

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일

2024년 12월 19일 (19.12.2024)



(10) 국제공개번호

WO 2024/257903 A1

(51) 국제특허분류:

H04L 9/00 (2006.01)

(21) 국제출원번호:

PCT/KR2023/008079

(22) 국제출원일:

2023년 6월 13일 (13.06.2023)

(25) 출원언어:

한국어

(26) 공개언어:

한국어

(71) 출원인: 엘지전자 주식회사 (LG ELECTRONICS INC.) [KR/KR]; 07336 서울특별시 영등포구 여의대로 128, Seoul (KR). 한국과학기술원 (KOREA ADVANCED INSTITUTE OF SCIENCE AND TECHNOLOGY) [KR/KR]; 34141 대전광역시 유성구 대학로 291, Daejeon (KR).

(72) 발명자: 정재훈 (CHUNG, Jaehoon); 06772 서울특별시 서초구 양재대로11길 19 LG전자 특허센터, Seoul

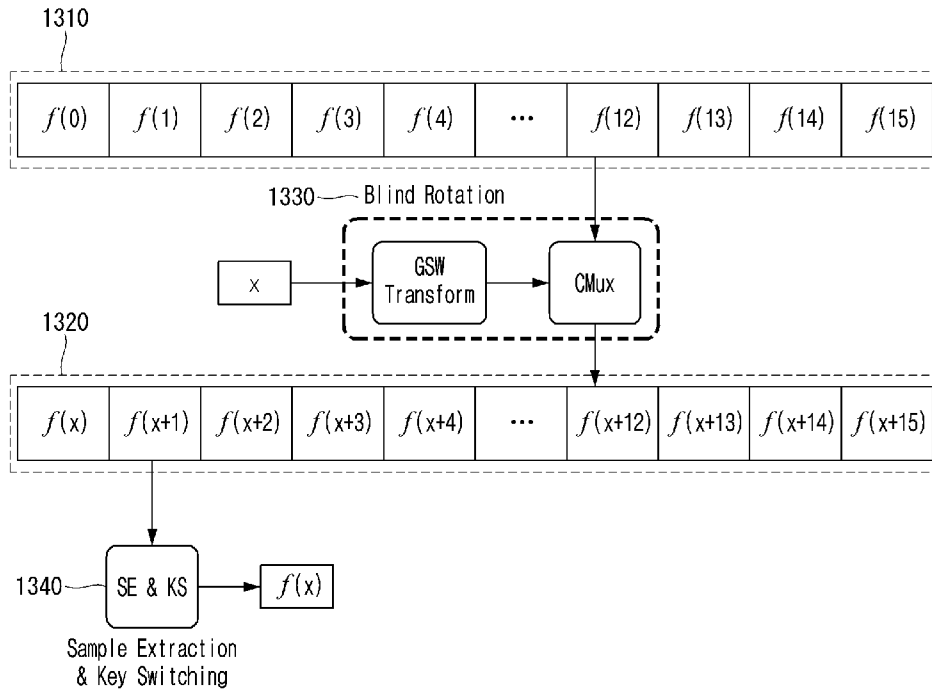
(KR). 하진철 (HA, Jincheol); 34141 대전광역시 유성구 대학로 291, Daejeon (KR). 오은결 (OH, Eun-Gyeol); 34141 대전광역시 유성구 대학로 291, Daejeon (KR). 이주영 (LEE, Jooyoung); 34141 대전광역시 유성구 대학로 291, Daejeon (KR). 손민철 (SON, Mincheol); 34141 대전광역시 유성구 대학로 291, Daejeon (KR).

(74) 대리인: 특허법인 로알 (ROYAL PATENT & LAW OFFICE); 06175 서울특별시 강남구 테헤란로108길 11 삼호빌딩 5층, Seoul (KR).

(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD,

(54) Title: METHOD FOR COMMUNICATION BASED ON HOMOMORPHIC ENCRYPTION IN COMMUNICATION SYSTEM AND DEVICE THEREFOR

(54) 발명의 명칭: 통신 시스템에서 동형 암호 기반의 통신 방법 및 이를 위한 장치



(57) Abstract: The present specification disclosure provides a method performed by a client in a communication system. More specifically, the present method comprises the steps of: receiving at least one synchronization signal from a server; receiving control information from the server; transmitting a homomorphic encryption secret key obtained by homomorphically encrypting a secret key used for data encryption and data decryption to the server; and transmitting encrypted data obtained by encrypting data on the basis of an encryption process repeated at least once, based on (i) the homomorphic encryption secret key and (ii) ROUND function, to the server. Each of the encryption process repeated at least once is performed on the basis of (i) a nonlinear layer for scrambling a part of the data encrypted in the corresponding encryption process and (ii) a linear layer for expanding a part of the scrambled data with regard to all

MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO,
NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW,
SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN,
TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

- (84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의
역내 권리의 보호를 위하여): ARIPO (BW, CV, GH, GM,
KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ,
UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ,
TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE,
ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC,
ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,
TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
KM, ML, MR, NE, SN, TD, TG).

공개:

— 국제조사보고서와 함께 (조약 제21조(3))

the data. The nonlinear layer is randomly generated with regard to each of the encryption process repeated at least once.

(57) 요약서: 본 개시는 통신 시스템에서 클라이언트에 의해 수행되는 방법을 제공한다. 보다 구체적으로, 본 방법은, 서버로부터, 적어도 하나의 동기 신호를 수신하는 단계; 상기 서버로부터, 제어 정보를 수신하는 단계; 상기 서버로, 데이터 암호화 및 데이터 복호화를 위해 사용되는 비밀키가 동형 암호화된 동형 암호 비밀키를 전송하는 단계; 및 상기 서버로, (i) 상기 동형 암호 비밀키 및 (ii) 라운드 함수에 기초한 적어도 한번의 반복되는 암호화 과정에 기초하여 데이터를 암호화한 암호화된 데이터를 전송하는 단계, 상기 적어도 한번의 반복되는 암호화 과정 각각은 (i) 해당 암호화 과정에서 암호화되는 상기 데이터의 일부를 스크램블링하는 비선형층 및 (ii) 상기 스크램블링된 데이터의 일부를 상기 데이터의 전체에 대해 확장시키는 선형층에 기반하여 수행되고, 상기 비선형층은 각각의 상기 적어도 한번의 반복되는 암호화 과정마다 랜덤하게 생성되는 것을 특징으로 하는 전송되는 것을 특징으로 한다.

명세서

발명의 명칭: 통신 시스템에서 동형 암호 기반의 통신 방법 및 이를 위한 장치

기술분야

- [1] 본 개시(disclosure)는 통신 시스템에 관한 것으로, 보다 구체적으로 통신 시스템에서 동형 암호 기반의 통신을 수행하기 위한 방법 및 이를 위한 장치에 관한 것이다.

[2]

배경기술

- [3] 무선 통신 시스템이 음성이나 데이터 등과 같은 다양한 종류의 통신 서비스를 제공하기 위해 광범위하게 전개되고 있다. 일반적으로 무선통신 시스템은 가용한 시스템 자원(대역폭, 전송 파워 등)을 공유하여 다중 사용자와의 통신을 지원할 수 있는 다중 접속(multiple access) 시스템이다. 다중 접속 시스템의 예들로는 CDMA(Code Division Multiple Access) 시스템, FDMA(Frequency Division Multiple Access) 시스템, TDMA(Time Division Multiple Access) 시스템, SDMA(Space Division Multiple Access), OFDMA(Orthogonal Frequency Division Multiple Access) 시스템, SC-FDMA(Single Carrier Frequency Division Multiple Access) 시스템, IDMA (Interleave Division Multiple Access) 시스템 등이 있다.

[4]

발명의 상세한 설명

기술적 과제

- [5] 본 개시는 통신 시스템에서 동형 암호 기반의 통신을 수행하기 위한 방법 및 이를 위한 장치를 제공함에 목적이 있다.
- [6] 또한, 본 개시는 동형 암호 친화적 대칭키 암호화 방식에서, 테이블 참조 동형 연산 시 두 번의 블라인드 로테이션을 수행하기 위한 방법 및 이를 위한 장치를 제공함에 목적이 있다.
- [7] 본 개시에서 이루고자 하는 기술적 과제들은 이상에서 언급한 기술적 과제들로 제한되지 않으며, 언급하지 않은 또 다른 기술적 과제들은 아래의 기재로부터 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

[8]

과제 해결 수단

- [9] 본 개시의 다양한 실시 예들에 따르면, 통신 시스템에서 서버에 의해 수행되는 방법에 있어서, 클라이언트로, 적어도 하나의 동기 신호를 전송하는 단계; 상기 클라이언트로, 제어 정보를 전송하는 단계; 상기 클라이언트로부터, 데이터에 대해 수행되는 적어도 한번의 라운드에 기초하여 암호화된 암호화 데이터를 수신

하는 단계, 상기 적어도 한번의 라운드 각각에서, (i) 상기 적어도 한번의 라운드에서 공통적으로 사용되는 공통 입력 데이터 및 (ii) 상기 적어도 한번의 라운드 각각에서 개별적으로 사용되는 라운드 키가 상기 적어도 한번의 라운드 각각의 라운드 함수에 입력되어 출력되고; 및 상기 암호화 데이터에 포함된 상기 적어도 한번의 라운드 각각의 라운드 함수의 출력 값에 대해 동형 연산을 수행하는 단계를 포함하되, 상기 적어도 한번의 라운드 각각의 라운드 함수의 출력 값에 대한 상기 동형 연산은 상기 동형 연산에 대한 입력 값과 상기 입력 값에 대한 상기 동형 연산의 결과 값 간의 사전 설정된 맵핑 관계에 기초하여 수행되고, 상기 사전 설정된 맵핑 관계에 기초한 상기 동형 연산을 위해, 상기 적어도 한번의 라운드 각각에서 개별적으로 사용되는 라운드 키에 대한 제1 암호문이 상기 동형 연산의 수행 전에 미리 계산되고, 상기 동형 연산의 수행 시에 상기 공통 입력 데이터에 대한 제2 암호문이 계산되고, 상기 사전 설정된 맵핑 관계에 대해 수행되는 (i) 상기 제1 암호문에 기초한 제1 블라인드 로테이션(blind rotation) 및 상기 제2 암호문에 기초한 제2 블라인드 로테이션에 기초하여, 상기 적어도 한번의 라운드 각각의 라운드 함수의 출력 값에 대한 상기 동형 연산의 결과 값이 계산되는 방법이 제공된다.

- [10] 본 개시의 다양한 실시 예들에 따르면, 통신 시스템에서 클라이언트에 의해 수행되는 방법에 있어서, 서버로부터, 적어도 하나의 동기 신호를 수신하는 단계; 상기 서버로부터, 제어 정보를 수신하는 단계; 상기 서버로, 데이터에 대해 수행되는 적어도 한번의 라운드에 기초하여 암호화된 암호화 데이터를 전송하는 단계, 상기 적어도 한번의 라운드 각각에서, (i) 상기 적어도 한번의 라운드에서 공통적으로 사용되는 공통 입력 데이터 및 (ii) 상기 적어도 한번의 라운드 각각에서 개별적으로 사용되는 라운드 키가 상기 적어도 한번의 라운드 각각의 라운드 함수에 입력되어 출력되고; 및 상기 서버로부터, 상기 암호화 데이터에 포함된 상기 적어도 한번의 라운드 각각의 라운드 함수의 출력 값에 대한 동형 연산에 기초하여 획득된 상기 데이터의 동형 암호문을 수신하는 단계를 포함하되, 상기 적어도 한번의 라운드 각각의 라운드 함수의 출력 값에 대한 상기 동형 연산은 상기 동형 연산에 대한 입력 값과 상기 입력 값에 대한 상기 동형 연산의 결과 값 간의 사전 설정된 맵핑 관계에 기초하여 수행되고, 상기 사전 설정된 맵핑 관계에 기초한 상기 동형 연산을 위해, 상기 적어도 한번의 라운드 각각에서 개별적으로 사용되는 라운드 키에 대한 제1 암호문이 상기 동형 연산의 수행 전에 미리 계산되고, 상기 동형 연산의 수행 시에 상기 공통 입력 데이터에 대한 제2 암호문이 계산되고, 상기 사전 설정된 맵핑 관계에 대해 수행되는 (i) 상기 제1 암호문에 기초한 제1 블라인드 로테이션(blind rotation) 및 상기 제2 암호문에 기초한 제2 블라인드 로테이션에 기초하여, 상기 적어도 한번의 라운드 각각의 라운드 함수의 출력 값에 대한 상기 동형 연산의 결과 값이 계산되는 방법이 제공된다.

- [11] 본 개시의 다양한 실시 예들에 따르면, 통신 시스템에서 통신을 수행하는 서버에 있어서, 무선 신호를 전송하기 위한 전송기(transmitter); 무선 신호를 수신하

기 위한 수신기(receiver); 적어도 하나의 프로세서; 및 상기 적어도 하나의 프로세서에 동작 가능하게 접속 가능하고, 상기 적어도 하나의 프로세서에 의해 실행될 때, 동작들을 수행하는 지시(instruction)들을 저장하는 적어도 하나의 컴퓨터 메모리를 포함하며, 상기 동작들은, 클라이언트로, 적어도 하나의 동기 신호를 전송하는 단계; 상기 클라이언트로, 제어 정보를 전송하는 단계; 상기 클라이언트로부터, 데이터에 대해 수행되는 적어도 한번의 라운드에 기초하여 암호화된 암호화 데이터를 수신하는 단계, 상기 적어도 한번의 라운드 각각에서, (i) 상기 적어도 한번의 라운드에서 공통적으로 사용되는 공통 입력 데이터 및 (ii) 상기 적어도 한번의 라운드 각각에서 개별적으로 사용되는 라운드 키가 상기 적어도 한번의 라운드 각각의 라운드 함수에 입력되어 출력되고; 및 상기 암호화 데이터에 포함된 상기 적어도 한번의 라운드 각각의 라운드 함수의 출력 값에 대해 동형 연산을 수행하는 단계를 포함하되, 상기 적어도 한번의 라운드 각각의 라운드 함수의 출력 값에 대한 상기 동형 연산은 상기 동형 연산에 대한 입력 값과 상기 입력 값에 대한 상기 동형 연산의 결과 값 간의 사전 설정된 맵핑 관계에 기초하여 수행되고, 상기 사전 설정된 맵핑 관계에 기초한 상기 동형 연산을 위해, 상기 적어도 한번의 라운드 각각에서 개별적으로 사용되는 라운드 키에 대한 제1 암호문이 상기 동형 연산의 수행 전에 미리 계산되고, 상기 동형 연산의 수행 시에 상기 공통 입력 데이터에 대한 제2 암호문이 계산되고, 상기 사전 설정된 맵핑 관계에 대해 수행되는 (i) 상기 제1 암호문에 기초한 제1 블라인드 로테이션(blind rotation) 및 상기 제2 암호문에 기초한 제2 블라인드 로테이션에 기초하여, 상기 적어도 한번의 라운드 각각의 라운드 함수의 출력 값에 대한 상기 동형 연산의 결과 값이 계산되는 서버가 제공된다.

- [12] 본 개시의 다양한 실시 예들에 따르면, 통신 시스템에서 통신을 수행하는 클라이언트에 있어서, 무선 신호를 전송하기 위한 전송기(transmitter); 무선 신호를 수신하기 위한 수신기(receiver); 적어도 하나의 프로세서; 및 상기 적어도 하나의 프로세서에 동작 가능하게 접속 가능하고, 상기 적어도 하나의 프로세서에 의해 실행될 때, 동작들을 수행하는 지시(instruction)들을 저장하는 적어도 하나의 컴퓨터 메모리를 포함하며, 상기 동작들은, 서버로부터, 적어도 하나의 동기 신호를 수신하는 단계; 상기 서버로부터, 제어 정보를 수신하는 단계; 상기 서버로, 데이터에 대해 수행되는 적어도 한번의 라운드에 기초하여 암호화된 암호화 데이터를 전송하는 단계, 상기 적어도 한번의 라운드 각각에서, (i) 상기 적어도 한번의 라운드에서 공통적으로 사용되는 공통 입력 데이터 및 (ii) 상기 적어도 한번의 라운드 각각에서 개별적으로 사용되는 라운드 키가 상기 적어도 한번의 라운드 각각의 라운드 함수에 입력되어 출력되고; 및 상기 서버로부터, 상기 암호화 데이터에 포함된 상기 적어도 한번의 라운드 각각의 라운드 함수의 출력 값에 대한 동형 연산에 기초하여 획득된 상기 데이터의 동형 암호문을 수신하는 단계를 포함하되, 상기 적어도 한번의 라운드 각각의 라운드 함수의 출력 값에 대한 상기 동형 연산은 상기 동형 연산에 대한 입력 값과 상기 입력 값에 대한 상기 동형 연

산의 결과 값 간의 사전 설정된 맵핑 관계에 기초하여 수행되고, 상기 사전 설정된 맵핑 관계에 기초한 상기 동형 연산을 위해, 상기 적어도 한번의 라운드 각각에서 개별적으로 사용되는 라운드 키에 대한 제1 암호문이 상기 동형 연산의 수행 전에 미리 계산되고, 상기 동형 연산의 수행 시에 상기 공통 입력 데이터에 대한 제2 암호문이 계산되고, 상기 사전 설정된 맵핑 관계에 대해 수행되는 (i) 상기 제1 암호문에 기초한 제1 블라인드 로테이션(blind rotation) 및 상기 제2 암호문에 기초한 제2 블라인드 로테이션에 기초하여, 상기 적어도 한번의 라운드 각각의 라운드 함수의 출력 값에 대한 상기 동형 연산의 결과 값이 계산되는 클라이언트가 제공된다.

- [13] 본 개시의 다양한 실시 예들에 따르면, 하나 이상의 명령어들을 저장하는 비밀시적 컴퓨터 판독 가능 매체(computer readable medium, CRM)에 있어서, 하나 이상의 프로세서들에 의해 실행 가능한 하나 이상의 명령어들은 송신단 수행하는 동작들을 포함하되, 상기 동작들은, 서버에 의하여 수행되는 방법의 모든 단계를 포함하는 비밀시적 컴퓨터 판독 가능 매체가 제공된다.
- [14] 본 개시의 다양한 실시 예들에 따르면, 하나 이상의 명령어들을 저장하는 비밀시적 컴퓨터 판독 가능 매체(computer readable medium, CRM)에 있어서, 하나 이상의 프로세서들에 의해 실행 가능한 하나 이상의 명령어들은 송신단 수행하는 동작들을 포함하되, 상기 동작들은, 클라이언트에 의하여 수행되는 방법의 모든 단계를 포함하는 비밀시적 컴퓨터 판독 가능 매체가 제공된다.
- [15] 본 개시의 다양한 실시 예들에 따르면, 하나 이상의 메모리들 및 상기 하나 이상의 메모리들과 기능적으로 연결되어 있는 하나 이상의 프로세서들을 포함하는 장치에 있어서, 상기 하나 이상의 프로세서들은 상기 장치가 수행하는 동작들을 실행시키되, 상기 동작들은, 서버에 의하여 수행되는 방법의 모든 단계를 포함하는 하는 장치가 제공된다.
- [16] 본 개시의 다양한 실시 예들에 따르면, 하나 이상의 메모리들 및 상기 하나 이상의 메모리들과 기능적으로 연결되어 있는 하나 이상의 프로세서들을 포함하는 장치에 있어서, 상기 하나 이상의 프로세서들은 상기 장치가 수행하는 동작들을 실행시키되, 상기 동작들은, 클라이언트에 의하여 수행되는 방법의 모든 단계를 포함하는 하는 장치가 제공된다.

[17]

발명의 효과

- [18] 본 개시는 통신 시스템에서 동형 암호 기반의 통신을 수행할 수 있는 효과가 있다.
- [19] 또한, 본 개시는 동형 암호 친화적 대칭키 암호화 방식에서, 테이블 참조 동형 연산 시 두 번의 블라인드 로테이션을 수행할 수 있는 효과가 있다.
- [20] 또한, 본 개시는, 동형 연산에 소요되는 시간이 감소될 수 있는 효과가 있다.

[21] 본 개시에서 얻을 수 있는 효과는 이상에서 언급한 효과로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 아래의 기재로부터 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

[22]

도면의 간단한 설명

[23] 이하에 첨부되는 도면들은 본 개시에 관한 이해를 돕기 위한 것으로, 상세한 설명과 함께 본 개시에 대한 실시 예들을 제공할 수 있다. 다만, 본 개시의 기술적 특징이 특정 도면에 한정되는 것은 아니며, 각 도면에서 개시하는 특징들은 서로 조합되어 새로운 실시 예로 구성될 수 있다. 각 도면에서의 참조 번호(reference numerals)들은 구조적 구성요소(structural elements)를 의미할 수 있다.

[24] 도 1은 본 개시에 적용 가능한 통신 시스템 예시를 나타낸 도면이다.

[25] 도 2는 본 개시에 적용 가능한 무선 기기의 예시를 나타낸 도면이다.

[26] 도 3은 본 개시에 적용 가능한 전송 신호를 처리하는 방법을 나타낸 도면이다.

[27] 도 4는 본 개시에 적용 가능한 무선 기기의 다른 예시를 나타낸 도면이다.

[28] 도 5는 본 개시에 적용 가능한 휴대 기기의 예시를 나타낸 도면이다.

[29] 도 6은 본 개시에 적용 가능한 물리 채널들 및 이들을 이용한 신호 전송 방법을 나타낸 도면이다.

[30] 도 7은 본 개시에 적용 가능한 무선 프레임의 구조를 나타낸 도면이다.

[31] 도 8은 본 개시에 적용 가능한 슬롯 구조를 나타낸 도면이다.

[32] 도 9는 본 개시에 적용 가능한 6G 시스템에서 제공 가능한 통신 구조의 일례를 나타낸 도면이다.

[33] 도 10은 다자간 통신의 일 예를 나타낸 도이다.

[34] 도 11은 동형암호-대칭키 암호 하이브리드 프레임워크의 일 예를 나타낸 도이다.

[35] 도 12는 SPN 구조 대칭키 암호의 라운드 함수의 일 예를 나타낸 도이다.

[36] 도 13은 SPN 구조 대칭키 암호의 라운드 함수의 또 다른 일 예를 나타낸 도이다.

[37] 도 14는 Feistel 구조 대칭키 암호의 일 예를 나타낸 도이다.

[38] 도 15는 Feistel 구조 대칭키 암호의 또 다른 일 예를 나타낸 도이다.

[39] 도 16은 본 개시에서 제안하는 방법이 클라이언트에서 수행되는 예시를 나타낸 도이다.

[40] 도 17은 본 개시에서 제안하는 방법이 서버에서 수행되는 예시를 나타낸 도이다.

[41]

발명의 실시를 위한 최선의 형태

[42] 이하의 실시 예들은 본 개시의 구성요소들과 특징들을 소정 형태로 결합한 것들이다. 각 구성요소 또는 특징은 별도의 명시적 언급이 없는 한 선택적인 것으

로 고려될 수 있다. 각 구성요소 또는 특징은 다른 구성요소나 특징과 결합되지 않은 형태로 실시될 수 있다. 또한, 일부 구성요소들 및/또는 특징들을 결합하여 본 개시의 실시 예를 구성할 수도 있다. 본 개시의 실시 예들에서 설명되는 동작들의 순서는 변경될 수 있다. 어느 실시 예의 일부 구성이나 특징은 다른 실시 예에 포함될 수 있고, 또는 다른 실시 예의 대응하는 구성 또는 특징과 교체될 수 있다.

- [43] 도면에 대한 설명에서, 본 개시의 요지를 흐릴 수 있는 절차 또는 단계 등은 기술하지 않았으며, 당업자의 수준에서 이해할 수 있을 정도의 절차 또는 단계는 또한 기술하지 아니하였다.
- [44] 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함(comprising 또는 including)"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다. 또한, 명세서에 기재된 "...부", "...기", "모듈" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다. 또한, "일(a 또는 an)", "하나(one)", "그(the)" 및 유사 관련어는 본 개시를 기술하는 문맥에 있어서(특히, 이하의 청구항의 문맥에서) 본 개시에 달리 지시되거나 문맥에 의해 분명하게 반박되지 않는 한, 단수 및 복수 모두를 포함하는 의미로 사용될 수 있다.
- [45] 본 개시의 실시예들은 기지국과 이동국 간의 데이터 송수신 관계를 중심으로 설명되었다. 여기서, 기지국은 이동국과 직접적으로 통신을 수행하는 네트워크의 종단 노드(terminal node)로서의 의미가 있다. 본 개시에서 기지국에 의해 수행되는 것으로 설명된 특정 동작은 경우에 따라서는 기지국의 상위 노드(upper node)에 의해 수행될 수도 있다.
- [46] 즉, 기지국을 포함하는 다수의 네트워크 노드들(network nodes)로 이루어지는 네트워크에서 이동국과의 통신을 위해 수행되는 다양한 동작들은 기지국 또는 기지국 이외의 다른 네트워크 노드들에 의해 수행될 수 있다. 이때, '기지국'은 고정국(fixed station), Node B, eNB(eNode B), gNB(gNode B), ng-eNB, 발전된 기지국(advanced base station, ABS) 또는 액세스 포인트(access point) 등의 용어에 의해 대체될 수 있다.
- [47] 또한, 본 개시의 실시 예들에서 단말(terminal)은 사용자 기기(user equipment, UE), 이동국(mobile station, MS), 가입자국(subscriber station, SS), 이동 가입자 단말(mobile subscriber station, MSS), 이동 단말(mobile terminal) 또는 발전된 이동 단말(advanced mobile station, AMS) 등의 용어로 대체될 수 있다.
- [48] 또한, 송신단은 데이터 서비스 또는 음성 서비스를 제공하는 고정 및/또는 이동 노드를 말하고, 수신단은 데이터 서비스 또는 음성 서비스를 수신하는 고정 및/또는 이동 노드를 의미한다. 따라서, 상향링크의 경우, 이동국이 송신단이 되고, 기지국이 수신단이 될 수 있다. 마찬가지로, 하향링크의 경우, 이동국이 수신단이 되고, 기지국이 송신단이 될 수 있다.

- [49] 본 개시의 실시 예들은 무선 접속 시스템들인 IEEE 802.xx 시스템, 3GPP(3rd Generation Partnership Project) 시스템, 3GPP LTE(Long Term Evolution) 시스템, 3GPP 5G(5th generation) NR(New Radio) 시스템 및 3GPP2 시스템 중 적어도 하나에 개시된 표준 문서들에 의해 뒷받침될 수 있으며, 특히, 본 개시의 실시 예들은 3GPP TS(technical specification) 38.211, 3GPP TS 38.212, 3GPP TS 38.213, 3GPP TS 38.321 및 3GPP TS 38.331 문서들에 의해 뒷받침될 수 있다.
- [50] 또한, 본 개시의 실시 예들은 다른 무선 접속 시스템에도 적용될 수 있으며, 상술한 시스템으로 한정되는 것은 아니다. 일 예로, 3GPP 5G NR 시스템 이후에 적용되는 시스템에 대해서도 적용 가능할 수 있으며, 특정 시스템에 한정되지 않는다.
- [51] 즉, 본 개시의 실시 예들 중 설명하지 않은 자명한 단계들 또는 부분들은 상기 문서들을 참조하여 설명될 수 있다. 또한, 본 개시에서 개시하고 있는 모든 용어들은 상기 표준 문서에 의해 설명될 수 있다.
- [52] 이하, 본 개시에 따른 바람직한 실시 형태를 첨부된 도면을 참조하여 상세하게 설명한다. 첨부된 도면과 함께 이하에 개시될 상세한 설명은 본 개시의 예시적인 실시 형태를 설명하고자 하는 것이며, 본 개시의 기술 구성이 실시될 수 있는 유일한 실시 형태를 나타내고자 하는 것이 아니다.
- [53] 또한, 본 개시의 실시 예들에서 사용되는 특정 용어들은 본 개시의 이해를 돕기 위해서 제공된 것이며, 이러한 특정 용어의 사용은 본 개시의 기술적 사상을 벗어나지 않는 범위에서 다른 형태로 변경될 수 있다.
- [54] 이하의 기술은 CDMA(code division multiple access), FDMA(frequency division multiple access), TDMA(time division multiple access), OFDMA(orthogonal frequency division multiple access), SC-FDMA(single carrier frequency division multiple access) 등과 같은 다양한 무선 접속 시스템에 적용될 수 있다.
- [55] 하기에서는 이하 설명을 명확하게 하기 위해, 3GPP 통신 시스템(e.g.(예, LTE, NR 등)을 기반으로 설명하지만 본 발명의 기술적 사상이 이에 제한되는 것은 아니다. LTE는 3GPP TS 36.xxx Release 8 이후의 기술을 의미할 수 있다. 세부적으로, 3GPP TS 36.xxx Release 10 이후의 LTE 기술은 LTE-A로 지칭되고, 3GPP TS 36.xxx Release 13 이후의 LTE 기술은 LTE-A pro로 지칭될 수 있다. 3GPP NR은 TS 38.xxx Release 15 이후의 기술을 의미할 수 있다. 3GPP 6G는 TS Release 17 및/또는 Release 18 이후의 기술을 의미할 수 있다. "xxx"는 표준 문서 세부 번호를 의미한다. LTE/NR/6G는 3GPP 시스템으로 통칭될 수 있다.
- [56] 본 개시에 사용된 배경기술, 용어, 약어 등에 관해서는 본 발명 이전에 공개된 표준 문서에 기재된 사항을 참조할 수 있다. 일 예로, 36.xxx 및 38.xxx 표준 문서를 참조할 수 있다.
- [57]
- [58] 본 개시에 적용 가능한 통신 시스템

- [59] 이로 제한되는 것은 아니지만, 본 개시에 개시된 다양한 설명, 기능, 절차, 제안, 방법 및/또는 동작 순서도들은 기기들 간에 무선 통신/연결(예, 5G)을 필요로 하는 다양한 분야에 적용될 수 있다.
- [60] 이하, 도면을 참조하여 보다 구체적으로 예시한다. 이하의 도면/설명에서 동일한 도면 부호는 다르게 기술하지 않는 한, 동일하거나 대응되는 하드웨어 블록, 소프트웨어 블록 또는 기능 블록을 예시할 수 있다.
- [61] 도 1은 본 개시에 적용되는 통신 시스템 예시를 도시한 도면이다. 도 1을 참조하면, 본 개시에 적용되는 통신 시스템(100)은 무선 기기, 기지국 및 네트워크를 포함한다. 여기서, 무선 기기는 무선 접속 기술(예, 5G NR, LTE)을 이용하여 통신을 수행하는 기기를 의미하며, 통신/무선/5G 기기로 지칭될 수 있다. 이로 제한되는 것은 아니지만, 무선 기기는 로봇(100a), 차량(100b-1, 100b-2), XR(extended reality) 기기(100c), 휴대 기기(hand-held device)(100d), 가전(home appliance)(100e), IoT(Internet of Thing) 기기(100f), AI(artificial intelligence) 기기/서버(100g)를 포함할 수 있다. 예를 들어, 차량은 무선 통신 기능이 구비된 차량, 자율 주행 차량, 차량간 통신을 수행할 수 있는 차량 등을 포함할 수 있다. 여기서, 차량(100b-1, 100b-2)은 UAV(unmanned aerial vehicle)(예, 드론)를 포함할 수 있다. XR 기기(100c)는 AR(augmented reality)/VR(virtual reality)/MR(mixed reality) 기기를 포함하며, HMD(head-mounted device), 차량에 구비된 HUD(head-up display), 텔레비전, 스마트폰, 컴퓨터, 웨어러블 디바이스, 가전 기기, 디지털 사이니지(signage), 차량, 로봇 등의 형태로 구현될 수 있다. 휴대 기기(100d)는 스마트폰, 스마트패드, 웨어러블 기기(예, 스마트워치, 스마트글래스), 컴퓨터(예, 노트북 등) 등을 포함할 수 있다. 가전(100e)은 TV, 냉장고, 세탁기 등을 포함할 수 있다. IoT 기기(100f)는 센서, 스마트 미터 등을 포함할 수 있다. 예를 들어, 기지국(120), 네트워크(130)는 무선 기기로도 구현될 수 있으며, 특정 무선 기기(120a)는 다른 무선 기기에게 기지국/네트워크 노드로 동작할 수도 있다.
- [62] 무선 기기(100a~100f)는 기지국(120)을 통해 네트워크(130)와 연결될 수 있다. 무선 기기(100a~100f)에는 AI 기술이 적용될 수 있으며, 무선 기기(100a~100f)는 네트워크(130)를 통해 AI 서버(100g)와 연결될 수 있다. 네트워크(130)는 3G 네트워크, 4G(예, LTE) 네트워크 또는 5G(예, NR) 네트워크 등을 이용하여 구성될 수 있다. 무선 기기(100a~100f)는 기지국(120)/네트워크(130)를 통해 서로 통신할 수도 있지만, 기지국(120)/네트워크(130)를 통하지 않고 직접 통신(예, 사이드링크 통신(sideline communication))할 수도 있다. 예를 들어, 차량들(100b-1, 100b-2)은 직접 통신(예, V2V(vehicle to vehicle)/V2X(vehicle to everything) communication)을 할 수 있다. 또한, IoT 기기(100f)(예, 센서)는 다른 IoT 기기(예, 센서) 또는 다른 무선 기기(100a~100f)와 직접 통신을 할 수 있다.
- [63] 무선 기기(100a~100f)/기지국(120), 기지국(120)/기지국(120) 간에는 무선 통신/연결(150a, 150b, 150c)이 이뤄질 수 있다. 여기서, 무선 통신/연결은 상향/하향링크 통신(150a)과 사이드링크 통신(150b)(또는, D2D 통신), 기지국간 통신(150c)

(예, relay, IAB(integrated access backhaul))과 같은 다양한 무선 접속 기술(예, 5G NR)을 통해 이뤄질 수 있다. 무선 통신/연결(150a, 150b, 150c)을 통해 무선 기기와 기지국/무선 기기, 기지국과 기지국은 서로 무선 신호를 송신/수신할 수 있다. 예를 들어, 무선 통신/연결(150a, 150b, 150c)은 다양한 물리 채널을 통해 신호를 송신/수신할 수 있다. 이를 위해, 본 개시의 다양한 제안들에 기반하여, 무선 신호의 송신/수신을 위한 다양한 구성정보 설정 과정, 다양한 신호 처리 과정(예, 채널 인코딩/디코딩, 변조/복조, 자원 매핑/디매핑 등), 자원 할당 과정 등 중 적어도 일부가 수행될 수 있다.

[64]

[65] 본 개시에 적용 가능한 무선 기기

[66] 도 2는 본 개시에 적용될 수 있는 무선 기기의 예시를 도시한 도면이다.

[67] 도 2를 참조하면, 제1 무선 기기(200a)와 제2 무선 기기(200b)는 다양한 무선 접속 기술(예, LTE, NR)을 통해 무선 신호를 송수신할 수 있다. 여기서, {제1 무선 기기(200a), 제2 무선 기기(200b)}은 도 1의 {무선 기기(100x), 기지국(120)} 및/또는 {무선 기기(100x), 무선 기기(100x)}에 대응할 수 있다.

[68] 제1 무선 기기(200a)는 하나 이상의 프로세서(202a) 및 하나 이상의 메모리(204a)를 포함하며, 추가적으로 하나 이상의 송수신기(206a) 및/또는 하나 이상의 안테나(208a)를 더 포함할 수 있다. 프로세서(202a)는 메모리(204a) 및/또는 송수신기(206a)를 제어하며, 본 개시에 개시된 설명, 기능, 절차, 제안, 방법 및/또는 동작 순서도들을 구현하도록 구성될 수 있다. 예를 들어, 프로세서(202a)는 메모리(204a) 내의 정보를 처리하여 제1 정보/신호를 생성한 뒤, 송수신기(206a)를 통해 제1 정보/신호를 포함하는 무선 신호를 전송할 수 있다. 또한, 프로세서(202a)는 송수신기(206a)를 통해 제2 정보/신호를 포함하는 무선 신호를 수신한 뒤, 제2 정보/신호의 신호 처리로부터 얻은 정보를 메모리(204a)에 저장할 수 있다. 메모리(204a)는 프로세서(202a)와 연결될 수 있고, 프로세서(202a)의 동작과 관련한 다양한 정보를 저장할 수 있다. 예를 들어, 메모리(204a)는 프로세서(202a)에 의해 제어되는 프로세스들 중 일부 또는 전부를 수행하거나, 본 개시에 개시된 설명, 기능, 절차, 제안, 방법 및/또는 동작 순서도들을 수행하기 위한 명령들을 포함하는 소프트웨어 코드를 저장할 수 있다. 여기서, 프로세서(202a)와 메모리(204a)는 무선 통신 기술(예, LTE, NR)을 구현하도록 설계된 통신 모듈/회로/칩의 일부일 수 있다. 송수신기(206a)는 프로세서(202a)와 연결될 수 있고, 하나 이상의 안테나(208a)를 통해 무선 신호를 송신 및/또는 수신할 수 있다. 송수신기(206a)는 송신기 및/또는 수신기를 포함할 수 있다. 송수신기(206a)는 RF(radio frequency) 유닛과 혼용될 수 있다. 본 개시에서 무선 기기는 통신 모듈/회로/칩을 의미할 수도 있다.

[69] 제2 무선 기기(200b)는 하나 이상의 프로세서(202b), 하나 이상의 메모리(204b)를 포함하며, 추가적으로 하나 이상의 송수신기(206b) 및/또는 하나 이상의 안테나(208b)를 더 포함할 수 있다. 프로세서(202b)는 메모리(204b) 및/또는 송수신

기(206b)를 제어하며, 본 개시에 개시된 설명, 기능, 절차, 제안, 방법 및/또는 동작 순서도들을 구현하도록 구성될 수 있다. 예를 들어, 프로세서(202b)는 메모리(204b) 내의 정보를 처리하여 제3 정보/신호를 생성한 뒤, 송수신기(206b)를 통해 제3 정보/신호를 포함하는 무선 신호를 전송할 수 있다. 또한, 프로세서(202b)는 송수신기(206b)를 통해 제4 정보/신호를 포함하는 무선 신호를 수신한 뒤, 제4 정보/신호의 신호 처리로부터 얻은 정보를 메모리(204b)에 저장할 수 있다. 메모리(204b)는 프로세서(202b)와 연결될 수 있고, 프로세서(202b)의 동작과 관련한 다양한 정보를 저장할 수 있다. 예를 들어, 메모리(204b)는 프로세서(202b)에 의해 제어되는 프로세스들 중 일부 또는 전부를 수행하거나, 본 개시에 개시된 설명, 기능, 절차, 제안, 방법 및/또는 동작 순서도들을 수행하기 위한 명령들을 포함하는 소프트웨어 코드를 저장할 수 있다. 여기서, 프로세서(202b)와 메모리(204b)는 무선 통신 기술(예, LTE, NR)을 구현하도록 설계된 통신 모듈/회로/칩의 일부일 수 있다. 송수신기(206b)는 프로세서(202b)와 연결될 수 있고, 하나 이상의 안테나(208b)를 통해 무선 신호를 송신 및/또는 수신할 수 있다. 송수신기(206b)는 송신기 및/또는 수신기를 포함할 수 있다. 송수신기(206b)는 RF 유닛과 혼용될 수 있다. 본 개시에서 무선 기기는 통신 모듈/회로/칩을 의미할 수도 있다.

[70] 이하, 무선 기기(200a, 200b)의 하드웨어 요소에 대해 보다 구체적으로 설명한다. 이로 제한되는 것은 아니지만, 하나 이상의 프로토콜 계층이 하나 이상의 프로세서(202a, 202b)에 의해 구현될 수 있다. 예를 들어, 하나 이상의 프로세서(202a, 202b)는 하나 이상의 계층(예, PHY(physical), MAC(media access control), RLC(radio link control), PDCP(packet data convergence protocol), RRC(radio resource control), SDAP(service data adaptation protocol)와 같은 기능적 계층)을 구현할 수 있다. 하나 이상의 프로세서(202a, 202b)는 본 개시에 개시된 설명, 기능, 절차, 제안, 방법 및/또는 동작 순서도들에 따라 하나 이상의 PDU(Protocol Data Unit) 및/또는 하나 이상의 SDU(service data unit)를 생성할 수 있다. 하나 이상의 프로세서(202a, 202b)는 본 개시에 개시된 설명, 기능, 절차, 제안, 방법 및/또는 동작 순서도들에 따라 메시지, 제어정보, 데이터 또는 정보를 생성할 수 있다. 하나 이상의 프로세서(202a, 202b)는 본 개시에 개시된 기능, 절차, 제안 및/또는 방법에 따라 PDU, SDU, 메시지, 제어정보, 데이터 또는 정보를 포함하는 신호(예, 베이스밴드 신호)를 생성하여, 하나 이상의 송수신기(206a, 206b)에게 제공할 수 있다. 하나 이상의 프로세서(202a, 202b)는 하나 이상의 송수신기(206a, 206b)로부터 신호(예, 베이스밴드 신호)를 수신할 수 있고, 본 개시에 개시된 설명, 기능, 절차, 제안, 방법 및/또는 동작 순서도들에 따라 PDU, SDU, 메시지, 제어정보, 데이터 또는 정보를 획득할 수 있다.

[71] 하나 이상의 프로세서(202a, 202b)는 컨트롤러, 마이크로 컨트롤러, 마이크로 프로세서 또는 마이크로 컴퓨터로 지칭될 수 있다. 하나 이상의 프로세서(202a, 202b)는 하드웨어, 펌웨어, 소프트웨어, 또는 이들의 조합에 의해 구현될 수 있다. 일 예로, 하나 이상의 ASIC(application specific integrated circuit), 하나 이상의

DSP(digital signal processor), 하나 이상의 DSPD(digital signal processing device), 하나 이상의 PLD(programmable logic device) 또는 하나 이상의 FPGA(field programmable gate arrays)가 하나 이상의 프로세서(202a, 202b)에 포함될 수 있다. 본 개시에 개시된 설명, 기능, 절차, 제안, 방법 및/또는 동작 순서도들은 펌웨어 또는 소프트웨어를 사용하여 구현될 수 있고, 펌웨어 또는 소프트웨어는 모듈, 절차, 기능 등을 포함하도록 구현될 수 있다. 본 개시에 개시된 설명, 기능, 절차, 제안, 방법 및/또는 동작 순서도들은 수행하도록 설정된 펌웨어 또는 소프트웨어는 하나 이상의 프로세서(202a, 202b)에 포함되거나, 하나 이상의 메모리(204a, 204b)에 저장되어 하나 이상의 프로세서(202a, 202b)에 의해 구동될 수 있다. 본 개시에 개시된 설명, 기능, 절차, 제안, 방법 및/또는 동작 순서도들은 코드, 명령어 및/또는 명령어의 집합 형태로 펌웨어 또는 소프트웨어를 사용하여 구현될 수 있다.

- [72] 하나 이상의 메모리(204a, 204b)는 하나 이상의 프로세서(202a, 202b)와 연결될 수 있고, 다양한 형태의 데이터, 신호, 메시지, 정보, 프로그램, 코드, 지시 및/또는 명령을 저장할 수 있다. 하나 이상의 메모리(204a, 204b)는 ROM(read only memory), RAM(random access memory), EPROM(erasable programmable read only memory), 플래시 메모리, 하드 드라이브, 레지스터, 캐쉬 메모리, 컴퓨터 판독 저장 매체 및/또는 이들의 조합으로 구성될 수 있다. 하나 이상의 메모리(204a, 204b)는 하나 이상의 프로세서(202a, 202b)의 내부 및/또는 외부에 위치할 수 있다. 또한, 하나 이상의 메모리(204a, 204b)는 유선 또는 무선 연결과 같은 다양한 기술을 통해 하나 이상의 프로세서(202a, 202b)와 연결될 수 있다.
- [73] 하나 이상의 송수신기(206a, 206b)는 하나 이상의 다른 장치에게 본 개시의 방법들 및/또는 동작 순서도 등에서 언급되는 사용자 데이터, 제어 정보, 무선 신호/채널 등을 전송할 수 있다. 하나 이상의 송수신기(206a, 206b)는 하나 이상의 다른 장치로부터 본 개시에 개시된 설명, 기능, 절차, 제안, 방법 및/또는 동작 순서도 등에서 언급되는 사용자 데이터, 제어 정보, 무선 신호/채널 등을 수신할 수 있다. 예를 들어, 하나 이상의 송수신기(206a, 206b)는 하나 이상의 프로세서(202a, 202b)와 연결될 수 있고, 무선 신호를 송수신할 수 있다. 예를 들어, 하나 이상의 프로세서(202a, 202b)는 하나 이상의 송수신기(206a, 206b)가 하나 이상의 다른 장치에게 사용자 데이터, 제어 정보 또는 무선 신호를 전송하도록 제어할 수 있다. 또한, 하나 이상의 프로세서(202a, 202b)는 하나 이상의 송수신기(206a, 206b)가 하나 이상의 다른 장치로부터 사용자 데이터, 제어 정보 또는 무선 신호를 수신하도록 제어할 수 있다. 또한, 하나 이상의 송수신기(206a, 206b)는 하나 이상의 안테나(208a, 208b)와 연결될 수 있고, 하나 이상의 송수신기(206a, 206b)는 하나 이상의 안테나(208a, 208b)를 통해 본 개시에 개시된 설명, 기능, 절차, 제안, 방법 및/또는 동작 순서도 등에서 언급되는 사용자 데이터, 제어 정보, 무선 신호/채널 등을 송수신하도록 설정될 수 있다. 본 개시에서, 하나 이상의 안테나는 복수의 물리 안테나이거나, 복수의 논리 안테나(예, 안테나 포트)일 수 있다. 하나 이상의

송수신기(206a, 206b)는 수신된 사용자 데이터, 제어 정보, 무선 신호/채널 등을 하나 이상의 프로세서(202a, 202b)를 이용하여 처리하기 위해, 수신된 무선 신호/채널 등을 RF 밴드 신호에서 베이스밴드 신호로 변환(Convert)할 수 있다. 하나 이상의 송수신기(206a, 206b)는 하나 이상의 프로세서(202a, 202b)를 이용하여 처리된 사용자 데이터, 제어 정보, 무선 신호/채널 등을 베이스밴드 신호에서 RF 밴드 신호로 변환할 수 있다. 이를 위하여, 하나 이상의 송수신기(206a, 206b)는 (아날로그) 오실레이터 및/또는 필터를 포함할 수 있다.

[74] 도 3은 본 개시에 적용되는 전송 신호를 처리하는 방법을 도시한 도면이다. 일 예로, 전송 신호는 신호 처리 회로에 의해 처리될 수 있다. 이때, 신호 처리 회로(300)는 스크램블러(310), 변조기(320), 레이어 매핑(330), 프리코더(340), 자원 매핑(350), 신호 생성기(360)를 포함할 수 있다. 이때, 일 예로, 도 3의 동작/기능은 도 2의 프로세서(202a, 202b) 및/또는 송수신기(206a, 206b)에서 수행될 수 있다. 또한, 일 예로, 도 3의 하드웨어 요소는 도 2의 프로세서(202a, 202b) 및/또는 송수신기(206a, 206b)에서 구현될 수 있다. 일 예로, 블록 310~350은 도 2의 프로세서(202a, 202b)에서 구현되고, 블록 360은 도 2의 송수신기(206a, 206b)에서 구현될 수 있으며, 상술한 실시 예로 한정되지 않는다.

[75] 코드워드는 도 3의 신호 처리 회로(300)를 거쳐 무선 신호로 변환될 수 있다. 여기서, 코드워드는 정보블록의 부호화된 비트 시퀀스이다. 정보블록은 전송블록(예, UL-SCH 전송블록, DL-SCH 전송블록)을 포함할 수 있다. 무선 신호는 도 6의 다양한 물리 채널(예, PUSCH, PDSCH)을 통해 전송될 수 있다. 구체적으로, 코드워드는 스크램블러(310)에 의해 스크램블된 비트 시퀀스로 변환될 수 있다. 스크램블에 사용되는 스크램블 시퀀스는 초기화 값에 기반하여 생성되며, 초기화 값은 무선 기기의 ID 정보 등이 포함될 수 있다. 스크램블된 비트 시퀀스는 변조기(320)에 의해 변조 심볼 시퀀스로 변조될 수 있다. 변조 방식은 $\pi/2$ -BPSK($\pi/2$ -binary phase shift keying), m-PSK(m-phase shift keying), m-QAM(m-quadrature amplitude modulation) 등을 포함할 수 있다.

[76] 복소 변조 심볼 시퀀스는 레이어 매핑(330)에 의해 하나 이상의 전송 레이어로 매핑될 수 있다. 각 전송 레이어의 변조 심볼들은 프리코더(340)에 의해 해당 안테나 포트(들)로 매핑될 수 있다(프리코딩). 프리코더(340)의 출력 z 는 레이어 매핑(330)의 출력 y 를 $N \times M$ 의 프리코딩 행렬 W 와 곱해 얻을 수 있다. 여기서, N 은 안테나 포트의 개수, M 은 전송 레이어의 개수이다. 여기서, 프리코더(340)는 복소 변조 심볼들에 대한 트랜스폼(transform) 프리코딩(예, DFT(discrete fourier transform) 변환)을 수행한 이후에 프리코딩을 수행할 수 있다. 또한, 프리코더(340)는 트랜스폼 프리코딩을 수행하지 않고 프리코딩을 수행할 수 있다.

[77] 자원 매핑(350)은 각 안테나 포트의 변조 심볼들을 시간-주파수 자원에 매핑할 수 있다. 시간-주파수 자원은 시간 도메인에서 복수의 심볼(예, CP-OFDMA 심볼, DFT-s-OFDMA 심볼)을 포함하고, 주파수 도메인에서 복수의 부반송파를 포함할 수 있다. 신호 생성기(360)는 매핑된 변조 심볼들로부터 무선 신호를 생

성하며, 생성된 무선 신호는 각 안테나를 통해 다른 기기로 전송될 수 있다. 이를 위해, 신호 생성기(360)는 IFFT(inverse fast fourier transform) 모듈 및 CP(cyclic prefix) 삽입기, DAC(digital-to-analog converter), 주파수 상향 변환기(frequency uplink converter) 등을 포함할 수 있다.

- [78] 무선 기기에서 수신 신호를 위한 신호 처리 과정은 도 3의 신호 처리 과정(310~360)의 역으로 구성될 수 있다. 일 예로, 무선 기기(예, 도 2의 200a, 200b)는 안테나 포트/송수신기를 통해 외부로부터 무선 신호를 수신할 수 있다. 수신된 무선 신호는 신호 복원기를 통해 베이스밴드 신호로 변환될 수 있다. 이를 위해, 신호 복원기는 주파수 하향 변환기(frequency downlink converter), ADC(analog-to-digital converter), CP 제거기, FFT(fast fourier transform) 모듈을 포함할 수 있다. 이후, 베이스밴드 신호는 자원 디-매핑 과정, 포스트코딩(postcoding) 과정, 복조 과정 및 디-스크램블 과정을 거쳐 코드워드로 복원될 수 있다. 코드워드는 복호(decoding)를 거쳐 원래의 정보블록으로 복원될 수 있다. 따라서, 수신 신호를 위한 신호 처리 회로(미도시)는 신호 복원기, 자원 디-매핑, 포스트코더, 복조기, 디-스크램블러 및 복호기를 포함할 수 있다.

[79] 본 개시에 적용 가능한 무선 기기 구조

- [80] 도 4는 본 개시에 적용되는 무선 기기의 다른 예시를 도시한 도면이다.

- [81] 도 4를 참조하면, 무선 기기(400)는 도 2의 무선 기기(200a, 200b)에 대응하며, 다양한 요소(element), 성분(component), 유닛/부(unit), 및/또는 모듈(module)로 구성될 수 있다. 예를 들어, 무선 기기(400)는 통신부(410), 제어부(420), 메모리부(430) 및 추가 요소(440)를 포함할 수 있다. 통신부는 통신 회로(412) 및 송수신기(들)(414)을 포함할 수 있다. 예를 들어, 통신 회로(412)는 도 2의 하나 이상의 프로세서(202a, 202b) 및/또는 하나 이상의 메모리(204a, 204b)를 포함할 수 있다. 예를 들어, 송수신기(들)(414)는 도 2의 하나 이상의 송수신기(206a, 206b) 및/또는 하나 이상의 안테나(208a, 208b)를 포함할 수 있다. 제어부(420)는 통신부(410), 메모리부(430) 및 추가 요소(440)와 전기적으로 연결되며 무선 기기의 제반 동작을 제어한다. 예를 들어, 제어부(420)는 메모리부(430)에 저장된 프로그램/코드/명령/정보에 기반하여 무선 기기의 전기적/기계적 동작을 제어할 수 있다. 또한, 제어부(420)는 메모리부(430)에 저장된 정보를 통신부(410)을 통해 외부(예, 다른 통신 기기)로 무선/유선 인터페이스를 통해 전송하거나, 통신부(410)를 통해 외부(예, 다른 통신 기기)로부터 무선/유선 인터페이스를 통해 수신된 정보를 메모리부(430)에 저장할 수 있다.

- [82] 추가 요소(440)는 무선 기기의 종류에 따라 다양하게 구성될 수 있다. 예를 들어, 추가 요소(440)는 파워 유닛/배터리, 입출력부(input/output unit), 구동부 및 컴퓨팅부 중 적어도 하나를 포함할 수 있다. 이로 제한되는 것은 아니지만, 무선 기기(400)는 로봇(도 1, 100a), 차량(도 1, 100b-1, 100b-2), XR 기기(도 1, 100c), 휴대 기기(도 1, 100d), 가전(도 1, 100e), IoT 기기(도 1, 100f), 디지털 방송용 단말, 홀로그램 장치, 공공 안전 장치, MTC 장치, 의료 장치, 핀테크 장치(또는 금융 장치),

보안 장치, 기후/환경 장치, AI 서버/기기(도 1, 140), 기지국(도 1, 120), 네트워크 노드 등의 형태로 구현될 수 있다. 무선 기기는 사용-예/서비스에 따라 이동 가능하거나 고정된 장소에서 사용될 수 있다.

- [83] 도 4에서 무선 기기(400) 내의 다양한 요소, 성분, 유닛/부, 및/또는 모듈은 전체가 유선 인터페이스를 통해 상호 연결되거나, 적어도 일부가 통신부(410)를 통해 무선으로 연결될 수 있다. 예를 들어, 무선 기기(400) 내에서 제어부(420)와 통신부(410)는 유선으로 연결되며, 제어부(420)와 제1 유닛(예, 430, 440)은 통신부(410)를 통해 무선으로 연결될 수 있다. 또한, 무선 기기(400) 내의 각 요소, 성분, 유닛/부, 및/또는 모듈은 하나 이상의 요소를 더 포함할 수 있다. 예를 들어, 제어부(420)는 하나 이상의 프로세서 집합으로 구성될 수 있다. 예를 들어, 제어부(420)는 통신 제어 프로세서, 어플리케이션 프로세서(application processor), ECU(electronic control unit), 그래픽 처리 프로세서, 메모리 제어 프로세서 등의 집합으로 구성될 수 있다. 다른 예로, 메모리부(430)는 RAM, DRAM(dynamic RAM), ROM, 플래시 메모리(flash memory), 휘발성 메모리(volatile memory), 비-휘발성 메모리(non-volatile memory) 및/또는 이들의 조합으로 구성될 수 있다.

[84] 본 개시가 적용 가능한 휴대 기기

- [85] 도 5는 본 개시에 적용되는 휴대 기기의 예시를 도시한 도면이다.

- [86] 도 5는 본 개시에 적용되는 휴대 기기를 예시한다. 휴대 기기는 스마트폰, 스마트패드, 웨어러블 기기(예, 스마트 워치, 스마트 글래스), 휴대용 컴퓨터(예, 노트북 등)를 포함할 수 있다. 휴대 기기는 MS(mobile station), UT(user terminal), MSS(mobile subscriber station), SS(subscriber station), AMS(advanced mobile station) 또는 WT(wireless terminal)로 지칭될 수 있다.

- [87] 도 5를 참조하면, 휴대 기기(500)는 안테나부(508), 통신부(510), 제어부(520), 메모리부(530), 전원공급부(540a), 인터페이스부(540b) 및 입출력부(540c)를 포함할 수 있다. 안테나부(508)는 통신부(510)의 일부로 구성될 수 있다. 블록 510~530/540a~540c는 각각 도 4의 블록 410~430/440에 대응한다.

- [88] 통신부(510)는 다른 무선 기기, 기지국들과 신호(예, 데이터, 제어 신호 등)를 송수신할 수 있다. 제어부(520)는 휴대 기기(500)의 구성 요소들을 제어하여 다양한 동작을 수행할 수 있다. 제어부(520)는 AP(application processor)를 포함할 수 있다. 메모리부(530)는 휴대 기기(500)의 구동에 필요한 데이터/파라미터/프로그램/코드/명령을 저장할 수 있다. 또한, 메모리부(530)는 입/출력되는 데이터/정보 등을 저장할 수 있다. 전원공급부(540a)는 휴대 기기(500)에게 전원을 공급하며, 유/무선 충전 회로, 배터리 등을 포함할 수 있다. 인터페이스부(540b)는 휴대 기기(500)와 다른 외부 기기의 연결을 지원할 수 있다. 인터페이스부(540b)는 외부 기기와의 연결을 위한 다양한 포트(예, 오디오 입/출력 포트, 비디오 입/출력 포트)를 포함할 수 있다. 입출력부(540c)는 영상 정보/신호, 오디오 정보/신호, 데이터, 및/또는 사용자로부터 입력되는 정보를 입력 받거나 출력할 수 있다. 입출력

부(540c)는 카메라, 마이크로폰, 사용자 입력부, 디스플레이부(540d), 스피커 및/또는 햅틱 모듈 등을 포함할 수 있다.

- [89] 일 예로, 데이터 통신의 경우, 입출력부(540c)는 사용자로부터 입력된 정보/신호(예, 터치, 문자, 음성, 이미지, 비디오)를 획득하며, 획득된 정보/신호는 메모리부(530)에 저장될 수 있다. 통신부(510)는 메모리에 저장된 정보/신호를 무선 신호로 변환하고, 변환된 무선 신호를 다른 무선 기기에게 직접 전송하거나 기지국에게 전송할 수 있다. 또한, 통신부(510)는 다른 무선 기기 또는 기지국으로부터 무선 신호를 수신한 뒤, 수신된 무선 신호를 원래의 정보/신호로 복원할 수 있다. 복원된 정보/신호는 메모리부(530)에 저장된 뒤, 입출력부(540c)를 통해 다양한 형태(예, 문자, 음성, 이미지, 비디오, 햅틱)로 출력될 수 있다.

[90] 물리 채널들 및 일반적인 신호 전송

- [91] 무선 접속 시스템에서 단말은 하향링크(downlink, DL)를 통해 기지국으로부터 정보를 수신하고, 상향링크(uplink, UL)를 통해 기지국으로 정보를 전송할 수 있다. 기지국과 단말이 송수신하는 정보는 일반 데이터 정보 및 다양한 제어 정보를 포함하고, 이들이 송수신 하는 정보의 종류/용도에 따라 다양한 물리 채널이 존재한다.

- [92] 도 6은 본 개시에 적용되는 물리 채널들 및 이들을 이용한 신호 전송 방법을 도시한 도면이다.

- [93] 전원이 꺼진 상태에서 다시 전원이 켜지거나, 새로이 셀에 진입한 단말은 S611 단계에서 기지국과 동기를 맞추는 등의 초기 셀 탐색(initial cell search) 작업을 수행한다. 이를 위해 단말은 기지국으로부터 주 동기 채널(primary synchronization channel, P-SCH) 및 부 동기 채널(secondary synchronization channel, S-SCH)을 수신하여 기지국과 동기를 맞추고, 셀 ID 등의 정보를 획득할 수 있다.

- [94] 그 후, 단말은 기지국으로부터 물리 방송 채널(physical broadcast channel, PBCH) 신호를 수신하여 셀 내 방송 정보를 획득할 수 있다. 한편, 단말은 초기 셀 탐색 단계에서 하향링크 참조 신호(DL RS: Downlink Reference Signal)를 수신하여 하향링크 채널 상태를 확인할 수 있다. 초기 셀 탐색을 마친 단말은 S612 단계에서 물리 하향링크 제어 채널(physical downlink control channel, PDCCH) 및 물리 하향링크 제어 채널 정보에 따른 물리 하향링크 공유 채널(physical downlink control channel, PDSCH)을 수신하여 조금 더 구체적인 시스템 정보를 획득할 수 있다.

- [95] 이후, 단말은 기지국에 접속을 완료하기 위해 이후 단계 S613 내지 단계 S616과 같은 임의의 접속 과정(random access procedure)을 수행할 수 있다. 이를 위해 단말은 물리 임의의 접속 채널(physical random access channel, PRACH)을 통해 프리앰블(preamble)을 전송하고(S613), 물리 하향링크 제어 채널 및 이에 대응하는 물리 하향링크 공유 채널을 통해 프리앰블에 대한 RAR(random access response)를 수신할 수 있다(S614). 단말은 RAR 내의 스케줄링 정보를 이용하여 PUSCH(physical uplink shared channel)을 전송하고(S615), 물리 하향링크 제어채

널 신호 및 이에 대응하는 물리 하향링크 공유 채널 신호의 수신과 같은 충돌 해결 절차(contention resolution procedure)를 수행할 수 있다(S616).

[96] 상술한 바와 같은 절차를 수행한 단말은 이후 일반적인 상/하향링크 신호 전송 절차로서 물리 하향링크 제어 채널 신호 및/또는 물리 하향링크 공유 채널 신호의 수신(S617) 및 물리 상향링크 공유 채널(physical uplink shared channel, PUSCH) 신호 및/또는 물리 상향링크 제어 채널(physical uplink control channel, PUCCH) 신호의 전송(S618)을 수행할 수 있다.

[97] 단말이 기지국으로 전송하는 제어정보를 통칭하여 상향링크 제어정보(uplink control information, UCI)라고 지칭한다. UCI는 HARQ-ACK/NACK(hybrid automatic repeat and request acknowledgement/negative-ACK), SR(scheduling request), CQI(channel quality indication), PMI(precoding matrix indication), RI(rank indication), BI(beam indication) 정보 등을 포함한다. 이때, UCI는 일반적으로 PUCCH를 통해 주기적으로 전송되지만, 실시 예에 따라(예, 제어정보와 트래픽 데이터가 동시에 전송되어야 할 경우) PUSCH를 통해 전송될 수 있다. 또한, 네트워크의 요청/지시에 의해 단말은 PUSCH를 통해 UCI를 비주기적으로 전송할 수 있다.

[98] 도 7은 본 개시에 적용 가능한 무선 프레임의 구조를 도시한 도면이다.

[99] NR 시스템에 기초한 상향링크 및 하향링크 전송은 도 7과 같은 프레임에 기초할 수 있다. 이때, 하나의 무선 프레임은 10ms의 길이를 가지며, 2개의 5ms 하프-프레임(half-frame, HF)으로 정의될 수 있다. 하나의 하프-프레임은 5개의 1ms 서브프레임(subframe, SF)으로 정의될 수 있다. 하나의 서브프레임은 하나 이상의 슬롯으로 분할되며, 서브프레임 내 슬롯 개수는 SCS(subcarrier spacing)에 의존할 수 있다. 이때, 각 슬롯은 CP(cyclic prefix)에 따라 12개 또는 14개의 OFDM(A) 심볼들을 포함할 수 있다. 일반 CP(normal CP)가 사용되는 경우, 각 슬롯은 14개의 심볼들을 포함할 수 있다. 확장 CP(extended CP)가 사용되는 경우, 각 슬롯은 12개의 심볼들을 포함할 수 있다. 여기서, 심볼은 OFDM 심볼(또는, CP-OFDM 심볼), SC-FDMA 심볼(또는, DFT-s-OFDM 심볼)을 포함할 수 있다.

[100] 표 1은 일반 CP가 사용되는 경우, SCS에 따른 슬롯 별 심볼의 개수, 프레임 별 슬롯의 개수 및 서브프레임 별 슬롯의 개수를 나타내고, 표 2는 확장된 CSP가 사용되는 경우, SCS에 따른 슬롯 별 심볼의 개수, 프레임 별 슬롯의 개수 및 서브프레임 별 슬롯의 개수를 나타낸다.

[101] [표1]

μ	$N_{\text{slot}}^{\text{slot}}$	$N_{\text{slot}}^{\text{frame}, \mu}$	$N_{\text{slot}}^{\text{subframe}, \mu}$
0	14	10	1
1	14	20	2
2	14	40	4

3	14	80	8
4	14	160	16
5	14	320	21

[102] [표2]

μ	$N_{\text{symb}}^{\text{slot}}$	$N_{\text{slot}}^{\text{frame}, \mu}$	$N_{\text{slot}}^{\text{subframe}, \mu}$
2	12	40	4

[103] 상기 표 1 및 표 2에서, $N_{\text{symb}}^{\text{slot}}$ 는 슬롯 내 심볼의 개수를 나타내고, $N_{\text{slot}}^{\text{frame}, \mu}$ 는 프레임 내 슬롯의 개수를 나타내고, $N_{\text{slot}}^{\text{subframe}, \mu}$ 는 서브프레임 내 슬롯의 개수를 나타낼 수 있다.

[104] 또한, 본 개시가 적용 가능한 시스템에서, 하나의 단말에게 병합되는 복수의 셀들간에 OFDM(A) 뉴모놀로지(numerology)(예, SCS, CP 길이 등)가 상이하게 설정될 수 있다. 이에 따라, 동일한 개수의 심볼로 구성된 시간 자원(예, SF, 슬롯 또는 TTI)(편의상, TU(time unit)로 통칭)의 (절대 시간) 구간이 병합된 셀들 간에 상이하게 설정될 수 있다.

[105] NR은 다양한 5G 서비스들을 지원하기 위한 다수의 numerology(또는 SCS(subcarrier spacing))를 지원할 수 있다. 예를 들어, SCS가 15kHz인 경우, 전통적인 셀룰러 밴드들에서의 넓은 영역(wide area)을 지원하며, SCS가 30kHz/60kHz인 경우, 밀집한-도시(dense-urban), 더 낮은 지연(lower latency) 및 더 넓은 캐리어 대역폭(wider carrier bandwidth)을 지원하며, SCS가 60kHz 또는 그보다 높은 경우, 위상 잡음(phase noise)을 극복하기 위해 24.25GHz보다 큰 대역폭을 지원할 수 있다.

[106] NR 주파수 밴드(frequency band)는 2가지 type(FR1, FR2)의 주파수 범위(frequency range)로 정의된다. FR1, FR2는 아래 표와 같이 구성될 수 있다. 또한, FR2는 밀리미터 웨이브(millimeter wave, mmW)를 의미할 수 있다.

[107] [표3]

Frequency Range designation	Corresponding frequency range	Subcarrier Spacing (SCS)
FR1	410MHz - 7125MHz	15, 30, 60kHz
FR2	24250MHz - 52600MHz	60, 120, 240kHz

[108] 또한, 일 예로, 본 개시가 적용 가능한 통신 시스템에서 상술한 뉴모놀로지(numerology)가 다르게 설정될 수 있다. 일 예로, 상술한 FR2보다 높은 주파수 대역으로 테라헤르츠 웨이브(Terahertz wave, THz) 대역이 사용될 수 있다. THz 대역에서 SCS는 NR 시스템보다 더 크게 설정될 수 있으며, 슬롯 수도 상이하게 설정될 수 있으며, 상술한 실시 예로 한정되지 않는다.

[109] 도 8은 본 개시에 적용 가능한 슬롯 구조를 도시한 도면이다.

- [110] 하나의 슬롯은 시간 도메인에서 복수의 심볼을 포함한다. 예를 들어, 보통 CP의 경우 하나의 슬롯이 7개의 심볼을 포함하나, 확장 CP의 경우 하나의 슬롯이 6개의 심볼을 포함할 수 있다. 반송파(carrier)는 주파수 도메인에서 복수의 부반송파(subcarrier)를 포함한다. RB(Resource Block)는 주파수 도메인에서 복수(예, 12)의 연속한 부반송파로 정의될 수 있다.
- [111] 또한, BWP(Bandwidth Part)는 주파수 도메인에서 복수의 연속한 (P)RB로 정의되며, 하나의 뉴모놀로지(numerology)(예, SCS, CP 길이 등)에 대응될 수 있다.
- [112] 반송파는 최대 N개(예, 5개)의 BWP를 포함할 수 있다. 데이터 통신은 활성화된 BWP를 통해서 수행되며, 하나의 단말한테는 하나의 BWP만 활성화될 수 있다. 자원 그리드에서 각각의 요소는 자원요소(Resource Element, RE)로 지칭되며, 하나의 복소 심볼이 매핑될 수 있다.
- [113] **6G 통신 시스템**
- [114] 6G (무선통신) 시스템은 (i) 디바이스 당 매우 높은 데이터 속도, (ii) 매우 많은 수의 연결된 디바이스들, (iii) 글로벌 연결성(global connectivity), (iv) 매우 낮은 지연, (v) 배터리-프리(battery-free) IoT 디바이스들의 에너지 소비를 낮추고, (vi) 초고신뢰성 연결, (vii) 머신 러닝 능력을 가지는 연결된 지능 등에 목적이 있다. 6G 시스템의 비전은 "intelligent connectivity", "deep connectivity", "holographic connectivity", "ubiquitous connectivity"와 같은 4가지 측면일 수 있으며, 6G 시스템은 하기 표 4와 같은 요구 사항을 만족시킬 수 있다. 즉, 표 4는 6G 시스템의 요구 사항을 나타낸 표이다.
- [115] [표4]

Per device peak data rate	1Tbps
E2E latency	1ms
Maximum spectral efficiency	100bps/Hz
Mobility support	Up to 1000km/hr
Satellite integration	Fully
AI	Fully
Autonomous vehicle	Fully
XR	Fully
Haptic Communication	Fully

- [116] 이때, 6G 시스템은 향상된 모바일 브로드밴드(enhanced mobile broadband, eMBB), 초-저지연 통신(ultra-reliable low latency communications, URLLC), mMTC (massive machine type communications), AI 통합 통신(AI integrated communication), 촉각 인터넷(tactile internet), 높은 스루풋(high throughput), 높은

네트워크 능력(high network capacity), 높은 에너지 효율(high energy efficiency), 낮은 백홀 및 접근 네트워크 혼잡(low backhaul and access network congestion) 및 향상된 데이터 보안(enhanced data security)과 같은 핵심 요소(key factor)들을 가질 수 있다.

- [117] 도 9는 본 개시에 적용 가능한 6G 시스템에서 제공 가능한 통신 구조의 일례를 도시한 도면이다.
- [118] 도 9를 참조하면, 6G 시스템은 5G 무선통신 시스템보다 50배 더 높은 동시 무선통신 연결성을 가질 것으로 예상된다. 5G의 핵심 요소(key feature)인 URLLC는 6G 통신에서 1ms보다 적은 단-대-단(end-to-end) 지연을 제공함으로써 보다 더 주요한 기술이 될 것으로 예상된다. 이때, 6G 시스템은 자주 사용되는 영역 스펙트럼 효율과 달리 체적 스펙트럼 효율이 훨씬 우수할 것이다. 6G 시스템은 매우 긴 배터리 수명과 에너지 수확을 위한 고급 배터리 기술을 제공할 수 있어, 6G 시스템에서 모바일 디바이스들은 별도로 충전될 필요가 없을 수 있다. 또한, 6G에서 새로운 네트워크 특성들은 다음과 같을 수 있다.
- [119] - 위성 통합 네트워크(Satellites integrated network): 글로벌 모바일 집단을 제공하기 위해 6G는 위성과 통합될 것으로 예상된다. 지상파, 위성 및 공중 네트워크를 하나의 무선통신 시스템으로 통합은 6G에 매우 중요할 수 있다.
- [120] - 연결된 인텔리전스(connected intelligence): 이전 세대의 무선 통신 시스템과 달리 6G는 혁신적이며, “연결된 사물”에서 “연결된 지능”으로 무선 진화가 업데이트될 것이다. AI는 통신 절차의 각 단계(또는 후술할 신호 처리의 각 절차)에서 적용될 수 있다.
- [121] - 무선 정보 및 에너지 전달의 완벽한 통합(seamless integration wireless information and energy transfer): 6G 무선 네트워크는 스마트폰들과 센서들과 같이 디바이스들의 배터리를 충전하기 위해 전력을 전달할 것이다. 그러므로, 무선 정보 및 에너지 전송 (WIET)은 통합될 것이다.
- [122] - 유비쿼터스 슈퍼 3D 연결(ubiquitous super 3-dimention connectivity): 드론 및 매우 낮은 지구 궤도 위성의 네트워크 및 핵심 네트워크 기능에 접속은 6G 유비쿼터스에서 슈퍼 3D 연결을 만들 것이다.
- [123] 위와 같은 6G의 새로운 네트워크 특성들에서 몇 가지 일반적인 요구 사항은 다음과 같을 수 있다.
- [124] - 스몰 셀 네트워크(small cell networks): 스몰 셀 네트워크의 아이디어는 셀룰러 시스템에서 처리량, 에너지 효율 및 스펙트럼 효율 향상의 결과로 수신 신호 품질을 향상시키기 위해 도입되었다. 결과적으로, 스몰 셀 네트워크는 5G 및 비온드 5G (5GB) 이상의 통신 시스템에 필수적인 특성이다. 따라서, 6G 통신 시스템 역시 스몰 셀 네트워크의 특성을 채택한다.
- [125] - 초 고밀도 이기종 네트워크(ultra-dense heterogeneous network): 초 고밀도 이기종 네트워크들은 6G 통신 시스템의 또 다른 중요한 특성이 될 것이다. 이기종 네트워크로 구성된 멀티-티어 네트워크는 전체 QoS를 개선하고 비용을 줄인다.

- [126] - 대용량 백홀(high-capacity backhaul): 백홀 연결은 대용량 트래픽을 지원하기 위해 대용량 백홀 네트워크로 특징지어진다. 고속 광섬유 및 자유 공간 광학(FSO) 시스템이 이 문제에 대한 가능한 솔루션일 수 있다.
- [127] - 모바일 기술과 통합된 레이더 기술: 통신을 통한 고정밀 지역화(또는 위치 기반 서비스)는 6G 무선통신 시스템의 기능 중 하나이다. 따라서, 레이더 시스템은 6G 네트워크와 통합될 것이다.
- [128] - 소프트화 및 가상화(softwarization and virtualization): 소프트화 및 가상화는 유연성, 재구성성 및 프로그래밍 가능성을 보장하기 위해 5GB 네트워크에서 설계 프로세스의 기초가 되는 두 가지 중요한 기능이다. 또한, 공유 물리적 인프라에서 수십억 개의 장치가 공유될 수 있다.
- [129] 양자 커뮤니케이션
- [130] 양자 통신이란 양자역학적 특성을 정보통신 분야에 적용하여 보안, 초고속 연산 등 기존 정보통신의 한계를 극복할 수 있는 차세대 통신 기술이다. 양자 통신은 기존 통신 기술에서 이용되는 2진 비트 정보에 따른 0과 1의 형태로 표현할 수 없거나, 표현하기 곤란한 형태의 정보를 생성, 전송, 처리, 저장하는 수단을 제공한다. 기존 통신 기술들에서는 파장이나 진폭 등이 송신단-수신단 간의 정보 전송에 이용되었으나, 이와 달리, 양자 통신에서는 빛의 최소 단위인 광자(photon)가 송신단-수신단 간의 정보 전송을 위해 이용된다. 특히, 양자 통신의 경우, 광자(빛)의 편광이나 위상차에 대해 양자 불확정성과 양자 비가역성, 복제 불가능성이 사용될 수 있으므로, 양자 통신은 완벽한 보안이 보장되는 통신이 가능하다는 특성을 가진다. 또한, 양자 통신은 특정한 조건에서 양자 얽힘을 이용해 초고속 통신이 가능할 수도 있다
- [131] 동형 암호
- [132] 동형 암호란 암호화한 데이터를 복호화하지 않은 상태에서 연산할 수 있는 암호화 방식을 일컫는다. 이 때, 암호화한 상태에서의 연산 결과 역시 암호화된 형식이며, 이를 복호화하여 얻은 평문(plaintext)은 연산에 이용된 암호문이 암호화되기 전의 데이터 간의 연산 결과와 같다. 예를 들어, 암호화 대상이 되는 데이터인 평문(plaintext) m_1 과 m_2 에 곱셈 연산($*$)에 대한 동형암호 E 를 사용하여 비밀 키 k 로 암호화한 암호문을 각각 $E_k(m_1)$, $E_k(m_2)$ 라 할 때 동형암호는 $E_k(m_1 * m_2) = E_k(m_1) * E_k(m_2)$ 를 만족한다. 즉, 동형(同型)이란, 암호화된 상태에서 연산한 결과가 연산을 한 뒤 암호화한 결과와 같다는 의미를 내포하고 있다. 동형암호는 크게 부분 동형암호(PHE: Partially Homomorphic Encryption), 제한 동형암호(SHE: Somewhat Homomorphic Encryption), 단계적 완전 동형암호(Leveled Fully Homomorphic Encryption), 완전 동형암호(FHE: Fully Homomorphic Encryption)의 4개로 분류될 수 있다. PHE는 덧셈 혹은 곱셈 연산 중 하나만 가능한 암호를 의미하며, SHE는 덧셈/곱셈 연산 모두 가능한 암호다. Leveled FHE는 덧셈, 곱셈 연산이 가능하지만 연산 가능 횟수에 제한이 있다. 마지막으로 FHE는 덧셈, 곱

샘 연산이 모두 가능하고, 연산 가능 횟수에 제한이 없는 암호로, 대부분이 격자(lattice) 위에서 정의된 수학적으로 풀기 어려운 난제에 기반을 두고 있다.

[133] 일반적으로 클라우드 컴퓨팅에서 대칭키 알고리즘(symmetric key algorithm)을 이용해 데이터를 암호화하면 암호화 속도도 빠르고 데이터가 효율적으로 저장될 수 있다. 그러나, 클라우드 컴퓨팅에서 암호화된 데이터에 연산이 수행되어야 할 경우, 반드시 암호화된 데이터를 복호화한 후 연산 한 후, 다시 암호화해야 한다. 이때 복호화 과정에서 클라우드 서버가 개인 비밀키를 알고 있어야 한다. 클라우드 서버가 개인 비밀키를 모르는 경우에는 개인이 자신의 자료를 다운로드한 뒤 복호화해야 하는 문제가 발생한다. 반면, 동형암호는 연산 수행 속도가 느리다는 단점이 있는 반면 정보를 안전하게 보호한 채로 연산이 가능하여 개인정보 보안이 필요한 클라우드 서비스에 주로 사용되며, 빅데이터 분석과 암호화폐 등에 활용될 수 있다.

[134] 동형 암호가 통신에 적용되는 대표적인 예시로는 동형 암호 기반의 다자간 통신 방법이 있다. 이하에서, 본 개시에서 제안하는 방법에 대한 이해를 돕기 위해, 도 10을 참조하여 다자간 통신의 일반적인 개념 및 기존 다자간 통신에서의 암호화 방법들에 대해서 설명한다.

[135] 도 10은 다자간 통신의 일 예를 나타낸 도이다. 보다 구체적으로, 도 10은 높은 수준의 설계 목표를 해결하기 위한 종단 간 암호화된 VoIP 원격 회의 기술에 관한 것이다. 도 10에서, 각 클라이언트(1010/1020/1030/1040)는 사용자의 음성 데이터를 샘플링하고 인코딩하고 암호화한 다음 암호화된 VoIP 데이터 스트림을 서버의 VoIP 믹서로 보낸다. 믹서는 암호화된 VoIP 데이터의 반환 스트림을 보낸 다음 클라이언트에서 암호를 해독하고 디코딩하여 클라이언트 사용자에게 재생한다. 이 때, 구현될 수 있는 추가 동형을 지원하는 모든 암호화 시스템이 사용될 수 있다. 도 10의 경우, 공유 비밀 키를 사용하는 데 중점을 두에 따라, 곱셈 동형을 사용하지 않는 것 외에도 공개 키 기능이 사용되지 않습니다. 클라이언트의 입력 음성 스트림은 샘플링되고 공유 비밀 키를 사용하여 동형 암호화된다. 암호화된 음성 샘플은 암호화 키에 액세스할 수 없는 SIPHER 지원 VoIP 서버로 전송된다. VoIP 서버는 암호화된 오디오 피드를 결합하고 밸런싱(balancing)을 수행한다. 결합된 출력은 클라이언트 핸드셋으로 전달되며 여기서 암호가 해독되고 사용자를 위해 재생된다. 처리 결과는 클라이언트로 전송되며 클라이언트 개인 키를 사용하여 해독된다. 원격 회의 서버에는 키가 저장되지 않으므로 공격자가 서버에서 모든 통신 링크 및 작업을 보는 경우에도 개인 정보가 보호될 수 있다.

[136] 이하에서, 본 개시에서 제안하는 동형 암호 기반의 통신 방법에 대해서 설명하기에 앞서, 본 개시에서 제안하는 방법에 대한 이해를 돕기 위해 대칭키 암호에 대해 설명한다.

[137] <본 발명 관련 내용>

[138] 대칭키 암호

- [139] 대칭키 암호란 암호화 및 복호화 과정에 동일한 비밀키를 사용하는 암호를 의미한다. 암호화에 필요한 키가 공개되고, 복호화에 필요한 키가 공개되지 않는 방식이 사용되는 공개키 암호와 비교하면, 대칭키 암호는 송신단과 수신단 사이의 키 공유 과정이 선행되어야 한다는 단점이 있으나, 데이터에 대한 계산 속도는 공개키 암호에 비하여 월등히 빠른 계산 속도를 가지므로, 실제 데이터 암호화 과정에서는 대칭키 암호 방식이 사용되며, 공개키 암호 방식은 키 공유 과정 등에서 활용될 수 있다.
- [140] 대칭키 암호에 대해서 보다 구체적으로 설명하면, 대칭키 암호는 일반적으로 정해진 라운드 함수를 여러 번 반복하는 형태로 구성되는데, 상기 라운드 함수 각각은 S(substitution)-box를 사용하여 암호화 과정에 대한 입력 데이터의 일부 비트를 복잡하게 섞는(스크램블링하는) 비선형층과, 복잡하게 섞인(스크램블링된) 일부의 비트를 전체적으로 넓게 퍼트리는데(입력 데이터 전체에 대해 확장시키는) 선형층으로 구성된다. 여기서, 비선형층의 복잡도는 대칭키 암호 알고리즘의 안전성을 결정하는 중요한 요소(factor)일 수 있다. 라운드 함수의 반복 횟수(라운드 수)를 증가시키는 경우, 알고리즘의 안전성이 강화될 수 있지만, 반대로 데이터 암호화에 소요되는 계산 시간이 증가되게 되어 전체적인 효율성은 저하될 수 있다. 상기 S-box는 블록암호를 이루고 있는 구성요소로, 입력과 출력 사이의 관계가 테이블 또는 수학적 관계로 정의되는 공개된 비선형 함수로 이해될 수 있다. 보다 구체적으로, S-box 자체가 데이터를 '암호화'하는 능력이 있다기 보다는, 암호화 함수 계산 과정에서 평문과 비밀키가 관계되어 생성되는 값이 S-box에 입력으로 되면 데이터가 암호화될 수 있다. 입력의 크기와 출력의 크기가 같지 않아도 되는데, 보다 구체적으로, 입력은 n 비트이고 출력은 m 일때, n 과 m 이 같을 필요는 없다. 또한, S-box는 입력값과 출력값 사이의 관계가 테이블 또는 수학적 관계로 정의되는 치환 암호로 이해될 수 있는데, S-box는 역함수가 존재할 수도 있고, 존재하지 않을 수도 있으며, 역함수가 존재하는 S-box는 입력 비트와 출력 비트의 크기가 동일하다. S-box 에서 사용되는 연산의 종류로는 substitution, Exclusive-OR, Shift, Swap, Split, Combine이 있을 수 있으며, 상기 연산의 종류들이 입력 데이터의 암호화에 사용될 수 있다.
- [141] **Feistel 구조의 대칭키 암호**
- [142] 도 11은 Feistel 구조 대칭키 암호의 일 예를 나타낸 도이다. Feistel 구조는 대칭키 암호를 설계하는 방법 중 하나로, 첫 번째 국제 표준 암호인 DES (Data Encryption Standard)에 사용된 방식이다. 도 11에 도시된 것과 같이, Feistel 구조는 같이 내부 상태의 절반과 라운드 키를 라운드 함수에 입력하고, 그 결과물을 나머지 상태에 더해주는 과정이 반복되는 구조이다. 즉, Feistel 구조는 적어도 한번 이상 반복되는 라운드 함수에 기반하는데, 각 라운드마다 라운드키 k_i 와 데이터의 전체 상태의 절반에 대해 고정된 비선형 함수 f 를 적용하고, 여기서 얻어지는 출력값에 데이터 전체 상태의 나머지 절반이 더해진다. 도 11의 1110은 Feistel 구조에서의 첫 번째 라운드를 나타내는데, 본 라운드에 라운드키 k_1 와 데이터의

전체 상태의 절반($R0$)에 대해 고정된 비선형 함수 f 를 적용하고, 여기서 얻은 출력값에 데이터 전체 상태의 나머지 절반($L0$)이 더해진다. 이 과정에서 내부 상태의 크기를 정확히 절반으로 나누는 것이 아니라, 나누어지는 내부 상태를 서로 다른 크기로 나누어 라운드 함수의 입출력 크기로 사용하는 구조는 **unbalanced Feistel** 구조로 호칭될 수 있다. 또한, 내부 상태를 여러 개의 브랜치로 나누는 구조는 일반화된(**generalized**) Feistel 구조로 호칭될 수 있다.

[143] **동형암호-대칭키 암호 하이브리드 프레임워크(Hybrid Framework)**

[144] 앞서 설명한 것과 같이, 동형암호는 데이터가 암호화된 상태에서도 비밀키 없이 데이터에 대한 연산이 가능하도록 설계된 암호이다. 일반적으로, 동형암호에 기반한 통신은 클라이언트가 서버에 데이터를 전송하여 계산을 위탁하는 공개키 암호 형태로 사용된다. 보다 구체적으로, 클라이언트는 데이터의 동형암호문을 생성하여, 생성된 동형암호문을 서버로 전달한다. 이후, 상기 서버는 상기 클라이언트로부터 전달받은 동형암호문에 대한 동형 연산을 통해 클라이언트가 원하는(위탁한) 계산을 수행하여 동형 연산의 결과를 획득한 후, 상기 획득된 동형 연산의 결과를 상기 클라이언트로 돌려준다. 다음, 상기 클라이언트는 상기 서버로부터 전달받은 동형암호문을 복호화하여 평문 데이터 상의 계산 결과를 획득할 수 있다.

[145] 이하에서, 클라이언트는 통신 시스템에서의 단말 등으로 이해될 수 있고, 서버는 통신 시스템에서의 기지국/네트워크 등으로 이해될 수 있다.

[146] 위와 같은 공개키 암호 형태의 동형암호 기반 통신의 경우(클라이언트-서버 시나리오), 클라이언트가 동형암호를 통해 직접 데이터를 암호화할 경우 동형암호의 특성상 동형암호문의 크기가 원본 데이터보다 커지는 암호문 확장이 필연적으로 일어난다는 문제가 있다. 또한, 동형암호화되는 파라미터에 따라 동형암호문의 크기는 원본 데이터와 대비하여 약 수십 배에서 수 백배까지 커질 수 있어, 클라이언트가 서버로 전송하는 데이터 전송량이 크게 늘어날 뿐만 아니라, 서버에서 동형암호문 데이터를 오래 저장해야 하는 경우, 서버 측의 저장 공간도 많이 차지하게 되는 문제가 있다. 위와 같은 문제 해결을 위해, 도 11의 동형암호-대칭키 암호 하이브리드 프레임워크가 사용될 수 있다.

[147] 도 12는 동형암호-대칭키 암호 하이브리드 프레임워크의 일 예를 나타낸 도이다. 동형암호-대칭키 암호 하이브리드 프레임워크에서는 클라이언트(1210)가 대칭키 암호를 통해 데이터를 암호화하여 서버(1220)로 전송하고, 서버(1220)는 대칭키 암호를 통해 암호화된 대칭키 암호문을 동형암호문으로 바꾸는 연산을 수행하는 방식이 사용된다. 보다 구체적으로, 도 12를 참조하면, 클라이언트(1210)는 대칭키 암호 E 에 대한 비밀키 k 를 동형암호를 이용해 암호화하여 $EncHE(k)$ 를 서버(1220)로 먼저 전송한다. 이후, 클라이언트(1210)는 데이터 m 을 대칭키 암호 E 와 비밀키 k 를 이용해 암호화하여 $E_k(m)$ 을 서버(1220)로 전송한다.

[148] 이후, 서버(1220)는 클라이언트(1210)로부터 수신한 대칭키 암호문 $c=E_k(m)$ 으로부터 데이터 m 에 대한 동형암호문 $EncHE(m)$ 을 얻기 위해, 동형암호문

EncHE(c)를 먼저 계산하고, EncHE(k)를 이용해 E의 복호화 연산 E-1을 동형 연산으로 수행한다(도 12의 EvalHE(E-1)). 동형암호-대칭키 암호 하이브리드 프레임워크에서, 클라이언트(1210)는 대칭키 암호의 비밀키가 변경되기 전까지는 EncHE(k)를 서버(1220)로 한 번만 전송되면 된다. 비밀키에 대한 동형 암호문 생성 이외에, 클라이언트(1210)는 실제 데이터를 암호문 확장이 일어나지 않는 대칭키 암호문 형태로 전송하므로, 클라이언트(1210)가 서버(1220)로 전송하는 데이터의 전송량은 늘어나지 않을 수 있다.

[149] 동형암호 친화적 대칭키 암호

[150] 앞서 설명한 하이브리드 프레임워크가 효율적으로 운용되기 위해서는 대칭키 암호에 대한 동형 연산이 효율적으로 수행될 수 있어야 한다. 즉, 도 11에 도시된 EvalHE(E-1)이 효율적으로 계산될 수 있는 대칭키 암호 E가 사용되어야 한다. 사용되는 동형암호 알고리즘에 따라 다를 수는 있지만, 일반적으로 동형 연산은 덧셈이나 상수 곱과 같은 선형 연산은 가벼운(계산 자원이 많이 요구되지 않는) 반면, 곱셈과 같은 비선형 연산의 경우 해당 연산을 위해 더 많은 계산 자원이 요구된다.

[151] 이러한 동형 연산의 특성을 고려하여 동형 연산을 통해 효율적으로 계산될 수 있도록 만들어진 암호를 동형암호 친화적 대칭키 암호라고 하며, 동형암호 친화적 대칭키 암호와 관련된 연구가 꾸준히 진행되고 있으며, 기존 동형암호 친화적 대칭키 암호 연구는 대부분 덧셈과 곱셈 연산을 지원하는 동형암호 알고리즘에 대한 것이었다. 앞서 설명한 것처럼 곱셈 연산이 덧셈 연산에 비해 계산 자원을 많이 소모하기 때문에, 덧셈과 곱셈 연산을 지원하는 동형암호 알고리즘 친화적 대칭키 암호는 기본적으로 간단한 비선형층과 적은 라운드 수를 가지도록 설계될 수 있다. 이와 같이 설계된 동형암호 알고리즘 친화적 대칭키 암호는 대칭키 암호의 안전성을 감소되는 문제가 있는데, 대칭키 암호의 안전성을 감소되는 문제를 해결하기 위한 방법으로 선형층을 매 암호화 과정마다 랜덤하게 생성하는 구조의 동형암호 알고리즘 친화적 대칭키 암호가 제안되었다. 매 암호화 과정마다 선형층이 달라지도록 설계함으로써, 동일한 함수에 대한 입출력 데이터를 수집하여 분석하는 공격 기법들에 대한 방어가 가능해지는데, 이 때 선형층을 랜덤하게 생성하는 과정은 비밀키에 대한 정보 없이 공개적으로 수행되므로, 대칭키 암호를 동형 연산으로 계산하는 과정에 큰 부담을 주지 않는다.

[152] Concrete 동형암호 알고리즘

[153] Concrete 동형암호 알고리즘이란, 비트 연산을 지원하는 TFHE 알고리즘이 확장된 형태의 동형암호 알고리즘이다. Concrete 동형암호 알고리즘에서는 덧셈 연산과 테이블 참조 연산을 지원하며, 덧셈 연산에 비해 테이블 참조 연산이 더 무겁다(계산 자원이 더 많이 요구된다.). 현재까지 개발된 유일한 Concrete 친화적 대칭키 암호로는 Elisabeth 암호가 있다.

[154] Concrete 동형암호 알고리즘에서의 테이블 참조 연산은 PBS(programmable bootstrapping)이라는 연산을 통해 수행될 수 있으며, 부트스트래핑

(bootstrapping)이란 암호문이 가지고 있는 노이즈를 제거하여 동형연산이 계속 수행될 수 있도록 만들어주는 과정이다. Concrete 동형암호 알고리즘의 경우, 부트스트래핑 과정에서 단순히 노이즈만 제거되는 것이 아니라, 부트스트래핑 과정을 통해 암호문이 가지고 있는 입력 값에 대한 테이블 참조 연산이 추가적으로 수행될 수 있도록 할 수 있다. 테이블 참조 연산이란, 동형 연산이 수행되는 입력 값과 상기 입력 값에 대한 상기 동형 연산의 결과 값(출력 값) 간의 맵핑 관계를 사전 설정하고, 상기 사전 설정된 맵핑 관계를 사용하여 수행되는 동형 연산을 의미할 수 있다. 즉, 예를 들어, x_1 이라는 입력 값에는 y_1 이라는 동형 연산의 결과 값(출력 값)이 대응되도록 맵핑 관계가 설정되면, x_1 이라는 입력 값에 대한 동형 연산 수행 시, 상기 사전 설정된 맵핑 관계를 사용하여 y_1 이라는 동형 연산의 결과 값이 획득될 수 있다. 여기서, 상기 사전 설정된 맵핑 관계가 테이블일 수 있다.

[155] 테이블 참조 연산을 가능하게 하는 상기 PBS 연산의 핵심은 블라인드 로테이션(blind rotation) 연산이다. 상기 블라인드 로테이션이란, 계산하고자 하는 함수가 테이블 형태로 주어지고 입력값이 암호문으로 주어졌을 때, 입력값을 복구하지 않고도 입력 값만큼 테이블을 회전시킨 결과가 암호문 형태로 획득될 수 있도록 하는 연산이다. 보다 구체적으로, 상기 블라인드 로테이션은 동형 연산의 입력 값이 암호화된 값인 경우, 상기 암호화된 값인 상기 동형 연산의 입력 값에 대한 복호화 없이, 상기 암호화된 값인 상기 동형 연산의 입력 값만큼 회전된 상기 사전 설정된 맵핑 관계(테이블)에 기초하여, 상기 암호화된 값인 상기 동형 연산의 입력 값에 대응되는 암호화된 결과 값이 획득되도록 하는 연산인 것으로 이해될 수 있다.

[156] 도 13은 PBS 연산이 수행되는 일 예를 나타낸 도이다. 도 13을 참조하면, 블라인드 로테이션을 수행하기 위해서는 입력값의 암호문을 GSW라는 특수한 형태의 암호문으로 변환해야 하는데, PBS 연산에 소요되는 시간 중, 대부분의 시간이 입력값의 암호문을 GSW(Gentry-Sahai-Waters) 암호문으로 변환하는 과정에 사용된다. 도 13에서, 1310은 암호화되지 않은 입력 값에 대한 테이블을 나타낸다. 1310을 참조하면, 입력 값 0에 대응하는 출력 값은 $f(0)$, 입력 값 1에 대응하는 출력 값은 $f(1)$ 등과 같다. 도 13을 참조하면, 특정한 입력 값에 대한 암호문 x 에 대한 출력 값인 $f(x)$ 를 얻기 위해 블라인드 로테이션(1330)이 수행될 수 있다. 블라인드 로테이션은 블라인드 로테이션을 가능하게 하기 위한 GSW 변환(GSW transform) 과정을 포함한다. 1310의 테이블에 대한 블라인드 로테이션의 결과, 블라인드 로테이션이 적용된 암호화된 입력값과, 암호화된 입력 값에 대응되는 출력 값들에 대한 맵핑 관계를 포함하는 1320의 테이블이 획득된다. 1320의 테이블을 참조하여 입력 값 x 에 대한 출력 값인 $f(x)$ 이 획득될 수 있으며, 이 때 샘플 추출 및 키 스위칭(1340)이 적용될 수 있다.

[157] 이중 블라인드 로테이션(double blind rotation)을 통한 동형 연산 방법

- [158] 본 개시는 이중 블라인드 로테이션(double blind rotation)을 통한 동형 연산 방법을 제안한다. 보다 구체적으로, 본 개시에서 제안하는 방법은 Concrete 동형암호 친화적 대칭키 암호 설계를 목적으로 특수한 구조의 unbalanced Feistel 암호를 Concrete 동형암호 알고리즘으로 계산할 때 PBS 연산 효율을 높일 수 있는 이중 blind rotation 방식일 수 있다.
- [159] 보다 구체적으로, 본 개시가 제안하는 이중 블라인드 로테이션 방식은, 계산하고자 하는 함수 f 에 대한 입력으로 $(x+y)$ 가 주어진 경우, $(x+y)$ 의 GSW 암호문을 계산하는 것이 아니라, x 에 대한 GSW 암호문 및 y 에 대한 GSW 암호문을 각각 별도로 계산하고, 블라인드 로테이션을 두 번 적용하여 $f(x+y)$ 를 계산하는 방식이다. 이중 블라인드 로테이션을 사용할 경우 GSW 암호문 변환이 수행되는 횟수가 한 번에서 두 번으로 증가하므로, 일반적으로는 비효율적일 수 있다. 하지만, 대칭키 암호를 계산하는 과정은 일반적으로 비선형 함수 f 에 대해 현재 상태 x 에 라운드키 k 를 더한 값을 입력으로 $f(x+k)$ 를 계산하는 구조를 갖는데, 라운드키 k 는 키를 업데이트 하기 전까지 계속 동일한 값을 사용하기 때문에 사전에 라운드키 k 에 대한 GSW 변환을 한 번만 수행하여 저장해두는 경우, 사전에 라운드키 k 에 대한 GSW 변환이 수행된 GSW 암호문은 여러 번의 암호화 과정에 계속해서 사용될 수 있다. 특히, 이와 같은 이중 블라인드 로테이션 방법은 하나의 상태 값이 여러 라운드 함수에 적용되는 unbalanced Feistel 구조에서의 계산 효율을 크게 증가시킬 수 있다.
- [160] 도 14는 PBS 연산이 수행되는 또 다른 일 예를 나타낸 도이다. 보다 구체적으로, 도 14는 PBS 연산 시 블라인드 로테이션이 두 번 수행되는 방식에 관한 것이다. 도 14에서, 1410은 암호화되지 않은 입력 값에 대한 테이블을 나타낸다. 1410을 참조하면, 입력 값 0에 대응하는 출력 값은 $f(0)$, 입력 값 1에 대응하는 출력 값은 $f(1)$ 등과 같다. 도 14를 참조하면, 특정한 입력 값에 대한 암호문 x_1 에 대한 출력 값인 $f(x_1)$ 를 얻기 위해 첫 번째 블라인드 로테이션(1420)이 수행될 수 있다. 첫 번째 블라인드 로테이션은 블라인드 로테이션을 가능하게 하기 위한 입력값 x_1 에 대한 GSW 변환(GSW transform) 과정을 포함한다. 이 때, 본 개시에서 제안하는 이중 블라인드 로테이션 방법에 따르면, 입력 값 (x_1+k_j) 에 대한 블라인드 로테이션이 수행되는 것이 아니라, 먼저 x_1 에 대한 첫 번째 블라인드 로테이션(1420)이 수행되므로, 그 결과 x_1 만큼 1410의 테이블이 회전된 형태를 갖는 테이블(1430)이 획득된다. 다음, 라운드 키 k_j 에 기초한 두 번째 블라인드 로테이션(1440)이 수행된다. 두 번째 블라인드 로테이션은 블라인드 로테이션을 가능하게 하기 위한 입력값 k_j 에 대한 GSW 변환(GSW transform) 과정을 포함하고, GSW 변환이 수행된 k_j 의 GSW 암호문은 사전 계산되어 저장될 수 있다. 두 번째 블라인드 로테이션(1440)의 결과, 1430의 테이블이 k_j 만큼 회전된 형태를 갖는 테이블(1450)이 획득된다. 결과적으로, 1450의 테이블은 1410의 테이블이 (x_1+k_j) 만큼 회

전된 형태를 가지며, 1450의 테이블을 참조하여 암호화된 입력 값 x_i+k_j 등에 대한 출력 값인 $f(x_i+k_j)$ 등이 획득될 수 있다.

[161] Unbalanced Feistel 구조에서의 이중 블라인드 로테이션 방식

[162] 앞서 설명한 것과 같이, 본 개시에서 제안하는 이중 블라인드 로테이션 방식이 Unbalanced Feistel 구조에 적용되는 경우 효과를 얻을 수 있다. 도 15는 unbalanced Feistel 구조의 일 예를 나타낸 도이다. 도 15를 참조하면, unbalanced Feistel 구조는 내부 상태가 여러 개의 브랜치($x_1, x_2, x_3, \dots, x_l$)로 이루어져있고, 라운드 함수는 공통 입력 브랜치를 가짐을 알 수 있다. unbalanced Feistel 구조는 적어도 한번의 라운드로 이루어지는데, 상기 적어도 한번의 라운드 각각에서, (i) 상기 적어도 한번의 라운드에서 공통적으로 사용되는 공통 입력 데이터(x_1) 및 (ii) 상기 적어도 한번의 라운드 각각에서 개별적으로 사용되는 라운드 키(k_{l-1})가 상기 적어도 한번의 라운드 각각의 라운드 함수에 입력되어 출력되고, 상기 적어도 한번의 라운드 각각에서, 상기 적어도 한번의 라운드 각각의 라운드 함수의 출력 값에 상기 적어도 한번의 라운드 각각에서 개별적으로 사용되는 개별 입력 값(x_l)이 더해져서 출력될 수 있다.

[163] 도 15를 참조하여 첫 번째 라운드의 수행 방식에 대해 설명하면, 해당 라운드에서 공통 입력 데이터(x_1)(1511) 및 해당 라운드에서 사용되는 라운드 키(k_1)(1513)가 해당 라운드의 라운드 함수(f_1)(1515)에 입력되어 출력되고, 상기 라운드 함수의 출력 값에 해당 라운드에서 개별적으로 사용되는 개별 입력 값(x_2)(1517)이 더해져서 출력될 수 있다(y_2). 이와 별개로, 공통 입력 값(x_1)에 대해서 어떤 연산도 수행되지 않은 y_1 도 출력될 수 있다. 여기서, $y_1, y_2, \dots, y_l$ 은 도 15의 실시 예에서 입력 값 $x_1, \dots, x_l$ 이 한 라운드를 거친 후의 결과 값에 해당한다. 입력 값이 여러 라운드를 거쳐 얻어진 최종 결과 값을 키스트림이라 호칭할 수 있다. 도 15의 unbalanced Feistel 구조에서 단일 블라인드 로테이션에 따르면, 한 라운드의 계산 시 f_i 가 x_i+k_i+1 를 입력으로 가지므로, 총 $l-1$ 개의 GSW 암호문이 계산되어야 하나, 본 개시에서 제안하는 이중 블라인드 로테이션 방식이 적용되는 경우, 각 k_i 대한 GSW 암호문을 사전 계산해두고, 실제 암호화 과정에서는 공통 입력값(x_1) 대한 GSW 암호문만 계산하여, f_i 를 나타내는 테이블이 x_1 으로 한 번, 이후 k_i 로 다시 한번 총 2번의 블라인드 로테이션을 수행하여 $f_i(x_1+k_i)$ 가 계산될 수 있다.

[164] 랜덤하게 생성되는 비선형층을 사용하는 Concrete 친화적 대칭키 암호 설계 방식에의 결합

[165] 본 개시에서 제안하는 방법은 랜덤하게 생성되는 비선형층을 사용하는 동형 암호 친화적(concrete 친화적) 대칭키 암호화 방식에 결합될 수 있다.

[166] 보다 구체적으로, 본 개시에서 제안하는 이중 블라인드 로테이션 기법은 계산하고자 하는 비선형 함수 f 의 구체적인 함수값에 의존하지 않으므로, 위의 unbalanced Feistel 구조에서 비선형 함수들이 매 암호화마다 랜덤하게 생성되는 구조를 가지고 있더라도 동일하게 적용될 수 있다.

- [167] 랜덤하게 생성되는 비선형층을 사용하는 동형 암호 친화적(concrete 친화적) 대칭키 암호화 방식에 이중 블라인드 로테이션 기법을 결합하면, 비선형층을 랜덤 생성함으로써 필요한 전체 라운드 수를 줄일 수 있을 뿐 아니라, 각 라운드를 계산하는 시간 또한 이중 블라인드 로테이션 기법을 통해 크게 감소될 수 있다.
- [168] 도 16은 랜덤하게 생성되는 비선형층을 사용하는 동형 암호 친화적 대칭키 암호화 방식에 이중 블라인드 로테이션 기법이 결합된 일 예를 나타낸 도이다. 도 16을 참조하면, 매 암호화 라운드마다 비선형 함수 $f_1, f_2, \dots, f_i$ 이 XOF(1610)로부터 테이블 형태로 랜덤하게 생성될 수 있으며, 동일한 입력 브랜치(1621)를 가지는 $f_2, \dots, f_i$ 함수의 계산은 본 개시에서 제안되는 이중 블라인드 로테이션 기법을 사용하여 효율적으로 이루어질 수 있다. 도 16을 참조하여 첫 번째 라운드의 수행 방식에 대해 설명하면, 해당 라운드에서 공통 입력 데이터(x_1)(1621) 및 해당 라운드에서 사용되는 라운드 키(rk_2)(1623)가 해당 라운드의 라운드 함수(f_2)(1625)에 입력되어 출력된다. 이 때, 상기 라운드 함수(1625)는 XOF(1610)에 의해 랜덤하게 생성된 것일 수 있다. 상기 라운드 함수의 출력 값에 해당 라운드에서 개별적으로 사용되는 개별 입력 값(x_2)(1627)이 더해져서 출력될 수 있다(y_2)(1629).
- [169] 다양한 방식의 PBS 계산 방식에의 이중 블라인드 로테이션 방식 적용
- [170] 본 개시에서 제안하는 이중 블라인드 로테이션을 이용한 최적화 기법은 도 13 및 도 14의 PBS 기법 외의 다양한 PBS 기법에서도 적용이 가능하다. 보다 구체적으로, 본 개시에서 제안하는 이중 블라인드 로테이션을 이용한 최적화 기법은 입력 암호문을 GSW 암호문 형태로 바꾸어서 블라인드 로테이션을 수행하는 것이 아니라, 입력 암호문을 GLWE(Generalized LWE, generalized Learning With Errors) 암호문 형식으로 바꾸어 계산하고자 하는 함수를 나타내는 다항식에 곱하는 방식에도 적용 가능하다.
- [171] GLWE 암호문이란 변수 X 에 대한 다항식을 메시지로 가지는 암호문을 의미한다. GLWE 암호문을 이용한 블라인드 로테이션 방식은 메시지 m 에 대한 동형 암호문을 X^m 에 대한 GLWE 형태의 동형암호문으로 바꾸는 과정을 통해 이루어진다. GLWE 암호문의 경우, 계산하고자 하는 함수 f 또한 X 에 대한 다항식 $P_f(X)$ 형태로 만들어지는데, 이때 P_f 의 각 계수에 f 의 함수값들이 저장된다. GLWE 암호문에 기반한 PBS 연산의 핵심 아이디어는 m 에 대한 동형암호문과 함수 f 가 주어졌을 때, 다항식 $X^m P_f(X)$ 의 상수항은 함수값 $f(m)$ 이 되도록 하는 것이다. 즉, P_f 라는 함수 f 에 대한 테이블이 GLWE 암호문 X^m 에 의해 m 의 값만큼 회전하게 되는 것이다.
- [172] 일반적으로, 동형 연산으로 $X^m P_f(X)$ 에 대한 암호문을 얻기 위해서는, 메시지 m 에 대한 동형암호문과 다항식 P_f 로부터 CMux 연산을 여러 번 반복하여 $X^m P_f(X)$ 에 대한 암호문이 획득된다. LWE 암호문에 기반한 PBS 연산에서도 unbalanced Feistel 구조 계산에 공통적으로 나타나는 $f(a+b)$ 형태의 테이블 참조 연산 시 이중 블라인드 로테이션을 사용하는 방식이 적용될 수 있는데, X^a 와 X^b 에 대한

GLWE 암호문을 CMux 연산을 통해 계산한 뒤, GLWE 암호문 사이의 곱셈 연산을 통해 $X^{a+b}P_f(X)$ 에 대한 암호문이 계산될 수 있다. a와 b 중 하나가 공통적으로 여러 번 사용되는 값이라면 GLWE 암호문은 한 번만 계산해두고 f에 대한 테이블을 두 번 회전하는 방식으로 이중 블라인드 로테이션 기법이 동일한 방식으로 사용할 수 있다.

[173] 효과

[174] 기존의 동형 암호 계산 방식의 경우, 매 라운드마다 계산되어야 하는 비선형 함수의 개수만큼 GSW 암호문이 계산되어야 한다. 반면, 본 개시에서 제안하는 방법에 따르면, 사전에 라운드 키에 대한 GSW 암호문만이 계산되어 있다면 이후 암호문 계산 단계에서는 입력 상태값에 대한 GSW 암호문 계산만이 필요하게 되어, 여러 블록의 암호문을 계산하는 경우 라운드 키에 대한 GSW 암호문은 계속 반복하여 사용될 수 있으므로, 암호문 계산에 필요한 전체 시간이 크게 감소될 수 있는 효과가 있다. 특히, 본 개시에서 제안하는 방법에 따르면, 암호문 계산에 필요한 전체 시간의 감소 정도는 매 라운드마다 계산해야 하는 비선형 함수 개수에 비례할 수 있다.

[175] 도 17은 본 개시에서 제안하는 방법이 서버에서 수행되는 예시를 나타낸 도이다.

[176] 먼저, 상기 서버는, 클라이언트로부터, 데이터에 대해 수행되는 적어도 한번의 라운드에 기초하여 암호화된 암호화 데이터를 수신한다(S1710).

[177] 다음, 상기 적어도 한번의 라운드 각각에서, (i) 상기 적어도 한번의 라운드에서 공통적으로 사용되는 공통 입력 데이터 및 (ii) 상기 적어도 한번의 라운드 각각에서 개별적으로 사용되는 라운드 키가 상기 적어도 한번의 라운드 각각의 라운드 함수에 입력되어 출력된다.

[178] 이후, 상기 서버는, 상기 암호화 데이터에 포함된 상기 적어도 한번의 라운드 각각의 라운드 함수의 출력 값에 대해 동형 연산을 수행한다.

[179] 이 때, 상기 적어도 한번의 라운드 각각의 라운드 함수의 출력 값에 대한 상기 동형 연산은 상기 동형 연산에 대한 입력 값과 상기 입력 값에 대한 상기 동형 연산의 결과 값 간의 사전 설정된 맵핑 관계에 기초하여 수행되고, 상기 사전 설정된 맵핑 관계에 기초한 상기 동형 연산을 위해, 상기 적어도 한번의 라운드 각각에서 개별적으로 사용되는 라운드 키에 대한 제1 암호문이 상기 동형 연산의 수행 전에 미리 계산되고, 상기 동형 연산의 수행 시에 상기 공통 입력 데이터에 대한 제2 암호문이 계산된다.

[180] 이 때, 상기 사전 설정된 맵핑 관계에 대해 수행되는 (i) 상기 제1 암호문에 기초한 제1 블라인드 로테이션(blind rotation) 및 상기 제2 암호문에 기초한 제2 블라인드 로테이션에 기초하여, 상기 적어도 한번의 라운드 각각의 라운드 함수의 출력 값에 대한 상기 동형 연산의 결과 값이 계산된다.

- [181] 이 때, 도 17에 도시되지는 않지만, 상기 서버는 상기 S1710 단계 이전, S1710 단계 내지 S1720 단계 중간에, 또는 S1720 단계 이후, 적어도 하나의 동기 신호를 전송하고, 제어 정보를 전송할 수 있다.
- [182] 또한, 상기 서버는, 무선 신호를 전송하기 위한 전송기(transmitter); 무선 신호를 수신하기 위한 수신기(receiver); 적어도 하나의 프로세서; 및 상기 적어도 하나의 프로세서에 동작 가능하게 접속 가능하고, 상기 적어도 하나의 프로세서에 의해 실행될 때, 동작들을 수행하는 지시(instruction)들을 저장하는 적어도 하나의 컴퓨터 메모리를 포함한다. 이 때 상기 동작들은 상기 도 17에서 설명한 단계들을 포함한다.
- [183] 또한, 도 17에서 설명된 동작들은 하나 이상의 명령어들을 저장하는 비일시적 컴퓨터 판독 가능 매체(computer readable medium, CRM)에 저장될 수 있다. 상기 비일시적 컴퓨터 판독 가능 매체는 하나 이상의 프로세서들에 의해 실행 가능한 하나 이상의 명령어들을 저장하고, 상기 하나 이상의 명령어들은 상기 서버가 도 17에서 설명된 동작을 수행하도록 한다.
- [184] 또한, 하나 이상의 메모리들 및 상기 하나 이상의 메모리들과 기능적으로 연결되어 있는 하나 이상의 프로세서들을 포함하는 장치는, 상기 하나 이상의 프로세서들이 상기 장치가 도 17에서 설명된 동작들을 수행하도록 제어한다.
- [185] 도 18은 본 개시에서 제안하는 방법이 클라이언트에서 수행되는 예시를 나타낸 도이다.
- [186] 먼저, 상기 클라이언트는, 서버로, 데이터에 대해 수행되는 적어도 한번의 라운드에 기초하여 암호화된 암호화 데이터를 전송한다(S1810).
- [187] 여기서, 상기 적어도 한번의 라운드 각각에서, (i) 상기 적어도 한번의 라운드에서 공통적으로 사용되는 공통 입력 데이터 및 (ii) 상기 적어도 한번의 라운드 각각에서 개별적으로 사용되는 라운드 키가 상기 적어도 한번의 라운드 각각의 라운드 함수에 입력되어 출력된다.
- [188] 이후, 상기 클라이언트는, 상기 서버로부터, 상기 암호화 데이터에 포함된 상기 적어도 한번의 라운드 각각의 라운드 함수의 출력 값에 대한 동형 연산에 기초하여 획득된 상기 데이터의 동형 암호문을 수신한다(S1820).
- [189] 이 때, 상기 적어도 한번의 라운드 각각의 라운드 함수의 출력 값에 대한 상기 동형 연산은 상기 동형 연산에 대한 입력 값과 상기 입력 값에 대한 상기 동형 연산의 결과 값 간의 사전 설정된 맵핑 관계에 기초하여 수행되고, 상기 사전 설정된 맵핑 관계에 기초한 상기 동형 연산을 위해, 상기 적어도 한번의 라운드 각각에서 개별적으로 사용되는 라운드 키에 대한 제1 암호문이 상기 동형 연산의 수행 전에 미리 계산되고, 상기 동형 연산의 수행 시에 상기 공통 입력 데이터에 대한 제2 암호문이 계산된다.
- [190] 여기서, 상기 사전 설정된 맵핑 관계에 대해 수행되는 (i) 상기 제1 암호문에 기초한 제1 블라인드 로테이션(blind rotation) 및 상기 제2 암호문에 기초한 제2 블

라인드 로테이션에 기초하여, 상기 적어도 한번의 라운드 각각의 라운드 함수의 출력 값에 대한 상기 동형 연산의 결과 값이 계산된다.

- [191] 이 때, 도 18에 도시되지는 않지만, 상기 단말은 상기 S1810 단계 이전, S1810 단계 내지 S1820 단계 중간에, 또는 S1820 단계 이후, 적어도 하나의 동기 신호를 수신하고, 제어 정보를 수신할 수 있다.
- [192] 또한, 상기 클라이언트는, 무선 신호를 전송하기 위한 전송기(transmitter); 무선 신호를 수신하기 위한 수신기(receiver); 적어도 하나의 프로세서; 및 상기 적어도 하나의 프로세서에 동작 가능하게 접속 가능하고, 상기 적어도 하나의 프로세서에 의해 실행될 때, 동작들을 수행하는 지시(instruction)들을 저장하는 적어도 하나의 컴퓨터 메모리를 포함한다. 이 때 상기 동작들은 상기 도 18에서 설명한 단계들을 포함한다.
- [193] 또한, 도 18에서 설명된 동작들은 하나 이상의 명령어들을 저장하는 비일시적 컴퓨터 판독 가능 매체(computer readable medium, CRM)에 저장될 수 있다. 상기 비일시적 컴퓨터 판독 가능 매체는 하나 이상의 프로세서들에 의해 실행 가능한 하나 이상의 명령어들을 저장하고, 상기 하나 이상의 명령어들은 상기 단말이 도 18에서 설명된 동작을 수행하도록 한다.
- [194] 또한, 하나 이상의 메모리들 및 상기 하나 이상의 메모리들과 기능적으로 연결되어 있는 하나 이상의 프로세서들을 포함하는 장치는, 상기 하나 이상의 프로세서들이 상기 장치가 도 18에서 설명된 동작들을 수행하도록 제어한다.
- [195] 이상에서 설명된 실시 예들은 본 개시의 구성요소들과 특징들이 소정 형태로 결합된 것들이다. 각 구성요소 또는 특징은 별도의 명시적 언급이 없는 한 선택적인 것으로 고려되어야 한다. 각 구성요소 또는 특징은 다른 구성요소나 특징과 결합되지 않은 형태로 실시될 수 있다. 또한, 일부 구성요소들 및/또는 특징들을 결합하여 본 개시의 실시 예를 구성하는 것도 가능하다. 본 개시의 실시 예들에서 설명되는 동작들의 순서는 변경될 수 있다. 어느 실시예의 일부 구성이나 특징은 다른 실시 예에 포함될 수 있고, 또는 다른 실시예의 대응하는 구성 또는 특징과 교체될 수 있다. 특허청구범위에서 명시적인 인용 관계가 있지 않은 청구항들을 결합하여 실시 예를 구성하거나 출원 후의 보정에 의해 새로운 청구항으로 포함시킬 수 있음은 자명하다.
- [196] 본 개시에 따른 실시 예는 다양한 수단, 예를 들어, 하드웨어, 펌웨어(firmware), 소프트웨어 또는 그것들의 결합 등에 의해 구현될 수 있다. 하드웨어에 의한 구현의 경우, 본 개시의 일 실시 예는 하나 또는 그 이상의 ASICs(application specific integrated circuits), DSPs(digital signal processors), DSPDs(digital signal processing devices), PLDs(programmable logic devices), FPGAs(field programmable gate arrays), 프로세서, 콘트롤러, 마이크로 콘트롤러, 마이크로 프로세서 등에 의해 구현될 수 있다.
- [197] 펌웨어나 소프트웨어에 의한 구현의 경우, 본 개시의 일 실시 예는 이상에서 설명된 기능 또는 동작들을 수행하는 모듈, 절차, 함수 등의 형태로 구현될 수 있다.

소프트웨어 코드는 메모리에 저장되어 프로세서에 의해 구동될 수 있다. 상기 메모리는 상기 프로세서 내부 또는 외부에 위치하여, 이미 공지된 다양한 수단에 의해 상기 프로세서와 데이터를 주고 받을 수 있다.

- [198] 본 개시는 본 개시의 필수적 특징을 벗어나지 않는 범위에서 다른 특정한 형태로 구체화될 수 있음은 통상의 기술자에게 자명하다. 따라서, 상술한 상세한 설명은 모든 면에서 제한적으로 해석되어서는 아니 되고 예시적인 것으로 고려되어야 한다. 본 개시의 범위는 첨부된 청구항의 합리적 해석에 의해 결정되어야 하고, 본 개시의 등가적 범위 내에서의 모든 변경은 본 개시의 범위에 포함된다.
- [199] 추가적으로 또는 대체적으로(additionally or alternatively), 본 개시의 장치(100, 200)에서 구현되는 무선 통신 기술은 LTE-M 기술을 기반으로 통신을 수행할 수 있다. 예를 들어, LTE-M 기술은 LPWAN 기술의 일례일 수 있고, eMTC(enhanced Machine Type Communication) 등의 다양한 명칭으로 불릴 수 있다. 예를 들어, LTE-M 기술은 1) LTE CAT 0, 2) LTE Cat M1, 3) LTE Cat M2, 4) LTE non-BL(non-Bandwidth Limited), 5) LTE-MTC, 6) LTE Machine Type Communication, 및/또는 7) LTE M 등의 다양한 규격 중 적어도 어느 하나로 구현될 수 있으며 상술한 명칭에 한정되는 것은 아니다.
- [200] 추가적으로 또는 대체적으로, 본 개시의 장치(100, 200)에서 구현되는 무선 통신 기술은 저전력 통신을 고려한 지그비(ZigBee), 블루투스(Bluetooth) 및 저전력 광역 통신망(Low Power Wide Area Network, LPWAN) 중 적어도 어느 하나를 포함할 수 있으며, 상술한 명칭에 한정되는 것은 아니다. 예를 들어, ZigBee 기술은 IEEE 802.15.4 등의 다양한 규격을 기반으로 소형/저-파워 디지털 통신에 관련된 PAN(personal area networks)을 생성할 수 있으며, 다양한 명칭으로 불릴 수 있다.
- 산업상 이용가능성**
- [201] 본 개시는 3GPP LTE/LTE-A, 5G/6G 시스템에 적용되는 예를 중심으로 설명하였으나, 3GPP LTE/LTE-A, 5G/6G 시스템 이외에도 다양한 무선 통신 시스템에 적용하는 것이 가능하다.

청구범위

- [청구항 1] 통신 시스템에서 서버에 의해 수행되는 방법에 있어서,
클라이언트로, 적어도 하나의 동기 신호를 전송하는 단계;
상기 클라이언트로, 제어 정보를 전송하는 단계;
상기 클라이언트로부터, 데이터에 대해 수행되는 적어도 한번의 라운드에 기초하여 암호화된 암호화 데이터를 수신하는 단계,
상기 적어도 한번의 라운드 각각에서, (i) 상기 적어도 한번의 라운드에서 공통적으로 사용되는 공통 입력 데이터 및 (ii) 상기 적어도 한번의 라운드 각각에서 개별적으로 사용되는 라운드 키가 상기 적어도 한번의 라운드 각각의 라운드 함수에 입력되어 출력되고; 및
상기 암호화 데이터에 포함된 상기 적어도 한번의 라운드 각각의 라운드 함수의 출력 값에 대해 동형 연산을 수행하는 단계를 포함하되,
상기 적어도 한번의 라운드 각각의 라운드 함수의 출력 값에 대한 상기 동형 연산은 상기 동형 연산에 대한 입력 값과 상기 입력 값에 대한 상기 동형 연산의 결과 값 간의 사전 설정된 맵핑 관계에 기초하여 수행되고,
상기 사전 설정된 맵핑 관계에 기초한 상기 동형 연산을 위해, 상기 적어도 한번의 라운드 각각에서 개별적으로 사용되는 라운드 키에 대한 제1 암호문이 상기 동형 연산의 수행 전에 미리 계산되고, 상기 동형 연산의 수행 시에 상기 공통 입력 데이터에 대한 제2 암호문이 계산되고,
상기 사전 설정된 맵핑 관계에 대해 수행되는 (i) 상기 제1 암호문에 기초한 제1 블라인드 로테이션(blind rotation) 및 상기 제2 암호문에 기초한 제2 블라인드 로테이션에 기초하여, 상기 적어도 한번의 라운드 각각의 라운드 함수의 출력 값에 대한 상기 동형 연산의 결과 값이 계산되는 방법.
- [청구항 2] 제1 항에 있어서,
상기 적어도 한번의 라운드 각각에서, 상기 적어도 한번의 라운드 각각의 라운드 함수의 출력 값에 상기 적어도 한번의 라운드 각각에서 개별적으로 사용되는 개별 입력 값이 더해져서 출력되는 방법.
- [청구항 3] 제1 항에 있어서,
상기 제1 블라인드 로테이션 및 상기 제2 블라인드 로테이션은, 상기 동형 연산의 입력 값이 암호화된 값인 경우, 상기 암호화된 값인 상기 동형 연산의 입력 값에 대한 복호화 없이, 상기 암호화된 값인 상기 동형 연산의 입력 값만큼 회전된 상기 사전 설정된 맵핑 관계에 기초하여, 상기 암호화된 값인 상기 동형 연산의 입력 값에 대응되는 암호화된 결과 값이 획득되도록 하는 연산인 방법.
- [청구항 4] 제1 항에 있어서,

상기 적어도 한번의 라운드 각각에서 개별적으로 사용되는 라운드 키 각각은 라운드 키 업데이트 이전까지 상기 적어도 한번의 라운드 각각에서 동일한 방법.

[청구항 5] 제1 항에 있어서.

상기 공통 입력 데이터의 크기는 상기 데이터의 크기의 절반이 아닌 방법.

[청구항 6] 제1 항에 있어서.

상기 클라이언트로부터, 상기 적어도 한번의 라운드에 기초한 암호화와 관련된, 동형 암호화된 비밀키를 수신하는 단계;

상기 동형 암호화된 비밀키 및 상기 암호화 데이터에 대한 상기 동형 연산의 결과에 기초하여 상기 데이터의 동형 암호문을 획득하는 단계; 및
상기 클라이언트로, 상기 데이터의 동형 암호문을 전송하는 단계를 더 포함하는 방법.

[청구항 7] 제1 항에 있어서.

상기 적어도 한번의 라운드 각각의 라운드 함수는 상기 적어도 한번의 라운드마다 랜덤하게 생성되는 방법.

[청구항 8] 통신 시스템에서 클라이언트에 의해 수행되는 방법에 있어서,

서버로부터, 적어도 하나의 동기 신호를 수신하는 단계;

상기 서버로부터, 제어 정보를 수신하는 단계;

상기 서버로, 데이터에 대해 수행되는 적어도 한번의 라운드에 기초하여 암호화된 암호화 데이터를 전송하는 단계,

상기 적어도 한번의 라운드 각각에서, (i) 상기 적어도 한번의 라운드에서 공통적으로 사용되는 공통 입력 데이터 및 (ii) 상기 적어도 한번의 라운드 각각에서 개별적으로 사용되는 라운드 키가 상기 적어도 한번의 라운드 각각의 라운드 함수에 입력되어 출력되고; 및

상기 서버로부터, 상기 암호화 데이터에 포함된 상기 적어도 한번의 라운드 각각의 라운드 함수의 출력 값에 대한 동형 연산에 기초하여 획득된 상기 데이터의 동형 암호문을 수신하는 단계를 포함하되,

상기 적어도 한번의 라운드 각각의 라운드 함수의 출력 값에 대한 상기 동형 연산은 상기 동형 연산에 대한 입력 값과 상기 입력 값에 대한 상기 동형 연산의 결과 값 간의 사전 설정된 맵핑 관계에 기초하여 수행되고,

상기 사전 설정된 맵핑 관계에 기초한 상기 동형 연산을 위해, 상기 적어도 한번의 라운드 각각에서 개별적으로 사용되는 라운드 키에 대한 제1 암호문이 상기 동형 연산의 수행 전에 미리 계산되고, 상기 동형 연산의 수행 시에 상기 공통 입력 데이터에 대한 제2 암호문이 계산되고,

상기 사전 설정된 맵핑 관계에 대해 수행되는 (i) 상기 제1 암호문에 기초한 제1 블라인드 로테이션(blind rotation) 및 상기 제2 암호문에 기초한 제2 블라인드 로테이션에 기초하여, 상기 적어도 한번의 라운드 각각의 라운드 함수의 출력 값에 대한 상기 동형 연산의 결과 값이 계산되는 방법.

- [청구항 9] 제8 항에 있어서,
상기 적어도 한번의 라운드 각각에서, 상기 적어도 한번의 라운드 각각의 라운드 함수의 출력 값에 상기 적어도 한번의 라운드 각각에서 개별적으로 사용되는 개별 입력 값이 더해져서 출력되는 방법.
- [청구항 10] 제8 항에 있어서,
상기 제1 블라인드 로테이션 및 상기 제2 블라인드 로테이션은, 상기 동형 연산의 입력 값이 암호화된 값인 경우, 상기 암호화된 값인 상기 동형 연산의 입력 값에 대한 복호화 없이, 상기 암호화된 값인 상기 동형 연산의 입력 값만큼 회전된 상기 사전 설정된 맵핑 관계에 기초하여, 상기 암호화된 값인 상기 동형 연산의 입력 값에 대응되는 암호화된 결과 값이 획득되도록 하는 연산인 방법.
- [청구항 11] 제8 항에 있어서,
상기 적어도 한번의 라운드 각각에서 개별적으로 사용되는 라운드 키 각각은 라운드 키 업데이트 이전까지 상기 적어도 한번의 라운드 각각에서 동일한 방법.
- [청구항 12] 제8 항에 있어서.
상기 공통 입력 데이터의 크기는 상기 데이터의 크기의 절반이 아닌 방법.
- [청구항 13] 제8 항에 있어서.
상기 서버로, 상기 적어도 한번의 라운드에 기초한 암호화와 관련된, 동형 암호화된 비밀키를 전송하는 단계; 및
상기 서버로부터, 상기 동형 암호화된 비밀키 및 상기 암호화 데이터에 대한 상기 동형 연산의 결과에 기초하여 획득된 상기 동형 암호문을 수신하는 단계를 더 포함하는 방법.
- [청구항 14] 제8 항에 있어서.
상기 적어도 한번의 라운드 각각의 라운드 함수는 상기 적어도 한번의 라운드마다 랜덤하게 생성되는 방법.
- [청구항 15] 통신 시스템에서 통신을 수행하는 서버에 있어서,
무선 신호를 전송하기 위한 송신기(transmitter);
무선 신호를 수신하기 위한 수신기(receiver);
적어도 하나의 프로세서; 및
상기 적어도 하나의 프로세서에 동작 가능하게 접속 가능하고, 상기 적어도 하나의 프로세서에 의해 실행될 때, 동작들을 수행하는 지시(instruction)들을 저장하는 적어도 하나의 컴퓨터 메모리를 포함하며,
상기 동작들은,
클라이언트로, 적어도 하나의 동기 신호를 전송하는 단계;
상기 클라이언트로, 제어 정보를 전송하는 단계;
상기 클라이언트로부터, 데이터에 대해 수행되는 적어도 한번의 라운드에 기초하여 암호화된 암호화 데이터를 수신하는 단계,

상기 적어도 한번의 라운드 각각에서, (i) 상기 적어도 한번의 라운드에서 공통적으로 사용되는 공통 입력 데이터 및 (ii) 상기 적어도 한번의 라운드 각각에서 개별적으로 사용되는 라운드 키가 상기 적어도 한번의 라운드 각각의 라운드 함수에 입력되어 출력되고; 및

상기 암호화 데이터에 포함된 상기 적어도 한번의 라운드 각각의 라운드 함수의 출력 값에 대해 동형 연산을 수행하는 단계를 포함하되,

상기 적어도 한번의 라운드 각각의 라운드 함수의 출력 값에 대한 상기 동형 연산은 상기 동형 연산에 대한 입력 값과 상기 입력 값에 대한 상기 동형 연산의 결과 값 간의 사전 설정된 맵핑 관계에 기초하여 수행되고,

상기 사전 설정된 맵핑 관계에 기초한 상기 동형 연산을 위해, 상기 적어도 한번의 라운드 각각에서 개별적으로 사용되는 라운드 키에 대한 제1 암호문이 상기 동형 연산의 수행 전에 미리 계산되고, 상기 동형 연산의 수행 시에 상기 공통 입력 데이터에 대한 제2 암호문이 계산되고,

상기 사전 설정된 맵핑 관계에 대해 수행되는 (i) 상기 제1 암호문에 기초한 제1 블라인드 로테이션(blind rotation) 및 상기 제2 암호문에 기초한 제2 블라인드 로테이션에 기초하여, 상기 적어도 한번의 라운드 각각의 라운드 함수의 출력 값에 대한 상기 동형 연산의 결과 값이 계산되는 서버.

[청구항 16] 통신 시스템에서 통신을 수행하는 클라이언트에 있어서,

무선 신호를 전송하기 위한 전송기(transmitter);

무선 신호를 수신하기 위한 수신기(receiver);

적어도 하나의 프로세서; 및

상기 적어도 하나의 프로세서에 동작 가능하게 접속 가능하고, 상기 적어도 하나의 프로세서에 의해 실행될 때, 동작들을 수행하는 지시(instruction)들을 저장하는 적어도 하나의 컴퓨터 메모리를 포함하며,

상기 동작들은,

서버로부터, 적어도 하나의 동기 신호를 수신하는 단계;

상기 서버로부터, 제어 정보를 수신하는 단계;

상기 서버로, 데이터에 대해 수행되는 적어도 한번의 라운드에 기초하여 암호화된 암호화 데이터를 전송하는 단계,

상기 적어도 한번의 라운드 각각에서, (i) 상기 적어도 한번의 라운드에서 공통적으로 사용되는 공통 입력 데이터 및 (ii) 상기 적어도 한번의 라운드 각각에서 개별적으로 사용되는 라운드 키가 상기 적어도 한번의 라운드 각각의 라운드 함수에 입력되어 출력되고; 및

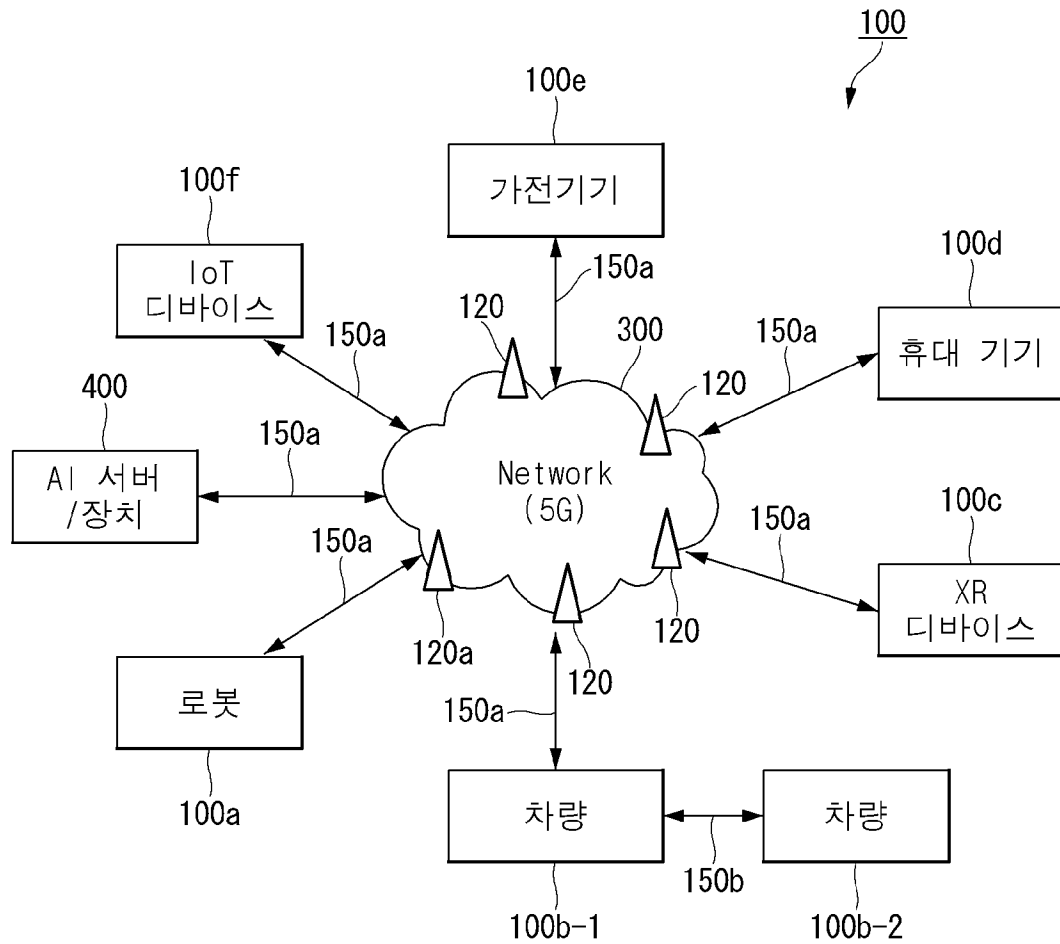
상기 서버로부터, 상기 암호화 데이터에 포함된 상기 적어도 한번의 라운드 각각의 라운드 함수의 출력 값에 대한 동형 연산에 기초하여 획득된 상기 데이터의 동형 암호문을 수신하는 단계를 포함하되,

상기 적어도 한번의 라운드 각각의 라운드 함수의 출력 값에 대한 상기 동형 연산은 상기 동형 연산에 대한 입력 값과 상기 입력 값에 대한 상기 동형 연산의 결과 값 간의 사전 설정된 맵핑 관계에 기초하여 수행되고, 상기 사전 설정된 맵핑 관계에 기초한 상기 동형 연산을 위해, 상기 적어도 한번의 라운드 각각에서 개별적으로 사용되는 라운드 키에 대한 제1 암호문이 상기 동형 연산의 수행 전에 미리 계산되고, 상기 동형 연산의 수행 시에 상기 공통 입력 데이터에 대한 제2 암호문이 계산되고, 상기 사전 설정된 맵핑 관계에 대해 수행되는 (i) 상기 제1 암호문에 기초한 제1 블라인드 로테이션(blind rotation) 및 상기 제2 암호문에 기초한 제2 블라인드 로테이션에 기초하여, 상기 적어도 한번의 라운드 각각의 라운드 함수의 출력 값에 대한 상기 동형 연산의 결과 값이 계산되는 클라이언트.

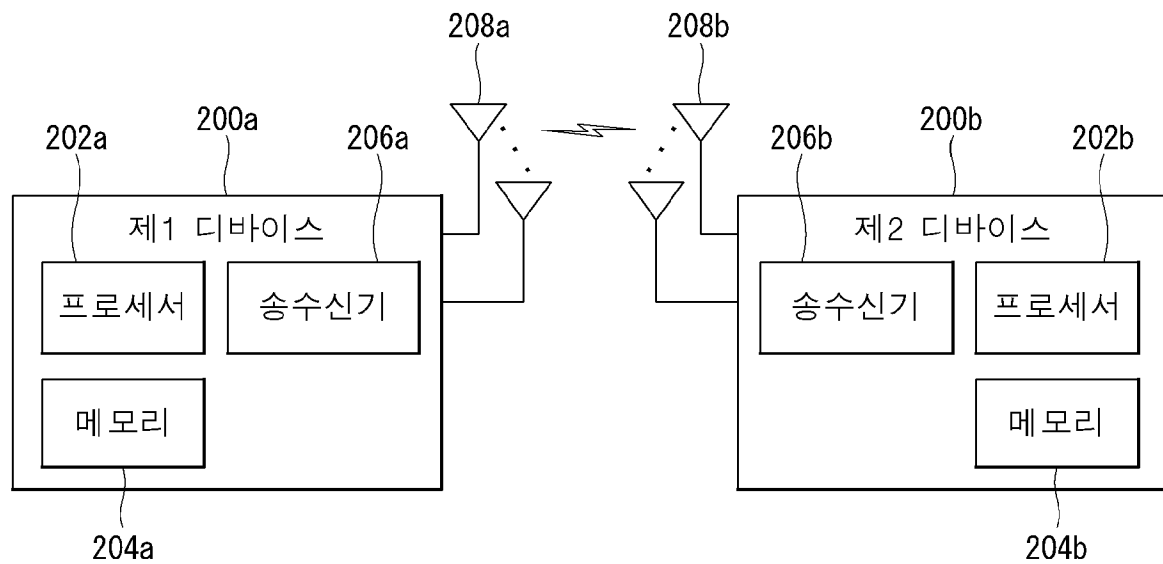
- [청구항 17] 하나 이상의 명령어들을 저장하는 비일시적 컴퓨터 판독 가능 매체 (computer readable medium, CRM)에 있어서,
 하나 이상의 프로세서들에 의해 실행 가능한 하나 이상의 명령어들은 송신단 수행하는 동작들을 포함하되,
 상기 동작들은,
 제1 항 내지 제7 항 중 어느 한 항에 따른 방법의 모든 단계를 포함하는 비일시적 컴퓨터 판독 가능 매체.
- [청구항 18] 하나 이상의 명령어들을 저장하는 비일시적 컴퓨터 판독 가능 매체 (computer readable medium, CRM)에 있어서,
 하나 이상의 프로세서들에 의해 실행 가능한 하나 이상의 명령어들은 송신단 수행하는 동작들을 포함하되,
 상기 동작들은,
 제8 항 내지 제14 항 중 어느 한 항에 따른 방법의 모든 단계를 포함하는 비일시적 컴퓨터 판독 가능 매체.
- [청구항 19] 하나 이상의 메모리들 및 상기 하나 이상의 메모리들과 기능적으로 연결되어 있는 하나 이상의 프로세서들을 포함하는 장치에 있어서,
 상기 하나 이상의 프로세서들은 상기 장치가 수행하는 동작들을 실행시키되,
 상기 동작들은,
 제1 항 내지 제7 항 중 어느 한 항에 따른 방법의 모든 단계를 포함하는 하는 장치.
- [청구항 20] 하나 이상의 메모리들 및 상기 하나 이상의 메모리들과 기능적으로 연결되어 있는 하나 이상의 프로세서들을 포함하는 장치에 있어서,
 상기 하나 이상의 프로세서들은 상기 장치가 수행하는 동작들을 실행시키되,
 상기 동작들은,

제8 항 내지 제14 항 중 어느 한 항에 따른 방법의 모든 단계를 포함하는
치.

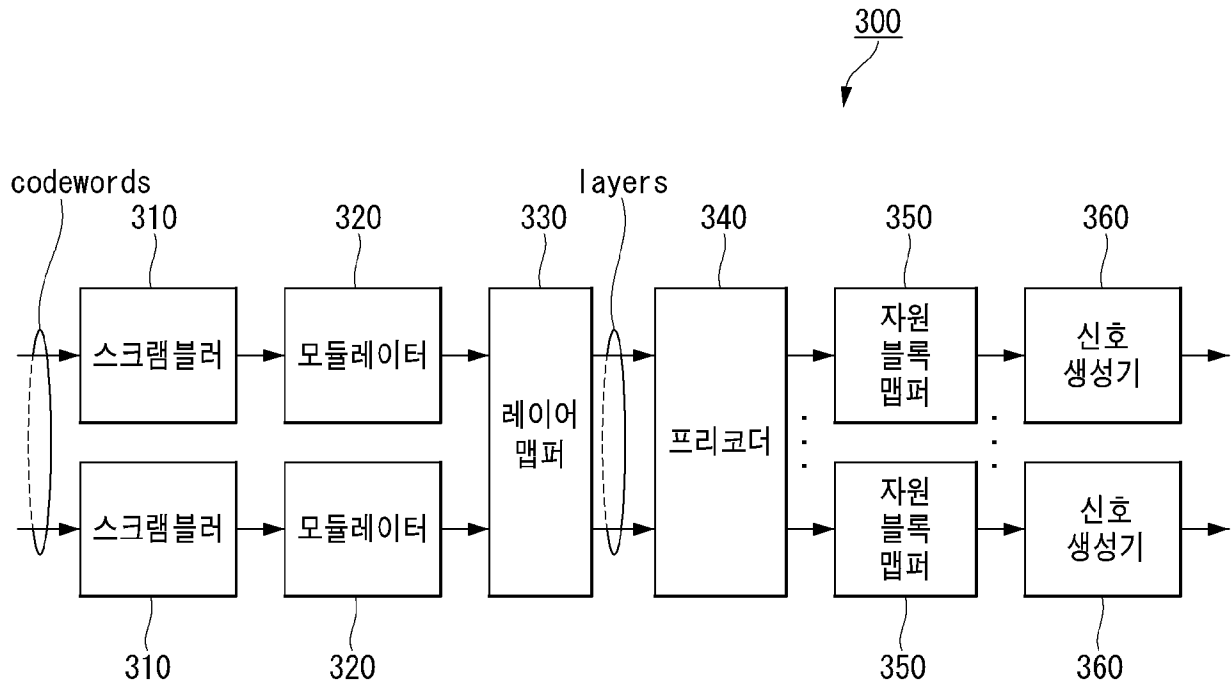
[도1]



[도2]

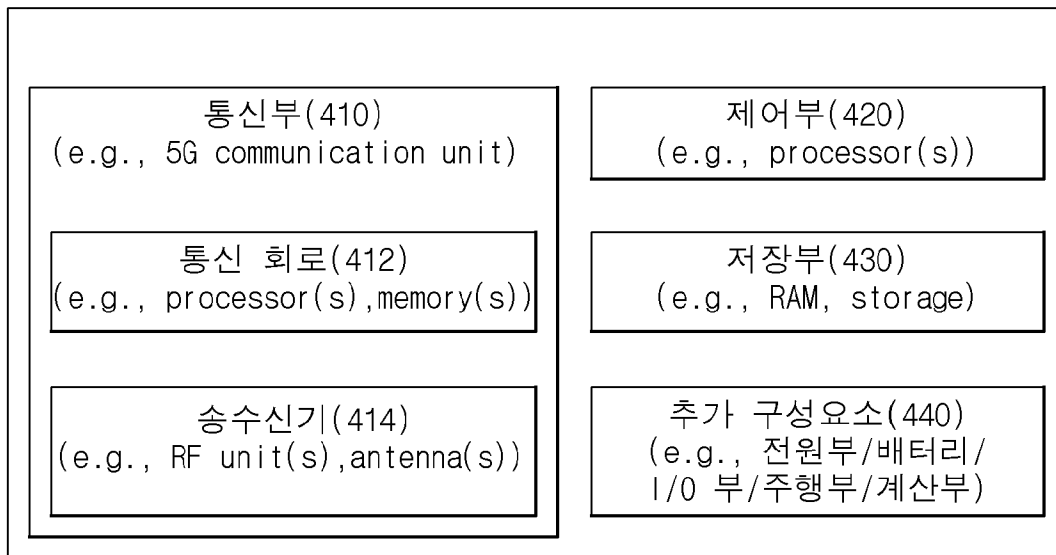


[도3]

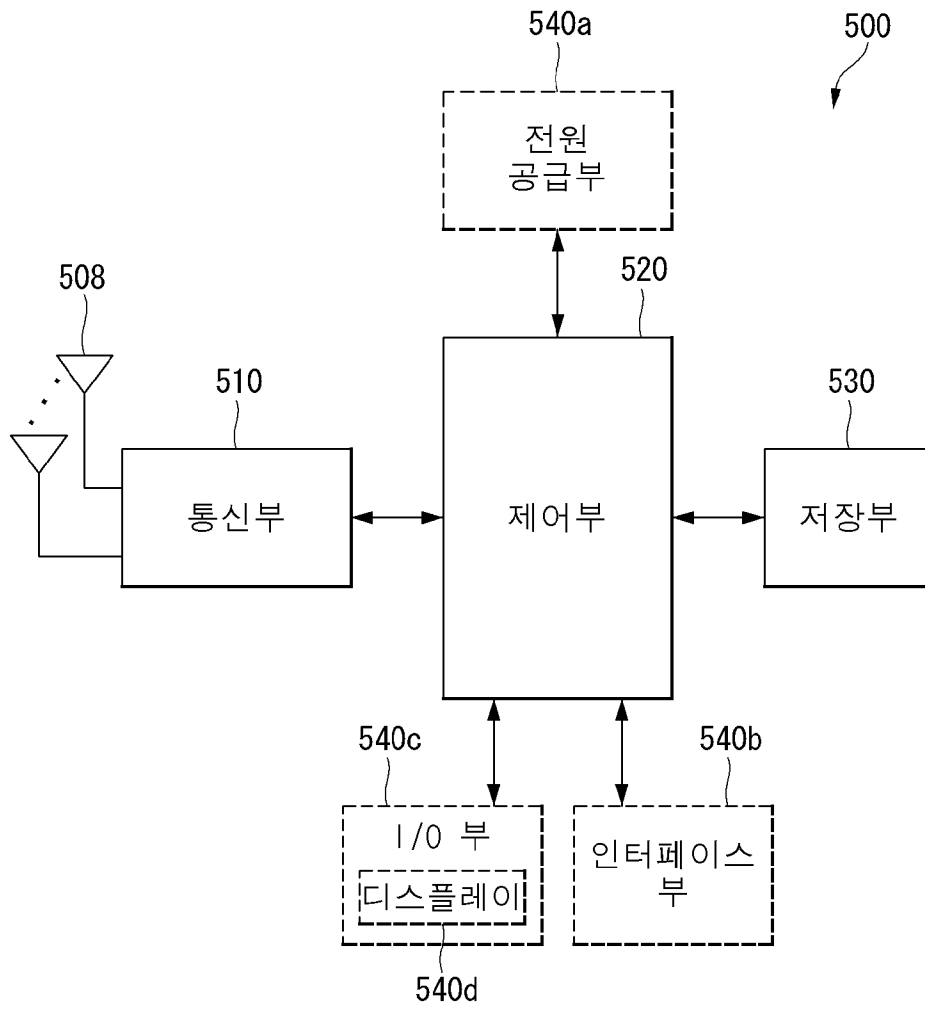


[도4]

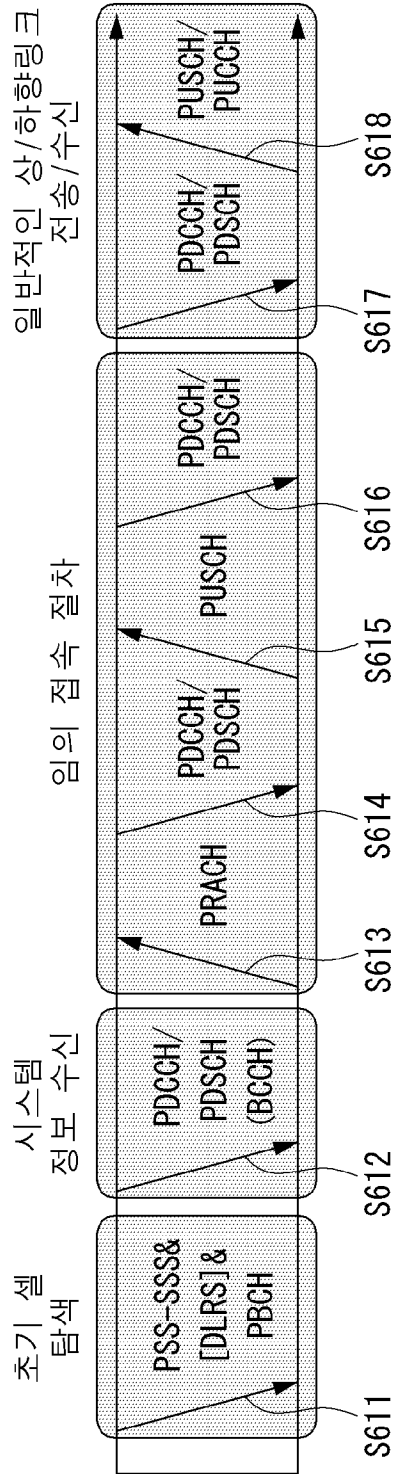
Device(400)



[도5]

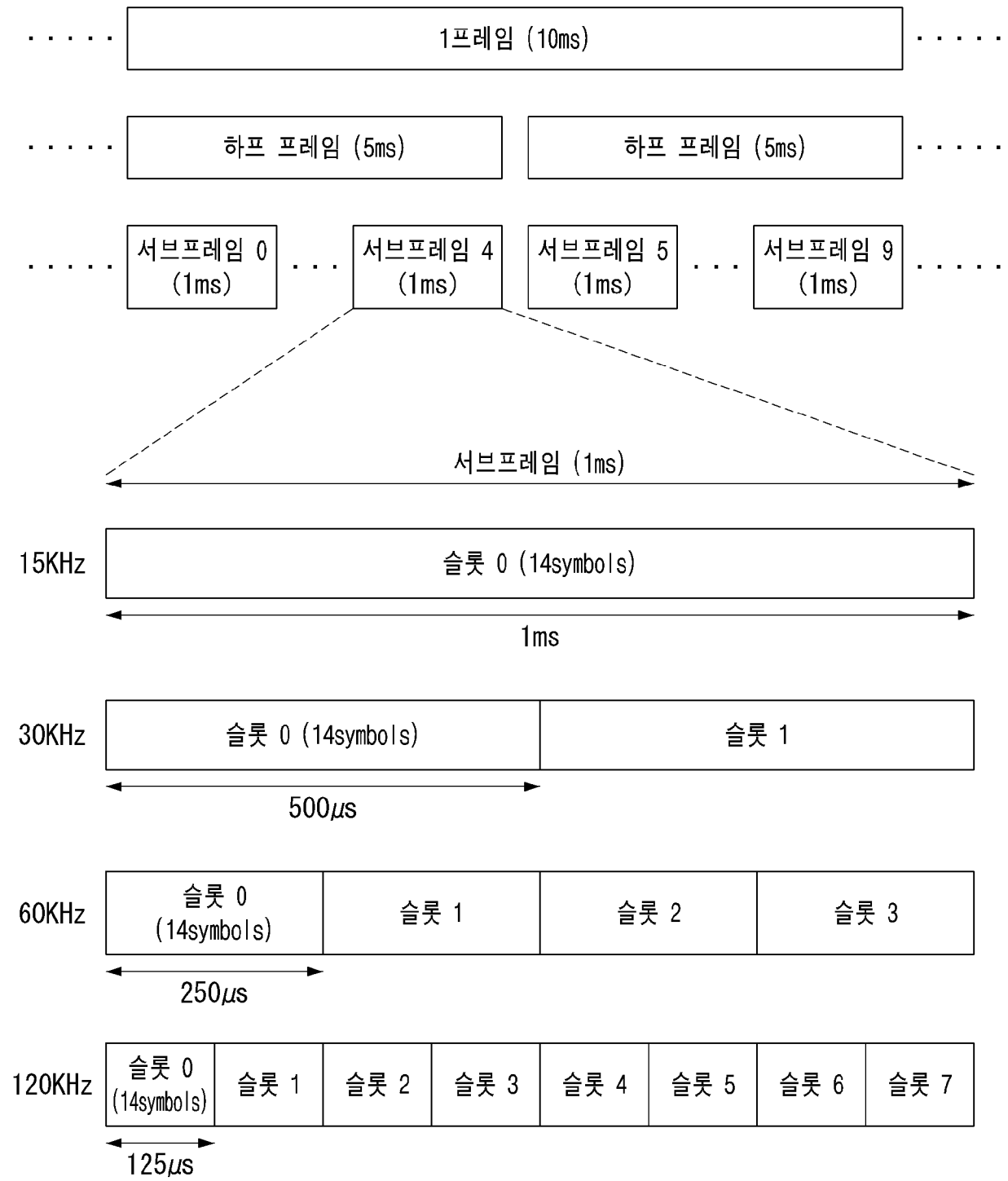


[도6]

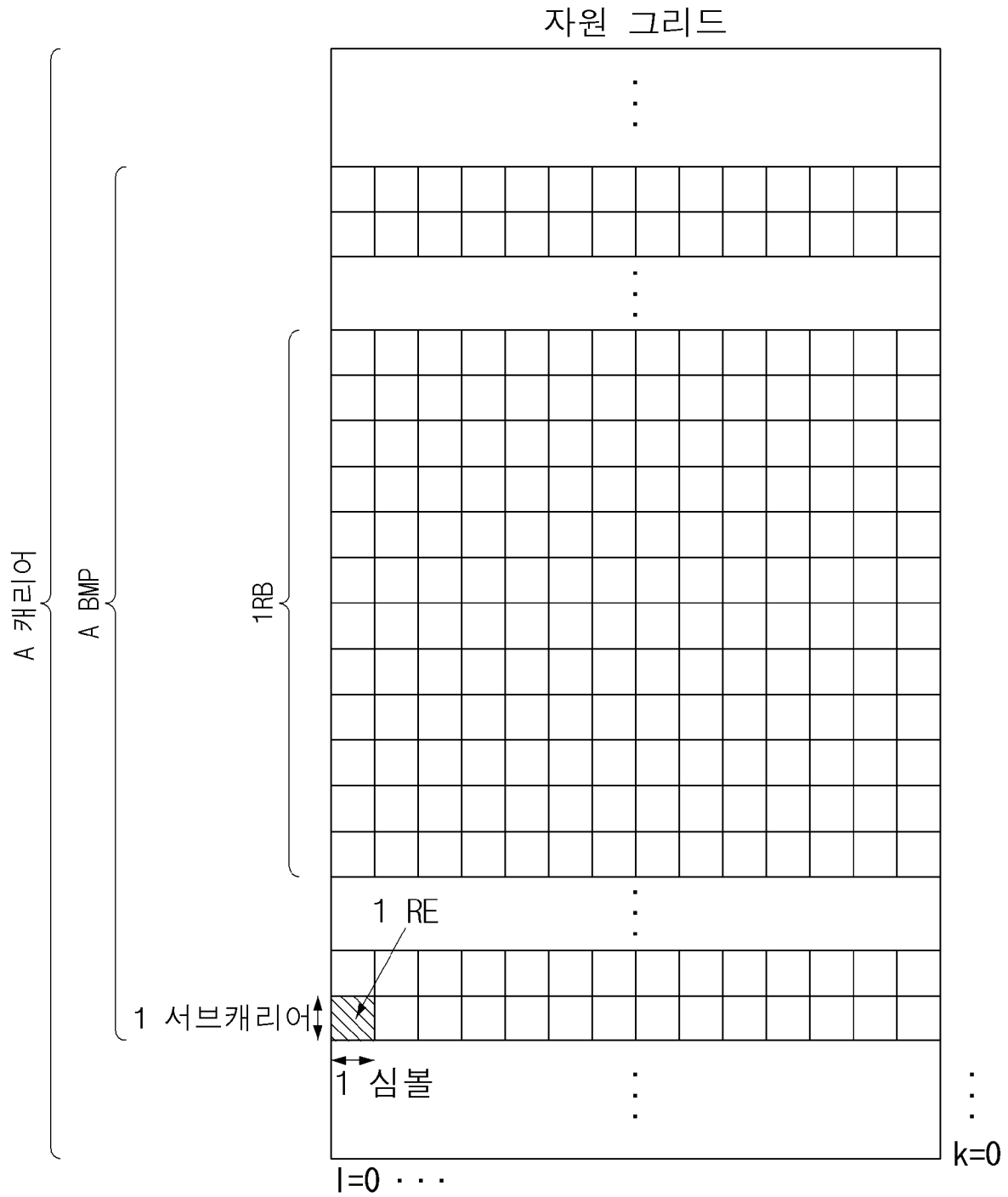


- DL/UL ACK/NACK
- PUSCH 및 PUCCH를 사용하는 단말의 CQI/PMI RI 보고

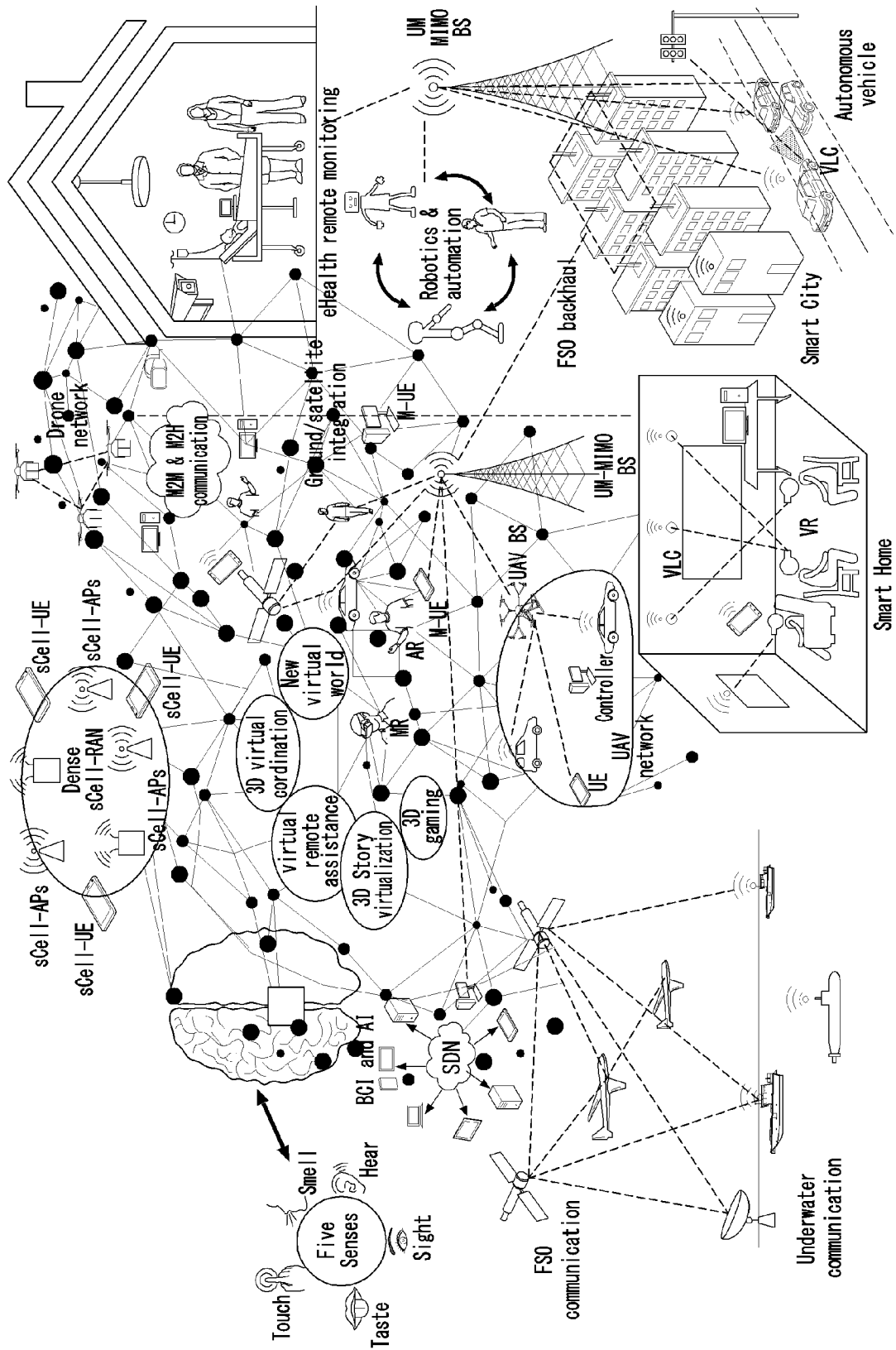
[도7]



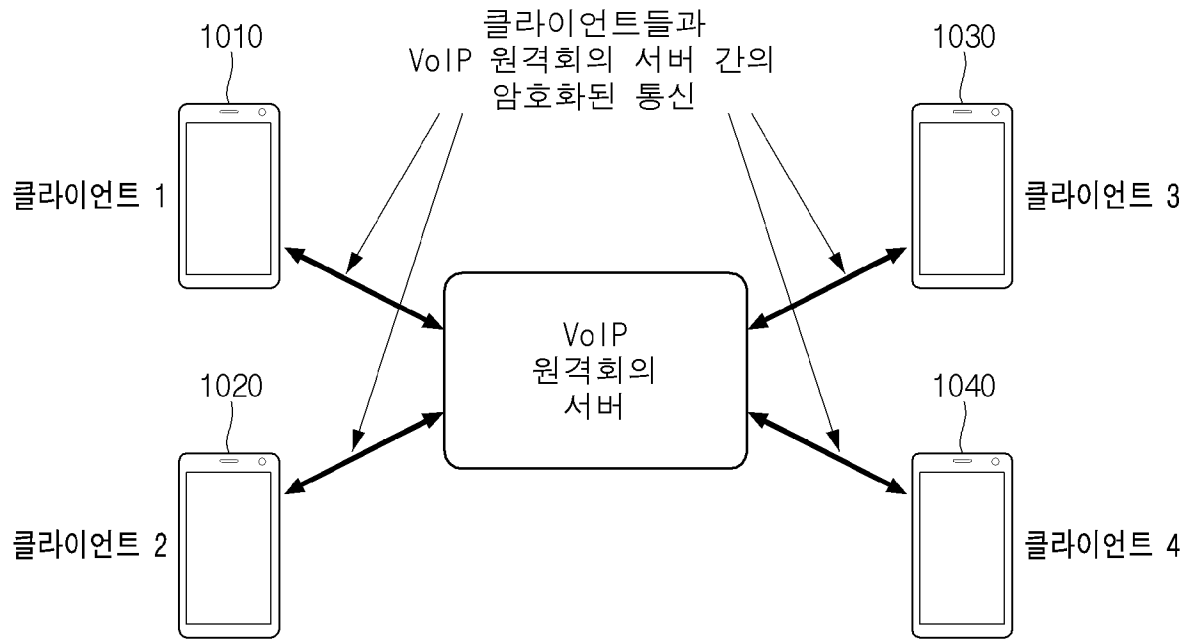
[도8]



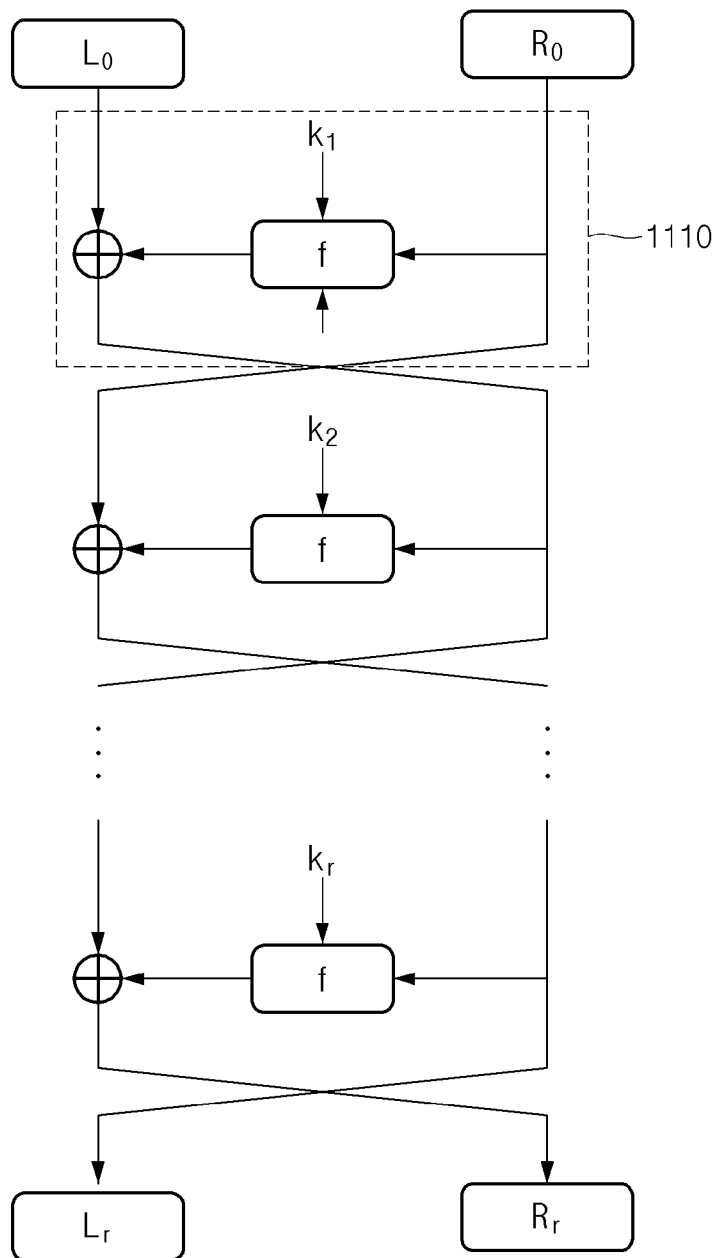
[도9]



[도10]

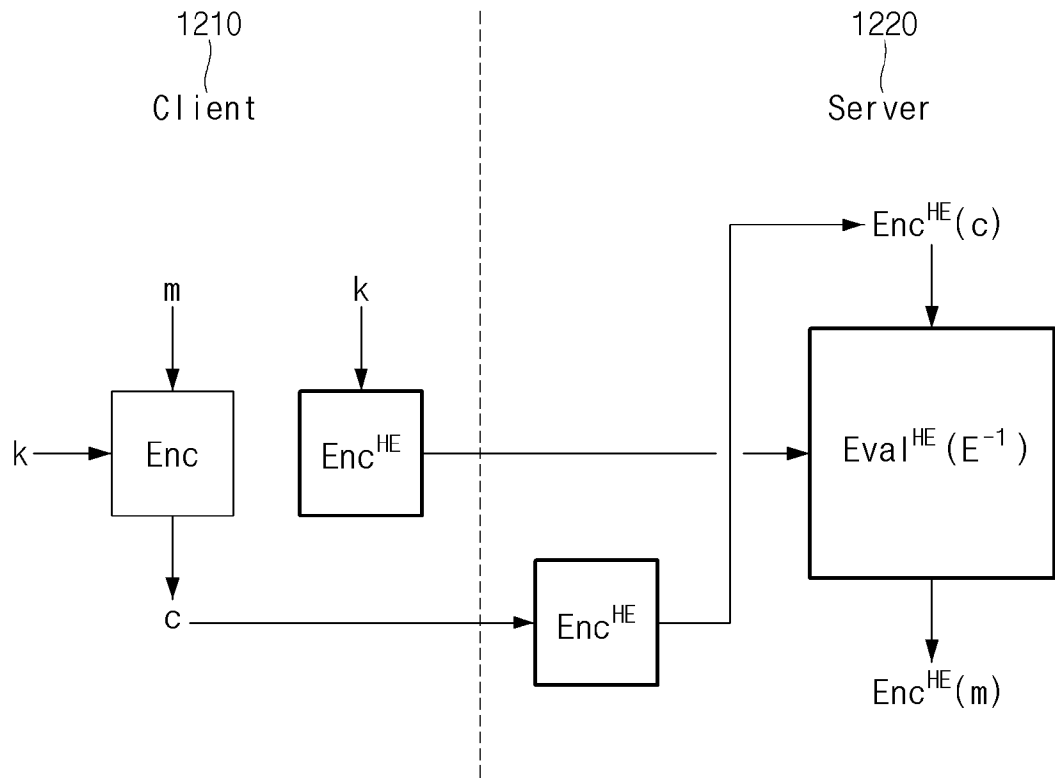


[51]

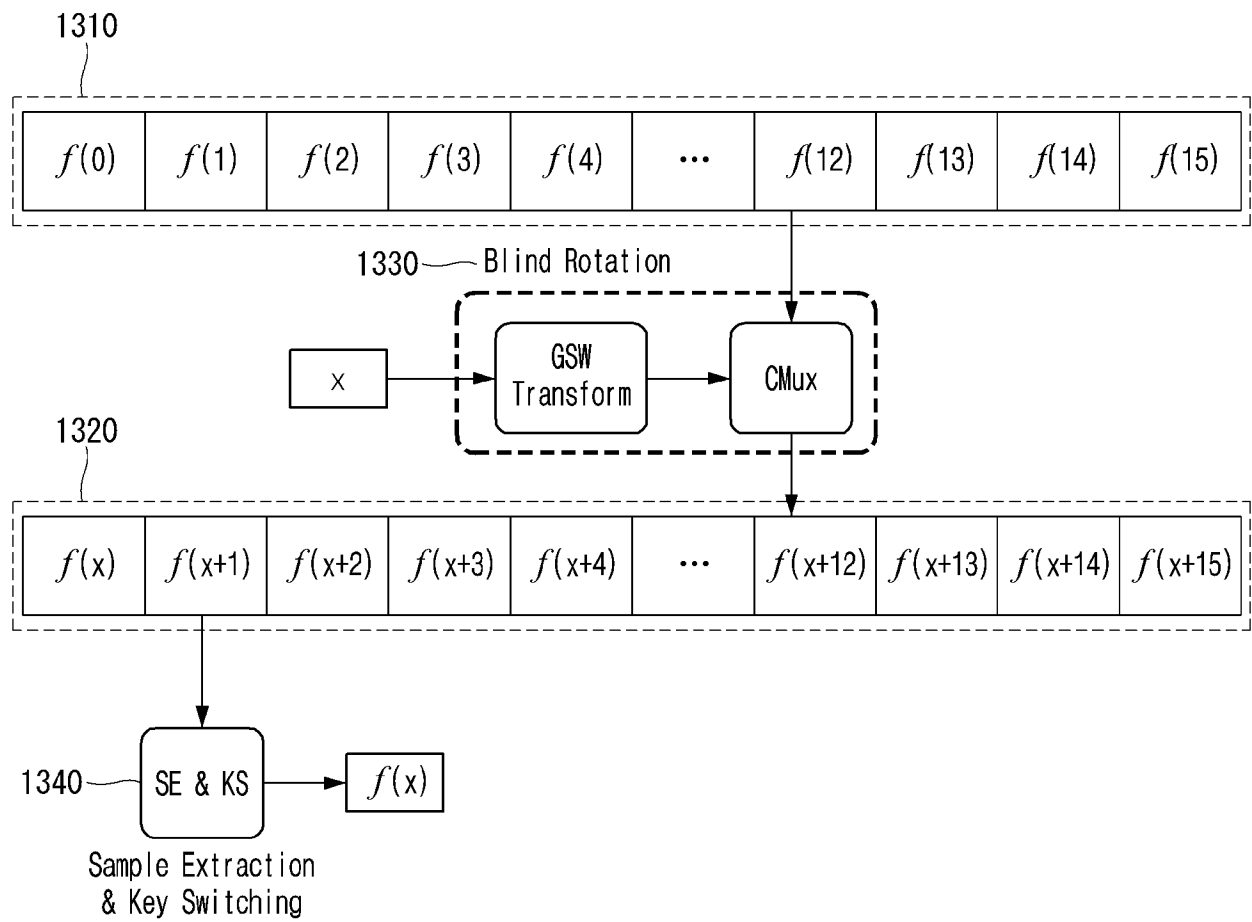

$$L_r$$

R_r

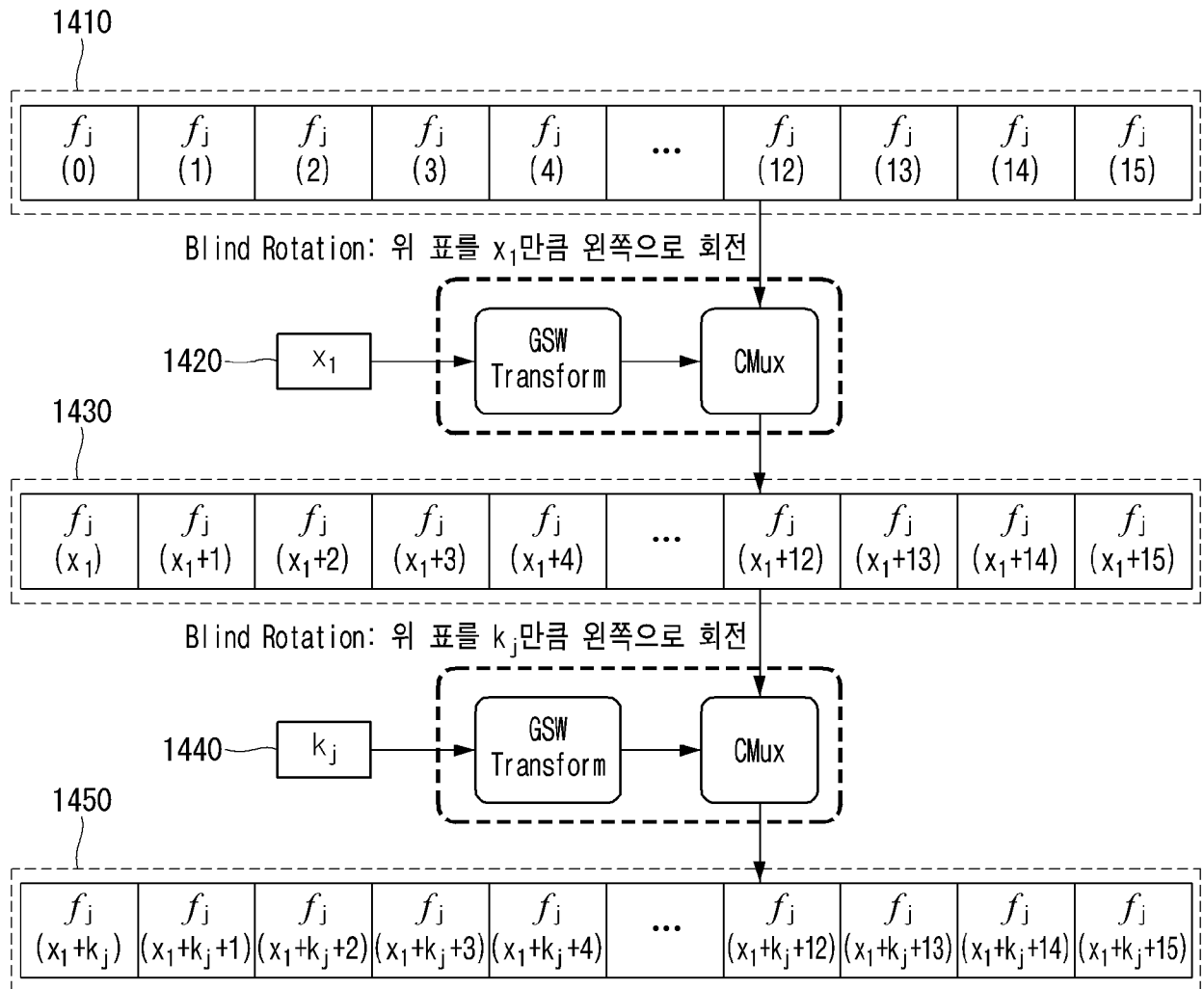
[도12]



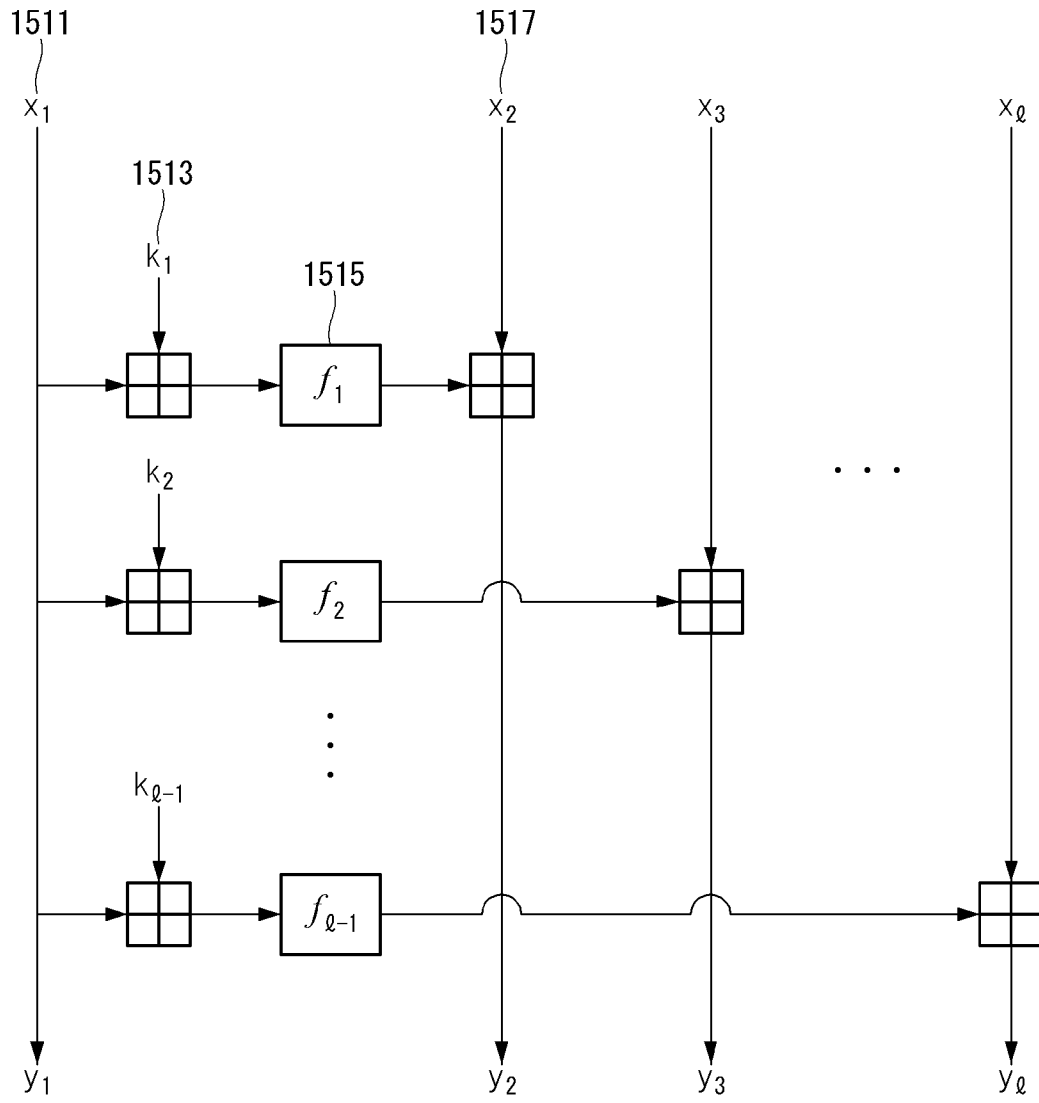
[도13]



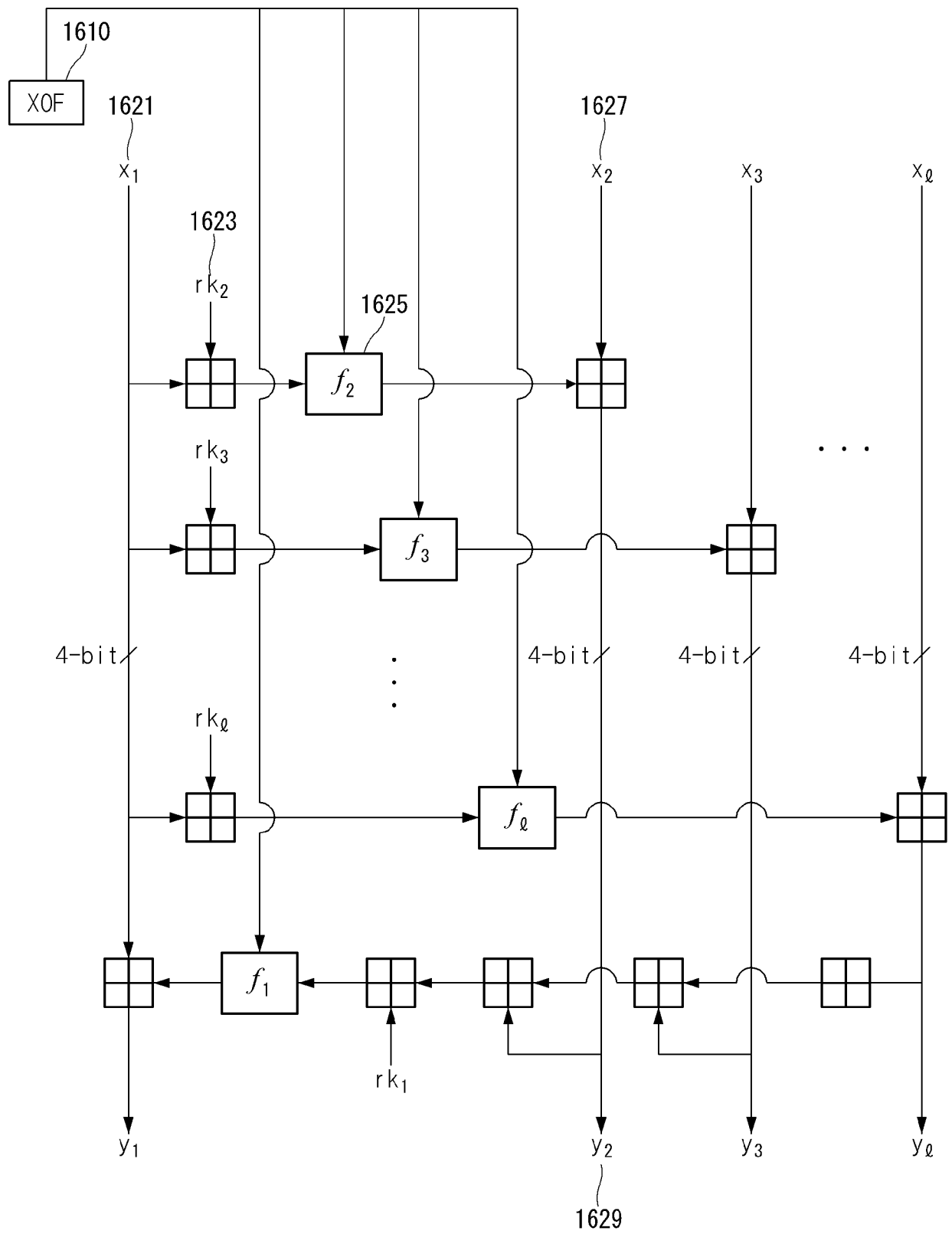
[도 14]



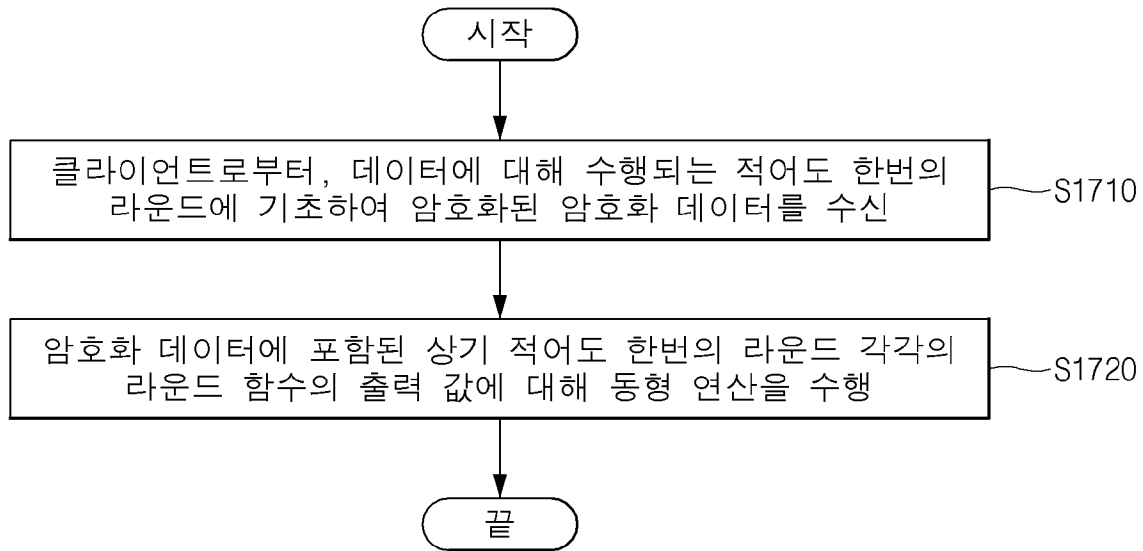
[도 15]



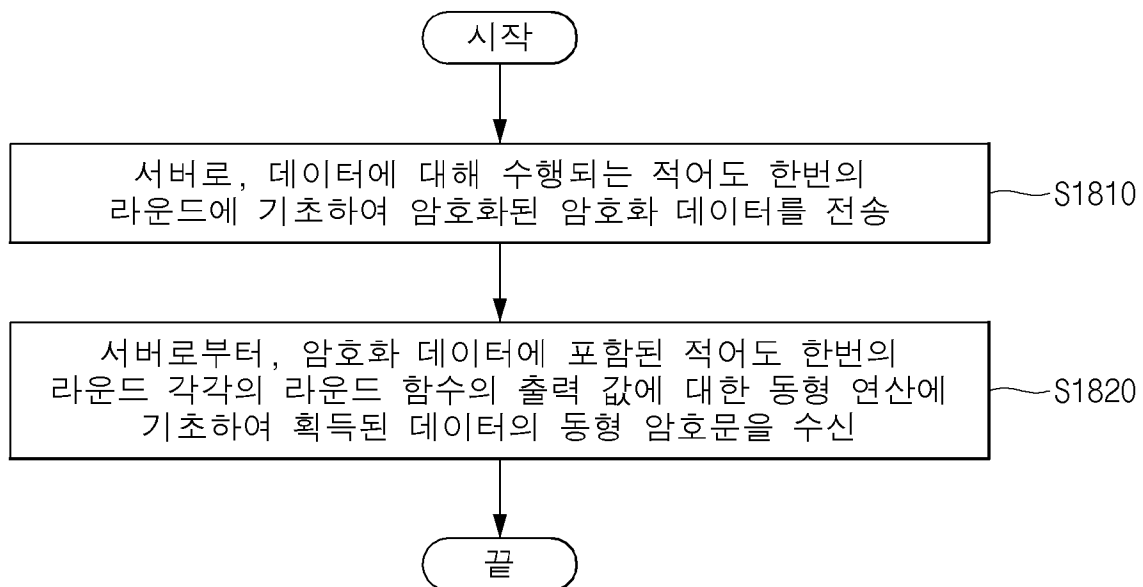
[도 16]



[도17]



[도18]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2023/008079

A. CLASSIFICATION OF SUBJECT MATTER H04L 9/00(2006.01)i According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) H04L 9/00(2006.01) Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Korean utility models and applications for utility models: IPC as above Japanese utility models and applications for utility models: IPC as above Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) eKOMPASS (KIPO internal) & keywords: 동형암호(homomorphic encryption), 라운드 키(round key), 라운드 함수(round function), 이중 블라인드 로테이션(double blind rotation)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	HA, Jincheol et al. Rubato: Noisy Ciphers for Approximate Homomorphic Encryption (Full Version). A major revision of an IACR publication in EUROCRYPT 2022. 10 May 2022. [Retrieved on 20 February 2024]. Retrieved from <URL: https://eprint.iacr.org/archive/2022/537/20220510:080623 >. See sections 2.4-3.1; and figures 1-2 and 5.	1-20
A	KR 10-2023-0078510 A (SAMSUNG ELECTRONICS CO., LTD.) 02 June 2023 (2023-06-02) See paragraphs [0101]-[0105]; and figure 2.	1-20
A	DOBRAUNIG, Christoph et al. Pasta: A Case for Hybrid Homomorphic Encryption. Preprint. MINOR revision, 03 June 2021. [Retrieved on 20 February 2024]. Retrieved from <URL: https://eprint.iacr.org/archive/2021/731/20210603:135802 >. See sections 1.1-6.2.	1-20
A	KIM, Andrey et al. LFHE: Fully Homomorphic Encryption with Bootstrapping Key Size Less than a Megabyte. Preprint. 26 May 2023. [Retrieved on 20 February 2024]. Retrieved from <URL: https://eprint.iacr.org/archive/2023/767/20230526:110741 >. See sections 2-3.3.	1-20
☒ Further documents are listed in the continuation of Box C. ☒ See patent family annex.		
* Special categories of cited documents: “A” document defining the general state of the art which is not considered to be of particular relevance “D” document cited by the applicant in the international application “E” earlier application or patent but published on or after the international filing date “L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) “O” document referring to an oral disclosure, use, exhibition or other means “P” document published prior to the international filing date but later than the priority date claimed “T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention “X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone “Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art “&” document member of the same patent family		
Date of the actual completion of the international search 29 February 2024		Date of mailing of the international search report 29 February 2024
Name and mailing address of the ISA/KR Korean Intellectual Property Office Government Complex-Daejeon Building 4, 189 Cheongsaro, Seo-gu, Daejeon 35208 Facsimile No. +82-42-481-8578		Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2023/008079

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 10-2022-0169930 A (KOREA UNIVERSITY RESEARCH AND BUSINESS FOUNDATION) 28 December 2022 (2022-12-28) See paragraphs [0020]-[0101]; and figures 1-4.	1-20

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2023/008079

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
KR	10-2023-0078510	A	02 June 2023	US	2023-0171085	A1	01 June 2023
KR	10-2022-0169930	A	28 December 2022	None			

A. 발명이 속하는 기술분류(국제특허분류(IPC)) H04L 9/00(2006.01)i		
B. 조사된 분야 조사된 최소문헌(국제특허분류를 기재) H04L 9/00(2006.01) 조사된 기술분야에 속하는 최소문헌 이외의 문헌 한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC 일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC 국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우)) eKOMPASS(특허청 내부 검색시스템) & 키워드: 동형암호(homomorphic encryption), 라운드 키(round key), 라운드 함수(round function), 이중 블라인드 로테이션(double blind rotation)		
C. 관련 문헌		
카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	JINCHEOL HA 등, 'Rubato: Noisy Ciphers for Approximate Homomorphic Encryption (Full Version)', A major revision of an IACR publication in EUROCRYPT 2022, 2022.05.10, [검색일: 2024.02.20]. 출처: <URL: https://eprint.iacr.org/archive/2022/537/20220510:080623 > 섹션 2.4-3.1; 및 도면 1-2, 5	1-20
A	KR 10-2023-0078510 A (삼성전자주식회사) 2023.06.02 단락 [0101]-[0105]; 및 도면 2	1-20
A	CHRISTOPH DOBRAUNIG 등, 'Pasta: A Case for Hybrid Homomorphic Encryption', Preprint. MINOR revision, 2021.06.03, [검색일: 2024.02.20]. 출처: <URL: https://eprint.iacr.org/archive/2021/731/20210603:135802 > 섹션 1.1-6.2	1-20
A	ANDREY KIM 등, 'LFHE: Fully Homomorphic Encryption with Bootstrapping Key Size Less than a Megabyte', Preprint, 2023.05.26, [검색일: 2024.02.20]. 출처: <URL: https://eprint.iacr.org/archive/2023/767/20230526:110741 > 섹션 2-3.3	1-20
A	KR 10-2022-0169930 A (고려대학교 산학협력단) 2022.12.28 단락 [0020]-[0101]; 및 도면 1-4	1-20
☐ 추가 문헌이 C(계속)에 기재되어 있습니다. ☒ 대응특허에 관한 별지를 참조하십시오.		
* 인용된 문헌의 특별 카테고리: “A” 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌 “D” 본 국제출원에서 출원인이 인용한 문헌 “E” 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌 “L” 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌 “O” 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌 “P” 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌 “T” 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌 “X” 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다. “Y” 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다. “&” 동일한 대응특허문헌에 속하는 문헌		
국제조사의 실제 완료일 2024년02월29일 (29.02.2024)	국제조사보고서 발송일 2024년02월29일 (29.02.2024)	
ISA/KR의 명칭 및 우편주소 대한민국 특허청 (35208) 대전광역시 서구 청사로 189, 4동 (둔산동, 정부대전청사) 팩스 번호 +82-42-481-8578	심사관 양정록 전화번호 +82-42-481-5709	

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-2023-0078510 A	2023/06/02	US 2023-0171085 A1	2023/06/01
KR 10-2022-0169930 A	2022/12/28	없음	