Insider Attack-Resistant OTP (One-Time Password) Based on Bilinear Maps

Yunjin Lee and Howon Kim

***Abstract*—For various services, OTP (One-Time Password) is increasingly employed to sign in services. The most popular OTP scheme is S/KEY. However, S/KEY scheme is vulnerable to hash collision. In order to solve this problem, Choi and Kim proposed an OTP scheme based on pairing operation. This scheme overcame hash collision problem. Unfortunately, the scheme is vulnerable against insider attack. In this paper, we propose insider attack-resistant OTP scheme based on pairing operation. Our scheme employed zero-knowledge proof to generate OTP values. In short, our scheme sends an OTP and two random numbers encoded with XOR; any adversary has no sense about the random numbers. Our scheme authenticates entities with an OTP and gain a hint on next OTP value from one of random numbers. Consequently, we present insider attack-resistant OTP scheme by eliminating shared parameter among insider (e.g. time stamp).**

***Index Terms*—OTP, zero-knowledge proof, authentication, password, pairing-based cryptography.**

I. Introduction

Recently, as increasing the concern about internet service, many researchers have focused on its security. Especially, services, which use password-based security, have been challenged to be broken by many attackers.

For example, most of internet users set identical passwords for more than two different web sites in static password mechanism. Therefore, there is high probability that a user's password is also valid for another web site. Due to this issue, if a password on a web service is revealed from specific attack (such as malware, eavesdropping, physical attack etc.), the adversary can disguise as the user on another web service.

For the reason, highly secured services (such as online banking, online shopping etc.) which are directly related to customers are required to be safe from this vulnerability. One of the solutions [1]-[6] is OTP (One-Time Password) [7]. Since OTP is valid for only one session, whenever session is changed, users shall sign in web services with different password; namely, the current password can be used only one time to log into the web service. In contrast, a fixed password can be used to sign in a web service consistently. Consequently, many important services recommend users to sign in with an OTP. Unfortunately, OTP schemes [8]-[17] failed to become popular. One of the reasons may be that the OTP requires independent token which generates an OTP.

The most popular OTP scheme is S/KEY [8] which is based on hash chain. The S/KEY scheme consists of registration phase and authentication phase. In registration phase, server generates hash chain of x selected by user. The length of hash chain is denoted as n, and the hash chain is valid for n-times; in other words, OTP based on S/KEY must update the hash chain after n-authentication. In authentication phase, the last hash value of n hash chain becomes the first OTP value.

However, S/KEY has vulnerability on hash function. In registration phase, hash collision may come up when hash chain is generated. In detail, collision in middle of hash chain makes two hash chains have same hash values after collision. From this collision, an adversary can easily predict the next OTP value.

For instance, assume that there are two users, Alice and Bob, using OTP based on S/KEY and an adversary, Eve. Eve gathers and stores all the used OTPs of Alice and Bob. From the collected OTP values, Eve tries to complete two hash chains of Alice and Bob. In this phase, we assume that Eve discovered that the end of hash value of Alice's hash chain and the front of hash value of Bob's hash chain is same; the first OTP value of Alice and the current OTP value of Bob is same. It has high probability that Alice's hash chain and Bob's hash chain have collision. From the examples above, we can easily recognize that the Alice's second OTP value becomes the next OTP value of Bob with high probability.

In order to overcome this problem, Choi and Kim [9] proposed pairing-based OTP scheme. This scheme has two advantages. One of advantages is that the scheme does not require an independent token to generate OTP; instead of the token, the scheme uses mobile device. The other advantage is that a collision have no influence on OTP in the scheme since it utilizes exponential of mobile personal identification number (MPIN) over finite field; although two numbers are same in current, two numbers can be different in future since each number after exponential operation can be different. However, since the scheme used only MPIN to generate next OTP value, it is vulnerable against insider attack.

A. Our Contribution

In this paper, we propose a new OTP scheme based on pairing operation. The scheme proposed by Choi and Kim [9] is vulnerable on masquerading by insider. In order to overcome the issue, we use a random number instead of MPIN; namely, OTP values are computed from exponential operation of a random number. Thereafter, users give the server a hint for next OTP whenever they log into web services. In order to announce the hint, we use zero-knowledge proof technology [18], [19]. The main point of our construction is to prevent insider attack with providing the advantages of pairing operations [20], [21]. Consequently, our scheme has two advantages. The first advantage is that

Manuscript received November 10, 2012; revised January 23, 2013.

The authors are with the Department of Computer Engineering, Pusan National University, Gumjeong-Gu, Busan, Korea (e-mail: astroium@ pusan.ac.kr, howonkim@ pusan.ac.kr).

the scheme is secure against insider attack. Our scheme employs a random exponential and zero-knowledge proof instead of exponential operation of MPIN. This employment makes the scheme secure against insider attack by eliminating shared parameter in authentication packet.

B. Organization

The remainder of this paper is organized as follows. In Section II, preliminary is presented. We review the related works on OTP on bilinear maps and define its problems in Section III. A new insider attack-resistant OTP scheme called Insider Attack-Resistant OTP (One-Time Password) Based on Bilinear Maps is proposed in Section IV and analyzed in Section V, Section VI and VII contains conclusions and acknowledgements respectively.

II. Preliminary

A. Bilinear Maps

The pairing-based cryptography is on the basis of the bilinear map. Consider two groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of prime order q. $\mathbb{G}_1$ is an additive group and $\mathbb{G}_2$ is a multiplicative group.

We denote two generators of $\mathbb{G}_1$ as P and Q, then for each element of $\mathbb{G}_1$, we can write as follow:

$$aP = \overbrace{P + P + \cdots + P}^{a \text{ times}} \tag{1}$$

The bilinear map $\hat{e}$ is defined as follows:

$$\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2 \tag{2}$$

Bilinear maps satisfy three properties:

1) Bilinearity

$$\begin{aligned} &\forall P, Q \in \mathbb{G}_1, \forall a, b \in \mathbb{Z}_q^*, \\ &\hat{e}(aP, bQ) = \hat{e}(P, Q)^{a,b} \end{aligned} \tag{3}$$

2) Non-degeneracy

$$\forall P \in \mathbb{G}_1, P \neq 0 \Rightarrow \langle \hat{e}(P, P) \rangle = \mathbb{G}_2 \tag{4}$$

It other expression,

$$P \neq 0 \Rightarrow \hat{e}(P, P) \neq 1 \tag{5}$$

If P is not an identity then $\hat{e}(P, P)$ also generates to $\mathbb{G}_2$ which is not the identity.

3) Computability

$\hat{e}$ is efficiently computable.

B. The Bilinear Diffie-Hellman Problem

The Bilinear Diffie-Hallman Problem (BDHP) defines the Computational Diffie-Hellman Problem (CDHP) on the bilinear map.

The CDHP is a problem of finding $h \in \mathbb{G}$ satisfies $h = g^{ab}$ when elements g, g^a, g^b of group $\mathbb{G}$ are provided.

The BDHP is a problem of finding $\hat{e}(P, P)^{abc}$ from given parameters $\langle P, aP, bP, cP \rangle$.

C. The Decisional Bilinear Diffie-Hellman Problem

Like BDHP, the Decisional Bilinear Diffie-Hellman Problem (DBDHP) defines the Decisional Diffie-Hallman Problem (DDHP) on the bilinear map.

The DDHP is a problem of finding whether $x \in \mathbb{G}$ satisfies $x = g^{ab}$ when four elements g, g^a, g^b, x of group $\mathbb{G}$ are given.

And the DBDHP is a problem of finding $x \in \mathbb{G}$ satisfies $x = \hat{e}(P, P)^{abc}$ from given parameters $\langle P, aP, bP, cP, x \rangle$. When $\hat{e} : \mathbb{G}_1 \to \mathbb{G}_2$, given parameters P, aP, bP, cP are elements of $\mathbb{G}_1$ and x is an element of $\mathbb{G}_2$.

D. One-Time Password (OTP)

One-Time Password (OTP) is a password valid only for one login session which overcomes shortcomings of static password. By using a fresh password for every new login session, the OTP scheme is more secure than traditional passwords since it is safe from eavesdropping and replay attack.

There are two major methods for generating the OTP. One is a time-synchronized OTP and the other is on the basis of mathematical algorithm, especially hash chain.

1) The time-synchronized OTP

In time-synchronized OTP, current time is used for new password generation. One example of time-synchronized OTP is The Time-based One-time Password (TOPT)[10], extension of HMAC-based OTP(HOTP)[11], and is an IETF standard.

2) The mathematical algorithm based OTP

In this kind of OTP, previous OTP is used for new OTP generation. S/KEY [8] is in this category of OTP.

S/KEY, based on the Lamport [6]'s scheme, is proposed by N. Haller in 1995. In S/KEY system, user generates OTP through secure hash function [2] calculation and sends the OTP to server. Thereafter, the server verifies received OTP. For each use of OTP, the number of computation is reduced by one, therefore server can verify OTP by applying one more secure hash function computation on received OTP. We can divide the procedure into registration and authentication.

3) Registration phase

Step 1 $U \Rightarrow S : x$

User (U) generates nonce x and sends it to server(S).

Step 2 $S \Rightarrow U : H^n(x), n$

Server computes, stores and sends $H^n(x)$ and n to user.

n is an initial value for certain limited number of hash computation. Registration phase uses secure channel.

4) Authentication phase

Step 1 $U \to S : OTP'$

User sends $OTP' = H^{n'-1}(x)$ to server.

Step 2 S : *verify* OTP'

Server computes $H(OTP') = H(H^{n'-1}(x)) = H^{n'}(x)$ and compares with stored $OTP = H^{n'}(x)$ to verify received OTP'.

Step 3 $S \rightarrow U$: *Accept or reject*

If $H(OTP') = OTP$ then server sends acceptance message to user and stores received OTP' as OTP .

After authentication phase, user reduces n' by one. For this reason, user must make a new registration after n uses of OTP .

III. Related Work

S/KEY uses hash chain to produce OTP and because of hash chain, it inherits collision problem. After one collision, following OTP values would be predictable. To solve this problem, Choi and Kim [9] proposed OTP based on pairing computation in 2012. The scheme has two phases like traditional S/KEY scheme and is as follows:

A. Registration Phase

User must register his/her mobile device to use mobile OTP. Registration phase uses secure channel.

Step 1 $S \Rightarrow U : \mathbb{G}_1, \mathbb{G}_2, P, q$

Server (S) sends parameters of bilinear map (two groups $\mathbb{G}_1$, $\mathbb{G}_2$, generator P and prime q) to user(U).

Step 2 $U \Rightarrow S : \hat{e}(M, R_U)^{MPIN}$

User computes $\hat{e}(M, R_U)$ derived from selected message (M and nonce R_U under pairing operation. Then computes $\hat{e}(M, R_U)^{MPIN}$ using mobile personal identification number ($MPIN$) and sends to server.

Step 3 $S \Rightarrow U : \hat{e}(M, R_U)^{MPIN \cdot X \cdot R_S}$

Server computes $\hat{e}(M, R_U)^{MPIN \cdot X \cdot R_S}$ from received value using secret key of server (X) and nonce R_S .

Step 4 $U \Rightarrow S : OTP, MPIN$

User computes $OTP = \left\langle \hat{e}(M, R_U)^{MPIN \cdot X \cdot R_S \cdot MPIN} \right\rangle$ and send OTP to server with MPIN.

Step 5 $S \rightarrow U$: *Accept or reject*, T

Server verifies OTP . If verification successes then stores MPIN and sends acceptance message and timestamp T to user.

B. Authentication Phase

Step 1 $U \rightarrow S : OTP', OTP \oplus T_U$

User computes $OTP' = \hat{e}(OTP, T_U)^{MPIN}$ and $OTP \oplus T_U$ using user-timestamp T_U and MPIN. Then user sends result of the computation to server.

Step 2 S : *Accept or reject*

Server gets user-timestamp T_U from $OTP \oplus T_U$ using stored OTP . Server compares T_U with server-timestamp T_S and if time interval is smaller than maximum time interval ΔT then compute OTP' with T_U and MPIN. Server compares computed OTP' with received OTP' and if it matches, server authenticates user.

This scheme has strong point to hash collision, but vulnerable to insider attack. Assume that the attacker is a different user on the same server and can eavesdrop $OTP \oplus T_U$ at authentication phase.

This scheme uses mobile pin (MPIN) for the computation of new OTP. Assume the attacker knows target user's MPIN and can eavesdrop target user's OTP' . Secondhand mobile phone users or mobile phone providers could be an potential attacker who might get a MPIN of victim. Eavesdropped OTP' will be used as OTP for next $OTP' = \hat{e}(OTP, T_U)^{MPIN}$ computation and MPIN is fixed value. This means that anyone who gets MPIN can make and predict new OTPs. For this reason, we suggest secure mobile OTP scheme which is strong against insider attack and hash collision problem.

IV. Insider Attack-Resistant OTP(One-Time Password) Based on Bilinear Maps

In this section, we suggest insider attack-resistant mobile OTP (One-Time Password) based on bilinear maps. This scheme employs zero knowledge proof. Registration and authentication procedure is as follows:

A. Registration Phase

We assume that registration is performed over secure channel.

Step 1 $S \Rightarrow U : \mathbb{G}_1, \mathbb{G}_2, P, q$

Server (S) sends parameters of bilinear map (two groups $\mathbb{G}_1$, $\mathbb{G}_2$, generator P and prime q) to user(U).

Step 2 $U \Rightarrow S : \hat{e}(X_U, R_U)^{MPIN}, R$

User computes $\hat{e}(X_U, R_U)^{MPIN}$ from user's secret key X_U , nonce R_U and mobile pin MPIN. Next, user sends computed value with nonce R to server. Server stores R .

Step 3 $S \Rightarrow U : \hat{e}(X_U, R_U)^{MPIN \cdot R_S \cdot X_S}, N$

Server computes $\hat{e}(X_U, R_U)^{MPIN \cdot R_S \cdot X_S}$ from nonce R_S and server's secret key X_S . Next, server sends computed result with N to user. N is an initial value for certain limited number of hash computation. User stores N .

Step 4 $U \Rightarrow S : OTP, R_H$

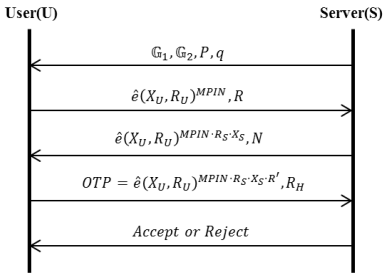


Fig. 1. Registration procedure.

Fig.1 shows flow of registration procedure.

User draws $R' = H^N(R)$ with secure hash function. With R' , user computes $OTP = \hat{e}(X_U, R_U)^{MPIN \cdot R_S \cdot X_S \cdot R'}$ and sends

to server with R_H for next R'.

Step 5 $S \rightarrow U$: *Accept or reject*

Server verifies OTP. If verification successes then server stores OTP, R_H and R' (as R) and server sends acceptance message to user.

B. Authentication Phase

We assume that following authentication phase runs on insecure channel.

Step 1 $U \rightarrow S : OTP', R_H' \oplus R'$

User sends $OTP' = \hat{e}(OTP, T_U)^{R'}$ and $R_H' \oplus R'$ to server. During the OTP' computation, user's timestamp T_U and $R' = H^{R_H \bmod N}(R)$ are used. User stores R_H' as R_H, R' as R and OTP' as OTP.

Step 2 S : *Accept or reject*

Server draws $R' = H^{R_H \bmod N}(R)$ with stored R_H and R and computes OTP' with server's timestamp T_S. Server compares received value with computed value and if it matches, server authenticates user. Then server stores R_H' as R_H, R' as R and OTP' as OTP.

We assume that server time and user time are synchronized. In other case, user can send its timestamp at Step1 in the form of $T_U \oplus R''$ with $R'' = H(R')$. Then server can compute T_U and compare with T_S to see if time interval between T_U and T_S is smaller than maximum time interval ΔT.

Following Fig. 2 shows authentication phase.

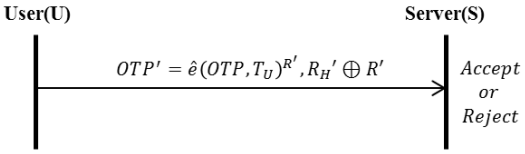


Fig. 2. Authentication procedure.

V. Analysis

A. Masquerading Attack

Masquerading attack is that an adversary disguise as other users to log into services. This attack can be classified as insider attack and outsider attack. Choi and Kim [9]'s scheme is safe from masquerading attack by outsider. In the case of insider attack, however, their scheme allows an adversary disguise as a legal user. The key point of Choi and Kim [9]'s scheme is that the time stamp, which is shared among insider registered in the same server, was used to encode previous OTP. This property makes the scheme depends on the security of MPIN. However, MPIN does not have enough length since OTP is very short in general condition. To solve this problem, we employed random numbers instead of MPIN and time stamp; namely, OTP (OTP') was computed as $\hat{e}(OTP, T_U)^{R'}$. For an adversary trying to compute OTP of another user, the adversary must find R' from $\hat{e}(OTP, T_U)^{R'}$ or $R_H' \oplus R'$. Firstly, assume that the adversary tries to find R' from $\hat{e}(OTP, T_U)^{R'}$. Let parameters $\langle g, g^{OTP}, g^{T_U}, g^{R'} \rangle$ be public parameters; our scheme is based on BDHP. Solving this problem is difficult as BDHP. We also show the proof of DBDHP. Assume that parameters $\langle g, g^{OTP}, g^{T_U}, g^{R'}, x \rangle$ is given; x is an element of $\mathbb{G}_2$. Deciding whether $\hat{e}(g^{OTP}, g^{T_U})^{R'} = x$ is also difficult as DBDHP. Therefore, our construction satisfies BDHP and DBDHP. Consequently, in order to masquerade as a legal user, the adversary must solve BDHP or DBDHP, which is known as strong security proofs.

B. Eavesdropping

Assume that an adversary tries to compute or find OTP of another legal user. He/she can easily eavesdrop the all the packets required for the authentication. Thereafter, the adversary analysis to gain OTP and next OTP for the user. The eavesdropper can acquire following:

$$\langle OTP', R_H' \oplus R' \rangle \Rightarrow \langle \hat{e}(OTP, T_U)^{R'}, R_H' \oplus R' \rangle \qquad (6)$$

In (6), $R' = H^{R_H \bmod N}(R)$ and R_H' are nonces. The key point is that R' is shared with server by using nonce R_H. In order to compute OTP, the adversary must find nonce R_H. The eavesdropper can try to exclusive-OR with $R_H' \oplus R'$ and arbitrary R_A. After computation, we obtain R_H''. In order to compute OTP, the adversary must also know random number R. However, server and users communicate under secure channel in registration phase. Therefore, the adversary cannot compute OTP. In addition, if R_H'' computed by the adversary is equal to R_H' generated by the legal user, verifying $R_H'' = R_H'$ is One-Time Pad [4], [5] problem. Consequently, the eavesdropper does not sense anything about parameters used to compute OTP.

Otherwise the eavesdropper might learn $T_U \oplus R''$ from authentication packet in time-unsynchronized circumstances. He/she might acquire R'' from $T_U \oplus R''$ by using their timestamp T_A. However the adversary cannot guess R' from R''. Hence attacker can't get any parameter used to compute OTP and our scheme is safe.

VI. Conclusion

Various services use password-based security to make users log into the services. Password technology can be divided into static password and dynamic password. Dynamic password (e.g. OTP) is stronger than static password since the password is changed whenever sessions are newly created. Especially, securely sensitive services (e.g. online banking, online shopping and etc.) recommend users to use OTP-based authentication.

The most popular OTP scheme is S/KEY. However, S/KEY scheme has hash collision problem. In order to overcome this issue, Choi and Kim [9] proposed pairing-based OTP scheme. Choi and Kim's scheme eliminated hash collision problem by exponential operation of MPIN. Unfortunately, the scheme is still vulnerable against insider attack.

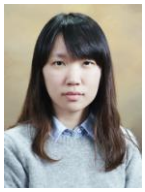
In this paper, we proposed insider attack–resistant OTP scheme based on bilinear maps. In order to generate OTP, our scheme uses two random numbers instead of MPIN. The main idea is that OTP is computed by exponential operation of a random number. When users are authenticated by the server using OTP mechanism, users give the server a hint for next OTP; namely, the users and the server prepare to authenticate future sessions in given session. The hint is formed as exclusive-OR of two random numbers. In an aspect of an adversary, solving the hint is difficult as complexity of solving one-time pad cipher since he/she cannot verify whether the value is correct although correct random number is given. Consequently, our scheme prevents insider attack and can be widely used to enhance OTP authentication.

ACKNOWLEDGEMENT

This work was supported by the IT R&D program of MKE/KEIT. [10039953, Network Centric Next Generation Active RFID Technology Development].

REFERENCES

[1] *The MD5 Message-Digest Algorithm*, RFC1321-1992.
[2] *Announcing the Secure Hash Standard*, FIPS 180-2-2002.
[3] *On Internet Authentication*, RFC1704-1994.
[4] F. G. Deng and G. L. Long, "Secure direct communication with a quantum one-time pad," *Phys. Rev. A*, vol. 69, no. 5, pp. 52319, May 2004.
[5] Y. Dodis and J. Spencer, "On the (non) universality of the one-time pad," in *Proc. 43rd Annual IEEE Symposium on Foundations of Computer Science*, 2002, pp. 376-385.
[6] L. Lamport, "Password authentication with insecure communication," *Commun. ACM*, vol. 24, no. 11, pp. 770-772, Nov. 1981.
[7] *A One-Time Password System*, RFC 2289-1998.
[8] *The S/KEY One-Time Password System*, RFC1760-1995.
[9] J. Choi and H. Kim, "One-Handled the mobile one-time password scheme," *Journal of the Korea Institute of Communications and Information Sciences*, vol. 37, no. 6, pp. 497-501, June 2012.
[10] *TOTP, Time-Based One-Time Password Algorithm*, RFC 6238-2011.
[11] HOTP, A HMAC-Based One-Time Password Algorithm, RFC 4226-2005.
[12] S. Y. Kang and I. Y. Lee, "A study on UICC (Universal IC Card)-Based authentication mechanism using OTP," *Journal of the Korea Institute of Information Security and Cryptology*, vol. 21, no. 5, pp. 21-31, 2008.
[13] Y. Kim, K. Baek, Y. Kim, J. Ryou, G. Baek, and J. Park, "The development of a one-time password mechanism improving on S/KEY," *Journal of the Korea Institute of Information Security and Cryptology*, vol. 9, no. 2, pp. 25-35, 1999.
[14] H. G. Kim and I. Y. Lee, "A study on one-time password authentication scheme in mobile environment," *Journal of Korea Multimedia Society*, vol. 14, no. 6, pp. 785-793, 2011.
[15] M. Lin and C. C. Chang, "A secure one-time password authentication scheme with low-computation for mobile communications," *SIGOPS Oper. Syst. Rev.*, vol. 38, no. 2, pp. 76-84, Apr. 2004.
[16] I. Liao, C. Lee, and M. Hwang, "A password authentication scheme over insecure networks," *Journal of Computer and System Sciences*, vol. 72, no. 4, pp. 727-740, June 2006.
[17] S. Lee and K. M. Sivalingam, "An efficient one-time password authentication scheme using a smart card," *International Journal of Security and Networks*, vol. 4, no. 3, pp. 145-152, Jan. 2009.
[18] O. Goldreich, S. Micali, and A. Wigderson, "Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems," *J. ACM*, vol. 38, no. 3, pp. 690-728.
[19] J. Boyar, K. Friedl, and C. Lund, "Practical zero-knowledge proofs: Giving hints and using deficiencies," in *Proc. Advances in Cryptology - EUROCRYPT '89*, 1990, pp. 155-172.
[20] D. Boneh, "The decision Diffie-Hellman problem," in *Proc. Algorithmic Number Theory*, 1998, pp. 48-63.
[21] M. Kim and K. Kim, "A new identification scheme based on the bilinear Diffie-Hellman problem," in *Proc. of Information Security and Privacy*, 2002, pp. 362-378.



Yunjin Lee is currently a master's candidate in the Computer Engineering Department, Pusan National University. She received B.S. in Computer Engineering, Pusan National University, Republic of Korea, in 2012. Her researches include Access Control on Smart Grid, authentication based on bilinear maps and APT (Advanced Persistent Threat).

Howon Kim received the BSEE degree from Kyungpook National University, Daegu, Republic of Korea, in 1993, and the MS and PhD degrees in electronic and electrical engineering from Pohang University of Science and Technology (POSTECH), Pohang, Rep. of Korea, in 1995 and 1999, respectively. From July 2003 to June 2004, he studied with the COSY group at the Ruhr-University of Bochum, Germany. He was a senior member of technical staff at the Electronics and Telecommunications Research Institute (ETRI), Daejeon, Rep. of Korea. He is currently working as an associate professor with the Department of Computer Engineering of Pusan National University, Busan, Rep. of Korea. His research interests include RFID technology, sensor networks, information security, and computer architecture. Currently, his main research focus is on mobile RFID technology and sensor networks, public key cryptosystems and their security issues. He is a member of the IEEE, IEEE Computer Society, and IACR.