(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2009-0084809
(43) 공개일자 2009년08월05일

(51) Int. Cl.
H04L 9/08 (2006.01) *H04W 12/04* (2009.01)
(21) 출원번호 10-2009-7006550
(22) 출원일자 2007년08월17일
심사청구일자 없음
(85) 번역문제출일자 2009년03월30일
(86) 국제출원번호 PCT/JP2007/066002
(87) 국제공개번호 WO 2008/053629
국제공개일자 2008년05월08일
(30) 우선권주장
JP-P-2006-294639 2006년10월30일 일본(JP)

(71) 출원인
소니 가부시끼 가이샤
일본국 도쿄도 미나토쿠 코난 1-7-1
(72) 발명자
구사카와 마사후미
일본 도쿄 미나토-쿠 코난 1-7-1 소니 가부시끼 가이샤내
아사노 토모유키
일본 도쿄 미나토-쿠 코난 1-7-1 소니 가부시끼 가이샤내
(74) 대리인
신관호

전체 청구항 수 : 총 22 항

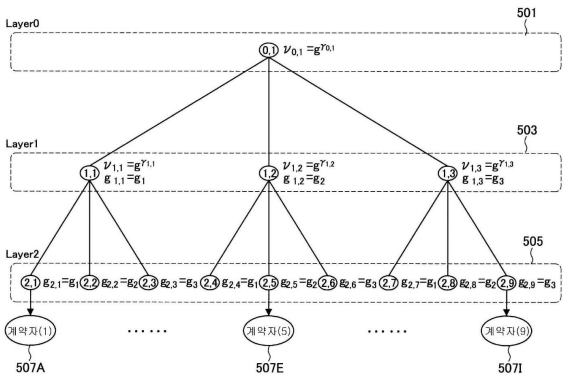
(54) 키생성장치, 암호화장치, 수신장치, 키생성방법, 암호화방법, 키처리방법 및 프로그램

(57) 요 약

본 발명과 관련되는 키생성장치는, n개의 수신장치가 리프에 할당된 Y분 나무를 계층적으로 구성하고, 해당 Y분 나무의 리프와 루트와의 사이에 존재하는 중간 노드를 각각 부모 노드로 하는 서브그룹을 구성한다.

중간 노드 각각에, 새롭게 파라미터를 부여함으로써, 서브그룹의 구성을 유연하게 실시할 수 있으며, 배제되는 계약자가 없거나 혹은 적은 경우에 있어서, 전달되는 헤더 사이즈 및 계약자가 실행할 필요가 있는 연산의 계산량을 삭감하는 것이 가능하다.

대 표 도



특허청구의 범위

청구항 1

n개의 수신장치가 리프(leaf)에 할당되며, 높이가 ($\log_Y n$)로 표시되는 Y분 나무를 계층적으로 구성하고, 상기 리프와 루트(root)와의 사이에 존재하는 중간 노드의 하위에 존재하는 복수의 상기 리프로 이루어지는 서브그룹을 구성하는, 나무구조 구성부와,

상기 리프 및 상기 중간 노드 각각에 대하여, 리프키(g_y)를 할당하는 리프키 할당부와,

상기 중간 노드 및 상기 루트에, 상이 되는 파라미터 $v_{x,y}$(x : 계층, y : 1, 2, …, Y^x)와 노드 파라미터 $\gamma_{x,y}$(x : 계층, y : 1, 2, …, Y^x)를 각각 할당하는 파라미터 할당부와,

상기 루트로부터 상기 리프에 이르는 패스를 특정하고, 해당 패스 상에 존재하는 상기 중간 노드 또는 상기 리프에 할당된 상기 리프키(g_y)와, 해당 중간 노드 또는 해당 리프의 친(親) 노드에 할당된 상기 파라미터($v_{x,y}$) 및 상기 노드 파라미터($\gamma_{x,y}$)에 의거하여, 키를 산출하는 키 산출부를 갖추는 것을 특징으로 하는 키생성장치.

청구항 2

제 1항에 있어서,

상기 키생성장치는, 상기 키 산출부에 의해 산출된 상기 패스 상의 키 세트를 각 수신장치 각각에 배포하는 배포부를, 더 갖추는 것을 특징으로 하는 키생성장치.

청구항 3

제 1항에 있어서,

상기키생성장치는,

소수(p)를 무작위로 선택하고, 상기 소수(p)를 위수(位數)라고 하는 쌍선형군(G)을 결정하여, 상기 G의 생성요소(g)를 무작위로 선택하고, 비밀의 난수 α(α는 정수)를 무작위로 선택하는 난수 결정부를 더 갖추며,

상기 리프키 할당부는, 이하의 식 A를 만족하는 상기 리프키(g_y)를 산출하는 것을 특징으로 하는 키생성장치.

[수학식 1]

$$g_y = g^{(\alpha)^y} \quad \cdots (\text{식 A})$$
$$(y = 1,\ 2,\ \cdots,\ Y,\ Y+2,\ \cdots,\ 2Y)$$

청구항 4

제 3항에 있어서,

상기 파라미터 할당부는, 상기 리프를 제외한 모든 노드와 상기 루트의 각각에 대하여, 노드 파라미터 $\gamma_{x,y}$($\gamma_{x,y}$는 정수)를 무작위로 선택하고, 이하의 식 B에서 표시되는 파라미터($v_{x,y}$)를 산출하는 것을 특징으로 하는 키생성장치.

[수학식 2]

$$v_{x,y} = g^{(\gamma_{x,y})} \quad \cdots (\text{식 B})$$

청구항 5

제 4항에 있어서,

상기 키 산출부는, 상기 중간 노드 또는 상기 리프에 할당된 상기 리프키(g_y)의, 해당 중간 노드 또는 해당 리프의 부모 노드에 할당된 상기 파라미터($\gamma_{x,y}$) 승으로 얻어지는 값을, 비밀키로 하는 것을 특징으로 하는 키생성장치.

청구항 6

제 5항에 있어서,

상기키 산출부는, 상기 리프키(g_y) 및 상기 파라미터($v_{x,y}$)에 의거하여, 공개키를 산출하고,

상기 배포부는, 상기 공개키를 공개하는 공개키 공개부를 갖추는 것을 특징으로 하는 키생성장치.

청구항 7

제 5항에 있어서,

상기 배포부는, 상기 키 산출부에 있어서 산출된 비밀키를 각 수신장치에 송신하는 송신부를 더 갖추는 것을 특징으로 하는 키생성장치.

청구항 8

n개의 수신장치 속에서 배제하는 수신장치를 특정하고, 배제되어 있지 않은 수신장치의 집합(S)을 결정하는, 배제 수신장치 특정부를 갖추는 것을 특징으로 하는 암호화장치.

청구항 9

제 8항에 있어서,

상기 암호화장치는, 정수(t)를 무작위로 선택하고, 세션 키 $s=e(g_Y, g_1)^t$를 결정하는 세션 키 결정부를, 더 갖추는 것을 특징으로 하는 암호화장치.

여기서, 상기 $e(g_Y, g_1)$는, 쌍선형군 상의 2개의 요소(g_Y, g_1)에 대한 쌍선형 사상(寫像)을 나타낸다.

청구항 10

제 9항에 있어서,

상기 암호화장치는, 상기 세션 키(s)를 이용하고, 전달하는 콘텐츠를 암호화하는 암호화부를 더 갖추는 것을 특징으로 하는 암호화장치.

청구항 11

제 9항에 있어서,

상기 세션 키 결정부는, 계층화된 나무구조에 있어서, 상기 배제된 수신장치가 할당된 리프로부터 상기 루트에 이르는 패스 상에 존재하는 모든 노드 각각에 마크를 첨부하고, 상기 마크된 노드에 할당된 상기 파라미터($v_{x,y}$)와, 상기 마크된 노드를 부모 노드로 하는 중간 노드에 할당된 리프키(g_y)에 의거하여, 이하의 식 C에서 표시되는 $c_{x,y}$를 산출하는 헤더 요소 산출부를, 더 갖추는 것을 특징으로 하는 암호화장치.

[수학식 3]

$$c_{x,y} = \left(v_{x,y} \cdot \prod_{j \in S_{x,y}} g_{Y+1-j}\right)^t \quad \cdots \text{(식 C)}$$

여기서, $S_{x,y}$는, 상기 마크된 노드를 부모 노드로 하는 각 서브그룹에 소속하는, 마크되어 있지 않은 자식 노드의 집합을 나타낸다.

청구항 12

제 11항에 있어서,

상기 세션 키 결정부는, 상기 헤더 요소 산출부에 있어서 얻어진 상기 $c_{x,y}$와, g^t를 헤더 정보로 하는 헤더 정보 생성부를 더 갖추는 것을 특징으로 하는 암호화장치.

청구항 13

키생성장치 및 암호화장치와 통신 가능한 수신장치이며,

상기 키생성장치에 있어서, n개의 수신장치가 리프에 할당되며, 높이가 ($\log_Y n$)으로 표시되는 Y분 나무를 계층적으로 구성하고, 상기 리프와 루트와의 사이에 존재하는 중간 노드의 하위에 존재하는 복수의 상기 리프로 이루어지는 서브그룹을 구성하고, 상기 리프 및 상기 중간 노드 각각에 대하여, 리프키(g_y)를 할당하고, 상기 중간 노드 및 상기 루트에, 서로 다른 파라미터 $v_{x,y}$(x : 계층, y : 1, 2, …, Y^x)와 노드 파라미터 $\gamma_{x,y}$(x : 계층, y : 1, 2, …, Y^x)를 각각 할당하고, 상기 루트로부터 상기 리프에 이르는 패스를 특정하고, 해당 패스 상에 존재하는 상기 중간 노드 또는 상기 리프에 할당된 상기 리프키(g_y)와, 해당 중간 노드 또는 해당 리프의 부모 노드에 할당된 상기 파라미터($v_{x,y}$) 및 상기 노드 파라미터($\gamma_{x,y}$)에 의거하여 산출된 키를 수신하는 수신부를 갖추는 것을 특징으로 하는 수신장치.

청구항 14

제 13항에 있어서,

상기 수신장치는, 암호화 콘텐츠를 세션 키(s)에 의해 복호하는 복호부를 더 갖추는 것을 특징으로 하는 수신장치.

청구항 15

제 14항에 있어서,

상기 수신부는, 배제하는 수신장치가 특정된 정보인, 배제되어 있지 않은 수신장치의 집합(S)에 관한 정보를 더 수신하고,

상기 수신장치는, 수신장치가 상기 집합(S)에 포함되어 있는지 아닌지를 판정하는 판정부를 더 갖추는 것을 특징으로 하는 수신장치.

청구항 16

제 14항에 있어서,

상기 판정부에 있어서, 수신장치가 상기 집합(S)에 포함되어 있다고 판정된 경우, 상기 복호부는, 세션 키(s)를 이하에 나타내는 식D에 의거하여 산출하고, 산출된 해당 세션 키(s)를 이용하는 것으로, 상기 암호화 콘텐츠를 복호화하는 것을 특징으로 하는 수신장치.

[수학식 4]

$$s = \frac{e(g_{i_{x'}}, c_{x,y})}{e(g_{i_{x'}}^{\gamma_{i_{x'-1}}} \cdot \prod_{\substack{j \in S_{x,y} \\ j \neq i_{x'}}} g_{Y+1-j+i_{x'}}, g^t)} \quad \cdots \text{(식D)}$$

청구항 17

n개의 수신장치가 리프에 할당되며, 높이가 ($\log_Y n$)로 표시되는 Y분 나무를 계층적으로 구성하고, 상기 리프와 루트와의 사이에 존재하는 중간 노드의 하위에 존재하는 복수의 상기 리프로 이루어지는 서브그룹을 구성하는

나무구조 구성 스텝과,

상기 리프 및 상기 중간 노드 각각에 대하여, 리프키(g_y)를 할당하는 리프키 할당 스텝과,

상기 중간 노드 및 상기 루트에, 서로 다른 파라미터 $v_{x,y}$(x : 계층, y : 1, 2, …, Y^x)와 노드 파라미터 $y_{x,y}$(x : 계층, y : 1, 2, …, Y^x)를 각각 할당하는 파라미터 할당 스텝과,

상기 루트로부터 상기 리프에 이르는 패스를 특정하고, 해당 패스 상에 존재하는 상기 중간 노드 또는 상기 리프에 할당된 상기 리프키(g_y)와, 해당 중간 노드 또는 해당 리프의 부모 노드에 할당된 상기 파라미터($v_{x,y}$) 및 상기 노드 파라미터($y_{x,y}$)에 의거하여, 키를 산출하는 키 산출 스텝을 갖추는 것을 특징으로 하는 키생성방법.

청구항 18

n개의 수신장치 속에서 배제하는 수신장치를 특정하고, 배제되어 있지 않은 수신장치의 집합(S)을 결정하는, 배제 수신장치 특정 스텝을 갖추는 것을 특징으로 하는 암호화방법.

청구항 19

n개의 수신장치가 리프에 할당되며, 높이가 ($\log_Y n$)로 표시되는 Y분 나무를 계층적으로 구성하고, 상기 리프와 루트와의 사이에 존재하는 중간 노드의 하위에 존재하는 복수의 상기 리프로 이루어지는 서브그룹을 구성하고, 상기 리프 및 상기 중간 노드 각각에 대하여, 리프키(g_y)를 할당하고, 상기 중간 노드 및 상기 루트에, 서로 다른 파라미터 $v_{x,y}$(x : 계층, y : 1, 2, …, Y^x)와 노드 파라미터 $y_{x,y}$(x : 계층, y : 1, 2, …, Y^x)를 각각 할당하고, 상기 루트로부터 상기 리프에 이르는 패스를 특정하여, 해당 패스 상에 존재하는 상기 중간 노드 또는 상기 리프에 할당된 상기 리프키(g_y)와, 해당 중간 노드 또는 해당 리프의 부모 노드에 할당된 상기 파라미터($v_{x,y}$) 및 상기 노드 파라미터($y_{x,y}$)에 의거하여 산출된 키를 수신하는 스텝을 갖추는 것을 특징으로 하는 키처리방법.

청구항 20

컴퓨터에,

n개의 수신장치가 리프에 할당되며, 높이가 ($\log_Y n$)로 표시되는 Y분 나무를 계층적으로 구성하고, 상기 리프와 루트와의 사이에 존재하는 중간 노드의 하위에 존재하는 복수의 상기 리프로 이루어지는 서브그룹을 구성하는, 나무구조 구성 기능과,

상기 리프 및 상기 중간 노드 각각에 대하여, 리프키(g_y)를 할당하는 리프키 할당 기능과,

상기 중간 노드 및 상기 루트에, 서로 다른 파라미터 $v_{x,}y$(x : 계층, y : 1, 2, …, Y^x)와 노드 파라미터 $y_{x,y}$(x : 계층, y : 1, 2, …, Y^x)를 각각 할당하는 파라미터 할당 기능과,

상기 루트로부터 상기 리프에 이르는 패스를 특정하고, 해당 패스 상에 존재하는 상기 중간 노드 또는 상기 리프에 할당된 상기 리프키(g_y)와, 해당 중간 노드 또는 해당 리프의 부모 노드에 할당된 상기 파라미터($v_{x,y}$) 및 상기 노드 파라미터($y_{x,y}$)에 의거하여, 키를 산출하는 키산출기능을 실현시키기 위한 프로그램.

청구항 21

컴퓨터에, n개의 수신장치 속에서 배제하는 수신장치를 특정하고, 배제되어 있지 않은 수신장치의 집합(S)을 결정하는, 배제 수신장치 특정 기능을 실현시키기 위한 프로그램.

청구항 22

컴퓨터에, n개의 수신장치가 리프에 할당되며 높이가 ($\log_Y n$)으로 표시되는 Y분 나무를 계층적으로 구성하고, 상기 리프와 루트와의 사이에 존재하는 중간 노드의 하위에 존재하는 복수의 상기 리프로 이루어지는 서브그룹

을 구성하고, 상기 리프 및 상기 중간 노드 각각에 대하여, 리프키(g_y)를 할당하고, 상기 중간 노드 및 상기 루트에, 서로 다른 파라미터 $v_{x,y}$(x : 계층, y : 1, 2, …, Y^x)와 노드 파라미터 $y_{x,y}$(x : 계층, y : 1, 2, …, Y^x)를 각각 할당하고, 상기 루트로부터 상기 리프에 이르는 패스를 특정하여, 해당 패스 상에 존재하는 상기 중간 노드 또는 상기 리프에 할당된 상기 리프키(g_y)와, 해당 중간 노드 또는 해당 리프의 부모 노드에 할당된 상기 파라미터($v_{x,y}$) 및 상기 노드 파라미터($y_{x,y}$)에 의거하여 산출된 암호키를 수신하는 수신기능을 실현시키기 위한 프로그램.

명 세 서

기 술 분 야

<1> 본 발명은, 키생성장치, 암호화장치, 수신장치, 키생성방법, 암호화방법, 키처리방법 및 프로그램에 관한 것이다.

배 경 기 술

<2> 최근, 퍼스널 컴퓨터(PC) 뿐만 아니라, 휴대 전화나 디지털 가전 등의 보급, 발달에 따라, 음악이나 영상 등의 콘텐츠 전달 비즈니스가 더욱더 중요하게 되어 오고 있다. 콘텐츠 전달 비즈니스로서는, 예를 들면, 케이블 텔레비전이나 위성방송, 또는 인터넷을 이용한 유료 방송이나, CD, DVD 등의 물리 미디어를 이용한 콘텐츠의 판매 등이 있지만, 어느 경우에 있어서도, 계약자만이 콘텐츠를 취득가능해지는 구조를 구성할 필요가 있다.

<3> 통상, 이러한 콘텐츠전달 시스템에서는, 시스템의 관리자(이하, 센터라고 표기한다.)가 미리 계약자에게만 키를 제공해 두고, 콘텐츠의 전달시에는, 콘텐츠(M)를 세션 키(s)로 암호화한 암호문(C)과, 계약자만이 세션 키(s)를 취득 가능하게 하기 위한 헤더(h)를 전달함으로써, 계약자만이 콘텐츠(M)를 취득 가능하게 된다.

<4> 상기와 같은 상황을 실현하는 콘텐츠 전달 방식으로서, 예를 들면 공개키를 이용한 방식이 있다(예를 들면, 비특허문헌 1 참조.).

<5> [비 특허문헌 1] D.Boneh, C.Gentry, B.Waters, “Collusion Resistant Broadcast Encryption With Short Ciphertexts and Private Keys”, CRYPTO '05, Proceedings of 25th Annual International Cryptology Conference on Advances in Cryptology, London, UK, Springer Verlag, 2005, pp.58~75.

발명의 상세한 설명

<6> 그렇지만, 상기의 비 특허문헌 1에 기재된 공개키 암호방식에서는, 전달이 배제되는 계약자 수가 적은 경우라도, 항상 일정 사이즈의 헤더(h)를 전달할 필요가 있기 때문에, 배제되는 계약자 수가 제로인 경우, 혹은, 계약자 전체에 차지하는 비율이 적은 경우라고 한 현실적으로 일어날 수 있는 상황에 있어서, 헤더 사이즈를 삭감하지 못하고, 암호화된 콘텐츠의 전달시에 있어서의 데이터의 장황성이 높아진다고 하는 문제가 있었다.

<7> 그래서, 본 발명은, 이러한 문제를 감안하여 이루어진 것이며, 그 목적은, 배제되는 계약자 수가 적은 경우라도 헤더 사이즈를 삭감하는 것이 가능한, 신규 또한 개량된 키생성장치, 암호화장치, 수신장치, 키생성방법, 암호화방법, 키처리방법 및 프로그램을 제공하는 것에 있다.

<8> 상기 과제를 해결하기 위해서, 본 발명의 제 1의 관점에 의하면, n개의 수신장치가 리프(leaf)에 할당되며, 높이가 ($\log_Y n$)로 표시되는 Y분 나무구조를 계층적으로 구성하고, 리프와 루트(root)와의 사이에 존재하는 중간 노드의 하위에 존재하는 복수의 리프로 이루어지는 서브그룹을 구성하는, 나무구조 구성부와, 리프 및 중간 노드 각각에 대하여, 리프키(g_y)를 할당하는 리프키 할당부와, 중간 노드 및 루트에, 서로 다른 파라미터 $v_{x,y}$(x:계층, y:1, 2, …, Y^x)와 노드 파라미터 $y_{x,y}$(x:계층, y:1, 2, …, Y^x)를 각각 할당하는 파라미터 할당부와, 루트로부터 리프에 이르는 패스를 특정하고, 해당 패스 상에 존재하는 중간 노드 또는 리프에 할당된 리프키(g_y)와, 해당 중간 노드 또는 해당 리프의 부모 노드에 할당된 파라미터($v_{x,y}$) 및 노드 파라미터($y_{x,y}$)에 의거하여, 키를 산출하는 키 산출부를 갖추는 키생성장치가 제공된다.

<9> 상기의 키생성장치는, 키 산출부에 의해 산출된 패스 상의 키 세트를 각에 수신장치 각각에 배포하는 배포부를,

더 갖추도록 구성해도 좋다.

<10> 상기의 키생성장치는, 소수(p)를 무작위로 선택하여, 소수(p)를 위수(位數)라고 하는 쌍선형군(G)을 결정하고, G의 생성요소인 g를 무작위로 선택하여, 비밀의 난수 α(α는 정수)를 무작위로 선택하는 난수 결정부를 더 갖추며, 상기의 리프키 할당부는, 이하의 식A를 만족하는 리프키(g_y)를 산출하도록 해도 좋다. 여기서, 이하의 식A에 있어서, y=1, 2, …, Y, Y+2, …, 2Y이다.

수학식 1

$$g_y = g^{(\alpha)^y} \quad \cdots (식\ A)$$

<11>

<12> 상기 파라미터 할당부는, 리프를 제외한 모든 노드와 루트의 각각에 대하여, 노드 파라미터 $\gamma_{x,y}$($\gamma_{x,y}$는 정수)를 무작위로 선택하고, 이하의 식B에 나타내는 파라미터($v_{x,y}$)를 산출하도록 해도 좋다.

수학식 2

$$v_{x,y} = g^{(\gamma_{x,y})} \quad \cdots (식\ B)$$

<13>

<14> 키 산출부는, 중간 노드 또는 리프에 할당된 리프키(g_y)의, 해당 중간 노드 또는 해당 리프의 부모 노드에 할당된 파라미터($\gamma_{x,y}$) 승으로 얻어지는 값을, 비밀키라고 해도 좋다. 즉, 중간 노드 또는 리프에 할당된 리프키(g_y)를 K로 약기(略記)하고, 해당 중간 노드 또는 해당 리프의 부모 노드에 할당된 파라미터($\gamma_{x,y}$)를 T로 약기하는 경우에, K^T로 얻어지는 값을, 비밀키라고 해도 좋다.

<15> 상기의 키 산출부는, 리프키(g_y) 및 파라미터($v_{x,y}$)에 의거하여, 공개키를 산출하고, 상기의 배포부는, 공개키를 공개하는 공개키 공개부를 갖추도록 해도 좋다.

<16> 상기의 배포부는, 키 산출부에 있어서 산출된 비밀키를 각 수신장치에 송신하는 송신부를 더 갖추도록 해도 좋다.

<17> 상기 과제를 해결하기 위해서, 본 발명의 제 2의 관점에 의하면, n개의 수신장치 속에서 배제하는 수신장치를 특정하고, 배제되어 있지 않은 수신장치의 집합(S)을 결정하는, 배제 수신장치 특정부를 갖추는 암호화장치가 제공된다.

<18> 상기의 암호화장치는, 정수(t)를 무작위로 선택하고, 세션 키 $s=e(g_Y,g_1)^t$를 결정하는 세션 키 결정부를 더 갖추어도 좋다.

<19> 여기서, 상기의 $e(g_Y,g_1)$는, 쌍선형군 상의 2개의 요소(g_Y,g_1)에 대한 쌍선형 사상을 나타낸다.

<20> 상기의 암호화장치는, 상기 세션 키(s)를 이용하여, 전달하는 콘텐츠를 암호화하는 암호화부를, 더 갖추도록 해도 좋다.

<21> 상기 세션 키 결정부는, 계층화된 나무구조에 있어서, 배제된 수신장치의 리프로부터 루트에 이르는 패스 상에 존재하는 모든 노드 각각에 마크를 첨부하고, 마크된 노드에 할당된 파라미터($v_{x,y}$)와, 마크된 노드를 부모 노드로 하는 중간 노드에 할당된 리프키(g_y)에 의거하여, 이하의 식C에 의해 헤더 요소를 산출하는 헤더 요소 산출부를, 더 갖추도록 해도 좋다. 여기서, $S_{x,y}$는, 마크된 노드를 부모 노드로 하는 각 서브그룹에 소속하는, 마크되어 있지 않은 자식 노드의 집합을 나타낸다.

수학식 3

$$c_{x,y} = (v_{x,y} \cdot \prod_{j \in S_{x,y}} g_{Y+1-j})^t \quad \cdots (식 C)$$

<22>

<23> 상기 헤더 요소 산출부에 있어서 얻어진 $c_{x,y}$와, g^t를 헤더 정보로 하는, 헤더 정보 생성부를 더 갖추도록 해도 좋다.

<24> 상기 과제를 해결하기 위해서, 본 발명의 제 3의 관점에 의하면, 키생성장치 및 암호화장치와 통신 가능한 수신장치이며, 키생성장치에 있어서, n개의 수신장치가 리프에 할당되며, 높이가 ($\log_Y n$)로 표시되는 Y분 나무구조를 계층적으로 구성하고, 리프와 루트와의 사이에 존재하는 중간 노드의 하위에 존재하는 복수의 리프로 이루어지는 서브그룹을 구성하고, 리프 및 중간 노드 각각에 대하여, 리프키(g_y)를 할당하여, 중간 노드 및 루트에, 서로 다른 파라미터 $v_{x,y}$(x:계층, y:1, 2, … ,Y^x)와 노드 파라미터 $\gamma_{x,y}$(x:계층, y:1, 2, …, Y^x)를 각각 할당하고, 루트부터 리프에 이르는 패스를 특정하여, 해당 패스 상에 존재하는 중간 노드 또는 리프에 할당된 리프키(g_y)와, 해당 중간 노드 또는 해당 리프의 부모 노드에 할당된 파라미터($v_{x,y}$) 및 노드 파라미터($\gamma_{x,y}$)에 의거하여 산출된 키를 수신하는 수신부를 갖추는 수신장치가 제공된다.

<25> 상기의 수신장치는, 암호화 콘텐츠를, 세션 키(s)에 의해 복호하는 복호부를 더 갖추도록 구성해도 좋다.

<26> 상기의 수신부는, 배제하는 수신장치가 특정된 정보인, 배제되어 있지 않은 수신장치의 집합(S)에 관한 정보를 더욱 수신하고, 상기 수신장치는, 수신장치가 집합(S)에 포함되어 있는지 아닌지를 판정하는 판정부를 더 갖추도록 구성해도 좋다.

<27> 상기 판정부에 있어서, 수신장치가 집합(S)에 포함되어 있다고 판정된 경우, 상기 복호부는, 세션 키(s)를, 이하의 식D에 의거하여 산출하고, 산출된 해당 세션 키(s)를 이용하는 것으로, 암호화 콘텐츠를 복호화해도 좋다.

수학식 4

$$s = \frac{e(g_{i_{x'}}, c_{x,y})}{e(g_{i_{x'}}^{\gamma_{i_{x'}-1}} \cdot \prod_{\substack{j \in S_{x,y} \\ j \neq i_{x'}}} g_{Y+1-j+i_{x'}}, g^t)} \quad \cdots (식 D)$$

<28>

<29> 상기 과제를 해결하기 위해서, 본 발명의 제 4의 관점에 의하면, n개의 수신장치가 리프에 할당되며, 높이가 ($\log_Y n$)로 표시되는 Y분 나무구조를 계층적으로 구성하고, 리프와 루트와의 사이에 존재하는 중간 노드의 하위에 존재하는 복수의 리프로 이루어지는 서브그룹을 구성하는 나무구조 구성스텝과, 리프 및 중간 노드 각각 대하여, 리프키(g_y)를 할당하는 리프키 할당 스텝과, 중간 노드 및 루트에, 서로 다른 파라미터 $v_{x,y}$(x:계층, y:1, 2, …, Y^x)와 노드 파라미터 $\gamma_{x,y}$(x:계층, y:1, 2, …, Y^x)를 각각 할당하는 파라미터 할당 스텝과, 루트부터 리프에 이르는 패스를 특정하고, 해당 패스 상에 존재하는 중간 노드 또는 리프에 할당된 리프키(g_y)와, 해당 중간 노드 또는 해당 리프의 부모 노드에 할당된 파라미터($v_{x,y}$) 및 노드 파라미터($\gamma_{x,y}$)에 의거하여, 키를 산출하는 키 산출 스텝을 갖추는 키생성방법이 제공된다.

<30> 상기 과제를 해결하기 위해서, 본 발명의 제 5의 관점에 의하면, n개의 수신장치 속에서 배제하는 수신장치를 특정하여, 배제되어 있지 않은 수신장치의 집합(S)을 결정하는 배제 수신장치 특정 스텝을 갖추는 암호화방법이 제공된다.

<31> 상기 과제를 해결하기 위해서, 본 발명의 제 6의 관점에 의하면, n개의 수신장치가 리프에 할당되며, 높이가 ($\log_Y n$)로 표시되는 Y분 나무구조를 계층적으로 구성하고, 리프와 루트와의 사이에 존재하는 중간 노드의 하위에 존재하는 복수의 리프로 이루어지는 서브그룹을 구성하고, 리프 및 중간 노드 각각에 대하여, 리프키(g_y)를 할당

하고, 중간 노드 및 루트에, 서로 다른 파라미터 $v_{x,y}$(x:계층, y:1, 2, …, Y^x)와 노드 파라미터 $y_{x,y}$(x:계층, y:1, 2, …, Y^x)를 각각 할당하고, 루트부터 리프에 이르는 패스를 특정하여, 해당 패스 상에 존재하는 중간 노드 또는 리프에 할당된 리프키(g_y)와, 해당 중간 노드 또는 해당 리프의 부모 노드에 할당된 파라미터($v_{x,y}$) 및 노드 파라미터($y_{x,y}$)에 의거하여 산출된 키를 수신하는 스텝을 갖추는 키처리방법이 제공된다.

<32> 상기 과제를 해결하기 위해서, 본 발명의 제 7의 관점에 의하면, 컴퓨터에, n개의 수신장치가 리프에 할당되며, 높이가 ($\log_Y n$)로 표시되는 Y분 나무구조를 계층적으로 구성하고, 리프와 루트와의 사이에 존재하는 중간 노드의 하위에 존재하는 복수의 리프로 이루어지는 서브그룹을 구성하는 나무구조 구성기능과, 리프 및 중간 노드 각각에 대하여, 리프키(g_y)를 할당하는 리프키 할당기능과, 중간 노드 및 루트에, 서로 다른 파라미터 $v_{x,y}$(x:계층, y:1, 2, …, Y^x)와 노드 파라미터 $y_{x,y}$(x:계층, y:1, 2, …, Y^x)를 각각 할당하는 파라미터 할당기능과, 루트부터 리프에 이르는 패스를 특정하여, 해당 패스 상에 존재하는 중간 노드 또는 리프에 할당된 리프키(g_y)와, 해당 중간 노드 또는 해당 리프의 부모 노드에 할당된 파라미터($v_{x,y}$) 및 노드 파라미터($y_{x,y}$)에 의거하여, 키를 산출하는 키 산출기능을 실현시키기 위한 프로그램이 제공된다.

<33> 이러한 구성에 의하면, 컴퓨터 프로그램은, 컴퓨터가 갖추는 기억부에 격납되며, 컴퓨터가 갖추는 CPU에 읽혀 실행됨으로써, 그 컴퓨터를 상기의 키생성장치로서 기능시킨다. 또, 컴퓨터 프로그램이 기록된, 컴퓨터에서 읽기 가능한 기록 매체도 제공할 수 있다. 기록 매체는, 예를 들면, 자기 디스크, 광디스크, 광학 자기 디스크, 플래시메모리 등이다. 또, 상기의 컴퓨터 프로그램은, 기록 매체를 이용하지 않고, 예를 들면 네트워크를 통하여 전달해도 좋다.

<34> 상기 과제를 해결하기 위해서, 본 발명의 제 8의 관점에 의하면, 컴퓨터에, n개의 수신장치 속에서 배제하는 수신장치를 특정하고, 배제되어 있지 않은 수신장치의 집합(S)을 결정하는, 배제 수신장치 특정 기능을 실현시키기 위한 프로그램이 제공된다.

<35> 이러한 구성에 의하면, 컴퓨터 프로그램은, 컴퓨터가 갖추는 기억부에 격납되며, 컴퓨터가 갖추는 CPU에 읽혀 실행됨으로써, 그 컴퓨터를 상기의 암호화장치로서 기능시킨다. 또, 컴퓨터 프로그램이 기록된, 컴퓨터에서 읽기 가능한 기록 매체도 제공할 수 있다. 기록 매체는, 예를 들면, 자기 디스크, 광디스크, 광학 자기 디스크, 플래시메모리 등이다. 또, 상기의 컴퓨터 프로그램은, 기록 매체를 이용하지 않고, 예를 들면 네트워크를 통하여 전달해도 좋다.

<36> 상기 과제를 해결하기 위해서, 본 발명의 제 9의 관점에 의하면, 컴퓨터에, n개의 수신장치가 리프에 할당되며, 높이가 ($\log_Y n$)로 표시되는 Y분 나무구조를 계층적으로 구성하고, 리프와 루트와의 사이에 존재하는 중간 노드의 하위에 존재하는 복수의 리프로 이루어지는 서브그룹을 구성하고, 리프 및 중간 노드 각각에 대하여, 리프키(g_y)를 할당하고, 중간 노드 및 루트에, 서로 다른 파라미터 $v_{x,y}$(x:계층, y:1, 2, …, Y^x)와 노드 파라미터 $y_{x,y}$(x:계층, y:1, 2, …, Y^x)를 각각 할당하고, 루트부터 리프에 이르는 패스를 특정하여, 해당 패스 상에 존재하는 중간 노드 또는 리프에 할당된 리프키(g_y)와, 해당 중간 노드 또는 해당 리프의 부모 노드에 할당된 파라미터($v_{x,y}$) 및 노드 파라미터($y_{x,y}$)에 의거하여, 키를 산출하는 키 산출기능을 실현시키기 위한 프로그램이 제공된다.

<37> 이러한 구성에 의하면, 컴퓨터 프로그램은, 컴퓨터가 갖추는 기억부에 격납되며, 컴퓨터가 갖추는 CPU에 읽혀 실행됨으로써, 그 컴퓨터를 상기의 수신장치로서 기능시킨다. 또, 컴퓨터 프로그램이 기록된 컴퓨터에서 읽기 가능한 기록 매체도 제공할 수 있다. 기록 매체는, 예를 들면, 자기 디스크, 광디스크, 광학 자기 디스크, 플래시메모리 등이다. 또, 상기의 컴퓨터 프로그램은, 기록 매체를 이용하지 않고, 예를 들면 네트워크를 통하여 전달해도 좋다.

실 시 예

<64> 이하에 첨부도면을 참조하면서, 본 발명의 매우 적합한 실시의 형태에 대하여 상세하게 설명한다. 또한, 본 명세서 및 도면에 있어서, 실질적으로 동일한 기능 구성을 가지는 구성요소에 대해서는, 동일한 부호를 첨부함

으로써 중복 설명을 생략한다.

<65> (제 1의 실시형태)

<66> 이하에, 본 발명의 제 1의 실시형태와 관련되는 암호키 전달시스템에 대하여, 상세하게 설명한다.

<67> 도 1은, 본 실시형태와 관련되는 암호키 전달시스템(10)을 나타낸 설명도이다. 암호키 전달시스템(10)은, 예를 들면, 통신망(12)과, 키생성장치(20)와, 암호화장치(30)와, 수신장치(40A)와, 수신장치(40B)를 포함한다.

<68> 통신망(12)은, 키생성장치(20), 암호화장치(30) 및 수신장치(40)를 쌍방향 통신 또는 한 방향 통신 가능하게 접속하는 통신회선망이다. 이 통신망은, 예를 들면, 인터넷, 전화회선망, 위성통신망, 동보(洞報) 통신로 등의 공중회선망이나, WAN(Wide Area Network), LAN(Local Area Network), IP-VPN(Internet Protocol-Virtual Private Network), 무선 LAN 등의 전용회선망 등으로 구성되어 있으며, 유선/무선을 불문한다.

<69> 키생성장치(20)는, 공개키와, 복수의 수신장치 각각에 고유의 비밀키를 생성하여, 공개키를 공개하는 동시에, 각 수신장치에 대해서, 안전한 통신로를 통하여, 각각의 비밀키를 전달한다. 또한, 이 키생성장치(20)는, 공개키 및 비밀키의 생성·관리를 행하는 센터가 소유한다.

<70> 암호화장치(30)는, 키생성장치(20)에 의해서 생성 및 공개된 공개키를 이용하여, 임의의 콘텐츠를 암호화하고, 통신망(12)을 통하여, 각 수신장치에 전달한다. 이 암호화장치(30)는, 임의의 제 3자가 소유하는 것이 가능하며, 또, 키생성장치(20)의 소유자나, 수신장치(40)의 소유자가 소유하는 것도 가능하다.

<71> 수신장치(40)는, 암호화장치(30)로부터 전달된 암호화된 콘텐츠를, 고유의 비밀키에 의해서 복호화하여 이용하는 것이 가능하다. 또한, 수신장치(40A)와 수신장치(40B)란, 통신망(12) 또는 유선을 통하여 서로 접속 가능하다. 또한, 이 수신장치(40)는, 각 계약자에 의해서 소유되는 것이다.

<72> 또한, 도시의 예에서는, 수신장치(40)로서 퍼스널 컴퓨터(Personal Computer:PC) 등의 컴퓨터 장치(노트형, 데스크 탑 형을 불문한다.)를 나타내고 있지만, 이러한 예로 한정되지 않고, 네트워크를 통한 통신 기능을 가지는 기기이면, 예를 들면 PDA(Personal Digital Assistant), 가정용 게임기, DVD/HDD 레코더, 텔레비젼 수상기 등의 정보 가전, 텔레비전 방송용의 튜너나 디코더 등으로 구성할 수도 있다. 또, 수신장치(40)는, 계약자가 운반할 수 있는 휴대용 디바이스(Portabale Device), 예를 들면, 휴대형 게임기, 휴대 전화, 휴대형 영상/음성 플레이어, PDA, PHS 등이어도 좋다.

<73> 다음에, 본 실시형태와 관련되는 키생성장치(20)의 하드웨어 구성에 대하여, 도 2를 참조하면서 간단하게 설명한다.

<74> 도 2는, 키생성장치(20)의 하드웨어 구성을 나타낸 블럭도이다. 키생성장치(20)는, 예를 들면, CPU(Central Processing Unit)(201)와, ROM(Read Only Memory)(203)과, RAM(Random Access Memory)(205)과, HDD(Hard Disk Drive)(207)와, 암호 처리부(209)와, 메모리(시큐어 모듈)(211)를 갖춘다.

<75> CPU(201)는, 연산처리장치 및 제어장치로서 기능하고, 각종 프로그램에 따라서 키생성장치(20) 내의 동작 전반을 제어한다. ROM(203)은, CPU(201)가 사용하는 프로그램이나 연산 파라미터 등을 기억한다. RAM(205)은, CPU(201)의 실행에 있어서 사용하는 프로그램이나, 이 프로그램의 실행에 있어서 적당 변화하는 파라미터 등을, 1차 기억한다.

<76> HDD(207)는, 본 실시형태와 관련되는 키생성장치(20)의 기억부의 일례로서 구성된 데이터 격납용의 장치이다. 이 HDD(207)는, 하드 디스크를 구동하여, CPU(201)가 실행하는 프로그램이나 각종 데이터를 격납한다. 암호 처리부(209)는, 본 실시형태와 관련되는 키생성장치(20)가 CPU(201)의 제어 아래에서 실행하는 각종의 암호 처리를 실행한다. 메모리(시큐어 모듈)(211)는, 주로, 개인 비밀키나, 센터 비밀인 난수 등의 은닉이 필요한 정보를 안전하게 격납하지만, 이 메모리(211)의 내부에 격납된 정보는, 외부로부터 참조할 수 없다고 하는 특징이 있다. 또, 메모리(시큐어 모듈)(211)는, 예를 들면, 내 탬퍼(tamper) 성을 가지는 기억장치에 의해 구성되어 있어도 좋다. 또한, 시큐어 모듈은 메모리인 뜻의 기재를 하고 있지만, 본 발명과 관련되는 시큐어 모듈은, 메모리에 한정되는 것이 아니라, 예를 들면, 자기 디스크, 광디스크, 광학 자기 디스크라도 좋고, 또, 반도체 메모리 등의 기억 매체라도 좋다.

<77> 상기의 CPU(201), ROM(203), RAM(205), HDD(207), 암호 처리부(209) 및 메모리(211)는, CPU 버스 등으로 구성되는 버스(213)에 의해, 서로 접속되고 있다.

<78> 버스(213)는, 브리지를 통하여, PCI(Peripheral Component Interconnect/Interface) 버스 등의 입출력 인터페

이스(215)에 접속되어 있다.

<79> 입력부(217)는, 예를 들면, 마우스, 키보드, 터치 패널, 버튼, 스위치 및 레버 등의 유저가 조작하는 조작 수단과, 사용자에 의한 조작에 의거하여 입력 신호를 생성하고, CPU(201)에 출력하는 입력 제어 회로 등으로 구성되어 있다. 키생성장치(20)의 사용자는, 이 입력부(217)를 조작함으로써, 키생성장치(20)에 대하여 각종의 데이터를 입력하거나 처리 동작을 지시하거나 할 수 있다.

<80> 출력부(219)는, 예를 들면, CRT(Cathode Ray Tube) 디스플레이 장치, 액정 디스플레이(LCD) 장치 및 램프 등의 표시장치와, 스피커 및 헤드폰 등의 음성 출력장치 등으로 구성된다. 출력부(219)는, 예를 들면, 재생된 콘텐츠를 출력하는 것이 가능하다. 구체적으로는, 표시장치는, 재생된 영상 데이터 등의 각종 정보를, 텍스트 또는 이미지로 표시한다. 또한, 음성 출력장치는, 재생된 음악 데이터 등을 음성으로 변환하여 출력한다.

<81> 통신부(221)는, 예를 들면, 통신망(12)에 접속하기 위한 통신 디바이스 등으로 구성된 통신 인터페이스이다. 이 통신부(221)는, 예를 들면 암호화장치(30)나 수신장치(40A, 40B)와의 사이에서, 통신망(12)을 통하여, 암호키에 관한 정보나, 콘텐츠 정보 등이라고 한 각종 데이터를 송수신한다.

<82> 드라이브(223)는, 기억 매체용 리더 라이터이며, 키생성장치(20)에 내장, 혹은 외부 부착된다. 드라이브(223)는, 장착되어 있는 자기 디스크, 광디스크, 광학 자기 디스크, 또는 반도체 메모리 등의 리무버블 기록매체(14)에 기록되어 있는 정보를 읽어내고, RAM(205)에 출력한다.

<83> 또한, 암호화장치(30) 및 수신장치(40)의 하드웨어 구성은, 키생성장치(20)의 하드웨어 구성과 실질적으로 동일하므로 설명을 생략한다.

<84> 이상, 본 실시형태와 관련되는 키생성장치(20), 암호화장치(30) 및 수신장치(40)의 기능을 실현 가능한 하드웨어 구성의 일례를 나타냈다. 상기의 각 구성요소는, 범용적인 부재를 이용하여 구성되어 있어도 좋고, 각 구성요소의 기능에 특화한 하드웨어에 의해 구성되어 있어도 좋다. 따라서, 본 실시형태를 실시하는 그때그때의 기술 레벨에 따라서, 적당, 이용하는 하드웨어 구성을 변경하는 것이 가능하다. 또, 상기의 하드웨어 구성은, 어디까지나 일례이며, 이것에 한정되는 것이 없음은 말할 필요도 없다. 예를 들면, HDD(207)와 메모리(시큐어 모듈)(211)를 동일한 기억장치에 의해 구성해도 좋다. 또, 이용 형태에 따라서는, 버스(213), 또는 입출력 인터페이스(215) 등을 생략하는 구성도 가능하다. 이하, 상기와 같은 하드웨어 구성에 의해 실현되는 암호키 생성 방식에 대하여 상술한다.

<85> <기반기술에 관한 설명>

<86> 우선, 본 발명과 관련되는 매우 적합한 실시형태에 대하여 상세한 설명을 하는데 앞서, 본 실시형태를 실현하는데 있어서 기반을 이루는 기술적 사항에 대하여 기술한다. 또한, 본 실시형태는, 이하에 기재하는 기반기술의 상에 개량을 가함으로써, 보다 현저한 효과를 얻을 수 있도록 구성된 것이다. 따라서, 그 개량과 관련되는 기술이 본 실시형태의 특징을 이루는 부분이다. 즉, 본 실시형태는, 여기서 말하는 기술적 사항의 기초 개념을 답습(踏襲)하지만, 그 본질은 오히려 개량 부분에 집약되어 있고, 그 구성이 명확하게 상위함과 동시에, 그 효과에 있어서 기반기술과는 선을 긋는 것임에 주의받고 싶다.

<87> 종래의 공개키를 이용한 콘텐츠 전달 방식으로는, 센터가 콘텐츠전달시스템의 시스템 파라미터(k)를 결정하고, 이 시스템 파라미터(k)에 의거하는 k차 센터 비밀 다항식을 구성한다. 그 후, 이 k차 비밀 다항식을 이용하여, 공개키(PK)와, 계약자(i)에게 고유의 비밀키(d_i)(이하, 개인 비밀키라고 표기한다.)를 생성하고, 공개키(PK)를 공개하는 동시에, 안전한 통신로를 이용하고, 계약자(i)에게 개인 비밀키(d_i)를 배포하고 있었다. 또, 콘텐츠 전달시에는, 암호문(C)과, 헤더(h)를 전달하지만, 헤더(h)는 공개키(PK)를 이용하여 생성되기 때문에, 임의의 전달자가 헤더(h)를 생성 가능하게 된다. 이 종래의 공개키를 이용한 콘텐츠 전달 방식으로는, 계약자(i)는 개인 비밀키(d_i) 하나만을 보관 유지하면 좋고, 또, 공개키(PK)를 공개함으로써, 센터 이외의 전달자가 콘텐츠를 전달하는 것이 가능해진다.

<88> 그렇지만, 개인 비밀키를 생성하기 위해서 시큐리티 파라미터인 k에 의거한 k차 다항식을 이용하고 있고, k+1명 이상의 계약자가 결탁하면, 시스템의 안전성이 보관 유지되지 않게 된다고 하는 결탁 문제가 존재하고 있었다.

<89> 그래서, 상기의 비 특허문헌 1에서는, 임의수의 계약자가 결탁해도 시스템의 안전성이 보관 유지된다고 하는 공개키 콘텐츠 전달법을 제안하고 있다.

<90> Boneh, Gentry, Waters 등에 의한 비 특허문헌 1에 기재한 방식은, 개인 비밀키의 생성에 k차 다항식을 이용하지 않고, 쌍선형군으로 불리는 순회 곱셈법 군의 일종을 이용하고, 이 군에 있어서의 계약자(i)에 고유의 요소를, 개인 비밀키(di)로서 제공한다. 또, 헤더(h)의 생성 및 각 계약자에 의한 세션 키(s)의 취득에, 쌍선형사상으로 불리는 연산을 이용함으로써, 종래의 공개키를 이용한 콘텐츠전달시스템에 있어서 큰 문제가 되고 있던 결탁 문제를 해결하고 있다.

<91> 비 특허 문헌 1에서는, 우선 기본 방식으로서, 계약자 집합을 하나의 그룹으로서 취급하는 방식을 나타내고 있다. 이하에서는, 도 3을 참조하면서, 이 기본 방식에 대하여 설명한다. 이 기본 방식에서는, 센터(51)가 쌍선형군의 생성요소(g)와, 센터 비밀인 α를 생성하고, 이들을 이용하여 계약자 i(i=1, …, n)에게, 파라미터

수학식 5

<92> $$g_i = g^{\alpha^i}$$

<93> 를 할당한다.

<94> 또, 계약자(55)의 집합을 하나의 그룹으로서 취급하기 위한 파라미터($v = g^{\gamma}$)를 생성하고, 이러한 생성요소(g) 및 파라미터(v)를, 공개키 PK=(g, g_1, …, g_n, g_{n+2}, …, g_{2n}, v)로서 공개한다. 또한 계약자(i)에게는, i에 할당된 파라미터

수학식 6

<95> $$g_i = g^{\alpha^i}$$

<96> 를 이용하고, 개인 비밀키

수학식 7

<97> $$d_i = g_i^{\gamma}$$

<98> 를, 안전한 일대일 통신로(53)를 통하여, 미리 제공해 둔다.

<99> 전달자는, 공개키 PK=(g, g_1, …, g_n, g_{n+2}, …, g_{2n}, v)로부터, 배제되어 있지 않은 모든 계약자에게 할당된 파라미터

수학식 8

<100> $$g_i = g^{\alpha^i}$$

<101> 와, 계약자를 하나의 그룹으로 정리하기 위한 파라미터($v = g^{\gamma}$)로부터, 배제되어 있지 않은 모든 계약자에게 대응하는 공통의 헤더 요소를 하나 작성하여, 이 헤더 요소와 세션 키 생성시에 이용되는 난수 요소를 포함한 헤더 요소를 이용하여, 헤더(h)를 생성하고, 암호문(C)과 함께 전달한다.

<102> 이와 같이, 기본 방식으로는, 계약자 집합을 하나의 그룹으로서 취급하고, 그 그룹에 대응하는 헤더 요소를 구성함으로써, 헤더(h)의 크기(이하, 헤더 사이즈라고 표기한다.)를 최소로 하고 있다.

<103> 그렇지만, 모든 계약자를 하나의 그룹으로서 취급하기 위해, 각 계약자에게 각각 다른 파라미터(g_1, …, g_n)를 할당할 필요가 있기 때문에, 공개키 사이즈가, 계약자수의 2배 이상의 크기가 된다. 또, 각 계약자가 헤더(h)로부터 세션 키(s)를 취득할 때에는, 자신을 제외하여 배제되어 있지 않은 전 계약자에게 대응하는 파라미터(g_1,

…, g_n)의 곱을 계산할 필요가 있기 때문에, 계약자의 총수인 n의 값이 매우 큰 값이 되는 경우에는, 계약자에 대한 계산량의 부담이 매우 커진다. 현실적인 콘텐츠 전달에 있어서는, 유료 방송이나 DVD 등의 물리 미디어, 인터넷 등을 통하여, 매우 많은 계약자에 대해서 콘텐츠를 전달할 필요가 있기 때문에, 이상과 같은 문제점을 고려하면, 기본 방식은 현실적으로 이용 불가능하다라고 말할 수 있다.

<104> 상기의 문제점을 해소하는 방법으로서, 비 특허문헌 1에서는, 계약자 집합을 복수의 서브그룹에 분할함으로써 공개키 사이즈를 억제하는 것이 가능해지는 일반화 방식을 제안하고 있다. 일반화 방식으로는, 계약자 집합을 복수의 서브그룹으로 분할하고, 분할된 각 서브그룹에 대해서, 기본 방식 같은 동작을 행하고 있다. 따라서, 서브그룹마다 다른 헤더 요소를 생성할 필요가 있으며, 헤더 사이즈는 증대하지만, 공개키 사이즈를 억제하는 것이 가능해지고 있다. 또, 각 계약자는, 분할된 서브그룹에 소속하는 각 계약자에게 할당된 파라미터의 곱을 계산할 필요가 있지만, 기본 방식과 비교하여, 계약자 집합이 서브그룹으로 분할되고 있기 때문에, 계산할 필요가 있는 파라미터 수를 억제하는 것이 가능해지며, 기본 방식에 있어서의 문제점을 해소하고 있다.

<105> 이하에서는, 비 특허문헌 1에 기재한 일반화 방식에 대하여, 도 4~도 8을 참조하면서, 상세하게 설명한다. 처음에, 상기의 일반화 방식을 설명하는데 있어서 필요한 기호의 정의를 나타내고, 비 특허문헌 1에 있어서 이용되는 쌍선형군 및 쌍선형 사상에 대해 설명한다. 계속하여, 이러한 정의를 이용하여, 비 특허문헌 1에 기재한 일반화 방식의 상세나 문제점 등에 대해 설명한다.

<106> <기호의 정의>

<107> 비 특허문헌 1에 기재한 일반화 방식을 설명하는데 있어서 사용하는 각 기호를, 이하와 같이 정의한다.

<108> n :계약자의 총수

<109> A :계약자 그룹을 복수의 서브그룹으로 분할할 때의 분할수

<110> B :분할된 서브그룹에 소속하는 계약자수

<111> PK :시스템의 공개키

<112> d_i :i번째의 계약자의 개인 비밀키

<113> r :배제되는 계약자의 총수

<114> p :쌍선형군의 위수가 되는 큰 소수

<115> G, G_1 :위수(p)의 쌍선형군

<116> g :G의 생성요소

<117> M :암호화되어 있지 않은 콘텐츠(평문)

<118> s :세션 키

<119> C :평문(M)을 세션 키(s)로 암호화했을 때의 암호문

<120> $E_s(M)$:평문(M)의 키(s)에 의한 암호화

<121> $D_s(C)$:암호문(C)의 키(s)에 의한 복호

<122> e(u, v) :쌍선형군(G) 상의 두 개의 요소(u, v)에 대한 쌍선형 사상

<123> <쌍선형군에 있어서의 쌍선형 사상>

<124> 계속하여, 비 특허문헌 1에 있어서 이용되는 쌍선형군 상의 쌍선형 사상에 관하여 설명한다. 쌍선형 사상 e(u, v)란, 순회 곱셈법 군(G)의 두 개의 요소 u, v 를 순회 곱셈법 군(G_1)의 요소로 변환하는 사상이며, 이하의 성질을 만족하는 것이다.

<125> 1. 쌍선형성 : 임의의 $u, v \in G$ 및 $a,b \in Z$에 대해서, $e(u^a, v^b) = e(u, v)^{ab}$가 성립한다.

<126> 2. 비 퇴화성 : $e(g,g) \neq 1$

<127> 계속하여, 비 특허문헌 1에 기재한 일반화 방법으로 대하여, 각 스텝을 상세하게 설명한다. 이 일반화 방법은,

주로, 키생성국면, 암호화국면, 복호국면이라는 세 개의 국면으로 구성된다. 키생성국면은, 센터가 시스템 구성시에 한 번만 실행하고, 암호화국면은 전달자, 복호국면은 계약자가, 각각 전달마다 실행한다. 이하, 각 국면의 설명을 행한다.

<128> <키생성국면>

<129> 이하에서는, 도 4 및 도 5를 참조하면서, 키생성국면에 대하여 설명한다. 도 4는, 비 특허문헌 1의 일반화 방식에 있어서의 키생성국면을 설명하기 위한 설명도이다. 도 5는, 비 특허문헌 1의 일반화 방식에 있어서의 키생성국면의 흐름도이다.

<130> 센터(51)는, 이하의 순서에 따라서, 각 계약자(55)의 개인 비밀키와 공개키를 생성한다. 우선, 센터(51)는, 큰 소수(p)를 무작위로 선택하고, 선택된 p를 위수라고 하는 쌍선형군(G)을 결정한다(스텝S11).

<131> 계속하여, 센터(51)는, 상기 스텝(S11)에서 결정한 쌍선형군(G)의 생성요소인 g와, 센터 비밀인 난수 α(α는 정수이다.)를, 각각 무작위로 선택한다(스텝S13).

<132> 다음에, 센터(51)는, 분할된 서브그룹에 소속하는 계약자의 수(B)를 결정하고, 분할수(A)를 이하의 계산에 의해 결정한다. 그 후, 계약자를 A개의 서브그룹에 분할한다(스텝S15).

수학식 9

$$A = \left\lceil \frac{n}{B} \right\rceil \quad \cdots(식\ 1)$$

<133>

<134> 여기서, 위 식의 우변에 나타나고 있는 기호는, 「(n/B) 이상의 최소의 정수」를 나타내는 기호이다.

<135> 계속하여, 센터(51)는, i(i=1, …B, B+2, …, 2B)에 대하여, 리프키(g_i)를 이하와 같이 하여 산출한다(스텝S17).

수학식 10

$$g_i = g^{(\alpha)^i} \quad \cdots(식\ 2)$$

<136>

<137> 다음에, 센터(51)는, 서브그룹 수 A에 대응하는 A개의 난수γ(γ1,…,γA, γ는 정수.)를 무작위로 선택한다. 계속하여, 쌍선형군(G)에 속하는 v_1, …, v_A를, 이하와 같이 하여 산출한다(스텝S19).

수학식 11

$$v_i = g^{\gamma_i} \in G(i = 1,..., A) \quad \cdots(식\ 3)$$

<138>

<139> 계속하여, 센터(51)는, 상기의 스텝(S13)에서 선택한 g와, 스텝(S17)에서 산출한 g_i와, 스텝(S19)에서 산출한 v_i에 의거하여, 이하에서 표시되는 공개키(PK)를 결정하여, 공개한다(스텝S21).

<140> $PK=(g, g_1, \cdots, g_B, g_{B+2}, \cdots, g_{2B}, v_1, \cdots, v_A)$ …(식 4)

<141> 계속하여, 센터(51)는, 계약자(i)가 소속하는 서브그룹 S_a(a는, i/B 이상의 최소의 정수이다.)와, 이 서브그룹에 있어서의 계약자(i)의 인덱스인 b=imodB(여기서, i는 1 이상 B 이하의 정수이다.)에 대응하는 파라미터 g_b, γ_a를 선택하고, 이하의 식에서 산출되는 계약자(i)의 개인 비밀키(d_i)를 생성한다(스텝S23).

수학식 12

$$d_i = g_b^{\gamma_a} = v_a^{\alpha^b} \in G \quad \cdots (식 5)$$

<142>

<143> 계속하여, 센터(51)는, 상기와 같이 하여 생성한 개인 비밀키(d_i)를, 안전한 일대일 통신로(53)를 통하여, 비밀리에 각각의 계약자(i)에게 전달한다(스텝S23).

<144> 상기와 같이, 비 특허문헌 1에 있어서의 키생성국면으로는, 스텝(S15)에 있어서, 센터(51)가 n인의 계약자로 이루어지는 계약자 집합을 B인씩 A개의 서브그룹으로 분할하고, 스텝(S11), 스텝(S13), 스텝(S17), 스텝(S19)에 있어서, 콘텐츠전달시스템을 운영하는데 있어서 필요한 각종 파라미터를 설정하고 있다.

<145> 또, 스텝(S21)에서는, 생성한 파라미터를 이용하여 공개키(PK)를 생성하고, 계속되는 스텝(S23)에서는, 스텝(S15)에 있어서 결정한 서브그룹의 분할수 A와, 하나의 서브그룹에 소속하는 계약자수인 B에 의거하고, 각 계약자의 개인 비밀키를 생성하고 있다.

<146> 이때, 각 계약자는, 자신에게 주어진 계약자 고유의 번호에 의해, 자신이 소속하는 서브그룹과, 그 서브그룹에 있어서의 인덱스가 결정된다. 상기에서 설명한 바와 같이, 개인 비밀키의 생성에 k차 다항식을 이용하고 있지 않기 때문에, 임의수의 계약자가 결탁했다고 해도, 타계약자의 개인 비밀키 위조나, 배제된 계약자가 헤더로부터 세션 키를 취득 가능해지는 부정키를 구성할 수 없게 되어 있다.

<147> <암호화국면>

<148> 이하에서는, 도 6 및 도 7을 참조하면서, 암호화국면에 대하여 설명한다. 도 6은, 비 특허문헌 1의 일반화 방식에 있어서의 암호화국면을 설명하기 위한 설명도이다. 도 7은, 비 특허문헌 1의 일반화 방식에 있어서의 암호화국면의 흐름도이다.

<149> 전달자(57)는, 이하의 순서에 따라서 전달하는 콘텐츠를 암호화하고, 동보 통신로(59)를 통하여, 비 계약자(61) 및 계약자(63)에게, 암호화한 콘텐츠를 정리하여 전달한다.

<150> 우선, 전달자(57)는, 정수(t)를 무작위로 선택하고, 세션 키(s)를 이하와 같이 계산한다(스텝S31).

<151> $s = e(g_{B+1}, g)^t = e(g_B, g_1)^t$ …(식 6)

<152> 계속하여, 전달자(57)는, 콘텐츠를 복호 가능한 계약자의 집합(S)을 결정하고, l=1, …, A에 대해서, 이하와 같이 각 서브그룹을 결정한다(스텝S33).

수학식 13

$$\hat{S}_l = S \cap \{(l-1)B+1,\ldots,lB\} \quad \cdots (식 7)$$

$$S_l = \{x - lB + B \mid x \in \hat{S}_l\} \subseteq \{1,\ldots,B\} \quad \cdots (식 8)$$

<153>

<154> 여기서, 첨자 l은 서브그룹을 나타내는 파라미터이며, 상기의 식 7에서 표시되는 집합은, 파라미터 l로 표시되는 서브그룹에 포함되는 계약자 및 비 계약자의 집합이며, 상기의 식 8에서 표시되는 집합은, 파라미터 l로 표시되는 서브그룹 내에 있어서, 계약자는 서브그룹 내의 몇 번째의 사람인가를 나타내는 집합이다.

<155> 계속하여, 전달자(57)는, 계약자(63)가 세션 키(s)를 산출하기 위해서 필요한 헤더(h)를 이하와 같이 구성한다(스텝S35).

수학식 14

$$h = (g^t, (v_1 \cdot \prod_{j \in S_1} g_{B+1-j})^t, \ldots, (v_A \cdot \prod_{j \in S_A} g_{B+1-j})^t) \in G^{A+1} \quad \cdots (식 9)$$

<156>

<157> 다음에, 전달자(57)는, 스텝(S31)에서 산출한 세션 키(s)에 의거하여, 식 10에 나타내는 바와 같이, 송신하는

콘텐츠를 암호화한다. 그 후, 암호화한 콘텐츠 C를, 스텝(S33)에서 결정한 집합(S)에 관한 정보 및 스텝(S35)에서 산출한 헤더(h)와 함께, 동보 통신로(59)를 통하여, 비 계약자(61), 계약자(63)를 불문하고, 송신한다(스텝 S37).

<158> $C=E_s(M)$ …(식 10)

<159> 상술한 바와 같이, 전달시에는, 전달자(57)는, 암호화국면의 스텝(S31)에 있어서 세션 키를 생성한 후, 스텝(S33)에 있어서 각 서브그룹에 소속하는 콘텐츠를 복호 가능한 계약자의 집합을 결정한다. 그 후, 스텝(S35)에 있어서, 각 서브그룹에 대응하는 요소를 포함한 헤더(h)를 작성하다. 이때, 헤더(h)의 각 요소는, 그 각 서브그룹에 있어서 복호 가능한 계약자에게 대응하는 파라미터 g_b에만 구성되어 있고, 배제된 계약자에게 대응하는 g_b는 포함되어 있지 않다. 이것에 의해, 후에 기술하는 복호 시에 있어서, 비 계약자의 배제를 실현하고 있다.

<160> <복호국면>

<161> 이하에서는, 도 8을 참조하면서, 복호국면에 대하여 설명한다. 도 8은, 비 특허문헌 1의 일반화 방식에 있어서의 복호국면의 흐름도이다.

<162> 암호화 콘텐츠 등의 전달을 받은 계약자(i)는, 이하의 순서에 따라서, 암호화 콘텐츠의 복호 처리를 행한다.

<163> 우선, 계약자(63)는, 자신의 인덱스인 i가, 전달자(57)에 의해 전달된 집합(S)에 포함되어 있는지 어떤지를 확인한다(스텝S51). 자신의 인덱스(i)가 집합(S)에 포함되어 있지 않다면, 자신은 배제된 것으로서, 복호 처리를 종료한다. 자신의 인덱스(i)가 집합(S)에 포함되어 있는 경우에는, 계속 이하의 처리를 행한다.

<164> 다음에, 계약자(63)는, 송신된 헤더(h) 중, 자신이 소속하는 서브그룹(S_a)에 대응하는 헤더 요소를 선택하고, 세션 키(s)를 산출한다(스텝S53). 즉, 헤더(h)는, $h=(C_0, C_1, \cdots, C_A)$와 같이, 각각의 서브그룹에 대응하는 헤더 요소에 의해 구성되어 있으며, 자신이 소속하는 서브그룹(S_a)에 대응하는 요소(C_0, C_a)를 선택하고, 이러한 헤더 요소에 의거하여, 이하의 계산과 같이 세션 키(s)를 취득한다.

수학식 15

$$s=\frac{e(g_b,C_a)}{e(d_i\cdot\prod_{\substack{j\in S_a\\ j\neq b}}g_{B+1-j+b},C_0)} \quad \cdots(식\ 11-1)$$

$$=\frac{e(g_b,(v_a\cdot\prod_{j\in S_a}g_{B+1-j})^t)}{e(v_a{}^{(\alpha^b)}\cdot\prod_{\substack{j\in S_a\\ j\neq b}}g_{B+1-j+b},g^t)} \quad \cdots(식\ 11-2)$$

$$=\frac{e(g_b,g_{B+1-b}{}^t)\cdot e(g_b,(v_a\cdot\prod_{\substack{j\in S_a\\ j\neq b}}g_{B+1-j})^t)}{e(v_a{}^{(\alpha^b)}\cdot\prod_{\substack{j\in S_a\\ j\neq b}}g_{B+1-j+b},g^t)} \quad \cdots(식\ 11-3)$$

$$=\frac{e(g,g_{B+1})^t\cdot e(g^t,(v_a{}^{(\alpha^b)}\cdot\prod_{\substack{j\in S_a\\ j\neq b}}g_{B+1-j+b})^t)}{e(v_a{}^{(\alpha^b)}\cdot\prod_{\substack{j\in S_a\\ j\neq b}}g_{B+1-j+b},g^t)} \quad \cdots(식\ 11-4)$$

$$=e(g,g_{B+1})^t \quad \cdots(식\ 11-5)$$

<165>

<166> 상기의 식 11-5와, 식 6에서 분명한 바와 같이, 계약자(63)는, 전달자(57)로부터 송신된 헤더(h)와 공개키(PK) 및 계약자(63) 자신이 보유하고 있는 개인 비밀키(d_i)를 이용함으로써, 전달자(57)가 암호화에 이용한 콘텐츠키(s)와 같은 것을 산출하는 것이 가능하다.

<167> 계속하여, 계약자(63)는, 상기의 스텝(S53)에서 산출한 세션 키(s)를 이용하여, 전달된 암호화 콘텐츠(C)를 평문(M)으로 복호한다(스텝S55).

<168> $M=D_s(C)$ …(식 12)

<169> 상술한 바와 같이, 복호 시에는, 계약자(63)는, 우선 스텝(S51)에 있어서, 자신이 배제되어 있는지 어떤지를 확인한다. 배제되어 있는 경우에는, 후술하는 이유에 의해서 세션 키(s)를 취득하는 것이 불가능하게 되기 때문에, 복호 처리를 종료한다. 스텝(S51)에서의 판정에 의해, 자신이 배제되어 있지 않다고 안 계약자는, 스텝(S53)에 있어서, 전달된 헤더 중 자신이 소속하는 서브그룹에 대응하는 헤더 요소를 꺼내고, 이 헤더 요소와, 자신의 개인 비밀키 및 공개키에 의거하여, 식 11-1에서 식 11-5에 나타낸 쌍선형 사상에 의한 복호연산을 행함으로써, 세션 키(s)를 취득한다. 그리고, 산출한 세션 키(s)를 이용하여, 암호문의 복호를 행한다.

<170> 여기서, 만약 배제된 계약자가 식 11-1에서 식 11-5에 나타낸 쌍선형 사상에 의한 복호연산을 실행했다고 해도, 스텝(S53) 중의 식 11-2에 있어서의

수학식 16

$$(v_a \cdot \prod_{j \in S_a} g_{B+1-j})^t \quad \cdots (식\ 13)$$

<171>

<172> 의 부분에, 자신의 g_b에 대응하는 값 g_{B+1-b}이 포함되어 있지 않기 때문에, 비 특허문헌 1에 있어서 안전성의 근거가 되는 BDHEP(Bilinear Diffie-Hellman Exponential Problem)의 곤란성에서, 식 11-3으로의 변형이 불가능으로 되며, 올바른 세션 키(s)를 계산하는 것이 불가능으로 되어 있다.

<173> 이와 같이, 비 특허문헌 1의 방식은 종래의 k차 다항식을 이용하는 공개키 콘텐츠 전달법에 있어서 문제가 되고 있던, 결탁의 문제를 해결하고 있다. 또, 키생성국면의 스텝(S15)에 있어서 센터가 계약자 집합을 A개의 서브그룹에 미리 분할해 두는 것으로, 전달자가 생성할 필요가 있는 헤더는, 항상 A+1개의 요소를 가지도록 구성 가능해진다. 따라서, 배제되는 계약자 수에 관계없이, 헤더 사이즈를 일정하게 유지하는 것이 가능해지고 있다.

<174> 상기와 같이, 비 특허문헌 1의 방식에서는, 항상 일정한 크기를 가지는 헤더를 송신할 필요가 있다. 그 때문에, 배제되는 계약자가 존재하지 않는, 또는 적은 경우에 있어서, 효율적인 콘텐츠 전달이 불가능하게 된다는 문제점이 존재한다. 실제의 콘텐츠전달시스템에서는, 계약자 수가 매우 큰 값으로 되는 것이 많기 때문에, 배제되는 계약자 수는, 계약자 수 전체에 대해서 작은 값으로 되는 것이 많다. 또, 만일 배제되는 계약자 수가 커져 버렸을 경우에는, 콘텐츠전달시스템 자체가, 붕괴해 버릴 가능성이 있다. 따라서, 콘텐츠전달시스템으로서는, 배제되는 계약자가 존재하지 않는지, 전체에 대해서 소수에 머무르고 있는 경우에 있어서는, 효율 좋게 콘텐츠를 전달하는 것이 요구된다.

<175> 그렇지만, 상술한 바와 같이, 비 특허문헌 1에서는, 이 조건을 만족하는 것이 곤란하게 된다. 또한 비 특허문헌 1에서는, 복호화 국면의 스텝(S53)의 식 11-1에 있어서, 쌍선형 사상에 의한 연산을 행하기 위해서, 이하의 식 14에서 표시되는, 자신이 소속하는 서브그룹 내에 존재하는 배제되어 있지 않은 계약자에게 할당된 파라미터와, 자신이 보관 유지하는 개인 비밀키와의 곱을, 미리 계산해 둘 필요가 있다.

수학식 17

$$d_i \cdot \prod_{\substack{j \in S_a \\ j \neq b}} g_{B+1-j+b} \quad \cdots (식\ 14)$$

<176>

<177> 여기서, 쌍선형 사상에 의한 연산을 PAIR, 쌍선형군(G_1) 상에서의 역원연산을 INV, 쌍선형군(G) 상에서의 곱셈을 MUL로 하고, 계약자(i)가 소속하는 서브그룹(S_a)에 있어서 배제된 계약자의 수를 r_a로 두면, 복호화 국면에 있어서 계약자가 실행할 필요가 있는 연산의 계산량은, 「$2PAIR+INV+(B-1-r_a)MUL$」로 나타낼 수 있다.

<178> 이것보다, 분할된 서브그룹에 소속하는 계약자수(B)의 값이 큰 경우나, 자신이 소속하는 서브그룹에 대해 배제되는 계약자의 수(r_a)가 작은 경우에는, 각 계약자가 복호 시에 필요로 하는 계산량이 증대한다고 하는 문제점도

존재하는 것을 알 수 있다.

<179> 이와 같이, 비 특허문헌 1에 있어서의 일반화 방식을 이용했다고 해도, 계약자 집합의 분할수를 크게 하면, 각 계약자에 있어서의 콘텐츠 복호 시의 계산량은 억제하는 것이 가능해지지만, 헤더 사이즈가 증대한다. 또, 반대로 계약자 집합의 분할수를 작게 하면, 헤더 사이즈는 억제되지만, 계산량이 증대한다고 하는 문제점이 존재한다. 또, 배제되는 계약자 수가 적은 경우라도, 항상 일정 사이즈의 헤더(h)를 전달할 필요가 있기 때문에, 배제되는 계약자 수가 없거나, 혹은 전체에 대하여 차지하는 비율이 적다라고 하는 현실적으로 가장 일어날 수 있을 것 같은 상황에 있어서, 헤더 사이즈를 삭감하지 못하고, 콘텐츠 전달시에 있어서의 데이터의 장황성이 높아진다고 하는 문제점이 존재한다.

<180> 그래서, 본원 발명자들은, 상기의 문제점을 해결하기 위하여 열심히 연구를 행하여, 이하에 설명하는 바와 같은, 본 발명의 일 실시형태와 관련되는 암호키 전달시스템을 개발했다. 본 실시형태와 관련되는 키생성장치에서는, 비 특허문헌 1의 방식으로 약간의 파라미터를 더해 논리목을 구성함으로써, 배제되는 계약자 수가 적은 경우에 있어서도, 비 특허문헌 1에 기재한 방식보다 헤더 사이즈를 삭감하는 것이 가능해진다. 또, 이러한 구성을 취함으로써, 계약자가 복호 시에 실행할 필요가 있는 연산의 계산량을, 동등 이하로 삭감하는 것이 가능해지며, 효율적인 콘텐츠 전달을 실현할 수 있다.

<181> <실시형태와 관련되는 설명>

<182> 지금까지 설명한 바와 같은 기반기술을 밟으면서, 이하에 있어서, 본 실시형태와 관련되는 키생성장치, 암호화장치 및 수신장치에 대하여, 상세하게 설명한다. 본 실시형태와 관련되는 키생성장치(20)는, 비 특허문헌 1의 방식을 이용한 논리목을 구성하고, 이 논리목을 이용함으로써, 배제되는 계약자가 존재하지 않는, 혹은 적은 경우에 있어서, 비 특허문헌 1의 방식보다 효율적인 콘텐츠 전달을 실현하는 것이다.

<183> 우선, 본 실시형태와 관련되는 키생성장치(20)의 구성에 대해서, 도 9를 참조하면서 설명한다. 도 9는, 본 실시형태와 관련되는 키생성장치(20)의 구성을 나타낸 블럭도이다.

<184> 키생성장치(20)는, 예를 들면, 나무구조 구성부(231)와, 난수 결정부(233)와, 리프키 할당부(235)와, 파라미터 할당부(237)와, 키 산출부(239)와, 기억부(241)와, 배포부(252)를 갖춘다.

<185> 나무구조 구성부(231)는, 본 실시형태와 관련되는 키생성장치의 중요한 요소인, 논리목을 구축한다. 즉, 대상이 되는 n개의 수신장치를 리프에 할당하여, 높이가 ($\log_Y n$)으로 표시되는 Y분 나무구조를 계층적으로 구축한다.

또한, 리프와 루트와의 사이에 존재하는 중간 노드를, 각각 부모 노드로 하는, Y분 나무로 이루어지는 서브그룹을 구성한다. 즉, 나무구조 구성부(231)에 의해, 1개의 노드로부터 아래를 향하고, 항상 Y개의 가지가 나오고 있는 Y분 나무구조가, 계층적으로 쌓인다. 구축된 계층화 Y분 나무구조의 전체를 보면, 최상위계층(이하, 제 0 계층이라고 칭한다.)에는 루트가 1개만 존재하고, 이 루트 아래에는, 이 루트를 부모 노드로 하는 Y개의 자식 노드가, 제 1 계층으로서 구축된다. 또, 이 제 1 계층에 존재하는 Y개의 자식 노드 각각을 부모 노드로서, 제 2 계층에는, 또한 Y^2개의 자식 노드가 존재한다. 이러한 구조가 반복되며, 맨 밑의 계층, 즉, 제 ($\log_Y n$)계층에는, 전체적으로 n개의 리프가 존재한다.

<186> 여기서, 1개의 노드로부터 하향에 1개의 가지가 성장하고 있고, 이 가지 끝에 1개의 노드가 존재하는 경우에, 상대적으로 위쪽의 노드를 부모 노드라고 부르며, 상대적으로 아래쪽의 노드를 자식 노드라고 부르는 것으로 한다. 이 부모 노드, 자식 노드라고 하는 개념은 상대적인 것이다. 예를 들면, 3개의 노드가 1개의 가지로 상하로 연결되어 있는 경우에, 최상부의 노드를 부모 노드로 한 경우에는, 중간에 위치하는 노드는 자식 노드가 된다. 또, 최하부의 노드에 착안한 경우에는, 최하부의 노드는, 중간에 위치하는 노드를 부모 노드로 하는 자식 노드가 된다.

<187> 또, 계층화된 나무구조에 있어서, 최상위 계층에 존재하는 루트와, 최하위 계층에 존재하는 n개의 리프와의 사이에 존재하는 각 노드를, 중간 노드라고 부르기로 한다.

<188> 난수 결정부(233)는, 본 실시형태와 관련되는 키생성장치가 이용하는 여러 가지 난수나, 쌍선형군을 결정한다. 즉, 난수 결정부(233)는, 소수(p)를 무작위로 선택하고, 이 소수(p)를 위수라고 하는 쌍선형군(G)을 결정하는 것 외에, G의 생성요소(g)를 무작위로 선택하거나, 비밀의 난수인 정수(α)를 무작위로 선택하거나 한다.

<189> 리프키 할당부(235)는, 나무구조 구성부(231)가 구축한, 계층화된 Y분 나무구조에 있어서, 말단의 n개의 리프와, 이 리프와 루트 이외의 모든 중간 노드에 대해서, 리프키(g_y)를 할당한다.

<190> 파라미터 할당부(237)는, 나무구조 구성부(231)가 구축한, 계층화된 Y분 나무구조에 있어서, 말단의 n개의 리프 이외의 모든 노드, 즉, 최상위 계층의 루트와, 루트와 리프와의 사이에 존재하는 모든 중간 노드에 대해서, 임의의 파라미터 $v_{x,y}$를 할당한다. 여기서, x,y는 각각 노드의 위치를 나타내는 첨자이며, x는 계층을 나타내는 것이고, y는 계층 x의 몇 번째의 노드에 적합한지를 나타내는 것이다.

<191> 키 산출부(239)는, 난수 결정부(233)가 결정된 쌍선형군(G)이나 난수, 리프키 할당부(235)가 할당한 리프키 및 파라미터 할당부(237)가 할당한 파라미터 등에 의거하여, 공개키 및 개인 비밀키를 산출한다.

<192> 기억부(241)는, 예를 들면, 나무구조 기억부(243), 난수 기억부(245), 리프키 기억부(247), 파라미터 기억부(249) 및 키 기억부(251) 등을 포함한다. 이러한 기억부에는, 각 처리부가 행한 처리 도중에 필요한 변수나 계산 결과, 또는, 처리의 결과 얻어진 것을 기억한다. 나무구조 구성부(231), 난수 결정부(233), 리프키 할당부(235), 파라미터 할당부(237) 및 키 산출부(239) 등의 각 처리부는, 이 기억부(241)에 대해서, 자유롭게 데이터를 쓰거나, 데이터를 읽어내거나 하는 것이 가능하다.

<193> 또, 이 기억부(241)에는, 상기의 기억부(243, 245, 247, 249, 251) 이외에도, 여러 가지 데이터를 기억하게 하는 것이 가능하다. 또한, 도 9에 있어서는, 기억부(241) 안에 여러 가지 기억부가 개별적으로 존재하도록 나타내고 있지만, 여러 가지 기억부를 개별적으로 존재시키지 않고, 전체적으로 1개의 기억부에 여러 가지 데이터를 기억하게 해두어도 좋다. 또, 기억부(241)로서는, 시큐어 모듈을 갖춘 기억 매체를 이용하는 것도 가능하다.

<194> 본 실시형태와 관련되는 키생성장치에 있어서의 배포부(252)는, 예를 들면, 송신부(253)와, 공개키 공개부(255)를 갖춘다. 송신부(253)는, 키 산출부(239)가 산출하여, 키 기억부(251)에 기억되고 있는 개인 비밀키를, 각 수신장치로 송신한다. 또, 공개키 공개부(255)는, 키 산출부(239)가 산출하여, 키 기억부(251)에 기억되고 있는 공개키를 각 수신장치에 공개한다.

<195> 계속하여, 본 실시형태와 관련되는 암호화장치(30)의 구성에 대해서, 도 10을 참조하면서 설명한다. 도 10은, 본 실시형태와 관련되는 암호화장치(30)의 구성을 나타낸 블럭도이다.

<196> 도 10에 나타낸 바와 같이, 암호화장치(30)는, 예를 들면, 수신부(301)와, 기억부(303)와, 배제 수신장치 특정부(305)와, 세션 키 결정부(307)와, 콘텐츠 기억부(313)와, 암호화부(315)와, 콘텐츠 송신부(317)를 갖춘다.

<197> 수신부(301)는, 키생성장치(20)에 의해 생성되며, 공개된 공개키를 수신한다. 또, 수신부(301)는, 공개키 이외에도, 키생성장치(20)에 의해 생성된 소수(p)나, 배제하는 수신장치가 특정된 정보인, 배제되어 있지 않은 수신장치의 집합(S)에 관한 정보를 더욱 수신할 수 있다.

<198> 기억부(303)는, 예를 들면, 키생성장치(20)에 의해서 생성된 공개키를 기억한다. 또, 공개키 이외에도, 소수(p)나 배제되어 있지 않은 수신장치의 집합(S)에 관한 정보 등의 정보를 기억하는 것이 가능하다.

<199> 배제 수신장치 특정부(305)는, 암호화장치(30)에 통신망(12)을 통하여 접속되어 있는 복수의 수신장치(40) 중에서, 콘텐츠의 전달을 배제하는 수신장치를 특정하고, 배제되어 있지 않은 수신장치의 집합(S)을 결정한다. 집합(S)의 결정을 할 때에는, 배제 수신장치 특정부(305)는, 기억부(303)에 기억되어 있는 여러 가지 데이터를 참조할 수 있다.

<200> 세션 키 결정부(307)는, 전달하려고 하는 콘텐츠를 암호화하기 위한 세션 키(s)를 결정한다. 이 세션 키 결정부(307)는, 예를 들면, 헤더 요소 산출부(309)와 헤더 정보 생성부(311)를 더 갖추어도 좋다.

<201> 세션 키 결정부(307)가 세션키(s)를 산출할 때에는, 정수(t)를 무작위로 선택하여, 공개되어 있는 공개키를 이용하고, 쌍선형 사상의 연산을 행한다.

<202> 헤더 요소 산출부(309)는, 키생성장치(20)에 의해 구축된 계층화 된 나무구조에 있어서, 배제된 수신장치가 할당된 리프로부터 루트에 이르는 패스 상에 존재하는 모든 노드 각각에 마크를 하고, 마크된 노드에 할당된 파라미터와, 마크된 노드를 부모 노드로 하는 중간 노드에 할당된 리프키와에 의거하여, 헤더 요소를 산출한다.

<203> 헤더 정보 생성부(311)는, 헤더 요소 산출부(309)에 있어서 얻어진 헤더 요소와, 공개키에 의거하여, 헤더 정보를 생성한다.

<204> 콘텐츠 기억부(313)는, 암호화되어 있지 않은 콘텐츠를 기억한다. 또, CD(Compact Disk), DVD(Digital Versatile Disk)나 메모리 카드 등의 미디어 매체로부터 취득한 콘텐츠를 기억한다고 해도 좋다. 여기서, 상기의 콘텐츠란, 예를 들면, 영화, 텔레비전 프로그램, 비디오 프로그램, 도표 등의 동영상 또는 정지화면으로

이루어지는 영상(Video) 콘텐츠, 음악, 강연, 라디오 프로그램 등의 음성(Audio) 콘텐츠나, 게임 콘텐츠, 문서 콘텐츠, 소프트웨어 등, 임의의 콘텐츠 데이터라도 좋다. 영상 콘텐츠는, 영상 데이터뿐만 아니라, 음성 데이터를 포함하고 있어도 좋다.

<205> 암호화부(315)는, 콘텐츠 기억부(313)로부터 전달하는 콘텐츠를 골라내고, 세션 키 결정부(307)에서 산출된 세션 키(s)를 이용하여, 콘텐츠를 암호화한다.

<206> 콘텐츠 송신부(317)는, 암호화부(315)에 의해서 암호화된 암호화 콘텐츠와, 헤더 정보 생성부(311)에 의해서 결정된 헤더와, 배제 수신장치 특정부(305)에 의해서 특정된 집합(S)을, 통신망(12)을 통하여, 각 수신장치에 송신한다.

<207> 계속하여, 본 실시형태와 관련되는 수신장치(40)의 구성에 대하여, 도 11을 참조하면서 설명한다. 도 11은, 본 실시형태와 관련되는 수신장치(40)의 구성을 나타낸 블럭도이다.

<208> 도 11에 나타낸 바와 같이, 수신장치(40)는, 예를 들면, 수신부(401)와, 기억부(403)와, 판정부(405)와, 복호부(407)를 갖춘다

<209> 수신부(401)는, 키생성장치(20)에 의해 생성된 개인 비밀키를 수신한다. 또, 수신부(401)는, 개인 비밀키 이외에도, 키생성장치(20)에 의해 생성된 공개키나, 배제하는 수신장치가 특정된 정보인, 배제되어 있지 않은 수신장치의 집합(S)에 관한 정보를 더 수신할 수 있다. 또, 암호화장치(30)에 의해서 암호화된 콘텐츠에 대해서도, 수신하는 것이 가능하다.

<210> 기억부(403)는, 예를 들면, 키생성장치(20)에 의해서 생성된 공개키나 개인 비밀키를 기억한다. 또, 이러한 암호키 이외에도, 배제되어 있지 않은 수신장치의 집합(S)에 관한 정보나, 전달된 암호화 콘텐츠나 복호된 콘텐츠 등의 콘텐츠 정보를 기억하는 것이 가능하다.

<211> 판정부(405)는, 수신장치 자신이, 수신한 집합(S) 안에 포함되어 있는지 아닌지를 판정한다. 판정부(405)의 판정 결과에 따라, 복호부(407)는, 암호화 콘텐츠의 복호 처리를 행한다.

<212> 복호부(407)는, 수신부(401)가 수신한 헤더(h)와, 기억부(403)가 기억하고 있는 공개키 및 개인 비밀키를 이용하여, 암호화 콘텐츠의 복호에 필요한 세션 키(s)를 산출한다. 세션 키(s)를 산출한 후에, 복호부(407)는 계속해서, 암호화 콘텐츠의 복호화를 행한다.

<213> 이상, 본 실시형태와 관련되는 키생성장치(20), 암호화장치(30) 및 수신장치(40)의 기능의 일례를 나타냈다. 상기의 각 구성요소는, 범용적인 부재나 회로를 이용하여 구성되어 있어도 좋고, 각 구성요소의 기능에 특화한 하드웨어에 의해 구성되어 있어도 좋다. 또, 각 구성요소의 기능을, CPU 등이 모두 행해도 좋다. 따라서, 본 실시형태를 실시하는 그때그때의 기술 레벨에 따라서, 적당, 이용하는 구성을 변경하는 것이 가능하다.

<214> 본 실시형태와 관련되는 암호키 전달시스템(10)은, 비 특허문헌 1과 같이, 키생성, 암호화 및 복호라고 하는 세 개의 국면으로 구성된다. 키생성국면은, 센터가 시스템 구성시에 한 번만 실행한다. 또, 암호화국면은 전달자가, 복호국면은 계약자가, 각각 전달마다 실행한다. 또한, 본 실시형태와 관련되는 암호키 전달시스템(10)을 설명하는데 있어서 사용하는 각 기호 및 연산은, 기반기술의 설명 시에 정의한 것과 동일한 것으로 한다. 이하, 처음에 본 실시형태에 있어서 구성하는 논리목에 관하여 정의 및 설명을 행하고, 그 후, 각 국면에 대하여, 상세하게 설명한다.

<215> <논리목의 구성과 정의>

<216> 본 실시형태와 관련되는 키생성장치(20)를 설명하는데 있어서 필요한 논리목에 관하여, 우선 설명 및 정의를 행한다. 본 실시형태와 관련되는 키생성장치(20)에서는, 각 계약자를 리프에 할당하고, 또한 비 특허문헌 1에 있어서의 계약자의 분할을 이 논리목에 할당함으로써, 효율적인 콘텐츠 전달을 실현하고 있다. 이 논리목은, 본 실시형태와 관련되는 키생성장치(20)에 있어서의, 나무구조 구성부(231)에 의해서 구성된다.

<217> 또한, 간단하기 때문에, 본 실시형태에서는, Y분 나무를 이용하는 것으로 한다. 또, 전 계약자를 리프에 할당할 필요가 있기 때문에, 계약자의 총수(n)가, Y의 제곱 승으로 표시되는 값이라고 가정한다. 다만, 실제의 콘텐츠 전달에 있어서는, n이 Y의 제곱 승이 되지 않는 경우도 많이 존재한다. 그러나, 이 경우에는, n보다 충분히 큰 Y의 제곱 승수의 리프를 미리 준비해 둠으로써, 용이하게 대응하는 것이 가능하다. 이하에, 논리목의 구성에 대해서, 각 정의를 나타낸다.

<218> 본 실시형태에 있어서 이용하는 Y분 나무는, 리프의 개수가 n이므로, 루트를 제외한 Y분 나무의 높이를 H로 하

면, H=$\log_Y n$이 된다. 또, 리프를 제외한 노드의 총수를 N으로 하면, N=(n-1)/(Y-1)이 된다. 따라서, Y분 나무에는 루트 이외에 H개의 계층이 존재하고, 여기에서는, 이 계층을 Layer라고 정의한다. 즉, 루트의 자식 노드의 집합을 Layer1로 하고, Layer1의 모든 노드의 자식 노드(즉, 루트의 손자 노드)의 집합을 Layer2, 라고 하는 형태로, Y분 나무의 각 계층을, Layer x(x=0, …, H)라고 정의한다. 여기서, x는, 계층을 나타내는 첨자이다. 또, Layer x에 포함되는 각 노드의 인덱스를, 노드 인덱스라고 부르기로 하고, (x,y), (y=1, …, Y^x)라고 정의한다. 이때, 루트는, Layer0의 노드이며, 그 인덱스는 (0,1)이 된다.

<219> 상기와 같이 정의한 Y분 나무의 예로서, 도 12에 계약자수(n)=9, 분기수(Y)=3으로 했을 경우를 나타낸다.

<220> 계약자수(n)가 9이기 때문에, 루트를 제외한 3분목의 높이(H)는, $\log_3 9=2$가 된다. 따라서, 이 3분목에는, 루트를 포함하여 3개의 계층이 존재한다. 즉, 루트를 포함한 계층(501)이 Layer0이 되고, 루트의 자식 노드인 3개의 노드를 포함한 계층(503)이, Layer1이 된다. Layer1에 존재하는 3개의 노드를 각각 부모 노드로 했을 경우의 자식 노드의 계층(505)이, Layer2가 된다. Layer2에는, Layer1에 존재하는 3개의 노드 각각으로부터, 3개의 자식 노드가 형성되기 위해, 전부 9개의 리프가 존재하게 된다.

<221> 또, 리프를 제외한 노드의 수(N), 즉, 루트와 중간 노드 수의 합은, (9-1)/(3-1)=4가 된다.

<222> 리프를 포함한 각각의 노드에 할당되는 노드 인덱스는, 예를 들면, 루트는 (0,1)이 되고, Layer1의 3개의 노드는, 각각 좌단으로부터 (1, 1), (1, 2), (1, 3)이 된다. 또, Layer2의 9개의 노드, 즉 리프에는, 좌단으로부터 각각 (2, 1), (2, 2), …, (2, 9)라고 하는 노드 인덱스가 첨부된다.

<223> 또, 본 실시형태와 관련되는 키생성장치(20)에서는, 이 리프 각각에 수신장치(40), 즉, 콘텐츠 전달에 관한 계약자(507)를 할당한다. 즉, Layer2의 리프 (2, 1), (2, 2), …, (2, 9)에는, 각각, 계약자(1)(507A), 계약자(2)(507B), …, 계약자(9)(507I)가 할당된다.

<224> 계속하여, 상술한 논리목에 관한 정의를 이용하여, 이하에, 본 실시형태와 관련되는 암호키 전달시스템의 구체적인 설명을 나타낸다.

<225> <키생성장치(20)의 동작 : 암호키생성국면>

<226> 센터는, 소유하는 키생성장치(20)를 조작하고, 이하의 순서에 따라서, 공개키와 각 계약자의 개인 비밀키를 생성한다. 이하에, 도 12, 도 13 및 도 14를 참조하면서, 본 실시형태와 관련되는 키생성장치(20)의 동작에 대해서, 상세하게 설명한다. 도 13은, 키생성장치(20)에 의한 키 생성의 개요를 설명하기 위한 설명도이다. 도 14는, 키생성장치(20)에 의한 암호키생성국면의 흐름도이다.

<227> 우선, 키생성장치(20)의 난수 결정부(233)는, 값이 큰 소수(p)를 무작위로 선택하고, 선택한 p를 위수라고 하는 쌍선형군(G)을 결정한다(스텝S101). 여기서, 값이 큰 소수(p)란, 자리수가 많은 소수를 의미한다. 난수 결정부(233)는, 용이하게 이산대수(離散對數)문제가 풀리지 않을 것 같은 자리수가 많은 소수를 선택하는 것으로, 본 실시형태와 관련되는 암호키의 안전성을 담보한다.

<228> 계속하여, 난수 결정부(233)는, 쌍선형군(G)의 생성요소(g)와, 센터 비밀인 난수 α(α는 정수)를, 무작위로 선택한다(스텝S103).

<229> 이러한 소수(p), 쌍선형군(G), 생성요소(g) 및 난수(α)에 관한 데이터는, 예를 들면, 기억부(241) 중의 난수 기억부(245) 안에 기억되며, 리프키 할당부(235), 파라미터 할당부(237), 또는 암호키 산출부(239) 등에 의해서 참조된다.

<230> 계속하여, 키생성장치(20)의 나무구조 구성부(231)는, 분할된 서브그룹에 소속하는 계약자수(Y)를 결정하고, 분할수(X)를 이하의 계산에 의해 결정한 후, 계약자를 X개의 서브그룹에 분할한다. 또한, 각 계약자를 리프로서 할당된 Y분 나무를 구성한다(스텝S105). 여기서, 이하의 식 101 중의 n은, 계약자의 총수이다.

수학식 18

<231>
$$X = \left\lceil \frac{n}{Y} \right\rceil \quad \cdots (식101)$$

<232> 예를 들면, 도 12에 나타낸 바와 같이, 계약자의 총수(n)가 9명이며, Y=3, 즉 3분목을 구축하는 경우에는, 분

할수(X)는, 식 101에서 3이 된다.

<233> 이상과 같이 하여 구축된 Y분 나무구조를, 나무구조 구성부(231)는, 기억부(241) 중의 나무구조 기억부(243)에 기억시킨다.

<234> 다음에, 키생성장치(20)의 리프키 할당부(235)는, i(i=1, …, Y, Y+2, …, 2Y)에 대하여, 리프키(g_i)를, 이하와 같이 하여 산출한다(스텝S107).

수학식 19

$$g_i = g^{(\alpha)^i} \quad \cdots(식102)$$

<235>

<236> 상기의 식 102에서도 분명한 바와 같이, 리프키(g_i)의 산출에 있어서는, 난수 결정부(233)가 결정된 생성요소(g) 및 센터 비밀인 난수(α)를 이용한다. 그 때문에, 리프키 할당부(235)는, 기억부(241) 중의 난수 기억부(245)에 액세스하고, 이러한 데이터를 읽어낸다. 리프키를 산출한 후에는, 리프키 할당부(235)는, 산출한 리프키(g_i)를, 기억부(241) 중의 리프키 기억부(247)에 보존한다.

<237> 또한, 스텝(S107)에 있어서는, 리프키(g_i)를, 서브그룹에 소속하는 계약자의 수인 Y개 뿐만이 아니라, i를 Y+1을 제외한 2Y까지 변화시키고, 리프키(g_i)를 산출하고 있다. g_{Y+1}을 산출하지 않는 이유는, 본 실시형태와 관련되는 암호키 전달시스템(10)의 안전성을 담보하기 때문이며, g_{Y+2}부터 g_{2Y}까지의 리프키(g_i)는, 후에 기술하는 복호국면으로 복호를 행할 때에 필요하기 때문이다.

<238> 계속하여, 암호키 작성 장치(20)의 파라미터 할당부(237)는, 리프를 제외한 모든 노드(x,y)에 대응하는 난수 $\gamma_{x,y}$($\gamma_{x,y}$는 정수)를 무작위로 선택한다. 계속하여, 파라미터($v_{x,y}$)를 이하와 같이 산출하고, Y분 나무의 리프를 제외한 각 노드에, 각각 할당한다(스텝S109). 여기서, x=0, …, H-1(H는, Y분 나무구조의 높이이다.)이며, y=1, …, Y^x이다.

수학식 20

$$v_{x,y} = g^{\gamma_{x,y}} \in G \quad \cdots(식103)$$

<239>

<240> 예를 들면, 도 12와 같이, 9명의 계약자에 대해서 3분나무구조를 구축했을 경우에는, 3분나무구조의 높이(H)는 2이기 때문에, x는 0 또는 1이 된다. 또, y는, 1, 2, 3이 된다. 즉, 도 12의 경우는, 파라미터 할당부(237)에 의해 할당되는 파라미터($v_{x,y}$)는, $v_{0,1}$, $v_{1,1}$, $v_{1,2}$, $v_{1,3}$의 합 4개가 된다. 따라서, $\gamma_{x,y}$에 대해서도, 4개의 정수가 무작위로 선택되게 된다. 이와 같이 하여 결정된 값에 의거하여, 식 103에 의해서, 각 노드에 파라미터가 할당된다.

<241> 또, 파라미터 할당부(237)에 의해서 산출된 파라미터($v_{x,y}$)나 노드 파라미터($\gamma_{x,y}$) 등은, 기억부(241) 중의 파라미터 기억부(249)에 기억된다.

<242> 계속하여, 리프키 할당부(235)는, 루트를 제외한 모든 노드에 대해서, $g_{x,y}$를 할당한다(스텝S111). 여기서, y=1, …, Y^x이며, $g_{x,y}$는, g_1, …, g_Y로 이루어지는 집합 {g_1, …, g_Y}의 요소이다. 이상과 같이, 리프키 할당부(235)는, 리프키(g_y)를 산출하는 기능과, 산출한 리프키를, 루트를 제외한 모든 노드에 할당하는 기능의 쌍방을 가진다. 할당한 결과는, 기억부(241) 중의 리프키 기억부(247)에, 나무구조로 관련지어 기억된다.

<243> 예로서, 도 12에 나타낸 경우를 생각한다. 이 경우, Layer1(503)에는, 루트를 부모 노드로 하는 3개의 자식 노드가 존재하고, 1개의 서브그룹을 구성하고 있다. 따라서, 노드(1,1)에는, $g_{1,1}$로서 g_1이, 노드(1,2)에는, $g_{1,2}$로서 g_2가, 노드(1,3)에는, $g_{1,3}$으로서 g_3이 할당된다.

<244> 또, Layer2(505)를 생각하면, 이 노드(1,1)를 부모 노드로 하는 3개의 자식 노드(2,1), (2,2), (2,3)로 이루어

지는 서브그룹과, 노드(1,2)를 부모 노드로 하는 3개의 자식 노드(2,4), (2,5), (2,6)로 이루어지는 서브그룹과, 노드(1,3)를 부모 노드로 하는 3개의 자식 노드(2,7), (2,8), (2,9)로 이루어지는 서브그룹의, 합계 3개의 서브그룹이 존재하고 있다. 이 경우, 노드(2,1)에는, $g_{2,1}$로서 g_1이, 노드(2,2)에는, $g_{2,2}$로서 g_2가, 노드(2,3)에는, $g_{2,3}$으로서 g_3이 할당된다. 마찬가지로 하여, 노드(2,4)에는, $g_{2,4}$로서 g_1이, 노드(2,5)에는, $g_{2,5}$로서 g_2가, 노드(2,6)에는, $g_{2,6}$으로서 g_3이 할당되며, 노드(2,7)에는, $g_{2,7}$로서 g_1이, 노드(2,8)에는, $g_{2,8}$로서 g_2가, 노드(2,9)에는, $g_{2,9}$로서 g_3이 할당된다.

<245> 계속하여, 키생성장치(20)의 키 산출부(239)는, 공개키(PK)를 이하와 같이 구성하고, 공개키 공개부(255)를 통하여 공개한다(스텝S113).

<246> $PK=(g, g_1, \cdots, g_Y, g_{Y+2}, \cdots, g_{2Y}, v_{0,1}, \cdots, v_{H-1,X})$…(식 104)

<247> 상기의 식 104에서 분명한 바와 같이, 공개키(PK)는, 난수 결정부(233)가 결정된 생성요소(g)와, 리프키 할당부(235)가 산출한 리프키(g_i)와, 파라미터 할당부(237)가 산출한 파라미터($v_{x,y}$)로 구성되어 있다. 따라서, 키 산출부(239)는, 기억부(241) 중의 각 기억부(245,247,249)를 참조하여, 공개키(PK)를 구성한다. 키 산출부(239)는, 구성한 공개키(PK)를, 기억부(241) 중의 키 기억부(251)에 기억한다. 공개키 공개부(255)는, 이 키 기억부(251)를 참조하여, 공개키를 공개한다. 또한, 키 산출부(239)는, 구성한 공개키(PK)를, 직접 공개키 공개부(255)로 송신해도 좋다.

<248> 예로서, 도 12에 나타낸 경우를 생각한다. 이 경우, 공개키(PK)로서 공개되는 것은, $(g, g_1, g_2, g_3, g_5, g_6, v_{0,1}, v_{1,1}, v_{1,2}, v_{1,3})$이 된다.

<249> 계속하여, 키 산출부(239)는, 계약자(i)(i=1, …, n)에 대해서, 루트로부터 계약자(i)에게 할당된 리프에 이르는 패스를 특정하고, 그 패스 상에 있는 Layer x상의 노드에 대한 계약자(i)의 인덱스를 i_x로 한다. 즉, $i_0=(0,1)$이고, $i_H=(H,i)$이다. 센터는, 계약자(i)에게 할당된 루트를 제외한 모든 노드(i_1, …, i_H)에 대하여, 이러한 노드에 할당된 파라미터(g_{ix})를 특정한다. 또, 리프를 제외한 모든 노드(i_0, …, i_{H-1})에 할당파라미터(γ_{ix})를 특정하고, 이하와 같이 하여 계약자(i)의 개인 비밀키(d_i)를 계산한다. 그 후, 송신부(253)는, 개인 비밀키(d_i)를, 안전한 통신로를 이용하여 계약자(i)에게 배포한다(스텝S115).

수학식 21

$$d_i=\{g_{i_1}^{\gamma_{i_0}},\ldots,g_{i_H}^{\gamma_{i_{H-1}}}\}=\{v_{i_0}^{\alpha^{i_1}},\ldots,v_{i_{H-1}}^{\alpha^{i_H}}\}\in G^H \quad \cdots(식105)$$

<250>

<251> 식 105에서 분명한 바와 같이, 개인 비밀키(di)의 각 요소는, 특정한 패스 상에 있는 노드(i_x)에 할당된 리프키(g_{ix})와, 노드(i_x)의 부모 노드가 되는 노드에 할당된 파라미터(γ_{ix-1})에 의거하여 계산된다. 즉, 각각의 개인 비밀키(d_i)는, 각 노드에 할당된 리프키에 의거하여 산출된 키 세트라고 말할 수 있다. 또한, 상기의 스텝(S115)의 구체적인 예에 대해서는, 이하에서, 도 15를 참조하면서 상세하게 설명한다.

<252> 또한, 키 산출부(239)에 있어서, 각 계약자 고유의 개인 비밀키(d_i)가 산출되면, 키 산출부(239)는, 이러한 개인 비밀키를, 기억부(241) 중의 키 기억부(251)에 기억한다. 송신부(253)가, 각 계약자에 대해서 개인 비밀키(d_i)를 송신하는 경우에는, 송신부(253)는, 기억부(241) 중의 키 기억부(251)를 참조하여, 필요한 정보를 취득한다. 또, 키 산출부(239)가, 생성한 개인 비밀키를, 직접 송신부(253)로 주고 받도록 해도 좋다.

<253> 계속하여, 도 15를 참조하면서, 상기의 스텝(S115)의 구체적인 예를 예시한다. 도 15에서는, 9명의 계약자에 대해서, 3분나무구조가 구축되어 있다. 여기서, 리프(2,3)에 할당되어 있는 계약자(3)에게, 개인 비밀키(d_3)를 송신하는 경우를 생각한다.

<254> 루트(0,1)에서, 계약자(3)인 리프(2,3)로 도달하는 패스는, 루트(0,1)에서, 중간 노드(1,1)를 경유하여, 리프(2,3)로 도달하는 패스가 된다. 이 경우, 루트(0,1) 이외의 패스 상의 노드인 (1,1)과 (2,3)이, 각각 i_1과 i_2

가 된다. 여기서, 노드 (0,1), (1,1), (2,3)에 각각 할당되어 있는 파라미터를 생각한다. 노드 (0,1)에는, γ_{i0}으로서, $\gamma_{0,1}$이 할당되어 있다. 노드(1,1)에는, γ_{i1}로서 $\gamma_{1,1}$이 할당되며, g_{i1}로서, $g_{1,1}$인 g_1이 할당되어 있다. 또, 리프(2,3)에는, g_{i2}로서 $g_{2,3}$인 g_3이 할당되어 있다.

<255> 계약자(3)가 보관 유지하게 되는 개인 비밀키(d_3)는, 식 105에서, 노드(1,1)에 할당된 리프키(g_1)를 노드(1,1)의 부모 노드인 루트(0,1)에 할당된 $\gamma_{0,1}$로 제곱 승한 것과, 리프(2,3)에 할당된 리프키(g_3)를 리프(2,3)의 부모 노드인 노드(1,1)에 할당된 $\gamma_{1,1}$로 제곱 승한 것의 세트가 된다.

<256> 이상 설명한 바와 같이, 본 실시형태와 관련되는 키생성장치(20)는, 도 13에 나타낸 바와 같이, 센터(509)가 소유하는 키생성장치(20)가, 쌍선형군(G)이나, 각종의 파라미터를 선택하여, 공개키(PK)와, 계약자 고유의 개인 비밀키(d_i)를 생성한다. 그리고, 센터(509)는, 공개키(PK)를 공개하는 동시에, 각 계약자(507)에 대해서, 안전한 일대일 통신로(511)를 이용하여, 개인 비밀키(d_i)를 배포한다.

<257> ＜암호화장치(30)의 동작 : 암호화국면＞

<258> 계속하여, 도 16 및 도 17을 참조하면서, 본 실시형태와 관련되는 암호화장치(30)의 동작, 즉 암호화국면을 상세하게 설명한다. 도 16은, 암호화장치(30)에 의한 암호화의 개요를 설명하기 위한 설명도이다. 도 17은, 암호화장치(30)에 의한 암호화국면의 흐름도이다. 또한, 이하에 설명하는 암호화국면은, 암호화장치(30)를 소유하는 임의의 제 3자가 실시하는 것도 가능하다. 또, 키생성장치(20)의 소유자나 수신장치(40)의 소유자라도, 암호화장치(30)의 소유자이면, 이하의 암호화국면을 행하는 것이 가능하다.

<259> 이하에 설명하는 암호화국면을 실행하는데 앞서, 암호화장치(30)의 수신부(301)는, 키생성장치(20)에 의해서 생성 및 공개된 공개키와, 소수(p)와, 나무구조에 관한 정보와, 배제되어 있지 않은 수신장치의 집합(S)에 관한 정보를 각각 수신한다. 수신부(301)가 취득한 이러한 정보는, 기억부(303)에 기억된다. 기억부(303)에 기억된 이러한 정보는, 암호화장치(30)의 각 처리부가, 자유롭게 읽어낼 수 있다.

<260> 우선, 배제 수신장치 특정부(305)는, 배제하고 싶은 모든 계약자에게 할당된 리프에서 루트에 이르는 패스 상에 있는 모든 노드를 마크하고, 배제되어 있지 않은 계약자가, 헤더(h)로부터 자신에게 할당된 헤더 요소를 특정하기 위한 노드 인덱스의 집합(S)을, $S=\phi$(ϕ는 공집합을 나타낸다.)로서 초기화한다(스텝S301).

<261> 계속하여, 세션 키 결정부(307)는, 임의의 정수(t)를 무작위로 선택하여, 세션 키(s)를 이하와 같이 산출한다(스텝S303).

<262> $s=e(g_{Y+1},g)^t=e(g_Y,g_1)^t$ …(식 106)

<263> 계속하여, 헤더 요소 산출부(309)는, 계층을 나타내는 파라미터인 x를 －1로 설정한다(스텝S305). 즉, 이 스텝(S305)은, 계층을 나타내는 파라미터(x)의 초기화 스텝이다.

<264> 계속하여, 헤더 요소 산출부(309)는, x에 x＋1을 대입하고, x의 값을 1개 증가시킨다(스텝S307).

<265> 다음에, 헤더 요소 산출부(309)는, y를 제로로서, 파라미터의 초기화를 도모한다(스텝S309).

<266> 계속하여, 헤더 요소 산출부(309)는, 각 layer에 있어서의 노드의 위치를 나타내는 파라미터인 y에, y＋1을 대입하고, y의 값을 1개 증가시킨다(스텝S311).

<267> 다음에, 헤더 요소 산출부(309)는, 노드(x,y)에 대응하는 헤더 요소 $c_{x,y}$를, $c_{x,y}=0$으로서 초기화한다(스텝S313).

<268> 이하에 나타내는 스텝에서, 헤더 요소 산출부(309)는, 헤더 요소를 산출하기 위한 구체적인 처리를 행하게 된다.

<269> 계속하여, 헤더 요소 산출부(309)는, 노드(x,y)의 자식 노드가, 모두 마크되어 있는지 아닌지를 판정한다(스텝S315). 판정의 결과, 모든 자식 노드가 마크되어 있는 경우에는, 이하에 나타내는 스텝(S321)으로 진행된다. 또, 마크되어 있지 않은 자식 노드가 존재하는 경우에는, 이하의 스텝(S317)으로 진행된다.

<270> 다음에, 헤더 요소 산출부(309)는, 마크되어 있지 않은 자식 노드의 집합을 $S_{x,y}$로 하고, $S_{x,y}$의 각 요소를 루트로 하는 부분목(部分木)(서브 그룹)에 소속하는 계약자에게 대응하는 헤더 요소를, 이하와 같이 산출한다(스텝

S317).

수학식 22

$$c_{x,y} = (v_{x,y} \cdot \prod_{j \in S_{x,y}} g_{Y+1-j})^t \in G \quad \cdots(식107)$$

<271>

<272> 또, 헤더 요소 산출부(309)는, 집합(S)을 이하와 같이 설정한다(스텝S317).

수학식 23

$$S \cup S_{x,y} \quad \cdots(식108)$$

<273>

<274> 다음에, 헤더 요소 산출부(309)는, $S_{x,y}$의 각 요소를 루트로 하는 부분목에 대해서, 그 부분목에 소속하는 모든 노드(리프를 포함한다.)를 마크한다(스텝S319).

<275> 계속하여, 헤더 요소 산출부(309)는, 현재 주목하고 있는 파라미터(y)가, Y^x에 해당하는지 아닌지를 판정한다(스텝S321). 판정결과, y가 Y^x인 경우에는, 이하에 나타내는 스텝(S323)으로 이행한다. 또, y가 Y^x가 아닌 경우에는, 스텝(S311)으로 돌아와, 파라미터(y)를 1 증가시킨다.

<276> 다음에, 헤더 요소 산출부(309)는, 현재 주목하고 있는 파라미터(x)가, H-1인지 아닌지를 판정한다(스텝S323). 판정결과, x가 H-1이면, 이하의 스텝(S325)으로 이행한다. 또, x가 H-1이 아닌 경우에는, 스텝(S307)으로 돌아와, 파라미터(x)를 1 증가시킨다.

<277> 상기와 같이, 스텝(S321) 및 스텝(S323)의 조건을 모두 만족할 때까지, 스텝(S307)~스텝(S323)을 반복하는 것으로, 헤더 요소 산출부(309)는, 헤더 생성에 필요한 모든 헤더 요소를 산출하는 것이 가능하다.

<278> 즉, 구체적인 헤더 요소의 산출에 앞서, 스텝(S313)에 있어서, 주목하고 있는 노드(x,y)에 대응하는 헤더 요소($c_{x,y}$)를 제로로 초기화하고 있기 때문에, 스텝(S315)에 있어서, 주목하고 있는 노드(x,y)의 자식 노드가 모두 마크되어 있는 경우에는, 노드(x,y)의 헤더 요소($c_{x,y}$)는 제로인 채로 기억된다. 또한, 주목하고 있는 노드(x,y)의 자식 노드가 모두 마크되어 있지 않은 경우에는, 스텝(S317)에 있어서, $c_{x,y}$에 새로운 값이 대입되기 때문에, $c_{x,y}$는 제로가 아닌 값을 가지게 된다.

<279> 상기의 스텝을 반복하는 것으로 얻어진 헤더 요소의 모두를, 헤더 요소 산출부(309)는, 헤더 정보 생성부(311)로 주고 받는다. 또, 헤더 요소 산출부(309)는, 산출한 헤더 요소를 기억부(303)에 기억해도 좋다.

<280> 계속하여, 헤더 정보 생성부(311)는, 생성요소(g)와, 스텝(S303)에서 선택한 t를 이용하여, g^t를 계산한다. 또, 헤더 요소($c_{x,y}$)가 제로가 아닌 헤더 요소만을 이용하여, 헤더(h)를 이하와 같이 구성한다(스텝S325).

<281> $h=(g^t, c_{0,1}, \cdots, c_{H-1,X})\ (c_{x,y} \neq 0)$ …(식 109)

<282> 헤더 정보 생성부(311)는, 헤더 정보를 생성하면, 생성한 헤더(h)를 암호화부(315)로 주고 받는다. 또, 헤더 정보 생성부(311)는, 생성한 헤더(h)를, 기억부(303)에 기억해도 좋다.

<283> 계속하여, 암호화부(315)는, 암호화되어 있지 않은 전달 예정의 콘텐츠(M)를 콘텐츠 기억부(313)로부터 받고, 세션키 결정부(307)가 결정된 세션 키(s)를 이용하여, 이하와 같이, 콘텐츠(M)를 암호화한다. 그 후, 콘텐츠 송신부(317)는, 암호화한 콘텐츠(C)를, 헤더 정보 생성부(311)가 생성한 헤더(h) 및 노드 인덱스의 집합(S)과 함께, 계약자에게 송신한다(스텝S327).

<284> $C=E_s(M)$ …(식 110)

<285> 계속하여, 도 18~도 20을 참조하면서, 본 실시형태와 관련되는 암호화국면에 대해서, 구체적으로 설명한다. 도 18~도 20은, 본 실시형태와 관련되는 암호화국면에 대해서, 구체적으로 설명하기 위한 설명도이다. 도 18~도 20에서는, 3분나무구조가 구축되며, 리프에 9명의 계약자가 할당되어 있는 경우이다.

<286> 이하의 예에서는, 배제하고 싶은 계약자가 계약자(2) 및 계약자(3)인 경우를 설명한다. 도 18에 나타낸 바와 같이, 계약자(2)에게는 리프(2,2)가 할당되며, 계약자(3)에게는 리프(2,3)가 할당되어 있다. 이 경우, 배제하고 싶은 계약자인 계약자(2)로부터 루트에 도달하는 패스는, 리프(2,2)로부터 노드(1,1)를 경유하여 루트(0,1)로 도달하는, 도 18에 있어서 점선으로 나타낸 패스이다. 마찬가지로, 배제하고 싶은 계약자인 계약자(3)로부터 루트에 도달하는 패스는, 리프(2,3)로부터 노드(1,1)를 경유하여 루트(0,1)로 도달하는, 도 18에 있어서 점선으로 나타낸 패스이다. 이 경우, 배제 수신장치 특정부(261)는, 루트(0,1), 노드(1,1), 리프(2,2) 및 리프(2,3)에 마크를 첨부하기로 한다. 또한, 도 18에서는, 마크가 첨부된 노드를, 점선으로 둘러싸 나타내고 있다. 그 후, 세션 키 결정부(307)에 의해, 스텝(S303)이 실행되며, 세션 키(s)가 결정된다.

<287> 계속하여, 헤더 요소 산출부(309)에 의해, 스텝(S305)~스텝(S311)이 실행된다. 그 결과, 파라미터(x)에는 0이 대입되며, 파라미터(y)에는 1이 대입된다. 계속하여, 헤더 요소 산출부(309)는, 스텝(S313)을 실행한다. 이 경우, 노드(0,1)에 대한 헤더 요소($c_{0,1}$)가 제로로 초기화된다. 계속하여, 헤더 요소 산출부(309)는, 스텝(S315)을 실행하고, 루트(0,1)의 자식 노드가 모두 마크되어 있는지를 판정한다. 도 19에서 분명한 바와 같이, 루트(0,1)의 자식 노드는 (1,1), (1,2), (1,3)의 3개지만, 노드 (1,2) 및 (1,3)에는, 마크가 첨부되어있지 않다. 따라서, 헤더 요소 산출부(309)는, 스텝(S317)을 실행하게 된다.

<288> 도 19의 경우, 마크되어 있지 않은 자식 노드의 집합($S_{0,1}$)은, {(1,2), (1,3)} 이 된다. 또, 노드(1,2)에는 g_2가, 노드(1,3)에는 g_3이 각각 할당되어 있기 때문에, 헤더 요소($c_{0,1}$)를 산출하면, $(v_{0,1} \cdot g_2 \cdot g_1)^t$가 된다.

<289> 계속하여, 헤더 요소 산출부(309)는, 스텝(S319)을 실행한다. 스텝(S319)에 의해, $S_{0,1}$의 요소인 노드 (1,2)를 루트로 하는 부분목의 모든 노드인, 노드(1,2), 리프(2,4), 리프(2,5), 리프(2,6)에 마크가 첨부되게 된다. $S_{0,1}$의 또 하나의 요소인 노드(1,3)에 대해서도 마찬가지로, 노드(1,3), 리프(2,7), 리프(2,8), 리프(2,9)에 마크가 첨부되게 된다.

<290> 헤더 요소 산출부(309)에 의한 스텝(S321)의 판정은, y=1로 되어 있기 때문에, 조건을 만족하게 된다. 따라서, 헤더 요소 산출부(309)는, 계속하여, 스텝(S323)의 판정을 행한다. 이 경우, $x=0 \neq 1$이므로, 분기 조건은 만족하고 있지 않다. 따라서, 헤더 요소 산출부(309)는, 스텝(S307)으로 돌아와, x=1로서 처리를 반복하게 된다.

<291> 재차 돌아온 스텝(S307)부터, 스텝(S311)까지 순으로 처리가 행해지면, x에는 1이, y에는 1이 대입되고 있다. 따라서, 다음은, 노드(1,1)에 대해서, 동일한 처리를 행한다.

<292> 이 경우, 노드(1,1)의 마크되어 있지 않은 자식 노드의 집합($S_{1,1}$)은, {(2,1)} 뿐인다. 이와 같이 하여, 헤더 요소의 산출이 행해지며, 헤더 요소($c_{1,1}$)로서 $(v_{1,1} \cdot g_3)^t$가 산출된다. 그리고, 스텝(S319)에 의해, 노드(1,1)를 루트로 하는 부분목의 모든 노드에 마크가 첨부되기 때문에, 아직도 마크가 첨부되어있지 않았던 리프(2,1)에 대해서도, 마크가 첨부되게 된다.

<293> 그 결과, 루트 및 리프를 포함한, 3분나무구조의 모든 노드에 대해서 마크가 첨부되기 때문에, 스텝(S323)에 있어서의 판정에서는, 분기 조건을 만족하게 된다.

<294> 상기의 처리에 의해, 헤더 정보 생성부(311)는, 헤더 요소($c_{x,y}$)의 값이 제로가 아닌 헤더 요소, 즉, $c_{0,1}$과 $c_{1,1}$을 이용하여, 헤더(h)를 구성하게 된다. 따라서, 헤더(h)로서는, (g_t, $c_{0,1}$, $c_{1,1}$)이 구성되게 된다. 또, 전달되는 콘텐츠를 복호 가능한 계약자의 집합을 의미하는 S는, 상기의 처리에 의해, {(1,2), (1,3), (2,1)} 이 된다.

<295> 이상 설명한 바와 같이, 본 실시형태와 관련되는 암호화 콘텐츠 전달 블록은, 도 16에 나타낸 바와 같이, 전달자(513)가, 공개키(PK)와, 자신이 선택한 난수(t)를 이용하여, 세션 키(s)와 헤더(h)를 산출한다. 마찬가지로, 전달자(513)는, 콘텐츠를 복호 가능한 계약자의 집합(S)도 결정한다. 그리고, 전달자(513)는, 동보 통신로(515)를 통하여, 계약자(507), 비계약자(517)를 불문하고, 암호화 콘텐츠(C), 헤더(h) 및 집합(S)을 전달한다.

<296> <수신장치(40)의 동작 : 복호국면>

<297> 계속하여, 도 21을 참조하면서, 본 실시형태와 관련되는 수신장치(40)의 동작, 즉 복호국면을, 상세하게 설명한

다. 도 21은, 수신장치(40)에 의한 키처리방법인 복호국면의 흐름도이다.

<298> 우선, 암호화 콘텐츠(C), 헤더(h), 집합(S)을 수신부(401)에 의해 수신한 수신장치(40)는, 이러한 정보를 일단 기억부(403)에 기억한다. 이 후, 암호화 콘텐츠(C)의 복호 처리를 한다.

<299> 우선, 수신장치(40)의 판정부(405)는, 기억부(403)에 기억되고 있는 집합(S)을 참조하여, 자신이 할당된 리프에서 루트에 이를 때까지의 각 노드 중, 집합(S)에 포함되는 것이 존재하는지 아닌지를 판정한다(스텝S501). 판정의 결과, 집합(S)에 포함되는 노드가 존재하지 않으면, 자신은 배제된 것으로서, 이하의 복호 처리를 종료한다. 또, 판정결과, 집합(S)에 포함되는 노드가 존재하는 경우에는, 집합(S)에 포함되는 노드의 노드 인덱스를 (x',y')로서, 이하의 스텝(S503)을 행하게 된다.

<300> 수신장치(40)의 복호부(407)는, 수신부(401)가 수신하여 기억부(403)에 기억되고 있는 헤더(h)의 각 요소 중, 노드(x',y')의 부모 노드(x,y)에 대응하는 헤더 요소($c_{x,y}$)와 g^t를 선택한다(스텝S503). 여기서, 노드(x',y')의 부모 노드(x,y)는, 이하의 식에서 표시된다.

수학식 24

$$(x,y)=(x'-1,\left\lceil\frac{y'}{Y}\right\rceil) \quad \cdots(식\ 111)$$

<301>

<302> 또, 복호부(407)는, 공개키와, 자신의 개인 비밀키(d_i)로부터 노드(x',y')에 대응하는 요소를 이용하고, 이하와 같이 세션 키(s)를 취득한다(스텝S503).

수학식 25

$$s=\frac{e(g_{i_{x'}},c_{x,y})}{e(g_{i_{x'}}^{\gamma_{(x'-1)}}\cdot\prod_{\substack{j\in S_{x,y}\\ j\neq i_{x'}}}g_{Y+1-j+i_{x'}},g^t)} \quad \cdots(식\ 112-1)$$

$$=\frac{e(g_{i_{x'}},(v_{x,y}\cdot\prod_{j\in S_{x,y}}g_{Y+1-j})^t)}{e(v_{i_x}^{(\alpha^{(x')})}\cdot\prod_{\substack{j\in S_{x,y}\\ j\neq i_{x'}}}g_{Y+1-j+i_{x'}},g^t)} \quad \cdots(식\ 112-2)$$

$$=\frac{e(g_{i_{x'}},g_{Y+1-i_{x'}}{}^t)\cdot e(g_{i_{x'}},(v_{i_x}\cdot\prod_{\substack{j\in S_{x,y}\\ j\neq i_{x'}}}g_{Y-1-j})^t)}{e(v_{i_x}^{(\alpha^{(x')})}\cdot\prod_{\substack{j\in S_{x,y}\\ j\neq i_{x'}}}g_{Y+1-j+i_{x'}},g^t)} \quad \cdots(식\ 112-3)$$

$$=\frac{e(g,g_{Y+1})^t\cdot e(g^t,(v_{i_x}^{(\alpha^{(x')})}\cdot\prod_{\substack{j\in S_{x,y}\\ j\neq i_{x'}}}g_{Y+1-j+i_{x'}})^t)}{e(v_{i_x}^{(\alpha^{(x')})}\cdot\prod_{\substack{j\in S_{x,y}\\ j\neq i_{x'}}}g_{Y+1-j+i_{x'}},g^t)} \quad \cdots(식\ 112-4)$$

$$=e(g,g_{Y+1})^t \quad \cdots(식\ 112-5)$$

<303>

<304> 계속하여, 복호부(407)는, 얻어진 세션 키(s)를 이용하여, 암호화된 콘텐츠(C)를 복호하고, 평문(M)을 얻는다(스텝S505).

<305> $M=Ds(C)$ …(식 113)

<306> 계속하여, 도 22를 참조하면서, 본 실시형태와 관련되는 복호국면을, 구체적으로 설명한다. 도 22는, 본 실시형태와 관련되는 복호국면을 구체적으로 설명하기 위한 설명도이다. 도 22에서는, 3분나무구조가 구축되며, 리프에 9명의 계약자가 할당되어 있는 경우이다.

<307> 이하의 예에서는, 배제하고 싶은 계약자가 계약자(2) 및 계약자(3)로서, 계약자(1~9)에게 암호화 콘텐츠(C), 헤더(h), 집합(S)이 전달되어 있는 경우를 상정한다. 이하에서는, 리프(2,4)에 할당된 계약자(4)가, 전달된 콘텐츠를 복호하는 경우에 대해서, 상세하게 설명한다.

<308> 도 22의 경우, 계약자(4) 자신이 할당된 리프(2,4)에서, 루트(0,1)에 이르기까지 포함되는 노드는, 상기의 리프(2,4), 노드(1,2), 루트(0,1)이다. 여기서, 계약자(4)가 사용하고 있는 수신장치(40)의 판정부(405)는, 수신부(401)가 수신한 집합(S)에 관한 정보 속에, 상기의 3개의 노드가 포함되어 있는지를 판정한다.

<309> 도 22의 경우, 계약자(2) 및 계약자(3)가 배제하고 싶은 계약자이기 때문에, 집합(S)은, {(1,2), (1,3), (2,1)} 으로 되어 있다. 이것보다, 계약자(4)가 할당된 리프(2,4)의 부모 노드인, 노드(1,2)가, 집합(S)에 포함되어 있는 것을 알 수 있다. 그 때문에, 판정부(405)는, 스텝(S501)의 분기 조건이 채워져 있다고 판단하여, 복호부(407)가, 계속 복호 처리를 행한다.

<310> 이 경우, 스텝(S503)에 있어서의 노드(x',y')가, 노드(1,2)에 해당한다. 그 때문에, 노드(x',y')의 부모 노드(x,y)는, 루트(0,1)가 된다. 그래서, 복호부(407)는, 노드(0,1)에 대응하는 헤더 요소($c_{0,1}$)와, g^t를 선택한다. 또, 자신의 개인 비밀키(d_4)로부터, 노드(0,1)에 대한 요소인, $v_{0,1}$에 관한 요소와, 공개키(PK)를 이용하여, 세션 키(s)를 산출한다. 구체적으로는, 세션 키(s)를 얻기 위한 쌍선형군 사상은, 이하의 식과 같이 된다.

수학식 26

$$s = \frac{e(g_{4_1}, c_{0,1})}{e(g_{4_1}^{\gamma_{4_0}} \cdot \prod_{\substack{j \in S_{0,1} \\ j \neq 4_1}} g_{\gamma+1-j+4_1}, g^t)}$$

<311>

<312> 이상, 본 실시형태와 관련되는 암호키 전달시스템(10)에 있어서의 키 생성, 암호화 및 복호라고 하는 세 개의 국면의 일례를 상세하게 설명했다.

<313> 또한, 컴퓨터를, 상술한 바와 같은 본 실시형태와 관련되는 키생성장치(20), 암호화장치(30) 및 수신장치(40)로서 기능시키기 위한 컴퓨터 프로그램을, 작성하는 것도 가능하다. 컴퓨터 프로그램은, 컴퓨터가 갖추는 기억부에 격납되며, 컴퓨터가 갖추는 CPU에 읽혀 실행됨으로써, 그 컴퓨터를 상기의 키생성장치(20), 암호화장치(30) 및 수신장치(40)로서 기능시킨다. 또, 컴퓨터 프로그램이 기록된 컴퓨터로 읽기 가능한 기록 매체도 제공할 수 있다. 기록 매체는, 예를 들면, 자기 디스크, 광디스크, 광학 자기 디스크, 플래시메모리 등이다. 또, 상기의 컴퓨터 프로그램은, 기록 매체를 이용하지 않고, 예를 들면 네트워크를 통하여 전달해도 좋다.

<314> 계속하여, 이하에서는, 본 실시형태와 관련되는 암호키 전달시스템(10)과, 기반기술인 비 특허문헌 1에 기재한 콘텐츠전달시스템과의 비교를 행하는 것으로 한다.

<315> 기반기술인 비 특허문헌 1의 방법은, 공개키를 이용한 콘텐츠전달시스템에 있어서, 쌍선형 사상을 이용함으로써, 결탁 문제를 해결한 방식이다. 이 방식은, 미리 계약자를 복수의 서브그룹에 분할해 두고, 콘텐츠 전달시에, 서브그룹마다 다른 헤더 요소를 모두 포함한 헤더를 전달하고 있다. 이것에 의해, 배제되는 계약자 수가 증가했다고 해도, 헤더 사이즈를 일정한 값으로 하는 것이 가능해진다. 그렇지만, 현실적인 콘텐츠전달시스템에 있어서 상정되는, 배제되는 계약자가 없거나 혹은 적은 경우에 있어서도, 항상 일정 사이즈의 헤더를 전달할 필요가 있기 때문에, 전달 효율이 나빠진다고 하는 문제점이 존재한다.

<316> 또, 분할된 서브그룹에 소속하는 계약자수(B)가 큰 값이거나 혹은 자신이 소속하는 서브그룹에 있어서, 배제되는 계약자수가 적은 경우에는, 복호 시에 계약자가 실행할 필요가 있는 연산의 계산량이 커진다고 하는 문제점도 존재한다.

<317> 이것에 대해서, 본 실시형태와 관련되는 키생성장치에서는, 기반기술의 방식을 이용하여 논리목을 구성하고, 약간의 파라미터 증가를 허용함으로써, 서브그룹의 구성을 유연하게 하고, 특히 배제되는 계약자가 없거나 혹은 적은 경우에 있어서, 전달되는 헤더 사이즈를 삭감 가능하게 하는 동시에, 계약자가 실행할 필요가 있는 연산의 계산량을, 기반기술에 기재한 방식과 동등 이하로 삭감하는 것을 가능하게 하는 것이다. 이하, 기반기술과 본 실시형태와의 주된 차이점에 대하여, 국면마다 차이에 주목하여 설명하는 동시에, 헤더 사이즈 및 복호 시에 필요한 계산량에 관하여, 구체적인 수치 예를 이용하여 비교한다.

<318> <키생성국면의 차이점>

<319> 처음에, 키생성국면에 있어서의 차이점에 대하여 말한다. 기반기술의 방식에서는, 스텝(S11) 및 스텝(S13)에

있어서 각종 파라미터를 설정한 후, 스텝(S15)에 있어서, 계약자를 B인씩 A개의 서브그룹에 분할하고 있다. 본 실시형태에 있어서도 마찬가지로, 스텝(S101) 및 스텝(S103)에 있어서 각종 파라미터를 설정하고, 스텝(S105)에 있어서, 계약자를 Y인씩 X개의 서브그룹에 분할하고 있다.

<320> 그렇지만, 본 실시형태에서는, 또한 스텝(S105)에 있어서, 계약자를 리프에 할당한 Y분 나무구조를 구성하고 있다. 이것에 의해, 기반기술에서는, 스텝(S19)에 있어서, 각 서브그룹에 대응하는 헤더 요소를 하나로 정리하기 위해서 이용하는 센터 비밀인 $y_1, \cdots, y_A$나, 이러한 센터 비밀에 대응하는 공개의 값($v_1, \cdots, v_A$)이, 서브그룹의 분할수인 A개 필요한데 대해, 본 실시형태에서는, 스텝(S105)에 있어서 구성한 Y분 나무 중, 리프를 제외한 모든 노드에 대해서 서브그룹을 구성하는 것이 가능하게 되기 때문에, 리프를 제외한 모든 노드 수인 N개의 값이 필요하다.

<321> 또, 기반기술에서는, 계약자(i)가 소속하는 서브그룹은, 이하의 식에서 표시되는 S_a하나뿐이다.

수학식 27

$$S_a(a = \left\lceil \frac{i}{B} \right\rceil)$$

<322>

<323> 그 때문에, 센터는, 계약자(i)에 대해서, 개인 비밀키

수학식 28

$$d_i = g_b^{\gamma_a} = v_a^{\alpha^b} \in G$$

<324>

<325> 를 비밀리에 배포하지만, 본 실시형태에서는, 스텝(S105)에 있어서 논리목을 구성한 후, 스텝(S109)에 있어서, 논리목의 각 노드를, 서브그룹의 재구성에 이용하는 것이 가능하기 때문에, 계약자(i)는, 자신에게 할당된 리프에서 루트에 이르는 모든 노드에 의해서 구성되는 복수의 서브그룹에 소속해 둘 필요가 있다.

<326> 따라서, 본 실시형태에 있어서의 스텝(S115)에서는, 계약자(i)에 대해서, 복수의 개인 비밀키를 보관 유지할 필요가 있다. 이와 같이, 키생성국면에 있어서, 본 실시형태에서는 논리목을 구성하고 있기 때문에, 필요하게 되는 파라미터가, 기반기술에 있어서의 것보다 약간 증가하고 있다. 그렇지만, 배제되는 계약자가 존재하지 않는, 또는 적은 경우에 있어서, 다음에 나타내는 암호화국면으로 생성되는 헤더의 헤더 사이즈를, 기반기술보다 삭감하는 것이 가능해진다.

<327> <암호화국면의 차이점>

<328> 다음에, 암호화국면에 관하여 설명한다. 기반기술에서는, 스텝(S31)에 있어서 세션 키를 생성하고, 그 후, 스텝(S33)에 있어서, 서브그룹마다 배제되지 않는 계약자를 선정하고, 그러한 계약자에게 할당된 서브그룹에 있어서의 계약자 인덱스의 집합 Sl(l=1, …, A)를 결정하고 있다. 그 후, 스텝(S35)에 있어서, 각 서브그룹에 있어서의 배제되어 있지 않은 계약자만이 세션 키를 취득 가능한 헤더 요소를 계산하여, 헤더를 구성하고 있다. 따라서, 서브그룹에 소속하는 계약자가 전원 배제되지 않는 한, 모든 서브그룹에 대응하는 헤더 요소를 계산할 필요가 있다. 그 때문에, 헤더 사이즈는, 배제되는 계약자수(r)의 대소에 관계없이, 항상 일정하게 된다.

<329> 이것에 대해서 본 실시형태에서는, 스텝(S301)에 있어서, 배제되는 계약자에게 할당된 리프에서 루트에 이르는 모든 노드를 마크하고, 배제되어 있지 않은 계약자가, 헤더(h)로부터 자신에게 할당된 헤더 요소를 특정하기 위한, 노드 인덱스의 집합을 S로 하고 있다. 그 후, 스텝(S303)에 있어서, 기반기술과 같은 수법에 따라 세션 키(s)를 생성하고, 스텝(S305)으로부터 스텝(S325)에 있어서, 마크되어 있지 않은 노드에 할당되어 있는 계약자만이, 세션 키(s)를 취득하는 것이 가능한 헤더 요소를 계산하여, 헤더(h)를 구성하고 있다.

<330> 보다 상세하게는, 본 실시형태의 스텝(S317)에 있어서, Layer x에 소속하는 노드 중, 마크되어 있지 않은 노드에 대한 헤더 요소를 작성하고 있다. 이것은, 기반기술에 있어서의 스텝(S35)의 동작과 같은 동작이다. 다만, 기반기술에서는, 벌써 서브그룹이 A개 존재하고 있기 때문에, 스텝(S35)에 있어서 A개의 헤더 요소를 생성할 필요가 있는데 비해, 본 실시형태에서는, 스텝(S317)에 있어서, 어느 노드의 자식 노드 집합에 대해서만 실행하고 있고, 스텝(S307)으로부터 스텝(S323)에 있어서, 이 처리를 반복하고 있다.

<331> 여기서, 스텝(S315)으로부터 스텝(S319)에 있어서 나타낸 바와 같이, 한 번 헤더 요소가 생성된 노드에 대해서는, 그 노드를 정점으로 하는 부분목에 소속하는 모든 노드를 마크함으로써, 이러한 노드에 대응하는 헤더 요소를 생성할 필요가 없어진다. 이것에 의해, 패스 상에, 그 노드를 포함한 모든 배제되어 있지 않은 계약자에 대한 헤더 요소를 정리하는 것이 가능하게 된다고 하는 이점이 생긴다. 따라서, 배제되어 있는 계약자가 적은 경우에는, 보다 많은 노드를 정리하는 것이 가능해지며, 헤더 사이즈를 삭감하는 것이 가능하게 되어 있다.

<332> <복호국면의 차이점>

<333> 마지막으로, 복호국면에 관하여 기술한다. 기반기술에서는, 스텝(S53)에 있어서, 배제되어 있지 않은 계약자가, 자신이 소속하는 서브그룹에 대응하는 헤더 요소를 취득하고, 이 헤더 요소와 공개키 및 개인 비밀키를 이용하여, 세션 키를 도출하고 있다. 이것에 대해서 본 실시형태에서는, 스텝(S503)에 있어서, 배제되어 있지 않은 계약자가, 자신에게 할당된 리프에서 루트에 이르는 패스 상에 존재하는 노드 중, S에 포함되는 노드의 부모 노드에 대응하는 헤더 요소를 취득하고, 이 헤더 요소와 공개키 및 개인 비밀키를 이용하여, 세션 키를 도출하고 있다.

<334> 이것은, 대응하는 헤더 요소 및 사용하는 개인 비밀키가 다를 뿐이며, 기반기술과 같은 동작이다. 다만, 기반기술의 복호국면에 있어서, 계약자가 실행할 필요가 있는 연산의 계산량은, $2PAIR+INV+(B-1-r_a)MUL$인데 비해, 본 실시형태에서는, $2PAIR+INV+(Y-1-r_a)MUL$이 된다.

<335> <헤더 사이즈 및 계산량에 관한 비교>

<336> 기반기술에서는, 계약자 집합을 B인씩 A개의 서브그룹에 분할하고, 콘텐츠 전달 시에는, 서브그룹마다 대응하는 헤더 요소를 생성하여, 모든 헤더 요소를 일괄하여 헤더로서 전달하고 있다. 따라서, 그 헤더 사이즈는 배제되는 계약자수(r)의 대소에 관계없이, 항상 A+1이 된다. 이것은, 헤더 사이즈가 일정하게 억제된다고 하는 이점을 가지는 한편, 배제되는 계약자수에 관계없이 헤더 사이즈를 삭감 불가능하다는 결점도 있다. 현실적인 콘텐츠전달시스템에서는, 전 계약자 수에 대한 배제되는 계약자수의 비율이 작은 범위에서, 효율적으로 콘텐츠를 전달 가능하다는 것이 요구되기 때문에, 안전성 및 편리성을 중시하여 기반기술의 방식을 이용했다고 해도, 콘텐츠 전달시에 있어서의 헤더 사이즈의 장황성이 커져 버린다는 문제점이 존재한다.

<337> 기반기술에 있어서 이 문제를 개선하기 위해서는, 계약자 집합의 분할수 A를 작게함으로써, 헤더 사이즈 그 자체를 작게 하는 것이 생각된다. 그러나, 이 경우에는, 분할된 서브그룹에 소속하는 계약자수인 B의 값이 커지며, 각 계약자가 실행할 필요가 있는 연산의 계산량의 값 $2PAIR+INV+(B-1-r_a)MUL$이 커져 버린다고 하는 문제점이 존재한다.

<338> 이것에 대해서 본 실시형태에서는, 기반기술 같이, 계약자 집합을 Y인씩 X개의 서브그룹에 분할하고 있다. 그러나, 또한, 약간의 파라미터를 추가함으로써, 분할한 서브그룹의 각 계약자를 리프로 하는 Y분 나무를 구성하고 있다. 이것에 의해, 기반기술에서는, 배제된 계약자가 존재하는지에 관계없이, 헤더 사이즈가 A+1이 되어 있는 것을, 배제된 계약자가 존재하지 않는 서브그룹에 소속하는 각 계약자는, 루트를 최상위로 한 경우, 보다 상위의 Layer의 멤버로서 취급하는 것이 가능하게 된다. 그 때문에, 복수의 서브그룹을 하나의 서브그룹으로서 취급하는 것이 가능해지며, 헤더 사이즈를 삭감하는 것을 가능하게 하고 있다. 또, 각 계약자가 실행할 필요가 있는 연산의 계산량은, 상기와 같이 $2PAIR+INV+(Y-1-r_a)MUL$이 되지만, Y는 B이하라고 하여 설정함으로써, 기반기술의 방식과 동등 이하에, 계산량을 삭감하는 것이 가능하게 되어 있다.

<339> 이상, 기반기술과 비교하면서 설명한 바와 같이, 본 발명은, 공개키를 이용한 콘텐츠 전달 방식의 한 방식이며, 기반기술과 비교하여, 이하의 특징을 가진다.

<340> 제 1에, 본 실시형태에서는, 기반기술의 방식으로 파라미터를 추가함으로써 논리목을 구성하고, 추가한 파라미터를, 논리목의 각 노드에 할당하고 있다.

<341> 제 2에, 센터인 키생성장치는, 각 계약자에 대해서, 논리목에 할당된 파라미터에 관련하는 정보를 추가의 개인 비밀키로서 미리 배포해 둔다.

<342> 제 3에, 암호화 콘텐츠의 전달자는, 암호화장치를 조작하여, 계약자가 배제된 경우에는, 공통키를 이용한 콘텐츠 전달 방식 같이, 노드마다의 배제를 행한 헤더(h)를 생성한다.

<343> 제 4에, 각 계약자는, 수신장치를 조작하고, 기반기술과 같은 방법에 의해, 공개키(PK), 헤더(h) 및 개인 비밀

키(d_i)로부터, 세션 키(s)를 산출한다.

<344> 제 5에, 기반기술의 방식을, 상기 제 1~제 4의 특징과 같이 하여 구성함으로써, 계약자에 있어서의 복호 시에 필요한 계산량을, 기반기술의 방식과 동등 이하로 삭감하는 것이 가능해진다.

<345> 제 6에, 기반기술의 방식을, 상기 제 1~제 4의 특징과 같이 하여 구성함으로써, 배제되는 계약자가 적은 경우에는, 기반기술보다 헤더 사이즈를 삭감하는 것이 가능해진다.

<346> 본 실시형태의 효과를 보다 상세하게 설명하기 위해, 구체적인 예로서 파라미터 n, A, B, X, Y를 작은 값으로 설정한 경우에 있어서의, 헤더 사이즈 및 복호 시에 필요한 계산량의 비교에 대해서, 도 23~도 26에 나타낸다.

<347> 기반기술에서는, 분할된 서브그룹에 포함되는 계약자수(B)의 값을, 계약자수(n)에 대해서 $B=(n)^{1/2}$로서 설정하는 것을 추천하고 있다. 이것에 대해서 본 실시형태에서는, 기반기술의 B에 대응하는 파라미터인 논리목의 분기수(Y)를, Y는 B이하라고 설정함으로써, 헤더 사이즈 및 계산량의 점으로 효율화를 도모하는 것이 가능하다.

<348> 따라서 이하에서는, 비교를 위해, 계약자수(n)를 동일로 하고, Y<B로 설정했다. 기반기술과 본 실시형태에 있어서의 헤더 사이즈 및 복호 시에 필요한 연산의 계산량 비교를, 각각 도 23 및 도 24에 나타낸다. 또, Y=B로 했을 경우의 헤더 사이즈 및 복호 시에 필요한 계산량 비교를, 각각 도 25 및 도 26에 나타낸다.

<349> 구체적인 수치로서, 도 23 및 도 24에서는, 기반기술의 방식에 있어서의 각 파라미터를, n=64, A=8, B=8로 하고, 본 실시형태에서는, n=64, X=16, Y=4로 했다. 또, 도 25 및 도 26에서는, n=64, X=8, B=Y=8로 했다. 다만, 이용하는 쌍선형군이나 그 크기에 대해서는, 간단하기 때문에 동일한 것으로 했다.

<350> (Y<B로 설정했을 경우에 대하여)

<351> 처음에, 도 23 및 도 24에 대해 설명한다. 도 23의 횡축은, 배제된 계약자수를 나타내고, 세로축은, 헤더 사이즈(헤더 요소의 총수)를 나타낸다. 또, 도 24의 횡축은, 배제된 계약자수를 나타내고, 세로축은, 복호 시에 필요한 연산의 계산량을 나타낸다. 다만, 복호 시에 필요한 연산의 계산량에 관해서, 기반기술과 본 실시형태의 차이에 영향을 주는 것은 쌍선형군(G) 상에서의 곱셈 부분에 있어서만이기 때문에, 도 24의 세로축은, 쌍선형군(G) 상에서의 곱셈 회수를 나타내는 것으로 한다. 또, 도 23에 있어서의 실선은, 기반기술 방식에 있어서의 헤더 사이즈를 나타내고, 파선은, 본 실시형태에 있어서의 헤더 사이즈를 나타내고 있다. 또, 도 24에 있어서의 실선은, 기반기술 방식에 있어서의 계산량을 나타내고, 파선은, 본 실시형태에 있어서의 계산량을 나타내고 있다.

<352> 헤더 사이즈의 비교에 관해서는, 도 23에서 분명한 바와 같이, 배제되는 계약자수(r)가 4보다 작은 경우에는, 본 실시형태와 관련되는 방식이, 기반기술의 방식에 비해 헤더 사이즈가 적어지게 되는 것을 알 수 있었다. 즉, 이 경우, 전 계약자에 대하여 약 6%정도까지의 계약자가 배제되어도, 본 실시형태와 관련되는 방식이, 효율적으로 콘텐츠를 전달 가능한 것을 나타내고 있다.

<353> 복호 시에 필요한 계산량의 비교에 관해서는, 도 24에서 분명한 바와 같이, 배제되는 계약자수(r)가 60보다 작은 경우에는, 본 실시형태와 관련되는 방식이, 기반기술의 방식보다, 계산량이 적은 것을 알았다. 이것은, 본 실시형태와 관련되는 방식의 쪽이, 효율적으로 콘텐츠를 복호 가능한 것을 나타내고 있다. 또, 배제되는 계약자수가 60을 넘었을 경우에 있어서도, 기반기술의 방식에 있어서의 계산량과 동등하다는 것을 알았다. 따라서, 상기와 같이 파라미터를 설정한 경우에 있어서는, 배제되는 계약자가 존재하지 않거나 혹은 적은 경우에 있어서, 본 실시형태와 관련되는 방식이, 기반기술과 관련되는 방식보다, 헤더 사이즈를 작게 하는 것이 가능하며, 또한, 각 계약자가 복호 시에 실행할 필요가 있는 연산의 계산량을 줄이는 것이 가능하다. 그 때문에, 본 실시형태와 관련되는 방식이, 기반기술과 관련되는 방식보다, 효율적으로 콘텐츠 전달을 실현하는 것이 가능하다고 말할 수 있다.

<354> (Y=B로 설정한 경우에 대하여)

<355> 다음에, 도 25 및 도 26에 대하여 설명한다. 도 25 및 도 26은, 상술한 도 23 및 도 24에 대해서 X 및 Y의 값을 변경했을 뿐이므로, 그 횡축 및 세로축 및 실선, 파선이 나타내는 것은, 도 23 및 도 24의 그것과 동일하다.

<356> X=A=8, Y=B=8로 한 경우의 헤더 사이즈의 비교에 관해서는, 도 25에서 분명한 바와 같이, 배제되는 계약자수(r)가 7보다 작은 경우에는, 본 실시형태와 관련되는 방식이, 기반기술과 관련되는 방식보다, 헤더 사이즈가 적어지게 되는 것을 알 수 있었다. 즉, 이 경우, 전 계약자에 대해서 약 9%정도까지의 계약자가 배제되어도, 본 실시형태와 관련되는 방식이, 효율적으로 콘텐츠를 전달 가능한 것을 나타내고 있다. 배제되는 계약자수가

7 이상으로 된 경우에 있어서도, 기반기술의 방식과 동등의 헤더 사이즈로 되어 있고, 배제되는 계약자수에 관계없이, 헤더 사이즈를 기반기술의 방식 이하로 삭감하는 것이 가능하게 되어 있다.

<357> 또, 복호 시에 필요한 계산량의 비교에 관해서는, 도 26에서 분명한 바와 같이, 배제되는 계약자수(r)에 관계없이, 기반기술의 방식과 동등하다는 것을 알았다. 따라서, 각 파라미터를 X=A=8, Y=B=8로 설정한 경우에는, 배제되는 계약자가 존재하지 않거나 혹은 적은 경우에 있어서, 헤더 사이즈를 삭감하는 것이 가능하다는 것과 동시에, 복호 시의 계산량은, 기반기술의 방식과 동등하게 끝나는 것을 알 수 있었다.

<358> 이상에서, 본 실시형태를 적용함으로써, 기반기술과 같은 편리성, 안전성을 유지한 채로, 보다 현실적인 콘텐츠 전달시스템에 있어서, 기반기술보다 효율적인 콘텐츠 전달을 실현하는 것이 가능하게 되는 것을 알 수 있다.

<359> 이상 설명한 바와 같이, 본 발명은, 공개키를 이용하여 콘텐츠를 안전하게 전달하는 콘텐츠전달시스템에 있어서, 종래의 방식보다, 전달되는 데이터량의 삭감 및 복호 시에 필요한 계산량의 삭감을 실현하는 방법이다. 본 발명의 실시에 의해, 종래의 공개키를 이용한 콘텐츠 전달법과 비교하여, 보다 효율적인 콘텐츠 전달이 실현 가능해진다.

<360> 이상, 첨부 도면을 참조하면서 본 발명의 매우 적합한 실시형태에 대하여 설명했지만, 본 발명은 이러한 예로 한정되지 않는 것은 말할 필요도 없다. 당업자라면, 특허청구의 범위에 기재된 범주 내에 있어서, 각종의 변경 예 또는 수정 예에 상도 할 수 있는 것은 분명하며, 그것들에 대해서도 당연하게 본 발명의 기술적 범위에 속하는 것으로 이해된다.

<361> 예를 들면, 상기의 나무구조 구성부(231)는, 위에서 아래로 가지가 퍼진 나무구조를 상정하고 있지만, 반드시 이것으로 한정되지 않고, 아래에서 위, 왼쪽에서 오른쪽, 또는 오른쪽에서 왼쪽을 향하여 가지가 퍼진 나무구조를 가지고있어도 좋다.

<362> 또, 본 명세서의 각 흐름도에 있어서의 각 스텝은, 반드시 흐름도로서 기재된 순서에 따라서 시계열로 처리할 필요는 없고, 병렬적 혹은 개별적으로 실행되는 처리(예를 들면, 병렬처리 혹은 오브젝트에 의한 처리)도 포함한다고 해도 좋다.

산업상 이용 가능성

<363> 본 발명에 의하면, 배제되는 계약자수가 적은 경우에도, 헤더 사이즈를 삭감하는 것이 가능하다.

도면의 간단한 설명

<38> 도 1은, 본 발명의 매우 적합한 실시형태와 관련되는 암호키 생성시스템을 설명하기 위한 설명도이다.

<39> 도 2는, 동 실시형태와 관련되는 키생성장치의 하드웨어 구성을 설명하기 위한 블럭도이다.

<40> 도 3은, 본 발명의 기반기술의 기본 방식과 관련되는 키생성의 개략을 설명하기 위한 설명도이다.

<41> 도 4는, 본 발명의 기반기술의 일반화 방식과 관련되는 키생성의 개략을 설명하기 위한 흐름도이다.

<42> 도 5는, 본 발명의 기반기술의 일반화 방식과 관련되는 키생성 국면을 설명하기 위한 흐름도이다.

<43> 도 6은, 본 발명의 기반기술의 일반화 방식과 관련되는 암호화의 개략을 설명하기 위한 설명도이다.

<44> 도 7은, 본 발명의 기반기술의 일반화 방식과 관련되는 암호화국면을 설명하기 위한 흐름도이다.

<45> 도 8은, 본 발명의 기반기술의 일반화 방식과 관련되는 복호국면을 설명하기 위한 흐름도이다.

<46> 도 9는, 본 발명의 매우 적합한 실시형태와 관련되는 키생성장치의 구성을 설명하기 위한 블럭도이다.

<47> 도 10은, 동 실시형태와 관련되는 암호화장치의 구성을 설명하기 위한 블럭도이다.

<48> 도 11은, 동 실시형태와 관련되는 수신장치의 구성을 설명하기 위한 블럭도이다.

<49> 도 12는, 동 실시형태와 관련되는 논리목(論理木)의 구체적인 예를 설명하기 위한 설명도이다.

<50> 도 13은, 동 실시형태와 관련되는 키생성의 개략을 설명하기 위한 설명도이다.

<51> 도 14는, 동 실시형태와 관련되는 키생성 국면을 설명하기 위한 흐름도이다.

<52> 도 15는, 동 실시형태와 관련되는 키생성의 구체적인 예를 설명하기 위한 설명도이다.

<53> 도 16은, 동 실시형태와 관련되는 암호화의 개략을 설명하기 위한 설명도이다.

<54> 도 17은, 동 실시형태와 관련되는 암호화국면을 설명하기 위한 흐름도이다.

<55> 도 18은, 동 실시형태와 관련되는 암호화의 구체적인 예를 설명하기 위한 설명도이다.

<56> 도 19는, 동 실시형태와 관련되는 암호화의 구체적인 예를 설명하기 위한 설명도이다.

<57> 도 20은, 동 실시형태와 관련되는 암호화의 구체적인 예를 설명하기 위한 설명도이다.

<58> 도 21은, 동 실시형태와 관련되는 복호국면을 설명하기 위한 흐름도이다.

<59> 도 22는, 동 실시형태와 관련되는 복호의 구체적인 예를 설명하기 위한 설명도이다.

<60> 도 23은, 계약자에게 전달되는 헤더의 헤더 사이즈를 비교한 그래프도이다.

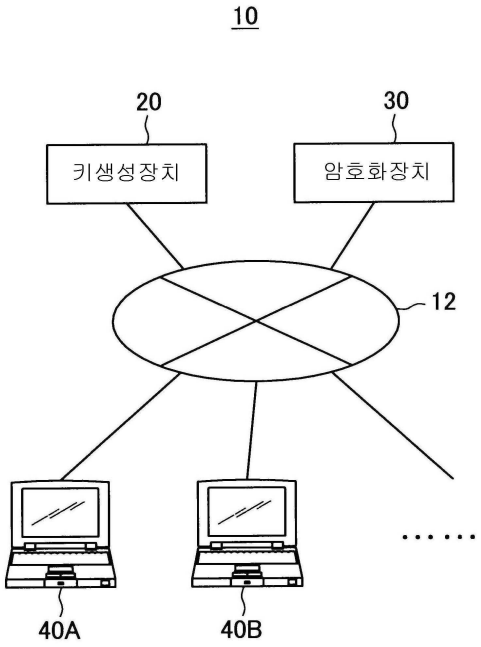
<61> 도 24는, 쌍선형군 상에서의 곱셈의 회수를 비교한 그래프도이다.

<62> 도 25는, 계약자에게 전달되는 헤더의 헤더 사이즈를 비교한 그래프도이다.

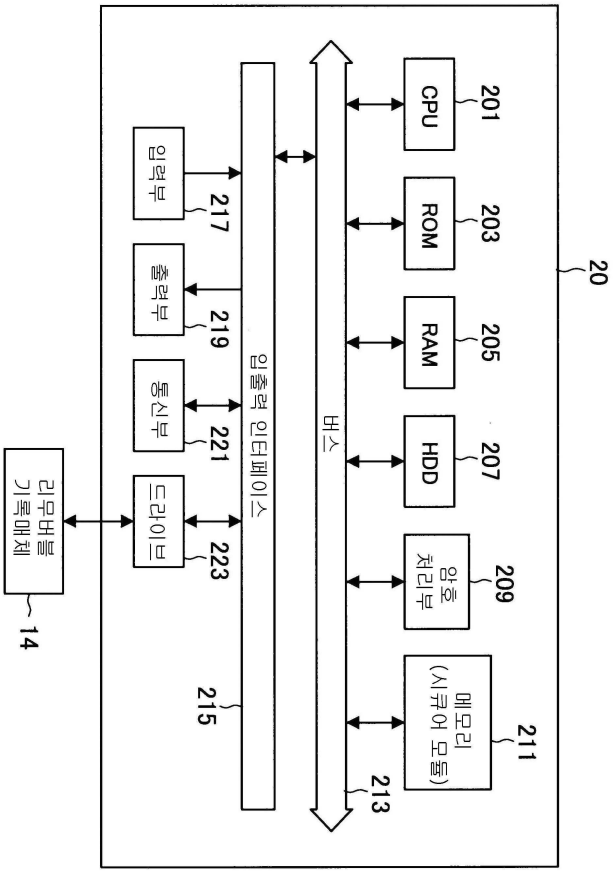
<63> 도 26은, 쌍선형군 상에서의 곱셈의 회수를 비교한 그래프도이다.

도면

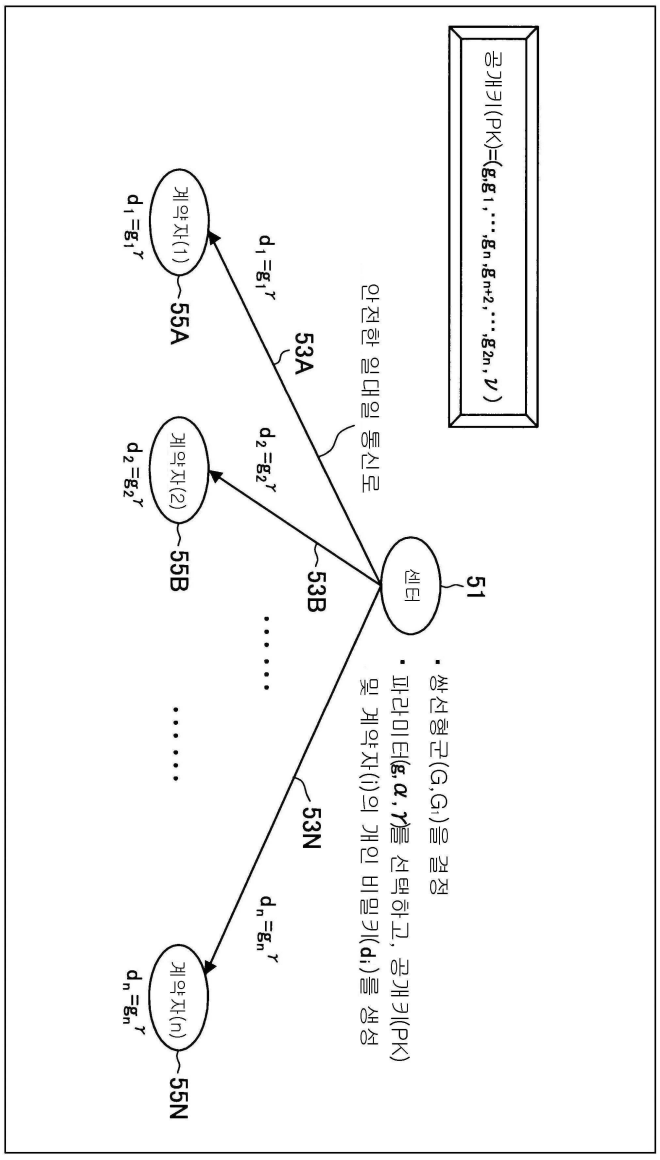
도면1



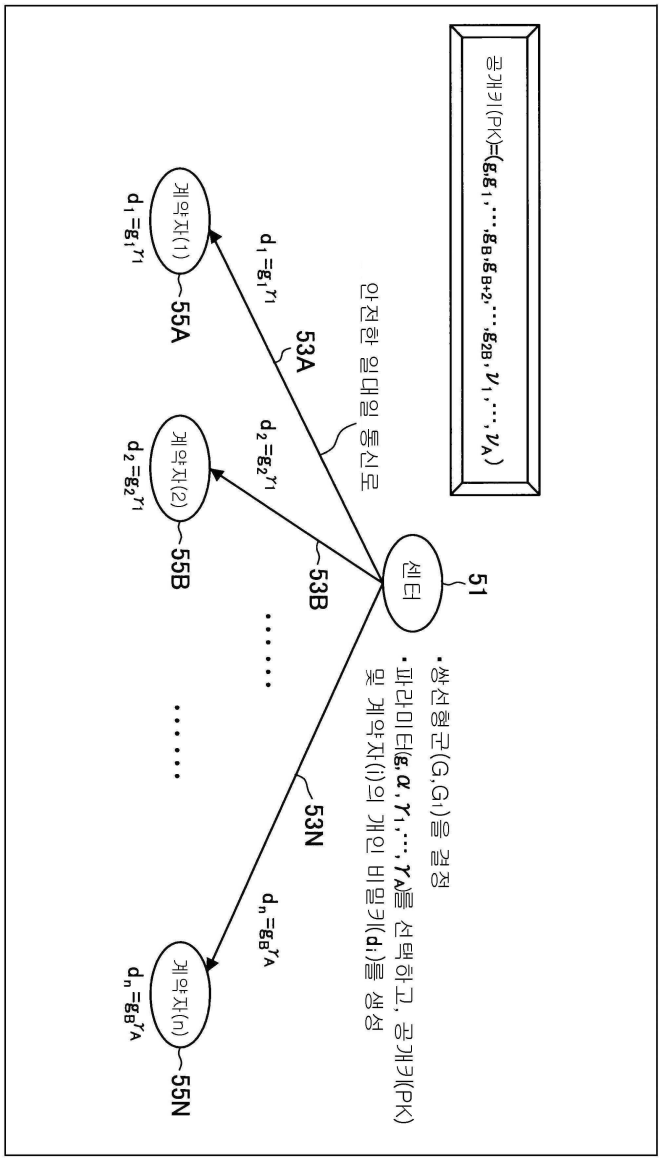
도면2


20
CPU
201
ROM
203
RAM
205
HDD
207
암호 처리부
209
메모리 (시큐어 모듈)
211
213
버스
입출력 인터페이스
215
입력부
217
출력부
219
통신부
221
드라이브
223
리무버블 기록매체
14

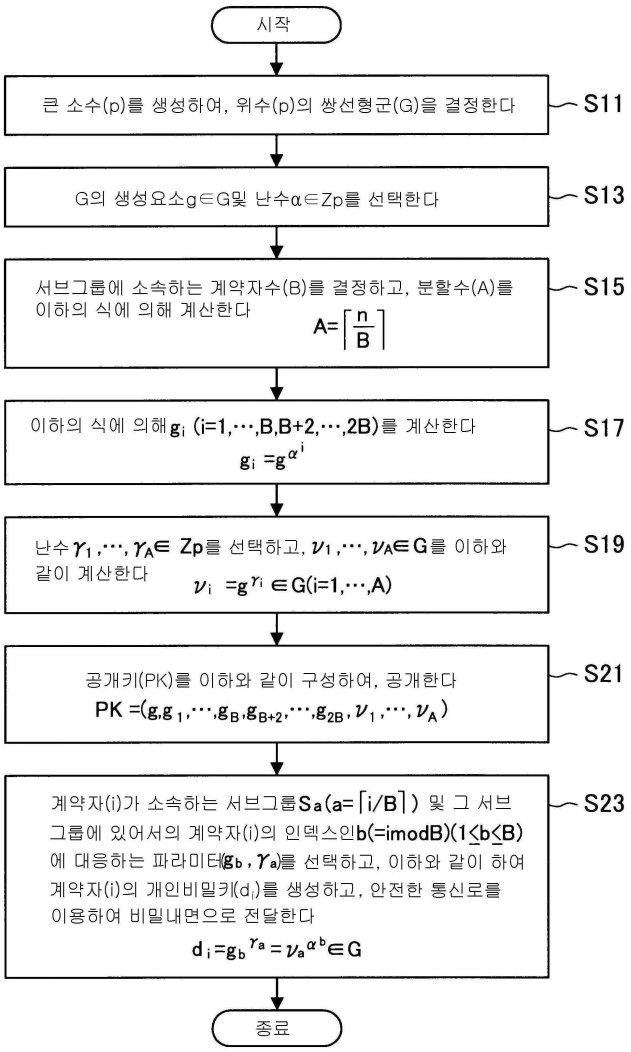
도면3


공개키(PK)=(g, g1, ..., gn, gn+2, ..., g2n, v)
센터
51
• 쌍선형군(G, G1)을 결정
• 파라미터(g, α, γ)를 선택하고, 공개키(PK) 및 계약자(i)의 개인 비밀키(di)를 생성
안전한 일대일 통신로
53A
53B
53N
d1=g1^γ
d2=g2^γ
dn=gn^γ
계약자(1)
d1=g1^γ
55A
계약자(2)
d2=g2^γ
55B
계약자(n)
dn=gn^γ
55N

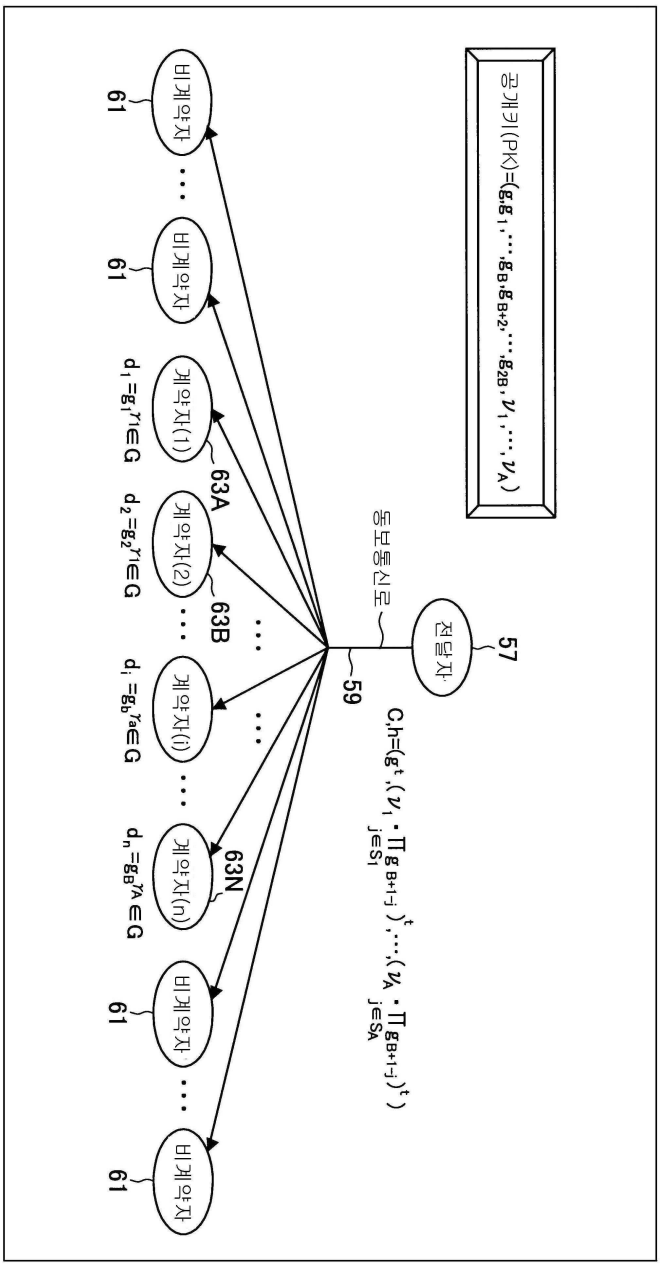
도면4


공개키(PK)=(g,g1,…,gB,gB+2,…,g2B,γ1,…,γA)
센터
51
•쌍선형군(G,G1)을 결정
•파라미터(g,α,γ1,…,γA)를 선택하고, 공개키(PK) 및 계약자(i)의 개인 비밀키(di)를 생성
안전한 일대일 통신로
53A
53B
53N
d1=g1γ1
d2=g2γ1
dn=gBγA
계약자(1)
계약자(2)
계약자(n)
55A
55B
55N

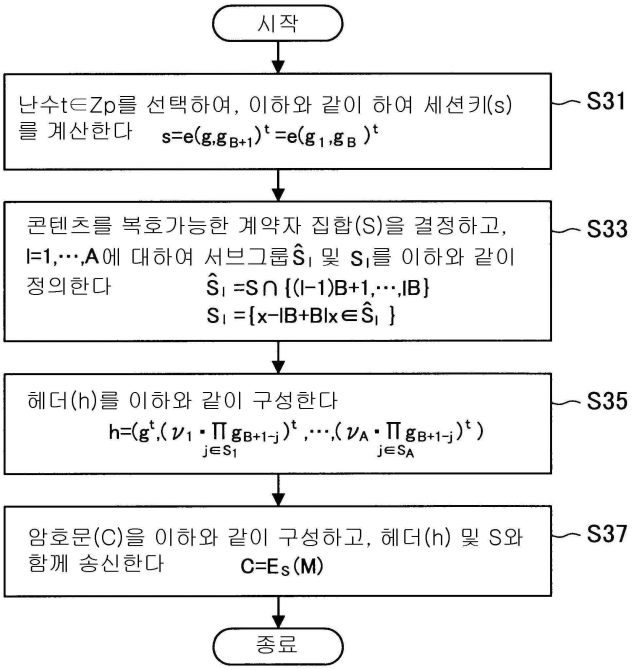
도면5


시작
큰 소수(p)를 생성하여, 위수(p)의 쌍선형군(G)을 결정한다
S11
G의 생성요소g∈G및 난수α∈Zp를 선택한다
S13
서브그룹에 소속하는 계약자수(B)를 결정하고, 분할수(A)를 이하의 식에 의해 계산한다
$A=\left\lceil \frac{n}{B} \right\rceil$
S15
이하의 식에 의해g_i (i=1,⋯,B,B+2,⋯,2B)를 계산한다
$g_i = g^{\alpha^i}$
S17
난수$\gamma_1,\cdots,\gamma_A \in Zp$를 선택하고, $\nu_1,\cdots,\nu_A \in G$를 이하와 같이 계산한다
$\nu_i = g^{\gamma_i} \in G(i=1,\cdots,A)$
S19
공개키(PK)를 이하와 같이 구성하여, 공개한다
$PK=(g,g_1,\cdots,g_B,g_{B+2},\cdots,g_{2B},\nu_1,\cdots,\nu_A)$
S21
계약자(i)가 소속하는 서브그룹$S_a(a=\lceil i/B \rceil)$ 및 그 서브그룹에 있어서의 계약자(i)의 인덱스인b(=imodB)(1≤b≤B)에 대응하는 파라미터(g_b, γ_a)를 선택하고, 이하와 같이 하여 계약자(i)의 개인비밀키(d_i)를 생성하고, 안전한 통신로를 이용하여 비밀내면으로 전달한다
$d_i = g_b^{\gamma_a} = \nu_a^{\alpha^b} \in G$
S23
종료

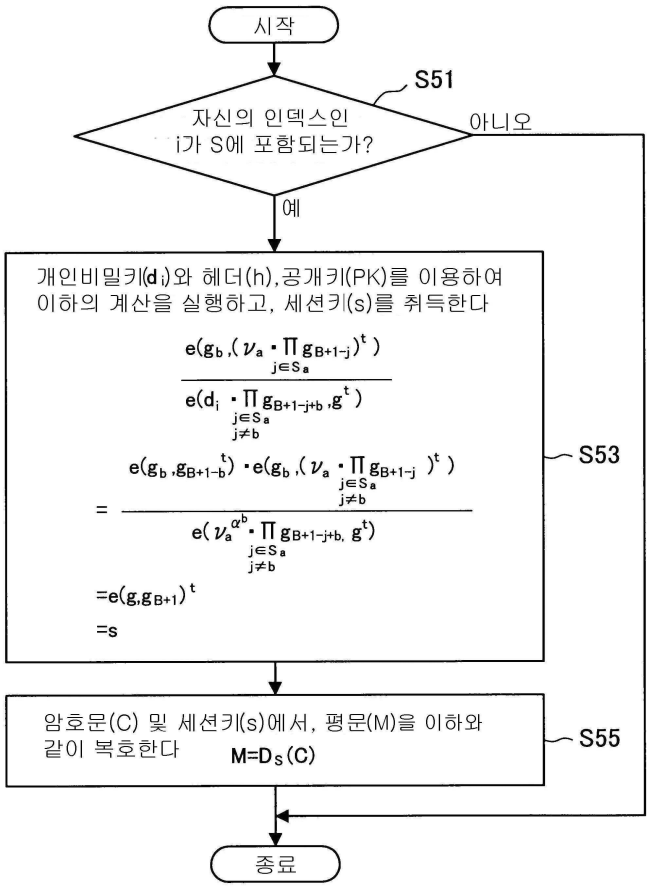
도면6


공개키(PK)=(g,g1,…,gB,gB+2,…,g2B,ν1,…,νA)
57
전달자
동보통신로
59
C,h=(g^t,(ν1·∏gB+1-j)^t,…,(νA·∏gB+1-j)^t)
j∈S1
j∈SA
63A
63B
63N
계약자(1)
계약자(2)
계약자(i)
계약자(n)
d1=g1^γ1∈G
d2=g2^γ1∈G
di=gb^γa∈G
dn=gB^γA∈G
비계약자
61

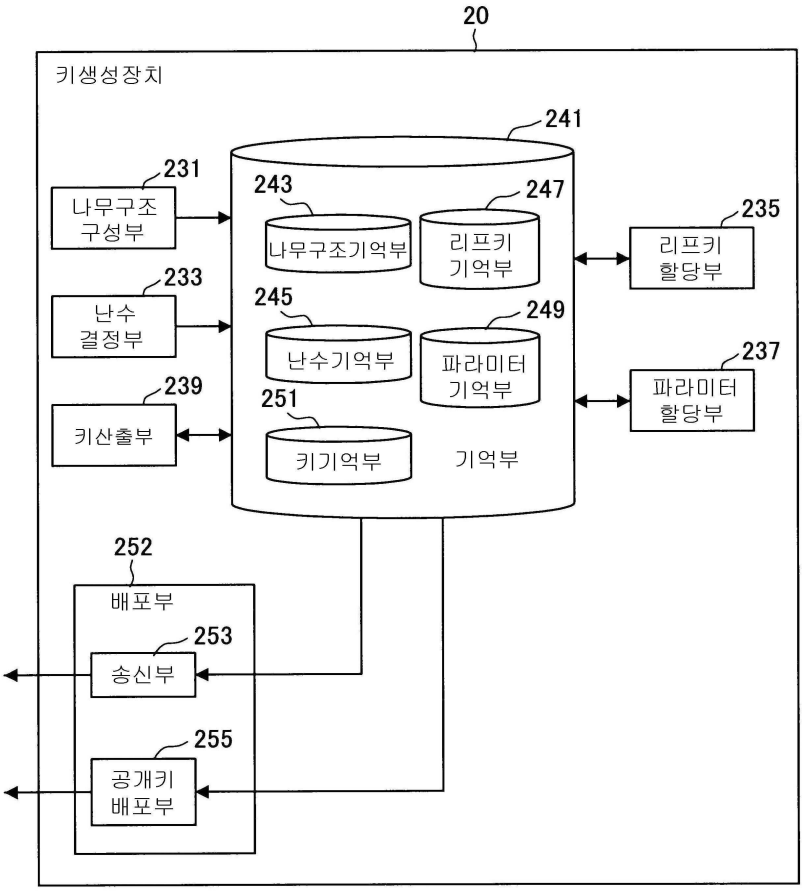
도면7


시작
난수t∈Zp를 선택하여, 이하와 같이 하여 세션키(s)를 계산한다 $s=e(g,g_{B+1})^t=e(g_1,g_B)^t$
S31
콘텐츠를 복호가능한 계약자 집합(S)을 결정하고, l=1,…,A에 대하여 서브그룹 $\hat{S}_l$ 및 S_l를 이하와 같이 정의한다 $\hat{S}_l=S\cap\{(l-1)B+1,\cdots,lB\}$ $S_l=\{x-lB+B|x\in\hat{S}_l\}$
S33
헤더(h)를 이하와 같이 구성한다 $h=(g^t,(\nu_1\cdot\prod_{j\in S_1}g_{B+1-j})^t,\cdots,(\nu_A\cdot\prod_{j\in S_A}g_{B+1-j})^t)$
S35
암호문(C)을 이하와 같이 구성하고, 헤더(h) 및 S와 함께 송신한다 $C=E_S(M)$
S37
종료

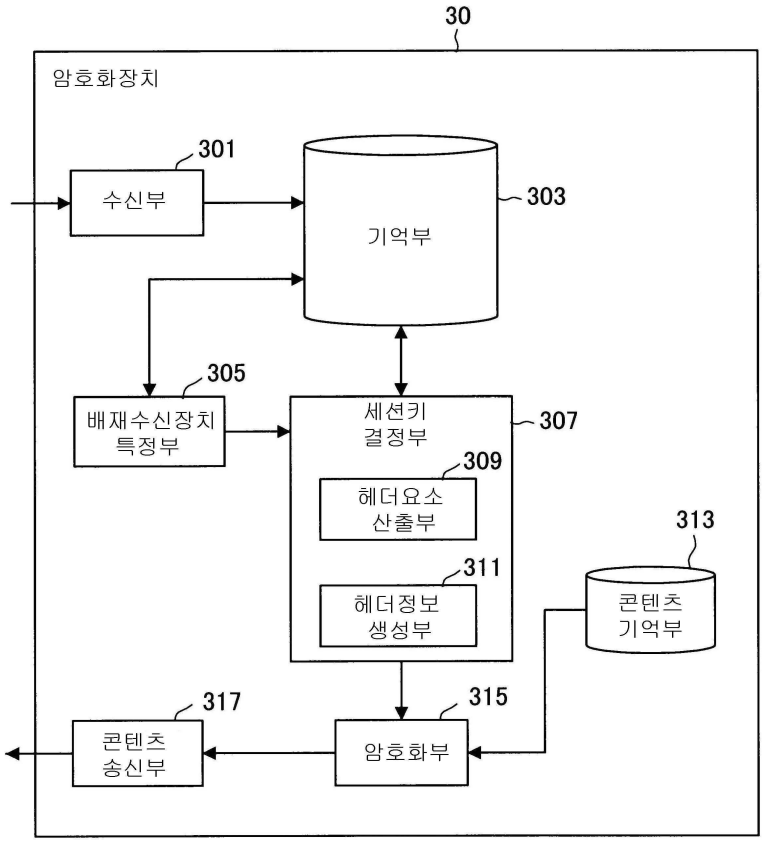
도면8


시작
S51
자신의 인덱스인
i가 S에 포함되는가?
아니오
예
개인비밀키(d_i)와 헤더(h),공개키(PK)를 이용하여
이하의 계산을 실행하고, 세션키(s)를 취득한다
S53
암호문(C) 및 세션키(s)에서, 평문(M)을 이하와
같이 복호한다
M=D_S(C)
S55
종료

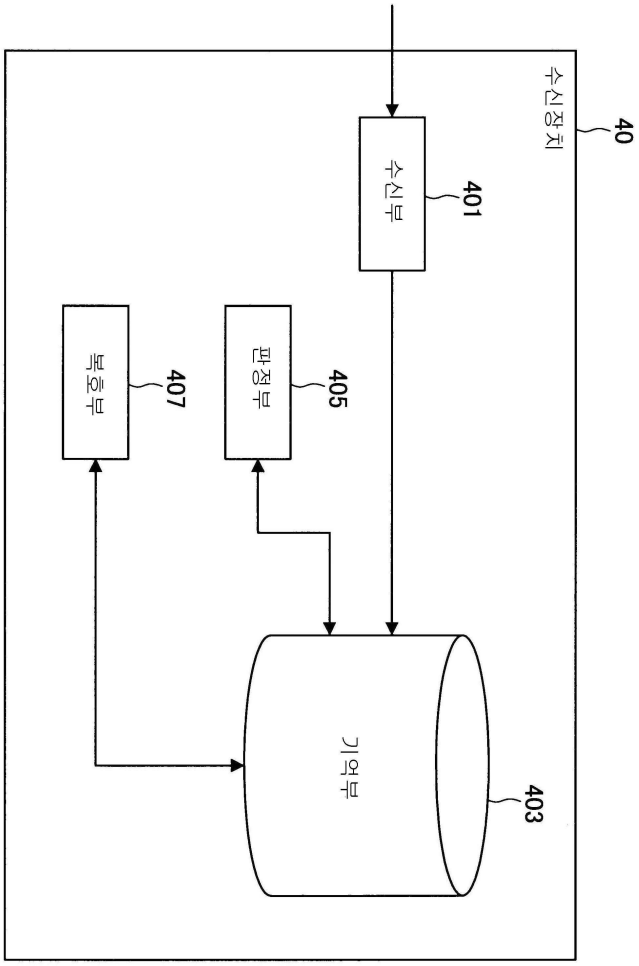
도면9


20
키생성장치
241
231
나무구조
구성부
243
247
나무구조기억부
리프키
기억부
235
리프키
할당부
233
난수
결정부
245
249
난수기억부
파라미터
기억부
237
파라미터
할당부
239
키산출부
251
키기억부
기억부
252
배포부
253
송신부
255
공개키
배포부

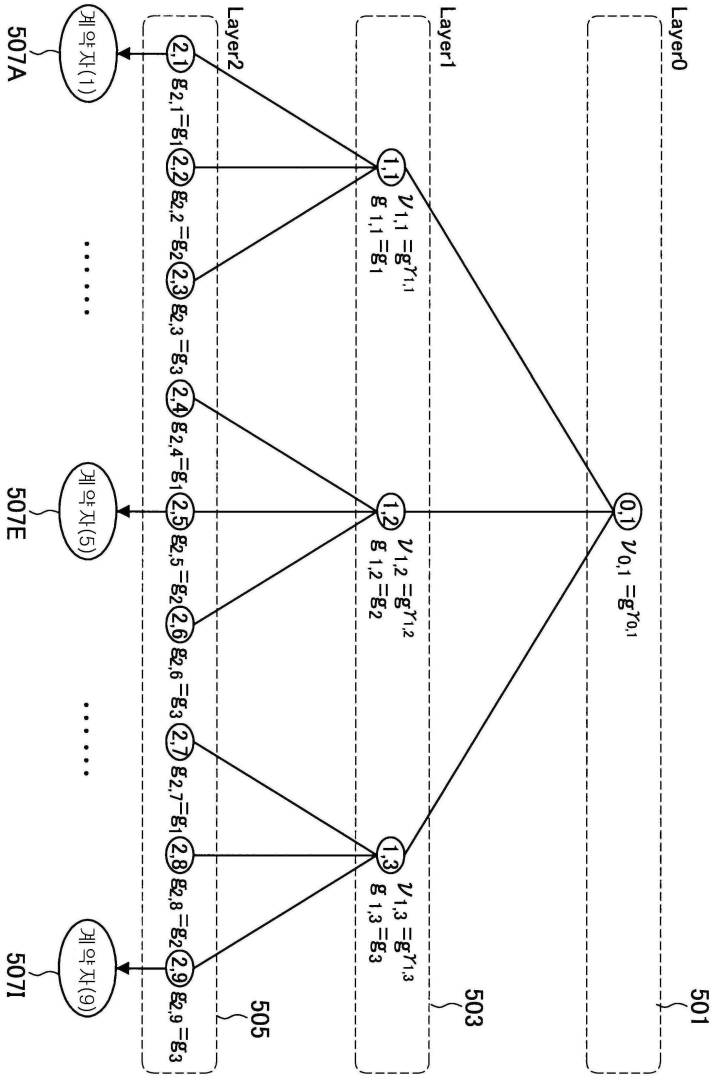
도면10


30
암호화장치
301
수신부
303
기억부
305
배재수신장치
특정부
307
세션키
결정부
309
헤더요소
산출부
311
헤더정보
생성부
313
콘텐츠
기억부
315
암호화부
317
콘텐츠
송신부

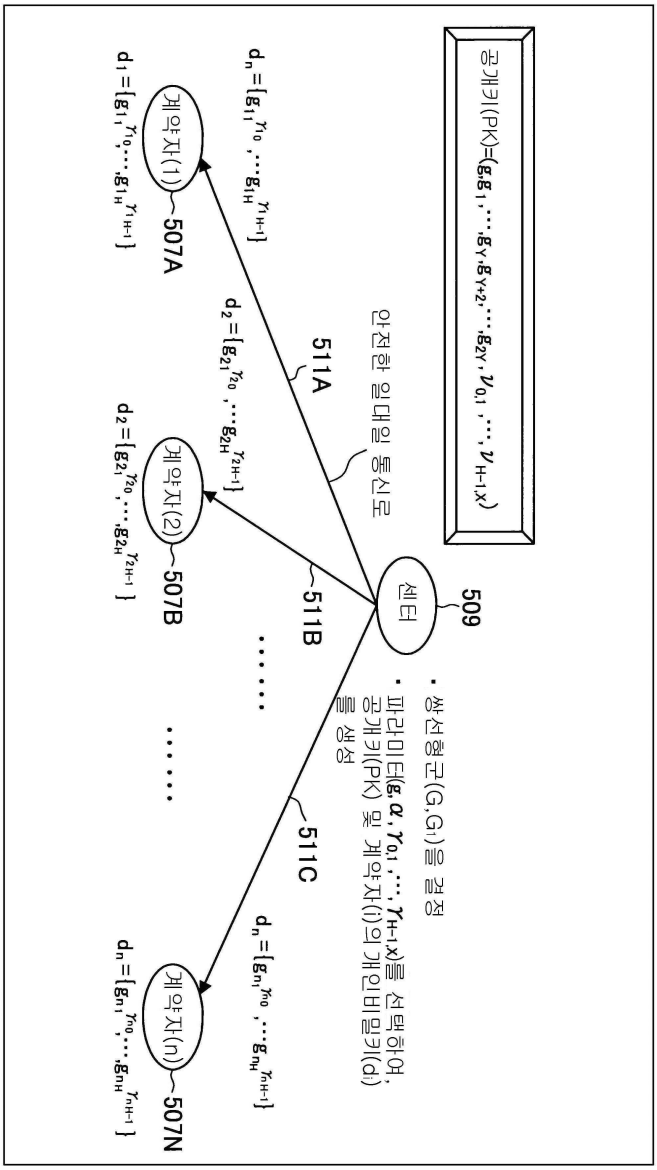
도면11



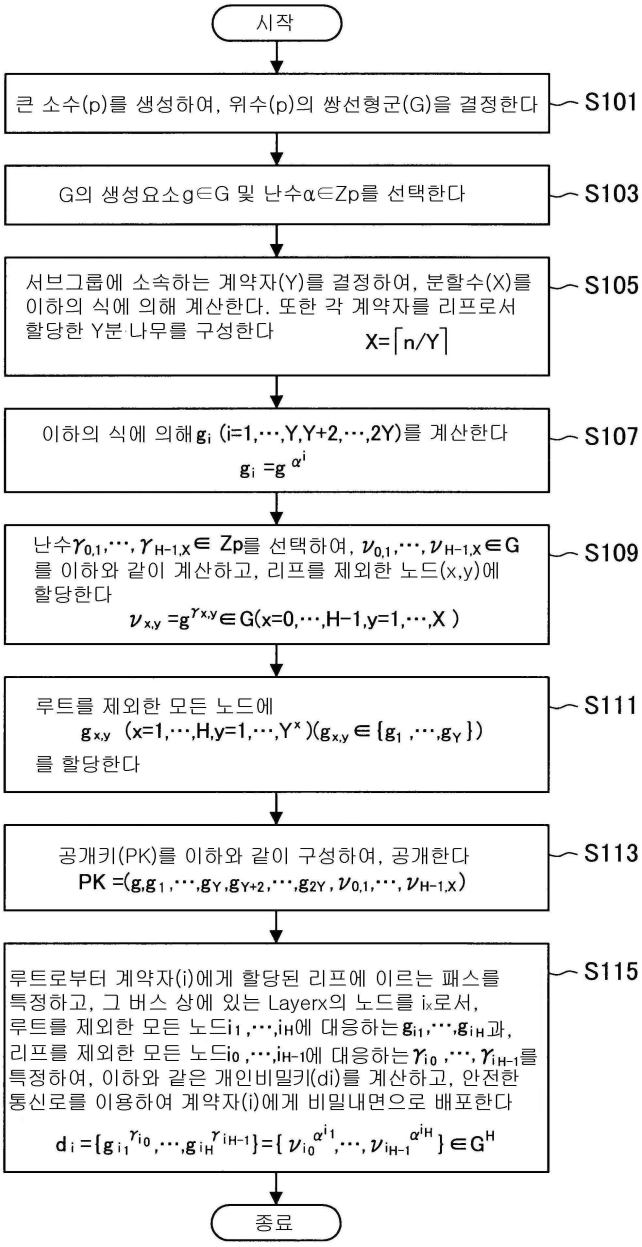
도면12


Layer0
Layer1
Layer2
501
503
505
507A
507E
507I
계약자(1)
계약자(5)
계약자(9)

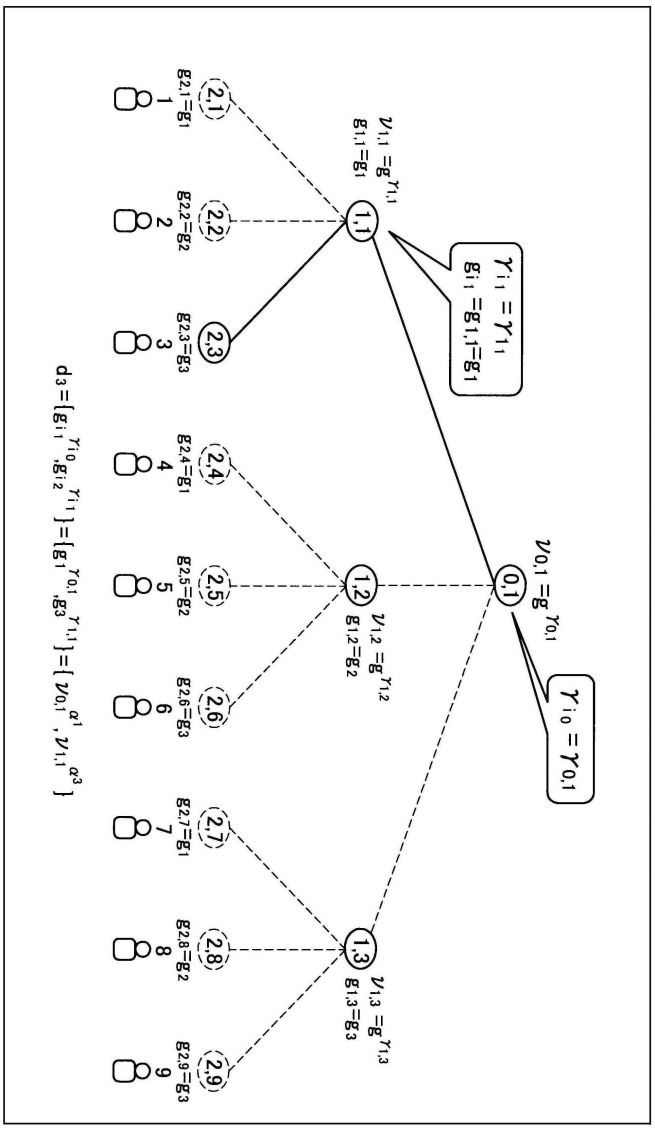
도면13


공개키(PK)=(g, g1, ..., gY, gY+2, ..., g2Y, γ0,1, ..., γH-1,X)
센터
509
• 쌍선형군(G,G1)을 결정
• 파라미터(g, α, γ0,1, ..., γH-1,X)를 선택하여, 공개키(PK) 및 계약자(i)의 개인비밀키(di)를 생성
안전한 일대일 통신로
511A
511B
511C
계약자(1)
507A
계약자(2)
507B
계약자(n)
507N
d1=[g1,1, γ1,0, ..., g1,H, γ1,H-1]
dn=[g1, γ1,0, ..., g1,H, γ1,H-1]
d2=[g2,1, γ2,0, ..., g2,H, γ2,H-1]
dn=[gn,1, γn,0, ..., gn,H, γn,H-1]
d2=[g2,1, γ2,0, ..., g2,H, γ2,H-1]
dn=[gn,1, γn,0, ..., gn,H, γn,H-1]

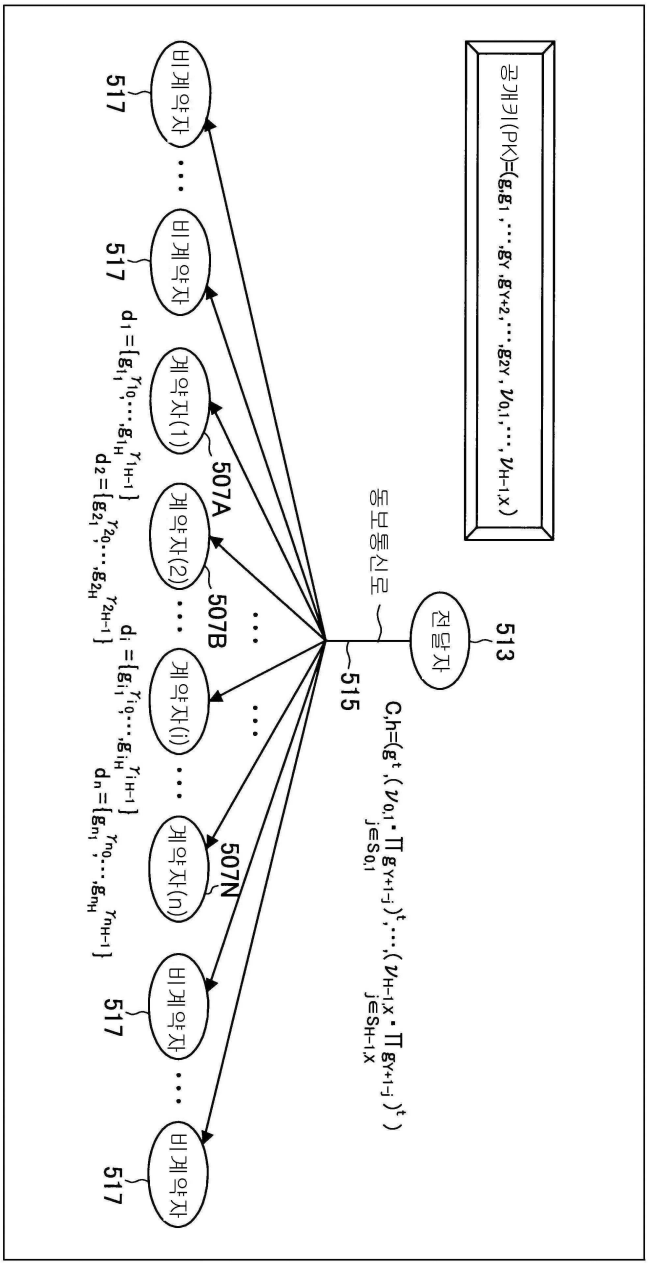
도면14


시작
큰 소수(p)를 생성하여, 위수(p)의 쌍선형군(G)을 결정한다
S101
G의 생성요소g∈G 및 난수α∈Zp를 선택한다
S103
서브그룹에 소속하는 계약자(Y)를 결정하여, 분할수(X)를 이하의 식에 의해 계산한다. 또한 각 계약자를 리프로서 할당한 Y분 나무를 구성한다
$X=\lceil n/Y \rceil$
S105
이하의 식에 의해g_i (i=1,⋯,Y,Y+2,⋯,2Y)를 계산한다
$g_i = g^{\alpha^i}$
S107
난수$\gamma_{0,1},\cdots,\gamma_{H-1,X}\in Zp$를 선택하여, $\nu_{0,1},\cdots,\nu_{H-1,X}\in G$를 이하와 같이 계산하고, 리프를 제외한 노드(x,y)에 할당한다
$\nu_{x,y}=g^{\gamma_{x,y}}\in G(x=0,\cdots,H-1,y=1,\cdots,X)$
S109
루트를 제외한 모든 노드에
$g_{x,y}$ $(x=1,\cdots,H,y=1,\cdots,Y^x)(g_{x,y}\in\{g_1,\cdots,g_Y\})$
를 할당한다
S111
공개키(PK)를 이하와 같이 구성하여, 공개한다
$PK=(g,g_1,\cdots,g_Y,g_{Y+2},\cdots,g_{2Y},\nu_{0,1},\cdots,\nu_{H-1,X})$
S113
루트로부터 계약자(i)에게 할당된 리프에 이르는 패스를 특정하고, 그 버스 상에 있는 Layerx의 노드를 i_x로서, 루트를 제외한 모든 노드$i_1,\cdots,i_H$에 대응하는$g_{i1},\cdots,g_{iH}$과, 리프를 제외한 모든 노드$i_0,\cdots,i_{H-1}$에 대응하는$\gamma_{i0},\cdots,\gamma_{iH-1}$를 특정하여, 이하와 같은 개인비밀키(di)를 계산하고, 안전한 통신로를 이용하여 계약자(i)에게 비밀내면으로 배포한다
$d_i=\{g_{i1}^{\gamma_{i0}},\cdots,g_{iH}^{\gamma_{iH-1}}\}=\{\nu_{i0}^{\alpha^{i1}},\cdots,\nu_{iH-1}^{\alpha^{iH}}\}\in G^H$
S115
종료

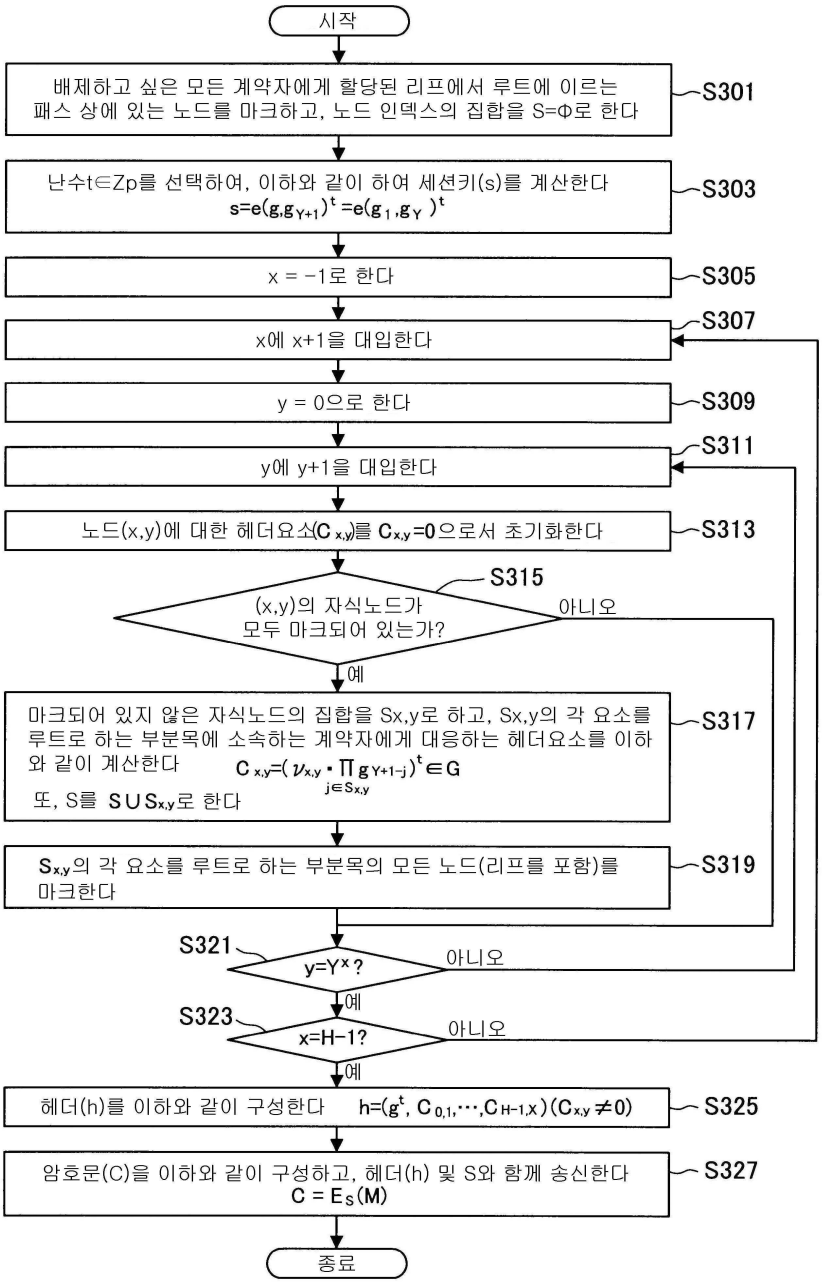
도면15


(0,1)
(1,1)
(1,2)
(1,3)
(2,1)
(2,2)
(2,3)
(2,4)
(2,5)
(2,6)
(2,7)
(2,8)
(2,9)
$\gamma_{i1} = \gamma_{11}$
$g_{i1} = g_{1,i} = g_1$
$\gamma_{i0} = \gamma_{0,1}$
$v_{0,1} = g^{\gamma_{0,1}}$
$v_{1,1} = g^{\gamma_{1,1}}$
$g_{1,1} = g_1$
$v_{1,2} = g^{\gamma_{1,2}}$
$g_{1,2} = g_2$
$v_{1,3} = g^{\gamma_{1,3}}$
$g_{1,3} = g_3$
$g_{2,1} = g_1$
$g_{2,2} = g_2$
$g_{2,3} = g_3$
$g_{2,4} = g_1$
$g_{2,5} = g_2$
$g_{2,6} = g_3$
$g_{2,7} = g_1$
$g_{2,8} = g_2$
$g_{2,9} = g_3$
1
2
3
4
5
6
7
8
9
$d_3 = [g_{i_1}^{\gamma_{i_0}}, g_{i_2}^{\gamma_{i_1}}] = [g_1^{\gamma_{0,1}}, g_3^{\gamma_{1,1}}] = [v_{0,1}^{\alpha^1}, v_{1,1}^{\alpha^3}]$

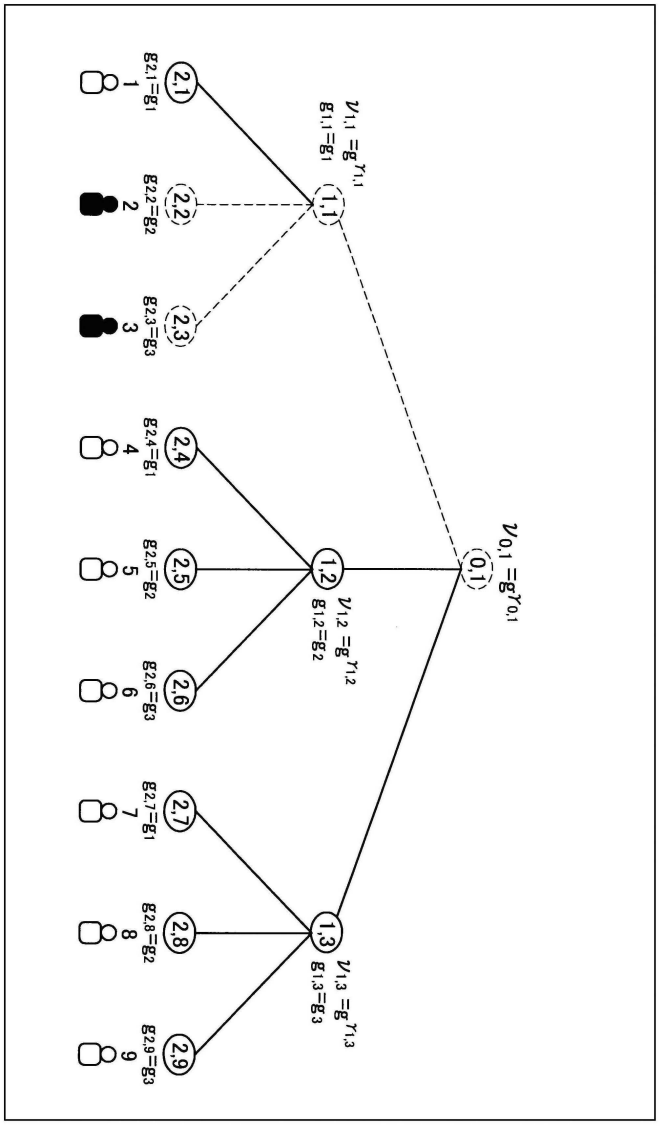
도면16


공개키(PK)=(g,g1,…,gY,gY+2,…,g2Y,ν0,1,…,νH-1,X)
513
전달자
동보통신로
515
C,h=(g^t,(ν0,1·∏gY+1-j)^t,…,(νH-1,X·∏gY+1-j)^t)
j∈S0,1
j∈SH-1,X
507A
507B
507N
계약자(1)
계약자(2)
계약자(i)
계약자(n)
비계약자
517
d1={g1^γ10,…,g1H^γ1H-1}
d2={g21^γ20,…,g2H^γ2H-1}
di={gi1^γi0,…,giH^γiH-1}
dn={gn1^γn0,…,gnH^γnH-1}

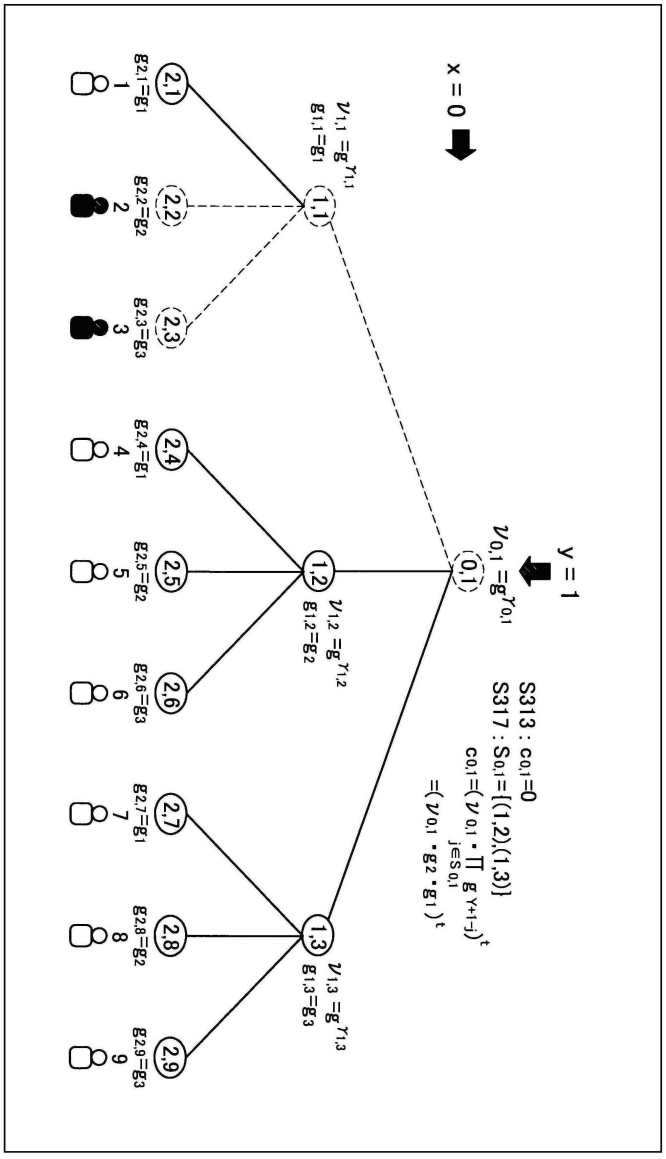
도면17


시작
배제하고 싶은 모든 계약자에게 할당된 리프에서 루트에 이르는 패스 상에 있는 노드를 마크하고, 노드 인덱스의 집합을 S=Φ로 한다
S301
난수t∈Zp를 선택하여, 이하와 같이 하여 세션키(s)를 계산한다
$s=e(g,g_{Y+1})^t=e(g_1,g_Y)^t$
S303
x = −1로 한다
S305
x에 x+1을 대입한다
S307
y = 0으로 한다
S309
y에 y+1을 대입한다
S311
노드(x,y)에 대한 헤더요소($C_{x,y}$)를 $C_{x,y}=0$으로서 초기화한다
S313
(x,y)의 자식노드가 모두 마크되어 있는가?
S315
아니오
예
마크되어 있지 않은 자식노드의 집합을 Sx,y로 하고, Sx,y의 각 요소를 루트로 하는 부분목에 소속하는 계약자에게 대응하는 헤더요소를 이하와 같이 계산한다
$C_{x,y}=(\nu_{x,y}\cdot\prod_{j\in S_{x,y}} g_{Y+1-j})^t\in G$
또, S를 $S\cup S_{x,y}$로 한다
S317
$S_{x,y}$의 각 요소를 루트로 하는 부분목의 모든 노드(리프를 포함)를 마크한다
S319
S321
$y=Y^x$?
아니오
예
S323
x=H−1?
아니오
예
헤더(h)를 이하와 같이 구성한다 $h=(g^t, C_{0,1},\cdots,C_{H-1,X})(C_{x,y}\neq 0)$
S325
암호문(C)을 이하와 같이 구성하고, 헤더(h) 및 S와 함께 송신한다
$C=E_S(M)$
S327
종료

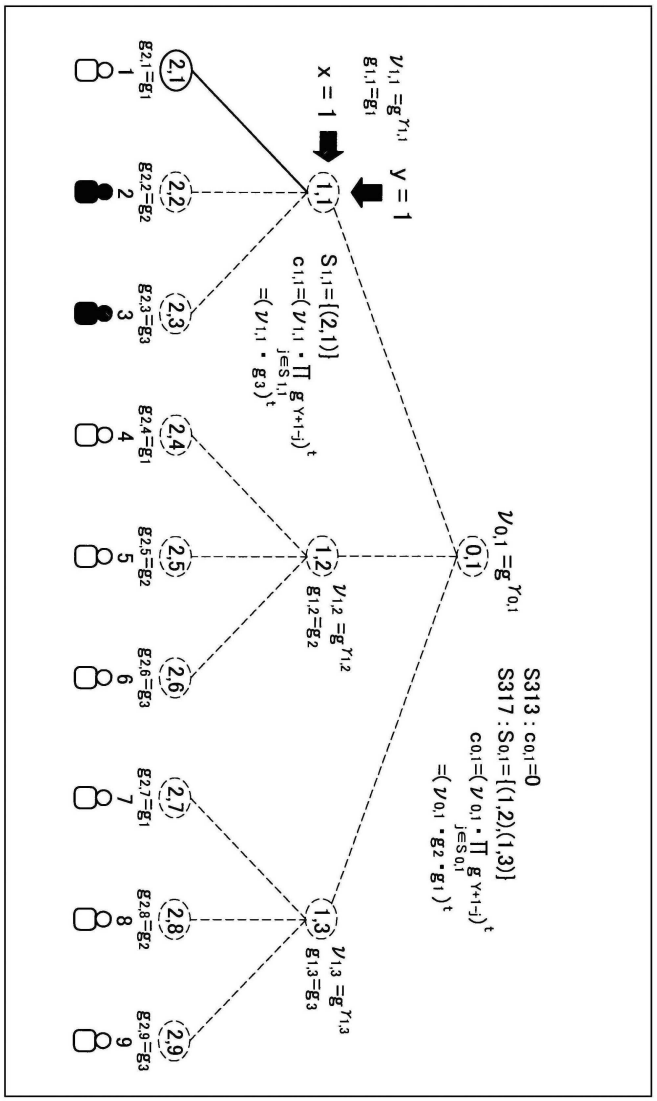
도면18



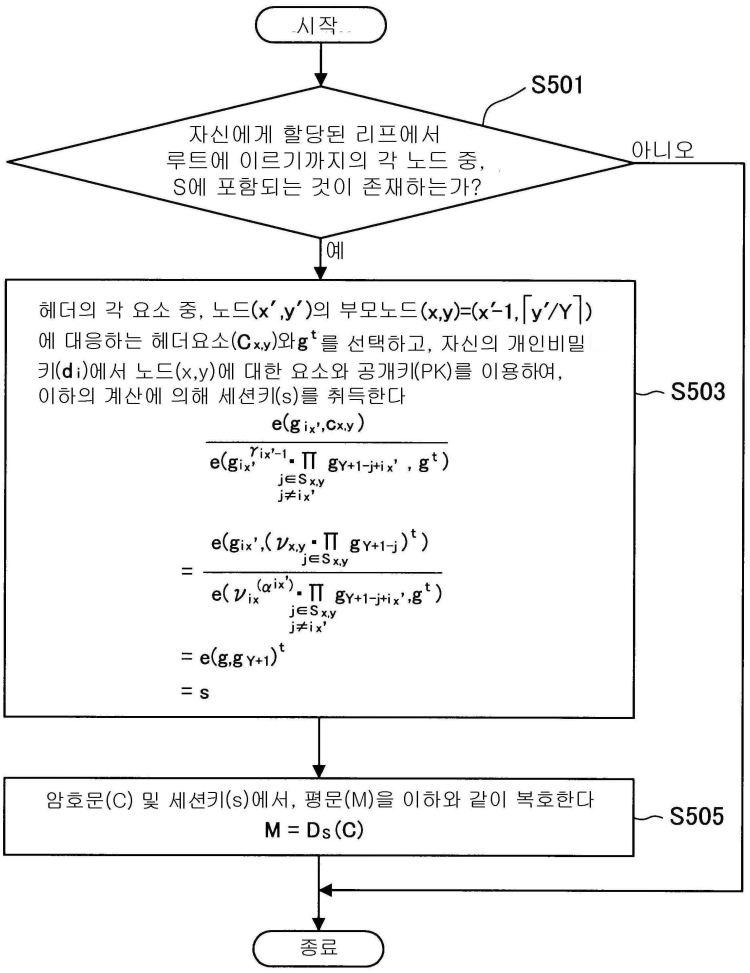
도면19


x = 0
y = 1
S313 : c0,1=0
S317 : S0,1={(1,2),(1,3)}
c0,1=(ν0,1 · ∏ g γ+1-j)t
j∈S0,1
=(ν0,1 · g2 · g1)t
ν0,1 =gγ0,1
(0,1)
ν1,1 =gγ1,1
g1,1=g1
(1,1)
ν1,2 =gγ1,2
g1,2=g2
(1,2)
ν1,3 =gγ1,3
g1,3=g3
(1,3)
(2,1)
g2,1=g1
1
(2,2)
g2,2=g2
2
(2,3)
g2,3=g3
3
(2,4)
g2,4=g1
4
(2,5)
g2,5=g2
5
(2,6)
g2,6=g3
6
(2,7)
g2,7=g1
7
(2,8)
g2,8=g2
8
(2,9)
g2,9=g3
9

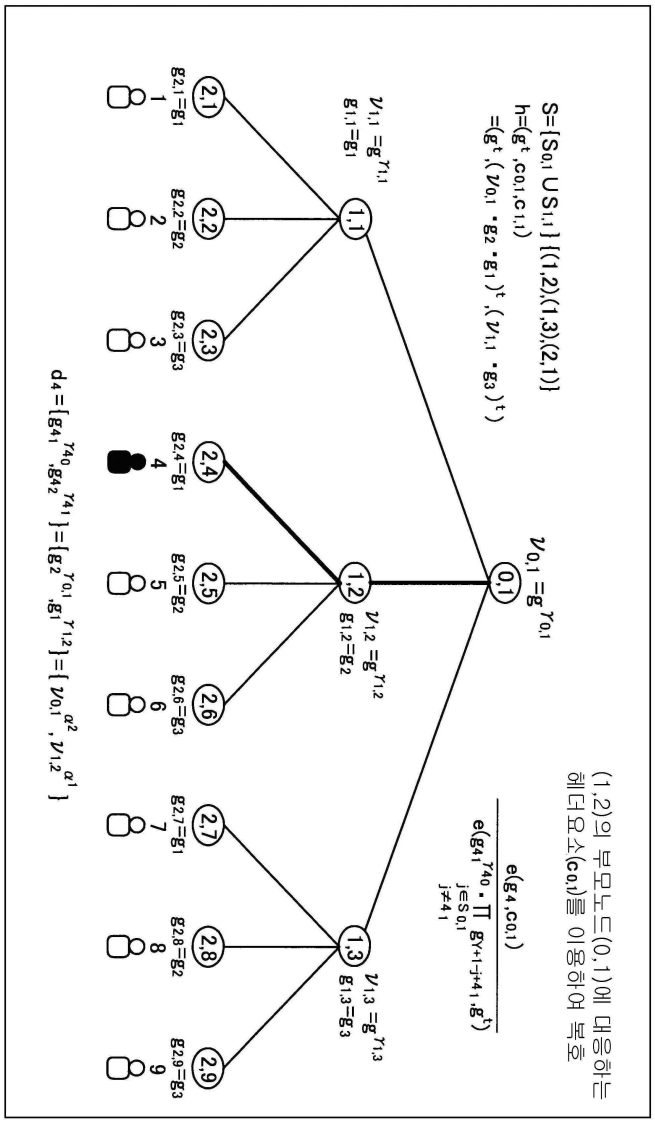
도면20



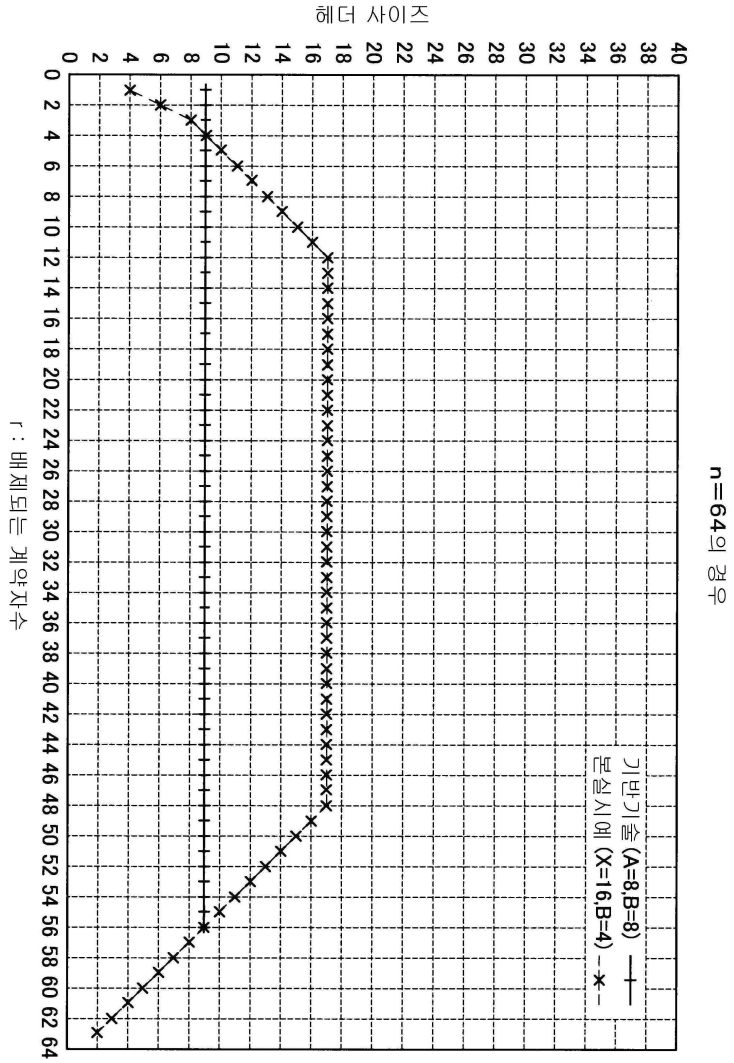
도면21


시작
S501
자신에게 할당된 리프에서
루트에 이르기까지의 각 노드 중,
S에 포함되는 것이 존재하는가?
아니오
예
헤더의 각 요소 중, 노드(x′,y′)의 부모노드(x,y)=(x′-1,⌈y′/Y⌉)
에 대응하는 헤더요소(Cx,y)와g^t를 선택하고, 자신의 개인비밀
키(di)에서 노드(x,y)에 대한 요소와 공개키(PK)를 이용하여,
이하의 계산에 의해 세션키(s)를 취득한다
S503
암호문(C) 및 세션키(s)에서, 평문(M)을 이하와 같이 복호한다
M = DS(C)
S505
종료

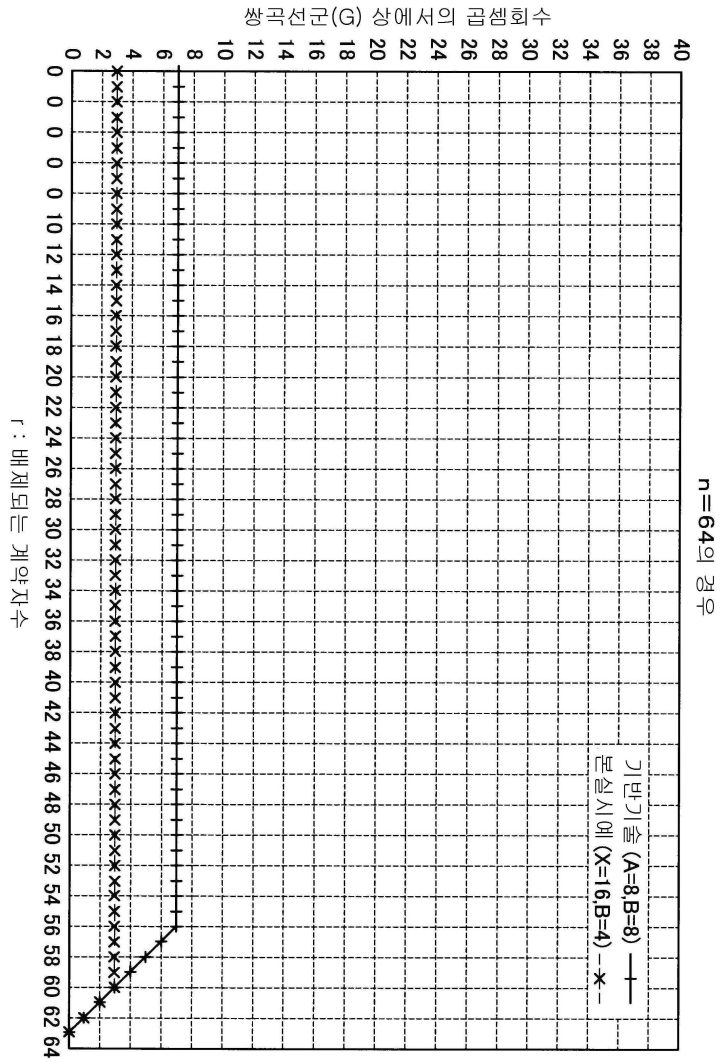
도면22


(1,2)의 부모노드(0,1)에 대응하는 헤더요소(c0,1)를 이용하여 복호
S=[S0,1 ∪ S1,1] {(1,2),(1,3),(2,1)}
h=(g^t, c0,1, c1,1)
=(g^t, (ν0,1 · g2 · g1)^t, (ν1,1 · g3)^t)
ν0,1 = g^γ0,1
ν1,1 = g^γ1,1
g1,1 = g1
ν1,2 = g^γ1,2
g1,2 = g2
ν1,3 = g^γ1,3
g1,3 = g3
e(g4, c0,1) / e(g41^γ40 · ∏ gγ+1-j+41, g^t)
j∈S0,1
j≠41
d4 = [g41^γ40, g42^γ41] = [g2^γ0,1, g1^γ1,2] = [ν0,1^α2, ν1,2^α1]
g2,1=g1
g2,2=g2
g2,3=g3
g2,4=g1
g2,5=g2
g2,6=g3
g2,7=g1
g2,8=g2
g2,9=g3

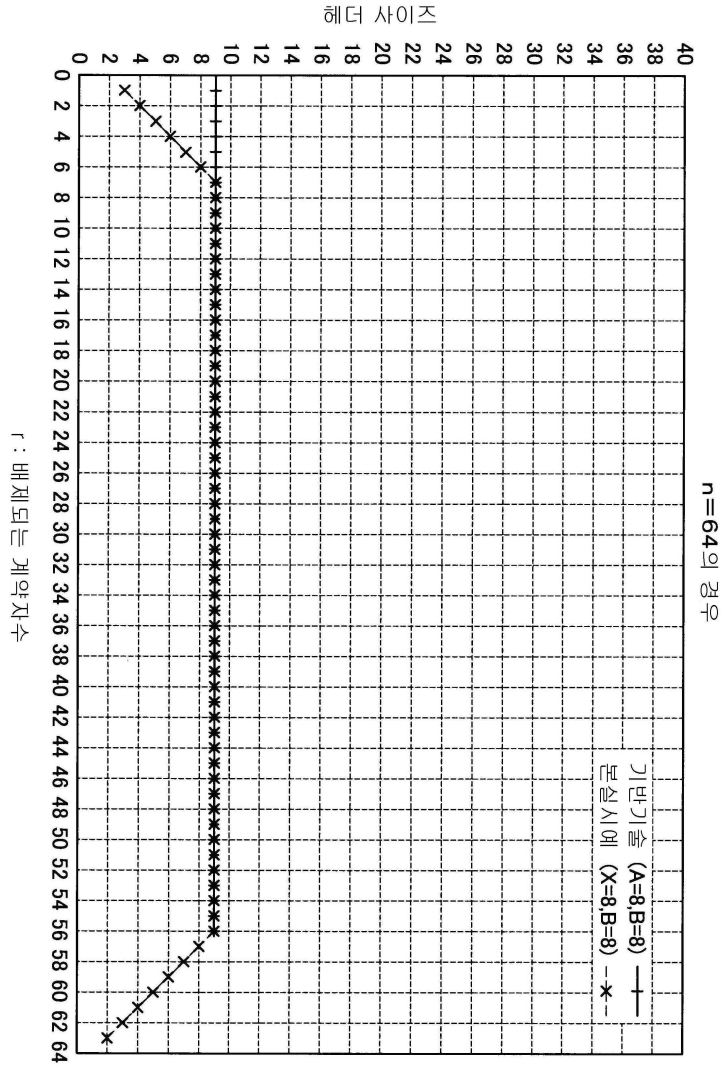
도면23



도면24


쌍곡선군(G) 상에서의 곱셈회수
n=64의 경우
기반기술 (A=8,B=8) ——
본실시예 (X=16,B=4) -*-
r : 배제되는 계약자수
0 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40
0 0 0 0 0 0 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 50 52 54 56 58 60 62 64

도면25



도면26

