Cryptanalysis of Improved Biometric-Based User Authentication Scheme for C/S System

Younsung Choi, Donghoon Lee, Jiye Kim, Jaewook Jung, and Dongho Won

***Abstract*—Password-based authentication schemes are convenient, but vulnerable to simple dictionary attacks. Cryptographic secret keys are safe, but difficult to memorize. Recently, biometric information has been used for authentication schemes because it is difficult to copy, share, forge, and distribute. In 2011, Das proposed a biometric-based authentication scheme, but it has various vulnerabilities such as replay attack, denial-of-service attack, user impersonation attack, and password change problem. To solve these problem, Jiping *et al*. improved Das's scheme, but some vulnerabilities have remained still. In this paper, we analyze the cryptanalysis of Jiping *et al*. authentication scheme. So this paper shows that Jiping *et al*.'s scheme is vulnerable against server masquerading attack and stolen smart card attack. And also we show the possibility of authentication without login phase in Jiping *et al*.'s authentication scheme.**

***Index Terms*—User authentication, biometric-base scheme, client/server system, cryptanalysis on authentication scheme.**

I. Introduction

Remote identity-based authentication schemes have been based primarily on passwords alone. Password-based authentication schemes provide a simple and convenient method to authenticate users before providing them with the services of a computing or communication system [1]–[7]. However, the use of passwords alone is a scheme that is easy to break by using simple dictionary attacks. To overcome this problem, cryptographic secret keys and passwords have been used in remote-user authentication schemes [8]–[10]. Long and random cryptographic keys are difficult to memorize, however, so they must be stored somewhere, which is a weak point. To solve this problem, various biometric-based authentication schemes have been proposed. Das proposed a new biometric-based authentication scheme, but it has various vulnerabilities [11]. Subsequently, Jiping *et al*. proposed a security-improved biometric-based user authentication scheme for C/S system based on Das's authentication scheme [12], but Jiping *et al.*'s scheme has some remaining the security problems.

The rest of this paper is organized as follows. In Section II, we review related works. In Section III, we briefly review Jiping et al.'s biometric-based remote user authentication scheme using smart cards. In Section IV, we analyze the security vulnerability of Jiping *et al.*'s scheme and suggest a solution. Finally, we conclude the paper in Section V.

Manuscript received April 5, 2014; revised June 5, 2014.

The authors are with the School of Information and Communication Engineering, Sungkyunkwan University, Korea (e-mail: yschoi@security.re.kr, dhlee@security.re.kr, jykim@security.re.kr, jwjung@security.re.kr, dhwon@security.re.kr).

II. Related Works

A. Smart Card Attack

Various researchers have observed that the confidential information stored in all smart cards could be extracted by physically monitoring power consumption, such as by using SPA and DPA. When a user loses a smart card, an attacker can analyze it. Various schemes leave it vulnerable to off-line password attacks in which an attacker can be authenticated to the server without having the user's ID and password.

B. Biometric-Based Authentication

Biometrics refers to the quantifiable data related to human characteristics and traits. Examples include fingerprints, face recognition, DNA, palm prints, hand geometry, iris, retina, odor/scent, typing rhythm, gait, and voice. Biometrics-based authentication can be used in user identification and access control. Biometric information cannot be lost or forgotten and is very difficult to copy, share, forge or distribute. In addition, biometric information cannot be guessed easily and such coding is more difficult to break than other types.

C. Das's Biometric-Based User Authentication Scheme

Das proposed biometric-based remote user authentication, which is inherently more reliable and secure than traditional password-based remote authentication schemes. However, this scheme has security vulnerabilities to replay attack, denial-of-service attack, user impersonation attack, and password change problems. Moreover, this scheme does not provide mutual authentication between the user and the server.

III. Review of Jiping *et al.*'s Scheme

TABLE I: Notation

Notation	Description
C_i	Client
S_i	Server
R_i	Registration center
PW_i	Password shared between C_i and S_i
ID_i	Identity of the user C_i
B_i	Biometric template of the user C_i
$d(\ )$	Symmetric parametric function
τ	Predetermined threshold
$h(\ )$	A secure one-way hash function
X_s	A secret information maintained by the server
R_c	A random number chosen by C_i
R_s	A random number chosen by S_i
$A \| B$	Data A concatenates with data B
$A \oplus B$	XOR operation of A and B

Das proposed a biometric-based authentication scheme that has various security problems. To solve these problems, Jiping *et al*. proposed an improved biometric-based authentication scheme [12]. In the following review of Jiping *et al*.'s scheme, for convenience, we use the notations shown in Table I.

A. Registration Phase

In the registration phase, remote user C_i must perform the following registration steps, as shown in Fig. 1 for the registration phase of Jiping's scheme.

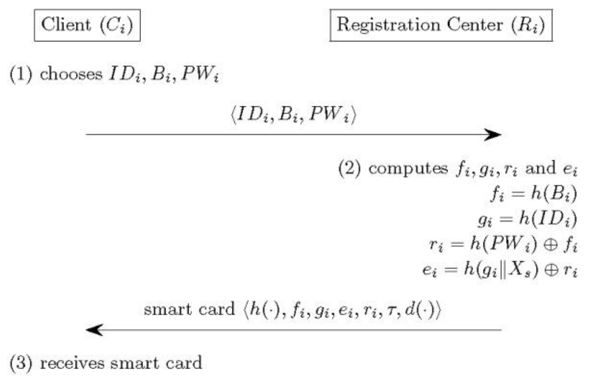


Fig. 1. Registration phase of Jiping *et al*.'s scheme.

1) The user C_i inputs personal biometric B_i on a device and sends the identity ID_i and password PW_i to the registration center R_i in person.
2) The registration center R_i computes $f_i = h(B_i)$, $g_i = h(\text{ID}_i)$, $r_i = h(\text{PW}_i) \oplus f_i$, and $e_i = h(g_i \parallel X_s) \oplus r_i$. X_s is secret information shared by R_i and S_i. X_s and the passwords of the corresponding users are not disclosed to any others for all future secure communications.
3) Registration center R_i loads ($h(\cdot)$, f_i, g_i, e_i, r_i, τ, $d(\cdot)$) on the user's smart card and sends this information to user C_i using a secure channel.

B. Login Phase

In the login phase, remote user C_i must perform the following login steps, as shown in Fig. 2.

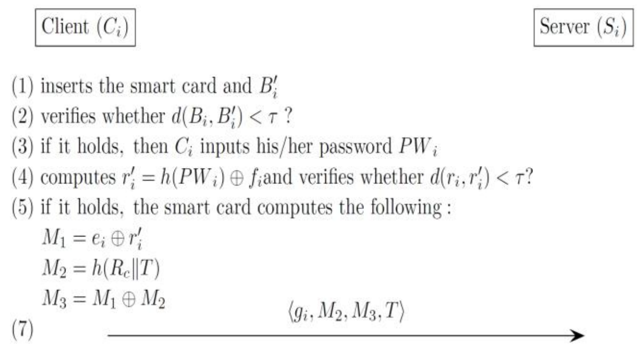


Fig. 2. Login phase of Jiping *et al*.'s scheme.

1) C_i first inserts the user's smart card into the card reader of a terminal and inputs the user's biometric template B'_i on the device. If $d(B_i, B'_i) > \tau$, the login phase is terminated. Otherwise, C_i passes the biometric verification and then inputs the user's password PW_i.
2) The smart card computes $r'_i = h(\text{PW}_i) \oplus f_i$. If $d(r'_i, r_i) > \tau$, then the password is not correct, so the system terminates the session; otherwise, the smart card computes $M_1 = e_i \oplus r'_i$, which is equal to $h(g_i \parallel X_s)$, $M_2 = h(R_c \parallel T)$, where R_c is a random number generated by the user Ci, T is the current timestamp of C_i's system, and $M_3 = M_1 \oplus M_2$.
3) Finally, user C_i sends the message $<g_i, M_2, M_3, T>$ to the remote server S_i.

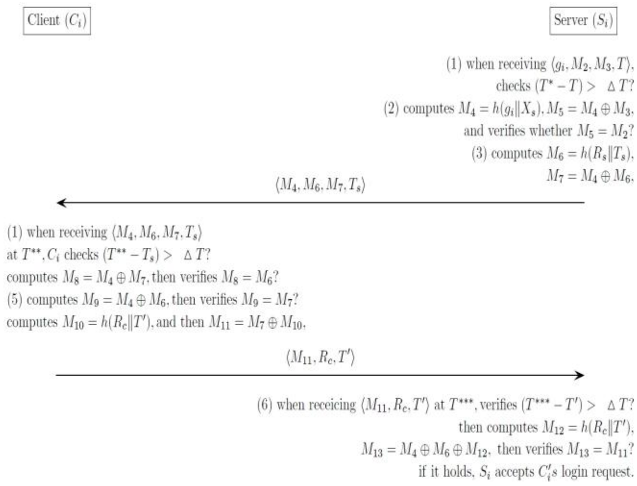


Fig. 3. Authentication phase of Jiping *et al*.'s scheme.

C. Authentication Phase

In the authentication phase, remote user C_i and server S_i must perform the following authentication phase. When the remote server S_i receives the login message $<g_i, M_2, M_3, T>$ at time T^*, it will perform the following steps, as shown in Fig. 3, to authenticate whether the user C_i is legitimate.

1) Check T. If $(T^* - T) > \Delta T$, the authentication phase is terminated, where ΔT is the expected time interval for the transmission delay of the system. Otherwise, if $(T^* - T) \leq \Delta T$, the authentication steps will be performed.
2) S_i checks the accuracy of C_i's ID_i. It computes $M_4 = h(g_i \parallel X_s)$ using the secret value X_s maintained by the server S_i and then computes $M_5 = M_4 \oplus M_3$ and verifies whether $M_5 = M_2$ or not. If it is not accurate, then S_i rejects C_i's login request. If the verification is successful, the next step will be performed.
3) S_i computes $M_6 = h(R_s \parallel T_s)$ and $M_7 = M_4 \oplus M_6$, where T_s is the timestamp of the server S_i, and then S_i sends message $\langle M_4, M_6, M_7, T_s \rangle$ to user C_i.
4) After receiving the message $\langle M_4, M_6, M_7, T_s \rangle$ at time T^{**}, C_i checks the freshness of T_s by verifying $(T^{**} - T_s) > \Delta T$. If it holds, the following session is terminated; otherwise C_i computes $M_8 = M_4 \oplus M_7$ and then verifies whether $M_8 = M_6$. If it does not hold, C_i terminates the session. Otherwise, it goes to the next step.
5) C_i computes $M_9 = M_4 \oplus M_6$ and then verifies whether $M_9 = M_7$. If it does not hold, S_i is rejected by C_i; otherwise, if it holds, C_i computes $M_{10} = h(R_c \parallel T')$, where T' is the current timestamp of user C_i, and then computes $M_{11} = M_7 \oplus M_{10}$ and sends the message $\langle M_{11}, R_c, T' \rangle$ to the remote server S_i.
6) Step 6: When S_i receives the message $\langle M_{11}, R_c, T' \rangle$ at time T^{***}, it checks $(T^{***} - T') > \Delta T$. If it holds, the authentication phase is terminated. Otherwise, if it does not hold, Si computes $M_{12} = \text{h}(R_c || T')$ and then computes $M_{13} = M_4 \oplus M_6 \oplus M_{12}$. After computing M_{13}, then S_i

verifies whether $M_{13} = M_{11}$. If it holds, S_i accepts C_i's login request; otherwise, S_i rejects the login request.

D. Password Change Phase

In Jiping *et al.*'s scheme, user C_i can freely change the password PW_{oldi} to a new one PW_{newi}. The password change procedure is performed as follows.

1) C_i inserts the smart card into the card reader and offers the user's personal biometrics B'_i. The smart card computes $f'i = h(B'_i)$ and verifies it by checking $d(f'_i, f_i) \leq \tau$. Where $f_i = h(B_i)$ is the information stored in the smart card.
2) If it holds, C_i inserts old password PW_{oldi} and new password P_{Wnewi}. Otherwise, the password change procedure is terminated.
3) The smart card performs $r'_i = h(PW_{oldi}) \oplus f'_i$ and checks $d(r'_i, r_i) \leq \tau$. r_i is the information stored in the smart card.
4) If it holds, the smart card computes $r'_i = h(PW_{newi}) \oplus f_i$, $e'_i = e_i \oplus r_i (= h(ID_i \| X_s))$, and $e''_i = e'_i \oplus r_i$.
5) Finally, replace e_i with e''_i and r_i with r''_i on smart card.

IV. Cryptanalysis of Jiping *et al.*'s Scheme

Jiping *et al*. enhanced the security of Das's authentication scheme and proposed a new authentication scheme. But Jiping *et al*.'s authentication scheme has some remaining the security problems of vulnerabilities to the server masquerading attack, stolen smart-card attack, and authentication without login phase.

A. Server Masquerading Attack

An attacker can masquerade as a legitimate server if the attacker knows $h(g_i \| X_s)$. For this reason, the server authenticates the user using only $h(g_i \| X_s)$. Fig. 4 shows the phases of a server-masquerading attack. First, the attacker intercepts the client's message <g_i, M_2, M_3, T>. Then, the attacker calculates $h(g_i \| X_s)$ using $M_2 \oplus M_3$. Because $h(g_i \| X_s) = e_i \oplus r_i = M_2 \oplus M_3$, the attacker computes M_4, M_6, M_7 and T_A using $h(g_i \| X_s)$ and sends them to the client. The client checks and authenticates messages. The attacker receives M_{11}, R_c, and T' and then checks whether the attacker is successful at masquerading as the server. The client is authenticated with the attacker. In Jiping *et al*.'s scheme, the attacker can execute the server-masquerading attack. To solve this problem, it is necessary to add another piece of security information to authenticate the client with the server, such that the attacker cannot compute the security information using messages communicated between the server and the client.

B. Stolen Smart Card Attack

Kocher *et al*. and Messerges et al. pointed out that the confidential information stored in all existing smart cards could be extracted by physically monitoring their power consumption. Therefore, if a user loses a smart card, all private information in the smart card could be revealed to an attacker [13]-[15]. In Jiping *et al*.'s scheme, a smart card stores various secrets for the login and authentication of the user.

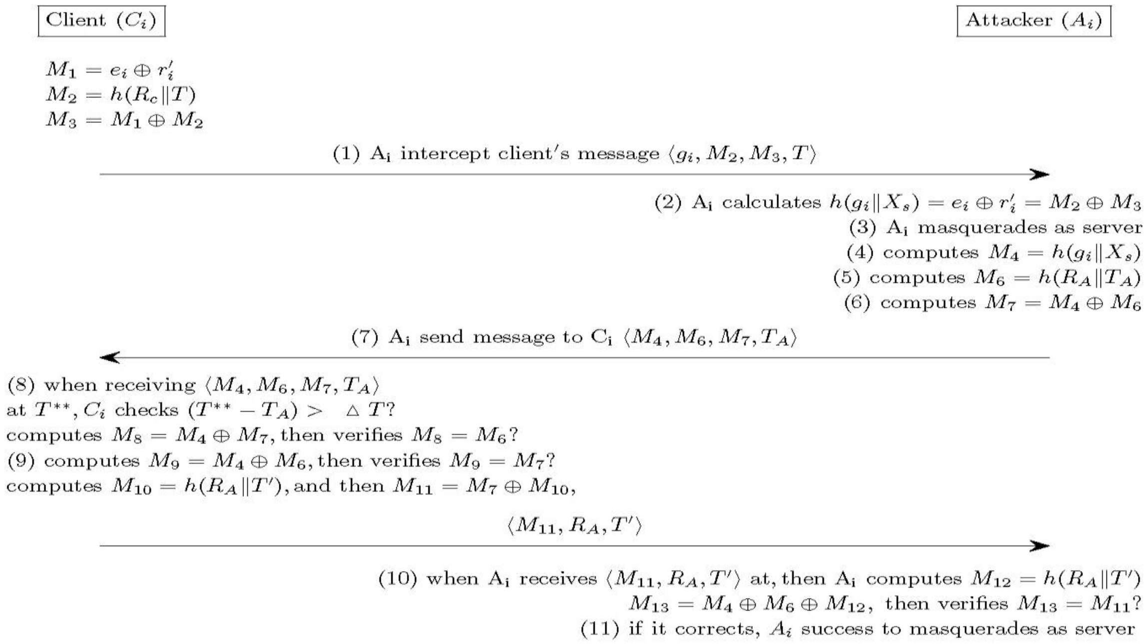


Fig. 4. Server masquerading attack.

The smart card for user ID_i includes ($h()$, f_i, g_i, e_i, r_i, τ, $d(\cdot)$). So, if an attacker obtains the user's smart card, the attacker can acquire the user's f_i, g_i, and r_i. The attacker can calculate $h(PW_i)$ and $h(ID_i)$, then execute an off-line password attack using the rainbow table, dictionary attack, and brute attack to obtain ID_i and PW_i. For this reason, the ID_i and PW_i are protected using $h()$. To solve this problem, it is necessary to add a random number with high-entropy. Fig. 5 shows the phases of a stolen smart card attack.

C. Authentication without Login Phase

In Jiping *et al.*'s scheme, attacker can be authenticate with server without login phase. To skip the login phase, the attacker need to still or get the user's smart card. In other words, if the attacker obtain user's smart card, the attacker can be authenticate to server without user's ID_i, PW_i and user's biometric information B_i. Fig. 6 shows the phase of authentication without login phase.

$$\boxed{Attacker}$$

gets(steals) user's smart card

obtains information from smart card using SPA and DPA

$\rightarrow$ gets $h(\cdot), f_i, g_i, e_i, r_i, \tau$ and $d(\cdot)$

Attacker knows f_i, g_i, r_i

$r_i = h(PW_i) \oplus f_i$

$\rightarrow h(ID_i) = g_i$

$\rightarrow h(PW_i) = r_i \oplus f_i$

executes off−line password attack

$\rightarrow$ figures out user's ID and password ID_i, PW_i

Fig. 5. Stolen smart-card attack.

Firstly, attacker gets or steals the user's smart card and obtains information from smart card using SPA and DPA. So the attacker can generate and compute the R_c, M_1, M_2 and M_3 using this information. And the attacker sends $\langle g_i, M_2, M_3, T \rangle$ to the server. Then, the attacker receives $\langle M_4, M_6, M_7, T_s \rangle$ and then, the attacker can computes $\langle M_{11}, R_c, T' \rangle$ and send these messages to server. So attacker can be authenticated to the server without user's ID_i, PW_i and the user's biometric information B_i. To solve this problem, it is necessary to add information of user's PW_i or B_i to authentication messages.

$$\boxed{Attacker}$$

gets(steals) user's smart card

obtains information from smart card using SPA and DPA

$\rightarrow$ gets $h(\cdot), f_i, g_i, e_i, r_i, \tau$ and $d(\cdot)$

computes M_1, M_2, M_3

$\rightarrow$ generates random number R_c

$\rightarrow M_1 = e_i \oplus r_i$

$\rightarrow M_2 = h(R_c \| T)$

$\rightarrow M_3 = M_1 \oplus M_2$

sends login and authentication message to S_i

$\rightarrow \langle g_i, M_2, M_3, T \rangle$

receives $S_i's$ message

$\rightarrow \langle M_4, M_6, M_7, T_s \rangle$

computes M_{11}, R_c, T'

$\rightarrow$ generates timestamp T'

$\rightarrow M_{10} = h(R_c \| T')$

$\rightarrow M_{11} = M_8 \oplus M_{10}$

sends authentication message to S_i

$\rightarrow \langle M_{11}, R_c, T' \rangle$

$\rightarrow$ attacker can be authenticated with S_i

Fig. 6. Authentication without login phase.

V. Conclusion

In this paper, we analyze the cryptanalysis of Jiping et al.'s biometric-based user authentication scheme for the client/server system. Jiping *et al*. proposed an improved authentication scheme to solve the problem of vulnerabilities in Das's scheme. However, Jiping *et al*.'s scheme has some remaining security problems: the server-masquerading attack, stolen smart-card attack and authentication without login phase. To solve this problem, it is necessary to add secret information to the registration, login and authentication phases.

Acknowledgments

This research was supported by the MSIP(Ministry of Science, ICT and Future Planning), Korea, under the ITRC(Information Technology Research Center) support program (NIPA-2014-H0301-14-1004) supervised by the NIPA(National IT Industry Promotion Agency)

References

[1] C. T. Li, "An enhanced remote user authentication scheme providing mutual authentication and key agreement with Smart Cards," in *Proc. the 5th International IEEE Computer Society Conference on Information Assurance and Security*, Xi'an, China, 2009, pp. 517–520.

[2] K. H. M. Wong, Z. Yuan, C. Jiannong, and W. Shengwei, "A dynamic user authentication scheme for wireless sensor networks," in *Proc. the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC '06)*, Taichung, Taiwan, June 2006, pp. 244–251.

[3] T. H. Lee, "Simple dynamic user authentication protocols for wireless sensor networks," in *Proc. the 2nd International Conference on Sensor Technologies and Application*, CapEsterel, France, August 2008, pp. 657–660.

[4] B. Vaidya, J. J. Rodrigues, and J. H. Park, "User authentication schemes with pseudonymity for ubiquitous sensor network in NGN," *International Journal of Communication Systems*, vol. 23, no. 9-10, pp. 1201–1222, 2010.

[5] N.Y. Lee and Y. C. Chiu, "Improved remote authentication scheme with smart card," *Computer Standards and Interfaces*, vol. 27, no. 2, pp. 177–180, 2005.

[6] M. Kim and C. K. Koc, "Asimple attackon a recently introduced hash-based strong-password authentication scheme," *International Journal of Network Security*, vol. 1, no. 2, pp. 77–80, 2005..

[7] L. C. Ko, "A novel dynamic user authentication scheme for wireless sensor networks," in *Proc. the IEEE International Symposium on Wireless Communication Systems*, Reykjavik, Iceland, October 2008, pp. 608–612.

[8] J. Nam, K. K. R. Choo, M. Kim, J. Paik and D. Won, "Dictionary Attacks against Password-Based Authenticated Three- Party Key exchange protocols," *KSII Transactions on Internet and Information Systems*, vol. 7, no. 12, December 2013, pp. 3244-3260.

[9] J. Nam, K. K. R. Choo, J. Kim, Kang, H. K. Kim, J. Paik, and D. Won, "Password-only authenticated three-party key exchange with provable security in the standard model," *The Scientific World Journal*, 2014.

[10] H. Jeong, D. Won, and S. Kim, "Weaknesses and improvement of secure hash-based strong-password authentication protocol," *Journal of Information Science and Engineering*, vol. 26, no. 5, September 2010, pp. 1845-1858.

[11] A. K. Das, "Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards," *Information Security*, IET 5.3, 2011, pp. 145-151.

[12] L. Jiping, D. Yaoming, X. Zenggang, and L, Shouyin, "An improved biometric-based user authentication scheme for C/S system," *International Journal of Distributed Sensor Networks*, 2014.

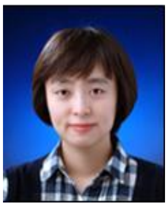
[13] P. Kocher, J. Jaffe, B. Jun, "Differential power analysis," in *Proc. the 19th Annual International Cryptology Conference on Advances in Cryptology*, 1999, pp. 388-397.

[14] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Transactions on Computers*, 2002, vol. 51, no. 5, pp. 541-552.

[15] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Transactions on Computers*, vol. 51, no. 5, pp. 541-552.

Younsung Choi received the B.S. degree in electrical and computer engineering from Sungkyunkwan University, Korea, in 2006 and the M.S. degree in electrical and computer engineering from Sungkyunkwan University, Korea, in 2007. He is currently undertaking a Ph.D. course on electrical and computer engineering in Sungkyunkwan University. His current research interest is in the area of digital forensic, cyber-crime, cryptography, authentication protocol, and mobile security.

Donghoon Lee received the B.S. degree Computer Science from National Institute for Lifelong Education (NILE), Korea, in 2009 and the M.S. degree in electrical and computer engineering from Sungkyunkwan University, Korea, in 2011. He is currently undertaking a Ph.D. course on electrical and computer engineering in Sungkyunkwan University. His current research interest is in the area of digital forensic, cryptography, forensic, authentication protocol, and mobile security.



Jiye Kim received the B.S. degree in information engineering from Sungkyunkwan University, Korea, in 1999 and the M.S. degree in computer science Education from Ewha Womans University, Korea, in 2007. He is currently undertaking a Ph.D. course on electrical and computer engineering in Sungkyunkwan University. His current research interest is in the area of cryptography, forensic, authentication protocol, and information security.

Jaewook Jung received the B.S. degree in electrical and computer engineering from Korea Aerospace University, Korea, in 2010 and the M.S. degree in electrical and computer engineering from Sungkyunkwan University, Korea, in 2012. He is currently undertaking a Ph.D. course on electrical and computer engineering in Sungkyunkwan University. His current research interest is in the area of cryptography, forensic, authentication protocol, and mobile security.

Dongho Won received his B.E., M.E., and Ph.D. from Sungkyunkwan University in 1976, 1978, and 1988, respectively. After working at ETRI (Electronics & Telecommunications Research Institute) from 1978 to 1980, he joined Sungkyunkwan University in 1982, where he is currently a professor of the School of Information and Communication Engineering. In the year 2002, he served as the president of KIISC (Korea Institute of Information Security & Cryptology). He was the program committee chairman of the 8th International Conference on Information Security and Cryptology (ICISC 2005). His research interests are on cryptology and information security.