情 報 保 護 學 會 誌
第 13 券 第 4 號, 2003. 8

부정사용 방지를 위한 익명성 제어 전자지불시스템 동향 분석

강 성 우*, 박 해 룡*, 심 경 아*

요 약

본 논문에서는 1982년 D.Chaum에 의해서 개발된 은닉서명 기법을 이용한 전자화폐로부터 최근에 개발된 전자지불시스템의 기술 동향을 살펴본다. 개인의 프라이버시를 제공하기 위하여 지나친 익명성을 보장하면, 강탈, 돈세탁 등과 같은 부정적인 사용을 할 수 있으므로 신뢰기관을 연계시킴으로써, 부정 사용시 익명성을 제어할 수 있는 전자화폐시스템이 개발되었다. 또한, 이러한 신뢰기관의 익명성 제어를 위해 전자거래상에서 많은 간섭이 있다면, 직권남용을 통하여 잘못 사용될 수 있다는 점도 고려하여야 한다. 이러한 전자지불시스템에서 발생 가능한 문제점과 이를 개선하기 위한 전자지불시스템의 개발 동향을 살펴보기로 한다.

Ⅰ. 서 론

최근에 전자거래의 활성화로 인하여, 네트워크로 전달되는 전자 정보를 이용한 전자지불시스템의 사용이 급속도로 증가하고 있다. 이러한 전자정보를 이용하는 전자거래에서 가장 핵심적인 기술인 전자지불시스템의 사용은 필수적인 요소이다. 전자지불시스템은 크게 은행에서 계좌개설(opening account), 은행으로부터의 인출(withdrawal), 상점에서 일어나는 지불(payment) 프로토콜로 구성된다. 그리고 전자지불시스템의 거래시 은행이 관여하느냐 하지 않느냐에 따라 온라인 혹은 오프라인으로 구분된다.

전자지불시스템에서 익명성(anonymity) 기능은 매우 중요한 요소로 작용한다. 익명성은 은행과 상점이 담합한다하더라도 사용자를 추적할 수 없어야 한다는 사용자의 프라버시(privacy)를 제공하는 기본적인 개념이다. 이러한 특성은 현재 사용되고 있는 현금(지폐, 동전)에서의 중요 기능중의 하나이다. 그러나, 지나치게 익명성이 제공된다면, 자칫 강탈(blackmailing), 돈세탁(money laundry) 등과 같은 부정적인 범죄로 악용될 가능성이 있다[21]. 따라서 부정사용 방지를 위하여 신뢰할 수 있는 기관(e.g. Trustee)을 통하여 필요시 익명성이 제어되어야(revocable) 한다.

일반적으로 익명성 보장과 제어 기능을 갖는 전자지불시스템을 "fair" 전자지불시스템이라 한다[3,22]. 이것은 범죄 행위 방지와 익명성을 동등하게 제공한다는 의미에서 fair 라는 용어를 사용한다. 본 논문에서는 온라인 혹은 오프라인 상에서 익명성을 제어할 수 있는 전자지불시스템의 기술 동향에 대해 논하고자 한다.

본 논문의 구성은 다음과 같이 구성되었다. 2장에서는 전자지불시스템에서의 일반적인 요구사항들을 살펴본다. 3장에서는 사용자의 프라이버시를 보장하기 위해 사용되는 익명성 기능을 갖는 전자지불시스템과 지나친 익명성 제공에 따른 부정사용 방지를 위한 익명성 제어 기능을 갖는 전자지불시스템 기술 개발 동향에 대해 살펴보기로 한다.

Ⅱ. 전자화폐의 일반적인 요구사항

전자지불시스템은 일반적으로 사용자, 은행, 상점 등을 비롯하여 문제 발생시 관여하는 신뢰기관, 인증기관, 그리고 전자지불시스템에서 위협요소인 공

* 한국정보보호진흥원 암호인증기술팀({swkang, hrpark, kashim}@kisa.or.kr,)

〔표 1〕 전자화폐 요구사항

구분	요구사항	설명
안전성	위조불가능성(Unforgeability)	단지 인가된 객체만이 유효한 전자화폐를 발행한다.
	추적불가능성(Untraceability)	전자화폐와 사용자 사이의 관계를 추적할 수 없어야 한다.
	비연계성(Unlinkability)	동일한 사용자에 의해서 사용된 서로 다른 전자화폐는 연계할 수 없다는 것으로써, 일반적으로 익명성보다 강력한 요구조건이다.
	모함 방지(No framing)	사용자나 상점은 은행이나 신뢰기관에 의한 모함이 불가능해야한다.
	이중사용 방지 (double-spending prevention)	사용자가 사용한 전자화폐를 다시 사용하지 못하도록 해야한다.
	범죄 방지(Crime prevention)	익명성 제어는 간접적이라 하더라도 보호되는 것보다 더 많은 범죄(강탈, 돈세탁 등)에 대한 동기 부여를 해서는 안된다.
	권력남용 방지(No overhead power)	신뢰기관은 필요시 추적할 수 있는 권한 외에는 어떠한 행위를 해서는 안된다.
	익명성 제어(Revocability)	부정 사용할 경우 사용자의 신원에 대한 익명성을 보장해주지 않는다.
기능성	분할성(Divisibility)	전자화폐는 주어진 화폐단위보다 더 작은 단위의 금액으로 나누어진다.
	양도성(Transferability)	한번 인출된 전자화폐를 다른 사용자에게 양도할 수 있다.

격자로 구성되어 있다. 흔히, 공격자는 blackmailer, kidnappers, robbers 등으로 통용되고 있다. 이러한 공격자들에 의해 전자지불시스템은 항시 공격 가능성에 노출되어 있다. 그래서, 이러한 부정적인 공격에 대한 내성을 갖도록 전자지불시스템은 설계되어야 한다.

또한, 전자지불시스템에서는 디지털화된 정보를 통해 이루어지기 때문에 다양한 위협요소들을 고려해야한다. 이러한 관점에서 〔표 1〕은 전자지불시스템은 안전성 측면과 기능성 측면에 대한 기본적인 요구사항을 말하고 있다.

Ⅲ. 부정사용 방지를 위해 익명성 제어 기능을 갖는 전자지불시스템

1. 익명성을 보장하는 전자지불시스템

익명성 기능을 갖는 전자지불시스템의 개발은 1982년 D.Chaum에 의해서 제안된 은닉서명 기법이 소개된 이후로 다양한 방식으로 개발되기 시작했다[5]. 이러한 방식은 사용자가 돈을 인출할 때, 은행이 사용자의 정보를 은닉서명 함으로써 화폐에 대한 정보를 알지 못하게 하여 익명성과 비연계성 같은 기능을 제공하도록 하고 있다.

이러한 D.Chaum의 익명성 전자화폐에 기반한 첫 번째 전자지불시스템은 온라인 상에서 처리 되도록 개발되었다[8,4]. 그러나, 효율적인 측면을 고려하여 cut-and-choose 방식을 통한 오프라인 시스템이 개발되었다[9,20,15]. 1993년에는 효율성을 더욱 증가시키기 위해 cut-and-choose 방식을 사용하지 않고 사용자의 익명성을 제공하는 새로운 시스템이 제안되었다[2,14].

또한, 은행이 많은 양의 데이터베이스를 관리해야 한다는 문제점을 갖고 있어 데이터베이스의 크기를 상당히 줄일 수 있는 실질적인 익명성을 제공하는 전자지불시스템이 개발되었다[11].

2. 익명성을 제어하는 전자지불시스템

본 절에서는 전자지불시스템의 일반적으로 발생되는 범죄를 방지하기 위해 익명성을 제어할 수 있는 전자지불시스템의 개발 현황 및 특성에 대해 논하고자 한다.

전자지불시스템에서 지나친 익명성을 제공함으로써, 발생되는 다양한 부정적인 문제점들을 살펴보기로 한다. 전자지불시스템에서는 이중 사용과 같은 부작용이 쉽게 발생할 수 있다. 온라인에서는 미리 예금된 기록을 체크하면서 이중 사용을 방지한다. 오프라인에서는 다른 방식으로 이중 사용에 대한 방지 대책을 마련한다. 즉, 사용자가 화폐를 이중 사용하게 된다면, 신뢰기관이나 은행에 의해서 익명성이 제어되는 기술을 통해 사전에 이중 사용을 방지하려 한다.

지나친 익명성 제공은 perfect crime[21]과 같은 범죄를 발생시킬 수 있다. 은닉서명 스킴은 서명 받기를 원하는 사람을 제외하고는 메시지와 서명 쌍의 연계성을 찾는 것이 불가능한 "perfect unlinkability"를 제공하기 때문에 전자지불시스템에서는 범죄로 악용

될 우려가 있다고 지적하였다[22]. 강탈(blackmailing), 돈세탁(money laundry), 비밀키 약탈 등과 같은 위협요소들이 일반적으로 이러한 범죄에 해당된다[21,3,17]

상호간의 연계성을 찾기 위해 서명자는 메시지-서명 쌍과 대응하는 프로토콜에 대한 정보를 얻기 위해 신뢰기관을 포함시킨다. 이러한 결과로서 "fair blind signature"가 소개되었다. 이러한 신뢰기관이 서명자에게 제공하는 정보에 따라 크게 두가지 형태로 구분할 수 있다.

첫째, 서명자에게 프로토콜의 관찰이 주어지면, 신뢰기관은 서명자가 대응하는 메시지-서명 쌍을 효과적으로 인식할 수 있는 정보를 제공한다.

둘째, 메시지-서명쌍이 주어지면, 신뢰기관은 서명자가 그 메시지를 보낸 사람을 식별하거나 서명 프로토콜의 대응하는 관찰을 찾을 수 있도록 하는 정보를 제공해준다.

대부분의 전자지불시스템들은 계좌를 개설하거나 인출할 때에 신뢰기관에 권한을 줌으로써 발생하는 문제를 해결하려 하였다. 그러나, 인출시 신뢰기관의 관여는 오히려 부정적으로 작용될 수 있다. 이에 따라, 신뢰기관의 참여를 초기화시에만 필요로 하는 전자지불시스템이 개발되었다[10,16].

신뢰기관은 일반적으로 다음과 같은 성질을 만족해야 한다. 첫째, 신뢰기관은 은행과의 협의를 통하여 거래의 익명성을 제거할 수 있다. 둘째, 신뢰기관은 거래에는 관여하지 않고 계좌 개설시에 시스템 setup하는 동안에만 관여한다. 셋째, 신뢰기관은 프라이버시 관련 문제에 대해서 신뢰성을 갖고 있어야 한다[13].

공개키는 사용자가 은행에 알려진 개인 계좌와 연계되고, 새로운 익명의 계좌를 개설하기 위해 사용자는 그의 개인 계좌의 공개키로부터 유도된 공개키를 제공해야한다는 개념을 이용한 시스템으로서, 이것은 사용되는 두 개의 공개키가 신뢰기관에 등록되어야한다. 실제로 익명계좌를 개설할 때, 은행은 이러한 등록이 있는지와 익명의 계좌의 공개키가 올바르게 생성되었는지를 체크한다. 개인 계좌로부터 인출된 전자화폐는 개인 계좌의 키에 대해 은행에 의해서 서명을 받는다. 고객은 대응하는 익명의 계좌의 공개키에 대해 유효한 서명을 유도한다. 이러한 대응하는 공개키의 등록으로 인하여 돈세탁, 강탈과 같은 부정 사용에 대한 거래를 추적하는 것이 가능하다.

신뢰기관은 시스템에서 다른 역할을 할 수 없으며, 문제 발생시에만 익명성을 제어할 수 있어야만 한다. 또한 신뢰기관의 관련 형태에 따라 신뢰기관이 모든 인출에 참여하는 경우, 계좌개설에만 참여하는 경우, 그리고 지불시스템에는 참여하지 않지만, 익명성 제어를 위해서 요구될 경우에만 사용되는 세 가지의 다른 접근 방법으로 구분한다.

온라인 시스템에서 이중 사용은 많은 deposit에 대한 체크를 통하여 방지될 수 있으나, 은행의 공개키의 유효기간 동안에 예치된 모든 거래정보는 은행에 저장해야 한다. 오프라인 시스템에서 이중 사용 방지는 일반적으로 불가능하지만, 돈이 이중 사용되었을 때, 사용자의 익명성을 제어하도록 시스템을 설계한다. 일반적으로 이러한 방식은 사용자의 ID를 서명된 메시지와 도전 메시지 등과 같은 정보에 담아 둠으로써, 부정 사용시 사용자를 추적한다. 신뢰기관에 의한 익명성 제어를 다음과 같이 구분할 수 있다[10].

- 인출 기반 익명성 제어 : 신뢰기관은 돈이 사용될 때 돈을 인식하기 위해 사용될 수 있는 정보를 계산할 수 있으며 이러한 형태는 blackmailing과 같은 경우에 사용된다.
- 지불 기반 익명성 제어 : 신뢰기관은 돈세탁과 같은 부정사용이 일어날 경우 돈을 인출했던 사람의 신원을 확인할 수 있다.

[16]에서는 Indirect Discourse Proofs 개념을 소개하고 이를 이용하여 fair 오프라인 전자화폐를 설명하고 있다. 일반적으로 오프라인 전자화폐는 포함된 사용자의 신원을 가지고 있으며, 이 시스템에서는 공개키 암호를 이용하여 사용자의 신원을 신뢰기관의 공개키를 이용하여 암호화하여 화폐와 연관시킨다. 만일 부정적인 거래로 인한 신원 확인을 하기 위해 신뢰기관은 암호문을 복호한다.

이러한 위협요소에 대한 대책마련을 강구하기 위하여 전자지불시스템은 익명성 제어 메카니즘을 제공하게 되었으며, 부정적으로 사용된 화폐를 추적하기 위해 신뢰기관의 필요성이 대두되었다. 이러한 강탈 및 돈세탁 등과 같은 공격을 방지하기 위한 시스템이 개발하였다[3,22,13,17]. 그러나 이러한 시스템은 계좌를 개설하거나 인출할 때에 신뢰기관의 관여를 필요로 한다. 따라서 신뢰기관의 관여를 초기화시에만 필요로 하는 전자지불시스템이 개발되었다[10,16]

더욱이, [PP97]에서는 오프라인 지불시스템에서 약탈 공격(extortion attack)의 경우, 신뢰기관에 의해서 익명성이 제어되는 지불시스템이다. 이러한 시스템은 인출하기 전에, 즉, 모든 참여자들의 시스템 파라메터와 키쌍을 선택하는 과정, 신뢰기관에서 익명의 사용자 키쌍을 등록하는 것으로써 이루어진다.

익명성 제어는 추적하는 대상에 따라 크게 두가지 모델로 구분할 수 있다.

- owner tracing : 전자화폐의 소유자를 식별하는 것으로써[3,22], 지불이 이루어진 이후에 신뢰기관에 의해서 이루어진다. 그러나, 이것은 식별자가 전자화폐에 직접적으로 관련된 것보다 구매(시간, 수량, 등)에 기반하기 때문에 많은 형태에 부정행위를 막는데 유용하지 않는다. 이것은 의심되는 화폐의 출처를 찾을 수 있기 때문에 돈세탁을 방지하게 한다.
- coin tracing : 은행으로부터 인출된 화폐를 식별하는 것으로써[22], 구매가 이루어지기 전에 법 집행을 통해 전자화폐의 경로를 추적하는 것이다. 또한, 이것은 신뢰기관이 은행으로부터 인출된 전자화폐를 결정할 수 있고 인출을 거래와 연계시킬 수 있다. 따라서 coin tracing 식별자는 직접적으로 전자화폐에 관련된 정보를 의미하게 된다. coin tracing의 주된 목적은 부정행위와 serial number에 기반하여 추적하는 방법으로 범죄행위를 추적하는데 있다. 이것은 blackmailer가 신원이 확인되지 않고 돈을 사용할 수 있도록 하는 강탈과 같은 부정행위를 방지하게 한다.

익명성 제어는 부정사용과 같은 범죄행위를 줄일 수 있지만, 익명성 제어는 또다른 범죄를 일으킬 수 있다. 예를들어, 범죄자가 사용자로 하여금 계좌에서 전자화폐를 인출하도록 한다. 그러나, coin tracing이 가능하기 때문에 범죄자는 사용자의 전자화폐를 잃어버렸다는 것을 발견하기 전에 돈을 사용하기 위해 사용자를 죽여야만 할 것이다.

[22],[3]에서는 추적 가능한 전자지불시스템으로서, owner tracing을 할 수 있으나, blackmailing과 같은 행위를 막을 수 없고 인출시 신뢰기관 온라인 되어야 한다. 다음은 부정사용에 따른 owner와 coin의 추적에 대한 소개이다.

- owner 혹은 coin tracing를 위해서는 신뢰기관이 각 인출시마다 관여해야한다는 것을 증명하였다[16].

[표 2] 익명성을 제어하는 전자지불시스템 특성

시스템	특성
[3]	- 최초의 tracing 메카니즘 - cut-and-choose 방식 사용 - on-line trustee(계좌개설) - owner tracing
[22]	- tracing 메카니즘 - cut-and-choose 방식 사용 - on-line trustee(계좌개설, 인출시 관여) - owner tracing - linkability
[7]	- owner tracing/coin tracing - on-line trustee(인출시 관여)
[6]	- trustee(지불과 계좌개설시 관여하지 않음) - passive trustee
[17]	- on-line trustee(인출시 관여)
[10]	- owner tracing/coin tracing - off-line trustee - passive trustee
[16]	- owner tracing/coin tracing - off-line trustee
[23]	- 계좌기반 owner tracing - non-interactive - owner/coin tracing
[18]	- marking coin 방법 - trustee 관여하지 않음

- owner와 coin tracing을 제안하였으나, 신뢰기관이 온라인으로 관여한다[13].
- owner와 coin tracing을 제안하였으며, 신뢰기관이 오프라인으로 관여한다[10,16].
- 신뢰기관은 권한이 강화되고, 화폐를 사용하지 못하도록 하고 은행과의 비밀채널을 공유하도록 한다. 그러나 신뢰기관은 인출 혹은 지불할 때에 온라인e으로 된다[17].

[18]에서는 익명성을 제어하기 위해 marking 메카니즘을 이용하였다. 이러한 방식은 신뢰기관을 거래에 관여시키지 않고 필요시 부정사용자를 추적할 수 있다는 것이다. 즉, 일반적인 현금 거래에서 은행에 의해 serial number 혹은 특별한 색 등과 같은 것으로 marking 하는 방법이다. 이러한 기술을 전자화폐에 적용하려 하였다.

Ⅳ. 결 론

D.Chaum에 의한 은닉서명 기술로 인해 전자지

불시스템에 개발이 활발히 진행되었다. 초기에는 익명성이 보장되는 전자지불시스템을 중심으로 기술개발이 이루어졌다. 그러나, 지나친 익명성을 제공함으로써 발생되는 문제점이 제기됨으로써, 이에 대한 해결책에 대해 연구되었다. 이러한 결과로써, 익명성을 제어 할 수 있는 새로운 전자지불시스템의 개발이 진행되었다. 이러한 시스템의 개발은 사용자, 은행, 상점 외의 신뢰성을 갖고 있는 제 3의 기관을 참여시킴으로써 거래를 하였다. 그러나, 최근에는 신뢰기관이 관여하는 부분을 축소하려는 연구가 진행되고 있다.

결론적으로, 전자지불시스템은 보다 효율적이고, 합법적인 사용자에 대해서는 완전한 프라이버시를 제공해주고, 부정적인 사용자에 대해서는 신원을 추적할 수 있는 기술에 대한 연구가 진행되어야 할 것이다. 또한 거래에 참여하지 않고 문제 발생시 해결할 수 있는 신뢰기관의 역할을 부여할 수 있는 전자지불시스템 개발이 이상적이라고 보인다.

참 고 문 헌

[1] S. Brands, "An efficient off-line electronic cash system based on the representation problem", technical Report CS-R9323, CWI, April 1993.

[2] S. Brands, "Untraceable Off-line Cash in Wallets with Observers, Advances in Cryptology", Crypto '93, LNCS 773, Springer-Verlag, pp.302~318.

[3] E. Brickell, P. Gemmell, D. Kravitz, "Trustee-based tracing Extensions to Anonymous Cash and the Making of Anonymous Exchange", Proc. 6th Annual ACM-SIAM Symposium on Discrete Algorithms(SODA), 1995, pp.457~466.

[4] H. Burk, A. Pfitzmann, "Payment systems enabling security and unobservability", Computers & Security, Vol. 8,(1989), pp.399~416.

[5] D. Chaum, "Blind signatures for untraceable payments", In David Chaum, Ronald L.Rivest, and Alan T.Sherman, editors, Advances in Cryptology,-Proceedings of CRYPTO '82, pp.199~203, 1983.

[6] J. Camenisch, and U. Mauer, "Digital Payment systems with passive Anonymity -Revoking Trustees", Copmputer Security-ESORICS '96, E.Bertino, H. Kurth, G. Martella, and E. Montolivo, editors, LNCS 1146, Springer-Verlag, pp.33~43, 1996..

[7] J. Camenisch, J. M. Piveteau, and M. Stadler, "Faire Anonyme Zahlungssysteme", In F.Huber-Waschle, H.Schauer, and P.Widmayer, editors, GISI 95, Informatickaktuell, pp.254~265, Springer-Verlag, Berlin, Sept, 1995.

[8] D. Chaum, "Privacy protected payments: Unconditional Payer and/or Payee Anonymity", Smart Card 2000: The future of IC Cards, North-Holland,(1989), pp. 69~92.

[9] D. Chaum, A. Fiat, and M. Naor, "Untraceable electronic cash", In Shafi Goldwasser, editor, Advances in Cryptology-CRYPTO '88, LNCS 403, pp.319~327, Springer-Verlag, 1990.

[10] J. Camenisch, U. Maurer, M. Stadler, "Digital Payment Systems with Passive Anonymity-Revoking Trustees", LNCS 1146, Proc. ESORICS '96, Springer-Verlag, 1996, pp.31~43.

[11] D. Chaum, T. Pedersen, "Wallet databases with observers", Advances in Cryptology, Crypto '92, LNCS 740, Springer-Verlag, pp.89~105.

[12] J. L. Camenish, J. M. Pieteau, and M. A. Stadler, "An efficient payment system protecting privacy", In Dieter Gollmann, editor, Computer Security-ESORICS '94, LNCS 875, pp.207~215, Springer-Verlag, 1994.

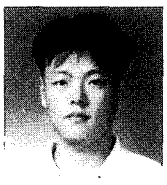
[13] J. Camenisch, J. M. Piveteau, and M. Stadler, "An efficient fair payment system", In 3rd ACM Conference on Computer and Communications Security, pp.88~94, New Delhi, March 1996, Association for Computing Machinery.

[14] N. Ferguson, "Single Term Off-line Coins", Advances in Cryptology, Eurocrypt '93, LNCS 765, Springer-Verlag, pp.318~328.
[15] M. Franklin, M. Yung, "Towards Provably Secure Efficient Electronic Cash", Columbia University, Dept. of Computer Science, TR CUCS-018-92, April, 1992.
[16] Y. Frankel, Y. Tsiounis, M. Yung, "Indirect discourse Proofs: Achieving Efficient Fair Off-Line E-Cash", LNCS 1163, Advances in Cryptology, Proc. Asiacrypt '96, Springer-Verlag, 1996, pp.286~300.
[17] M. Jakobsson, M. Yung, "Revokable and Versatile Electronic Money", Proc. 3rd ACM Conference on Computer and Communications Security, ACM Press, 1996, pp.76~87.
[18] D. Kugler, H. Vogt, "Marking: A Privacy Protectin Approach Against Blackmailing", PKC '01, LNCS 1992, Springer-Verlag, pp.137~152, 2001.
[19] T. Okamoto, "An efficient divisible electronic cash scheme", In Don Coppersmith, editor, Advances in Cryptology, Proc. of Crypto '95, LNCS 963, pp.438~451, Springer-Verlag, 1995.
[20] T. Okamoto, and K. Ohta, "Universal electronic cash", In Joan Feigenbaum, editor, Advances in Cryptology-CRYPTO '91, LNCS, pp.324~337, Springer-Verlag, 1992.
[21] S. von Solms, and D. Naccache, "On blind signatures and perfect crimes", Computer & Security, 11(6):581-583, 1993.
[22] M. Stadler, J. M. Piveteau, and J. Camenisch, "Fair blind signature", In Louis C.Guillou and J.J.Quisquater, editors, Advances in Cryptology-EUROCRYPT '95, LNCS 921, pp.209~219, Springer-Verlag, 1995.
[23] T. Sander, and A. Ta-Shma, "Flow Control: A New Approach For Anonymity Control In Electronic Cash Systems", LNCS 1648, Springer-Verlag, 1998.

〈著 者 紹 介〉

강 성 우 (Sungwoo Kang)

1996년 2월 : 중앙대학교 수학과 이학사
2001년 8월 : 서울대학교 대학원 수학과 이학석사
2000년 12월~2003월 6월 17일 : 한국정보보호진흥원 암호기술팀 연구원
2003년 6월 18일~현재 : 한국정보보호진흥원 암호인증기술팀 연구원
〈관심분야〉 암호학, 정보보호, 전자화폐



박 해 룡 (Haeryong Park)

1998년 2월 : 전남대학교 수학과 이학사
2001년 2월 : 서울대학교 대학원 수학과 이학석사
2000년 12월~2003월 6월 17일 : 한국정보보호진흥원 암호기술팀 연구원
2003년 6월 18일~현재 : 한국정보보호진흥원 암호인증기술팀 연구원
〈관심분야〉 암호학, 전자화폐, DRM

심 경 아 (Kyung-Ah Shim)

1992년 2월 : 이화여자대학교 수학과 이학사
1994년 2월 : 이화여자대학교 대학원 수학과 이학석사
1999년 2월 : 이화여자대학교 대학원 수학과 이학박사
2000년 2월~2003월 6월 30일 : 한국정보보호진흥원 암호기술팀 선임연구원
2003년 7월~현재 : 한국정보보호진흥원 암호인증기술팀 선임연구원
〈관심분야〉 타원곡선, 암호프로토콜, 전자화폐