공정한 DSS 은닉 서명 기법을 기반으로 한 전자화폐 시스템

장석철* • 이임영*

A Electronic Cash System based on Fair Blind DSS Signature Scheme

Seok-Cheol Jang, Im-yeong Lee

요 약

전자화폐 시스템은 인출(withdrawal), 지불(payment) 그리고 예치(deposit)의 기본적인 과정을 수행하는데, 이러한 단계에서 사용자의 사생활(privacy)을 보호하기 위해 사용자와 사용자의 구입 내용 및 지불 내용을 연계시키지 않고 인출 단계와 지불 단계가 연결되지 않도록 기본적으로 익명성을 제공하고 있다. 하지만 이러한 완전한 익명성을 제공하므로 인해 돈 세탁, 약탈, 불법 거래와 같은 불법적인 범죄 행위들에 이용 될 수 있으며 이 때 이와 같은 범죄행위를 한 사용자와 그 돈에 대한 행방을 찾을 수가 없다. 따라서 이를 방지하기 위해 일정한 조건 아래에서 익명성을 제어하기 위한 연구들이 많이 진행되어 왔다. 본 논문에서는 DSS에 기반한 새로운 공정한 은닉 서명 방식을 제안하고 이를 전자화폐 시스템에 적용시킨다.

Key words : Electronic Cash, DSS, Anonymity Control, Blind Signature, Fair Blind Signature

1. 서론

동전과 지폐로 대별되던 화폐에 신용카드가 나오면서 화폐의 혁명이 시작되었다. 이른바 플라스틱 머니로 불리며 급속한 확산속도를 보이던 신용카드는 국민 1인당 1장 이상을 소유할 정도로 대중화된 화폐로 자리잡고 있다. 최근에는 정보통신 및 컴퓨터 기술의 발달로 신용카드, 전자 자금이체, 인터넷 뱅킹 등 현금대체 결제수단이 보편화되고 있다. 하지만 이러한 현금 대체 결제 수단을 인터넷에서 사용할 경우 신용카드 번호 누출 등으로 개인 사생활이 노출될 수 있고 범죄에 이용될 수도 있다. 또한 실물화폐가 갖는 동일한 재질의 입수가 곤란한 점, 투명성이나 고도의 인쇄, 제조기술이 필요한 점 등 이러한 이점을 가지고 있는 실물화폐는 정보화사회에 대응하기는 곤란하다. 왜냐하면 실물화폐는 종이와 금속이라는 물리 매체에 의해 실현되기 때문에 실제 사용이 그 물리적 이동을 전제로 하고 정보로써 취급하기 어렵기 때문이다. 따라서 인터넷과 같은 네트워크 상에서 지불수단으로써 전자화폐의 필요성이 증가되고 있다.

이제는 제2의 화폐혁명인 전자화폐 시대가 열리고 있다. 보이지 않는 돈을 가상의 공간에서 자유롭게 사용할 수 있는 화폐가 전자화폐이다. 특히 눈부시게 발전하고 있는 디지털 기술, 인터넷의 급부상과 컴퓨터의 급속한 보급으로 인한 전자상거래의 발전은 기존 시장의 개념을 네트워크 상에서의 인터넷 쇼핑몰 개념으로 바꾸게 했다. 원시시대의 물물교환 시장에서부터 현대의 대형 쇼핑몰 거래까지 모든 상업적 거래는 상인과 고객이 직접 대면해서 거래가 이루어졌으나 컴퓨터를 통해 이루어지는

* 순천향대학교 정보기술공학부 정보보호연구실
(scjang@cse.sch.ac.kr, imylee@sch.ac.kr)

본 연구는 정보통신부의 대학 S/W 연구센터 지원 사업에 의해 수행된 것임.

전자상거래에서 고객은 물건을 직접 만져보지 못하고 그 물건을 파는 상인의 얼굴도 모른 채 컴퓨터를 통해 웹브라우저 앞에서 마우스를 이용해서 자신이 원하는 물건을 검색하고 선택해서 물건을 구매한다.

현재 전자상거래시장은 급속히 성장하고 있다. 국내 인터넷 및 전자상거래 현황에 대한 IDC(International Data Corporation)의 1999년 11월 조사결과를 살펴보면, 한달 동안에 한번 이상 인터넷을 이용하는 국내 인터넷 이용자수는 지난 1998년 175만 명, 1999년에는 331만 명, 향후 2004년에는 1,021만 명에 이를 것으로 IDC는 전망하고 있다. 또한 인터넷 이용자 중에 최근 3개월 동안 인터넷을 통해 물건을 구입한 경험이 있는 전자상거래 이용자수는 지난 1998년 국내 인터넷 이용자수의 9.7%에 해당하는 17만 명에서, 1999년 인터넷 이용자수의 17.5%인 58만 명, 향후 2003년에는 인터넷 이용자수의 47.6%인 486만 명에 이를 것으로 IDC는 전망하고 있다. 인터넷 이용자수와 전자상거래 이용자수에 대한 연평균 성장률은 각각 25.3%와 52.9%로 미국이나 일본의 성장률 보다 큰 것으로 나타났다. 국내 전자상거래 규모는 지난 1998년 5,650만 달러에서, 1999년에는 2억 4,400만 달러, 향후 2004년에는 약 181억 달러로 연평균 성장률 136.6%의 급성장을 이룰 것으로 IDC는 전망하고 있는데, 이는 미국의 80.2%와 일본의 87%에 비해 큰 성장률을 전망하고 있는 것이다. 이처럼 급성장하고 있는 전자상거래에서 많은 부분이 인터넷 쇼핑몰을 이용하여 물건을 구매하는 것이다. 인터넷 쇼핑몰 이용의 가장 큰 이유는 시간절약과 편리성 때문이다. 이렇게 인터넷 쇼핑몰의 사용이 급증함에 따라 지불수단도 변하게 된다. 그래서 요즘 화제가 되고 있는 전자화폐, IC 카드도 이러한 상거래의 변화에 따라 등장하게 되었다. 새로운 전자상거래의 등장으로 새로운 지불방식을 요구하는 환경이 조성되고 있다. 특히 최근에 전자화폐는 전자상거래 등 정보시대에 필수적인 화폐로 소액거래에 편리한 장점을 지니고 있다.

일반적으로 전자화폐 프로토콜은 사용자, 상점 그리고 은행의 세 개체간의 거래에 의해 이루어지며 인출단계, 지불단계, 예치단계의 기본적인 프로토콜을 가지고 있다. 인출단계는 사용자와 은행간에 이루어지며 사용자가 자신의 식별 정보를 은행에 제공하면 은행에서는 이를 바탕으로 전자화폐를 발행하여 사용자에게 전송한다. 이때 사용자와 은행간에는 은닉서명(Blind Signature)이라는 특수 서명 방식을 이용하여 사용자의 식별 정보를 은닉시키게 되며 은행은 자신의 서명을 통해 정당한 화폐라는 것을 확인할 수 있도록 한다[1]. 지불단계는 사용자와 상점간에 이루어지며 은행으로부터 발행된 전자화폐를 상점에 제공한다. 상점에서는 사용자로부터 받은 전자화폐가 은행으로부터 받은 정당한 전자화폐인지를 확인하고 유효한 전자화폐임이 밝혀지면 해당 전자화폐를 받아들인다. 예치단계에서 상점은 사용자로부터 받은 전자화폐를 예치하고 은행은 해당 전자화폐의 이중사용여부를 자신의 DB를 통해 검사하게 된다. 이와 같이 전자화폐 시스템은 인출(withdrawal), 지불(payment) 그리고 예치(deposit)의 기본적인 과정을 수행하는데, 이러한 단계에서 사용자의 사생활(privacy)을 보호하기 위해 사용자와 사용자의 구입 내용 및 지불 내용을 연계시키지 않고 인출 단계와 지불 단계가 연결되지 않도록 기본적으로 익명성을 제공하고 있다. 하지만 이러한 완전한 익명성을 제공하므로 인해 돈세탁, 약탈과 불법 거래와 같은 불법적인 범죄 행위들에 이용 될 수 있으며 이 때 이와 같은 범죄행위를 한 사용자와 그 돈에 대한 행방을 찾을 수가 없다. 따라서 이를 방지하기 위해 일정한 조건 아래에서 익명성을 제어하기 위한 연구들이 많이 진행되어 왔다. 본 논문에서는 DSS에 기반한 새로운 공정한 은닉 서명 방식을 제안하고 이를 전자화폐 시스템에 적용시킨다.

2. 전자화폐에 있어서 은닉 서명

D.Chaum이 전자화폐를 사용하는데 있어서 사용자의 프라이버시를 보호하기 위해 은닉 서명이라는 새로운 서명 방법을 제시한 이후로 전자화폐에 있어서 기본 요구 사항인 '정당한 사용자에 대한 불추적성', 즉 '사용자에 대한 프라이버시 보호'를 만족시키기 위해 여러 가지 형태의 은닉 서명 방식이 제안되어 왔다. 전자화폐에서 사용되는 은닉 서명 방식은 크게 RSA 방식에 근거한 기법[2]과 이산대수 문제를 이용하는 ElGamal 방식에 근거한 기법[3]으로 나누어 볼 수 있다.

RSA 방식에 근거한 기법을 이용하는 전자화폐 프로토콜은 D.Chaum[4], T.Okamoto-K.Ohta[5], T.Okamoto[6], M.Jakobsson-M.Yung[7] 등에 의해 제안이 되었다. RSA 방식을 이용하는 은닉 서명 방식들은 송신자가 서명을 받기 위한 메시지가 아닌 다른 변형된 메시지를 서명자에게 보내더라도 이를 서명자가 알 수가 없다는 문제점을 해결하기 위해 cut-and-choose 방식과 T.Okamoto[8]가 제안한 이산대수 문제에 기반한 새로운 Bit Commitment를 사용하는 zero-knowledge 방법, 그리고 Range Bounded Commitment(RBC)의 개념을 형식화하고 이산대수 가정에 근거한 방법을 사용하고 있다.

이산대수 문제를 이용하는 ElGamal 방식에 근거한 기법은 ElGamal이 이산대수 문제를 이용한 최초의 서명 방식이다. 1992년 Chaum-Pedersen 방식[10] 이외에 representation problem을 이용하는 제한적인 은닉 서명이라는 새로운 primitive를 제안하고 있는 S.Brands가 제안한 방식[11]과 기존의 DSA서명 방식을 변형한 방식, 그리고 Nyberg-Ruppel 서명 방식에 기반한 방식[12] 등이 있다. 이밖에 대부분의 많은 전자화폐 프로토콜들은 이러한 ElGamal 형태의 서명 방식을 이용한 은닉 서명 방식을 사용하고 있다.

3. 전자화폐에 있어서 공정성

전자화폐에 있어서 익명성은 개인의 사생활 보호라는 긍정적인 측면 이외에 불법적으로 사용된 돈의 정보를 알지 못하게 함으로서 완전한 돈 세탁(money laundering)과 약탈(black- mailing)을 가능하게 한다[13][14][15][16]. 또한 전자화폐가 강도에 의해 약탈되더라도 그 익명성은 유지할 뿐만 아니라 강도는 이러한 전자화폐를 아무런 제재 없이 사용할 수가 있게 된다. 이와 같이 익명성이 보장되는 전자화폐는 범죄자들에 의해 이용이 가능하며

각종 범죄 활동의 도구 될 수가 있다. 또한, 돈 세탁과 약탈이 가능한 전자화폐는 비록 작은 금액에서 사용이 되더라도 그 거래량이 엄청나기 때문에 전체 통화 시스템에 큰 위험 요소를 제공할 수 있다. 따라서 다양한 단계로 제공될 수 있는 전자화폐의 익명성은 그 강도가 증가할수록 비례하여 잠재적인 위험성도 증가하게 된다. 그래서 완전한 익명성을 제공함으로써 일어날 수 있는 문제점을 분류한다.

- 위조(Counterfeiting) : 은행을 제외한 나머지 참여 개체들에게 금액 한도를 넘어 지불을 할 수 있을 때, 은행에 의해 유효한 화폐로 받아들여질 수 있다. 이러한 물리적인 화폐의 위조와 유사한 전자화폐 상에서의 위조는 두 가지 방법이 존재한다. 첫 번째로 토큰 위조(Token forgery)로서 은행에서 인출하지 않고서 유효한 전자화폐를 생성하는 경우이고, 두 번째로서 다중 사용(Multiple spending)으로서 해당 전자화폐가 사용되기 전처럼 사용 후에도 유효한 전자화폐로 보일 수 있다.

- 돈 세탁(Money laundering) : 전자화폐는 기본적으로 순환 구조를 가지고 있기 때문에 돈 세탁을 좀 더 어렵게 하고 있으나, 반면에 많은 작은 구매들이 발생할 수 있으며 이를 통해 자금이 은닉된 상태로 교환될 수 있다.

- 약탈, 공갈, 갈취(Blackmail) : 공격자는 사용자가 그의 계좌로부터 자금을 인출하도록 하고, 그 자금을 공격자의 계좌로 예치시키거나 또는 추적 당하는 것 없이 공격자가 사용할 수 있다.

- 불법적 구매(Illegal purchases) : 마약 구매, 불법 무기 구매 등과 같은 불법적인 구매 행위를 하는 사람의 식별자를 동전 식별 정보와 연계시킬 수 없기 때문에 사용자를 밝혀낼 수가 없다.

- 초과사용(Overspending) : 금액을 초과 사용하더라도 초과 사용한 사용자의 식별값과 계좌 번호를 연계시킬 수 없기 때문에 금액의 초과 사용이 가능해 질 수 있다.

- 모방, 흉내(Impersonation) : 공격자가 어떤 다른 사용자의 협력 없이 그 사용자의 자금에 접근하여 해당 금액을 획득할 수 있다.

- 은행 강도(Bank robbery) : 공격자는 은행이 인출 과정에서 이루어지는 은닉 프로토콜에 관여하게끔 함으로써 불법적으로 발행된 이러한 형태의 동전을 추적하는 것은 불가능하다.

이러한 면은 전자상거래의 발전을 저해할 수 있다. 이에 대한 해결 방안으로 공정성 개념이 등장하게 되었다.

공정성(Fairness)이라는 조건은 오늘날 전자화폐 시스템을 설계하는데 있어서 매우 중요한 조건으로 등장하고 있다. 2절에서 언급하였듯이 익명성이 제공된 전자화폐는 그 장점에도 불구하고 많은 부작용을 불러일으키고 있으며 이에 대한 문제 해결 없이는 화폐를 발행하고 운용해야하는 정부/금융기관에서는 도입하기가 어렵다. 따라서 등장하게 된 요구 조건이 익명성 제어(Anonymity Control)이다. 그러나 이 요구조건 역시 남용하였을 경우 개인의 사생활 침해와 연관될 수 있기 때문에 사용자 입장에서 볼 때 받아들이기 쉽지 않은 문제이다. 여기에서 사용자 측면의 익명성과 관계 기관의 익명성 제어 부분을 절충한 방법이 필요한데, 이로부터 공정성이라는 개념[14],[18],[19]이 돌출 된다.

전자화폐는 크게 사용자측과 화폐 발행자 측으로 구분해 볼 수 있다. 일반 화폐 사용자와 상점, 기업 등 화폐를 이용하는 모든 개체들을 사용자측으로 볼 수 있고 이를 발행, 운용, 감독하는 개체를 묶어서 화폐 발행자 측으로 구분할 수 있다. 이러한 사용자측과 화폐 발행자 측은 익명성 문제에 대해 서로 상반되는 입장을 가지고 있다. 즉, 사용자 측에서는 되도록 완전한 익명성을 가지기를 원할 것이고 화폐 발행자 측에서는 익명성이 제공되지 않는 시스템을 원할 것이다. 이에 두 참여 개체들 간에 익명성 제공과 익명성 제어를 위한 합의점을 찾아야 할 것이며 이를 만족시키는 시스템이 공정한 전자화폐 시스템[14],[15],[17],[18],[19]이 될 것이다.

다시 말해 공정성이란 사용자의 프라이버시를 만족시키면서 동시에 적법한 과정을 통해 익명성을 제어할 수 있는 기능을 말한다.

익명성 제어 기능은 사용자의 계좌 정보나 사용자 식별 정보를 노출시키기 때문에 화폐 발행 기관이나 또는 추적 기관의 임의 제어를 방지하고 사용자 프라이버시를 보호하기 위해 다음과 같은 사항[14],[15],[18],[17]을 고려해야 한다.

- 합법적 사용자들에 대한 익명성(Anonymity for legitimate users) : 합법적인 사용자들의 전자화폐는 익명성을 유지해야 한다. 즉 사용자들이 사용한 동전들과 사용자는 서로 연결이 되어서는 안된다.
- 정당성(Revocation upon warrant presentation) : 익명성은 취소가 가능하다. 그러나 익명성 취소는 판사나 또는 기타 보편적으로 인정될 수 있는 중립적인 기관의 명령에 의해서만 가능하여야 한다.
- 제어능력의 제한(Limitation of control ability) : 익명성을 제어하는 기관은 추적 기능 외에 어떠한 능력도 가지고 있지 않아야 한다. 즉, 그러한 능력을 이용하여 위조나 사용자 모방 등과 같은 행위가 불가능하여야 한다.
- 조작 불가능성(Framing-freeness) : 화폐 발행 기관은 trustee나 또는 다른 기관들과 결탁하더라도 사용자를 모방하여서는 안된다. 이를 통해 사용자는 조작된 화폐로 인해 고발될 수 없다.
- 선택성(Selectivity) : 익명성의 취소는 선택적으로 이루어져야 하며 나머지 화폐들에 대해서는 완전한 익명성을 유지해야 한다.
- 환불, 변제, 반환성(Refundability) : 화폐 발행 기관의 실수나 고의로 인한 잘못된 화폐의 발행은 법원과 같은 중립적인 기관에 의해 그 주체가 밝혀질 수 있어야 하며 동시에 금액을 환불 할 수 있어야 한다.
- 화폐 취소성(Revocability of funds) : 사용자의 불법적인 구매나 또는 세금 포탈로 인해 법원의 명령이 있을 경우 인출된 금액을 취소하고 해당 금액을 압류할 수 있어야 한다.
- 속임 방지(Blindfold-freeness) : 어떤 특정한 동전이 은닉되었다는 것을 은행이 알지 못한 채 은닉된 동전을 얻는 것은 불가능해야 한다.
- 효율성(Efficiency) : 익명성 제어 기관이 전자화폐 시스템에 참여하면서 다른 개체들에게 부담을 주어서는 안된다. 따라서 이러한 요구조건에 맞게 새로운 전자화폐 시스템인 공정한 전자화폐 시스템(Fair payment systems)이 등장하게 되었다.

공정한 전자화폐 시스템이라고도 불리는 익명성 제어 가능한 전자화폐 시스템에 대한 개념은 Solms-Naccache[20]가 처음으로 소개하였으며 Brickell-Gemmell-Kravitz[21]에 의해서 그 방안이 제안이 되었다. 이 방안에서는 전자화폐의 소유자

를 식별하는 소유자 추적(Owner Tracing) 개념을 소개하고 있다. 또한 Stadler-Piveteau-Camenisch [22]는 전자화폐의 소유자 추적과 화폐 추적(Cash Tracing)의 두 가지 익명성 취소 모델에 대해 소개하고 있다.

먼저 소유자 추적(Owner Tracing)에 있어서 익명성 제어 파라메타는 상품 대금 지불이 이루어지고 난 후에 예치된 화폐 정보로부터 추적 기관이 동전의 소유자를 식별해 낼 수 있도록 해준다. 이 방식을 역추적(Backward Traceability) 방식이라고도 하며, 예치 기록이 주어졌을 때 인출 기록을 식별한다. 이를 통해, 추적기관은 누구로부터 화폐를 받았는지 알아 낼 수 있다.

이 방식은 화폐에 직접적으로 관련된 것들에 기반하기 보다는 사용자들이 구입한 것들, 즉 시간, 구입량, 구입 상점 등에 기반하여 소유자를 추적하기 때문에 여러 가지 사기 형태에는 유용하지 못하다.

이와 같은 형태의 추적 메커니즘을 위해 인출 번호는 공통적으로 신뢰되는 기관들의 공개키로 암호화되며 동전 자체와 합쳐진다. 이러한 암호화된 인출 정보는 지불 프로토콜의 일부분으로서 수취인(상점)을 통과하게 되며, 수취인에 의해 동전이 예치되었을 때 은행에 들어가게 될 것이다. 추적기관은 법원의 영장과 같은 신뢰되는 기관의 명령에 의해 이러한 정보를 은행으로부터 넘겨받아 복구하게 된다. 다음으로 화폐 추적(Coin Tracing) 모델은 물건을 구입하기 전에 추적하는 기능을 제공한다. 즉, 화폐 발행시에 사용자가 은행에 제시한 데이터로부터 추적 기관은 동전 식별 정보를 얻어내고, 이를 통해 사용자가 은행으로부터 인출한 동전을 확인한다. 그리고 나서 물품 구입에 사용한 화폐와 인출된 동전을 연결시킬 수가 있다. 이때 화폐를 추적하기 위한 식별자는 동전에 직접적으로 관련된 정보가 되며, 사기와 같은 범죄 활동을 추적할 수 있다. 이 방식은 순차추적(Forward Traceability) 방식이라고도 하며, 추적 기관은 인출 기록이 주어졌을 때 예치 기록을 식별하기 위한 능력을 가지게 된다. 즉, 사용자에 대한 추적 근거가 제공되면, 사용자가 화폐를 어디에 사용했는지를 드러내게 된다. 이와 같이 화폐 추적은 불법적인 상품들을 구매하는데 사용된 화폐들의 목적지를 추적함으로써 판매자의 계좌를 알아낼 수 있다.

또한 추가적으로 화폐 추적은 전자화폐의 약탈 문제를 해결해 준다. 만약 어떤 사용자가 전자화폐를 약탈당하고 익명으로 그 화폐가 인출되었다면 약탈자는 자신의 신원을 확인하지 않기 때문에 불법으로 인출된 동전들을 사용할 수가 있게 되는데 이 모델을 적용하여 인출 정보로부터 동전 식별자를 얻어내고 이를 각 상점의 블랙리스트에 올림으로서 약탈자의 활동을 추적할 수가 있다.

4. 새로운 공정한 은닉 DSS 서명

본 장에서는 미국내 전자서명 표준인 DSS (Digital Signature Standard)[24]를 이용하여 새로운 공정한 은닉 DSS 서명 기법을 제안한다.

가. 시스템 파라메터

시스템 파라메터는 DSS에서 사용한 파라메터들을 사용하며 서명문은 서명자가 제공한 파라메터로부터 사용자가 추출한다.

- p : $2^{L-1}<p<2^{L}$, $512\le L\le 1024$인 소수
- q : $p-1$로 나누는 소수이고 $2^{519}<q<2^{160}$
- $g\in Z_p$: $g=h^{(p-1)/q} \bmod p$ $(g>1,$ $1<h<p-1)$, 즉 g의 위수가 q이다.
- a, b : 검증자가 선택하는 은닉 인자이다. a, $b\in_R Z_q^*$
- $H(\cdot)$: 일방향 해쉬함수
- x : $0<x<q$인 비공개 서명키
- y : $y=g^x \bmod p$로 계산되는 공개 검증키

나. 초기화 단계

이 단계에서는 프로토콜을 시작하기 전에 참여 객체가 생성해야 할 파라메터들을 생성한다.

(1) 사용자
- ID : 사용자 식별값으로 사용자가 랜덤하게 선택하며 비밀로 보관. $ID\in_R Z_p$
- I : 사용자가 생성하여 서명자에게 등록. $I\equiv(g_1)^{ID} \bmod p$ 여기서, g_1은 GF(p)상의 원시근으로 서명자가 생성하여 공개한 값이다.

(2) 서명자
- p, q : DSS 서명 방식에서 사용한 소수로서 서명자가 생성하여 공개.
- g_1 , g_2 , g_3 : GF(p)상의 원시근으로 서명자가 생성하여 공개.
- $x\in_R Z_p$: 개인키
- $y\equiv(g_1)^x \bmod p$: 공개키

(3) 신뢰기관
- $X_T\in_R Z_p^*$: 개인키
- $Y_T\equiv(g_2)^{X_T} \bmod p$: 공개키

다. 서명 단계

서명 단계를 통해 사용자는 서명자로부터 은닉된 서명문을 얻는다. 이때 사용자의 프라이버시 보호를 위해 DSS 프로토콜을 변형하여 은닉 서명문을 생성하며, 부정행위 발생시에 신뢰기관에 의해 사용자의 신원을 검출 할 수 있도록 하기 위해 사용자가 추적 인자를 생성하여 서명자에게 제공한다. 이때 추적 인자값은 서명자가 공개한 값과 사용자가 생성한 I값, 그리고 신뢰기관의 공개키 값을 이용하여 생성하며 서명자는 사용자가 생성한 추적 인자가 올바르게 생성되었는지 확인한다.

(1) Step 1

사용자는 랜덤하게 $v\in_R Z_q$를 생성한다. 그리고 추적인자 생성에 사용될 A_1'과 A_2'을 계산하여 서명자에게 전송한다.

$$A_1' \equiv (Y_T)^v \bmod p,$$

$$A_2' \equiv I \cdot g_2 \cdot (g_3)^{v^{-1}} \bmod p$$

(2) Step 2

서명자는 사용자가 A_1', A_2'이 올바르게 생성하였는지 증명과정을 수행한 뒤 $k \in {}_RZ_q$를 생성하고 이를 이용하여 다음과 같이 R을 생성한다. 그리고 R을 사용자에게 전송한다.

prove : $\log_{g_3}(A_2'/Ig_2) \stackrel{?}{=} \log_{A_1 \cdot Y_T}$

$$R \equiv g^k \bmod p$$

여기서, $\log_{g_3}(A_2'/Ig_2) \stackrel{?}{=} \log_{A_1 \cdot Y_T}$에 대한 증명은 (그림 1)과 같이 v값을 노출시키지 않고 추적인자 생성에 대한 증명을 수행하도록 한다. 그와 같은 증명은 G.Davida, Y.Frankel, Y.Tsiounis, 그리고 M.Yung[23] 등에서 언급되고 있으며 그것들은 knowledge에 대한 Schnorr 증명에 기반하고 있다[9].

(3) Step 3

사용자는 자신의 식별값 I를 은닉시키기 위한 은닉 인자 $a \in {}_RZ_q^*$와 $b \in {}_RZ_q^*$를 생성하고 이 파라메터와 서명자가 전송한 R을 이용하여 r'값을 계산한다.

$$r' \equiv IR^a g^b \bmod p$$

다시 이 r'값을 일방향 해쉬 함수를 이용 I'을 계산하여 서명자에게 전송한다.

$$I' = H(r')$$

(4) Step 4

서명자는 Step 2에서 랜덤하게 선택한 k의 역원을 구하고 사용자로부터 받은 I'과 서명자의 비밀키 값 x를 이용하여 s을 다음과 같이 계산하고 이를 사용자에게 전송한다.

$$k^{-1}k \bmod q = 1$$

$$s = k^{-1}(I' + xR)$$

(5) Step 5

사용자는 서명자가 계산하여 보내 준 값 s을 이용하여 $w = s^{-1} \bmod q$을 구하고, 다음과 같이 M, N, V을 구한다.

$$M = I'w \bmod q$$
$$N = Rw \bmod q$$
$$V = (g^M y^N \bmod p) \bmod q$$

그리고 다음과 같이 서명문이 올바른 서명문인지 검사한다.

$$V \stackrel{?}{=} R$$

올바른 서명문인지를 확인 후, 서명문을 구성하기 전에 사용자는 공개 파라메터 p, Y_T, g_2와 Step 1에서 생성한 v, A_2'를 바탕으로 신뢰기관에 의해 추적 인자로 사용될 추적 파라메터 A, A_1, A_2, A_3를 생성하여 서명문을 구성한다.

$$A \equiv (A_2' \cdot Y_T)^v \cdot I \bmod p,$$
$$A_1 \equiv g_2^v \bmod p,$$
$$A_2 \equiv I^v \bmod p,$$
$$A_3 \equiv I \cdot (Y_T)^v \bmod p$$

서명문 : $[(R, s), A, A_1, A_2, A_3]$

이때, 추적 파라메터에 대한 유효성 검증은 수신자에 의해 이루어지며 유효하지 않을 경우 서명문의 수신은 거부가 된다 .

$$A \stackrel{?}{=} A_1 \cdot A_2 \cdot A_3 \cdot g_3 \bmod p$$

라. 사용자 신원 검출 단계

사용자가 은닉된 서명문을 부정하게 사용한 경

---

prove $\log_{g_3}(A_2'/Ig_2) \stackrel{?}{=} \log_{A_1 \cdot Y_T}$

$\delta \in {}_RZ_q$

$\alpha \equiv (Y_T)^{\delta} \bmod p$

$\beta \equiv (g_3)^{\delta} \bmod p$

$A_1' \equiv (Y_T)^v \bmod p$

$A_2' \equiv I \cdot g_2 \cdot (g_3)^{v^{-1}} \bmod p$

$r = \lambda\mu + \delta$

$\alpha,\ \beta,\ A_1'\ A_2'$ →

← λ ($\lambda \in {}_RZ_q$)

r →

verify :

$(Y_T) \stackrel{?}{=} a \cdot A_1'^{\lambda}$

$(g_3)^{-r} \stackrel{?}{=} (A_2'/Ig_2) \cdot \beta$

(그림 1) 추적인자 확인 과정

우에 있어서 사용자가 제시한 은닉 서명문을 받은 서명자는 사용자 신원을 파악하기 위해 추적인자 A_1, A_3를 신뢰기관에 제공함으로써 사용자 추적이 이루어진다.

(1) Step 1

서명문을 수신한 서명자는 서명문 으로부터 추적인자 A_1, A_3를 신뢰기관에 전송한다.

(2) Step 2

신뢰기관은 다음과 같이 A_1과 A_3로부터 $A_3' \equiv I^{X_T^{-1}} \cdot g_2^v \bmod p$을 구하고, 신뢰기관의 비밀키 X_T를 이용하여 다시 I를 계산한다.

$$A_3' \equiv A_3^{X_T^{-1}} \bmod p \equiv I^{X_T^{-1}} \cdot g_2^v \bmod p$$

$$A_3'/A_1 \bmod p \equiv (I^{X_T^{-1}} \cdot g_2^v)/g_2^v \bmod p$$

$$\equiv I^{X_T^{-1}} \bmod p$$

$$\therefore I = (I^{X_T^{-1}})^{X_T} \bmod p$$

5. 새로운 전자화폐 시스템

제안된 방식은 크게 시스템 초기화 단계, 인출 단계, 지불단계 그리고 예치단계의 기본적인 4단계와 그리고 불법행위 발생 할 경우 불법행위자를 추적할 수 있는 추적단계로 구성이 된다. 그리고 인출단계에서 사용자의 프라이버시를 보호하기 위해 4장에서 제안한 공정한 은닉 DSS를 적용하여 전자화폐를 인출한다. 먼저 각 개체는 시스템을 시작하기 전에 다음과 같은 초기화 단계를 수행하여 각 단계에서 사용할 파라메터를 생성한다.

가. 초기화 단계

(1) 사용자(u_i)

- ID_{u_i} : 사용자 식별값으로 사용자가 랜덤하게 선택하며 비밀로 보관한다. $ID_{u_i} \in {}_RZ_p$
- I_{u_i} : 사용자가 생성하여 은행에 계좌 개설시에 등록하는 값으로 사용자 식별값 ID_{u_i}을 이용하여 생성한다.

  $I_{u_i} \equiv (g_1)^{ID_{u_i}} \bmod p$
- w : 사용자가 은행으로부터 처음으로 발급받은 금액

사용자		서명자
$v \in {}_RZ_q$		
	추적인자 검증	
$A_1' \equiv (Y_T)^v \bmod p$		
$A_2' \equiv I \cdot g_2 \cdot (g_3)^{v^{-1}} \bmod p$	$\log_{g_3}(A_2'/Ig_2) \stackrel{?}{=} \log_{A_1 \cdot Y_T}$	
	$\longrightarrow$	$k \in {}_RZ_q$, $R \equiv g^k \bmod p$
	R	
$a \in {}_RZ_q^*$ $b \in {}_RZ_q^*$	$\longleftarrow$	
$r' \equiv IR^a g^b \bmod p$		
$I' = H(r')$	I'	
	$\longrightarrow$	$k^{-1}k \bmod q = 1$ 인 k 구함
		$s = k^{-1}(I' + xR)$
	s	
	$\longleftarrow$	
$w = s^{-1} \bmod q$		
$M = I'w \bmod q$		
$N = Rw \bmod q$		
$V = (g^M y^N \bmod p) \bmod q$		
$V \stackrel{?}{=} R$		
$A \equiv (A_2' \cdot Y_T)^v \cdot I \bmod p$		
$A_1 \equiv g_2^v \bmod p$		
$A_2 \equiv I^v \bmod p$		
$A_3 \equiv I \cdot (Y_T)^v \bmod p$		
서명문 : $[(R, s), A, A_1, A_2, A_3]$		

(그림 2) DSS에 기반한 공정한 은닉 서명

- w_i : i번째 사용자가 i+1번째 사용자에게 양도한 금액
- C : 사용자가 은행으로부터 발급 받은 전자화폐 데이터

(2) 은행(Bank)
- p, q : DSS 서명 방식에서 사용한 소수로서 은행이 생성하여 공개.
- g_1 , g_2 , g_3 : GF(p)상의 원시원으로 은행이 생성하여 공개.
- $x \in {}_R Z_p$: 개인키
- $y \equiv (g_1)^x \bmod p$: 공개키
- TS : Time Stamp

(3) 신뢰기관(Trustee)
- $X_T \in {}_R Z_p^*$: 개인키
- $Y_T \equiv (g_2)^{X_T} \bmod p$: 공개키

나. 인출단계

인출단계를 통해 사용자는 은행으로부터 전자화폐(C)를 발급받는다. 이때 사용자의 프라이버시 보호를 위해 4장에서 언급하였던 공정한 은닉 DSS 서명 프로토콜을 이용하며, 부정행위 발생시에 법원의 명령에 의해 은행과 공정한 추적기관이 추적할 수 있도록 하기 위해 사용자가 추적 인자를 생성하여 은행에게 제공한다. 이때 추적 인자값은 은행이 공개한 값과 사용자가 생성한 I값, 그리고 추적기관의 공개키 값을 이용하여 생성하며 은행은 사용자가 생성한 추적 인자가 올바르게 생성되었는지 확인한 뒤 전자화폐를 발행한다.

(1) Step 1

사용자 u_i는 랜덤하게 $v \in {}_R Z_q$를 생성한다. 그리고 추적인자 생성에 사용될 A_{1u_i}'과 A_{2u_i}'을 계산하여 은행에게 전송한다.

$$A_{1u_i}' \equiv (Y_T)^v \bmod p,$$

$$A_{2u_i}' \equiv I_{u_i} \cdot g_2 \cdot (g_3)^{v^{-1}} \bmod p$$

(2) Step 2

은행은 (그림 1)과 같이 사용자 u_i가 A_{1u_i}', A_{2u_i}'이 올바르게 생성하였는지 증명과정을 수행한 뒤 $k \in {}_R Z_q$를 생성하고 이를 이용하여 다음과 같이 R을 생성한다. 그리고 R을 사용자 u_i에게 전송한다.

prove : $\log_{g_3}(A_{2u_i}'/I_{u_i}g_2) \stackrel{?}{=} \log_{A_{1u_i}} Y_T$

$$R \equiv g^k \bmod p$$

(3) Step 3

사용자 u_i는 자신의 식별값 I_{u_i}를 은닉시키기 위한 은닉 인자 $a \in {}_R Z_q^*$와 $b \in {}_R Z_q^*$를 생성하고 이 파라메터와 은행이 전송한 R을 이용하여 r' 값을 계산한다.

$$r' \equiv I_{u_i} R^a g^b \bmod p$$

다시 이 r'값을 일방향 해쉬 함수를 이용 I_{u_i}'을 계산하여 서명자에게 전송한다.

$$I_{u_i}' = H(r')$$

(4) Step 4

은행은 Step 2에서 랜덤하게 선택한 k의 역원을 구하고 사용자 u_i로부터 받은 I_{u_i}'과 은행의 비밀키 값 x를 이용하여 s을 다음과 같이 계산하고 사용자 u_i의 계좌로부터 인출한 인출 금액 w에 은행의 서명을 한 뒤 s와 $sign_B(w)$를 사용자 u_i에게 전송한다.

$$k^{-1}k \bmod q = 1$$

$$s = k^{-1}(I_{u_i}' + xR)$$

(5) Step 5

사용자 u_i는 은행이 계산해서 보내 준 값 s을 이용하여 $\Phi = s^{-1} \bmod q$을 구하고, 다음과 같이 M, N, V을 구한다.

$$M = I_{u_i}' \Phi \bmod q$$

$$N = R\Phi \bmod q$$

$$V = (g^M y^N \bmod p) \bmod q$$

그리고 다음과 같이 서명문이 올바른 서명문인지 검사한다.

$$V \stackrel{?}{=} R$$

올바른 서명문인지를 확인 후, 서명문을 구성하기 전에 사용자 u_i는 공개 파라메터 p, Y_T, g_2와 Step 1에서 생성한 v, A_{2u_i}'를 바탕으로 신뢰기관에 의해 추적 인자로 사용될 추적 파라메터 A_{u_i}, A_{1u_i}, A_{2u_i}, A_{3u_i}를 생성하여 화폐를 구성한다.

$$A_{u_i} \equiv (A_{2u_i}' \cdot Y_T)^v \cdot I_{u_i} \bmod p,$$

$$A_{1u_i} \equiv g_2^v \bmod p,$$

$$A_{2u_i} \equiv I_{u_i}^v \bmod p,$$

$$A_{3u_i} \equiv I_{u_i} \cdot (Y_T)^v \bmod p$$

$$C = [(R, s), w, A_{u_i}, A_{1u_i}, A_{2u_i}, A_{3u_i}]$$

다. 지불단계

사용자 u_i이 전자화폐 C를 이용하여 인출금액보다 적은 금액 w_1 ($\leq w$)를 상점 V에게 지불하기 원한다고 가정하면 다음과 같은 단계를 수행한다.

(1) Step 1

사용자 u_i는 먼저 $\theta \in {}_R Z_p^*$를 선택하고 대금지불의 유효성을 확인하기 위한 파라메터 V_{1u_i}, V_{2u_i}을 계산한다.

$$V_{1u_i} \equiv (g_2)^{\theta} \bmod p,$$

$$V_{2u_i} \equiv g_1^{ID_{u_i} \cdot \theta} \mod p,$$

그리고 은행으로부터 받은 전자화폐 C와 지불하기 원하는 금액 w_1을 연접시키고 이 값에 사용자 u_i의 서명을 수행한다.

$$T_{u_i} = sign_{u_i}(C \| w_1)$$

또한 $B_{u_i} = [B_{1u_i}, B_{2u_i}]$을 계산하여 대금 지불을 위해 이 값들을 모두 상점에 전송한다.

$$B_{1_{u_i}} \equiv (g_1)^{\alpha} \mod p,$$

$$B_{2u_i} \equiv (g_2)^{\beta} \mod p,$$

$$(V_{1u_i}, V_{2u_i}, B_{u_i} w_i, C, T_{u_i})$$

(2) Step 2

상점은 사용자 u_i가 지불한 금액의 유효성을 검사하기 위해 우선 T_{u_i}에 대한 사용자 u_i의 서명을 확인하고 C에 포함된 사용자 u_i의 추적인자 값들에 대한 유효성 검증을 수행한다. 만약, 이때 추적인자값들이 유효하지 않을 경우 전자화폐의 수신은 거부가 된다.

$$A_{u_i} \stackrel{?}{=} A_{1u_i} \cdot A_{2u_i} \cdot A_{3u_i} \cdot g_2 \mod p$$

그리고 유효하다면 사용자 u_i가 상점에 보낸 파라메터들의 유효성을 확인하기 위해 challenge값으로서 d값을 계산하여 사용자 u_i에게 전송한다.

$$d = H(V_{1u_i} V_{2u_i} B_{u_i} C, T_{u_i}, TS)$$

(3) Step 3

사용자 u_i는 상점이 전송해 온 d값을 이용하여 response값으로 r_1'과 r_1''을 계산하여 상점에 다시 전송한다.

$$r_1' \equiv d \cdot ID_{u_i} \cdot \theta + \alpha \mod p,$$

$$r_1'' \equiv d\theta + \beta \mod p$$

(4) Step 4

상점은 사용자 u_i가 보내 온 r_1'과 r_2'' 값을 이용하여 Step 1에서 사용자 u_i가 전송한 파라메터들에 대한 유효성을 확인한 뒤 유효하다면 사용자 u_i가 지불한 금액을 받아들인다.

$$g_1^{r_1'} \stackrel{?}{=} (V_{2u_i})^d B_{1u_i} \mod p,$$

$$g_2^{r_1''} \stackrel{?}{=} (V_{1u_i})^d B_{2u_i} \mod p$$

라. 예치단계

상점 또는 최종 전자화폐 수신자는 자신이 받은 전자화폐 w_i을 은행에 전송하기 위해서 거래내역서 D를 은행에 전송한다.

$$D = (C, w_i, I_{u_i} T_{u_i}, V_{1u_i}, V_{2u_i}, B_{u_i}, r_i', r_i'')$$

은행은 자신이 받은 전자화폐들의 합계액이 $\sum w_i \le w$인지를 판단한다.

6. 제안 방식의 고찰

가. 전자화폐의 양도

사용자 u_{i+1}가 다른 사용자 u_{i+2}에게 자신이 받은 전자화폐 w_i보다 작은 전자화폐 w_{i+1}를 전송하기 위해서 사용자 u_{i+1}와 사용자 u_{i+2}는 5장에서 수행한 지불 단계를 수행한다. 여기서 사용자 u_{i+1}는 $(V_{1u_i}, V_{2u_i}, B_{u_i}, w_{i+1}, C, T_{u_{i+1}})$를 사용자 u_{i+2}에게 전송한다. 나머지 지불 단계는 동일하며 유효성을 검사해서 일치하면 지불을 받아들인다. 여기서 초기 사용자 u_i가 받은 w만큼의 금액은 그 한도 w가 넘지 않는 한도 내에서 지불인의 서명 아래에서 사용된다. 이때 i번째 사용자는 자신이 받은 w_{i-1} 금액보다 적은 금액을 사용해야 하며 그 한도액과 사용하고자 하는 금액이 T_i에 들어가게 되어 사용자가 사용자의 서명을 확인함으로써 금액의 초과 사용을 검증할 수가 있다. 또한 같은 금액을 여러 번 다른 사용자에게 사용하더라도 은행에서 부정한 사용자의 서명을 검사하여 전자화폐의 초과 사용을 검사할 수가 있기 때문에 부정 사용자를 밝혀낼 수 있다.

나. 익명성 제어

익명성 제어는 사용자가 부정사용 하였을 경우에 거래 내역서에 포함된 추적인자를 통해 사용자 식별자를 드러내거나 또는 화폐 사용시 부가되는 화폐 고유 식별값을 드러냄으로서 이루어진다. 이러한 익명성 제어 모델은 크게 두 개로 구분해 볼 수 있다. 하나는 전자화폐의 소유자를 식별하는 소유자 추적(Owner Tracing)과 은행으로부터의 화폐 인출을 식별하기 위한 동전 추적(Coin Tracing)이 있다. 소유자 추적에 있어서 익명성 제어 파라메타는 추적기관이 지불이 이루어지고 난 후, 화폐의 소유자를 판별해 낼 수 있도록 해준다. 이것의 목적은 지불이 이루어지고 난 후에 많은 화폐 유통들에 대해 합법적인 단속 요구로 이중 사용이나 위·변조와 같은 불법 사용이 일어나지 않았더라도 추적하는 것을 가능하게 해준다. 반면에 화폐의 일련번호를 추적하는 것과 유사한 동전 추적은 물건을 구입하기 전에 추적하는 기능을 제공한다. 화폐 추적에 있어서 추적기관은 은행으로부터 인출된 화폐를 확인하고 물품 구입에 사용한 것과 인출된 화폐를 연결시킬 수 있다.

(1) 화폐 추적

화폐 추적 기능을 통해 추적기관은 법원의 명령을 통해 사용자가 전자화폐를 사용하기 전에 은행에 추적 기능을 부여 할 수 있다. 즉, 인출 단계에서 사용자가 은행에 전송한 인출 사본 중 A_{1u_i}'으로부터 추적기관은 A_{1u_i}을 생성하고 이를 은행에 재 전송해 줌으로써 은행측에서는 이를 통해 화폐를 추적한다. 즉, 해당 화폐를 블랙리스트에 올림으로서 상점측에서 인수를 거부하도록 할 수 있으

며, 사용화폐와 인출화폐를 연결함으로써 화폐를 추적할 수가 있다. 화폐 발행 단계에서는 다음 과정을 수행시킴으로서 화폐 추적 기능을 제공한다.

- Step 1

은행은 사용자가 제시한 인출 사본 중 A_{1u_i}을 추적기관에게 제공한다.

- Step 2

추적기관은 A_{1u_i}'로부터 A_{1u_i}을 계산해낸다.

$$(A_{1u_i}')^{X_T^{-1}} \equiv (Y_T^v)^{X_T^{-1}}$$
$$\equiv g_2^{X_T \cdot v \cdot X_T^{-1}}$$
$$\equiv g_2^v \equiv A_{1u_i}$$

- Step 3

추적기관은 A_{1u_i}을 은행에게 전송한다.

이때 은행은 추적기관이 전송해 준 A_{1u_i}을 사용자가 생성하여 지불 단계에서 상점에 제공하는 A_{1u_i}과 연결시킴으로서 물품을 구입하기 전에 지불의 적법성과 상관없이 추적 기능을 제공한다.

(2) 사용자 추적

사용자 추적 단계는 지불이 성립되고 난 후에 사용자를 판별하는 방법으로서 합법적인 화폐 교환이 이루어지고 난 후에 사용자 추적을 가능케 한다. 이러한 기능을 통해 추적기관은 사용자가 불법적인 물품을 구입한 장소로부터 전자화폐를 찾아 그 화폐의 사용자를 추적하게 된다. 이 단계는 예치 단계에 추가하여 구성되며 사용자가 상점에 대금 지불시 $A_{3u_i} = ID_{u_i} \cdot (Y_T)^v \bmod p$가 추가된다.

- Step 1

은행은 상점이 예치한 거래 내역서로부터 A_{1u_i}, A_{3u_i}를 추적기관에 전송한다.

- Step 2

추적기관은 A_{1u_i}과 A_{3u_i}로부터 $A_{3u_i}' \equiv ID_{u_i}^{X_T^{-1}} \cdot g_2^v \bmod p$을 구하고, 다시 ID_{u_i}를 계산한다.

$$A_{3u_i}' \equiv A_{3u_i}^{X_T^{-1}} \bmod p$$
$$\equiv ID_{u_i}^{X_T^{-1}} \cdot g_2^v \bmod p$$

$$A_{3u_i}'/A_{1u_i} \bmod p \equiv (ID_{u_i}^{X_T^{-1}} \cdot g_2^v)/g_2^v \bmod p$$
$$\equiv ID_{u_i}^{X_T^{-1}} \bmod p$$

$$\therefore ID_{u_i} = (ID_{u_i}^{X_T^{-1}})^{X_T} \bmod p$$

- step 3

추적기관은 A_{1u_i}와 A_{3u_i} 그리고 ID_{u_i}에 자신의 서명을 한 후 은행의 공개키로 암호화하여 은행에 전송한다.

$$E_{K_B^v}(A_{1u_i} || A_{3u_i} || ID_{u_i} || sign_T(A_{1u_i} || A_{3u_i} || ID_{u_i}))$$

7. 결론

인터넷에서 이루어지는 전자상거래에서 가장 중요한 요소중에 하나가 전자화폐이다. 초기에 전자화폐에 대한 연구는 개인의 사생활을 보호하기 위해 완전한 익명성에 중점을 두고 연구되었다. 하지만 완전한 익명성을 제공함으로써 약탈, 돈세탁 및 불법적인 사용과 같은 범죄 행위에 사용될 가능성이 높아졌다. 따라서 개인의 사생활은 보호하면서 불법적인 사용에 대해 추적할 수 있는 새로운 요구조건인 익명성 제어가 등장하게 되었다. 하지만 익명성 제어 기능의 남용으로 은행, 신뢰기관 그리고 사용자 사이의 공평성 문제가 발생하게 되었다. 이에 공정성이라는 개념이 도입되었다. 그리고 공정성에 대한 연구가 활발하게 진행되었다. 따라서 본 논문에서는 미국 전자서명 표준인 DSS에 공정성과 은닉 서명을 추가하여 새로운 공정한 은닉 DSS를 제안하였다. 또 이 서명방식을 기반으로 하여 추적 가능한 공정한 전자화폐 시스템을 제안하였다. 본 제안 방식은 기존의 전자화폐 시스템의 기본 프로토콜인 인출, 지불, 예치 프로토콜에 추적 할 수 있는 추적 파라메터를 추가하여 평상시에는 사용자의 익명성을 제공해주지만 문제가 발생할 경우 이 추적 파라메터를 이용하여 사용자와 동전 추적을 할 수 있도록 제안했다.

참고문헌

[1] D.Chaum, "Blind Signautures for untraceable payments", In Advances in Cryptology, Crypto'82, pp 199-203, 1983

[2] R.Rivest, A.Shamir and L.Adleman, "A Method for Obtining Digital Signatures and Public-Key Cryptosystem", Communications of the ACM, Vol.21, No. 2, pp.120-126

[3] T.ElGamal, "A Public Key Cryptosystem and A Signature Scheme Based On Discrete Logarithms", Advances in Cryptology : Proceedings of Crypto'84, Springer LNCS 196, pp10-18, 1985

[4] T.Okamoto and K.Ohta, "Universal Electronic Cash", In Advances in Cryptology-Crypto'91, pp324-337

[5] T.Okamoto and K.Ohta, "Disposable Zero-knowledge Authentications and Their Applications to Untraceable Electronic Cash", Proceeding of Crypto'89, pp481-496, 1989.

[6] T.Okamoto, "An Effieient Divisible Electronic Cash Scheme", Advances in Cryptology, Proceeding of Crypto '95, pp438-451, 1995

[7] M.Jakobsson and M.Yung, "Revokable and Versatile Electronic Money", In Proceedings of the third annual ACM security '96, 1996

[8] W.Diffie and M.E.Hellman, "New Directions in Cryptography", IEEE Trans. Info. Theory IT-22, Nov. 1976, pp.644-654

[9] C.P.Schnorr, "Efficient Signature Generation for Smart Cards", Proceeding of Cypto'89, pp. 239-252, 1989

[10] D.Chaum and T.P.Pederson, "Wallet databases with observes", Proproceeding of CRYPTO '92, Springer - Verlay, pp89-105, 1992

[11] S.Brands, "Untraceable off-line Cash in wallets with observers", In Advances in Cryptology-Crypto'93, Proceedings, pp302-318, 1993

[12] J.Camenisch, J.M. Piveteau, and M.Stadler, "Blind signatures based on the discrete logarithm problem", Advances in Cryptology-EUROCRYPT '94, volume 950 of Lecture Notes in Computer Science, page2428-432, 1994
[13] S. von Solms and D. Naccache, "On Blind Signatures and Perfects Crimes", Computers and Security, 11 (1992) pp. 581-583
[14] M.Stadler, J-M.Piveteau and J.Camenisch, "Fair Blind Signatures", Advances in Cryptology-Proceedings of Eurocrypto '95, pp.209-219, 1995.
[15] M.Jakobsson and M.Yung, "Revokable and Versatile Electronic Money", In Proceedings of the third annual ACM security '96, 1996
[16] L.Law, S.Sabett and J.Solinas, "How to make a mint : the cryptography of anonymous electronic cash", No. 96-10-17, National Security Agency, Office of Information Security Research and Technology, Cryptology Division, jun 18 1996.
[17] Y.Frankel, Y.Tsiounis and M.Yung, "Indirect discourse proofs : achieving fair off-line e-cash", In Advances in Cryptology, Proc. of Asiacrypt'96, pp. 286-300, November 3-7 1996
[18] G.Davida, Y.Frankel and Y.Tsiounis, "Anonymity Control in E-Cash Systems", In Proceedings of the 1st Financial Cryptography conference, Anguilla, BWI, February24-28, 1997.
[19] 오형근, 이임영, "익명성 제어 기능을 가지는 전자화폐 프로토콜에 관한 연구", 한국통신정보보호학회 종합학술발표회 논문집 Vol 8. No 1. pp 109-121. 1998.
[20] S. von Solms and D. Naccache, "On Blind Signatures and Perfects Crimes", Computers and Security, 11 (1992) pp. 581-583
[21] E.F.Brickell, P.Gemmell and D.Kravitz, "Trustee-based tracing extension to anonymous cash and the making of anonymous change", In Symposium On Distributed Algorithms(SODA), Albuquerque, NM. Available at http://www.cs.sandia.gov/~psgemme/, 1995
[22] M.Stadler, J.M.Piveteau and J.Camenisch, "Fair blind signatures", In Advances in Cryptology, Eurocrypto '95, pp209-219, 1995
[23] G.Davida, Y.Frankel and Y.Tsiounis, "Anonymity Control in E-Cash Systems", In Proceedings of the 1st Financial Cryptography conference, Anguilla, BWI, February24-28, 1997. http://www.ccs.neu.edu/home/hiannis/pubs.html
[24] DIGITAL SIGNATURE STANDARD (DSS) http://www.itl.nist.gov/fipspubs/fip186.htm