전자상거래 인증 서비스를 위한 검증 가능한 자체인증 방식

주 미 리[†] · 이 보 영[††] · 양 형 규[†††] · 원 동 호[††††]

요 약

본 논문에서는 전자상거래 인증 서비스를 제공하기 위하여 인증서에 기반한 방식의 장점과 Girault의 자체인증 공개키 방식의 장점을 결합한 검증 가능한 자체인증 방식을 고차잉여류 문제에 기반하여 제안한다. 제안한 방식의 안전성은 고차잉여류 문제와 이산대수 문제에 기반을 두고 있다.

Verifiable Self-Certified Schemes for Authentication Service of Electronic Commerce

Mi-Ri Joo[†] · Bo-Young Lee[††] · Hyung-kyu Yang[†††] · Dong-Ho Won[††††]

ABSTRACT

In this paper, for authentication service of electronic commerce, we propose the verifiable self-certified schemes based on the γ^{th}-residuosity, which are combine the benefit of certification based schemes and Girault's self-certified public keys. The security of our schemes is based on the difficulty of γ^{th}-residuosity problem and discrete logarithm problem simultaneously.

1. 서 론

최근 컴퓨터 및 네트워크 기술의 발전에 힘입어 인터넷은 비약적인 성장을 이루었고, 이를 기반으로 등장한 전자상거래는 시간적, 공간적 제약을 극복한 새로운 시장으로 부각되고 있다. 현재, 세계 각국은 국가 경쟁력 제고를 위한 핵심 수단으로 전자상거래 활성화를 추진하고 있으며 세계 시장을 선점하기 위한 노력을 가속화하고 있다.

현재 인터넷에서는 전자상거래를 위한 다양한 서비스들을 제공하고 있으나 인터넷 공간의 비대면 특성을 보완하고 상거래 행위의 신뢰성을 보장하기 위하여 제공되어야 할 기능들이 완전하지 않은 실정이다. 안전한 전자상거래 환경을 구축하기 위해서는 통신하는 상대방의 동일성을 확인할 수 있는 기능, 통신하는 메시지의 무결성을 확인할 수 있는 기능 및 송수신 사실을 부인할 수 없는 부인 봉쇄 기능 등을 가진 인증 서비스가 제공되어야 한다. 전자상거래의 필수 불가결한 요소인 인증 서비스는 암호 기술을 통하여 구현될 수 있으며, 불특정 다수를 대상으로 하는 전자상거래의 특성 상 공개키 암호 방식이 적합하다.

본 논문에서는 전자상거래의 필수 요소인 인증 서비스를 제공하고자 고차잉여류 문제를 기반으로 전자상거래에서 적용할 수 있는 검증 가능한 자체인증 방식을 제안하였다. 제안된 방식은 전자상거래의 전제가

※ 본 연구는 한국과학 재단의 특정기초연구(97-01-00-13-01-5) 지원 사업에 의해 수행하였습니다.
† 준 회 원 : 성균관대학교 전기전자및컴퓨터공학부
†† 정 회 원 : 인덕대학 정보통신학과 교수
††† 정 회 원 : 강남대학교 전자계산학과 교수
†††† 종신회원 : 성균관대학교 전기전자및컴퓨터공학부 교수
논문접수 : 2000년 6월 2일, 심사완료 : 2000년 9월 6일

되는 키 분배 프로토콜과 통신 상대의 동일성 및 통신 메시지의 무결성을 확인하고 송수신 사실에 대한 부인 봉쇄 기능을 제공하는 개인 식별 프로토콜과 디지털 서명 프로토콜 등으로 이루어진다.

본 논문은 다음과 같이 구성된다. 서론에 이어 2장에서는 전자상거래의 인증 서비스에 대하여 소개하고, 3장에서는 검증 가능한 자체인증 방식에 대하여 설명한다. 또한 4장에서는 제안하는 고차잉여류 문제에 기반한 검증 가능한 자체인증 방식을 제시하고 5장에서 결론으로 끝을 맺는다.

2. 전자상거래 인증 서비스

2.1 전자상거래

컴퓨터 및 통신 기술이 발전하면서 인터넷 사용자가 기하급수적으로 증가하고 있으며, 인터넷이라는 가상 공간을 무대로 하는 전자상거래(electronic commerce)는 시간과 공간의 제약을 탈피하고 국경의 한계를 초월하는 범세계적인 특성 때문에 일반인에게 급속도로 확산되고 있다.

전자상거래란 기업, 개인, 정부 등 경제 주체들이 정보통신기술을 활용하여 상품 및 서비스를 교환하는 거래 방식이라고 정의할 수 있으며, 좁은 의미로는 인터넷 확산에 따라 거래 활동에 인터넷을 이용하는 방식이라고 볼 수도 있다[1].

전자상거래는 다음과 같은 여러 가지의 장점을 가지고 있다. 먼저, 소비자가 번거롭게 직접 상품 매장에 나가지 않더라도 컴퓨터 화면으로 물건을 확인하고 구매할 수 있으며, 기업의 경우 유통 비용이나 건물 임대료 등의 비용이 거의 들지 않는다. 또한 기업은 시간과 장소의 제약없이 전세계의 모든 이용자와 직접 거래할 수 있기 때문에 전세계에 시장을 구축할 수 있을 뿐만 아니라 자사 서버의 홈페이지에 엑세스한 고객에 대해 보다 치밀한 서비스를 제공할 수 있다.

전자상거래를 행하는 목적은 상거래의 신속화와 효율화를 실현하고자 하는 것으로 인터넷 상에서 거래처 선택을 비롯한 상품 구매, 가격 교섭, 계약 체결, 대금 결제 등 상거래에 관련된 모든 업무를 전자적으로 처리할 수 있는 환경을 실현하는 것이다.

현재, 인터넷에서는 전자상거래를 위한 다양한 서비스들이 등장하고는 있으나 대부분이 기업과 개인 간의 거래에 있어서 개인 및 기업의 비밀 정보 보호와 대금 결제의 신뢰성 보장 등에 가해지는 위협에 대한 대책 수립이 완전하지 않은 실정이다. 안전한 전자상거래를 구현하기 위해서는 사용자에게 신뢰성을 보장해 주는 인증 서비스가 필요하다.

2.2 전자상거래 인증 서비스

불특정 다수의 개인이나 기업을 대상으로 한 인터넷 상의 상거래는 현실의 상거래와는 다른 특징을 갖는다. 인터넷 상에서 거래를 성립하고자 하는 경우 가격이나 구입 행위를 부인할 수 없는 구조가 필요하다. 또한 불특정 다수를 대상으로 한 인터넷 상에서는 상호 신원 확인이 어렵기 때문에 신뢰 및 보안 유지를 위해서 서버나 클라이언트의 인증 구조를 구축할 필요가 있으며 인터넷 상에서 거래 정보에 대한 도청, 개조 등의 문제를 방지하기 위한 기술 등이 필요하다. 즉, 인터넷 전자 공간의 비대면 특성을 보완하고 상거래 행위의 신뢰성을 보장하기 위하여 거래 당사자(양자 혹은 다자)간 신분 확인이 이루어져야 한다.

전자상거래에서의 신뢰 구축에 필수적인 거래 당사자의 신분 확인은 전문적이고 신뢰할 수 있는 기술을 이용한 인증 기술 및 서비스를 통하여 거래 사실 부인 및 거래 내용 시비 등의 제반 분쟁 해결에 사용된다. 따라서 인증 기술의 개발 보급은 국내외 상거래 및 민원 업무 등 전자거래의 활성화에 주요 기반 요소가 되며, 현재 암호 기법에 기반한 디지털 서명 방식, 사람의 생체 특성 방식 등의 기술 개발이 이루어지고 있다. 공개키 암호 방식을 이용한 디지털 서명 기술은 수학적으로 그 안전성을 증명할 수 있는 가장 확실한 인증 서비스로, 세계 선진 각국에서 전자 서명법을 제정·시행하고 있으며, 일부 국가들도 법 제정을 추진하고 있다.

2.3 인증서 발급 서비스 현황

안전한 전자상거래 환경을 구축하기 위해 사용되는 인증, 무결성, 기밀성, 부인 봉쇄 등의 인증 서비스는 공개키 암호 방식에 기반하고 있으며, 공개키의 무결성을 보장하고, 이를 실제 적용하기 위해서는 인증기관으로부터 공개키에 대한 인증서를 발급 받아야 한다.

인증서 발급 서비스는 일반적으로 두 가지로 분류된다. 첫 번째는 범용적인 보안 프로토콜의 확산으로 인해 요구되는 인증서 발급 서비스로서, 이 경우 인증기관은 각 객체들에 대한 인증서를 발급하고, 이에 대한

수수료를 받음으로써 경제적 이득을 취하게 된다. 두 번째는 안전한 인트라넷, 익스트라넷, 기업망, 폐쇄 네트워크 시스템 등의 구축을 위해 요구되는 서비스로서, 이때 사업자는 인증서 발급에 대한 수수료를 목적으로 하는 것이 아니라 자사의 안전한 네트워크 환경 구축을 목적으로 한다.

일반적으로 상업적 인증서 발급 서비스를 제공하는 인증기관들은 범용 프로토콜 지원을 목적으로 하는 인증서를 발급하고 있기 때문에, 특정 도메인에서 안전한 네트워크 환경 구축을 위해 제공되는 인증서 발급 서비스는 현황 파악에서 배제하고자 한다. 현재 세계적으로 제공되고 있는 상업적 목적의 인증서 발급 서비스 종류는 <표 1>과 같다[2].

〈표 1〉 인증서 발급 서비스 종류

종 류	용 도
S/MIME (Secure Multi-purpose Internet Mail Extension)	안전한 e-mail용(암호화·디지털 서명) 인증서
SSL (Secure Socket Layer)	웹 보안 프로토콜인 SSL을 웹 서버에 적용하기 위해 필요한 인증서(미국의 512비트)
Global 서버 ID	미국 외에서 강한 SSL을 사용하고자 하는 경우 필요한 인증서(1,024비트, 미국 상무부 허가 필요, 금융권으로만 제한)
OFX를 위한 금융 서버 ID	OFX(Open Financial Exchange) 프로토콜 적용에 필요한 인증서
EDI 서버 ID	안전한 EDI(Elcetronic Data Interchange) 구현에 필요한 인증서
Microsoft AuthenticCode ID	OCX, CLASS, CAB 등 마이크로소프트사에서 제공하는 기술을 사용하여 제작한 S/W의 온라인 판매시 사용되는 인증서
Netscape Object Signing	JavaScript, Java 등으로 제작된 S/W의 온라인 판매시 사용되는 인증서
SET (Secure Electronic Transaction)	SET 프로토콜 구현에 사용되는 인증서

3. 검증 가능한 자체인증 방식

대칭키 암호 시스템의 키 분배 문제 등을 해결하고자 제시된 공개키 암호 방식은 공개키 디렉토리 관리라는 새로운 문제를 발생시켰다. 공개키 디렉토리 관리 문제를 해결하기 위하여 제안된 방법으로는 개인식별정보에 기반(identity-based)을 둔 방식[3]과 인증서에 기반한(certification-based) 방식[4]이 있으며, 1991년 Girault는 위의 두 가지 방식의 중간 개념인 자체인증 공개키 방식(self-certified public key)을 제안하였다[4]. 이 방식은 별도의 인증서를 요구하지 않고 공개키 자체가 인증서의 역할을 하는 방식이므로, 인증서에 기반한 방식이 아니며, 공개키가 사용자의 개인식별정보에 제한되지 않기 때문에 역시 개인식별정보에 기반을 둔 방식도 아니다[5].

그러나 인증서에 기반한 방식에서는 인증 정보를 알면 곧바로 공개키가 검증될 수 있는 반면에, Girault가 제시한 자체인증 공개키 방식에서 공개키는 메시지 암호화나 서명 검증 또는 키 분배 프로토콜 등에서 공개키가 사용될 때 검증되므로, 자체인증 공개키를 사용하는 프로토콜이 실패하는 경우, 프로토콜에 오류가 발생하였는지 아니면 공개키에 오류가 발생하였는지 정확히 알 수 없다는 단점을 가지고 있다. 1999년 김승주 등은 이를 개선한 자체 인증(self certification)과 검증 가능성(verification)을 가진 검증 가능한 자체 인증 공개키 방식을 제안하였다[6].

3.1 검증 가능한 자체인증 방식의 정의[6]

검증 가능한 자체인증 공개키(Verifiable self-certified public keys) 방식은 다음 두 가지 조건을 만족한다.

3.3.1 자체인증(self-certification)

인증 정보는 공개키와 같다. 사용자의 개인식별정보(ID)나 비밀키/공개키 등은 어떠한 암호 프로토콜에서도 사용 중에 암시적으로 검증되며, 계산적으로 위조 불가능한 관계를 만족한다.

3.2.1 검증 가능(verifiability)

필요할 경우에는 인증 정보를 알고 난 후 공개키를 검증할 수 있는 효율적인 방법이 존재한다.

3.2 검증 가능한 자체인증 공개키 생성

검증 가능한 자체인증 공개키를 획득하기 위해서는, 먼저 신분이 확인된 사용자가 자신의 공개키를 인증기관에게 전달하고, 인증기관은 사용자의 개인식별정보와 전달받은 공개키를 이용하여 인증 정보를 생성한 후 사용자에게 전달한다.

다음은 RSA 디지털 서명 방식을 이용하여 검증 가능한 자체인증 공개키를 생성하는 과정을 3단계로 나타내고 있다.

[단계 1]

사용자 A는 임의의 정수 값 S_A를 자신의 비밀키로

선택하고 공개키 P_A를 다음과 같이 계산한 후, 인증기관에 P_A를 전송한다.

$$P_A \equiv g^{-S_A} \pmod{n}$$

[단계 2]

인증기관은 사용자 A의 신분을 확인한 후, A의 공개키와 개인식별정보 ID_A를 이용하여 인증 정보 w_A를 다음과 같이 계산한 후 사용자 A에게 전송한다.

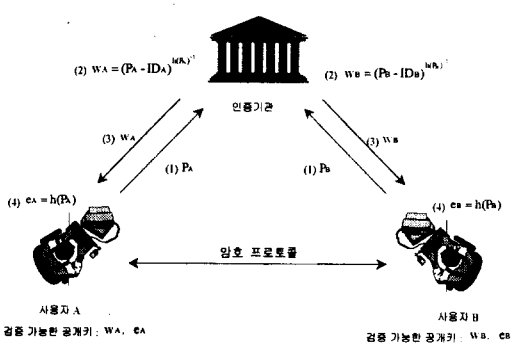
$$w_A \equiv (P_A - ID_A)^{h(P_A)^{-1}} \pmod{n}$$

[단계 3]

사용자 A의 검증 가능한 자체인증 공개키는 w_A와 e_A이다.

$$e_A \equiv h(P_A) \equiv h(b^{S_A}) \pmod{n}$$

(그림 1)은 사용자 A와 사용자 B가 각각 검증 가능한 자체인증 공개키를 발급 받는 과정을 나타낸 것으로, 앞의 3단계를 거쳐 검증 가능한 공개키를 생성한다. 각 사용자들은 검증 가능한 공개키를 이용하여 프로토콜에 참여한다.



(그림 1) 검증 가능한 자체 인증 공개키 방식

4. 제안하는 방식

이 절에서는 본 논문에서 제안하는 방식의 기본 개념인 고차잉여류 문제에 대한 수학적인 개념들을 정리하고 전자상거래에 적용할 수 있는 검증 가능한 자체인증 방식을 제안한다. 제안하는 방식은 이산대수 문제와 결합한 고차잉여류 문제에 기반을 두고 있다.

4.1 수학적 배경[7-10]

● 고차잉여류 문제

양의 정수 γ, n이 주어질 때 정수 z가 다음의 조건을 만족하면, z를 법 n에 관하여 고차잉여류(γ^{th}-residue)라 한다.

[조건] $\gcd(z, n) = 1$이고 $z \equiv x^{\gamma} \pmod{n}$을 만족하는 x가 존재한다.

위의 조건을 만족하지 않는 z는 고차비잉여류(γ^{th}-nonresidue)라 한다. 고차잉여류 문제(γ^{th}- Residuosity Problem : 약어로 γ^{th}- RP)란 주어진 $\gcd(z, n) = 1$인 양의 정수 $z \in Z_n^*$가 고차잉여류인지 고차비잉여류인지를 결정하는 문제이다.

n이 소수인 경우 위의 문제는 쉽게 해결되지만, n의 소인수를 알 수 없는 합성수인 경우 위의 문제는 매우 어렵다고 알려져 있다. 고차잉여류 문제의 계산 복잡도는 γ가 다항식 크기(polynomial size)일 때는 n의 소인수 분해 문제와 동치이고 γ가 지수적 크기(exponential size)일 때는 n의 소인수 분해 문제보다 어렵다고 간주되고 있다[7].

● 이산 대수 문제

소수 p가 주어지고 $y \equiv g^x \bmod p$인 경우, 역으로 $x \equiv \log_g y \bmod p$인 x를 계산하는 문제로, x를 법 p상에서 y의 이산 대수라 한다. 소수 p가 매우 크고 (2^{512}이상), g의 위수(order) k가 2^{140}이상인 경우, 다항식 시간 내에 x를 찾는 효율적인 알고리즘은 존재하지 않는다.

● Acceptable triple (n, γ, y)

(n, γ, y)가 아래의 세 가지 조건을 만족할 때 acceptable triple이라 한다.

[조건 1] $n = n_1 n_2 \cdots n_t$, 여기서 각 n_i는 홀수의 소수이다.

[조건 2] γ는 $1 \le k \le t$인 하나의 k에 대해 $\gcd(\gamma, \phi(n_k)) = \gamma$이고, 나머지 $i(\neq k)$에 대해 $\gcd(\gamma, \phi(n_i)) = 1$인 2 보다 큰 홀수이다.

[조건 3] $y \equiv h_1^{b_1 \gamma + e} \prod_{j=2}^{t} h_j^{b_j} \pmod{n}$, 여기서 모

든 $i \neq k$, $1 \leq j \leq t$에 대해 $0 < e < \gamma$, $\gcd(e, \gamma) = 1$, $k \leq b_j \leq \phi(n_j)$ 이고, $\langle h_1, h_2, \ldots, h_t \rangle$는 Z_n^*의 생성 벡터(generator -vector)이다.

- 잉여류 지수(class-index)

Acceptable triple (n, γ, y)과 $z \in Z_n^*$가 주어졌을 때 $z \equiv y^i u^\gamma \bmod n$을 만족하는 i를 z의 잉여류 지수(class-index)라 한다.(단 u는 Z_n^*상에서 임의로 선택된 수이다.)

4.2 시스템 초기화

제안하는 프로토콜에 참여하는 주체들은 다음과 같다.

- 인증기관(CA) 사용자의 공개키에 대한 인증 정보를 생성해 주는 기관
- 사용자(User) 구매자 또는 판매자로써 인증기관으로부터 인증 정보를 받고 통신을 하는 주체
- 검증자(Verifier) 상대방의 신분, 정당성 및 디지털 서명을 확인하는 주체
- 증명자(Prover) 자신의 신분 및 정당성을 검증자에게 확인시키려는 주체
- 서명자(Signer) 메시지(문서)에 서명한 주체

인증기관(Certification Authority)은 acceptable triple (n, γ^d, y)을 선택한다. 단, n은 소수 p와 q의 곱($n = p \cdot q$)이고, d는 γ가 지수적 크기를 갖도록 하는 임의의 정수이며 형태는 다음과 같다.

$$n = p \cdot q = (2\gamma^d fp' + 1) \cdot (2fq' + 1)$$

여기서, f, p', q'는 서로 다른 소수이고, $\gcd(\gamma, q') = 1$, $\gcd(\gamma, f) = 1$이다. y는 modulus n 상에서 $(\gamma^d)^{th}$-비잉여류이고, b는 modulus p와 modulus q 상에서 위수(order)가 f인 Z_n의 원소로, 법 n상에서의 위수(order)도 f이다. 인증기관의 공개키는 (n, γ^d, y, b, f)이고 비밀키는 (p', q')이다.

4.3 검증 가능한 자체인증 공개키 생성[11]

전자상거래에 참여하는 모든 사용자(판매자, 구매자 모두 포함)들은 인증기관으로부터 자신의 공개키에 해당하는 인증 정보를 발급 받아야 한다. 즉, 사용자 A는 인증기관 CA에 의해서 자신의 신분이 정당하다는 것을 확인 받은 후에, 인증기관으로부터 인증 정보(witness) w_A를 받는다. 사용자 A의 검증 가능한 자체인증 공개키는 인증 정보 w_A와 자신의 공개키를 해쉬 함수에 입력하여 나온 출력값 e_A이며, 생성 과정은 다음과 같다.

[단계 1]

사용자 A는 f보다 적은 임의의 수 S_A를 자신의 비밀키로 선택하고 자신의 개인식별정보 ID_A와 공개키 P_A를 다음과 같이 계산하여, 인증기관을 방문하여 공개키 P_A를 전달한다.

$$P_A \equiv b^{S_A} \pmod n$$

사용자의 공개키는 이산 대수 문제에 근거하여 생성하므로 다른 사용자 A의 공개키 P_A와 b를 알아도 S_A를 구하는 것은 매우 어렵다.

[단계 2]

사용자의 공개키 P_A를 받은 인증기관은 사용자 A의 신분을 확인 한 후, 사용자 A의 개인식별정보 ID_A와 공개키 P_A를 이용하여 $(h(ID_A) \oplus h(b^{S_A}) b^{S_A})^{-1} \pmod n$의 잉여류 지수 i_A와 $(h(ID_A) \oplus h(b^{S_A}) b^{S_A} y^{i_A})^{-1} \pmod n$의 γ^d의 근 x_A를 계산한다. 이 때, 정당한 i_A와 x_A값은 n의 소인수 분해를 알아야 구할 수 있으며, 이는 고차잉여류 문제에 기반하고 있으므로, 인증기관만이 값을 구할 수 있다.

인증기관은 다음 수식을 만족하는 인증 정보 w_A $(= (i_A, x_A))$를 계산하여 사용자 A에게 전송한다. 특히 i_A와 x_A는 비밀일 필요가 없다. 즉, 사용자 A의 비밀키는 S_A뿐이다.

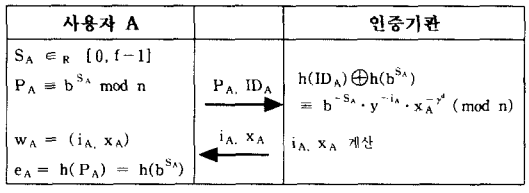
$$h(ID_A) \oplus h(b^{S_A}) \equiv b^{-S_A} \cdot y^{-i_A} \cdot x_A^{-\gamma^d} \pmod n$$

[단계 3] 검증 가능한 자체인증 공개키 생성

사용자 A의 검증 가능한 자체인증 공개키는 (i_A,

x_A)와 e_A이다.

$$e_A = h(P_A) = h(b^{S_A})$$



(그림 2) 고차잉여류에 기반한 검증 가능한 자체인증 공개키 생성

4.4 키 분배 프로토콜

인증기관에 의해서 신분이 확인된 사용자 A(구매자)와 사용자 B(판매자)는 각각 검증 가능한 자체인증 공개키 (i_A, x_A, e_A)와 (i_B, x_B, e_B)를 갖는다. 구매자 A와 판매자 B가 공통키를 분배하고자 할 때의 프로토콜은 다음과 같다.

[단계 1]

구매자 A는 자신의 검증 가능한 자체인증 공개키 (i_A, x_A, e_A)를 판매자 B에게 전송한다.

[단계 2]

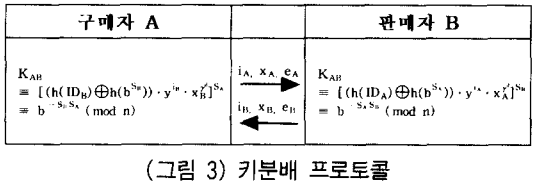
판매자 B도 자신의 검증 가능한 자체인증 공개키 (i_B, x_B, e_B)를 구매자 A에게 전송한다.

[단계 3]

구매자 A와 판매자 B의 공통키 K_{AB}를 다음 식에 의해서 얻는다.(modulus n 상에서)

$$\begin{aligned} K_{AB} &\equiv [(h(ID_A) \oplus h(b^{S_A})) \cdot y^{i_A} \cdot x_A^{\gamma^d}]^{S_B} \pmod n \\ &\equiv [(h(ID_B) \oplus h(b^{S_B})) \cdot y^{i_B} \cdot x_B^{\gamma^d}]^{S_A} \pmod n \\ &\equiv b^{-S_A S_B} \pmod n \end{aligned}$$

생성된 공통키 $b^{-S_A S_B}$는 $g^x \bmod p$와 $g^y \bmod p$가 주어졌을 때 $g^{xy} \bmod p$를 결정하는 Diffie-Hellman



(그림 3) 키분배 프로토콜

의 문제에 근거하고 있으므로, 어떤 공격자도 Diffie-Hellman 문제를 풀 수 없다면 공통키를 구할 수 없다.

4.5 개인식별 프로토콜

전자상거래는 불특정 다수와의 통신이므로 구매자와 판매자 간에 서로의 신분을 확인하고자 할 경우 다음에서 제시된 개인식별 프로토콜을 따라 상대방의 정당성을 확인한다. 판매자가 구매자의 신분을 확인하고자 할 경우 증명자는 구매자가 되며 검증자는 판매자가 된다. 반대의 경우 증명자는 판매자가 되며 검증자는 구매자가 된다.

증명자 A가 검증자 B에게 자신이 A임을 증명하고자 할 때의 프로토콜은 다음과 같다.

[단계 1]

증명자 A는 $[0, f-1]$ 상에서 난수 r을 선택하여, R을 다음과 같이 계산하여 검증자 B에게 전송한다.

$$R \equiv b^r \pmod n$$

[단계 2]

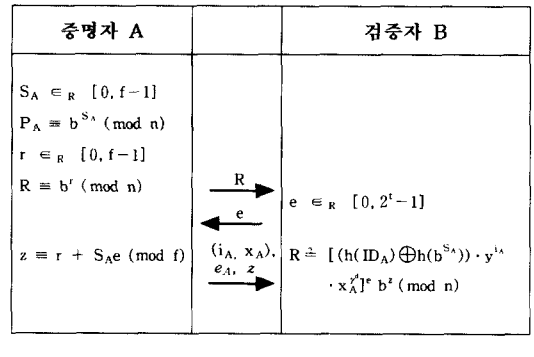
검증자 B는 $[0, 2^t-1]$상에서 난수 e를 선택하여 증명자 A에게 전송한다.

[단계 3]

증명자 A는 $z \equiv r + S_A e \pmod f$를 계산하여, ($i_A$, x_A), e_A, z를 검증자 B에게 전송한다.

[단계 4]

검증자 B는 modulus n상에서 사용자 A로부터 수신한 R이 $[(h(ID_A) \oplus h(b^{S_A}))y^{i_A}x_A^{\gamma^d}]^e b^z$ 인지를 검증한다.



(그림 4) 개인 식별 프로토콜

4.6 디지털 서명 프로토콜

전자상거래에서 다양한 문서들을 교환할 때 메시지(영수증, 계약서 등)의 무결성을 보증하기 위해서 디지털 서명을 사용한다. 다음에 제시된 디지털 서명 프로토콜은 전자상거래에서 교환되는 문서들에 대한 무결성을 보증하며, 서명자 A가 메시지 m에 서명을 하여 검증자 B에게 전달하고자 할 때의 프로토콜은 다음과 같다.

[단계 1]

서명자 A는 $[0, f-1]$상에서 난수 r을 선택하여 R을 계산한다.

$$R \equiv b^r \pmod n$$

[단계 2]

또한 e를 다음과 같이 계산한다.(단 h는 공통의 해쉬 함수이다.)

$$e = h(R \| m)$$

[단계 3]

서명자 A는 $z \equiv r + S_A e \pmod f$를 계산한 후, (i_A, x_A), e_A, e, z를 검증자 B에게 전송한다.

[단계 4]

검증자 B는 $[(h(ID_A) \oplus h(b^{S_A}))y^{i_A}x_A^{\gamma^d}]^e b^z$과 수신한 R이 같은지를 modulus n 상에서 검증한다.

[단계 5]

검증자 B는 $e \stackrel{?}{=} h(R \| m)$인지를 검증한다.

사용자 A		사용자 B
$S_A \in_R [0, f-1]$ $P_A \equiv b^{S_A} \pmod n$ $r \in_R [0, f-1]$ $R \equiv b^r \pmod n$ $e = h(R \| m)$ $z \equiv r + S_A e \pmod f$	(i_A, x_A), e_A, e, z →	$R \equiv [(h(ID_A) \oplus h(b^{S_A})) \cdot y^{i_A} \cdot x_A^{\gamma^d}]^e \cdot b^z \pmod n$ 계산 $e \stackrel{?}{=} h(R \| m)$검증

(그림 5) 디지털 서명 프로토콜

4.7 공개키 검증

Girault의 자체인증 공개키 방식에서는 프로토콜이 실패하는 경우, 프로토콜에서 오류가 발생하였는지 공개키에서 오류가 발생하였는지 정확히 알 수 없다. 그러나, 제안한 키분배, 개인식별, 디지털 서명 프로토콜들은 검증 가능한 자체인증 공개키를 사용하므로, 만일 프로토콜이 실패할 경우, 각 사용자들은 다음과 같이 공개키를 검증함으로써 프로토콜에서 사용되었던 공개키의 정당성을 확인하여, 사용자의 부정을 검출할 수 있다.

$$\widetilde{P_{A(B)}} \equiv [(h(ID_{A(B)}) \oplus h(b^{S_{A(B)}})) \cdot y^{i_{A(B)}} \cdot x_{A(B)}^{\gamma^d}]^{-1} \pmod n$$

$$\equiv \widetilde{b^{S_{A(B)}}} \pmod n$$

$$e_{A(B)} \stackrel{?}{=} h(\widetilde{b^{S_{A(B)}}})$$

즉, 위의 식이 정당하다고 검증되면 프로토콜에 오류가 발생한 것이므로 다시 프로토콜을 실행하고, 만일 식이 정당하지 않으면 사용자가 올바른 공개키를 사용하지 않은 것이다. 이런 공개키 검증을 통해 사용자의 부정 행위를 검출할 수 있으며, 프로토콜에 오류가 발생하였다라는 부인을 방지할 수 있다.

4.8 제안하는 방식의 특징

대칭키 암호 시스템의 키 분배 문제 등을 해결하고자 제시된 공개키 암호 방식은 공개키 디렉토리 관리라는 새로운 문제를 발생시켰다. 공개키 디렉토리 관리 문제를 해결하기 위해서 제안된 방법으로는 개인식별정보에 기반한 방식과 인증서에 기반한 방식이 있다.

인증서에 기반한 방식은 인증기관이 각 사용자의 공개키를 사용자의 개인식별정보와 함께 인증기관의 비밀키로 서명한 인증서를 발행함으로써 각 사용자의 공개키를 인증하는 방식이다. 이 방식은 인증서 검증시 사용되는 추가적인 파라미터를 저장하기 위한 메모리와 전송 정보 및 계산량을 요구한다.

개인식별정보에 기반한 방식은 각 사용자들의 개인식별정보 자체가 공개키이며, 인증기관이 사용자들의 개인식별정보를 이용하여 그에 상응하는 비밀키를 생성하여 스마트 카드에 저장하여 발행한다. 이 방식에서는 비밀키 자체가 공개키 인증서이므로 특별한 인증절차를 요구하지 않지만, 인증기관이 사용자의 비밀키를 생성하므로 인증기관이 임의의 가입자를 위장할 수 있다는 문제점을 갖고 있다.

1991년 Girault는 인증서에 기반한 방식과 개인식별

정보에 기반한 방식의 중간 개념인 자체인증 공개키 방식을 제안하였다. 이 방식은 별도의 인증서를 요구하지 않고 공개키 자체가 인증서의 역할을 하지만, 프로토콜이 실패하는 경우, 프로토콜에서 오류가 발생하였는지 공개키에서 오류가 발생하였는지 정확히 알 수 없다는 단점을 가지고 있다.

본 논문에서 제안한 방식은 자체인증 공개키 방식의 단점을 보완하여 공개키를 검증할 수 있으며, 인증서 없이 자체적으로 공개키를 인증할 수 있다.

〈표 2〉 제안하는 방식과 기존의 방식 비교

	시스템 (생성)	공개키 (생성)	비밀키 (생성)	인증정보 (생성)	자체 인증	공개키 검증
공개키 방식	(S, P)	P : 사용자	S : 사용자	-	-	-
인증서에 기반한 방식	(ID, S, P, W)	I, P : 사용자 W : 인증기관	S : 사용자	(ID, P)에 대한 인증기관의 서명	×	○
개인식별 정보에 기반한 방식	(ID, S) P=ID, W=S	ID	S : 인증기관	인증기관	×	×
자체인증 공개키 방식	(ID, S, P) W=P	ID, P : 인증기관	S : 사용자	인증기관	○	×
제안하는 방식	(ID, S, P)	P : 사용자 W : 인증기관	S : 사용자	인증기관	○	○

※ S : 비밀키, P : 공개키, ID : 개인식별정보, W : 인증 정보

5. 결 론

불특정 다수의 개인이나 기업을 대상으로 하는 인터넷 상의 전자상거래는 개인의 프라이버시 보호, 기업의 비밀 정보 보호와 대금 결제의 신뢰성 보장 등이 무엇보다도 중요하다. 다양한 정보 위협에 대한 대책으로 기밀성, 메시지 인증, 구매자 및 판매자 인증, 송수신 부인 방지 등을 제공하는 인증 서비스가 요구되며, 이는 공개키 암호 방식으로 구현될 수 있다.

그러나 공개키 암호 방식은 공개키 디렉토리 관리 문제를 야기시켰으며, 이를 해결하기 위해 Girault는 공개키 자체가 인증서 역할을 하는 자체인증 공개키 방식을 제안하였다. 인증서에 기반한 방식에서는 공개키가 인증 정보를 알게 된 후에 곧바로 검증될 수 있는 반면, 자체인증 공개키 방식은 메시지 암호화나 서명 검증 또는 키 분배 등에서 공개키가 사용될 때 비로소 검증되므로, 자체인증 공개키를 사용하는 프로토콜이 실패하는 경우, 프로토콜에 오류가 발생하였는지 아니면 공개키에 오류가 발생하였는지를 정확히 알 수 없다는 단점을 가지고 있다.

본 논문에서는 전자상거래를 성립하고자 하는 경우 가격이나 구입 행위를 부인할 수 없도록 상호 신원 확인을 위해서 인증 서비스를 제공하고자 위의 문제를 개선한 검증 가능한 자체인증 공개키 방식을 고차 잉여류 문제에 적용하여 키분배 및 개인 식별 프로토콜, 디지털 서명 프로토콜을 제안하였다. 이 방식은 프로토콜이 실패하면 사용자의 부정 행위가 발생하였는지 프로토콜에 오류가 발생하였는지 알 수 있어 사용자들에게 신뢰감을 줄 수 있다. 제안한 키 분배 프로토콜은 사용자들이 공통키를 분배하고 이를 이용하여 암호통신을 할 수 있도록 하며, 또한 개인식별 프로토콜과 디지털 서명을 이용하여 사용자들의 신분을 확인할 수 있으며, 특히 디지털 서명은 부정한 사용자의 행위에 대한 부인 및 위조를 방지할 수 있다.

제안한 방식의 안전성은 고차잉여류 문제와 이산 대수 문제에 기반을 두고 있으며, 사용자의 개인식별정보와 공개키를 해쉬 함수에 적용하여 인증 정보와 검증 가능한 공개키를 생성하므로 매우 효율적이다.

참 고 문 헌

[1] 이승원, "전자상거래 정책 추진 방향", 정보처리학회지'99, Vol.6. No.1, pp.3-6.

[2] 김홍근, 최영철, "전자상거래 정보보호기술 현황 및 대응 방안", 정보처리학회지99, Vol.6, No.1, 22-34.

[3] Shamir, "Identity-Based Cryptosystems and Signature Schemes", Crypto'84, pp.47-53, 1984.

[4] M. Girault, "Self-certified public keys", Advances in Cryptology EUROCRYPT'91, pp.490-497, 1991.

[5] C. Y. Kwon, D. H. Won, "A study on self-certified public key scheme", The Review of Korea Institute of Information Security & Cryptology, Vol.3, No.3, 1993. 9.

[6] Seung-joo Kim, Soo-hyun Oh, Sang-joon Park and Dong-ho Won, "Verifiable self-certified public keys", Daniel AUGOT and Claude CARLET (Eds.) : Proc. of WCC'99, INRIA Workshop on Coding and Cryptography, pp.139-148, 1999.

[7] Y. Zneng, T. Matsumoto and H. Imai, "Residuosity Problem and its Application to Cryptography", Trans, IEICE, Vol.E71, No.8, pp.759-767, 1988.

[8] S. J. Park, H. K. Yang, D. H. Won, "A class of public key residue cryptosystems", Proc. of CISC'95, Conference on Information Security & Cryptology, Vol.5, No.1, 1995.

[9] S. J. Kim, C. Y. Kwon, S. G. Kang, D. H. Won, "A study on public key authentication schemes", The Review of Korea Institute of Information Security & Cryptology, Vol.6, No.4, 1996.

[10] B. Y. Lee, Y. Y. Choi, M. R. Joo, D. H. Won, "An efficient ID-based authentication scheme based on the γ^{th}-residuosity problem in wireless environment", Journal of the Korea Institute of Information Security and Cryptology, Vol.9, No.2, 1999. 6.

[11] M. R. Joo, B. Y. Lee, H. K Yang, D. H. Won, "Verifiable self-certified schemes based on γ^{th}- residuosity problem", Journal of the Korea Institute of Information Security and Cryptology, Vol.9, No.4, 1999. 12.

주 미 리

e-mail : mrjoo@dosan.skku.ac.kr

1996년 성균관대학교 정보공학과 졸업(학사)

1998년 성균관대학교 정보공학과 석사(공학석사)

1999년~현재 성균관대학교 전기전자 및 컴퓨터공학부 박사과정

관심분야 : 암호이론, 전자상거래보안, 이동통신보안

이 보 영

e-mail : bylee@mail.induk.ac.kr

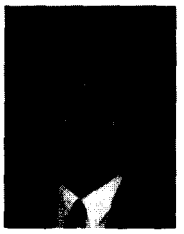
1989년 성균관대학교 정보공학과 졸업(학사)

1995년 성균관대학교 정보공학과 석사(공학석사)

2000년 성균관대학교 전기전자 및 컴퓨터공학부 박사(공학박사)

2000년~현재 인덕대학 정보통신학과 전임강사

관심분야 : 암호이론, 이동통신보안



양 형 규

e-mail : hkyang@kns.kangnam.ac.kr

1983년 성균관대학교 전자공학과 졸업(학사)

1985년 성균관대학교 전자공학과 석사(공학석사)

1994년 성균관대학교 정보공학과 박사(공학박사)

1984년~1990년 삼성전자 컴퓨터부문 선임연구원

1995년~현재 강남대학교 이공대학 전자계산학과전공 조교수

관심분야 : 네트워크 보안, 암호화 프로토콜

원 동 호

e-mail : dhwon@dosan.skku.ac.kr

1976년 성균관대학교 전자공학과 졸업(학사)

1978년 성균관대학교 전자공학과 석사(공학석사)

1988년 성균관대학교 전자공학과 박사(공학박사)

1978년~1980년 한국전자통신연구원 연구원

1985년~1986년 일본 동경공대 객원연구원

1996년~1998년 정보화 추진위원회 자문위원

1982년~현재 성균관대학교 공과대학 전기전자 및 컴퓨터공학부 교수

1999년~현재 한국통신정보보호학회 부회장

1999년~현재 성균관대학교 전기전자 및 컴퓨터공학부 학부장

1999년~현재 성균관대학교 정보통신대학원 원장

관심분야 : 암호이론, 정보이론