通信情報保護學會誌
第6卷 第2號, 1996. 6

전자화폐가 세계를 바꾼다.

Electronic Money changes the world

박 춘 식*, 이 대 기*

요 약

본 논문에서는, 세계적으로 불붙고 있는 전자화폐를 암호학적인 측면에서 살펴보고, 전자화폐의 가장 핵심적인 기술인 추적 불가능성, 프라이버시 제공 기술 그리고 이중 사용 방지 기술 등과 암호 이론과의 관련성을 중심으로 정리하였다. 특히 기존에 제안되어 있는 대표적인 전자화폐 방식들에 대해서 암호 프로토콜 관점에서 고찰하여 보았으며 전반적인 전자화폐 관련 내용도 추가하였다.

1. 서 론

전자메일, EDI(Electronic Data Interchange), 전자화폐, 전자상거래(Electronic commerce) 그리고 CALS(Commerce At Light Speed) 등으로 인한 관심이 인터네트의 영향으로 그 어느 때보다도 대단하다. 이는 컴퓨터망의 발달과 인터네트의 급속한 보급으로 인한 영향으로 생각되며, 정보화 물결의 위력을 새삼 느끼게 한다. 국내적으로도 초고속정보통신이라는 국가적인 대형 프로젝트가 진행중이며 전 산업과 모든 국민에게 미치는 영향은 실로 막대할 것이다. 이중에서도 개인과 밀접한 관계를 갖고 우리에게 다가오고 있는 전자화폐는 통화혁명의 주체가 되어 금융계는 물론이고 경제계 그리고 온 세상을 변화시키려 하고 있다.

인류가 사용하고 있는 화폐는 조개껍질, 금속(금,은,동 등) 화폐를 거쳐 현재는 종이로 된 지폐시대와 신용카드시대가 공존하고 있다. 그러나 정보화의 높은 물결로 전자화폐가 서서히 새로운 통화수단으로 등장하고 있다. 전자화폐는 현금을 대신하는 결재수단으로 전자현금, 전자지갑, 사이버화폐, 디지털현금, 스마트화폐, 가상현실화폐 등 많은 관심만큼이나 다양하게 불리고 있다.

이러한 전자화폐의 관심은 지폐가 중심이 된 기존 화폐가 갖고 있는 여러가지 문제점들이 그 출현 배경이 되고 있다. 그중 하나로는, 기존 화폐는 통화발행이 인가된 기관(우리나라의 경우는 한국은행)외에는 화폐 제작을 할 수 없다는 사실과 물리적인 안전 대책에만 화폐 제도의 안전성이나 신용이 의존하고 있다는 점이다. 또한, 인터네트와 같은 정보화의 거대한 물결이 닥쳐 오고 있는 정보화 사회에서는 기존의 지폐로는 정보화에 쉽게 대처할 수 가 없다는 사실도 전자화폐에 대한 관심과 경쟁을 고조시키는 요인이 되고 있다. 기존 화

* 한국전자통신연구소

폐제도의 문제점이자 전자화폐의 출현 배경을 요약하여 보면 다음과 같다.

- 화폐의 제작, 관리, 파기에 막대한 예산과 인력 소요로 특히 소액관리에 따른 관리가 심각하며 우리나라의 10원짜리 동전 생산에 드는 비용이 27원 정도로 소요되고 있음[1].
- 컬러 복사기와 고해상도 레이저 프린트의 등장으로 화폐 위조 기술의 급격한 발달
- 카드의 보편화로 인한 카드 복제와 위조 급증
- 금융 EDI인 SWIFT(Society for Worldwide Interbank Financial Telecommunication)와 사이버쇼핑 등 컴퓨터 통신망을 통한 금융 거래의 활발

이러한 출현 배경으로 등장한 각종 전자화폐는 각국의 지대한 관심으로 개발과 보급이 시작되고 있다. 넷스케이프, 사이버캐쉬, 퍼스트버츌, 오픈 마켓, 디지 캐쉬 등의 전자화폐 관련 회사들이 인터네트의 급속한 보급과 멀티미디어 산업과 맞물려 전자화폐 개발 경쟁에 박차를 가하고 있다. 스마트 카드 기술이 앞선 유럽의 전자화폐 개발 프로젝트인 CAFE(Conditional Access For Europe)[35], 영국의 네쇼날 웨스트민스트 은행, 미드랜드 운행, British Telecommunication사의 연합 벤쳐 기업이 개발하여 실험 운용중인 몬덱스 전자화폐 시스템은 세계의 주목을 받고 있으며, 일본의 대장성과 NTT 그리고 민간 기업도 연합하여 전자화폐 개발에 박차를 가하고 있다.

본 논문에서는, 세계적으로 불붙고 있는 전자화폐를 암호학적인 측면에서 살펴보고, 전자화폐의 가장 핵심적인 기술인 추적 불가능성, 프라이버시 제공 기술 그리고 이중 사용 방지 기술 등과 암호 이론과의 관련성을 중심으로 정리하였다. 특히 기존에 제안되어 있는 대표적인 전자화폐 방식들에 대해서 암호 프로토콜 관점에서 고찰하여 보았으며 전반적인 전자화폐 관련 내용도 추가하였다.

이 논문은 모두 7개장으로 구성, 진행된다. 먼저, 전자화폐가 최소한 갖추어야 할 요구 사항, 그리고 전자화폐에 대한 주요 용어들의 설명을 2장에서 행하고, 전자화폐에 대한 개발 및 연구 현황을 3장에서 소개한다. 4장에서는 전자화폐 분류에 따른 내용들을 설명하고, 전자화폐의 대표적인 방식들인 인터네트형 방식과 이론적인 방식들에 대해서는 5장에서 다루기로 한다. 전자화폐에 대한 앞으로의 남은 과제와 향후 전망을 6장에서 설명한다. 마지막으로 결론부를 7장에 둔다.

2. 전자화폐

2.1 전자화폐란?

기본적으로 전자화폐는 그림 1과 같이 은행(Bank), 상점(Shop) 그리고 구매자(Consumer)로 구성되어 구매자와 은행간에 이루어지는 발행단계(Withdrawal phase), 발행단계에서 받은 전자화폐를 물건을 사고 상점에 전자화폐를 지불하는 지불단계(Payment phase) 그리고 구매자로 부터 받은 전자화폐를 은행에 제출하여 상점의 계좌로 자금이체를 시켜주는 결재단계(Deposit phase)로 구성되어 있다.

먼저 구매자인 A가 은행으로 부터 만원권 전자화폐를 자신의 계좌로 부터 받아 상점에서 물건을 산다고 가정해보자. 이때 은행과 상점이 결탁을 하게 되면 구매자인 A의 구매에 관한 정보인, 언제, 어디서 무엇을 사는 지에 대한 개인의 프라이버시 관련 정보가 쉽게 노출되게 된다. (참고로 개인의 프라이버시를 전자화폐에서 제공하여야만 하는 지의 여부는 아직

도 논란의 소지가 많이 있으나 본 논문에서는 프라이버시를 제공하는 전자화폐를 고려한다. 좀더 자세한 내용은 Privacy와 Untraceability의 내용을 참조하기 바란다.) 이러할 경우 과연 어떻게 하면 개인의 프라이버시를 유지하면서 안전한 전자화폐를 만들 수가 있을까.

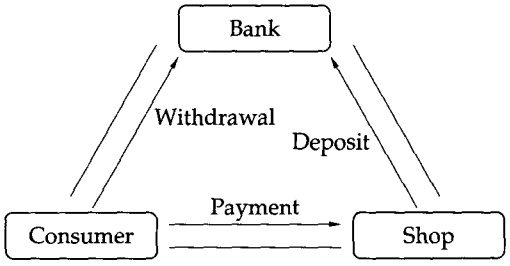


그림 1. 전자화폐

2.2 마법종이를 이용한 전자화폐

개인의 프라이버시를 유지하면서 전자화폐를 사용할 수 있는 방안은, 한번 부치기만 하면 부친 사람외에는 누구도 떼어낼 수 없는 마법종이가 이 세상에 있다면 간단하게 만들 수 가 있다. 전자화폐에서의 각 단계를 마법종이를 이용하여 구현한 개념적인 내용은 다음과 같다.

(발행단계)

(step 1) 구매자는 보통종이위에 난수 r를 써 넣는다.

(step 2) 그 종이위에 난수 r만이 보이지 않도록 마법종이를 붙인 후 은행에 제출한다.

(step 3) 은행은 구매자의 계좌로 부터 만원을 빼낸 후

(step 4) 구매자가 제출한 종이위에 은행의 만원용 도장을 찍어 구매자에게 되돌려 준다.

(지불단계)

(step 1) 구매자는 마법종이를 떼어낸 후 만원권 전자화폐로써 사용한다. 즉, 구매자는 원하는 물건을 사기 위해 상점에 전자화폐를 지불한다.

(step 2) 상점은 구매자가 제시한 전자화폐에 있는 은행의 도장을 확인한 후 구매자가 요구한 물건을 제공한다.

(결재단계)

(step 1) 상점은 구매자로 부터 받은 전자화폐를 은행에 제시한다.

(step 2) 은행은 상점의 계좌에 만원을 넣어준다.

마법종이를 이용한 이 방법에서는 은행과 상점이 결탁할 지라도 마법종이로 숨긴 난수 r를 알 수가 없으므로 구매자의 구매에 관한 정보를 전혀 알 수가 없게 된다. 즉 구매자의 프라이버시를 만족하는 전자화폐를 실현할 수가 있게 된 것이다. 그러나 문제는 이러한 마법종이가 실제로 존재할 것인가가 문제이다. 다행히도 이러한 마법종이는 암호를 이용하면 쉽게 만들 수가 있다. 내용은닉서명(Blind signature)이라는 암호 도구를 이용하면 된다. 내용은닉서명에 대한 내용은 참고문헌 [7][9]을 참고하기로 하고 여기서는 암호를 이용하여, 마법종이를 구현하는 방법을 설명한다.

2.3 암호를 이용한 마법종이의 구현

프라이버시가 제공될 수 있는 이러한 마법종이는 구체적으로 어떻게 구현할 수 있을 것인가. 공개키 암호를 이용한 내용은닉서명을 사용하면 마법종이는 쉽게 구현할 수 있다. 공개키 암호인 RSA 암호[11]를 이용하여 구현한

마법종이 전자화폐는 다음과 같다. 여기서, 은행의 RSA 공개키 암호의 공개 키를 (N,e)라고 하고 비밀 키를 d라고 하자.

(step 1) 구매자는 먼저 난수 r, a를 선택하여 $Z = r^e a \bmod N$를 계산한 후 은행에 보낸다.

(step 2) 은행은 비밀 키 d를 이용하여 $Z^d = ra^d \bmod N$를 계산한 후 구매자에게 돌려준다.

(step 3) 구매자는 자신만이 알고 있는 난수 r를 이용하여 $Z^d/r = a^d \bmod N$를 계산하면 (a, a^d)가 은행으로 부터 받은 전자화폐가 된다.

마법종이를 RSA 암호[11]를 이용하여 발행단계만을 구현했지만 지불, 결재단계도 쉽게 구현될 수 있다. 그러나 위의 방식에서는 구매자가 2개의 전자화폐로 부터 은행의 승인 없이 다른 전자화폐를 만들 수 있는 부정이 가능하게 된다. 이러한 문제점은 출력과 함수가 주어졌을 때 입력을 구하기가 계산상 어려운 일방향함수 f를 도입하여 마법종이를 만들면 즉, 전자화폐가 $(a, f(a)^d)$가 되도록 하면 쉽게 해결할 수가 있다.

그러나, 위와같은 마법종이를 사용한 전자화폐는 구매자의 프라이버시는 보호할 수 있지만, 구매자가 동일한 전자화폐를 몇번이던지 사용하는 것(Double spending)은 막을 수가 없다. 이중사용(Double spending)은 은행에 있어서 막대한 손실을 초래하는 문제로 전자화폐가 갖추어야 할 가장 기본적인 요구 조건이 될 수 있기 때문에 이중사용방지가 가능한 마법종이 전자화폐가 구현되어야만 한다. 5.2절에서 이러한 기능들이 가능한 이론적인 전자화폐들을 소개하기로 하고 여기서는 기본적인 전자화폐가 갖추어야 할 사항들을 먼저 살펴보기로 한다.

2.4 전자화폐의 요구조건

이러한 사항들을 기본적으로 고려한 전자화폐의 요구 사항, 즉 전자화폐 시스템에서 제공해야 할 사항은 다음과 같이 요약할 수 있다.

- 안전성 : 전자화폐의 복사, 위조 등에 의한 이용 불가
- 프라이버시 : 은행 또는 상점에 의한 구매 관련 내용의 추적이 불가능 해야 한다.
- 이중사용(Double spending) 금지 : 전자화폐의 이중 사용이 방지되어야 한다.
- 양도성 : 현금과 같이 타인에게도 양도가 가능해야 한다.
- Off-Line : 상점과 은행간의 처리는 Off-Line이어야 한다.
- 분할성 : 적은 금액으로 전자화폐가 분할 사용되어야 한다.

물론 위의 요구 사항은 최소한의 것이며 또한 경우에 따라서는 필요 없는 것이 있을 수도 있으며 시스템의 특성에 따라서는 별도의 요구 사항이 추가될 수도 있다.

2.5 전자화폐 관련 주요 용어들

2.5.1 Double spending

전자화폐와 현행 화폐 제도중의 하나인 지폐사이에 일어날 수 있는 부정행위를 살펴보면 지폐에 있어서는 위조가 있으며 전자화폐에 있어서는 이중사용(Double spending)이 있다. 지폐에서의 위조는 은행 또는 정당한 발행기관의 허가없이 돈을 만들거나 기존의 돈으로 부터 새로운 돈을 만드는 행위를 말한다.

한편, 전자화폐는 전자정보로 이루어져 쉽게 복사가 가능한 점을 이용하여 1회 사용후 다시 다른 곳에 동일한 전자화폐를 사용하는 것을 말한다. 지폐에 대한 위조를 방지하기 위해서는 복사하기가 어려운 특수 잉크, 특수 용지, 특수 문안이나 도안 등이 사용되어 위조 지폐의 발행을 어렵게 하거나 위조 지폐의 식별을 용이하게 하는 수단을 사용하고 있다. 전자화폐에 대한 이중사용 방지는 사용된 전자화폐의 정보로 부터 컴퓨터가 동일한 전자화폐를 조사하여 이중사용자의 계좌번호와 사용자의 신분을 알아내는 방식을 주로 취하고 있다. On-Line인 경우는 이중사용의 방지가 용이하며 즉시 거래를 중지시킬 수 있으나 Off-Line인 경우는 전자화폐 사용전 거래 중지가 곤란하며 추후 부정사용자 Blacklist에 공개하거나 신용거래를 중지하는 방안으로 취하고 있다.

2.5.2 Privacy/Untraceability

전자화폐에 있어서 안전성이나 효율성 외에 가장 중요한 관심사가 되고 있는 것이 Privacy다. 특히 미국보다는 유럽을 중심으로 활발히 거론되고 있는 것으로 네덜란드의 암호학자인 D. Chaum은 Privacy를 만족하지 않는 전자화폐는 실질적인 전자화폐로 고려하기는 곤란하다고 주장하고 있다.

전자화폐에 있어서의 Privacy는 구매자가 돈을 지불하거나 상점이 돈을 받거나 할 경우의 돈의 액수를 다른 사람이 알 수 없게 하는 것이 아니다. 어디에 전자화폐를 사용하였거나 어디서 전자화폐를 가져왔는 가에 대한 개인의 비밀정보를 다른 사람이 알 수 없게 하는 것이다.

전자화폐에서 고려될 수 있는 Privacy는 크게 두종류로 지불자외의 다른 모든 사람들이 결탁한다 하더라도, 지불자가 구매한 정보에 대해서 알 수 없는 지불자 추적 불가능(Payer untraceability)과 수취인외의 다른 모든 사람들이 결탁한다 하더라도, 수취인이 어디로 부터 받은 전자화폐인지에 대해서 알 수 없는 수취인 추적 불가능(Payee untraceability)이 있다.

지불자 추적 불가능은 자신의 계좌번호와 연결되어 있는 발행단계와 지불단계가 서로 연결될 수 없음을 의미하며, 수취인 추적 불가능은 결재단계와 지불단계가 연결될 수 없음을 의미한다. 대부분의 전자화폐에서는 지불자 추적 불가능이 요구되나 수취인 추적 불가능은 요구되지 않는다. 수취인 추적 가능은 자신이 고소되었거나 익명의 금전 강탈을 막기위해 사용할 수 있다.

그러나 이러한 Privacy는 돈 세탁이나 탈세 그리고 통화 통제 불가능 등의 부정적인 면이나 전자화폐 시스템의 효율을 떨어뜨리거나 시스템을 복잡하게 하는 요인이 될 수 있다. 또한 Privacy에 대한 사회적인 관념이 아직 성숙되어 있지 않는 상황에서 과연 전자화폐에 이러한 기능을 제공하여야 할지의 여부는 많은 논란의 여지가 있다.

2.5.3 Transferable/Non-transferable

Non-transferable 전자화폐는 1회 사용 후에는 바로 상점과 은행간의 결재단계가 이루어져야 하는 것을 말하며, 이에 반해 Transferable 전자화폐는 발행단계이후의 지불단계가 여러번 이루어지는 즉, 지불자와 지불자간이나 지불자와 상점간의 단계가 복수회 이루어 진 후에 결재단계로 향하는 것을 말한다[22]. 상점에서 수령한 전자화폐를 바로 은행에 제출하지 않고 상점 자신이 지불인이 되어 또 다른 상점에 지불할 수가 있는 것을 의미한다. 현재 통용되고 있는 화폐제도는 Transferable하므로 전자화폐도 Transferable하는 것이 바람직하나

Transferable한 전자화폐를 구현할 경우 전자화폐를 위한 정보량은 transfer되는 횟수에 비례하여 증가하게 된다[22].

2.5.4 On-Line/Off-Line

On-Line은 고객 관리 및 전자화폐 관련 정보를 수록한 거대한 데이터베이스를 유지하여 매 지불단계시 마다 허가를 해주는 중앙 허가 기관 즉 은행과 직접 모든 참가자가 접촉하는 것을 말한다. 다시말해서 지불단계와 결재단계가 거의 동시에 행하여지는 것을 말하며 이중사용을 지불단계에서 사전에 방지할 수가 있으나 많은 통신량이 한곳으로 집중화되는 문제점과 거래에 따른 통신 비용이 증가하게 되는 문제점이 생기게 된다.

Off-Line은 지불단계와 결재단계가 동시에 이루어지지 않는 형태이며 일정 시간 경과후 수신된 전자화폐를 일괄 처리하여 은행에 결재 요구하는 것으로, 모든 단계가 완료된 후에 그리고 이중사용이 이루어지고 난 이후 은행에서 이중사용자에 대한 신분 검출이 가능한 점이 문제점으로 생각할 수 있다. 즉 이중사용 후 해외도피를 하거나 외국인이 사용 후 귀국해버리는 등의 사건이 발생할 소지가 있다. 그러나 통신량의 집중화 방지와 거래에 따른 통신 비용은 적게 소요된다. 두 방식의 응용면에서 고려해보면, On-Line은 고액거래로 높은 안전성을 요구하면서 운용비에 대한 부담이 크게 중요하지 않는 현금 시장에 적합하다. Off-Line은 많은 량의 소액거래가 이루어지는 곳으로 이중사용으로 인한 부정 가능 금액이 소규모인, 그리고 운용비 부담이 문제가 되는 곳에 적합하다.

미국을 중심으로 한 전자화폐는 On-Line형태를 이루고 있는 반면 유럽을 중심으로한 전자화폐는 스마트 카드의 발달 및 보급으로 인하여 Off-Line 형태로 많이 검토되어 지고 있다.

엄격한 의미에 있어서 On-Line에 의한 것은 전자화폐로 고려하지 않으며 전자화폐의 요구 사항에서 살펴 본 바와 같이 Off-Line으로 이루어 지는 것을 전자화폐로 다루고 있다. 전자화폐에 있어서의 가장 관심사는 Privacy를 만족하는 Off-Line에서의 이중사용 방지이다.

3. 전자화폐 현황

3.1 개발 현황

전자화폐에 대한 각국의 개발 현황은 마치 전쟁을 방불하게 할 만큼 치열하다. 미국은 정보통신에 대한 네트워크 기반이 잘 구축되어 있는 관계로 On-Line이나 인터네트를 이용한 전자화폐 개발이 중심이 되고 있으며 개인의 Privacy를 중시하며 스마트 카드 기술이 앞선 유럽에서는 Off-Line형 전자화폐가 주류를 이루고 있다.

미국

- VISA사 Stored Value Card 개발, 호주 시범 운용
- 마스터카드사 SEPP(Security Electronic Payment Protocol) 개발
- First Virtual사/Cyber Cash사[6]가 인터네트상에서 서비스 실시

유럽

- 영국 : 내셔날 웨스트 민스트/미들랜드 은행/BT의 몬덱스 카드 시범 운영
- 네덜란드 : Digicash사 e-Cash 시범 운영
- 핀란드 : Avant사의 카드 시스템을 이용한 시범 운용
- 포루투칼 :ATM 및 POS 네트워크 운영자인 SIBS(the Sociedade Interbancaria de Servicos)가 MEP(Multibanco Electronic

Purse)라는 전자지갑을 개발하여 1995년 2월 가동에 들어감.

- 벨지움 : BANKSYS라는 지급결재기관의 회원 은행이 중심이 되어 Proton이라는 카드를 이용하여 실험중에 있음.
- 덴마크 :은행, 통신회사가 중심으로 Dammont 카드를 이용하여 1993년 3월 가동하였음.
- 유럽 : CAFE(Conditional Access For Europe) 프로젝트에서 수행중

일본

- 일본 대장성 1998년 부터 전자화폐 실용화를 발표
- 일본 NTT 전자현금시스템 개발
- 몬덱스 카드 1997년 부터 사용

한국

- 동남은행과 광주은행 개발 및 시범 운용(1995년)[3]
- 한국은행, 금융결재원 등을 중심으로 한 IC 카드 표준 제정 완료.

3.2 연구 현황

전자화폐와 관련한 연구 방향은 On-Line에서 Off-Line으로 그리고 Cut & Choose에서 Challenge Response로 바뀌어 진행되고 있다. 현재 주된 관심 사항으로는 Privacy의 제공여부와 이에 따른 연구가 진행되고 있으며 D. Chaum을 중심으로 한 추적불가능한 전자화폐의 연구가 가장 활발하며 이 분야의 토대가 되고 있는 실정이다. 년도별 연구 현황은 다음과 같으며 1988년의 D. Chaum, A. Fiat, M. Noar에 의해 제안된 전자화폐 방식[26]이 가장 뛰어난 아이디어라 생각되며 그외의 대부분의 방식은 개선 또는 기능 추가로 생각되는 연구결과들이다.

1981년

네덜란드 암호학자인 D. Chaum에 의한 전자화폐 기초 기술인 추적불가능성 연구[8]

1982년

D. Chaum에 의한 On-Line 방식의 추적불가능 전자화폐를 위한 내용은닉서명 연구[13]

1983년

이스라엘 암호학자들인 S. Even 등이 Off-Line 방식으로 RSA 암호와 Tamper-proof device를 이용한 전자지갑을 구현[20]

1985년

D. Chaum에 의한 추적불가능 서명법인 구체적인 내용은닉서명 제안[9]

1988년

- D. Chaum 등에 의한 최초의 이론적인 전자화폐 방식인 추적불가능 전자화폐를 제안[26]
- On-Line 전자화폐를 I.B. Damgard가 제안[36]

1989년

- On-Line 전자화폐를 D. Chaum도 제안[29]
- 일본 NTT의 T. Okamoto와 K. Ohta에 의한 ZKIP[10]와 추적불가능을 연계시켜 Transferability를 제공하는 전자화폐 방식 제안[16]
- CFN[26] 방식의 효율을 개선한 방식을 D. Chaum 등에 의해 제안[14]

1990년

- 미국의 B. Heyes는 1회용 추적불가능서명을 이용한 전자화폐를 제안[15]
- CFN 방식을 보다 개선한 효율적인 Off-Line 전자화폐를 H.V. Antwerpen이 제안[40]

1991년

- 일본의 T. Okamoto와 K. Ohta는 분할 사용이 가능한 전자화폐를 제안[18]
- I.B. Damgard가 제안한 On-Line 전자화폐의 추적가능함을 보이고 개선안을 제안[37]
- Antwerpen[40] 방식의 문제점을 지적하고 개선한 방식을 미국의 R. Hirschfeld가 제안[33]

1992년

- Tamper-proof device를 이용한 전자지갑이 제안됨[19],[29]
- Transferable 전자화폐는 정보량이 증가하지 않고서는 구현할 수 없음을 D. Chaum과 T.P. Pedersen이 증명[22]
- Schnorr 방식을 이용하여 분할 가능하며 효율적인 전자화폐 제안[21]

1993년

- S. Brands[25], N. Ferguson[27],[28], M. Yung[17] 등이 효율적인 Challenge Response 방식의 전자화폐를 제안
- 이전 전자지갑[19]의 Privacy를 개선한 방식을 R.J.F. Cramer와 T.P. Pedersen이 제안[23]
- 지불단계에 Schnorr의 인증 방식을 이용한 전자화폐 방식[30]과 필요시 추적 가능한 전자화폐 방식[31]이 제안됨

1994년

- S. Brands[25]의 전자화폐에 분할성을 추가한 전자화폐가 제안[38]
- ElGamal 서명 방식[12]을 이용한 전자화폐를 제안하여 S. Brands 방식의 효율을 개선[41]
- NIZK(Non-Interactive Zero-Knowledge)에 안전성을 두어 구성된 추적 불가능 전자화폐를 S. D'Amiano와 G. Di. Crescenzo가 제안하여 transferable할지라도 정보량이 증가하지 않음을 보임[42]
- 은행이 관리해야할 거대한 데이터베이스의 양을 줄이는 방안을 제안[34]

1995년

- NIZK를 이용한 전자화폐[42]가 추적가능함을 B. Pfitzmann 등이 보임[43]
- 전자화폐에서의 추적불가능성이 돈 세탁 등의 범죄에 악용될 수 있다. 이러한 문제를 해결하고자 하는 공정한 내용은닉 서명이 제안[44]
- 전자화폐의 지불단계에서의 구매자(Payer)와 상점(Payee) 사이의 공정한 거래를 제공하는 방안 제안[45]
- 내용은닉서명이 아닌 Secret-Key Certificates라는 개념을 이용하여 보다 효율적인 전자화폐 방식을 제안[46]

4. 전자화폐의 분류

전자화폐의 분류는 분류 방법에 따라 여러 가지로 나눌 수 있다. 본 논문에서는 먼저 예금 인출 여부 및 결재 종료성에 따른 분류, 결재 방식에 의한 분류, 그리고 결재액의 규모에 의한 분류로 나열하였다.

4.1 예금의 인출여부에 의한 분류[2]

문헌 [2]에 의하면 전자지갑에의 가치 저장시 예금의 인출여부 및 결재 종료성 등에 따라 범용 선불형 전자화폐, Off-Line 직불형 전자화폐와 Mondex형 전자화폐로 나누고 있다. 범용 선불형 전자화폐는 비밀번호를 사용해서 자신의 은행계좌로부터 예금을 인출하여 전자지갑에 저장한 후 지불단계에서 Off-Line 단말기를 이용하여 비밀번호의 확인없이 익명으로 거래할 수 있는 것으로 기존의 단일용도

선불카드와 자기띠를 이용한 선불카드의 보완적인 전자화폐인 셈이다. Off-Line 직불형 전자화폐는 지불단계에서 Off-Line 단말기에 의해서 비밀번호의 확인 후 익명으로 거래하는 것을 말하며 Mondex형 전자화폐는 전자화폐 공급업자가 현금 또는 예금과 교환하여 카드 사용자에게 공급하며 은행계정을 통하지 않고 카드사용자, 가맹점 그리고 가맹 은행간에 자유로이 이체될 수 있는 것을 말한다. 보다 자세한 내용은 참고문헌 [2]를 이용하여 주기 바라며 각각의 기능과 특징은 표 1과 같다.

4.2 결재방식에 의한 분류[47]

현금이나 신용카드로 지불하는 기존의 결재방법, 거래 액수가 중간 정도인 결재가 중심이 될 인터네트상의 지불 방법 그리고 소액 결재가 중심이 될 스마트 카드에 의한 지불 방법으로 분류될 수 있다. 전자화폐에서 요구되는 사항별 결재 방식의 비교를 표 2에 나타내었다. 그리고 이론형으로 분류되는 대표적인 두 방식에 대한 비교는 표 3과 같다.

표 1. 전자화폐의 유형별 기능

종류 구분	범용 선불형 전자화폐	Off-Line 직불형 전자화폐	Mondex형 전자화폐
화폐저장 기능	○	○	○
저장시 비밀번호 사용	○	○	○
거래전 이자지급	×	○	×
거래시 비밀번호 사용	×	○	×
예금 인출 시점	저장시	통보시	저장시
단말기 방식	Off-Line	Off-Line	Off-Line
은행간 차액 결제	○	○	×
카드간 자금이체	×	×	○
법정화폐성	×	×	○

본 자료는 참고문헌 [2]에 수록된 내용임.

표 2. 결제 방식의 비교

방식	기존 서비스		인터네트 서비스		스마트카드 지불	
요구조건	현금	신용카드	Cyber Cash류	e-Cash	Mondex	이론형
안전성	×	×	○	○	○	
이중사용금지	×	×	×	○	×	표
프라이버시	○	×	×	○	○	3
off-line성	○	○	○	×	○	참
양도가능성	○	-	-	○	○	조
분할성	×	-	-	×	○	

표 3. 이론형 전자현금 방식의 비교

방식 요구조건	CFN88 전자화폐	Brands 전자화폐
안전성	○	○
이중사용금지	○	○
프라이버시	○	○
off-line성	○	○
양도가능성	×	×
분할성	×	×
기본기술	Cut & Choose	Challenge Response

4.3 결재액에 의한 분류

전자화폐의 결재단계에서 거래되는 금액에 따라 분류할 수도 있다. 이 분류는 특별한 의미는 없고 결재단계에 있어서의 거래액에 따른 분류로 전자화폐의 응용별 발전단계에 따른 적합한 분류로 전자화폐의 발전 방향을 예측할 수 있다.

- 고액(100만원 이상) 결재 : 기업간의 거래가 중심으로 EDI를 중심으로 발전하리라 예상된다.
- 중액 결재 : 개인과 기업 또는 소매점과의 거래 등이 중심으로 현재 사용되고 있는 신용카드를 이용한 지불방법을 전자화로 가능하다.
- 소액(만원 또는 십만원 이하) 결재 : 개인과 개인의 거래가 중심으로 후불 또는 선불 방식의 전자화폐도 필요하게 된다.

5. 전자화폐의 대표적인 방식들

전자화폐의 대표적인 방식들은 현재 시험 또는 이용중인 실제적인 방식(보다 정확하게 표현한다면 전자지불 시스템)과 암호학자들에 의해 연구되고 있는 이론적인 방식으로 나누어 볼 수 있다. 이들 각각에 대한 내용을 본절에서는 설명하고자 한다.

5.1 인터네트형 방식들

현실적인 전자화폐 방식인 공용망이나 인터네트를 이용하는 전자화폐는 First Virtual, Cyber Cash 그리고 e-Cash로 대별할 수가 있다.

5.1.1 First Virtual형

First Virtual형은 미리 신용카드나 은행 계좌번호, 전자메일 주소 등의 정보를 전화나 팩시밀리로 등록해 두고 ID 번호를 이용자에게 발행하는 방식이다. 인터네트상에서 상품을 사고자 하는 경우 ID번호를 이용하여 구입의사를 나타낸다. First Virtual은 이 번호를 받아서 등록되어 있는 개인정보를 탐색하여 전자메일로 본인에게 확인을 받는다. ID번호나 전자메일의 송수신시에는 암호나 특수한 소프트웨어를 사용하지 않기 때문에 소요 경비를 줄일 수 있는 특징이 있다. First Virtual형 전자화폐의 구조는 그림 2와 같다.

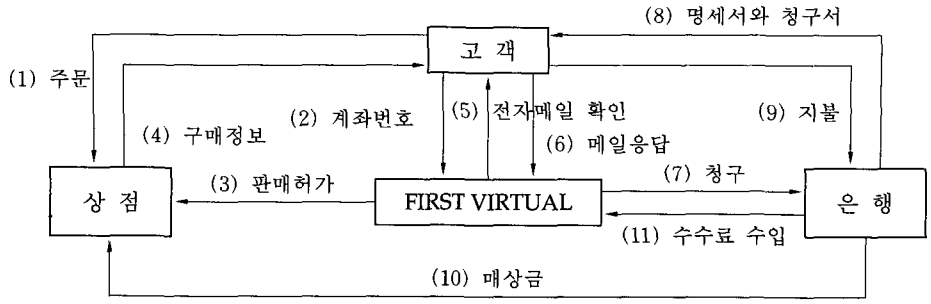


그림 2. First Virtual 전자화폐

5.1.2 Cyber Cash형

Cyber Cash형은 인터네트에서 암호 소프트웨어를 사용하여 신용카드 회사나 금융기관과 신용카드 등의 정보를 안전하게 교환한 후 이용자가 전용 소프트웨어를 사용해서 자신의 카드번호를 입력하면 Cyber Cash와 신용카드 회사간의 거래이후 자동적으로 물품 구매가 이루어지는 방식이다. 768비트의 RSA 암호에 의한 인증이 이루어지며, 고객이 보낸 신용카드 번호는 상점에서는 볼 수 없으며 Cyber Cash사에서 복호되어 카드 심사가 이루어지는 높은 안전성이 제공되는 특징이 있다. Cyber Cash형 전자화폐의 구조는 그림 3과 같다.

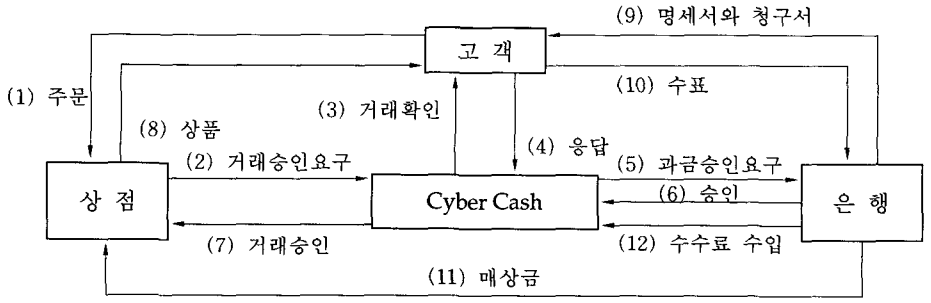


그림 3. Cyber Cash 전자화폐

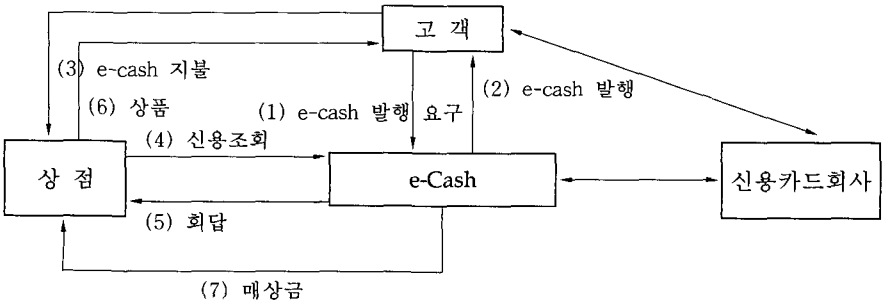


그림 4. e-Cash 전자화폐

5.1.3 e-Cash형

엄밀한 의미에 있어서의 전자화폐는 이 e-Cash형을 의미한다해도 과언이 아닐 것이다. Off-Line과 Privacy 등의 전자화폐로써의 요구조건을 갖춘 네덜란드 DigiCash사의 시스템으로 현재 미국의 마크트웨인 뱅크에서 상품 구매와 자금 이체로 1995년 11월부터 사용되고 있다. 본 논문 전체에서 설명되고 있는 전자화폐의 주된 내용은 e-Cash형의 전자화폐이며 그림으로 나타낸 구조는 그림 4와 같다.

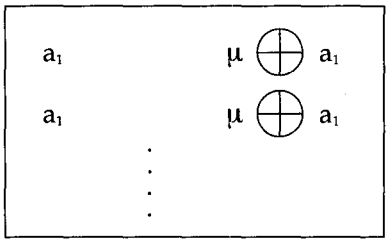


그림 5. 보통용지 이용

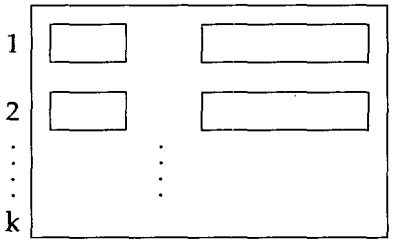


그림 6. 마법종이 이용

5.2 이론적인 방식들

전자화폐에 대한 이론적인 연구는 D. Chaum이 독보적이라 해도 과언이 아닐 것이다. D. Chaum이 제안한 Off-Line이며 Cut & Choose 전자화폐 그리고 S.Brands가 제안한 Challenge Response 전자화폐 그리고 T. Okamoto와 K. Ohta의 분할 가능한 전자화폐[18] 등이 대표적인 전자화폐의 이론적인 방식들이다. 여기서는 가장 대표적인 두방식인 CFN 방식[26]과 Brands 방식[25]을 소개한다.

5.2.1 CFN 방식

CFN 방식은 D. Chaum, A. Fiat, M. Naor가 제안한 이론적인 전자화폐의 대표적인 방식으로 Off-Line이며, Privacy를 제공하면서도 이중사용을 검출할 수 있는 즉 이중사용자만 색출이 가능한 Cut & Choose 방식의 전자화폐다. 이 방식은 다른 이론적인 방식의 기초가 되었으며 많은 개선과 기능 추가가 계속되고 있다. 여기에서는 마법종이 개념을 이용하여 간략히 설명하고자 한다.

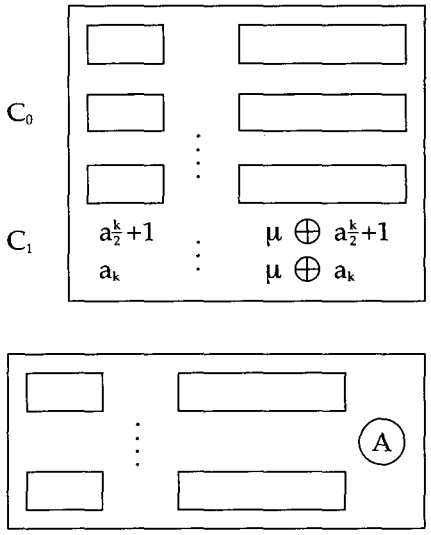


그림 7. 마법종이를 이용한 전자화폐

(발행단계)

(step 1) 구매자 Alice는 난수 $\{a_1, a_2, \cdots, a_k\}$를 선택하여 그림 5와 같이 보통용지위에 기록한다. 여기서 μ는 Alice의 계좌번호이다.)

(step 2) Alice는 기록된 종이위에 마법종이를 붙여서 은행에 제출한다(그림 6 참조).

(step 3) 은행은 $k/2$개의 난수로 Alice가 숨긴 내용을 밝히기를 요구한다. (간단히 하기 위하여 $k/2$개의 난수를 $\{k/2+1, \cdots, k\}$로 한다.)

(step 4) Alice는 은행이 지정한 난수 번호, $\{k/2+1, \cdots, k\}$에 해당하는 마법종이를 떼어서 step 1의 그림에서와 같은 형태의 식으로 되어 있다는 것을 증명한다.

(step 5) 은행은 마법종이를 떼어 낸 부분 C_1 부분을 확인한다(그림 7의 상단 부분 참조).

(step 6) 은행은 마법종이가 떼어지지 않은 부분에 은행 도장을 찍어 Alice에게 양도하며 Alice 계좌에서 해당 금액을 빼낸다. 은행으로 부터 수령한 이것이 최종 전자화폐 $\hat{C}_0$가 되게 된다(그림 7의 하단 부분 참조).

(지불단계)

(step 1) Alice는 상점에 물건 구매와 함께 전자화폐를 제시한다.

(step 2) 상점에서는 난수열 $\{e_1, e_2, \cdots, e_{k/2}\}$를 Alice에게 건네주며 전자화폐중의 마법종이로 덮힌 부분을 보여줄 것을 요구한다.

(step 3) Alice는 $e_i = 0$인경우 a_i를, $e_i = 1$인 경우는 $\mu \oplus a_i$를 마법종이를 떼내어 상점에 보여준다. 예를들어 $(e_1, e_2, \cdots,) = (0, 1, \cdots)$라면 그림 8의 $\hat{C}_0'$와 같이 된다.

(결재단계)

(step 1) 상점은 은행에 $\hat{C}_0'$를 제출한다.

(step 2) 은행은 상점의 계좌에 해당금액을 이체 시켜준다.

이중사용자의 검출법

Alice가 $\hat{C}_0'$를 다른 상점에 다시 사용하여 이중 사용하였다고 가정해보자. 이때, 그 상점이 건네 준 난수열을 (1, 0, ⋯)라고 하면, Alice는 그림 9와 같은 $\hat{C}_0''$를 상점에 건네주게 되며 은행은 이들 정보를 상점으로 부터 받게 된다. 은행은 상점들로 부터 받은 $\hat{C}_0'$와 $\hat{C}_0''$를 이용하여 a_1과 $\mu \oplus a_1$으로 부터 이중사용자의 계좌번호인 μ를 알게된다. 여기서 상점이 건네주는 난수열의 랜덤성과 난수열의 길이에 이중사용자의 검출 확률이나 안전성이 의존하게 된다.

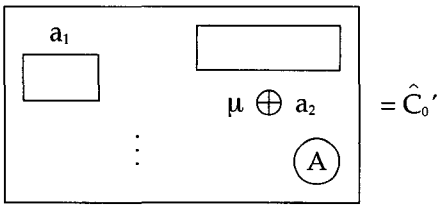


그림 8. 전자화폐 $\hat{C}_0'$

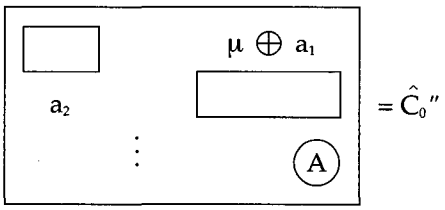


그림 9. 전자화폐 $\hat{C}_0''$

5.2.2 Brands 방식

Cut & Choose 방식의 비효율적인 발행단계를 보다 개선한 Challenge Response 방식을 처음으로 고려한 전자화폐 방식이다. 현재 가장 많은 각광을 받고 있는 방식으로 인터네트상

에서도 활용 가능한 방식과 내용은닉서명을 사용하지 않는 방식들로 발전하고 있다. 여기서는 Brands 방식을 알기 쉽게 약간 변형하여 소개한다.

(발행단계)

(step 1) Alice는 식 (1)를 만족하는 x_1, x_2, y_1, y_2를 임의로 선정한 다음, $I_A = f(\mu)$를 공개한다. 또 G도 계산한다. 여기서 H는 암호학적으로 안전한 일방향 해쉬 함수이다.

$$\left.\begin{aligned} a &= x_1+x_2 \bmod P\text{-}1 \\ a+\mu &= y_1+y_2 \bmod P\text{-}1 \end{aligned}\right\} \quad (1)$$

$$G = H(g_1^{x} g_2^{y_1},\ g_1^{x_2} g_2^{y_2}) \quad (2)$$

(step 2) Alice는 은행에

$$Z = r \times G \bmod N \quad (3)$$

을 제출한다.

(step 3) Alice는 영지식증명(ZKIP)으로 (I_A, Z)가 식(1), (2), (3)을 만족하고 있음을 은행에 증명한다.

(step 4) 은행은 $Z^d = r \times G^d \bmod N$ 계산하여 Alice에게 양도한다.

(step 5) Alice는 $Z^d/r = G^d$를 계산하여 전자화폐 C를 얻게된다.

$$C = (G,\ G^d,\ g_1^{x_1} g_2^{y_1},\ g_1^{x_2} g_2^{y_2})$$

(지불단계)

(step 1) Alice는 상점에 전자화폐 C를 제시한다.

(step 2) 상점은 $G \stackrel{?}{=} H(g_1^{x_1} g_2^{y_1},\ g_1^{x_2} g_2^{y_2})$, $(G^d)^e \stackrel{?}{=} G$를 검사한다.

(step 3) 상점은 Alice에게 난수 α를 보낸다.

(step 4) Alice는 상점에 v, w를 보낸다.

$$v = x_1+\alpha x_2 \bmod P\text{-}1$$
$$w = y_1+\alpha y_2 \bmod P\text{-}1$$

(step 5) 상점은 다음식이 성립하는지를 검사한 후 맞으면 요구하는 물건을 Alice에게 제공한다.

$$g_1^{v} g_2^{w} \stackrel{?}{=} g_1^{x_1} g_2^{y_1} (g_1^{x_2} g_2^{y_2})^{\alpha} \bmod P$$

(결재단계)

(step 1) 상점은 은행에 Alice와 주고 받은 모든 통신내용, C, α, v, w를 은행에 제시한다.

(step 2) 은행은 Double spending 여부를 확인한 후 전자화폐 C에 해당하는 돈을 상점에 양도한다.

이중사용자의 검출법

Alice가 만일 이중 사용을 하게 되면 은행은 상점들로 부터 다음과 같은 거래 정보를 얻게 된다.

$$\begin{cases} v_1 = x_1+\alpha_1 x_2 \\ v_2 = x_1+\alpha_2 x_2 \end{cases} \quad \begin{cases} w_1 = y_1+\alpha_1 y_2 \\ w_2 = y_1+\alpha_2 y_2 \end{cases}$$

이들 정보로 부터 (x_1, x_2), (y_1, y_2)를 알게되며 식 (1)로 부터 이중 사용자의 계좌번호인 μ를 알게되어 이중 사용자를 검출하게 된다.

6. 향후 전망

전쟁이라 할 만큼 많은 관심과 경쟁을 불러 일으키고 있는 전자화폐 사회에 대해서 부정적인 요소를 제기하거나 아직은 시기상조라는 의견도 많이 제기되고 있다. 또, 현금이 없이 전자화폐만으로 이루어지는 사회는 생각할 수 없으며 지금의 화폐제도속에 전자화폐를 포함하는 사회가 계속될 것으로 약간 중도적인 입장에서 예상하는 전문가들도 많다. 그러나 분명한 사실은 통화혁명이라 할 만큼의 급격한 변화는 없다할 지라도 표준화와 안전 대책만 수립된다면 전자화폐는 예상보다 빨리 보급될 것으로 생각된다.

현재 문제가 되고 있거나 앞으로 해결해야 할 과제들로는 다음과 같은 것들을 예상할 수 있다. 이들은 이미 어느 정도의 문제점들이 해결된 것도 있으며, 이외의 많은 문제점도 발생할 소지가 있다.

- 완전 범죄 가능 (추적 불가능성)
- 돈 세탁이나 탈세 등의 악용 여부와 통화 통제의 곤란
- 양도에 따른 통신량 증가
- Black List 작성에 따른 개인의 프라이버시 침해
- 개인의 프라이버시 제공 여부
- 새로운 화폐 통용을 위한 기반 구축
- 전자화폐 사용의 홍보
- 전자화폐의 표준화 확립 등

7. 결 론

전자화폐에 대한 관심이 고조되고 있는 시점에서 암호학적인 측면에서의 안전대책을 고려한 전자화폐를 살펴 보았다. 산업혁명 이후의 최대 혁명이 될 통화혁명의 주체인 전자화폐는 많은 나라들이 관심을 가지고 추진하고 있지만 아직 우리나라는 다른 나라의 기술을 연구하거나 활용하는 단계에 머물러 있는 실정이며 안전 대책을 고려한 연구는 아직 초보단계다. 이에 우리나라에서도 금융 전문가, 암호 전문가 그리고 컴퓨터 전문가 등을 중심으로 한 활발한 연구가 이루어져 독자적인 전자화폐의 개발과 보급으로 세계의 전자화폐 전쟁에 참여할 수 있어야 할 것이다. 마지막으로 이 자료가 전자화폐 관련 기초 자료로써 활용될 수 있기를 기대한다.

참 고 문 헌

[1] 전자신문, "위조지폐와 전자화폐", 1996. 4.22. 일자

[2] 탁승호, "전자화폐와 결재 시스템", 더벵커사, 1996.

[3] 화폐혁명의 주역 전자화폐 국내 첫선, 이코노미스트, No.302, pp.62-63, August, 1995.

[4] 박승안, 신형용, "전자화폐의 연구현황", 통신정보보호학회지, Vol.4, No.4, pp.29-34, 1994.

[5] 박승안, 신형용, "Internet을 위한 전자화폐", 통신정보보호학회지, Vol.5, No.3, pp.122-126, 1995.

[6] 디지털 시대의 통화혁명, Cyber Cash, 인터네트, No.8, pp.94-112, Feb., 1996.

[7] 박 춘식, "전자투표", 통신정보보호학회지, Vol.6, No.1, pp.5-20, 1996.

[8] D. Chaum, "Untraceble Electronic Mail, Return Addresses, and Digital Pseudonyms", Communications of the ACM, Vol.24, No.2, pp.84-88, 1981.

[9] D. Chaum, " Security without Identification : Transaction Systems to Make Big Brother Obsolete", Communications of the ACM, Vol.28, No.10, pp.1030-1044, 1985.

[10] S. Goldwasser, S. Micali and C. Rackoff, "The Knowledge Complexity of Interactive Proof Systems", Proceedings of the 17th ACM Symposium on Theory of Computing, pp.291-304, 1985.

[11] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital

signatures and public-key cryptosystems", Communications of the Association for Computing Machinery, Vol.21, No.2, pp.120-126, 1978.

[12] T. ElGamal, "A public key cryptosystem and signature scheme based on discrete logarithms", IEEE Trans. Inform. Theory, Vol.31, No.4, pp.469-472, 1985.

[13] D. Chaum, "Blind Signatures for Untraceable Payments", Proc. of Crypto'82, Plenum Press, pp.199-203, 1983.

[14] D. Chaum, B. den Boer, E. van Heyst, S. Mjolsnes and A. Steenbeek, "Efficient Offline Electronic Checks", Advances in Cryptology, Proceedings of EUROCRYPT'89, pp.294-0301, 1989.

[15] B. Hayes, "Anonymous One-Time Signatures and Flexible Untraceable Electronic Cash", Advances in Cryptology, Proceedings of AUSCRYPT'90, Springer-Verlag, pp.294-305, 1990.

[16] T. Okamoto and K. Ohta, "Disposable Zero-Knowledge Authentications and Their Applications to Untraceable Electronic Cash", Advances in Cryptology, Proceedings of Crypto'89, pp.481-496, 1989.

[17] M. Franklin and M. Yung, "Secure and Efficient Off-Line Digital Money", Proc. of 20th International Colloquium on Automata, Languages and Programming (ICALP), pp.449-460, 1993.

[18] T. Okamoto and K. Ohta, "Universal Electronic Cash", Advances in Cryptology, Proceedings of Crypto'91, pp.324-337, 1991.

[19] D. Chaum and T.P. Pedersen, "Wallet Databases with Observers", Advances in Cryptology, Proceedings of Crypto'92, pp.89-105, 1992.

[20] S. Even, O. Goldreich and Y. Yacobi, "Electronic Wallet", Advances in Cryptology, Proceedings of Crypto'83, pp.383-386, 1983.

[21] J.C. Pailles, "New Protocols for Electronic Money", Advances in Cryptology, Proceedings of AUSCRYPT'92, pp.263-274, 1992.

[22] D. Chaum and T.P. Pedersen, "Transferred Cash Grows in Size", Advances in Cryptology, Proceedings of EUROCRYPT'92, pp.390-407, 1992.

[23] R.J.F. Cramer and T.P. Pedersen, "Improved privacy in wallets with observers", Advances in Cryptology, Proceedings of EUROCRYPT'93, pp.329-343, 1993.

[24] D. Chaum, "Achieving Electronic Privacy", Scientific American, Vol.267, No.2, pp.76-81, August, 1992.

[25] S. Brands, "Untraceable Off-Line Cash in Wallet with Observers" Advances in Cryptology, Proceedings of Crypto'93, pp.302-317, 1993.

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

[27] N. Ferguson, "Single term off-line coins", Advances in Cryptology, Proceedings of EUROCRYPT'93, pp.318-328, 1993.

[28] N. Ferguson, "Extensions of Single term coins", Advances in Cryptology, Proceedings of Crypto'93, pp.292-301, 1993.

[29] D. Chaum, "Online Cash Checks", Advances in Cryptology, Proceedings of EUROCRYPT'89, pp.288-293, 1989.

[30] H.Y. Youm, S.L. Lee and M.Y. Rhee, "Practical Protocols for Electronic Cash", 1993 Korea-Japan Joint Workshop on Information Security and Cryptography, Proceedings of JW-ISC'93, pp.02.01-02.13, Oct., 1993.

[31] C.H. Lim and P.J. Lee, "A Practical Electronic Cash System for Smart Cards", 1993 Korea-Japan Joint Workshop on Information Security and Cryptography, Proceedings of JW-ISC'93, pp.04.01-04., Oct., 1993.

[32] S.von Soloms and D. Naccache, "On Blind Signatures and Perfect Crimes", Computer & Security, Vol.11, pp.581-583, 1992.

[33] R. Hirschfeld, "Making Electronic Refunds Safer", Advances in Cryptology, Proceedings of Crypto'92, Springer-Verlag, pp.106-112, 1992.

[34] J.L. Camemisch, J.M. Piveteau and M.A. Stadler, "An Efficient Electronic Payment System Protecting Privacy", Computer Security-ESORICS'94, Springer-Verlag, pp.207-215, 1994.

[35] J-P. Boly, A. Bosselaers, R. Cramer, R. Michelsen, S. Mjolsnes, F. Muller, T. Pedersen, B. Pfitzmann, P. Rooij, B. Schoemakers, M. Schunter, L. Vallee and M. Waidner, "The ESPRIT Project CAFE - High Security Digital Payment Systems -", Computer Security-ESORICS'94, Springer-Verlag, pp.217-230, 1994.

[36] I.B. Damgard, "Payment systems and Credential Mechanisms with Provable Security Against Abuse by Individuals", Advances in Cryptology, Proceedings of Crypto'88, Springer-Verlag, pp.328-335, 1988.

[37] B. Pfitzmann and M. Waidner, "How to Break and Repair a Provably Secure Untraceable Payment System", Advances in Cryptology, Proceedings of Crypto'91, Springer-Verlag, pp.338-350, 1991.

[38] T. Eng and T. Okamoto, "Single-Term Divisible Electronic Coins", Advances in Cryptology, Proceedings of EUROCRYPT'94, Springer-Verlag, pp.306-319, 1994.

[39] S.H. Low, N.F. Maxemchuk and S. Paul, "Anonymous Credit Cards", Proceedings of the 2nd Annual ACM Conference on Computer and Communications Security, ACM Press, pp.108-117, 1994.

[40] H. Van. Antwerpen, "Off-Line electronic Cash", Master's thesis, Eindhoven University of Technology, 1990.

[41] Y. Yacobi, "Efficient electronic money", Advances in Cryptology, Proceedings of ASIACRYPT'94, Springer, pp.153-163, 1994.

[42] S. D'Amiano and G. Di. Crescenzo, "Methodology for Digital Money based on General Cryptographic Tools", Advances in Cryptology, Proceedings of

EUROCRYPT'94, Springer, pp.156-170, 1994.

[43] B. Pfitzmann, M. Schunter and M. Waidner, "How to Break Another "Provably Secure" Payment System", Advances in Cryptology, Proceedings of EUROCRYPT'95, pp.121-132, 1995.

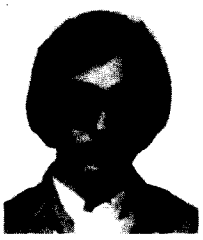
[44] M. Stadler, J-M. Piveteau and J. Camenisch, "Fair Blind Signatures", Advances in Cryptology, Proceedings of EUROCRYPT'95, pp.209-219, 1995.

[45] M. Jakobsson, "Ripping Coins for a Fair Exchange", Advances in Cryptology, Proceedings of EUROCRYPT'95, pp.220-230, 1995.

[46] S. Brands, "Restrictive Binding of Secret-Key Certificates", Advances in Cryptology, Proceedings of EUROCRYPT'95, pp.231-247, 1995.

[47] K. Ohta, M. Abe, E. Fujisaki and H. Moribatake, "Electronic Money Schemes", NTT R&D, Vol.44, No.10, pp.931-938, 1995(in Japanese).

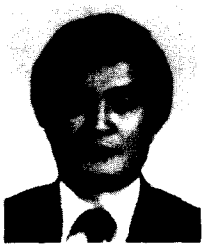
□ 著者紹介



박 춘 식(정회원)

광운대학교 전자통신과 졸업(학사)
한양대학교 대학원 전자통신과 졸업(석사)
일본 동경공업대학 전기전자공학과 졸업(암호학 전공, 공학박사)
1989년 10월 ~ 1990년 9월 일본 동경공업대학 객원 연구원
1982년 ~ 현재 한국전자통신연구소 책임연구원

※ 주관심 분야 : 암호이론, 정보이론, 통신이론



이 대 기

1966년 한양대학교 전자공학과(학사)
1987년 한양대학교 전자공학과(석사)
1980년 ~ 1992년 ETRI 산업기술개발부장, 지상시스템연구부장
1992년 ~ 현재 ETRI 책임기술원
한국통신정보보호학회 산학이사