Journal of Digital Contents Society Vol. 14 No. 1 Mar. 2013(pp. 81-88)
http://dx.doi.org/10.9728/dcs.2013.14.1.81

무인증서 서명 암호화 기법을 이용한 안전한 모바일 신용카드 결제 프로토콜

최희진*, 김형중**

요 약

스마트폰 사용의 증가로 인해 모바일을 통한 결제가 대중화되고 모바일카드 이용자도 급격하게 증가하고 있다. 현재 사용되어지는 모바일카드의 대부분은 USIM(Universal Subscriber Identification Module) 칩에 신용카드 정보를 다운받아 사용자에게 서비스를 제공한다. USIM에 저장되는 모바일카드는 통신사의 USIM 칩에 보안을 위한 최소한의 정보를 저장하고 관리하며 PKI(Public Key Infrastructure) 기반의 인증서 체계를 사용하고 있다. 그러나 PKI 기반의 결제 시스템의 경우 처리 절차가 복잡하고, 인증서 및 CRL(Certificate Revocation List) 관리에 많은 비용이 필요하다. 특히 인증서가 없는 외국인의 경우 국내 전자상거래를 이용할 수 없기 때문에 국내 전자상거래 발전을 저해하는 요인으로 작용할 수 있다. 따라서 본 논문에서는 인증서 사용의 문제를 해결한 모바일 환경에 적합한 무인증서(certificateless) 기반의 서명 암호화 기법을 이용한 안전한 신용카드 결제 프로토콜을 제안한다.

키워드 : 모바일 신용카드, 무인증서, 결제 프로토콜, 서명암호화

Secure Mobile Credit Card Payment Protocol based on Certificateless Signcryption

Hui-Jin Choi*, Hyung-Jung Kim**

Abstract

The increase of the smartphone users has popularized the mobile payment and the mobile credit card users are rapidly getting increased. The mobile credit cards that currently used provide its users with the service through downloading mobile credit card information into USIM. The mobile credit card saved in USIM has the minimized information for the security and is based on PKI. However certificate-based payment system has a complicated procedure and costs a lot of money to manage the certificates and CRL(Certificate Revocation List). Furthermore, It can be a obstacle to develop local e-commerce in Korea because it is hard for foreigners to use them. We propose the secure and efficient mobile credit card payment protocol based on certificateless signcryption which solve the problem of certificate use.

Keywords : Mobile Credit Card, Certificateless, Payment Protocol, Signcryption

※ 교신저자(Corresponding Author): Hyung-Jung Kim
접수일:2013년 01월 24일, 수정일:2013년 03월 17일
완료일:2013년 03월 28일
* 고려대학교 정보보호대학원 정보보호학과
email: astehelen@gmail.com
** 고려대학교 정보보호대학원 정보보호학과
Tel: +82-2-3290-4258 , Fax: +82-2-928-9109
email: khj-@korea.ac.kr
▣ 본 연구는 문화체육관광부 및 한국콘텐츠진흥원의 콘텐츠산업기술지원사업(R2012050022), 지식경제부 및 한국산업기술평가관리원의 산업융합원천기술개발사업(정보통신)의(10039670) 일환으로 수행되었음

1. 서론

스마트폰의 빠른 확산으로 사용자의 생활 패턴의 변화 뿐 아니라 금융 거래 산업에도 영향을 주고 있다. 모바일 뱅킹을 비롯한 주식거래 및 물품 구매 등의 전자상거래를 스마트폰을 통

해 편리하게 이용할 수 있다. 스마트폰의 확산은 2013년 전체 휴대폰 시장의 38.5%로 전망되었으며, 2012년 가트너의 '모바일 결제 시장 현황 보고서에 따르면 모바일 결제 시장은 지난해 1059억불 에서 61.9% 성장한 1715억불을 넘어설 것으로 보이며, 모바일 결제 이용자는 2억1220만에 이를 것으로 예상된다고 밝혔다.[1][14]

모바일 신용카드 결제 방식은 크게 두 가지 서비스로 분류되는데 첫 번째는 기존 보유한 신용카드 정보로 모바일 매체를 통해 결제하는 방식이고 두 번째는 모바일용 신용카드를 발급받아 사용하는 방식이다. 신용카드 거래를 위해서는 두 가지 방식 모두 공인 인증서가 필요하며 각각의 금융서비스 및 결제서비스 어플리케이션별로 해당 웹사이트를 통해 PC에서 스마트폰으로 공인인증서를 다운받아 사용해야 하는 불편함이 있다. 최근 모바일 결제서비스 중 30만원 미만의 소액 결제 시 인증서를 사용하지 않는 결제 수단으로 SMS, 폰빌 등이 등장하였지만 여전히 고액 결제에서는 공인 인증서를 사용해야 한다. 공인인증서를 사용하는 PKI 기반의 결제 시스템의 경우 처리 절차가 복잡하고, 인증서 및 CRL(Certificate Revocation List) 관리에 많은 비용이 필요하다. 특히 인증서가 없는 외국인의 경우 국내 전자상거래를 이용할 수 없기 때문에 국내 전자상거래 발전을 저해하는 요인으로 작용할 수 있다.

본 논문에서는 인증기관, 인증서의 유지비용, 상호 인증과정의 복잡성 등의 불필요한 요소를 제거하고, 실제 모바일 환경에서 적용하여 안전한 결제 서비스를 제공할 수 있는 무인증서 서명암호화 기반의 안전한 모바일 신용카드 결제 프로토콜을 제안한다. 2장에서는 선행된 ID기반 암호시스템 및 무인증서 서명 암호 시스템에 대한 연구동향을 살펴보고, 3장에서는 무인증서 서명암호화 기법에 기반한 모바일 결제 프로토콜을 제안한다. 4장에서는 제안된 프로토콜의 성능과 안정성에 대하여 기 제안된 기술과 비교·분석하고, 끝으로 결론 및 향후 연구 방향을 제시한다.

2. 관련연구

전통적인 공개키 암호(PKC, Public Key Cryptography) 시스템은 송신자가 수신자의 공인된 공개키를 얻어 전달하고자 하는 메시지를 공개키로 암호화하여 전달하고, 수신자는 자신의 개인키로 복호화 하는 기술이다. 이를 통해 사전에 비밀 키를 나눠가지지 않은 사용자들이 안전하게 통신할 수 있도록 한다. 이를 위해 공개 키는 누구나 쉽게 얻을 수 있고 알 수 있지만 그에 대응하는 비밀 키는 키의 소유자만이 알 수 있어야 한다. 그러나 공개키 암호 시스템의 경우 대칭키 암호 시스템에 비해 많은 계산 비용이 발생하며, 특히 안전하게 공개키를 관리하기 위한 인증서기반의 PKI를 사용함에 따라 복잡한 인증서 관리 문제가 발생한다. 특히 인증서는 유효기간 전에 폐기될 가능성이 있기에 인증서 이용 시 CRL(Certificate Revocation List)에 기반한 유효성 검증을 위한 추가적인 비용과 부하가 발생한다.

이러한 전통적인 공개키 암호 시스템의 문제를 해결하기 위해 1984년 Shamir[2]에 의해 ID 기반 암호시스템(ID-PKC)이 소개되었다. 송신자는 수신자와 관련된 이메일 주소, IP 정보 등 전체 시스템에서는 유일하지만 이미 공개되어진 정보를 공개키로 사용하므로 누구든지 상대방의 공개된 정보를 통하여 간단하게 메시지를 전달할 수 있다는 것이 장점이며, 수신자가 KGC(Key Generation Center)에서 자신의 개인키를 생성하기 전에도 송신자는 암호화된 메시지 전달이 가능하다. 그러나 ID 기반 공개키 시스템에서는 KGC가 참여한 모든 사람의 메시지를 복호화하거나 또는 대신 전자서명을 할 수 있는 키 에스크로 문제를 가지고 있다.

2003년 Al-Riyami와 Paterson[3]은 전통적 공개키 암호시스템의 인증서 관리 문제와 ID기반 공개키 시스템의 키 에스크로 문제를 해결할 수 있는 무인증서 공개키 시스템(CL-PKC)을 제안했다. CL-PKC에서 KGC는 사용자의 부분 비밀키를 생성하고, 사용자는 KGC로부터 받은 부분 개인키와 자신이 생성한 비밀값을 이용하여 본인만이 아는 공개키, 개인키 쌍을 생성하여 사용한다.

2008년 Barbosa와 Farshim[4]이 인증서 없는 인증암호화(CLSC) 기법을 처음으로 제안하였고, Wu와 Chen[5]에 의해 효율적인 CLSC 스킴이

소개되었으나, Selvi 등[6]에 의해 안전하지 않음이 밝혀졌다. Xie 등[7]은 쌍선형지도에 의해 signcrypt 와 unsigncrypt 두 단계에서 2개의 페어링 연산만을 사용한 CLSC 스킴을 제안했으나, 이 스킴 역시 계산 비용이 높은 페어링 연산 때문에 실제 필드에서 적용하기에는 어려움이 있다. 이에 Xie와 Zhang은 페어링을 사용하지 않는 효율적인 무인증서 암호화 기법을 제안하였다.[8]

한편 스마트폰을 이용한 모바일 결제 프로토콜에 대한 연구는 전통적인 공개키 암호 시스템을 이용한 연구가 가장 활발하게 이루어졌다.[9][10][11][12][13] 특히 지은화, 김애영, 이상호는 USIM을 기반으로 하여 대칭키 암호와 비대칭키 암호를 혼용하여 사용함으로써 안전성을 높이는 결제 프로토콜을 제안했다.[9] 그러나 USIM이 가지고 있는 비밀키, 공개키를 그대로 결제 프로토콜에 사용함에 따라 사용자측의 인증서 갱신이 불가능하고, 최초 신용카드 등록 및 발급 시 오프라인으로 신용카드 발급기관을 이용해야 하는 불편함이 있다.

3. 무인증서 기반 안전한 모바일 결제 프로토콜

본 장에서는 제안하는 프로토콜의 기반이 되는 무인증서 기반의 서명암호화 기법을 살펴보고, 이를 이용한 안전한 모바일 결제 프로토콜을 제안한다. 본 논문에서 사용되는 기호들은 <표 1>과 같다.

<표 1> 표기법

ID_A	identifier of A
d_A	partial private key of A
p_A	partial public key of A
s_A	secret value of A
pk_A	public key of A
sk_A	private key of A
σ_i	i-th encrypted message
$h(X)$	hash value of X

<Table 1> Notations

3.1 무인증서 기반 서명 암호화 기법

무인증서 암호화 기법(Certificateless Signcryption Scheme)은 다음과 같은 7개의 알고리즘으로 구성된다.

- **Setup** : 임의의 k로부터 시스템 파라미터 $params$과 마스터 비밀키 $master-key$를 생성한다.
- **Partial-Key-Extract** : Setup 알고리즘에서 얻어진 $params$, $master-key$ 및 사용자 식별값 ID로부터 부분 개인키 d_{ID}와 부분 공개키 p_{ID}를 생성한다.
- **Set-Secret-Value** : $params$ 와 사용자 식별값 ID로부터 비밀값 s_{ID}를 생성한다.
- **Set-Public-Key** : $params$, 사용자의 부분 공개키 p_{ID}와 비밀값 s_{ID}로부터 사용자의 공개키 pk_{ID} 를 생성한다.
- **Set-Private-Key** : $params$, 사용자의 부분 개인키 d_{ID}와 비밀값 s_{ID}로부터 사용자의 개인키 sk_{ID}를 생성한다.
- **Signcrypt** : $params$, 송신자의 개인키 sk_{ID_S}, 수신자의 식별값 ID_R 과 공개키 pk_{ID_R}, 메시지 m으로부터 암호문 σ를 생성한다. 즉 $\sigma = signcrypt(params, sk_{ID_s}, ID_R, pk_{ID_R}, m)$ 이다.
- **Unsigncrypt** : $params$, 송신자의 식별값 ID_s 와 공개키 pk_{ID_s}, 수신자의 개인키 sk_{ID_R}와 암호문 σ로부터 메시지 m을 복원한다. 암호문 σ가 올바르다고 증명되면 메시지 m을 복원하고, 그렇지 않으면 복호화가 되지 않는다. 즉 $\rho = unsigncrypt(params, ID_S, pk_{ID_s}, sk_{ID_R}, \sigma)$ 이고, ρ가 정상적으로 복호화되면 메시지 m을, 그렇지 않으면 에러가 출력된다.

Setup과 Partial-Key-Extract 알고리즘은 KGC에 의해 수행된다. 부분 개인키 d_{ID}와 부분 공개키 p_{ID}는 사용자에게 비밀채널을 통해 전달되고, 사용자의 공개키 및 개인키 쌍을 생성하는 알고리즘과 Set-Secret-Value 알고리즘은 사용자에 의해 수행된다.

3.2 모바일카드 결제 프로토콜

일반적으로 사용되고 있는 모바일 신용카드 결제 프로토콜에서는 PKI에 기반한 인증서를 사용한다. 따라서 사용자가 모바일 결제 서비스를 이용하기 위해서는 최초 혹은 인증서 갱신 시마다 PC를 이용하여 자신의 모바일장치에 인증기관으로부터 발급받은 공인인증서를 이관해야 한다. 그러나 제안한 프로토콜에서는 무인증서 기반의 서명암호화기법을 사용함으로써 사용자의 모바일 장치에서 바로 KGC를 통해 필요 시 언제든지 쉽게 서명 암호화키를 발급받을 수 있다.

일반적인 국내 전자상거래 카드 거래는 카드사, 가맹점 및 전자지불결제대행사인 PG로 구성되다. 일반적으로 사용자가 가맹점에서 카드를 사용하면 가맹점은 사전에 계약된 PG업체에 카드승인요청을 하고 PG는 카드사로부터 승인처리를 받은 후 가맹점에 회신하여 사용자의 카드승인이 정상처리 되었음을 전달한다. 이는 모바일 결제에도 동일하게 적용된다.

본 논문에서 제안하는 모바일 신용카드 결제 프로토콜에 참여하는 객체는 공인된 키 생성 센터 KGC, 카드사 CARD, 전자지불결제대행사 PG, 전자 상점 M, 모바일폰 사용자 USER가 있다. 카드정보는 실제 실물카드의 정보(카드번호, CVC 또는 CVV, 유효기간, 소유자명, PIN의 해쉬값$h(PIN)$ 등)를 나타내며, 가상카드정보는 사용자의 모바일에 발급받은 모바일카드 정보(모바일카드번호, 유효기간, 소유자명, 기기식별정보와 모바일카드의 PIN인 mPIN의 해쉬값 $h(mPIN,$기기식별정보$)$ 등)를 나타낸다. 그 외에 본 논문에서 사용되는 주요기호는 메시지인증을 위한 키는 MACKEY, 구매하는 물품의 가격 price로 나타나며, 구매내역의 트렌젝션 정보 TID, 모바일카드 번호는 VNO로 표기한다.

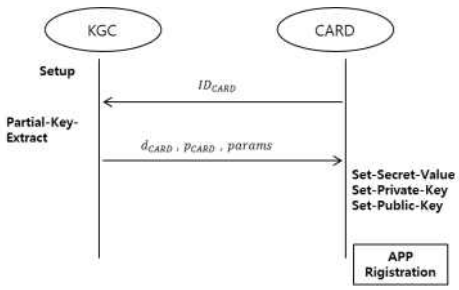
무인증서 기반의 모바일카드 전체 프로토콜은 초기화 및 APP배포 단계, 모바일카드 발급 단계, 모바일카드 거래 단계의 3단계로 구성된다.

3.2.1 초기화 및 모바일 APP 배포 단계

KGC는 Setup 알고리즘을 수행하여 자체 시스템에서 사용할 시스템 파라미터를 정의한다. 카드사는 KGC에 카드사의 식별정보 ID_{CARD}를 전달하고, KGC는 Partial-Key-Extract 알고리즘을 통해 카드사의 부분 개인키, 공개키쌍을 생성하여 카드사에 회신한다. KGC로부터 부분 개인키d_{CARD}, 부분 공개키p_{CARD}와 $params$를 전달받으면, 카드사는 자신이 생성한 비밀값을 이용하여 카드사 개인키 sk_{CARD}와 카드사 공개키 pk_{CARD}를 생성하고, KGC로부터 수신한 $params$, 카드사 공개키pk_{CARD}와 카드사 식별값 ID_{CARD}를 스마트폰용 결제용 APP에 포함하여 앱스토어(APP Store) 또는 마켓(Market)에 배포한다.

본 논문에서는 사용자가 신뢰할 수 있는 마켓에서 변조되지 않은 앱을 설치했음을 가정한다. 사용자는 마켓에서 앱 설치 후 최초 카드사 접속 요청 시 카드사는 사용자의 앱 위변조 여부와 공개키 여부를 검증한 후 모바일카드 발급진행을 처리한다.

(그림 1) 초기화 및 모바일 앱 배포단계



(Figure 1) Initialize and Mobile APP Distribution

3.2.2 모바일 카드 발급 단계

모바일카드를 사용하는 사용자는 카드사의 결제용 APP을 설치하고, KGC에 사용자 식별정보 ID_{USER}를 전달하고 사용자의 부분 개인키d_{USER} , 사용자의 부분 공개키p_{USER}와 $params$ 값을 전달받아 사용자의 비밀값을 이용하여 사용자의 개인키sk_{USER}와 사용자의 공개키pk_{USER}를 생성한다.

사용자의 키쌍이 생성된 후에는 카드사에 모바일카드 발급 과정을 진행한다.

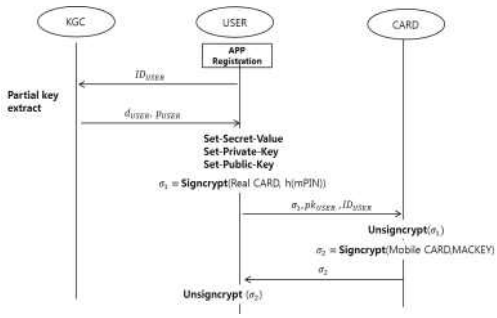
사용자가 자신의 카드 비밀번호 PIN과 모바일카드에서 사용할 비밀번호 mPIN을 입력하면, 사용자의 개인키 sk_{USER}, 카드사의 식별정보 ID_{CARD}, 카드사의 공개키 pk_{CARD}와 실카드정보,

기기식별정보와 mPIN을 해쉬한 값 $h(mPIN, 기기식별정보)$을 Signcrypt 알고리즘에 입력하여 서명 암호화한 메시지 σ_1를 생성하여 카드사에 전달한다.

카드사는 서명 암호화된 메시지 σ_1와 사용자의 식별정보 ID_{USER}, 공개키 pk_{USER}, 카드사의 개인키 sk_{CARD}를 Unsigncrypt 알고리즘에 입력하여 복원된 사용자의 실제 카드정보를 확인하고 $h(PIN)$과 기 등록된 PIN의 해쉬값을 비교하여 합법적인 사용자인지 확인한다. 카드사의 고객으로 확인되면, 카드사는 실제 카드번호 유출을 방지하기 위해 실제 카드번호가 아닌 모바일카드 번호 VNO를 생성하고, VNO, $h(mPIN, 기기식별정보)$, ID_{USER}, pk_{USER}를 사용자의 DB에 저장한다.

카드사는 랜덤한 메시지 인증키 MACKEY를 생성하여 기 생성된 모바일카드 정보와 함께 Signcrypt 알고리즘으로 서명 암호화하여 σ_2 생성 후 사용자에게 전달한다. 메시지 인증키는 결제 결과를 카드사가 사용자에게 전달할 때 사용된다. 이는 서명 암호화보다 가벼운 MAC 알고리즘을 이용함으로써 효율성을 높여준다. 사용자는 Unsigncrypt 알고리즘을 이용하여 카드사로부터 받은 암호문σ_2로부터 모바일 카드번호 VNO와 인증키를 복원한다.

(그림 2) 모바일카드 발급단계



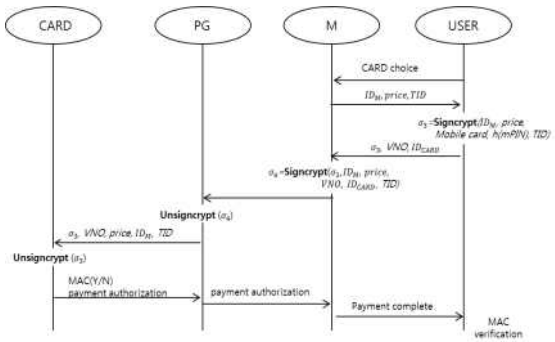
(Figure 2) Phase of Mobile Card Issue

3.2.3 모바일 카드 결제 단계

모바일카드를 이용하여 전자상거래를 할 경우, 사용자는 전자 상점으로부터 선택한 물건과 가격을 확인한 후 모바일카드 결제를 진행한다. 전자 상점은 선택한 상품에 대해 전자 상점의 식별정보 ID_M, 가격 price, 트랜젝션 정보 TID를 사용자에게 전달하고, 사용자는 Signcrypt 알고리즘을 이용하여 ID_M, 가격 price, 모바일카드 정보, $h(mPIN, 기기식별정보)$, 트랜젝션 정보 TID를 서명 암호화한 메시지 σ_3을 모바일카드 번호 VNO, 카드사 식별정보 ID_{CARD}와 함께 전자 상점에 전달한다.

전자 상점은 결제대행사에 결제를 요청하기 위해 수신된 정보에 자신의 식별정보 ID_M, 트랜젝션 정보 TID를 포함하여 Signcrypt하여 전송한다. 결제대행사는 수신된 정보를 복원한 후 σ_3, VNO, price, ID_M, TID를 카드사에 전달한다. 카드사는 결제한 카드정보의 유효성을 검증하고 정상 모바일카드 결제 승인처리 후 해당 결과를 PG 에 통보한다. 이때 사용자에게 전달할 결과 메시지는 MACKEY를 이용하여 MAC값을 생성하여 전달한다.

(그림 3) 모바일카드 결제단계



(Figure 3) Phase of Mobile Card Payment

4. 안전성 및 성능 분석

4.1 안전성 분석

본 논문에서 제안하는 모바일 결제 프로토콜은 ID기반 공개키 시스템의 키 에스크로 문제를 해결한 무인증서 기반의 서명암호화 기법에 기반하여 부분 비밀키와 부분 공개키를 사용하고 있으므로, 서명 암호화된 메시지를 KGC에서 복호화하거나 새로운 메시지에 대한 서명위조를 할 수 없다. 사용자는 모바일 결제정보를 카드사의 공개키와 자신의 개인키를 이용하여 서명 암

호화하여 카드사에 전송함으로써, 키가 없는 전자상점과 PG 및 도청을 통해 정보를 획득하려는 공격로부터 메시지에 대한 기밀성을 보장하고, 메시지 위변조에 대한 무결성을 보장한다. 또한 전자서명을 통해 메시지에 대한 부인방지를 보장하고 있으며, 서명암호화에 사용된 키가 없는 PG와 도청을 통해 정보를 획득하려는 공격자는 모바일 카드번호 VNO외에는 사용자에 대한 어떠한 정보도 얻을 수 없기 때문에, 구매자에 대한 프라이버시를 보호한다.

만약 전자상점과 PG가 결제 정보를 악의적으로 조작하여 이익을 취하려 할 때, 카드사는 사용자가 전송한 정보와 자신이 받은 정보인 VNO, price, TID, 모바일 카드 정보를 확인함으로써, 가격정보 및 카드정보에 대한 변조공격이나 중복 결제를 유발시키는 재전송 공격을 막을 수 있다.

4.2 성능 분석

본 절에서는 제안한 프로토콜과 지은화 등이 제안한 프로토콜[9]의 성능을 비교·분석한다. 지은화 등이 제안한 프로토콜에서는 최초 모바일 카드 발급 시 신용카드 발급기관을 직접 방문해야 하는 불편함이 있으나, 제안하는 프로토콜은 온라인 카드발급이 가능한 장점을 가지고 있다. 그러나 두 프로토콜의 경우 인증서 등록 등 초기화 단계가 서로 상이하기 때문에 본 절에서의 비교 범위에서는 제외하고 결제 단계만을 비교 범위로 한다.

성능 비교를 위해 제안하는 프로토콜의 무인증서 기반 서명암호화 기법은 Xie와 Zhang이 제안한 페어링 없는 무인증서 기반 서명암호화 기법[8]을 사용하였다. 또한 공정한 비교를 위해 지은화 등이 제안한 프로토콜의 암호화 통신용 키를 생성하기 위한 트래픽과 연산과정은 비교 범위에서 제외하였고, 암호화 알고리즘과 전자서명 알고리즘으로 RSAES-OAEP와 KCDSA를 사용하였다.

두 프로토콜의 연산량에 기반한 성능은 <표 2>와 같다. 제안 프로토콜은 지수연산(^), 곱셈(×), 덧셈(+), 뺄셈(-), XOR, 해쉬연산 및 RNG(Random Number Generator)를 이용한 난수생성연산으로 성능을 비교한다. 지은화 등의 프로토콜은 성능향상을 위해 대칭키를 사용하고 있어, 전체 연산량은 본 논문에서 제안한 프로토콜보다 높은 성능을 보이고 있다. 그러나 연산량의 영향을 가장 많이 받는 사용자 측에서의 연산만을 비교했을 때, 가장 큰 연산 비용이 발생하는 지수연산은 동일하게 4번의 연산을 사용하고 있어 사용자 측에서의 전체 연산량에서는 큰 차이가 없다고 할 수 있다.

<표 2> 성능비교표

		^	×	+/-	XOR	Hashing	RNG
Proposed Protocol	USER	4	4	2		6	1
	Market	4	4	2		4	1
	PG	6	4			4	
	CARD	6	4			5	
Jhee's Protocol [9]	USER	4	2	2	6	11	3
	Market	5	3	1	3	7	1
	PG	3	2	1	2	4	1
	CARD	4	1		5	8	1

<Table 2> Performance Comparisons

5. 결론

스마트폰 사용의 증가로 모바일 단말을 이용한 결제가 대중화 되고 모바일카드 이용자의 수도 증가함에 따라 모바일 환경에 적합한 모바일 결제 시스템이 필요하다. 기존 PKI 기반 결제시스템은 공인인증서 사용에 따른 상호 인증과정의 복잡성과 CRL 관리 비용 등의 문제로 모바일 환경에 적합하지 않다. 이에 본 논문에서는 공인인증서를 사용하지 않는 무인증서 서명 암호화 기법을 이용한 모바일카드 결제 프로토콜을 제안하여 기존 PKI 기반 결제 시스템에서의 문제점을 해결하고 모바일 환경에 적합하고 안전한 모바일카드 결제 프로토콜을 제안했다. 제안된 프로토콜은 기밀성, 무결성 및 부인방지는 물론이고 사용자의 프라이버시도 보호함으로써 모바일 결제 서비스에 대한 신뢰도 향상에 도움이 된다. 다만 본 프로토콜을 실제 카드 결제서비스에 적용하기 위해서는 전자상거래 안정성 강화 정책 및 전자금융거래법에 의한 규제 완화가 필요하며, 효율성이 보다 개선되고 안전성이 증명된 무인증서 서명기법에 대한 연구가 선행되어야 할 것이다.

References

[1] http://www.gartner.com/it/page.jsp?id=208315, “Worldwide Mobile Payment Transaction calue to Surpass $171.5 Billion”

[2] A. Shamir. “Identity-based crypto systems and signature schemes.” In Advances in Cryptology, volume 196 of LNCS, pages 47-53. Springer-Verlag, 1985

[3] Kenneth G. Paterson “A comparison between traditional public key infrastructures and Identity-based Cryptography” Information Security Technical Report Volume 8, Issue 3, pp. 57 - 72, July 2003,

[4] M. Barbosa and P.Farshim “Certificateless signcryption” Cryptology eprint archive :report 2008/143. Available from: http://eprint.iacr.org/2008/143.

[5] C. Wu and Z. Chen. “A new efficient certificateless signcryption scheme.” In International Symposium on Information Science and Engineering, ISISE'8., volume 1,pages 661 - 64, 2008.

[6] S.S.D. Selvi, S.S. Vivek, and C.P. Ragan. “On the security of certificateless signcryption schemes.” Cryptology ePrint Archive: Report 2009/298, Available from: http://eprint.iacr.org/2009/298.

[7] W. Xie and Z. Zhang. “Efficient and provably-secure certificateless signcryption from bilinear maps.” Cryptology ePrint Archive: Report 2009/578, Available from: http://eprint.iacr.org/2009/578.

[8] W. Xie and Z. Zhang. “Certificateless Signcryption without Pairing.” Cryptology ePrint Archive: Report 2010/187, Available from: http://eprint.iacr.org/2010/187

[9] Eun wha Jhee, Ae young Kim, Sang ho Lee “Improving the Security of Mobile Credit Card Payment Protocol for USIM-based Smart Phone” Journal of Computing Science and Engineering, 17(4), April 2011.

[10] S. Kungpisdan, B. Srinivasan and P. Le, "A secure account-based mobile payment protocol," Proc. of ITCC 2004, vol.1, pp.35-39, 2004.

[11] X. Wu, O. Dandash and P. Le, "The design and implementation of a smartphone payment system based on limited-used key generation scheme,"Third International Conference on Information Technology: New Generations, pp.458-463, 2006.

[12] X. Wang and N. Cui, "Research of security mobile payment protocol in communication restrictions scenarios," Computational Intelligence and Security, pp.213-217, 2009.

[13] S. Fourati, "Protocol specification core functions of Visa International 3-D security protocol," Wireless Communications, Issue 7, pp.353-360, 2002.

[14] Sang-Kyu Byun "Analysis for the Smart Phone Ecosystem and its Economic Spillover Effects" Journal of Digital Contents Society Vol.12,pp.205-216, 2011.

최 희 진

2009년 : 고려대학교 정보보호대학원
(석사수료)

2007년~2011년: 다음커뮤니케이션 정보보안팀
2011년~현 재: 하나SK카드 정보보안팀
관심분야 : 모바일 결제시스템, EMV, 로그분석

김 형 중

1986년 : 서울대학교 대학원
(공학석사)
1989년 : 서울대학교 대학원
(공학박사-제어계측공학)

1989년~2006년: 강원대학교 교수
2010년~2012년: 국제암호학회 이사
2006년~현재: 고려대학교 정보보호대학원 교수
관심분야 : 멀티미디어 공학, 보안공학, 보안통계