



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2013-0053839
(43) 공개일자 2013년05월24일

(51) 국제특허분류(Int. Cl.)

H04N 7/167 (2011.01)

(21) 출원번호 10-2011-0119516

(22) 출원일자 2011년11월16일

심사청구일자 없음

기술이전 희망 : 기술양도, 실시권허여, 기술지도

(71) 출원인

한국전자통신연구원

대전광역시 유성구 가정로 218 (가정동)

고려대학교 산학협력단

서울 성북구 안암동5가 1

(72) 발명자

장구영

대전광역시 유성구 관평동 대덕테크노밸리아파트
407-1002

조남수

대전광역시 유성구 온천북로33번길 22-9, 정다운
집 402호 (봉명동)

(뒷면에 계속)

(74) 대리인

제일특허법인

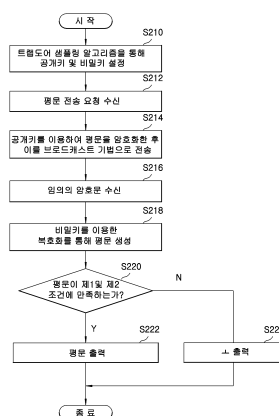
전체 청구항 수 : 총 1 항

(54) 발명의 명칭 래티스 기반의 브로드캐스트 방법

(57) 요약

본 발명은 의미론적 안전성과 복호화 일관성을 만족할 수 있는 래티스 기반의 브로드캐스트 방법에 관한 것이다. 이를 위하여 본 발명의 실시 예에 따른 래티스 기반의 브로드캐스트 방법은 시큐리티 파라미터(n)와 소정 상수 값(q 는 2 보다 큰 소수)을 입력받아 트랩도어 샘플링 방법을 적용하여 행렬 공개키($A_i \in \mathbb{Z}_q^{m \times n}$)와 m ($m \geq 8n \log q$)차원 풀-랭크 정수 래티스의 특정한 형태의 트랩도어($T_i \in \mathbb{Z}^{m \times m}$)인 비밀키를 생성하는 단계와, 행렬 공개키의 집합과 평문을 입력받아 암호문을 생성한 후 암호문을 브로드캐스트 방법으로 송신하는 단계와, 행렬 공개키를 기반으로 생성된 임의의 암호문이 외부로부터 수신되면, 행렬 공개키에 대한 m 차원 풀-랭크 정수 래티스의 특정한 형태의 트랩도어를 얻기 위한 트랩도어 확장 알고리즘을 수행하며, 트랩도어 확장 알고리즘을 수행한 결과를 기반으로 임의의 암호문에 대한 평문을 생성하는 단계를 포함할 수 있다.

대표도 - 도2



(72) 발명자

노건태

서울특별시 강남구 개포2동 주공아파트 707동 1304호

정익래

서울특별시 성동구 성수동1가 709번지 성수2차 대우아파트 101동 1704호

특허청구의 범위

청구항 1

시큐리티 파라미터(n)와 소정 상수 값(q 는 2보다 큰 소수)을 입력받아 트랩도어 샘플링 방법을 적용하여 행렬 공개키($A_2 \in \mathbb{Z}_q^{m \times n}$)와 m ($m \geq 8n \log q$)차원 폴-랭크 정수 래티스의 특정한 형태의 트랩도어($T_j \in \mathbb{Z}^{m \times m}$)인 비밀키를 생성하는 단계와,

상기 행렬 공개키의 집합과 평문을 입력받아 암호문을 생성한 후 상기 암호문을 브로드캐스트 방법으로 송신하는 단계와,

상기 행렬 공개키를 기반으로 생성된 임의의 암호문이 외부로부터 수신되면, 상기 행렬 공개키에 대한 m 차원 폴-랭크 정수 래티스의 특정한 형태의 트랩도어를 얻기 위한 트랩도어 확장 알고리즘을 수행하며, 상기 트랩도어 확장 알고리즘을 수행한 결과를 기반으로 상기 임의의 암호문에 대한 평문을 생성하는 단계를 포함하는 래티스 기반의 브로드캐스트 방법.

명세서

기술분야

[0001] 본 발명은 브로드캐스트 방법에 관한 것으로, 더욱 상세하게는 상기와 같은 문제점을 해결하기 위해 안출된 것으로서, 본 발명의 목적은 의미론적 안전성과 복호화 일관성을 만족할 수 있는 래티스 기반의 브로드캐스트 방법에 관한 것이다.

배경기술

[0002] 일반적으로, 브로드캐스트 기법은 다수의 정당한 사용자가 동시에 동일한 정보를 수신하는 환경에서 유용하게 사용될 수 있으며, 가장 대표적인 예로 케이블 TV 관련 시장이 존재한다. 케이블 TV 채널 제공자는 정당하게 비용을 지불한 사용자에게만 콘텐츠를 제공해야 하며, 그렇지 않은 사용자는 콘텐츠를 볼 수 없어야 한다. 이러한 기능을 제공하기에 가장 적합한 방법이 브로드캐스트 기법을 사용하는 것이다. 1997년, Eric R. Verheul과 Henk C.A. van Tilborg는 랜덤 오라클(random oracle) 모델에서 증명 가능한 브로드캐스트 기법을 제안하였다. 그 이후, Craig Gentry와 Brent Waters는 공모에 완전히 안전한 브로드캐스트 기법을 제안하였으며, 공격할 대상을 제외한 모든 사용자들을 악의적으로 포획할 수 있는 공격자에도 안전함을 증명하였다. 그리고, Ik Rae Jeong 등은 표준 모델에서 안전한 브로드캐스트 기법을 제안하였고, 이후에 Shuhua Wu 등은 이 기법이 기반한 안전성 모델이 약함을 지적하였다.

[0003] 브로드캐스트 기법은 암호화 기법이 기본적으로 만족해야 하는 안전성(의미론적 안전성, semantic security)을 만족해야 하며, 추가적으로 정당한 모든 데이터 수신자들이 동시에 동일한 데이터를 수신하였는지에 대한 안전성(복호화 일관성, decryption consistency)을 만족해야 한다.

[0004] 하지만, 종래에 제안되었던 브로드캐스트 기법들은 모두 복호화 일관성을 온전히 만족하지 못한다. 다시 말해서, 악의적인 공격자에 의해 서로 다른 정당한 데이터 수신자가 동일한 데이터를 얻지 못하는 경우가 발생한다. 즉, 의미론적 안전성과 복호화 일관성을 동시에 온전히 만족하는 브로드캐스트 기법은 지금까지 제안되지 않았다.

발명의 내용

해결하려는 과제

[0005] 상기와 같은 문제점을 해결하기 위해 안출된 것으로서, 본 발명의 목적은 의미론적 안전성과 복호화 일관성을

만족할 수 있는 래티스 기반의 브로드캐스트 방법을 제공하는데 있다.

[0006] 본 발명의 목적은 이상에서 언급한 목적으로 제한되지 않으며, 언급되지 않은 또 다른 목적들은 아래의 기재로부터 본 발명이 속하는 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0007] 본 발명의 일 측면에 따르면, 본 발명의 실시 예에 따른 래티스 기반의 브로드캐스트 방법은 시큐리티 파라미터 (n) 와 소정 상수 값(q 는 2보다 큰 소수)을 입력받아 트랩도어 샘플링 방법을 적용하여 행렬 공개키 $(A_i \in \mathbb{Z}_q^{m \times n})$ 와 m ($m \geq 8n \log q$)차원 풀-랭크 정수 래티스의 특정한 형태의 트랩도어($T_i \in \mathbb{Z}^{m \times m}$)인 비밀키를 생성하는 단계와, 상기 행렬 공개키의 집합과 평문을 입력받아 암호문을 생성한 후 상기 암호문을 브로드캐스트 방법으로 송신하는 단계와, 상기 행렬 공개키를 기반으로 생성된 임의의 암호문이 외부로부터 수신되면, 상기 행렬 공개키에 대한 m 차원 풀-랭크 정수 래티스의 특정한 형태의 트랩도어를 얻기 위한 트랩도어 확장 알고리즘을 수행하며, 상기 트랩도어 확장 알고리즘을 수행한 결과를 기반으로 상기 임의의 암호문에 대한 평문을 생성하는 단계를 포함할 수 있다.

[0008] 본 발명의 실시 예에 따른 래티스 기반의 브로드캐스트 방법에서 상기 비밀키를 생성하는 단계는, 시큐리티 파라미터 (n) 와 소정 상수 값($q > 1$)을 입력받아 트랩도어 샘플링 방법을 적용하여 행렬 공개키($A_i \in \mathbb{Z}_q^{m \times n}$)와 m ($m \geq 8n \log q$)차원 풀-랭크 정수 래티스의 특정한 형태의 트랩도어($T_i \in \mathbb{Z}^{m \times m}$)인 비밀키를 획득하며, 상기 행렬 공개키와 트랩도어는, $T_i A_i = 0 \pmod{q}$, $T_i \in \mathbb{Z}^{m \times m}$ 는 $\Lambda^\perp(A_i)$ 의 기저이며, 역행렬이 존재한다. $T_i \in \mathbb{Z}^{m \times m}$ 의 모든 행들의 유클리디안 거리는 특정한 마운드 내에 존재하는 것을 특징으로 한다.

[0009] 본 발명의 실시 예에 따른 래티스 기반의 브로드캐스트 방법에서 상기 암호문을 브로드캐스트 방법으로 송신하는 단계는, 균일하고 랜덤한 벡터($s \in \mathbb{Z}_q^n$)와 가우시안 에러 벡터($x \in \Psi_s(q)^m$)를 랜덤하게 선택하고, 행렬 $(A = A_1 \parallel \dots \parallel A_i \in \mathbb{Z}_q^{m \times n})$ 을 구성한 후 상기 암호문(C)을 수학적식($C = As + px + \mu \pmod{q}$)을 이용하여 생성하는 것을 특징으로 한다.

[0010] 본 발명의 실시 예에 따른 래티스 기반의 브로드캐스트 방법에서 상기 평문을 생성하는 단계는, 상기 임의의 암호문이 수신됨에 따라 상기 행렬을 구성한 후 상기 구성된 행렬을 이용한 트랩도어 확장 알고리즘 $TE(T_i, A)$ 를 수행하여 $\Lambda^\perp(A)$ 의 트랩도어 $T \in \mathbb{Z}^{m \times m}$ 를 추출하는 단계와, 상기 추출된 트랩도어를 수학적식($\mu = T^{-1}(TC \pmod{q}) \pmod{p}$)에 적용하여 평문을 계산하는 단계와, 상기 평문을 수학적식($T^{-1}(TC \pmod{q}) = T^{-1}(T(px + \mu)) \pmod{q} = (px + \mu)$)에 적용하여 상기 $(px + \mu)$ 의 모든 원소들이 q 보다 작은지를 검사하는 단계와, 상기 모든 원소들이 q 보다 작은 경우 수학적식($C = As + px + \mu \pmod{q}$)을 만족하는 상기 s 를 계산할 수 있는지를 검사하는 단계와, 상기 검사 결과, 상기 s 를 계산할 수 있을 경우 상기 평문을 출력하는 단계를 포함하는 것을 특징으로 한다.

[0011]

발명의 효과

[0012] 본 발명은 래티스 기반으로 각 참여자의 공개키와 비밀키를 생성하여 설정한 후 각 참여자의 공개키를 기반으로 평문을 암호화하여 브로드캐스트 기법으로 전송하고, 암호화된 평문을 복호화시킴으로써, 의미론적 안정성과 복호화 일관성을 동시에 만족시킬 수 있는 브로드캐스트 기법을 제공할 수 있다.

도면의 간단한 설명

- [0013] 도 1은 본 발명의 실시 예에 따른 브로드캐스팅 방법이 적용되는 네트워크 구성도,
도 2는 본 발명의 실시 예에 따라 래티스 기반의 브로드캐스트 방법을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

- [0014] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시 예들을 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 개시되는 실시 예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시 예들은 본 발명의 개시가 완전하도록 하고, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다. 명세서 전체에 걸쳐 동일 참조 부호는 동일 구성 요소를 지칭한다.
- [0015] 이하, 도면을 참조하여 본 발명의 실시 예에 따른 래티스 기반의 브로드캐스팅 데이터 전송 방법에 대해 설명한다.
- [0016] 도 1은 본 발명의 실시 예에 따른 브로드캐스팅 방법이 적용되는 네트워크 구성도로서, 각기 다른 공개키와 비밀키를 갖는 다수의 참여자로 구성된 참여자 그룹(100)과, 참여자 그룹(100) 내 각 참여자의 공개키를 이용하여 데이터를 암호화한 후 브로드캐스팅 방법으로 전송하는 전송 장치(200)로 구성될 수 있다. 여기에서 전송 장치(200)는 다수의 참여자 그룹(100) 중 어느 하나가 될 수 있다.
- [0017] 본 발명의 실시 예에 대한 설명에 앞서, 본 발명의 실시 예에서 사용될 표기법에 대해 정의하면 아래와 같다.
- [0018] 먼저 두 행렬 $A \in \mathbb{Z}^{n \times n}$ 와 $B \in \mathbb{Z}^{(m+n) \times n}$ 를 연결하는 것을 $A || B \in \mathbb{Z}^{(m+n) \times n}$ 로 정의하며, 모듈식 연산 $x \pmod{q}$ 는 정수 x 를 $\left[-\frac{q}{2}, \frac{q}{2}\right]$ 로 매핑한다.
- [0019] 본 발명의 실시 예 적용되는 래티스는 m 차원 풀-랭크(full-rank) 정수 래티스 $\Lambda \subseteq \mathbb{Z}^m$ 의 특정한 형태를 사용하며, 이것의 정의는 아래의 수학식 1과 같다.

수학식 1

$$\Lambda = L(B) = \left\{ cB = \sum_{i=1}^m b_i c_i : c \in \mathbb{Z}^m \right\}$$

[0020]

- [0021] 상기의 수학식 1에서 $B = \{b_1, \dots, b_m\} \subset \mathbb{Z}^m$ 는 m 개의 선형 독립 기저 벡터들이다.

- [0022] 또한, 본 발명의 실시 예에서는 m 차원 풀-랭크 정수 래티스의 특정한 형태인 $\Lambda^\perp(A) \subseteq \mathbb{Z}^m$ 를 사용하며, 이것의 정의는 아래의 수학식 2와 같다.

수학식 2

$$\Lambda^\perp(A) = \{x \in \mathbb{Z}^m : xA = 0 \pmod{q}\}$$

[0023]

- [0024] 상기의 수학식 2에서 $A \in \mathbb{Z}_q^{m \times n}$ 는 균일하고 랜덤한 행렬이며, $0 \in \mathbb{Z}_q^n$ 은 영벡터이며, q 는 2 보다 큰 소수이다.
- [0025] 상기와 같은 표기법을 토대로 참여자 그룹(100)과 전송 장치(200)가 브로드캐스트 기법을 이용하여 평문을 전송하는 과정에 대해 도 2를 참조하여 설명한다.
- [0026] 도 2는 본 발명의 실시 예에 따라 래티스 기반의 브로드캐스트 방법을 설명하기 위한 흐름도이다.
- [0027] 본 발명의 실시 예에 따른 브로드캐스트 기법에서는 트랩도어 샘플링 알고리즘과 트랩도어 확장 알고리즘이 사용될 수 있다.
- [0028] 먼저, 도 2에 도시된 바와 같이, 각 참여자 그룹(100)인 $P_i (i \in [1, l])$ 는 $Key(1^*)$ 알고리즘을 통해 공개키($pk_i = A_i$)와 비밀키($sk_i = T_i$)를 생성한 후 이를 설정(S210)할 수 있다. $Key(1^*)$ 알고리즘은 균일하고 랜덤한 행렬 공개키($A_i \in \mathbb{Z}_q^{m \times n}$)와 비밀키($\Lambda^\perp(A_i)$ 의 트랩도어 $T_i \in \mathbb{Z}^{m \times m}$)를 얻기 위해 트랩도어 샘플링 알고리즘 $TS(1^*, 1^m, q)$ 를 수행할 수 있다. 여기에서, l 은 그룹의 크기이다.
- [0029] 공개키와 비밀키 생성을 위해 수행하는 트랩도어 샘플링 알고리즘 $TS(1^*, 1^m, q)$ 는 아래와 같다.
- [0030] 트랩도어 샘플링 알고리즘은 시큐리티 파라미터 n 및 $m \geq 8n \log q$, 정수 $q > 1$ 을 입력으로 받아서 균일하고 랜덤한 행렬 $A_i \in \mathbb{Z}_q^{m \times n}$ 와 이것의 트랩도어 $T_i \in \mathbb{Z}^{m \times m}$ 를 출력한다. 여기에서, $A_i \in \mathbb{Z}_q^{m \times n}$ 와 $T_i \in \mathbb{Z}^{m \times m}$ 는 아래와 같은 성질을 가질 수 있다.
- [0031] 먼저, $T_i A_i = 0 \pmod{q}$, $T_i \in \mathbb{Z}^{m \times m}$ 는 $\Lambda^\perp(A_i)$ 의 기저이며, 역행렬이 존재한다. $T_i \in \mathbb{Z}^{m \times m}$ 의 모든 행들의 유클리디안 거리는 특정한 바운드 내에 존재한다.
- [0032] 각 참여자 그룹(100)인 P_i 는 공개키 $pk_i = A_i$ 와 비밀키 $sk_i = T_i$ 를 설정한다.
- [0033] 그런 다음, 참여자 그룹(100) 내 하나 또는 그 이상의 참여자(P_i)가 자신의 공개키(A_i)를 이용하여 임의의 참여자에게 데이터(평문) 전송을 요청(S212)하면, 임의의 참여자는 자신의 전송 장치(200)를 이용하여 데이터(평문)를 전송할 수 있다. 즉, 전송 장치(200)는 평문 전송을 요청한 참여자의 공개키(A_i)를 이용하여 평문(μ)에 대한 암호문(C)을 생성한 후 이를 브로드캐스트 기법으로 전송(S214)할 수 있다.
- [0034] 여기에서, 암호문(C)은 $Enc(PK, \mu)$ 알고리즘을 이용하여 생성될 수 있는데, $Enc(PK, \mu)$ 알고리즘은 랜덤한 벡터 $s \in \mathbb{Z}_q^n$ 와 가우시안 에러 벡터 $x \in \Psi_{\rho}(q)^m$ 를 랜덤하게 선택한 후 행렬 $A = A_1 \parallel \dots \parallel A_i \in \mathbb{Z}_q^{l \times n}$ 를 구성하고, 암호문 $C = As + px + \mu \pmod{q}$ 를 생성할 수 있다. 여기에서, $\Psi_{\rho}(q)$ 는 $\mathbb{Z}_q$ 상에서의 가우시안 에러 분포이며, PK 는 공개키의 집합($\{pk_1, \dots, pk_l\}$)을 의미한다.
- [0035] 이와 같은 과정을 통해 생성된 암호문(C)은 전송 장치(200)를 이용하여 다수의 참여자 그룹(100)에 브로드캐스트 기법으로 전송될 수 있다.
- [0036] 한편, 임의의 암호문(C)을 수신(S216)하면 암호문(C)을 수신한 참여자 그룹(100)인 P_i 는 자신의 비밀키(sk_i)를 이용하여 복호화를 수행(S218)함으로써, 평문을 추출할 수 있다. 다시 말해서, $Dec(sk_i, C)$ 알고리즘을 이용하여 평문(μ)을 추출할 수 있다.

[0037] $Dec(sk_i, C)$ 알고리즘은 먼저 행렬 $A = A_1 \parallel \dots \parallel A_i \in Z_q^{l \times n}$ 를 구성하고, $\Lambda^\perp(A)$ 의 트랩도어 $T \in Z^{l \times l}$ 를 얻기 위해 트랩도어 확장 알고리즘 $TE(T_i, A)$ 를 수행한 다음, 아래의 수학적 3을 통해 평문(μ)을 계산한다.

수학적 3

[0038] $\mu = T^{-1} (TC \pmod{q}) \pmod{p}$

[0039] 본 발명의 실시 예에 따른 $Dec(sk_i, C)$ 알고리즘에 적용되는 트랩도어 확장 알고리즘 $TE(T_i, A)$ 에 대해 설명하면 아래와 같다.

[0040] 한편, 본 발명의 실시 예에서 이용하는 트랩도어 확장 알고리즘 $TE(T_i, A = A_1 \parallel \dots \parallel A_i)$ 는 아래와 같다. 여기서는 참여자 P_i 인 경우에만 대해서만 설명한다. P_i 이 아닌 다른 참여자들도 알고리즘의 특성상 유사하게 $\Lambda^\perp(A)$ 의 트랩도어 $T \in Z^{l \times l}$ 를 생성할 수 있다.

[0041] 참여자 P_i 은 $\Lambda^\perp(A_i)$ 의 트랩도어 $T_i \in Z^{m \times m}$ 과 행렬 $A = A_1 \parallel \dots \parallel A_i \in Z_q^{l \times n}$ 를 입력으로 받아서 $\Lambda^\perp(A = A_1 \parallel \dots \parallel A_i)$ 의 트랩도어 $T = \begin{pmatrix} T_i & 0 \\ W & I \end{pmatrix} \in Z^{l \times l}$ 을 출력한다. 여기에서, $0 \in Z^{m \times (l-1)m}$ 은 영벡터이고, $I \in Z^{(l-1)m \times (l-1)m}$ 는 항등 행렬이고, $W \in Z^{(l-1)m \times m}$ 는 $WA = -\bar{A} \pmod{q}$, $\bar{A} = A_1 \parallel \dots \parallel A_i$ 을 만족하는 행렬이다.

[0042] 또한, 트랩도어 확장 알고리즘은 아래와 같은 성질을 갖는다. $TA = 0 \pmod{q}$. T 는 $\Lambda^\perp(A)$ 의 기저이며, 역행렬이 존재한다. T 는 A 의 행들이 랜덤하게 치환되더라도 쉽게 계산될 수 있다. 이러한 특성 때문에 본 알고리즘은 참여자 P_i 의 경우에만 국한되지 않는다. T 의 모든 행들의 유클리디안 거리는 특정한 바운드 내에 존재한다.

[0043] 상기와 과정을 통해 생성된 평문(μ)이 두 가지의 조건이 맞는지 검사한다.

[0044] 먼저, $T^{-1} (TC \pmod{q}) = T^{-1} (T(px + \mu)) \pmod{q} = (px + \mu)$ 를 계산하고 $(px + \mu)$ 의 모든 원소들이 q 보다 작은지를 검사(제 1 조건)함과 더불어 $C = As + px + \mu \pmod{q}$ 를 만족하는 s 를 계산할 수 있는지를 검사(제 2 조건)함으로써, 평문(μ)이 제 1 및 제 2 조건에 만족하는지를 판단(S220)한다.

[0045] S220의 판단 결과 상기의 제 1 및 제 2 조건을 만족하면, $Dec(sk_i, C)$ 알고리즘은 평문(μ)을 출력(S222)하고, 그렇지 않은 경우 $\perp$ 를 출력(S224)한다.

[0046] 상술한 바와 같이, 본 발명은 래티스 기반으로 각 참여자의 공개키와 비밀키를 생성하여 설정한 후 각 참여자의 공개키를 기반으로 평문을 암호화하여 브로드캐스트 기법으로 전송하고, 암호화된 평문을 복호화시킴으로써, 의미론적 안정성과 복호화 일관성을 동시에 만족시킬 수 있는 브로드캐스트 기법을 제공할 수 있다.

[0047] 이상 첨부된 도면을 참조하여 본 발명의 실시 예를 설명하였지만, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 본 발명이 그 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다.

부호의 설명

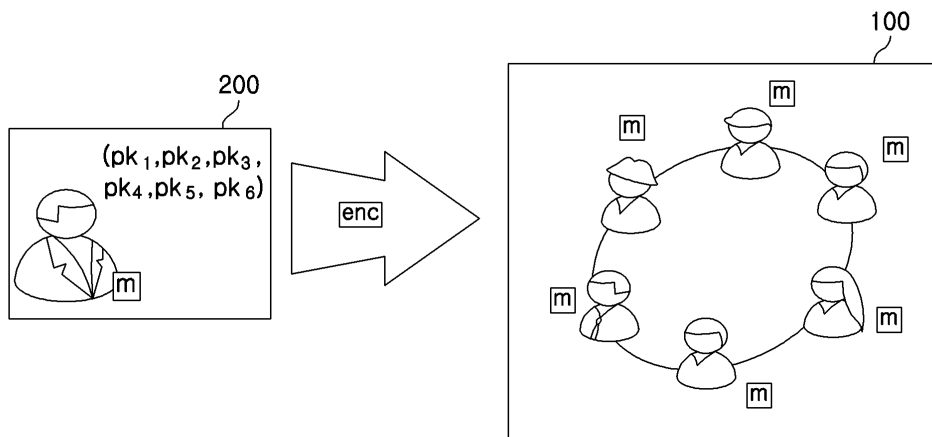
[0048]

100 : 참여자 그룹

200 : 전송 장치

도면

도면1



도면2

