情報保護學會論文誌
第12券 第1號, 2002. 2

XTR 버전의 개인식별 프로토콜을 이용해 블랙메일링을 막는 실질적인 방법

한 동 국*, 박 혜 영*, 박 영 호*, 김 창 한**, 임 종 인*

A Practical Approach Defeating Blackmailing by using XTR-version Identification protocol

Dong-Guk Han*, Hye-Young Park*, Young-Ho Park*, Chang-Han Kim**, Jong-In Lim*

요 약

블라인드 서명을 기반으로 만든 전자화폐 시스템이 David Chaum에 의하여 처음으로 제안되었다. 그러나 von Solms과 Naccache는 블라인딩된 화폐는 블랙메일링 공격을 쉽게 허용한다는 것을 발견했다. 본 논문에서는 XTR을 이용해 Schnorr 개인식별 프로토콜을 구성하여 블랙메일링 공격이 있을 경우에 은행에게 블랙메일링 공격에 대한 정보를 개인식별 과정에서 알려주는 방법을 제안한다. 일반적으로 전자화폐가 가지는 여러 가지 문제점 중에서 블랙메일링이 가장 심각하다. 특히 고객을 납치한 상태에서의 블랙메일링은 전자화폐 시스템에 치명적인 결과를 가져오게 된다. 그러나 본 논문에서 제안한 XTR 버전의 Schnorr 개인식별 프로토콜을 사용하면 기존의 방법들이 블랙메일링 공격을 막기 위해 필요로 하는 가정들을 사용하지 않고도 효과적으로 블랙메일링 공격을 막을 수 있는 실질적인 방법이 된다.

ABSTRACT

Electronic cash system based on anonymous coins have been invented by David Chaum. However, von Solms and Naccache discovered that such anonymous coins also very well suited to support criminals in Blackmailing. In this paper, we suggest a method that a client informs a bank of the information about blackmailing attack by using Schnorr identification protocol of XTR version at the stage of identification, whenever he is blackmailed. In general, blackmailing is the most serious among the various drawbacks of electronic cash system. Especially, blackmailing to be done when the client is kidnapped brings a fatal result to electronic cash system. But if the Schnorr identification protocol of XTR version is used, we can efficiently defeat blackmailing without assumption required in the existing method to defeat blackmailing.

keyword : *Electronic cash system, identification protocol, XTR public key system*

Ⅰ. 서 론

인터넷과 전자상거래의 중요성이 부각되면서, 전자화폐는 활발한 연구분야가 되었다. David Chaum에 의하여 전자화폐의 확고한 틀을 형성하는 기본적인 암호학적 개념들이 소개되었다. 초기 전자화폐 시스템(electronic cash system)에서는 은행 또는 상점에 대한 안전성과 사용자에 대한 익명성(anonymity)을 동시에 부여할 수 없다고 생각되어 졌다. 그러나 공개키 암호 기술의 개발로 말미암아 정직한 구매자의

* 고려대학교 정보보호기술연구센터(CIST)({christa, hypark, youngho, jilim}@cist.korea.ac.kr)
** 세명대학교(chkim@venus.semyung.ac.kr)

익명성이 보장되는 새로운 전자화폐 시스템이 제안되기 시작했다. 여기서 정직한 구매자의 익명성이 보장된다는 것은 전자화폐의 지불장소, 지불과정에서의 물품 구입 내용, 구매자 식별정보가 어느 누구에 의해서도 추적될 수 없다는 것을 의미한다. 이런 목적으로 1983년에 David Chaum에 의하여 처음으로 통신상의 지불시스템에서 개인의 프라이버시를 보호하기 위해 블라인드 서명(blind signature)을 기반으로 한 익명지불 시스템(anonymous payment systems)이 제안되었다.[2~4] 그러나 1992년 von Solms와 Naccache에 의하여 이러한 무조건적인 익명(unconditional anonymity)은 화폐의 이중사용, 돈세탁, 돈약탈 등과 같은 범죄에 악용될 수 있음이 증명되었다.[11] 예를 들어 블랙메일러(blackmailer)가 피해자로부터 블라인드 서명을 이용하여 인출한 돈을 강제로 갈취하였을 경우에 블라인드 서명의 특성상 사후에 강제로 갈취된 돈에 대하여 은행이나 피해자는 확인이 불가능하게 된다. 더욱이 블랙메일러에 의하여 블랙메일된 돈이 관찰할 수 없는 통신 채널(anonymous channel)을 통하여 익명으로 전달될 경우에는 블랙메일러의 신분을 확인하거나 추적하는 것은 불가능하게 된다. 즉 완벽한 범죄(perfect crime)가 되는 것이다.

위에서 언급한 익명성을 보장함으로써 생기는 문제들을 개선한 여러 대안들이 제안되었다. 특별히 Kugler와 Vogt는 사용자의 익명성을 보장하면서 블랙메일링을 막는 방법을 제안하였다.[8] 그러나 [8]에서 블랙메일링 공격을 막기 위해서는 블랙메일링 공격이 있을 경우에 은행과 고객사이에 이루어지는 통신 내용-블랙메일링 공격을 받고 있다는 정보-을 블랙메일러가 알 수 없어야 한다는 가정이 필요하다.[8] 만약에 블랙메일러가 피해자를 납치(kidnapping)하여 블랙메일링 공격을 할 경우에는 피해자가 은행에게 블랙메일링 공격에 대한 정보를 줄 수 없게 된다. 따라서 피해자가 납치된 경우에는 위장된 채널(covert channel)의 존재를 가정하여 블랙메일링 공격에 대한 정보를 은행에게 전달하게 된다.[8] [8]에서 제안한 블랙메일링 공격을 막는 방법이 적용되려면 위에서 언급한 가정이 반드시 필요하다. 그러나 이런 가정이 필요하다는 것은 그 만큼 공격을 막는 것이 쉽지 않음을 의미한다.

본 논문에서는 현실적으로 쉽지 않은 가정을 바탕으로 제안된 블랙메일링 공격을 막는 방법 대신에 Schnorr 개인식별(identification) 프로토콜을 변형하여 만든 새로운 XTR 버전의 Schnorr 개인식별 프로토콜을 이용함으로써 인출과정 전에 필요한 개인식별 과정에서 블랙메일링 공격에 대한 정보를 은행에게 알려주는 방법을 제안한다. 특별히 납치나 신분 위장(impersonation)과 같은 공격에서는 은행과 피해자가 통신을 하는 것이 아니라 블랙메일러가 은행과 직접 통신을 하기 때문에 [8]에서 하는 가정이 없으면 블랙메일링 공격에 대한 정보를 은행에게 전달하기는 쉽지 않다.[8] 그러나 본 논문에서는 완벽한 범죄의 경우 개인식별 과정에서 100% 범죄 사실을 은행에게 알려 줄 수 있고, 신분 위장이나 납치와 같은 공격에 대해서도 2/3 확률로 개인식별 과정에서 블랙메일링 공격에 대한 정보를 은행에게 줄 수 있다. 즉 신분 위장이나 납치와 같은 공격에서 블랙메일러가 개인식별 과정을 정당한 사용자처럼 통과할 확률은 1/3이다. 따라서 블랙메일러는 신분 위장이나 납치와 같은 방법을 이용해 블랙메일링 공격을 할 경우 생기는 위험 부담이 크기 때문에 기존의 방법을 이용한 범죄는 급격히 감소할 것이다.

본 논문의 구성은 다음과 같다. 2절에서는 전자화폐 시스템에서 생기는 블랙메일링 공격을 막는 기존의 방법들을 살펴보고, 3절에서는 2절에서 살펴본 방법들을 개선하기 위하여 사용되는 XTR 공개키 시스템의 구성을 살펴본다.[9] 그리고 4절에서는 개선된 XTR-Schnorr 개인식별 프로토콜을 제안한다. 5절에서는 블랙메일링을 막는 실질적인 방법을 소개하고 마지막으로 6절에서는 결론을 살펴보도록 하겠다.

II. 기존의 블랙메일링 공격을 막는 방법들

전자화폐의 요구조건 중 특별히 익명성(anonymity)에 대한 중요성을 많이 강조한다. 초기에는 무조건적인 익명성을 제공함으로써 소비자의 익명성을 보장하였는데, 이것은 또한 공격의 빌미가 되기도 하였다. 따라서 블랙메일링, 돈세탁, 불법적 구매 등과 같은 전자화폐에서 생기는 문제도 해결하고, 또한 소비자의 익명성도 보장하기 위하여 나타난 새로운 방법이 취소 가능한 익명성(revokable anonymity)을 가진 전자화폐 시스템이다.[1,5,7] 이와 같은 전자화폐 시스템에서는 언제든지 사용자의 익명성을 취소할 능력을 가진 신뢰할 수 있는 제3의 기관(trusted third party)의 존재를 가정한다. 따라서 블랙메일링과 같은 불법적인 행동이 적발되었을 때에 신뢰할 수 있는 제3의 기관이 개입하여 돈의 추적과 사용자의

추적을 가능하게 함으로 전자화폐에서 생기는 여러 공격을 막을 수 있게 하였다. 그러나 만약에 신뢰할 수 있는 제3의 기관이 자신의 능력을 남용한다면, 정직한 사용자의 프라이버시, 즉 사용자의 익명성이 침해받을 수 있다는 문제를 갖게 된다. 이러한 문제를 해결하기 위하여 Kugler와 Vogt는 신뢰할 수 있는 제3의 기관의 존재를 배제하고, 사용자의 익명성은 제한하지 않으며, 취소 가능한 익명성을 가지는 온라인 전자화폐 시스템을 제안하였다.[8]

블랙메일링이 이루어지는 시나리오를 3가지 정도로 요약해 볼 수 있다.[8]

1) 완벽한 범죄(Perfect crime)

이것은 블랙메일러(blackmailer)가 피해자에게 익명채널(anonymous channel)을 통해 접근하여 자신에 의하여 선택되어지고 블라인딩된 화폐를 인출하도록 협박하는 것이다. 여기서 블랙메일러는 피해자와만 통신을 한다.

2) 신분 위장(Impersonation)

이것은 블랙메일러가 피해자의 은행 계좌에 대한 정보-신분확인에 쓰이는 개인키-를 얻어서 그 자신이 인출을 하는 것이다. 여기서는 블랙메일러가 자신이 은행 계좌의 주인인 것처럼 직접 은행과 통신을 한다.

3) 피해자를 납치(Kidnapping)

이것은 블랙메일러가 피해자를 육체적으로 제압하여 신분 위장과 유사한 방법으로 화폐를 인출하는 방법이다. 신분 위장과 마찬가지로 블랙메일러가 직접 은행과 통신을 한다.

[8]에서는 위 3가지 시나리오에 대한 공격을 막을 수 있는 방법을 제안했다.[8] 그것은 블라인드 부인 방지 서명(blind undeniable signature)을 이용하여 만든 새로운 온라인 전자화폐 시스템이다. [8]에서 제안한 전자화폐 시스템은 블랙메일링 공격이 있을 경우에 소비자의 요청에 의해 발급되어지는 화폐에 적당한 표시(marking)를 하는 것이다. 블랙메일러가 정당한 화폐와 표시가 이루어진 화폐를 구별하는 것은 불가능하게 되어 있다.
이 시스템이 가지는 몇 가지 장점이 있다.

첫째. 사용되지 않은 표시된 화폐에 대하여는 그 화폐 자체를 무효화시킬 수 있고, 소비자에게 그 만큼의 돈은 반환되어진다. 그러나 이미 사용된 표시된 돈(marked coins)에 대하여는 손실을 볼 수밖에 없다.

둘째. 모든 표시된 돈은 입금과정에서 효과적으로 찾아낼 수 있다. 이것은 블랙메일러 추적을 가능하게 한다.

셋째. 블랙메일링과 같은 범죄를 막기 위하여 화폐에 표시(marking)하는 방법은 정직한 사용자에 대해서 불법적으로 추적하는 것을 허용하지 않는다.

그러나 [8]에서 제시한 방법이 가능하기 위해서는 블랙메일링 공격이 있을 때에 소비자가 은행에게 블랙메일링 공격에 대한 정보를 주어야 한다는 것이다.[8] [8]에서는 이것을 해결하기 위하여 완벽한 범죄와 신분 위장과 같은 범죄에서는 피해자가 블랙메일링 공격을 당하고 있다는 정보를 블랙메일러가 알 수 없게 은행에게 줄 수 있다는 가정을 한다.[8] 그리고 납치 공격에서는 당연히 블랙메일러가 피해자와 은행사이의 연락을 하지 못하도록 강제적인 행동을 취하겠지만, 위장된 채널(covert channel)의 존재를 가정하고, [6]에서 언급한 distress 화폐시스템의 아이디어를 적용함으로써 은행과 피해자 사이에 블랙메일링 공격에 대한 정보를 주어야 하는 문제를 해결했다.[6]

우리는 [8]에서 3가지 블랙메일링 공격을 막는 시나리오에 대한 가정들이 대단히 강력함을 알 수 있다. 그리고 만약에 이런 가정이 성립하지 않을 경우에는 블랙메일링을 막을 수 있는 다른 방법이 없게 되므로 Kugler와 Vogt에 의하여 제안된 전자화폐 시스템에 치명적인 결함이 생기게 된다.

Ⅲ. XTR

이번 장에서는 XTR의 특성과 XTR-Schnorr 개인식별 프로토콜을 살펴보도록 하겠다. XTR 공개키 시스템을 살펴보기에 앞서, 유한체, $GF(p^2)$, $GF(p^6)$에서 몇 가지 용어에 대한 정의를 알아보도록 한다.

- conjugate : $h \in GF(p^6)$의 $GF(p^2)$ 위에서의 conjugates은 h, h^{p^2}, h^{p^4} 이다.
- trace : $h \in GF(p^6)$의 $GF(p^2)$ 위에서의 trace $Tr(h)$는 h의 $GF(p^2)$ 위에서의 conjuates의 합이다. 즉,

$$Tr(h) = h + h^{p^2} + h^{p^4} \in GF(p^2)$$

XTR은 유한체의 부분집합의 원소를 표현하고 그것의 지수승을 계산하는 데에 trace를 이용하는 방법이다. XTR은 $GF(p^6)$의 명확한 구성없이 $GF(p^6)$의 안전성을 가지면서 $GF(p^2)$의 연산을 사용하는 최초의 방법이다. XTR의 시스템 파라메터에 대해 살펴보자. $p \equiv 2 \pmod 3$을 만족하는 170비트 정도의 소수이며, q는 160비트 정도의 소수로 sixth cyclotomic polynomial $\Phi_6(p) = p^2 - p + 1$의 인수가 되게 잡는다. $g \in GF(p^6)$는 위수가 q인 원소이다. 여기서 XTR 부분군의 생성원으로서 $Tr(g)$를 사용한다. $GF(p^2)$의 원소들의 연산의 효율성을 위해, $GF(p)$상에서 $GF(p^2)$에 대한 최적정규기저를 사용하여 $GF(p^2)$의 원소들을 표현한다. $\{\alpha, \alpha^2\}$를 $GF(p)$상에서 $GF(p^2)$에 대한 최적정규기저라고 하자. 여기서 α와 α^2은 $(X^3-1)/(X-1) = X^2+X+1$의 근이 된다. 또한 $\alpha^i = \alpha^{i \pmod 3}$이므로 $GF(p^2)$는 다음과 같다.

$$GF(p^2) \cong \{x_1\alpha + x_2\alpha^2 : x_1, x_2 \in GF(p)\}$$

XTR은 다음과 같은 몇 가지 특징을 갖는다.

[정리 1]

위수가 q인 원소 $g \in GF(p^6)$에 대해, $Tr(g^i) = Tr(g^j)$는 g^i와 g^j가 $GF(p^2)$에서 conjugate이라는 것과 동치이다.

[증명]

($\Rightarrow$) 위수가 q인 원소 $g \in GF(p^6)$에 대해 $F(X) = X^3 - Tr(g^i)X^2 + Tr(g^i)^p X - 1 \in GF(p^2)[X]$는 $GF(p^2)$에서 기약 다항식이며 그것의 근들은 $GF(p^2)$에서 g^i의 conjugate이다. 즉, g^i, g^{ip^2}, g^{ip^4}이 $F(X)$의 근이 된다. $Tr(g^i) = Tr(g^j)$이기 때문에,

$$\begin{aligned} F(X) &= X^3 - Tr(g^i)X^2 + Tr(g^i)^p X - 1 \\ &= X^3 - Tr(g^j)X^2 + Tr(g^j)^p X - 1 \in GF(p^2)[x] \end{aligned}$$

가 된다. 따라서 g^j는 $F(X)$의 근이 된다. 그러므로 g^i와 g^j가 $GF(p^2)$에서 conjugate이다. ($\Leftarrow$) g^i와 g^j가 $GF(p^2)$에서 conjugate이므로, $g^i = g^j$, $g^i = g^{jp^2}$ 또는 $g^i = g^{jp^4}$이 된다. $h \in GF(p^6)$에 대해, $h^{p^6} = h$이므로 $Tr(g^i) = Tr(g^j)$를 만족하게 된다. □

[정리 2]

p와 q는 $q \mid (p^2 - p + 1)$을 만족하는 소수라고 하자. 만약 $g \in GF(p^6)$의 위수가 q 이면 부분군 $\langle g \rangle$는 $GF(p^6)$의 부분체 $GF(p)$ $GF(p^2)$ $GF(p^3)$에 속하지 않는다.[9]

암호 프로토콜에서 XTR의 응용은 안전성을 감소시키지 않으면서 통신량과 계산량 둘 다에 있어서 실질적인 감소를 가져다 준다. XTR은 부분군의 이산대수문제에 의존하는 암호시스템에 적용될 수 있다.

3.1 XTR-Schnorr 개인식별 프로토콜

이번 절에서는 XTR을 Schnorr 개인식별 프로토콜에 적용한 것을 살펴보겠다. 이 프로토콜을 XTR-Schnorr 개인식별 프로토콜이라고 부르도록 하자. 먼저 [그림 1]에서 보여주는 Schnorr 개인식별 프로토콜 대해 알아보자.

■ System Setup

1. 적당한 소수 p를 잡고 $p-1$을 나누는 q를 택한다.
2. 위수가 q인 원소 g를 선택한다.
   단, $1 \le g \le p-1$
3. 변수 t를 $2^t < q$가 되게 선택한다. 예를 $t \ge 40$이면 된다.

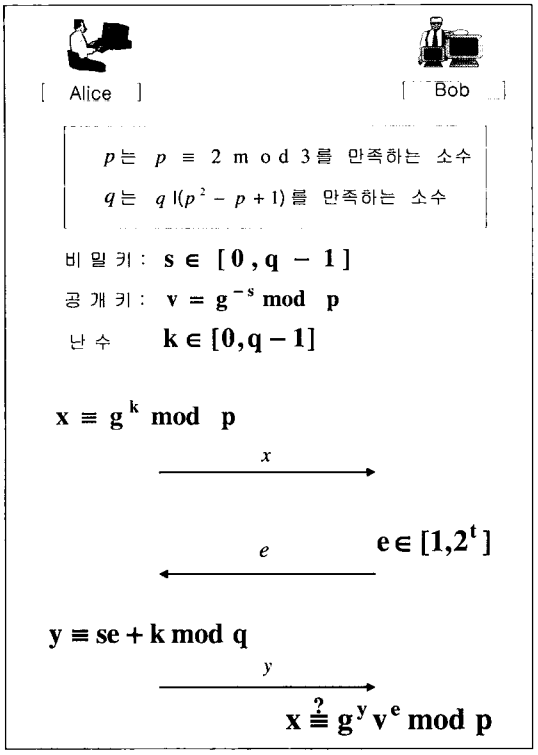
■ 사용자의 변수 선택

Alice의 개인키 : $s \in [0, q-1]$
Alice의 공개키 : $v \equiv g^{-s} \bmod p$

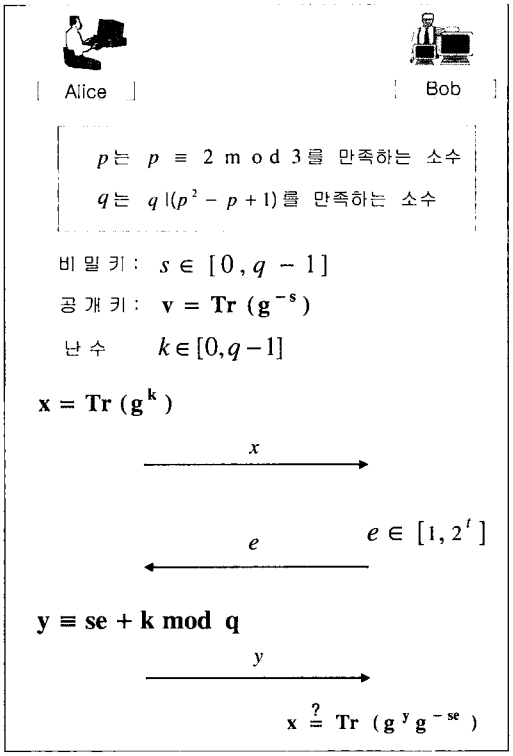
■ 프로토콜

1. Alice는 난수 k $0 \le k \le q-1$)를 선택하고 $x \equiv g^k \bmod p$를 계산한 후 x를 Bob에게 보낸다.
2. Bob은 Alice에게 난수 e를 보낸다. 여기서 e는 $1 \le e \le 2^t$을 만족하는 값이다.
3. Alice는 $1 \le e \le 2^t$를 확인하고 $y \equiv se + k \bmod q$를 계산하여 y를 Bob에게 보낸다.
4. Bob은 $z \equiv g^y v^e \bmod p$를 계산하여, $z = x$ 이면 Alice임을 확인하게 된다.

이제 [그림 2]에서 보여주는 XTR-Schnorr 개인식별 프로토콜을 살펴보자. 이 프로토콜은 [그림 1]에서 보였던 Schnorr 개인식별 프로토콜을 XTR 버전으로 전환한 것이다.



〔그림 1〕 Schnorr 개인식별 프로토콜



〔그림 2〕 XTR-Schnorr 개인식별 프로토콜

■ System Setup

XTR-Schnorr 개인식별 프로토콜에서 시스템 파라메터는 $q \mid (p^2-p+1)$를 만족하는 소수 p, q, t 그리 $Tr(g)$이다.

1. $p \equiv 2 \pmod 3$는 170비트 정도의 소수이며 q는 160비트 정도의 소수이다.
2. 위수가 q인 원소 $g \in GF(p^6)$에 대해 $Tr(g)$를 찾는다.
3. $2^t < q$인 변수 $t > 40$를 선택한다.

■ 사용자의 변수 선택

Alice의 개인키 : $s \in [0, q-1]$
Alice의 공개키 : $v = Tr(g^{-s})$

■ XTR-Schnorr 개인식별 프로토콜

1. Alice는 난수 $k\,(0 \le k \le q-1)$를 선택하고 $x = Tr(g^k)$를 계산한 후 x를 Bob에게 보낸다.
2. Bob은 Alice에게 난수 e를 보낸다. 여기서 e는 $1 \le e \le 2^t$을 만족하는 값이다.
3. Alice는 $1 \le e \le 2^t$를 확인하고 $y \equiv se + k \bmod q$를 계산하여 y를 Bob에게 보낸다.
4. Bob은 $z = Tr(g^y g^{-se})$를 계산하여, $z = x$이면 Alice임을 확인하게 된다.

Remark. $Tr(g^y g^{-se})$ $Tr(g)$, $v = Tr(g^{-s})$ 그리고 y, e에 기반 하여 알고리즘 2.4.8에 의해 계산된다.[9] 이때 Bob은 Alice의 비밀키 s를 모른다는 사실에 주목하자.[9,10]

Ⅳ. 개선된 XTR-Schnorr 개인식별 프로토콜

이번 장에서는 은행에게 블랙메일링에 대한 정보를 주기 위한 개선된 XTR-Schnorr 개인식별 프로토콜을 구성하고, 그 특징들에 대해 살펴보도록 한다. 다음의 시나리오에서 Alice는 자신의 신원을 은행에게 증명하기를 원한다. 전체적인 프로토콜은 〔그림 3〕 에 나타나 있다.

■ Advance Preparations

1. 은행의 비밀키 : b ($< q$)
   은행의 공개키 : $Tr(g^b)$

2. 사전에 사용자와 은행사이에 약속된 대칭키 알고리즘 E
3. Alice는 일반적인 과정에서 사용하는 응답의 크기를 은행과 약속해 놓는다.

■ System setup

개인식별 프로토콜에서 시스템 파라메터는 $q \mid (p^2-p+1)$를 만족하는 소수 p, q, $Tr(g)$ 그리고 t이다.

1. $p \equiv 2 \pmod 3$는 170비트 정도의 소수이며 q는 160비트 정도의 소수이다.
2. 위수가 q인 원소 $g \in GF(p^6)$에 대해 적당한 $Tr(g)$를 찾는다.
3. $2^t < q$인 변수 $t > 40$를 선택한다.

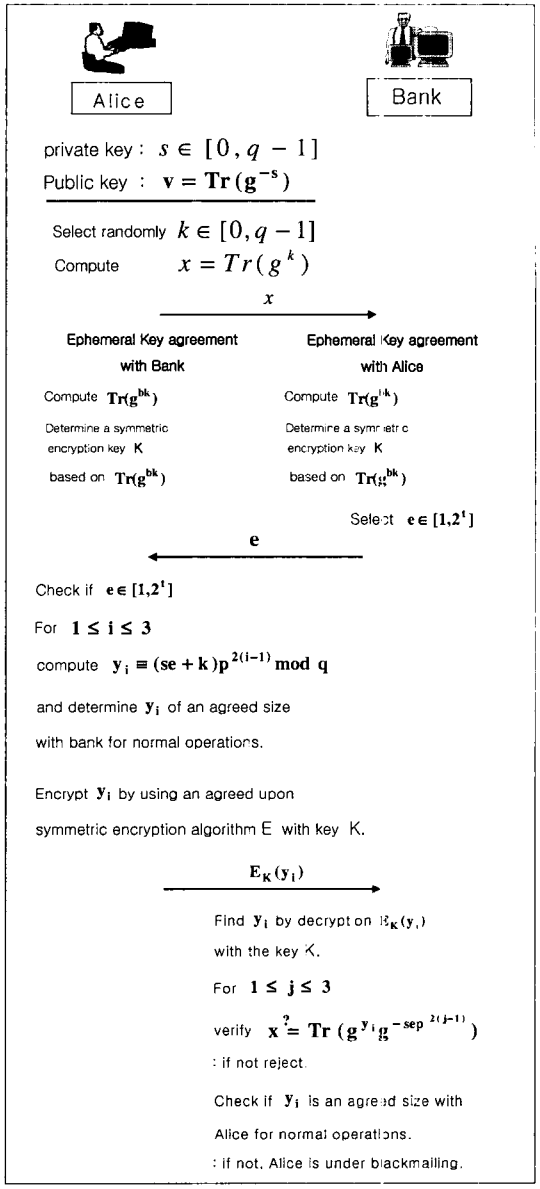
■ 사용자의 변수 선택

Alice의 개인키 : $s \in [0, q-1]$

Alice의 공개키 : $v = Tr(g^{-s})$

■ 개선된 XTR-Schnorr 개인식별 프로토콜

1. Alice는 난수 k $0 \le k \le q-1$)를 선택하고 $x = Tr(g^k)$를 계산한 후 x를 Bob에게 보낸다. Alice는 $Tr(g^{kb})$를 계산하고 $Tr(g^{kb})$에 기반하여 대칭키 알고리즘의 K를 결정한다.
   여기서 대칭키 알고리즘의 키 K를 결정방법은 사전에 은행과 고객사이에 약속된 방법을 이용한다. 예를 들어 K가 l 비트라고 하면, 340비트 길이를 갖는 $Tr(g^{kb})$로부터 최상위 l 비트를 K로 사용할 수 있다.
2. 은행 $Tr(g^{kb})$를 계산하고 마찬가 $Tr(g^{kb})$에 기반하여 대칭키 알고리즘의 키 K를 한다. 은행은 Alice에게 $1 \le e \le 2^t$인 난수 e를 보낸다.
3. Alice는 $1 \le e \le 2^t$를 확인하고 $y_1 \equiv (se+k) \bmod q$ $y_2 \equiv y_1 \cdot p^2 \bmod q$ 그리고 $y_3 \equiv y_1 \cdot p^4 \bmod q$을 계산한다. 이때, 만약 $y_1 = 0$이면 이 프로토콜을 끝내고 1.부터 다시 프로토콜을 시작한다(그러나 $y_1 = 0$일 확률은 $1/q$로써 무시할 정도로 작다). 만약 $y_1 \neq 0$이면 $1 \le i \le 3$에 대해, 일반적인 과정에서 사용하기로 은행과 약속 된 크기 y_i를 선택한다. 이 값을 공유된 비밀 K를 사용하여 사전에 약속된 대칭키 알고리즘 E로 암호화하여 $E_K(y_i)$을 은행에 전달한다.
4. 은행은 $E_K(y_i)$를 공유된 비밀키 K를 사용하여 복호화한 후 y_i를 구한다. $1 \le i \le 3$에 대해 $x = Tr(g^{y_i} g^{-sep^{2(i-1)}})$인지를 확인한다. 만약 이 값이 같지 않다면 개인식별과정을 통과하지 못한다.
   은행은 y_i가 일반적인 과정에서 사용하 Alice와 약속했던 크기인지 확인한다. 만약 y_i가 일반적인 과정에서 사용되는 크기의 값이 아니면 은행은 Alice가 블랙메일링 공격을 받고있다는 것을 의심하게 된다.



〔그림 3〕 개선된 XTR-Schnorr 개인식별 프로토콜

개선된 XTR-Schnorr 개인식별 프로토콜은 다음

과 같은 특징을 가진다.

[정리 3]

$y_1 \equiv (se+k) \bmod q$, $y_2 \equiv y_1 \cdot p^2 \bmod q$, $y_3 \equiv y_1 \cdot p^4 \bmod q$ 일 때, $1 \le i \le 3$에 대한 세 개의 y_i는 개선된 XTR-Schnorr 개인식별 프로토콜의 확인과정 4를 통과한다.

[증명]

만약 $y_1 \equiv (se+k) \bmod q$이 은행에 보내진다면, $i=1$인 경우에 다음을 만족한다. $Tr(g^{y_1} g^{-se \bmod q}) = Tr(g^{(se+k) \bmod q} g^{-se \bmod q}) = Tr(g^k) = x$이므로 $x = Tr(g^{y_1} g^{-se})$이 된다. 만약 $y_2 \equiv (se+k) \cdot p^2 \bmod q$가 은행에 보내진다면, $i=2$인 경우에 다음을 만족한다.

$Tr(g^{y_2} g^{-sep^2 \bmod q})$
$= Tr(g^{(se+k)p^2 \bmod q} g^{-sep^2 \bmod q})$
$= Tr(g^{kp^2})$이고 $x = Tr(g^{y_2} g^{-sep^2})$이 된다. 왜냐하면 [정리 1]에 의해, $Tr(g^{kp^2}) = Tr(g^k) = x$이기 때문이다.

만약 $y_3 \equiv (se+k) \cdot p^4 \bmod q$이 은행에 보내질 경우, $i=3$인 경우 다음을 만족한다. $Tr(g^{y_3} g^{-sep^4 \bmod q}) = Tr(g^{(se+k)p^4 \bmod q} g^{-sep^4 \bmod q}) = Tr(g^{kp^4})$이 므로 $x = Tr(g^{y_3} g^{-sep^4})$이 된다. 왜냐하면 [정리 1]에 의해, $Tr(g^{kp^4}) = Tr(g^k) = x$이기 때문이다. □

[보조정리1]

만약 $y_1 \neq 0$이면 y_1, y_2, y_3는 모두 다른 값이다. 즉 서로 다른 크기의 값이다.

[증명]

다음과 같은 세 가지 경우를 고려해 보자.

경우1)
만약 $y_1 = y_2$이면,
$se+k \equiv (se+k) \cdot p^2 \bmod q$이고
$(se+k) \cdot (p^2-1) \equiv 0 \bmod q$가 된다. 따라서
$se+k \equiv 0 \bmod q$ 또는 $p^2-1 \equiv 0 \bmod q$가 성립한다. 가정에 의해 $y_1 \neq 0$이므로 $p^2-1 \equiv 0 \bmod q$이다. 그러면 $g \in GF(p^2)$이 되어 [정리 2]에 모순이 된다. 따라서 $y_1 \neq y_2$ 이다.

경우2)
만약 $y_1 = y_3$이면,
$se+k \equiv (se+k) \cdot p^4 \bmod q$이고 $(se+k) \cdot (p^4-1) = (se+k) \cdot (p^2-1) \cdot (p^2+1) \equiv 0 \bmod q$가 된다. 따라서 $se+k \equiv 0 \bmod q$, $p^2-1 \equiv 0 \bmod q$ 또는 $p^2+1 \equiv 0 \bmod q$가 성립한다. 경우1에 의해 q는 p^2-1을 나누지 않고 가정에 의해 $y_1 \neq 0$이므로 $p^2+1 \equiv 0 \bmod q$이다. 그러나 $p^2-p+1 \equiv 0 \bmod q$이므로 $(p^2-p+1) - (p^2+1) = -p \equiv 0 \bmod q$가된다. 따라서 $q \mid p$가 되어 $q < p$와 p, q가 소수라는 것에 모순이 된다. 따라서 $y_1 \neq y_3$이다.

경우3)
만약 $y_2 = y_3$이면,
$(se+k) \cdot p^2 \equiv (se+k) \cdot p^4 \bmod q$이고
$(se+k) \cdot (p^4-p^2) = (se+k) \cdot (p^2-1) \cdot p^2 \equiv 0 \bmod q$가 된다.

따라서 $se+k \equiv 0 \bmod q$, $p^2-1 \equiv 0 \bmod q$ 또는 $p^2 \equiv 0 \bmod q$가 성립한다. 경우1에 의해 q는 p^2-1을 나누지 않고 가정에 의해 $y_1 \neq 0$이므로 $p^2 \equiv 0 \bmod q$이다. 그러나 p, q가 소수이므로 이것은 불가능하다. 따라서 $y_2 \neq y_3$ 이다. □

개선된 XTR-Schnorr 개인식별 프로토콜이 가지는 특징을 살펴보자.

1. 개선된 XTR-Schnorr 개인식별 프로토콜에서는 Alice가 전달하는 $x = Tr(g^k)$와 은행의 공개키 $Tr(g^b)$를 이용하여 임시적으로 사용하는 공유키를 생성한다.
2. 개선된 XTR-Schnorr 개인식별 프로토콜에서는 은행이 전달하는 하나의 시도값 e에 대하여 서로 다른 값을 가지는 세개의 응답값 $\{y_i\}$가 존재하고, 세개 모두는 Alice의 신분을 은행에게 확인시키는 과정을 통과한다.
3. 개선된 XTR-Schnorr 개인식별 프로토콜에서는 응답값 y_i을 전달할 경우에 대칭키 알고리즘을 사용하여 암호화하여 은행에게 전달한다.

개선된 XTR-Schnorr 개인식별 프로토콜에서 같은 시도값 e에 대해 서로 다른 세 개의 응답 $\{y_i\}$을 생성하는 특성을 사용해서, 피해자는 돈이 인출되기 전에 은행에게 블랙메일링을 알려줄 수 있어야 한다는 [8]에서의 특별한 가정 없이도 피해자가 블랙메일링에 대해 은행에게 알려줄 수 있는 방법을 제안한다.

V. 블랙메일링을 막는 실질적인 방법

[8]에서 블라인드 부인방지 서명에 기반 하여 사용자의 프라이버시를 보호하면서 블랙메일링을 막을 수 있는 지불시스템을 제안하였다.[8] 이 전자화폐 시스템은 전자화폐 시스템에서 일어나는 세 가지 블랙메일링 시나리오에 대하여 다음과 같은 특별한 가정을 필요로 한다.

- 가정: 완벽한 범죄, 신분 위장의 경우

블랙메일러는 완벽한 범죄나 신분 위장의 경우에 은행과 피해자 사이의 블랙메일링에 대한 통신을 알아챌 수 없어야한다.

- 가정 : 납치의 경우

은행에게 납치되었다는 것을 알려줄 수 있는 비밀 채널이 존재한다.

만약 피해자가 블랙메일링에 관한 정보를 항상 줄 수 있다면 [8]에서 제안한 전자화폐 지불 시스템은 실질적인 것이 된다. 그러나 정보를 줄 수 없다면 비현실적인 것이 된다. 이번 장에서는 개선된 XTR-Schnorr 개인식별 프로토콜을 사용하여 피해자가 다른 방법으로 은행과 통신을 할 수 없는 경우에도 블랙메일링을 막을 수 있는 실질적인 방법을 소개한다.

전자화폐시스템에서 구매자는 화폐의 인출 전에 개인식별과정을 거쳐야 한다. 이 과정에서 블랙메일링 공격에 처한 구매자의 상태를 은행과 통신을 할 수 있는 다른 방법이 없어도 은행에게 알려줄 수 있는 기법을 첨가한다. 이 방법은 개인식별 프로토콜이 전자화폐시스템의 기본적인 과정이기 때문에 어떠한 부가적이 가정도 필요로 하지 않는다. 이러한 제안에 대해 정리3에서 보였듯이 개인식별과정을 만족하는 세 개의 다른 응답 $\{y_i \mid 1 \le i \le 3\}$이 존재하는 특성을 가진 개선된 XTR-Schnorr 개인식별 프로토콜을 사용한다. 이 특성을 이용하기 위해서 사용자는 새로운 계좌를 열 때에 은행과 다음과 같은 약속을 하게된다. 개선된 XTR-Schnorr 개인식별 프로토콜에서는 정리3에서 살펴본 것과 같이 자신의 신분을 확인시키는데 필요한 응답이 서로 다른 크기를 가지는 세 개가 항상 존재함을 알 수 있다. 그러면 사용자는 이 세 개의 크기 중에서 일반적인 과정 -평상시-에서 사용하는 크기를 결정한다. 그러면 나머지 두 크기의 값은 블랙메일링의 경우에 사용하기로 한다. 예를 들어 한 사용자가 정당한 경우에 사용하는 크기를 서로 다른 세 개의 응답 $\{y_i\}$ 중에서 가장 큰 값이라고 은행과 사전에 정하였다고 하자. 그러면 만약에 사용자가 블랙메일링 공격을 당하고 있다는 정보를 은행에게 알려주고 싶다면 사용자는 세 개의 응답 중에서 중간 크기의 값이나 가장 작은 값을 사용하여 은행에게 보내게 되면 자신의 신분을 확인시키면서 또한 자신의 상태를 은행에게 알려줄 수 있게 된다. 은행으로부터 받은 시도값 e에 대한 선택된 응답값 y_i는 키 K로 사전에 약속된 대칭키 알고리즘 E를 이용하여 암호화한 $E_K(y_i)$를 은행에 보낸다. 그러면 위의 세 가지 블랙메일링 시나리오에 대해 특별한 가정 없이, 화폐가 인출되기 전에 블랙메일링에 대해 은행에 알려줄 수 있게 된다.

위에서 살펴보았듯이, 반드시 암호화된 y_i가 은행에 보내져야한다. 왜냐하면 암호화되지 않은 y_i가 보내질 경우 다음과 같은 문제가 발생하기 때문이다. 만약 y_i가 암호화되지 않고 보내진다면, 블랙메일러는 먼저 은행과 사용자사이의 일반적인 과정에서 전송되는 y_i를 관찰한 후 y_i $y_i \cdot p^2 \bmod q$ $y_i \cdot p^4 \bmod q$을 계산하여 이 값들의 크기를 비교할 수 있다. 따라서 블랙메일러는 일반적인 경우에서 사용되는 y_i의 크기를 알아낼 수 있다. 이것은 다음과 같이 증명된다.

1. y_1이 은행에 보내질 경우

이 경우 y_1, $y_2 \equiv y_1 \cdot p^2 \bmod q$, $y_3 \equiv y_1 \cdot p^4 \bmod q$의 크기를 비교하여 일반적인 과정에서 사용되는 y_1의 정확한 크기를 알 수 있다.

2. $y_2 \equiv y_1 \cdot p^2 \bmod q$가 은행에 보내질 경우

이 경우 $y_1 \cdot p^2 \bmod q$ $y_1 \cdot p^4 \bmod q$ $y_1 \cdot p^6 \bmod q$를 계산한다. $p^2 - p + 1 \equiv 0 \bmod q$이기 때문 $p^6 - 1 \equiv 0 \bmod q$이고 $y_1 \cdot p^6 \bmod q = y_1$이 된다. 따라서

$\{y_1 \cdot p^2 \bmod q, y_1 \cdot p^4 \bmod q, y_1 \cdot p^6 \bmod q\}$

$= \{y_1 \cdot p^2 \bmod q,\ y_1 \cdot p^4 \bmod q,\ y_1\}$

$= \{y_2, y_1, y_3\}$이다. 그러므로

$\{y_1 \cdot p^2 \bmod q, y_1 \cdot p^4 \bmod q, y_1 \cdot p^6 \bmod q\}$의 크기를 비교해 봄으로써 일반적인 과정에서 사용되는 y_2의 정확한 크기를 알 수 있다.

3. $y_3 \equiv y_1 \cdot p^4 \bmod q$가 은행에 보내질 경우

이 경우 $y_1 \cdot p^4 \bmod q$ $y_1 \cdot p^6 \bmod q$ $y_1 \cdot p^8 \bmod q$를 계산한다.

$p^6 \equiv 1$이고 $p^8 \equiv p^2 \bmod q$이므로 $y_1 \cdot p^6 \bmod q \equiv y_1$, 그리고 $y_1 \cdot p^8 \bmod q \equiv y_1 \cdot p^2 \bmod q$이다. 따라서

$\{y_1 \cdot p^4 \bmod q, y_1 \cdot p^6 \bmod q, y_1 \cdot p^8 \bmod q\}$

$= \{y_1 \cdot p^4 \bmod q,\ y_1,\ y_1 \cdot p^2 \bmod q\}$

$= \{y_3, y_1, y_2\}$이다. 그러므로

$\{y_1 \cdot p^4 \bmod q, y_1 \cdot p^6 \bmod q, y_1 \cdot p^8 \bmod q\}$의 크기를 비교해 봄으로써 일반적인 과정에서 사용되는 y_3의 정확한 크기를 알 수 있다.

5.1 블랙메일링에 관한 정보를 주는 방법

여기서는 개선된 XTR-Schnorr 개인식별 프로토콜을 사용하여 세 가지 블랙메일링 시나리오의 경우에 은행에게 블랙메일링에 대한 정보를 주는 방법을 살펴보도록 한다.

예를 들어 본 논문에서는 개선된 XTR-Schnorr 개인식별 프로토콜을 사용할 때에 자신의 신분을 확인시키는 과정에 필요한 응답값의 크기를 일반적인 경우에 가장 작은 값을 사용하도록 하고, 중간 크기의 값과 가장 큰 값은 블랙메일링의 경우에 사용하도록 약속되었다고 가정한다.

5.1.1 완벽한 범죄를 막는 방법

완벽한 범죄의 경우 블랙메일러는 피해자와만 통신을 한다. 블랙메일러가 익명채널을 통해 피해자와 접촉하여 화폐를 인출하도록 협박할 때, 피해자는 돈을 인출하기 위해 개선된 XTR-Schnorr 개인식별 프로토콜을 통하여 은행에게 자신의 신분을 증명해야만 한다. 이 때 사용되어지는 서로 다른 크기를 가지는 세 개의 응답 중에서 중간 값이나 가장 큰 값을 사용함으로써 범죄의 정보를 은행에 줄 수 있다. 따라서 피해자는 화폐인출 전에 항상 은행에게 블랙메일링을 알려 줄 수 있다.

5.1.2 신분 위장이나 납치를 막는 방법

신분 위장이나 납치의 경우 블랙메일러는 그의 신분을 위장하여 화폐인출과정 뿐만 아니라 개인식별 프로토콜에도 은행과 직접 통신하게 된다. 납치의 경우 피해자의 비밀키 s는 블랙메일러에게 쉽게 드러나게 된다. 왜냐하면 만약 피해자가 블랙메일러에게 잘못된 개인키를 알려준다면 블랙메일러는 개인식별 프로토콜과정에서 즉시 그 결과를 알게된다. 이것은 피해자에게 치명적인 결과를 초래할 수 있으므로 잘못된 키를 알려주는 것은 쉽지 않다. 그러나 정확한 피해자의 비밀키 s를 알아도 응답으로 보내어지는 값의 크기를 알지 못하게 되면 서로 다른 크기를 가지는 y_i중에서 임의로 선택할 수밖에 없다. 응답의 크기는 비밀키와는 달라서 피해자가 블랙메일러의 협박을 받고 잘못된 정보를 주어도 블랙메일러는 그것을 확인할 방법이 없게 된다. 따라서 블랙메일러는 세 개의 응답 중 한 값을 선택하지 않을 수 없다. 그러나 세 값들 중에서 가장 작은 값을 택할 확률은 1/3이 되므로 블랙메일러가 은행에게 블랙메일링의 정보를 알려주는 위험이 비교적 높다. 결과적으로 사용자의 비밀키 s가 드러난다 할지라도 공격은 2/3의 확률로 은행에 알려지게 된다. 여기서 2/3의 확률이 의미하는 것은 블랙메일러가 은행으로부터 인출 받은 전자화폐가 표시된 돈(marked coins)일 확률이다. 즉 사후에 표시된 돈을 사용함으로 인해 추적되어 검거될 확률이 2/3이라는 것이다. 따라서 성공적인 공격을 하는 것이 어렵게 되고 블랙메일러는 이와 같은 공격을 피하게 된다.

5.2 개선된 XTR-Schnorr 개인식별프로토콜의 안전성

이번 절에서는 개선된 XTR-Schnorr 개인식별 프로토콜의 안전성을 세 가지 관점에서 분석한다.

- 위조의 확률 : 이 프로토콜에서는 Schnorr 개인식별 프로토콜에서처럼 시도값 e를 정확하게 추측할 확률인 2^{-t}이 무시할 만하게 작게 하기 위해서 t값은 충분히 커야한다. 시도값 e을 정확하게 추측하는 것은 공격자가 Alice로 가장하는 것을 가능하게 한다. 왜냐하면 공격자는 임의로 선택한 y로 $x = Tr(g^y g^{-se})$을 은행에게 보내고, 다시 시도값 e에 대한 응답값으로 y을 보냄으로 Alice의 정확한 개인키 s를 모르고도 신분위장이 가능하다. 그러나 기존의 Schnorr 개인식별 프로토콜에서는 시도값 e의 추측이 신분위장을 가능하게 하지만 본 논문에서 제안한 개선된 XTR-Schnorr 개인식별 프로토콜에서는 시도값 e을 정확하게 추측하는 것이 Alice의 신분 위장을 가능하게 하지 않는다. 왜냐하면 Alice의 개인키 s에 대한 정보

없이도 신분확인 과정을 통과하는 y_i는 생성할 수 있지만 일반적인 과정에서 사용하는 y_i의 크기는 알 수 없기 때문이다. 따라서 기존의 Schnorr 개인식별 프로토콜보다 좀 더 안전하다.

- Soundness : 이 프로토콜은 일반적인 과정에서 사용되는 응답값 y_i의 크기와 s를 안다는 것을 증명하는 것으로 볼 수 있다. 즉, Alice처럼 프로토콜을 제대로 수행하고자하는 공격자는 s와 일반적인 과정에서 사용하는 y_i의 크기를 알아야 계산을 할 수 있다. 그러나 대칭키 알고리즘을 사용하여 y_i가 암호화되어 보내지므로 대칭키 알고리즘의 키 K를 모르고는 y_i와 그것의 크기를 알 수가 없게 된다. 또한 공격자가 비밀키 s를 알게 되어도 각 개인식별 프로토콜에서 사용된 난수 k를 알 수가 없기 때문에 공유된 비밀키 K를 찾아낼 수 없다. 그러므로 이 프로토콜에서 y_i의 크기의 안전성은 대칭키 암호 알고리즘에 의존한다. $K = Tr(g^{kb})$를 알기 위해 공격자는 b또는 k를 알아야 한다. 그러나 $Tr(g^k)$, $Tr(g^b)$로부터 b 또 k를 찾는 것은 이산대수문제를 푸는 것만큼 어렵다. 그러므로 일반적인 경우에 사용되는 y_i의 크기를 계산하는 것은 이산대수문제를 푸는 것만큼 어렵다.
- Forward secrecy : 이 프로토콜에서 Alice의 개인키는 s이고 Alice와 은행 사이에 만들어진 세션키 $Tr(g^{kb})$이다. 세션키는 Alice의 개인키 s와는 독립이기 때문에 세션키 $Tr(g^{ib})$는 사후에 Alice의 개인키가 노출이 된다고 할지라도 노출되지 않게 된다. 그러나 세션키 $Tr(g^{kb})$는 사후에 은행의 개인키 b가 노출이 된다면 드러나게 된다. 공격자가 b와 $Tr(g^k)$를 안다 $Tr(g^{kb})$를 쉽게 계산을 할 수 있기 때문이다.

Ⅵ. 결 론

지금까지 본 논문에서는 개선된 XTR-Schnorr 개인식별 프로토콜을 이용하여 PKC'01에서 Kugler와 Vogt에 의해 제안된 블랙메일링을 막는 온라인 전자화폐시스템을 보완한 실질적인 방법을 살펴보았다. 제안된 프로토콜은 사용자의 프라이버시를 보장하면서 블랙메일링을 막을 수 있는 Kugler와 Vogt에 의하여 제안된 지불시스템을 실질적이지 않은 가정 없이도 사용할 수 있게 해 준다. 그러므로 지불시스템에서 개선된 XTR-Schnorr 개인식별 프로토콜을 사용하면 비현실적인 가정 없이도 Kugler와 Vogt이 제안한 지불시스템에서 발생하는 블랙메일링 범죄를 현저하게 감소시킬 수 있다. 본 논문에서는 신분 위장이나 납치와 같은 공격이서는 2/3의 확률로 블랙메일링에 대한 정보를 피해자가 은행에게 전달할 수 있었다. 앞으로의 연구 방향은 이 확률을 좀더 높여 블랙메일링 공격에 대하여 좀더 효율적인 알고리즘을 개발하는 것이다.

참 고 문 헌

[1] J. Camenisch, U. Mauer, and M. Stadler. Digital payment systems with passive anonymity-revoking trustees. *In Computer Security-ESORICS '96*, volume 1146 of Lecture Notes in Computer Scienc, pp. 31~43. Springer-Verlag, 1996.

[2] D.Chaum. Blind signature for untraceable payments. *In Advances in Cryptology-CRYPTO '82*, pp. 199~203, Plenum,1 983.

[3] D. Chaum. Security Without Identification: Transaction Systems to Make Big Brother Obsolete. *Communications of the ACM 28*, 10, October 1985.

[4] D. Chaum. Privacy Protected Payments: Unconditional Payer And/Or Payee Untraceability. *In Smartcard 2000*, pp. 69~93, 1989.

[5] G.Davida, Y.Frankel, Y.Tsiounis, M. Yung, "Anonymity Control in E-Cash Systems", *Proceedings of Financial Cryptography Workshop, February, (1997)*, 15 pages.

[6] G. Davide, Y, Tsiounis, and M. Young. Anonymity control in e-cash systems. *In Financial Cryptography '97*, volume 1318 of Lecture Notes in Computer Science, pages 1-16. Springer-Verlag, 1997.

[7] M. Jakobsson and J. Muller. Improved magic ink signatures using hints. *In Financia lCryptography: Third International Conference, FC '98*, Anguilla, British West Indies, 1999. Springer-Verlag.

[8] D. Kugler and H. Vogt. Marking: A Privacy Protecting Approach Against

Blackmailing, *Proceedings PKC 2001*, LNCS 1992, Springer-Verlag, 2001, 137-152.

[9] A.K. Lenstra, E.R. Verheul, The XTR public key system, *Proceedings of Crypto 2000*, LNCS 1880, Springer-Verlag, 2000, 1-19; available from www.ecstr.com.

[10] A.K. Lenstra, E.R. Verheul, Key improvements to XTR, *Proceeding of Asiacrypt 2000*, LNCS 1976, Springer-Verlag, 2000, 220-233; available from www.ecstr.com.

[11] B. von Solms and D.Naccache. On blind signatures and perfect crimes. *Computers and Security*, 11(6): 581-583, 1992.

〈著者紹介〉

한 동 국 (Dong-Guk Han) 정회원
1999년 2월 : 고려대학교 수학과 학사
1999년 3월~현재 : 고려대학교 수학과 석사 과정
〈관심분야〉 정수론, 공개키 암호 ,CMVP

박 혜 영 (Hye-Young Park)
2001년 2월 : 고려대학교 수학과 학사
2001년 3월~현재 : 고려대학교 정보보호대학원 석사 과정
〈관심분야〉 정수론, 공개키 암호, 암호 프로토콜

박 영 호 (Young-Ho Park) 정회원
1990년 2월 : 고려대학교 수학과 학사
1993년 2월 : 고려대학교 수학과 석사
1997년 2월 : 고려대학교 수학과 박사
2001년~현재 : 고려대 정보보호기술연구센터 객원조교수
〈관심분야〉 정수론, 공개키 암호, 암호 프로토콜

김 창 한 (Chang-Han Kim) 정회원
1985년 2월 : 고려대학교 수학과 학사
1987년 2월 : 고려대학교 수학과 석사
1992년 2월 : 고려대학교 수학과 박사
2000년 2월~현재 : 세명대학교 컴퓨터수리정보학과 부교수
〈관심분야〉 정수론, 공개키 암호, 암호 프로토콜

임 종 인 (Jong-in Lim) 정회원
1980년 2월 : 고려대학교 수학과 학사
1982년 2월 : 고려대학교 수학과 석사
1986년 2월 : 고려대학교 수학과 박사
1999년 2월~현재 : 고려대학교 자연과학대학 정교수, 한국통신정보보호학회 편집위원장
고려대학교 정보보호대학원 원장, 고려대학교 정보보호기술연구센터 센터장
〈관심분야〉 블록 암호 및 스트림 암호의 분석 및 설계, 암호 프로토콜, 공개키 암호 분석