안전한 전자화폐를 위한 정보보호 기술

정보사회가 고도화될수록 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 정보보호 프로토콜(Cryptographic Protocol : 또는 암호 프로토콜) 분야이다. 〈편집자 주〉

박 성 준 정보보호센터 연구원

현재 우리나라도 고도 정보사회를 조기에 구축하여 국민들의 삶의 질을 향상시키기 위하여, 초고속정보통신망 구축, 멀티미디어 교육 SW개발, 원격진료시스템 구축 등을 국가사업으로 지정하여 추진중에 있다. 그러나 사회가 고도로 정보화될수록 그 역기능적인 측면으로 개인의 프라이버시를 비롯하여, 전산망의 불법적인 해킹 등 많은 정보보호 문제가 대두되고 있는 실정이다.

이러한 정보보호 문제를 해결하는 분야가 보안(Security)기술이다. 보안기술은 그 응용분야에 따라 다시 컴퓨터보안(Computer Security), 통신보안(Communication Security), 망보안(Network Security)으로 세분된다. 그리고 이러한 보안기술의 핵심 기반기술이 암호기술(Cryptology)이다.

일반적으로 암호기술이란 서로 신뢰하지 않는 사람들간에서 제기되는 비밀성(Secrecy), 인증(Authentication), 무결성(Integrity) 문제를 해결하는 기술이라 정의할 수 있다.

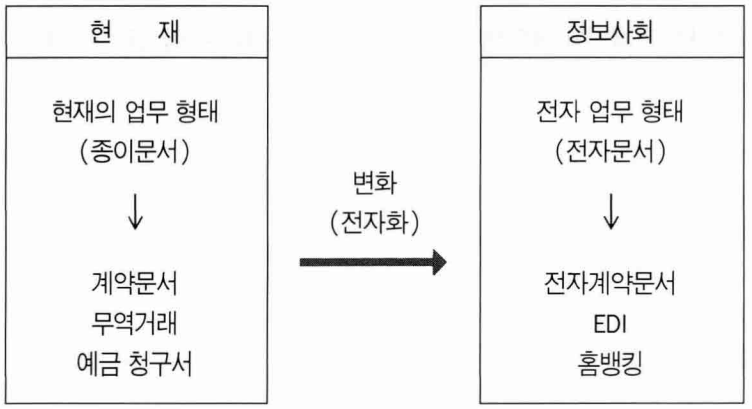
현재까지 암호기술 중에서 가장 많이 사용된 기술은 물론 통신보안의 핵심인 암호화 기술(Encryption)이다. 암호화 기술이란 평문을 허가받은 사람만이 해독가능한 암호문을 변환할 수 있는 기술이다. 이 기술은 공개된 전산망에서의 불법적인 도청을 방지하기 위하여 사용된다. 암호화기술은 사용되는 키의 종류에 따라 관용 암호알고리즘과 공개키 암호알고리즘으로 구분할 수 있다. 관용 암호알고리즘이란 암호화 키와 복호화 키가 같은 알고리즘이고, 공개키 암호알고리즘이란 암호화 키와 복호화 키가 다른 암호알고리즘을 말한다. 또한 관용암호알고리즘은 변화하는 방법에 따라 블럭암호알고리즘과 스트림암호알고리즘으로 구분될 수 있다.

또한 정보사회가 고도화될수록 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 정보보호 프로토콜(Cryptographic Protocol : 또는 암호 프로토콜) 분야이다. 대표적인 정보보호 프로토콜로는 전산망에서의 상대방의 신분을 확인하는 개인식별 및 인증기술, 현재의 도장이나 사인을 정보사회에 적합하게 변환시킨 전자서명기술 등이 있으며 현재 많은 관심과 시급히 개발이 요구되는 전자화폐도 정보보호 프로토콜 기술의 응용분야이다.

정보보호 프로토콜은 고도 정보사회에 야기되는 안전성 문제를 해결하는 암호학의 새로운 기술분야이다.

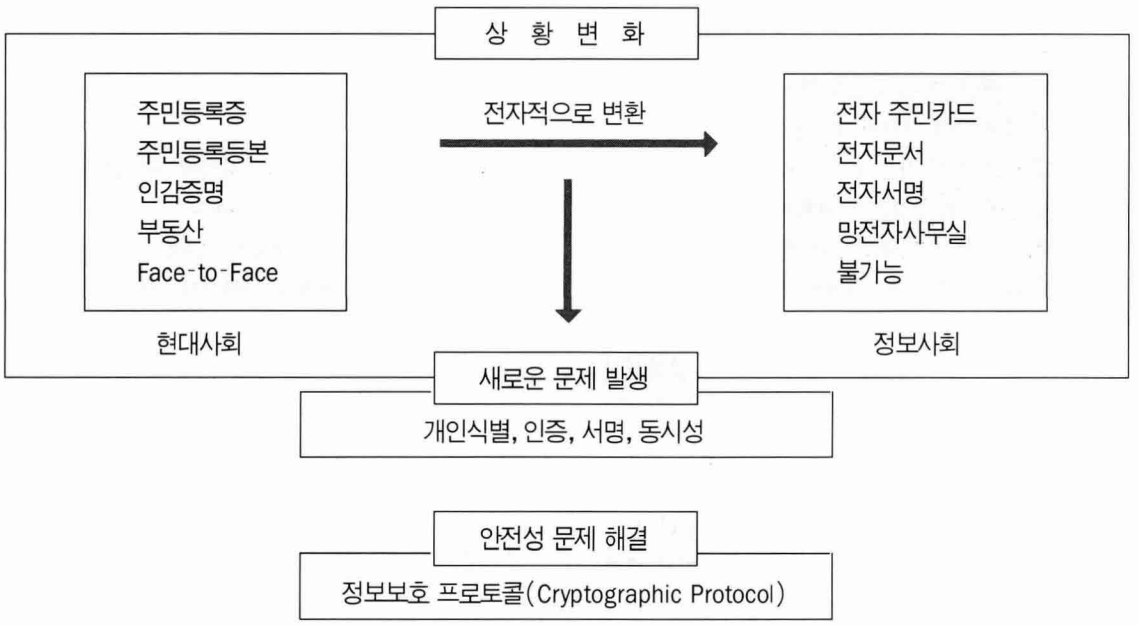
정보사회에서는 종이문서에 기반을 둔 기존의 모든 업무가 고도로 발달된 통신처리 및 정보처리 기술에 의해 전자문서에 기반을 둔 새로운 형태의 업무(전자적인 방식)로 변환된다〈그림1〉.

〈그림1〉 업무의 전자화



그러나 현재의 업무가 정보사회에 알맞은 전자적인 방법을 이용한 업무로 변환되기 위해서는 해결해야 할 몇가지 문제가 발생한다. 예를들어 현재의 부동산 계약이 정보사회에서의 전자계약으로 변환되는 과정을 분석하여 본다〈그림2〉.

〈그림2〉 전자계약에서의 안전성 문제



현대사회의 계약 관계를 자세히 고찰해보면 다음과 같은 안전성에 관련된 중요한 특성을 내포하고 있다.

- ○ 계약 당사자간의 상대방의 신분 인증(주민등록증, 주민등록등본 등)
- ○ 계약문서의 확인(문서 인증)
- ○ 계약 도장의 인증(인감증명)
- ○ 동일성(동일장소에서의 동시에 계약서에 인감을 날인)

물론 정보사회에서의 전자계약도 위의 특성을 만족해야 한다. 계약 당사자간의 상대방의 신분을 확인하는 것이 개인식별 문제, 계약문서의 내용을 확인하는 것이 인증 문제, 인감도장을 전자적으로 실현하는 것이 전자서명 문제이다. 특히 통신망을 통하여 전자적으로 동시성 특성을 해결하는 문제는 매우 어려운 문제로 현실적으로 불가능해 보이기도 한다. 이렇게 현실적으로 불가능해 보이는 안전성에 관련된 문제들을 해결해 주는 분야가 암호기술 분야의 정보보호 프로토콜(Cryptographic Protocol)이다.

정보보호 프로토콜 분야에는 기본적인 키분배 프로토콜, 인증 프로토콜, 비밀분산 프로토콜 등이 있으며, 복잡한 프로토콜로는 영지식 증명시스템, 전자결재, 전자선거, 전자지불, 전자화폐 등을 예로 들 수 있다.

전자화폐 요구 조건

인간이 수백년전부터 오늘날까지 사용해 온 화폐는 사회의 특성에 따라 다양한 형태를 가진다. 그것은 그 사회의 요구에 맞게 자신이 가지고 있는 기능을 효율적이고 안정적으로 수행하기 위함이다.

통신과 네트워크 기술의 비약적 발전으로 세계는 인터넷이라는 커다란 네트워크에 연결되어 있다고 해도 과언이 아니다. 이러한 인터넷을 이용한 전자상거래가 새로운 사업의 하나로 부상하고 있다. 전자상거래에서 가장 중요한 문제는 지불 방법에 관한 것이다. 가장 일반적으로 사용할 수 있는 지불 방법은 신용카드번호를 이용하는 것이다. 그러나 이 경우에는 은행이 사용자의 거래 내역을 추적하여 개인이 어디서 무엇을 샀는지에 관한 정보를 알 수 있는 문제점이 생긴다. 즉, 정보화사회에서의 핵심인 개인의 프라이버시를 침해하는 문제가 발생한다.

만약 전자상거래에서 익명성을 지닌 물리적 화폐(지폐 또는 동전)를 사용할 수 있다면 위에서의 문제점을 해결할 수 있다. 그러나 물리적 화폐는 전자상거래에 이용하기에는 그 형태가 적절하지 않다. 이러한 이유로 네트워크의 요구에 맞는 새로운 형태의 화폐인 전자화폐가 필요한 것이다.

전자화폐란 네트워크의 사용에 적합환 물리적 화폐의 변형된 형태이므로 물리적 화폐의 특성을 지녀야 한다. 우선 물리적 화폐의 특성을 살펴보면, 다음과 같다.

특성 1) 유통성
현금은 많은 사람에게 보편적인 가치를 가지고 양자간의 거래에 머물지 않고 계속해서 유통된다.

특성 2) 상징성(유일성)
현금의 거래는 은행 등에 일일이 문의하지 않더라도 Security가 지켜진다. 왜냐하면 지질, 인쇄의 특수성에 의해 현금 자신의 가치를 증명하기 때문이다.

특성 3) 익명성(프라이버시(Privacy) 보호기능)
현금이 어떠한 유통 경로로 사용되는지 추적이 불가능하도록 하여 프라이버시를 보호하는 기능이 있다.

물리적 화폐의 특성을 지니는 전자화폐의 기본 요구조건은 다음과 같다.

조건 1) 안전성
물리적 화폐의 상징성에 해당하는 특성으로 위조되어서는 안된다.

조건 2) 불추적성(Privacy : Untraceability)
물리적 화폐의 익명성에 해당하는 특성으로 은행은 사용자의 거래 내역을 보고 사용자가 자신의 돈을 어디에 얼마큼 사용했는지를 알 수 없어야 한다.

조건 3) 오프라인(Off-Line)
물리적 화폐의 유통성에 해당하는 특성으로 사용자가 전자현금을 사용할 때마다 은행이 개입할 필요는 없어야 한다

조건 4) 양도성(Transferability)

물리적 화폐의 유통성에 해당하는 특성으로 사용자가 다른 사용자에게 자신의 현금을 양도할 수 있어야 한다. 즉, 은행의 개입없이도 전자현금이 현금으로 유통될 수 있어야 한다.

조건 5) 이중 사용 방지

전자 화폐가 복사되어 두번 이상 사용되어서는 안된다.

전자 화폐의 효율성을 증가시키거나 특정 응용 분야에 이용될 경우, 추가되는 요구조건은 다음과 같다.

조건 6) 분할성

전자현금의 액면 가격을 사용자의 편의대로 나누어서 사용할 수 있다.

조건 7) n회 사용가능

일정한 현금을 일정한 횟수로 지불하는 응용, 예를 들어 교통료 징수 또는 정기 회수권 등에 이용될 수 있는 특성으로 한 번 발행받은 전자현금을 n번 사용이 가능하도록 한다. 그리고 만약 (n+1)번째 사용하면 사용자의 개인식별 정보가 노출되도록 한다.

전자화폐와 정보 보고 기술

위에서 언급한 전자화폐 요구조건을 만족시키기 위하여 정보보호 프로토콜이 사용된다. 사용되는 정보보호 기술은 여러 가지가 있지만 본문에서는 전자화폐의 가장 중요한 요구 조건인 프라이버시(불추적성, 익명성)을 보장하기 위한 암호 기술을 중점으로 설명하도록 하겠다.

전자화폐는 물리적 화폐가 그렇듯이 은행의 서명문이다.

일반적인 전자서명을 이용한다면 불추적성을 만족할 수 없다. 그래서 특수 서명의 일종인 은닉서명기법(Blind Signature)을 이용한다.

은닉서명방식(Blind Signature)

David Chaum이 1983년 CRYPTO '83에 제안한 특수전자 서명으로 서명자가 자신이 서명하는 메시지 M과 그 메시지를 전송한 사용자를 연결할 수 없는 특성을 가지고 있다.

RSA 방식을 이용하여 Chaum이 제한한 방식은 〈그림1〉과 같다.

〈그림1〉 D.Chaum의 은닉서명기법

갑 돌 이	(e,n) : 서명자의 공개키	서 명 자
랜덤한 r을 선택 $C=r^eM \bmod n$		d : 서명자의 비밀키
	C →	
		$C^d \bmod n$
	← $C^d \bmod n$	
메시지 M의 서명을 다음과 같이 계산 $C^d/r \bmod n = M^d \bmod n$		

위의 은닉서명기법을 전자화폐 발행 프로토콜에 작용하면 〈그림2〉와 같다.

〈그림2〉 D.Chaum의 은닉서명기법

갑 돌 이	(e,n) : 일정한 금액에 해당하는 서명자의 공개키	은 행 (서 명 자)
랜덤한 r을 선택 $C=r^eM \bmod n$		d : 서명자의 비밀키
	C →	
		갑돌의 계좌에서 e에 해당하는 금액을 인출
	← $C^d \bmod n$	
메시지 M의 서명을 다음과 같이 계산 $C^d/r \bmod n = M^d \bmod n$ 전자화폐 : (M,M^d)		$C^d \bmod n$

은행이 갑돌이에 대해서 알 수 있는 정보는 (r^eM, rM^d)이므로 나중에 전자화폐인(M, M^d)를 보아도 그것을 갑돌이와 연관지울 수 없다. 즉, 사용자의 불추적성이 만족된다.

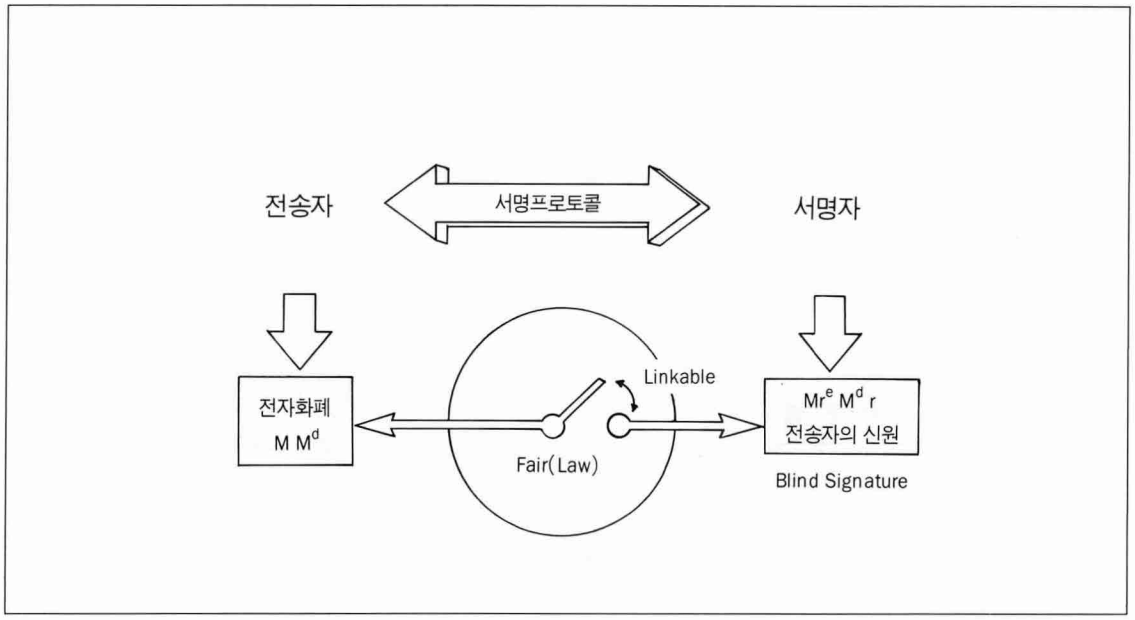
공정한 은닉서명방식(Fair Blind Signature)

전자화폐의 불추적성은 사용자의 프라이버시를 보장하는 반면 그 특성은 범죄에 악용되어 완전범죄를 용이하도록 하고 돈세탁이나 탈세 등의 문제점을 발생한다.

이러한 문제점을 막기 위해 필요시(법원의 요청)에는 사용자와 메시지(전자화폐)를 연결하는 fair 은닉서명방식이 1995년 Eurocrypt '95에 Stadler등에 의해 제안되었다.

fair 은닉서명방식의 개념은 〈그림3〉과 같다.

〈그림3〉 Fair 은닉서명 기법



〈그림3〉에서 보듯이 법원의 요청과 같이 특별한 경우에는 판사가 전자 화폐를 그 화폐의 주인과 연결지어 돈세탁이나 탈세 그리고 범죄에 악용되는 것을 방지할 수 있다.

결 론

전자화폐가 활성화되고 실용화되기 위해서는 전자화폐와 관련된 정보보호 문제 해결이 선결과제이며, 관련기관 또는 전문가들의 상호 협조가 매우 중요하다.

무엇보다도 전자화폐에 대한 올바른 개념 정립과 정보보호 기술의 필요성 인식을 바탕으로, 한국형 전자화폐에 대한 요구조건을 정립해야 할 것이다.

그리고 전자 상거래의 활성화를 위해 모든 정보보호 기술의 기반이 되는 키관리에 관한 인프라(PKI : Public Key Infrastructure)가 구축되어야 한다.