전자화폐의 역기능을 고려한 전자화폐시스템 모델

°권성호*, 이성우*, 송유진**, 홍기융***, 신재호*
*동국대학교 전자공학과, **정보산업학과, ***한국정보보호센터

A electronic cash system model considering crime-prevention

°Sungho Kwon*, Sungwoo Lee*, Yujin Song**, Kiyung Hong***, Jaeho Shin*,
Department of Electronics*, Department of Information Industries**, Dongguk University
Korea Information Security Agency***
ekdsk@cakra.dongguk.ac.kr

요 약

본 논문에서는 향후 전자상거래 시대를 대비하여 전자화폐의 역기능을 검토하고 국제결제은행(BIS)의 전자화폐시스템 모델과 일본 NTT의 전자화폐시스템 모델을 분석하였다. 그리고 전자화폐의 역기능에 대처할 수 있는 요구조건을 만족하는 전자화폐시스템 모델을 제안한다.

제 1 장 서 론

최근 정보통신기술의 발전과 인터넷 사용의 폭발적인 증가로 인해 디지털 정보와 정보통신망을 이용한 전자상거래의 움직임이 활발히 진행되고 있다. 이러한 인터넷상의 전자상거래에 의해 새로운 전자지불 수단의 필요성과 안전한 전자지불을 실현하기 위한 수단으로 전자화폐가 등장하게 되었다.

전자화폐는 디지털 정보이기 때문에 데이터로서의 취급이 용이한 반면에 암호기술에 의한 위조 대책이 필요하고, 사용자의 지불이력이 수집 관리되는 등의 사용자의 프라이버시가 침해될 위험성이 생길 수 있기 때문에 보다 익명성이 높은 전자화폐시스템이 요구되어 왔다. Chaum, Fiat, Naor[9]등이 오프라인 전자화폐 시스템 제안 이후로 완전한 익명성을 제공하여 사용자의 프라이버시를 보호하는 방향으로 연구가 진행되고 있다. 그러나 완전한 전자화폐의 익명성 때문에 추적이 불가능하게 되어 돈세탁, 탈세, 유괴, 협박등

과 같은 범죄에 악용될 수 있는 역기능이 생기게 되었다. 그래서 이러한 전자화폐의 역기능에 대응하기 위해서 강제적으로 익명성을 취소할 필요가 생겼고 익명성 취소기능을 실현하기 위해 은행과 별도로 신뢰할 만한 제3기관(수탁기관, Trustee, Trusted Third Party)이 법원으로부터 발부된 수사영장 제시 등의 조건이 만족되면 은행과 협조하여 전자화폐의 익명성을 취소하거나 부정한 전자화폐를 추적할 수 있게 되었다. 그래서 본 논문에서는 향후 전자상거래 시대를 대비하여 전자화폐의 역기능을 분석하고 이러한 역기능에 대처할 수 있는 요구조건을 만족하는 전자화폐시스템 모델을 제시하고자 한다. 본 논문은 2장에서 전자화폐의 개념과 요구조건에 대해 설명하고, 3장에서는 국제결제은행(BIS)의 전자화폐시스템 모델과 일본 NTT의 전자화폐시스템 모델을 분석하고, 4장에서는 전자화폐의 역기능을 검토하여 이러한 전자화폐의 역기능을 고려한 전자화폐시스템 모델을 제안하고 5장에서 결론을 맺는다.

제 2 장 전자화폐 개념 및 요구조건

2.1 전자화폐의 개념

전자화폐란 액면가치를 보증하기 위해 은행이 서명한 디지털화된 가치정보로 인터넷 등의 네트워크상에서 지불이 요구되는 정보화 시대의 지불수단으로 대두되었다. 전자화폐는 정보 그 자체가 가치를 갖기 때문에 현실의 화폐에 비교해서 쉽게 복사, 위조될 가능성이 있다. 그래서 전자화폐를 안전하게 실현하는게 중요한 전자화폐의 과제이다.

2.2 전자화폐의 요구조건

일반적으로 전자화폐는 다음과 같은 요구조건을 만족해야 한다.

- 완전 정보화 : 완전하게 정보만으로서 실현되는 것
- 재사용 불가능성 : 복사, 위조등으로 인한 부정 이용을 할 수 없는 것
- 추적불가능성(프라이버시) : 이용자의 구매에 관한 프라이버시가 상점이나 은행이 결탁해도 노출되지 않는 것
- 오프라인성 : 상점에서의 지불시, 처리를 은행의 개입없이 처리할 수 있는 것
- 양도성 : 중간에 은행을 거치지 않고 직접 전달이 가능한 것. 타인으로부터 화폐를 전달 받은 후 은행을 통하지 않고 제3자에게 다시 전달할 수 있는 것
- 분할성 : 합계금액이 액면 금액이 될 때까지 분할해서 사용할 수 있는 것
- 위조불가능성 : 위조화폐를 발행할 수 없어야 하며 어느 한쪽이 거래 사실을 부인할 경우 그 진위여부를 판명할 수 있을 것

제 3 장 전자화폐시스템 모델

3.1 국제결제은행(BIS) 전자화폐시스템 모델

BIS(Bank for International Settlement)는 전자화폐시스템을 일반모델과 샘플모델 2가지로 구분하고 있다.

3.1.1 일반모델

BIS 전자화폐시스템 모델에서는 다음과 같이 3가지의 독립된 영역을 정의하고 있다.

- 결제 영역 : 이 영역에서는 금융기관 Clearing house 및 경우에 따라서는 중앙은행이 전자적 가치를 거래한 결과 생기는 은행간의 금융거래에 대하여 결제를 행한다.
- 발행, 회수, 운용 영역: 이들 영역에서는 전자적 가치의 발행과 회수, 및 결제 영역과의 교환을 행한다.
- 소액결제영역: 이 영역에서는 사용자간에 다음과 같은 가치 이전이 행하여진다.
  - 충전: 발행기관으로부터 사용자에게 가치이전
  - 지불: 사용자간 가치전송
  - 예금: 사용자로부터 발행기관 또는 회수기관으로 가치이전

3.1.2 샘플모델

BIS는 단순화한 2가지 전자화폐시스템 모델을 제시하고 있다. 하나는 소비자간의 가치이동을 자유로이 할 수 있는 단일 발행 기관 모델과 다른 하나는 소비자간의 가치이전 가능한 복수 발행기관 모델이다.

먼저 단일 발행기관 모델 (그림.2)에 있어서 전자적 가치의 흐름은 발행기관(중앙은행), 은행, 소액결제시스템이 함께 관여하는 기존의 현금결제의 흐름과 유사하다. 먼저 단일 발행기관이 전자적 가치를 창조해서 그것을 참가기관(통상은행)에 발행하고 이들 기관은 전자적 가치를 고객(소비자)의 장치에 충전한다. 소비자는 이 전자적 가치를 지불을 위해 사용하고, 소매업자와 소비자는 이 자금을 은행(참가기관)에 맡긴다. 이 가치에 대하여 발행기관에 회수요구를 한다. 전자적 가치의 이동 결과 생기는 은행간의 지불(발행 및 회수)은 결제영역 내에서 최종적으로 결제된다.

위와 같은 모델에서 통상 발행기관은 시스템 운용기관이기도 하고 참가기관은 회수기관(통상은 은행)의 역할도 하게 된다.

소액 결제영역에서의 소비자는 소비자간(전자지갑간 거래) 또는 소매업자에 대해 자유

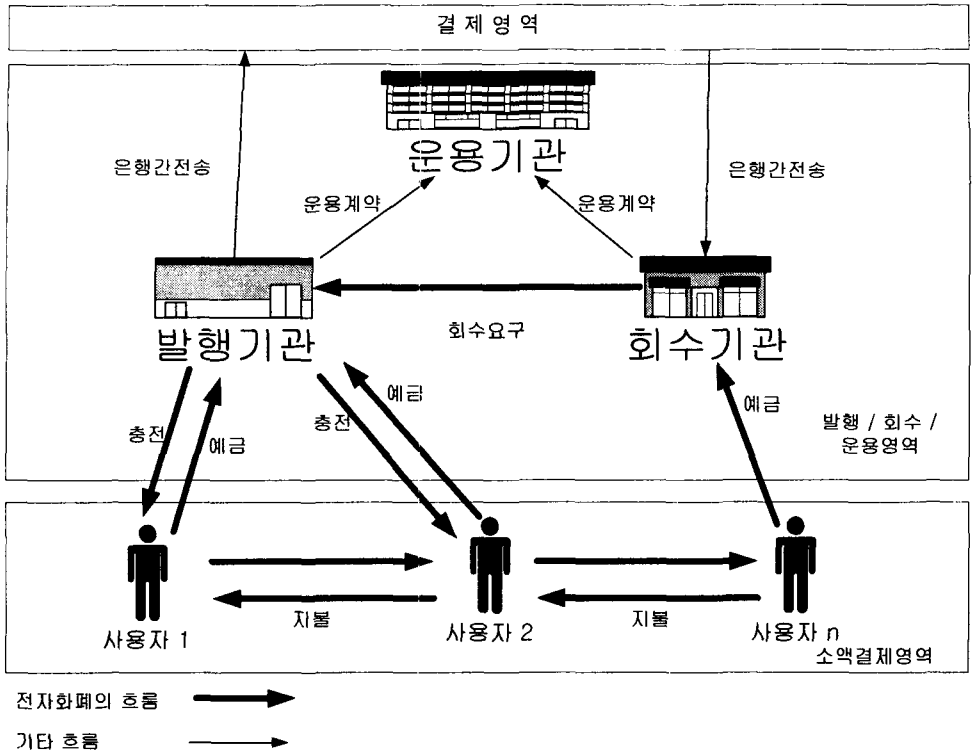


그림.1 BIS 전자화폐시스템 일반모델

로이 가치를 이전할 수 있지만 소매업자는 지불로써 수취한 전자적 가치를 예금할 의무가 있다.

복수발행기관 모델(그림.3)의 발행/회수/운용영역에 있어 중요한 구성요소는 발행기관, 회수기관 및 운용기관이다. 그림.3 에서는 명확하게 발행기관 회수기관을 구분하고 있지만 같은 기관이 발행기관이면서 동시에 회수기관인 경우가 많다.

각각의 발행기관이 전자화폐를 작성하고 그것을 고객(소비자)에게 발행한다. 소매업자는 소비자로부터 지불을 수취하고, 그 자금을 회수기관에 예금한다. 운용기관은 발행기관에 대해 회수 요구를 회수기관으로부터 받아 그들의 회수요구를 발행기관마다 모아서 관련정보와 함께 발행기관에 이전한다. 이들의 회수요구결과 생기는 은행간의 지불은 결제영역에서 최종적으로 결제된다.

소액결제영역에서 소비자가 보유하고 있는 전자적 가치는 소매업자와의 거래용만으로 사용할 수 있고 소매업자가 회수한 전자적 가치는 회수기관에만 예금할 수밖에 없다. 소비자는 전자적 가치를 발행기관에 예금하는 것이 가능하다.

그림 3은 단일 운용기관이 발행할 수 있는 기능을 나타낸 것이지만 운용기관의 역할은 아주 다양하고 복수의 운용기관을 갖는 경우도 있다

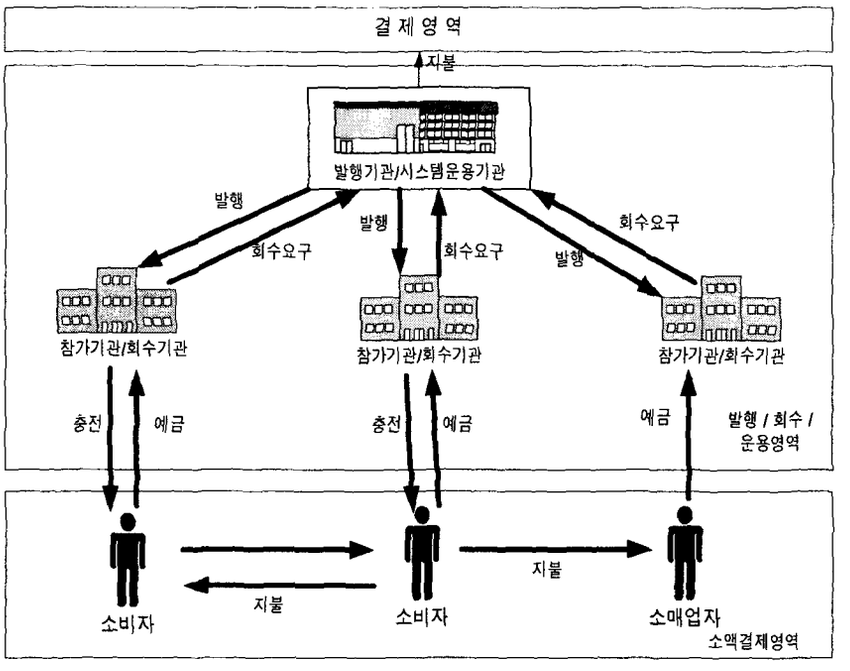
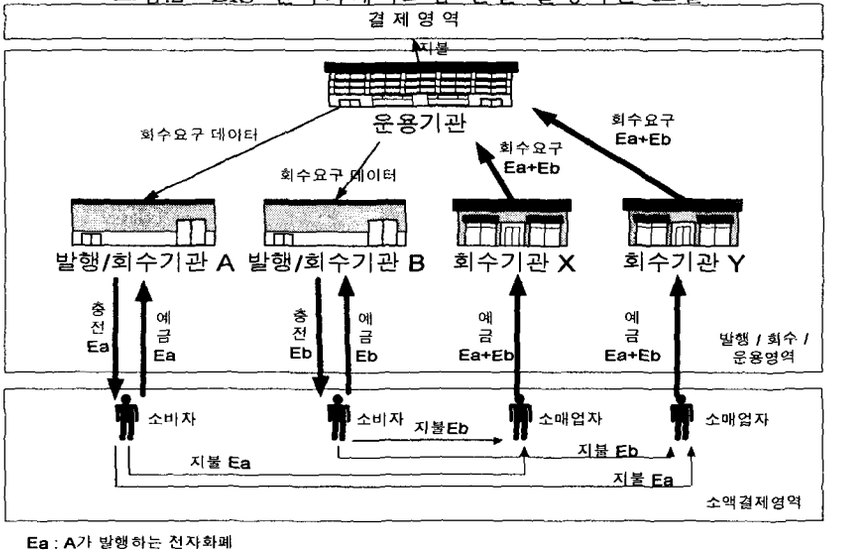


그림.2 BIS 전자화폐시스템 단일 발행기관 모델



Ea : A가 발행하는 전자화폐

Eb : B가 발행하는 전자화폐

그림.3 BIS 전자화폐시스템 복수발행기관 모델

3.2 NTT 전자화폐시스템 모델

NTT 전자화폐는 일본은행금융 연구소와 NTT 정보통신 연구소의 공동연구성과를 활용하여 개발된 전자화폐시스템이다. 이 시스템은 복수 금융기관에 공통적인 전자화폐의

발행이 가능하고 부정방지와 부정검출등의 보안기능과 전자화폐의 분할·양도 기능을 제공한다.

NTT 전자화폐시스템의 전체 구성은 아래의 그림(그림.4)과 같다

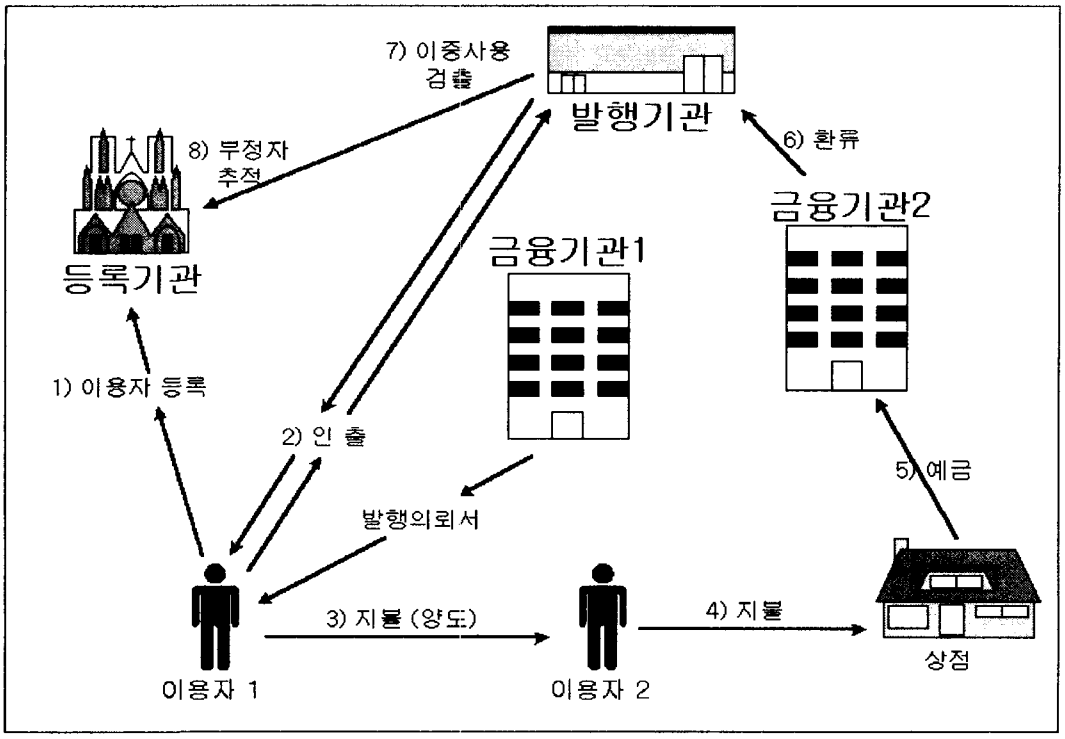


그림.4 NTT 전자화폐시스템 모델

등록기관은 이용자가 전자화폐를 사용하기 위해 미리 등록을 하기 위한 기관이고 이용자의 부당성을 보증하는 것이다. 발행기관은 전자화폐의 「발행」,「관리」,「부정사용 검출」을 행하는 기관이다. 전자화폐는 금융기관이 개별적으로 발행하는 것이 아니고 발행기관이 공통의 전자화폐를 발행할 수 있는 방식으로 하고 있다.

이용자 등록처리부분은 전자화폐를 이용할 때에 필요하게 되는 등록서를 작성하는 부분이다. 등록서는 이용자 공개키, 등록기관의 디지털 서명으로 구성된다.

전자화폐의 인출은 이용자가 금융기관 및 발행기관으로부터 전자화폐를 취득하는 부분이다. 전자화폐의 인출처리는 이용자 관점에서 금융기관으로부터 발행의뢰서를 취득하고 발행기관으로부터 전자화폐를 취득한다는 두 가지 단계를 밟는다.

전자화폐의 예금은 전자화폐가 어느정도 모아진 시점에서, 상점은 자신의 구좌에 파일 전송의 형태를 이용하여 입금한다.

전자화폐의 회수는 금융기관에서 발행기관으로 전자화폐을 송부하는 것이다.

부정검출의 메커니즘은 Tamper resistance가 있는 IC카드에 전자화폐정보를 격납하여 복사등의 부정을 방지하고 있다. 또 NTT 전자화폐는 칩내 메모리의 유출등에 의한

사태에 대비하여 부정검출, 부정자의 추적을 할 수 있는 장치를 소프트웨어적으로 실현하고 있다. NTT 전자화폐시스템의 특징은 다음과 같은 네가지이다. 첫째로 복수 금융기관에 공통적인 전자화폐의 발행이 가능하다. 둘째는 IC 카드의 시큐리티 구조에 의한 사전의 부정방지라는 사전대책, 소프트웨어에 의해 부정검출 추적이라는 사후대책을 겸용하여 안전성이 높다. 셋째로 프라이버시의 보호가 가능하다. 네번째로는 전자지폐형에도 상관없이 분할, 양도의 기능이 있다.

제 4 장 전자화폐의 역기능을 고려한 전자화폐시스템 모델

4.1 전자화폐의 역기능

전자화폐는 디지털 정보이기 때문에 데이터로서의 취급이 용이한 반면 암호기술에 의한 위조대책이 필요하고 사용자의 지불이력이 수집·관리되어 사용자의 프라이버시가 침해될 문제점이 있기 때문에 보다 익명성이 높은 전자화폐 방식이 요구되어 왔다. Chaum, Fiat, Naor등이 오프라인 전자화폐시스템 제안 이후로 대부분이 사용자의 프라이버시를 보호하기 위한 완전한 익명성을 강조하고 있다. 그러나 전자화폐의 완전한 익명성 확보는 돈세탁, 유괴, 협박, 은행강도와 같은 범죄에 악용될 소지가 있다. 그래서 돈세탁이나 강탈등의 범죄 행위에 대응하기 위해 강제적으로 익명성을 취소할 필요가 있다. 익명성 취소 기능을 실현하기 위해 은행과 별도로 신뢰할 만한 제3기관을 두어서, 법원으로부터 발부된 수사영장 제시등의 조건이 만족되면 제3기관은 은행과 함께 전자화폐의 익명성을 취소하거나 부정한 전자화폐 사용자를 추적할 수 있게 하는 것이다.

4.2 전자화폐 역기능을 고려한 전자화폐시스템 모델

기본 전자화폐시스템 모델에 역기능을 고려하여 추가되는 요소는 신뢰할 수 있는 제3기관인 수탁자이다. 즉, 사용자, 은행, 상점, 수탁자로 구성되는 익명성 전자화폐시스템 모델은 7개의 주요한 단계로 구분 가능하다.

- 초기화(Initialization) : 시스템변수의 선택과 모든 참가자의 키쌍들.
- 계좌 개설(Opening account) : 은행은 사용자 계좌를 개설하고 사용자의 개인 자료를 등록한다.
- 등록(Registration) : 사용자는 수탁자에게 등록한다.
- 인출(Withdrawal) : 사용자는 은행으로부터 전자화폐를 발급받는다.
- 지불(Payment) : 사용자는 그의 장치에 저장된 화폐를 사용하는 상점에 지불한다.
- 예금(Deposit) : 상점은 은행에 디지털 화폐를 예금하고 그에 따라 신용을 받게 된다.
- 취소(Revocation) : 수탁자는 인출이력으로부터 화폐의 형태를 산출할 수 있고 어떤

완전범죄를 막기 위해 지불 이력으로부터 사용자의 신분을 알 수 있다.

4.2.1 역기능을 고려한 전자화폐시스템에 대한 공격

전자화폐시스템에 행하는 공격은 다음과 같다.

• 사기성 있는 이용자(Fraudulent User)

- 초과사용(Overspending) : 사용자는 그들에게 허락된 가치를 초과하는 전자화폐를 사용한다.

• 사기성 있는 상점(Fraudulent Shop)

- 위장(Impersonation) : 상점은 사용자로부터 여러 번에 걸쳐 획득한 전자화폐를 재사용 또는 예금한다.
- 돈세탁(Money Laundering) : 상점은 불법적 행동을 통해 전자화폐를 획득한다. 그 돈의 출처를 숨기기위해 가공의 영수증을 발행한다.

• 사기성 있는 은행(Fraudulent Bank)

- 사용자 추적(Tracing a User) : 은행은 전자화폐와 사용자 사이의 관계를 추적한다.
- 수탁자의 협력하에 사용자 추적 : 화폐가 초과 사용되었다는 것에 대한 수탁자의 잘못된 유죄판결. 그 결과로 정직한 사용자가 이 화폐를 위해 그의 신분추적 후 범죄사실을 뒤집어 쓰게 된다.
- Framing a Shop : 잘못된 판결은 유용한 화폐의 이중 예치를 검출한다.
- Coin forgery after overspending : 은행은 이미 초과 사용한 화폐를 위해 가공된 지불이력를 산출해 낸다.

• 사기성 있는 수탁자(Fraudulent Trustee)

- Framing a User : 수탁자는 정직한 사용자를 잘못 정의한다. 그러므로 그 은행은 공정함없이 이 사용자에게 범죄를 뒤집어씌울 수도 있다.

• 사기성 있는 외부인(Fraudulent Outsider)

사기성의 외부인은 수탁자에게 등록하거나 은행계좌를 가질지도 모른다.

- 전자화폐 위조(Coin forgery): 전자화폐 위조를 위한 3가지 공격이 있다.
  - Universal forgery : 지불이력을 아는 참가자는 유통가능한 화폐를 획득하기 위해 서명방식를 위조한다.
  - One-more forgery : n인출 프로토콜에 참여하는 참가자는 n+1개의 유효한 전자화폐를 획득한다.
  - Overspending forgery : 초과 사용된 화폐의 몇몇의 지불이력를 아는 참가자는 예치가능한 새로운 전자화폐를 위한 지불이력을 생산한다.
- Eavesdropping of coins or pesudonyms: 공격자들은 전자화폐를 획득하기 위해 인출, 지출 및 예치의 통신를 엿듣는다. 능동적인 공격자는 또한 중간자처럼 행동하고 프로토콜 자료를 수정할 지도 모른다.

- 사용자로부터 전자화폐의 절도나 강탈(Theft or extortion of coins from the user) : 공격자는 사용자의 장치로부터 화폐이력을 훔치거나 사용자에게 그의 계좌로부터 화폐를 인출하도록 강요한다. 그리고 나중에 그 돈을 사용하기 위해 사용자로부터 인출된 돈을 공격자의 장치에 전송하도록 강요한다.
- 상점으로부터 전자화폐의 절도나 강탈(Theft or extortion of coins from the shop) : 공격자는 상점의 장치로부터 아직 전자화폐를 예금하지 않은 transcript를 훔치거나 transcripts를 공개할 것을 강요한다.
- 비밀키의 절도나 강탈(Theft or extortion of secret keys) : 공격자는 은행시스템을 해킹함으로서 또는 공개하도록 함으로서 은행(사용자/수탁자)의 비밀키를 훔친다. 공개하도록 하는 경우에 있어서 은행(사용자/수탁자)은 공격이 발생했고 도둑에 의한 것이 아니라고 생각한다. 만약 이 공격이 사용자에게 발생한다면 공격자는 전자지갑을 훔칠 수 있다. 사용자의 비밀키가 그의 tamper proof H/W(위조증명 하드웨어)장치에 저장되었기 때문에 만약 공격자가 POS터미널이나 염탐하는 것을 (Spying)을 수정함으로서 사용자의 PIN을 획득한다면 강탈이 가능해 질 수 있다.
- Blindfolding : 공격자는 전자화폐를 획득하기 위해 은행이 blindfolded 프로토콜을 사용할 것을 강요한다.

이러한 공격들은 은행과 상점이나 사용자와 상점 같은 몇몇의 참가자들의 결탁에 의해 수행될 수 있다. 사기성의 외부인(Fraudulent Outsider)은 공격들 중 한가지를 수행하기 위해 은행과 사용자 또는 은행과 수탁자와 같은 몇몇의 참가자들을 즉각 공격할 지도 모른다.

4.2.2 역기능을 고려한 전자화폐시스템의 요구조건

역기능을 고려한 전자화폐시스템은 다음과 같은 요구조건이 필요하다.

- 위조 불가능성(Unforgeability) : 단지 은행과 같이 권한이 부여된 참가자만이 전자화폐를 발행할 수 있다.
- 추적불가능성(Untraceability) : 전자화폐와 사용자 사이의 관계는 권한이 부여된 취소(익명성 취소)의 경우를 제외하고는 은행이 추적할 수 없다.
- 연결불가능성(Unlinkability) : 동일 사용자가 사용한 다른 전자화폐는 연결 불가능하다.
- Framing : 어떤 사용자나 상점도 은행이나 수탁자에 의해서 그릇되게 고소되어 질 수 없다. 능동적인 도청공격자(eavesdropper attacker)로 부터 사용자를 보호하기 위해 필요하다면 모든 통신는 근거가 있고 믿을 수 있어야 한다.
- 초과사용 추적(Overspent-tracing) : 은행은 전자화폐를 초과 사용한 사용자의 신분을 결정할 수 있다. 그것은 분리된 메커니즘이나 사용자 추적과 같은 방식으로 사용되어진다.

- 사용자 추적(User-tracing): 은행과 수탁자는 사용된 전자화폐와 사용자를 연결시키기 위해 협동한다.
- 화폐추적(Coin-tracing) : 은행과 수탁자는 사용될 전자화폐와 예치된 전자화폐와 관련된 정보로 일치하는지를 계산하기 위해 협동한다. 어떤 시스템에서는 전자화폐가 강탈당한 후 필요한 정보를 사용자 자신이 공개하는 것이 가능할 지도 모른다.
- 강탈추적(Extortion-tracing) : 은행과 수탁자는 사용된 또는 예치된 전자화폐의 일치를 허락하는 정보를 계산하기 위해 협동한다.

4.2.3 역기능을 고려한 전자화폐시스템 모델

역기능을 고려한 전자화폐시스템 모델의 구성도는 그림.5와 같다.

등록기관은 이용자가 전자화폐를 사용하기 위해 미리 등록을 하기 위한 기관이고, 이용자의 정당성을 보증하는 것이다.

발행기관은 전자화폐의 「발행」,「관리」,「부정사용 검출」을 행하는 기관이다. 전자화폐는 금융기관이 개별적으로 발행하는 것이 아니고 발행기관이 공통의 전자화폐를 발행할 수 있는 방식으로 하고 있다. 수사기관은 등록기관의 도움을 얻어서 부정사용자를 추적한다.

금융기관은 발행의뢰서를 이용자에게 발행해 주고 그 금액에 해당하는 금액을 이용자의 계좌로부터 발행기관으로 이체를 한다.

이용자는 금융기관으로부터 얻은 발행의뢰서를 발행기관에 제출하여 전자화폐를 발행받는다. 이렇게 발행받은 전자화폐를 다른 이용자에게 양도하거나 상점에서 상품을 구입하는데 사용한다. 상점에서는 이용자에게로부터 받은 전자화폐를 은행에 입금하여 실물화폐로 전환한다. 상점으로부터 입금받은 전자화폐는 다시 발행기관으로 환류되고 발행기관은 이에 해당하는 금액을 금융기관에 돌려 준다.

발행기관에서 이중 사용이 검출이 되면 이를 등록기관에 보내고 등록기관은 다시 수사기관과 협력하여 부정 사용자를 추적하게 된다. 여기서 익명성이 파괴된다.

제 5 장 결 론

본 논문에서는 전자화폐가 가지고 있는 역기능을 검토하고 역기능에 대응하기 위한 전자화폐시스템의 요구조건을 살펴보았다. 그리고 국제결제은행과 일본 NTT의 전자화폐시스템 모델을 분석하여 전자화폐의 역기능을 고려한 전자화폐시스템 모델을 제안했다. 향후 제안한 전자화폐시스템 모델을 토대로 구체적인 각 참여자들 간의 프로토콜과 기능에 대한 논의와 연구가 진행되어야 할 것이다.

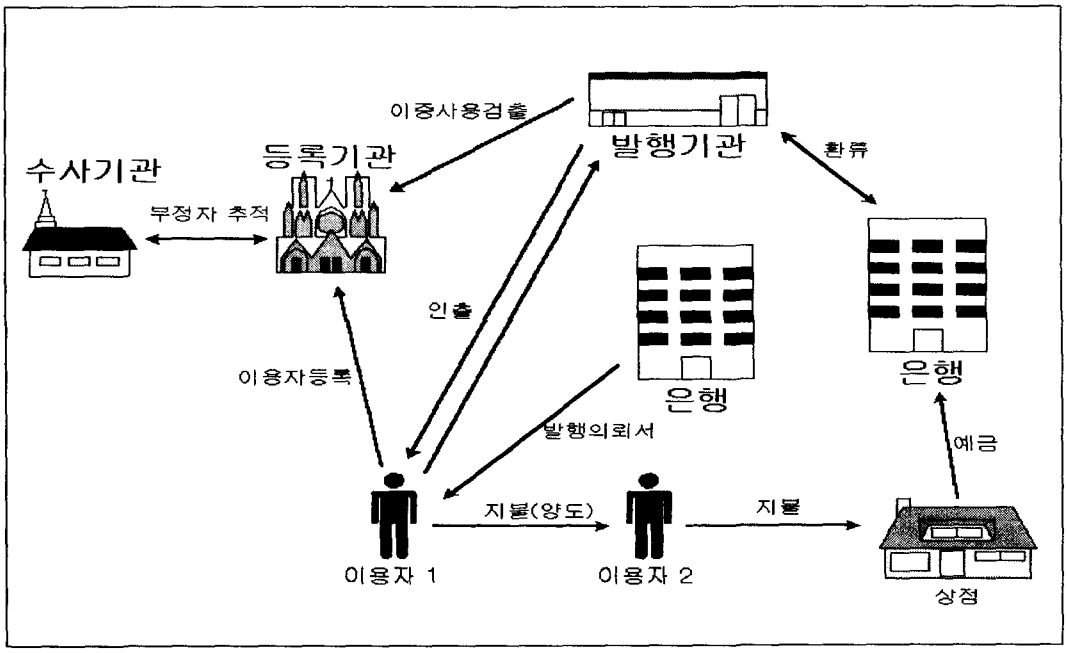


그림.5 역기능을 고려한 전자화폐시스템 모델

[참고문헌]

[1] Security of Electronic-money, Bank for International Settlement, 1996.

[2] S. Brands, "Untraceable off-line Cash in Wallets with Observers," Proceedings of Crypto '93, pp. 302-318, 1993.

[3] S. Brands, "An efficient off-line electronic cash system based on the representation problem," Technical Report CS-R9323, CWI (Centre for Mathematics and Computer Science), Amsterdam, 1993.

[4] E. Brickell, P. Gemmell, D. Kravitz, "Trustee-based Tracing Extensions to Anonymous Cash and the Making of Anonymous Change," Proceedings of Cryto '93, pp.302-318, 1993.

[5] J. Camenisch, U. Maurer, M. Stadler, "Digital Payment Systems with Passive Anonymity -Revoking Trustees," Cumputer Security - ESORICS '96, pp.33-43, 1996.

[6] J. Camenisch, J-M. Piveteau, M. Stadler, "An Effcient Fair Payment System," 3rd ACM Conference on Computer and Communications Security, pp.88-94, 1996.

[7] D. Chaum, "Blind Signatures for Untraceable Payments," Advances in Cryptology - Proceedings of Crypto '82, pp.199-203, 1983.

[8] A. Chan, Y. Frankel, P. MacKenzie, and Y. Tsiounis, "Mis-representiation of

identities in e-cash schemes and how to prevent it. In Advances in Cryptology," Proceedings of Asiacrypt '96 (Lecture Notes in Computer science 1163), pp. 276-285, Springer-Verlag, Nov. 1996.

[9] D. Chaum, A. Fiat, and M. Naor, "Untraceble Electronic Cash," Advances in Cryptology - Proceedings of Crypto '88, pp.319-327, 1988.

[10] D. chaum, and T.P. Pedersen, "Wallet databases with observers," In E. Brickell, editor, Advances in Cryptology - Crypt '92, proceedings (Lecture Notes in Computer Science), pp. 90-106, Springer-Verlag, 1993.

[11] Fujioka, Okamoto, Practical escrow cash, CCS96, 1996.

[12] Y. Frankel, Y. Tsiounis, and M. Yung, "Idirect discourse proofs: achieving fair off-line e-cash," In advances in Cryptology, Proc. of Asiacrypt '96 (Lecture Notes in Computer Science 1163), pp 286-300, Springer-Verlag, Nov. 1996.

[13] 전자지불시스템 요구사항(한국전산원 번역), St.Gallen 대학교 경영정보연구소, 1996.

[14] M. Jakobsson and M. Yung, " Revokable and Versatile Electronic Money," 3rd ACM Conferenceon Computer and Communications Security, pp.76-87, 1996.

[15] M. Jakobsson, and M. Yung, "Distibuted 'Magic Ink' Signatures," Eurocrypt '97, 19??.

[16] 전자지불 표준동향 분석에 관한 연구보고서, 한국전산원, 1998.6.

[17] 한국형 전자화폐를 활용한 유통시스템 모델 연구, 한국정보통신진흥협회. 1997.12.

[18] NTT 전자화폐시스템 보고서, NTT 정보통신연구소, 1997.

[19] T. Okamoto, and K. Ohta, "Universal Electronic Cash," Advances in Cryptology-proceedings of crypto '91, pp.324-337, 1992.

[20] T. Okamoto, "An Efficient Divisible Electronic Cash Scheme, "Crypto '95, pp.438-451 1995.

[21] H. Petersen, G. Poupard, Efficient Scable Fair Cash with off-line Extortion Prevention, Technical Report, 1997.

[22] S. von Solms, and D. Naccache, "On Blind Signatures and Perfect Crimes," Computers and Security, pp.581-583, 1992.11.

[23] M. Stadler, J-M. Piveteau, J. Camenisch, "Fair Blind Signatures," Advances in Cryptology - Proceedings of Eurocrypt '95, 1995.