사용자 프라이버시 보호 및 추적이 가능한 EPC 시스템

정회원 곽 진*, 오 수 현**, 이 근 우***, 김 승 주****, 원 동 호*****

Fair EPC System

Jin Kwak*, Soohyun Oh**, Keunwoo Rhee***, Seungjoo Kim****, Dongho Won*****
Regular Members

요 약

저가의 RFID 시스템은 유비쿼터스 컴퓨팅 환경에서 유용하게 사용될 것으로 기대되고 있다. 그러나 RFID 시스템이 많은 장점을 가지고 있는 반면에 사용자의 프라이버시 침해라는 새로운 유형의 문제점 또한 가지고 있다. 본 논문에서는 저가의 RFID 시스템을 위한 "Fair EPC 시스템"을 제안한다. 제안하는 시스템은 원하지 않는(사용자가 인식하지 못하는) 스캐닝으로부터 사용자의 프라이버시 보호가 가능하고, 필요시 인가된 관리자들에 의해서만 태그의 추적이 가능하다 본 논문에서 제안하는 Fair EPC 시스템은 서로 다른 리더와 백-엔드 데이터베이스들의 연동을 통한 태그의 정보 유출이 불가능하므로 태그 정보의 노출에 대해 안전하며, 실제 시리얼 넘버의 복구(추적)이 필요한 경우, 암호학적인 비밀분산 방식을 사용하여 오직 인가된 관리자들에 의해서만 실제 시리얼 넘버를 복구(추적)할 수 있다 또한, 태그와 백-엔드 데이터베이스의 동기화를 제공하므로 백-엔드 데이터베이스에서의 계산 효율성을 제공할 수 있다

Key Words RFID system, EPC; privacy; unlinkable tag, traceable tag

ABSTRACT

The low-cost RFID system is expected to be widely used in the ubiquitous computing environment as an intelligent device. Although RFID systems have several advantages, they may create new threats to users' privacy. In this paper, a traceable and unlinkable RFID system called "Fair EPC System" is proposed for low-cost RFID tags The proposed system enables the protection of users' privacy from unwanted scanning, and it is traceable to the tag by authorized administrators when necessary The proposed system has some advantages, (1) eliminating any danger of exposing users' information via tag tracking through the cooperation between readers or back-end databases, (2) enabling the tracking of real serial number of the tag only through the cooperation of authorized administrators using a cryptographic secret sharing scheme, and (3) providing the efficiency of the proposed system reduce the computational workloads of back-end databases.

Ⅰ. 서 론

RFID(Radio Frequency Identification) 시스템은 RF 신호(Radio Frequency signal)를 통해 태그(tag)를 인식하고 관리하는 기술로, 유비쿼터스 컴퓨팅 (*Ubiquitous computing*) 환경에서 가장 중요한 기술로 많은 연구가 진행되고 있다. RFID 시스템은 물리적인 접촉 없이 태그의 정보를 읽거나 기록할 수 있

* 성균관대학교 정보통신공학부 정보통신보호연구실 박사과정(jkwak@dosan skku ac kr)
** 호서대학교 컴퓨터공학부 정보보호 전공 전임강사(shoh@office hoseo ac kr)
*** 성균관대학교 정보통신공학부 정보통신보호연구실 석사과정(kwrhee@dosan skku ac kr)
**** 성균관대학교 정보통신공학부 조교수(skim@ece skku ac kr)
***** 성균관대학교 정보통신공학부 정교수(dhwon@dosan skku ac kr)
논문번호 KICS2004-09-207, 접수일자 2004년 9월 27일
※ 본 논문은 2004년도 한국학술진흥재단의 지원에 의하여 연구되었음 (KRF-2004-003-D00390)

는 기술이며, 빠른 인식 속도와 기존의 바코드(barcode) 시스템에 비해 많은 저장 공간을 가지고 있으므로, 유통환경에서의 물류관리시스템(SCM Supply Chain Manage- ment) 등과 같은 분야에서 바코드 시스템을 대체할 새로운 시스템으로 주목받고 있다.[1,2,3,4]

RFID를 이용하는 인증 기술은 태그와 리더(reader) 사이의 물리적인 접촉 없이 인식이 가능하다는 장점을 가지고 있는 반면, 태그에 저장된 정보의 노출로 인한 사용자 프라이버시 침해와 같은 새로운 문제를 야기한다. 즉, RFID 시스템이 물류관리시스템에서 도난 방지와 위조 방지 등에 효율적인 사용이 가능하지만, 공격자가 특별한 지식 없이도 사용자의 신용정보와 물품 구매 성향 등과 같은 프라이버시에 관련된 정보에 접근 가능하다는 문제를 내포하고 있다

현재까지 이러한 사용자 프라이버시 문제를 해결하기 위한 몇몇 방법들이 제안되었으며, 대표적인 방법으로 kill 명령어를 이용한 "kill 명령어 기법(Kill Command method)"[5,6], "블로커 태그 기법(Brocker Tag)"[7], "해쉬 락 기법(Hash-Lock me- thod)"[8], "확장된 해쉬 락 기법(Randomized Hash- Lock method)"[9], "외부 재 암호화 기법(Re-en- cryption method)"[10], 그리고 "해쉬 체인 기반 기법(Hash-Chain based method)"[11] 등이 있다

먼저, 본 논문에서는 기존에 제안된 인증 기법들이 문제점을 분석하고, 이를 바탕으로 태그에 저장된 실제 시리얼 넘버(serial number)의 노출 없이 태그를 인증할 수 있는 "Fair EPC 시스템(FEPC)"을 제안한다 본 논문에서 제안하는 시스템은 리더와 백-엔드 데이터베이스(Back-end Database)에서도 실제 시리얼 넘버의 노출이 없으며, 이를 바탕으로 사용자의 프라이버시를 효율적으로 보호할 수 있는 시스템이다. 그러나 실제 시리얼 넘버를 추적해야 하는 필요성이 있을 경우, 인가된 관리자(authorized administrator)들의 협조에 의해서만 실제 시리얼 넘버를 추적할 수 있다

본 논문의 구성은 다음과 같다. 2장에서는 RFID 시스템과 EPC(Electronic Product Code) 시스템, 그리고 기존의 RFID 인증기법들의 특징과 문제점을 분석한다 3장에서는 2장의 연구 결과를 바탕으로 본 논문에서 제안하는 시스템의 요구사항에 대하여 정의하며, 4장에서 이러한 요구사항들을 만족시킬 수 있는 FEPC 시스템을 제안한다 제 5장에서는 제안하는 방식의 안전성에 대하여 분석하며, 마지막으로 6장에서 결론을 맺는다

Ⅱ. 관 련 연 구

1. RFID 시스템

RFID 시스템은 일반적으로 태그와 리더, 그리고 백-엔드 데이터베이스로 구성된다 그림 1은 RFID 시스템의 구성에 대하여 도식화 한 것이다. 그림 1에서의 전방위 영역(Forward range)은 리더가 RF 신호를 태그로 전송할 수 있는 영역이며, 후방위 영역(Backward range)은 태그가 리더의 요청에 대하여 태그의 정보를 리더에게 전송할 수 있는 영역이다 일반적으로, RFID 시스템에서의 공격자는 전방위 영역에서 전송되는 정보를 모니터링(monitoring) 할 수 있는 것으로 가정하며,[12,13,14] 리더와 태그 간의 통신 채널은 RF 신호를 이용하므로 도청이 가능한 불안전한 채널(insecure channel)이라 가정하고 백-엔드 데이터베이스와 리더 간의 통신 채널은 안전한 채널(secure channel)이라 가정한다.

□ 태그(Tag)

태그는 RFID 시스템에서 리더의 요청에 대하여 식별 데이터 정보를 송신하는 것으로 트랜스폰더(transponder)라고도 한다 태그는 일반적으로 IC 칩(Integrated Circuit chip)과 안테나(antenna)로 구성된다 태그 내의 IC 칩은 데이터의 저장과 논리적인 동작을 담당하고 안테나는 리더와의 통신에 사용된다. 태그는 전력을 공급받는 방식에 따라 능동형(Active tag)과 수동형 태그(Passive tag)로 구분된다

- **능동형 태그(Active tag)** · 태그에 자체 내장된 배터리로부터 전력을 공급 받으며, 원거리 정보 전송이 가능하다 그러나 배터리가 내장되어 있으므로 태그의 가격이 높으며, 태그의 수명이 배터리의 수명에 의해 좌우 된다는 단점이 있다.

- **수동형 태그(Passive tag)** 리더로부터 수신한 전자기파에 의한 유도전류를 태그의 전원으로 사용하며, 태그의 전송 전력이 리더의 전송 전력에 비해 상대적(1/10 정도)으로 낮기 때문에 주로 근거리 정보 전송에 이용된다. 수동형 태그는 배터리를 내장하고 있지 않으므로 태그의 가격이 낮으며, 태그의 수명이 반영구적이라는 장점을 갖고 있기 때문에 물류관리 분야에 주로 사용된다 본 논문에서는

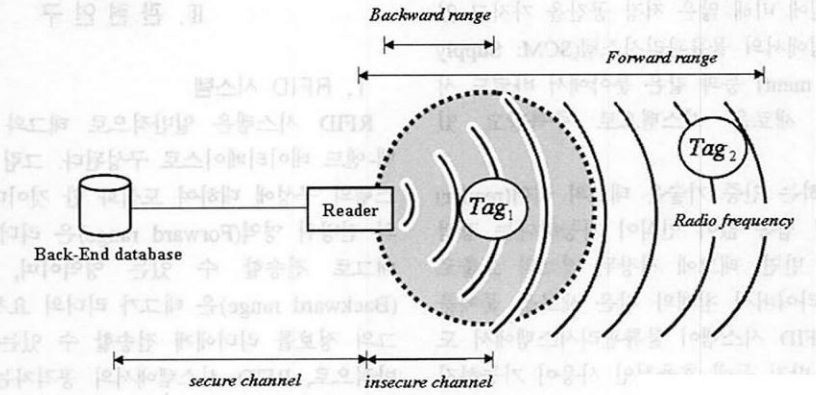

그림 1. 기본적인 RFID 시스템의 구성[14]

수동형 태그를 고려하여 시스템을 제안한다.

□ 리더(Reader)

리더는 태그가 송신한 식별 정보를 수신하여 태그를 인식하는 역할을 하는 장치로서 트랜시버 (transceiver) 라고도 한다. 리더는 태그에게 RF 신호를 전송하여 전력을 공급하고, 태그로부터 수신한 정보를 백-엔드 데이터베이스로 전송한다. 리더는 태그의 정보를 읽거나 기록할 수 있다. 일반적으로 리더는 RF 모듈(module)과 컨트롤 유닛 (control unit), 그리고 태그와의 RF 통신을 위한 결합장치(coupling element) 등으로 구성되어 있다.

□ 백-엔드 데이터베이스(Back-end Database)

백-엔드 데이터베이스(이하 DB)는 리더가 수집한 정보(예를 들어, 상품의 제조자 정보, 로그기록, 리더의 위치 등)를 저장하며, 연산 능력이 낮은 태그 또는 리더를 대신하여 복잡한 연산을 수행하는 장치다. 리더는 태그를 식별할 수 있는 정보를 저장하고 있으므로 리더가 태그로부터 수집한 정보의 진위 여부를 판별하는 기능을 수행한다.

2. EPC(Electronic Product Code) 시스템

RFID 태그가 차세대 바코드 시스템으로 물류관리시스템 등과 같은 분야에서 개별적인 상품에 대한 물류 추적 등에 광범위하게 사용될 것으로 기대하고 있다. 이에 1999년에 설립된 MIT의 Auto-ID Center[15]에서는 상품에 대한 식별 코드로서 EPC(Electronic Product Code)를 제안하였다. EPC는 각각의 상품에 할당되어 유일한 개체를 식별할 수 있도록 해주는 코드로서 특정 데이터 구조를 가지고 있다.[16,17,18] EPC는 헤더(Header), EPC 메니저(EPC Manager), 오브젝트 클래스(Object Class), 그리고 시리얼 넘버(Serial Number)로 구성되어 있다. 그림 2는 EPC의 종류를 나타낸 것이다.

- 헤더(Header) : EPC 버전(version), 시리얼 넘버의 길이(length), 태그의 종류 등을 나타내는 것으로 64비트

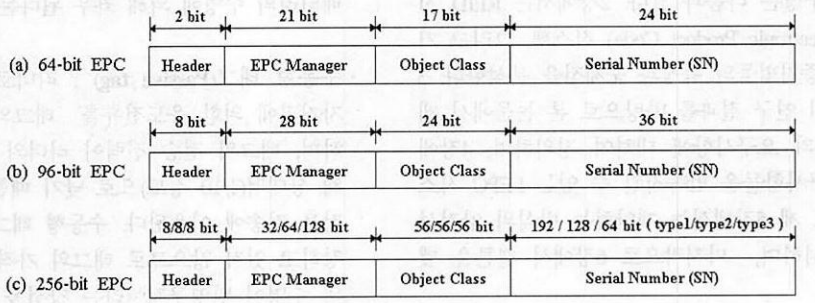

그림 2. (a)EPC-64, (b)EPC-96, (c)EPC-256 비트

(bit) EPC의 경우 2비트의 헤더를 가지고 있으며, 96/256비트 EPC의 경우 8비트의 헤더를 가지고 있다
- **EPC 메니저(EPC Manager)** 상품 번호와 상품의 일련번호 등의 관리 책임을 맡고 있는 상품 제조자를 나타낸다. (예, Coca-Cola Company)
- **오브젝트 클래스(Object Class)** 상품 분류번호를 나타내는 것으로 각 상품마다 유일한 식별 번호가 부여된다 (예, Coke 280ml can)
- **시리얼번호(Serial Number)** : 각 품목 내의 개별 상품에 대한 유일한 식별 번호를 나타낸다 시리얼 넘버는 각 품목 내에서 중복되어서는 안된다 (예, 유일한 Coke-280ml can)

3 기존 RFID 인증 기법들의 문제점

본 절에서는 물리적 보안 기법과 암호학적 보안 기법으로 분류하여 각 인증 기법들의 특징과 문제점에 대하여 분석한다

3.1 물리적 보안 기법

본 절에서는 물리적 보안 기법인 Kill 명령어 기법,[5,6] 페러데이 케이지(Faraday cage) 기법,[9] 액티브 재밍(Active Jamming) 기법,[7] 블로커 태그(Blocker tag) 기법,[7]에 대하여 분석한다

□ Kill 명령어 기법

Kill 명령어 기법은 MIT의 Auto-ID 센터에서 제안한 보안 기법으로, 태그가 자신의 데이터 필드에 저장된 패스워드(password)를 외부에서 받은 경우, 태그를 영구적으로 비활성화시킴으로써 더 이상 리더의 질의에 응답하지 않게 만드는 방법이다 태그가 Kill 명령어를 받으면, "self-destruct"라는 명령을 수행함으로써 태그 내의 메모리에 저장된 값을 모두 0으로 초기화한다. 그러나 Kill 명령어 기법은 명령이 수행된 이후, 제대로 완료되었는지 확인하기 어렵다는 단점을 가지고 있다. 또한 패스워드의 길이가 단지 8비트에 불과하므로 전수조사에 의한 공격(brute-force attack)이 가능하다는 문제점을 가지고 있다

□ 페러데이 케이지

페러데이 케이지 기법은 리더가 임의로 태그의 위치를 파악할 수 없도록 주파수가 투과할 수 없는 물질로 만들어진 페러데이 케이지 내부에 밀폐하는 기법을 말한다 이 기법은 태그를 소유한 주체의 위치 프라이버시 보호가 가능하지만, 페러데이 케이지의 크기와 설치 장소 등의 문제로 활용범위가 제한적이라는 문제점을 가지고 있다

□ 액티브 재밍

액티브 재밍 기법은 페러데이 케이지 기법과 유사하게 태그의 프라이버시를 보호하기 위한 물리적인 보안 기법이다. 태그를 소유한 주체는 주변에 설치된 리더의 동작을 방해하거나 차단하기 위해 또 다른 주파수 신호를 송출하는 장치를 휴대함으로써 태그에 대한 프라이버시를 보장 받을 수 있다. 그러나 이 장비에서 송출되는 신호가 너무 강하게 되면 프라이버시를 보장하지 않아도 되는 주변의 다른 태그나 리더들의 합법적인 동작을 방해할 수 있다는 단점을 가지고 있다

□ 블로커 태그

이 기법은 블로커 태그라고 불리는 태그를 추가적으로 부착함으로써 프라이버시를 보호하는 보안 기법이다 블로커 태그의 역할은 프라이버시가 요구되는 태그 정보를 요구하는 불법적인 리더의 요청에 대해 정당한 태그와 동일하게 정당한 인증 정보를 전송하지만 이에 그치지 않고 이진 트리와 연계된 모든 태그의 정보를 전송한다 이와 같은 동작을 수행함으로써 특정 태그에 대한 프라이버시를 보호한다 블로커 태그 기법은 액티브 재밍 기법보다 수동적인 형태를 갖지만 리더와 태그 사이의 통신에 참여한다.

이 기법은 태그에 대한 응답에 대해 충돌 회피 기법으로 제안된 tree-walking singulation protocol을 이용한다 이 기법을 사용함으로써 얻을 수 있는 장점으로는 이진 트리의 영역을 세분화하여 프라이버시가 요구되는 태그와 그렇지 않은 태그를 구분하고 특정 영역을 할당함으로써 유연성을 가질 수 있으며 분류된 영역을 통해 다양한 정책을 적용할 수 있다

3.2 암호학적 보안 기법

본 절에서는 해쉬 락 프로토콜(Hash-Lock)[8], 확장된 해쉬 락 프로토콜(Randomized hash-lock)[9], 외부 재 암호화 프로토콜(re-encryption)[10], 그리고 해쉬 체인 기반 프로토콜(Hash-chain based pro- tocol)[11]에 대하여 분석한다

□ 해쉬 락 프로토콜

해쉬 락 프로토콜은 태그의 ID를 은닉하기 위해 metaID를 이용하는 "locked"과정과 ID를 마지막 단계에서 노출하는 "unlocked"과정으로 분류할 수 있다. 태그가 가지고 있는 metaID는 매 세션마다 고정적으로 사용되기 때문에 공격자가 리더와 태그사이의 메시지를 모두 획득한다면, 동일한 metaID와 ID를 전송함으로써 재전송 공격을 수행할 수 있다 또한 공격자가 정당한 리더로 위장하여 태그에게 응답을 요청하고 획득한 metaID를 이용하여 키(key)를 획득하는 것이 가능하게 되고, 이를 이용하여 정당한 RFID 태그로 위장할 수 있는 스푸핑 공격이 가능하다는 단점을 가지고 있다

□ 확장된 해쉬 락 프로토콜

확장된 해쉬 락 프로토콜은 해쉬-락 프로토콜의 확장된 형태를 가진다 이 프로토콜에서 태그는 해쉬함수와 난수생성기의 기능을 가지고 있다 태그는 매 세션마다 난수생성기와 해쉬함수를 이용하여 새로운 인증 정보를 리더에게 전송하지만, 프로토콜의 마지막 부분에서 리더가 태그가 가지고 있는 것과 동일한 ID를 전송함으로써 공격자에 의한 프라이버시 침해 문제가 발생한다 또한, 리더와 태그사이에 전송된 메시지를 획득한 공격자는 해쉬 락 프로토콜과 동일하게 재전송 공격을 수행할 수 있다.

□ 외부 재 암호화 기법

외부 재 암호화 기법은 뱅크노트(banknote)[10]에 탑재된 태그의 프라이버시를 보장하기 위해 뱅크노트의 일련번호를 신뢰기관의 공개키를 이용하여 암호화하는 기법이다. 암호화된 일련번호는 추적을 어렵게 하기 위해서 주기적으로 재 암호화된다
이 프로토콜은 태그의 ID에 관련된 정보를 공개키 암호화 기법을 사용하여 개인 정보보호를 제공하기 때문에 기존의 프로토콜에 비해 높은 안전성을 갖는다 그러나 태그 내에서는 제한적인 연산 능력으로 인해 공개키 암호화 연산은 외부 장치에서 수행해야 한다. 암호화된 태그의 ID는 재 암호화를 수행하기 위한 주기 내에서 고정되어 있으므로 주기가 너무 길어서는 안된다 또한, 실질적인 공개키 암호화 연산을 외부 장치를 이용하여 수행하기 때문에 비현실적인 측면을 내포하고 있다.

□ 해쉬-체인 기반 기법

해쉬-체인(Hash-chain) 프로토콜은 서로 다른 두개의 해쉬함수를 사용하고 초기 비밀 정보를 갖는다 이 프로토콜은 두 개의 해쉬함수를 이용하여 리더에 대한 응답메시지들 간의 상관관계를 공격자가 추측하기 어렵도록 설계하였다. 따라서 이전의 응답메시지를 공격자가 알고 있다하더라도 다음 세션의 응답메시지를 생성할 수 없다.

이 프로토콜은 매 세션마다 서로 다른 인증정보를 사용하기 때문에 어떤 태그의 인증정보인지 구별할 수 없다 그러나 백-엔드 데이터베이스가 매 세션마다 고정된 초기 비밀 정보를 이용하기 때문에 이전 세션의 인증정보를 이용하여 재전송 공격과 스푸핑 공격을 수행할 수 있다.

Ⅲ. 제안하는 FEPC 시스템에 대한 보안 요구사항

사용자의 프라이버시를 보호하기 위해서는 정당한 리더와 DB라 할지라도 태그에 저장된 실제 시리얼 넘버를 알 수 없어야 하며, 단지 정당한 태그인지에 대한 인증 기능만을 제공해야 한다. 본 장에서는 제안하는 FEPC 시스템에 대한 요구사항을 설명한다

(1) 익명성 (Anonymity)

- 약 익명성(**weak anonymity**) . 태그로부터 전송된 응답의 수신자는 쿼리에 대한 정당한 응답임을 검증할 수 있어야 하지만, 어떤 태그로부터 생성된 것인지는 알 수 없어야 한다 본 논문에서의 약 익명성은 구별불가능성(**indistinguishability**)의 의미와 동일하다

- 강 익명성(**strong anonymity**) 태그로부터 전송된 응답의 수신자는 쿼리에 대한 정당한 응답임을 검증할 수 있어야 하지만, 동일한 태그로부터 생성된 여러 개의 응답들 중 어느 것인지 결정할 수 없어야 한다 본 논문에서의 강 익명성은 연동불가능성(***unlinkability***)의 의미와 동일하다.

(2) 키의 독립성 (Key Independence)

모든 태그에 사용되는 키(key)가 동일할 경우, 특정 태그에 저장된 키가 노출되었을 경우 모든 태그의 안전성에 영향을 미치게 된다 이러한 안전성의 이유로 인해 하나의 태그에 저장되어 있는 키의 노출이 다른 태그들의 안전성에 아무런 영향이 없어야 한다. 그러

므로, **forwad secrecy**를 만족시키기 위해 각각의 태그에는 서로 다른 키들이 저장되어야 한다.

(3) 추적가능성 (Traceability)

태그의 실제 시리얼 넘버는 평문형태가 아닌 암호화되어 AdminDB에 저장되어야 하며, 필요 시 관리자들의 상호 협력에 의해 실제 시리얼 넘버를 복구(또는 추적) 가능해야 한다.

Ⅳ. 제안하는 시스템

본 장에서는 사용자의 프라이버시를 제공하고, 필요 시 실제 시리얼 넘버를 복구(또는 추적)할 수 있는 개선된 EPC 시스템을 제안한다.

1 기본적인 FEPC 시스템

[시스템 파라미터]

- $g(),h()$. 일방향 해쉬함수 (one-way hash function)
- $\|$: 연접(concatenation)
- $query_i$ 리더로부터 태그로 전송되는 쿼리
- ID_{R_i} , ID_{DB_i} 리더 R 과 DB의 ID(Identity)

[초기 설정]

· 태그(***RFID tag, T***) 본 논문에서는 수동형 태그를 고려한다. 태그 T_i는 키 k_i와 시리얼 넘버 SN_i를 가지고 있다

- k_i : 각각의 태그 T_i에 저장되어 있는 유일한 키 k_i는 SN_i와 오브젝트 클래스에 해당하는 마스터 키 MK에 의해 생성된다 여기서 f 는 키 생성 함수이다.

$$k_i = f(SN_i, MK_{object})$$

- $metaSN_i$, SN_i와 ID_{DB_i}, 그리고 k_i를 사용하여 생성되는 값으로, T_i는 SN_i 대신 이 값을 리더에게 전송한다

· 리더(***RFID reader, R***) : R_i는 T_i에게 RF 신호를 보내고($query_i$) 태그로부터 수신한 정보를 DB에게 전송한다.

· 백-엔드 데이터베이스(***Back-end Database, DB***) : DB_i는 R_i로부터 수신한 데이터를 처리하는 시스템으로 충분한 계산 능력을 가지고 있다. 또한 DB_i는 실제 시리얼 넘버 SN_i가 아닌 각 T_i에 해당하는 $metaSN_i$을 저장하고 있다.

· **Admin** 데이터베이스(***AdminDB***) AdminDB는 모든 태그 T_i에 해당하는 $metaSN_i$를 저장하고 있으며, 각 태그에 해당하는 실제 SN_i는 마스터 키 K에 의해 암호화 되어 저장되어 있다 키 K는 n명의 관리자들에게 비밀분산 방식(secret sharing method)을 이용하여 분산되어 있다. 그러므로, 만약 AdminDB가 필요성에 SN_i을 복구(또는 추적)하기 위해서는 n개의 비밀 정보 중 적어도 $t(n \geq t)$개 이상의 정보를 수집하여 SN_i을 복구(또는 추적)할 수 있다.[20,21,22,23,24,25,26]

- Adm_i : AdminDB의 Adm_i는 키 K를 복구할 수 있는 비밀 분산 정보를 각각 나누어 가지고 있다.

- K · SN_i를 암호화 하는데 사용되는 비밀키

다음 그림 3은 일반적인 FEPC 시스템을 도식화 한 것이며, 동작 과정은 다음과 같다.

(1) R_i는 $query_i(= \{ID_{DB_i} \| ID_{R_i}\})$를 T_i에게 전송한다.
(2) $query_i$를 받은 T_i는 $metaSN_i(= h_{k_i}(SN_i, ID_{DB_i}))$을 계산한다.
(3) T_i는 계산한 $metaSN_i$을 $query_i$에 대한 응답으로 R_i에게 전송한다.
(4) R_i은 T_i으로부터 전송받은 $metaSN_i$과 함께 요청 메시지 $request_R (= \{ID_R \| metaSN_i\})$를 DB_i에게 전송한다
(5) DB_i는 ID_{R_i}를 검사하고, 자신이 저장하고 있는 모든 $metaSN_i$중에 전송받은 $metaSN_i$와 일치하는 값이 있는지를 검사한다. 일치하는 결과 값이 있을 경우 R_i에게 태그를 인증하는 $response_{R_i}$를 전송한다
(6) $response_R$를 전송받은 R_i는 그 값을 확인 한 후, 고객에게 상품의 가격을 부과하는 등의 처리를 수행한다

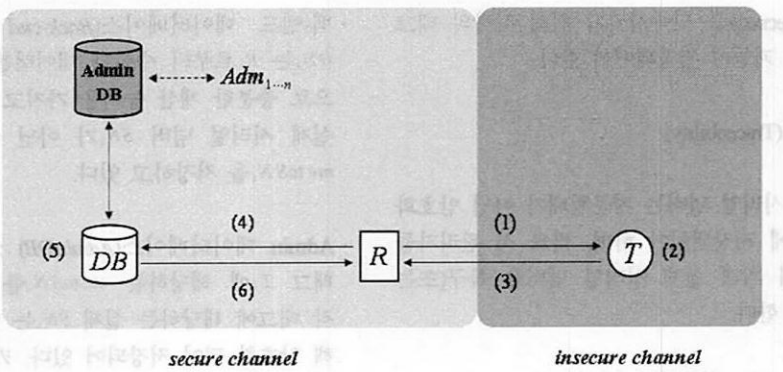

그림 3. 기본적인 FEPC 시스템

2. 제안하는 FEPC 시스템

앞 절의 일반적인 FEPC 시스템에서는 기존의 RFID 인증 기법들이 가지고 있는 트래킹과 재전송 공격에 대한 문제점이 여전히 존재한다.

- 트래킹(tracking) : 기존의 인증 기법들과 마찬가지로 태그에서 리더로 전송되는 정보가 고정되어 있으므로, 리더의 쿼리에 대한 응답이 항상 동일하다. 그러므로 공격자에 의한 트래킹이 가능하다는 문제점이 존재한다.

- 재전송 공격 (replay attack) : ID_R과 ID_{DB}가 공개정보 이므로 공격자에 의한 재전송 공격이 가능하다. 공격자는 리더와 태그 사이에 전송되는 정보를 도청(eavesdropping)하여 정당한 리더나 태그로 위장할 수 있다.

본 절에서는, $metaSN$과 랜덤 수 r을 사용하여 공격자에 의한 트래킹 문제를 해결하고, 리더에 의해 선택된 랜덤 수 r_R을 사용하여 재전송 공격을 방지할 수 있는 FEPC 시스템을 제안한다.

- T_i : i번째 RFID 태그를 의미하며, k_i와 SN_i를 저장하고 있다. 그림 4는 SN_i로부터 $metaSN_i$가 생성되는 과정을 나타낸다.

  - $metaSN_{ij}$: T_i의 j번째 $metaSN$. SN_i와 ID_{DB_i}, $r_{R_{ij}}$, 그리고 k_i에 의해 생성된다. T는 실제 시리얼 넘버 SN대신 $metaSN$값을 리더에게 전송한다. 예) $metaSN_{11}$ 은 DB_1에 저장되어 있으며, $metaSN_{12}$는 DB_2, $metaSN_{21}$은 DB_1에 저장되어 있다.

  - $count$: 이것은 T가 얼마나 많은 응답을 리더에게 하였는지를 나타내는 것으로, 본 논문에서는 DB의 계산 효율을 높여주는 역할을 한다. 또한 리더의 요청에 의한 T의 응답이 매번 다른 값이 출력되도록 랜덤화 하는 역할을 한다.

  - r_i : $metaSN_i$, $count$, 그리고 $r_{R_{ij}}$에 의해 생성되는 랜덤 값

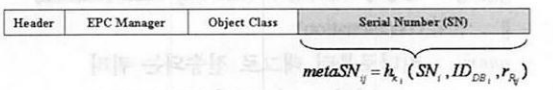

그림 4. SN_{ij}에 의해 생성되는 $meta\text{-}SN_{ij}$

- R_{ij} : i번째 DB에 연결되어 있는 j번째 리더

  - $r_{R_{ij}}$: R_{ij}에 의해 선택 된 랜덤 값

- DB : 리더로부터 전송된 정보를 처리하는 데이터 처리 시스템. DB는 데이터를 처리하기 위한 충분한 능력을 가지고 있다고 가정한다. DB_i는 $metaSN_{ij}$를 가지고 있으며, 그림 5는 각 DB_i에 저장되어 있는 데이터를 나타낸 것이다.

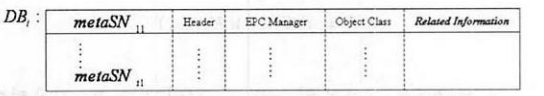

그림 5. DB에 저장되어 있는 정보

다음의 그림 6은 제안하는 FEPC 시스템을 나타낸 것이며, 동작과정은 다음과 같다.

(1) DB_i에 연결된 R_{ij}는 $query_i$를 T_i에게 전송한다.

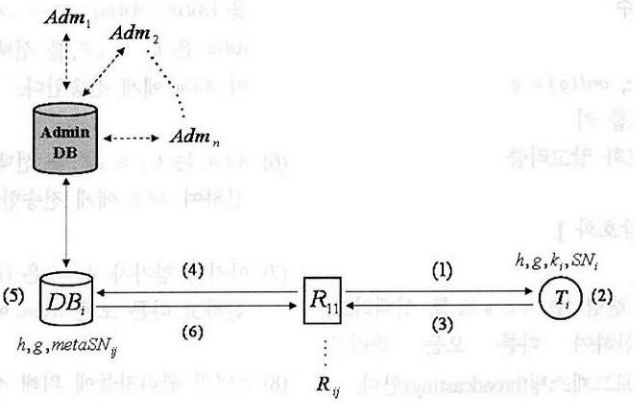

그림 6. FEPC : Fair EPC 시스템

$$query_i = \{ID_{DB_i} \,||\, ID_{R_{ij}} \,||\, r_{R_q}\}$$

(2) $query_i$를 수신한 T_i는 $metaSN_{ij}$와 r_i를 생성한다.

$$metaSN_{ij} = h_{k_i}\{SN_i, ID_{DB_i}, r_{R_q}\}$$
$$r_i = h(metaSN_{ij}, count = i, r_{R_q})$$

(3) T_i는 $metaSN_{ij}$값을 이용하여 응답을 생성하고 R_{ij}에게 다음을 전송한다.

$$g(r_i, metaSN_{ij}),\ count = i$$

(4) $g(r_i, metaSN_{ij})$과 $count$를 수신한 리더 R_{ij}는 $request_{R_q}$를 DB_i에게 전송한다.

$$request_{R_q} = \{ID_{R_q} \,||\, g(r_i, metaSN_{ij}) \,||\, count = i \,||\, r_{R_q}\}$$

(5) $request_{R_q}$를 수신 한 DB_i는 ID_{R_q}와 $count$를 확인하고, 자신이 저장하고 있는 $metaSN_{ij}$값과 수신한 $count$값을 이용하여 랜덤 값 r_i를 생성한다.

$$r_i = h(_{stored}\ metaSN_{ij},\ _{received}\ count = i,\ r_{R_q})$$

그리고 저장된 모든 $metaSN_{ij}$값에 대해서 계산한 r_i값을 이용하여 $g(r_i, _{stored}\ metaSN_{ij})$을 계산한다. 다음으로, 수신한 $g(r_i, metaSN_{ij})$값과 일치하는 값이 있는지 확인한다.

$$_{received}g(r_i, metaSN_{ij}) \stackrel{?}{=} _{computed}\ g(r_i, metaSN_{ij})$$

일치하는 값이 확인되면, DB_i는 $metaSN_{ij}$에 해당하는 관련 정보(예, 가격정보 등)를 R_{ij}에게 자신의 ID_{DB_i}와 함께 전송한다.

$$response_{R_{ij}} = \{ID_{DB_i} \,||\, related\ \ information\}$$

(6) $response_{R_{ij}}$를 수신한 R_{ij}는 사용자에게 요금부과 등과 같은 과정을 수행한다.

3. 개선된 FEPC 시스템 (Improved FEPC System without TTP)

제안하는 시스템의 경우, AdminDB의 관리자들이 동일한 마스터 키 K로 모든 SN_i를 암호화하여 저장하므로 하나의 SN_i가 복구되면 다른 $SN_j\,(i \neq j)$의 안전성에 영향을 미치게 된다. 본 절에서는 이러한 안전성의 문제를 해결하기 위해 암호학적인 비밀 분산 방식[23,24]을 적용한다. 비밀분산 방식은 TTP (Trusted Third Party, 신뢰기관)에 의해 마스터 키 K를 복구할 수 있는 분산 정보(share)를 관리자들에게 분배해 주는 방식으로, 한번 비밀정보가 복구되면 TTP에 의해 또 다시 분산 정보를 분배해야 한다. 그러나 본 논문에서 제안하는 개선된 FEPC(Improved FEPC) 시스템은 TTP를 사용하지 않으며, 하나의 비밀이 복구되더라도 분산 정보의 재사용이 가능하다.

[시스템 파라미터]

- Adm_i : AdminDB의 관리자
- P : 참가자 Adm_i의 집합,
  $P = \{Admin_1, Admin_2, \cdots\cdots Admin_n\}$

- p , $p > 2^{512}$인 큰 소수
- q $q \mid p-1$인 소수
- g , Z_p상의 원시 원소, $ord(g) = q$
- y_{Adm} : 관리자들의 그룹 키
- $ENC()$ 공개키 암호화 알고리즘

[시리얼 넘버 SN_i의 암호화]

(1) 각 Adm_i는 임의의 랜덤 수 $r_i \in_R Z_p$를 선택하고, $y_i = g^r \bmod p$를 계산하여 다른 모든 관리자 $Adm_j (i \neq j)$에게 브로드캐스팅(broadcasting)한다.

(2) r_i값에 대한 비밀분산을 수행하기 위해, 각 Adm_i는 Z_q상에서 $f_i(0) = r_i$를 만족하는 $t-1$차 다항식 f_i를 랜덤하게 선택한다.

$$f_i(x) = r_i + a_{i,1} x - a_{i,2} x^2 + \quad + a_{i,t-1} x^{t-1}$$

단, $a_{i,1}$, $a_{i,t-1} \in_R Z_q$이며, 각 Adm_i는 $f(j) \bmod q$를 계산하여 $Adm_j (i \neq j)$에게 안전하게 전송하고, 다음 값들을 브로드캐스팅한다.

$$g^{a_{i,1}} \bmod p, \quad \cdots, g^{a_{i,t-1}} \bmod p$$

(3) Adm_i는 $Adm_j (i \neq j)$로부터 받은 $f_j(i) (\forall j \neq i)$ 값에 대해 다음을 검사한다

$$g^{f_j(i)} = y_j \cdot (g^{a_{j,1}})^{i^1} \quad (g^{a_{j,t-1}})^{i^{t-1}} \bmod p$$

(4) $H = \{Adm_j\}$ 단계 (3)에서 속임(cheating)이 발견되지 않은 관리자} 라 하자 각 Adm_i는 자신의 분산 정보 s_i값을 다음과 같이 계산한다.

$$s_i = \sum_{j \in H} f_j(i)$$

그리고, 관리자들의 그룹 공개키 y_{Adm}과 $g^{a_0}, g^{a_1}, \cdots, g^{a_{t-1}}$값을 다음과 같이 계산한다.

$$y_{Adm} = \prod_{j \in H} y_j \cdot g^{a_{j,1}} = \prod_{j \in H} g^{a_{j,1}} \quad g^{a_{t-1}} = \prod_{j \in H} g^{a_{j,t-1}}$$

(5) SN_i를 암호화하기 위해 참가하는 관리자들의 집합을 $\{Adm_1, Adm_2, \cdots, Adm_n\}$이라 하자. 먼저, Adm_1은 $t_{1,1} \in_R Z_q$를 선택하고 $g^{t_{1,1}} \bmod p$를 계산하여 Adm_2에게 전송한다

(6) Adm_2는 $t_{1,2} \in_R Z_q$를 선택하고 $(g^{t_{1,1}})^{t_{1,2}} \bmod p$를 계산하여 Adm_3에게 전송한다.

(7) 마지막 참가자 Adm_n은 $(g^{t_{1,1} t_{1,2} \cdots})^{t_{1,n}} \bmod p$를 계산하고 다른 모든 Adm_r에게 전송한다.

(8) n명의 관리자들에 의해 생성된 SN_i의 암호문은 다음과 같다

$$ENC(SN_i) = (g^{k_i}, (y_{Adm})^{k_i} \cdot SN_i \bmod p)$$

(9) 각 Adm_i는 자신의 $AdminDB$에 $ENC(SN_i)$값과 관련 정보를 저장한다. 그림 7은 $AdminDB$에 저장되어 있는 정보를 나타낸 것이다.

$ENC(SN_1)$	$metaSN_1$	k_1	Header	EPC Manager	Object Class	ID_{SN_1}	
$ENC(SN_n)$	$metaSN_n$	k_n					

그림 7 $AdminDB$에 저장되어 있는 정보

[**AdminDB**에 의한 시리얼 넘버(SN_i) 복구]

SN_i를 복구하기 위한 허가된 관리자들의 집합을 $X = \{Adm_1, Adm_2, \cdots, Adm_t\}$라 하면, 복구 과정은 다음과 같다

(1) X에 속하는 모든 $Adm_i (Adm_i \in X)$들은 다항식 보간법을 이용하여 $r_1 + r_2 + \cdots r_t$를 계산한다[22]

(2) 각 $Adm_i (Adm_i \in X)$는 자신의 데이터베이스에 저장된 g^{k_i}값을 이용하여 다음을 계산한다.

$$K = (g^{k_i})^{r_1 + r_2 + \cdots + r_t}$$

(3) 각 $Adm_i (Adm_i \in X)$는 다음과 같이 SN_i를 복구한다

$$SN_i = ((y_{Adm})^{k_i} \cdot SN_i) / K$$

V. 안전성 분석

본 장에서는 Okubo et al[11]의 방법을 적용하여 제안하는 시스템의 안전성을 분석한다

[Definition 1] ***FEPC 시스템.*** 제안하는 **FEPC** 시스템은 태그(T), 리더(R), 백-엔드 데이터베이스(DB), 그리고 마스터 데이터베이스($AdminDB$)로 구성되며 다음과 같이 동작한다.

- T는 다음과 같이 동작한다.
  - 리더로부터의 쿼리 $query = \{ID_{DB} \mid\mid ID_R \mid\mid r_R\}$를 수신 한 후, 태그 T는 (k, SN)을 이용하여 $metaSN = h\{SN, ID_{DB}, r_R\}$과 $\imath = h(metaSN, count = \imath, r_R)$를 계산
  - $count = \imath + 1$로 업데이트(rewrite)
  - $g(r, metaSN)$과 $count = \imath$를 출력

- DB 는 $metaSN$을 저장하고 있으며, 다음과 같이 동작한다.
  - 리더로부터 $g(r, metaSN)$과 $count = \imath$를 수신
  - $(metaSN, count = \imath)$를 이용하여 T를 식별하고 응답으로 $response_R$ 전송

먼저, 구별불가능성**(Indistinguishability)**에 대한 안전성을 분석한다 이를 위해 인가되지 않은 개체, 즉 공격자 Eve_{md}를 가정한다. 공격자 Eve_{md}는 구별불가능성 특성에 대한 공격(예, 트래킹 시도)을 시도한다. 공격자는 태그의 출력을 언제든지 도청 가능하며, 랜덤 수와 T의 출력 $g(r, metaSN)$의 구별을 시도한다

[Definition 2] ***구별불가능성(Indistingushability).*** 인가되지 않은 공격자 Eve_{md}는 다음과 같은 공격을 수행한다.

- 오라클(oracle) T에 adaptively하게 접근 가능
  - . $query = (ID_{DB}, ID_R, r_R)$를 보내고 이의 응답으로 $(s, \imath)$ 를 수신, 여기서 $s = g(r, metaSN)$이고 $\imath = count$이다
- 오라클 DB에 adaptively하게 접근 가능.
  - · $(s, \imath)$를 DB에게 보내고 이에 대한 응답으로 $response_R = (ID_{DB} \mid\mid related\ \ information)$을 수신

공격자 Eve_{md}는 태그 T에게 $query = (ID_{DB}, ID_R, r_R)$를 보낼 때, $r \in_R \{0, 1\}$은 랜덤하게 선택한다 $r = 0$인 경우, Eve_{md}는 $(s', \imath)$를 수신하고, $r = 1$인 경우 Eve_{md}는 랜덤 수와 $\imath$를 수신한다 (단, s'은 Eve_{md}가 이전에 수신한 적이 없는 값이다) 마지막으로, Eve_{md}는 r을 추측하여 r'을 출력한다

$$Advantage_{Eve_{md}} = \{ \Pr [\ r' \leftarrow Eve_{md}, r = r'] - \frac{1}{2}\ \}$$

제안하는 FEPC 시스템에서, 임의의 확률론적 다항식 시간(probabilistic polynomial-time) 공격자 Eve_{md}의 어드벤티지(advantage)는 무시할 수 있다(negligible) 따라서, 제안하는 FEPC 시스템은 구별불가능성(indistinguishability) 특성을 갖는다

또한, $metaSN$이 비밀키 k_i를 이용하여 생성되므로 태그의 출력이 매번 다르게 출력된다 그러므로 비밀키 k를 알지못하는 공격자 Eve_{md}가 $metaSN$을 계산하는 것이 불가능하며, 인가되지 않은 공격자에 의한 트래킹이 불가능하다

[Theorem 1] ***함수 $h()$와 $g()$가 랜덤 오라클(random oracle)이라 가정하면, 제안하는 FEPC 시스템은 구별불가능성(Indistinguishability) 특성을 갖는다***

두 번째로, 연동불가능성**(Unlinkability)** 특성에 대한 안전성을 분석한다 이를 위해 인가되지 않은 개체, 즉 공격자 Eve_{lmk}를 가정한다. 공격자 Eve_{lmk}는 연동불가능성 특성에 대한 공격(즉, DB 간의 연동을 통해 출력 정보의 연관성을 알아내려는 공격)을 시도한다 공격자는 태그 T의 출력 (s, a)와 (s, s') 쌍에 대한 구별을 시도한다 여기서 $s = g(r, metaSN)$, $s' = g(r', metaSN)$, 그리고 a는 랜덤 수이다 공격자 Eve_{lmk}는 T에게 서로 다른 DB의 ID를 이용하여 $query$를 전송하고, 이에 대한 응답을 DB에게 전송하면 DB들은 서로 연동하여 응답에 대한 연관성을 찾고자 시도한다

[Definition 3] ***연동불가능성(Unlinkability).*** 공격자 Eve_{lmk}는 다음과 같은 공격을 수행한다.

- 오라클 T에 adaptively하게 접근 가능
  - : $query = (ID_{DB}, ID_R, r_R)$를 보내고 응답으로 $(s, \imath)$를 수신, 여기서 $s = g(r, metaSN)$이고 $\imath = count$이다

- 오라클 DB_1과 DB_2에 adaptively하게 접근 가능
  (s, t)를 DB에게 전송하고 이에 대한 응답으로 $response_R = (ID_{DB} \| related\ \ information)$을 수신

공격자 Eve_{lmk}가 데이터베이스 T에게 $query = (ID_{DB}, ID_R, r_R)$과 (ID_{DB}, ID_R, r_R)를 보낼 때, $r \in_R \{0\ 1\}$은 랜덤하게 선택한다. $r = 0$인 경우, 공격자는 $((s', t), (s'', t))$ 쌍을 받고, $r = 1$인 경우 공격자는 $((s', t), (a, t))$쌍을 받는다.(단, s', s''은 공격자가 이전에 받은 적이 없는 값이다) 마지막으로, 공격자 Eve_{lmk}는 r을 추측하여 r'을 출력한다.

$$Advantage_{Eve_{lmk}} = [\Pr[r' \leftarrow Eve_{lmk},\ r = r'] - \frac{1}{2}]$$

제안하는 FEPC 시스템에서, 임의의 확률론적 다항식 시간 공격자 Eve_{lmk}의 어드벤티지는 무시 할 수 있다(negligible) 따라서, 제안하는 시스템에서 DB 간의 연동을 통해서 태그 T의 출력 값 사이의 연관성을 찾는 것은 불가능하다.

또한, 비밀키 k와 실제 시리얼 넘버 SN을 알지 못하는 DB경우, 다른 DB들에 저장되어 있는 $metaSN$을 계산하는 것은 불가능하다

리더가 전송되는 데이터들을 수집하여 트래킹을 시도하는 경우, 태그로부터 전송되는 응답들이 매번 다르므로 동일한 태그로부터 전송되는지에 대한 판별이 불가능하다

[Theorem 2] *함수 $h()$와 $g()$가 랜덤 오라클(random oracle)이라 가정하면, 제안하는 FEPC 시스템은 연동 불가능성(Unlinkability) 특성을 갖는다.*

마지막으로, forward secrecy에 대한 공격자 $Eve_{forward}$는 하나의 태그(T_j)의 키가 노출된 경우, 이를 이용하여 다른 태그(T_i)의 키를 알아내려는 공격을 수행한다.

제안하는 시스템에서는, T_i는 일방향 해쉬함수를 이용하여 키 $k_i = f(SN_i, MK_{object})$를 생성한다 그러므로, 공격자 $Eve_{forward}$가 k_i를 획득하더라도 이를 이용하여 $key_i = f(SN_i, MK_{object})(i \neq j)$를 계산하기 위해서는 반드시 태그 j의 실제 시리얼 넘버 SN_j를 알아야한다. 그러나 제안하는 시스템에서 실제 SN_i은 평문 형태로 전송되거나 저장되지 않으므로, 노출된 하나의 키를 이용하여 다른 태그의 키를 구하는 것은 불가능하다. 즉, 제안하는 시스템에서 각 태그에서 사용하는 키들은 독립적(independent)이므로 제안하는 시스템은 forward secrecy를 만족한다.

VI. 결 론

본 논문에서는 "사용자 프라이버시 보호 및 추적이 가능한 EPC 시스템"을 제안하였다 본 논문에서 제안한 시스템은 일회용 $metaSN$을 사용하여 태그를 인증하며, 이는 리더의 쿼리에 대해 매번 다른 응답이 가능하게 해주는 역할을 하므로 실제 시리얼넘버의 노출 없이 태그를 인증하는 것이 가능하다 "Fair EPC 시스템"은, (1) 서로 다른 리더와 백-엔드 데이터베이스들의 연동을 통한 태그의 정보 유출이 불가능하므로 태그 정보의 노출에 대해 안전하며, (2) 필요 시, 암호학적인 비밀분산 방식을 사용하여 오직 인가된 관리자들에 의해서만 실제 시리얼 넘버를 복구(추적)할 수 있다. 또한 (3) $count$ 정보를 이용하여, 태그와 백-엔드 데이터베이스의 동기화를 제공하므로 백-엔드 데이터베이스에서의 계산 효율성을 제공할 수 있다 이러한 특징으로 인해 본 논문에서 제안하는 "Fair EPC 시스템"은 보다 안전한 사용자의 프라이버시 기능을 제공할 수 있으며, 기존의 방식들에서 문제가 되었던 데이터베이스에서의 보안문제를 해결할 수 있다. 본 논문에서 제안하는 시스템은 RFID를 이용한 물류관리스시템(SCM) 등에서 보다 효율적인 기능을 제공할 수 있을 것이다

참 고 문 헌

[1] D. M Ewatt and M Hayes "Gillette razors get new edge: RFID tags". *Information Week*, 13 January 2003. http //www informationweek.com

[2] S. E. Sarma "Towards the five-cent tag". *Technical Report MIT-AUTOID-WH-006*, MIT Auto ID Center, 2001. http //www autoidcenter.org

[3] S. E Sarma, S A Weis, and D W Engels "Radio-frequency identification security risks and challenges" *CryptoBytes*, 6(1), 2003.

[4] "Security technology: Where's the smart money?" *The Economist*, pp 69-70 9 February

2002

[5] S. E. Sarma, S. A.Weis, and D W Engels. "RFID systems, security and privacy implications" *Technical Report MIT-AUTOID-WH-014*, AutoID Center, MIT, 2002

[6] S. E. Sarma, S. A. Weis, and D W Engels. "Radio-frequency identification systems". *Workshop on Cryptographic Hardware and Embedded Systems*, CHES02, LNCS 2523, pp. 454-469, Springer-Verlag, 2002

[7] A Juels, R L Rivest and M Szydlo. "The Blocker Tag · Selective Blocking of RFID Tags for Consumer Privacy" *In Proceedings of 10th ACM Conference on Computer and Communications Security*, CCS 2003, pp 103-111, 2003.

[8] S A Weis. "Radio-frequency identification secu- rity and privacy" *Master's thesis*, M I.T May 2003.

[9] S A Weis, S Sarma, R Rivest, and D. Engels "Security and privacy aspects of low-cost radio frequency identification systems" *In First International Conference on Security in Pervasive Computing 2003*, LNCS 2802, pp 201-212, Springer-Verlag, 2004.

[10] A. Juels and R. Pappu. "Squealing Euros Privacy protection in RFID-enabled banknotes". *Financial Cryptography 03*, LNCS 2742, pp 103-121, Springer-Verlag, 2003.

[11] M. Ohkubo, K. Suzuki, and S. Kinoshita. "A Cryptographic Approach to "Privacy-Friendly" tag" RFID Privacy Workshop, Nov 2003 http·//www.rfid edu com/

[12] D Engels. "The Reader Collision Problem" *Technical Report MIT-AUTOID-WH-007*, MIT Auto ID Center, 2001 http·//www autoidcenter.org.

[13] K. Finkenzeller. *RFID Handbook*, John Wiley and Sons. 1999.

[14] T. Scharfeld. "An Analysis of the Fundamental Constraints on Low Cost Passive Radio-Frequency identification System Design" *MS Thesis, Department of Mechanical Engineering, Massachusetts Institute of Technology*, Cambridge, MA 02139, 2001

[15] MIT Auto-ID Center, http://www autoidcenter.org.

[16] D. L. Brock. "The electronic product code (EPC): A naming scheme for objects". *Technical Report MIT-AUTOID-WH-002*, MIT Auto ID Center, 2001. Available from http://www autoidcenter.org.

[17] D. L. Brock. "EPC Tag Data Specification". *Technical Report MIT-AUTOID-WH-025*, MIT Auto ID Center, 2003. http·//www autoidcenter org.

[18] D Engels. "EPC-256. The 256-bit Electronic Product Code Representation". Technical Report MIT- AUTOID-WH-010, MIT Auto ID Center, 2003. Available from http·//www autoidcenter org.

[19] "mCloak · Personal/corporate management of wireless devices and technology", 2003. Abailable form http://www.mobilecloak com

[20] C Cachin "On-Line Secret Sharing" *Cryptography and Coding: The 5th IMA Conf.*, LNCS 1025, pp. 190-198, Springer-Verlag, 1995

[21] L. Chen, D Gollmann, C J. Mitchell and P. Wild "Secret sharing with Reusable Polynomial" *Australasian Conference on Information Security and Privacy*, ACISP 97, LNCS 1270, pp 183-193, Springer-Verlag, 1997

[22] P. Fedlman "A Practical scheme for Non-interactive Verifiable secret sharing" *Proceeding of the 28th Annual Symposium on the Foundation of Computer Science*, pp. 427-437, 1987.

[23] S. J Kim, S J Park and D. H. Won. "Proxy Signatures, Revisited" *Proceedings of ICICS'97, International Conference on Information and Com- munications Security*, LNCS 1334, pp 223-232, Springer-Verlag, 1997

[24] T. P. Pedersen. "A Threshold cryptosystem without a trusted party". *Proceedings of Eurocrypt '91*, LNCS 547, Springer-verlag, 1991, pp 522-526.

[25] A. Shamir, "How to share a secret". *Communication of the ACM*, vol. 21, pp. 120-126, 1979.

[26] M. Tompa and H. Woll. "How to share a secret with cheater". *Journal of Cryptology*, vol. 1, pp. 133-138, 1988.

곽 진(Jin Kwak) 정회원

2000년 8월 : 성균관대학교 생물기전공학과 공학사.

2003년 2월 : 성균관대학교 대학원 전기전자및컴퓨터공학부 컴퓨터공학전공 공학석사.

2003년 3월~현재 : 성균관대학교 대학원 정보통신공학부 컴퓨터공학전공 박사과정.

<관심분야> 암호 알고리즘/프로토콜, 유비쿼터스 보안

오 수 현(Soo-hyun Oh) 정회원

1998년 2월 : 성균관대학교 정보공학과 공학사.

2000년 2월 : 성균관대학교 대학원 전기전자및컴퓨터공학부 컴퓨터공학전공 공학석사

2003년 8월 : 성균관대학교 대학원 전기전자및컴퓨터공학부 컴퓨터공학 전공 공학박사.

2004년 3월~현재 : 호서대학교 컴퓨터공학부 정보보호 전공 전임강사.

<관심분야> 암호 알고리즘/프로토콜, 유비쿼터스 보안

이 근 우(Keun-woo Rhee) 정회원

2004년 2월 : 성균관대학교 정보통신공학부 공학사

2004년 3월~현재 : 성균관대학교 대학원 정보통신공학부 컴퓨터공학전공 석사과정

<관심분야> 유비쿼터스 센서네트워크 보안

김 승 주(Seung-joo Kim) 정회원

1994년 2월 : 성균관대학교 정보공학과 공학사.

1996년 2월 : 성균관대학교 대학원 정보공학과 공학석사.

1999년 2월 : 성균관대학교 대학원 정보공학과 공학박사.

1998년 12월~2004년 2월 : 한국정보보호진흥원(KISA) 팀장.

2001년 4월~현재 : 한국정보보호학회 논문지편집위원

2002년 4월~현재 : 한국정보통신기술협회(TTA) IT 국제표준화 전문가

2004년 3월~현재 : 성균관대학교 정보통신공학부 조교수

<관심분야> 암호이론, 정보보호표준, 정보보호제품 및 스마트카드 보안성 평가, PET

원 동 호(Dong-ho Won) 정회원

성균관대학교 전자공학과 졸업(학사, 석사, 박사)

1978년~1980년 : 한국전자통신연구원 전임연구원

1985년~1986년 : 일본 동경공업대 객원연구원

1988년~2003년 : 성균관대학교 교학처장, 전기전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장, 한국정보보호학회장

1996년~1998년 : 국무총리실 정보화추진위원회 자문위원.

현재 : 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장, 정통부지정 정보보호인증기술연구센터장.

<관심분야> 암호이론, 정보이론, 신호처리