(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2008-0092611
(43) 공개일자 2008년10월16일

(51) Int. Cl.
H04L 9/30 (2006.01) *H04L 9/28* (2006.01)
H04L 9/08 (2006.01)
(21) 출원번호 10-2007-0036133
(22) 출원일자 2007년04월12일
심사청구일자 없음

(71) 출원인
삼성전자주식회사
경기도 수원시 영통구 매탄동 416
고려대학교 산학협력단
서울 성북구 안암동5가1 고려대학교 내
(72) 발명자
성맹희
서울시 서초구 서초동 신동아 8동 306호
진원일
경기도 수원시 장안구 천천동 비단마을 우방아파트 711동 1703호
(뒷면에 계속)
(74) 대리인
특허법인무한

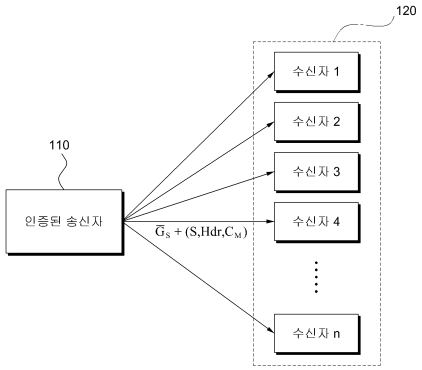
전체 청구항 수 : 총 17 항

(54) 브로드캐스트 암호화 및 복호화 장치 및 그 방법

(57) 요 약

브로드캐스트 암호화 방법 및 그 복호화 방법이 개시된다. 본 발명의 일실시예에 따른 브로드캐스트 암호화 방법은 인증된 송신자에게만 알려진 암호화용 비밀키를 이용하여 메시지 암호화 키를 생성하는 단계, 상기 메시지 암호화 키를 이용하여 메시지를 암호화하는 단계, 및 정당한 사용자에 대응하는 스트롱 디프-헬만 터플(Strong Diffie-Hellman tuple)과 상기 암호화용 비밀키를 이용하여 메시지 헤더를 생성하는 단계를 포함하는 것을 특징으로 한다.

대 표 도 - 도1



(72) 발명자

김희진

경기도 용인시 기흥구 상갈동 금화마을대우현대아파트 105동704호

정배은

경기도 성남시 분당구 이매동 이매촌삼성아파트 1003동 903호

정태철

경기도 성남시 분당구 정자동 판테온리젠시 1918호

박종환

서울시 성북구 안암동5가 고려대학교 생명과학관140호

이동훈

서울시 성북구 안암동5가 고려대학교 생명과학관140호

임종인

서울시 성북구 안암동5가 고려대학교 생명과학관140호

최규영

서울시 성북구 안암동5가 고려대학교 생명과학관140호

황정연

서울시 성북구 안암동5가 고려대학교 생명과학관140호

특허청구의 범위

청구항 1

인증된 송신자에게만 알려진 암호화용 비밀키를 이용하여 메시지 암호화 키를 생성하는 암호화 키 생성부;

상기 메시지 암호화 키를 이용하여 메시지를 암호화하는 암호화부;

정당한 사용자에 대응하는 스트롱 디프-헬만 터플(Strong Diffie-Hellman tuple)과 상기 암호화용 비밀키를 이용하여 메시지 헤더를 생성하는 헤더 생성부; 및

상기 암호화된 메시지와 메시지 헤더를 송신하는 송신부

를 포함하는 것을 특징으로 하는 브로드캐스트 암호화 장치.

청구항 2

제1항에 있어서,

상기 암호화키 생성부는

하기 수학식 1에 의하여 상기 메시지 암호화 키를 생성하는 것을 특징으로 하는 브로드캐스트 암호화 장치.

[수학식 1]

$$K = e(W, G)^{s}$$

(K: 메시지 암호화키, G: 타원곡선 위에서 위수 p인 그룹을 구성하는 생성원, W: 암호화용 비밀키로서 G로 생성된 그룹 내의 임의의 원소, s: Zp에서 선택한 임의의 원소, e(): 타원 곡선 위에서 정의되는 페어링(pairing) 함수)

청구항 3

제1항에 있어서,

상기 헤더 생성부는

하기 수학식 2를 이용하여 상기 메시지 헤더를 생성하는 것을 특징으로 하는 브로드캐스트 암호화 장치.

[수학식 2]

$$Hdr = (s(H + \sum_{j \in S} G_j), sG)$$

(Hdr: 메시지 헤더, G: 타원곡선 위에서 위수 p인 그룹을 구성하는 생성원, H: 암호화용 비밀키로서 G로 생성된 그룹 내의 임의의 원소, s: Zp에서 선택한 임의의 원소, Gj =(1/(x+j))G, x: Zp에서 선택한 임의의 원소, S: 정당한 사용자 그룹, j: 정당한 사용자에 대응하는 인덱스)

청구항 4

제1항에 있어서,

상기 헤더 생성부는

모든 사용자를 포함하는 그룹을 소정의 수의 소그룹으로 분할하고, 각각의 상기 소그룹 내의 정당한 사용자에 대응하는 스트롱 디프-헬만 터플(Strong Diffie-Hellman tuple)과 상기 암호화용 비밀키를 이용하여 메시지 헤더를 생성하는 것을 특징으로 하는 브로드캐스트 암호화 장치.

청구항 5

제4항에 있어서,

상기 메시지 헤더는 하기 수학식 3을 이용하여 생성되는 것을 특징으로 하는 브로드캐스트 암호화 장치.

[수학식 3]

$$Hdr = \left[s\left(H_1 + \sum_{j \in S_1} G_j\right), s\left(H_2 + \sum_{j \in S_2} G_j\right), s\left(H_3 + \sum_{j \in S_3} G_j\right), s\left(H_4 + \sum_{j \in S_4} G_j\right), s\left(H_5 + \sum_{j \in S_5} G_j\right), sG \right]$$

(Hdr: 메시지 헤더, G: 타원곡선 위에서 위수 p인 그룹을 구성하는 생성원, S_1 내지 S_5: 소그룹, H_1 내지 H_5: 각각 소그룹 S_1 내지 S_5에 대응하는 암호화용 비밀키로서 G로 생성된 그룹내의 임의의 원소, s: Zp에서 선택한 임의의 원소, Gj =(1/(x+j))G, x: Zp에서 선택한 임의의 원소, j: 각 소그룹 내의 정당한 사용자에 대응하는 인덱스)

청구항 6

메시지 헤더, 암호화된 메시지 및 정당한 사용자에 대응하는 스트롱 디프-헬만 터플을 수신하는 수신부;

정당한 사용자에게만 알려진 사용자별 복호화 키, 상기 메시지 헤더 및 상기 스트롱 디프-헬만 터플을 이용하여 페어링 연산을 수행하여 암호화 키를 복원하는 암호화 키 복원부; 및

상기 암호화키를 이용하여 암호화된 메시지를 복호화하는 복호화부

를 포함하는 것을 특징으로 하는 브로드캐스트 복호화 장치.

청구항 7

제6항에 있어서,

상기 암호화 키 복원부는 하기 수학식 4 및 수학식 5를 이용하여 상기 페어링 연산을 수행하는 것을 특징으로 하는 브로드캐스트 복호화 장치.

[수학식 4]

$$K = \frac{e(D_i + \sum_{j \in S, j \neq i} a_{ij} G_i + b_{ij} G_j, B)}{e(A, G_i)} = e(W, G)^s$$

$$Hdr = (s(H + \sum_{j \in S, j \neq i} G_j), sG) = (A, B)$$

(K: 암호화 키, e(): 타원곡선 위에서 정의되는 페어링 함수, Hdr: 메시지 헤더, G: 타원곡선 위에서 위수 p인 그룹을 구성하는 생성원, H 및 W: 각각 G로 생성된 그룹 내의 임의의 원소, s: Zp에서 선택한 임의의 원소, a_{ij}=1/(j-i), b_{ij}=-1(j-i), S: 정당한 사용자 그룹, Gi=(1/(x+i))G), Gj =(1/(x+j))G, i: 암호화된 메시지를 수신한 정당한 사용자에 상응하는 인덱스, Di: 정당한 사용자 i에 상응하는 사용자별 복호화 키, j: i를 제외한 정당한 사용자에 상응하는 인덱스)

[수학식 5]

$$\frac{1}{(x+i)(x+j)} = \frac{a_{ij}}{x+i} + \frac{b_{ij}}{x+j} \quad \rightarrow \quad aij = \frac{1}{(j-i)} \;\; bij = \frac{-1}{(j-i)}$$

(x: Zp에서 선택한 임의의 원소, i는 암호화된 메시지를 수신한 사용자에 상응하는 인덱스, j는 i를 제외한 정당한 사용자 그룹에 속하는 멤버의 인덱스)

청구항 8

제6항에 있어서,

상기 사용자 별 복호화 키는 하기 수학식 6을 이용하여 생성되는 것을 특징으로 하는 브로드캐스트 복호화 장치.

[수학식 6]

$$Di = W + \frac{1}{x+i}H + \frac{1}{(x+i)^2}G$$

(Di: 사용자 중 i에 상응하는 사용자의 비밀키, G: 타원곡선 위에서 위수 p인 그룹을 구성하는 생성원, W 및 H: G로 생성된 그룹내의 임의의 원소, x: Zp에서 선택한 임의의 원소, i: 1이상 n이하의 자연수, n: 전체사용자수)

청구항 9

인증된 송신자에게만 알려진 암호화용 비밀키를 이용하여 메시지 암호화 키를 생성하는 단계;

상기 메시지 암호화 키를 이용하여 메시지를 암호화하는 단계; 및

정당한 사용자에 대응하는 스트롱 디프-헬만 터플(Strong Diffie-Hellman tuple)과 상기 암호화용 비밀키를 이용하여 메시지 헤더를 생성하는 단계

를 포함하는 것을 특징으로 하는 브로드캐스트 암호화 방법.

청구항 10

제9항에 있어서,

상기 메시지 암호화 키를 생성하는 단계는

하기 수학식 7에 의하여 상기 메시지 암호화 키를 생성하는 것을 특징으로 하는 브로드캐스트 암호화 방법.

[수학식 7]

$$K = e(W, G)^s$$

(K: 메시지 암호화키, G: 타원곡선 위에서 위수 p인 그룹을 구성하는 생성원, W: 암호화용 비밀키로서 G로 생성된 그룹 내의 임의의 원소, s: Zp에서 선택한 임의의 원소, e(): 타원 곡선 위에서 정의되는 페어링(pairing) 함수)

청구항 11

제9항에 있어서,

상기 메시지 헤더를 생성하는 단계는

하기 수학식 8을 이용하여 상기 메시지 헤더를 생성하는 것을 특징으로 하는 브로드캐스트 암호화 방법.

[수학식 8]

$$Hdr = (s(H + \sum_{j \in S} G_j), sG)$$

(Hdr: 메시지 헤더, G: 타원곡선 위에서 위수 p인 그룹을 구성하는 생성원, H: 암호화용 비밀키로서 G로 생성된 그룹 내의 임의의 원소, s: Zp에서 선택한 임의의 원소, Gj =(1/(x+j))G, x: Zp에서 선택한 임의의 원소, S: 정당한 사용자 그룹, j: 정당한 사용자에 대응하는 인덱스)

청구항 12

제9항에 있어서,

상기 메시지 헤더를 생성하는 단계는

모든 사용자를 포함하는 그룹을 소정의 수의 소그룹으로 분할하고, 각각의 상기 소그룹 내의 정당한 사용자에 대응하는 스트롱 디프-헬만 터플(Strong Diffie-Hellman tuple)과 상기 암호화용 비밀키를 이용하여 메시지 헤더를 생성하는 것을 특징으로 하는 브로드캐스트 암호화 방법.

청구항 13

제12항에 있어서,

상기 메시지 헤더는 하기 수학식 9를 이용하여 생성되는 것을 특징으로 하는 브로드캐스트 암호화 방법.

[수학식 9]

$$Hdr = \left[s\left(H_1 + \sum_{j \in S_1} G_j\right), s\left(H_2 + \sum_{j \in S_2} G_j\right), s\left(H_3 + \sum_{j \in S_3} G_j\right), s\left(H_4 + \sum_{j \in S_4} G_j\right), s\left(H_5 + \sum_{j \in S_5} G_j\right), sG \right]$$

(Hdr: 메시지 헤더, G: 타원곡선 위에서 위수 p인 그룹을 구성하는 생성원, S_1 내지 S_5: 소그룹, H_1 내지 H_5: 각각 소그룹 S_1 내지 S_5에 대응하는 암호화용 비밀키로서 G로 생성된 그룹내의 임의의 원소, s: Zp에서 선택한 임의의 원소, Gj =(1/(x+j))G, x: Zp에서 선택한 임의의 원소, j: 각 소그룹 내의 정당한 사용자에 대응하는 인덱스)

청구항 14

메시지 헤더, 암호화된 메시지 및 정당한 사용자에 대응하는 스트롱 디프-헬만 터플을 수신하는 단계;

정당한 사용자에게만 알려진 사용자별 복호화 키, 상기 메시지 헤더 및 상기 스트롱 디프-헬만 터플을 이용하여 페어링 연산을 수행하여 암호화 키를 복원하는 단계; 및

상기 암호화키를 이용하여 암호화된 메시지를 복호화하는 단계

를 포함하는 것을 특징으로 하는 브로드캐스트 복호화 방법.

청구항 15

제14항에 있어서,

상기 암호화 키를 복원하는 단계는 하기 수학식 10 및 수학식 11을 이용하여 상기 페어링 연산을 수행하는 것을 특징으로 하는 브로드캐스트 복호화 방법.

[수학식 10]

$$K = \frac{e(D_i + \sum_{j \in S, j \neq i} a_{ij} G_i + b_{ij} G_j, B)}{e(A, G_i)} = e(W, G)^s$$

$$Hdr = (s(H + \sum_{j \in S, j \neq i} G_j), sG) = (A, B)$$

(K: 암호화 키, e(): 타원곡선 위에서 정의되는 페어링 함수, Hdr: 메시지 헤더, G: 타원곡선 위에서 위수 p인 그룹을 구성하는 생성원, H 및 W: 각각 G로 생성된 그룹 내의 임의의 원소, s: Zp에서 선택한 임의의 원소, a_{ij}=1/(j-i), b_{ij}=-1(j-i), S: 정당한 사용자 그룹, Gi=(1/(x+i))G), Gj =(1/(x+j))G, i: 암호화된 메시지를 수신한 정당한 사용자에 상응하는 인덱스, Di: 정당한 사용자 i에 상응하는 사용자별 복호화 키, j: i를 제외한 정당한 사용자에 상응하는 인덱스)

[수학식 11]

$$\frac{1}{(x+i)(x+j)} = \frac{a_{ij}}{x+i} + \frac{b_{ij}}{x+j} \rightarrow aij = \frac{1}{(j-i)} \quad bij = \frac{-1}{(j-i)}$$

(x: Zp에서 선택한 임의의 원소, i는 암호화된 메시지를 수신한 사용자에 상응하는 인덱스, j는 i를 제외한 정당한 사용자 그룹에 속하는 멤버의 인덱스)

청구항 16

제14항에 있어서,

상기 사용자 별 복호화 키는 하기 수학식 12를 이용하여 생성되는 것을 특징으로 하는 브로드캐스트 복호화 방법.

[수학식 12]

$$Di = W + \frac{1}{x+i} H + \frac{1}{(x+i)^2} G$$

(PK: 공개키, Di: 사용자 중 i에 상응하는 사용자의 비밀키, G: 타원곡선 위에서 위수 p인 그룹을 구성하는 생성원, W 및 H: G로 생성된 그룹내의 임의의 원소, x: Zp에서 선택한 임의의 원소, i: 1이상 n이하의 자연수, n: 전체사용자수)

청구항 17

제9항 내지 제16항 중 어느 한 항의 방법을 실행하기 위한 프로그램이 기록되어 있는 것을 특징으로 하는 컴퓨터에서 판독 가능한 기록 매체.

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

<9> 본 발명은 브로드캐스트 암호화 방법 및 그 복호화 방법에 관한 것으로, 특히 스트롱 디프-헬만 터플(Strong Diffie-Hellman tuple)을 이용하여 공개키 및 비밀키를 생성하는 브로드캐스트 암호화 방법 및 그 복호화 방법에 관한 것이다.

<10> 최근 브로드캐스트 암호화에 관한 연구가 활발하게 이루어지고 있다. 브로드캐스트 암호화란 전송자가 다수의 사용자에게 사용자 집합(S), 헤더(Header) 및 암호화된 메시지를 전송하면 사용자 집합(S)에 속한 사용자만이 헤더를 이용하여 메시지 암호키를 복원한 후 복원된 메시지 암호키를 이용하여 암호화된 메시지를 복호화하는 것이다.

<11> 이 때, 사용자 집합(S)에 속하는 사용자를 정당한 사용자라고 하고, 이들만이 메시지를 얻는 것이 가능해야 하고 사용자 집합(S)에 속하지 않는 사용자는 메시지를 얻을 수 없어야 한다.

<12> 브로드캐스트 암호화는 단 한번의 브로드캐스팅을 통해 정당한 사용자만이 암호키를 얻을 수 있다는 점에서 유료 채널의 위상 TV 수신 서비스나 저작권으로 보호되는 컨텐츠의 전송에 효율적으로 사용될 수 있다.

<13> 브로드캐스트 암호화에는 대칭키 기반 방식(symmetric key setting) 및 공개키 기반 방식(public key setting)이 있다. 대칭키 기반 방식은 신뢰된 전송자만이 사용자의 비밀키를 생성하여 분배하고, 사용자에게 브로드캐스트 메시지를 전송한다. 이 경우 신뢰된 전송자는 브로드캐스트 암호화에 대한 모든 책임을 진다.

<14> 공개키 기반 방식은 시스템에서 공통으로 사용하는 공개키를 이용하여 그룹 구성원 누구라도 브로드캐스트 메시

지를 전송할 수 있다.

<15> 일반적으로, 서비스 제공자가 한 명이고 서비스의 수용자가 여러 명인 경우, 대칭키 기반 방식이 보다 유효한 접근 방법일 수 있다.

<16> D. Boneh, C. Gentry, 및 B. Waters는 2005년 CRYPTO vol.3621, pp.258-275에 발표한 "Collusion resistant broadcast encryption with short ciphertexts and private keys"라는 논문을 통해 타원곡선 위의 페어링을 이용하여 전송량과 저장량에서 효율성을 갖는 공개키 기반의 브로드캐스트 암호화기법을 제안하였다.

<17> 그러나, D. Boneh, C. Gentry, 및 B. Waters가 제안한 방법에 따르면 n명의 사용자에 대하여 2n+1개의 공개키가 필요하고, 복호화를 할 때에도 2n-1개의 공개키가 필요하므로, 전송량을 줄일 수 있는 새로운 브로드캐스트 암호화 방법 및 복호화 방법의 필요성이 절실하게 대두된다.

발명이 이루고자 하는 기술적 과제

<18> 본 발명은 상술한 바와 같은 종래기술의 문제점을 해결하기 위해 안출된 것으로서, 스트롱 디프-헬만 터플을 이용하여 전송량 및 저장량을 줄이면서 브로드캐스트 암호화/복호화가 가능하도록 하는 것을 목적으로 한다.

<19> 또한, 본 발명은 전체 사용자들을 복수 개의 소그룹으로 나누고 각각의 소그룹에 대하여 스트롱 디프-헬만 터플을 공유하도록 하여 효과적으로 브로드캐스트 암호화의 전송량을 줄이는 것을 목적으로 한다.

발명의 구성 및 작용

<20> 상기의 목적을 달성하고 종래 기술의 문제점을 해결하기 위하여, 본 발명의 브로드캐스트 암호화(encrypt) 장치는 인증된 송신자에게만 알려진 암호화용 비밀키를 이용하여 메시지 암호화 키를 생성하는 암호화 키 생성부, 상기 메시지 암호화 키를 이용하여 메시지를 암호화하는 암호화부, 및 정당한 사용자에 대응하는 스트롱 디프-헬만 터플(Strong Diffie-Hellman tuple)과 상기 암호화용 비밀키를 이용하여 메시지 헤더를 생성하는 헤더 생성부를 포함하는 것을 특징으로 한다.

<21> 또한, 본 발명의 일 실시예에 따른 브로드캐스트 복호화(decrypt) 장치는 메시지 헤더, 암호화된 메시지 및 정당한 사용자에 대응하는 스트롱 디프-헬만 터플(Strong Diffie-Hellman tuple)을 수신하는 수신부, 정당한 사용자에게만 알려진 사용자별 복호화 키, 상기 메시지 헤더 및 상기 스트롱 디프-헬만 터플을 이용하여 페어링 연산을 수행하여 암호화 키를 복원하는 암호화 키 복원부, 및 상기 암호화키를 이용하여 암호화된 메시지를 복호화하는 복호화부를 포함하는 것을 특징으로 한다.

<22> 본 발명에서 설명하는 스트롱 디프-헬만 터플(Strong Diffie-Hellman tuple)에 대한 자세한 내용은 Dan Boneh, Xavier Boyen, and Hovav Shacham. Short group signatures. In CRYPTO 2004, volume 3152 of LNCS, pages 41-55. Springer-Verlag, 2004. 등에 상세히 개시되어 있다.

<23> 본 발명에서 사용되는 기호들은 다음과 같이 정의된다.

<24> G: 타원곡선 위에서 위수(order) p인 그룹을 구성하는 생성원(generator)

<25> H, W: 인증된 송신자에게만 알려진 암호화용 비밀키

<26> Zp: 위수가 p인 그룹

<27> x: Zp에서 선택한 임의의 원소(키를 생성하는데 난수로 사용)

<28> s: Zp에서 선택한 임의의 원소(매번 전송되는 메시지 암호화 키 K를 랜덤하게 생성하는데 사용)

<29> S: 전체 사용자 수 n명 중 정당한 사용자들의 집합

<30> i: S에 속하는 정당한 사용자로서 Hdr(메시지 헤더)로부터 메시지 암호화 키 K를 구하려는 사용자

<31> j: S에 속하는 정당한 사용자로서 i가 아닌 사용자들

<32> e(): 타원곡선 위에서 정의되는 페어링(pairing) 함수

<33> Gi: $G_i = (1/(x+i))G$ for $i = 1, \cdots, n$

<34> $\overline{G}_S$: S와 관련된 Gi 들의 집합

<35> 본 발명에서 스트롱 디프-헬만 터플은 ((1/(x+i))G, i) 중에서 (1/(x+i))G만을 나타내는 것일 수 있다.

<36> 이하, 본 발명에 따른 바람직한 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.

<37> 도 1은 본 발명의 일실시예에 따른 브로드캐스트 암호화 메시지 전송을 나타낸 도면이다.

<38> 도 1을 참조하면, 본 발명의 일실시예에 따른 브로드캐스트 암호화 메시지 전송은 인증된 송신자(110)가 다수의 수신 측 사용자들(120)에게 정당한 사용자 그룹(S)에 해당하는 스트롱 디프-헬만 터플($\overline{G_S}$), 정당한 사용자 그룹(S)에 대한 정보, 메시지 헤더(Hdr) 및 암호화된 메시지(C_M)를 전송한다.

<39> 이 때, 정당한 사용자 그룹(S)에 해당하는 스트롱 디프-헬만 터플($\overline{G_S}$)은 Gi들 중 정당한 사용자 그룹(S)과 관련된 것들의 집합일 수 있다.

<40> 암호화된 메시지(C_M)는 암호화 키(K)를 이용하여 암호화된다. 이 때, 암호화 키는 인증된 송신자(110)에게만 알려진 암호화용 비밀키를 이용하여 생성된다. 이 때, 상기 암호화용 비밀키는 G로 생성된 그룹 내의 임의의 원소 중에서 랜덤하게 선택된 것일 수 있다.

<41> 헤더(Hdr)는 정당한 사용자에 대응하는 스트롱 디프-헬만 터플과 상기 암호화용 비밀키를 이용하여 생성될 수 있다. 이 때, 헤더(Hdr)는 스트롱 디프-헬만 터플 중 정당한 사용자에 대응하는 것들의 합을 이용하여 생성될 수 있다.

<42> 상기 암호화용 비밀키를 알고 있는 인증된 송신자(110)는 암호화 키(K)와 헤더(Hdr)를 생성할 수 있고, 상기 암호화용 비밀키를 알지 못하는 다른 사용자들은 암호화 키(K)와 헤더(Hdr)를 생성할 수 없다.

<43> 수신 측 사용자들(120) 중 정당한 사용자 집합(S)에 속하는 사용자들은 미리 알려진 사용자 별 복호화 키와 수신한 정보들을 이용하여 암호화 키(K)를 복원할 수 있고, 사용자 별 복호화 키를 알지 못하는, 정당한 사용자 집합(S)에 속하지 않는 사용자들은 전송된 정보들로부터 암호화 키(K)를 복원할 수 없다.

<44> 도 2는 본 발명의 일 실시예에 따른 브로드캐스트 암호화 장치를 나타내는 블록도이다.

<45> 도 2를 참조하면, 본 발명의 일 실시예에 따른 브로드캐스트 암호화 장치는 암호화 키 생성부(210), 암호화부(220), 헤더 생성부(230) 및 송신부(240)를 포함한다.

<46> 암호화 키 생성부(210)는 인증된 송신자에게만 알려진 암호화용 비밀키를 이용하여 메시지 암호화 키를 생성한다.

<47> 이 때, 상기 암호화용 비밀키는 G로 생성된 그룹 내의 임의의 원소 중에서 랜덤하게 선택된 것일 수 있다.

<48> 이 때, 상기 메시지 암호화 키는 하기 수학식 1을 이용하여 생성된 것일 수 있다.

<49> [수학식 1]

<50> $K = e(W, G)^s$

<51> 여기서 K는 상기 메시지 암호화 키, W는 상기 암호화용 비밀키로서 G로 생성된 그룹 내의 임의의 원소이며, s는 위수 p인 그룹 Zp에서 선택한 임의의 원소로서 매번 전송되는 메시지 암호화 키 K를 랜덤하게 생성하는데 사용된다.

<52> 상기 암호화용 비밀키를 알고 있는 인증된 송신자는 암호화 키를 생성할 수 있고, 상기 암호화용 비밀키를 알지 못하는 다른 사용자들은 암호화 키를 생성할 수 없다.

<53> 암호화부(220)는 상기 메시지 암호화 키를 이용하여 메시지를 암호화한다.

<54> 헤더 생성부(230)는 정당한 사용자에 대응하는 스트롱 디프-헬만 터플(Strong Diffie-Hellman tuple)과 상기 암호화용 비밀키를 이용하여 메시지 헤더를 생성한다.

<55> 이 때, 상기 메시지 헤더는 스트롱 디프-헬만 터플 중 정당한 사용자에 대응하는 것들의 합을 이용하여 생성될 수 있다.

<56> 이 때, 상기 메시지 헤더는 하기 수학식 2를 이용하여 생성된 것일 수 있다.

<57> [수학식 2]

$$Hdr = (s(H + \sum_{j \in S} G_j), sG)$$

<58>

<59> 여기서 Hdr는 메시지 헤더, G는 타원곡선 위에서 위수 p인 그룹을 구성하는 생성원, H는 암호화용 비밀키로서 G로 생성된 그룹 내의 임의의 원소, s는 Zp에서 선택한 임의의 원소이다.

<60> Gj =(1/(x+j))G이고, x는 Zp에서 선택한 임의의 원소, S는 정당한 사용자 그룹, j는 정당한 사용자에 대응하는 인덱스이다.

<61> 즉, Gj 는 정당한 사용자에 대응하는 스트롱 디프-헬만 터플이고, 상기 메시지 헤더는 Gj 들의 합과 상기 암호화용 비밀키 H를 이용하여 생성된다.

<62> 이 때, 상기 헤더 생성부(230)는 모든 사용자를 포함하는 그룹을 소정의 수의 소그룹으로 분할하고, 각각의 상기 소그룹 내의 정당한 사용자에 대응하는 스트롱 디프-헬만 터플과 상기 암호화용 비밀키를 이용하여 메시지 헤더를 생성할 수 있다.

<63> 즉, 전체 사용자가 25명인 경우에 5명으로 구성된 5개의 소그룹들 각각에 대하여 정당한 사용자에 대응하는 스트롱 디프-헬만 터플과 상기 암호화용 비밀키를 이용하여 메시지 헤더를 생성하여 브로드캐스트할 수도 있다. 이 때, 상기 메시지 헤더는 하기 수학식 3을 이용하여 생성될 수 있다.

<64> [수학식 3]

$$Hdr = \left[s\left(H_1 + \sum_{j \in S_1} G_j\right), s\left(H_2 + \sum_{j \in S_2} G_j\right), s\left(H_3 + \sum_{j \in S_3} G_j\right), s\left(H_4 + \sum_{j \in S_4} G_j\right), s\left(H_5 + \sum_{j \in S_5} G_j\right), sG \right]$$

<65>

<66> 여기서 Hdr는 메시지 헤더, G는 타원곡선 위에서 위수 p인 그룹을 구성하는 생성원, S_1 내지 S_5은 소그룹, H_1 내지 H_5은 각각 소그룹 S_1 내지 S_5에 대응하는 암호화용 비밀키로서 G로 생성된 그룹내의 임의의 원소, s은 Zp에서 선택한 임의의 원소, Gj =(1/(x+j))G이고, x는 Zp에서 선택한 임의의 원소, j는 각 소그룹 내의 정당한 사용자에 대응하는 인덱스이다.

<67> 송신부(240)는 상기 암호화된 메시지와 메시지 헤더를 송신한다.

<68> 이 때, 송신부(240)는 정당한 사용자 그룹에 대응하는 스트롱 디프-헬만 터플을 상기 암호화된 메시지 및 상기 메시지 헤더와 함께 송신할 수 있다.

<69> 실시예에 따라, 인증된 사용자는 정당한 사용자 그룹에 대응하는 스트롱 디프-헬만 터플을 브로드캐스트 메시지와 함께 전송하지 아니하고, 수신 측 사용자가 이를 미리 저장하고 있을 수도 있다.

<70> 도 3은 본 발명의 일 실시예에 따른 브로드캐스트 복호화 장치를 나타내는 블록도이다.

<71> 도 3을 참조하면, 본 발명의 일 실시예에 따른 브로드캐스트 복호화 장치는 수신부(310), 암호화 키 복원부(320) 및 복호화부(330)를 포함한다.

<72> 수신부(310)는 메시지 헤더, 암호화된 메시지 및 정당한 사용자에 대응하는 스트롱 디프-헬만 터플을 수신한다.

<73> 실시예에 따라, 정당한 사용자 그룹에 대응하는 스트롱 디프-헬만 터플은 브로드캐스트 메시지와 함께 전송되지 아니하고, 수신 측 사용자가 이를 미리 저장하고 있을 수 있다.

<74> 이 때, 상기 메시지 헤더는 모든 사용자를 포함하는 그룹이 소정의 수의 소그룹으로 분할되고, 각각의 상기 소그룹 내의 정당한 사용자에 대응하는 스트롱 디프-헬만 터플을 이용하여 생성된 것일 수 있다.

<75> 암호화 키 복원부(320)는 정당한 사용자에게만 알려진 사용자별 복호화 키, 상기 메시지 헤더 및 상기 스트롱 디프-헬만 터플을 이용하여 페어링 연산을 수행하여 암호화 키를 복원한다.

<76> 이 때, 상기 암호화 키 복원부(320)는 하기 수학식 4 및 수학식 5를 이용하여 상기 페어링 연산을 수행할 수 있다.

<77> [수학식 4]

$$K = \frac{e(D_i + \sum_{j \in S, j \neq i} a_{ij} G_i + b_{ij} G_j, B)}{e(A, G_i)} = e(W, G)^s$$

$$Hdr = (s(H + \sum_{j \in S, j \neq i} G_j), sG) = (A, B)$$

<78>

<79> 여기서 K는 암호화 키, e()는 타원곡선 위에서 정의되는 페어링 함수, Hdr는 메시지 헤더, G는 타원곡선 위에서 위수 p인 그룹을 구성하는 생성원, H 및 W는 각각 G로 생성된 그룹 내의 임의의 원소, s는 Zp에서 선택한 임의의 원소, a_{ij}=1/(j-i), b_{ij}=-1(j-i)이다. S는 정당한 사용자 그룹, Gi=(1/(x+i))G), Gj =(1/(x+j))G이며, i는 암호화된 메시지를 수신한 정당한 사용자에 상응하는 인덱스, Di는 정당한 사용자 i에 상응하는 사용자별 복호화 키, j는 i를 제외한 정당한 사용자에 상응하는 인덱스이다.

<80> [수학식 5]

$$\frac{1}{(x+i)(x+j)} = \frac{a_{ij}}{x+i} + \frac{b_{ij}}{x+j} \rightarrow aij = \frac{1}{(j-i)} \quad bij = \frac{-1}{(j-i)}$$

<81>

<82> 여기서 x는 Zp에서 선택한 임의의 원소, i는 암호화된 메시지를 수신한 사용자에 상응하는 인덱스, j는 i를 제외한 정당한 사용자 그룹에 속하는 멤버의 인덱스이다.

<83> 상기 메시지 헤더(Hdr)는 상기 수학식 4와 같이 생성되지만 전송되어 수신되는 것은 그 결과인 A, B 뿐이고, 생성 과정에서 이용된 상기 G로 생성된 그룹 내의 임의의 원소 H는 수신 측 사용자에게는 비밀로 취급된다.

<84> 마찬가지로, 상기 암호화 키(K) 및 그 생성 과정에서 이용된 상기 G로 생성된 그룹 내의 임의의 원소 W는 수신 측 사용자에게는 비밀로 취급된다.

<85> 상기 암호화 키 복원부(320)는 정당한 사용자에게만 알려진 사용자별 복호화 키(Di), 상기 메시지 헤더(Hdr = (A, B)) 및 상기 정당한 사용자에 대응하는 스트롱 디프-헬만 터플(Gi)를 이용하여 상기 암호화 키(K)를 복원하고, 상기 수학식 4의 연산의 결과가 최초의 암호화 키와 같음은 증명될 수 있다.

<86> 이 때, 상기 사용자 별 복호화 키는 하기 수학식 6을 이용하여 생성되는 것일 수 있다.

<87> [수학식 6]

$$Di = W + \frac{1}{x+i} H + \frac{1}{(x+i)^2} G$$

<88>

<89> 여기서 Di는 사용자 중 i에 상응하는 사용자의 비밀키, G는 타원곡선 위에서 위수 p인 그룹을 구성하는 생성원, W 및 H는 G로 생성된 그룹내의 임의의 원소, x는 Zp에서 선택한 임의의 원소, i는 1이상 n이하의 자연수, n는 전체 사용자 수이다.

<90> 이 때, 상기 정당한 사용자에게 알려지는 값은 Di 뿐이고, 그 생성 과정에서 이용된 상기 G로 생성된 그룹 내의 임의의 원소 W와 H는 수신 측 사용자에게는 비밀로 취급된다.

<91> 복호화부(330)는 상기 암호화키를 이용하여 암호화된 메시지를 복호화한다.

<92> 도 4는 본 발명의 일 실시예에 따른 브로드캐스트 암호화 방법을 나타내는 동작 흐름도이다.

<93> 도 4를 참조하면, 본 발명의 일 실시예에 따른 브로드캐스트 암호화 방법은 인증된 송신자에게만 알려진 암호화용 비밀키를 이용하여 메시지 암호화 키를 생성한다(S410).

<94> 이 때, 상기 암호화용 비밀키는 G로 생성된 그룹 내의 임의의 원소 중에서 랜덤하게 선택된 것일 수 있다.

<95> 이 때, 상기 메시지 암호화 키는 하기 수학식 7을 이용하여 생성된 것일 수 있다.

<96> [수학식 7]

<97> $K = e(W, G)^{s}$

<98> 여기서 K는 상기 메시지 암호화 키, W는 상기 암호화용 비밀키로서 G로 생성된 그룹 내의 임의의 원소이며, s는 위수 p인 그룹 Zp에서 선택한 임의의 원소로서 매번 전송되는 메시지 암호화 키 K를 랜덤하게 생성하는데 사용된다.

<99> 상기 암호화용 비밀키를 알고 있는 인증된 송신자는 암호화 키를 생성할 수 있고, 상기 암호화용 비밀키를 알지 못하는 다른 사용자들은 암호화 키를 생성할 수 없다.

<100> 또한, 본 발명의 일 실시예에 따른 브로드캐스트 암호화 방법은 상기 메시지 암호화 키를 이용하여 메시지를 암호화한다(S420).

<101> 또한, 본 발명의 일 실시예에 따른 브로드캐스트 암호화 방법은 정당한 사용자에 대응하는 스트롱 디프-헬만 터플(Strong Diffie-Hellman tuple)과 상기 암호화용 비밀키를 이용하여 메시지 헤더를 생성한다(S430).

<102> 이 때, 상기 메시지 헤더는 스트롱 디프-헬만 터플 중 정당한 사용자에 대응하는 것들의 합을 이용하여 생성될 수 있다.

<103> 이 때, 상기 메시지 헤더는 하기 수학식 8을 이용하여 생성된 것일 수 있다.

<104> [수학식 8]

<105> $$Hdr = (s(H + \sum_{j \in S} G_j), sG)$$

<106> 여기서 Hdr는 메시지 헤더, G는 타원곡선 위에서 위수 p인 그룹을 구성하는 생성원, H는 암호화용 비밀키로서 G로 생성된 그룹 내의 임의의 원소, s는 Zp에서 선택한 임의의 원소이다.

<107> Gj =(1/(x+j))G이고, x는 Zp에서 선택한 임의의 원소, S는 정당한 사용자 그룹, j는 정당한 사용자에 대응하는 인덱스이다.

<108> 즉, Gj 는 정당한 사용자에 대응하는 스트롱 디프-헬만 터플이고, 상기 메시지 헤더는 Gj 들의 합과 상기 암호화용 비밀키 H를 이용하여 생성된다.

<109> 이 때, 상기 메시지 헤더는 모든 사용자를 포함하는 그룹을 소정의 수의 소그룹으로 분할하고, 각각의 상기 소그룹 내의 정당한 사용자에 대응하는 스트롱 디프-헬만 터플과 상기 암호화용 비밀키를 이용하여 생성될 수 있다.

<110> 즉, 전체 사용자가 25명인 경우에 5명으로 구성된 5개의 소그룹들 각각에 대하여 정당한 사용자에 대응하는 스트롱 디프-헬만 터플과 상기 암호화용 비밀키를 이용하여 메시지 헤더를 생성하여 브로드캐스트할 수도 있다. 이 때, 상기 메시지 헤더는 하기 수학식 9를 이용하여 생성될 수 있다.

<111> [수학식 9]

<112> $$Hdr = \left[s\left(H_1 + \sum_{j \in S_1} G_j\right), s\left(H_2 + \sum_{j \in S_2} G_j\right), s\left(H_3 + \sum_{j \in S_3} G_j\right), s\left(H_4 + \sum_{j \in S_4} G_j\right), s\left(H_5 + \sum_{j \in S_5} G_j\right), sG \right]$$

<113> 여기서 Hdr는 메시지 헤더, G는 타원곡선 위에서 위수 p인 그룹을 구성하는 생성원, S_1 내지 S_5은 소그룹, H_1 내지 H_5은 각각 소그룹 S_1 내지 S_5에 대응하는 암호화용 비밀키로서 G로 생성된 그룹내의 임의의 원소, s은 Zp에서 선택한 임의의 원소, Gj =(1/(x+j))G이고, x는 Zp에서 선택한 임의의 원소, j는 각 소그룹 내의 정당한 사용

자에 대응하는 인덱스이다.

<114> 도 5는 본 발명의 일 실시예에 따른 브로드캐스트 복호화 방법을 나타내는 동작 흐름도이다.

<115> 도 5를 참조하면, 본 발명의 일 실시예에 따른 브로드캐스트 복호화 방법은 메시지 헤더, 암호화된 메시지 및 정당한 사용자에 대응하는 스트롱 디프-헬만 터플을 수신한다(S510).

<116> 실시예에 따라, 정당한 사용자 그룹에 대응하는 스트롱 디프-헬만 터플은 브로드캐스트 메시지와 함께 전송되지 아니하고, 수신 측 사용자가 이를 미리 저장하고 있을 수 있다.

<117> 이 때, 상기 메시지 헤더는 모든 사용자를 포함하는 그룹이 소정의 수의 소그룹으로 분할되고, 각각의 상기 소그룹 내의 정당한 사용자에 대응하는 스트롱 디프-헬만 터플을 이용하여 생성된 것일 수 있다.

<118> 또한, 본 발명의 일 실시예에 따른 브로드캐스트 복호화 방법은 정당한 사용자에게만 알려진 사용자별 복호화 키, 상기 메시지 헤더 및 상기 스트롱 디프-헬만 터플을 이용하여 페어링 연산을 수행하여 암호화 키를 복원한다(S520).

<119> 이 때, 상기 페어링 연산은 하기 수학식 10 및 수학식 11을 이용하여 수행될 수 있다.

<120> [수학식 10]

$$K = \frac{e(D_i + \sum_{j \in S, j \neq i} a_{ij} G_i + b_{ij} G_j, B)}{e(A, G_i)} = e(W, G)^s$$

$$Hdr = (s(H + \sum_{j \in S, j \neq i} G_j), sG) = (A, B)$$

<121>

<122> 여기서 K는 암호화 키, e()는 타원곡선 위에서 정의되는 페어링 함수, Hdr는 메시지 헤더, G는 타원곡선 위에서 위수 p인 그룹을 구성하는 생성원, H 및 W는 각각 G로 생성된 그룹 내의 임의의 원소, s는 Zp에서 선택한 임의의 원소, a_{ij}=1/(j-i), b_{ij}=-1(j-i)이다. S는 정당한 사용자 그룹, Gi=(1/(x+i))G), Gj =(1/(x+j))G이며, i는 암호화된 메시지를 수신한 정당한 사용자에 상응하는 인덱스, Di는 정당한 사용자 i에 상응하는 사용자별 복호화 키, j는 i를 제외한 정당한 사용자에 상응하는 인덱스이다.

<123> [수학식 11]

$$\frac{1}{(x+i)(x+j)} = \frac{a_{ij}}{x+i} + \frac{b_{ij}}{x+j} \rightarrow aij = \frac{1}{(j-i)} \; bij = \frac{-1}{(j-i)}$$

<124>

<125> 여기서 x는 Zp에서 선택한 임의의 원소, i는 암호화된 메시지를 수신한 사용자에 상응하는 인덱스, j는 i를 제외한 정당한 사용자 그룹에 속하는 멤버의 인덱스이다.

<126> 상기 메시지 헤더(Hdr)는 상기 수학식 10과 같이 생성되지만 전송되어 수신되는 것은 그 결과인 A, B 뿐이고, 생성 과정에서 이용된 상기 G로 생성된 그룹 내의 임의의 원소 H는 수신 측 사용자에게는 비밀로 취급된다.

<127> 마찬가지로, 상기 암호화 키(K) 및 그 생성 과정에서 이용된 상기 G로 생성된 그룹 내의 임의의 원소 W는 수신 측 사용자에게는 비밀로 취급된다.

<128> 상기 암호화 키(K) 는 정당한 사용자에게만 알려진 사용자별 복호화 키(Di), 상기 메시지 헤더(Hdr = (A, B)) 및 상기 정당한 사용자에 대응하는 스트롱 디프-헬만 터플(Gi)를 이용하여 복원된다. 상기 수학식 10의 연산의 결과가 최초의 암호화 키와 같음은 증명될 수 있다.

<129> 이 때, 상기 사용자 별 복호화 키는 하기 수학식 12를 이용하여 생성되는 것일 수 있다.

<130> [수학식 12]

$$Di = W + \frac{1}{x+i} H + \frac{1}{(x+i)^2} G$$

<131>

<132> 여기서 Di는 사용자 중 i에 상응하는 사용자의 비밀키, G는 타원곡선 위에서 위수 p인 그룹을 구성하는 생성원, W 및 H는 G로 생성된 그룹내의 임의의 원소, x는 Zp에서 선택한 임의의 원소, i는 1이상 n이하의 자연수, n는 전체 사용자 수이다.

<133> 이 때, 상기 정당한 사용자에게 알려지는 값은 Di 뿐이고, 그 생성 과정에서 이용된 상기 G로 생성된 그룹 내의 임의의 원소 W와 H는 수신 측 사용자에게는 비밀로 취급된다.

<134> 또한, 본 발명의 일 실시예에 따른 브로드캐스트 복호화 방법은 상기 암호화키를 이용하여 암호화된 메시지를 복호화한다(S530).

<135> 본 발명에 따른 브로드캐스트 복호화 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 상기 매체는 프로그램 명령, 데이터 구조 등을 지정하는 신호를 전송하는 반송파를 포함하는 광 또는 금속선, 도파관 등의 전송 매체일 수도 있다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

<136> 이상과 같이 본 발명은 비록 한정된 실시예와 도면에 의해 설명되었으나, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상의 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

<137> 그러므로, 본 발명의 범위는 설명된 실시예에 국한되어 정해져서는 아니 되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

발명의 효과

<138> 본 발명의 브로드캐스트 암호화 방법 및 그 복호화 방법은, 스트롱 디프-헬만 터플을 이용하여 전송량 및 저장량을 줄이면서 브로드캐스트 암호화/복호화를 할 수 있다.

<139> 또한, 본 발명은 전체 사용자들을 복수 개의 소그룹으로 나누고 각각의 소그룹에 대하여 스트롱 디프-헬만 터플을 공유하도록 하여 효과적으로 브로드캐스트 암호화의 전송량을 줄일 수 있다.

도면의 간단한 설명

<1> 도 1은 본 발명의 일실시예에 따른 브로드캐스트 암호화 메시지 전송을 나타낸 도면이다.

<2> 도 2는 본 발명의 일실시예에 따른 브로드캐스트 암호화 장치를 나타낸 블록도이다.

<3> 도 3은 본 발명의 일실시예에 따른 브로드캐스트 복호화 장치를 나타낸 블록도이다.

<4> 도 4는 본 발명의 일실시예에 따른 브로드캐스트 암호화 방법을 나타낸 동작 흐름도이다.

<5> 도 5는 본 발명의 일실시예에 따른 브로드캐스트 복호화 방법을 나타낸 동작 흐름도이다.

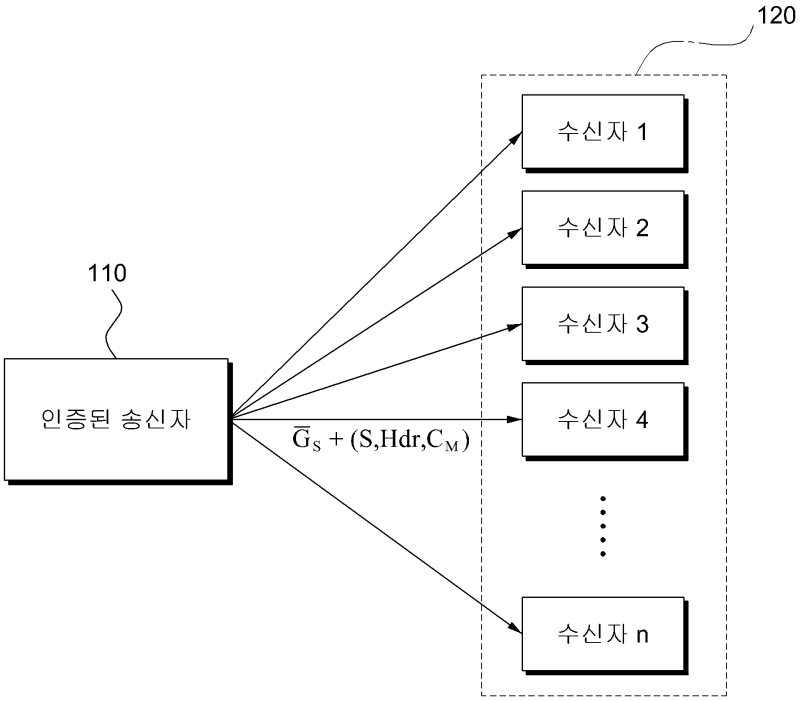
<6> <도면의 주요 부분에 대한 부호의 설명>

<7> 110: 인증된 송신자

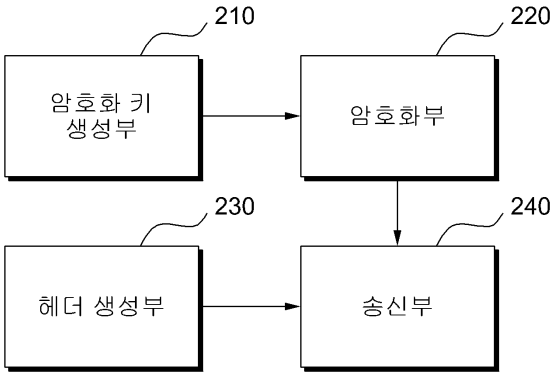
<8> 120: 수신 측 사용자들

도면

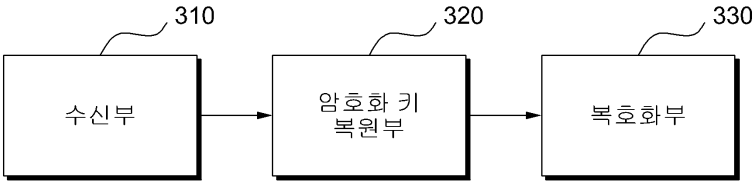
도면1



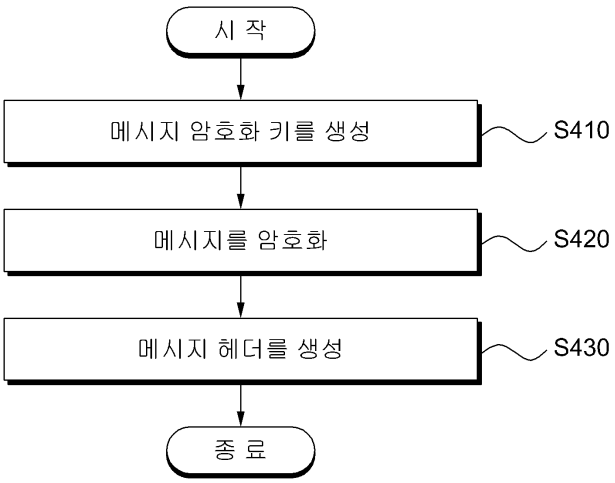
도면2



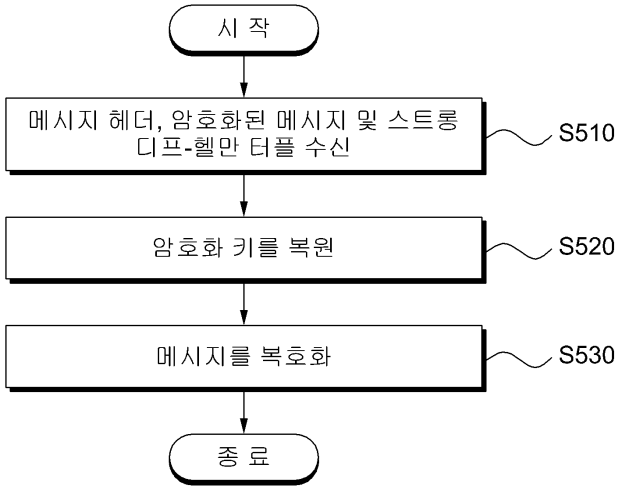
도면3


310
320
330
수신부
암호화 키
복원부
복호화부

도면4


시 작
메시지 암호화 키를 생성
S410
메시지를 암호화
S420
메시지 헤더를 생성
S430
종 료

도면5


시 작
메시지 헤더, 암호화된 메시지 및 스트롱 디프-헬만 터플 수신
S510
암호화 키를 복원
S520
메시지를 복호화
S530
종 료