비밀정보 교환을 위한 안전한 비대화형 전송 프로토콜

김 순 곤* · 박 인 규**

A Secure Non-Interactive Transfer Protocol for the Exchange of Secret Information.

Soon-Gohn Kim* , In-Kyu Park**

요 약

본 논문에서는 기존의 비대화형 전송 프로토콜을 기반으로 하여 비밀정보교환을 위한 여러 가지 부가기능을 가지는 새로운 비대화형 전송 프로토콜을 설계 제안한다. 제안한 방식은 기존의 프로토콜의 구조를 그대로 따르면서 Bit Commitment 기법을 적용한 형태로서 여러 가지 안전한 기능을 가진다. 본 논문에서 제안한 기법은 서로 신뢰하지 못하는 두 당사자 사이에서 비밀 정보를 교환하고자 하는 분야에 있어서 보다 안전한 프로토콜로서 활용될 수 있다.

Keywords : 암호화프로토콜, 이산대수문제, ElGamal암호, Bit Commitment, Non-Interactive Oblivious Transfer

1. 서 론

오늘날 정보화사회에서 인터넷과 멀티미디어 통신이 활성화됨에 따라 개방형 시스템에서 사용가능한 정보서비스인 전자상거래등의 성공적 실현을 위해서는 멀티미디어 데이터 처리와 디지털 컨텐츠 정보보호가 필수적이며, 이를 실현하기 위해서는 암호화 기법 및 암호화 프로토콜이 필연적으로 사용된다. 그리고 점점 더 많은 정보가 컴퓨터간 통신을 통하여 전송됨에 따라 멀티미디어 데이터와 디지털컨텐츠의 처리를 위하여 네트워크를 활용하게 되는데, 이러한 디지털 컨텐츠의 정보보호 및 멀티미디어 데이터 서비스의 보호를 위해서도 암호화 프로토콜이 필요하다.

암호화 프로토콜이란 서로 다른 이용자들간의 비밀정보 교환을 위한 알고리즘 이라고 정의할 수 있다. 이러한 암호화 프로토콜은 공동의 목표를 달성하기 위해서 비밀의 어떤 부분을 공유하거나, 이용자들 중 어느 누구와도 비밀을 개별적으로 공개하기 위하여 서로 힘을 합치거나, 서로 멀리 떨어져 있는 두 이용자가 하나의 확률적인 비트열을 만들기 위하여 이용자가 정보 그 자체는 알리지 않고 자신이 어떤 정보를 가지고 있음을 상대방에게 납득시키기 위한 것 등에서 볼 수 있다.

특히 개방환경하에서의 전자화폐, 전자선거, 전자계약, 전자서명 및 전자결재등의 전자상거래로 대표되는 전자사회에서는 다양한 암호화 프로토콜의 응용이 요구된다. 암호 응용분야로서는 동시문서전송

*중부대학교 컴퓨터멀티미디어학과
**중부대학교 전자계산학과

프로토콜을 이용한 전자계약 서명종류와 다자간 프로토콜을 이용한 전자선거 등에의 응용 및 동전 던지기와 재산비교 프로토콜과 같은 게임에 응용된 프로토콜 등 다양하다. 이러한 다양한
암호화 응용 프로토콜의 기본적인 도구로서 불확정전송(Oblivious Transfer)프로토콜과 공정한 비밀정보교환 프로토콜이 필수적인 요소가 될 것이다.

중요한 정보가 전송될 때 정보의 안전성이 문제가 되는데 이때 암호기술이 핵심적인 역할을 하게 된다. 이 과정에서 기본적인 암호기술은 물론 이를 응용한 암호화 프로토콜이 정보보호 기술의 기초가 되고 있다. 그리고 컴퓨터 네트워크의 발달로 전자결재나 전자계약 등의 네트워크를 통한 응용 서비스의 창출이 가능하게 되었으며 통신에 의한 모든 서비스가 가능하게 되었다. 이 과정에서 통신 서비스
제공을 위한 프로토콜이 필요하게 되었으며 특히 서비스 보호를 위한 암호화 프로토콜이 필요하다.

그러나 아직까지 불확정전송 프로토콜과 공정한 비밀정보교환 프로토콜에 대한 개념정립이 미흡한 상태이고, 관련 기초 및 응용연구 실적 또한 미흡한 실정이다. 따라서 불확정전송 프로토콜 및 공정한 비밀정보교환 프로토콜에 대한 개념정립이 필요하고, 불확정전송 프로토콜 및 공정한 비밀정보 교환 프로토콜에 관한 연구와 암호화 응용 프로토콜에 대한 응용 연구가 요청되어진다. 또 국외로부터 기술도입이 가능하게 된다고 하더라도 많은 기술료를 지불해야하고 국내 환경에 적용하는 과정에서의 어려움을 감수해야 하며 독점성이 강한 암호화 응용 기술의 특성으로 인하여 기술 속박상태에 빠질 우려가 있다고 판단된다. 따라서 전자결재, 전자계약, 전자화폐, 전자선거 등의 다양한 암호화 응용 프로토콜의 기본 도구가 되는 불확정전송 프로토콜 및 공정한 비밀정보교환 프로토콜의 연구가 절실히 요구된다.

본 논문에서는 기존의 공정한 비밀정보교환 프로토콜과 그 기본도구가 되어 있는 불확정전송 프로토콜에 대한 분석을 통하여 보다 안전하고 공정하며 신뢰성이 보장되는 공정한 비밀정보교환을 위한 불확정전송 프로토콜을 설계하였다. Bit Commitment를 적용하여, 기존의 비대화형 불확정전송 프로토콜에 있어서 간과되어 왔던 다양한 부가기능을 갖도록 하였다.

본 논문은 2장에서는 기존의 프로토콜을 살펴보고 3장에서는 제안한 프로토콜과 검증내용을 기술하며, 4장에서는 제안한 프로토콜의 특성과 효율성, 기능 등을 고찰 분석하며, 5장에서는 결론을 맺는다.

2. 기존의 프로토콜

본 논문에서는 Bellare 와 Micali[1]등에 의해서 제안된 비대화형 불확정전송 프로토콜을 살펴보고 새로운 비대화형 불확정전송 프로토콜의 확장 방안을 제안한다. 제안하는 방식은 기존의 대화형 방식보다 전송될 정보의 양이 감소된다. 또한 Bit Commitment 기법을 적용함으로써 보다 안전하고 다양한 부가기능을 갖게된다.

2.1 ElGamal 암호

본 논문에서 제안하는 비대화형 불확정전송 프로토콜의 수학적 기초가 되고 있는 이산대수 문제와 ElGamal 암호를 살펴보자.

이산대수문제란 소수 P, m, y(단 0<m, y<p)가 주어졌을 때

$$y \equiv m^x \bmod p$$

를 만족시키는 $0 \le x < p-1$ 범위의 x 를 구하는 문제이다.

m, x, p 가 주어져 y를 구하는 계산은 RSA 암호에서도 이용되는 멱승계산이고 비교적 간단히 계산 가능하다. 그러나 이산대수를 구하는 계산은 다항식시간으로 실행 가능한 알고리즘이 발견되고 있지 않고 큰 법에서 곤란한 문제라고 간주된다.

ElGamal 암호는 p 를 소수로 했을 때 법 p의 이산대수문제의 곤란함을 이용한 암호방식이다.

키의 생성

단계 1 : 큰 소수 p (10진 100자 이상)를 선택

단계 2 : Z_p^* 의 생성원 (법 p의 원시근) g를 하나 선택

단계 3 : $Z_{p-1} - \{0\}$ 의 요소 x를 하나 선택

$y = g^x \pmod p$ 를 계산한다.

단계 4 : y, g, p를 암호화키로서 공개하고 x를 비밀로 보유한다.

암호화

단계 1 : 공개화일에 액세스해서 송신상대의 암호화키 (y, g, p) 를 입수한다.

단계 2 : 난수 $k (\in Z_{p-1} - \{0\})$를 생성한다.(k는 암호화때 갱신)

단계 3 : 평문M $(\in Z_p^*)$를 다음과 같이 암호화한다.

$$c = (c_1, c_2) = (g^k \pmod p, My^k \pmod p)$$

단계 4 : 암호문 c (Z_p^*의 요소 c_1, c_2 2조)를 송신한다.

복호화

단계 1 : 수신한 c에 대해 비밀키 x를 사용해서 d를 계산한다.

$$d = c_1^x \pmod{p}$$

단계 2 : d의 Z_p^*상의 승법역원을 사용해서 다음과 같은 식으로부터 M을 복원한다.

$$\begin{aligned} c_2 d^{-1} &= M y^k (g^{kx})^{-1} \pmod{p} \\ &= M (g^{xk})(g^{kx})^{-1} \pmod{p} \\ &= M \pmod{p} \end{aligned}$$

2.2 1-out-of-2 NIOT

Bellare와 Micali[1]는 센터와 공개게시판을 이용한 1-out-of-2 NIOT를 제안하였다. (그림 2-1)

사전처리단계

- 센터는 소수 p, $g \in Z_p$ 및 $c \in Z_p$를 공개게시판에 등록한다.
  갑돌이는 비밀 난수 x를 선택하여
  $(\beta_0, \beta_1) = \left(g^x, \frac{c}{g^x}\right)$ 또는 $\left(\frac{c}{g^x}, g^x\right)$라하고,
  β_0, β_1을 공개게시판에 등록한다.
- 갑순이는 $\beta_0\beta_1 = c$를 계산하여 갑돌이의 공개키가 정당한가를 확인한다.

프로토콜

- 갑순이는 (p, g, β_0) 및 (p, g, β_1)를 ElGamal 암호의 공개키로 보고 S_0, S_1를 각각 암호화해서 갑돌이에게 보낸다.
- 갑순이는 $y_0, y_1 \in \{0, 1, \ldots, p-2\}$를 임의로 선택하여 $(g^{y_0}, S_0\beta_0^{y_0})$,
  $(g^{y_1}, S_1\beta_1^{y_1})$을 갑돌이에게 보낸다.
- 갑돌이는 β_0, β_1 중 어느 한 쪽만의 이산대수를 알고 있다.
  따라서
  S_0, S_1 중 어느 한 쪽만 구할 수 있다.

NIOT'$_2$ 프로토콜

(사전 처리 단계)

- 센타는 공개게시판에 소수 p, 원시근 g, c $\in Z_p$ 공개
- B는 공개게시판에 $(\beta_0, \beta_1) = (g^x, c/g^x)$ or $(c/g^x, g^x)$ 공개

(프로토콜)

- 공개키 (p, g, β_0)
  (p, g, β_1)

-ElGamal 암호

$y_0, y_1 \in \{0, 1, \ldots, p-2\}$

$X_1 = (g^{y_0}, S_0 \beta_0^{y_0})$

$X_2 = (g^{y_1}, S_1 \beta_1^{y_1})$

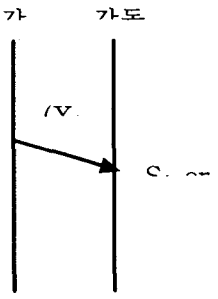


그림 2-1 Bellare와 Micali의 NIOT 방법
Fig 2-1 NIOT Method of Ballare and Micali

3. 제안한 프로토콜

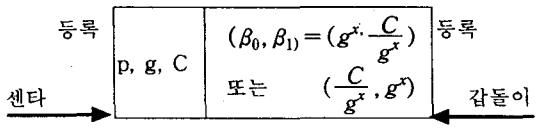
본 절에서는 Bellare와 Micali가 제안한 1-out-of-2 NIOT에 Bit Commitment기법을 적용하여 NIOT를 확장 제안한 방법을 기술한다.

3.1 Bit Commitment를 이용한 NIOT

공증정보와 Bit Commitment 기법을 이용하여 기존의 검증가능 불확정전송에서 고려하지 않은 송신자의 신원확인과 송신자의 송신사실부인 방지의 부가적인 기능을 갖도록 기존 방법을 확장하였다.

R_1, R_2는 갑순이가 생성하는 두 개의 임의의 비트 스트링이고 H는 갑순이가 사용하는 일방향함수이다. 또, HR_1은 갑순이가 일방향함수 H를 메세지 (R_1, R_2, X_A)에 적용하여 계산한 결과이고 HR_2는 갑돌이가 갑순이가 보내온 일방향함수 H를 메세지(R_1, R_2, X_A)에 적용하여 계산한 결과이다.

본 논문에서 제안한 Bit Commitment를 이용한 비대화형 불확정전송 프로토콜의 개요는 그림 3-1과 같다.



	(갑순이)		(갑돌이)
단계 1	· (p, g, β_0) 및 ElGamal 암호 공개키로 보고 S0, S1을 암호화 $X_0=(g^{y_0}, S_0\beta_0^{y_0})$ $X_1=(g^{y_1}, S_1\beta_1^{y_1})$ $X_A=(X_0, X_1)$ · 임의의 비트 스트링 R_1, R_2를 생성 · 메세지 구성 : (R_1, R_2, X_A) · 일방향 함수 (H) 적용 HR_1을 계산 $HR_1 \equiv H(R_1, R_2, X_A)$ · HR_1과 R_1을 전송 · 원래 메세지와 일방향 함수 전송	HR_1, R_1 → $(R_1,R_2,X_A),H$ →	
단계 2			· 수신한 메시지와 함수로 계산 $HR_2 \equiv H(R_1, R_2, X_A)$ · (HR_1, R_1)과 (HR_2, R_1)비교 같으면 프로토콜 계속 다르면 프로토콜 중지 · HR_1, R_1을 저장 · β_0, β_1 중 어느 한쪽만의 이산대수를 알고 있으므로, X_A로부터 S_0, S_1중 어느 하나만을 복호화 할 수 있다.

그림 3-1 Bit Commitment를 이용하여 제안한 NIOT
Fig. 3-1 Proposed NIOT using Bit Commitment scheme

3.2 프로토콜 설명

제안기법의 프로토콜 전개 순서를 살펴보면 다음과 같다.

사전 처리 단계

• 센타는 소수 p, g∈Zp 및 C∈Zp를 공개 게시판에 등록한다.

• 갑돌이는 비밀난수 x를 선택하여

$(\beta_0, \beta_1)=(g^x, \frac{C}{g^x})$ 또는 $(\frac{C}{g^x}, g^x)$ 라하고, (β_0, β_1)을 공개 게시판에 등록한다.

• 갑순이는 $\beta_0 \cdot \beta_1$ = C를 계산하여 갑돌이의 공개키가 정당한가를 확인한다.

프로토콜

단계 1 : • 갑순이는 (p, g, β_0)와 (p, g, β_1)을 ElGamal 암호의 공개키로 보고 다음과 같이 S_0, S_1을 암호화한다.

$$X_0=(g^{y_0}, S_0\beta_0^{y_0})$$

$$X_1=(g^{y_1}, S_1\beta_1^{y_1})$$

$$X_A=(X_0, X_1)$$

• 갑순이는 임의의 비트 스트링 R_1과 R_2를 생성한다.

• 생성한 비트 스트링과 X_A를 이용하여 메세지를 구성한다.

(R_1, R_2, X_A)

• 갑순이는 이 메세지에 자신의 일방향 함수 H를 적용하여 HR_1을 계산한다.

$HR_1 \equiv H(R_1, R_2, X_A)$

• 갑돌이는 계산한 결과치 HR_1과 두 개의 스트링중 하나인 R_1을 갑돌이에게 전송한다.

HR_1, R_1

• 갑순이는 원래의 메세지와 자신이 일방향 함수(H)를 갑돌이에게 전송한다.

(R_1, R_2, X_A),H

단계 2 : • 갑돌이는 나중에 수신한 원래의 일방향 함수로부터 HR_2를 계산한다.

$HR_2 \equiv H(R_1, R_2, X_A)$

• 갑돌이는 단계 1에서 먼저 수신한 (HR_1, R_1)과 계산한 결과치 (HR_2, R_1)을 서로 비교하여 이들이 서로 일치하면 프로토콜을 계속하고, 일치하지 않으면 프로토콜을 즉시 중지한다.

• 분쟁시 갑순이의 송신사실 사후 부인 방지를 위해서 갑돌이는(HR_1, R_1)을 저장한다(이것은 갑순이가 갑돌이에게 메세지를 전송했다는 증거가 된다.)

• 갑돌이는 β_0, β_1 중 어느 한쪽만의 이산대수를 알고 있으므로 X_A로부터 S_0, S_1중 어느 하나의 비밀만을 복호화할 수 있다.

3.3 프로토콜 검증

제안한 프로토콜은 다음과 같이 그 특성을 검증 할 수 있다.

(정리 3.1)
이 프로토콜에 따르면 갑순이와 갑돌이는 서로 상대방을 속이는 부정행위를 할 수 없다.

(증명)
그림 3-1 의 제안한 프로토콜 **단계 1**에서 갑순이가 갑돌이에게 $HR_1 \equiv H(R_1, R_2, C_2)$과 R_1을 전송하는 것은 갑순이가 갑돌이에게 비밀정보를 위임했다는 증거이다. 이때 갑순이의 일방향함수(H)는 갑돌이로 하여금 그 함수를 역변환하여 그 비밀정보 누출을 방지한다.

이 프로토콜의 특성은 **단계 2**에서 갑돌이가 어떠한 메세지도 보낼 필요가 없다는 점이다. 갑순이는 갑돌이에게 비밀정보를 맡기기 위해서 하나의 메세지를 전송하고, 그 비밀정보를 공개하기 위해서 다른 메세지를 전송하면 된다. 이때 갑돌이의 임의의 스트링은 필요하지 않게 된다. 왜냐하면 갑순이가 갑돌이에게 비밀정보를 위임했다는 사실의 결과가 곧 일방향함수에 의해 계산된 메세지이기 때문이다.

(정리 3.2)
이 프로토콜에 따르면 서로가 위임한 값을 마음대로 유추하거나 계산해 낼 수 없다.

(증명)
그림 3-1의 **단계 2** 에서 갑돌이는 상대방을 속이는 부정행위를 할 수 없고 다른 메세지 즉 $H(R_1, R, _2, X_A) = H(R_1, R_2', X'_A)$와 같은 $H(R_1, R'_2, X'_A)$를 찾을 수 없다. 또 갑순이는 R_1을 갑돌이에게 전송함으로써 비밀정보(X_A)의 값을 위임하고 있는 것이다. 만약 갑순이가 R_2를 비밀로서 가지고 있지 않다면, (즉 갑돌이가 R_2를 알고 있다면) 갑돌이는 $H(R_1, R, _2, X_A)$와 $H(R_1, R_2', X'_A)$을 둘 다 계산할 수 있을 것이고 그리고 어떠한 것이 갑순이로부터 받은 것과 같은지를 알 수 있을 것이다. 즉 R_2를 갑순이가 비밀로서 가지고 있음으로서 갑돌이는 갑순이가 위임한 X_A의 값을 마음대로 유추하거나 계산해 낼 수 없다.

4. 프로토콜 고찰

4.1 특성비교

제안한 Bit Commitment를 이용한 비대화형 불확정 전송 기법과 기존의 ElGamal과 Micali에 의한 비대화형 불확정전송기법의 특성을 비교 분석하였다. 표 4-1에서는 각 기법을 Primitive Problem, 서명기법, 비교특성 측면에서 분석하였다.

표 4-2에서는 기존의 기법과 제안한 기법들의 프로토콜 실행중의 특성메세지 노출가능성, 송수신자 부정행위가능성, 송신사실 부인가능성, 분쟁시 해결가능성, 송신자 확인가능성, 통신단계수 및 송수신자의 계산량 등 효율성과 부가기능 측면에서 비교 분석하였다.

제안한 방식은 기존의 프로토콜의 절차를 그대로 따르면서 Bit Commitment 기법 을 추가한 형태로서 기존 프로토콜의 특성을 그대로 가진다.

표 4-1 제안기법의 특성 비교
Table 4-1 Comparison of characteristics int the Proposed Method

기법 / 비교항목	기존기법	제안기법
Primitive Problem	Discrete Logarithm Problem	Discrete Logarithm Problem
서명기법 (Signature Scheme)	없음	Bit Commitment
비교 특성	ElGamal 암호	ElGamal 암호 + B.C
송신자 확인기능	없음	있음
송신부인 방지기능	없음	있음

4.2 효율성 및 기능 비교

표 4-2 제안기법의 효율성 및 부가기능 비교표
Table 4-2 Comparison of Efficiency and Additional Functions in the Proposed Method

○ : 양호 , × : 불리

비교항목 \ 기법	기존기법	제안기법
프로토콜 실행중 특성 메세지 노출 가능성	없음(○)	없음(○)
송수신자 부정행위 가능성 (cheating)	많음(×)	적음(○)
송신사실 사후 부인 가능성	있음(×)	없음(○)
사후분쟁 해결 가능성	적음(×)	많음(○)
송신자 확인 가능성	불가(×)	가능(○)
통신단계수	적음(○) 1회	많음(×) 2회
송수신자의 계산량	적음(○)	많음(×)

표 4-2는 제안한 기법들과의 효율성 및 부가기능을 비교 분석한 결과이다.
표 4-2에서 보는바와 같이 제안한 기법들은 기존의 기법과 비교 할 때 송수신자 부정 행위 가능성, 송신자신원 확인가능성, 분쟁시 해결가능성 측면에서 양호함을 보이고 있으며, 통신단계수와 송수신자의 계산량 측면에 있어서는 기존의 기법에 비해 많은 계산량을 요구하여 다소 불리함을 알 수 있다. (표 4-3참조)

효율성 측면에서는 다소 불리하나 송신자 확인 및 송신사실 사후 부인 방지 등 여러 부가적인 기능을 가지는 측면에서는 제안된 기법이 우월함을 알 수 있다.

표 4-3 제안기법의 통신량 및 계산량 비교
Table 4-3 Comparison on Amount of Communication and Computation in the Proposed Method

구분	통신단계수	송수신자 계산량
기존기법	1 회	1.0
제안기법	2 회	1.02 ~ 1.10

5. 결 론

본 논문에서는 Bellare와 Micali가 제안한 비대화형 불확정전송 프로토콜을 기반으로 송신자의 신원 확인 및 송신 사실의 부인 방지기능 등 여러 가지 부가기능을 가지는 새로운 비대화형 불확정전송 프로토콜을 설계하고 제안하였다.

제안한 방식은 기존의 프로토콜을 그대로 따르면서 Bit Commitment 기법을 추가한 형태로서 기존 프로토콜의 공정성, 검증가능성, 안전성을 그대로 가진다. 부가된 기능에 따라 두 당사자는 송신자의 신원 확인 및 송신 사실을 부인 할 수 없게 된다. 따라서 이 프로토콜에 따르면 양자 부정 행위가능성, 분쟁 해결 가능성, 송신자 신원 확인 가능성, 송신 사실 부인 방지 가능성 면에서 우수하나 통신량 및 계산량 면에서는 다소 불리하다.

본 논문에서 제안한 기법은 서로 신뢰하지 못하는 두 당사자 사이에서 공정하게 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 당사자 사이에서도 적용 가능한(Multi-party protocol로의)확장이 될 것이다. 또한 본 논문 내용을 바탕으로 한 보다 구체적인 구조 설계와 시스템 구현이 필요하다.

참 고 문 헌

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

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

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

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

[5] S. Even, O. Goldreich, and A. Lempel. "A Randomized Protocol for Singing Contracts", Comm. of the ACM 28:6, 1985, 637-647. Early version : Proceedings of Crypto 1982, Springer-Verlag, pp205-210, 1983.

[6] M. J. Fisher, S. Micali and C. Rackoff, "A Seccure Protocol for the Oblivious Transfer", Journal of Cryptology, Vol. 9, No. 3, pp. 191-195, 1996.

[7] L. Harn and H. Lin, "Non interactive oblivious transfer", Electronic Letters, Vol.26, NO.10, pp.635-636, 1990.

[8] S. G. Kim, N. Lee, S. Chung, and H. Kwack, "A Non- interactive Oblivious Transfer Protocol for the Exchange of Secrets", Proceedings of the 6th IEEE International Workshop on Intelligent Signal Processing and Communication Systems(ISPACS '98) Volume II, pp.904 - 907, Nov, 1998

[9] S. G. Kim, N. Lee, S. Chung, and H. 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.

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

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

[12] 김순곤, 송유진, 강창구, 안동언, 정성종, "Bit Commitment와 디지털서명을 이용한 대화형 불확정전송 프로토콜", 한국통신학회논문지 제 24권 8호, pp.1227-1237, 1999. 8

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