通信情報保護學會誌
第5卷 第3號, 1995. 9

Internet을 위한 전자화폐

박 승 안*, 신 현 용**

1. 서 론

최근의 정보화 사회는 Internet 이라는 거대한 통신망에 의하여 움직이고 발전해 가는 것 같다. 이미 150여 나라의 수천만명이 Internet에 접속하고 있는 것으로 조사되며 그 수는 급격히 증가하는 추세라고 한다. 특히 Internet의 기존의 다양한 서비스를 통합한 WWW (World-Wide-Web)과 그를 위한 Netscape와 같은 web-browser의 출현은 Internet의 무한한 잠재력을 실감케 하고 있다.

Internet을 통한 많은 정보교환은 필연적으로 Internet 안에 시장(market place)이 생기게 하고 다양한 사업(business)을 가능하게 한다. 이에 따라서 Internet 실정에 맞는 요금 지불 체계(payment system)가 필요하게 되었고 현재 개발중이다.

사실, 이미 여러 형태의 방안이 소개된 바 있다[2, 3, 4, 5, 6, 7, 8]. 본 글에서는 네델란드 CWI의 Stefan Brands에 의하여 최근에 제안된 방안을 소개하고자 한다. 편의상 이 방안을 ECI (Electronic Cash for Internet)라고 부르기로 한다.

* 서강대학교
** 한국교원대학교

2. ECI의 특징

ECI의 가장 큰 특징은 모든 고객은 은행이 제공하는 tamper-resistant device(이하 TRD라고 나타내기로 함.)를 자신의 컴퓨터와 함께 사용한다는 점이다. 이 TRD는 8비트의 마이크로 프로세서인 PCMCIA 카드로써 충분하다. 이 TRD는 고객에 의하여 소유되고 사용되며 또한 통제(moderate)도 받지만 가지고 있는 비밀 열쇠(은행이 제공한)는 노출시키지 않는다. 즉, TRD는 고객과 서로 통제와 협조를 하여 현금지불시 중요한 역할을 하게 된다. 한편 TRD는 고객의 계좌의 잔고를 거래때마다 정리하는 역할도 한다.

이 TRD는 값이 저렴하여 고객에게 부담을 주지 않으며, TRD를 고객이 공격하기도 쉽지 않지만 공격에 성공하여도 그 득이 크지 않도록 체계가 설계된다. 설령 공격이 성공하여 그 TRD 고유의 비밀 열쇠를 꺼낸다 해도 후에 그 사실이 드러나도록 설계된다.

결국, TRD는 여러 측면에서 안전하게 설계되어 전 체계의 안정성은 오직 부분적으로만 TRD에 의존하도록 하는 것이다.

현재로서는 TRD의 사용으로 말미암아 이 금융체계가 비현실적으로 보이지만 앞으로는 충분히 현실성있는 것으로 여겨진다.

사실, 지금까지 off-line인 전자 금융 체계에

서 고객에 의한 전자화폐의 중복사용(double spending)을 원천적으로 막는 방법은 TRD의 사용외에 제안된 바가 없기 때문에 만족스러운 안정성을 위해서는 TRD의 사용은 필연적인 것으로 여겨진다.

기존의 방안들과 비교할 때 ECI의 또 하나의 큰 특징은 공개 열쇠 암호체계(public-key cryptographic system)에 기반을 둔다는 것이다. 다양한 서명(signature)기법과 TRD를 활용하여 다음과 같은 괄목할 만한 기능(feature)들을 구현하고 있다.

(1) 안정성(security)

일반적인 은행거래시 고객은 자신의 금융거래가 노출되는 것을 원치않는 경우가 많다. ECI 방안에서는 사용된 돈(electronic cash)으로 부터 그 돈의 사용자를 추적 불가능(untraceable)하고 또 똑같은 계좌에서 두 번의 거래가 이루어져도 그 두 거래가 똑같은 계좌에서 이루어졌다는 사실을 알길이 없도록(unlinkable) 설계되었다. 이 두 기능은 은행과 사업자가 공모하여도 보장된다. 결국 고객의 금융행위는 완벽하게 그 비밀이 보장되게 된다. 은행측면에서의 안전성도 이상적이다. 특히 TRD의 기능으로 말미암아 전자화폐의 중복사용은 원천적으로 봉쇄되고 있다. 사업자 측면에서의 안전성은 증서(certificate, cert(PK))의 기능으로 부터 보장되고 있다. 이와 같은 이 체계의 다중적인 안전성(multi-party security)은 상대방등 그 누구나 기관을 신뢰할 필요없이 보장되는 것이 이 체계의 중요한 장점이다.

(2) Off-line 체계

On-line 금융체계에서는 안전에 관한 대부분의 문제는 해결된다. 그러나 On-line 체계는 운영경비와 효율성 측면에서 Internet 시장과 사업에는 적절하지 못하다.

ECI 방안은 매우 효율적인 off-line 체계로 설계되었다. 결국 사업자(service provider)는 받은 전자화폐를 모아서 편리한 시간에 Internet 은행에 예치할 수 있다.

(3) 효율성(efficiency)

ECI 방안에서 고객이 사업자에게 돈을 지불할 때에 고객은 마우스(mouse)를 한 번 click 함으로써 지불이 완료된다. 한편 이 지불은 World-Wide-Web을 여행하는 도중이나 또는 e-mail 등의 말미에 전자화폐를 보낼 수 있도록 편리하게 설계되었다. 물론 고객은 지불할 때에 은행이나 사업자와 대화(interaction)할 필요가 없다.

Internet 은행으로서는 50 기가바이트(Gigabyte)의 하드디스크 용량이면 10만개의 계좌가 매일 30번의 지불을 할 경우에도 1년을 감당할 수 있는 정도이다.

사업자는 10 Megabyte의 하드디스크 용량으로 65000건의 거래를 은행과의 접촉없이 처리할 수 있게 된다.

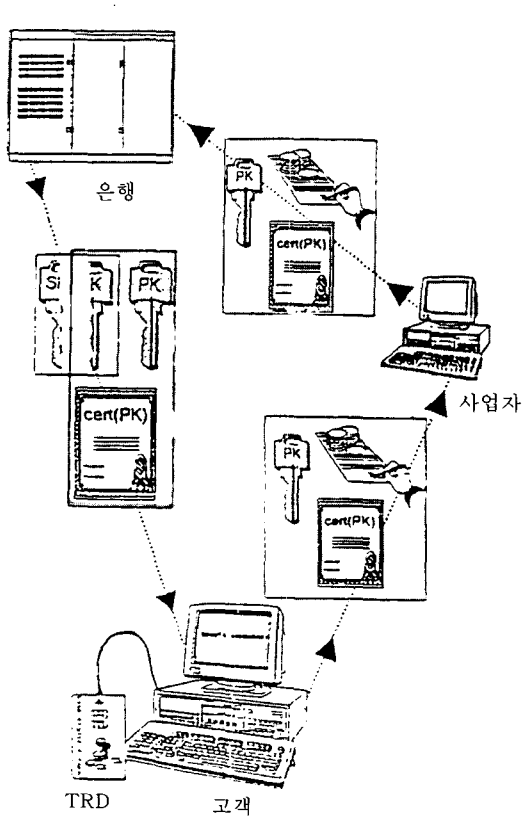
한편, 난수(pseudo-random number)를 사용하여 효율성을 극대화하는 것도 가능하다. 특히 난수를 사용하여 고객의 비밀 보장 특히 연계불가성(unlinkability)과 효율성을 교환(trade-offs)할 수 있다는 것은 주목할 만하다.

(4) 열린체계(open system)

이 체계의 관련자 즉 고객, 사업자, 은행은 아무런 사전 준비나 고지(告知) 없이 이 체계를 이탈하고 가입할 수 있다.

3. 체 계

ECI 체계를 대략적으로 나타내면 다음과 같다.



이제 ECI 체계에서의 각 단계를 간단히 설명하자.

(1) 은행(B)이 고객(U_i)에게 공개열쇠 PK를 제공한다.

(2) 은행은 고객에게 위의 공개열쇠에 대한 증서(certificate, cert(PK))를 준다.

(3) 은행은 위의 공개열쇠에 대응하는 (corresponding) 비밀열쇠 SK를 U_i의 컴퓨터 C_i와 U_i의 TRD(T_i)에 분산(shared) 한다. 즉 그 비밀 열쇠는 $((\beta_1,\alpha_1), (\beta_2,\alpha_2))$의 형태인데 네 개의 정보 α_1, α_2, β_1, β_2를 적절히 분산하여 C_i 또는 T_i 단독으로는 비밀열쇠에 관한 정보가 노출되지 않도록 한다. T_i에 의하여 소유된 비밀열쇠는 U_i로 하여금 한 전자돈의 중복 사용(double spending)을 원천적으로 막는 역할을 한다.

한편, C_i에 의하여 소유된 비밀 열쇠는 다음과 같은 역할을 담당한다.

첫째로, 고객이 정당한 거래행위를 통하여 전자돈을 한 번 밖에 사용하지 않았는데 은행이 두번 이상 사용하였다고 주장할 경우 그 주장을 반증할 수 있게 하여 준다.

둘째로, 고객의 TRD가 도난당하고 그 안의 비밀 열쇠가 노출되었어도 증서(certificate)를 사용할 수 없게 하는 기능이 있다.

은행에 의하여 제공되는 비밀 열쇠는 앞에서 언급한 바와 같이 T_i와 C_i에 의하여 적절히 공유(shared)되는데 C_i에 소유된 비밀 열쇠는 공개열쇠, 그리고 증서와 함께 Chaum이 소개한 blind 서명기법에 의하여 blind 됨으로 고객 U_i의 비밀을 완벽하게 보장해 준다. 즉 계좌추적을 불가능(untraceable)하게 하며 똑같은 계좌에서 두 번의 거래가 이루어졌을 때 그 두 거래가 연계불가능(unlinkable)하게 한다. T_i에 의하여 소유된 비밀 열쇠는 blind 될 수 없다.

(4) 고객이 사업자에게 대금을 지불할 때 고객은 금액, 사업자 명, 거래 일자등에 모두 서명한다.이렇게 함으로써 사업자가 같은 전자돈을 중복하여 예치할 수 없게 할 수 있다.

한편 이 서명은 TRD와 고객이 함께 참여해야 하므로 고객은 같은 전자 화폐를 중복하여 사용할 수 없게 된다.

4. 기 타

(1) T_i가 은행에 의하여 제공되고 U_i는 T_i에 제한적으로만 접근하므로 은행과 T_i 사이의 비밀채널(subliminal channel)이 가능할 수 있겠지만 C_i에 의하여 소유된 비밀열쇠는 은행과

TRD 사이의 모든 정보흐름을 조정(moderate)할 수 있게 하므로써 그런 비밀채널을 불가능하게 할 수 있다.

(2) 고객의 비밀보장을 위하여 은행으로 제공받는 공개열쇠와 그에 상응하는 증서, 그리고 비밀열쇠는 모두 일회용이어야 한다. 따라서 증서발급프로토콜(certificate issuing protocol)을 활용하여 간편하고 경제적 부담없이 비밀 열쇠와 그들에 대응하는 유효한(certified) 공개열쇠를 필요한 만큼 다량으로 제공받을 수 있게 설계 되어 있다.

(3) TRD는 간단한 계산만 하게 된다. 복잡한 계산 즉 암호학적 연산들(cryptographic operations)은 모두 C_i가 감당할 수 있게 할 수 있다.

(4) ECI의 모든 기능들을 구현하기 위하여 사용되는 기본(primitive) 프로토콜들은 다음과 같다.

① Schnorr 신분확인(identification) 기법
② Schnorr 서명기법
③ collision-free hash 함수
④ blind 서명기법
(이것에 관하여 [1]을 참조하기 바람.)
⑤ 소수 위수 군(group)의 표현 문제(representation problem)
(이것에 관하여 [1]에서도 언급되어 있음.)

5. 결 론

현재까지 제안된 Internet을 위한 금융체계 중에서 가장 주목할 만한 것으로 여겨지는 ECI 체계를 소개하였다. TRD와 PKC(공개 열쇠 암호체계)를 활용하여 여러가지 중요한 기능들을 구현할 수 있음을 언급하였다.

ECI 체계는 좀 더 섬세하게 설계하면 환전(conversion of differrent currency)이나 이체(transferability)가 가능하게 할 수 있다. 본 글에서 단계마다의 프로토콜(opening an account, withdrawal protocol, certificate issuing protocol, payment protocol, deposit protocol)을 자세히 설명하지 않았고 특히 수학적인 구현방법은 언급하지 않았다. 관심있는 독자는 World-Wide-Web을 통하여 자세한 프로토콜을 제시받을 수 있을 것이다.

마지막으로 본 체계의 안전성의 보장은 Schnorr 서명기법의 안전성과 이산 대수 문제(Discrete Log Problem)의 복잡성에 근거를 둔다는 것을 밝힌다.

참 고 문 헌

[1] 박승안, 신현용, 전자화폐의 연구현황, 통신정보보호학회지, Vol. 4, No. 4, 1994.

[2] Birch, D., "Downloading Software, Uploading Money-Business on the Infobahn," April 1994, presented in June 1994 at the Technology Appraisal's conference "Internet and Enterprise" in London.

[3] "World's first electronic cash payment over computer networks," DigiCash B.V. press release, May 27, 1994.

[4] Dukach, S., "SNNP: A simple network payment protocol," Proceedings of Computer Security Applications Conference, November 1992, pp. 173-179.

[5] Stein, L., Stefferud, E., Borenstein, N., Rose, M., "The Green Commerce Model," October 1994.

[6] Low, S., Maxemchuk, N., Paul, S., "Anonymous credit cards," Globecom '94.

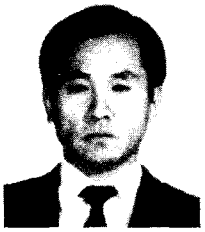
[7] Medvinsky, G., Neumann, B., "NetCash: a design for practical electronic currency on the Internet," *Proceedings of the First ACM Conference on Computers and Communications Security*, November 1993.

[8] "System planned for shopping in the Internet," Wall Street Journal, September 13, 1994.

□ 著者紹介

박 승 안 (종신회원)

서울대학교 사범대학 수학과 (이학사)
서울대학교 대학원 수학과 (이학석사)
University of Illinois at Urbana 대학원 수학과 (이학석사, 이학박사)
University of Illinois at Urbana 객원 교수
현재 : 서강대학교 이과대학 수학과 교수
한국통신정보보호학회 교육이사



신 현 용 (정 회 원)

서울대학교 사범대학 수학교육과 졸업 (學士)
서울대학교 대학원 수학교육과 졸업 (碩士)
미국 University of Alabama 졸업 (Ph. D)
네델란드 CWI(Centre for Mathematics and Computer Science) (Post Doc.)
해군 제2사관학교 수학교관
현재 : 한국교원대학교 제3대학 수학교육과 부교수

※ 주관심분야 : 무한군론, 응용대수학, 수학교육학