An Improved Secure Anonymous Protocol for Distributed Computer Networks

Kai Chain[1], Wen-Chung Kuo[2] and Jiin-Chiou Cheng[3]

[1] *Department of Computer and Information Science, R.O.C. Military Academy, Taiwan*

[2] *Department of Computer Science and Information Engineering, National Yunlin University of Science & Technology, Taiwan, R.O.C.*

[3] *Department of Computer Science and Information Engineering, Southern Taiwan University, Taiwan, R.O.C.*

chainkai@mail2000.com.tw, simonkuo@sunws.nfu.edu.tw, chiou@mail.stut.edu.tw

Abstract

Many various kinds of network applications have arisen due to rapid development of network techniques. For preventing sensitive personal information from being disclosed on an open and unsecure network, it is necessary to provide some appropriate secure protocols. Concerning secure protocols, key agreement and authentication between user and server are paramount. In 2010, Cui and Cao proposed a secure anonymous key agreement for distributed networks, in which users collect other identities to utilize in communication so attackers cannot determine the real identity of the user. However, this protocol suffers the drawback of high calculation requirements. In this paper, we adopt Elliptic Curve Cryptography (ECC) to reduce the computational cost in Cui and Cao's protocol, and propose an indexing trick to speed up searches of legitimate users. Our proposed scheme maintains the characteristic of obfuscating user identity to thwart identification attempts.

Keywords: *key change, elliptic curve cryptography, anonymity, RSA*

1. Introduction

Computer networks connect hosts and users into a distributed computing environment which provides the advantages of increasing reliability, sharing information and computing power. Usually, the process of authentication involves the exchange of identities and authenticated key generation. It is increasingly important to protect systems and user privacy and provide security from malicious adversaries. In distributed computing environments, it may be advantageous to maintain user anonymity. That is, only the service provider can identify the user, while all other entities cannot.

In 2000, Lee and Chang [5] proposed a user identification and key distribution protocol that maintains user anonymity based on public key cryptography (RSA) and hash functions for distributed environments. Their scheme has four advantages: (1) users can request services without publically revealing their identities; (2) each user only needs to maintain one secret; (3) the service provider is not required to record the user password; (4) if a new service provider is added into the system, no master key updating is needed. In 2004, Wu and Hsu [8] pointed out that Lee et al.'s protocol has vulnerabilities. The first can occur when a user requests service from the service provider. Since only one-way authentication of the user is implemented, an attacker can impersonate the service provider. The second occurs when an

expired session key is disclosed, then an attacker can ascertain the user identity of the corresponding previous session [9]. So they proposed an improved method for enhancing security and efficiency. However, Yang, et. al., [9] showed a new weakness in Wu and Hsu's protocol where a service provider could obtain a valid user's secret token after an exchange of messages. As such, Yang et al. proposed a protocol to overcomes the weakness of Wu and Hsu's protocol to achieve user anonymity, user identification and key agreement. In 2006, Mangipudi and Katti [6] pointed out that Yang et al.'s protocol possessed a Denial-of Service (DoS) vulnerability. At the same time, Mangipudi and Katti proposed a secure identification and key agreement protocol with user anonymity (SIKA) [6]. In 2009, Hsu and Chuang [4] demonstrated an identity disclosure attack on the Mangipudi-Katti scheme [6] to show the identity of the communicating user can be easily ascertained from the exchanged messages. They proposed a novel user identification scheme with key distribution to preserve user anonymity which eliminates these security leaks and achieves all of the above-mentioned properties [1]. Later, in 2011, Cui and Cao [1] proposed a novel user identification scheme with key distribution preserving user anonymity (SAIKA) which eliminated previous security vulnerabilities and described the forward and backward security. However, the server and user must use considerable computational resources and the verification time is long.

In this paper, we adopt Elliptic Curve Cryptography (ECC) to reduce the computational cost in Cui and Cao's protocol and propose indexing to speed up the search of legitimate users. Our proposed protocol also maintains user anonymity during illicit identification attempts.

The paper is organized as follows: In Section 2, we review Cui and Cao's scheme [1] and analyze its weaknesses. In Section 3, we propose our scheme. In Section 4, the security analysis of our proposed scheme is discussed in comparison with Cui and Cao's scheme. Finally, in Section 5, we conclude the paper.

2. Review and Analysis of the Cui and Cao's Scheme

In 2011, Cui and Cao [1] proposed a novel user identification scheme with key distribution preserving user anonymity (SAIKA) which eliminated know security vulnerabilities and described the forward and backward security. A review and analysis of the Cui and Cao's scheme is given in this section.

2.1. The Cui and Cao's Scheme

The Cui and Cao's scheme [1] consists of three phases: registration phase, anonymous user identification and key agreement phase and reveal user identity phase. Descriptions of these phases are given below.

Registration phase

The related steps in this scheme are as follows (as depicted in Figure 1):

Step 1: The user U_i collects a group of n identities, and composes an identity list $L = \{ID_1, ..., ID_n\}$, including U_i's own identity $ID_i = ID_s (s \in [1, n])$. Then the user U_i submits L to the smart card producing center (SCPC) for registration.

Step 2: After the SCPC receives L, it uses a private key d to generate U_i's private key $\{S_i\}$ as $S_i = ID_i^d \bmod N (i \in [1, n])$. Then, the SCPC sends the private key $\{S_i\}$ to U_i via a secure channel. The server P_j submits an ID_j to the SCPC for registration. After the

SCPC receives ID_j, it uses the private key d to generate P_j's private key S_j as $S_j = ID_j^d \bmod N$. Then, the SCPC sends the private key S_j to P_j via a secure channel.

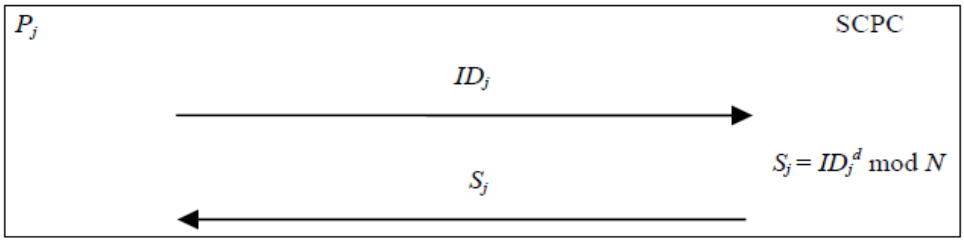

Figure 1. Registration Phase of SAIKA

Anonymous user identification and key agreement phase

User U_i performs the following steps to log-in to the server (as depicted in Figure 2):

Step 1: The user U_i selects a random number r and the timestamp T_0, and calculates $C = r \oplus h(ID_j || T_0)$. C and T_0 are passed to the server P_j.

Step 2: After the server receives C and T_0, it will calculate $r = C \oplus h(ID_j || T_0)$. Then, the server chooses a random number k and calculates Z to send back to U_i.

Step 3: After receiving Z from P_j, the user U_i chooses a random number t and calculates $\alpha = Z^e ID_j^{-r} \bmod N$, $K_{ij} = \alpha^t \bmod N$, $w = g^{et} \bmod N$, $x_i = g^t S_i^{h(K_{ij}||Z||w||T)} \bmod N$, and $y = E_{K_{ij}}(ID_1,...,ID_n)$, where T is the current timestamp. Then, U_i sends the message $(w, \{x_i\}, y, T)$ to P_j.

Step 4: After P_j receives $(w, \{x_i\}, y, T)$, it will check the validity of T. If this check is false, P_j revokes the agreement. If this check is true, P_j calculates $K_{ij} = w^k \bmod N$ and decrypt y as $L = D_{K_{ij}}(y)$. Then, P_j verifies the validity of the recovered identifier ID_i by checking $wID_i^{h(K_{ij}||Z||w||T)} \stackrel{?}{=} x_i^e \pmod N$. If this equation holds, P_j is convinced that U_i is an authorized user and calculates $D_i = h(K_{ij} || T' || \{ID_i || ID_j\})$. Finally, P_j sends (D_i, T') to user U_i.

Step 5: When U_i receives (D_i, T') from P_j, the validity of T' is checked. Then, U_i calculates $D_i' = h(K_{ij} || T' || \{ID_i || ID_j\})$ and checks if D_i' is identical the received D_i. If it holds, U_i is convinced that P_j is a valid server.

Reveal user identity phase

If P_j wants to confirm that U_i is a legal user, it can make a request to the SCPC. The SCPC will check U_i's identity. The related steps are as follows:

Step 1: P_j calculates $E_{S_j}(\{x_i\} || T_1)$, and sends it to the SCPC as a request to verify U_i's identity.

Step 2: U_i calculates $x_S = g^t S_S^{h(K_{ij}||Z||w||T)} \bmod N$ and $E_{S_i}(x_S||T_2)$. Then, U_i sends $E_{S_i}(x_S||T_2)$ to the SCPC.

Step 3: The SCPC decrypts $E_{S_j}(\{x_i\}||T_1)$ and $E_{S_i}(x_S||T_2)$, and then verifies x_s. If x_i is equal to x_s, SCPC affirms that U_i is a legal user and sends $\{x_i, T_2\}$ to P_j.

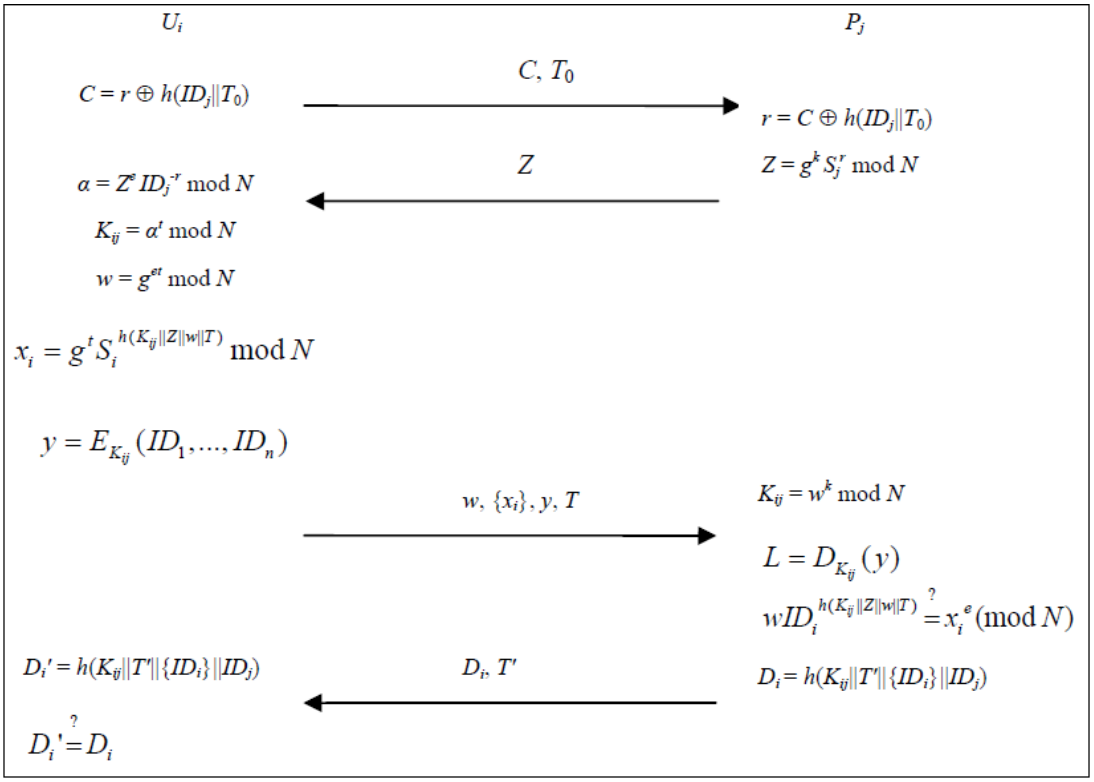

Figure 2. Anonymous Authentication and Key Agreement Phase

2.2. Security analysis of Cui and Cao's scheme

In Cui and Cao's scheme, the user will have an identity table that contains his own identity and other additional randomly selected identities in the registration phase. This table is stored in the registration information of the SCPC. When the user requests to log-in to the server, the user sends the identity table to the server for mutual authentication. After the server receives the table, it will verify that the correct user is located in the identity table. However, the burden on the SCPC increases. In reveal user identity phase, the SCPC, in order to looking for the legitimate user, must calculate $wID_i^{h(K_{ij}||Z||w||T)} \stackrel{?}{=} x_i^e \pmod N$. Therefore, a large amount of computation time is used, and the communication times are likewise extended. In this paper, we adopt Elliptic Curve Cryptography (ECC) to reduce the computational cost inherent in Cui and Cao's protocol, and propose indexing to speed up the verification of legal users.

3. The Proposed Scheme

We improve on Cui and Cao's scheme [1] and propose an improved secure anonymous identity-based key agreement protocol for distributed computer networks. Our proposed scheme consists of two phases: a parameter generation phase, and an anonymous user identification and key agreement phase.

Parameter generation phase

The related parameters in this scheme are as follows:

(1) A smart card producing center (SCPC) chooses a large prime number q ($q > 2^{160}$) and two field elements (a, b). Where $a \in q, b \in q$ must satisfy $4a^3 + 27b^2 (\mathrm{mod}\, q) \neq 0$, and the elliptic curve equation is defined as: $E_P : y^2 = x^3 + ax + b$.

(2) The server generates a point G from order n which satisfies $n \times G = O$ and $n > 2^{160}$.

(3) Every user (ID_C, ID_P) has to register with the SCPC. For each user, the SCPC selects a random number x_i and computes a public key $PK_i = X_i \times G$, where $X_i < n$.

(4) A public key table is produced which contains the identities and the public keys of the registered users in the SCPC.

Anonymous user identification and key agreement phase

User U_i performs the following steps to log-in to the server (as depicted in Figure 3):

Step 1: The user selects a random number t_1, obtains the server's public key $PK_S = X_S \times G$ and calculates $K_1 = t_1 \times PK_S$ and $T_1 = t_1 \times G$. Then, the user selects a random point P and generates $C' = H(2^{array_{ID_i}} P)$. The user obtains d of ID and P from the SCPC, and encrypts $M_1 = E_{K_1}(ID_1, ID_2, ID_i, .. ID_d \,||\, C \,||\, P)$ using K_1. Then, T_1 and M_1 will be passed to the server.

Step 2: After the server receives T_1 and M_1, it will calculate $K_1 = T_1 \times X_S$ to allow decryption of M_1 and get the random identity table, C' and P. The server will verify $H(2^{array_{ID_i}} P)$ is equal to the value of C' obtained from the user. If either of these checks is false, the server revokes the agreement. If the checks are true, the server chooses a random number t_2 and retrieves ID_C's public key $PK_{ID_i} = X_{ID_i} \times G$ from public key table. The server calculates $K_3 = X_S \times PK_{ID_i}$ and $T_2 = t_2 \times G$. Then, the server encrypts $M_2 = E_{K_2}(H(K_3 \,||\, C') \,||\, Nonce_2)$ by using K_2. Finally, the server sends (T_2, M_2) to the user.

Step 3: The user calculates $K_2 = T_2 \times X_{ID_i}$ and employs it to decrypt M_2 and uses $K_3 = X_C \times PK_S$ to verify $H(K_3 \,||\, C')$. Then the user calculates $K_4 = t_1 \times T_2$, $M_3 = E_{K_4}(H(K_3 \,||\, N_{once2}) \,||\, N_{once1})$ and the session key $SK = H(Nonce_1 \,||\, Nonce_2 \,||\, K_3)$.

Step 4: The server will verify $H(K_3 \,||\, N_{once2})$. If it holds, the server is convinced that the user is an authorized user and calculates the session key $SK = H(Nonce_1 \,||\, Nonce_2 \,||\, K_3)$.

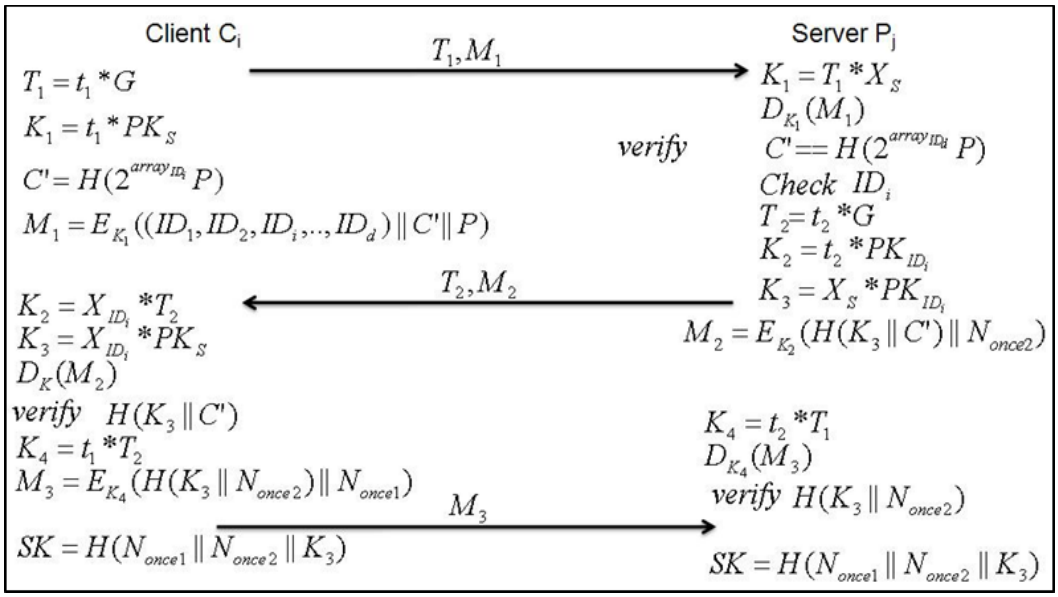

Figure 3. Anonymous User Identification and Key Agreement Phase

4. Security Analysis and Comparison

In this section, we will analyze the security of our proposed scheme and make comparisons with related schemes.

4.1. Security Analysis

We discuss three different aspects of our approach:

4.1.1. Identity Leak: In the process of communication between the user and the server, the user generates a random identity table, calculates $C' = H(2^{array_{ID_i}} P)$, and sends it to the server as a request to verify the user identity. The server calculates K_1 to decrypt M_1 and verifies $H(2^{array_{ID_i}} P)$, and then finds the index value of the legitimate user. Because the user's identity table is a random number of public identities selected by the server, both of which also does not have any association, so attackers cannot deduce the order of their identities or rely on the public identity table of the server. Therefore, it can prevent the attacker from determining who is the real user in the random identity table.

4.1.2. Mutual Authentication: The user can verify the server by using C' and the value of K_3 to check if the server is not legitimate. The attacker does not know the random number t_1 and the value of ID_i in $C' = H(2^{array_{ID_i}} P)$. In addition, the attacker also does not know the value X_s in $K_3 = X_S \times PK_{ID_i}$ from the server. But the server can check $H(K_3 || N_{once2})$ to verify the user's identity. These steps can achieve security from mutual authentication.

4.1.3. Low Computational Cost: In Cui and Cao's scheme [1], the server verifies the validity of the recovered identifier ID_i by checking $wID_i^{h(K_{ij}||Z||w||T)} \stackrel{?}{=} x_i^e \pmod N$. If this equation holds, the server is convinced that the user is an authorized user. However, in

this phase, the server expends resources to verify the equation and generate D_i, and then send it to the user for certification. In our proposed scheme, the server does not require huge computing cost to find legitimate users. The server just calculates K_1 to decrypt M_1 and verifies $H(2^{array_{ID_i}} P)$, and then finds the index value of the legal user. In our proposed scheme, the cost of computation and time of communication is less than Cui and Cao's method.

4.2. Comparison

The following table compares the properties of the proposed scheme and previous schemes:

C1: No password table required

C2: Mutual authentication

C3: Low communication and computation cost

C4: Time-synchronization is not required

C5: The user is not required to know the system or other participant's public key

C6: The identity of the user will be protected

C7: Illegitimate servers cannot deceive the user

C8: Users cannot be masqueraded to obtain services from the server

C9: Denial of service attack is not effective in this protocol

C10: Improve the accuracy of the reliability and safety analysis

Table 1. Properties of the Proposed Scheme versus Previous Schemes

	Lee-Chang's protocol	SIKA	Cui-Cao's protocol	Our protocol
C1	Yes	Yes	Yes	Yes
C2	No	Yes	No	Yes
C3	No	No	Yes	Yes
C4	No	No	Yes	Yes
C5	No	No	Yes	Yes
C6	No	Yes	Yes	Yes
C7	No	Yes	Yes	Yes
C8	Yes	No	Yes	Yes
C9	Yes	Yes	Yes	Yes
C10	No	No	Yes	Yes

5. Conclusion

In this paper, we review Cui and Cao's scheme [1] and discuss the major drawbacks of their scheme. Then we proposed an improved scheme that not only maintains all the benefits of the Cui and Cao's scheme but also reduces the computational cost and search time. Our proposed scheme also achieves the goal preventing attackers from identifying users in a distributed networks environment.

Acknowledgements

This work was supported by NSC 100-2221-E-224-016.

Excursus

Portions of this paper were presented at the 4th International Conference on Advanced Communication and Networking (ACN 2012), August 30-31, Jeju, Korea, 2012.

References

[1] H. Cui and T. Cao, "A Secure Anonymous Identity-based Key Agreement Protocol for Distributed Computer Networks", Journal of Networks, vol. 6, no. 9, **(2011)** September, pp. 1337-1343.
[2] W. Diffie and M. Hellman, "New directions in cryptography", IEEE Transactions on Information Theory IT, vol. 22, no.6, **(1976)**, pp. 644-654.
[3] T. ElGamal, "A public-key crypto system and a signature scheme based on discrete logarithms", IEEE Transactions on Information Theory IT, vol. 31, no. 4, **(1985)**, pp. 469-472.
[4] C. L. Hsu and Y. -H. Chuang, "A novel user identification scheme with key distribution preserving user anonymity for distributed computer networks", Information Sciences, vol. 179, **(2009)**, pp. 422-429.
[5] W. B. Lee and C. C. Chang, "User identification and key distribution maintaining anonymity for distributed computer network", Computer Systems Science and Engineering, vol. 15, no. 4, **(1999)**, pp. 113-116.
[6] K. Mangipudi and R. Katti, "A secure identification and key agreement protocol with user anonymity (SIKA)", Computers and Security, vol. 25, no. 6, **(2006)**, pp. 420-425.
[7] B. Z. Wan, Z. G., Kankanhalli, M. S. Feng and B. Deng, "Anonymous secure routing immobile ad-hoc networks", Local Computer Networks, Annual IEEE International Conference, **(2004)** November 16-18, pp. 102 -108.
[8] T. S. Wu and C. L. Hsu, "Efficient user identification scheme with key distri bution preserving anonymity for distr ibuted computer networks", Computers and Security, vol. 23, no. 2, **(2004)**, pp. 120-125.
[9] Y. Yang, S. Wang, F. Bao, J. Wang and R. H. Deng, "New efficient user iden tification and key distribution scheme providing enhanced security", Computers and Security, vol. 23, no. 8, **(2004)**, pp. 697-704.
[10] H. Cui and T. Cao, "A New Secure Anonymous Protocol for Distributed Computer Networks", Proceedings of the Third International Symposium on Electronic Commerce and Security Workshops, **(2010)**, pp. 197-201.
[11] J. W. Byun, D. H. Lee and J. I. Lim, "EC2C-PAKA, An Efficient Client-to-Client Password-authenticated Key Agreement", Information Science, vol. 177, no. 19, **(2007)**, pp. 3995-4013.
[12] Y. Cai and Y. Wang, "Identity-based Conference Key Distribution Protocol with User Anonymity", Chinese Journal of Electronica, vol. 16, no. 1, **(2008)**, pp. 179-181.
[13] T. J. Cao and H. Lei, "Privacy-enhancing Authenticated Key Agreement Protocols based on Elliptic Curve Cryptosystem", Acta Electronica Sinica, vol. 36, no. 2, **(2008)**, pp. 397-401.
[14] A. O. Freier, P. Karlton and P. C. Kocher, "Secure Socket Layer 3.0", Internet Draft, **(1996)**.
[15] L. Chen, Z. Cheng and N. P. Smart, "Identity-based Key Agreement Protocols from Pairings", International Journal of Information Security, vol. 6, no. 4, **(2007)**, pp. 213-241.
[16] J. Kohl and C. Neuman, "The Kerberos Authentication Service (v5)", Internet RFC 1510, **(1993)**.
[17] R. Rivest, A. Shamir and L. Adleman, "A Method for obtaining Digital Signature and Public-Key Cryptosystem", Communications of the ACM, vol. 21, no. 2, **(1978)**, pp. 120-126.
[18] T. C. Wu, T. T. Huang, C. L. Hsu and K. Y. Tsai, "Recursive Protocol for group-oriented Authentication with Key Distribution", Journal of Systems and Software, vol. 81, no. 7, **(2008)**, pp. 1227-1239.
[19] Y. Yang, S. Wang, F. Bao, J. Wang and R. H. Deng, "New Efficient User Identification and Key Distribution Scheme Providing Enhanced Security", Computers and Security, vol. 23, no. 8, **(2004)**, pp. 697-704.

Authors

Kai Chain

He received the M.S. degree in Electrical Engineering from National Taiwan University in 2001-2003. He is a lecturer in the Department of Computer and Information Science at the Republic of China Military Academy. He is currently pursuing his Ph.D. degree in Cryptography from the Institute of Computer Science and Communication Engineering at National Cheng Kung University under Profs. Chi-Sung Laih and Jar-Ferr Yang. His research interests include Network and Information Security, with a concentration on applied Cryptography.

Wen-Chung Kuo

He received the B.S. degree in Electrical Engineering from National Cheng Kung University and M.S. degree in Electrical Engineering from National Sun Yat-Sen University in 1990 and 1992, respectively. Then, He received the Ph.D. degree from National Cheng Kung University in 1996. Now, he is an associate professor in the Department of Computer Science and Information Engineering at National Yunlin University of Science & Technology. His research interests include steganography, cryptography, network security and signal processing.

Jiin-Chiou Cheng

He received his M.S. degree in Communication Engineering from National Chiao Tung University, Taiwan, R.O.C. in 1985 and Ph.D. degree in Electrical Engineering form National Cheng Kung University in 2009. He is an associate professor in the Department of Computer Science and Information Engineering at Southern Taiwan University from 1990. He is engaged in the research of application of Elliptic Curve Cryptography. His research interests also include network security and Stegography.