Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/090156

An Efficient Dynamic ID-based User Authentication Scheme using Smart Cards without Verifier Tables

Tian-Fu Lee[*]

Department of Medical Informatics, Tzu Chi University, No.701, Zhongyang Rd., Sec .3, Hualien, 97004, Taiwan, R.O.C.

Received: 23 Apr. 2014, Revised: 24 Jul. 2014, Accepted: 25 Jul. 2014
Published online: 1 Jan. 2015

Abstract: Smart-card based user authentication schemes provide that legal users conveniently and securely access remote services with smart cards through unsecure networks. Lee recently showed that the dynamic ID-based remote user authentication scheme proposed by Das et al. cannot resist password guessing attacks and impersonation attacks. In order to solve these weaknesses, Lee also presented an improved authentication scheme and claimed that the proposed scheme can resist modification, password guessing, impersonation and smart-card-theft attacks. However, this investigation indicates that the authentication scheme of Lee cannot resist the above attacks and violates users' untracibility. Additionally, this investigation also develops an efficient and secure dynamic ID-based user authentication scheme based on the quadratic residues. The proposed scheme not only avoids the weakness in the previous schemes, but also does not require verifier tables in the authentication server and still retains low computational cost in clients.

Keywords: smart card, password, authentication, dynamic ID, network security

1 Introduction

A smart-card based user authentication scheme provides that legal users use smart cards to access remote services conveniently and securely. It is widely used in open communication networks. Recently, numerous smart-card based authentication approaches were proposed. For example, Das et al.[1] in 2004 proposed a smart-card based remote user authentication scheme, which used the dynamic ID to prevent the leakage of identity information during login and to resist ID-theft attacks. Later, Liao et al. [2] showed that the scheme of Das et al. cannot protect against guessing attack and proposed an enhanced scheme that achieves mutual authentication. However, Misbahuddin et al. [3] in 2008 showed that the scheme of Liao et al. cannot withstand impersonation attack and reflection attack. Wang et al. [4] in 2009 proposed an improved scheme to correct security flaws of the scheme of Das et al. Nevertheless, their improved scheme still cannot resist the password guessing, masquerade, denial of service and modification attacks [5,6]. Additionally, several researches on this issue were continually presented [7,8,9,10,11,12,13,14].

Lee in 2012 [15] also demonstrated that the authentication scheme of Das et al. cannot resist password guessing attacks and impersonation attacks, and then proposed an improved scheme for security enhancement. The improved scheme also tried to use a dynamic ID and a nonce for each login in order to prevent attackers from tracibility such that an adversary cannot trace the users. However, the authentication scheme of Lee used a common secret key to encrypt each user's password such that any malicious legal user can employ the common secret key to perform off-line password guessing, impersonation attacks and modification attacks, and to trace the other users. Besides, if an adversary steals a smart card, then he/she can derive the knowledge about the user's password. Subsequently, he/she can impersonate the legal user and successfully login the authentication server. That is, the scheme of Lee still cannot withstand the smart-card-theft attack. Many authentication schemes tried to use lower computational operations such as one-way hash or exclusive-or (Xor) operations to solve users' privacy problems. However, if the authentication server does not use verifier tables to keep users' secrets, that is, each user and the authentication server do not share any secret, it is hard to resist insider attacks.

This investigation first discusses the weakness of the authentication scheme of Lee, and then presents an efficient and secure dynamic ID-based authentication

[*] Corresponding author e-mail: jackytflee@mail.tcu.edu.tw, tflee@ismail.csie.ncku.edu.tw

scheme based on the quadratic residue assumption. The proposed scheme uses the server's secret key to hide the user's identity with hash functions and keeps this hidden user's identity in the smart card such that none can verify users' identities except the authentication server. Then, the user employs the server's public key (a modular squaring operation) to encrypt the hidden user's identity and sends the ciphertext to the authentication server. Therefore, the proposed scheme can keep users' privacy and untraceability, and resist the insider attacks and possible attacks.. Although using the quadratic residues requires more computations in the authentication server, the proposed scheme still retains low computational cost in clients, and keeps a constant computational cost in the authentication server. Additionally, the server does not require the verifier table for storing users' secrets.

The remainder of this investigation is organized as follows. Section 2 reviews the concepts of the dynamic ID-based authentication scheme of Lee, and describes the weaknesses of the authentication scheme of Lee. Section 3 presents the proposed scheme based on the quadratic residues assumption without verifier tables. Section 4 provides security analysis and performance evaluation of the proposed authentication scheme. Finally, Section 5 draws conclusions.

2 Related Works

This section first explicates the used notation and definition, and then briefly reviews the authentication scheme created by Lee and its weaknesses. Assume that U_i is the qualified user; S is the authentication server, which the U_i is registered in. PW_i is the password of U_i. Table 1 details the notation throughout this investigation.

Table 1 Notations

Notations	Meanings
x	The secret key of S.
DID_i	The user's dynamic identity.
T	A timestamp.
$\oplus$	The bitwise Xor operator.
$h(M)$	A one-way hash function applied to M.
$A \rightarrow B : M$	A sends M to B through a common channel.
$A \Rightarrow B : M$	A sends M to B through an authenticated and private channel.

2.1 Quadratic Residue Assumption

Let $n = p \times q$, where p and q are two large primes. The symbol QR_n denotes the set of all quadratic residues in [1, n-1]. If $y = x^2 \bmod n$ has a solution, i.e. $\exists$ a square root for y, then y is a quadratic residue modulo n. Assume that $y \in QR_n$. It is computationally infeasible to find x satisfying $y = x^2 \bmod n$ without the knowledge of p and q since no polynomial algorithm has been found to solve the factoring problem [16,17,18].

2.2 The authentication scheme of Lee

The authentication scheme of Lee includes registration phase, authentication phase, and password update phase.

2.2.1 Registration phase

LR-1 $U_i \Rightarrow S : PW_i$
The user U_i sends password PW_i to the remote server S.
LR-2 $S \Rightarrow U_i$: smart card
The server S computes $N_i = h(PW_i) \oplus h(x)$, installs $\{h(.), N_i, h(x)\}$ in the smart card, and sends the smart card to U_i.

2.2.2 Authentication phase

The authentication phase comprises login phase and verification phase, which describe as follows.

Login phase
U_i inserts his/her smart card into the card-reader, inputs password PW_i, and performs the following steps.
LL-1 Generate a random number R and compute $DID_i = h(PW_i) \oplus h(N_i \oplus h(x) \oplus R)$.
LL-2 Compute $B_i = h(N_i \oplus h(N_i \oplus h(x)) \oplus R)$.
LL-3 Compute $C_i = h(B_i \oplus h(x)) \oplus T)$, where T is the current timestamp.
LL-4 $U_i \rightarrow S : \{DID_i, C_i, T\}$
Then U_i sends $\{DID_i, C_i, T\}$ to S.

Verification phase
Upon receiving the login message from U_i, S performs the following steps.
LV-1 Verify the validity of timestamp T.
LV-2 Compute $B_i' = h(DID_i \oplus h(x))$.
LV-3 Compute $C_i' = h(B_i' \oplus h(x) \oplus T)$ and check $C_i' = ?C_i$. If successful, accept this login request; otherwise, reject this request.

2.2.3 Password update phase

In this authentication scheme, users are allowed to freely update their passwords by performing the following steps.
U-1 U_i inserts his/her smart card into the card-reader and inputs his/ her password PW_i.
U-2 U_i chooses a new password $PW_{i(new)}$.
U-3 Next, the smart card computes $N_{i(new)} = N_i \oplus h(PW_i) \oplus h(PW_{i(new)})$.

U-4 Finally, the smart card updates N_i as $N_{i(new)}$. Then U_i can use the new password $PW_{i(new)}$ to login the authentication server S.

2.3 The weaknesses of the scheme of Lee

This subsection will demonstrates that the authentication scheme of Lee is not secure against smart-card-theft attacks, and a malicious legal user can employ the common secret key $h(x)$ to conduct off-line password guessing attacks and traces a fixed user U_i. Additionally, this malicious user can employ the secret $h(x)$ and used messages to perform impersonation attacks and modification attacks. The scenarios are described as follows.

2.3.1 Security against smart-card-theft attacks

If the adversary steals a smart card, then he/she can impersonate the user U_i and successfully login the authentication server S. First, he/she gets $\{h(.), N_i, h(x)\}$ from the smart card and derive PW_i from $N_i \oplus h(x)$. Next, he/she selects a random number R^*, computes $DID_i{}^* = h(PW_i) \oplus R^*$, $B_i{}^* = h(N_i \oplus R^*)$ and $C_i{}^* = h(B_i)^* \oplus h(x) \oplus T$. Then he/she sends $\{DID_i, C_i{}^*, T\}$ to S. After receiving the login message, S will verify T and compute $B_i{}' = h(DID_i^* \oplus h(x) (= h(h(PW_i) \oplus R^* \oplus h(x)) = h(N_i \oplus R^*))$ and $C_i{}' = h(B_i{}' \oplus h(x) \oplus T)$. Thus, S will successfully verify $C_i{}'$ and C_i, and accept this login request.

2.3.2 Security against impersonation attacks

The malicious legal user U_j tries to impersonate another user U_i. When U_i communicates with S, U_j copies the message $\{DID_i, C_i, T\}$. Next, he/she computes $B_i{}^* = h(DID_i \oplus h(x))$ and $C_i{}^* = h(B_i{}^* \oplus h(x) \oplus T')$, where T' is the current timestamp. Then U_j impersonate another user U_i and sends $\{DID_i, C_i{}^*, T\}$ to S. After receiving the login message, S verifies the validity of timestamp T' and computes $B_i{}' = h(DID_i \oplus h(x)$ and $C_i{}' = h(B_i{}' \oplus h(x) \oplus T)$. Then S will successfully verify that $C_i{}'$ and C_i are equal, and accept this login request.

2.3.3 Security against modification attacks

The malicious legal user U_j tries to modify the communications between U_i and S, and intercepts the message $\{DID_i, C_i, T\}$. Next, he/she selects a random number R^*, computes $DID_i{}^* = DID_i \oplus R^*$, $B_i^* = h(DID_i^* \oplus h(x))$ and $C_i{}^* = h(B_i{}^* \oplus h(x) \oplus T')$. Then U_j sends DID_i^*, C_i^*, T to S. After receiving the login message, S successfully verifies T and computes $B_i{}' = h(DID_i^* \oplus h(x)$ and $C_i{}' = h(B_i{}' \oplus h(x) \oplus T)$ since U_j only requires the time of computing four Xor operations and two hash operations to modify the transmitted message and the spent time is within the range of tolerable time [22]. Finally, S will verify $C_i{}'$ and C_i, and accept this login request.

2.3.4 Security against off-line password guessing attacks

The malicious legal user U_j has the secret $h(x)$ and tries to perform off-line password guessing attacks. When U_i communicates with S, U_j copies the message $\{DID_i, C_i, T\}$, guesses PW_i^* for U_i, and computes $N_i^* = h(PW_i^*) \oplus h(x)$, $B_i^* = h(N_i^* \oplus DID_i \oplus h(PW_i^*))$ and $C_i{}^* = h(B_i{}^* \oplus h(x) \oplus T)$. Next, U_j checks whether $C_i{}^*$ and C_i are equal or not. If false, he/she repeats guessing a new password PW_i^* and performing the same steps until $C_i{}^*$ and C_i are equal.

2.3.5 Violating users' untracibility

The malicious legal user can derive another user's password PW_i by performing the off-line password guessing attacks, he/she can trace a fixed U_i by PW_i.

3 The proposed dynamic ID-based user authentication scheme without verifier tables

This section proposes an efficient dynamic ID-based authentication scheme using smart cards. An authentication scheme only uses the one-way hash functions and exclusive-or (Xor) operations to solve users' privacy problems. If the authentication server does not use verifier tables to keep users' secrets, it is hard to resist the insider attacks. Thus, the proposed employs the quadratic residues to solve the problems of user privacy and untraceability. Although using the quadratic residues requires more computations in the authentication server, the proposed still retains low computational cost in clients and keeps a constant computational cost in the server. The proposed password authentication scheme consists of registration, authentication, and password update phases, which works as follows.

3.1 Registration phase

LR-1 $U_i \Rightarrow S : PW_i$
The user U_i sends password PW_i to the remote server S.
LR-2 $S \Rightarrow U_i$: smart card
The server S computes $M_i = h(ID_i \oplus x)$ and $N_i = ID_i \oplus h(PW_i)$, installs $\{h(.), M_i, N_i, n\}$ in the smart card,, where p and q are two large primes and $n = p \times q$, and sends the smart card to U_i.

3.2 Authentication phase

The authentication phase also comprises login phase and verification phase, which describe as follows.

Login phase
U_i inserts his/her smart card into the card-reader, inputs his/her password PW_i, and performs the following steps.
LL-1 Compute $ID_i = N_i \oplus h(PW_i)$, $b = h(M_i \oplus T)$ and $DID_i = ID_i \oplus b$, where T is the current timestamp.
LL-2 Compute $B_i = h(N_i \oplus h(N_i \oplus h(x)) \oplus R)$.
LL-3 Compute $C_i = b^2 \mod n$.
LL-4 $U_i \rightarrow S : \{DID_i, C_i, T\}$
Then U_i sends $\{DID_i, C_i, T\}$ to S.

Verification phase
Upon receiving the login message from U_i, S performs the following steps.
LV-1 Verify the validity of timestamp T.
LV-2 Solve C_i by using the Chinese Remainder with p and q to obtain four (b_1, b_2, b_3, b_4).
LV-3 Determine b by checking $h(h(b_i \oplus DID_i \oplus x) \oplus T) =? b$. If successful, accept this login request; otherwise, reject this request.

The password update phase of the proposed scheme is similar to that of the scheme of Lee, and thus is not presented herein.

4 Security analysis and performance evaluation

This section analyzes the security of the proposed authentication scheme, which includes resisting impersonation, replay, password guessing, modification, smart-card-theft attacks, and providing anonymity and unlinkability, and evaluates the performance.

4.1 Security analysis

4.1.1 Resisting impersonation attacks

In the proposed scheme, only U_i can compute $ID_i = N_i \oplus h(PW_i)$, $b = h(M_i \oplus T)$ and $DID_i = ID_i \oplus b$ since only he/she has the secrets N_i, M_i and password PW_i. The authentication server S authenticates U_i by checking $h(h(b_i \oplus DID_i \oplus x) \oplus T) =? b$ for $i = 1, 2, 3, 4$ in Step LV-3, and thus the proposed scheme can resist impersonation attacks.
Note that:
$h(h(b \oplus DID_i \oplus x) \oplus T) = h(h(b \oplus (ID_i \oplus b) \oplus x) \oplus T) = h(h(ID_i \oplus x) \oplus T) = h(M_i \oplus T) = b$

4.1.2 Providing users' anonymity

In the proposed scheme, DID_i and C_i implicitly involve the user's identity ID_i. An attacker cannot solve b from C_i, where $C_i = b^2 \mod n$ and $b = h(M_i \oplus T)$, because of the quadratic residue assumption. Also, he/she cannot obtain ID_i form $DID_i (= ID_i \oplus b)$ due to the one-way property of the hash function. Thus the proposed scheme provides anonymity.

4.1.3 Providing data unlinkability

The proposed authentication scheme provides users' login with the dynamic identity $DID_i (= ID_i \oplus b)$, in which $b (= h(M_i \oplus T))$ is generated in different runs and is independent due to the one-way property of the hash function. So is $C_i (= b^2 \mod n)$. Thus, the proposed scheme exhibits the property of unlinkability.

4.1.4 Preventing replay attacks

In the proposed authentication scheme, an attacker cannot correctly modifies DID_i, C_i and T without ID_i, PW_i, N_i, M_i, and x, where $ID_i = N_i \oplus h(PW_i)$, $b = h(M_i \oplus T)$, $DID_i = ID_i \oplus b$ and $C_i = b^2 \mod n$. When an attacker tries to use the previous message $\{DID_i, C_i, T\}$ to login S, a failed attack will be detected by checking the invalid timestamp T. Thus, the proposed authentication scheme is secure against the replay attacks.

4.1.5 Resisting password guessing attacks

In the proposed scheme, the password PW_i (or $h(PW_i)$) is not related to the communicating message $\{DID_i, C_i, T\}$. An attacker cannot derive the valuable information about PW_i (or $h(PW_i)$) from $\{DID_i, C_i, T\}$, and thus has no enough information to verify the guess. Furthermore, even if the adversary obtains the smart card and gets $\{h(.), M_i, N_i, n\}$. When he/she inputs a candidate password PW_i^* computes $ID_i^* = N_i \oplus h(PW_i^*)$, $b = h(M_i \oplus T)$, $DID_i^* = ID_i^* \oplus b$ and $C_i = b^2 \mod n$, his/her attempt fails because that he/she still has no enough information to verify the guess. If the attacker tries to send $\{DID_i^*, C_i, T\}$ to S, then a failed attack will be detected by S since he/she has no corrected password. Thus, the proposed authentication scheme is secure against the password guessing attacks.

4.1.6 Resisting smart-card-theft attacks

If an adversary steals a smart card, then he/she cannot derive the valuable information about password from the message $\{h(.), M_i, N_i, n\}$ in the smart card since ID_i in $M_i (= h(ID_i \oplus x))$ is protected by S's long-term secret key

x and the one-way hash function $h(.)$, and PW_i in $N_i(= ID_i \oplus h(PW_i))$ is encrypted with ID_i. Thus, the adversary has no enough information to verify the password guessing. Besides, if the adversary tries to guess a password to log into the system, then a fail attack will be detected by S since the adversary has no corrected password.

4.1.7 Resisting modification attacks

For each user U_i whose password is PW_i and identity ID_i, secrets $N_i(= ID_i \oplus h(PW_i))$ and $M_i(= h(ID_i \oplus x))$, where x is S's secret key, the temporary secret $b(= h(M_i \oplus T))$ is fixed in the timestamp T. Thus, $DID_i(= ID_i \oplus b)$ and $C_i(= b^2 \mod n)$ are also fixed and cannot be modified. Therefore, if an outside attacker or a malicious legal user U_j, who has no the knowledge of x, PW_i, ID_i, M_i and N_i, tries to modify the message $\{DID_i, C_i, T\}$ between U_i and S. S will detect the failed attack and reject this login request.

4.2 Performance evaluation

The authentication phase of the scheme of Lee requires generating a nonce, four hash operations and six Xor operations in clients, and requires two hash operations and three Xor operations in the authentication server. The authentication phase of the proposed scheme requires two hash operations, two Xor operations and a modular squaring operation in clients, and requires eight hash operations, twelve Xor operations and one squaring root solving operation in the authentication server.

The traditional hash function MD5 costs 16 K gates; SHA-1 costs 20 K gates; and the universal hash function still requires 1.7 K gates. Nevertheless, the implementation of a modular squaring can be reduced to only a few hundred gate-equivalents [18,19,20,21], and is not more expensive than the implementation of a hash function. Thus, a modular squaring operation will not affect the efficiency of the client in the proposed scheme.

Besides, although the proposed authentication scheme requires one squaring root solving operation and more hash and Xor operations in the server, it ensures users authentication and guarantees security against possible attacks.

5 Conclusions

This investigation addresses the weaknesses of the dynamic ID-based authentication scheme of Lee, including suffering from the modification, password guessing, impersonation and smart-card-theft attacks, and violating users' untracibility. This investigation also presents an efficient and secure dynamic ID-based authentication scheme using smart cards. The proposed authentication scheme is based on quadratic residues and solves the security problems in previous schemes and withstands possible attacks. Although the proposed authentication scheme uses the public-key cryptosystem to solve the security problems, it still keeps low computational cost in clients and an invariable response time in the authentication server. Additionally, the server does not require verifier tables for storing users' secrets. Thus the proposed authentication scheme is suitable for practical environment.

Acknowledgement

The authors are grateful to the Editor-in-Chief and the anonymous referee for valuable and helpful comments. This work was supported in part by the National Science Council of the Republic of China under the Grant NSC 100-2221-E-320-003 and NSC 101-2221-E-320-004.

References

[1] M.L. Das, A. Saxena and V.P. Gulati, A Dynamic ID-based Remote User Authentication Scheme. IEEE Transactions on Consumer Electronics **50**, 629-631 (2004).
[2] I.E. Liao, C.C. Lee and M.S. Hwang, Security Enhancement for A Dynamic ID-Based Remote User Authentication Scheme. Proceedings of the International Conference on the Next Generation Web Services Practices, 22-26 (2005).
[3] M. Misbahuddin and C.S. Bindu, Cryptanalysis of Liao-Lee-Hwang's Dynamic ID Scheme. International Journal of Network Security **6**, 211-213 (2008).
[4] Y.Y. Wang, J.Y. Liu, F.X. Xia and J. Dan, A More Efficient and Secure Dynamic ID-Based Remote User Authentication Scheme. Computer Communications,**32**, 586-585 (2009).
[5] M.A. Ahmed, D.R. Lakshmi and S.A. Sattar, Cryptanalysis of A More Efficient and Secure Dynamic ID-Based Remote User Authentication Scheme. International Journal of Network Security & Its Applications **1**, 32-37 (2009).
[6] H. Lee, D. Choi, Y. Lee, D. Won and S. Kim, Security Weaknesses of Dynamic ID-based Remote User Authentication Protocol. Proceedings of the World Academy of Science Engineering and Technology, Is. **59**, 190-193 (2009).
[7] H.M. Sun, An Efficient Remote User Authentication Scheme Using Smart Cards. IEEE Transactions on Consumer Electronics **46**, 958-961 (2000).
[8] J.J. Shen, C.W. Lin and M.S. Hwang, A Modified Remote User Authentication Scheme Using Smart Cards. IEEE Transactions on Consumer Electronics **49**, 414-416 (2003).
[9] A.K. Awasthi and S. Lal, A Remote User Authentication Scheme Using Smart Cards with Forward Secrecy. IEEE Transactions on Consumer Electronics **49**, 1246-1248 (2003).
[10] A.K Awasthi, Comment on A Dynamic ID-based Remote User Authentication Scheme. Transaction on Cryptology **1**, 15-16 (2004).
[11] W.C. Ku and S.T. Chang, Impersonation Attack on a Dynamic ID-Based Remote User Authentication Scheme Using Smart Cards. IEICE Transactions on Communications **E88-B**, 2165-2167 (2005).

[12] Y.P. Liao and S.S. Wang, A Secure Dynamic ID-Based Remote User Authentication Scheme for Multi-Server Environments. Computer Standards & Interfaces **31**, 24-29 (2009).
[13] M. Misbahuddin, M.A. Ahmed, A.A. Rao, C.S. Bindu and M.A.M. Khan, A Novel Dynamic ID-Based Remote User Authentication Scheme. Proceedings of the 2006 Annual India Conference, 1-5 (2006).
[14] X. Zhang, Q. Feng and M. Li, A Modified Dynamic ID-based Remote User Authentication Scheme. Proceedings of the 2006 International Conference on Communications, Circuits and Systems **3**, 1602-1604 (2006).
[15] CT Li, MS Hwang, An efficient biometrics-based remote user authentication scheme using smart cards, Journal of Network and Computer Applications, Elsevier, (2010).
[16] W. Patterson, Mathematical Cryptology for Computer Scientists and Mathematicians, Rowman (1987).
[17] K. H. Rosen, Elementary Number Theory and its Applications, Addison-Wesley, Reading, MA (1988).
[18] Y. Chen, J.S. Chou and H.M. Sun, A Novel Mutual-Authentication Scheme Based on Quadratic Residues for RFID Systems. Computer Networks **52**, 2373-2380 (2008).
[19] M.B. Burmester, R. Medeiros and R. Motta, Robust, Anonymous RFID Authentication with Constant Key-Lookup, Proceedings of the 2008 ACM symposium on Information, computer and communications security, 283-291 (2008).
[20] P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador and A. Ribagorda, M2AP: A Minimalist Mutual-Authentication Protocol for Low-Cost RFID Tags, Proceedings of International Conference on Ubiquitous Intelligence and Computing UIC'06, LNCS **4195**, 912-923 (2006).
[21] A. Shamir, Squash: A New One-Way Hash Function with Provable Security Properties for Highly Constrained Devices such as RFID Tags, in: Invited Talk, International Conference on RFID Security (RFIDSec'07), (2007).
[22] J. Kurose, K. Ross, Computer Networking: A Top Down Approach Featuring the Internet, Addison-Wesley, 276-279 (2000).

Tian-Fu Lee received his B.S. degree in Applied Mathematics from National Chung Hsing University, Taiwan, his M.S. degree in Computer Science and Information Engineering from National Chung Cheng University, Taiwan, and his Ph.D. degree in Department of Computer Science and Information Engineering, National Cheng Kung University, Taiwan. He works as an associate professor in Department of Medical Informatics, Tzu Chi University. His research interests include Cryptography, Network security, Medical information security, Wireless networks, Algorithmic graph theory, Database and data engineering.