(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.[6]
H04L 9/06

(45) 공고일자 2005년10월06일
(11) 등록번호 10-0519839
(24) 등록일자 2005년09월29일

(21) 출원번호 10-1999-0021673
(22) 출원일자 1999년06월11일

(65) 공개번호 10-2000-0006093
(43) 공개일자 2000년01월25일

(30) 우선권주장 09/097,782 1998년06월15일 미국(US)

(73) 특허권자
루센트 테크놀러지스 인크
미합중국 뉴저지 머레이 힐 마운틴 애비뉴 600 (우편번호 : 07974-0636)

(72) 발명자
베렌즈웨이그아담엘
미국뉴욕주10003뉴욕#12-0이스트12스트리트70

괠코스티븐앤쏘니
미국뉴저지주07950모리스플레인스피치스트리트6

미지코브스키셈욘비
미국뉴저지주07751모간빌옐로우나이프로드227

페크럴윈스턴에드워드
미국뉴저지주08854피스카타웨이루트거스로드85-비

랜스로버트존
미국메사츄세츠주01810앤도버윈터그린서클6

요우트쿠스도날드요셉
미국뉴저지주07920바스킹릿지제임스타운로드82

(74) 대리인
김창세
장성구

심사관 : 전용해

(54) 메시지 프레임 암호화 방법

요약

본 발명은 외부의 암호화동기(cryptosync)를 사용하는 일 없이 음질 열화(speech degradation)를 최소화하여 개량된 보안성을 제공하는 암호화 스피치 프로세서 구조(encrypting speech processor architecture)에 관한 것이다. 이는 (음성 암호기에서 구현되는 것들과 같은 고정된 비밀 마스크 암호화 방안(fixed secret mask encryption scheme) 대신에) 송신기 측에서 인코딩된 스피치 비트 블럭을 암호화하는 블럭 암호화기(34)와 키 스트림 발생기(36)를 도입함으로써 달성

된다. 블럭 암호화기(34)는 가역 암호 작성 알고리즘과 내부 암호화동기를 채용하여 인코딩된 스피치 비트의 제 1 블럭을 제 1 암호텍스트 블럭(출력 34)으로 변환한다. 제 1 암호텍스트 블럭(출력 34)은 키 스트림(출력 36)을 생성하는 데 사용되고, 그런 다음 이 키 스트림은 제 2 암호텍스트 블럭(도 2)을 암호화하는 데 사용된다.

대표도

도 2

명세서

도면의 간단한 설명

도 1은 종래 기술의 스피치 프로세서, 에러 방지, 음성 암호화 구조를 도시하는 도면,

도 2는 본 발명에 따라 사용되는 송신기 내에서 구현되는 스피치 프로세서 구조를 도시하는 도면,

도 3은 본 발명의 특징이 되는 인코딩된 스피치 비트를 나타내는 대표도,

도 4는 본 발명의 일 실시예에 따라 48 비트의 일반텍스트(plaintext) 블럭을 암호텍스트로 암호화하기 위해 개량된 셀룰러 메시지 암호화 알고리즘(Enhanced Cellular Message Encryption Algorithms : ECMEA)을 채용하는 블럭 암호화기의 기능적 블럭도,

도 5는 도 4에 도시한 블럭 암호화기의 반대 동작을 수행하는 48 비트 블럭 암호 해독기의 기능적 블럭도,

도 6은 본 발명의 일 실시예에 따라 ECMEA를 채용하는 키 스트림 생성기의 기능적 블럭도,

도 7은 본 발명에 따라 사용되는 수신기 내에서 구현되는 스피치 프로세서 구조를 도시하는 도면,

도 8은 본 발명의 일 실시예에 따라 ECMEA를 채용하는 40 비트 블럭 암호화기의 기능 블럭도,

도 9는 도 8에 도시한 블럭 암호화기의 반대 동작을 수행하는 40 비트 블럭 암호 해독기의 기능적 블럭도,

도 10은 본 발명의 일 실시예에 따라 RC5를 채용하는 48 비트 블럭 암호화기의 기능적 블럭도.

도면의 주요 부분에 대한 부호의 설명

30 : 송신기 32 : 스피치 코더

34 : 블럭 암호화기 36 : 키 스트림 생성기

38, 40 : XOR 연산기 42 : 7 비트 사이클릭 용장 코더

44 : ½ 레이트 컨볼루션 코더 46 : 펑쳐

48 : 2 슬롯 인터리버

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 전반적으로 통신 시스템에 관한 것으로서, 보다 상세하게는, 무선 통신 시스템에서 사용되는 암호화 기법에 관한 것이다.

무선 통신 시스템은 암호 작성법(cryptography)을 사용하여 가입자에 대한 보안 통신 수단을 제공한다. 암호 작성법은 의도된 수신기만이 인증된 송신기가 송신한 메시지(예를 들어, 음성 데이터, 사용자 데이터, 또는 FACCH/SACCH 메시지일 수 있다)의 내용을 이해할 수 있도록, 그리고 인증된 송신기만이 메시지를 의도된 수신기로 보낼 수 있도록 보안성을 제공한다. 암호 작성법의 목표는 메시지의 내용을 의도된 수신기만이 이해할 수 있는 형태로 바꾸는 것이다. 이는 송신기와 의도된 수신기 모두에 대해 경제적인 방법으로 수행되어야 한다. 동시에, 인증되지 않은 수신기(즉, 의도된 수신기가 아닌 것)가 그 내용을 이해하는 것이 (시간 및/또는 장비의 관점에서) 매우 어려워야 한다. 인증되지 않은 수신기와 송신기가 보다 정교해짐에 따라, 통신 보안의 필요성이 증대되고 있다.

도 1은 주지의 시분할 다중 액세스(Time Division Multiple Access : TDMA)에 대한 원격 통신 산업 협회(Telecommunication Industrial Association : TIA)의 IS136(과 그 개정) 표준과, 대수 코드 여기 선형 예측(Algebraic Code Excited Linear Prediction : ACELP)에 대한 IS641 표준에 기초하여 송신기(10) 내에서 구현되는 암호화 스피치 프로세서 구조를 도시한다. 송신기(10)는 스피치 코더(12), 7 비트 사이클릭 용장 코더(Seven Bit Cyclical Redundancy Coder : 7Bit CRC)(14), ½(half) 레이트 컨볼루션 코더(½- 레이트 CC)(16), 펑쳐((Puncture)(18), 음성 암호화기(20), 2 슬롯 인터리버(TwoSlot Interleaver)(22)를 포함한다. 스피치 코더(12)는 160 개의 16 비트 스피치 샘플을 특징으로 하는 메시지 프레임을 인코딩하여, 96 개의 클래스 1 비트와 52 개의 클래스 2 비트를 갖는 148 개의 인코딩된 스피치 비트를 생성하는데, 클래스 1 비트는 48 개의 클래스 1A 비트와 48 개의 클래스 1B 비트를 포함하는 것을 특징으로 한다. 클래스 1 비트는 무선 링크를 통해 송신될 때 에러 제어 보호를 필요로 하는 중요한 비트(예컨대, 피치(pitch), 억양 등을 나타내는 비트)로서, 사이클릭 용장 코드, 컨볼루션 코딩, 비트 인터리빙을 이용하여 에러 제어 보호가 실현되는 것을 특징으로 한다. 클래스 1A 비트는 7Bit CRC(14)에 대한 입력으로서 제공되어 7 개의 에러 제어 비트를 생성한다. 에러 제어 비트, 클래스 1 비트, 5 개의 테일(tail) 비트(컨볼루션 코드 상태 정보를 특징으로 함)는 ½- 레이트 CC(16)에 대한 입력으로서 제공되어 216 개의 코드워드 비트를 생성한다. 그런 다음, 코드워드 비트에 (펑쳐(18)를 거쳐서) 삭제 삽입(erasure insertion)을 실시하므로써 208 개의 펑쳐링된 코드워드 비트가 생성된다.

다음으로, 음성 암호화기(20)는 의도된 수신기만이 메시지의 내용을 이해할 수 있도록 메시지를 보호하는 데 사용된다. 특히, 펑쳐링된 코드워드 비트와 클래스 2 비트가 음성 암호화기(20)에 입력으로서 제공된다. 음성 암호화기(20)는 의도된 수신기와 연관된 260 비트 고정 비밀 마스크(260 bit fixed secret mask)를 사용하여 입력을 암호화하여 260 개의 암호화 비트를 생성한다. 자세하게는, 암호화는 비밀 마스크를 사용하여 펑쳐링된 코드워드 비트와 클래스 2 비트에 XOR 이진 연산을 수행함으로써 이루어진다. 부호화 비트는 (비트 인터리버(22)에 의해) 비트 인터리빙(bit interleaving)되어, 260 개의 인터리빙된 비트를 생성한다. 그 후, 메시지는 다중화되고, 변조되어 송신기(10)에 의해 송신된다.

송신된 메시지는 도시하지 않은 수신기에 의해 수신되는데, 수신기에서는 송신기(10)의 반대 동작이 수행된다. 송신된 메시지를 수신하면, 수신기는 송신된 메시지를 복조하고 역다중화하여 260 개의 인터리빙된 비트를 얻는다. 이어서, 비트 인터리빙 과정이 (비트 역인터리버(deinterleaver)에 의해) 역으로 수행되어 260 개의 암호화 비트를 얻는다. 암호화 비트는 (음성 암호 해독기에 의해) 암호 해독되어, 208 개의 펑쳐링된 코드워드 비트와 52 개의 클래스 2 비트를 갖는 출력을 얻는다. 수신기가 송신기(10)에 의해 채용된 260 비트 고정 비밀 마스크를 알지 못하는 경우(즉, 수신기가 의도된 수신기가 아닌 경우), 수신기는 암호화 비트를 적절히 해독할 수 없을 것이다.

펑쳐링된 코드워드 비트는 펑쳐링된 코드워드 비트가 역컨볼루션되는 ½레이트 컨볼루션 디코더로 제공되어 (48 개의 클래스 1A 비트와 48 개의 클래스 1B 비트를 특징으로 하는) 96 개의 클래스 1 비트와 7 개의 에러 제어 비트를 갖는 출력을 얻는다. 수신기에서는 삭제 삽입 과정의 반대 동작이 없음에 유의하여야 한다. 삭제 삽입으로 인한 비트 손실은 본 기술 분야에서 잘 알려진 바와 같이 역컨볼루션 과정 중에 복원된다.

클래스 1A 비트는 수신기에서 7 비트 CRC가 사용하여 (제 1 세트의 7 개의 에러 제어 비트는 ½ 레이트 컨볼루션 디코더 출력의 일부분임을 특징으로 하는) 제 2 세트의 7 개의 에러 제어 비트를 생성한다. 제 1 및 제 2 세트의 에러 제어 비트는 (CRC 확인을 이용하여) 비교되어, 클래스 1A 비트의 송신에 대해 에러가 발생하였는지를 결정한다(즉, 불량 프레임이 존재하는지를 결정한다). 송신 에러가 발생하지 않은 경우, 클래스 1 비트와 (음성 암호 해독기로부터의) 클래스 2 비트는 스피치 디코더로 전달되어 디코딩된다. 송신 에러가 발생한 경우 (즉, 불량 프레임이 검출된 경우), 클래스 1A 비트와 32 개의 최상위 클래스 1B 비트는 폐기되고, 최후의 우량 프레임(들)의 클래스 1A 비트와 32 개의 최상위 클래스 1B 비트의 일정 함수 또는 보간법(interpolation)에 의해 대체되어, 스피치 디코더로 전달된다. (음성 암호 해독기로부터의) 클래스 2 비트와 (½ 레이트 컨볼루션 디코더로부터의) 16 개의 최하위 클래스 1B 비트는 스피치 디코더로 전달되어, 최후의 우량 프레임(들)의 클래스 1A 비트와 32 개의 최상위 클래스 1B 비트의 전달된 함수 또는 보간법과 함께 디코딩된다. 클래스 2 비트와 16 개의 최하위 클래스 1B 비트 내에 비트 에러가 존재하는 경우, 이들 에러가 음질에 미치는 지각적인 영향은 나머지 클래스 1B와 클래스 1A 비트 내의 에러가 미치는 영향에 비해 덜하다.

음성 암호를 구현하는 종래의 암호화 구조는 일정한 장점을 제공한다. 첫째, 양단에서(즉, 송신기와 수신기에서) 260 비트 고정 비밀 마스크를 동기화하기 위해, 외부 소스로부터의 암호화동기(cryptosync)(여기서부터 "외부 암호화동기"라 지칭함)가 필요하지 않은데, 이 암호화동기는 두 개의 암호 작성 알고리즘이 서로 동기화되는 것을 보장하기 위한 데이터 입력으로 특징지워진다. 둘째로, 송신 에러가 존재해도 음질의 열화가 발생하지 않는다. 클래스 1A 비트와 32 개의 최상위 클래스 1B 비트의 송신에 있어서 에러는 가장 최근의 우량 프레임(들)의 클래스 1A 비트와 32 개의 최상위 클래스 1B 비트의 일정 함수 또는 보간법을 이용하여 마스킹될 수 있다. 그러나, 종래의 암호화 구조는 두 가지 방식에서 보안 문제를 일으키기 쉽다. 첫째, 260 비트 고정 비밀 마스크가 알려진 일반텍스트(즉, 음성 암호화기로의 입력)를 사용하여 결정될 수 있는데, 이는 다음에 암호화 비트를 이해(또는 암호 해독)하는 데 사용될 수 있으므로, 송신된 메시지의 보안을 손상시키게 된다. 둘째, 알려진 일반텍스트가 없더라도, 단지 인접 260 비트 프레임에 XOR을 실시하는 것에 의해, 고정 비밀 마스크를 제거하여, ACELP 스피치 알고리즘 파라미터가 어떻게 변화하였는지에 관한 정보를 얻을 수도 있다. 따라서, 외부 암호화동기를 사용하는 일 없이, 보안성이 향상되며 음질 열화가 적은 스피치 프로세서 구조가 필요하다.

발명이 이루고자 하는 기술적 과제

본 발명은 외부의 암호화동기(cryptosync)를 사용하는 일 없이 음질 열화가 최소가 되도록 하면서 개량된 보안성을 제공하는 암호화 스피치 프로세서 구조에 관한 것이다. 이는 송신기 측에서, 인코딩된 스피치 비트 블럭을 암호화하는 블럭 암호화기와 키 스트림 생성기를 (음성 암호기에서 구현되는 것들과 같은 고정된 비밀 마스크 암호화 방안(fixed secret mask scheme) 대신에) 구현함으로써 달성된다. 블럭 암호화기는 가역 암호 작성(invertible cryptographic) 알고리즘과 내부 암호화동기를 채용하여 인코딩된 스피치 비트의 제 1 블럭을 제 1 암호텍스트(ciphertext) 블럭으로 변환하되, 인코딩된 스피치 비트의 제 1 블럭은, 그 송신 중에 에러가 발생하는 경우 감지가능한 심각한 음질 열화를 초래할 수 있는 제 1 레벨 비트를 포함하는 것(과, 이전 우량 프레임의 비트들의 일정 함수 또는 보간법을 사용하는 대신 에러가 발생된 비트가 사용된다는 것)을 특징으로 한다.

그런 다음, 제 1 암호텍스트 블럭은 키 스트림 생성기와 사이클릭 용장 확인기에 입력된다. 키 스트림 생성기는, 키잉된 일방 함수(keyed oneway function)로 사용되는 가역 암호 작성 알고리즘과 내부 암호화동기를 채용하여, 제 1 암호텍스트 블럭을 암호화된 제 1 암호텍스트 블럭으로 특징지워지는 키 스트림으로 변환한다. 다음에, 키 스트림은 부호화된 스피치 비트의 제 2 및 제 3 블럭을 암호화하여 각각 제 2 및 제 3 암호텍스트 블럭을 생성하는 데 사용되는데, 인코딩된 스피치 비트의 제 3 블럭은 제 1 암호텍스트 블럭의 송신 중에 에러가 발생해도 음질 열화를 거의 또는 전혀 초래하지 않는 제 2 레벨 비트를 포함하고, 인코딩된 비트의 제 2 블럭은 제 1 및 제 2 레벨 비트를 포함하는 것을 특징으로 한다.

사이클릭 용장 확인기에서, 제 1 암호텍스트 블럭은 에러 제어 비트를 생성하는 데 사용되는데, 에러 제어 비트는 제 1 암호텍스트 블럭의 송신 중에 에러가 발생하였는지를 검출하는 데 사용되고, 이는 다시 말하면, 제 1 암호텍스트 블럭은 일종의 송신 에러 검출 메커니즘에 의해 보호된다. 이어서, 제 1, 2, 3 암호텍스트 블럭과 에러 제어 비트가 처리되어 송신된다.

수신기 측에서, 에러 제어 비트와 수신된 제 1 암호텍스트 블럭은 제 1 암호텍스트 블럭의 송신 중에 에러가 발생하였는지를 판단하는 데 사용된다. 에러가 검출되지 않은 경우, 수신된 제 1 암호텍스트 블럭은 블럭 암호 해독기에 의해 암호 해독되고, (송신기 측의 키 스트림 생성기와 동일한 키 스트림 생성기에 의해) 수신된 제 2 및 3 암호텍스트 블럭을 암호 해독하는 데 사용된다. 에러가 검출된 경우, (제 1 및 제 2 암호텍스트 블럭 내의) 제 1 레벨 비트는 하나 이상의 최후의 우량 프레임 내의 제 1 레벨 비트의 일정 함수 또는 보간법을 사용하여 마스킹된다. (제 2 및 제 3 암호텍스트 블럭 내의) 제 2 레벨 비트는 처리 사이클을 절약하기 위해, (잘못) 암호 해독되는 대신 스피치 디코더로 직접 전달된다.

바람직하게도, 본 발명의 이 실시예는 제 1 레벨 비트로부터 에러를 확장시키지는 않는다. 특히, 수신된 제 1 암호텍스트 블럭 내의 임의의 비트에 에러가 발생한 경우, 모든 제 1 레벨 비트가 하나 이상의 최후 우량 프레임의 제 1 레벨 비트의 일정 함수 또는 보간법을 이용하여 마스킹되기 때문에, 그 에러가 다른 제 1 레벨 비트로 확장되지 않는다. 수신 암호텍스트 블럭 내의 임의의 비트에 발생한 에러가 제 2 레벨 비트로 확장되더라도, 그 에러는 음질에 있어 지각할 수 있는 영향을 거의 또는 전혀 미치지 않을 것이다. 수신된 제 1 암호텍스트 블럭 내의 어떤 비트에도 에러가 발생하지 않은 경우, 어떤 에러도 임의의 다른 제 1 레벨 또는 제 2 레벨 비트로 확장되지 않을 것이라는 점에 주목하여야 한다. 또한, 키 스트림이 일반텍스트와 XOR되는 키 스트림 생성기 구조 때문에, 수신된 제 2 및 제 3 암호텍스트 블럭 내의 어떤 에러도 다른 비트로 확장되지 않는다는 점에도 주목하여야 한다.

나아가, 블럭 암호화기와 키 스트림 생성기는 바람직하게, 종래 기술에서 사용되는 음성 암호화기에 의해 채용되는 260 비트 고정 비밀 마스크보다, 훨씬 더 암호 작성 측면에서 안전한 암호 작성 알고리즘(즉, 키잉된 일방 함수)을 채용한다. 따라서, 본 발명의 암호화 스피치 프로세서는 종래 기술에 비해 훨씬 더 암호 작성 측면에서 안전하다. 또한, 내부 암호화동기를 사용하여 암호화 및 암호 해독 암호 작성 알고리즘을 동기화시킨다. 따라서, 외부 암호화동기가 필요하지 않다.

발명의 구성 및 작용

본 발명의 특성, 양상, 장점은 도면과 함께 다음의 상세한 설명, 첨부한 청구 범위를 참조하면 더 잘 이해될 것이다.

도 2는 본 발명에 따라 사용되는 송신기(30) 내에서 구현되는 스피치 프로세서 구조를 도시한다. 설명을 위해, 본 발명은 잘 알려진, 시분할 다중 액세스(TDMA)에 관한 IS136 (및 이들의 수정) 표준과 대수 코드 여기 선형 예측(ACELP)에 관한 IS641 표준에 기반한 스피치 프로세서 구조를 예로 들어 기술할 것이다. 그러나, 이는 어떤 방식으로든 본 발명을 제한하려는 의도는 아니다.

송신기(30)는 스피치 코더(32), 블럭 암호화기(34), 키 스트림 생성기(36), XOR 연산기(38, 40), 7 비트 사이클릭 용장 코더(7Bit CRC)(42), ½ 레이트 컨볼루션 코더(½ 레이트 CC)(44), 펑쳐(46), 2 슬롯 인터리버(48)를 구비하는 스피치 프로세서 구조를 포함한다. 스피치 프로세서 구조는 컴퓨터 프로세서나 주문형 반도체(ASIC) 칩 등에서 실행되는 소프트웨어로서 구현될 수 있다. 스피치 코더(32), XOR 연산기(38, 40), 7 비트 CRC(42), ½ 레이트 CC(44), 펑쳐(46), 2 슬롯 인터리버(48)는 본 기술 분야에서 이미 잘 알려져 있다. 블럭 암호화기(34)와 키 스트림 생성기(36)는 본 명세서에서 설명될 것이다.

스피치 코더(32)는 송신될 160 개의 16 비트 스피치 표본(speech samples)으로 특징지워지는 메시지 프레임을 수신한다. "스피치 표본"이라는 용어는, 본 발명에서는, 스피치 데이터, 사용자 데이터, 제어 채널 메시지를 포함하지만, 여기에 한정되지는 않는 것으로 이해되어야 한다. 메시지 프레임은 스피치 코더(32)에 의해 인코딩되어, 제 1 및 제 2 레벨로 인코딩된 스피치 비트를 갖는 148 개의 인코딩된 스피치 비트로 특징지워지는 출력$_{32}$를 생성하는데, 여기서 제 1 레벨 (인코딩된 스피치) 비트는, 제 1 블럭의 임의의 비트에서 송신 에러가 발생한 경우, 감지할 수 있는 음질의 열화를 초래하는 스피치 특성을 나타내고, 제 2 레벨 (인코딩된 스피치) 비트는 송신 에러가 제 1 블럭의 임의의 비트에서 발생하더라도, 감지할 수 있는 정도의 음질 열화를 초래하지는 않는 스피치 특성을 나타내는 것을 특징으로 한다. 도 3은 본 응용에서 특징으로 하는 인코딩된 스피치 비트를 설명하는 표(45)를 도시한다.

인코딩된 스피치 비트는 후속적으로 세 블럭으로 분배되어 처리된다. (본 명세서에서 클래스 1A 비트 또는 출력$_{32-1}$로도 지칭하는) 제 1 블럭은 48 개의 제 1 레벨 비트를 포함하고, (본 명세서에서 클래스 1B 비트 또는 출력$_{32-2}$로도 지칭하는) 제 2 블럭은 32 개의 제 1 레벨 비트와 16 개의 제 2 레벨 비트를 포함하며, (본 명세서에서 클래스 2 비트 또는 출력$_{32-3}$으로도 지칭하는) 제 3 블럭은 52 개의 제 2 레벨 비트를 포함한다. 이 중에서 제 2 블럭에 대해서는, 제 1 레벨 비트는 32 개의 최상위 비트이고, 제 2 레벨 비트는 16 개의 최하위 비트이다. 본 발명이 인코딩된 스피치 비트가 분배되는 블럭의 개수나 각 블럭 내의 비트 수에 한정되는 것이 아니라는 점에 유의하여야 한다. 제 1 레벨 비트는 송신 에러가 발생하는 경우 감지할 수 있는 정도의 음질 열화를 초래하기 때문에, 에러 제어 보호가 이들 비트의 가능한 많은 수에 적용되는데, 에러 제어 보호는, 예를 들어, 사이클릭 용장 코드와 컨볼루션 코딩을 통해 제공되는 것이 특징이다.

클래스 1A 비트(제 1 블럭)는 스피치 코더(32)로부터 블럭 암호화기(34)에 입력되고, 클래스 1B(제 2 블럭)는 XOR 연산기(38)에 입력되며, 클래스 2 비트(제 3 블럭)는 XOR 연산기(40)에 입력된다. 블럭 암호화기(34)는 일반텍스트 블럭을 암호텍스트로 암호화하기 위해 의도된 수신기와 연관된 키를 갖는 가역 암호 작성 알고리즘을 채용한다. 이러한 암호 작성 알고리즘의 예로는 RC5와 개량된 셀룰러 메시지 암호화 알고리즘(Enhanced Cellular Messaging Encryption Algorithm : ECMEA) 등이 있다. RC5는 론 리베스트(Ron Rivest)에 의해 개발되어 본 기술 분야에서 잘 알려져 있다. ECMEA는 로버트 랜스(Robert Rance), 다니엘 히어(Daniel Heer), 세미온 미치코프스키(Semyon Mizikovsky) 등에 의해 개발되었다. ECMEA는 1997년 10월 28일 TIA 회원들이 참석한 TIA TR45 AdHoc 인증 그룹 회의에서 공표되었으며, 수출 관리 규정(Export Administration Regulation) (타이틀 15 CFR 파트 730 내지 774)에서 규정된 대로 미합중국 상무성(United States Department of Commerce) 수출 관할(export jurisdiction)에 따르는 TIA가 통제하여 제한적으로 배포하고 있어 구해 볼 수는 있다.

블럭 암호화기(34)에서, 클래스 1A 비트는 암호화되어 48 개의 클래스 1A 암호텍스트 비트(또는 제 1 암호텍스트 블럭)로 특징지워지는 출력$_{34}$를 생성한다. 도 4는 본 발명의 일 실시예에 따라 48 비트 블럭의 일반텍스트를 암호텍스트로 변환하기 위해 ECMEA를 채용하는 블럭 암호화기(34)의 기능적 블럭도를 도시한다. 블럭 암호화기는 (입력을 암호화하는 암호화 모드에서 동작하는) 제 1, 2, 3 함수 호출기(52, 54, 58)와 XOR 연산기(56)를 포함한다. 클래스 1A 비트의 제 1 및 제 2의 16 비트 부분(여기서부터는 각각 제 1 및 제 2 클래스 1A 부분으로 지칭함)은 제 1 및 제 2 ECMEA 함수 호출기(52, 54)의 입력으로 제공된다. 제 1 ECMEA 함수 호출기(52)는 제 2 클래스 1A 부분을 암호화동기 입력으로 사용하여 제 1 클래스 1A 부분을 암호화하여 16 비트 출력$_{52}$를 생성한다.

본 기술 분야에서 잘 알려져 있듯이, 암호화동기는 암호화 및 암호 해독 암호 작성 알고리즘을 동기시키기 위해 사용된다. 그러나, 특히 ECMEA에서 암호화동기는 ECMEA의 암호 작성 강도를 높이기 위한 키잉(keying) 비트로도 사용된다. 이 역할을 할 때, ECMEA는 키잉된 해쉬 함수(keyed hash function)로 사용되어 제 1 및 제 2 클래스 1A 부분의 암호화에 전념하면서 48 비트 블럭 암호화기의 전반적인 암호 작성 강도를 증가시키는 데 사용된다.

출력$_{52}$는 XOR 연산기(56)에서 클래스 1A 비트의 제 3의 16 비트 부분(여기서부터는 제 3 클래스 1A 부분으로 지칭함)과 XOR되어 16 비트 출력$_{56}$을 생성한다.

출력$_{56}$은 제 2 및 제 3 ECMEA 함수 호출기(54, 58)에 입력된다. 제 2 ECMEA 함수 호출기(54)는 출력$_{56}$을 암호화동기로 사용하여 제 1 및 제 2 클래스 1A 부분을 암호화하고 16 비트 출력$_{54-1}$과 16 비트 출력$_{54-2}$를 각각 생성한다. 제 3 ECMEA 함수 호출기(58)는 출력$_{54-2}$를 암호화동기로 사용하여 출력$_{56}$과 출력$_{54-1}$을 암호화하여 32 비트 출력$_{58}$을 생성한다. 도 5는 도 4에 도시한 블럭 암호화기(34)의 반대 동작을 수행하는 48 비트 암호 해독기(35)의 기능적 블럭도를 도시한다.

출력$_{58}$과 출력$_{54-2}$는 합쳐져서 블럭 암호화기(34)의 출력$_{34}$를 이룬다. 출력$_{34}$는 7 비트 CRC(42), ½ 레이트 CC(44), 키 스트림 발생기(36)에 입력된다. 7 비트 CRC(42)에서 출력$_{34}$는, 7 개의 에러 제어 비트로 특징지워지는 출력$_{42}$를 생성하는 데 사용된다. 이어서 출력$_{42}$는 ½ 레이트 CC(44)로 제공된다.

키 스트림 생성기(36)는 비트의 키 스트림을 출력하기 위해, RC5와 ECMEA와 같은 가역 암호 작성 알고리즘이나 의도된 수신기와 연관된 키를 갖는 적절하게 비가역으로 키잉된 일방 함수(oneway function)를 채용한다. 일방 함수는 일반적인 암호 작성 동작 유형으로서, 사실상 가역 암호 작성 알고리즘도 이에 속한다. 키잉된 일방 함수의 출력만 가지고는, 키 또는 입력을 유추할 수 없다.

키 스트림 생성기(36)는 104 비트 블럭을 채우기 위해 키 스트림 생성기(34)의 입력에서 충분한 회수만큼 반복되는 48 개의 클래스 1A 암호텍스트 비트(즉, 출력$_{34}$)에 의해 구동된다. 키 스트림 생성기(36)에서 클래스 1A 암호텍스트 비트는 암호화되어, 100 비트의 암호화된 클래스 1A 암호텍스트 비트로 특징지워지는 키 스트림 출력$_{36}$을 생성한다. 더 자세하게는, 출력$_{36}$은 사실상 클래스 1A 암호텍스트 비트인 공지의 의사 랜덤 데이터(pseudo random data)를 암호화하여 (키 스트림 생성기(36)에 의해 채용된) 암호 작성 알고리즘을 실행함으로써 생성된다. ECMEA(와 대부분의 다른 블럭 알고리즘)가 정수 개수의 바이트만을 암호화하기 때문에, (104 비트 블럭으로 특징지워지는) 클래스 1A 암호텍스트 비트 중 4 비트가 폐기된다는 점에 유의하여야 한다.

도 6은 본 발명의 일 실시예에 따라 ECMEA를 채용하는 키 스트림 생성기(36)의 기능적 블럭도를 도시한다. 키 스트림 생성기(36)는 ECMEA 함수 호출기(62)를 포함하는데, 이는 (블럭 암호화기(34)로부터의) 반복된 출력$_{34}$로 특징지워지는 104 비트의 블럭 입력을 수신한다. 블럭 암호화기(34)의 출력이 자신에 부가되거나 이어져서 96 비트를 생성하고, 그런 다음 한 번 더 부분적으로 부가되어 키 스트림 생성기에 대한 104 비트 입력을 생성한다는 것에 유의하여야 한다. 104 비트 블럭 입력은, 출력$_{34}$의 16 개의 최상위 비트(즉, 48 개의 클래스 1A 암호텍스트 비트 중 16 개의 최상위 비트)를 암호화동기로 사용하여, ECMEA 함수 호출기(62)에 의해 암호화되어 출력$_{36}$을 생성한다.

출력$_{36}$은 XOR 연산기(38, 40)에 입력된다. 특히, 출력$_{36}$의 48 비트 부분은 XOR 연산기(38)에 입력되고, 출력$_{36}$의 52 비트 부분은 XOR 연산기(40)에 입력된다. XOR 연산기(38)에서, 클래스 1B 비트(즉, 제 2 블럭)는 출력$_{36}$의 48 비트 부분과

XOR되어 48 개의 클래스 1B 암호텍스트 비트(즉, 제 2 암호텍스트 블럭)로 특징지워지는 출력$_{38}$을 생성한다. 이어서, 출력$_{38}$은 ½ 레이트 CC(44)에 입력된다. 이와 마찬가지로, XOR 연산기(40)에서, 클래스 2 비트(즉, 제 3 블럭)는 출력$_{36}$이 52 비트 부분과 XOR되어 52 개의 클래스 2 암호텍스트 비트(즉, 제 3 암호텍스트 블럭)로 특징지워지는 출력$_{40}$을 생성한다. 그런 다음, 출력$_{40}$은 2 슬롯 인터리버(48)로 제공된다.

½ 레이트 CC(44)에서, 출력$_{42}$, 출력$_{34}$, 출력$_{38}$은 (컨볼루션 코드 상태 정보를 특징으로 하는) 5 개의 테일 비트와 함께 사용되어 216 개의 코드워드 비트로 특징지워지는 출력$_{44}$를 생성한다. 출력$_{44}$는 펑쳐(46)로 제공되어 208 개의 펑쳐링된 코드워드 비트로 특징지워지는 출력$_{46}$을 생성한다. 이어서, 출력$_{46}$은 출력$_{40}$으로 비트 인터리빙되는 2 슬롯 인터리버(48)로 제공되어 260 개의 인터리빙된 비트로 특징지워지는 출력$_{48}$을 생성한다. 출력$_{48}$은 이어서 다중화되고, 변조되어 송신기(30)에 의해 송신된다.

송신된 메시지는 송신기(10)의 반대 동작이 수행되는 수신기에 의해 수신된다. 도 7은 본 발명에 따라 사용되는 수신기(70) 내에서 구현되는 스피치 프로세서 구조를 도시한다. 수신기(70)는 스피치 디코더(72), 블럭 암호 해독기(74), 키 스트림 생성기(76), XOR 연산기(78, 80), 7 비트 CRC(82), ½ 레이트 컨볼루션 디코더(84), 2 슬롯 비트 역인터리버(86)를 포함하는 스피치 프로세서 구조로 이루어져 있다. 이러한 스피치 프로세서 구조는 컴퓨터 프로세서나 주문형 반도체 등에서 실행되는 소프트웨어로 구현될 수 있다. 스피치 디코더(72), XOR 연산기(78, 80), 7 비트 CRC(82), ½ 레이트 컨볼루션 디코더(84), 2 슬롯 비트 역인터리버(86)는 본 기술 분야에서 이미 잘 알려져 있다. 블럭 암호 해독기(74)와 키 스트림 생성기(76)는 여기에서 설명될 것이다.

송신된 메시지를 수신하면, 수신기는 송신된 메시지를 복조하고 역다중화하여 출력$_{48}$(즉, 260 개의 인터리빙된 비트)을 얻는데, 여기서 프라임(')이 붙은 참조 부호는 송신 버전에 대응하는 수신 버전을 나타내는 것이다. 2 슬롯 비트 역인터리버(86)는 출력$_{48'}$을 사용하여 출력$_{46'}$(즉, 208 개의 펑쳐링된 코드워드 비트와 52 개의 클래스 2 암호텍스트 비트 또는 제 3 암호텍스트 블럭)을 생성한다. 그런 다음, 208 개의 펑쳐링된 코드워드 비트는 ½ 레이트 컨볼루션 디코더(84)에 의해 역컨볼루션되어 5 개의 테일 비트, 출력$_{42'}$(즉, 7 개의 에러 제어 비트), 출력$_{34'}$(즉, 48 개의 클래스 1A 암호텍스트 비트 또는 제 1 암호텍스트 블럭), 출력$_{38'}$(즉, 48 개의 클래스 1B 암호텍스트 비트 또는 제 2 암호텍스트 블럭)을 얻는다. 수신기(70)에서는 펑쳐(46)의 삭제 삽입 과정을 반대로 수행하는 동작이 없다는 점에 유의하여야 한다. 삭제 삽입으로 인한 비트 손실은 수신기 내의 ½ 레이트 컨볼루션 디코더(84)에 의해 복원된다.

출력$_{34'}$은 7 비트 CRC(82)에 입력되어 (7 개의 에러 제어 비트의 제 1 세트는 ½ 레이트 컨볼루션 디코더에서 출력된 7 개의 에러 제어 비트인 출력$_{42'}$을 총괄하여 포함하는 것으로 특징지워지는) 7 개의 에러 제어 비트의 제 2 세트를 생성한다. 에러 제어 비트의 제 1 및 제 2 세트를 조사하여 제 1 암호텍스트 블럭(즉, 클래스 1A 암호텍스트 비트)의 전송 중에 에러가 발생하였는지를 판단한다(즉, 불량 프레임이 존재하는 지를 판단한다). 송신 에러가 발생하지 않은 경우, 출력$_{34'}$(즉, 클래스 1A 암호텍스트 비트)는 블럭 암호 해독기(74)와 키 스트림 생성기(76)로 전달된다. 블럭 암호 해독기는 블럭 암호화기(34)의 반대 동작을 수행한다. 도 5를 참조하면, 도 4에 도시한 블럭 암호화기(34)의 반대 동작을 수행하는 48 비트 암호 해독기(35)의 기능적 블럭도가 도시되어 있다. 키 스트림 생성기(76)는 키 스트림 생성기(36)와 동일하다.

블럭 암호 해독기(74)에서, 출력$_{34'}$는 암호 해독되어 출력$_{32\text{-}1'}$(즉, 48 개의 클래스 1A 비트)을 얻는다. 키 스트림 생성기(76)에서, 출력$_{34'}$는 키 스트림 출력$_{36'}$(즉, 100 개의 암호화된 클래스 1A 암호텍스트 비트)을 생성하는 데 사용된다. 이어서, 이 키 스트림은 출력$_{32\text{-}2'}$(즉, 클래스 1B 비트)와 출력$_{32\text{-}3'}$(즉, 클래스 2 비트)을 얻기 위해 출력$_{38'}$(즉, 클래스 1B 암호텍스트 비트)과 출력$_{40'}$(즉, 클래스 2 암호텍스트 비트)을 XOR하는 데 사용된다. 출력$_{32\text{-}1'}$, 출력$_{32\text{-}2'}$, 출력$_{32\text{-}3'}$(즉, 클래스 1A 비트, 클래스 1B 비트, 클래스 2 비트)은 스피치 디코더(72)에 의해 디코딩되어 원래의 메시지 프레임을 얻는다.

송신 에러가 발생한 경우, 제 1 레벨 비트(즉, 클래스 1A 비트와 32 개의 최상위 클래스 1B 비트)는 폐기되고, (잘 알려진 IS641 표준에서 설명한 바와 같이) 하나 이상의 이전 우량 프레임의 제 1 레벨 비트들의 일정 함수 또는 보간법으로 대체되어, 스피치 디코더(72)로 전달된다. 클래스 1A 비트를 블럭 암호 해독하거나 (키 스트림 생성기(76)를 사용하여) 키 스트림을 생성할 필요가 없을 것이고, 이는 왜냐하면, 이들 데이터는 CRC가 실패하면 더 이상 쓸모없기 때문이다. 따라서,

제 2 레벨 비트(즉, 클래스 2 비트와 16 개의 최하위 클래스 1B 비트)를 암호 해독할 수 없다. 이들 작업을 하지 않음으로써, 프로세서 사이클을 절약할 수 있다. 이들 제 2 레벨 비트가 암호화된 채로 남아 있다 하더라도 음질 열화에 거의 또는 전혀 영향을 미치지 않는다.

암호화동기가 외부적으로가 아니라 내부적으로 발생하는 음성 프라이버시와 유사한 방식으로 FACCH와 SACCH 암호화가 본 발명에 의해 제공될 수 있다는 점에 주목하여야 한다. 각각의 FACCH와 SACCH 메시지의 제 1 워드는, 암호화되지 않고 남아 있을 필요가 있는 8 비트 메시지 유형을 포함한다. 따라서, 각각의 FACCH나 SACCH 메시지의 제 1 워드는 도 8(과 도 9)에 도시한 것과 같이 40 비트 블럭 암호화기(80)(과 암호 해독기(90))를 사용할 것이고, 나머지 워드는 도 4의 48 비트 블럭 암호화기를 사용할 것이다.

본 발명이 특정 실시예에 대해 상당히 상세하게 설명되었지만, 이들과 다른 버전으로 구성될 수도 있다. 예를 들어, 다른 암호화기와 암호 해독기를 사용할 수도 있다. 도 10에는, RC5를 채용한 48 비트 블럭 암호화기(100)가 도시되어 있다. 당업자는 다른 유형의 스피치 코더, 에러 제어 방식, 암호화 및/또는 암호 작성 알고리즘을 활용하는 스피치 프로세서 구조에 본 발명의 개념을 응용할 수 있을 것이다. 따라서, 본 발명의 사상과 범주는 본 명세서에 포함된 실시예에 국한되어서는 안 된다.

발명의 효과

본 발명에 따른 암호화 스피치 프로세서 구조에 의하면, 종래의 음성 암호기에서 구현되는 것과 같은 고정된 비밀 마스크 암호화 방식(fixed secret mask scheme) 대신에, 송신기 측에서 인코딩된 스피치 비트 블럭을 암호화하는 블럭 암호화기와 키 스트림 생성기를 구현함으로써, 외부의 암호화동기(cryptosync)를 사용하는 일 없이 음질 열화(speech degradation)를 최소로 하면서 개량된 보안성을 제공할 수 있다.

(57) 청구의 범위

청구항 1.

제 1 레벨 인코딩된 스피치 비트(speech bit)를 갖는 제 1 블럭과 제 2 레벨 인코딩된 스피치 비트를 갖는 제 2 블럭을 포함하는 메시지 프레임(message frame)을 암호화하는 방법에 있어서,

제 1 블럭을 암호화하여 제 1 암호텍스트(ciphertext) 블럭을 생성하는 단계와,

상기 제 1 암호텍스트 블럭을 이용하여 비트들의 키 스트림(keystream)을 생성하는 단계와,

상기 비트들의 키 스트림을 이용하여 제 2 블럭을 암호화하여 제 2 암호텍스트 블럭을 생성하는 단계와,

상기 제 1 암호텍스트 블럭을 이용하여 에러 제어 비트를 생성하는 단계

를 포함하는 것을 특징으로 하는 메시지 프레임 암호화 방법.

청구항 2.

제 1 항에 있어서,

상기 제 2 블럭이 제 1 레벨 인코딩된 스피치 비트를 더 포함하는 것을 특징으로 하는 메시지 프레임 암호화 방법.

청구항 3.

제 1 항에 있어서,

상기 제 1 블럭이 48 개의 제 1 레벨 비트를 포함하는 것을 특징으로 하는 메시지 프레임 암호화 방법.

청구항 4.

제 1 항에 있어서,

상기 제 2 블럭이 52 개의 제 2 레벨 비트를 포함하는 것을 특징으로 하는 메시지 프레임 암호화 방법.

청구항 5.

제 1 항에 있어서,

상기 메시지 프레임은 제 1 레벨 인코딩된 스피치 비트와 제 2 레벨 인코딩된 스피치 비트를 갖는 제 3 블럭을 더 포함하고, 상기 메시지 프레임 암호화 방법은 상기 비트들의 키 스트림을 이용하여 상기 제 3 블럭을 암호화하여 제 3 암호텍스트 블럭을 생성하는 단계를 더 포함하는 것을 특징으로 하는 메시지 프레임 암호화 방법.

청구항 6.

제 1 항에 있어서,

상기 비트들의 키 스트림을 생성하는 단계는,

상기 제 1 암호텍스트 블럭을 반복하여, 반복된 제 1 암호텍스트 블럭을 생성하는 단계와,

상기 제 1 암호텍스트 블럭의 일부분을 이용하여 상기 반복된 제 1 암호텍스트 블럭을 암호화하여 비트들의 키 스트림을 생성하는 단계

를 포함하는 것을 특징으로 하는 메시지 프레임 암호화 방법.

청구항 7.

제 1 항에 있어서,

상기 제 1 암호텍스트 블럭을 이용하여 에러 제어 비트를 생성하는 추가 단계를 더 포함하는 것을 특징으로 하는 메시지 프레임 암호화 방법.

청구항 8.

제 1 항에 있어서,

상기 제 1 블럭을 암호화하여 제 1 암호텍스트 블럭을 생성하는 단계가,

제 1 암호텍스트 블럭의 제 2 부분을 암호화동기(cryptosync)로 사용하여 제 1 암호텍스트 블럭의 제 1 부분을 암호화하여 제 1 출력을 생성하는 단계와,

이진 연산(binary operation)을 이용하여 상기 제 1 출력을 상기 제 1 암호텍스트 블럭의 제 3 부분과 결합하여 제 2 출력을 생성하는 단계와,

상기 제 2 출력을 암호화동기로 이용하여 상기 제 1 암호텍스트 블럭의 상기 제 1 및 제 2 부분을 암호화하여 제 1 파트와 제 2 파트를 갖는 제 3 출력을 생성하는 단계와,

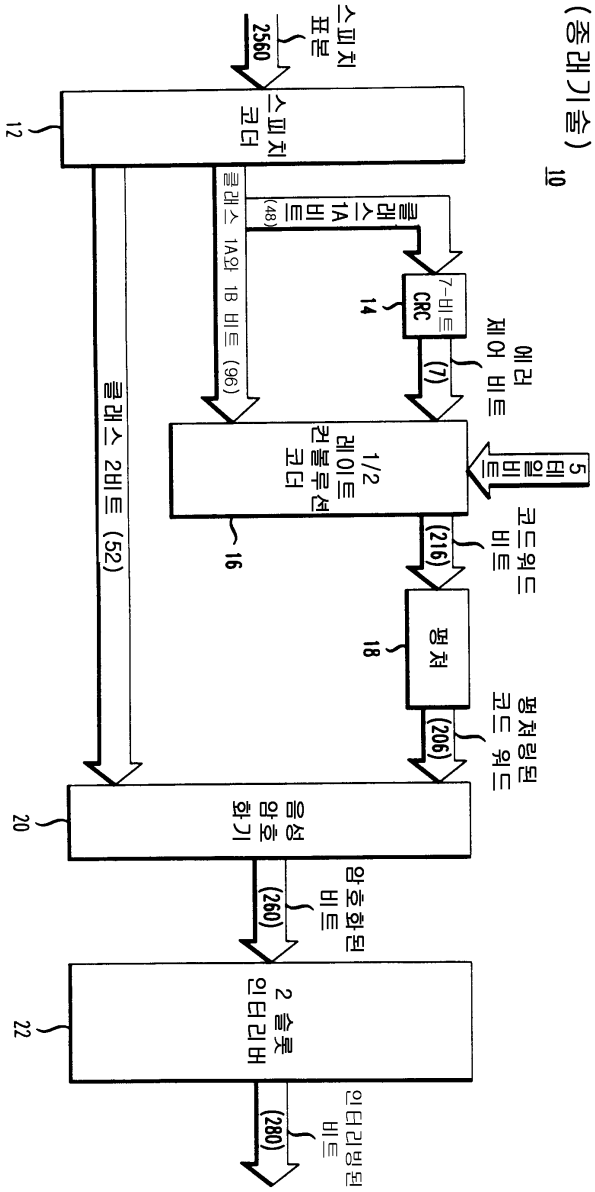
상기 제 3 출력의 제 2 파트를 암호화동기로 이용하여 상기 제 2 출력과 상기 제 3 출력의 제 1 파트를 암호화하여 제 1 및 제 2 파트를 갖는 제 4 출력을 생성하는 단계와,

상기 제 4 출력의 제 1 파트를 암호화동기로 이용하여 상기 제 4 출력의 제 1 파트와 제 3 출력의 제 2 파트를 암호화하여 제 5 출력을 생성하는 단계

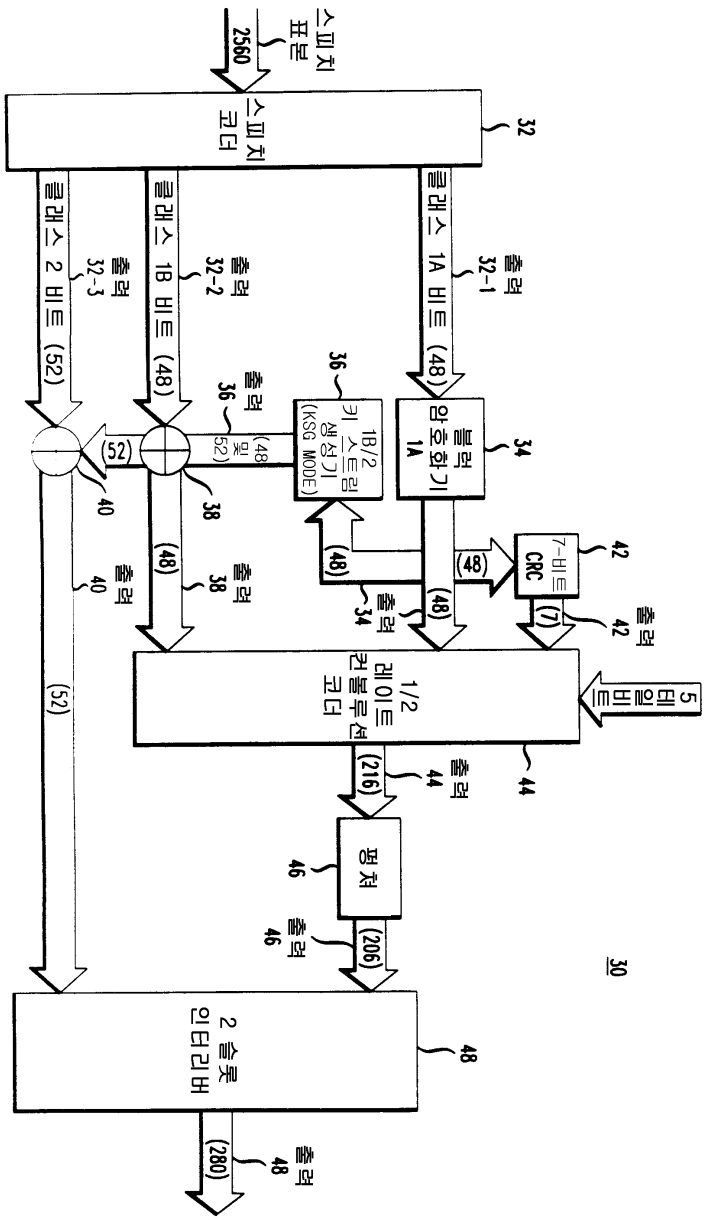
를 더 포함하는 것을 특징으로 하는 메시지 프레임 암호화 방법.

도면

도면1



도면2

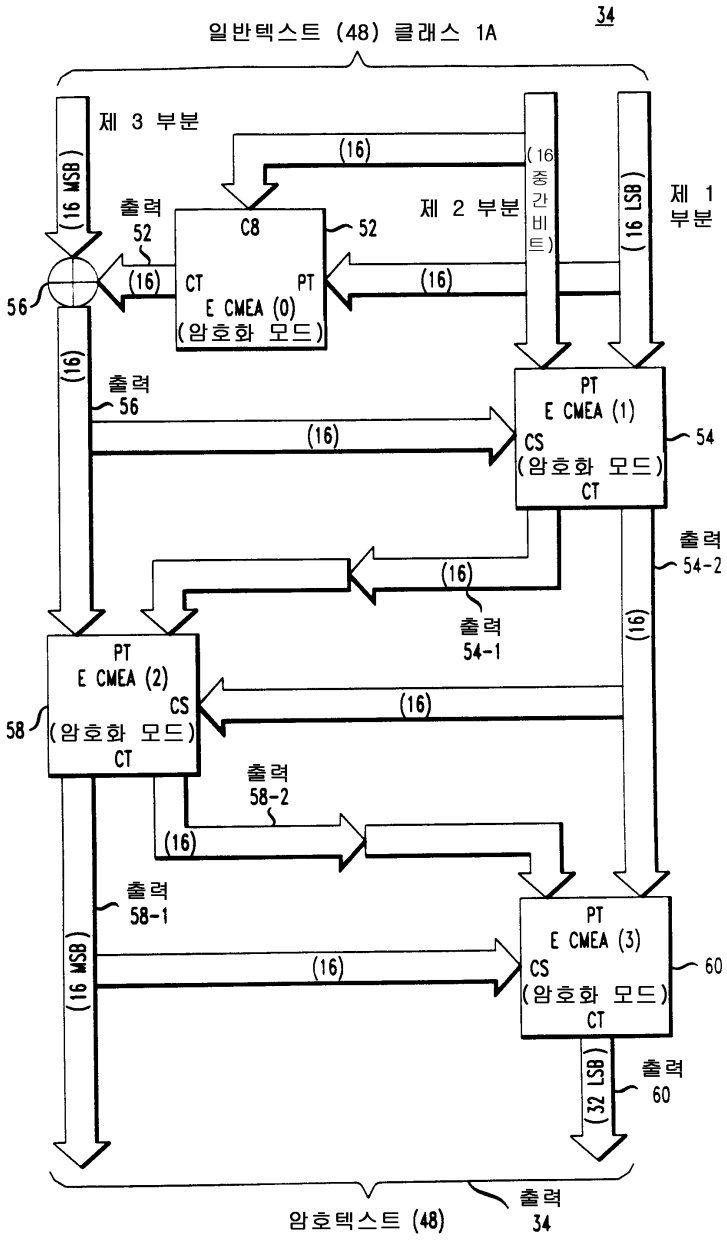

스피치 표본
2560
스피치 코더
32
클래스 1A 비트 (48)
출력 32-1
클래스 1B 비트 (48)
출력 32-2
클래스 2 비트 (52)
출력 32-3
블럭 암호화기 1A
34
1B/2 키 스트림 생성기 (KSG MODE)
36
(48 및 52)
(52)
40
38
(48)
7-비트 CRC
42
(7)
1/2 레이트 컨볼루션 코더
5 테일비트
44
(216)
평처
46
(206)
2 슬롯 인터리버
48
(280)
30

도면3

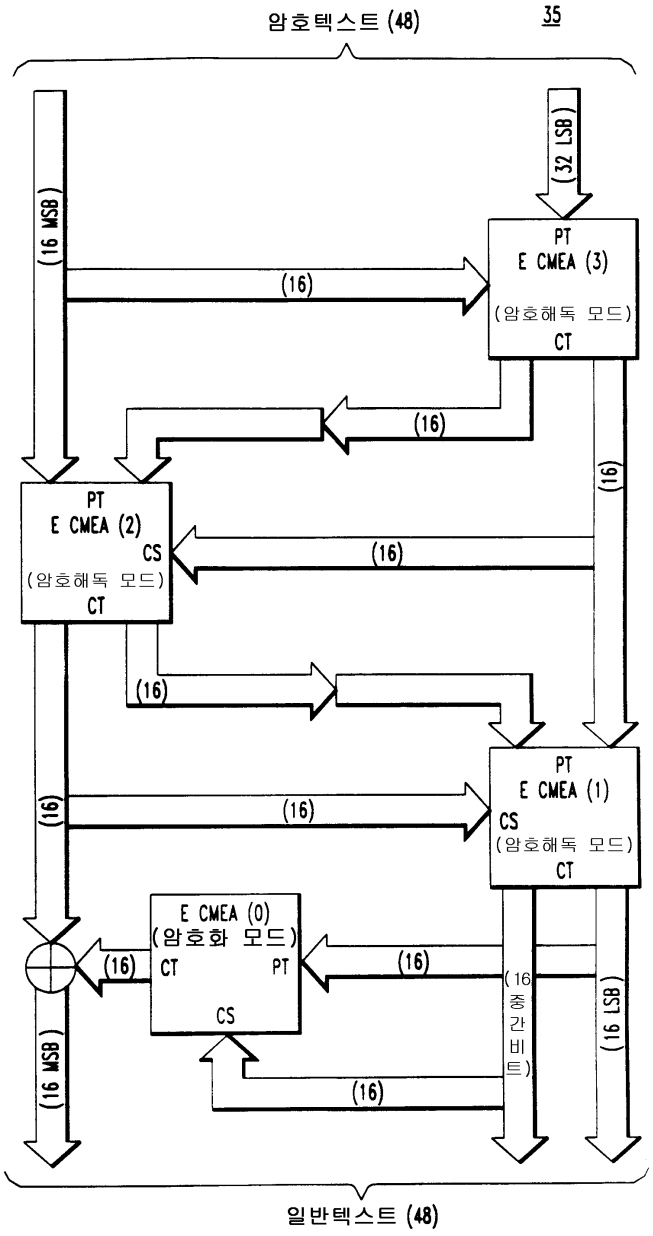
45

<table>
<tr><td colspan="3">148개의 인코딩된 스피치 비트</td></tr>
<tr><td colspan="2">80개의 제 1 레벨 비트</td><td>68개의 제 2 레벨 비트</td></tr>
<tr><td>출력 32-1</td><td>출력 32-2</td><td>출력 32-3</td></tr>
<tr><td>제 1 블럭</td><td>제 2 블럭</td><td>제 3 블럭</td></tr>
<tr><td>48개의 클래스 1A 비트</td><td>48개의 클래스 1B 비트
32개의 제 1 레벨 비트
16개의 제 2 레벨 비트</td><td>52개의 클래스 2 비트</td></tr>
</table>

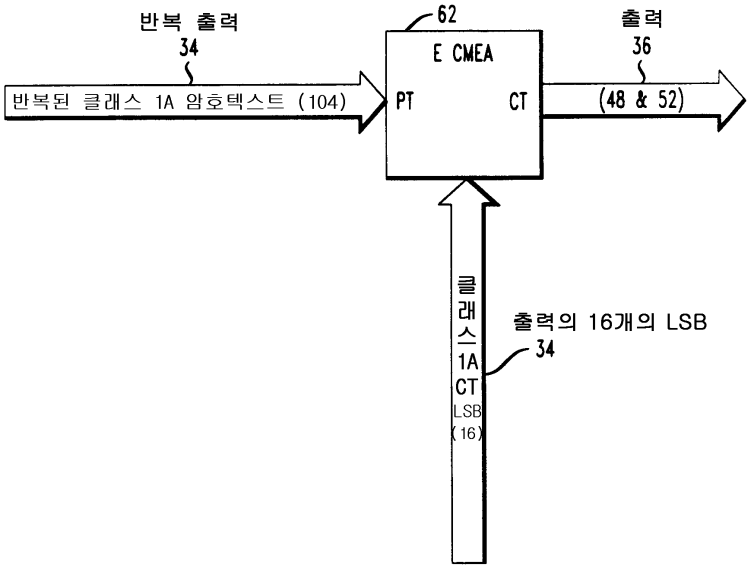
도면4


일반텍스트 (48) 클래스 1A
34
제 3 부분
(16 MSB)
(16)
(16 중간비트)
제 2 부분
(16 LSB)
제 1 부분
출력 52
C8
52
(16)
CT
PT
E CMEA (0)
(암호화 모드)
56
(16)
출력 56
(16)
PT
E CMEA (1)
CS
(암호화 모드)
CT
54
출력 54-2
(16)
출력 54-1
PT
E CMEA (2)
CS
(암호화 모드)
CT
58
(16)
(16)
출력 58-2
출력 58-1
(16 MSB)
(16)
PT
E CMEA (3)
CS
(암호화 모드)
CT
60
(32 LSB)
출력 60
암호텍스트 (48)
출력 34

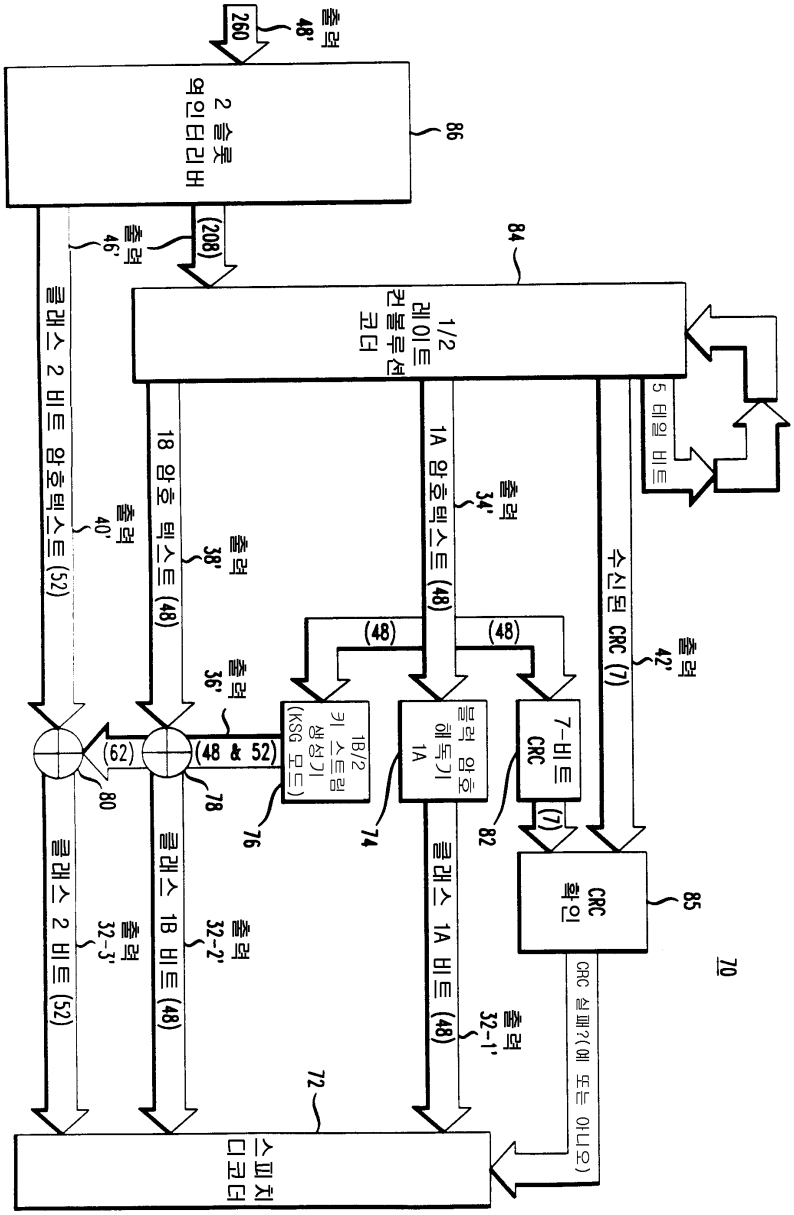
도면5


암호텍스트 (48)
35
(16 MSB)
(32 LSB)
PT
E CMEA (3)
(암호해독 모드)
CT
(16)
(16)
(16)
PT
E CMEA (2)
CS
(암호해독 모드)
CT
(16)
(16)
(16)
PT
E CMEA (1)
CS
(암호해독 모드)
CT
(16)
(16)
E CMEA (0)
(암호화 모드)
CT
PT
CS
(16)
(16)
(16 중간 비트)
(16 MSB)
(16 LSB)
(16)
일반텍스트 (48)

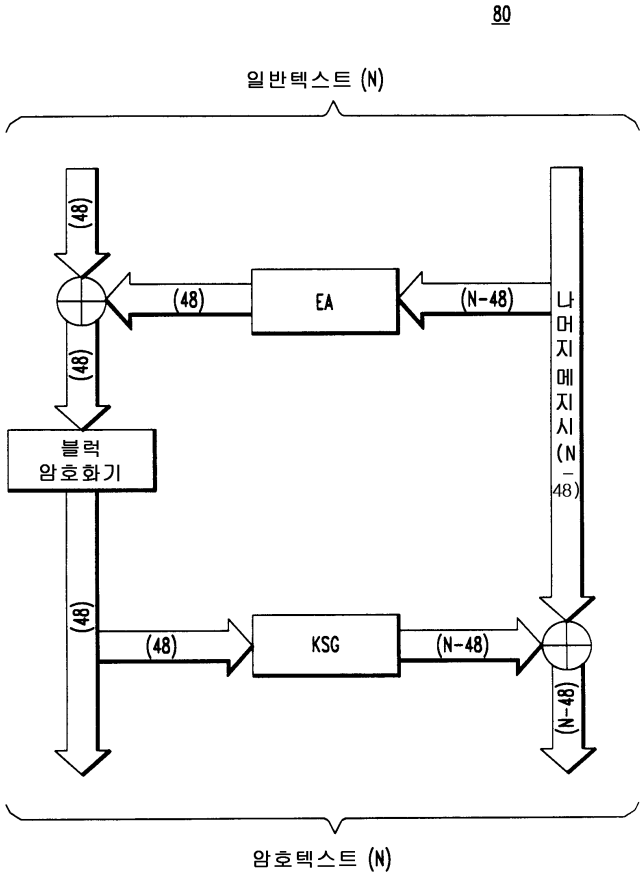
도면6


반복 출력
34
반복된 클래스 1A 암호텍스트 (104)
62
E CMEA
PT
CT
출력
36
(48 & 52)
클래스 1A CT LSB (16)
출력의 16개의 LSB
34

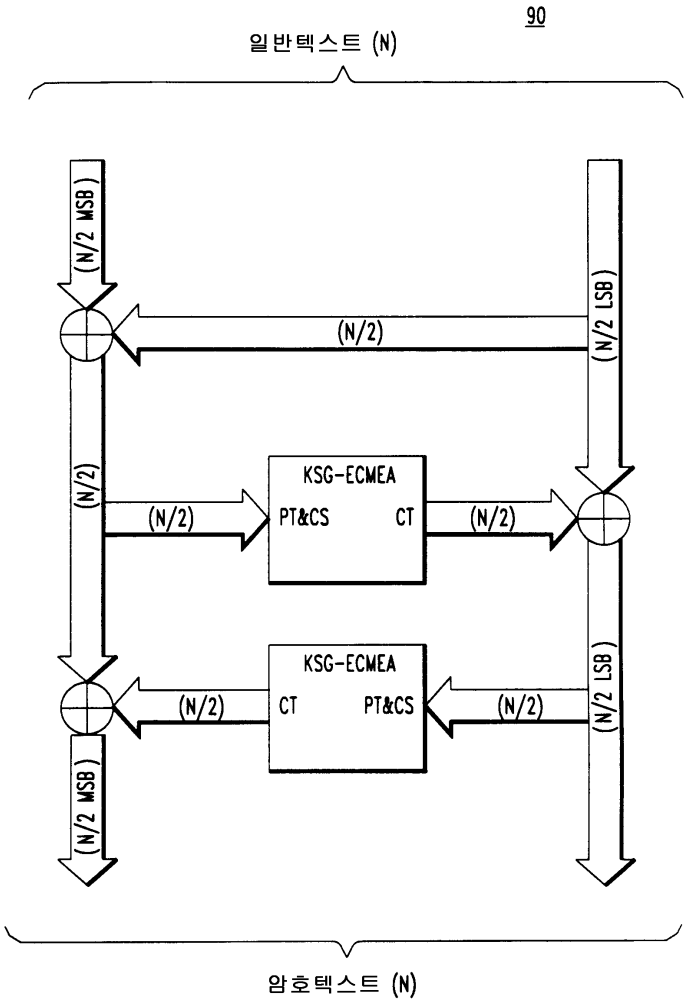
도면7


출력
48'
260
2 슬롯
역인터리버
86
출력
46'
(208)
84
1/2
레이트
컨볼루션
코더
5 테일 비트
수신된 CRC (7)
출력
42'
클래스 2 비트 암호텍스트 (52)
출력
40'
1B 암호 텍스트 (48)
출력
38'
1A 암호텍스트 (48)
출력
34'
(48)
(48)
출력
36'
1B/2
키 스트림
생성기
(KSG 모드)
블럭 암호
해독기
1A
7-비트
CRC
(62)
(48 & 52)
80
78
76
74
82
(7)
CRC
확인
85
70
클래스 2 비트 (52)
출력
32-3'
클래스 1B 비트 (48)
출력
32-2'
클래스 1A 비트 (48)
출력
32-1'
CRC 실패?(예 또는 아니오)
72
스피치
디코더

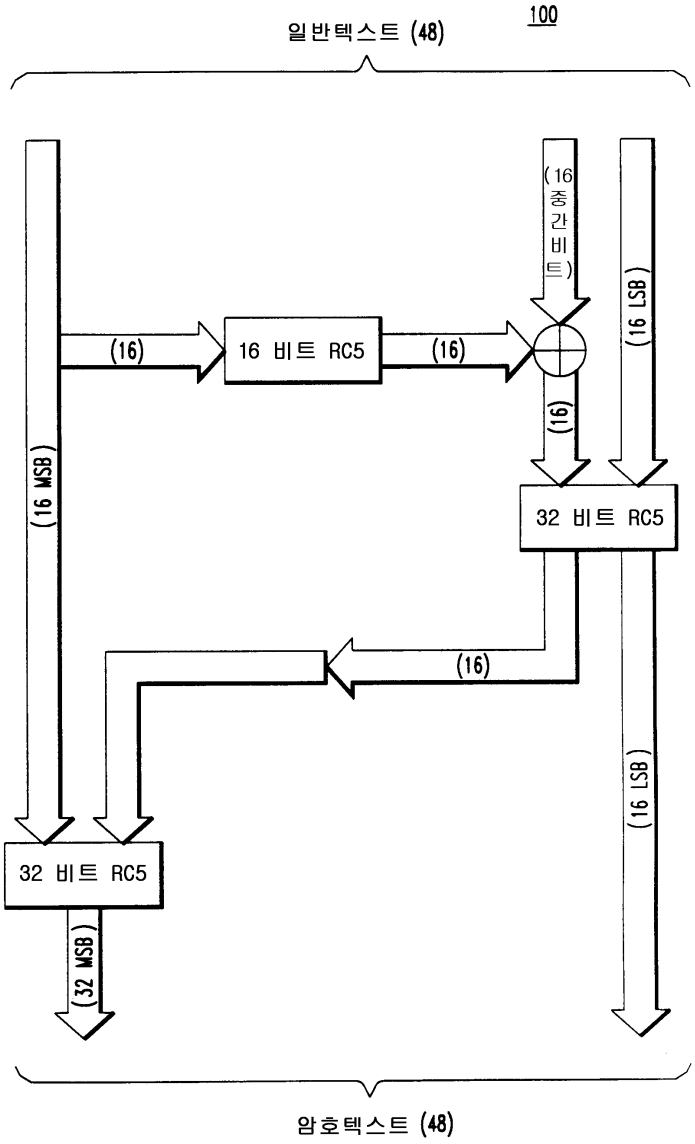
도면8


80
일반텍스트 (N)
(48)
(48)
EA
(N-48)
나머지 메시지 (N-48)
(48)
블럭 암호화기
(48)
(48)
KSG
(N-48)
(N-48)
암호텍스트 (N)

도면9


90
일반텍스트 (N)
(N/2 MSB)
(N/2 LSB)
(N/2)
(N/2)
KSG-ECMEA
PT&CS
CT
(N/2)
(N/2)
KSG-ECMEA
CT
PT&CS
(N/2)
(N/2 LSB)
(N/2 MSB)
암호텍스트 (N)

도면10


100
일반텍스트 (48)
(16 중간 비트)
(16 LSB)
(16)
16 비트 RC5
(16)
(16 MSB)
(16)
32 비트 RC5
(16)
(16 LSB)
32 비트 RC5
(32 MSB)
암호텍스트 (48)