(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2010년07월07일
(11) 등록번호 10-0968181
(24) 등록일자 2010년06월29일

(51) Int. Cl.
H04B 7/26 (2006.01) *H04L 29/06* (2006.01)
(21) 출원번호 10-2006-7023089
(22) 출원일자(국제출원일자) 2005년06월22일
심사청구일자 2008년03월28일
(85) 번역문제출일자 2006년11월03일
(65) 공개번호 10-2007-0026495
(43) 공개일자 2007년03월08일
(86) 국제출원번호 PCT/EP2005/052924
(87) 국제공개번호 WO 2006/000566
국제공개일자 2006년01월05일
(30) 우선권주장
0414253.5 2004년06월24일 영국(GB)
0414254.3 2004년06월24일 영국(GB)
(56) 선행기술조사문헌
Secure Group Communications Using Key Graphs, IEEE/ACM Transactions On Networking, Vol. 8, No. 1, February 2000.
전체 청구항 수 : 총 7 항

(73) 특허권자
인터내셔널 비지네스 머신즈 코포레이션
미국 10504 뉴욕주 아몬크 뉴오차드 로드
(72) 발명자
카멜리 보아즈
이스라엘 코라닛 20181 코라닛 27
듀이게난 존 저스틴
영국 도르셋 비에이치1 4디에이 번마우스 크리스트처치 로드 80린덴 홀 27
(뒷면에 계속)
(74) 대리인
김태홍, 신정건

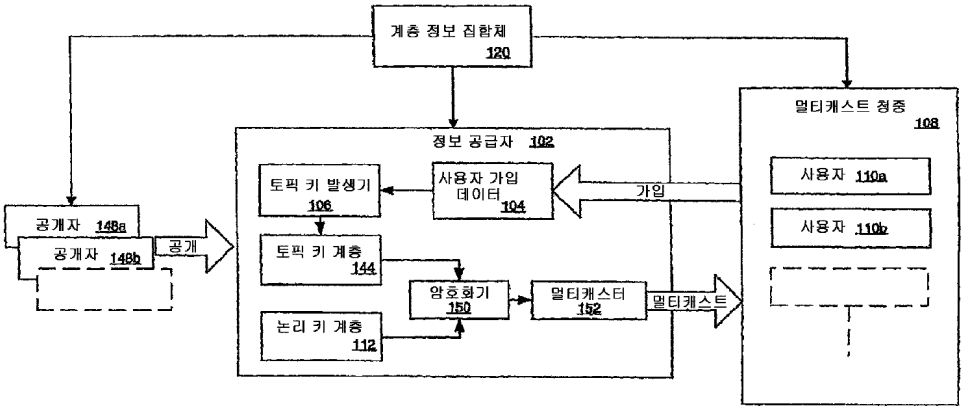
심사관 : 박성웅

(54) 멀티캐스트를 통한 액세스 제어

(57) 요 약

토픽의 집합 중 임의의 토픽에 대해 공개된 정보를 그 토픽에 대한 하나 이상의 인증된 가입자에게 통신하기 위한 멀티캐스트 호스트를 제공하는데, 상기 토픽의 집합은 하나 이상의 분할 요소로 분할되고, 각 분할 요소는 서로 관련된 분할 요소 암호화 키를 가지며, 상기 하나 이상의 분할 요소는 각각 토픽 집합의 서로소 진 부분집합이며, 상기 멀티캐스트 호스트는 토픽과 관련된 정보를 수신하는 수단과; 토픽용의 분할 요소를 결정하는 수단과; 분할 요소와 관련된 분할 요소 암호화 키를 검색하는 수단과; 정보를 검색된 분할 요소 암호화 키로 암호화하는 수단과; 정보를 하나 이상의 인증된 가입자에게 통신하는 수단을 포함한다.

대 표 도



(72) 발명자

엘데르 마이클 다메인

미국 노스캐롤라이나주 27713 더햄 코트니 크릭 불바드 3100아파트먼트 316

게르신스키 기드온

이스라엘 하이파 34780 코이프만 스트리트 16/2

특허청구의 범위

청구항 1

토픽(topic)의 집합 중 임의의 토픽에 대해 공개된 정보를 그 토픽에 대한 하나 이상의 인증된 가입자에게 통신하기 위한 멀티캐스트 호스트(multicast host)로서, 상기 토픽의 집합은 하나 이상의 분할 요소로 분할되고, 각 분할 요소는 서로 관련된 분할 요소 암호화 키를 가지며, 상기 하나 이상의 분할 요소는 각각 토픽 집합의 서로소 진 부분집합(disjoint proper subset)인 멀티캐스트 호스트에 있어서,

토픽과 관련된 정보를 수신하는 수단과;

토픽용의 분할 요소를 결정하는 수단과;

분할 요소와 관련된 분할 요소 암호화 키를 검색하는 수단과;

정보를 검색된 분할 요소 암호화 키로 암호화하는 수단과;

정보를 하나 이상의 인증된 가입자에게 통신하는 수단

을 포함하는 멀티캐스트 호스트.

청구항 2

삭제

청구항 3

삭제

청구항 4

삭제

청구항 5

삭제

청구항 6

제1항에 있어서, 분할 요소 암호화 키를 하나 이상의 가입자에게 안전하게 통신하는 수단을 더 포함하는 멀티캐스트 호스트.

청구항 7

삭제

청구항 8

삭제

청구항 9

제1항에 있어서, 분할 요소 복호 키를 하나 이상의 인증된 가입자에게 안전하게 통신하기 위한 수단을 더 포함하고,

상기 분할 요소 복호 키는 분할 요소 암호화 키에 대응하는 것인 멀티캐스트 호스트.

청구항 10

삭제

청구항 11

삭제

청구항 12

제1항에 있어서, 분할 요소의 토픽에 대한 새로운 가입을 수신하는 수단과;

분할 요소를 위한 새로운 분할 요소 암호화 키를 발생하는 수단을 더 포함하는 멀티캐스트 호스트.

청구항 13

삭제

청구항 14

삭제

청구항 15

삭제

청구항 16

멀티캐스트 시스템에 있어서,

청구항 제1항에 따른 멀티캐스트 호스트와;

상기 멀티캐스트 호스트에 의해 통신된 정보를 수신하기 위한 하나 이상의 멀티캐스트 가입자

를 포함하는 멀티캐스트 시스템.

청구항 17

삭제

청구항 18

토픽의 집합 중 임의의 토픽에 대해 공개된 정보를 그 토픽에 대한 하나 이상의 인증된 가입자에게 통신하기 위한 방법으로서, 상기 토픽의 집합은 하나 이상의 분할 요소로 분할되고, 각 분할 요소는 서로 관련된 분할 요소 암호화 키를 가지며, 상기 하나 이상의 분할 요소는 각각 토픽 집합의 서로소 진 부분집합(disjoint proper subset)인 정보 통신 방법에 있어서,

토픽과 관련된 정보를 수신하는 단계와;

토픽용의 분할 요소를 결정하는 단계와;

분할 요소와 관련된 분할 요소 암호화 키를 검색하는 단계와;

정보를 검색된 분할 요소 암호화키로 암호화하는 단계와;

정보를 하나 이상의 인증된 가입자에게 통신하는 단계

를 포함하는 것인 정보 통신 방법.

청구항 19

삭제

청구항 20

삭제

청구항 21

삭제

청구항 22

삭제

청구항 23

삭제

청구항 24

삭제

청구항 25

삭제

청구항 26

삭제

청구항 27

삭제

청구항 28

삭제

청구항 29

삭제

청구항 30

삭제

청구항 31

삭제

청구항 32

삭제

청구항 33

삭제

청구항 34

삭제

청구항 35

삭제

청구항 36

삭제

청구항 37

삭제

청구항 38

삭제

청구항 39

삭제

청구항 40

삭제

청구항 41

삭제

청구항 42

삭제

청구항 43

삭제

청구항 44

삭제

청구항 45

삭제

청구항 46

삭제

청구항 47

삭제

청구항 48

삭제

청구항 49

삭제

청구항 50

삭제

청구항 51

삭제

청구항 52

삭제

청구항 53

삭제

청구항 54

삭제

청구항 55

삭제

청구항 56

삭제

청구항 57

삭제

청구항 58

삭제

청구항 59

삭제

청구항 60

삭제

청구항 61

삭제

청구항 62

삭제

청구항 63

데이터 처리 시스템에서 실행될 때 데이터 처리 시스템이 청구항 제18항에서 청구된 정보 통신 방법을 수행하도록 명령하는, 컴퓨터 판독가능한 기록 매체에 저장된 컴퓨터 프로그램 코드를 포함하는 컴퓨터 프로그램을 기록한 컴퓨터 판독가능한 기록 매체.

청구항 64

삭제

명 세 서

기 술 분 야

[0001] 본 발명은 공개된 정보에 대한 액세스 제어와 관련이 있다. 특히, 본 발명은 멀티캐스트 공개/가입 시스템에서의 액세스 제어와 관련이 있다.

배 경 기 술

[0002] 공개/가입 시스템(publish/subscribe system)에서, 정보는 계층적 정보 집합체라고 알려진 토픽(topic)의 계층(hierarchy)으로서 구성될 수 있다. 사용자는 하나 이상의 토픽에 대해 공개된 정보를 수신하기 위해 가입할 수 있다. 정보가 정보 집합체 내의 토픽에 대해 공개된 때, 정보 공급자는 토픽에 가입된 사용자의 부분집합(subset)만이 메시지에 액세스할 수 있게 하는 방식으로 일련의 사용자에게 정보를 메시지로서 안전하게 통신한다. 메시지가 안전하게 통신되고 가입된 사용자에 의해서만 액세스될 수 있게 하기 위해 정보 공급자는 공중/사설 키 암호화와 같은 키 기반 암호화 방법을 이용하여 메시지를 암호화할 필요가 있다.

[0003] 공개 정보가 가입된 사용자에게만 액세스 가능하도록 보장하는 한가지 방법은 유니캐스트(unicast) 공개/가입 시스템을 이용하는 것이다. 유니캐스트 시스템에서, 정보 공급자는 정보가 공개되는 토픽에 가입된 일련의 사용자를 결정한다. 가입된 사용자 각각에 대하여, 정보 공급자와 가입된 사용자 간의 통신 채널은 공개된 정보를 메시지로서 가입된 사용자에게 전달하기 위해 사용된다. 통신 채널은 가입된 사용자용의 키 및 각각의 가입된 사용자에 대해 존재하는 별도의 통신 채널을 이용하여 안전하게 된다. 이 방법으로, 공개된 정보는 별도의 통신 채널을 이용하여 각각의 가입된 사용자에게 안전하게 전달되고, 그래서 가입된 사용자만이 공개된 정보를 수신하고 그 정보에 액세스할 수 있게 보장된다. 유니캐스트 공개/가입 시스템은 통신 채널이 각각의 가입된 사용자용으로 존재하여야 하고 공개된 정보가 각 사용자에 대하여 별도로 통신되어야 한다는 단점을 갖는다.

[0004] 유니캐스트 공개/가입 시스템에 대안적인 것으로서 각 사용자에 대한 별도의 통신 채널을 포함하지 않는 멀티캐스트(multicast) 공개/가입 시스템이 있다. 멀티캐스트 시스템에서, 공개 정보는 잠재적으로 비가입 사용자를 포함한 다수의 사용자에게 공통인 통신 채널을 통해 가입 사용자에게 메시지로서 통신된다. 메시지가 가입 사용자에게만 액세스가능한 것을 보장하기 위하여, 메시지는 각 사용자에게 특수한 키를 이용하여 각각의 가입 사용자용으로 1회 암호화된다. 가입 사용자용으로 1회 암호화된 후, 메시지는 공동 통신 채널을 통하여 통신된다. 메시지가 특정 사용자용으로 암호화되었을 때 그 특정 사용자만이 자신의 특수 키를 이용하여 공개 정보에 액세스할 수 있다. 이러한 멀티캐스트 공개/가입 시스템은 공개 정보를 포함한 메시지가 각 가입 사용자용으로 1회 암호화되고 안전하게 통신되어야 한다는 단점을 갖는다. 이것은 특히 가입 사용자가 많은 경우에 자원 집약적(resource intensive)이다.

[0005] "키 그래프를 이용한 안전한 그룹 통신"(Secure Group Communications Using Key Graphs)이라는 명칭의 논문[웡(Wong) 외, IEEE/ACM Transactions on Networking, 제8권, 제1호, 2000년 2월, 16-30페이지]에서는 논리 키 계층(logical key hierarchy)이라고 알려진 키 계층을 이용함으로써 상기 문제점들을 부분적으로 경감한 기술이 개시되어 있다. 웡(Wong) 등의 논문은 멀티캐스트 청중(audience) 내의 사용자를 논리 나무(logical tree)의 잎 노드(leaf node)로서 나타내는 것에 대하여 설명하고 있다. 각 노드는 키(key)를 포함하고, 각 사용자는 나무의 잎으로부터 뿌리까지의 경로에 있는 모든 키에 대하여 알고 있다. 정보가 공개된 때, 정보 공급자는 그 정보를 멀티캐스트 통신 채널을 통하여 메시지로서 통신한다. 통신 전에, 메시지는 랜덤 키(K_r)를 이용하여 암호화된다. 그 다음에, 정보 공급자는 랜덤 키(K_r)를 암호화하기 위해 사용할 수 있는 키의 집합을 결정한다. 여기에서, 상기 키 집합은 일련의 가입 사용자에 대응하는 것이다. 따라서, 메시지는 랜덤 키(K_r)를 이용하여 1회만 암호화되고, 한편, 랜덤 키는 가입 사용자에 대응하는 키 집합을 이용하여 복수회 암호화된다. 논리 나무의 가지의 모든 사용자들이 공개 정보의 가입자인 때, 나무의 가지를 나타내는 노드의 키는 랜덤 키(K_r)를 암호화하기 위해 사용될 수 있다. 이 방법에서, 랜덤 키(K_r)는 각 가입 사용자용의 개별 키를 이용하여 암호화될 필요가 없다. 그러므로, 웡 등이 설명하는 논리 키 계층 방법은 공개 정보 메시지를 1회 이상 암호화할 필요성을 제거하고 일련의 가입 사용자를 수용하기 위해 필요한 키 집합을 감소시킴으로써 멀티캐스트 통신 채널을 통한 안전한 공개/가입 분배로 상기 문제점들을 경감한다.

[0006] 논리 키 계층 방법이 단순한 공개 정보 구조에는 효과적이지만, 이것은 각 공개 정보 메시지에 대하여 랜덤 키(K_r)의 발생을 요구한다는 점에서 단점이 있다. 정보를 빈번하게 공개하는 하이 볼륨 시스템(high volume system)에서, 랜덤 키의 반복적인 발생은 자원 집약적일 수 있다. 이것은 사용자가 정보 집합체(information aggregate)에서 특별하고 구체적인 토픽에 대한 매우 미세한 입상 가입(grained subscription)을 가질 수 있고 공개 정보 메시지의 수가 높을 수 있는 계층적 정보 집합체에 특히 관련이 있다. 예를 들어서, 사용자는 각각의 사용자가 포트폴리오의 특수한 주식에 대한 스톡 쿼트(stock quote) 정보에 대응하는 계층적 정보 집합체의 토픽에 가입하는 스톡 쿼트 시스템과 같이, 다른 사용자들과는 매우 상이한 특수한 가입 이익을 가질 수 있다.

[0007] 그러므로, 계층적 정보 집합체에서 공개된 정보의 각 공개 정보 메시지용의 랜덤 키를 발생할 필요없이 멀티캐스트 통신 채널을 통해 공개 정보를 안전하게 통신하는 것이 유리하다.

발명의 상세한 설명

[0008] 따라서, 본 발명은, 제1 태양에서, 토픽의 집합 중 임의의 토픽에 대해 공개된 정보를 그 토픽에 대한 하나 이상의 인증된 가입자에게 통신하기 위한 멀티캐스트 호스트를 제공하는데, 상기 토픽 집합은 하나 이상의 분할 요소(partition element)로 분할되고, 각 분할 요소는 서로 관련된 분할 요소 암호화 키를 가지며, 상기 하나 이상의 분할 요소는 각각 토픽 집합의 서로소 진 부분집합(disjoint proper subset)이며, 상기 호스트는 토픽과

관련된 정보를 수신하는 수단과; 토픽용의 분할 요소를 결정하는 수단과; 분할 요소와 관련된 분할 요소 암호화 키를 검색하는 수단과; 정보를 검색된 분할 요소 암호화키로 암호화하는 수단과; 정보를 하나 이상의 인증된 가입자에게 통신하는 수단을 포함한다.

[0009] 따라서, 본 발명은 토픽에 대해 공개된 정보가 멀티캐스트 메시지용의 랜덤 키를 발생할 필요없이 토픽 키를 이용하여 암호화되는 장점을 제공한다. 토픽용의 토픽 키는 그 토픽에 가입된 사용자만이 토픽 키에 액세스할 수 있도록 분배된다.

[0010] 바람직하게, 토픽 집합의 각각의 서로소 진 부분집합은 액세스 제어 리스트에 따라 정의된다.

[0011] 바람직하게, 액세스 제어 리스트는 복수의 롤(role)에 대한 정의를 포함한다.

[0012] 바람직하게, 복수의 롤 각각은 토픽 집합의 부분집합이다.

[0013] 바람직하게, 토픽 집합의 각각의 서로소 진 부분집합은 복수의 롤의 차집합 및 교집합 중의 하나가 되도록 정의된다.

[0014] 바람직하게, 멀티캐스트 호스트는 분할 요소 암호화 키를 하나 이상의 가입자에게 안전하게 통신하는 수단을 더 포함한다.

[0015] 바람직하게, 분할 요소 암호화 키는 분할 요소 암호화 키를 암호화함으로써 안전하게 통신된다.

[0016] 바람직하게, 분할 요소 암호화 키는 논리 키가 하나 이상의 인증된 가입자에게 대응하는 논리 키 계층을 이용하여 암호화된다.

[0017] 바람직하게, 멀티캐스트 호스트는 분할 요소 복호 키를 하나 이상의 인증된 가입자에게 안전하게 통신하기 위한 수단을 더 포함하고, 상기 분할 요소 복호 키는 분할 요소 암호화 키에 대응한다.

[0018] 바람직하게, 분할 요소 복호 키는 분할 요소 복호 키를 암호화함으로써 안전하게 통신된다.

[0019] 바람직하게, 분할 요소 복호 키는 논리 키가 하나 이상의 인증된 가입자에 대응하는 논리 키 계층을 이용하여 암호화된다.

[0020] 바람직하게, 멀티캐스트 호스트는 분할 요소의 토픽에 대한 새로운 가입을 수신하는 수단과; 분할 요소용의 새로운 분할 요소 암호화 키를 발생하는 수단을 더 포함한다.

[0021] 바람직하게, 멀티캐스트 호스트는 새로운 분할 요소 암호화 키에 대응하는 새로운 분할 요소 복호 키를 발생하는 수단을 더 포함한다.

[0022] 바람직하게, 멀티캐스트 호스트는 분할 요소의 토픽에 대한 가입 취소를 수신하는 수단과; 분할 요소에 대한 새로운 분할 요소 암호화 키를 발생하는 수단을 더 포함한다.

[0023] 바람직하게, 멀티캐스트 호스트는 새로운 분할 요소 암호화 키에 대응하는 새로운 분할 요소 복호 키를 발생하는 수단을 더 포함한다.

[0024] 따라서, 본 발명은, 제2 태양에서, 제1 태양에 따른 멀티캐스트 호스트; 및 멀티캐스트 호스트에 의해 통신된 정보를 수신하기 위한 하나 이상의 멀티캐스트 가입자를 포함하는 멀티캐스트 시스템을 제공한다.

[0025] 따라서, 본 발명은, 제3 태양에서, 토픽의 집합 중 임의의 토픽에 대해 공개된 정보를 그 토픽에 대한 하나 이상의 인증된 가입자에게 통신하기 위한 방법을 제공하는데, 상기 토픽 집합은 하나 이상의 분할 요소로 분할되고, 각 분할 요소는 서로 관련된 분할 요소 암호화 키를 가지며, 상기 하나 이상의 분할 요소는 각각 토픽 집합의 서로소 진 부분집합이며, 상기 호스트는 토픽과 관련된 정보를 수신하는 단계와; 토픽용의 분할 요소를 결정하는 단계와; 분할 요소와 관련된 분할 요소 암호화 키를 검색하는 단계와; 정보를 검색된 분할 요소 암호화키로 암호화하는 단계와; 정보를 하나 이상의 인증된 가입자에게 통신하는 단계를 포함한다.

[0026] 따라서, 본 발명은, 제4 태양에서, 데이터 처리 시스템에서 실행될 때 데이터 처리 시스템이 상기 제3 태양에서 설명한 방법을 수행하도록 명령하는, 컴퓨터 판독가능 기억 매체에 저장된 컴퓨터 프로그램 코드를 포함한 컴퓨터 프로그램 제품을 제공한다.

[0027] 따라서, 본 발명은, 제5 태양에서, 컴퓨터가 이용가능한 매체에 저장되어 토픽의 집합 중 임의의 토픽에 대해 공개된 정보를 그 토픽에 대한 하나 이상의 인증된 가입자에게 통신하기 위한 컴퓨터 프로그램 제품을 제공하는데, 상기 토픽 집합은 하나 이상의 분할 요소로 분할되고, 각 분할 요소는 서로 관련된 분할 요소 암호화 키를

가지며, 상기 하나 이상의 분할 요소는 각각 토픽 집합의 서로소 진 부분집합이며, 상기 컴퓨터 프로그램 제품은 토픽과 관련된 정보를 수신하기 위한 컴퓨터 판독가능한 프로그램 수단과; 토픽용의 분할 요소를 결정하기 위한 컴퓨터 판독가능한 프로그램 수단과; 분할 요소와 관련된 분할 요소 암호화 키를 검색하기 위한 컴퓨터 판독가능한 프로그램 수단과; 정보를 검색된 분할 요소 암호화키로 암호화하기 위한 컴퓨터 판독가능한 프로그램 수단과; 정보를 하나 이상의 인증된 가입자에게 통신하기 위한 컴퓨터 판독가능한 프로그램 수단을 포함한다.

실 시 예

[0052] 도 1a는 멀티캐스트 정보 공급자(102)를 포함한 멀티캐스트 공개/가입 시스템을 나타내는 개략적 블록도이다. 멀티캐스트 공개/가입 시스템에서, 공개자(publisher)(148a, 148b)는 계층 정보 집합체(120) 내의 토픽에 대한 정보를 공개하는 장치 또는 엔티티의 하드웨어 또는 소프트웨어 설비이다. 계층 정보 집합체(120)는 정보가 공개될 수 있는 계층적으로 배열된 토픽의 논리 구조이고, 이것에 대해서는 도 1b와 관련하여 뒤에서 자세히 설명된다. 공개자(148a, 148b)에 의해 공개된 정보는 공개자들(148a, 148b) 사이의 통신 채널을 통하여 정보 공급자(102)에게 통신된다. 이러한 통신 채널의 예로는 유선 또는 무선 컴퓨터 네트워크가 있고, 당업자라면 공개자(148a, 148b)와 정보 공급자(102) 간에 임의의 통신 채널이 사용될 수 있음을 알 수 있을 것이다.

[0053] 정보 공급자(102)는 공개자(148a, 148b)로부터 공개 정보를 수신하는 장치 또는 엔티티의 하드웨어 또는 소프트웨어 설비이다. 정보 공급자는 공개 정보를 멀티캐스트 메시지로서 멀티캐스트 청중(108)에게 통신하기 위한 하드웨어 또는 소프트웨어 장치 또는 엔티티인 멀티캐스터(152)를 포함한다. 멀티캐스트 메시지는 네트워크 상의 복수의 장치 또는 사용자에게 보내지고 이는 당업계에 잘 알려져 있다. 예를 들면, 멀티캐스터(152)는 멀티캐스트 청중(108)에게 멀티캐스트 메시지를 보내도록 구성된 응용 소프트웨어이다. 멀티캐스트 청중(108)은 사용자(110a, 110b)의 집합이다. 사용자(110a, 110b)는 정보 공급자(102)로부터의 공개 정보에 대응하는 멀티캐스트 메시지를 수신하도록 구성된 장치 또는 엔티티의 하드웨어 또는 소프트웨어 설비이다. 예를 들면, 정보 공급자(102)는 멀티캐스트 청중(108)에 통신적으로 접속된 컴퓨터 시스템일 수 있고, 공개 정보는 바이너리 데이터 등의 데이터일 수 있다. 정보 공급자(102)와 멀티캐스트 청중(108) 간의 접속의 일 예는 컴퓨터 네트워크이다. 사용자(110a, 110b)는 가입 요구를 정보 공급자(102)에게 보냄으로써 계층적 정보 집합체(120) 내의 하나 이상의 토픽에 가입할 수 있다. 정보 공급자(102)는 계층적 정보 집합체(120) 내의 토픽에 대한 사용자(110a, 110b)의 가입에 관한 정보를 저장하는 사용자 가입 데이터(104)를 포함한다. 예를 들어서, 만일 사용자(110a)가 계층적 정보 집합체(120)의 특수 토픽에 가입되면, 이 가입은 사용자의 식별(identification)과 토픽의 식별을 포함해서 사용자 가입 데이터(104)에 기록된다. 사용자 가입 데이터(104)는 데이터베이스에 기록될 수 있다. 대안적으로, 사용자 가입 데이터(104)는 컴퓨터 시스템의 메모리에 기록될 수 있고 또는 컴퓨터 시스템의 기억 장치에 파일로서 기록될 수 있다. 당업자라면 사용자 가입 데이터(104)를 저장하기 위한 다른 적당한 수단이 사용될 수 있음을 알 것이다.

[0054] 정보 공급자(102)는 토픽 키 발생기(106), 토픽 키 계층(144), 논리 키 계층(112) 및 암호화기(encrypter)(150)를 또한 포함한다. 토픽 키 발생기는 당업계에 잘 알려져 있는 바와 같이 공중/사설 키 암호화를 위해 필요한 공중 키(public key) 및 사설 키(private key)와 같은 암호화키를 발생하기 위한 하드웨어 또는 소프트웨어 장치 또는 엔티티이다. 토픽 키 발생기(106)의 예로는 "프리티 굿 프라이버시"(Pretty Good Privacy)(PGP) 제품(프리티 굿 프라이버시 및 PGP는 PGP 코포레이션의 등록 상표이다)이 있다. 토픽 키 발생기(106)는 계층 정보 집합체(120)의 각 토픽에 대하여 키를 발생하고, 그 키를 토픽 키 계층(144)에 저장한다. 토픽 키 계층(114)에 대해서는 도 1c를 참조하여 뒤에서 자세히 설명한다. 논리 키 계층(112)은 잘 알려져 있는 바와 같이 키의 논리 나무 구조이고, 이것에 대해서는 도 1d를 참조하여 뒤에서 자세히 설명한다. 암호화기(150)는 하나 이상의 암호화 키를 이용하여 데이터 아이템의 암호화 버젼을 발생하는 하드웨어 또는 소프트웨어 장치 또는 엔티티이다. 예를 들어서, 암호화기(150)는 공중 암호화 키를 이용하여 데이터의 아이템을 암호화할 수 있다. 암호화기(150)의 예로는 "프리티 굿 프라이버시"(PGP) 제품이 있다.

[0055] 도 1a에서, 멀티캐스트 청중(108)은 2개의 사용자를 갖는 것으로 도시되어 있지만, 당업자라면 임의의 복수의 사용자가 멀티캐스트 청중(108)을 구성할 수 있다는 것을 알 것이다. 유사하게, 단지 2개의 공개자(148a, 148b)가 도시되어 있지만, 당업자라면 임의의 복수의 공개자가 상기 멀티캐스트 공개/가입 시스템에서 정보를 공개할 수 있다는 것을 알 것이다.

[0056] 도 1b는 도 1a의 계층 정보 집합체(120)의 예를 도시한 것이다. 계층 정보 집합체(120)는 도시를 생략한 장치의 기억 장치 또는 메모리에 저장되고, 각각의 공개자(148a, 148b), 정보 공급자(102) 및 멀티캐스트 청중(108) 내의 사용자(110a, 110b)에게 액세스 가능하다. 대안적으로, 계층 정보 집합체(120)는 임의의 하나 또는 복수의

공개자(148a, 148b), 정보 공급자(102) 또는 멀티캐스트 청중(108) 내의 사용자(110a, 110b)의 기억 장치 또는 메모리에 저장되고 이들 장치 또는 엔티티의 각각에 액세스될 수 있다. 계층 정보 집합체(120)는 토픽 "뉴스"(122), 토픽 "재정"(124), 토픽 "스포츠"(126), 토픽 "사업"(128) 및 토픽 "개인"(130)을 포함하고, 이들은 토픽 "뉴스"(122)가 계층의 뿌리 토픽이 되도록 계층적으로 배열된다. 토픽 "재정"(124)과 "스포츠"(126)는 토픽 "뉴스"(122)로부터 내려오고, 토픽 "사업"(128)과 "개인"(130)은 토픽 "재정"(124)으로부터 내려온다. 각 토픽은 공개자(148a, 148b)에 의해 정보가 공개될 수 있는 카테고리이다. 사용자(110a, 110b)는 하나 이상의 특수 토픽에 대해 공개된 정보에 액세스하기 위해 가입할 수 있다. 예를 들어서, 사용자(110a)는 "뉴스/재정"에 대해 공개된 정보에 액세스하기 위해 가입할 수 있다. 기호 "/"는 계층 내 특수 토픽을 독특하게 식별하기 위해 계층 내 뿌리 토픽으로부터 계층 정보 집합체(120)의 경로를 표시하기 위해 사용된다. 따라서, "뉴스/재정"은 계층 내의 토픽 "재정"(124)을 독특하게 식별한다. 예를 들어서, 만일 사용자(110a)가 "뉴스/재정"에 대해 공개된 정보에 액세스하기 위해 가입하면, 사용자(110a)는 정보 공급자(102)에 의해 토픽 "재정"(124)에 대해 공개된 임의의 정보에 액세스할 수 있다. 유사하게, 사용자는 와일드카드를 이용하여 계층 정보 집합체(120)의 가지(branch)에 가입할 수 있다. 예를 들어서, 사용자(110b)는 "뉴스/재정/#"에 대해 공개된 정보에 액세스하기 위해 가입할 수 있다. 여기에서 기호 "#"는 토픽 "재정"(124)으로부터 내려오는 모든 토픽에 대한 와일드카드 가입을 표시하기 위해 사용된다. 따라서, 만일 사용자(110b)가 "뉴스/재정/#"에 가입하면, 그 사용자(110b)는 토픽 "재정"(124), "사업"(128) 및 "개인"(130)의 임의의 것에 대해 공개된 임의의 정보에 액세스할 수 있다. 계층 정보 집합체(120)는 5개의 토픽을 갖는 것으로 도시되어 있지만, 당업자라면 임의의 복수의 토픽이 계층 정보 집합체(120)를 구성할 수 있다는 것을 알 것이다.

[0057] 도 1c는 도 1a의 토픽 키 계층(144)의 예를 도시한 것이다. 토픽 키 계층(144)은 계층 정보 집합체(120) 내의 각 토픽(122-130)과 관련된 토픽 키를 포함한다. 토픽 키 K_A(132)는 토픽 "뉴스"(122)와 관련되고, 토픽 키 K_B(134)는 토픽 "재정"(122)과 관련되며, 이하 이와 같다. 토픽 키 K_A(132), K_B(134), K_C(136), K_D(138) 및 K_E(140)는 토픽 키 발생기(106)에 의해 발생된 암호화 키이다. 예를 들어서, 토픽 키 발생기(106)가 공중/사설 키 발생기이면, 토픽 키(144)는 계층 정보 집합체(120) 내의 각 토픽에 대한 공중 키 및 사설 키를 포함한다. 계층 정보 집합체(120) 내의 토픽에 대해 공개된 정보는 토픽과 관련된 토픽 키를 이용하여 정보 공급자(102)의 암호화기(150)에 의해 암호화된다. 비록 토픽 키 계층(144)이 정보 공급자(102) 내에 위치하고 계층 정보 집합체(120)로부터 분리된 것으로 도시되어 있지만, 당업자라면 토픽 키 계층(144)이 계층 정보 집합체(120) 내에 통합될 수 있고 정보 공급자(102)로부터 떨어져서 저장될 수 있다는 것을 알 것이다. 예를 들어서, 계층 정보 집합체(120)는 계층 내 각 토픽과 관련된 토픽 키를 가진 토픽의 계층을 포함할 수 있다.

[0058] 도 1d는 당업계에 공지된 것과 같은, 도 1a의 논리 키 계층(112)의 예를 도시한 것이다. 논리 키 계층은 "키 그래프를 이용한 안전한 그룹 통신"(Secure Group Communications Using Key Graphs)이라는 명칭의 논문(웡 외, IEEE/ACM Transactions on Networking, 제8권, 제1호, 2000년 2월, 16-30페이지)에서 자세히 설명되어 있다. 논리 키 계층(112)은 암호화 키 A(114a), A1(116a) 및 A2(118a)의 논리 나무 구조이다. 논리 키 계층(112)에서, 멀티캐스트 청중(108)의 사용자(110a, 110b) 각각에 대한 표시는 논리 나무 구조의 '잎'(leaf) 키와 관련된다. 다시 말해서, 사용자(110a)의 표시자(140a)는 논리 키 계층(112)의 잎에서 키 A1(116a)과 관련된다. 유사하게, 사용자(110b)의 표시자(140b)는 논리 키 계층(112)의 잎에서 키 A2(118a)와 관련된다. 멀티캐스트 청중(108) 내의 모든 사용자는 이러한 방식으로 논리 키 계층(112)의 잎 키와 관련될 것이다. 논리 키 계층(112) 내의 키의 배열은 당업계에 공지되고 웡 등의 논문에서 알 수 있는 바와 같이 특수 멀티캐스트 청중(108)이 특수 멀티캐스트 분배 시스템의 멀티캐스트 청중(108)에 대하여 가장 효과적이고 효율적인 키 분배를 수용하도록 구성된다. 논리 키 계층(112)의 설계에 관한 특수한 방법 및 생각은 본 발명의 범위를 벗어난 것이고, 따라서 여기에서 자세히 설명하지 않는다.

[0059] 각각의 사용자(110a, 110b)는 사용자 관련 잎 키로부터 논리 키 계층(112)의 뿌리까지의 경로에서 각 키에 대응하는 키에 대한 액세스를 갖는다. 제1 사용자(110a)를 생각하면, 도 1e는 도 1d의 표시자(140a)에 의해 논리 키 계층(112)의 키 A1(116a)과 관련된 사용자(110a)의 예를 도시한 것이다. 사용자(110a)는 키 A1(116a) 및 A(114a)의 각각에 대응하는 키에 대한 액세스를 갖는데, 그 이유는 이 키들이 그 관련 잎 키로부터 뿌리까지의 경로에 있기 때문이다. 그러므로, 사용자(110a)는 논리 키 계층(112)의 키 A1(116a)에 대응하는 키 A1(116b)에 대한 액세스를 갖는다. 그러므로, 사용자(110a)는 논리 키 계층(112)의 키 A(114a)에 대응하는 키 A(114b)에 대한 액세스를 또한 갖는다. 키 A1(116b)과 A(114b)는 대응하는 키 A1(116a)과 A(114a)의 카피일 수 있다. 대안적으로, 공중/사설 키 암호화는 키 A1(116b)과 A(114b)가 복호용 사설 키이고 키 A1(116a)과 A(114a)가 암호화용 공중 키일 때 사용될 수 있다. 사용자(110a)는 하나 이상의 복호 키를 이용하여 암호화기 데이터 아이템의

복호 버젼을 발생하기 위한 하드웨어 또는 소프트웨어 장치 또는 엔티티인 복호기(156a)를 또한 포함한다. 예를 들어서, 복호기(156a)는 키 A1(116b)과 같은 사설 복호 키를 이용하여 데이터의 아이템을 복호할 수 있다. 복호기(156a)의 일 예로는 "프리티 굿 프라이버시"(PGP) 제품이 있다. 이제, 사용자(110b)를 생각하면, 도 1f는 도 1d의 표시자(140b)에 의해 논리 키 계층(112)의 키 A2(118a)와 관련된 사용자(110b)의 예를 도시한 것이다. 사용자(110b)는 키 A2(118a) 및 A(114a)의 각각에 대응하는 키에 대한 액세스를 갖는데, 그 이유는 이 키들이 그 관련 잎 키로부터 뿌리까지의 경로에 있기 때문이다. 그러므로, 사용자(110b)는 논리 키 계층(112)의 키 A2(118a)에 대응하는 키 A2(118b)에 대한 액세스를 갖는다. 그러므로, 사용자(110b)는 논리 키 계층(112)의 키 A(114a)에 대응하는 키 A(114b)에 대한 액세스를 또한 갖는다. 키 A2(118b)와 A(114b)는 대응하는 키 A2(118a)와 A(114a)의 카피일 수 있다. 대안적으로, 공중/사설 키 암호화는 키 A2(118b)와 A(114b)가 복호용 사설 키이고 키 A2(118a)와 A(114a)가 암호화용 공중키일 때 사용될 수 있다. 사용자(110a)는 사용자(110a)의 복호기(156a)와 동일한 복호기(156b)를 또한 포함한다. 이 예에서 사용자(110a, 110b)는 모두 논리 키 계층 내의 키 A(114a)에 대응하는 키 A(114b)에 대한 액세스를 갖는다는 점에 주목하여야 한다. 따라서, 키 A(114a)를 이용하여 정보 공급자(102)에 의해 암호화된 데이터는 사용자(110a, 110b) 모두에 의해 복호될 수 있다.

[0060] 논리 키 계층(112)은 3개의 키를 갖는 것으로 도시되어 있지만, 당업자라면 임의의 복수의 키가 논리 키 계층(112)에 구성될 수 있음을 알 것이다.

[0061] 도 2는 멀티캐스트 시스템에서 정보를 공개하는 방법을 도시하는 흐름도이다. 하나의 공개자(148a 또는 148b)가 계층 정보 집합체(120) 내의 토픽에 대한 정보를 공개할 때, 정보 공급자(102)는 도 2의 방법을 사용하여 정보를 멀티캐스트 메시지로서 멀티캐스트 청중(108)에게 멀티캐스트한다. 처음에, 단계 202에서, 정보 공급자(102)는 정보가 공개되는 토픽에 가입된 멀티캐스트 청중(108)의 모든 사용자의 부분집합을 결정한다. 이 결정은 사용자 가입 데이터(104)에 따라 행하여진다. 이어서, 단계 204에서, 공개된 정보는 토픽 키 계층(144)의 토픽 키를 이용하여 암호화기(150)에 의해 멀티캐스트 메시지로서 암호화된다. 암호화에 사용된 토픽 키는 공개 정보가 계층 정보 집합체(120)에서 공개되는 토픽과 관련된 키이다. 단계 206에서, 토픽 키는 논리 키 계층(112)을 이용하여 가입 사용자용으로 자체 암호화된다. 따라서, 토픽 키는, 당업계에 잘 알려져 있는 바와 같이, 공개 정보가 공개되는 토픽에 가입된 사용자만이 토픽 키를 복호할 수 있도록 논리 키 계층(112)으로부터의 키들을 이용하여 1회 이상 암호화된다. 이 기술은 웡 등의 논문에 자세히 설명되어 있다. 마지막으로, 단계 208에서, 암호화 토픽 키 및 암호화 멀티캐스트 메시지는 멀티캐스터(152)에 의해 멀티캐스트 청중(108)에게 통신된다. 이 방법에서, 공개 정보는 멀티캐스트 메시지용의 랜덤 키를 발생할 필요없이 적당한 토픽용의 토픽 키를 이용하여 암호화된다. 또한, 이 방법을 이용하여 토픽 키는 정보가 공개되는 토픽에 가입된 사용자만이 멀티캐스트 메시지에 액세스할 수 있도록 가입 사용자에게 분배된다.

[0062] 멀티캐스트 시스템에서 정보를 공개하는 도 2의 방법 외에, 토픽 키는 계층 정보 집합체(120)의 각 토픽(122-130)에 대하여 토픽 키 계층(144)에서 발생된다. 토픽 키 계층(144)에서 토픽 키의 발생은 토픽이 계층 정보 집합체에서 최초로 정의될 때 수행될 수 있다. 예를 들어서, 토픽 키는 정보가 공개자(148a 또는 148b)에 의해 새로운 토픽에 최초 공개될 때 발생될 수 있다. 그 다음에, 발생된 토픽 키는 논리 키 계층(114)으로부터의 키를 이용하여 1회 이상 암호화되고 도 2의 단계 208에서 설명한 바와 같이 공개 정보를 포함한 멀티캐스트 메시지와 함께 멀티캐스트 청중(108)에게 통신된다. 대안적으로, 발생된 토픽 키는 논리 키 계층(112)을 이용하여 암호화되고, 공개 정보를 포함하지 않는 멀티캐스트 메시지와 같은 별도의 멀티캐스트 메시지로 멀티캐스트 청중(108)에게 통신될 수 있다. 따라서, 각 멀티캐스트 메시지에 대한 랜덤 키의 사용이 배제된다.

[0063] 토픽에 대한 가입 사용자를 추가 또는 제거하기 위해 사용자 가입 데이터(104)가 갱신될 때 토픽에 대한 토픽 키를 재발생하는 것이 바람직하다. 토픽 키는 토픽 키를 버리고 토픽 키 발생기(106)를 이용하여 새로운 토픽 키를 발생함으로써 재발생된다. 토픽 키의 재발생은 새로 가입된 사용자가 이전에 송신된 멀티캐스트 메시지를 복호하지 못하게 하는 것이 바람직하다. 또한, 토픽 키의 재발생은 새로운 비가입 사용자가 미래의 멀티캐스트 메시지의 복호를 계속하지 못하게 하는 것이 바람직하다. 도 3은 토픽 키를 재발생하는 방법을 도시하는 흐름도이다. 이 방법은 단계 302에서 사용자 가입 데이터(104)의 변화에 응답한다. 계층 정보 집합체(120) 내의 하나 이상의 토픽에 대한 사용자 가입 데이터(104)의 변화에 응답하여, 단계 304에서 토픽 키 계층(144) 내의 각각의 영향을 받은 토픽에 대한 토픽 키를 토픽 키 발생기(106)를 이용하여 재발생한다. 이 방법에서 토픽 키 계층(144) 내 토픽 키는 새로운 사용자가 대응 토픽에 가입한 때 또는 가입 사용자가 대응 토픽으로부터 탈퇴한 때에만 재발생된다.

[0064] 이제 전술한 방법을 사용자(110a)가 계층 정보 집합체(120) 내의 토픽 "개인"(130)에 가입한 상황에 이용하는 경우를 단지 예로서 생각한다. 토픽 "개인"(130)에 가입하기 위하여, 사용자(110a)는 "뉴스/재정/개인"에 가입

하기 위한 요구를 정보 공급자(102)에게 보낸다. 이 요구는 사용자 가입 데이터(104)를 변화시킨다. 토픽 키를 재발생하기 위한 도 3의 방법을 생각하면, 단계 302에서, 상기 방법은 사용자 가입 데이터(104)에서 토픽 "개인"(130)에 대한 가입자로서 사용자(110a)의 추가에 응답한다. 이어서, 단계 304에서, 토픽 "개인"(130)에 대한 새로운 토픽 키 K_E(140)가 토픽 키 발생기(106)를 이용하여 발생된다. 따라서, 사용자 가입 데이터(104)가 토픽 "개인"(130)에 대하여 변화할 때 토픽 키 K_E(140)가 재발생된다.

[0065] 제2 예에서, 사용자(110b)는 "뉴스/재정/#"에 가입하기 위한 요구를 정보 공급자(102)에게 보낸다. 이 요구는 토픽 "재정"(124), "사업"(128) 및 "개인"(130)에 대한 가입자로서 사용자(110b)를 포함시키도록 사용자 가입 데이터(104)를 변화시킨다. 토픽 키를 재발생하기 위한 도 3의 방법을 생각하면, 단계 302에서, 상기 방법은 사용자 가입 데이터(104)에서 토픽 "재정"(124), "사업"(128) 및 "개인"(130)에 대한 가입자로서 사용자(110b)의 추가에 응답한다. 이어서, 단계 304에서, 새로운 토픽 키가 토픽 키 계층(144) 내의 영향을 받은 토픽 "재정"(124), "사업"(128) 및 "개인"(130)에 대하여 발생된다. 이것은 토픽 키 발생기(106)를 이용하여 토픽 키 K_B(134), K_D(138) 및 K_E(140)의 재발생을 가져온다. 따라서, 사용자(110b)가 "뉴스/재정/#"에 가입한 때 토픽 "재정"(124), "사업"(128) 및 "개인"(130)에 대한 가입 데이터(104)가 변화하고, 대응하는 토픽 키가 재발생된다.

[0066] 이제, 도 2의 방법을 사용자(110b)가 토픽 "재정"(124)에 가입한 유일한 사용자이고 정보가 공개자(148a, 148b)에 의해 토픽 "재정"(124)에 대하여 공개되는 상황에 이용하는 경우를 생각하자. 단계 202에서 정보 공급자(102)는 사용자(110b)가 토픽 "재정"(124)에 가입되었는지를 사용자 가입 데이터(104)를 참조하여 결정한다. 단계 204에서, 암호화기(150)는 토픽 "재정"(124)에 대해 공개된 정보를 토픽 키 계층(144) 내의 토픽 "재정"(124)에 대응하는 토픽 키 K_B(134)를 이용하여 멀티캐스트 메시지로서 암호화한다. 이어서, 단계 206에서, 암호화기(150)는 논리 키 계층(112)을 이용하여 가입 사용자(110b)용의 토픽 키 K_B(134)를 암호화한다. 이것은 논리 키 계층(112) 내의 키 A2(118a)의 사용을 수반하는데, 그 이유는 상기 키가 계층 정보 집합체(120) 내의 토픽 "재정"(124)에 가입된 유일한 사용자인 사용자(110b)에 대응하기 때문이다. 이어서, 단계 208에서, 키 A2(118a)를 이용하여 암호화된 토픽 키 K_B(134) 및 토픽 키 K_B(134)를 이용하여 암호화된 공개 정보가 멀티캐스터(152)에 의해 멀티캐스트 메시지로서 통신된다. 멀티캐스트 메시지는 멀티캐스트 청중(108) 내의 사용자(110a, 110b) 모두에 의해 수신된다. 이 방법에서, 사용자(110b)는 정보 공급자(102)로부터 토픽 키 K_B(134)를 수신한다. 사용자(110b)는 토픽 키 K_B(134)를 암호화 한 키 A2(118a)에 대응하는 키 A2(118b)에 액세스할 수 있기 때문에 토픽 키 K_B(134)를 복호할 수 있다. 사용자(110b)가 일단 토픽 키 K_B(134)를 복호하면, 사용자(110b)는 토픽 키 K_B(134)를 이용하여 암호화된 공개 정보를 복호할 수 있다. 그러나, 사용자(110a)는 논리 키 계층(112) 내의 키 A2(118a)에 대응하는 키에 액세스할 수 없기 때문에 토픽 키 K_B(134)를 복호할 수 없다. 그러므로, 사용자(110a)는 토픽 키 K_B(134)를 이용하여 암호화된 공개 정보에 액세스할 수 없다. 따라서 공개 정보는 멀티캐스트 청중(108) 내의 가입 사용자에게만 이용가능하고, 토픽 "재정"(124)에 대한 토픽 키 K_B(134)는 토픽 "재정"(124)에 대한 각각의 정보 공개를 위하여 재발생될 필요가 없다.

[0067] 이제, 도 2의 방법을 사용자(110a, 110b)가 토픽 "개인"(130)에 가입하고 정보가 하나의 공개자(148a 또는 148b)에 의해 토픽 "개인"(130)에 대하여 공개되는 상황에 이용하는 경우를 생각하자. 단계 202에서 정보 공급자(102)는 사용자(110a, 110b)가 모두 토픽 "개인"(130)에 가입되었는지를 사용자 가입 데이터(104)를 참조하여 결정한다. 단계 204에서, 암호화기(150)는 토픽 "개인"(130)에 대해 공개된 정보를 토픽 키 계층(144) 내의 토픽 "개인"(130)에 대응하는 토픽 키 K_E(140)를 이용하여 멀티캐스트 메시지로서 암호화한다. 이어서, 단계 206에서, 암호화기(150)는 논리 키 계층(112)을 이용하여 가입 사용자(110a, 110b)용의 토픽 키 K_E(140)를 암호화한다. 사용자가 모두 토픽 "개인"(130)에 가입하였기 때문에, 사용자(110a, 110b) 모두에게 공통으로 액세스가능한 논리 키 계층(112)으로부터의 키가 토픽 키 K_E(140)를 암호화하기 위해 선택된다. 키 A(114b)는 사용자(110a, 110b) 모두에게 공통으로 액세스가능하고, 따라서 논리 키 계층(112) 내의 대응하는 키 A(114a)가 토픽 키 K_E(140)를 암호화하기 위해 사용될 수 있다. 이어서, 단계 208에서, 키 A(114a)를 이용하여 암호화된 토픽 키 K_E(140) 및 토픽 키 K_E(140)를 이용하여 암호화된 공개 정보가 멀티캐스터(152)에 의해 멀티캐스트 메시지로서 통신된다. 멀티캐스트 메시지는 멀티캐스트 청중(108) 내의 사용자(110a, 110b) 모두에 의해 수신된다. 사용

자(110a)는 토픽 키 K_E(140)를 암호화 한 키 A(114a)에 대응하는 키 A(114b)에 액세스할 수 있기 때문에 토픽 키 K_E(140)를 복호할 수 있다. 사용자(110a)가 일단 토픽 키 K_E(140)를 복호하면, 사용자(110a)는 토픽 키 K_E(140)를 이용하여 암호화된 공개 정보를 복호할 수 있다. 마찬가지로, 사용자(110b)는 토픽 키 K_E(140)를 암호화 한 키 A(114a)에 대응하는 키 A(114b)에 액세스할 수 있기 때문에 토픽 키 K_E(140)를 복호할 수 있다. 사용자(110b)가 일단 토픽 키 K_E(140)를 복호하면, 사용자(110b)는 토픽 키 K_E(140)를 이용하여 암호화된 공개 정보를 복호할 수 있다. 따라서 공개 정보는 멀티캐스트 청중(108) 내의 가입 사용자(110a, 110b) 모두에 의해 액세스 가능하고, 토픽 "개인"(130)에 대한 토픽 키 K_E(140)는 토픽 "개인"(130)에 대한 각각의 정보 공개를 위하여 재발생될 필요가 없다. 또한, 공통으로 액세스가능한 키 A(114a)를 이용하여 토픽 키 K_E(140)를 암호화하기 위해 논리 키 계층(112)을 사용함으로써 토픽 키를 1회 이상 암호화할 필요가 없게 된다.

[0068] 계층 정보 집합체 내의 토픽에 가입하는 개별 사용자 외에, 정보 공급자는 사용자가 액세스하도록 인증된 토픽을 정의하는 액세스 제어 리스트를 포함할 수 있다. 이러한 시스템에서, 공개 정보는 인증된 사용자(가입된 사용자와는 다름)만이 액세스 가능하도록 보호되고, 사용자는 그들이 액세스 제어 리스트에 따라 액세스하도록 인증된 토픽에만 가입할 수 있다. 이러한 구성에서, 각 토픽에 대한 키의 발생 및 유지는 사용자가 계층 정보 집합체 내의 토픽의 집합에 액세스하도록 인증될 것이기 때문에 번거로워질 수 있다. 원리적으로는 계층 정보 집합체를 액세스 제어 리스트에 따라 복수의 토픽 그룹으로 분할하고 이러한 토픽 그룹 각각에 대하여 키를 유지하는 것이 유리할 것이다. 이제, 본 발명의 양호한 실시예를 설명한다.

[0069] 도 4a는 본 발명의 양호한 실시예에 따라 멀티캐스트 정보 공급자(402)를 포함하는 멀티캐스트 공개/가입 시스템을 개략적으로 도시한 것이다. 도 4a의 많은 요소들은 도 1a와 관련하여 설명한 요소들과 동일하고, 따라서 이들에 대해서는 여기에서 반복하여 설명하지 않는다. 도 4a의 요소들 중 도 1a의 요소들과 공통되지 않는 요소에 대해서 이하 상세히 설명한다.

[0070] 정보 공급자(402)는 멀티캐스트 청중(408) 내의 사용자들이 액세스하도록 인증되는 계층 정보 집합체(420) 내 토픽들을 정의하는 액세스 제어 리스트(460)를 포함한다. 액세스 제어 리스트(460)는 데이터베이스에 기록될 수 있다. 대안적으로, 액세스 제어 리스트(460)는 컴퓨터 시스템의 메모리에 또는 컴퓨터의 기억 장치에 파일로서 기록될 수 있다. 당업자라면 액세스 제어 리스트(460)를 저장하기 위한 다른 적당한 수단을 이용할 수 있다는 것을 알 것이다. 정보 공급자(402)는 액세스 제어 리스트(460)를 이용하여 사용자 가입 데이터(404)에서 정의된 사용자 가입이 액세스 제어 리스트(460)에서 정의된 인증과 일치하는 것을 보장할 수 있다. 이것은 사용자가 액세스하도록 인증되지 않은 토픽에 사용자가 가입할 수 없게 하기 때문에 바람직하다.

[0071] 일 실시예에서, 액세스 제어 리스트(460)는 특수한 사용자가 액세스하도록 인증된 계층 정보 집합체(420) 내의 토픽 또는 가지의 리스트로서 정의된다. 이제, 이러한 액세스 제어 리스트(460)의 일 예를 도 6a에 도시된 예시적인 계층 정보 집합체(420)를 참조하여 설명한다. 도 6a의 계층 정보 집합체(420)는 뿌리 토픽 "비행기 여행"(600)을 포함한다. 뿌리 토픽으로부터는 토픽 "국내"(602)와 "국제"(604)가 내려온다. 토픽 "국내"(602)로부터는 토픽 "중부지역"(606), "동해안"(608) 및 "서해안"(610)이 내려온다. 토픽 "국제"(604)로부터는 토픽 "유럽"(612)과 "아시아"(614)가 내려온다. 이러한 예시적인 계층 정보 집합체(420)에 기초하여, 아래의 표 1은 일 실시예에서 사용자(410a~410d)에 대한 액세스 제어 리스트(460)를 나타낸다. 사용자(410a~410d) 각각에 대하여, 표 1은 토픽 집합의 정의를 포함한다. 각 사용자는 액세스 제어 리스트(460)에서 그 사용자에 대한 토픽 집합 내의 토픽에 대해 공개된 정보에만 액세스하도록 인증된다. 예를 들어서, 사용자(410a)는 {비행기 여행/국내/#}에 대해 공개된 정보에 액세스하도록 인증된다. 따라서, 사용자(410a)는 집합 {비행기 여행/국내/#}에 속하는 토픽인 토픽 "국내"(602), "중부지역"(606), "동해안"(608) 및 "서해안"(610) 중 임의의 것에 대해 공개된 정보에 액세스하도록 인증된다.

[0072] [표 1]

[0073] 액세스 제어 리스트(460)

[0074]

사용자	인증된 토픽
사용자(410a)	{비행기 여행/국내/#}
사용자(410b)	{비행기 여행/국제/#, 비행기 여행/국내/서해안}
사용자(410c)	{비행기 여행/국내/#, 비행기 여행/국제/유럽}
사용자(410d)	{비행기 여행/국내/#}

[0075] 도 4b는 액세스 제어 리스트(460)의 다른 실시예를 도시하고 있다. 도 4b의 액세스 제어 리스트는 롤(role)(4602)과 사용자(4604)를 포함하고 있다. 롤(4602)은 계층 정보 집합체(420)의 하나 이상의 지명된 토픽 또는 가지의 집합을 포함한다. 사용자(4604)는 각 사용자(410a~410d)에 대한 엔트리를 포함하고, 각 사용자에 대하여 사용자가 어느 롤(4602)에 관련되는지를 지정한다. 롤과 관련된 사용자는 그 롤의 토픽에 대해 공개된 정보에만 액세스하도록 인증된다. 이제, 이러한 액세스 제어 리스트(460)의 예를 도 6a의 계층 정보 집합체(420)를 참조하여 설명한다. 아래의 표 2a는 도 4b의 롤(4602)의 예시적인 정의를 나타낸다. 표 2a의 각 행은 계층 정보 집합체(420)의 지명된 토픽 집합이다.

[0076] [표 2a]

[0077] 롤(4602)

[0078]

롤 명	인증된 토픽
태평양(622)	{비행기 여행/국제/#, 비행기 여행/국내/서해안} {비행기 여행/국내/#}
국내(624)	{비행기 여행/국내/#, 비행기 여행/국제/유럽}
국내-유럽(626)	
모두(628)	{비행기 여행/#}

[0079] 따라서, 예를 들어서, 롤 "국내"(624)는 계층 정보 집합체(420) 내의 "비행기 여행/국내/#}의 토픽 집합를 포함한다. 따라서, 롤 "국내"(624)는 "국내"(602), "중부지역"(606), "동해안"(608) 및 "서해안"(610)에 대응한다. 아래의 표 2b는 도 4b의 사용자(4604)의 예시적인 정의를 나타낸다. 표 2b의 각 행은 멀티캐스트 청중(408)의 사용자(410a~410d) 중의 하나에 대응한다.

[0080] [표 2b]

[0081] 사용자(4604)

[0082]

사용자	롤
사용자(410a)	국내(624)
사용자(410b)	태평양(622)
사용자(410c)	국내-유럽(626)
사용자(410d)	국내(624)

[0083] 따라서, 예를 들어서, 사용자(410a)는 롤 "국내"(624)에 속하는 것으로 지정된다. 그러므로, 사용자(410a)는 롤 "국내"(624)에 포함된 토픽에 대해 공개된 정보에만 액세스하도록 인증된다. 전술한 바와 같이, 롤 "국내"(624)는 {비행기 여행/국내/#}의 토픽 집합을 포함한다. 따라서, 사용자(410a)는 "국내"(602), "중부지역"(606), "동해안"(608) 및 "서해안"(610)의 토픽에 대해 공개된 정보에만 액세스하도록 인증된다.

[0084] 이 방법에서, 계층 정보 집합체(420) 내의 개별 토픽에 대해 공개된 정보에 대한 개별 사용자의 액세스를 제어할 수 있다. 전술한 액세스 제어 리스트(460)의 2개의 예시적인 실시예는 각각 사용자가 액세스하게끔 인증되는 정보가 공개될 수 있는 토픽 또는 가지의 집합의 정의를 포함한다. 당업자라면 사용자가 액세스하게끔 인증되지 않는(즉, 인증에서 제외된) 정보가 공개될 수 있는 토픽 또는 가지의 집합의 정의를 동일하게 포함할 수 있다는 것을 알 것이다. 더 나아가, 액세스 제어 리스트(460)의 2개의 예시적인 실시예를 위에서 설명하였지만, 당업자

라면 멀티캐스트 청중(408) 내의 사용자에 대한 액세스 제어를 지정하기 위한 임의의 적당한 메카니즘이 사용될 수 있다는 것을 알 것이다.

[0085] 다시 도 4a로 돌아가서, 정보 공급자(402)는 정보 집합체 분할기(462)를 또한 포함한다. 정보 집합체 분할기(462)는 계층 정보 집합체(420)를 하나 이상의 분할 요소(468)로 분할한다. 각 분할 요소(468)는 계층 정보 집합체(420)로부터 토픽의 서로소 진 부분집합으로서 수학적으로 정의된다. 서로소 진 부분집합은 집합론(set theory)에서 잘 알려져 있고, 계층 정보 집합체(T)에 대하여 T의 토픽의 집합 S_1, S_2, S_3,...S_n의 컬렉션(collection)으로서 정의될 수 있고, 여기에서, 임의의 2개의 집합 S_i, S_j에 대하여:

[0086] (S_i 3 S_j=A) 및 (S_1 4 S_2 4 S_3...4 S_n=T)이다.

[0087] 따라서, 집합 S1, S2, S3,...Sn 중 2개가 교차되는 것은 없고 모든 집합의 조합은 전체 계층 정보 집합체(T)와 정확히 동일하다. 분할 요소(468)는 계층 정보 집합체(420)를 분할하기 위해 액세스 제어 리스트(460)를 이용하여 정의된다. 각 분할 요소(468)는 액세스 제어 리스트(460)의 빌딩 블록을 나타낸다. 예를 들어서, 각각의 롤(4602)은 분할 요소의 불연속 리스트(discrete list)의 항목으로 정의될 수 있다. 분할 요소의 목적은 암호화 키가 토픽의 그룹에 할당되어 계층 내 각 토픽에 대한 키를 발생할 어떠한 필요성을 회피할 수 있도록 계층 정보 집합체(420) 내의 토픽의 적당한 그룹핑을 정의하기 위한 것이다.

[0088] 분할 요소(468)를 정의하는 방법은 도 5a에 제시되어 있으며, 이제 도 6a의 계층 정보 집합체(420) 및 상기 표 2a 및 표 2b에 정의된 액세스 제어 리스트(460)를 참조하여 설명한다.

[0089] 도 5a의 방법의 제1 단계(502)에서, 계층 정보 집합체(420)의 부분집합이 액세스 제어 리스트(ACL)(460)에 따라서 정의된다. 실제로 이것을 설명하기 위해, 도 6b는 굵은 선을 이용하여 표시한 액세스 제어 리스트(460)의 표 2a에 정의된 부분집합과 함께 도 6a의 계층 정보 집합체를 묘사한다. 표 2a는 4개의 롤(4602)을 정의하고, 각 롤은 계층 정보 집합체(420)의 부분집합을 포함한다. 롤 "태평양"(622)은 토픽 "국제"(604), "서해안"(610), "유럽"(612) 및 "아시아"(614)를 포함하는 부분집합을 정의한다는 것을 도 6b로부터 알 수 있다. 또한, 롤 "국내"(624)는 토픽 "국내"(602), "중부지역"(606), "동해안"(608), "서해안"(610)을 포함하는 계층 정보 집합체의 부분집합을 정의한다. 유사하게, 롤 "국내-유럽"(626) 및 "모두"(628)는 계층 정보 집합체(420) 내의 부분집합들을 정의한다. 또한, 롤(4602)에 의해 정의된 부분집합은 서로 교차하고, 그래서 이 단계에서 서로소 부분집합을 형성하지 않는다는 것을 알 수 있다.

[0090] 이제, 도 5a의 방법의 단계 504를 참조하면, 액세스 제어 리스트(460)에서 롤(4602)에 대응하는 부분집합은 계층 정보 집합체(420)를 서로소 진 부분집합으로 분할하기 위해 사용된다. 이 서로소 진 부분집합은 분할 요소(468)에 대응한다. 도 6c는 분할 요소(468)로 분할된 계층 정보 집합체(420)를 도시하고 있다. 각 요소는 도 6b의 부분집합의 교집합 또는 차집합으로부터 유도된 서로소 부분집합이다. 서로소 부분집합의 리스트를 발생하기 위한 상세한 방법은 뒤에서 도 5b 및 도 5c를 참조하여 설명된다. 5개의 분할 요소(468), 즉 분할 요소 "L"(4680); 분할 요소 "M"(4682); 분할 요소 "N"(4684); 분할 요소 "O"(4686); 및 분할 요소 "P"(4688)이 있다. 아래의 표 3은 도 5a의 방법에 따라서 집합 기호를 이용하여 각 분할 요소(468)의 정의를 제공한다.

[0091] [표 3]

[0092] 분할 요소(468)

[0093]

분할 요소	분할 요소 정의
분할 요소 "L"(4680)	{비행기 여행}
분할 요소 "M"(4682)	{비행기 여행/국내, 비행기 여행/국내/중부지역, 비행기 여행/국내/동해안}
분할 요소 "N"(4684)	{비행기 여행/국내/서해안}
분할 요소 "O"(4686)	{비행기 여행/국제/유럽}
분할 요소 "P"(4688)	{비행기 여행/국제, 비행기 여행/국제/아시아}

[0094] 따라서, 분할 요소 "L"(4680) 내지 "P"(4688)는 2개의 분할 요소가 교차하는 것이 없고, 모든 분할 요소의 조합은 계층 정보 집합체(420) 내의 모든 토픽을 포함하기 때문에 계층 정보 집합체(420)의 서로소 진 부분집합임을 알 수 있다. 정보 집합체 분할기(462)는 액세스 제어 리스트(460)가 변화될 때마다 분할 요소(468)를 발생하는 것이 바람직하다. 이것은 분할 요소(468)가 액세스 제어 리스트(460)를 정확히 반영하는 것을 보장한다.

[0095] 도 5b는 본 발명의 양호한 실시예에서 부분집합의 리스트로부터 서로소 부분집합의 리스트를 발생하는 방법을 나타내는 흐름도이다. 예를 들어서, 도 5b의 방법은 롤의 리스트로부터 계층 정보 집합체(420) 내 토픽들의 서로소 부분집합의 리스트를 발생하기 위해 사용될 수 있고, 여기에서 각 롤은 계층의 부분집합을 정의한다. 이제, 도 5b의 방법을 도 5c에 도시된 계층 정보 집합체(420)의 추가적이고 더 간단한 예를 참조하여 설명하겠다. 도 5c의 계층 정보 집합체(420)는 7개의 토픽(550-560)을 포함하고, 토픽(550)이 계층의 뿌리가 되도록 배열된다. 토픽(552, 553)은 토픽(550)으로부터 내려온다. 토픽(554, 556)은 토픽(552)으로부터 내려오고, 토픽(558, 560)은 토픽(553)으로부터 내려온다. 도 5c는 액세스 제어 리스트(460)의 롤(4602)과 같이 계층 정보 집합체(420)의 3개의 부분집합을 추가로 도시한 것이다. 제1 부분집합 i(570)는 모든 토픽(552-560)을 포함한다. 제2 부분집합 j(572)는 토픽(552, 554, 556)을 포함한다. 제3 부분집합 k(574)는 토픽(553, 558, 560)을 포함한다. 모든 부분집합의 리스트는 편리성을 위해 아래의 표 4a에 요약되어 있다.

[0096] [표 4a]

[0097] (도 5c의) 모든 부분집합의 리스트

[0098]

부분집합	부분집합 정의
부분집합 i(570)	{550, 552, 553, 554, 556, 558, 560}
부분집합 j(572)	{552, 554, 556}
부분집합 k(574)	{554, 556, 558, 560}

[0099] 이제, 도 5b를 참조하면, 단계 510에서 상기 표 4a의 부분집합의 리스트로부터 부분집합 쌍의 모든 조합이 결정된다. 이것은 3개의 부분집합 i(570), j(572) 및 k(574)와 함께, 부분집합 쌍의 모든 조합이 아래의 표 4b에 표시된 대로 요약될 수 있다. 각 부분집합의 쌍은 부분집합명을 이용하여 괄호 안에 표시하였다.

[0100] [표 4b]

[0101] 부분집합의 모든 조합

[0102]

조합 1	(i,j)
조합 2	(i,k)
조합 3	(j,k)

[0103] 이어서, 단계 512에서, 루프는 부분집합 쌍의 모든 조합을 통하여 시작된다. 조합 1(i,j)에서 시작하여, 단계 (514)는 (i 3 j g $\hat{A}$)인지를 판정한다. 표 4a에서 부분집합 i(570) 및 j(572)의 정의를 이용하면,

[0104] i 3 j = {552, 554, 556}

[0105] 임을 알 수 있고, 따라서 (i 3 j g $\hat{A}$)는 참(true)이고 방법은 단계 516으로 진행한다. 단계 516에서, 새로운 부분집합(우리는 이것을 부분집합 l이라고 부른다)이 모든 부분집합들의 리스트에 추가되고, 여기에서 상기 새로운 부분집합은 (i 3 j)에 대응한다. 따라서, 새로운 부분집합 l은 {552, 554, 556}으로서 정의된다. 더 나아가, 단계 518에서, 새로운 부분집합(우리는 이것을 부분집합 m이라고 부른다)이 모든 부분집합들의 리스트에 추가되고, 여기에서 상기 새로운 부분집합은 (i - j)에 대응한다. 따라서, 새로운 부분집합 m은 {550, 553, 558, 560}으로서 정의된다. 더 나아가, 단계 520에서, 새로운 부분집합(우리는 이것을 부분집합 n이라고 부른다)이 모든 부분집합들의 리스트에 추가되고, 여기에서 상기 새로운 부분집합은 (j - i)에 대응한다. 따라서, 새로운 부분집합 n은 {552, 554, 556}으로서 정의된다. 따라서, 단계 516 내지 520은 3개의 새로운 부분집합 l, m 및 n이 표 4a의 부분집합의 리스트에 추가되게 한다. 단계 522에서, 부분집합 i(570) 및 j(572)는 모든 부분집합의 리스트로부터 제거된다. 따라서, 이 단계에서, 모든 부분집합의 리스트는 아래의 표 4c에 정의된 바와 같다.

[0106] [표 4c]

[0107]

부분집합	부분집합 정의
부분집합 k(574)	{554, 556, 558, 560}
부분집합 l	{552, 554, 556}
부분집합 m	{550, 553, 558, 560}
부분집합 n	{552, 554, 556}

[0108] 이어서, 단계 524에서, 복제(duplicate) 부분집합이 모든 부분집합의 리스트로부터 제거된다. 모든 부분집합의 리스트는 부분집합 l과 n을 포함하는데 상기 부분집합 l과 n은 둘 다 {552, 554, 556}으로 정의되고 따라서 복제물이다. 그러므로, 부분집합 n은 단계 524에서 모든 부분집합의 리스트로부터 제거된다. 이 단계에서, 모든 부분집합의 리스트는 아래의 표 4d에서 정의된 것과 같다.

[0109] [표 4d]

[0110] 모든 부분집합의 리스트

[0111]

부분집합	부분집합 정의
부분집합 k(574)	{554, 556, 558, 560}
부분집합 l	{552, 554, 556}
부분집합 m	{550, 553, 558, 560}

[0112] 단계 526에서, 부분집합 쌍들의 모든 조합들은 모든 부분집합의 새로운 리스트에 비추어 재결정된다. 표 4e는 부분집합 쌍의 모든 조합의 새로운 리스트를 제공한다. 그 다음에, 방법은 단계 512로 복귀하여 다음 부분집합 쌍을 통하여 루핑한다.

[0113] [표 4e]

[0114] 부분집합들의 모든 조합

[0115]

조합 1	(k, l)
조합 2	(k, m)
조합 3	(l, m)

[0116] 단계 512에서, 부분집합 쌍의 조합의 리스트로부터의 처리를 위해 다음 부분집합 쌍이 선택된다. 부분집합 쌍의 조합의 리스트는 갱신되었기 때문에, 처리를 위한 다음 부분집합 쌍은 리스트에서 새로운 제1 조합, 즉 (k, l)이다. 단계 514는 (k 3 l g $\hat{A}$)인지 여부를 결정한다. 표 4d의 부분집합 k(574) 및 l의 정의를 이용하여

[0117] k 3 l = {554, 556}

[0118] 이고, 따라서 (k 3 l g $\hat{A}$)는 참(true)임을 알 수 있고, 방법은 단계 516으로 진행한다. 단계 516에서, 새로운 부분집합(우리는 이것을 부분집합 o라고 부른다)이 모든 부분집합들의 리스트에 추가되고, 여기에서 상기 새로운 부분집합은 (k 3 l)에 대응한다. 따라서, 새로운 부분집합 o는 {554, 556}으로서 정의된다. 더 나아가, 단계 518에서, 새로운 부분집합(우리는 이것을 부분집합 p라고 부른다)이 모든 부분집합들의 리스트에 추가되고, 여기에서 상기 새로운 부분집합은 (k - l)에 대응한다. 따라서, 새로운 부분집합 p는 {558, 560}으로서 정의된다. 더 나아가, 단계 520에서, 새로운 부분집합(우리는 이것을 부분집합 q라고 부른다)이 모든 부분집합들의 리스트에 추가되고, 여기에서 새로운 부분집합은 (l - k)에 대응한다. 따라서, 새로운 부분집합 q는 {552}로서 정의된다. 따라서, 단계 516 내지 520은 3개의 새로운 부분집합 o, p 및 q가 표 4d의 부분집합의 리스트에 추가되게 한다. 단계 522에서, 부분집합 k(574) 및 부분집합 l은 모든 부분집합의 리스트로부터 제거된다. 따라서, 이 단계에서, 모든 부분집합의 리스트는 아래의 표 4f에 정의된 바와 같다.

[0119] [표 4f]

[0120] 모든 부분집합의 리스트

[0121]

부분집합	부분집합 정의
부분집합 m	{550, 553, 558, 560}
부분집합 o	{554, 556}
부분집합 p	{558, 560}
부분집합 q	{552}

[0122] 이어서, 단계 524에서, 복제 부분집합이 모든 부분집합의 리스트로부터 제거된다. 모든 부분집합의 리스트는 어떠한 복제물도 포함하지 않고 있고, 따라서 방법은 단계 526으로 진행하여 여기에서 부분집합 쌍의 모든 조합들이 모든 부분집합의 새로운 리스트에 비추어 재결정된다. 표 4g는 부분집합 쌍의 모든 조합의 새로운 리스트를 제공한다. 그 다음에, 방법은 단계 512로 복귀하여 부분집합의 다음 쌍을 통하여 루핑된다.

[0123] [표 4g]

[0124] 부분집합의 모든 조합

[0125]

조합 1	(m, o)
조합 2	(m, p)
조합 3	(m, q)
조합 4	(o, p)
조합 5	(o, q)
조합 6	(p, q)

[0126] 단계 512에서, 부분집합의 다음 쌍이 부분집합 쌍의 조합의 리스트로부터 처리를 위해 선택된다. 부분집합의 쌍의 조합의 리스트는 갱신되었기 때문에, 처리를 위한 부분집합의 다음 쌍은 리스트에서 새로운 제1 조합, 즉 (m, o)이다. 단계 514는 (m 3 o g $\hat{A}$)인지 여부를 결정한다. 표 4f에서 부분집합 m과 o의 정의를 이용하여

[0127] m 3 o = {} = $\hat{A}$

[0128] 이고, 따라서 (k 3 l g $\hat{A}$)는 거짓(false)임을 알 수 있다. 그 다음에 방법은 단계 528로 진행하고, 여기에서 처리할 부분집합의 쌍의 조합이 더 있는지가 판정된다. 처리는 부분집합의 다음 쌍(m, p)을 위하여 단계 512로 복귀한다. 단계 514에서는 (m 3 p g $\hat{A}$)인지 여부가 판정된다. 표 4f의 부분집합 m과 p의 정의를 이용하면,

[0129] m 3 p = {558, 560}

[0130] 이고 따라서 (m 3 p g $\hat{A}$)는 참임을 알 수 있고, 방법은 단계 516으로 진행한다. 단계 516에서, 새로운 부분집합(우리는 이것을 부분집합 r이라고 부른다)이 모든 부분집합들의 리스트에 추가되고, 여기에서 새로운 부분집합은 (m 3 p)에 대응한다. 따라서, 새로운 부분집합 r은 {558, 560}으로서 정의된다. 더 나아가, 단계 518에서, 새로운 부분집합(우리는 이것을 부분집합 s라고 부른다)이 모든 부분집합들의 리스트에 추가되고, 여기에서 새로운 부분집합은 (m - p)에 대응한다. 따라서, 새로운 부분집합 s는 {550, 553}으로서 정의된다. 더 나아가, 단계 520에서, 새로운 부분집합(우리는 이것을 부분집합 t라고 부른다)이 모든 부분집합들의 리스트에 추가되고, 여기에서 새로운 부분집합은 (p - m)에 대응한다. 따라서, 새로운 부분집합 t는 {}로서 정의된다. 부분집합 t는 공집합(empty set)이고, 따라서 모든 부분집합의 리스트에 추가되지 않는다. 따라서, 단계 516 내지 520은 2개의 새로운 부분집합 r과 s가 표 4f의 부분집합의 리스트에 추가되게 한다. 단계 522에서, 부분집합 m 및 부분집합 p는 모든 부분집합의 리스트로부터 제거된다. 따라서, 이 단계에서, 모든 부분집합의 리스트는 아래의 표 4h에 정의된 바와 같다.

[0131] [표 4h]

[0132] 모든 부분집합의 리스트

[0133]

부분집합	부분집합 정의
부분집합 o	{554, 556}
부분집합 q	{552}
부분집합 r	{558, 560}
부분집합 s	{550, 553}

[0134] 이어서, 단계 524에서, 복제 부분집합이 모든 부분집합의 리스트로부터 제거된다. 모든 부분집합의 리스트는 어떠한 복제물도 포함하지 않고 따라서 방법은 단계 526으로 진행하여 여기에서 부분집합 쌍의 모든 조합들이 모든 부분집합의 새로운 리스트에 비추어 재결정된다. 표 4i는 부분집합 쌍의 모든 조합의 새로운 리스트를 제공한다. 그 다음에 방법은 단계 512로 복귀하여 부분집합의 다음 쌍을 통하여 루핑한다.

[0135] [표 4i]

[0136] 부분집합의 모든 조합

[0137]

조합 1	(o, q)
조합 2	(o, r)
조합 3	(o, s)
조합 4	(q, r)
조합 5	(q, s)
조합 6	(r, s)

[0138] 단계 512에서, 부분집합의 다음 쌍이 부분집합 쌍의 조합의 리스트로부터 처리를 위해 선택된다. 부분집합 쌍의 조합의 리스트는 갱신되었기 때문에, 처리를 위한 부분집합의 다음 쌍은 리스트에서 새로운 제1 조합, 즉 (o, q)이다. 단계 514는 (o 3 q g $\hat{A}$)인지 여부를 결정한다. 표 4h에서 부분집합 o와 q의 정의를 이용하면,

[0139] o 3 q = {} = $\hat{A}$

[0140] 이고 따라서 (o 3 q g $\hat{A}$)는 거짓임을 알 수 있다. 그 다음에 방법은 단계 528로 진행하고, 여기에서 처리할 부분집합 쌍의 조합이 더 있는지가 판정된다. 처리는 부분집합의 다음 쌍(o, r)을 위하여 단계 512로 복귀한다. 단계 514에서는 (o 3 r g $\hat{A}$)인지 여부가 판정된다. 표 4h의 부분집합 o와 r의 정의를 이용하면,

[0141] o 3 r = {} = $\hat{A}$

[0142] 이고 따라서 (o 3 r g $\hat{A}$)는 거짓임을 알 수 있다. 방법은 이러한 방식으로 진행하고 부분집합 쌍의 모든 조합을 처리하여 각 조합이 교차하지 않는지를 확인한다. 일단 모든 조합이 처리되면, 방법은 단계 528에서 종료한다.

[0143] 따라서, 도 5b의 방법은 서로소 진 부분집합의 리스트인 표 4h의 모든 부분집합의 리스트를 발생한다. 상기 서로소 진 부분집합은 본 발명의 양호한 실시예에서 분할 요소에 대응한다. 도 5d는 도 5b의 방법을 이용하여 발생된 서로소 진 부분집합을 도시한 것이다.

[0144] 다시 도 4a로 돌아가서, 정보 공급자(402)는 분할 요소 키 발생기(470)를 더 포함한다. 분할 요소 키 발생기(470)는 분할 요소 키(472)를 발생하기 위한 하드웨어 또는 소프트웨어 장치 또는 엔티티이다. 분할 요소 키(472)는 공중/사설 키 암호화에 필요한 공중 키 및 사설 키와 같은 암호화 키이다. 각각의 분할 요소 키(472)는 분할 요소(468) 중의 하나에 대응한다. 분할 요소 키 발생기(470)의 일 예는 "프리티 굿 프라이버시"(PGP) 제품이다(프리티 굿 프라이버시 및 PGP는 PGP 코포레이션의 등록 상표이다). 아래의 표 5는 도 6c 및 표 3을 참조하

여 위에서 정의된 분할 요소(468)에 대한 분할 요소 키(472)를 나타낸 것이다.

[0145] [표 5]

[0146] 분할 요소 키(472)

[0147]

분할 요소	분할 요소 키
분할 요소 "L"(4680)	키 K_L(4720)
분할 요소 "M"(4682)	키 K_M(4722)
분할 요소 "N"(4684)	키 K_N(4724)
분할 요소 "O"(4686)	키 K_O(4726)
분할 요소 "P"(4688)	키 K_P(4728)

[0148] 따라서, 분할 요소 키 K_L(4720)는 분할 요소 "L"(4680)과 관련되고 분할 요소 키 K_M(4722)는 분할 요소 "M"(4682)과 관련되는 등으로 관련된다. 분할 요소 키 발생기(470)는 분할 요소(468)가 정보 집합체 분할기(462)에 의해 최초 생성될 때 분할 요소 키(472)를 발생한다. 대안적으로, 분할 요소 키는 제1 사용자가 분할 요소의 토픽에 가입한 때 특수 분할 요소에 대하여 발생될 수 있다. 이것은 사용자가 분할 요소의 어느 토픽에도 가입하지 않았을 때 분할 요소에 대한 키 발생을 회피하는 장점을 갖는다. 추가적으로, 액세스 제어 리스트(460)에 대한 변화는 분할 요소(468)에 대한 변화를 가져올 수 있다. 분할 요소(468) 중의 하나가 변화(추가의 토픽을 분할 요소에 포함시키거나 토픽을 분할 요소로부터 배제하는 것과 같은)할 때, 그 대응하는 분할 요소 키(472)를 재발생하는 것이 바람직하다. 분할 요소 키의 재발생은 액세스 제어 리스트(460)를 통하여 특수 토픽에 대해 공개된 정보에 액세스하도록 새로 인증된 사용자가 예전에 전송된 멀티캐스트 메시지를 복호하는 것을 방지하도록 하는 것이 바람직하다. 또한 토픽 키의 재발생은 새로 비인증된 사용자가 액세스 제어 리스트(460)를 통하여 미래의 멀티캐스트 메시지의 복호를 계속하는 것을 방지하도록 하는 것이 바람직하다.

[0149] 도 4a로 돌아가서, 정보 공급자(402)는 도 1a의 것과 동일한 논리 키 계층(412)을 또한 포함한다. 본 발명의 양호한 실시예에서, 논리 키 계층은 분할 요소 키(472)를 멀티캐스트 청중(408) 내의 인증된 사용자에게 안전하게 통신하기 위해 사용된다. 도 7a는 도 4a의 논리 키 계층(412)의 일 예이다. 논리 키 계층(412)은 공중/사설 키 암호화에 사용하기 위한 공중 암호화 키의 논리 나무 구조이다. 공중 키 F(41202a)는 논리 키 계층(412)의 뿌리에 있다. 공중 키 F1(41204a)와 F2(41206a)는 공중 키 F(41202a)로부터 직접 내려온다. 공중 키 F11(41208a)와 F12(41210a)는 공중 키 F1(41204a)로부터 직접 내려온다. 공중 키 F121(41212a)와 F122(41214a)는 공중 키 F12(41210a)로부터 직접 내려온다. 논리 키 계층(412)은 사용자(410a-410d) 각각을 위한 표시자를 포함한다. 각 표시자는 논리 나무 구조의 '잎' 키와 관련된다. 표시자(480a)는 사용자(410a)에 대응하고 공중 키 F11(41208a)과 관련된다. 표시자(480b)는 사용자(410b)에 대응하고 공중 키 F121(41212a)과 관련된다. 이하 같다.

[0150] 각각의 사용자(410a-410d)는 사용자의 관련 잎 키로부터 논리 키 계층(412)의 뿌리까지의 경로에 있는 각 공중 키에 대응하는 사설 키에 대한 액세스를 갖는다. 제1 사용자(410a)를 생각해서, 도 7b는 도 7a의 표시자(480a)에 의해 논리 키 계층(112)에서의 공중 키 F11(41208a)과 관련된 사용자(410a)의 예를 도시한 것이다. 사용자(410a)는 키 F(41202a), F1(41204a) 및 F11(41208a)의 각각에 대응하는 사설 키에 대한 액세스를 갖는데, 그 이유는 이들 키가 그 관련된 잎 키로부터 뿌리까지의 경로에 있기 때문이다. 그러므로, 사용자(410a)는 공중 키 F(41202a)에 대응하는 사설 키 F(41202b), 공중 키 F1(41204a)에 대응하는 사설 키 F1(41204b) 및 공중 키 F11(41208a)에 대응하는 사설 키 F11(41208b)에 대한 액세스를 갖는다.

[0151] 사용자(410a)는 또한 하나 이상의 복호 키를 이용하여 암호화 데이터 아이템의 복호 버젼을 발생하기 위한 하드웨어 또는 소프트웨어 장치 또는 엔티티인 복호기(4102a)를 포함한다. 예를 들어서, 복호기(4102a)는 사설 키 F11(41208b) 등의 사설 복호 키를 이용하여 데이터의 아이템을 복호하기 위해 사용할 수 있다. 복호기(4102a)의 일 예는 "프리티 굿 프라이버시"(PGP) 제품이다.

[0152] 유사하게, 사용자(410b-410d)는 각 사용자의 관련 잎 키로부터 논리 키 계층(412)의 루트까지의 경로에서 각 공중 키에 대응하는 사설 키에 대한 액세스를 갖는다. 사용자(410a-410d)와의 대응관계는 도 7c 내지 도 7e에 제공된다. 이 예시적인 실시예에서, 각 사용자(410a-410d)는 논리 키 계층(412)의 공중 키 F(41202a)에 대응하는 사설 키 F(41202b)에 대한 액세스를 갖는다는 점에 주목하여야 한다. 따라서 공중 키 F(41202a)를 이용하여 정

보 공급자(402)에 의해 암호화된 데이터는 모든 사용자(410a-410d)에 의해 복호될 수 있다. 유사하게, 다른 사용자 그룹이 논리 키 계층(412)에 따라 공동 키를 공유한다. 예를 들어서, 사용자 410b와 410c는 둘 다 사설 키 F12(41210b)에 대한 액세스를 갖고, 한편 다른 사용자는 사설 키 F12(41210b)에 대한 액세스를 갖지 못한다. 따라서, 공중 키 F12(41210a)를 이용하여 정보 공급자(402)에 의해 암호화된 데이터는 대응하는 사설 키 F12(41210b)를 이용하여 사용자(410b, 410c)에 의해서만 복호될 수 있다. 이 방법에서, 논리 키 계층(412)은 멀티캐스트 청중(408)의 인증된 사용자에게만 분할 요소 키(472)를 분배하기 위해 사용될 수 있다.

[0153] 도 8은 본 발명의 양호한 실시예에 따라 멀티캐스트 시스템의 정보를 공개하기 위한 방법을 나타내는 흐름도이다. 공개자(448a, 448b) 중의 하나가 계층 정보 집합체(420)의 토픽에 대해 정보를 공개할 때, 정보 공급자(402)는 도 8의 방법을 이용하여 정보를 멀티캐스트 청중(408)에게 멀티캐스트 메시지로서 멀티캐스팅한다. 처음에, 단계 802에서, 정보 공급자(402)는 정보가 공개될 토픽을 분할 요소(468) 중의 어느 것이 포함하는 지를 결정한다. 결정된 분할 요소는 분할 요소 키(472)로부터의 관련 키를 가질 것이다. 이어서, 단계 804에서, 공개된 정보는 상기 결정된 분할 요소용의 분할 요소 키를 이용하여 멀티캐스트 메시지로서 암호화된다. 단계 806에서, 분할 요소 키는 논리 키 계층(412)으로부터의 공중 키를 이용하여 인증된 사용자용으로 자체 암호화된다. 따라서, 분할 요소 키는 토픽에 대해 공개된 정보에 액세스하도록 인증된 사용자만이 분할 요소 키를 복호할 수 있도록 암호화된다. 이 논리 키 계층을 사용하는 기술은 당업계에 잘 알려져 있고, 웽 등의 논문에 자세히 설명되어 있다. 마지막으로, 단계 808에서, 암호화된 분할 요소 키 및 암호화된 멀티캐스트 메시지는 멀티캐스터(452)에 의해 멀티캐스트 청중(408)에게 통신된다. 이 방법에서, 공개 정보는 정보가 공개되는 토픽을 포함한 분할 요소에 대응하는 분할 요소 키를 이용하여 암호화된다. 따라서, 계층 정보 집합체(420) 내의 각 토픽용의 별도의 키를 필요로 하지 않는다.

[0154] 이제, 도 8의 방법을 도 6a에 정의된 계층 정보 집합체(420)의 구성 및 상기 표 2a 및 2b에 정의된 액세스 제어 리스트(460)에 대하여 사용하는 것과 관련하여 설명한다. 도 6c 및 표 3의 분할 요소(468)의 정의가 또한 적용된다. 정보가 공개자(448a, 448b)에 의해 공개되는 3가지의 시나리오가 생각된다. 이 3가지의 시나리오는 아래의 표 6에 표시되어 있다.

[0155] [표 6]

[0156] 시나리오

[0157]

시나리오	공개자	토픽
시나리오 1	공개자(448a)	"유럽"(612)
시나리오 2	공개자(448b)	"서해안"(610)
시나리오 3	공개자(448a)	"아시아"(614)

[0158] 먼저, 시나리오 1에 대하여 도 8의 방법을 생각하자. 시나리오 1에서, 공개자(448a)는 토픽 "유럽"(612)에 대한 정보를 공개한다. 초기에, 단계 802에서, 정보 공급자(402)는 정보가 공개되는 토픽을 분할 요소(468) 중의 어느 것이 포함하는지를 결정한다. 표 3의 분할 요소의 정의를 참조해서, 정보 공급자(402)는 토픽 "유럽"(612)이 분할 요소 "0"(4686)에 존재한다고 결정할 수 있다. 또한, 표 5로부터, 분할 요소 "0"(4686)는 관련된 분할 요소 키 K_0(4726)를 갖는다. 이어서, 단계 804에서, 공개 정보는 분할 요소 키 K_0(4726)를 이용하여 멀티캐스트 메시지로서 암호화된다. 단계 806에서, 분할 요소 키 K_0(4726)는 논리 키 계층(412)으로부터의 공중 키를 이용하여 인증된 사용자용으로 자체 암호화된다. 정보 공급자(402)는 표 2a 및 표 2b에 정의된 액세스 제어 리스트(460)를 참조하여 토픽 "유럽"(612)에 대해 공개된 정보에 액세스하도록 어느 사용자가 인증되는 지를 결정할 수 있다. 표 2a로부터, 토픽 "유럽"(612)은 ("비행기 여행/국제/#"에 의해) 롤 "태평양"(622)에 포함되고, ("비행기 여행/국제/유럽"에 의해) 롤 "국내-유럽"(626)에 포함되며 ("비행기 여행/#"에 의해) 롤 "모두"(628)에 포함됨을 알 수 있다. 따라서, 이들 롤에 속하는 사용자는 토픽 "유럽"(612)에 대해 공개된 정보에 액세스하도록 인증된다. 표 2b로부터, 사용자(410b)는 롤 "태평양"(622)의 멤버이고, 사용자(410c)는 롤 "국내-유럽"(626)의 멤버임을 알 수 있다. 따라서, 사용자(410b, 410c)는 토픽 "유럽"(612)에 대해 공개된 정보에 액세스하도록 인증된다. 그래서, 단계 806에서, 사용자(410b, 410c)에게만 액세스가능한 논리 키 계층(412)으로부터의 키는 분할 요소 키 K_0(4726)를 암호화하도록 선택된다. 도 7a 내지 도 7e로부터, 단지 사용자(410b 및 410c)만이 대응하는 사설 키 F12(41210b)를 갖기 때문에, 공중 키 F12(14210a)가 적당하다는 것을 알 수 있다. 그러므로, 분할 요소 키 K_0(4726)는 공중 키 F12(41210a)를 이용하여 정보 공급자(402)에 의해 암호화된다. 마지막으로, 단계

808에서, 암호화된 분할 요소 키 K_0(4726) 및 암호화된 멀티캐스트 메시지가 멀티캐스터(452)에 의해 멀티캐스트 청중(408)에게 통신된다. 이 방법에서, 암호화된 분할 요소 키 K_0(4726)는 인증된 사용자(410b, 410c)에게만 액세스가능하고, 따라서 이들 사용자만이 공개 정보를 포함한 멀티캐스트 메시지를 복호할 수 있다.

[0159] 다음에 시나리오 2에 대하여 도 8의 방법을 생각하자. 시나리오 2에서, 공개자(448b)는 토픽 "서해안"(610)에 대한 정보를 공개한다. 초기에, 단계 802에서, 정보 공급자(402)는 정보가 공개되는 토픽을 분할 요소(468) 중의 어느 것이 포함하는지를 결정한다. 표 3의 분할 요소의 정의를 참조해서, 정보 공급자(402)는 토픽 "서해안"(610)이 분할 요소 "N"(4684)에 존재한다고 결정할 수 있다. 또한, 표 5로부터, 분할 요소 "N"(4684)은 관련된 분할 요소 키 K_N(4724)을 갖는다. 이어서, 단계 804에서, 공개 정보는 분할 요소 키 K_N(4724)을 이용하여 멀티캐스트 메시지로서 암호화된다. 단계 806에서, 분할 요소 키 K_N(4724)은 논리 키 계층(412)으로부터의 공중 키를 이용하여 인증된 사용자용으로 자체 암호화된다. 정보 공급자(402)는 표 2a 및 표 2b에 정의된 액세스 제어 리스트(460)를 참조하여 토픽 "서해안"(610)에 대해 공개된 정보에 액세스하도록 어느 사용자가 인증되는 지를 결정할 수 있다. 표 2a로부터, 토픽 "서해안"(610)은 ("비행기 여행/국내/서해안"에 의해) 롤 "태평양"(622)에 포함되고, ("비행기 여행/국내/#"에 의해) 롤 "국내-유럽"(626)에 포함되며 ("비행기 여행/#"에 의해) 롤 "모두"(628)에 포함됨을 알 수 있다. 따라서, 이들 롤에 속하는 사용자는 토픽 "서해안"(610)에 대해 공개된 정보에 액세스하도록 인증된다. 표 2b로부터, 사용자(410a)는 롤 "국내"(624)의 멤버이고, 사용자 (410b)는 롤 "태평양"(622)의 멤버이며, 사용자(410c)는 롤 "국내-유럽"(626)의 멤버임을 알 수 있다. 따라서, 사용자(410a, 410b, 410c)는 토픽 "서해안"(610)에 대해 공개된 정보에 액세스하도록 인증된다. 그래서, 단계 806에서, 사용자(410a, 410b, 410c)에게만 액세스가능한 논리 키 계층(412)으로부터의 키는 분할 요소 키 K_N(4724)를 암호화하도록 선택된다. 도 7a 내지 도 7e로부터, 단지 사용자(410a, 410b, 410c)만이 대응하는 사설 키 F1(41204b)를 갖기 때문에, 공중 키 F1(41204a)가 적당하다는 것을 알 수 있다. 그러므로, 분할 요소 키 K_N(4724)는 공중 키 F1(41204a)를 이용하여 정보 공급자(402)에 의해 암호화된다. 마지막으로, 단계 808에서, 암호화된 분할 요소 키 K_N(4724) 및 암호화된 멀티캐스트 메시지가 멀티캐스터(452)에 의해 멀티캐스트 청중(408)에게 통신된다. 이 방법에서, 암호화된 분할 요소 키 K_N(4724)는 인증된 사용자(410a, 410b, 410c)에게만 액세스가능하고, 따라서, 이들 사용자만이 공개 정보를 포함한 멀티캐스트 메시지를 복호할 수 있다.

[0160] 다음에 시나리오 3에 대하여 도 8의 방법을 생각하자. 시나리오 3에서, 공개자(448a)는 "아시아"(614)에 대한 정보를 공개한다. 초기에, 단계 802에서, 정보 공급자(402)는 정보가 공개되는 토픽을 분할 요소(468) 중의 어느 것이 포함하는지를 결정한다. 표 3의 분할 요소의 정의를 참조해서, 정보 공급자(402)는 토픽 "아시아"(614)가 분할 요소 "P"(4688)에 존재한다고 결정할 수 있다. 또한, 표 5로부터, 분할 요소 "P"(4688)는 관련된 분할 요소 키 K_P(4728)를 갖는다. 이어서, 단계 804에서, 공개 정보는 분할 요소 키 K_P(4728)를 이용하여 멀티캐스트 메시지로서 암호화된다. 단계 806에서, 분할 요소 키 K_P(4728)는 논리 키 계층(412)으로부터의 공중 키를 이용하여 인증된 사용자용으로 자체 암호화된다. 정보 공급자(402)는 표 2a 및 표 2b에 정의된 액세스 제어 리스트(460)를 참조하여 토픽 "아시아"(614)에 대해 공개된 정보에 액세스하도록 어느 사용자가 인증되는 지를 결정할 수 있다. 표 2a로부터, 토픽 "아시아"(614)는 ("비행기 여행/국제/#"에 의해) 롤 "태평양"(622)에 포함되고, ("비행기 여행/#"에 의해) 롤 "모두"(628)에 포함됨을 알 수 있다. 따라서, 이들 롤에 속하는 사용자는 토픽 "아시아"(614)에 대해 공개된 정보에 액세스하도록 인증된다. 표 2b로부터, 사용자(410b)는 롤 "태평양"(622)의 멤버임을 알 수 있다. 따라서, 사용자(410b)는 토픽 "아시아"(614)에 대해 공개된 정보에 액세스하도록 인증된다. 그래서, 단계 806에서, 사용자(410b)에게만 액세스가능한 논리 키 계층(412)으로부터의 키는 분할 요소 키 K_P(4728)를 암호화하도록 선택된다. 도 7a 내지 도 7e로부터, 단지 사용자(410b)만이 대응하는 사설 키 F121(41212b)를 갖기 때문에, 공중 키 F121(14212a)가 적당하다는 것을 알 수 있다. 그러므로, 분할 요소 키 K_P(4728)는 공중 키 F121(41212a)를 이용하여 정보 공급자(402)에 의해 암호화된다. 마지막으로, 단계 808에서, 암호화된 분할 요소 키 K_P(4728) 및 암호화된 멀티캐스트 메시지가 멀티캐스터(452)에 의해 멀티캐스트 청중(408)에게 통신된다. 이 방법에서, 암호화된 분할 요소 키 K_P(4728)는 인증된 사용자(410b)에게만 액세스가능하고, 따라서, 이 사용자만이 공개 정보를 포함한 멀티캐스트 메시지를 복호할 수 있다.

[0161] 따라서, 액세스 제어 리스트(460)가 제공된 경우, 키는 각각의 개별 토픽 대신에 분할 요소(468)로서 토픽의 그룹에 할당될 수 있다. 이 방법에서, 액세스 제어의 입상이 요구하지 않는 한(즉, 액세스 제어가 토픽 당 기준으

로으로 정의되지 않는 한) 각 토픽에 대하여 키를 할당할 필요가 없다.

도면의 간단한 설명

[0028] 이하, 본 발명의 바람직한 실시예를 첨부 도면을 참조하여 단지 예로서 상세히 설명하겠다.

[0029] 도 1a는 본 발명의 양호한 실시예에 따른 멀티캐스트 정보 공급자를 포함한 멀티캐스트 공개/가입 시스템을 나타내는 개략적 블록도이다.

[0030] 도 1b는 본 발명의 양호한 실시예에 따른 도 1a의 계층 정보 집합체의 예를 나타낸 도이다.

[0031] 도 1c는 본 발명의 양호한 실시예에 따른 도 1a의 토픽 키 계층의 예를 나타낸 도이다.

[0032] 도 1d는 종래 기술에서 공지된 것인 도 1a의 논리 키 계층(112)의 예를 나타낸 도이다.

[0033] 도 1e는 도 1d의 표시자(indicator)에 의해 도 1a의 논리 키 계층의 키 A1과 관련된 사용자의 예를 나타낸 도이다.

[0034] 도 1f는 도 1d의 표시자에 의해 논리 키 계층의 키 A2와 관련된 사용자의 예를 나타낸 도이다.

[0035] 도 2는 본 발명의 양호한 실시예에 따라 멀티캐스트 시스템에서 정보를 공개하는 방법을 나타낸 흐름도이다.

[0036] 도 3은 본 발명의 양호한 실시예에 따라 토픽 키를 재발생하는 방법을 나타낸 흐름도이다.

[0037] 도 4a는 본 발명의 양호한 실시예에 따라 멀티캐스트 정보 공급자를 포함한 멀티캐스트 공개/가입 시스템을 나타내는 개략적 블록도이다.

[0038] 도 4b는 본 발명의 양호한 실시예에 따라 도 4a의 액세스 제어 리스트를 나타낸 도이다.

[0039] 도 5a는 본 발명의 양호한 실시예에 따라 도 4a의 분할 요소를 정의하기 위한 방법의 흐름도이다.

[0040] 도 5b는 본 발명의 양호한 실시예에서 부분집합의 리스트로부터 서로소 부분집합의 리스트를 발생하는 방법을 나타낸 흐름도이다.

[0041] 도 5c는 본 발명의 양호한 실시예에 따라 계층 정보 집합체의 부분집합의 정의를 포함한, 도 4a의 계층 정보 집합체의 예를 나타낸 도이다.

[0042] 도 5d는 본 발명의 양호한 실시예에 따라 도 5c의 계층 정보 집합체에 대하여 도 5b의 방법을 이용하여 발생된 서로소 진 부분집합을 나타낸 도이다.

[0043] 도 6a는 본 발명의 양호한 실시예에 따라 도 4a의 계층 정보 집합체의 예를 나타낸 도이다.

[0044] 도 6b는 본 발명의 양호한 실시예에 따라 도 4a의 액세스 제어 리스트 및 도 6a의 계층 정보 집합체를 나타낸 개략도이다.

[0045] 도 6c는 본 발명의 양호한 실시예에 따라 도 4a의 분할 요소의 예를 나타낸 도이다.

[0046] 도 7a는 본 발명의 양호한 실시예에 따라 도 4a의 논리 키 계층의 예를 나타낸 도이다.

[0047] 도 7b는 도 7a의 표시자에 의해 도 4a의 논리 키 계층 내의 키 F11과 관련된 사용자의 예를 나타낸 도이다.

[0048] 도 7c는 도 7a의 표시자에 의해 도 4a의 논리 키 계층 내의 키 F121과 관련된 사용자의 예를 나타낸 도이다.

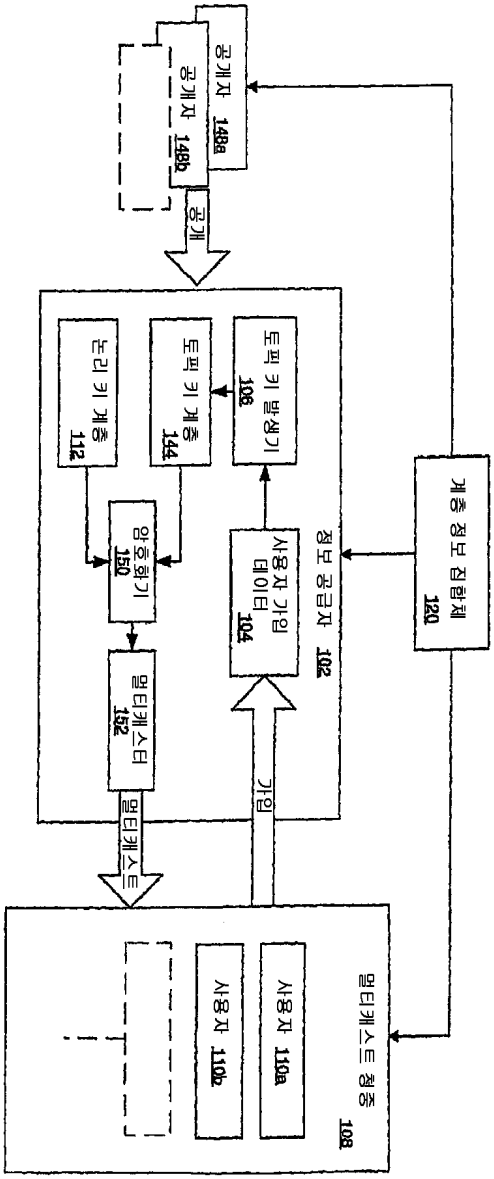
[0049] 도 7d는 도 7a의 표시자에 의해 도 4a의 논리 키 계층 내의 키 F122와 관련된 사용자의 예를 나타낸 도이다.

[0050] 도 7e는 도 7a의 표시자에 의해 도 4a의 논리 키 계층 내의 키 F2와 관련된 사용자의 예를 나타낸 도이다.

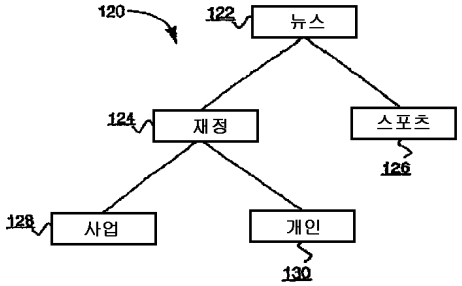
[0051] 도 8은 본 발명의 양호한 실시예에 따라 멀티캐스트 시스템에서 정보를 공개하기 위한 방법을 나타낸 흐름도이다.

도면

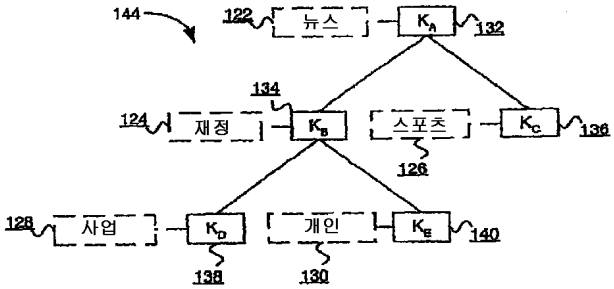
도면1a


공개자 148a
공개자 148b
공개
토픽 키 발생기 106
토픽 키 계층 144
논리 키 계층 112
암호화기 150
사용자 가입 데이터 104
정보 공급자 102
계층 정보 집합체 120
멀티캐스터 152
가입
멀티캐스트
사용자 110b
사용자 110a
멀티캐스트 청중 108

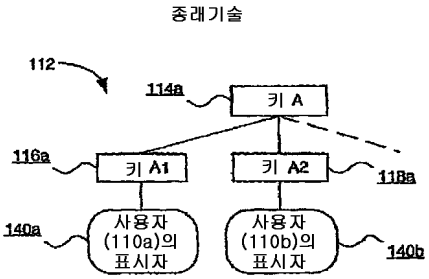
도면1b


120
122
뉴스
124
재정
스포츠
126
128
사업
개인
130

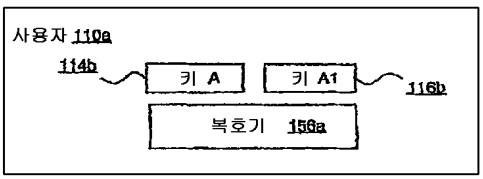
도면1c



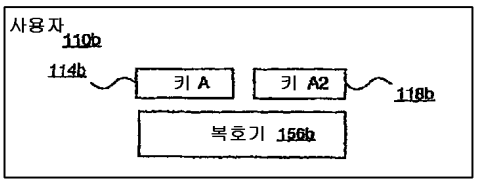
도면1d



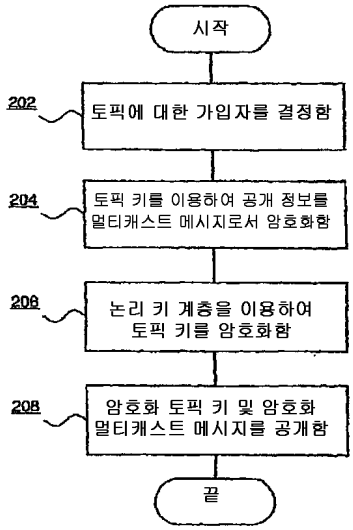
도면1e



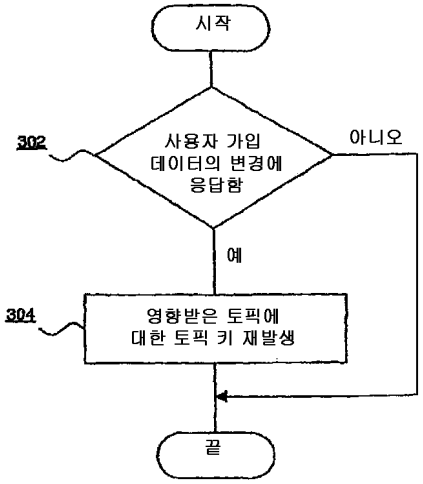
도면1f



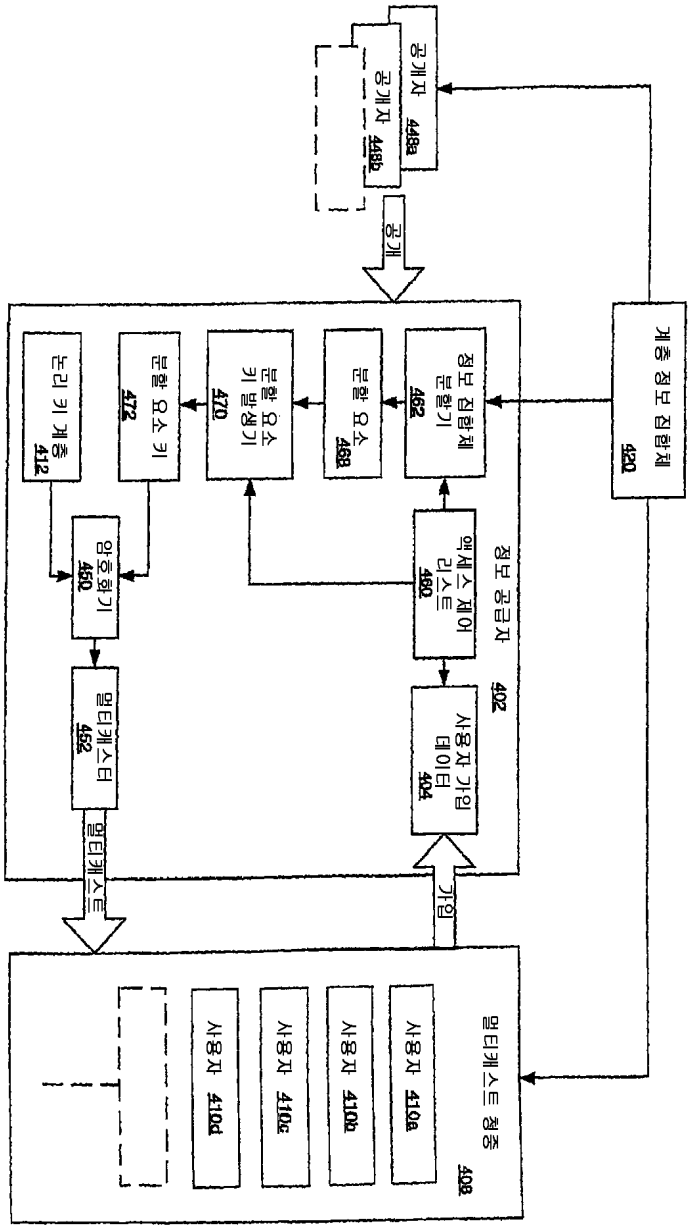
도면2


시작
202
토픽에 대한 가입자를 결정함
204
토픽 키를 이용하여 공개 정보를 멀티캐스트 메시지로서 암호화함
206
논리 키 계층을 이용하여 토픽 키를 암호화함
208
암호화 토픽 키 및 암호화 멀티캐스트 메시지를 공개함
끝

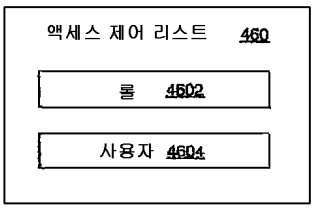
도면3


시작
302
사용자 가입 데이터의 변경에 응답함
아니오
예
304
영향받은 토픽에 대한 토픽 키 재발생
끝

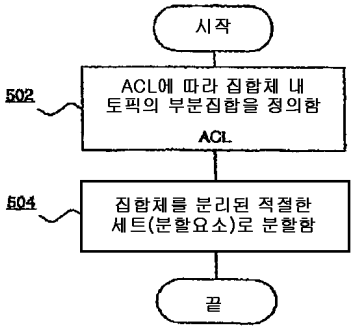
도면4a


공개자 448a
공개자 448b
공개
계층 정보 집합체 420
정보 집합체 462
분할 요소 468
분할 요소 키 발생기 470
분할 요소 키 472
논리 키 계층 412
암호화기 460
멀티캐스터 452
멀티캐스트
액세스 제어 리스트 492
사용자 가입 데이터 494
가입
정보 공급자 402
멀티캐스트 청중 408
사용자 410a
사용자 410b
사용자 410c
사용자 410d

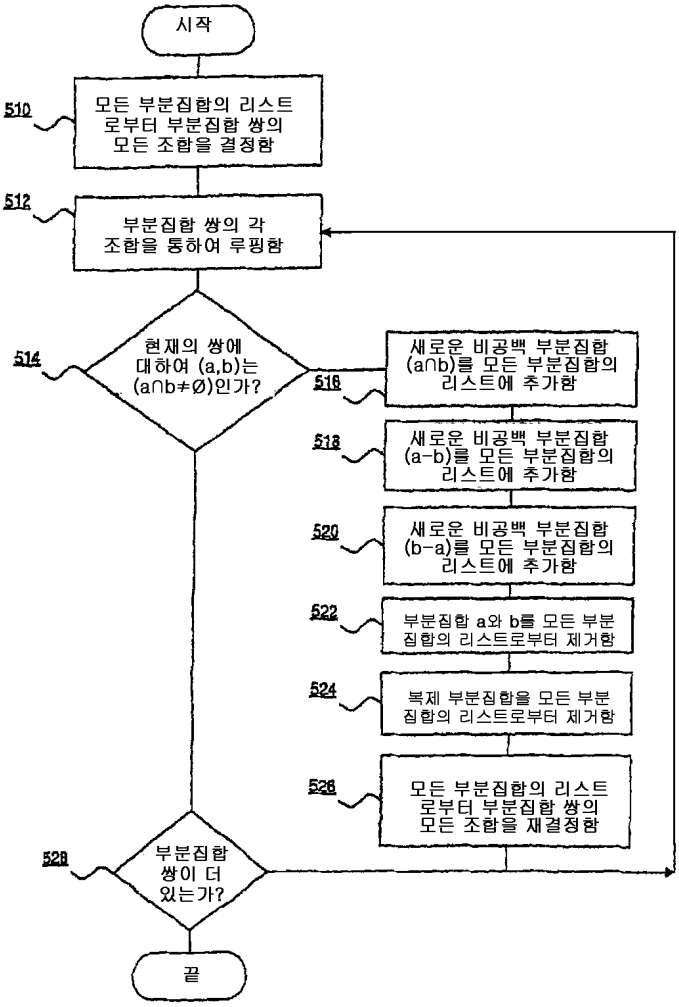
도면4b


액세스 제어 리스트 460
롤 4602
사용자 4604

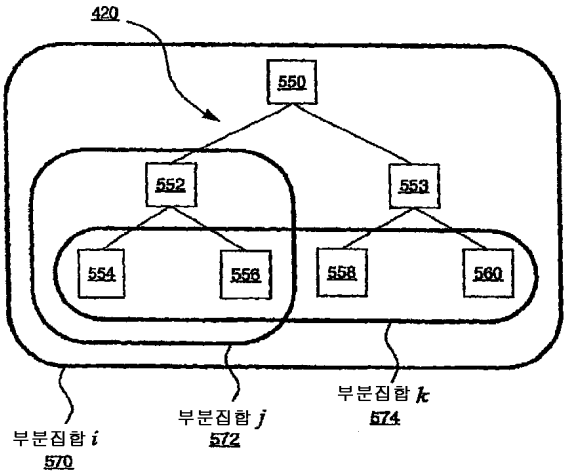
도면5a


시작
502
ACL에 따라 집합체 내 토픽의 부분집합을 정의함
ACL
504
집합체를 분리된 적절한 세트(분할요소)로 분할함
끝

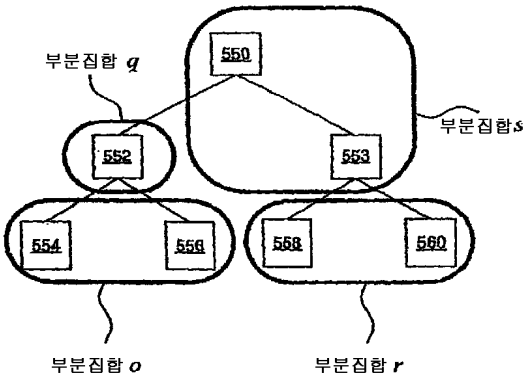
도면5b


시작
510
모든 부분집합의 리스트로부터 부분집합 쌍의 모든 조합을 결정함
512
부분집합 쌍의 각 조합을 통하여 루핑함
514
현재의 쌍에 대하여 (a,b)는 (a∩b≠Ø)인가?
516
새로운 비공백 부분집합 (a∩b)를 모든 부분집합의 리스트에 추가함
518
새로운 비공백 부분집합 (a-b)를 모든 부분집합의 리스트에 추가함
520
새로운 비공백 부분집합 (b-a)를 모든 부분집합의 리스트에 추가함
522
부분집합 a와 b를 모든 부분집합의 리스트로부터 제거함
524
복제 부분집합을 모든 부분집합의 리스트로부터 제거함
526
모든 부분집합의 리스트로부터 부분집합 쌍의 모든 조합을 재결정함
528
부분집합 쌍이 더 있는가?
끝

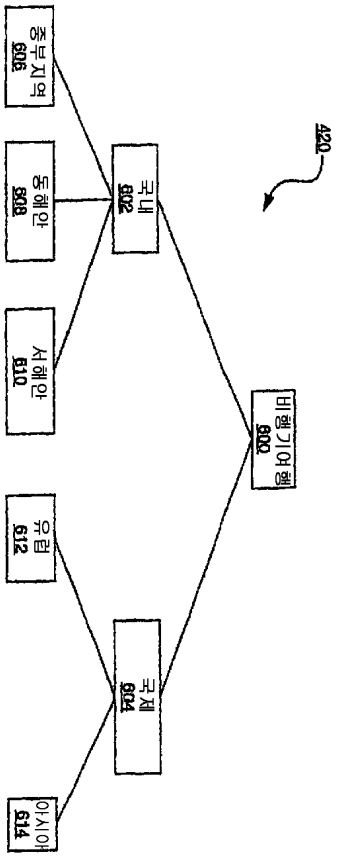
도면5c


420
550
552
553
554
556
558
560
부분집합 i
570
부분집합 j
572
부분집합 k
574

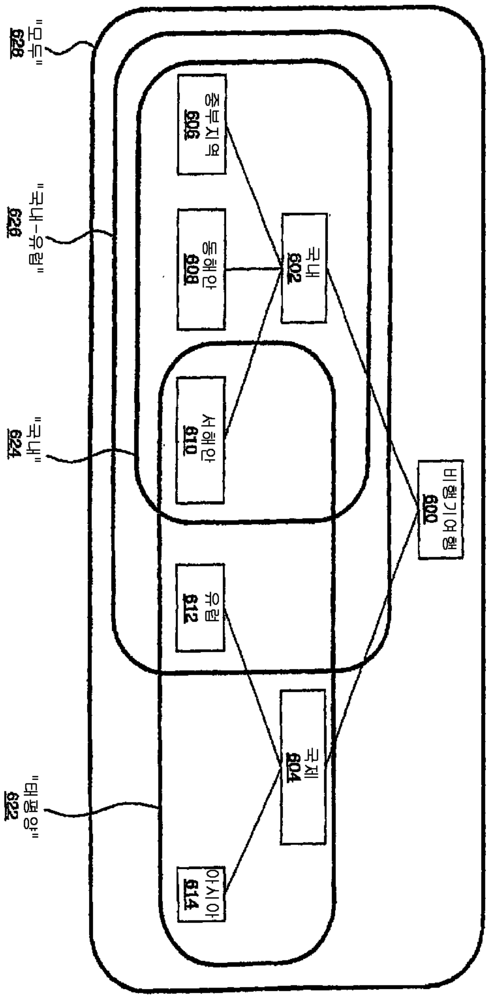
도면5d


부분집합 q
550
부분집합s
552
553
554
556
558
560
부분집합 o
부분집합 r

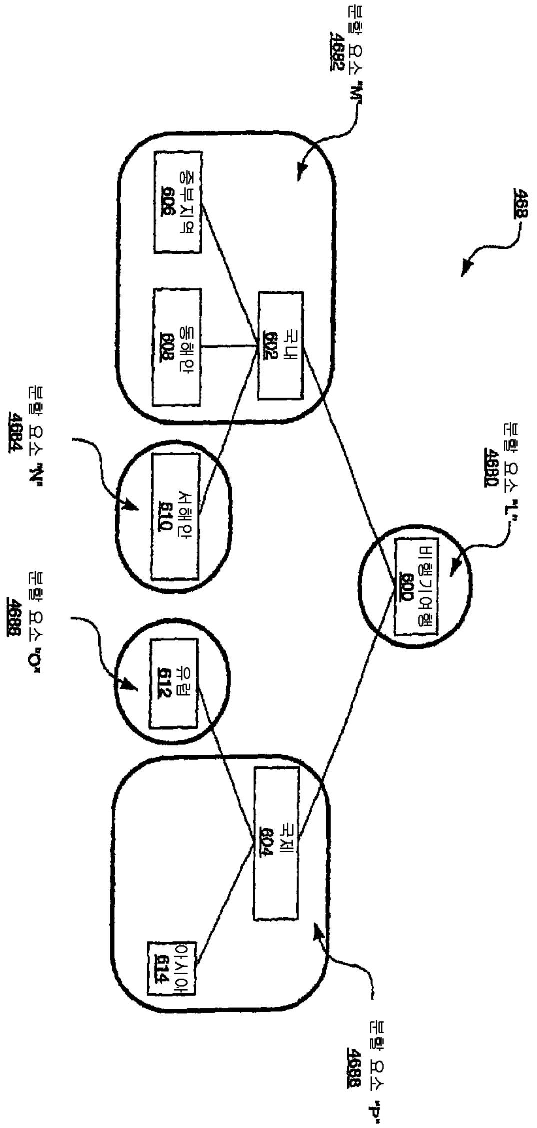
도면6a


420
중부지역
606
동해안
608
서해안
610
유럽
612
아시아
614
내륙
602
해양
604
비행기여행
600

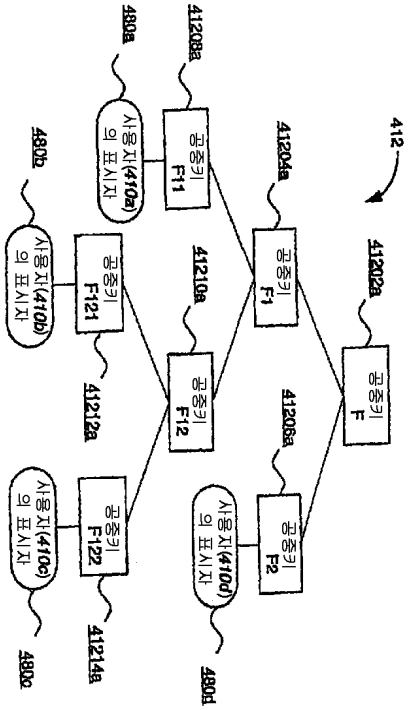
도면6b


"모두"
628
"국내-유럽"
626
"국내"
624
"태평양"
622
중부지역
606
동해안
608
서해안
610
유럽
612
아시아
614
국내
602
국제
604
비행기여행
600

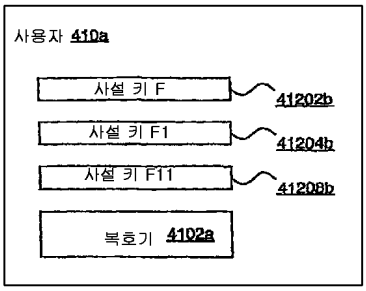
도면6c


468
분할 요소 "M" 4682
분할 요소 "N" 4684
분할 요소 "O" 4686
분할 요소 "P" 4688
분할 요소 "L" 4680
중부지역 606
동해안 608
국내 602
서해안 610
비행기여행 600
유럽 612
국제 604
아시아 614

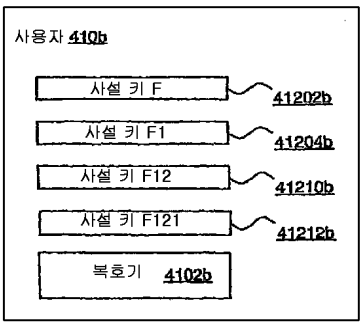
도면7a



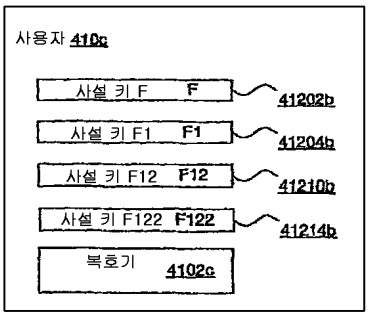
도면7b



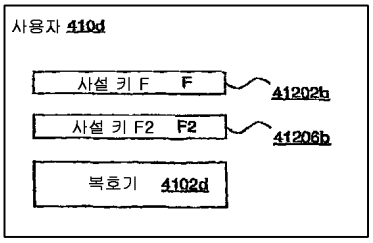
도면7c



도면7d



도면7e



도면8