RFID 시스템에 적용시 안전한 보안인증 프로토콜의 모델검증

배우식*, 정석용**, 한군희***

Model Verification of a Safe Security Authentication Protocol Applicable to RFID System

WooSik Bae*, SukYong Jung, KunHee Han*****

요 약 RFID는 IC 칩과 무선통신을 통해 다양한 개체의 정보를 관리할 수 있는 인식기술이다. 생산에서 판매에까지의 과정을 초소형 IC 칩에 내장하여 이를 무선으로 추적하는 기술로써 전자태그, 스마트태그 또는 전자라벨 등으로 불러지고 있다. 현재 의료, 국방, 물류, 보안 등에 응용하여 사용하기위해 적용 및 개발이 진행되고 있으나 구조상 태그의 정보를 읽어 들이는 리더와 정보를 제공하는 태그, 데이터를 관리하는 데이터베이스로 구성되는데 리더와 태그 구간이 무선구간으로 보안에 취약한 문제가있다. 따라서 취약한 부분을 해결하고자 보안프로토콜의 연구가 활발히 진행되고 있으나 구현부분이 어려워 정리증명 단계의 제안이 대부분이다. 이는 추후 다른 연구자에 의해 취약성이 발견되는 부분이 많아 실제시스템에 적용시 많은 어려움이 존재한다. 본 논문에서는 제안한 보안프로토콜을 CasperFDR 정형검증 도구를 사용하여 제안한 프로토콜의 보안성을 실험 검증하였으며 각종공격에 안전한 방식임이 확인되었다. 향후 실제 태그에 적용할시 보안성에 대한 안전보장 및 새로운 공격에 대한 안전성을 충족하였다.

주제어 : 인증프로토콜, RFID 보안, Casper, RFID 인증, 정형검증

Abstract RFID is an automatic identification technology that can control a range of information via IC chips and radio communication. Also known as electronic tags, smart tags or electronic labels, RFID technology enables embedding the overall process from production to sales in an ultra-small IC chip and tracking down such information using radio frequencies. Currently, RFID-based application and development is in progress in such fields as health care, national defense, logistics and security. RFID structure consists of a reader that reads tag information, a tag that provides information and the database that manages data. Yet, the wireless section between the reader and the tag is vulnerable to security issues. To sort out the vulnerability, studies on security protocols have been conducted actively. However, due to difficulties in implementation, most suggestions are concerned with theorem proving, which is prone to vulnerability found by other investigators later on, ending up in many troubles with applicability in practice. To experimentally test the security of the protocol proposed here, the formal verification tool, CasperFDR was used. To sum up, the proposed protocol was found to be secure against diverse attacks. That is, the proposed protocol meets the safety standard against new types of attacks and ensures security when applied to real tags in the future.

Key Words : authentication protocol, RFID security, Casper, RFID authentication, Model Checking

1. 서론

RFID(Radio Frequency Identification)는 자동인식(Automatic Identification) 기술의 하나로써 데이터를 무선으로 인식하는 기술이다. 현재 많이 사용하고 있는 바코드를 대체하여 각 산업 분야에 적용되고 있으며 바코

*아주자동차대학 전산실(교신저자)
**동양미래대학교 전산정보학부 교수
***백석대학교 정보통신학부 교수
논문접수: 2013년 3월 4일, 1차 수정을 거쳐, 심사완료: 2013년 4월 12일, 확정일: 2013년 4월 20일

드기술이 극복하지 못했던 여러 개의 태그정보를 동시에 판독하거나 수정, 갱신할 수 있는 장점이 있다. 아울러 재사용이 가능하며 먼지, 습기, 온도, 비 등에 많은 제한을 받지 않고 데이터전송을 할 수 있다. 현재 물류관리, 공정관리, 출입통제, 주차관리, 도서관리, 전자화폐 등에 응용되어 사용 중이다. 그러나 RFID 동작의 필수인 태그와 리더구간의 통신이 무선으로 이루어지기 때문에 이 구간에 보안적으로 취약한 문제가 발생한다[8][9].

공격유형으로 도청공격, 정보노출, 트래픽분석, 스푸핑공격, 서비스거부공격, 트래킹공격 등 취약점에 대한 대비가 필요하며, 정보누출로 인하여 심각한 문제를 야기할 수 있다[7][10].

이러한 RFID 시스템의 문제를 해결하고자 다양한 방법의 프로토콜이 제안되고 있다[3][4]. 그러나 정리증명으로 제안되다보니 미처 생각하기 못했던 부분의 취약성이 타 연구자에 의해 발견되고 있으며 또는 너무 복잡하게 설계되어 있어 자원의 한계가 있는 태그에 사용하지 못하는 프로토콜로 전락되고 있는 실정이다[11].

따라서 본 논문에서는 RFID 보안 취약점을 해결하고 실제 현장 시스템에서 적용 가능한 보안 프로토콜의 설계를 목적으로 한다.

제안방식은 보안성은 충족하면서 실제 시스템에서 사용 가능성에 중점을 두고 실험하였으며 다음과 같은 연구결과를 얻었다. 첫째, 프로토콜 검증에서 정형검증기법으로 검증하여 정리증명에 비해 신뢰성을 높였다. 둘째, 제안프로토콜은 통신에서 세션키, 해시락, 타임스탬프 및 난수를 적용하여 보안성을 높였다. 셋째, 최종 데이터 전송 세션에서 해시와 타임스탬프 방식을 사용하여 유일한 데이터를 전송함으로 보안을 강화하고, 해시방식으로 데이터를 줄임으로 RFID 시스템의 효율을 높였다. 따라서 제안 방식으로 RFID 보안프로토콜에 적용하면 안전한 시스템의 구축이 가능하다.

2. 관련연구

2.1 Casper

Caster(A Compiler for the Analysis of Security Protocols)[2]는 보안속성을 순차적으로 표현하고 프로토콜을 명세하기 쉽게 Gavin Lowe에 의해 개발되어진 컴파일러이다. Casper에서 프로토콜의 동작과 검증해야할 시스템을 두 부분으로 나뉘어 명세 한다. 첫째, 호스트들 간에 전달되는 메시지, 데이터타입, 함수, 변수, 및 동작순서 등을 정의한다. 둘째, 실 시스템에서 동작하는 각각 호스트의 역할, 함수선언, 공격자의 상태정보 등 검증해야 할 실제 시스템을 정의한다.

Casper에서 검증하기 위해 8개의 세부 항목으로 명세 및 분류하는데 각 항목의 헤더 부분은 #으로 시작하며 다음과 같다.

#Free variables : 변수타입 및 함수선언
#Process : 통신에이전트의 초기상태
#Protocol description : 에이전트 간의 메시지 교환순서
#Specification : 검증하고자 하는 보안속성 선언
#Actual Variables : 실제 데이터타입 및 이름선언
#Functions : 프로토콜에서 사용하는 함수선언
#System : 에이전트의 초기상태 표현
#Intruder Information : 공격자의 최초 상태정보

2.2 FDR(Failure Divergence Refinements)

FDR 도구는 CSP(Communicating Sequential Processes)[6]를 입력언어로 받아 모델이 속성을 만족하는지 검사하는 모델 검사도구 이다. 만일 만족하지 않을 경우에는 반례(counterexample)을 보여주어 각종 보안 취약점을 분석하기에 용이하다. 보안프로토콜의 요구사항인 비밀성, 무결성, 인증, 부인방지 등의 속성을 만족하는지 검사하는 도구이며 안전성(safety) 검증, 교착상태(deadlock) 검증, 라이브락(livelock)검증 의 3가지 검증방법을 지원한다. 아울러 추적모델(trace model), 실패모델(failure model), 실패/분기모델(failure/divergence model)을 지원한다[1].

가) 추적모델(trace model)

프로세스는 그 프로세스가 갖는 행위에 의해 유한 순서 집합으로 표현되며, P 프로세스가 Q 프로세스의 모든 행위를 포함할 때 $P \sqsubseteq TQ$ 라고 표기한다.

$$P \sqsubseteq TQ \triangleq traces(Q) \subseteq traces(P)$$

나) 실패모델(failure model)

실패(failure)는 (s, X)의 쌍으로, s는 추적(P)에서의 추적을 말하고 X는 s 이후에 프로세스가 거부하는 모든 이

벤트의 집합을 말한다. 즉 교착상태를 의미하며, 다음과 같이 표기한다.

$$P \sqsubseteq FQ \triangleq failures(Q) \subseteq failures(P)$$

다) 실패/분기 모델(failure/divergence model)

프로세스의 분기는 라이브락(livelock)을 의미한다. 즉 실패/분기 모델은 교착(deadlock)상태이면서 라이브락 상태를 의미하며, 다음과 같이 표기한다.

$$P \sqsubseteq FDQ \triangleq failures(Q) \subseteq failures(P) \wedge divergences(Q) \subseteq divergences(P)$$

2.3 기존 프로토콜

2.3.1 Kenji *et al.* 프로토콜

Kenji *et al.* 프로토콜은 서버가 사용자에게 사전에 배포한 비밀값을 이용하여 One-time ID를 생성하여 연속된 수 1을 프로토콜이 동작할 때 마다 1씩 동기화 된 값을 증가시킨다. 리더와 서버는 1씩 증가시킨 I 와 공유된 비밀 값을 공격자가 사용할 수 없도록 복잡한 공식을 적용하여 계산한다. 이후 서버는 One-time ID를 수신한 후 자신이 계산한 값과 비교하여 식별하게 되는 방식이다. 따라서 공격자는 복잡한 공식으로 생성되어진 One-time ID를 역으로 유추해낼 수 없게 된다. 다음은 Kenji *et al.* 기법의 데이터 전송 방식을 나타낸다.

(1) A → B : $S, O_{AS}, (B, g^x, O_{AS})_{kAS}$

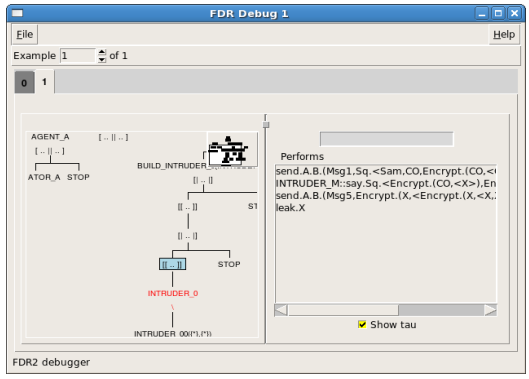
(2) B → S : $O_{AS}, (B, g^x, O_{AS})_{kAS}, (g^y, O_{AS})_{kBS}$

(3) S → B : $S, (A, g^x, g^y, (g^x, g^y)_{kAS})_{kBS}$

(4) B → A : $g^x, (g^x, g^y)_{kAS}, (g^x, N_b)_{kAB}$

(5) A → B : $(N_b - 1)_{kAB}$

Kenji *et al.* 프로토콜은 처음 세션에서 O_{AS} 를 암호화하지 않고 전송하는 부분이 있는데 이 때문에 공격자가 데이터를 수집할 경우 위조하여 공격 할 수 있는 문제가 있다[5]. 공격자가 메시지를 임의로 작성하여 공격할 경우 시스템의 무결성에 문제가 생기며 보안상 많은 취약성이 나타난다. [그림 1]은 FDR 검증결과 관련된 취약성을 확인할 수 있는 상태창을 보여주었다.



[그림 1] Kenji *et al.* 의 FDR 디버그결과

3. 제안하는 프로토콜과 검증

3.1 제안하는 보안 프로토콜

본 논문에서 제안한 프로토콜에서 사용되는 기호에 대한 정의는 <표 1>과 같이 표기한다.

〈표 1〉 기호 정의

기호	설명
T	태그
R	리더
S	데이터베이스 서버
Query	질의신호
x, k	Nonce
sk1, sk2	SessionKey
Var	Variable
Ta, Tb	Timestamp
H( )	HashFunction

본 논문에서 제안하는 프로토콜의 단계별 처리내용을 pseudo code 형식으로 기술하면 다음과 같다.

◎ (Step ① : 태그 → 리더) $Ta, (x)(sk1) \% Var$

Step 1 Tag → Reader

Input Query
Output $Ta, (x)(sk1) \% Var$

```
1:  Begin
2:    Create a timestamp Ta;
3:    Initialize (sk1);
4:    Update a Tag Key (sk1);
5:    Create a Session Key (x);
6:    Compute the Ta, (x)(sk1) % Var;
7:    Send Ta, (x)(sk1) % Var To Reader;
8:  End;
```

[그림 2] 태그에서 리더에게 전송하는 데이터 생성

태그 T는 리더로부터 Query를 수신한 후 [그림 2]와 같은 순서로 태그에서 Ta 값과 $Ta,(x)(sk1)\%Var$ 값을 생성하고 각 값을 연접하여 리더에게 전송한다. 이때 Ta 값은 고유한 값으로 다른 태그에서 생성할 수 없는 값이다.

◎ (Step ② : 리더 → 데이터베이스)
$Tb,H(R),(m1\%(x)(sk1),sk2,k)(sk2)$

Step 2 Reader → Database

Input $Ta,(x)(sk1)\%Var$
Output $Tb,H(R),(m1\%(x)(sk1),sk2,k)(sk2)$

```
1:  Begin
2:    Create a timestamp Tb;
3:    Initialize sk2;
4:    Create a Session Key sk2;
5:    Compute the ; Ta,(x)(sk1)%Var;
6:    Concatenation operation
        Tb,H(R),(m1%(x)(sk1),sk2,k)(sk2);
7: Send Tb,H(R),(m1%(x)(sk1),sk2,k)(sk2)
   To Database;
8:  End;
```

[그림 3] 리더에서 DB에 전송하는 데이터생성

태그에서 전송한 $Ta,(x)(sk1)\%Var$ 값과 리더가 계산한 Tb, $Tb,H(R),(m1\%(x)(sk1),sk2,k)(sk2)$ 값을 [그림 3]과 같이 데이터베이스로 전송한다.

◎ (Step ③ : 데이터베이스 → 리더)
$(T,x,(k)(sk1)\%m2)(sk2)\oplus H(R)$

Step 3 Database → Reader

Input $Tb,H(R),(m1\%(x)(sk1),sk2,k)(sk2)$
Output $(T,x,(k)(sk1)\%m2)(sk2)\oplus H(R)$

```
1:  Begin
2:    Compute the
        Tb,H(R),(m1%(x)(sk1),sk2,k)(sk2);
3:    Compute the
(T,x,(k)(sk1)%m2)(sk2)⊕H(R);
4:      Send (T,x,(k)(sk1)%m2)(sk2)⊕H(R) To
        Reader;
5:  End;
```

[그림 4] DB에서 인증한 후 리더에게 전송하는 데이터

리더에게서 전송된 $Tb,H(R),(m1\%(x)(sk1),sk2,k)(sk2)$ 값과 데이터베이스에서 생성한 값을 다음의 $(T,x,(k)(sk1)\%m2)(sk2)\oplus H(R)$ 인증 값을 생성하고 [그림 4]와 같이 리더에게 전송한다.

◎ (Step ④ : 리더 → 태그)
$m2\%(k)(sk1),H((x)(k))$

Step 4 Reader → Tag

Input $(T,x,(k)(sk1)\%m2)(sk2)\oplus H(R)$
Output $m2\%(k)(sk1),H((x)(k))$

```
1:  Begin
2:    Create a (k)(sk1);
3:    Compute the m2%(k)(sk1),H((x)(k))
4:    Send m2%(k)(sk1),H((x)(k)) To Tag;
5:  End;
```

[그림 5] 리더 인증을 위해 태그에 전송하는 데이터

리더는 데이터베이스에서 수신한 $(T,x,(k)(sk1)\%m2)(sk2)\oplus H(R)$ 값을 [그림 5]와 같이 인증을 위해 $m2\%(k)(sk1),H((x)(k))$ 값을 생성한 후 태그에게 전송한다. 이 부분은 태그에서의 연산을 줄여 전송한다.

◎ (단계 ⑤ : 태그 → 리더) $H(T),Ta$

Step 5 Tag → Reader

Input $m2\%(k)(sk1),H((x)(k))$
Output $H(T),Ta$

```
1:  Begin
2:    Tag receive m2%(k)(sk1),H((x)(k));
3:      Compare a m2%(k)(sk1),H((x)(k)) with
        m2%(k)(sk1),H((x)(k));
4:    Compute the H(T),Ta;
5:    Send H(T),Ta to Reader;
6:  End;
```

[그림 6] 해시된 태그정보를 생성

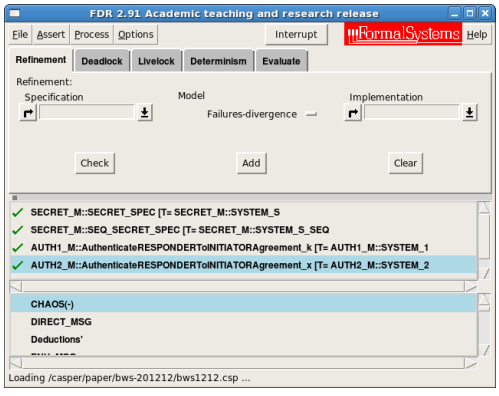
마지막으로 태그는 리더에게 $m2\%(k)(sk1),H((x)(k))$값을 전송한 이후 태그에서 생성한 값과 비교하여 확인되면 [그림 6]과 같이 자신의 ID를 해시연산 암호화하여 Ta와 함께 리더에게 전송함으로 태그에서의 인증 세션을 완료한다. 이후 리더는 태그 값을 데이터베이스에 전송하게 되면 데이터베이스는 태그의 해시된 값을 검색하게 된다. 정상적인 검색이 완료되면 해시된 코드와 태그코드를 확인 할 수 있음으로 세션을 종료한다.

3.2 Casper 코드 명세

제안하는 보안 프로토콜을 Casper 코드로 변수유형선언, 초기상태, 동작절차, 보안속성, 데이터 타입, 함수선언, 에이전트 상태, 공격자 모델 등 총 8개 영역을 명세한다. 변수유형선언, 초기상태, 동작절차, 보안속성의 주요 3개의 영역을 <부록>으로 첨부하였으며 간단한 설명은 다음과 같다. 변수들과 함수타입은 <#Free variables> 부분에 정의된다. <#Processes> 부분은 호스트의 역할, 변수, 함수들을 정의한다. <#Protocol description>에는 프로토콜에서의 주요부분으로 메시지 전송순서에 대한 정의이다. 0번 메시지는 통신을 시작할 때 R 이 통신해야 하는대상을 알려주기 위해 사용된다. 표현식 m%enc에서 m은 전달하고자 하는 메시지를 의미하고, enc는 메시지를 저장하기 위한 변수로 사용된다. 전체적으로 타임스탬프와 세션키를 적용하여 보안통신과 상호인증방식으로 전송하며 이때 구간별로 해시함수를 사용하여 데이터 송신량을 줄인 것이 특징이다. <#Specification> 부분 명세코드로써 검증하고자하는 프로토콜의 보안속성을 정의한다.

3.3 검증결과

FDR 2.91 버전의 모델검증 도구를 이용하여 본 논문에서 설계한 프로토콜의 안전성(safety), 교착상태(deadlock), 라이브락(livelock) 등의 동작을 검증하기위해 FDR을 실행한다. 제안하는 프로토콜을 FDR 도구를 이용한 프로토콜 검증하기 위해 각각 항목을 순차적으로 실행해본 결과 [그림 7]과 같이 검증한 프로토콜이 모든 항목에서 안전함을 확인하였다.



[그림 7] 제안 프로토콜 검증결과

[그림 7]에는 4가지 검증 결과가 제시되며 각 결과의 표현은 다음과 같이 분석된다.

1) SECRET_M::SECRET_SPEC[T=SECRET_M::SYSTEM_S

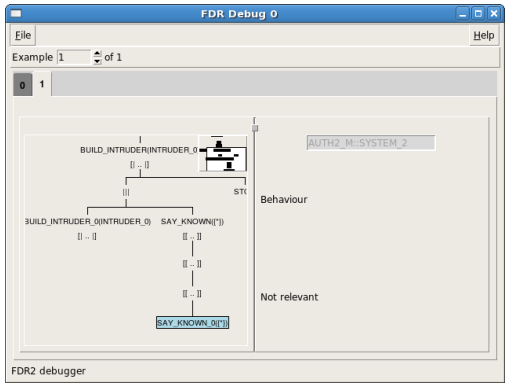
제안 프로토콜이 보안적 으로 안전하며 메시지 프로토콜이 공격자에게 노출되지 않았다는 결과이다.

2) SECRET_M::SEQ_SECRET_SPEC[T=SECRET_M::SYSTEM-S_SEQ

이 항목은 프로토콜이 시스템에서 정상적인 프로세스로 동작하는지를 확인 한 결과이며 안전한 프로세스로 동작함이 확인되었다.

3) AUTH1_M::AuthenticateRESPONDERToINITIATOR Agreement_k[T=AUTH1_M::SYSTEM_1
4) AUTH2_M::AuthenticateRESPONDERToINITIATOR Agreement_x[T=AUTH2_M::SYSTEM_2

3, 4는 k, x를 통해서 Responder와 Initiator가 서로 인증하는지 검증하여 서로 안전하게 인증함이 확인되었다.



[그림 8] 제안프로토콜의 디버그상태

[그림 8]에는 FDR이 세부적으로 제공하는 디버그 상태이다. 프로토콜에 취약성이나 문제가 발생하면 단계별로 확인하여 프로토콜의 취약점을 확인 및 제거 할 수 있도록 지원된다. 제안 프로토콜은 오류 없이 검증됨을 확인할 수 있었다.

3.4 기존 프로토콜과의 비교 검토

본 논문에서 제안한 프로토콜은 <표 2>와 같이 보안 요구사항을 만족함으로써 보안에 안전함을 알 수 있다.

〈표 2〉 프로토콜의 안전성비교

	Kenji *et al.*기법 [5]	제안 프로토콜
스푸핑 공격	중간	안전
재전송 공격	취약	안전
트래픽분석 공격	안전	안전
위치추적 공격	중간	안전
도청 공격	취약	안전

Kenji *et al.* 기법은 초기에 암호화하지 않은 형태의 데이터전송으로 위조가 가능하여 [그림 1]의 Kenji *et al.* 프로토콜의 FDR 검증결과와 같이 재전송 공격, 도청 공격 등에 취약하다. 반면 본 논문에서 제안한 프로토콜은 공격자가 정당한 리더로 가장하여 Query를 전송한다면, 태그로부터 $Ta,(x)(sk1)\%Var$를 획득할 수 있다. 그러나 이 정보를 공격자의 태그로 가장하여 리더에 대한 응답으로 전송하게 될 경우, 공격자는 다음 세션의 타임스탬프 Ta 값을 알아낼 수가 없다. 아울러 각 세션별 모든 단계를 암호화 전송함으로써 동일한 값이 전달되는 경우는 없다. 따라서 제안 프로토콜의 안전성이 정리증명으로 입증되며 모델검증 FDR 실험에서도 안전함이 확인되었다.

4. 결론

RFID 시스템은 무선구간의 통신 취약성으로 보안적인 문제를 가지고 있다. 따라서 이 분야의 인증프로토콜에 대한 다양한 연구가 진행중이다. 본 논문에서 제안한 프로토콜은 타임스탬프, 세션키, 난수 및 해시락를 사용하여 동작하며 FDR 정형검증 기법으로 각종 보안속성을 만족하는지 실험하였다. 제안 프로토콜을 Casper, FDR 프로그램을 사용하여 검증한 결과 보안적인 안전성, 교착상태, 라이브락 등 전체적인 보안 측면에서 안전함을 보였다. 따라서 제안 프로토콜을 RFID 시스템에 응용할 경우 다음과 같은 효과가 기대된다. 첫째, 프로토콜 제안 분야에서 정리증명에 비해 검증된 프로그램을 실행하여 신뢰성을 보장한다. 둘째, 설계된 프로토콜을 그대로 시스템에 적용할시 설계오류를 줄일 수 있다. 셋째, 최근 제안되는 타 프로토콜에 비해 복잡하거나 계산 량이 많지 않아 자원낭비를 줄이고 효율적인 시스템을 구성할 수 있다. 끝으로 향후 태그의 종류별로 각각 다른 프로토콜을 적용하는 연구를 진행할 계획이다.

참고문헌

[1] Formal Systems(Europe) Ltd, Oxford University Computing Laboratory, "Failures-Divergence Renement," FDR2 User Manual, 19th October 2010.

[2] G. Lowe. " Casper: A compiler for the analysis of security protocols." User Manual and Tutorial. Version 1.12 2009

[3] I. Syamsuddin, T. Dillon, E. Chang, and S. Han, "A survey of RFID authentication protocols Based on Hash-Chain method," *ICCIT*, pp. 559-564, November 2008.

[4] Jihwan Lim, Heekuck Oh, SangJin Kim, A new hash-based RFID mutual authentication protocol providing enhanced user privacy protection, *ISPEC 2008, LNCS*, vol. 4991, pp. 278 - 289 , April 2008.

[5] Kenji Imamoto and Kouichi Sakurai, "Design and Analysis of Diffie-Hellman Based Key Exchange Using ID by SVO Logic," *Proc. Electronic Notes in Theoretical Computer Science*, pp. 79-94, June 2005.

[6] Mala Mitra. "Privacy for RFID Systems to Prevent Tracking and Cloning", *International Journal of Computer Science and Network Security*, Vol 8 No 1, pp. 1-5, January 2008.

[7] S. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," *In Security in Pervasive Computing, LNCS*2802, pp. 201-202, 2005

[8] Yang, M. H., and Hu, H. Y. Protocol for ownership transfer across authorities: with the ability to assign transfer target. Security and Communication Networks, vol 5, 164 - 177, February 2012.

[9] Yeha, T. C, Wua, C. H, Tsengb, Y. M,

"Improvement of the RFID authentication scheme based on quadratic residues", Computer Communications, vol 34, pp. 337 - 341, March 2011.

[10] Yu Shucheng, Ren Kui, Lou, Wenjing, "A privacy-preserving lightweight authentication protocol for low-cost RFID tags," *IEEE MILCOM*, pp. 1-7, October 2007.

[11] Yu Tian-tian, Feng Quan-yuan, "A Security RFID Authentication Protocol Based on Hash Function," *ieec*, pp.804-807, 2009 International Symposium on Information Engineering and Electronic Commerce, 2009

〈부록〉 제안 프로토콜의 Casper 소스코드(3개영역)

```
#Free variables

T, R : Agent
S : Server
x, k : Nonce
H : HashFunction
sk1, sk2, y : SessionKey
Ta, Tb : TimeStamp
InverseKeys = (k,k),(sk1,sk1),(sk2,sk2),(x,x),(y,y)

#Processes

INITIATOR(T, R, S, x, sk1)
RESPONDER(R, S, k, sk2)
SERVER(S, T, R, sk1, sk2)

#Protocol description

0.    -> T : R
1. T -> R : Ta,{x}{sk1}%m1
[R!=T]
2. R -> S : Tb,H(R),{m1%{x}{sk1},sk2,k}{sk2}
3. S -> R : {T,x,{k}{sk1}%m2}{sk2}(+)H(R)
4. R -> T : m2%{k}{sk1},H({x}{k})
5. T -> R : H(T),Ta

#Specification

Secret(T,x,[R])
Secret(T,k,[R])
Agreement(R,T,[k])
Agreement(R,T,[x])
```

배 우 식

- 1997년 3월 ~ 현재 : 아주자동차대학 전산소
- 2006년 8월 : 백석대학교 정보기술대학원(공학석사)
- 2012년 2월 : 충북대학교 대학원 컴퓨터교육과(교육학박사)
- 2009년 1월 ~ 2010년 12월 : 한국산학기술학회 이사 역임
- 2010년 1월 ~ 현재 : 한국융합학회 상임총무이사
- 2010년 1월 ~ 현재 : 중소기업정보기술융합학회 연구이사
- 관심분야 : RFID 보안, 무선 네트워크, 암호 프로토콜/알고리즘, 정보시스템
- E-Mail : bws@motor.ac.kr

정 석 용

- 1996년 3월 ~ 현재 : 동양미래대학교 전산정보학부 교수
- 관심분야 : 정보통신. 실시간시스템
- E-Mail : syjung@dongyang.ac.kr

한 군 희

- 2001년 3월 ~ 현재 : 백석대학교 정보통신학부 교수
- 관심분야 : 멀티미디어, 유비쿼터스, DB보안, 암호 프로토콜/알고리즘
- E-Mail : hankh@bu.ac.kr