효율적인 식별기능을 갖는 RFID 가변 정보화 방식

한승우, 최재귀, 박지환
부경대학교 전자계산학과
부경대학교 정보보호학과

RFID Variable ID Scheme with Efficient Identification

Seung-Wu Han, Jae-Gwi Choi, Ji-Hwan Park
Dept. of Computer Science, Pukyong Nat'l University
Dept. of Information Security, Pukyong Nat'l University

요 약

RFID 시스템에서 태그와 리더 사이의 통신은 Radio Frequency를 이용해서 이루어짐으로 공격자에 의해 도청될 수 있으며, 태그의 정보가 노출되면 사용자의 프라이버시 침해 문제를 가져올 수 있다. RFID 태그의 프라이버시를 보호하기 위해 제안된 대부분의 기존 방식들은 태그의 ID를 식별하기 위해 모든 태그에 대한 정보를 가지고 식별 과정을 수행해야 하는 비효율성을 가지고 있다. 본 논문에서는 태그의 출력을 매번 다르게 변화시켜, 태그에 대한 위치 추적을 불가능하게 하고, 3번의 지수연산만으로 해당 태그를 식별할 수 있는 RFID 가변 정보화 방식을 제안한다.

1. 서론

RFID(Radio Frequency IDentification)란 유비쿼터스 컴퓨팅의 요소기술이라 할 수 있는 무선인식 기술로서 Micro-chip을 내장한 태그(Tag)에 저장된 Data를 무선 주파수를 이용하여 리더(Reader)에서 자동 인식시켜 기존의 모든 바코드 시스템을 대체하여 사용되어 질 수 있다[1]. 또한 RFID는 바코드 시스템과 같은 다른 자동 인식 시스템과 공존 또는 보충하는 역할로서의 사용도 가능하며, 비 가시거리의 무선인식, Read & Write(Data Update), 재활용, Anti-collision (동시에 30~40개의 ID를 인식), 대량의 정보 저장 기능을 가지므로 칩의 저장능력과 인식능력의 정도에 따라 물류관리, 유통관리, 도난방지 등의 다양한 분야에 적용 가능한 핵심 기술로 주목받고 있다. 그러나 상품에 부착된 태그로 인해 소비자의 프라이버시(Privacy)가 침해되어질 수 있으므로 태그 사용자의 프라이버시 보호를 위한 방법을 필요로 한다.

본 논문에서는 효율적인 태그 식별기능을 갖는 RFID 가변 정보화 방식을 제안한다. 2절에서 RFID 시스템에 대하여 알아보고, 3절에서는 기존의 ID가변 정보화 방식을 분석하고, 4절에서는 기존의 방식을 개선한 제안방식을 기술하며, 5절에서 결론은 맺는다.

2. RFID 시스템

일반적인 RFID 시스템은 크게 안테나가 포함된 리더와 정보를 저장하고 프로토콜을 이용하여, 데이터를 교환하는 태그, Database로 구성된다. 그림1은 RFID 시스템의 구성을 나타내고 있다.

- **Reader**:읽기 쓰기가 가능하도록 하는 장치.

- **Tag**:데이터를 저장하는 핵심 기능을 담당.

- **Database**:태그와 관련된 정보를 저장·관리.

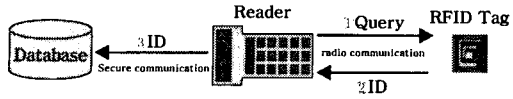

그림1. RFID 시스템의 구성도

일반적인 RFID 시스템의 통신에서 리더와 Database 사이의 통신은 안전한 통신방식을 이용하여 이루어지는데 반해[2], 태그와 리더 사이의 무선통신은 Radio Frequency를 사용하기 때문에 공격자에 의한 도청 가능성이 존재하게 된다. 공격자의 도청에 의해 태그의 정보가 노출되면 사용자는 프라이버시 침해를 입을 수 있다. 이에 RFID 프라이버시 문제를 해결하기 위해 많은 연구들이 이루어지고 있으며[3][4],다음 장에 제안방식의 기반이 되는 RFID가변 정보화 방식을 간단히 기술, 분석한다.

3. ID가변 정보화 방식[4]

이 방식은 Universal re-encryption[5]을 이용하여 태그의 정보를 가변 시켜 RFID시스템의 프라이버시 침해를 보호하는 방식이다. ID가변 정보화 방식을 적용한 시스템의 구성요소로는 태그, Database, 리더가 있으며, 리더는 ID판독용 리더와 One-time pad갱신용 리더로 세분화되어진다. 그림2는 ID가변 정보화 방식을 적용한 RFID시스템의 모델에 대한 구성을 나타낸다.

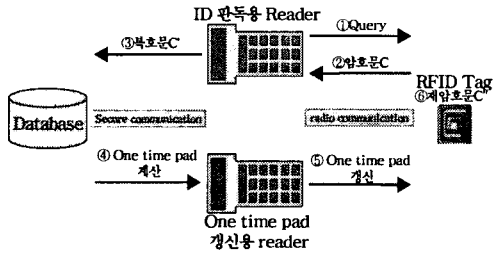

그림2. ID가변 정보화 방식을 적용한 RFID시스템의 구성

3.1 프로토콜

RFID시스템에서 ID가변 정보화 방식의 적용은 ElGamal 암호를 바탕으로 이루어진다[6][7].

- **키 생성**:태그의 비밀 키 x_t, 공개키 $y_t = g^{x_t}$를 생성하며, 각각의 키는 Database에서 보존된다.

- **암호화**:메시지 m, 공개키 y_t, 난수 $r=(k_0, k_1)$을 이용하여 식(1)과 같이 암호문 C를 생성한다.

$$C=[(\alpha_0, \beta_0);(\alpha_1, \beta_1)] \quad (1)$$

$$\alpha_0 = m y_t^{k_0},\ \beta_0 = g^{k_0},\ \alpha_1 = y_t^{k_1},\ \beta_1 = g^{k_1}$$

- **One-time pad생성**:Database는 태그의 암호문 C와 난수 $r=(l_1,\cdots,l_n)$을 이용 식(2)와 같이 One-time pad Δ를 생성.

$$\Delta = [(\alpha_1^{l_1}, \beta_1^{l_1}),\cdots,(\alpha_1^{l_n}, \beta_1^{l_n})] \quad (2)$$

One-time pad의 갱신은 갱신용 리더에 의해서 이루어진다.

- **복호화**:RFID Tag의 ID정보를 판독한 리더는 태그에 기입된 암호문 $C=[(\alpha_0, \beta_0);(\alpha_1, \beta_1)]$를 Database에게 전송. Database는 태그의 비밀 키를 이용하여 $\alpha_0 / \beta_0^{x_t} = m_0$와 $\alpha_1 / \beta_1^{x_t} = m_1$ 을 계산, $m_1=1$이라면 메시지 m_0가 태그의 ID정보가 되며, $m_1=1$이 아니면 복호화가 실패된 것을 나타낸다. 암호문 C가 여러 번 re-encryption 되었다 할지라도 한번의 복호화 과정으로 평문을 획득 할 수 있다.

- **re-encryption**:태그는 리더와 최초 통신을 한 후에는 다음의 One-time pad를 이용하여 태그의 이전 암호문 C를 재 암호화(re-encryption)한다. One-time pad $[(\alpha_1^{l_k}, \beta_1^{l_k}), (\alpha_1^{l_{k+1}}, \beta_1^{l_{k+1}})]$ $(k=1,2,\cdots,n)$에서 1회 갱신 시 2개의 요소씩 $\frac{n}{2}$번 사용 가능하며, 태그의 적절한 사용분야에 따라 크기는 가변적일 수 있다. re-encryption 은 식(3)과 같이 계산되어진다.

$$C'=[(\alpha_0', \beta_0');(\alpha_1', \beta_1')] \quad (3)$$

$$=[(\alpha_0 \cdot \alpha_1^{l_k}, \beta_0 \cdot \beta_1^{l_k});$$

$(\alpha_1 \cdot \alpha_1^{l_{k+1}},\ \beta_1 \cdot \beta_1^{l_{k+1}})]$

- **One-time pad갱신**:One-time pad는 Database에 의해 생성되고, One-time pad갱신용 리더를 통해 태그에 전송, 갱신된다. 그림3은 One-time pad 갱신과정을 나타낸다.

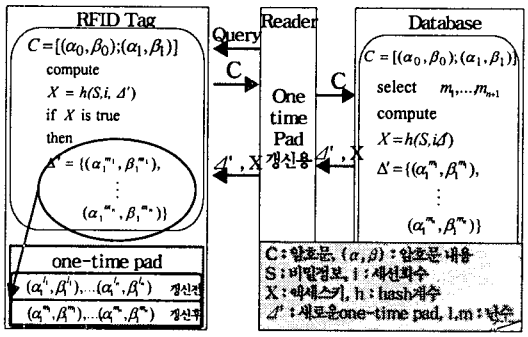

그림3. One-time pad 갱신

3.2 ID가변 정보화 방식의 문제점

ID가변 정보화 방식에서는 Database에서 판독용 리더로부터 수신 된 암호문 $C=[(\alpha_0, \beta_0);(\alpha_1, \beta_1)]$를 복호화 할 때, 보존되어 있는 모든 태그 사용자의 비밀 키로 $m_0 = \alpha_0 / \beta_0^{x_t}$와 $m_1 = \alpha_1 / \beta_1$ 를 계산해서 $m_1 = 1$이 되면 $m = m_0$로 복호화 되어 평문을 얻는다. 이 과정에서 $m_1 = 1$이 되는 것을 검색하기 위해서 최대 Database에 보관된 전체 태그 N개에 대해서 N번 지수연산의 계산 량을 가지게 된다. 계산 량을 줄이기 위해 태그의 공개키를 전송해서 해결가능 하지만, 통신을 할 때마다 같은 공개키가 전송되어진다면 익명성을 보장할 수 없다. 다음 장에서 우리는 3번의 지수연산만으로 태그의 ID를 식별할 수 있는 방식을 제안하여, ID가변 정보화 방식의 비효율적인 식별과정을 개선하고자 한다.

4. 제안방식

Database의 비밀 키를 x_B, 공개키를 y_B라 할 때, 태그에서 암호화 기법에 y_B를 적용하여 암호화하고 Database에서 x_B를 이용하여 이를 복호화 하게 되면 태그의 공개키를 익명화 시켜 전송할 수 있다. 즉, 데이터베이스에서 태그의 공개키를 가짐으로 이와 쌍이 되는 비밀 키를 쉽게 추출하여 기존의 N번 지수연산을 3번으로 줄일 수 있다. 제안 기법에서는 Database의 공개키를 re-encryption하는 부분이 추가되어짐으로 One-time pad의 크기가 늘어나게 되지만 태그의 적절한 사용분야에 따라 One-time pad의 길이를 가변적으로 사용한다면 이는 문제가 되지 않는다.

매개변수

- p: $q=(p-1)/2$인 소수, q:소수
- G:위수 $(p-1)$를 갖는 그룹
- g:그룹 G의 원시원소
- x_t:태그의 비밀 키
- y_t: $y_t = g^{x_t} \bmod p$인 태그의 공개키
- x_B:database의 비밀 키
- y_B: $y_B = g^{x_B} \bmod p$인 Database의 공개키

프로토콜

- **키 생성**:각 태그마다 비밀 키 x_t와 공개키 y_t, Database의 비밀 키 x_B, 공개키 y_B를 생성하며, 각각의 생성된 키는 Database에 보존된다.

- **암호화**:메시지 m, 태그의 공개키 y_t, 태그의 공개키를 전송하기 위해 Database의 비밀 키 x_B와 공개키 y_B 난수 $r=(k_0, k_1)$을 이용, 식(4)와 같이 암호문 C를 생성한다.

$C=[(\alpha_0, \beta_0, \gamma_0);(\alpha_1, \beta_1, \gamma_1)]$

(4)

$\alpha_0 = m y_t^{k_0}$, $\beta_0 = g^{k_0}$, $\alpha_1 = y_t^{k_1}$, $\beta_1 = g^{k_1}$

$\gamma_0 = y_t \cdot y_B^{k_0}$, $\gamma_1 = y_B^{k_1}$

암호화되어진 암호문 C는 판독용 리더에 의해서 Database에 전송된다.

- **복호화**:Database는 자신의 비밀 키로 태그가 송신한 태그의 공개키를 식(5)와 같이 복호화.

$\gamma_1/(\beta_1)^{x_B}=1$이 면 , $\gamma_0/(\beta_0)^{x_B}=y_t$

(5)

$y_B^{k_1} / g^{x_B \cdot k_1} = 1$, $y_t \cdot y_B^{k_0} / g^{x_B \cdot k_0} = y_t$

이와 같이 태그의 공개키 y_t를 획득하게 되면 공

개 키와 쌍이 되는 태그의 비밀 키 (x_t)를 쉽게 추출해낼 수 있고 이를 이용, $\alpha_0 / \beta_0^{x_t} = m_0$를 계산, m_0는 태그의 ID정보 m이 된다.

- **re-encryption**:태그가 리더와 최초 통신을 한 후, 태그는 다음의 One-time pad Δ에서 2개를 선택하여 이전 암호문 C를 re-encryption 한다.

$\Delta = [(\alpha_1^{l_k}, \beta_1^{l_k}, \gamma_1^{l_k}); (\alpha_1^{l_{k+1}}, \beta_1^{l_{k+1}}, \gamma_1^{l_{k+1}})]$ $(k=1,2,\cdots,n)$에서 1회 갱신 시 2개의 요소씩 $\frac{n}{2}$번 사용할 수 있으며, 태그의 사용분야에 따라 크기는 가변적일 수 있다. re-encryption은 식(6)과 같이 계산된다.

$$C' = [(\alpha_0', \beta_0', \gamma_0'); (\alpha_1', \beta_1', \gamma_1')] \quad (6)$$
$$= [(\alpha_0 \cdot \alpha_1^{l_k}, \beta_0 \cdot \beta_1^{l_k}, \gamma_0 \cdot \gamma_1^{l_k}); (\alpha_1 \cdot \alpha_1^{l_{k+1}}, \beta_1 \cdot \beta_1^{l_{k+1}}, \gamma_1 \cdot \gamma_1^{l_{k+1}})]$$

- **One-time pad갱신**:기존의 One-time pad갱신 기법과 같이 Database에 의해서 계산, 갱신용 리더에 의해서 갱신된다. 그림4는 제안기법의 One-time pad 갱신과정을 나타낸다.

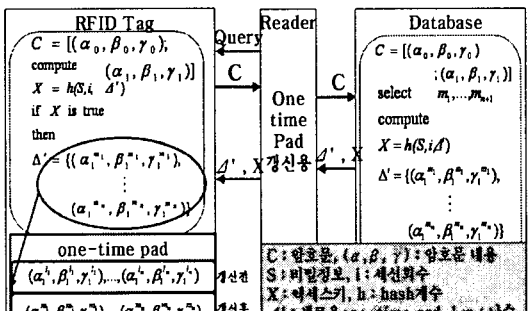

그림4. 제안기법의 One-time pad 갱신과정

5. 결론

본 논문에서는 RFID 시스템의 효율적인 식별과정을 가지는 ID가변 정보화 방식을 제안하여 태그 사용자의 익명성을 제공하였다. 기존의 RFID 시스템에서는 태그의 암호문을 ID정보 판독용 리더가 읽어 들인 후 Database에 전송하고, Database가 암호문을 복호화 한다. 이 과정에서 Database에 보관된 태그의 비밀 키를 가지고 복호화 과정을 수행하게 됨으로 최대 태그의 수만큼 N번 지수연산을 가져야 하지만 태그의 공개키를 전송함으로서 계산 량을 줄였다. 공개키를 전송하는 과정에 있어 태그의 익명성을 제공해야 함으로 Database의 비밀 키와 공개키를 생성, 이를 이용하여 태그의 공개키를 re-encryption하는 기법으로 기존 Database의 N번의 지수연산을 3번으로 수행, 효율적인 RFID 시스템을 구성하였다.

참고문헌

[1] S. Sarma. "Radio-frequency Identification systems", In B. Kalisky, editor, CHES '02. Springer-Verlag, 2002.

[2] D. Chaum. "Untraceable electronic mail, return address, and digital pseudonyms", Communication of ACM, 24(2):84-88. 1981.

[3] Stephen A. Weis, Sanjay E.Sarma, Ronald L. Rivest and Daiel W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification System", First International Conference on Security in Pervasive Computing, 2003.

[4] J. Saito. "Variable ID scheme for anonymity in RFID tags", The 2004 Symposium on Cryptography and Information Security, Vol.1, pp. 713-718, Jan. 2004.

[5] P. Golle, M. Jakobasson, A. Juels and P.Syverson, "Universal re-encryption for mixnet", To be appeared at RSA2004.

[6] Y. Tsiounis and M. Yung. "On the security of Elgmal-Based encryption", In Workshop on Practice and Theory in Public Key Cryptography(PKC '98), pp. 117-134. Springer, 1998. LNCS n0. 1431.

[7] T. ElGamal. "A public key cryptosystem and a signature scheme based on discrete logarithms", IEEE Transactions on information Theory, 31:469-472, 1985.