Journal of the Korea Academia-Industrial cooperation Society
Vol. 14, No. 11 pp. 5872-5878, 2013

http://dx.doi.org/10.5762/KAIS.2013.14.11.5872

온라인 소액결제 시스템에서 금융정보 보호를 위한 스마트카드 기반의 프로토콜 설계

이광형[1*], 박정효[2]
[1]서일대학교 인터넷정보과, [2]숭실대학교 컴퓨터학과

A Design of Protocol Based on Smartcard for Financial Information to Protect in E-payment System

Kwang-Hyoung Lee[1*] and Jeong-Hyo Park[2]
[1]**Dept. of Internet Information, Seoil University**
[2]**Dept. of Computer Science, Soongsil University**

요 약 본 논문에서는 기존 온라인 소액결제 시스템의 취약점을 해결하고자 제안 시스템의 구매 요청은 유선망으로 사용자 인증 및 결제 승인 과정은 이동통신사망으로 수행하여 2 Channel 구조를 가지도록 설계하였고, 스마트카드와 스마트폰에 저장된 부분 인자값과 공인인증서의 비밀번호를 활용하여 소지하고 있다는 것과 알고 있는 것에 대한 2 Factor 인증을 지원한다. 또한 스마트카드에 공인인증서를 저장하여 보관상의 안정성을 향상시켰으며, 전자상거래에서 요구하는 가이드라인을 만족시키기 위해 기밀성, 무결성, 인증, 부인방지 등의 특성을 지원한다. 기존 시스템과의 비교 분석을 한 결과 제안 시스템의 효율성 측면에서는 기존 시스템과 큰 차이를 보이지 않았지만 안전성 측면에서는 다양한 위협 요소들에 대한 증명을 통해 안전함을 확인할 수 있었다.

Abstract This study provides two channel structure and two factor authentication. First, a purchasing request by Internet and then user certification and a settlement approval process by mobile communication. Second, it support that proposal protocol utilize a partial factor value of stored in users smartcard, smart phone and password of certificate. Third, storage stability is improved because certificate store in smartcard. Finally, proposal protocol satisfy confidentiality, integrity, authentication, and non- repudiation on required E-commerce guideline. In comparative analysis, Efficiency of the proposal protocol with the existing system was not significantly different. But, In terms of safety for a variety of threats to prove more secure than the existing system was confirmed.

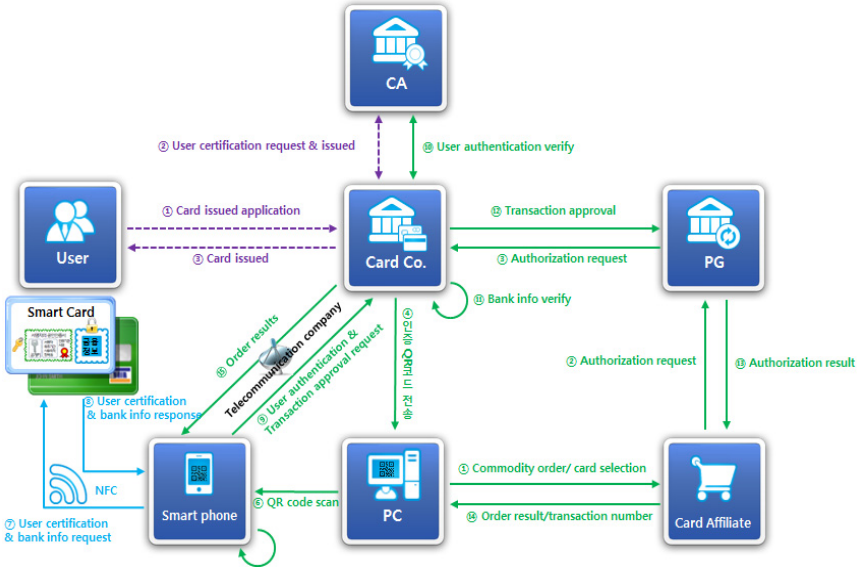
Key Words : Smart-Card, Two-Channel Authentication, Two-Factor Authentication

1. 서 론

1.1 연구배경

정보의 유출 사고는 금융정보가 흘러가는 모든 경로에서 발생할 수 있다[11-13]. 각 구간에서 발생할 수 있는 문제의 대응책으로서 카드사와 PG사는 홈페이지에 접속하거나 카드 결제 시 구매자의 확실한 신원확인 및 부인방지를 위해 인터넷 뱅킹처럼 공인인증서 방식을 채택하여 안전성을 향상할 필요가 있다[9,10]. 또한, 거래내역 조회는 카드사에서 일괄적으로 제공해야 하며 가맹점과 PG사는 구매자에 대한 일체의 금융정보를 인지하거나 저장하고 있지 말아야 한다. 그리고 사용자의 인증서를 안전하게 보관할 필요가 있고 제삼자로부터의 해킹시도를 차단할 수 있도록 사용자 인증 및 결제 승인을 위한

본 논문은 2012년도 서일대학교 학술연구비에 의해 연구되었음.
*Corresponding Author : Kwang-Hyoung Lee(Seoil Univ.)
Tel: +82-2-490-7226 email: dreamace@seoil.ac.kr
Received September 25, 2013 Revised October 23, 2013 Accepted November 7, 2013



[Fig. 1] Configuration of a proposed system

별도의 안전한 채널을 구축해 요청과 응답을 분리하여 처리하는 기술이 필요하다[1,4]. 본 논문은 상위에서 언급한 내용을 실현하기 위해 스마트카드, 스마트폰, NFC, QR코드 등 다양한 기술과 접목하여 구매자의 금융정보 유출을 방지하는 스마트카드 기반의 안전한 소액결제 프로토콜을 제안한다.

본 논문의 구성은 4장으로 이루어져 있으며, 각 장의 내용은 다음과 같다. 제 2장은 제안 내용으로 기존 소액결제 시스템의 취약점을 고려해 스마트카드에 사용자의 공인증서와 암호화된 카드정보를 저장하고 스마트폰을 이용하여 이동통신사망을 통해 사용자 인증 및 결제 승인을 수행하는 안전한 소액결제 시스템을 제안한다. 제 3장은 제안 내용의 구현을 제시하고 기존 시스템과의 비교 분석 및 성능 평가를 함으로써 제안 시스템의 안전성을 증명한다. 제 4장은 본 논문의 결론을 제시하고 향후 연구 및 방향에 대해 기술한다.

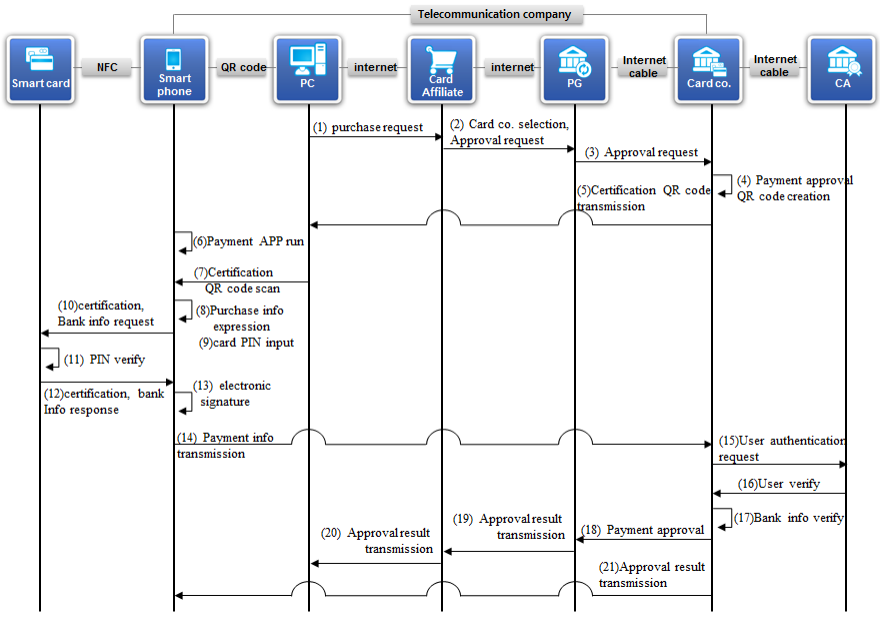
2. 본 론

2.1 제안시스템의 구성

기존 온라인 소액결제 시스템의 취약점을 보완하고자 본 논문에서는 스마트카드에 저장된 공인인증서로 금융정보를 전자서명하여 스마트폰을 통해 카드사로부터 사용자 인증 및 결제 승인을 직접 수행하는 구조로 가맹점과 PG사에 사용자의 금융정보를 노출하지 않는 프로토콜을 제안하였다. 시스템의 전체 구성은 Fig. 1과 같다.

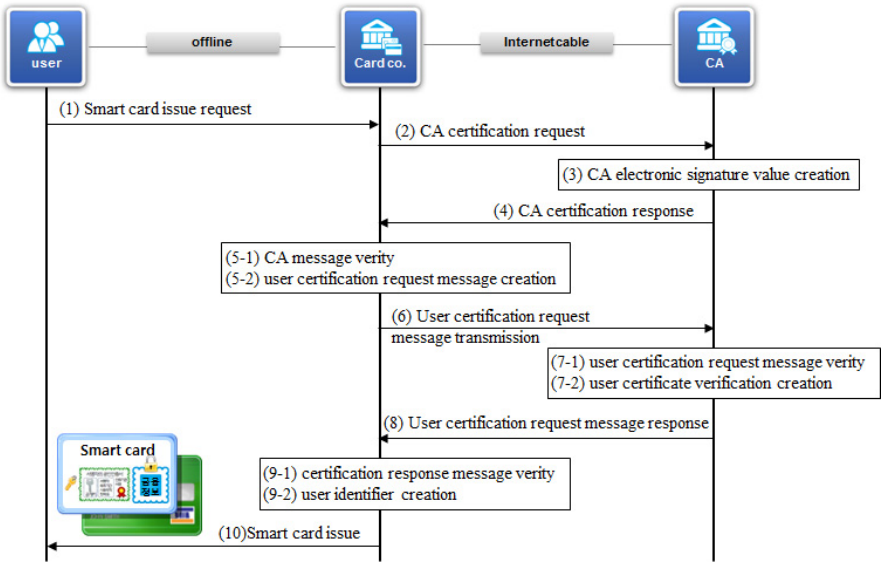
사용자는 PC, 스마트폰, 스마트카드를 활용하여 온라인 소액결제 시스템을 이용한다. 사용자는 PC를 통해 가맹점의 사이트에 접속하여 원하는 물품을 선택한 후 결제 승인을 받기 위한 Plug-in 프로그램을 실행하고, 대칭키 알고리즘인 SEED 암호화를 통해 PC에서 PG사 구간까지 안전한 채널을 형성할 수 있다. Plug-in의 결제 유형을 신용카드로 선택한 후 해당 카드사를 선택하고 PG사로 결제를 위한 승인 요청을 한다. 승인 요청을 받은 PG사는 선택된 카드사로 해당 사용자의 승인 요청을 재전송한다. 카드사는 PG사로부터 받은 사용자의 정보를 DB에 임시로 저장해 놓고 해당 사용자의 인증 및 결제 승인을 위한 QR코드를 생성한 후 사용자의 PC로 QR코드 메시지를 전송한다. 이때 QR코드의 역할은 구매정보와 사용자 인증 및 금융정보 요청메시지를 스마트폰으로 전달함으로써 2 Channel 구조를 형성하기위한 정보전달의 매개체로 활용한다.

사용자는 스마트폰의 결제 Application을 실행시켜 QR코드의 정보를 읽어온 후 화면에 구매정보를 나타내어 자신이 구매한 내역이 맞는지 확인하고, 스마트폰의 NFC 기능을 활용하여 스마트카드에 저장되어있는 공인인증서와 금융정보를 전송받게 된다. 여기서 스마트카드의 정보를 가져올 때 PIN번호를 통해 세션키를 생성하고 NFC 구간의 안전한 채널 및 카드소지자에 대한 1차 사용자 인

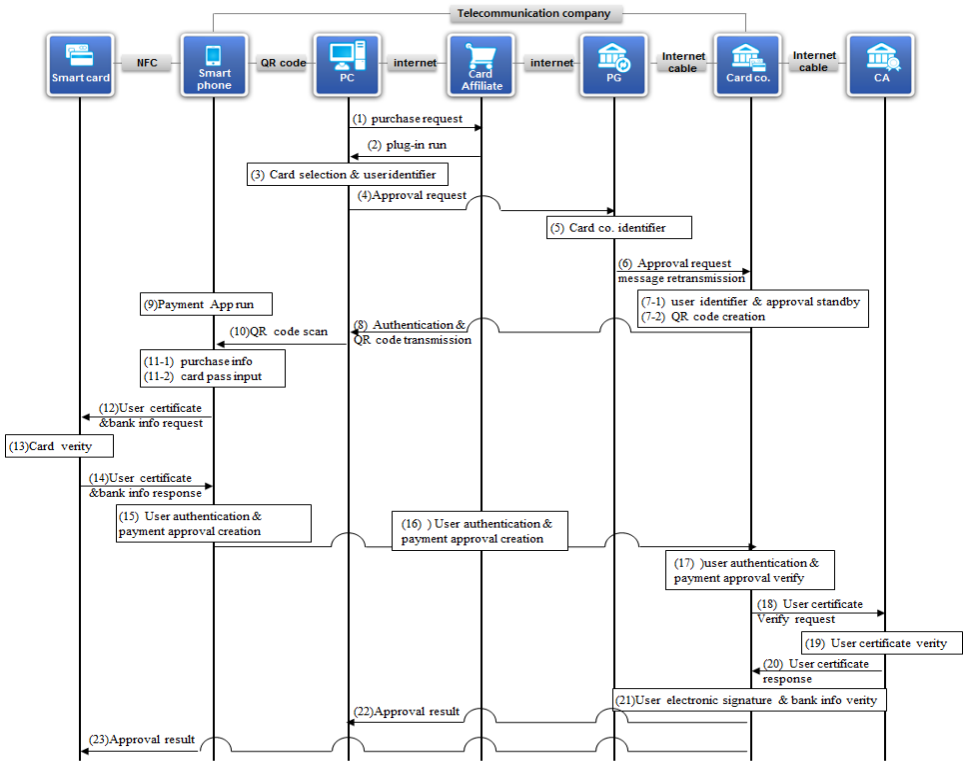


[Fig. 2] System Flow of a proposed system

증을 실행한다. 또한, 스마트카드와 스마트폰은 사전에 카드사로 부터 카드를 발급 받을 때 부여받은 부분 인자 값을 통해서 전자서명에 필요한 인자 값을 생성하는데 필요하므로 둘 중 하나를 분실했다 하더라도 도용해서 사용할 수 없는 구조를 가진다. 다음으로 사용자는 공인 인증서의 비밀번호를 입력하여 구매정보에 RSA 알고리즘으로 전자서명을 생성 한 후에 카드사의 공개키로 암호화된 금융정보와 같이 이동통신사망을 통해 카드사로 데이터를 전송한다. 스마트폰과 카드사간의 채널은 기존 PC단에서 발생할 수 있는 해킹으로부터의 위협을 차단할



[Fig. 3] Enroll Protocol



[Fig. 4] Payment Protocol

수 있고, PKI 기반 구조를 통해 암호화된 채널을 형성하여 안전성 있는 통신채널을 구축할 수 있다. 카드사는 이동통신사망을 통해 수신한 데이터를 임시 DB에 저장하고 인증기관으로부터 해당 사용자에 대한 신원확인 절차를 거쳐 사용자 인증을 수행한 후에 카드사의 개인키로 금융정보를 복호화하여 사용자의 결제 정보가 맞는지 검증을 수행한다. 결제 정보에 대한 검증이 완료되면 카드사는 결제 승인 내역을 저장하고 모든 참여자에게 결제 완료정보를 전송한다. 그리고 사용자는 차후에 승인내역을 검색할 때에는 PG사가 아닌 카드사로부터 해당 내역을 직접 검색함으로써 보다 안전하고 엄격하게 금융정보를 관리할 수 있다. 제안하는 프로토콜의 전체적인 시스템의 흐름은 Fig. 2와 같다.

2.2 상세 프로토콜

제안 시스템은 안전한 온라인 소액결제를 위해 사용자와 카드사간 직접 사용자 인증 및 결제 승인을 받는 구조로 등록 프로토콜, 결제 프로토콜, 공인인증서 갱신 프로토콜로 나누어 자세히 설명한다.

2.2.1 등록 프로토콜

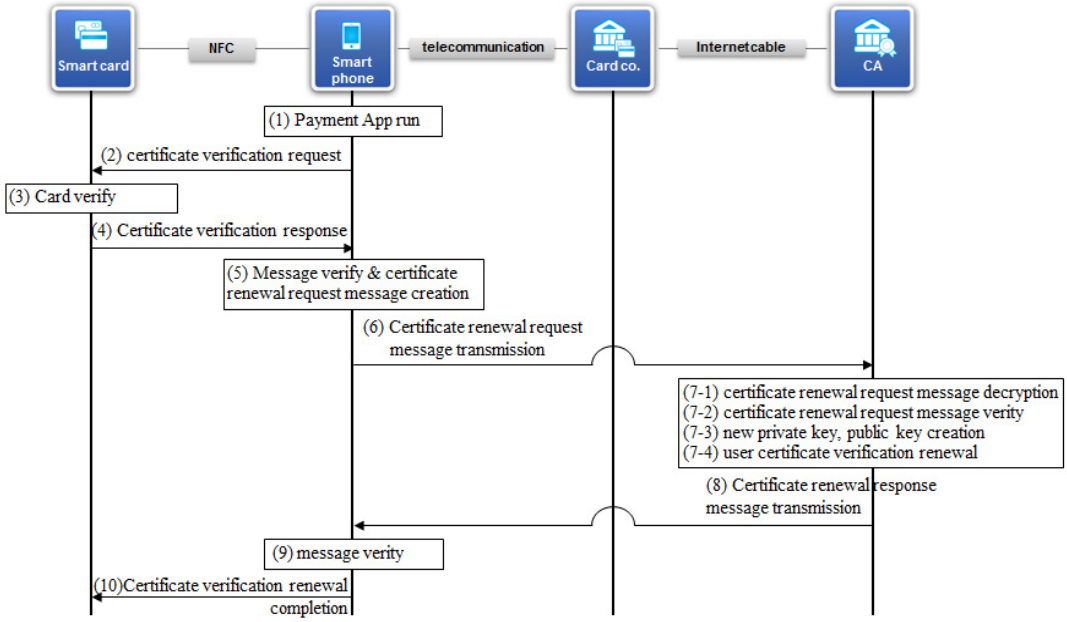
등록 프로토콜은 사용자가 카드사를 직접 방문하여 대면으로 확실한 신원 인증을 거쳐 스마트카드를 발급받는다. 이때 스마트카드에는 사용자 인증을 위한 공인인증서와 카드사의 공개키로 암호화된 금융정보 및 전자서명에 필요한 부분 인자값 등을 포함하고 있다. 등록 프로토콜의 상세 절차는 Fig. 3과 같다.

2.2.2 결제 프로토콜

결제 프로토콜은 안전한 소액결제 시스템을 이용하기 위해 스마트폰, 스마트카드 등의 요소를 활용하여 사용자와 카드사간 직접적으로 사용자 인증 및 결제 승인을 받는 구조이다. 결제 프로토콜의 상세 절차는 Fig. 4와 같다.

2.2.3 공인인증서 갱신 프로토콜

사용자는 스마트카드에 저장되어있는 공인인증서의 유효기간이 만료되면 카드사를 직접 방문하지 않고 스마트폰을 통해 사용자의 공인인증서를 갱신할 수 있다. 상세 프로토콜은 Fig. 5와 같다.



[Fig. 5] Update Certification Protocol

3. 성능분석

3.1 안전성 분석

본 절에서는 제안하는 프로토콜의 안정성을 전자금융 거래 시 인증방법에 대한 가이드라인을 기반으로 하여 무결성, 기밀성, 인증, 부인방지 등의 항목으로 구분하여 제안 시스템의 안전성을 분석하였다. 다음 Table 1는 기존 시스템과 제안 시스템의 안전성에 대한 비교분석을 기술한 내용이다.

[Table 1] Comparative analysis of the existing system

separate	Key-in	relax click	ISP	propose system
integrity	O	O	O	O
security	O	O	O	O
certification	O	O	O	O
non-repudiation			O	O
certificate management convenience				O
2 Channel structure				O
2 Factor certification				O

3.2 거래 수단에 따른 보안성 분석

[Table 2] Comparative analysis of the existing authentication methods

separate	propose system	existing system		
		relax click	ISP	Key-in system
storage method	smart card	user memory	PC	user memory
input method	smart phone	keyboard	keyboard	keyboard
certification path	mobile communication	internet communication	internet communication	internet communication
outflow course	robbery, lost	PC hacking, PG hacking	PC hacking, PG hacking	PC hacking, PG hacking, robbery, lost
channel cipher	PKI	SSL	PKI	SSL
attack method	-	keyboard hacking memory hacking	keyboard hacking memory hacking, remote control	keyboard hacking memory hacking

제안 시스템과 기존 소액결제 시스템의 인증 방식을 비교 분석 하면 Table 2와 같다. 소액결제 인증요소들의 보관 수단은 금융정보, ISP 인증서 비밀번호, 안심클릭

비밀번호와 같은 사용자의 기억에 의존하는 요소들이 있다. 인증을 위한 값을 입력하는 방식으로 키보드를 통해 이뤄진다. 제안 시스템은 PC의 키보드가 아닌 스마트폰을 통해 이동통신사 망을 이용하여 입력하는 방식을 취하고 있다. 각각의 인증을 위한 수단별로 유출 방식을 살펴보면 사용자의 PC를 해킹하여 금융정보의 유출이 발생할 수 있으며, 물리적인 인증요소는 도난 및 분실을 통하여 유출이 일어날 수 있다. 인증 수단별 공격 방법으로는 키로깅, 백도어, 피싱 등과 같은 알려진 해킹 방법을 통하여 공격이 일어날 수 있다. 하지만 제안하는 시스템은 스마트카드의 고유정보와 공인인증서를 통하여 기존 시스템의 SSL 암호화 채널보다 PKI구조의 통신 채널을 형성하여 안전한 거래를 할 수 있다.

4. 결 론

본 논문은 기존 시스템에 존재하는 취약점을 보완하고자 스마트카드에 저장된 공인인증서로 금융정보를 전자서명하여 스마트폰을 통해 카드사로부터 사용자 인증 및 결제 승인을 받는 구조로 가맹점과 PG사에 사용자의 금융정보를 노출하지 않는 프로토콜을 제안하였다.

제안하는 프로토콜은 온라인 소액결제 시스템의 보안성을 향상 시킬 수는 있지만, 기존 PC단에서 처리하던 인증 및 결제 업무를 스마트폰으로 연장시켰기 때문에 사용자의 번거로움을 초래할 수 있다. 그렇지만 사용자의 사용성을 향상시키기 위해 QR코드를 정보전달의 매개체로 사용함으로써 PC의 정보를 스마트폰으로 손쉽게 공유할 수 있다.

기존의 시스템은 가맹점과 PG사에서 보관하고 있는 금융정보가 유출될 수 있으며 공인인증서 갈취, 메모리 해킹, 키로깅 등 다양한 형태의 위협에 노출되는 구조적 한계점을 가지고 있다. 그래서 제안 시스템의 구매 요청은 유선망으로 사용자 인증 및 결제 승인 과정은 이동통신사망으로 수행하도록 2 Channel 구조로 설계하였고, 스마트카드 소지자에 대한 비밀번호 인증과 공인인증서 인증을 통해 2 Factor 사용자 인증을 거치도록 하였다. 또한 스마트카드에 공인인증서를 저장하여 보관의 안정성을 높였고, 전자상거래에서 요구하는 가이드라인을 만족시키기 위해 기밀성, 무결성, 인증, 부인방지 등의 요건을 충족시켰다.

향후 제안한 시스템을 현재의 온라인 소액결제 시스템에 적용하기 위해서는 참여 주체자간의 역할 분담에 대한 조율이 필요하고, 결제 시스템의 익명성과 부정 사용자에 대한 추적 등 다양한 보안기법과 연계하여 시스템의 안전성 향상에 꾸준한 노력을 해야 한다. 그리고 아직까지 알려지지 않은 공격 유형에 대한 연구와 분석이 필요할 것이다.

References

[1] *Ki-young Kim, "A one-time password-based authentication system for Consideration", proceeding of KIISC, Vol.17 No.3, pp.26-31, 2007.*

[2] *Yi-Roo Baek, Doo-Hwan Oh, Kwang-Eun Gil and Jae-Cheol Ha1, "Implementation of a Remote Authentication System Using Smartcards to Guarantee User Anonymity to Third Party", Journal of KAIS, v.12, no.5, pp.2322-2326, 2011.*
DOI: http://dx.doi.org/10.5762/KAIS.2009.10.10.2750

[3] *Wang-Seong Park, Jong-Pil Jung, Chang-Sub Park, Dong-Hoon Lee, "Password authentication protocol for Consideration", proceeding of KIISC, Vol.9 No.4, pp.51-63, 1999.*

[4] *Cheol-Oh Kang, Joong0Gil Park, Soon-Jwa Hong, Byung-Cheol Bae, "A Study on the Algorithm of Improved One-Time Password using Time and Time Correction", The KIPS Transactions : Part 8-C No.4, pp.373-378, 2001.*

[5] *Je-Ho Song, "Design of Inner Key scheduler block for Smart Card", Journal of KAIS, v.11, no.12, pp.4962-4967, 2011.*
DOI: http://dx.doi.org/10.5762/KAIS.2010.11.12.4962

[6] *Je-Ho Song, Woochoun Lee, "The Design of Hybr id Cryptosystem for Smart Card", Journal of KAIS, v.12, no.5, pp. 232-2326, 2011.*

[7] *Sung-Woon Lee, Hyun-Sung Kim, Kee-Young Yoo, "A Password - based Efficient Key Exchange Protocol", Journal of KIISE : Information Networking Vol.31 No.4, pp.347-352, 2004.*

[8] *Dong-Hyun Choi, Seung-Joo Kim, Dong-Ho Won, "One-time password Technical Analysis and Standardization", proceeding of KIISC, Vol.17 No.3, pp.12-17, 2007.*

[9] *Eun-Jeong Choi, Chan-Oe Kim, Joo-Seok Song, "Password-Based Authentication Protocol for Remote Access using Public Key Cryptography", Journal of KIISE : Information Networking, Vol.30 No.1, pp.75-83, 2003.*

[10] *Jong-Seok Choi, Seung-Soo Shin, Kun-Hee Han, "Three-Party Key Exchange Protocol Providing Usser*

Anonymity based on Smartcards", Journal of KAIS, v.10, no.2, pp.388-395, 2009.
DOI: http://dx.doi.org/10.5762/KAIS.2009.10.2.388

[11] J.Lv and Y.Han, "Enhanced DES Implementation Secure Against High-Order Differential Power Analysis in Smartcards", ACISP 2005, LNCS 3502, pp.195-206, 2005.
DOI: http://dx.doi.org/10.1007/11506157_17

[12] J.R.Rao, P.Rohatgi and H. Scherzer, "Partitioning Attacks: Or How to Rapidly Clone Some GSM Cards". IBM Watson Research Center, in 2002 IEEE Symposium on Security and Privacy, Oakland, CA, May 2002.
DOI: http://dx.doi.org/10.1109/SECPRI.2002.1004360

[13] L.Goublin and J.Patarin, "DES and differential power analysis", in proceedings of Workshop on Cryptographic Hardware and Embedded Systems, Springer-Verlag, 1999.

[14] T.S.Messerges, E.A.Dabish and R.H.Sloan, "Investigation of Power Analysis Attacks on Smartcards", in Proceedings of USENIX workshop on Smartcard Technology, pp.151-161, May 1999.

[15] Y.S.Son and D.H.Lee, "The Key Management System using the Secret Sharing Scheme Applicable to Smart Card", KIPS Transaction, VOL.11-C, NO 5, pp.373-378, 2004.
DOI: http://dx.doi.org/10.3745/KIPSTC.2004.11C.5.585

[16] S. Ha, D. Park, "Image Features Based Secure Access Control for Data Content Protection", Journal of The Institute of Webcasting, Internet and Telecommunication, Vol 13, No 1, pp. 171~180, 2013.

[17] T.-H. Kim, H.-G. Kang, Y.-H. Kim, S.-H. Cho, "A Study of License acquisition Method Supporting Mutual Compatibility of EPUB-based eBook DRM", Journal of The Institute of Webcasting, Internet and Telecommunication, Vol 13, No 1, pp. 205~214, 2013.

[18] Y.-H. An, Y.-D. Joo, "Security Enhancement of Biometrics-based Remote User Authentication Scheme Using Smart Cards", Journal of The Institute of Webcasting, Internet and Telecommunication, Vol 12, No 1, pp. 231~237, 2012.

[19] H. Han, N. Kim, "Mobile Message Platform Supporting Dynamic Services based on Templates", Journal of The Institute of Webcasting, Internet and Telecommunication, Vol 12, No 2, pp. 19~27, 2012.

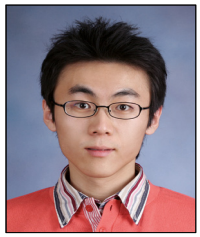
[20] Y.-D. Joo, "Security Improvements on Smart-Card Based Mutual Authentication Scheme", Journal of The Institute of Webcasting, Internet and Telecommunication, Vol 12, No 6, pp. 91~98, 2012.

이 광 형(Kwang-Hyoung Lee) **[종신회원]**

- 1998년 2월 : 광주대학교 컴퓨터공학과 졸업 (공학사)
- 2002년 2월 : 숭실대학교 컴퓨터공학과 (공학석사)
- 2005년 2월 : 숭실대학교 컴퓨터공학과 (공학박사)
- 2005년 3월 ~ 현재 : 서일대학 인터넷정보과 부교수

<관심분야>
멀티미디어 데이터 검색, 영상처리, 멀티미디어 보안, DRM, USN, 학습콘텐츠

박 정 효(Jeong-Hyo Park) **[정회원]**



- 2009년 2월 : 숭실대학교 컴퓨터학과 졸업 (공학사)
- 2011년 2월 : 숭실대학교 일반대학원 정보보안 (정보보안석사)
- 2011년 3월 ~ 현재 : 숭실대학교 일반대학원 컴퓨터공학과 (박사수료)

<관심분야>
정보통신, 통신보안, 암호이론