http://dx.doi.org/10.3745/KIPSTC.2012.19C.1.039

칩셋 페어링 접근제한시스템 환경에서 다중 셋톱박스를 지원하는 키 분배 기법

이 훈 정[†] · 손 정 갑[†] · 오 희 국[††]

요 약

본 논문에서는 유연한 칩셋 페어링 접근제한시스템을 위한 새로운 키 분배 기법을 제안하였다. 칩셋 페어링 접근제한시스템은 셋톱박스에 내장된 보안 칩과 스마트카드를 함께 사용해 CA(Conditional Access) 모듈을 구현한 것으로, 셋톱박스에 내장된 보안 칩은 스마트카드와 셋톱박스 사이에 보안 채널을 형성한다. 즉, 스마트카드는 암호화된 제어단어를 셋톱박스로 출력하고, 셋톱박스는 내장된 보안 칩을 이용해 암호화된 제어단어를 복호화하는 시스템이다. 이 방식은 셋톱박스와 스마트카드를 바인딩 하는 방식으로 하나의 스마트카드는 정해진 하나의 셋톱박스에서만 사용이 가능하다는 단점을 가진다. 제안하는 키 분배 기법은 중국인의 나머지 정리를 이용하여 기존의 칩셋 페어링 접근제한시스템이 가지는 문제를 해결하였다. 우리의 키 분배 기법은 하나의 스마트카드를 다수의 셋톱박스에서 사용하는 것이 가능하며, 큰 변경 없이 현재의 칩셋 페어링 접근제한시스템에 적용이 가능하다는 장점을 가진다.

키워드 : 키 분배 기법, 그룹키, IPTV, 접근제한시스템

Key Distribution Scheme for Supporting Multiple Set-Top Box in Chipset Pairing Conditional Access System

Hoonjung Lee[†] · Junggab Son[†] · Heekuck Oh[††]

ABSTRACT

In this paper, we propose a key distribution scheme for flexible chipset pairing conditional access system. Chipset pairing conditional access system is the implementation of CA (Conditional Access) module by using both embedded secure chip in a Set-Top Box(STB) and smartcard, and the secure chip embedded in a STB forms a secure channel between the smartcard and the STB. In short, it is the system that a smartcard outputs encrypted CW (Control Word) to the STB, and the STB decrypts an encrypted CW by using the embedded secure chip. The drawback of this chipset pairing conditional access system is that one smartcard is able to be used for only one specified STB since it is the system using the STB bound to a smartcard. However, the key distribution scheme proposed in this paper overcomes a drawback of current chipset pairing conditional access system by using Chinese Remainder Theorem(CRT). To be specific, with this scheme, one smartcard can be used for multiple, not single, STBs, and applied to current chipset pairing without great changes.

Keywords : Key Distribution Scheme, Grouip Key, IPTV, Conditional Access System

1. 서 론

접근제한시스템(Conditional Access System, CAS)은 사용자의 조건에 따라 접근을 제한하는 시스템으로 유료 TV 시스템에서 인가된 사용자만이 해당 프로그램에 접근할 수 있도록 하는 콘텐츠 보안 솔루션이다[1]. 현재 위성, 지상파, 케이블 방송시스템에서 널리 사용되고 있는 접근제한시스템은 하나의 스마트카드로 동일한 접근제한시스템을 사용하는 서로 다른 셋톱박스(Set-Top BOX, STB)에서 사용하는 것이 가능하다. 2001년 Kanjanarin 등은 접근제한시스템의 이러한 특성 때문에 생겨난 스마트카드 복제 문제와 McCormac Hack 공격에 대해 소개하였다[2]. 스마트카드 복제 문제는 권한이 있는 사용자의 스마트카드를 복제하여 권한이 없는 사용자들이 동일한 종류의 접근제한시스템을 사용하는 STB에서 인가된 사용자처럼 사용하는 문제이고,

※ 본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었슴(NIPA-2011-C1090-1111-0010).
※ 이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임(No. 2011-0000189).
† 준 회 원 : 한양대학교 컴퓨터공학과 박사과정
†† 종신회원 : 한양대학교 컴퓨터공학과 교수(교신저자)
논문접수 : 2011년 9월 5일
수 정 일 : 1차 2011년 11월 8일
심사완료 : 2011년 11월 8일

McCormac Hack 공격은 STB와 스마트카드 간의 통신 채널을 공격하여 제어단어(Control Word, CW)를 얻어낸 후, 그것을 불법적으로 사용하는 문제이다. 방송 수신단인 STB에서는 자격관리메시지(Entitlement Maanagement Message, EMM)와 자격제어메시지(Entitlement Control Message, ECM)를 이용해 CW를 얻는 모든 과정이 사용자의 스마트카드에서 이루어진다. 스마트카드가 CW를 얻은 후, 스크램블링된 콘텐츠의 디스크램블링을 위하여 이 CW를 STB의 디스크램블러에 전달해 주게 되는데, 이 전달 과정에서 스마트카드와 STB간의 통신채널을 도청하여 CW를 획득하는 것이 가능하다. 공격자에 의해 획득된 제어 단어를 STB의 디스크램블러에 직접 입력하면 유료 방송 콘텐츠에 불법적으로 접근하는 것이 가능하다. 스마트카드 복제와 McCormac Hack 공격 등으로 비인가된 사용자의 불법적인 방송시청이 가능할 경우 이는 방송 사업자들의 이익과 직결되는 커다란 문제가 된다. Kanjanarin 등의 제안 이후 스마트카드 복제와 McCormac Hack공격에 대한 많은 연구가 진행되었다[3]-[7].

최근에 방송 사업자들은 이러한 문제를 해결하기 위해 STB에 보안 칩을 내장하는 방식인 칩셋 페어링 접근제한 시스템(Chipset Pairing CAS)을 도입하였다. 칩셋 페어링 CAS는 기존의 CAS들과 마찬가지로 스마트카드를 기반으로 하고 있지만 여기에 STB에 내장된 보안 칩을 함께 사용하는 방식이다. 내장된 보안 칩은 스마트카드와 STB 사이에 안전한 통신채널을 형성하는 역할을 한다. 이러한 칩셋 페어링 CAS는 기존의 CAS들보다 안전성은 크게 증가하였지만 내장된 보안 칩과 쌍을 이루는 스마트카드만이 사용가능하다는 단점이 있다.

방송환경의 발달로 서비스제공자가 제공하는 콘텐츠가 다양해졌으며 사용자들의 요구도 다양화되었다. 또한 TV가격의 하락으로 한 가구당 2대 혹은 그 이상의 TV를 소유하고 각각의 TV에 STB를 연결해서 사용하고 있는 환경이 증가하고 있다. 칩셋 페어링 CAS 이전의 CAS는 가입자가 자신의 스마트카드를 다른 셋톱박스에 꽂아도 가입자 인증이 되어 STB에 상관없이 유료 콘텐츠의 시청이 가능했었으나 칩셋 페어링 CAS에서는 이 같은 것이 불가능하다. 본 논문에서는 칩셋 페어링 CAS의 이러한 단점을 해결하기 위해 중국인의 나머지 정리(Chinese Remainder Theorem, CRT)를 이용한 키 분배 기법을 제안한다. 이어지는 논문의 구성은 다음과 같다. 2장에서는 칩셋 페어링 CAS와 CRT에 대해 설명하고, 3장에서 이 논문에서 제안하는 방법에 대해 자세히 기술한다. 4장에서는 제안하는 기법의 대해 분석하고 기존의 칩셋 페어링 CAS와 비교한다. 6장에서는 결론과 향후 연구방향을 제시한다.

2. 배경지식

이 장에서는 CAS와 CRT에 대해 알아본다. CAS를 구현 형태에 따라 분류하고 각각의 형태가 가지는 특징에 대해 알아본 후, 논문에서 다루고자 하는 칩셋 페어링 CAS에 대해 자세히 설명한다. 또한, 제안하는 기법에서 사용한 CRT와 CRT 기반의 그룹키인 CRGK에 대해 살펴본다.

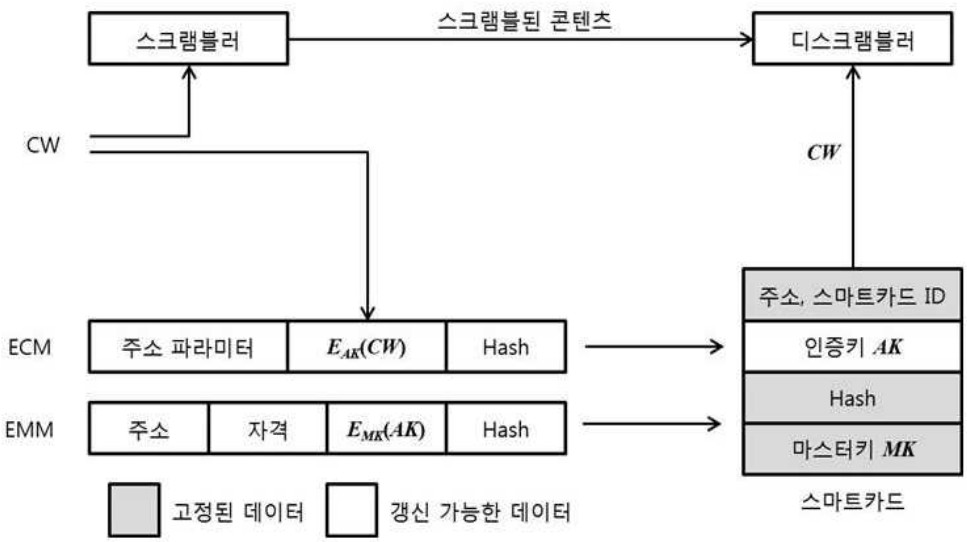
2.1 CAS의 분류와 칩셋 페어링 CAS

1) 일반 OS에 클라이언트 형태로 CAS를 구현

이 방식에서는 키 관리와 자격관리 프로그램을 단순히 일반적인 형태의 마이크로프로세서에 탑재한다. 하지만, 이 방식은 역공학 공격에 매우 취약하다.

2) 보안이 강화된 소프트웨어 형태로 CAS를 구현

이 방식은 보안 메커니즘을 포함하고 있는데 이는 프로그램 내 키 관리와 자격관리 부분이 해커에 의해 역공학 공격



(그림 1) CAS의 구성도

을 당하는 것을 방지하기 위한 것이다. 또한, 이 방식은 양방향 네트워크를 통해 CAS에 대한 인증을 실시함으로써 복제와 같은 공격에 대해 안전하다.

3) STB 내 SoC칩에 CAS를 구현

STB에서 사용되는 일반적인 SoC를 디자인할 때 부가적으로 키 관리와 자격관리 기능을 추가하여 구현하게 된다. 칩 자체는 스마트카드에서 사용된 칩 수준의 보안을 제공하지는 않지만, 소프트웨어만으로 구현된 것보다는 안전하다.

4) STB에 내장된 소프트웨어와 스마트카드를 함께 사용하여 CAS를 구현

이 유형에서 소프트웨어는 스마트카드가 획득한 CW를 보호하고 스마트카드로 전송되는 메시지 흐름을 제어하는 역할을 수행한다. 하지만, STB 내 소프트웨어는 해커에 의한 역공학 공격에 취약하기 때문에 CW를 안전하게 보호할 수는 없다.

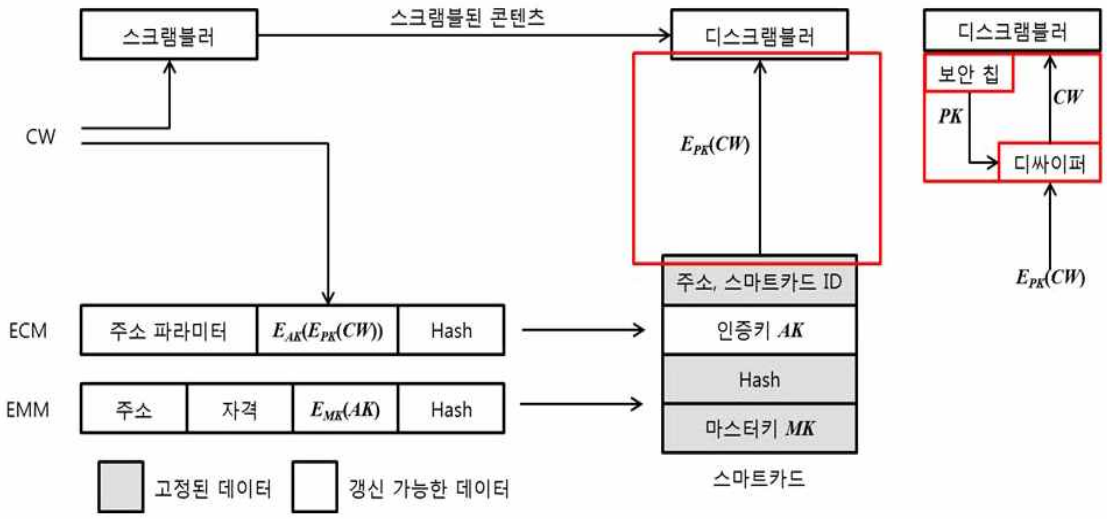
5) STB에 내장된 보안 칩과 스마트카드를 함께 사용하여 CAS를 구현

STB에 내장된 보안 칩은 스마트카드와 셋톱박스 사이에 보안 채널을 형성한다. 스마트카드는 암호화된 CW를 STB로 출력하고, STB는 내장된 보안 칩을 사용해 암호화된 CW를 복호화 한다. 이 방식에서는 키나 자격정보와 같이 매우 중요한 정보가 스마트카드에 저장되기 때문에 STB 내 보안 칩의 보안수준은 높지 않아도 된다.

6) 보안 칩만을 내장해 CAS를 구현

칩이 키와 자격정보와 같이 중요한 정보를 저장해야 하기 때문에, 5)에 사용된 보안 칩보다는 높은 레벨의 물리적 보안이 요구된다. 하지만, 이 유형은 단방향 네트워크상에서 보안의 결함으로 인해 키 관리 및 자격관리 알고리즘 갱신이 요구될 때 STB 자체를 교환해야 한다. 따라서, 스마트카드를 사용한 방식보다 유연한 운용을 할 수 없다.

앞서 살펴본 구현 방식에 따라 나눈 CAS중 4)가 칩셋 페어링 CAS 이전에 주로 사용되던 방식이며 (그림 1)은 그 구성도이다. 칩셋 페어링 CAS는 5)에 해당하며 (그림 2)가 그 구성도이다. 칩셋 페어링 CAS의 동작 원리는 CW 대신 암호화된 CW가 사용된다는 점을 제외하곤 기존 CAS의 동작원리와 동일하다. 방송을 전송하는 쪽인 SMS(Subscriber Management System)에서는 STB와 공유하고 있는 키(Pairing Key, PK)를 이용하여 암호화된 CW를 생성하고 생성된 암호화된 CW를 이용해 방송 콘텐츠를 스크램블링하여 전송한다. 이때 생성된 암호화된 CW는 인증 키(Authorization Key, AK)로 암호화 되어 ECM을 통해 전송되고, AK는 각 사용자의 스마트카드에 저장되어 있는 마스터 키(Master Key, MK)로 암호화 되어 EMM을 통해 전송된다. 방송 수신측인 STB에서는 송신측과 반대 과정을 수행하게 되는데 EMM을 통해 전송되는 MK로 암호화된 AK를 복호화하여 사용자의 스마트카드에 저장되어 있는 AK를 갱신하고 ECM을 통해 전송되는 AK로 암호화 되어 있는 암호화된 CW를 복호화하여 STB의 디스램블러에게 전달한다. STB의 디스크램블러는 STB내에 저장되어 있는 PK를 이용하여 CW를 복호화 하여 스크램블링 되어 있는 콘텐츠를 디스크램블링할 수 있게 된다. 칩셋 페어링 CAS에서 STB와 SMS가 공유하게 되는 PK는 STB의 메인 칩마다 고유한 값을 가진다. ECM내에는 서로 다른 PK로 암호화되어 있는 다수의 CW와 암호화된 CW의 올바른 STB로의 전달을 위한 암호화된 CW와 스마트카드 ID의 매핑정보가 포함되어 있어야 한다. 이렇듯 하나의 스마트카드와 하나의 STB의 메인칩이 쌍을 이루게 되므로 이러한 방식을 칩셋 페어링이라 한다.



(그림 2) 칩셋 페어링 CAS 구성도

2.2 CRT와 CRGK

CRT[8]는 연립 합동식을 하나의 합동식으로 만드는 것에 대한 정리로서 안전한 방송 전송기법[9], 유료 방송을 위한 키 분배 기법[10]등 여러 응용들에 많이 이용되고 있다. 서로소인 자연수 $n_1, ..., n_k$와 임의의 정수 $a_1, ..., a_k$가 있을 때

$$\begin{aligned} x &\equiv a_1 (\mathrm{mod} n_1) \\ &\vdots \\ x &\equiv a_k (\mathrm{mod} n_k) \end{aligned}$$

는 mod $a_1, ..., a_k$안에서 유일한 해 X를 갖는다. X를 구하는 방법은 다음과 같다.

$$\sum_{i=1}^{k} a_i M_i M_i' (\mathrm{mod} M)$$

여기서, $M = n_1 \cdots n_k$이고, $M_i = M / n_i$ 이며, M_i'은 $M_i \bmod n_i$ 의 역원이다. M_i는 u_i와 서로소이기 때문에 mod u_i에 대한 유일한 역원이 존재한다. 그러면 위의 식에 의하여 유일한 해 X를 구할 수 있다. 역원을 효율적으로 구하기 위해서는 확장 유클리드 알고리즘을 사용한다. 확장 유클리드 알고리즘의 자세한 내용은 논문의 범위를 벗어난 내용으로 본 논문에서는 다루지 않는다.

2007년, Zheng 등은 CRT 기반의 그룹키 프로토콜인 CRGK(Chinese Remainder Group Key Protocol)을 제안하였다[11]. Zheng 등의 제안 이후 무선센서네트워크, 키 관리 분야 등에서 CRGK를 기반으로 한 연구들이 진행되었다[12]-[14]. CRGK의 키 생성과 공유 방법은 아래와 같다.

$$\begin{aligned} X &\equiv k_1 (\mathrm{mod} u_1) \\ X &\equiv k_2 (\mathrm{mod} u_2) \\ &\vdots \\ X &\equiv k_n (\mathrm{mod} u_n) \end{aligned}$$

여기서 $u_1, ..., u_n$은 각각의 그룹 멤버가 서버와 공유하는 비밀키이고, n은 현재 그룹의 크기이며, k_i은 멤버들의 비밀키와 최초 그룹키 K와의 XOR한 값이다.

$$k_i = K \oplus u_i (i \in 1, 2, ..., n)$$

합동식의 해 X는 CRT를 이용하여 다음과 같은 식을 통해 쉽게 계산할 수 있다.

$$X = \sum_{i=1}^{n} k_i U_i U_i^{-1} (\mathrm{mod} u_i)$$

여기서 U_n는 $\frac{u_1 u_2 \cdots u_n}{u_n}$이며 U_n^{-1}는 법 u_n에서 U_n의 역원이다.

CRGK에서 가입/탈퇴시 키 서버는 해당 k_i값을 추가하거나 삭제하여 X를 재계산하면 된다. 예를 들어 새로운 멤버 new가 가입할 경우 아래와 같은 식을 추가하여 새로운 X를 계산하면 된다.

$$X \equiv k_{new} (\mathrm{mod} u_{new})$$

3. 제안하는 기법

이 장에서는 현재의 칩셋 페어링 CAS와 Zheng 등이 제안한 CRGK가 가지는 문제점에 대해 각각 살펴보고 이를 개선한 칩셋 페어링 CAS 환경에서 다수의 STB 지원이 가능한 CRT 기반의 키 분배 기법을 제안한다.

3.1 현재 칩셋 페어링 CAS의 한계

칩셋 페어링 CAS는 스마트카드와 STB를 하나의 쌍으로 만드는 방법을 사용함으로써 CAS의 보안성은 향상시켰으나 유연성을 떨어뜨리게 되었다. 즉, 이러한 방법을 사용하면 앞서 언급한 스마트카드 복제와 McCormac Hack 공격에는 강건해지지만 하나의 스마트카드는 오직 하나의 STB에서만 사용이 가능하게 된다. 스마트카드로 사용자의 자격을 인증하는 현재의 DTV(Digital Television) / IPTV(Internet Protocol Television) 방송환경에서 칩셋 페어링 CAS는 시스템의 유연성을 저해한다. 사용자가 가입되어 있는 방송사업자가 제공한 STB라면 사용자는 STB에 상관없이 자신의 스마트카드를 사용하는 것이 가능해야 한다.

제안하는 기법은 하나의 스마트카드로 사용자가 지정한 다수의 STB에서 사용이 가능하도록 설계되었다. 칩셋 페어링 CAS는 칩 자체에 비밀키가 내장되어 있기 때문에 추후에 그 키를 갱신하는 것은 STB나 칩을 바꾸지 않는 이상 불가능 하다. 이러한 이유 때문에 기존의 그룹키 기법을 현재의 칩셋 페어링 CAS에 적용하는 것은 굉장히 어려운 일이다. 제안하는 기법에서는 하드웨어의 교체나 수정 없이 기존의 칩셋 페어링 기법에 적용 가능한 공유키 생성을 위해 중국인의 나머지 정리를 이용하였다.

3.2 CRGK의 문제점

CRGK에서 사용하는 $k_i = K \oplus u_i$에서 u_i는 사용자의 비밀키 이다. K는 그룹의 모든 멤버가 알고 있는 값이다. 이런 환경에서 k_i가 노출될 경우 XOR 연산의 특성 때문에 사용자의 비밀키인 u_i 역시 노출되게 되는데 이는 굉장히 큰 문제라 할 수 있다. 또한, 키 서버가 보내는 그룹키 K에 대한 키 확인 과정이 없어 키 전송 시 발생하는 오류로 인해 키가 변경되는 문제에 취약하다. 제안하는 기법에서는 위의 문제점들을 해결하기 위해 암호학적 해쉬함수의 단방향성을 이용하였다.

3.3 제안하는 키 분배 기법

제안하는 키 분배 기법은 앞서 설명한 칩셋 페어링 CAS에 CRT를 적용하여 다중 셋톱박스를 지원할 수 있도록 개선한다. (그림 3)은 현재의 칩셋 페어링 CAS에서 개선된 부분을 보여준다. SMS는 PK_i가 아닌 세션키 SK로 CW를 암호화 하며, ECM에 합동식의 해 X를 포함하여 전송한다. STB의 보안 칩은 PK_i로 CW를 복호화 하는 대신 PK_i로 SK를 계산한 후 SK로 암호화 되어 있는 CW를 복호화 하여 콘텐츠 디스크램블링에 사용한다. 제안하는 기법은 등록 단계와 키 확립 단계, STB의 추가와 삭제단계로 구성된다. 제안하는 기법에서 사용하는 표기법 <표 1>과 같다.

〈표 1〉 제안하는 기법에서 사용하는 표기법

표기법	내용
STB_i	사용자가 등록한 STB
ID_{SC}	스마트카드의 ID
SK	CW를 암호화하기 위한 세션키
PK_i	i번째 STB의 보안 칩에 내장된 고유키
MK	스마트카드에 저장 된 마스터키
X	합동식의 해

1) 등록 단계

새로운 가입자는 ID, 마스터키 $[ID_{SC}, MK]$가 저장된 스마트카드를 발급받는다. 이때, 자신이 갖고 있는 STB에 대한 정보를 SMS에 등록한다. 등록하는 절차는 오프라인으로 안전하게 이루어진다고 가정한다. 또한, STB는 사전에 인증된 기기이어야 하며 SMS는 STB_i를 제조한 제조업체로부터 칩셋 페어링에 사용되는 페어링 키 PK_i의 정보를 알 수 있다고 가정한다. PK_i는 STB_i에 내장되는 보안키로 STB의 메인칩을 공급하는 칩셋 제조업체에 의해 생성된다. 키 생성과정에서 칩 제조업체는 CRT를 이용한 연산이 가능하도록 각각의 PK_i가 서로 소의 관계가 되도록 PK_i를 생성하여야한다. 등록 단계가 끝난 후, SMS에 저장되는 정보는 다음과 같다.

$$[ID_{SC}, MK, PK_i]$$

SMS에 저장된 가입자 정보는 가입자가 소유하고 있는 STB가 추가 또는 제거될 때마다 사용자에 의해 변경되어야 한다. 변경 절차는 온라인을 사용하지 않고 가입자가 전화 또는 대리점 방문 등을 통하여 가입자 인증 절차를 거친 후 안전하게 변경된다고 가정한다.

2) 키 확립 단계

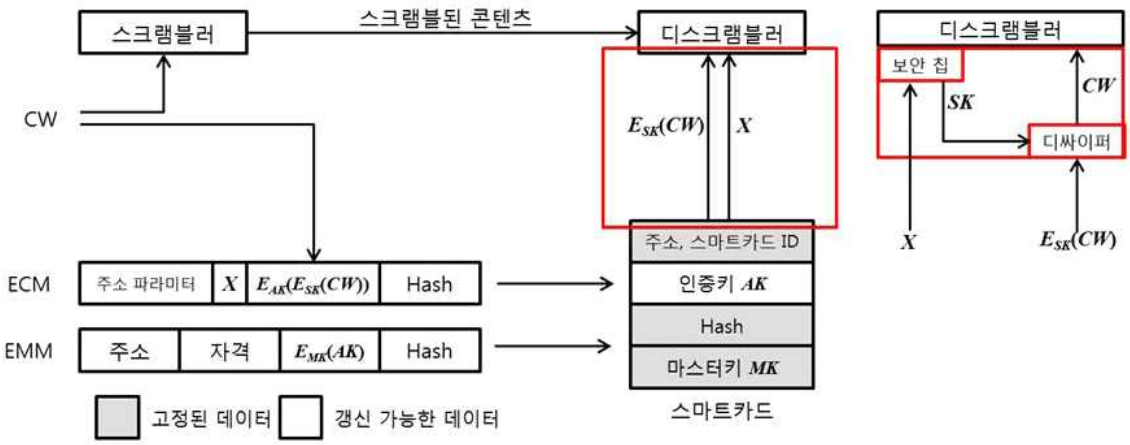
SMS가 제어단어를 EMM, ECM을 통하여 가입자에게 전달하는 과정에서, 등록 단계에서 저장된 정보와 SK를 생성하여 다음의 합동식을 만든다.

$$\begin{aligned} X &\equiv a_1 \pmod{PK_1} \\ &\vdots \\ X &\equiv a_k \pmod{PK_k} \end{aligned}$$

$$a_i = [SK \| h(SK, PK_i)] \oplus PK_i$$

여기서 $i \in \{1, 2, ..., k\}$이고, k는 SMS에 등록된 가입자 STB의 개수이다. 위와 같이 합동식을 생성하게 되면 CRT를 이용하여 합동식의 유일한 해 X를 구할 수 있다. X가 계산되면 ECM에 X를 포함시켜 전송함으로써 가입자에게 전달한다. 이때, EMM과 ECM이 갖고 있는 정보는 다음과 같다.

$$\begin{aligned} EMM &= [E_{MK}(AK)] \\ ECM &= [X, E_{AK}(E_{SK}(CW))] \end{aligned}$$



(그림 3) 제안하는 기법의 구성도

STB는 전송스트림으로부터 EMM과 ECM을 추출하여 스마트카드에 전송하고, EMM과 ECM을 전송받은 스마트카드는 MK를 이용하여 AK를 복호화하고, AK를 이용하여 $E_{SK}(CW)$를 복호화하여 STB에게 다시 전송한다. STB 내의 보안 칩에서는 ECM에 포함괴어 있는 다항식의 해 X와 보안 칩 안에 내장되어 있는 PK_i를 이용하여 SK를 구한다. SK를 구함으로써 SMS와 가입자의 보안 칩 간에 SK를 공유할 수 있게 된다. SK를 계산하는 식은 다음과 같다.

$$[SK \| h(SK, PK_i)] = (X \bmod PK_i) \oplus PK_i$$

위의 식을 통해 계산된 값 중 $h(SK, PK_i)$는 키 확인과 PK_i의 노출을 방지 하는 값으로 실제로는 $h(SK, PK_i)$를 제외한 SK만이 사용된다. 이 때, X는 가입자가 소유하고 있는 STB의 보안 칩 내의 PK_i들로 생성한 합동식의 해이므로, SMS에 등록되지 않은 STB에서는 SK를 계산할 수 없게 된다. (그림 3)은 제안하는 키 분배 기법의 전제적인 구성도를 나타낸다.

3) STB의 추가와 삭제

STB의 추가 또는 삭제 될 경우 SMS는 새로운 세션키 SK를 생성하고 추가 또는 삭제 된 STB의 PK_i를 반영하여 새로운 합동식의 해 X를 계산하여 각각 EMM과 ECM에 포함하여 전송하면 된다.

$$\begin{aligned} X &\equiv a_1 (\bmod PK_1) \\ &\vdots \\ X &\equiv a_k (\bmod PK_k) \\ X &\equiv a_{new} (\bmod PK_{new}) \end{aligned}$$

$$a_i = [SK \| h(SK, PK_i)] \oplus PK_i$$

4. 분 석

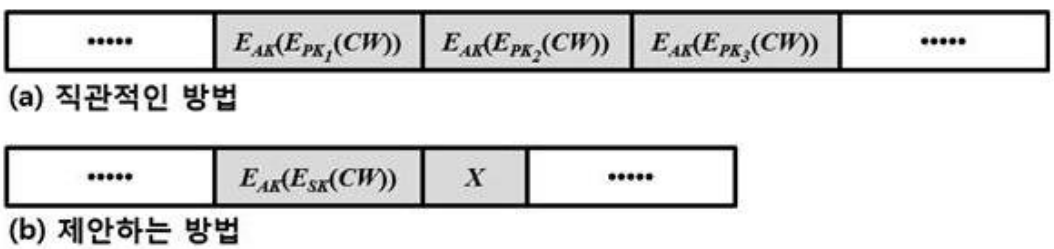
이 장에서는 제안하는 기법의 효율성과 안전성에 대해 분석한다. 효율성은 기존의 칩셋 페어링 CAS 환경에서 다수의 STB를 사용할 때와 제안기법을 사용하여 다수의 STB를 사용할 때의 ECM 구성을 비교하였으며, 안전성은 CAS와 그룹키 분배 기법의 보안요구사항들을 만족하지에 대해 논의한다. 또한 Zheng 등의 CRGK에서 가지고 있던 페어링 키 노출과 키 확인이 가능함을 보인다.

4.1 효율성 분석

제안하는 기법은 기존의 칩셋 페어링 CAS에서 지원하지 못하는 하나의 스마트카드와 다수의 STB의 페어링이 가능하다. STB의 고유의 키인 PK로 암호화된 CW가 올바른 STB로 전달되기 위해서는 ECM안에 암호회된 CW의 도착지 정보가 포함되어 있어야 한다. 현재의 칩셋 페어링 CAS에선 그 도착지 정보가 스마트카드의 ID이다. 스마트카드의 ID와 암호화된 CW의 매핑정보를 ECM을 통해 전송해 줌으로써 서로 다른 STB의 비밀키로 암호화된 CW가 올바른 STB에 수신될 수 있는 것이다. 이는 ECM에 스마트카드와 암호화된 CW의 매핑 정보만 있으면 올바른 STB로의 전송이 가능하다는 것을 의미한다.

SMS는 각각의 사용자를 위한 스마트카드와 암호화된 CW의 매핑 정보를 생성해 ECM을 통해 전달한다. 한명의 사용자가 다수의 STB를 사용하길 원한다면 SMS는 그 사용자의 모든 스마트카드와 암호화된 CW의 매핑 정보를 전송하면 된다. 이러한 직관적인 방법에서는 STB의 수가 n이라 할 때 n만큼의 매핑정보가 더 필요하다. STB의 수가 늘어나면 늘어날수록 ECM을 통해 전송해야 하는 정보가 늘어나게 되고 그에 따라 전체 방송 스트림의 크기 역시 증가하게 된다. 이는 매우 비효율적이라 할 수 있다. 그러나 제안하는 기법에서는 STB의 수가 늘어난다 해도 SK를 계산하기 위한 해 X만을 새로 계산하면 되므로 훨씬 효율적이라 할 수 있다. (그림 4)는 직관적인 방법과 제안하는 방법의 비교이다. STB가 3대일 경우, 직관적인 방법으로는 각각의 PK를 이용해 암호화한 CW $E_{PK_1}(CW)$, $E_{PK_2}(CW)$, $E_{PK_3}(CW)$를 전송해야 하지만 제안하는 방법을 사용 할 경우에는 다항식의 해 X와 각각의 PK를 이용해 계산이 가능한 SK로 암호화한 CW $E_{SK}(CW)$만을 전송하면 된다.

또한, 제안하는 기법에서 각각의 PK를 위한 해 X의 계산은 SMS 측에서 이루어지기 때문에 STB 측에서는 한번



(그림 4) 직관적인 방법과 제안하는 방법의 효율성 비교

의 modular 연산과 한번의 XOR 연산만 수행하게 된다. 이 두 연산은 매우 간단한 연산으로 현재 사용되고 있는 의 동작에 큰 영향을 미치지 않는다고 할 수 있다.

4.2 안전성 분석

CAS가 만족해야 하는 보안 요구사항으로는 인증(Authentication)과 기밀성(Confidentiality)이 있고. 그룹키 분배 기법이 만족해야 하는 보안 요구사항은 전방향 안전성(Forward Secrecy), 후방향 안전성(Backward Secrecy), 공모 공격(Collision Attack)이 있다.

• 인증: CAS에서 사용자 인증은 EMM내의 $E_{MK}(AK)$를 복호화 여부로 하는 단방향 인증이다. 즉, 위의 메시지를 복호화하여 AK를 획득할 수 있으면 인증이 된 것이고 그렇지 않으면 인증이 되지 않은 것이다. 사용자는 자신의 비밀키인 MK가 저장된 스마트카드를 SMS로부터 발급받는다. MK는 스마트카드의 TRH(Temper Resistant Hardware) 영역에 저장되는데 이는 물리적 공격이나 역공학과 같은 공격으로부터 안전하다고 할 수 있다. 제안하는 기법은 기존 CAS의 사용자 인증 기법을 그대로 따른다.

• 기밀성: CAS에서 데이터는 CW로 암호화되어 전송된다. 암호화된 데이터가 노출된다 하더라도 CW를 알지 못하면 그 데이터의 내용을 알아내는 것은 불가능 하다. 제안하는 기법은 CAS의 이러한 특성을 그대로 가진다.

• 전방향 안전성: 전방향 안전성이란 그룹에서 탈퇴한 사용자로부터 그 사용자의 탈퇴 이후의 그룹키의 안전성을 보장하는 것이다. 제안하는 기법에서 STB가 삭제될 경우 새로운 세션키 SK를 생성하고 그 STB의 PK를 제외한 합동식의 새로운 해 X를 만들어서 전송하기 때문에 삭제된 STB에서 새로운 SK를 계산하는 것은 불가능하다.

• 후방향 안전성: 후방향 안전성은 새로 가입한 사용자로부터 그 사용자의 가입 이전의 그룹키의 안전성을 보장하는 것이다. 전방향 안전성에서 보인 것과 마찬가지로 제안하는 기법에서는 STB가 추가될 경우에도 세션키 SK와 합동식의 해 X를 새로 만들기 때문에 추가된 STB에서 이전의 SK를 계산하는 것은 불가능하다.

• 공모 공격: 공모 공격은 이전 그룹키를 사용하던 사용자들이 공모하여 현재 사용되고 있는 그룹키를 알아내려는 공격이다. 제안하는 기법에서는 STB의 매 추가/삭제시 마다 새로운 세션키 SK와 합동식의 해 X를 새로 만들기 때문에 이전 사용자들이 공모를 한다해도 현재 사용되고 있는 그룹키에 대한 어떠한 정보도 얻는 것이 불가능하다.

• 페어링 키 노출과 키 확인: CRGK처럼 $a_i = SK \oplus PK_i$ 형태의 값을 사용하게 되면 a_i의 노출시 XOR 연산만으로 STB_i 의 보안 칩에 내장된 페어링 키 PK가 쉽게 노출되는 문제를 가진다. PK의 노출은 STB의 칩 교체를 야기하는 큰 문제이다. 또한, SK의 경우 SMS가 생성한 후 이에 대한 키 확인 과정이 없어 키 전송시 발생하는 오류로 인해 키가 변경되는 문제에 취약하다. 제안하는 기법에서는 $a_i = [SK \| h(SK, PK_i)] \oplus PK_i$ 형태의 값을 사용하였다. a_i가 노출된다 하더라도 PK_i를 알 수 없으면 $h(SK, PK_i)$를 계산 할 수 없기 때문에 PK_i의 노출을 방지할 수 있다. 또한, SK와 PK_i를 이용한 $h(SK, PK_i)$를 통해 SK의 확인이 가능하다.

5. 결론 및 향후 과제

본 논문에서는 CRT를 이용하여 유연한 칩셋 페어링 CAS를 위한 키 분배 기법을 제안하였다. 이는 현재 많이 사용되고 있는 CAS의 칩셋 페어링 방식에서 스마트카드와 STB가 1:1로만 매핑이 되기 때문에 생겨난 시스템의 유연성 저하 문제를 개선한 것이다. 제안하는 기법은 하나의 스마트카드와 사용자가 원하는 수 만큼의 STB를 매핑하는 것이 가능하다. 이러한 유연한 칩셋 페어링 CAS는 방송 환경 발달, 하드웨어의 가격하락에 따라 발생 가능한 한명의 가입자가 다수의 STB를 소유하게 되는 환경에서 가입자의 자격관리에 매우 유용하게 사용될 수 있다.

제안하는 기법은 XOR과 modular 같은 매우 가벼운 연산만이 추가되었다. 또한, 제안하는 키 분배 기법은 DTV 표준에 위배되지 않으며 하드웨어의 교체나 수정 없이 현재의 칩셋 페어링 CAS에 그대로 적용이 가능한 장점을 가지고 있다. 향후에는 제안하는 기법의 실제 구현 또는 시뮬레이션을 통해 기존 칩셋 페어링 CAS와 제안하는 기법간의 ECM의 메시지 효율성에 대한 정량적인 비교에 대한 연구가 진행되어야 할 것이다.

참 고 문 헌

[1] EBU Project Group B/CA, “Functional model of a conditional access system”, EBU Technical Review, pp.64-77, 1995.

[2] W. Kanjanarin and T. Amornraksa, “Scrambling and key distribution scheme for digital television”, IEEE International Conference on Networks (ICN), pp.140-145, 2001.

[3] T. Jiang, Y. Hou and S. Zheng, “Secure communication between set-top box and smart card in DTV broadcasting”, IEEE Transaction on Consumer Electronics, Vol.50, No.3, pp.882-886, 2004.

[4] T. Hou, J. Lai and C. Yeh, “Based on cryptosystem secure communication between set-top box and smart card in DTV broadcasting”, TENCON 2007, IEEE Region 10 Conference, pp.1-5, 2007.

[5] H. Kim, “Secure communication in digital TV broadcasting”,

International Journal of Computer Science and Network Security (IJCSNS), Vol.8, No.9, pp.1-5, 2008.
[6] E. Yoon and K. Yoo, "Robust key exchange protocol between set-top box and smart card in DTV broadcasting", INFORMATICA, Vol.20, No.1, pp.139-150, 2009.
[7] S. Lee, N. Park, S. Kim and J. Choi, "Cryptanalysis of secure key exchange protocol between STB and smart card in IPTV broadcasting", International Conference on Information Security and Assurance (ISA), LNCS 5576, pp.797-803, 2009.
[8] T. Comen, C. Leiserson, R. Rivest and C. Stein, "Introduction to algorithms," Second Edition. MIT Press and Mcgraw-Hill, 2001. ISBN 09262-03293-7.
[9] G. Chiou and W. Chen, "Secure broadcasting using the secure lock," IEEE Transaction on Software Engineering, Vol.15, No.8, pp.929-934, 1989
[10] B. Hu, W. Ye, S. Feng and X. Wang, "Key distribution scheme based on two cryptosystems for hierarchical access control," IEEE International Conference on Advanced Communication Technology (ICACT), pp.1723-1728, 2006.
[11] X. Zheng, C. Huang and M. Matthews, "Chinese remainder theorem based group key management," ACM Southeast Regional Conference, pp.206-271, 2007.
[12] J. Zhou and Y. Ou, "Key tree and Chinese remainder theorem based group key distribution scheme," Journal of Chinese Institute of Engineers, Transactions of the Chinese Institute of Engineers, Series A/Chungk-kuoKung Ch'eng Hsuck K'an Vol.32, Issue7, pp.967-974, 2009.
[13] Y. Ren, V. Oleshchuk and F. Li, "An efficient Chinese remainder theorem based node capture resilience scheme for Mobile WSNs," IEEE International Conference on Information Theory and Information Security (ICITIS), pp.689-692, 2010.
[14] Y. Song and Y. Zhang, "A mixed key management scheme of clustering wireless sensor network," International Conference on Computer Application and System Modeling (ICCASM), pp.v7198-v7201, 2010.

이 훈 정

e-mail : hjlee@infosec.hanyang.ac.kr
2003년 단국대학교 전자컴퓨터학부(학사)
2005년 한양대학교 컴퓨터공학과(석사)
2005년~2009년 (주)한단정보통신 전임연구원
2009년~현 재 한양대학교 컴퓨터공학과 박사과정
관심분야 : 암호기술 응용, 키 관리

손 정 갑

e-mail : jgson@infosec.hanyang.ac.kr
2009년 한양대학교 컴퓨터공학과(학사)
2011년 한양대학교 컴퓨터공학과(석사)
2011년~현 재 한양대학교 컴퓨터공학과 박사과정
관심분야 : 암호기술 응용, IPTV보안

오 희 국

e-mail : hkoh@hanyang.ac.kr
1983년 한양대학교 전자공학과(학사)
1989년 아이오와주립대학교 전자계산학과 (석사)
1992년 아이오와주립대학교 전자계산학과 (박사)
1993년~1994년 한국전자통신연구원 선임연구원
1995년~현 재 한양대학교 컴퓨터공학과 교수
2009년~현 재 한국정보보호학회 부회장
2009년~현 재 대검찰청 디지털수사 자문위원
관심분야 : 암호프로토콜, 네트워크 보안