Enhanced Attribute-Based Proxy Re-Encryption for Home Network

Jongseok Choi and Howon Kim

***Abstract*—This paper studies security on home network to apply access control and encryption. It is difficult to implement and run a database server for access control as individual. For both access control and encryption, home network employs a series of Attribute-Based Encryption (ABE) schemes. In a string of the encryption schemes, we apply Attribute-Based Proxy Re-Encryption (ABPRE) to the network. In our scheme, authenticated people can encrypt all the data, control access to the data and temporarily delegate their permission to another they trust implicitly. A framework we propose for the security of the network use a ticket, an arbitrary bit sequence, to protect a key to decrypt the data and to decide whether the people have been fully allowed by home gateway or authorized people. The members of the family can obtain the ticket by decrypting security message in home gateway or delegate it by re-encrypting the ticket. Periodically updated by the gateway, the ticket would be automatically expired. The representative can search and control the data by using the delegated ticket up to when the ticket is valid.**

***Index Terms*—Home network, attribute based encryption, proxy re-encryption, authentication, ticket encryption.**

I. Introduction

As increasing the concern of home network, its security has been focused by people interesting to implement networks and design security models. It has been proposed to implement home network [1]-[6]. Disregarding the security for home network, they are useless in the real world. If anyone access home network of others, violent crime will easily occur by controlling home appliances. For example, let us assume that resources (such as gas, electricity and etc.) can be adjusted by home network service. An adversary can steal connection between authority and home. He/she, then, set the resources as dangerous as possible. If the house has the unsafe condition for a long time, it can cause any problem such as explosion, electrical short or etc. For the reason, it began to study authentication for home network. So far, most of security articles [7] and [8] on home network have been concerned with access control allowing only rigid authorities.

In this paper, we proposed a new attribute-based proxy re-encryption for home network. Attribute-Based encryption [9]-[12] presented so far is difficult to apply to home network. By employing this scheme, the home network can not only provide both authentication and data encryption but also temporarily delegate the permission of authorities to indirect people they trust. This system synchronizes tickets with entire appliances over the home network. The whole appliances should allow valid tickets to control and read their data. If an authority delegates the permission to another, the person can get a ticket at the time. The ticket is updated periodically to a new one. After the period, the delegated ticket is automatically expired.

Manuscript received November 2, 2012; revised January 22, 2013.

The authors are with the Department of Computer Engineering, Pusan National University, Gumjeong-Gu, Busan, Korea (e-mail: jschoi85@ pusan.ac.kr, howonkim@ pusan.ac.kr).

A. Our Contributions

This paper enhanced security of home network. In order to improve both authentication and confidentiality, a new attribute-based proxy re-encryption (ABPRE) can be designed. The new ABPRE scheme does not require individual database servers. If the scheme is adapted to all data of appliances over home network, computational cost was rapidly increased. To solve this problem, this paper also described ticket-based framework in which the new ABPRE was employed. Using a ticket encrypted data is timely decrypted by, the framework helps home network efficiently manipulate ABPRE. In the proposed framework users are classified into two groups: friends and members of the network. The framework consists of levels of friends, authorities, gateway and appliances. Authorities gain direct access to home gateway and obtain a ticket to decrypt all the data from appliances. When a friend wants to gain access to the network and control of appliances, he/she can obtain a ticket through an authority re-encrypting the ticket. After acquiring the ticket, the representative gains control of appliances over the home network. We note that the home gateway has no hand in the connection between the representative and appliances.

B. Organization

The remainder of this paper is composed of five sections. The next section gives preliminary. The section describes three properties of bilinear maps and complexity for evaluating security of our scheme. The third section shows a novel framework for home network access control then the next section describes enhanced attribute-based proxy re-encryption for home network. We analysis our scheme in Section V. Finally, we conclude this paper in Section VI.

II. Preliminary

This section describes properties of bilinear maps, bilinear Diffie-Hallman assumption [13] and [14] and attribute based proxy re-encryption [15].

A. Properties of Bilinear Map

Let G_1 , G_2 be cyclic groups over order q . $\hat{e}: G_1 \times G_2 \to G_T$ is a bilinear map. The map has three properties. At the first, the bilinear map has to satisfy bilinearity, $\hat{e}(P^a, Q^b) = \hat{e}(P,Q)^{ab}$ where $P \in G_1$, $Q \in G_2$

DOI: 10.7763/IJCCE.2013.V2.192

and $a,b \in Z$. In the next, if two elements P,Q are not identity element such as zero, the result is also one, $\hat{e}(P,Q) \neq 1$. Namely, bilinear maps have to satisfy non-degeneracy. Finally, $\hat{e}$ has to be efficiently computable.

B. Complexity

LP (Logarithm Problem) is known that it has enough security from being solved in polynomial time. Therefore, PKC (Public-Key cryptosystem) has been designed with based on LP. Especially, many PKC schemes have used Diffie-Hellman assumption to evaluate new PKC schemes since Diffie-Hellman key exchange protocol [16] based on LP was proposed. In this section, we describe two Diffie-Hellman problems: Computational Diffie-Hellman Problem [17] and Decision Diffie-Hellman Problem [18].

However, Diffie-Hellman assumption has less complexity than LP complexity in the special condition; in other word, Diffie-Hellman problem becomes unsecure in some condition. For this problem, Joux [19] proposed third-parties Diffie-Hellman key exchange protocol. A shared key among three users can be generated based on bilinear map.

Many PBC (Pairing-Based Cryptography) schemes can be proved by bilinear Diffie-Hellman problems. In this section, we also describe two bilinear Diffie-Hellman problems: bilinear Diffie-Hellman problem [20] and decision bilinear Diffie-Hellman problem [20].

1) Computational diffie-hellman problem

CDHP (Computational Diffie-Hellman Problem) [17] means computational complexity to solve the shared key by Diffie-Hellman protocol from given Diffie-Hellman parameters. To generalize, CDHP is solving g^{ab} by using given parameters $\langle g, g^a, g^b \rangle$.

From given parameters $\langle g, g^a, g^b \rangle$, it is difficult to find g^{ab}. In order to compute g^{ab}, g^a and b, g^b and a or g and ab can be known or computed. However, difficulty of computing or recognizing a, b or ab is similar to difficulty of LP.

Consequently, algorithms based on CDHP assumption is secure.

2) Decision diffie-hellman problem

DDHP (Decision Diffie-Hellman Problem) [19] means decisional complexity to decide whether given parameter g^c was derived from other parameters g, g^a and g^b where parameters $\langle g, g^a, g^b, g^c \rangle$ is given. In order to recognize that g^c is same with g^{ab}, we have to know g^{ab}; namely, DDHP and CDHP have same complexity in general condition.

Assume that g^c is same with g^{ab}. Given parameters is followings:

$$\langle g, g^a, g^b, g^{c=ab} \rangle \quad (1)$$

In this condition, sensing $g^c = g^{ab}$ is difficult as LP and CDHP over finite field. However, this problem is easier over bilinear map. g^a and g^b can be computed to $\hat{e}(g^a, g^b) = \hat{e}(g,g)^{ab}$ by pairing operation. Similarly, g and g^c can be computed to $\hat{e}(g, g^c) = \hat{e}(g,g)^c$. We assumed $g^c = g^{ab}$. According to the hypothesis, $\hat{e}(g,g)^c$ becomes $\hat{e}(g,g)^{ab}$. Finally, we can decide whether g^{ab} and g^c is same by following:

$$\hat{e}(g^a, g^b) = \hat{e}(g, g^c) = \hat{e}(g,g)^{c=ab} \quad (2)$$

Consequently, DDHP is easier than LP in this condition; where $g^c = g^{ab}$, DDHP can easily reveal the key.

3) Bilinear diffie-hellman problem

BDHP (Bilinear Diffie-Hellman Problem)[20] is extended from CDHP to bilinear maps; it means difficulty of computing a key of Bilinear Diffie-Hellman key exchange protocol. Through the bilinear Diffie-Hellman protocol, three users share a same key. When the users establish the key, each user generates a random number and computes their public parameter; three public parameters $\langle g, g^a, g^b, g^c \rangle$ is generated by each user. After sharing public parameters, each user computes $\hat{e}(g^a, g^b)^c = \hat{e}(g^b, g^c)^a = \hat{e}(g^c, g^a)^b = \hat{e}(g,g)^{abc}$. Therefore, BDHP means to find $\hat{e}(g,g)^{abc}$ from parameters $\langle g, g^a, g^b, g^c \rangle$. Complexity of BDHP is also similar with CDHP.

4) Decision bilinear diffie-hellman problem

DBDHP (Decision Bilinear Diffie-Hellman Problem)[20] is also extended from DDHP to bilinear maps. However, DBDHP is stronger than DDHP; DBDHP is secure although given arbitrary selected parameter was derived from other given operands. In DBDHP, $\langle g, g^a, g^b, g^c, x \rangle$ is given. Among these parameters, x is an element of G_2 where a bilinear map is defined as $\hat{e}: G_1 \times G_1 \rightarrow G_2$. While other parameters g, g^a, g^b, g^c is elements of G_1. In this condition, DBDHP means complexity of deciding whether x is equal to $\hat{e}(g,g)^{abc}$. From given parameters, deciding the statement is difficult as difficulty of BDHP. If given x is equal to $\hat{e}(g,g)^{abc}$, it is difficult to sense that x was derived from g, g^a, g^b, g^c.

III. A Novel Framework

So far, most people have been interested in studies on applying access control (such as RBAC) to home network. However, in general it is hard to operate individual database server for access control over home network. Existing studies also excluded encryption of data of appliances over the network; if an adversary skips access control in some way or other, the adversary can know all the data over the network

The proposed frame work not only provide integrity and confidentiality of the data but also eliminate running database server by employing attribute based encryption for access control. If all of the data are encrypted by attribute based

encryption, the users, who connect to the home network, spend much time to decrypt the data due to complexity of ABE schemes. Fig. 1 describes four levels of the framework.

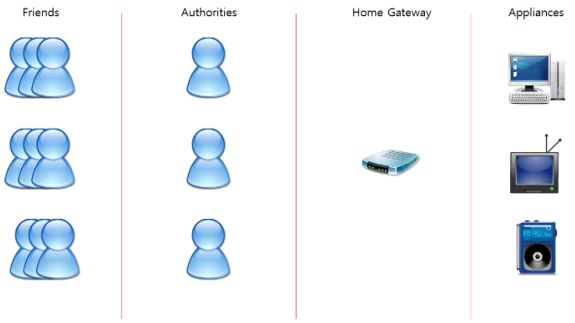

Fig. 1. Levels of the proposed framework.

In the framework, home gateway manages a ticket distributed to all the appliances over home network. Authorities can gain access by decrypting a ticket. The ticket can be used to encrypt encryption key of data from appliances. Think a scenario. One of authority group wants to gain access to home network. He/she has to obtain a ticket by decrypting his/her key and permission of a member. Thereafter, the ticket helps appliances decrypt a key used to encrypt their data by symmetric key cryptography. However, traditional ABE schemes is little flexible against exceptional condition. For example, all authorities leaved their house for business trip, however, wireless communication nearby the place is blocked as security problems. While the business trip, the house is regularly checked for safety. However there is no authority to do it. For this condition, the proposed framework employed attribute based proxy re-encryption (ABPRE) instead of traditional ABE schemes. ABPRE makes the authorities delegate their permission to others; friends of authorities can gain a ticket. Fig. 2 describes the procedures for delegating an authority to friends.

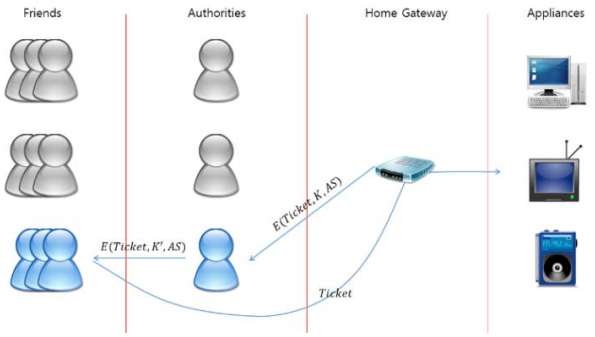

Fig. 2. Communication of friends.

IV. Enhanced Attribute-Based Proxy Re-Encryption

This section introduction attributes based proxy re-encryption combined with symmetric key encryption. ABPRE is difficult to be applied to all the data over the whole network since one of public key encryption requiring heavy computation. Enhanced ABPRE scheme is a tuple of algorithms (Setup, Encryption, Delegation, Authentication).

A. Definition of Enhanced ABPRE Model

Setup (1^k) generates some parameters.

Encryption (*Ticket, K, AS*) encrypts data and send members of family respectively where *AS* is access structure for the members.

Delegation (*Ticket, K', AS*) re-encrypts the data by a member adding some extra to own encrypted data and then notify that to home gateway. Upon recognizing the extra, the home gateway temporarily changes the key of the member.

Authentication (*data, K or K', AS*) decrypts the received data. If it is accepted, the gateway issues session key.

B. Enhanced ABPRE

1) Setup

In this phase, home gateway chooses some parameters and then issues credentials to all members who have access to the home. Several parameters are generated by home gateway. Let G, G_T and $\hat{e}: G \times G \to G_T$ be two algebraic groups and a bilinear map, respectively. At this time, G and G_T have order of prime q. Appliances then encrypts their contents by using $k \in Z_q$ generated by the home gateway. The main point at the issue is that the appliances stores $T \oplus k$ rather then k, where T means time stamp and k is hash value of a element in G_T; namely, we use hash function $H: G_T \to Z_q$. We also assume that the appliances and the gateway share the same time stamp. In addition, the time stamp between them has to be as close as fixed distance ΔT because the time stamp will be periodically updated.

2) Encryption

The gateway issues credentials to the members. The credentials is generated as following.

$$\langle \hat{e}(sP, Q), \hat{e}(sP, kQ + uQ) \rangle \tag{3}$$

By using operation of bilinear map, the equation, $\hat{e}(sP, kQ + uQ) = \hat{e}(sP, Q) \cdot \hat{e}(sP, uQ)$, is established. This operation makes our members possible to delegate credential to another.

3) Delegation

A member who wants to delegate own permission to his or her friends randomly chooses a temporary number as a key cloak. The member results a temporary credential (TC) for the friend; at this time, the temporary credential should be derived from the credential (C) the member has. The credential (TC) is computed as following.

$$\begin{aligned} TC &= C \cdot \hat{e}(sP, Q)^t \\ &= \hat{e}(sP, kQ + uQ) \cdot \hat{e}(sP, Q)^t \end{aligned} \tag{4}$$

After this computation, the member sends it to the friend. The member then notifies the home gateway that $\hat{e}(sP, Q)$ was issued as temporary verification. Upon recognizing the temporary parameter, the gateway stores it for its verification.

4) Authentication

During delegation phase, the gateway obtained the temporary verification from the family member.

Step 1. A member or a friend sends their credential to the gateway. At this time, the credential would be

$\hat{e}(sP, kQ+uQ)$ or $\hat{e}(sP, kQ+uQ)\cdot\hat{e}(sP,Q)^t$.

Step 2. The gateway decrypts the received data. Whether or not the temporary verification will be used to decrypt the data is decided by the gateway; if a member delegates his or her credential and send temporary information to help a person have access to the home, the gateway has to recognize whether the member was delegated his or her permission to other people. Assume that the received data and decrypted data are denoted as R and D, respectively. In this condition, the gateway computes as following:

$$D = \begin{cases} \dfrac{R}{\hat{e}(sP,uQ)} \\ \dfrac{R}{\hat{e}(sP,uQ)\cdot\hat{e}(sP,Q)^t} \end{cases} \quad (5)$$

Step 3. The gateway generates a session key and issues it to the family members or their friends. At this, the session key is computed as $SK = H(D)\oplus T$.

Step 4. The entity obtains access with the session key. In order to control the appliances over the home network, the entity sends the session key to an appliance which the entity wants to approach. Upon receiving the session key, the appliance at first computes a key as $SK \oplus T$. The appliance then accepts the entity to adjust or observe the contents. The session key can be used to approach the appliances for the fixed period ΔT.

V. Analysis

A. Proof of Delegation

The family members of this network can delegate their permission to trusted friends. In delegation phase, there are two issues. The first issue is how the home gateway can decrypt the re-encrypted messages. The solution is very simple. We did overcome this issue by the members announcing their re-key, which was used to re-encrypt the message, to home gateway. Members, who delegated their permission to their trusted friends, used $\hat{e}(sP,Q)^t$ to re-encrypt credential; namely, a temporary credential is derived from credential and $\hat{e}(sP,Q)^t$. Consequently, home gateway can decrypt the received message from friends of the members.

$$\frac{R}{\hat{e}(sP,Q)\cdot\hat{e}(sP,Q)^t} = \frac{R}{\hat{e}(sP,uQ+tQ)} \quad (6)$$

The second issue is possibility to revoke temporary credentials. If temporary credential could not be revoked, the friends can consistently have access to the home network. In order to prevent it, our scheme used time stamp to re-encrypt the message; a public parameter $\hat{e}(sP,Q)$ multiply by exponential of time stamp t. This computation means that after fixed time interval, the temporary credentials will be expired.

B. Key Exposure

This scheme is based on bilinear logarithm problem and can be proved by bilinear Diffie-Hellman problem. In this section we show how to prevent key exposure. The main issue is that whether the credential known to the only members of the home network is reveled in delegation phase to friends. For the proof of this issue, we assume that the friends received temporary credential and know it. The credential is formed as following:

$$\begin{aligned} C\cdot\hat{e}(sP,Q)^t &= \hat{e}(sP,kQ+uQ)\cdot\hat{e}(sP,Q)^t \\ &= \hat{e}(sP,kQ+uQ+tQ) \end{aligned} \quad (7)$$

The key is $\hat{e}(sP,kQ)$. From the above equation, the friends have to find $\hat{e}(sP,uQ+tQ)$ in order to obtain the key. However, finding $\hat{e}(sP,uQ+tQ)$ from $\hat{e}(sP,kQ+uQ+tQ)$ is logarithm problem over bilinear map.

Although $\langle g=(P,Q), g^u=uQ, g^k=kQ, g^t=tQ\rangle$ is given, our scheme is secure as the friends have no sense about the secret *S*; our scheme satisfies BDHP. Furthermore, where $\langle g, g^u, g^k, g^t, x=\hat{e}(sP,k'Q)\rangle$ is given, the proposed scheme is also secure similarly; DBDHP is also satisfied on this scheme.

C. Complexity

Michael Scott [21] implemented cryptographic pairings on 3GHz Pentium IV processor. Brown *et al* [22] implemented ECC (Elliptic Curve Cryptography) on Pentium II 400 MHz. In this section, we evaluated the proposed scheme by using these performances. Our scheme requires 3 scalar multiplication, 2 pairing operation and 1 point addition or 1 finite field multiplication for encryption phase. In delegation phase, 1 finite field multiplication and 1 finite field exponential are required. Authentication phase can be divided by two conditions: delegated credentials and original credentials. In order to verify delegated credentials, 2 finite field multiplication and 1 inversion are required. 1 finite field multiplication and 1 inversion are required for original credentials. Our scheme uses scalar multiplication, pairing operation, point addition, field exponential, field multiplication and inversion. According to two implementations [21] and [22], these operations require 1.82ms, 3.88ms, 0.168 μs (0.00ms), 1.14ms, 2.884 μs (0.00ms) and 249.69 μs (0.25ms). Finally, each phase can be evaluated as following:

TABLE I: The Performance of the Proposed Scheme

	Encryption	Delegation	Authentication	
			Delegated	Non-delegated
Cost	3S+2P+1A 3S+2P+1M	1M+1E	2M+1I	1M+1I
Latency	≈ 18.68ms	≈ 1.14ms	≈ 0.25ms	≈ 0.25ms

VI. Conclusion

In this paper, we proposed enhanced attribute-based proxy re-encryption (ABPRE) scheme for home network. Enhanced ABPRE aimed to improve both authenticity and confidentiality. In addition, the proposed scheme allows the members of home network to temporarily delegate their own

permission; the trusted friends of the members are possible to gain access to home network. For the issue, we used home network consisting of appliances sharing time stamp. Also, by using re-key, temporary credentials could be generated by the members for their friends. At the delegation phase, two issues come up: how home gateway decrypt the re-encrypted message (decryption problem) and how temporary credentials can be revoked (revocation problem). In order to analysis two issues, we gave a proof in section 5. After home gateway authenticate the entities, the entities acquire ticket to control or read appliances; the entities have permission as same as the members delegating the entities.

In short, our scheme is one of functional encryptions. We proposed attribute-based proxy re-encryption for home network. The main construction of our scheme is to delegate the permission of members in special event. In the construction, we solved decryption problem and revocation problem. In addition, in order to increase efficiency, we employed tickets; because appliances can be controlled by ticket, home network does not need to update key used to encrypt data from appliances consistently.

ACKNOWLEDGMENT

This work was supported by the Industrial Strategic Technology Development Program (No.10043907) funded by the Ministry of Knowledge Economy (MKE, Korea).

REFERENCES

[1] X. Li and W. J. Zhang, "The design and implementation of home network system using OSGi compliant middleware," *IEEE Trans. on Consumer Electronics*, vol. 50, no. 2, pp. 528-534, May 2004.

[2] D. S. Kim, J. M. Lee, and W. H. Kwon, "Design and implementation of home network systems using UPNP middleware for networked appliances," *IEEE Trans. on Consumer Electronics*, vol. 48, no. 4, pp. 965-970, Nov. 2002.

[3] P. M. Corcoran, "Mapping home-network appliances to TCP/IP sockets using a three-tiered home gateway architecture," *IEEE Trans. on Consumer Electronics*, vol. 44, no. 3, pp. 729-736, Aug. 1988.

[4] B. A. Miller, T. Nixon, C. Tie, and M. D. Wood, "Home networking with universal play and plug," *IEEE Communication Magazine*, vol. 39, no. 12, pp. 104-109, Dec. 2001.

[5] S. Y. Cho, "Framework for the composition and interoperation of the home applications based on Heterogeneous Middleware in Residential Network," *IEEE Trans. on Consumer Electronics*, vol. 48, no. 3, pp. 484-489, Aug. 2002.

[6] D. S. Kim, W. H. Kwon, Y. H. Kim, H. J. Shin, and Y. I. Kwan, "Home network message specification for white goods and its applications," *IEEE Trans. on Consumer Electronics*, vol. 48, no. 1, pp. 1-10, Feb. 2002.

[7] G. W. Kim, D. W. Kim, J. H. Lee, J. B. Hwang, and J. W. Han, "Considerations on security model of home network," in *Proc. Advanced Communication Technology 2006*, 2006, pp. 4-112.

[8] E. Callaway, P. Gorday, L. Hester, J. A. Gutierrez, M. Naeve, B. Heile, and V. Bahl, "Home networking with IEEE 802.15.4: A developing standard for low-rate wireless personal area networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 70-77, Aug. 2002.

[9] G. Vipul, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based encryption for fine-grained access control of encrypted data," in *Proc. the 13th ACM conference on Computer and communications security*, 2006, pp. 89-98.

[10] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," *in Proc IEEE Symposium Security and Privacy*, 2007, pp. 321-334.

[11] B. Waters, "Ciphertext-Policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Proc. Public Key Cryptography*, 2011, pp. 53-70.

[12] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in *Proc Advances in Cryptology–EUROCRYPT 2010*, 2010, pp. 62-91.

[13] D. Boneh and X. Boyen, "Efficient selective- id secure identity based encryption without random oracles," in *Proc. Eurocrypt'04*, 2004, pp. 223-238.

[14] D. Boneh and X. Boyen, "Secure identity based encryption without random oracles," in *Proc. Crypto'04*, pp. 443-459, 2004.

[15] X. H. Liang, Z. F. Cao, L. Huang, and J. Shao "Attribute based proxy re-encryption with delegating capabilities," in *Proc. ASIACCS '09*, 2009, pp. 276-286.

[16] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. on Information Theory*, vol. 22, no. 6, pp. 644-654, Nov. 1976.

[17] A. Joux and K. Nguyen, "Separating decision diffiehellman from computational diffiehellman in cryptographic groups," *Journal of Cryptology*, vol. 16, no. 4, pp. 239-247, Sep. 2003.

[18] D. Boneh, "The decision diffie-hellman problem," in *Proc. Algorithmic Number Theory*, 1998, pp. 48-63.

[19] A. Joux, "A one round protocol for tripartite diffiehellman," *Journal of Cryptology*, vol. 17, no. 4, pp. 263-276, Sep. 2004.

[20] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Proc. Advances in Cryptology-CRYPTO 2001*, 2001, pp. 213-229.

[21] M. Scott, "Implementing cryptographic pairings," in *Proc International Conference on Pairing-based Cryptography 2007*, 2007, pp. 177-196.

[22] M. Brown, D. Hankerson, J. López, and A. Menezes. "Software implementation of the NIST elliptic curves over prime fields," in *Proc Topics in Cryptology-CT-RSA 2001*, 2001, pp. 250-265.

Jongseok Choi is currently a master's candidate in the Computer Engineering Department, Pusan National University. He received B.S. in Information Security, Tongmyong University, Republic of Korea, in 2011. His researches include IBE (Identity-Based Encryption), PBC (Pairing-Based Encryption), mobile security, enhanced privacy protection, PKC (Public Key Cryptography).

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.