Domain-verifiable Signcryption 기법을 이용한 전자자금이체 프로토콜

서문석, 김광조

한국정보통신대학원대학교

EFT Protocol using Domain-verifiable Signcryption Scheme

Moonseog Seo, Kwangjo Kim

Information and Communications Univ.

요약

금융기관의 고객이 전자적인 수단을 이용하여 자금이체를 의뢰하여 금융기관 사이에 자금이 전달되는 전자자금이체(EFT) 프로토콜은 거래의 안전한 처리를 위해서 전자서명 기법과 암호화 기법을 동시에 요구한다. 이러한 유형의 응용에 있어서 Signcryption 기법은 효율성을 성취하기 위한 중요한 도구로 사용되어질 수 있다. Zheng에 의해 제안된 Signcryption[3] 기법은 전자서명과 암호화 기능을 계산비용을 절감하면서 논리적 한 스텝으로 통합할 수 있는 암호의 기본요소이다.

본 논문에서는 전자자금이체 프로토콜에 적용하기 위해서 프로토콜 참여자 집합(Domain) 내에서만 복호화 및 검증이 가능한 Domain-verifiable signcryption 기법을 제시한다. 이러한 Domain-verifiable signcryption 기법은 각 프로토콜 참여자의 해당 부분 정보에 대한 기밀을 유지하기 위해 TTP를 가정해야만 하는 Zheng의 기법과 효율성 면에서 대등한 반면, TTP의 역할을 필요로 하지 않는다.

I. 서론

금융관련 서비스 중 그 이용도가 높고 안전이 요구되는 중요한 서비스로 전자자금이체(EFT:Electronic Funds Transfer) 서비스가 있다. 전자자금이체 서비스는

금융기관의 고객이 전자적인 수단을 이용하여 자금이체 거래를 의뢰함으로써 관련 금융기관사이에서 자금이체가 이루어지도록 하는 서비스이다. 이러한 서비스를 인터넷과 같은 개방형 네트워크 상에서 제공하기 위해서는 기밀성 및 인증 서비스를 동시에 이용할 수 있어야 한다.

금융거래의 특성 상, 효율성은 금융 서비스가 요구하는 가장 중요한 요소 중의 하나이며, 이러한 효율성을 충족시키기 위하여 signcryption 기법은 훌륭한 해결책을 제시하고 있다. Y. Zheng에 의해 최초로 제안된 Signcryption[3]은 새로운 암호의 기본 요소로써 서명과 암호 기능을 논리적인 한 스텝으로 동시에 처리할 수 있으며 계산 비용 측면에 있어서도 전통적인 서명-후-암호 패러다임에 의해 요구되는 계산량 보다 현저히 낮다고 할 수 있다[1,2,3].

많은 참여자가 프로토콜에 참여해야하는 EFT 프로토콜에 이러한 signcryption 기법을 적용하기 위해서는 프로토콜 참여자 집합인 도메인내의 기 지정된 n명의 참여자만이 전체 메시지 내에서 자신의 부분정보만을 복호화할 수 있고 전체 메시지에 대해 검증이 가능한 변형된 signcryption 기법이 요구된다. 우리는 이러한 변형된 signcryption 기법을 Domain-verifiable signcryption 기법이라고 부를 것이며, 여기서 도메인의 의미는 프로토콜 참여자들로 구성된 집합을 의미한다.

Zheng의 signcryption 기법에서, unsigncryption(복호화와 서명검증)은 메시지 수신자의 개인키를 필요로 한다. 결국, 메시지의 정당 수신자만이 서명을 검증할 수 있음을 의미한다. 이러한 Zheng의 signcryption 기법은 서명이 제삼자에 의해 검증되어져야하는 경우에는 이용될 수 없는 단점을 가지고 있다.

이러한 문제를 해결하기 위하여 Bao와 Deng(이하 "BD기법"이라 함)[4]이 Zheng의 signcryption 기법을 수정하여 서명 검증에 수신자의 개인키를 요구하지 않는 기법을 제시하였으나 BD기법은 계산량 측면에서 Zheng의 기법만큼 효율적이지 못하다. 또한, 이 기법은 제 삼자에 의해 검증되기 위해서는 메시지가 복원되어야 하기 때문에 메시지의 기밀성이 유지될 수 없는 단점을 가지고 있다. 메시지의 기밀성을 유지하면서 방화벽 시스템에 이용하기 위해 Gamage, Leiwo, Zheng(이하 "GLZ기법"이라 함)[5]은 BD기법을 수정한 새로운 signcryption 기법을 제시하였다. 그러나 이 기법에서는 임의의 제삼자에 의해 서명 검증이 가능하나 단지 한사람 즉, 원래의 메시지 수신자만이 평문을 얻을 수 있다.

EFT 및 SET(Secure Electronic Transactions) 프로토콜[10]과 같은 응용에서

는 하나의 트랜잭션 처리를 위해 다수의 참여자가 존재한다. 트랜잭션 처리를 위한 메시지는 각 참여자에 의해 처리되어질 비밀 정보들로 구성되어진다. 각 참여자는 자신과 관련된 정보에 대해 기밀성 유지를 요구할 것이며 전체 메시지에 대한 인증도 동시에 요구할 것이다. 이러한 측면에서, 지금까지 제시되었던 signcryption 기법들은[6,7] 이러한 유형의 응용에 직접 적용되어 질 수 없다.

본 논문에서 GLZ기법을 근간으로 EFT 및 SET 프로토콜과 같은 응용에 쉽게 적용되어 질 수 있는 Domain-verifiable signcryption 기법을 제시하고 그 응용의 예로써 고객의 요구에 의해 두 은행간에 자금이체가 이루어지는 은행간 EFT 프로토콜을 설계하였다. Domain-verifiable signcryption 기법은 계산량 측면에서 각 프로토콜 참여자의 부분정보에 대한 기밀성 유지 및 다중 검증을 가능하게 하기 위하여 TTP의 존재를 가정해야만 하는 Zheng의 기법만큼 효율적이며, TTP와의 상호작용 없이 EFT 프로토콜을 구성할 수 있다.

본 논문은 다음과 같이 구성되어진다. 지금까지 제시된 다양한 signcryption 기법에 대해 2장에서 간단히 살펴보았으며, domain-verification을 위해 제안된 기법이 3장에 제시된다. 4장에서는 Domain-verifiable signcryption 기법의 응용으로서 EFT 프로토콜을 설계하였으며, 5장에서 결론을 맺는다.

II. 관련 연구

본 장에서는 지금까지 제시된 세 가지 signcryption 기법들에 대해 설명한다. [3]에서 Zheng 에 의해 제시된 signcryption 기법은 메시지의 기밀성과 인증성을 만족하기 위해 서명 후 암호라는 두 단계의 처리과정을 한 단계로 통합하여 계산량 및 통신비용의 절감을 도모한 방식이다. 그러나 단지 지정된 수신자만이 메시지를 검증할 수 있다는 단점이 있다.

[4]에서 Bao와 Deng에 의해 이러한 단점을 극복할 수 있는 변형된 signcryption 기법이 제시되었다. 그러나 이 기법은 Zheng의 기법에 비해 통신량은 적절히 보장되나 계산량 측면에서 비효율적이다. 이 기법이 가지고 있는 두 가지 단점은 다음과 같다.

- signature verification-only mode는 원래 메시지 수신자가 복원된 평문메시지를 제시한 후에야만 사용되어질 수 있다.
- 서명 검증을 위해서는 제 삼 검증자에게 메시지의 평문이 전달되야 하며, 이로 인해 메시지의 기밀성이 손실된다.

[5]에서, GLZ기법은 기밀성을 보존하기 위해 평문의 요구 없이도 서명 검증을 수행할 수 있도록 BD기법을 수정하였다. 그러나 이 기법에서는 임의의 검증자도 서명 검증을 할 수 있는 반면 단지 한사람만이 평문을 얻을 수 있다.

결국, 이러한 모든 기법들은 트랜잭션의 메시지가 프로토콜 참가자 자신의 정보에 대해서는 다른 참여자를 포함한 임의의 제삼자에 대해서조차 기밀성이 유지되기를 원하는 부분정보들로 구성된 EFT 프로토콜의 메시지 처리를 위해서는 직접 적용되어질 수 없다.

1. Zheng 기법

처리가 요구되는 작업은 A가 B에게 메시지를 전송하는 경우 A는 signature-then-encryption과 동일한 효과를 얻기 위해 signcryption을 수행하고 B는 unsigncryption을 수행하는 것이다.

공개 변수 :

p : 큰 소수

q : $p-1$을 나누는 큰 소수

g : 위수가 q인 Z_p^*상의 원소

$hash$: 일방향 해쉬 함수

KH : keyed-일방향 해쉬 함수

(E, D) : 대칭키 암호 시스템의 암,복호 알고리즘

A의 키 :

x_a : A의 개인키, $x_a \in Z_q^*$

$y_a = g^{x_a} \bmod p$: A의 공개키

B의 키 :

x_b : B의 개인키, $x_b \in Z_q^*$

$y_b = g^{x_b} \bmod p$: B의 공개키

Signcrypting :

A는 $x \in Z_q^*$를 랜덤하게 선택한 후 다음을 계산한다.

$(k_1, k_2) = hash(y_b^{\,x} \bmod p)$

$c = E_{k_1}(m)$

$r = KH_{k_2}(m)$

$s = x/(r + x_a) \mod q.$

A는 (c, r, s)를 B에게 전송한다.

Unsigncrypting :

B는 다음을 계산한다.

$(k_1, k_2) = hash((y_a g^r)^{sx_b} \mod p).$

평문을 복원하기 위하여 $m = D_{k_1}(c)$을 계산하고, 서명의 검증을 위해 $KH_{k_2}(m) = r$를 검사한다.

unsigncryption과정에서 B의 개인키 x_b가 사용됨을 인식할 수 있다.

2. BD 기법

Signcrypting :

A는 $x \in Z_q^*$를 랜덤하게 선택한 후 다음을 계산한다.

$k_1 = hash(y_b^x \mod p)$

$k = hash(g^x \mod p)$

$c = E_{k_1}(m)$

$r = KH_k(m)$

$s = x/(r + x_a) \mod q.$

A는 (c, r, s)를 B에게 전송한다.

Unsigncrypting :

B는 다음을 계산한다.

$t_1 = (y_a g^r)^s \mod p$

$t_2 = t_1^{x_b} \mod p$

$k_1 = hash(t_2)$

$k = hash(t_1).$

평문을 얻기 위하여 $m = D_{k_1}(c)$를 계산한 후, 서명 검증을 위해 $KH_k(m) = r$ 여부를 검사한다.

추후 필요시, B는 (m, r, s)를 다른 제삼자에게 전송할 수 있으며, 수신한 제삼자는 서명 검증을 위해 $k = hash((y_a g^r)^s \mod p)$과 $r = KH_k(m)$ 여부를 검

사함으로써 (m, r, s)가 A로부터 송신된 것임을 확인할 수 있다. 이러한 서명 검증 과정에서 검증자는 평문의 정보를 얻을 수 있다.

3. GLZ 기법

Signcrypting :

A는 $x \in Z_q^*$를 랜덤하게 선택한 후 다음을 계산한다.

$k = hash(y_b^x \bmod p)$

$y = g^x \bmod p$

$c = E_k(m)$

$r = hash(y, c)$

$s = x/(r + x_a) \bmod q.$

A는 (c, r, s)를 B에게 전송한다.

Unsigncrypting :

B는 (c, r, s)로부터 다음을 계산한다.

$y = (y_a g^r)^s \bmod p$

$k = hash(y^{x_b} \bmod p).$

평문을 얻기 위해 $m = D_k(c)$를 계산한다.

B는 $hash(y, c) = r$이 성립될 경우만 서명을 인정한다.

signature-verification-only만을 갖는 부분적인 unsigncryption을 위해, 어떠한 검증자도 (c, r, s)로부터 $y = (y_a g^r)^s \bmod p$를 계산할 수 있다. 검증자는 $hash(y, c) = r$인 경우에 만 서명을 인정한다. 이러한 서명 검증 과정은 평문에 대한 접근을 요구하지 않는다.

III. Domain-verifiable Signcryption 기법

여기서는 EFT 또는 SET 프로토콜과 같이 다수의 프로토콜참여자가 존재하며 참가자들 사이에서 처리되는 트랜잭션이 각 참여자들의 비밀정보로 구성되어 각각에 대해 기밀성이 유지되어야 하고 동시에 전체 트랜잭션 메시지는 각 참여자들에 의해 검증이 가능하도록 하는 요구사항을 충족할 수 있는 Domain-verifiable signcryption 기법을 제시한다.

1. domain-verification 기법

일관성 유지를 위해 수신자의 키를 제외하고 Zheng의 기법과 동일한 표기법을 사용한다.

n명의 참여자로 구성된 도메인 내의 수신자 B_i의 키($i \in \{1, \ldots, n\}$)

x_{b_i} : B_i의 개인키

y_{b_i} : B_i의 공개키

Signcrypting :

A는 $x \in Z_q^*$를 랜덤하게 선택한 후 다음을 계산한다.

$k_1 = hash(\ y_{b_1}{}^{x} \mod p), k_2 = hash(\ y_{b_2}{}^{x} \mod p), \ldots, k_n =$

$hash(\ y_{b_n}{}^{x} \mod p)$

$k = hash(g^x \mod p)$

$c_1 = E_{k_1}(m_1), c_2 = E_{k_2}(m_2), \ldots, c_n = E_{k_n}(m_n)$

$r_1 = KH_k(m_1 \| c_2 \| \cdots \| c_n), r_2 = KH_k(c_1 \| m_2 \| \cdots \| c_n), \ldots, r_n =$

$KH_k(c_1 \| c_2 \| \cdots \| m_n)$

$s = x/(r_1 r_2 \ldots r_n + x_a) \mod q.$

A는 $(c_1, c_2, \ldots, c_n, r_1, r_2, \ldots, r_n, s)$를 B_i에게 전송한다.

Unsigncrypting :

수신자 B_i는 다음을 계산한다.

$t = (y_a g^{r_1 r_2 \ldots r_n})^s \mod p$

$t_i = t^{x_{b_i}} \mod p$

$k = hash(t)$

$k_i = hash(t_i),$

B_i 자신의 평문을 얻기 위하여 $m_i = D_{k_i}(c_i)$를 수행한 후, 서명 검증을 위해 $KH_k(c_1 \| \cdots \| m_i \| \cdots \| c_n) = r_i$ 여부를 검사한다.

추후 필요시, B_i는 $(c_1, c_2, \ldots, c_n, r_1, r_2, \ldots, r_n, s)$를 다른 프로토콜 참여자에게 전송하여 unsigncryption을 통해 자신의 부분 메시지를 복원하고 해당 메시지가

A로부터 전송되었음을 확인할 수 있도록 한다.

2. 성능 및 안전성

Domain-verifiable signcryption 기법이 적용되어져야만 하는 상황을 고려하면 Zheng의 기법에는 트랜잭션 메시지를 각 참여자를 위한 부분메시지로 안전하게 나누기 위해 제 삼의 신뢰기관인 TTP(Trusted Third Party)를 반드시 포함시켜야 한다[6]. 그러나 Domain-verifiable signcryption 기법은 이러한 TTP를 필요로 하지 않는다. 계산비용으로 지수승 비용만을 고려하고, n명의 참여자가 있다고 가정할 때, Domain-verifiable signcryption 기법은 signcryption을 위한 $n+1$번의 지수승과 unsigncryption을 위한 $3n$번의 지수승을 필요로 한다. 2 또는 3명 이상의 n명의 참여자가 참가하는 일반적인 상황에서 본 기법의 통신량은 TTP의 존재를 가정한 Zheng의 기법보다 적지 않다. 이는 n명의 참가자를 위한 전체 트랜잭션 메시지가 항상 n명에게 전달되어져야 하기 때문이다.

Domain-verifiable signcryption 기법은 도메인 내에 자신의 비밀키 x_{b_i}를 가지고 있는 참가자 B_i만이 자신의 부분정보인 m_i를 획득할 수 있고 이러한 m_i를 얻을 수 있는 사람만이 전체 메시지에 대한 서명의 검증을 위해 $KH_k(c_1\|\cdots\|m_i\|\cdots\|c_n)=r_i$이 성립하는 지 여부를 검사할 수 있기 때문에 프로토콜 참가자의 도메인 내에서만 메시지에 대한 unsigncryption이 가능하다. 즉, 비밀정보 x_{b_i}를 갖지 못한 어느 누구도 unsigncryption에 참가할 수 없다.

[5]에서는 하나의 비밀 값 x를 이용하여 $y_b^x \bmod p$과 $g^x \bmod p$의 두 값을 계산하는 것에 대한 안전성과 관련하여 random oracle model하에서 그 안전성을 증명하였을 뿐만 아니라 서명기법의 안전성을 보장하기 위해서는 두 계산 값이 의사 독립성(pseudo-independence) 이 있어야 함을 보여주었다. 즉, 서명자가 정수 x를 랜덤하게 선택하면, 위수가 q(소수)인 Z_p^*상에서 생성원(generator)인 두 값은 의사 독립적이다. 이것은 서명 검증과 정보의 복구가 메시지의 기밀성을 파괴하거나 서명을 위조할 수 있는 공격에 사용되어질 수 있는 정보를 누출하지 않음을 보장한다.

이러한 안전성 증명 방법은 Domain-verifiable Signcryption 기법에도 그대로 적용되어질 수 있다. 서명자가 임의의 정수 x를 랜덤하게 선택하면

Domain-verifiable signcryption에서 위수가 q(소수)인 Z_p^*상에서 생성원인 $y_{b_1}{}^x \bmod p, \ldots, y_{b_n}{}^x \bmod p$ 그리고 $g^x \bmod p$과 같은 $n+1$개의 값들은 의사 독립적이다. 이것은 Domain-verifiable signcryption 기법이 메시지의 기밀성과 서명 위조 불가능성을 보장한다.

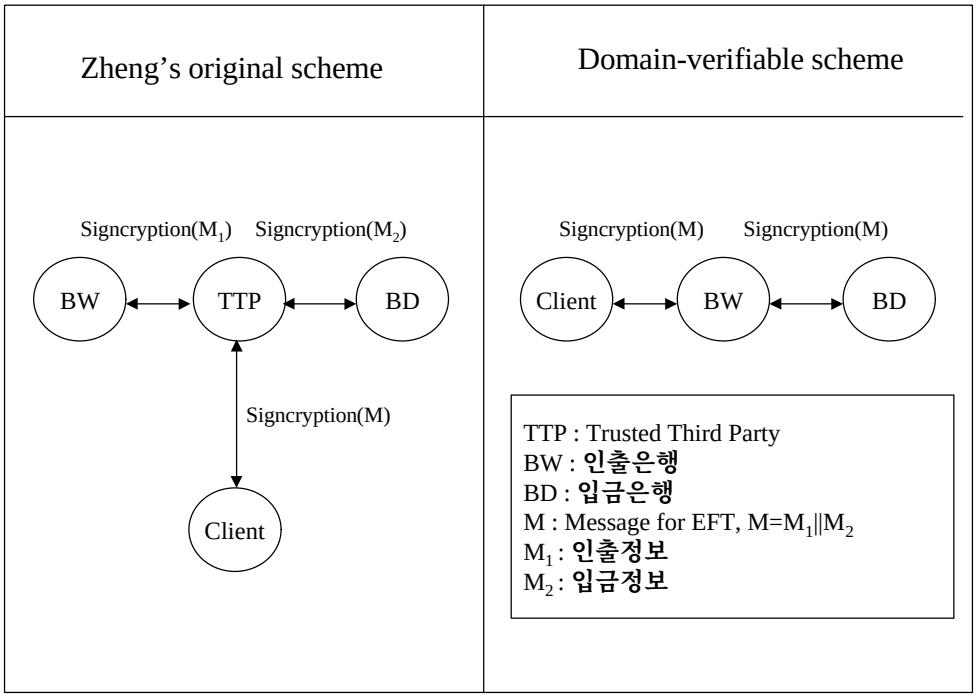
IV. Domain-verifiable Signcryption에 근간한 EFT 프로토콜

EFT는 현금 또는 수표 등과 같은 종이에 기반한 금융거래와는 달리 터미널, 전화, 컴퓨터 또는 자기테입과 같은 전자적인 시스템을 이용하여 거래가 시작되는 자금이체 방법이다. 은행간 전자자금이체 프로토콜은 인출계좌와 입금계좌가 서로 다른 은행에 존재하고 이들 두 은행사이에서 자금이 이체되는 형태이다.

고객은 계좌개설을 통해 자신과 거래 관계에 있는 은행에 자금이체거래를 의뢰하고 의뢰를 받은 은행은 거래의 정당성을 검증한 후 해당 금액을 의뢰 고객의 계좌로부터 인출하고 입금은행에 입금을 의뢰한다. 입금은행은 수신자의 계좌에 해당 금액을 입금한다. 입금은행으로부터 입금결과를 통보 받은 인출은행은 입금결과의 정상처리 여부에 따라 해당 처리를 한 후 자금이체를 의뢰한 고객에게 최종 자금이체 거래에 대한 처리 결과를 전송한다[8].

고객이 인출은행에 보내는 메시지는 고객의 계좌번호, 해당계좌의 비밀번호 등과 같은 고객정보 및 입금은행, 입금계좌번호 등과 같은 수신자 정보와 이체금액 등으로 구성된다. 이러한 메시지는 무결성 확보를 위하여 서명이 되어야 하고 기밀성 유지를 위해 암호화되어져야 한다. 즉, 고객의 정보는 인출은행만이 알 수 있도록 암호화되어져야 하고 입금정보는 입금은행만이 알 수 있도록 암호화되어져야 한다. 또한, 전자자금이체 프로토콜을 위한 전체 메시지는 인출은행 및 입금은행 모두에 의해 인증되어야만 한다. 이를 위해서 본 논문에서 제안한 Domain-verifiable signcryption 기법을 이용한다.

은행간 전자자금이체 프로토콜에 signcryption 기법을 적용하기 위해, Zheng의 기법을 사용하는 경우에는 TTP를 필요로 하지만 Domain-verifiable signcryption을 사용하는 경우, (그림 1)에서와 같이 별도의 TTP를 필요로 하지 않는다.



(그림 1) signcryption 기법을 사용한 EFT 프로토콜

1. 은행간 전자자금이체 프로토콜

이 프로토콜을 기술하기 위해 다음의 표기법을 사용한다.

참여자 및 사용도구

고객 : A

인출은행 : BW

입금은행 : BD

$Signcrypt_A(\cdot)$: 고객 A에 의한 Domain-verifiable signcryption으로 signature-verification-only mode를 포함한다[3].

$Unsigncrypt_A(\cdot)$: 고객 A에 의한 Domain-verifiable unsigncryption

$Sign_A(\cdot)$: 고객 A에 의한 서명

|| : 메시지 연접

$hash(\cdot)$: hash 알고리즘

사전준비

자금이체 정보의 생성 : $M = M_1 \| M_2 \| COM$

- M_1 : 인출계좌번호, PIN 등으로 구성된 고객 A의 정보로서 인출은행을 위해 암호화된다.
- M_2 : 입금은행, 입금계좌번호 등과 같은 입금정보로서 입금은행을 위해 암호화된다.
- COM : 이체금액, 날짜 그리고 일련번호 등과 같이 인출은행 및 입금은행에 의해 사용될 전자자금이체 처리를 위한 공통정보로서 프로토콜 수행 동안 평문으로 유지되는 정보이다.

이체 프로토콜

1) 고객 A는 $Signcrypt_A(M)$를 통해 $SM = (c_1, c_2, COM, r_1, r_2, s)$을 생성한 후 SM을 인출은행인 BW전달한다. 여기서
$c_1 = E_{k_1}(M_1), c_2 = E_{k_2}(M_2), r_1 = KH_k(M_1 \| c_2 \| COM), r_2 = KH_k(c_1 \| M_2 \| COM)$
이고 $s = x/(r_1 r_2 + x_A) \bmod q$이다.
2) BW는 자신의 암호문인 c_1으로부터 평문인 M_1를 생성하고 SM을 검증하기 위해 $Unsigncrypt_A(SM)$을 수행한다.
3) BW는 날짜 및 일련번호 등을 이용하여 고객으로부터 의뢰 받은 거래의 부정중복거래 여부를 검사한 후 정당한 경우 M_1에 기재되어 있는 고객 A의 계좌로부터 해당 금액을 인출하고 SM을 입금은행 BD로 송부한다.
4) BD는 $Unsigncrypt_A(SM)$를 수행하여 c_2로부터 자신의 메시지 M_2를 얻고 SM을 검증한다.
5) BD는 평문으로 유지된 COM에 있는 정보를 이용하여 부정 중복 거래 여부를 검사한 후 정당한 경우 M_2에 있는 해당 계좌에 금액을 입금한다.
6) BD는 $r = Sign_{BD}(SM \| 입금결과)$을 생성한 후 $(입금결과, r)$을 BW에 전송한다.
7) BW는 BD로 부터 수신한 입금결과에 따라 필요한 처리를 한 후 $\hat{r} = Sign_{BW}(이체결과)$를 생성하여 고객 A에게 전송한다.
8) 고객 A는 수신한 $(이체결과, \hat{r})$를 자금 수령인을 위한 영수증으로 사용할 수 있다.

2. 안전성 측면

Domain-verifiable signcryption에 근간한 EFT 프로토콜의 안전성은 다음과 같이 요약되어질 수 있다.

- 기밀성 : 공격자는 고객과 은행들 사이에 전달되는 평문 M을 알아낼 수 없다. 이는 전송 전에 해당은행을 위해 암호화되어있기 때문이다. 특히, 자금인출을 위한 고객의 비밀 정보로서 M_1에 포함되어 있는 PIN정보는 인출은행을 제외한 프로토콜 참여자 및 임의의 제삼자에게 노출되어지지 않는다.
- 인증 및 무결성 : 자금이체 메시지를 전송하기 위하여 고객은 자신의 개인키를 이용하여 메시지에 서명을 해야 한다. 자금이체 메시지를 수신한 은행들은 고객을 위한 개인키로 서명한 메시지를 수신함으로써 해당 고객을 인증할 수 있으며 무결성도 검사할 수 있다.
- 부인방지 : 자금이체 메시지에 대한 고객의 서명은 전자자금이체 거래 의뢰 사실 여부를 증명할 수 있는 부인방지 증거로서도 사용되어질 수 있다[9].
- 중복 재전송 방지 : 만약 공격자가 프로토콜 수행 상에서 습득한 정보를 이용하여 재 전송코자 한다면, 은행은 메시지 내에 있는 날짜 및 일련번호를 이용하여 기 수신한 메시지와의 중복 여부를 검출해 낼 수 있다.
- 영수증으로의 활용 : 은행에 의해 서명된 이체결과는 자금 수령인에 대해 자금이체결과에 대한 전자 영수증으로 활용될 수 있다. 수령자는 전자영수증을 은행의 공개키를 이용하여 검증할 수 있다.

V. 결론

본 논문에서 우리는 프로토콜 참여자들로 구성된 도메인 내에서만 복호화 및 검증이 가능한 상황에 적용될 수 있는 Domain-verifiable signcryption 기법을 제안하였다. 이 기법은 프로토콜의 각 참여자가 전체 트랜잭션 메시지 중 자신과 관련된 일부 메시지만을 복호화하고 전체 메시지에 대한 검증이 가능해야 하는 응용들에 사용되어질 수 있다.

우리는 Domain-verifiable signcryption의 적용 가능한 예로써 은행간 전자자금이체 프로토콜을 설계하였다. 이는 TTP의 개입 없이 거래 당사자들간에 거래가 완료되어질 수 있는 형태로 인터넷과 같은 개방형 네트워크에서도 사용되어질 수 있는 실세계 적용이 가능한 효율적인 방식으로 생각된다.

또 다른 적용 가능한 예로는 다중 계층 키 분배 및 SET 프로토콜에 적용이 가능

하다고 판단되며 자세한 설계를 위해서는 더욱 많은 연구가 필요하다.

참고문헌

[1] T.ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory, IT-31(4):469-472, 1985.

[2] C.P. Schnorr, Efficient identification and signature for smart cards, Advances in Cryptology-CRYPTO '89, LNCS 435, Springer-Verlag, pp. 239-251,1989.

[3] Y. Zheng, Digital signcryption or how to achieve cost(signature and encryption) << cost(signature)+cost(encryption), Advances Cryptology-CRYPTO'97, LNCS 1294, Springer-Verlag, pp. 165-179, 1997.

[4] F.Bao and R.H.Deng, A Signcryption Scheme with Signature Directly Verifiable by Public Key, Proc. of PKC'98, LNCS, Vol. 1431, Springer-Verlag, pp. 55-59, 1998.

[5] C.Gamage, J.Leiwo, and Y.Zheng, Encrypted Message Authentication by Firewalls, Proc. of PKC'99, LNCS, Vol. 1560, Springer-Verlag, pp. 69-81, 1999.

[6] Y. Zheng, Signcryption and its application in efficient public key solutions, Proc. of Information Security Workshop(ISW'97), LNCS, Vol. 1396, Springer-Verlag, pp. 291-312, 1998.

[7] Y.Zheng and H. Imai, Efficient Signcryption on Elliptic Curves, Proc. of the IFIP 14th International Information Security Conference (IFIP/SEC98), Chapman & Hall, Sep., 1998, Vienna, Austria.

[8] Electronic Funds Transfer Act (EFTA), 15 U.S.C. Sec. 1693.

[9] J. Zhou and D.Gollmann, Observation on Non-repudiation, Advances in Cryptology-ASIACRYPT'96, LNCS 1163, Springer-Verlag, pp. 133-144, 1996.

[10] Visa International and MasterCard International, Secure Electronic Transaction(SET) Specification book 1:Business Description, May 1997.