한국산학기술학회논문지
Vol. 10, No. 8, pp. 1977-1985, 2009

e-Seal을 위한 다항식 해시 함수를 이용한 암호화기법 연구

연용호[1], 신문선[2*], 이종연[2], 황익수[3], 석창부[4]
[1]목원대학교 공학교육혁신센터
[2]충북대학교 컴퓨터교육과
[3]한국무역정보통신 전자무역사업본부
[4]코리아컴퓨터(주)

A Study on Encryption using Polynomial Hash Function for e-Seal

YongHo Yon[1], MoonSun Shin[2*], Jongyon Lee[2], Iksoo Hwang[3] and Changkboo Seok[4]
[1]**Engineering Education Innovation Center, MokWon University**
[2]**Dept. of Computer Education, ChungBuk National University**
[3]**eBiz Center, KTNET**
[4]**Korea Computer Corporation**

요 약 e-Seal은 RFID기술을 사용하여 원격에서 자동으로 봉인상태를 확인할 수 있는 컨테이너 봉인 장치를 말한다. RFID의 특징상 반도체 칩에 기록된 정보를 제 삼자가 쉽게 판독 및 변조할 수 있다는 취약점을 가지고 있다. 이러한 RFID 취약점을 해결한 e-Seal 인증 프로토콜을 적용하기 위해서는 e-Seal과 리더 간의 데이터를 암/복호화를 위한 PRF를 이용한다. 기존의 PRF에 사용되는 해시함수는 일방향 해시함수로써 e-Seal에 사용되기는 부적합하며 강력한 해시함수가 요구된다. 해시 함수는 데이터 무결성 및 메시지 인증, 암호화 등에서 사용할 수 있는 함수로써 정보보호의 여러 메커니즘에서 이용되는 핵심요소기술이다. 따라서 본 논문에서는 e-seal 인증 프로토콜을 위한 다항식을 기반으로 하는 강력한 해시함수를 제안한다.

Abstract An e-Seal is an active RFID device that was set on the door of a container. e-Seal provides both the state of the seal and the remote control of the device automatically. But it has vulnerabilities like eavesdrop and impersonate because of using RFID system. A secure e-Seal authentication protocol must use PRF for encryption/decryption of reader and e-Seal. The existing PRF uses simple hash function such as MD5 or SHA which is not available for e-Seal. It is required to use strong hash functions. The hash function is a essential technique used for data integrity, message authentication and encryption in the mechanism of information security. Therefore, in this paper, we propose more secure and effective hash function based on polynomial for e-Seal authentication protocol.

Key Words : e-Seal, Hash Function, Encryption, Authentication Protocol, Polynomial

1. 서론

RFID(Radio Frequency IDentification) 시스템은 RFID 태그, RFID 리더 , Back-end 서버로 이루어져서 짧은 거리의 무선통신을 통해 정보를 인식하는 시스템이다. 최근 RFID기술은 다양한 응용 분야에서 활용되고 있으며 보안과 프라이버시 침해에 대한 우려와 문제점을 해결해야 한다는 논의가 높아지고 있다. 태그의 인증과정에서 RFID 시스템은 다음과 같은 제한사항으로 인한 취약점을 가지고 있다.

첫째, 태그는 값싼 칩으로 한정된 기계적 성능을 가지고 있어 컴퓨팅 능력이 제약적이다.

본 논문은 2008년도 지식경제부 성장동력기술개발 사업의 일환으로 (주)코리아컴퓨터의 위탁과제로 수행되었음.
*교신저자 : 신문선(msshin9@nate.com)
접수일 09년 07월 24일 수정일 09년 08월 11일 게재확정일 09년 08월 19일

둘째, RFID 시스템은 무선 주파수를 사용함으로써 쉽게 도청될 수 있어 중간자 공격및 위조 공격들에 쉽게 노출된다.

셋째, 수동형 태그의 경우 상호인증을 제공하는데 어려움이 따른다. 따라서 태그와 리더 간 상호 인증을 위한 다양한 프로토콜이 연구되고 있다.

전자봉인(e-Seal: Electronic Seal)은 RFID기술을 사용하여 원격에서 자동으로 봉인상태를 확인할 수 있는 컨테이너 봉인 장치를 말한다.

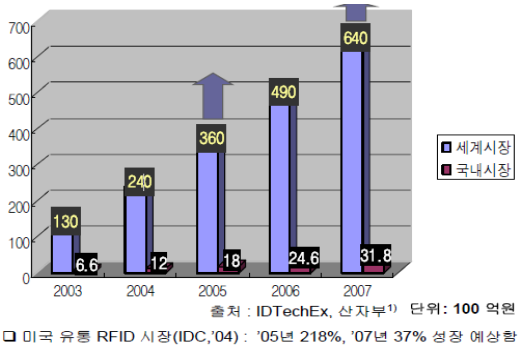
컨테이너가 운송에 사용된 이후 지속적으로 사용되어 온 봉인은 IT기술의 발달과 증가하는 물류보안 요구에 따라 전자봉인으로 발전하고 있다. e-Sea이라 불리는 전자봉인은 능동형 RFID기술을 응용하는 대표적인 사례로 꼽히고 있으며 국제표준화기구(ISO)를 중심으로 2003년부터 사용에 대한 논의가 시작되어 2007년에 국제표준이 확정되었다. 즉 전자봉인은 기존의 금속봉인이 제공하던 컨테이너의 개폐유무뿐 아니라 데이터 정보처리 등의 추가적인 서비스를 제공하는 수단으로 활용되게 되었다.

RFID의 특징상 반도체 칩에 기록된 정보를 제 삼자가 쉽게 판독 및 변조할 수 있다는 취약점을 가지고 있다. 이러한 RFID 취약점을 해결한 e-Seal 보안 프로토콜을 적용하기 위해서는 e-Seal과 리더 간의 데이터를 암/복호화할 키가 필요하지만, 키 서버를 통해 전달받은 마스터 키를 데이터 암/복호화 키로 바로 사용하는 것은 보안상의 문제점을 야기할 수 있기 때문에 PRF(Pseudo Random Function)을 이용하여 마스터 키로부터 MTK(Mutual Transient Key)를 유도하고, MTK를 암/복호화 키로 사용해야 한다. 기존의 PRF는 일방향 해시 함수(MD5, SHA 등)를 기반으로 하는 HMAC[13]을 일반적으로 사용하였다. 그러나 일방향 해시 함수는 e-Seal과 같은 제한된 자원을 갖는 환경에 적합하지 않다. 따라서, 본 논문에서는 e-Seal 보안 프로토콜을 위한 강력한 해시함수를 제안한다. 제안된 해시함수는 기존의 일방향 해시 함수 기반이 아닌 블록 암호화 알고리즘을 기반으로 하며 다항식의 소인수분해의 난해성을 이용한 다항식 해시함수이다.

논문의 구성은 다음과 같다. 2장에서는 관련연구로서 RFID시스템과 e-Seal의 보안 취약성에 대해서 분석하고 해시 알고리즘에 관해 기술한다. 3장에서는 e-Seal 보안 프로토콜과 PRF 에 사용되는 해시함수의 설계에 대해서 기술한다. 4장에서 수학적 검증 과정과 적용 가능한 응용예를 기술하고 마지막으로 결론을 맺는다.

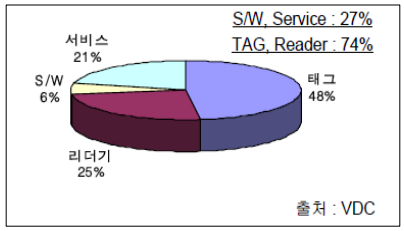
2. 관련 연구

2.1 RFID 시스템 환경



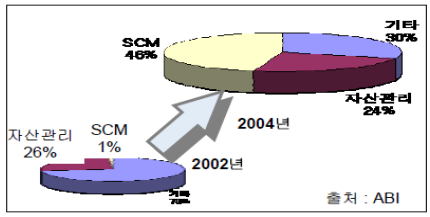
[그림 1] 국내외 RFID 시장 성장율 예측

RFID 시장은 그림 1에서 보여지는 것처럼 국내외시장에서 매년20~30% 이상의 성장을 할 것으로 예측이 되어지고 있으며 특히 물류, 유통 서비스 분야에서 많은 비용효과를 낼 것으로 전망된다. 또한 그림 2의 도표에서 보여지는 것과 같이 RFID 시장은 리더 태그 산업쪽이 74%를 차지할 것으로 예상되어 RFID 산업 활성화를 위해서는 보안과 개인 프라이버시 문제를 우선적으로 해결해야 될 것으로 보인다.



[그림 2] RFID 산업 시장 구성

특히 SCM 이나 고가의 자산관리 등의 분야에서 효율적으로 적용이 될 수 있을 것이라는 조사가 그림 3에서의 결과이다



[그림 3] RFID 적용 분야의 확대

RFID 시스템 환경은 무선통신이라는 환경적 제약 사

항으로 인해 다양한 보안 위협이 존재한다[1]. RFID 시스템에서의 가능한 공격 모델들을 살펴보면 다음과 같다.

MITM공격(Man In The Middle Attack) :공격자는 정당한 리더로 흉내 내어서 태그의 정보를 얻거나, 공격자는 정당한 태그로 흉내내서 리더에게 응답 후 다음 세션에 정당한 리더에 의해서 공격자는 쉽게 인증을 받음.

Replay attack : 공격자는 T로 부터의 공격 메시지를 도청하거나 정당한 리더에게 메시지를 계속해서 전송하는 공격

Forgery :도청에 의한 태그의 정보를 위한 단순한 복사는 적에 의해 가능

Data loss: Dos, Power interruption, hijacking은 스니핑이나 무작위 추측 공격을 도용하여 데이터 손실을 가져오는 공격

따라서 이러한 공격 모델에 안전한 RFID 태그 리더간 상호 인증이 요구되어 이와 관련된 많은 연구가 이루어지고 있다[2].

제시된 공격 모델에 대응하기 위해서 RFID 리더 태그간 상호 인증 프로토콜에서 필요로 하는 보안 요구사항은 다음과 같다[3-5].

데이터 기밀성(Data Confidentiality) : 태그의 응답이 공격자에겐 무의미해야 함.

태그 익명성(Tag Anonymity) : 그의 ID를 공격자가 알 수 없어야 함. 사용자의 소지품 정보 노출 방지

데이터 무결성(Data Integrity) :수신된 데이터가 정확히 권한 있는 실체가 송신한 것임을 확신. 수정, 삽입, 삭제, 재전송이 없음

태그 비추적성(Tag Untracebility) : 태그를 추적할 수 없어야 함.

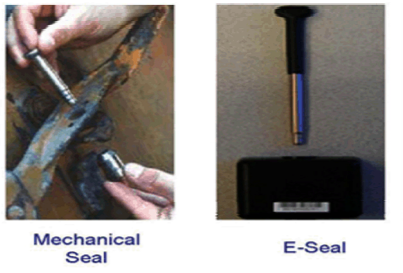
따라서 위의 보안 요구사항을 만족하면서 공격자에게 공격이 쉽지 않은 강력한 복잡도를 가지는 해시함수를 활용한 보안메커니즘의 구현은 위의 보안 요구사항을 만족시킬 수 있다.

2.2 e-Seal 개요

전자봉인은 RFID기술을 사용하여 원격에서 자동으로 봉인상태를 확인할 수 있는 컨테이너 봉인 장치이다. 컨테이너가 운송에 사용된 이후 지속적으로 사용되어온 봉인은 IT기술의 발달과 증가하는 물류보안 요구에 따라 전자봉인으로 발전하고 있다.

e-Seal의 국제 표준화는 ISO산하 TC104에서 주도되고 있으며, RFID 공급망 관리분야의 표준화는 TC104 및 TC122의 JWG(Joint Working Group)에서 진행되고 있다. e-Seal에 대한 쟁점은 범죄에 대비한 데이터 보호 분야이며 이에 대한 검토 및 연구가 진행되고 있다[7-9].

즉 전자봉인은 RFID를 기반으로 만들어진 것이 일반적이며, 컨테이너의 문이 비정상적인 형태로 개폐됨을 감지하거나 또는 비정상적인 개폐의 시도를 감지하여 주변의 리더기에게 알리고 그 이력을 유지하는 역할을 한다. 송하주가 전자봉인을 한 이후 해당정보를 통신망을 이용해 수하주에게 보내고 수화주는 그 정보를 이용하여 도착지에서 화물의 안전 여부를 확인하게 된다. 그림 4는 e-Seal 의 예를 보여주는 것이다.



[그림 4] 기계적 seal 과 e-seal

전자적인 수단을 이용한 Seal의 검증은 기존의 수동 방식의 Seal 검증과 동등하거나 그 이상의 성능을 지녀야 한다. 따라서 e-Seal은 다음과 같은 일반적인 특성을 가져야 한다.

고유번호와 제조사 코드에 의해 구분이 가능하여야 한다.

물리적 Seal의 상태 변화 시 이를 실시간으로 기록할 수 있어야 한다.

상태변화 기록이 수정되거나 이전 상태로 변경될 수 없어야 한다.

e-Seal을 복제(cloning)하거나 위작(spoofing)이 어렵도록 제작되어야 한다.

e-Seal의 기능이 강화 되는 것과 맞물려 그 방식이 능동형으로 기울어지게 되었다. 따라서, e-Seal의 사용 주파수 대역도 방식과 많은 상관 관계를 가지므로, Savi가 제안한 433 MHZ 대역이 선정되게 되었다. 최근에는 능동형 RFID 태그를 이용하는 e-Seal 이 일반적이다.

Seal의 등장은 초기 단순 절도범죄 예방 및 그 결과에 대한 책임소재 확인 등의 목적이었으나, 점차적으로 컨테이너를 이용한 적극적이고도 극단적인 범죄 도발행위의 가능성이 증가함에 따라서 Seal에 대한 보안 또는 안전장치를 더욱 요구하게 되었다.

보안관련 이슈들은 ISO 18185 표준 제정 초기부터 계속적으로 관심을 갖고 제기 되어 왔으며, 주로 e-Seal과

리더간의 통신 프로토콜에 대한 보안이 주 쟁점 사항이었다. 보안 규격은 e-Seal의 표준이 정해지기도 전에 구체적으로 규정하기는 어려워 2003년 1월에 다음의 기본적인 원칙만 설정하였다.

데이터 보안(Data Security)
-허가 받은(authorized) 사용자만이 Seal의 사실적인 데이터를 볼 수 있어야 한다.
-배송자는 허가 받은 사용자에게 복호 알고리즘 및 Key를 동시에 제공하여야 한다.
-이 외의 사용자가 이 데이터를 볼 경우 원시 데이터만 볼 수 있도록 한다.

데이터 무결성(Data Integrity)
-데이터를 복호하여 허가를 득한 사용자가 데이터를 확인하기도 전 타인에 의해 미리 수정되었는지를 검증할 수 있어야 한다.
-추후, 허가를 득한 사용자가 데이터의 잠금(lock) 및 해제(unlock) 기능을 추가할 수도 있다.

데이터 유효성(Data validity)
-데이터를 암호화 하여 Seal의 데이터가 허가 받지 않은 자에 의해 무단으로 다른 Seal에 복제되어 불법으로 사용되지 않도록 하여야 한다.

이와 관련, 2004년 12월 중국 베이징에서 개최된 TC 104/SC 4/WG 2 회의에서 “vulnerability and threats for e-Seal” 규격 제안을 위해 평가 태스크 포스팀이 결성되었으며 리더와 태그(e-Seal)간의 무선 인터페이스 영역에 대하여 작업이 진행 중이다.

악의적 조직의 가능한 위협(threats)으로는 (1) e-Seal 및 태그의 복제(cloning), (2) e-Seal 및 태그의 위작(spoofing), (3) e-Seal 및 태그의 정보를 획득할 수 있는 불법 리더 사용, (4) 전파교란(Jamming), (5) 전송차단(Shielding) 등 5가지로 정의하고 있다.

또한, 취약성(vulnerability 분야는 다음과 같이 11가지를 정의하고 있다.

Imposter/Substitution(Cloned Seal)
Imposter/Substitution Reader(Cloned Reader)
Spoof message between the Seal and Reader(Rogue Seal)
Spoof message between the Seal and Reader(Rogue Reader)
Communication disruption: Jamming(Denial of Service – DOD Attack)
Communication disruption: Shielding(Denial of Service – DOD Attack)
Seal disruption – increased power utilization
Passive information gathering
Seal probing(Physical information extraction)
Seal destruction
Man-in-the-middle air interface attack (Intercept and Alter)

2.3 해시 알고리즘 개요

e-Seal 보안 프로토콜[14]을 적용하기 위해서는 e-Seal과 리더 간의 데이터를 암호화/복호화할 키가 필요하다. 하지만 생성된 키를 바로 사용하게 되면 보안상의 문제점이 노출된다. 따라서 Pseudo Random Function을 이용하여 원래의 키를 감추고 이 키로 암호화/복호화를 해야 한다.

기존의 PRF는 MD5 나 SHA 와 같은 일방향 해시함수를 기반으로 하는 HMAC(Keyed-Hash Message Authentiction Code)를 일반적으로 사용한다.

그러나 일방향 해시함수는 하드웨어로 구현하였을 때 많은 면적을 차지하고 처리효율성이 떨어진다는 단점이 있다[13]. 따라서 본 논문에서는 e-Seal 인증 프로토콜을 위한 해시함수를 다항식의 곱집합 연산에 기반하여 설계한다. e-Seal과 같은 강력한 인증을 요구하는 능동형 태그의 응용에는 강력한 암호화와 인증이 필요하다.

제안하는 다항식 해시함수는 역원이 존재하는 경우와 존재하지 않는 경우 모두에 대해서 해시함수의 정의가 가능하다. MD5보다 좀 더 복잡성을 가지는 해시함수로 강력한 인증에 활용될 수 있을 것이다.

3. 다항식 해시 함수의 설계

인증 암호기법은 크게 메시지복구 기법과 키 분산 기법으로 분류된다. 인증 암호 문제는 크게 네 가지로 구분되는데 첫째, 인수분해의 난해성 문제, 둘째, 이산대수 문제, 셋째, 타원 곡선 문제 넷째, 인수분해와 이산대수 문제의 복합 문제로 나누어진다.

따라서 이산대수, 인수분해, 타원곡선 등의 이산 수학의 어려운 해법에 기반을 둔 인증 암호기법에 관한 연구[7,8]가 수행되었으며, [9]에서는 공개키를 이용한 인증암호기법에 관한 연구가 수행되었다.

다항식의 곱집합연산 기반의 해시함수는 인수분해의 어려운 해법에 기반을 인증 암호의 범주에 속한다.

Tillich와 Zémor[2]는 유한체(finite field) F_{2^n} 상의

2×2 행렬 군(group) SL_2 에서 정의된 해시함수를 소개하였다. [6]에서 결합법칙의 성립과 역원의 존재성으로부터 발생되는 Tillich-Zémor 해시함수의 취약성에 대하여 제안하고[2] 이의 해결방법으로 결합법칙과 교환법칙이 성립하지 않으며 역원이 존재하지 않는 다항식을 이용한 해시함수를 설계하였다.

본 절에서 SL_2 보다 성분의 수가 적어 메모리의 사용이 적고 연산의 횟수가 적은 곱집합(Cartesian Product) $K\times F$ 을 이용하여 해시함수를 설계하는 방법에 대하여 다룬다. 먼저 곱집합에서의 이항연산(binary operation)을 정의하고 이 이항연산으로 정의된 곱집합의 구조가 결합법칙과 교환법칙이 성립하고 역원을 갖기 위한 필요충분조건을 알아본다. 이를 이용하면 경우에 따라 결합법칙과 교환법칙은 성립하지 않으나 역원을 갖는 수학적 구조로 복호화가 가능한 해시함수의 설계도 가능할 것이다.

체(field) K 와 F 에 대하여 다음의 성질을 만족하는 함수 $\alpha : K\times F \to F$ 를 오른쪽 가법함수(right additive map)라 한다.

$\alpha(a,\ u+v)=\alpha(a,\ u)+\alpha(a,\ v)$

[정의] 체 K 와 F 의 곱집합 $K\times F$ 에서 F 로의 주어진 두 함수 α 와 β 에 대하여 $K\times F$ 에서의 이항연산 $\circ$ 을 다음과 같이 정의하면 $(K\times F,\ \circ)$ 는 준군(groupoid)를 형성한다.

$(a,u)\circ(b,v)=(ab,\ \alpha(a,v)+\beta(b,u))$,
$a,\ b\in K,\ u,\ v\in F$

위에서 정의된 준군은 함수
$\alpha,\ \beta : K\times F \to F$ 에 따라 그 구조가 달라진다.

[정리1] 함수 $\alpha,\ \beta : K\times F \to F$ 가 오른쪽 가법함수라 할 때, 이항연산 $\circ$ 가 결합법칙이 성립하기위한 필요충분조건은 α 와 β 가 다음의 세 가지 성질을 만족하는 것이다.

(A1) $\alpha(a,\ \alpha(b,u))=\alpha(ab,\ u)$,
(A2) $\beta(a,\ \beta(b,u))=\beta(ba,\ u)$,
(A3) $\alpha(a,\ \beta(b,u))=\beta(b,\ \alpha(a,u))$

위의 정리에 따라 α 와 β 가 성질 A1~A3를 모두 만족하면 $(K\times F,\ \circ)$ 는 반군(semigroup)이 된다.

[정리2] 이항연산 $\circ$ 가 교환법칙이 성립하기 위한 필요충분조건은 $\alpha=\beta$ 이다.

위의 정리에 따라 $\alpha=\beta$ 이면 $(K\times F,\ \circ)$ 는 가준군(commutative groupoid)이 된다.

[정리3] 함수 α 와 β 가 정리1의 성질 A1~A3를 모두 만족할 때, $(K\times F,\ \circ)$ 가 항등원 $(1,0)$ 를 갖기 위한 필요충분조건은 α 와 β 가 모두 전사함수인 것이다.

[정리4] 함수 α 와 β 가 모두 정사함수이고 정리1의 성질 A1~A3를 모두 만족하면 $a\neq 0$ 인 모든 원소 $(a,u)\in K\times F$ 는 역원 $(a,u)^{-1}$ 을 갖는다.

위에서 정의된 다항식 해시 함수인
$h:(K\times F,\ \circ)$ 의 적용및 해시코드 생성과정은 다음 장에서 예를 들어 기술한다.

4. 적용

4.1 다항식 해시함수의 해시코드 생성 예

3장에서 정의된 정리를 이용하여 다음의 예제와 같은 준군들을 만들 수 있다.

[예제1] 두 함수 $\alpha,\ \beta : K\times F \to F$ 를 $\alpha(a,u)=au,\ \beta(a,u)=au+u$ $(a\in K,\ u\in F)$ 로 정의하면 α 와 β 는 오른쪽 가법함수이고 정리 1의 A3를 만족한다. 또한 α 는 정리1의 A1을 만족하지만 β 는 A2를 만족하지 못한다. 따라서 이 두 함수에 의해 정의된 연산 $\circ$ 은 정리1에 의해 결합법칙이 성립하지 않으며 $\alpha\neq\beta$ 이므로 정리2에 의해 교환법칙도 성립하지 않는다. 실제로 K 와 F 가 모두 실수의 집합 $\mathbb{R}$ 이라 할 때

$(1,1)\circ(1,2)=(1,\ 2+1+1)=(1,\ 4)$,
$(1,2)\circ(1,1)=(1,1+2+2)=(1,5)$
이므로 $(1,1)\circ(1,2)\neq(1,2)\circ(1,1)$이고,
$((1,2)\circ(1,1))\circ(1,2)$
$=(1,5)\circ(1,2)=(1,2+5+5)=(1,12)$,
$(1,2)\circ((1,1)\circ(1,2))$
$=(1,2)\circ(1,4)=(1,4+2+2)=(1,8)$
이므로

$((1,2)\circ(1,1))\circ(1,2)\neq(1,2)\circ((1,1)\circ(1,2))$
이다. 그러나 왼쪽 항등원 $(1,0)$ 과 모든 $a\neq 0$ 인 원

소 (a,u) 에 대하여 오른쪽 역원이 존재한다. 즉,

$$(a,u)^{-1}=(a^{-1},-a^{-1}(a^{-1}u+u)),$$
$$(1,0)\circ(a,u)=(1a,\alpha(1,u)+\beta(a,0))$$
$$=(a,1u+a0+0)=(a,u),$$
$$(a,u)\circ(a^{-1},-a^{-1}(a^{-1}u+u))$$
$$=(aa^{-1},-aa^{-1}(a^{-1}u+u)+a^{-1}u+u)$$
$$=(1,0).$$

[예제2] 두 함수 $\alpha,\beta: K\times F\to F$ 를 $\alpha(a,u)=au$, $\beta(a,u)=u$ $(a\in K, u\in F)$로 정의하면 α 와 β 는 오른쪽 가법함수이고, 정리1의 A1~A3를 모두 만족하며 모두 전사함수로 $\circ$ 는 결합법칙을 만족하고 항등원 $(1,0)$ 을 갖고 $a\neq 0$ 인 모든 원소 $(a,u)\in K\times F$ 의 역원 $(a,u)^{-1}$ 가 존재한다.

[예제3] 두 함수 $\alpha,\beta: K\times F\to F(K\subseteq F)$ 를 $\alpha(a,u)=au$, $\beta(a,u)=a$ $(a\in K, u\in F)$로 정의하면 β 가 오른쪽 가법함수도 아니고 정리1의 A2도 만족하지 않으므로 결합법칙이 성립하지 않고 항등원과 역원이 존재하지 않는다.

예제3에서 설계한 이항연산은 결합법칙과 교환법칙도 성립하지 않으며 역원이 존재하지 않는 예로 [6]에서 제안한 해시함수와 같은 성질을 갖지만 그 연산의 횟수가 [6]의 해시함수보다 적다.

예제3에서 설계한 이항연산을 이용하여 인증을 위한 해시함수를 만드는 과정은 다음과 같다. 이는 블록을 이용한 해시함수이고 [6]과 [2]와 같은 방법으로 해시코드를 생성한다.

주어진 평문의 비트스트링을 $b_1b_2\cdots b_n$ 이라 하고 이의 해시 코드를 생성한다. 위에서 다룬 연산에 사용된 두 체를 $K=\boldsymbol{F}_{2^k}$, $F=\boldsymbol{F}_{2^l}$ $(k\le l)$이라 하고, 적당한 $a,b\in\boldsymbol{F}_{2^k}$와 $u,v\in\boldsymbol{F}_{2^l}$ 에 대하여 함수 $\pi:\{0,1\}\to\boldsymbol{F}_{2^k}\times\boldsymbol{F}_{2^l}$ 를 다음과 같이 정의한다.

$$\pi(0)=(a,u),\ \pi(1)=(b,v)$$

비트스트링 $b_1b_2\cdots b_n$ 을 일정한 길이 t $(t<n)$의 블록으로 다음과 같이 나눈다. 이때, 마지막 블록에 비트가 부족한 경우 0으로 채운다.

$$B_1=b_{11}\cdots b_{1t},\ \cdots,\ B_m=b_{m1}\cdots b_{mt}$$

두 함수 $\alpha,\beta:\boldsymbol{F}_{2^k}\times\boldsymbol{F}_{2^l}\to\boldsymbol{F}_{2^l}$ 를 각각 다음과 같이 정의하자.

$$\alpha(f,g)=fg\ ,\ \beta(f,g)=f\ (\mathrm{mod}\ q(x))$$

α , β 를 이용하여 만든 연산 $\circ$ 을 이용하여 다음과 같이 블록의 해시코드를 생성한다.

$$H(B_i)=(\cdots(((\pi(b_{i1})\circ\pi(b_{i2}))\circ\pi(b_{i3}))\cdots)\circ\pi(b)$$
$$\in\boldsymbol{F}_{2^k}\times\boldsymbol{F}_{2^l}$$

각각의 블록 해시 코드를 같은 연산을 사용하여 다음과 같이 해시코드를 생성한다.

$$H(b_1b_2\cdots b_n)=(\cdots((H(B_1)\circ H(B_2))\circ H(B_3))\cdots)\circ H(B_m)$$

다음의 예에서 위의 해시코드 생성방법을 이용하여 비트스트링 10111의 해시코드를 생성하였다.

[예제4] 비트 스트링 10111의 해시코드 생성

체 $\boldsymbol{F}_2=\{0,1\}$ 에서의 다항식 환 $\boldsymbol{F}_2[x]$ 에서의 기약다항식

$$p(x)=x^2+x+1,\quad q(x)=x^3+x+1$$

에 대한 유한체 $K=\boldsymbol{F}_{2^2}=\boldsymbol{F}_2[x]/(p(x))$, $F=\boldsymbol{F}_{2^3}=\boldsymbol{F}_2[x]/(q(x))$ 에 대하여 함수 π 를 다음과 같이 정의하자.

$$\pi(0)=(10,\,011),\ \pi(1)=(11,\,010)$$

주어진 비트 스트링 10111을 길이 3인 두 개의 블록 $B_1=101$, $B_2=110$으로 나누고 이들을 해시화하면 다음과 같다. 여기에서 K와 F의 원소의 곱은 $K\subseteq F$로 보고 mod $q(x)$의 연산을 시행하였다.

$$H(B_1)=(\pi(1)\circ\pi(0))\circ\pi(1)$$
$$=((11,\,010)\circ(10,\,011))\circ(11,\,010)$$
$$=(01,\,111)\circ(11,\,010)$$
$$=(11{,}001)=11001$$
$$H(B_2)=(\pi(1)\circ\pi(1))\circ\pi(0)$$
$$=((11,\,010)\circ(11,\,010))\circ(10,\,011)$$
$$=(10,\,101)\circ(10,\,011)$$
$$=(11{,}100)=11100$$
$$H(10111)=H(B_1)\circ H(B_2)$$
$$=(11\,,001)\circ(11,\,100)$$
$$=(10,\,100)=10100$$

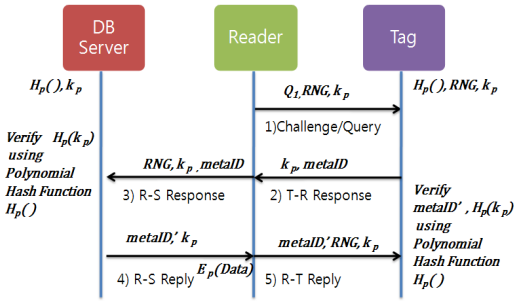
위의 예에서 설계한 해시함수의 실제응용에서의 안전전성을 높이기위해서는 기약다항식의 차수를 고려할 필요가 있다.

4.2 다항식 해시함수를 적용한 RFID인증 프로토콜

이 절에서는 본 논문에서 제안한 다항식 해시 함수의 적용 예를 통해 그 유용성을 검증한다.

일반적인 RFID 인증 프로토콜에서 PRF 가 사용된 다항식 해시함수는 인증의 복잡도를 증가시킴으로써 강력한 암호화와 인증을 제공해줄 수 있다.

본 논문에서 제안하는 다항식 해시함수를 이용한 RFID 인증 프로토콜은 다음 그림 5와 같다.



[그림 9] 다항식 해시함수를 이용한 RFID 인증 프로토콜

먼저 초기화 단계에서는 다항식 해시함수를 이용한 키 값을 생성한다.

백엔드 디비 서버는 생성된 키값을 저장한다. 리더가 쿼리를 보내면 상호 인증을 위한 과정은 5단계로 수행된다.

1) Challenge

리더 태그구간의 안전성을 확보하기 위해 리더는 RNG(Random Number Generator) 값과 키 값 kp 를 쿼리와 함께 태그에 보낸다.

2) T-R Response

쿼리를 받은 태그는 익명성 보장을 위해 metaID와 키값 kp 를 보내 리더에 응답한다.

3) R-S Response

리더는 태그로부터 받은 metaID와 키값 kp 를 백엔드 디비 서버에 보낸다.

4) R-S Reply

백엔드 디비 서버는 키 테이블에서 리더로부터 받은 metaID와 키값 kp를 확인한 후 인증된 태그이면 metaID ‘과 키값 kp를 리더에 보낸다.

5) R-T Reply

리더는 디비서버로부터 받은 metaID‘과 키값 kp를 태그에 보내 인증된 리더임을 태그에 알린다.

본 논문에서 제안한 다항식 해시함수를 적용한 RFID 인증 프로토콜의 장점은 해시함수 기반의 키 생성에 초점을 맞추어 복잡도가 높다는 것이다. 이는 공격에 쉽게 노출되지 않는 강력한 인증 프로토콜임을 의미한다.

5. 결론

RFID 시스템은 환경적 제약으로 인해 다양한 공격모델에 취약하다. 특히 중간자 공격이나 재생 공격과 같은 공격에 강력하게 대응하여 데이터 기밀성과 데이터 무결성, 태그 익명성 등의 보안 요구사항을 충족하여야 한다. 본 논문에서는 e-Seal 의 보안 프로토콜을 위한 다항식 기반의 해시함수를 설계하였다. 제안된 해시함수는 기존의 일방향 해시 함수 기반이 아닌 블록 암호화 알고리즘을 기반으로 하며 다항식의 소인수분해의 난해성을 이용한 다항식 해시함수로서 강력한 암호화와 인증을 제공한다. 암호화와 복호화가 필요한 e-Seal 에서는 역원과 항등원이 존재하는 다항식 해시함수로 활용할 수 있으며 복호화가 필요하지 않고 인증만이 필요한 경우에는 RFID 역원이 존재하지 않는 해시 함수로 사용하는 것도 가능하다. 향후 논문에서 제안한 해시 함수를 PRF에 적용하여 일방향 해시 함수와의 성능 비교 연구를 수행할 계획이며 e-Seal 인증 프로토콜에 실제 적용하고 검증하는 과제가 남아 있다.

참고문헌

[1] Istv Vajda and Levente Butty. Lightweight authentication protocols for low-cost rd tags. Workshop on Security in Ubiquitous Computing, October, 2003.

[2] J.-P. Tillich and G. Zémor, *Hashing with* SL_2, in CRYPTO 1994, Lecture Notes Comp. Sc. 839, 1994.

[3] Gene Tsudik. Ya-trap: Yet another trivial rd authentication protocol. International Conference on Pervasive Computing and Communications, PerCom, 2006.

[4] Jeongkyu Yang and Kui Ren and Kwangio Kim. Security and Privacy on Authentication Protocol for Low-cost RFID. Symposium on Cryptography and Information Security, January, 2005.

[5] D. Henrici and P. Muller. Hashed-based Enhancement of Location Privacy for Radio-Frequency Identication Devices using Varying Identiers. . PerSec '04, March 2004.

[6] V. Shpilrain, Hashing with Polynomials, The City College of NewYork, 2006.
[7] C.Ma and K. Cheng, "Publicly verifiable authenticated encryption," IEEE Electronics Letters, Vol.39, No.3, 2003.
[8] Heiko Knospe and Hartmut Pohl, RFID security, Information Security Technical Report, Volume 9, Issue 4, pp39-50, December, 2004.
[9] Hung-Yu Chien and Che-Hao Chen, Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards, Computer Standards & Interfaces, 2006.
[10] Iris F.A. Vis and Rene de Koster, Transshipment of containers at a container terminal: An overview, European Journal of Operational Research, 147, 2003.
[11] Kampers, F. W. H., W. Rossing and W. J. Eradus, The ISO standard for radiofrequency identification of animals, Computers and Electronics in Agriculture, Volume 24, Issues 1-2, pp27-43, November, 1999.
[12] Ngaia, E.W.T., T.C.E. Chengb, S. Au , and Kee-hung Laib, Mobile commerce integrated with RFID technology in a container depot, Decision Support Systems 2005.
[13] 민정기, 강석훈,정상화, 김동규, “e-Seal 보안프토콜을 위한 효율적인 Pseudo Random Function", 한국 컴퓨터 종합 학술 대회, 2006.
[14] ETRI, "Report of ePP(eSeal Protection Protocol) for ISO 18185-4", October 2005.
[15] 박성수,이문규, 김동규, 김근수, 김호원, 정교일, “안전한 전자봉인을 위한 인증 프로토콜의 설계”,한국 정보과학회 추계 학술 발표 대회논문집, 2005.
[16] NIST FIPS PUB 198," The Keyed Hash Message Authentication Code(HMAC),MARCH 2002.

연 용 호(Yong-Ho Yon) **[정회원]**

- 1997년 8 월 : 충북대학교대학원 수학과(이학박사)
- 2007년 3월 ~ 현재 : 목원대학교 공학교육혁신센터 전임강사

<관심분야>
암호화 알고리즘,

신 문 선(Moon-Sun Shin) **[정회원]**

- 2004년 8월 : 충북대학교대학원 전자계산학과(이학박사)
- 2005년 8월 ~ 2008년 8월 : 건국대학교 컴퓨터시스템 강의교수
- 2008년 10월 ~ 현재 : 표준과학연구원 연구원. 건국대학교 겸임교수

<관심분야>
데이터베이스, 정보보안, USN, RFID 보안

이 종 연(Jong-Yon Lee) **[정회원]**

- 1999년 2월 : 충북대학교 대학원 전자계산전공(이학박사)
- 1994년 3월 ~ 1996년 2월 : 현대정보기술(주) CIM사업부 책임연구원
- 1999년 3월 ~ 2003년 2월 : 삼척대학교 정보통신공학과 조교수
- 2003년 3월 ~ 현재 : 충북대학교 컴퓨터교육과 부교수

<관심분야>
데이터베이스 질의 최적화, 시공간데이터베이스, 유비쿼터스 컴퓨팅, e-러닝, RFID 보안

황 익 수(Ik-Soo Hwang) **[정회원]**

- 1984년 2월 : 세종대학교 졸업 (경영학사)
- 1993년 2월 : 한국외국어대학교 무역대학원수료
- 1990년 3월 ~ 현재 : 한국무역정보통신 근무
- 2008년 1월 ~ 현재 : 전자무역본부 본부장 역임

<관심분야>
정보관리, EPCGlobal network, RFID기반 국제물류 시스템

석 창 부(Chang-Boo Seok) **[정회원]**

- 1987년 2월 : 동아대학교 졸업 (경영학사)
- 1990년 1월 ~ 2000년 8월 : 흥아해운 전산팀장
- 2000년 9월 ~ 현재 : (주) 코리아컴퓨터 상무이사

<관심분야>
RFID/USN미들웨어, EPCglobal Network, RFID보안, Real Time Location System