(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0013960
(43) 공개일자 2018년02월07일

(51) 국제특허분류(Int. Cl.)
*H04L 29/06* (2006.01) *G06F 17/30* (2006.01)
*H04M 7/00* (2006.01) *H04W 12/04* (2009.01)
*H04W 12/08* (2009.01)
(52) CPC특허분류
*H04L 63/065* (2013.01)
*G06F 17/30312* (2013.01)
(21) 출원번호 10-2017-7035757
(22) 출원일자(국제) 2016년05월27일
심사청구일자 없음
(85) 번역문제출일자 2017년12월12일
(86) 국제출원번호 PCT/EP2016/061966
(87) 국제공개번호 WO 2016/193135
국제공개일자 2016년12월08일
(30) 우선권주장
14/726,108 2015년05월29일 미국(US)

(71) 출원인
**나그라비젼 에스에이**
스위스 체하-1033 세조-쉬르-로잔느 루뜨 드 쥬네브 22-24
(72) 발명자
**페르, 프랑소와**
스위스 1033 체슈아-주르-로잔, 루트 드 제네바 22-24, 나그라비젼 에스에이 내
**맥체티, 마르코**
이탈리아 22070 카스네이트 콘 버네이트, 비아 보카치오 42
*(뒷면에 계속)*
(74) 대리인
**김해중**

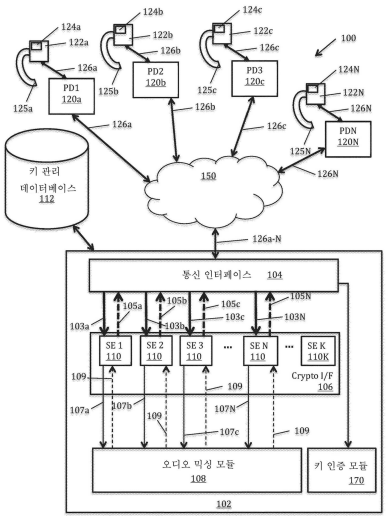
전체 청구항 수 : 총 15 항

(54) 발명의 명칭 **보안 VOIP 다자 통화를 수행하는 시스템 및 방법**

## (57) 요 약

보안 컨퍼런스 콜을 성립시키는 시스템 및 방법이 제공된다. 일 예시적인 실시예에서, 중앙 컨퍼런스 콜 서버는, 보안 소자를 포함하고 대응하는 참가자 장치에 접속된 액세서리 장치와 점대점 접속을 성립시킨다. 컨퍼런스 콜 서버는 액세서리 장치와 통신되는 매체 신호의 스크램블링 및 언스크램블링하도록 구성된 복수의 보안 소자에 대한 인터페이스를 포함한다. 다른 예에서, 참가자 장치 중 하나는 중앙 컨퍼런스 콜 서버로서 동작한다. 또 다른 예에서, 참가자 장치는, 거기에 접속된 모든 액세서리 장치 사이의 점대점 접속을 통해서 컨퍼런스 콜에서 통신한다. 액세서리 장치는, 액세서리 장치 사이에서 통신되는 매체 신호를 해독 및 암호화하는 보안 소자를 포함한다.

*대 표 도* - 도1



(52) CPC특허분류
*H04L 65/1006* (2013.01)
*H04L 65/403* (2013.01)
*H04L 65/605* (2013.01)
*H04M 7/006* (2013.01)
*H04W 12/04* (2013.01)
*H04W 12/08* (2013.01)
(72) 발명자
**가우테론, 로랑**
스위스 1033 체슈아-주르-로잔, 루트 드 제네바 22-24, 나그라비전 에스에이 내
**페린, 제롬**
스위스 1122 로마넬 수르 모르쥬, 뤼 데 라 포스테 3

# 명 세 서

## 청구범위

### 청구항 1

서버에서 컨퍼런스 콜을 수행하는 방법으로서,

컨퍼런스 콜 통신에서 복수의 참가자 장치 각각으로부터 인바운드 통신을 수신하는 단계 - 상기 복수의 참가자 장치 각각은, 오디오 신호를 자신이 저장하고 있는 참가자 키 정보를 사용해서 스크램블 및 언스크램블하도록 구성된 보안 소자를 구비한 액세서리 장치에 대한 접속을 포함하고, 상기 인바운드 통신은, 보안 매체 세션의 참가자 엔드포인트에서 상기 액세서리 장치로부터 통신되며 상기 참가자 장치에 의해 릴레이되는 스크램블된 매체 신호를 포함함 - 와,

각각의 인바운드 통신으로부터의 상기 스크램블된 매체 신호를 복수의 서버 보안 소자를 가진 암호화 인터페이스로 릴레이하는 단계 - 상기 서버 보안 소자는, 상기 복수의 액세서리 장치 중 대응하는 것과의 상기 보안 매체 세션의 서버측 엔드포인트에서, 상기 서버 보안 소자에 의해서 유지되며 상기 서버에 의한 액세스는 불가능한 서버 키 정보를 이용해서, 오디오 신호를 스크램블 및 언스크램블하도록 구성됨 - 와,

상기 복수의 서버 보안 소자 각각에 의해서, 상기 복수의 참가자 장치와의 상기 매체 세션에서 수신된 스크램블된 매체 신호 각각으로부터 생성된 오디오 신호를, 상기 암호화 인터페이스로부터 수신하는 단계와,

상기 복수의 오디오 신호를 믹스해서 컨퍼런스 콜 데이터를 생성하여서 믹스된 오디오 신호로서 모든 사용자에게 통신하는 단계와,

상기 믹스된 오디오 신호를 상기 암호화 인터페이스에 제공하고, 상기 믹스된 오디오 신호를 상기 복수의 서버 보안 소자 각각이 스크램블해서 복수의 아웃바운드 스크램블된 매체 신호를 생성하는 단계와,

상기 아웃바운드 스크램블된 매체 신호를 상기 복수의 참가자 장치 각각으로 아웃바운드 통신으로서 통신하는 단계

를 포함하는 방법.

### 청구항 2

제 1 항에 있어서,

상기 복수의 참가자 장치의 각각의 장치로부터 보안 통신 접속을 개시하라는 요청을 수신하는 단계와,

상기 보안 접속을 개시하라는 요청 각각에 응답해서, 각각의 액세서리 장치로부터 각각의 대응하는 서버 보안 소자로 키 정보를 릴레이함으로써, 각각의 참가자 장치에 접속된 액세서리 장치와 복수의 서버 보안 소자 중 대응하는 것 사이의 상기 보안 매체 세션을 성립하는 단계

를 더 포함하는

방법.

### 청구항 3

제 2 항에 있어서,

상기 보안 매체 세션을 성립하는 단계에서, 상기 서버 보안 소자 각각은 키 교환 방법을 수행해서, 상기 대응하는 액세서리 장치로부터의 스크램블된 매체 부분을 언스크램블하기 위한 서버 해독 키 및 상기 대응하는 액세서리 장치에 의해 언스크램블하기 위해 상기 믹스된 오디오 신호를 스크램블하기 위한 서버 암호화 키를 생성하는

방법.

**청구항 4**

제 1 항에 있어서,

상기 복수의 참가자 장치의 각각의 장치로부터 보안 통신 접속을 개시하라는 요청을 수신하는 단계 - 상기 각각의 참가자 장치로부터의 요청은 전체 키(a global key)를 포함함 - 와,

상기 전체 키가 상기 요청을 수신한 컨퍼런스 콜 서버에서 컨퍼런스 콜에 참여하는데 사용하기에 유효한지 판정함으로써, 상기 전체 키를 인증하는 단계

를 더 포함하는

방법.

**청구항 5**

제 1 항 내지 제 4 항 중 어느 한 항에 있어서,

상기 컨퍼런스 콜 서버에서 수행되는 컨퍼런스 콜에 참가하기 위해서 상기 참가자 장치 중 하나로부터 전체 키에 대한 요청을 수신하는 단계와,

상기 전체 키를 키 관리 데이터베이스로부터 취득하는 단계와,

상기 전체 키를 요청하는 상기 참가자 장치로 송신하는 단계

를 더 포함하는

방법.

**청구항 6**

제 1 항에 있어서,

상기 복수의 참가자 장치의 각각의 장치로부터 보안 통신 접속을 개시하라는 요청을 수신하는 단계 - 상기 각각의 참가자 장치로부터의 요청은 상기 참가자 장치의 사용자가 속하는 그룹을 나타내는 세그먼트 키를 포함함 - 와,

상기 세그먼트 키를, 상기 요청을 수신한 컨퍼런스 콜 서버에서 컨퍼런스 콜에 참여하는데 사용하기에 유효한지 판정함으로써, 인증하는 단계

를 더 포함하는

방법.

**청구항 7**

제 6 항에 있어서,

상기 보안 통신 접속을 개시하라는 요청을 수신하는 단계 이전에,

상기 참가자 장치 중, 상기 참가자 장치의 사용자가 속하는 그룹에 대응하는 참가자 장치로부터 세그먼트 키에 대한 요청을 수신하는 단계와,

상기 세그먼트 키를 키 관리 데이터베이스로부터 취득하는 단계와,

상기 세그먼트 키를 요청하는 상기 참가자 장치로 송신하는 단계

를 더 포함하는

방법.

**청구항 8**

컨퍼런스 콜 서버로서,

데이터 네트워크를 통해서 복수의 참가자 장치와 통신하도록 구성된 통신 인터페이스 - 상기 참가자 장치는 각각 참가자 키 정보를 유지하기 위한 참가자 보안 소자 및 오디오 입력 및 출력 장치를 구비한 액세서리 장치에 접속되고, 상기 통신 인터페이스는, 상기 관련된 참가자 장치에 의해서 릴레이되는 대응하는 보안 매체 세션으로 각각의 액세서리 장치와 스크램블된 오디오 신호를 통신함 - 와,

복수의 서버 보안 소자에 접속된 암호화 인터페이스 - 상기 서버 보안 소자는, 대응하는 참가자 장치에 접속된 상기 액세서리 장치와 통신되는 오디오 신호를, 자신이 저장하고 있는 서버 보안 키 정보를 사용해서 스크램블 및 언스크램블하도록 구성됨 - 와,

오디오 신호를 믹스해서 컨퍼런스 콜 데이터를 생성하여 상기 암호화 인터페이스로 제공하는 오디오 믹서 - 상기 오디오 신호는 인커밍 스크램블된 오디오 신호를 상기 복수의 참가자 장치에 접속된 상기 액세서리 장치에 대응하는 상기 서버 보안 소자가 언스크램블한 것이고, 상기 컨퍼런스 콜 데이터는 믹스된 오디오 신호로서 상기 컨퍼런스 콜의 상기 사용자에게 통신됨 -

를 포함하고,

상기 암호화 인터페이스는, 각각의 서버 보안 소자가 제공하는 스크램블된 믹스된 오디오 신호를 생성해서 상기 통신 인터페이스를 통해서 각각의 참가자 장치로 통신해서, 관련된 액세서리 장치로 릴레이하는

컨퍼런스 콜 서버.

**청구항 9**

제 8 항에 있어서,

상기 암호화 인터페이스는 상기 복수의 서버 보안 소자에 대한 하드웨어 인터페이스를 포함하고,

상기 복수의 서버 보안 소자는 복수의 하드웨어 보안 모듈을 포함하는

컨퍼런스 콜 서버.

**청구항 10**

제 9 항에 있어서,

상기 복수의 하드웨어 보안 모듈은, 각각이 보안 소자로서 구성되는 복수의 마이크로 SD 카드를 포함하는

컨퍼런스 콜 서버.

**청구항 11**

제 9 항 또는 제 10 항에 있어서,

상기 복수의 서버 보안 소자에 대한 상기 하드웨어 인터페이스는, 스마트 카드 인터페이스, BGA(ball grid array) 인터페이스, SMD(surface mount device) 인터페이스 및 인쇄 회로 기판 인터페이스로 이루어진 그룹에서 선택되는

컨퍼런스 콜 서버.

**청구항 12**

제 8 항 내지 제 11 항 중 어느 한 항에 있어서,

상기 서버 보안 소자 각각의 상기 서버 키 정보는, 상기 서버 보안 소자와의 매체 세션으로 접속된 상기 액세서리 장치의 상기 참가자 보안 소자로부터 수신한 키 정보를 사용해서 상기 스크램블된 매체 세션의 개시 동안에 수행되는 키 교환 정보를 이용해서 생성되는 서버 암호화 키 및 서버 해독 키를 포함하고,

상기 서버 해독 키는, 대응하는 상기 액세서리 장치로부터의 상기 스크램블된 오디오 신호를 언스크램블하는데 사용되고,

상기 서버 암호화 키는, 대응하는 상기 액세서리 장치에 의해 언스크램블하기 위해 상기 믹스된 오디오 신호를 스크램블하는데 사용되는

컨퍼런스 콜 서버.

**청구항 13**

제 8 항 내지 제 12 항 중 어느 한 항에 있어서,

상기 컨퍼런스 콜 서버에 대한 보안 접속을 개시하는 동안에 상기 참가자 장치가 제공하는 전체 참가자 키를 인증하는 참가자 장치 인증 모듈

을 더 포함하고,

상기 참가자 장치 인증 모듈은 (i) 상기 전체 참가자 키와 관련된 날자 및 시간 및 (ii) 상기 컨퍼런스 콜 서버에 대한 상기 보안 접속을 개시하는 동안 상기 참가자 장치가 제공하는 세그먼트 키 중 적어도 하나를 확인하도록(validate) 구성되고,

상기 세그먼트 키는 상기 참가자 장치의 상기 사용자의 그룹 식별자를 나타내는

컨퍼런스 콜 서버.

**청구항 14**

제 13 항에 있어서,

상기 전체 참가자 키를 유지하고 상기 전체 참가자 키를 상기 참가자 장치에 의해 수행되는 등록 처리 동안 상기 참가자 장치 중 하나에 제공하도록 구성된 키 관리 데이터베이스

를 더 포함하는

컨퍼런스 콜 서버.

**청구항 15**

제 14 항에 있어서,

상기 키 관리 데이터베이스는 또한 그룹 식별자를 나타내는 값을 가진 세그먼트 키를 유지하고,

상기 키 관리 데이터베이스는 상기 등록 처리 동안에 상기 참가자 장치 중 하나에 상기 세그먼트 키를 제공하도록 구성되는

컨퍼런스 콜 서버.

## 발명의 설명

### 기 술 분 야

[0001] (관련 출원과의 상호 참조)

[0002] 본 발명은 2015년 5월 29일 출원된 미국 출원 제14/726,108호 "SYSTEMS AND METHODS FOR CONDUCTING SECURE VOIP MULTI-PARTY CALLS"를 우선권으로 주장한다.

### 배 경 기 술

[0003] 사람들은 끊임없이 무선으로 통신하고 있다. 이를 가능하게 장치 중에는 개인용 모바일 장치라는 것 있다. 개인용 모바일 장치의 예로는 특히 셀 폰, 스마트 폰, 워키토키 및 휴대형 핫스팟이 있다. 개인용 모바일 장치는 예컨대, 휴대될 수도 있고(워키토키로 사용되는 경우에), 신체에 장착될 수도 있으며, 혹은 차량(차량의 루프와 같은)에 부착될 수도 있다.

[0004] 무선 신호는 비교적 용이하게 인터셉트될 수 있다는 점에서, 개인용 모바일 장치와의(혹은 이들 사이의) 통신은 제3자에 의한 통신의 인터셉트를 방지하도록 암호화된다. 암호화는 가청 음성 혹은 다른 데이터를 이해할 수 없는 음성으로 변환하는 처리이고, 해독은 이해할 수 없는 음성을 원래의 가청 음성으로 되돌리는 처리이다. 암호화 및 해독에 사용되는 각각의 알고리즘은 종종 함께 사이퍼(cipher)라고 한다. 일반적인 사이퍼의 예로는 특히, AES(Advanced Encryption Standard), 블로피시, 3DES(Triple Data Encryption Algorithm) 및 RC4 등을 들 수 있다.

[0005] 호출자(caller) 및/또는 통신되는 음성이나 데이터를 암호화 및 인증함으로써, 점대점 통신에 포함되는 개인용 모바일 장치들 사이의 통신의 참가자의 보안, 프라이버시 및 기밀성을 증가시켰다. 특히 "VOIP(Voice-over-Internet Protocol)" 인프라스트럭처를 통한 컨퍼런스 콜과 같은 다자간 콜의 경우에, 오디오 및 콜 데이터가 보안되지 않은 인프라스트럭처에서는 문제가 남아있다. 호출자는 개인용 모바일 장치로부터 콜이 올 때 헤드셋과 같은 액세서리 장치를 종종 이용한다. 헤드셋 엔드포인트 사이에 보안 매체 세션이 성립될 수는 있지만, 컨퍼런스 콜로 접속하는 것은, 음성 및 콜 데이터가 서버의 통신 인터페이스에서 신뢰되지 않는 컴포넌트로 노출되는 것을 포함할 수 있다.

[0006] 이와 같은 견지에서, 특히 VOIP 콜로 컨퍼런스 콜에 참여하는 호출자의 보안, 프라이버시 및 기밀성을 향상시킬 필요가 있다.

## 발명의 내용

### 과제의 해결 수단

[0007] 이와 같은 견지에서, 컨퍼런스 콜 서버가 컨퍼런스 콜을 호스팅하고 유지하는 방법이 제공된다. 이 방법의 예에 따라서, 서버는 컨퍼런스 콜 통신의 복수의 참가자 장치 각각으로부터의 인바운드 통신을 수신한다. 복수의 참가자 장치 각각은, 오디오 신호를 자신이 저장하고 있는 참가자 키 정보를 사용해서 스크램블 및 언스크램블하도록 구성된 보안 소자를 구비한 액세서리 장치에 대한 접속을 포함한다. 인바운드 통신은, 보안 매체 세션의 참가자 엔드포인트에서 액세서리 장치로부터 통신되며 참가자 장치에 의해 릴레이되는 스크램블된 매체 신호를 포함한다. 각각의 인바운드 통신으로부터의 이 스크램블된 매체 신호는 복수의 서버 보안 소자를 가진 암호화 인터페이스로 릴레이된다. 서버 보안 소자는, 복수의 액세서리 장치 중 대응하는 것과의 보안 매체 세션의 서버 측 엔드포인트에서, 서버 보안 소자에 의해서 유지되며 서버에 의한 액세스는 불가능한 서버 키 정보를 이용해서, 오디오 신호를 스크램블 및 언스크램블하도록 구성된다. 암호화 인터페이스로부터 오디오 신호가 수신되며, 이 오디오 신호는 복수의 서버 보안 소자 각각에 의해서, 복수의 참가자 장치와의 매체 세션에서 수신된 스크램블된 매체 신호 각각으로부터 생성된다. 복수의 오디오 신호는 믹스되어서 컨퍼런스 콜 데이터를 생성하고, 이는 믹스된 오디오 신호로서 모든 사용자에게 통신된다. 믹스된 오디오 신호는 암호화 인터페이스에 제공되어서 복수의 서버 보안 소자 각각이 믹스된 오디오 신호를 스크램블하여서 복수의 아웃바운드 스크램블된 매체 신호를 생성한다. 각각의 아웃바운드 스크램블된 매체 신호는 아웃바운드 통신으로서 복수의 참가자 장치 각각으로 통신된다.

[0008] 이 방법의 일 실시예에서, 서버는 또한 복수의 참가자 장치의 각각의 장치로부터 보안 통신 접속을 개시하라는 요청을 수신할 수 있다. 이후 서버는 보안 통신 접속을 개시하라는 요청 각각에 응답해서, 각각의 참가자 장치

에 접속된 액세서리 장치와 복수의 서버 보안 소자 중 대응하는 것 사이의 보안 매체 세션을 성립할 수 있다. 보안 매체 세션은, 각각의 액세서리 장치로부터 각각의 대응하는 서버 보안 소자로 키 정보를 릴레이함으로써 성립될 수 있다.

[0009] 이 방법의 적어도 다른 실시예에서 보안 매체 세션을 성립할 때, 각각의 서버 보안 소자는 키 교환 방법을 수행할 수 있다. 이 키 교환 방법은 대응하는 액세서리 장치로부터의 스크램블된 매체 부분을 언스크램블하기 위한 서버 해독 키 및 대응하는 액세서리 장치에 의해 언스크램블하기 위해 믹스된 오디오 신호를 스크램블하기 위한 서버 암호화 키를 생성한다.

[0010] 방법의 적어도 하나의 실시예에서, 키 교환 방법은 디피-헬만 키 교환(Diffie-Hellman key exchange) 방법을 사용해서 수행될 수 있다.

[0011] 또 다른 예시적인 구현예에서, 컨퍼런스 콜 서버가 제공된다. 컨퍼런스 콜 서버는 데이터 네트워크를 통해서 복수의 참가자 장치와 통신하도록 구성된 통신 인터페이스를 포함한다. 각각의 참가자 장치는 참가자 키 정보를 유지하기 위한 참가자 보안 소자 및 오디오 입력 및 출력 장치를 구비한 액세서리 장치에 접속된다. 통신 인터페이스는, 관련된 참가자 장치에 의해서 릴레이되는 대응하는 보안 매체 세션으로 각각의 액세서리 장치와 스크램블된 오디오 신호를 통신한다. 대응하는 참가자 장치에 접속된 액세서리 장치와 통신되는 오디오 신호를, 자신이 저장하고 있는 서버 보안 키 정보를 사용해서 스크램블 및 언스크램블하도록 구성된 복수의 서버 보안 소자에 암호화 인터페이스가 접속된다. 복수의 참가자 장치에 접속된 액세서리 장치에 대응하는 서버 보안 소자가 인커밍 스크램블된 오디오 신호를 언스크램블한 오디오 신호를, 오디오 믹서가 믹스한다. 이 오디오 믹서는 오디오 신호를 믹스해서 컨퍼런스 콜 데이터를 생성하고, 이는 컨퍼런스 콜의 사용자에게 믹스된 오디오 신호로서 통신된다. 믹스된 오디오 신호는 암호화 인터페이스에 제공된다. 서버 보안 소자 각각은 스크램블된 오디오 신호를 생성해서 암호화 인터페이스로 제공하고, 암호화 인터페이스는 이를 통신 인터페이스를 통해서 각각의 참가자 장치로 통신해서 관련 액세서리 장치로 릴레이시킨다.

[0012] 본 발명의 다른 장치, 기기, 시스템, 방법, 특성 및 이점은 이하의 도면 및 상세한 설명을 실시하는 당업자에게 자명할 것이다. 모든 추가적인 시스템, 방법, 특성 및 이점은 이 설명에 포함되고, 본 발명의 범주 내에 들어가며, 첨부된 청구항에 의해 보호되도록 했다.

## *도면의 간단한 설명*

[0013] 다양한 예시적인 실시예를 도면을 참조해서 설명하며, 도면에서 같은 참조 번호는 동일한 개체를 가리킨다.

도 1은 중앙 컨퍼런스 콜 서버를 사용해서 컨퍼런스 콜을 수행하는 예시적인 시스템의 개략도,

도 2는 복수의 참가자 장치 사이에서 컨퍼런스 콜을 수행하는 시스템의 예를 나타내는 개략도,

도 3은 참가자 장치 중 하나가 컨퍼런스 콜 서버로서 동작하는 컨퍼런스 콜을 수행하는 예시적인 시스템을 나타내는 개략도,

도 4는 컨퍼런스 콜 기능이 참가자 장치들에 분산되는, 복수의 참가자 장치 사이에서 컨퍼런스 콜을 수행하는 시스템의 예를 나타내는 개략도이다.

## *발명을 실시하기 위한 구체적인 내용*

[0014] 도 1은 중앙 컨퍼런스 콜 서버(102)를 사용해서 컨퍼런스 콜을 수행하는 예시적인 시스템(100)의 개략도이다. 컨퍼런스 콜 서버(102)는 통신 인터페이스(104), 암호화 인터페이스(106) 및 오디오 믹싱 모듈(108)을 포함한다. 컨퍼런스 콜 서버(102)는 N개의 참가자 장치(120a~n)의 컨퍼런스 콜을 호스팅하는 것으로 도시되어 있다. 컨퍼런스 콜은 데이터 네트워크(즉, 인터넷(105))를 통한 VOIP 접속으로 수행된다. 각각의 참가자 장치(120a~n)는 컨퍼런스 콜 서버(102)와 VOIP 접속을 성립시킴으로써 컨퍼런스 콜에 전화를 건다. VOIP 접속은, 시스템(100)의 예시적인 구현예에 대한 설명에 개시되어 있는 바와 같이, 엔드포인트 사이에서 보안되도록 성립되어 있다. 통신 인터페이스(104)는 참가자 장치(120a~n)와의 데이터 네트워크(150)를 통한 VOIP 접속을 관리하도록 구성된다.

[0015] 각각의 참가자 장치(120a~n)는 액세서리 장치(122a~n)에 접속되고, 이 액세서리 장치(122a~n)는 오디오 입력(125a~n) 및 오디오 출력 장치(도시 생략), 및 참가자 키 정보를 관리하는 참가자 보안 소자(124a~n)를 구비하고 있다. 통신 인터페이스(104)는 대응하는 보안 매체 세션(126a~n)으로 스크램블된 오디오 신호를 각각의 액세서리 장치(122a~n)와 통신한다. 각각의 참가자 장치(120a~n)에서, 대응하는 보안 매체 세션(126a~n)이 관련된

액세서리 장치(122a~n)로 릴레이됨으로써, 액세서리 장치(122a~n) 내의 참가자 보안 소자(124a~n)가 보안 매체 세션(126a~n)의 하나의 엔드포인트가 되게 된다. 각각의 액세서리 장치(122a~n)의 참가자 보안 소자(124a~n)는 대응하는 보안 매체 세션(126a~n)의 매체 부분을 스크램블링 및 언스크램블링하도록 구성되며, 매체 부분은 일반적인 컨퍼런스 콜에서 적어도 오디오 신호를 포함하지만, 일부 실시예에서는 비디오를 포함할 수도 있다.

[0016] 암호화 인터페이스(106)는 복수의 서버 보안 소자(110a~n)에 접속되고, 이 서버 보안 소자(110a~n) 각각은 자신이 저장하고 있는 서버 키 정보를 이용해서, 대응하는 참가자 장치(120a~n)에 접속된 액세서리 장치(122a~n)와 통신되는 오디오 신호를, 스크램블 및 언스크램블하도록 구성되어 있다. 암호화 인터페이스(106)는, 스크램블된 오디오 신호를, 보안 매체 세션(126a~n)으로 서버 보안 소자(110a~n)와 릴레이함으로써, 보안 매체 세션(126a~n)을 통한 통신에 접속되고, 이로써 서버 보안 소자(110a~n)는 복수의 보안 매체 세션(126a~n)의 서버측 엔드포인트를 포함하게 된다. 도 1에 도시된 바와 같이, 제 1 보안 매체 세션(126a)은, 제 1 참가자 장치(120a)의 하나의 엔드포인트로서, 제 1 액세서리 장치(122a) 내의 제 1 참가자 보안 소자(124a)에 접속된다. 제 1 참가자 장치(120a)는 제 1 보안 매체 세션(126a)을 인터넷(150) 그리고 컨퍼런스 콜 서버(102)의 통신 인터페이스(104)에 릴레이한다. 컨퍼런스 콜 서버(102)는 제 1 보안 매체 세션(126a)을 제 1 서버 보안 소자(110a)로 릴레이한다. 제 2 부터 n번째 매체 세션(126b~n)도 유사한 방식으로 성립된다.

[0017] 서버 보안 소자(110a~n)는 보안 매체 세션(126a~n)의 서버측 엔드포인트에서 컨퍼런스 콜 서버(102)와 통신되는 매체의 모든 스크램블링 및 언스크램블링을 수행하도록 구성된다. 각각의 서버 보안 소자(110a~n)는 암호화 및 해독 기능을 수행하도록, 암호화 및 해독 모듈 그리고 적어도 하나의 프로세서를 갖고 구성될 수 있다. 각각의 서버 보안 소자(110a~n)는 또한 매체 세션의 개시 동안에 생성되는 서버 키 정보를 저장하고 이는 매체 신호의 암호화 및 해독을 수행하는데 사용된다. 시스템(100)의 일부 예에서, 서버 보안 소자(110a~n)는 매체 신호와 관련된 모든 보안 처리를 수행하고, 이러한 처리를 수행하는데 사용되는 모든 보안 정보를 저장한다. 컨퍼런스 콜 서버(102)는 서버 보안 소자(110a~n)가 사용하는 어떠한 암호화 정보에도 액세스할 수 없다.

[0018] 도 1에 도시된 바와 같이, 서버 보안 소자(110a~n)는 인커밍 스크램블된 오디오 신호(103a~n)를 수신한다. 대응하는 서버 보안 소자(110a~n)는 이 인커밍 스크램블된 오디오 신호(103a~n)를 언스크램블해서, 언스크램블된 오디오 신호(107a~n)를 생성한다. 액세서리 장치(122a~n)에 대응하는 서버 보안 소자(110a~n)가 인커밍 스크램블된 오디오 신호(103a~n)를 언스크램블해서 생성한 오디오 신호(107a~n)를 오디오 믹서(108)가 수신하고, 오디오 믹서(108)는 이 오디오 신호를 믹스해서 믹스된 오디오 신호(109)를 생성하여 암호화 인터페이스(106)에 제공한다.

[0019] 암호화 인터페이스(106)는 서버 보안 소자(110a~n)에 의해서 스크램블된 믹스된 오디오 신호(105a~n)를 생성하고, 이는 통신 인터페이스(104)를 통해서 각각의 참가자 장치(120a~n)로 통신되고 관련 액세서리 장치(122a~n)로 릴레이된다. 도 1의 암호화 인터페이스(106)는 k개의 서버 보안 소자(110a~k)에 대한 인터페이스를 포함한다. 이하 상세하게 설명하는 바와 같이, 서버 보안 소자(110a~n)와의 점대점 접속이 만들어진다. 이후 컨퍼런스 콜 서버(102)는 N=K명의 호출자까지와의 컨퍼런스 콜을 핸들링할 수 있다.

[0020] 일부 예시적인 실시예에서, 암호화 인터페이스(106)는, 복수의 하드웨어 보안 모듈로서 구현되기도 하는 복수의 서버 보안 소자(110a~n)에 대한 하드웨어 인터페이스를 포함한다. 예컨대, 상술한 암호화/해독 기능 및 정보가 저장되어 있는 보안 소자로서 각각이 구성된 복수의 마이크로 SD 카드와 같이, 복수의 하드웨어 보안 모듈이 구현될 수 있다. 복수의 서버 보안 소자에 대한 하드웨어 인터페이스는, 스마트 카드 인터페이스, USB, BGA(ball grid array) 인터페이스, SMD(surface mount device) 인터페이스, 인쇄 회로 기판 인터페이스 혹은 유사한 데이터 접속 중 어느 하나가 될 수 있다.

[0021] 예시적인 실시예에서, 각각의 보안 매체 세션은, SIP(Session Initiation Protocol)를 이용한 개시 동안 보안 RTP(Real-Time Protocol) 세션으로서 동작하도록 성립될 수 있다. 보안 매체 세션의 SIP 기반 개시는 SIP 핸드셰이킹 동안의 추가적인 보호를 위해서 TLS(Transport Layer Security)를 포함할 수도 있다.

[0022] 상술한 바와 같이, 각각의 서버 보안 소자(110a~n)는 서버 키 정보를 저장하고, 이는 서버 암호화 키 및 서버 해독 키를 포함할 수 있다. 서버 암호화 키 및 서버 해독 키는, 보안 매체 세션(126a~n)의 개시 동안에 수행되는 키 교환 방법을 통해서, 서버 보안 소자(110a~n)와의 대응하는 보안 매체 세션(126a~n)에서 접속되는 액세서리 장치(122a~n) 내의 참가자 보안 소자(124a~n)로부터 수신되는 키 정보를 사용해서, 생성될 수 있다. 서버 해독 키는 대응하는 액세서리 장치로부터의 스크램블된 오디오 신호를 언스크램블하는데 사용되고, 서버 암호화 키는 대응하는 액세서리 장치에 의해 언스크램블하기 위해 믹스된 오디오 신호를 스크램블하는데 사용된다.

[0023] 예시적인 구현예에서, 오디오 신호는, 헤더 및 패킷 페이로드를 포함하는 RTP 패킷으로서 VOIP로 통신된다. 패킷 페이로드는 AES(advanced encryption standard) 알고리즘 혹은 다른 적절한 사이퍼링 및 디사이퍼링 알고리즘을 사용해서 암호화 및 해독될 수 있다. 각각의 보안 소자의 키 정보는 또한 사이퍼링 혹은 디사이퍼링 이전에 각각의 패킷을 인증하기 위한 세션 키를 포함할 수 있다.

[0024] 일 예시적인 구현예에서, 키 교환 방법은 ZRTP에 따라서 수행된다. 다른 예시적인 구현예에서, 키 교환 방법은 타원 곡선 디피-헬만 키 교환(ECDH) 방법을 사용할 수 있다. 키 교환의 다른 프로토콜은 브레인 풀 타원 곡선("brainpoolP256r1" 및 "brainpoolP384r1")을 포함한다.

[0025] 예시적인 실시예에서, 컨퍼런스 콜 서버(102)는 참가자 장치 인증 모듈(170)을 포함해서, 컨퍼런스 콜 서버(102)에 대한 보안 접속을 개시하는 동안에 참가자 장치(120a~n)가 제공하는 전체(global) 참가자 키를 인증할 수 있다. 전체 참가자 키는 특정한 컨퍼런스 콜 세션에서 참가자 장치의 참가를 확인하는 인증 메커니즘을 생성하도록 임의의 적절하게 구현된 인증 메커니즘이나 혹은 정보가 될 수 있다. 예컨대, 참가자 장치 인증 모듈(170)은 전체 참가자 키 자체를 검증해서 해당 참가자 장치의 사용자를 인증할 수 있다. 참가자 장치(120a~n)가 어떤 전체 참가자 키도 제시하지 않거나 혹은 해당 컨퍼런스 콜에 대해 유효하지 않은 것이면, 사용자는 컨퍼런스 콜에 대한 액세스가 거부된다. 참가자 장치 인증 모듈(170)은 전체 참가자 키가 발행된 컨퍼런스 콜의 날자 및 시간을 이러한 기준을 갖고 확인할 수도 있다. 사용자가 그 컨퍼런스 콜의 날자 및 시간에 유효하지 않은 전체 참가자 키를 제시하면, 사용자는 액세스가 거부될 것이다. 참가자 장치(120a~n)의 사용자는 컨퍼런스 콜 서버(102)를 통한 등록 단계에서 지정된 컨퍼런스 콜에 대한 필요한 전체 참가자 키를 획득할 수 있다. 등록 동안에, 컨퍼런스 콜 서버(102)는 키 관리 데이터베이스(112)에 액세스해서 사용자에게 발행된 전체 참가자 키를 획득할 수 있다.

[0026] 예시적인 실시예에서, 참가자 장치 인증 모듈(170)은 컨퍼런스 콜 서버(102)에 대한 보안 접속의 개시 동안에 참가자 장치(120a~n)가 제공하는 세그먼트 키를 확인할 수 있다. 이 세그먼트 키는, 사용자의 멤버십에 따른 사용자에게나 혹은 그 컨퍼런스 콜이 의도하는 사용자의 그룹이나 그룹들에 속하는 사용자에게 액세스를 제공함으로써, 참가자 장치의 사용자의 그룹 아이덴티티를 나타내도록 구성될 수 있다. 키 관리 데이터베이스(112)는 그룹 아이덴티티를 나타내는 값을 가진 세그먼트 키를 유지하도록 구성될 수 있고, 또한 등록 처리 동안에 참가자 장치에게 세그먼트 키를 제공하도록 구성될 수 있다.

[0027] 액세서리 장치(122a~n)는, 도 1 내지 4에 도시된 헤드셋과 같은, 오디오 입력 및 출력 성능을 가진 임의의 적절한 장치를 포함할 수 있다는 점에 주의한다. 적절한 장치는, 참가자 장치와 인터페이스할 수 있는 A/V 장치나 혹은 헤드셋과 유사하지만 장치를 사용자의 머리에 유지시키는 구조는 없이 구성된 오디오 박스를 포함할 수 있다.

[0028] 참가자 장치(120a~n)는 특히 VOIP 기능을 가진 스마트폰, 워키토키 및 휴대형 핫스팟을 포함할 수 있다. 참가자 장치(120a~n)는 또한 랩톱, 데스크톱 컴퓨터 혹은 적어도 소형 사용자 인터페이스를 가진 임의의 다른 컴퓨팅 장치를 포함할 수 있다.

[0029] 도 2는 복수의 참가자 장치(202, 204, 206) 사이에서 컨퍼런스 콜을 수행하는 시스템(200)의 예를 나타내는 개략 블록도이다. 복수의 참가자 장치(202, 204, 206)는 각각 관련 액세서리 장치(212, 214, 216)에 접속되어 있다. 액세서리 장치(212, 214, 216) 각각은 참가자 보안 소자(222, 224, 226), 오디오 입력(203, 205, 207) 및 데이터 네트워크 인터페이스를 포함한다. 각각의 참가자 보안 소자(222, 224, 226)는 관련 참가자 장치(202, 204, 206)가 엑세스할 수 없는 키 정보를 유지하고 있으며, 각각의 참가자 보안 소자(222, 224, 226)는 컨퍼런스 콜 동안 통신되는 매체 신호(오디오 및/또는 비디오)의 스크램블링 및 언스크램블링을 수행하도록 구성된다. 각각의 액세서리 장치(212, 214, 216)의 데이터 네트워크 인터페이스는 다른 액세서리 장치(212, 214, 216) 각각과 보안 매체 세션을 유지하도록 구성된다.

[0030] 액세서리 장치(212, 214, 216) 중 제 1 액세서리 장치(212)는 오디오 입력(203)으로부터 아날로그 오디오 입력 신호를 수신하도록 구성된 오디오 보코더(250)를 포함한다. 보코더(250)는 아날로그 신호를 디지털 오디오 입력 신호로 변환한다. 보코더(250)는 G.723 혹은 G.729에 따라서 구현될 수 있고, 혹은 간단한 아날로그-디지털(ADC)/디지털-아날로그(D/A) 변환기가 될 수도 있다. 보코더(250)는 압축/압축해제를 수행할 수도 있고, 또한 공지된 다른 적절한 기능을 수행할 수 있다. 제 1 액세서리 장치(212)의 보안 소자(222)는 오디오 보코더(250)에 접속되고, 적어도 2개의 별개의 암호화 키를 사용해서, 디지털 오디오 입력 신호에 기초해서 아웃바운드 암호화된 음성 패킷의 적어도 2개의 각각의 스트림을 생성한다. 제 1 액세서리 장치(212)는 보안 소자(222)에 접속된 PAN(personal area network) 무선 인터페이스(254)를 포함한다. PAN 무선 인터페이스(254)는 아웃바운드

암호화된 음성 패킷의 적어도 2개의 각각의 스트림을 제 1 참가자 통신 장치(202)에 통신하고, 제 1 참가자 통신 장치(202)로부터 적어도 2개의 인바운드 암호화된 음성 패킷 스트림을 수신한다.

[0031] 보안 소자(222)는 적어도 2개의 인바운드 암호화된 음성 패킷 스트림을 해독해서 2개의 인바운드 음성 패킷 스트림을 보코더(254)에 제공한다. 적어도 2개의 인바운드 음성 패킷 스트림은 오디오 신호 믹서(252)로 통신되어서, 2개의 인바운드 음성 패킷 스트림을 믹스된 오디오 아날로그 신호로 결합한다. 믹스된 오디오 신호는 보코더(254)로 통신되고, 이는 믹스된 오디오 신호를 아날로그 오디오 신호로 변환해서 오디오 출력 장치(209)로 통신하며, 이로써 아날로그 오디오 신호는 제 1 액세서리 장치(222)의 사용자에게 들리게 된다.

[0032] 도 2의 시스템(200)을 사용하는 컨퍼런스 콜에서, 제 1 참가자 장치(202)와 제 2 참가자 장치(204) 사이에 제 1 매체 세션(240)이 성립되고, 여기서 제 1 매체 세션(240)은, 제 1 참가자 장치(202)와 제 1 액세서리 장치(212) 사이의 제 1 액세서리 접속을 통해서 제 1 참가자 보안 소자(222)에 접속된다. 이 제 1 매체 세션(240)은 또한 제 2 참가자 장치(204)와 제 2 액세서리 장치(214) 사이의 제 2 액세서리 접속(232)을 통해서 제 2 참가자 보안 소자(224)에 접속된다. 제 2 매체 세션(242)은 제 1 참가자 장치(202)와 제 3 참가자 장치(206) 사이에 성립되고, 여기서 제 2 매체 세션(242)은 제 1 액세서리 접속(230)를 통해서 제 1 참가자 보안 소자(222)에 접속된다. 제 2 매체 세션(242)은 또한 제 3 참가자 장치(206)와 제 3 액세서리 장치(216) 사이의 제 3 액세서리 접속(234)을 통해서 제 3 참가자 보안 소자(226)에도 접속된다. 제 3 매체 세션(244)은 제 2 참가자 장치(204)와 제 3 참가자 장치(206) 사이에 성립되고, 여기서 제 3 매체 세션(244)은 제 2 액세서리 접속(232)을 통해서 제 2 참가자 보안 소자(224)에 접속된다. 제 3 매체 세션(244)은 또한 제 3 액세서리 접속(234)을 통해서 제 3 보안 소자(226)에도 접속된다. 암호화된 음성 패킷 스트림은 참가자 장치(202, 204, 206) 사이의 컨퍼런스 콜 동안에 제 1 매체 세션(240), 제 2 매체 세션(242) 및 제 1 매체 세션(244)을 통해서 액세서리 장치(212, 214, 216)의 보안 소자들(222, 224, 226) 사이에서 통신된다.

[0033] 참가자 장치(202, 204, 206) 각각은 보안 매체 세션(240, 242, 244)을 개시하도록 구성된 컨퍼런스 콜 프로세서를 포함한다. 참가자 장치(202, 204, 206)는 또한 관련 액세서리 장치(212, 214, 216) 사이에서 암호화된 음성 패킷 스트림을 통신하도록 구성된다.

[0034] 각각의 참가자 보안 소자(222, 224, 226)는, 자신이 갖고 있는 키 정보를 사용해서, 다른 액세서리 장치 각각으로부터 수신한 각각의 암호화된 음성 패킷 스트림을 해독해서 대응하는 인커밍 음성 패킷 스트림을 생성하도록 구성된 해독 모듈을 포함한다. 참가자 보안 소자(222, 224, 226)는 또한, 액세서리 장치에 접속된 참가자 보안 소자 내의 키 정보를 사용해서, 오디오 입력(203, 205, 207)에서 수신한 오디오 입력 신호를 암호화함으로써 암호화된 음성 패킷 스트림을 생성하는 암호화 모듈을 포함한다. 암호화된 음성 패킷 스트림은, 암호화된 음성 패킷 스트림 중 대응하는 하나를 수신할 각각의 액세서리 장치 내의 참가자 보안 소자에 의한 해독을 위해서 통신된다. 이 실시예에서, 각각의 참가자 장치는 복수의 암호화된 세션을 수신하고, 각각의 세션을 해독한 이후에 액세서리 장치의 오디오 출력을 통해서 재생할 믹스된 오디오 신호를 형성한다.

[0035] 각각의 참가자 보안 소자(222, 224, 226)는 키 정보를 포함하고, 이는 복수의 암호화 키를 포함한다는 점에 주의한다. 각각의 암호화 키는, 컨퍼런스 콜 세션의 다른 액세서리 장치 중 대응하는 것으로 송신될 음성 패킷 스트림을 암호화하기 위해서 생성된다. 키 정보는 또한 복수의 해독 키를 포함한다. 각각의 해독 키는 컨퍼런스 콜 세션 내의 다른 액세서리 장치 중 대응하는 것으로부터 수신한 음성 패킷 스트림을 해독하기 위해서 생성된다. 각각의 참가자 보안 소자(222, 224, 226)는 키 정보를 유지하고, 각각의 참가자 보안 소자(222, 224, 226)가 각각의 다른 참가자 보안 소자(222, 224, 226)와 유지하고 있는 다수의 보안 매체 세션에 대한 암호화/해독 기능을 수행한다. 보안 소자의 성능에 따라서, 컨퍼런스 콜에 참가할 수 있는 참가자 장치의 수가 제한될 수 있다.

[0036] 각각의 참가자 보안 소자(222, 224, 226)는 보안 매체 세션(240, 242, 244)의 초기화 동안에 키 정보를 생성한다. 예컨대, 키 정보는 보안 매체 세션(240, 242, 244)의 초기화 동안에 수행되는 키 교환 방법의 결과로서 생성될 수 있다. 예컨대, 제 1 매체 세션(240)의 개시 동안에, 제 1 참가자 보안 소자(222) 및 제 2 참가자 보안 소자(224)에서 키 정보를 생성하도록 키 교환 방법이 수행될 수 있다. 제 1 참가자 보안 소자(222)의 키 정보는, 제 2 참가자 보안 소자(224)와 통신되는 오디오 신호를 각각 암호화 및 해독하기 위한 제 1 암호화 키 및 제 1 해독 키를 포함할 수 있다. 제 2 매체 세션(242)의 개시 동안에, 제 1 참가자 보안 소자(222) 및 제 3 참가자 보안 소자(226)에서 키 정보를 생성하도록 키 교환 방법이 수행될 수 있다. 상술한 제 1 암호화 키 및 제 1 해독 키에 더해서, 제 1 참가자 보안 소자(222)의 키 정보는 제 3 참가자 보안 소자(226)와 통신되는 오디오 신호를 암호화 및 해독하기 위한 제 2 암호화 키 및 제 2 해독 키를 또한 포함할 수 있다. 제 1 및 제 2 보

안 매체 세션(240, 242)의 개시 동안 수행되는 키 교환 방법은, 제 2 및 제 3 참가자 보안 소자(224, 226)에 저장된 키 정보 내의 암호화 및 해독 키를 생성할 것이다. 각각의 참가자 보안 소자(222, 224, 226) 내의 키 정보는, 참가자 보안 소자(222, 224, 226)를 모두 서로 접속하고 있는 각각의 보안 매체 세션(240, 242, 244)에 대응하는 암호화/해독 키의 세트를 포함할 것이다.

[0037] 예시적인 구현예에서, 수행되는 키 교환 방법은 타원 곡선 디피-헬만 키 교환(ECDH) 방법이다. zRTP 프로토콜이 사용될 수도 있다. 도 2의 시스템의 보안 소자의 동작은 도 1을 참조로 상기 설명한 서버 보안 소자(110a~n)의 동작과 유사할 수도 있다는 점에 주의한다.

[0038] 도 3은 컨퍼런스 콜을 수행하는 예시적인 시스템(300)의 개략도이며, 여기서 참가자 장치 중 하나가 컨퍼런스 콜 서버로서 동작한다. 시스템(300)은 통신 장치(302)를 포함하고, 이는 컨퍼런스 콜 서버로서 동작하도록 구성된 참가자 장치이다. 통신 장치는, N명의 참가자를 가진 컨퍼런스 콜 세션에서 복수의 참가자 장치(330a~n) 각각과 데이터 네트워크 접속을 형성하도록 구성된다. 복수의 참가자 장치(330a~n) 각각은 대응하는 액세서리 장치(332a~n)에 접속되고, 이는 대응하는 참가자 보안 소자(334a~n)를 포함한다.

[0039] 통신 장치(302)는 서버 액세서리 장치(304)를 포함하고, 이는 키 정보가 저장되어 있는 서버 보안 소자(310), 오디오 입력(311), 오디오 출력(313)(즉, 스피커) 및 보코더(370)를 포함한다. 보코더(370)는 도 2를 참조로 상기 설명한 타입의 임의의 적절한 보코더가 될 수 있다. 서버 보안 소자(310) 내의 키 정보는, 컨퍼런스 콜 세션 내의 각각의 참가자 장치(330a~n)와 관련된 각각의 액세서리 장치(332a~n)에 대응하는 복수의 보안 매체 세션을 성립시키는데 사용된다. 스크램블된 오디오 신호는 스크램블된 혹은 암호화된 음성 패킷 스트림으로서 복수의 보안 매체 세션을 통해서 통신된다.

[0040] 서버 보안 소자(310)는, 각각의 참가자 액세서리 장치(332a~n) 내의 참가자 보안 소자(334a~334n)와의 보안 매체 세션(301a~n)에 대응하는 암호화 키(320a~n)를 저장하는 암호화 모듈을 포함한다. 암호화 모듈은 또한 오디오 신호에 대한 암호화를 수행해서 참가자 액세서리 장치(332a~n)로 통신하도록 구성된다. 서버 보안 소자(310)는 또한, 각각의 참가자 액세서리 장치(332a~n) 내의 참가자 보안 소자(334a~334n)와의 보안 매체 세션(301a~n)에 대응하는 해독 키(322a~n)를 저장하는 해독 모듈을 포함한다. 해독 모듈은 또한 참가자 액세서리 장치(332a~n)로부터 수신되는 오디오 신호에 대한 해독을 수행하도록 구성된다.

[0041] 서버 액세서리 장치(304)는 오디오 입력(311)에서 오디오 신호를 사용자로부터 아날로그 형태로 수신하고 이는 보코더(370)에 의해 디지털화된다. 오디오 믹서(306)는 오디오 입력(311)으로부터의 디지털 오디오 신호를, 서버 보안 소자(310)에 의한 인커밍 스크램블된 오디오 신호의 해독 이후에 생성된 인커밍 오디오 신호와 믹스한다. 오디오 믹서는 서버 보안 소자(310)에 의한 암호화를 위해서 믹스된 오디오 신호를 생성한다.

[0042] 통신 장치(302)는, 참가자 장치(330a~n) 각각과 관련된 복수의 액세서리 장치(332a~n) 각각과 서버 액세서리 장치(304)와의 사이에 복수의 보안 매체 세션을 개시하도록 구성된 컨퍼런스 콜 프로세서(320)를 포함한다. 컨퍼런스 콜 프로세서(320)는 인커밍 스크램블된 오디오 신호를 서버 액세서리 장치(304)로 릴레이하고, 복수의 스크램블된 믹스된 오디오 신호를 보안 매체 세션을 통해서 복수의 참가자 장치(330a~n)와 릴레이한다.

[0043] 예시적인 구현예에서, 컨퍼런스 콜 프로세서(320)는 키 생성 정보를 서버 액세서리 장치(304)로 릴레이해서 서버 보안 소자(310)로 전달하게 하도록 구성된다. 키 생성 정보는 서버 보안 소자(310)에 의해, 서버 보안 소자(310)에 저장되는 키 정보를 생성하는데 사용된다. 예시적인 구현예에서, 키 정보는 복수의 암호화 키(320a~n)를 포함하고, 각각의 암호화 키는 다른 액세서리 장치(334a~n) 중 대응하는 것으로 송신될 오디오 신호를 스크램블하기 위해서 생성된다.

[0044] 서버 보안 소자(310)에 저장되는 키 정보는 또한 복수의 해독 키(322a~n)를 포함한다. 각각의 해독 키는, 컨퍼런스 콜 세션의 복수의 참가자 장치(330a~n)와 관련된 다른 액세서리 장치(332a~n) 중 대응하는 것으로부터 수신된 스크램블된 오디오 신호를 언스크램블하도록 생성된다.

[0045] 다른 액세서리 장치 각각에 대응하는 복수의 암호화 키 각각 및 복수의 해독 키 각각은, 키 생성 정보를 이용해서 키 교환 방법에 의해 생성된다. 키 교환 방법은 액세서리 장치(332a~n) 각각과의 보안 매체 세션의 개시 동안에 수행될 수 있다. 예시적인 구현예에서, 수행되는 키 교환 방법은 타원 곡선 디피-헬만 키 교환 방법이다. zRTP 프로토콜이 사용될 수도 있다. 도 2의 시스템의 보안 소자의 동작은 도 1을 참조로 상기 설명한 서버 보안 소자(110a~n)의 동작과 유사할 수도 있다는 점에 주의한다.

[0046] 도 3의 시스템(300)에서, 액세서리 장치(304)의 보안 소자(310)는 복수의 참가자 장치(330a~n) 각각과 점대점 통신한다. 컨퍼런스 콜을 위해서 성립될 수 있는 접속의 수 K는, 보안 소자(310)에 사용되는 컴포넌트의 성능

제한에 의해서 제한될 수 있다.

[0047] 도 4는 복수의 참가자 장치 사이에서 컨퍼런스 콜을 수행하는 시스템(400)의 예를 나타내는 개략도로, 여기서 컨퍼런스 콜 기능은 참가자 장치 사이에 분산된다. 이 시스템은, 중앙 믹싱 모듈(406) 및 중앙 보안 소자(408)를 구비한 중앙 액세서리 장치(404)에 접속된 중앙 참가자 장치(402)를 포함한다.

[0048] 시스템(400)은 또한 제 1 중간 참가자 장치(420) 및 제 2 중간 참가자 장치(430)를 포함한다. 제 1 중간 참가자 장치(420) 및 제 2 중간 참가자 장치(430)는 각각 대응하는 제 1 및 제 2 중간 액세서리 장치(422, 432)에 접속된다. 제 1 중간 액세서리 장치(422) 및 제 2 중간 액세서리 장치(432)는 각각 대응하는 제 1 및 제 2 중간 보안 소자(426, 436)를 포함한다.

[0049] 컨퍼런스 콜에서, 제 1 및 제 2 중간 액세서리 장치(422, 432) 각각은 대응하는 제 1 및 제 2 보안 매체 세션을 통해서 중앙 액세서리 장치에 접속된다. 제 1 보안 매체 세션은 중앙 액세서리 장치(404)와 제 1 중간 액세서리 장치(422)를 접속해서, 중앙 아웃바운드 믹스된 오디오 신호(CO1)를 암호화된 음성 패킷 스트림으로서 중앙 액세서리 장치(404)로부터 통신하고, 제 1 중간 인바운드 믹스된 오디오 신호(MCI1)를 암호화된 음성 패킷 스트림으로서 제 1 중간 액세서리 장치(422)로부터 중앙 액세서리 장치(404)로 통신한다. 제 1 보안 매체 세션의 실제 엔드포인트는 중앙 보안 소자(408) 및 제 1 중간 보안 소자(426)이므로, 중앙 보안 소자(408) 및 제 1 중간 보안 소자(426)는 제 1 보안 매체 세션으로 통신되는 오디오 신호를 암호화/해독하는 것이 가능하다.

[0050] 컨퍼런스 콜에서, 제 2 보안 매체 세션은 중앙 액세서리 장치(404)와 제 2 중간 액세서리 장치(430)를 접속해서, 중앙 아웃바운드 믹스된 오디오 신호(CO2)를 암호화된 음성 패킷 스트림으로서 중앙 액세서리 장치(404)로부터 통신하고, 제 2 중간 인바운드 믹스된 오디오 신호(MCI2)를 암호화된 음성 패킷 스트림으로서 제 2 중간 액세서리 장치(430)로부터 중앙 액세서리 장치(404)로 통신한다. 제 2 보안 매체 세션의 실제 엔드포인트는 중앙 보안 소자(408) 및 제 2 중간 보안 소자(436)이므로, 중앙 보안 소자(408) 및 제 1 중간 보안 소자(426)는 제 1 보안 매체 세션으로 통신되는 오디오 신호를 암호화/해독하는 것이 가능하다.

[0051] 시스템(400)은 또한 제 1 분산 참가자 장치(440), 제 2 분산 참가자 장치(450), 제 3 분산 참가자 장치(460) 및 제 4 분산 참가자 장치(470)를 포함한다. 제 1 분산 참가자 장치(440)는 제 1 분산 보안 소자(444)를 구비한 제 1 분산 액세서리 장치(442)를 포함한다. 제 1 분산 보안 소자(444)는 제 1 분산 액세서리 장치(442)와의 중앙 인바운드 매체 세션을 형성해서, 제 1 분산 참가자 장치(440)의 사용자로부터의 암호화된 음성 패킷 스트림으로서의 오디오를 중앙 인바운드 오디오 신호(CI1)로서 통신한다. 제 1 분산 보안 소자(444)는 중앙 보안 소자(408)와의 중앙 아웃바운드 매체 세션을 형성해서, 중앙 아웃바운드 오디오 신호(CO3)를 중앙 액세서리 장치(404)로부터 암호화된 음성 패킷 스트림으로서 수신한다.

[0052] 제 2 분산 참가자 장치(450)는 제 2 분산 보안 소자(454)를 구비한 제 2 분산 액세서리 장치(452)를 포함한다. 제 2 분산 보안 소자(454)는 제 1 중간 보안 소자(422)와의 중앙 인바운드 매체 세션을 형성해서, 제 2 분산 참가자 장치(450)의 사용자로부터의 스크램블된 오디오를, 암호화된 음성 패킷 스트림으로서의 중앙 인바운드 오디오 신호(CI2)로서 통신한다. 제 2 분산 보안 소자(454)는 중앙 보안 소자(408)와의 중앙 아웃바운드 매체 세션을 형성해서, 스크램블된 중앙 아웃바운드 오디오 신호(CO4)를 중앙 액세서리 장치(404)로부터 암호화된 음성 패킷 스트림으로서 수신한다.

[0053] 제 1 중간 보안 소자(426)가 오디오 신호를 언스크램블한 이후에, 제 1 중간 액세서리 장치(422)는 제 1 및 제 2 분산 액세서리 장치(440, 450)로부터 오디오 신호를 수신한다. 제 1 중간 액세서리 장치(422)는, 제 1 및 제 2 분산 액세서리 장치(440, 450)로부터 수신한 오디오 신호를 제 1 중간 보안 소자(422)의 사용자로부터 입력되는 오디오 신호와 믹스하는 제 1 분산 믹싱 모듈(424)을 포함한다. 제 1 중간 보안 소자(426)는 제 1 분산 믹싱 모듈(424)로부터의 믹스된 오디오 신호를 스크램블하고, 이 스크램블된 믹스된 오디오 신호를 상술한 바와 같이 제 1 중간 인바운드 믹스된 오디오 신호(MCI1)로서 통신한다.

[0054] 제 3 분산 참가자 장치(460)는 제 3 분산 보안 소자(464)를 구비한 제 3 분산 액세서리 장치(462)를 포함한다. 제 3 분산 보안 소자(464)는 제 2 중간 보안 소자(432)와의 중앙 인바운드 매체 세션을 형성해서, 제 3 분산 참가자 장치(460)의 사용자로부터의 스크램블된 오디오를 중앙 인바운드 오디오(CI3)로서 통신한다. 제 3 분산 보안 소자(464)는 중앙 보안 소자(408)와의 중앙 아웃바운드 매체 세션을 형성해서, 스크램블된 중앙 아웃바운드 오디오 신호(CO5)를 중앙 액세서리 장치(404)로부터 수신한다.

[0055] 제 4 분산 참가자 장치(470)는 제 4 분산 보안 소자(474)를 구비한 제 4 분산 액세서리 장치(472)를 포함한다. 제 4 분산 보안 소자(474)는 제 2 중간 보안 소자(432)와의 중앙 인바운드 매체 세션을 형성해서, 제 4 분산 참

가자 장치(470)의 사용자로부터의 스크램블된 오디오를 중앙 인바운드 오디오(CI4)로서 통신한다. 제 4 분산 보안 소자(474)는 중앙 보안 소자(408)와의 중앙 아웃바운드 매체 세션을 형성해서, 스크램블된 중앙 아웃바운드 오디오 신호(CO6)를 중앙 액세서리 장치(404)로부터 수신한다.

[0056] 제 2 중간 보안 소자(436)가 오디오 신호를 언스크램블한 이후에, 제 2 중간 액세서리 장치(432)는 제 3 및 제 4 분산 액세서리 장치(460, 470)로부터 오디오 신호를 수신한다. 제 2 중간 액세서리 장치(432)는 제 1 및 제 2 분산 액세서리 장치(460, 470)로부터 수신한 오디오 신호를, 제 2 중간 보안 소자(430)의 사용자로부터 입력되는 오디오 신호와 믹스하는 제 2 분산 믹싱 모듈(434)을 포함한다. 제 2 중간 보안 소자(436)는 제 2 분산 믹싱 모듈(434)로부터의 믹스된 오디오 신호를 스크램블하고, 이 스크램블된 믹스된 오디오 신호를 상술한 바와 같이 제 2 중간 인바운드 믹스된 오디오 신호(MCI2)로서 통신한다.

[0057] 중앙 보안 소자(408)에서 수신된 인바운드 믹스된 오디오 신호(MCI1, MCI2)는 해독되어서, 대응하는 중간 액세서리 장치(422, 432)로부터 오디오 신호를 생성한다. 인바운드 믹스된 오디오 신호(MCI1)는 제 1 분산 참가자 장치(440), 제 2 분산 참가자 장치(450) 및 제 1 중간 액세서리 장치(422)로부터의 인커밍 오디오를 나타낸다. 인바운드 믹스된 오디오 신호(MCI2)는 제 3 분산 참가자 장치(460), 제 4 분산 참가자 장치(470) 및 제 2 중간 액세서리 장치(432)로부터의 인커밍 오디오를 나타낸다. 중앙 액세서리 장치(404)는 신호(MCI1, MCI2)를 수신하고, 중앙 믹싱 모듈(406)을 사용해서 이 신호를 믹스해서 합성 믹스된 오디오 신호를 생성한다. 중앙 보안 소자(408)는 이 합성 믹스된 오디오 신호를 암호화하고, 스크램블된 합성 믹스된 오디오 신호를 상술한 바와 같이 중앙 아웃바운드 통신(CO1, CO2, CO3, CO4, CO5, CO6)으로 통신한다.

[0058] 상술한 관점에서 보안 컨퍼런스 콜 시스템 및 방법의 구현예는 다음을 포함한다.

[0059] 1. 중앙 컨퍼런스 콜 서버에 의해 제어되는 컨퍼런스 콜을 수행하는 방법.

[0060] 서버는 컨퍼런스 콜 통신의 복수의 참가자 장치 각각으로부터의 인바운드 통신을 수신한다. 복수의 참가자 장치 각각은, 오디오 신호를 자신이 저장하고 있는 참가자 키 정보를 사용해서 스크램블 및 언스크램블하도록 구성된 보안 소자를 구비한 액세서리 장치에 대한 접속을 포함한다. 인바운드 통신은, 보안 매체 세션의 참가자 엔드포인트에서 액세서리 장치로부터 통신되며 참가자 장치에 의해 릴레이되는 스크램블된 매체 신호를 포함한다. 각각의 인바운드 통신으로부터의 이 스크램블된 매체 신호는 복수의 서버 보안 소자를 가진 암호화 인터페이스로 릴레이된다. 서버 보안 소자는, 복수의 액세서리 장치 중 대응하는 것과의 보안 매체 세션의 서버측 엔드포인트에서, 서버 보안 소자에 의해서 유지되며 서버에 의한 액세스는 불가능한 서버 키 정보를 이용해서, 오디오 신호를 스크램블 및 언스크램블하도록 구성된다. 암호화 인터페이스로부터 오디오 신호가 수신되며, 이 오디오 신호는 복수의 서버 보안 소자 각각에 의해서, 복수의 참가자 장치와의 매체 세션에서 수신된 스크램블된 매체 신호 각각으로부터 생성된다. 복수의 오디오 신호는 믹스되어서 컨퍼런스 콜 데이터를 생성하고 이는 믹스된 오디오 신호로서 모든 사용자에게 통신된다. 믹스된 오디오 신호는 암호화 인터페이스에 제공되어서 복수의 서버 보안 소자 각각이 믹스된 오디오 신호를 스크램블하여서 복수의 아웃바운드 스크램블된 매체 신호를 생성하게 한다. 각각의 아웃바운드 스크램블된 매체 신호는 복수의 참가자 장치 각각으로의 아웃바운드 통신으로서 통신된다.

[0061] 컨퍼런스 콜을 수행하는 방법에서, 서버는 또한 복수의 참가자 장치의 각각의 장치로부터 보안 통신 접속을 개시하라는 요청을 수신할 수 있다. 이후 서버는 보안 접속을 개시하라는 요청 각각에 응답해서, 각각의 참가자 장치에 접속된 액세서리 장치와 복수의 서버 보안 소자 중 대응하는 장치 사이의 보안 매체 세션을 성립할 수 있다. 보안 매체 세션은, 각각의 액세서리 장치로부터 각각의 대응하는 서버 보안 소자로 키 정보를 릴레이함으로써 성립될 수 있다.

[0062] 컨퍼런스 콜을 수행하는 방법에서 보안 매체 세션을 성립할 때, 각각의 서버 보안 소자는 키 교환 방법을 수행할 수 있다. 이 키 교환 방법은 대응하는 액세서리 장치로부터의 스크램블된 매체 부분을 언스크램블하기 위한 서버 해독 키 및 대응하는 액세서리 장치에 의해 언스크램블하기 위해 믹스된 오디오 신호를 스크램블하기 위한 서버 암호화 키를 생성한다.

[0063] 컨퍼런스 콜을 수행하는 방법에서, 키 교환 방법은 디피-헬만 키 교환 방법을 사용해서 수행될 수 있다.

[0064] 컨퍼런스 콜을 수행하는 방법에서, 서버는 복수의 참가자 장치의 각각의 장치로부터 보안 통신 접속을 개시하라는 요청을 수신할 수 있다. 각각의 참가자 장치로부터의 요청은 전체 키를 포함할 수 있다. 전체 키는, 이 요청을 수신한 컨퍼런스 콜 서버에서 컨퍼런스 콜에 참여하는데 사용하기에 유효한지 판정함으로써 인증될 수 있다.

[0065] 이 방법은, 이 전체 키가 요청을 수신한 시간 및 날짜에 대해 유효한지 판정함으로써 전체 키를 인증하는 단계

를 더 포함할 수 있다.

[0066] 이 방법은 컨퍼런스 콜 서버에서 수행되는 컨퍼런스 콜에 참가하기 위해서 참가자 장치 중 하나로부터 전체 키에 대한 요청을 수신하는 것을 포함하는 등록 처리를 더 포함할 수 있다. 전체 키는 키 관리 데이터베이스로부터 취득되어서 요청하는 참가자 장치로 송신된다.

[0067] 이 방법은, 복수의 참가자 장치의 각각의 장치로부터 보안 통신 접속을 개시하라는 요청을 수신하는 단계를 더 포함할 수 있고, 이 요청은 참가자 장치의 사용자가 속하는 그룹을 나타내는 세그먼트 키를 포함한다. 세그먼트 키는 이 요청을 수신한 컨퍼런스 콜 서버에서 컨퍼런스 콜에 참여하는데 사용하기에 유효한지 판정함으로써 인증될 수 있다.

[0068] 이 방법은 참가자 장치 중 참가자 장치의 사용자가 속하는 그룹에 대응하는 참가자 장치로부터 세그먼트 키에 대한 요청을 수신하는 등록 처리를 더 포함할 수 있다. 세그먼트 키는 키 관리 데이터베이스로부터 취득되어서 요청하는 참가자 장치로 송신된다.

[0069] 2. 컨퍼런스 콜 서버

[0070] 컨퍼런스 콜 서버는 데이터 네트워크를 통해서 복수의 참가자 장치와 통신하도록 구성된 통신 인터페이스를 포함한다. 각각의 참가자 장치는 참가자 키 정보를 유지하기 위한 참가자 보안 소자 및 오디오 입력 및 출력 장치를 구비한 액세서리 장치에 접속된다. 통신 인터페이스는, 관련된 참가자 장치에 의해서 릴레이되는 대응하는 보안 매체 세션으로 각각의 액세서리 장치와 스크램블된 오디오 신호를 통신한다. 대응하는 참가자 장치에 접속된 액세서리 장치와 통신되는 오디오 신호를, 자신이 저장하고 있는 서버 보안 키 정보를 사용해서 스크램블 및 언스크램블하도록 구성된 복수의 서버 보안 소자에 암호화 인터페이스가 접속된다. 오디오 믹서는, 복수의 참가자 장치에 접속된 액세서리 장치에 대응하는 서버 보안 소자에 의해서 언스크램블되는, 인커밍 스크램블된 오디오 신호로부터의 오디오 신호를 믹스한다. 오디오 믹서는 오디오 신호를 믹스해서 컨퍼런스 콜 데이터를 생성하고, 이는 컨퍼런스 콜의 사용자에게 믹스된 오디오 신호로서 통신된다. 믹스된 오디오 신호는 암호화 인터페이스에 제공된다. 서버 보안 소자 각각은 스크램블된 오디오 신호를 생성해서 암호화 인터페이스로 제공하고, 이는 통신 인터페이스를 통해서 각각의 참가자 장치로 통신되고 관련 액세서리 장치로 릴레이된다.

[0071] 컨퍼런스 콜 서버의 암호화 인터페이스는 복수의 서버 보안 소자에 대한 하드웨어 인터페이스를 포함할 수 있다. 복수의 서버 보안 소자는 복수의 하드웨어 보안 모듈로서 구현될 수 있다.

[0072] 컨퍼런스 콜 서버의 복수의 하드웨어 보안 모듈은, 각각이 보안 소자로서 구성되는 복수의 마이크로 SD 카드를 포함할 수 있다.

[0073] 복수의 서버 보안 소자에 대한 하드웨어 인터페이스는 스마트 카드 인터페이스, BGA 인터페이스, SMD 인터페이스 혹은 인쇄 회로 기판 인터페이스로 이루어진 그룹으로부터 선택될 수 있다.

[0074] 복수의 보안 소자는 입출력 컴포넌트와의 소프트웨어 인터페이스로서 구현될 수도 있다.

[0075] 컨퍼런스 콜 서버의 각각의 서버 보안 소자의 서버 키 정보는 서버 암호화 키 및 서버 해독 키를 포함할 수 있다. 서버 암호화 키 및 서버 해독 키는, 서버 보안 소자와의 매체 세션으로 접속된 액세서리 장치의 참가자 보안 소자로부터 수신한 키 정보를 사용해서 스크램블된 매체 세션의 개시 동안에 수행되는 키 교환 정보를 이용해서, 생성될 수 있다. 서버 해독 키는 대응하는 액세서리 장치로부터의 스크램블된 오디오 신호를 언스크램블하는데 사용되고, 서버 암호화 키는 대응하는 액세서리 장치에 의해 언스크램블하기 위해 믹스된 오디오 신호를 스크램블하는데 사용된다. 키 교환 방법은 디피-헬만 키 교환 방법을 사용해서 수행될 수 있다.

[0076] 컨퍼런스 콜 서버는 또한 참가자 장치 인증 모듈을 포함해서, 컨퍼런스 콜 서버에 대한 보안 접속을 개시하는 동안에 참가자 장치가 제공하는 전체 참가자 키를 인증할 수 있다.

[0077] 참가자 장치 인증 모듈은 전체 참가자 키와 관련된 날자 및 시간을 확인해서 날자 및 시간이 전체 참가자 키에 대해 유효하지 않으면 인증을 거부하도록 구성될 수 있다.

[0078] 컨퍼런스 콜 서버는 컨퍼런스 콜 서버에 대한 보안 접속을 개시하는 동안 참가자 장치가 제공하는 세그먼트 키를 확인하도록 구성된 참가자 장치 인증 모듈을 포함할 수 있다. 세그먼트 키는 참가자 장치의 사용자의 그룹 식별자를 나타낼 수 있다.

[0079] 컨퍼런스 콜 서버는 전체 참가자 키를 유지하고 전체 참가자 키를 참가자 장치에 의해 수행되는 등록 처리 동안 참가자 장치 중 하나에 제공하도록 구성된 키 관리 데이터베이스를 포함할 수 있다.

[0080] 컨퍼런스 콜 서버의 키 관리 데이터베이스는 또한 그룹 식별자를 나타내는 값을 가진 세그먼트 키를 유지할 수 있다. 키 관리 데이터베이스는 등록 처리 동안에 참가자 장치 중 하나에 세그먼트 키를 제공하도록 구성될 수 있다.

[0081] 3. 멀티-오디오 스트림을 이용한 컨퍼런스 콜

[0082] 멀티-오디오 스트림을 이용한 컨퍼런스 콜이, 아날로그 오디오 입력 신호를 수신해서 디지털 오디오 입력 신호를 제공하도록 구성된 오디오 보코더를 포함하는 장치로서, 구현될 수 있다. 이 장치는, 오디오 보코더에 접속되며, 디지털 오디오 입력 신호에 기초해서 아웃바운드 암호화된 음성 패킷의 적어도 2개의 각각의 스트림을 적어도 2개의 별개의 암호화 키를 사용해서 생성하도록 구성된 적어도 하나의 보안 소자를 포함한다. 적어도 하나의 보안 소자에는 PAN(personal area network) 무선 인터페이스가 접속된다. PAN 무선 인터페이스는 아웃바운드 암호화된 음성 패킷의 적어도 2개의 각각의 스트림을 참가자 통신 장치에 통신하고, 참가자 통신 장치로부터 적어도 2개의 인바운드 암호화된 음성 패킷 스트림을 수신하도록 구성된다. 적어도 하나의 보안 소자는 또한 적어도 2개의 인바운드 암호화된 음성 패킷 스트림을 해독하고, 2개의 인바운드 음성 패킷 스트림을 보코더에 제공하도록 구성된다. 오디오 신호 믹서는 이 2개의 인바운드 음성 패킷 스트림을 믹스된 오디오 아날로그 신호로 결합한다.

[0083] 장치의 적어도 하나의 보안 소자는 적어도 2개의 인바운드 암호화된 음성 패킷 스트림을 해독하기 위해서 적어도 2개의 암호해제 키를 더 포함할 수 있다. 적어도 2개의 해독 키 및 적어도 2개의 암호화 키는, 적어도 2개의 인바운드 암호화된 음성 패킷 스크림의 개시 동안에 수행되는 키 교환 방법을 사용해서 생성될 수 있다.

[0084] 이 장치는 키 교환 방법을 수행하는데 디피-헬만 키 교환 방법을 사용할 수 있다. 디피-헬만 방법은 암호화 키 및 해독 키를 포함하는 암호화 키 정보를 생성한다.

[0085] 4. 참가자 장치 사이에서 멀티-오디오 스트림을 이용한 컨퍼런스 콜을 수행하는 방법.

[0086] 참가자 장치 사이에서 멀티-오디오 스트림을 사용하는 방법에서, 적어도 2개의 인바운드 암호화된 음성 패킷 스트림이 제 1 액세서리 장치의 PAN 무선 인터페이스에서 수신된다. 제 1 액세서리 장치는 제 1 보안 소자를 포함하고, PAN 무선 인터페이스를 통해서 제 1 참가자 장치에 접속된다. 적어도 2개의 인바운드 암호화된 음성 패킷 스트림이, 각각이 보안 소자를 포함하고 각각이 적어도 2개의 다른 참가자 장치에 접속되는 적어도 2개의 액세서리 장치로부터 수신된다. 인바운드 암호화된 음성 패킷 스트림은 제 1 보안 소자로 통신되고, 이는 인바운드 암호화된 음성 패킷 스트림을 자신이 저장하고 있는 적어도 2개의 해독 키를 사용해서 해독한다. 해독을 통해서 적어도 2개의 인바운드 음성 패킷 스트림을 생성한다. 제 1 액세서리 장치의 오디오 입력으로부터 아날로그 오디오 신호를 수신하도록 접속된 보코더로부터 디지털 입력 오디오 신호가 수신된다. 적어도 2개의 음성 패킷 스트림은 믹스되어서 믹스된 오디오 신호를 생성한다. 믹스된 오디오 신호는 보코더로 통신되어서 아날로그 믹스된 오디오를 생성하고, 이는 제 1 액세서리 장치의 오디오 출력으로 출력된다. 디지털 입력 오디오 신호는 제 1 보안 소자로 통신되고, 이는 디지털 입력 오디오 신호를, 자신이 저장하고 있는 적어도 2개의 암호화 키를 사용해서 암호화해서 적어도 2개의 아웃바운드 암호화 음성 패킷 스트림을 생성한다. 적어도 2개의 아웃바운드 암호화된 음성 패킷 스트림은 PAN 무선 인터페이스를 통해서 제 1 참가자 장치로 통신되어서, 적어도 2개의 다른 참가자 장치로 통신된다.

[0087] 이 방법은, 관련된 적어도 2개의 참가자 장치에 접속된 적어도 2개의 액세서리 장치 각각과 인바운드 및 아웃바운드 암호화된 음성 패킷 스트림을 통신하기 위해 보안 매체 세션을 개시하는 요청을, 제 1 액세서리 장치에서 수신하는 단계를 더 포함할 수 있다. 적어도 2개의 액세서리 장치 각각과의 보안 매체 세션은, 각각의 액세서리 장치로부터 수신한 키 정보를 제 1 보안 소자로 통신함으로써 보안 매체 세션을 개시하는 각각의 요청에 응답해서 성립된다.

[0088] 보안 매체 세션을 성립할 때, 제 1 보안 소자는 적어도 2개의 액세서리 장치 각각의 보안 소자 각각과 키 교환 방법을 수행해서, 각각의 대응하는 액세서리 장치로부터의 인바운드 암호화된 음성 패킷 스트림을 해독하기 위한 적어도 2개의 해독 키를 생성하고, 대응하는 액세서리 장치의 보안 소자에 의한 해독을 위해서 디지털 오디오 입력 신호를 암호화하는 적어도 2개의 암호화 키를 생성한다.

[0089] 수행되는 키 교환 방법은 디피-헬만 키 교환 방법이 될 수 있다.

[0090] 5. 컨퍼런스 콜 서버로서 참가자 장치

[0091] 통신 장치는 컨퍼런스 콜의 호출자로서 및 컨퍼런스 콜 서버로서 참가하도록 구성될 수 있다. 예시적인 구현예

에서, 통신 장치는, 컨퍼런스 콜 세션 내의 복수의 참가자 장치 각각과 데이터 네트워크 접속을 형성하는 데이터 네트워크 인터페이스를 포함한다. 키 정보를 저장하고 있는 서버 보안 소자를 구비한 서버 액세서리 장치가 포함되어서, 컨퍼런스 콜 세션 내의 각각의 참가자 장치와 관련된 각각의 액세서리 장치에 대응하는 복수의 매체 세션을 성립시킨다. 서버 보안 소자는 각각의 보안 매체 세션으로 수신한 각각의 스크램블된 오디오 신호를 해독해서, 각각의 참가자 장치와 관련된 각각의 액세서리 장치로부터 대응하는 인커밍 오디오 신호를 생성한다. 서버 보안 소자는 키 정보를 사용해서 믹스된 오디오 신호를 암호화해서, 대응하는 복수의 스크램블된 믹스된 오디오 신호를 생성하여서 대응하는 보안 매체 세션을 통해서 액세서리 장치로 통신한다. 오디오 입력은 서버 액세서리 장치에 접속되어서 오디오 신호를 수신한다. 오디오 믹서는 오디오 입력으로부터의 오디오 신호를 각각의 보안 인커밍 스크램블된 오디오 신호로부터의 인커밍 오디오 신호와 믹스해서, 믹스된 오디오 신호를 생성한다.

[0092] 통신 장치는, 참가자 장치 각각과 관련된 복수의 액세서리 장치 각각과 서버 액세서리 장치와의 사이에 복수의 보안 매체 세션을 개시하도록 컨퍼런스 콜 프로세서를 포함할 수 있다. 컨퍼런스 콜 프로세서는 인커밍 스크램블된 오디오 신호를 서버 액세서리 장치로 릴레이하고, 복수의 스크램블된 믹스된 오디오 신호를 보안 매체 세션을 통해서 복수의 참가자 장치와 릴레이한다.

[0093] 컨퍼런스 콜 프로세서는 또한 서버 액세서리 장치에 키 생성 정보를 릴레이해서 서버 보안 소자로 전달하도록 구성될 수 있다. 키 생성 정보는, 서버 보안 소자가 서버 보안 소자에 저장된 키 정보를 생성하는데 사용된다. 키 정보는, 컨퍼런스 콜 세션의 복수의 참가자 장치와 관련된 다른 액세서리 장치 중 대응하는 것으로 송신될 오디오 신호를 스크램블하기 위해서 각각 생성되는 복수의 암호화 키 및 컨퍼런스 콜 세션의 복수의 참가자 장치와 관련된 다른 액세서리 장치 중 대응하는 것으로부터 수신된 스크램블된 오디오 신호를 언스크램블하기 위해서 각각 생성되는 복수의 해독 키를 포함한다. 다른 액세서리 장치 각각에 대응하는 복수의 암호화 키 각각 및 복수의 해독 키 각각은, 키 생성 정보를 사용해서 키 교환 방법으로 생성된다. 키 교환 방법은, 다른 액세서리 장치 각각과의 보안 매체 세션의 개시 동안에 수행된다.

[0094] 키 교환 방법은 디피-헬만 키 교환 방법이 될 수 있으며, 이는 암호화 키 및 해독 키를 포함하는 암호화 키 정보를 생성하는 것이다.

[0095] 6. 컨퍼런스 콜에 참여하는 통신 장치에 의해서 호스팅되는 컨퍼런스 콜을 수행하는 방법.

[0096] 참가자 장치에 의해서 호스팅되는 컨퍼런스 콜을 포함하는 방법에서, 통신 장치는 서버 보안 소자를 포함하는 서버 액세서리 장치에 접속된다. 통신 장치는 컨퍼런스 콜의 복수의 참가자 장치 각각으로부터 인바운드 통신을 수신한다. 복수의 참가자 장치 각각은 특정 보안 소자를 구비한 참가자 액세서리 장치에 대한 접속을 포함한다. 인바운드 통신은, 복수의 보안 매체 세션의 참가자 엔드포인트에서 액세서리 장치로부터 통신되는 스크램블된 매체 신호를 포함한다. 각각의 인바운드 통신으로부터의 이 스크램블된 매체 신호는 서버 보안 소자로 릴레이된다. 서버 보안 소자는, 보안 매체 세션의 서버측 엔드포인트에서, 서버 보안 소자에 의해서 유지되는 서버 키 정보를 이용해서 오디오 신호를 스크램블 및 언스크램블하도록 구성된다. 복수의 오디오 신호는 암호화 인터페이스로부터 수신되고, 여기서 복수의 오디오 신호 각각은 서버 보안 소자에 의해 생성된다. 각각의 오디오 신호는, 복수의 액세서리 장치와의 매체 세션으로 수신한 스크램블된 매체 신호 중 하나에 대응한다. 복수의 오디오 신호는 믹스되어서 믹스된 오디오 신호를 생성한다. 믹스된 오디오 신호는 암호화 인터페이스에 제공되어서 서버 보안 소자가 믹스된 오디오 신호를 스크램블하여서 복수의 스크램블된 오디오 신호를 생성하게 한다. 복수의 스크램블된 오디오 신호 각각은 복수의 액세서리 장치 각각으로 아웃바운드 통신으로서 통신된다.

[0097] 이 방법은 복수의 참가자 장치 각각으로부터 보안 통신 접속을 개시하라는 요청을 수신하는 단계를 더 포함한다. 각각의 요청에 응답해서, 각각의 액세서리 장치에 대응하는 키 생성 정보를 서버 보안 소자로 릴레이함으로써 서버 액세서리 장치와 복수의 액세서리 장치 각각 사이에 복수의 보안 매체 세션이 성립된다.

[0098] 이 방법은, 보안 매체 세션을 성립하는 단계에서, 키 생성 정보를 사용해서, 각각의 대응하는 액세서리 장치로부터의 스크램블된 오디오 신호를 언스크램블하기 위한 복수의 해독 키 및 대응하는 액세서리 장치의 보안 소자에 의해 언스크램블하기 위해 믹스된 오디오 신호를 스크램블하기 위한 복수의 암호화 키를 생성하는 키 교환 방법을 수행하는 단계를 더 포함할 수 있다.

[0099] 키 교환 방법은 디피-헬만 키 교환 방법을 사용해서 수행될 수 있다.

[0100] 7. 분산 컨퍼런스 콜 기능

[0101] 컨퍼런스 콜은, 기능이 참가자 장치 사이에 분산되는 방식으로 수행될 수 있다. 참가자 장치의 기기는 아날로그

오디오 입력 신호를 수신하고 디지털 오디오 입력 신호를 제공하도록 구성된 오디오 보코더를 포함한다. 보안 소자는 오디오 보코더에 접속되고, 대응하는 제 1 참가자 장치에 접속된 제 1 액세서리 장치에 대응하는 암호화 키를 사용해서, 디지털 오디오 입력 신호를 포함하는 아웃바운드 암호화된 음성 패킷의 스트림을 생성하도록 구성된다. 보안 소자에는 PAN 무선 인터페이스가 접속된다. PAN 무선 인터페이스는 아웃바운드 암호화된 음성 패킷의 스트림을 참가자 통신 장치에 통신해서 제 1 액세서리 장치에 통신하고 제 2 액세서리 장치로부터 통신되는 인바운드 암호화된 음성 패킷 스트림을 참가자 통신 장치로부터 수신한다. 보안 소자는 또한, 제 2 액세서리 장치에 대응하는 해독 키를 사용해서 인바운드 암호화된 음성 패킷 스트림을 해독하고, 오디오 출력을 위해서 보코더로 인바운드 음성 패킷 스트림을 제공하도록 더 구성된다.

[0102] 이 기기에서, 해독 키는, 제 1 액세서리 장치와의 인바운드 암호화된 음성 패킷 스트림의 개시 동안에 수행되는 키 교환 방법을 사용해서 생성될 수 있다. 암호화 키는 제 2 액세서리 장치와의 아웃바운드 암호화된 음성 패킷 스트림의 개시 동안에 키 교환 방법을 사용해서 생성된다.

[0103] 키 교환 방법은 디피-헬만 키 교환 방법이 될 수 있다.

[0104] 이 기기는 분산 기능 텔레컨퍼런싱 시스템에서 분산 액세서리 장치로서 동작하도록 구성될 수 있다. 분산 기능 텔레컨퍼런싱 시스템에서, 분산 액세서리 장치는, 적어도 분산 액세서리 장치로부터의 오디오 스트림과 중간 액세서리 장치에 접속된 디지털 오디오 입력을 믹스하도록 구성된 제 1 중간 액세서리 장치로, 아웃바운드 음성 패킷 스트림을 통신한다. 분산 액세서리 장치는, 제 1 중간 액세서리 장치, 제 2 중간 액세서리 장치 및 중앙 액세서리 장치에 접속된 디지털 오디오 입력으로부터의 오디오 스트림을 믹스하도록 구성된 중앙 액세서리 장치로부터, 인바운드 음성 패킷 스트림을 수신한다.

[0105] 이 기기는 분산 기능 텔레컨퍼런싱 시스템에서 중간 액세서리 장치로서 동작하도록 구성될 수 있다. 분산 기능 텔레컨퍼런싱 시스템에서, 중간 액세서리 장치는 제 1 분산 액세서리 장치로부터 제 1 인커밍 암호화된 음성 패킷 스트림으로서 인커밍 암호화된 음성 패킷 스트림을, 그리고 제 2 분산 액세서리 장치로부터 제 2 인커밍 암호화된 음성 패킷 스트림을 수신한다. 중간 액세서리 장치는, 아웃바운드 음성 패킷 스트림으로부터의 오디오 스트림, 적어도 하나의 다른 중간 액세서리 장치로부터 오디오 스트림 및 중앙 액세서리 장치에 접속된 디지털 오디오 입력을 믹스하도록 구성된 중앙 액세서리 장치에, 아웃바운드 음성 패킷 스트림으로 통신한다. 보안 소자의 해독 키는, 제 1 인커밍 음성 패킷 스트림을 생성하기 위한, 제 1 분산 액세서리 장치로부터의 제 1 인커밍 암호화된 음성 패킷 스트림에 대응하는 제 1 개별 해독 키이다. 보안 소자는, 제 2 분산 액세서리 장치와의 통신에 대응하는 제 2 개별 해독 키를 사용해서 제 2 인커밍 암호화된 음성 스트림을 해독해서, 제 2 인커밍 음성 패킷 스트림을 생성하도록 구성된다. 중간 액세서리 장치는 또한 제 1 인커밍 음성 패킷 스트림, 제 2 인커밍 음성 패킷 스트림 및 디지털 입력 신호를 믹스해서 믹스된 오디오 신호를 생성하도록 구성된 분산 믹싱 모듈을 더 포함한다. 보안 소자는 믹스된 오디오 신호로부터 아웃바운드 암호화된 음성 패킷의 스트림을 생성한다.

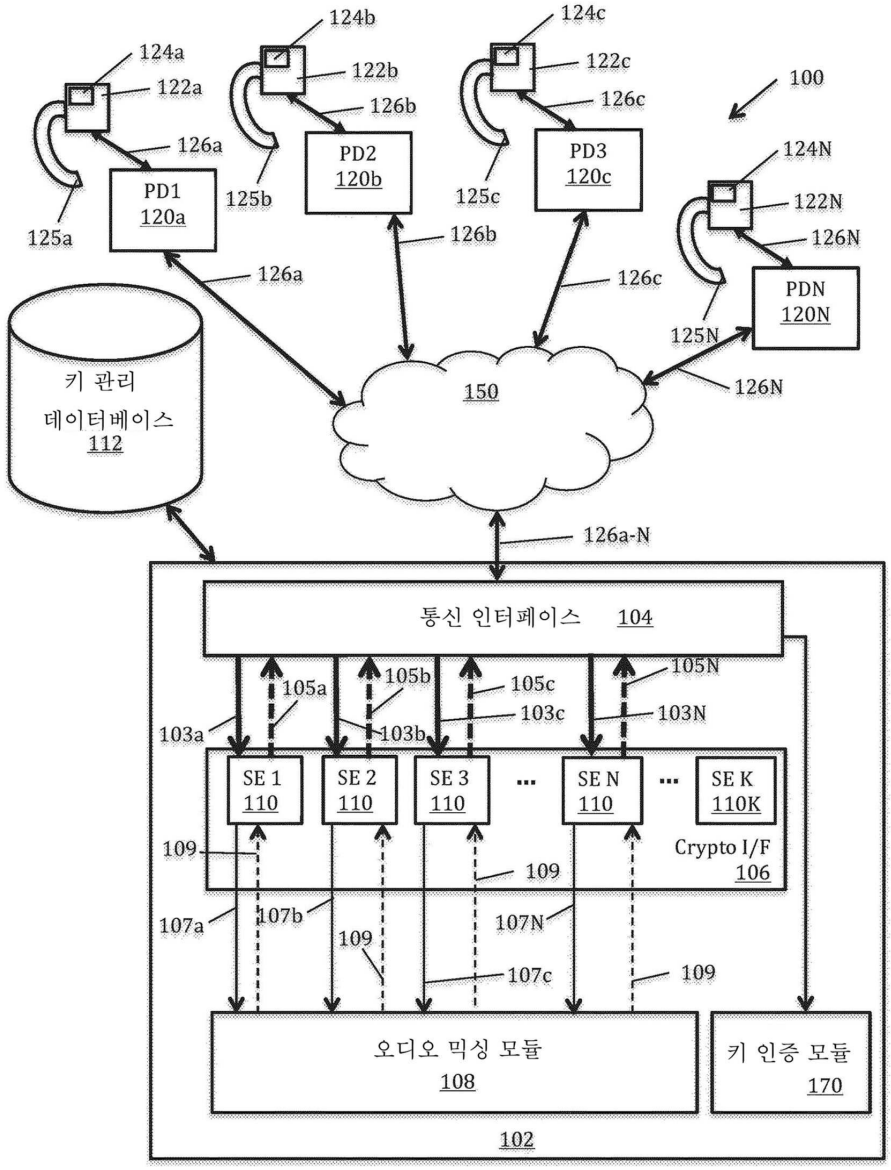
[0106] 이 기기는 분산 기능 텔레컨퍼런싱 시스템에서 중앙 액세서리 장치로서 동작하도록 구성될 수도 있다. 분산 기능 텔레컨퍼런싱 시스템에서, 중앙 액세서리 장치는 아웃바운드 암호화된 음성 패킷 스트림을 제 1 아웃바운드 암호화된 음성 패킷 스트림으로서 제 1 중간 액세서리 장치로 통신한다. 이 중앙 액세서리 장치는 제 2 아웃바운드 암호화된 음성 패킷 스트림을 제 2 중간 액세서리 장치로 통신하고, 복수의 분산 아웃바운드 암호화된 음성 패킷 스트림을 복수의 분산 액세서리 장치로 통신하도록 구성된다. 중앙 액세서리 장치는 제 1 중간 액세서리 장치로부터 제 1 인커밍 암호화된 음성 패킷 스트림으로서 인커밍 암호화된 음성 패킷 스트림을, 그리고 제 2 중간 액세서리 장치로부터 제 2 인커밍 암호화된 음성 패킷 스트림을 수신한다. 보안 소자의 해독 키는 제 1 인커밍 음성 패킷 스트림을 생성하는데 사용되는 제 1 중간 액세서리 장치로부터 제 1 인커밍 암호화된 음성 패킷 스트림에 대응하는 제 1 별개 해독 키이다. 보안 소자의 암호화 키는 제 1 중간 장치로의 제 1 아웃바운드 암호화된 음성 패킷 스트림에 대응하는 제 1 별개 암호화 키이다. 보안 소자는 제 2 중간 액세서리 장치와의 통신에 대응하는 제 2 개별 해독 키를 사용해서 제 2 인커밍 암호화된 음성 패킷 스트림을 해독해서 제 2 인커밍 음성 패킷 스트림을 생성하고, 제 2 중간 액세서리 장치로의 통신에 대응하는 제 2 별개 암호화 키를 사용해서 아웃바운드 음성 패킷 스트림을 암호화하며, 복수의 분산 액세서리 장치로의 통신에 대응하는 복수의 별개 암호화 키를 사용해서 아웃바운드 음성 패킷 스트림을 암호화하도록 구성된다. 중앙 액세서리 장치는 또한 제 1 인커밍 음성 패킷 스트림, 제 2 인커밍 음성 패킷 스트림 및 디지털 입력 신호를 믹스해서 믹스된 오디오 신호를 생성하는 중앙 믹싱 모듈을 더 포함한다. 보안 소자는 믹스된 오디오 신호로부터 아웃바운드 암호화된 음성 패킷의 스트림을 생성한다.

[0107] 본 발명의 다양한 측면 혹은 세부 사항은 본 발명의 범주로부터 벗어남없이 변경될 수 있다는 것을 이해할 것이

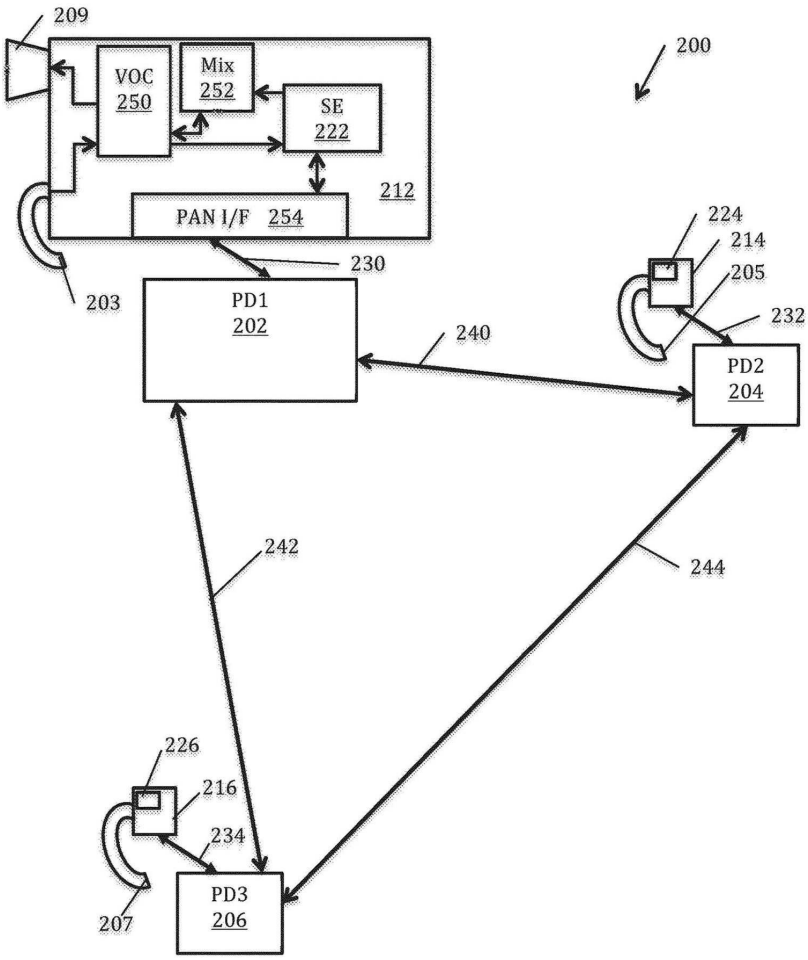
다. 또한, 상기 설명은 예시를 위한 목적일 뿐 한정의 목적이 아니며, 이 방법은 청구항에 의해 정의된다.

## 도면

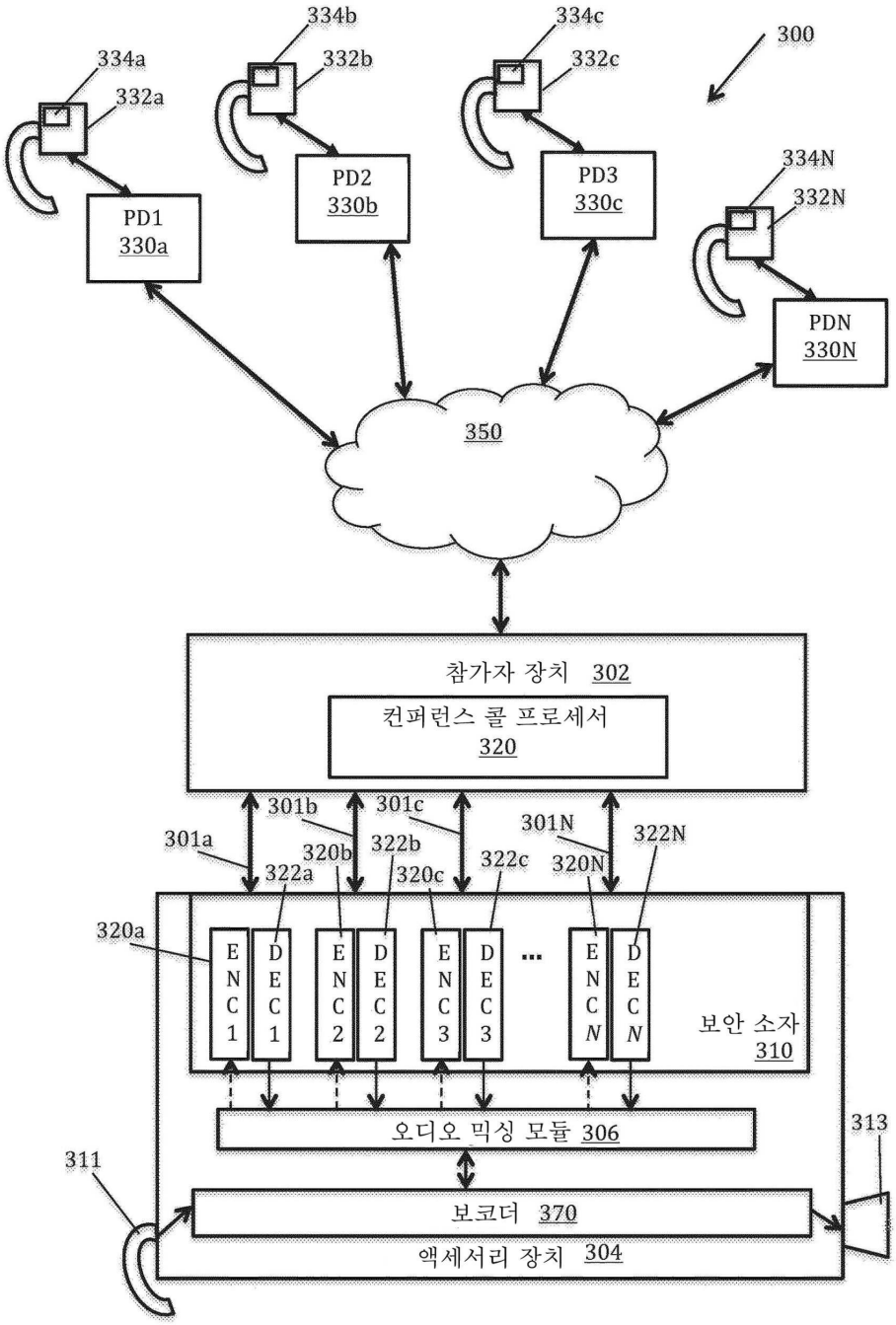
### 도면1



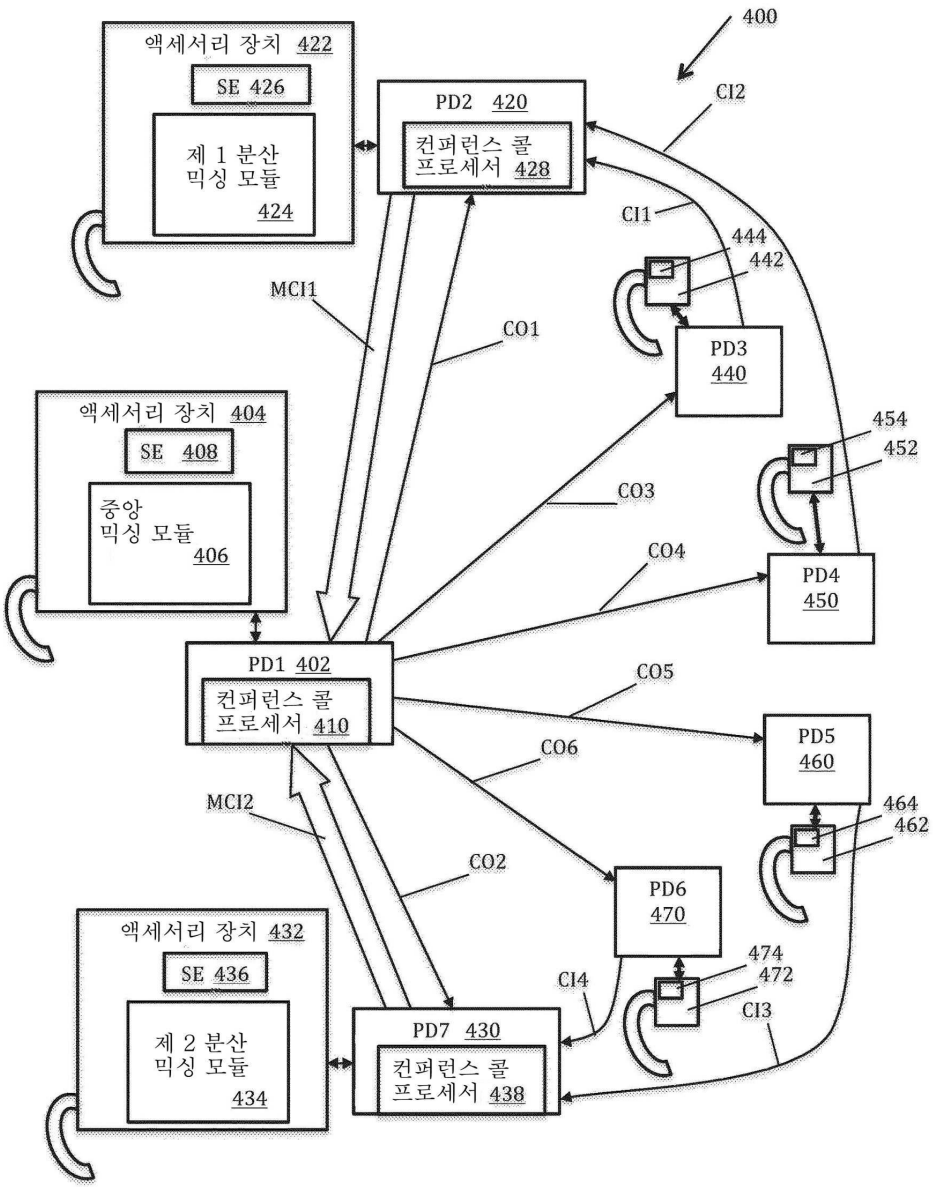
도면2


209
VOC
250
Mix
252
SE
222
212
PAN I/F 254
230
203
PD1
202
200
224
214
205
232
240
PD2
204
242
244
226
216
234
PD3
206
207

도면3


334b
334c
300
334a
332b
332c
332a
PD2
330b
PD3
330c
334N
PD1
330a
332N
PDN
330N
350
참가자 장치 302
컨퍼런스 콜 프로세서
320
301b
301c
301N
322N
301a
320b
322b
322c
320N
322a
320c
320a
ENC1
DEC1
ENC2
DEC2
ENC3
DEC3
...
ENCN
DECN
보안 소자
310
오디오 믹싱 모듈 306
313
311
보코더 370
액세서리 장치 304

도면4


400
액세서리 장치 422
SE 426
제 1 분산 믹싱 모듈 424
PD2 420
컨퍼런스 콜 프로세서 428
CI2
CI1
444
442
PD3 440
MCI1
CO1
액세서리 장치 404
SE 408
중앙 믹싱 모듈 406
CO3
454
452
CO4
PD4 450
PD1 402
컨퍼런스 콜 프로세서 410
CO5
PD5 460
CO6
MCI2
464
462
CO2
PD6 470
액세서리 장치 432
SE 436
제 2 분산 믹싱 모듈 434
CI4
474
472
CI3
PD7 430
컨퍼런스 콜 프로세서 438