PVNIOT를 적용한 공정한 은닉 서명 프로토콜 설계

김 상 춘* · 권 기 현*

요 약

불확정 전송 프로토콜의 가장 큰 문제점은 단일 프로토콜로 사용될 경우에는 그 통신량과 계산량이 적지만 암호 프로토콜의 서브프로토콜로 사용될 경우 그 통신량과 계산량이 급증한다는 것이다. 이러한 문제점을 해결하기 위해 통신 트래픽이 적은 시간에 사전 계산을 실행함으로써 통신량과 계산량을 줄일 수 있도록 설계한 검증 가능한 비대화형 불확정 전송 프로토콜을 적용하여 기존에 Fiat-Shamir 서명 방식(Fiat 86)에서 평방 근을 사용하던 방식 대신에 third root를 사용하고 1-out-of-2 불확정 전송을 이용하는 <Type I>에 관한 공정한 은닉 서명 기법에 사전 계산에 의한 검증 가능한 비대화형 불확정 전송 프로토콜을 적용하여 공정한 은닉 서명 프로토콜을 설계하였다. 또한 제안한 프로토콜을 Lein Harn, VNIOT 프로토콜 방식과 비교하여 분석하고, 프로토콜에 대하여 분석하였다.

A Design of Fair Blind Signatures Protocol using PVNIOT

Sang Choon Kim* · Ki Hyeon Kwon*

ABSTRACT

The biggest problem for the oblivious transfer protocol is the rapid increasement of network traffic and computational complexity if the protocol is used as a sub-protocol compare to the case that when it is used as a standalone protocol. To fix such problems, in this paper, we propose a verifiable Non-interactive OT protocol that reduces the network traffic and computational complexity by preprocessing the necessary computations when the network traffic is low. The proposed protocol uses third root mechanism instead of square root mechanism that is used for the Fiat-Shamir signature mechanism and also uses 1-out-of-2 oblivious transfer based on <Type I> signature mechanism. We also analyze the proposed protocol by comparing to the Lein Harn, VNIOT protocols.

* 삼척대학교 정보통신공학과

1. 서 론

컴퓨터의 보급과 인터넷 사용이 급증하면서, 컴퓨터 네트워크를 통한 정보량이 급격히 증가하고 있다. 정보량의 급격한 증가는 방해(interruption), 가로채기(interception), 위조(fabrication), 신분위장(masquerade), 재전송(replay), 서비스 부인(denial of service), 불법수정(modification) 등 합법적인 사용자에 대한 안전성과 인증 문제를 유발시켰고 이를 기반으로 한 보다 세분화된 안전성 요구되고 있다. 이에 따라 정보보호에 대한 중요성이 증가되었고 전자 인증 시장의 확대도 요구되고 있다.

분산 환경하에서 암호 프로토콜을 효율적으로 실현하려면 합법적인 사용자에 대한 안전한 통신을 확보하는 것과 더불어 적용환경 및 적용업무에 따라서 여러 가지 추가적인 요구 조건이 부가된 다양한 기능을 갖는 암호 프로토콜에 대한 연구가 요구된다.

따라서 본 논문에서는 여러 분야에서 다양하게 연구되고 있는 암호 프로토콜에 대한 연구를 통해 정보사회가 요구하는 새로운 안전 요구사항에 대한 해결을 모색코자 하였고, 일반적으로 암호 프로토콜을 설계하기 위한 기본적인 도구로서 유용하게 쓰이는 서브프로토콜인 불확정 전송(Oblivious Transfer : OT) 프로토콜[1]~[5]중 부인봉쇄 기능을 갖는 검증 가능한 비대화형 불확정 전송(Verifiable NIOT : VNIOT)[6]에서 전송량과 계산량이 증가하는 문제를 해결하기 위하여 통신 트래픽이 적은 시간에 사전처리를 수행하는 PVNIOT 프로토콜을 이용하여, 공정한 은닉서명 프로토콜을 설계하고 프로토콜의 안전성에 대하여 분석하였다.

2. 내용 은닉 서명(Blind Signature)

내용 은닉서명은 D. Chaum이 CRYPTO '82에서 제안한 것으로, 메시지 내용은 상대방에게 알려주지 않으면서도 메시지에 대한 서명자의 서명을 얻게 되는 것으로 전자 화폐(electronic cash)나 전자 선거(electronic vote)등에서 사용자의 프라이버시(privacy)를 제공하고 사용자가 익명성을 가질 수 있게 하는 추적 불가능 서명 기법(untraceability signature technique)이다[12].

(1) RSA 암호를 이용한 내용 은닉 서명은 다음과 같다.

서명자(B)의 공개키(public key)를 e, 비밀키(secret key)를 d라고 하자.

RSA 파라메타(n) = p · q는 공개 정보이고, m은 메시지이다.

[단계 1] 송신자(A)는 난수(random number) r을 생성하여 서명자(B)에게 C = re m(mod n)을 계산하여 보낸다.

[단계 2] 서명자(B)는 송신자(A)로부터 수신한 C에 대하여 다음과 같이 계산하여, 송신자(A)에게 전송한다. $C^d = (re\ m)^d \pmod n$ 난수 r은 송신자만 알고 있으므로 서명자는 메시지의 내용을 알지 못한다.

[단계 3] 송신자(A)는 서명문(S) = $C^d / r = (re\ d\ md) / r = md \pmod n$을 계산하여 서명자(B)의 메시지(m)에 대한 서명문(S)을 획득하게 된다.

3. 사전 계산 기능을 갖는 비대화형 불확정전송 프로토콜

PVNIOT(Precomputing VNIOT)프로토콜은 부인봉쇄 기능을 갖는 검증 가능한 비대화형 불확정 전송 프로토콜에서 송신자와 TTP와의 교환 데이터의 단위를 비트 단위가 아닌 메시지 단위로 전송한다. [사전 계산 단계]에서 송신자(Alice)는 서명 메세지를 사전에 선택하고 선택한 메세지에 대한 정보를 TTP로부터 획득함으

로써 [온라인 단계]에서는 TTP와의 통신을 하지 않아도 된다. 사전 계산 기능을 갖는 검증 가능한 비대화형 불확정 전송 프로토콜의 수행 절차는 다음과 같다.

● 파라메타 정의

- x_i, d_B : Bob의 비밀키
- d_A : Alice의 비밀키
- p_0, p_1, y_0, y_1 : Alice가 선택한 값
- r : 비밀 난수로서 Alice가 선택한 값
- p, g, C : TTP의 공개 정보
- M_0, M_1 : Alice가 Bob에게 보내는 비밀 정보(메세지 단위)
- i : Bob이 선택한 값
- β_0, β_1 : Bob의 공개키
- e_T : TTP의 공개키
- d_T : TTP의 비밀키

● 키생성단계

① 키발급센터는 임의의 소수(p)와 Z_p^*의 생성원(g)을 선택한다. 임의의 소수 (p, g)와 Z_p^*의 임의의 원소(C)를 시스템 내의 모든 사용자에게 공개한다. 사용자들은 C의 이산대수를 못한다.

② 수신자(B)는 랜덤하게 i∈{0, 1}을 선택하고 xi∈{0, 1, …, p-2}를 선택한 후 다음을 계산한다.

$$\beta_i = g^{x_i} \pmod p,$$

$$\beta_{1-i} = C(g^{x_i})-1 \pmod p$$

자신의 공개키(β_0, β_1)을 공개하고 i, x_i를 비밀리에 유지한다.

누구든지 $\beta_0 \cdot \beta_1$ =C를 점검하므로 β_0, β_1이 정확한지 확인이 가능하며, C의 이산대수가 알려지지 않는 한 수신자(B)는 β_0와 β_1 모두의 이산대수를 알 수 없고, 수신자(B)가 알고 있는 이산대수가 β_0인지 β_1인지 다른 사용자들이 알 수 없다.

● 사전 계산 단계

[단계 1] Alice는 비밀 정보(M_0, M_1)를 자신의 비밀키(d_A)로 암호화한 후 난수(r)를 생성하여 $D_0 = M_0{}^{d_A} r^{e_T} \pmod n$, $D_1 = M_1{}^{d_A} r^{e_T} \pmod n$계산하고 결과 값(D_0, D_1)을 TTP에게 전송한다.

[단계 2] TTP는 Alice로부터 수신한 결과 값(D_0, D_1)에 대한 서명 값 $D_0{}^{d_T} = (M_0{}^{d_A} r^{e_T})^{d_T} \pmod n$, $D_1{}^{d_T} = (M_1{}^{d_A} r^{e_T})^{d_T} \pmod n$을 계산한 후 저장하고 결과 값($D_0^{d_T}$, $D_1^{d_T}$)을 Alice에게 전송한다.

[단계 3] Alice는 $S_0 = D_0{}^{d_T}/r = (M_0{}^{d_A})^{d_T} r/r \pmod n$, $S_1 = D_1{}^{d_T}/r = (M_1{}^{d_A})^{d_T} r/r \pmod n$를 계산하고 p_0, p_1∈{1, 2, …, p-1}을 랜덤하게 선택하여 $K_0 = \beta_0{}^{p_0} \pmod p$, $K_1 = \beta_1{}^{p_1} \pmod p$, $A_0 = S_0 \oplus K_0$, $A_1 = S_1 \oplus K_1$, $C_0 = g^{p_0} \pmod p$, $C_1 = g^{p_1} \pmod p$를 계산한 후 결과 값(A_0, A_1, C_0, C_1)을 TTP에게 의뢰한다.

● 온라인 단계

[단계 1] Alice는 y_0, y_1 ∈{1, 2, …, p-1}을 랜덤하게 선택하여 $\alpha_0 = g^{y_0} \pmod p$, $\alpha_1 = g^{y_1} \pmod p$, $r_0 = \beta_0^{y_0} \pmod p$, $r_1 = \beta_1^{y_1} \pmod p$, $R_0 = A_0 \oplus r_0$, $R_1 = A_1 \oplus r_1$를 계산하고 결과 값(α_0, α_1, R_0, R_1)을 Bob에게 전송한다.

[단계 2] Bob은 Alice로부터 결과 값(α_0, α_1, R_0, R_1)을 수신하면 자신의 비밀키(x_i)로 $r_i = \alpha_i^{x_i} \pmod p$, $Q_i = R_i \oplus r_i$를 계산한 후 ${Q_i}^{d_B}$를 계산한다.

[단계 3] Bob은 TTP에게 결과 값(${Q_i}^{d_B}$)을 제출하며 TTP는 ${Q_i}^{d_B}$ 저장한다.

[단계 4] Bob는 Alice가 TTP에게 의뢰한 정보를 검색하여 만약 $Q_i = A_0$이면, $K_0 = {C_0}^{x_i} \pmod p$, $S_0 = Q_i \oplus K_0$, $M_0 = (S_0{}^{e_A})^{e_T}$, $Q_i = A_1$이 면 $K_1 = {C_1}^{x_i} \pmod p$, $S_1 = Q_i \oplus K_1$, $M_1 = (S_1{}^{e_A})^{e_T}$. 그렇지 않으면 Alice의 부정이 탐지되므로 Bob는 Alice의 부정에 대해 추궁할 수 있다.

4. PVNIOT를 적용한 공정한 은닉 서명 프로토콜

이 절에서는 공정한 은닉 서명 기법, Fiat-Shamir 서명 프로토콜과 Fiat 1-out-of-2 OT 프로토콜을 분석하고, 앞 절에서 설계한 사전 계산에 의한 검증 가능한 비대화형 불확정 전송 프로토콜을 적용하여 기존에 Fiat-Shamir 서명 방식(Fiat 86)에서 평방 근을 사용하던 방식 대신에 third root를 사용하고 1-out-of-2 불확정 전송을 이용하는 <Type I>에 관한 공정한 은닉 서명 기법에 사전 계산에 의한 검증 가능한 비대화형 불확정 전송 프로토콜을 적용하여 공정한 은닉 서명 프로토콜 설계하였다.

D. Chaum이 제안한 공정한 은닉 서명 기법 [12]은 사용자에게 강력한 익명성을 제공하고 있다. 강력한 익명성은 화폐의 인출과 서명 사이의 연결을 방해하고, 같은 고객에 의해 지불되는 것을 방지한다. 인출과 지불 사이의 연결이 불가능해짐에 따라 불법적인 사용자에 의한 돈세탁, blackmail과 같은 불법 사용이 가능하게 되었다. 이러한 문제점은 1995년 M. Stadler, J. Marc Piveteau, J. Camenisch의 논문[13]에서 제안한 공정한 은닉 서명 기법을 통해 서명과 화폐의 인출 사이의 연결성(linkability)을 제공해 줌으로써 불법적인 사용자에 의한 불법 사용을 막을 수 있도록 개선되었다.

(2) 공정한 은닉 서명 기법은 다음의 두 가지 형태로 분류한다.

<Type Ⅰ>

프로토콜이 수신자의 관점에서 주어진다면 메세지를 추출할 수 있는 TTP는 수신자에게 [메세지-서명] 쌍에 대한 정보를 제공한다.

<Type Ⅱ>

[메세지-서명] 쌍이 주어졌을 때 TTP는 수신자가 메세지 송신자의 신원을 확인할 수 있는 정보를 전송한다.

third root를 사용한 1-out-of-2 OT 프로토콜의 수행 절차는 다음과 같다.

- 파라메타 정의
  - p, q : 소수
  - $n = p \cdot q$, $y \in {Z_n}^*$(n, y : Bob의 공개키)
  - $k > 80$: 보안 변수(security parameter)
  - $y_i = H(y+1) \pmod n$ (H : One way hash function)
  - $x_i = {y_i}^{1/3} \pmod n$ $(i = 1, 2, \cdots, k)$ (Bob의 비밀키)
  - C_i : C의 i번째 비트
  - S, t : 메세지(m)에 대한 서명

[단계 1] Bob은 소수(p, q)를 선택하여 $n = p \cdot q$를 계산하고 ${Z_n}^*$ 상의 임의의 값(y)을 선택하여 메세지(m)에 서명을 하

기 위해 Z_n^*상에서 랜덤하게 r을 선택하고 $t = r^3 \pmod n$을 계산한 후 $C_i = H(t \| m)$을 계산하고, 서명$(S) = r\Pi_{i=1}^{k} x_i^{C_i} \pmod n$을 계산한다.

[단계 2] Bob은 서명을 검증하기 위하여 $S^3 \stackrel{?}{=} t\Pi_{i=1}^{k} y_i^{C_i} \pmod n$을 계산한다.

1-out-of-2 불확정 전송 프로토콜은 Alice와 Bob 사이의 프로토콜로서 Bob은 Alice가 전송한 두 메세지(m_0, m_1) 중 하나를 선택하고 Bob은 Alice가 선택한 메세지가 무엇인지 알 수 없다. m_0와 m_1은 Alice가 전송한 메세지를 의미하고 C_i는 Bob이 선택한 비트이다. Fiat 1-out-of-2 불확정 전송 프로토콜은 TTP가 선택 비트를 결정하는 프로토콜이다.

(3) Fiat 1-out-of-2 불확정 전송 프로토콜의 수행 절차는 다음과 같다.

- 파라메타 정의
  - $g \in QR_{n_j}$: 큰 위수를 갖는 Quadratic Residue
  - $h \in QNR_{n_j}$: Z_n^*에서 Jacobi symbol을 가지는 Quadratic Non-Residue
  - p_j, q_j : 소수, $n_j = p_j \cdot q_j$
  - E : Alice의 메세지 전송에 사용하는 암호화 함수(공개)
  - D : Alice의 메세지 전송에 사용하는 복호화 함수(비밀)

평방잉여가설에 의해 Alice는 Bob이 m_0, m_1 중 어느 것을 취했는지 알 수 없다. TTP는 t가 Z_n^* 상에서 quadratic residue 인지를 확인함으로써 C를 쉽게 계산할 수 있다.

Diffie-Hellman 가정에 의해 Bob은 k_{1-c}을 계산할 수 없기 때문에 m_{1-c}를 계산할 수 없다.

[단계 1] Bob은 $r \in Z_{n_j}$을 랜덤하게 선택 하고 $t = g^r h^c \pmod{n_j}$을 계산하여 결과 값(t)을 Alice에게 전송한다.

[단계 2] Alice는 $\alpha \in Z_{n_j}$을 선택하고 $A = g^{\alpha} \pmod{n_j}$, $k_0 = t^{\alpha} \pmod{n_j}$, $k_1 =, (th^{-1})^{\alpha} \pmod{n_j}$, $y_0 = E(m_0, k_0)$, $y_1 = E(m_1, k_1)$을 계산한 후 Bob에게 결과값(A, y_0, y_1)을 전송한다.

[단계 3] Bob은 $k_c = A^r \pmod{n_j}$, $m_c = D(y_c, k_c)$을 계산하여 메세지를 얻는다.

이 절에서 설계한 사전 계산에 의한 검증 가능한 비대화형 불확정 전송 프로토콜을 적용한 공정한 은닉 서명 프로토콜의 수행 절차는 다음과 같다.

[단계 1] Bob은 $r_1, r_2, \cdots, r_k \in Z_n^*$을 선택하고 $t = \Pi_{i=1}^{k} r_i^3 \pmod n$를 계산한 후 Alice에게 전송한다.

[단계 2] Alice는 랜덤하게 $\alpha \in Z_n^*$을 선택한 후 $t' = t\alpha^3 \pmod n$, $C_i = H(t' \| m)$을 계산한다(C_i는 C의 i번째 비트).

[단계 3] 이 단계를 k회 수행한다.

[단계 3-1] Alice는 랜덤하게 $r' \in Z_{n_j}$을 선택하고 $\rho = g^{r'} h^{c_i} \pmod{n_j}$을 계산해서 Bob에게 전송한다.

[단계 3-2] Bob은 $\alpha' \in Z_{n_j}$, $r'' \in Z_n^*$을 선택한 후 다음을 계산한다.

$A = g^{\alpha'}$, $k_0 = \rho^{\alpha'}$,

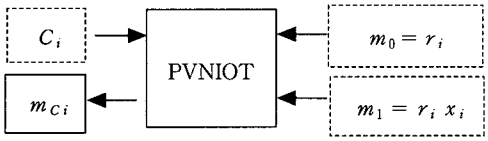
$k_1 = (\rho h^{-1})^{\alpha'}$, $M_0 = E(m_0, k_0)$,

$M_1 = E(m_1, k_1)$

〈표〉 공정한 은닉 서명, VNIOT를 적용한 공정한 은닉 서명과 PVNIOT를 적용한 공정한 은닉 서명 프로토콜 비교

비 교 내 용	공정한 은닉 서명	VNIOT을 이용한 공정한 은닉 서명	PVNIOT을 이용한 공정한 은닉 서명
양자 부정행위 가능성	많 음	적 음	적 음
프로토콜 중간 과정에서의 송신 사실의 검증	불가능	가 능	가 능
송신 사실 추후 부인 해결 가능성	있 음	없 음	없 음
사후 분쟁 해결 가능성	적 음	적 음	적 음
통신량 및 계산량	많 음	많 음	적 음

[단계 3-3] Alice와 Bob은 앞 절에서 설계한 PVNIOT의 [온라인 단계]를 실행한다.



[단계 3-4] Alice는 Bob의 부정을 탐지하여 메시지가 올바르다면 $k_{C_i} = A^r \pmod{n_j}$을 계산하고 $m_{C_i} = D(M_{C_i}) = D(m_{C_i}, k_{C_i})$ 계산함으로써 M_{C_i}를 복호화한다.

[단계 4] Bob은 $S' = \alpha \Pi_{i=1}^{k} S_i \pmod{n}$을 계산하여 서명($S'$)을 얻는다. 이때 쌍($S'$, t')은 메시지(m)의 서명이다.

$$S'^3 = t' \cdot \Pi_{i=1}^{k} y_i^{c_i} \pmod{n}$$

● 프로토콜 분석

사전 계산에 의한 검증 가능한 비대화형 불확정 전송 프로토콜을 이용한 공정한 은닉 서명 기법은 사용자에 대한 익명성과 공평성, 검증 가능성, 안전성을 따른다. 이 절에서 적용한 사전 계산에 의한 검증 가능한 비대화형 불확정 전송 프로토콜의 특성에 의해서 Alice는 서명에 부정이 발생했을 경우 TTP에게 중재를 의뢰하고 TTP는 Bob의 난수(r'')를 요구함으로써 의뢰된 서명을 검증할 수 있다.

TTP가 Alice에게 난수(r')를 요구할 때 Alice가 이를 거절한다면 자신의 부정을 인정하는 결과가 되므로 거부할 이유가 없다. Alice는 자신의 비밀키로 암호화되어 있으므로 송신을 부인할 수 없으며, Bob에게서 정보를 받았을 때만 자신의 키로 서명된 정보를 TTP에게 제시하고 TTP에 등록된 A_0, A_1, C_0, C_1을 검색함으로써 수신을 부인할 수 없다. 위의 <표>는 기존의 공정한 은닉 서명 프로토콜, 검증 가능한 비대화형 불확정 전송 프로토콜을 적용한 공정한 은닉 서명 프로토콜과 사전 계산에 의한 검증 가능한 비대화형 불확정 전송 프로토콜을 적용한 공정한 은닉 서명 프로토콜을 비교한 것이다.

5. 결론 및 향후 연구 방향

통신망을 통한 다양한 데이터 전송이 가능해지면서, 목적에 맞는 유용한 정보통신 서비스의 요구가 더욱 확대되고 있다. 그런데, 일상생활에서 일어나는 여러 활동들을 통신망을 통해 제공할 경우, 정보와 정당한 사용자의 보호를 위한 안전성에 대한 문제는 기존의 단순한 정보와 사용자에 대한 안전성(secrecy) 및 인증(authenti-

cation)이외에도 보다 세분화된 새로운 안전성 문제가 대두되는 것이다. 따라서 안전성과 신뢰성을 바탕으로 한 공평성, 익명성, 동시성 등 정보화 사회가 요구하는 새로운 안전 요구사항에 대한 해결책이 요구되고 있다.

이 논문에서는 Lein 등이 제안한 검증 가능한 불확정 전송 프로토콜(VNIOT)은 대화형 전송 방식을 사용하고 있기 때문에 통신량이 많이 발생한다. 이러한 문제점을 해결하기 위하여, 기존에 제안된 NIOT 방식[7, 8]과 VNIOT 방식으로 발전하였다. 또한 TTP에게 내용은닉 서명을 받음으로써 송수신 부인봉쇄 기능을 갖는 더욱 안전한 VNIOT 방식에서 발생하는 전송량과 계산량을 줄이기 위하여 제안한 사전 계산 능력을 갖는 검증 가능한 불확정 전송 프로토콜 분석 및 안전성을 분석하였다.

부인봉쇄 기능을 갖는 검증 가능한 비대화형 불확정 전송 프로토콜에서는 Bellare와 Micali 등이 제안한 NIOT의 키생성 및 프로토콜[7] 절차를 따랐으며, 검증 가능한 비대화형 불확정 전송 프로토콜에서의 기능상의 문제점들을 TTP와의 보증정보를 보완하여 부정행위 탐지 기능을 강화함으로써 부정행위의 가능성을 배제하였다. 또한 TTP가 모든 비밀을 보유하고 있기 때문에 송수신 사실을 사후에 보인할 수 없도록 송수신 부인봉쇄 기능을 갖도록 확장하여, 사후 분쟁 해결을 할 수 있도록 기능을 강화함으로서 두 방법의 장점과 안전성을 모두 포함하도록 하였다.

불확정 전송 프로토콜은 그 자체만으로는 통신량이나 계산량이 그리 많지 않지만 각 응용 프로토콜에 적용될 경우, 이 서브 프로토콜이 수 회 이상 반복되어야 하므로 엄청난 통신량의 증가를 야기한다.

이러한 문제를 해결하기 위하여 설계한 사전 계산 기능을 갖는 검증 가능한 비대화형 불확정 전송 프로토콜을 제안하였다.

향후에는 이 논문의 연구를 바탕으로 송신자(A)와 수신자(B)와 TTP와의 통신량과 계산량을 최소화하기 위한 효율성에 대한 연구와 다양한 환경에 적용 가능한 연구가 요구된다.

이 논문에서는 PVNOIT를 실제 서명 프로토콜에 적용함으로써 공정한 은닉 서명의 참가자인, 서명자와 발신자 사이의 부인봉쇄 기능을 추가했다. 그러나 부인봉쇄 기능을 추가함으로써 서명자와 발신자는 강력한 계산 능력을 갖아야 하는 문제점이 발생한다. 향후 PVNOIT 참가자의 계산량을 최소화 하는 문제와 PVNOIT가 수회 이상 반복됨으로써 발생하는 통신량 문제에 관한 연구가 이루어져야 할 것이다.

참 고 문 헌

[1] Rabin, M., "How to Exchange Secret by Oblivious Transfer", harvard Center for Research in computer Technology, Cambridge, Mass., 1981.

[2] M, Blum, "How to Exchange Secret Keys", ACM Transaction Compute System, pp.175-193, May 1983.

[3] T. Tedrick, "How to Exchange half a Bit", Proceedings of Crypto'83, pp.147-151, 1983.

[4] R. Berger, R. Peralta and T. Tedrick, "A Provably Secure Oblivious Transfer Protocol", Proceedings of Crypto'84, pp.379-386, 1984.

[5] T. Tedrick, "Fair Exchange of Secrets", Proceedings of Crypto'84, pp.434-438, 1984.

[6] 김상춘, 오영실, 이상호, "부인봉쇄 기능을 갖는 불확정 전송", 정보과학회 논문지(A), 제26권, 제3호, 1999. 3.

[7] M. Bellare and S. Micali, "Non-Interactive Oblivious Transfer and Applications", Advanced in Cryptology : CRYPTO '89, pp.547-557, 1989.

[8] Lein Harn and Hung-Yu Lin, "Non-Inter-

active Oblivious Transfer", Electronic Letters, Vol.26, No.10, pp.635-636, 1990.

[9] L. Harn and Hung-Yu Lin, "An Oblivious Transfer Protocol and its Application for the Exchange of Secrets", ASIACRYPTO'91, pp. 187-190, 1991.

[10] W. Diffie and M. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory IT-22, pp.644-654, November 1976.

[11] D. Chaum, "Blind Signatures for Untraceable Payments", Advances in Cryptology : Proceedings of CRYPTO '82, Plenum Press, pp.199-203, 1982.

[12] Chaum, "Blind Signatures for Untraceable Payments", Advances in Cryptology : Proceedings of CRYPTO'82, Plenum Press, pp. 199-203, 1982.

[13] M. Stadler, J. Marc Piveteau, J. Camenisch, "Fair Blind Signatures", Advances in Crtpyology EUROCTYPYO '95 Springer-verlag, pp.209-219, 1995.

김 상 춘

1986년 한밭대 전자계산학과 (공학사)

1989년 청주대 전자계산학과 (공학석사)

1999년 충북대 전자계산학과 (이학박사)

1983년~2001년 한국전자통신연구원 정보보호기술연구본부(선임기술원)

2001년~현재 삼척대학교 정보통신공학과 조교수

권 기 현

1993년 강원대 전자계산학과 (이학사)

1995년 강원대 전자계산학과 (이학석사)

2000년 강원대 컴퓨터과학과 (이학박사)

1998년~2002년 동원대학 인터넷 정보과 조교수

2002년~현재 삼척대학교 정보통신공학과 전임강사

관심분야 : 분산 소프트웨어, 임베디드 소프트웨어, 데이터마이닝, 정보보안