전자현금 프로토콜의 요구사항과 비교분석

김희선, 서문석, 백준상, 김광조
한국정보통신대학원대학교

Requirements and Comparison of the existing Electronic Cash protocols

Heesun Kim, Moonseog Seo, Joonsang Paek, Kwangjo Kim
Information and Communications University

요 약

컴퓨터 보급의 확산과 함께 인터넷이 급속히 발전하면서 전자 상거래에 대한 관심이 높아지고 암호 기술의 발전으로 스마트 카드가 실용화됨에 따라 전자상거래 수행에 필수적으로 요구되는 기술인 전자현금에 대한 연구가 다양하게 이루어져 왔다. 지금까지의 전자현금에 대한 연구는 익명성, 이중사용 방지 등을 중심으로 하여 분할성, 양도성, 공정성 등의 새로운 속성들을 지원하는 방향으로 발전되어왔다.

본 논문에서는 기존에 제시되었던 다양한 전자현금 프로토콜에서 채택하고 있는 기술들을 분석하고 각 프로토콜이 만족하고 있는 요구사항들을 서로 비교함으로써 앞으로의 전자현금 프로토콜이 만족해야 할 요구사항들을 제시하고자 한다.

1. 서론

공개된 정보통신망을 통하여 신뢰할 수 없는 다자간이 자신의 비밀은 노출하지 아니하고 상대방에게 비밀의 소유 사실만을 납득하는 쌍방 및 다자간 프로토콜을 구성하기 위하여 비트 위탁, Oblivious Transfer 프로토콜 등의 기반 프로토콜 연구가 80년도에 연구가 시작된 이래, 전자 계약, 전자 현금, 전자 선거, 전자 입찰, 전자 증권 등과 같은 사이버 공간에서 적용 가능한 다양한 응용 프로토콜로 연구가 진전되었다.

그 중 전자현금 프로토콜은 D. Chaum이 은닉 서명[Cha83]을 근간으로 한 추적 불가능한 전자현금 프로토콜을 제시한 이후 분할성 및 양도성 등 전자현금이 가져야 할 기능들을 추가하는 방향으로 새로운 전자현금 프로토콜들이 제시되어 왔다. 초기 전자현금 프로토콜은 지불과 이체가 하나의 트랜잭션으로 이루어지는 온라인 방식에서 시작되었으나 [CFN88]에서 이중사용 검출의 기법이 제시된 이후 지불과 이체가 별도의 트랜잭션으로 이루어지는 오프라인 전자현금 프로토콜이 주류를 이루게 되었다.

또한 [OO91]에서는 계층적 트리 구조를 바탕으로 전자현금이 분할성을 갖도록 하는 기법이 제시되기도 하였다. 전자현금 프로토콜의 안전성 측면에서 가장 중요한 속성으로는 이

중사용 검출이 필수적으로 요구되고 있으며, 이에 대한 연구는 Cut-and-Choose기법이 Chaum[CFN88] 등에 의해서 처음 소개되었다. 그러나 Cut-and-Choose기법은 계산 및 통신량의 효율성 측면에서 많은 문제점을 가지고 있어 이를 개선하여 단항(Single term)으로 이중사용을 방지하는 전자현금 기법들이 새롭게 제시되었다.

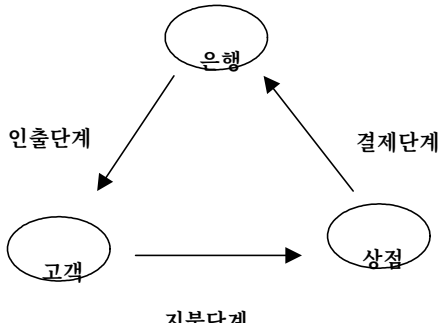
최근에는 전자현금의 완전한 익명성이 갖는 역기능을 방지하기 위하여 신뢰기관에 의존하여 필요시 익명성을 철회할 수 있는 전자현금 프로토콜들이 제시되고 있으며 약탈(Blackmailing), 돈 세탁과 같은 부정사용과 은행 모함 공격(Bank Framing attack)과 같은 공격에 대해 견딜 수 있는 전자현금 프로토콜에 대한 연구도 활발히 이루어지고 있다. 그러나 현재까지 제시된 전자현금 프로토콜에 대해서 그 안전성을 증명하는 데는 어려움이 있다.

본 논문에서는 기존에 제시되어 왔던 전자현금 프로토콜에 사용된 암호학적 기법들을 분석해 보고 이들이 만족하고 있는 요구사항들을 정리하여 새롭게 제시될 전자현금 프로토콜이 가져야 할 요구사항들을 제시하고자 한다.

본 논문의 내용으로 2장에서는 우리가 일반적으로 언급하는 전자현금 프로토콜의 기본모델에 대해서 간략하게 언급하고, 3장에서는 새로운 전자현금 프로토콜을 설계할 때 고려해야 할 요구사항들을 제시하고 있다. 이를 바탕으로 4장에서 기존의 제시된 전자현금 프로토콜 중 대표적인 [CFN88], [Bra93], [JY96] 등에서 사용된 기술들을 살펴보고, 이들간의 비교분석을 통하여 전자현금 프로토콜의 향후 발전방향에 대하여 논의하고자 한다.

2. 전자현금 프로토콜의 기본 모델

전자현금은 (그림 1)과 같이 기본적으로 은행 B, 사용자 U, 상점 S로 구성되어 구매자와 은행간에 이루어지는 발행단계(withdrawal phase), 발행단계에서 받은 전자현금을 물건을 사고 상점에 전자현금을 지불하는 지불단계(payment phase), 구매자로부터 받은 전자현금을 은행에 제출하여 상점의 계좌로 자금이체를 시켜주는 결제단계(deposit phase)로 다음의 그림과 같은 기본적인 처리 단계를 수행한다.



(그림 1) 전자현금

이 때, 결제단계에서 상점 S가 은행 B가 서로 통신을 하지 않는다면 이 전자현금 시스템은 오프라인 전자현금 시스템이 되고, 은행 B가 상점 S와 결탁한다고 하더라도 고객 U에

대한 동전을 추적할 수 없다면 익명성이 보장되는 것이다. 그러나 변조방지(tamper-proof) 하드웨어가 없다면, 전자현금은 사용자 U에 의해서 복사되거나 여러 번 사용될 수 있다 [Tsio97]. 따라서 이러한 이중사용(double-spending)을 방지할 수 있는 기법에 대한 연구와 익명성을 함께 보장할 수 있는 전자현금을 구현하는 것이 초기 전자현금 연구의 주요 관심이었다. 온라인 전자현금 시스템에서는 결제단계가 이루어지기 전에 은행의 데이터베이스를 검색하여 사용되는 현금의 이중사용 여부를 확인하여 이중사용을 방지하였으나 이러한 온라인 전자현금 시스템은 매 결제단계마다 상점이 은행과 연결되어야 하는 단점이 있으므로, 오프라인 전자현금 시스템을 기본으로 전자현금 시스템을 고려한다면 이러한 방법은 오프라인 전자현금 시스템에서는 적용이 불가능한 것이다. 그러나 이에 대한 연구가 [CFN88]에서 Chaum 등에 의해서 제안되어 전자현금 프로토콜 연구에 새로운 발판을 마련하게 되었다.

전자현금 프로토콜의 연구는 이와 같이 기본적인 전자현금의 참여자인 은행, 고객, 상점의 입장에서 고려할 수 있는 요구사항들을 만족시키는 것으로 많은 발전을 거듭하여 왔다. 따라서 다음 장에서는 전자현금 프로토콜이 기본적으로 만족해야하는 조건들과 추가적으로 만족시켜야 하는 요구사항들을 살펴보기로 하겠다.

3. 전자현금 프로토콜의 위협요소와 요구사항

지금까지의 연구되어 온 전자현금에 대한 연구들을 토대로 검토해본 결과 전자현금 프로토콜에 대한 요구사항과 고려해야 할 위협요소들을 다음과 같이 정리해 볼 수가 있다.

먼저, 전자현금 프로토콜에서 고려해야 할 위협요소들에는 다음과 같은 것들이 있다.

가. 위협요소

- 위조(Forgery) : 은행을 제외한 참가자가 인출 프로토콜에 참가한 후에 인출한 전자현금의 금액을 액면가에 초과하는 전자 현금으로 바꾸어 그것이 은행에 의해 유효하게 받아들여지게 하는 공격
- 이중사용(Double spending) : 사용자가 발급 받은 전자현금을 한 번 이상 사용하는 행위
- 초과사용(Overspending) : 사용자가 발급 받은 액면가 이상의 금액을 사용하는 행위
- 위장(Impersonation) : 공격자가 마치 사용자인 것처럼 사용자의 계좌에 접근하여 돈을 가로채는 공격
- 돈 세탁(Money laundering) : 불법적인 돈의 출처를 감추기 위하여 행해지는 이체
- 불법 구매 (Illegal purchases) : 마약의 구매와 같은 불법적인 물품 구매
- 약탈(Blackmail) : 공격자가 사용자에게 사용자의 계좌에서 돈을 인출할 것을 강요하고 공격자가 추적 당하지 않고 돈을 입금시키거나 사용할 수 있는 방법으로 공격자에게 돈을 전송하도록 하는 공격
- 은행 강탈(Bank robbery) : 공격자들의 집단이 은행에게 추후 사용할 수 있는 돈을 얻도록 프로토콜에 참여하기를 강요하는 공격

나. 요구사항

따라서 이러한 공격에 대응하여 전자현금 프로토콜에서 만족해야 할 요구사항들은 다음

과 같이 기본적인 요구사항과 그에 추가적인 기능을 만족시키는 추가적인 요구사항으로 나누어 볼 수 있다.

1) 기본적인 요구사항

- 이중 사용 방지(Double-Spending prevention) : 사용자가 같은 전자 현금을 두 번 사용할 수 없도록 한다.
- 익명성(Anonymity) : 은행이 신뢰기관의 협조 없이 동전과 정직한 사용자의 신원을 연결시키는 것을 불가능하게 한다.
- 추적불가능성(Untraceability) : 전자현금과 사용자 사이의 관계는 권한이 부여된 익명성 취소의 경우를 제외하고는 은행이 추적할 수 없다.
- 완전정보화 : 전자현금에서 다루는 모든 정보는 디지털화 되어있어 Bit의 기본요소로 구성되어 있다.
- 위조 불가능성(Unforgeability) : 단지 은행과 같이 권한이 부여된 참가자만이 전자현금을 발행할 수 있다.

2) 추가적인 요구사항

- 분할성(Divisibility) : 정확한 금액의 지불을 위하여 전자현금의 액면금액에 대해서 더 작은 단위로 나누어질 수 있다.
- 양도성(Transferability) : 한번 인출된 전자현금이 다른 사용자에게 양도가 가능하다.
- 공정성(Fairness) : 사용자는 신뢰기관과 은행에 대해서 각각 익명성이 보장되어야 하는데, 이 두 기관의 합법적인 협조에 의해서만 익명성이 조건적으로 철회될 수 있다.
- 연결불가능성(Unlinkability): 동일 사용자가 사용한 서로 다른 전자현금을 연결시키는 것이 불가능하다.
- 익명성 취소(Revocability) : 은행의 강탈자가 얻은 어떠한 돈이라도 즉시 사용될 수 없도록 블랙리스트에 올려지거나 익명성이 철회되어야 한다.
- 환불가능성(Refundability) : 은행과 신뢰기관과 같은 기관이 공모하지 않는 한 신뢰기관이 인출 프로토콜을 따라할 수 없다는 것을 법정에 증명해 보이는 것이 가능해야 하며, 올바르게 인출된 돈이 은행이나 신뢰기관에 의해 받아들여지지 않은 경우는 사용자에게 그 금액을 환원해 주어야한다.
- 모함 방지(Framing-freeness) : 어떤 사용자나 상점도 은행이나 신뢰기관에 의해서 그릇되게 고소되어 질 수 없다. 능동적인 도청공격자(eavesdropper attacker)로부터 사용자를 보호하기 위해 필요하다면 모든 통신은 근거가 있고 믿을 수 있어야 한다.
- 초과사용 추적(Overspent-tracing) : 은행은 전자현금을 초과 사용한 사용자의 신분을 알 필요가 있다. 그것은 분리된 메커니즘이나 사용자 추적과 같은 방식으로 가능하다.
- 사용자 추적(User-tracing): 은행과 신뢰기관은 사용된 전자현금과 사용자를 연결시키기 위해 협동한다.
- 현금추적(Coin-tracing): 은행과 신뢰기관은 사용될 전자현금과 예치된 전자현금과 관련된 정보가 일치하는지를 계산하기 위해 협동한다. 어떤 시스템에서는 전자현금이 강탈당한 후 필요한 정보를 사용자 자신이 공개하는 것이 가능할 지도 모른다.
- 강탈추적(Extortion-tracing): 은행과 신뢰기관은 사용된 또는 예치된 전자현금의 일치

를 허락하는 정보를 계산하기 위해 협동한다.

- 효율성(Efficiency) : 제안된 기법은 저장용량, 통신량, 계산량에 있어서 효율적이어야 한다.
- 속임 방지(Blindfolded-freeness) : 특정한 동전이 은닉되었다는 사실을 은행이 알지 못하는 가운데 그 은닉된 동전을 얻는 것이 불가능하다.

4. 기존 전자현금 프로토콜 분석

이번 장에서는 기존에 제시되었던 전자현금 프로토콜들을 전자현금의 요구 사항을 만족시키기 위해 사용된 기법과 사용된 기술을 중심으로 분석한다.

가. Chaum, Fiat, Naor의 기법 [CFN88]

오프라인 지불형태로 익명성을 보장한 전자현금은 Chaum, Fiat, Naor에 의해 처음으로 소개되었다[CFN88]. 그들은 기존에 제시되었던 전자현금 프로토콜에서 전자현금 시스템의 참가자들 각각은 다른 제3자들에 의해서 사기를 당하기 쉬우며, 특히 카드의 소유자인 고객은 이러한 사기로부터 보호될 수 없다는 문제점을 지적하면서 근본적으로는 전자현금에 대한 일련 번호가 현금에 대한 추적을 가능하게 만들지만, 프라이버시 측면에서 신용카드에 대한 장점을 충분히 반영할 수 있는 추적 불가능한 전자현금을 제시하였다. 이에 대한 안전성은 몇 가지 가정을 바탕으로 하고 있으며 제시된 기법이 실용적이지 못하다는 점이 단점으로 지적되기는 하지만 전자현금에 대한 연구에 새로운 방향을 제시해 주었으며, 이를 토대로 전자현금에 대한 연구가 매우 활발히 진행되어 왔다는 점에서 전자현금 연구에 초석이 되었다고 볼 수 있다.

1) 인출 단계

[CFN88]에서 제안된 기법은 고객이 은행으로부터 전자현금을 얻을 때 RSA 디지털 서명 기법을 사용하여 추적 불가능한 전자현금을 구체화시켰다. 고객은 현금을 얻기 위해 자신의 신원정보가 쓰여진 은닉된 후보들을 생성하여 은행에 제시하는데 영지식 증명 기법을 이용하여 이것을 은행에게 확인시킨다. 그러면 은행은 은닉 서명을 이용하여 서명한 현금을 고객에게 전달하게 되고, 고객은 자신만이 알고있는 정보를 이용하여 지불 가능한 현금을 추출해낸다.

2) 지불 단계

이렇게 얻어진 현금을 상점에 지불할 경우에 상점은 지불된 현금이 올바른 정보로 구성되었고 은행의 서명을 받은 것임을 확인한 다음 지불된 현금에 대한 금액을 은행에게 입금할 것을 요구하게 된다. 여기서 누구나 현금의 올바른 구성과 은행으로부터 서명을 받은 현금임을 확인할 수 있지만, 은행이 특정한 현금을 그 현금 수령인의 계좌와 바로 연결시킬 수 없다는 점이 고객에 대한 추적을 불가능하게 해준다. 또한 오프라인으로 지불단계가 이루어져 같은 동전을 두 번 사용한 고객은 은행에 의해 추적될 수 있다. 그들은 이러한 기법에 대해 실용적인 예를 들기 위해서 Cut-and-Choose 기법을 이용하였다.

3) Cut-and-Choose 방법

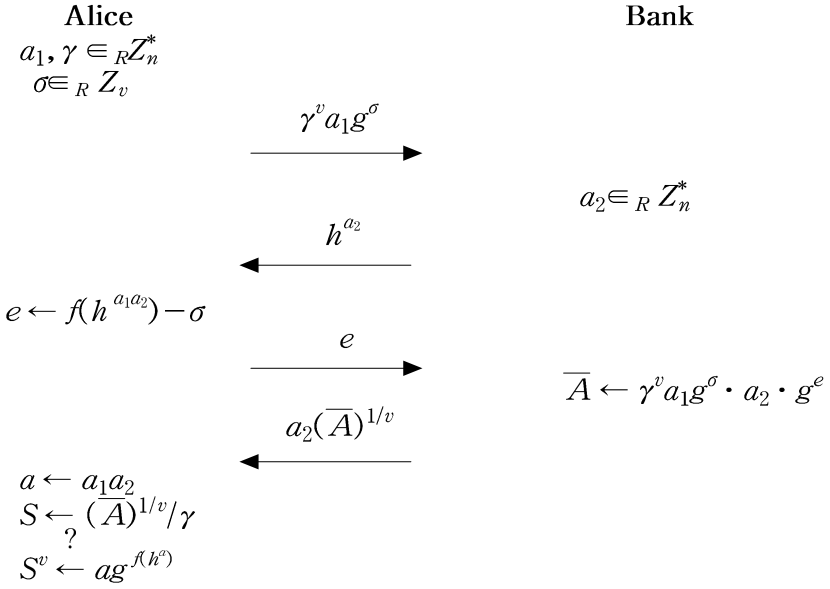
이 기법은 먼저 은행은 고객이 제시한 현금의 구성을 확인할 수 있도록 충분한 길이의 항(term)을 위한 안전성 변수 k를 정하고, 고객은 2k개의 은닉된 항들을 은행에 제시한다. 제시된 항들 중에서 은행은 k개 항의 구성을 보여줄 것을 요구하고 고객은 요구된 항에 대해 은닉되었던 값들을 보여줌으로써 은행이 이를 확인하게 한다. 그런 다음 은행은 나머지 k개의 은닉된 항에 서명을 하여 고객에게 전달한다. 마지막으로 고객은 항의 은닉을 위해 이용했던 자신만이 알고있는 정보를 제거하는 것으로 전자현금을 추출해낸다.

인출된 전자현금을 정상적으로 사용한 사용자에 대해서는 사용자가 상점에 제공하는 힌트 정보에도 사용자의 계좌번호가 전혀 노출되지 않지만 전자현금이 이중 사용이 되었을 경우 상점이 고객에게 보내는 challenge 정보가 높은 확률로 0이 아닌 Hamming distance의 값을 갖게 된다는 점을 이용하게 된다. 즉, 고객, 은행, 상점간에 주고받는 모든 정보들은 은행에 기억되어 있다가 같은 전자화폐를 제시한 둘 이상의 상점들의 challenge 정보 중 일치하지 않는 인덱스 정보에서 계좌가 노출되는 것이다.

이러한 Cut-and-Choose 방법은 오프라인에서 이중사용 검출 시 매우 효과적이지만, 안전성을 위한 정보 k에 따른 통신 데이터 량의 증가와 고객과 은행간에 주고받는 데이터 중 반 정도만이 전자현금이 될 수 있다는 비효율적인 측면을 지니기 때문에 현실에 반영시키기에는 어려움이 있다. 또한 이들의 전자현금 방식은 현금의 최고액이 미리 정해져 있으며 지불 후 나머지 금액에 대해서는 버려야 하며, 현금의 단위가 고정되어 있다는 단점이 있어 후에 [CB89]에서 이를 보완하였다.

나. Niels Ferguson의 기법 [Fer93]

Niels Ferguson은 지금까지의 모든 전자현금은 비효율적인 Cut-and-Choose방식을 이용하였던 것을 지적하며 전자현금의 인출 프로토콜에서 직접 동전을 구성하여 현금 각각이 고정된 값을 갖는 동전 방식을 제안하였다[Fer93].



(그림 2) Randomized blind signature scheme

그의 기법은 각 동전을 3개의 숫자들과 2개의 RSA 서명으로 구성하여 약 250bytes 정도의 저장용량을 제시하였다(원래의 서명을 쉽게 복원하기 위해 네 개의 서로 다른 동전들의 서명을 저장 공간을 절약하기 위해 한꺼번에 수행한다는 가정을 한다[Cha90]). Ferguson의 중심 아이디어는 동전을 Z_n^*를 Z_v로 변환하는 일방향 함수 f를 이용한 $C := f_c(c)$, $A := f_a(a)$, $B := f_b(b)$과 같은 세 개의 숫자로 나타내며, 은행으로부터 $(C^k A)^{1/v}$, $(C^U B)^{1/v}$의 RSA 서명을 받는다. 여기서 v는 소수를, U는 고객의 신원을, k는 랜덤 수를 각각 의미한다.

Ferguson은 또한 전자현금을 효율적인 방법으로 얻기 위해 (그림 2)와 같이 랜덤한 은닉 서명을 이용한다. 랜덤한 은닉 서명은 얻어진 전자현금을 위조하는 것이 계산상 어렵고 은행이 랜덤한 은닉 서명의 프로토콜을 수행하는 동안 전자현금에 대한 어떠한 정보도 알 수 없다는 가정을 하고 있다. 그러나 이 서명 기법을 그대로 이용하면 고객이 랜덤하게 선택하는 값에 대해서 임의의 조정이 가능하게 된다. 따라서 가능한 지수 공격을 방지하기 위해서는 다음과 같이 변형된 은닉서명을 이용해야 한다. 은행이 h^{a_2}를 전달하므로 고객 임의의 h^{a_2}를 이용한 계산을 불가능하게 한다. 따라서 이를 이용하여 수행되는 동전의 인출 프로토콜에서는 동전을 이루는 세 개의 수 C, A, B가 다음과 같이 얻어진다.

$$C = c g_c^{f(h_c)} \qquad A = a g_a^{f(a)} \qquad B = b g_b^{f(h_b)}$$

여기서 g를 다르게 사용한 것은 수들을 구별시키기 위함이고 하나의 서명에 함께 곱해질 경우에도 혼합되지 않게 하기 위한 것이다. 이해를 돕기 위해 전자현금의 인출 프로토콜을 간략화 시켜 다음과 같이 설명하고자 한다.

단계 1) 고객은 랜덤하게 수들을 선택하는데, c_1, a_1, b_1는 계산절차에서 밑수로, σ, τ, ψ는 blinding factor의 지수 값으로, γ, α, β는 blinding factor의 곱셈으로 사용하여 계산한 것을 은행에게 전달한다.

단계 2) 은행은 c_2, a_2, b_2을 랜덤하게 선택하여 $h_c^{c_2}$, a_2, $h_b^{b_2}$를 고객에게 전달한다.

단계 3) 고객은 k_1을 랜덤하게 선택하고 e_c와 e_b를 계산하고 이 값들을 이용하여 a를 계산한 후, e_a를 구하고, 계산된 e_c, e_b, e_a를 은행에게 전달한다.

단계 4) 은행은 다음과 같은 C, A, B에 대한 은닉된 값 C', A', B'를 계산하여 유효성을 확인하고 k_2를 랜덤하게 선택하여 계산에 이용한다. 이전에 선택한 값과 함께 그 결과인 c_2, b_2, k_2, $(C'^{k_2} \cdot A')^{1/v}$, $(C'^{U} \cdot B')^{1/v}$를 고객에게 전달한다.

단계 5) 고객은 은행으로부터 받은 c_2, b_2를 이용하여 c와 b를 계산하고 C, A, B의 값을 만들게 된다. 또한 서명 S_a와 S_b도 계산해 낼 수 있다.

$$S_a = ((C'^{k_2} \cdot A')^{1/v} / \gamma^{k_2} \alpha)^{k_1}, \quad S_b = (C'^{U} \cdot B')^{1/v} / \gamma^{U} \beta$$

그리고, 마지막으로 고객은 자신이 받은 서명이 맞는지를 다음과 같이 확인할 수 있다.

$$S_a^v = C^k A, \quad S_b^v = C^U B$$

위의 결과 얻어진 전자현금을 지불단계에 이용할 때 수행되는 절차를 간략화 시키면 다음과 같다.

단계 1) 고객은 상점에게 동전을 이루는 c, a, b의 숫자들을 전달한다.
단계 2) 상점은 랜덤하게 선택한 challenge x를 고객에게 전달한다.
단계 3) 고객은 $r := kx + U \pmod{v}$와 자신이 갖고 있던 두개의 서명으로부터 서명 $(C^r A^x B)^{1/v}$를 계산하여 상점에게 전달한다.
단계 4) 상점은 고객으로부터 받은 정보들의 일관성을 확인한다.

동시에 여러 개의 동전을 사용할 때에도 모든 동전에 같은 challenge를 사용하고 모든 서명을 곱하여 전달하므로 각 동전에 대해서는 두 번의 곱셈과 한번의 x 제곱의 연산만 수행하면 된다. 만일 고객이 사용한 동전이 두 번 사용되었다면 상점의 challenge x가 서로 다르다는 것을 이용하여 $kx + U$로부터 고객의 신원 U를 검출해 낼 수가 있다.

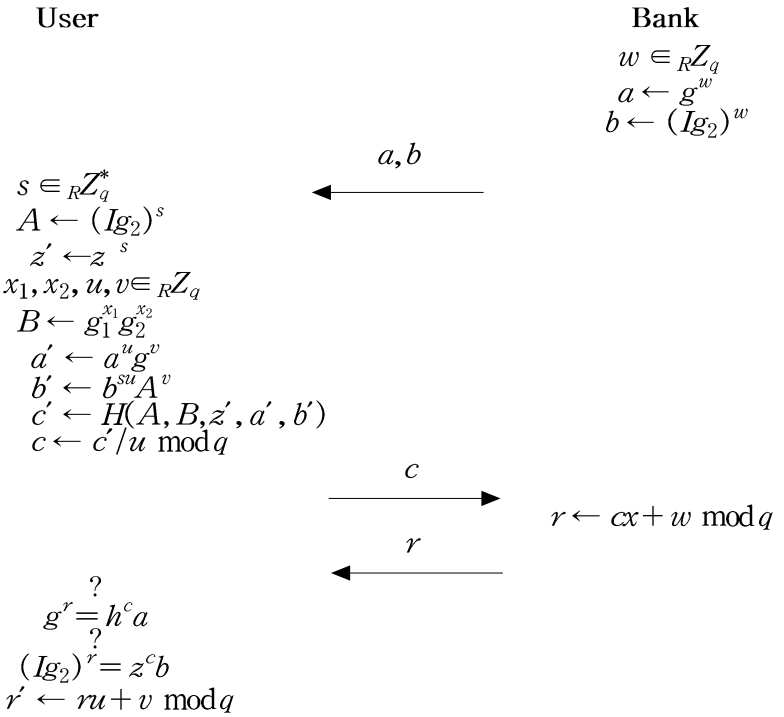
그러나 위의 기법은 은행으로부터의 모함 공격을 방지할 수 없으므로 고객의 신원 정보인 U를 고객의 신원정보와 동전의 유일한 값으로 구성하여 모든 동전들의 U의 값을 구별시킨다. 그러므로, 은행이 고객의 동전이 이중 사용되었다고 주장할 경우, 그 동전에 대한 인출 프로토콜의 복사를 제시해야만 하며, 이중 사용된 동전으로부터 a, b, c 값을 보여주기도 해야 한다. 만일 고객이 이중 사용자가 아니라면 은행은 a, b, c에 대한 어떠한 지식도 가지고 있지 않기 때문에 은행이 고객을 속이기 위해서는 a, b, c가 고객이 사용한 실제 값과는 다른 값이 될 것이다. 따라서 모함 공격을 방지할 수 있게 된다.

다. S. Brands의 기법 [Bra93]

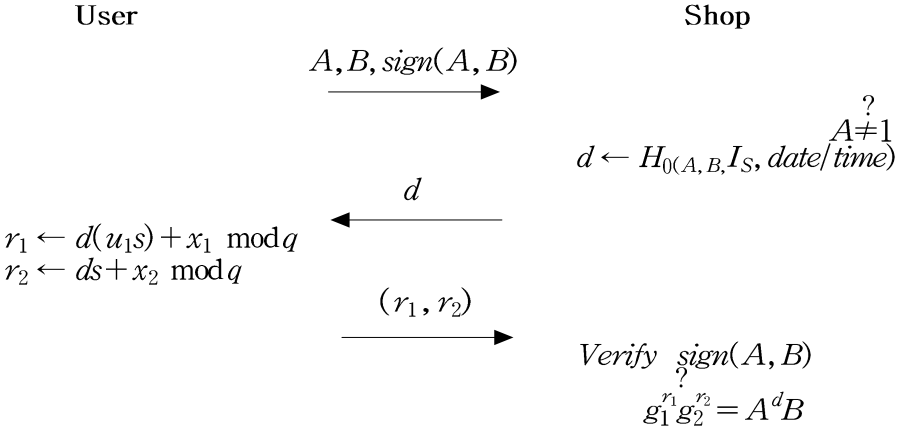
S. Brands는 군 표현 문제(group representation problem)를 응용하여 제한적 내용은닉 서명(restrictive blind signature)을 제안하였으며 이 새로운 형태의 내용은닉 서명을 전자현금 프로토콜에 적용되었다. 군 표현 문제란, "어떤 유한군 G_q의 원소 h와 G_q의 생성자들 $g_1, g_2, \ldots, g_k$에 대하여 $h = g_1^{x_1} g_2^{x_2} \cdots g_k^{x_k}$가 되는 $x_1, x_2, \ldots, x_k$를 찾는 문제가 어렵다(다항식 시간의 알고리즘이 존재하지 않는다)"는 것이다. Brands는 개인 정보 u를 생성자의 지수에 대응시켜 $I = g^u$ 를 계산한 후 군 표현형 문제를 이용하여 이 I가 프로토콜의 중간에 변형되는 것을 막았다.

전자현금의 인출 단계에서 내용은닉 서명을 이용하여 사용자는 은행으로부터 전자현금을 발급 받는다. (그림 3)에서 A와 B가 발급 받은 전자 현금이 된다.

지불 단계에서는 사용자가 전자현금을 두 번 사용하였을 때 사용자의 개인 정보를 드러나게 하여 이중 사용자의 검출을 가능하게 하였다. 사용자가 지불단계에서 현금을 이중 사용하였다고 가정하자. 즉 (그림 4)의 프로토콜에서 사용자 U는 $(r_1, r_2), (r_1', r_2')$ 두 번의 현금을 사용한다. 이 때 이 현금을 받아본 은행에서는 $(r_1 - r_1')/(r_2 - r_2')$을 계산하여 사용자의 개인정보 u_1을 알 수 있다.



(그림 3) 전자현금의 인출단계



(그림 4) 전자현금의 지불단계

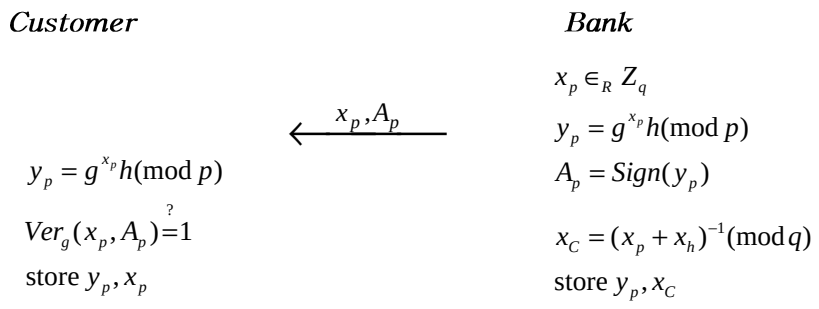
라. J. Camenisch, J. M. Piveteau, M. Stadler의 기법 [CPS96]

기존에 제안되었던 많은 지불 시스템들은 지불인의 익명성을 무조건적으로 제공하고 있다. 그러나 이러한 무조건적인 기밀 보호는 갈취나 돈 세탁 등과 같은 범죄에 악용될 소지가 있어 [CPS96]에서는 이러한 문제점을 해결하기 위하여 공정한 지불 시스템을 제시하고 있다. 이는 기존의 지불 시스템과 동일하게 익명성을 보장하면서 필요 시 거래에 직접 관여하지 않은 신뢰기관의 도움으로 익명성을 철회할 수 있는 시스템을 지칭하는 것으로 본 기법에서는 제3의 신뢰기관이 인출, 지불 및 예치거래에 직접 참여하지 않으면서도 시스템이

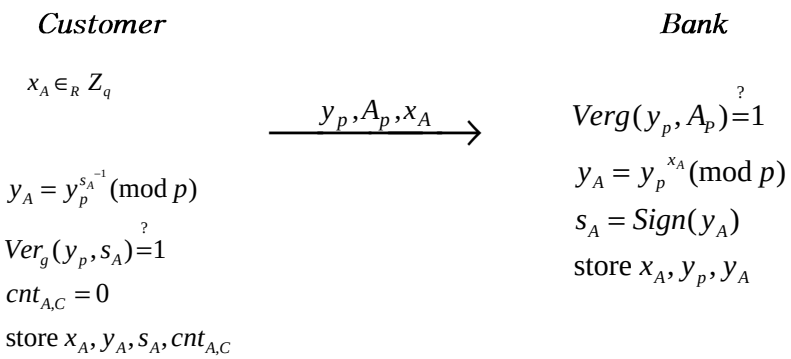
범죄에 의해 악용되어질 경우에는 신뢰기관의 도움을 받아 거래의 익명성이 철회될 수 있도록 프로토콜을 구현하고 있다. 프로토콜상의 특징으로는 일반적인 전자현금 시스템이 지불단계와 예치단계가 오프라인으로 이루어지는 데 반해 고객, 상점, 은행이 모두 참여하는 하나의 트랜잭션으로 이루어지는 온라인의 성격을 가지고 있다.

전반적인 프로토콜을 살펴보면 다음과 같다. 은행은 고객과 관련하여 두 가지 유형의 계좌를 가지고 있는데 하나는 소유자가 은행에 알려지는 실명계좌(Personal account), 소유자의 가명만이 알려지는 익명계좌(Anonymous account)를 관리하게 된다. 익명지불은 고객의 익명계좌로부터 상점의 계좌로 이체되며 이러한 익명성을 보장받기 위해서는 고객의 실명계좌로부터 익명계좌로 자금이체가 일어나는 시점에서 둘 사이의 관계가 노출되어서는 안 된다는 것이다. 또한 공정성을 확보하기 위해 이 시스템에서는 판사만이 실명계좌와 익명계좌 사이의 관계를 알고 있도록 하고 있으며, 실명계좌로부터 인출된 현금은 판사에게 등록된 해당 익명계좌로만 예치가 가능하도록 제한하고 있다. 고객은 실명계좌에 해당하는 공개키를 가지고 있고 익명계좌를 개설하기 위하여 그 공개키로부터 유도된 공개키를 판사에 등록하여야만 한다. 고객이 은행에 익명계좌를 개설하기 위해서는 은행은 판사에 등록이 이루어졌는지, 익명계좌는 올바로 구성되어 있는지를 확인하여야 한다. 실명계좌로부터 인출은 실명계좌의 공개키에 대해 은행에 의해 서명되어지고 고객은 해당하는 익명계좌의 공개키에 대한 유효한 서명 값을 도출할 수 있게 된다. 해당 공개키 쌍이 판사에 등록되기 때문에 돈세탁의 경우에 거래의 추적이 가능하고 만약 사기꾼이 자신의 익명계좌를 개설해 놓고 고객의 전자현금을 갈취할 경우 이의 추적이 가능하다.

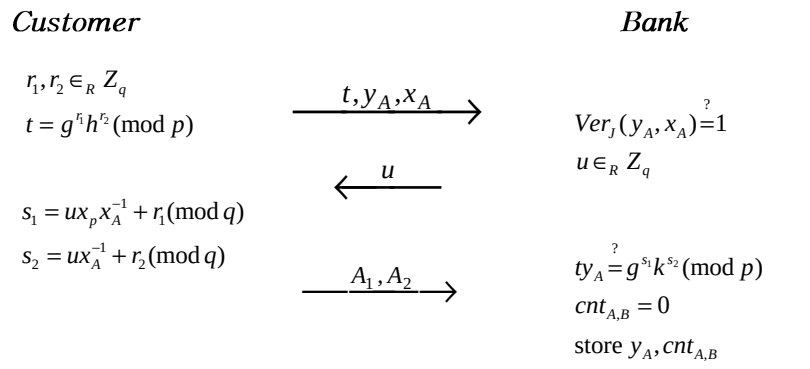
프로토콜의 상세 구성 내용을 살펴보면 (그림) 5에서 (그림) 9와 같다. 시스템 초기화는 실명계좌의 개설, 등록, 익명계좌의 개설 등 세 단계로 구분되어 지고 초기화가 완료되어진 후에 실명계좌로부터 해당 익명계좌로 이체가 일어나게 된다. 이것은 실명계좌로부터의 인출과 익명계좌로의 예치로서 두 단계로 나누어져 있다. 상점에 대한 지불은 고객의 익명계좌로부터 상점의 계좌로 온라인 상에서 단순 이체가 된다. 대부분의 단계에서 참가자의 상호 인증이 필요하나 등록, 익명계좌 개설, 익명계좌로의 예치단계에서는 익명성 보장을 위해 고객의 인증이 이루어져서는 안 된다.



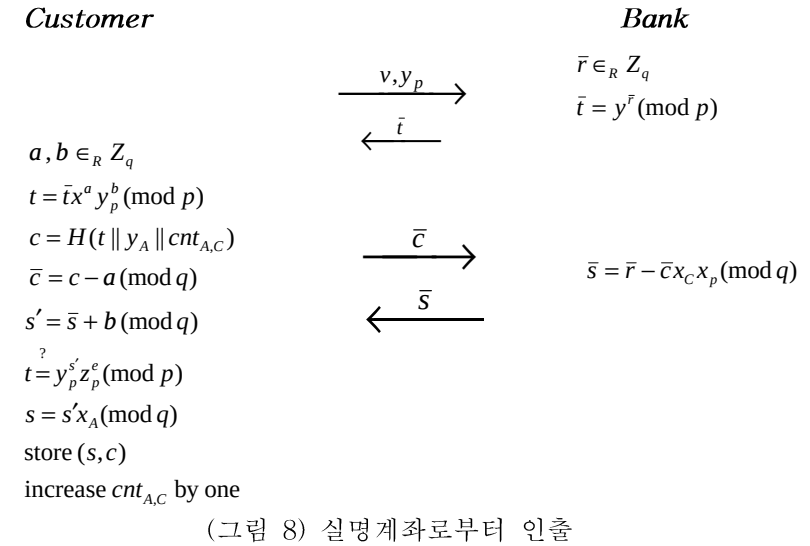
(그림 5) 실명계좌 개설



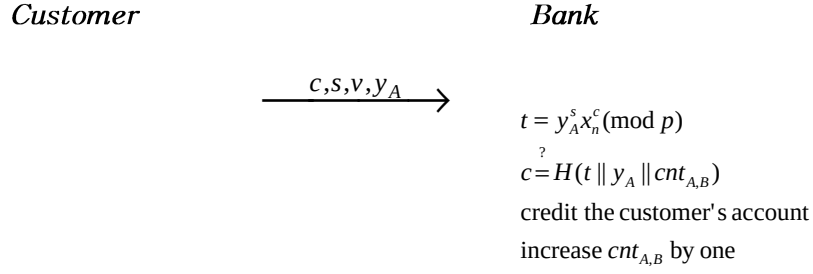
(그림 6) 신뢰기관에 등록



(그림 7) 익명계좌 개설



(그림 8) 실명계좌로부터 인출



(그림 9) 은행으로 예치

등록 단계에서 판사는 실명계좌와 익명계좌의 관계를 알고 있기 때문에 프로토콜에서 사용된 실명계좌번호 및 익명계좌번호가 판사에게 제시되면 언제든지 자금이체의 출처를 확인할 수 있게 된다.

안전성 분석측면에서 살펴보면, 인출 프로토콜 동안에 사용된 서명은 Schnorr 기법을 이용한 Okamoto의 은닉서명 방식의 안전성에 의존하고 있으며 이는 근본적으로 이산대수 문제의 어려움에 근간하고 있다.

다중 지불의 경우 고객은 인출한 현금마다 고유의 카운터인 $cnt_{A,C}$를 저장하고 있고 은행은 익명계좌에 예치할 때 해당 카운터인 $cnt_{A,B}$를 저장하고 있으므로 이의 비교를 통해 다중 지불은 방지할 수 있다. 이체 값 v의 수정 또한 이산 대수 문제를 근간으로 하여 변경이 불가능하며 실명계좌로부터의 인출과 익명계좌로의 예치는 다수의 거래가 발생하고 인출과 예치사이에 시간 간격이 적절히 선택되어 진다면 상호 연결이 불가능하다. 또한 실명계좌 y^P로부터 다른 실명계좌 $\tilde{y}^P$에 해당하는 익명계좌 $\tilde{y}^A$로의 이체인 교차지불(cross-payment)은 불가능한데 이는 그러한 지불이 가능하기 위해서는 공격자가 y^P에 대한 $\tilde{y}^P$의 이산대수를 알아야만 가능해지나 이는 풀기 어려운 것으로 간주되고 있다.

본 기법에서 제시된 공정한 지불 시스템은 그 실용성과 효율성을 보이기 위해 프로타입으로 구현되어져 있으며 이러한 효율적인 측면을 고려할 경우 스마트 카드상의 구현을 통해 인터넷 등과 같은 네트워크를 통한 지불시스템으로는 적합한 것으로 판단하고 있다.

마. M. Jakobsson, M. Yung의 기법 [JY96]

[JY96]은 은행과 옴버즈맨이라고 불리우는 고객권리조직의 협력이 이루어진 경우에 한해서 이체금액과 사용자의 익명성이 철회될 수 있는 전자현금 시스템을 제안하고 있으며 능동적 공격자에 의해 은행에 대한 강탈 행위가 발생한 경우에 대한 방지 대책을 고려하기 위해 익명성 철회 개념을 도입하고 있다. 또한 분할성, 전자수표, 신용카드 구입 등으로의 다양한 전환이 용이하도록 하는 Challenge semantics라는 개념을 채택하고 있으며 이는 Challenge의 다른 비트들에 다른 의미를 부여함으로써 현금의 기능성을 묘사하는 것으로 일단 현금이 소비된 후에 해당 Challenge semantics를 변경하는 것은 불가능하다.

은행의 부정 이용을 방지하기 위하여 서명기능을 은행과 옴버즈맨 사이에 분할하여 놓았으며 옴버즈맨은 매 인출에 관한 정보를 등록하고 있고 법원 명령이 제출되어졌을 경우에 한해서 은행에 추적 정보를 제공하게 된다. 이러한 정보는 은행이 현금 인출자에 대한 ID를 식별하거나 어떤 사람에 의해 인출된 현금에 관한 정보를 얻을 수 있게 한다. 자금 인출 시

은행 단독의 서명 검증에 의해서만 현금이 발행될 경우 내부인 사기 및 강제은닉(Blindfolding)과 같은 은행 강탈 공격에 대처할 수 없게 된다. 결국 사용자의 익명성을 포기하지 않고도 이러한 은행 강탈 공격 및 기타 공격들에 대처하기 위해 본 기법에서는 인증자인 옴버즈맨을 필요로 하는 Dual Verification Signature라는 개념을 소개하고 있다.

또한 본 기법을 위해서는 두개의 프리미티브를 필요로 하고 있는 것으로 가정하고 있는데, 첫째는 은행 강탈 공격을 방지하기 위해 서명수신자에 의해 강제 은닉되지 않는 서명기법이며. 둘째는 합법적인 사용자의 익명성을 보장하면서 필요 시 익명성 철회가 가능한 메커니즘이다. 이를 위해 옴버즈맨의 개입 없이 은행이 현금을 ID와 연결시킬 수 없도록 하는 방법이 채택되어 지고 있다.

제시되어 있는 시스템의 기본 프로토콜을 살펴보면 다음과 같다.

1) 시스템 파라미터

k : security parameter

Mk : Message Space

KG : Key Generation algorithm

S : signing scheme

V : Verification algorithm

t : triggering condition

$E(\cdot)$: 공개키 암호 시스템의 암호화

$D(\cdot)$: 공개키 암호 시스템의 복호화

$coin : (x,s)$ x: 난수, $y=f(x)$이고 $s=S_{Bank}(S_{Ombudsman}(y))$

2) 현금인출 단계

사용자, 은행 그리고 옴버즈맨이 참여하고 있으며 옴버즈맨은 y는 알지만 사용자의 id는 알지 못하는 반면 은행은 사용자의 id는 알게 되지만 현금에 대한 서명은 옴버즈맨이 서명한 후에 자신이 서명하는 방식을 채택하고 있다.

(1) 고객은 세션 키 K_B, K_O 및 현금에 해당하는 비밀 키 x를 선택하고 다음을 계산한다.

$\overline{K_B} = E_{Bank}(K_B)$

$\overline{K_O} = E_{Ombudsman}(K_O)$

$y = f(x)$

$\bar{y} = E_{K_O}(y)$

$\overline{id} = E_{Bank}(id)$

$\overline{\overline{id}} = E_{K_O}(\overline{id})$: id는 고객의 식별자

고객은 은행으로 ($\overline{K_B}, \overline{K_O}, \bar{y}, \overline{\overline{id}}$)를 전송한다.

(2) 은행은 옴버즈맨에게 ($\overline{K_O}, \bar{y}, \overline{\overline{id}}, n$)를 전송한다

(3) 옴버즈맨은 다음을 계산하고 $\overline{id}$를 은행에 보내고 은행은 $\overline{id}$로부터 id를 복원한다.

$K_O = D_{Ombudsman}(\overline{K_O})$

$y = D_{K_O}(\overline{y})$

$\overline{id} = D_{K_O}(\overline{\overline{id}})$

$\sigma = S_{Ombudsman}(y)$

은행과 옴버즈맨의 상호 협동을 통해 $s = S_{Bank}(\sigma)$를 생성하고 옴버즈맨은 이를 검증한 후 $\overline{s} = E_{K_O}(s)$를 은행에 전송하고 $(n, y, K_O, \overline{id})$를 저장한다.

(4) 은행은 고객에게 $\overline{s}$를 전송하고 $(n, id, \overline{s}, \overline{\overline{id}})$를 저장한 후 고객의 계좌에서 현금 값에 해당하는 금액을 차기한다.

(5) 고객은 $s = D_{K_O}(\overline{s})$를 계산한 후 (y, s)를 검증한 후 (x, s)를 저장한다.

3) 지불 단계

(1) 고객은 상점에 (y, s)를 전송한다.

(2) (y, s)를 검증한 후 랜덤 Challenge c를 고객에게 전송한다.

(3) 고객은 challenge c에 대해 $a = S_{Coin}(x,c)$로 응답한다.

(4) 상점은 (y, s, c)를 검증하고 은행 강탈 공격에 대해 보고된 것이 없으면 현금의 유효기간을 확인하고 지불을 승인하고 지불단계를 마친다. 그렇지 않을 경우 다음 단계로 계속 진행한다.

(5) 상점은 (y, s)을 옴버즈맨에 전송하고 옴버즈맨은 현금이 만기 되었는지의 여부와 (y, s)의 정당성을 검증한 후 합법적 인출 목록에 있는지를 확인하여 있으면 지불승인을 지시하고 없으면 공격자를 잡는 데 필요한 행동을 취한다.

(6) 상점은 옴버즈맨으로부터 지불승인 지시를 받으면 지불을 승인한다.

4) 예치 단계

상점은 여유 시간에 은행에 (y, s, c, a)를 보냄으로써 고객으로부터 받은 지불을 예치할 수 있다.

5) 안전성

은행은 고객으로부터 받은 (y, s, c_1, a_1), ..., (y, s, c_k, a_k)로 축적된 값이 공개키 y가 허용하는 값의 범위를 초과하는가를 판단하여 초과할 경우 사용자가 초과소비를 한 것으로 판단할 수 있다. 인출 시에 해당 인출을 식별하는 순서번호가 부여되어 있고 현금별로 식별번호 y가 명시되어 있으므로 이를 이용하여 은행과 옴버즈맨이 협력할 경우 은행은 (id, y, s) 정보를 알아낼 수 있어 익명성의 철회가 가능하여 고객의 비밀을 제한할 수 있게 된다. 또한 사용자가 인출 프로토콜을 수행한 후 올바른 현금을 수신하지 못한 경우 사용자는 (s, y, K_O)을 보내고 은행은 정당성 여부를 검증하고 올바른 정보일 경우 해당 고객의 계좌로 해당금액을 환불하게 된다.

6) 다양한 형태로의 이용이 가능한 지불 시스템

Challenge semantics라고 불리는 개념을 근간으로 해서 효율적인 기능 확장이 가능하다.

그 적용 가능한 범위로는 첫째, 분할 가능한 현금으로의 확장이 가능하며, 전자수표나 신용카드로의 확장이 가능하고 공정한 상호 교환도 달성할 수 있다. 또한 지불 효과가 특정사건의 발생과 연관되어 질 수 있는 Event triggered 지불 시스템에 적용이 가능하다. 효율성 측면에서 고려할 때 사용자는 현금이 사용된 횟수와 은행과 옴버즈맨의 서명 값 (x, s)만을 저장하고 있으면 되므로 기존에 k번 사용 가능한 전자현금 프로토콜과 비교해 볼 때 더 효율적이다.

바. Y. Frankel, Y. Tsiounis, M. Yung의 기법 [FTY96]

[FTY96]은 신뢰 기관이 프로토콜 수행에는 개입되어 있지 않지만, 앞으로 계좌의 추적이나 동전의 추적이 요구되는 경우 이에 대한 추적 가능성을 간접적이지만 효율적으로 증명할 수 있다는 "Indirect Discourse Proofs"의 개념을 제안하였다. 이 개념을 제안하기 위해 이들은 공정한 오프라인 전자화폐(Fair Off-Line e-Cash :FOLC) 시스템의 개념을 제시하고 있는데, 이는 동전이나 혹은 동전의 소유자를 식별하기 위한 추적 프로토콜을 말한다. 최근에 약탈과 돈세탁과 같은 악용 사례를 피하기 위해 소유자와 인출에 따른 동전을 추적하고 식별할 필요성이 대두되었다. 이러한 추적성을 보장하기 위한 기존의 해결책은 신뢰기관과 같은 제3의 기관을 돈의 인출단계에 개입시켰다. 반면, 공정한 오프라인 전자화폐는 어떠한 제3의 기관도 개입시키지 않는 "fully off-line e-cash"라고 할 수 있다.

이들이 제시한 프로토콜의 안전성은 Brands [Bra93]의 전자화폐 기법의 안전성을 기반으로 하고 있으며, 익명성을 보장하기 위해 이산대수 문제의 어려움에 대한 새로운 변형인 "matching Diffie-Hellman assumption"이라는 개념을 소개하고 있다.

익명의 오프라인 전자화폐를 확장한 개념이며, 은행(B), 사용자(U), 수신자(R), 그리고 신뢰기관(T)의 참여로 구성되는 공정한 오프라인 전자화폐는 다섯 가지의 기본적인 프로토콜을 포함하고 있다: 인출, 지불, 결제, 소유자 추적(owner tracing), 동전 추적(coin tracing). 소유자 추적 프로토콜. 소유자 추적 프로토콜은 특정 동전의 소유자의 신원을 추적하는 프로토콜을 말하며, 동전 추적 프로토콜은 인출 단계의 동전을 추적하는 프로토콜을 말한다. 소유자 추적 프로토콜은 의심스런 돈의 근원을 발견할 수 있기 때문에 돈세탁을 방지할 수 있도록 해주며, 동전 추적 프로토콜은 의심스런 돈이 인출된 행방을 찾도록 해준다.

이 논문에서 제시하고 있는 기본적인 프로토콜들은 Brands 기법을 변형한 것이며 동전 추적 프로토콜과 소유자 추적 프로토콜은 기본 프로토콜에 추가적인 단계를 더하므로써 신뢰기관과는 오프라인 형태를 유지하면서도 익명성 보장과 추적 가능성을 indirect discourse proof를 통해 증명해 보이고 있다. 또한 각 프로토콜의 단계별 검증과정과 안전성, 정확성 혹은 효율성 분석을 통해 공정한 오프라인 전자화폐의 개념을 소개하고 있다. 이 시스템은 스마트 카드에서 구현 가능하며 기존의 기법들과 비교해 볼 때 비교적 높은 안전성을 제공하고 있다.

프로토콜들의 기본 단계는 다음과 같다.

1) 은행의 설정 프로토콜

(1) 은행은 소수를 선택한다.

소수 p, q를 선택 : $|p-1| = \delta + \kappa$, δ는 특정 상수,

$p = \gamma q + 1$, r은 특정한 작은 정수

(2) 생성자와 비밀키를 생성한다.

G_q의 생성자 g, g_1, g_2 생성

비밀 키 $X_B \in_R Z_q$ 생성

(3) 해쉬 함수들을 정의한다.

H, H_0, H_1, ...,

(4) p, q, g, g_1, g_2, (H, H_0, H_1) 과 은행의 공개키 $h=g^{XB}$, $h_1=g_1^{XB}$, $h_2=g_2^{XB}$을 공개한다.

2) 사용자 설정 (계좌 개설) 프로토콜

(1) 은행과의 협조로 은행의 개인 계좌 정보 $I = g_1^{u1}$을 알고 있다.

$u_1 \in G_q$는 사용자 U에 의해 생성되며, $g_1^{u1} g_2 \neq 1$ 이어야 한다.

(2) 사용자는 Schnorr 개인 식별 기법을 이용하여 $z' = h_1^{u1} h_2 = (Ig_2)^{XB}$ 을 계산하는 것으로 g_1에 대한 I의 값을 알고 있음을 증명할 수 있다.

3) 인출단계

(그림 10)에서와 같이 Brands의 기법에서 제시하고 있는 I에 대한 제한적 은닉서명이 이용된다. 사용자는 자신이 선택하여 비밀값으로 유지하는 랜덤수 s를 이용하여 $(Ig_2)^s$에 대한 Schnorr 타입의 서명을 한다. 서명의 정확한 형태는 $sig(A, B) = (z, a, b, r)$이며, 이때 $g^r = h^{H(A,B,z,a,b)} a$ 과 $A^r = z^{H(A,B,z,a,b)} b$의 수식이 만족된다. 인출 프로토콜의 흐름은 다음과 같다. 사용자 U는 프로토콜의 마지막에서 $g^{r'} \stackrel{?}{=} h^{c'a'}$, $(Ig_2)r' \stackrel{?}{=} z'^{c'} b'$을 검증한다.

User		***Bank***
		$w \in_R Z_q$
$s \in_R Z_q$	a', b' ←	$a' = g^w$, $b' = (Ig_2)^w$
$A = (Ig_2)^s$		
$z = z'^s$		
$x_1, x_2, u, v \in_R Z_q$		
$B_1 = g_1^{x_1}$, $B_2 = g_2^{x_2}$		
$a = (a')^u g^v$		
$b = (b')^{su} A^v$		
$c = H(A, B, z, a, b)$		
$c' = c/u$	c' →	
$r = r'u + v \bmod q$	r' →	$r' = c' X_B + w$

(그림 10) 인출단계

4) 지불단계

(그림 11)에서 제시하고 있는 지불단계에서 사용자는 사용된 동전이 두 번 사용되었다면 사용자 U를 식별할 수 있도록 수신자에게 정보를 제공해주어야 한다.

여기서 만일 은행 B가 사용자 U를 추적할 수 있다면 이는 다음의 문제들을 풀 수 있다는 것을 증명하는 것이다. 즉, 랜덤한 a_i, b_i (i=0,1) 에 대한 안전 변수 k이 존재할 때, 주어진 $[g^{a_0}, g^{a_0 b_0}], [g^{a_1}, g^{a_1 b_1}]$과 $g^{b_r} g^{b_{1-r}}, r \in R \{0,1\}$에 대해서 충분히 큰 k에 대한 상수 c에

대해서 $1/2+1/k^c$보다 더 큰 확률로 r을 발견할 수 있다는 것을 제시하고 있으며 이와 같은 문제의 어려움을 matching Diffie-Hellman assumption이라 한다.

User		*Receiver*
$A_1 = g_1^{u_1 s}$		
$A_2 = g_2^s$	$a_1, A_2, A, B, (z, a, b, r)$ $\rightarrow$	$A \stackrel{?}{=} A_1 A_2,\ A \neq 1$
$sig(A,B) \stackrel{?}{=} (z, a, b, r)$		
$r_1 = d(u_1 s) + x_1$	d $\leftarrow$	$d = H_1(A_1, B_1, A_2, B_2, I_R, date/time)$
$r_2 = ds + x_2$	r_1, r_2 $\rightarrow$	$g_1^{r_1} \stackrel{?}{=} A_1^d B_1$
		$g_1^{r_1} \stackrel{?}{=} A_1^d B_1$

(그림 11) 지불단계

5) 소유자 추적

소유자 추적 프로토콜은 앞의 기본적인 지불 단계에 추가적인 기법들을 적용시킴으로써 영지식 증명을 이용하여 안전성과 정확성을 설명하고 있다. 역시 신뢰기관은 인출, 지불, 결제 단계 모두에 오프라인이다. 또한 이 단계는 수신자가 신뢰기관에 의한 신뢰성 여부를 판단하여 그에 따른 기법들을 구별하여 적용하고 있다. 수신자가 신뢰기관에 의해서 신뢰를 받을 경우 영지식 증명을 통해 안전성이 보장되는 것을 볼 수 있으며, 수신자가 신뢰기관에 의해 신뢰를 받지 못한 경우 최소 지식 증명과 Schnorr 지식 증명 등을 이용하여 이 기법의 안전성과 효율성을 설명하고 있다.

6) 동전 추적

인출단계에서, 사용자 U는 신뢰기관의 키를 기반으로 하는 ElGamal 암호화를 이용하여 지불단계에서 나타날 몇 가지 정보들을(예를 들면, $A_2 = g_2^s$) 암호화한다. 은행은 이 암호문을 검증하기 위해서 사용자 U에 의해서 제공되는 $A' = A'_1 A'_2$를 필요로 한다. 그런 다음 indirect discourse proof로 은행은 사용자 U가 A'_1에 포함된 수를 암호화했다는 것을 검증할 수 있다. 결과적으로 은행은 Brands의 제한적 내용은닉 서명을 이용하여 A′를 내용은닉 서명하게 되며, 이 서명은 즉, 사용자가 A′에 관련된 내용들을 암호화했음을 은행이 점검했음을 보여주는 것이다.

수신자는 이제 지불단계에서 이 서명을 검증하고 A′에 포함된 정보가 A_2임을 검증한다. A_2는 인출단계에서는 숨겨져 있으므로 지불단계에서 검증이 수행되는 것이다. 이와 같은 수신자의 검증은 결제단계에서 은행에 의해서도 행해진다.

동전 추적 프로토콜 또한 모든 단계에서 신뢰기관은 오프라인을 유지한다. 단지 서명이 요구되어 값을 확인해야 하는 경우에만 사용자, 은행, 수신자에 대한 부담을 최소화시키기 위해 신뢰기관에 의해 해당 값이 공개 될 수 있다.

5. 기존의 전자현금 프로토콜의 비교

본 장에서는 기존의 전자현금 프로토콜에 사용된 기법을 <표 1>과 같이 비교하고, 각 프로토콜이 요구 사항에의 만족 여부를 <표 2>에 비교하였다. [CFN88]에서 제안하고 있는 전자현금 프로토콜에서는 익명성 확보 및 이중 사용 검출을 위하여 은닉서명과 Cut-and-Choose방식을 활용하고 있으나 계산량 및 은행과 고객 그리고 고객과 상점간에 전달되는 정보의 양이 너무 많고 이중사용 검출을 위해 은행이 저장하여야할 거래 정보가 너무 많아 현실에 적용하여 구현하기에는 어려운 점이 있다.

이에 전달되는 통신 량을 줄이기 위해 적은 정보량만으로도 이중사용 검출이 가능한 단항 오프라인 전자현금 시스템이 [Fer93], [Bra93], [CPS93]등에 의해 제시되었다. [Fer93]에서는 익명성 확보를 위해 RSA를 근간으로 한 은닉서명 기법을 채택하고 있으며 단항 방식에 의한 이중사용 검출을 가능하게 하는 방법을 제시하고 있으나 그 안전성에 대해서는 입증되지 않고 있다. 비슷한 시기에 군 표현문제 및 단항 방식의 채택으로 효율성을 향상시킨 기법이 [Bra93]에서 제시되었다. 그러나 [Bra93]의 방식은 항상 변조 방지가 되어있는 스마트 카드의 사용을 전제로 하고 있으므로 이러한 조건이 위배될 경우 은행 모함 공격에 약해지는 문제점도 가지고 있다.

전자현금의 기능추가 측면에서는 [Oka95]에서 계층적 트리 구조를 채택한 분할 가능한 전자현금 프로토콜에 대해 Cut-and-Choose기법 및 단항 기법을 근간으로 한 프로토콜을 제시하였으며 최근 Y. S. Tsiounis등에 의해 연구되어지고 있는 정확한 지불에 대한 연구의 기초가 되고 있다. 지금 까지 제시된 대부분의 전자현금 프로토콜은 은닉서명 기법에 기반을 둔 완전한 익명 성을 만족하고 있으나 이는 범죄자에 의해 돈 세탁 및 약탈 등과 같은 범죄에 오용될 수 있으므로 필요시 익명성이 철회되어 질 수 있는 전자현금 프로토콜이 요구되게 되었다.

이에 [CPS96]에서 제시한 기법은 군 표현 문제와 이산대수 문제를 바탕으로 하였으며, Schnorr의 서명기법과 단항 방식을 이용하였다. 필요 시 신뢰기관의 도움을 받아 익명성이 철회될 수 있는 공정한 지불 시스템으로 구성되어졌으며 신뢰기관이 인출, 지불 및 예치거래에 직접 관여하지 않고 있어 효율적인 측면이 있다. 그러나 은행이 한 명의 고객을 위해 실명계좌와 익명계좌 두 개를 관리하여야 하고 다중지불을 방지하기 위하여 카운터를 사용하고 있으나 고객별 사용 빈도 수에 따른 적정 길이 및 순서 유지에 어려움이 있고 은행을 전적으로 신뢰하고 있다는 가정 하에 프로토콜이 구현되어 있으므로 은행의 모함 공격이 가능하게 되는 단점이 있다.

[JY96]에서 제시한 기법은 기존의 전자현금 시스템이 고려하지 않았던 은행 강탈 공격에 대해 견딜 수 있도록 고안되었으며 법원의 명령에 따라 현금 및 사용자 ID의 추적이 가능한 공정한 지불 시스템으로 설계되어졌다. 그러나 현금 인출단계에서 신뢰기관의 일종인 옴버즈맨이 개입되어 효율성 측면에서 기타 오프라인 전자현금 프로토콜에 비해 떨어진다고 할 수 있다. 또한 다중사용, 전자수표 및 신용카드, Event triggered 지불 시스템 등 다양한 적용이 가능하다고 설명하고 있는 challenge semantics의 경우는 구체적인 언급이 없어 이를 실제 구현하는 데는 어려움이 있을 것으로 생각된다.

또 다른 공정한 지불 시스템인 [FTY96]에서 의해 제시된 기법은 제한적 내용은닉 서명과 Schnorr 개인식별 서명 기법을 이용하였으며 신뢰기관이 프로토콜에 직접 온라인으로는 참여하지는 않지만, 익명성 보장과 그에 대한 역기능을 방지하기 위해 소유자 추적, 동전 추

적 프로토콜을 통해 신뢰기관이 익명성을 철회하는 것이 가능함을 보장한다. 이전에 제시되었던 공정한 전자화폐 시스템들은 신뢰기관이 온라인으로 개입되거나 최소한 인출단계에서는 신뢰기관의 개입이 요구되었으나, 이들의 기법에서 제시하고 있는 공정한 오프라인 전자화폐 시스템은 어떠한 신뢰기관의 개입도 요구하지 않는다. 이들의 기법은 특정한 동전의 소유자를 식별하기 위한 소유자 추적 프로토콜과 인출단계로부터 원래의 동전을 추적하는 동전 추적 프로토콜을 제시하고 있어 이러한 프로토콜들을 통해서 신뢰기관이 직접 프로토콜에 참여하고 있지 않아도 필요시 동전이나 소유자가 추적 가능함을 보여주는 indirect discourse proof의 개념을 제시하고 있다. 이 개념은 신뢰기관을 이용한 공정한 지불 시스템을 제시하는데 있어 신뢰기관이 온라인으로 개입하는 기존의 시스템에 비해 보다 속도와 효율성의 측면을 보다 향상 시켰다. 이들은 최근 [FTY98]에서 이 공정한 오프라인 전자화폐의 개념을 보다 쉽고 보다 향상된 효율적인 기법으로 제시하고 있다.

<표 1> 각 프로토콜들의 요구사항 비교

기법	특성 및 사용된 주요기술
[CFN88]	RSA, 해쉬함수, 영지식 증명, Cut-and-Choose
[OO91]	RSA, 소인수분해 문제, 해쉬함수, 계층적 트리 구조, Cut-and-Choose
[Fer93]	RSA, 해쉬함수, randomized blind signature, 단항 방식
[Bra93]	DLA, 해쉬함수, 단항 방식, 익명성, 이중사용 검출, 은행의 모함 공격에 대해 변조방지 장비의 안전성에 의존
[Oka95]	Bit Commitment, 계층적 트리 구조, 단항 방식
[CPS96]	실명계좌 및 익명계좌 동시 개설, representation problem, Schnorr 서명기법(blind version), 이산대수 문제, 신뢰기관, 단항 방식
[JY96]	Dual verification signature, Challenge semantics, 옴버즈맨과 협력에 의한 현금발행, 단항 방식, 익명성 철회가능, 다중사용 가능, 전자수표 및 신용카드로 이용 가능, Event triggered 지불 시스템으로 적용 가능
[FTY96]	인출, 지불, 결제, 소유자 추적, 동전 추적의 프로토콜 제시, 스마트 카드에서 구현가능, 익명성 철회가능, 신뢰기관은 프로토콜에 오프라인 형태로 참여, 제한적 내용은닉 서명, Schnorr 개인식별 및 서명 기법

<표 2> 각 프로토콜의 특성 및 주요기술 비교

요구사항 / 기법	익명성	이중사용검출	오프라인	양도성	분할성	익명성 철회가능	초과사용방지	Bank robbery	Bank framing	동전추적	소유자추적
[CFN88]	○	○	○	×	×	×	×	×	×	×	×
[OO91]	○	○	○	○	○	×	×	×	×	×	×
[Fer93]	○	○	○	×	×	×	×	×	×	×	×
[Bra93]	○	○	○	×	×	×	×	×	×	×	×
[Oka95]	○	○	○	○	○	×	×	×	×	×	×
[CPS96]	○	○	×	×	×	○	○	×	×	×	×
[JY96]	○	○	○	×	×	○	○	○	○	×	×
[FTY96]	○	○	○	×	×	○	×	×	×	○	○

6. 결론

본 논문에서는 기존에 제시된 다양한 전자현금 프로토콜에 대해 분석하여 각 프로토콜들이 만족하는 요구사항들을 제시하였다. 전자현금의 초기 프로토콜들은 오프라인성이나 추적불가능성, 이중사용 방지 등을 중심으로 한 연구가 진행되었고 특히 이중 사용방지를 위한 보다 효율적인 방법들을 찾아내는 데 연구의 초점이 맞추어져 왔다. 그러나 최근에는 정확한 지불 및 은행 모함 등과 같은 은행 강탈 공격 등에 관한 연구를 통해 보다 실용적인 측면이 강조된 전자현금 프로토콜이 제시되었다. 본 논문에서는 기존에 제시된 전자현금 프로토콜들에 대한 분석을 통하여 새롭게 제시되는 전자현금 프로토콜이 가져야 할 요구사항을 제시하였다. 앞으로 여기서 제시한 기본 요구 사항을 포함하여 선별적인 추가 요구사항을 만족하는 전자현금 프로토콜에 대한 연구가 계속적으로 이루어져야 할 것이다.

참고 문헌

[Cha83] D. Chaum, "Blind Signature Systems," Advances in Cryptology-Proc. of CRYPTO'83, Springer-Verlag, pp. 153, 1983.

[CFN88] D. Chaum, A. Fiat and M. Noar, "Untraceable Electronic Cash," Advances in Cryptology-Proc. of CRYPTO'88, LNCS, Vol. 403, Springer-Verlag, pp.319-327, 1989.

[CB89] D. Chaum, B.d. Boer, E.v. Heyst, S. Mjolsnes and A. Steenbeek, "Efficient offline Electroic Checks," Advances in Cryptology-Proc. of EUROCRYPT'89, LNCS, Vol. 434, Springer-Verlag, pp.294-301, 1990.

[OO91] T. Okamoto and K. Ohta, "Universal Electronic Cash," Advances in Cryptology-Proc. of CRYPTO'91, LNCS, Vol. 576, Springer-Verlag, pp.324-337, 1992.

[Fer93] Niels Ferguson, "Single Term Off-Line Coins," Advances in Cryptology-Proc. of EUROCRYPT'93, LNCS, Vol. 765, Springer-Verlag, pp.318-328. 1993.

[Bra93] S. Brands, "Untraceable Off-line Cash in Wallets with Observer," Advances in Cryptology-Proc. of CRYPTO'93, LNCS, Vol. 773, Springer-Verlag, pp.302-318, 1993.

[Oka95] T. Okamotom, "An Efficient Divisible Electronic Cash Scheme," Advances in Cryptology-Proc. of CRYPTO'95, LNCS, Vol. 963, Springer-Verlag, pp.438-451, 1995.

[SPC95] M.Stadler, J-M Piveteau, J. Camenisch, "Fair Blind Signature," Advances in

Cryptology-Proc. of EUROCRYPT'95, LNCS, Vol. 921, Springer-Verlag, pp.209-219, 1995.

[CPS96] J. Camenisch, J. M. Piveteau, and M. Stadler, "An Efficient Fair Payment System," Proc. of the third annual ACM-CCS, pp. 88-94, March 1996.

[JY96] M. Jakobsson and M. Yung, "Revokable and Versatile E-money," Proc. of the third annual ACM-CCS, pp. 76-87, March 1996.

[FTY96] Y.Frankel, Y. Tsiounis, and M. Yung. "Indirect Discourse Proofs : Achieving Fair Off-line E-cash", Advances in Cryptology-Proc. of ASIACRYPT'96, LNCS, Vol. 1163, Springer-Verlag, pp. 286-300, 1996.

[Tsio97] Yiannis S. Tsiounis, Efficent Electronic Cash, "New Notions and Techniques," Ph.D. Thesis, June 1997. Northeastern University.

[FTY98] Y.Frankel, Y. Tsiounis, and M. Yung. "Fair Off-line e-cash Made Easy", Advances in Cryptology-Proc. of ASIACRYPT'98, LNCS, Vol. 1514, Springer-Verlag, pp. 257-270, 1998.