(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2010년08월24일
(11) 등록번호 10-0977969
(24) 등록일자 2010년08월18일

(51) Int. Cl.
H04L 9/14 (2006.01)
(21) 출원번호 10-2004-7002713
(22) 출원일자(국제출원일자) 2002년08월23일
심사청구일자 2007년08월09일
(85) 번역문제출일자 2004년02월24일
(65) 공개번호 10-2004-0029023
(43) 공개일자 2004년04월03일
(86) 국제출원번호 PCT/FR2002/002928
(87) 국제공개번호 WO 2003/019899
국제공개일자 2003년03월06일
(30) 우선권주장
01/11078 2001년08월24일 프랑스(FR)
(56) 선행기술조사문헌
KR1020010112428 A
WO2000062540 A1
WO2000062505 A1
전체 청구항 수 : 총 4 항

(73) 특허권자
톰슨 라이센싱
프랑스 92648 블로뉴 세데 께 알퐁스 르 갈로 46
(72) 발명자
안드레우스,장-피에르
프랑스에프-35000레네스뤼데로제닐20
디에흘,에릭
프랑스에프-35340리프레라브자르디에레
두란드,알라인
프랑스에프-35000레네스뤼데디난79
(74) 대리인
백만기, 전경석, 주성민

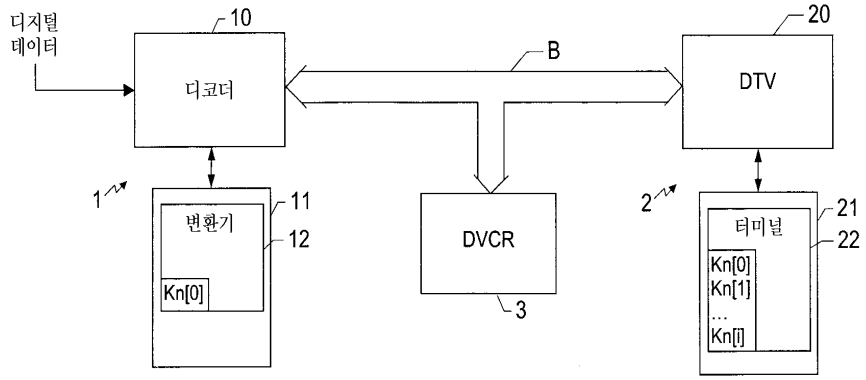
심사관 : 성인구

(54) 네트워크에서의 데이터 전송 및 수신 방법

(57) 요 약

본 발명은 네트워크 상에서 데이터(60)를 방송하는 적어도 하나의 소스 장치(1)와, 데이터(60)를 수신하는 적어도 하나의 수신기 장치(2)를 포함하고, 소스 장치(1)는 네트워크 활성 암호화 키(Kn[0])를 사용하여 네트워크에서 방송되어야 할 데이터를 암호화하고, 수신기 장치(2)는 활성 암호화 키를 사용하여 암호화된 데이터를 해독하기 위한 네트워크 활성 해독 키(Kn[0])와, 네트워크에서 이전에 사용된 암호화 키에 의해 암호화된 데이터를 해독하기 위한 적어도 하나 이상의 네트워크 해독 키(Kn[i])를 포함하는 로컬 디지털 네트워크에 관한 것이다. 또한 본 발명은 이러한 네트워크에 새로운 장치들을 설치하고, 소스 장치로부터 수신기 장치로 데이터를 전송하는 것에 관한 것이다.

대 표 도 - 도1



특허청구의 범위

청구항 1

로컬 디지털 네트워크에 연결된 소스 장치(1)에 의해 데이터를 전송하는 방법으로서,

상기 로컬 디지털 네트워크는 상기 데이터를 수신하기 위한 적어도 하나의 수신기 장치를 더 포함하고, 상기 소스 장치는 네트워크 활성 암호화 키를 포함하며, 상기 수신기 장치는 상기 네트워크 활성 암호화 키를 사용하여 암호화된 데이터를 해독하기 위한 네트워크 활성 해독 키와 상기 로컬 디지털 네트워크의 생성 이래로 사용된 상기 로컬 디지털 네트워크의 모든 해독 키를 포함하고, 상기 소스 장치와 상기 수신기 장치는 암호화 키와 대응하는 해독 키가 동일한 대칭 암호화 처리를 사용하며,

상기 데이터를 전송하는 방법은, 상기 소스 장치에서,

상기 네트워크 활성 암호화 키에 의해 상기 데이터를 암호화하는 단계; 및

상기 네트워크 활성 암호화 키에 적용되는 일방향 함수(one-way function)에 의해 계산된, 상기 네트워크 활성 암호화 키의 지문(fingerprint)과, 상기 암호화된 데이터(611)를 전송하는 단계를 포함하는 것을 특징으로 하는 데이터 전송 방법.

청구항 2

로컬 디지털 네트워크에 연결된 수신기 장치(2)에서 데이터를 수신하는 방법으로서,

상기 로컬 디지털 네트워크는 상기 로컬 디지털 네트워크를 통해 데이터를 방송하기 위한 적어도 하나의 소스 장치를 포함하고,

상기 수신기 장치는 복수의 해독 키를 포함하고, 상기 복수의 해독 키는 네트워크 활성 암호화 키를 사용하여 암호화된 데이터를 해독하기 위한 네트워크 활성 해독 키와 상기 로컬 디지털 네트워크의 생성 이래로 사용된 상기 로컬 디지털 네트워크의 모든 해독 키를 포함하며,

상기 수신기 장치는 상기 복수의 해독 키 각각의 지문을 더 포함하고, 상기 지문은 각각의 해독 키에 적용되는 일방향 함수에 의해 계산되며,

상기 소스 장치와 상기 수신기 장치는 암호화 키와 대응하는 해독 키가 동일한 대칭 암호화 처리를 사용하고,

상기 데이터는 제1항의 데이터 전송 방법에 따라 방송되었으며,

상기 데이터를 수신하는 방법은,

수신된 데이터로부터 지문을 추출하는 단계;

상기 추출된 지문을 상기 수신기 장치에 포함된 해독 키들의 지문들과 비교하는 단계; 및

상기 추출된 지문과 상기 수신기 장치에 저장된 지문들 중 하나가 동일한 경우에, 상기 지문에 대응하는 해독 키에 의해 상기 데이터를 해독하는 단계를 포함하는 것을 특징으로 하는 데이터 수신 방법.

청구항 3

로컬 디지털 네트워크에 연결된 소스 장치에 의해 데이터를 전송하는 방법으로서,

상기 로컬 디지털 네트워크는 상기 데이터를 수신하기 위한 적어도 하나의 수신기 장치를 더 포함하고, 상기 소스 장치는 네트워크 활성 암호화 키를 포함하며, 상기 수신기 장치는 상기 네트워크 활성 암호화 키를 사용하여 암호화된 데이터를 해독하기 위한 네트워크 활성 해독 키와 상기 로컬 디지털 네트워크의 생성 이래로 사용된 상기 로컬 디지털 네트워크의 모든 해독 키를 포함하는 복수의 해독 키를 포함하고,

상기 데이터를 전송하는 방법은,

(a) 상기 데이터의 제1 부분에 일방향 함수를 적용시키는 단계;

(b) 단계 (a)에서 수행된 계산 결과와 보호되어야 할 상기 데이터의 제2 부분을 상기 네트워크 활성 암호화 키에 의해 암호화하는 단계; 및

(c) 단계 (b)에서 암호화된 데이터와 상기 데이터의 제1 부분을 상기 로컬 디지털 네트워크를 통해 전송하는 단계를 포함하는 것을 특징으로 하는 데이터 전송 방법.

청구항 4

로컬 디지털 네트워크에 연결된 수신기 장치에서 데이터를 수신하는 방법으로서,

상기 로컬 디지털 네트워크는 상기 로컬 디지털 네트워크를 통해 데이터를 방송하기 위한 적어도 하나의 소스 장치를 포함하고, 상기 소스 장치는 상기 로컬 디지털 네트워크에서 방송되어야 할 데이터를 암호화하기 위하여 네트워크 활성 암호화 키를 사용할 수 있으며, 상기 수신기 장치는 상기 네트워크 활성 암호화 키를 사용하여 암호화된 데이터를 해독하기 위한 네트워크 활성 해독 키와 상기 로컬 디지털 네트워크의 생성 이래로 사용된 상기 로컬 디지털 네트워크의 모든 해독 키를 포함하는 복수의 해독 키를 포함하고, 상기 데이터는 제3항의 데이터 전송 방법에 따라 방송되었으며,

상기 데이터를 수신하는 방법은,

(a) 상기 데이터의 암호화되지 않은 제1 부분에 일방향 함수를 적용시키는 단계;

(b) 상기 수신기 장치에 포함된 상기 복수의 해독 키 중 하나에 의해 상기 데이터의 제2 부분을 해독하는 단계; 및

(c) 단계 (b)에서 해독된 데이터의 적어도 일부분의 해독 결과를 단계 (a)에서 수행된 계산 결과와 비교하여, 동일한 경우에는 단계 (b)에서 해독된 데이터의 나머지 부분을 복구하고, 상이한 경우에는 단계 (b)로 돌아가 상기 수신기 장치에 포함된 상기 복수의 해독 키 중 다른 해독 키에 의해 상기 데이터의 제2 부분의 해독을 수행하는 단계를 포함하는 것을 특징으로 하는 데이터 수신 방법.

청구항 5

삭제

청구항 6

삭제

청구항 7

삭제

청구항 8

삭제

청구항 9

삭제

청구항 10

삭제

청구항 11

삭제

청구항 12

삭제

청구항 13

삭제

명 세 서

기 술 분 야

[0001] 본 발명은 일반적으로 로컬 디지털 네트워크 분야에 관한 것으로, 특히 가정내의 디지털 네트워크(domestic digital network) 분야에 관한 것이다. 보다 구체적으로는, 이와 같은 네트워크 상에서 흐르는 디지털 데이터의 복제를 방지하는 것과 관련되어 있다.

배 경 기 술

[0002] 이와 같은 네트워크는, 예컨대 IEEE 1394 표준에 따른 버스와 같은 디지털 버스에 의해 서로 연결되는 장치들의 집합으로 구성된다. 이것은 특히 두가지 유형의 장치, 즉 네트워크를 통해 데이터를 전송할 수 있는 소스 장치(이러한 장치는 상기 네트워크와는 별개의(external) "채널"로부터의 데이터를 복구할 수 있음)와, 데이터를 처리하거나 사용자에게 제공하기 위해 네트워크를 통해 흐르는 데이터를 수신하기에 적합한 수신기 장치를 포함한다.

[0003] 따라서, 오디오 및/또는 비디오 데이터를 집안의 여러 방들로 전달하기 위한 가정내의 디지털 네트워크를 예로 들자면, 소스 장치는, 예컨대 위성 안테나 또는 케이블 접속을 통하여 상기 네트워크의 외부로부터 비디오 프로그램을 수신하는 디지털 디코더, 또는 상기 네트워크 상으로 디스크로부터 판독된 (오디오 및/또는 비디오) 데이터를 디지털 형태로 전송하는 기타 광 디스크 판독기(이 경우 디스크는 네트워크의 외부로부터 생성된 데이터를 포함함)일 수 있다. 수신기 장치는, 예를 들어, 상기 네트워크로부터 수신된 비디오 프로그램을 시청할 수 있도록 해 주는 텔레비젼 수상기, 또는 보다 일반적으로는 암호화된 데이터를 해독하는 능력을 가진 임의의 형태의 응용장치이다.

[0004] 로컬 네트워크의 외부로부터 생성된 데이터를 제공하는 콘텐트 제공자, 특히 예를 들어, 유료-TV 프로그램을 전송하는 서비스 제공자 또는 기타 광 디스크 발매자의 관점에서 볼 때, 이러한 전송된 데이터가 복제되어 하나의 로컬 네트워크에서 다른 로컬 네트워크로 (예컨대, 광 디스크 또는 그 외의 임의의 기록 매체로 복제됨으로써) 손쉽게 유출되는 것을 방지하는 것이 필요하다.

[0005] 이를 위하여, 데이터를 수신하도록 권한을 부여받은 장치에 미리 알려진 키들, 또는 콘텐트 제공자와 이러한 장치 사이의 특정 보안 프로토콜에 따라 교환되는 키들을 사용하는 암호화 알고리즘에 의해 데이터를 암호화함으로써, 암호 형태로 데이터를 전송하는 기술이 알려져 있다.

[0006] 톰슨 멀티미디어의 명의로 1999년 4월 13일에 출원되어, FR-A-2 792 482로 공개된 프랑스 특허출원은, 가정내 네트워크 장치 사이, 통상적으로 전술한 소스 장치로부터 수신기 장치로 흐르는 데이터를 암호화하기 위하여, 그 네트워크에 특정된 공개키(public key)를 사용하는 가정내 네트워크에 관한 것이다. 상기 네트워크의 수신기 장치만이 위 공개키에 대응하는 비밀키(private key)를 갖게 된다. (공개키, 비밀키) 쌍은 상기 네트워크에 대하여 특정되어 있으므로, 이러한 네트워크의 구조 내에서 암호화된 데이터는 다른 네트워크의 장치들에 의해 해독될 수 없다.

[0007] 톰슨 라이센싱 S.A.의 명의로 2001년 4월 25일 출원된 프랑스 특허출원번호 01 05568는, 전술한 바와 같이 기본적으로 대칭키를 이용하는 네트워크에서 키를 관리하는 방법과 부분적으로 관련이 있다. 소스 장치는 매우 자주 갱신되는 제1 대칭 키에 의해 데이터를 암호화하고, 네트워크에 특정된 제2 대칭키에 의해 암호화된 형태로 제1 대칭키를 상기 네트워크의 다른 장치들로 전송한다. 제2 대칭키는 수신기 장치들이 보유하게 된다.

[0008] 전술한 2가지 방법에 있어서, 데이터는 네트워크에 특정된 하나의 동일한 암호화 키 (또는 하나의 동일한 공개키/비밀키 쌍) 및 하나의 동일한 암호화 알고리즘에 의하여 보호된다. 하지만, 사용되는 암호화 알고리즘 및/또는 키를 갱신할 필요가 종종 있는데, 특히 암호화 알고리즘이 매우 짧은 키를 사용하는 경우, 또는 키의 길이와는 상관없이 길이가 더 긴 키 또는 보다 강력한 암호화 알고리즘을 사용하기 위하여 더 이상 안전하지 않은 경우에 더욱 필요하다. 불행하게도, 이와 같은 경우에, 네트워크에서 이전에 기록된 데이터는 새로운 키 및/또는 새로운 암호화 알고리즘을 가지고는 더 이상 해독될 수 없을 수도 있다.

발명의 상세한 설명

[0009] 본 발명의 대상은, 네트워크 상에서 데이터를 방송하기 위한 적어도 하나의 소스 장치와, 상기 데이터를 수신하기 위한 적어도 하나의 수신기 장치를 포함하는 로컬 디지털 네트워크이다.

[0010] 본 발명에 따르면, 소스 장치는 네트워크에서 방송되어야 할 데이터를 암호화하기 위하여 네트워크 활성 암호화 키(network active encryption key)를 사용하며, 수신기 장치는 상기 활성 암호화 키를 이용하여 암호화된 데이터를 해독하기 위한 네트워크 활성 해독 키(network active decryption key)와, 상기 네트워크에서 이전에 사용된 암호화 키에 의해 암호화된 데이터를 해독하기 위하여 적어도 하나의 다른 네트워크 해독 키를 갖는다.

[0011] 로컬 디지털 네트워크는 또한 하나 이상의 다음과 같은 특징들을 포함할 수 있다.

[0012] - 수신기 장치는 네트워크의 생성 이래로 이전에 사용된 네트워크의 모든 해독 키를 포함한다.

[0013] - 소스 장치는 네트워크 활성 암호화 키를 포함하고, 네트워크에서 방송되어야 할 데이터를 네트워크의 활성 키로 암호화한다.

[0014] - 소스 장치는 제1 대칭키와, 네트워크 활성 암호화 키로 암호화된 제1 대칭키도 포함하고, 네트워크에서 방송되어야 할 데이터를 제1 대칭키로 암호화하며, 네트워크 활성 암호화 키로 암호화된 제1 대칭키를 암호화된 데이터와 함께 전송하도록 구축된다.

[0015] - 소스 장치 및 수신기 장치는 대칭 암호화 기법을 사용하며, 네트워크에서 사용되는 암호화 키 및 이에 대응하는 해독 키는 동일하다.

[0016] 본 발명은 또한 전술한 바와 같이 적어도 하나의 수신기 장치를 이미 포함하는 로컬 디지털 네트워크에 새로운 수신기 장치를 설치하는 방법에 관한 것이다. 이 방법에 따르면, 네트워크 활성 해독 키와, 네트워크에서 이전에 사용된 적어도 하나의 해독 키를 갖고, 안전한(secure) 방법으로 키들을 전송할 수 있는 네트워크의 기존 수신기 장치가 이러한 해독 키들을 새로운 수신기 장치에 전송한다.

[0017] 본 발명의 다른 형태는, 전술한 바와 같이 소스 장치 및 수신기 장치가 대칭 암호화 기법을 사용하고, 네트워크에서 사용되는 암호화 키 및 이에 대응하는 해독 키가 동일한 로컬 디지털 네트워크에서 새로운 소스 장치를 설치하는 방법에 관한 것이다. 이 방법에 따르면, 네트워크 활성 암호화/해독 키와, 네트워크에서 이전에 사용된 적어도 하나의 암호화/해독 키를 갖고, 안전한 방법으로 키들을 전송할 수 있는 네트워크의 기존 수신기 장치가 네트워크 활성 암호화/해독 키를 새로운 소스 장치에 전송한다.

[0018] 본 발명은 또한 전술한 바와 같이 사용되는 암호화 키들과 해독 키들이 동일한 네트워크에 연결된 소스 장치에 의해 데이터를 전송하는 방법에 관한 것이다. 이 방법은, 네트워크 활성 암호화/해독 키에 의해 데이터를 암호화하는 단계와, 상기 암호화된 데이터를 활성 키의 지문(fingerprint)(이 지문은 네트워크의 활성 키에 적용되는 일방향 함수(one-way function)에 의해 산출됨)과 함께 전송하는 단계를 포함한다.

[0019] 본 발명은 또한 전술한 네트워크에 연결된 수신기 장치에서 암호화된 데이터를 수신하는 방법에 관한 것으로, 이 데이터는 전술한 방법에 따라 방송된 것이고, 수신기 장치는 자신이 갖고 있는 각각의 암호화/해독 키에 대하여 그 키에 적용된 일방향 함수에 의해 산출된 지문을 더 포함한다. 이 방법은 수신된 데이터로부터 키의 지문을 추출하는 단계와, 추출된 지문을 수신기 장치에 포함된 암호화/해독 키들에 대한 지문과 비교하는 단계와, 추출된 지문과, 수신기 장치에 저장된 지문 중 어느 하나가 동일한 경우 이 지문에 대응하는 키로 데이터를 해독하는 단계를 포함한다.

[0020] 본 발명은 또한 전술한 네트워크에 연결된 소스 장치에 의해 데이터를 전송하는 또 다른 방법에 관한 것이다. 이 방법은, (a) 일방향 함수를 데이터의 제1 부분에 적용하는 단계와, (b) 단계 (a)에서 수행된 계산 결과와 보호되어야 할 데이터의 제2 부분을 네트워크 활성 암호화 키에 의해 암호화하는 단계와, (c) 데이터의 제1 부분과 단계 (b)에서 암호화된 데이터를 네트워크 상에서 전송하는 단계를 포함한다.

[0021] 본 발명은 또한 전술한 네트워크에 연결된 수신기 장치에서 상술한 방법에 따라 방송된 데이터를 수신하는 방법에 관한 것이다. 이 방법은, (a) 일방향 함수를 암호화되지 않은 데이터의 제1 부분에 적용하는 단계와, (b) 수신기 장치에 포함된 네트워크 해독 키에 의해 데이터의 제2 부분을 해독하는 단계와, (c) 단계 (b)에서 해독된 데이터의 일부분에 대한 해독 결과를 단계 (a)에서 수행된 계산 결과와 비교하여, 동일한 경우에는 단계 (b)에서 해독된 데이터의 나머지 부분을 복구하는 단계와 상이한 경우에는 단계 (b)로 돌아가, 수신기 장치에 포함된 다른 네트워크 해독 키에 의해 데이터의 제2 부분의 해독을 수행하는 단계를 포함한다.

[0022] 본 발명은 또한 전술한 네트워크에 연결된 소스 장치에 의해 데이터를 전송하는 제3의 방법에 관한 것이다. 이 방법은, 네트워크 활성 암호화 키에 의해 데이터를 암호화하는 단계와 상기 네트워크 활성 키에 대응하는 인덱스와 더불어 암호화된 데이터를 전송하는 단계를 포함한다.

[0023] 전술한 바와 같은 네트워크에 연결된 수신기 장치에서 전술한 방법에 따라 방송된 데이터를 수신하는 방법은, 데이터를 암호화하는데 사용되는 네트워크 암호화 키에 대응하는 인덱스를 수신된 데이터로부터 추출하는 단계와, 이 인덱스로부터 대응하는 네트워크 해독 키를 유도하는(deducing) 단계와, 해독 키에 의해 데이터를 해독하는 단계를 포함한다.

[0024] 본 발명의 다른 특징 및 장점은, 첨부된 도면에 의해 명확히 표현되고, 한정하고자 하는 것이 아닌 여러 특정 실시예에 대한 상세한 설명을 통하여 명백해질 것이다.

실 시 예

[0027] 도 1에 보다 상세한 설명을 위해 참조될 수 있는, 전술한 특허 출원(톰슨 멀티미디어 명의의 출원 FR-A-2 792 482와 톰슨 라이센싱 S.A 명의의 출원 FR No. 01 05568)에서 설명된 원리를 이용하여 데이터의 복제를 방지하는, 예시적인 가정내의 디지털 네트워크를 개략적으로 나타내었다.

[0028] 이 네트워크는 소스 장치(1), 수신기 장치(2) 및 기록 장치(3)를 포함하고, 이들은 예를 들어 IEEE 1394 표준에 따른 버스인 디지털 버스(B)에 의해 함께 연결된다.

[0029] 소스 장치(1)는 스마트 카드(11)를 수용하는 스마트 카드 판독기가 구비된 디지털 디코더(10)를 포함한다. 이 디코더는 디지털 데이터, 특히 서비스 제공자에 의해 제공되는 오디오/비디오 프로그램을 수신한다.

[0030] 수신기 장치(2)는 스마트 카드(21)를 수용하는 스마트 카드 판독기가 구비된 디지털 텔레비젼 수상기(DTV; 20)를 포함하고, 기록 장치(3)는 특히 디지털 비디오 레코더(DVCR)이다.

[0031] 소스 장치(1)를 통해 네트워크에 진입하는 디지털 데이터는 일반적으로 유료-TV의 원리에 따라 스크램블된(scrambled) 데이터이다. 이 데이터는, 암호화 키 K에 의해 암호화된 형태로 데이터 스트림 내에 전송되면서, 제어 메시지(Entitlement Control Message; ECM)에 포함되는 제어 워드들(control words; CW)에 의해 스크램블된다. 암호화 키 K는, 데이터를 수신하기 위해 요금을 지불한 사용자들에게, 특히 스마트 카드에 저장됨으로써 사용할 수 있게 된다. 도 1의 예에서, 스마트 카드(11)가 이러한 키 K를 포함하는 것으로 가정한다.

[0032] 이러한 스크램블된 디지털 데이터를 수신하는 소스 장치(1)는, 다음으로 데이터를 가공하여(shape) 디지털 네트워크 상에서 방송한다. 이를 위해, 키 K에 의해 암호화된 제어 워드들을 포함하는 ECM 메시지들은 스마트 카드(11)에 포함된 변환기 모듈(12)에 의해 해독된 제어 워드들을 포함하는 LECM 메시지들(Local Entitlement Control Message)로 변환되고, LECM 메시지들은 가정내의 로컬 네트워크에 특정된 키에 의해 보호된다.

[0033] 따라서, 네트워크을 통해 흐르는 데이터는 도 2에 도시된 바와 같이 패킷(60)으로 구성된다. 이 패킷(60)은 스크램블된 데이터(62)와 LECM 메시지(61)를 포함한다. LECM 메시지는,

[0034] - 평문 데이터, 즉, 암호화되지 않은 데이터를 포함하는 부분(610)(이 부분은 특히 LECM 메시지의 크기와 복제 방지 시스템의 버전 번호 등을 갖는 패킷 헤더들일 수 있음) 및

[0035] - 보호되는 데이터, 특히 제어 워드들(CW)을 포함하는 부분(611)

[0036] 의 두 부분을 포함한다.

[0037] 다음으로, 단순화를 위해, LECM 메시지의 부분(611)에서 보호되는 데이터는 네트워크 Kn의 비밀 키(또는 대칭 키)에 의해 암호화된다. 그러나, 본 발명은 또한 키들을 관리하기 위해 더욱 복잡한 시스템이 사용되는 경우, 예를 들면, 전술한 톰슨 라이센싱 S.A 명의의 출원 FR No. 01 05568에서와 같이 변형되어 이용된다. 이러한 변형은 후술되는 실시예에서 보다 간략히 설명될 것이다.

[0038] 패킷(60)과 같은 데이터 패킷들은 수신기 장치(2)에 의해 수신되고, 이 수신기 장치는 스마트 카드(21)의 터미널 모듈(22) 내에서 LECM 메시지들을 처리한다. 터미널 모듈(22)은 네크워트 Kn의 비밀 키를 포함하므로, LECM 메시지들에서 보호되는 부분을 해독할 수 있다. 이렇게 해독된 메시지들의 내용에 의해, 수신기 장치는 "유용한" 데이터(62)를 스크램블하는데 사용된 제어 워드들(CW)을 복구하므로, 이러한 데이터를 역스크램블(descramble)하여 이를 사용자에게 제공할 수 있다.

[0039] 스크램블된 데이터를 포함하는 패킷(60)의 형태로 기록될 데이터를 기록 장치(3)가 수신한다는 것을 알아야 한다.

[0040] 물론 가정내의 로컬 네트워크는 몇개의 소스 장치들, 몇개의 수신기 장치들 및 몇개의 기록 장치들을 포함할 수 있다. 이 경우에, 소스 장치들의 모든 변환기들이 네크워크의 비밀 키 Kn을 포함하여 LECM 메시지들을 생성하

여야 하고, 수신기 장치들의 모든 터미널들은 키 Kn을 포함하여 LECM 메시지들에서 보호되는 부분을 해독하여야 한다.

[0041] 또한, 가정내의 디지털 네트워크는 차츰 발전할 수 있다. 따라서, 사용자는 네트워크에 장치들을 추가하거나 네트워크로부터 장치들을 제거할 수 있다. 특히 시스템의 보안 체계가 위협받을 때, 네트워크 Kn의 키를 변경하거나, 새로운 암호화 알고리즘을 사용하는 것이 필요할 수 있다.

[0042] 본 발명의 실시예에 따르면, 수신기 장치의 각각의 터미널 모듈은 가정내의 디지털 네트워크의 생성 이래로 사용되어 온 키들 Kn[i]을 보유한다. 이들 중에, 하나의 키가 "활성화"되면, 이후 이것은 Kn[0]로 지칭될 것이다. 한편, 소스 장치들의 변환기 모듈들은 이러한 활성 네트워크 키 Kn[0]만을 포함한다.

[0043] 따라서, 네트워크에서 초기에 기록된 데이터는, 네트워크의 생성 이래로 LECM 메시지들을 암호화하는데 사용되었던 모든 키들을 보유하는 수신기 장치들에 의해 계속 판독될 수 있다. 이들에 관한 한, 네트워크에 진입하는 새로운 데이터에 대하여 LECM 메시지들을 생성하기 위해, 소스 장치들은 활성 키 Kn[0]만을 필요로 한다.

[0044] 이점과 관련해서, 네트워크에 진입하는 디지털 데이터는 반드시 전술한 형태(ECM 메시지들 내에서 암호화된 형태로 포함된 제어 워드들에 의해 스크램블된 데이터)일 필요는 없으나, 소스 장치가 네트워크의 외부로부터 데이터를 수신하는 형태에 관계없이, 도 2에 나타낸 패킷들의 형태로 네트워크 상으로 데이터를 전송한다는 것을 알아야 한다. 필요하다면, 소스 장치는 제어 워드들을 생성하고, LECM 메시지의 보호된 부분으로 데이터를 전송하기 전에, 이러한 제어 워드들에 의해 데이터를 스크램블한다.

[0045] 이상 살펴본 바와 같이, 모든 수신기 장치들은 (그들의 터미널 모듈에) 모든 키들 Kn[i]을 보유한다. 새로운 수신기 장치가 네트워크에 연결되면, 그 수신기 장치는 네트워크의 특정 수신기 장치로부터 이러한 모든 키들을 수신하는데, 이 특정 수신기 장치는 프로제니터(progenitor)라 하며, 어느 키가 활성화된 것인지를 지시한다.

[0046] 각각의 수신기 장치는, 실제 버진(Virgin), 프로제니터(Progenitor) 또는 스테릴(Sterile)의 상태들 중 어느 하나일 수 있다.

[0047] 버진 수신기 장치는, 네트워크 Kn[i]의 키들을 포함하지 않는 장치로 정의된다. 이는 통상적으로 아직 네트워크에 연결되지 않은 장치이다. 이는 수신기 장치의 디폴트(default) 상태를 말한다.

[0048] 스테릴 장치는 네트워크 Kn[i]의 키들을 보유하지만, 이들을 다른 장치에 전송할 수 없는 장치로 정의된다.

[0049] 프로제니터 장치는 네트워크 Kn[i]의 키들을 보유하고, 이들을 네트워크의 다른 장치들에 전송할 수 있는 장치로 정의된다. 네트워크에는 하나의 프로제니터 장치만이 존재한다.

[0050] 수신기 장치의 상태는, 예컨대 수신기 장치의 터미널 모듈(22) 내에 위치한 레지스터(register)와 같은 상태 지시자에 저장된다.

[0051] 새로운 네트워크를 생성하는 방식과, 새로운 장치들이 네트워크에 연결될 때 장치들 사이에서 키들을 교환하는 방식에 관한 자세한 설명은, 전술한 특허 출원(톰슨 멀티미디어 명의의 출원 FR-A-2 792 482와 톰슨 라이센싱 S.A 명의의 출원 FR No. 01 05568)에서 찾아볼 수 있다.

[0052] 새로운 소스 장치가 네트워크에 연결되면, 프로제니터 수신기 장치는 이 장치로 활성 네트워크 키 Kn[0]만을 전송한다. 키 Kn[0]는 그 후 새로운 소스 장치의 변환기 모듈 내에 저장된다. 키들을 관리하기 위해 더욱 복잡한 시스템을 사용하는 변형된 실시예에서, 소스 장치는 활성 네트워크 키 자체가 아니라 이 키에 기초한 정보 항목을 수신한다. 보다 구체적으로는, 전술한 출원 FR No. 01 05568에 설명되어 있는 바와 같이, 새로운 소스 장치는 대칭 암호화 키 Kc를 생성하는데, 이 대칭 암호화 키는 이후 LECM 메시지에서 보호되는 데이터를 암호화하기 위해 사용된다. 소스 장치는 이 대칭 키 Kc를 네트워크의 프로제니터 장치로 보안 방식으로 전송하는데, 이 프로제니터 장치는 상기 키 Kc를 활성 네트워크 키 Kn[0]로 암호화하여 소스 장치로 되돌려 준다. 새로운 소스 장치는 그 후 이러한 암호화 $E_{kn[0]}(Kc)$의 결과를 자신의 변환기 모듈에 저장한다. 이 새로운 수신기 장치가 그 후 네트워크 상에서 데이터를 전송할 때, 수신기 장치는 LECM 메시지들에서 암호화되지 않은 부분(610)에 활성 네트워크 키 Kn[0]와 함께, 대칭 키 Kc가 암호화된 $E_{kn[0]}(Kc)$를 포함한다.

[0053] 수신기 장치가, 스크램블된 데이터와 LECM 메시지를 각각 포함하는 패킷(60)의 형태로 전송된 데이터를 수신하여 사용자에게 제공하면, 수신기 장치는 우선 LEMC 메시지의 데이터를 암호화하는데 사용된 키 Kn[i]를 결정해야만 한다.

[0054] 이것은 수신기 장치의 터미널 모듈 내에 저장된 모든 키들에 대하여 빠짐없이 시도하거나(이하 설명되는 실시예 B), 또는 인덱스를 사용하거나(이하 설명되는 실시예 C), 또 한편, 선호되는 것으로서 LECM 메시지에 포함된 키 지문들을 사용하여(이하 설명되는 실시예 A) 수행될 수 있다.

[0055] [실시예 A] 지문을 사용함

[0056] 이 실시예에서, 각각의 수신기 장치는, 자신의 터미널 모듈 내에 저장되는 이하의 표 1과 같은 표를 포함하는 것으로 가정한다.

[0057] - "키" 열은 (네트워크에서 활성화되었었거나 활성화되어 있는) 네트워크의 N개의 비밀 키 각각을 포함하며, 활성화된 네트워크 키는 키 Kn[0]이다. 이러한 키를 포함하는 필드는 고정된 크기를 가지며, 이는 추후의 키 크기 변경에 대비하도록 충분히 큰 크기이지만, 저장된 키들은 필드의 크기보다 작은 크기를 가질 수 있다.

[0058] - "H(키)" 열은 키 Kn[i] 각각에 적용된 일방향 함수 H의 결과를 포함하며, 여기에는 해시 함수 SHA-1이 사용되는 것이 바람직하다.

[0059] - "@처리_함수(processing_function)" 열은 터미널 모듈을 포함하는 스마트 카드에 내장된 소프트웨어 내에 포함된 처리 함수에 대한 포인터를 포함한다.

표 1

[0060]

키	H(키)	@처리_함수
Kn[0]	H(Kn[0])	@처리_함수[0]
...	...	...
Kn[i]	H(Kn[i])	@처리_함수[i]
...	...	...
Kn[N]	H(Kn[N])	@처리_함수[N]

[0061] 이 실시예에 따르면, 새로운 소스 장치가 네트워크에 연결되는 경우, 프로제니터 수신기 장치는 그 소스 장치에 활성 네트워크 키 Kn[0]을 전송한다. 키 Kn[0]은 소스 장치의 변환기 모듈 내에 저장되며, 변환기 모듈은 전술한 일방향 함수 H에 의해 그 키의 지문 H(Kn[0])를 계산한다.

[0062] 따라서, 네트워크의 소스 장치의 모든 변환기 모듈은 키 Kn[0]과 이것의 지문 H(Kn[0])를 보유한다.

[0063] 소스 장치의 변환기 모듈이 새로운 데이터를 네트워크 상에서 전송하기 위하여 새로운 LECM 메시지를 생성해야 하는 경우, 상기 모듈은 활성 키 Kn[0]을 사용하여 LECM 메시지에서 보호되는 부분의 데이터를 암호화하고(특히 제어 워드 CW를 암호화함), 상기 활성 키의 지문 H(Kn[0])를 암호화되지 않은 데이터를 포함하는 LECM 메시지의 일부분 내에 삽입한다.

[0064] 키를 관리하기 위한 더욱 복잡한 시스템을 이용하는 변형 실시예에서는, 소스 장치가 활성 네트워크 키 Kn[0] 자체를 수신하는 대신, 그 키에 기초한 정보 항목 $E_{Kn[0]}(Kc)$을 수신한다. 실시예 A에 따르면, 이 소스 장치는 활성 키의 지문 H(Kn[0])를 더 수신하며, 이를 자신의 변환기 모듈 내에 저장한다. 변환기 모듈이 새로운 LECM 메시지를 생성하는 경우, 변환기 모듈은 보호될 부분의 데이터를 대칭 암호화 키 Kc로 암호화하며, 활성 키 Kn[0]에 의해 키 Kc를 암호화한 것과 활성 키의 지문 H(Kn[0])를 LECM 메시지의 암호화되지 않은 부분 내에 삽입한다.

[0065] 네트워크가 시간에 따라 차츰 발전되고 새로운 키가 활성 네트워크 키로서 사용됨에 따라, 네트워크 내에 기록된 데이터는, 활성 네트워크 키로서 순차적으로 사용되었던 다양한 키로 암호화된 LECM 메시지를 포함한다.

[0066] 사용자가 이전에 기록된 데이터를 수신기 장치 상에서 재생하고자 하는 경우, 수신기 장치의 터미널 모듈은 표 1에 저장된 적합한 키를 사용하여 해독해야 하는 LECM 메시지를 수신한다. 이를 위해, 터미널 모듈은 우선 LECM 메시지의 암호화되지 않은 부분으로부터 LECM 메시지에서 보호되는 부분의 데이터를 암호화하는데 사용된 키의 지문 H(Kn[j])를 추출한다. 그 후 이 지문 H(Kn[j])를 표 1에 저장된 모든 지문과 비교하여 어떤 값이 그에 대응하는 경우, 어드레스 @처리_함수[j]에 위치한 함수를 호출함으로써, 키 Kn[j]에 의해 LECM 메시지에서 보호되는 부분의 해독을 수행한다.

[0067] 반대로 표 1에서 어느 지문도 대응하지 않는 경우, 이는 수신된 데이터가 가정내의 네트워크에서 기록된 것이

아님을 의미한다. 따라서, LECM 메시지는 해독될 수 없으며, 대응하는 데이터는 역스크램블될 수 없다.

[0068] 여기서 주목해야 할 점은, 사용되는 다양한 처리 함수는 상이한 암호화 알고리즘을 사용할 수 있을 뿐만 아니라, 데이터에 대하여 상이한 처리도 수행할 수 있다는 점이다.

[0069] 예컨대, 변형 실시예에서 전술한 바와 같이 대칭 키 Kc에 의해 LECM 메시지에서 보호되는 부분이 암호화된 경우, 처리 함수는 우선 LECM 메시지의 암호화되지 않은 부분으로부터 추출된 정보 항목 $E_{Kn[0]}(Kc)$의 해독을 수행함으로써, 그 키 Kc로 보호된 데이터를 해독하기에 앞서 키 Kc를 복구한다.

[0070] [실시예 B] 키들에 대한 규칙적인 시도

[0071] 이 실시예에 따르면, 수신기 장치의 터미널 모듈 각각은 네트워크 생성 이래로 그곳에서 사용되어 온 키 Kn[0], ... , Kn[i], ... , Kn[N]의 목록을 포함한다.

[0072] 소스 장치의 변환기 모듈 각각은 활성 네트워크 키 Kn[0]을 포함한다. 상기 모듈이 LECM 메시지를 생성해야 하는 경우, 변환기는 키 Kn[0]으로 보호될 데이터를 암호화한다. 이는 또한 LECM 메시지의 암호화되지 않은 부분의 전부 또는 일부에 대한 일방향 함수의 결과, 특히 "CRC"(Check Redundancy Code)를 계산하며, 이 CRC를 Kn[0]으로 암호화하는 바, 이러한 암호화의 결과는 LECM 메시지에서 보호되는 부분 내에 삽입된다.

[0073] 수신기 장치의 터미널 모듈이 해독될 LECM 메시지를 수신하는 경우, 상기 모듈은 LECM 메시지에서 보호되는 부분에 포함된 데이터의 해독을 터미널 모듈에 저장된 각각의 키 Kn[i]에 의해 규칙적으로 수행한다. 이는 또한 LECM 메시지의 암호화되지 않은 부분에 포함된 데이터로부터 CRC를 계산하며, 이 후 CRC의 해독 결과 각각을 암호화되지 않은 데이터로부터 계산된 것과 비교한다. 결과가 동일하면, 이는 해독에 사용된 키가 LECM 메시지를 암호화하는데 사용된 키라는 것을 의미한다.

[0074] 따라서, 터미널 모듈은 LECM 메시지에서 보호되는 데이터(제어 워드 포함)를 복구할 수 있고, 데이터를 역스크램블하여 이를 사용자에게 제공할 수 있게 된다.

[0075] 키들을 관리하기 위한 더욱 복잡한 시스템을 갖는 상술한 변형 실시예가 이용되는 경우, 소스 장치의 변환기 모듈은 LECM 메시지에서 보호될 데이터(CRC의 결과를 포함)를 대칭 키 Kc로 암호화하며, 활성 네트워크 키 Kn[0]에 의해 키 Kc를 암호화한 것을 LECM 메시지의 암호화되지 않은 부분 내에 삽입한다.

[0076] 이러한 LECM 메시지를 수신하는 수신기 장치의 터미널 모듈은 전술한 것과 동일한 동작을 수행하지만, 여기에 부가적인 단계가 더해진다. 즉, 상기 모듈은 우선 LECM 메시지의 암호화되지 않은 부분으로부터 추출된 항목 $E_{Kn[j]}(Kc)$의 해독을 제1 키 Kn[i]에 의해 수행함으로써 가정 키(assumed key) Kc를 복구한다. 이 후, LECM 메시지에서 보호되는 부분을 그 키 Kc로 해독하려는 시도를 한다. 키 Kn[i]가 키 Kc를 암호화하는데 사용된 키에 대응하는 경우, 데이터의 보호된 부분으로부터 얻은 CRC는 데이터의 암호화되지 않은 부분에 대하여 계산된 CRC에 대응하게 된다. 그렇지 않으면, 터미널 모듈은 계속 다른 키 Kn[i+1]을 시도한다.

[0077] [실시예 C] 인덱스를 이용함

[0078] 이 실시예에 따르면, 수신기 장치의 터미널 모듈 각각은 "키_스페이스(Key_space)"라 불리는 큰 크기의 난수(random number)를 보유한다. 이 수는 시스템의 초기화 시에, 예컨대 터미널 모듈을 포함하는 스마트 카드를 만들때 생성되는 것이 바람직하다.

[0079] 네트워크에서 사용되는 일련의 키들 Kn[i] 모두가 이러한 난수 키_스페이스로부터 추출된다.

[0080] - 키 각각은 난수 키_스페이스의 부분집합을 나타내거나,

[0081] - 그렇지 않을 경우 키 각각은 난수 키_스페이스에 기초하여, 또는 그 난수의 일부에 기초하여 수행되는 계산의 결과이다.

[0082] 이 실시예에서, 수신기 장치 각각은 자신의 터미널 모듈 내에 저장된 이하의 표 2와 같은 표를 포함하는 것으로 가정되는 바, 이 표는 인덱스들을 포함하며, 또한 각각의 인덱스에 대하여 터미널 모듈을 포함하는 스마트 카드에 내장된 소프트웨어 내에 포함된 처리 함수에 대한 포인터를 포함한다.

표 2

[0083]

인덱스	@처리_함수
[0]	@처리_함수[0]
...	...
[i]	@처리_함수[i]
...	...
[N]	@처리_함수[N]

[0084] 표 2의 인덱스 각각은 상이한 키 Kn[i]를 사용하는 것에 대응하며, 어드레스 @처리_함수[i]에 위치한 처리 함수는 난수 키_스페이스에 기초하여 이러한 키를 추출하는 것을 가능하게 한다.

[0085] 소스 장치 내에 위치한 변환기 모듈은 활성 네트워크 키 Kn[0] 및 대응하는 인덱스 [0]을 포함한다. 상기 모듈이 LECM 메시지를 생성하는 경우, 키 Kn[0]을 사용하여 보호될 부분의 데이터를 암호화하고, LECM 메시지의 암호화되지 않은 부분에 상기 인덱스 [0]을 삽입한다.

[0086] 따라서, 터미널 모듈이 LECM 메시지를 수신하는 경우, 암호화되지 않은 부분으로부터 그 부분에 포함된 인덱스 [i]를 판독하고, 어드레스@처리_함수[i]에 위치한 함수를 호출하여 LECM 메시지의 일부를 암호화하는데 사용된 키 Kn[i]를 계산한다. 이어서 상기 모듈은 이러한 키 Kn[i]에 의해 LECM 메시지에서 보호되는 부분을 해독할 수 있다.

[0087] 더욱 복잡한 키 관리를 사용하는 변형 실시예에서, 변환기 모듈은 LECM 메시지에서 보호될 데이터를 대칭 키 Kc로 암호화하고, 활성 네트워크 키 Kn[0]으로 키 Kc를 암호화한 것과 활성 키의 인덱스 [0]을 LECM 메시지의 암호화되지 않은 부분에 삽입한다. 이러한 메시지를 수신하는 터미널 모듈은 메시지의 암호화되지 않은 부분으로부터 추출된 인덱스 [0]에 의해, 전술한 바와 같이 키 Kn[0]을 복구한다. 이어서 상기 모듈은 항목 $E_{Kn[0]}(Kc)$을 해독함으로써 키 Kc를 얻을 수 있고, 그 후 보호된 데이터를 Kc에 의해 해독할 수 있다.

[0088] 본 발명에 의하면, 불법 복제를 방지하고 선의의 사용자가 이전에 기록된 데이터를 판독할 수 있도록 하면서도 가정내의 디지털 네트워크에 대하여 변경을 가할 수 있게 된다.

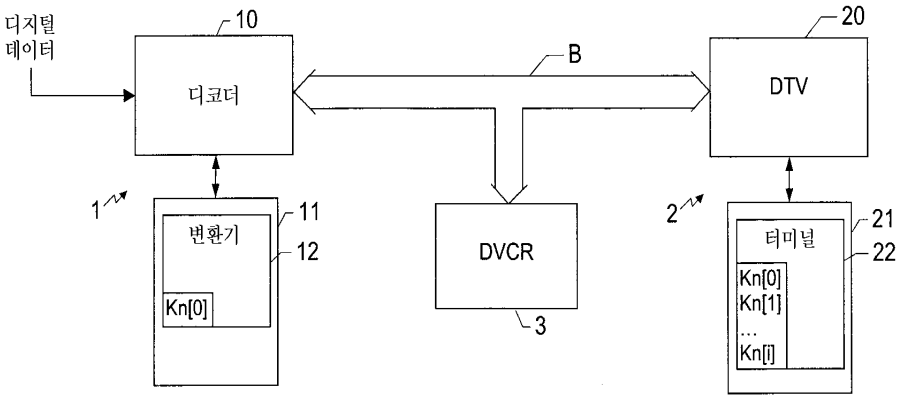
도면의 간단한 설명

[0025] 도 1은 본 발명에 따른 네트워크를 개략적으로 도시한 도면.

[0026] 도 2는 이러한 네트워크을 따라 흐르는 데이터를 도시하는 도면.

도면

도면1



도면2