(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2010-0014483
(43) 공개일자 2010년02월10일

(51) Int. Cl.
H04L 9/08 (2006.01) *H04W 12/04* (2009.01)
(21) 출원번호 10-2009-7019573
(22) 출원일자 2008년02월04일
심사청구일자 없음
(85) 번역문제출일자 2009년09월18일
(86) 국제출원번호 PCT/JP2008/051745
(87) 국제공개번호 WO 2008/114540
국제공개일자 2008년09월25일
(30) 우선권주장
JP-P-2007-073172 2007년03월20일 일본(JP)

(71) 출원인
소니 주식회사
일본국 도쿄도 미나토쿠 코난 1-7-1
(72) 발명자
아사노 도모유끼
일본 1080075 도쿄도 미나토쿠 코난 1-7-1 소니 가부시끼 가이샤 내
구사까와 마사후미
일본 1080075 도쿄도 미나토쿠 코난 1-7-1 소니 가부시끼 가이샤 내
(74) 대리인
장수길, 이중희, 박충범

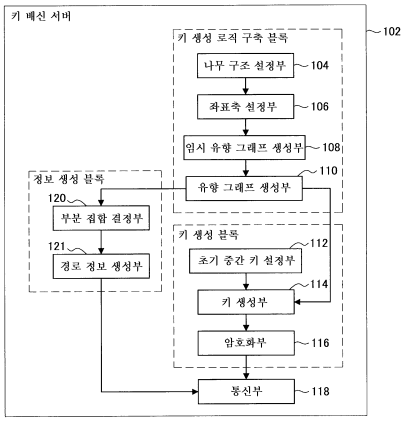
전체 청구항 수 : 총 23 항

(54) 키 제공 시스템, 키 제공 장치, 단말 장치, 키 제공 방법, 및 키 생성 방법

(57) 요 약

데이터의 암호화 또는 복호에 이용하는 키를 소정의 단말 장치에 제공하는 것이 가능한 키 제공 장치가 제공된다. 이 키 제공 장치는, 복수의 단말 장치의 조합을 나타내는 부분 집합이 각각에 대응된 복수의 좌표점을 갖는 좌표축 상에, 좌표점간을 연결하는 적어도 1개의 유향 가지를 배치하여 형성된 유향 그래프를 취득하는 취득부와, 유향 그래프의 시작점과 소정의 좌표점을 연결하는 유향 패스에 포함되는 모든 유향 가지의 정보를 추출하는 추출부와, 유향 그래프에 기초하여, 소정의 단말 장치가 소속되는 부분 집합에 대응된 키를 생성하는 키 생성부를 포함하고, 유향 가지의 정보를 소정의 단말 장치에 제공한다.

대 표 도 - 도8



특허청구의 범위

청구항 1

복수의 단말 장치와, 상기 복수의 단말 장치에 대해 정보의 암호화 또는 복호에 이용하는 키 정보를 제공하는 키 제공 장치를 포함하는 키 제공 시스템이며,

상기 키 제공 장치는,

상기 복수의 단말 장치의 다른 조합을 각각 나타내는 복수의 집합 정보 및 상기 복수의 집합 정보 중 하나에 대응하는 키 정보로부터 다른 하나에 대응하는 키 정보를 생성하는 데 필요한 키 생성 경로를 나타내는 키 생성 경로 정보를 복수 포함하는 집합 관계 정보를 취득하는 집합 관계 정보 취득부와,

상기 집합 관계 정보에 포함되는 복수의 상기 키 생성 경로 정보로부터 복수의 상기 키 생성 경로 정보 중 일부의 키 생성 경로 정보를 추출하는 키 생성 경로 정보 추출부와,

상기 키 생성 경로 정보 추출부에서 추출된 상기 일부의 키 생성 경로 정보를 상기 단말 장치에 제공하는 키 생성 경로 정보 제공부를 포함하고,

상기 단말 장치는,

상기 일부의 키 생성 경로 정보를 취득하는 키 생성 경로 정보 취득부와,

상기 일부의 키 생성 경로 정보에 기초하여, 상기 복수의 집합 정보 중 하나에 대응하는 키 정보로부터 상기 복수의 집합 정보 중 다른 하나에 대응하는 키 정보를 생성하는 키 정보 생성부를 포함하는 것을 특징으로 하는 키 제공 시스템.

청구항 2

복수의 단말 장치에 대해 정보의 암호화 또는 복호에 이용하는 키 정보를 제공하는 키 제공 장치이며,

상기 복수의 단말 장치의 다른 조합을 각각 나타내는 복수의 집합 정보 및 상기 복수의 집합 정보 중 하나에 대응하는 키 정보로부터 다른 하나에 대응하는 키 정보를 생성하는 데 필요한 키 생성 경로를 나타내는 키 생성 경로 정보를 복수 포함하는 집합 관계 정보를 취득하는 집합 관계 정보 취득부와,

상기 집합 관계 정보에 포함되는 복수의 상기 키 생성 경로 정보로부터 복수의 상기 키 생성 경로 정보 중 일부의 키 생성 경로 정보를 추출하는 키 생성 경로 정보 추출부와,

상기 키 생성 경로 정보 추출부에서 추출된 상기 일부의 키 생성 경로 정보를 상기 단말 장치에 제공하는 키 생성 경로 정보 제공부를 포함하는 것을 특징으로 하는 키 제공 장치.

청구항 3

제2항에 있어서, 상기 키 생성 경로 정보 제공부는 네트워크를 통해 상기 키 생성 경로 정보를 상기 단말 장치에 송신하는 통신부를 포함하는 것을 특징으로 하는 키 제공 장치.

청구항 4

제2항에 있어서, 상기 키 생성 경로 정보 제공부는, 상기 키 생성 경로 정보를 상기 단말 장치에 제공하기 위해 기록 매체에 기록하는 기록부를 포함하는 것을 특징으로 하는 키 제공 장치.

청구항 5

제2항에 있어서, 상기 복수의 집합 정보 중 하나에 대응하는 키 정보를 이용하여 정보를 암호화하는 암호화부와,

암호화된 상기 정보를 상기 단말 장치에 제공하는 암호 정보 제공부를 더 포함하는 것을 특징으로 하는 키 제공 장치.

청구항 6

제2항에 있어서, 상기 키 생성 경로 정보 취득부는, 상기 집합 관계 정보로서, 상기 복수의 단말 장치의 다른

조합을 각각 나타내는 복수의 집합 정보에 대응된 복수의 좌표점에 대해, 상기 복수의 좌표점간을 연결하는 유향 가지(directional branch)에 의해 형성된 유향 그래프를 취득하는 것을 특징으로 하는 키 제공 장치.

청구항 7

제6항에 있어서, 상기 키 생성 경로 정보 추출부는, 상기 일부의 키 생성 경로 정보로서, 상기 단말 장치가 속하는 상기 집합 정보에 대응된 좌표점에 도달하는 상기 유향 그래프의 일부를 추출하는 것을 특징으로 하는 키 제공 장치.

청구항 8

제7항에 있어서, 상기 키 생성 경로 정보 추출부는, 상기 일부의 키 생성 경로 정보로서, 상기 유향 그래프의 일부를 구성하는 유향 가지의 종단부 위치를 나타내는 정보를 추출하는 것을 특징으로 하는 키 제공 장치.

청구항 9

제7항에 있어서, 상기 키 생성 경로 정보 추출부는, 상기 일부의 키 생성 경로 정보로서, 상기 유향 그래프의 일부를 구성하는 유향 가지의 길이를 나타내는 정보를 추출하는 것을 특징으로 하는 키 제공 장치.

청구항 10

제6항에 있어서, 상기 좌표점 S_0에 대응하는 상기 키 정보 $k(S_0)$의 입력에 따라서, 상기 좌표점 S_0을 시단부로 하는 모든 상기 유향 가지의 종단부의 좌표점 S_1,…, S_m에 대응하는 상기 키 정보 $k(S_1)$,…, $k(S_m)$를 생성하는 키 정보 생성부를 더 포함하는 것을 특징으로 하는 키 제공 장치.

청구항 11

제6항에 있어서, 상기 키 정보는, 정보를 암호화 또는 복호하기 위한 세트 키 k와, 상기 세트 키 k를 생성하기 위한 중간 키 t에 의해 구성되고,

상기 좌표점 S_0에 대응하는 상기 중간 키 $t(S_0)$의 입력에 따라서, 상기 좌표점 S_0에 대응하는 상기 세트 키 $k(S_0)$와, 상기 좌표점 S_0을 시단부로 하는 모든 상기 유향 가지의 종단부의 좌표점 S_1,…, S_m에 대응하는 상기 중간 키 $t(S_1)$,…, $t(S_m)$를 생성하는 키 정보 생성부를 더 포함하는 것을 특징으로 하는 키 제공 장치.

청구항 12

복수의 단말 장치에 대해 정보의 암호화 또는 복호에 이용하는 키 정보를 제공하는 키 제공 장치이며,

상기 복수의 단말 장치의 다른 조합을 각각 나타내는 복수의 집합 정보 및 상기 복수의 집합 정보 중 하나에 대응하는 키 정보로부터 다른 하나에 대응하는 키 정보를 생성하는 데 필요한 키 생성 경로를 나타내는 키 생성 경로 정보를 복수 포함하는 집합 관계 정보를 생성하는 집합 관계 정보 생성부와,

상기 집합 관계 정보에 포함되는 복수의 상기 키 생성 경로 정보로부터, 복수의 상기 키 생성 경로 정보 중 일부의 키 생성 경로 정보를 추출하는 키 생성 경로 정보 추출부와,

상기 키 생성 경로 정보 추출부에서 추출된 상기 일부의 키 생성 경로 정보를 상기 단말 장치에 제공하는 키 생성 경로 정보 제공부를 포함하는 것을 특징으로 하는 키 제공 장치.

청구항 13

정보의 암호화 또는 복호에 이용하는 키 정보를 생성하는 단말 장치이며,

복수의 단말 장치의 다른 조합을 각각 나타내는 복수의 집합 정보 및 상기 복수의 집합 정보 중 하나에 대응하는 키 정보로부터 다른 하나에 대응하는 키 정보를 생성하는 데 필요한 키 생성 경로를 나타내는 키 생성 경로 정보를 복수 포함하는 집합 관계 정보 중에서 추출된, 복수의 상기 키 생성 경로 정보 중 일부의 키 생성 경로 정보를 취득하는 키 생성 경로 정보 취득부와,

상기 일부의 키 생성 경로 정보에 기초하여, 상기 복수의 집합 정보 중 하나에 대응하는 키 정보로부터 상기 복수의 집합 정보 중 다른 하나에 대응하는 키 정보를 생성하는 키 정보 생성부를 포함하는 것을 특징으로 하는

단말 장치.

청구항 14

제13항에 있어서, 상기 키 생성 경로 정보 취득부는, 네트워크를 통해 상기 키 생성 경로 정보를 수신하는 통신부를 포함하는 것을 특징으로 하는 단말 장치.

청구항 15

제13항에 있어서, 상기 키 생성 경로 정보 취득부는, 상기 키 생성 경로 정보가 기록된 기록 매체를 취득하고, 상기 기록 매체로부터 상기 키 생성 경로 정보를 판독하는 판독부를 포함하는 것을 특징으로 하는 단말 장치.

청구항 16

제13항에 있어서, 상기 복수의 집합 정보 중 다른 하나에 대응하는 키 정보를 이용하여 암호화된 정보를 취득하는 암호 정보 취득부와,

상기 키 정보 생성부에 의해 생성된 상기 복수의 집합 정보 중 다른 하나에 대응하는 키 정보를 이용하여, 상기 암호화된 정보를 복호하는 암호 정보 복호부를 더 포함하는 것을 특징으로 하는 단말 장치.

청구항 17

제13항에 있어서, 상기 키 생성 경로 정보 취득부는, 상기 복수의 단말 장치의 다른 조합을 각각 나타내는 복수의 집합 정보에 대응된 복수의 좌표점에 대해, 상기 복수의 좌표점간을 연결하는 유향 가지에 의해 형성된 유향 그래프 중에서 추출된, 상기 단말 장치가 속하는 상기 집합 정보에 대응된 좌표점에 도달하는 상기 유향 그래프의 일부를 상기 일부의 키 생성 경로 정보로서 취득하는 것을 특징으로 하는 단말 장치.

청구항 18

제17항에 있어서, 상기 키 생성 경로 정보 취득부는, 상기 일부의 키 생성 경로 정보로서, 상기 유향 그래프의 일부를 구성하는 유향 가지의 종단부 위치를 나타내는 정보를 취득하는 것을 특징으로 하는 단말 장치.

청구항 19

제17항에 있어서, 상기 키 생성 경로 정보 취득부는, 상기 일부의 키 생성 경로 정보로서, 상기 유향 그래프의 일부를 구성하는 유향 가지의 길이를 나타내는 정보를 취득하는 것을 특징으로 하는 단말 장치.

청구항 20

제17항에 있어서, 상기 유향 가지의 시단부 S_0에 대응하는 상기 키 정보 $k(S_0)$의 입력에 따라서, 상기 유향 가지의 종단부의 좌표점 S_1에 대응하는 상기 키 정보 $k(S_1)$를 생성하는 키 정보 생성부를 더 포함하는 것을 특징으로 하는 단말 장치.

청구항 21

제17항에 있어서, 상기 키 정보는, 정보를 암호화 또는 복호하기 위한 세트 키 k와, 상기 세트 키 k를 생성하기 위한 중간 키 t에 의해 구성되고,

상기 유향 가지의 시단부 S_0에 대응하는 상기 중간 키 $t(S_0)$의 입력에 따라서, 상기 유향 가지의 시단부 S_0에 대응하는 상기 세트 키 $k(S_0)$와, 상기 유향 가지의 종단부 S_1에 대응하는 상기 중간 키 $t(S_1)$를 생성하는 키 정보 생성부를 더 포함하는 것을 특징으로 하는 단말 장치.

청구항 22

복수의 단말 장치에 대해 데이터의 암호화 또는 복호에 이용하는 키 정보를 제공하기 위한 키 제공 방법이며,

상기 복수의 단말 장치의 다른 조합을 각각 나타내는 복수의 집합 정보 및 상기 복수의 집합 정보 중 하나에 대응하는 키 정보로부터 다른 하나에 대응하는 키 정보를 생성하는 데 필요한 키 생성 경로를 나타내는 키 생성 경로 정보를 복수 포함하는 집합 관계 정보를 취득하는 집합 관계 정보 취득 스텝과,

상기 집합 관계 정보에 포함되는 복수의 상기 키 생성 경로 정보로부터, 복수의 상기 키 생성 경로 정보 중 일부의 키 생성 경로 정보를 추출하는 키 생성 경로 정보 추출 스텝과,

상기 키 생성 경로 정보 추출 스텝에서 추출된 상기 일부의 키 생성 경로 정보를 상기 단말 장치에 제공하는 키 생성 경로 정보 제공 스텝을 포함하는 것을 특징으로 하는 키 제공 방법.

청구항 23

정보의 암호화 또는 복호에 이용하는 키 정보를 생성하기 위한 키 생성 방법이며,

복수의 단말 장치의 다른 조합을 각각 나타내는 복수의 집합 정보 및 상기 복수의 집합 정보 중 하나에 대응하는 키 정보로부터 다른 하나에 대응하는 키 정보를 생성하는 데 필요한 키 생성 경로를 나타내는 키 생성 경로 정보를 복수 포함하는 집합 관계 정보 중에서 추출된, 복수의 상기 키 생성 경로 정보 중 일부의 키 생성 경로 정보를 취득하는 키 생성 경로 정보 취득 스텝과,

상기 일부의 키 생성 경로 정보에 기초하여, 상기 복수의 집합 정보 중 하나에 대응하는 키 정보로부터 상기 복수의 집합 정보 중 다른 하나에 대응하는 키 정보를 생성하는 키 정보 생성 스텝을 포함하는 것을 특징으로 하는 키 생성 방법.

명 세 서

기 술 분 야

[0001] 본 발명은, 키 제공 시스템, 키 제공 장치, 단말 장치, 키 제공 방법, 및 키 생성 방법에 관한 것이다.

배 경 기 술

[0002] 최근, 퍼스널 컴퓨터(이하, PC), 휴대 전화, 및 디지털 가전 제품 등의 정보 기기가 일반적으로도 널리 보급되어 오고 있다. 또한, 이들 정보 기기나 그들 사이를 연결하는 정보 통신에 관한 기술이 매우 크게 발달되고 있고, 이들 정보 기기를 이용한 음악 배신이나 영상 배신 등의 콘텐츠 배신 서비스가 널리 전개되도록 되고 있다. 예를 들어, CATV(Community Antenna TeleVision), 위성 방송, 또는 인터넷 등을 이용한 유료 방송, CD(Compact Disc) 또는 DVD(Digital Versatile Disc) 등 물리 미디어를 이용한 콘텐츠 판매 등이 콘텐츠 배신 서비스의 일례이다.

[0003] 그러나, 이와 같은 콘텐츠 배신 서비스를 제공하기 위해서는, 이 서비스의 제공자(이하, 시스템 관리자)와 시청자 사이에 체결한 계약에 기초하여, 그 계약자만이 콘텐츠를 취득할 수 있도록 하는 구조가 필요하게 된다. 이 문제에 대해, 예를 들어 시스템 관리자가 계약자에 대해 소정의 키를 제공해 두고, 암호화된 콘텐츠 M과 함께, 콘텐츠 M을 암호화하기 위해 이용한 콘텐츠 키 mek를 상기 소정의 키에 의해 생성하기 위한 헤더 정보 h를 배신하는 구조가 고안되고 있다.

[0004] 상기한 구조를 실현시키는 구체적인 한 수단으로서, 브로드캐스트 엔크립션(Broadcast Encryption) 방식이라 불리는 콘텐츠 배신 방식이 알려져 있다. 이 브로드캐스트 엔크립션 방식이라 함은, 각 계약자를 집합 요소에 대응시킨 후에, 계약자 전체를 나타내는 계약자 집합을 복수의 부분 집합으로 분할하고, 특정한 부분 집합에 속하는 계약자만이 콘텐츠 키 mek를 취득할 수 있는 헤더 h를 배신하는 방식이다. 즉, 이 방식을 적용하면, 시스템 관리자가 지정한 특정 계약자를 배제하고 콘텐츠 C의 배신을 실현할 수 있다. 그러나, 현실적으로는, 시스템 관리자측의 서버 장치(이하, 센터) 및 계약자측의 단말 장치에 있어서의 콘텐츠 키 mek의 생성에 관한 연산 부하, 및 서버 장치와 단말 장치 사이의 통신 부하 등을 고려하면, 종래의 브로드캐스트 엔크립션 방식을 보다 효율화할 필요가 있다.

[0005] 구체적으로는, 상기한 콘텐츠 배신을 할 때에, 센터가 배신하는 헤더 h의 사이즈에 따라서 증대하는 통신량, 각 단말 장치가 유지해야 할 키수에 따라서 증대하는 메모리량, 및 각 단말 장치가 콘텐츠 키 mek를 생성하기 위해 필요한 계산량을 어떻게 저감시킬 것인지가 문제가 된다. 상기한 각 양은, 계약자 집합의 분할 방법에 따라 크게 다르다. 따라서, 효율적인 콘텐츠 배신을 실현시키기 위해, 계약자 집합의 분할 방법에 고안한 다양한 브로드캐스트 엔크립션 방식이 제안되어 있다. 예를 들어, 하기의 비특허 문헌 1에는, 상기한 각 양을 저감시키기 위한 하나의 수단으로서, Nuttapong Attrapadung and Hideki Imai들에 의해, Subset Incremental Chain Based Broadcast Encryption 방식이라 불리는 콘텐츠 배신 방식이 개시되어 있다(이하, AI05 방식).

[0006] 비특허 문헌 1 : Nuttapong Attrapadung and Hideki Imai, "Subset Incremental Chain Based Broadcast Encryption with Shorter Ciphertext", The 28th Symposium on Information Theory and Its Applications(SITA2005)

발명의 상세한 설명

[0007] 또한, 본건 출원인은, 상기한 비특허 문헌 1에 기재된 콘텐츠 배신 방식보다도, 각 단말 장치가 키를 유지하기 위해 요구되는 메모리량을 저감시키는 것이 가능한 제1 개량 방식[이하, A06(A) 방식], 각 단말 장치가 콘텐츠 키를 생성하기 위해 요구되는 계산량을 저감시키는 것이 가능한 제2 개량 방식[이하, A06(B) 방식], 및 상기한 메모리량과 계산량을 저감시키는 것이 가능한 제3 개량 방식[이하, A06(A+B) 방식]을 개발하고, 이미 일본 특허청에 특허 출원하였다[A06(A) 방식 : 일본 특허 출원 제2006-310182, A06(B) 방식 : 일본 특허 출원 제2006-310213, A06(A+B) 방식 : 일본 특허 출원 제2006-310226]. 각 방식의 특징은, 의사 난수 생성기를 이용하여 콘텐츠 키 mek를 생성할 때에, 각 방식 고유의 유향 그래프에 의해 표현되는 키 생성 알고리즘에 기초하여, 의사 난수 생성 연산을 실행하는 점에 있다.

[0008] 그러나, 상기한 각 방식에 한하지 않고, 어느 방식에 따라서 하나의 부분 집합에 대응하는 키로부터 다른 부분 집합에 대응하는 키를 생성하는 경우, 예를 들어 복수의 키 생성 경로의 정보를 포함하는 유향 그래프와 같은 집합 관계 정보를 단말 장치측에서 모두 유지해야만 한다고 하면, 복수의 키 생성 경로의 정보를 유지하기 위해 필요로 하는 기억 용량이 커지게 된다는 문제가 있다. 한편, 키 제공 장치가 갖는 복수의 키 생성 경로의 정보를 단말 장치가 모두 취득해야만 한다고 하면, 복수의 키 생성 경로의 정보를 단말 장치가 취득하기 위해 전파되는 용량이 커지게 되는 문제도 있다.

[0009] 본 발명은, 상기 문제를 감안하여 이루어진 것으로, 본 발명이 목적으로 하는 바는, 단말 장치가 미리 모든 키 생성 경로 정보를 전파 또는 유지하고 있는 경우에 비해, 단말 장치가 키 생성에 필요로 하는 정보를 전파 또는 유지하기 위해 필요한 용량을 저감시키는 것이 가능한, 신규 또한 개량된 키 제공 시스템, 키 제공 장치, 단말 장치, 키 제공 방법 및 키 생성 방법을 제공하는 것에 있다.

[0010] <과제를 해결하기 위한 수단>

[0011] 상기 과제를 해결하기 위해, 본 발명이 있는 관점에 따르면, 복수의 단말 장치와, 이들 복수의 단말 장치에 정보의 암호화 또는 복호에 이용하는 키 정보를 제공하는 키 제공 장치를 구비하는 키 제공 시스템이 제공된다.

[0012] 또한, 상기 키 제공 장치는, 상기 복수의 단말 장치의 다른 조합을 각각 나타내는 복수의 집합 정보 및 이들 복수의 집합 정보 중 하나에 대응하는 키 정보로부터 다른 하나에 대응하는 키 정보를 생성하는 데 필요한 키 생성 경로를 나타내는 키 생성 경로 정보를 복수 포함하는 집합 관계 정보를 취득하는 집합 관계 정보 취득부와, 상기 집합 관계 정보에 포함되는 복수의 상기 키 생성 경로 정보로부터 이들 복수의 상기 키 생성 경로 정보 중 일부의 키 생성 경로 정보를 추출하는 키 생성 경로 정보 추출부와, 이 키 생성 경로 정보 추출부에서 추출된 상기 일부의 키 생성 경로 정보를 상기 단말 장치에 제공하는 키 생성 경로 정보 제공부를 구비하고 있어도 된다.

[0013] 또한, 상기 단말 장치는, 상기 일부의 키 생성 경로 정보를 취득하는 키 생성 경로 정보 취득부와, 상기 일부의 키 생성 경로 정보에 기초하여, 상기 복수의 집합 정보 중 하나에 대응하는 키 정보로부터 상기 복수의 집합 정보 중 다른 하나에 대응하는 키 정보를 생성하는 키 정보 생성부를 구비하고 있어도 된다.

[0014] 또한, 상기 과제를 해결하기 위해, 본 발명의 다른 관점에 따르면, 복수의 단말 장치에 대해 데이터의 암호화 또는 복호에 이용하는 키 정보를 제공하는 키 제공 장치가 제공된다. 이 키 제공 장치는, 상기 복수의 단말 장치의 다른 조합을 각각 나타내는 복수의 집합 정보 및 이들 복수의 집합 정보 중 하나에 대응하는 키 정보로부터 다른 하나에 대응하는 키 정보를 생성하는 데 필요한 키 생성 경로를 나타내는 키 생성 경로 정보를 복수 포함하는 집합 관계 정보를 취득하는 집합 관계 정보 취득부와, 상기 집합 관계 정보에 포함되는 복수의 상기 키 생성 경로 정보로부터 이들 복수의 상기 키 생성 경로 정보 중 일부의 키 생성 경로 정보를 추출하는 키 생성 경로 정보 추출부와, 이 키 생성 경로 정보 추출부에서 추출된 상기 일부의 키 생성 경로 정보를 상기 단말 장치에 제공하는 키 생성 경로 정보 제공부를 구비하는 것을 특징으로 한다.

[0015] 또한, 상기 키 생성 경로 정보 제공부는, 네트워크를 통해 상기 키 생성 경로 정보를 상기 단말 장치에 송신하는 통신부를 구비하고 있어도 된다.

[0016] 또한, 상기 키 생성 경로 정보 제공부는, 상기 키 생성 경로 정보를 상기 단말 장치에 제공하기 위해 기록 매체

에 기록하는 기록부를 구비하고 있어도 된다.

[0017] 또한, 상기 복수의 집합 정보 중 하나에 대응하는 키 정보를 이용하여 정보를 암호화하는 암호화부와, 암호화된 상기 정보를 상기 단말 장치에 제공하는 암호 정보 제공부를 더 구비하고 있어도 된다.

[0018] 또한, 상기 키 생성 경로 정보 취득부는, 상기 집합 관계 정보로서, 상기 복수의 단말 장치의 다른 조합을 각각 나타내는 복수의 집합 정보에 대응된 복수의 좌표점에 대해, 이 복수의 좌표점간을 연결하는 유향 가지에 의해 형성된 유향 그래프를 취득하도록 구성되어 있어도 된다.

[0019] 또한, 상기 키 생성 경로 정보 추출부는, 상기 일부의 키 생성 경로 정보로서, 상기 단말 장치가 속하는 상기 집합 정보에 대응된 좌표점에 도달하는 상기 유향 그래프의 일부를 추출하도록 구성되어 있어도 된다.

[0020] 또한, 상기 키 생성 경로 정보 추출부는, 상기 일부의 키 생성 경로 정보로서 상기 유향 그래프의 일부를 구성하는 유향 가지의 종단부 위치를 나타내는 정보를 추출하도록 구성되어 있어도 된다.

[0021] 또한, 상기 키 생성 경로 정보 추출부는, 상기 일부의 키 생성 경로 정보로서, 상기 유향 그래프의 일부를 구성하는 유향 가지의 길이를 나타내는 정보를 추출하도록 구성되어 있어도 된다.

[0022] 또한, 상기 좌표점 S_0에 대응하는 상기 키 정보 $k(S_0)$의 입력에 따라서, 상기 좌표점 S_0을 시단부로 하는 모든 상기 유향 가지의 종단부의 좌표점 $S_1,\cdots, S_m$에 대응하는 상기 키 정보 $k(S_1),\cdots, k(S_m)$를 생성하는 키 정보 생성부를 더 구비하고 있어도 된다.

[0023] 또한, 상기 키 정보는, 정보를 암호화 또는 복호하기 위한 세트 키 k와, 이 세트 키 k를 생성하기 위한 중간 키 t로 구성되어 있어도 된다. 또한, 상기 좌표점 S_0에 대응하는 상기 중간 키 $t(S_0)$의 입력에 따라서, 상기 좌표점 S_0에 대응하는 상기 세트 키 $k(S_0)$와, 상기 좌표점 S_0을 시단부로 하는 모든 상기 유향 가지의 종단부의 좌표점 $S_1,\cdots, S_m$에 대응하는 상기 중간 키 $t(S_1),\cdots, t(S_m)$를 생성하는 키 정보 생성부를 더 구비하고 있어도 된다.

[0024] 또한, 상기 과제를 해결하기 위해, 본 발명의 다른 관점에 따르면, 복수의 단말 장치에 대해 데이터의 암호화 또는 복호에 이용하는 키 정보를 제공하는 키 제공 장치가 제공된다. 이 키 제공 장치는, 상기 복수의 단말 장치의 다른 조합을 각각 나타내는 복수의 집합 정보 및 이들 복수의 집합 정보 중 하나에 대응하는 키 정보로부터 다른 하나에 대응하는 키 정보를 생성하는 데 필요한 키 생성 경로를 나타내는 키 생성 경로 정보를 복수 포함하는 집합 관계 정보를 생성하는 집합 관계 정보 생성부와, 상기 집합 관계 정보에 포함되는 복수의 상기 키 생성 경로 정보로부터 이들 복수의 상기 키 생성 경로 정보 중 일부의 키 생성 경로 정보를 추출하는 키 생성 경로 정보 추출부와, 이 키 생성 경로 정보 추출부에서 추출된 상기 일부의 키 생성 경로 정보를 상기 단말 장치에 제공하는 키 생성 경로 정보 제공부를 구비하는 것을 특징으로 한다.

[0025] 또한, 상기 과제를 해결하기 위해, 본 발명의 다른 관점에 따르면, 정보의 암호화 또는 복호에 이용하는 키 정보를 생성하는 단말 장치가 제공된다. 이 단말 장치는, 복수의 단말 장치의 다른 조합을 각각 나타내는 복수의 집합 정보 및 이들 복수의 집합 정보 중 하나에 대응하는 키 정보로부터 다른 하나에 대응하는 키 정보를 생성하는 데 필요한 키 생성 경로를 나타내는 키 생성 경로 정보를 복수 포함하는 집합 관계 정보 중으로부터 추출된, 이들 복수의 상기 키 생성 경로 정보 중 일부의 키 생성 경로 정보를 취득하는 키 생성 경로 정보 취득부와, 상기 일부의 키 생성 경로 정보에 기초하여, 상기 복수의 집합 정보 중 하나에 대응하는 키 정보로부터 상기 복수의 집합 정보 중 다른 하나에 대응하는 키 정보를 생성하는 키 정보 생성부를 구비하는 것을 특징으로 한다.

[0026] 또한, 상기 키 생성 경로 정보 취득부는, 네트워크를 통해 상기 키 생성 경로 정보를 수신하는 통신부를 구비하고 있어도 된다.

[0027] 또한, 상기 키 생성 경로 정보 취득부는, 상기 키 생성 경로 정보가 기록된 기록 매체를 취득하고, 상기 기록 매체로부터 상기 키 생성 경로 정보를 판독하는 판독부를 구비하고 있어도 된다.

[0028] 또한, 상기 복수의 집합 정보 중 다른 하나에 대응하는 키 정보를 이용하여 암호화된 정보를 취득하는 암호 정보 취득부와, 상기 키 정보 생성부에 의해 생성된 상기 복수의 집합 정보 중 다른 하나에 대응하는 키 정보를 이용하여, 상기 암호화된 정보를 복호하는 복호부를 더 구비하고 있어도 된다.

[0029] 또한, 상기 키 생성 경로 정보 취득부는, 상기 복수의 단말 장치의 다른 조합을 각각 나타내는 복수의 집합 정보에 대응된 복수의 좌표점에 대해, 이 복수의 좌표점간을 연결하는 유향 가지에 의해 형성된 유향 그래프 중으

로부터 추출된, 상기 단말 장치가 속하는 상기 집합 정보에 대응된 좌표점에 도달하는 상기 유향 그래프의 일부를 상기 일부의 키 생성 경로 정보로서 취득하도록 구성되어 있어도 된다.

[0030] 또한, 상기 키 생성 경로 정보 취득부는, 상기 일부의 키 생성 경로 정보로서 상기 유향 그래프의 일부를 구성하는 유향 가지의 종단부 위치를 나타내는 정보를 취득하도록 구성되어 있어도 된다.

[0031] 또한, 상기 키 생성 경로 정보 취득부는, 상기 일부의 키 생성 경로 정보로서, 상기 유향 그래프의 일부를 구성하는 유향 가지의 길이를 나타내는 정보를 취득하도록 구성되어 있어도 된다.

[0032] 또한, 상기 유향 가지의 시단부 S_0에 대응하는 상기 키 정보 $k(S_0)$의 입력에 따라서, 상기 유향 가지의 종단부의 좌표점 S_1에 대응하는 상기 키 정보 $k(S_1)$를 생성하는 키 정보 생성부를 더 구비하고 있어도 된다.

[0033] 또한, 상기 키 정보는, 정보를 암호화 또는 복호하기 위한 세트 키 k와, 이 세트 키 k를 생성하기 위한 중간 키 t에 의해 구성되어 있어도 된다. 또한, 상기 유향 가지의 시단부 S_0에 대응하는 상기 중간 키 $t(S_0)$의 입력에 따라서, 상기 유향 가지의 시단부 S_0에 대응하는 상기 세트 키 $k(S_0)$와, 상기 유향 가지의 종단부 S_1에 대응하는 상기 중간 키 $t(S_1)$를 생성하는 키 정보 생성부를 더 구비하고 있어도 된다.

[0034] 또한, 상기 과제를 해결하기 위해, 본 발명의 다른 관점에 따르면, 복수의 단말 장치에 대해 데이터의 암호화 또는 복호에 이용하는 키 정보를 제공하기 위한 키 제공 방법이 제공된다. 이 키 제공 방법은, 상기 복수의 단말 장치의 다른 조합을 각각 나타내는 복수의 집합 정보 및 이들 복수의 집합 정보 중 하나에 대응하는 키 정보로부터 다른 하나에 대응하는 키 정보를 생성하는 데 필요한 키 생성 경로를 나타내는 키 생성 경로 정보를 복수 포함하는 집합 관계 정보를 취득하는 집합 관계 정보 취득 스텝과, 상기 집합 관계 정보에 포함되는 복수의 상기 키 생성 경로 정보로부터, 이들 복수의 상기 키 생성 경로 정보 중 일부의 키 생성 경로 정보를 추출하는 키 생성 경로 정보 추출 스텝과, 이 키 생성 경로 정보 추출부에서 추출된 상기 일부의 키 생성 경로 정보를 상기 단말 장치에 제공하는 키 생성 경로 정보 제공 스텝을 포함하는 것을 특징으로 한다.

[0035] 또한, 상기 과제를 해결하기 위해, 본 발명의 다른 관점에 따르면, 정보의 암호화 또는 복호에 이용하는 키 정보를 생성하기 위한 키 생성 방법이 제공된다. 이 키 생성 방법은, 복수의 단말 장치의 다른 조합을 각각 나타내는 복수의 집합 정보 및 이들 복수의 집합 정보 중 하나에 대응하는 키 정보로부터 다른 하나에 대응하는 키 정보를 생성하는 데 필요한 키 생성 경로를 나타내는 키 생성 경로 정보를 복수 포함하는 집합 관계 정보 중으로부터 추출된, 이들 복수의 상기 키 생성 경로 정보 중 일부의 키 생성 경로 정보를 취득하는 키 생성 경로 정보 취득 스텝과, 상기 일부의 키 생성 경로 정보에 기초하여, 상기 복수의 집합 정보 중 하나에 대응하는 키 정보로부터 상기 복수의 집합 정보 중 다른 하나에 대응하는 키 정보를 생성하는 키 정보 생성 스텝을 포함하는 것을 특징으로 한다.

[0036] 상기한 각 구성에 따르면, 키 제공 장치에 의해 추출된 일부의 키 생성 경로 정보가 단말 장치에 제공되어, 단말 장치가 하나의 집합에 대응하는 키로부터 다른 집합에 대응하는 키를 도출할 수 있으므로, 키 제공 장치가 갖는 모든 키 생성 경로 정보의 제공을 받는 경우에 비해, 키 제공 장치로부터 단말 장치에 키 생성 경로 정보를 전파하기 위해 필요한 용량을 제한할 수 있다. 또한, 단말 장치가 미리 모든 키 생성 경로 정보를 유지하고 있는 경우에 비해서도, 단말 장치가 유지를 위해 필요로 하는 용량을 제한할 수 있다.

[0037] <발명의 효과>

[0038] 이상 설명한 바와 같이 본 발명에 따르면, 단말 장치가 미리 모든 키 생성 경로 정보를 전파 또는 유지하는 경우에 비해, 단말 장치가 키 생성에 필요로 하는 정보를 전파 또는 유지하기 위해 필요한 용량을 저감시키는 것이 가능해진다.

실 시 예

[0088] 이하에 첨부 도면을 참조하면서, 본 발명의 적합한 실시 형태에 대해 상세하게 설명한다. 또한, 본 명세서 및 도면에 있어서, 실질적으로 동일한 기능 구성을 갖는 구성 요소에 대해서는, 동일 부호를 부여함으로써 중복 설명을 생략한다.

[0089] <제1 실시 형태>

[0090] 이하, 본 발명의 제1 실시 형태에 관한 키 제공 시스템(100)의 구성, 및 키 배신에 관한 구체적인 방식에 대해

상세하게 설명한다.

[0091] [개요]

[0092] 우선, 본 실시 형태에 관한 키 제공 시스템(100)의 구성에 대해 상세하게 설명하는 것에 앞서, 본 실시 형태에 관한 키 배신 방식의 개요에 대해 간단하게 설명한다.

[0093] 본 실시 형태는, 다양한 키 배신 방식에 적용하는 것이 가능하지만, 설명의 사정상, 본 실시 형태를 AI05 방식, 및 A06(A+B) 방식에 적용하는 케이스를 예로 들어 설명한다. 따라서, 본 실시 형태를 적용 가능한 AI05 방식 등의 기본적인 사고 방식에 대해 간단하게 설명한다.

[0094] AI05 방식 등에서는, 통상의 브로드 캐스트 엔크립션 방식과 마찬가지로, 키 제공 시스템에 포함되는 각 단말 장치를 집합 요소에 대응시키고, 단말 장치 전체의 집합을 고려한다. 그리고, 이 집합을 분할하여 얻어지는 복수의 부분 집합을 사용하여 키 배신을 실행한다. 즉, 이 부분 집합에 의해 단말 장치의 조합이 표현된다. 우선, 키 배신 서버는, 논리 이분목(BT ; Binary Tree)을 형성하여 각 단말 장치를 잎 노드에 대응시킨다. 계속해서, 키 배신 서버는, 소정의 규칙에 준하여 상기한 부분 집합을 요소로 하는 복수의「부분 집합의 집합」을 생성하고, 이 각 부분 집합의 집합을 BT의 뿌리 노드 및 각 중간 노드에 대응시킨다. 또한, 키 배신 서버는, 상기한 부분 집합의 집합에 포함되는 복수의 부분 집합을 소정의 규칙(이하, 점프라 부르는 경우가 있음)에 기초하여 관련시킨다. 그리고, 이 부분 집합간의 관계를 나타내는 것이 유향 그래프 또는 유향 가지이다. 또한, 집합 및 그 집합의 요소인 부분 집합은, 상기한 집합 정보의 일례이다. 또한, AI05 방식 등에 의해 생성되는 유향 그래프는, 상기한 집합 관계 정보의 일례이다. 또한, 그것을 구성하는 유향 가지는, 상기한 키 생성 경로 정보의 일례이다. 단, 상기한 키 생성 경로 정보는, 예를 들어 1개 이상의 유향 가지에 의해 구성되는 키 생성 경로를 나타내는 정보이거나, 또는 공집합에 대응하는 유향 그래프이다.

[0095] 상기한 유향 그래프는, 상기한 부분 집합의 집합에 포함되는 각 부분 집합이 각 좌표점에 대응된 좌표축 상에 형성되고, 상기한 점프에 기초하여 복수의 좌표점간을 연결하는 유향 가지에 의해 구성되어 있다. 키 배신 서버는, 상기한 BT에 포함되는 뿌리 노드 및 각 중간 노드에 대응된 부분 집합의 집합마다, 거기에 포함되는 복수의 부분 집합간의 관계가 표현된 유향 그래프를 형성한다.

[0096] 또한, 키 배신 서버는, 배신처가 되는 단말 장치가 포함되는 부분 집합을 선택하고, 이 부분 집합이 포함되는 유향 그래프를 특정한다. 그리고, 키 배신 서버는, 특정된 유향 그래프에 기초하여 의사 난수 생성기(PRSG ; Pseudo-Random Sequence Generator)에 의한 연산을 반복함으로써 키를 생성한다. AI05 방식의 특징은, 종래의 브로드 캐스트 엔크립션 방식에 비해, 통신량, 각 단말 장치가 유지해야 할 키수, 각 단말 장치가 키 생성에 필요로 하는 계산량을 삭감하도록, 모든 단말 장치를 나타내는 집합을 부분 집합으로 분할하는 점에 있다. 이와 같이, AI05 방식 등을 적용한 키 배신 방식에서는, 유향 그래프를 이용하여 각 단말 장치에 배신하는 키를 생성할 수 있다.

[0097] 또한, A06(A) 방식에서는, 유향 그래프를 구성하는 유향 가지의 길이를 짧게 하는 처리를 가함으로써, 상기한 AI05 방식보다도 각 단말 장치가 유지해야 할 키수를 저감시키는 개량이 실시되어 있다. 또한, A06(B) 방식에서는, 유향 가지의 길이가 길어지도록 유향 그래프를 형성함으로써, 상기한 AI05 방식보다도 각 단말 장치가 키 생성에 필요로 하는 계산량을 저감시키는 개량이 실시되어 있다. 또한, A06(A+B) 방식에서는, A06(B) 방식과 마찬가지로 하여 유향 가지가 긴 유향 그래프를 형성한 후, A06(A) 방식과 마찬가지로 소정의 유향 가지를 짧은 유향 가지로 치환함으로써, 상기한 AI05 방식보다도 각 단말 장치가 키 생성에 필요로 하는 계산량 및 유지해야 할 키수를 저감시키는 개량이 실시되어 있다. 따라서, A06(A), A06(B) 및 A06(A+B)의 각 방식을 적용함으로써, AI05 방식보다도 단말 장치에 걸리는 부하를 저감시킬 수 있다.

[0098] 그러나, 상기한 AI05 방식 등에는, 각 단말 장치가 키를 생성하기 위해 필요한 유향 그래프의 정보를 어떻게 취득할 것인지에 대해 명확한 수단이 개시되어 있지 않고, 각 단말 장치가 미리 유향 그래프의 정보를 모두 유지하고 있거나, 또는 각 단말 장치가 키 배신 서버와 같은 알고리즘에 기초하여 각자 유향 그래프를 생성하고 있다는 암묵의 가정이 존재하고 있다. 그러나, 현실적인 상황을 감안하여, 키 제공 시스템에 포함되는 단말 장치의 수를 상정하면, 각 단말 장치가 유지해야 할 유향 그래프의 정보량, 및 유향 그래프를 생성하기 위한 계산량은 방대하므로, 일반적인 단말 장치가 갖는 한정된 리소스 중에서는 실현이 곤란하다.

[0099] 보다 구체적으로, 상기한 A06(B) 방식의 경우에서 고려해 보면, 통상, 키 제공 시스템에 포함되는 단말 장치의 수 n은 $n=2^{32}$ 정도이므로, 유향 가지 1개의 정보를 4byte 정도로 표현할 수 있었다고 해도, 각 단말 장치가 유지해야 할 정보량은 약 32GByte나 된다. 또한, 각 단말 장치가 유향 그래프를 생성하는 경우에는, 단말 장치의

수 $n=2^{32}$에 대해, (n-1)개의 유향 가지를 산출할 필요가 있으므로, 각 단말 장치가 유향 그래프를 생성하는 데 걸리는 연산 부하는 매우 크다고 할 수 있다.

[0100] 그러나, 상기한 각 방식에서는, 각 단말 장치가 콘텐츠 키 mek를 생성할 때에, 미리 각 단말 장치가 유지하고 있는 각 유향 그래프의 정보를 이용하는 것이 시사되어 있을 뿐이며, 구체적인 수단에 대해서는 나타내어져 있지 않았다. 상기한 바와 같이, 계약자수가 많은 경우에는, 각 단말 장치가 유지해야 할 유향 그래프의 정보량이 방대해지므로, 그 정보를 단말 장치에 저장해 두는 것은 현실적으로 곤란하다. 또한, 각 단말 장치가 각각 유향 그래프를 산출하는 경우에는, 각 단말 장치의 연산량이 방대해져 실현이 곤란하다.

[0101] 따라서, 본 실시 형태에 관한 키 배신 서버는, 각 단말 장치가 키 생성에 필요로 하는 유향 그래프의 정보를 제공하는 구성을 갖는다. 또한, 각 단말 장치는, 키 배신 서버로부터 취득한 유향 그래프의 정보에 기초하여 의사 난수 연산을 실행하여 필요한 키를 생성하는 구성을 갖는다.

[0102] 이상, 본 실시 형태를 적용 가능한 키 배신 방식에 대해 간단하게 설명하였다. 물론, 본 실시 형태를 적용 가능한 키 배신 방식은, 상기한 AI05, A06(A), A06(B), A06(A+B)의 각 방식에 한정되는 것은 아니며, 다른 키 배신 방식에도 적용하는 것이 가능하다. 이하에서는, 설명의 사정상, 본 실시 형태를 AI05 방식 및A06(A+B) 방식에 적용하는 경우에 대해 상세하게 설명하지만, 당업자라면 해당 기재에 기초하여 용이하게 다른 키 배신 방식에의 적용 수단을 상기하는 것이 가능하다.

[0103] [키 제공 시스템(100)의 구성]

[0104] 여기서, 도 1을 참조하면서, 본 발명의 제1 실시 형태에 관한 키 제공 시스템(100)의 구성에 대해 간단하게 설명한다. 도 1은, 본 실시 형태에 관한 키 제공 시스템(100)의 구성을 도시하는 설명도이다.

[0105] 도 1을 참조하면, 키 제공 시스템(100)은, 주로 키 배신 서버(102)와, 단말 장치(122)와, 네트워크(10)에 의해 구성된다. 또한, 키 배신 서버(102)는 키 제공 장치의 일례이다.

[0106] (네트워크(10))

[0107] 네트워크(10)는, 키 배신 서버(102)와 단말 장치(122)를 쌍방향 통신 또는 일방향 통신 가능하게 접속하는 통신 회선망이다. 네트워크(10)는, 예를 들어 인터넷, 전화 회선망, 위성 통신망, 동보 통신로 등의 공중 회선망, WAN(Wide Area Network), LAN(Local Area Network), IP-VPN(Internet Protocol-Virtual Private Network), 무선 LAN 등의 전용 회선망 등에 의해 구성되어 있어 유선/무선을 불문한다.

[0108] (키 배신 서버(102))

[0109] 키 배신 서버(102)는 콘텐츠 배신시에 다양한 전자 데이터를 암호화하여 배신하는 것이 가능하다. 예를 들어, 키 배신 서버(102)는 콘텐츠를 암호화 또는 복호화하기 위한 콘텐츠 키를 생성하여 배신하는 것이 가능하다. 또한, 콘텐츠 키는, 예를 들어 의사 난수 생성기에 의해 산출된 난수(의사 난수), 소정의 문자열, 또는 수열 등에 의해 표현되어 있어도 된다. 또한, 콘텐츠 키는 암호화용 콘텐츠 키와 복호용 콘텐츠 키로 구성되어 있어도 된다. 그리고, 키 배신 서버(102)는, 이 콘텐츠 키를 이용하여, 소정의 암호화 로직에 기초하여 콘텐츠를 암호화할 수 있다. 또한, 키 배신 서버(102)는 콘텐츠 및 콘텐츠 키의 한쪽 또는 양쪽을 임의의 단말 장치(122)에 대해 배신하는 것이 가능하다.

[0110] 또한, 키 배신 서버(102)는 콘텐츠 키를 암호화 또는 복호하기 위한 복수의 세트 키를 생성하는 것이 가능하다. 이때, 키 배신 서버(102)는, 의사 난수 생성기를 이용하여, 소정의 유향 그래프에 기초하여 복수의 세트 키를 생성한다. 또한, 키 배신 서버(102)는 각 세트 키를 이용하여 콘텐츠 키를 암호화하고, 이 암호화된 콘텐츠 키를 소정의 단말 장치(122)에 대해 배신한다. 또한, 키 배신 서버(102)는, 소정의 세트 키를 생성하기 위해 이용한 유향 그래프의 정보를 소정의 단말 장치(122)에 대해 배신하는 것도 가능하다. 또한, 세트 키는, 상기한 키 정보의 일례이다. 또한, 콘텐츠 키는 상기한 키 정보에 의해 암호화/복호되는 정보의 일례이다.

[0111] 상기한 복수의 세트 키는, 각각 다수의 계약자 중으로부터 선택된 복수의 계약자의 부분 집합군에 대응되어 있고, 키 배신 서버(102)는, 콘텐츠의 재생을 허락하는 계약자(이하, 허락 계약자)의 집합만이 콘텐츠 키를 복호할 수 있도록 세트 키를 생성하고, 그것을 이용하여 콘텐츠 키를 암호화하고, 모든 계약자의 단말 장치(122)에 대해 암호화된 콘텐츠 키를 배신한다. 이와 같이, 키 배신 서버(102)는, 콘텐츠뿐만 아니라, 콘텐츠 키도 암호화하여 배신하도록 구성된다. 물론, 콘텐츠를 암호화하여 배신함으로써, 어느 정도의 시큐리티 레벨을 확보할 수 있지만, 다수의 계약자 중에서 콘텐츠의 사용이 허락되는 계약자를 추가 또는 삭제할 때에 플렉시블하게 대

응하기 위해서는 콘텐츠 키를 암호화하여 배신하는 쪽이 유리하다.

[0112] 상기한 구성에 의해, 소정의 단말 장치(122)에만 암호화된 콘텐츠 키를 복호하는 것이 가능해지므로, 소정의 단말 장치(122)만이 콘텐츠를 복호하여 시청할 수 있게 된다. 만약, 허락 계약자의 집합이 변경된 경우에는, 키 배신 서버(102)는 콘텐츠 키의 암호화에 이용하는 세트 키를 변경함으로써 대응 가능하다.

[0113] 또한, 상기한 의사 난수 생성기는, 소정의 시드치를 입력함으로써 장주기의 의사적인 난수열을 출력하는 것이 가능한 장치 또는 프로그램이며, 선형 합동법이나 메르센 트위스터법 등을 이용하여 실현되는 것이다. 물론, 본 실시 형태에 적용 가능한 의사 난수 생성기는, 이에 한정되는 것은 아니며, 다른 로직을 이용하여 의사 난수를 발생시켜도 되고, 혹은 특수한 정보 또는 조건을 포함한 의사 난수열을 생성하는 것이 가능한 장치 또는 프로그램이어도 된다.

[0114] 또한, 키 배신 서버(102)는, 서버 기능을 구비한 퍼스널 컴퓨터(PC ; Personal Computer) 등의 정보 처리 장치에 의해 구성되고, 네트워크(10)를 통해 각종 정보를 외부 장치에 송신 가능하다. 예를 들어, 키 배신 서버(102)는, 브로드 캐스트 엔크립션 방식의 암호키를 생성하여, 이 암호키를 단말 장치(122)에 배신할 수 있다. 또한, 키 배신 서버(102)는, 예를 들어 영상 배신 서비스, 또는 전자 음악 배신 서비스 등의 콘텐츠 배신 서비스를 제공하는 콘텐츠 배신 서버로서의 기능을 구비하고 있어도 되고, 단말 장치(122)에 대해 콘텐츠를 배신하는 것이 가능한 기능을 갖고 있어도 된다. 또한, 키 배신 서버(102)와 콘텐츠 배신 서버를 별도 장치로 하여 구성하는 것도 물론 가능하다.

[0115] 여기서, 콘텐츠라 함은, 예를 들어 영화, 텔레비전 프로그램, 비디오 프로그램, 도표 등의 동화상 또는 정지 화상을 포함하는 영상(Video) 콘텐츠, 음악, 강연, 라디오 프로그램 등의 음성(Audio) 콘텐츠, 게임 콘텐츠, 문서 콘텐츠, 또는 소프트웨어 등이 포함되는 임의의 콘텐츠 데이터이어도 된다. 또한, 영상 콘텐츠라 함은, 영상 데이터뿐만 아니라, 음성 데이터를 포함하고 있어도 된다.

[0116] (단말 장치(122))

[0117] 단말 장치(122)는, 키 배신 서버(102)로부터 다양한 정보를 수신할 수 있다. 예를 들어, 단말 장치(122)는 키 배신 서버(102)에 의해 배신된 콘텐츠 또는 콘텐츠 키를 수신할 수 있다. 또한, 단말 장치(122)는 키 배신 서버(102)로부터 수신한 콘텐츠 키를 이용하여 암호화된 콘텐츠를 복호할 수 있다. 단, 키 배신 서버(102)로부터 송신되는 콘텐츠 또는 콘텐츠 키는, 소정의 세트 키에 의해 암호화되어 있으므로, 그 콘텐츠 또는 콘텐츠 키를 복호해야만 한다. 따라서, 단말 장치(122)는 키 배신 서버(102)로부터 취득한 소정의 세트 키를 이용하여 암호화된 콘텐츠 또는 콘텐츠 키를 복호할 수 있다. 또한, 단말 장치(122)는 미리 유지하고 있는 세트 키 또는 소정의 세트 키를 생성 가능한 중간 키를 이용하여, 키 배신 서버(102)가 콘텐츠 또는 콘텐츠 키를 암호화할 때에 이용한 세트 키를 생성할 수 있다. 이때, 단말 장치(122)는, 키 배신 서버(102)로부터 취득한 유향 그래프에 관한 정보에 기초하여, 자기가 유지하는 세트 키 또는 중간 키를 의사 난수 생성기에 입력하여 원하는 세트 키를 생성할 수 있다. 또한, 중간 키는 상기한 키 정보의 일례이다.

[0118] 상기한 구성에 의해, 단말 장치(122)는 원하는 세트 키를 생성하기 위해 필요한 유향 그래프를 생성할 필요가 없어지고, 유지해야 할 정보량을 저감시키는 것이 가능한 데다가, 세트 키의 생성에 걸리는 연산 부하를 저감시키는 것이 가능해진다.

[0119] 또한, 단말 장치(122)는, 네트워크(10)를 통해 외부 장치와 데이터 통신이 가능한 단말 장치이며, 각 계약자에 의해 소유된다. 단말 장치(122)는, 예를 들어 도시한 바와 같이 퍼스널 컴퓨터 등의 정보 처리 장치에 의해 구성되지만, 이러한 예에 한정되지 않고, 네트워크(10)를 통해 정보 통신이 가능한 통신 기능을 갖는 기기이면, 예를 들어 PDA(Personal Digital Assistant), 가정용 게임기, DVD/HDD 레코더, 또는 텔레비전 수상기 등의 정보 가전 제품, 텔레비전 방송용 튜너나 디코더 등에 의해 구성하는 것도 가능하다. 또한, 단말 장치(122)는, 예를 들어 휴대형 게임기, 휴대 전화, 휴대형 영상/음성 플레이어, PDA, 또는 PHS 등의 계약자가 운반 가능한 휴대 단말기(Portable Device)이어도 된다.

[0120] 이상, 본 실시 형태에 관한 키 제공 시스템(100)의 구성에 대해 간단하게 설명하였다. 다음에, 키 제공 시스템(100)을 구성하는 키 배신 서버(102) 및 단말 장치(122)의 하드웨어 구성의 구체예에 대해 간단하게 설명한다.

[0121] [키 배신 서버(102) 및 단말 장치(122)의 하드웨어 구성]

[0122] 여기서, 도 2를 참조하면서, 본 실시 형태에 관한 키 배신 서버(102) 및 단말 장치(122)의 하드웨어 구성에 대해 간단하게 설명한다. 도 2는, 본 실시 형태에 관한 키 배신 서버(102) 또는 단말 장치(122)의 기능을 실현

가능한 하드웨어 구성의 일례이다.

[0123] 도 2를 참조하면, 키 배신 서버(102) 및 단말 장치(122)는, 예를 들어 컨트롤러(202)와, 연산 유닛(204)과, 입출력 인터페이스(206)와, 시큐어 기억부(208)와, 메인 기억부(210)와, 네트워크 인터페이스(212)와, 미디어 인터페이스(216)에 의해 구성된다.

[0124] (컨트롤러(202))

[0125] 컨트롤러(202)는 버스를 통해 다른 구성 요소에 접속되어 있고, 주로 메인 기억부(210)에 저장된 프로그램 및 데이터에 기초하여 장치 내의 각 부를 제어하는 역할을 담당한다. 또한, 컨트롤러(202)는 CPU(Central Processing Unit) 등의 연산 처리 장치에 의해 구성되어 있어도 된다.

[0126] (연산 유닛(204)(키 배신 서버(102)의 경우))

[0127] 키 배신 서버(102)가 구비하는 연산 유닛(204)은, 예를 들어 콘텐츠의 암호화, 콘텐츠 키의 암호화, 유향 그래프의 생성, 세트 키의 생성 및 세트 키를 생성하기 위해 이용하는 중간 키의 도출을 실행할 수 있다. 따라서, 연산 유닛(204)은, 소정의 데이터(시드치 등)에 기초하여 의사 난수를 발생시키는 의사 난수 생성기로서 기능할 수 있는 동시에, 소정의 알고리즘에 기초하여 콘텐츠 또는 콘텐츠 키를 암호화하는 것이 가능하다. 또한, 상기 소정의 알고리즘은, 연산 유닛(204)이 판독 가능한 프로그램으로서 메인 기억부(210)에 저장되어 있어도 된다. 또한, 상기 소정의 데이터는 메인 기억부(210) 또는 시큐어 기억부(208)에 저장되어 있어도 된다. 또한, 연산 유닛(204)은, 상기한 각종 연산 처리를 실행하여 얻어진 출력 결과를 메인 기억부(210) 또는 시큐어 기억부(208)에 기록할 수 있다. 또한, 연산 유닛(204)은 CPU 등의 연산 처리 장치에 의해 구성된다. 또한, 연산 유닛(204)은, 상기한 컨트롤러(202)와 일체로 형성되어 있어도 된다.

[0128] (연산 유닛(204)(단말 장치(122)의 경우))

[0129] 단말 장치(122)가 구비하는 연산 유닛(204)은, 예를 들어 콘텐츠의 복호, 콘텐츠 키의 복호, 세트 키의 생성, 및 세트 키를 생성하기 위해 이용하는 중간 키의 생성을 실행할 수 있다. 따라서, 연산 유닛(204)은 소정의 데이터(시드치 등)에 기초하여 의사 난수를 발생시키는 의사 난수 생성기로서 기능할 수 있는 동시에, 소정의 알고리즘에 기초하여 콘텐츠 또는 콘텐츠 키를 복호하는 것이 가능하다. 또한, 소정의 알고리즘은, 연산 유닛(204)이 판독 가능한 프로그램으로서 메인 기억부(210)에 저장되어 있어도 된다. 또한, 소정의 데이터는, 메인 기억부(210) 또는 시큐어 기억부(208)에 저장되어 있어도 된다. 또한, 연산 유닛(204)은 상기한 각종 연산 처리를 실행하여 얻어진 출력 결과를 메인 기억부(210) 또는 시큐어 기억부(208)에 기록하는 것이 가능하다. 또한, 연산 유닛(204)은, 예를 들어 CPU 등의 연산 처리 장치에 의해 구성된다. 또한, 연산 유닛(204)은 상기한 컨트롤러(202)와 일체로 형성되어 있어도 된다.

[0130] (입출력 인터페이스(206))

[0131] 입출력 인터페이스(206)는, 주로 유저가 데이터를 입력하기 위한 입력 디바이스와, 연산 결과 또는 콘텐츠의 내용을 출력하는 출력 디바이스에 접속되어 있다. 예를 들어, 입력 디바이스는 키보드, 마우스, 트랙볼, 터치 펜, 키패드, 또는 터치 패널 등이어도 된다. 이들 입력 디바이스는 입출력 인터페이스(206)에 대해 유선 또는 무선에 의해 접속되어 있어도 된다. 또한, 입력 디바이스는, 유선 또는 무선에 의해 접속된 휴대 전화나 PDA 등의 휴대 정보 단말기이어도 된다. 한편, 출력 디바이스는, 예를 들어 디스플레이 등의 표시 장치, 또는 스피커 등의 음성 출력 디바이스 등이어도 된다. 그리고, 출력 디바이스는 입출력 인터페이스(206)에 대해 유선 또는 무선에 의해 접속되어 있어도 된다. 또한, 상기한 입출력 디바이스는, 키 배신 서버(102) 또는 단말 장치(122)에 대해 일체로서 형성되어 있어도 된다.

[0132] 또한, 입출력 인터페이스(206)는, 버스를 통해 다른 구성 요소에 접속되어 있고, 입출력 인터페이스(206)를 통해 입력된 데이터를 메인 기억부(210) 등에 전달하는 것이 가능하다. 반대로, 입출력 인터페이스(206)는, 메인 기억부(210) 등에 저장된 데이터, 네트워크 인터페이스(212) 등을 통해 입력된 데이터, 또는 연산 유닛(204)에 의해 해당 데이터에 기초하여 연산하여 얻어진 결과 등을 출력 디바이스에 출력할 수 있다.

[0133] (시큐어 기억부(208))

[0134] 시큐어 기억부(208)는, 주로 콘텐츠 키, 세트 키, 및 중간 키 등의 은닉이 필요한 데이터를 안전하게 저장하기 위한 기억 장치이다. 시큐어 기억부(208)는, 예를 들어 하드 디스크 등의 자기 기억 장치, 광 디스크 등의 광 기억 장치, 광자기 기억 장치, 또는 반도체 기억 장치 등에 의해 구성되어 있어도 된다. 또한, 시큐어 기억부

(208)는, 예를 들어 내탬퍼성을 갖는 기억 장치에 의해 구성되어 있어도 된다.

[0135] (메인 기억부(210))

[0136] 메인 기억부(210)는, 예를 들어 콘텐츠 또는 콘텐츠 키 등을 암호화하기 위한 암호화 프로그램, 암호화된 콘텐츠 또는 콘텐츠 키 등을 복호하기 위한 복호 프로그램, 또는 세트 키나 중간 키를 생성하기 위한 키 생성 프로그램 등이 저장되어 있어도 된다. 또한, 메인 기억부(210)는 연산 유닛(204)으로부터 출력된 계산 결과를 일시적 또는 영속적으로 저장하거나, 입출력 인터페이스(206), 네트워크 인터페이스(212), 또는 미디어 인터페이스(216) 등으로부터 입력된 데이터를 저장해도 된다. 메인 기억부(210)는, 예를 들어 하드 디스크 등의 자기 기억 장치, 광 디스크 등의 광 기억 장치, 광 자기 기억 장치, 또는 반도체 기억 장치 등에 의해 구성되어 있어도 된다.

[0137] (네트워크 인터페이스(212))

[0138] 네트워크 인터페이스(212)는 네트워크(10)를 통해 다른 통신 장치 등에 접속되어 있고, 예를 들어 암호화된 콘텐츠 또는 콘텐츠 키, 세트 키, 중간 키 등의 데이터, 암호화에 이용하는 파라미터 정보, 및 허락 계약자의 집합에 관한 데이터를 송수신하기 위한 인터페이스 수단이다. 네트워크 인터페이스(212)는, 버스를 통해 다른 구성 요소에 접속되어 있고, 네트워크(10) 상에 있는 외부 장치로부터 수신한 데이터를 다른 구성 요소에 전달하고, 또는 다른 구성 요소가 갖는 데이터를 네트워크(10) 상에 있는 외부 장치에 송신하는 것이 가능하다.

[0139] (미디어 인터페이스(216))

[0140] 미디어 인터페이스(216)는 정보 미디어(218)를 착탈하여 데이터를 판독 기입하기 위한 인터페이스이며, 버스를 통해 다른 구성 요소에 접속되어 있다. 이 미디어 인터페이스(216)는, 예를 들어 장착된 정보 미디어(218)로부터 데이터를 판독하여 다른 구성 요소에 전달하거나, 또는 다른 구성 요소로부터 공급된 데이터를 정보 미디어(218)에 기입하는 것이 가능하다. 정보 미디어(218)는, 예를 들어 광 디스크, 자기 디스크, 반도체 메모리 등의 포터블 기억 매체(착탈 가능한 기억 매체)이어도 되고, 또는 네트워크(10)를 거치지 않고 비교적 근거리에서 유선/무선 접속된 정보 단말기의 기억 매체 등이어도 된다.

[0141] 이상, 본 실시 형태에 관한 키 배신 서버(102) 및 단말 장치(122)의 기능을 실현 가능한 하드웨어 구성의 일례를 나타냈다. 상기한 각 구성 요소는, 범용적인 부재를 사용하여 구성되어 있어도 되고, 각 구성 요소의 기능에 특화한 전용의 하드웨어에 의해 구성되어 있어도 된다. 따라서, 본 실시 형태를 실시하는 때때로의 기술 레벨에 따라서, 적절하게 이용하는 하드웨어 구성을 변경하는 것이 가능하다. 또한, 상기한 하드웨어 구성은, 어디까지나 일례이며, 이에 한정되는 것이 아닌 것은 물론이다. 예를 들어, 컨트롤러(202)와 연산 유닛(204)을 동일한 연산 장치에 의해 구성해도 되고, 시큐어 기억부(208)와 메인 기억부(210)를 동일한 기억 장치에 의해 구성해도 된다. 또한, 이용 형태에 따라서는, 미디어 인터페이스(216), 또는 입출력 인터페이스(206) 등을 생략하는 구성도 가능하다.

[0142] [본 실시 형태를 적용 가능한 키 배신 방식]

[0143] 다음에, 본 실시 형태를 적용 가능한 키 배신 방식의 예로서, AI05 방식과 A06(A+B) 방식에 대해 상세하게 설명한다. 물론, 본 실시 형태를 적용 가능한 키 배신 방식이 이에 한정되지 않는 것은 물론이고, 당업자라면 이하의 기재로부터 다른 키 배신 방식에 본 실시 형태를 적용하는 수단을 용이하게 상기하는 것이 가능하다.

[0144] (AI05 방식)

[0145] 여기서, 본 실시 형태를 적용 가능한 AI05 방식에 대해 설명한다. AI05 방식은, 콘텐츠가 배신되는 단말 장치(122)의 집합을 복수의 부분 집합으로 나누고, 각 부분 집합에 대응된 세트 키에 의해 콘텐츠 키를 암호화하여 배신하는 방식이다. 또한, 이하에서 설명하는 각 처리는, 주로 키 배신 서버(102)에 의해 실행되는 것이지만, 단말 장치(122)에 있어서도, 콘텐츠 또는 콘텐츠 키를 복호하기 위한 키를 생성하기 위해 하기 알고리즘의 적어도 일부가 이용될 수 있다.

[0146] AI05 방식에서는, 콘텐츠 배신의 대상이 되는 단말 장치(122)의 집합을 복수의 부분 집합으로 나누어 고려한다. 따라서, 도 3을 참조하면서, AI05 방식에 관한 부분 집합의 나누는 방법에 대해 설명한다. 물론, 부분 집합의 나누는 방법은 1가지는 아니지만, AI05 방식에서는, 이분목 구조를 이용한 부분 집합의 나누는 방법을 채용하고 있다. AI05 방식에서는, 이분목 구조를 형성하는 각 결절점(노드)에 대해, 노드간의 위치 관계를 고려하여 소정의 부분 집합을 대응시킴으로써, 소정의 조합을 갖는 단말 장치(122)의 부분 집합을 망라적으로 선택한다. 우선, 도 3을 참조하면서, 이분목 구조의 구축 방법에 대해 설명한다. 또한, 그 설명에 이용하는 표현을 하기

와 같이 정의한다.

[0147] (각종 정의)

[0148] ·모든 단말 장치(계약자)의 집합 N={1,…, n}(n은 2의 멱승)

[0149] 자연수 i 및 j(단, i≤j)에 대해,

[0150] ·[i, j]={i, i+1,…, j}

[0151] ·(i→i)=(i←i)={{i}}

[0152] ·(i→j)={{i}, {i, i+1},…, {i, i+1,…, j}}

[0153] ={[i, i], [i, i+1],…, [i, j]}

[0154] ·(i←j)={{j}, {j, j-1},…, {j, j-1,…, i}}

[0155] ={[j, j], [j, j-1],…, [j, i]}

[0156] 또한, 이분목 구조 상의 말단에 위치하는 노드를 잎 노드, 정점에 위치하는 노드를 뿌리 노드, 뿌리 노드와 잎 노드 사이에 위치하는 각 노드를 중간 노드라 부르기로 한다. 또한, 각 잎 노드는 각 단말 장치(122)에 대응되어 있다. 도 3의 예에서는, BT의 잎 노드수 n이 n=64인 경우가 나타내어져 있다.

[0157] (이분목 구조의 형성)

[0158] 우선, 잎 노드의 수가 n(예를 들어, n=64)이 되도록 BT를 작성한다. 그리고, 각 잎 노드에 대해, 좌측 단부로부터 우측 방향을 향해 번호 1,…, n을 대응시킨다. 즉, 번호 1,…, n은, 각 단말 장치(122)에 대응된다. 계속해서, 어느 중간 노드 v에 할당하는 부분 집합을 규정하기 위한 지표 l_v 및 r_v를 정의한다. 또한, 어느 중간 노드 v의 하위에 위치하는 잎 노드 중, 가장 좌측에 있는 잎 노드의 번호를 l_v, 가장 우측에 있는 잎 노드의 번호를 r_v라 정의한다. 또한, 중간 노드 v는, v를 지표로 하는 BT 상의 중간 노드를 나타낸다.

[0159] 다음에, BT 상의 중간 노드를 2개의 집합으로 분류한다. BT 상의 중간 노드 중, 친(親) 노드의 좌측에 위치하는 중간 노드의 집합을 BT_L이라 정의하고, 친 노드의 우측에 위치하는 중간 노드의 집합을 BT_R이라 정의한다. 또한, BT 상에서 접속된 2개의 노드간의 위치 관계에 대해, 상위에 위치하는 노드를 친 노드라 부르고, 하위에 위치하는 노드를 자 노드라 부르기로 한다.

[0160] (뿌리 노드에 대한 집합의 대응시키기)

[0161] 다음에, BT 상의 뿌리 노드에 대응시키는 집합을 설정한다. 뿌리 노드에는, 그 하위에 모든 잎 노드가 연결되어 있으므로, 모든 단말 장치(122)의 일부 또는 전부가 포함되는 부분 집합을 요소에 갖는 집합이 대응된다. 즉, 뿌리 노드에 대응시키는 집합으로서, 집합 (1→n)과 집합 (2←n)이 설정된다. 예를 들어, 도 3의 뿌리 노드에는, 집합 (1→64)와 집합 (2←64)가 대응된다.

[0162] 이 대응시키기는, 이하의 이유에 의한다. 상기한 정의에 의해, 집합 (1→64)는, 부분 집합 [1, 1],…, [1, 64]를 요소로 하여 포함되어 있으므로, 모든 단말 장치(122)(번호 1 내지 64)를 포함하는 단말 장치(122)의 그룹을 [1, 64]={1,…, 64}에 의해 표현할 수 있다. 마찬가지로, 부분 집합 [1, 15]와 부분 집합 [64, 17]을 이용함으로써, 번호 16의 단말 장치(122)를 제외한 모든 단말 장치(122)를 표현할 수 있다. 이때, 부분 집합 [1, 15]는 집합 (1→64)에 포함되어 있고, 부분 집합 [64, 17]은 집합 (2←64)에 포함되어 있다. 즉, 뿌리 노드에 대응된 집합의 부분 집합을 이용함으로써, 뿌리 노드의 하위에 위치하는 잎 노드[즉, 단말 장치(122)]의 임의의 조합을 표현할 수 있는 것이다.

[0163] (중간 노드에 대한 집합의 대응시키기)

[0164] 다음에, BT 상의 각 중간 노드에 부분 집합을 대응시킨다. 우선, 모든 v에 대해, 상기한 집합 BT_L에 속하는 중간 노드 v에 집합 $(l_v+1\leftarrow r_v)$를 대응시킨다. 마찬가지로, 모든 v에 대해, 상기한 집합 BT_R에 속하는 중간 노드 v에 집합 $(l_v\rightarrow r_v-1)$을 대응시킨다. 도 3에는, 각 중간 노드에 대응된 집합이 기재되어 있다.

[0165] 예를 들어, 집합 (2←4)가 대응된 중간 노드를 참조하면, 이 중간 노드의 하위에 위치하는 2개의 중간 노드에는, 집합 (2←2)와 집합 (3→3)이 대응되어 있다. 또한, 2개의 중간 노드의 하위에는, 번호 1 내지 4의

잎 노드가 연결되어 있다. 따라서, 번호 3을 제외한 잎 노드의 조합을 표현하는 경우에는, {[1, 1], [2, 2], [4, 4]} 또는 {[1, 2], [4, 4]}라는 부분 집합의 세트를 대응시키면 된다. 부분 집합 [1, 1] 및 [1, 2]는, 뿌리 노드에 할당된 집합 (1→64)의 요소이며, 부분 집합 [2, 2] 및 [4, 4]는, 각각 집합 (2←2) 및 (2←4)의 요소이다. 즉, 각 중간 노드에 대응된 집합의 부분 집합을 이용함으로써, 잎 노드[단말 장치(122)]의 원하는 조합을 표현할 수 있다.

[0166] 상기한 바와 같이, AI05 방식에서는, BT를 사용하여 단말 장치(122)의 조합을 나타내는 부분 집합의 세트를 정의하고 있다. 또한, 상기한 부분 집합에 의해 형성된 전체 집합을 세트 시스템(SS)이라 부르기로 한다. 또한, 세트 시스템(SS)은, 하기 수학식 1과 같이 수학적으로 표현된다.

수학식 1

[0167] $$SS=\left\{\bigcup_{v\in BT_L}(l_v+1\leftarrow r_v)\right\}\cup\left\{\bigcup_{v\in BT_R}(l_v\rightarrow r_v-1)\right\}\cup(1\rightarrow n)\cup(2\leftarrow n)$$

[0168] 이상, AI05 방식에 있어서의 이분목 구조의 형성 방법에 대해 설명하였다. AI05 방식의 기본 개념은, 상기한 각 부분 집합에 대해, 콘텐츠 또는 콘텐츠 키를 암호화하기 위한 복수의 세트 키를 생성하고, 각 세트 키에 의해 콘텐츠 또는 콘텐츠 키를 암호화하여 소정의 단말 장치(122)에 대해 배신하는 것에 있다. 지금까지의 기재로부터는 그다지 명시적은 아닐지도 모르지만, 상기한 규칙에 따라서 부분 집합을 정의함으로써, 단말 장치(122)의 조합을 효율적으로 분류하는 수단이 제공 가능해진다. 이하에서는, 상기한 부분 집합을 이용하여 세트 키를 생성하는 알고리즘에 대해 설명한다.

[0169] (유향 그래프의 생성)

[0170] 여기서, 도 4를 참조하면서, 세트 키를 생성하기 위한 알고리즘에 대해 설명한다. 이 알고리즘은, 복수의 유향 가지에 의해 형성되는 유향 그래프에 의해 표현된다. 따라서, 이 유향 그래프의 생성 방법에 대해 상세하게 설명한다. 우선, 콘텐츠 키를 암호화하는 세트 키와, 세트 키를 생성하기 위한 중간 키에 대해 설명한다.

[0171] AI05 방식에서는, 세트 키를 생성하기 위해 의사 난수 생성기 PRSG를 사용한다. 이 PRSG는, 어느 부분 집합 S_0에 대응하는 중간 키 $t(S_0)$가 입력되면, 부분 집합 S_0에 대응하는 세트 키 $k(S_0)$와, 부분 집합 S_1, S_2,…, S_k에 대응하는 중간 키 $t(S_1)$, $t(S_2)$,…, $t(S_k)$를 출력한다. 여기서, 부분 집합 S_0과, 다른 부분 집합 S_1,…, S_k의 관계는, 후술하는 유향 그래프에 의해 규정된다.

[0172] 또한, 집합 S_0, S_1,…, S_k는, 상기한 세트 시스템(SS)을 구성하는 부분 집합 중 어느 하나이며, 상기한 바와 같이, 단말 장치(122)의 조합을 표현하는 것이다. AI05 방식의 특징은, PRSG의 입력[예를 들어, $t(S_0)$]과 출력[예를 들어, $k(S_0)$, $t(S_1)$,…, $t(S_k)$]의 관계를 규정하는 로직이 표현된 유향 그래프의 형상에 있다. 따라서, AI05 방식에 관한 유향 그래프의 생성 방법에 대해 설명한다. 우선, 이하에서 사용하는 기호 등을 정의한다.

[0173] (각종 정의)

[0174] ・부분 집합 S_i에 대응하는 중간 키 : $t(S_i)$

[0175] ・부분 집합 S_i에 대응하는 세트 키 : $k(S_i)$

[0176] ・콘텐츠 키 : mek

[0177] ・의사 난수 생성기 : PRSG

[0178] ・유향 가지 : E

[0179] ・유향 패스(경로) : P

[0180] ・유향 그래프 : H

[0181] ・부분 집합 S_i에 대응하는 좌표점을 시작점으로 하는 유향 가지의 수 : d

[0182] 또한, 집합 (i→j), 또는 집합 (i←j)에 대응하는 AI05 방식의 유향 그래프를 H(i→j), 또는 H(i←j)로 표기한다. 또한, 유향 패스 P는 상기한 키 생성 경로 정보의 일례이다. 또한, PRSG의 입출력을 하기 수학식 2와 같

이 표기한다. 이는, PRSG에 중간 키 $t(S_0)$가 입력된 결과, 세트 키 $k(S_0)$와, 복수의 중간 키 $t(S_1),\cdots, t(S_d)$가 출력된 것을 나타낸다.

수학식 2

[0183] $$t(S_1)\,||\,\cdots\,||\,t(S_d)\,||\,k(S_0) \leftarrow PRSG(t(S_0))$$

[0184] (알고리즘)

[0185] 우선, 파라미터 k(k는 자연수)를 결정한다. 단, 간단하게 하기 위해, k|log(n)(이하, log의 밑은 2)로 한다. 파라미터 k는, 결과적으로 단말 장치(122)가 유지해야 할 중간 키의 개수, 및 단말 장치(122)가 세트 키를 생성하는 데 필요한 계산량에 관계된다. 따라서, 파라미터 k는 실시 형태에 따라서 적절하게 설정되어야 하는 파라미터이다. 도 4의 예에서는 k=6으로 설정하고 있다.

[0186] 여기서, 도 4를 참조하면서, 어느 중간 노드 v에 대응하는 유향 그래프 $H(l_v \rightarrow r_v-1)$에 관하여, 유향 그래프의 생성 방법에 대해 구체적으로 설명한다.

[0187] (스텝 1)

[0188] 우선, 유향 그래프 $H(l_v \rightarrow r_v-1)$를 구성하기 위한 수평 좌표축을 설정한다. 이 수평 좌표축의 각 좌표점에는, 집합 $(l_v \rightarrow r_v-1)$을 구성하는 각 부분 집합 S_i가 대응된다. 단, 각 좌표점에 대응되는 부분 집합 S_i는, 좌측으로부터 우측을 향해 포함 관계가 커지도록 배치된다. 예를 들어, 유향 그래프 H(5→7)=H({[5, 5], [5, 6], [5, 7]})를 예로 들면, 수평 좌표축의 좌표점에는, 좌측으로부터 차례로 부분 집합 [5, 5], [5, 6], [5, 7]이 대응된다.

[0189] 또한, 도 4를 참조하면, 각 유향 그래프 H가 형성되는 수평 좌표축에 대해 직교하는 복수의 세로선 z(z=1 내지 64)가 그어져 있다. 이 세로선 z와 유향 그래프 H의 교점이 상기한 좌표치를 나타내고 있다. 예를 들어, 유향 그래프 $H(l_v+1 \leftarrow r_v)$와 세로선 z의 교점은, 부분 집합 $[r_v, z]$에 대응된 좌표점을 나타내고, 유향 그래프 $H(l_v \rightarrow r_v-1)$와 세로선 z의 교점은, 부분 집합 $[l_v, z]$에 대응된 좌표점을 나타낸다. 이하, 부분 집합 S_i에 대응된 좌표점인 것은 좌표점 S_i로 표기하는 경우가 있다.

[0190] 상기한 규칙에 준하여 수평 좌표축이 설정된 후, 수평 좌표축 상의 가장 좌측에 위치하는 좌표점의 좌측에 1개의 임시 좌표점을 설정한다. 또한, 수평 좌표축의 가장 우측에 위치하는 좌표점의 우측에 1개의 임시 좌표점을 설정한다. 그리고, 좌측 단부의 임시 좌표점을 시작점으로 하고, 우측 단부의 임시 좌표점을 종점으로 한다. 또한, 좌측 단부에 위치하는 임시 좌표점으로부터 우측 단부에 위치하는 임시 좌표점까지의 길이 L_v는 $L_v=r_v-l_v+1$이 된다.

[0191] (스텝 2) 유향 그래프 $H(l_v \rightarrow r_v-1)$를 형성하는 유향 가지를 설정한다.

[0192] (2-1) $n^{(x-1)/k}<L_v \leq n^{x/k}$를 만족하는 정수 x를 산출한다. 단, 정수 x는 $1 \leq x \leq k$이다.

[0193] (2-2) 카운터 i를 0부터 x-1까지 움직이면서, 다음 조작을 반복하여 실행한다. 수평 좌표축 상의 시작점부터 개시하여, 유향 가지의 종단부가 수평 좌표축 상의 종점에 도달하거나, 혹은 다음에 형성되는 유향 가지의 종단부가 수평 좌표축 상의 종점을 초과할 때까지, 그 좌표점으로부터 $n^{i/k}$만큼 이격된 좌표점으로 연장되는 우측 방향의 유향 가지(즉, 그 좌표점으로부터 $n^{i/k}$만큼 이격된 좌표점으로의 점프)를 반복하여 생성한다.

[0194] (스텝 3)

[0195] 임시 좌표점을 시작점 또는 종점으로 하는 유향 가지를 모두 삭제한다.

[0196] (스텝 4)

[0197] 어느 좌표점에 도달하는 유향 가지가 복수 있는 경우, 최장의 유향 가지만을 남기고 다른 유향 가지를 모두 삭제한다.

[0198] 상기한 알고리즘(스텝 1 내지 스텝 4)을 실행함으로써, 유향 그래프 $H(l_v \rightarrow r_v-1)$를 구축할 수 있다.

[0199] 여기서, 도 4의 유향 그래프 H(33→63)를 예로 들어 유향 그래프의 구성에 대해 구체적으로 설명한다. 유향 그래프 H(33→63)는 복수의 아치 형상의 곡선과, 각 아치 형상의 곡선의 일단부에 접속되어 수평 방향으로 연신한 직선에 의해 구성된다. 이 아치 형상의 곡선과 수평 방향으로 연신한 직선이 유향 가지이다. 그리고, 각 유향 가지의 단부와 세로선의 교점이 수평 좌표축의 좌표점이다. 또한, 연결한 복수의 유향 가지에 의해 형성되는 좌표점간의 경로를 유향 패스라 부르기로 한다.

[0200] 또한, 유향 그래프 H(33→63)의 상측에 표시된 백색의 화살표는 유향 가지의 방향을 나타내고 있다. 이 유향 그래프(33→63)는, l_v=33, r_v=64, k=6, n=64의 케이스에 있어서, 상기한 알고리즘을 실행한 결과로서 얻어진 것이다. 또한, 도 4의 최하단에 그려진 흑색 동그라미는, 좌측으로부터 각각 유향 그래프 H(2←2),…, H(63→63)를 나타내고 있다.

[0201] 상기한 알고리즘은, 우측 방향의 유향 그래프 $H(l_v \rightarrow r_v-1)$를 생성하기 위한 것이었지만, 좌측 방향의 유향 그래프 $H(l_v+1 \leftarrow r_v)$에 대해서도 같은 알고리즘을 적용하여 생성하는 것이 가능하다. 단, 유향 그래프 $H(l_v+1 \leftarrow r_v)$ 및 H(2←n)를 형성하는 수평 좌표축을 설정하는 경우, 수평 좌표축 상에 우측으로부터 좌측을 향해 포함 관계가 커지도록 부분 집합 S_i를 배열하는 점, 및 유향 가지의 방향을 좌측 방향으로 하는 점에 주의할 필요가 있다.

[0202] 이상, AI05 방식에 관한 유향 그래프 H의 생성 방법에 대해 설명하였다. 이하에서는, 유향 그래프 H를 이용하여 세트 키를 생성하는 로직에 대해 설명한다.

[0203] (세트 키의 생성)

[0204] AI05 방식에서는, 세트 시스템(SS)을 구성하는 각 부분 집합 S_i에 대응하는 각 세트 키 $k(S_i)$를 이용하여 콘텐츠 키 mek가 암호화된다. 또한, 상기한 바와 같이, 유향 그래프 H의 각 좌표점은, 단말 장치(122)의 조합을 나타내는 부분 집합 S_i에 대응한다. 그리고, 세트 키 $k(S_i)$ 및 중간 키 $t(S_i)$는, 상기한 각 부분 집합 S_i에 대응되어 있다. 이들 대응 관계를 근거로 하여, 유향 그래프 H에 기초하여 세트 키 $k(S_i)$를 생성하는 방법에 대해 설명한다.

[0205] 이하, 좌표점 S_0을 시단부로 하는 1개 이상의 유향 가지의 종단부가 나타내는 좌표점을 그 유향 가지의 시단부 S_0에 가까운 순(유향 가지가 짧은 순)으로 S_1, S_2,…, S_k로 표현한다. 단, 좌표점 S_0을 시단부로 하는 유향 가지의 개수가 q개(q<k)인 경우, 좌표점 $S_{(q+1)}$, $S_{(q+2)}$,…, S_k는 더미로서 카운트하지만 실제로는 사용하지 않는다. 또한, 상기한 (스텝 2-2)에 있어서의 반복 처리의 횟수가 x회($1 \leq x \leq k$)이므로, 유향 그래프 H의 각 좌표점을 시단부로 하는 유향 가지의 개수는 최대로 k개이다.

[0206] AI05 방식에 따르면, λ비트의 입력에 대해 (k+1)*λ비트를 출력하는 PRSG를 이용하여 세트 키 $k(S_i)$를 생성한다. 이 PRSG는, 좌표점 S_0에 대응하는 중간 키 $t(S_0)$를 입력하면, 좌표점 S_0을 시단부로 하는 유향 가지가 도달하는 각 좌표점(예를 들어, 좌표점 S_1, S_2,…, S_k)에 대응하는 중간 키 $t(S_1)$, $t(S_2)$,…, $t(S_k)$와, 입력한 중간 키(S_0)에 대응하는 세트 키 $k(S_0)$가 출력된다. 즉, $t(S_1)||\cdots||t(S_k)||k(S_0) \leftarrow PRSG(t(S_0))$가 된다. 따라서, PRSG의 출력을 좌측으로부터 λ비트마다 구획함으로써, 중간 키 $t(S_1)$, $t(S_2)$,…, $t(S_k)$와, 세트 키 $k(S_0)$를 생성할 수 있다.

[0207] 예를 들어, 도 4를 참조하여, 유향 그래프 H(1→64)의 좌표점 S_0=[1, 8](좌측 단부로부터 8번째의 좌표점)에 주목하면, 좌표점 S_0으로부터는 4개의 유향 가지가 나와 있는 것을 알 수 있었다. 이 유향 가지의 종점은, 각각 좌표점 S_1=[1, 9], S_2=[1, 10], S_3=[1, 12], S_4=[1, 16]이다. 따라서, 중간 키 $t(S_0)$를 PRSG에 입력하면, 세트 키 $k(S_0)$와, 중간 키 $t(S_1)$, $t(S_2)$, $t(S_3)$, $t(S_4)$를 생성할 수 있다. 또한, 중간 키 $t(S_4)$를 PRSG에 입력함으로써, 세트 키 $k(S_4)$와, S_{11}=[1, 17], S_{12}=[1, 18], S_{13}=[1, 20], S_{14}=[1, 24], S_{15}=[1, 32]에 대응하는 중간 키 $t(S_{11})$, $t(S_{12})$, $t(S_{13})$, $t(S_{14})$, $t(S_{15})$를 생성할 수 있다. 이와 같이, PRSG를 반복하여 사용함으로써 복수의 세트 키를 산출할 수 있다.

[0208] 상기한 바와 같이, 소정의 중간 키 $t(S_0)$를 유지하고 있으면, 유향 그래프 H에 기초하여 중간 키와 세트 키를 생성하는 것이 가능해진다. 그러나, 유향 그래프 H의 정보를 참조할 수 없는 경우에는, 소정의 중간 키 $t(S_0)$를 PRSG에 입력하여 생성되는 중간 키 또는 세트 키가 불분명하므로, 원하는 세트 키를 생성하는 것이 곤란하다. 이 문제에 대한 해결책을 제공하는 것이 본 실시 형태의 목적이다. 이에 대해서는 후술한다.

[0209] 지금까지, 중간 키를 이용하는 키 생성 방법에 대해 설명하였지만, 기존의 AI05 방식에 있어서도, 후술하는 본 실시 형태에 있어서도 중간 키를 이용하는 구성은 필수는 아니다. 애당초, 중간 키는 안전성을 높일 목적으로 사용하고 있는 것이며, 안전성에 각별히 주의를 하지 않아도 되는 경우, 또는 세트 키 생성을 위한 연산량을 줄이고 싶은 경우 등에 있어서는, 중간 키를 사용하지 않고, 세트 키 $k(S_0)$로부터 다른 세트 키 $k(S_1)$ 등을 직접적으로 산출 가능한 구성으로 해도 된다. 예를 들어, 세트 키 $k(S_0)$가 PRSG에 입력되면, 좌표점 S_0으로부터 뻗어나가는 유향 가지의 도달처에 대응하는 세트 키 $k(S_1)$, $k(S_2)$, $k(S_3)$, $k(S_4)$가 출력되도록 구성해도 된다.

[0210] 이상, 세트 키의 생성 방법에 대해 설명하였다. 상기한 예로부터 용이하게 이해되는 바와 같이, 어느 중간 키를 유지하고 있으면, 그 중간 키를 이용하여 PRSG를 반복하여 실행함으로써, 그 중간 키에 대응하는 좌표점으로부터 뻗어나간 유향 가지의 쇄에 의해 도달 가능한 모든 좌표점에 대응하는 중간 키와 세트 키를 도출할 수 있는 것이다. 따라서, 각 단말 장치(122)는, 자기가 요소로서 포함되는 부분 집합에 대응하는 중간 키를 모두 도출할 수 있는 최저한의 중간 키를 유지하고 있으면 되게 된다.

[0211] 또한, 키 배신 서버(102)는, 각 유향 그래프 H의 선두 좌표점(이하, 루트라 부름)에 대응하는 중간 키를 이용하여, PRSG에 의한 연산을 반복하여 실행함으로써, 각 유향 그래프를 구성하는 유향 가지가 도달 가능한 모든 좌표점에 대응하는 세트 키를 도출할 수 있다.

[0212] 따라서, 키 제공 시스템(100)의 관리자는, 키 제공 시스템(100)의 셋업시에, 예를 들어 λ비트의 난수를 생성하고, 키 배신 서버(102)에 있어서 각 유향 그래프 H의 루트의 중간 키로서 설정하면 된다. 상기한 유향 그래프 H의 루트라 함은, 그 좌표점으로부터 유향 가지가 나와 있지만, 그 좌표점에 도달하지 않는 좌표점을 말한다. 예를 들어, 도 4의 유향 그래프 H(1→64)의 루트는, 수평 좌표축의 좌측 단부에 위치하는 좌표점 [1, 1]이다.

[0213] 이상, 세트 키의 생성 방법에 대해 설명하였다. 이 방법은, 콘텐츠 또는 콘텐츠 키의 송신자측인 키 배신 서버(102)가 콘텐츠 또는 콘텐츠 키를 암호화하기 위한 세트 키와, 각 단말 장치(122)에 배신하는 중간 키를 생성할 때에 이용될 뿐만 아니라, 수신자측의 단말 장치(122)에 있어서도, 자기가 미리 유지하는 중간 키를 이용하여 원하는 세트 키를 생성하기 위해 이용된다.

[0214] (중간 키의 배신 방법)

[0215] 계속해서, 키 배신 서버(102)가 각 단말 장치(122)에 대해 소정의 중간 키를 배신하는 방법에 대해 설명한다. 또한, 각 단말 장치(122)에 대해서는, 그 단말 장치(122)가 포함되는 모든 부분 집합에 대응하는 세트 키를 도출 가능한 복수의 중간 키가 미리 부여되어 있다. 반대로, 그 단말 장치(122)에 대해, 이 단말 장치(122)가 포함되어 있지 않은 부분 집합에 대응하는 세트 키를 도출하는 것이 가능한 중간 키를 부여해서는 안 되고, 이 단말 장치(122)에 부여하는 중간 키의 수가 최소한이 되는 쪽이 바람직하다.

[0216] 따라서, 키 배신 서버(102)는, 계약자 u의 단말 장치(122)가 포함되는 부분 집합에 대응하는 좌표점에 도달 가능한 유향 그래프 H를 모두 추출한다. 그 중, 유향 그래프 H의 루트에 대응하는 부분 집합에 계약자 u의 단말 장치(122)가 포함되는 경우에는, 그 루트에 대응하는 중간 키만을 계약자 u의 단말 장치(122)에 부여한다.

[0217] 또한, 유향 그래프 H의 루트 이외의 좌표점에 대응하는 부분 집합 중 어느 하나에 계약자 u의 단말 장치(122)가 포함되는 경우에는, 계약자 u의 단말 장치(122)가 부분 집합 S_0에 포함되고, 또한 부분 집합 S_0의 친(親)인 부분 집합 $parent(S_0)$에 포함되지 않는 부분 집합 S_0을 추출한다. 그리고, 그 부분 집합 S_0에 대응하는 중간 키 $t(S_0)$를 계약자 u의 단말 장치(122)에 대해 부여한다.

[0218] 즉, 유향 그래프 H의 루트 이외의 복수의 좌표점에 대응하는 부분 집합에 계약자 u의 단말 장치(122)가 포함되는 경우에는, 각 좌표점에 도달하는 유향 가지의 시단부를 참조하여, 각 좌표점의 시단부에 대응하는 부분 집합이 계약자 u에 대응하는 단말 장치(122)를 포함하지 않는 좌표점을 선택한다. 이 좌표점에 대응하는 부분 집합을 S_0으로 하고, 좌표점 S_0에 도달하는 유향 가지의 시단부(친)에 대응하는 부분 집합을 $parent(S_0)$로 하면, 부분 집합 $parent(S_0)$를 포함하지 않는 좌표점 S_0에 대응하는 중간 키 $t(S_0)$를 계약자 u의 단말 장치(122)에 부여

하면 되게 된다.

[0219] 만약, 그와 같은 좌표점 S_0이 복수개 존재하는 경우에는, 각각의 중간 키 $t(S_0)$를 계약자 u의 단말 장치(122)에 부여한다. 또한, 좌표점의 친자 관계는, 유향 가지에 의해 규정된다. 즉, 유향 가지의 시단부가 종단부의 친이 되고, 유향 가지의 종단부가 시단부의 자가 된다. 또한, 좌표점 S_0의 친을 $parent(S_0)$로 표기한다. 물론, 좌표점 S_0이 유효 그래프 H의 루트인 경우에는 좌표점 S_0의 친은 존재하지 않는다. 또한, 유효 그래프 H의 루트가 아닌 경우에는 좌표점 S_0의 친은 오직 1개 존재한다.

[0220] 여기서, 도 4의 예를 참조하면서, 중간 키의 배신 방법에 대해 구체적으로 설명한다.

[0221] (예 1)

[0222] 계약자(1)의 단말 장치(122)에 대해 배신되는 중간 키에 대해 고려한다. 우선, 계약자(1)의 단말 장치(122)가 포함되는 부분 집합에 도달 가능한 유향 그래프 H를 추출한다. 도 4를 참조하면, 그와 같은 유향 그래프 H는, 유향 그래프 H(1→64)뿐인 것을 알 수 있다. 그리고, 계약자(1)의 단말 장치(122)는, 유향 그래프 H(1→64)의 루트에 대응하는 부분 집합 [1, 1]에 속해 있다. 따라서, 계약자(1)의 단말 장치(122)에는, 중간 키 t([1, 1])가 배신된다.

[0223] (예 2)

[0224] 계약자 3의 단말 장치(122)에 대해 배신되는 중간 키에 대해 고려한다. 우선, 계약자 3의 단말 장치(122)가 포함되는 부분 집합에 도달 가능한 유향 그래프 H를 추출한다. 도 4를 참조하면, 그와 같은 유향 그래프 H는, 유향 그래프 H(1→64), H(2←64), H(2←32), H(2←16), H(2←8), H(2←4), H(3→3)인 것을 알 수 있다. 우선, 유향 그래프 H(1→64)에 대해 검토하면, 계약자 3의 단말 장치(122)는, 유향 그래프 H(1→64)의 루트에 대응하는 부분 집합 [1, 1]에 포함되어 있지 않은 것을 알 수 있다.

[0225] 그러나, 계약자 3의 단말 장치(122)는, 3번째의 좌표점 이후의 부분 집합 [1, 3], [1, 4],…, [1, 64]에 포함되어 있다. 따라서, 이들 좌표점의 친의 부분 집합을 참조하면, 친의 부분 집합에 계약자 3의 단말 장치(122)를 포함하지 않는 좌표점은, [1, 3] 및 [1, 4]뿐인 것을 알 수 있다. 따라서, 좌표점 [1, 3], [1, 4]의 친 parent([1, 3]) 및 parent([1, 4])에 해당하는 좌표점 [1, 2]는, 계약자 3의 단말 장치(122)를 포함하고 있지 않은 것을 알 수 있다.

[0226] 그 결과, 계약자 3의 단말 장치(122)에는, 유향 그래프 H(1→64)에 대응하는 중간 키 t([1, 3]) 및 t([1, 4])가 배신된다. 마찬가지로, 다른 유향 그래프 H(2←64), H(2←32), H(2←16), H(2←8), H(2←4), H(3→3)에 대해서도 중간 키가 선택되어 계약자 3의 단말 장치(122)에 배신된다. 결국, 계약자 3의 단말 장치(122)에는, 합계 8개의 중간 키가 배신된다.

[0227] 다음에, 도 5를 참조하면서, 키 배신 서버(102)가 각 단말 장치(122)에 중간 키를 배신하는 처리에 대해 간단하게 설명한다. 도 5는, 시스템을 셋업할 때에 키 배신 서버(102)가 각 단말 장치(122)에 중간 키를 배신하는 처리를 나타낸 흐름도이다.

[0228] 도 5를 참조하면, 키 배신 서버(102)는, 계약자수 n, 세트 키 및 중간 키의 비트수 λ, 소정의 파라미터 k, 및 PRSG에 의한 의사 난수 생성 알고리즘 등을 결정하고, 모든 단말 장치(122)에 대해 공개한다(S102). 계속해서, 키 배신 서버(102)는, 단말 장치(122)의 집합을 소정의 부분 집합으로 나눈 후, 그 합집합에 의해 표현되는 세트 시스템(SS)(상기 수학식 1)을 결정하여 모든 단말 장치(122)에 대해 공개한다(S104). 계속해서, 키 배신 서버(102)는 복수의 유향 가지 T에 의해 형성되는 유향 그래프 H를 결정하고, 그 정보의 일부 또는 전부를 모든 단말 장치(122)에 대해 공개한다(S106). 계속해서, 세트 시스템(SS)을 구성하는 각 부분 집합에 대응하는 중간 키를 결정한다(S108). 그리고, 각 단말 장치(122)에 대해, 각 단말 장치(122)가 유향 그래프에 기초하여 원하는 세트 키를 도출하기 위해 필요한 중간 키를 배포한다(S110).

[0229] 이상, 중간 키의 배신 방법에 대해 설명하였다. 이 배신 방법을 이용하면, 각 허락 계약자의 단말 장치(122)가 세트 키를 생성하기 위해 필요한 중간 키를 효율적으로 배신하는 것이 가능해지고, 키 배신 서버(102)와 단말 장치(122) 사이의 통신량, 및 각 단말 장치(122)가 키의 유지에 필요로 하는 메모리량을 절약할 수 있다.

[0230] (콘텐츠 키의 배신 방법)

[0231] 다음에, 키 배신 서버(102)에 의해 암호화된 콘텐츠 키 mek의 배신 방법에 대해 설명한다.

[0232] 우선, 키 배신 서버(102)는, 허락 계약자의 단말 장치(122)만이 생성 가능한 세트 키를 이용하여 콘텐츠 키 mek를 암호화한다. 키 배신 서버(102)는, 배제해야 할 계약자(이하, 배제 계약자)의 단말 장치(122)가 포함되는 집합 R을 결정하고, 전체 계약자 1 내지 n의 단말 장치(122)가 포함되는 집합 N으로부터 집합 R을 제외한 집합 $N \setminus R$을 결정한다.

[0233] 그리고, 세트 시스템(SS)을 구성하는 부분 집합 중으로부터 1 또는 복수의 부분 집합 S_i(i=1, 2,…, m)를 선택하고, 선택된 부분 집합을 이용하여 집합 $N \setminus R=S_1 \cup S_2 \cup \cdots \cup S_m$을 표현한다. 이때, 부분 집합 S_i의 조합은 다수 존재하지만, m이 최소가 되는 부분 집합 S_i를 선택하는 쪽이 바람직하다.

[0234] 키 배신 서버(102)는, 상기한 부분 집합 S_i를 선택한 후, 각 부분 집합 S_i에 대응하는 세트 키 $k(S_i)$를 이용하여 콘텐츠 키 mek를 암호화하고, 세트 키 $k(S_1)$, $k(S_2)$,…, $k(S_m)$에 의해 암호화된 m개의 콘텐츠 키 mek를 생성한다. 그리고, 키 배신 서버(102)는, m개가 암호화된 콘텐츠 키 mek가 전체 계약자 1 내지 n의 단말 장치(122)에 대해 배신한다. 이때, 키 배신 서버(102)는 집합 $N \setminus R$의 정보, 및 m개의 부분 집합 S_i의 정보의 한쪽 또는 양쪽도 동시에 각 단말 장치(122)에 대해 배신한다.

[0235] 다음에, 도 6을 참조하면서, 키 배신 서버(102)에 의해 암호화된 콘텐츠 키 mek의 배신 처리에 대해 간단하게 설명한다. 도 6은, 콘텐츠 키의 배신 처리의 흐름을 나타내는 설명도이다.

[0236] 도 6을 참조하면, 키 배신 서버(102)는 배제 계약자의 집합 R을 결정하고, 허락 계약자의 집합 $N \setminus R$을 결정한다(S112). 계속해서, 키 배신 서버(102)는, 세트 시스템(SS)을 구성하는 부분 집합으로부터, 합집합이 $N \setminus R$이 되는 m개의 부분 집합 S_i(i=1, 2,…, m)를 선택한다(S114). 계속해서, 키 배신 서버(102)는 선택된 각 부분 집합 S_i에 대응하는 세트 키 $k(S_i)$를 이용하여 콘텐츠 키 mek를 각각 암호화한다(S116). 계속해서, 키 배신 서버(102)는 집합 $N \setminus R$ 또는 각 부분 집합 S_i를 나타내는 정보와, m개의 암호화된 콘텐츠 키 mek를 모든 단말 장치(122)에 대해 배신 한다(S118).

[0237] 이상, 키 배신 서버(102)에 의한 콘텐츠 키 mek의 암호화 방법 및 배신 방법에 대해 설명하였다. 상기한 암호화 방법을 이용하면, 암호화에 필요로 하는 세트 키수가 최소한이 되도록 부분 집합 S_i를 선택할 수 있다. 그로 인해, 콘텐츠 키 mek를 암호화할 때에, 암호화에 필요로 하는 계산량을 저감시킬 수 있는 동시에, 배신해야 할 암호화된 콘텐츠 키 mek의 수를 저감시키는 것이 가능해지고, 통신량의 저감화도 실현될 수 있다.

[0238] (콘텐츠 키의 복호 방법)

[0239] 다음에, 각 단말 장치(122)에 있어서의 콘텐츠 또는 콘텐츠 키의 복호 처리에 대해 설명한다. 단말 장치(122)는, 상기 키 배신 서버로부터 수신한 집합 $N \setminus R$ 또는 m개의 부분 집합 S_i의 정보와, m개가 암호화된 콘텐츠 키에 기초하여 콘텐츠 키 mek를 복호 한다.

[0240] 단말 장치(122)는, 키 배신 서버(102)로부터 암호화된 콘텐츠 키 mek와, 집합 $N \setminus R$을 나타내는 정보 또는 m개의 부분 집합 S_i를 나타내는 정보를 수신한다. 계속해서, 단말 장치(122)는 이들 정보를 해석하여, 자신이 m개의 부분 집합 S_i 중 어느 하나에 포함되는지 여부를 판단한다. 계속해서, 단말 장치(122)는, 자신이 어떤 부분 집합에도 포함되지 않는다고 판단한 경우, 자신이 배제 계약자의 단말 장치(122)라 판단하여 복호 처리를 종료한다. 반대로, 자신이 포함되는 부분 집합 S_i가 발견된 경우, 단말 장치(122)는 상기한 PRSG를 이용하여 그 부분 집합 S_i에 대응하는 세트 키 $k(S_i)$를 도출한다. 단, 단말 장치(122)가 이용하는 PRSG의 구성은, 상기한 키 배신 서버(102)가 암호화에 이용한 PRSG의 구성과 마찬가지이다.

[0241] 또한, 단말 장치(122)는, 시스템의 셋업시에, 키 배신 서버(102)로부터 상기의 부분 집합 S_i에 대응하는 중간 키 $t(S_i)$ 또는 이 중간 키 $t(S_i)$를 도출 가능한 중간 키 $t(S_j)$가 미리 배신되어 있는 것으로 한다. 따라서, 단말 장치(122)는 유지하고 있는 중간 키 $t(S_i)$ 또는 $t(S_j)$를 PRSG에 입력하고, 상기 부분 집합 S_i에 대응하는 세트 키 $k(S_i)$를 도출하는 것이 가능하다. 이때, 단말 장치(122)는, 유향 그래프의 정보를 참조하여 PRSG의 처리를 반복하여 실행하고, 상기한 세트 키 $k(S_i)$를 산출할 필요가 있을지도 모른다. 계속해서, 단말 장치(122)는, 도출한 세트 키 $k(S_i)$를 이용하여 암호화된 콘텐츠 키 mek를 복호한다.

[0242] 여기서, 다시 도 4를 참조한다. 도 4를 참조하면서, 단말 장치(122)에 있어서의 상기 세트 키 $k(S_i)$의 도출 방법에 대해 구체예를 들어 설명한다.

[0243] (예 1)

[0244] 도 4에 나타낸 유향 그래프 H에 기초하여, 계약자 3의 단말 장치(122)가 부분 집합 [1, 8]에 대응하는 세트 키를 도출하는 과정에 대해 고려한다. 또한, 키 배신 서버(102)는, 시스템 셋업시, 계약자 3의 단말 장치(122)에 대해 미리 부분 집합 [1, 4]의 중간 키를 배신하고 있다.

[0245] 우선, 유향 그래프 H(1→64)를 참조하면, 좌표점 [1, 4]로부터 좌표점 [1, 8]로 연장되는 유향 가지가 존재한다. 이 유향 가지는, 좌표점 [1, 4]를 시단부로 하는 유향 가지 중 3번째로 거리가 짧은 것이다. 따라서, 계약자 3의 단말 장치(122)는, 좌표점 [1, 4]에 대응하는 중간 키 t([1, 4])를 PRSG에 입력하여 얻어지는 출력 중, 선두로부터 제3번째 λ비트의 부분을 추출한다. 출력의 제3번째 λ비트 부분이 부분 집합 [1, 8]에 대응하는 중간 키 t([1, 8])이다. 따라서, 계약자 3의 단말 장치(122)는, PRSG의 출력으로부터 중간 키 t([1, 8])를 추출한 후, 중간 키 t(S[1, 8])를 다시 PRSG에 입력하여 얻어진 출력의 최종 λ비트를 추출한다. 출력의 최종 λ비트가 원하는 세트 키 k([1, 8])이다. 이상의 처리에 의해, 계약자 3의 단말 장치(122)는, 원하는 세트 키 k([1, 8])를 생성할 수 있다.

[0246] (예 2)

[0247] 마찬가지로, 도 4의 유향 그래프 H에 기초하여, 계약자(1)의 단말 장치(122)가 세트 키 k([1, 8])를 생성하는 경우에 대해 고려한다. 계약자(1)의 단말 장치(122)는, 부분 집합 [1, 1]에 대응하는 중간 키 t([1, 1])를 미리 유지하고 있다. 따라서, 계약자(1)의 단말 장치(122)는, 중간 키 t([1, 1])를 PRSG에 입력하여 얻어진 출력의 선두로부터 제1번째의 λ비트의 부분[중간 키 t([1, 2])]을 추출한다. 계속해서, 계약자(1)의 단말 장치(122)는, 중간 키 t([1, 2])를 다시 PRSG에 입력하여 얻어진 출력의 선두로부터 제2번째의 λ비트의 부분[중간 키 t([1, 4])]을 추출한다. 또한, 계약자(1)의 단말 장치(122)는, 중간 키 t([1, 4])를 다시 PRSG에 입력하여 얻어진 출력의 선두로부터 제3번째의 λ비트의 부분[중간 키 t([1, 8])]을 추출한다. 마지막에, 계약자(1)의 단말 장치(122)는, 중간 키 t([1, 8])를 PRSG에 입력하여 얻어진 출력의 최종 λ비트[세트 키 k([1, 8])]를 추출하여, 원하는 세트 키 k([1, 8])를 취득할 수 있다.

[0248] 다음에, 도 7을 참조하면서, 각 단말 장치(122)에 있어서의 암호화된 콘텐츠 키 mek의 복호 처리에 대해 설명한다. 도 7은, 각 단말 장치(122)에 있어서의 콘텐츠 키의 복호 처리의 흐름을 나타내는 설명도이다.

[0249] 도 7을 참조하면, 단말 장치(122)는, 키 배신 서버(102)로부터 m개가 암호화된 콘텐츠 키 mek와, 집합 N\R을 나타내는 정보 또는 m개의 부분 집합 S_i(i=1, 2,…, m)를 나타내는 정보를 수신한다(S120). 계속해서, 단말 장치(122)는 자신이 포함되는 부분 집합 S_i를 검색하고(S122), 자신이 m개의 부분 집합 S_i 중 어느 하나에 포함되어 있는지 여부를 판단한다(S124).

[0250] 자신이 포함되는 부분 집합 S_i가 존재하는 경우, 단말 장치(122)는 상기한 PRSG를 이용하여, 그 부분 집합 S_i에 대응하는 세트 키 $k(S_i)$를 도출한다(S126). 계속해서, 단말 장치(122)는 도출한 세트 키 $k(S_i)$를 이용하여 암호화된 콘텐츠 키 mek를 복호한다(S128).

[0251] 한편, 자신이 어느 부분 집합 S_i에도 포함되지 않는다고 판단한 경우, 단말 장치(122)는 자신이 허락 계약자의 단말 장치(122)가 아닌 취지(배제 계약자인 취지)를 표시 출력하여(S130), 콘텐츠 키의 복호 처리를 종료한다.

[0252] 이상, 단말 장치(122)에 있어서의 콘텐츠 키의 복호 방법에 대해 설명하였다. 상기한 복호 방법에는, 단말 장치(122)측에도 유향 그래프의 정보와 PRSG가 필요하게 된다. 그러나, 유향 그래프의 정보를 모두 단말 장치(122)가 유지해 두는 것은 단말 장치(122)의 메모리량을 크게 압박한다는 점에서 곤란하고, 또한 단말 장치(122)가 모든 유향 그래프를 생성하는 것도 단말 장치(122)의 연산 부하를 증대시킨다는 점에서 곤란하다. 물론, 유향 그래프의 정보를 모두 배신하는 것도 통신량의 현저한 증대 또는 배신 매체의 기억 용량의 압박이라는 점으로부터 곤란하다. 본 실시 형태에 관한 키 제공 시스템(100)은, 이러한 문제점을 해결하는 수단을 제공하는 것이며, 그 특징에 대해서는 후술한다.

[0253] (AI05 방식의 정리)

[0254] 이상, 본 실시 형태를 적용 가능한 AI05 방식에 대해 설명해 왔다. 이 AI05 방식을 이용하면, 각 단말 장치

(122)가 유지해야 할 중간 키의 개수를 O(k*log(n))으로 억제할 수 있다. 또한, 세트 키의 생성에 필요로 하는 계산량(PRSG의 동작 횟수)을 $(2k-1)*(n^{1/k}-1)$ 정도 또는 그 이하로 억제할 수 있다. 그러나, 본건 출원인이 이미 지적하고 있는 바와 같이, AI05 방식에는 효율화의 관점으로부터 몇 가지의 개선의 여지가 남겨져 있다. 예를 들어, A06(A) 방식에서는 단말 장치(122)가 유지해야 할 키수를 삭감하는 것에 성공하고 있고, A06(B) 방식에서는 단말 장치(122)가 키 생성에 필요로 하는 연산량을 저감시키는 것에 성공하고 있다. 그리고, A06(A+B) 방식에 있어서 단말 장치(122)가 유지해야 할 키수와 키 생성에 필요로 하는 연산량을 밸런스 좋게 저감시키는 것에 성공하고 있다. 본 실시 형태의 특징은, 단말 장치(122)가 키 생성할 때에 필요한 유향 그래프의 정보를 어떻게 제공할 것인가라는 점에 있으므로, 적어도 상기한 각 방식의 전체에 적용이 가능하다.

[0255] (A06(A+B) 방식)

[0256] 다음에, 본 실시 형태를 적용 가능한 A06(A+B) 방식에 대해 설명한다. 상기한 바와 같이, A06(A+B) 방식은, AI05 방식에 비해 효율적인 키 배신을 실현 가능한 방식이다. 따라서, 본 실시 형태를 적용하는 데 있어서, A06(A+B) 방식을 적용하는 쪽이 보다 효율적이다.

[0257] A06(A+B) 방식에 대해 설명하는 것에 앞서, 키 배신의 효율에 대해 간단하게 설명한다. 우선, 단말 장치(122)가 원하는 키 생성에 필요로 하는 계산량은, 원하는 중간 키를 도출하기 위해 PRSG를 실행하는 횟수에 의존하고 있다. 이 최악치는, 유향 그래프 H를 따라가면서, 루트로부터 가장 먼 말미의 좌표점(유향 가지가 나와 있지 않은 리프)에 도달할 때까지 존재하는 유향 가지의 개수에 대응한다. 도 4의 유향 그래프 H(1→64)를 참조하면, 루트 [1, 1]로부터 말미의 좌표점[1, 64]에 도달하기까지 11개의 유향 가지를 경유하고 있고, 중간 키 t([1, 1])를 유지하는 단말 장치(122)가 중간 키 t([1, 64])를 도출하기 위해 PRSG를 11회나 실행해야만 하는 것을 의미하고 있다. 따라서, 수평 좌표축 상의 모든 좌표점에 도달 가능한 경로를 확보하면서, 유향 그래프의 최장 패스를 구성하는 유향 가지수를 저감시킬 수 있으면, 단말 장치(122)의 연산량을 저감시킬 수 있는 것이다. 이 과제에 대한 하나의 어프로치가 A06(B) 방식이며, 이를 또한 개량한 것이 A06(A+B) 방식이다. 따라서, 본 실시 형태를 A06(A+B) 방식에 적용한 경우를 예로 들어 상세하게 설명한다.

[0258] [키 배신 서버(102)의 구성]

[0259] 우선, 도 8을 참조하면서, 본 실시 형태에 관한 키 배신 서버(102)의 구성에 대해 설명한다. 도 8은, 본 실시 형태에 관한 키 배신 서버(102) 및 단말 장치(122)의 구성을 도시하는 설명도이다.

[0260] 도 8을 참조하면, 키 배신 서버(102)는, 주로 나무 구조 설정부(104)와, 좌표축 설정부(106)와, 임시 유향 그래프 생성부(108)와, 유향 그래프 생성부(110)와, 초기 중간 키 설정부(112)와, 키 생성부(114)와, 암호화부(116)와, 통신부(118)와, 부분 집합 결정부(120)에 의해 구성된다. 또한, 나무 구조 설정부(104)와, 좌표축 설정부(106)와, 임시 유향 그래프 생성부(108)와, 유향 그래프 생성부(110)를 통합하여 키 생성 로직 구축 블록이라 부르기로 한다. 마찬가지로, 초기 중간 키 설정부(112)와, 키 생성부(114)를 통합하여 키 생성 블록이라 부르기로 한다. 또한, 좌표축 설정부(106), 임시 유향 그래프 생성부(108), 유향 그래프 생성부(110)는, 상기한 집합 관계 정보 생성부 또는 집합 관계 정보 취득부의 일례이다. 또한, 통신부(118)는 상기한 키 생성 경로 정보 제공부 또는 암호 정보 제공부의 일례이다.

[0261] [키 생성 로직 구축 블록]

[0262] 우선, 키 생성 로직 구축 블록에 대해 상세하게 설명한다.

[0263] (나무 구조 설정부(104))

[0264] 우선, 나무 구조 설정부(104)에 대해 설명한다. 나무 구조 설정부(104)는, 상기 AI05 방식과 마찬가지의 이분목 구조(도 3을 참조)를 생성할 수 있다. 우선, 나무 구조 설정부(104)는, 번호 1 내지 n(n은 자연수)의 n개의 잎 노드와, 뿌리 노드와, 뿌리 노드 및 잎 노드 이외의 복수의 중간 노드에 의해 형성되는 이분목 구조를 설정한다. 계속해서, 나무 구조 설정부(104)는, 어느 중간 노드 v 또는 뿌리 노드 v의 하위에 배치된 복수의 잎 노드 중, 좌측 단부에 위치하는 상기 잎 노드의 번호를 l_v로 하고, 우측 단부에 위치하는 상기 잎 노드의 번호를 r_v로 설정한다. 계속해서, 나무 구조 설정부(104)는 뿌리 노드에 대해 집합 (1→n)과 집합 (2←n)을 할당한다. 계속해서, 나무 구조 설정부(104)는, 상기한 이분목을 형성하는 임의의 중간 노드 v에 대해, 중간 노드 v가 친 노드의 좌측에 위치하는 경우에는 집합 $(l_v+1 \leftarrow r_v)$를 대응시키고, 반대로 중간 노드 v가 친 노드의 우측에 위치하는 경우에는 집합 $(l_v \rightarrow r_v-1)$을 대응시킨다.

[0265] (좌표축 설정부(106))

[0266] 다음에, 좌표축 설정부(106)에 대해 설명한다. 좌표축 설정부(106)는, 상기 AI05 방식과 유사한 규칙에 기초하여 수평 좌표축을 설정한다. 우선, 좌표축 설정부(106)는 복수의 수평 좌표축을 설정한다. 계속해서, 좌표축 설정부(106)는 집합 (1→n-1)에 포함되는 복수의 부분 집합을 좌측으로부터 차례로 우측 방향을 향해 포함 관계가 커지도록, 하나의 수평 좌표축 상의 각 좌표점에 대응시킨다. 마찬가지로, 좌표축 설정부(106)는, 집합 (l_v→r_v-1)에 포함되는 복수의 부분 집합을 좌측으로부터 차례로 우측 방향을 향해 포함 관계가 커지도록, 다른 하나의 수평 좌표축 상의 각 좌표점에 대응시킨다. 물론, 좌표축 설정부(106)는 상기한 이분목을 형성하는 중간 노드에 대응된 모든 집합 (l_v→r_v-1)에 대해 마찬가지의 처리를 반복한다.

[0267] 계속해서, 좌표축 설정부(106)는 집합 (2←n)에 포함되는 복수의 부분 집합을 우측으로부터 차례로 좌측 방향을 향해 포함 관계가 커지도록, 또한 다른 하나의 수평 좌표축 상의 각 좌표점에 대응시킨다. 마찬가지로, 좌표축 설정부(106)는, 집합 (l_v+1←r_v)에 포함되는 복수의 부분 집합을 우측으로부터 차례로 좌측 방향을 향해 포함 관계가 커지도록, 또한 다른 하나의 수평 좌표축 상의 각 좌표점에 대응시킨다. 물론, 좌표축 설정부(106)는 상기한 이분목을 형성하는 중간 노드에 대응된 모든 집합 (l_v+1←r_v)에 대해 마찬가지의 처리를 반복한다.

[0268] 계속해서, 좌표축 설정부(106)는, 집합 (1→n-1)에 대응하는 수평 좌표축의 우측 단부에 위치하는 좌표점의 우측에 2개의 임시 좌표점을 생성한다. 계속해서, 좌표축 설정부(106)는, 집합 (l_v→r_v-1)에 대응하는 수평 좌표축의 우측 단부에 위치하는 좌표점의 우측에 2개의 임시 좌표점을 생성한다. 계속해서, 좌표축 설정부(106)는, 집합 (2←n)에 대응하는 수평 좌표축과, 집합 (l_v+1←r_v)에 대응하는 수평 좌표축의 좌측 단부에 위치하는 좌표점의 좌측에 2개의 임시 좌표점을 생성한다.

[0269] 이상의 처리에 의해, 좌표축 설정부(106)는 이분목을 형성하는 모든 노드에 대응된 집합에 대해 유향 그래프를 형성하기 위한 수평 좌표축을 설정할 수 있다. 이하, 좌표축 설정부(106)에 의해 생성된 각 수평 좌표축 상에 유향 그래프를 형성하는 수단에 대해 설명한다.

[0270] (임시 유향 그래프 생성부(108))

[0271] 다음에, 임시 유향 그래프 생성부(108)에 대해 설명한다. 임시 유향 그래프 생성부(108)는, 상기한 AI05 방식으로 유향 그래프 H를 생성한 것과 유사한 방법에 의해 임시 유향 그래프 I'를 생성한다. 우선, 임시 유향 그래프 생성부(108)는 소정의 정수 k를 파라미터로서 설정한다. 계속해서, 임시 유향 그래프 생성부(108)는, $n^{(x-1)/k} < r_v - l_v + 1 \leq n^{x/k}$를 만족하는 정수 x를 결정한다. 계속해서, 임시 유향 그래프 생성부(108)는, 집합 (1→n-1) 및 집합 (l_v→r_v-1)에 대응하는 수평 좌표축 상에 $n^{i/k}$(i=0 내지 x-1)의 길이를 갖는 우측 방향을 향한 유향 가지를 형성한다. 계속해서, 임시 유향 그래프 생성부(108)는, 집합 (2←n) 및 집합 (l_v+1←r_v)에 대응하는 수평 좌표축 상에 $n^{i/k}$(i=0 내지 x-1)의 길이를 갖는 좌측 방향을 향한 유향 가지를 형성한다.

[0272] 상기한 바와 같이, AI05 방식에 있어서, 부분 집합 중에서 가장 요소수가 적은 부분 집합(즉, 한 사람의 유저를 포함하는 부분 집합)에 대응하는 좌표점의 이웃에 배치된 임시 좌표점으로부터 유향 가지의 생성이 개시된다. 이에 대해, A06(A+B) 방식에서는, 부분 집합 중에서 가장 요소수가 적은 부분 집합(즉, 한 명의 유저를 포함하는 부분 집합)에 대응하는 좌표점으로부터 유향 가지의 생성이 개시되는 점에 주의가 필요하다.

[0273] 계속해서, 임시 유향 그래프 생성부(108)는, 상기한 모든 수평 좌표축 상의 유향 가지에 대해, 수평 좌표축 상의 임시 좌표점을 시단부 또는 종단부로 하는 모든 유향 가지를 소거한다. 계속해서, 임시 유향 그래프 생성부(108)는, 상기한 모든 수평 좌표축 상의 모든 좌표점에 대해, 하나의 좌표점에 도달하는 유향 가지가 복수 존재하는 경우, 그 좌표점에 도달하는 복수의 유향 가지 중으로부터 최장의 유향 가지 이외의 모든 유향 가지를 소거한다. 계속해서, 임시 유향 그래프 생성부(108)는, 집합 (1→n-1)에 대응하는 수평 좌표축 상에 생성된 임시 좌표점 중, 좌측에 위치하는 임시 좌표점을 종단부로 하는 길이 1의 우측 방향 유향 가지를 추가한다. 즉, 임시 유향 그래프 생성부(108)는, 하기 수학식 3의 처리를 실행함으로써, 뿌리 노드에 대응된 집합 (1→n)에 대응하는 임시 유향 그래프 I'(1→n)를 생성할 수 있다.

수학식 3

[0274] $$E\ (I'\ (1 \rightarrow n-1)) \cup \{([1,\ n-1],\ [1,\ n])\}$$

[0275] 이상의 처리에 의해, 임시 유향 그래프 생성부(108)는, AI05 방식에 비해 긴 유향 가지에 의해 구성되는 임시 유향 그래프 I'를 형성할 수 있다. 이 알고리즘은, A06(B) 방식의 기본 개념에 기초하는 것이다. 이 알고리즘을 적용함으로써, 단말 장치(122)가 키 생성에 필요로 하는 연산량을 저감시키는 효과를 얻을 수 있다.

[0276] (알고리즘)

[0277] 여기서, 도 9를 참조하면서, 좌표축 설정부(106) 및 임시 유향 그래프 생성부(108)에 의해 실행되는 처리의 흐름에 대해 간단하게 정리한다. 또한, 도 9에 나타내는 흐름도는, 일례로서, 집합 $(l_v \rightarrow r_v-1)$에 대응하는 임시 유향 그래프 $I'(l_v \rightarrow r_v-1)$의 생성 방법을 나타낸 것이다.

[0278] (S140) 우선, 집합 $(l_v \rightarrow r_v-1)$의 요소를 수평 직선 상에 좌측으로부터 우측으로 포함 관계가 커지도록 배열한다. 그리고, 가장 좌측 좌표점을 시작점으로 한다. 또한, 최우측 좌표점의 우측에 2개의 임시 좌표점을 배치한다. 그러면, 시작점으로부터 최우측 임시 좌표점까지의 길이는, $L_v=r_v-l_v+1$이 된다. 또한, $n^{(x-1)/k}<L_v \leq n^{x/k}$를 만족하는 정수 $x(1 \leq x \leq k)$를 산정한다.

[0279] (S142) 계속해서, 카운터 i를 0 내지 x-1까지 움직이면서 하기의 조작을 행한다. 시작점부터 개시하여, 그 좌표점으로부터 $n^{i/k}$만큼 이격된 좌표점으로의 점프를 계속하여, 임시 좌표점에 도달하거나, 다음의 점프가 임시 좌표점을 지나간 상태에서 종료한다. 그 후, 각 점프에 대응하는 유향 가지를 생성한다.

[0280] (S144) 계속해서, 임시 좌표점에 도달하는 유향 가지를 모두 소거한다.

[0281] (S146) 어느 좌표점 T에 도달하는 유향 가지가 복수 있는 경우에는, 점프의 거리가 가장 긴 것만을 남기고, 그 이외의 유향 가지는 소거한다.

[0282] 상기한 알고리즘을 적용함으로써, 도 10에 나타낸 임시 유향 그래프 I'를 생성할 수 있다. 단, 도 10의 임시 유향 그래프 I'는, 잎 노드수 n=64, 파라미터 k=6으로 설정한 케이스이다. 이하, 이 임시 유향 그래프 I'를 형성하는 복수의 유향 가지의 일부를 소정의 규칙에 기초하여 치환하고, 유향 그래프 I를 생성하는 알고리즘에 대해 설명한다. 또한, 유향 가지의 치환 처리는, 주로 유향 그래프 생성부(110)에 의해 실행된다.

[0283] (유향 그래프 생성부(110))

[0284] 우선, 유향 그래프 생성부(110)에 대해 설명한다. 유향 그래프 생성부(110)는, 임시 유향 그래프 I'를 구성하는 복수의 유향 가지의 일부를 치환하여 유향 그래프 I를 생성한다. 우선, 유향 그래프 생성부(110)는 임시 유향 그래프 I'에 포함되는 유향 패스 중, 그것을 구성하는 유향 가지수가 최대의 유향 패스를 선택한다. 그 유향 패스를 최장 유향 패스 LP(Longest Path)라 부르기로 한다. 그리고, 유향 그래프 생성부(110)는, 모든 유향 패스의 유향 가지수가 최장 유향 패스 LP의 유향 가지수를 초과하지 않는다는 조건 하에서, 임시 유향 그래프 I'에 포함되는 유향 패스를, 보다 짧은 유향 가지의 세트로 구성되는 유향 패스로 치환한다.

[0285] (알고리즘)

[0286] 여기서, 도 11 내지 도 14를 참조하면서, 유향 그래프 I를 생성하는 알고리즘에 대해 상세하게 설명한다. 도 11은, 유향 그래프 I를 생성하는 처리의 전체적인 흐름을 나타낸 설명도이다. 도 12는, 최장 유향 패스 LP를 추출하는 처리의 흐름을 나타낸 설명도이다. 도 13은, 최장 유향 패스 LP 이외의 유향 패스 중으로부터 최장의 유향 패스 PLP(Partially Longest Path)를 추출하는 처리의 흐름을 나타낸 설명도이다. 도 14는, 임시 유향 그래프 I'의 유향 패스를 보다 짧은 유향 가지의 세트로 구성되는 유향 패스로 치환하는 처리를 나타낸 설명도이다.

[0287] 도 11에 도시한 바와 같이, 우선 유향 그래프 I'를 형성하는 유향 패스 중으로부터 최장 유향 패스 LP가 추출된다(S150). 계속해서, 임시 유향 그래프 I'의 최장 유향 패스 LP 이외의 유향 패스 중으로부터 최장의 유향 패스 PLP가 추출된다(S152). 또한, 각 부분 집합에 대응하는 임시 유향 그래프 I'에 대해 최장의 유향 패스 PLP가 추출되어도 된다. 계속해서, 임시 유향 그래프 I'의 유향 패스를 구성하는 소정의 유향 가지가, 보다 짧은 유향 가지로 치환된다(S154). 이때, 모든 유향 패스의 유향 가지수가 최장 유향 패스 LP의 유향 가지수를 초과

하지 않도록 유향 가지가 치환된다. 즉, 이 치환 처리를 실행하였다 해도, AI05 방식 또는 A06(B) 방식보다도 키 생성에 필요로 하는 계산량의 최악치가 증가하지 않도록 한다.

[0288] 이하, 도 11에 나타낸 각 스텝에 대해, 보다 상세하게 설명한다.

[0289] (S150의 상세)

[0290] 우선, 도 12를 참조하면서, 최장 유향 패스 LP가 추출되는 스텝(S160)에 대해 상세하게 설명한다. 여기서, 이하에 나타내는 2개의 표기를 도입한다.

[0291] ·DD_T : 최장 유향 패스 LP의 유향 가지수를 나타낸다.

[0292] ·J(a, b) : 길이 b의 유향 가지가 a개 연속하여 존재하는 것을 나타낸다.

[0293] 우선, $t=n^{1/k}-1$로 놓는다. 계속해서, 임시 유향 그래프 I'(1→n)의 좌표점 [1, 1]로부터 좌표점 [1, n]까지의 유향 패스 P([1, 1], [1, n])를 고려한다. 유향 패스 P([1, 1], [1, n])는 $J(t, n^{(k-1)/k})$, $J(t, n^{(k-2)/k})$,…, $J(t, n^{1/k})$, $J(t, n^{0/k})$로 표현된다. 이 유향 패스를 최장 유향 패스 LP라 부른다. 이때, 최장 유향 패스 LP의 유향 가지수 DD_T는, $DD_T=k*(n^{1/k}-1)$이 된다. 계속해서, 최장 유향 패스 LP를 구성하는 모든 유향 가지에 대해 active 마크를 설정한다.

[0294] (S152의 상세)

[0295] 다음에, 도 13을 참조하면서, 최장 유향 패스 LP를 포함하는 임시 유향 그래프 I' 이외의 모든 부분 집합에 대응하는 임시 유향 그래프 I'에 대해, 최장의 유향 패스 PLP를 추출하는 처리(S162 내지 S176)에 대해 설명한다. 여기서, 이하에 나타내는 2개의 표기를 도입한다.

[0296] ·CP(Current Path) : 참조 중의 유향 패스(현재 패스)

[0297] ·#JP(CP) : 현재 패스의 유향 가지수

[0298] 우선, 유향 그래프 I'의 시작점으로부터 종점으로의 현재 패스 CP를 결정한다. 이때, 현재 패스가 유향 그래프 I'(a→b)에 포함되는 경우에는, 유향 패스 P([a, a], [a, b])를 현재 패스 CP로 하고, 유향 그래프 I'(a←b)에 포함되는 경우에는, 유향 패스 P([b, b], [b, a])를 현재 패스 CP로 한다(S162). 계속해서, 현재 패스 CP를 구성하는 유향 가지 중, 최장의 유향 가지를 선택하여, 그 길이를 J로 한다(S164). 계속해서, J≤1인지 여부를 판단한다(S166).

[0299] J≤1인 경우, 현재 패스 CP를 최장의 유향 패스 PLP로 결정하여, 현재 패스 CP에 포함되는 모든 유향 가지에 active 마크를 설정한다(S176). J>1인 경우, $\#JP(CP)+t \leq DD_T$인지 여부를 판단한다(S168). $\#JP(CP)+t \leq DD_T$가 아닌 경우, 현재 패스 CP를 유향 패스 PLP로 결정하여, 현재 패스에 포함되는 모든 유향 가지에 active 마크를 설정한다(S176). $\#JP(CP)+t \leq DD_T$인 경우, $J=n^{j/k}$가 되는 자연수 j를 산출한다(S170).

[0300] 계속해서, 현재 패스 CP에 포함되는 길이 J의 유향 가지 중에서 현재 패스 CP의 시작점으로부터 가장 먼 유향 가지를 추출한다(S172). 스텝 S172에서 추출된 유향 가지의 시작점으로부터 뻗어나간 t개의 길이 $n^{(j-1)/k}$의 유향 가지의 직후에 $n^{(j-1)/k}$의 길이를 갖는 1개의 유향 가지를 추가하여, 스텝 S172에서 추출된 유향 가지를 제거하고(S174), 스텝 S162로 복귀하여 상기한 처리를 반복한다.

[0301] 또한, 스텝 S162 내지 스텝 S174 사이에 발생하는 루프 처리는, 유향 그래프 I'의 시작점으로부터 종점으로의 유향 패스가 모두 길이 1의 유향 가지로 구성되거나, 또는 그 이상의 유향 가지의 치환을 실행함으로써, 그 유향 패스를 구성하는 유향 가지수가 DD_T를 초과하게 되는 경우에 루프 처리를 종료한다.

[0302] (S154의 상세)

[0303] 다음에, 도 14를 참조하면서, 임시 유향 그래프 I'에 포함되는 유향 가지를 짧은 유향 가지로 치환하는 처리(S180 내지 S202)에 대해 상세하게 설명한다.

[0304] 우선, 그래프 중 active이면서 미실시(done 마크가 부여되어 있지 않음) 유향 가지 중, 최장의 길이 J'를 갖는 유향 가지를 추출한다. 만일 최대의 유향 가지가 복수 존재하는 경우에는, 임시 유향 그래프 I'의 시작점으로

부터 가장 먼 유향 가지를 선택한다(S180). 여기서 선택된 유향 가지를 WJ(Working Jump)라 부르기로 한다. 또한, 유향 가지 WJ의 시작점을 WJ_S, 종점을 WJ_E라 부르기로 한다. 또한, 임시 유향 그래프 I'의 시작점으로부터 WJ_S까지의 유향 패스에 포함되는 유향 가지수를 D로 표기한다.

[0305] 계속해서, 유향 가지의 길이 J'가 J'≤1인지 여부를 판단한다(S182). J'≤1인 경우, active 마크가 부여되어 있지 않은 유향 가지를 모두 소거하고, active 마크가 부여되어 있는 유향 가지를 모두 합친 것을 E(I(a→b)) 또는 E(I(a←b))로 설정한다(S202). 반대로, J'≤1이 아닌 경우, WJ_S로부터 WJ_E-1까지의 유향 패스를 현재 패스 CP로 설정한다(S184). 단, WJ_E-1은, WJ_E의 하나 앞의 요소를 나타낸다.

[0306] 계속해서, 현재 패스 CP에 포함되는 유향 가지 중으로부터 최장의 유향 가지를 추출하고, 그 길이를 J로 한다(S186). 계속해서, 유향 가지의 길이 J가 J≤1인지 여부를 판단한다(S188). J≤1인 경우, 현재 패스 CP에 포함되는 모든 유향 가지에 active 마크를 부여한다(S198). 그리고, WJ에 done 마크를 부여하고(S200), 스텝 S180의 처리로 복귀한다. 반대로, J≤1이 아닌 경우, #JP(CP)+t≤DD_T-D인지 여부를 판단한다(S190). #JP(CP)+t≤DD_T-D가 아닌 경우, 스텝 S198 및 S200의 처리를 거쳐서 스텝 S180의 처리로 복귀한다. #JP(CP)+t≤DD_T-D인 경우, $J=n^{j/k}$를 만족하는 j를 산출한다(S192).

[0307] 계속해서, 현재 패스 CP에 포함되는 길이 J의 유향 가지가 복수 존재하는 경우, 현재 패스 CP의 시작점으로부터 가장 먼 위치에 있는 유향 가지를 추출한다(S194). 계속해서, 스텝 S194에서 추출된 유향 가지의 시작점으로부터 뻗어나간$n^{1/k}$-1개의 길이 $n^{(j-1)/k}$의 유향 가지의 직후에 $n^{(j-1)/k}$의 길이를 갖는 1개의 유향 가지를 추가하고, 스텝 S194에서 추출된 유향 가지를 소거한다(S196). 그리고, 스텝 S184의 처리로 복귀한다.

[0308] 단, 스텝 S184 내지 S196 사이에 발생하는 루프 처리는, WJ_S로부터 WJ_E-1로의 유향 패스가 모두 길이 1의 유향 가지로 구성되거나, 또는 그 이상의 유향 가지를 치환함으로써 WJ_S로부터 WJ_E-1로의 유향 패스에 포함되는 유향 가지수가 DD_T를 초과하게 되는 경우에 종료한다. 또한, 상기한 스텝 S180 내지 S200 사이에 발생하는 루프 처리는, 임시 유향 그래프 I'에 포함되는 유향 가지 중으로부터, done이 설정되어 있지 않고, 또한 길이가 2 이상인 유향 가지가 모두 없어진 시점에서 종료한다.

[0309] 이상 설명한 알고리즘을 임시 유향 그래프 I'에 적용함으로써, 도 15에 나타내는 유향 그래프 I가 생성된다. 이 유향 그래프 I는, 계약자수 n=64, 파라미터 k=6의 경우에 대해 생성된 것이다. 이 유향 그래프 I를 이용하면, AI05 방식에 비해, 각 단말 장치(122)가 키 생성에 필요로 하는 계산량과, 각 단말 장치(122)가 유지해야 할 키수를 저감시키는 것이 가능해진다.

[0310] [키 생성 블록]

[0311] 다음에, 다시 도 8을 참조하면서, 키 생성 블록의 상세에 대해 설명한다. 키 생성 블록은, 주로 초기 중간 키 설정부(112)와, 키 생성부(114)와, 암호화부(116)에 의해 구성된다.

[0312] (초기 중간 키 설정부(112))

[0313] 초기 중간 키 설정부(112)는, 논리 이분목에 포함되는 모든 중간 노드 및 뿌리 노드의 유향 그래프 I의 루트에 대응하는 중간 키를 생성한다. 예를 들어, 초기 중간 키 설정부(112)는, PRSG에 의해 의사 난수를 발생시켜 각 루트에 대응하는 중간 키를 설정해도 되고, 또는 소정의 수치에 의해 각 루트의 중간 키를 설정해도 된다.

[0314] (키 생성부(114))

[0315] 키 생성부(114)는, PRSG를 이용하여 중간 키 또는 세트 키를 생성한다. 이때, 키 생성부(114)는, AI05 방식의 유향 그래프 H, AO6(A+B) 방식의 유향 그래프 I, AO6(A) 방식의 유향 그래프, AO6(B) 방식의 유향 그래프, 또는 그 밖의 방식의 유향 그래프에 기초하여 의사 난수 생성 연산을 실행함으로써, 원하는 중간 키 또는 세트 키를 생성할 수 있다. 상기한 바와 같이, PRSG는 유향 그래프를 구성하는 유향 가지의 시단부에 대응하는 중간 키를 입력하면, 그 중간 키에 대응하는 세트 키와, 그 유향 가지의 종단부에 대응하는 중간 키를 출력한다. 유향 그래프의 수평 좌표축 상에 있는 하나의 좌표점으로부터 복수의 유향 가지가 뻗어나가고 있는 경우에는, 그 좌표점에 대응하는 중간 키를 입력하면, 복수의 중간 키를 도출할 수 있다.

[0316] 또한, AI05 방식에서는, 상기 수학식 2에서 PRSG의 입출력이 정의되어 있었지만, 본 실시 형태에서는, $t(S_1)||$

…||$t(S_k)$||$k(S_0)$←PRSG($t(S_0)$)에 의해 PRSG의 입출력이 정의된다. 즉, AI05 방식에 의한 PRSG의 출력은, 입력된 중간 키에 대응하는 좌표점을 시작점으로 하는 유향 가지의 수를 d로 하였을 때, λ비트의 입력에 대해 (d+1)λ비트의 출력을 내도록 구성되어 있었다. 이에 대해, 본 실시 형태에 관한 PRSG는, d의 값에 관계없이 (k+1)λ비트의 출력을 내도록 구성된다. 단, k는 시스템 파라미터이다.

[0317] 본 실시 형태에 있어서, 부분 집합 S_0에 대응하는 중간 키 $t(S_0)$가 그 PRSG에 입력된 경우, 그 출력을 $t(S_1)$||…||$t(S_k)$||$k(S_0)$로 하고 있다. 그 출력에 포함되는 $t(S_1)$||…||$t(S_k)$의 부분은, 부분 집합 S_0에 대응하는 좌표점을 시작점으로 하는 유향 가지의 종점인 좌표점의 각각에 대해, 대응하는 부분 집합 S_1,…, S_k의 중간 키이다. 또한, 부분 집합 S_0에 대응하는 좌표점과 부분 집합 S_i에 대응하는 좌표점을 연결하는 유향 가지의 길이가 $n^{(i-1)/k}$가 된다. 예를 들어, 부분 집합 S_0에 대응하는 좌표점과 부분 집합 S_i에 대응하는 좌표점을 연결하는 유향 가지의 길이가 $n^{2/k}$이면, PRSG($t(S_0)$)의 출력의 처음부터 3번째의 λ비트의 부분이 $t(S_i)$가 된다. 만일, 부분 집합 S_0에 대응하는 좌표점으로부터 길이 $n^{(i-1)/k}$의 유향 가지가 나와 있지 않은 경우, $t(S_i)$의 부분이 PRSG으로부터 출력되지만 사용되지 않는다.

[0318] 예를 들어, 키 생성부(114)는, PRSG에 대해, 유향 그래프 I 상의 좌표점 S_0에 대응하는 중간 키 $t(S_0)$를 입력하면, 좌표점 S_0을 시단부로 하는 복수의 유향 가지에 대해, 그 종단부의 좌표점 S_1, S_2,…, S_m에 대응하는 중간 키 $t(S_1)$, $t(S_2)$,…, $t(S_m)$와, 세트 키 $k(S_0)$를 도출할 수 있다. 또한, m은 좌표점 S_0으로부터 뻗어나가는 유향 가지의 개수를 나타내고 있다. 또한, 중간 키를 이용하지 않는 경우에는, 예를 들어 세트 키 $k(S_0)$를 PRSG에 입력하고, 복수의 세트 키 $k(S_1)$, $k(S_2)$,…, $k(S_m)$를 도출하도록 구성하는 것도 가능하다.

[0319] (암호화부(116))

[0320] 암호화부(116)는, 세트 키를 이용하여 콘텐츠 또는 콘텐츠 키를 암호화하여 암호문을 생성한다. 암호화부(116)는, 세트 시스템(SS)을 구성하는 모든 부분 집합 중, 소정의 부분 집합에 대응하는 1개 이상의 세트 키를 이용하여 콘텐츠 또는 콘텐츠 키를 암호화한다. 따라서, 하나의 콘텐츠 또는 콘텐츠 키에 대해 복수의 암호문이 생성되는 경우도 있다.

[0321] [정보 생성 블록]

[0322] 다음에, 다시 도 8을 참조하면서, 정보 생성 블록의 상세에 대해 설명한다. 정보 생성 블록은, 주로 부분 집합 결정부(120)와, 경로 정보 생성부(121)에 의해 구성된다. 또한, 통신부(118)에 대해서도 함께 설명한다.

[0323] (부분 집합 결정부(120))

[0324] 부분 집합 결정부(120)는, 콘텐츠 또는 콘텐츠 키를 암호화하는 세트 키를 결정한다. 즉, 부분 집합 결정부(120)는 소정의 허락 계약자의 단말 장치(122)가 포함되는 적어도 1개의 부분 집합을 추출하고, 각 단말 장치(122)에 배포되는 세트 키의 종류를 결정한다. 예를 들어, 부분 집합 결정부(120)는 콘텐츠 또는 콘텐츠 키의 재생을 허락하지 않는 배제 계약자의 집합 (R), 및 전체 계약자의 집합 (N)으로부터 배제 유저의 집합 (R)을 제외한 허락 계약자의 집합 (N\R)을 결정한다. 즉, 세트 시스템(SS)에 포함되는 부분 집합에 의해, 허락 계약자의 집합 ($N \setminus R = S_1 \cup S_2 \cup \cdots \cup S_m$)을 구성하는 부분 집합의 세트($S_1$, S_2,…, S_m)를 결정한다.

[0325] (경로 정보 생성부(121))

[0326] 경로 정보 생성부(121)는, 유향 그래프에 포함되는 유향 가지의 정보를 참조하여, 이 유향 그래프의 시작점으로부터 소정의 좌표점에 도달하는 유향 패스의 정보를 추출한다. 소정의 좌표점이라 함은, 부분 집합 결정부(120)에 의해 선택된 각 부분 집합에 대응하는 좌표점이다. 또한, 경로 정보 생성부(121)는 상기한 키 생성 경로 정보 추출부의 일례이다.

[0327] 이미 설명한 바와 같이, 상기한 AI05 방식 등의 키 배신 방식은, 모든 단말 장치(122)가 유향 그래프의 정보를 보유하고 있거나, 또는 각 단말 장치(122)가 각 키 배신 방식의 알고리즘에 기초하여 유향 그래프를 산출하는 것을 전제로 하고 있다. 그러나, 이 전제는, 단말 장치(122)의 메모리량을 압박하여, 연산 부하를 현저하게 증대시키기 위해, 현실적이지 않다고 하는 문제가 있다.

[0328] 예를 들어, AI05 방식의 유향 그래프 H(도 16을 참조)의 경우, 계약자 3의 단말 장치(122)는, 부분 집합 S_0=[1, 4]에 대응하는 중간 키 $t(S_0)$를 미리 유지하고 있다. 가령, 부분 집합 결정부(120)가 부분 집합 S=[1, 8]을 선택하고, 이에 대응하는 세트 키 k(S)를 이용하여 콘텐츠 키를 암호화한 경우를 고려하면, 계약자 3의 단말 장치(122)는, 우선 중간 키 $t(S_0)$와 PRSG를 이용하여 중간 키 t(S)를 도출할 필요가 있다. 그러나, 이를 도출하기 위해, 계약자 3의 단말 장치(122)는, 유향 그래프 H(1→64) 상에 좌표점 S_0=[1, 4]로부터 좌표점 S_1=[1, 8]에 유향 가지가 존재한다는 정보(도 16의 굵은 선의 일부)를 유지하고 있을 필요가 있다.

[0329] 그러나, 하기 수학식 4에 나타내는 바와 같이, 유향 그래프 H(1→n) 상에는 (n-1)개의 유향 가지가 존재하므로, n이 커지면 모든 유향 가지의 정보를 보유하는 것이 곤란해진다. 예를 들어, 1개의 유향 가지의 정보가 8Byte 정도의 정보량으로 표현할 수 있다고 가정하면, 현실적인 계약자수 n이 $n=2^{32}=4,294,967,296$이므로, 유향 그래프 H(1→n)의 정보만으로 약 32GByte나 되는 기억 용량을 필요로 한다.

수학식 4

$$t \cdot n^{0/k} + t \cdot n^{1/k} + \cdots + t \cdot n^{k-1/k}$$

[0330] $$= t\sum_{i=0}^{k-1} t \cdot n^{i/k}$$

$$= n-1$$

[0331] 따라서, 본건 출원인은, 선택한 부분 집합(상기한 예에서는 [1, 8])의 정보에 부가하여, 그 유향 그래프의 시작점으로부터, 그 부분 집합에 대응하는 좌표점에 도달하는 유향 패스의 정보도 단말 장치(122)에 배신하는 방식을 고안한 것이다. 예를 들어, 상기한 예와 마찬가지로, 부분 집합 [1, 8]이 선택되면, 유향 그래프 H(1→64)의 시작점 [1, 1]로부터 좌표점 [1, 8]에 도달하는 유향 패스(도 16의 굵은 선)의 정보가 단말 장치(122)에 배신된다. 이 특징을 실현시키는 구성이 경로 정보 생성부(121)이다.

[0332] 이하의 설명에 있어서, 콘텐츠 키 mek를 세트 키 $k(S_0)$로 암호화한 암호문을 $C(k(S_0), mek)$로 표기한다. 또한, 부분 집합 S_i=[SP_i, TP_i]의 SP_i, TP_i, S_i는 하기의 의미를 갖는다.

[0333] (1) 좌표점 S_i가 우측 방향의 유향 그래프에 포함되는 경우

[0334] SP_i : 부분 집합 S_i의 요소 중에서 가장 작은 번호

[0335] TP_i : 부분 집합 S_i의 요소 중에서 가장 큰 번호

[0336] ⇒ S_i={SP_i, SP_{i+1},…, TP_i}

[0337] (2) 좌표점 S_i가 좌측 방향의 유향 그래프에 포함되는 경우

[0338] SP_i : 부분 집합 S_i의 요소 중에서 가장 큰 번호

[0339] TP_i : 부분 집합 S_i의 요소 중에서 가장 작은 번호

[0340] ⇒ S_i={SP_i, SP_{i-1},…, TP_i}

[0341] (3) SP_i=TP_i의 경우

[0342] ⇒ S_i={SP_i}

[0343] 또한, SP_i와 TP_i는 1 이상 n 이하의 값이다. 또한, SP_i는 유향 그래프의 시작점과 교차하는 세로선의 번호(계약자의 번호)를 나타내고, TP_i는 선택된 부분 집합의 좌표점과 교차하는 세로선의 번호(계약자의 번호)를 나타낸다.

[0344] 우선, 경로 정보 생성부(121)는, 하기 수학식 5에 나타내는 바와 같이, 상기한 부분 집합 S_i에 포함되는 계약자

의 정보에 대해, 그 부분 집합 S_i를 도출하는 데 필요한 유향 패스의 정보를 생성하여 부가한다. 또한, 본 실시 형태에 관한 경로 정보 생성부(121)는, 유향 패스의 정보로서, 이 유향 패스에 포함되는 각 유향 가지의 종단부를 나타내는 정보(교차하는 종축의 번호 IP_{ij} ; $1 \leq IP_{ij} \leq n$)를 부가한다. 단, 유향 그래프 상의 좌표점 $[SP_i, SP_i]$와 좌표점 $[SP_i, TP_i]$를 연결하는 유향 패스에 p개($p \leq DD_T$)의 유향 가지가 존재하는 것으로 한다.

수학식 5

[0345] $$S_i = (SP_i, IP_{i1}, \cdots, IP_{i(p-1)}, TP_i)$$

[0346] (예 1)

[0347] 예를 들어, 계약자수 n=64, 파라미터 k=6의 AI05 방식에 있어서, 부분 집합 결정부(120)가 부분 집합 S=[1, 8]을 선택한 경우를 고려한다. 그러면, 경로 정보 생성부(121)는, 유향 패스의 정보를 포함하는 부분 집합 S의 정보로서, S=(1, 2, 4, 8)을 생성한다[도 16의 굵은 선(유향 패스)을 참조].

[0348] (예 2)

[0349] 다른 예로서, 계약자수 n=64, 파라미터 k=6의 AI05 방식에 있어서, 계약자(45)와 계약자(55)가 배제된 경우를 고려한다. 이때, 부분 집합 결정부(120)가 부분 집합 S_1=[1, 44], S_2=[48, 46], S_3=[49, 54], S_4=[64, 56]을 선택하였다고 하면, 경로 정보 생성부(121)는, 각 부분 집합에 유향 패스의 정보를 부가한 하기의 정보를 생성한다[도 17의 굵은 선(유향 패스)을 참조].

[0350] S_1=(1, 2, 4, 8, 16, 32, 40, 44),

[0351] S_2=(48, 47, 46),

[0352] S_3=(49, 50, 52, 54),

[0353] S_4=(64, 63, 61, 57, 56).

[0354] (예 3)

[0355] 다른 예로서, 계약자수 n=64, 파라미터 k=6의 A06(A+B) 방식에 있어서, 계약자 45와 계약자 55가 배제된 경우를 고려한다. 이때, 부분 집합 결정부(120)가 부분 집합 S_1=[1, 44], S_2=[48, 46], S_3=[49, 54], S_4=[64, 56]을 선택하였다고 하면, 경로 정보 생성부(121)는, 각 부분 집합에 유향 패스의 정보를 부가한 하기의 정보를 생성한다[도 18의 굵은 선(유향 패스)을 참조].

[0356] S_1=(1, 33, 37, 41, 42, 43, 44),

[0357] S_2=(48, 47, 46),

[0358] S_3=(49, 53, 54),

[0359] S_4=(64, 60, 56).

[0360] 상기한 바와 같이, 하나의 부분 집합에 대해 유향 패스의 정보가 p+1개의 번호 IP_{ij}에 의해 나타내어진다. 또한, $p \leq DD_T$이며, 각 번호 IP_{ij}를 표현하는 데 log(n)비트의 메모리 영역을 필요로 하므로, 하나의 부분 집합을 나타내는 데 최대 $(DD_T+1)*\log(n)$비트가 필요한 것을 알 수 있다. 단, DD_T의 값은 채용하는 키 배신 방식마다 다르다. 예를 들어, AI05 방식에서는 $DD_T=(2k-1)*(n^{1/k}-1)$이며, A06(A+B) 방식에서는 $DD_T=k(n^{1/k}-1)$이다.

[0361] (통신부(118))

[0362] 통신부(118)는, 암호화부(116)에 의해 암호화된 콘텐츠 또는 콘텐츠 키를 잎 노드에 대응하는 모든 단말 장치(122)에 대해 배신한다. 또한, 통신부(118)는 유향 그래프 I에 기초하여 소정의 중간 키를 단말 장치(122)에 대해 배신한다. 이때, 통신부(118)는 각 단말 장치(122)가 자신이 포함되는 부분 집합에 대응하는 중간 키를 모두 도출할 수 있도록 필요 최저한의 중간 키를 배신한다. 또한, 통신부(118)는 소정의 유향 그래프의 정보를

각 단말 장치(122)에 대해 배신한다. 또한, 통신부(118)는 허락 계약자의 집합 (N\R), 또는 허락 계약자의 집합 ($N\setminus R=S_1\cup S_2\cup\cdots\cup S_m$)을 구성하는 부분 집합 ($S_1$, S_2,…, S_m)의 정보를 각 단말 장치(122)에 배신한다. 이때, 통신부(118)는 경로 정보 생성부(121)에 의해 부가된 유향 패스의 정보도 배신한다.

[0363] [단말 장치(122)의 구성]

[0364] 다음에, 도 19를 참조하면서, 본 실시 형태에 관한 단말 장치(122)의 구성에 대해 설명한다. 도 19는 단말 장치(122)의 구성을 도시하는 설명도이다.

[0365] 도 19를 참조하면, 단말 장치(122)는, 주로 통신부(124)와, 판단부(126)와, 키 생성부(128)와, 복호부(130)에 의해 구성된다. 또한, 단말 장치(122)는 상기의 유저에 대응하고 있다. 또한, 통신부(124)는 상기한 키 생성 경로 정보 취득부 및 암호 정보 취득부의 일례이다. 그리고, 키 생성부(128)는 상기한 키 정보 생성부의 일례이다. 또한, 복호부(130)는 상기한 암호 정보 복호부의 일례이다.

[0366] (통신부(124))

[0367] 통신부(124)는 키 배신 서버(102)로부터 배신된 정보를 수신한다. 예를 들어, 통신부(124)는 키 배신 서버(102)로부터 배신된 콘텐츠, 콘텐츠 키, 중간 키, 유향 그래프에 관한 정보, 또는 허락 계약자에 관한 정보 등을 수신한다. 또한, 통신부(124)는, 유선 또는 무선의 네트워크에 접속된 복수의 정보원[예를 들어, 키 배신 서버(102)], 또는 네트워크를 통하지 않고 직접적 또는 간접적으로 접속된 정보원(예를 들어, 광 디스크 장치, 자기 디스크 장치, 또는 휴대형 단말 장치 등의 정보 미디어)으로부터 정보를 취득하는 구성이어도 된다.

[0368] (판단부(126))

[0369] 판단부(126)는 세트 키에 대응하는 부분 집합 중 어느 하나에 자신이 요소로서 포함되는지 여부를 판단한다. 판단부(126)는 키 배신 서버(102)의 부분 집합 결정부(120)에 의해 선택된 부분 집합 중 어느 하나에 자신이 포함되는지 여부를 판단한다. 이때, 판단부(126)는 키 배신 서버(102)로부터 취득한 상기 부분 집합의 정보를 참조한다.

[0370] (키 생성부(128))

[0371] 키 생성부(128)는 미리 배신된 중간 키와 PRSG를 이용하여 원하는 중간 키 또는 세트 키를 생성한다. 이때, 키 생성부(128)는, 키 배신 서버(102)로부터 취득한 유향 패스의 정보를 참조하여, 이 정보에 기초하여 원하는 중간 키 또는 세트 키를 생성한다. 또한, 판단부(126)에 의해 자신이 포함되는 부분 집합이 존재하지 않는다고 판단된 경우에는, 중간 키 또는 세트 키의 생성 처리를 종료한다. 상기한 PRSG는, 키 배신 서버(102)가 유지하는 PRSG와 실질적으로 동일하고, 소정의 유향 그래프에 기초하여, 유향 가지의 시단부에 대응하는 중간 키를 입력하면, 이 중간 키에 대응하는 세트 키와, 그 유향 가지의 종단부에 대응하는 중간 키가 출력된다. 물론, 하나의 좌표점으로부터 복수의 유향 가지가 뻗어나가고 있는 경우에는, 해당 좌표점에 대응하는 중간 키를 입력하면 각 유향 가지의 종단부에 대응하는 복수의 중간 키를 얻을 수 있다.

[0372] (알고리즘)

[0373] 여기서, 도 20을 참조하면서, 계약자 u의 단말 장치(122)에 의한 키 도출 알고리즘에 대해 설명한다. 도 20은, 계약자 u의 단말 장치(122)가 키를 도출하는 처리를 나타낸 설명도이다. 또한, 이 처리는, 주로 키 생성부(128)에 의해 실행된다.

[0374] 우선, 계약자 u의 단말 장치(122)에는, 키 배신 서버(102)의 부분 집합 결정부(120)에 의해 선택된 m개의 부분 집합 (S_1,…, S_m)을 나타내는 정보와, 경로 정보 생성부(121)에 의해 부분 집합마다 부가된 유향 패스의 정보 $S_j=(SP_j, IP_{j,1},\cdots, IP_{j,(p-1)}, TP_j)$(단, j=1,…, m)이 부여되어 있다. 또한, 판단부(126)에 의해, 자신이 부분 집합 $S_i=[SP_i, TP_i]$에 포함되어 있다고 판단된 것으로 가정한다. 따라서, 키 생성부(128)는, 원하는 중간 키 또는 세트 키를 생성하는 처리에 있어서, 유향 패스의 정보 $S_i=(SP_i, IP_{i,1},\cdots, IP_{i,(p-1)}, TP_i)$를 참조한다. 이하, 도 20에 나타낸 흐름도를 따라 구체적으로 설명한다.

[0375] 도 20을 참조하면, 우선, 변수 $IP_{i,p}$에 TP_i의 값을 설정한다(S402). 계속해서, 카운터 j를 1로 초기화한다(S404). 계속해서, 계약자 u의 단말 장치(122)가 부분 집합 $[SP_i, IP_{i,j}]$에 포함되는지 여부를 판단한다(S406). 포함되지 않는 경우, 카운터 j를 인크리먼트하여(S408), 다시 스텝 S406으로 복귀한다. 반대로, 포함되는

경우, 변수 sp에 SP_i를 설정하고, 변수 ep에 $IP_{i,j}$를 설정한다(S410). 이때, 계약자 u의 단말 장치(122)는, 부분 집합 [sp, ep]에 대응하는 중간 키 t([sp, ep])를 미리 유지하고 있다.

[0376] 계속해서, 중간 키 t([sp, ep])를 변수 $t_{current}$로 설정한다(S412). 계속해서, ep=TP_i인지 여부를 판단한다(S414). ep=TP_i인 경우, $t_{current}$를 PRSG에 입력하고, 그 출력 PRSG($t_{current}$)를 λ비트마다 구획한 k+1번째의 부분[부분 집합[SP_i, TP_i]의 세트 키 k([SP_i, TP_i])에 해당]을 취출하여(S424), 세트 키의 생성 처리를 종료한다.

[0377] 반대로, ep=TP_i가 아닌 경우, 변수 logd(하기 수학식 6을 참조)를 계산한다(S416). 즉, logd는, $IP_{i,j}$로부터 $IP_{i,j+1}$로의 유향 가지의 길이가 $n^{1/k}$의 몇 승인지를 나타내는 수치이다. 계속해서, 카운터 j를 인크리먼트하여(S418), ep에 대해 $IP_{i,j}$를 설정한다(S420). 계속해서, $t_{current}$를 PRSG에 입력하고, 그 출력 PRSG($t_{current}$)를 λ비트마다 구분한 logd+1번째의 부분을 새로운 $t_{current}$로 설정한다(S422). 그 후, 스텝 S414로 복귀한다.

수학식 6

[0378] $$\log d = \log_{n^{1/k}} \left| IP_{i,(j+1)} - IP_{i,j} \right|$$

[0379] (복호부(130))

[0380] 복호부(130)는 키 생성부(128)에 의해 생성된 세트 키를 이용하여 콘텐츠 또는 콘텐츠 키를 복호한다. 또한, 복호부(130)는 콘텐츠 키를 이용하여 콘텐츠를 복호하는 처리도 실행 가능하다.

[0381] 이상, 본 실시 형태에 관한 단말 장치(122)의 구성에 대해 설명하였다. 상기한 구성에 의해, 단말 장치(122)는 키 배신 서버(102)로부터 취득한 유향 패스의 정보를 이용하여 원하는 세트 키를 생성하는 것이 가능해진다. 그 결과, 단말 장치(122)는, 방대한 유향 그래프의 정보를 모두 유지 또는 생성할 필요가 없어지고, 메모리량 및 연산 부하를 현실적인 레벨까지 억제하는 것이 가능해진다.

[0382] <제2 실시 형태>

[0383] 다음에, 본 발명의 제2 실시 형태에 관한 키 제공 시스템의 구성 및 키 배신에 관한 구체적인 방식에 대해 상세하게 설명한다. 단, 상기한 제1 실시 형태와 실질적으로 동일한 기능 구성을 갖는 구성 요소에 대해서는 동일 부호를 부여함으로써 상세한 설명을 생략한다.

[0384] 상기한 제1 실시 형태에 있어서의 키 제공 시스템(100)의 특징은, 키 배신 서버(102)로부터 단말 장치(122)에 대해 제공되는 유향 그래프의 정보에 있는 것은 이미 설명하였다. 특히, 유향 그래프의 정보로서, 소정의 좌표점에 도달하는 유향 패스에 포함되는 모든 유향 가지의 정보를 단말 장치(122)에 제공하는 수단에 특징을 갖는 것이다. 제1 실시 형태에서는, 해당 유향 가지의 정보로서 각 유향 가지의 종단부를 나타내는 정보를 고려하였지만, 소정의 좌표점에 도달 가능한 경로를 단말 장치(122)가 인식 가능하면 반드시 이에 한정되는 것은 아니다.

[0385] 따라서, 제2 실시 형태에서는, 키 배신 서버(102)가 구비하는 부분 집합 결정부(120)에 의해 선택된 소정의 부분 집합 S_i=[SP_i, TP_i]에 대응하는 좌표점 S_i에 대해, 이 좌표점 S_i에 도달하는 유향 패스의 정보로서, 이 유향 패스에 포함되는 각 유향 가지의 길이를 나타내는 정보 $LD_{i,j}$를 단말 장치(122)에 제공하는 수단[경로 정보 생성부(121)]에 대해 설명한다.

[0386] 또한, 상기한 각 유향 가지의 길이 LD_{ij}는, 어느 유향 그래프의 좌표점 [SP_i, SP_i]로부터 좌표점 [SP_i, TP_i]에 도달하는 유향 패스 상의 j번째에 위치하는 유향 가지의 길이 $len_{i,j}$에 대해, 하기 수학식 7에 의해 표현되는 값이다. 즉, 각 유향 가지의 길이는, $n^{1/k}$의 $LD_{i,j}$승으로서 표현된다(단, $0 \leq LD_{i,j} < k$임).

수학식 7

[0387] $$LD_{i,j} = \log_{n^{1/k}} len_{i,j}$$

[0388] 따라서, 키 배신 서버(102)가 구비하는 경로 정보 생성부(121)는, 각 유향 가지의 길이를 나타내는 정보 $LD_{i,j}$를 이용하여, 상기한 부분 집합 S_i를 하기 수학식 8과 같이 표현한다. 즉, 경로 정보 생성부(121)는, 부분 집합 S_i에 관한 것으로, 하기 수학식 8로 표현되는 유향 패스의 정보를 생성한다. 물론, 선택된 모든 부분 집합 S_i(i=1,…, m)에 대해 마찬가지로 유향 패스의 정보가 생성된다.

수학식 8

[0389] $$S_i = (SP_i, LD_{i,1}, \cdots, LD_{i,p-1}, LD_{i,p})$$

[0390] (예 1)

[0391] 예를 들어, 계약자수 n=64, 파라미터 k=6의 AI05 방식에 있어서, 계약자 45와 계약자 55가 배제된 경우를 고려한다. 이때, 부분 집합 결정부(120)가 부분 집합 S_1=[1, 44], S_2=[48, 46], S_3=[49, 54], S_4=[64, 56]을 선택하였다고 하면, 제1 실시 형태에 관한 경로 정보 생성부(121)가 생성되는 정보는 하기와 같이 표현된다(도 17을 참조).

[0392] (제1 실시 형태의 경우)

[0393] S_1=(1, 2, 4, 8, 16, 32, 40, 44),

[0394] S_2=(48, 47, 46),

[0395] S_3=(49, 50, 52, 54),

[0396] S_4=(64, 63, 61, 57, 56).

[0397] 한편, 상기한 제1 실시 형태와 동일 조건 하에, 제2 실시 형태에 관한 경로 정보 생성부(121)가 유향 가지의 길이에 기초하여 생성하는 정보는 하기와 같이 표현된다.

[0398] (제2 실시 형태의 경우)

[0399] S_1=(1, 0, 1, 2, 3, 4, 3, 2),

[0400] S_2=(48, 0, 0),

[0401] S_3=(49, 0, 1, 1),

[0402] S_4=(64, 0, 1, 2, 0).

[0403] (예 2)

[0404] 다른 예로서, 계약자수 n=64, 파라미터 k=6의 A06(A+B) 방식에 있어서, 계약자 45와 계약자 55가 배제된 경우를 고려한다. 이때, 부분 집합 결정부(120)가 부분 집합 S_1=[1, 44], S_2=[48, 46], S_3=[49, 54], S_4=[64, 56]을 선택하였다고 하면, 제1 실시 형태에 관한 경로 정보 생성부(121)가 생성하는 정보는 하기와 같이 표현된다(도 18을 참조).

[0405] (제1 실시 형태의 경우)

[0406] S_1=(1, 33, 37, 41, 42, 43, 44),

[0407] S_2=(48, 47, 46),

[0408] S_3=(49, 53, 54),

[0409] S_4=(64, 60, 56).

[0410] 한편, 상기한 제1 실시 형태와 동일 조건 하에, 제2 실시 형태에 관한 경로 정보 생성부(121)가 유향 가지의 길이에 기초하여 생성하는 정보는 하기와 같이 표현된다.

[0411] (제2 실시 형태의 경우)

[0412] S_1=(1, 5, 2, 2, 0, 0, 0),

[0413] S_2=(48, 0, 0),

[0414] S_3=(49, 4, 0),

[0415] S_4=(64, 2, 2).

[0416] 상기한 바와 같이, 제2 실시 형태를 적용하면, 하나의 부분 집합에 관한 유향 패스의 정보는, 1개의 시작점 정보 SP_i($1 \le SP_i \le n$)와 p개의 길이 정보 $IP_{i,j}$($0 \le IP_{i,j} \le k-1$)에 의해 표현된다. 또한, $p \le DD_T$이며, 각 부분 집합은 $\log(n)+DD_T*\log(k)$ 비트의 데이터로 나타내어진다. 한편, 상기한 제1 실시 형태의 경우에는, 하나의 부분 집합을 나타내는 데 $(DD_T+1)*\log(n)$ 비트가 필요했다. 또한, $k|\log(n)$이므로, $\log(k) \le \log(\log(n)) < \log(n)$이 되고, $\log(n)+DD_T*\log(k) < (DD_T+1)*\log(n)$이라는 관계를 얻을 수 있다. 따라서, 제2 실시 형태를 적용함으로써, 상기한 제1 실시 형태를 적용하기보다도 각 부분 집합 S_i를 표현하기 위한 정보를 저감시킬 수 있다. 그 결과, 키 배신 서버(102)로부터 단말 장치(122)에 대해 제공되는 정보량을 저감(통신량의 삭감 또는 기록 매체의 용량을 절약)하는 것이 가능해진다.

[0417] 그런데, 부분 집합으로서, S_i=[3, 3] 등의 한 명의 유저를 포함하는 부분 집합이 선택된 경우에, 그것을 어떻게 표현할지에 대해 고려한다. 이 경우, 상기한 제1 실시 형태의 방식에서는 S_i=(3, 3)으로 표현된다. 또한, 상기한 제2 실시 형태의 방식에서는 몇 가지의 표현 방법을 고려할 수 있지만, 1개의 표현 방법으로서는, S_i=(3)과 같이 오직 하나의 수치로 표현하는 방법을 고려할 수 있다. 다른 표현 방법으로서는, 특수 기호 ⊥를 사용하여, S_i=(3, ⊥)로 표현할 수도 있다. 후자의 방법을 채용하면, 유저수가 2 이상인 부분 집합에 있어서 2번째 이후가 반드시 0 이상의 정수가 되므로, 유저수가 1인 것을 인식하는 것이 가능해진다.

[0418] (알고리즘)

[0419] 다음에, 도 21을 참조하면서, 제2 실시 형태에 관한 단말 장치(122)에 의해, 상기한 키 배신 서버(102)로부터 취득한 각 부분 집합의 정보를 이용하여 키가 생성되는 알고리즘에 대해 설명한다. 도 21은, 계약자 u의 단말 장치(122)가 키를 도출하는 처리를 나타낸 설명도이다. 또한, 이 처리는, 주로, 단말 장치(122)가 구비하는 키 생성부(128)에 의해 실행된다.

[0420] 우선, 계약자 u의 단말 장치(122)에는, 키 배신 서버(102)의 부분 집합 결정부(120)에 의해 선택된 m개의 부분 집합 (S_1,…, S_m)을 나타내는 정보와, 경로 정보 생성부(121)에 의해 부분 집합마다 부가된 유향 패스의 정보 S_j=(SP_j, $LD_{j,1}$,…, $LD_{j,p-1}$, $LD_{j,p}$)(단, j=1,…, m)가 부여되어 있다. 또한, 판단부(126)에 의해, 자신이 부분 집합 S_i=[SP_i, TP_i]에 포함되어 있다고 판단된 것으로 가정한다. 따라서, 키 생성부(128)는, 원하는 중간 키 또는 세트 키를 생성하는 처리에 있어서, 유향 패스의 정보 S_i=(SP_i, $LD_{i,1}$,…, $LD_{i,p-1}$, $LD_{i,p}$)를 참조한다. 이하, 도 21에 나타낸 흐름도를 따라 구체적으로 설명한다.

[0421] 도 21을 참조하면, 우선, 변수 $IP_{i,0}$에 SP_i의 값을 설정한다(S432). 계속해서, SP_i의 홀수/짝수를 판단하여, SP_i가 홀수이면 변수 sign에 1을 설정하고, SP_i가 짝수이면 -1을 설정한다(S434). 계속해서, 카운터 j를 1부터 p까지 움직이면서, $IP_{i,j}$(하기 수학식 9)를 계산한다(S436). 여기서, p는 부분 집합 S_1의 표현에 있어서, SP_i에 이어지는 0 이상의 정수치의 개수를 나타낸다. 즉, S_1=[3, 3] 등과 같이S_1=(3)이나 S_1=(3, ⊥)로 표현되는 유저수 1의 부분 집합의 경우, p=0이 되므로 S436의 처리가 실행되지 않는다. 계속해서, 카운터 j를 0으로 초기화한다(S438).

수학식 9

[0422] $$IP_{i,j} = IP_{i,j-1} + sign * n^{LD_{i,j}/k}$$

[0423] 계속해서, 계약자 u의 단말 장치(122)가 부분 집합 [SP_i, $IP_{i,j}$]에 포함되는지 여부를 판단한다(S440). 계약자 u의 단말 장치(122)가 부분 집합 [SP_i, $IP_{i,j}$]에 포함되지 않는 경우, 카운터 j를 인크리먼트하여 다시 스텝 S440으로 복귀한다(S442). 반대로, 계약자 u의 단말 장치(122)가 부분 집합 [SP_i, $IP_{i,j}$]에 포함되는 경우, 변수 sp에 SP_i의 값을 설정하고, 또한 변수 ep에 $IP_{i,j}$의 값을 설정한다(S444). 계속해서, 계약자 u의 단말 장치(122)가 미리 유지하고 있는 중간 키 중으로부터 중간 키 t([sp, ep])를 선택하여 $t_{current}$로 설정한다(S446).

[0424] 계속해서, 변수 ep가 $IP_{i,p}$인지 여부를 판단한다(S448). ep=$IP_{i,p}$인 경우, $t_{current}$를 PRSG에 입력하고, 그 출력 PRSG($t_{current}$)를 λ비트마다 구획한 k+1번째의 부분[세트 키 k([SP_i, $IP_{i,p}$])에 해당]을 추출하여(S456), 세트 키의 생성 처리를 종료한다. 반대로, ep=$IP_{i,p}$가 아닌 경우, 카운터 j를 인크리먼트한다(S450). 계속해서, 변수 ep에 $IP_{i,j}$의 값을 설정한다(S452). 계속해서, $t_{current}$를 PRSG에 입력하고, 그 출력 PRSG($t_{current}$)를 λ비트마다 구획한 $LD_{i,j}$+1번째의 부분을 추출하고, $t_{current}$로 설정한다(S454). 그리고, 스텝 S448로 복귀한다.

[0425] 이상 설명한 알고리즘을 이용하여 원하는 키를 생성할 수 있다. 물론, 본 실시 형태에 관한 키 생성부(128)는, 이에 한정되는 것은 아니며, 키 배신 서버(102)로부터 취득한 유향 패스의 정보 S_i에 포함되는 각 유향 가지의 길이를 나타내는 정보 $LD_{i,j}$로부터, 각 유향 가지의 종단부를 나타내는 정보 $IP_{i,j}$를 미리 산출하고, 상기한 제1 실시 형태와 마찬가지인 알고리즘을 이용하여 키를 산출해도 된다.

[0426] [효과]

[0427] 본 발명의 각 실시 형태에 관한 구성을 적용함으로써, AI05 방식 등에 대표되는 브로드캐스트 엔크립션 방식에 있어서, 키 배신 서버(102)에 의해 선택된 각 부분 집합에 대응하는 세트 키를 도출할 때에, 단말 장치(122)가 키 생성에 필요로 하는 유향 그래프의 정보를 미리 유지해 둘 필요가 없어지므로, 단말 장치(122)의 메모리량에 대한 부담이 저감된다.

[0428] 상기한 제1 실시 형태에서는, 단말 장치(122)가 키 생성에 필요로 하는 유향 패스의 정보로서, 이 유향 패스에 포함되는 모든 유향 가지의 종단부를 나타내는 정보를 부가하여 배신하는 구성으로 하였다. 한편, 상기한 제2 실시 형태에서는, 단말 장치(122)가 키 생성에 필요로 하는 유향 패스의 정보로서, 이 유향 패스에 포함되는 모든 유향 가지의 길이를 나타내는 정보를 부가하여 배신하는 구성으로 하였다. 상기한 제2 실시 형태를 채용하면, 제1 실시 형태에 비해 단말 장치(122)에 배신하는 정보량을 저감시키는 것이 가능해진다.

[0429] [키 제공 시스템(100)의 응용예]

[0430] 마지막으로, 도 22 및 도 23을 참조하면서, 상기한 각 실시 형태에 관한 키 제공 시스템(100)의 응용예에 대해 간단하게 설명한다.

[0431] (응용예 1)

[0432] 우선, 키 제공 시스템(100)의 일 응용예로서, 방송 암호화 시스템(300)의 구성에 대해 설명한다. 도 21은, 방송 위성을 사용한 방송 암호화 시스템(Broadcast Encryption System)(300)의 구성을 도시하는 설명도이다.

[0433] 도 22를 참조하면, 방송 암호화 시스템(300)은, 주로 위성 방송국(302)과, 관리 센터(304)와, 방송 위성(306)과, 주거(308)와, 수신기(310)에 의해 구성된다. 여기서, 방송 암호화 시스템(300)은, 방송 채널을 통해 암호화된 데이터(암호 텍스트 ; Ciphertext)를 주거(308)에 설치된 수신기(310)에 대해 배신하는 시스템이다. 단, 방송 채널이라 함은, 예를 들어 위성 방송 배신 채널이다. 또한, 암호 텍스트라 함은, 예를 들어 암호키, 음성 데이터, 영상 데이터, 또는 텍스트 데이터 등을 포함하는 콘텐츠이다.

[0434] 우선, 위성 방송국(302)에는, 방송 위성(306)을 통해 암호 텍스트 등의 데이터를 송신하는 관리 센터(Broadcast Trusted Center)(304)가 설치된다. 관리 센터(304)는, 예를 들어 암호화용 키를 선택하거나, 데이터의 암호화 및 데이터의 배신 제어를 실행한다. 즉, 관리 센터(304)는 상기한 각 실시 형태에 관한 키 배신 서버(102)의 일례이다. 또한, 주거(308)에 설치된 수신기(310)는 상기한 각 실시 형태에 관한 단말 장치(122)의 일례이다.

[0435] 방송 위성(306)은, 관리 센터(304)와 각 주거(308)에 설치된 수신기(310)와의 사이를 매개하여, 이 수신기(310)에 대해 암호 텍스트 등의 데이터를 방송한다. 또한, 수신기(310)는, 예를 들어 위성 방송 수신기 등이며, 방송 위성(306)을 통해 방송된 데이터를 수신한다. 또한, 도 22에 도시한 바와 같이, 방송 암호화 시스템(30

0)에는 복수의 수신기(310)가 포함되어 있어도 되고, 그 경우, 관리 센터(304)는 복수의 수신기(310)를 포함하는 수신기 그룹에 대해 데이터를 배신한다. 이때, 관리 센터(304)는 인증된 수신기(310)만이 데이터를 복호할 수 있도록 방송 데이터를 암호화하여 배신한다.

[0436] 이상, 키 제공 시스템(100)의 일 응용례인 방송 암호화 시스템(300)에 대해 설명하였다. 도 22에서는, 위성 방송의 예를 들었지만, 방송 암호화 시스템(300)은, 예를 들어 케이블 텔레비전이나 컴퓨터 네트워크 등의 다른 방송 채널을 이용한 암호화 시스템에 대해서도 용이하게 응용하는 것이 가능하다.

[0437] (응용예 2)

[0438] 다음에, 키 제공 시스템(100)의 다른 응용예로서, 방송 암호화 시스템(400)의 구성에 대해 설명한다. 도 23은, 기록 매체를 이용한 방송 암호화 시스템(400)의 구성을 도시하는 설명도이다.

[0439] 도 23을 참조하면, 방송 암호화 시스템(400)은, 주로 매체 제조업자(402)와, 관리 센터(404)와, 기록 매체(406)와, 배포 중개자(408)와, 주거(412)와, 수신기(414)에 의해 구성된다. 여기서, 방송 암호화 시스템(400)에 있어서의 방송 채널은 데이터가 기록된 기록 매체(406)이다.

[0440] 우선, 매체 제조업자(402)에는, 기록 매체(406)를 이용하여 배포 중개자(408)를 통해 암호 텍스트 등의 데이터를 주거(412)에 제공하는 관리 센터(404)가 설치되어 있다. 단, 관리 센터(404)는 기록 매체(406)에 암호 텍스트 등의 데이터를 기록할 뿐이며, 기록 매체(406)를 이용하여 간접적으로 암호 텍스트 등의 데이터를 제공한다. 또한, 기록 매체(406)는, 예를 들어 판독 전용 매체(예를 들어, CD-ROM, DVD-ROM 등), 또는 재기입 가능 매체(예를 들어, CD-RW, DVD-RW 등) 등이다. 상기한 응용예 1과 마찬가지로, 관리 센터(404)는 상기한 각 실시 형태에 관한 키 배신 서버(102)에 상당한다. 단, 암호 텍스트 등의 데이터를 기록 매체에 기록하여 제공하는 점에서 약간 상이하지만, 본 발명에 관한 키 배신 서버는, 이 응용예와 같이, 실시 형태에 따라서 암호 텍스트 등의 정보를 배신하는 수단을 적절하게 변경하는 것이 가능하다.

[0441] 매체 제조업자(402)는, 예를 들어 소매점 등의 배포 중개자(Distribution Outlet)(408)에 대해 암호 텍스트 등의 데이터가 기록된 기록 매체(406)를 송부한다. 계속해서, 배포 중개자(408)는 매체(406)를 각 주거(412)에 대해 제공한다. 예를 들어, 배포 중개자(408)는 기록 매체(406)를 각 주거(412)에 대응하는 개인에 대해 판매한다. 이 개인은, 기록 매체(406)를 주거(412)로 갖고 돌아가고, 수신기(414)를 이용하여 기록 매체(406)에 기록된 데이터를 재생한다. 이 수신기(414)는, 상기한 각 실시 형태에 관한 단말 장치(122)의 일례이지만, 암호 텍스트 등의 데이터를 기록 매체를 통해 취득하는 점에서 약간 상이하다. 그러나, 본 발명에 관한 단말 장치는, 이 응용예와 같이, 실시 형태에 따라서 암호 텍스트 등의 정보를 취득하는 수단을 적절하게 변경하는 것이 가능하다. 또한, 수신기(414)는, 예를 들어 CD 플레이어, DVD 플레이어, 또는 DVD-RW 드라이브를 구비한 컴퓨터 등이며, 기록 매체(406)에 기록되어 있는 데이터를 판독하여 재생하는 것이 가능한 장치에 의해 구성될 수 있다.

[0442] 이상, 키 제공 시스템(100)의 일단 용례인 방송 암호화 시스템(400)에 대해 설명하였다. 도 23에서는, 기록 매체(406)를 통해 암호 텍스트 등의 데이터를 계약자에 제공하는 수단을 예로 들어 설명하였다. 이와 같이, 본 발명에 관한 키 배신 서버 및 단말 장치는, 실시 형태에 따라서 각종 정보의 배포 수단에 관한 구성을 변경하는 것이 가능하다.

[0443] 이상, 첨부 도면을 참조하면서 본 발명의 적합한 실시 형태에 대해 설명하였지만, 본 발명은 이러한 예에 한정되지 않는 것은 물론이다. 당업자라면 청구범위에 기재된 범주 내에 있어서, 각종 변경예 또는 수정예에 상도할 수 있는 것은 명백하고, 그들에 대해서도 당연히 본 발명의 기술적 범위에 속하는 것으로 이해된다.

[0444] 예를 들어, 상기한 논리 이분목은, 위로부터 아래로 가지가 퍼지는 구조를 갖는 것으로 가정하였지만, 반드시 이에 한정되는 것은 아니고, 아래로부터 위, 좌측으로부터 우측, 또는 우측으로부터 좌측을 향해 가지가 퍼지도록 구성하는 것도 가능하다. 이와 같은 배치에 관한 변경은, 단순히 논리 이분목을 회전하여 배치함으로써 실현되므로, 이러한 변경에 따른 어느 구성에 대해서도 실질적으로 동일한 기술적 범위에 속하는 것이라 할 수 있다. 또한, 임시 유향 그래프 및 유향 그래프를 형성하는 수평 좌표축을 좌우 반전시키는 변경에 대해서도 마찬가지이다.

[0445] 그런데, 상기한 각 실시 형태에 관한 키 배신 서버(102)는, 스스로 유향 그래프를 생성하는 구성 요소를 포함하고 있지만, 반드시 이에 한정되지는 않는다. 예를 들어, 본 발명에 관한 키 배신 서버(102)는, 소정의 유향 그래프에 관한 정보를 취득하는 취득부를 구비하고 있어도 되고, 이 경우, 나무 구조 설정부(104), 좌표축 설정부(106), 임시 유향 그래프 생성부(108), 및 유향 그래프 생성부(110)의 일부 또는 전부를 구비하고 있을 필요는

없다.

[0446] 또한, 상기한 각 실시 형태에 관한 키 배신 서버(102)는, 콘텐츠, 콘텐츠 키, 세트 키, 중간 키, 허락 계약자에 대응하는 부분 집합의 정보, 또는 유향 그래프의 정보 등을 단말 장치(122)에 배신하는 통신부(118)를 구비하고 있지만, 상기한 응용예 2에도 도시한 바와 같이, 이들 정보를 제공하기 위해 항상 네트워크를 이용하는 것에는 한정되지 않는다. 예를 들어, 키 배신 서버(102)는, 통신부(118) 대신에, 기록 매체에 정보를 기록하기 위한 기록부를 구비하고 있어도 된다. 그 경우, 단말 장치(122)는 통신부(124)를 구비하는 대신에, 정보가 기록된 기록 매체를 읽어들이기 위한 판독부를 구비하고 있어도 된다.

도면의 간단한 설명

[0039] 도 1은 본 발명의 제1 및 제2 실시 형태에 관한 키 제공 시스템(100)의 구성을 도시하는 설명도.

[0040] 도 2는 제1 및 제2 실시 형태에 관한 키 배신 서버(102) 및 단말 장치(122)의 하드웨어 구성을 도시하는 설명도.

[0041] 도 3은 제1 및 제2 실시 형태에 관한 논리 이분목의 구조를 도시하는 설명도.

[0042] 도 4는 AI05 방식의 유향 그래프 H를 나타내는 설명도.

[0043] 도 5는 AI05 방식에 관한 키 배신 처리의 흐름을 나타내는 설명도.

[0044] 도 6은 AI05 방식에 관한 키 배신 처리의 흐름을 나타내는 설명도.

[0045] 도 7은 제1 및 제2 실시 형태에 관한 암호문의 복호 처리의 흐름을 나타내는 설명도.

[0046] 도 8은 제1 및 제2 실시 형태에 관한 키 배신 서버(102)의 기능 구성을 도시하는 설명도.

[0047] 도 9는 A06(A+B) 방식에 관한 임시 유향 그래프 I'를 생성하는 처리의 흐름을 나타내는 설명도.

[0048] 도 10은 A06(A+B) 방식의 임시 유향 그래프 I'를 나타내는 설명도.

[0049] 도 11은 A06(A+B) 방식에 관한 유향 그래프 I를 생성하는 처리의 흐름을 나타내는 설명도.

[0050] 도 12는 A06(A+B) 방식에 관한 유향 그래프 I를 생성하는 처리의 흐름을 나타내는 설명도.

[0051] 도 13은 A06(A+B) 방식에 관한 유향 그래프 I를 생성하는 처리의 흐름을 나타내는 설명도.

[0052] 도 14는 A06(A+B) 방식에 관한 유향 그래프 I를 생성하는 처리의 흐름을 나타내는 설명도.

[0053] 도 15는 A06(A+B) 방식의 유향 그래프 I를 나타내는 설명도.

[0054] 도 16은 AI05 방식의 유향 그래프 H에 제1 및 제2 실시 형태를 적용할 때에 참조되는 유향 패스의 일례를 나타내는 설명도.

[0055] 도 17은 AI05 방식의 유향 그래프 H에 제1 및 제2 실시 형태를 적용할 때에 참조되는 유향 패스의 일례를 나타내는 설명도.

[0056] 도 18은 A06(A+B) 방식의 유향 그래프 I에 제1 및 제2 실시 형태를 적용할 때에 참조되는 유향 패스의 일례를 나타내는 설명도.

[0057] 도 19는 제1 및 제2 실시 형태에 관한 단말 장치(122)의 기능 구성을 도시하는 설명도.

[0058] 도 20은 본 발명의 제1 실시 형태에 관한 키 생성 처리의 흐름을 나타내는 설명도.

[0059] 도 21은 본 발명의 제2 실시 형태에 관한 키 생성 처리의 흐름을 나타내는 설명도.

[0060] 도 22는 본 발명의 제1 및 제2 실시 형태의 응용예인 방송 암호화 시스템(300)의 구성을 도시하는 설명도.

[0061] 도 23은 본 발명의 제1 및 제2 실시 형태의 응용예인 방송 암호화 시스템(400)의 구성을 도시하는 설명도.

[0062] <부호의 설명>

[0063] 100 : 키 제공 시스템

[0064] 102 : 키 배신 서버

[0065] 104 : 나무 구조 설정부

[0066] 106 : 좌표축 설정부

[0067] 108 : 임시 유향 그래프 생성부

[0068] 110 : 유향 그래프 생성부

[0069] 112 : 초기 중간 키 설정부

[0070] 114 : 키 생성부

[0071] 116 : 암호화부

[0072] 118 : 통신부

[0073] 120 : 부분 집합 결정부

[0074] 121 : 경로 정보 생성부

[0075] 122 : 단말 장치

[0076] 124 : 통신부

[0077] 126 : 판단부

[0078] 128 : 키 생성부

[0079] 130 : 복호부

[0080] 202 : 컨트롤러

[0081] 204 : 연산 유닛

[0082] 206 : 입출력 인터페이스

[0083] 208 : 시큐어 기억부

[0084] 210 : 메인 기억부

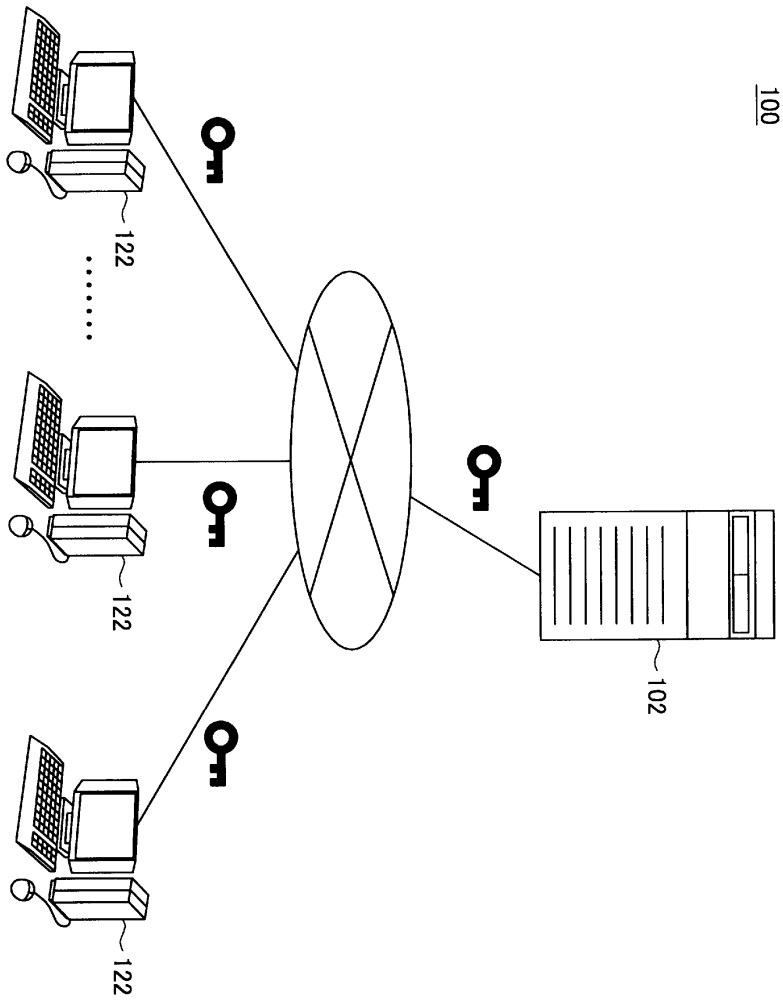
[0085] 212 : 네트워크 인터페이스

[0086] 216 : 미디어 인터페이스

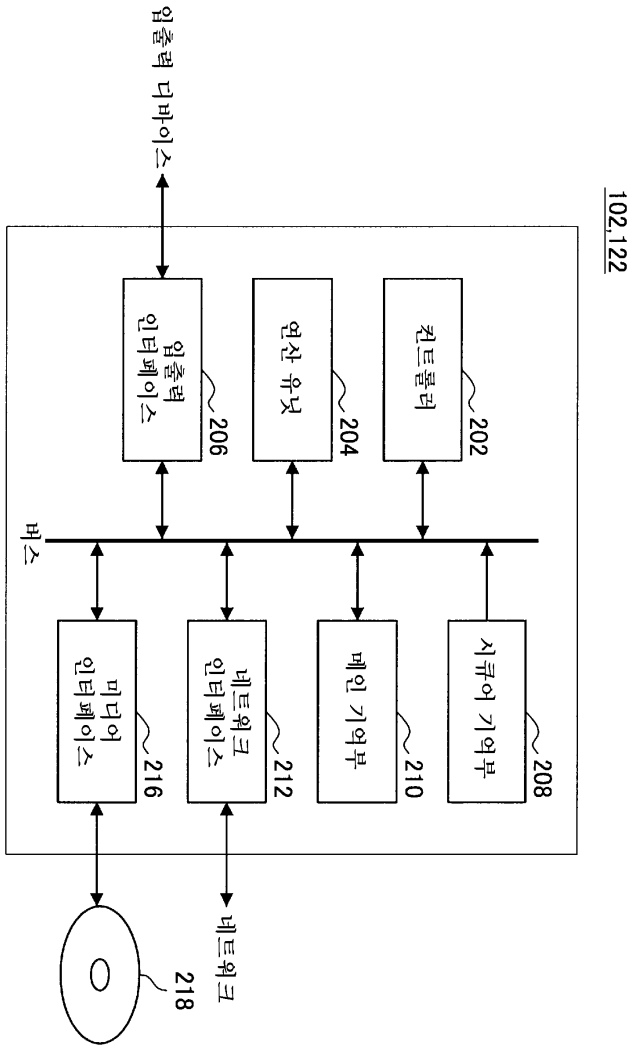
[0087] 218 : 정보 미디어

도면

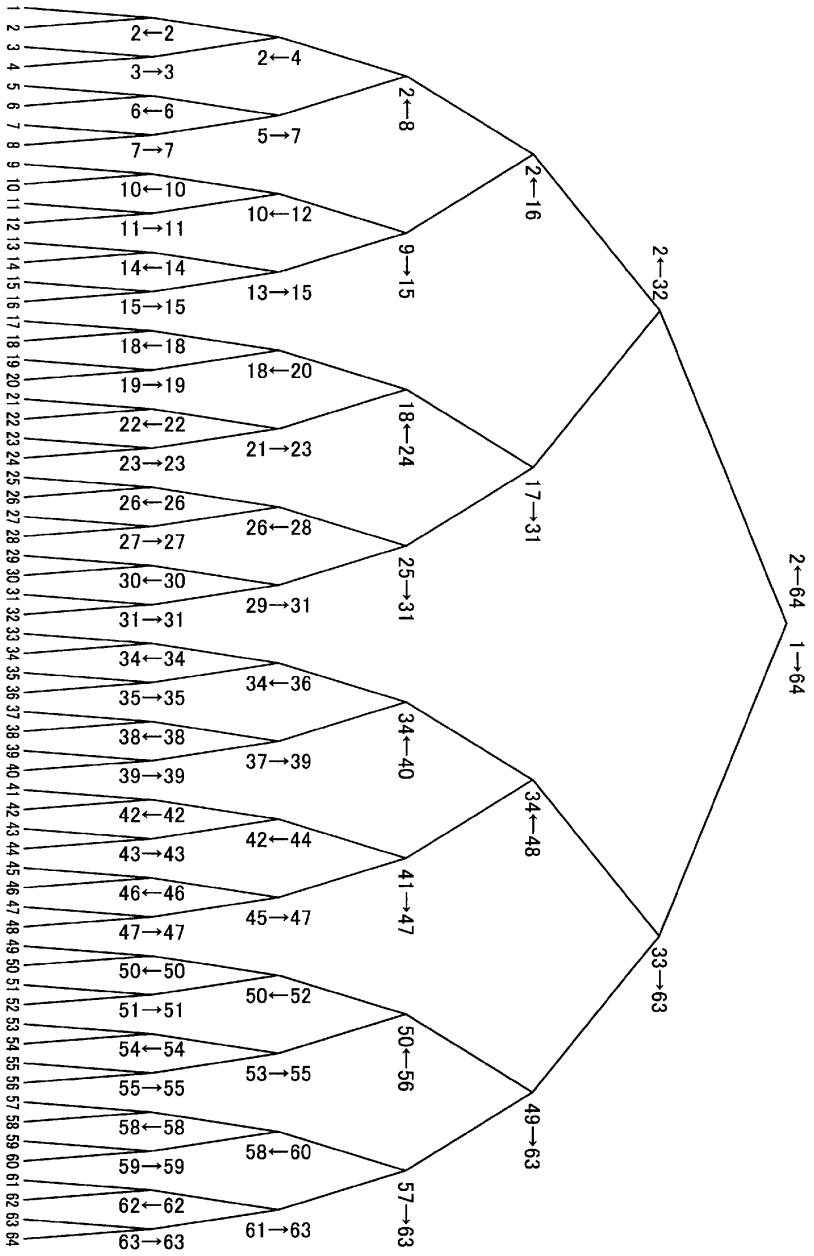
도면1



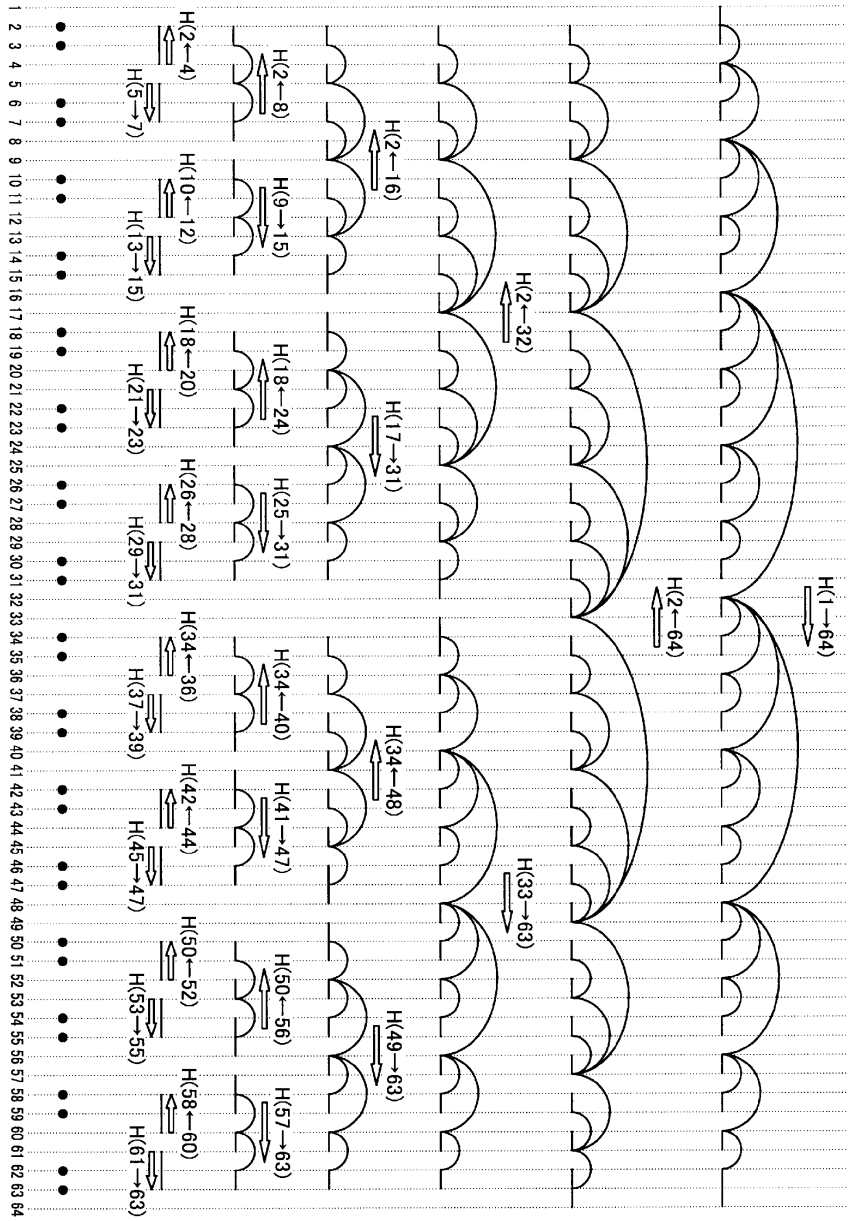
도면2


102,122
입출력 디바이스
입출력 인터페이스
206
연산 유닛
204
컨트롤러
202
버스
미디어 인터페이스
216
네트워크 인터페이스
212
메인 기억부
210
시큐어 기억부
208
218
네트워크

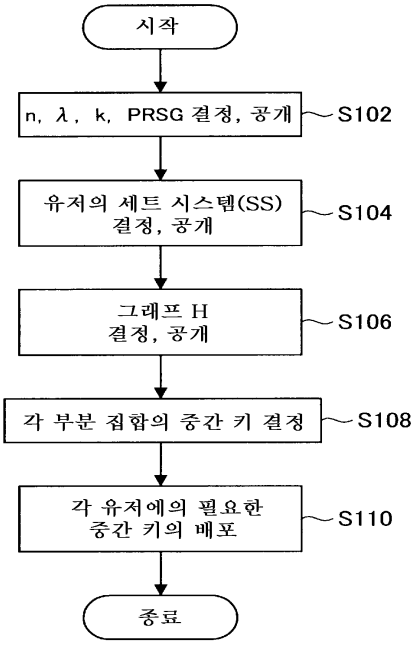
도면3


1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64
2←2
3→3
2←4
6←6
7→7
5→7
2←8
10←10
11→11
10←12
14←14
15→15
13→15
9→15
2←16
18←18
19→19
18←20
22←22
23→23
21→23
18←24
26←26
27→27
26←28
30←30
31→31
29→31
25→31
17→31
2←32
34←34
35→35
34←36
38←38
39→39
37→39
34←40
42←42
43→43
42←44
46←46
47→47
45→47
41→47
34←48
50←50
51→51
50←52
54←54
55→55
53→55
50←56
58←58
59→59
58←60
62←62
63→63
61→63
57→63
49→63
33→63
2←64
1→64

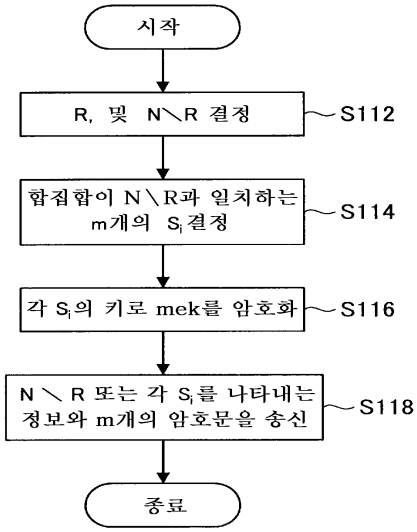
도면4


H(1→64)
H(2←64)
H(2←32)
H(33→63)
H(2←16)
H(17→31)
H(34←48)
H(49→63)
H(2←8)
H(9→15)
H(18←24)
H(25→31)
H(34←40)
H(41→47)
H(50←56)
H(57→63)
H(2←4)
H(5→7)
H(10←12)
H(13→15)
H(18←20)
H(21→23)
H(26←28)
H(29→31)
H(34←36)
H(37→39)
H(42←44)
H(45→47)
H(50←52)
H(53→55)
H(58←60)
H(61→63)
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64

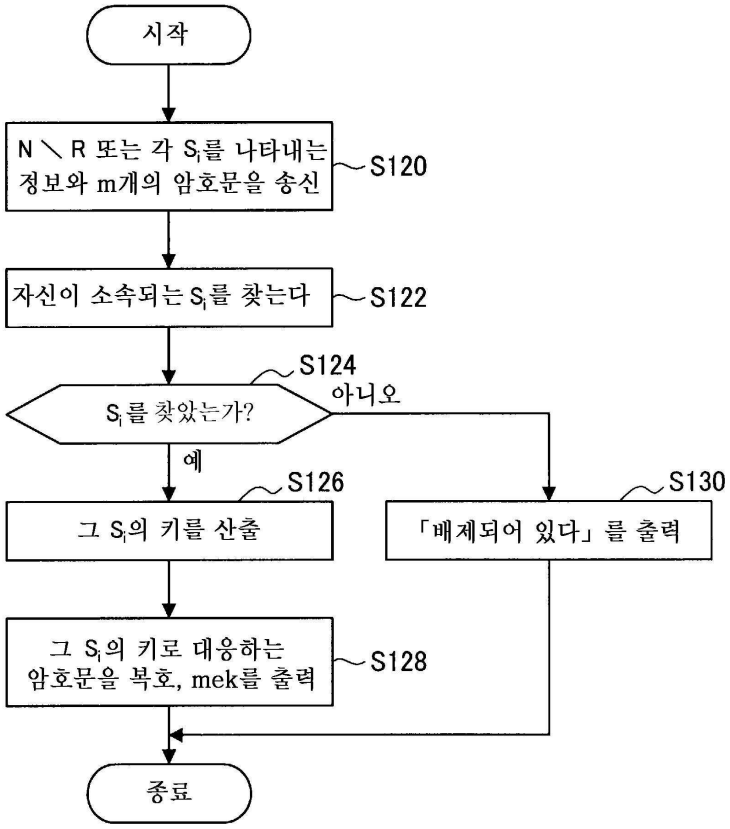
도면5


시작
n, λ, k, PRSG 결정, 공개
S102
유저의 세트 시스템(SS) 결정, 공개
S104
그래프 H 결정, 공개
S106
각 부분 집합의 중간 키 결정
S108
각 유저에의 필요한 중간 키의 배포
S110
종료

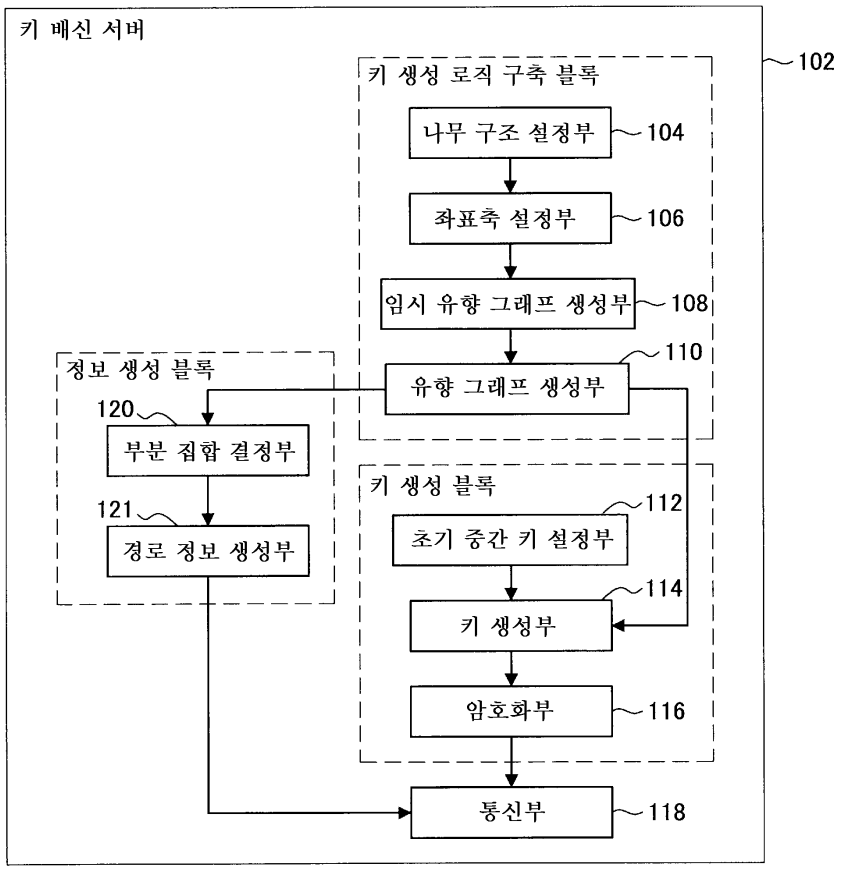
도면6


시작
R, 및 N＼R 결정
S112
합집합이 N＼R과 일치하는 m개의 S_i 결정
S114
각 S_i의 키로 mek를 암호화
S116
N ＼ R 또는 각 S_i를 나타내는 정보와 m개의 암호문을 송신
S118
종료

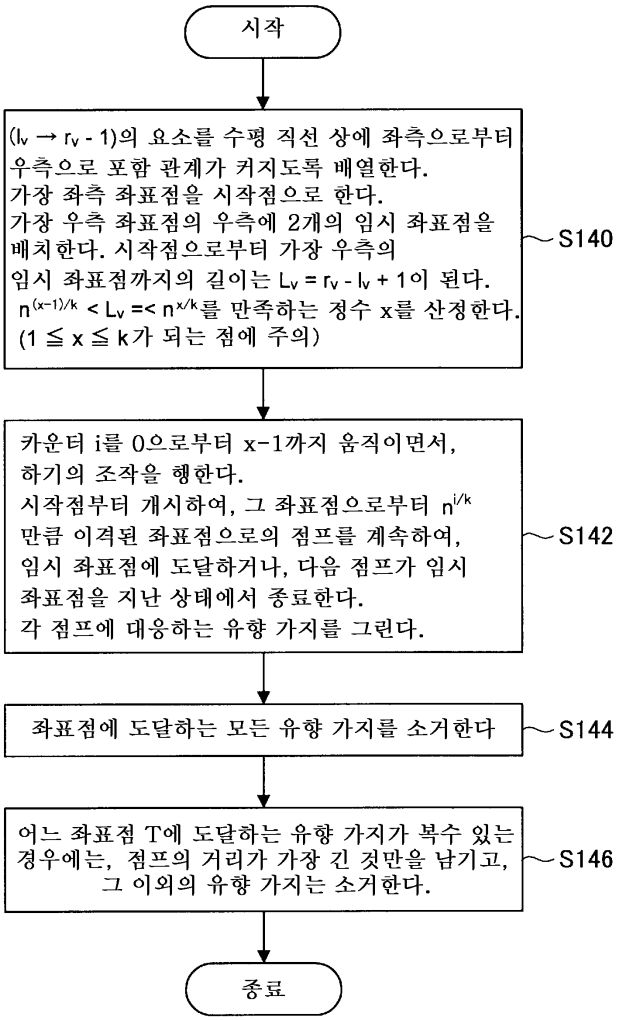
도면7


시작
N ＼ R 또는 각 S_i를 나타내는 정보와 m개의 암호문을 송신
S120
자신이 소속되는 S_i를 찾는다
S122
S124
S_i를 찾았는가?
아니오
예
S126
그 S_i의 키를 산출
S130
「배제되어 있다」를 출력
그 S_i의 키로 대응하는 암호문을 복호, mek를 출력
S128
종료

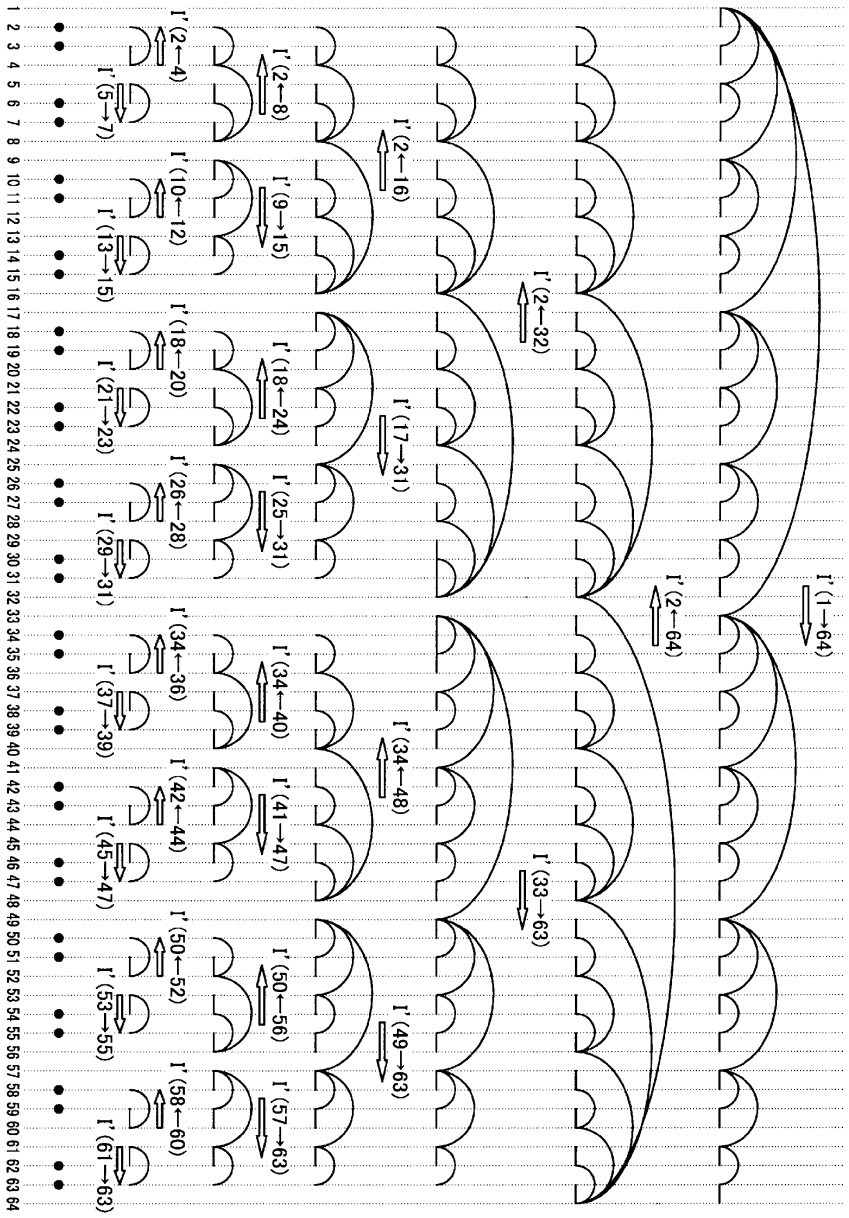
도면8


키 배신 서버
102
키 생성 로직 구축 블록
나무 구조 설정부
104
좌표축 설정부
106
임시 유향 그래프 생성부
108
110
유향 그래프 생성부
정보 생성 블록
120
부분 집합 결정부
121
경로 정보 생성부
키 생성 블록
112
초기 중간 키 설정부
114
키 생성부
암호화부
116
통신부
118

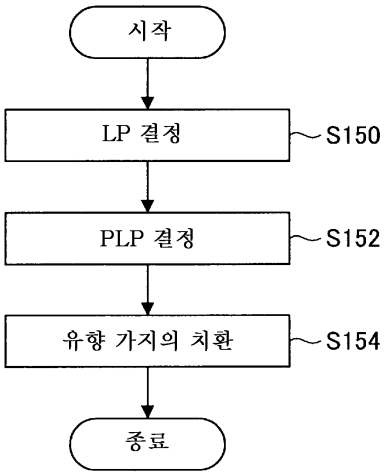
도면9


시작
(lv → rv - 1)의 요소를 수평 직선 상에 좌측으로부터 우측으로 포함 관계가 커지도록 배열한다.
가장 좌측 좌표점을 시작점으로 한다.
가장 우측 좌표점의 우측에 2개의 임시 좌표점을 배치한다. 시작점으로부터 가장 우측의 임시 좌표점까지의 길이는 Lv = rv - lv + 1이 된다.
n^(x-1)/k < Lv =< n^x/k를 만족하는 정수 x를 산정한다. (1 ≦ x ≦ k가 되는 점에 주의)
S140
카운터 i를 0으로부터 x-1까지 움직이면서, 하기의 조작을 행한다.
시작점부터 개시하여, 그 좌표점으로부터 n^i/k 만큼 이격된 좌표점으로의 점프를 계속하여, 임시 좌표점에 도달하거나, 다음 점프가 임시 좌표점을 지난 상태에서 종료한다.
각 점프에 대응하는 유향 가지를 그린다.
S142
좌표점에 도달하는 모든 유향 가지를 소거한다
S144
어느 좌표점 T에 도달하는 유향 가지가 복수 있는 경우에는, 점프의 거리가 가장 긴 것만을 남기고, 그 이외의 유향 가지는 소거한다.
S146
종료

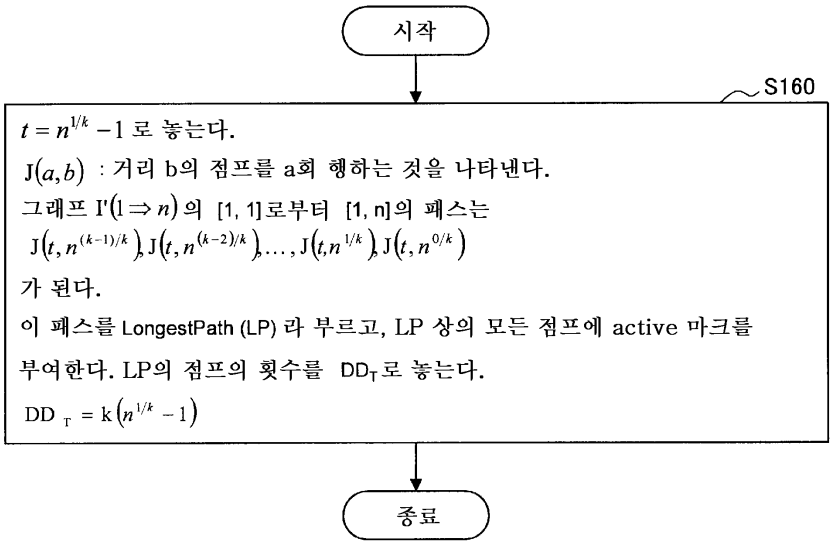
도면10


I'(1→64)
I'(2←64)
I'(2←32)
I'(33→63)
I'(2←16)
I'(17→31)
I'(34←48)
I'(49→63)
I'(2←8)
I'(9→15)
I'(18←24)
I'(25→31)
I'(34←40)
I'(41→47)
I'(50←56)
I'(57→63)
I'(2←4)
I'(5→7)
I'(10←12)
I'(13→15)
I'(18←20)
I'(21→23)
I'(26←28)
I'(29→31)
I'(34←36)
I'(37→39)
I'(42←44)
I'(45→47)
I'(50←52)
I'(53→55)
I'(58←60)
I'(61→63)
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64

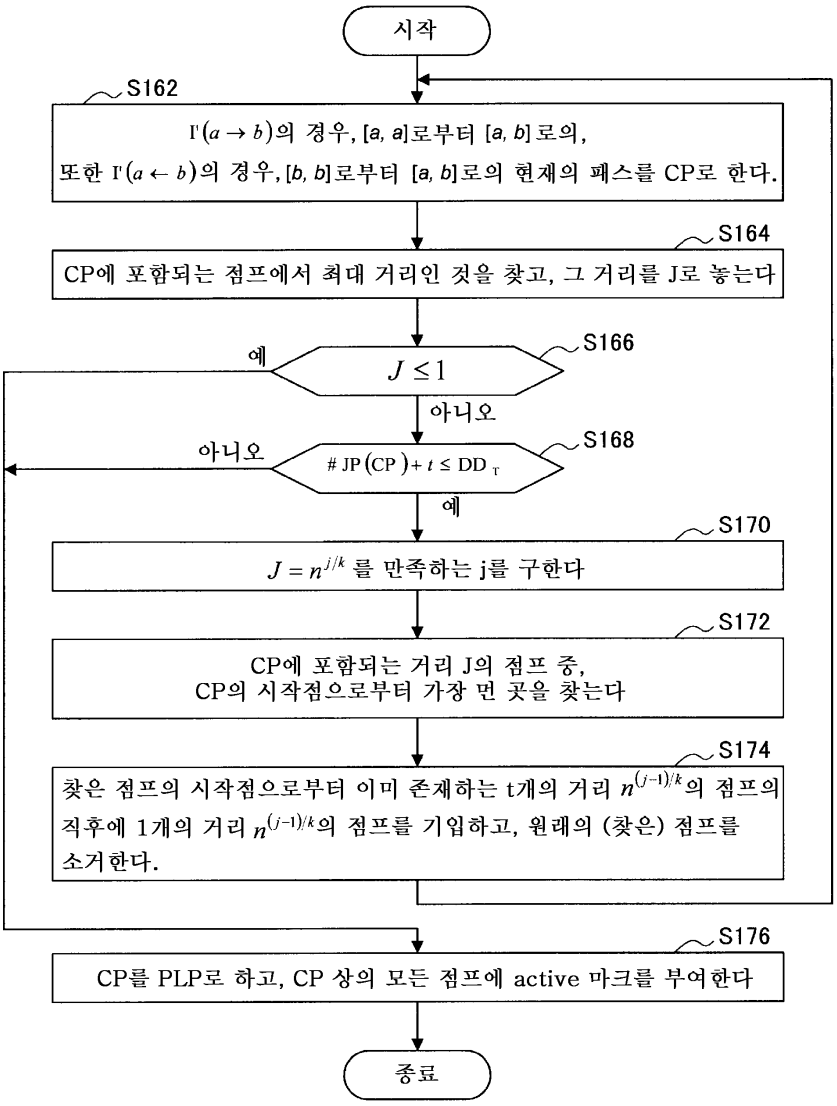
도면11


시작
LP 결정
S150
PLP 결정
S152
유향 가지의 치환
S154
종료

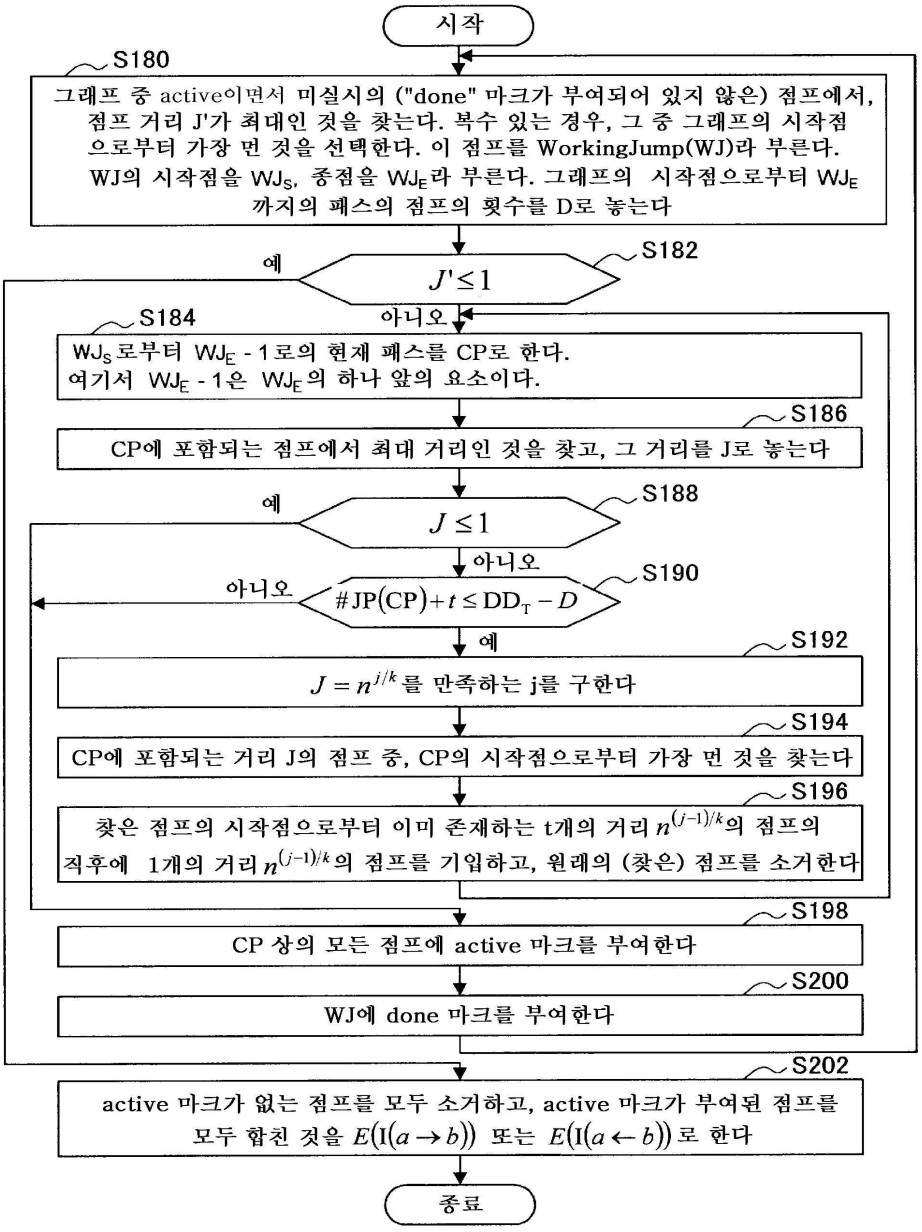
도면12


시작
S160
$t = n^{1/k} - 1$ 로 놓는다.
$J(a,b)$: 거리 b의 점프를 a회 행하는 것을 나타낸다.
그래프 $I'(1 \Rightarrow n)$의 [1, 1]로부터 [1, n]의 패스는
$J(t, n^{(k-1)/k}), J(t, n^{(k-2)/k}), \ldots, J(t, n^{1/k}), J(t, n^{0/k})$
가 된다.
이 패스를 LongestPath (LP) 라 부르고, LP 상의 모든 점프에 active 마크를
부여한다. LP의 점프의 횟수를 DD_T로 놓는다.
$DD_T = k(n^{1/k} - 1)$
종료

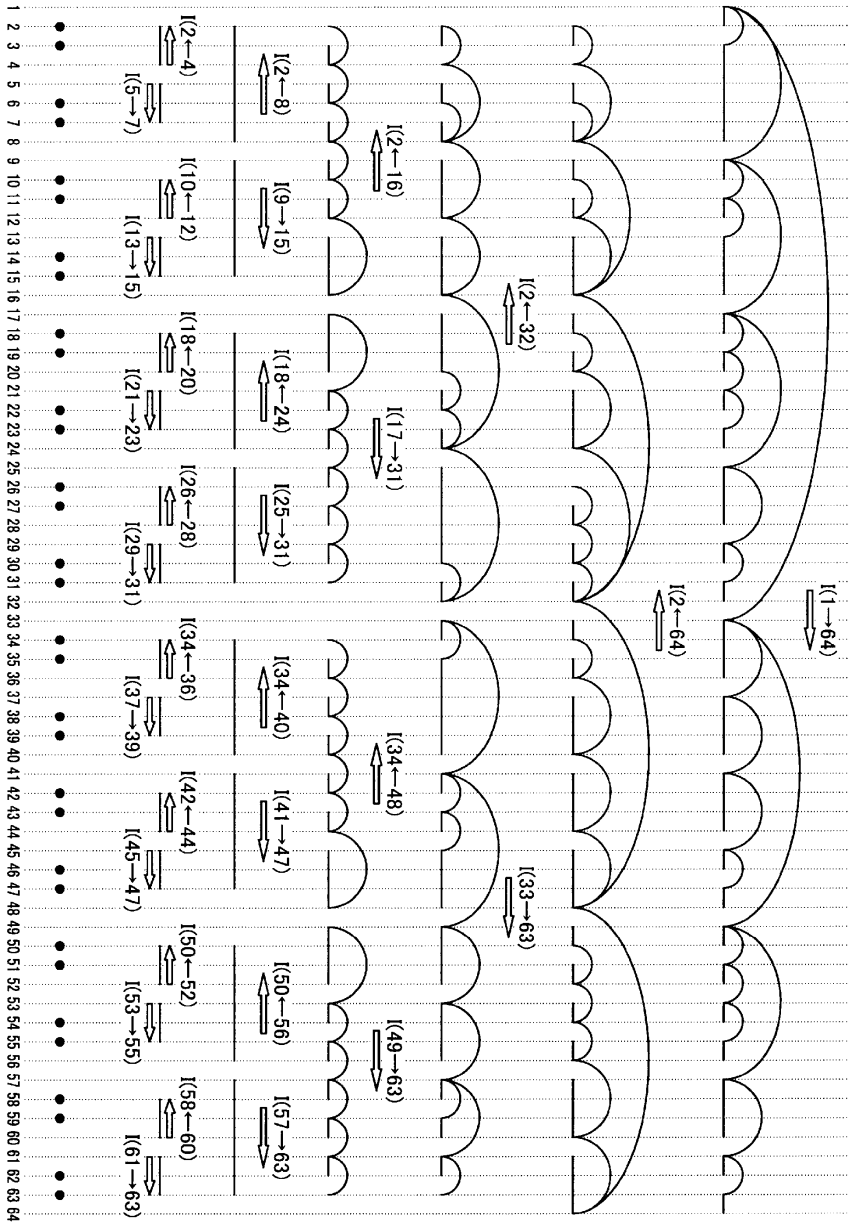
도면13


시작
S162
$\Gamma'(a \to b)$의 경우, [a, a]로부터 [a, b]로의,
또한 $\Gamma'(a \leftarrow b)$의 경우, [b, b]로부터 [a, b]로의 현재의 패스를 CP로 한다.
S164
CP에 포함되는 점프에서 최대 거리인 것을 찾고, 그 거리를 J로 놓는다
S166
$J \leq 1$
예
아니오
S168
$\#\,\mathrm{JP}(\mathrm{CP}) + t \leq \mathrm{DD}_T$
아니오
예
S170
$J = n^{j/k}$ 를 만족하는 j를 구한다
S172
CP에 포함되는 거리 J의 점프 중,
CP의 시작점으로부터 가장 먼 곳을 찾는다
S174
찾은 점프의 시작점으로부터 이미 존재하는 t개의 거리 $n^{(j-1)/k}$의 점프의 직후에 1개의 거리 $n^{(j-1)/k}$의 점프를 기입하고, 원래의 (찾은) 점프를 소거한다.
S176
CP를 PLP로 하고, CP 상의 모든 점프에 active 마크를 부여한다
종료

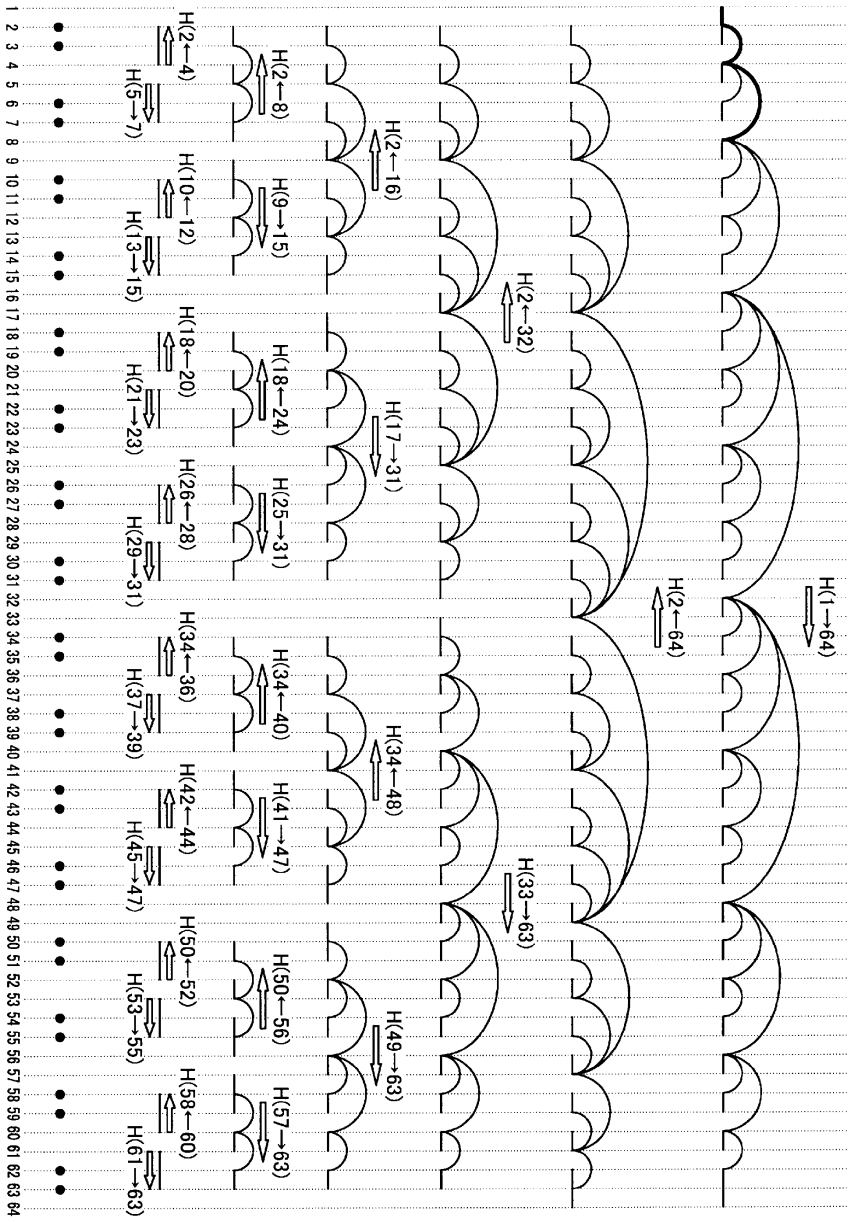
도면14


시작
S180
그래프 중 active이면서 미실시의 ("done" 마크가 부여되어 있지 않은) 점프에서, 점프 거리 J'가 최대인 것을 찾는다. 복수 있는 경우, 그 중 그래프의 시작점으로부터 가장 먼 것을 선택한다. 이 점프를 WorkingJump(WJ)라 부른다. WJ의 시작점을 WJ_S, 종점을 WJ_E라 부른다. 그래프의 시작점으로부터 WJ_E까지의 패스의 점프의 횟수를 D로 놓는다
S182
예
$J' \leq 1$
아니오
S184
WJ_S로부터 WJ_E - 1로의 현재 패스를 CP로 한다. 여기서 WJ_E - 1은 WJ_E의 하나 앞의 요소이다.
S186
CP에 포함되는 점프에서 최대 거리인 것을 찾고, 그 거리를 J로 놓는다
S188
예
$J \leq 1$
아니오
S190
아니오
$\#JP(CP)+t \leq DD_T - D$
예
S192
$J = n^{j/k}$를 만족하는 j를 구한다
S194
CP에 포함되는 거리 J의 점프 중, CP의 시작점으로부터 가장 먼 것을 찾는다
S196
찾은 점프의 시작점으로부터 이미 존재하는 t개의 거리 $n^{(j-1)/k}$의 점프의 직후에 1개의 거리 $n^{(j-1)/k}$의 점프를 기입하고, 원래의 (찾은) 점프를 소거한다
S198
CP 상의 모든 점프에 active 마크를 부여한다
S200
WJ에 done 마크를 부여한다
S202
active 마크가 없는 점프를 모두 소거하고, active 마크가 부여된 점프를 모두 합친 것을 $E(I(a \rightarrow b))$ 또는 $E(I(a \leftarrow b))$로 한다
종료

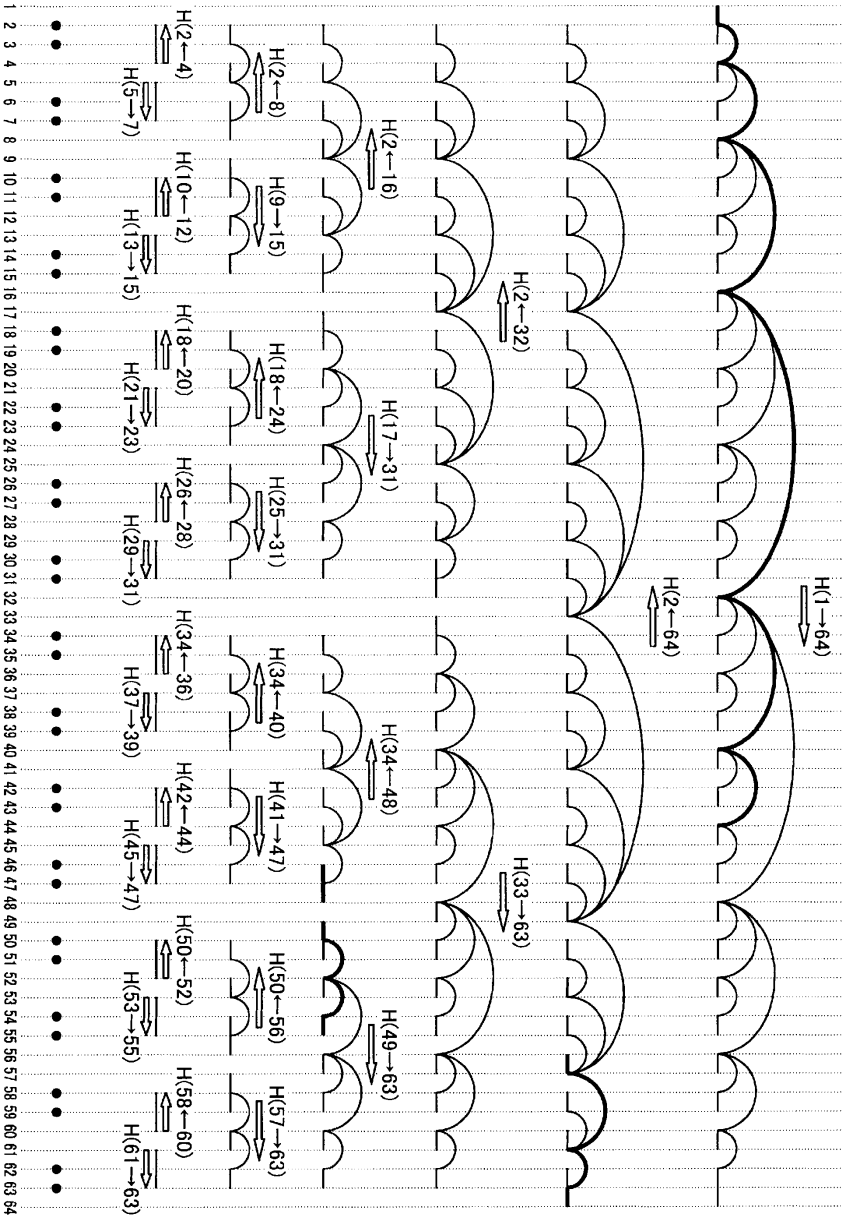
도면15


I(1→64)
I(2←64)
I(2←32)
I(33→63)
I(2←16)
I(17→31)
I(34←48)
I(49→63)
I(2←8)
I(9→15)
I(18←24)
I(25→31)
I(34←40)
I(41→47)
I(50←56)
I(57→63)
I(2←4)
I(5→7)
I(10←12)
I(13→15)
I(18←20)
I(21→23)
I(26←28)
I(29→31)
I(34←36)
I(37→39)
I(42←44)
I(45→47)
I(50←52)
I(53→55)
I(58←60)
I(61→63)
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64

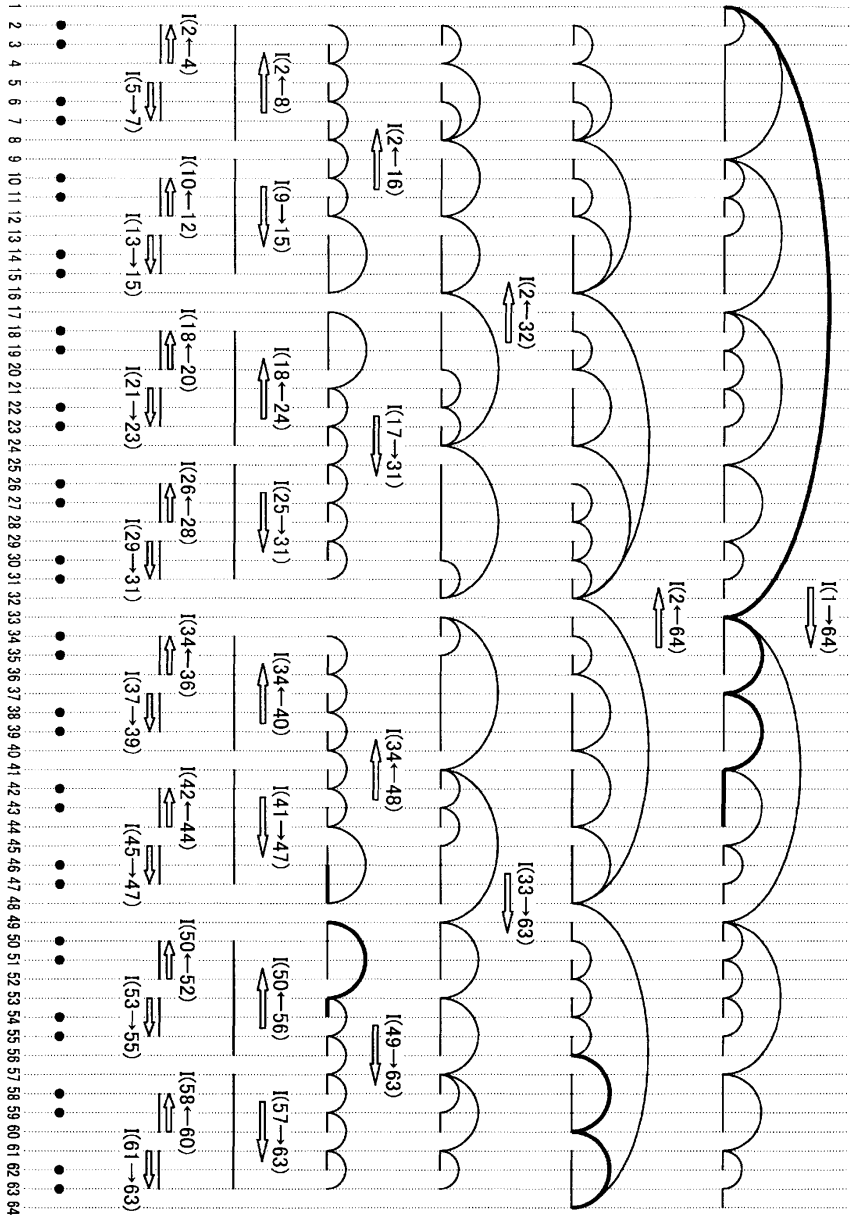
도면16


H(1→64)
H(2←64)
H(2←32)
H(33→63)
H(2←16)
H(17→31)
H(34←48)
H(49→63)
H(2←8)
H(9→15)
H(18←24)
H(25→31)
H(34←40)
H(41→47)
H(50←56)
H(57→63)
H(2←4)
H(5→7)
H(10←12)
H(13→15)
H(18←20)
H(21→23)
H(26←28)
H(29→31)
H(34←36)
H(37→39)
H(42←44)
H(45→47)
H(50←52)
H(53→55)
H(58←60)
H(61→63)
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64

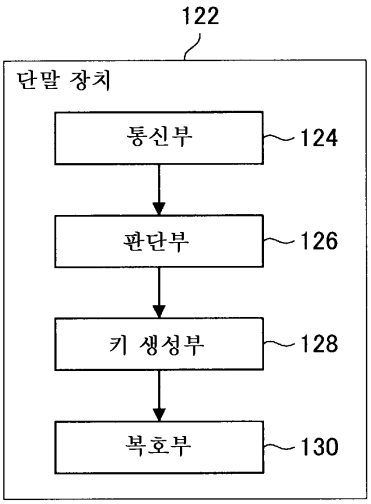
도면17


H(1→64)
H(2←64)
H(2←32)
H(33→63)
H(2←16)
H(17→31)
H(34←48)
H(49→63)
H(2←8)
H(9→15)
H(18←24)
H(25→31)
H(34←40)
H(41→47)
H(50←56)
H(57→63)
H(2←4)
H(5→7)
H(10←12)
H(13→15)
H(18←20)
H(21→23)
H(26←28)
H(29→31)
H(34←36)
H(37→39)
H(42←44)
H(45→47)
H(50←52)
H(53→55)
H(58←60)
H(61→63)
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64

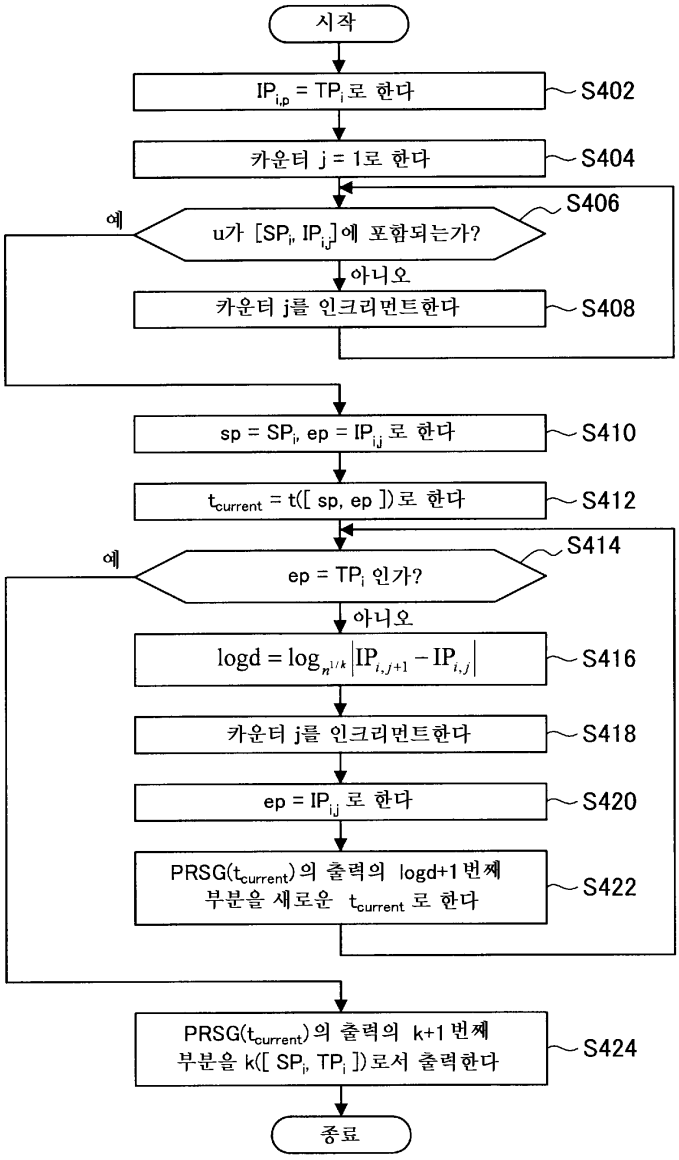
도면18


I(1→64)
I(2←64)
I(2←32)
I(33→63)
I(2←16)
I(17→31)
I(34←48)
I(49→63)
I(2←8)
I(9→15)
I(18←24)
I(25→31)
I(34←40)
I(41→47)
I(50←56)
I(57→63)
I(2←4)
I(5→7)
I(10←12)
I(13→15)
I(18←20)
I(21→23)
I(26←28)
I(29→31)
I(34←36)
I(37→39)
I(42←44)
I(45→47)
I(50←52)
I(53→55)
I(58←60)
I(61→63)
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64

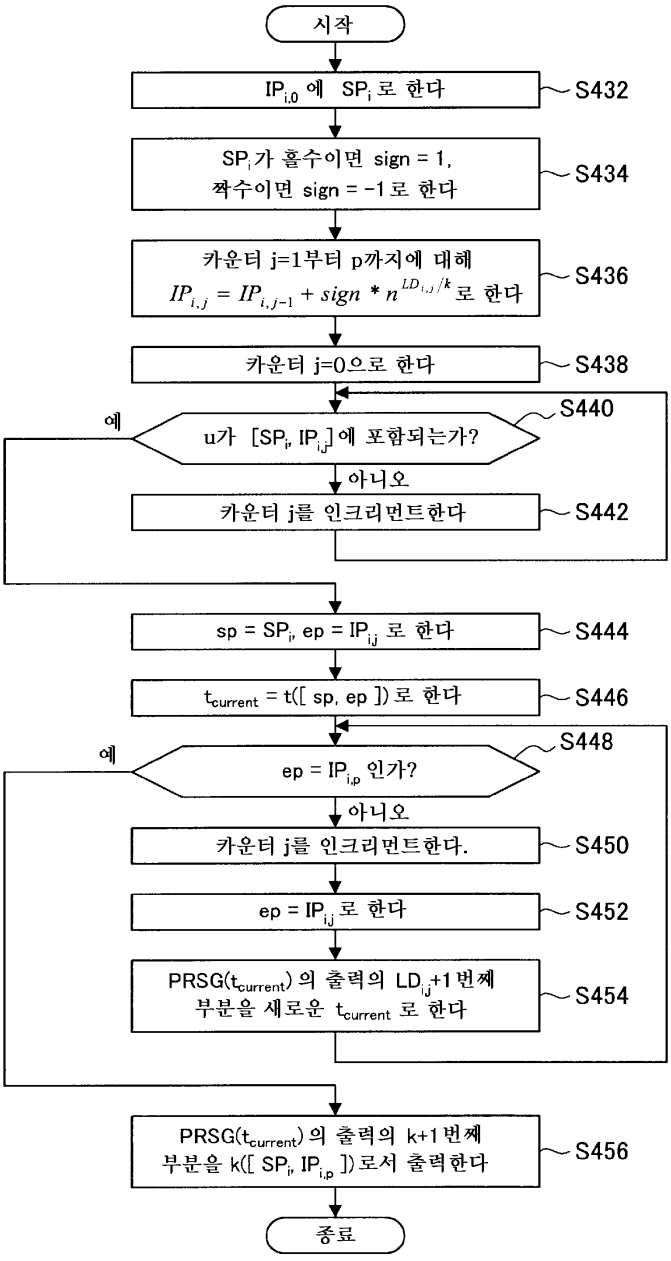
도면19



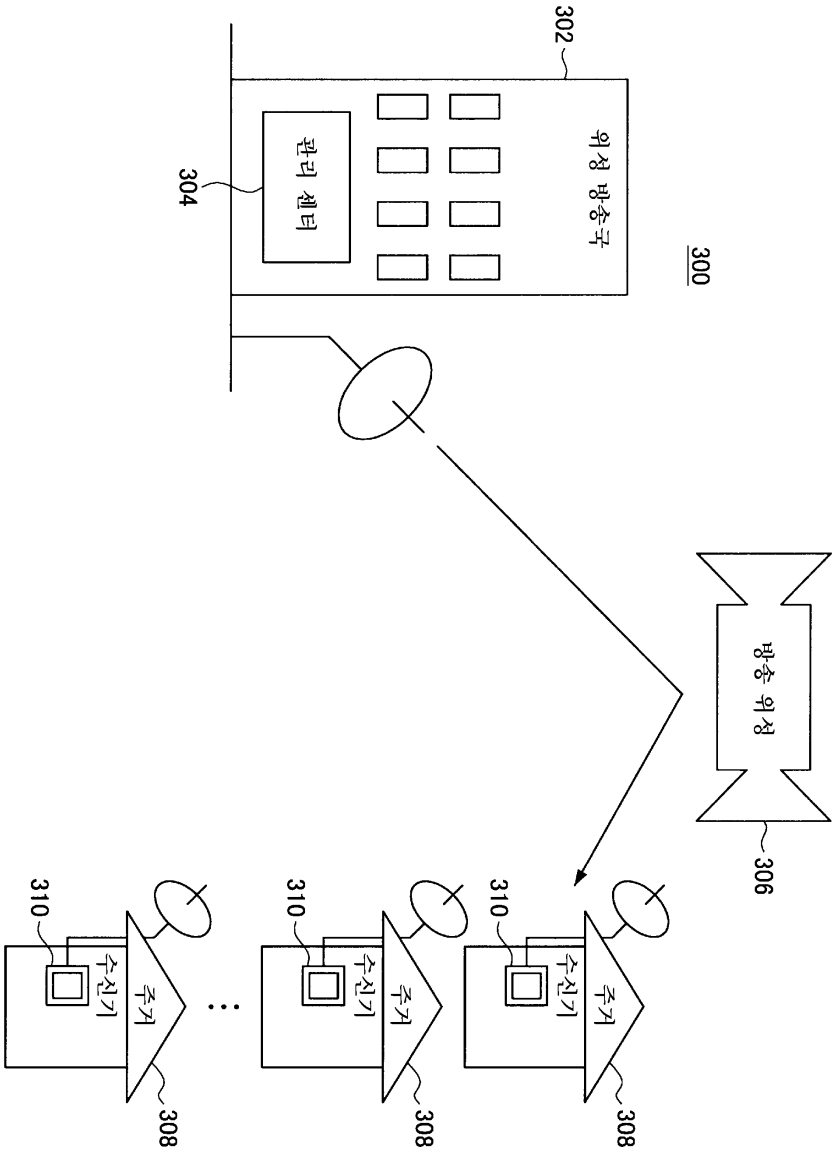
도면20


시작
$IP_{i,p} = TP_i$ 로 한다
S402
카운터 j = 1로 한다
S404
S406
예
u가 $[SP_i, IP_{i,j}]$에 포함되는가?
아니오
카운터 j를 인크리먼트한다
S408
sp = SP_i, ep = $IP_{i,j}$ 로 한다
S410
$t_{current}$ = t([sp, ep]) 로 한다
S412
S414
예
ep = TP_i 인가?
아니오
$logd = \log_{n^{1/k}} |IP_{i,j+1} - IP_{i,j}|$
S416
카운터 j를 인크리먼트한다
S418
ep = $IP_{i,j}$ 로 한다
S420
PRSG($t_{current}$)의 출력의 logd+1 번째 부분을 새로운 $t_{current}$ 로 한다
S422
PRSG($t_{current}$)의 출력의 k+1 번째 부분을 k([SP_i, TP_i])로서 출력한다
S424
종료

도면21


시작
$IP_{i,0}$ 에 SP_i 로 한다
S432
SP_i가 홀수이면 sign = 1,
짝수이면 sign = -1 로 한다
S434
카운터 j=1부터 p까지에 대해
$IP_{i,j} = IP_{i,j-1} + sign * n^{LD_{i,j}/k}$ 로 한다
S436
카운터 j=0으로 한다
S438
S440
u가 $[SP_i, IP_{i,j}]$에 포함되는가?
예
아니오
카운터 j를 인크리먼트한다
S442
sp = SP_i, ep = $IP_{i,j}$ 로 한다
S444
$t_{current}$ = t([sp, ep]) 로 한다
S446
S448
ep = $IP_{i,p}$ 인가?
예
아니오
카운터 j를 인크리먼트한다.
S450
ep = $IP_{i,j}$ 로 한다
S452
PRSG($t_{current}$) 의 출력의 $LD_{i,j}$+1번째
부분을 새로운 $t_{current}$ 로 한다
S454
PRSG($t_{current}$) 의 출력의 k+1번째
부분을 k([SP_i, $IP_{i,p}$])로서 출력한다
S456
종료

도면22



도면23