특 집

전자화폐를 위한 암호 프로토콜

최 은 화*, 서 창 호**, 김 석 우***

*공주대학교 대학원 수학과, **공주대학교 응용수학과(정보보호전공), ***한세대학교 정보통신공학

I. 서 론

인터넷상의 전자상거래와 이를 이용한 가상의 시장에서 가장 관심을 끄는 지불 방법이 바로 전자화폐이다. 전자화폐의 관심이 인터넷의 영향으로 그 어느 때보다도 대단하다. 이는 컴퓨터의 발달과 인터넷의 급속한 보급으로 인한 영향으로 생각되며, 정보화 물결의 위력을 새삼 느끼게 한다.

전자상거래의 지불 방법이나 보안 요소는 다른 학문적인 요소와는 달리 그 실용적인 성격과 파급 효과로 인하여 세계 각국의 정보 기관이나 연구소에서 주도권 쟁탈을 위한 노력을 기울이고 있다. 이러한 전자상거래의 기법들은 전자 상거래의 기술을 연구하고 제시하는 쪽보다는 현실적인 필요성에 의해 금융기관이나 전자상거래 서비스를 제공하는 업체들에 의해 주도적으로 개발하고 있는 사항이며, 전 산업과 모든 국민에게 미치는 영향은 실로 막대할 것이다. 개인과 밀접한 관계를 갖고 우리에게 다가오고 있는 전자화폐는 통화혁명의 주체가 되어 금융계는 물론이고 경제계 그리고 온 세상을 변화시키려 하고 있다.

이러한 전자화폐는 지금까지의 화폐와는 다르다. 더 이상 금속이나 종이로 만들어지는 것이 아니라 기억장치에 저장된 전자적 기호와 중앙처리장치(CPU) 그리고 운영체제(O/S)로 이루어져 있다. 그리하여 통신회선을 통한 네트워크에서 네트워크로 이동할 수 있을 뿐만 아니라, 지금처럼 주머니에 동전과 여러 개의 카드로 불룩한 지갑을 가지고 다녀야 하는 불편을 덜어 준다. 또한 물건 구매시에도 신용카드와 달리 계산서 금액만큼 바로 빼낼 수 있어, 불과 3~4초만에 결제를 끝내는 등 매우 신속하고 간편하다. 또한 금전을 주고받을 필요 없이 명함 만한 카드에 반도체 칩을 내장, 쇼핑은 물론 각종 신용거래 등 경제활동을 수반하는 행위를 할 수 있다. 웹(web)에서의 전자상거래는 대금결제 및 조세처리와 같은 회계 ERP에 연결될 수 있다. 이러한 연결고리의 중개자가 전자화폐인 것이다. 이러한 전자화폐는 IC형과 네트워크형의 형태에 따라 그 효과가 다양하다.

전자화폐의 본격적인 상용화를 위한 중요한 과제 중의 하나는 고도 정보사회에서 야기되는 안전성 문제를 해결하는 암호 프로토콜(Cryptographic protocol) 분야이다. 정보사회가 고도화할수록 통신정보의 불법적인 도청과 함께, 원거리 엑세스에 발생되는 개인식별 문제, 컴퓨터 정보의 무단삭제 및 변조 등의 무결성 문제가 심각한 문제로 대두되고 있다. 이런 문제를 해결하는 암호기술이 암호 프로토콜 분야이다.

전자화폐 프로토콜은 D. Chaum이 은닉 서명[1]을 근간으로 한 추적 불가능한 전자화폐 프로토콜을 제시한 이후 분할성 및 양도성 등 전자화폐가 가져야 할 기능들을 추가하는 방향으로 새로운 전자화폐 프로토콜들이 제시되어 왔다. 초기 전자화폐 프로토콜은 지불과 이체가 하나의 트랜잭션으로 이루어지는 온라인 방식에서 시작되었으나, [2]에서 이중 사용 검출의 기법이 제시된 이후 지불과 이체가 별도의 트랜잭션으로 이루어지는 오프라인 전자화폐 프로토콜이 주류를 이루게 되었다.

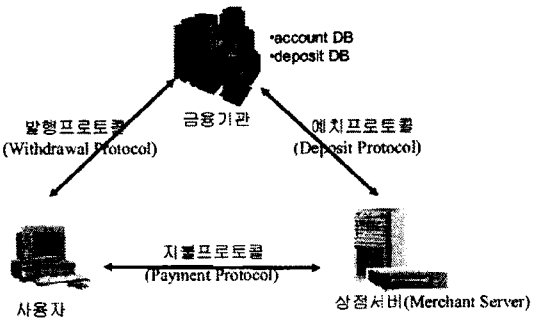
본 논문에서는, 전자화폐를 암호학적인 측면에서 살펴보고, 전자화폐의 가장 핵심적인 기술인 추적 불가능성, 프라이버시 제공 기술 그리고 이중 사용 방지 기술 등과 암호 이론과의 관련성을 중심으로 정리하였다. 특히 기존에 제안되어 있는 대표적인 전자화폐 방식들에 대해서 암호 프로토콜 관점에서 고찰하여 보았으며, 전반적인 전자화폐 관련 내용도 추가하였다.

II. 전자화폐

1. 전자화폐란?

기본적으로 전자화폐는 〈그림 1〉과 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 구매자로부터 받은 전자화폐를 은행에 제출하여 상점의 계좌로 자금이체를 시켜주는 결제단계(Deposit phase)로 구성되어 있다.

먼저 구매자인 A인 은행으로부터 만원자리 전자화폐를 자신의 계좌로부터 받아 상점에서 물건을 산다고 가정해보자. 이때 은행과 상점이 결탁을 하게 되면 구매자인 A의 구매에 관한 정보인, 언제, 어디서 무엇을 사는지에 대한 개인의 프라이버시 관련 정보가 쉽게 노출되게 된다. (참고로 개인의 프라이버시를 전자화폐에서 제공여야만 하는지의 여부는 아직도 논란의 소지가 많이 있으나 본 논문에서는 프라이버시를 제공하는 전자화폐를 고려한다. 좀더 자세한 내용은 Privacy와 Untraceability의 내용을 참조하기 바란다.) 이러할 경우 관연 어떻게 하면 개인의 프라이버시를 유지하면서 안전한 전자화폐를 만들 수가 있을까?



〈그림 1〉 전자화폐

2. 전자화폐 분류

전자화폐는 물리적 정보 기록 방식, 휴대 가능 여부에 따라 IC카드형 전자화폐와 네트워크형 전자화폐로 나뉜다. 또한 양도 여부에 따라 개방형 전자화폐와 폐쇄형 전자화폐로 분류한다. IC카드형 전자화폐는 휴대가 간편하고 일반상점에서 사용하기가 편리하다는 장점이 있다. 이에 반해 네트워크형 전자화폐는 컴퓨터를 통해 원거리에 있는 사람에게 이전시키는 것이 편리하다는 장점을 지니고 있지만, 휴대하고 다니는 것이 불가능하다는 단점을 가지고 있다.

IC카드형 전자화폐의 경우 외형은 기존의 현금카드 및 신용카드와 거의 비슷하다. 기존의 현금카드 및 신용카드는 플라스틱카드에 판독만 가능한 마크네틱테이프가 부착되어 있지만, IC카드는 집적회로를 사용하여 자체에 기억장치와 처리장치가 내장되어 있다. 따라서 기억용량이 크고 정보기록이 가능하여 개인의 신상, 금융거래, 신용 등에 관한 다양한 정보를 동시에 수록할 수 있다. 그러나 IC카드를 전자화폐의 보관처리로서 사용하기 위해서는 IC카드 및 IC카드 판독기 등을 보급시켜야 하기 때문에 막대한 투자가 필요하다. 따라서 IC카드형 전자화폐는 이러한 투자비용을 누가 부담하느냐가 관건인 것이다. 즉 소비자, 상점, 전자화폐 발행자중 부담자가 누구냐는 것이다. 현재 전자화폐는 발행자의 부담으로 보급되어 한계점에 왔다. 주로 유럽과 일본 등에서 활용되고 있다.

한편 정보네트워크가 급속히 발달하고 암호기술이 고도화되면서 인터넷을 이용하여 세계 각지로부터 필요한 물품을 주문할 수 있게 되었다. 대

〈표 1〉 전자화폐 분류

구분	네트워크형(on-line)	IC카드형(off-line)
사례	E-Cash, CyberCash, NetCash	개방형 : Mondex (양도 허용) 폐쇄형 : ViaCash (양도 불가)

금결제에는 신용카드, 수표 등과 같이 은행을 경유해야 하는 불편 없이 PC에 내장된 단말기를 통해 직접 결제가 이루어질 수 있도록 하는 새로운 수단이 필요하게 되었다. 이에 따라 인터넷상의 가상은행 계좌나 인터넷과 연결된 고객의 PC 또는 발행사의 메인 컴퓨터에 화폐가치정보를 저장시키는 전자화폐가 개발되고 있다. 미국을 중심으로 사용되고 있는 E-Cash와 CyberCash 그리고 국내의 Angelplus등이 대표적이다.

네트워크형 전자화폐의 장점은 전자화폐용 소프트웨어만을 구비하면 되기 때문에 보급을 위해 막대한 신규투자를 필요로 하지 않는다는 점이다. 그러나 결제정보가 인터넷과 같은 개방된 통신망을 통해 전달되기 때문에 종래의 PC통신보다는 더욱 엄중한 안전성이 요구되고 있다. 따라서 안전성 확보를 위한 암호기술이 현재 중요한 과제로 대두되고 있다.

양도 여부에 따라 분류하기도 한다. 양도 가능한 전자화폐를 개방형 전자화폐라고 한다. 그러나 현재 도입되고 있는 전자화폐 중에서 개인 간 자금이체가 가능한 것은 극히 일부분에 불과하다. Mondex는 개방형 화폐이다. 그러나 덴마크의 단몬트, 미국의 SVC(Stored Value Card), 그리고 과거 우리 나라 동남은행의 전자지갑 등은 개인 간 자금이체가 불가능하다. 이러한 전자화폐를 폐쇄형 전자화폐라고 한다〈표 1〉.

3. 전자화폐 관련 주요 용어들

1) Double spending

전자화폐와 현행 화폐 제도중의 하나인 지폐 사이에 일어 날 수 있는 부정행위를 살펴보면 지폐에 있어서는 위조가 있으며 전자화폐에 있어서는 이중사용(Double spending)이 있다. 지폐에서의 위조는 은행 또는 정당한 발행기관의 허가 없이 돈을 만들거나 기존의 돈으로부터 새로운 돈을 만드는 행위를 말한다. 한편, 전자화폐는 전자정보로 이루어져 쉽게 복사가 가능한 점을 이용하여 1회 사용 후 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 정보로부터 컴퓨터가 동일한 전자화폐를 조사하여 이중사용자의 계좌번호와 사용자의 신분을 알아내는 방식을 주로 위하고 있다. On-Line인 경우는 이중사용의 방지가 용이하며 즉시 거래를 중시시킬 수 있으나 Off-Line인 경우는 전자화폐 사용전 거래 중지가 곤란하며 추후 부정사용자 Blacklist에 공개하거나 신용거래를 중지하는 방안으로 취하고 있다.

2) Privacy/Untraceability

전자화폐에 있어서 안전성이나 효율성 외에 가장 중요한 관심사가 되고 있는 것이 Privacy다. 특히 미국보다는 유럽을 중심으로 활발히 거론되고 있는 것으로 네덜란드의 암호학적인 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 가져왔는가에 대한 개인의 비밀정보를 다른 사람이 알 수 없게 하는 것이다.

전자화폐에서 고려될 수 있는 Privacy는 크게 두 종류로 지불자외의 다른 모든 사람들이 결탁한다 하더라도, 지불자가 구매한 정보에 대해서 알 수 없는 지불자 추적 불가능(Payer untraceability)과 수취인 외의 다른 모든 사람들이 결

탁한다 하더라도, 수취인이 어디로부터 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 결제단계와 지불단계가 연결될 수 없음을 의미한다. 대부분의 전자화폐에서는 지불인 추적 불가능이 요구되나 수취인 추적 불가능은 요구되지 않는다. 수취인 추적 가능은 자신이 고소되었거나 익명의 금전 강탈을 막기 위해 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 관연 전자화폐에 이러한 기능을 제공하여야 할지의 여부는 많은 논란의 여기가 있다.

3) Transferable/Non-transferable

Non-transferable 전자화폐는 1회 사용 후에는 바로 상점과 은행간의 결제단계가 이루어져야 하는 것을 말하며, 이에 반해 Transferable 전자화폐는 발행단계이후의 지불단계가 여러번 이루어지는 즉, 지불자와 지불자 간이나 지불자와 상점 간의 단계가 복수회 이루어진 후에 결제단계로 향하는 것을 말한다[3]. 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[3].

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. 다시 말해서 지불단계와 결제단계가 거의 동시에 행하여지는 것을 말하며 이중사용을 지불단계에서 사전에 방지할 수가 있으나 많은 통신량이 한 곳으로 집중화되는 문제점과 거래에 따른 통신비용이 증가하게 되는 문제점이 생기게 된다.

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

미국을 중심으로 한 전자화폐는 On-Line형태를 이루고 있는 반면 유럽을 중심으로 한 전자화폐는 IC카드의 발달 및 보급으로 인하여 Off-Line 형태로 많은 검토되어지고 있다.

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

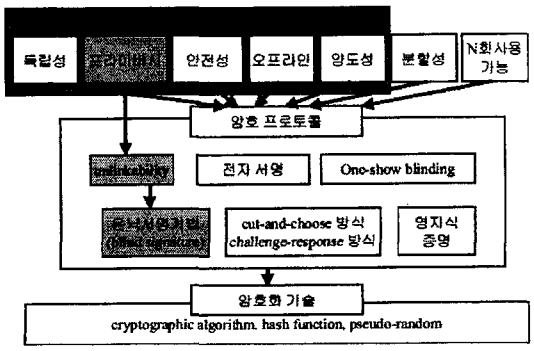
Ⅲ. 전자화폐의 위협요소와 요구조건

1. 위협요소

- 위조(Forgery) : 은행을 제외한 참가자가 발행 프로토콜에 참가한 후에 발행한 전자화폐의 금액을 액면가에 초과하는 전자화폐로 바꾸어 그것이 은행에 의해 유효하게 받아들여지게 하는 공격
- 이중사용(Double spending) : 사용자가 발급받은 전자화폐를 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
- 은행 강탈(Bank robbery) : 공격자들의 집단이 은행에게 추후 사용할 수 있는 돈을 얻도록 프로토콜에 참여하기를 강요하는 공격

2. 전자화폐의 요구조건

이러한 사항들을 기본적으로 고려한 전자화폐의 요구 사항, 즉 전자화폐 시스템에서 제공해야 할 사항은 〈그림 2〉와 같이 요약할 수 있다.



〈그림 2〉 전자화폐의 요구조건

- 안전성 : 전자화폐의 복사, 위조 등에 의한 이용 불가
- 프라이버시 : 은행 또는 상점에 의한 구매 관련 내용의 추적이 불가능해야 한다.
- 이중사용(Double spending) 금지 : 전자화폐의 이중 사용이 방지되어야 한다.
- 양도성 : 화폐와 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 수 도 있다.

Ⅳ. 전자화폐 암호 프로토콜

1. Chaum, Fiat, Naor의 기법

오프라인 지불형태로 익명성을 보장한 전자화폐는 Chaum, Fiat, Naor에 의해 처음으로 소개되었다[2]. 그들은 기종에 제시되었던 전자화폐 프로토콜에서 전자화폐 시스템의 참가자들 각각은 다른 제3자들에 의해서 사기를 당하기 쉬우며, 특히 카드의 소유자인 고객은 이러한 사기로부터 보호될 수 없다는 문제점을 지적하면서 근본적으로는 전자화폐에 대한 일련 번호가 화폐에 대한 추적을 가능하게 만들지만, 프라이버시 측면에서 신용카드에 대한 장점을 충분히 반영할 수 있는 추적 불가능한 전자화폐를 제시하였다. 이에 대한 안전성은 몇 가지 가정을 바탕으로 하고 있으며 제시된 기법이 실용적이지 못하다는 점이 단점으로 지적되기는 하지만 전자화폐에 대한 연구에 새로운 방향을 제시해 주었으며, 이를 토대로 전자화폐에 대한 연구가 매우 활발히 진행되어 왔다는 점에서 전자화폐 연구에 초석이

되었다고 볼 수 있다.

1) 발행 단계

고객이 은행으로부터 전자화폐를 얻을 때 RSA 디지털 서명 기법을 사용하여 추적 불가능한 전자화폐를 구체화시켰다. 고객은 화폐를 얻기 위해 자신의 신원정보가 쓰여진 은닉된 후보들을 생성하여 은행에 제시하는데 영지식 증명 기법을 이용하여 이것을 은행에게 확인시킨다. 그러면 은행은 은닉 서명을 이용하여 서명한 화폐를 고객에게 전달하게 되고, 고객은 자신만이 알고있는 정보를 이용하여 지불 가능한 화폐를 추출해 낸다.

2) 지불 단계

발행한 화폐를 상점에 지불할 경우에 상점은 지불된 화폐가 올바른 정보로 구성되었고 은행의 서명을 받은 것임을 확인한 다음 지불된 화폐에 대한 금액을 은행에게 입금할 것을 요구하게 된다. 여기서 누구나 화폐의 올바른 구성과 은행으로부터 서명을 받은 화폐임을 확인할 수 있지만, 은행이 특정한 화폐를 그 화폐 수령인의 계좌와 바로 연결시킬 수 없다는 점이 고객에 대한 추적을 불가능하게 해준다. 또한 오프라인으로 지불 단계가 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

먼저 은행은 고객이 제시한 화폐의 구성을 확인할 수 있도록 충분한 길이의 항(term)을 위한 안전성 변수 k를 정하고, 고객은 $2k$개의 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 알고 있는 보를 제거하는 것으로 전자화폐를 추출해낸다.

2. Brands 방식

Cut-and-Choose 방식의 비효율적인 발행단계를 보다 개선한 Challenge Response 방식을 처음으로 고려한 전자화폐 방식이다. 현재 가장 많은 각광을 받고 있는 방식으로 인터넷상에서도 활용 가능한 방식과 내용은 닉서명을 사용하지 않는 방식들로 발전하고 있다[4].

1) 발행 단계

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

$$\begin{aligned} a &= x_1+x_2 \mod p-1 \\ a+\mu &= y_1+y_2 \mod p-1 \end{aligned} \quad (1)$$

$$G=H(g_1^{x_1}g_2^{y_1},\ g_1^{x_2}g_2^{y_2}) \quad (2)$$

단계 2) Alice는 은행에

$$Z=r^e\times G \mod n \quad (3)$$

을 제출한다.

단계 3) Alice는 영지식 증명으로 (I_A, Z)가 식 (1), (2), (3)을 만족하고 있음을 은행에 증명한다.

단계 4) 은행은 $Z^d=r\times G^d \mod n$ 계산하여 Alice에게 양도한다.

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

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

2) 지불단계

단계 1) Alice는 상점에 전자화폐 C를 제시한다.

단계 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.

단계 3) 상점은 Alice에게 난수 a를 보낸다.

단계 4) Alice는 상점에 v, w를 보낸다.

$$v=x_1+ax_2 \mod p-1$$
$$w=y_1+ay_2 \mod p-1$$

단계 5) 상점은 다음 식이 성립하는지를 검사한 후 맞으면 요구하는 물건을 Alice에게 제공한다.

$$g_1^{v}g_2^{w} \stackrel{?}{=} g_1^{x_1}g_2^{y_1}(g_1^{x_2}g_2^{y_2})^{a} \mod p$$

3) 결제단계

단계 1) 상점은 은행에 Alice와 주고받은 모든 통신내용, 를 은 C, a, v, w 행에 제시한다.

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

V. 결 론

전자화폐에 대한 관심이 고조되고 있는 시점에서 암호학적인 측면에서의 안전대책을 고려한 전자화폐를 살펴보았다. 산업혁명 이후 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 연구를 수행하고 있는 사항이다. 앞으로 여기서 제시한 기분 요구 조건을 포함하여 선별적인 추가 요구사항을 만족하는 전자화폐 프로토콜에 대한 연구가 계속적으로 이루어져야 할 것이다.

부 록

1. SEED 암호화 방식

SEED 암호화 방식은 대칭적 알고리즘으로서 정보의 암호화와 해독에 128bits의 동일한 키를 사용한다. 정보를 교환하는 양측이 암호화에 사용된 키를 상대방에게 건네주는 방식이다. 그런데 거래의 상대방이 불특정 다수일 경우에는 방대한 고객의 수만큼 키를 만들어 나누어주어야 하고 이를 각각의 고객과 연관하여 유지하여야 하는데 이는 실제적으로 매우 비효율적이다. 또한 공개키 방식을 이용한 암호화 문장은 상당히 쉽게 해독될 수 있음이 입증되었으며, 이에 따라 공개키 방식이 제안되었다.

2. RSA 암호화 방식

RSA 암호화 방식은 제안자의 이름을 따라서 RSA(Rivest, Shamir, Adoleman) 이름에 붙여졌다. RSA 알고리즘에서는 개인이 보관하는 개인키와 공개해 놓은 공개키의 두 개의 키를 이용하며, 공개키로 암호화한 문장은 공개키에 대응하는 개인키를 이용하여 해독할 수 있으며, 반대로 개인키로 암호화할 경우, 대응되는 공개키를 이용하여 야만 원문을 재생해낼 수 있다.

3. 전자 서명과 디지털 증명

전송하고자하는 메시지를 암호화했다고 해서 메시지의 무결성이 보장되는 것은 아니다. 즉 전자상거래를 이용한 거래에서는 모든 정보가 전자문서의 흐름에 의해 처리되기 때문에 거래 당사자들이 거래에 참여했다는 것을 기술적으로, 또는 법적으로 보장할 수 있어야 한다. 전자서명은 메시지가 전달 또는 수정되지 않았음을 보장하는 프로토콜로서 메시지 인증과 암호화기술로 구성된다.

전자 서명은 구매자가 거래 내역을 자신의 개인키로 암호화하여 판매자에게 전송하며, 판매자는 구매자의 공개키로 메시지를 해독하여 정상적인 메시지일 경우에만 거래를 진행한다. 이 때 구매자의 공개키는 공개된 정보이므로 누구나 이 메시지를 해독할 수 있다. 이를 막기 위해 구매자가 전송하기 전 자신의 개인키로 암호화한 메시지를 다시 판매자의 공개키로 암호화하여 지정된 상대방만이 최종적으로 자신의 메시지를 해독할 수 있도록 함과 동시에 거래의 주체가 누구인지를 입증하는 기능을 동시에 수행하게 된다.

네트워크상에서 거래를 하는 각각의 개체가 실

제 누구인지를 증명하는 것은 쉽지 않다. 이를 정확히 증명해주기 위해 디지털 증명을 이용한다. 디지털 증명서를 이용하면 구매자와 판매자의 신분을 네트워크상에서 확인할 수 있게 되므로 전자상거래의 신용을 높일 수 있다.

대칭적, 비대칭적 암호화 방법을 네트워크상의 socket 계층에 적용한 보안 방법으로 Netscape 등의 WWW 검색기에서 사용하고 있는 SSL (Secured Socket Layer)가 있다.

4. SET(Secured Electronic Transaction)

1996년 2월 전 세계적으로 가장 큰 신용카드 회사들인 VISA International과 Master 카드사는 인터넷상에서 신용카드를 이용하여 대금의 지불함에 있어 개인의 정보와 재산을 보호해줄 수 있는 안전한 방법을 찾기 위해 공동으로 연구를 시작하였고, 97년 5월 SET 1.0을 발표하였다. SET 프로토콜은 대칭적 암호화 방법인 DES와 비대칭적 암호화 방식인 RSA 및 디지털 봉투를 이용하여 암호화에 걸리는 시간을 줄이고 해독의 가능성을 더욱 낮추었다. SET 지불 정보 및 주문 정보에 대한 보안, 전송되는 데이터에 대한 기밀성 보장, 카드 및 카드 사용자에 대한 인증, 판매자에 대한 인증 및 각 구성 요소들 간의 상호 운용성을 보장해주는 거래 프로토콜이다.

SET을 이용한 데이터의 암호화 및 전송 방식은 다음과 같다.

1. 구매자는 전송메시지를 자신의 개인 키를 이용하여 RSA 방식으로 암호화한다.
2. 원문과 1의 결과를 구매자의 인증서와 함께 DES 방식으로 암호화한다.
3. 2에서 사용된 DES 키를 판매자의 공개키를 이용 RSA 방식으로 암호화한다.
4. 2의 결과(메시지 내용)와 3의 결과(봉투)를 판매자에게 보낸다.

이 메시지를 수신한 판매자는

1. 수신자의 비밀키를 이용 RSA 방식으로 봉투를 해독한다.
2. 이 때 봉투에는 송신자의 DES 키가 들어있다.
3. 암호화된 메시지를 2의 DES 키를 이용하여 원문 및 송신자의 디지털 서명과 송신자의 인증서를 얻는다.
4. 3에서 얻은 디지털 서명을 송신자의 공개키로 복호화하면 원문을 얻을 수 있다.

이 방법은 DES 방법의 간편성과 빠른 처리 속도를 이용하여 본문을 암호화한 후, 여기에 사용된 키와 관련 정보를 속도는 느리지만 보안 성능이 보다 뛰어난 RSA 방법으로 암호화하여 마치 봉투처럼 만들어서 연산의 속도와 암호화의 성능 등 두 가지 측면에서의 장점을 수용하는 방법이다.

참 고 문 헌

〔1〕 D. Chaum, "Blind Signature Systems." Advances in Cryptology-Proc. of CRYPTO'83 Springer-Verlag, pp.153, 1983.

〔2〕 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.

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

〔4〕 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

저 자 소 개

崔 恩 華

2002년 2월 공주대학교 응용수학과 졸업, 2002년 3월 공주대학교 일반대학원 수학과, 〈주관심 분야 : 암호 알고리즘〉

徐 彰 浩

1990년 고려대학교 수학과 졸업 (학사), 1992년 고려대학교 일반대학원 수학과 (이학석사), 1996년 고려대학교 일반대학원 수학과 (이학박사), 1996년~1997년 : 국방과학연구소 선임연구원, 1997년~2000년 : 한국전자통신연구원 선임연구원, 팀장, 2000년~현재 : 공주대학교 응용수학과 조교수, 〈주관심 분야 : 암호 알고리즘, PKI, 시스템 보안 등〉

金 錫 佑

1979년 한국항공대학 통신정보공학과 (학사), 1989년 뉴저지 공과대학 전자계산학과 (공학석사), 1995년 아주대학교 컴퓨터공학과 정보통신전공 (공학박사), 1980년~1997년 : 한국전자통신연구원 책임연구원 실장, 1997년~현재 : 한세대학교 정보통신학과 교수/전산소장/정보보호연구소장/군포창육보육센타 소장, 〈주관심 분야 : 시스템 보안, 네트워크 보안, 시스템 평가 등〉