추적 가능한 새로운 전자화폐 프로토콜 제안

정철종 , 전병욱, 권용진
한국항공대학교 항공통신정보공학과

A proposal of new traceable Electronic cash protocol

Cheol Jong Jeong°, Byeong Wook Jun and Yong Jin Kwon
Dept. of Telecomm. and Inform Eng. Hankuk Aviation University

요 약

현재 전자 상거래에서 사용되는 전자 지불 시스템은 있어서 핵심적인 기술인 전자 지불 시스템에 대한 연구가 활발하게 진행되고 있으며 많은 시스템이 제안 및 구현되고 있다. 초기의 전자 지불 시스템은 안전성과 편리함, 그리고 개인적인 Privacy에 초점을 맞추었지만 최근에는 여러 가지 사회, 경제적인 문제점들이 제기되어 이의 해결을 위한 연구가 진행되고 있다. 특히 전자 지불 시스템은 실물 경제와 달리 전자 화폐를 사용함으로서 화폐의 이중사용 또는 돈 세탁 등이 용이하다는 문제가 발생하게 된다. 이와 같은 부정사용을 사전에 차단하기 위해서는 화폐에 어떠한 조건을 부가하여 추적이 가능하도록 하는 조건부 추적 가능성이 요구되며, 이는 전자 화폐의 저변 확대를 위해서 해결해야만 할 문제로 간주되고 있다. 본 논문에서는 blind signature 기법을 이용하여 필요시에 전자 화폐와 사용자를 연결할 수 있는 조건부 추적 가능성을 갖는 새로운 전자 지불 시스템을 제안한다.

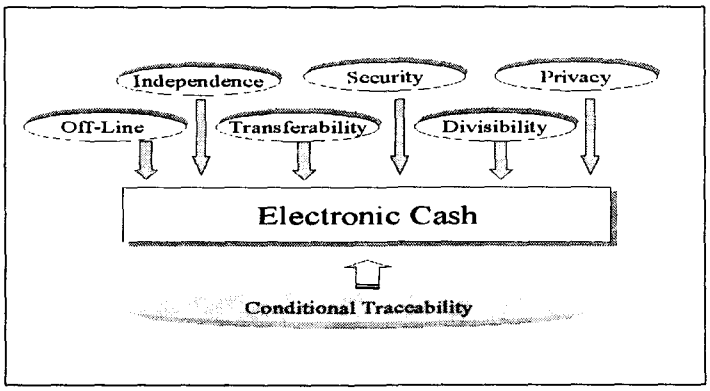
1. 서 론

현대 사회가 산업 사회에서 정보 사회로 변화됨에 따라 기존의 상거래의 개념에서 벗어난 새로운 개념의 상거래 형태가 정립되고 있다. 특히 최근 관심이 증대되고 있는 분야가 인터넷 환경을 배경으로 하는 전자 상거래(Electronic Commerce)이다. 이러한 전자

상거래에 있어 고려되어야 할 사항들 중에서 큰 비중을 차지하고 있는 것이 전자 지불 시스템(Electronic Payment Systems)이다. 기존의 화폐를 대체하는 전자 지불 방식은 전자 화폐, 전자 수표, 신용 카드, EFT 등이 있으며 이 중에서 전자 화폐는 실물 화폐와 유사한 성질을 갖도록 디지털화 된 화폐이고, 가장 현실성 있는 대안으로 평가되고 있다. 전자 화폐에 대한 연구 개발은 1982년 David Chaum의 On-Line형 전자 화폐 시스템[1]이 처음 등장한 이후에 전자 화폐에 요구되는 여러 가지 조건을 만족시키는 방법들이 제안되고 있다. 전자 화폐가 지녀야 할 대표적인 성질들은 다음과 같다[2].

- Independence(비 의존성)
- Security(보안성)
- Privacy(익명성)
- Off-Line Payment(오프라인 상에서의 지불)
- Transferability(양도성, 가치이전성)
- Divisibility(분할성)

개발 초기에는 화폐의 안전성과 편리함 및 개인의 Privacy에 초점을 맞추었지만 최근에는 여러 가지 사회, 경제적인 문제점의 해결을 위한 연구가 진행되고 있다. 이러한 문제점의 하나는 은행이 전자 화폐 사용자가 전자 화폐의 익명성을 이용하여 여러 상점에서 하나의 전자 화폐를 여러 번 사용한 경우 이 전자 화폐의 중복 사용을 방지 할 수 없다는 것이다. 또 다른 문제로는 범죄자들에 의해 초래되는 돈 세탁의 용이 함이다. 익명성이 보장된 경우에는 어느 누가 이 전자 화폐를 보냈는지 또 누가 그 전자 화폐를 받았는지를 알 수 없는 문제가 발생한다. 이러한 문제를 방지하기 위해서 모든 화폐 사용자의 신원을 파악하고 있어야 한다. 그러나 이것은 전자 화폐의 익명성이 제거됨을 의미한다. 따라서 익명성은 보장되면서 전자 화폐의 이중 사용이나 돈 세탁의 문제점을 해결해야 한다. 이러한 부정 행위를 방지하기 위해 추가된 것이 조건부 추적 가능성이다. 부정 행위를 한 경우 은행과 신뢰 기관은 서로 협조하여 부정 사용자의 신원을 확인할 수 있어야 한다. 그러나 어느 기관도 단독으로는 사용자의 신원을 확인 할 수 있다면 개인의 privacy는 보장받을 수 없을 것이다.



[그림 1] 전자지불 시스템의 조건
(Condition of Electronic Payment System)

본 논문에서는 Blind Signature 기법을 이용하여 전자 지불 프로토콜에 조건부 추적성을 부여하는 새로운 방법을 제안하고자 한다. 2장에서 기본 blind signature에 대하여 소개하고 3장에서 추적 가능한 전자 화폐 시스템을 제안하고 4장에서 제안 방식의 특성 및 안전성에 대해 검토한다.

2. 기본 프로토콜

David Chaum에 의해 제안된 Blind Signature 기법을 이용하여 신뢰 기관과 은행에서 각각의 서명을 얻어 사용자의 신원을 Blinding하는 방법으로 은행과 신뢰 기관이 서로 협조하지 않으면 사용자의 신원을 알 수 없도록 하는 것이 본 논문의 기본 개념이다. 다시 말하면 신뢰 기관 단독으로 사용자를 추적하여 사용자의 화폐와 사용한 곳을 알 수 없으며 또한 은행은 누가 이 화폐를 사용했는지 알 수 없다. 다만 은행과 신뢰 기관이 정당하게 법원 등으로부터 허가를 얻고 신뢰 기관과 은행이 서로 협조하면 그 사용자의 신원은 물론 어느 곳에 사용했는지를 알 수 있다. 또한 정당한 사용자라도 법원 등의 정당한 기관으로부터의 사용자 확인이 요구되면 사용자의 신원을 확인 할 수 있어야 한다.

2.1 Blind Signature 기본 프로토콜

Blind signature scheme의 기본 개념은 Chaum 의해 소개되었다. Blind signature scheme 은 기본적으로 송신자와 수신자, 두 개의 Entity를 가진다. 송신자가 수신자에게 메시지를 전송하면 수신자는 자신의 서명을 덧붙여 송신자에게 다시 전송한다. 그러면 송

신자는 그 서명된 정보로부터 임의의 정보를 제거하여 익명성을 갖는다. 이러한 프로토콜 사용의 예로는 전자 선거 프로토콜이나 전자 지불 프로토콜 등이 있다 3)4)5)6)7).

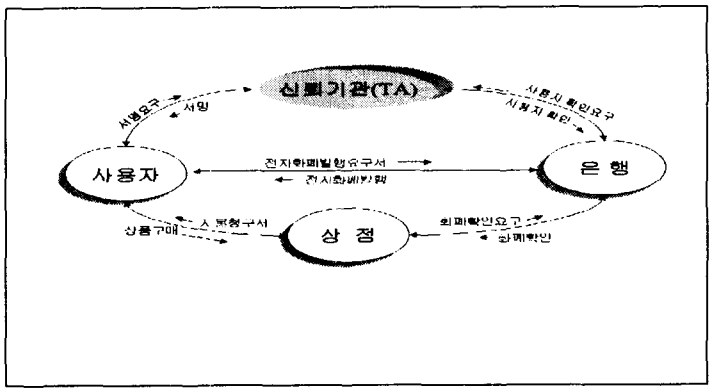


그림 2 전자상거래의 기본 모델
The Model of Electronic Commerce scheme

먼저 David Chaum에 의해 제안된 Blind Signature 프로토콜을 간단히 살펴보면 다음과 같이 세 단계로 구성된다.

- Blinding 단계 : 수신자는 0과 n 사이의 랜덤한 정수인, blinding factor r을 선택하고 $m' = mr^e \bmod n$ (m은 메시지)을 계산한 후, 서명자에게 이 m'을 보낸다.
- Signing 단계 : 서명자는 자신의 비밀키 d을 이용하여 $s' = m'^d \bmod n$ 을 계산하고 수신자에게 s'을 돌려보낸다.
- Unblinding 단계 : 수신자는 서명 $s = s'/r \bmod n$ 을 얻는다.

본 논문에서 제안하고자 하는 방식은 RSA[8] 알고리즘을 이용한 각 Entity의 키 생성과 이산 대수 문제 및 해쉬 함수에 기반을 둔 서명 기법을 사용하고 있다.

2.2 새로운 추적 가능한 전자 화폐의 기본 프로토콜

익명성이 유지되는 전자 화폐를 사용하는 경우 이 전자 화폐는 범죄자들에 의해 오용될 위험이 있다. 이러한 익명성이 존재하는 지불 시스템은 blind signature scheme에 의해 인출과 지불간의 관계를 서로 연결시키지 못하게 된다. 이러한 인출과 지불의 비연결성으로 인해 돈 세탁 또는 해외 자금 유출 등의 불법적인 일에 전용 될 것이다. 그러나

전자 화폐가 소액인 경우 이러한 문제는 크게 대두되지 않는다. 하지만 우리는 이러한 문제가 존재하며 완전한 디지털 지불 시스템에서 필연적으로 발생될 것을 알고 있다. 이것은 또한 고액의 경우에 적용하면 많은 양의 돈을 익명으로 전송 할 수 있게 된다. 따라서 불법적인 거래가 발생 될 위험이 있다.

그러나 법적인 절차에 따라 신뢰기관에 의해 익명성이 제거되어 진다면 아주 유용하게 될 것이다. Micali는 사용자들에 의한 불법 사용을 막기 위해 fair cryptosystems의 개념을 제안했다.[9)]

본 논문에서는 이러한 개념을 중심으로 새로운 조건부 추적 가능성을 갖는 전자 화폐 프로토콜을 제안한다. 먼저 추적 가능성을 부여하기 위해 신뢰 기관을 두고 또한 은행, 사용자 등이 존재하는 모델로 구성되어 있다. 사용자는 신뢰 기관으로부터 자신의 ID를 사용하여 서명을 받는다. 그 서명된 값을 blind 기법을 사용하여 신뢰 기관이 자신을 알지 못하도록 하되 신뢰 기관의 인증은 유효하도록 한다. 그 값을 이용하여 은행으로부터 돈을 인출하고 다시 은행으로부터 은닉하기 위해 blinding을 실시한다. 따라서 은행은 이 돈에 대해 사용자를 알 수 없고 서명자 또한 사용자를 알 수 없다. 그러나 적당한 방법, 즉 은행과 신뢰 기관의 상호 협력에 의해 사용자를 알아 낼 수 있다.

3. 제안 방식

3.1 시스템 파라메타 (System Parameter)

본 논문에서는 임의 길이의 비트 스트링을 입력으로 받아 고정된 짧은 길이의 비트 스트링으로 출력하는 해쉬 함수를 사용한다. 현재까지 많은 해쉬 함수가 제안되었지만, 본 논문에서 사용되는 해쉬 함수는 Rivest에 의해 제안된 MD5, 또는 SHA-1등 지금까지 안전하다고 알려진 해쉬 함수[10)]를 사용한다. 각 사용자는 자신의 ID를 사용하여 신뢰 기관으로부터 인증을 받고 은행으로부터 자신의 계좌에서 돈을 인출한다.

f( ) : 안전한 hash
ID : 은행, 신뢰기관(TA) 모두 공통 소유

가. 신뢰기관(Trust Center : TA)

신뢰 기관은 큰 두 개의 소수를 구하고 그 소수의 곱(n)을 공개하고 이 두 소수를 비밀로 한다. 신뢰 기관에서는 사용자의 인증을 위한 공개키(e_{TA})와 비밀키(d_{TA})를 생성한다. 또한 Data 암호화와 복호화를 위해 신뢰 기관은 암호화 공개키와 복호화 비밀키를 생성한다.

p_{TA}, q_{TA} : 소수 , $n = p_{TA} \times q_{TA}$
e_{TA} = 신뢰기관의 인증 비밀 *Key*
d_{TA} = 신뢰기관의 인증 공개 *Key*
E_{TA} = 신뢰기관의 암호화 공개 *Key*
D_{TA} = 신뢰기관의 복호화 비밀 *Key*

나. 사용자

사용자는 신뢰 기관이 공개한 n 을 사용하여 큰 소수 p와 q를 구한다. 그리고 그 두 소수의 곱을 M이라 한다. 또한 p상의 임의의 랜덤 정수 r을 선택하며, 화폐의 일련 번호로 사용 할 랜덤 한 정수(x)를 선택한다. 또한 은행과의 전자 화폐 인출에 사용 될 은닉 서명용 랜덤 정수를 선택한다. 사용자의 생성 parameter는 다음과 같다.

$p, q \in Z_n$: prime
$M = p \times q \pmod{n}$
r : Random number in Z_p
x : 화폐 일련 번호
m : 인출 금액
a : random prime [1, n-1]

다. 은행(BANK)

은행은 화폐 서명을 위해 은행의 공개키와 비밀키와 공개키를 생성한다. 은행에서는 다음과 같은 parameter를 생성한다.

e_B = 은행의 공개키
d_B = 은행의 비밀키

3.2 사용자 인증

사용자는 신뢰기관으로부터 자신이 올바른 사용자임을 서명 받기 위해 [그림 3]과 같이 행한다.

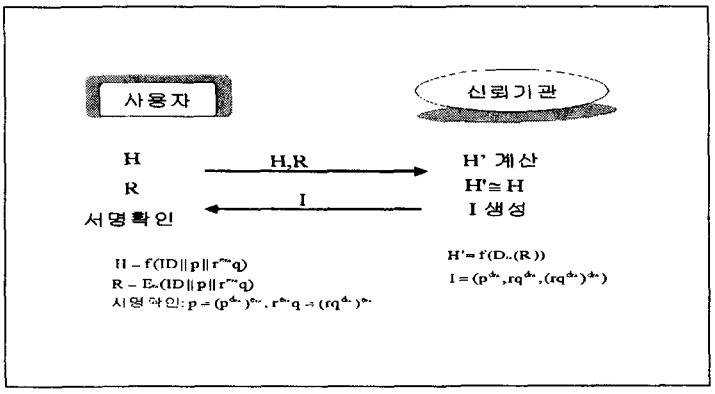


그림 3 사용자 인증 프로토콜
User's Certification protocol

사용자 인증 프로토콜을 구체적으로 알아보면 다음과 같은 단계를 거친다.

step 1. 사용자는 소수 p와 q, 랜덤 r을 생성한다. 이를 이용하여 H와 R을 신뢰기관에 보낸다.

$$H = f(ID||p||r^{e_{T.1}}q)$$

$$R = E_{TA}(ID||p||r^{e_{T.1}}q)$$

step 2. 신뢰기관에서는 H'를 구한다. 이때 사용자로부터 전송된 R을 복호화 한 후 해쉬하여 사 용자로부터 전송되어진 H와 H'과 비교하여 서로 같으면 p와 $r^{e_{T.1}}q$ 에 신뢰 기관의 비 밀키로 서명하고, I를 계산하고 사용자에게 전송한다. 이때 신뢰기관은 S와 ID를 기억한 다. 이 때 H'과 S는 다음과 같다.

$$H' = f(D_{TA}(R)) \ , \ S = (rq^{d_{T.1}})^{d_{T.1}}$$

step 3. 사용자는 자신의 수신한 서명된 값이 제대로 된 값인지를 검증한다.

3.3 전자화폐 발행 단계

사용자는 은행으로부터 전자 화폐를 발행 받기 위해 다음 [그림 4]와 같은 프로토콜을 행한다.

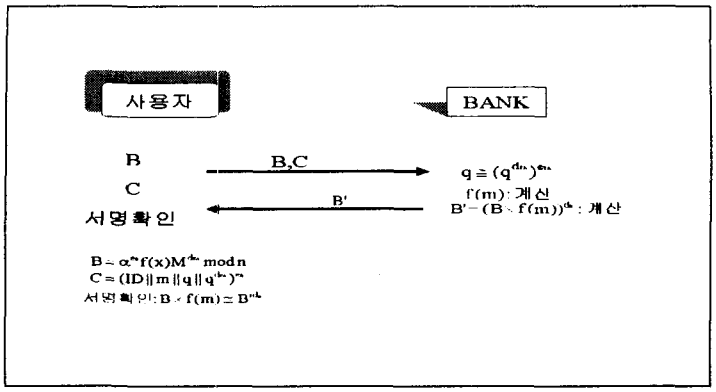


그림 4 은행과 사용자간의 화폐 인출
Electronic Cash withdraw between user and bank

step 1. 사용자는 화폐 일련 번호와 인출할 금액, 그리고 랜덤 한 값을 생성하여 B와 C를 계산 한 후 은행측에 전송한다.

$$B = \alpha^{e_B} f(x) M^{d_{T\cdot1}} \bmod n$$

$$C = (ID \| m \| q \| q^{d_{T\cdot1}})^{e_B}$$

step 2. 은행은 사용자로부터 전송된 B와 C를 받아서 먼저 C의 값으로부터 각각의 값을 복원하 여 신뢰 기관의 서명을 확인한다. 신뢰 기관의 서명이 유효하다면 전자 화폐를 발행한다.

전자 화폐를 발행하는 과정은 다음과 같다.

① 사용자로부터 전송된 m을 사용하여 f(m)를 구하여 f(m)를 B에 곱한다.

② 그 값에 다시 은행의 비밀키 d_B로 은행의 서명(sign)을 한다.

$$(Bf(m))^{d_B}$$

③ 은행이 서명한 값을 사용자에게 전송한다.

step 3. 사용자는 은행으로부터 전송된 값을 검증한다. 그 값이 유효하면 전송된 값을 Blind 한 다.

$$D = (Bf(m))^{d_B} \times \alpha^{-1} \bmod n$$

3.4 대금 지불 단계

은행으로부터 인출된 전자화폐를 사용하여 지불한다.

step 1. 사용자는 다음의 정보를 상점에 제공한다.

$$(x,\ m,\ D,\ M,\ (r^{e_{TA}}p^{-1},\ S)^{e_B})$$

step 2. 상점은 사용자로부터 수신한 전자화폐를 은행에 보내어 이중 사용유무에 대한 검사를 의 뢰한다.

step 3. 은행은 상점으로부터 수신한 전자 화폐의 정보를 이용하여 f(m)과 f(x)를 계산한다. 계산값 f(m)과 f(x)의 곱에 e_{TA} 을 사용하여 계산한 후 이를 사용하여 $D^{e_B e_{TA}}$ 항을 나눈다. 그 결과 M과 비교하여 같음을 확인한다. $(r^{d_{TA}}p^{-1},\ S)^{e_B}$ 을 은행의 비밀키 d_B를 사용 한 후

$$r^{d_{TA}}p^{-1} \doteq (S^{e_{TA}})^{e_{TA}}$$

을 조사한다. 같으면 화폐의 이중 사용 유무를 조사한다. 만약 처음 사용되었다면 그 x값을 자신의 Data Base 저장하고 이전에 사용된 경우 이중 사용자로 간주하여 S 을 신뢰기관에 통보하여 화폐 사용자를 확인한다.

step 4. 은행으로부터 통보 받은 S을 이용하여 사용자의 ID를 확인한다. 그 ID를 은행에 알린다.

4. 제안 방식의 특성 및 안전성

4.1 사용자 추적 과정

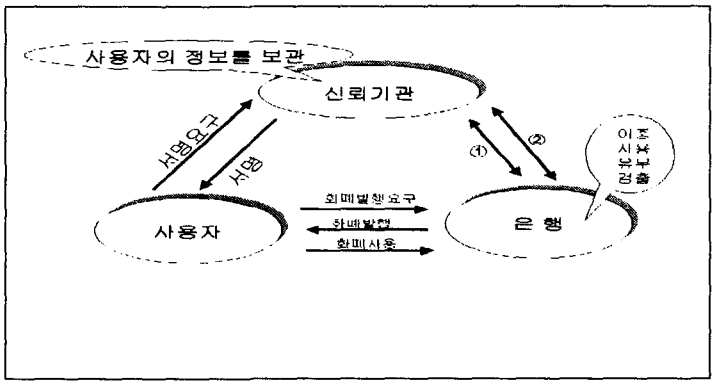


그림 5 사용자 추적
Trace of User

신뢰 기관이 정당한 화폐 사용자의 신원을 검출하기 위해서는 먼저 법원 등의 허가를 얻은 뒤에 ①의 과정을 통해 자신이 가지고 있는 ID에 대한 정보 S 을 은행측에 제

시한다. S 을 받은 은행은 들어온 정보에서 적법성 확인 과정에서 이와 동일한 정보를 가지는 정보를 검출한다. ②의 과정은 은행은 전자화폐의 이중 사용을 검사하는 과정에서 이 화폐가 전에 이미 사용되어진 화폐인 경우 이 화폐 사용자가 제시한 S 을 신원 확인용으로 신뢰 기관에 전송하여 이 정보를 제공한 사용자의 신원을 확인한다. 또한 정당한 사용자라도 법원이나 다른 정당한 기관으로부터 사용자 추적을 요구받은 경우 은행과 신뢰 기관이 서로 협조하여 사용자를 찾아낸다.

4.2 안전성

은행은 모든 사용자의 S을 알 수 있다고는 하지만 이 정보를 특정한 사용자와 matching 하지 못한다. 또한 신뢰기관 단독으로 은행의 정보의 가로채기가 가능하다고 해도 은행의 비밀 key를 알아내는 것은 이산 대수 문제에 속하는 것이다. 그러므로 은행이나 신뢰 기관 단독으로 특정 사용자의 신원을 밝히는 것은 불가능하다. 또한 사용자가 자신의 정보를 제공하지만 그 제공 정보 또한 사용자임으로 조작할 수 없으므로 안전하다.

5. 결 론

본 논문에서는 사용자의 익명성을 유지함에 있어서 돈 세탁 등의 불법적인 사용자들에 대한 대책으로서 그리고 사회, 경제적인 문제 즉 자금 해외 반출 등을 고려 해야한다. 따라서 법원이나 기타 법 집행 기관의 결정이 있으면 사용자가 설령 정당하게 사용하였다하더라도 화폐 사용자가 누구인지를 확인할 수 있는 기능이 전자 화폐 시스템 내에 포함되어 있어야 한다. 이에 본 논문에서는 사용자의 익명성 유지뿐만 아니라 필요시 전자 화폐 사용자를 추적 할 수 있는 기능을 추가하였다. 그리고 추적 시 어느 한 기관이 단독으로 사용자를 추적할 수 있는 것이 아니라 두 기관이 협력해야만 추적할 수 있도록 함으로써 추적성의 남용으로 인한 사용자의 privacy의 침해를 방지하고자 하였다.

[1] D.Chaum, "Blind signatures for Untraceable Payments", Proceeding of Cryto'82, pp.199-203, 1982

[2] T. Okamoto and K. Ohta, "Universal Electronic Cash", Advance in Cryptology-crypto'91, Lecture Notes in CS, Springer-Verlag, 1992, pp32-37

[3] S. Brand: Untraceable Off-line Cash in Wallets with Observe, Proceedings of Crypto '93, LNCS 773, Springer Verlag, pp. 302-318.

[4] J.Camenisch, j.-M. Piveteau, M. Stadler: An Efficient Payment System Protectiong Privacy, Proceedings of ESORICS'94, Lecture Note in Computer Science 875, Springer Verlag, pp.27-215.

[5] D. Chaum, A. Fiat, M.Naor : Untraceable Electronic Cash, Proceedings of Crypto'88, LNCS 740, Springer verlag, pp.319-327.

[6] D. Chaum : Privacy Protected Payment, SMART CARD 2000, Elsevier Science Publishers B.V.(North -Holland),1989, pp.69-93

[7] D. Chaum, B.den Boer, E.van Heyst, S.Mjolesnes, A.SteenBe다: Efficient Offline Electronic Checks, Proceedings of Eurocrypt '89, LNCS 434, Springer verlag, pp.294-301.

[8] R.L.Rivest, A.Shamor and L.Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystem", ACM, vol.21, no.2, pp.120-126,1997

[9] S.Micali: Fair Cryptosystems, Technical Report MIT/LCS/TR-579.b, 1993.

[10] R. Rivest, The MD5 message-digest algorithm, Request For Comments(RFC) 1320, Internet Activities Board, Internet Privacy Task Force, April 1992