GDHP 은닉서명기법을 이용한 전자지불 프로토콜

Electronic Payment Protocol using GDHP Blind Signature Scheme

이현주, 이충세
충북대학교 전기전자컴퓨터공학부

Hyun-Ju Lee(hjlee86@chungbuk.ac.kr), Chung-Sei Rhee(csrhee@chungbuk.ac.kr)

요약

본 논문에서는 유/무선 통합 환경에서 전자상거래를 활성화시키기 위한 지불 수단으로 GDHP 은닉서명 기법을 이용한 전자지불 프로토콜을 제안한다. GDHP 기반의 타원곡선 알고리즘을 적용하여 통신횟수, 계산량 측면에서 기존의 은닉서명 방식의 효율성을 개선하였다. 또한, 기존의 PayWord 프로토콜에서 사용한 인증서 대신 유한체

Abstract

In this paper, we propose electronic payment protocol using GDHP blind signature scheme to activate e-business in the wire/wireless integrated environment. The protocol applied elliptic curve algorithm on the GDHP base and improved the efficiency of the existing blind signature technique on the basis of communication frequency and calculation number. And the protocol accelerated speed and strengthened safety against man-in-the-middle attacks and forward secrecy because the certification between individuals is performed by the session key created by Weil paring using elliptic curve cryptosystem in the limited entity

Ⅰ. 서 론

유/무선 통합 서비스 환경에서의 전자지불과정 컨텐츠의 복제와 무단 배포 방지를 위한 자료의 암호화뿐만 아니라, 개인의 프라이버시를 보호할 수 있는 환경이 구축되어야 한다. 최근 무선인터넷이 급성장하면서 멀티미디어 다운로드, 인터넷 뱅킹, 증권거래에서 전자상거래까지 다양한 서비스가 제공되고 있다[1]. 그러나 이 서비스들 중에서 인터넷 뱅킹이나 전자상거래의 경우는 사용자의 비밀정보가 교환되는 민감한 서비스이므로 비밀정보들을 안전하게 전송하기 위한 보안 기술이 필수적이다. 무선환경에서 전자상거래의 보안 요구사항으로는 효율적인 무선인터넷 암호화 기술이 필요하다. 무선환경과 무선 단말기가 갖는 저장 공간 및 대역폭의 특성상 현재 인터넷에서 사용되고 있는 보안 기술을 그

* 본 연구는 2005년도 충북대학교 학술연구지원 사업의 연구비 지원에 의해 연구되었습니다.

접수번호 : #080907-003
접수일자 : 2008년 09월 07일
심사완료일 : 2008년 12월 12일
교신저자 : 이충세, e-mail : csrhee@chungbuk.ac.kr

대로 무선인터넷에 적용하는 것은 부적절하다. 그러므로 효율적이면서도 안전성의 유선을 그대로 유지될 수 있는 보안 기술 방안이 필요하다.

기존 PayWord 프로토콜은

이산대수문제(DLP: Discrete Logarithm Problem)의 어려움에 두고 있는 이 서명 방식은 T.Okamoto에 의해 제안되었다[5]. 키 설정과정, 서명 생성과정, 서명 검증과정은 다음과 같다.

① 키 설정

서명자

람의 공개키는 사전에 이메일 주소와 같은 정보에 의해 결정된다. 1984년 Shamir에 의해 제안된 이 개념은 원래 e-mail 시스템에서 인증 관리를 단순화 하기 위한 것이었다[9]. Alice가 Bob에게 bob@hotmail.com으로 메일을 보낼 때 공개키 스트링 bob@hotmail.com을 사용하여 메시지를 암호화한다. Alice는 Bob의 공개키 인증서를 획득할 필요가 없다. Bob은 메시지를 복호화하기 위해 KGC(Key Generation Center)에게 자신을 인증한 후 자신의 개인키를 얻는다. 기존의 e-mail 구조와 달리, Alice는 Bob이 사전에 공개키 인증을 설정하지 않아도 암호화된 메일을 보낼 수 있다. ID-based 시스템에서는 신뢰할 수 있는 KGC가 필요하다. KGC에서는 각 개체의 ID 기반 공개키를 사용하여 개인키를 생성한다. Weil pairing은 타원곡선 이산대수 문제의 공격에 사용되어왔으며 3자 키 공유 시스템의 구성도 가능하다[10]. 최근 D.Boneh와 D.Franklin은 Weil-pairing을 이용한 타원곡선에 bilinear 함수를 적용한 새로운 ID 기반의 암호 방식을 제안하였다[10]. Weil pairing은 초특이 타원곡선 상에서 정의되는 쌍선형사상(bilinear map)이다.

을 생성, 검증하는데 걸리는 시간을 감소시킨다. 또한 서명의뢰자와 서명자간의 통신량과 통신횟수의 감소로 효율성을 높였다. [표 2]에서 M은 모듈라 곱셈에 대한 계산량, E는 모듈라 지수승에 대한 계산량, I는 모듈라 역원에 대한 계산량, H는 해쉬함수의 계산량, A는 타원곡선위에서 Weil-pairing에 대한 계산량을 의미한다.

Chaum서명생성 과정에서의 통신횟수는 가

ID기반 전자지불 프로토콜을 제안하였다. 제안한 기법은 타원곡선상에서 연산이 이루어지기 때문에 연산속도, 계산량, 키의 길이 등을 줄인 효율적인 프로토콜이다. 또한, 제안한 프로토콜은 ID기반 공개키암호 시스템의 적용으로 효율성 및 세션키의 분실이나 오용등에 의해 발생하는 문제점을 해결할 수 있다. 향후 모바일 단말기를 통해 지급 결제를 하는 M-Payment는 다양한 장점을 보유하고 있어 차세대 지불 수단으로 주목 받고 있다. 의료카드, SIM카드, 신분증 등에 사용되는 스마크카드는 복제가 불가능하기 때문에 높은 보안성을 제공한다. 여기에 ID기반 타원곡선 알고리즘을 적용한다면 보안성 및 속도 향상측면에서 효율성을 높일 수 있을 것이다.

참 고 문 헌

[1] K. Lyytinen, "M-commerce - mobile commerce: a new frontier for E-business," System Sciences, Proceedings of the 34th Annual Hawaii International Conference on, pp.3509-3509, 2001.

[2] M. H. Lee and K. G. Kim, "A Micro-payment System for Multiple-Shopping," SCIS 2002, Vol.1, No.2, pp.229-234, Jan/Feb. 2002.

[3] D. Chaum, "Blind Signature for Untraceable Payments," Advances in Cryptology-Proceeding of Crypto '82, Springer-Verlag, pp.199-204, 1982.

[4] R. L. Riverst, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystem," Commun. ACM, Vol. 21, pp.120-126, 1978.

[5] T. Okamoto, "Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes," Advances in Cryptology -Proceeding of Crypto'92, Springer-Verlag, pp.31-53, 1993.

[6] C. P. Schnorr, "Efficient Signature Generation by Smart Cards," Journal of Cryptology, Vol.4, No.3, pp.161-174, 1991.

[7] R. L. Rivest, "PayWord and MicroMint: Two simple micropayment schemes," CryptoBytes, pp.7-11, 1996.

[8] R. Rivest, *The MD5 Message-Digest Algorithm*, Internet RFC 1321, Apr. 1992.

[9] D. Nalla and K. C. Reddy, *ID-based tripartite Authenticated Key Agreement Protocols from pairings*, Cryptology ePring Archive, Report 2003/004, 2002.

[10] N. P. Smart, *An Identity based authenticated Key Agreement Protocol based on the Weil pairing*, Cryptology ePrint Archive, Report 2001/111, 2001.

저 자 소 개

이 현 주(Hyun-Ju Lee) 정회원

- 2000년 8월 : 청주대학교 대학원 수학과 (이학박사)
- 2004년 8월 : 충북대학교 대학원 전기전자컴퓨터공학부 (이학박사)
- 2006년 3월 ~ 현재 : 충북대학교 전기전자컴퓨터공학부 초빙교수

<관심분야> : 정보보호, 알고리즘, M-Commerce

이 충 세(Chung-Sei Rhee) 정회원

- 1989년 : University of South Carolina, 전산학 (박사)
- University of North Dakota 전산학과 (조교수)
- 1991년 ~ 현재 : 충북대학교 전기전자 및 컴퓨터공학부 교수

<관심분야> : 결함허용, 알고리즘 및 전문가 시스템, 정보보안