情報保護學會論文誌
第20卷 第5號, 2010. 10

최근 제안된 두 그룹서명기법의 암호분석*

하 등 과,[1†] 김 기 태,[1] 양 대 헌,[1] 이 경 희[2‡]
[1]인하대학교, [2]수원대학교

Cryptanalysis on Two Recent Group Signature Schemes*

DengKe Ha,[1†], KiTae Kim,[1] DaeHun Nyang,[1] KyungHee Lee[2‡]

요 약

연결불가능성(unlinkability)과 추적불가능성(traceability)은 그룹서명이 만족해야 하는 기본적인 요구사항이다. 본 논문에서 최근 Lee등과 Zhu등에 의해서 제안된 두 그룹 서명기법들이 갖는 취약점을 분석하였다. Lee등의 기법은 합법적인 서명자가 생성한 서명을 검증할 수 없는 설계상의 치명적인 문제를 갖고 있으며, 검증과정이 안고 있는 문제와 별개로 동일한 서명자가 생성한 서명을 항상 링크할 수 있음을 보인다. 또, Zhu등의 그룹서명기법에서 그룹의 관리자가 추적할 수 없도록 서명을 생성하는 것이 가능함을 보이고, 저자들의 주장과 달리, 그들의 기법이 전방향 안전성을 만족하지 않음을 보인다.

ABSTRACT

Unlinkability and traceability are basic security requirements of a group signature scheme. In this paper, we analyze two recent group signature schemes, Lee et al.'s scheme and Zhu et al.'s scheme. We show that Lee et al.'s scheme does not work correctly. Further, it fails to meet unlinkability, that is, anyone who intercepts or receives group signatures are able to check if they are from the same signer. We also show that Zhu et al.'s scheme is unable to satisfy traceability, that is, a malicious group member can generate valid group signatures that cannot be opened. Moreover, once becoming group member, the malicious group member will never be revoked from group. Besides, Zhu et al.'s scheme fails to satisfy forward security, a requirement claimed by authors.

Keywords: Unlinkability, Traceability, Forward Security, Attacks, Group Signature

I. Introduction

Group signature schemes allow a group member to sign messages anonymously on behalf of the group. Moreover, in case of disputes, group authority can reveal a signer's identity. The concept of group signatures was introduced by Chaum and van Heyst [4], in which unforgeability, anonymity and traceability were noted as basic security requirements for group signature schemes. Later, more security requirements such as unlinkability, coalition resistance, exculpability, and framing have been introduced.

Informally, a secure group signature scheme must satisfy the following properties:

(1) Correctness: Signatures produced by a group member in signing phase

접수일: 2010년 4월 26일, 수정일: 2010년 7월 19일,
게재확정일: 2010년 7월 30일
* 이 논문은 인하대학교의 지원에 의하여 연구되었음.
† 주저자, dengke.he@inha.edu
‡ 교신저자, khlee@suwon.ac.kr

must be accepted in verification phase.

(2) Unforgeability: Only group members can sign messages on behalf of the group.

(3) Anonymity: Given a valid signature of a message, it is computationally hard for everyone but group authority to identify the actual signer.

(4) Unlinkability: Unless to open signatures, it is computationally hard for everyone but group authority to decide whether two different valid signatures were generated by the same group member or not.

(5) Exculpability: Neither a coalition of group members nor group authority can generate a valid signature that will be opened in the identification phase as generated from another group member.

(6) Traceability: Group authority can always open a valid signature using the identification procedure and identify the actual signer.

Following the work [4] several group signature schemes have been proposed and analyzed [1, 2, 3, 7]. Lee and Chang proposed an efficient group signature scheme based on the discrete logarithm [6]. However, their scheme does not satisfy unlikability requirement due to some deterministic information involved in signatures. Tseng and Jan [9] tried to improve Lee-Chang scheme [6], but this improvement was shown to be still linkable by Sun [8]. Though security flaws exist, Lee-Chang scheme has merits in viewpoint of efficiency, such as efficiency in computation, in communication and in storage. Recently, Lee, Chang and Hwang [5] (LCH scheme) suggested an efficient group signature scheme based on Lee-Chang scheme which was claimed to overcome all the earlier drawbacks. Another efficient group signature scheme, using an online third party called the SEM (Security Mediator), have been proposed by Zhu, Cui and Zhou [10, 11] (ZCZ scheme). The authors of [10, 11] claimed that their scheme realizes the full features of unforgeability, unlinkablility, anonymity, traceability, revocability, and forward security. Revocability indicates that group authority has the power to revoke group member. Forward security enables group member's signing key to be evolved in order to minimize the consequence of key leak-out.

In this paper, we analyze LCH scheme [5] to prove that this is not a correct group signature scheme. We also launch attacks on the schemes [5, 10, 11] to show that the schemes are not really secure group signature schemes. More precisely, we show that LCH scheme does not provide the unlinkablility because one can easily derive user specific information from signatures. Next, in ZCZ scheme [10, 11], we show that a group member can generate signatures without help of SEM so that group authorities cannot trace the signer, as well as delete the signer from group. As a result, ZCZ scheme does not satisfy traceability, revocability, and forward security.

II. Analysis of LCH scheme

2.1. Review of LCH scheme

Initiation phase.

Let p and q be two large primes such that $p|q-1$. Let g be a generator with order q in $GF(p)$. Every group member U_i chooses the secret key x_i and computes the public key $y_i = g^{x_i} \bmod p$. Let T be the group authority which has the secret key x_T and the public key $y_T = g^{x_T} \bmod p$. T chooses a random number k_i, where $\gcd(k_i, q) = 1$ and computes $r_i = g^{-k_i} y_i^{k_i} \bmod p$ and $s_i = k_i - r_i x_T \bmod q$ for each group member. Then T sends (r_i, s_i) to the group member U_i secretly. After receiving (r_i, s_i), U_i can verify the information by checking congruence relation $g^{s_i} y_T^{r_i} r_i = (g^{s_i} y_T^{r_i})^{x_i} \bmod p$.

Signing phase.

(1) Choose two random numbers w and z satisfying $\gcd(w, z) = 1$, so there must be exactly two integers e and d satisfying $ew + dz = 1$.

(2) Choose one random number a and a constant c.

(3) Compute $\{R_1, R_2, S_1, S_2, A, B\}$ as

$$R_1 = a \cdot c \cdot e \cdot w \cdot r_i \bmod p$$
$$R_2 = a \cdot c \cdot d \cdot z \cdot r_i \bmod p$$
$$S_1 = a \cdot c \cdot e \cdot w \cdot s_i \bmod q$$
$$S_2 = a \cdot c \cdot d \cdot z \cdot s_i \bmod q$$
$$A = r_i^{ac} \bmod p$$
$$B = y_T^{x_i} ac \bmod p$$

(4) Compute $\alpha_1, \alpha_2, \alpha_i$ as

$$\alpha_1 = g^{S_1} y_T^{R_1} \bmod p$$
$$\alpha_2 = g^{S_2} y_T^{R_2} \bmod p$$
$$\alpha_i = \alpha_1 \cdot \alpha_2 \bmod p$$

(5) Choose a random number $t \in Z_p^*$ and compute $R = \alpha_i^t \bmod p$. Then solves the congruence relation $h(m) = Rx_i + tS \bmod q$ for the parameter S.

The information $\{h(m), R, S, R_1, R_2, S_1, S_2, A, B\}$ is the group signature.

Verification phase.

(1) Compute $\alpha_1, \alpha_2, \alpha_i$ as

$$\alpha_1 = g^{S_1} y_T^{R_1} \bmod p$$
$$\alpha_2 = g^{S_2} y_T^{R_2} \bmod p$$
$$\alpha_i = \alpha_1 \cdot \alpha_2 \bmod p$$

(2) Compute $DH_i = \alpha_i A \bmod p$.

(3) Verify the congruence relation as follows.

$$\alpha_i^{h(m)} = R^S DH_i^R \bmod p$$

Identification phases are not listed here because our analyses are not related to this phase. Interested readers may refer to the original paper [5] for details.

2.2. Incorrectness of LCH scheme

A group signature scheme should satisfy correctness. That is, signatures produced by a group member in signing phase must be accepted in verification phase.

Suppose that a group member whose public key is y_i generated a group signature $\{h(m), R, S, R_1, R_2, S_1, S_2, A, B\}$. As authors said, in order for the signature to pass the verification test, the following equation is necessary:

$$\alpha_1 = g^{S_1} y_T^{R_1} \bmod p$$
$$= g^{S_1} g^{x_T R_1} \bmod p$$
$$= g^{acews_i} g^{x_T acewr_i} \bmod p$$
$$= g^{acew(k_i - r_i x_T)} g^{x_T acewr_i} \bmod p$$
$$= g^{acewk_i} \bmod p$$

where,

$$g^{acews_i} g^{x_T acewr_i} = g^{acews_i \bmod q} g^{x_T [acewr_i \bmod p]} \bmod p$$
$$= g^{acews_i \bmod q + x_T [acewr_i \bmod p]} \bmod p$$
$$g^{acewk_i} \bmod p = g^{acew(s_i + r_i x_T) \bmod q} \bmod p$$
$$= g^{acews_i \bmod q + x_T [acewr_i \bmod q]} \bmod p$$

If the equation $\alpha_1 = g^{acewk_i} \bmod p$ holds, then $x_T [acewr_i \bmod p]$ is equal to $x_T [acewr_i \bmod q] \bmod q$. Now since $\gcd(x_T, q) = 1$, we have $acewr_i \bmod q \equiv$ $\equiv [acewr_i \bmod p] \bmod q$.

However, this is not true. For instance, if $p = 7, q = 3, acewr_i = 10$, then $acewr_i \bmod q = 10 \bmod 3 = 1$, while $[acewr_i \bmod p] \bmod q = [10 \bmod 7] \bmod 3 = 0$.

We can conclude that group signatures generated by signing phase cannot pass the verification test due to the designing flaw of this scheme.

We do not attempt to solve the above problem in this paper. If one wants to improve LCH scheme, another problem showed in next section should also be considered.

2.3. Attack on LCH scheme

Given a group signature $h(m), R, S, R_1, R_2, \{S_1, S_2, A, B\}$, one can do the following steps:

(1) Compute $R_1 + R_2$.

$R_1 + R_2$
$= (a \cdot c \cdot e \cdot w \cdot r_i + a \cdot c \cdot d \cdot z \cdot r_i) \bmod p$
$= a \cdot c \cdot r_i (ew + dz) \bmod p$
$= a \cdot c \cdot r_i \bmod p$

(2) Compute $\gamma = (R_1 + R_2) \cdot B^{-1} \bmod p$.

$(R_1 + R_2) \cdot B^{-1} \bmod p$
$= (R_1 + R_2) \cdot (y_T^{x_i} ac)^{-1} \bmod p$
$= (acr_i) \cdot (y_T^{-x_i} (ac)^{-1}) \bmod p$
$= r_i y_T^{-x_i} \bmod p$

That is, anyone can compute such value $\gamma = r_i y_T^{-x_i} \bmod p$ from a group signature. Note that γ varies for different signers, since x_i and r_i are related to each signer U_i and group authority's public key y_T will not change for different group signatures. Therefore, one can always determine whether signatures are from the same signer or not.

III. Analysis of ZCZ scheme

3.1. Review of ZCZ scheme

Setup.

Group Manager (GM) chooses a gap Diffie-Hellman group G_1 of prime order q and a multiplicative group G_2 of the same order and a bilinear map $e: G_1 \times G_1 \rightarrow G_2$, together with an arbitrary generator $P \in G_1$, and chooses $x \in Z_q^*$ as his private key and computes $X = xP$ as his public key. Then GM makes $\{G_1, G_2, e, q, P, X, H_1, H_2\}$ as the group public message, where H_1 and H_2 are two hash functions: $H_1 : Z_q^* \rightarrow G_1$ and $H_2 : \{0,1\}^* \rightarrow Z_q^*$.

Security Mediator (SEM) chooses $s \in Z_q^*$ as his private key and computes $S = sP$ as his public key.

Join.

When a user U_i with idientifier $ID_i \in Z_q^*$ wants to join this group in time period j. GM computes $Y_i = H_1(ID_i)$ as the public key of U_i, and computes $X_i = x^{-1} Y_i$ as a signing sub-key sending to U_i secretly. User U_i can verify the correctness of X_i by $e(X, X_i) = e(P, Y_i)$.

Meanwhile SEM chooses a random number $e_i \in Z_q^*$ for user U_i, and computes $S_{i,j} = se_i^{-j} Y_i$ and $V_{ij} = e_i^j P$. Then SEM sends $(S_{i,j}, V_{i,j})$ to U_i secretly. U_i can verify the correctness of $S_{i,j}$ by $e(V_{i,j}, S_{i,j}) = e(S, Y_i)$.

After X_i and $S_{i,j}$ pass the correctness verification, user U_i becomes a group member and saves the pair $(X_i, S_{i,j})$ as his signing key for time period j.

Revoke.

There is a Certificate Revocation List (CRL) which records information of revoked group members. The item of CRL is (Y_i, t) means a group member with public key Y_i was revoked in time period t.

Evolve.

While time period evolves from j to $j+1$, group member U_i's signing key $(X_i, S_{i,j})$ will be evolved to $(X_i, S_{i,j+1})$ by SEM with equation:

$$S_{i,j+1} = e_i^{-1} S_{i,j}$$

and $S_{i,j}$ will be destroyed by U_i.

Sign.

To generate a group signature on message m in time period j, Group member U_i selects a random number $k \in Z_q^*$, computes:

$$r_1 = kY_i$$
$$\sigma = kH_2(m\|j)S_{i,j}$$
$$c = kH_2(m\|j)X_i$$

then sends (Y_i, r_1, σ, c, j) to SEM secretly. Firstly, SEM checks whether signer is a valid group member by CRL, then by equation

$$H_2(m\|j)r_1 = s^{-1}e_i^j\sigma$$

to verify whether $S_{i,j}$ was used to signature, finally computes

$$r_2 = k'P$$
$$r_3 = s^{-1}e_i r_1$$
$$r_4 = s^2P + k'(r_1 + r_3 + c)$$

$(r_1, r_2, r_3, r_4, c, j)$ is group member U_i's signature for message m in time period j.

Verify.

The correctness of a signature $(r_1, r_2, r_3, r_4, c, j)$ is verified by:

$$e(P, r_4) = e(S, S)e(r_2, r_1)e(r_2, r_3)e(r_2, c)$$
and
$$e(X, c) = e(P, H_2(m\|j)r_1)$$

Open.

In the case of a dispute, SEM has to open a signature $(r_1, r_2, r_3, r_4, c, j)$ according the saved (e_i, Y_i). If there is a e_i satisfies equation:

$$se_i^{-1}r_3 = r_1$$

then signer is Y_i.

3.2. Attack on ZCZ scheme

A malicious group member constructs specific values of (r_1, σ, c) and interacts with SEM several times to get s^2P which should be blinded in signatures. Then he can generate group signatures that cannot be opened by group authority, which means he cannot be traced. Besides, the malicious group member cannot be revoked from group and be affected by group evolution.

A malicious group member U_i can do the following steps to generate a group signature:

(1) U_i chooses a random number $k \in Z_q^*$, computes:

$$r_1 = kY_i$$
$$\sigma = kH_2(m)S_i$$
$$c = kH_2(m)X_i$$

then sends (Y_i, r_1, σ, c, j) to SEM, and gets a group signature $(r_1, r_2, r_3, r_4, c, j)$ from SEM.

Since SEM computes r_3 as:

$$r_3 = s^{-1}e_i r_1$$
$$= s^{-1}e_i kY_i$$

U_i can compute $\alpha = r_3/k = s^{-1}e_i Y_i$ as U_i knows value k.

(2) U_i chooses a random number $l \in Z_q^*$, computes:

$$r_1 = l\alpha = ls^{-1}e_i Y_i$$
$$\sigma = lH_2(m)Y_i$$
$$c = lH_2(m)X_i$$

then sends (Y_i, r_1, σ, c, j) to SEM.

SEM first verifies if $H_2(m)r_1 = s^{-1}e_i\sigma$:

$$H_2(m)r_1 = H_2(m\|j)ls^{-1}e_i Y_i$$
$$s^{-1}e_i\sigma = s^{-1}e_i lH_2(m)Y_i = H_2(m)r_1$$

r_1 pass the above test. Then a group signature $(r_1, r_2, r_3, r_4, c, j)$ is generated by SEM to U_i.

Since SEM computes r_3 as:

$$r_3 = s^{-1}e_i r_1 \\ = s^{-1}e_i(ls^{-1}e_i Y_i) \\ = s^{-2}e_i^2 l Y_i$$

U_i can compute $\beta = r_3/l = s^{-2}e_i^2 Y_i$ as U_i knows value l.

(3) U_i chooses a random number $l' \in Z_q^*$, computes:

$$r_1 = l'\alpha = l's^{-1}e_i Y_i \\ \sigma = l'H_2(m)Y_i \\ c = -l'(\alpha+\beta)$$

then sends (Y_i, r_1, σ, c, j) to SEM.

SEM first verifies if $H_2(m)r_1 = s^{-1}e_i\sigma$:

$$H_2(m)r_1 = H_2(m\|j)l's^{-1}e_i Y_i \\ s^{-1}e_i\sigma = s^{-1}e_i l' H_2(m)Y_i = H_2(m)r_1$$

r_1 pass the above test. Then a group signature $(r_1, r_2, r_3, r_4, c, j)$ is generated by SEM to U_i.

Since SEM computes r_3 as:

$$r_3 = s^{-1}e_i r_1 \\ = s^{-1}e_i(l's^{-1}e_i Y_i) \\ = s^{-2}e_i^2 l' Y_i \\ = l'\beta$$

and computes r_4 as:

$$r_4 = s^2P + k'(r_1 + r_3 + c) \\ = s^2P + k'((l'\alpha) + (l'\beta) + (-l'(\alpha+\beta))) = s^2P$$

U_i knows $r_4 = s^2P$.

Above steps should be done within time period $j=1$. Now U_i can generate a group signature of message m without the help of SEM:

$$c = kH_2(m\|j)X_i \\ r_1 = kY_i \\ r_2 = lP \\ r_3 = k'P \\ r_4 = s^2P + l(r_1 + r_3 + c)$$

where k, l, k' are random values chosen from Z_q^*.

By checking verification equations $e(P, r_4) = e(S, S)e(r_2, r_1)e(r_2, r_3)e(r_2, c)$ and $e(X, c) = e(P, H_2(m\|j)r_1)$, we can see this forged signature passes the verification phase:

$$e(P, r_4) = e(P, (s^2P + l(r_1 + r_3 + c))) \\ = e(P, s^2P)e(P, l(r_1 + r_3 + c)) \\ = e(sP, sP)e(lP, (r_1 + r_3 + c)) \\ = e(S, S)e(r_2, (r_1 + r_3 + c)) \\ = e(S, S)e(r_2, r_1)e(r_2, r_3)e(r_2, c)$$

and

$$e(X, c) = e(xP, kH_2(m\|j)X_i) \\ = e(xP, kH_2(m\|j)x^{-1}Y_i) \\ = e(P, kH_2(m\|j)Y_i) \\ = e(P, H_2(m\|j)r_1)$$

So any verifier will take this group signature $(r_1, r_2, r_3, r_4, c, j)$ on message m in time period j as a valid group signature.

Most importantly, this group signature cannot be opened. This means SEM cannot trace the actual signer U_i from the signature, which is against traceability, one essential property of group signature. The reason is that SEM verifies whether $se_i^{-1}r_3 = r_1$ to determine if the signer is Y_i or not. But the malicious user U_i in the above attack uses $r_1 = kY_i$ and $r_3 = k'P$, so the equation $se_i^{-1}r_3 = r_1$ will never hold for user U_i.

Additionally, the malicious group member U_i will never be revoked from this group. Notice that, in signing phase, SEM checks whether the signer is a valid group member or revoked one by using CRL. But the above attacker U_i can generate signatures without the help of SEM, which means SEM does not have opportunity to check whether the user is legal or revoked one. That is, U_i can always skip the CRL validation step performed by SEM and freely generate valid signatures by himself. Thus SEM cannot revoke the user U_i.

Furthermore, evolve operation has no effect on group member U_i anymore because in signing phase SEM checks whether $S_{i,j}$ was used to sign signature by equation $H_2(m\|j)r_1 = s^{-1}e_i^j\sigma$. But U_i generates signatures without the help of SEM. This violates forward security, a requirement of their scheme as authors claimed.

IV. Conclusion

In this paper, we have analyzed two recent group signature schemes, LCH scheme and ZCZ scheme. We showed that LCH scheme does not work correctly and not meet unlinkability. We presented that ZCZ scheme fails to satisfy traceability. Furthermore, ZCZ scheme is unable to meet forward security, a requirement claimed in their paper.

참 고 문 헌

[1] Giuseppe Ateniese, Jan Camenisch, Marc Joye, and Gene Tsudik, "A practical and provably secure coalition-resistant group signature scheme," Proceedings of Crypto 2000, LNCS 1880, Springer-Verlag, pp. 255-270, 2000.

[2] Giuseppe Ateniese, Dawn Song, and Gene Tsudik, "Quasi-efficient revocation of group signatures," Proceedings of Financial Cryptography 2002, pp. 183-197, Mar. 2002.

[3] M. Bellare, D. Micciancio, and B. Warinschi, "Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions," Proccedings of Eurocrypt 2003, LNCS 2656, pp. 614-629, 2003.

[4] Jan Camenisch and Anna Lysyanskaya, "Signature schemes and anonymous credentials from bilinear maps," Advances in Cryptology-CRYPTO 2004, LNCS 3152, Springer-Verlag, 2004.

[5] D. Chaum, and E.V. Heyst, "Group signatures," Advances in Cryptology-EuroCrypt91, LNCS 547, Springer-Verlag, pp. 257-265, 1991.

[6] Cheng-Chi Lee, Ting-Yi Chang, Min-Shiang Hwang, "A New Group Signature Scheme Based on the Discrete Logarithm," Journal of Information Assurance and Security, vol. 5, no. 1, pp. 054 - 057, 2010.

[7] W.B. Lee and C.C. Chang, "Efficient group signature scheme based on the discrete logarithm," IEE Proc.-Computer Digital Technology, vol. 145, no. 1, pp. 15-18, Jan. 1998.

[8] Dawn Xiaodong Song, "Practical forward secure group signature schemes," ACM Conference on Computer and Communications Security 2001, pp. 225-234, Nov. 2001.

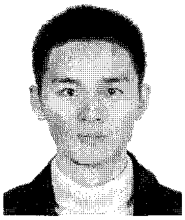
[9] Hung-Min Sun, "Comment improved group signature scheme based on discrete logarithm problem," IEE Electronics Letters, vol. 35, no. 16, pp. 1323-1324, Apr. 1999.

[10] Yuh-Min Tseng and Jinn-Ke Jan, "Improved group signature scheme based on discrete logarithm problem," IEE Electronics Letters vol. 35, no. 1, pp. 37-38, Jan. 1999.

[11] Jianhua Zhu, Guohua Cui, and Shiyang Zhou, "Two Group Signature Schemes with Multiple Strategies Based on Bilinear Pairings," I.J. Information Technology and Computer Science, vol. 1, no. 1, pp. 16-22, Nov. 2009.

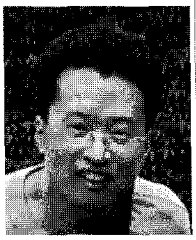
[12] Guohua Cui, Jianhua Zhu, and Shiyang Zhou, "A Group Signature Schemes with Multiple Strategies Based on Bilinear Pairings," 2009 First International Workshop on Education Technology and Computer Science, IEEE, vol. 3, pp. 848-852, Mar. 2009.

〈著者紹介〉



하 등 과 (DengKe Ha) 학생회원
2003년 6월 : Navy Submarine College 정보관리학과 졸업
2006년 6월 : 중경우전대학교 컴퓨터과학과 석사
2009년 3월~현재 : 인하대학교 정보공학과 석사과정
〈관심분야〉 정보보호, 네트워크 보안

김 기 태 (Kitae Kim) 정회원
1997년 2월 : 건양대학교 수학과 졸업
2000년 2월 : 인하대학교 수학과 석사
2009년 8월 : 인하대학교 수학과 박사
2009년 9월~현재 : 인하대학교 정보통신대학원 박사 후 연구원
〈관심분야〉 전자서명, 암호분석, 대수적 정수론



양 대 헌 (DaeHun Nyang) 종신회원
1994년 2월 : 한국과학기술원 과학기술대학 전기·전자공학/컴퓨터공학과 졸업
1996년 2월 : 연세대학교 컴퓨터과학과 석사
2000년 8월 : 연세대학교 컴퓨터과학과 박사
2000년 9월~2003년 2월 : 한국전자통신연구원 정보보호연구본부 선임연구원
2003년 2월~현재 : 인하대학교 컴퓨터정보공학부 부교수
〈관심분야〉 암호 이론, 암호 프로토콜, 인증 프로토콜

이 경 희 (KyungHee Lee) 정회원
1993년 2월: 연세대학교 컴퓨터과학과 학사
1998년 8월: 연세대학교 컴퓨터과학과 석사
2004년 2월: 연세대학교 컴퓨터과학과 박사
1993년 1월~1996년 5월: LG소프트(주) 연구원
2000년 12월~2005년 2월: 한국전자통신연구원 선임연구원
2005년 3월~현재: 수원대학교 전기공학과 조교수
〈관심분야〉바이오인식, 정보보호, 컴퓨터비전, 인공지능, 패턴인식