# 전자서명 기록기를 이용한 공정한 부인방지 프로토콜의 설계

정회원 이 용 준*, 오 해 석**

# Design of An Fair Non-Repudiation Protocol Using Digital Signature Recorder

Yong-Joon Lee*, Hae-Seok Oh* *Regular Members*

요 약

최근 인터넷의 중요성으로 보다 다양한 보안 서비스가 요구되고 있다. 부인방지 서비스는 새로운 보안 요구사항이다. 인터넷뱅킹, 증권거래시스템, 전자의무기록, 전자상거래 등의 많은 어플리케이션은 부인방지 서비스와 관련이 있다. 그러나 통신의 기밀성이나 신원확인에 대한 보안에 비교하여 부인방지에 대한 연구는 부족했다. 이론적으로, 부인방지 프로토콜이 종료되었을 때 발신자가 수신부인 방지증거를 획득하고 수신자가 발신부인 방지증거를 동시에 획득하거나 쌍방 모두 유효한 증거를 획득하지 못하였을 때 공정하다고 정의한다. 기존의 대부분의 부인방지서비스는 신뢰된 제3자인 TTP(Trusted Third Party)를 기반으로 하여 프로토콜의 단계마다 통신에 관여한다. 따라서 TTP는 통신부하를 발생시키는 단점이 있다. 제안하는 전자서명기록기는 논리적으로 부인방지의 공정성을 보장하면서, 물리적으로 검증서버와 함께 구성하여 네트워크의 부하를 최소화한다.

**Key Words :** Fairness, Non-Repudiation Service, Without TTP, Digital Signature Recorder

ABSTRACT

Due to the overwhelming importance the Internet gained nowadays, more and more sophisticated security services are requested. However many applications such as Internet Banking, Home Trading System, Electronic Medical Recode, electronic commerce, etc. are related to non-repudiation. Non-repudiation services are one of these new security requirements. In comparison to other security issues, such as privacy or authenticity of communications, non-repudiation has not been studied intensively. Informally, we say that a protocol is fair if at the end of the protocol execution either originator receives a non-repudiation of receipt evidence and recipient receives a non-repudiation of origin evidence or none of them receives any valid evidence. The most non-repudiation protocols rely on a trusted third party(TTP) that has to intervene during each protocols run. the TTP may create a communication bottleneck. In this paper, we suggest the digital signature recorder that guarantees fairness logically and supplies minimal network bottleneck to be composed verification server physically.

* 숭실대학교 멀티미디어연구실 (yjlee@koscom co.kr)
** 경원대학교 소프트웨어대학 (oh@kyungwon.ac kr)
논문번호 : KICS2004-7-1114, 접수일자 2004년 7월 22일

## Ⅰ. 서 론

인터넷 기반 통신의 놀라운 성장은 새로운 보안 관련 문제를 발생시켰다. 부인방지 서비스는 새로운 보안관련 문제 중 하나임에 틀림이 없으나 신원확인, 무결성, 기밀성과 같은 다른 보안 요구와 비교하여 연구가 부족했다[1]. 인터넷뱅킹, 증권거래시스템, 전자의무기록, 전자상거래 등의 어플리케이션은 부인방지 서비스와 밀접한 관련이 있다. 부인방지서비스는 발신자가 수신자에게 특정 정보를 전송했을 때, 통신상의 전체 또는 부분적인 참여에 대하여 어느 누구도 부인할 수 없어야 한다. 분쟁이 발생한 경우, 판단하는 기관은 모호함 없이 증거들을 평가하고 올바른 참여자가 누구인지를 결정해야 한다. 발신부인방지는 정보에 대한 전자서명으로 쉽게 제공된다. 전자서명은 발신의 증거에 대하여 반박할 수 없는 부인방지가 가능하다 그러나 수신부인방지는 보다 어렵게 제공된다. 따라서 발신자와 수신자는 부인방지기능을 제공하는 프로토콜을 준수해야 한다. 교환된 부인방지증거의 정확성을 보장하기 위해서 프로토콜은 공정해야 한다. 프로토콜의 수행이 완료되었을 때, 발신자에게 수신부인방지가 제공되며 수신자에게 발신부인방지가 동시에 제공되거나, 송신자와 수신자 모두 유효한 정보를 제공되지 않아야 프로토콜이 공정하다고 말한다[2].

공정성문제를 해결하기 위해 많은 부인방지 프로토콜이 제안되었다 TTP기반 방식과 TTP 배제 방식으로 분류된다. TTP배제 방식은 확률적으로 공정성을 제공하기 때문에 완전한 공정성을 보장할 수 없다[3]. 또한 TTP기반 방식은 프로토콜의 단계마다 통신에 관여한다. 따라서 TTP는 통신부하를 발생시키는 단점이 있다.[4] TTP기반 방식은 E-mail과 전자지불과 같이 P2P(Peer to Peer) 구성에서 적합하지만 인터넷뱅킹, 증권거래시스템과 같은 클라이언트-서버의 구성에는 부적합하다. 서버는 다수의 사용자가 전송한 전자서명을 검증해야 하는 부담이 있기 때문에 TTP 기반의 방식은 현실적으로 적합하지 않는다.

제안하는 전자서명기록기는 논리적으로 부인방지의 공정성을 보장하면서, 물리적으로 검증서버와 함께 구성하여 네트워크의 부하를 최소화한다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 TTP기반 부인방지 프로토콜에 대하여 검토한다. 3장에서는 제안하는 전자서명 기록기를 설계하고 4장에서는 부인방지 프로토콜이 제공해야 하는 필수 요구사항과 비교분석을 한다. 5장에서는 결론을 맺는다.

## Ⅱ. TTP기반 부인방지 프로토콜의 분석

### 2.1 Cooffey and Saidha Protocol

발신자는 세션키키로 암호문발신증거를 수신제안된 TTP는 Non-Repudiation Server(NRS)로 명명하였다. TTP는 발신자와 수신자간의 부인방지 증거를 저장한 후 데이터를 전송한다. 발신자는 TSA(Time Stamp Authority)에 초기발신증거를 전자서명하며 전송한다. 발신자의 전자서명이 유효한 경우 TSA는 최종발신증거를 발신자에게 전송한다. 발신자는 최종발신증거와 함께 초기수신증거를 TTP에 제출한다. TTP는 수신자에게 초기수신증거를 전송한다. 수신자는 초기수신증거를 전자서명하여 TSA에 전송한다 TSA는 수신자의 전자서명이 유효한 경우 최종수신증거를 수신자에게 응답한다. 수신자가 최종수신증거를 TTP에 제출하면 TTP는 발신자에게는 수신부인방지증거 전달하고 수신자에게는 발신부인방지증거를 전달한다. 제안한 프로토콜은 TTP가 전송되는 모든 정보를 저장하기 때문에 강한 공정성을 제공한다. 발신자와 수신자와의 직접통신을 제공하지 않기 때문에 TTP는 전송단계마다 중계자로 사용되어 inline TTP로 분류된다[5].

제안된 inline TTP의 밀접한 간섭에 의해 통신부하가 발생한다. 또한 통신시 발생하는 부인방지정보를 관리해야 하는 부담이 있다.

### 2.2 Zhou and Gollmann Protocol

발신자는 세션키키로 암호문발신증거를 수신자에게 전송한다. 수신자가 정해진 시간 여부를 확인한 후 암호문수신증거를 서명하여 발신자에게 전송한다 발신자는 TTP에 세션키를 서명해서 전송한다. TTP는 발신자의 전자서명을 검증하고 정해진 시간을 초과하지 않는지 확인한다. 정해진 시간이후 TTP는 수신자에는 세션키와 키확인증거를, 발신자에게는 키확인증거를 제공한다. 발신자는 수신자의 암호수신증거와 키확인증거로 수신부인방지를 획득한다. 수신자는 암호문발신증거와 TTP의 키확인증거로써 발신부인방지를 획득한다[6, 7].

제안한 방식은 TTP 기능을 최소화하는 방법으로 online TTP로 분류된다. TTP의 통신부하를 줄이고

부인방지정보를 관리하는 책임을 개선하였다. 그러나 세션키와 암호문이 외부에 노출될 수 있으므로 기밀성이 보장되지 않는 문제가 있다.

### 2.3 Zhou, Deng and Bao Protocol

제안하는 TTP는 문제가 발생하지 않으면 쌍방의 통신에 대하여 관여하지 않는다. 통신정보의 오류, 악의적인 참여자, 통신장애와 같은 문제가 발생하면, 발신자 또는 수신자는 TTP에게 프로토콜의 중지나 종료를 요청할 수 있다[8].

TTP의 참여가 최소화되었기 때문에 offline TTP로 분류된다.

### 2.4 Markowitch and Kremer Protocol

Zhou, Deng and Bao 프로토콜은 문제가 발생하지 않을 경우, 발신자와 수신자만의 통신으로 부하를 최소화하고 문제발생시 TTP가 관여한다. TTP가 관여하지 않은 경우와 TTP가 관여한 경우의 증거가 다르기 때문에 TTP의 관여여부를 파악할 수 있는 문제가 있었다[9]. Markowitch and Kremer Protocol은 TTP가 관여와 상관없이 부인방지증거가 동일하기 때문에 transparent TTP로 분류되며 인터넷기반의 전자상거래에서 좋은 방안으로 제안되었다.

## Ⅲ. 전자 명 기록기의 설계

국내에서 공인인증이 도입된 시스템은 서버에서 일방적으로 전자서명 로그를 확보하고 있다. 따라서 수신자에게 편향된 불공정한 부인방지 프로토콜이 적용되었다는 문제점 있다. 부인방지서비스를 제공해야하는 인터넷뱅킹, 증권거래시스템, 전자의무기록, 전자상거래 등과 같이 다수의 프로그램이 클라이언트-서버 환경이라는 특징이 있다. 그러나 기존의 제안된 TTP 기반의 부인방지 프로토콜은 E-mail, 전자지불시스템과 같이 통신중간에 구조적으로 특정서버를 경유해야 하는 경우에 적합하게 제안되었다. 따라서 클라이언트-서버 프로그램에는 통신부하로 인하여 적용하기 어렵다.

제안하는 전자서명 기록기는 다수의 사용자를 검증하는 서버와 물리적으로 동일 선상에 적용함으로써 통신부하를 최소하 시키고자 한다. 또한 제안하는 프로토콜은 클라이언트-서버의 쌍방에 대하여 공정한 부인방지 서비스를 제공한다.

### 3.1 구성 요소

본 논문에서 제안하는 공정한 부인방지 프로토콜의 구성요소는 다음과 같다.

1) 발신자

클라이언트 관점이며, 온라인 서비스를 제공받는 사용자로써 거래정보에 대하여 전자서명을 수행한다.

2) 수신자

서버 관점이며, 온라인 서비스 제공자로써 다수의 사용자가 전송한 전자서명을 검증해야 하는 책임이 있다.

3) 전자서명 기록기

서버와 물리적으로 동일선상에 적용되어 통신부하를 최소하며 논리적인 부인방지 프로토콜을 제공하여 강한 공정성을 제공한다.

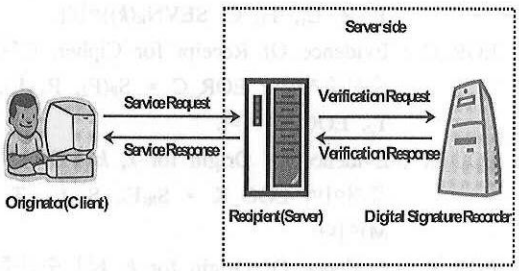



그림 5. 제안하는 전자서명 기록기의 구성요소

그림 1은 제안하는 전자서명 기록의 구성요소를 도식화하였다. 발신자가 온라인서비스를 제공하는 수신자에게 서비스 요청을 한다. 이때 발신자는 거래내용에 대해 전자서명을 수행하며 수신자는 전자서명에 대한 검증을 전자서명 기록기를 통해 확인을 받는다. 검증기록기는 해당 거래에 대한 데이터를 보관하며 발신자 또는 수신자가 요청할 경우에 응답할 수 있도록 설계되었다.

### 3.2 용어 정의

제안하는 공정한 부인방지 프로토콜에서 인용하는 용어는 다음과 같이 정의한다.

- U : User, 클라이언트로써 사용자
- P : Provider, 서버로써 서비스 제공자
- R : Digital Signature Recorder, 전자서명 기록기

- M : 발신자가 수신자에게 전송하는 메시지
- $k$ : 메시지 M에 대한 암호화에 사용되는 세션키
- C : C = $E_k$(M) 메시지 M을 세션키 $k$로 암호화한 암호문
- F : 메시지의 목적을 구분하는 플래그
- L : 프로토콜의 식별자
- T : 서명이 수행되는 시간
- $Ek()$ : 세션키 $k$로 대칭키 암호화 함수
- $Dk()$ : 세션키 $k$로 대칭키 복호화 함수
- $SEVN_X()$ : X의 공개키로 비대칭키 암호화 함수
- $SDVN_X()$ : X의 개인키로 비대칭키 복호화 함수
- $S_X()$ : X의 개인키로 전자서명 함수
- $V_X()$ : X의 공개키로 검증 함수

제안하는 프로토콜의 수행될 때 다음과 같은 증거가 생성된다.

- EOO_C : Evidence Of Origin for Cipher, 암호문의 발신증거이며 EOO_C = $S_U(F_1, P, R, L_1, T_1, C, SEVN_R(k))$이다.
- EOR_C : Evidence Of Receipt for Cipher, C의 수신증거이며 EOR_C = $S_P(F_2, R, L_2, T_2, EOO_C)$이다.
- EOO_K : Evidence Of Origin for $k$, $k$의 발신의 증거이며 EOO_K = $S_R(F_3, S, L_2, T_3, M)$이다.
- EOR_K : Evidence Of Origin for $k$, $k$의 수신증거이며 EOR_K = $S_R(F_4, U, L_1, T_3)$이다.
- $REQ_X$ : X의 개인키로 전자서명한 요청
- $RES_X$ : X의 개인키로 전자서명한 응답
- NRO : Non-Repudiation of Origin, 발신부인방지 증거이며 EOO_C와 EOO_K를 확보해야 한다.
- NRR : Non-Repudiation of Receipt, 수신부인방지증거이며 EOR_C와 EOR_K를 확보해야 한다

### 3.3 제안하는 공정한 부인방지 프로토콜

제안하는 부인방지 프로토콜은 주 프로토콜과 복구 프로토콜로 구성되어 있다 사용자와 서비스제공자 간의 문제가 발생하지 않는 경우는 주 프로토콜에 따라 수행이 되며, 문제 발생시에는 사용자가 전자서명 기록기에 복구 프로토콜을 요청하게 된다.

*Main Protocol*

1) $U \rightarrow P$ : $F_1, P, R, L_1, T_1, C, SEVN_R(k)$, EOO_C

2) $P \rightarrow R$ $F_2, R, L_2, T_2, \{ F_1, S, R, L_1, T_1, C, SEVN_R(k), EOO\_C \}$, EOR_C

3) $R \rightarrow P$ : $F_3, S, L_2, T_3, M, \{ F_4, U, L_1, T_3, EOR\_K \}$, EOO_K

4) $P \rightarrow U$ : $F_5, C, L_1, T_4, \{ F_4, U, L_1, T_3, EOR\_K \}, RES_P$

그림 2 주 프로토콜

그림 2는 주 프로토콜을 표시한 것으로 다음과 같은 순서로 수행된다.

1) 사용자 U는 서비스제공자 P에게 암호발신증거를 전송하며, 암호문 C와 함께 세션키 $k$를 기록기 R의 공개키로 서명한 보안봉투 $SEVN_R(k)$를 전송한다.
2) 서비스제공자 P는 암호문 C를 전달받았으나 세션키 $k$는 기록기 R만이 복호할 수 있으므로 메시지 M를 확인할 수 없다. P는 R에게 암호수신증거를 전송한다.
3) 기록기 R은 전송된 암호발신증거와 암호수신증거에 대하여 검증을 하여 유효할 경우, R의 개인키로 세션키 $k$를 복호화한다. 세션키 $k$로 메시지 M을 복구해서 서비스제공자 P에게 결과를 전송한다. 이때 기록기는 키수신증거, 키발신증거를 함께 전송하고 유효한 모든 증거를 보관해야 한다.
4) 서비스제공자 P는 기록기 R로부터 전송받은 키수신증거를 사용자 U에게 전송한다.

4단계의 절차가 완료되면, 발신자는 암호수신증거(EOR_C)와 키수신증거(EOR_K)를 확보하여 수신부인방지증거(NRR)를 확보한다. 수신자는 암호발신증거(EOO_C)와 키발신증거(EOO_K)를 확보하여 발신부인방지증거(NRO)를 확보함으로 공정을 보장한다.

그림 3은 복구 프로토콜을 나타내었다. 만약, 발신자가 제한시간 내에 NRO을 전송하지 않으면 전자서명 기록기에 요청한다

*Recoverz Protocol*

5) $U \rightarrow P : F_6, P, R, L_1, T_5, \{ F_1, S, R, L_1, T_1, C, SEVN_R(k), EOO\_C \}, REQ_U$

6) $R \rightarrow P . F_7, U, L_1, T_6, \{ F_4, U, L_1, T_3, EOR\_K \}, RES_R$

그림 3. 복구 프로토콜

5) 사용자 U는 제한시간에 서비스제공자 P로부터 응답이 없는 경우, 기록기 R에게 암호발신증거와 함께 결과를 요청한다.
6) 기록기 R은 3)번 단계에서 보관한 정보와 요청한 정보를 확인한 후 그 결과를 응답한다.

## Ⅳ. 프로토콜의 비교분석

### 4.1 부인방지 프로토콜의 필수 요구사항

1) 공정성

부인방지 프로토콜은 수행되는 단계마다 어느 한편의 잇점이 없으면서, 프로토콜이 완료되어 발신자와 수신자가 반박할 수 없는 증거를 확보하도록 해야 한다.

2) 시간제한

어느 한편이 정확 프로토콜을 준수하면, 정해진 시간 후에는 프로토콜이 완료되어야 한다. 따라서 참여자가 무한 대기하는 상태가 없어야 한다.

3) 보안성

참여자가 프로토콜을 준수했을 때 해당정보에 대하여 외부의 노출이 되지 않도록 보안 기능이 제공되어야 한다.

4) TTP 관여도

TTP가 발신자와 수신자간의 통신에 어느정도 관여하는지에 따라서 부인방지 프로토콜의 효율성을 나타낸다. 공정성과 보안성을 보장하면서 TTP의 관여가 적을수록 우수하다.

5) 통신부하

통신부하는 발신자, 수신자, TTP간의 전체통신의 측정결과로써, TTP 관여도를 최소화시키거나 프로토콜 내에서 통신의 횟수를 감소시킴으로써 통신부하를 줄일 수 있다.

### 4.2 비교분석

기존의 부인방지 프로토콜과 본 논문의 전자서명 기록기(Digital Signature Recorder : DSR)와 공정성, 시간제한, 보안성, TTP관여도, 통신부하의 5가지 요구사항에 대하여 비교한다.

공정성이 편향적인 경우는 weak, 강한 공정성인 경우는 strong, TTP의 관여여부를 인지할 수 없을 경우는 true로 분류된다. 기존의 Coffey-Saidha, Zhou-Gallmann는 프로토콜이 수행될 때 TTP를 반드시 거쳐야 하기 때문에 강한 공정성을 제공하므로 strong으로 분류된다. Zhou-Deng-Bao는 정상모드에는 TTP가 관여하지 않으며 장애모드에만 관여하여 공정성을 보장함으로 strong으로 분류된다. Markowitch-Kremer는 일반모드와 장애 발생시 TTP가 복구를 한 경우에 TTP의 관여여부를 파악할 수 없기 때문에 true로 분류된다. 제안한 DSR은 일반모드와 장애모드의 경우 동일한 부인방지증거인 EOO_K와 EOR_K를 제공하기 때문에 제3자는 TTP의 관여를 판단할 수 없도록 설계되었다. 따라서 DSR은 true로 분류된다.

시간제한은 Coffey-Saidha은 시간의 설정이 없기 때문에 참여자가 무한 대기할 수 있는 가능성이 있다. Zhou-Gallmann, Zhou-Deng-Bao, Markowitch-Kremer는 시간토콘을 사용하여 시간제한이 가능하다 제안한 DSR의 경우도 시간토콘을 적용하여 시간제한을 제공하도록 설계되었다.

보안성은 제3자의 열람과 프로토콜의 종료전 수신자의 열람이 불가능하도록 제공되어야 한다. Coffey-Saidha, Zhou-Deng-Bao, Markowitch-Kremer는 TTP의 공개키를 이용한 보안봉투를 적용하여 보안성을 보장한다. 그러나 Zhou-Gallmann의 전자서명만을 검증하기 때문에 제3자의 열람이 가능하다. 따라서 보안성이 제공되지 않는다. 제안한 DSR은 기록기의 공개키를 이용한 보안봉투를 적용했기 때문에 보안성을 보장한다.

TTP관여도는 최소화할수록 효율성이 증대된다. Coffey-Saidha은 모든 통신에 TTP가 관여함으로 inline으로 분류된다. Zhou-Gallmann은 암호문과 세션키로 전송으로 분류하여 세션키에 대한 부분만 TTP가 관여하기 때문에 online으로 분류된다. Zhou-Deng-Bao, Markowitch-Kremer는 일반모드에는 TTP가 관여하지 않으면 장애모드에만 TTP가

복구를 위해 관여한다. 따라서 관여도가 최적화되어 offline으로 분류된다. 제안하는 DSR은 TTP의 관여를 배제하기 위해 서비스제공자와 동일선상에 구축하도록 하였다. 따라서 TTP의 관여도가 전혀없기 때문에 none으로 분류된다.

통신부하는 최소화될수록 우수한 프로토콜로 입증된다. Coffey-Saidha은 모든 통신에 TTP가 관여함으로써 통신부하는 high로 분류된다. Zhou-Gallmann은 세션키의 복호화를 위해 TTP를 경유하도록 감소시켰으나 프로토콜 종료전에 반드시 거쳐야 함으로 통신부하는 high로 분류된다. Zhou-Deng-Bao, Markowitch-Kremer는 정상모드에는 TTP가 관여가 없고 장애모드에만 관여하기 때문에 middle로 분류되었다. 제안하는 DSR는 TTP와 통신이 없으며, 프로토콜의 설계에서 전체통신 횟수를 최적화시킴으로써 부하를 감소시켰다. 따라서 low를 분류된다.

표 1은 제안하는 DSR과 기존의 프로토콜과 비교내용을 정리하였다.

표 1. 부인방지 프로토콜의 비교분석

| 프로토콜 | 공정성 | 시간제한 | 보안성 | TTP 관여도 | 통신부하 |
|---|---|---|---|---|---|
| Coffey-Saidha | s | n | y | inline | h |
| Zhou-Gollmann | s | y | n | online | h |
| Zhou-Deng-Bao | s | y | y | offline | m |
| Markowitch-Kremer | t | y | y | offline | m |
| DSR | t | y | y | none | l |

* 공정성 : w=weak, s=strong, t=true
* 시간제한 : n=not, y=yes
* 보안 : n=not, y=yes
* TTP관여 : inline>online>offline>none
* 통신부하 : h=high, m=middle, l=low

## V. 결 론

공인인증이 적용한 온라인서비스는 부인방지를 위해 일방적으로 전자서명 로그를 확보하고 있다. 따라서 발신자는 수신자의 부인을 방지하기 위해 어떠한 증거도 확보하지 못하는 편향된 부인방지 프로토콜이라는 문제점 있다.

기존의 제안된 TTP 기반의 부인방지 프로토콜은 E-mail, 전자지불시스템과 같이 통신간에 구조적으로 특정서버를 경유해야 하는 P2P에 적합하도록 제안되었다. 그러나 인터넷뱅킹, 증권거래시스템, 전자의무기록, 전자상거래 등의 프로그램은 클라이언트-서버 환경이라는 특징이 있다. 따라서 클라이언트-서버 프로그램에는 통신부하로 인하여 기존의 프로토콜이 적용되기 어렵다.

제안하는 전자서명 기록기는 다수의 사용자를 검증하는 서버와 물리적으로 동일 선상에 적용함으로써 통신부하를 최소화시켰다 또한 프로토콜의 설계에서 전체통신 횟수를 최적화시킴으로써 부하를 감소시켰다. 기존의 서비스제공자가 보관해야 하는 부인방지증거를 전자서명 기록기가 담당함으로써 정보관리의 부담을 감소시켰다. 공정성, 시간제한, 보안성의 필수 요구조건에 대해서도 기존의 프로토콜과 동일수준을 보장하고 있다.

향후 연구로써는 제안한 프로토콜의 관리차원에 대한 보안성을 검토해야 하며 부인방지증거의 저장과 관리에 대하여 연구가 요구된다.

## 참 고 문 헌


[1] O. Markowitch and Y. Roggeman, "Probabilistic non-repudiation without trusted third party," Second Conference on Security in Communication Networks (SCN99), September 1999

[2] O. Markowitch, D. Gollmann, and S. Kremer. "On Fairness in Exchange Protocols," Lecture Notes in Computer Science 2587, Proceedings of 5th International Conference on Information Security and Cryptology, pp. 451-464, November 2002.

[3] O. Markowitch and S. Kremer. "An Optimistic Non-repudiation Protocol with Transparent Trusted Third Party," Lecture Notes in Computer Science 2200, Proceedings of 2001 International Conference on Information Security, pp.363--378, October 2001.

[4] J. Zhou and D. Gollmann. "Observations on Non-repudiation," Lecture Notes in Computer Science 1163, Advances in Cryptology· Proceedings of Asiacrypt'96,

pp.133-144, November 1996.

[5] T. Coffey and P. Saidha, "Non-repudiation with Mandatory Proof of Receipt," Computer Communication Review, vol.26, no.1, pp.6-17, January 1996.

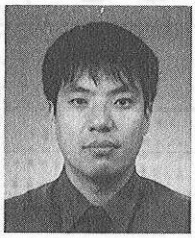
[6] J. Zhou and D. Gollmann. "A Fair Non-repudiation Protocol," Proceedings of 1996 IEEE Symposium on Security and Privacy, pp.55--61, May 1996.

[7] J. Zhou and D. Gollmann, "An Efficient Non-repudiation Protocol," Proceedings of 10th IEEE Computer Security Foundations Workshop, IEEE Computer Society Press, Silver Spring, MD, pp.126--132, June 1997.

[8] J. Zhou, R. Deng and F. Bao, "Evolution of Fair Non-repudiation with TTP," Lecture Notes in Computer Science 1587, Proceedings of Australasian Conference on Information Security and Privacy, pp.258--269, 1999.

[9] S. Kremer, O. Markowitch, and J. Zhou, "An Intensive Survey of Fair Non-repudiation Protocols," Computer Communications, vol.25, no.17, pp.1606-1621, November 2002.

이 용 준(Yong-jun Lee) 정회원



1999년 : 강남대학교 전자계산학과 졸업
2001년 : 숭실대학교 컴퓨터학과 석사
2004년 : 숭실대학교 컴퓨터학과 박사수료

<관심분야> 정보보호, 암호학, PKI

오 해 석(Hae-Seok Oh) 정회원

1975년 서울대학교 응용수학과 학사
1981년 서울대학교 계산통계학과 석사
1989년 : 서울대학교 계산통계학과 박사
1976년 " 1982년 : 태평양화학(주), (주)삼호 전산실
1982년 " 2003년 : 숭실대학교 정보과학대학 교수
1990년 " 1991년 : 일본 동경대학교 객원교수
1997년 " 1999년 : 숭실대학교 부총장
2000년 " 2001년 : 스탠포드대학교 객원교수
2003년 " 현재 : 경원대학교 소프트웨어대학 교수

<관심분야> 멀티미디어, 데이터 이스, 정보보호