Journal of the Korea Academia-Industrial cooperation Society
Vol. 13, No. 10 pp. 4814-4821, 2012

http://dx.doi.org/10.5762/KAIS.2012.13.10.4814

전자여권의 향상된 채널생성 기법 설계

이기성[1], 전상엽[2*], 전문석[2]
[1]호원대학교 컴퓨터게임학부, [2]숭실대학교 컴퓨터학부

A Design of Advanced Channel Creation in e-Passport

Gi-Sung Lee[1], Sang-Yeob Jeon[2*] and Moon-Seog Jun[2]
[1]**Department of Computer & Game, Howon University**
[2]**Department of Computer Science, SoongSil University**

요 약 전자여권은 기존의 여권정보에 비접촉식 스마트 기능의 IC칩을 추가하여 바이오 정보를 탑재한 것으로 전자여권의 보안 위협으로부터 보호하기 위해 BAC, PA, AA, EAC 메커니즘을 사용하고 있다. 그러나 BAC 메커니즘에 사용되는 암호 키는 MRZ 값들의 조합으로 만들어 지기 때문에 MRZ 조합규칙을 알아낸 후 무차별 공격 프로그램을 사용하여 암호 해독이 가능한 단점이 있다. 본 논문은 전자여권 칩과 판독시스템간의 안전한 채널 형성 시 해시된 이미지 정보와 지문 정보를 이용하여 전자여권의 위·변조를 확인하고 타임스탬프 값을 통하여 효율성이 향상된 메커니즘을 제안하였다.

Abstract An e-passport is equipped with bio information by adding the non-attachable IC chip with a smart function. In order to solve such a problem, the user's privacy is protected by using the BAC, PA, AA and EAC mechanisms. However, the password key used in the BAC mechanism is made of the combination of the MRZ values. As a result, it is possible to decode the password by using the indiscriminate attacking program after finding out the combined rules of MRZ.
This thesis suggests the mechanism with an improved level of efficiency through the time-stamp values by using the information of images and fingerprints and checking the forge or falsification of the e-passport when establishing a safe channel between the chip of the e-passport and the decoding system.

Key Words : e-Passport, BAC, RFID, Hash,, Digital Signatures, security

1. 서론

전자여권은 기존의 여권정보에 비접촉식 스마트 기능의 IC(Integrated Circuit) 칩을 추가하여 바이오정보를 탑재한 것이다. 전자여권은 새로운 형태의 출입국 관리 시스템으로 기존의 여권보다 보안 기능이 강화되고 자동화된 출입국 관리를 할 수 있는 장점으로 인해 전 세계적으로 도입하기 위한 연구가 진행되고 있다[1].

전자여권의 개인 식별 기술은 전자여권 칩과 판독 시스템 사이의 물리적인 접촉 없이 인식이 가능한 장점이 있는 반면에 skimming, 데이터의 위·변조, 바이오정보 노출, 여권 복제 등의 개인 신원 정보 침해 문제를 야기할 수 있다. 이러한 문제를 해결하기 위해 ICAO에서는 많은 연구가 진행되어 왔으며, 표준 지침으로 정해지고 있는 PA, BAC, AA와 같은 전자여권 인증 메커니즘이 있다. 또한 유럽연합을 중심으로 EAC 메커니즘을 사용하여 사용자의 프라이버시를 보호하고 있다.

RFID의 리더기는 암호 키를 제공하기 전에는 잠겨있어 안전하다. 그러나 암호 키는 MRZ의 값들의 조합으로 만들어지기 때문에 MRZ 조직규칙을 알아낸 후 무차별 공격 프로그램을 사용하여 암호 해독이 가능하다[2].

따라서 본 논문에서는 BAC 메커니즘에서 전자여권의

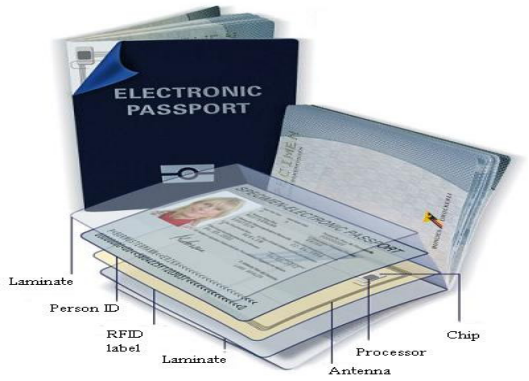
본 연구는 2012년도 호원대학교 학술연구조성비 지원에 의하여 연구되었음.
*Corresponding Author : Sang-Yeob Jeon
Tel: +82-10-4059-4377 email: yeobi0070@naver.com
접수일 12년 09월 11일 수정일 12년 10월 05일 게재확정일 12년 10월 11일

이미지 정보와 지문 정보의 변경여부를 확인함과 동시에 타임스탬프를 이용하여 효율성과 안정성이 뛰어난 메커니즘을 제안한다.

2. 관련연구

2.1 전자여권의 개념

전자여권은 UN 산하 국제민간항공기구와 국제 표준화 기구의 국제 규격에 따라 바이오 정보를 내장한 IC칩이 탑재된 기계 판독식 여권을 말한다. IC칩에는 여권번호, 인적사항 등이 신원 정보 면에 기재되어 있는 정보와 얼굴, 지문, 홍채 이미지와 같은 바이오 정보가 수록되어 져있다. 그림 1은 전자여권의 구성을 보여주고 나타내며, 신원정보면, ICAO로고, 비접촉시 IC칩, MRZ로 구성된다[3].



[그림 1] 전자여권 구성
[Fig. 1] The configuration of the e-passport

2.2 전자여권의 보안기술

2.2.1 BAC(Basic Access Authentication)

BAC는 전자여권 칩에 저장된 데이터들이 공격자들에게 불법적으로 읽히는 것을 방지하고, 전자여권 칩과 판독시스템 간에 전송되는 정보를 도청하지 못하도록 전자여권 칩과 판독시스템 간 안전한 통신 채널을 구성하기 위한 접근통제 메커니즘이라 할 수 있다.

판독시스템은 전자여권 신원정보면의 기계판독영역 정보에서 여권번호, 생년월일, 여권 만기일과 각각의 검증 숫자를 OCR 리더로부터 읽어 들인다. 이를 통해 판독기와 전자여권 칩 사이에서 안전한 메시지 교환을 위해 사용되는 세션키를 유도해 내고, 전자여권 칩과 판독기간 안전한 통신채널을 구성하게 된다[4].

2.2.2 PA(Passive Authentication)

PA는 전자여권 칩의 LDS에 포함되어 있는 정보가 수정되지 않았음을 알려주며, 이 메커니즘은 Document Security Object를 사용한다. 이것은 전자여권 발행 기관이 암호화 방식을 적용하여 여권 속의 칩에 대한 정보를 저장하고, 해쉬를 이용하여 전자적인 서명을 통해 칩 안의 정보를 암호화 한다.

Document Security Object 서명 값의 해쉬를 인증하는 방식은 DOS와 LDS를 비교하여 정보가 일치하였을 경우 데이터가 변경되지 않았음을 증명함으로써 인증을 수행한다[5].

2.2.3 AA(Active Authentication)

AA는 전자여권 칩의 데이터 복제나 전자여권 칩의 대체와 같은 보안 위협으로부터 전자여권을 보호하기 위한 메커니즘으로 강제사항이 아니라 전자여권 발행국의 선택사항이다. AA 기술은 칩안에 내장된 키 쌍을 이용해 판독기와 전자여권 내의 칩과 질의-응답 방식의 인증 방법을 사용하여 칩이 복제되지 않았음을 알아내게 된다. 공개키는 LDS 구조 중 Data Group 15에 저장되며 공개키는 RFC 3280의 SubjectPublickeyInfo구조로 ASN.1 DER 인코딩되어 있으며 이 방법은 전자여권 내의 LDS 구조 중 DG15의 공개키정보를 이용하여 해쉬값 생성후 Document Security Object에 저장하고, 해쉬값에 발행 국가의 전자서명을 포함한다. 이 과정에서 비밀키는 전자여권에 내장된 칩의 안전한 메모리 영역에 보관되어 노출되지 않는다.

2.2.4 EAC(Extended Access Control)

EAC은 전자여권 칩에 저장된 바이오 정보를 권한이 없는 국가에게 정보를 열람할 수 없도록 방지하는 접근통제 메커니즘이다. BAC 보안 채널 생성 이후 Diffie-Hellman 알고리즘을 사용한 키 동의 방식을 통해 더욱 더 안전한 보안 채널을 생성한다. 그 후, 각 여권 발행국 CVCA가 발급한 인증서가 탑재된 판독기임이 판명된 경우에만 바이오 정보를 제공하도록 되어 있다. 즉 검증할 수 있는 키를 제공받은 국가들에게만 전자여권 칩 내에 저장되어 있는 바이오 정보들을 제공하게 된다[6-13].

3. 제안하는 인증 메커니즘

본 논문에서 제안하는 인증 메커니즘은 바이오 정보의 해시 값을 이용하여 안전한 채널이 형성되기 이전에 전

자여권의 위·변조에 안전성을 제공하며 타임스탬프 값을 이용하여 리더기에 대한 인증 및 전자여권 칩과 판독 시스템 사이의 연산을 감소시킬 수 있는 인증 메커니즘을 제안한다. 따라서 본 장에서는 전체 메커니즘을 위·변조 검사 메커니즘과 키 생성 및 인증 메커니즘으로 구분하여 기술한다.

3.1 메커니즘에 사용되는 파라미터

· RNDChip ∈ R{0,1}64 : 칩에서 생성한 64비트 난수
· RNDIS ∈ R{0,1}64 : IS에서 생성한 64비트 난수
· IDReader : 리더기 아이디
· ‖ : 연접
· PN : 전자여권 번호
· (H_IMG), (H_IMG)` : 해시된 사진정보
· (H_fprint), (H_fprint)` : 해시된 지문정보
· Timestamp : 키생성을 위한 시간 정보
· hash : 해시함수
· ⊕ : 배타적 논리합
· KENC : 사전에 공유된 암호키
· KMAC : 사전에 공유된 MAC키
· Kseed : 안전한 채널을 유지하기 위한 키
· DSCert : DS인증서
· CRL : 인증서 폐기 목록
· KPubDS : DS인증서에 있는 공개키
· Passport_Info : DS의 개인키로 전자 서명된 전자여권 정보

3.2 위 · 변조 검사 메커니즘

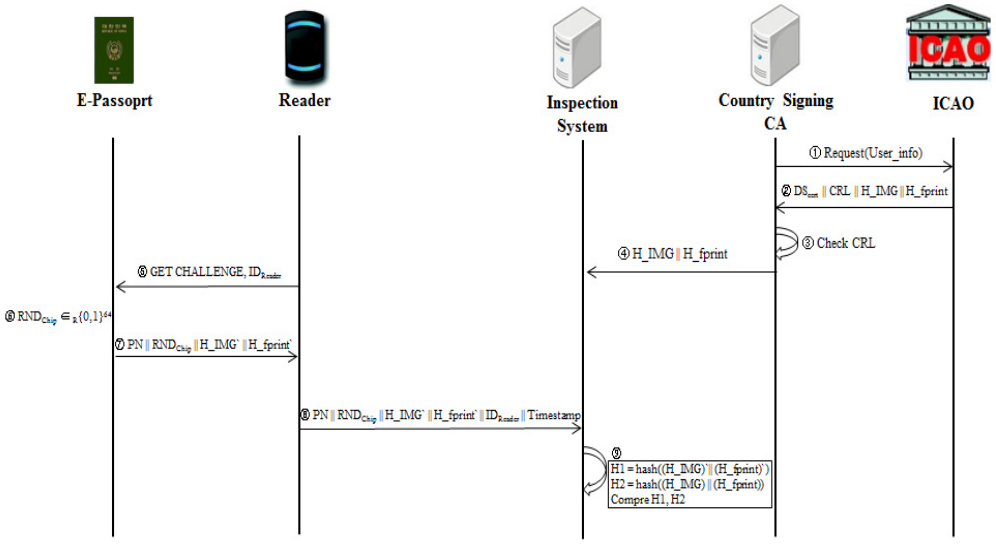
그림 2는 위·변조를 검사하기 위한 메커니즘으로 CSCA(Country Signing CA)는 전자여권 소지자의 해시된 이미지 정보와 지문 정보를 ICAO부터 내려 받게 되고 다시 에게 전달하게 된다.

판독 시스템은 전자여권을 확인하기 위해서 전자여권에서 보내온 해시된 이미지 정보와 지문 정보를 해시하여 해시하고 자신이 소유하고 있는 해시된 이미지 정보와 지문 정보를 각각 해시하여 비교함으로써 전자여권의 위·변조를 확일 할 수 있다. 세부내용은 다음과 같다.

Step 1 : CSCA에서 입국자의 정보를 ICAO에 요청한다.
① Request(User_info)
Step 2 : ICAO는 입국자를 확인하기 위한 정보인 즉 DS인증서, CRL, 해시된 이미지 정보와 지문 정보를 CSCA로 보낸다.

① DScert ‖ CRL ‖ H_IMG ‖ H_fprint
Step 3 : CRL 목록을 검사하여 전자여권의 유효한지를 판별한다.

① Check CRL
Step 4 : 판독 시스템은 CSCA로부터 전자여권의 해시된 이미지 정보와 지문 정보를 받는다.



[그림 2] 위·변조 검사 메커니즘
[Fig. 2] Forgery checking mechanism

① (H_IMG) ‖ (H_fprint)

Step 5 : 리더기는 자신의 고유 식별 ID를 전송함과 동시에 임의 값을 요청한다.

① GET CHALLENGE, IDReader

Step 6 : 칩은 8바이트의 임의 값을 생성한다.

① RNDChip ∈{0,1 }64

Step 7 : 여권번호, 칩의 임의 값, 해시된 이미지 정보와 지문 정보를 연접하여 리더기에 전송한다.

① PN ‖ RNDChip ‖ (H_IMG)` ‖ (H_fprint)`

Step 8 : 리더는 칩에게서 받은 여권 번호, 임의 값, 해시된 이미지 정보, 지문 정보와 리더기 고유 식별 ID 그리고 현재 시간을 연접하여 판독 시스템에 전송한다.

① PN ‖ RNDChip ‖ H_IMG ‖ H_fprint ‖ IDReader ‖ Timestamp

Step 9 : 전자여권에서 받은 해시된 이미지 정보와 지문 정보를 다시 한 번 해시하여 H1을 생성한다.

① H1 = hash((H_IMG)`‖ (H_fprint)`)
CSCA에서 받은 해시된 이미지 정보와 지문 정보를 다시 한 번 해시하여 H2를 생성한다.

② H2= hash((H_IMG)‖ (H_fprint))
H1 값과 H2 값을 비교함으로써 전자여권의 위·변조를 확인한 수 있다.

③ Compre H1, H2

3.3 키 생성 및 인증 메커니즘

그림 3은 키 생성 및 인증 메커니즘으로 난수와 타임스탬프 값 그리고 H1 값들을 통하여 서로 공통된 Kseed를 생성하게 되고 Kseed를 통하여 안전한 채널을 형성할 수 있다. 그 후 DS인증서의 공개키를 이용하여 전자여권의 정보를 풀어봄으로써 전자여권의 개인 정보를 확인할 수 있다. 세부 절차는 다음과 같다.

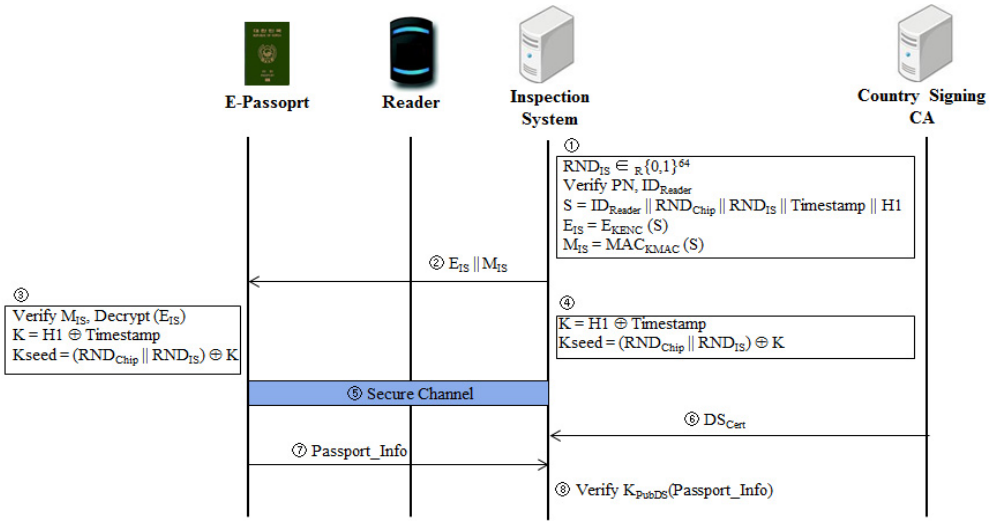
Step 1 : 판독시스템은 64비트의 임의 값을 생성

① RNDIS ∈{0,1 }64
판독시스템에서 전자여권 번호와 리더기의 고유 식별 ID를 확인한다.

② Verify PN, IDReader
리더기의 고유 식별 ID, 칩과 판독시스템의 임의 값, 타임스탬프 그리고 H1을 연접하여 S를 생성한다.

③ S = IDReader ‖ RNDChip ‖ RNDIS ‖ Timestamp ‖ H1
BAC 인증용 암호 키인 KENC를 이용하여 S를 암호화 하여 EIS를 생성한다.

④ EIS = EKENC (S)
BAC 인증용 MAC 키인 KMAC를 이용하여 S의 해시 값인 MIS를 생성한다.



[그림 3] 키 생성 및 인증 메커니즘
[Fig. 3] Key generation and authentication mechanisms

⑤ MIS = MACKMAC (S)

Step 2 : 암호 값과 MAC 값을 연접한 값을 판독 전자여권에 전송한다.

① EIS ‖ MIS

Step 3 : MIS를 통하여 무결성을 확인하고 EIS의 값을 확인한다.

① Verify MIS, Decrypt (EIS)

16바이트 키를 생성하기 위해 H1과 타임스탬프를 XOR 연산하여 K를 생성한다.

② K = H1⊕Timestamp

칩과 리더기의 임의 값을 연접한 결과에 K를 XOR하여 Kseed를 생성한다.

③ Kseed = (RNDChip ‖ RNDIS)⊕K

Step 4 : 16 바이트 키를 생성하기 위해 H1과 타임스탬프를 XOR 연산하여 K를 생성한다.

① K = H1⊕Timestamp

칩과 리더기의 임의 값을 연접한 결과에 K를 XOR하여 전자여권에서 생성한 Kseed와 동일한 Kseed를 생성한다.

② Kseed = (RNDChip ‖ RNDIS)⊕K

Step 5 : 전자여권과 판독 시스템 간에 동일한 Kseed를 통하여 안전한 채널을 생성한다.

① Secure Channel

Step 6 : 전자여권의 개인 정보를 을 검증하기 위해 CVCA에서 DS인증서를 판독 시스템으로 보낸다.

① DSCert

Step 7 : 전자여권은 안전한 채널을 통하여 전자여권의 정보를 판독 시스템에 전송한다.

① Passport_Info

Step 8 : 판독시스템은 전자여권으로부터 받은 정보를 DS인증서의 공개키를 이용하여 전자여권 정보를 확인한다.

① Verify KPubDS(Passport_Info)

4. 구현 및 비교 분석

4.1 구현

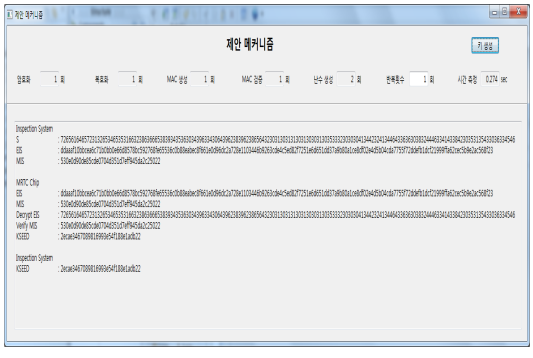
본 실험은 전자여권의 칩과 판독 시스템 사이의 데이터를 안전하게 전송하기 위한 채널을 생성하기 위한 실험으로 결과물로써 전자여권의 칩과 판독 시스템 사이의 서로 공유된 키를 생성하는 것이다.

4.1.1 이미지 정보 및 지문 정보 해시

[그림 4] 사진 이미지 및 지문정보 해시 생성
[Fig. 4] Photographic images and fingerprints generated hash information

그림 4는 이미지 정보 및 지문 정보의 해시 정보를 생성하는 실험이다. 이미지 정보 및 지문 정보는 SAH-1을 이용하여 생성되며 생성된 정보는 전자여권의 DS2와 DS3에 저장되어 진다. 또한 이 정보는 CSCA에 저장되어 전자여권 검증 시 서로 비교하여 위·변조여부를 확인 할 때 사용되어진다.

4.1.2 제안 메커니즘



[그림 5] 제안 메커니즘
[Fig. 5] Proposed mechanism

그림 5은 제안 메커니즘에 대한 실험을 구현한 화면의 인터페이스를 보여주고 있다. 위 실험은 판독 시스템과 전자여권 Chip간의 통신하는 형식으로 구성하였으며 전달되는 값들을 화면에 출력하였다. 그리고 화면 아래쪽에 전자여권 Chip와 판독 시스템간의 서로 같은 SEED 값이 생성 된 것을 확인 할 수 있다.

제안 메커니즘은 MRZ 정보로부터 유도된 EKEN과 EMAC를 이용하여 암·복호화 및 MAC생성·검증한다. 그리고 해시된 사진정보와 이미지정보를 확인하기 위해 사용되는 해시는 SHA-1을 사용한다.

인터페이스에서는 암호화, 복호화, MAC 생성, MAC 검증, 난수생성 의 수행 횟수를 측정하였고 키 생성 시 반복 횟수 및 수행 시간을 측정할 수 있는 부분을 추가하여 기존 BAC 메커니즘과의 연산 횟수 및 시간을 비교할 수 있는 환경을 구축하였다.

4.2 비교분석

4.2.1 안전성 평가

표 1은 BAC 메커니즘과 제안 메커니즘을 비교한 내용이다. BAC 메커니즘에서는 사전에 공유된 키를 이용하여 암·복화 및 MAC 연산을 수행함으로써 중간자 공격을 방지 하였고, 난수 생성 및 질의-응답 방식을 통하여 재생 공격을 방지하며 이를 통해서 서로 공유된 세션키를 유지함으로써 도청공격을 방지할 수 있지만 데이터 위·변조나 리더기의 위·변조를 발견하지 못하는 단점이 있다. 제안 메커니즘 역시 암·복호화 및 MAC 연산을 수행하여 중간자 공격을 방지할 수 있고, 타임스탬프 값을 생성하여 재생 공격을 방지 하며 이를 통해서 서로 공유된 세션키를 유지함으로써 도청 공격을 방지 할 수 있다. 뿐만 아니라 리더기에서 생성한 타임스탬프 값을 이용하여 리더기의 위·변조를 확인 할 수 있고 해시된 이미지와 해시된 지문 정보를 통하여 데이터의 위·변조 역시 확인 가능하다.

[표 1] 안전성 비교
[Table 1] Security comparison

구분	BAC 메커니즘	제안 메커니즘
중간자 공격	안전	안전
재생 공격	안전	안전
도청 공격	안전	안전
데이터 위·변조	불안전	안전
리더기 위·변조	불안전	안전

4.2.2 효율성 평가

표 2는 제안 메커니즘과 기존 BAC 메커니즘의 비교분석은 암·복호화 및 주요 연산의 수행 횟수에 대하여 정량적인 분석을 수행하였다.

기존의 BAC 메커니즘에서는 칩과 판독 시스템 사이의 암·복호화 및 MAC 생성·검증이 각각 2회씩 실행되며 난수 생성이 총 4회가 실행된다. 그에 비해 제안하는 메커니즘은 타임스탬프 값을 생성하여 사용함으로써 암·복호화 및 MAC 생성·검증이 각각 1회씩 수행되며 난수 생성은 칩과 판독 시스템에서 1회씩만 수행됨으로 기존의 BAC 메커니즘에 비해 정량적으로 계산 량을 감소시킬 수 있는 장점을 가진다.

[표 2] 전자여권의 연산에 따른 주요 항목 비교
[Table 2] According to the operation of the e-passport major item comparing

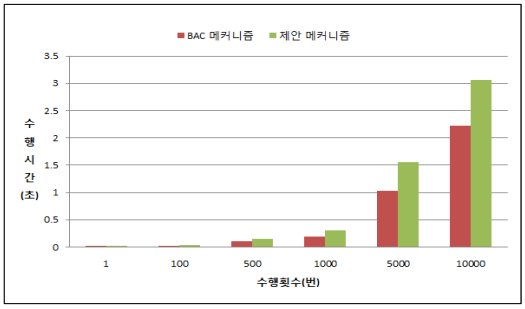
성능 비교	전자여권 칩과 판독 시스템 사이의 연산 횟수				
	암호화	복호화	난수 생성	MAC 생성	MAC 검증
BAC	2	2	4	2	2
제안 시스템	1	1	2	1	1

4.3 성능평가

MRTD 칩과 판독 시스템 사이의 서로 같은 세션키를 생성하는데 걸리는 연산 시간을 측정한다. 표 3은 기존 BAC 메커니즘과 비교하여 키 생성 시간을 측정한 결과이고, 그림 6는 측정결과를 그래프로 표현한 것이다. 측정 결과 효율성 평가에서 나타나듯이 적은 연산횟수를 가진 제안 메커니즘이 BAC 메커니즘에 비해 우수한 성능을 나타난 것을 확인 할 수 있었다.

[표 3] 세션키 생성 시 수행 시간
[Table 3] Session key is generated at run-time

구분(회)	BAC 메커니즘	제안 메커니즘
1	0.001	0.001
100	0.010	0.031
500	0.108	0.147
1000	0.197	0.307
5000	1.027	1.562
10000	2.224	3.055



[그림 6] 세션키 생성 시 수행 시간 그래프
[Fig. 6] Session key is generated at run-time graph

5. 결론

본 논문에서는 전자여권 칩과 판독 시스템 간의 안전한 채널을 형성하기 위하여 사용되는 BAC 메커니즘을 개선한 메커니즘을 제안하였다. 전자여권 칩과 판독 시스템 사이의 안전한 채널을 생성하기 이전에 전자여권의 위·변조 여부를 판별 할 수 있어 여권 분실 시 여권의 위·변조의 위협으로부터 보호 가능하였다. 또한 리더기에서 타임스탬프 값을 생성하여 전자여권의 Chip과 판독 시스템으로 보내 줌으로써 리더기에 대한 확인을 거칠 수 있게 된다.

결과적으로 제안하는 메커니즘은 현재 사용되고 있는 BAC 메커니즘에서의 단점인 단말기 인증 및 전자여권의 위·변조 여부를 확인하지 않는 점을 보완하였다. 그리고 안전성 및 효율성이 더 뛰어나기 때문에 현재 전자여권 칩과 판독 시스템 사이의 안전한 채널을 형성 시 사용하는 BAC 메커니즘을 대신해서 사용 할 수 있을 것을 기대하고 있다.

향후에는 전자여권의 조작을 통한 위조의 위험뿐만 아니라 여권 RFID 태그에 손상된 데이터를 넣어 검사 시스템을 망가뜨리거나 출입국 감시 컴퓨터에 악성코드를 퍼트릴 가능성이 있기 때문에 이에 따른 전자여권 보안 기술에 대한 연구가 필요 할 것이다.

References

[1] ICAO. "Biometric Deployment of Machine Readable Travel Documents", Version 2.0 2004.

[2] Eili Bjelkasen, Linda Walbeck Olsen, "Security Issues in ePassports", May, 2006.

[3] ICAO, "Development of a Logical Data Structure-LDS for Optional Capacity Expansion Technologies", Revision 1.7, 2004

[4] ICAO, 'PKI for Machine Readable Travel Documents offering ICC Read-Only Access', Version 1.1, 2004.

[5] Gaurav S., Kc and Paul A., Karger., "Security and privacy issues in machine readable travel documents (MRTDs)", IBM Technical Report (RC23575). IBM T. J., Watson Research Labs, April, 2005.

[6] NIST, "Recommendation for Key Management. Technical Report Special Publication 800-57 Draft", 2005.

[7] S. J. Oh, "An Anomaly Detection Method for the Security of VANETs", *Journal of The Institute of Webcasting, Internet and Telecommunication,* VOL.10, No.2, pp. 77-83, Apr., 2010.

[8] Y. H. Cho, G. S. Lee, "Prediction on Clusters by using Information Criterion and Multiple Seeds", *Journal of The Institute of Webcasting, Internet and Telecommunication,* VOL.10 No.6, pp.145-152, Dec., 2010.

[9] H. Y. Hwang, H. J. Suh, "The Multi-path Power-aware Source Routing(MPSR) for the Maximum Network Lifetime in Ad-Hoc Networks", *Journal of The Institute of Webcasting, Internet and Telecommunication,* VOL.10No.5, pp. 21-29, Oct., 2010.

[10] E. C. Kim, S. I. Seo, J. Y. Kim, "Performance of Tactics Mobile Communication System Based on UWB with Double Binary Turbo Code in Multi-User Interference Environments", *Journal of The Institute of Webcasting, Internet and Telecommunication,* VOL.10, No.1, pp. 39-50, Feb., 2010.

[11] J. P. Cho, S. I. Cho, K. M. Kang, H. J. Hong, "Analysis on Characteristics for Sharing Co-channel between Communication Systems", *Journal of The Institute of Webcasting, Internet and Telecommunication,* VOL.11, No.4, pp. 251-256, Aug., 2011.

[12] H. Y. Hwang, Namyun Kim, "Personal Information Protection System for Web Service", *Journal of The Institute of Webcasting, Internet and Telecommunication,* VOL.11 No.6, pp. 267-273, Dec., 2011.

[13] YeWang, Xiao-LeiZhang, WeiweiChen, J. G. Ki, K. T. Lee, "Comparative study of an integrated QoS in WLAN and WiMAX", *Journal of The Institute of Webcasting, Internet and Telecommunication,* VOL.10, No.3, pp. 103-110, Jun., 2010.

이 기 성(Gi Sung Lee) **[정회원]**

- 1996년 8월 : 숭실대학교 컴퓨터학과 (공학석사)
- 2001년 8월 : 숭실대학교 대학원 컴퓨터학과 (공학박사)
- 2001년 9월 ~ 현재 : 호원대학교 컴퓨터게임학부 교수

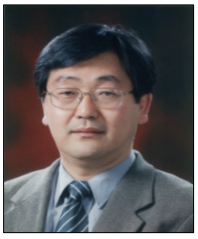
<관심분야>
정보통신, 통신보안, 암호이론

전 상 엽(Sang-Yeob Jeon) **[정회원]**

- 2009년 2월 : 숭실대학교 컴퓨터학과 (학사)
- 2011년 2월 : 숭실대학교 일반대학원 정보보안 (공학석사)
- 2011년 8월 ~ 현재 : 숭실대학교 일반대학원 통신 (박사과정)

<관심분야>
정보통신, 통신보안, 암호이론

전 문 석(Moon-Seog Jun) **[정회원]**



- 1989년 2월 : University of Maryland Computer Science 공학박사
- 1989년 3월 ~ 1991년 2월 : New Mexico State University physical Science Lab 책임 연구원
- 1991년 3월 ~ 현재 : 숭실대학교 정교수

<관심분야>
인터넷 보안, 멀티미디어 보안, 인증 시스템