



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2009-0079465
(43) 공개일자 2009년07월22일

(51) Int. Cl.

H04L 9/08 (2006.01) H04L 9/30 (2006.01)

(21) 출원번호 10-2008-0005443

(22) 출원일자 2008년01월17일

심사청구일자 2008년01월17일

(71) 출원인

고려대학교 산학협력단

서울 성북구 안암동5가1 고려대학교 내

(72) 발명자

임종인

서울 성북구 안암동5가 고려대학교 생명과학관
140호

이동훈

서울 성북구 안암동5가 고려대학교 생명과학관
140호

(뒷면에 계속)

(74) 대리인

현종철

전체 청구항 수 : 총 11 항

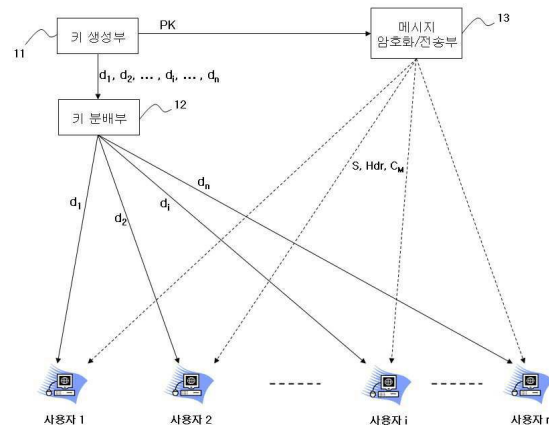
(54) 브로드캐스트 암호화 시스템 및 그 방법

(57) 요약

본 발명은 브로드캐스트 암호화 파라미터로 사용되는 공개키의 전송량, 저장량 및 사이즈 측면에서 효율성을 꾀할 수 있는 브로드캐스트 암호화 시스템에 관한 것이다.

본 명세서에서 개시하는 브로드캐스트 암호화 시스템은 메시지 수신자들을 다수의 수신자 그룹으로 분할하고 상기 그룹의 수만큼의 난수와 상기 분할된 각 그룹에 속한 수신자의 수만큼의 난수를 발생시켜 상기 수신자들에게 브로드캐스팅 할 메시지의 공개키를 생성하고, 상기 암호화 메시지의 복호를 위한 비밀키를 생성하는 키 생성부; 상기 생성된 공개키와 비밀키를 상기 수신자들에게 분배(브로드캐스팅)하는 키 분배부; 및 상기 브로드캐스팅 메시지를 암호화하여 상기 다수 사용자에게 전송하는 메시지 암호화/전송부를 포함하여 본 발명의 과제를 해결한다.

대표도 - 도1



(72) 발명자

박종환

서울 성북구 안암동5가 고려대학교 생명과학관 14
0호

이광수

서울 성북구 안암동5가 고려대학교 생명과학관 14
0호

김기탁

서울 성북구 안암동5가 고려대학교 생명과학관 14
0호

구영주

서울 성북구 안암동5가 고려대학교 생명과학관 14
0호

특허청구의 범위

청구항 1

메시지 수신자들을 다수의 수신자 그룹으로 분할하고 상기 그룹의 수만큼의 난수와 상기 분할된 각 그룹에 속한 수신자의 수만큼의 난수를 발생시켜 상기 수신자들에게 브로드캐스팅 할 메시지의 공개키를 생성하고, 상기 암호화 메시지의 복호를 위한 비밀키를 생성하는 키 생성부;

상기 비밀키를 상기 수신자들에게 분배(브로드캐스팅)하는 키 분배부; 및

상기 브로드캐스팅 메시지를 암호화하여 상기 다수 사용자에게 전송하는 메시지 암호화/전송부를 포함하는 브로드캐스트 암호화 시스템.

청구항 2

제 1 항에 있어서, 상기 키 생성부는

상기 공개키를 생성할 때 상기 수신자의 수에 해당하는 수만큼만 생성하는 것을 특징으로 하는 브로드캐스트 암호화 시스템.

청구항 3

제 2 항에 있어서, 상기 키 생성부는

상기 각 분할된 그룹의 인덱스와 상기 각 분할된 그룹에서의 개별 수신자의 인덱스를 직접 반영하여 상기 비밀키를 생성하는 것을 특징으로 하는 브로드캐스트 암호화 시스템.

청구항 4

제 3 항에 있어서, 상기 메시지 암호화/전송부는

상기 브로드캐스팅 할 메시지의 암호화키를 생성하는 암호화키 생성부;

상기 두 인덱스를 반영하여 헤더를 생성하는 헤더 생성부; 및

상기 암호화키로 상기 브로드캐스팅 할 메시지를 암호화한 암호문을 작성하고, 상기 암호문에 상기 헤더를 부가하여 상기 수신자들에게 브로드캐스팅하는 암호화 메시지 작성/브로드캐스팅부를 포함하는 것을 특징으로 하는 브로드캐스트 암호화 시스템.

청구항 5

제 1 항에 있어서,

상기 암호화 메시지에 대한 복호에는 상기 공개키가 필요 없는 것을 특징으로 하는 브로드캐스트 암호화 시스템.

청구항 6

(a)메시지 수신자들을 다수의 수신자 그룹으로 분할하고 상기 그룹의 수만큼의 난수와 상기 분할된 각 그룹에 속한 수신자의 수만큼의 난수를 발생시켜 상기 수신자들에게 브로드캐스팅 할 메시지의 공개키를 생성하는 단계;

(b)상기 암호화 메시지의 복호를 위한 비밀키를 생성하는 단계;

(c)상기 비밀키를 상기 수신자들에게 분배(브로드캐스팅)하는 단계; 및

(d)상기 브로드캐스팅 메시지를 암호화하여 상기 다수 사용자에게 전송하는 단계를 포함하는 브로드캐스트 암호화 방법.

청구항 7

제 6 항에 있어서, 상기 (a)단계는

상기 공개키를 상기 수신자의 수에 해당하는 수만큼만 생성하여 이루어지는 것을 특징으로 하는 브로드캐스트 암호화 방법.

청구항 8

제 7 항에 있어서, 상기 (a)단계는

상기 비밀키를 상기 각 분할된 그룹의 인덱스와 상기 각 분할된 그룹에서의 개별 수신자의 인덱스를 직접 반영하여 생성하여 이루어지는 것을 특징으로 하는 브로드캐스트 암호화 방법.

청구항 9

제 8 항에 있어서, 상기 (d)단계는

(d1)상기 브로드캐스팅 할 메시지의 암호화키를 생성하는 단계;

(d2)상기 두 인덱스를 반영하여 헤더를 생성하는 단계;

(d3)상기 암호화키로 상기 브로드캐스팅 할 메시지를 암호화한 암호문을 작성하는 단계; 및

(d4)상기 암호문에 상기 헤더를 부가하여 상기 수신자들에게 브로드캐스팅하는 단계를 포함하는 것을 특징으로 하는 브로드캐스트 암호화 방법.

청구항 10

제 9 항에 있어서,

상기 암호화 메시지에 대한 복호에는 상기 공개키가 필요 없는 것을 특징으로 하는 브로드캐스트 암호화 방법.

청구항 11

제 6 항 내지 제 10 항의 어느 한 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체.

명세서

발명의 상세한 설명

기술 분야

- <1> 본 발명은 브로드캐스트 암호화 시스템 및 그 방법에 관한 것으로, 보다 상세하게는 브로드캐스트 암호화 파라미터로 사용되는 공개키의 전송량, 저장량 및 사이즈 측면에서 효율성을 꾀할 수 있는 브로드캐스트 암호화 시스템 및 그 방법에 관한 것이다.

배경 기술

- <2> 브로드캐스트 암호화(Broadcast Encryption)는 전체 사용자들 중에서 메시지 송신자가 원하는 사용자(수신자, user)들에게만 메시지를 암호화시켜 전달하는 방식으로, 단 한 번의 암호 브로드캐스팅을 통해 정당 사용자만이 암호키(encryption key)를 얻을 수 있다는 점에서 유료 채널의 위성 TV 수신 서비스나 저작권으로 보호되는 콘텐츠의 전송에 효율적으로 사용될 수 있다.
- <3> 브로드캐스트 암호화는 정보를 받을 사용자들의 집합이 임의적이고 동적으로 변화하는 경우에 효과적으로 이용될 수 있어야 한다. 브로드캐스트 암호화에서의 가장 중요한 사항은 메시지 송신자가 원치 않는 사용자(예컨대, 불법 사용자 또는 기간이 만료된 사용자)를 효과적으로 배제(revocation)시키는 것이다.
- <4> 브로드캐스트 암호화에 의하면, 메시지 송신자가 메시지를 암호화시켜 다수의 사용자(수신자)에게 송신하면(암호화 전송시 사용자 집합(S), 헤더(Header) 및 암호화 키 K를 암호문에 부가시켜 전송한다) S에 속한 사용자만이 메시지 암호화 키(K)를 추출한 후 추출된 키로 암호화된 메시지(C_K)를 복호하여 볼 수 있도록 한다.
- <5> 여기서 사용자 집합 S에 속한 사용자를 정당한 사용자(permitted user)라고 하는데, 브로드캐스트 암호화 기법에 의하면 이들 정당 사용자만이 메시지를 얻을 수 있게 하고 S에 속하지 않는 사용자는 메시지를 얻을 수 없게

해야 하므로 기본적으로 수신자의 권한이 취소된(revoked) 경우에 대한 대응 메커니즘을 제공해야 한다. 즉, 권한이 취소된 수신자들이 공모(collusion)하여 공격할 수 있기 때문에 브로드캐스트 암호 기법은 권한이 취소된 수신자들의 공모 공격(collusion attack)에 대하여 안전해야(secure) 한다.

- <6> 브로드캐스트 암호화 방식에는 대칭키(비밀키) 기반 방식(symmetric(private) key setting)과 공개키 기반 방식(public key setting)이 있다. 대칭키 기반 방식에 의하면 우선 신뢰된(trusted) 송신자만이 사용자의 비밀키(private key)를 생성하여 분배하고 사용자에게 브로드캐스트 메시지를 전송한다. 사용자는 분배받은 비밀키를 이용하여 전송된 메시지를 복호화하여 확인한다. 대칭키 기반 방식에 의하면 신뢰된 송신자가 암호화에 대한 모든 책임을 지므로 암호화 시스템 작동 불능시 전체 브로드캐스트 암호 시스템이 마비된다. 그리고 구성원의 가입과 탈퇴시 복잡한 키 갱신 프로세스가 필요한 단점이 있다.
- <7> 이에 반해 공개키 기반 방식은 공통으로 사용하는 공개키를 이용하여 그룹 구성원(사용자) 누구라도 브로드캐스트 메시지를 전송할 수 있고, 복잡한 키 갱신 프로세스를 요구하지 않으므로 대칭키 기반 방식의 단점을 극복할 수 있다. 또한 공개키 기반 방식의 브로드캐스트 암호화 방식은 쉽게 대칭키 기반 방식으로 변환될 수 있는 우수성도 갖는다. 따라서 현재의 브로드캐스트 암호화는 공개키 기반 방식으로 구현됨이 거의 대부분이다.
- <8> 브로드캐스트 암호화 방식의 구현을 위한 여러 기법이 제안되었는데, 대표적인 기법으로 Boneh, Gentry와 Water에 의해 제안된 기법(BGW 기법)을 들 수 있다.
- <9> 이 기법은 총 사용자수가 크거나 정당 사용자로부터 배제된 자의 수가 작을 때 효과적인 방안이 될 수 있으나, 암호문 전송량, 공개키 저장량 및 공개키 사이즈 측면에서 매우 비효율적이다.

발명의 내용

해결 하고자하는 과제

- <10> 본 발명이 해결하고자 하는 과제는 상기한 기법들과 마찬가지로 공모 공격에 완전히 안전한 공개키 브로드캐스트 암호화 기법을 제안하되, 암호문 전송량, 공개키 저장량 및 공개키 사이즈 측면에서에서 이점을 가지는 브로드캐스트 암호화 기법을 제안하는 것이다.

과제 해결수단

- <11> 상기와 같은 과제를 해결하기 위해 본 명세서에서 개시하는 브로드캐스트 암호화 시스템은
- <12> 메시지 수신자들을 다수의 수신자 그룹으로 분할하고 상기 그룹의 수만큼의 난수와 상기 분할된 각 그룹에 속한 수신자의 수만큼의 난수를 발생시켜 상기 수신자들에게 브로드캐스팅 할 메시지의 공개키를 생성하고, 상기 암호화 메시지의 복호를 위한 비밀키를 생성하는 키 생성부; 상기 생성된 공개키와 비밀키를 상기 수신자들에게 분배(브로드캐스팅)하는 키 분배부; 및 상기 브로드캐스팅 메시지를 암호화하여 상기 다수 사용자에게 전송하는 메시지 암호화/전송부를 포함하여 본 발명의 과제를 해결한다.
- <13> 키 생성부는 공개키를 생성할 때 수신자의 수에 해당하는 수만큼만 생성하여 본 발명의 과제를 해결한다. 키 생성부는 아울러 각 분할된 그룹의 인덱스와 각 분할된 그룹에서의 개별 수신자의 인덱스를 직접 반영하여 비밀키를 생성하여 본 발명의 과제를 해결한다.
- <14> 메시지 암호화/전송부는 브로드캐스팅 할 메시지의 암호화키를 생성하는 암호화키 생성부; 상기 두 인덱스를 반영하여 헤더를 생성하는 헤더 생성부; 및 암호화키로 브로드캐스팅 할 메시지를 암호화한 암호문을 작성하고, 암호문에 헤더를 부가하여 상기 수신자들에게 브로드캐스팅하는 암호화 메시지 작성/브로드캐스팅부를 포함하여 본 발명의 과제를 해결한다.
- <15> 한편 암호화 메시지에 대한 복호에는 상기 공개키가 필요 없게 하여 본 발명의 과제를 해결한다.
- <16> 상기와 같은 과제를 해결하기 위해 본 명세서에서 개시하는 브로드캐스트 암호화 방법은
- <17> (a)메시지 수신자들을 다수의 수신자 그룹으로 분할하고 상기 그룹의 수만큼의 난수와 상기 분할된 각 그룹에 속한 수신자의 수만큼의 난수를 발생시켜 상기 수신자들에게 브로드캐스팅 할 메시지의 공개키를 생성하는 단계; (b)상기 암호화 메시지의 복호를 위한 비밀키를 생성하는 단계; (c)상기 생성된 공개키와 비밀키를 상기 수신자들에게 분배(브로드캐스팅)하는 단계; 및 (d)상기 브로드캐스팅 메시지를 암호화하여 상기 다수 사용자에게 전송하는 단계를 포함하여 본 발명의 과제를 해결한다.

- <18> (a)단계는 공개키를 수신자의 수에 해당하는 수만큼만 생성하여 본 발명의 과제를 해결한다.
- <19> (a)단계는 비밀키를 각 분할된 그룹의 인덱스와 각 분할된 그룹에서의 개별 수신자의 인덱스를 직접 반영하여 생성하는 것으로 본 발명의 과제를 해결한다.
- <20> (d)단계는 브로드캐스팅 할 메시지의 암호화키를 생성하는 단계; 두 인덱스를 반영하여 헤더를 생성하는 단계; 암호화키로 브로드캐스팅 할 메시지를 암호화한 암호문을 작성하는 단계; 및 암호문에 헤더를 부가하여 수신자들에게 브로드캐스팅하는 단계를 포함하여 본 발명의 과제를 해결한다.

효 과

- <21> 본 발명에 의한 브로드캐스트 암호화 기법은 기존에 제시된 기법에 비하여 암호문 전송량, 공개키 저장량, 공개키 사이즈 측면에서 뛰어난 성능을 보인다.

발명의 실시를 위한 구체적인 내용

- <22> 본 발명에 관한 구체적인 내용의 설명에 앞서 이해의 편의를 위해 본 발명이 해결하고자하는 과제의 해결 방안의 개요를 우선 제시한다.
- <23> 본 발명에 의한 브로드캐스트 암호화 기법은 BGW 기법과 마찬가지로 암호문 전송량과 공개키 저장량 사이에 트레이드-오프(trade-off)를 피한다. 총 $n(=a*b)$ 명의 사용자를 동일한 크기를 갖는 a 개의 사용자 그룹(부분집합) $S_1, \dots, S_a$ 로 나누고(각 부분집합에는 b 명의 사용자가 있다), 각 부분집합에서 권한이 취소된 사용자의 수 $r_1, \dots, r_a$ 중 최소의 수를 r' 이라고 할 때, 본 발명에 의한 암호화 기법은 암호문 전송량은 $(a+1)G+r\log_2 n$, 공개키 저장량은 $(b+1-r')$ 이며, 따라서 권한이 취소된 사용자의 수가 커질수록 공개키 저장량은 작아진다. 여기서 r 은 사용자 그룹에서 권한이 취소된 사용자의 총 수를 의미하는 것으로 $r_1 + \dots + r_a$ 이다.
- <24> 본 발명에 의한 암호화 기법의 출발점은 Boneh, Boyen, Goh의 계층적인 ID 기반의 암호화 기법(BBG Hierarchical Identity Based Encryption, BBG HIBE)에 의한 개인키 생성 방안이다. b -단계 BBG HIBE에서 키 생성 알고리즘은, 간략히 언급하면, 위수(prime order)가 p 인 그룹(Z_p)에 속하는 임의의 난수 r 에 대하여 깊이 1의 $ID=I_1$ 에 대한 개인키(d_{ID})를 다음과 같이 생성한다.
- <25>
$$d_{ID} = (g_2, (g_3 h_1^{11})^r, g^r, h_2^r, \dots, h_b^r).$$
- <26> g_3 을 제외하면 각 $S_1, \dots, S_a$ 에 해당하는 a 개의 공개키를 추가해야 한다. 다음으로 $i=(u-1)b+v$ 를 만족하고 $\{1, \dots, n\}$ 에 속하는 사용자 i 의 개인키(d_{ID})를 $(g_2(x_u h_v)^r, g^r, h_1^r, \dots, h_{v-1}^r, h_{v+1}^r, \dots, h_b^r)$ 로 계산한다.
- <27> 이러한 변환은 본 발명에 의한 암호화 기법이 총 $n(=ab)$ 명의 사용자를 다룰 수 있도록 해 준다. Bilinear Diffie-Hellman Exponent(BDHE) 가정 하에서 본 발명에 의한 암호화 기법의 안전성을 증명할 수 있다.
- <28> 이하, 본 발명의 기술적 과제의 해결 방안을 명확화하기 위한 발명의 구성을 본 발명의 바람직한 실시예에 근거하여 첨부 도면을 참조하여 상세히 설명하되, 도면의 구성요소들에 참조번호를 부여함에 있어서 동일 구성요소에 대해서는 비록 다른 도면상에 있더라도 동일 참조번호를 부여하였으며 당해 도면에 대한 설명시 필요한 경우 다른 도면의 구성요소를 인용할 수 있음을 미리 밝혀둔다.
- <29> 먼저 본 발명의 설명을 위해 사용되는 노테이션(notation)들은 다음과 같이 정의된다.
- <30> G : 위수가 p 인 곱셈 순환 그룹.
- <31> G_T : 위수가 p 인 곱셈 순환 그룹.
- <32> $e(,)$: 그룹 G 에서 정의되는 페어링(pairing) 함수.
- <33> Z_p : 위수가 p 인 그룹.
- <34> g : 그룹 G 의 생성원(generator).
- <35> α : 그룹 Z_p^* 에서 선택한 난수로 사용자의 비밀키를 생성하는데 사용.

- <36> h : G 그룹에서 선택한 난수로 공개키, 비밀키 및 암호화키를 생성하는데 사용.
- <37> x_u : G 그룹에서 선택한 난수로 공개키 및 비밀키를 생성하는데 사용. u 는 1에서 a 까지의 값을 갖는다.
- <38> y_v : G 그룹에서 선택한 난수로 공개키 및 비밀키를 생성하는데 사용. v 는 1에서 b 까지의 값을 갖는다.
- <39> i : 개별 사용자를 나타내는 정수 값으로 1에서 n 까지의 값을 가짐.
- <40> S : 전체 사용자 n 명중 정당한 사용자의 집단.
- <41> r : Z_p 그룹에서 선택한 난수. 사용자의 비밀키를 임의적으로(randomly) 생성하는데 사용.
- <42> s : Z_p 그룹에서 선택한 난수. 메시지 암호화키를 임의적으로 생성하는데 사용.
- <43> 도 1 내지 도 2는 본 시스템 발명의 바람직한 일실시예의 구성을 제시한 도면이고, 도 3은 본 방법 발명의 바람직한 일 흐름을 제시한 도면이다.
- <44> 키 생성부(11)는 메시지의 암호화 파라미터로 사용될 공개키(PK)와 각 사용자 $i(i \in \{1, \dots, n\})$ 의 비밀키(d_i)를 생성하며(S11), 키 분배부(12)는 생성된 공개키와 비밀키를 각 사용자 i 에게 분배하는데(S12), 공개키와 비밀키의 생성 및 분배는 다음과 같이 이루어진다.
- <45> 키 생성부(11)는 우선 위수가 p 인 두 그룹 G, G_T 를 설정하고 이들 두 그룹 간의 페어링 함수(pairing function) $e(,)$ 를 설정한다(S111). 페어링 함수는 사용자에게 전송할 메시지의 암호화에 필요한 암호화키 K 의 생성과 사용자(메시지 수신자)가 암호화된 메시지를 복호화하는데 필요한 키 K 를 암호화된 메시지로부터 추출하는데 이용하기 위해서 설정되는 것이다.
- <46> 키 생성부(11)는 다음으로 그룹 G 의 생성원 g 를 임의로 선택하고, 난수 a 를 선택하여 $g_1 = g^a$ 로 설정한다. 그리고 그룹 G 에 속하는 난수 $h, x_1, \dots, x_a, y_1, \dots, y_b$ 를 선택한다. 여기서 a 와 b 는 상기에서 언급한 노테이션(notation)과 같다. 키 생성부(11)는 상기한 생성원 및 난수들을 이용하여 공개키 PK를 다음과 같이 생성한다(S112).
- <47> $PK = (g, g_1 (=g^a), h, x_1, \dots, x_a, y_1, \dots, y_b)$.
- <48> 여기서 h 와 g_1 은 사용자에게 전송할 암호문(C_M)을 생성하는데 필요한 암호화키 K 의 생성에 이용하기 위해 삽입되는 것이며, g 는 암호문(C_M)에 부가시킬 헤더(Hdr)를 생성하기 위해 삽입되는 것이다.
- <49> 한편 본 발명에 의한 공개키 PK의 개수는 사용자의 수 즉, n 개만이 필요한데 이는 BGW 기법과 다른 점이다. BGW 기법에 의하면 n 명의 사용자에게 대해 $2n$ 개의 공개키가 필요하다.
- <50> 본 발명에 의한 기법과 BGW 기법의 공개키의 개수가 동일한 사용자 수에 대하여 다른 이유는 암호화키 K 를 생성하는 대수적 구조(algebraic structure)가 다르기 때문이다.
- <51> BGW 기법에 의한 암호화키 K 는 다음과 같이 생성된다.

<52>
$$K = (g^{(\alpha^i)}, (v \prod_{j \in S} g^{(\alpha^{n+1-j})})^z) / e(v \prod_{j \in S} g^{(\alpha^{n+1-j+i})}, g^z)$$
 --- 식 (1).

- <53> 이 식을 살펴보면, 분자에서 $g^{(ai)}$ 와 $g^{(an+1-j)}$ 가 페어링의 성질에 의해 지수끼리 곱해진다. 그러므로 $n+1-j+i$ 의 차수를 갖는 지수가 생기는데, 만일 $j=1$ 이고 $i=n$ 이면, $n+1-j+i=2n$ 이 된다. 또한 $j=n$ 이고 $i=1$ 이면 $n+1-j+i=2$ 가 된다. 따라서 이를 분모와 맞추어 주기 위해서는 $g_2, \dots, g_{2n}$ 의 거의 $2n$ 개의 원소가 필요하게 된다. 여기서 $g_i = g^{(ai)}$ 이다.

- <54> 반면 본 발명에 의한 암호화 기법에서 복호화키 K 는 다음과 같이 생성된다.

<55>
$$K = (h^\alpha \cdot (xy_i)^r \cdot \prod_{j \in S} k_{i,j}, g^z) / e((x \prod_{j \in S} y_j)^z, g^r)$$
 --- 식 (2).

- <56> 여기서 $k_{i,j}$ 는 상기 비밀키 $d_i = (h^{\alpha} \cdot (xy_i)^r, g^r, y_1^r, \dots, y_{i-1}^r, y_{i+1}^r, \dots, y_n^r)$ 인데(여기서 $k_{i,j} = y_j^r$ 이다), 저장된 n 개의 $k_{i,j}$ 값들을 가지고 복호를 수행할 수 있다.
- <57> 이 식에서 알 수 있는 바와 같이 본 발명에 의한 암호화 기법에서는 BGW 기법처럼 지수끼리 곱함으로써 분자와 분모의 차수를 동일하게 만드는 것이 아니고, 단순히 분자와 분모를 동일 차수를 갖는 형태로 세팅시키기만 하면 된다. 따라서 공개키 PK의 구현에 있어 $2n$ 개가 아닌 n 개의 원소만 있으면 된다.
- <58> 키 생성부(11)는 공개키 PK를 상기와 같이 생성한 후 각 사용자 i 가 전송받은 암호화 메시지를 추후 복호하는데 필요한 비밀키 d_i 를 생성한다(S113).
- <59> 비밀키 d_i 를 생성하기 위해서 먼저 $i = (u-1)b + v$ 를 만족하는 두 값 u, v 를 계산하고 그룹 Z_p 에 속하는 난수 r 을 선택한다. 여기서 u 는 메시지 수신자들을 분할하여 이루어진 각 수신자 그룹(즉, S 의 부분집합 S_u)의 인덱스(index)이며, v 는 각 사용자 i 의 부분집합 S_u 에서의 인덱스이다. 따라서 u 는 1에서 a 까지 값을, v 는 1에서 b 까지 값을 취하게 된다.
- <60> u 와 v 가 계산된 후 사용자 i 의 비밀키 d_i 는 다음과 같이 획득된다.
- <61> $d_i = (h^a * (x_u * y_v)^r, g^r, y_1^r, \dots, y_{v-1}^r, y_{v+1}^r, \dots, y_b^r)$.
- <62> 키 분배부(12)는 각 사용자 i 에게 공개키 PK와 생성된 비밀키 d_i 를 브로드캐스트(분배) 한다(S12).
- <63> 브로드캐스트 암호화의 파라미터로 사용될 공개키 PK와 각 사용자의 비밀키 d_i 를 생성하는 본 발명에 의한 방안은 본 발명의 배경이 되는 BGW 기법과 다음과 같은 차이를 가지고 있다.
- <64> 공개키의 사이즈(size) 측면에서, 본 발명에 의한 기법의 경우 공개키 PK는 위에 제시된 바와 같이 그룹 G 에 속하는 $(a+b+3)$ 개의 원소만을 이용하여 구현된다.
- <65> 이에 반하여 BGW-1 기법과 BGW-2 기법에 의한 공개키는 그룹 G 에 속하는 $(a+2b)$ 개의 원소를 이용하여 구현되므로, 공개키의 구현을 위해 본 발명에 의한 암호화 기법보다 b 개 정도 많은 원소가 필요하다. 따라서 본 발명에 의한 암호화 기법은 공개키 사이즈 측면에서 BGW 기법보다 이점을 보인다.
- <66> 예를 들어보면 전체 사용자의 수(n)를 1백만 명이라 하고 a, b 는 각각 1천으로 가정하자. 이 경우 한 개의 그룹 G 의 원소를 표현하기 위해서 필요한 데이터의 양이 대략 160 bit이기 때문에 BGW 기법의 경우 공개키의 크기는 최소 480 Kbit이다. 하지만 본 발명의 경우 320 Kbit이다. 따라서 기존 기법에 비하여 공개키의 크기가 33% 줄어든다.
- <67> 한편, BGW 기법에 의하면 사용자측 단말의 저장 장치에는 암호화 메시지의 복호를 위하여 사용자의 비밀키가 저장되고 아울러 공개키도 저장되어야 한다. 그러나 본 발명의 경우 사용자의 비밀키 d_i 는 위에 제시된 바와 같이 대략 $(b+1)$ 개(정확히는 $(b+1-r')$ 개)의 그룹 G 의 원소로 이루어져 있고 복호화를 위하여 추가적으로 공개키를 저장하고 있을 필요는 없다.
- <68> 즉, BGW 기법에서는 암호화 메시지의 복호를 위해 공개키 PK가 필요하기 때문에 수신자가 암호화 메시지를 복호하려면 자신의 단말에 공개키를 저장하고 있어야 한다. PKBE(Public Key Based Encryption) 기법을 채용한 암호화 기법에서는 복호의 신속성을 위해 일반적으로 수신자(사용자) 단말에 공개키가 개별적으로 저장된다.
- <69> 하지만 본 발명에 의한 암호화 기법에 의하면 암호화 메시지의 복호에 공개키가 필요 없이 비밀키만으로 복호를 할 수 있다. 본 발명에 의한 암호화 기법에 의하면 공개키는 메시지 송신자가 사용자들에게 메시지를 암호화하여 전송하는 경우에만 필요하다. 따라서 공개키를 별도로 저장할 필요가 없으며 본 발명에 의한 기법이 BGW 기법보다 총 저장량을 줄이는 효과를 볼 수 있다.
- <70> 이에 반해서 BGW-1 기법의 경우는 복호화를 위해서 필요한 공개키를 암호문에 모두 포함시켜 각 사용자에게 보내주어야 하기 때문에 암호문의 크기가 크게 늘어나고 따라서 공개키 저장량이 크게 늘어나게 된다.
- <71> 한편 BGW-2 기법의 경우 복호화에 필요한 공개키를 사용자 단말의 저장 장치에 저장하는 방식을 취하므로 공개키 저장량은 대략 $(2b+1)$ 개의 그룹 G 의 원소로 이루어진다. 그러므로 본 발명의 경우 BGW 기법에 비해 암호문

전송량 측면에서 이득을 볼 수 있고, 공개키 저장량 측면에서도 b개의 원소를 줄일 수 있는 이득을 볼 수 있다.

<72> 공개키 PK와 각 사용자 i의 비밀키 d_i 의 생성 및 분배가 이루어지면, 메시지 암호화/전송부(13)는 수신자들로부터 메시지 전송 요청을 받아 집합 S에 속하는 수신자(사용자)들에게 전송되는 메시지 M을 암호화하여 사용자에게 전송하는데(S13) 메시지 M에 대한 암호화는 다음과 같이 이루어진다.

<73> 우선 암호화키 생성부(131)는 Z_p 그룹에서 난수 s를 선택하여 메시지 암호화키 K를 다음과 같이 생성한다(S131). $K = e(h, g^s)$. 여기서 $e(,)$ 는 상기 설정된 페어링 함수를 의미한다.

<74> 다음으로 헤더 생성부(132)는 수신자 사용자들의 집합 S가 $S_1, \dots, S_a$ 의 부분집합으로 나누어진다고 가정할 때, 암호화 메시지의 헤더(Hdr)를 다음과 같이 생성한다(S132).

<75>
$$Hdr = ((x_1 * \prod_{j \in S_1} y_j)^s, \dots, (x_a * \prod_{j \in S_a} y_j)^s, g^s)$$

<76> 암호화 메시지 작성/브로드캐스팅부(133)는 대칭키 알고리즘을 이용하여 암호화키 K로 메시지 M을 암호화하여 암호문 C_M 을 작성하고(S133), 암호문 C_M 에 사용자 그룹(S)과 헤더(Hdr)를 부가한 암호화 메시지를 작성하여 수신자(사용자)들에게 브로드캐스트 한다(S134). 즉, $C_M = E_K(M)$ 이며, (S, Hdr, C_M)을 사용자에게 브로드캐스트(전송)한다.

<77> 본 발명이 제공하는 기법에 의한 메시지의 암호화는 BGW 기법에 비하여 다음과 같은 장점을 가진다. 본 발명의 경우 단지 (a+1)개의 그룹 G의 원소들만을 이용하여 암호문을 생성할 수 있다(Hdr이 (a+1)개의 원소로 구현되기 때문에).

<78> 이에 반해서 BGW-1 기법의 경우 위에서 언급한 바와 같이 암호문의 복호화를 위해 필요한 공개키를 암호문의 전송때마다 일일이 암호문에 모두 포함시켜 전송하기 때문에 헤더를 구현함에 (a+2b)개의 그룹 G의 원소가 필요하다.

<79> BGW-2 기법의 경우 본 발명의 경우와 마찬가지로 (a+1)개의 그룹 G의 원소만으로 암호문을 생성할 수 있으나, 공개키 저장량이 본 발명에 비하여 b개의 원소를 보다 많이 사용한다(본 발명의 경우 최소된 사용자수가 많으면 저장량을 더욱 줄일 수 있다). 따라서 본 발명의 기법은 암호문 전송량 내지는 공개키 저장량 측면에서 BGW 기법과 동일하거나 더욱 강점을 가진다.

<80> 각 사용자 i의 단말에 있는 복호화 모듈은 정당한 사용자 집합 S에 속하는 수신자(사용자)가 수신한 암호문 C_M 을 복호화(decryption)하는데 복호화는 다음과 같이 이루어진다(S14).

<81> 각 사용자(수신자) i는 부분집합 S_u 의 v번째 인덱스를 가지는 사용자이며, 자신의 비밀키가 $d_i = (d_{i,1}, d_{i,2}, k_{i,1}, \dots, k_{i,v-1}, k_{i,v+1}, \dots, k_{i,b})$ 이고, 송신자로부터 받은 암호화 메시지의 Hdr = $(A_1, \dots, A_a, B)$ 이다. 여기서 $d_{i,1}$ 은 상기한 $h * (x_u * y_v)^r$ 에, $d_{i,2}$ 는 상기한 g^r , $k_{i,1}$ 은 상기한 y_1^r 에, $k_{i,v-1}$ 은 상기한 y_{v-1}^r 에, $k_{i,v+1}$ 은 상기한 y_{v+1}^r 에, $k_{i,b}$ 은 상기한 y_b^r 에 각각 해당한다. 그리고 Hdr의 A_1 은 상기한 $(x_1 * \prod_{j \in S_1} y_j)^s$ 에, A_a 은 상기한 $(x_a * \prod_{j \in S_a} y_j)^s$ 에, B는 상기한 g^s 에 각각 해당한다.

<82> 각 사용자 i의 단말에 있는 복호화 모듈은 우선 메시지 암호화/전송부(13)로부터 전송받은 암호화 메시지에서 각 사용자 i에 대한 암호화키 K를 추출하는데(S141), 키 분배부(12)로부터 전송받은 비밀키 d_i 와 메시지 암호화/전송부(13)로부터 전송받은 헤더로부터 추출하며 구체적으로는 다음 식을 통해 추출한다.

<83>
$$K = e(d_{i,1} * \prod_{j \in S_u, j \neq v} k_{i,j}, B) / e(A_u, d_{i,2})$$

<84> K에 관한 이 식은 상기 제시된 식(2)와 동일하다.

<85> 여기서 $e(,)$ 는 상기 설정된 페어링 함수이다. 각 사용자 i의 단말에 있는 복호화 모듈은 추출된 암호화키 K로 대칭키 알고리즘을 이용하여 암호문 C_M 을 복호화하여 메시지 M을 복호한다(S142). 즉, $M = D_K(C_M)$.

<86> 이처럼 본 발명에 의한 암호화 기법은 BGW기법과는 다르게 PK를 메시지 M의 복호에 사용하지 않음을 알 수 있다.

<87> 간단한 실시예를 이용하여 본 발명에 의한 브로드캐스팅 암호화 기법을 설명하면 다음과 같다.

<88> 전체 사용자(수신자) 수 n은 25명으로 설정되었다고 가정하면 전체 사용자 25명은 5명씩의 소그룹(a=5)으로 나누어진다. 즉, 소그룹 $S_1, \dots, S_5$ 로 나누어지고 각 그룹에는 5명씩 포함이 된다(b=5).

<89> 키 생성부(11)는 그룹 G의 생성원 및 난수들을 이용하여 공개키 PK를 다음과 같이 생성한다.

<90> $PK = (g, g_1, h, x_1, x_2, x_3, x_4, x_5, y_1, y_2, y_3, y_4, y_5)$.

<91> 키 생성부(11)는 PK를 생성 후 각 사용자 $i (i \in \{1, \dots, 25\})$ 의 비밀키 d_i 를 생성하는데 우선 각 사용자 i 에 해당하는 u, v 를 구한다. 예를 들어 $i=24$ 인 경우 u, v 를 구하는 상기의 식에 의하면 $b=5$ 이므로 $u=5, v=4$ 이며, 따라서 $i=24$ 에 대한 비밀키 d_{24} 는 다음과 같이 생성된다.

<92> $d_{24} = (h^a * (x_5 * y_4)^r, g^r, y_1^r, y_2^r, y_3^r, y_5^r)$.

<93> 생성된 공개키 PK와 비밀키 d_i 는 키 분배부(12)에 의해 각 사용자에게 분배된다.

<94> 메시지 암호화/전송부(13)는 집합 S에 속하는 수신자 사용자에게 전송되어야 할 메시지 M을 암호화하여 사용자에게 전송하는데, 송신측의 암호화키 설정부(131)는 Z_p 그룹에서 난수 s 를 선택하여 메시지 암호화키 K를 다음과 같이 설정한다. $K = e(h, g^s)$.

<95> 헤더 생성부(132)는 사용자들의 집합 S가 $S_1, \dots, S_5$ 의 부분집합으로 나누어지므로, 암호화 메시지의 헤더(Hdr)를 다음과 같이 생성한다.

$$Hdr = ((x_1 * \prod_{j \in S_1} y_j)^s, (x_2 * \prod_{j \in S_2} y_j)^s, (x_3 * \prod_{j \in S_3} y_j)^s, (x_4 * \prod_{j \in S_4} y_j)^s, (x_5 * \prod_{j \in S_5} y_j)^s, g^s).$$

<96>

<97> 암호화 메시지 작성/브로드캐스팅부(133)는 대칭키 알고리즘을 이용하여 암호화키 K로 메시지 M을 암호화하여 암호문 C_M 을 작성하고, 암호문 C_M 에 사용자 집합(S)과 상기 헤더를 부가한 암호화 메시지를 작성하여 수신자(사용자)들에게 브로드캐스트 한다.

<98> 각 사용자 i 의 단말에 있는 복호화 모듈은 정당한 사용자 집합 S에 속하는 수신자(사용자)가 수신한 암호문 C_M 을 복호화(decryption)한다.

<99> 각 사용자(수신자) i 는 부분집합 S_u 의 v 번째 인덱스를 가지는 사용자이며, $i=24$ 인 사용자인 경우 비밀키가 $d_{24} = (d_{24,1}, d_{24,2}, k_{24,1}, k_{24,2}, k_{24,3}, k_{24,5})$ 이고, 송신자로부터 받은 암호화 메시지의 $Hdr = (A_1, \dots, A_5, B)$ 이다. 여기서 $d_{24,1}$ 은 상기한 $h * (x_5 * y_4)^r$ 에, $d_{24,2}$ 는 상기한 g^r , $k_{24,1}$ 은 상기한 y_1^r 에, $k_{24,3}$ 은 상기한 y_3^r 에, $k_{24,5}$ 는 상기한 y_5^r 에 각각 해당한다. 그리고 Hdr의 A_1 은 상기한 $(x_1 * \prod_{j \in S_1} y_j)^s$ 에, A_5 는 상기한 $(x_5 * \prod_{j \in S_5} y_j)^s$ 에, B는 상기한 g^s 에 각각 해당한다.

<100> 각 사용자 i 의 단말에 있는 복호화 모듈은 메시지 암호화/전송부(12)로부터 전송받은 암호화 메시지에서 각 사용자 i 에 대한 암호화키 K를 추출한다. $i=24$ 인 경우의 암호화키는 다음과 같이 추출된다.

$$K = e(d_{24,1} * \prod_{j \in S_5, j \neq 4} k_{24,j}, B) / e(A_5, d_{24,2})$$

<101>

<102> 여기서 $e(,)$ 는 상기 설정된 페어링 함수이다. 각 사용자 i 의 단말에 있는 복호화 모듈은 추출된 암호화키 K로 대칭키 알고리즘을 이용하여 암호문 C_M 을 복호화하여 메시지 M을 복호화한다. 즉, $M = D_K(C_M)$.

<103> 다음 표는 전송량, 저장량, 계산량 그리고 공개키 사이즈 측면에서 본 발명의 성능을 BGW 기법과 비교하여 제시한 표이다. 총 사용자 수는 $n(=a*b)$ 명 이다. 먼저 표에서 나타난 기호를 설명하면 다음과 같다.

<104> G : G 그룹의 원소, $r' = \min(r_1, \dots, r_a)$, r : 사용자 그룹 내의 총 탈퇴자 수.

	암호문 전송량	공개키 저장량	공개키 사이즈
BGW-1	$(a+2b)G + r \log_2 n$	$1G$	$(a+2b)G$
BGW-2	$(a+1)G + r \log_2 n$	$(2b+1)G$	$(a+2b)G$
본 발명	$(a+1)G + r \log_2 n$	$(b+1-r')G$	$(a+b+3)G$

<105>

<106> BGW-1, BGW-2는 상기한 BGW 기법의 두 가지 버전이다. 상기 표에 제시된 바와 같이 본 발명의 암호화 기법에 의한 암호문 전송량, 공개키 저장량과 공개키 사이즈는 BGW 기법에 의해 동일하거나 더욱 향상되었음을 알 수 있다.

<107> 본 방법발명은 또한 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다.

<108> 컴퓨터가 읽을 수 있는 기록매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 인터넷을 통한 전송)의 형태로 구현되는 것도 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

<109> 이제까지 본 발명에 대하여 그 바람직한 실시예를 중심으로 살펴보았다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다.

<110> 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 균등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

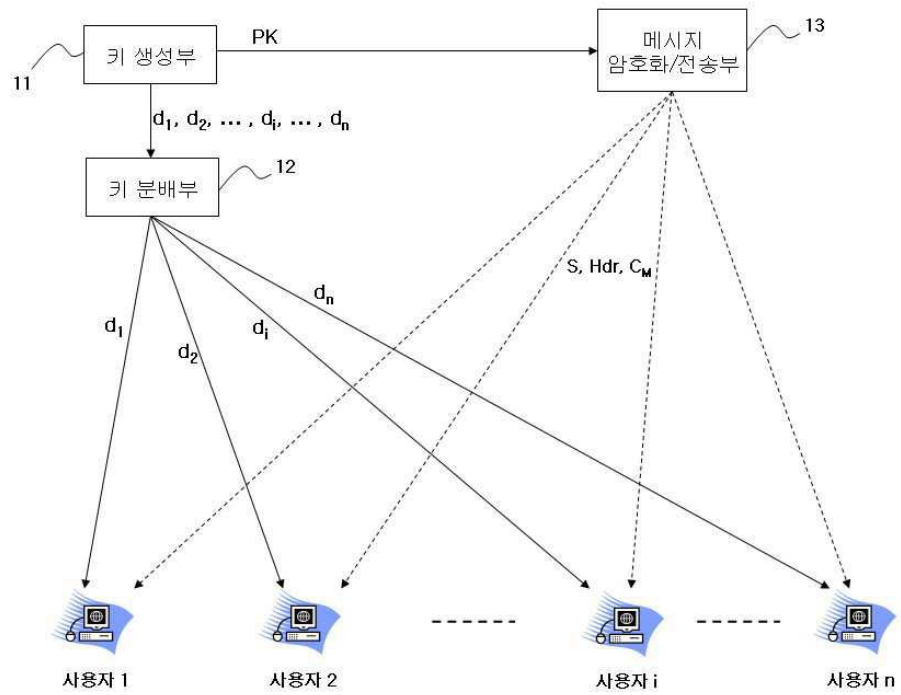
도면의 간단한 설명

<111> 도 1 과 도 2는 본 시스템 발명의 바람직한 일실시예의 구성을 제시한 도면이다.

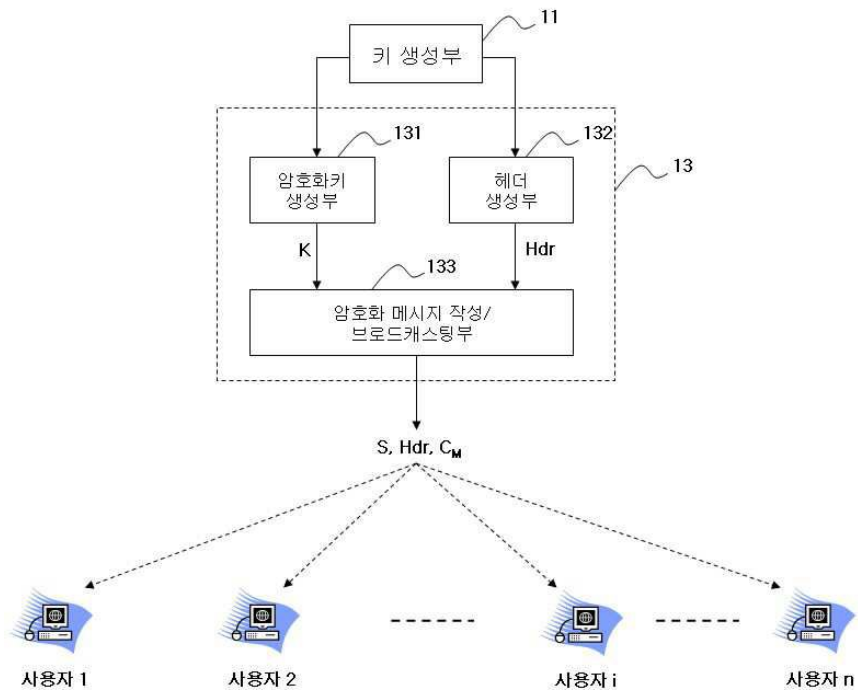
<112> 도 3은 본 방법 발명의 바람직한 일 흐름을 제시한 도면이다.

도면

도면1



도면2



도면3

