향상된 경계 결정 기반의 Diffie-Hellman 키 일치 프로토콜

준회원 박 선 영*, 김 주 영*, 종신회원 송 홍 엽*

Design of Improved Diffie-Hellman Key Agreement Protocol Based on Distance Bounding for Peer-to-peer Wireless Networks

Sern-Young Park*, Ju Young Kim* *Associate Members*, Hong-Yeop Song* *Lifelong Member*

요 약

본 논문은 무선 환경에서의 향상된 경계 결정 기반의 Diffie-Hellman (DH) 키 일치 프로토콜을 제안한다. 제안하는 프로토콜에서는 경계 결정을 통해 두 사용자간에 주고받는 메시지의 무결성과 안정성을 보장한다. 본 논문은 종래의 경계 결정 기반의 DH 키 일치 프로토콜의 비효율적이고 불안정적인 측면을 보완하여 교환되어야 할 메시지 수와 관리해야 할 파라미터 수를 줄였으며 2(7682(k/64)-64) 개의 XOR 연산을 절감하였다. 또한 DH 공개 정보의 안전한 재사용을 가능하게 함으로써 사용자의 개입을 감소시킬 수 있다.

Key Words : Diffie-Hellman protocol, Key agreement protocol, MITM(man-in-the-middle) attack, Distance bounding, Security

ABSTRACT

We propose an improved Diffie-Hellman (DH) key agreement protocol over a radio link in peer-to-peer networks. The proposed protocol ensures a secure establishment of the shared key between two parties through distance bounding (DB). Proposed protocol is much improved in the sense that we now reduce the number of messages exchanged by two, the number of parameters maintained by four, and 2(7682(k/64)-64) of XOR operations, where k is the length of the random sequence used in the protocol. Also, it ensures a secure reusability of DH public parameters.Start after striking space key 2 times.

Ⅰ. 서 론

As the data communication is possible between personal device (e.g., a PDAs, laptops, and mobile phones), the peer-to-peer communication frequently occurs. Also, the communication systems are scattered on the fields. Therefore, the establishment of system requires auto configuration of mobile routers.

In this situation, the communication between devices must be properly secured. For this work, DH (Diffie-Hellman) key agreement protocol[1] is conventionally used. It achieves key agreement by calculating simple integer parameter without shared secret. It is appropriate for systems which have limited-power and limited-memory. However, it is vulnerable to an active adversary who uses a MITM (man-in-the-middle) attack. Also, it can be attacked by mathematical methods such as degenerate message attack[5].

* 연세대학교 전기전자공학과 부호 및 정보이론 연구실 {sy.park, jy.kim, hysong}@yonsei.ac.kr

논문번호 : KICS2007-06-247, 접수일자 : 2007년 6월 8일, 최종논문접수일자 : 2008년 1월 4일

Recently proposed protocol cope with these attacks by using various methods. Especially, we focused on DH-DB (DH based on distance-bounding) protocol[3]. S. Brand and D. Chaum proposed distance bounding protocol[2] and it ensures security based on the distance between two parties. M. Cagalj and et al. combined DH and DB protocols. In DH-DB protocol, pair of devices has the means to accurately estimate the distance between them. Based on the distance, each device upper-bounds its distance to the device of peer. If there is no other user in the boundary, the exchanged DH public parameters are accepted.

However, existing DH-DB protocol still has weakness for security. Also, it has inefficiency when it checks the integrity. Through this research, we analyze the complexity and problems of existing DH-DB. Based on the analysis we improve the DH-DB. Finally we compare the complexity and security of proposed and existing protocol. The paper is organized as follows. In Section Ⅱ we analyze the existing DH-DB. In Section Ⅲ we present our protocol. In Section Ⅳ we provide analysis of our protocols. Finally, we conclude the paper in Section Ⅴ.

Ⅱ. 논문 인용의 예

We analyze the following protocol. Two users, A (Alice) and B (Bob), each equipped with a personal device capable of communicating over a radio link, get together and want to establish a shared key. We assume that they do not share any authenticated cryptographic information (e.g., public keys or shared secrets) prior to this meeting. Also, we assume that each device has the means to accurately estimate the distance between them.

2.1 Symbols and Notations

The following symbols and notations are used through this paper.

p: large prime number

q: prime number that divides $p-1$

Z_p^*: multiplicative group

g: generator of Z_p^*, $(2 \le g \le p-2)$

$X \| Y$: concatenation operator of X and Y

$X \oplus Y$: XOR operation of X and Y

$(c,d) \leftarrow Commit(m)$: the commitment/opening pair (c,d) for message m

$m' \leftarrow Open(c,d)$: opens the commitment with the opening key d

We assume that p and g are selected and published.

2.2 Commitment Scheme

In this paper we will make use of a collision-free hash function based commitment scheme[6]. This scheme is a very practical commitment scheme based solely on collision-free hashing. To commit to a message m, the sender picks at random string x and a universal hash function f so that $f(x)=m$. Then the user applies the collision-free hash function h to get $y=h(x)$ and sends the random string x. The efficiency of this commitment scheme comes from the fact that it makes use of inexpensive hash functions only.

2.3 Protocol Description

The DH-DB protocol is shown in Figure 1. The protocol is divided into three steps: initialization, distance-bounding, and verification. In the initialization step, A and B select their secret exponents X_A and X_B randomly from Z_q^* (q=large prime) and calculate DH public parameters g^{X_A} and g^{X_B}, respectively. A and B generate k-bit random string N_A and N_B, respectively. A and B concatenate $0 \| ID_A \| g^{X_A} \| N_A$ and $1 \| ID_B \| g^{X_B} \| N_B$, respectively. Here, 0 and 1 are used to prevent a reflection attack. Then, A and B compute commitment/opening pairs, respectively. A and B also concatenate $0 \| R_A$ and $1 \| R_B$ and calculate (c_A', d_A') and (c_B', d_B'), respectively. A sends the commitment c_A and c_A' to B. B responds with this own commitment c_B and c_B'. A sends out d_A. B opens $(\widehat{c_A}, \widehat{d_A})$ and get $\widehat{m_A}$. B checks the correctness of $(\widehat{c_A}, \widehat{d_A})$ by verifying that 0 appears at the beginning of $\widehat{m_A}$. If it is successful, B sends d_B. A checks $(\widehat{c_B}, \widehat{d_B})$ by verifying that 1 appears

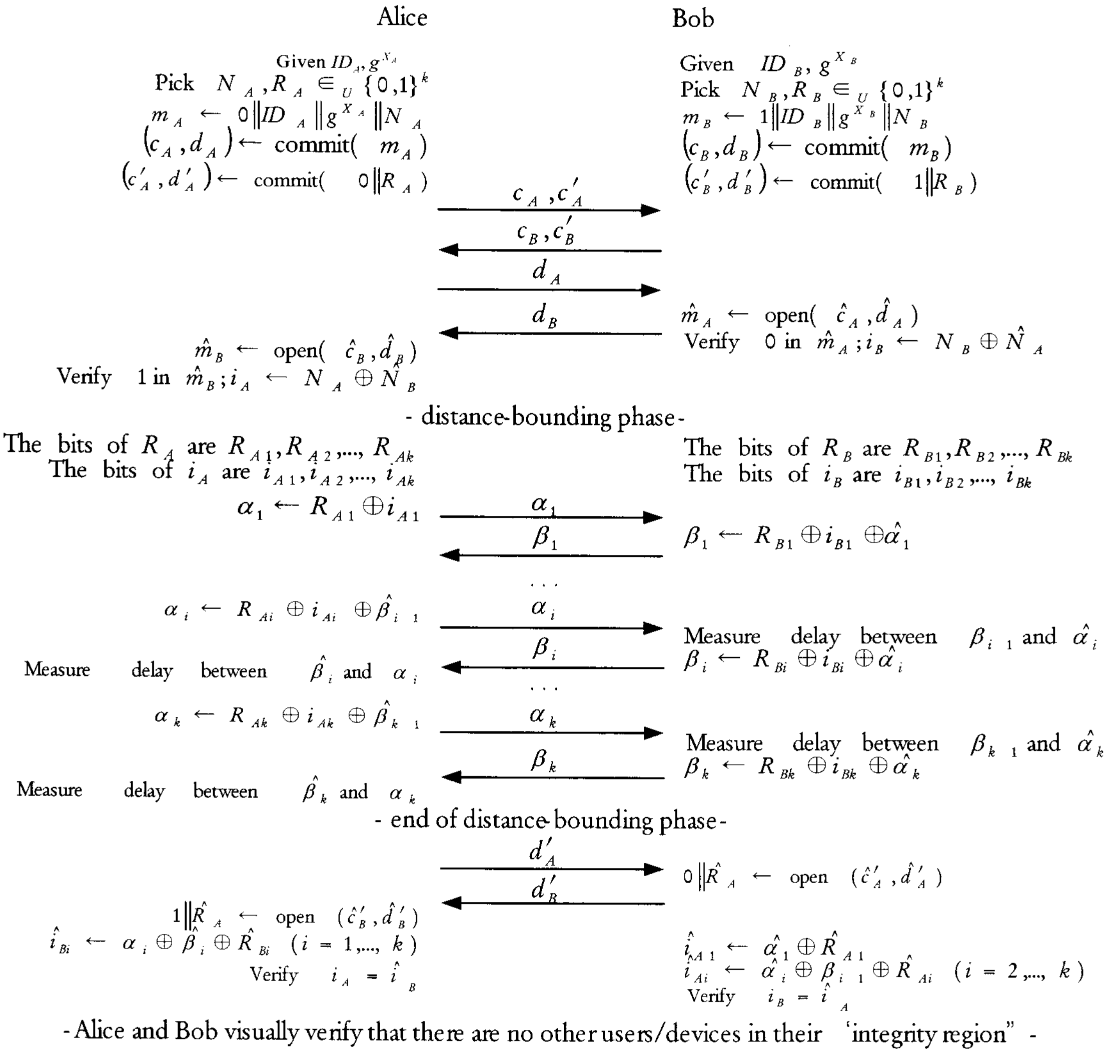

Alice
Bob
Given ID_A, g^{X_A}
Pick $N_A, R_A \in_U \{0,1\}^k$
$m_A \leftarrow 0\|ID_A\|g^{X_A}\|N_A$
$(c_A, d_A) \leftarrow$ commit(m_A)
$(c'_A, d'_A) \leftarrow$ commit($0\|R_A$)
Given ID_B, g^{X_B}
Pick $N_B, R_B \in_U \{0,1\}^k$
$m_B \leftarrow 1\|ID_B\|g^{X_B}\|N_B$
$(c_B, d_B) \leftarrow$ commit(m_B)
$(c'_B, d'_B) \leftarrow$ commit($1\|R_B$)
c_A, c'_A
c_B, c'_B
d_A
d_B
$\hat{m}_A \leftarrow$ open($\hat{c}_A, \hat{d}_A$)
Verify 0 in $\hat{m}_A; i_B \leftarrow N_B \oplus \hat{N}_A$
$\hat{m}_B \leftarrow$ open($\hat{c}_B, \hat{d}_B$)
Verify 1 in $\hat{m}_B; i_A \leftarrow N_A \oplus \hat{N}_B$
- distance-bounding phase -
The bits of R_A are $R_{A1}, R_{A2}, ..., R_{Ak}$
The bits of i_A are $i_{A1}, i_{A2}, ..., i_{Ak}$
The bits of R_B are $R_{B1}, R_{B2}, ..., R_{Bk}$
The bits of i_B are $i_{B1}, i_{B2}, ..., i_{Bk}$
$\alpha_1 \leftarrow R_{A1} \oplus i_{A1}$
α_1
β_1
$\beta_1 \leftarrow R_{B1} \oplus i_{B1} \oplus \hat{\alpha}_1$
...
$\alpha_i \leftarrow R_{Ai} \oplus i_{Ai} \oplus \hat{\beta}_{i-1}$
α_i
β_i
Measure delay between β_{i-1} and $\hat{\alpha}_i$
$\beta_i \leftarrow R_{Bi} \oplus i_{Bi} \oplus \hat{\alpha}_i$
Measure delay between $\hat{\beta}_i$ and α_i
...
$\alpha_k \leftarrow R_{Ak} \oplus i_{Ak} \oplus \hat{\beta}_{k-1}$
α_k
β_k
Measure delay between β_{k-1} and $\hat{\alpha}_k$
$\beta_k \leftarrow R_{Bk} \oplus i_{Bk} \oplus \hat{\alpha}_k$
Measure delay between $\hat{\beta}_k$ and α_k
- end of distance-bounding phase -
d'_A
d'_B
$0\|\hat{R}_A \leftarrow$ open $(\hat{c}'_A, \hat{d}'_A)$
$1\|\hat{R}_A \leftarrow$ open $(\hat{c}'_B, \hat{d}'_B)$
$\hat{i}_{Bi} \leftarrow \alpha_i \oplus \hat{\beta}_i \oplus \hat{R}_{Bi}$ $(i = 1,..., k)$
Verify $i_A = \hat{i}_B$
$\hat{i}_{A1} \leftarrow \hat{\alpha}_1 \oplus \hat{R}_{A1}$
$\hat{i}_{Ai} \leftarrow \hat{\alpha}_i \oplus \beta_{i-1} \oplus \hat{R}_{Ai}$ $(i = 2,..., k)$
Verify $i_B = \hat{i}_A$
- Alice and Bob visually verify that there are no other users/devices in their 'integrity region" -

Fig. 1 Operation of DH-DB

at the beginning of $\widehat{m_B}$. If it is successful, A and B generate the verification string i_A and i_B.

In the distance-bounding step, A and B execute distance bounding by exchanging bit by bit all the bits of R_A, R_B, i_A, and i_B. Here, A and B execute XOR operation before exchange the bit. This work protects the verification string by giving dependency to exchanged bits. During distance bounding time the devices measure round-trip times between sending a bit and receiving a response bit. The device estimates the distance-bound to the other device by multiplying the round trip time by the speed of light in the case of the radio or by the speed of sound in the case of ultrasound communication.

In the verification step, A and B retrieve $\widehat{R_B}$, $\widehat{i_B}$ and $\widehat{R_A}$, $\widehat{i_A}$, respectively. Then, A and B verify $\widehat{i_B}$ and $\widehat{i_A}$ against i_A and i_B. (By the devices A and B, not users A and B) If it is successful, devices A and B display the measured distance bounds on their screens. The users A and B then visually verify that there are no other users/devices in their integrity regions. Then the users accept the exchanged DH public parameters and IDs as being authentic.

2.4 Analysis of the complexity and problems of DH-DB

We analyze the vulnerability against the MITM attack and the complexity of DH-DB protocol. Active adversary M tries to collect information exchanged between A and B. Since the existence of adversary is checked at last step in DH-DB protocol, adversary can get m_A and m_B, which contains DH public parameter in readable manners, through collected information. Therefore, this protocol is not secure in the situation where DH public parameters are frequently reused.

In the aspect of complexity, this protocol performs complicated procedures for measuring the round-trip times. It generates additional random sequence and performs XOR operation with bits used for measuring the round-trip times. We can hide the verification string from adversary and obtain security through this procedure. However, we can reduce the overhead from random generator and XOR operation by designing new commitment scheme and reordering the procedure of protocol.

Ⅲ. Improved DH-DB

3.1 New Commitment Scheme

We define commitment/opening triplet (c,b,d). Sender picks collision-free hash function whose output y is b, k-bit string. c means a universal hash function f and d means the random string x, where f and x are referred at Section Ⅱ. Since many hash functions are used as random Oracle, these hash function can ensure randomness of b[7]. String b is used as exchanged bits for measuring round-trip time in proposed protocol. Since

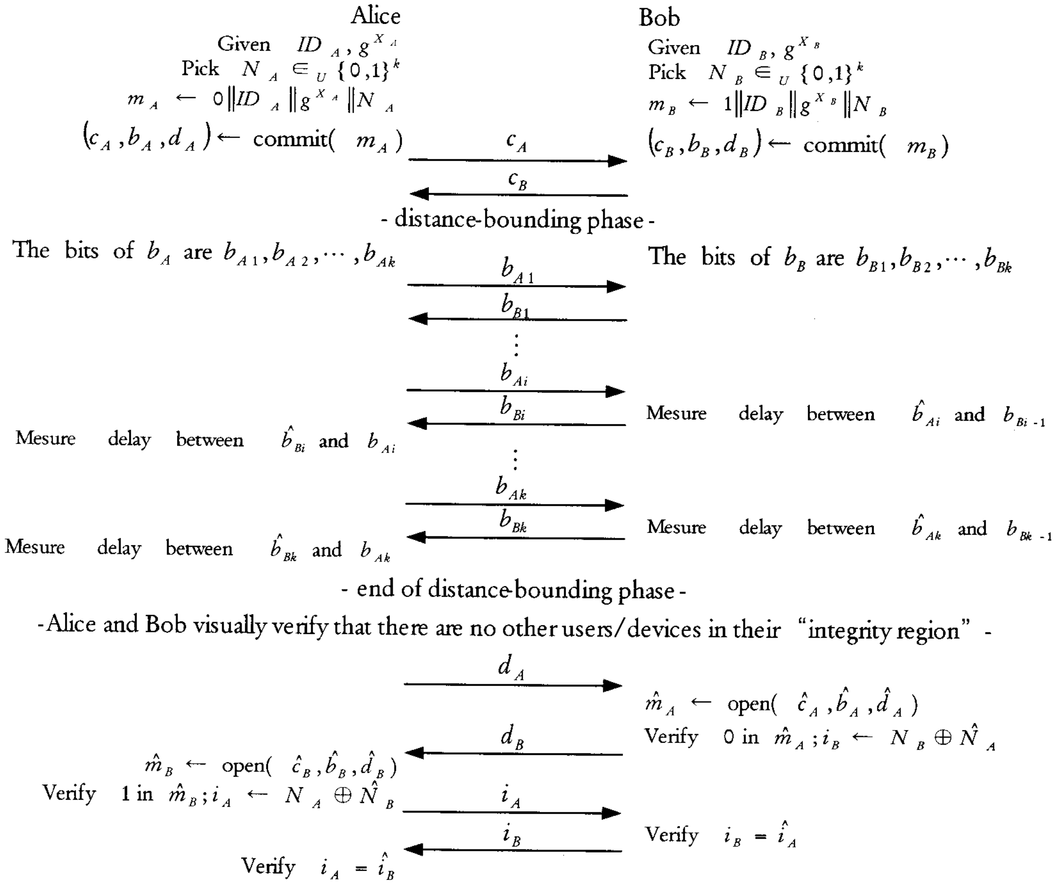

Alice
Bob
Given ID_A, g^{X_A}
Pick $N_A \in_U \{0,1\}^k$
$m_A \leftarrow 0\|ID_A\|g^{X_A}\|N_A$
$(c_A, b_A, d_A) \leftarrow$ commit(m_A)
Given ID_B, g^{X_B}
Pick $N_B \in_U \{0,1\}^k$
$m_B \leftarrow 1\|ID_B\|g^{X_B}\|N_B$
$(c_B, b_B, d_B) \leftarrow$ commit(m_B)
c_A
c_B
- distance-bounding phase -
The bits of b_A are $b_{A1}, b_{A2}, \cdots, b_{Ak}$
The bits of b_B are $b_{B1}, b_{B2}, \cdots, b_{Bk}$
b_{A1}
b_{B1}
b_{Ai}
b_{Bi}
Mesure delay between $\hat{b}_{Ai}$ and b_{Bi-1}
Mesure delay between $\hat{b}_{Bi}$ and b_{Ai}
b_{Ak}
b_{Bk}
Mesure delay between $\hat{b}_{Ak}$ and b_{Bk-1}
Mesure delay between $\hat{b}_{Bk}$ and b_{Ak}
- end of distance-bounding phase -
-Alice and Bob visually verify that there are no other users/devices in their "integrity region" -
d_A
$\hat{m}_A \leftarrow$ open($\hat{c}_A, \hat{b}_A, \hat{d}_A$)
Verify 0 in $\hat{m}_A; i_B \leftarrow N_B \oplus \hat{N}_A$
d_B
$\hat{m}_B \leftarrow$ open($\hat{c}_B, \hat{b}_B, \hat{d}_B$)
Verify 1 in $\hat{m}_B; i_A \leftarrow N_A \oplus \hat{N}_B$
i_A
i_B
Verify $i_B = \hat{i}_A$
Verify $i_A = \hat{i}_B$

Fig. 2 Operation of improved DH-DB

probabilities of 0 and 1 are equally likely, adversary can make attack at most $1/2^k$ of probability. Therefore, we can secure the integrity against the MITM attack without additional use of random generator.

3.2 Protocol Description

Fig. 2 shows proposed protocol. It is also divided into three steps: initialization, distance-bounding, and opening. The initialization step is similar to the initialization step of existing protocol. However, proposed protocol does not generate k-bit random string N_A and N_B. In the distance-bounding step A and B exchange b_A and b_B without XOR operation. Therefore, we can reduce the computational complexity. Also, since we use collision-free hash function, adversary rarely get pre-image of b_A and b_B.

It is different from existing protocol that A and B visually verify that there are no other users/devices in their integrity regions between second step and third step. Even though adversary exists in integrity regions, adversary cannot open triplet with collected information. Therefore, adversary cannot get DH public parameters. With this, we can ensure the secure reuse of DH public parameters.

In third step, A sends d_A to B and B opens commitment $\widehat{c_A}$ and examines that $\widehat{m_A}$'s first bit is 0. If it is successful, B sends d_B and A does similar procedure. After that A and B generate verification string i_A and i_B, respectively. Since we check the existence of other user before the third step, it is possible to send i_A and i_B in readable forms. Then, A and B verify $\widehat{i_B}$ and $\widehat{i_A}$ against i_A and i_B. If it is successful the users accept the exchanged DH public parameters and IDs as being authentic.

Ⅳ. Performance Analysis

In this chapter, we confirm improvement by comparing security, the number of messages exchanged, required amount of parameters, and number of operations of proposed protocol and existing protocol.

In the existing protocol, adversary can obtain m_A and m_B, even though A and B discontinue the communication. On the other hand, in the proposed protocol, adversary cannot get m_A and m_B. It means that the security of reused DH parameter depends on the powerfulness of commitment scheme.

In the aspect of the number of messages exchanged, $2k+6$ messages are exchanged in the existing protocol if the protocol is finished successfully and $2k+4$ messages are exchanged if the protocol is discontinued due to the other users in the integrity region. In proposed protocol, it also uses $2k+6$ messages when the protocol is finished successfully. However, it exchanges $2k+2$ messages when the protocol is discontinued. Therefore, two messages are reduced.

Existing protocol needs 18 parameters ID, X, g^X, N, R, c, d, α, and i of A and B. Since proposed protocol does not need R and α, 14 parameters are required.

Finally, we compare the computational complexity between two protocols. For fair comparison, we assume that two protocols use same universal hash function and collision-free hash function. Also, we count the number of XOR operation. We do not consider complexity due to memory access and table lookup. We assume that the random generator defined at ANSI X9.17[8] is used.

The random generator generates 64-bit random string by using 3-DES which uses two keys. For generating 64-bit random string, 3-DES is used twice and additional 64 XOR operations are needed for every use of 3-DES except final use. 3840 XOR (=16 [round/DES]×(32+48) [XOR/round]×3 [DES]) operations are needed for use of 3-DES. Therefore, total number of operations is as follow:

$$\begin{aligned} & 2\lceil k/64 \rceil \times 3840 + 2\lceil k/64 \rceil - 64 \\ & = 7628\lceil k/64 \rceil - 64. \end{aligned} \tag{1}$$

In the case of $k=64$, 7618 XOR operations are needed.

Table 1. Comparison between DH-DB and improved DH-DB

	DH-DB	Proposed DH-DB
Exchanged messages (success)	$2k+6$	$2k+6$
Exchanged messages (fail)	$2k+4$	$2k+2$
Required parameters	18	14
XOR operations	-	2(7628(k/64)-64) are reduced
Reusability of DH public parameters	vulnerable against MITM attack	ensured

Table 1 summarizes the comparison of two protocols. It is important to note that we improve the resistance against the MITM attack without increasing computational power or complexity.

V. Conclusion

In this paper we provide a solution to the fundamental problem of key agreement over a radio link. We improve the existing DH-DB protocol. We confirm that its resistance against the MITM attack is increased and its computational complexity and the number of required parameters is reduced. Therefore, the proposed protocol now becomes more appropriate for devices which have limited power, limited memory, and limited computational power.

참고문헌

[1] W. Diffie and M. Hellman, "New Directions in Cryptography," *IEEE Transaction on Information Theory*, 1976.

[2] S. Brands and D. Chaum, "Distance-bounding protocols," in EUROCRYPT. Heidelberg, Germany: Springer-Verlag, 1993, vol. 765, *Lecture Notes in Computer Science*, pp. 344-359.

[3] M. Cagalj, S. Capkun and J.-P. Hubaux, "Key agreement in peer-to-peer wireless networks," *Proceedings of IEEE*, Vol. 94, Issue 2, Feb. 2006.

[4] M. Cagalj and J.-P. Hubaux, "Key agreement over a radio link," EPFL-IC-ICA, Tech. Rep. IC/2004/16, Jan. 2004.

[5] J.-F. Raymond and A. Stiglic, "Security Issues in the Diffie-Hellman Key Agreement Protocol," Sep. 2000. (http://citeseer.nj.nec.com/453885.html)

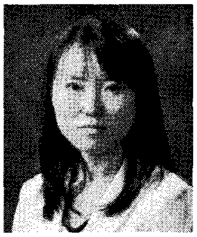
[6] S. Halevi and S. Micali, "Practical and Provably-Secure Commitment Schemes from Collision-Free Hashing," In N. Koblitz, editor, Advances in Cryptology-CRYPTO 96, pages 201-215, *Lecture Notes in Computer Science*, Springer-Verlag, 1996.

[7] M. Bellare and P. Rogaway, *Random Oracles are Practical:* A Paradigm for Designing Efficient Protocols, ACM Conference on Computer and Communications Security 1993.

[8] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC press, 1997.

[9] 박선영, 김주영, 송홍엽, "Design of improved DH (Diffie-Hellman) key agreement protocol based on distance bounding for peer-to-peer wireless networks," 2007 제 17회 통신정보 합동학술대회 (JCCI), 보광 휘닉스파크, 2007년 5월 2-4일.

박 선 영 (Sern-Young Park) 준회원



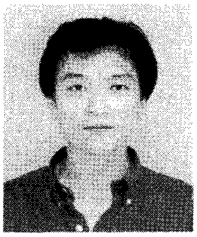
2006년 2월 연세대학교 전기전자공학과 학사

2008년 2월 연세대학교 전기전자공학과 석사

2008년 3월~현재 삼성전자 정보통신총괄

<관심분야> Cryptography, Information Theory, Error Correcting Codes

김 주 영 (Ju Young Kim) 준회원



1995년 2월 한양대학교 전자계산학과 학사

1995년~1998년 다우기술

2001년 2월 연세대학교 컴퓨터과학과 석사

2001년-현재 삼성전자 정보통신총괄, 책임연구원

2005년~현재 연세대학교 전기전자공학과 박사과정

<관심분야> Cryptography, Information Theory

송 홍 엽 (Hong-Yeop Song) 종신회원

1984년 2월 연세대학교 전자공학과 졸업

1986년 5월 USC 대학원 전자공학과 석사

1991년 12월 USC 대학원 전자공학과 박사

1992년~1993년 Post Doc., USC 전자공학과

1994년~1995년 Qualcomm Inc., 선임연구원

1995년 9월~현재 연세대학교 전기전자공학과 교수

<관심분야> PN sequences, Error Correcting Codes, Spread Spectrum Communication Systems, Stream Cipher Systems