전자경매를 위한 보안 프로토콜

A Secure Protocol for the Electronic Auction

원보스(Wenbo Shi)*, 장인주(InJoo Jang)*, 유형선(Hyeong Seon Yoo)**

초 록

Collins[1]등이 제안한 멀티 에이전트 테스트 베드는 발행/가입 시스템, 타임 릴리즈 암호법, 그리고 익명 통신 기법에 기반을 두고 있다. 최근 Jaiswal[2]등은 Collins의 멀티 에이전트 테스트 베드를 향상시키는 프로토콜을 제안하였다. 그러나 Jaiswal의 프로토콜 또한 데이터 재전송 공격, DOS 공격, 익명성 폭로 등과 사용자와 공급자 사이의 충돌 등의 문제에 대하여 취약함을 보인다. 본 논문에서는 DOS 공격의 가능성을 줄이고, 공급자에게 티켓 토큰과 처리 순번 제공함으로써 데이터 재전송 공격을 피할 수 있는 프로토콜을 제안한다. 또한 본 논문의 제안 프로토콜에서, 마켓은 공급자에게 난수 생성 방법과 결정과정의 데이터를 공유하기 위한 보간 다항식을 제공하여 사용자와 특정한 공급자 사이의 충돌을 피할 수 있게 한다.

ABSTRACT

Recently, Jaiswal et al. proposed a protocol to improve the multi agent negotiation test-bed which was proposed by Collins et al. Using publish/subscribe system, time release cryptography and anonymous communication, their protocol gives an improvement on the old one. However, it is shown that the protocol also has some security weaknesses: such as replay data attack and DOS (denial of-service) attack, anonymity disclosure, collusion between customers and a certain supplier. So proposed protocol reduces DOS attack and avoids replay data attack by providing ticket token and deal sequence number to the supplier. And it is proved that the way that market generates random number to the supplier is better than the supplier do by himself in guaranteeing anonymity. Market publishes interpolating polynomial for sharing the determination process data. It avoids collusion between customer and a certain supplie

키워드 : 전자 경매, 보안, 익명성, 티켓 토큰
Electronic Auctions, Security, Anonymity, Ticket Token

본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 육성 지원사업의 연구 결과로 수행되었음.

* 인하대학교 컴퓨터정보공학
** 인하대학교 컴퓨터 공학부 교수

1. 서 론

2002년 Collins는 기업과 기업간의 전자 마켓을 위한 멀티 에이전트 시장(MAGNET: Multi-Agent Negotiation Test-bed)을 제안하였다[1]. 전자처리에 대한 사업 가치와 그 임계치가 증가함에 따라, 보안문제의 중요성이 급증되었다. MAGNET 초기 시스템은 보안문제에 많은 주의를 기울이지 않았기 때문에, Jaiswal 등은 2004년 온라인 시스템을 위한 보안 프로토콜을 제안하였고, 실세계 네트워크 상에서의 보안 문제를 분석하였다[2]. 여기서 중요하게 고려되는 사항은 경매 참여 에이전트들을 위한 발행/가입 시스템을 이용하는 것과 입찰자들의 개별 정보를 숨기기 위해 익명 통신을 사용하는 것, 입찰에 대해 비공개를 유지하기 위해 타임 릴리즈 암호기법을 사용하는 것이다. 이것에 의하여 MAGNET는 기존의 것보다 보안성에 있어서 향상을 가져왔으나, 몇 가지의 취약점은 그대로 남았다. 특히 데이터 재전송 공격과 DOS 공격, 익명성의 폭로 및 사용자와 공급자 사이의 충돌 등에 있어서 더욱 취약하다.

본 논문은 이러한 취약점을 해결하기위해 보완된 프로토콜을 제안한다. 본 논문에서 제안하는 프로토콜은 다운로드를 엄격히 관리하기 위해 티켓 토큰을 사용하고, 난수와 처리 순번을 생성하여 사용한다. 마켓은 간단한 해시 계산을 이용하여 DOS 공격을 줄이고, 데이터 재전송 공격을 피할 수 있다. 익명성을 유지하기 위해 난수의 생성은 공급자가 하는 것보다 마켓이 공급자에게 생성해 주는 방식을 채택한다. 마켓은 간단한 보간 다항식을 구축하여 공급자들 사이에서 규명 정보의 공유를 용이하게 한다. 이것으로 사용자와 공급자 사이의 충돌을 피할 수 있다. 제 5장에서는 Jaiswal 등의 프로토콜과의 비교 분석을 통하여 본 논문에서 제시한 프로토콜과의 차이를 보여준다.

2. MAGNET 스킴

Jaiswal등이 제안한 온라인 시스템의 보안 프로토콜인 MAGNET은 주문(Planning)과정, 입찰(bidding), 경매(Auction)와 낙찰과정(Winner Determination)으로 구성되어 있다. MAGNET의 통신 과정은 재전송 공격 부분을 제외하면 <그림 1>과 같다. 통신 과정 중에 사용되는 용어를 정의하면 다음과 같다. 이 용어들은 이 논문 안에서 계속적으로 사용된다.

- 용어정의

  RFQ(requests for quotes) : 주문 의뢰
  r(random number) : 난수
  k_a(auction-session key) : 경매 세션 키
  bid(bid data) : 입찰 데이터
  TE(time-release encryption) : 타임 릴리즈 기법을 사용한 암호화[7]
  $S_{Sks}(bid)$: 공급자의 비밀키로 서명한 입찰 데이터
  $E_{pkc}()$: 사용자의 공개키를 사용한 암호정보
  $E_{pkm}()$: 마켓의 공개키를 사용한 암호정보

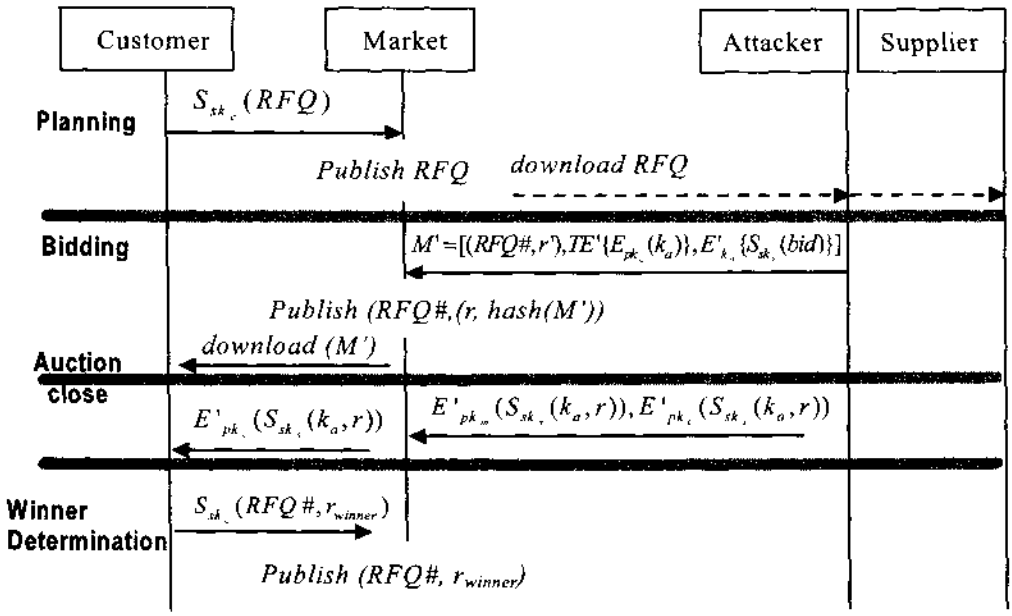
3. MAGNET 스킴의 취약점

3.1 재전송 공격

Jaiswal 등이 제안한 프로토콜은 정보 재

전송 공격에 대하여 취약하다. 정보 재전송 공격 과정은 <그림 1>에서 보는 바와 같이 이루어진다. 한 공격자가 침입하여 공급자가 전송하는 메시지를 가로채었다고 가정하자. 분실된 데이터는 $M = [(RFQ\#, r), TE\{E_{pkc}(k_a)\}, E_{ka}\{S_{sks}(bid)\}]$과 $E_{pkm}(S_{sks}(k_a, r)), E_{pkc}(S_{sks}(k_a, r))$이다. 이 때 공격자가 기회를 얻게 되면, 현재의 입찰과정에서 정보 재전송을 사용하게 된다.

메시지 $M = [(RFQ\#, r), TE\{E_{pkc}(k_a)\}, E_{ka}\{S_{sks}(bid)\}]$에서 RFQ 수 $(RFQ\#)$와 난수(r)은 정보보호를 받지 못하고 있다. 이로 인하여 공격자는 가로챈 정보로 정보 재전송을 통해 위장 할 수 있다. 적법한 공급자가 현재의 입찰과정을 취하지 못하거나 공격자가 마켓과 공급자 사이의 통신을 두절 시켰을 때, 공격자는 공격자 자신이 선택한 공급자의 정보로 위조된 입찰정보 $M' = [(RFQ\#, r'), TE' \{E_{pkc}(k_a)\}, E'_{ka}\{S_{sks}(bid)\}]$를 생성시킬 수 있다. 정보 M'에서 $RFQ\#$는 현재의 RFQ 수이며, 다른 정보군은 이미 사용된 정보 군이다. 마켓은$(RFQ\#, (r', hash(M'))$을 발행하고 공급자가 정보 M'의 해시 값을 확인하도록 기다린다. 그러나 이때 공표된 정보는 위조된 내용이므로 해당 공급자가 발행 정보에 대하여 확인하게 될 가능성이 적다. 마켓 역시 타임 릴리즈 암호기법의 사용으로 공급자를 인식 할 수 없으며 정보의 기밀성도 판단할 수 없게 된다. 경매가 끝날 경우, 공격자는 정보 $E'_{pkm}(S_{sks}(k_a, r)), E'_{pka}(S_{sks}(k_a, r))$을 마켓에 전송한다. 이 때 마켓은 정보 중 (k_a, r)을 확인하게 되지만 난수 r과 키k_a에 관한 재전송 여부를 확인 할 방법이 없다. 따라서 공격자가 공급자의 서명을 위조할 수는 없으나, 과거의 정보를 사용할 수는 있다. 따라서 재전송 공격에 관하여 취약하다.



〈그림 1〉 재전송 공격 과정

3.2 공급자의 익명성 노출

익명성을 강조하는 많은 프로토콜들은 난수기법을 사용한다. Jaiswal등의 프로토콜에서도 경매가 종료될 때까지 입찰자의 신원을 감추기 위해 익명 통신을 사용한다. 그러나 이 부분에서도 몇 가지 약점을 나타내고 있다. 우선 생성한 난수에 대하여 우수한 랜덤성이 확인 되지 않았다. 또한 Jaiswal등의 프로토콜에서는 난수의 반복적인 사용에 의하여 공급자가 마켓과 사용자에게 자신의 익명성을 노출시켜 결탁하기 위한 조건을 만들기 용이하다. 이로써 익명 통신이 실패하게 된다.

3.3 특정 공급자와 사용자와의 공모

사용자는 받은 메시지로부터 낙찰자를 결정하게 된다. 사용자가 지속적으로 퍼즐을 복호화하고 모든 공급자들의 신원을 알게 된다면, 사용자는 다른 공급자들을 고려하지 않은 채 특정 공급자만을 그의 파트너로 선택할 수 있게 될 것이다. 이는 공평하지 못한 입찰 시스템이기에 본 논문에서는 입찰자를 결정하는 모든 과정의 공평성을 확인 할 수 있도록 설계하였다.

4. 제안 프로토콜

본 절에서는 Jaiswal등이 제안한 프로토콜의 취약점을 보완하고, 향상시키기 위한 프로토콜을 제안하고자 한다. 제안하는 프로토콜은 주문, 입찰, 계약, 경매 마감, 낙찰의 과정으로 구성되며, <그림 2>에서 이를 표현 하였고, 그 자세한 설명은 다음과 같다.

4.1 주문 과정

사용자는 발행을 위해 마켓에 서명된 RFQ를 전송한다.

4.2 입찰 과정

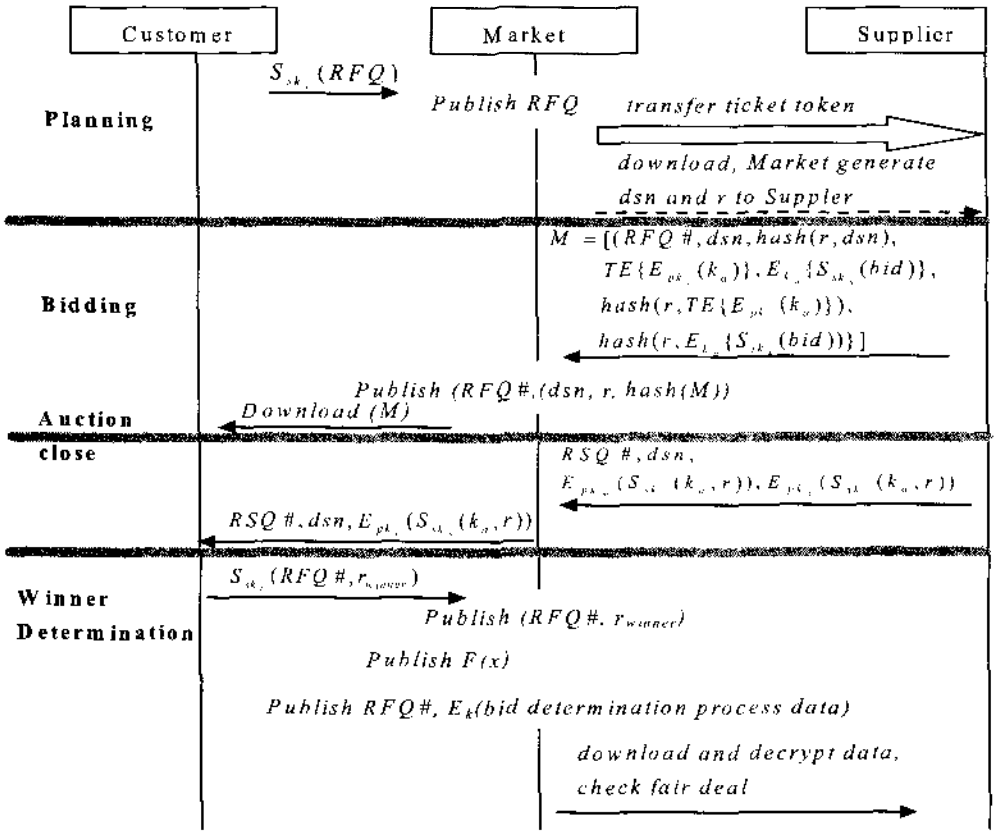
마켓은 티켓 토큰을 생성하여 공급자 그룹에게 전송한다. 합법적인 공급자가 관심 있는 RFQ를 다운 받게 되면, 마켓은 처리 순번 *dsn*과 난수 *r*을 공급자에게 생성시켜 준다. 공급자는 마켓으로부터 정보를 받은 뒤 RFQ의 수*(RFQ#)*,와 처리 순번*(dsn)*, 난수*(r)*, 경매-세션키*(k_a)*, 입찰 자료(bid)를 포함한 입찰 정보를 생성한다. 그 정보는 서명, 해싱, 암호화 등을 거친 정보*(M)*으로 마켓에 전송된다. 마켓은 모든 정보*(RFQ#, (dsn, r, hash(M)))*를 발행/가입 시스템에 출판한다. 공급자는 마켓에 의하여 제공받고, 나타내진 자신의 입찰 정보를 확인하고 입증할 수 있다. 사용자는 발행/가입 시스템으로부터 정보 *M*을 얻을 수 있게 된다.

4.3 경매 과정

공급자는 마켓에 암호화된 정보 $E_{pkm}(S_{skS}(k_a, r))$, $E_{pkc}(S_{skS}(k_a, r))$의 형태로 k_a를 제공 한다.

4.4 낙찰자 결정과정

사용자는 낙찰자를 결정하고, 이를 마켓의 알림판을 통해 공급자들에게 알려주어야 한



〈그림 2〉 제안 프로토콜

다. 마켓은 사용자들의 메시지를 받은 후 낙찰자의 정보를 공표하고 대칭 세션키인 K, $K = k \bmod p$,를 계산한다. 그 후 입찰 결정 과정의 데이터를 암호화 하여*(RFQ#, Ek(bid determination process data))*를 생성한 뒤 공표한다. 마켓은 식 (1)을 통해 공급자들의 서명 데이터 값을 만들어 사용하고 그 데이터들을 공표한다.

$$F(x) = \prod_{i=1}^{n}(x - h_i) + k \bmod p \qquad (1)$$
$$; \ h_i = g^{S_{sk_i}(k_{a_i}, r_i) \bmod (p-1)}$$

식 (1)은 간단한 보간 다항식이다[6 9]. 이 식에서 보듯이 정확한 k를 얻기 위하여 공격자는 유효한 x를 알아내어야 $F(x) = k \bmod p$를 계산 할 수 있다. 그러나 공격자는 보간 다항식 $h_i = g^{S_{sk_i}(k_{a_i}, r_i) \bmod (p-1)}$의 계산 값을 얻는 과정에서 DL(discrete logarithm)문제에 직면하게 되며 이를 해결하는 것이 불가능하여 유효한 x를 얻는데 실패하게 된다. 이로써 마켓은 간단히 식을 수립하고 그것을 안전하게 공표할 수 있게 된다. 경매에 참여하는 합법적인 공급자들은 데이터 K를 얻기 위하여 $K = k \bmod p$를 계산한다. 이 공급자들은 함수를 확인하기 위해 자신들의 서명 $S_{sk_i}(k_a, r)$을 사용하고, 얻어낸 K값을 이용해 입찰 과정의

공정성을 분석하기 위한 메시지를 복호화한다.

5. MAGNET 스킴의 향상된 보안

5.1 주문 과정

Aschen 대학과 IBM 연구소가 함께 한 그룹 통신 프로토콜 및 익명 프로토콜에 대한 토의는 방송망을 안전하게 할 수 있는 몇 가지 방법을 제시 해 주었으며, 티켓 토큰이 좋은 해결책임도 알려 주었다[3, 4]. 마켓은 관심을 지니고 RFQ를 다운받은 합법적인 모든 공급자에게 티켓 토큰을 전송한다. 이것은 입찰과정에 참여하려는 공격자들을 효과적으로 피하게 해 준다. 그리고 공급자들이 마켓에 전송하는 메시지에는 데이터 처리 순번*(dsn)*와 난수 *(r)*이 사용되며 이는 DOS 공격을 줄이는 방법이 된다.

그러나 이 방법이 합법적인 공급자와 혼합되어있는 공격자들을 완전히 피하게 할 수는 없다. 합법적인 공급자가 공격자에게 티켓 토큰을 누출 시켰다고 가정해 볼 때, 그 공격자는 역시 RFQ를 다운 받을 수 있으며, 처리 순번과 난수를 얻을 수 있고 입찰과정에 참여할 수 있게 된다. 이러한 문제는 경매 종료 시까지 공급자의 신원을 드러내지 않기 때문에 발생된다[2].

5.2 입찰 과정

기존의 프로토콜에서는 한 공급자가 마켓에 메시지 $M = \{(RFQ\#, r), TE\{E_{pkc}(k_a)\}, E_{ka}\{S_{skc}(bid)\}\}$를 전송한다. 공급자는 메시지 M 안의 난수 r을 노출시키기 때문에 공급자의 익명성을 유지하지 못하게 된다. 또한 마켓이 메시지의 재사용 여부와 정보의 위조 여부를 식별하지 못하기 때문에 마켓은 "time-lock puzzle"을 해결하기 위한 자원낭비가 심하게 된다. 따라서 공격자가 공격을 위해 많은 양의 정크 데이터를 생성하게 되면 마켓은 쉽게 마비된다.

본 논문의 개선된 프로토콜에서는 메시지 M에 마켓이 제공한 처리 순번*(dsn)*와 난수 *(r)*를 포함하고 있다. 모든 *dsn*은 모든 공급자들을 식별하기 위한 임시 정보가 된다. 마켓에 의하여 생성된 난수는 모든 공급자에게 있어 공평하다. 이것은 공급자가 난수를 생성하고 자신의 신원을 노출시키기 쉬워 발생되는 취약점을 피해가도록 한다.

공급자가 마켓에 메시지 M을 전송할 때, 마켓은 해당 *dsn*와 난수 *r*을 찾아내고, 해당 해시값 *hash(r, dsn)*을 식별해 낸다. 이 때 공격자는 정확한 난수를 지닐 수 없기 때문에 정보의 위조나 정보의 재사용에 대한 공격이 실패로 돌아가게 된다. 따라서 본 논문이 제시하는 프로토콜은 정크 데이터의 빠르고 효율적인 식별을 가능하게 하며, 재전송 공격과 DOS공격을 피하게 해 주며, 공급자의 익명성을 보호해 주는 장점을 지니고 있다.

5.3 낙찰자 선정 과정

기존의 프로토콜은 사용자와 마켓만이 입찰 시에 낙찰자 선정 과정을 알게 되고 공급자는 그 결과만을 알도록 되어 있었다. 이는 사용자가 특정한 공급자들과 결탁하여 결과를 조작할 가능성을 제공하기도 한다.

본 논문에서 제시하는 프로토콜은 사용자

가 마켓에게 메시지 $S_{skc}(RFQ\#, rwinner)$를 전송한 후, 마켓이 낙찰자 정보를 공표하고 낙찰 과정의 데이터를 비밀키 K를 이용하여 암호화 한 뒤 공표한다. 그 후 마켓은 보간 다항식을 사용하여 키 유도식을 세우고 그것을 공표한다. 공격자는 자신의 $S_{sks}(k_a,r)$을 유도식에 넣어 정보를 복호화 하는 키를 계산한다. 정보의 복호화를 통해 입찰에 참가한 모든 공급자는 입찰의 공정성을 확인할 수 있게 된다.

많은 논문에서는 비밀 공유스키마와 그룹 서명을 위해 라그랑주 보간 다항식과 한계치 함수를 이야기 하고 있다[5-9]. 만일 공격자가 데이터의 복호화를 위해 키를 계산하기 원한다면, 그는 이산 로그문제와 보간 다항식 문제를 해결해야만 한다. 본 논문이 제시하는 프로토콜은 사용자와 공급자사이의 비합법적인 결탁을 막을 수 있다는 장점을 마켓에 제공하게 된다.

6. 결 론

본 논문에서는 Jaiswal등의 프로토콜이 정보 재전송 공격, 익명성의 보호 및 사용자와 공급자 사이의 결탁 등에 취약함을 보이고 있음에 따라 이를 향상시키기 위해 제안하였다. Jaiswal등의 프로토콜과는 달리 본 논문에서 제안하는 프로토콜은 티켓 토큰의 사용과 공급자를 위한 난수와 처리 순번의을 생성 및 제공으로 재전송 공격과 DOS 공격을 피하고 공급자의 익명성을 보호하며, 사용자와 공급자 사이의 결탁을 막을 수 있다는 점에서 진보적인 마켓을 제공할 수 있다.

참 고 문 헌

[1] Collins, J., Ketter, W., and Gini, M., "A multi-agent negotiation testbed for contracting tasks with temporal and precedence constraints," International Journal of Electronic Commerce, Vol. 7, No. 1, 2002, pp. 35-57.

[2] Jaiswal, A., Kim, Y., and Gini, M., "design and implementation of a secure multi-agent marketplace," Electronic Commerce Research and Applications, Vol. 3, No. 4, 2004, pp. 355-368.

[3] Kesdogan, D. and Palmer, C., "Technical challenges of network anonymity," Computer Communications, 29, No. 3, 2006, pp. 306 324.

[4] Levente Buttyan and Naouel Ben Salem, "A Payment Scheme for Broadcast Multimedia Streams," In Proceedings ofthe 6th IEEE Symposium on Computers and Communications, 2001, pp. 668-673.

[5] Yang, Y. J., Wang, S. H. and Bao, F., "New efficient user identification and key distribution scheme providing enhanced security," Computers & Security, Vol. 23, No. 8, 2004, pp. 697-704.

[6] Woei-Jiunn Tsaur, Chia-Chun Wu, and Wei-Bin Lee, "A smart card-based remote scheme for password authentication in multi-server internet services," Computer Standards & Interfaces, Vol. 27, No. 1, 2004, pp. 39-51.

[7] Lee, N. Y. and Hwang, T., "Group-ori-

ented undeniable signature schemes with a trusted center," Computer Communications, Vol. 22, No. 8, 1999, pp. 730-734.

[8] Tan, K. J. and Zhu, H. W., "General secret sharing scheme," Computer Communications, Vol. 22, No. 8, 1999, pp. 755-757.

[9] Tan, K. J. and Zhu, H. W., "General secret sharing and monotone functions," Computer Communications, Vol. 22, No. 8, 1999, pp. 755-757.

저 자 소 개

원보스 (E-mail : swb319@hotmail.com)
Chengdu university of technology in China, Department of Computer science and technology, MS
현재 인하대학교 컴퓨터정보공학 (석사)
관심분야 Applied Cryptography

장 인 주 (E-mail : jangij@dreamwiz.com)
현재 인하대학교 컴퓨터정보공학 (석사)
관심분야 Applied Cryptography

유형선 (E-mail : hsyoo@inha.ac.kr)
Ghent University, Belgium 기계공학 (박사)
현재 인하대학교 컴퓨터 공학부 교수
관심분야 Applied Cryptography, Scientific Computation