通信情報保護學會誌
第7卷 第3號, 1997. 9

전자화폐 기술과 연구동향

Technology and Trend of Electronic Cash

송 유 진*, 강 창 구**

1. 서 론

최근 인터넷의 급속한 확대와 정보처리 기술의 발전과 함께 인터넷상의 거래나 정보서비스를 제공하는 사이버 비지니스가 급증하고 있다. 이러한 사이버 비지니스로서 디지탈 도서관이나 소프트웨어 이용에 대한 새로운 상품과 판매형태가 제공되어 있고 향후 컴퓨터 네트워크의 발전에 따라 상거래 회수가 크게 증가할 것으로 예측된다. 예를 들면, 백과사전 1페이지를 100원으로 판매하는 등 소액의 거래 형태가 주류를 이룰 것이며 현금을 대신하는 전자화폐는 소액거래에 대한 지불수단으로서 주목되고 있다. 또한, 전자화폐는 CALS/EC 등 디지털 기술을 사용한 데이터의 교환에 의해 현실통화와 같도록 상품의 지불을 완료하는 전자상거래의 지불수단으로서 중요하다.

인터넷상의 전자상거래가 급속하게 부상하면서 전자지불 시스템 구축을 위한 움직임이 세계적인 규모로 행해지고 있다. 전자화폐도 이러한 전자지불시스템 구축의 일환으로서 DigiCash사, CyberCash사 등의 프로젝트나 영국의 도시은행을 중심으로 추진되고 있는 Mondex 등 다양한 실증실험이 이루어지고 있다.

전자화폐는 현대 암호기술의 가장 중요한 응용의 하나이고 종래 IC카드를 전자화폐의 지갑(전자 지갑)이라 하는 형태로 전자화폐가 널리 사용될 것으로 예상된다. 이때, 전자화폐는 여하한 물리 매체에도 의존하지 않고 정보 그 자체가 전자화폐가 되는 형태로 전자 지갑에 저장되는 형태가 가장 바람직하다. 전자화폐는 금전가치를 표현하는 전자데이터인 금액데이터를 암호화해서 IC카드 또는 PC에 저장하여 통신망을 통해 송수신되는 형태에 따라 실용화를 위한 2가지 커다란 흐름이 있다.

첫째, IC카드등 Tamper Resistant 장치를 이용하는 것이다. 여기서 Tamper Resistant란 장치내의 내부정보에 대한 부정한 읽기/기록이 불가능하다는 의미로서 소유자일지라도 데이터의 부정 사용이 곤란한 IC카드를 전자지갑으로서 사용하여 안전한 전자 화폐를 실현하려고 하는 것이다. Mondex가 그 대표적인 예이다.

둘째, 완전한 소프트웨어로 전자화폐를 실현하려는 것으로서 하드웨어의 안전성에 의존하지 않는다. 특별한 하드웨어가 불필요하므로 인터넷상의 전자상거래 지불수단에 활용할 수

* 동국대학교 정보산업학과
** 한국전자통신연구원

있다. 이러한 전자화폐로서는 ecash가 그 대표적인 예이다.

이러한 두 가지 형태의 전자화폐는 암호기술을 토대로 하고 있기 때문에 암호기술이나 디지털 서명 등을 이해하는 것이 전자화폐 기술을 이해하기 위한 요건이 된다.

본 논문에서는 2장에서 전자화폐의 필요성과 요구조건을 살펴보고 지불방식, 적용영역 등에 따라 전자화폐 방식을 분류한다. 3장에서는 전자화폐의 기본적인 프로토콜에 대해 검토하고 4장에서는 전자화폐 기술등 최근의 연구동향에 대하여 소개한다. 마지막으로 5장에서 결론을 맺는다.

2. 전자화폐의 요구조건 및 분류

2.1 전자화폐의 필요성과 요구조건

종이 또는 금속으로 만들어진 실물 화폐의 안전성은 동일한 재질의 입수가 곤란한 점, 투명성이나 고도의 인쇄, 제조기술이 필요한 점 등에 의해 유지되고 있다.

그러나, 실물 화폐의 결점은 정보화에 대응하기 곤란하다는 점이다. 즉, 종이(금속)이라는 물리 매체에 의해 실현되기 때문에 실제 사용시 그 물리적 이동을 전제로 하고 정보로써 취급하기 어렵다는 점이다. 여기서 인터넷 등의 네트워크상에서의 지불을 필요로 하는 사이버 비지니스의 지불 수단으로써 전자화폐의 필요성이 대두된다.

그럼 전자화폐란 무엇인가? 전자화폐는 액면가치를 보증하기 위해 은행이 서명한 디지탈 정보라고 정의할 수 있다. 이러한 전자 화폐는 어떠한 물리 매체에도 의존하지 않고 정보 그 자체가 가치를 갖는 형태로 전자지갑(워크스테이션,IC카드,개인휴대단말 등)에 저장되는 형태가 많다. 이같은 형태의 전자화폐는 통신 회선을 통해 자유롭게 전송할 수 있고 유통성, 편리성이 높은 시스템 실현을 가능하게 한다.

그러나 전자화폐의 속성인 디지털 정보 형태는 정보 그 자체가 화폐로서의 가치를 부여하기 위해 안전한 사용이 중요한 과제가 된다. 디지탈 정보는 쉽게 복사가 가능하고 또 아무런 흔적도 없이 변조도 가능하다. 즉 디지탈 정보를 전자 화폐로 사용하는 경우 현실의 화폐와 비교해 쉽게 복사, 위조될 가능성이 생긴다.

전자화폐를 안전하게 실현하기 위한 한가지 방법은 물리적인 수단에 의해 안전성을 보증하는 방법이다. 예를 들면 텔레폰 카드등의 자기카드는 카드상의 자기 상태를 다른 카드에 물리적으로 복사하는 것이 곤란한 점을 안전성의 근거로 하고 있다. 그러나 이러한 안전성의 조건은 현실의 자기카드 제조기술 수준의 추이에 의해 크게 변화될 수 있다. 또 다른 방법은 신용카드와 같은 전자 ID카드에 의해 사후 지불하는 방식이다. 이 방법은 보통의 화폐와는 이용형태가 다르지만 전자화폐와 유사하고 문서에 행하는 서명 대신에 디지탈 서명을 이용하는 것으로 정보화를 실현할 수 있고 그 지불 정보를 통신 회선으로 전송하는 장점을 갖는다. 그러나 이 방식의 단점은 현금 지불에 비교해서 사용자의 프라이버시가 보증되지 않는 점이다. 즉, 신용카드를 발행.관리하는 기관은 쉽게 사용자의 구매.지불 이력등을 입수할 수 있기 때문에 프라이버시 침해가 우려된다. 또한, 상점이 각 사용자의 구매시 관리 센타에 엑세스하는 것은 처리시간, 통신 비용, 관리센타에서의 온라인 처리비용 및 데이타베이스 유지관리 비용등을 고려하면 현실적인 해결책이라고 할 수 없다. 따라서 전자화폐 지불시 처리는 오프라인 형태가 바람직하다.

이상의 점을 고려하면 전자 화폐의 요구 조건은 다음과 같다.

- 완전 정보화 : 완전하게 디지털 정보만으로서 실현할 수 있는 것.
- 이중사용 불가능성 : 복사, 위조 등으로 인한 부정사용을 할 수 없는 것.
- 추적 불가능성(익명성) : 사용자의 구매. 지불에 관한 프라이버시가 상점이나 은행이 결탁해도 노출되지 않는 것.
- 오프라인성 : 거래시 고객과 상점 이외 제삼자(예를들면, 은행)이 개재하지 않고 상점에서의 지불을 처리할 수 있는 것.
- 양도 가능성 : 사용자가 전자적으로 다른 사용자에게 현금 가치의 이동이 가능한 것.
- 분할이용 가능성 : 발행된 전자화폐의 합계금액이 액면 금액이 될때까지 분할해서 사용할 수 있는 것.

이외에도 추적 불가능성에 의한 프라이버시 보호를 강조한 나머지 돈세탁이나 탈세등의 사회적 범죄가 발생할 수 있기 때문에 조건부로 전자화폐나 사용자를 추적할 수 있는 조건부 추적가능성에 대한 요구조건도 필요하다.

실물 화폐를 디지탈 정보화하는 이점은 화폐 그 자체가 갖는 익명성, 오프라인성, 양도가능성, 분할이용 가능성 등을 전자화폐에 부여해서 소액의 현금에 대해서도 이동성을 갖게 할 수 있으므로 네트워크를 통한 원격지로의 지불시 요하는 비용을 대폭 줄일 수 있는 점에 있다. 이러한 전자 화폐가 실용화되어 보급될 경우 기대효과로서

- 소규모 사업자의 비즈니스 기회의 확대(원격지 소비자와의 상거래가 용이)
- 소프트웨어 상품의 수요확대(통신망에서의 주문 배달, 지불에 의한 유통, 지불 비용의 절감)
- Contents비즈니스의 확립(정보사용에 대한 과금의 용이)
- 전자화폐에 관련된 상품, 서비스 수요의 창출(전자화폐 관련 기기, 전자 화폐 발행, 관리시스템 구축을 위한 수요 창출)

등을 들 수 있다.

2.2 전자화폐의 분류

현재 실용화되고 있는 전자화폐는 크게 IC 카드형과 네트워크형으로 분류할 수 있다.

(1) IC 카드형은 실현시 Tamper Resistant성을 갖는 하드웨어가 필요한 전자화폐이다. 이에 반해

(2) 네트워크형은 인터넷등의 컴퓨터 네트워크의 존재를 가정하여 네트워크에 접속되어 있는 PC등으로 이용할 수 있는 전자화폐이다.

IC 카드형 전자화폐는 사용자에 의한 취급이 편리한 반면 대규모 설비투자에 드는 비용을 서비스 제공자와 사용자가 부담하는 문제가 있으며 네트워크형 전자화폐는 기존의 네트워크 자원을 활용하기 때문에 서비스 제공자에게 필요한 설비투자는 적지만 컴퓨터 설비를 갖는 사람에게만 이용이 제한된다는 점이 있다. 본 절에서는 전자화폐를 지불방식, 적용영역의 관점에서 분류한다.

1) 지불 방식

전자지불 방식에는 온라인, 오프라인, 신용카드 지불, 선불등 여러 가지 방식이 있다.

- 온라인 지불방식

온라인 지불방식의 전자화폐는 은행의 비밀키로 발행하고 은행의 공개키로 검증할 수 있는 디지탈 서명으로 실현된다. 또한 지불의 익명성을 실현하기 위해 블라인드

서명 기술이 이용된다. 블라인드서명 방법은 디지털 서명 발행시 서명 의뢰자인 사용자가 은행에 보내는 정보에 랜덤요소를 부가함으로써 사용자와 서명정보를 은행이 연결시킬 수 없는 서명 방법이다.

예치시 전자화폐가 은행에 되돌아 온 시점에서 은행은 이미 사용된 전자화폐 데이터와 비교해서 이중사용 여부를 검사한다. 이때 지불시 사용자와 상점뿐만 아니라 은행도 개재되는 경우를 온라인형 지불방식이라 한다.

이 지불방식의 단점은 모든 기사용 전자화폐 데이터를 저장하고 온라인으로 상점의 검사요구에 대응할 수 있어야 하므로 데이터베이스의 비용은 막대하게 된다. 또한 인터넷과 같은 대규모 네트워크에서는 전세계에 분산된 정보를 하나의 데이터베이스로 집중관리해야 하는 문제점도 있다.

- 오프라인 지불방식

온라인 지불방식과 같이 데이터베이스에 온라인 검색을 요구하는 이중사용 방지대책은 데이터베이스 검색시간, 조회시의 통신등 큰 부하를 갖는다. 따라서 지불시 은행이 관여하지 않고 사용자와 상점간의 통신만으로 실현하는 오프라인 전자지불 방식이 요구된다. 오프라인의 이중사용 방지대책은 사용자와 상점의 거래가 완료한 후에 상점이 예치할 때 이중사용 검출을 한다.

- 신용카드 지불방식

신용카드 지불방식은 기존의 신용카드 지불시 교환되는 정보를 전자화하는 것만으로 실현이 용이하지만 지불이 최종적으로 하나의 은행 계좌에 대하여 행하여지므로 추적불능성은 보증할 수 없다. 신용카드 지불을 위해서 상점은 미리 신용 카드 회사와 계약을 맺을 필요가 있다.

- 선불 방식

선불 방식에서는 추적 불능성은 실현가능하지만 텔레폰카드의 위조문제와 같이 이중사용 불가능성 보증의 문제가 있다. 예를들면 사용한 정보를 관리 센타에 일원관리해 놓고 상점이 사용자가 제시한 정보의 이중사용 여부를 지불시 관리센타에 온라인으로 확인하면 이중사용을 검출할 수 있다. 그러나, 실시간성을 보증하기 위해 검색 비용등이 높아진다.

2) 적용 영역

운용형태, 지불에 필요한 비용 등에 의해 고액, 중액, 소액 영역으로 분류한다.

- 고액 지불

기업간의 거래가 중심이 되고 EDI (Electronic Data Iinterchange)로 규정된 프로토콜을 기반으로 하는 지불 영역이다.

- 중액 지불

개인 대 기업(상점)의 거래 형태(카타로그 쇼핑등)가 중심이 되고 현재 사용되고 있는 신용카드를 이용한 지불방법을 전자화함으로 실현가능한 지불 영역이다.

- 소액 지불

개인 대 개인을 중심으로 한 거래이고 소액 상품 거래 형태에 적용될 수 있는 지불 영역이다.

3) 각 지불방식의 비교

전자 화폐의 요구 조건에 대해 네트워크상의 지불, IC카드 지불에 대한 비교를 〈표 1〉에 나타낸다.

표 1 지불방식의 비교

양식 / 평가 항목		기존 지불서비스		전자 지불 방식		
		현 금	신용 카드	네트워크		IC 카드
조 건 명	개 요			신용카드 이용	온라인 검사	물리적인 장치
완전 정보화	bit만이 기본요소	×	×	○	○	×
이중 사용 불가능성	복사에 의한 부정 사용을 할 수 없음	△ (위조 지폐의 존재 가능)	△ (신용 카드 위조 가능)	△ (카드 번호 유출)	○	△
추적 불가능성	이용자의 구매력이 노출되지 않음	○	×	○ / ×	×	○
오프라인성	은행이 개재하지 않음	○	×	×	×	○
양도 가능성	개인간 가치를 양도 가능	○	-	△	△	○
분할 이용 가능성	액면 금액 만큼 분할 이용 가능	×	-	-	×	○

기호 : ○는 조건을 만족시킴. ×는 조건을 충족시키지 못함. △는 제약 조건. -는 조건이 의미를 갖지 않음.

3. 전자 화폐 기본 프로토콜

전자화폐의 기본 개념은 80년대 초반 Chaum [Ch82]에 의해 제안되었고 88년에 Chaum, Fiat, Naor[CFN88]의 추적 불가능한 전자화폐 방식이 제안된 이후 많은 연구의 기초가 되고 있다. 본 장에서는 전자화폐 방식의 기본 프로토콜인 인출 프로토콜 및 지불 프로토콜에 대하여 설명한다.

3.1 인출 프로토콜

인출 프로토콜은 사용자가 은행으로부터 전자화폐를 인출하는 프로토콜이다. 인출 프로토콜에서는 인출된 전자화폐와 사용자를 연결시키지 못하도록 하는 기법즉, 사용자의 프라이버시를 보호하기 위해 블라인드 서명이라는 기법을 사용하고 있다. 블라인드 서명의 이해를 돕기 위해 색종이의 예를 들어 설명한다.

- 사용자는 예를 들면, 100140 색(난수)의 색종이(일련번호가 있는 종이) 가운데 1색을 선택하여 복사용 먹지와 함께 봉투

에 넣는다.
- 계좌의 소유자인 것을 증명하는 ID 카드와 인출할 금액과 함께 위에서 작성한 봉투를 은행에 전달한다.
- 은행은 ID 카드에 의해 사용자를 인증하고 사용자의 계좌로부터 지정된 금액을 인출하고 봉투 위에 서명한다.
- 사용자는 이 봉투를 개봉하고 봉투내의 색종이에 은행의 서명이 되어 있음을 확인한다.

이 프로토콜에서는 사용자가 랜덤하게 선택한 색종이를 봉투에 넣어 내용이 보이지 않도록 해서 은행에게 서명시킴으로써(블라인드 서명) 화폐의 익명성을 실현한다. 블라인드 서명에 의해 이후 전자화폐(즉, 서명된 색종이)가 은행에 예치되더라도 이 전자화폐가 원래 어떤 사용자에 의해 인출된 것인가는 은행은 전혀 알 수 없다. 따라서, 사용자는 익명성을 유지한 채 전자화폐를 상점 등에 지불할 수 있다.

인출 프로토콜을 형식화하기 위해 전자화폐를 $(x, f(x)^{d_B})$ 형태의 수식으로 나타낸다. 여기서, x는 사용자가 선택한 난수(전자화폐의 일련번호), f는 일방향성 함수, d_B 는 전자화폐의 액면에 대응한 은행의 비밀키(은행은 전자화폐의 액면에 대응한 복수의 비밀키를 갖고 있다). mod n의 n은 은행의 RSA잉여이다.

- 사용자는 x와 난수 r을 랜덤하게 선택하고 인출하고자 하는 금액에 대응하는 은행의 공개키 e_B 를 사용하여 $B = r^{e_B} f(x)$ 를 계산한다.
- 사용자는 ID카드를 제시하고 인출하고자 하는 금액 (예를 들어, 100만원)과 함께 B를 은행에 송신한다.
- 은행은 B에 100만원에 대응한 서명 B^{d_B}(mod n)을 계산하고 사용자에 보낸다. 동시에 사용자의 계좌로부터 100만원을 인출한다.
- 사용자는 B^{d_B} 를 r로 나누어 $C = f(x)^{d_B}$ 을 얻는다. $C^{e_B} = f(x)$에 의해 은행의 서명을 확인한다.

이 프로토콜에서 은행은 B밖에 수신할 수 없으므로 x나 C의 값에 대해 전혀 모른다. 그러나, 사용자의 ID카드가 제시되어 계좌로부터 지정 금액을 인출할 수 있고, 실제 전자화폐로써 이용되는 C의 내용을 모른채 B에 서명해도 은행에 위험은 없다. 은행의 서명 결과인 B^{d_B}는 $(r^{e_B})^{d_B} \equiv r \pmod n$ 으로부터 $r \cdot f(x)^{d_B}$ 의 형태로 되며 사용자는 이를 자신의 비밀난수 r로 나누면 최종적으로 은행이 서명한 정당한 전자화폐 $(x, f(x)^{d_B})$를 얻을 수 있다.

이와같이 전자화폐는 난수와 그 난수에 대한 은행의 RSA 서명으로 구성되고 이 전자화폐의 위조의 곤란성은 RSA 서명의 위조의 곤란성에 의존하고 있다.

3.2 지불 프로토콜

인출된 전자화폐를 상점에 지불할 경우의 프로토콜을 살펴본다.

- 사용자와 상점간에 상품과 금액의 교섭이 성립되면 사용자는 상품을 지정해서 전자화폐를 상점에 지불한다.
- 상점은 전자화폐를 받고 은행에게 이중사용 유무에 대한 검사를 의뢰한다.
- 은행은 우선 전자화폐에 있는 은행의 서명을 확인하고 다음에 동일한 색의 전자화폐가 과거에 예치된 적이 있는가를 은행의 예치 데이타베이스를 사용하여 조사한다. 만약 예치되어 있지 않으면 데이타베이스에 이 전자화폐의 색을 등록한다.
- 상점은 이 전자화폐가 은행에 정확히 예

치된 것을 확인하고 상품을 사용자에게 배달한다.

지불 프로토콜을 인출 프로토콜과 같이 수식으로 설명하면 다음과 같다.

- 사용자는 (x, C)를 상점에 송신한다.
- 상점은 이를 수령하면 은행에게 동일한 (x, C)가 이미 예치되어 있는가를 조회한다.
- 은행은 이 전자화폐의 서명을 $C^{e_B} = f(x)$에 의해 확인하고 만약, 예치되어 있지 않으면 (x, C)를 데이터베이스에 예치한다.
- 예치를 확인하면 상점은 상품을 사용자에게 배달한다.

지불 프로토콜에서는 과거 은행에 축적된 전자화폐를 모두 데이타베이스에 기록해 두고 새롭게 예치되는 전자화폐와의 중복을 검사한다. 만약 동일 전자화폐가 예치된 경우 이중사용으로 간주하고 예치를 거부한다. 이와같이 은행은 과거에 예치한 전자화폐를 모두 데이타베이스에 등록하고 새로 예금되는 전자화폐를 이 데이타베이스와 비교함으로써 이중사용을 검출한다.

4. 전자화폐의 연구동향

본 장에서는 전자화폐의 최근 연구 동향에 대하여 소개한다. 연구개발의 흐름은 안전성뿐만 아니라 편리성 등의 부가기능을 갖춘 전자화폐 시스템이 주류를 이루고 있다. 그리고 전자화폐는 소액지불에 적합한 IC카드형 전자화폐가 주류를 이룰 것으로 예상된다. 전자지갑으로써 활용가능한 IC카드는 계산 능력이 부가되어 비밀 정보를 카드의 외부로 노출하지 않고 내부에서 계산할 수 있으므로 종래의 자기카드에 비해 안전성을 향상시킬 수 있다. 그러나 IC카드는 불특정 다수에게 발행, 소유되므로 악의를 가진 사람이 IC 카드를 분해해서 전자화폐를 위조할 가능성이 있기 때문에 IC 카드의 물리적 안전성에만 의존하는 것은 위험하다.

전자화폐 시스템은 다음과 같은 형태로 나누어 볼 수 있다.

- 프라이버시 보호를 고려하지 않는 시스템. 프라이버시 문제를 전혀 고려하고 있지 않거나 은행, 정부기관 등은 사용자의 거래 내역을 조회하지 않는 것을 전제로 하는 시스템.
- 프라이버시 보호를 고려하는 시스템.

프라이버시 보호 시스템은 은행이 사용자에 대한 정보를 알려고 하는 것을 방지해야 되기 때문에 프로토콜 설계가 복잡하다. 이 유형의 시스템 대부분은 블라인드 서명이라는 개념을 사용한다. 블라인드 서명이란 서명자(은행)가 사용자에게 그 서명이 어디에 사용되는지 모른채 문서에 서명 하는 프로토콜이다. 블라인드 서명을 전자화폐에 적용하여 사용자는 은행에서 전자화폐를 인출하고, 상점에 지불할 경우 그리고 현금을 예치할 때, 은행은 그 전자화폐가 어떤 사용자가 지불한 전자화폐였다는 것을 알지 못한다. [CFN88][OO92][FY93][B93a][B93b]

즉, 안전한 전자화폐 실현 기술로서 블라인드 서명 기술은 사용자의 프라이버시를 보증하기 위해 사용자가 서명자에게는 문서를 비밀로 한 채 서명을 받는 서명 방법으로서 프라이버시를 보증받는 기술이다. 블라인드 서명 기술은 추적불능성을 실현하기 위한 기본 기술이고, RSA방식을 기반으로 한 블라인드 서명[Ch82], 영지식 증명을 근거로 한 블라인드 서명 방법[OO89]등이 있다.

그러나, 전자화폐의 추적불가능성은 사용자의 프라이버시를 보장하는 반면 돈세탁이나 탈세 등의 범죄에 악용되어 사회,경제적인 문

제가 될 수 있다. 이러한 문제점을 방지하기 위해 법원 등의 기관이 요구하는 경우 사용자의 ID번호와 전자화폐의 일련번호를 연결시키는 공정한 블라인드 서명 방식이 제안되었다[SPC95]. 이와같이 공정한 블라인드 서명기술은 익명성을 갖는 전자화폐를 그 사용자와 연결시켜 돈세탁이나 탈세 등의 범죄에 전자화폐가 이용되는 것을 방지하고 있다.

이외에 부분 블라인드 서명은 다른 정보가 블라인드된 채로 남아있는 동안에 인증된 정보가 clear 부분에 있는 서명집합에 포함되는 것을 서명자와 사용자에게 보증하는 방법을 제공한다. 부분 블라인드 서명의 RSA방식에 기반을 둔 실현은 [AC97]에서 소개되었다.

부분 블라인드 서명은 은행이 일련번호 m이나 서명 sig(c,m)에서 어떤 정보도 갖지 않도록사용자가 은행으로부터 메세지(c,m)의 디지탈 서명을 얻는다. 메세지의 첫 부분 c는 clear 부분이라 부르고 서명 생성/확인 프로토콜로 구성되어 있다. 서명 생성 프로토콜에 대한 은행의 출력값은 c를 포함하고, 대개 은행의 'view'라고 부르며 사용자의 프로토콜 출력은 메시지(c,m)에 대한 은행의 유효 서명 sig(c,m)이다.

고정된 clear 부분 c에 대하여, 서명 생성 프로토콜에 대한 은행의 view가 통계적으로 m과 sig(c,m)에 대해 독립적이라면 이때 서명 방식을 부분 블라인드서명이라고 부른다.

한편, Chaum[Ch82]에 의한 온라인형 전자화폐을 기점으로서 그 후 여러 가지 전자화폐 방식이 제안되어 왔다. 본 장에서는 오프라인형 전자화폐, Observer형 전자화폐, 분할이용 가능한 전자화폐, Escrow형 전자화폐를 중심으로 소개한다.

4.1 오프라인형 전자화폐

온라인형 전자화폐는 지불시 은행으로의 액세스가 필요하므로 거래량의 증가로 인한 은행의 부하가 무시할 수 없게 되는 문제점이 있다. 이에 대해 오프라인형 전자화폐는 하루가 끝나는 시간 등 적당한 시간에 상점이 전자화폐을 모아 정리하여 은행에 예치하는 사용자와 상점 사이에서만 거래가 행해지는 전자화폐이다. 그러나 오프라인형의 최대 문제는 악의의 사용자에 의해 전자화폐가 이중 사용될 경우에 상점이 이중 사용인줄 모르고 상품을 전달하게 되는 것이다. Chaum등[CFN90]은 이 문제에 대한 하나의 해결책으로서 미리 전자화폐에 사용자의 ID를 부여하고 있다. 이 방식에서는 평상시 전자화폐 사용에서는 사용자의 ID에 관한 정보는 전혀 노출되지 않지만 이중사용시 대단히 높은 확률로 이 ID를 노출시키는 것으로 이중사용을 방지하고 있다. 이 방식을 3장의 인출프로토콜에서 서술했던 색종이 예를 들면, 우선 사용자가 미리 정해진 방법을 사용해서 자신의 ID를 색종이에 부여한다. 여기서 ID를 색종이에 부여하는 방법은 두 Bit A,B 양쪽이 갖춰지면 사용자의 ID가 구해지도록 A,B를 일방향성 함수로 감춰서 색종이에 넣는다.

사용자는 색을 은행에 밝히지 않고 서명받아 전자화폐를 인출한다. 이때 사용자가 정직하게 전자화폐속에 자신의 ID를 부여했다고 보증할 수 없기 때문에 "Cut and Choose법"(둘이서 케이크를 공평하게 나누기에는 나이프로 자른 사람과 먼저 선택하는 사람을 구분하는 방법)을 이용해서 사용자가 자신의 ID를 정확하게 부여하는 것을 보증하고 있다. 예를 들면, 이중사용시 ID를 검출 할 수 있는 구조에 대해 사용자에게 색종이를 40장 정도 만들게 해서 은행이 이중 반을 랜덤하게 선택하고 이들을 정확하게 만들었는가를 증명시킨다. 그 다음에 이 증명에 사용한 전자화폐는 버리고 나머지 20장을 1매의 전자화폐로서 은행이 서명한다. Cut and Choose방법을 이용하면 사용

자가 고의로 40장의 색종이 중 K장에 타인의 ID를 부여했더라도 높아야 $1/2^k$ 이하의 확률밖에 성공시키지 못하고 정확하게 색종이를 만들 수 밖에 없게 된다. 다음 이 전자화폐를 상점에 지불할 때 색종이 20장으로 만들어진 전자화폐를 상점에 건네준다. 상점은 20장의 한 장 한장에 대하여 색종이에 감춰진 두 Bit A, B의 한 쪽을 랜덤하게 뽑아서 사용자에게 제시시킨다. 나중에 이 전자화폐를 은행에 예치할 경우 상점은 20장의 색종이에 대응하는 20개의 Bit를 은행에 건네준다. 만약 전자화폐가 이중 사용되고 이미 같은 색의 전자화폐와 별도 20개의 Bit가 은행의 데이터베이스에 저장되었으면 은행은 같은 전자화폐에 대응하는 20개의 Bit가 2쌍 갖추어지게 된다. 여기서 20개중 적어도 1개의 Bit는 압도적으로 높은 확률로 A, B 양쪽의 Bit가 모아질 것이고, 이들 두 Bit를 이용해서 사용자의 ID를 검출할 수 있다.

4.2 효율 좋은 오프라인형 전자화폐

Chaum의 오프라인형 전자화폐는 사용자의 프라이버시가 완전히 보호된다는 점에서 획기적이었지만 전자화폐 시스템 자체에 대한 안전성의 증명이 없고 효율이 좋지 않은 문제점이 있다. 그후 '89년 오오까모토, 오오타[OO89]에 의해 영지식 증명을 사용해서 안전성이 증명되고 보다 효율적인 오프라인형 전자화폐을 실현할 수 있는 방법이 제시되었다. 또한 '93년 Franklin과 Yung[FY93]은 영지식비대화 증명과 비밀분산법을 사용해 효율좋은 전자화폐방식이 구성될 수 있음을 나타냈다. 이 방식의 개요를 이하에 나타낸다. 우선

(1)사용자의 ID를 부착한 전자화폐와 전자화폐로부터 ID를 복원하기 위한 키(Witness)를 Oblivious Authentication이라는 기법을 사용해 은행 사용자에게 발행한다(단 은행은 이 전자화폐와 사용자의 ID를 연결시키지 못한다).

(2)지불시 사용자는 상점에게 전자화폐와 키에 대한 힌트를 전한다. 단지 이 힌트는 키와 상점 ID, 시각정보 등으로 유일하게 계산되어 한 개의 힌트로는 이에 관한 정보를 전혀 알지 못한다. 그러나 이중사용으로 서로 다른 상점, 시각정보를 근거로 만들어진 힌트를 두 개 갖추면 키가 복원되어 이중 사용한 사용자의 ID가 노출되는 구조로 되어 있다.

이 전자화폐 시스템은 인출시에는 2라운드 메세지가 필요하지만 지불과 예치시에는 1메세지로 실현 할 수 있으므로 통신량이 대폭 삭감된다. 그러나 Franklin, Yung의 방식은 Oblivious Authentication을 효율적으로 실현하기 위하여 중립적인 센타의 존재를 가정했다. 그 후 Brands[B93a]는 센타의 존재를 가정하지 않고 전자화폐를 단일항(Single-Term)으로 나타내는 전자화폐 시스템을 제안했다. 이에 의해 전자화폐 관리에 필요한 기억장소와 프로토콜 실행에 필요한 통신량이 감소되고 오프라인형 전자화폐가 효율화된다.

4.3 Observer형 전자화폐

95년 Chaum, Pedersen[CP93]은 은행 또는 카드 발행회사(서비스 제공자)의 지시대로 움직이는 Tamper Resistant 장치(Observer)와 사용자가 자유로 제어할 수 있는 컴퓨터 C를 적절하게 조합시킨다. 이와같이 서비스 제공자와 Observer사이의 모든 통신에 C가 개재하도록 구성하면 사용자의 프라이버시 등의 권리를 컴퓨터C로 지키고 컴퓨터C가 부정한 동작을 행하지 않는다는 것을 Observer로 보증할 수 있다.

Chaum은 Tamper Resistant 장치(IC카드 등)를 서비스 제공자가 발행하는 종래 방식의 문제점으로서 사용자의 프라이버시에 관계되는 정보를 마음대로 이 하드웨어가 서비스제공자에게 노출하지 않는 것을 보증할 수 없고 결국 사용자는 서비스 제공자를 신뢰할 수 밖에 없다는 점을 지적하고

- C가 예정된 프로토콜을 지키는 한 C에게 비밀로 서비스 제공자와 T가 서로 정보를 교환할 수 없고
- 서비스 제공자와 T가 승인한 서비스 요구 밖에 응할 수 없어서 C가 프로토콜을 지키는 T의 승인을 얻지 않는 한 사용자는 서비스를 이용할 수 없는 프로토콜을 실현할 수 있다는 것을 나타내고 이 프로토콜을 사용하면 서비스 제공자의 신뢰에만 의존하지 않아도 됨을 제시했다. 93년 Brands[B93]는 이 Observer의 아이디어를 응용해서 전자화폐의 이중사용을 사전에 방지하는 방식을 제안했다. 이들은 은행에서 인출된 모든 전자화폐를 사용자의 컴퓨터와 Observer양쪽으로 관리시켜 전자화폐를 사용할때 전자화폐에 Observer의 서명이 필요한 구조를 제안했다. 즉, Observer는 한 번 전자화폐에 서명하면 두번 다시 같은 전자화폐에는 서명하지 않고, 은행도 전자화폐에 Observer의 서명이 없으면 상점으로부터 전자화폐를 예치받지 않는다. 따라서 상점도 Observer의 서명이 없으면 전자화폐를 받아들이지 않으므로 악의의 사용자가 컴퓨터를 조작해 이중 사용해도 상점에서 바로 알게되어 이중사용은 사전에 방지된다. 또한 이 방식은 만약 Observer가 파괴되어 Observer의 가짜서명이 이중 사용된 전자화폐에 행해졌다 하더라도 은행이 이중사용 검사를 행하면 예치시에 부정사용자의 ID가 노출되도록 이중검사 체제를 구축하고있다.

4.4 분할이용 가능한 전자화폐

분할이용 가능성은 실제의 화폐에는 실현되어 있지 않지만 편리성을 제공하기 위해 전자화폐에 실현하는 것이 바람직하다.

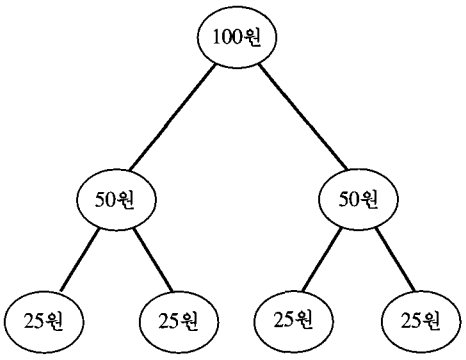


그림 1 계층 구성 테이블(현금 구조)

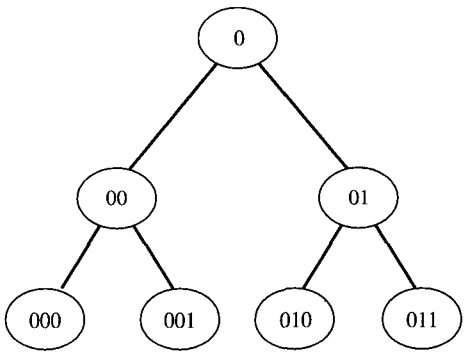


그림 2 계층 구성 테이블

분할이용 가능성(1회 발행된 전자화폐를 액면금액이 될 때까지 몇 회라도 사용할 수가 있는 성질)을 효율적으로 실현하기 위해 계층구성 테이블이라 하는 목구조의 테이블을 도입한다. 이 계층구성 테이블은 전자화폐 금액 및 그 사용 최소단위(예를 들면, 1원 단위 등)

에 대응하여 정해진다. 예를 들어, 25원 단위로, 100원의 지폐를 사용할 경우 계층 구조 테이블을 〈그림 1〉 및 〈그림 2〉에 나타낸다.

여기서, 예를 들어 75원을 사용할 경우, 노드00(50원 상당)과 노드010(25원 상당)이 해당하는 노드가 된다. 이 해당 노드는 다음의 규정으로 정해진다.

(1)어떤 노드와 노드의 해당 금액 합계가 위 노드의 해당 금액이 된다.
(2)어떤 노드가 한 번 사용된 후에는 부모 노드 및 자손 노드를 이용해서는 안된다.
(3)각 노드는 1회 이상 사용해서는 안 된다.

이 규칙에 따르면, 노드 00와 노드 010이 뿐이다. 즉, 위의 규정에 따르는 것에 의해 사용할 수 있는 합계 금액은 액면 대로 100원이 됨과 함께 25원 단위로 어떤 방법으로도 사용할 수 있다. 이 계층 구조 테이블은 전자 화폐의 액면 금액을 크게 하고 이용 단위 금액을 작게 하면 그 계층이 증가하게 된다. 예를 들면, 액면이 100만원으로 1원 단위로 이용할 수 있는 전자화폐의 경우 그 계층은 거의 20이 된다($\log_2 100000020$).

분할 이용가능성은 실물 화폐에도 없는 성질이지만 소액관리가 필요없게 되는 등 이점이 있다. Mondex나 선불카드 등은 이미 이 성질을 지니고 있다. 단, Mondex나 선불카드 등과 같이 금액을 연속치로 나타내는 시스템은 분할이용을 쉽게 실현할 수 있지만 동시에 잔고데이터를 바꿔 쓸 수 있는 위험이 있기 때문에 이 같은 위조로부터 보호하기 위해 매체의 물리적인 안전성에 의존하는 측면이 있다.

한편, 은행의 디지털 서명으로 전자화폐를 나타내는 시스템에서는 전자화폐가치의 분할은 쉽지 않다. 그러나 만약 전자화폐의 가치를 분할해서 이용할 수 있다면 앞에서 서술한 소액 관리가 필요 없게 된다는 이점과 전자화폐 관리에 필요한 기억량을 적게 할 수 있는 이점이 있고 특히 기억용량이 적은 IC카드에서의 실현이 유리하다. 분할이용 가능한 전자화폐의 하나로서 Chaum[CFN88]은 익명성을 갖는 수표와 유사한 구조를 제안했다. 이 구조는 한 번에 한해서 액면 이하의 임의의 금액에 대한 지불이 가능하지만 잔금은 은행에서 환불 받아야 된다는 제약이 있다. 지불액의 합계가 액면금액이 될 때까지 몇 번이든 이용할 수 있는 전자화폐 시스템 구성법의 개요를 간단히 설명한다.

우선, 각 노드가 부모 금액의 반액을 나타내는 2분목을 설정한다

예를들면, 부모가 100원 일 때는 그 두 개의 자식은 각각 50원을 나타낸다.

이 2분목을 사용하면 분할이용의 조건을 다음과 같이 나타낼 수 있다.

(1)어떤 노드가 이용되면 그 노드의 부모 및 자손은 모두 이용할 수 없다.
(2)각 노드는 한 번밖에 이용할 수 없다.

이와같은 조건을 실현하기 위해 RSA잉여 n에서 임의의 평방잉여가 갖는 4개의 평방근 중에 어떤 성질을 만족하는 두 개의 평방근이 판명되면 n을 소인수분해 할 수 있는 것을 이용한다. 즉, 조건에 위반한 이용이 존재할 경우 2개의 평방근으로부터 n이 소인수분해되어 전자화폐에 부여되어있는 사용자의 ID가 판명된다.

4.5 Escrow형 전자화폐

효율적인 전자화폐 시스템은 전자상거래에 있어서 중요한 구성요소이다. 이러한 전자화폐 시스템의 설계는 보안과 관련된 많은 문제가 발생한다. 부정 사용방지와 같은 보안 요구사

항뿐만 아니라 사용자 프라이버시 보호가 중요한 이슈이다[CPS96]. 사용자의 프라이버시 보호는 관리적, 법적 대책 이외에 블라인드 서명과 같은 암호학적 도구의 사용으로 거래시 사용자의 익명성을 유지하는 전자 화폐시스템을 설계하는 것이 가능하다. 기존의 많은 전자화폐 시스템들은 거래하는 동안 익명성을 사용자에게 부여한다. 그러나 완전한 프라이버시 보호는 사회. 경제적 범죄 예를 들면, 협박 또는 돈세탁 등에 의해 악용될 수 있다[vSN92]. 익명의 지불이 가능하지만 Escrow형 전자화폐에 의해 익명성은 거래 자체에는 포함되지 않는 제3자 (수탁자)의 도움으로 제거될 수 있다. 수탁자는 전자화폐가 범죄자들에 의해 잘못 사용되어질 때 은행과 협조하여 거래의 익명성을 제거할 수 있다. 이와같이 Escrow형 전자화폐 시스템의 개념은 범죄자들에 의한 부정사용의 효과적인 방지와 프라이버시 보호의 필요성에 대한 절충안을 제시한다.

한편 정부기관 등은 사용자의 프라이버시를 부분적으로 제한할 수 있으며 사용자의 익명성을 보호할 수 있고 조건부로 익명성을 제한하는 수탁자 기반의 추적시스템(trustee-based tracing)이라는 전자화폐시스템을 도입하려는 움직임이 있다. 전자화폐의 사회.경제적인 문제점을 방지하려는 노력의 일환이다. 수탁자 기반의 전자화폐 시스템은 정부기관등에서 '어떤 사람이 누구에게 얼마나 지불했는가'라는 사용자의 지불이력을 추적할 수 있다는 점을 제외하고는 완전한 익명성을 유지한다. 수탁자는 불필요한 정보의 노출 없이도 특정 지불행위가 누구에 의해 이루어졌는가에 대한 응답을 할 수 있는 데, 수탁자 기반 추적시스템은 tamper-resistant 장치가 필요하지 않으며 온라인이나 오프라인으로도 구현될 수 있다[BGK95]. 수탁자에 대한 신뢰도를 높이기 위하여 사람을 수탁자로 하는 시스템 대신에 컴퓨터 수탁자를 이용하는 시스템도 있다. 이 시스템은 tamper-resistant와 tamper-detecing 장치를 사용하며, 컴퓨터 수탁자에 의해 저장되어 있는 사용자의 비밀 정보가 노출되었을 때 자동으로 경고하는 장치이다.

그러나 추적가능한 전자화폐는 많은 범죄를 방지할 수 있지만 동시에 사용자의 프라이버시를 위협하게 될지 모른다.

한편, 실제 현금은 익명성을 가지고 있음에도 불구하고 익명 사용은 아래의 문제 때문에 심각하게 억제되는 경우가 있다.

- 부피(Bulk) : 매우 많은 돈은 많은 공간을 차지한다. 때때로 이런 부피는 돈을 추적하는 근거가 될 수 있다.
- 처리지연 : 전달하거나 확인하고 현금을 헤아리는데 시간이 걸린다.
  양이 많으면 요구되는 시간은 상당할 것이다.
- 감지가능성(Palpability) : 실제 현금은 전산망으로 전달될 수 없고 멀리 있는 수신자에 안전하게 전달하기 위해 시간이 걸린다.
- 추적가능성(Traceability) : 법집행기관에서 화폐의 일련번호를 알면 추적당할 수 있고 금융기관이 화폐를 예치한 후 사용자를 식별하는 것이 가능하게 된다.

현금이 갖는 이러한 특징들은 범죄활동, 강도, 유괴, 그 밖의 다른 유형의 강탈들을 방지하는 요소중의 하나이다. 예를 들어, 유괴의 중요한 도전중의 하나는 익명의 형태로 몸 값을 받는 것이다. 실제 현금을 제공할 경우 문제는 어려워질 수 있다 : 만약 지불자와 경찰이 협동한다면 돈을 가득 채운 가방을 이동하는 것은 어려울 것이다 또한, 유괴의 강제적인 보강장치에도 불구하고 무엇보다도 일단 현금이 전달되면 현금을 사용하는 것은 일련번호가 기록될 수 있기 때문에 문제가 있다. 그러

나 이러한 문제는 현금이 전자화폐로 대체될 경우 거의 문제가 될 수 없다. 이 때문에 완전히 추적이 불가능한 전자화폐는 많은 법집행 기관에게 새로운 어려움에 직면하게 한다. 추적가능한 전자화폐 연구의 필요성은 실제현금이 갖는 이와 같은 추적성의 특징을 전자화폐에 부여하는 동기로부터 생긴다.

5. 결 론

본 논문에서는 최근 주목되고 있는 전자화폐 기술과 연구동향에 대하여 서술했다. 컴퓨터 네트워크, CPU 속도, 데이터베이스 기술의 발전과 더불어 위조기술까지 발전하고 개인과 기업은 원격지에서의 인출 등 편리한 거래를 원하고 있다. 전자화폐가 앞으로 더욱 경제.사회에 기여하기 위해서 기술, 사회 및 법.제도 등에서의 종합적인 연구가 필요하다. 그리고, 완전한 추적 불능성(익명성)은 전자화폐의 역기능적 측면인 돈세탁이나 완전 범죄의 위험성을 증대할 가능성이 있다. 프라이버시 보호와 범죄 방지를 양립시키기 위한 연구도 필요할 것이다. 예를 들면, 법적인 절차를 거쳐서 인정된 경우에 한하여 특정의 거래에 관해 사용자의 익명성을 제한할 수 있는 Escrow 전자화폐의 연구 등이 필요하다.

향후 전자화폐을 수용하기 위한 법.제도의 개혁이나 돈 세탁, 거래분쟁 등의 사회적 문제를 해결하기 위한 기술 개발이 이루어져야 할 것이다. 본 논문이 전자화폐에 관심있는 뜻 있는 분들에게 도움이 되기를 바란다.

참 고 문 헌

[AC97] M.Abe and J.Camenisch, Partially blind signature, SCIS97, 1997.

[AF96] M.Abe and E.Fujisaki. How to date blind signatures, Advances in Cryptology-ASIACRYPT '96, 244-251, Springer Verlag, 1996

[B93a] S.Brands, An efficient off-line electronic cash system based on the representation problem, Technical Report CS-R9323, CWI, Apr.1993

[B93b] S.Brands, Untraceable off-line cash in wallets with observers, Crypto93 pp302-318, 1993

[BGK95] E.Brickell,P.Gemmel, and D.Kravitz, Trustee-based tracing extensions to anonymous cash and the making of anonymous change, Proc. 6th Ann. Symposium on Discrete Algorithms pp407-466, 1995

[Ch82] D.Chaum, Blind signature for untraceable payments Crypto82 pp199-203, 1982

[CMS96] J.Camenisch, U.Maurer,and M.Stadler, Digital payment systems with passive anonymity-revoking trustees, ESORICS 96, pp33-43. Springer Verlag, 1996.

[CFN88] D.Chaum.A.Fiat,and M.Naor. Untraceable electronic cash, Advances in Cryptology-CRYPTO '88, pp 319-327, Springer Verlag,1990.

[CP93] D.Chaum, T.P.Pedersen, Wallet databases with observers, Crypto93, 1993

[CPS96]J.Camenish,J.M.Piveteau, M.Stadler, An efficient fair payment system, ACM CCS96 1996.

[EO94] T.Eng, T.Okamoto, Single-term divisible electronic coins, Eurocrypt94, pp311-325, 1994

[FO96] E.Fujisaki and T.Okamoto. Practical escrow Cash. Cambrige workshop 96.

[FY93] M. Franklin, M. Yung, Secure and efficient offline digital money, ICALP' 93, pp 265-276, 1993

[JY96] M.Jakobsson,M.Yung, Revokable and versatile electronic money, 3rd ACM Conf. Computer and communications security,pp76-87, 1996

[OO89] T. Okamoto and K. Ohta. Disposable zero-knowledge authentication and their applications to untraceable electronic cash. Crypto '89, pages 481-496. Springer-Verlag, 1990.

[OO92] T.Okamoto, K.Ohta, Universal electronic cash, Crypto91, pp 324-337, 1992

[SPC95] M.Stadler,J.M.Peveteau, and J.Camenish, Fair Blind Signatures, Eurocrypt95, 1995

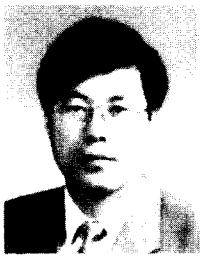
[vSN92] S.von Solms and D.Naccache, On blind signatures and perfect crimes, Computers and Security, 11, pp581-583, 1992

□ 著者紹介

송 유 진

1982년 한국항공대학교 졸업(학사)
1987년 경북대학교 대학원 졸업(석사)
1995년 일본 Tokyo Institute of Technology 졸업(박사)
1983년 - 1986년 한국공군 기술장교
1986년 - 1988년 금성정보통신
1988년 - 1996년 한국전자통신연구원
1996년 - 현재 동국대학교 정보산업학과

※ 주관심분야 : 암호 이론, 부호 이론, CALS/EC 보안 응용, 전자 화폐



강 창 구

1975년 한국항공대학 항공전자공학과 졸업(공학사)
1986년 충남대학교 대학원 전자공학과(공학석사)
1993년 충남대학교 대학원 전자공학과(공학박사)
1979년 ~ 1982년 한국공군 기술장교
1987년 ~ 현재 한국전자통신연구원 부호기술연구부 실장 책임연구원