



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2010년07월22일
(11) 등록번호 10-0971992
(24) 등록일자 2010년07월16일

(51) Int. Cl.
H04L 9/08 (2006.01)
(21) 출원번호 10-2007-7027203
(22) 출원일자(국제출원일자) 2006년04월24일
심사청구일자 2007년11월22일
(85) 번역문제출일자 2007년11월22일
(65) 공개번호 10-2008-0004625
(43) 공개일자 2008년01월09일
(86) 국제출원번호 PCT/IB2006/000992
(87) 국제공개번호 WO 2006/114684
국제공개일자 2006년11월02일
(30) 우선권주장
60/674,959 2005년04월25일 미국(US)
(56) 선행기술조사문헌
US20040037424 A1
US20040120529 A1
전체 청구항 수 : 총 11 항

(73) 특허권자
노키아 코포레이션
핀란드핀-02150 에스푸 카일알라텐티에 4
(72) 발명자
타르칼라 라우리
핀란드 에스아이-02660 에스푸 티클린쿠자 8비4
(74) 대리인
리앤목특허법인

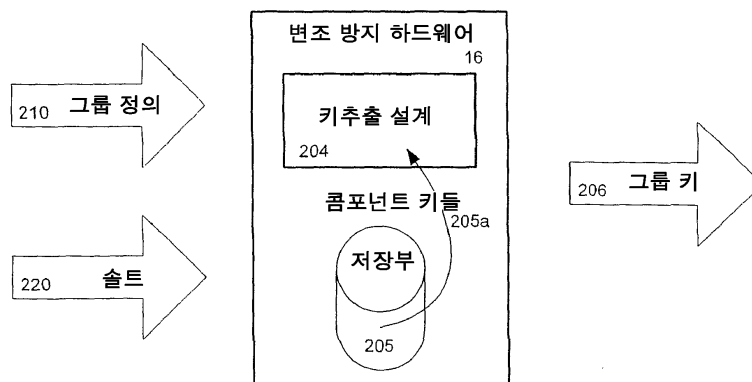
심사관 : 유선중

(54) 그룹 키 생성을 위한 방법 및 장치

(57) 요약

키 생성 시스템은 권한이 부여된 그룹의 입력에 기반을 둔 권한이 부여된 그룹 키들의 생성을 제공하는 것으로 개시된다. 키 생성을 수행하는 시스템은 일차 집합의 모든 가능한 부분집합 X에 상응하는 콤포넌트 키들을 저장하고, 여기서 부분집합 X는 k 또는 그 이하의 구성원들을 갖는다. 권한이 부여된 그룹 키는 의사 무작위 함수로 권한이 부여된 집합의 구성원을 포함하지 않는 부분집합들 X의 배열된 콤포넌트 키들을 전달함에 의하여 권한이 부여된 집합에 대하여 생성된다.

대표도 - 도2



특허청구의 범위

청구항 1

그룹 키 생성 방법에 있어서,

수신기들의 집합에 대하여, 미리 정의된 상수인 k 보다 더 적은 구성원들을 갖는 수신기들의 각각의 가능한 부분집합 X 에 대하여 콤포넨트 키를 제공하는 단계;

상기 부분집합들 X 를 배열하는 반복 배열 함수를 정의하는 단계;

권한이 부여된 수신기들의 부분집합에 대하여, 어떤 부분집합들 X 가 권한이 부여된 부분집합의 구성원들을 포함하지 않는지를 결정하고 각각의 그러한 부분집합 X 와 관련된 상기 콤포넨트 키들을 식별하는 단계;

입력 및 출력 그룹 키로서 콤포넨트 키들의 임의의 수를 취하는 의사 무작위 함수를 정의하는 단계; 및

상기 권한이 부여된 부분집합의 구성원들을 포함하지 않는 k 보다 작은 크기의 X 의 부분집합들과 관련된 상기 콤포넨트 키들을 상기 의사 무작위 함수에 입력으로서 이용하는 단계를 포함하고,

상기 콤포넨트 키들은 상기 반복 배열 함수에 의하여 주어진 순서로 상기 의사 무작위 함수에 적용되고 상기 의사 무작위 함수의 출력은 권한이 부여된 수신기에 특정된 그룹 키인 것을 특징으로 하는 그룹 키 생성 방법.

청구항 2

제1항에 있어서,

각각의 부분집합 X 에 콤포넨트 키들을 할당하는 추가적인 반복 배열 함수를 더 포함하는 것을 특징으로 하는 그룹 키 생성 방법.

청구항 3

제1항에 있어서, 상기 방법은 상기 수신기에 의하여 수행되고, 상기 수신기는 자신이 상기 권한이 부여된 부분집합의 구성원인 경우에만 오직 상기 방법을 수행하는 것을 특징으로 하는 그룹 키 생성 방법.

청구항 4

제1항에 있어서, 상기 의사 무작위 함수는 AES-XCBC-MAC에 기반을 둔 것을 특징으로 하는 그룹 키 생성 방법.

청구항 5

제1항에 있어서, 상기 의사 무작위 함수는 HMAC_SHA1에 기반을 둔 것을 특징으로 하는 그룹 키 생성 방법.

청구항 6

제1항에 있어서, 상기 의사 무작위 함수는 추가적인 솔트(salt) 파라미터를 취하는 것을 특징으로 하는 그룹 키 생성 방법.

청구항 7

수신기에 있어서,

저장부 및 로직을 포함하는 변조 방지 환경; 및

상기 변조 방지 환경에 저장된 복수의 콤포넨트 키들 및 장치 ID로서, 상기 수신기를 포함하지 않는 각각의 가능한 부분집합 X 에 상응하는 적어도 하나의 콤포넨트 키가 있고, 상기 부분집합들 X 는 k 보다 적은 구성원들을 갖는 수신기들의 모든 집합을 나타내는 복수의 콤포넨트 키들 및 장치 ID를 포함하고,

권한이 부여된 그룹 정의의 수신에 따라, 상기 변조 방지 환경의 로직은 상기 권한이 부여된 그룹의 구성원들을 포함하지 않는 부분집합들 X 를 결정하고, 각각의 그러한 그룹은 주사 배열(injective ordering) 함수에 의하여 결정된 것과 같이 배열되고, 상기 배열된 그룹들과 관련된 콤포넨트 키들은 의사 무작위 함수에 대한 파라미터들로서 이용되고 상기 배열 함수에 의하여 표시된 순서로 적용되고;

상기 의사 무작위 함수의 출력은 권한이 부여된 그룹 키인 것을 특징으로 하는 수신기.

청구항 8

제7항에 있어서, 상기 의사 무작위 함수는 AES-XCBC_MAC에 기반을 둔 것을 특징으로 하는 수신기.

청구항 9

제7항에 있어서, 상기 의사 무작위 함수는 HMAC_SHA1에 기반을 둔 것을 특징으로 하는 수신기.

청구항 10

제7항에 있어서, 상기 의사 무작위 함수는 추가적인 솔트 파라미터를 취하는 것을 특징으로 하는 수신기.

청구항 11

그룹 키 생성을 제공하는 프로그램 제품에 있어서,

컴퓨터로 판독 가능한 매체;

부분집합들 X를 배열하는 반복 배열 함수를 정의하는 상기 컴퓨터로 판독 가능한 매체에 저장된 프로그램 코드로서, 부분집합들 X는 미리 지정된 수보다 적은 구성원들을 갖는 모든 수신기들의 집합의 부분집합들인 프로그램 코드;

그룹 정의의 수신에 따라 어떤 부분집합들 X가 상기 그룹 정의 내의 구성원들을 포함하지 않는지 결정하고 각각의 그러한 부분집합 X와 관련된 키를 식별하는 상기 컴퓨터로 판독 가능한 매체에 저장된 프로그램 코드;

입력 및 출력 그룹 키로서 콤포넌트 키들의 임의의 수를 취하는 의사 무작위 함수를 포함하는 상기 컴퓨터로 판독 가능한 매체에 저장된 프로그램 코드; 및

상기 의사 무작위 함수에 대한 입력으로서 상기 그룹 정의 내의 구성원들을 포함하지 않는 X의 부분집합들과 관련된 상기 콤포넌트 키들을 이용하는 상기 컴퓨터로 판독 가능한 매체에 저장된 프로그램 코드를 포함하고,

상기 콤포넌트 키들은 상기 반복 배열 함수에 의하여 주어진 순서로 상기 의사 무작위 함수에 적용되고 상기 의사 무작위 함수의 출력은 권한이 부여된 수신기에 특정된 그룹 키인 것을 특징으로 하는 그룹 키 생성을 제공하는 프로그램 제품.

명세서

기술분야

[0001] 본 발명은 일반적으로 보안 및 암호 작성법(cryptography) 분야에 관련된다. 본 발명은 보다 구체적으로 콘텐츠 전달 시스템에서 키(key) 분산에 관련된다.

배경기술

[0002] 방송 부호화 방법 기술의 상태가 뒤따르는 출판물에서 묘사되고, 상기 출판물의 개시는 여기에서 참조로서 편입된다.

[0003] A. Fiat and M. Naor, *Broadcast Encryption*, Advances in Cryptology - CRYPTO'93 Proceedings, Lecture Notes in Computer Science, Vol. 773, 1994, pp. 480-491.

[0004] NIST. FIPS-197: Advanced Encryption Standard.

[0005] <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

[0006] S. Frankel. AES-XCBC-MAC-96 Algorithm And Its Use With IPSec.

- [0007] <http://www.ietf.org/rfc/rfc3566.txt>
- [0008] NIST. FIPS-81: DES Modes Of Operation.
- [0009] <http://www.itl.nist.gov/fipspubs/fip81.htm>
- [0010] H.Krawzyk.RFC2104 - Keyed-Hashing for Message Authentication.
- [0011] <http://www.faqs.org/rfcs/rfc2104.html>
- [0012] NIST. FIPS 180-1: Secure Hash Standard.

발명의 상세한 설명

[0013] 게시된 발명의 한 측면은 인증된 사용자의 수신기의 집합에 대한 그룹 키 생성 방법을 제공한다. 상기 방법은 k 보다 적은 수의 구성원들을 갖는 수신기의 각각의 가능한 부분집합 X 에 대하여 컴포넌트 키를 제공하고, 여기서 k 는 미리 정의된 상수이다. 주사 배열 함수는 특정 순서로 부분집합 X 를 위치시킨다. 인증된 수신기들의 부분집합에 대하여, 권한이 부여된 부분집합의 구성원들을 포함하지 않는 부분집합 X 가 결정된다. 각각의 그러한 부분집합 X 와 관련된 컴포넌트 키들이 식별된다. 부분집합들과 관련된 컴포넌트 키들을 입력으로서 취하는 의사 무작위 함수(pseudo random function)는 주사 배열 함수에 의해 정의된 순서로 k 보다 작은 크기로 권한이 부여된 집합으로부터 분리되고, 그룹 키를 출력한다.

[0014] 게시된 발명의 다른 측면은 그룹 키 생성을 수행하는 변조 방지 환경(tamper resistant environment)을 갖는 수신기를 제공한다. 변조 방지 환경은 복수의 컴포넌트 키들 및 장치 ID를 저장한다. 각각의 장치에 대하여, 그것의 장치가 구성원이 아닌 각각의 가능한 부분집합 X 에 상응하는 적어도 하나의 저장된 컴포넌트 키가 있고, 여기서 부분집합 X 는 k 보다 적은 구성원들을 갖는 수신기들의 모든 집합을 나타낸다. 권한이 부여된 그룹 정의의 수신에 따라, 수신기의 변조 방지 하드웨어는 수신기가 권한이 부여된 그룹의 구성원인지 여부를 결정한다. 만약 그렇다면, 변조 방지 환경에서 로직은 권한이 부여된 그룹의 구성원들을 포함하지 않는 k 보다 작은 크기의 부분집합 X 를 결정하고, 이러한 그룹들은 주사 배열 함수에 의해 결정된 것과 같이 배열된다. 배열된 그룹들과 관련된 컴포넌트 키들은 배열 함수에 의해 지시된 순서로 의사 무작위 함수에 대한 파라미터들로서 적용된다. 의사 무작위 함수의 출력은 권한이 부여된 그룹 키이다.

실시 예

[0020] 콘텐츠 전달 시스템에서, 도 1에 도시된 바와 같이, 콘텐츠 제공부(10)는 전송 매체(20)를 통하여 하나 또는 그 이상의 수신기(15)로 콘텐츠를 전송한다. 그러한 콘텐츠 전달 시스템의 한 예는 공중 전송, 케이블, 디지털 비디오 방송(digital video broadcast, DVB), 위성, 또는 인터넷 프로토콜 네트워크 및 디지털 멀티미디어 방송(Digital Multimedia Broadcasting, DMB) 및 MediaFLO™ Of course를 포함하는 다른 멀티미디어 전달 시스템을 통하여 전송되는 텔레비전 방송이고, 수많은 다른 유형의 콘텐츠 및 전송 매체들이 또한 이러한 콘텐츠 전달 모델에 적합할 것이고 본 발명의 내용에 적합할 것이다. 이러한 모델을 통하여 분산될 수 있는 콘텐츠 유형들의 다른 예들은 오디오, 텍스트, 비디오 게임들 또는 쌍방향 미디어를 포함한다. 적절한 전송 매체의 다른 예들은 라디오 방송, 셀 기반, 블루투스(Bluetooth), IEEE 802.11x, 그물형 네트워크(mesh network) 및 유선/광학 WANs 또는 LAN을 포함한다.

[0021] 콘텐츠 제공부는 종종 그들의 이용자들에게 다양한 서비스를 제공한다. 이는 사용자들이 그들이 수신한 서비스를 그들의 개별 필요에 적합하도록 가공하는 것을 허용한다. 텔레비전 서비스의 내용에서, 예를 들면, 사용자들은 프리미엄 채널, 시청 이벤트마다 지불 및 주문형 프로그램 중 선택할 수 있다. 이러한 다양성을 촉진하기 위하여, 콘텐츠 제공부들은 일반적으로 그들의 콘텐츠 중 일부 또는 전부를 암호화하고, 오직 인증된 수신기만이 사용자가 구매한 서비스들에 상응하는 콘텐츠를 해독하는 것을 허용한다.

[0022] 암호화 시스템과 일관되게, 콘텐츠 제공부(10)는 전송된 콘텐츠 중 적어도 일부를 암호화하기 위한 하드웨어 및 소프트웨어를 이용할 것이고 수신기(15)는 콘텐츠를 해독하는 하드웨어 및 소프트웨어를 구비할 것이다. 수신기

의 하드웨어는 넓은 범위의 다양한 장치들로 구비될 수 있고, 예를 들면, 텔레비전 셋톱박스, 휴대용 단말기 또는 범용 컴퓨터이다. 암호화 기술의 보안을 유지하기 위하여, 수신기의 하드웨어 및/또는 소프트웨어는 암호화 시스템에 참여하기 위해 요구되는 정보 및 로직을 포함하는 변조 방지 환경(16)을 포함할 것이다. 변조 방지 환경(16)은 암호화 시스템을 무력화하기 위한 사용자의 시도가 시스템의 비밀에 접근하지 못하게 하는 것을 보장하도록 한다. 변조 방지 환경(16)은 본 기술분야에서 알려진 시스템 및 방법들 중 어느 것에 의해서라도 구성될 수 있다.

[0023] 그러나 암호화/해독화 시스템의 관리는 수많은 어려움을 초래한다. 한 특정 어려움은 실제 시스템에 이용되는 보안키들 및 알고리즘들의 관리 및 분배이다. 시스템 수신기의 수 및 개별 암호화 이벤트들의 수가 커짐에 따라 키 관리는 취약해진다.

[0024] 개시된 시스템들 및 방법들은 콘텐츠를 암호화하고 해독하는데 요구되는 키들의 효율적이고 안전한 생성 및 분배를 제공한다. 개시된 시스템들 및 방법들은 콘텐츠 제공부 및 인증된 수신기의 변조 방지 환경(16) 모두 공유된 비밀 정보 및 로직의 집합으로부터 매칭 키들을 생성하는 것을 허용한다. 나아가, 개시된 시스템은 콘텐츠 제공부 및 수신기의 변조 방지 환경(16)이 인증된 사용자의 부분집합에 대하여 매칭 그룹 키들을 생성하는 것을 허용한다. 인증된 그룹의 정의는 콘텐츠 제공부가 암호화 이벤트의 수를 제한하는 것을 허용하고, 이는 또한 그것에 의하여 전송되는 정보의 양을 제한하고 시스템의 보안을 강화한다.

[0025] 특히, 개시된 시스템들 및 방법들은 그룹 키들이 수신기의 변조 방지 환경(16)에서 저장된 비밀들에 대한 정보를 나타내지 않는 방송 환경에서 그룹 키들의 추출을 제공한다. 변조 방지 환경(16)은 키 추출 설계를 구성하고 컴포넌트 키들을 저장하기 위하여 요구된다. 컴포넌트 키들은 수신기의 변조 방지 환경(16)에 저장된 보안 키들이고, 이는 사용자에게 장치의 분배에 앞서 수신기에 위치될 수 있다. 바람직하게는, 각각의 변조 방지 환경은 오직 수신기가 그 한 구성원인 인증된 집합들에 대하여 그룹 키를 생성하기 위하여 요구되는 키들을 저장한다. 변조 방지 환경은 그것이 한 구성원이 아닌 그룹들에 대하여 그룹 키들을 생성하기 위하여 이용되는 키들을 저장할 필요가 없다.

[0026] 예를 들면, 도 2에 도시된 바와 같이, 수신기의 변조 방지 환경(16)은 키 추출 설계(204) 및 보안 저장(205)을 포함하고, 보안 저장(205)은 컴포넌트 키들(205a)을 저장한다.

[0027] 특정 그룹 키(206)를 생성하기 위하여, 변조 방지 환경(16)은 그룹 정의(210) 및 선택적으로 솔트(salt, 220)를 입력으로써 취하고, 솔트는 예를 들면 범용 상수, 어떤 그룹 정의에 특정된 것, 하루 중 시간 또는 컴포넌트 키들에 독립적인 어떠한 다른 파라미터이다. 암호화 시스템의 완전함을 유지하는 것을 보장하기 위하여, 수신기의 변조 방지 환경(16)은 사용자가 그룹의 일원이라면 오직 그룹 키를 출력할 것이다. 이는 보안 저장에 저장될 장치 ID를 필요로 하고, 그러므로 수신기는 이것이 그룹 정의(210)에서 제공된 그룹의 일원인지 여부를 인식할 수 있다. 유리하게, 추출된 그룹 키들 중 일부가 비록 암호화 시스템을 회피하기 위한 사용자들의 시도에 노출될지라도, 변조 방지 환경(16)에서 장기간 비밀들은 비밀상태로 유지된다. 더 나아가, 그룹 키 노출의 위험은 솔트 파라미터를 빈번하게 변경함으로써 완화될 수 있다. 추가적으로, 인증된 그룹의 일원이 아닌 수신기는 그것이 요구되는 파라미터를 갖지 않기 때문에 개시된 방법을 이용하여 그룹 키를 계산할 수 없을 것이다. 시스템 보호는 그러므로 그것이 인증된 그룹의 일원인지 여부를 판별하는 변조 방지 환경의 판별에 홀로 기반을 두지 않는다.

[0028] 이러한 논의의 목적으로, 집합 U는 모든 사용자의 집합으로 가정된다. 물론 전체 시스템의 구성에서 콘텐츠 제공부는 복수의 독립적인 도메인 U를 작업할 것이다. $n = |U|$ 는 이러한 집합의 크기라고 하자. 콘텐츠 제공부는 시스템의 저항을 정의하는 값 k를 뽑아내고, 여기서 $k < n$ 이다. 이러한 저항은 변조 방지 환경을 깨뜨리고 암호화 설계를 무력화하기 위하여 공모해야 하는 사용자들의 최소수를 정의한다. k의 선택은 설계에서 결정되는 것이다. k에 대한 큰 값은 키들의 더 많은 수를 야기하지만 무력화하기 어려운 암호화 시스템을 만든다. 반대로 k의 작은 값은 더 강력하지 못한 시스템을 야기하지만, 상대적으로 적은 수의 키들을 요구한다. 예를 들면, 만약 k가 2로 설정되었다면, 시스템은 변조 방지 환경이 보안상태로 남아있는 한 보안 상태로 있지만, 만약 두 사용자가 변조 방지 환경에서 비밀을 취득한다면 그들은 상기 시스템을 공모하여 깨뜨릴 수 있다.

[0029] 집합 U의 구성원을 집합 Z의 구성원으로 변환하는 제1 주사 배열(injective ordering) 함수 f, 즉, $f: U \rightarrow Z$ 는, U의 구성원들이 Z로 배열되도록 한다. 나아가, U의 두 구성원 a, b에 대해 오직 만약 $f(a) < f(b)$ 인 경우에만 $a < b$ 이다. 다른 주사 배열 함수 $g(X)$ 는 U의 부분집합을 배열하기 위하여 정의된다. 그러한 함수의 예는 $g(X) = \sum_{u \in X} 2^{f(u)}$ 이다. 그러나 U의 부분집합들에 대한 주사 배열을 제공하는 다른 어떠한 함수라도 이용될 수 있

고 본 기술분야에서 용의하게 추론해낼 수 있다. 키는 $|X| < k$ 인 집합 U 에서 각각의 가능한 그룹 X 에 대하여 할당된다. 키 K_i 는 $i = g(x)$ 인 경우에 할당된다. 대안적인 디자인에서, 키들에 관련하는 모든 개시는 키의 나머지가 다른 과정을 이용하여 생성되는 경우 키의 부분을 생성한다.

[0030] 각각의 장치에 대하여, 변조 방지 환경은 그것이 일원이 아닌 k 보다 작은 크기의 U 의 부분집합에 상응하는 키들 K_i 를 단지 저장하기만 한다. 이는(아래 설명된 키 추출과 함께) U 중에서 k 구성원들보다 적은 것이 그들이 일원이 아닌 그룹의 그룹 키를 계산하는 것이 가능하지 않음을 의미한다.

[0031] 인증된 사용자들의 그룹은 Y 로서 정의되고, 이는 인증된 수신기들을 포함하는 U 의 부분집합이다. Y 는 콘텐츠 제공부에 의해 전송된 그룹 정의(210)로서 기능한다. 대안적으로, Y 에 없는 사용자들의 집합은 그룹 정의로서 기능할 수 있다. 인증된 그룹 U 에 대하여 그룹 키(206)는 $\text{mix}()$ 라 불리는 개시의 내용에서, 임의의 길이의 입력의 임의의 수를 취할 수 있는 의사 무작위 함수를 이용함으로써 생성된다. 주어진 그룹 Y 에 대하여, $\text{mix}()$ 에 대한 파라미터들은 Y 의 구성원들을 포함하지 않는, 즉, $U-Y$ 이고 $|X| < k$ 인 모든 부분집합 X 로부터 추출된다. 각각의 그러한 부분집합은 X 의 일원이고, 그러므로 각각의 수신기에 의하여 저장된 관련된 키 K_i 를 갖는다. $U-Y$ 로부터의 각각의 X 에 대한 키들 K_i 는 $\text{mix}()$ 를 위한 파라미터들로서 이용된다. 나아가 그들은 $g(X)$ 에 의하여 정의된 순서로 이용된다. 배열된 키들 K_i 에 더하여, 상기에서 논의된 바와 같은 솔트 파라미터는 또한 선택적으로 그룹 정의와 함께 전송될 수 있고 $\text{mix}()$ 에 파라미터로서 더해질 수 있다.

[0032] 언급된 바와 같이, 솔트 파라미터는 그룹 정의로부터 개별 파라미터로서 전달될 수 있다. 이러한 솔트는 특정 형태(예를 들면, 길이에서 정확히 m 비트 또는 길이에서 최대한 m 비트)일 것이 요구될 수 있다. 그러므로 만약 솔트가 그것에 대한 기준 설정을 만족하지 않으면 그 경우 그룹 키 추출은 실패하고 그로인해 추가적인 보안을 제공한다.

[0033] 세 가지 예시적인 $\text{mix}()$ 함수 구성들이 아래 개시되었고, 두 개는 HMAC_SHA1에 기반을 두고 하나는 AES_XCBC_MAC에 기반을 둔다. 제공된 개시들에 대하여, 2진 연산자 \parallel 는 접합을 나타내기 위하여 이용된다. 물론, 적절한 $\text{mix}()$ 함수들의 수많은 다른 구성들 및 예시들이 본 발명의 사상에서 벗어남 없이 용이하게 고안될 수 있을 것이다.

[0034] - AES-XCBC-MAC에 기반을 둔 $\text{MIX}()$ 함수 예

[0035] 본 섹션은 위에서 인용된 S. Frankel, 위에서 인용된 바와 같이 NIST. FIPS-81:DES Modes Of Operation에서 묘사된 Counter-Mode and Cipher Feedback mode에서 묘사된 바와 같은 AES-XCBC-MAC에 기반을 둔 $\text{mix}()$ 함수를 설명한다. AES-CBC-MAC는 NIST. FIPS-81에서 설명된 바와 같은 CBC 모드에서 AES를 이용함에 의하여 메시지 인증 부호(message authentication code)를 생성함으로써 이용된다.

[0036] 의사 무작위 함수는 필요하다면 j 개까지의 AES 블록들을 출력하는 AES-XCBC-MAC에 기반을 둔 파라미터들 (k, x, j)을 취하도록 정의된다. 함수의 입력은 AES 블록들의 비트 스트링 x 인 AES 키이다. 블록들은 $x_1, x_2 \dots$ 로 기재된다.

[0037] $\text{AES}_k(x)$ 는 키 k 를 이용하여 단일 평면 텍스트 블록 x 상에 AES로 부호를 표시하기 위하여 이용된다.

[0038] $\text{AES_CBC_MAC}_k(x)$ 는 평문 블록들 x 상에 키 k 를 갖는 AES를 이용하여 CBC-mode MAC의 계산을 표시하기 위하여 이용된다. 입력은 적절한 길이(즉, AES 블록 크기의 배수)인 것으로 가정된다.

[0039] 의사 무작위 함수는 다음과 같이 계산된다:

[0040] 1. Let $k_1 = \text{AES}_k(P_1)$.

[0041] 2. Let $k_2 = \text{AES}_k(P_2)$.

[0042] 3. $C_1 = \text{AES}_{k_1}(\text{AES_CBC_MAC}_{k_1}(x) \text{ XOR } k_2 \text{ XOR } 0x01)$

[0043] 4. For $\text{cnt} = 2$ to j

[0044] $C_{\text{cnt}} = \text{AES}_{k_1}(\text{AES_CBC_MAC}_{k_1}(x \parallel C_{\text{cnt-1}}) \text{ XOR } k_2 \text{ XOR } \text{cnt})$

[0045] 의사 무작위 함수는 항상 데이터의 AES 블록들을 j 까지 생성한다. $\text{mix}(\text{salt}, k_1, \dots, k_m)$ 함수는 이제 다음과 같이 정의된다.

[0046] 1. $T_1 = \text{pseudo random function}(k_1, \text{SALT}, j)$

- [0047] 2. For cnt = 2 to m
- [0048] a. $T_{cnt} = \text{pseudo random function}(k_{cnt}, T_{\{cnt-1\}}, j)$
- [0049] 상수 P1 및 P2는 $P1 \neq P2$ 인 동안 의지대로 정의될 수 있다. 예를 들면 어떤 경우 값 $P1 = 0x01010101010101010101010101010101$ 및 $P2 = 0x02020202020202020202020202020202$ 를 이용할 수 있다.
- [0050] 이러한 $\text{mix}()$ 함수는 인증된 그룹에 대한 키인 비트 스트링 $T_m(m$ 은 입력에서 키들의 수이다)을 야기한다.
- [0051] 도 3은 $i = 1$ 이고 $cnt > 1$ 인 경우에 대하여 AES-XCBC-MAC에 기반을 둔 예시적인 mix 함수의 구성을 도시하고 솔트는 정확히 한 AES 블록의 길이이다. $K_i(301)$ 는 AES 블록들(302, 303, 및 304)에 적용된다. $P1 \neq P2$ 이도록 자유롭게 정의되는 상수(305) P1은 키(301)를 갖는 입력과 함께 AES 블록(307)에 적용된다. $T_{i, \{j-1\}}$ 의 XOR(311) 및 AES 블록(307)의 출력은 AES 블록(302)의 출력과 함께 AES 블록(308)에 적용된다. 키(301) 및 상수 P2(306)는 AES 블록(303)에 적용된다. 위에서 정의된 바와 같이, $j(312)$ 및 AES 블록(303)의 출력의 XOR(313)은 AES 블록(308)의 출력과 함께 XOR(214)에 적용된다. XOR(314)의 출력 및 키(301)는 AES 블록(304) 내지 출력 $T_{i, j}(315)$ 에 적용된다. 이러한 과정은 블록 $T_{i, j}$ 로 귀결된다. 만약 오직 하나의 키가 권한이 부여된 집합의 구성원이고 $j = 2$ 라면, 이러한 블록은 출력 그룹 키의 두 번째 블록이 될 것이다.
- [0052] -HMAC_SHA1에 기반을 둔 MIX() 함수의 예
- [0053] HMAC_SHA1 기반 $\text{mix}()$ 함수는 위에서 설명된 구현보다 다소 더 간단하다. 의사 무작위 함수는 파라미터 (k, x, j)를 취하고, 키 k 및 비트 스트링 x 로 주어진 데이터의 블록들(160-비트)인, NIST. FIPS 180-1: Secure Hash Standard에 묘사된 바와 같은, SHA1 블록들로 j 를 출력한다. 여기에 HMAC_SHA1(k, x)에 의하여 키 k 및 입력 비트 스트링 x 를 이용하여 계산된 HMAC_SHA1을 표시한다. 의사 무작위 함수는 다음과 같다.
- [0054] 1. $C_1 = \text{HMAC_SHA1}(k, x \parallel 0x01)$
- [0055] 2. For cnt = 2 to j
- [0056] $C_{cnt} = \text{HMAC_SHA1}(k, x \parallel C_{\{cnt-1\}} \parallel cnt)$
- [0057] 의사 무작위 함수는 항상 데이터의 SHA1 블록들(160-비트)을 j 까지 생성한다. $\text{mix}(\text{salt}, k_1, \dots, k_m)$ 함수는 이제 다음과 같이 정의된다.
- [0058] 1. $T_1 = \text{prf}(k_1, \text{salt}, j)$
- [0059] 2. For cnt = 2 to m
- [0060] $T_{cnt} = \text{prf}(k_{cnt}, T_{\{cnt-1\}}, j)$
- [0061] 이러한 $\text{mix}()$ 과정은 권한이 부여된 그룹에 대한 키인 비트 스트링 $T_m(m$ 은 입력에서 키의 수이다)로 귀결된다.
- [0062] 도 4는 HMAC_SHA1 기반 mix 함수를 도시한다. $C_{i,0}$ 은 비어있는 스트링으로 간주된다. Ipad(405) 및 K_i 의 반복의 XOR(404)가 j 와 접합된 $C_{i, \{j-1\}}$ 과 접합하는 Salt와 함께 Secure Hash Algorithm 1(SHA1, 402)에 적용된다. Opad(405) 및 $K_i(403)$ 의 반복의 XOR(407)은 $C_{i, j}(409)$ 를 생성하기 위하여 SHA1(408)로 SHA1(402)의 출력과 함께 적용된다. 이러한 과정은 출력의 하나의 SHA1 블록을 생성한다. 1 내지 j 의 모든 요구되는 블록들 상의 I의 각각의 값에 대한 반복은 접합되었을 때 그룹 키를 생성하는 블록들 $C_{m, j}(m$ 은 입력 키들의 수이다)의 시퀀스를 생성한다.
- [0063] - 가변 길이 키를 갖는 HMAC_SHA1에 기반을 둔 MIX() 함수의 예
- [0064] HMAC_SHA1을 갖는 가변 길이 키들의 이용은 $\text{mix}()$ 함수를 현저하게 간소화하고 속도를 증가시킨다. $\text{mix}(\text{salt}, k_1, \dots, k_n)$ 함수는 다음과 같이 계산된다.
- [0065] 1. $T_1 = \text{HMAC_SHA1}(K_1 \parallel \dots \parallel K_n, \text{salt} \parallel 0x01)$
- [0066] 2. For cnt = 2 to j
- [0067] $T_{cnt} = \text{HMAC_SHA1}(K_1 \parallel \dots \parallel K_n, \text{salt} \parallel T_{\{cnt-1\}} \parallel cnt)$
- [0068] 이러한 함수에서 모든 키들은 주사 배열 함수에 의하여 정의된 순서로 함께 접합된다. 시퍼-피드백(cipher-feedback) 및 반대 모드는 솔트 상에서 HMAC_SHA1에 의하여 결합되고 계산된다.

[0069] 도 5는 가변 길이 키 HMAC_SHA1에 기반을 둔 mix 함수를 도시한다. T₀은 비어있는 스트림인 것으로 고려된다. Ipad(505) 및 K₁ || ... || K_n의 XOR(504)는 j와 접합되고 t_{j-1}과 접합되는 Salt(501)와 함께 Secure Hash Algorithm 1(SHA1, 502)에 적용된다. Opad(505) 및 K₁ || ... || K_n의 접합(503)의 XOR(507)은 T_j(509)를 생성하기 위하여 SHA1(502)의 출력과 함께 SHA1(508)로 적용된다. 개시된 함수에 대하여, j>1 (만약 j=1이면 이전 블록은 생략될 것이다)인 경우이다. Ipad 및 Opad는 다시 H. Krawczyk. RFC 2104 - Keyed-Hashing for Message Authentication에서 정의된 바와 같은 키들의 접합과 동일한 길이의 상수이다.

[0070] 본 발명의 많은 특징들 및 이점들은 상세한 설명으로부터 명료하고, 그러므로 첨부된 청구항들에 의하여 본 발명의 실제 사상 및 범위 내로 귀결하는 본 발명의 모든 그러한 특징들 및 이점들이 포함되도록 되었다.

[0071] 더 나아가, 수많은 변경 및 다양화들이 본 기술분야에서 숙련된 자들에게 용이하게 발생할 것이고, 본 발명이 여기에 설명되고 묘사된 정확한 소개 및 동작들로 한정되는 것을 바람직하지 않다. 그러므로 인지되는 모든 적절한 변형들 및 균등물들은 청구항들의 범위 내로 귀결되어야 할 것이다.

도면의 간단한 설명

[0015] 도 1은 개시된 시스템들 및 방법들의 내용에서 예시적인 콘텐츠 분포이다.

[0016] 도 2는 예시적인 수신기의 키 유도 시스템이다.

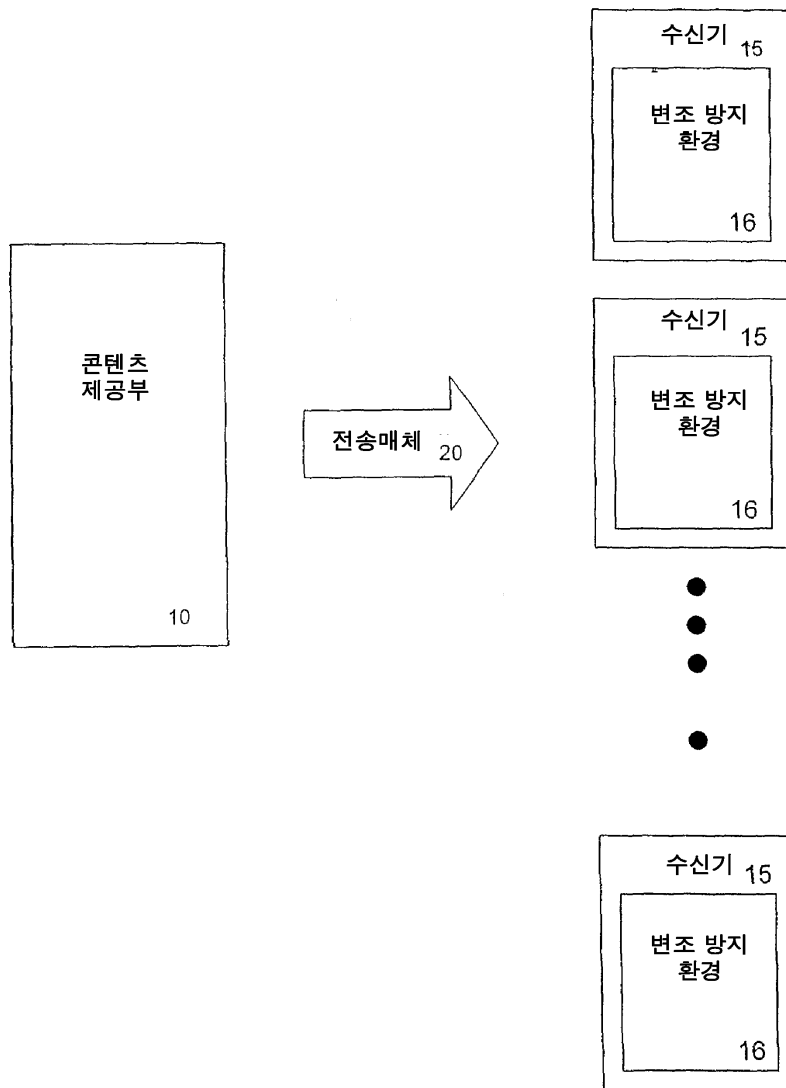
[0017] 도 3은 AES-XCBC-MAC 기반 예시적인 mix() 함수이다.

[0018] 도 4는 HMAC_SHA1 기반 예시적인 mix() 함수이다.

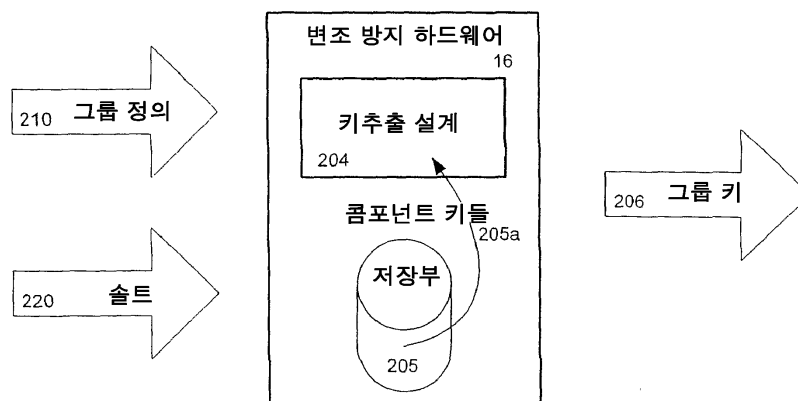
[0019] 도 5는 HMAC_SHA1 기반 가변 길이 키를 갖는 예시적인 mix() 함수이다.

도면

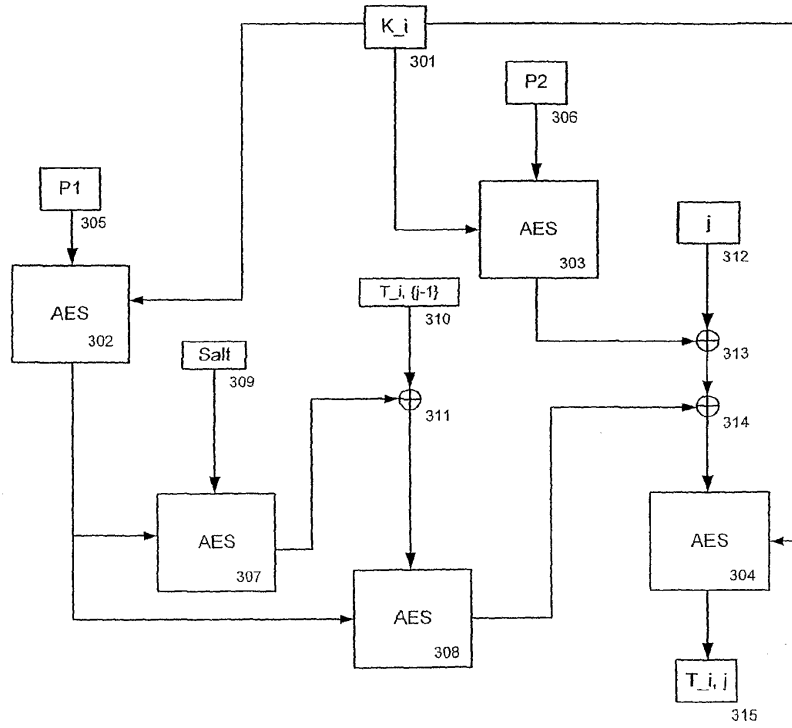
도면1



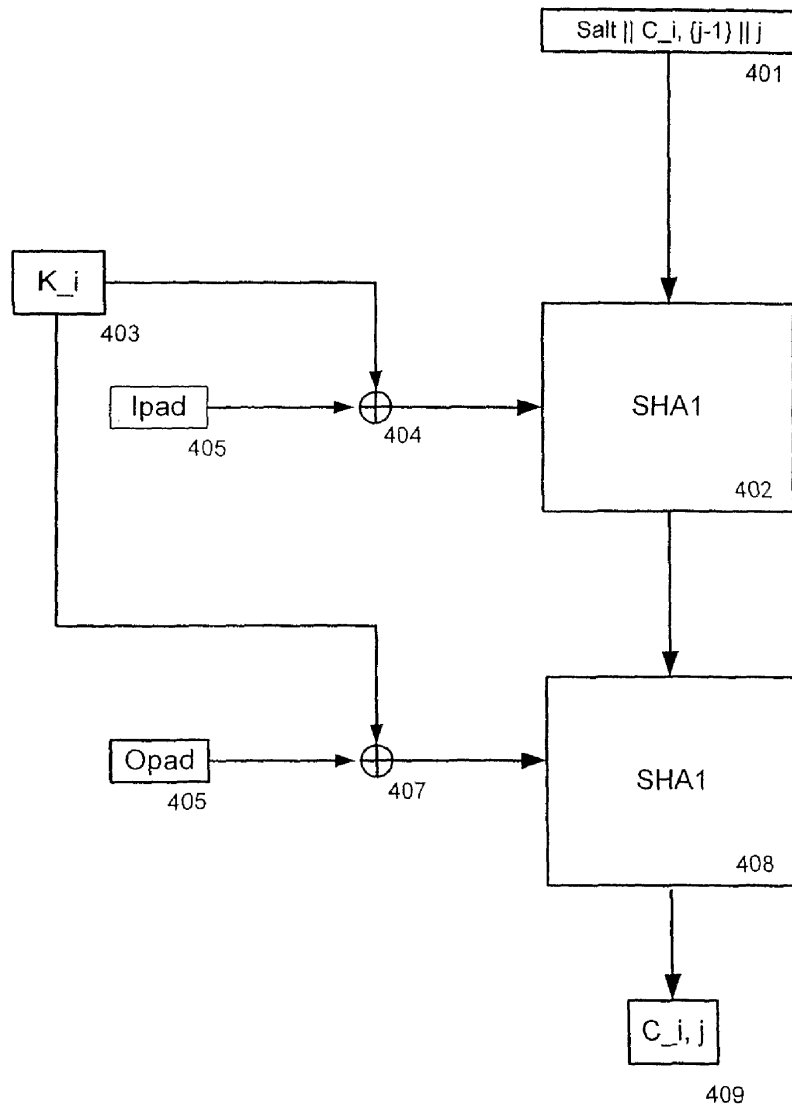
도면2



도면3



도면4



도면5

