通信情報保護學會論文誌
第 7 卷 第 3 號. 1997. 9

Zhou-Gollmann 부인봉쇄 프로토콜 분석 및 개선

박 상 준*, 김 광 조*, 원 동 호**

Analysis and Enhancement of Zhou-Gollmann's Non-repudiation Protocol

Sangjoon Park, Kwangjo Kim, Dong Ho Won

요 약

본 논문에서는 Zhou-Gollmann 부인봉쇄 프로토콜의 두가지 문제점에 대하여 다루었다. Zhou-Gollmann 프로토콜에서 메시지는 암호문과 키로 나뉘어 지며 암호문은 수신자에게 직접 전달되지만 키는 수신자로 부터 영수증을 받은 후에 *TTP*의 공개 디렉토리에 게시된다. 따라서, 키를 *TTP*에 등록하느냐 하지 않는냐는 전적으로 발신자의 의지에 좌우된다. 본 논문에서는 발신자가 이러한 자신의 역할을 이용하여 프로토콜을 불공정하게 만들수 있음을 보이고 개선 방법을 제시하였다. Zhou-Gollmann 프로토콜의 두번째 문제점은 수신자에게 전달된 암호문은 *TTP*에 게시된 키에 의하여 누구라도 쉽게 복호화하여 평문 메시지를 얻을 수 있다는 것이다. 따라서, 발신자가 비밀 메시지를 수신자에게 보내기 위해서는 부가적인 암호 방법을 사용하여야 한다. 본 논문에서는 Zhou-Gollmann 프로토콜에 Diffie-Hellman 키분배 방식을 사용하여 메시지 보호가 가능한 부인봉쇄 프로토콜을 제안하고자 한다.

Abstract

In this paper, we analyze two claws of Zhou-Gollmann's protocol. The protocol divide the message into a key K and a ciphertext C. The ciphertext C is delivered to the recipient, but the key K is submitted to the TTP, after the message originator receive the recipient's receipt for the ciphertext. TTP puts the key in the directory which is accessible to the public. So, the recipient's obtaining the message dependson whether the originator submits the key or not. We will show that the originator, which is in such an advantageous position, could make the protocol be unfair and present how to improve the protocol. On the other hand, Zhou-Gollmann's protocol doesn't provide the secrecy of the

* 한국전자통신연구원
* * 성균관대학교 정보공학과

message, since the key K is published. This means that, to send a secret message, additional mechanism is required. In this paper, we will present an improvement of Zhou-Gollmann's protocol to keep the message secret. The key distribution of the proposed protocol is based on the Diffie-Hellman's one.

1. 서 론

통신 단말기 보급과 전산망의 발전으로 기존의 종이로 작성된 각종 서류들이 전자 문서 형태로 보관되고 유통된다. 인터넷의 발전은 전자 정보의 단순 유통 뿐 아니라 구매자와 생산자를 연결시켜 전산망을 통한 상거래도 가능하게 하였다. 기존의 종이로 만들어진 계약서, 견적서, 구매 입찰, 상품 구매, 화물 송장 등과 같은 서류들은 전자 문서화할 경우 부인봉쇄와 같은 새로운 암호 응용 서비스가 요구된다.[9] 그러나, 부인봉쇄 프로토콜에서 발신자와 수신자 어느 한쪽이 유리한 위치에 놓이지 않고 발신자와 수신자 모두에게 공정한 서비스를 제공한다는 것은 매우 어려운 일이다. 1996년 Zhou와 Gollmann은 *TTP*(Trusted Third Party)를 이용하지만 전체 프로토콜에서 *TTP*의 역할을 최소화하는 방법으로 매우 효과적인 공정한 부인 봉쇄 프로토콜을 제안하였다.[12] 공정한 부인봉쇄 프로토콜이란 프로토콜 수행중 어느 한쪽이 우월적인 위치에 이르지 못하며 프로토콜 종료후에는 발신자와 수신자 모두가 상대방이 거부할 수 없는 명백한 증거를 갖게 되는 것을 의미한다. 일반적으로 *TTP*를 이용하는 부인봉쇄 서비스에서는 발신자와 수신자가 *TTP*를 통하여 정보를 주고 받으며 각 단계에서 *TTP*가 발신자(또는 수신자)에게 확인증을 발행하기 때문에 전체 프로토콜에서 *TTP*가 차지하는 비중이 매우 높아지는 문제점을 갖는다. 그러나 Zhou-Gollmann의 프로토콜에서는 *TTP*를 이용하면서도 *TTP*의 역할을 상대적으로 줄여 *TTP* 의존도를 줄였다.

Zhou-Gollmann 프로토콜에서 메시지는 암호문(C)과 키(K)로 나누어 지며 암호문은 수신자에게 직접 전달되지만 키는 수신자가 암호문 수신에 대한 영수증(*NRR*)을 발신자에게 주고 난 이후에 *TTP*의 공개 디렉토리에 게시된다. 이때 *TTP*는 발신자가 제출한 키와 함께 자신의 서명(키 제출 확인증: *con_K*)을 부가하여 공개한다. 따라서, 발신자가 수신자로 부터 받은 영수증(*NRR*)은 *con_K*와 짝을 이루어야만 유효하며 발신자가 *con_K*를 얻을 수 있다면 수신자 또한 *con_K*로 부터 키 K를 얻을 수 있다. 그러나, *con_K*가 공개 디렉토리에 게시되는 것은 발신자가 키 K를 *TTP*에게 제출해야 하므로 전적으로 발신자에게 의존한다. 발신자는 *NRR*을 언제든지 유효화시킬 수 있으며 수신자는 발신자가 키 K를 *TTP*에게 제출할 때 까지 기다려야만 한다. 본 논문에서는 발신자가 이러한 자신의 우월적인 지위를 이용하여 프로토콜을 불공정하게 만들수 있음을 보이고자 한다. Zhou-Gollmann 프로토콜의 두번째 문제점은 수신자에게 전달된 암호문이 *TTP*에 게시된 키에 의하여 누구라도 메시지 내용을 알 수 있다는 것이다. 그러나, 일반적으로 부인봉쇄 서비스가 요구되는 정보들은 메시지의 비밀이 요구될 가능성이 클 것이다. 따라서, 발신자와 수신자는 메시지의 비밀을 유지하기 위하여 부가적인 암호 방법을 사용하여야 한다. 본 논문에서는 Zhou-Gollmann 프로토콜에 Diffie-Hellman 키분배 방식을 사용할 경우 메시지 보호가 가능한 부인봉쇄 프로토콜을 만들 수 있음을 보였다.

본 논문은 모두 6개 절로 구성된다. 2절에서

는 공정한 부인봉쇄 프로토콜을 기술하였으며, 3절에서는 Zhou-Gollmann 프로토콜을 소개하였다. 4절에서는 Zhou-Gollmann 프로토콜의 불공정성을 지적하고 개선 방법을 제안하였으며, 5절에서는 Diffie-Hellman 키분 방식을 이용하여 Zhou-Gollmann 프로토콜에 메시지 보호 기능을 추가하는 방안을 제안하였다. 마지막으로, 6절은 결론부이다.

2. Zhou-Gollmann의 공정한 부인봉쇄 프로토콜

초기의 부인 봉쇄 프로토콜에서는 메시지 발신자와 수신자가 정해진 프로토콜을 수행한 이후에 양쪽이 갖게 되는 증거에 초점을 맞추고 있다. 그러나, 프로토콜이 중간에서 중단되어도 어느 한쪽이 다른쪽 보다 유리한 위치에 서지 않도록 하는 것은 전체 프로토콜의 안전성에서 매우 중요하다. 예를들어, 어떤 자료를 발송하는 발신자는 문서 발송과 함께 수신자로 부터 문서를 수신하였다는 영수증을 받고 싶어할 것이나 문서 수신자는 문서를 받기 이전에는 영수증을 제공하려 하지 않을 것이다. 발신자가 문서 수신자의 정직성만을 믿고 수신자에게 문서를 발송하였으나 수신자가 문서를 수신하였다는 영수증을 발신자에게 보내지 않을 수 있다. 이 경우, 문서 수신자는 자신이 문서를 받았다는 사실을 부인할 수 있으며 발신자는 자신이 문서를 발신했음에도 불구하고 문서를 발신했다는 사실을 입증할 방법이 없다. 따라서, 부인봉쇄 프로토콜은 각 단계에서 발신자와 수신자 모두에게 공정한 서비스를 제공하여야만 한다.

그러나, 발신자와 수신자에게 모두 공정한 서비스를 제공하기 위해서는 정보의 동시 교환이 실현되어야 한다. 즉, 발신자가 메시지를 수신자에게 메시지를 발신하는 과정과 수신자가 메시지를 받았다는 영수증이 동시에 교환되어야 한다. 메시지의 동시 교환은 매우 복잡한 암호 프로토콜을 요구하기 때문에 현실적으로 실현이 용이하지 않다.[1][2][4][5][7][10] 또 다른 방법으로는 신뢰할 수 있는 제3의 기관(*TTP*)을 이용하는 방안을 생각할 수 있다. *TTP*를 이용하는 방안은 현실적인 접근 방법이라고 생각되나 프로토콜의 각 단계에서 *TTP*에 의존하여야 하므로 *TTP* 의존도가 상대적으로 높은 문제점이 있다.

Zhou와 Gollmann은 *TTP*를 이용하는 공정한 부인 봉쇄 프로토콜을 제안하였다.[12] Zhou-Gollmann의 프로토콜은 *TTP*를 이용하지만 *TTP*는 단지 프로토콜의 마지막 단계에서 발신자가 제출한 키 정보와 연결 꼬리표(link label)에 대한 *TTP*의 서명을 자신의 공개 디렉토리에 공개하는 역할만 수행한다.

다음은 Zhou-Gollmann 프로토콜에서 사용되는 주요 표기이다.

- $X||Y$: X와 Y가 연접되었음을 의미
- $H(\cdot)$: 일방향 해쉬 함수
- $E(X, K, e)$: 메시지 X를 키 K에 의하여 암호화 ($E(\cdot)$는 관용키 알고리즘을 의미)
- $E(X, K, d)$: 메시지 X를 키 K에 의하여 복호화
- s_A : 사용자 A의 서명용 비밀키
- p_A : 사용자 A의 서명 검증용 공개키
- $S(X, s_A)$: 사용자 A의 서명용 비밀키 s_A에 의한 X의 서명

2.1 Zhou-Gollmann 프로토콜

Zhou-Gollmann 프로토콜에서는 메시지를 메시지 암호 키 K와 암호문 C로 나누어 처리한다. 암호문 C는 발신자 A와 수신자 B 사이에 먼저 교환되고 키는 *TTP*에게 제출한다. 이

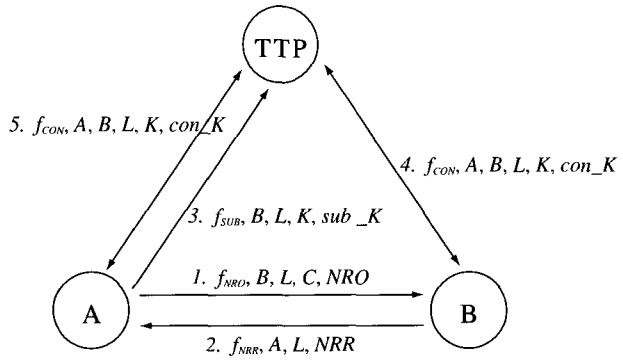


그림 1 : Zhou-Gollmann의 공정한 부인봉쇄 프로토콜

때 A와 B는 분쟁시를 대비하여 TTP로 부터 부인 봉쇄에 사용할 증거로 키 K의 등록 확인증(con_K)을 받아야 한다. TTP는 키 K에 대한 확인증을 공개 디렉토리에 공개하며 A와 B는 공개 디렉토리에서 TTP의 확인증을 받아온다. 또한, 발신자 A는 수신자에게 전송하는 암호문 C와 TTP에게 제출하는 키 K를 연결 꼬리표에 의하여 상호 연결시킨다.

다음은 Zhou-Gollmann 프로토콜을 기술하기 위하여 사용된 표기이다.

- A : 메시지 발신자
- B : 메시지 수신자
- TTP : 네트워크 서비스를 제공하는 온-라인 Trusted Third Party
- M : A로 부터 B로 보내지는 메시지
- C : 키 K에 의한 메시지 M의 암호문 ($C=E(M, K, e)$)
- K : A에 의하여 정의된 메시지 키
- L : 각 메세지에 유일하게 부여되며 키와 암호문을 연결하는 연결 꼬리표
- f_{NRO} : 발신자 부인봉쇄를 나타내는 플래그 정보
- f_{NRR} : 수신자 부인봉쇄를 나타내는 플래그 정보
- f_{SUB} : 키 K의 등록을 나타내는 플래그 정보
- f_{CON} : TTP가 발행하는 등록 확인증을 나타내는 플래그 정보
- $NRO=S(f_{NRO}||B||L||C, s_A)$: 발신자 부인봉쇄 정보 (Non-repudation of Origin)
- $NRR=S(f_{NRR}||A||L||C, s_B)$: 수신자 부인봉쇄 정보 (Non-repudiation of Receipt)
- $sub\_K=S(f_{SUB}||B||L||K, s_A)$: A에 의한 키 K의 등록 (submit)
- $con\_K=S(f_{CON}||A||B||L||K, s_T)$: TTP에 의한 키 등록 확인증

A, B, TTP는 그 자신만의 서명용 비밀키 s_A, s_B, s_T을 갖고 있으며 검증을 위한 공개키 p_A, p_B, p_T도 있다. 프로토콜 각 단계별 처리 과정은 다음과 같다.

(1) A는 메시지 M을 위한 연결 꼬리표 L과 키 K를 결정한 다음, 키 K에 의하여 메시지 M의 암호문 C를 만든다. 연결 꼬리표 L은 각 메시지에 유일하게 할당된다. A는 f_{NRO}, B, L, C, NRO를 B에게 전송한다. 이 때, 이러한 정보가 B에 도달하지 못한다면 프로토콜은 분쟁없이 끝난다.

(2) B는 NRO가 f_{NRO}, B, L, C에 대한 A의 서명임을 A의 공개 검증키 p_A로 검증하여 A의 서명이 아니라고 판정되면 프로토콜을 중지한다. B는 A에게 f_{NRR}, A, L, NRR을 전송한다. 만일 B가 NRR을 A에게 보내지 않는다면 프로토콜은 분쟁없이 끝난다. 왜냐하면 B는 키 K없이 C로 부터 메시지 M을 복원할 수 없기 때문이다. 암호문 C를 복호화하고 메시지 M의 발신자가 A임을 증명하기 위해서는 TTP로 부터 키 K와 con_K를 받아야 한다. 그러나 B가 TTP로 부터 K와 con_K을 받기 위해서는 B는 A에게 NRR을 보내야만 한다.

(3) B로 부터 NRR을 받은 후 A는 NRR에 포함된 연결 꼬리표 L이 자신이 B에게 보낸 연결 꼬리표 L과 같은지 비교하여 일치하지 않으면 프로토콜을 중지한다. A는 TTP에게 f_{SUB}, B, L, K, sub_K를 전송한다. 만일 A가 sub_K와 K를 TTP에게 보내지 않으면 프로토콜은 분쟁없이 끝난다. 메시지 M을 수신자가 받았다고 주장하기 위해서는 TTP로 부터 con_K를 받아야 하며, TTP로 부터 con_K를 받기 위해서는 TTP에게 sub_K를 보내야 한다. sub_K와 K를 받은 후에 TTP는 con_K를 생성하여 공개적으로 접근 가능한(read only) 공개 디렉토리에 (f_{CON}, A, B, L, K, con_K)를 공개한다.

(4) B는 TTP의 공개 디렉토리에서 f_{CON}, A, B, L, K, con_K를 받은 후 TTP의 공개 검증키 p_T에 의하여 con_K가 TTP의 서명임을 확인한다. 또한, B는 K를 이용하여 암호문 C를 복호화하여 평문 M을 얻는다.

(5) A는 B와 마찬가지로 TTP의 공개 디렉토리로 부터 f_{CON}, A, B, L, K, con_K를 받은 후 TTP의 공개 검증키 p_T에 의하여 con_K가 TTP의 서명임을 확인한다. 단계 (4)와 (5)의 순서는 바뀔 수 있다.

본 부인봉쇄 프로토콜에서는 TTP가 프로토콜을 중개하는 역할을 수행하지 않으며 대신 발신자 A가 제출한 키 K에 대한 등록 확인서를 공개 디렉토리에 게시하는 역할을 수행한다. 이렇게 함으로서 두가지 장점을 얻을 수 있다. TTP는 전체 메시지 크기에 비하여 상대적으로 적은 키만을 다루면 된다. 또한 TTP가 중개자(Delivery Agency) 역할을 수행해야 하는 경우에는 수신자가 그 메시지를 받았다는 확인을 받을 때 까지 메시지를 계속 보유하고 있어야 하나 본 프로토콜에서는 공개 디렉토리로 부터 등록 확인증을 가지고 가야할 책임이 발신자와 수신자에게 있다.

2.2 분쟁의 해결

분쟁은 메시지 M의 발신 및 수신에서 발생한다. 첫번째 경우는 발신자 A가 메시지 M을 B에게 보내지 않았다고 주장할 경우에 발생하며, 두번째 경우는 수신자 B가 메시지 M을 받지 않았다고 주장할 경우에 발생한다.

발신 부인봉쇄

A가 메시지 M을 보내지 않았다고 주장할 경우 B는 판사에게 M, C, K, L과 증거물로서 NRO, con_K를 제출한다. 판사는 다음과 같은 과정을 통하여 메시지 M을 A가 보냈음을 확인할 수 있다.

- con_K가 $f_{CON}||A||B||L||K$에 대한 TTP의 서명임을 확인한다.
- NRO가 $f_{NRO}||B||L||C$에 대한 A의 서명임을 확인한다.
- $M=E(C, K, d)$임을 확인한다.

수신 부인 봉쇄

B가 M을 수령했다는 사실을 부인한다면 A는 판사에게 M, C, K, L과 증거물 NRR, con_K를 제출한다. 판사는 다음과 같은 과정을 통하여 메시지 M을 B가 받았음을 확인할 수 있다.

- con_K가 $f_{CON}||A||B||L||K$에 대한 TTP의 서명임을 확인한다.
- NRR이 $f_{CON}||A||L||C$에 대한 B의 서명임을 확인한다.
- $M=E(C, K, d)$를 확인한다.

2.3 게시 기간

현실적으로 TTP는 메시지 키를 영원히 저장할 수 없다. 그러므로, K, con_K를 TTP의 공개 디렉토리에 게시하는 기간을 정한다. 게시 기간 T는 TTP의 시간을 참조하여 발신자 A가 결정하며 게시 기간은 NRO, NRR, sub_K, con_K내에 포함된다. 또한, 선택적으로 con_K내에는 time stamp T_0가 찍힐 수 있다. 이경우 프로토콜은 다음과 같다.

$$
\begin{aligned}
NRO &= S(f_{NRO}||B||L||T||C, s_A)\\
NRR &= S(f_{NRR}||A||L||T||C, s_B)\\
sub\_K &= S(f_{SUB}||B||L||T||K, s_A)\\
con\_K &= S(f_{CON}||A||B||L||T||T_0||K, s_T)
\end{aligned}
$$

1. $A \rightarrow B$: f_{NRO}, B, L, T, C, NRO
2. $B \rightarrow A$: f_{NRR}, A, L, NRR
3. $A \rightarrow TTP$: $f_{SUB}, B, L, T, K, sub\_K$
4. $B \leftrightarrow TTP$: $f_{CON}, A, B, L, T_0, K, con\_K$
5. $A \leftrightarrow TTP$: $f_{CON}, A, B, L, T_0, K, con\_K$

만일 B가 게시 기간 T에 동의하지 않는다면 단계 2에서 프로토콜은 정지된다. 만일 sub_K와 K가 TTP에 게시 기간 보다 늦게 도착된다면 TTP는 공개 디렉토리에 con_K를 공개하지 않을 것이므로 프로토콜은 분쟁없이 끝난다. 게시 기간 T가 되면 TTP는 f_{CON}, A, B, L, T, T_0, con_K를 공개 디렉토리에서 삭제한다.

3. Zhou-Gollmann 프로토콜의 불공정성

Zhou-Gollmann 프로토콜에서 A가 수신자 B로 부터 f_{NRR}, A, L, NRR을 받았음에도 불구하고 키 K와 sub_K를 TTP에게 제출하지 않을 경우를 생각하여 보자. 이 경우 물론 A가 가지고 있는 NRR은 TTP로 부터 con_K를 받지 못하였으므로 의미를 갖지 못한다. 그러나, B는 A가 보낸 f_{NRO}, B, L, C, NRO를 계속 보관하여야 한다. 만일 B가 A로 부터 받은 정보를 삭제하고 A가 f_{SUB}, B, L, K, sub_K를 TTP에게 제출하면 TTP는 f_{CON}, A, B, L, K, con_K를 공개 디렉토리에 공개하게 된다. 따라서, A는 메시지 M을 B가 받았다는 확인증(con_K)을 얻게되며 B는 여전히 메시지 M의 내용을 알 수 없게된다. 또한, 발신자가 메시지를 철회하려는 진정한 의사가 있다 하여도 이러한 사실을 B가 TTP에게 증명할 수 없기 때문에 NRO을 버릴 수 없다.

이러한 문제점은 게시 기간 T를 정의하는 방법으로 해결될 수 있다. A와 B는 게시 기간 T에 합의하였으며, A는 키 K를 TTP에게 제출할 때 T를 함께 보내야 한다. 따라서, TTP는 A로 부터 sub_K를 받은 시간 T_0가 T를 넘어설 경우 con_K를 만들어 자신의 공개 디렉토리에 게시하는 것을 거부할 것이다. 만일 A가 B와 합의한 시간 T 대신 $T'(>T)$을 sub_K와 함께 TTP에게 보낸다면TTP는 T'이 포함된 con_K를 게시하게 될 것이나, NRR과 con_K에 포함된 정보 T와 T'이 서로 다르기

때문에 A는 분쟁에서 이길 수 없다. 그러므로, A는 T 시각 이전에 TTP에 키 K를 등록하여야 하며, B는 T 시각까지 NRO을 보관하고 TTP의 공개 디렉토리에 등록되지 않을 경우 삭제할 수 있다.

그러나 게시 시간 T를 사용하는 프로토콜은 새로운 문제를 야기시킬 수 있다. A가 T 시각 바로 직전에 키 K를 보내는 경우를 생각하여 보자. 이 경우 con_K는 게시되는 즉시 공개 디렉토리에서 삭제될 것이다. 따라서, B는 T 시각이 가까워지면 TTP의 공개 디렉토리를 계속적으로 주시하여야 한다. 이때, A는 B가 TTP의 공개 디렉토리로 부터 con_K를 받아올 수 없도록 B가 이용하는 시스템에 장애를 유발시킬 수도 있다. 또한, 시각 T는 원래 TTP가 공개 디렉토리에서 공개되는 게시 기간을 나타내는 시각이므로 B에게는 상대적으로 긴 시간이 될 것이다. 위와 같은 문제는 키 K를 TTP에 등록하는 권한이 전적으로 발신자에게 있기 때문에 발생하며 상대적으로 수신자는 불리한 위치에 놓이게 된다. 따라서, B는 공개 열람 가능한 게시 기간 T 이외에 자신이 A에게 전송한 서명 NRR의 유효 시간 T_1을 정의할 필요가 있다. 이경우 Zhou-Gollmann 프로토콜은 다음과 같이 변경된다.

$$
\begin{aligned}
NRO &= S(f_{NRO}||B||L||T||C,\ s_A)\\
NRR &= S(f_{NRR}||A||L||T||T_1||C,\ s_B)\\
sub\_K &= S(f_{SUB}||B||L||T||K,\ s_A)\\
con\_K &= S(f_{CON}||A||B||L||T||T_0||K,\ s_T)
\end{aligned}
$$

1. $A \rightarrow B$: f_{NRO}, B, L, T, C, NRO
2. $B \rightarrow A$: f_{NRR}, A, L, T_1, NRR
3. $A \rightarrow TTP$: $f_{SUB}, B, L, T, K, sub\_K$
4. $B \leftrightarrow TTP$: $f_{CON}, A, B, L, T_0, K, con\_K$
5. $A \leftrightarrow TTP$: $f_{CON}, A, B, L, T_0, K, con\_K$

시간 T와 T_1 사이에 충분한 시간을 두면 B는 T_1 시간과 T 시간 사이에 아무때나 TTP의 공개 디렉토리로 부터 con_K를 받아올 수 있을 것이다. 만일 T_1 시간 이후 TTP의 공개 디렉토리에 con_K가 게시되지 않는다면, A가 키 K를 TTP에 등록하지 않은 것이므로 A가 가지고 있는 NRR은 더이상 의미를 갖지 못한다. 따라서, B는 NRO를 보관할 필요 없이 삭제할 수 있다.

위와같은 프로토콜에서 발신 부인봉쇄 과정은 Zhou-Gollmann과 같으나 수신 부인봉쇄 과정은 다음과 같이 변경된다.

수신 부인 봉쇄

A는 판사에게 M, C, K, T, T_0, T_1, L과 증거물 NRR, con_K를 제출한다. 판사는 다음과 같은 과정을 통하여 메시지 M을 B가 받았음을 확인할 수 있다.

(1) con_K가 $f_{CON}||A||B||L||T||T_0||K$에 대한 TTP의 서명임을 확인한다.
(2) NRR이 $f_{CON}||A||L||T||T_1||C$에 대한 B의 서명임을 확인한다.
(3) $T_0<T_1<T$를 만족하는지 확인한다.
(4) $M=E(C, K, d)$를 확인한다.

그러므로, A는 B가 NRR에서 지정한 T_1 시간 이전에 sub_K를 TTP에 등록하여야 한다. 만일 T_1 시간 이후 $T_0(T_1<T_0)$ 시간에 sub_K를 TTP에 보내면 NRR과 con_K에 이러한 증거가 남게된다. 사용자 B는 같은 연결 꼬리표 L로 연결된 NRR에 대응되는 NRO를 T_1 시각까지만 보관하고, 만일 T_1 시간까지 TTP의 공개 디렉토리에 TTP의 확인증 con_K가 등록되지 않으면 자신의 메모리에서 삭제하여도 상관없다.

이러한 방법은 시간 정보에 의존하기 때문에 A, B, TTP가 사용하는 시스템의 시계를 공통된 시간 정보로 유지하는 것이 중요하다. A

와 B는 서로 독립된 시계를 가지고 있기 때문에 두개의 시계를 일치시키는 것은 쉽지않다. 따라서, 보다 신뢰할 수 있는 시간 정보를 얻기 위해서는 신뢰할 수 있는 기관으로부터 시간 정보를 제공 받는 방법을 생각할 수 있다.

4. 메시지 보호

Zhou-Gollmann 프로토콜에서는 암호문 C에 대응되는 키 정보 K가 TTP의 공개 디렉토리에 공개적으로 게시되기 때문에 누구나 A가 B에게 보내는 평문 메시지를 알 수 있다. 따라서, A와 B가 메시지의 내용을 제3자에게 비밀로 하고자 할 경우에는 A와 B는 부가적으로 또 다른 암호 체계를 도입하여야 하는 문제가 발생한다. 또한, 부인봉쇄 서비스가 요구되는 메시지는 일반적인 메시지 보다 비밀이 요구될 가능성이 높기 때문에 부인봉쇄 서비스와 메시지 보호 기능이 함께 제공되는 것이 바람직 하다.

본 절에서는 Zhou-Gollmann 프로토콜에서 메시지 암호키 K를 Diffie-Hellman 공개키 분배 방법[6]에 의하여 분배할 경우 수신자 B 이외에 어느 누구도 암호문 C로 부터 평문을 얻을 수 없도록 할 수 있음을 보이고자 한다. Zhou-Gollmann 프로토콜은 RSA 서명[11], ElGamal 형태의 서명[8] 등 임의의 서명 기법에 모두 적용 가능하다. 따라서, Zhou-Gollmann 프로토콜에서 사용하는 서명용 키와 독립적으로 키 분배를 위한 Diffie-Hellman 암호용 키를 각 사용자가 가지고 있을 경우에 제안된 방법을 적용할 수 있다. 그러나, 이 경우 각 사용자는 두개의 공개키 암호 시스템을 유지해야 하는 어려움이 있으며 시스템 구현의 복잡도 또한 증가된다. 그러므로, 제안되는 방식은 Zhou-Gollmann 프로토콜에서 각 사용자가 ElGamal 형태의 서명을 할 경우에 매우 효과적이다.[8] 이 경우, 각 사용자는 하나의 키를 가지고 서명을 생성할 수 있을 뿐만 아니라 메시지 암호를 위한 세션키 K를 분배할 수 있기 때문이다.

이제 메시지 암호키 분배를 위하여 각 사용자는 키분배용 공개키와 비밀키를 생성한다. p, q는 소수, $p=2q+1$이고 g는 $GF(p)$의 원시원소라 할 때, 사용자 A, B의 비밀키와 공개키는 다음과 같다.

$$p_A=g^{s_A} \bmod p,\ p_B=g^{s_B} \bmod p$$

사용자 A가 사용자 B의 공개키 p_B를 이용하여 메시지 암호 키 K를 분배하는 과정은 다음과 같다.

- 사용자 A에 의한 키 생성
  - A는 난수 $0<r<p-1$을 생성한다.
  - $K=p_B^r \bmod p$
  - $K_{sub}=g^r \bmod p$
  - K_{sub}를 사용자 B에게 전송한다.
- 사용자 B의 메시지 암호키 K 계산 : $K=K_{sub}^{s_B}=g^{rs_B} \bmod p$

K_{sub}로 부터 메시지 암호키 K를 계산할 수 있는 사람은 사용자 비밀키 s_B를 가지고 있는 사용자 B 밖에 없다. 따라서 A는 자신이 K로 암호화시킨 메시지를 B만이 받을 수 있다고 확신할 수 있다. 그러나, B는 K_{sub}가 A가 보낸 키 정보인지를 확신할 수 없다. 이러한 문제는 부인 봉쇄 프로토콜에서 A가 K_{sub}에 대한 A의 서명을 TTP가 확인하고, B가 K_{sub}에 대한 TTP의 서명을 받음으로서 해결 가능하다.

다음의 프로토콜은 앞에 기술된 Diffie-Hellman 키 분배 프로토콜을 이용하여 메시지 보호가 가능한 부인봉쇄 프로토콜이다.

$$\begin{aligned}
NRO &= S(f_{NRO}||B||L||T||C,\ s_A)\\
NRR &= S(f_{NRR}||A||L||T||T_1||C,\ s_B)\\
sub_K &= S(f_{SUB}||B||L||T||K_{sub},\ s_A)\\
con_K &= S(f_{CON}||A||B||L||T||T_0||K_{sub}\},\ s_T)
\end{aligned}$$

1. $A \rightarrow B$: f_{NRO}, B, L, T, C, NRO
2. $B \rightarrow A$: f_{NRR}, A, L, T_1, NRR
3. $A \rightarrow TTP$: $f_{SUB}, B, L, T, K_{sub}, sub\_K$
4. $B \leftrightarrow TTP$: $f_{CON}, A, B, L, T_0, K_{sub}, con\_K$
5. $A \leftrightarrow TTP$: $f_{CON}, A, B, L, T_0, K_{sub}, con\_K$

단계 3.에서 보듯이 A는 TTP에게 K_{sub}와 함께 K_{sub}의 서명 sub_K를 보낸다. 이때, TTP는 sub_K가 K_{sub}에 대한 A의 서명임을 확인하고 나서 K_{sub}가 포함된 정보에 대한 TTP의 서명 con_K와 함께 K_{sub}를 공개 디렉토리에 공개한다. 단계 4.에서 B는 공개 디렉토리로 부터 con_K를 얻어 K_{sub}가 A가 보낸 정보임을 확인한다. 또한, B는 자신의 비밀키 s_B를 이용하여 메시지 암호키 $K=K_{sub}^{s_B}=p^{r_B} \bmod p$를 계산한다. 제안된 프로토콜에서 발신자 A는 $K_{sub}=g^r \bmod p$에 사용된 난수 r를 수신 부인봉쇄에서 사용하여야 하기 때문에 비밀로 보관하고 있어야 한다. 본 프로토콜에서는 TTP 조차도 K_{sub}으로 부터 키 K를 구할 수 없기 때문에 메시지 정보를 알 수 없다. 따라서, TTP는 단순히 발신자 A가 제출한 키 정보 K_{sub}과 L 정보를 확인하는 역할만 수행한다.

발신 부인봉쇄

B는 판사에게 M, C, K_{sub}, L, T, T_0와 증거물로서 NRO, con_K를 제출한다. 판사는 다음과 같은 과정을 통하여 메시지 M을 A가 보냈음을 확인할 수 있다.

(1) con_K가 $f_{CON}||A||B||L||T||T_0||K_{sub}$에 대한 TTP의 서명임을 확인한다.
(2) K_{sub}에 대응되는 키가 K가 됨을 B로 부터 확인받는다.
(3) NRO가 $f_{NRO}||B||L||T||C$에 대한 A의 서명임을 확인한다.
(4) $M=E(C, K, d)$임을 확인한다.

단계 (2)에서 B는 판사에게 $K= K_{sub}^{s_B} \bmod p$ 됨을 증명하여야 한다. 판사가 B에게 관계식 $K= K_{sub}^{s_B} \bmod p$에 대한 증명을 요구하지 않으면 B는 키 정보를 적당히 가변시켜 M과 다른 메시지 $M'=E(C, K', d)$을 받았다고 주장할 수 있다. B가 판사에게 $K= K_{sub}^{s_B} \bmod p$가 됨을 증명하는 방법은 Chaum의 undeniable signature에서 서명 확인 프로토콜(Confirmation Protocol)과 같다.[3]

(1) 판사 : 난수 $0<a, b<p-1$를 생성하고 $R=K_{sub}^{a} \cdot g^b \bmod p$를 B에게 전송한다.
(2) B : 난수 $0<t<p-1$을 생성하고 $T_1=R \cdot g^t \bmod p$, $T_2=T_1^{s_B} \bmod p$를 계산하여 T_1, T_2를 판사에게 전송한다.
(3) 판사 : a, b를 B에게 전송한다.
(4) B : $R \stackrel{?}{=} K_{sub}^{a} \cdot g^b \bmod p$임을 확인한 후 만족되면 t를 판사에게 전송한다.
(5) 판사 : $T_1 \stackrel{?}{=} R \cdot g^t \bmod p$와 $T_2 \stackrel{?}{=} K^a \cdot p^{b+t_B} \bmod p$임을 확인하여 만족되면, $K=K_{sub}^{s_B} \bmod p$라고 판정한다.

수신 부인봉쇄

A는 판사에게 $M, C, K_{sub}, T, T_0, T_1, L, r$과 증거물 NRR, con_K를 제출한다. 판사는 다음과 같은 과정을 통하여 메시지 M을 B가 받았음을 확인할 수 있다.

(1) con_K가 $f_{CON}||A||B||L||T||T_0||K_{sub}$에 대한 TTP의 서명임을 확인한다.
(2) r, K_{sub}에 의하여 $K_{sub}=g^r \bmod p$임을 확인하고, B의 공개키 p_B에 의하여 메시지 암호키 $K=p^{r_B} \bmod p$를 계산한다.
(3) NRR이 $f_{CON}||A||L||T||T_1||C$에 대한 B의 서명임을 확인한다.
(4) $T_0<T_1<T$를 만족하는지 확인한다.
(5) $M=E(C, K, d)$를 확인한다.

5. 결 론

본 논문에서는 Zhou-Gollmann 부인봉쇄 프로토콜의 두가지 문제점을 지적하고 이러한 문제점을 해결할 수 있는 방안을 제시하였다. 첫번째 문제점은 암호키를 등록하는 권한이 발신자에게 있기 때문에 발신자가 수신자 보다 상대적으로 유리한 위치에 있다는 것이다. 발신자의 유리한 지위는 프로토콜을 공정하지 못하게 만들 수도 있다. 두번째 문제점은 메시지의 비밀을 보장하지 못한다는 것이다. Zhou-Gollmann 프로토콜에서는 발신자가 수신자에게 메시지 암호문을 주고, 암호키는 나중에 TTP의 공개 디렉토리에 게시함으로서 메시지의 비밀이 보장되지 않는다. 따라서, 발신자가 비밀 메시지를 수신자에게 보내기 위해서는 부가적인 암호 방법을 사용하여야 한다. 본 논문에서는 발신자와 수신자 사이의 불공정성을 개선하기 위하여 수신자가 발신에게 주는 메시지 수신 영수증(NRR)내에 암호키의 등록 마감 시한(T_1)을 정하여 암호키 등록에 대한 수신자의 권한을 강화하였다. 또한, Diffie-Hellman 키 분배 방법에 의하여 암호키를 수신자에게 분배하여 TTP에 등록되는 키(K_{sub})로 부터 실제 암호키 K를 얻을 수 없도록 함으로서 메시지의 비밀이 유지되도록 하였다.

본 논문에서 제안된 프로토콜은 Zhou-Gollmann 프로토콜에

기반을 두고 있기 때문에 Zhou-Gollmann 프로토콜과 마찬가지로 TTP 의존도가 적으며 통신량도 매우 적다. 다만, 발신 부인봉쇄에서 수신자는 암호키 K와 등록키 K_{sub} 사이의 관계를 판사에게 증명하여야 한다. 제안된 프로토콜의 공정성은 시간 정보의 비중이 상대적으로 매우 높은 문제점이 있다.

참 고 문 헌

[1] M. Ben-Or, O. Goldreich, S. Micali, and R. Rivest, 'A fair protocol for signing contracts', *IEEE Transactions on Information Theory*, 36(1):40-46, January 1990.

[2] E. F. Brickell, D. Chaum, I. B. Damgard, and J. van de Graaf, 'Gradual and verifiable release release of a secret', *In Advances in Cryptology: Proceedings of Crypto'87, LNCS 293*, pp. 156-166, Springer-Verlag, 1988.

[3] D. Chaum, 'Zero-Knowledge Undeniable Signatures', *In Advances in Cryptology: Proceedings of Eurocrypt'90, LNCS 473*, pp. 458-464, Springer-Verlag, 1991.

[4] R. Cleve, 'Controlled gradual disclosure schemes for random bits and their applications', *In Advances in Cryptology: Proceedings of Crypto'89, LNCS 435*, pp. 573-588, Springer-Verlag, 1990.

[5] I. B. Damgard, 'Pratical and provably secure release of a secret and exchange of signatures', *In Advances in Cryptology: Proceedings of Eurorypto'93, LNCS 765*, pp. 200-217, Springer-Verlag, 1994.

[6] W. Diffie and M. Hellman, 'New Directions in Cryptography', *IEEE Trans. on Information Theory*, 22(1976), 644-654.

[7] S. Even, O. Goldreich, and A. Lempel, 'A randomized protocol for signing contracts', *Communications of the ACM*, 28(6), pp. 637-647, June 1985.

[8] L. Harn and Y. Xu, 'Design of Generalized ElGamal Type Digital Signature Schemes Based on Discrete Logarithm', *Electronics Letters*, Vol.30, No.24, 2025-2026, Nov 1994.

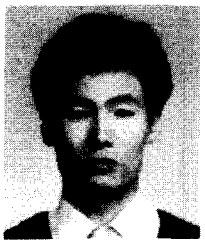
[9] ISO/IEC JTC1, Information technology - Open systems interconnection - Security frameworks in open systems, Part 4: Non-repudiation, ISO/IEC DIS 10181-4, April 1995.

[10] T. Okamoto and K. Ohta, 'How to simultaneously exchange secrets by general assumptions', *In Proceedings of 2nd ACM Conference on Computer and Communications Security*, pp. 184-192, Nove,ber 1994.

[11] Rivest, R. L., Shamir, A., and Adleman, L., "A method for obtaining digital signatures and public-key cryptosystem", *Commun. ACM*, 1978, 21, (2), pp. 120-126

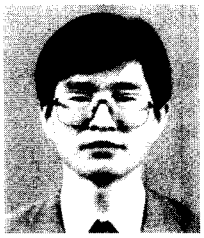
[12] J. Zhou, *A fair non-repudiation protocol*, Technical Report CSD-TR-95-08, Department of Computer Science, Royal Holloway, University of London, March 1995.

□ 著者紹介



박 상 준

1984년 2월 한양대학교 자연과학대학 수학과(이학사)
1986년 2월 한양대학교 대학원 수학과(이학석사)
1986년 1월 ~ 현재 한국전자통신연구원 선임연구원
1995년 3월 ~ 현재 성균관대학교 대학원 정보공학과 박사과정



김 광 조

1973년 ~ 1980년 연세대학교 전자공학과(학사)
1981년 ~ 1983년 연세대학교 대학원 전자공학과(석사)
1988년 ~ 1991년 요꼬하마 국립대학 대학원 전자정보공학과(박사)
현 한국전자통신연구원 실장
본 학회 암호이론연구회 및 ISO/IEC JTCI JSC-27 의장
KIISC, IEICE, IEEE, IACR 각 회원

※ 주관심 분야 : 암호학 및 응용 분야, M/W 통신

원 동 호

1976년 2월 성균관대학교 전자공학과 졸업(공학사)
1978년 2월 성균관대학교 대학원 졸업(공학석사)
1988년 2월 성균관대학교 대학원 전자공학과(공학박사)
1978년 4월 ~ 1980년 3월 한국전자통신연구소 연구원
1985년 9월 ~ 1986년 8월 일본 동경 공대 객원 연구원
1982년 3월 ~ 현재 성균관대학교 공과대학 정보공학과 교수
1991년 ~ 현재 한국통신정보보호학회 편집이사
1996년 4월 ~ 현재 정보화추진위원회 자문위원

※ 주관심 분야 : 암호이론, 정보이론