https://doi.org/10.5392/JKCA.2021.21.02.113

오프라인 검증을 지원하는 안전한 요킹증명 프로토콜

A Secure Yoking-Proof Protocol Providing Offline Verification

함형민
배재대학교 사이버보안학과

Hyoungmin Ham(aham@pcu.ac.kr)

요약

RFID (Radio Frequency Identification) 요킹증명은 여러 객체의 물리적 근접성을 보장하기 위해 한 쌍의 RFID 태그를 하나의 리더 장치로 동시에 스캔하고 이를 검증하기 위한 방법을 제공한다. 최초 제안된 요킹증명 프로토콜들은 생성된 증명을 검증하기 위해 리더 장치와 온라인으로 연결된 온라인 검증자가 필수적이며, 이 조건은 요킹증명이 적용 가능한 환경을 제한한다. 이 같은 제한 조건을 완화하기 위해, 온라인 검증자가 필요하지 않은 오프라인 요킹증명에 대한 연구가 제안되었다. 그러나 이 프로토콜들은 안전한 요킹증명의 생성 및 검증을 보장하지 못하며, 최초 제안된 요킹증명 기법에 비해 상대적으로 더 많은 연산을 태그에게 요구한다. 본 논문에서는, 온라인 검증자가 필요 없는 안전하고 효율적인 오프라인 요킹증명 프로토콜을 제안한다. 제안하는 오프라인 요킹증명 프로토콜은 기존의 프로토콜들보다 상대적으로 적은 횟수의 연산으로 안전한 요킹증명의 생성 및 검증이 가능하며, 별도의 추가 장치 없이 한 쌍 이상의 태그에 대한 증명이 가능한 그룹증명으로의 확장도 지원한다. 분석 결과는 제안된 프로토콜이 안전하고 효과적으로 오프라인 검증을 제공한다는 것을 보인다.

■ 중심어 : | RFID | 요킹증명 | 오프라인 요킹증명 | 위치추적 | 비구별성 | 프라이버시 |

Abstract

RFID (Radio Frequency Identification) yoking authentication provides methods scanning a pair of RFID tags with a reader device and verifying them to ensure the physical proximity of objects. In the first yoking proof protocols, a verifier connected to a reader device online is essential to verify the yoking proof, and this condition limits the environment in which yoking proof can be applied. To solve this limitation, several studies have been conducted on offline yoking proof protocol that does not require the online connection between a reader and a verifier. However, the offline yoking proof protocols do not guarantee the basic requirements of yoking proof, and require relatively more operations on the tag compared to the previous yoking proof protocols. This paper proposes an efficient offline yoking proof protocol that supports offline verification without the need for an online verifier. The proposed protocol provides a secure yoking proof with fewer number of operations than the existing ones, and it also can be extended to the group proof for more than a pair of tags without additional devices. The analysis in this paper shows that the proposed protocol provides offline verification securely and effectively.

■ keyword : | RFID | Yoking-proof | Offline Yoking-proof | Tracking | Unlinkability | Privacy |

* 이 논문은 2020학년도 배재대학교 교내학술연구비 지원에 의하여 수행된 것임

접수일자 : 2020년 11월 02일
수정일자 : 2021년 01월 14일
심사완료일 : 2021년 01월 14일
교신저자 : 함형민, e-mail : aham@pcu.ac.kr

I. 서 론

RFID (Radio Frequency Identification) 태그는 고유한 식별자가 있는 작은 마이크로 칩이다. 각 태그는 무선 채널을 통해 RFID 리더에 식별자를 전달한다. RFID 시스템을 통한 객체 식별의 자동화는, 대량의 물류 관리에 효과적이며, 이 같은 장점으로 인하여, 다양한 연구와 상용 솔루션이 지속적으로 제안되고 있다. 2004년, A. Juels는 한 쌍의 RFID 태그가 인접해 있다는 것을 보장하기 위해 요킹증명이라는 새로운 아이디어를 제안했다[1]. 요킹증명에서 단일 RFID 리더는 한 쌍의 태그를 동시에 스캔하고, 이 사실을 확인할 수 있는 특수한 형태의 결과 값을 생성한다. 이 결과 값은 검증자에게 제출되고, 검증자는 제출된 결과 값을 통해 한 쌍의 태그들이 동시에 스캔 되었다는 사실을 확인할 수 있다.

요킹증명에는 여러 가지 유망한 응용 프로그램이 있다. 예를 들어, 의약품 생산 공정에서, 의약품과 의약품 설명서가 같이 포장되어 있는지 확인해야 하는 경우를 생각해볼 수 있다. 의약품과 의약품 설명서에 태그를 부착하면, 정상적인 제품을 스캔했을 때 한 쌍의 태그 응답을 얻을 수 있을 것이다. 이 태그 응답들이 동시에 스캔되었다는 것을 보장할 수 있다면, 특정 제품의 구성요소가 누락되지 않았다는 점을 확인할 수 있다. 그러나 일반적인 태그 스캐닝과 식별 과정으로는, 한 쌍의 태그 응답이 동시에 스캔되었는지 여부를 증명할 수 없다. 한 쌍의 태그 응답이 동시에 스캔 되었는지 여부를 증명하기 위해서는 일반적인 태그 스캐닝에 태그 스캐닝 시점에 관한 정보가 추가되어야 할 필요가 있다. 요킹증명은 태그 응답에 태그 스캐닝 시점에 대한 정보를 추가하여, 한 쌍의 태그가 동시에 스캔되었다는 것을 증명할 수 있다.

그러나 이전에 제안된 요킹증명 기법은 RFID 리더 장치와 검증자가 상호 연결되어 있어야 한다는 조건이 필수적이다[1-13]. 더욱이 [1-4]의 요킹증명 기법들은 올바른 증명 생성 프로세스를 방해하는 재전송 공격, 태그 위장, 증명 위조에 대한 적절한 대응책을 제공하지 않는다. Z. Zhou 등은 RFID 리더 장치와 검증자의 상호 연결 조건이 필요하지 않은 오프라인 그룹증명을 제안하였다[14]. 하지만, 해당 기법은 태그에게 ECC기반의 암호화 연산을 요구하며, 기존의 기법들에 비해 태그에 요구되는 계산량이 상대적으로 높다.

이 논문에서는 오프라인 검증을 보장하는 새로운 요킹증명 프로토콜을 제안한다. 이 연구의 기여는 다음과 같이 요약할 수 있다.

- 이 연구는 요킹증명의 새로운 접근 방식을 제안한다. 오프라인 검증 가능 요킹증명 프로토콜(OFF-V-Yoking proof)은 태그의 공간 데이터 및 약정 공개를 통해 오프라인 검증을 제공한다. 제안하는 오프라인 요킹증명 프로토콜의 검증 과정은 리더 단독으로 수행되며, 검증자는 검증에 필요한 약정 정보를 받는 초기 단계를 제외하면, 리더와 온라인으로 연결될 필요가 없다.
- 보안 및 프라이버시 보호 프로토콜 : 제안하는 프로토콜은 요킹증명 (재생 공격, 재조립 증명)을 위조하는 공격으로부터 안전하며 프라이버시 보호를 유지하기 위한 요구사항을 충족한다 (3장에 정의된 SR1 기밀성 및 SR2 연결 불가능성).
- 경량 프로토콜 : 오프라인으로 검증 가능한 요킹증명 프로토콜에는 암호화 해시 기능이 있는 태그가 필요하다. [2][7][14]에서 사용되는 암호화 기능이나 [1][2][4][8]에서 사용되는 타이머는 필요하지 않다.

II. 배경지식 및 관련연구

1. 온라인 검증이 가능한 요킹증명 프로토콜

A. Juels는 기본 요킹증명 프로토콜을 제안했다[1]. 요킹증명 프로토콜은 태그 쌍의 응답을 포함하는 증명을 생성하여, 해당 태그 쌍이 단일 세션에서 스캔 되었음을 증명한다. 증명 생성 과정에서, RFID 리더는 한 태그의 응답을 다른 태그에 대한 요청으로 사용 한다. 그러나 응답 사이의 시간 간격이 너무 길면 응답이 동시에 생성되었는지 여부를 확인할 수 없다. 따라서 모든 세션은 신뢰할 수 있는 증명을 생성하기 위해 적절한 시간 내에 완료되어야 한다. 이 프로토콜은 증명 생성 완료에 시간 제한을 적용하여 세션 시간을 제한한

다. 좀 더 구체적으로, 태그는 미리 정의된 시간이 만료되면 증명생성 과정을 종료한다. 요킹증명 프로토콜은 각 태그가 고유한 비밀키로 초기화되고 신뢰할 수 있는 검증자가 데이터베이스에 저장된 비밀키를 알고 있다고 가정한다. [표 1]은 프로토콜 및 기타 요킹증명 프로토콜의 절차를 표한하기 위한 표기법을 설명한다. [그림 1]은 TagA와 TagB라는 두 태그에 대한 요킹증명 생성 과정을 나타내며 세부 절차는 다음과 같다.

1. R은 Tag_A에 왼쪽 증명 쿼리를 보낸다.
2. Tag_A는 난수 r_A를 생성하고 ID A와 함께 R로 다시 보낸다.
3. R은 r_A를 사용하여 Tag_B에 올바른 증명 쿼리를 보낸다.
4. Tag_B는 비밀키 X_B 및 r_A를 사용하여 $mB = MAC_{XB}[r_A]$를 계산한다. 그런 다음 Tag_B는 난수 r_B를 생성하고 m_B 및 ID B와 함께 R로 다시 보낸다.
5. R은 r_B를 Tag_A로 보낸다.
6. Tag_A는 비밀키 X_A 및 r_B를 사용하여 $m_A = MAC_{XA}[r_B]$를 계산하고 이를 R로 다시 보낸다.
7. R은 그런 다음 증명, $P_{AB} = (A, B, m_A, m_B)$를 V로 보낸다.
8. V에는 태그의 비밀 매개 변수가 있는 데이터베이스가 있으므로 수신된 m_A 및 m_B로 자체 증명 P_{AB}를 생성하고 수신한 P_{AB}와 비교한다. 이 두 값이 동일하면 V는 Tag_A와 Tag_B가 동시에 존재하는지 확인한다. 시간 초과 또는 잘못된 입력 시 모든 참여자는 프로토콜 참여를 종료한다.

표 1. 표기법

Symbol	Description
V	검증자
R	리더 장치
Tag_A	태그 그룹의 초기 태그
Tag_B	태그 그룹의 다른 태그
ID_A or A	태그 A의 ID
ID_R	리더 장치의 ID
r_A	태그 A가 생성한 난수
r	검증자가 생성한 난수
C_A	태그 A의 카운터
X_A	태그 A의 대칭키
MACx[m]	키 x와 메시지 m을 입력받은 일방향 해시 함수
cmt, $cmtd$	요킹증명의 약정 (Commitment)와 공표 (Disclosure)
P_{AB}	태그 A와 태그 B의 요킹증명
Δ	사전에 정의된 Time window

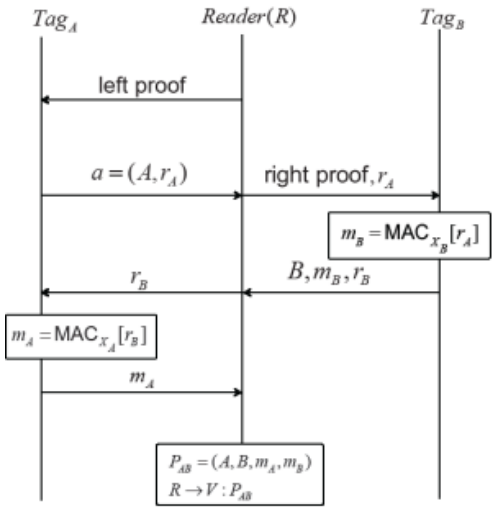

그림 1. Yoking-proof protocol

[1-4]의 시스템은 유효한 증명을 생성하기 위한 기본 요구사항을 만족할 수 없다. 이 문제를 해결하기 위해 [5-14]의 기법이 제안되었다. 그러나 해당 기법들은 암호화[2][7][10][14], PRNG[1][3][8-12], MAC [1-7][9][10], 타임 스탬프[2] 및 타이머[1][2][4][8] 같은 연산을 태그에서 수행해야 하며, [1-11][13]의 기법들은 해당 연산을 태그에서 하나 이상 수행해야 한다. 이 때문에 해당 기법들은 성능이 낮은 태그들 (예. 수동형 태그, 소형 태그 등)에 구현되기 어렵다.

2. 보안 위협

이 논문에서 가정하는 공격자의 목표는 1) 유효한 증명을 위조하고 2) 태그를 추적하는 것이다. 유효한 증명을 위조하기 위해 공격자는 다음 공격을 사용한다..

1. 재생 공격 [2][3] : 공격자는 이전에 스니핑 된 메시지를 재생하여 유효한 태그를 가장한다.
2. 재조립된 증명 : 공격자는 여러 개의 불완전한 증명을 결합하여 다중 증명 (N) 세션 공격 [5]과 같이 위조 증명을 생성하고, 검증 과정을 통과하는 것을 목표로 해당 공격을 시도한다.

Ⅲ. 제안 기법

이 절에서는 온라인 상의 검증자 없이 요킹증명을 검증하는 새로운 오프라인 요킹증명 프로토콜을 제안한다. 제안하는 프로토콜은 안전성 측면에서 기존에 제안된 기법들 [1-8]과 동등하거나 더 높은 안전성을 보장하며, 태그에게 더 적은 수의 연산 횟수를 필요로 한다. 좀 더 구체적으로, 제안 기법은 2절의 보안 위협에 대해 안전하며, 기존에 제안된 프로토콜과 동등하거나 더 낮은 연산량을 요구한다. 추가적으로, 제안 프로토콜은 한 쌍 이상의 태그에 대한 요킹증명을 효율적으로 생성할 수 있는 그룹 요킹증명 프로토콜로 확장을 지원한다.

1. 요킹증명 프로토콜에 대한 요구사항

RFID에 대한 요킹증명은 두 개체의 공존을 인증 할 수 있다. 요킹증명 프로토콜의 기본 요구사항 (R1, R2)와 안전한 요킹증명 생성을 위한 보안 요구사항 (SR1, SR2)는은 다음과 같다.

- R1 : 동일한 세션에서 단일 리더가 스캔 한 여러 태그는 증명을 생성 할 수 있어야 한다.
- R2 : 증명은 신뢰할 수 있는 개체에 의해 검증 가능하여야 한다.
- SR1 (기밀성) : 태그의 응답 과정에서, 태그를 식별할 수 있는 정보가 노출되지 않아야 한다.
- SR2 (연결 불가능성) : 태그의 응답 메시지를 통해 해당 태그를 특정할 수 없어야 한다.

2. 가정

다음은 요킹증명 프로토콜에 널리 적용되는 가정이다.

- 태그에는 일방향 해시 기능이 있다.
- 태그에는 유휴 시간 동안 무단 쿼리를 방지하기 위해 [15][16]의 프로토콜과 같은 액세스 제어 방법이 있다.
- 태그에는 타이머가 없다.
- 검증자와 리더는 신뢰할 수 있다.

3. 참여자 및 초기 설정

프로토콜의 참여자는 태그, 리더, 검증자이다. 프로토콜의 초기 설정 단계는 다음과 같다.

- RFID 시스템 S = {T1, T2,…, Tn}은 미리 정의된 m 개의 하위 그룹으로 나눌 n 개의 태그로 구성된다.
- Tsub = {$Tsub_1$, $Tsub_2$,…, $Tsub_m$} 각각에 대해 gt 태그가 있다. 여기서 n, m 및 gt는 각각 S의 태그 수, Tsub의 하위 그룹 수, 각 하위 그룹의 태그 수이다.
- 각 태그 Ti ($0 < i \leq n$)는 e-bit IDi, d-bit 비밀키 Xi 및 0으로 초기화되는 c-bit 카운터 값 Ci로 초기화된다.
- 검증자는 태그의 초기 매개 변수를 저장한다. 데이터베이스 VDB에서 확인 (ID, X, C, 하위 그룹 및 하위 그룹에있는 각 태그의 역할)을 수행한다.
- 검증자는 리더의 초기 매개 변수 (IDr 및 Xr) 를 사용하여 상호 인증을 수행한다.

하위 그룹의 분류는 기존의 일반 쿼리 기반 태그 스캔을 통해 달성할 수 있다. 하나의 쿼리에 여러 태그가 응답하면 서로 가까운 영역에 있음을 의미한다. 각 하위 그룹의 위치가 고정되어 있을 때, 리더가 하위 그룹 분류를 위해 태그를 스캔한 위치 정보는 n 개의 태그를 m 개의 하위 그룹으로 나누기 위해 사용되며, 하위 그룹 위치 정보 (SGLI)로 VDB에 저장된다.

4. 제안하는 오프라인 요킹증명 프로토콜

본 논문에서 제안하는 오프라인 검증 (OFF-V) 요킹증명 프로토콜은 다음 3단계로 구성된다 : (1) 태그별 Commit 생성 (2) 오프라인 요킹증명 생성 (3) 오프라인 검증

[그림 2]는 제안 프로토콜의 동작 과정을 나타낸 것이다. 한 쌍의 태그 Tag_A와 Tag_B의 오프라인 요킹증명 생성 및 검증 과정은 다음과 같다.

- **태그별 Commit 생성 단계**

1. 리더 R과 검증자 V 사이의 성공적인 상호 인증 단계 후, V는 k 비트 임의 값 r, 사전 계산된 증명 $PP_{AB} = (m_A, m_B, r)$ 및 Commit $cmt = f_{XR}[PP_{AB}, r]$를 생성한다. 그런 다음 SGLI 및 태그의 액세스 제어 권한과 함께 R에 해당 값들을 제공한다.

- **오프라인 증명 생성 단계**

2. R은 r을 두 부분 (r_{left} 및 r_{right})으로 나누고, r_{left}를 사용하여 시작 태그 Tag_A에 대한 증명 생성을 요청

한다. 여기서 r_{left} (또는 r_{right})는 최상위 비트 (또는 최하위 비트)의 r/2 비트 부분이다.

3. Tag_A는 왼쪽 증명 쿼리를보고 자신의 역할을 인식하고 각각 ra과 ma를 $f_{XA}[r_{left}, C_A]$ 및 $f_{XA}[ra, ID_A]$로 계산한다. 그런 다음 Tag_A는 ra과 ma를 모두 포함하는 메시지 m_A를 R에 다시 보내고 카운터 C_A를 1 증가시킨다.
4. R은 r_{right} 및 ma를 사용하여 오른쪽 증명 요청을 다른 태그 Tag_B로 보낸다. Tag_B는 rb와 mb를 각각 f_{XB} $[r_{right}, C_B]$와 $f_{XB}[rb, ID_B, ma]$로 계산하고, rb와 mb로 구성된 메시지 m_B로 리더에게 응답한 다음, 카운터 C_B를 1 증가시킨다.

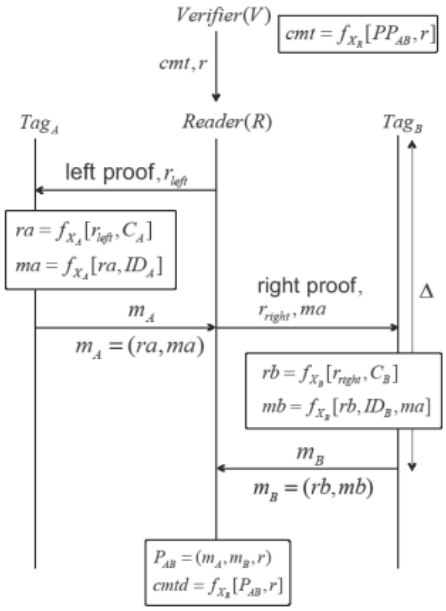

그림 2. 제안하는 OFF-V 요킹증명 프로토콜

- **오프라인 검증 단계**

5. 리더는 확약 공개 값 $cmtd$ = $f_{XR}[P_{AB}, r]$을 계산하여 증명 P_{AB} = (m_A, m_B, r)을 검증한다. cmt가 $cmtd$와 같으면 확인이 완료된다.

4. 그룹 요킹증명을 위한 확장

OFF-V 요킹증명 프로토콜은 추가 장치 없이도 오프라인 그룹 요킹증명 (OFF-V group proof) 프로토콜로 쉽게 확장될 수 있다. 한 쌍 이상의 태그에 대한 증명 생성 및 검증을 위해, 응답할 태그의 순서를 나타내는 left proof와 right proof는, 초기 설정 과정에서, Tsub에 미리 정의된 태그의 순차적 순서를 나타내는 일련 번호로 대체된다. 리더가 일련 번호로 쿼리를 보내면 태그가 그에 따라 응답하고 그룹 증명이 생성된다. 제안하는 OFF-V 그룹 요킹증명 프로토토콜은 생성된 그룹 증명의 검증은 일련번호를 확인하는 과정을 제외하면 확장 전의 과정과 동일하며, 그룹 증명의 생성 및 검증을 지원하는 기존의 기법들[2][7]처럼, 팔레트 태그와 같은 추가 장치가 필요하지 않다.

Ⅳ. 분석

1. 안전성

여기서는 제안 프로토콜이 3.1절의 R1, R2, SR1, SR2를 충족하면서 2.2절의 공격에 대해 안전함을 보인다. 안전성 분석을 위해, 2.2절의 공격을 통해 위조된 증거를 만들고 태그를 추적하려는 공격자 Adv를 가정한다. 공격자는 태그와 리더 구간의 모든 메시지를 수집할 수 있으며, 수집한 메시지의 수정, 재전송이 가능하다.

정리 : Adv는 ra, ma, rb, mb와 같은 해시 값을 얻을 수 있다. 하지만 해당 해시 값의 입력인 X_i, ID_i, C_i를 얻을 수 없다.

증명 : 임의 오라클 가정에서 Adv가 비밀 매개변수 (X_i, ID_i, C_i)로 생성된 l-bit 해시 (ra, ma, rb, mb)를 추측했을 때, 성공 확률은 2^{-l}이다.

주장 1 : 제안 프로토콜은 공격에 대해 R1 및 R2를 만족하는 요킹증명을 생성한다.

증명 (사례 1-재생 공격) : P_{AB} 및 cmt는 태그의 응답 메시지 (m_A 및 m_B)와 함께 생성된다. 해시 된 메시지는 C_A (또는 C_B)로 인해 변경된다 (3.4절, (2)오프라인 증명 생성의 3, 4단계). 따라서 Adv는 도청을 통해 얻은 이전 메시지의 재생 공격이 불가능하다.

증명 (사례 2 - 재조립된 증명) : 모든 하위 그룹이 이미 Tsub에 정의되어 있고 검증자가 VDB에 저장된 Tsub의 사전 지식을 통해 PP_{AB}를 계산하기 때문에 재조립된 증명은 검증할 수 없다 (3.4, 오프라인 검증 단

계, 5단계). 따라서 Adv는 재조립된 증명으로 검증을 통과할 수 없다.

주장 2 : 제안 프로토콜은 태그의 비밀 매개 변수를 공개하기 위해 위협에 대해 SR1을 충족한다.

증명 (기밀성) : 제안 프로토콜은 해시된 응답 메시지(**정리**)를 통해 SR1을 만족한다.

주장 3 : 제안 프로토콜은 특정 태그를 추적하는 위협에 대해 SR2를 만족한다.

증명 (연결 불가능성) : Adv에게 증명 생성 과정에서 스캔된 두 개의 태그 응답이 제시되었을 때, Adv는 증가된 카운터 (CA 및 CB)를 포함하여 해시된 응답 메시지가 동일한 태그에서 온 것인지, 서로 다른 태그로부터 온 것인지 구분할 수 없다. (3.4절, 2)오프라인 증명 생성의 3, 4단계). 따라서 제안 프로토콜은 SR2를 만족한다.

2. 효율성

태그의 계산 비용. 태그의 연산 비용을 기존에 제안된 요킹증명 프로토콜과 비교한다. 비교 대상의 조건은 1) 오프라인 요킹증명 혹은 오프라인 그룹증명을 지원하는 기법, 2) 태그 익명성을 보장하는 기법, 3) 태그에 공개키 연산을 적용하지 않은 기법, 이상 세 가지이다. [표 2]는 위 조건 1), 2)를 만족하는 기법들과 제안하는 OFF-V 요킹증명 프로토콜의 태그 연산 비용을 보여준다. 여기서 CTIMER, Cf, CMAC, CXOR, Cshift, CE는 각각 타이머, 해시 (또는 PRNG), MAC, XOR, Shift, Encryption 연산에 대한 비용이다. 결과는 제안된 프로토콜이 다른 방식보다 더 적은 연산을 태그에게 요구하는 것을 보여준다.

검색 비용. 태그 응답의 랜덤화로 인해 [5][6][8]의 프로토콜들의 검색 비용은 O(n)이다 ([2]의 경우 비용은 $O(n^2)$). 반면, 제안 기법인 OFF-V 요킹증명 프로토콜에서 검증 프로세스는 증명 태그를 식별하기 위한 검색 비용이 필요하지 않다. 태그별 Commit는 오프라인 확인 단계 (3.4절, 5 단계) 전에 미리 계산되어 있기 때문에, 리더는 스캔한 태그의 응답과 Disclosure 값을 비교하여 일치하는 값을 찾게 되며, 이 비용은 O(1)이다.

V. 결 론

이 논문에서는, 온라인 검증 없이 요킹증명을 검증하는 새로운 방법을 제안하였다. OFF-V 요킹증명 프로토콜은 태그의 위치 데이터 및 Commit 정보 공개를 통해 안전한 오프라인 검증을 제공한다. 분석에 따르면 제안하는 OFF-V 요킹증명 프로토콜은 태그의 위치추적 공격에 대해 안전하고, 증명생성 과정 동안 리더와 검증자의 연결이 유지될 필요가 없으며, 기존의 온라인 요킹증명 프로토콜보다 태그에 더 적은 양의 연산을 요구한다.

제안하는 프로토콜은 하나의 증명 생성에 참여하는 태그의 수가 한 쌍 이상일 경우에 그룹증명으로 확장을 지원한다. 하지만, 실제로 한 그룹에 포함될 수 있는 태그의 수에는 한계가 있을 것으로 보인다. 이는 다수의 태그를 스캔하고 증명을 생성하기 위해 필요한 시간이

표 2. 증명 생성 과정에 요구되는 태그의 연산 비용 비교

	Tag_A	Tag_B	Total
Anonymous yoking [4]	1CTIMER+2Cf+1CMAC+1Cshift	1CTIMER+1Cf+1CMAC+1Cshift	2CTIMER+3Cf+2CMAC+2Cshift
Clumping proof [5]	1CTIMER+1Cf+2CMAC+1CXOR+1Cshift	1CTIMER+1Cf+1CMAC+1CXOR+1Cshift	2CTIMER+2Cf+3CMAC+2CXOR+2Cshift
Kazahaya [9]	14Cf+12CXOR	11Cf+9CXOR	25Cf+21CXOR
MR-GP [10]	1CE+3Cf+1CMAC	1CE+3Cf+1CMAC	2CE+6Cf+2CMAC
제안기법	2MAC+1Cshift	2MAC+1Cshift	4MAC+2Cshift

길어질수록, 생성된 증명의 신뢰성이 떨어지기 때문이며, 향후에는 제안 기법을 실제로 구현하고, 증명 생성 시간이 일정 기준 이상으로 길어질 때 발생할 수 있는 공격 유형과 대응책에 대해 연구할 필요가 있다.

참 고 문 헌

[1] A. Juels, "Yoking proofs for RFID tags," Proceedings of the 2nd IEEE Annual Conference on Computing and Communication Workshops, pp.138-143, 2008.

[2] J. Saito and K. Sakurai, "Grouping proof for RFID tags," Proceedings of the 19th International Conference on Advanced Information Networking and Applications, Vol.2, pp.621-624, 2005.

[3] S. Piramuthu, "On existence proofs for multiple RFID tags," Proceeding of ACS/IEEE International Conference on Pervasive Services, pp.317-320, 2005.

[4] L. Bolotnyy and G. Robins, "Generalized yoking proofs for a group of RFID tags," Proceeding of the 3rd International Conference on Mobile and Ubiquitous Systems Workshops, pp.1-4, 2006.

[5] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda, "Solving the Simultaneous Scanning Problem Anonymously: Clumping Proofs for RFID Tags," Third International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, pp.55-60, 2007.

[6] J. S. Cho, S. S. Yeo, S. C. Hwang, S. Y. Rhee, and S. K. Kim, "Enhanced yoking proof protocols for RFID tags and tag groups," Proceedings of the 22nd International Conference on Advanced Information Networking and Applications Workshops, WAINA'08, pp.1591-1596, 2008.

[7] Y. Lien, X. Leng, K. Mayes, and J. Chiu, "Reading order independent grouping proof for RFID tags," Proceedings of the IEEE International Conference on Intelligence and Security Informatics, pp.128-136, IEEE, 2008.

[8] M. Burmester, B. Medeiros, and R. Motta, "PrOFF-Vably secure grouping proofs for RFID tags," Proceedings of the 8th IFIP international conference on Smart Card Research and Advanced Applications, pp.176-190, Springer Verlag, Berlin, Heidelberg, 2008.

[9] P. Peris-Lopez, A. Orfila, J. C. Hernandez-Castro, Vander Lubbe, and C. A. Jan, "Flaws on RFID Grouping-Proofs," Guidelines for Future Sound, J. Netw. Comput. Appl, Vol.4, No.3, pp.833-845, 2011.

[10] Yang, Ming-Hour, Luo, Jia, Lu, Shao, "A Novel Multilayered RFID Tagged Cargo Integrity Assurance Scheme," Sensors, Vol.15, No.10, MDPI, 2015.

[11] Z. Shi, X. Zhang, and J. Liu, "The Lightweight RFID Grouping-Proof Protocols with Identity Authentication and Forward Security," Wireless Communications and Mobile Computing, Article ID 8436917, 2020.

[12] Hong Liu, Huansheng Ning, Yinliang Yue, Yueliang Wan, and Laurence T. Yang, "Selective disclosure and yoking-proof based privacy-preserving authentication scheme for cloud assisted wearable devices," Future Generation Computer Systems, Vol.78, Part.3, pp.976-986, 2018.

[13] Wei Zhang, Shiming Qin, Shengming Wang, Longkai Wu, and Baolin Yi, "A New Scalable Lightweight Grouping Proof Protocol for RFID systems," Wireless Personal Communications, Vol.103, pp.133-143, 2018.

[14] Z. Zhou, P. Liu, Q. Liu, and G. Wang, "An Anonymous Offline RFID Grouping-Proof Protocol," Future Internet, Vol.10, No.1, p.2, 2018.

[15] "EPCglobal class1 gen2 RFID specifications," Whitepaper, 2008

[16] K. Finkenzeller, "RFID Handbook,

Fundamentals and Applications in Contactless Smart Cards and Identification," John Wiley and Sons Ltd,, pp.226-232, 2003.

저 자 소 개

함 형 민(HyoungMin Ham) 종신회원

- 2007년 2월 : 배재대학교 컴퓨터공학과(공학사)
- 2009년 2월 : 한양대학교 컴퓨터공학과(공학석사)
- 2018년 2월 : 연세대학교 컴퓨터과학과(공학박사)
- 2018년 4월 : 충남대학교 핀테크보안연구소 (책임연구원)
- 2020년 3월 : 배재대학교 사이버보안학과(조교수)

〈관심분야〉 : 정보보안, RFID, 스마트컨트랙트