1-out-of-n Proxy Oblivious Signature Schemes and its E-voting Application

Shin-Yan Chiou, Tsung-Ju Wang, Jiun-Ming Chen

***Abstract*—**In a proxy signature scheme, an original signer delegates his signing authority to one or more proxy signers, which helps the proxy signers to sign messages on behalf of the original signer. In an oblivious signature scheme, a signee is allowed to choose one of the predetermined messages to get signed while not revealing any information about the selected message to the signer. Since the protocol provides ambiguity of the signee's selection, it is very suitable for electronic voting applications. In this paper, we first propose a proxy oblivious signature scheme based on discrete logarithm problem (DLP), which combines the advantages of proxy signature and oblivious signature and satisfies the security properties of both signatures. Performance comparisons are also given which shows that our scheme is not only capable but also efficient.

***Keywords*—**Electronic voting, oblivious signature, proxy oblivious signature, proxy signature**.**

I. Introduction

In the past decades, as the network transaction evolves rapidly, more and more consumers rely on internet auction and banking. Technologies of network security play important roles in users' privacy protection. One of the products which has received great attention and been in heated discussion is digital signature. A digital signature can be considered as those signatures signed by hand, but it has several properties that a traditional signature doesn't have: completeness, unforgeability, undeniability and verifiability. By using the public-key cryptography, a signer could sign a message with his private key, which is owned only by himself, a digital signature of the message then is created. Afterward any verifier can validate the correctness of the signature by using the signer's public key, unlike a traditional signature, a digital signature cannot be forged, the signer cannot deny any signature produced by him after the signature generation. Digital signatures are able to convince anyone the agreement from the signers, meanwhile they are transferable in the electronic world. This technique is very useful in many scenarios such as signer authenticity, product validation, data integrity assurance and so on. For a recent work, E.S. Ismail [1] in 2011 proposed a signature scheme based on two hard number theoretic problems.

However, in some situations, it is necessary to protect the privacy of signature receivers. In 1982, D. Chaum [2] introduced a blind signature, which is a special form of digital signature that satisfies the requirement. In a blind signature scheme, a signee could get a message signed from a signer without revealing any information about the message. Compare with a normal signature, a blind signature offers an additional property, blindness, which means it has the ability for protecting the privacy of signees. It is very important in some applications such as electric payment systems and secure voting systems, due to the messages from the requesters may be sensitive.

In 1994, L. Chen [3] first proposed the concept of oblivious signatures. He considered two types of oblivious signature schemes. The first one consisted of n keys and one message; the second one consisted of n messages and one key. In the first scheme the receiver can get a message signed with one of n keys which is chosen by him while the signers cannot find out with which key the signature is got by the receiver. The second scheme allows a signee to choose one of the predetermined messages to get signed while not revealing any information about the selected message to the signer. Different from blind signatures, oblivious signatures could guarantee the signed message is actually one of the predetermined messages, that is, if a receiver submitted some other messages beyond those messages, the signature would not be accepted by the scheme.

R. Tso et al. [4] in 2008 pointed out that Chen's proposal did not crisply formalize the notion and the security properties of the scheme. As a result they gave the formal definitions and the security requirements of the oblivious signature scheme which included: completeness, unforgeability and ambiguity. They also improved the performance of it. Possessing the above properties, oblivious signatures are very suitable for applying to electronic voting applications.

Furthermore, before the presentation of oblivious signatures, a concept of oblivious transfer was introduced by M.O. Rabin [5] in 1981. It is a protocol that the sender sends some subsets of some messages and doesn't know what the receiver has received. By this way the receiver could get the particular message he wants without revealing any information of the message to the sender, and the sender doesn't give a clue of other messages to the receiver, either. J.S. Chou [6] in 2012 also proposed a k-out-of-n oblivious transfer which was more efficient and secure.

Although the present signature schemes seem to be practical, but they still are unable to fulfill the signers who are not always available. Motivated by solving the problem, M. Mambo et al. [7] in 1996 inspired a new concept called proxy signature. Some proxy signature schemes have been proposed [8, 9]. Proxy signature schemes consist of three entities: an original signer, a proxy signer and a signee. By executing the protocol, an original signer is allowed to delegate his signing power to one or more proxy signers, which helps the proxy

Manuscript received December 21, 2014. This work was supported in part by the MOST project under Grant 103-2221-E-182-047.

Shin-Yan Chiou is with Department of Electrical Engineering, Chang Gung University, Tao-Yuan 333, Taiwan. (e-mail: ansel@mail.cgu.edu.tw).

Tsung-Ju Wang was with Department of Electrical Engineering, Chang Gung University, Tao-Yuan 333, Taiwan. He is now with the Shuttle Inc., Taipei 114, Taiwan (e-mail: alliedcw@hotmail.com).

Jiun-Ming Chen is with Changingtec, Hsinchu 300, Taiwan on leave from Department of Electrical Engineering, Chang Gung University (e-mail: c755324@hotmail.com).

signers to sign messages submitted on behalf of the original signer.

In 2000, W.D. Lin et al. [10] proposed the first proxy blind signature scheme, which is a scheme that has the functionalities of both proxy signatures and blind signatures, security properties of the two signatures are also satisfied. Later in 2002, Z. Tan et al. [11] proposed a proxy blind signature scheme, but it was pointed out insecure by S. Lal et al. [12] in 2003. Lal further proposed a new scheme that was secure and more efficient than Tan's scheme. F.Y. Yang et al. [13] in 2013 proposed a new proxy blind signature scheme that allowed revocation.

Proxy signatures and oblivious signatures have specific advantages. However, in some real situations, it is necessary to apply them both concurrently, for example, an anonymous proxy electronic voting system. In reality, a voting system requires numerous polling booths; in electronic voting systems, there also are needs for polling booths with proxy ability, which can not only decrease the loading of the voting center but also avoid the jams. Moreover, if the voting functionality can be mobilized, which allows people to vote anywhere with mobile devices, the electronic voting system would be more convenient for the masses and people with disabilities. Although several proxy blind signature schemes have been proposed, so far there is no paper introduces a scheme that inherits the properties of both proxy signature and oblivious signature.

Motivated by the mentioned demands, in this paper, we first propose a proxy oblivious signature schemes based on Schnorr signature [14], which combines the advantages of proxy signature and oblivious signature and satisfies the security properties of these two signature schemes. Utilizing the concept of [15], performance comparisons are also given in this paper, which show that our scheme is not only capable but also efficient.

II. Related Works

In this section, we present two representative protocols corresponding to our scheme, oblivious signature and proxy signature.

A. Oblivious Signature

The operating process of the oblivious signature scheme [4] (as shown in Fig. 1) is as follows.

Step 1. The recipient chooses n messages as the candidates and computes c as the blinded selection. Then he sends them to the signer.

Step 2. The signer chooses n random numbers k_i, for $i = 1, 2, ..., n$ and computes K_i to generate $\hat{e}_i$ and $\hat{s}_i$, then sends $(\hat{e}_i, \hat{s}_i)$ back to the recipient.

Step 3. The recipient picks out the oblivious signature of the selected message from $(\hat{e}_i, \hat{s}_i)$ by computing δ_i and checking the examining equations.

Step 4. To obtain the valid generic signature, the recipient calculates e and s as the signature $\sigma = (e, s)$.

Step 5. A verifier could verify the signature σ by using the public key of the signer.

Note that in Step 2, the signer couldn't learn which the message is selected by the recipient, this is what is called the ambiguity of the protocol. Moreover in Step 5, we can observe that unless the selected message m_l is one of the elements of m_l, or the signature won't be accepted by a verifier. The protocol ensures that the message from the signee is one of the predetermined messages, which is one of the features of an oblivious signature scheme.

B. Proxy Signature

The earliest proxy signature scheme [7] is a proxy signature for ElGamal scheme [16]. The executing procedure (as shown in Fig. 2) is as follows.

Step 1. The original signer randomly picks a number k to blind his private key x, delivers (σ, K) to the proxy signer.

Step 2. The proxy signer verifies the original signature with the original signer's public key y, if it's correct, he accepts.

Step 3. The proxy signer chooses a random number r and signs the message with σ and r.

Step 4. The signee gets the signature (m, (R, s, K)) and sends it to the verifier.

Step 5. The verifier then verifies the validity of the signature by using the public key of the original signer.

III. Security Goals

In this paper, the proposed schemes consist of four entities: an original signee $\mathcal{A}$, a proxy signer $\mathcal{B}$, a receiver $\mathcal{R}$ and a verifier $\mathcal{V}$. Corresponding to a proxy electronic voting system, $\mathcal{A}$, $\mathcal{B}$, $\mathcal{R}$ and $\mathcal{V}$ plays the role of a central government, a local government, a voter and a bulletin (or anyone) respectively. We define the security properties of a proxy oblivious signature scheme as below.

(1) **Completeness.** If all the entities follow the protocol honestly, then at the end of the protocol $\mathcal{R}$ will certainly obtain the valid signature σ of the selected message.

(2) **Unforgeability.** $\mathcal{B}$ can sign messages on behalf of $\mathcal{A}$ without having the responsibility of the signature. $\mathcal{V}$ can merely know that the signature is signed by some proxy delegated by $\mathcal{A}$, and no one except $\mathcal{B}$ (or $\mathcal{A}$) can produce a valid signature. That is, the signing key of $\mathcal{A}$ and the proxy signing key are practically unbreakable, so that an attacker can hardly create a valid signature even though the algorithm is published.

(3) **Unlinkability.** $\mathcal{B}$ can identify neither the message nor the proxy signature he generates associated with the scheme after the signature is revealed when necessary.

(4) **Undeniability.** Neither $\mathcal{A}$ nor $\mathcal{B}$ can deny the signature they created after the signature generation.

(5) **Verifiability.** The signature that $\mathcal{R}$ receives should be able to convince $\mathcal{V}$ of the agreement from $\mathcal{A}$ and $\mathcal{B}$.

(6) **Distinguishability.** The proxy signature is distinguishable from the normal one.

(7) **Ambiguity.** $\mathcal{B}$ cannot find out which message $\mathcal{R}$ has selected while signing the messages.

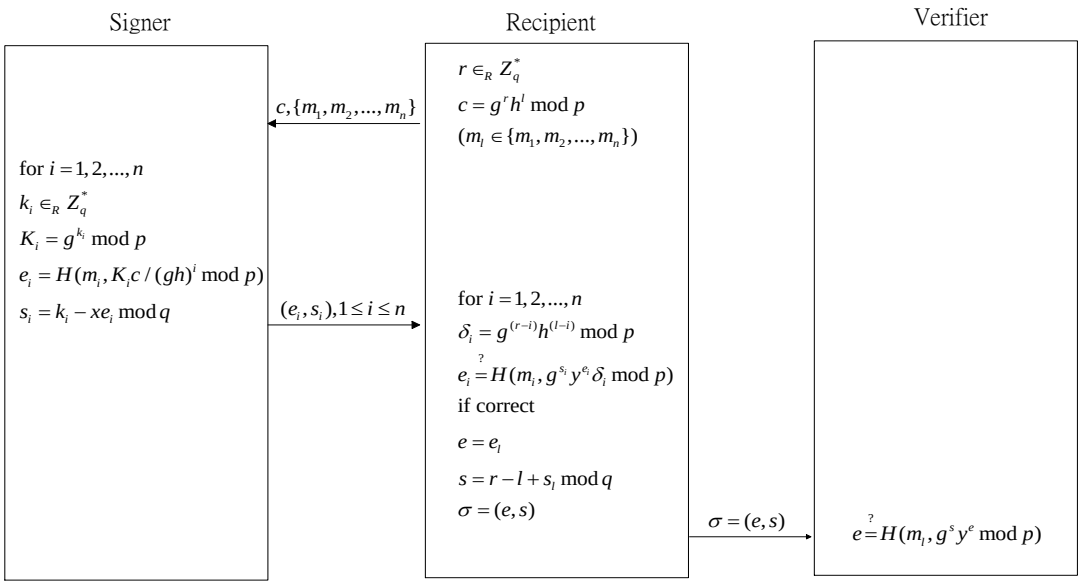


Fig. 1. Oblivious signature scheme

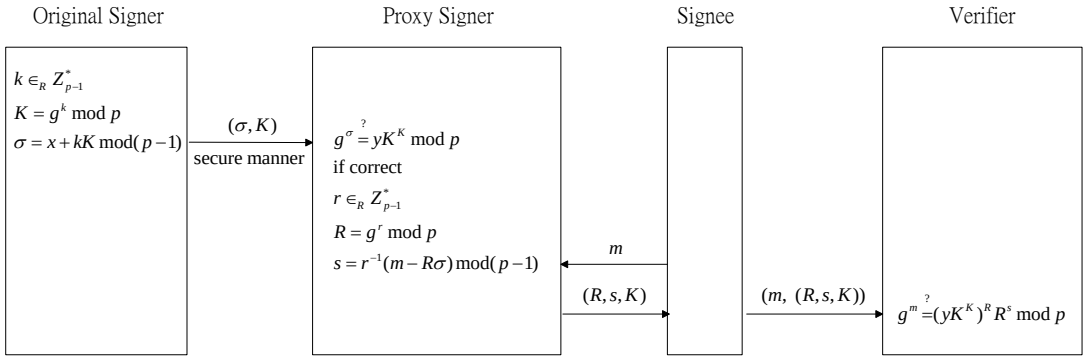


Fig. 2. Proxy signature scheme

TABLE I
NOTATIONS

$\mathcal{A}$	The original signer.
$\mathcal{B}$	The proxy signer.
$\mathcal{R}$	The recipient.
$\mathcal{V}$	The verifier.
p, q	Two large prime numbers such that $q \mid p$.
g, h	Two elements of Z_p* of the same order q.
x_i	i's private key.
y_i	i's public key.
s_p	The signing key.
n	The number of messages.
m_i	The ith message.
b	The value of the subscript of the selected message m_b.
σ	The signature on m_b.
$H(\cdot)$	A public one way hash function.

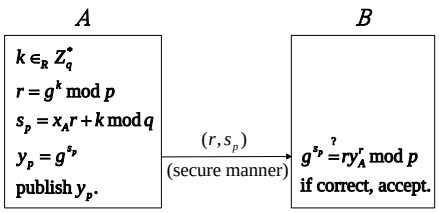


Fig. 3. Proxy phase

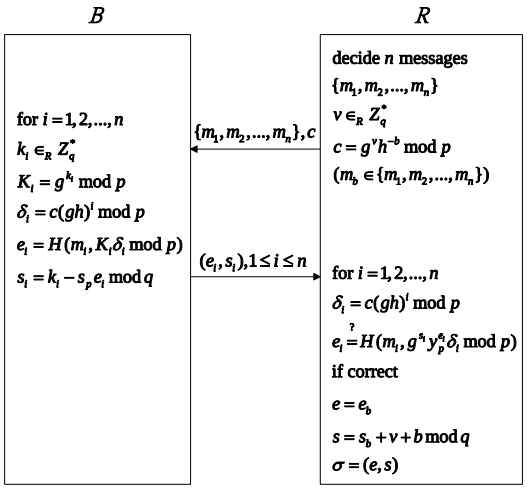


Fig. 4. Signing phase

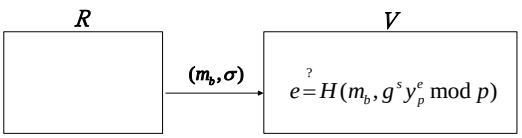


Fig. 5. Verification phase

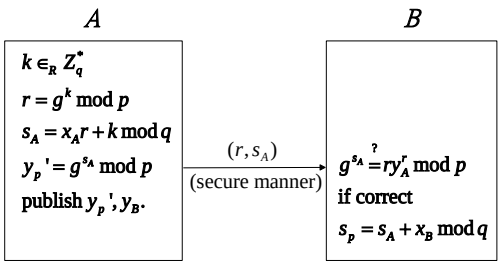


Fig. 6. Proxy phase

IV. Proposed Scheme

Our proposed signature scheme includes four phases: (1) system setup phase, (2) proxy phase, (3) signing phase, and (4) verification phase. Table I shows the notations that used in the protocol. Our protocol runs as follows.

(1) System Setup Phase

Step 1. Choose two large primes $p, q \ni q \mid (p-1)$.

Step 2. Choose two generators $g, h \in Z_p^*$, $Ord_p g = q$, $Ord_p h = q$.

Step 3. Original signer $\mathcal{A}$ chooses $x_A \in Z_q^*$, computes $y_A = g^{x_A} \bmod p$.

Step 4. Proxy signer $\mathcal{B}$ chooses $x_B \in Z_q^*$, computes $y_B = g^{x_B} \bmod p$.

(2) Proxy Phase

Step 1. (Commission generation) $\mathcal{A}$ randomly chooses $k \in_R Z_q^*$, computes $r = g^k \bmod p$, $s_p = x_A r + k \bmod q$ and $y_p = g^{s_p} \bmod p$.

Step 2. (Proxy delivery) $\mathcal{A}$ forwards the pair (r, s_p) to the proxy signer $\mathcal{B}$ in a secure manner and publishes y_p.

Step 3. (Proxy verification) $\mathcal{B}$ checks if $g^{s_p} = r y_A^r \bmod p$ holds. If it does, $\mathcal{B}$ accepts the proxy and uses s_p as his secret proxy signature key.

(3) Signing Phase

Step 1. $\mathcal{R}$ decides n messages $\{m_1, m_2, ..., m_n\}$ and selects a message $m_b \in \{m_1, m_2, ..., m_n\}$, randomly chooses $v \in_R Z_q^*$ and computes $c = g^v h^{-b} \bmod p$, then sends the determined messages and c to $\mathcal{B}$.

Step 2. For $i = 1, 2, ..., n$, $\mathcal{B}$ chooses n random numbers $k_i \in_R Z_q^*$, computes

$$K_i = g^{k_i} \bmod p$$
$$\delta_i = c(gh)^i \bmod p$$
$$e_i = H(m_i, K_i \delta_i \bmod p)$$
$$s_i = k_i - s_p e_i \bmod q$$

and sends (e_i, s_i) to $\mathcal{R}$, $1 \le i \le n$.

Step 3. For $i = 1, 2, ..., n$, $\mathcal{R}$ computes $\delta_i = c(gh)^i \bmod p$, and accepts the oblivious signature if and only if $e_i = H(m_i, g^{s_i} y_p^{e_i} \delta_i \bmod p)$.

Step 4. To convert the oblivious signature into a generic signature, $\mathcal{R}$ lets $e = e_b$, and computes $s = s_b + v + b \bmod q$. The signature on m_b is $\sigma = (e, s)$.

(4) Verification Phase

The verifier $\mathcal{V}$ accepts the signature σ as a valid signature if and only if

$$e = H(m_b, g^s y_p^e \bmod p).$$

V. Comparison

This section compares our scheme with other related schemes including oblivious signature schemes [3,4] and proxy blind signature scheme [13]. Table II, Table III and Table IV display the computation cost, communication cost and ability comparison respectively. Since the modular exponentiation is the most significant operation of computation, we denote its time cost as "*Ex.*" and ignore the other operations in the schemes.

Table II
Computation Comparison

Scheme	Original Signer	(Proxy) Signer	Receiver	Verifier
Chen [3]	-	3*nEx.*	(2*n*+10)*Ex.*	8*Ex.*
Tso [4]	-	2*nEx.*	(2*n*+2)*Ex.*	2*Ex.*
Yang [13]	1*Ex.*	4*Ex.*	2*Ex.*	3*Ex.*
Our Protocol	2*Ex.*	(*n*+2)*Ex.**	(2*n*+2)*Ex.*	2*Ex.*

Table III
Communication Comparison

Scheme	A→B	B→R	R→B	R→V
Chen [3]	-	$3n\|p\|+n\|p\|$	$\|q\|$	$7\|p\|+\|q+H\|$
Tso [4]	-	$n\|q+H\|$	$\|p\|$	$\|q+H\|$
Yang [13]	$\|q+H\|$	$\|p+q+H\|$	$\|q\|$	$\|q+2H\|$
Our Protocol	$\|p+q\|$	$n\|q+H\|$	$\|p\|$	$\|q+H\|$

Table IV
Ability Comparison

Scheme	Blindness	Ambiguity	Proxy Ability
Chen [3]	✓	✓	
Tso [4]	✓	✓	
Yang [13]	✓		✓
Our Protocol	✓	✓	✓

Compare with other related schemes, our scheme provides the most abilities with a low increment of computation cost. The communication cost is no higher than other oblivious signature schemes as well.

*In the proxy phase, $\mathcal{B}$ processes 2*Ex.* to examine $g^{s_A} \stackrel{?}{=} r y_A^r \bmod p$. In the signing phase, $\mathcal{B}$ processes *nEx.* to calculate $K_i = g^{k_i} \bmod p$, for i = 1, 2, …, n. As for $\delta_i = c(gh)^i \bmod p$, $\mathcal{B}$ may compute δ_i by letting $\delta_0 = c$, and generates $\delta_i = \delta_{i-1}(gh) \bmod p$, for i = 1, 2, …, n, consequently the computation cost is concluded n modular multiplication rather than *nEx.*

VI. Conclusion

This paper first constructs 1-out-of-*n* proxy oblivious signature schemes and gives the security requirements of them. The proposed scheme combines the advantages of proxy signature and oblivious signature and satisfies the security properties of both signatures including completeness, unforgeability, unlinkability, undeniability, verifiability, distinguishability and ambiguity. Moreover, providing extra

proxy ability, our schemes perform well in both complexity and usability among the related schemes.

ACKNOWLEDGMENT

This work is partially supported by the MOST project under Grant 103-2221-E-182-047. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

[1] E. S. Ismail, N. M. F. Tahat, "A new signature scheme based on multiple hard number theoretic problems," ISRN Communications and Networking, 2011. http://dx.doi.org/10.5402/2011/231649

[2] D. Chaum, "Blind signatures for untraceable payments," Crypto, Vol. 82, 1982.

[3] L. Chen, "Oblivious signatures," Computer Security–ESORICS 94, Lecture Notes in Computer Science 875, pp.161–172, 1994. http://dx.doi.org/10.1007/3-540-58618-0_62

[4] R. Tso, T. Okamoto, E. Okamoto, "1-out-of-n oblivious signatures," Information Security Practice and Experience. Springer Berlin Heidelberg, pp.45–55, 2008. http://dx.doi.org/10.1007/978-3-540-79104-1_4

[5] M. O. Rabin, "How to exchange secrets by oblivious transfer," IACR Cryptology ePrint Archive, 2005.

[6] J. S. Chou, "A novel k-out-of-n oblivious transfer protocol from bilinear pairing," Advances in Multimedia, 2012. http://dx.doi.org/10.1155/2012/630610

[7] M. Mambo, K. Usuda, E. Okamoto, "Proxy signatures: Delegation of the power to sign messages," IEICE transactions on fundamentals of electronics, communications and computer sciences 79.9, pp.1338–1354, 1996.

[8] J. S. Chou, "A novel anonymous proxy signature scheme," Advances in Multimedia, 2012. http://dx.doi.org/10.1155/2012/427961

[9] R. Dhir, "Cryptanalysis and Performance Evaluation of Enhanced Threshold Proxy Signature Scheme Based on RSA for Known Signers," Mathematical Problems in Engineering, 2013.

[10] W. D. Lin, J. K. Jan, "A security personal learning tools using a proxy blind signature scheme," Intl Conference on Chinese Language Computing, pp.273–277, 2000.

[11] A. Z. Tan, Z. Liu, C. Tang, "Digital proxy blind signature schemes based on DLP and ECDLP," MM Research Preprints 21.7, pp.212–217, 2002.

[12] S. Lal, A. K. Awasthi, "Proxy Blind Signature Scheme," Journal of Information Science and Engineering, 2003.

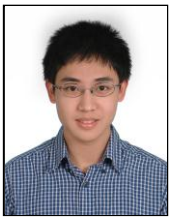
[13] F. Y. Yang, L. R. Liang, "A proxy partially blind signature scheme with proxy revocation,"Journal of Ambient Intelligence and Humanized Computing 4.2, pp.255–263, 2013. http://dx.doi.org/10.1007/s12652-011-0071-1

[14] C. P. Schnorr, "Efficient signature generation for smart cards," Journal of Cryptology, pp.161–174, 1991. http://dx.doi.org/10.1007/BF00196725

[15] M. Bellare, P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols,"Proceedings of the 1st ACM conference on Computer and communications security. ACM, 1993. http://dx.doi.org/10.1145/168588.168596

[16] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Transactions on 31.4, pp. 469–472, 1985. http://dx.doi.org/10.1109/TIT.1985.1057074

Shin-Yan Chiou received the PhD degree in Electrical Engineering from National Cheng Kung University, Taiwan, in 2004. From 2004 to 2009, he worked at Industrial Technology Research Institute as a RD Engineer. Since 2009, he joined the faculty of the Department of Electrical Engineering, Chang Gung University, Taoyuan, Taiwan, where he is currently an Associate Professor. His research interests include information security, cryptography, social network security, and secure applications between mobile devices.



Tsung-Ju Wang received the MS degree in Electrical Engineering from Chang Gung University, Taiwan, in 2014. Since 2014, he joined the faculty of Changing Information Technology Inc., Hsinchu, Taiwan, where he is currently an Engineer. His research interests include information security and secure applications between mobile devices.

Jiun-Ming Chen received the MS degree in Electrical Engineering from Chang Gung University, Taiwan, in 2013. Since 2013, he joined the faculty of the Shuttle Inc., Taipei, Taiwan, where he is currently an Engineer. His research interests include information security and secure applications between mobile devices.