Study on A Secure Remote User Authentication Scheme Using Smart Cards[1]

Jin Qiuyan, Kwangwoo Lee and Dongho Won[2]

Information Security Group, Sungkyunkwan University, Korea
{qyjin,kwlee,dhwon}@security.re.kr

Abstract

Remote user authentication scheme is a kind of way to authenticate the communication parties who transmit messages through an insecure channel. Researchers in this area have proposed some approaches during the last couple of decades. Unfortunately, most of them are proved to be insecure against various attacks. In 2009, Kim and Chung improved Yoon and Yoo's scheme, and claimed that their scheme can prevent masquerading attack as well as resist to other malicious attacks. However, we found that Kim and Chung's scheme is still not secure enough, especially in preventing off-line password guessing attack. In this study, we proposed a more secure and practical remote user authentication scheme to resolve all of the aforementioned security vulnerabilities while preserving the merits of Kim-Chung's scheme.

Keywords: *Remote user authentication, Cryptanalysis, Smart card, Network security*

1. Introduction

During the last couples of decades, remote user authentication scheme [1-10] has become one of the most convenient mechanisms which authenticate the communication parties who transmit messages through insecure channel. In the smart card based remote user authentication scheme, three essential phases are contained: registration, login and authentication phase. Usually, there are three components in remote user authentication scheme: a remote server, a remote user and an insecure channel. Recently, Manoj Kumar [1] summarized some security flaws in the three components:

• Security Flaws Due to Remote User

A remote user, who registers to get the access of a remote sever, can use his identity and password to get the certificate from the server and request to login. A malicious legal user can get some secret data of the remote server by using the certificate. Also, the user can construct some kinds of guessing attacks and impersonation attacks.

• Security Flaws Due to Remote Server

One of the most powerful attackers is the insider at the server. He can get the information sent to the server in a secure channel. With the information, the attacker can guess the password of the remote user and get some useful information stored at the server. Even with the information, the attacker can impersonation as a server and communicate with some other users.

• Security Flaws Due to Insecure Channel

[1] Extened abstract of "A Practical and Secure Remote User Authentication Scheme Using Smart Cards" published in conference proceeding of the ASP 2012
[2] Correspondence author : Dongho Won (dhwon@security.re.kr)

In a remote user authentication mechanism, it is assumed that all the information transmitted through the insecure channel can be intercepted by attackers. Some information forging and attacks may be constructed by the attacker who obtains the intercepted information.

In 2009, Kim-Chung proposed a secure remote user authentication scheme [2] which is an improvement of Yoon-Yoo's scheme [3], unfortunately, some security flaws are presented by C.-T. Li [4] and Horng [5]. Considering the vulnerabilities summarized above, in this paper we proposed a more secure remote authentication scheme which is an improvement of Kim and Chung's scheme. Our scheme keeps the merits of Kim-Chung's scheme and is secure against the possible attacks.

The rest of the paper is organized as follows. In Section 2, we briefly review Kim-Chung's scheme. In Section 3, we show security weaknesses of Kim-Chung's scheme. The proposed scheme and the security analysis are presented in Section 4 and Section 5. Also, we compare our scheme with some related schemes in Section 6. Finally, we conclude this paper in Section 7.

2. A Review of Kim-Chung's Scheme

In this section, we review the remote user authentication scheme proposed by Kim and Chung. Kim-Chung's scheme consists of four phases: registration, login, verification and password change phases. For convenience of description, terminology and notations used in the paper are summarized in Table 1.

Table 1. Terminology and Notations used in the Paper

Symbol	Description
U	A user
ID, PW, SC	U 's identity, password and the smart card of U
N	Random number unique to U
x	S 's master secret key, which is kept secret and only known by S . $\|x\|$ is a security parameter
S	A remote server
$\otimes$	The bitwise XOR operation
$h(.)$	A collision free one-way hash function
$\|$	String concatenation
$\Rightarrow$	A secure channel
$\rightarrow$	A public channel

2.1 Registration Phase

In this phase, the user U initially registers with the server S as follows:

(1) $U \Rightarrow S: \{ID, PW\}$. U selects his ID and PW then sends them to S over a secure channel.

(2)After receiving ID and PW, S computes $K_1 = h(ID \oplus x) \oplus N$ and $K_2 = h(ID \oplus x \oplus N) \oplus h(PW \oplus h(PW))$, where N is a random number unique to the user U. Then, S computes $R = K_1 \oplus h(PW)$.

(3) S stores the secure information K_1, K_2, R, and $h(.)$ into U 's smart card SC.

(4) $S \Rightarrow U : \{SC\}$. S sends the smart card SC through a secure channel to U then completes the registration phase.

2.2 Login Phase

When U wants to login to S , he sends a login request message.

(1) U inserts his SC into a card reader and inputs his ID and PW .

(2) SC computes $C_1 = R \oplus h(PW)$. If C_1 is not equal to the stored K_1 , then SC rejects the login request. Otherwise, it computes $C_1^{'} = K_2 \oplus h(PW \oplus h(PW))$ and $C_2 = h(C_1^{'} \oplus T_1)$, where T_1 is the current timestamp.

(3) $U \rightarrow S : \{ID, T_1, C_1, C_2\}$

2.3 Verification Phase

(1) After receiving the login message $\{ID, T_1, C_1, C_2\}$, S checks U 's ID and the freshness of T_1 .

(2) If ID is not valid or T_1 is not fresh, S rejects the session. Otherwise, S computes $N^{'} = C_1 \oplus h(ID \oplus x)$. S terminates the current session if computed $h(h(ID \oplus x \oplus N^{'}) \oplus T_1)$ is not equal to the received C_2 . Otherwise, S computes $C_3 = h(h(ID \oplus x \oplus N^{'} \oplus C_2 \oplus T_2)$, where T_2 is the current timestamp.

(3) $S \rightarrow U : \{T_2, C_3\}$.

(4) Receiving $\{T_2, C_3\}$, U first checks the freshness of T_2 . If T_2 is not fresh or $h(C_1^{'} \oplus C_2 \oplus T_2)$ is not equal to the received C_3 , U terminates the current session. Otherwise, U has successfully authenticated S .

2.4 Password Change Phase

(1) U inserts his SC into a card reader or a terminal then inputs his ID and PW .

(2) The smart card computes $K_1^{'} = R \oplus h(PW)$ with the received PW . If $K_1^{'}$ is not equal to stored K_1 , SC rejects the password change request. Otherwise, U inputs a new password $PW^{'}$.

(3) The smart card computes $R^{'} = \oplus h(PW^{'})$ and $K_2^{'} = K_2 \oplus h(\mathrm{PW} \oplus h(PW)) \oplus h(PW^{'} \oplus h(PW^{'}))$. Then, it replaces R and K_2 with $R^{'}$ and $K_2^{'}$.

3. Security Analysis of Kim-Chung's Scheme

3.1 Off-line Password Guessing Attack through Password Change Phase [6]

An attacker UA can guess the password PW^{*} of U through initiating the password change phase. UA inserts the stolen SC of U into the smart card reader or a terminal, then

enters ID of U which he can get from intercepting the login request and a guessed PW^*. SC allows UA to enter a new password if the verification of password change phase has been successfully implemented. It means UA guesses the correct password of U successfully; otherwise UA tries again.

3.2 Off-line Password Guessing Attack

Suppose an attacker steals U 's smart card SC and obtains the information $\{K_1, K_2, R, h(.)\}$ stored in the SC, he can guess a password PW^* and compute $R^* = K_1 \oplus h(PW^*)$ and compare R^* with stored R, until he get the correct password [4].

4. Proposed Scheme

In this section, we describe a new remote user authentication scheme which resolves all the above security flaws and keeps the merits of Kim-Chung's scheme. Fig. 1 shows the new proposed authentication scheme.

Our improved scheme consists of four phases: the registration phase, the login phase, the authentication phase and the password change phase. We describe these phases as follows.

4.1 Registration Phase

The registration phase is operated when the user U initially registers to S and is described as follows.

R.1. $U \Rightarrow S : \{ID, h(PW)\}$

U chooses his identity ID and password PW, then computes $h(PW)$ and sends $\{ID, h(PW)\}$ to the server S via a secure communication channel.

R.2. After receiving the registration message from U, S generates a random number N unique to U. Then S computes three values K_1, K_2 and R with ID, $h(PW)$, N, and S's secret key x. Note that N is a fixed length value.

$K_1 = h(x) \oplus (ID \| N)$

$K_2 = h((ID \| N) \oplus x) \oplus h(PW)$

$R = K_1 \oplus h(ID \oplus h(PW))$

S stores $\{K_1, K_2, R, h(.)\}$ into U ' smart card SC.

R.3. $S \Rightarrow U : \{SC\}$ S sends SC to U through a secure channel and the registration phase is completed.

Note that $|x| = l$, l is a security parameter.

4.2 Login Phase

If U wants to login S, firstly, U inters his SC into a card reader or a terminal, then U enters his own ID and PW. Receiving U's ID and PW, SC computes as follows:

L.1. SC uses received ID, PW and stored R to compute C_1 and compares C_1 with K_1.

$C_1 = R \oplus h(ID \oplus h(PW))$

If C_1 is equal to K_1, SC acquires current timestamp T_1 and computes $C_1^{'}$ and C_2. Otherwise, SC rejects login request.

$C_1^{'} = K_2 \oplus h(PW)$,

$C_2 = h(C_1^{'} \oplus (T_1 \| ID))$

L.2. $SC \rightarrow S$ $\{T_1, C_1, C_2\}$

SC sends login request $\{T_1, C_1, C_2\}$ to S through a common channel.

User (U)		Server(*S*)
Registration phase: Select *ID, PW*		
	ID, h(PW) ⇢	*K₁=h(x) ⊕(ID||N)* *K₂=h((ID||N) ⊕x) ⊕h(PW)* *R= K₁ ⊕h(ID ⊕h(PW))* Store *K₁, K₂, R, h(.)* in smart card
	⇠ {smart card}	
Login phase: Input *ID, PW* *C₁=R ⊕h(ID ⊕h(PW))* If *C₁*≠stored *K₁,* reject. Acquire current timestamp *T₁* *C₁'= K₂ ⊕h(PW)* *C₂=h(C₁' ⊕(T₁||ID))*	*{ T₁, C₁, C₂ }* →	
Verification phase:		Acquire current timestamp *T₂* Check freshness of *T₁* *(ID||N)'= C₁ ⊕h(x)* *C₂'=h(h((ID||N' ⊕x) ⊕(T₁ ||ID '))* If *C₂*≠ *C₂'*, reject. *C₃=h(h(C₁ ⊕h(x) ⊕x) ⊕ T₂ ⊕ID)*
	← *{ C₃, T₂}*	
Check freshness of *T₂* *C₃'=h(C₁' ⊕ T₂ ⊕ID)* Terminate if *C₃*≠ *C₃'*		
User (*U*)		Smart card

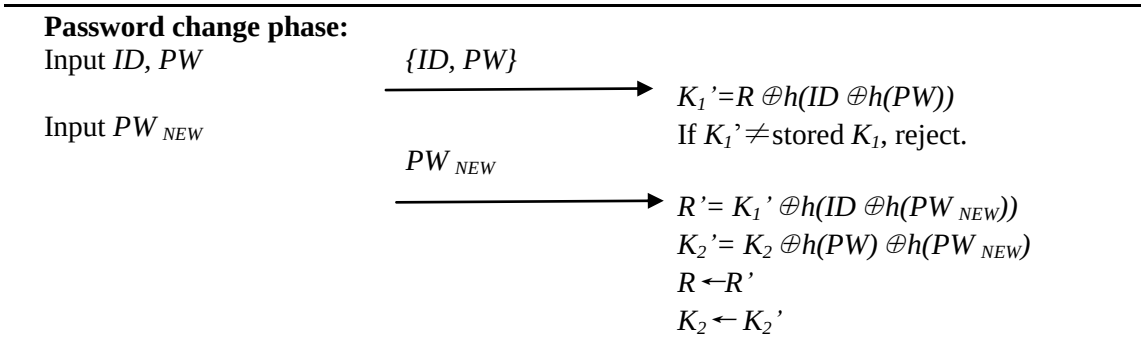

Figure 1. Proposed Scheme

4.3 Authentication Phase

After receiving the login request, S authenticates U as follows:

A.1. S checks freshness of T_1. If $T_1 = T_2$ or $T_2 - T_1 \geq \Delta T$, S rejects U's login request. Where T_2 is current timestamp and ΔT is the expected legal time interval for transmission delay.

A.2. $S \rightarrow SC\{C_3, T_2\}$

S obtains ID' and N' by computing $C_1 \oplus h(x)$ with received C_1 and S's secret key x: $(ID \| N)' = C_1 \oplus h(x)$

Then S computes out C_2'. If C_2' is equal to received C_2, S accepts U's login request, and sends $\{C_3, T_2\}$ to SC via a common channel, otherwise, S terminates this session.

$$C_2' = h(h((ID \| N)' \oplus x) \oplus (T_1 \| ID'))$$

$$C_3 = h(h(C_1 \oplus h(x) \oplus x) \oplus T_2 \oplus ID)$$

A.3. When receiving the response message from S, SC checks the freshness of T_2 as the same way with step A.1. Then SC calculates C_3': $C_3' = h(C_1' \oplus T_2 \oplus ID)$.

U confirms that S is valid if C_3' is equal to received C_3, otherwise U terminates this session.

Herein, U and S correctly authenticate each other.

4.4 Password change phase

If U want to change his password, he inserts his own SC into a card reader then enters his ID and PW into SC. Upon receiving ID and PW, SC performs the following steps:

P.1. SC computes K_1' : $K_1' = R \oplus h(ID \oplus h(PW))$

If $K_1' \neq K_1$, SC rejects password changing request. Otherwise, SC allows U to enter a new password PW_{new}.

P.2. SC computes $R^{'}$ and $K_2^{'}$ to replace the old R and K_2.

$R^{'} = K_1^{'} \oplus h(ID \oplus h(PW_{new}))$

$K_2^{'} = K_2 \oplus h(PW) \oplus h(PW_{new})$

Therefore U succeed changing his password with no registration with remote server S.

5. Security Analysis

In this section, we give a security analysis of our improved scheme to show how it is more secure than Kim-Chung's scheme.

5.1 Masquerading User Attack

If an attacker *UA* wants to impersonate as a legal user U, *UA* needs to forge a login request message $\{T_1, C_1, C_2\}$. Where $C_1 = h(x) \oplus (ID \| N)$, $C_2 = h(h((ID \| N) \oplus x) \oplus (T_1 \| ID))$. *UA* cannot forge C_1 and C_2 without knowing the server's secret key x, U's ID and the random number N unique to U. Suppose that *UA* obtains U's smart card SC, which including $\{K_1, K_2, R, h(.)\}$, *UA* can get C_1 from K_1, but still cannot get $C_2 = h(K_2 \oplus h(PW) \oplus (T_1 \| ID))$, because *UA* cannot obtain U's ID and PW through the stolen smart card or intercepting the communication. Herein, our scheme is secure against masquerading user attack.

5.2 Masquerading Server Attack

If an attacker *UA* wants to impersonate as the server S, *UA* needs to forge a response message $\{C_3, T_2\}$, where $C_3 = h(h((ID \| N) \oplus x) \oplus T_2 \oplus ID)$. However *UA* cannot compute C_3 without the knowledge of ID, N and x. Suppose that *UA* obtains the stolen SC, so he can get K_2, but he still cannot get $C_3 (= h(C_1^{'} \oplus T_2 \oplus ID) = h(K_2 \oplus h(PW) \oplus T_2 \oplus ID))$, because it is impossible to get U's PW and ID at the same time. Likewise, if *UA* obtains C_1 by intercepting the login request message, it is still impossible to compute $C_3 (= h(h(C_1 \oplus h(x) \oplus x) \oplus T_2 \oplus ID))$ without the knowledge of x and ID. Therefore, our scheme can defeat masquerading server attack.

5.3 Off-line Password Guessing Attack

Suppose that *UA* can obtain the secret information $\{K_1, K_2, R, h(.)\}$ from the stolen SC. Also, *UA* can intercept the communication message $\{T_1, C_1, C_2\}$ and $\{C_3, T_2\}$. There are some appearances of U' password PW as follows:

$K_2 = h((ID \| N) \oplus x) \oplus h(PW)$

$R = K_1 \oplus h(ID \oplus h(PW))$

$C_2 = h(K_2 \oplus h(PW) \oplus (T_1 \| ID))$

$C_3 = h(K_2 \oplus h(PW) \oplus T_2 \oplus ID)$

However, *UA* cannot guess the correctly PW, since it is impossible to get ID, N and x. Furthermore, it is computationally infeasible to invert the one-way hash function $h(.)$. In conclusion, our scheme can resist the off-line password guessing attack.

5.4 Server's Secret Key Guessing Attack

UA can obtain K_1 and K_2 from the stolen *SC* and try to guess the *S*' secret key *x* by computing:

$(ID \| N) = h(x) \oplus K_1$

$K_2 = h((ID \| N) \oplus x) \oplus h(PW)$

Likewise *UA* may try to guess *S* 's secret key by using $C_3 (= h(h(C_1 \oplus h(x) \oplus x) \oplus T_2 \oplus ID))$.

Here, we impress that *x* 's length is security parameter. Therefore, it is impossible to guess *S* 's secret key correctly.

5.5 Replay Attack

Our scheme is secure against replay attack, since both the request login message $\{T_1, C_1, C_2\}$ and the response verification message $\{C_3, T_2\}$ are verified by checking the freshness of the timestamps. Even if *UA* chooses a timestamp T^* which can pass the verification, he cannot compute the correct $C_2^{'}$ $(= h(h((ID \| N)^{'} \oplus x) \oplus (T^* \| ID^{'})))$, since we check the computed $C_2^{'}$ with received C_2.

5.6 Password Guessing Attack through Password Change Phase

When *UA* wants to guess *U* ' *PW* through the password change phase, he must get *U* 's ID, which is hard to obtain both by stealing the *SC* and intercepting the communication messages.

5.7 Secure Password Change

In our proposed scheme, U can change his PW at will without registering with the server S. Also, our scheme is secure when changing password, since if U wants to change his password, he must enter the correct *ID* and *PW*, so that *SC* can check if $K_1^{'}$ is equal to stored K_1. Thus, although *UA* obtains the stolen *SC*, he cannot change the password as he wishes.

5.8 Smart Card Lost Attack

In our scheme, an attacker cannot obtain ID and PW of the user U. Suppose that *UA* gets the *SC*, he cannot login without any knowledge of *ID* and *PW*. Although, *UA* guesses ID^* and PW^*, it is impossible to login successfully, because *SC* verifies by computing $K_1^{'} = R \oplus h(ID^* \oplus h(PW^*))$ and checks with stored K_1.

6. Comparison with Other Related Schemes

In this section, we compare our proposed scheme with some related schemes in the field of some security features [16, 17, 18]. Table 2 shows the comparison.

Table 2. Comparison of Security Features

	Kim-Chung's [2]	C.-T. Li, *et al.*'s [4]	ours
Mutual authentication	No	Yes	Yes
Freely choose and change PW	Yes	No	Yes
Prevention of masquerading user attack	No	Yes	Yes
Prevention of masquerading server attack	No	Yes	Yes
Prevention of off-line PW guessing attack	No	No	Yes
Prevention of server's secret key guessing attack	Yes	Yes	Yes
Prevention of replay attack	Yes	Yes	Yes
Prevention of off-line PW guessing in PW change	No	No	Yes
Prevention of smart card lost attack	No	No	Yes

7. Conclusion

In this paper, we have proposed an enhanced scheme of Kim-Chung's. Our scheme keeps the merits of Kim-Chung's scheme and resolves some security flaws such as masquerading attack, off-line password guessing attack, server's secret key guessing attack, replay attack, off-line password guessing in password change phase and smart card lost attack. It is impossible to obtain any important information even if an attacker is malicious legal user. Moreover, we have compared our scheme with some related schemes to assess that our scheme is more secure than others.

Acknowledgements

"This research was supported by the KCC(Korea Communications Commission), Korea, under the R&D program supervised by the KCA(Korea Communications Agency)" (KCA-2012-12-912-06-003).

References

[1] M. Kumar, "A New Secure Remote User Authentication Scheme with Smart Cards", International Journal of Network Security, vol. 11, no. 3, **(2010)** November, pp. 112–118.
[2] S. K. Kim and M. G. Chung, "More secure remote user authentication scheme", Computer Communications, vol. 32, no. 6, **(2009)**, pp. 1018–1021.
[3] E. Yoon and K. Yoo, "More efficient and secure remote user authentication scheme using smart cards", Proceedings of 11th International Conference on Parallel and Distributed System, vol. 2, **(2005)**, pp. 73–77.

[4] C. -T. Li, C. -C. Lee, C. -J. Liu and C. -W. Lee, "A Robust Remote User Authentication Scheme against Smart Card Security Breach", Data and Applications Security and Privacy XXV, LNCS 6818, 2011.c_IFIP International Federation for Information Processing **(2011)**, pp. 231–238.
[5] W. -B. Horng, C. -P. Lee and J. -W. Peng, "Cryptanalysis of a More Secure Remote User Authentication Scheme", 2010 International Computer Symposium (ICS), **(2010)** December 16-18, pp. 284–287.
[6] Kumar, "A New Secure Remote User Authentication Scheme with Smart Cards", Journal of Applied Computer Science & Mathematics, vol. 11, no. 5, **(2011)**, Suceava, pp. 38-46.
[7] H. Y. Chien, J. K. Jan and Y. M. Tseng, "An efficient and practical solution to remote authentication: smart card", Comp. Security, vol. 21, **(2002)**, pp. 372-375.
[8] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards", IEEE Trans. on Cons. Elect., vol. 46, **(2000)**, pp. 28-30.
[9] H. C. Hsiang and W. K. Shih, "Weaknesses and improvements of the Yoon-Ryu-Yoo remote user authentication scheme using smart cards", Computer Communications, vol. 32, **(2009)**, pp. 649-652.
[10] S. Lee, H. Kim and K. Yoo, "Improvement of Chien, *et al.*'s remote user authentication scheme using smart card", Computer Standards & Interfaces, vol. 27, **(2004)**, pp. 181-183.
[11] A. Irshad, W. Noshairwan, M. Shafiq, S. Khurram, E. Irshad and M. Usman, "Security Enhancement in MANET Authentication by checking the CRL status of Servers", Communications in Computer and Information Science, vol. 78, **(2010)**, pp. 86-95, DOI: 10.1007/978-3-642-16444-6_13.
[12] X. Zhao and X. -D. Wang, "Design and Implementation of Hybrid Broadcast Authentication Protocols in Wireless Sensor Networks", Second International Conference on Future Generation Communication and Networking 2008, FGCN '08, **(2008)** December 13-15.
[13] I. V. Koskosas and N. Asimopoulos, "Information System Security Goals", International Journal of Advanced Science and Technology, vol. 27, **(2011)** February.
[14] A. Tudzarov and T. Janevski, "Functional Architecture for 5G Mobile Networks", International Journal of Advanced Science and Technology, vol. 32, **(2011)** July.
[15] F. Imran and M. Hussain, "Advance Security Aspects of Universal Mobile Telecommunication System (UMTS)", International Journal of Advanced Science and Technology, vol. 33, **(2011)** August.
[16] N. Park, S. Kim and D. Won, "Secure group communication over combined wired and wireless networks", Lecture Note in Computer Science, vol. 3592, Springer-Verleg, **(2005)**, pp. 90-99.
[17] K. Lee, D. Won and S. Kim, "A Secure and Efficient E-Will System Based on PKI", Information - An International Interdisciplinary Journal, International Information Institute, vol. 14, no. 7, **(2011)**, pp. 2187-2206.
[18] N. Park, S. Kim and D. Won, "Security analysis and implementation leveraging globally networked RFIDs", Lecture Note in Computer Science, vol. 4217, Springer-Verleg, **(2006)**, pp. 494-505.

Authors

Jin Qiuyan received her B.E. in Software Engineering from Dalian Nationalities University, China, in 2011. She is currently undertaking a M.S. course in Electrical and Computer Engineering at Sungkyunkwan University, Korea. Her current research interests are in the areas of cryptography, information security and user authentication.

Kwangwoo Lee received his B.E. degree in Computer Engineering from Sungkyunkwan University, Korea, in 2005 and M.E. degree in Electrical and Computer Engineering from Sungkyunkwan University, Korea, in 2007 and Ph.D. degrees from Sungkyunkwan University in 2011. He is currently engineer of the Samsung electronics. His interests are cryptology, information security and assurance, digital forensic, printer security, and e-voting.

Dongho Won received his B.E., M.E., and Ph.D. degrees from Sungkyunkwan University in 1976, 1978, and 1988, respectively. After working at the Electronics & Telecommunications Research Institute (ETRI) from 1978 to 1980, he joined Sungkyunkwan University in 1982, where he is currently a Professor of the College of Information and Communication Engineering. His interests are cryptology and information security. He was the president of the Korea Institute of Information Security & Cryptology (KIISC) in 2002.