Available online at www.sciencedirect.com

SCIENCE DIRECT®

Computer Standards & Interfaces 27 (2005) 415–422

COMPUTER STANDARDS & INTERFACES

www.elsevier.com/locate/csi

Design of a fair proxy raffle protocol on the Internet

Yu-Yi Chen[a], Jinn-Ke Jan[b,*], Chin-Ling Chen[c]

[a]*Department of International Business, Providence University, Taichung, Taiwan, ROC*
[b]*Institute of Computer Science, National Chung Hsing University, Taichung, Taiwan, ROC*
[c]*Institute of Applied Mathematics, National Chung Hsing University, Taichung, Taiwan, ROC*

Received 11 May 2004; received in revised form 9 November 2004; accepted 9 November 2004
Available online 13 December 2004

Abstract

We proposed a practical, anonymous, and publicly verifiable raffle protocol for use on the Internet. This method integrates cryptology such as public key infrastructure, hashing chain, and blind signature et al. We also involve a trust proxy center to coordinate the raffle. The winning number generation is publicly verifiable. All of the participant's raffle tickets must be involved with each one having an equal chance to win the prize. This will give the raffle higher credibility and practicability. Most importantly our scheme can be easily implemented on the Internet. The proposed method will be very useful for network marketing.

Keywords: Lottery; Raffle; Fairness; Anonymity; Internet

1. Introduction

Promotion and advertising can be a heavy expense. Smart business people know that it costs more time and money to win over new customers than to keep current customers. Keeping current customers loyal produces more profits from repeat purchases in the long run. The most familiar, low-cost sales promotion is offering a raffle draw upon purchase. As we know, many merchants hold attractive raffles at their annual celebrations. Customers must accumulate a certain number of purchases in exchange for a raffle ticket to encourage purchases. As usual, the prizes must be large, ranging from electronic gadgets to vacation trips. The size and number of prize depend entirely on the raffle period length, the number of raffle tickets to be issued, and how much money is spent on the prizes. This is an extremely powerful method to excite consumer desire to purchase product.

With the prosperous growth of the Internet, more enterprises are paying much attention to network marketing. At the present time, how to implement a fair and secure raffle drawing technology on the Internet has still not been proposed. We reviewed

* Corresponding author. Tel.: +886 4 22858200.
E-mail addresses: yuyichen@pu.edu.tw (Y.-Y. Chen), jkjan@cs.nchu.edu.tw (J.-K. Jan), sd64cgli@cht.com.tw (C.-L. Chen).

0920-5489/$ - see front matter © 2004 Elsevier B.V. All rights reserved.
doi:10.1016/j.csi.2004.11.002

some e-lottery papers [1–7] to determine a solution. However, we found that such e-lottery protocols were not suitable for implementing a raffle on the Internet. Therefore, we decided to pioneer a fair proxy raffle protocol for use on the Internet. When reviewing the traditional raffle processes, we noticed that the raffle coordinator must always invite a witness, such as a lawyer, to assure the fairness of the raffle drawing. Fairness cannot depend on the presupposition of that the raffle issuer can be trusted. The chance for any participant to win the prize must be equal. No one must be able to predict or control the outcome. When these conditions are achieved, people will believe that the raffle is fair. Therefore, a good raffle must meet the following requirements.

- Anonymity: The participant should be anonymous during the raffle ticket casting and drawing phases to ensure a fair.
- Accuracy: Each valid raffle ticket must be inviolate. Participants' raffle tickets cannot be altered or removed.
- Fairness: The chance for any participant to win the prize must be equal. No one can predict the outcome.
- Verifiability: All valid raffle tickets and generating the winning number must be publicly verifiable.
- Security: The prize should be rewarded only to the actual raffle winner.
- Practicability: The proposed raffle system is implemented on the Internet for network marketing purposes.

2. Preliminary

In the proposed scheme, any participant can freely choose a random seed to join the winning ticket generation during the raffle drawing phase. However, these random seeds must be verified via the raffle proxy center according to the raffle originator's signature. For fairness, the random seed must be blindly signed by the raffle originator. An example is now presented based on [8,9] to illustrate this technology.

In a RSA context [8], we have a large composite number n, a public key e, and a secret key d. The m message signature is $\sigma=m^d \bmod n$. In order to obtain the signature from a secret message m, the requester blinds it with a random value $b^e \bmod n$, and sends $m'=m\cdot b^e \bmod n$ to the signer. The signer later return a signature $\sigma=\sigma'\cdot b^{-1} \bmod n$. The signature can be unblinded as $\sigma=\sigma'\cdot b^{-1} \bmod n$ to get the valid signature. The requester can obtain a valid signature σ of m without revealing the m.

The above descriptions are based on RSA technology. Another technology may be used that is based on the Discrete Logarithms Problem (for example: ElGamal [10] scheme). However, we will involve this methodology in our scheme.

3. The proposed raffle scheme

The structure of our scheme is illustrated in Fig. 1. There are three parties in our scheme as follows.

- □ Participant (P): People who have the right to participate in the raffle.
- □ Raffle Originator (RO): Any company or organization that provides the raffle prizes and holds the raffle.
- □ Raffle Proxy Center (RPC): A trustee web site that is committed to coordinate the raffle.

To hold a fair and verifiable raffle, the RPC is involved in our scheme to make the winning number generation publicly verifiable. Cryptology such as Public Key Infrastructure (PKI) [8], hashing chain [7], and blind signature [9,10] are applied in our scheme. The Internet Secure Socket Layer (SSL) protocol [11,12] is also applied to protect the end-to-end communications for raffle ticket issuing and casting. Before proceeding with more details, the following notations are introduced.

- $E_X(\,)$ The encryption function using X's public key to encrypt a message.
- $D_X(\,)$ The decryption function using X's secret key to encrypt a message.
- $S_X(\,)$ The signature function using X's secret key to sign a message.
- $V_X(\,)$ The verification function using the X's public key to verify a message.
- $B(\,)$ The blinding function using the blind factor to blind a message.

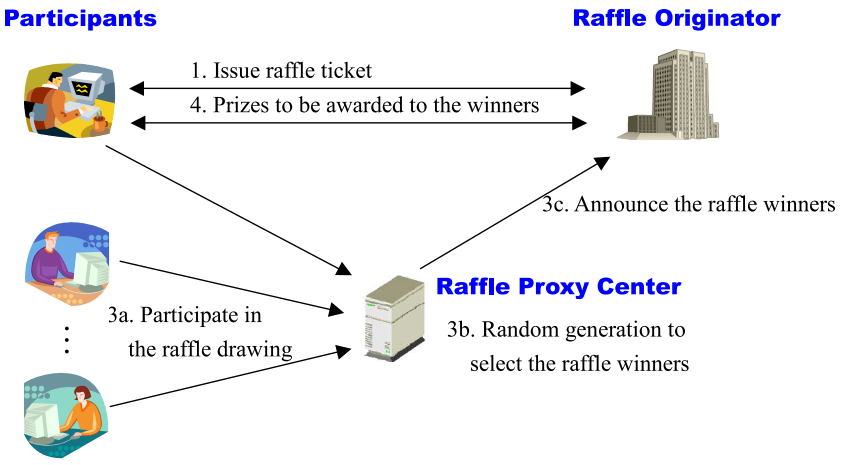

Fig. 1. The structure of our scheme.

$U(\ )$ The un-blinding function using the blind factor b to recover the original message, for example: $U(S_X(B(m,b))b)=S_X(m)$ for any message m and blind factor b, and it is infeasible to derive $S_X(m)$ from $S_X(B(m,b))$ without b.

PID_i P's identity with personal digital certification that can be verified.

t_c The casting deadline in the raffle ticket casting phase.

t_d The drawing deadline in the raffle ticket drawing phase.

t_a The winner announcement time in the raffle drawing phase.

t_p The prize claim deadline in the raffle prizing phase.

TK_i The raffle ticket $\mathrm{TK}_i=(\mathrm{TK}_{i\text{-info}}, \mathrm{TK}_{i\text{-sign}})$ issued by the RO. The ticket information $\mathrm{TK}_{i\text{-info}}=(E_{\mathrm{RO}}(\mathrm{PID}_i), \mathrm{no}_i, t_c, t_d, t_a, t_p)$ contains the encrypted P identity PID_i, ticket serial number no_i and some important time marks t_c, t_d, t_a, t_p, etc. The second part $\mathrm{TK}_{i\text{-sign}}=S_{\mathrm{RO}}(\mathrm{TK}_{i\text{-info}})$ is the signature of $\mathrm{TK}_{i\text{-info}}$.

$H(\ )$ The public one way hash function used to generate a series of un-dividable hash chains $a_0, a_1, a_2,\ldots, a_n$, where $a_1=H(a_0)$, $a_2=H(a_1),\ldots, a_n=H(a_{n-1})$.

$\{C_i\}$ The published hash chain set of the cast raffle ticket information where C_0 is the initial vector, $C_1=H(C_0, \mathrm{TK}_{1\text{-info}}),\ldots, C_i=H(C_{i-1}, \mathrm{TK}_{i-\mathrm{info}})$.

p_j The RPC's signature for P's receipt in the raffle ticket casting phase.

$\{R_j\}$ The published hash chain set of valid random seeds r_i selected by P, who is involved in generating the winning number, where R_0 is the initial vector, $R_1=H(R_0, r_1),\ldots, R_j=H(R_{j-1}, r_i)$.

q_j The RPC's signature for P's receipt in the raffle drawing phase.

Random( ) The public pseudo-random number generating function via input valid random seeds.

WNG( ) The winning number generating algorithm which is publicly verifiable.

Now, we introduce how our raffle scheme is implemented on the Internet. It is divided into the following four phases.

3.1. Raffle ticket issuing phase

In the raffle ticket issuing phase, P must be qualified. The RO then issues a valid raffle ticket and blindly signs a random seed for P. The raffle ticket is then cast into the RPC to participate in the raffle drawing. The signed random seed could be involved in generating the winning number in the raffle drawing phase.

Step 1: Any P that has the right to participate in the raffle proposes a request. He selects a blind factor b_i to blind another random selected seed r_i.

$$x_i = B(r_i,b_i)$$

P then sends his personal identity PID_i with x_i to the RO.

Step 2: Upon receiving P's request, the RO verified P's identity. The RO then generates a raffle ticket as follows.

$$TK_i = \left(TK_{i-info}, TK_{i-sign}\right)$$

The first part $TK_{i\text{-info}}=(E_{RO}(PID_i), no_i, t_c, t_d, t_a, t_p)$ is embedded the P's encrypted identity. The second part $TK_{i\text{-sign}}=S_{RO}(TK_{i\text{-info}})$ is the signature of $TK_{i\text{-info}}$. The RO signs the blind message x_i as follows.

$$y_i = S_{RO}(x_i)$$

The raffle ticket TK_i and the blind signature y_i are then submitted back to P.

Step 3: When P received the raffle ticket TK_i, it can be verified using the RO's public key.

$$\left(E_{RO}(PID_i), no_i, t_c, t_d, t_a, t_p\right) \stackrel{?}{=} TK_{i-info}$$

$$V_{RO}\left(TK_{i-sign}\right) \stackrel{?}{=} TK_{i-info}$$

Afterwards, the blind signature y_i can be un-blinded to get the signature of r_i as follows.

$$S_i = U(Y_i, b_i) = U(S_{RO}(X_i), b_i)$$
$$= U(S_{RO}(B(r_i, b_i)), b_i) = S_{RO}(r_i)$$

3.2. Raffle ticket casting phase

In this phase, the raffle ticket is cast into the RPC to participate in the raffle. All of the raffle tickets are linked to an un-dividable hash chain. The hash chain and the cast raffle tickets are then published, allowing the P's to verify if their raffle tickets are included or not.

Step 1: P must send the raffle ticket $TK_i=(TK_{i\text{-info}}, TK_{i\text{-sign}})$ to the RPC before the casting deadline t_c.

Step 2: Upon receiving the raffle ticket, the RPC must verify the raffle ticket TK_i using the RO's public key.

$$V_{RO}\left(TK_{i-sign}\right) \stackrel{?}{=} TK_{i-info}$$

If the raffle ticket TK_i is valid, the $TK_{i\text{-info}}$ is linked into the following hash chain.

$$C_i = H(C_{i-1}, TK_{i-info})$$

The RPC then signs and issues the following receipt p_i.

$$p_i = S_{RPC}(C_i, TK_{i-info})$$

The receipt p_i is then sent back to P.

Step 3: Both the hash value C_i and the cast raffle ticket information $TK_{i\text{-info}}$ are recorded and published for the next phase.

3.3. Raffle drawing phase

In this phase, each P could be involved in generating the winning number by submitting his random seed r_i to the RPC. Of course, if a P does not want to be involved in generating the winning number, he can give up the right. Only valid random seeds are used in generating the winning number. The RPC publishes the submitted random seeds and notifies the RO the winning ticket.

Step 1: After the casting deadline t_c, any P could be involved in generating the winning number by submitting his random seed r_i and the corresponding signature s_i to the RPC.

Step 2: Upon receiving the random seed r_i, the RPC must verify the signature s_i using the RO's public key.

$$V_{RO}(S_i) \stackrel{?}{=} r_i$$

If the random seed r_i is valid, it is linked into the following hash chain.

$$R_j = H\left(R_{j-1}, r_i\right)$$

The RPC then uses his secret key to generate the signature q_j for P as follows.

$$q_j = S_{RPC}\left(R_j, r_i\right)$$

The receipt q_j is then sent back to the P. All of the R_j and r_i are published such that anyone can verify those random seeds included in generating the winning number.

Step 3: Until the drawing deadline t_d, the RPC uses a public algorithm WNG( ) with the submitted random

seeds r_1, r_2,..., r_k to generate a pseudo-random number to map the winning ticket.

Procedure WNG(r_1, r_2,..., r_k)

{

1. w=Random(r_1, r_2,..., r_k) mod n+1, where n is the number of all raffle tickets.
2. located on the w^{th} index of records to get the winning ticket information $\text{TK}_{w\text{-info}}$ and the number C_w.
3. both $\text{TK}_{w\text{-info}}$ and C_w must published at the announce time t_a.

}

3.4. Raffle prize claim phase

In this phase, the raffle winner claims his prize after the winning ticket is announced. The prize can only be awarded to a verified P.

Step 1: Before the prize claim deadline t_p, the winner must propose his PID_i, $\text{TK}_{i\text{-sign}}$ and p_i to the RO.

Step 2: According to the announced winning raffle ticket information, the RO uses its secret key to decrypt part of the encrypted identity in the $\text{TK}_{w\text{-info}}$. The result must be the same as the PID_i such that only the original P can be rewarded.

$$\text{PID}_w = D_{\text{RO}}(\text{the part of encrypted identity in the } \text{TK}_{w-\text{info}})$$

$$\text{PID}_w \stackrel{?}{=} \text{PID}_i$$

The raffle ticket signature $\text{TK}_{i\text{-sign}}$ is verified using the RO's public key as follows.

$$V_{\text{RO}}(\text{TK}_{i-\text{sign}}) \stackrel{?}{=} \text{TK}_{w-\text{info}}$$

The corresponding receipt p_i must be also verified using the RPC's public key as follows.

$$V_{\text{RPC}}(P_i) \stackrel{?}{=} (C_w, \text{TK}_{w-\text{info}})$$

Hence, only the real winner that proposes the correct PID_i, $\text{TK}_{i\text{-sign}}$, and p_i can claim the prize.

4. Analysis

In this section, we will discuss the criteria proposed in Section 1 for our scheme.

4.1. Anonymity issue

In our scheme, each P's identity is embedded in the raffle ticket TK_i=($\text{TK}_{i\text{-info}}$, $\text{TK}_{i\text{-sign}}$), where $\text{TK}_{i\text{-info}}$=($E_{\text{RO}}(\text{PID}_i)$, no_i, t_c, t_d, t_a, t_p) and $\text{TK}_{i\text{-sign}}$= $S_{\text{RO}}(\text{TK}_{i\text{-info}})$. Because the P's identity PID_i is encrypted by the RO's public key, it will not be revealed during the raffle casting and raffle drawing phases.

4.2. Accuracy issue

Each cast raffle tickets is signed with a receipt p_i from the RPC. This means that the RPC cannot repudiate any verifiable cast raffle ticket. Moreover, all of the raffle tickets are linked in the following hash chain.

$$C_1 = H(C_0, \text{TK}_{1-\text{info}})$$

$$C_2 = H(C_1, \text{TK}_{2-\text{info}})$$

$$\vdots$$

$$C_n = H(C_{n-1}, \text{TK}_{n-\text{info}})$$

The hash chain and the cast raffle ticket information is published for each P to allow verification of the corresponding hash value C_i=$H(C_{i-1}, \text{TK}_{i\text{-info}})$ to ensure that his raffle ticket is involved in the raffle drawing. Based on the un-divided property of the hash chain, a valid raffle ticket cannot be miscounted or removed.

4.3. Fairness issue

Let us review the traditional raffle processes. Note that the RO must always invite a witness such as a lawyer to assure the fairness of the raffle drawing. The fairness issue cannot depend on the presupposition that the RO can be trusted. Applying the raffle drawing on the Internet, people will be convinced of the drawing fairness by inviting a trusted raffle proxy website to coordinate the raffle. This is the reason why we involved a trusted RPC in our scheme. The trustworthiness of the RPC is based on the public raffle drawing procedure. The winning number generating algorithm WNG( ) is publicly verifiable. Each P could be involved in generating the winning number

by submitting his random seed r_i to the following hash chain.

$$R_1 = H(R_0, r_1)$$

$$R_2 = H(R_1, r_2)$$

$$\vdots$$

$$R_k = H(R_{k-1}, r_k)$$

All of the valid submitted random seeds are involved in the function Random( ) to generate the winning number.

$$w = \text{Random}(r_1, r_2, \ldots, r_k) \bmod n + 1$$

No one can predict the outcome because all involved random seeds are freely selected by the participants. The winning number is therefore fairly generated. The chance for any P to win the prize is equal.

4.4. Verifiability issue

In the raffle ticket-casting phase, the Ps cast their raffle ticket to the RPC. Since all of the hash chain values C_1, C_2,..., C_n and the raffle ticket information $\text{TK}_{1\text{-info}}$, $\text{TK}_{2\text{-info}}$, ..., $\text{TK}_{n\text{-info}}$ are published, anyone can verify the completeness of the hash chain as follows.

$$C_1 = H(C_0, \text{TK}_{1-\text{info}})$$

$$C_2 = H(C_1, \text{TK}_{2-\text{info}})$$

$$\vdots$$

$$C_n = H(C_{n-1}, \text{TK}_{n-\text{info}})$$

Therefore, all of the valid raffle tickets are publicly verifiable. Similarly, anyone can verify the completeness of the other hash chain since all of the R_j and r_i are also published in the raffle drawing phase.

$$R_1 = H(R_0, r_1)$$

$$R_2 = H(R_1, r_2)$$

$$\vdots$$

$$R_k = H(R_{k-1}, r_k)$$

All of the random seeds involved in generating a pseudo-random number can be publicly verifiable.

$$w = \text{Random}(r_1, r_2 \ldots, r_k) \bmod n + 1$$

The winning number cannot be unfairly generated since each step in generating the winning number using the generating algorithm WNG( ) is publicly verifiable.

4.5. Security issue

In our scheme, only the actual winner can be awarded the prize because the winner's identity PID_w is embedded in the winning ticket information $\text{TK}_{w\text{-info}}$

$$\text{TK}_{w-\text{info}} = \left(E_{\text{RO}}(\text{PID}_w), \text{no}_i, t_c, t_d, t_a, t_p\right)$$

When someone claims the prize, the RO uses its secret key to decrypt part of the encrypted identity in the $\text{TK}_{w\text{-info}}$ such that only the actual winner that proposed the correct PID_i can make the claim.

$$\text{PID}_w = D_{\text{RO}}(\text{the part of encrypted identity in the } \text{TK}_{w-\text{info}})$$

$$\text{PID}_w \stackrel{?}{=} \text{PID}_i$$

The raffle ticket signature $\text{TK}_{i\text{-sign}}$ and corresponding receipt p_i proposed by the actual winner must pass the following verification.

$$V_{\text{RO}}\left(\text{TK}_{i-\text{sign}}\right) \stackrel{?}{=} \text{TK}_{w-\text{info}}$$

$$V_{\text{RPC}}(p_i) \stackrel{?}{=} (C_w, \text{TK}_w)$$

Clearly, only the actual winner that proposed the correct PID_i, $\text{TK}_{i\text{-sign}}$, and p_i can claim the prize.

4.6. Practicability issue

As we mentioned before, people will be convinced of the raffle's fairness by inviting a trusted raffle proxy website to coordinate the raffle on the Internet. The proposed raffle design can be easily implemented on the Internet. Our method makes the raffle fair and efficient on the current WWW infrastructure. For example, each year the U.S. Diversity Immigrant Visa

Lottery program (Green Card Lottery) makes available 55 000 permanent residence visas through a computer-generated raffle drawing [13]. If our scheme can be used in this application, it will have higher credibility and practicability.

5. Conclusions

Emerging Internet businesses may lead the market into an exciting and unknown world. The characteristics of the Internet have reshaped the marketing principles. In this paper, we proposed a fair and publicly verifiable raffle protocol for use on the Internet. The proposed method will be very useful for network marketing. The involved RPC is a trusted third party that coordinates the raffle. This will give the raffle higher credibility and practicability. The winning number generating algorithm can be verified publicly. All of the issued raffle tickets are guaranteed not to be altered or removed. All participants remain anonymous during the raffle drawing and each one has an equal chance to win the prize. Only the actual winner can be awarded the prize. These fair and secure features make the Internet raffle attractive to people. Our scheme is a novel solution to implement a fair and secure raffle on the Internet.

References

[1] D.M. Goldschlag, S.G. Stubblebine, Publicly verifiable lotteries: applications of delaying functions, Financial Cryptography: Second International Conference, Anguilla, British West Indies, February, 1998.
[2] K. Kobayashi, H. Morita, M. Hakuta, T. Nakanowatari, An electronic soccer lottery system that uses bit commitment, IEICE Trans. Inf. Syst. E83-D (5) (2000 May) 980–987.
[3] E. Kushilevitz, T. Rabin, Fair e-lotteries and e-casinos, The Cryptographer's Track at RSA Conference 2001 San Francisco, CA, USA, April 8–12, 2001.
[4] T. Nakanishi, N. Haruna, Y. Sugiyama, Unlinkable electronic coupon protocol with anonymity control, 1999 (http://citeseer.nj.nec.com/nakanishi99unlinkable.html).
[5] R.L. Rivest, Electronic Lottery Tickets as Micropayments Proceeds of Financial Cryptography, LNCS, vol. 1318, Springer Verlag, 1997, pp. 307–314.
[6] P. Syverson, Weakly secret bit commitment: applications to lotteries and fair exchange, 11th IEEE Computer Security Foundations Workshop, 1998.
[7] J. Zhou, C. Tan, Playing lottery on the internet, information and communications security, Proceedings of 3rd International Conference, ICICS 2001, Xian, China, Nov. 13–16, 2001.
[8] R.L. Rivest, A. Shamir, L. Adelman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM 21 (2) (1978 February) 120–126.
[9] D. Chaum, Blind signature for untraceable payments, Advances in cryptology; Proceeding Crypto'82, 1982, pp. 199–203.
[10] J.L. Camenisch, J.M. Piveteau, M.A. Stadler, Blind signature schemes based on the discrete logarithm problem, Rump Session of Eurocrypt '94, 1994 (5 pp.).
[11] A.O. Freier, P. Karlton, P.C. Kocher, The SSL Protocol Version 3.0", URL:http://www.netscape.com/eng/ssl3/draft302.txt, 1996.
[12] D. Wagner, B. Schneier, Analysis of the SSL 3.0 protocol, Proceedings of the Second USENIX Workshop on Electronic Commerce, USSENIX Press, 1996, pp. 29–40.
[13] The USA immigration service website, http://www.usaimmigrationservice.org/.

Yu-Yi Chen was born in Kaohsiung, Taiwan, in 1969. He received the B.S., M.S., and Ph.D. degrees in Applied Mathematics from the National Chung Hsing University in 1991, 1993, and 1998, respectively. He is presently an assistant professor of the Department of International Trade at Providence University, Taiwan. His research interests include computer cryptography, network security, and e-commerce.

Jinn-Ke Jan was born in Taiwan in 1951. He received the B.S. degree in physics from the Catholic Fu Jen University in 1974 and the M.S. degree in information and computer science from University of Tokyo in 1980. He studied Software Engineering and Human–Computer Interface in the University of Maryland, College Park, MD, during 1984-1986. He is presently a professor in the institute of Computer Science at National Chung Hsing University. He is currently also an editor of Information and Education, an editor of Journal of Computers, and an executive member of the Chinese Association for Information Security. He is a member of IACR and member of IEEE. From 1995 to 1997, he was the Director of the Counseling Office for Overseas Chinese and Foreign Students. From 1997 to 2000, he was the Director of the Computer Center at National Chung Hsing University. His research interests include computer cryptography, human factors of designing software and information systems, ideograms I/O processing, data structures and coding theory.

Chin-Ling Chen was born in Taiwan in 1961. He received the B.S. degree in Computer Science and Engineering from Feng Cha University, Taichung, Taiwan, in 1991 and the M.S. degree in Computer and Applied Mathematics at National Chung Hsing University, Taichung, Taiwan, in 1999. He is currently pursuing his doctoral degree in Applied Mathematics at National Chung Hsing University. He is presently a senior engineer at the Chunghwa Telecom Co., Ltd., and a member of the Chinese Association for Information Security. His research interests include cryptography, network security and electronic commerce.