



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0079084
(43) 공개일자 2017년07월10일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) H04L 29/06 (2006.01)
H04L 9/32 (2006.01)
(52) CPC특허분류
H04L 9/0819 (2013.01)
H04L 63/065 (2013.01)
(21) 출원번호 10-2015-0189266
(22) 출원일자 2015년12월30일
심사청구일자 2015년12월30일

(71) 출원인
이화여자대학교 산학협력단
서울특별시 서대문구 이화여대길 52 (대현동, 이화여자대학교)
(72) 발명자
리시
서울시 서대문구 이화여대7길 46,4층 영채리빙텔 207호 (대현동)
도인실
인천광역시 연수구 센트럴로 194, 201동 2705호(송도동, 더샵 센트럴파크2)
채기준
서울특별시 강남구 강남대로136길 34
(74) 대리인
특허법인(유한)아이시스

전체 청구항 수 : 총 15 항

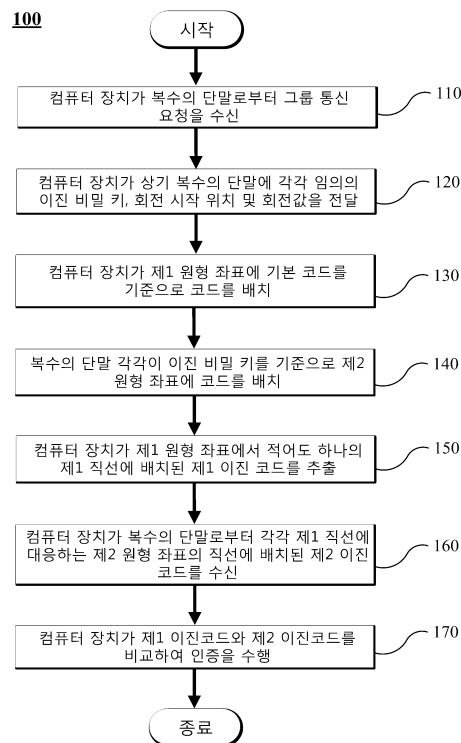
(54) 발명의 명칭 **상보적 인증 키를 생성하는 방법 및 상보적 인증 키에 기반한 그룹 통신 인증 기법**

(57) 요약

상보적 인증 키에 기반한 그룹 통신 인증 기법은 컴퓨터 장치가 복수의 단말로부터 그룹 통신에 대한 참여 요청을 수신하는 단계, 상기 컴퓨터 장치가 상기 복수의 단말 각각에 임의의 이진 비밀 키, 회전 시작 위치 및 회전값을 전달하는 단계, 상기 컴퓨터 장치가 복수의 원과 복수의 축을 갖는 제1 원형 좌표에서 상기 복수의

(뒷면에 계속)

대표도 - 도5



원 중 어느 하나인 제1 원에 상기 회전 시작 위치를 시작으로 배치되는 기본 코드를 기준으로 상기 복수의 원 중 상기 제1 원을 제외한 나머지 원에 코드를 배치하는 단계, 상기 컴퓨터 장치가 상기 제1 원형 좌표에서 복수의 축 중 어느 하나의 축인 제1 축과 상기 제1 축에서 연장되는 반대 축이 구성하는 직선에 배치된 제1 이진 코드를 추출하는 단계, 상기 컴퓨터 장치가 상기 복수의 단말 각각으로부터 상기 이진 비밀 키를 기준으로 코드가 배치된 상기 제1 원형 좌표와 동일한 형태의 제2 원형 좌표에서 상기 제1 축에 대응하는 제2 축과 상기 제2 축에서 연장되는 반대 축이 구성하는 직선에 배치된 제2 이진 코드를 수신하는 단계 및 상기 컴퓨터 장치가 상기 제1 이진 코드의 값과 상기 제2 이진 코드의 값을 비교하여 상기 복수의 단말에 대한 인증을 수행하는 단계를 포함한다. 상기 기본 코드는 상기 복수의 단말 각각에 전달한 이진 비밀 키를 연결한 제1 부분 코드 및 상기 제1 부분 코드에 상보적인 제2 부분 코드를 연결한 코드이다.

(52) CPC특허분류

H04L 9/0861 (2013.01)

H04L 9/3226 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 2012R1A1A3019459

부처명 미래창조과학부

연구관리전문기관 한국연구재단

연구사업명 기초연구사업(학술진흥)-일반연구자지원사업-여성과학자

연구과제명 사물지능통신(M2M) 응용분야 보안 연구

기 여 율 1/2

주관기관 이화여자대학교 산학협력단

연구기간 2012.05.01 ~ 2015.04.30이 발명을 지원한 국가연구개발사업

과제고유번호 2013R1A1A2011788

부처명 교육부

연구관리전문기관 한국연구재단

연구사업명 기초연구사업(학술진흥)

연구과제명 CDNi 환경에서의 안전하고 효율적인 서비스보안 기법

기 여 율 1/2

주관기관 이화여자대학교 산학협력단

연구기간 2015.06.01 ~ 2016.05.31

명세서

청구범위

청구항 1

컴퓨터 장치가 임의의 이진 코드인 제1 코드와 상기 이진 코드에 상보적인 제2 코드가 연결(concatenation)된 기본 코드를 생성하는 단계;

상기 컴퓨터 장치가 상기 기본 코드의 길이와 같은 개수인 복수의 축과 상기 기본 코드의 길이와 같은 개수인 복수의 원을 갖는 원형 좌표를 생성하는 단계;

상기 컴퓨터 장치가 상기 원형 좌표의 중심에서 가장 가까운 원인 제1 원상에 상기 복수의 축 중 어느 하나의 축을 시작으로 상기 기본 코드를 배치하는 단계;

상기 컴퓨터 장치가 상기 복수의 원에 코드가 모두 배치될 때까지 상기 중심을 기준으로 상기 원형 좌표에서 코드가 배치된 가장 바깥쪽 원에 배치된 코드를 상기 복수의 축상에서 기준값만큼 기준 방향으로 회전한 코드를 상기 중심을 기준으로 상기 바깥쪽 원의 다음에 위치한 원에 배치하는 과정을 반복하는 단계; 및

상기 컴퓨터 장치가 상기 복수의 축 중 하나인 제1 축과 상기 제1 축에서 연장되는 반대 축이 구성하는 직선상에 배치된 일련의 코드를 추출하는 단계를 포함하는 상보적 인증 키를 생성하는 방법.

청구항 2

제1항에 있어서,

상기 제2 코드는 상기 이진 코드와 XOR 연산하여 모든 비트 자리수가 1이 나오는 코드인 상보적 인증 키를 생성하는 방법.

청구항 3

제1항에 있어서,

상기 컴퓨터 장치는 상기 기본 코드 중 일부 코드를 통신에 참여하는 제1 기기에 전달하는 단계; 및

상기 컴퓨터 장치가 상기 제1 기기에서 전달한 단말 코드와 상기 일련의 코드를 비교하여 상기 제1 기기에 대한 인증을 수행하는 단계를 더 포함하는 상보적 인증 키를 생성하는 방법.

청구항 4

제3항에 있어서,

상기 제1 기기가 상기 기본 코드의 길이와 같은 개수인 복수의 축과 상기 기본 코드의 길이와 같은 개수인 복수의 원을 갖는 제2 원형 좌표의 중심에서 가장 가까운 원인 제1 원상에 상기 복수의 축 중 어느 하나의 축을 시작으로 상기 일부 코드를 배치하는 단계;

상기 제1 기기가 상기 복수의 원에 코드가 모두 배치될 때까지 상기 중심을 기준으로 상기 제2 원형 좌표에서 코드가 배치된 가장 바깥쪽 원에 배치된 코드를 상기 복수의 축상에서 기준값만큼 기준 방향으로 회전한 코드를 상기 중심을 기준으로 상기 바깥쪽 원의 다음에 위치한 원에 배치하는 과정을 반복하는 단계; 및

상기 제1 기기가 상기 복수의 축 중 상기 제1 축에 대응하는 제2 축과 상기 제2 축에서 연장되는 반대 축이 구성하는 직선상에 배치된 일련의 코드를 추출하여 상기 단말 코드를 생성하는 단계를 더 포함하는 상보적 인증 키를 생성하는 방법.

청구항 5

컴퓨터 장치가 복수의 단말로부터 그룹 통신에 대한 참여 요청을 수신하는 단계;

상기 컴퓨터 장치가 상기 복수의 단말 각각에 임의의 이진 비밀 키, 회전 시작 위치 및 동일한 회전값을 전달하는 단계;

상기 컴퓨터 장치가 복수의 원과 복수의 축을 갖는 제1 원형 좌표에서 상기 복수의 원 중 어느 하나인 제1 원에 상기 회전 시작 위치를 시작으로 배치되는 기본 코드를 기준으로 상기 복수의 원 중 상기 제1 원을 제외한 나머지 원에 코드를 배치하는 단계;

상기 컴퓨터 장치가 상기 제1 원형 좌표에서 복수의 축 중 어느 하나의 축인 제1 축과 상기 제1 축에서 연장되는 반대 축이 구성하는 직선에 배치된 제1 이진 코드를 추출하는 단계;

상기 컴퓨터 장치가 상기 복수의 단말 각각으로부터 상기 이진 비밀 키를 기준으로 코드가 배치된 상기 제1 원형 좌표와 동일한 형태의 제2 원형 좌표에서 상기 제1 축에 대응하는 제2 축과 상기 제2 축에서 연장되는 반대 축이 구성하는 직선에 배치된 제2 이진 코드를 수신하는 단계; 및

상기 컴퓨터 장치가 상기 제1 이진 코드의 값과 상기 제2 이진 코드의 값을 비교하여 상기 복수의 단말에 대한 인증을 수행하는 단계를 포함하되,

상기 기본 코드는 상기 복수의 단말 각각에 전달한 이진 비밀 키를 연결한 제1 부분 코드 및 상기 제1 부분 코드에 상보적인 제2 부분 코드를 연결한 코드인 상보적 인증 키에 기반한 그룹 통신 인증 기법.

청구항 6

제5항에 있어서,

상기 컴퓨터 장치는 상기 복수의 단말 중 어느 하나의 단말 또는 별도의 서버인 상보적 인증 키에 기반한 그룹 통신 인증 기법.

청구항 7

제5항에 있어서,

상기 컴퓨터 장치는 상기 복수의 단말 각각에 서로 다른 임의의 이진 비밀 키를 전달하는 상보적 인증 키에 기반한 그룹 통신 인증 기법.

청구항 8

제5항에 있어서,

상기 컴퓨터 장치는 상기 복수의 단말 각각에 서로 다른 회전 시작 위치를 전달하는 상보적 인증 키에 기반한 그룹 통신 인증 기법.

청구항 9

제5항에 있어서,

상기 제1 부분 코드와 상기 제2 부분 코드는 XOR 연산하여 모든 비트 자리수가 1이 나오는 관계인 상보적 인증 키에 기반한 그룹 통신 인증 기법.

청구항 10

제5항에 있어서,

상기 컴퓨터 장치는 상기 회전 시작 위치 및 상기 회전값 중 적어도 하나를 상기 이진 비밀 키로 암호화하여 전달하는 상보적 인증 키에 기반한 그룹 통신 인증 기법.

청구항 11

제5항에 있어서,

상기 제1 이진 코드를 추출하는 단계는

상기 컴퓨터 장치가 상기 기본 코드의 길이와 같은 개수인 복수의 축과 상기 기본 코드의 길이와 같은 개수인 복수의 원을 갖는 상기 제1 원형 좌표의 중심에서 가장 가까운 원인 상기 제1 원상에 상기 복수의 축 중 어느 하나의 축을 시작으로 상기 기본 코드를 배치하는 단계;

상기 컴퓨터 장치가 상기 복수의 원에 코드가 모두 배치될 때까지 상기 중심을 기준으로 상기 제1 원형 좌표에

서 코드가 배치된 가장 바깥쪽 원에 배치된 코드를 상기 복수의 축상에서 상기 회전값만큼 기준 방향으로 회전한 코드를 상기 중심을 기준으로 상기 바깥쪽 원의 다음에 위치한 원에 배치하는 과정을 반복하는 단계; 및
상기 컴퓨터 장치가 상기 제1 축 및 상기 제1 축에서 연장되는 반대 축이 구성하는 직선상에 배치된 일련의 코드를 추출하는 단계를 포함하는 상보적 인증 키에 기반한 그룹 통신 인증 기법.

청구항 12

제5항에 있어서,

상기 제2 이진 코드를 수신하는 단계는

상기 복수의 단말 각각이 상기 기본 코드의 길이와 같은 개수인 복수의 축과 상기 기본 코드의 길이와 같은 개수인 복수의 원을 갖는 상기 제2 원형 좌표의 중심에서 가장 가까운 원인 상기 제2 원상에 상기 복수의 축 중 상기 회전 시작 위치를 시작으로 상기 이진 비밀 키를 배치하고, 상기 이진 비밀 키가 배치된 위치의 대칭된 축에 상기 이진 비밀 키에 상보적인 키를 배치하는 단계;

상기 복수의 단말 각각이 상기 복수의 원에 코드가 모두 배치될 때까지 상기 중심을 기준으로 상기 제2 원형 좌표에서 코드가 배치된 가장 바깥쪽 원에 배치된 코드를 상기 복수의 축상에서 상기 회전값만큼 기준 방향으로 회전한 코드를 상기 중심을 기준으로 상기 바깥쪽 원의 다음에 위치한 원에 배치하는 과정을 반복하는 단계; 및

상기 복수의 단말 각각이 상기 제2 축 및 상기 제2 축에서 연장되는 반대 축이 구성하는 직선상에 배치된 일련의 코드를 추출하는 단계를 포함하는 상보적 인증 키에 기반한 그룹 통신 인증 기법.

청구항 13

제5항에 있어서,

상기 컴퓨터 장치는 상기 제1 이진 코드와 상기 제2 이진 코드를 XOR 연산하여 나온 결과가 0인 경우 상기 복수의 단말에 대한 인증이 성공했다고 판단하는 상보적 인증 키에 기반한 그룹 통신 인증 기법.

청구항 14

제5항에 있어서,

상기 컴퓨터 장치는 상기 복수의 단말에 기준 함수를 단계를 더 포함하고,

상기 컴퓨터 장치는 상기 기준 함수에 상기 제1 이진 코드를 적용하여 제1 값을 생성하고, 상기 컴퓨터 장치는 상기 복수의 단말 각각으로부터 상기 기준 함수에 상기 제2 이진 코드를 적용한 제2 값을 수신하고, 상기 컴퓨터 장치는 상기 제1 값과 상기 제2 값을 비교하여 상기 복수의 단말에 대한 인증을 수행하는 상보적 인증 키에 기반한 그룹 통신 인증 기법.

청구항 15

제14항에 있어서,

상기 컴퓨터 장치는 상기 복수의 단말 각각에 임의의 숫자 또는 시간값 중 적어도 하나를 전달하는 단계를 더 포함하고,

상기 컴퓨터 장치는 상기 기준 함수에 상기 숫자 또는 시간값 중 상기 복수의 단말에 전달한 값을 상기 기준 함수에 대한 입력값으로 더 사용하여 상기 제1 값을 생성하고, 상기 컴퓨터 장치는 상기 복수의 단말 각각으로부터 상기 숫자 또는 시간값 중 수신한 값을 상기 기준 함수에 대한 입력값으로 더 사용하여 상기 제2 값을 생성하는 상보적 인증 키에 기반한 그룹 통신 인증 기법.

발명의 설명

기술 분야

이하 설명하는 기술은 그룹 통신 인증을 위한 기법에 관한 것이다.

배경 기술

[0001]

[0002] 무선 네트워크를 통해 통신을 수행하는 주체는 일반적으로 인증을 받는다. RSA(Rivest Shamir Adleman)는 1:1 통신에서 사용하는 주요한 인증방법 중 하나이다. 통신 기술 발달과 함께 그룹 통신 기법이 등장하였다. 그룹 통신에서도 통신에 참여하는 다수의 주체는 인증을 받아야 한다. 그룹 통신을 위한 인증 기법은 크게 인증서버가 인증을 수행하는 기법과 인증서버 없이 통신에 참여하는 주체가 서로를 인증하는 기법이 있다.

[0003] 한편 이동성을 갖는 모바일 단말이 그룹 통신을 수행하는 경우도 많이 증가하였다. 이 경우 그룹 통신에 참여하는 단말이 자유롭게 해당 통신에 참여하거나, 통신을 그만둘 수 있다. 즉 모바일 단말이 참여하는 그룹 통신은 통신에 참여하는 주체가 동적으로 변경될 수 있다. 이러한 네트워크를 사용자 중심 네트워크(User-centric wireless network)라고 부르기도 한다.

선행기술문헌

비특허문헌

- [0004] (비특허문헌 0001) M.A. Catur Bhakti, A. Abdullah, and L.T. Jung, "EAP-Based Authentication for Ad Hoc Network," Proc. Seminar Nasional Aplikasi Teknologi Informasi (SNATI) Conf., pp. C-133-C-137, 2007
- (비특허문헌 0002) A.A. Pirzada and C. McDonald, "Kerberos Assisted Authentication in Mobile Ad-Hoc Networks," Proc. 27th Australasian Computer Science Conf. (ACSC), vol. 26, no. 1, pp. 41-46, 2004.
- (비특허문헌 0003) S. Capkun, L. Buttyan, and J.P. Hubaux, "Self-Organized Public-Key Management for Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 2, no. 1, pp. 52-64, Jan.-Mar. 2003.

발명의 내용

해결하려는 과제

- [0005] 이하 설명하는 기술은 사용자 중심 네트워크에서 그룹 통신을 수행하는 주체들을 인증하는 기법을 제공하고자 한다. 또한 이하 설명하는 기술은 통신에 참여하는 주체를 인증하기 위한 상보적 코드(complementary code)를 생성하는 기법을 제공하고자 한다.

과제의 해결 수단

- [0006] 상보적 인증 키를 생성하는 방법은 컴퓨터 장치가 임의의 이진 코드인 제1 코드와 상기 이진 코드에 상보적인 제2 코드가 연결(concatenation)된 기본 코드를 생성하는 단계, 상기 컴퓨터 장치가 상기 기본 코드의 길이와 같은 개수인 복수의 축과 상기 기본 코드의 길이와 같은 개수인 복수의 원을 갖는 원형 좌표를 생성하는 단계, 상기 컴퓨터 장치가 상기 원형 좌표의 중심에서 가장 가까운 원인 제1 원상에 상기 복수의 축 중 어느 하나의 축을 시작으로 상기 기본 코드를 배치하는 단계, 상기 컴퓨터 장치가 상기 복수의 원에 코드가 모두 배치될 때까지 상기 중심을 기준으로 상기 원형 좌표에서 코드가 배치된 가장 바깥쪽 원에 배치된 코드를 상기 복수의 축 상에서 기준값만큼 기준 방향으로 회전한 코드를 상기 중심을 기준으로 상기 바깥쪽 원의 다음에 위치한 원에 배치하는 과정을 반복하는 단계 및 상기 컴퓨터 장치가 상기 복수의 축 중 하나인 제1 축과 상기 제1 축에서 연장되는 반대 축이 구성하는 직선상에 배치된 일련의 코드를 추출하는 단계를 포함한다.

- [0007] 상보적 인증 키에 기반한 그룹 통신 인증 기법은 컴퓨터 장치가 복수의 단말로부터 그룹 통신에 대한 참여 요청을 수신하는 단계, 상기 컴퓨터 장치가 상기 복수의 단말 각각에 임의의 이진 비밀 키, 회전 시작 위치 및 동일한 회전값을 전달하는 단계, 상기 컴퓨터 장치가 복수의 원과 복수의 축을 갖는 제1 원형 좌표에서 상기 복수의 원 중 어느 하나인 제1 원에 상기 회전 시작 위치를 시작으로 배치되는 기본 코드를 기준으로 상기 복수의 원 중 상기 제1 원을 제외한 나머지 원에 코드를 배치하는 단계, 상기 컴퓨터 장치가 상기 제1 원형 좌표에서 복수의 축 중 어느 하나의 축인 제1 축과 상기 제1 축에서 연장되는 반대 축이 구성하는 직선에 배치된 제1 이진 코드를 추출하는 단계, 상기 컴퓨터 장치가 상기 복수의 단말 각각으로부터 상기 이진 비밀 키를 기준으로 코드가 배치된 상기 제1 원형 좌표와 동일한 형태의 제2 원형 좌표에서 상기 제1 축에 대응하는 제2 축과 상기 제2 축에서 연장되는 반대 축이 구성하는 직선에 배치된 제2 이진 코드를 수신하는 단계 및 상기 컴퓨터 장치가 상기 제1 이진 코드의 값과 상기 제2 이진 코드의 값을 비교하여 상기 복수의 단말에 대한 인증을 수행하는 단계를 포함한다.

[0008] 상기 기본 코드는 상기 복수의 단말 각각에 전달한 이진 비밀 키를 연결한 제1 부분 코드 및 상기 제1 부분 코드에 상보적인 제2 부분 코드를 연결한 코드이다.

발명의 효과

[0009] 이하 설명하는 기술은 그룹 통신에 참여하는 각 주체에 대한 보상적 코드를 부여하고, 한번에 그룹 통신에 참여한 주체를 인증할 수 있다.

도면의 간단한 설명

[0010] 도 1은 8자리 이진 코드를 원형 좌표에 표시한 예이다.

도 2는 기본 코드를 회전하여 서로 다른 이진 코드를 생성한 예이다.

도 3은 3개의 단말에 대한 보상적 코드를 생성하기 위한 원형 좌표에 대한 예이다.

도 4는 그룹 통신에 참여하는 단말이 이진 비밀 코드를 원형 좌표에 배치한 예이다.

도 5는 상보적 인증 키에 기반한 그룹 통신 인증 기법에 대한 순서도의 예이다.

도 6은 상보적 인증 키에 기반한 그룹 통신 인증 기법에 대한 순서도의 다른 예이다.

도 7은 상보적 인증 키에 기반한 그룹 통신 인증 기법이 수행되는 네트워크 시스템에 대한 예이다.

발명을 실시하기 위한 구체적인 내용

[0011] 이하 설명하는 기술은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세하게 설명하고자 한다. 그러나, 이는 이하 설명하는 기술을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 이하 설명하는 기술의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.

[0012] 제1, 제2, A, B 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 해당 구성요소들은 상기 용어들에 의해 한정되지는 않으며, 단지 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 이하 설명하는 기술의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[0013] 본 명세서에서 사용되는 용어에서 단수의 표현은 문맥상 명백하게 다르게 해석되지 않는 한 복수의 표현을 포함하는 것으로 이해되어야 하고, "포함한다" 등의 용어는 실시된 특징, 개수, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것이 존재함을 의미하는 것이지, 하나 또는 그 이상의 다른 특징들이나 개수, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 배제하지 않는 것으로 이해되어야 한다.

[0014] 도면에 대한 상세한 설명을 하기에 앞서, 본 명세서에서의 구성부들에 대한 구분은 각 구성부가 담당하는 주기능 별로 구분한 것에 불과함을 명확히 하고자 한다. 즉, 이하에서 설명할 2개 이상의 구성부가 하나의 구성부로 합쳐지거나 또는 하나의 구성부가 보다 세분화된 기능별로 2개 이상으로 분화되어 구비될 수도 있다. 그리고 이하에서 설명할 구성부 각각은 자신이 담당하는 주기능 이외에도 다른 구성부가 담당하는 기능 중 일부 또는 전부의 기능을 추가적으로 수행할 수도 있으며, 구성부 각각이 담당하는 주기능 중 일부 기능이 다른 구성부에 의해 전담되어 수행될 수도 있음은 물론이다.

[0015] 또, 방법 또는 동작 방법을 수행함에 있어서, 상기 방법을 이루는 각 과정들은 문맥상 명백하게 특정 순서를 기재하지 않은 이상 명기된 순서와 다르게 일어날 수 있다. 즉, 각 과정들은 명기된 순서와 동일하게 일어날 수도 있고 실질적으로 동시에 수행될 수도 있으며 반대의 순서대로 수행될 수도 있다.

[0017] 이하 설명하는 기술은 전술한 바와 같이 네트워크를 통해 그룹 통신에 참여하는 주체에 대한 인증 기법에 관한 것이다. 그룹 통신은 PC, 스마트폰 등과 같은 기기를 통해 사용자들이 참여하는 통신을 말한다. 설명의 편의를 위해 이하 그룹 통신에 참여하는 주체를 '단말'이라고 명명한다. 단말은 네트워크에 접속할 수 있는 다양한 컴퓨팅 장치를 포함한다. 단말은 PC, 태블릿 PC, 노트북, 스마트폰, 웨어러블 기기 등과 같은 장치를 포함한다.

- [0019] **상보적 코드 생성**
- [0020] 그룹 통신에 참여하는 단말은 각각 하나의 코드를 할당받는다. 한 쌍의 코드는 서로 상보적인 관계이다. 여기서 상보적 관계란 두 개의 이진 코드를 XOR 연산하면 모든 코드의 자리가 1이 되는 관계를 의미한다. 먼저 상보적 코드를 생성하는 과정에 대해 설명한다.
- [0022] 정의1: 두 개의 이진 코드 $code_A = \{a_i\}$ 및 $code_B = \{b_i\}$ 는 크기(자리수)가 동일하다. 즉 $a_i, b_i \in \{0, 1\}$, $i = 0, 1, 2, \dots, n$ 이다. 이때 $a_i \oplus b_i = 1$ 이라면 $code_A$ 와 $code_B$ 는 한쌍의 상보적 코드에 해당한다. $\oplus$ 는 XOR 연산을 의미한다.
- [0024] 이하 8비트의 길이를 갖는 상보적 코드를 기준으로 상보적 코드를 생성하는 과정에 대해 설명한다.
- [0026] 과정 1: 임의의 4비트 코드 c_0 를 선택하고(예컨대, 0110), 선택한 코드 c_0 에 대해 상보적 코드인 $\overline{c_0}$ (1001)를 c_0 의 뒤에 연결(concatenation)한다. 즉, 새롭게 생성된 코드를 u_0 라고 하면 $u_0 = c_0 \parallel \overline{c_0}$ 이다. $\parallel$ 는 문자열 접합(concatenation) 연산을 의미한다. 새롭게 생성된 코드 u_0 (0110 1001)는 이후 다른 코드를 생성하는데 사용된다. 처음 생성된 8자리 코드 u_0 를 이하 기본 코드라고 명명한다.
- [0028] 과정 2: 기본 코드 u_0 (0110 1001)를 8개의 축($x_0 \sim x_7$)에 배치한다. 이진 코드의 자리수와 축의 순서를 서로 대응되게 배치하면 도 1과 같다. 도 1은 8자리 이진 코드를 원형 좌표에 표시한 예이다. 도 1에 도시한 8자리 이진 코드는 전술한 기본 코드에 해당한다. 도 1에서 흰색 점은 이진수 '0'을 나타내고, 검은색 점은 이진수 '1'을 나타낸다. 도 1에서 기본 코드는 가장 안쪽에 있는 원에 도시하였다. 원형 좌표에서 원의 순서는 중심 위치로부터 가까운 순서로 설명한다. 즉 원형 좌표의 중심점에서 가장 가까운(안쪽) 원이 첫 번째 원이고, 그 다음 가까운 원이 두 번째 원에 해당한다. 이하 설명의 편의를 위해 $u_{0,i}$ 는 u_0 의 x_i 축에 배치된 비트를 의미한다고 전제한다. 예컨대, $u_{0,0} = 0$ 이고, $u_{0,4} = 1$ 이다. 도 1에 도시한 원형 좌표에서 기본 코드를 일정하게 이동하여 모두 8개의 서로 다른 좌표를 생성할 수 있다.
- [0030] 과정 3: 기본 코드를 이용하여 다른 상보적 코드를 생성하기 위해 원형 좌표에서 기본 코드를 일정하게 회전 이동(일종의 shift)한다. 임의의 정수 d 를 선택하고, d 만큼 기본 코드를 회전한다. 예를 들어 $d=1$ 이라고 가정하면 u_0 를 도 1의 원형 좌표에서 시계 방향으로 1비트씩 회전 이동하여 다른 코드인 u_1 (1011 0100)를 생성할 수 있다. 새롭게 생성한 u_1 를 u_0 가 배치된 원의 바깥쪽 원(즉 중심으로부터 2번째 원)에 배치할 수 있다. u_1 을 시계 방향으로 1비트씩 회전하여 u_2 라는 코드를 생성할 수 있고, u_2 를 중심으로부터 3번째 원에 배치할 수 있다. 이와 같은 과정을 반복하면 기본 코드를 포함하여 $u_0 \sim u_7$ 까지 모두 8개의 이진 코드를 생성할 수 있다.
- [0031] 도 2는 기본 코드를 회전하여 서로 다른 이진 코드를 생성한 예이다. 도 2(a)는 전술한 u_0 를 시작으로 시계방향으로 1비트씩 회전하면서 $u_1 \sim u_7$ 까지 생성한 예이다. 원형 좌표에서 중심으로부터의 순서대로 원에 $u_0 \sim u_7$ 을 배치한 예이다. 이하 설명의 편의를 위해 w_{ij} 를 x_i 의 축에서 $j(j \geq 0)$ 번째 원에 배치된 이진수라고 한다. $w_{ij} = u_{ji}$ 인 관계이다. 예컨대, $w_{1,2} = u_{2,1} = 1$ 이고, $w_{3,0} = u_{0,3} = 0$ 이다. 원형 좌표에서 하나의 같은 직선에 배치된 이진 코드는 서로 상보적이다. 예를 들어 축 x_1 에 배치된 이진 코드(1010 0101)와 축 x_5 에 배치된 이진 코드(0101 1010)는 한 쌍의 상보적인 코드에 해당한다. 도 2(a)를 살펴보면 모두 4개의 상보적인 코

드 쌍이 존재한다.

[0032] 도 2(b)는 기본 코드 u_0 에 $d = -2$ 를 적용하여 생성한 코드의 예이다. 즉, 8비트 코드를 반시계 방향으로 2자리씩 회전 이동하면서 코드를 생성한 예이다. 역시 하나의 직선을 이루는 두 개의 마주보는 축은 상보적인 코드를 갖고 있다. 따라서 도 2(b)에서도 4개의 상보적인 코드 쌍이 존재한다. 이하 기본 코드와 원형 좌표를 이용하여 생성한 상보적인 코드를 이용한 인증 기법에 대해 설명한다.

[0034] 상보적 코드에 기반한 그룹 인증 기법

[0035] 이하 설명하는 그룹 인증 기법은 전술한 보상적 코드를 이용하여 그룹에 참여하는 모든 단말을 한 번에 인증하는 기법이다. 그룹 인증은 어떤 하나의 장치가 그룹에 참여하는 단말에 대한 인증을 수행한다. 인증을 수행하는 주체가 되는 장치를 GM(Group Manager)라고 명명한다. GM은 그룹 인증에 참여하는 하나의 단말이 될 수도 있고, 그룹 인증 서비스를 제공하는 별도의 서버일 수도 있다. 일정한 인증 작업을 수행하는 GM은 컴퓨터 장치에 해당한다.

[0037] (1) 그룹 인증 단계

[0038] 먼저 GM은 그룹 통신에 참여하려는 단말 각각에 이진 비밀 코드 c_0^i 를 할당한다. 여기서 $1 \leq i \leq n$ 이고, n 은 그룹 통신에 참여하는 단말의 수이다. 각 단말은 자신에게 할당된 이진 비밀 코드 c_0^i 만을 알고, 다른 단말에 할당된 이진 비밀 코드는 알지 못한다. 예컨대, 그룹 통신에 3개의 단말(m_1, m_2 및 m_3)이 참여한다면 각각의 이진 비밀 코드는 $c_0^1 = 100$, $c_0^2 = 110$, $c_0^3 = 01$ 일 수 있다. 후술하겠지만 GM이 각 단말에 할당하는 이진 비밀 코드는 기본 코드를 생성하는데 사용된다.

[0039] 그리고 GM은 그룹 통신에 참여하는 각 단말에 일방향 함수 f 를 전달한다. f 는 고정된 x_i 축에서 서로 다른 원을 생성하는데 사용되는 값이다. 구체적인 내용은 후술한다. 또 GM은 그룹 통신에 참여하는 단말의 수에 대응하는 원형 좌표의 크기를 결정하고, 결정한 크기를 각 단말에 알려준다.

[0041] (2) 그룹 인증 단계

[0042] 이 과정에서 GM은 그룹 통신에 참여하는 단말을 모두 한 번에 인증한다. GM은 그룹 통신에 참여하는 모든 단말에 대해 c_0^i 의 전체 길이에 대응하는 축의 개수를 갖는 크기의 원형 좌표상에 각 이진 비밀 코드 c_0^i 를 전달한다.

[0044] 과정 1: 전술한 기본 코드를 구성하는 c_0 는 $c_0 = c_0^1 \| c_0^2 \| \dots \| c_0^n$ 로 표현할 수 있고, $\bar{c}_0$ 는 $\bar{c}_0 = \bar{c}_0^1 \| \bar{c}_0^2 \| \dots \| \bar{c}_0^n$ 라 표현될 수 있다. 따라서 원형 좌표에 최초로 배치되는 기본 코드는 $u_0 = c_0 \| \bar{c}_0 = c_0^1 \| c_0^2 \| \dots \| c_0^n \| \bar{c}_0^1 \| \bar{c}_0^2 \| \dots \| \bar{c}_0^n$ 라고 표현될 수 있다. 원형 좌표에서 축의 개수는 u_0 의 길이와 동일하다.

[0045] 예를 들어 전술한 바와 같이 그룹 통신에 참여하는 단말이 3개(m_1, m_2 및 m_3)라고 가정하면, $c_0 = 100 \ 110 \ 01$, $\bar{c}_0 = 011 \ 001$, $u_0 = 100 \ 110 \ 01 \ 011 \ 001 \ 10$ 을 사용할 수 있다. u_0 는 원형 좌표에서 중심에서 가장 가까운 첫 번째 원에 배치된다. 도 3은 3개의 단말에 대한 보상적 코드를 생성하기 위한 원형 좌표에 대한 예이다. 도 3은 첫 번째 원에 $u_0 = 100 \ 110 \ 01 \ 011 \ 001 \ 10$ 가 배치된 상태를 도시한다. 도 3에서 u_0 는 x_0 부터 x_{15} 까지 배치된 예를 도시한다. 그러나 원형 좌표의 어떤 축에서 u_0 의 배치를 시작할지는 다양할 수 있다. u_0 의 첫째 비트가 원형 좌표의 $x_0 \sim x_{15}$ 중 어느 하나의 자리부터 배치를 시작해도 관계없다. GM은 원형 좌표의 원에서 이진 코드가 배

치되는 시작점(x_{start}^i)를 아래의 수학적 식 1과 같이 암호화할 수 있다.

수학적 식 1

$$E(x_{start}^i) = x_{start}^i \oplus c_0^i$$

여기서 $\oplus$ 는 XOR 비트 연산자이다. GM은 $E(x_{start}^i)$ 를 각 단말 m_i 에 전송한다.

도 3은 기본 코드를 첫 번째 원에 배치하고, 시계 방향으로 2자리씩 회전 이동하면서 이진 코드를 원형 좌표에 배치한 예이다. 도 3에서 녹색은 m_1 에 대한 코드, 적색은 m_2 에 대한 코드, 파란색은 m_3 에 대한 코드를 각각 나타낸다. GM은 도 3과 같은 원형 좌표에 배치된 이진 코드를 마련한 상태라고 가정한다.

과정 2: 단말 m_i 는 $E(x_{start}^i)$ 를 수신한 후 자신이 보유한 이진 비밀 코드 c_0^i 를 사용하여 원형 좌표의 원에서 이진코드의 배치가 시작되는 시작점 x_{start}^i 을 복호한다. 그리고 도 4와 같이 원형 좌표의 첫 번째 원에서 시작점을 기준으로 자신의 c_0^i 를 배치한다. 도 4는 그룹 통신에 참여하는 단말이 이진 비밀 코드를 원형 좌표에 배치한 예이다. 도 4(a)는 m_1 이 첫 번째 원에서 시작점 $x_{start}^1 = x_0$ 부터 c_0^1 (100)을 배치하고, 원형 좌표에서 대칭되는 위치에 상보적 코드인 $\overline{c_0^1}$ (011)를 배치한 예이다. 도 4(b)는 m_2 가 첫 번째 원에서 시작점 $x_{start}^2 = x_1$ 부터 c_0^2 (110)을 배치하고, 원형 좌표에서 대칭되는 위치에 상보적 코드인 $\overline{c_0^2}$ (001)를 배치한 예이다. 도 4(c)는 m_3 가 첫 번째 원에서 시작점 $x_{start}^3 = x_6$ 부터 c_0^3 (01)을 배치하고, 원형 좌표에서 대칭되는 위치에 상보적 코드인 $\overline{c_0^3}$ (10)를 배치한 예이다.

과정 3: GM은 임의의 정수 d 를 선택하고, 각 단말 m_i 에 $d \oplus c_0^i$ 를 전달한다. 각 단말은 자신의 이진 비밀 코드 c_0^i 를 사용하여 d 를 복호한다. 각 단말은 원형 좌표의 첫 번째 원에 배치한 c_0^i 및 $\overline{c_0^i}$ (c_0^i 의 상보적 코드)를 d 만큼 회전 이동하여 두 번째 원에 배치한다. 그리고 각 단말은 원형 좌표의 나머지 원들에서도 동일한 방식으로 이진 코드를 배치한다. 도 4에서 $d = 2$ 인 경우를 도시한다. 이 과정이 완료되면 각 단말 m_i 는 원형 좌표에서 하나의 축 x_j 에 일련의 코드 세트 $\{w_{x_j}^i\}$ 를 마련하게 된다. 예컨대, $w_{x_2}^1 = 01**10**$, $w_{x_3}^2 = 1**10**0$, $w_{x_4}^3 = ***1***0$ 이다. 여기서 *는 이진수가 없는 빈 자리를 의미한다. GM은 각 단말에 원형 좌표가 몇 개의 원인지 또는 몇 번 회전하면서 코드를 생성할지에 대한 정보를 전송할 수 있다. 또한 전송한 바와 같이 각 단말이 생성한 코드도 마주보는 축에서 상보적인 관계를 갖는다. p 번째 원에서 축 x_j 에 배치된 코드를 $w_{x_j}^i$ 이고 x_j 에 대칭인 축에 배치된 코드를 $w_{x_j}^i$ 라고 하면 $w_{x_j,p}^i \oplus w_{x_j,p}^i = 1$ 인 관계를 갖는다. 도 4(a)는 단말 m_1 이 원형 좌표에 모든 코드를 생성하여 배치한 경우에 대한 예이고, 도 4(b)는 단말 m_2 가 원형 좌표에 모든 코드를 생성하여 배치한 경우에 대한 예이고, 도 4(c)는 단말 m_3 가 원형 좌표에 모든 코드를 생성하여 배치한 경우에 대한 예이다.

도 4(a)에서 $w_{x_2}^1 = 01**10**$ 이고 반대방향 축에 위치한 상보적인 코드는 $w_{x_{10}}^1 = 10**01**$ 이다. 결국 x_2 와

x_{10} 으로 구성되는 직선 $l_{x_2, x_{10}}^1$ 에 위치한 코드는 $l_{x_2, x_{10}}^1 = w_{x_2}^1 \oplus w_{x_{10}}^1 = 11^{**}11^{**}$ 인 관계를 갖는다. 각 단말은 자신이 관리하는 원형 좌표에서 축 x_j 에 대해 $l_{x_j, \bar{x}_j}^i$ 를 연산해 볼 수 있다.

[0056] 나아가 그룹 통신에 참여하는 각 단말에서 생성한 원형 좌표상에서 하나의 직선(예컨대, x_2 및 x_{10} 이 구성하는)에서 각 축에 배치된 코드를 XOR 연산한 결과를 합산하면 $l_{x_2, x_{10}}^1 + l_{x_2, x_{10}}^2 + l_{x_2, x_{10}}^3 = 11^{**}11^{**} + ***1^{***}1 + **1^{***}1^* = 11111111$ 과 같다.

[0057] 도 4(d)는 도 4(a) 내지 도 4(c)에서 각 단말(m_1 , m_2 및 m_3)이 생성한 코드를 합산한 결과이다. 도 4(d)는 도 3과 동일하다.

[0059] 과정 4: GM은 임의의 숫자 r 을 생성하고, 각 단말 m_i 에 각 단말에 부여한 이진 비밀 코드 c_0^i 로 r 을 아래의 수학식 2와 같이 암호화하여 전달한다. 그리고 GM은 타임 스탬프(time stamp) TS도 아래의 수학식 2와 같이 암호화하여 각 단말 m_i 에 전달한다.

수학식 2

$$E(r) = r \oplus c_0^i$$

$$E(TS) = TS \oplus c_0^i$$

[0061]

[0063] 각 단말 m_i 는 GM으로부터 수신했던 함수 f 를 이용하여 특정 직선(예컨대, $x_j, \bar{x}_j$)을 기준으로 자신의 원형 좌표의 각 원에 대해 특정 값을 연산한다. 각 단말 m_i 는 각 원에 대해 특정 값을 연산하므로 원의 개수만큼의 요소를 갖는 연산값을 보유하게 된다. 각 단말 m_i 는 아래와 같은 수학식 3을 사용하여 각 원에 대한 특정 값을 연산한다. 이하 각 단말 m_i 가 연산한 특정값을 단말 연산값이라고 명명한다.

수학식 3

$$f(ID_i \parallel l_{x_j, \bar{x}_j}^i \parallel x_j \parallel r \parallel TS \parallel k) = \{a_1, a_2 \dots a_k\}$$

[0065]

[0066] 여기서, ID_i 는 각 단말 m_i 에 대한 식별자이고, k 는 $l_{x_j, \bar{x}_j}^i$ 의 길이이다. $l_{x_j, \bar{x}_j}^i$ 가 1인 값을 갖는 경우에만 상기 수학식 3으로 표현되는 함수 f 의 결과값이 산출된다.

[0067] 한편 후술하겠지만 GM도 자신이 보유한 원형 좌표의 각 원에 대해 상기 수학식 3과 같은 연산을 수행한다. GM이 연산한 특정값을 GM 연산값이라고 명명한다. 단말 연산값 또는 GM 연산값은 복수의 원에 대해 각각 연산한 결과이므로 각각 복수의 요소를 갖는 집합 $\{a_1, a_2, \dots a_k\}$ 으로 산출된다.

[0069] 아래 표 1은 도 3 및 도 4에 도시한 예에서 직선(x_2 및 x_{10})을 기준으로 상기 수학식 3을 적용한 연산 결과에 대

한 예이다.

표 1

Group members		$l_{x_2, x_{10}}^i$							
GM		1	1	1	1	1	1	1	1
m_1		1	1	*	*	1	1	*	*
m_2		*	*	*	1	*	*	*	1
m_3		*	*	1	*	*	*	1	*

Group members		The result of function f_i							
GM		a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
m_1		a_1	a_2	*	*	a_5	a_6	*	*
m_2		*	*	*	a_4	*	*	*	a_8
m_3		*	*	a_3	*	*	*	a_7	*

[0071]

[0072]

상기 표 3을 살펴보면 각 단말에서 연산한 결과는 서로 다르고, 각 단말이 연산한 결과를 합산한 것이 GM이 연산한 결과와 같다는 것을 알 수 있다.

[0074]

과정 5: 각 단말 m_i 는 아래의 표 2와 같이 f_i 의 결과를 XOR 연산한 $result_i$ 를 연산할 수 있다. 그리고 각 단말 m_i 는 자신이 연산한 $result_i$ 를 GM에 전송한다. 한편 GM도 자신이 연산한 f_i 의 결과를 XOR 연산한다.

표 2

Group members		f_i							
GM		a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
m_1		a_1	a_2	*	*	a_5	a_6	*	*
m_2		*	*	*	a_4	*	*	*	a_8
m_3		*	*	a_3	*	*	*	a_7	*

Group members		$result_i$							
GM		$a_1 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_5 \oplus a_6 \oplus a_7 \oplus a_8$							
m_1		$a_1 \oplus a_2 \oplus a_5 \oplus a_6$							
m_2		$a_4 \oplus a_8$							
m_3		$a_3 \oplus a_7$							

[0076]

[0078]

과정 6: GM은 각 단말로부터 $result_i$ 를 수신하고, 아래의 수식 4와 같은 연산을 통해 한 번에 인증을 수행할 수 있다.

수학식 4

$$result_{GM} \oplus result_1 \oplus result_2 \oplus result_3 \stackrel{?}{=} 0$$

result_i를 전달한 모든 단말이 그룹 통신에 참여할 수 있는 주체라면, 수학식 4는 아래의 수학식 5와 같이 표현할 수 있다.

수학식 5

$$(a_1 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_5 \oplus a_6 \oplus a_7 \oplus a_8) \oplus (a_1 \oplus a_2 \oplus a_5 \oplus a_6) \oplus (a_4 \oplus a_8) \oplus (a_3 \oplus a_7) \stackrel{?}{=} 0$$

$a \oplus a = 0$ 이기 때문에 상기 수학식 5의 좌측항의 결과는 0이 나온다. 따라서 GM은 수학식 5의 결과(좌측항이 0인지 여부에 대한 논리 연산값)과 참(true)이 나오면 그룹 통신에 참여를 요청한 모든 단말 m_i가 승인된 적법한 단말이라고 판단한다. GM은 수학식 5의 결과가 거짓(false)이라면 현재 그룹 통신에 참여를 요청한 단말 중 적어도 하나는 그룹 멤버가 아니라고 판단한다.

이하 전술한 그룹 통신 인증 기법을 정리하면서 가능한 실시예에 대해 살펴본다.

도 5는 상보적 인증 키에 기반한 그룹 통신 인증 기법(100)에 대한 순서도의 예이다. 도 5는 원형 좌표를 사용하여 생성 가능한 상보적 코드 자체를 이용한 인증 기법에 대한 예이다. 컴퓨터 장치는 복수의 단말로부터 그룹 통신에 대한 요청을 수신한다(110). 컴퓨터 장치는 통신 요청을 전달한 단말에 대해 각각 임의의 이진 비밀키, 회전 시작 위치 및 회전값을 전달한다(120). 전술한 바와 같이 이진 비밀 키 c_0^i 는 각 단말마다 서로 다른 값(나아가 서로 다른 길이)일 수 있다. 회전 시작 위치는 각 단말이 원형 좌표에 수신한 이진 비밀 키 배치를 시작하는 지점을 의미한다. 회전 시작 위치는 전술한 x_{start}^i 에 해당한다. 회전 시작 위치는 각 단말마다 서로 다른 값이다. 회전값을 모든 단말에 동일한 값이다.

컴퓨터 장치는 기본 코드의 길이와 같은 개수의 원 및 기본 코드 길이와 같은 개수의 축을 갖는 제1 원형 좌표에 기본 코드를 기준으로 코드를 배치한다(130). 기본 코드는 복수의 단말 각각에 대한 이진 비밀 키를 연결(concatenation)한 제1 부분 코드와 상기 제1 부분 코드에 상보적인 제2 부분 코드를 연결한 코드에 해당한다. 기본 코드는 도 3에서 설명한 u_0 에 해당한다. 컴퓨터 장치가 기본 코드를 기준으로 제1 원형 좌표에 코드를 배치하는 과정은 전술한 도 3 및 그룹 인증 과정에서 설명한 바 있다.

복수의 단말은 각각 수신한 이진 비밀 키를 기준으로 제2 원형 좌표에 코드를 배치한다(140). 제2 원형 좌표는 제1 원형 좌표와 동일한 형태를 갖는다. 복수의 단말이 자신이 수신한 이진 비밀 키를 기준으로 제2 원형 좌표에 코드를 배치하는 과정은 도 4 및 그룹 인증 과정에서 설명한 바와 같다.

컴퓨터 장치는 제1 원형 좌표에서 두 개의 축이 이루는 하나의 직선(제1 직선)상에 배치된 일련의 이진 코드인 제1 이진 코드를 추출한다(150). 또한 복수의 단말도 각각 제2 원형 좌표에서 제1 직선에 대응하는 위치에 있는 직선에 배치된 일련의 이진 코드인 제2 이진 코드를 추출한다. 컴퓨터 장치는 복수의 단말로부터 각각 추출한 제2 이진 코드를 수신한다(160). 이때 컴퓨터 장치는 제1 원형 좌표에서 하나의 직선에 배치된 코드를 추출할 수도 있고, 복수의 직선에 배치된 코드를 모두 추출할 수도 있다. 복수의 직선에 배치된 코드를 이용하는 경우 각 단말로 대응되는 복수의 직선에 배치된 코드를 추출해야 한다.

- [0091] 컴퓨터 장치는 제1 이진 코드와 제2 이진 코드를 비교하여 인증을 수행한다(170). 컴퓨터 장치는 제1 이진 코드와 모든 복수의 단말로부터 수신한 제2 이진 코드를 XOR 연산하여 인증을 수행할 수 있다. 컴퓨터 장치는 XOR 연산 결과 모든 비트의 자리수에서 1이 나오면 복수의 단말은 모두 그룹 통신에 참여 가능한 단말이라고 인증할 수 있다. 컴퓨터 장치가 원형 좌표에서 복수의 직선에서 추출한 코드를 이용하는 경우 복수의 직선에서 추출한 코드 각각에 대해 XOR 연산을 하거나, 복수의 직선에서 추출한 코드를 일정한 순서로 연결한 전체 코드에 대해 XOR 연산을 수행할 수 있다.
- [0093] 도 6은 상보적 인증 키에 기반한 그룹 통신 인증 기법(200)에 대한 순서도의 다른 예이다. 도 6은 기준 함수를 추가로 이용한 예이다. 컴퓨터 장치는 복수의 단말로부터 그룹 통신에 대한 요청을 수신한다(210). 컴퓨터 장치는 통신 요청을 전달한 단말에 대해 각각 임의의 이진 비밀키, 회전 시작 위치, 회전값 및 기준 함수를 전달한다(120). 전송한 바와 같이 이진 비밀 키 c_0^i 는 각 단말마다 서로 다른 값(나아가 서로 다른 길이)일 수 있다. 회전 시작 위치는 각 단말이 원형 좌표에 수신한 이진 비밀 키 배치를 시작하는 지점을 의미한다. 회전 시작 위치는 전송한 x_{start}^i 에 해당한다. 회전 시작 위치는 각 단말마다 서로 다른 값이다. 회전값을 모든 단말에 동일한 값이다. 기준 함수는 전송한 f 에 해당한다. 한편 컴퓨터 장치는 수학적 2에서 설명한 일정한 임의의 수 및 타임스탬프도 각 단말에 전달할 수 있다. 컴퓨터 장치는 이진 비밀 키를 제외한 나머지 정보는 모두 이진 비밀 키를 사용하여 암호화한 후 전달할 수 있다.
- [0094] 컴퓨터 장치는 기본 코드의 길이와 같은 개수의 원 및 기본 코드 길이와 같은 개수의 축을 갖는 제1 원형 좌표에 기본 코드를 기준으로 코드를 배치한다(230). 기본 코드는 복수의 단말 각각에 대한 이진 비밀 키를 연결(concatenation)한 제1 부분 코드와 상기 제1 부분 코드에 상보적인 제2 부분 코드를 연결한 코드에 해당한다.
- [0095] 복수의 단말은 각각 수신한 이진 비밀 키를 기준으로 제2 원형 좌표에 코드를 배치한다(240). 제2 원형 좌표는 제1 원형 좌표와 동일한 형태를 갖는다. 복수의 단말이 자신이 수신한 이진 비밀 키를 기준으로 제2 원형 좌표에 코드를 배치하는 과정은 도 4 및 그룹 인증 과정에서 설명한 바와 같다.
- [0096] 컴퓨터 장치는 제1 원형 좌표에서 두 개의 축이 이루는 하나의 직선(제1 직선)상에 배치된 일련의 이진 코드인 제1 이진 코드를 추출하고, 제1 이진 코드를 기준 함수에 적용하여 제1 값을 생성한다(150). 또한 복수의 단말도 각각 제2 원형 좌표에서 제1 직선에 대응하는 위치에 있는 직선에 배치된 일련의 이진 코드인 제2 이진 코드를 추출하고, 제2 이진 코드를 기준 함수에 적용하여 제2 값을 생성한다. 컴퓨터 장치는 복수의 단말로부터 각각 추출한 제2 값을 수신한다(160). 이때 컴퓨터 장치는 제1 원형 좌표에서 하나의 직선에 배치된 코드를 추출할 수도 있고, 복수의 직선에 배치된 코드를 모두 추출하여 각각 기준 함수를 적용하거나, 복수의 직선에 배치된 코드를 연결하여 기준 함수에 적용할 수도 있다. 각 단말도 컴퓨터 장치와 대응되게 복수의 코드를 기준 함수에 적용해야 한다. 나아가 컴퓨터 장치 및 단말은 각각 수학적 3과 같이 단말의 ID, 축의 식별자, r , TS 및 k 값 중 적어도 하나를 제1 코드 및 제2 코드에 연결하여 기준 함수에 적용할 수도 있다.
- [0097] 컴퓨터 장치는 제1 값과 제2 값을 비교하여 인증을 수행한다(170). 컴퓨터 장치는 제1 값과 모든 복수의 단말로부터 수신한 제2 값을 XOR 연산하여 인증을 수행할 수 있다. 컴퓨터 장치는 XOR 연산 결과 모든 비트의 자리수에서 1이 나오면 복수의 단말은 모두 그룹 통신에 참여 가능한 단말이라고 인증할 수 있다.
- [0099] 도 7은 상보적 인증 키에 기반한 그룹 통신 인증 기법이 수행되는 네트워크 시스템(300)에 대한 예이다. 도 7에서 310A 및 310B는 전송한 컴퓨터 장치(GM)이다. 310A는 통신에 참여하는 하나의 단말 또는 별도의 단말이 GM의 기능을 수행하는 예이고, 310B는 별도의 서버가 GM의 기능을 수행하는 예이다. 도 7에서 그룹 통신에 참여하는 단말은 320A, 320B 및 320C이다.
- [0100] 컴퓨터 장치(310A 또는 310B)는 이진 비밀키, 회전 시작 위치 및 회전값을 각 단말에 전달한다(①). 각 단말(320A, 320B 및 320C)은 원형 좌표를 이용하여 제2 이진 코드 또는 제2 값을 생성한다(②). 컴퓨터 장치(310A 또는 310B)는 단말로부터 제2 이진 코드 또는 제2 값을 수신한다(③). 컴퓨터 장치(310A 또는 310B)는 자신이 원형 좌표를 이용하여 제1 이진 코드 또는 제1 값을 생성한다(④). 마지막으로 컴퓨터 장치(310A 또는 310B)는 제1 이진 코드와 제2 이진 코드를 일정하게 비교하거나, 제1 값과 제2 값을 일정하게 비교하여 단말에 대한 인증을 수행한다(④). 도 7에 도시한 바와 달리 제1 이진코드/제1 값을 생성하는 과정과 제2 이진 코드/제2 값을

생성하는 과정은 순서에 관계가 없다.

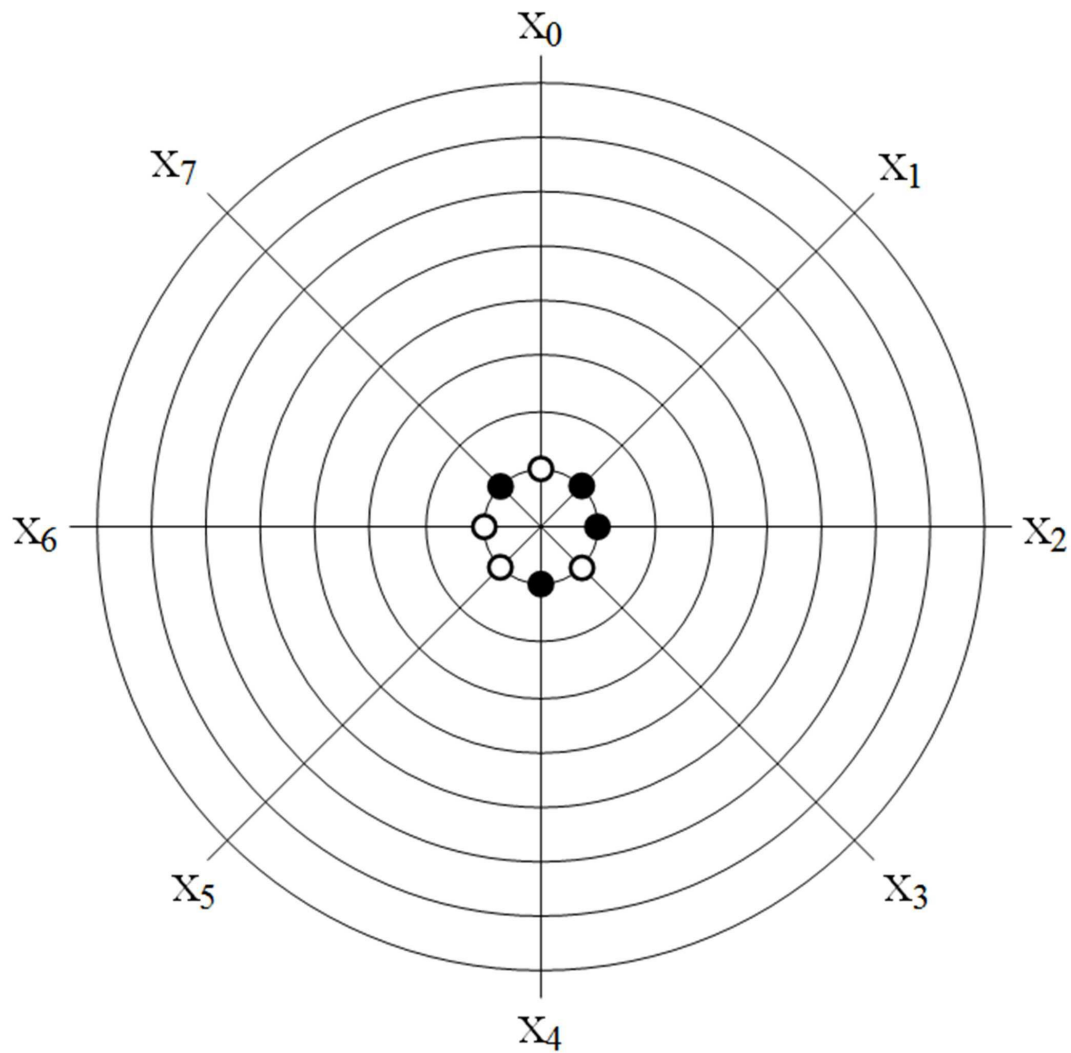
- [0102] 본 실시예 및 본 명세서에 첨부된 도면은 전술한 기술에 포함되는 기술적 사상의 일부를 명확하게 나타내고 있는 것에 불과하며, 전술한 기술의 명세서 및 도면에 포함된 기술적 사상의 범위 내에서 당업자가 용이하게 유추할 수 있는 변형 예와 구체적인 실시예는 모두 전술한 기술의 권리범위에 포함되는 것이 자명하다고 할 것이다.

부호의 설명

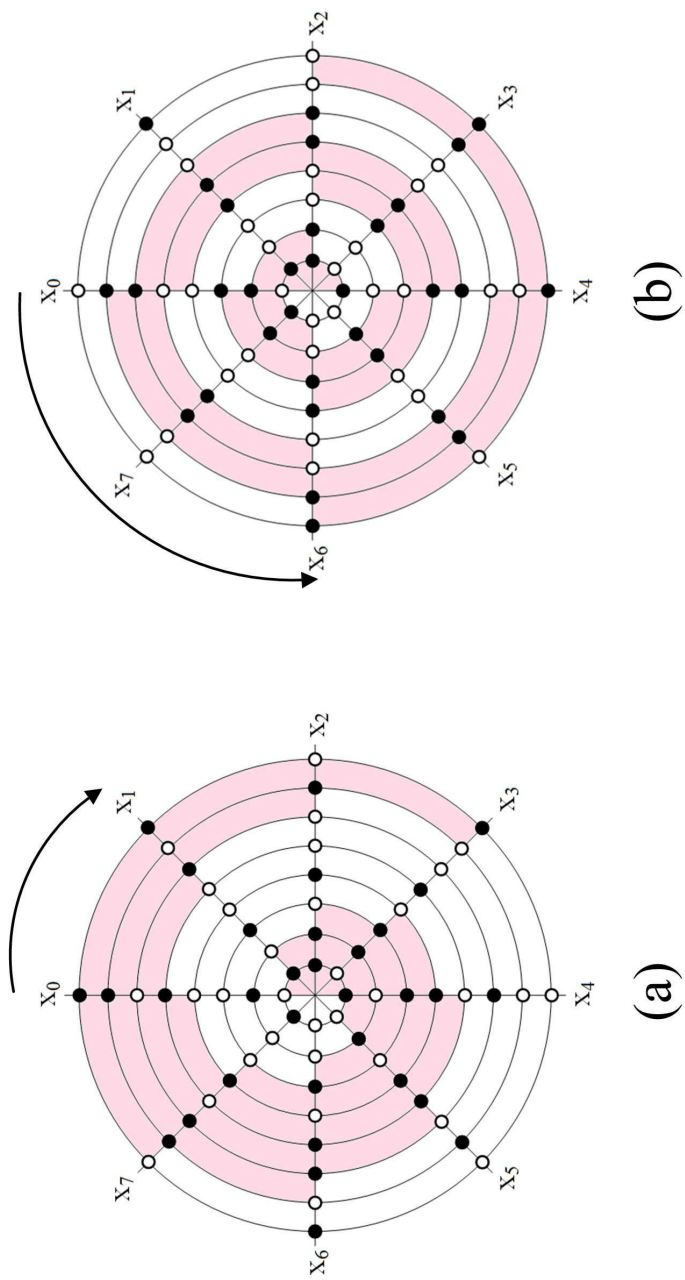
- [0103] 310A, 310A : 컴퓨터 장치
320A, 320B, 320C : 단말

도면

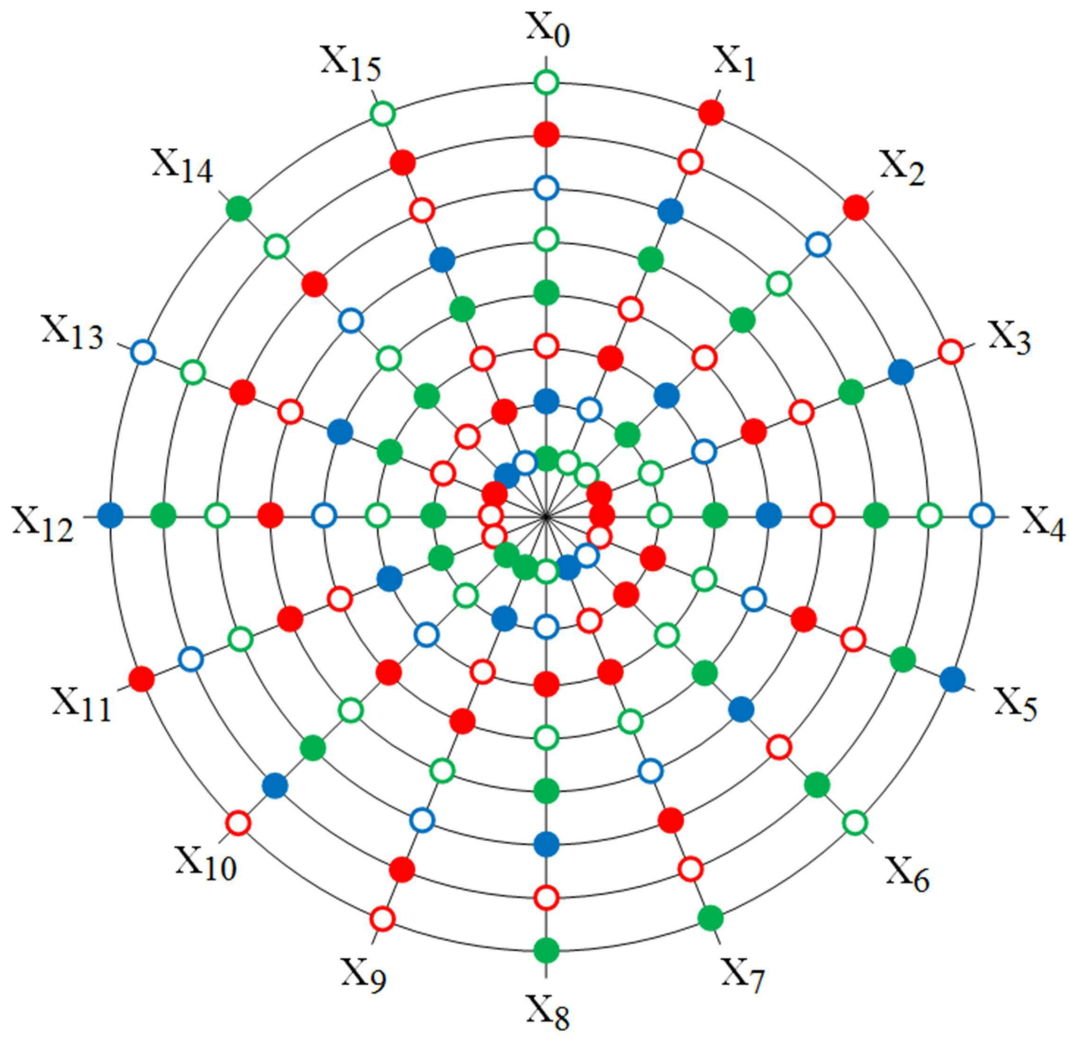
도면1



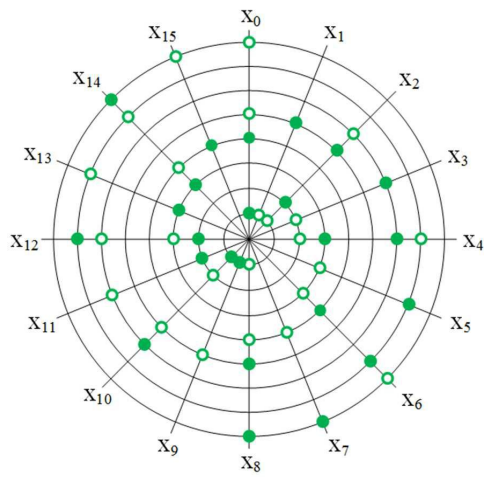
도면2



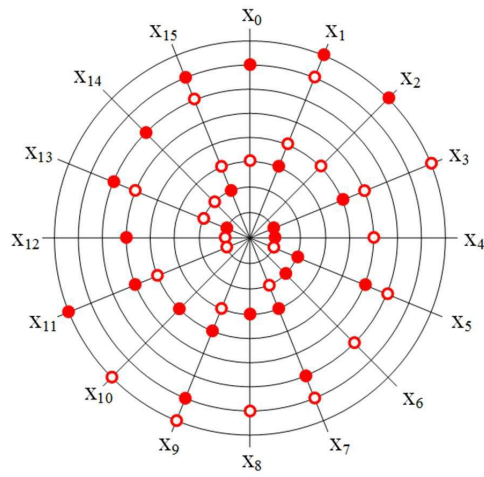
도면3



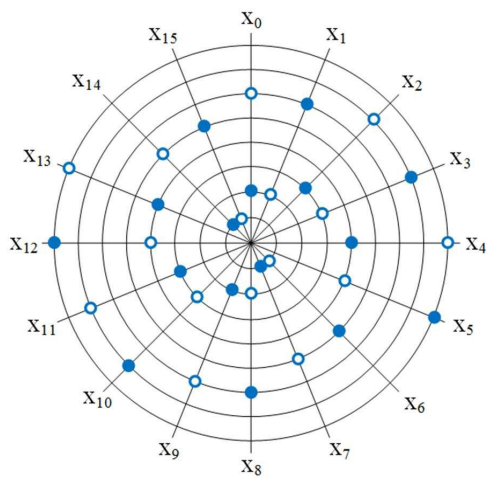
도면4



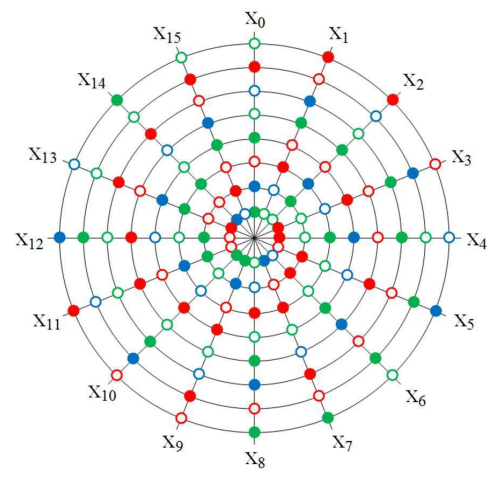
(a)



(b)



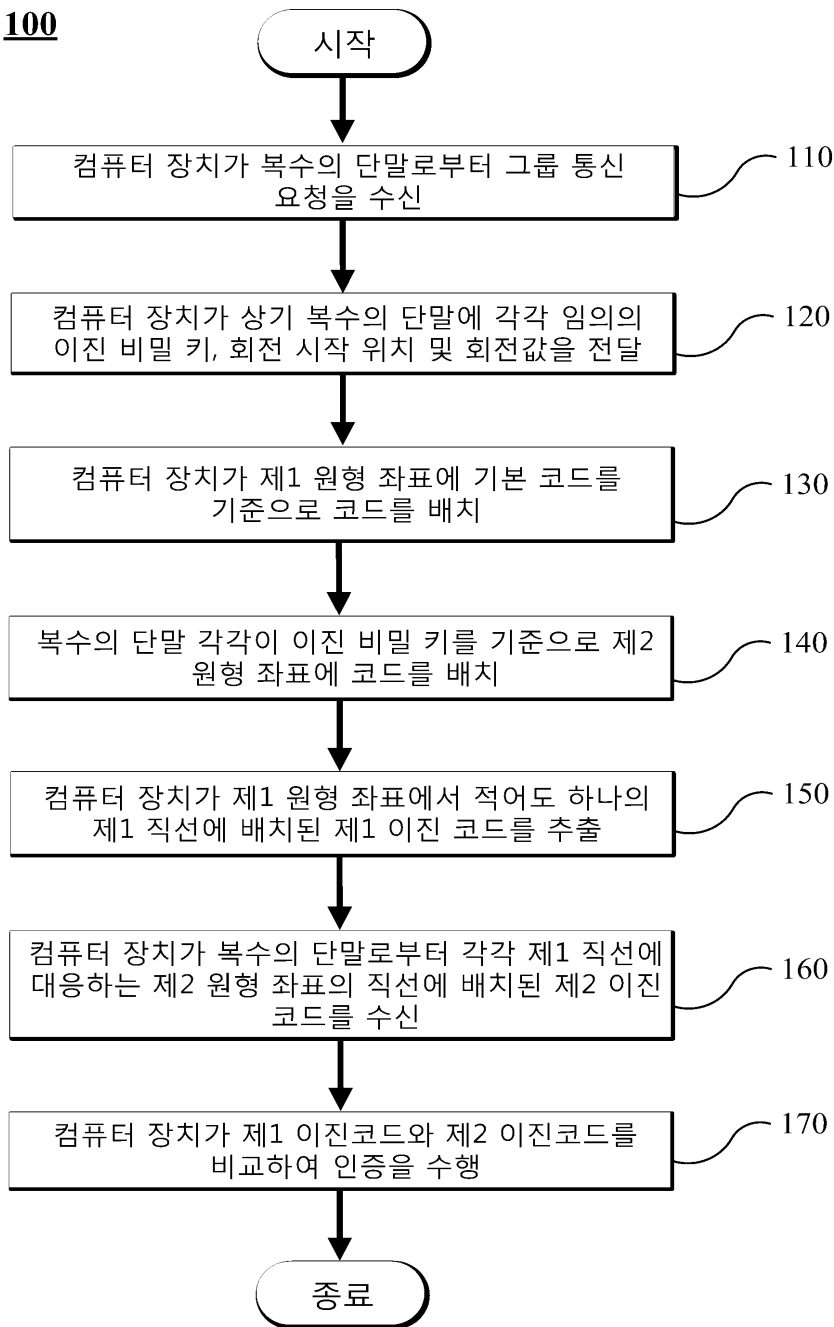
(c)



(d)

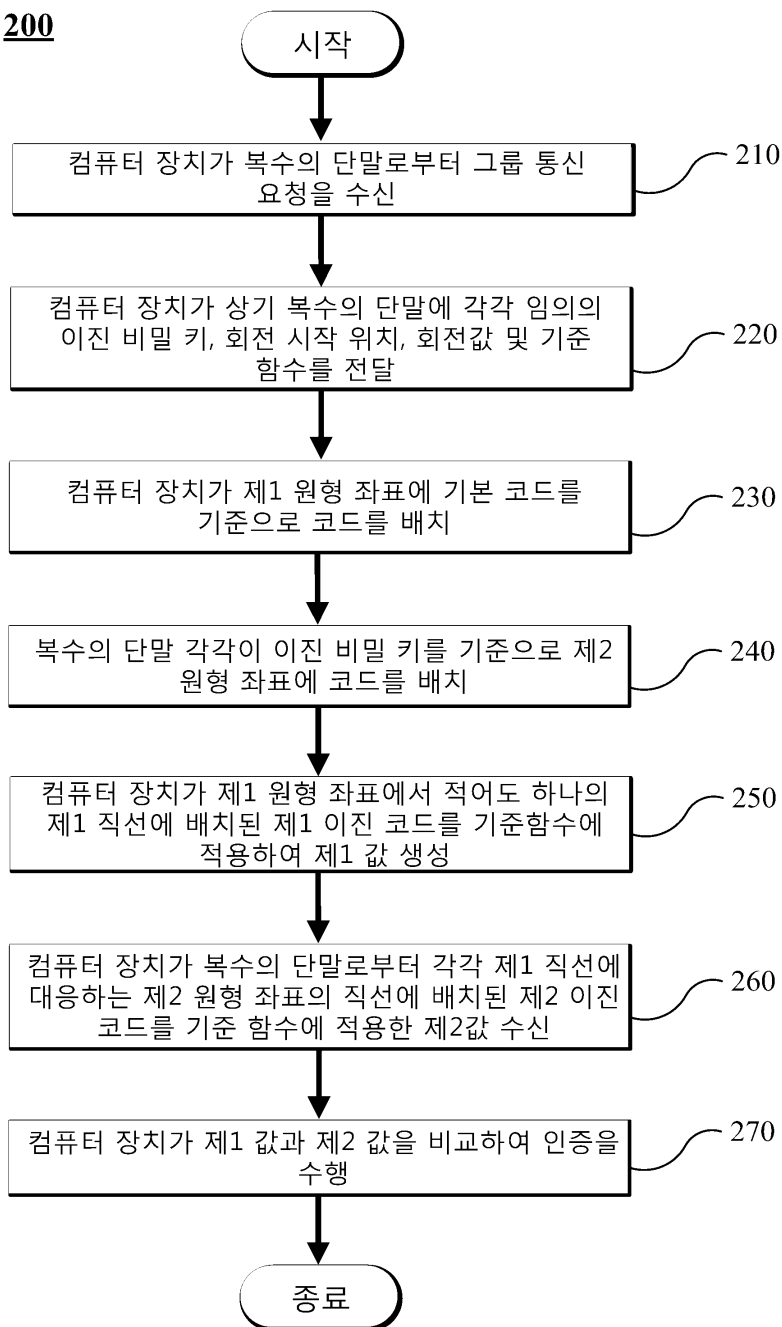
도면5

100



도면6

200



도면7

