通信情報保護學會誌
第4卷 第2號, 1994. 6

유료 방송 시스템의 스마트 카드

원 치 선*, 김 재 공**

1. 서 론

TV 방송이 지상방송에서 Cable TV 및 직접위성방송(DBS) 등의 다양한 매체를 통하여 실현되고 있다. 방송의 매체가 다양해지면서 방송 채널의 수도 증가하고 있다. 또한 방송 신호의 완전 디지탈화의 추세와 함께 영상신호가 차지하는 주파수의 대역폭을 상당히 줄일 수 있는 영상 압축의 기술 발달에 따라 방송 채널의 수는 더욱 증가될 수 있다. 방송 채널의 증가는 전문 방송 채널의 탄생을 가능케하고, 전문 방송의 운영은 가입자들이 낸 시청료에 의존하게 된다. 유료방송 시스템의 지속적인 재정적 안정을 유지하기 위해 가입들은 모두 시청료를 내고, 시청료를 지불하지 않은 가입자들은 정상적인 방송 신호를 수신할 수 없도록 하는 한정수신 시스템(Conditional Access System)이 도입되어야 한다. 유료 방송 시스템이 도입된 이래로 방송업자들은 도시청자들로부터 계속적인 도전을 받아왔다. 실제로 1989년 미국의 FCC(Federal Communications Commision)의 보고[1]에 의하면 그당시 위성방송의 모든 디스크램블러(Descrambler)의 적어도 50%가 도시청(Pirate Box)에 의한 불법 수신이었다. Cable TV도 예외일 수는 없다. Cable TV와 위성 방송업자들이 도시청으로부터 절대 안전 시스템으로 믿고 도입된 시스템들이 계속적으로 그 안전성이 깨지고 있고, 그때마다 방송업자들이 도산하고, 또 진일보한 한정수신 시스템을 갖고 새로운 방송이 탄생하는 과정이 반복되어 왔다.

과거의 한정수신 시스템에 많은 도시청이 발생할 수 있었던 것은 TV 수상기의 위에 고정된 디스크램블러 상자에 암호화 키의 해독을 위한 해독 알고리즘과 비밀 키가 저장되어 있는 구조[2]와 무관하지 않다. 만약 각 가입자의 디스크램블러 상자를 주기적으로 바꾸어 주어 해독 알고리즘이나 비밀키를 갱신해줄 수 있다면 상당수의 도시청을 방지할 수 있었을 것이다. 그러나 값비싼 디스크램블러 상자를 주기적으로 바꾸어 주는 것은 비경제적인 해결책으로 채택될 수 없었다. 최근에 반도체 기술의 발달과 함께 고집적 반도체 칩이 값싸게 공급되면서 모든 해독 알고리즘과 비밀키를 TV의 디스크램블러로부터 분리 가능한 스마트 카드(Smart Card)에 저장하는 시스템이 제안되고 있다. 상대적으로 저렴한 가격으로 공급될 수 있는 스마트 카드는 모든 가입자들의 계약 갱신주기(즉, 매 1-3개월 주기 등) 혹은 도시청의 발생이 의심될 때마다 각 가입자들에게 새로운 스마트 카드로 대치된다. 이때, 해독 알고리즘, 비밀키 및 자격(Entitlement) 정보 등이 바뀔 수 있어 보안성이 한층 향상된 시스템이 될 수 있다.

* 동국대학교 전자공학과 조교수
** 동국대학교 전자공학과 교수

2. 한정수신 시스템의 구성

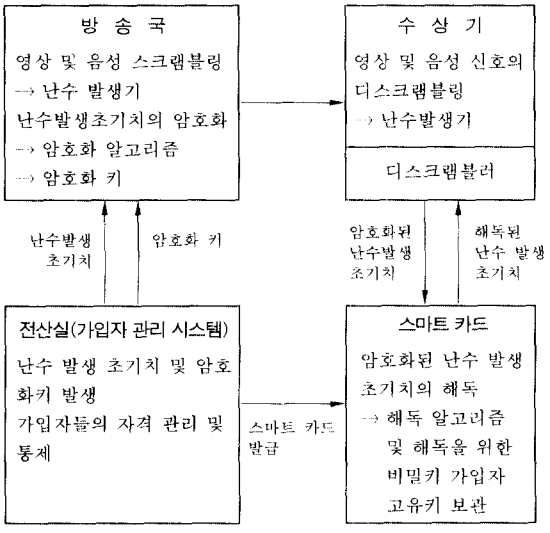

그림 1 한정 수신 시스템의 구성

한정수신 시스템을 갖춘 방송은 그림1과 같이 크게 4개의 블럭으로 구성되어 있다. 즉 방송국, 전산실(가입자 관리 시스템), TV 수상기, 그리고 스마트 카드를 갖춘 디스크램블러 등이다. 방송국에서는 전송될 영상 및 음성 신호를 제작하고 제작된 신호를 난수 발생기에서 발생된 난수로 스크램블링 한다. 이때 사용된 난수 발생기의 초기치는 전산실의 컴퓨터에서 제공되며 역시 컴퓨터에서 발생된 키로 암호화되어 스크램블링된 영상 및 음성 데이타와 함께 각 TV 수상기에 전달된다. 디스크램블링에 필요한 난수 발생기 초기치의 해독은 그것을 암호화할때 사용된 키를 얻으면 가능하다. 전산실의 컴퓨터에서 발생된 이 키는 다시 각 가입자의 고유번호로 암호화되어 스마트 카드에 저장된 채 계약 갱신 주기마다 가입자들에게 전달된다. 이때 난수 발생 초기치를 암호화했던 키도 계약 갱신 주기마다 바뀔 수 있다. TV 수상기에서는 수신된 신호중 암호화된 난수 발생 초기치를 디스크램블러에 보내면 디스크램블러의 스마트 카드는 가입자의 고유키로 난수발생 초기치를 암호화했던 키를 해독하고, 해독된 키로 다시 난수발생 초기치를 해독하여 난수발생 초기치를 수상기의 디스크램블러로 보내 영상 및 음성 데이타를 디스크램블링하는데 사용한다. 같은 키로 해독된 프로그램 정보나 개별 정보는 스마트 카드내 자격 정보와 비교되어 수신자의 수신자격 여부도 판정된다.

3. 스마트 카드의 동작

스마트 카드는 EEPROM(Electrically Erasable Programmable Read Only Memory), RAM (Random Access Memory), Masked ROM, 그리고 마이크로 프로세서로 이루어져 있다. Masked ROM에는 카드의 운영 프로그램과 해독 알고리즘이 저장되어 있고 EEPROM에는 가입자의 자격이나 가입자의 고유번호, 난수 발생기의 초기치를 암호화했던 키(암호화된) 등의 서비스 키들이 저장되며 RAM에는 해독 알고리즘등이 동작하면서 사용되는 데이타들이 잠시 저장된다. 이들 메모리와 마이크로 프로세서는 단일 칩상에 설계되어 메모리와 프로세서 사이의 데이타 흐름을 외부에 노출시키지 않고 또 그런 시도가 있으면 EEPROM의 내용이 자동 삭제되도록 설계되어 있다.

스마트 카드가 디스크램블러에 삽입되면 스마트 카드와 디스크램블러의 리셋핀이 동작하여 양쪽의 boot-up 프로그램이 시작된다. 이때 스마트 카드와 디스크램블러는 서로 통신하여 합법적인 상대임을 확인한다. 스마트 카드와 디스크램블러의 확인 과정은 Fiat-Shamir의 영지식 인증을 사용할 수 있다[3][4]. 즉, 방송국의 가입자 관리 시스템에서는 공개된 modulus n과 (n은 두개의 소수 p와 q의 곱이며 512bit 정도의 길이로 p와 q는 가입자 관리 시스템에서만 비밀로 보관한다.) 의사 랜덤 함수 f를 갖고 각 가입자의 고유 개인정보(또는 가입자의 고유키) I로부터 f와 n의 함수로 k개의 값 s_i를 만들어 스마트 카드내에 I와 함께 저장

한다. 즉, $v_j=f(I,j)$를 계산하고 이때 함수 값중 quadratic residue(mod n)가 되는 v_j만 취하고 v_j^{-1}(mod n)의 가장 작은 자승근이 s_j이다. 스마트 카드를 발급할 때에는 가입자의 고유정보 I와 그것으로부터 발생된 k개의 s_j값과 그들의 인덱스를 스마트 카드내에 저장한다.

디스크램블러는 verifier로서 모두 같은 함수 f와 modulus n을 알고 있다. 스마트 카드가 디스크램블러에 삽입되어 상호증명 작업이 시작되면 스마트 카드는 디스크램블러에게 자신의 고유정보 I를 보내고 디스크램블러는 자신이 갖고 있는 f와 n으로 스마트 카드내 $s_1, \cdots, s_k$를 알고 있다는 것을 보임으로써 스마트 카드를 인정한다. 그러나 Fiat-Shamir 방법을 사용하면 디스크램블러의 ID는 구별되지 않는다. 즉, 유효한 스마트 카드만 있으면 어떤 디스크램블러로 부터도 인증을 받아 프로그램을 시청할 수 있어, 디스크램블러의 구별이 없어진다. 그러나 다양한 서비스를 위해 또는 도난된 스마트 카드의 도용을 막기 위해 디스크램블러도 고유의 ID를 갖고 구별될 필요가 있다. 이를 위해 디스크램블러도 스마트 카드에 보관된 고유 개인정보 I를 갖고 있도록 할 수 있다. 보통 디스크램블러 제조시 각 디스크램블러는 가입자 관리 부서에서 부여하는 고유의 ID번호를 갖는다. 이 ID번호로부터 각 가입자의 고유키를 발생하고 스마트 카드내 저장하여 전달하는데, 이 ID번호를 고유정보 I로도 사용할 수 있다. 즉, 스마트 카드의 최초 사용시 그때의 스마트 카드와 연결된 디스크램블러에게 스마트 카드는 그것의 고유정보 I를 전달하고, 고유정보 I를 전달받은 디스크램블러는 $v_j=f(I, j)$를 발생하여 보관하고 그 이후의 스마트 카드의 인증 작업에서 I가 없어도 이미 보관된 v_j로부터 인증한다. 일단 스마트 카드가 최초로 사용된 이후 다시 디스크램블러에 삽입되어 재사용될 때는 절대로 고유정보 I가 디스크램블러에 전달되지 않는다. 그러므로 디스크램블러는 특정 스마트 카드만 인증할 수 있어, 좀더 다양하고 안전한 가입자 관리를 할 수 있다. 또한 매번 스마트 카드가 I를 전달하고 디스크램블러는 $v_j=f(I,j)$를 계산하는 과정이 생략될 수 있다. 이때 Fiat-Shamir의 인증 과정은 아래와 같다.

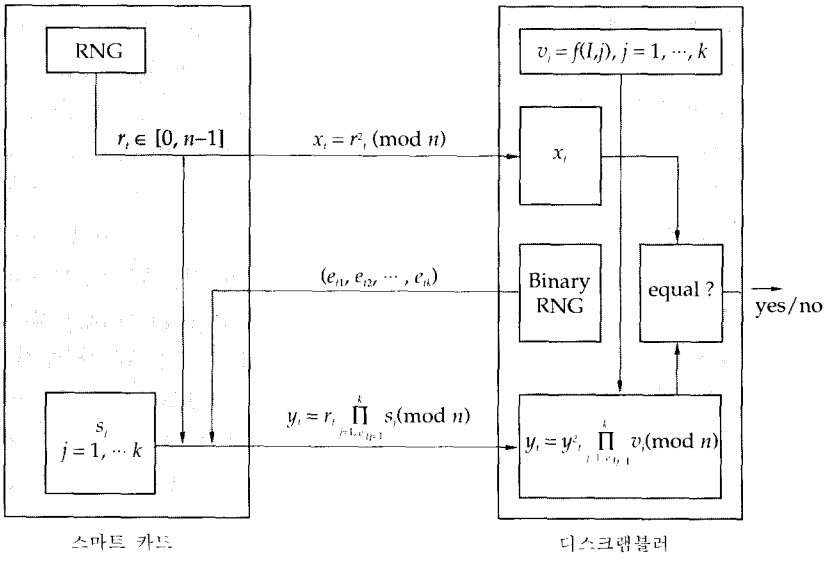

그림 2 스마트 카드와 디스크램블러의 상호증명

다음의 과정 a)-d)를 $i=1, \cdots, t$에 대해 반복한다.(그림 2 참조)

a) 스마트 카드는 random number $r_i \in [0, n]$를 발생하여 $x_i=r_i^2 (\mathrm{mod}\ n)$을 디스크램블러에 보낸다.

b) 디스크램블러에서는 random binary vector $(e_{i1}, \cdots, e_{ik})$를 스마트 카드에 보낸다.

c) 스마트 카드는 $y_i=r_i \prod_{eij=1} S_j (\mathrm{mod}\ n)$을 디스크램블러에 보낸다.

d) 디스크램블러는 자신이 보관하고 있는 v_j로 $y_i^2 \prod_{eij=1} v_j (\mathrm{mod}\ n)=x_i$인지 확인한다.

디스크램블러는 위의 t번의 검사가 통과되야 스마트 카드를 인증한다. 일단 스마트 카드가 디스크램블러에 의해 인증되면 TV 수상기로부터 받은 암호화된 난수 발생기의 초기치와 그것을 암호화했을때 사용된 키(역시 암호화된)가 디스크램블러를 거쳐 스마트 카드에 전달되며 난수 발생기의 초기치가 스마트 카드에서 해독되어 디스크램블러에 다시 전달되고 영상 및 음성을 디스크램블링하는데 사용된다. 그러므로 모든 해독관련 보안작업은 스마트 카드에서 행해지고 디스크램블러는 스마트 카드의 인증 작업과 영상 및 음성 신호의 디스크램블링을 담당한다. 스마트 카드는 디스크램블러로부터 분리 가능하며 상대적으로 가격이 저렴하여 주기적으로 새로운 카드로 대치될 수 있고 해독 알고리즘과 암호화 키도 그때마다 변경이 가능하다.

4. 스마트 카드 관리

스마트 카드를 관리하는 방법은 크게 두 가지로 나눌 수 있다. 즉, over-the-air addressing 방법과 카드교체 방법이 그것이다[5]. Over-the-air addressing은 각 가입자의 자격 통제 및 정보전달을 가입자 관리 시스템(Subscriber Management System)으로부터 전달받아 스크램블된 비디오 신호와 함께 또는 별도의 통신 채널을 통해 각 가입자의 고유 주소로 전달하여 가입자의 스마트 카드의 자격 내용을 변경할 수 있다. 이때 스마트 카드내 pay-per-view를 위한 토큰이나 특정 채널 또는 특정 프로그램의 시청 자격을 통제할 수 있다. 또한 가입자의 시청료 수납 관계를 on-screen display하는 등 각 가입자에게 개별적인 메세지도 전달할 수 있다. 예를 들어 가입자가 계약 갱신 주기내에 서비스의 확장(또는 축소나 폐지)을 전화로 가입자 관리 시스템에 요청할 수 있고, 이때 가입자 관리 시스템에서는 즉시 over-the-air addressing으로 자격 변동 신호를 만들어 해당 가입자의 주소로 송신하고, 가입자는 새로운 자격을 스마트 카드의 교체없이 갱신받고 가입자의 TV 수상기에 자격 갱신 내용이 디스플레이되어 확인된다. 스마트 카드는 계약주기 또는 그 보다 긴 주기로 새로운 카드로 교체되어 자격, 암호화 키, 또는 해독 알고리즘 등을 변경시켜 시스템의 비도를 높일 수 있다. VideoCrypt시스템에서는 3개월을 주기로 새로운 스마트 카드가 발송되거나 도시청의 의심이 있을 때마다 교체된다.

5. 스마트 카드의 안전

스마트 카드에 대한 역엔지니어링(reverse engineering)은 비경제적인 해킹(hacking)이다. 스마트 카드의 칩은 엑포시 수지(epoxy resin)로 덮여있어 엑포시 수지를 벗겨낼 때 칩이 손상될 수 있다. 그러므로 디스크램블러의 콘트롤 하드웨어를 포함한 암호화 칩의 보호는 엑포시 수지처리로 가능하다. 스마트 카드의 EEPROM의 내용을 읽어 무효화된 스마트 카드에 복사하므로써 해킹이 발생할 수 있다. 그러나 새로운 카드 발급시 ROM내 데이타가 바뀌어 해독 알고리즘에 대한 데이타가 서로 맞지 않게되므로 이와같은 해킹은 방지될 수 있다. 스마트 카드 시스템의 또 다른 가능한 해킹은 카드와 디스크램블러 사이의 데이타 흐름을 모니터하여 다른 미가입 디스크램블러들을 동작시키는 것이다. McCormac Hack[6]으로 알려

진 이 가상적인 해킹은 그림 3에서와 같이 스마트 카드와 디스크램블러 사이의 데이타 흐름 신호를 전화 모뎀이나 라디오 전송으로 한개 이상의 미가입 디스크램블러와 가상의 스마트 카드에 전달하여 미가입자도 정상적인 신호를 수신하도록 한다.

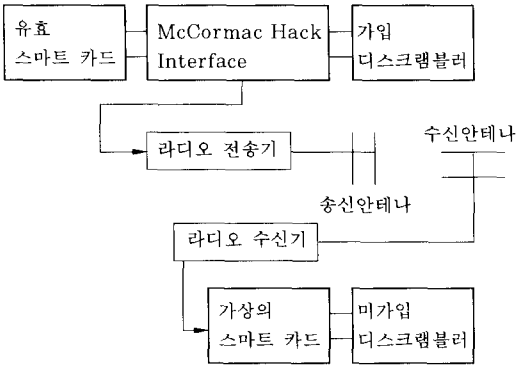

그림 3 McCormac Hack

가상의 스마트 카드는 다음의 4가지 요소로 구성되어 있다. 첫째는 라디오 신호 수신 장치로 UHF 형태의 축소된 안테나를 사용하고, 둘째는 데이타 디코더, 세번째는 마이크로 프로세서 콘트롤, 그리고 마지막 네번째는 가상의 스마트 카드와 디스크램블러를 연결해주는 인터페이스 회로다. McCormac Hack은 가상적인 해킹으로 실제 실현여부는 알려져있지 않다. 실제로 McCormac Hack이 실현되려면 스카트 카드와 디스크램블러 사이의 최초 인증 작업이 모든 가상 스마트 카드와 디스크램블러 사이에서도 정상적으로 이루어져야 한다. 그러나 Fiat-Shamir 인증 방법등 대부분의 스마트 카드 인증 알고리즘들이 인증 과정중 디스크램블러가 random binary vector (혹은 random number)를 발생하여 인증 자료로 사용하므로 가상의 스마트 카드와 연결된 모든 미가입 디스크램블러와 원래의 가입 디스크램블러가 동기화되어 있어야하며 그렇지 않은 경우 디스크램블러마다 발생된 random binary vector가 서로 달라 인증에 실패할 수 있다. 이것을 가능하게하기 위해 가입 디스크램블러와 미가입 디스크램블러의 동기화를 위한 하드웨어가 일부 수정되야 한다. McCormac Hack의 또 다른 방지책으로 스마트 카드와 디스크램블러 사이의 데이타 중에 중요한 것들은 암호화되어 통신되도록하여 결코 키값 즉, 난수발생 초기치의 원래 값대로 스마트 카드와 디스크램블러 사이를 통과하지 못하도록 할 수도 있다.

6. 맺음말

집적회로와 반도체 기술의 발달과 함께 스마트 카드의 가격이 저렴해지면서 암호화 키의 해독뿐만이 아니라 가입자의 시청 자격을 통제하는 기능을 디스크램블러와 분리될 수 있는 스마트 카드에서 행하는 형태의 한정 수신 시스템이 도입되고 있다. 디스크램블러 상자는 매번 서비스 시작시 스마트 카드의 인증에만 관여하고 그밖의 모든 키의 해독이나 시청 자격의 점검은 스마트 카드에서 이루어진다. 그러므로 도시청이 발생해도 스마트 카드를 교체하면서 해독 알고리즘이나 관련 키를 바꿀 수 있어 시스템의 대폭적인 교체없이 도시청을 방지할 수 있다. 그러므로 스마트 카드를 사용한 한정 수신 시스템은 확장성이 좋다. 그러나 아직은 상대적으로 비싼 스마트 카드의 제작비 때문에 여러 프로그램 제공자들이 같은 스마트 카드를 공유한다거나, 스마트 카드의 교체 주기를 상당히 길게 잡고 그 사이 자격정보의 통제는 over-the-air-addressing으로 각 가입자에게 직접 전달된 신호에 의해 통제되도록 한다. 어쨌든 스마트 카드에 의한 한정 수신 방법은 시스템의 확장성을 상당히 유지하므로 최초 도입 가격에 다소 무리가 있더라도 처음부터 스마트 카드에 의한 디스크램블링을 채택할 필요가 있다.

스마트 카드의 도입으로 난수의 복원에 의한 도시청의 발생에 대한 보안이 강화되면서, 도시청자들이 난수발생 초기치의 해독을 포기하고 스크램블링된 영상 신호를 직접 디스크램블링하려는 시도를 할 수 있다. 영상 신호의 공간적 및 시간적 중복성은 이런 시도를 가능케할 수 있으므로 스크램

블링 알고리즘(즉, 데이타 섞음(data shuffling))에 대한 비도를 향상시킬 필요도 있다. 최초의 한정 수신 시스템에 적용된 영상 및 음성의 스크램블링 알고리즘은, 스마트 카드내에 저장된 키의 암호화 알고리즘과는 달리, 그후 계속 사용되어 고정되므로 도시청이 발생하여도 스마트 카드에서처럼 암호화 알고리즘을 쉽게 교체할 수 없고 모든 디스크램블러의 하드웨어를 교체해야 하는 부담을 갖고 있다. 그러므로 최초의 한정 수신 시스템에 가능한 높은 비도의 영상 및 음성 스크램블링(혹은 shuffling) 알고리즘을 채택할 필요가 있다.

참 고 문 헌

[1] FCC 89-104, Notice of Inquiry, Washington DC: Federal Communications Commission, April 1989.

[2] B. Gale and F.Baylin, "Satellite and Calbe TV Scrambling and Descrambling," Baylin/Gale Productions, 1986.

[3] M.Y.Rhee, "Cryptography and Secure Communicatios," McGraw-Hill, Singapore, 1994.

[4] M.Fiat and A.Shamir, "How to prove yourself: practical solution to identification and signature problems," Proc. Crypto 86, Santa Babara, Springer-Verlag, LNCS vol.263, pp.186-199, 1986.

[5] J.Hashkes and M.Cohen, "Managing smart cards for pay television: the VideoCrypt approach," Proc. of First Int. Seminar on Conditional Access for Audiovisual Services, pp.214-224, France, 1990.

[6] F.Baylin, R.Maddox, and J.McCormac, "World Satellite TV and Scrambling Methods," Baylin Publications, 1991.

[7] O. Hansrold, "Eurocrypt-s Smart Card for Mac/Packet Television," Proc. of First Int. Seminar on Conditional Access for Audiovisual Services, pp. 266-272, 1990.

□ 著者紹介

元 致善

1982년 2월 高麗大學校 電子工學科, 學士
1986년 2월 Univ. of Massachusetts, 電氣 및 컴퓨터, 碩士
1990년 2월 Univ. of Massachusetts, 電氣 및 컴퓨터, 博士
1985년 1월 ~ 1989년 10월 Univ. of Massachusetts, 研究助教
1989년 11월 ~ 1992년 8월 金星社, 先任研究員
1992년 9월 ~ 현재 東國大學校 電子工學科 助教授

金 在 功

1961년 3월 漢陽大學校 工科大學 電氣工學科 卒業
1964년 8월 同 大學院 電氣工學科 卒業 (工學 碩士)
1966년 4월 日本國 早稻田 大學 電氣通信科 研究
1970년 3월 ~ 현재 東國大學校 電子工學科 教授1976년 3월 工學博士
1980년 2월 ~ 1990년 2월 英國 Loughborough大學校 電子工學科 研究