Bit Commitment와 디지털 서명을 이용한 대화형 불확정 전송 프로토콜

정회원 김 순 곤*, 송 유 진**, 강 창 구***, 안 동 언****, 정 성 종****

Interactive Oblivious Transfer Protocol using Bit Commitment and Digital Signature

S.G.Kim*, Y.J.Song**, C.G.Kang***, D.U.An****, S.J.Chung**** *Regular Members*

요 약

본 논문에서는 공평한 비밀정보 교환을 위한 기본 프로토콜인 불확정전송 프로토콜을 제안한다. 이를 위해 Lein Harn등이 앞서 제안한 이산대수문제에 기반을 둔 검증가능 불확정전송방식에 대하여 고찰하고 기존의 방식에다 부가적인 기능을 가지는 새로운 불확정전송 프로토콜을 제안한다. 이들의 방식에서 고려하지 않았던 송신자 확인 및 송신자의 송신사실 사후 부인방지등의 여러 기능이 부가된 대화형 불확정전송 프로토콜을 제안한다. 이를 위해 Bit Commitment 기법을 이용하는 방법과 RSA에 기반한 디지털서명기법을 이용하는 두 가지 방법을 제안한다.

ABSTRACT

In this paper, we present an oblivious transfer protocol which is the basic protocol for the fair exchange of secrets. For this, we investigate the verifiable oblivious transfer protocol based on discrete logarithm problem proposed by Lein Harn etc. And we propose a new oblivious transfer protocol that has the additional functions on the existing method. This proposed method has the additional functions that enable to authenticate sender and to protect denial of what he/she has sent message to the other. To do this, we make use of bit commitment scheme and digital signature scheme based on RSA.

I. 서 론

암호화 프로토콜을 분산환경에서 실현가능하게 하려면 합법적인 사용자에 대한 안전한 통신채널을 확보하는 것과 더불어 암호화 프로토콜의 기본도구로서 공평한 비밀정보 교환을 위한 불확정 전송기법(OT : Oblivious Transfer)에 대한 연구가 요구된다.

여러 사람이 각자 비밀정보를 갖고 있고 이들 비밀정보를 서로 공평하게 교환할 수 있는 방법은 암호화 프로토콜에서 중요한 문제이다. 특히 계약 혹은 합의문서에 서명할 때 어느 한쪽이 자신의 서명을 먼저 보냄으로써 야기될 수 있는 문제점이 있을 수 있다. 이러한 문제점을 해결하기 위해서 공평한 비밀정보 교환에 관한 연구가 되어왔다[1]-[7], [9]-[11], [16]-[20], [22]-[25]

불확정 전송의 기본개념은 Rabin[1]에 의해서 처음으로 소개되었으며 일반적으로 암호 프로토콜을 설계하기 위한 기본적인 도구로서 유용하게 쓰이는 프로토콜이다. 일반적인 암호화 프로토콜에서 비밀을 보장하면서 그것에 관련한 임의의 정보를 보내야 되는 경우 OT 프로토콜이 유용하다.

서로 상대방을 신뢰하지 못하면서 비밀정보를 교

* 중부대학교 정보공학부
** 동국대학교 정보산업학과
*** 한국전자통신연구원 부호 3팀
**** 전북대학교 컴퓨터공학과
논문번호 : 99029-0128, 접수일자 : 1999년 1월 28일
※ 이 논문은 1998년도 중부대학교 학술연구개발비 지원에 의하여 이루어진 것임.

환하기를 원하는 두 당사자 영희와 철수가 있다고 가정한다. 두 사람간에 있어서 비밀정보의 공평한 교환은 다음과 같은 프로토콜에 의해서 수행될 수 있다.

두 사람 영희와 철수가 비트길이 m인 두 개의 비밀정보를 각각 가지고 있을 때 영희와 철수는 1-out-of-2 OT에 의해 두 개의 비밀정보를 불확정 전송한다. 철수는 영희의 두 개의 비밀정보 중에서 정확히 한 개의 비밀정보를 알게되고 영희는 철수가 자신의 비밀정보 중에서 어떤 것을 알고 있는지 모른다. 즉, OT 프로토콜은 영희가 철수에게 어떤 비밀을 보내고자 할 때, 철수가 그 비밀을 1/2의 확률로 취할 수 있게 하고 영희는 철수가 그 비밀을 취했는지의 여부를 1/2의 확률로 추측할 수 있게 하는 프로토콜이다. 물론 철수가 그 비밀을 취했다면, 철수는 그 비밀의 내용을 알 수 있게 된다. 여러 비밀에 대해서도 OT를 확장 적용할 수 있다.

또한 OT는 양자간의 비밀정보 교환이 대화 형식인지의 여부에 따라 대화형 불확정 전송(IOT: Interactive OT), 비대화형 불확정 전송(NIOT: Noninteractive OT)으로 분류할 수 있다. 대화형 불확정 전송은 송수신자간에 자기의 정보에 대한 몇번의 상호교환을 통하여 이루어지며 이렇게 프로토콜의 전개가 대화형식으로 진행될 때를 IOT라 한다. NIOT는 프로토콜의 전개가 대화형식이 아니다. 즉 송신자에 의한 수신자로의 통신만이 존재한다. 이런 경우, 송수신자 간에 통신회수는 줄어들며 실제의 응용에 있어서 OT를 사용할 때 OT에 의한 통신로의 과부하를 줄일 수 있다. 그러나 NIOT는 송수신측의 계산 능력에 의존하기 때문에 IOT와 비교 했을 때, 계산 소요시간이 길어지는 점도 있다.

본 논문에서는 공평한 비밀정보 교환을 위한 기본프로토콜인 불확정 전송의 개념을 살펴보고 검증가능 대화형 불확정 전송 프로토콜을 분석하고, 새로운 대화형 불확정 전송 프로토콜을 제안한다. 제안하는 방식은 기존의 방식에다 부가적인 기능을 갖도록 확장하였다.

본 논문은 5 개의 장으로 구성된다. 제 1 장에서는 불확정 전송의 기본 개념을 살펴보고, 제 2 장에서는 불확정 전송의 기존방식 중 검증가능 불확정 전송 및 본문에서 적용한 기법에 대하여 살펴본다. 제 3 장에서는 새로운 대화형 불확정 전송 프로토콜을 제안하고, 제 4 장에서는 제안방식의 특성을 비교하고 고찰한 다음 마지막으로 제 5 장에서 결론을 맺는다.

Ⅱ. 불확정 전송 기법과 비밀정보의 교환

2.1 검증가능 불확정 전송 및 적용기법

본 논문에서는 Lein Harn 등이 제안한 이산대수 문제에 기반을 둔 대화형 불확정 전송 방식[6]에 대하여 고찰하고, 이 방식에서 고려하지 않았던 문제에 대하여 언급하고 그 확장방안을 제안 한다.

2.1.1 검증가능 불확정 전송(Verifiable Oblivious Transfer)[6]

(가정)

◦ 영희와 철수는 서로 상대방을 신뢰하지 못하면서도 비밀정보를 교환하고자 하는 두 당사자이다.

◦ p는 큰 소수(prime number)이고 p' 또한 소수이다.

◦ $p=4*p'+1,\ p=1 \bmod 4$

◦ ϵ는 p의 Galois Field 의 원시 원소(Primitive element)이다.

◦ p와 ϵ는 영희와 철수에게 공개되어 있다.

◦ 영희는 자신만의 비밀 α 를 선택한다.

◦ α 는 다음과 같은 성질을 갖는다.

$$\text{“}\alpha\text{”} \rightarrow \begin{cases} \gcd(\alpha, p-1)=1 \\ \alpha \in QNR_p \ (p\text{의 평방 비잉여}) \end{cases}$$

◦ 영희는 공증정보인 A_s와 A_{1-s},p, ϵ를 신뢰할 수 있는 제3자(TTP: Trusted Third Party)에 의뢰한다. 이때 $s \in \{0,1\}$이고 s는 영희만이 알고 있다.

(프로토콜)

<단계 1> 철수는 비밀번호 b (b는 gcd(b,p-1)=1인)를 임의로 선택해서 C_1을 아래와 같이 계산한 다음 영희에게 보낸다.

$$C_1 = A_0^b \bmod p \text{ or } C_1 = A_1^b \bmod p$$

<단계 2> 영희는 다음 계산을 해서 철수에게 보낸다.

$$C_2 = C_1^{\alpha^{-1}} \bmod p$$

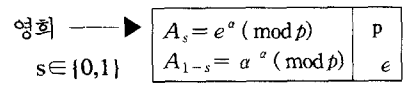
<단계 3> 철수는 C_3을 계산한다.

$$C_3 = C_2^{b^{-1}} \bmod p$$

만약 $C_3 = \epsilon$ 라면 철수는 영희의 비밀에 대해서는 아무 것도 모른다.

$C_3 = \alpha$ 라면 철수는 영희의 비밀을 알게된다. 둘 다 아니라면 철수는 영희의 부정행위를 처벌할 수 있다.

이를 그림으로 표현하면 다음 그림 1과 같다.



	(영회)		(철수)
단계 1		←C1-	b를 임의로 선택 (gcd(b,p-1)=1) C_1을 계산 $C_1 = A_0^{\,b} \bmod p$ or $C_1 = A_1^{\,b} \bmod p$
단계 2	$C_2 = C_1^{\,a^{-1}} \bmod p$ 를 계산	-C2-▶	
단계 3			C_3를 계산 $C_3 = C_2^{\,b^{-1}} \bmod p$ C_3가 e이면 철수는 비밀을 얻지 못하고 C_3가 α이면 철수는 비밀을 얻고 그 외의 경우라면 철수는 영회의 부정행위를 고발가능

그림 1. 검증가능 불확정 전송 프로토콜

2.1.2 Bit Commitment 프로토콜

Bit Commitment 프로토콜은 서로 상대편을 신뢰하지 못하는 두 당사자 사이에 비밀정보를 공평하게 교환하기 위한 강력하고 유용한 암호화 응용프로토콜 도구중의 하나이다.

영회가 철수에게 어떤 비밀 내용을 맡기고 싶지만, 일정기간이 지나기 전까지는 그 내용을 알리고 싶지 않고, 한편 철수는 영회가 비밀내용을 자신에게 맡긴 뒤 그 내용을 변화시킬 수 없기를 바라는 경우 Bit Commitment 프로토콜을 사용하게 된다. 이것은 다음의 두 단계로 이루어진다.

(Commitment 단계)

영회는 철수에게 맡기고 싶은 비트 m이 있다. 영회와 철수는 메시지를 교환하고 이 단계가 끝나면 철수는 m을 나타내는 정보를 가지게 된다.

(Reveal 단계)

이 단계에서 철수는 m의 값을 알게 된다.

이러한 Bit Commitment 프로토콜은 사용하는 암호화방식에 따라서 대칭적 암호방식을 이용한 Bit Commitment 방법[12]과 일방향함수를 이용한 Bit Commitment방법[12]과 의사난수 생성기를 이용하는 Bit Commitment방법[13],[14]등이 있는데 본 논문에서는 일방향함수를 이용한 Bit Commitment방법에 관하여 살펴보고 이를 적용한다.

• 일방향함수를 이용한 Bit Commitment

서로 신뢰하지 못하는 두 당사자 영회와 철수가 있다. 영회는 철수에게 비밀정보(하나 혹은 여러 개의 bit)를 맡기고자 한다. 이때 영회는 그 비밀정보의 내용을 일정기간이 지나기 전까지는 철수에게 알리고 싶지 않다. 한편 철수는 영회가 비밀정보를 자신에게 맡긴 후 그 비밀정보의 내용을 변화시킬 수 없기를 바라는 상황이라고 가정한다.

(Commitment 단계)

<단계 1>

· 영회는 임의의 비트 스트링 두 개(R_1과 R_2)를 생성한다 : R_1, R_2

<단계 2>

· 영회는 <단계 1>에서 생성한 두 개의 비트 스트링과 그녀가 맡기고자 하는 비밀정보 b(하나 혹은 여러 개의 비트 가능)로 구성되는 하나의 메시지를 생성한다 : (R_1, R_2, b)

<단계 3>

· 영회는 <단계 2>에서 생성된 메시지에 일방향함수(H)를 적용하여 계산한 결과를 두 개의 임의 비트 스트링 중 하나(R_1)와 같이 철수에게 전송한다.

H(R_1, R_2, b), R_1

(Reveal 단계)

<단계 4>

· 영회는 철수에게 본래의 메시지와 일방향함수를 전송한다 : (R_1, R_2, b), H

<단계 5>

· 철수는 받은 메시지에 일방향함수를 적용하여 계산하고 그 계산결과와 R_1을 <단계 3>에서 받은 계산결과와 임의 스트링(R_1)과 비교한다.

· 이때 그들이 일치하면 그 비밀정보는 유효한 것이다.

2.1.3 디지털 서명

(1) 공개키 암호 시스템의 디지털 서명.

공개키 암호 시스템은 암호화할 때 사용하는 공개키(public key)와 복호화할 때 사용하는 비밀키(private key)를 다르게 작성하여, 공개키는 공개하고 비밀키만을 안전하게 보관 유지하는 방식이다. 예를 들면 영수에게 비밀통신을 하고자 하는 사람이 있다면 누구든지 영수가 공개한 영수의 공개키를 이용하여 보내고자하는 내용을 암호화하여 영수에게 전송하면 영수는 자신만이 가지고 있는 비밀키를 이용하여 암호문을 복호화 하는 것이다.

공개키 암호 시스템의 특징으로는 다음과 같은 세 가지로 요약할 수 있다. 첫째, 키를 분배할 필요가 없고, 둘째, 관리할 키의 개수가 관용키 암호 시스템에 비하여 적으며 셋째, 디지털 서명이 가능하다는 점이다.

공개키 암호 시스템에서 일반적인 서명의 특징을 만족시키면서 전자적으로 서명을 실현시킬 수 있는 방법이 있는데 이는 다음과 같다. 즉 영희가 철수에게 서명이 부가된 메시지 M을 전송하려고 하면, 영희는 자신의 비밀키를 가지고 M을 암호화한 후 철수에게 메시지 M과 M의 암호문을 전송한다. 철수는 영희의 공개키를 이용하여 M의 암호문을 복호화 한 다음 이것이 M과 같은지 비교하여 영희의 신원확인을 한다. 이때 M의 암호문은 영희만이 생성할 수 있으며, 영희의 공개키를 이용하여 누구든지 영희가 전송한 것임을 확인할 수 있으므로 서명으로 간주할 수 있다.

(2) RSA 암호 시스템

Rivest, Sharmir, Adleman은 1978년 소인수분해의 어려움에 근거한 공개키 암호화 시스템인 RSA 암호화 시스템을 제안하였는데 이 암호시스템을 간단히 살펴본다.[15]

RSA 암호시스템은 매우 큰 정수의 소인수분해가 어렵다는 가정하에서 설계된 것으로 이 시스템의 구성은 다음과 같다.

(i) 두 개의 큰 소수 p와 q를 생성하여 n = p q를 계산한다.

(ii) Euler 함수값 $\varnothing(n)=(p-1)(q-1)$과 서로소가 되는 e를 계산한다 : $(\gcd(e,\varnothing(n))=1)$

(iii) $\varnothing(n)$과 e로부터 유클리드 알고리즘을 이용하여 $ed\equiv 1(\mathrm{mod}\,\varnothing(n))$ 가 되는 d를 계산한다.

이로부터 다음과 같은 공개키 암호 시스템을 구성한다.

* 공개키 : n, e
* 비밀키 : p, q, d
* 메시지 공간 = $\{ M\in Z \mid 0\le M< n-1\}$
* 암호화 : $C=E(M)\equiv M^e \pmod n$
* 복호화 :

$$M=D(C)=D(E(M))\equiv C^d \bmod n\equiv M^{ed} \bmod n$$

(3) 디지털 서명

공개키 암호시스템의 공통적인 특징은 송신자의 신원 확인이 어려우며, 따라서 별도의 방법을 통하여 신원 확인을 하여야 한다. RSA 시스템에서는 다음과 같은 방법으로 신원확인이 가능하다.

영희가 철수에게 영희의 서명이 포함된 암호문을 보낸다고 할 때 :

영희의 공개키를 $E_A=\{n_A, e_A\}$, 철수의 공개키를 $E_B=\{n_B, e_B\}$ 라하고, 영희의 비밀키를 $D_A=\{p_A, q_A, d_A\}$, 철수의 비밀키를 $D_B=\{p_B, q_B, d_B\}$ 라 하자.

영희는 보내고자 하는 메시지 M_A를 자신의 비밀키와 철수의 공개키를 이용하여

$C_A\equiv (M_A^{d_A} \bmod n_A)^{e_B} \bmod n_B$ 를 계산후 이 C_A를 철수에게 전송한다.

철수는 수신한 C_A를 자신의 비밀키를 이용하여 S_A를 계산한 후 영희의 공개키를 이용하여 다음과 같이 M_A를 계산한다.

$$S_A\equiv C_A{}^{d_B} \pmod{n_B} \quad M_A\equiv S_A{}^{e_A} \pmod{n_A}$$

즉 다음과 같이 메시지 M_A를 복호화 한다.

$$M_A\equiv((C_A{}^{d_B} \bmod n_B)^{e_A}) \bmod n_A$$

이때 영희의 비밀키는 영희이외의 사람은 알 수 없으므로 영희의 신원 확인이 가능하다. 또한 수신자 자신을 포함하여 영희이외의 어떤 사람도 S_A를 위조할 수 없으므로 철수는 S_A를 보유하고 있음으로써 영희가 나중에 메시지 M_A를 철수에게 보냈다는 사실을 부정할 수 없도록 한다.

Ⅲ. 제안한 방법

3.1 Bit Commitment을 이용한 OT (제안기법 1)

기존의 검증가능 불확정전송 프로토콜은 공정성, 검증가능성 및 안전성을 가진다. 본 논문에서는 기존의 프로토콜을 분석한 결과 기존의 프로토콜에서 고려하지 않았던 다음과 같은 사항을 고려하여 새로운 대화형 불확정전송 프로토콜을 제안하였다.

기존 프로토콜 과정 중에서는 송신자의 신원확인 및 송신자의 송신사실의 사후부인 방지에 관한 내용이 고려되어 있지 않았다. 따라서 송신자가 송신사실을 사후에 부인할 수 없도록 하는 문제에 관한 보완방법이 필요하였다. 이를 위하여 본 논문에서는 두 가지 암호기법을 이용하였다. 첫 번째 방법으로 제Ⅱ장에서 전술한 바 있는 일방향 함수를 적용한 Bit Commitment기법을 이용하였다. 공증정보와 Bit Commitment 기법을 이용하여 기존의 검증가능 불

확정 전송에서 고려하지 않은 송신자의 신원확인과 송신자의 송신사실사후부인 방지의 부가적인 기능을 갖도록 기존 방법을 확장하였다.

3.1.1 제안방식의 개요

먼저 그 파라미터를 살펴보면 R_1, R_2는 철수가 생성하는 두 개의 임의의 비트 스트링이고 R_{11}, R_{22}는 영희가 생성하는 두 개의 임의의 비트 스트링이다. H_1은 철수가 사용하는 일방향 함수이고 H_2 는 영희가 사용하는 일방향 함수이다. 또, HR_1은 철수가 일방향함수 H_1을 메시지(R_1, R_2, C_1)에 적용하여 계산한 결과이고 HR_{11}은 영희가 철수가 보내온 일방향함수 H_1을 메시지(R_1, R_2, C_1)에 적용하여 계산한 결과이다. HR_2는 영희가 일방향함수 H_2를 메시지(R_{11}, R_{22}, C_2)에 적용하여 계산한 결과이고 HR_{22}는 철수가 영희가 보내온 일방향함수 H_2를 메시지(R_{11}, R_{22}, C_2)에 적용하여 계산한 결과이다.

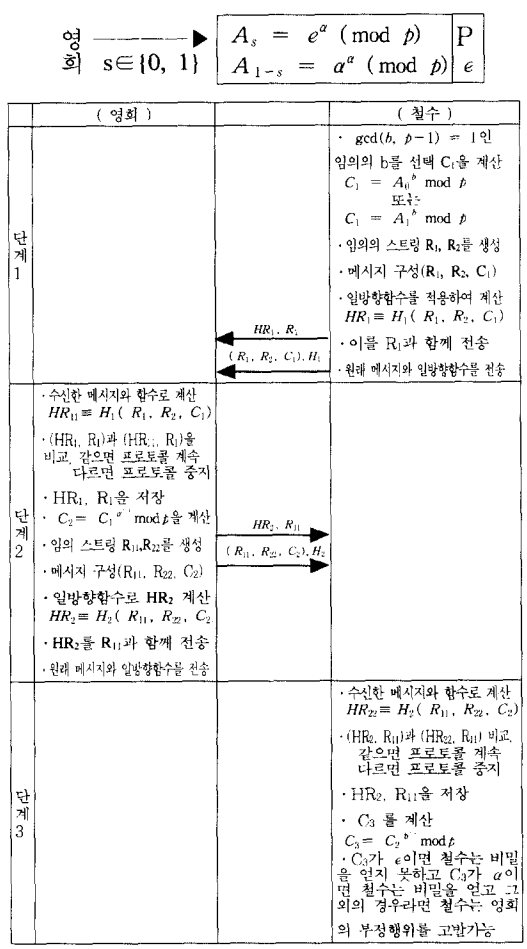


그림 2. Bit commitment를 이용한 확장된 불확정전송기법

제안한 프로토콜의 개념도를 살펴보면 다음 그림 2와 같다.

3.1.2 프로토콜 설명

제안방식의 프로토콜 전개 순서를 살펴보면 다음과 같다.

· 영희가 철수에게 비밀정보를 불확정 전송하고자 할 때 기존 프로토콜의 순서를 그대로 따르면서 일방향함수를 적용한 Bit Commitment 기법만 추가된 형태이다.

· 철수가 영희에게 비밀정보를 불확정전송하고자 할 때는 영희가 철수의 역할을 대칭적으로 바꾸면 된다.

<사전준비 단계>

영희와 철수는 신뢰할 수 있는 제3자 (TTP)에 일방향함수 H_1과 H_2를 사전에 등록한다.

<단계 1>

· 철수는 gcd(b, p-1)=1인 비밀번호 b를 임의로 선택해서 C_1을 다음과 같이 계산한다.

$$C_1 \equiv A_0^b \pmod p \text{ 또는 } C_1 \equiv A_1^b \pmod p$$

· 철수는 두 개의 임의의 비트 스트링 R_1과 R_2를 생성한다 : R_1, R_2

· 철수는 R_1, R_2와 C_1으로 하나의 메시지를 구성한다 : (R_1, R_2, C_1)

· 철수는 그 메시지에 일방향함수를 적용하여 다음을 계산한다 : $HR_1 \equiv H_1(R_1, R_2, C_1)$

그리고 그 결과와 두 개의 스트링 중의 하나를 (여기서는 R_1) 영희에게 전송한다 : (HR_1, R_1)

· 철수는 원래의 메시지와 일방향함수를 영희에게 전송한다 : (R_1, R_2, C_1), H_1

<단계 2>

· 영희는 수신한 메시지에 수신한 일방향함수를 이용하여 계산한다 : $HR_{11} \equiv H_1(R_1, R_2, C_1)$

· 이 계산 결과치(HR_{11}, R_1)와 <단계 1>에서 먼저 수신한 (HR_1, R_1)을 서로 비교한다.

· 이들이 서로 일치하면 프로토콜을 계속하고, 일치하지 아니하면 프로토콜을 즉시 중지한다.

· 분쟁시 철수의 송신사실사후부인방지를 위해서 HR_1과 R_1을 저장한다.(이는 영희에게 메시지를 전송했다는 증거가 된다)

· 영희는 자신의 비밀 α 를 이용하여 C_2를 계산한다 $C_2 \equiv C_1^{\alpha^{-1}} \pmod p$

· 영희는 두 개의 임의의 비트 스트링을 생성한다 : R_{11}, R_{22}

· 영희는 R_{11}, R_{22}와 C_2로 하나의 메시지를 구성한다 : (R_{11}, R_{22}, C_2)

· 영희는 그 메시지에 자신의 일방향함수를 적용하여 다음을 계산한다 : $HR_2 \equiv H_2(R_{11}, R_{22}, C_2)$

· 영희는 계산한 결과치 HR_2와 두 개의 스트링 중 하나(여기서는 R_{11})를 철수에게 전송한다: (HR_2, R_{11})

· 영희는 원래의 메시지 (R_{11}, R_{22}, C_2)와 자신의 일방향함수 H_2를 철수에게 전송한다 : (R_{11}, R_{22}, C_2), H_2

<단계 3>

· 철수는 수신한 메시지에 수신한 일방향함수를 적용하여 계산한다 : $HR_{22} \equiv H_2(R_{11}, R_{22}, C_2)$

· 철수는 이 계산 결과치 (HR_{22}, R_{11})와 <단계 2>에서 먼저 수신한 (HR_2, R_{11})를 서로 비교한다.

· 이들이 서로 일치하면 프로토콜을 계속하고, 일치하지 않으면 프로토콜을 즉시 중지한다.

· 분쟁시 영희의 송신사실사후부인방지를 위해서 철수는 HR_2와 R_{11}을 저장한다.(이는 영희가 철수에게 메시지를 전송했다는 증거가 된다)

· 철수는 자신의 비밀번호 b를 이용하여 C_3를 계산한다 : $C_3 \equiv C_2^{b^{-1}} \pmod{p}$

· $C_3 = \epsilon$ 이면 철수는 비밀을 얻지 못하고

$C_3 = \alpha$ 이면 철수는 비밀을 얻고

그 외의 경우라면 철수는 영희의 부정행위를 고발 가능하다.

3.2 디지털 서명을 이용한 OT(제안기법 II)

검증가능 불확정전송에 대하여 기존 프로토콜의 공정성, 검증가능성, 안전성 등을 검토 분석한 결과 고려하지 않았던 프로토콜 과정중에서의 송신자의 신원확인 및 송신사실의 사후 부인 방지에 관한 내용에 대하여 공증정보(Notarized Information) 및 RSA를 기반으로한 디지털 서명기법을 이용하여 이를 해결할 수 있는 알고리즘을 추가함으로써 새로운 대화형 불확정전송기술을 설계하고 대화형 불확정전송 프로토콜을 확장하였다.

3.2.1 제안한 방식의 개요

사용된 파라미터를 살펴보면

M_A : 영희가 철수에게 보내는 메시지, M_B : 철수가 영희에게 보내는 메시지 , $\{ p_A, q_A, d_A \}$: 영희의 비밀키, $\{ n_A, e_A \}$: 영희의 공개키, $\{ p_B, q_B, d_B \}$: 철수의 비밀키, $\{ n_B, e_B \}$: 철수의 공개키, S_A : 영희가 보내는 메시지 M_A를 자신의 비밀키로 서명한 것, S_B : 철수가 보내는 메시지 M_B를 자신의 비밀키로 서명한 것이다.

RSA 암호를 이용한 디지털 서명과 공증정보를 이용하여 대화형 불확정 전송을 확장한 내용을 살펴보면 다음 그림 3과 같다.

영희→ $s \in \{0, 1\}$	$A_s = e^{\alpha} \pmod{p}$	p	$\{n_A, e_A\}$
	$A_{1-s} = \alpha^{\alpha} \pmod{p}$	ϵ	$\{n_B, e_B\}$

	(영희)		(철수)
	비밀키 : $\{p_A, q_A, d_A\}$ 메시지 : M_A		비밀키 : $\{p_B, q_B, d_B\}$ 메시지 : M_B
단계 1		(C_1, C_B, M_B) ←	b를 임의로 선택 C_1을 계산 $(\gcd(b, p-1) = 1)$ $C_1 = A_0^b \bmod p$ or $C_1 = A_1^b \bmod p$ · 암호화 C_B를 계산 $C_B \equiv (M_B^{d_B} \bmod n_B)^{e_A} \bmod n_A$
단계 2	· C_B를 복호화 M_B를 계산 $M_B \equiv (C_B^{d_A} \bmod n_A)^{e_B} \bmod n_B$ "S_B" · M_B 확인, S_B 보유 · C_2를 계산 $C_2 = C_1^{\alpha} \bmod p$ · M_A를 암호화 C_A를 계산 $C_A \equiv (M_A^{d_A} \bmod n_A)^{e_B} \bmod n_B$	(C_2, C_A, M_A) →	
단계 3			· C_A를 복호화 M_A를 계산 $M_A \equiv (C_A^{d_B} \bmod n_B)^{e_A} \bmod n_A$ "S_A" · M_A 확인, S_A 보유 · C_3를 계산 $C_3 = C_2^{b^{-1}} \bmod p$ · C_3가 ϵ이면 철수는 비밀을 얻지 못하고 C_3가 α이면 철수는 비밀을 얻고 그 외의 경우라면 철수는 영희의 부정행위를 고발가능

그림 3. 디지털서명을 이용한 확장된 불확정전송 기법

3.2.2 프로토콜 설명

제안방식의 프로토콜 전개순서를 살펴보면 다음과 같다.

· 영희가 철수에게 비밀을 검증가능 불확정 전송하고자 할 때 기존 프로토콜을 그대로 따르면서 공

개키를 이용한 서명 과정만 추가된 형태이다.

· 철수가 영희에게 비밀을 검증가능 불확정전송하고자 할 때는 영희와 철수의 역할을 대칭적으로 바꾸면 된다.

<단계 1>

· 철수는 비밀번호 b(b는 gcd(b, p-1)=1인)를 임의로 선택해서 C_1을 아래와 같이 계산한다.

$$C_1 = A_0^b (\bmod p) \text{ 또는 } C_1 = A_1^b (\bmod p)$$

· 철수는 영희에게 보낼 메시지 M_B를 자신의 비밀키와 영희의 공개키를 이용하여 암호화하여 C_B를 계산한다 : $C_B \equiv (M_B^{d_B} \bmod n_B)^{e_A} \bmod n_A$

· 철수는 (C_1, C_B, M_B)를 영희에게 보낸다.

<단계 2>

· 영희는 철수로부터 수신한 C_B를 자신의 비밀키를 이용하여 다음을 계산한다 :

$$S_B \equiv C_B^{d_A} (\bmod n_A)$$

이 S_B를 다시 철수의 공개키를 이용하여 M_B를 복호화 한다: $M_B \equiv S_B^{e_B} (\bmod n_B)$

· 철수가 보내온 M_B와 복호화한 M_B를 서로 비교 확인한다.

이때 확인 결과 일치하면 철수의 송신사실 사후 부인방지를 위해 S_B를 보유하고 프로토콜을 계속 진행하고, 일치하지 않으면 프로토콜을 즉시 중지한다.

· 영희는 자신의 비밀 α 로 C_2를 계산한다.

$$C_2 = C_1^{\alpha^{-1}}$$

· 영희는 철수에게 보낼 메시지 M_A를 자신의 비밀키와 철수의 공개키로 암호화하여 C_A를 계산한다: $C_A \equiv (M_A^{d_A} \bmod n_A)^{e_B} \bmod n_B$

· 영희는 (C_2, C_A, M_A)를 철수에게 보낸다.

<단계 3>

· 철수는 영희로부터 수신한 C_A를 자신의 비밀키를 이용하여 다음을 계산한다 : $S_A = C_A^{d_B} (\bmod n_B)$

이 S_A를 다시 영희의 공개키를 이용하여 M_A를 복호화 한다 : $M_A = S_A^{e_A} (\bmod n_A)$

· 철수는 영희가 보내온 M_A와 복호화한 M_A를 비교 확인한다.

이때 확인 결과 일치하면 영희의 송신사실 사후 부인 방지를 위해 S_A를 보유하고 프로토콜을 계속 진행하고, 일치하지 않으면 프로토콜을 즉시 중지한다.

· 철수는 C_3를 계산하여 프로토콜을 완성시킨다.

$$C_3 = C_2^{b^{-1}} (\bmod p)$$

· C_3가 ε이면 철수는 비밀을 얻지 못하고 C_3가 α 이면 철수는 비밀을 얻고 그 외의 경우라면 철수는 영희의 부정행위를 고발 가능하다.

Ⅳ. 제안한 방식의 특성비교 및 고찰

4.1 개요

제안한 Bit Commitment를 이용한 불확정전송 기법 및 디지털 서명을 이용한 불확정전송 기법과 기존의 검증가능 불확정전송 기법의 특성을 비교 분석한다. 표 1에서는 각 기법의 특성을 근본적 기본문제(Primitive Problem), 서명기법, 공정성, 검증가능성, 안전성, 송신자 확인 가능성, 송신사실 부인방지 기능 측면에서 비교 분석한다.

표 2에서는 기존의 기법과 제안한 기법들의 프로토콜 실행중의 특성메시지 노출가능성, 송수신자 부정행위(cheating)가능성, 프로토콜 실행과정에서의 메시지 송신사실의 검증가능성, 송신사실 부인가능성, 분쟁시 사후 해결가능성, 프로토콜 실행중 송신자 확인 가능성, 통신단계수 및 송수신자의 계산량 등 효율성과 부가기능 측면에서 비교 분석한다.

표 1. 제안방법의 특성 비교

기법 / 비교항목	기존방법 : VOT[6]	제안기법 (Ⅰ)	제안기법 (Ⅱ)
근본적 기반문제	이산대수 문제	이산대수 문제	이산대수 문제
서명기법	없음	Bit Commitment	RSA에 기반한 디지털 서명
공정성	가짐	가짐	가짐
검증가능성	가짐	가짐	가짐
안전성	가짐	가짐	가짐
송신자 확인기능	없음	있음	있음
송수신 부인 방지기능	없음	있음	있음

표 1은 제안한 기법들과 기존기법과의 공정성, 검증가능성, 안전성 및 서명기법 그리고 근본적인 기반 문제, 송신자 확인 및 송수신사실 부인 방지 기능 존재 여부에 대해서 비교분석한 결과이다.

제안한 방식들은 기존의 프로토콜의 절차를 그대

로 따르면서 Bit Commitment 기법과 RSA를 기반으로 하는 디지털 서명을 추가한 형태로서 기존 프로토콜의 공정성, 검증가능성, 안전성의 특성을 그대로 가진다. 다만 서명기법으로서 Bit Commitment와 디지털 서명이 가지고 있는 특성이 부가된 것이다.

4. 2 제안기법(Ⅰ)의 특성 고찰

Bit Commitment를 이용한 제안기법(Ⅰ)을 살펴보면 그림 2 의 제안한 프로토콜<단계 2>에서 영희가 철수에게 $HR_2 \equiv H_2(R_{11}, R_{22}, C_2)$과 R_{11}을 전송하는 것은 영희가 철수에게 비밀정보를 맡겼다는 증거이다. 이 증거가 바로 송신사실 부인방지 기능과 송신자 확인의 결정적인 요인이 되는 것이다. 즉 영희의 일방향 함수 H_2를 적용하여 계산한 (HR_{22}, R_{11})과 전송되어온 (HR_2, R_{11})과의 일치여부가 송신자가 영희임을 입증해 주는 것이며 동시에 영희가 부정행위를 하고 있는지의 여부를 즉각 철수가 알아차릴 수 있는 결정적 계기가 된다.

만약 일치한다면 철수는 영희가 올바르게 프로토콜을 따른다는 사실과 송신자가 영희라는 사실을 확인할 수 있고 사후 부인방지 기능을 수행하기 위해서 (HR_2, R_{11})을 보관하면 되고, 만약 일치하지 않는다면 영희가 올바르게 프로토콜을 따르지 않는 부정행위를 한 사실을 탐지하거나 아니면 송신자가 영희가 아니라는 사실을 즉각 탐지할 수 있는 것이다. 이때 영희의 일방향함수(H_2)는 철수로 하여금 그 함수를 역변환하여 그 비밀정보를 알아차리게 하는 것을 막아준다.

이 프로토콜의 특성은 <단계 2>에서 철수가 어떠한 메시지도 보낼 필요가 없다는 점이다. 영희는 철수에게 비밀정보를 맡기기 위해서 하나의 메시지를 전송하고, 그 비밀정보를 공개하기 위해서 다른 메시지를 전송하면 된다. 이때 철수의 임의의 스트링은 필요하지 않게 된다. 왜냐하면 영희가 철수에게 비밀정보를 맡겼다는 사실의 결과가 곧 일방향함수에 의해 계산된 메시지이기 때문이다.

영희는 상대방을 속이는 부정행위를 할 수 없고 다른 메시지 - 즉 H(R_{11}, R_{22}' , C_2') = H(R_{11}, R_{22}, C_2)와 같은 - (R_{11} , R_{22}' , C_2')를 찾을 수 없다. 또 영희는 R_{11}을 철수에게 전송함으로써 비밀정보(C_2)의 값을 맡기고 있는 것이다. 만약 영희가 R_{22}를 비밀로서 가지고 있지 않다면, (즉 철수가 R_{22}를 알고 있다면) 철수는 H(R_{11}, R_{22}, C_2)와 H(R_{11}, R_{22}' , C_2')을 둘 다 계산할 수 있을 것이고 그리고 어떠한 것이 영희로부터 받은 것과 같은지를 알 수 있을 것이다.

즉 R_{22}를 영희가 비밀로서 가지고 있음으로서 철수는 영희가 위임한 C_2의 값을 마음대로 유추하거나 계산해 낼 수 없는 것이다.

4. 3 제안기법(Ⅱ)의 특성고찰

다음으로 디지털 서명을 이용한 제안기법(Ⅱ)를 살펴본다.

공개키 디지털서명의 안전성은 공개키로부터 비밀키를 유추할 수 없는 수학적 함수에 기반한다. 디지털서명은 서명자들만이 만들 수 있는 고유한 것으로 다른 사람이 서명을 위조할 수 없어야 하며 모든 사람이 서명된 문서의 정당성을 확인할 수 있어야 한다. 공개키 디지털서명 방식에서 비밀키는 서명자만이 알고 있기 때문에 비밀키를 이용하여 전자문서에 대해서 손으로 쓴 서명과 똑같은 의미를 갖는 디지털서명을 생성할 수 있다. 생성된 디지털서명은 서명자의 공개키를 이용하여 모든 사용자가 전자문서의 정당성을 확인할 수 있다.

그림 3의 <단계 2>에서의 S_B와 <단계 3>에서의 S_A는 각각 철수와 영희 이외의 사람들은 각각의 비밀키를 모르기 때문에 그 서명을 생성할 수 없다. 그러므로 S_B 와 S_A는 각각 철수와 영희에 의해서 생성된 서명인 것이다. 따라서 프로토콜 각 단계에서 이 서명을 보관함으로써 상대방의 송신사실 사후 부인방지 기능을 수행할 수 있고 또한 프로토콜 과정에서의 송신자의 확인이 가능하며 분쟁시 사후 해결가능성을 높일 수 있는 부가기능을 가진다.

4. 4 제안기법의 효율성 및 부가기능 고찰

표 2는 제안한 기법들과의 효율성 및 부가기능 측면에서 8가지의 항목을 비교 분석한 결과이다. 표 2에서 보는바와 같이 제안한 기법들은 기존의 기법과 비교 할 때 송수신자 부정 행위 가능성, 송신자 신원확인 가능성, 메시지 송신사실 검증 가능성, 송신사실 사후 부인 가능성, 분쟁시 사후 해결가능성 측면에서 양호함을 보이고 있으며, 프로토콜 과정 중 통신단계수에 있어서는 디지털 서명을 이용한 제안 기법은 동등함을 (2회), Bit Commitment 기법을 이용한 제안기법은 불리함을 보이며(4회), 송수신자의 계산량 측면에 있어서는 기존의 방법에 비해 상대적으로 많은 계산량을 요구하여 두 방법 모두 불리함을 알 수 있다.

효율성 측면에서는 다소 불리하나 송신자 확인

및 송신사실 사후 부인 방지등 여러 부가적인 기능을 가지는 측면에서는 제안된 기법들이 응용분야에 따라서 달라지겠지만 비교적 유리하다.

표 2. 제안방식의 효율성 및 부가기능 측면 비교표

○ : 양호 , × : 불리

기법 / 비교항목	기존방법	제안기법(Ⅰ)	제안기법(Ⅱ)
프로토콜 실행중 특성 메시지 노출 가능성	없음(○)	없음(○)	없음(○)
송수신자 부정행위 가능성(cheating)	많음(×)	적음(○)	적음(○)
프로토콜 실행과정에서 메시지 전송 검증가능성	불가(×)	가능(○)	가능(○)
송신사실 사후 부인 가능성	있음(×)	없음(○)	없음(○)
사후분쟁 해결 가능성	적음(×)	많음(○)	많음(○)
프로토콜 실행과정에서 송신자 확인 가능성	불가(×)	가능(○)	가능(○)
통신단계수	적음(○) : 2회	많음(×) : 4회	적음(○) : 2회
송수신자의 계산량	적음(○)	많음(×)	많음(×)

V. 결 론

본 논문에서는 이산대수문제에 기반을 둔 대화형 불확정 전송 프로토콜에 대하여 고찰하였다.

효율성을 고려하고 두 당사자 사이에서의 송신자의 신원 확인 및 송신사실의 사후부인 문제에 대하여 Bit Commitment 기법과 공개키 암호시스템의 디지털 서명기법을 이용하여 그 문제에 대한 해결책으로서 확장된 대화형 불확정 전송 프로토콜을 제안하였다.

제안한 방식은 기존의 프로토콜을 그대로 따르면서 Bit Commitment와 RSA 암호를 기반으로한 디지털 서명을 추가한 형태로서 기존 프로토콜의 공정성, 검증가능성, 안전성을 그대로 가진다. 거기에다 부가된 기능에 따라 두 당사자는 송신자의 신원확인 및 송신사실을 사후 부인 할 수 없게 된다. 따라서 이 프로토콜에 따르면 양자 부정 행위가능성, 프로토콜 중간과정에서의 메시지전송 검증가능성, 사후분쟁해결 가능성, 송신자 신원확인 가능성, 송신사실 사후 부인 방지 가능성 면에서 우수하나 통신량 및 계산량면에서는 동등하거나 다소 불리하다.

본 논문에서 제안한 기법은 서로 신뢰하지 못하는 두 당사자 사이에서 공평하게 비밀정보를 교환하고자 하는 분야에 있어서 보다 안전한 프로토콜로서 활용될 수 있다.

앞으로의 연구과제는 부가적인 기능을 만족시키면서도 통신량 및 계산량을 최소한으로 줄일 수 있는 방법을 모색하는 것과, 두 당사자가 아닌 다수의 사용자 사이에서도 적용 가능한 프로토콜(Multi-party protocol)로의 확장이 될 것이다.

참 고 문 헌

[1] M.O. Rabin, "How to Exchange Secrets by Oblivious Transfer." TR-81, Harvard, 1981.

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

[3] D. Beaver, "How to Break a 'Secure' Oblivious Transfer Protocol" . *Advances in Cryptology-Eurocrypt' 92 Proceeding* Springer-Verlag LNCS 658, 285-296, 1993.

[4] Lein Harn and Hung-Yu Lin, "Non interactive oblivious transfer" , Electronic Letters, Vol.26, NO.10, pp. 635-636, 1990.

[5] C. Crépeau, "Equivalence Between Two Flavours of Oblivious Transfers." *Advances in Cryptology-Crypto'87, Proceedings,* Springer-Verlag LNCS 293, pp.350-354, 1988.

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

[7] B. den Boer, "Oblivious Transfer Protecting Secrecy." *Advances in Cryptology-Eurocrypt '91 Proceedings,* Springer-Verlag LNCS 547, pp.31-45, 1991.

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

[9] S. Even, O. Goldreich, A. Lempel, "A Randomized Protocol for Singing Contracts." *Comm. of the ACM, Vol.* 28. No. 6, pp. 637-649, 1985.(Early version : *Proceedings of Crypto 1982,* Springer-Verlag, 205-210, 1983).

[10] 김순곤, 송유진, 강창구, 안동언, 정성종, "은닉서명을 이용한 검증가능 불확정 전송" , 대한전자공학회 추계 종합학술대회 논문집 Vol 19, No. 2 pp.661-664, 1996.11.

[11] 송유진, 김순곤, 강창구, 정성종, "비밀정보교환을 위한 불확정 전송" , 대한전자공학회 추계 종합학술대회 논문집 Vol 19, No. 2, pp. 677-680, 1996.11.

[12] Bruce Schneier, "Applied Cryptography" , John Willey & Sons, 1996.

[13] M. Naor, "Bit Commitment Using Pseudo-Randomness" , Advances in Cryptology-CRYPTO '89 Proceedings, Springer-Verlag. pp.128-136, 1990.

[14] M. Naor, "Bit Commitment Using Pseudo-Randomness" , Journal of Cryptology(1991)4, pp.151-158, 1991.

[15] R. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems" , Communications of the ACM, 21(2), pp.120-126, 1978.

[16] R. Berger, R. Peralta, and Tedric, "A provably secure oblivious transfer protocol" , Advances in Cryptology : Proc. of EUROCRYPT, pp.379-386, 1984.

[17] M. Blum, "Three applications of oblivious transfer" : 1. Coin flipping by telephone, 2. How to exchange secrets, 3. How to send certified electronic mail, Dept.,EECS, University of California, Berkeley, Calif. 1981.

[18] M. Blum, "How to exchange (secret)key" , ACM Transaction on Computer System, Vol. 1, No. 2, pp.175-193, 1983.

[19] E. Brickle, D. Chaum, I. Damgard, and J. Van de Graaf, "Gradual and verifiable release of a secret" , Advances in Cryptology : CRYPTO '89, pp. 156-166, 1987.

[20] T. Tedric, "How to exchange half a bit" , Advances in Cryptology : Proc. of CRYPTO pp.147-151, 1983.

[21] T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms" , IEEE Transactions on Information Theory, Vol. IT-30, No.4, pp.469-472, 1985.

[22] SoonGohn Kim, NamJae Lee, SeongJong Chung, HoonSung Kwack, "An Interactive Verifiable Oblivious Transfer Protocol with Additional Functions" , Proceedings of the 6th IEEE International Workshop on Intelligent Signal Processing and Communication Systems(ISPACS'98) Volume Ⅰ, pp. 183~187, Nov. 1998.

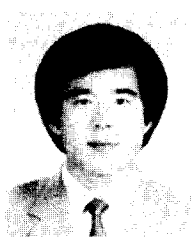
[23] 김순곤, 신승중, 박인규, "공개키 암호를 이용한 대화형 불확정 전송의 확장", 한국통신학회 하계종합학술발표회 논문집, pp.967-970, 1997.7.

[24] SoonGohn Kim, NamJae Lee, SeongJong Chung, HoonSung Kwack, "A Secure Transfer Protocol for Multimedia Data" , Proceedings of International Conference on Multimedia and Telecommunications Management (ICMTM'98), Springer-Verlag, pp. 398~409, Dec. 1998.

[25] 정성종,강창구,김순곤,송유진외3인, "정보보호 방식 설계 및 검증 기술에 관한 연구" , 한국전자통신연구소, 연구보고서, 1996. 12

[26] 한국전자통신연구소, "현대암호학" , 1991. 8.

김 순 곤(Soon-Gohn Kim) 정회원



1957년 9월 5일생

1979년 : 전북대학교 자원공학과 (공학사)

1984년 : 동국대학교 대학원 전산교육학과 (교육학석사)

1999년 : 전북대학교 대학원 전자계산기공학과 (공학박사)

1979년~1981년 : 대한민국 육군장교(ROTC)

1982년~1987년 : 동아생명보험(주)전산실근무

1987년~1995년 : 한국원자력연구소 선임연구원

1993년 : 정보처리기술사(전자계산조직응용)

1999년 : 멀티미디어기술사

1995~현재 : 중부대학교 정보공학부 교수

1997~현재 : 중부대학교 전산정보원 원장, 컴퓨터멀티미디어학과 학과장

<주관심 분야> Network Security, 정보보호이론, 멀티미디어 데이터베이스, 멀티미디어

정보보호, 전산 및 정보통신 정보보호 기술, 인터넷 컴퓨팅

송 유 진(Yu-Jin Song) 정회원

1982년 : 한국항공대학교 졸업 (학사)
1987년 : 경북대학교 졸업(석사)
1995년 : 일본 Tokyo Institute of Technology 졸업(박사)
1988~1996년 : 한국전자통신연구원
1996년~현재 : 동국대학교 정보산업학과, 국제정보대학원(정보보호학과) 교수, 동국대학교 부설 전자상거래 연구소 연구위원
1998년~현재 : 한국통신정보보호학회 교육이사
1998년~현재 : ISO/IEC JTC1/SC27-Korea 전문위원
1997년~현재 : 한국정보시스템학회 종신이사
<주관심 분야> 암호이론, 인증 및 부호이론, 전자상거래보안 응용, 전자화폐/전자지불

강 창 구(Chang-Goo Kang) 정회원

한국통신학회논문지 제18권 제9호 참조.
1987년~현재 : 한국전자통신연구원 책임연구원 부호 3팀장
1997년~현재 : 한국통신정보보호학회 충청지부 부지부장
<주관심 분야> 부호 및 통신이론, 정보보호 이론, 디지털서명, 전산 및 통신 정보보호 기술

안 동 언(Dong-Un An) 정회원

1958년 5월 25일생
1981년 : 한양대학교 전자공학과 (공학사)
1987년 : 한국과학기술원 전산학과 (공학석사)
1995년 : 한국과학기술원 전산학과 (공학박사)
1982년~1991년 : 한국외국어대학교 강사
1991년~1995년 : 충남대학교 강사
1995년~현재 : 전북대학교 전자·정보공학부 조교수
<주관심 분야> 한국어정보처리, 기계번역, 정보검색, 에이전트

정 성 종(Seong-Jong Chung) 정회원

1950년 2월 19일생
1975년 : 한양대학교 전기공학과 (공학사)
1981년 : 미국 Houston대학교 대학원 전자공학과 (공학석사)
1988년 : 충남대학교 대학원 전산공학과(공학박사)
1990년~1991년 : Penn. State Univ. 객원교수
1985년 ~현재 : 전북대학교 컴퓨터공학과 교수
1996년~현재 : 전북대학교 전자계산소 소장
<주관심 분야> 패턴인식, 인공지능, 정보보호, 컴퓨터그래픽스