유비쿼터스 환경을 위한 암호 기술 동향

Trend of Cryptography for Ubiquitous Environment

홍도원(D.W. Hong) 정보보호기반연구팀 선임연구원, 팀장
장구영(K.Y. Chang) 정보보호기반연구팀 선임연구원
박태준(T.J. Park) 정보보호기반연구팀 선임연구원
정교일(K.I. Chung) 정보보호기반그룹 책임연구원, 그룹장

언제 어디서나 네트워크에 접근하여 경제적이고 편리하게 정보를 교환할 수 있는 유비쿼터스 환경이 제대로 갖추어지기 위해서는 보안 기술이 필수적인 요소이다. 기존 디바이스보다 작고, 경량이며, 값싸고, 이동 가능한 디바이스를 필요로 하는 유비쿼터스 컴퓨팅 및 네트워크 환경에서는 기존의 보안 기술을 그대로 적용하기는 어렵다. 그러므로 정보보호 기술의 핵심인 암호 기술도 유비쿼터스 환경에 적합한 형태로 변화 및 발전되어야 한다. 본 고에서는 유비쿼터스 환경에 적용하기 위해 개발되고 있는 최신 암호 기술에 대해 살펴본다. 특히 유비쿼터스 환경을 위한 구체적인 첫걸음인 RFID와 USN 시스템에 적용하기 위해 개발되고 있는 암호 기술과 앞으로의 환경 변화에서 더욱 중요성이 부각되고 있는 개인의 프라이버시 보호를 위한 암호 기술을 중심으로 분석한다.

I. 서 론

다가올 미래의 정보 통신 환경은 컴퓨터와 네트워크 기술이 융합되어 언제 어디서나 사용자가 네트워크에 접속 가능한 유비쿼터스 환경으로 진화할 것이다. 유비쿼터스 컴퓨팅 환경은 우리의 생활 속에 스며들어 사용자 자신이 인식하지 못하고 있는 사이에 이들 디바이스들의 도움을 받으며 좀 더 편리한 생활을 추구하고자 하는 것이다.

언제 어디서나 네트워크에 접근하여 경제적이고 편리하게 정보를 교환할 수 있는 유비쿼터스 환경이 제대로 갖추어지기 위해서는 보안 기술이 필수적인 요소이다. 현재의 유선 환경이 가지고 있는 보안 취약성과 마찬가지로 유비쿼터스 컴퓨팅 역시 보안에 취약한 점을 가지고 있다. 유비쿼터스 컴퓨팅 환경에서는 각 디바이스들이 생활의 곳곳에 널리 퍼져 있고 이러한 디바이스를 통해서 어느 곳에서나 정보의 이동이 용이하다. 이것은 어디에서든지 정보가 유출될 수 있음을 의미한다. 또한 이러한 정보 유출 문제 외에 개인의 프라이버시(privacy) 문제가 발생하게 된다. 최적의 유비쿼터스 환경을 구축하기 위해서 모여지는 정보는 사용자가 외부로 드러내지 않기를 원하는 정보일 수 있기 때문에 이러한 프라이버시 이슈의 경우 유비쿼터스 환경 구현에 심각한 문제점으로 드러나게 될 것이다.

따라서 유비쿼터스 환경이 제대로 갖추어지기 위해서는 보안 기술이 필수적인 요소이다. 기존 디바이스보다 작고(small), 경량(light weight)이며, 값싸고(cheap), 이동 가능한(mobile) 디바이스를 필요로 하는 유비쿼터스 컴퓨팅 및 네트워크 환경에서는 기존의 보안 기술을 그대로 적용하기는 어렵다. 그러므로 정보보호 기술의 핵심인 암호 기술도 유비쿼터스 환경에 적합한 형태로 변화 및 발전되어야 한다.

본 고에서는 유비쿼터스 환경에 적용하기 위해 개발되고 있는 최신 암호 기술에 대해 살펴본다. 특히 유비쿼터스 환경을 위한 구체적인 첫걸음인 RFID와 USN 시스템에 적용하기 위해 개발되고 있는 암호 기술과 앞으로의 환경 변화에서 더욱 중요성이 부각되고 있는 개인의 프라이버시 보호를 위한 암호 기술을 중심으로 분석한다.

II. RFID/USN을 위한 암호 기술

USN(Ubiquitous Sensor Network)은 필요한 것(곳)에 RFID(Radio Frequency IDentification) 태그를 부착하고 이를 통하여 기본적인 사물의 인식 정보는 물론 주변의 환경정보(온도, 습도, 오염 정보, 균열 정보 등)까지 센싱하여 이를 실시간으로 네트워크에 연결하고, 그 정보를 관리하는 것을 의미한다. 우선 인식 정보를 제공하는 RFID 태그를 중심으로 발전하고, 센싱 기능이 추가될 것으로 예상되며, 그 후 다기능 센싱 태그에 의한 상황인지처리 수준으로 진화하며, 최종적으로 개체간 통신 기능을 갖춘 지능형 네트워크로 발전될 전망이다[1].

USN은 동물 이력 관리 서비스, 홈네트워크와 연계된 환경 정보 센싱 서비스, 의료 약품 분야와 관련된 환경 정보 센싱 서비스, 자동차 분야의 RFID 태그 간 통신 서비스, 환경 관리 분야의 RFID 태그 간 통신 서비스, 물류 유통 분야의 RFID 태그 제어 서비스 등 다양한 응용 분야를 포함하고 있다. 하지만, RFID/USN의 도입에 따라 개인 프라이버시 위협을 비롯한 다양한 보안 문제점들이 제기되고 있다. 특히 태그 정보의 위변조, 위장 리더, DoS 공격, 네트워크에서 개인 추적 정보 유출 등의 보안 위협에 노출될 우려가 있다. 또한 RFID/USN 환경에서의 공격 대상은 기존의 컴퓨터에 저장된 정보 또는 통신 정보만이 아닌, 개인이 소유한 모든 물체 단위까지 침해 범위가 확대될 수 있기 때문에, 이는 RFID/USN 서비스 활성화에 심각한 장애 요인이 될 수 있다. 따라서, RFID/USN 서비스 활성화를 위해서는 이러한 RFID/USN에서의 보안 문제를 해결하기 위한 연구가 선행되어야만 한다.

USN은 전통적인 네트워크와 다른 특징을 가진다. 센서 네트워크를 경제적으로 구성하기 위해서 센서 디바이스는 에너지, 계산 능력 및 통신 능력이 제한되어 있으며, 전통적인 네트워크와는 달리 센서 노드는 종종 물리적 공격의 위협에 취약한 접근 영역(accessible area) 내에 배치될 수 있다. 또한 센서 네트워크는 주변의 물리적 환경이나 사람과 밀접하게 상호 작용을 하며, 이것은 새로운 보안 문제들을 야기시킨다. 이러한 이유로 기존의 보안 메커니즘을 RFID/USN에 직접 적용할 수 없으며, RFID/USN을 위한 새로운 보안 기술을 필요로 한다.

본 장에서는 RFID/USN에서의 이러한 보안 문제를 해결하기 위해 현재까지 알려진 RFID/USN 암호 기술을 분석한다.

1. 키 설정 기술

RFID/USN을 구성하기 위해 가장 먼저 고려해야 할 사항은 암호학적 키(cryptographic key)를 설정하는 문제이다. 이러한 키는 센서 노드 사이의 인증이나 센서 노드 사이에서 교환되는 정보의 보호를 제공하는 데 사용된다. 우선 공개키를 이용한 전통적인 키 설정 방법을 고려할 수 있다. 이 방법의 주요한 이점은 노드가 네트워크 내의 다른 노드와 안전하게 키를 설정할 수 있다는 것이다. 그러나, 현재의 센서 노드들은 제한된 컴퓨팅 파워를 가지기 때문에 공개키를 이용한 키 설정은 비현실적으로 판단된다. 키 설정 기술은 수백 또는 수천의 노드를 가지는 네트워크에서 적용된다. 게다가 기존의 네트워크와는 달리, 센서 네트워크 내의 센서 노드는 자신 근방의 노드 및 데이터 집합 노드(date aggregation node)와 키를 공유할 필요가 있다.

키 설정에 대한 단순한 방법은 네트워크 전체가 하나의 키를 공유하는 것이다. 그러나, 이 방법은 네트워크 내의 단지 하나의 노드가 훼손됨으로써 공유된 비밀키가 드러날 수 있고, 이에 따라 모든 네트워크의 트래픽에 대한 복호화가 가능해진다. 이러한 아이디어의 다른 적용으로 하나의 공유 키를 링크키(link key)들을 설정하는 데 사용하는 방법이 있다. 하나의 공유 키는 통신하는 노드 쌍 사이의 세션 키를 설정하는 데 사용하며, 세션 키 설정 후에는 노드들은 공유 키를 삭제한다. 그러나 이 방법은 초기 키 설정 이후, 새로운 노드의 추가가 불가능하다는 단점이 존재한다.

다른 기본적인 방법으로는 사전에 각각의 노드들의 쌍 사이에 유일한 대칭키를 공유하는 방법이 있

다. n개의 노드를 가지는 센서 네트워크에서, 각각의 노드는 n-1개의 키를 저장해야 하며, n(n-1)/2개의 키들이 설정될 필요가 있다. 이 방법은 전체 노드의 키를 저장해야 하는 메모리 요구사항 때문에, 메모리 제한적인 센서 네트워크 환경에서는 비현실적이다.

인가된(trusted) base station을 이용한 키 설정 기법이 대안일 수 있다[2]. 여기에서, 각각의 노드는 base station과 단지 하나의 키를 공유하며, base station을 통해 다른 노드와 키를 설정한다. 이 방법은 base station이 single point of failure가 되게 한다. 그러나, 하나의 base station만이 존재하기 때문에, 네트워크는 base station에 물리적 공격에 대한 위협을 개선한 tamper-resistant 패키징을 결합함으로써 이러한 문제점을 해결할 수 있다.

최근에는 대칭키의 큰 풀(pool)을 선택하고, 풀의 랜덤한 부분 집합을 각각의 센서 노드에 분배하는 random-key predistribution 프로토콜[3]이 제안되었다. 통신하기를 원하는 두 개의 노드는 그들이 공통 키(common key)를 공유할 수 있는지의 여부를 결정하기 위해 그들의 풀을 조사한다. 만약 원하는 키를 찾았다면, 그들은 공통 키를 공유한다. 그러나, 모든 노드들의 쌍이 공통 키를 공유할 수 있는 것은 아니다. 만약 키 설정 확률이 충분히 크다면, 노드들은 충분히 많은 노드와 키를 설정할 수 있다. 이러한 키 설정 방법은 인가된 base station 없이 키 설정을 할 수 있다는 장점이 있다. 하지만, 이러한 접근 방법은 충분히 많은 노드를 훼손시킬 수 있는 공격자가 키 풀을 완전이 재구성함으로써 이 스킴을 깰 수 있다는 단점이 존재한다.

향후 노드 훼손에 대한 회복력을 가지는 보다 좋은 random-key predistribution 프로토콜이나 공개키 암호에 대한 하드웨어 지원에 대한 조사 및 보다 효율적인 공개키 암호 스킴 등이 연구되어야 할 것으로 보인다. 궁극적으로 큰 규모의 센서 네트워크에 대한 단순한 키 설정을 지원하는 안전하고 효율적인 키 분배 메커니즘이 필요할 것으로 예상된다.

2. 기 제안된 보안 프로토콜

보안이 적용되지 않은 RFID/USN 기술은 개인 프라이버시 위협을 비롯한 다양한 문제점에 노출될 수 있다. 예를 들어, 태그가 부착된 소비자의 물건에 대한 추적을 통해 소비자의 위치 추적이 가능하며, 개개인이 가지고 다니는 물건들을 소비자 모르게 비밀리에 목록화하여 악용할 수 있다. 또한 태그가 출입 통제 시스템에 사용될 경우 악의적인 리더가 태그의 정보를 쉽게 읽어 들이고, 여기서 얻은 정보를 이용하여 태그를 위조하는 것이 가능하다. 이것은 태그의 정보에 대한 인증되지 않은 접근에서 비롯된다. 만약 태그의 메모리에 민감한 데이터가 저장되어 있다면, 이것은 심각한 보안 문제를 야기시킬 수 있다.

현재 RFID/USN에서의 이러한 보안 문제를 해결하기 위한 다양한 연구가 진행되고 있다. 이러한 연구의 일환으로 RFID 시스템에서 사용자 프라이버시를 보호를 위해 kill tag, faraday cage, 방해 전파(active jamming), blocker tag 등과 같은 물리적 레벨의 대응 기법[4]과 hash lock[5], 재암호화[6],[7] 등과 같이 암호 기술을 이용한 보호 기법이 제안되고 있다. 본 절에서는 물리적 레벨의 보호 기법이 아닌 암호 기술을 중심으로 한 RFID/USN에서의 보안 프로토콜을 분석한다.

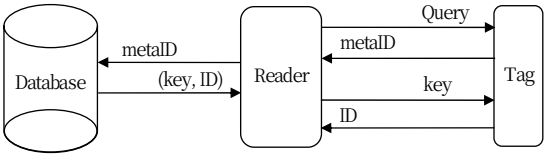
가. Hash Lock[5]

- Hash Lock의 locking 프로토콜

① 리더 R은 랜덤한 키 *key*를 선택하고, *meta ID* 값으로 *hash*(*key*)를 계산한다.
② R은 *metaID*를 태그 T에 기록한다.
③ T는 잠긴 상태(locked state)에 들어간다.
④ R은 (*metaID*, *key*)를 저장한다.

- Hash Lock의 unlocking 프로토콜((그림 1) 참조)

① 리더 R은 태그 T에게 T의 *metaID*를 질의한다.
② R은 데이터베이스에서 (*metaID*, *key*)를 조사한다.
③ R은 T에게 *key*를 전송한다.
④ 만약 hash(*key*)와 *metaID*가 일치하면, T는 잠긴 상태에서 빠져 나온다(unlock).



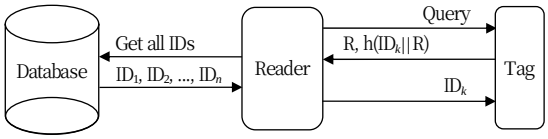
(그림 1) Hash Lock의 Unlocking 프로토콜

일방향 해시 함수의 역함수 계산 어려움에 기반한 Hash Lock 스킴은 인가받지 않은 리더기가 태그 콘텐츠 읽는 것을 방지할 수 있다. 위장(spoofing)은 방지하지 못하지만 탐지는 가능하다. 공격자는 태그에게 metaID를 요구한 후에 재전송 공격(replay attack)에서 합법적 리더기에게 태그를 위장하는 것이 가능하다. 그러면 합법적 리더기는 위장된 태그에게 키를 주게 된다. 그러나 리더기는 태그의 콘텐츠(일반적으로 태그의 ID)를 체크하여 백엔드 데이터베이스로부터 적절한 metaID인지를 검증할 수 있다. metaID가 부적절한 경우, 리더기는 적어도 위장이 발생했음을 경고할 수 있다.

Hash Lock은 태그에 해시 함수의 구현만을 요구하고, 백앤드에 키관리를 요구한다. 이러한 요구조건은 가까운 장래에 경제적인 것이 될 수 있다. 그러나, 위 방식에서는 metaID가 식별자처럼 사용되기 때문에 사용자 추적(tracking of individuals)이 가능하다.

나. Randomized Hash Lock[5]

Hash Lock 기법에서 가능한 사용자 추적을 방지하기 위한 방식이다. 태그는 인가되지 않은 사용자에 의한 질의에 대하여 예상 가능한 응답을 하지 않지만, 합법적인 리더기에 의해서는 여전히 식별 가능해야 하는 방식이다. 이 기법에서는 태그에 일방향 해시 함수와 난수발생기(PRNG)가 구축되어 있어야 한다. 합법적인 리더기는 태그를 스캔하기 전에 "knows what she owns"를 가정한다. 태그를 lock 상태로 만드는 것은 프로토콜이 필요 없는 간단한 과정이나, 태그를 unlock 상태로 하는 프로토콜은 필요하다. 태그를 unlock 상태로 하는 프로토콜은 다음과 같다((그림 2) 참조).



(그림 2) Randomized Hash Lock의 Unlocking 프로토콜

① 리더 R은 태그 T에게 질의를 보낸다.
② T는 랜덤한 난스(nonce) R을 생성하고, hash $(ID||R)$ 값을 계산한다.
③ T는 R에게 $(R, \text{hash}(ID||R))$을 전송한다.
④ R은 모든 알려진 ID_i값에 대해 $\text{hash}(ID_i||R)$을 계산한다.
⑤ 만약 $\text{hash}(ID_i||R) == \text{hash}(ID||R)$을 만족하는 ID_i를 찾는다면, R은 T에게 ID_i를 전송한다.
⑥ 만약 ID_i와 ID가 일치한다면, T는 잠긴 상태에서 빠져나온다.

이 방식은 초당 100~200개의 태그를 읽어야 하는 많은 개수의 태그를 소유한 환경에서는 비현실적이다. 그러나 상대적으로 적은 수의 태그 사용자를 갖는 환경에서는 가능한 방식이다. 소매 상점은 일반 사용자에 비해서 위치 프라이버시와 연관성이 적기 때문에 소매 상인들은 Hash Lock 기법을 적용하고, 구매하는 소비자에게는 randomized Hash Lock 기법을 적용한다. 한 가지 문제는 합법적인 리더기들이 어떻게 그들의 태그를 알게 되느냐는 것이다. 물건이 팔렸을 때, 그것의 ID도 반드시 같이 전송되어야 한다. 그렇지 않으면 새로운 소유주가 태그를 읽을 수 없다. 새로운 소유주가 자신의 태그에 접근하는 한 가지 방식이 printed master key를 사용하는 것이다.

위 방식이 충분히 현실적이지만 이론적으로 완벽하지는 않다. 이는 일방향 함수의 정의가 역함수 계산의 어려움만을 의미하기 때문이다. ID 비트가 노출되지 않음을 보장하기 위해서 보다 강한 프리미티브의 사용이 가능하다. 각 태그는 리더기와 유일한 비밀키를 공유한다고 하고, PRF(Pseudo-Random Function) 앙상블(ensemble)을 지원한다고 가정하면, 이론적으로 ID 비트 노출 방지가 가능하다. 구현상의 문제로 PRF 앙상블을 대칭키 암호화보다 아주

적은 자원으로 구현 가능하냐의 문제가 발생하는데, PRF 앙상블의 최소 하드웨어 복잡도는 open problem이다.

다. 재암호화

ECB(European Central Bank)는 법 집행 기관(law enforcement agent)에 의한 추적이 가능하도록 2005년부터 RFID를 고액의 유로화에 삽입하도록 제안하였다. 이에 Juels과 Pappu[7]는 지폐의 시리얼 넘버를 법 집행 공개키로 암호화하는 스킴을 제안하였다. 공개키에 의해 암호화된 암호문은 주어진 태그의 연결성(linkability)을 감소시키기 위해 주기적으로 재암호화(re-encryption) 된다. RFID 태그는 제한된 컴퓨팅 리소스를 가지기 때문에, 재암호화는 외부의 계산 기관(computing agent)에서 수행한다. 그러한 재암호화 기관의 정당한 행위는 은행이나 상점에서 지폐를 처리할 때 증명될 수 있다.

재암호화 스킴에서 RFID 태그는 공개키를 이용한 암호 연산을 수행할 수 없기 때문에 재암호화 기관 및 optical verifier에 대한 인프라가 필요하다. 그러나, 이러한 인프라는 부담이 될 수 있다.

Golle et al.[6]은 소비자의 상품에 삽입된 RFID 태그의 프라이버시 보호에 보다 적합한 universal re-encryption 스킴을 제안하였다. 이 스킴은 여러 개의 공개키를 사용하며, 연관된 공개키의 정보없이 암호문을 재암호화하는 것이 가능한 ElGamal 암호의 확장이다. 그러나, 이 기법도 Juels과 Pappu의 기법과 마찬가지로 재암호화 디바이스에 대한 별도의 인프라가 필요하다는 단점이 있다.

라. SPINS[2]

버클리 대학은 Smart-Dust 프로그램의 일환으로 작은 센서 디바이스의 네트워크에 대한 프로토타입을 구성하였다. 이 프로토타입은 외부 네트워크와의 연결을 담당하는 보다 강한 파워를 가지는 base station과 base station과 통신하는 작은 배터리 파워를 가지는 디바이스인 노드들로 구성된다. <표 1>은 이러한 Smart-Dust 노드들의 프로토타입에 대한 특징을 나타낸다.

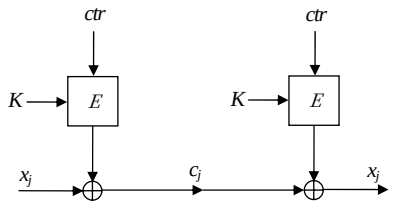
<표 1> Smart-Dust 노드들의 프로토타입에 대한 특징

CPU	8bit, 4 MHz
Storage	8 kbytes instruction flash
	512 bytes RAM
	512 bytes EEPROM
Communication	916 MHz radio
Bandwidth	10 kbps
Operating system	TinyOS
OS code space	3500 bytes
Available code space	4500 bytes

버클리 대학은 이러한 센서 네트워크 프로토타입에 대한 보안 프로토콜로 SNEP(Sensor Network Encryption Protocol)과 μTESLA로 구성된 SPINS (Security Protocol for Sensor Networks)를 채택하였다. SNEP는 기밀성, 양자간 데이터 인증, 무결성 및 적시성(freshness)을 제공하며, μTESLA는 데이터 브로드캐스트에 대한 인증을 제공한다. SPINS는 base station이 소스 라우팅(source routing)을 사용하여 노드들에 접근하는 아키텍처를 나타낸다.

SNEP에서 각각의 노드 N_j는 base station과 마스터 키 K_j를 공유하며, 이 마스터 키는 모든 다른 키를 유도하는 데 사용된다. 데이터 암호화 과정에서, 노드는 K_j로부터 유도된 키와 counter를 암호 알고리듬 RC5의 입력으로 사용하며, RC5는 one time 키로서 사용되는 비트 스트림을 생성한다. 이러한 one time 키를 메시지와 XOR하여 전송하며, 다음 메시지의 전송을 위해 counter 값을 증가시킨다. 노드의 counter 값과 마스터 키로부터 유도된 키를 알고 있는 base station은 같은 one time 키를 생성하여, 암호화된 메시지에 XOR 함으로써 원래의 메시지를 알 수 있다((그림 3) 참조).

μTESLA는 TESLA[8]의 확장이라고 볼 수 있다. TESLA는 초기(initial) 패킷을 인증하기 위해 디지털 서명을 사용하기 때문에, 이 기법을 센서 네트워크에 적용하는 것은 비현실적이다. μTESLA는 지연된 대칭키 공개 기법을 통해 비대칭키 도입에 따른 이러한 문제점를 극복하고 있다. μTESLA에서 base station이 인증된 정보를 노드에게 브로드캐



(그림 3) Counter를 이용한 암복호화 과정

스트하는 과정은 다음과 같다.

Base station은 패킷을 인증하기 위해 그 당시에는 비밀로 유지되는 있는 키를 사용하여 패킷에 대한 MAC을 계산한다. 센서 노드가 패킷을 전송받았을 때, 노드는 해당되는 MAC 키가 base station에 의해 아직 공개되지 않았다는 것을 증명할 수 있다. 노드는 MAC 키가 단지 base station만이 알고 있다는 사실을 알 수 있기 때문에, 어떤 공격자도 전송된 패킷을 변경할 수 없다는 사실을 확신할 수 있다. 이때에 노드는 버퍼에 패킷을 저장한다. 키 공개 시기가 오면, base station은 모든 노드에게 증명 키를 브로드캐스트한다. 공개된 키를 전송받은 노드는 그 키가 정당하는 것을 증명할 수 있다. 이러한 키의 정당성을 입증하기 위해서 μTESLA는 일방향 함수(one-way function)를 이용한 일방향 키 체인(one-way key chain) 기법을 사용한다. 만약 전송받은 키가 정당하다면, 노드는 전송받은 키를 이용하여 버퍼에 저장된 패킷을 인증한다. 이 기법은 수천 개 이상이 노드로 구성될 수 있는 큰 규모의 센서 네트워크에서는 비효율적이 될 수 있다.

3. 경량 암호 알고리듬 기술

지금까지 대부분의 RFID 시스템은 자동차, 마이크로칩 등과 같은 고가 품목들을 위해서 장착되었다. 이는 태그 비용을 US$0.50~US$1.00 또는 그 이상이 되도록 허락하였다. 이러한 가격에서는 태그에 많은 게이트 수를 허락하여 강한 암호 기능을 지원하는 것도 가능하였다. 더욱이 이러한 고가 태그는 물리적 차원의 제한 요소도 낮출 수 있다. 이들은 잘 보호되어서 상품에 안정적으로 부착되어질 수도 있다.

RFID 태그를 위해 가장 수지맞는 시장은 소비자 품목으로 UPC를 대체하는 것이다. 제조사들은 가격대가 5~10센트 정도면 간단한 EPC(Electronic Product Code)를 적용할 여유가 있다고 알려져 있다. 저비용 RFID 태그를 위한 더 많은 참고 자료는 단순한 5센트 EPC 타입 태그를 내포하고 있다. 이러한 저가형 태그에서 보안 기능을 제공하기 위해 사용할 수 있는 게이트의 수는 2,500~5,000개로 제한된다[9]. 하지만, 현재 사용되는 기존의 해시 함수나 블록 암호 알고리듬의 경우 저가형 태그에 그대로 적용할 수 없다. 따라서, 초경량, 저전력 환경에 적용 가능한 경량 암호 알고리듬의 필요성이 제기되고 있다.

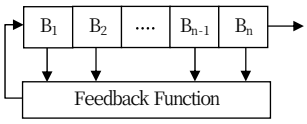
최근 CHES 2004에서 RFID 시스템에서의 인증을 위한 블록 암호 AES의 저전력, 저면적 구현 기법이 제안되었다[10]. 제안된 방법은 AES를 구현하기 위해 3,595게이트와 100kHz에서 8.15μA의 전류 소비량(0.35μm CMOS 공정)을 가지며, 128비트 암호화를 위해 약 1,000 clock cycle이 요구된다.

Weis[11]는 그의 MIT 석사 학위 논문에서 RFID 환경에 적합한 저비용 해시 함수 구현을 위한 핵심 논리로 CA로 불리는 셀룰러 오토마타(cellular automata)와 NLFSR(NonLinear Feedback Shift Register)로 명명한 비선형 궤환 시프트 레지스터를 추천하였다.

그러나, CA 기반 암호 논리는 Wolfram[12]이 처음 제안한 이후로 안전성에 많은 문제가 노출되어 암호학계의 주목을 끌지 못하고 있다. 다만, 하드웨어적으로 구현이 용이하다는 이유 때문에 아직도 관심 대상에 올라와 있는 것으로 보여진다.

NLFSR은 LFSR에서 궤환 함수(feedback function)를 비선형으로 택한 논리이다. (그림 4)의 궤환 함수 내에 P-box라고 불리는 작은 비선형 치환 테이블을 놓고 이를 이용하여 레지스터의 상태(state)를 변환시킨다.

NLFSR은 기존의 LFSR 기반 스트림 암호에 비해서 낮은 복잡도로 비선형성이 높은 출력 수열을 얻을 수 있다. 그러나 주기와 선형 복잡도 등과 같은



(그림 4) NLFSR의 구조

기본적인 안전성 분석 요소도 알려져 있지 않은 새로운 논리이기 때문에 앞으로 많은 연구가 이루어져야 한다. 안전성이 보장되지 않는 암호 논리는 아무리 구현이 용이할지라도 사용될 수 없기 때문이다.

Ⅲ. 프라이버시 보호를 위한 암호기술

프라이버시는 익명성과 밀접한 관계가 있다. 프라이버시는 대중 속에 섞여 구분되지 않는 한 보장되지만, 반대로 익명성을 악용한 불법적인 행위를 막아야 한다. 따라서 익명성 보호를 위한 암호 프로토콜은 법적인 분쟁이 있을 때를 대비한 추적 기능도 포함하는 경우가 많다. 익명성을 보호하는 암호 프로토콜은 그룹 서명(group signature), blind 서명, ring 서명, anonymous credential, mix network 등이 있다.

유비쿼터스 환경에서는 정보보호의 대상이 일대일 관계가 아니라 개인 대 그룹, 그룹 대 그룹으로 바뀌어 간다. 따라서 전통적인 방법으로는 안전성을 유지할 수 없다. 비밀 키를 그룹의 일원이 공유함으로써 비밀 유출을 막는 것을 threshold cryptography라 하며, 현재 활발히 연구되고 있는 분야이다.

1. 그룹 서명

그룹 서명은 1991년 D. Chaum과 Van Heyst [13]에 의해 처음으로 제안되었다. 그룹 서명은 그룹의 구성원이 그룹을 대표하여 서명하며, 서명자가 누구인지 알려져서는 안되며, 분쟁 시 그룹 관리자에 의해 서명자의 신원이 밝혀져야 한다. 그룹서명은 효율성 제고와 부가기능 향상이라는 두 가지 측면에서 발전하여 왔다. 현재 가장 효율적인 그룹 서명은 Strong-RSA 가정에 기반을 둔 것이다[14]. 그룹 서명에는 위의 세 가지 성질 이외에 다른 부가적인 기능을 갖고 있는 것들이 있는데 예를 들면, 그룹 멤버가 탈퇴할 경우 전체 그룹 서명에 영향을 미치지 않는 것(revocation)[15] 등이 있다. 최근에 그룹서명의 성질을 요구하는 여러 프로젝트들이 있었다. 일례로 미국 Department of Transportation이 진행중인 Vehicle Safety Communications 시스템은 그룹 서명을 이용한다. 이 시스템은 자동차에 근거리 송신기를 장착하여 위급 상황이 되면 주변 자동차에 자신의 정보를 알려준다. 예를 들어 급브레이크를 밟는 상황이 되면 주변의 모든 자동차에게 주의 메시지를 보내는 식이다. 메시지 스푸핑을 막기 위해 이 시스템에서 전송되는 모든 메시지는 서명이 되어야 하며 자동차 운전자의 프라이버시 보호를 위해 그룹서명을 사용하게 된다. 효율적인 그룹서명을 위해 서명의 길이가 짧아야 하며 현재 가장 짧은 그룹 서명은 대략 200비트 정도이다[16].

2. Ring 서명

Ring 서명은 2001년 Rivest, Shamir 그리고 Tauman[17]에 의해 제안되었다. Ring 서명은 그룹서명과 거의 유사하며, 그룹 관리자가 없다는 점이 다르다. 따라서 서명자가 누구인지 추적할 수가 없다. Ring 서명의 응용으로는 내부 고발을 생각할 수 있다. 내부의 비리를 외부 언론에 알릴 때 그룹서명을 이용하면 그룹 관리자에 의해 누가 고발자인지 알 수 있지만 ring 서명을 하면 고발자에 대한 무조건적인 익명성이 지켜진다. 또 다른 응용으로는 ad-hoc 그룹에 대한 것이 있다. 유비쿼터스 환경에서는 수많은 컴퓨팅 디바이스들이 통신을 하며 필요에 따라 그룹을 만들기도 하고 해체하기도 한다. 이를 ad-hoc 그룹이라고 하는데, 그룹 관리자를 두는 것이 불가능하기 때문에 그룹 구성원 n명 중 k명의 동의에 의해 서명을 만드는 threshold ring 서명으로 응용된다[18].

3. Blind 서명

Blind 서명은 프라이버시 보호를 위한 기본 프리미티브로서 전자화폐를 위한 프로토콜이며, 1981년

에 Chaum[19]이 RSA에 기반을 둔 프로토콜을 제안하였다. Blind 서명이란 사용자가 메시지에 대한 서명을 받는 경우, 서명자는 서명한 메시지에 대한 정보를 전혀 알 수 없도록 해야 하며, 사용자는 메시지 하나에 오직 한 번만 유효한 서명을 받아야 한다. 예를 들어, 은행은 서명을 통해 화폐에 대한 신용을 보장하지만, 화폐 소유자에 대한 익명성을 보증해야 하고 중복 발행을 막아야 한다. 필요에 따라서는 불법적인 돈의 유통을 막기 위해 법 집행기관을 통한 추적 기능을 첨가하는 추세이다. 실제 사용 가능한 시스템은 Brands[20]에 의해 1993년에 제안되었고, 안전성에 대한 증명은 2001년에 Bellare 등[21]에 의해 이루어지기 시작했다. Blind 서명은 사용자에게 완벽한 익명성을 주기 때문에 전자 투표에 이용되기도 한다. 현재 blind 서명에 대한 연구 동향은 효율성 향상, 추적기능 강화에 있다.

4. Anonymous Credential

Anonymous credential 시스템은 pseudonym 시스템이라고도 불리며, 1985년 Chaum[22]에 의해 제안되었다. 이 시스템은 기관과 사용자로 구성되며 기관은 사용자의 가명(pseudonym)만을 알고 그에 대한 credential을 발급할 뿐 사용자의 신원에 대해선 알 수 없다. 한 사용자가 여러 개의 가명을 사용할 수 있고, 반대로 한 기관이 사용자의 가명에 대해 발급한 credential을 다른 기관에 사용할 수 있다. 기관은 credential을 받은 사용자의 가명 이외의 어떠한 정보도 알 수 없으므로 사용자의 프라이버시를 보호한다. Anonymous credential 시스템은 최근에 와서야 실용적인 스킴이 제안되었다. Camenisch와 Lysyanskaya[23]은 최근 bilinear 사상을 이용한 효율적인 anonymous credential을 제안하였다. 유비쿼터스 환경에서 제공되는 많은 서비스에 대한 가입 시 발생되는 프라이버시 보호문제를 해결해 줄 것으로 기대된다.

5. Mix Network

익명성을 보호하는 여러 가지 방법이 있지만 실제 통신하는 네트워크 상에서 익명성을 유지하지 못한다면 아무 소용이 없다. Mix network는 1981년 Chaum[24]에 의해 고안되었으며, 네트워크에서 익명성을 유지하도록 해준다. Mix network는 암호화된 메시지를 입력 받아 재암호화한 후 랜덤한 순서로 출력하는 방식으로 입력 메시지와 출력 메시지 간의 대응관계를 알 수 없게 한다. 이것은 anonymous 이메일, 웹 브라우징, 익명화 지불 시스템 등에 응용된다. 현재 연구 동향은 ad-hoc, peer-to-peer 네트워크처럼 동적인 환경에서 익명성을 유지하는 효율적인 mix network를 개발하는 것과 mix network에 의해 얻게 되는 익명성의 정도를 수치화하려는 데 있다.

6. Threshold Cryptography

전통적인 암호학에서는 주로 송신자 한 명과 수신자 한 명이 있는 상황을 고려했지만 실제 상황은 다르다. 개인과 그룹 사이의 통신이 있을 수 있고 그룹과 그룹 사이의 통신이 있을 수 있다. 유비쿼터스 환경에서는 수많은 컴퓨팅 디바이스들이 잠시 동안 그룹을 이루었다가 흩어지는 일이 반복될 것이므로 전통적인 암호학으로는 접근할 수가 없다. 이런 상황에 대한 해결책으로 threshold cryptography가 유력하다. Threshold cryptography는 분산 암호(distributed cryptography)라고도 한다.

1979년 Shamir[25]가 최초로 마스터 비밀 키에 대한 비밀 공유 문제를 다루었다. 마스터 키를 한 사람에게 맡겨 놓는 것은 정보보호 차원에서 매우 위험하다. 왜냐하면 키가 유출되었을 경우나 키를 맡은 사람이 배신을 할 경우 대책이 없기 때문이다. 그러므로 키에 대한 정보를 모두에게 나누어서 위험을 줄이려는 것이다. n명의 구성원이 있다면 적어도 k명 이상이 모여야 키를 복구할 수 있고, k명 이하일 경우는 키에 대한 어떤 정보도 얻을 수 없는 (n, k)-threshold 스킴을 만든다. 대부분의 전통적인 암호 스킴은 threshold 형태로 바꿀 수 있으며 이에 대한 연구가 계속 진행중이다. 예를 들면 그룹 암호의 경우 그룹 관리자가 필요한데, 그룹 관리자 역할을 임

의의 k명 이상인 집단이 맡도록 하는 threshold 그룹 암호로 바꿀 수 있다. Threshold cryptography에 대한 안전성 분석은 현재 진행되고 있는 연구 과제이다.

프라이버시 보호를 위한 암호 프로토콜 분야에서 랜덤 오라클모델이 아닌 실용적인 모델에서의 안전성 증명 기법 개발, 계층 구조(hierarchical structure)를 갖는 기법 또는 멤버십을 대리할 수 있는 기법 개발, mix network에서 익명성의 정도를 측정하는 도구 개발 등이 앞으로 활발히 연구되어야 할 대표적인 분야이다[26].

Ⅳ. 결 론

유비쿼터스 환경이 제대로 갖추어지기 위해서는 보안 기술이 필수적인 요소이다. 본 고에서는 유비쿼터스 환경에 적용할 수 있는 최신 암호 기술을 분석하였다. RFID/USN 환경을 위한 암호 기술로 키 설정 기술 및 개발된 암호 프로토콜 기술과 현재까지 제시된 경량 암호 알고리듬에 대한 분석 및 문제점을 제시하였다. 실제로 이러한 암호기술들이 RFID/USN 환경에서 활용되기 위해서는 좀 더 효율적인 키 설정 프로토콜과 경량의 암호 알고리듬 및 인증 프로토콜에 대한 개발이 요구된다.

또한 본 고에서는 개인의 프라이버시 보호와 밀접한 익명성 보호에 관련된 암호 기술로 그룹 서명, ring 서명, 은닉 서명 등을 분석하였으며 최근 많은 관심을 받고 있는 분산 암호기술에 대한 연구 동향을 살펴보았다. 이러한 익명성 보호 프로토콜이 다양한 환경에 적용되기 위해서는 안전성과 효율성을 향상시키면서 법적인 분쟁이 있을 때를 대비한 추적성에 대한 연구가 함께 병행되어야 한다.

참 고 문 헌

[1] 김동석, "u-센서 네트워크 구축을 위한 정책 추진 방향," 전파 116호, 2004년 1월~2월호, 2004.

[2] A. Perrig et al., "SPINS: Security Protocols for Sensor Networks," Wireless Nets, Sep. 2002, pp.521-534.

[3] L. Eschenauer and V. Gligor, "A Key-management Scheme for Distributed Sensor Networks," *ACM CCS'02*, Nov. 2002, pp.41-47.

[4] A. Juels et al., "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," ACM CCS'03, pp.103-111.

[5] S. Weis et al., "Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems," *Security and Pervasive Computing 2003*, LNCS 2802, pp.201-212.

[6] P. Golle et al., "Universal Re-encryption for Mixnets," CT-RSA 2004, LNCS 2964, pp.163-178.

[7] A. Juels and R. Pappu, "Squealing Euros: Privacy Protection in RFID-enabled Banknotes," *Financial Cryptography 2003*, LNCS 2742, pp.103-121.

[8] A. Perrig et al., "Efficient Authentication and Signing of Multicast Streams Over Lossy Channels," *In Proc. Of IEEE Security and Privacy Symposium*, May 2000.

[9] M. Ohkobu et al., "Cryptographic Approach to Privacy-Friendly Tags," 2003, submitted

[10] M. Feldhofer et al., "Strong Authentication for RFID Systems Using the AES Algorithms," CHES 2004, LNCS 3156, pp.357-370.

[11] S. Weis, "Security and Privacy in Radio-frequency Identification Devices," MIT, May 2003.

[12] S. Wolfram, "Cryptography with Cellular Automata," CRTPTO'85, LNCS 218, pp.429-432.

[13] D. Chaum and Van Heyst, "Group Signature," EUROCRYPT'91, LNCS 547, pp.257-265.

[14] G. Ateniese et al., "Some Open Issues and Directions in Group Signatures," *Financial Cryptography'99*, LNCS 1648, pp.196-211.

[15] G. Ateniese et al., "Quasi-efficient Revocation of Group Signature," *Financial Cryptography 2002*, LNCS 2357, pp.183-197.

[16] D. Boneh et al., "Short Signature Scheme," CRYPTO 2004, LNCS 3152, pp.41-55.

[17] R. Rivest et al., "How to Leak a Secret," ASIACRYPT 2001, LNCS 2248, pp.552-565.

[18] E. Bresson et al., "Threshold Ring Signatures and Applications to Ad-hoc Groups," CRYPTO 2002, LNCS 2442, pp.465-480.

[19] D. Chaum, "Blind Signature for Untraceable Payments," CRYPTO'82, pp.199-203.

[20] S. Brands, "Untraceable Off-line Cash in Wallets with Observers," CRYPTO'93, LNCS 773, pp.302-318.

[21] M. Bellare et al., "The One-More_RSA-Inversion Problems and the Security of Chaum's Blind Signature Scheme," *Journal of Cryptology*, June 2003, pp.185-215.

[22] D. Chaum, "Security Without Identification: Transaction Systems to Make Big Brother Obsolete," *Commun. ACM*, 1985, pp.1030-1044.

[23] J. Camenisch and A. Lysyanskaya, "Signature Schemes and Anonymous Credentials from Bilinear Map," CRYPTO 2004, LNCS 3152, pp.56-72.

[24] D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," *Communications of the ACM*, 1981, pp.84-88.

[25] A. Shamir, "How to Share a Secret," *Commun. ACM, 22*, 1979, pp.612-613.

[26] STORK, Open Problems in Cryptology