Journal of Digital Contents Society Vol. 8 No. 4 Dec. 2007(pp. 631-637)

의사난수생성기를 이용한 공평한 비밀정보교환을 위한 적응형 암호화 프로토콜

김순곤*

요 약

본 논문에서는 공평한 비밀정보교환을 위한 적응형 암호화 프로토콜을 제안한다. 이를 위해 Lein Harn등이 제안한 이산대수 문제에 기반한 검증가능 불확정전송 프로토콜을 분석하고 부가적인 기능을 가진 적응형 암호화 프로토콜을 제안한다. 기존의 방식에서 고려하지 않았던 송신자확인 및 송신사실 사후부인방지 등의 여러 기능이 부가되고 적응적 기능을 가지는 암호화 프로토콜을 제안한다. 이를 위해 의사난수생성기를 이용한 Bit Commitment 기법을 도입한 방법을 제안한다.

Adaptive Cryptographic Protocol for Fair Exchange of Secrets using Pseudo-Random-Sequence Generator

Soon-Gohn Kim*

Abstract

In this paper, I propose an adaptive cryptographic protocol which is basic protocol for fair exchange of secrets. For this, I investigate the verifiable oblivious transfer protocol based on discrete logarithm problem proposed by Lein Harn etc. And I propose a new adaptive cryptographic protocol that has the additional funtions 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, I make use of bit commitment scheme using pseudo-random-sequence generator.

Keywords : adaptive protocol, oblivious transfer, bit commitment, pseudo-random-sequence generator

1. 서론

1.1 공평한 비밀정보 교환 방법

최근 인터넷을 이용한 비즈니스 등의 전자상거래가 활성화 되고 있다. 이와 같이 네트워크상의 비즈니스가 활성화됨에 따라 여러 가지 업무, 특히 계약 등의 업무도 네트워크를 통해서 실현되고 있는 추세이다. 네트워크 기술이 발전됨에 따라 모든 일상생활속의 일을 분산환경 하에서 네트워크를 이용하여 실현하고자 하는 경향이 강해지고 있다. 예를 들면 네트워크를 이용한 계약, 게임, 선거 등이 그것이다. 여기서 중요한 것은 어떻게 비밀정보를 공평하게 교환할 수 있느냐 하는 것이다. 본 논문에서는 분산환경 즉 네트워크상에서 이루어지는 공평한 비밀정보교환 프로토콜에 대하여 분석 검토한다.

네트워크를 이용하여 비밀정보를 교환함에 있어서 중요한 요소는 송신자, 수신자 각각이 공평하게 정보를 서로 교환하는 것이다. 예를 들면 계약문서에 서명할 때 어느 한쪽이 자신의 서명정보를 먼저 송신함으로써 발생할 수 있는 불리한 점이 있을 수 있다.이러한 문제점을 해결하기 위해서 불특정 다수가 각자의 비밀정보를 네트워크상에서 서로 공평하게 교환하는 프로토콜이 필요하고 이에 대한 연구가 많은 학자들에 의해서 연구되어 왔다[1~20]. 본 논문에서는 네트워크를 이용하여 동시에 비밀정보를 공평하게 교

※ 제일저자(First Author) : 김순곤
접수일자:2007년09월14일, 심사완료:2007년09월28일
* 중부대학교 컴퓨터학과
sgkim@joongbu.ac.kr
▣ 이 논문은 2006년도 중부대학교 학술연구개발비 지원에 의하여 이루어진 것임

환하는 문제에 대하여 기존의 연구결과를 중심으로 검토한다.

1.2 관련연구

서로 상대방을 신뢰하지 못하면서 비밀정보를 공평하게 교환하기를 원하는 대표적인 암호화 프로토콜로서 연구되어 온 것이 불확정전송 프로토콜(OT : Oblivios Transfer Protocol)이다. 일상적인 암호화 프로토콜에서 비밀을 보장하면서 그것에 관련한 임의의 정보를 보내야 하는 경우 OT 프로토콜은 유용하게 쓰일 수 있다.

1981년에 불확정전송 기법에 의한 비밀정보교환 방법에 대하여 M. Rabin이 OT의 개념을 소개하고 연구하였으며[1], 1983년에 비밀키를 교환하는 방법에 대하여 M. Blum이 연구하였고[2,3] 반 비트를 교환하는 방법에 대하여 T. Tedrick이 연구하였다[4]. 1984년에 가능한 안전한 불확정 전송방법에 대하여 T. Tedrick과 R. Peralta 등이 연구하였으며[5], 공평한 비밀정보의 교환에 대하여 T. Tedrick이 연구하였다[6].

1987년에 검증 가능한 비밀의 공유를 위한 실제적 기법에 대하여 P. Feldman이 연구하였으며[7]. 1989년에 이산대수 문제에 기반한 비대화형 불확정전송과 그 응용에 대하여 M. Bellare와 S. Micali가 연구하였다[8]. 또 같은 해에 이차잉여가설(QRA)에 기반한 비대화형 불확정전송에 대하여 Santis와 Persiano가 연구하였으며[9], 1990년에 불확정전송에 기초한 영지식 증명에 관하여 K. Sakurai, T. Itoh, K. Kurosawa 등이 연구하였다[10].

1991년에 검증가능 불확정 전송에 대하여 L. Harn등이 연구한 내용을 ASIACRYPTO '91에서 발표하였고[11], 1992년에 안전한 OT를 깨뜨리는 방법에 대하여 D, Beaver가 연구하였다[12]. 1995년에는 Precomputing OT에 대하여 D. Beaver가[13], Committed OT에 대하여 C. Crepeau가[14], Quantum OT의 안전성에 대하여 D. Mayers가[15] 각각 연구하였다.

1996년에는 Equivocable OT에 관하여 D. Beaver가[16], 노이즈 채널에서의 스트링 OT에 관하여 D. Mayers가[17] 각각 연구 결과를 발표하였다. 1997년에 OT와 Privacy Amplification에 대하여 G. Brassard등이 연구 결과를 발표하였다[18].

본 논문에서는 공평한 비밀정보 교환을 위한 기본 프로토콜인 불확정 전송의 개념을 살펴보고 검증가능 블확정 전송 프로토콜을 분석하고 새로운 적응형 암호화 프로토콜을 제안한다. 제안하는 방식은 기존의 방식에다 부가적인 기능을 갖도록 확장하였다.

본 논문은 5 개의 장으로 구성된다. 제 1장에서는 공평한 비밀정보 교환 방법과 관련연구를 살펴보고, 제 2장에서는 기존방식에 대하여 살펴보고, 제 3장에서는 새로운 적응형 암호화 프로토콜을 제안하고, 제 4장에서는 제안방식의 특성을 비교 고찰한 다음 마지막으로 제 5장에서 결론을 맺는다.

2. 공평한 비밀정보 교환기법

2.1 기존방법 고찰

공평한 비밀정보 교환을 위한 기존기법을 고찰하기 위하여 기존의 검증가능 암호화 프로토콜을 살펴보고자 한다[11].

(가정)

- p는 큰 소수(prime number)이고 p′ 또한 소수이다.
- $p=4*p'+1,\ p=1 \bmod 4$
- e는 p의 Galois Field 의 원시 원소(원시근)이다.
- p와 e는 A와 B에게 공개되어 있다.
- A는 자신만의 비밀 α를 선택한다.
- α는 다음과 같은 성질을 갖는다.

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

- A는 공증정보인 As와 A1-s, p, e를 신뢰할 수 있는 제3자 (TTP)에 의뢰한다. 이때 $s \in \{0, 1\}$이고 A만이 알고 있다.

(프로토콜)

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

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

< 단계 2 > : A는 다음 계산을 해서 B에게 보낸다.

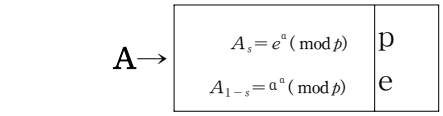
$$C_2 = C_1^{a^{-1}} \bmod p$$

< 단계 3 > : B는 C_3을 계산한다.

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

만약 $C_3 = e$ 라면 B는 A의 비밀에 대해서는 모른다. 그렇지 않다면 ($C_3 \neq e$) B는 A의 비밀 $a = C_3$을 안다. 그 외의 경우라면 B는 A의 부정행위를 처벌할 수 있다.

이를 그림으로 표현하면 다음 (그림 1)과 같다.



	(A)		(B)
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_2를 계산 $C_2 = C_1^{a^{-1}}$	C2→ mod p	
단계 3			C_3를 계산 $C_3 = C_2^{\,b^{-1}} \bmod p$ $C_3 = e$이면 비밀을 얻지 못하고 $C_3 = a$이면 비밀을 얻 고 그 외의 경우라면 B는 A의 부정 행위를 고발 가능하다.

(그림 1) 기존 검증가능 프로토콜 개념도

2.2 Bit Commitment 프로토콜

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

A 가 B에게 어떤 비밀내용을 맡기고 싶지 않지만, 일정기간이 지나기 전 까지는 그 내용을 알리고 시지 않고, 한편 B는 A가 비밀내용을 자신에게 맡긴 뒤 그 내용을 변화시킬 수 없기를 바라는 경우 Bit Commitment 프로토콜을 사용하게 된다. 이것은 다음의 두 단계로 이루어진다.

(Commitment단계)

A는 B에게 맡기고 싶은 비트 m이 있다. A와 B는 메시지를 교환하고 이 단계가 끝나면 B는 m을 나타내는 정보를 가지게 된다.

(Reveal 단계)

이 단계에서 B는 m의 값을 알게 된다. 이러한 Bit Commitment 프로토콜은 사용하는 암호화방식에 따라서 대칭적 암호방식을 이용한 Bit Commitment 방법[21]과 일방향함수를 이용한 Bit Commitment방법[21]과 의사난수 생성기를 이용하는 Bit Commitment방법[19, 20] 등이 있는데 본 논문에서는 의사난수 생성기를 이용한 Bit Commitment 방법에 관하여 살펴보고 이를 적용한다.

· 의사난수 생성기를 이용한 Bit Commitment 방법

서로 신뢰하지 못하는 두 당사자 A와 B가 있다. A는 B에게 비밀정보 (하나 혹은 여러개의 bit)를 맡기고자 한다. 이때 A는 그 비밀정보의 내용을 일정기간 지나기 전 까지는 B에게 알리고 싶지 않다. 한편 B는 A가 비밀정보를 자신에게 맡긴 후 그 비밀정보의 내용을 변화시킬 수 없기를 바라는 상황이라고 가정한다.

(Commit ment 단계)

< 단계 1 > B는 임의의 비트스트링(R_B) 를 생성하고 이것을 A에게 보낸다.

< 단계 2 > A는 의사난수생성기에 대한 난수 씨앗(Random Seed)을 생성한 다음, B가 보내온 임의의 비트스트링에 잇는 모든 비트에 대하여

B에게 다음중의 하나를 보낸다.

(1) B의 비트가 0이면 난수생성기의 출력값, 또는

(2) B의 비트가 1이면 A의 난수씨앗의 비트와 난수생성기의 출력값과의 XOR값

(Reveal 단계)

< 단계 3 >

- A는 자신의 난수씨앗을 B에게 보낸다.
- B는 A가 공평하게 이행하였는지를 확인하기 위하여 그 난수씨앗을 적용하여 < 단계2 >를 수행하여본다.

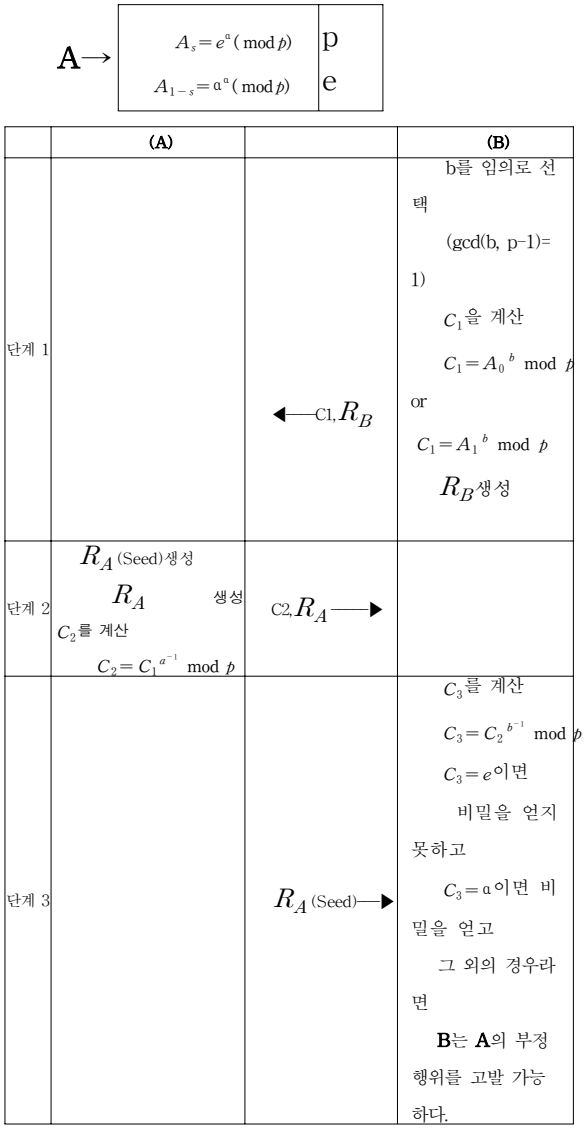
만약 B의 임의의 비트가 충분히 길고, 의사난수생성기가 예측 불가능 하다면, A가 부정행위를 할 수 있는 실질적인 방법은 없다.

3. 제안한 방법

3.1 Bit Commitment 를 이용한 제안방식 개요

기존의 암호화 프로토콜은 공정성, 검증가능성 및 안정성을 가진다. 본 논문에서는 기존의 프로토콜을 분석한 결과 기존의 프로토콜이 가지고 있는 특성에다가, 그들이 고려하지 않았던 다음과 같은 사항을 고려하여 새로운 적응형 암호화 프로토콜을 제안하였다. 기존 프로토콜 과정 중에는 송신자의 신원 확인 및 송신자의 송신사실의 사후부인방지에 관한 내용이 고려되어 있지 않았다. 따라서 송신자가 송신사실을 사후에 부인할 수 없도록 하는 문제에 관한 보완 방법이 필요하였다. 이를 위하여 본 논문에서는 의사난수 생성기를 적용한 Bit Commitment 기법을 이용하였다. 공중정보와 Bit Commitment 기법을 이용하여 기존의 프로토콜에서 고려하지 않은 송신자의 신원확인과 송신자의 송신사실 사후부인 방지의 부과적인 기능을 갖도록 기존방법을 확장하였다.

제안방식의 파라미터를 살펴보면 R_B는 B가 생성하는 임의의 비트스트링이고,R_A는 A가 난수씨앗을 적용하여 B에게 보내는 비트스트링이고, R_A(Seed)는 A가 B에게 보내는 난수씨앗이다. 제안방식의 개념도를 살펴보면 다음 (그림 2)와 같다.



(그림 2) Bit Commitment를 이용한 제안프로토콜

3.2 프로토콜 설명

제안방식의 프로토콜 전개 순서를 살펴보면 다음과 같다.

- A가 B에게 비밀정보를 전송하고자 할때 기존프로토콜 순서를 그대로 따르면서 의사난수생성기를 적용한 Bit Commitment 기법을 추가한 형태이다.
- B가 A에게 비밀정보를 전송하고자 할 때는

A와 B의 역할을 대칭적으로 바꾸면 된다.

< 단계 1 >

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

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

- B는 임의의 비트스트링 R_B를 생성한다.
- B는 C_1과 R_B를 A에게 전송한다.

< 단계 2 >

- A는 자신의 비밀 α를 이용하여 C_2를 계산한다.

$$C_2 \equiv C_1^{\alpha^{-1}} \pmod{p}$$

- A는 임의의 난수씨앗을 생성하고(R_A(Seed)), 이 난수 씨앗을 적용하여 비트스트링(R_A)을 생성한다.
- A는 C_2와 R_A를 B에게 보낸다.

< 단계 3 >

- B는 자신의 비밀번호 b를 이용하여 C3를 계산한다.

$$C_3 \equiv C_2^{b^{-1}} \pmod{p}$$

C3가 e이면 B는 비밀을 얻지 못하고 C3가 α이면 B는 비밀을 얻고 그 외의 경우라면 B는 A의 부정행위를 고발가능하다.

- A는 자신의 난수씨앗 R_A(Seed)를 B에게 보낸다.
- B는 A가 공평하게 이행하였는지를 확인하기 위하여 A가 보내온 난수씨앗 R_A(Seed)를 이용하여 < 단계 2 >에서 A가 수행한 과정을 수행하여본다. 이때 결과가 일치하면 프로토콜을 정상적으로 끝내고, 일치하지 않으면 A의 부정행위를 고발 가능하다.

4. 제안방식의 특성비교 및 고찰

4.1 개요

제안한 의사난수생성기를 이용한 적응형 암호화 프로토콜과 기존 검증가능 암호와 프로토콜의 특성을 비교 분석하면 <표 1>과 같다. 이는 기존기법과 제안한 기법에 대하여 근본적 기반문제, 공정성, 검증가능성, 안정성 및 서명기법 그리고 송신자 확인 및 송신사실 부인방지 기능 존재 여부에 대해서 비교 분석한 결과이다. 제안한 방식은 기존의 프로토콜의 절차를 그대로 따르면서 의사난수발생기를 이용한 Bit Commitment 기법을 추가한 형태로서 기존 프로토콜의 공정성, 검증가능성, 안전성의 특성을 그대로 가진다. 다만 부가기능으로 송신자 확인 및 송신사실 부인방지기능을 가진다.

<표 2>에서는 기존의 기법과 제안한 기법의 프로토콜 실행중의 특성 메시지 노출가능성, 송수신자 부정행위 가능성, 프로토콜실행 과정에서의 메시지 송신사실 검증가능성, 송신사실 부인가능성, 분쟁시 사후해결 가능성, 프로토콜 실행중 송신자 확인가능성, 통신 단계 수 및 송수신자 계산량 등 효율성과 부가기능 측면에서 비교분석한 결과이다.

<표 1> 제안기법의 특성 비교

기법 / 비교항목	기존기법	제안기법
Primitive Problem	Discrete Logarithm Problem	Discrete Logarithm Problem
서명기법 (Signature Scheme)	없음	Bit Commitment
공정성 (Fairness)	가짐	가짐
검증가능성 (Verifiability)	가짐	가짐
안전성 (Security)	가짐	가짐
송신자 확인기능	없음	있음
송신부인 방지기능	없음	있음

4.2 제안기법 분석

의사난수생성기를 이용한 제안기법을 분석해보면 (그림 2)의 제안한 프로토콜 < 단계 2 >에서 A가 B에게 R_A를 전송하는 것은 A가 B에게 비밀정보를 보냈다는 증거이다. 이 증거가 바로 송신사실 부인방지 기능과 송신자 확인의 결정적인 요인이 되는 것이다. 즉 A의 난수씨앗을 적용하여 계산한 R_A와 < 단계 3 >에서 전송되어온 R_A(seed)를 적용한 결과와의 일치여부가

송신자가 A임을 입증해 주는 것이며 동시에 A가 부정행위를 하고 있는지의 여부를 B가 알아차릴 수 있는 계기가 된다. 만약 일치한다면 B는 A가 올바르게 프로토콜을 따른다는 사실과 송신자가 A라는 사실을 확인할 수 있고 사후 부인방지기능을 수행하기 위해서 R_A와 R_A(seed)를 보관하면 되고, 만약 일치하지 않는다면 A가 올바르게 프로토콜을 따르지 않는 부정행위를 한 사실을 탐지하거나 아니면 송신자가 A가 아니라는 사실을 탐지할 수 있는 것이다.

4.3 제안기법의 효율성 및 부가기능 고찰

<표 2>는 제안한 기법의 효율성 및 부가기능 측면에서 8 가지의 항목을 비교 분석한 결과이다. 여기에서 보는 바와 같이 제안한 기법은 기존의 기법과 비교할 때 송신자 부정행위가능성, 송신자 신원확인 가능성, 메시지 송신사실 검증가능성, 송신사실 사후부인 가능성, 분쟁시 사후해결 가능성 측면에서 양호함을 보이고 있다. 제안기법의 통신량 및 계산량 비교를 보여주는 <표 3>에서 보는 바와 같이 프로토콜 과정중 통신단계 수 에 있어서는 다소 불리함을 보이며(3회), 송수신자의 계산량 측면에 있어서는 기존의 방법에 비해 상대적으로 약간 많은 계산량(4%~8%)을 요구하여 조금 불리함을 알 수 있다.

효율성 측면에서는 다소 불리하나 송신자 확인 및 송신 사실 사후부인 방지 등 여러 부가적인 기능을 가지는 측면에서는 제안된 기법이 비교적 유리하다.

<표 2> 제안기법의 효율성 및 부가기능 비교

○ : 양호 , × : 불리

비교항목 \ 기법	기존 기법	제안 기법
프로토콜 실행 중 특성 메세지 노출 가능성	없 음 (○)	없음(○)
송수신자 부정행위 가능성	많음(×)	적음(○)
프로토콜 실행과정에서 메세지 전송 검증가능성	불가(×)	가능(○)
송신사실 사후 부인 가능성	있음(×)	없음(○)
사후분쟁 해결 가능성	적음(×)	많음(○)
프로토콜 실행과정에서 송신자 확인 가능성	불가(×)	가능(○)
통신단계수	적 음 (○) 2회	많음(×) 3회
송수신자의 계산량	적 음 (○)	많음(×)

<표 3> 제안기법의 통신량 및 계산량 비교

구분	통신단계수	송수신자 계산량
기존기법	2 회	1.0
제안기법	3 회	1.04 ~ 1.08

5. 결론

본 논문에서는 이산대수문제에 기반을 둔 암호화 프로토콜에 대하여 고찰하였다. 신뢰하지 못하는 두 당사자 사이에서 송신자의 신원 확인 및 송신사실 부인방지 문제에 대하여 의사난수생성기를 이용한 Bit Commitment 기법을 적용하여 적응형 암호화 프로토콜을 제안하였다.

제안한 방식은 기존의 프로토콜을 그대로 따르면서 의사난수생성기의 특성을 추가한 형태로서 기존 프로토콜의 공정성, 검증가능성, 안전성을 그대로 가진다. 그리고 제안한 방식은 송신자의 신원확인 및 송신사실 사후부인 방지 등의 부가된 기능을 가진다. 따라서 이 프로토콜에 따르면 양자 부정행위 가능성, 사후분쟁 해결 가능성, 송신자 신원확인 가능성, 송신사실 사후부인 방지 가능성 면에서 우수함을 보인다. 다만 통신량 및 계산량 면에서는 다소 불리하다.

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

향후 연구과제는 부가적인 기능을 만족시키면서도 통신량 및 계산량을 최소한으로 줄일 수 있는 방법을 찾는 것과, 두 당사자가 아닌 다수의 사용자 사이에서도 적용 가능한 멀티프로토콜로의 확장이 될 것이다.

참 고 문 헌

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

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

[3] M. Blum, "Three applications of the 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.

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

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

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

[7] P. Feldman, "A Protocol Scheme for Verifiable Secret Sharing", Proceedings of 28th FOCS, pp 427-438, 1987.

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

[9] A. D. Santis and G. Persiano, "Public-Randomness in Public-key Cryptography", Proceedings of Eurocrypto '90, pp. 46-62, 1990.

[10] K. Sakurai, T. Itoh, and K. Kurosawa, "Some Remarks on Zero-Knowledge Proofs based on Oblivious Transfer", ISEC90-13, Japan, 1990.

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

[12] D. Beaver, "How to break a secure Oblivious Transfer Protocol", Proceedings of Eurocrypto '92, pp. 285-296. 1992.

[13] D. Beaver, "Precomputing Oblivious Transfer", Proceedings of Crypto 1995, pp.97-109, 1995

[14] C. Crepeau, J. van de Graaf and A. Tapp, "Committed Oblivious Transfer and Private Multi-Party Computation", Proceedings of Crypto 1995, pp.110-122, 1995.

[15] D. Mayers, "On the Security of the Quantum Oblivious Transfer and Key Distribution Protocols", CRYPTO 1995, pp. 124-135, 1995.

[16] D. Beaver, "Equivocable Oblivious Transfer", EUROCRYPT 1996, pp. 119-130, 1996.

[17] D. Mayers, "Quantum Key Distribution and String Oblivious Transfer in Noisy Channels", CRTPTO 1996, pp. 343-357, 1996.

[18] G. Brassard, C. Crepeau, "Oblivious Transfers and Privacy Amplification", EUROCRYPT 1997, pp. 334-347, 1997.

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

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

[21] B. Schneier, "Applied Cryptography", John Willey & Sons, 1996.

김 순 곤

1999년 : 전북대학교 대학원 전자계산기공학과(공학박사)
1987년 : 동국대학교 교육대학원 전산교육학과(교육학석사)
1987년～1995년 : 한국원자력연구소(선임연구원)
1995년～현 재 : 중부대학교 컴퓨터학과 교수
관심분야 : 정보보호, 유비쿼터스컴퓨팅, 데이터베이스, 멀티미디어컴퓨팅, 프로그래밍언어 등