무선인터넷에서 신용카드기반의 안전한 소액 지불 프로토콜

김 석 매*, 김 장 환**, 이 충 세***

A Secure Micro-Payment Protocol based on Credit Card in Wireless Internet

Jin Shi Mei*, Jang-Hwan Kim**, ChungSei Rhee

요 약

최근 정보통신기술의 급속한 발달로 무선인터넷을 이용한 전자상거래 사용자가 폭발적으로 증가하고 유선에서 유/무선 통합 환경으로 변화함에 따라 보안상의 많은 문제점이 제시되고 있다. 특히 무선전자상거래에서는 무선 환경의 제한적 특징에 따라 경량화된 보안기술, 종단간 보안 기술 및 프라이버시 보안 등에 관한 연구가 활발하게 진행되고 있다. 현재 무선 전자상거래에서는 주로 신용카드기반의 지불 프로토콜인 WPP와 ASPeCT에서 제안한 인증과 지불초기화를 위한 AIP프로토콜을 사용하고 있다. WPP에서 사용하는 보안 프로토콜 WAP는 무선과 유선을 연계하는 G/W에서 전달되는 데이터의 모든 내용이 누출되는 보안상의 취약점이 있어 종단간 보안도 제공하지 못하는 단점이 있고, AIP 프로토콜은 인증서 체인을 이용하여 인증을 수행하므로 계산량이 많은 단점과 인증서에서 사용자의 신원이 노출되어 프라이버시 보호를 위한 익명성이 보장되지 않는 단점이 있다. 이 논문에서는 기존 AIP프로토콜을 기반으로 초특이 타원곡선인 Weil Pairing을 적용한 ID 기반 공개키 암호기법을 사용하여 거래정보의 기밀성을 보장하고 은닉전자서명 기법을 통한 인증서를 사용하여 프라이버시 보호, 공개키와 사용자 인증 및 부인방지를 해결했으며 또한 두 객체만 공유하는 세션키를 사용하여 종 단간 보안이 제공되는 특정 무선 플랫폼에 독립적이며 안전하고 효율적인 지불 프로토콜을 제안하였다. 또한 제안한 프로토콜은 사용자와 서비스 제공자간의 온라인 인증기관이 지불 프로토콜의 인증과정에 참여함으로써 다른 도메인에 존재하는 서비스 제공자에게도 효율적이고 안전한 서비스를 받을 수 있도록 하였다.

Key Words : 모바일, ID 기반 공개키 암호기법, 전자 지불, 종단간 보안, 인증서

ABSTRACT

Recently, there are rapid developement of information and communication and rapid growth of e-business users. Therefore we try to solve security problem on the internet environment which charges from wire internet to wireless internet or wire/wireless internet. Since the wireless mobile environment is limited, researches such as small size, end-to-end and privacy security are performed by many people.

Wireless e-business adopts credit card WPP protocol and AIP protocol proposed by ASPeCT. WAP, one of the protocol used by WPP has weakness of leaking out information from WG which conned wire and wireless communication. certification chain based AIP protocol requires a lot of computation time and user IDs are known to others.

We propose a Micro-Payment protocol based on credit card. Our protocol use the encryption techniques of the public key with ID to ensure the secret of transaction in the step of session key generation. IDs are generated using ECC based Weil Paring. We also use the certification with hidden electronic sign to transmit the payment result. The proposed protocol solves the privacy protection and Non-repudiation problem.

We solve not only the safety and efficiency problem but also independent of specific wireless platform. The protocol requires the certification organization attent the certification process of payment. Therefore, other domain provide also receive an efficient and safe service.

Keywords: mobile, ID based Public Key Cryptosystem, electronic payment, end-to-end security, certificate

* 충북대학교 컴퓨터과학과 박사과정 ** 대덕대 IT계열 교수 *** 컴퓨터과학과 교수

논문번호 : #KICS2004-10-214 접수일자 : 2004년 10월 5일

※ 이 논문은 2004년도 충북대학교 학술 지원 사업의 연구비와 충북대학교 유비쿼터스 바이오 정보기술 연구 센터의 지원을 받았음.

Ⅰ. 서 론

정보통신기술의 발전과 초고속 인터넷의 폭발적인 이용으로 전자상거래를 기반으로 한 디지털 경제는 사회의 전반에서 새로운 패러다임으로 작용하면서 일대 혁신과 변화를 가져오고 있다. 급격히 늘어나고 있는 인터넷 사용자를 기반으로 하여 전자상거래는 점차 활성화되고 있으며, 상품의 판매나 그 대금의 지불, 기업 및 제품 광고, 신문과 잡지 기사 등 정보 제공서비스, 홈뱅킹/펌뱅킹을 비롯한 금융 거래나 주식 매매, 보험 서비스 등 그 영역이 넓혀지고 있다. 특히 무선의 이동성과 편리성이 상거래와 결합된 무선 전자상거래는 산업이용과 시장규모 측면에서 무선 인터넷의 중추가 되어 핵심 산업으로 부가되고 있다.

1.1 연구 배경

최근 정보통신기술의 급속한 발달로 무선인터넷을 이용한 전자상거래 사용자가 폭발적으로 증가되고 있다. 유선에서 유/무선 통합 환경으로 변화함에 따라 보안상의 많은 문제점이 제시되고 있다. 무선 환경에서의 전자상거래는 많은 편리함을 제공하지만 무선이 원래 신뢰도가 떨어지는 매체이기 때문에 새로운 문제들이 발생되고 있다. 이와 같은 문제점들 가운데 주로 다음과 같은 사항들이 논의의 쟁점으로 되고 있다.

첫째: 효율적인 무선인터넷 암호화기술이 필요하다.

저장 공간 및 대역폭에 제한을 갖는 무선인터넷 환경과 무선 단말기가 갖는 제한, 및 무선인터넷의 고유특성을 고려할 때, 현재 인터넷에서 사용되고 있는 보안기술을 그대로 무선인터넷에 적용할 경우 유선에서와 같은 성능을 기대하기 어렵다. 이에 따라 보다 간단하고 효율적이면서도 안전성이 유선의 그대로 유지되는 보안기술 방안을 강구할 필요가 있다. 또한 기존의 소프트웨어를 통한 보안 서비스의 한계점을 암호 알고리즘을 하드웨어적으로 구현하여 단말기에 장착함으로써 해결이 가능하다.

둘째: 종 단간(End to End) 보안 제공 방안이 필요하다.

무선인터넷과 기존 유선인터넷과의 연동이 불가피한 상황에서 무선인터넷 상의 단말기에서부터 유선인터넷 상의 서버에 이르는 종 단간 보안 서비스 제공은 계속해서 문제가 되고 있다. 특히 WAP(Wireless Application Protocol)과 같이 무선인터넷에서 별도의 프로토콜을 사용하는 경우 이 문제는 더욱 심각하다. 이의 해결을 위해서 양 구간 모두에서 같은 프로토콜 HTTP/SSL 또는 WAP/WTLS(Wireless Transport Layer Security)를 통해 보안 서비스를 제공하는 방법들이 연구되고 있지만 아직까지 미비한 것이 사실이며 이에 대한 지속적인 연구가 필요하다.

현재 유선환경에서의 상거래에서는 주로 신용카드 기반의 SET(Secure Electronic Transaction) 또는 안전한 채널을 제공하는 TLS(Transport Layer Security)를 이용한 보안 프로토콜이 사용되고 있다. 그러나 이런 보안 프로토콜은 저장 공간, 계산량 및 통신량의 제약성으로 무선 환경 사용에 직접 적용하기에는 적합하지 않다. 무선인터넷에서는 보다 간단하고 효율적이며 또 종단 간 안전성도 보장되는 보안 프로토콜이 필요하다. 현재 주로 신용카드기반의 지불 프로토콜 WPP(Wireless Payment Protocol)와 ASPeCT(Advanced Security for Personal Communications Telecommunications System)에서 제안한 인증과 지불을 위한 AIP(Authentication and Initialization of Payment)프로토콜을 사용하고 있다 [1, 7, 9].

1.2 연구 내용 및 구성

이 논문에서는 기존 무선 환경 전자상거래에서 사용되는 안전한 지불을 위한 보안 프로토콜인 WPP프로토콜과 AIP프로토콜에 대한 안전성과 효율성을 분석하여 기존 WPP프로토콜의 보안상 문제점과 AIP프로토콜의 효율상 문제점을 도출하고, 해결책으로 초 특이 타원곡선 Weil Pairing을 이용한 ID 기반 공개키 암호 기법을 제시하고 이를 적용한 종 단간 보안이 제공되는 안전하고 효율적이며 무선 환경에 적합한 새로운 지불 프로토콜을 제안한다. 또한 온라인 인증기관이 참여하는 경우에 기존 프로토콜과 제안프로토콜에 대한 비교분석을 통하여 제안 프로토콜의 안전성 및 효율성을 입증한다.

이 연구에서는 전자상거래에서의 보안 요구사항 정리하고 이를 기반으로 기존 전자상거래에서 사용되고 있는 지불 프로토콜, 특히 무선 환경에서의 지불프로토콜에 대한 안전성과 성능을 철저하게 분석하여 기존 지불프로토콜의 문제점을 도출하고 이 문제해결을 위한 효율적인 암호알고리즘을 선정하여 이를 적용한 간단하고 편리하며 안전한 지불프로토콜을 제시한다. 또한 제안 지불프로토콜 대한 안전성과 성능에 대한 평가를 통하여 제안 프로토콜의 가치를 분석한다.

Ⅱ. 관련 연구

이 장에서는 전자상거래에서의 보안의 필요성과 보안대책의 기본 요구사항에 대해 기술한다. 그리고 유선환경에서 유/무선 통합 환경으로의 진화에 따른 유/무선 보안기술에 대하여 기술하고 기존 지불을 위한 프로토콜에 대한 분석을 통하여 그들의 보안상 문제점을 기술한다.

2.1 전자상거래 보안의 개요

인터넷에서는 안전한 전자상거래를 위한 다양한 보안 서비스들이 등장하고 있으나 대부분이 기밀성, 메시지 인증, 구매자 및 판매자 인증, 송수신 부인방지, 재 전송 방지 등과 같이 사용자나 거래정보 위협에 대한 대책 수립이 완전하지 않다. 이와 같이, 전자상거래 등의 응용서비스를 안전하게 제공하기 위해서 정보보호 서비스 요구 수준을 유지하면서 사용자에게 신뢰성을 보장해 주는 정보보호 기술이 필요하다.

이러한 문제는 상거래 관련 데이터를 암호화하고 제3자가 그 데이터를 도청하더라도 그 내용을 판별할 수 없도록 함으로써 기술적으로 해결하는 것이 가능하다. 또한 전자상거래에서는 일반적인 상거래와는 달리 직접 대면하지 않고 이루어지므로 다음과 같은 보안이 요구된다[22, 18].

① 사용자 인증: 거래 상대에 대한 신원에 대한 상호 확인 할 수 있어야 한다.
② 메시지 기밀성: 신용정보, 거래정보 등 메시지가 제3자에게 노출됨을 방지해야 한다.
③ 메시지 무결성: 제3자에 의한 거래정보의 위/변조를 방지해야 한다.
④ 부인방지: 거래상대의 거래정보에 대한 부인을 방지해야 한다.
⑤ 추적불가: 특별기관(사법기관)외에 합법적인 사용자의 거래정보에 대한 추적이 불가능해야 한다.
⑥ 익명성: 사용자의 프라이버시 보호를 위한 익명성을 보장해야 한다.

2.2 유선 및 무선 인터넷 보안

2.2.1 유선인터넷 보안

[그림2.1]에서 보는 바와 같이 유선인터넷에서 보안은 현재 표준으로 자리 잡은 TLS 프로토콜을 사용하여 이루어진다. 공개키와 개인키를 이용한 키 교환

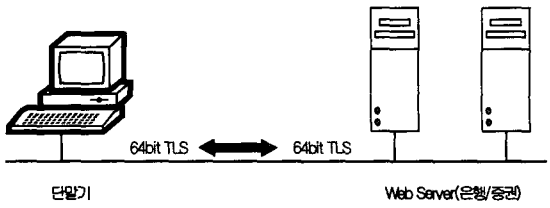


그림 2.1. 유선환경에서의 TLS프로토콜

(Key Exchange)기법을 이용하여 클라이언트와 서버가 공유하는 세션키(Session key)를 안전하게 생성한 다음 이 세션키를 이용하여 클라이언트와 서버사이의 모든 전송 데이터를 암호화/복호화 한다. TLS에서 사용자와 서버 양쪽을 연결해주는 유선인터넷은 다음의 보안요소 들을 충족시킨다. 우선, 로그인 과정을 통해 사용자의 당사자 여부를 판단하는 인증이 보장 받게 되며, 세션키를 알지 못하는 제 3자는 클라이언트와 서버에서 암호화된 데이터의 내용을 알 수 없으므로 기밀성이 보장된다. 클라이언트에서 암호화된 데이터는 서버에 도착하는 동안 누군가에 의해 가로채어 질 수 있지만 데이터를 임의로 변화시키게 되면 데이터의 해쉬(Hash)값이 변하게 되므로 무결성이 보장된다. 인증을 받은 특정 사용자에 대해 적절한 권한 부여를 하여 인증을 최종적으로 수행한다[5].

2.2.2 무선인터넷 보안

일반적으로 인터넷에서의 보안 기술은 네트워크상의 도청, 메시지 변조, 신분 위장 등의 공격에 대해 기밀성, 사용자 인증, 데이터 무결성, 부인 방지 등의 정보보호 서비스를 제공한다. 현재 이와 같은 정보보호 서비스를 제공하기 위한 보안 메커니즘들은 대부분 공개키 암호방식을 비롯한 암호 기술에 기반을 두고 있다. [표 2.1]에서는 현재 주로 사용되고 있는 무선인터넷에서의 솔루션들을 보여준다. 무선인터넷 기술이 WAP과 같은 별도의 프로토콜을 기반으로 하

표 2.1. 무선 인터넷 솔루션

구 분	WAP	STINGER	i-MODE
개발주도업체	WAP forum (Nokia, Phone.com, Ericsson등)	마이크로소프트 +퀄컴	NTTDocomo
컨텐츠 기술언어	WML/WML scrip	m-HTML	C-HTML
전송프로토콜	WSP/WTP/WDP	HTTP	HTTP
단말기 브라우저	WAP 브라우저	Mobile Explorer	Compact NetFront
보안메커니즘	WTLS	mSSL	SSL

는 솔루션과 기존의 TCP/IP를 기반으로 하는 솔루션으로 나누어짐에 따라 무선인터넷에서 보안기술 역시 크게 2가지로 구분할 수 있다.

WAP에서의 보안 프로토콜인 WTLS는 SSL을 모델로 만들어지기 때문에 그 구조에는 큰 차이가 없다. 차이점은 WTLS에서 메시지 크기를 조금씩 줄인 것과 ECC 알고리즘의 수용, 작은 크기의 인증서 지원 등이다. 이 중 인증서는 기존의 표준인 X.509 인증서를 지원하며 추가로 WTLS 인증서, X9.68 인증서 형식을 지원한다. WTLS 인증서는 컴팩트한 사이즈의 인증서 형식으로 정의한 것으로 X.500 DN 대신 Identifier만을 사용함으로써 크기를 줄이고 있다. X9.69 인증서는 아직 표준으로 정의되지는 않았으나 WTLS 인증서와 비슷한 개념으로 작은 크기의 인증서 형식으로 정의되고 있다[5].

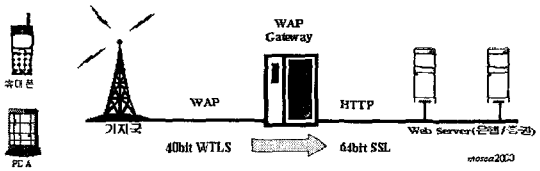


그림 2.3. WAP에서 WTLS-SSL프로토콜

무선인터넷에서의 보안은 위 [그림 2.3]에서 보는 바와 같은 구조를 갖는다. 무선구간에서는 WTLS를 이용하고 유선구간에서는 기존 유선인터넷의 TLS/SSL를 그대로 적용하여 유선, 무선 각각에서 보안을 달성할 수 있도록 구성되어 있다. 하지만, 무선인터넷 보안에서의 문제점은 유무선 각 구간별 보안에서 발생하는 것이 아니라, 안전한 유무선 구간 쌍방을 연결하는 WAP GW 에서 발생하게 된다[5, 7].

2.3 전자지불을 위한 보안 프로토콜

2.3.1 SET 프로토콜

SET은 세계의 2대 신용카드 회사인 MasterCard, VISA 및 통신, 컴퓨터, 소프트웨어 관련 기업인 GTE, IBM, Microsoft, Netscape Communication, SAIC, Terisa Systems, Versign 등 7개 컴퓨터 및 보안 업체가 공동제안하고, RSA Data Security사의 암호기술을 베이스로 한 신용카드 기반 지불 프로토콜

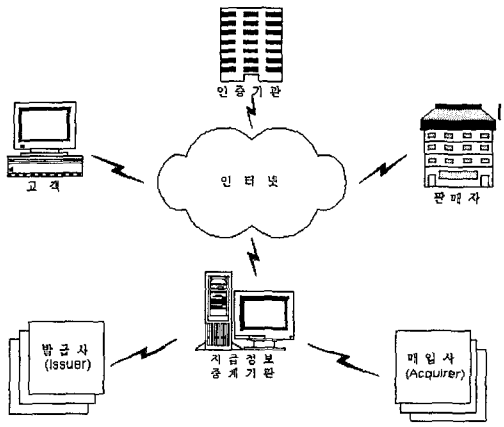
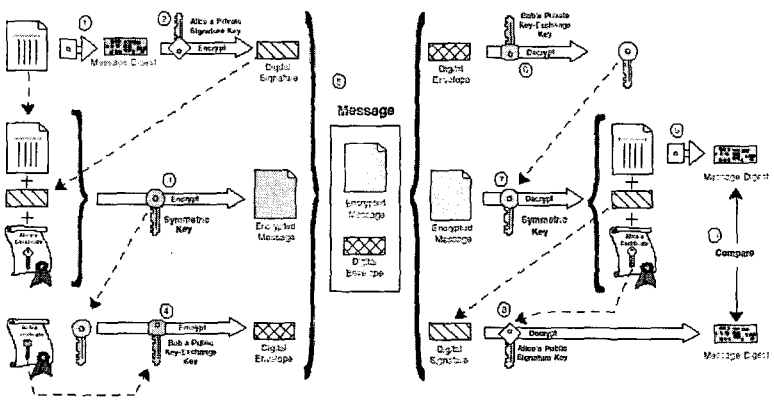


그림 2.4. SET을 이용한 전자지불 시스템 구성

이다.

[그림 2.4]에서 판매자는 카드번호 등의 결제정보를 고객으로부터 받아 그 정보를 금융 기관에 넘긴다. 그러나 카드번호 등은 금융 기관만이 볼 수 있도록 암호화되어져 있다. 이와 같이 고객, 판매자, 금융기관의 3자간에 걸친 정보의 주고받음에 있어서 보안제어는 OSI 7계층의 응용계층에서 실시하고 있다. 고



2.5. SET프로토콜에서의 암호화 과정

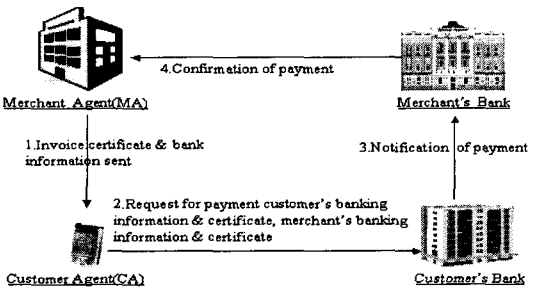


그림 2.6. WPP의 구성도 및 지불 흐름도

객, 판매자, 금융기관은 전자결제를 실시하기 전에 각각 인증기관(CA: Certification Authority)으로부터 인증서(Certificate)의 발행을 받을 필요가 있다. 그 다음 고객, 판매자, 금융 기관 사이에서 인터넷 등의 개방형 정보 네트워크를 통해 인증서를 교환하면서 신용카드 결제를 실시하게 된다.

[그림 2.5]은 SET에서의 기본적인 암호화 과정을 보이고 있다. Alice가 Bob에게 어떤 문서에 서명을 한 다음 암호화하여 전송하는 가상적인 시나리오를 보이고 있다. SET 프로토콜은 메시지의 암호화, 개인을 인증(Authentication) 할 수 있는 전자증명서, 그리고 디지털 서명(Digital Signature) 등을 통해 안전한 거래가 이루어지도록 하고 있다[21].

2.3.2 WPP 프로토콜

WPP 프로토콜은 SET을 기초하여 무선 인터넷에서 신용카드 지불을 할 수 있도록 제안된 지불 프로토콜이다. WPP는 사용자와 사용자의 은행(신용 카드사), 서비스제공자(상점),서비스 제공자의 은행으로 구성되

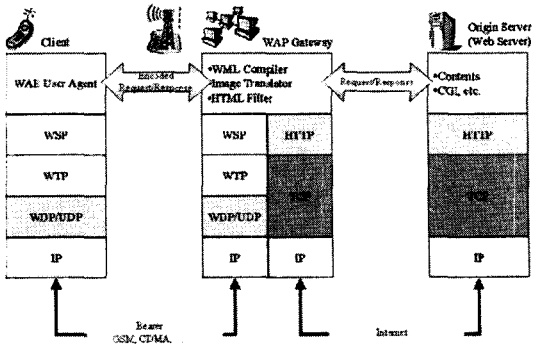


그림 2.7. WTLS-SSL프로토콜 변환

며 사용자와 은행, 서비스제공자를 연결해주는 WG(WAP Gateway)가 필요하다. [그림 2.6]는 WPP의 구성도 및 지불 흐름도를 나타낸 것으로써 WAP 프로토콜 스택을 인터넷 프로토콜로 변환하는 WG를 생략하였다.

WPP는 신용카드 정보를 보호하기 위해서 스마트카드 기술과 WAP의 WTLS를 사용하였다. WAP에서는 소형 이동 단말기에 적합하도록 XML을 기반으로 작성된 문서 작성 언어인 WML을 이용해 컨텐츠를 기술하며, 인터넷의 HTTP, TCP/IP에 해당하는 WSP/WTP/WDP 등의 프로토콜 스택을 정의하였다. [그림 2.7]에서 보는 바와 같이 WG에서는 WTLS-SSL프로토콜 변환 시 암호화된 메시지가 복호화되어 원본 메시지가 노출될 위험성을 가지고 있어 종 단간 보안을 제공하지 못한다는 단점을 가지고 있

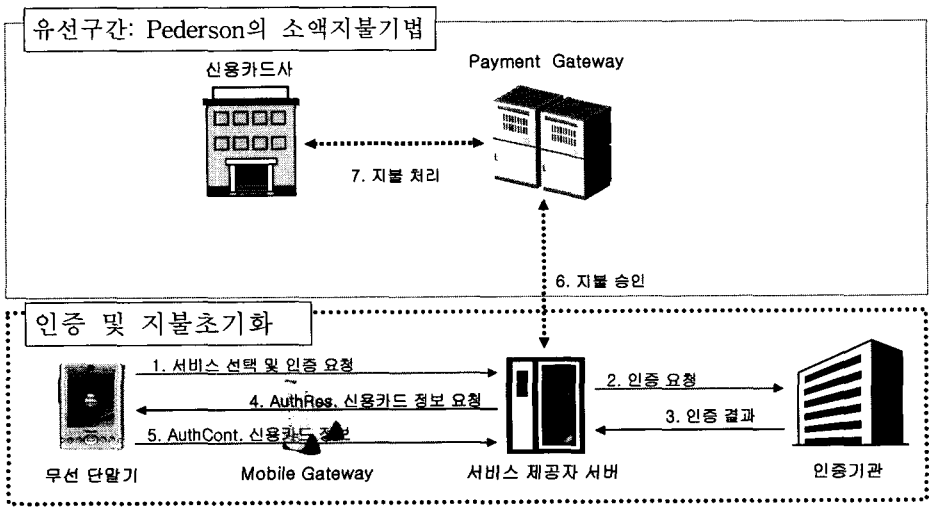


그림 2.8. AIP프로토콜 기반 지불 시스템 구성도

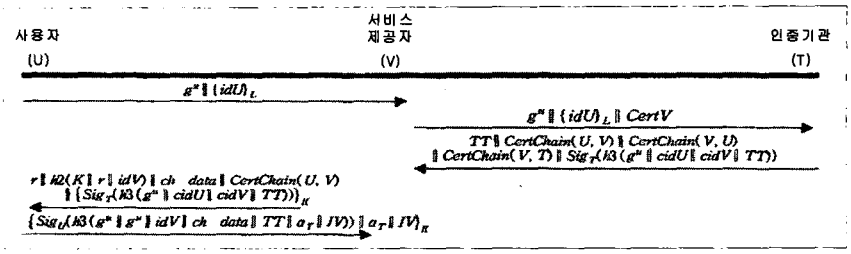


그림 2.9. 온라인 인증기관 참여하는 AIP프로토콜

다. [17, 7, 8].

2.3.3 AIP 프로토콜

AIP프로토콜은 무선 환경에서 UMTS에서의 사용자와 서비스제공자간의 인증과 지불을 위하여 ASPeCT에서 최초로 제안하였다[9]. AIP프로토콜은 인증 단계와 지불초기화 단계 두 개 단계로 구분한다. 인증단계에서는 먼저 사용자, 서비스제공자 및 지불게이트웨이들 간의 상호 인증을 수행하고 지불초기화 단계에서는 거래정보교환을 위한 세션키를 생성하고 지불초기화 정보를 교환한다. 지불수행은 Pederson의 소액 지불 기법을 이용하여 지불을 수행하게 된다.

AIP프로토콜은 온라인 인증기관이 참여여부에 따라 두 가지로 구분된다. [그림 2.8]은 기존 인증기관이 참여한 AIP프로토콜 사용을 위한 시스템 구성도 및 데이터 흐름을 보여준다. 여기서 사용자는 서비스 제공자와 Diffie-Hellman 키 설정 기법을 사용하여 세션키를 생성하고 사용자와 인증기관은 Elgamal기법을 사용하여 세션키를 만든다. 생성된 세션키로 인증과정을 거치고 지불을 위한 초기화 정보를 교환한다[6, 10].

AIP 프로토콜은 유한체(finite field)의 곱셈군(multiplicative group) 또는 타원 곡선의 부분군(subgroup)과 같은 유한군 G와 생성원 g에서 이산대수 문제(discrete logarithm problem)에 기반하고 있다. 온라인 인증기관이 참여하는 AIP프로토콜 구조는 [그림 2.9] 에서 보는 바와 같이 U는 사용자, V는 상점/서비스 제공자, T는 온라인 인증기관을 의미한다. U는 V와 Diffie-Hellman 키 설정 방식에 의하여 세션키를 생성하고 U와 T는 ELGamal 방식에 의하여 세션키를 만들어 낸다. $CertChain(X, Y)$는 X가 Y의 인증서를 검증할 수 있도록 생성된 인증서 체인을 나타낸다. 메시지 M을 세션키 K로 암호화한 경우는 $\{M\}_K$와 같이 표기 한다. U와 T의 서명은 각각 Sig_U와 Sig_T와 같이 나타낸다. T의 타임스탬프는 TT로 표기한다. U와 V의 신원은 각각 idU와 idV로 표기한다. $h1, h2, h3$는 충돌회피 해쉬 함수이다[11, 9].

① 프로토콜이 시작되면 U는 난수 u를 생성하고 키 설정용 공개키 g^u를 계산해낸다. 그리고 T의 공개키 g^t를 이용하여 세션키 $L = g^{tu}$를 생성한다. U는 공개키 g^u와 자신의 신원 idU를 생성한 세션키 L로 암호화 하여 V에게 보낸다.

② V는 U로부터 메시지를 받아 자신의 인증서 $CertV$와 같이 온라인 인증기관인 T에게 전송한다.

③ T는 V로부터 받은 메시지에서 $CertV$를 이용하여 U가 V의 공개키를 검증할 수 있도록 $CertChain(U, V)$를 생성하고 V가 U와 TTP의 인증서를 검증할 수 있도록 각각 $CertChain(U, V)$와 $CertChain(V, T)$를 생성해서 V에게 전송한다.

④ V는 $CertChain(U, V)$를 통하여 U의 키 설정용 공개키를 얻어서 U와의 세션키 $K = h(g^{uv} \mid r)$을 생성한다. 그리고 $CertChain(V, T)$를 이용하여 T의 서명을 검증할 수 있는 공개키를 얻게 되면 T로부터 받은 g^u,$cidU$,$cidV$, TT에 대한 서명을 U에게 전달해 주게 된다.

⑤ U는 $CertChain(U, V)$를 이용해서 V의 인증서를 검증할 수 있으며 V와 동일한 세션키 $K = h(g^{uv} \mid r)$을 생성한다. 그리고 U는 지불에 관련된 ch_data, a_T, 그리고 지불 초기

화 벡터 IV를 공개키 g^u와 g^v와 같이 서명을 하여서 V에게 전송한다.

⑥ 마지막으로 V는 U로부터의 서명을 검증하고 지불에 관련된 파라미터들을 전송 받게 된다. 검증에 성공하게 되면 V는 U에게 서비스를 제공하기 시작한다.

AIP프로토콜에서 종단간 보안을 제공하려면 다음과 같은 요구 조건을 만족 시켜야 한다[11, 9].

① 사용자와 서비스제공자간의 명확한 상호 인증;
② 사용자와 서비스제공자간의 함축적 키 인증을 통한 세션키 생성;
③ 서비스제공자에게 전송되는 사용자 데이터의 부인 방지;
④ 사용자와 서비스제공자가 인터페이스에서의 사용자 신원의 기밀성.

AIP프로토콜에서 온라인 인증기관이 참여하지 않는 프로토콜은 사용자와 서비스 제공자간에 이루어지는 것으로 프로토콜이 간단한 장점이 있지만 사용자의 인증서 취소 여부를 파악할 수 없어 서비스 제공자는 제공한 서비스에 대해 사용자가 지불을 완료할 것인지에 대한 검증을 할 수가 없는 단점이 있다. 온라인 인증기관을 이용한 AIP 프로토콜에서 서비스 제공자는 온라인 인증기관과 프로토콜 수행을 통해 사용자의 인증서의 취소 여부를 파악함으로써 제공한 서비스에 대한 지불 가능 여부를 검사할 수 있다. 그러나 온라인 TTP와의 원거리 통신에서 인증서 체인(certificate chain)을 이용하여 검증을 수행하므로 계산량이 많아지게 된다. 또한 AIP프로토콜은 사용자의 인증서가 서비스 제공자에게 전달이 되므로 사용자의 신원이 서비스 제공자에게 노출되어 프라이버시보호를 위한 익명성이 보장되지 않는 단점이 있다.

2.4 Weil-pairing을 적용한 ID기반 공개키 암호기술

이 절에서는 GDHP와 초특이 타원곡선 Weil-pairing 및 Weil-pairing을 적용한 ID기반 공개키 암호기술에 대해 기술한다.

2.4.1 GDHP와 Weil-pairing

공개키 암호 방식 개념은 관용 암호 방식에서의 키 관리 문제 등을 해결하기 위하여 1976년 W. Diffie와 M. Hellman이 처음 제안하였으며 이후 공개키 암호 방식은 주로 소인수분해문제와 이산대수문제(DLP: Discrete Logarithm Problem)를 기반으로 하고 있다. 이산 대수 문제를 이용한 암호 방식의 안전성은 Diffie-Hellman 시스템의 어려움에 기반하고 있다. Weil-Pairing은 초 특이 타원곡선 상에서 정의되는 bilinear 함수로써 다음과 같이 정의한다[14].

G_1과 G_2는 위수가 소수 l인 순환군이다. G_1은 타원곡선 F_l위에 점들로 이루어진 군이고 G_2는 F_l의 부분군으로 G_1은 덧셈군이며 G_2는 곱셈군이 된다. 함수 $e: G_1 \times G_1 \rightarrow G_2$가 다음 조건을 만족하면 e를 Weil-pairing이라고 한다.

- Bilinearity

: 임의의 $P, Q, R \in G_1$와 $a, b \in Z/l$ 에 대하여

$e(P+Q, R) = e(P, R) \cdot e(Q, R)$

$e(P, Q+R) = e(P, Q) \cdot e(P, R)$ 또는

$e(aP, bQ) = e(P, Q)^{ab}$를 만족한다.

- Identity

: 임의의 $P \in G_1$에 대하여 $e(P, P) = 1$를 만족한다.

- Alternation

: 임의의 $P, Q \in G_1$에 대하여 $e(P, Q) = e(Q, P)^{-1}$를 만족한다.

- Non-degenerate

: 임의의 $P, Q \in G_1$에 대하여 $e(P, Q) \neq 1$이다.

- Efficiency

: $e(P, Q)$의 계산이 효율적인 알고리즘이 존재한다.

타원곡선 위에 점 P, aP, bP, cP가 주어졌다고 가정하자. 이 때, CDHP 즉, P, aP, bP가 주어졌을 때 abP를 구하는 문제는 쉽게 해결되지 않는다. 그러나 DDHP 즉, P, aP, bP, cP가 주어졌을 때 $abP = cP$가 성립하는지 결정하는 문제는 Weil-pairing을 사용하여 $e(aP, bP) = e(P, cP)$가 성립하는지를 확인함으로써 쉽게 해결할 수 있다. 식 $e(aP, bP) = e(p, cP)$이 성립하면 (P, aP, bP, cP)은 DDH쌍이 된다. 따라서 이들은

GDHP 특성을 만족하는 예로써 암호 방식 등에 사용할 수 있다[2, 4].

이 논문에서는 GDHP 특성을 만족하는 bilinear 함수 Weil-pairing을 적용한 초특이 타원곡선 공개키 암호화 기법을 사용하여 세션키 생성, 사용자 인증 및 은닉전자서명을 한다.

2.4.2 ID 기반 공개키 암호화 기법

ID 기반 공개키 암호기법은 Shamir가 1984년에 처음으로 제안하였으며 이 개념은 원래 e-mail 시스템에서 인증 관리를 단순화하기 위한 것이었다[16]. 일반 공개키 암호시스템에서는 공개키 저장을 위한 키 디렉토리(key directory)를 유지함으로서 통신 개시시 키 센터와의 과도한 트래픽과 메모리가 요구된다. ID 기반 암호시스템은 이 단점을 보완하여 통신 상대의 공개키를 상대방의 이름, 망 주소, 또는 메일주소 등의 조합으로 생성함으로 별도의 공개키 파일을 관리하거나 공개키를 증명할 필요가 없다. 따라서 파일센터의 지속적인 유지를 요구하지 않는다. 공개키에 해당하는 ID와 ID에 대응되는 개인키가 있으며, 개인키는 KGC(Key Generation Center)에서 ID를 이용하여 생성하여 인증된 사용자에게 발급한다. 이 방식은 e-mail 구조와 달리 이용자 모두가 신뢰할 수 있는 KGC가 필요하다. KGC에서는 각 개체의 ID 기반 공개키를 사용하여 개인키를 생성한다[15, 1].

2001년 Dan Boneh, Ben Lynn와 Hovav Shacham은 타원곡선상에서의 이산대수문제의 공격에 이용되었던 Weil-pairing을 암호에 응용하여, GDH군에서 실제로 구현 가능한 새로운 서명 방식을 제안하였다. 그들은 서명을 수신한 사람 누구든지 수신된 서명의 정당성을 쉽게 확인 할 수 있어야 하지만, 서명의 생성자 이외에는 누구도 서명을 생성할 수 없어야 한다는 사실에 착안하여 GDHP특성을 만족하는 예를 찾았다. 그리고 같은 년도에 Dan Boneh와 Matthew Franklin은 Weil-pairing을 이용한 ID기반의 암호 방식도 제안하였으며 2003년에는 J. Cha와 J. Cheon이 GDH군에서의 ID 기반 서명 방식을 제안하였다. GDH군을 이용한 새로운 ID기반 암호화 및 서명은 그의 독특한 효율성으로 최근에 활발히 연구되고 있다[2, 3, 4, 12].

Ⅲ. 제안 지불 프로토콜

이 절에서는 우선 제안하는 지불프로토콜에서 이용하는 초특이 타원곡선 Well-pairing을 적용한 ID기반 공개키 암호기법을 이용하여 세션키 생성 및 전자서명기법을 기술한다. 그리고 제안하는 지불프로토콜을 위한 시스템을 구성하고, 제안하는 지불프로토콜의 구조 및 수행과정에 대해 기술한다.

이 논문에서 인증기관은 ID 기반 시스템의 KGC 역할을 한다고 가정한다.

3.1 세션키 생성

사용자는 인증기관에게 자신의 인증서 암호화에 필요한 공개키 생성 요청을 위해 안전한 채널로 자신의 ID를 전송한다. 인증기관은 비밀키 $s \in \{1, \cdots l-1\}$와 G의 생성원P을 선택한 후 $P_{CA} = [s]P$를 계산한다. 그리고 (P, P_{CA})는 공개한다. 사용자, 서비스제공자, 지불게이트웨이 중 임의의 두 개체가 세션키를 공유하길 원한다고 정의한다. 사용자는 인증기관에게 자신의 ID를 보낸다. 인증기관은 사용자의 공개키 $W_U = H(id_U)$를 생성하고 개인키 $w_U = [s]W_U$를 생성한다. 서비스제공자와 지불 게이트웨이의 공개키/개인키도 같은 방법으로 인증기관에 의해 생성된다.

표 3.1. 각 개체 공개키와 개인키

	공개키	개인키
사용자	$W_U = H(id_U)$	$w_U = [s]W_U$
서비스제공자	$W_V = H(id_V)$	$w_V = [s]W_V$
지불게이트웨이	$W_{PG} = H(id_{PG})$	$w_{PG} = [s]W_{PG}$

[표3.1]에서 보는 바와 같다. 사용자, 서비스제공자, 지불게이트웨이는 각각 개인키 역할을 하는 난수 $a, b, c \in Z_q^*$를 생성하고 각각 $[a]P_{CA}$, $[b]P_{CA}$, $[c]P_{CA}$를 계산하여 다른 두 개체에 전송한다.

- $U \rightarrow V, PG : [a]P_{CA}$
- $V \rightarrow U, PG : [b]P_{CA}$
- $PG \rightarrow U, V : [c]P_{CA}$

각 개체들은 받은 정보를 이용하여 세션키를 계산한다. 사용자와 서비스제공자가 각각 생성한 세션키는 두 개체간의 공동 세션키가 된다.

표 3.2. 서명에 사용될 초기화정보

초기화 정보	설 명
G	소수l을 위수로 하는 GDH군
P	G의 생성원
e	bilinear 함수 Weil-Pairing
$H_1\{0,1\}^* \times G \rightarrow Z/l$ $H_2 : \{0,1\}^* \rightarrow G$	충돌회피 해쉬함수
id_X	서명자X의 ID
$t, r \in Z/l$	난수
$W_X = H_2(ID_X)$	서명자의 공개키
$w_X = t \cdot H_2(ID_X) = t \cdot W_X$	서명자의 개인키
$P_X = tP$	공개
M	서명될 메시지

$$
\begin{aligned}
k_U &= \hat{e}([a]w_U, P) \cdot \hat{e}(W_V, [b]P_{CA}) \\
&= \hat{e}([a][s]W_U, P) \cdot \hat{e}(W_V, [b][s]P) \\
&= \hat{e}([a]W_U, P)^s \cdot \hat{e}(W_V, [s]P)^b \\
&= \hat{e}([a]W_U, [s]P) \cdot \hat{e}([b]W_V, [s]P) \\
&= \hat{e}([a]W_U + [b]W_V, [s]P)
\end{aligned}
$$

$$
\begin{aligned}
k_V &= \hat{e}(W_U, [a]P_{CA}) \cdot \hat{e}([b]w_V, P) \\
&= \hat{e}(W_U, [a][s]P) \cdot \hat{e}([b][s]W_V, P) \\
&= \hat{e}(W_U, [s]P)^a \cdot \hat{e}([b]W_V, P)^s \\
&= \hat{e}([a]W_U, [s]P) \cdot \hat{e}([b]W_V, [s]P) \\
&= \hat{e}([a]W_U + [b]W_V, [s]P)
\end{aligned}
$$

그러므로

$$K_{UV} = k_U = k_V = \hat{e}([a]W_U + [b]W_V, [s]P)$$

이다. 따라서 다른 두 개체가 공유하는 세션키도 같은 방법으로 생성한다.

$$K_{VPG} = k_V = k_{PG} = \hat{e}([b]W_V + [c]W_{PG}, [s]P)$$

$$K_{UPG} = k_U = k_{PG} = \hat{e}([a]W_U + [c]W_{PG}, [s]P)$$

만일 세 개체가 공유하는 세션키를 원한다면 아래와 같이 계산하여 생성하면 된다.

$$
\begin{aligned}
k_U &= \hat{e}([a]w_U, P) \cdot \hat{e}(W_V, [b]P_{CA}) \cdot \hat{e}(W_{PG}, [c]P_{CA}) \\
&= \hat{e}([a]W_U + [b]W_V + [c]W_{PG}, [s]P)
\end{aligned}
$$

$$
\begin{aligned}
k_V &= \hat{e}(W_U, P_{CA}) \cdot \hat{e}([b]w_V, P) \cdot \hat{e}(W_{PG}, [c]P_{CA}) \\
&= \hat{e}([a]W_U + [b]W_V + [c]W_{PG}, [s]P)
\end{aligned}
$$

$$
\begin{aligned}
k_{PG} &= \hat{e}(W_U, [a]P_{CA}) \cdot \hat{e}(W_V, [b]P_{CA}) \cdot \hat{e}([c]w_{PG}, P) \\
&= \hat{e}([a]W_U + [b]W_V + [c]W_{PG}, [s]P)
\end{aligned}
$$

따라서 공통 세션키는 다음과 같다.

$$K_{UVPG} = k_U = k_V = k_{PG} = \hat{e}([a]W_U + [b]W_V + [c]W_{PG}, [s]P)$$

3.2 Weil-Pairing 적용한 ID기반 은닉서명

은닉서명은 서명의뢰자가 서명자로부터 메시지의 내용을 보여주지 않고 메시지에 대한 유효한 값을 얻는 서명방식이다. 은닉서명은 전자상거래에서 고객의 완전한 익명성관 불추적성을 제공하므로 개인 프라이버시가 중요시되는 현대사회의 전자상거래에서 고객의 행동이 노출 되여서는 안 되는 보안서비스에 중요하게 활용되고 있다[20].

이 논문에서는 [4]에서의 서명기법을 기반으로 하고 있으며 초특이 타원곡선인 Weil Pairing 적용한 ID 기반 공개키 암호기법을 사용하여 지불내용에 대하여 은닉서명방법을 제안한다. 구체적 은닉서명과정은 다음과 같다.

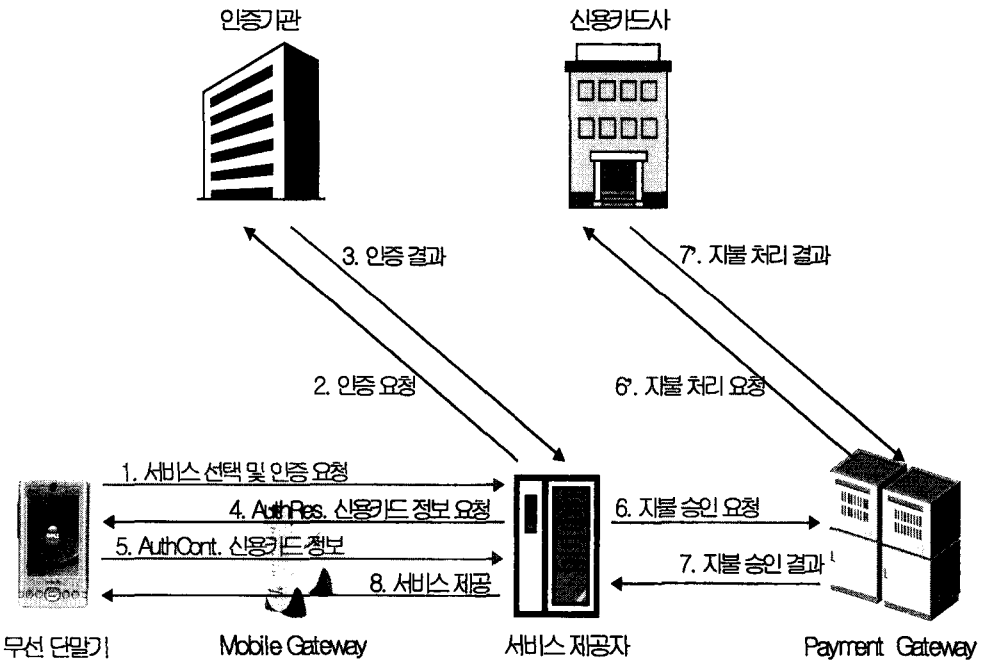


그림 3.1. 제안하는 지불프로토콜을 위한 시스템 구조

① 초기화단계:

초기화단계에서는 [표 3.2]에서와 같이 서명에 필요한 객체들에 대한 정의, 파라메터 생성 및 등록한는 단계이다.

②서명생성단계:

서명자는 난수 $r \in Z/l$를 선택하고 $A = rW_X$, $h = H_1(M.A)$와 $B = (r+h)w_X$를 계산하여 메시지 M에 서명$Sign_X(A, B)$한다.

③서명검증단계:

$$\begin{aligned}
&\hat{e}(P_X, A + hW_X) \\
&= \hat{e}(tP, rW_X + hW_X) \\
&= \hat{e}(P, (r+h)W_X)^t \\
&= \hat{e}(P, (r+h)tW_X) \\
&= \hat{e}(P, (r+h)w_X) \\
&= \hat{e}(P, B)
\end{aligned}$$

서명 검증은 bilinear 함수 e를 사용하여 $\hat{e}(P_X, A + hW_X) = \hat{e}(P, B)$인지 확인하면 된다.

3.3 제안하는 지불프로토콜을 위한 시스템 설계

이 논문에서 제안하는 지불프로토콜은 무선 환경에서 안전한 신용카드기반 지불프로토콜이다. 제안하는 지불프로토콜을 위한 시스템은 [그림 3.1]에서 보여준다. 이 지불 시스템은 사용자의 무선단말기, 모바일게이트웨이, 상품/서비스제공자, 지불게이트웨이, 인증기관, 신용카드사로 구성되며 여기서 모바일게이트웨이는 무선구간과 유선구간의 연계하는 역할을 할뿐 직접 프로토콜의 수행과정에 참여하지 않는다. 그리고 지불을 수행하기 전에 사용자, 상품/서비스제공자, 지불게이트웨이는 인증기관에서 공개키 인증서를 발급받아야한다.

3.4 제안하는 지불프로토콜

지불프로토콜의 흐름은 우선 사용자의 무선단말기가 서비스 제공자의 서버에 접속하여 구매를 원하는 상품 및 서비스를 선택하고 다음은 공개키 기반 인증서 체인을 이용하여 서비스 제공자와의 상호인증과정을 거치고 사용자는 구매할 상품/서비스 정보와 암호화된 신용카드정보를 서비스제공자 서버에 전송하며 그 다음은 서비스제공자는 사용자 구매정보와 암호화된 신용카드정보 및 자신의 은행 계좌 정보 등을 지불 게이트웨이에 전송하여 지불처리를 요청한다. 지불게이트웨이는 서비스제공자로부터 지불정보를 받아 지불을 수행하고 지불수행결과를 서비스제공자서버에

전송한 후 프로토콜은 종료된다. 이 논문에서 제안하는 지불프로토콜에서는 지불프로토콜에서 필요한 알고리즘과 파라메터에 대한 의미는 [표 3.3]에서 설명하고 시스템을 구성하는 개체를 사용자의 무선단말기 U, 모바일게이트웨이 MG, 상품/서비스 제공자 V, 지불게이트웨이 PG, 인증기관 CA로 [표 3.4]에서와 같이 간단한 기호로써 표현한다.

표 3.3. 제안한 프로토콜에 필요한 파라메터

데이터 요소	설 명
id_X	X의 신원
cid_X	X의 인증서용 신원
W_X	X의 공개키
w_X	X의 개인키
K_{XY}	X, Y의 세션키
$Cert_U$	서명 확인 U의 공개키 인증서
$Cert_V$	세션키 생성용 V의 공개키 인증서
$CertChain(X, Y)$	X가 Y의 인증서를 검증용 인증서 체인
T_X	X에 의해 생성된 타임스탬프
ch_data	지불 명세서를 의미하며, 상품이나 서비스 명칭과 수량, 가격이 포함된다
$card\_data$	신용카드 정보를 의미한다.

표 3.4. 시스템에 사용된 개체 설명

개 체	설 명
U	사용자의 무선단말기(Mobile Pone/PDA)
MG	모바일게이트웨이(Mobile Gateway)
V	서비스 제공자
PG	지불게이트웨이(Payment Gateway)
CA	인증기관

인증 과정에 온라인 인증기관이 참여 시 사용자와 서비스제공자 그리고 서비스 제공자와 지불게이트웨이사이에 두 개체만이 알고 있는 세션키 K_{XY}가 필요하다. 이 경우에는 3.1절에서 기술한 알고리즘을 이용하여 세션키(K_{UV}, K_{UPG}, K_{VPG})를 생성한다.

제안한 지불프로토콜의 인증 및 지불 수행과정을 [그림 3.2]에서 보여준다. 이 지불 프로토콜에서 U가 인증서를 가지고 있지 않거나 V와 다른 도메인에 속하면 인증기관인 CA가 인증과정에 참여하여 프로토콜을 수행해야 한다.

① U는 V와 연결하기 위해 자신의 신원 id_U를 세션키 K_{UCA}로 암호화하고, U의 CA에서의 신원 cid_U, 선택한 서비스 정보 $data$와 세션키 K_{UV} 생성에 필요한 임시 공개키 $[u]P$를 V에게 전송한다.

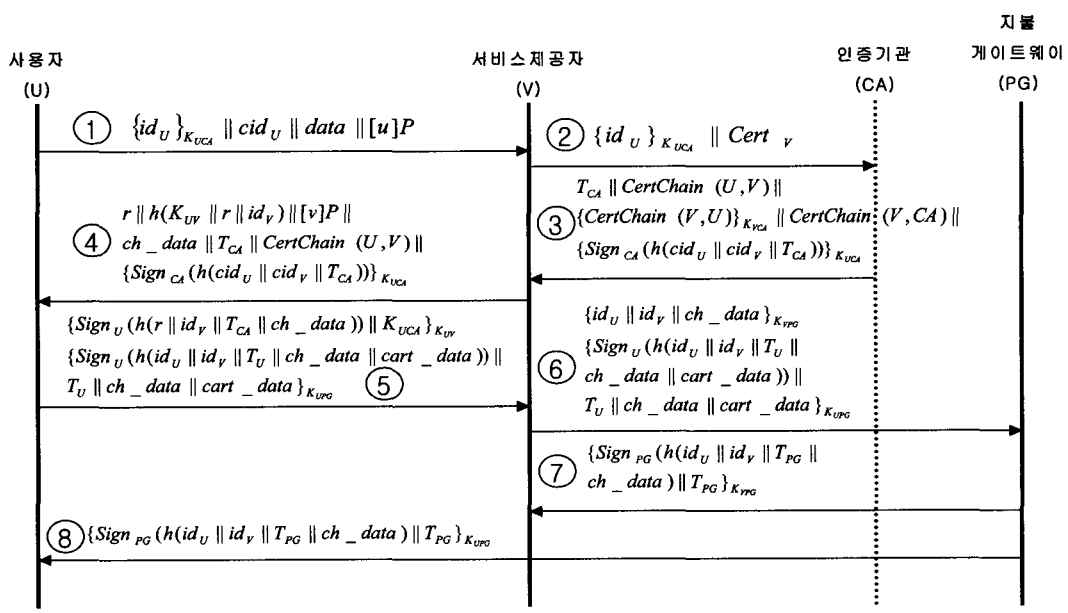


그림 3.2. 제안 지불 프로토콜 수행과정

② V는 U가 전송한 메시지와 자신의 인증서 $Cert_V$를 온라인 인증기관인 CA에게 전송한다.

③ CA는 V에게 받은 메시지에서 V의 신원을 확인하고 U가 V의 공개키를 확인할 수 있는 $CertChain(U, V)$를 생성하고 또한 V가 U와 CA의 공개키를 확인할 수 있도록 $CertChain(V, U)$와 $CertChain(V, CA)$를 생성한 다음 $CertChain(V, U)$는 세션키 K_{UCA}로 암호화하여 V에게 전송한다.

④ V는 난수 r을 생성한 후 U와의 세션키 K_{UV}를 생성하여 지불 명세서와 인증서 체인 그리고 CA의 서명이 포함된 데이터를 U에게 전송한다.

⑤ U는 $CertChain(U, V)$를 통해서 V의 인증서를 검증하고 지불 명세서와 타임스탬프를 확인한 후 신용카드 정보가 포함되어 있는 메시지 및 은닉서명한 서명값을 세션키 K_{UPG}로 암호화하고, 또 V가 $CertChain(V, U)$를 검증할 수 있도록 세션키 K_{UCA}를 U와 V의 세션키로 암호화하여 전송한다.

⑥ V는 U에게서 받은 세션키 K_{UCA}로 $CertChain(V, U)$을 확인한다. 그리고 U가 서명한 메시지를 확인하고, PG에게 전송할 메시지 $\{id_U \mid id_V \mid ch\_data\}_{K_{VPG}}$ 를 생성하여 신용카드 정보가 포함되어 있는 U가 서명한 메시지를 PG에게 함께 전송한다.

⑦ PG는 U와 V 가 보낸 메시지를 확인하고 지불 명세서를 비교하여 동일하면 신용카드 정보 $card_data$를 사용하여 지불을 수행한다. 사용자의 신용카드 정보로 지불이 성공적으로 이루어지면 거래에 참여한 참여자의 신원 id_U, id_V와 지불이 수행된 시간 T_{PG}, 지불 명세서 ch_data 을 메시지로 3.2절에서 기술한 알고리즘을 이용하여 은닉 서명하여 V 에게 전송하고 V 를 통하여 U에게도 전송한다. 이 과정이 수행되면 U는 선택한 상품이나 서비스를 제공받게 된다.

Ⅳ. 안전성 분석 및 성능 평가

이 장에서는 제안한 지불 프로토콜의 안전성 대한 분석 및 기존의 지불프로토콜과의 성능분석을 통하여 제안한 지불프로토콜이 효율적이고 안전함을 입증한다.

4.1 안전성 분석

- 개체들의 상호인증 : 제안한 프로토콜에서는 두 개체만 공유하는 세션키를 생성한 다음 세션키(K_{XY}), 난수(r) 및 신원(id_X)을 해쉬한 메시지($h(K_{XY} \mid r \mid id_X)$)를 세션키로 암호화하여 교환함으로 세션키의 안전한 전송과 개체 상호인증을 제공한다. 때문에 신원위장공격에 안전하다.
- 거래정보의 기밀성: 제안한 프로토콜에서는 구매정보는 U와 V의만이 갖고 있는 세션키 K_{UV}로 암호화하여 전달하고 신용카드정보는 U와 PG의 세션키K_{UPG}로 암호화하여 전달함으로 거래정보에 대한 기밀성을 보장한다. 세션키 생성과정에 난수r를 첨가하여 세션키의 재사용 방지한다.
- 거래정보의 무결성: 제안한 프로토콜에서는 랜덤 난수r를 첨가한 해쉬값을 이용하여 거래정보의 무결성을 보장한다. 따라서 거래정보에 대한 위-변조 공격에 안전하다.
- 부인 방지: 제안한 프로토콜에서는 각 개체들의 은닉전자서명을 통하여 거래 개체들의 부인방지를 제공한다. 여기서의 은닉전자서명은 거래사실을 증명할 뿐만 아니라 사용자의 프라이버시도 보호된다.

이 논문에서 제안한 지불 프로토콜에서 사용하는 초특이 타원곡선 Well-pairing을 적용한 ID기반 공개키 암호방식은 GDHP의 어려움을 기반으로 하고 있으며 이는 RSA에서의 1024비트와 같은 강도의 안전성을 갖는다. 또한 은닉서명기법을 사용하여 사용자의 익명을 제공하여 고객 프라이버시를 보호한다고 할 수 있다.

4.2 성능 평가

제안한 지불프로토콜에서 사용한 초 특이 타원곡선

표 4.1. 제안 프로토콜과 기존 지불프로토콜과의 보안특성 비교

보안 요소	SET 프로토콜	WPP 프로토콜	AIP 프로토콜	제안한 프로토콜
인증과 지불 통합	×	×	○	○
종단간 보안 제공	○	×	○	○
익명성(privacy 보호)	×	×	×	○
키 교환알고리즘	RSA/DES	RSA/ Deffie-Hellman	Deffie-Hellman/ Elgamal	Deffie-Hellman

Well-pairing을 적용한 ID기반 공개키 암호방식은 GDHP의 어려움을 기반으로 하고 있으며 타원곡선상에서 연산이 이루어지므로 유한체상의 어느 연산보다 연산속도가 빠르고 짧은 길이의 키에 비해 강인한 안전성을 갖는다. [표 4.1] 에서는 제안한 지불프로토콜과 기존 지불프로토콜을 보안특성을 기반으로 비교분석한 결과를 보여준다. 특히 제안프로토콜에서는 은닉서명으로 익명성과 불추적성을 제공하여 사용자의 프라이버시를 보호한다.

WPP프로토콜, AIP 프로토콜 및 제안한 프로토콜과의 성능(통신량과 계산량) 분석 결과는 [표 4.2]에 나타낸다. 성능 분석은 무선 인터넷 환경에서는 주로 사용자와 서비스 제공자간의 정보교환이 프로토콜의 효율성에 많은 영향을 끼친다. 따라서 이 논문에서는 성능 분석을 사용자 측면에서의 통신량과 계산량을 비교하였다.

표 4.2. 사용자 측면에서 통신량과 계산량 비교

	WPP 프로토콜	AIP 프로토콜	제안한 프로토콜
메시지 교환 횟수	10	4	4
세션키 생성 횟수	3	4	2
세션키 생성 연산법	공개키 암호의 멱승(곱셈군)	타원곡선의 덧셈군	타원곡선의 덧셈군

통신량은 전송되는 메시지 전송 횟수이고, 계산량은 ID기반 공개키 암호에서 세션키 생성 횟수를 계산하였다. 제안한 프로토콜과 WPP 프로토콜을 비교한 결과 계산량에서 세션키 생성 횟수는 비슷하지만 연산법이 곱셈군에서 덧셈군으로 대치되었고, 통신량에서의 메시지 교환 횟수도 제안한 프로토콜에서 감소되었다. 그리고 기존 AIP프로토콜[19]과 비교한 결과 제안 프로토콜에서는 세션키를 일시 세션키(사용자와 서비스제공자간의 세션키K_{UV} 및 서비스제공자와 지불게이트웨이간의 세션키K_{VPGA})와 장기 세션키 ($K_{UCA}, K_{UPG},$)로 분리하여 지불 프로토콜에서의 세션키 생성회수를 절반으로 줄이여 보다 효율적이고 안전한 무선 환경에 적합한 지불방법을 제시하였다.

V. 결론

최근 정보통신기술의 급속한 발달로 무선인터넷을 이용한 전자상거래 사용자가 폭발적으로 증가되고 있다. 유선에서 유/무선 통합 환경으로 변화함에 따라 보안상의 많은 문제점이 제시되고 있다. 무선 환경에서의 전자상거래는 많은 편리함을 제공하지만 무선이 신뢰도가 떨어지는 매체이기 때문에 새로운 문제들이 발생되고 있다.

현재 무선 전자상거래에서는 주로 신용카드기반의 지불 프로토콜 WPP와 ASPeCT에서는 제안한 인증과 지불초기화를 위한 AIP프로토콜을 사용하고 있다.

WPP에서 사용되는 보안 프로토콜 WAP에서의 게이트웨이는 무선 구간의 WTLS 와 유선 구간의 TLS를 연결해 주기 위해서 사용자로부터 전달된 데이터를 해독하고 다시 암호화하여 Web Server로 전달하며, 반대로 Web Server 로부터 전달된 데이터를 해독하고 이를 다시 암호화하여 사용자에게 전달한다. 이 과정에서 WAP 게이트웨이는 사용자와 서버사이의 전달되는 데이터의 모든 내용을 해독하므로 보안의 허점이 발생할 수 있다. 따라서 WAP에서는 "어느 정도 신뢰 있는 보안"을 제공하지만 완벽한 종 단간 보안은 제공하지 못한다.

AIP프로토콜에서 온라인 인증기관이 참여하지 않는 프로토콜은 사용자와 서비스 제공자간에 이루어지는 것으로 프로토콜이 간단한 장점이 있지만 사용자의 인증서 취소 여부를 파악할 수 없어 서비스 제공자는 제공한 서비스에 대해 사용자가 지불을 완료할 것인지에 대한 검증을 할 수가 없는 단점이 있다. 온라인 인증기관을 이용한 AIP 프로토콜에서 서비스 제공자는 온라인 인증기관과 프로토콜 수행을 통해 사용자

의 인증서의 취소 여부를 파악함으로써 제공한 서비스에 대한 지불 가능 여부를 검사할 수 있다. 그러나 온라인 TTP와의 원거리 통신에 따른 문제점이 있으면 인증서 체인을 이용하여 검증을 수행하므로 계산량이 많아지게 된다. 또한 AIP프로토콜은 사용자의 인증서가 서비스 제공자에게 전달이 되므로 사용자의 신원이 서비스 제공자에게 노출되어 프라이버시보호를 위한 익명성이 보장되지 않는 단점이 있다.

이 논문에서는 기존 AIP프로토콜을 기반으로 초특이 타원곡선인 Weil Pairing 적용한 ID 기반 공개키 암호기법을 사용하여 세션키를 생성하여 거래정보의 기밀성을 보장하고 은닉전자서명기법을 통한 인증서를 사용하여 프라이버시 보호, 공개키와 사용자 인증 및 부인방지를 해결했으며 또한 두 객체만 공유하는 세션키를 사용하여 종단간 보안이 제공되는 특정 무선 플랫폼에 독립적이며 안전하고 효율적인 지불 프로토콜을 제안하였다. 또한 제안한 프로토콜은 사용자와 서비스 제공자간의 온라인 인증기관이 지불 프로토콜의 인증과정에 참여함으로써 다른 도메인에 존재하는 서비스 제공자에게서도 효율적이고 안전한 서비스를 받을 수 있게 하였다.

향후 무선인터넷 보안기술의 발전은 유·무선 통합 환경으로 변화함에 따른 기존의 인터넷이나 무선통신에서의 보안 서비스와는 다른 새로운 패러다임에 대한 연구 및 개발이 시급한 상황이다. 그리고 무선통신 환경에서의 대역폭, 단말기 등의 제한을 고려한 인증서 프로파일, 암호 알고리즘, 키 크기, 인증서 취소 여부 확인 메커니즘 등의 연구개발이 이루어져야 할 것이다. 이를 위한 무선인터넷 환경에 적합한 무선 공개키 기반 구조(WPKI)를 구축하고 유선 인터넷에서의 공개키 기반구조와의 원활한 연동에 관한 연구도 필요하다.

참 고 문 헌

[1] Dan Boneh, "The decision Diffie-Hellman problem", in Proc. Third Algorithmic Number Theory Symposium, Lecture Notes in Computer Science, Vol. 1423, Springer-Verlag, pp. 48-63, 1998.

[2] Dan Bonehy Matthew Franklin, "Identity-based encryption from the Weil Pairing". extended abstract in Advances in Cryptology-Crypto 2001, Lecture Notes in Computer Science, Vol. 2139, Springer-Verlag, pp. 231-229, Aug. 2001.

[3] Dan Boneh, Ben Lynn, Hovav Shacham, "Short signatures from the Weil pairing", in Advances in Cryptology-AsiaCrypt 2001, Lecture Notes in Computer Science, Vol. 2248, Springer-Verlag, pp. 514-532, 2001.

[4] Jae Choon Cha and Jung Hee Cheon, An identity-based signature from gap Diffie-Hellman groups, PKC 2003, Lecture Notes in Computer Science 2567 (2002), pp. 18-30.

[5] Tim Dierks and Christopher Allen, "The TLS Protocol Version 1.0" IETF RFC 2246, January 1999

[6] Whitfield Diffie and Martin E. Hellman, "New Directions in Cryptography" IEEE Transactions on Informations Theory, Vol, IT-22, No 6, pp.472-492, Nov,1976.

[7] WAP Fourm, "Wireless Application Protocol Wireless Transport Layer Security Spectification version 18-FEB-2000", 2000

[8] Jeyanthi Hall, Susan Kilbank, Michel Barbeau and Evangelos Kranakis, "WPP: A Secure Payment Protocol for Supporting Credit-card and Debit-card Transactions Over Wireless Networks," IEEE International Conference on Telecommunications (ICT), Bucharest, June, 2001.

[9] Gunter Horn, Bart Preneel, "Authentication and Payment in Future Mobile Systems, " ESORICS, LNCS 1485,pp.277-293, 1998.

[10] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Handbook of Applied Cryptography" CRC Press, October 16, 1996, ISBN: 0849385237

[11] Keith M. Martin , Bart Preneel , Chris J. Mitchell , Hans-Joachim Hitz , Günther Horn , A. Poliakova , P. Howard, "Secure Billing for Mobile Information Services in UMTS", Proceedings of the 5th International Conference on Intelligence and Services in Networks: Technology for Ubiquitous Telecom Services, p.535-548, May 25-28, 1998

[12] Divya Nalla, and K.C.Reddy, "ID-based tripartite Authenticated Key Agreement Protocols from pairings" available at

http://eprint.iacr.org/2003/004.pdf

[13] Pekka Niskanen and Jukka Heika "Inside WAP : Programming Applications with WML and WMLScript"Addison-Wesley, 2000

[14] Tatsuaki Okamoto and David Pointcheval "The gap-problems: a new class of problems for the security of cryptographic Schemes, Proc. of PKC '01, Lecture Nores in Computer Sciences,Vol. 1992, pp. 104-118, Springer-Verlag, 2001.

[15] Nigel P. Smart, "An Identity based authenticated Key Agreement Protocol based on the Weil pairing", Cryptology ePrint Archive, Report 2001/111,2001. http://eprint.iacr.org/.

[16] Adi Shamir "Identity based cryptosystems and signature schemes" Advances in Cryptology Proceedings of Crypto'84, pp.47-57

[17] 이동훈, 임채훈, "TLS와 WTLS의 비교 분석", (주)퓨처시스템 암호체계센터 기술보고서, Oct. 2000.

[18] 이만영, 김지홍, 류재철, 송유진, 염흥렬, 이임영, "전자상거래 보안 기술", 생능출판사, 1999.

[19] 이병래, 장경아, 김태윤 "3세대 이동통신을 위한 티켓 기반 인증 및 지불 기법" 정보과학회논문지: 정보통신 제29권 제4호, 2002.8.

[20] 이상곤, 윤태은 "EC - KCDSA 부분 은닉서명을 이용한 거스름 재사용 가능한 전지수표지불 시스템" 한국정보보호학회논문지 제13권 제1호, 2003. 2

[21] 조유근, "SET 프로토콜을 위한 안전하고 효율적인 지불 게이트웨이의 설계 및 구현", 서울대학교 석사논문, 2000년 2월.

[22] 한대완, 이동훈, 황상철, 류재철 "WISA2002에 제안된 무선 전자 지불 시스템의 안전성" 정보보호학회 논문지 13권 6호, 2003.12

김 석 매 (Jin Shi Mei) 학생회원

1994년6월: 중국길림성 연변대학 물리학과 졸업(이학사)

2004년8월: 충북대학교 자연대학 전기전자컴퓨터학과 졸업(이학석사)

2004년9월~현재: 충북대학교 전기전자컴퓨터공학과 박사과정

<관심분야> 전자상거래 보안, 전자지불 프로토콜, 유비쿼터스 보안

김 장 환

1980년 서울대학교 경제학 학사.

1997년 한국과학기술원 전산학 석사.

2003년 충북대학교 전산학 박사.

1984년~1988년 쌍용정보통신 연구원.

1988년~1993년 Qnix Data System 연구원.

1993년~1998년 SK Telecom 연구원.

1998년~현재 대덕대 IT계열 교수. ITU-R, WIPO member, 전자상거래 관리사.

<관심분야> Mobile & Wireless Communication, Performance Analysis of Networks, Database System, Information Security, Mobile Multimedia, Mobility Managements, Mobile Embedded System, Ubiquitous Computing, 알고리즘 및 계산이론, 정보통신 경제 예측

이 충 세

한국통신학회 논문지 '04-2 Vol.29 No.2A 참조