{j=1}^{n} H(ID_{A_j}, i)) \qquad \text{(by Eq. (5))} \\
&= d_A \cdot [\prod\nolimits_{j=1}^{n} \sigma_{A_j} \; e(P_{HK}, \sum\nolimits_{j=1}^{n} H(ID_{A_j}, i))]^{F(i, M, R, d_A)}
\end{aligned}$$

which leads to the right-hand side of Eq. (10).

III. Security Proof

The crucial security requirements of proposed IB-KIMS scheme is unforgeability against existential forgery under adaptive chosen-message attacks (EF-CMA). In this section, we first briefly review some security notions along with related computational assumptions [2, 23] and then prove that the proposed scheme achieves the EF-CMA security in the random oracle model as Theorem 1.

A. Bilinear Diffie-Hellman Problem; BDHP

Let ($\boldsymbol{G}_1$, +) and ($\boldsymbol{G}_2$, ×) denote two groups of the same prime order q and e: $\boldsymbol{G}_1 \times \boldsymbol{G}_1 \rightarrow \boldsymbol{G}_2$ a bilinear map. The BDHP is, given an instance $(P, A, B, C) \in \boldsymbol{G}_1{}^4$ where P is a generator, $A = aP$, $B = bP$ and $C = cP$ for some $a, b, c \in Z_q$, it is computationally infeasible to compute $e(P, P)^{abc} \in \boldsymbol{G}_2$.

B. Computational Diffie-Hellman Problem; CDHP

Let P be a generator of $\boldsymbol{G}_1$. The computational

Diffie-Hellman problem is, given an instance (P, aP, bP) for some $a, b \in Z_q$, it is computationally infeasible to derive abP.

Theorem 1. (Proof of Unforgeability) The proposed IB-KIMS scheme is secure against existential forgery under adaptive chosen-message attacks (EF-CMA) in the random oracle model if there is no probabilistic polynomial-time adversary that can break the CDHP with a non-negligible probability.

Proof: We use the Forking Lemma introduced by Pointcheval and Stern [24] to prove this theorem. Suppose that a probabilistic polynomial-time adversary $\mathcal{A}$ can break the proposed IB-KIMS scheme with an non-negligible advantage under the adaptive chosen-message attack after asking at most q_H H, q_F F, q_{KE} KE, q_{HK} HK, q_{KU} KU and q_{MSG} MSG queries. Then we will be able to take $\mathcal{A}$ as a subroutine to construct another algorithm $\mathcal{B}$ breaking the CDHP. Given (P, xP, yP) as inputs, the objective of $\mathcal{B}$ is to derive xyP. In this proof, $\mathcal{B}$ simulates a challenger to $\mathcal{A}$ in the following game.

Setup: The challenger $\mathcal{B}$ runs the Setup(1^k) algorithm to obtain the system's public parameters $params = \{\boldsymbol{G}_1, \boldsymbol{G}_2, q, P, e\}$ and comes up with a random tape composed of a long sequence of random bits. Then $\mathcal{B}$ sets $P_{TA} = uP$ and $P_{HK} = xP$ where $u \in_R Z_q$. After that, $\mathcal{B}$ simulates two runs of the proposed scheme to the adversary $\mathcal{A}$ on input ($params$, P_{TA}, P_{HK}) and the random tape.

Phase 1: $\mathcal{A}$ makes the following queries adaptively:

–*H oracle:* When $\mathcal{A}$ queries an H oracle of $H(ID_{A_j})$, $\mathcal{B}$ first checks the H_list for a matched entry. Otherwise, $\mathcal{B}$ chooses $h_{A_j} \in_R Z_q$, adds the entry (ID_{A_j}, h_{A_j}, $h_{A_j}P$) to the H_list, and returns $h_{A_j}P$ as a result. Note that when $\mathcal{A}$ queries an H oracle of $H(ID_{A_1}, i)$, $\mathcal{B}$ returns yP. When $\mathcal{A}$ makes an HK query for ($i + 1$, ID_{A_1}), $\mathcal{B}$ directly terminates.

–*F oracle:* When $\mathcal{A}$ queries an F oracle of $F(i, M, R, d_A)$, $\mathcal{B}$ first checks the F_list for a matched entry. Otherwise, $\mathcal{B}$ chooses $f \in_R Z_q$ and adds the entry (i, M, R, d_A, f) to the F_list. Finally, $\mathcal{B}$ returns f as a result.

–*KE queries:* When $\mathcal{A}$ makes a KE query for ID_{A_j}, $\mathcal{B}$ returns the initial private key $S_{A_j, 0} = h_{A_j}(uP) + (h_{A_j, 0})xP$ to $\mathcal{A}$.

–*HK queries:* When $\mathcal{A}$ makes an HK query for (i, ID_{A_j}) where $i \in \{1, \ldots, N\}$ is the time period, $\mathcal{B}$ returns the helper key $HK_{A_j, i} = (h_{A_j, i})xP - (h_{A_j, i-1})xP$ to $\mathcal{A}$.

–*KU queries:* When $\mathcal{A}$ makes a KU query for (i, ID_{A_j}) where $i \in \{1, \ldots, N\}$ is the time period, $\mathcal{B}$ returns the corresponding private key $S_{A_j, i} = h_{A_j}(uP) + (h_{A_j, i})xP$ to $\mathcal{A}$.

–*MSG queries:* When $\mathcal{A}$ makes an MSG query with respect to (i, M, ID_{A_1}, ID_{A_2}, …, ID_{A_n}) where $i \in \{1, \ldots, N\}$ is the time period, $\mathcal{B}$ runs the MSG algorithm with the derived private key $S_{A_j, i} = h_{A_j}(uP) + (h_{A_j, i})xP$ and then returns the corresponding multi-signature $\delta = (i, R, Q, d_A)$.

Analysis of the game: In the second round, $\mathcal{B}$ again runs $\mathcal{A}$ on input ($params$, $P_{TA} = uP$, $P_{HK} = xP$) and the same random tape. Since the adversary $\mathcal{A}$ is given the same sequence of random bits, we can anticipate that $\mathcal{A}$ always asks the same queries as those in the first simulation. $\mathcal{B}$ directly returns identical results as those he responds in the first time until $\mathcal{A}$ makes the $F(i^*, M^*, R^*, d_A^*)$ query. At this time, $\mathcal{B}$ gives another answer $f^{**} \in_R Z_q$ rather than original f^*. Meanwhile, $\mathcal{A}$ is then supplied with a different random tape which also consists of a long sequence of random bits. According to the "Forking lemma", when $\mathcal{A}$ finally makes another valid forgery $\delta^{**} = (i^*, R^*, Q^{**}, d_A^*)$ where $F(i^*, M^*, R^*, d_A^*) \neq F'(i^*, M^*, R^*, d_A^*)$, $ID_{A_1}^* = ID_{A_1}$ and $i^* = i$, $\mathcal{B}$ could obtain

$$e(P, Q^*) = d_A^* \cdot [\prod_{j=1}^{n} \sigma_{A_j}^* \cdot e(P_{HK}, \sum_{j=1}^{n} H(ID_{A_j}^*, i^*))]^{f^*},$$

$$e(P, Q^{**}) = d_A^* \cdot [\prod_{j=1}^{n} \sigma_{A_j}^* \cdot e(P_{HK}, \sum_{j=1}^{n} H(ID_{A_j}^*, i^*))]^{f^{**}}.$$

Combining the above two equalities, we have

$$e(P, Q^* - Q^{**}) = [\prod_{j=1}^{n} \sigma_{A_j}^* \cdot e(P_{HK}, \sum_{j=1}^{n} H(ID_{A_j}^*, i^*))]^{(f^* - f^{**})}$$
$$= [e(uP, \sum_{j=1}^{n} (h_{A_j^*})P)e(xP, yP) \; e(xP, \sum_{j=2}^{n} (h_{A_j}^*, {}_{i^*})P)]^{(f^* - f^{**})}$$

which implies

$$[e(P, (Q^* - Q^{**}) - (f^* - f^{**})u \sum_{j=1}^{n} (h_{A_j^*})P)] = [e(P, xyP + \sum_{j=2}^{n} (h_{A_j}^*, {}_{i^*})xP)]^{(f^* - f^{**})}.$$

Consequently, $\mathcal{B}$ could solve the CDHP by computing

$$xyP = (f^* - f^{**})^{-1}[(Q^* - Q^{**}) - (f^* - f^{**})u \sum_{j=1}^{n} (h_{A_j^*})P] - \sum_{j=2}^{n} (h_{A_j}^*, {}_{i^*})xP.$$

Q.E.D.

Table I summarizes the functional and computational analyses among the proposed and previous works including the Ma-He [6] (MH for short) and Reddy *et al.*' [7] (RRG for short) schemes. The computational costs are evaluated by the number of required bilinear pairing. From the table, one can observe that the proposed scheme not only has lower computational efforts, but also can effectively reduce the impact caused by key exposure.

TABLE I: COMPARISONS OF FUNCTIONALITY AND COMPUTATION COSTS

Item \ Scheme	MH	RRG	Ours
Key-insulted signature	X	X	O
Computational costs (#bilinear pairings)*	$4n + 4$	$4n + 3$	$n + 2$

Remark: n is the number of signers. To obtain a fair comparison results, the costs for key pair generation and verification of all evaluated schemes are ignored.

IV. Conclusions

Key exposure is considered the most serious attack against identity-based systems, as the compromised private key cannot be used anymore, which also means the corresponding user has to be deleted from the system. For solving the problem and facilitating group-oriented applications, in this paper, we combined key-insulated systems and the multi-signature scheme to propose an efficient identity-based key-insulted multi-signature (IB-KIMS) scheme from pairings. Inherited from key-insulted systems, our scheme enables each user to periodically update his short-term private key with the assistance of his helper while the corresponding public key remains unchanged. Extra properties of the proposed scheme include unbounded time periods and random-access key-updates. Compared with previous multi-signature schemes, ours not only has better functionalities, but also lower computational costs. Moreover, we also proved the crucial security of EF-CMA for our scheme in the random oracle model.

References

[1] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, pp. 644-654, 1976,

[2] H. Delfs and H. Knebl, *Introduction to Cryptography: Principles and Applications*, Springer, 2002.

[3] B. Meng, S. Wang, and Q. Xiong, "A fair non-repudiation protocol," in *Proc. the 7th International Conference on Computer Supported Cooperative Work in Design (CSCW'02)*, Brazil, 2002, pp. 68-73.

[4] H. Doi, M. Mambo, and E. Okamoto, "RSA-based multisignature scheme for various group structure," *Journal of Information Processing Society of Japan*, vol. 41, no. 8, pp. 2080-2091, 2000.

[5] K. Kawauchi, Y. Komano, K. Ohta, and M. Tada, "Probabilistic multi-signature schemes using a one-way trapdoor permutation," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E87-A, no. 5, pp. 1141-1153, 2004.

[6] C. Ma and D. He, "A new Chameleon multi-signature based on bilinear pairing", in *Proc. Grid and Cooperative Computing (GCC 2004)*, LNCS 3252, Springer, 2004, pp. 329-334.

[7] P. P. Reddy, B. U. Rao and T. Gowri, "ID-based directed threshold multisignature scheme from bilinear pairings", *International Journal on Computer Science and Engineering*, vol. 2, no. 1, pp. 74-79, 2009.

[8] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signature for delegating signature operation," in *Proc. the 3rd ACM Conference on Computer and Communications Security*, ACM press, 1996, pp. 48-57.

[9] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures: delegation of the power to sign messages," *IEICE Transactions on Fundamentals of Electronic Communications and Computer Science*, vol. E79-A, no. 9, pp. 1338-1354, 1996.

[10] X. Huang, W. Susilo, Y. Mu, and F. Zhang, "Short designated verifier signature scheme and its identity-based variant," *International Journal of Network Security*, vol. 6, no. 1, pp. 82-93, 2008.

[11] B. Kang, C. Boyd, E. Dawson, "A novel identity-based strong designated verifier signature scheme," *The Journal of Systems and Software*, vol. 82, no. 2, pp. 270-273, 2009.

[12] A. Shamir, "Identity-based cryptosystems and signature schemes," *Advances in Cryptology – CRYPTO'84*, Springer-Verlag, 1984, pp. 47-53.

[13] Y. Dodis, J. Katz, S. Xu, and M. Yung, "Key-insulated public key cryptosystems," in *Advances in Cryptology – EUROCRYPT'02*, Springer-Verlag, pp. 65-82, 2002.

[14] Y. Dodis, J. Katz, S. Xu and M. Yung, "Strong key-insulated signature schemes," in *Proc. Public Key Cryptography 2003 (PKC'03)*, LNCS 2567, Springer-Verlag, 2003, pp. 130-144.

[15] 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.

[16] 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.

[17] C. P. Schnorr, "Efficient signature generation by smart cards," *Journal of Cryptology*, vol. 4, no. 3, pp. 161-174, 1991.

[18] Y. Hanaoka, G. Hanaoka, J. Shikata, and H. Imai, "Identity-based hierarchical strongly key-insulated encryption and its application," in *Advances in Cryptology – ASIACRYPT'05*, Springer-Verlag, 2005, pp. 495-514.

[19] Y. Zhou, Z. Cao, and Z. Chai, "Identity based key insulated signature," in *Proc. ISPEC 2006*, LNCS 3903, 2006, pp. 226-234.

[20] G. Hanaoka, Y. Hanaoka, and H. Imai, "Parallel key-insulated public key encryption," in *Proc. Public Key Cryptography 2006 (PKC'06)*, LNCS 3958, 2006, pp. 105-122.

[21] J. Weng, S. Liu, K. Chen, D. Zheng, and W. Qiu, "Identity-based threshold key-insulated encryption without random oracles," in *Proc. CT-RSA 2008*, LNCS 4964, 2008, pp. 203-220.

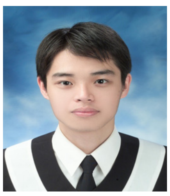
[22] T. Y. Wu, Y. M. Tseng and C. W. Yu, "ID-based key-insulated signature scheme with batch verification and its novel application," *International Journal of Innovative Computing, Information and Control*, vol. 8, no. 7(A), pp. 1349-4198, 2012.

[23] W. Stallings, *Cryptography and Network Security: Principles and Practices*, 4th. Ed., Pearson, 2005.

[24] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *Journal of Cryptology*, vol. 13, pp. 361-369, 2000.

Han-Yu Lin received BA degree in economics from the Fu-Jen University, Taiwan in 2001, his MS degree in information management from the Huafan University, Taiwan in 2003, and his Ph.D. degree in computer science and engineering from the National Chiao Tung University, Taiwan in 2010. He has been an Assistant Professor in the Department of Computer Science and Engineering of National Taiwan Ocean University since August 2012. His research interests include Cryptology, Network Security, Digital Forensics, Cloud Computing Security and E-commerce Security.

Tzong-Sun Wu received his BS degree in electrical engineering from the National Taiwan University, Taiwan in 1990, and his PhD in information management from the National Taiwan University of Science and Technology, Taiwan in 1998. From August 1998 to July 2001, he has been an Assistant Professor in the Department of Information Management of Huafan University. From August 2001 to January 2007, he has been an Associate Professor in the Department of Informatics of Fo Guang University. He is now with the Department of Computer Science, National Taiwan Ocean University. His research interests include information security, watermarking, digital right management, and e-commerce.



Ming-Lun Lee received his MS degree in informatics from Fo Guang University, Taiwan in 2008. He is now a Ph.D. candidate in the Department of Computer Science and Engineering of National Taiwan Ocean University, Taiwan. His research interests include cryptography, information security, and digital watermarking.

Chi-Kuang Yeh received his BS degree in computer science and information engineering from Fu Jen Catholic University, Taiwan in 2012. Now he is a graduate student in the department of computer science and engineering of National Taiwan Ocean University, Taiwan. His research interest is Network Security.