情報保護學會論文誌
第13券 第6號, 2003. 12

WISA 2002에 제안된 무선 전자 지불 시스템의 안전성

한 대 완*†, 이 동 훈*‡, 황 상 철**, 류 재 철**

On the Security of a Mobile Payment System Proposed at WISA 2002

Daewan Han*†, Dong Hoon Lee*‡, Sang Cheol Hwang**, Jae-Cheol Ryou**

요 약

WISA 2002에서 함우석 등은 무선 환경에 적합한 단방향 지불 시스템을 제안하였고, 제안 시스템의 전자 화폐가 모듈러 멱승과 같은 공개키 연산 없이 위조 불가능성과 이중 사용 방지의 특성을 지닌다고 주장하였다. 본 논문에서는 제안된 전자 화폐가 제안자들의 주장과는 달리 실제로는 구매 내역의 위조가 가능함을 보임으로써, 올바른 서명이 없이는 다양한 공격이 가능함을 보인다.

ABSTRACT

In WISA 2002, Ham *et al.* proposed a one-way mobile payment system. They claimed that the electronic cash of the system satisfies unforgeability and double spending prevention. In this paper, we point out that their system is not secure as they claimed by showing that the forgery of payment scripts is possible.

keyword : *Electronic cash, Payment protocol*

Ⅰ. 서 론

전자 상거래는 인터넷을 매개로 재화나 서비스를 구매/판매하는 행위를 포함한 일반적인 상거래를 의미한다. 전자 화폐(전자 현금)는 전자 상거래의 과정에서 실 화폐와 같은 역할을 하는 것을 의미하는데, 그 특성상 실 화폐를 전자적(0, 1의 나열)으로 표현한 것에 불과하므로, 쉽게 복사가 가능할 뿐만 아니라 진품과 복사품을 구별할 수 없기 때문에 재사용이 가능하다. 따라서 전자 화폐가 선불 방식일 경우에는 반드시 사용자의 이중 사용(double spending) 방지나 초과 사용(overspending) 방지를 위한 구조가 반드시 포함되어야 한다.

그 밖에도 전자 화폐가 만족시켜야하는 성질로 다음과 같은 것들이 있다.

- 익명성(anonymity)
- 추적 불가능성(untraceability)
- 위조 불가능성(unforgeability)

전자 화폐의 용도가 다양해지면서 위의 성질 이외에도 분할성, 양도성, 연결 불가능성, 익명성 취소 등 다양한 성질을 가지는 전자 화폐가 연구되고 있다. 전자 화폐의 이론적인 출발은 Chaum에 의하여 오프라인 지불이 가능한 추적 불가능한 전자 화폐가 발표되면서 시작되었다.[1,2] 그 후 다양한 성질을 가지

* 한국전자통신연구원 부설 국가보안기술연구소({dwh,dlee}@etri.re.kr
** 충남대학교 공과대학 정보통신공학부 컴퓨터공학과({schwang,jcryou}@cnu.ac.kr)
† 주저자, ‡ 교신저자, 논문접수일 : 2003년 8월 4일, 심사완료일 : 2003년 10월 15일

는 전자 화폐들이 Ferguson, Okamoto, Brands 등에 의하여 발표되었다.[3~6]

대부분의 전자 화폐는 일반적인 PC처럼 유선망에 의하여 각 상거래 주체(고객, 상점, 은행 등)들이 연결되어 충분한 정도의 계산 능력과 데이터 전송 능력을 가지고 있다고 가정하고 있어서, 기존의 결과를 무선 통신 환경에 그대로 적용하기 어렵다. 즉, 계산 능력과 통신량에서 제한을 받을 수밖에 없는 무선 장비에서 상거래(mobile commerce)가 점차 증가하면서, 안전성이나 성능 측면에서 여러 가지 문제를 야기하고 있다. 따라서 무선 상거래에서는 전자 화폐의 요구 조건의 일부를 희생하더라도 간단한 프로토콜을 설계하는 것이 필요하다.

최근 WISA 2002에서 함우석 등은 무선 환경에 알맞도록 단 방향 통신을 하면서 고객은 매우 적은 양의 계산량만을 필요로 하는 지불 시스템을 제안하였다.[7] 이 시스템의 전자 화폐는 위조 불가능성과 이중 사용 방지의 성질을 가진다고 제안자들은 주장하고 있다.

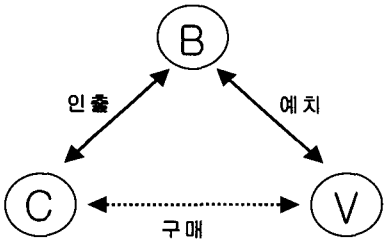
그러나 제안된 방식의 구매 프로토콜이 너무 간단하기 때문에 충분한 인증기능을 수행하지 못함을 본 논문에서 보인다. 즉, 도청자나 악의적인 상점은 고객의 개인키의 일부를 알아냄으로써 합법적인 구매 내역을 위조할 수 있어서 전자 화폐를 부정 사용할 수 있다. 따라서 구매 프로토콜에서는 반드시 위조 불가능성을 만족할 수 있도록, 고객의 서명(공개키 연산)이 포함되어야 한다고 결론 내릴 수 있다.

본 논문의 2장과 3장에서는 전자 지불 시스템의 모델과 WISA 2002에서 제안된 시스템을 기술하고 4장에서 안전성 분석 및 공격 시나리오를 예시한 뒤, 마지막 5장에서 결론을 맺는다.

II. 무선 전자 지불 시스템의 모델

전자 지불 시스템은 다양한 모델이 존재하지만, 본 논문에서는 함우석 등이 설정한 모델을 그대로 따르도록 한다. 전자 상거래는 3종류의 주체(고객(C), 상점(V), 은행(B))가 관여하며, 인출, 구매, 예치 프로토콜로 이루어진다.

- 인출 (고객 <-> 은행): 고객의 예금 인출 요구에 대하여 은행은 고객의 인증을 거쳐 전자 화폐를 발행한다.
- 구매 (고객 <-> 상점): 발행된 전자 화폐를 사용하여 필요한 재화를 상점으로부터 구매한다.
- 예치 (상점 <-> 은행): 상점은 판매 후 저장된 구매 내역을 은행에 전송하여 실제 화폐로 재 입금 받는다.



[그림 1] 전자 지불 시스템의 모델

이때, 인출, 예치 프로토콜의 경우는 유선망을 통해 이루어지는 반면, 구매 프로토콜은 무선망을 통해 이루어지므로 외부의 도청 등의 공격의 위협이 높다. 구매는 **오프라인 지불 시스템**으로 이루어지는 것을 가정한다. 즉, 고객이 구매 프로토콜 과정에서는 은행과의 직접적인 통신이 없음을 가정한다. 온라인 지불 시스템의 경우 전자 화폐의 부정사용을 어렵지 않게 탐지/방지할 수 있다.

무선 환경을 위한 전자 화폐는 최소의 요구조건으로 다음을 만족시키도록 한다.

- 위조 불가능성
- 이중 사용 방지
- 효율성

III. WISA 2002에서 제안된 지불 시스템

3.1 기호 정의

다음과 같은 기호를 사용한다.

- C, V, B: 각각 고객, 상점, 은행을 나타낸다.
- p, q: p와 q는 소수로 q는 p-1을 나눈다.
- Z_p^*: 모듈러 p로의 곱셈군.
- G_q: Z_p^*의 위수가 q인 부분군.
- g: G_q의 생성원.
- [2, q-1]: 2와 q-1사이의 정수 집합.
- $r \in_R$[2, q-1]: r은 [2, q-1]에서 임의로 선택되는 것을 나타냄.
- a^{-1}: Z_p^*에서의 a의 역원.

■ ‖: 두개의 비트열의 연접.
■ $H:\{0,1\}^* \rightarrow \{0,1\}^l$ ($l >= 160$): 충돌 회피성을 가지는 일방향 해쉬 함수.
■ SK_{ID}, PK_{ID}: ID를 식별자로 가지는 객체의 개인키와 공개키.

프로토콜에서 덧셈과 곱셈은 g의 지수부분에 나타나므로 mod q 연산으로 수행되고, 멱승은 Z_p^*의 원소로 나타나므로 mod p 연산으로 수행된다.

3.2 키의 생성과 해쉬 체인

WISA 2002에서 제안된 프로토콜에서 각 고객은 2개의 개인키/공개키의 쌍 $(x_i; y_i(=g^{x_i}))$ $(i=1,2)$을 가지며 공개키는 공개한다. 이들에 대한 생성 및 분배는 일반적인 공개키 암호와 동일하다.

추가적으로 다음과 같은 비밀 정보를 포함한 해쉬 체인을 정의한다. k를 비밀 정보라고 하고, $KH_0 = k$라고 한다. 그러면 KH_i를 다음과 같이 순차적으로 정의한다.

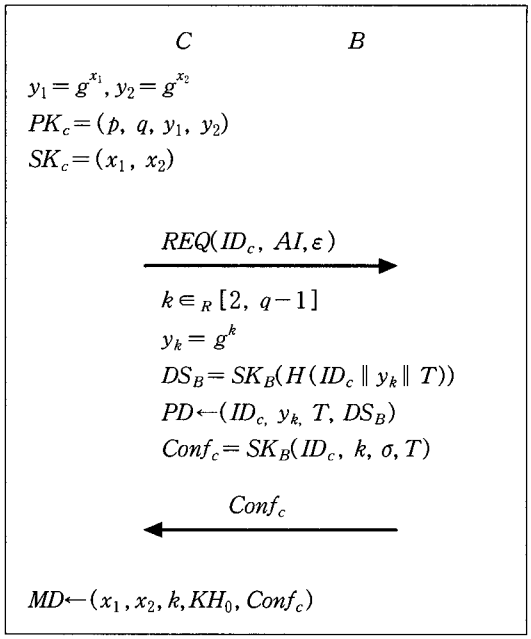
$$KH_i = H(k \| KH_{i-1}), j = 1, \cdots, l$$

3.3 프로토콜

3.3.1 인출 프로토콜

고객은 은행으로부터 σ_0원을 다음과 같은 절차를 거쳐서 인출한다.

■ 고객은 먼저 자신의 신원 ID_C, 계좌 정보 AI 및 계좌와 신원을 증명해 줄 추가적인 정보 ε을 은행에게 전달하는 것으로 인출 요청을 한다.
■ 은행은 $[2, q-1]$에서 임의로 k를 선택한 후 $y_k = g^k$를 계산한다.
■ 은행은 ID_C, y_k와 k의 유효기간 T를 공개적인 장소 PD에 게시한다. 이 때, 게시하는 데이터 ID_C, y_k, T의 무결성을 은행의 개인키 SK_B를 이용한 서명값 DS_B를 같이 게시한다.
■ 은행은 인출금의 한계 σ_0를 설정한 후, 영수증 $Conf_C = SK_B(ID_C, k, \sigma_0, T)$를 생성한 후 안전한 경로를 통하여 고객에게 전달한다.
■ 고객은 $Conf_C$를 은행의 공개키를 이용하여 복호화하여 k, σ_0, T를 확인하고, 이동 단말기 MD에 자신의 개인키 x_1, x_2, 은행으로부터 받은 k 및 $Conf_C$, 초기 해쉬 체인 값 KH_0를 안전한 방법으로 저장한다.



〔그림 2〕 인출 프로토콜

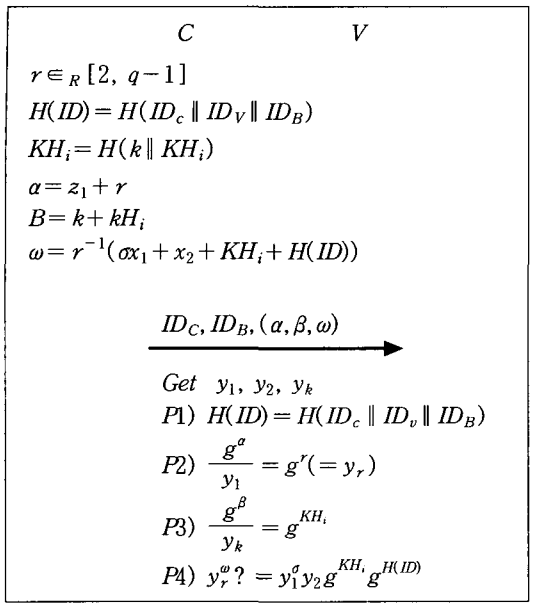
고객과 은행은 다음 상황이 발생할 때마다 인출 프로토콜을 다시 수행한다.

- k의 유효기간이 지나거나 값이 노출되었을 때
- 지불금의 합이 σ_0를 초과하였을 때
- 은행의 공개키쌍이 다시 생성될 때

3.3.2 구매 프로토콜

인출한 전자 화폐는 여러 번 분할되어 사용되며, 다음 그림은 i번째 구매를 의미한다. 고객은 가격이 σ원인 재화에 대한 구매를 다음과 같이 수행한다.

■ 고객은 $[2, q-1]$에서 임의로 r을 선택한다.
■ 고객, 상점, 은행의 신원 정보를 차례로 연결한 후 해쉬한 값 $H(ID)$와 i번째 해쉬 체인값 KH_i, 그리고 α, β, ω를 [그림 3]에서와 같이 계산한다.
■ ID_C, ID_B와 (α, β, ω)를 상점에게 전송한다.
■ 상점은 공개키 저장소로부터 y_1, y_2를, PD로부터 y_k를 가져온 후, 다음과 같이 지불 프로토콜 P1~P4를 수행한다.



〔그림 3〕 구매 프로토콜

- P1 : 고객으로부터 전송받은 ID_C, ID_B와 자신의 신원정보 ID_V를 이용하여 $H(ID)$를 계산한다.
- P2 : α와 y_1으로부터 g^r을 구한다.
- P3 : β와 y_k로부터 g^{KH_i}를 구한다.
- P4 : $y_r^{\omega} = y_1^{\sigma} y_2 g^{KH_i} g^{H(ID)}$의 관계식이 성립하는지 검증한다.

P4의 검증을 통과하면 ID_C와 g^{KH_i}를 k의 유효 기간동안 저장한다. 이미 저장된 값들 중에서 g^{KH_i}와 같은 값이 있으면 이중 사용된 것으로 간주하고 거래를 중단한다.

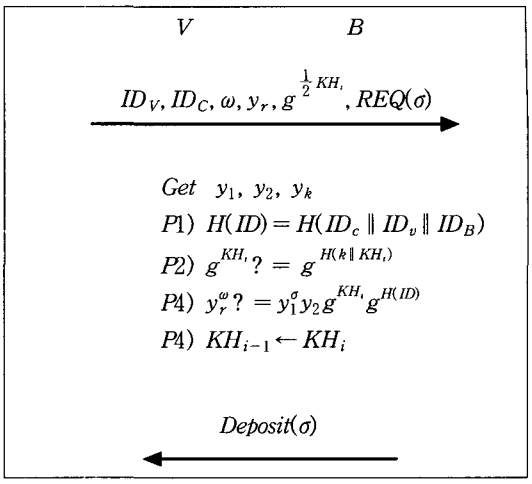
P4가 올바른 지불에 대한 검증이 되는 이유 및 기타 관련 사항에 대해서는 참고문헌 [7]을 참고하기 바란다.

3.3.3 예치 프로토콜

상점은 구매 프로토콜 과정에서 저장된 정보를 추후 은행에 전송하여 인증을 거친 뒤에 σ원을 그림 4의 R1~R4의 과정을 거쳐 예치한다. 각 과정에서 나오는 수식들의 의미는 구매 프로토콜에서의 설명과 비슷하므로 자세한 내용은 생략한다.

Ⅳ. 제안된 스킴의 분석 및 공격

본 장에서는 제안된 스킴이 위조 불가능성을 주지



〔그림 4〕 예치 프로토콜

못한다는 것을 보인다. 즉, 공격자는 고객의 개인키 중의 x_1을 계산할 수 있다. 공격자는 또한 x_1을 이용하여 정당한 구매 내역을 위조할 수 있고, 따라서 고객의 명의를 사용하여 구매 프로토콜을 수행할 수 있다. 공격은 다음의 가정을 바탕으로 한다.

[가정 1] 공격자는 고객과 임의의 상점 사이에서 이루어진 같은 k로 발급된 화폐를 사용한 구매 프로토콜의 내역 중에서 2개를 알고 있다.
[가정 2] 공격자는 구매 내역 내의 $H(ID)$를 알고 있다.
[가정 3] 공격자는 구매 대상의 가격 정보 σ를 알고 있다.

위의 [가정 1]과 [가정 2]는 구매 프로토콜이 무선으로 이루어지므로 자연스러운 가정이다. [가정 3]의 경우 프로토콜 내에서 직접적으로 가격정보가 드러나 있지 않지만, 일반적인 경우 알려져 있다고 가정해도 큰 무리가 없다. 적어도 공격자가 상점이라면 모든 정보를 알 수 있다.

4.1 개인키 X_i의 추출

공격자는 가정에 따라서 서로 다른 구매 내역인 (α, β, ω)와 $(\alpha', \beta', \omega')$을 알고 있다. 각각은 같은 상점에서의 구매 내역일 필요는 없다. 그러면 프로토콜에 의해 다음의 식이 성립한다.

$$\alpha = x_1 + r \tag{1}$$

$$\beta = k + KH_i \quad (2)$$

$$\omega = r^{-1}(\sigma x_1 + x_2 + KH_i + H(ID_i)) \quad (3)$$

$$\alpha' = x_1 + r' \quad (4)$$

$$\beta' = k + KH_j \quad (5)$$

$$\omega' = r'^{-1}(\sigma' x_1 + x_2 + KH_j + H(ID_j)) \quad (6)$$

식(1)과 (3)으로부터 다음을 계산할 수 있다.

$$\alpha\omega = (\sigma + \omega)x_1 + x_2 + KH_i + H(ID_i)$$

마찬가지로 식(4)와 (6)으로부터 다음을 계산할 수 있다.

$$\alpha'\omega' = (\sigma' + \omega')x_1 + x_2 + KH_j + H(ID_j)$$

$KH_i - KH_j = \beta - \beta'$ 이므로 두 식을 서로 빼면 다음이 성립한다.

$$(\sigma - \sigma' + \omega - \omega')x_1 = (\alpha\omega - \alpha'\omega') - (\beta - \beta') - (H(ID_i) - H(ID_j))$$

공격자가 가격 정보를 모두 알고 있다면, 위 식에서 x_1을 제외한 모든 값들은 이미 알려진 값들이고, $(\sigma - \sigma' + \omega - \omega')$가 0일 확률은 매우 적으므로 위 식에서 고객의 개인키의 일부인 x_1을 구할 수 있다.

4.2 구매 내역의 위조

공격자가 x_1을 알고 있으면 (α, β, ω)으로부터 유효한 $(\alpha'', \beta'', \omega'')$을 생성하여 임의의 상점과 구매 프로토콜을 수행하여 고객 C인 것처럼 행동할 수 있다.

식(1)에서 r을 구할 수 있고, 따라서 식(3)에서

$$x_2 + KH_i$$

를 구할 수 있다. 그러면 새로운 상점 V''에 대하여 다음과 같이 $(\alpha'', \beta'', \omega'')$을 계산한다.

$$ID'' = ID_C \| ID_{V''} \| ID_B$$

$$\alpha'' = \alpha$$

$$\beta'' = \beta$$

$$\omega'' = r^{-1}(\sigma'' x_1 + (x_2 + KH_i) + H(ID''))$$

그러면 $(ID_C, ID_B, (\alpha'', \beta'', \omega''))$는 다음과 같이 [P1]~[P4]를 통과하므로 상점 V''에게 올바른 구매 내역으로 인증 받을 수 있다.

[P1] $H(ID'') = H(ID_C \| ID_{V''} \| ID_B)$

[P2] $g^{\alpha''}/y_1 = g^r$

[P3] $g^{\beta''}/y_k = g^{KH_i}$

[P4] $y_r^{\omega''} ? = y_1^{\sigma''} y_2 g^{KH_i} g^{H(ID'')}$

4.3 공격 시나리오

4.3.1 초과 사용

제안된 프로토콜에서는 σ_0원의 화폐를 발급받은 뒤에 구매과정에서 σ원의 재화를 구매할 수 있도록 하였다. 즉, 제안된 전자 화폐는 분할성을 함축적으로 가지고 있다고 볼 수 있다.

그러나 구매 과정에서 σ_0에 대한 인증을 하지 않을 뿐만 아니라 현재 잔액에 대한 정보를 확인하지 않는다. 따라서 고객이 고의적으로 σ를 현재 잔액보다 크도록 구매 프로토콜을 수행할 지라도 상점을 이것을 확인할 방법이 없다. 즉, 초과 사용 방지 기능이 없다.

4.3.2 제 삼자의 화폐 위조

구매 프로토콜을 무선으로 전송되므로 쉽게 전송 내용을 도청할 수 있다. 이 경우 제 삼자도 구매 액수 (σ, σ')을 알 수 있다고 가정한다. 따라서 4.1, 4.2절의 방법으로 공격자는 고객 C의 구매내역 (α, β, ω)와 $(\alpha', \beta', \omega')$를 도청하고 $(\alpha'', \beta'', \omega'')$를 생성할 수 있으므로 상점 V''에게 자신이 고객 C임을 가장하여 구매 프로토콜을 수행할 수 있다. 이 경우 σ''은 잔액에 대한 인증이 없으므로 임의의 액수로 설정할 수 있다.

상점이 위조된 $(\alpha'', \beta'', \omega'')$를 사용하여 예치 프로토콜을 수행할 때, 이미 (α, β, ω)에 의한 예치 프로토콜이 수행되었다면 g^{KH_i}가 중복 제출되어, 은행은 사용자가 이중 사용을 했다고 판단하게 된다.

4.3.3 상점의 공모

상점은 [가정 1]~[가정 3]이 당연히 성립한다. 따라서 같은 화폐가 사용된 상점 2개 이상이 공모하게 되면 4.1, 4.2절의 방법으로 공모한 상점은 고객의 개인키 x_1과 함께 유효한 구매 내역을 생성할 수 있다. 이때 구매 액수만 크게 한 구매 내역을 생성하고 원래의 구매 내역은 버린다. 그러면 예치 프로토콜에서는 사용자는 σ원을 사용했지만, 상점은 $\sigma'(>\sigma)$원을 사용하였다고 주장할 수 있다.

V. 결 론

지금까지 WISA 2002에서 함우석 등이 제안한 무선 환경에서의 단 방향 지불 시스템에 대하여 살펴보고, 제안자들의 주장과는 달리 개인키의 노출과 화폐의 위조 등의 가능함을 보였다.

제안자들은 무선 환경임을 감안하여 구매 프로토콜에서 무거운 멱승과 같은 공개키 연산을 피하고 간단한 곱셈과 역원으로 설계하려고 하였으나, 이로부터 쉽게 개인키의 일부가 노출되는 약점이 발생하였다. 또한 잔액이나 총액에 대한 인증기능이 없다면, 앞서 기술한 바와 같이 다양한 공격이 가능하므로 전자 화폐에 대한 서명이 반드시 포함되어야 한다. 따라서 구매 과정에서 고객의 서명과 같은 공개키 연산은 필수적이라고 판단된다.

그리고 제안자들이 제시한 것과 같이 구매 과정에서 발행된 화폐를 임의로 분할하고자 할 때는 초과사용을 막기 위하여 이전의 구매 내역이나 사용 액수에 대한 인증이 필수적이라고 판단된다.

참 고 문 헌

[1] D. Chaum, Blind signature for untraceable payment, *Advances in Cryptology - CRYPTO'82*, Springer-Verlag, pp.199~203, 1983.

[2] D. Chaum, A. Fiat, and M. Naor, Untraceable electronic cash, *Advances in Cryptology - CRYPTO'88*, LNCS 403, Springer-Verlag, pp.319 - 327, 1990.

[3] T. Okamoto and K. Ohta, Universal electronic cash, *Advances in Cryptology - CRYPTO'91*, LNCS 576, Springer-Verlag, pp.324~337, 1992.

[4] N. Ferguson, Single term off-line coins, *Advances in Cryptology - Eurocrypt'93*, LNCS 765, Springer-Verlag, pp.318~328, 1994.

[5] S. Brands, Untraceable off-line cash in wallets with observer, *Advances in Cryptology - CRYPTO'93*, LNCS 773, Springer-Verlag, pp.302~318, 1994.

[6] T. Okamoto, An efficient divisible electronic cash scheme, *Advances in Cryptology - CRYPTO'95*, LNCS 963, Springer-Verlag, pp.438~451, 1995.

[7] W. Ham, H. Choi, Y. Xie, M. Lee, and K. Kim, Secure one-way mobile payment system keeping low computation in mobile devices, The 3rd Workshop on Information Security Applications (WISA 2002), pp.287~301, 2002.

〈著者紹介〉

한 대 완 (Daewan Han) 정회원
1995년 2월 : 서울대학교 수학과 학사
1997년 2월 : 서울대학교 수학과 석사
2001년 3월~현재 : 국가보안기술연구소 연구원
2003년 9월~현재 : 서울대학교 수학과 박사과정
<관심분야> 공개키 암호, 암호의 응용

이 동 훈 (Dong Hoon Lee) 정회원
1994년 2월 : 서울대학교 수학교육과 학사
1996년 2월 : 한국과학기술원 수학과 석사
2000년 2월 : 한국과학기술원 수학과 박사
2000년 2월~2002년 3월 : (주)퓨쳐시스템 선임 연구원
2002년 4월~현재 : 국가보안기술연구소 선임연구원
<관심분야> 응용 정수론, 암호론, 인터넷 보안

황 상 철 (Sang Cheol Hwang)
1989년 3월 : 숭실대학교 전자공학과 학사
1994년 3월~1996년 8월 : 숭실대학교 전자 및 컴퓨터공학과 석사
2002년 9월~현재 : 충남대학교 컴퓨터공학과 박사 과정
<관심분야> 인터넷 보안, 전자 상거래, 응용 프로토콜

류 재 철 (Jae-Cheol Ryou) 정회원
1985년 2월 : 한양대학교 산업공학과 학사
1988년 5월 : Iowa State Univ. 전산학 석사
1990년 12월 : Northwestern Univ. 전산학 박사
1991년 2월~현재 : 충남대학교 정보통신공학부 교수
<관심분야> 인터넷 보안, PKI, 스마트카드 보안