RSA 서명에 기반한 효율적인 공정한 예약과 교환 프로토콜

성인제[0] 장직현
서강대학교 컴퓨터학과
{ijsung[0], jchang,}@alglab.sogang.ac.kr

Efficient Fair Reservation and Exchange Protocol based on RSA Signature

In-Jeu Sung[0] Jik Hyun Chang
Dept. of Computere Science, Sogang University

요 약

우리는 RSA 서명에 기반한 효율적인 공정한 예약과 교환 프로토콜을 위해 검증 가능한 암호화를 일반화한 부분적인 검증 가능한 암호화를 제안한다. 부분적인 검증 가능한 암호화를 이용해서 서명에 대한 공정한 교환과 더불어 전자 계약 시 사전 계약이나 비행기 티켓에 대한 예약을 할 수 있도록 프로토콜을 확장했다. 또한 예약과 교환 시에 공정성을 보장하도록 했다. 이로써 우리는 공정한 교환 프로토콜의 교환 단계에서 발생하는 계산 양과 전송 양을 예약과 교환 단계로 분산시키는 효과를 얻었다. 그리고 마지막으로 Ateniese가 제안한 RSA 서명에 기반한 공정한 교환 프로토콜과 성능 비교를 하였다.

1. 서 론

공정한 교환 프로토콜은 두 명의 사용자가 서로의 아이템을 교환할 때, 프로토콜 수행의 종료 후에 두 명의 사용자 모두가 각자 상대방의 아이템을 정상적으로 획득하거나, 또는 어느 누구도 서로의 아이템을 획득하지 못해야 하는 특징을 만족하는 교환 프로토콜이다. 그리고 공정한 예약과 교환 프로토콜의 목적은 위와 같은 교환 프로토콜에 현재에 사용하고 있는 시스템에 맞춰 예약이라는 개념을 추가한 프로토콜이다.

공정한 예약과 교환 프로토콜은 공정한 교환 프로토콜을 예약과 교환에 두 번 사용해서 쉽게 구현할 수 있다. 본 논문에서는 예약과 교환 시에 좀 더 효율적인 성능 향상을 위해 효율적인 공정한 교환 프로토콜을 기반으로 효율적인 공정한 예약과 교환 프로토콜을 제안한다.

이전에 연구된 공정한 교환 프로토콜 중 Ateniese는 'Optimistic'한 오프라인 TTP(Trusted Third Party)를 이용한 검증 가능한 암호화 방식(Verifiable encryption)을 이용하여 여타의 프로토콜보다 효율적인 공정한 교환 프로토콜을 구현하고 있다[1].

본 논문에서는 Ateniese가 제안한 RSA 서명의 공정한 교환 프로토콜을 기반으로 해서, 교환하는 아이템에 예약 또는 사전 계약을 할 수 있도록 프로토콜을 확장하였다. 또한 부분적인 검증 가능한 암호화 방식을 제안하고 예약과 교환에 대한 전송 양과 계산 양에 대한 성능을 향상시켰다.

2. 효율적인 공정한 예약과 교환 프로토콜

효율적인 공정한 예약과 교환 프로토콜을 설계하기 위해 Ateniese가 공정한 교환 프로토콜에서 제안한 검증 가능한 암호화[1]를 변형한 부분적인 검증 가능한 암호화(Partial Verifiable Encryption) 방식을 제안한다. 그리고 RSA 서명에 기반한 효율적인 예약과 교환 프로토콜의 초기화 단계, 예약과 교환단계, 그리고 부정 방지 단계에 대해 제안한다. 먼저 앞으로 사용될 표기법은 다음과 같은 것들이 있다.

$P_X(m)$: 어떤 메시지 m에 대해서 사용자 X의 공개키를 사용하여 암호화된 메시지를 의미한다.

$S_X(m)$: 어떤 메시지 m에 대해서 사용자 X의 서명을 의미한다.

$H(m)$: 어떤 메시지 m에 대한 충돌을 회피할 수 있는 (collision-intractable) 해시 함수의 값을 의미한다 [5]. [1]

정의 1.

부분적인 검증 가능한 암호화란 서명이 올바로 삽입되었는지 TTP가 그 서명을 올바로 복호화 해낼 수 있는지에 대한 암호화이다. 이것은 각각 다음과 같이 표시한다.

$$P_T^R(S_X(m)) = \{K_1, V_1\}\ P_T^E(S_X(m)) = \{K_2, V_2\}$$

여기서 $P_T^R(S_X(m)) = \{K_1, V_1$은 서명이 삽입된 암호화($K_1$)와 그것이 올바로 삽입되었는지에 대한 증거(V_1)이고 이것은 예약 시에 검증하게 된다. $P_T^E(S_X(m)) = \{K_2, V_2\}$는 K_1에 삽입된 서명을 TTP가 올바로 복호화해 낼 수 있는지에 대한 암호화(K_2)와 증거(V_2)이다.[2]

검증 가능한 암호화는 이산 대수(Discrete Logarithm)의 동등성을 통해서 검증된다. 이산 대수의 동등성은 증명자가 검증자에게 이산 대수 문제가 같음을 확인시키는 서명 스킴이다[2]. 주어진 g_1^x, g_2^x 에 대해서 증명자(prover)가 검증자(verifier)에게 x가 같다는 것($Dlog_{g_1}g_1^x = Dlog_{g_2}g_2^x$)을 x에 대한 정보를 드러냄 없이 확인시키는 것이다. 또한 RSA 서명에서 사용할 위수를 공개하지 않고 이산 대수의 동등성을 보이는 방법에 대한 서명 스킴[3,4]은 본논문에서 제안한 RSA에 서명에 기반

1) 이러한 해쉬 함수에는 MD5, SHA등과 같은 것이 쓰이고 있다.
2) R은 Reservation의 약자, E는 Exchange의 약자, 그리고 T는 TTP의 약자이다.

한 효율적인 공정한 예약과 교환 프로토콜에 사용한다. 우리는 이것을 EQ_DLOG(m; g_1^x, g_2^x; g_1, g_2) 라고 표시한다.

위에서 설명한 부분적인 검증 가능한 암호를 토대로 한 RSA 서명에 기반한 효율적인 공정한 예약과 교환 프로토콜의 단계는 다음과 같다. 여기서 서로의 전자서명을 교환하기를 원하는 사용자를 각각 Alice와 Bob이라고 한다.

2.1 초기화 단계

사용자는 자신의 공개키와 ID등에 대한 확인서를 TTP와 교환한다. 여기서 d, p, q는 RSA 서명의 비밀키이고 e, n=pq는 RSA 서명의 공개키이다. $CERT_A$는 Alice의 확인서, $CERT_{T:A}$는 Alice에 대한 TTP의 확인서, x는 TTP의 비밀키 y, g는 TTP의 공개키이다. RSA 서명에 기반한 효율적인 공정한 예약과 교환프로토콜에서 사용자는 그림 1과 같이 TTP에게 자신의 공개키(e, n, $CERT_A$)에 대한 검증을 받고, TTP의 공개키, 서명자의 공개키에 대한 확인서($CERT_{T:A}$)를 받는다.

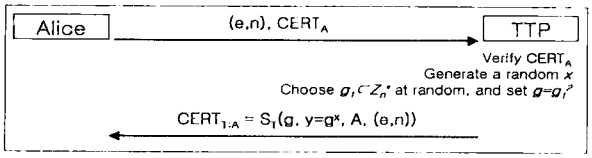

그림 1. 초기화 단계

예약 단계와 교환 단계에서는 전자서명을 교환하기를 원하는 사용자 중, 일반성을 잃지 않고, Alice가 프로토콜을 먼저 시작한다고 가정한다.

2.2 예약 단계

TTP에 등록단계를 거쳐서, 공개키와 예약에 사용될 티켓을 얻은 Alice는 다음 그림 2와 같이 예약 단계를 수행한다. 여기서 r은 Alice가 임의로 선택한 비밀정수이고 m_A와 m_B는 각각 Alice와 Bob에 대한 예약과 실제 서명에 대한 메시지이다.

1. Alice는 서명을 검증할 수 있는 부분적인 검증 가능한 암호화($P_T^R(S_{Alice}(m_A))$ = (K_1, $V_1 = c_A$를 다음 그림 2와 같이 계산해서 Bob에게 보낸다.
2. Bob은 Alice에게서 받은 $P_T^R(S_{Alice}(m_A))$를 가지고 Alice의 서명이 올바로 암호화되었는지 증거 $V_1 = c_A$을 가지고 그림 2와 같은 과정을 거쳐서 검증한다. 맞으면 Alice에게 예약이 되었다는 메시지(예약 확인서, m_B)와 그것을 확인할 수 있는 증거(c_B)를 보낸다.
3. Alice는 예약이 되었다는 것을 Bob에게서 받은 m_B를 검증하고 프로토콜을 종료한다.

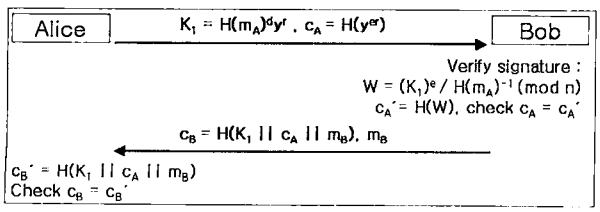

그림 2 . 예약단계

2.3 교환 단계

1. Alice는 예약단계에서 보낸 부분적인 검증 가능한 암호화에서 TTP가 올바로 서명을 복호화 할 수 있는 부분적인 검증 가능한 암호화($P_T^E(S_{Alice}(m_A))$ = (K_2, V_2 = (c,s)))를 그림 3과 같이 계산해서 Bob에게 보낸다. 여기서 (c,s)는 예약단계에서 서명을 암호화 시킬 때 쓴 임의의 비밀정수 r값이 같은 값인지 검증하는 증거로서 이산 대수의 동등성을 보인다.[3)]
2. Bob은 예약단계에서 받은 부분적인 검증 가능한 암호화, $P_T^R(S_{Alice}(m_A))$의 K_1과 $P_T^E(S_{Alice}(m_A))$의 K_2, 그리고 증거 V_2 = (c,s)를 가지고 TTP가 올바로 서명을 복호화 할 수 있는지 그림 3과 같은 과정을 거쳐서 검증한다. 이것이 맞으면 Bob은 Alice에게 자신의 서명, $S_{Bob}(m_B)$을 보낸다. 그렇지 않으면 프로토콜을 종료한다.
3. Alice는 Bob의 서명, $S_{Bob}(m_B)$을 받아서 검증한 후 맞으면 Bob에게 자신의 서명, $S_{Alice}(m_A)$을 보낸다.

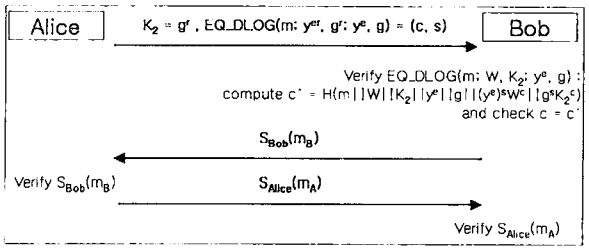

그림 3. 교환 단계

2.4 부정 방지 단계

다음은 예약 단계와 교환 단계에서 일어 날 수 있는 사용자의 전송거부나 기타 예측할 수 없는 이유로 인한 프로토콜의 비정상적인 종료 시에 수행하는 부정 방지 단계에서의 프로토콜을 설명하고 있다.

2.4.1 예약단계

예약 프로토콜 종료 후 Alice는 예약을 했다는 사실을 부정할 수 없어야 한다. 이는 Bob이 $P_T^R(S_{Alice}(m_A))$을 가지고 서명이 삽입되어 있다는 것을 보임으로서 Alice가 예약했다는 사실을 TTP에게 증명할 수 있다. 만약에 Bob이 예약 확인서를 Alice에게 주지 않고 Alice가 예약했다고 주장 할 수 있다. 이것은 사전에 Alice가 예약 확인서를 받지 못하면 TTP에게 $P_T^R(S_{Alice}(m_A))$의 증거 V_1를 보내서 미리 방지 할 수 있다.

2.4.2 교환단계

만약 Bob이 Alice의 서명을 받지 못했거나 잘못된 서명을 받았을 경우에 그는 (K_1, K_2)와 $S_{Bob}(m_B)$를 TTP에게 보낸다. TTP는 Bob의 서명을 검증한 후 (K_1, K_2)에서 Alice의 서명을 복호화 한 후 Bob에게 Alice의 서명을, Alice에게는 Bob의 서명을 보낸다.

3) K_1과 K_2의 r값이 같아야 TTP가 복호화해 낼 수 있다. 이는 K_1과 K_2의 이산 대수의 동등성을 보임으로서 검증하게 된다.

2.5 필요한 성질들

기본적으로 예약 단계에서 필요한 성질은 이전의 공정한 교환 프로토콜의 교환 단계에서 만족해야 하는 성질을 기반으로 한다. 하지만 예약을 한 후 사용자가 예약에 대한 취소를 할 수 있을 것이다. 이를 위해 예약 프로토콜의 종료 후에 한 사용자가 TTP에게 접근해서 올바른 서명을 얻어낼 수 없어야 한다. 다시 말해서 단지 예약을 했다는 메시지만 검증 할 수 있어야 하며, 실질적인 아이템을 얻어내서는 안 된다. 이를 위해서는 예약 단계에서는 다음과 같은 성질을 만족한다.

2.5.1 예약단계

예약 단계에서 각각의 사용자의 진정한 공정성을 위해서는 다음과 같은 특징을 만족하고 있어야 한다.

성질 1. (Completeness)
프로토콜의 수행이 끝난 후에, 두 명의 사용자 모두가 서로 예약되었다는 증거를 획득해야 한다.
성질 2. (Soundness)
부분적인 검증 가능한 암호화를 제작한 서명자 외에 어떠한 사용자에 의해서도 완전한 서명으로 전환 될 수 없다.
성질 3 (Zero Knowledge, Fairness)
Bob의 입장에서 부분적인 검증 가능한 암호화를 가지고 서명 또는 K_2에 대한 값을 알아낼 수 없어야 한다. 만약에 K_2를 알아낸다면, 실제 교환 프로토콜 전에 Bob은 TTP에게 접근해서 Alice의 서명을 얻어낼 수 있다. 이것은 Alice가 예약을 취소하는 것을 방해한다.

2.5.2 교환단계

예약 단계와 마찬가지로 공정성을 만족하기 위해서는 Completeness, Soundness, Zero Knowledge를 만족해야 한다. 공정한 예약과 교환 프로토콜에서의 교환 단계는 기본적으로 공정한 교환 프로토콜의 개념에 예약단계를 추가 한 것이기 때문에, 교환 단계의 기본적인 성질은 이전의 공정한 교환 프로토콜을 따르고 있다.

2.6 보안성

RSA 서명의 성질 1은 위에서 제안된 프로토콜에서 명확하다는 것을 알 수 있고 성질 3을 만족하면 성질 2는 만족하게 된다. 또한 효율적인 공정한 예약과 교환 프로토콜은 기존의 공정한 교환 프로토콜을 기반으로 했기 때문에 교환 단계의 성질을 만족한다. 따라서 성질 3이 만족하는 것만 보이면 된다. 이러한 성질 3은 다음의 정리 1을 증명하면 만족한다. 증명은 논문 [6]을 참고하기 바란다.

정리 1.
이산 대수 문제의 해결이 어렵다면, 제안된 예약 프로토콜에서 서명과 g^r에 대해 알아 낼 수 있는 정보는 계산상 불가능하다.

3. 성능 비교

효율적인 공정한 예약과 교환 프로토콜과 기존의 공정한 교환 프로토콜과의 성능을 비교하면 표 1에서 이전에 제안된 공정한 교환 프로토콜의 계산 양과 전송 양을 분산시키는 것을 볼 수 있다.

표 1. 성능 비교

프로토콜	지수 계산 양			전송 양(byte)		
	예약 단계	교환 단계	총 계산 양	예약 단계	교환 단계	총 전송 양
공정한 교환 프로토콜		8.5	8.5		400	400
공정한 예약과 교환 프로토콜	3.17	5.3	8.5	218	214	432

4. 결론

효율적인 공정한 예약과 교환 프로토콜은 부분적인 검증 가능한 암호화 방식을 적용하면 RSA 서명 뿐만 아니라 Cramrre-Shoup, Guillou-Quisquater, Schnorr, DSA, ElGamal 서명 등 여러 가지 서명에 대해서도 적용할 수 있다 [6]. 앞으로 전 세계적으로 전자 무역과 전자 상거래는 더욱 더 증가할 것이다. 따라서 어떤 전자적인 교환에 있어서 예약 또는 사전 계약 또한 증가할 것이다. 그리고 네트워크가 소형화 됨에 따라 좀 더 효율적이고 안전한 장치가 필요할 것이다. 이러한 시기에 본 논문이 제시한 효율적인 공정한 예약과 교환 프로토콜은 공정한 교환이라는 특성에 예약이라는 개념을 추가함으로서 좀더 현실 세계에 맞춰, 많은 작업들을 네트워크로 흡수했다. 또한 교환 시에 계산 양과 전송 양을 예약 단계로 분산시켰다는 데에 의의를 찾을 수 있겠다.

5. 참고문헌

[1] G. Ateniese., Efficient Verifiable Encryption (and Fair Exchange) of Digital Signatures., In 6th ACM Conferences on Computer and Communications Security, 1999
[2] D. Chaum and T. Pedersen. Wallet databases with observers. In Advances in Cryptology - Crypto '92, pp 89-105, 1992.
[3] D. Pointcheval and J. Stern. Security proofs for signature schemes. In Advances in Cryptology - EUROCRYPTO '96, volume 1070 of Lecture Notes in Computer Science, pp 387-398, Springer-Verlag, 1996.
[4] G. Poupard and J. Stern. Security analysis of a pracical "on the fly" authentication and signature generation. In Advances in Cryptology - EUROCRYPTO '98, volume 1403 of Lecture Notes in Computer Science, pp 422-436, Springer-Verlag, 1998.
[5] I. Damgard. Collision free hash functions and public key signature schemes. In Advances in Cryptology - EUROCRYPTO '87, volume 304, pp 203-216, Springer-Verlag, 1987.
[6] 성인재. 효율적인 공정한 예약과 교환 프로토콜. 서강대학교 석사학위 논문. 2001.