전자화폐 시스템에서 블랙메일링 공격을 막는 새로운 방법

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

*정보보호기술연구센터, **세명대학교

New Method of Protecting Against Blackmailing in Electronic Cash System

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

*Center for Information Security Technologies, **Semyung Univ

요 약

본 논문에서는 XTR을 이용해 Schnorr 개인식별 프로토콜을 구성하여 블랙메일링 공격이 있을 경우에 은행에게 블랙메일링 공격에 대한 정보를 개인식별 과정에서 알려주는 방법을 제안한다. 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 새로운 방법이 된다.

Ⅰ. 서론

1983년에 David Chaum[1]에 의하여 처음으로 통신상의 지불시스템에서 개인의 프라이버시를 보호하기 위해 블라인드 서명(Blind signature)을 기반으로 한 익명지불 시스템(anonymous payment systems)이 제안되었다. 그러나 1992년 B.v Solms 과 D.Naccache[2]에 의하여 이러한 무조건적인 익명(unconditonal anonymity)은 화폐의 이중사용, 돈세탁, 돈약탈 등과 같은 범죄에 악용될 수 있음이 증명되었다. 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 블랙메일러에 대한 신분을 확인하거나 추적하는 것은 불가능하게 된다. 즉 완벽한 범죄(Perfect crime)가 되는 것이다.

그러나 블랙메일링, 돈세탁, 불법적 구매 등과 같은 전자화폐에서 생기는 문제도 해결하고, 또한 소비자의 익명성도 보장하기 위해 나타난 새로운 방법인 취소가능한 익명성(revokable anony -mity)을 가진 전자화폐 시스템[3]이 제안되었다. 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 했다. 그러나 만약에 신뢰할 수 있는 제3의 기관이 자신의 능력을 남용한다면, 정직한 사용자의 프라이버시 즉 사용자의 익명성이 침

해받을 수 있다는 문제를 가지고 있다. 이러한 문제를 해결하기 위하여 [6]에서는 신뢰할 수 있는 제3의 기관의 존재를 배제하고, 사용자의 익명성은 제한하지 않으며, 취소 가능한 익명성의 성질을 가지는 블라인드 부인방지 서명(blind undeniable signature)을 이용하여 만들어진 온라인 전자화폐 시스템을 제안했다.

전자화폐 시스템에서 생길수 있는 블랙메일링 공격 시나리오를 다음과 같이 3 가지 정도로 요약해 볼 수 있다.

- **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.
- **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.
- **피해자를 납치(Kidnapping)**
  이것은 블랙메일러가 피해자를 육체적으로 제압하여 신분 위장과 유사한 방법으로 화폐를 인출하는 방법이다. 신분위장과 마찬가지로 블랙메일러가 직접 은행과 통신을 한다.

[6]에서는 위 3가지 시나리오에 대한 공격을 막을 수 있는 방법을 제안했다.

그러나 [6]에서 제시한 방법이 가능하기 위해서는 블랙메일링 공격이 있을 때에 소비자가 은행에게 블랙메일링 공격에 대한 정보를 주어야 한다는 것이다. [6]에서는 이것을 해결하기 위하여 완벽한 범죄와 신분 위장과 같은 범죄에서는 피해자가 블랙메일링 공격을 당하고 있다는 정보를 블랙메일러 가 알 수 없게 은행에게 줄 수 있다는 가정을 한다. 그리고 납치 공격에서는 당연히 블랙메일러가 피해자와 은행사이의 연락을 하지 못하도록 강제적인 행동을 취하겠지만, 위장된 채널(covert channel)의 존재를 가정하고, [4]에서 언급한 distress 화폐시스템의 아이디어를 적용함으로 은행과 피해자 사이에 블랙메일링 공격에 대한 정보를 주어야 하는 문제를 해결했다.

우리는 [6]에서 3가지 블랙메일링 공격을 막는 시나리오에 대한 가정들이 대단히 강력함을 알 수 있다. 그리고 만약에 이런 가정이 성립되지 않을 경우에는 블랙메일링을 막을 수 있는 다른 방법이 없게 됨으로 전자화폐 시스템에 치명적인 결함이 생기게 된다.

II. 전자화폐 시스템에서 블랙메일링 공격을 막는 새로운 방법

[6]에서 3가지 블랙메일링 공격 즉 완벽한 범죄, 신분 위장, 납치와 같은 공격에 대한 해결 방법을 제안하면서 두가지 가정을 하였다. 완벽한 범죄와 신분 위장과 같은 공격에 대해서 은행과 블랙메일링을 당하는 피해자가 갖는 통신을 블랙메일러는 알아챌 수 없어야 한다는 것이다. 그리고 피해자를 납치하는 공격에 대해서는 피해자가 직접 은행에게 블랙메일링을 당한다는 정보를 알려줄 수는 없지만 위장된 채널의 존재를 가정함으로 문제를 해결하려 하였다.

본 논문에서는 위의 3가지 공격에 대하여 [6]에서 제안한 은행과 블랙메일링 공격을 당하는 피해자사이의 통신을 블랙메일러가 관찰할 수 없다는 가정을 하지 않는다. 즉 만약의 경우에 피해자가 은행에게 블랙메일을 당한다는 정보를 항상 알려줄 수 있으면 문제가 없지만, 그렇지 않은 경우에는 [6]에서 제안한 방법은 의미가 없게 된다. 따라서 본 논문에서는 만약 피해자가 은행에게 블랙메일링 공격을 받고 있다는 정보를 다른 통신을 통하여 주지 못한다 하더라도 자연스럽게 블랙메일링 공격을 당한다는 정보를 은행에게 전달할 수 있는 방법을 제안한다. 중심 되는 아이디어를 요약하면 다음과 같다.

전자화폐 시스템에서 고객이 은행과 거래를 시작하기 위해서는 개인식별(identification)하는 과정을 반드시 거쳐야 한다. 개인식별 과정중에 고객은 자신의 상태 즉 블랙메일링 공격을 당하고 있다는 정보를 개인식별 프로토콜을 통하여 알려주는 것이다. 이 과정은 모든 전자화폐 시스템에서 기본적으로 이루어져야 하는 과정이므로 특별한 부가적인 가정이 필요하지 않다는 장점을 가지고 있다. 예를 들어 Schnorr 개인식별 프로토콜을 이용하여 개인의 신분을 인증받는다고 가정을 하면, 정확하게 자신의 개인키를 알고 있는 사람만이 상대에게 자신의 신분을 확인 시켜줄 수 있다. 그러나 XTR을 이용하여 Schnorr 개인별 프로토콜을 구성하면 개인 식별 프로토콜을 성사시키는 값이 하나만 있는 것이 아니라 3개의 서로 다른 크기의 값이 생긴다. 사전에 은행과 이 3개의 정보 중에서 원하는 크기를 결정하여, 아무 문제가 없을 때에 그 크기의 값을 사용하도록 약속하고, 나머지 2개의 값은 블랙메일링 공격을 당할 경우 사용하는 정보로 약속하게 되면 [6]에서의 가정 없이도 높은 확률로 블랙메일링 공격을 막을 수 있게 된다.

1 XTR-version Schnorr 개인식별 프로토콜

XTR을 기존의 Schnorr 개인식별 프로토콜에 적용하여 Alice가 은행에게 자신의 신분을 확인시키는

과정을 다음과 같이 구성한다.

사전 정보 : ▸ 은행의 공개키를 $Tr(g^b)$, 개인키를 b ($< q$) 라 가정한다.
▸ 은행과 고객사이에 사용하기로 약속된 대칭키 알고리즘이 있다.

1) 시스템 파라메터를 선택

(가) 소수 p 는 170 비트 정도로 $p \equiv 2 \bmod 3$ 를 만족하고 , q 는 160 비트 보다 크거나 같은 소수 중에서 $q \mid p^2-p+1$를 만족하는 것으로 선택한다.

(나) 위수가 q 인 g 에 대한 $Tr(g)$ 를 선택한다.

(다) $2^t < q$ 인 40보다 큰 t 를 선택한다.

2) Alice의 파라메터 선택

$[0, q-1]$ 사이의 값 s를 선택하여 개인키로 하고, 공개키는 $v = Tr(g^{-s})$ 로 한다.

3) 프로토콜

(가) Alice는 $[0, q-1]$ 사이의 값 중에서 랜덤하게 k 를 선택하여 $x = Tr(g^k)$ 를 계산하여 은행에게 전달한다.

▸ 은행과 Alice 사이의 키공유

Alice는 은행의 공개키 $Tr(g^b)$ 와 자신의 $x = Tr(g^k)$ 로 은행과 공유키 $K = Tr(g^{kb})$ 를 만들어 은행과 약속된 알려진 대칭키 알고리즘의 비밀키로 사용한다.

(나) 은행은 $[1, 2^t]$ 사이의 e 를 선택하여 Alice에게 보낸다.

(다) $1 \le i \le 3$ 에 대하여 $y_i = (se+k)p^{2(i-1)} \bmod q$ 를 계산하여 3개의 서로 다른 $y_i = y_1 p^{2(i-1)} \bmod q$ 들 중에서 사전에 은행과 약속된 크기의 값을 결정한다. 그리고 은행과 공유하고 있는 비밀키 K 로 은행과 약속된 대칭키 알고리즘 E 을 사용하여 암호화한 $E_K(y_i)$ 을 은행에 전달한다.

(라) 은행은 공유키 K 로 $E_K(y_i)$ 를 복호화 하여 y_i 를 찾아낸다. 그리고 주어진 $Tr(g)$ 와 $Tr(g^{-s})$ 를 이용하여 $x = Tr(g^{y_i} g^{-sep^{2(j-1)}})$ 를 $1 \le j \le 3$ 에 대하여 검증한다. 검증된 y_i 의 값과 $y_i \cdot p^2 \bmod q$, $y_i \cdot p^4 \bmod q$ 값을 비교하여 사전에 소비자와 약속된 크기의 값인지 확인한다. 만약 약속된 크기의 값이 아니면 정당한 사용자가 아닌 블랙메일러가 신분을 위장한 것이 된다.

XTR 버전의 개인식별 프로토콜의 3)의 (다),(라) 과정이 정확한지 살펴보자.

정리 1. 단계 3의 (다) 에서 서로 다른 3개의 $\{y_i \mid y_i = (se+k)p^{2(i-1)} \bmod q,\ 1 \le i \le 3\}$ 값 중 어떤 값이 사용되어도 개인 식별 과정의 검증 (라)을 통과한다.

[증명.] 만약 $y_1 = (se+k) \bmod q$ 를 은행에게 전달하였다면 (라)의 과정에서 $j=1$ 인 경우가 성립하게 된다. 즉 $Tr(g^{y_1} g^{-se \bmod q})$
$= Tr(g^{(se+k) \bmod q} g^{-se \bmod q}) = Tr(g^k) = x.$
만약 $y_2 = (se+k)p^2 \bmod q$ 를 은행에게 전달하였다면 (라)의 과정에서 $j=2$ 인 경우가 성립하게 된다. 즉

$Tr(g^{y_2} g^{-sep^2})$
$= Tr(g^{(se+k)p^2 \bmod q} g^{-sep^2 \bmod q}).$
$= Tr(g^{kp^2}) = Tr(g^k) = x.$

y_3 인 경우도 위와 동일하게 증명가능하다. □

신분위장과 납치와 같은 공격에서는 블랙메일러가 피해자의 개인키 s 를 안다고 할 수 있다. 그리고 기존의 개인식별 프로토콜에서는 피해자의 개인키가 노출되면 개인식별 과정에서 쉽게 신분위장이 가능하게 된다. 그러나 XTR 버전의 개인식별 프로토콜을 사용하면 피해자의 개인키를 아는 블랙메일러가 은행과의 개인식별 과정에서 정확하게 피해자로 신분을 위장할 확률은 1/3 이다.

정리 2. Alice의 개인키 s 를 아는 공격자가 y_i 를 생성하여 Alice로 신분을 위장할 수 있을 확률은 1/3 이다.

[증명.] Alice의 개인키 s 를 아는 공격자는 자신이 Alice 인 것처럼 은행과 개인식별 프로토콜을 시작하여 임의로 생성한 x를 은행에게 전달하고, 은행이 생성한 e를 받아 y_i를 계산할 수 있다. 그러나 공격자가 생성한 3개의 y_i , $y_i \cdot p^2 \bmod q$, $y_i \cdot p^4 \bmod q$ 중에서 어떤 크기의 값을 Alice가 사용하는지 공격자는 알 수 없다. 따라서 결국 공격자는 임의로 3개의 크기를 가지는 y_i 중에서 하나를 택하는 방법 밖에 없기 때문에 정확하게 Alice로 신

분을 위장할 확률은 1/3이 된다. □

위 프로토콜에서 y_i 를 암호화해서 보내는 이유는 다음과 같다. 서로 다른 크기의 y_i 를 사용함으로 개인식별 과정에서 블랙메일링 공격을 효과적으로 은행에게 알려 줄 수 있다. 그러나 만약에 y_i 를 그대로 은행에게 전달한다면 블랙메일러는 y_i, $y_i \cdot p^2 \bmod q$, $y_i \cdot p^4 \bmod q$ 을 계산하여 비교함으로 실제로 정당한 거래에 사용하는 y_i 의 크기를 알아낼 수가 있다. 그러면 신분 위장이나 납치와 같은 공격에서는 블랙메일러가 쉽게 정당한 사용자처럼 개인식별 프로토콜을 통과하게 된다.

그러므로 전달되어지는 y_i 의 크기가 노출되면 신분 위장이나 납치 공격에서 블랙메일러는 쉽게 정당한 사용자처럼 개인식별 프로토콜을 통과하게 되고 은행에게 블랙메일링 공격에 대한 정보를 줄 수 없게 된다.

2. XTR 버전의 Schnorr 개인식별 프로토콜를 이용해 블랙메일링 공격을 효과적으로 막는 방법

여기서는 블랙메일링 공격 시나리오 3개에 대해 XTR-version Schnorr 개인식별 프로토콜을 이용 어떻게 블랙메일링 공격에 대한 정보를 은행에게 전달할 수 있는지 자세히 살펴보도록 한다.

사전에 은행과 XTR-version Schnorr 개인식별 프로토콜 3)의 (다)단계에서 생기는 3개의 y_i 중에 평상시에 쓰는 y_i 의 크기와 블랙메일링 공격과 같은 경우에 쓰는 크기를 약속한다. 예를 들어 본 논문에서는 정상적인 거래에서는 가장 작은 값을 쓰고, 블랙메일링 공격이 있을 경우에는 중간 값이나 가장 큰 값을 쓰기로 약속한다.

가) 완벽한 범죄(Perfect crime)를 막는 방법

완벽한 범죄에서 블랙메일러는 피해자와만 통신을 하게된다. 완벽한 범죄를 막기 위하여 [6]에서는 블랙메일링 공격을 당하는 피해자가 은행에게 블랙메일링 공격을 당한다는 정보를 블랙메일러 몰래 알림으로써 인출과정에서 표시된 화폐를 은행이 발급할 수 있도록 하였다. 완벽한 범죄에서는 인출과정에서 은행과 블랙메일링 공격을 당하는 피해자와의 통신이 이루어지고 있기 때문에 피해자는 개인식별 프로토콜을 통하여 자신의 신분을 확인시킬 때에 블랙메일링 공격을 당한다는 정보를 줌으로써 인출되는 화폐에 은행이 표시하는 것을 가능하게 한다.

그러면 XTR-version Schnorr 개인식별 프로토콜을 이용하여 어떻게 블랙메일링 공격에 대한 정보를 줄 수 있는지 살펴보자.

완벽한 범죄와 같은 방법으로 블랙메일링 공격을 하려고 하는 블랙메일러가 피해자에게 익명의 통신채널을 통하여 접근하여 협박을 할 경우, 피해자는 먼저 개인식별 프로토콜을 통하여 자신의 신분을 은행에 검증 받는다. 이때에 사전에 은행과 약속된 중간 값이나 최대값의 y_i 를 사용함으로 자신의 신분을 확인시키면서 블랙메일링 공격에 대한 정보를 은행에게 전달할 수 있게 된다. 따라서 완벽한 범죄의 경우 XTR 버전의 Schnorr 개인식별 프로토콜을 사용하면 화폐의 인출 전에 범죄 사실을 은행에 전달할 수 있다.

나) 신분 위장(Impersonation)과 납치(Kidnapping) 공격을 막는 방법

신분 위장과 납치와 같은 공격에서는 블랙메일러가 신분을 위장하여 인출과정에서 은행과 직접 거래를 하게 된다. 이 때에 개인식별이 이루어져야 하는데, 두 경우 모두 블랙메일러가 피해자의 개인키를 안다고 하더라도 은행과 사전에 약속된 y_i 의 크기는 알 수 없기 때문에 정당한 사용자처럼 위장할 확률은 1/3이다. 따라서 피해자의 개인키가 노출되더라도 블랙메일링 공격을 2/3 의 확률로 은행에게 알려 줄 수 있게 된다.

납치 공격에서 피해자의 개인키는 쉽게 블랙메일러에게 드러난다. 왜냐하면 만약에 피해자가 자신의 개인키를 협박을 통하여 블랙메일러에게 알려 줄 때에 옳지 않은 값을 알려주게 되면 개인 식별 프로토콜에서 그 결과를 바로 확인 할 수 있게 된다. 따라서 신변의 위협을 느끼는 납치와 같은 공격에서는 신변에 대한 극단적인 결과를 가져올 수 있기 때문에 자신의 개인키를 속이는 것은 쉽지 않다. 그러나 y_i 의 크기는 피해자가 최소의 값이 아닌 다른 값을 사용한다고 잘못된 정보를 주어도 확인 가능한 방법이 없다. 물론 블랙메일러가 그것을 100% 신뢰하지 않겠지만, 스스로 알아 낼 수 있는 방법이 없기 때문에 결국 3개의 y_i 값 중에서 임의로 선택할 수밖에 없다. 그러나 정확한 y_i 의 크기를 사용할 확률은 1/3이기 때문에 블랙메일링 공격에 대한 정보가 은행에 전달될 위험부담이 커지게 된다. 그러므로 실제 신분위장이나 납치와 같은 공격에서도 블랙메일링 공격을 쉽게 성공할 수 없게 되고, 위와 같은 방법의 공격을 지양하게 될 것이다.

3. 안전성

신분위장이나 납치와 같은 공격에서 블랙메일러가 은행과 피해자 사이에 약속된 y_i 의 크기를 알 수 없게 되는 이유는 XTR-version Schnorr 개인식별 프로토콜에서 y_i 의 값을 그대로 은행에게 전달하는

것이 아니라 서로 공유된 대칭키 K로 y_i 를 암호화하여 보내기 때문이다. 만약에 y_i 를 암호화하지 않고 일반적인 **Schnorr** 개인식별 프로토콜에서처럼 그대로 보내게 되면 은행과 피해자 사이에 사전에 약속된 y_i 의 크기를 쉽게 알아낼 수 있다. 왜냐하면 블랙메일러가 공격하기로 결정한 대상이 은행과의 개인식별 프로토콜을 관찰하다가 정상적인 거래에 사용되어지는 y_i 값을 얻어내어 자신이 나머지 **2**개의 $y_i \cdot p^2 \bmod q$, $y_i \cdot p^4 \bmod q$ 를 계산 후에 y_i 의 값이 **3**개중에서 어떤 크기인지를 결정할 수 있기 때문이다. 즉 정상적인 거래에 사용하는 y_i 의 크기를 알아낼 수 있게 된다. 따라서 신분위장이나 납치와 같은 공격에서 피해자의 개인키 s 만 알게 되면 쉽게 정당한 거래에 사용하는 y_i 의 크기를 사용하여 정당한 사용자처럼 은행으로부터 인출을 받을 수 있게 된다.

그러나 y_i 를 그대로 보내지 않고 은행과 공유한 비밀키 K 로 y_i 를 암호화하여 보내기 때문에 절대로 비밀키 K를 알지 않고서는 y_i 의 값과 그 크기도 알 수 없게 된다. 따라서 y_i 크기의 보안에 대한 안전성은 사용하는 대칭키 알고리즘에 의존하게 되고, y_i 의 값을 정확하게 알 수 있다는 것은 대칭키 알고리즘을 공격하는 것과 같은 것이 된다. 그리고 비록 피해자의 개인키 s 를 안다고 하더라도 은행과 공유하는 공유키 K 는 개인식별 프로토콜 각 세션마다 랜덤한 수 k 에 의존하여 변하기 때문에 k 를 알지 않고서는 공유키 K 를 알아낼 수 없다.

그러므로 정당한 거래에서 사용하는 y_i 의 크기를 구하는 것은 이산대수 문제를 푸는 것과 같은 정도의 어려움을 가지게 된다.

참 고 문 헌

[1] D. Chaum. Blind signature for untraceable payments.*In Advances in Cryptology- CRYPTO '82*,pages 199-203, Plenum,1983.

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

[3] 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, pages 31-43. Springer-Verlag, 1996.

[4] 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.

[5] 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.

[6] D. Kugler and H. Vogt. Marking: A Privacy Protecting Approach Against Blackmailing, *Proceedings PKC 2001*, LNCS 1992, Springer_Verlag, 2001, 137-152.