(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2013년09월24일
(11) 등록번호 10-1310439
(24) 등록일자 2013년09월12일

(51) 국제특허분류(Int. Cl.)
G09C 1/00 (2006.01) *H04L 9/08* (2006.01)
(21) 출원번호 10-2012-7019705
(22) 출원일자(국제) 2010년12월20일
심사청구일자 2012년07월25일
(85) 번역문제출일자 2012년07월25일
(65) 공개번호 10-2012-0112654
(43) 공개일자 2012년10월11일
(86) 국제출원번호 PCT/JP2010/072912
(87) 국제공개번호 WO 2011/083678
국제공개일자 2011년07월14일
(30) 우선권주장
JP-P-2010-002709 2010년01월08일 일본(JP)
(56) 선행기술조사문헌
T. Okaraoto and K. iakashiraa, "Hierarchical Predicate Encryption for Inner-Products" Lecture Notes i n Computer Science (2010.12.01)
T. Okaraoto and K. Takashiraa, "A Geometric Approach on Pairings and Hierarchical Predicate Encryption" in Poster Session, Eurocrypt (2009년 4월)
D. Boneh and L. Ducas, "Anonymity from Asymmetry : New Constructions for Anonymous HIBE" in Poster Session, Eurocrypt (2009년 4월)

(73) 특허권자
니폰덴신뎅와 가부시키가이샤
일본국 도쿄토 치요다쿠 오테마치 2쵸메 3반 1고
미쓰비시덴키 가부시키가이샤
일본국 도쿄도 지요다쿠 마루노우치 2쵸메 7반 3고
(72) 발명자
다카시마 가츠유키
일본 도쿄도 지요다쿠 마루노우치 2쵸메 7반 3고 미쓰비시덴키 가부시키가이샤 내
오카모토 다츠아키
일본 도쿄도 무사시노시 미도리쵸 3쵸메 9반 11고 엔티티 지적 재산 센터 내
(74) 대리인
제일특허법인

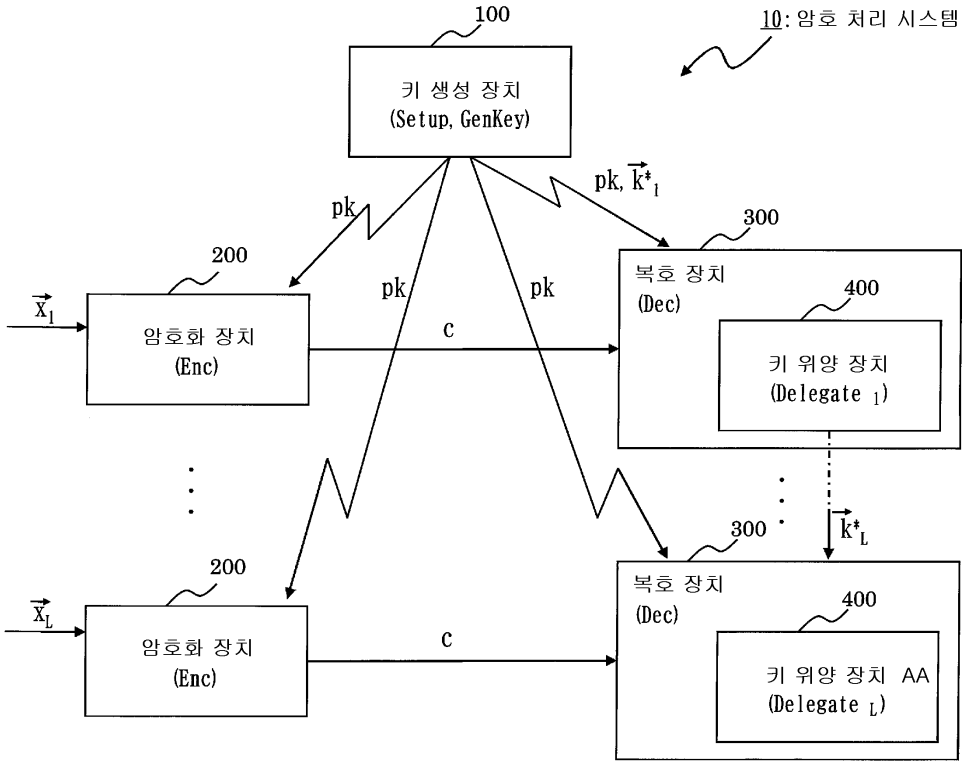
전체 청구항 수 : 총 35 항 심사관 : 장상배

(54) 발명의 명칭 **암호 처리 시스템, 키 생성 장치, 키 위양 장치, 암호화 장치, 복호 장치, 암호 처리 방법 및 암호 처리 프로그램을 기록한 컴퓨터 판독 가능한 기록 매체**

(57) 요 약

권한 위양을 가능하게 한 술어 암호를 실현하는 것을 목적으로 한다. 페어링 연산에 의해 관련지어진 쌍대 벡터 공간(쌍대 디스토션 벡터 공간)인 공간 V와 공간 V^*를 이용하여 암호 처리를 행한다. 암호화 장치는, 공간 V에 있어서의 벡터로서, 송신 정보를 삽입한 벡터를 암호 벡터로서 생성한다. 복호 장치는, 공간 V^*에 있어서의 소정의 벡터를 키 벡터로 하여, 암호화 장치가 생성한 암호 벡터와 키 벡터에 대하여, 페어링 연산을 행하여 상기 암호 벡터를 복호하여 송신 정보에 관한 정보를 추출한다. 특히, 암호화 장치 및 복호 장치는, 공간 V와 공간 V^*의 일부의 차원을 사용하지 않고서 암호 처리를 행한다.

대 표 도



10 암호 처리 시스템
100 키 생성 장치(Setup, GenKey)
200 암호화 장치(Enc)
300 복호 장치(Dec)
400 키 위양 장치(Delegate $_1$)
AA 키 위양 장치(Delegate $_L$)

특허청구의 범위

청구항 1

수학식 1에 나타내는 페어링 연산에 의해 관련지어진 쌍대 벡터 공간(dual vector space)인 공간 V와 공간 V^*를 이용하여 술어 암호 처리를 행하는 암호 처리 시스템으로서,

상기 공간 V에 있어서의 소정의 기저 B를 구성하는 기저 벡터 b_i(i=1, …, n, …, S, …, N)(N은 3 이상의 정수, S는 n+1 이상 N-1 이하의 정수, n은 1 이상 N-2 이하의 정수) 중 기저 벡터 b_i(i=S+1, …, N)를 제외한 적어도 기저 벡터 b_i(i=1, …, n+1)를 갖는 기저 B^와, 소정의 속성 정보가 공개 키로서 주어지고, 상기 기저 B^의 기저 벡터 b_i(i=1, …, n) 중 적어도 일부의 기저 벡터에 대한 계수로서 속성 정보를 설정함과 아울러, 기저 벡터 b_{n+1}에 대한 계수로서 소정의 정보를 설정한 벡터를 암호 벡터 c_1로서 처리 장치에 의해 생성하는 암호화 장치와,

상기 공간 V^*의 기저 B^*에 있어서의 벡터로서, 기저 B^*를 구성하는 기저 벡터 b^*_i(i=1, …, n, …, S, …, N)의 기저 벡터 b^*_i(i=1, …, n) 중 적어도 일부의 기저 벡터에 대한 계수로서 술어 정보를 설정함과 아울러, 상기 기저 B^*의 기저 벡터 b^*_{n+1}에 대한 계수로서 소정의 값을 설정한 벡터를 키 벡터 $k^*_{L,\,dec}$로 하여, 상기 암호화 장치가 생성한 암호 벡터 c_1과 상기 키 벡터 $k^*_{L,\,dec}$에 대하여, 처리 장치에 의해 수학식 1에 나타내는 페어링 연산 $e(c_1, k^*_{L,\,dec})$를 행하여 상기 암호 벡터 c_1을 복호하여 상기 소정의 정보에 관한 값을 추출하는 복호 장치

를 구비하는 것을 특징으로 하는 암호 처리 시스템.

[수학식 1]

$$e(p,q) := \prod_{i=1}^{N} e(\chi_i b_i, \eta_i b_i^*)$$

여기서,

$p := \sum_{i=1}^{N} \chi_i b_i$,

$q := \sum_{i=1}^{N} \eta_i b_i^*$,

χ_i, η_i : 계수

이다

청구항 2

제 1 항에 있어서,

상기 복호 장치는, 상기 기저 B^*를 구성하는 기저 벡터 b^*_i(i=1, …, n, …, R, …, S, …, N)(N은 4 이상의 정수, S는 n+2 이상 N-1 이하의 정수, R은 n+1 이상 S-1 이하의 정수, n은 1 이상 N-3 이하의 정수)의 기저 벡터 b^*_i(i=1, …, n) 중 적어도 일부의 기저 벡터에 술어 정보를 설정하고, 상기 기저 B^*의 기저 벡터 b^*_{n+1}에 대한 계수로서 소정의 값을 설정하고, 기저 벡터 b^*_i(i=R+1, …, S)에 대한 계수로서 난수치를 설정한 벡터를 키 벡터 $k^*_{L,\,dec}$로 하여, 상기 암호 벡터 c_1과 상기 키 벡터 $k^*_{L,\,dec}$에 대하여, 상기 페어링 연산 $e(c_1, k^*_{L,\,dec})$를 행하는 것을 특징으로 하는 암호 처리 시스템.

청구항 3

제 2 항에 있어서,

상기 암호 처리 시스템은, 상기 기저 B^*를 구성하는 기저 벡터 b^*_i(i=1, …, n, …, R, …, S, …, N) 중, 기저 벡터 b^*_i(i=1, …, n)의 적어도 일부의 기저 벡터에 대한 계수로서 술어 정보를 설정하고, 기저 벡터 b^*_{n+1}에 대한 계수로서 소정의 값을 설정하고, 기저 벡터 b^*_i(i=R+1, …, S)에 대한 계수로서 난수치를 설정한 벡터를 키 벡터 $k^*_{L,\,dec}$로서 처리 장치에 의해 생성하는 키 생성 장치를 더 구비하고,

상기 복호 장치는, 상기 키 생성 장치가 생성한 키 벡터 $k^*_{L,\,dec}$를 취득하여, 취득한 키 벡터 $k^*_{L,\,dec}$와 암호 벡터 c_1에 대하여 상기 페어링 연산을 행하는

것을 특징으로 하는 암호 처리 시스템.

청구항 4

제 3 항에 있어서,

상기 암호 처리 시스템은, 상기 키 생성 장치가 생성한 키 벡터 $k^*_{L,\,dec}$로 복호 가능한 암호 벡터 중 일부의 암호 벡터를 복호 가능한 벡터로서, 술어 정보를 설정한 기저 벡터에 대한 계수로서 균등하게 분포시킨 값을 갖는 난수치를 설정한 벡터를 키 벡터 $k^*_{L+1,\,dec}$로서 생성하는 키 위양 장치를 더 구비하는 것을 특징으로 하는 암호 처리 시스템.

청구항 5

술어 암호에 있어서의 비밀 키인 키 벡터 $k^*_{L,\,dec}$를 생성하는 키 생성 장치로서, 수학식 2에 나타내는 페어링 연산에 의해 관련지어진 쌍대 벡터 공간인 공간 V와 공간 V^* 중 상기 공간 V에 있어서의 소정의 기저 B를 구성하는 기저 벡터 b_i(i=1, …, n, …, S, …, N)(N은 3 이상의 정수, S는 n+1 이상 N-1 이하의 정수, n은 1 이상 N-2 이하의 정수) 중 기저 벡터 b_i(i=S+1, …, N)를 제외한 적어도 기저 벡터 b_i(i=1, …, n+1)를 갖는 기저 B^가 공개 키로서 주어진 경우에 있어서의 비밀 키인 키 벡터 $k^*_{L,\,dec}$를 생성하는 상기 키 생성 장치로서,

상기 공간 V^*에 있어서의 소정의 기저 B^*를 기억 장치에 기억하는 마스터 키 기억부와,

상기 마스터 키 기억부가 기억한 상기 기저 B^*를 구성하는 기저 벡터 b^*_i(i=1, …, n, …, S, …, N) 중, 기저 벡터 b^*_i(i=1, …, n)의 적어도 일부의 기저 벡터 b^*_i(i=1, …, μ_L)에 대한 계수로서 술어 정보를 설정함과 아울러, 기저 벡터 b^*_{n+1}에 대한 계수로서 소정의 값을 설정한 벡터를 키 벡터 $k^*_{L,\,dec}$로서 처리 장치에 의해 생성하는 키 벡터 생성부

를 구비하는 것을 특징으로 하는 키 생성 장치.

[수학식 2]

$$e(p,q) := \prod_{i=1}^{N} e(\chi_i b_i, \eta_i b_i^*)$$

여기서,

$p := \sum_{i=1}^{N} \chi_i b_i$,

$q := \sum_{i=1}^{N} \eta_i b_i^*$,

χ_i, η_i : 계수

이다

청구항 6

제 5 항에 있어서,

상기 키 벡터 생성부는, 상기 기저 B^*를 구성하는 기저 벡터 b^*_i(i=1, …, n, …, R, …, S, …, N)(N은 4 이상의 정수, S는 n+2 이상 N-1 이하의 정수, R은 n+1 이상 S-1 이하의 정수, n은 1 이상 N-3 이하의 정수) 중, 기저 벡터 b^*_i(i=1, …, n)의 적어도 일부의 기저 벡터 b^*_i(i=1, …, μ_L)에 대한 계수로서 술어 정보를 설정함과 아울러, 기저 벡터 b^*_{n+1}에 대한 계수로서 소정의 값을 설정하고, 기저 벡터 b^*_i(i=R+1, …, S)에 대한 계수로서 난수치를 설정한 벡터를 키 벡터 $k^*_{L,\,dec}$로서 처리 장치에 의해 생성하는 것을 특징으로 하는 키 생성 장치.

청구항 7

제 6 항에 있어서,

상기 키 벡터 생성부는, 수학식 3에 나타내는 키 벡터 $k^*_{L,\,dec}$를 생성하는 것을 특징으로 하는 키 생성 장치.

[수학식 3]

$$k^*_{L,\mathrm{dec}} := \sum_{t=1}^{L} \sigma_{0,t} \left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b_i^* \right) + b^*_{n+1} + \sum_{h=1}^{r} \eta_{0,h} b^*_{n+2+h}$$

여기서,

$\sigma_{0,i}, \eta_{0,h} \quad (i = 1,\ldots,L;\ h = 1,\ldots,r)$: 난수치,

$v_i \quad (i = 1,\ldots,\mu_L)$: 술어 정보,

r : 1 이상의 정수로서, $n+2 = R,\ n+2+r = S$

이다

청구항 8

제 6 항에 있어서,

상기 키 벡터 생성부는, 수학식 4에 나타내는 키 벡터 $k^*_{L,\,dec}$를 생성하는 것을 특징으로 하는 키 생성 장치.

[수학식 4]

$$k^*_{L,\mathrm{dec}} := \sum_{t=1}^{L} \sigma_{\mathrm{dec},t} \left(\sum_{i=1}^{n} v_{t,i} b^*_i \right) + b^*_{n+1} + \sum_{h=1}^{r} \eta_{\mathrm{dec},h} b^*_{n+2+h}$$

여기서,

$\sigma_{\mathrm{dec},t}, \eta_{\mathrm{dec},h} \quad (t = 1,\ldots,L;\ h = 1,\ldots,r)$: 난수치,

$v_{t,i} \quad (t = 1,\ldots,L; i = 1,\ldots,n)$: 술어 정보,

r : 1이상의 정수로서, $n+2 = R,\ n+2+r = S$

이다

청구항 9

제 6 항에 있어서,

상기 키 생성 장치는, 상기 키 벡터 생성부가 생성한 키 벡터 $k^*_{L,\ dec}$로 복호 가능한 암호 벡터 중 일부의 암호 벡터를 복호 가능한 키 벡터 $k^*_{L+1,\ dec}$를 생성하기 위한 벡터로서, 적어도 $j=\mu_L+1$, …, n의 각 j에 대하여, 기저 벡터 b^*_j에 대한 계수로서 난수치가 설정되는 것과 아울러, 기저 벡터 b^*_i(i=R+1, …, S)의 일부의 기저 벡터에 대한 계수로서 난수치가 설정된 적어도 $n-\mu_L$개의 벡터를 키 생성용 벡터 $k^*_{L,\ del,\ j}$로서 처리 장치에 의해 생성하는 키 생성용 벡터 생성부와,

상기 키 생성용 벡터 생성부가 생성한 키 생성용 벡터 $k^*_{L,\ del,\ j}$로 생성되는 키 벡터 $k^*_{L+1,\ dec}$ 중, 술어 정보가 설정되는 기저 벡터의 계수에 균등하게 분포한 값을 설정하기 위한 벡터로서, 기저 벡터 b^*_i(i=1, …, μ_L)에 대한 계수로서 난수치가 승산된 술어 정보가 설정되는 것과 아울러, 기저 벡터 b^*_i(i=R+1, …, S)의 일부의 기저 벡터에 대한 계수로서 난수치가 설정된 적어도 L+1개의 벡터를 랜덤화 벡터 $k^*_{L,\ ran,\ j}$로서 처리 장치에 의해 생성하는 랜덤화 벡터 생성부

를 더 구비하는 것을 특징으로 하는 키 생성 장치.

청구항 10

제 9 항에 있어서,

상기 키 벡터 생성부는, 수학식 5에 나타내는 키 생성용 벡터 $k^*_{L,\ del,\ j}$를 생성하고,

상기 랜덤화 벡터 생성부는, 수학식 6에 나타내는 랜덤화 벡터 $k^*_{L,\ ran,\ j}$를 생성하는

것을 특징으로 하는 키 생성 장치.

[수학식 5]

$$k^*_{L,\mathrm{del},j} := \sum_{t=1}^{L} \sigma_{j,t} \left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b^*_i \right) + \psi b^*_j + \sum_{h=1}^{r} \eta_{j,h} b^*_{n+2+h} \qquad (j = \mu_L + 1,\ldots,n)$$

여기서,

$\sigma_{j,i}, \psi, \eta_{j,h} \quad (j = \mu_L + 1,\ldots,n;\ i = 1,\ldots,L;\ h = 1,\ldots,r)$: 난수치,

$v_i \quad (i = 1,\ldots,\mu_L)$: 술어 정보,

r : 1이상의 정수로서, $n+2 = R,\ n+2+r = S$

이다.

[수학식 6]

$$k^*_{L,\mathrm{ran},j} := \sum_{t=1}^{L} \sigma_{j,t} \left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b_i^* \right) + \sum_{h=1}^{r} \eta_{j,h} b^*_{n+2+h} \quad (j = 1,\ldots,L+1)$$

여기서,

$\sigma_{j,i}, \eta_{j,h}$ $(j = 1,\ldots,L+1;\ i = 1,\ldots,L;\ h = 1,\ldots,r)$: 난수치,

v_i $(i = 1,\ldots,\mu_L)$: 술어 정보,

r : 1이상의 정수로서, $n+2 = R,\ n+2+r = S$

이다.

청구항 11

제 9 항에 있어서,

상기 키 벡터 생성부는, 수학식 7에 나타내는 키 생성용 벡터 $k^*_{L,\mathrm{del},j}$를 생성하고,

상기 랜덤화 벡터 생성부는, 수학식 8에 나타내는 랜덤화 벡터 $k^*_{L,\mathrm{ran},j}$를 생성하는

것을 특징으로 하는 키 생성 장치.

[수학식 7]

$$k^*_{L,\mathrm{del},j} := \sum_{t=1}^{L} \sigma_{\mathrm{del},j,t} \left(\sum_{i=1}^{n} v_{t,i} b_i^* \right) + \psi b_j^* + \sum_{h=1}^{r} \eta_{\mathrm{del},j,h} b^*_{n+2+h} \quad (j = 1,\ldots,n)$$

여기서,

$\sigma_{\mathrm{del},j,t}, \eta_{\mathrm{del},j,h}, \psi$ $(j = 1,\ldots,n;\ t = 1,\ldots,L;\ h = 1,\ldots,r)$: 난수치,

$v_{t,i}$ $(t = 1,\ldots,L; i = 1,\ldots,n)$: 술어 정보,

r : 1 이상의 정수로서, $n+2 = R,\ n+2+r = S$

이다.

[수학식 8]

$$k^*_{L,\mathrm{ran},j} := \sum_{t=1}^{L} \sigma_{\mathrm{ran},j,t} \left(\sum_{i=1}^{n} v_{t,i} b_i^* \right) + \sum_{h=1}^{r} \eta_{\mathrm{ran},j,h} b^*_{n+2+h} \quad (j = 1,\ldots,L+1)$$

여기서,

$\sigma_{\mathrm{ran},j,t}, \eta_{\mathrm{ran},j,h}$ $(j = 1,\ldots,L+1;\ t = 1,\ldots,L;\ h = 1,\ldots,r)$: 난수치,

$v_{t,i}$ $(t = 1,\ldots,L; i = 1,\ldots,n)$: 술어 정보,

r : 1이상의 정수로서, $n+2 = R,\ n+2+r = S$

이다.

청구항 12

술어 암호에 있어서의 비밀 키인 키 벡터 $k^*_{L,\mathrm{dec}}$로 복호 가능한 암호 벡터 중 일부의 암호 벡터를 복호 가능한 키 벡터 $k^*_{L+1,\mathrm{dec}}$를 생성하는 키 위양 장치로서, 수학식 9에 나타내는 페어링 연산에 의해 관련지어진 쌍대 벡터 공간인 공간 V와 공간 V^* 중 상기 공간 V에 있어서의 소정의 기저 B를 구성하는 기저 벡터 b_i(i=1, …, n, …, R, …, S, …, N)(N은 4 이상의 정수, S는 n+2 이상 N-1 이하의 정수, R은 n+1 이상 S-1 이하의 정수, n은 1 이상 N-3 이하의 정수) 중 기저 벡터 b_i(i=S+1, …, N)를 제외한 적어도 기저 벡터 b_i(i=1, …, n+1)를 갖는 기저 B^가 공개 키로서 주어진 경우에 있어서의 비밀 키인 키 벡터 $k^*_{L+1,\mathrm{dec}}$를 생성하는 상기 키 위양 장치로서,

기저 B^*를 구성하는 기저 벡터 b^*_i(i=1, …, n, …, R, …, S, …, N) 중, 기저 벡터 b^*_i(i=1, …, n)의 적어도 일부의 기저 벡터 b^*_i(i=1, …, μ_L)에 대한 계수로서 술어 정보가 설정되고, 기저 벡터 b^*_{n+1}에 대한 계수로서 소정의 값이 설정되고, 기저 벡터 b^*_i(i=R+1, …, S)에 대한 계수로서 난수치가 설정된 키 벡터 $k^*_{L,\,dec}$를 취득하는 키 벡터 취득부와,

적어도 j=μ_L+1, …, n의 각 j에 대하여, 기저 벡터 b^*_j에 대한 계수로서 난수치가 설정되는 것과 아울러, 기저 벡터 b^*_i(i=R+1, …, S)에 대한 계수로서 난수치가 설정된 적어도 n-μ_L개의 키 생성용 벡터 $k^*_{L,\,del,\,j}$를 취득하는 키 생성용 벡터 취득부와,

상기 키 생성용 벡터 취득부가 취득한 상기 키 생성용 벡터 $k^*_{L,\,del,\,j}$의 적어도 일부의 상기 키 생성용 벡터 $k^*_{L,\,del,\,j}$의 각 기저 벡터의 계수를 술어 정보로 승산하고, 상기 키 벡터 취득부가 취득한 상기 키 벡터 $k^*_{L,\,dec}$에 가산하여 키 벡터 $k^*_{L+1,\,dec}$를 생성하는 키 벡터 생성부

를 구비하는 것을 특징으로 하는 키 위양 장치.

[수학식 9]

$$e(p,q) := \prod_{i=1}^{N} e(\chi_i b_i, \eta_i b_i^*)$$

여기서,

$p := \sum_{i=1}^{N} \chi_i b_i$,

$q := \sum_{i=1}^{N} \eta_i b_i^*$,

χ_i, η_i : 계수

이다.

청구항 13

제 12 항에 있어서,

상기 키 위양 장치는, 기저 벡터 b^*_i(i=1, …, μ_L)에 대한 계수로서 난수치가 승산된 술어 정보가 설정되는 것과 아울러, 기저 벡터 b^*_i(i=R+1, …, S)에 대한 계수로서 난수치가 설정된 적어도 L+1개의 랜덤화 벡터 $k^*_{L,\,ran,\,j}$를 취득하는 랜덤화 벡터 취득부를 더 구비하고,

상기 키 벡터 생성부는, 상기 랜덤화 벡터 취득부가 취득한 상기 랜덤화 벡터 $k^*_{L,\,ran,\,j}$의 적어도 일부의 상기 랜덤화 벡터 $k^*_{L,\,ran,\,j}$의 각 기저 벡터의 계수를 난수치로 승산하고, 상기 키 벡터 $k^*_{L+1,\,dec}$에 더 가산하여 키 벡터 $k^*_{L+1,\,dec}$를 생성하는

것을 특징으로 하는 키 위양 장치.

청구항 14

제 13 항에 있어서,

상기 키 벡터 취득부는, 수학식 10에 나타내는 키 벡터 $k^*_{L,\,dec}$를 취득하고,

상기 키 생성용 벡터 취득부는, 수학식 11에 나타내는 키 생성용 벡터 $k^*_{L,\,del,\,j}$를 취득하고,

상기 랜덤화 벡터 취득부는, 수학식 12에 나타내는 랜덤화 벡터 $k^*_{L,\,ran,\,j}$를 취득하고,

상기 키 벡터 생성부는, 수학식 13에 나타내는 키 벡터 $k^*_{L+1,\,dec}$를 생성하는

것을 특징으로 하는 키 위양 장치.

[수학식 10]

$$k^*_{L,\mathrm{dec}} := \sum_{t=1}^{L}\sigma_{0,t}\left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b_i^*\right) + b^*_{n+1} + \sum_{h=1}^{r}\eta_{0,h} b^*_{n+2+h}$$

여기서,

$\sigma_{0,i},\eta_{0,h} \quad (i=1,\ldots,L;\ h=1,\ldots,r)$: 난수치,

$v_i \quad (i=1,\ldots,\mu_L)$: 솔어 정보,

r : 1 이상의 정수로서, $n+2=R,\ n+2+r=S$

이다.

[수학식 11]

$$k^*_{L,\mathrm{del},j} := \sum_{t=1}^{L}\sigma_{j,t}\left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b_i^*\right) + \psi b_j^* + \sum_{h=1}^{r}\eta_{j,h} b^*_{n+2+h} \quad (j=\mu_L+1,\ldots,n)$$

여기서,

$\sigma_{j,i},\psi,\eta_{j,h} \quad (j=\mu_L+1,\ldots,n;\ i=1,\ldots,L;\ h=1,\ldots,r)$:난수치,

$v_i \quad (i=1,\ldots,\mu_L)$: 솔어 정보,

r : 1 이상의 정수로서, $n+2=R,\ n+2+r=S$

이다.

[수학식 12]

$$k^*_{L,\mathrm{ran},j} := \sum_{t=1}^{L}\sigma_{j,t}\left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b_i^*\right) + \sum_{h=1}^{r}\eta_{j,h} b^*_{n+2+h} \quad (j=1,\ldots,L+1)$$

여기서,

$\sigma_{j,i},\eta_{j,h} \quad (j=1,\ldots,L+1;\ i=1,\ldots,L;\ h=1,\ldots,r)$: 난수치,

$v_i \quad (i=1,\ldots,\mu_L)$: 솔어 정보,

r : 1 이상의 정수로서, $n+2=R,\ n+2+r=S$

이다.

[수학식 13]

$$k^*_{L+1,\mathrm{dec}} := k^*_{L,\mathrm{dec}} + \sum_{t=1}^{L+1}\alpha_{0,t} k^*_{L,\mathrm{ran},t} + \sigma_0\left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^*_{L,\mathrm{del},i}\right)$$

여기서,

$\alpha_{0,t},\sigma_0 \quad (t=1,\ldots,L+1)$: 난수치,

$v_i \quad (i=\mu_L+1,\ldots,\mu_{L+1})$: 솔어 정보,

이다.

청구항 15

제 13 항에 있어서,

상기 키 벡터 취득부는, 수학식 14에 나타내는 키 벡터 $k^*_{L,\,dec}$를 취득하고,

상기 키 생성용 벡터 취득부는, 수학식 15에 나타내는 키 생성용 벡터 $k^*_{L,\,del,\,j}$를 취득하고,

상기 랜덤화 벡터 취득부는, 수학식 16에 나타내는 랜덤화 벡터 $k^*_{L,\,ran,\,j}$를 취득하고,

상기 키 벡터 생성부는, 수학식 17에 나타내는 키 벡터 $k^*_{L+1,\,dec}$를 생성하는

것을 특징으로 하는 키 위양 장치.

[수학식 14]

$$k^*_{L,\mathrm{dec}} := \sum_{t=1}^{L} \sigma_{\mathrm{dec},t}\left(\sum_{i=1}^{n} v_{t,i} b_i^*\right) + b^*_{n+1} + \sum_{h=1}^{r} \eta_{\mathrm{dec},h} b^*_{n+2+h}$$

여기서,

$\sigma_{\mathrm{dec},t}, \eta_{\mathrm{dec},h} \quad (t = 1,\ldots,L;\ h = 1,\ldots,r)$: 난수치,

$v_{t,i} \quad (t = 1,\ldots,L; i = 1,\ldots,n)$: 술어 정보,

r : 1 이상의 정수로서, $n+2 = R,\ n+2+r = S$

이다.

[수학식 15]

$$k^*_{L,\mathrm{del},j} := \sum_{t=1}^{L} \sigma_{\mathrm{del},j,t}\left(\sum_{i=1}^{n} v_{t,i} b_i^*\right) + \psi b_j^* + \sum_{h=1}^{r} \eta_{\mathrm{del},j,h} b^*_{n+2+h} \quad (j = 1,\ldots,n)$$

여기서,

$\sigma_{\mathrm{del},j,t}, \eta_{\mathrm{del},j,h}, \psi \quad (j = 1,\ldots,n;\ t = 1,\ldots,L;\ h = 1,\ldots,r)$: 난수치,

$v_{t,i} \quad (t = 1,\ldots,L; i = 1,\ldots,n)$: 술어 정보,

r : 1 이상의 정수로서, $n+2 = R,\ n+2+r = S$

이다.

[수학식 16]

$$k^*_{L,\mathrm{ran},j} := \sum_{t=1}^{L} \sigma_{\mathrm{ran},j,t}\left(\sum_{i=1}^{n} v_{t,i} b_i^*\right) + \sum_{h=1}^{r} \eta_{\mathrm{ran},j,h} b^*_{n+2+h} \quad (j = 1,\ldots,L+1)$$

여기서,

$\sigma_{\mathrm{ran},j,t}, \eta_{\mathrm{ran},j,h} \quad (j = 1,\ldots,L+1;\ t = 1,\ldots,L;\ h = 1,\ldots,r)$: 난수치,

$v_{t,i} \quad (t = 1,\ldots,L; i = 1,\ldots,n)$: 술어 정보,

r : 1 이상의 정수로서, $n+2 = R,\ n+2+r = S$

이다.

[수학식 17]

$$k^*_{L+1,\mathrm{dec}} := k^*_{L,\mathrm{dec}} + \sum_{t=1}^{L+1} \alpha_{\mathrm{dec},t} k^*_{L,\mathrm{ran},t} + \sigma_{\mathrm{dec}}\left(\sum_{i=1}^{n} v_{L+1,i} k^*_{L,\mathrm{del},i}\right)$$

여기서,

$\sigma_{\mathrm{dec},t}, \sigma_{\mathrm{dec}} \quad (t = 1,\ldots,L+1)$: 난수치,

$v_{L+1,i} \quad (i = 1,\ldots,n)$: 술어 정보,

이다.

청구항 16

제 13 항에 있어서,

상기 키 위양 장치는, 상기 키 벡터 생성부가 생성한 키 벡터 $k^*_{L+1,\,dec}$로 복호 가능한 암호 벡터 중 일부의 암호

벡터를 복호 가능한 키 벡터 $k^*_{L+2,\,dec}$를 생성하기 위한 벡터로서, 적어도 $j=\mu_{L+1}+1$, …, n의 각 j에 대하여, 기저 벡터 b^*_j에 대한 계수로서 난수치를 설정한 적어도 $n-\mu_{L+1}$개의 벡터를 키 생성용 벡터 $k^*_{L+1,\,del,\,j}$로서 처리 장치에 의해 생성하는 키 생성용 벡터 생성부와,

상기 키 생성용 벡터 생성부가 생성한 키 생성용 벡터 $k^*_{L+1,\,del,\,j}$로 생성되는 키 벡터 $k^*_{L+2,\,dec}$ 중, 술어 정보가 설정되는 기저 벡터의 계수에 균등하게 분포한 값을 설정하기 위한 벡터로서, 기저 벡터 b^*_i(i=1, …, μ_L)에 대한 계수로서 난수치가 승산된 술어 정보를 설정한 적어도 L+2개의 벡터를 랜덤화 벡터 $k^*_{L+1,\,ran,\,j}$로서 처리 장치에 의해 생성하는 랜덤화 벡터 생성부

를 더 구비하는 것을 특징으로 하는 키 위양 장치.

청구항 17

제 16 항에 있어서,

상기 키 생성용 벡터 취득부는, 수학식 18에 나타내는 키 생성용 벡터 $k^*_{L,\,del,\,j}$를 취득하고,

상기 랜덤화 벡터 취득부는, 수학식 19에 나타내는 랜덤화 벡터 $k^*_{L,\,ran,\,j}$를 취득하고,

상기 키 벡터 생성부는, 수학식 20에 나타내는 키 생성용 벡터 $k^*_{L+1,\,del,\,j}$를 생성하고,

상기 랜덤화 벡터 생성부는, 수학식 21에 나타내는 랜덤화 벡터 $k^*_{L+1,\,ran,\,j}$를 생성하는

것을 특징으로 하는 키 위양 장치.

[수학식 18]

$$k^*_{L,\mathrm{del},j} := \sum_{t=1}^{L}\sigma_{j,t}\left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b^*_i\right) + \psi b^*_j + \sum_{h=1}^{r}\eta_{j,h} b^*_{n+2+h} \qquad (j=\mu_L+1,\ldots,n)$$

여기서,

$\sigma_{j,t},\psi,\eta_{j,h}$ $\quad (j=\mu_L+1,\ldots,n;\ t=1,\ldots,L;\ h=1,\ldots,r)$: 난수치,

v_i $\quad (i=1,\ldots,\mu_L)$: 술어 정보,

r : 1 이상의 정수로서, $n+2=R,\ n+2+r=S$

이다.

[수학식 19]

$$k^*_{L,\mathrm{ran},j} := \sum_{t=1}^{L}\sigma_{j,t}\left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b^*_i\right) + \sum_{h=1}^{r}\eta_{j,h} b^*_{n+2+h} \qquad (j=1,\ldots,L+1)$$

여기서,

$\sigma_{j,t},\eta_{j,h}$ $\quad (j=1,\ldots,L+1;\ t=1,\ldots,L;\ h=1,\ldots,r)$: 난수치,

v_i $\quad (i=1,\ldots,\mu_L)$: 술어 정보,

r : 1 이상의 정수로서, $n+2=R,\ n+2+r=S$

이다.

[수학식 20]

$$k^{*}_{L+1,\mathrm{del},j} := \sum_{t=1}^{L+1} \alpha_{j,t} k^{*}_{L,\mathrm{ran},t} + \sigma_j \left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^{*}_{L,\mathrm{del},i} \right) + \psi' k^{*}_{L,\mathrm{del},j} \quad \left(j = \mu_{L+1}+1, \ldots, n \right)$$

여기서,

$\alpha_{j,t}, \sigma_j, \psi' \quad \left(j = \mu_{L+1}+1, \ldots, n;\ t = 1, \ldots, L+1 \right)$: 난수치,

$v_i \quad \left(i = \mu_L + 1, \ldots, \mu_{L+1} \right)$: 술어 정보,

이다.

[수학식 21]

$$k^{*}_{L+1,\mathrm{ran},j} := \sum_{t=1}^{L+1} \alpha_{j,t} k^{*}_{L,\mathrm{ran},t} + \sigma_j \left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^{*}_{L,\mathrm{del},i} \right) \quad \left(j = 1, \ldots, L+2 \right)$$

여기서,

$\alpha_{j,t}, \sigma_j \quad \left(j = 1, \ldots, L+2;\ t = 1, \ldots, L+1 \right)$: 난수치,

$v_i \quad \left(i = \mu_L + 1, \ldots, \mu_{L+1} \right)$: 술어 정보,

이다.

청구항 18

제 16 항에 있어서,

상기 키 생성용 벡터 취득부는, 수학식 22에 나타내는 키 생성용 벡터 $k^{*}_{L,\mathrm{del},j}$를 취득하고,

상기 랜덤화 벡터 취득부는, 수학식 23에 나타내는 랜덤화 벡터 $k^{*}_{L,\mathrm{ran},j}$를 취득하고,

상기 키 벡터 생성부는, 수학식 24에 나타내는 키 생성용 벡터 $k^{*}_{L+1,\mathrm{del},j}$를 생성하고,

상기 랜덤화 벡터 생성부는, 수학식 25에 나타내는 랜덤화 벡터 $k^{*}_{L+1,\mathrm{ran},j}$를 생성하는

것을 특징으로 하는 키 위양 장치.

[수학식 22]

$$k^{*}_{L,\mathrm{del},j} := \sum_{t=1}^{L} \sigma_{\mathrm{del},j,t} \left(\sum_{i=1}^{n} v_{t,i} b^{*}_i \right) + \psi b^{*}_j + \sum_{h=1}^{r} \eta_{\mathrm{del},j,h} b^{*}_{n+2+h} \quad \left(j = 1, \ldots, n \right)$$

여기서,

$\sigma_{\mathrm{del},j,t}, \eta_{\mathrm{del},j,h}, \psi \quad \left(j = 1, \ldots, n;\ t = 1, \ldots, L;\ h = 1, \ldots, r \right)$: 난수치,

$v_{t,i} \quad \left(t = 1, \ldots, L; i = 1, \ldots, n \right)$: 술어 정보,

r : 1 이상의 정수로서, $n+2 = R,\ n+2+r = S$

이다.

[수학식 23]

$$k^*_{L,\mathrm{ran},j} := \sum_{t=1}^{L} \sigma_{\mathrm{ran},j,t}\left(\sum_{i=1}^{n} v_{t,i} b_i^*\right) + \sum_{h=1}^{r} \eta_{\mathrm{ran},j,h} b^*_{n+2+h} \quad (j = 1,\ldots,L+1)$$

여기서,

$\sigma_{\mathrm{ran},j,t}, \eta_{\mathrm{ran},j,h}$ $(j = 1,\ldots,L+1;\ t = 1,\ldots,L;\ h = 1,\ldots,r)$: 난수치,

$v_{t,i}$ $(t = 1,\ldots,L; i = 1,\ldots,n)$: 술어 정보,

r : 1 이상의 정수로서, $n+2 = R$, $n+2+r = S$

이다.

[수학식 24]

$$k^*_{L+1,\mathrm{del},j} := \sum_{t=1}^{L+1} \alpha_{\mathrm{del},j,t} k^*_{L,\mathrm{del},t} + \sigma_{\mathrm{del},j}\left(\sum_{i=1}^{n} v_{L+1,i} k^*_{L,\mathrm{del},i}\right) + \psi' k^*_{L,\mathrm{del},j} \quad (j = 1,\ldots,n)$$

여기서,

$\alpha_{\mathrm{del},j,t}, \sigma_{\mathrm{del},j}, \psi'$ $(j = 1,\ldots,n;\ i = 1,\ldots,L+1)$: 난수치,

$v_{L+1,i}$ $(i = 1,\ldots,n)$: 술어 정보,

이다.

[수학식 25]

$$k^*_{L+1,\mathrm{ran},j} := \sum_{t=1}^{L+1} \alpha_{\mathrm{ran},j,t} k^*_{L,\mathrm{ran},t} + \sigma_{\mathrm{ran},j}\left(\sum_{i=1}^{n} v_{L+1,i} k^*_{L,\mathrm{del},i}\right) \quad (j = 1,\ldots,L+2)$$

여기서,

$\alpha_{\mathrm{ran},j,t}, \sigma_{\mathrm{ran},j}$ $(j = 1,\ldots,L+2;\ t = 1,\ldots,L+1)$: 난수치,

$v_{L+1,i}$ $(i = 1,\ldots,n)$: 술어 정보,

이다.

청구항 19

페어링 연산에 의해 관련지어진 쌍대 벡터 공간인 공간 V와 공간 V^*에 있어서 실현되는 술어 암호 처리에 있어서의 암호문인 암호 벡터 c_1을 생성하는 암호화 장치로서,

상기 공간 V에 있어서의 소정의 기저 B를 구성하는 기저 벡터 b_i(i=1, …, n, …, S, …, N)(N은 3 이상의 정수, S는 n+1 이상 N-1 이하의 정수, n은 1 이상 N-2 이하의 정수) 중 기저 벡터 b_i(i=S+1, …, N)를 제외한 적어도 기저 벡터 b_i(i=1, …, n+1)를 갖는 기저 B^를 취득함과 아울러, 소정의 속성 정보를 취득하는 공개 키 취득부와,

상기 공개 키 취득부가 취득한 기저 B^에 있어서의 벡터로서, 기저 벡터 b_{n+1}에 대한 계수로서 소정의 정보를 설정한 벡터를 송신 정보 벡터 ζv로서 처리 장치에 의해 생성하는 송신 정보 설정부와,

상기 기저 B^의 상기 기저 벡터 b_i(i=1, …, n) 중 적어도 일부의 기저 벡터에 대한 계수로서 상기 속성 정보를 설정한 속성 정보 벡터를, 상기 송신 정보 설정부가 생성한 송신 정보 벡터 ζv에 가산하여 암호 벡터 c_1을 처리 장치에 의해 생성하는 암호 벡터 생성부

를 구비하는 것을 특징으로 하는 암호화 장치.

청구항 20

제 19 항에 있어서,

상기 송신 정보 설정부는, 수학식 26에 나타내는 송신 정보 벡터 ζv를 생성하고,

상기 암호 벡터 생성부는, 수학식 27에 나타내는 암호 벡터 c_1을 생성하는

것을 특징으로 하는 암호화 장치.

[수학식 26]

$$\zeta v := \zeta b_{n+1}$$

여기서,

ζ : 난수치

이다.

[수학식 27]

$$c_1 := \sum_{t=1}^{d} \delta_t \left(\sum_{i=\mu_{t-1}+1}^{\mu_t} x_i b_i \right) + \zeta b_{n+1}$$

여기서,

$\left(\vec{x}_1,\ldots,\vec{x}_L\right) := \left(\left(x_1,\ldots,x_{\mu_1}\right),\ldots,\left(x_{\mu_{L-1}+1},\ldots,x_{\mu_L}\right)\right)$: 속성 정보,

$\left(\vec{x}_{L+1},\ldots,\vec{x}_d\right) := \left(\left(x_{\mu_L+1},\ldots,x_{\mu_{L+1}}\right),\ldots,\left(x_{\mu_{d-1}+1},\ldots,x_{\mu_d}\right)\right)$: 난수치,

$\delta_1,\ldots,\delta_d$: 난수치

이다.

청구항 21

제 19 항에 있어서,

상기 송신 정보 설정부는, 수학식 28에 나타내는 송신 정보 벡터 ζv를 생성하고,

상기 암호 벡터 생성부는, 수학식 29에 나타내는 암호 벡터 c_1을 생성하는

것을 특징으로 하는 암호화 장치.

[수학식 28]

$$\zeta v := \zeta b_{n+1}$$

여기서,

ζ : 난수치

이다.

[수학식 29]

$$c_1 := \sum_{t=1}^{L} \delta_t \left(\sum_{i=1}^{n} x_{t,i} b_i \right) + \zeta b_{n+1}$$

여기서,

$\left(\vec{x}_1,\ldots,\vec{x}_L\right) := \left(\left(x_{1,1},\ldots,x_{1,n}\right),\ldots,\left(x_{L,1},\ldots,x_{L,n}\right)\right)$: 속성 정보,

$\delta_1,\ldots,\delta_d$: 난수치

이다.

청구항 22

제 19 항에 있어서,

상기 암호화 장치는, 수학식 30에 나타내는 암호 정보 c_2를 생성하는 암호 정보 생성부를 더 구비하는 것을 특징으로 하는 암호화 장치.

[수학식 30]

$$c_2 := g_T^{\xi} m$$

여기서,

$g_T = e(a_i, a_i^*) \neq 1$,

$\mathbb{A}$는 공간 $\mathbb{V}$의 기저로서, $\mathbb{A} := (a_1, ..., a_N)$,

$\mathbb{A}^*$는 공간 $\mathbb{V}^*$의 기저로서, $\mathbb{A}^* := (a_1^*, ..., a_N^*)$

이다.

청구항 23

수학식 31에 나타내는 페어링 연산에 의해 관련지어진 쌍대 벡터 공간인 공간 V와 공간 V^*에 있어서 실현되는 술어 암호 처리에 있어서의 암호문을 복호하는 복호 장치로서,

상기 공간 V에 있어서의 소정의 기저 B를 구성하는 기저 벡터 b_i(i=1, …, n, …, S, …, N)(N은 3 이상의 정수, S는 n+1 이상 N-1 이하의 정수, n은 1 이상 N-2 이하의 정수) 중 기저 벡터 b_i(i=S+1, …, N)를 제외한 적어도 기저 벡터 b_i(i=1, …, n+1)를 갖는 기저 B^가 공개 키로서 주어진 경우에 생성되는 암호문인 암호 벡터 c_1로서, 상기 기저 B^의 기저 벡터 b_i(i=1, …, n) 중 적어도 기저 벡터 b_i(i=1, …, μ_h)에 대한 계수로서 속성 정보가 설정되는 것과 아울러, 상기 기저 벡터 b_{n+1}에 대한 계수로서 소정의 정보가 설정된 벡터인 암호 벡터 c_1을 입력하는 벡터 입력부와,

상기 공간 V^*에 있어서의 소정의 기저 B^*의 기저 벡터 b^*_i(i=1, …, n, …, S, …, N) 중, 기저 벡터 b^*_i(i=1, …, n)의 적어도 기저 벡터 b^*_i(i=1, …, μ_L)($\mu_L \leq \mu_h$)에 대한 계수로서 술어 정보 v_i(i=1, …, μ_L)가 설정되고, 기저 벡터 b^*_{n+1}에 대한 계수로서 소정의 값이 설정된 키 벡터 $k^*_{L,\,dec}$를 기억 장치에 기억하는 키 벡터 기억부와,

상기 벡터 입력부가 입력한 암호 벡터 c_1과, 상기 키 벡터 기억부가 기억한 키 벡터 $k^*_{L,\,dec}$에 대하여 처리 장치에 의해 수학식 31에 나타내는 페어링 연산을 행하고, 상기 암호 벡터 c_1로부터 상기 소정의 정보에 관한 값을 추출하는 페어링 연산부

를 구비하는 것을 특징으로 하는 복호 장치.

[수학식 31]

$$e(p,q) := \prod_{i=1}^{N} e(\chi_i b_i, \eta_i b_i^*)$$

여기서,

$p := \sum_{i=1}^{N} \chi_i b_i$,

$q := \sum_{i=1}^{N} \eta_i b_i^*$,

χ_i, η_i : 계수

이다.

청구항 24

제 23 항에 있어서,

상기 키 벡터 기억부는, 상기 기저 B^*를 구성하는 기저 벡터 b^*_i(i=1, …, n, …, R, …, S, …, N)(N은 4 이상의 정수, S는 n+2 이상 N-1 이하의 정수, R은 n+1 이상 S-1 이하의 정수, n은 1 이상 N-3 이하의 정수)의 적어도 기저 벡터 b^*_i(i=1, …, μ_L)($\mu_L \leq \mu_h$)에 대한 계수로서 술어 정보 v_i(i=1, …, μ_L)가 설정되고, 기저 벡터 b^*_{n+1}에 대한 계수로서 소정의 값이 설정되고, 기저 벡터 b^*_i(i=R+1, …, S)의 일부의 기저 벡터에 대한 계수로서 소정의 값이 설정된 키 벡터 $k^*_{L,\,dec}$를 기억하는 것을 특징으로 하는 복호 장치.

청구항 25

제 24 항에 있어서,

상기 벡터 입력부는, 수학식 32에 나타내는 암호 벡터 c_1을 입력하고,

상기 키 벡터 기억부는, 수학식 33에 나타내는 키 벡터 $k^*_{L,\,dec}$를 기억하고,

상기 페어링 연산부는, 수학식 34에 나타내는 페어링 연산을 행하고, 상기 암호 벡터로부터 상기 소정의 정보에 관한 값을 추출하는

것을 특징으로 하는 복호 장치.

[수학식 32]

$$c_1 := \sum_{t=1}^{d} \delta_t \left(\sum_{i=\mu_{t-1}+1}^{\mu_t} x_i b_i \right) + \zeta b_{n+1}$$

여기서,

$\left(\vec{x}_1,\ldots,\vec{x}_h\right) := \left(\left(x_1,\ldots,x_{\mu_1}\right),\ldots,\left(x_{\mu_{L-1}+1},\ldots,x_{\mu_h}\right)\right)$: 속성 정보,

$\left(\vec{x}_{h+1},\ldots,\vec{x}_d\right) := \left(\left(x_{\mu_{h+1}+1},\ldots,x_{\mu_{h+2}}\right),\ldots,\left(x_{\mu_{d-1}+1},\ldots,x_{\mu_d}\right)\right)$: 난수치,

$\delta_1,\ldots,\delta_d,\zeta$: 난수치

이다.

[수학식 33]

$$k^*_{L,\mathrm{dec}} := \sum_{t=1}^{L} \sigma_{0,t} \left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b^*_i \right) + b^*_{n+1} + \sum_{h=1}^{r} \eta_{0,h} b^*_{n+2+h}$$

여기서,

$\sigma_{0,i}, \eta_{0,h} \quad (i = 1,\ldots,L;\ h = 1,\ldots,r)$: 난수치,

$v_i \quad (i = 1,\ldots,\mu_L)$: 술어 정보,

r : 1 이상의 정수로서, $n+2 = R,\ n+2+r = S$

이다.

[수학식 34]

$$e\left(c_1, k^*_{L,\mathrm{dec}}\right)$$

여기서,
$e(p,q) := \prod_{i=1}^{N} e(\chi_i b_i, \eta_i b_i^*)$,
$p := \sum_{i=1}^{N} \chi_i b_i$,
$q := \sum_{i=1}^{N} \eta_i b_i^*$,
χ_i, η_i : 계수
이다.

청구항 26

제 24 항에 있어서,

상기 벡터 입력부는, 수학식 35에 나타내는 암호 벡터 c_1을 입력하고,

상기 키 벡터 기억부는, 수학식 36에 나타내는 키 벡터 $k^*_{L,\,dec}$를 기억하고,

상기 페어링 연산부는, 수학식 37에 나타내는 페어링 연산을 행하고, 상기 암호 벡터로부터 상기 소정의 정보에 관한 값을 추출하는

것을 특징으로 하는 복호 장치.

[수학식 35]

$$c_1 := \sum_{t=1}^{h} \delta_t \left(\sum_{i=1}^{n} x_{t,i} b_i \right) + \zeta b_{n+1}$$

여기서,
$\left(\vec{x}_1, \ldots, \vec{x}_h\right) := \left(\left(x_{1,1}, \ldots, x_{1,n}\right), \ldots, \left(x_{h,1}, \ldots, x_{h,n}\right)\right)$: 속성 정보,
$\delta_1, \ldots, \delta_d, \zeta$: 난수치
이다.

[수학식 36]

$$k^*_{L,\mathrm{dec}} := \sum_{t=1}^{L} \sigma_{\mathrm{dec},t} \left(\sum_{i=1}^{n} v_{t,i} b_i^* \right) + b^*_{n+1} + \sum_{h=1}^{r} \eta_{\mathrm{dec},h} b^*_{n+2+h}$$

여기서,
$\sigma_{\mathrm{dec},t}, \eta_{\mathrm{dec},h} \quad (t = 1, \ldots, L;\ h = 1, \ldots, r)$: 난수치,
$v_{t,i} \quad (t = 1, \ldots, L; i = 1, \ldots, n)$: 술어 정보,
r : 1 이상의 정수로서, $n + 2 = R$, $n + 2 + r = S$
이다.

[수학식 37]

$$e\left(c_1, k^*_{L,\mathrm{dec}}\right)$$

여기서,
$e(p,q) := \prod_{i=1}^{N} e(\chi_i b_i, \eta_i b_i^*)$,
$p := \sum_{i=1}^{N} \chi_i b_i$,
$q := \sum_{i=1}^{N} \eta_i b_i^*$,
χ_i, η_i : 계수
이다.

청구항 27

제 24 항에 있어서,

상기 벡터 입력부는, 수학식 38에 나타내는 암호 벡터 c_1과, 평문 정보 $\mathbb{m}$을 암호화한 수학식 39에 나타내는 암호 정보 c_2를 입력하고,

상기 키 벡터 기억부는, 수학식 40에 나타내는 키 벡터 $k^*_{L,\,dec}$를 기억하고,

상기 페어링 연산부는, 수학식 41에 나타내는 연산을 행하고, 상기 암호 벡터 c_1로부터 상기 평문 정보 $\mathbb{m}$을 추출하는

것을 특징으로 하는 복호 장치.

[수학식 38]

$$c_1 := \sum_{t=1}^{d} \delta_t \left(\sum_{i=\mu_{t-1}+1}^{\mu_t} x_i b_i \right) + \zeta b_{n+1}$$

여기서,
$\left(\vec{x}_1,\ldots,\vec{x}_h\right) := \left(\left(x_1,\ldots,x_{\mu_1}\right),\ldots,\left(x_{\mu_{L-1}+1},\ldots,x_{\mu_h}\right)\right)$: 속성 정보,
$\left(\vec{x}_{h+1},\ldots,\vec{x}_d\right) := \left(\left(x_{\mu_{h+1}+1},\ldots,x_{\mu_{h+2}}\right),\ldots,\left(x_{\mu_{d-1}+1},\ldots,x_{\mu_d}\right)\right)$: 난수치,
$\delta_1,\ldots,\delta_d,\zeta$: 난수치
이다.

[수학식 39]

$$c_2 := g_T^{\zeta} m$$

여기서,
$g_T = e(a_i, a_i^*) \neq 1$,
$\mathbb{A}$는 공간 $\mathbb{V}$의 기저로서, $\mathbb{A} := \left(a_1,\ldots,a_N\right)$,
$\mathbb{A}^*$는 공간 $\mathbb{V}^*$의 기저로서, $\mathbb{A}^* := \left(a_1^*,\ldots,a_N^*\right)$
이다.

[수학식 40]

$$k^*_{L,\mathrm{dec}} := \sum_{t=1}^{L} \sigma_{0,t} \left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b_i^* \right) + b^*_{n+1} + \sum_{h=1}^{r} \eta_{0,h} b^*_{n+2+h}$$

여기서,
$\sigma_{0,i}, \eta_{0,h} \quad (i = 1,\ldots,L;\ h = 1,\ldots,r)$: 난수치,

$v_i \quad (i = 1,\ldots,\mu_L)$: 술어 정보,

r : 1 이상의 정수로서, $n+2 = R,\ n+2+r = S$
이다.

[수학식 41]

$$m := c_2 / e\left(c_1, k^*_{L,\mathrm{dec}}\right)$$

여기서,
$e(p,q) := \prod_{i=1}^{N} e(\chi_i b_i, \eta_i b_i^*)$,

$p := \sum_{i=1}^{N} \chi_i b_i$,

$q := \sum_{i=1}^{N} \eta_i b_i^*$,

χ_i, η_i : 계수
이다.

청구항 28

제 24 항에 있어서,

상기 벡터 입력부는, 수학식 42에 나타내는 암호 벡터 c_1과, 평문 정보 m을 암호화한 수학식 43에 나타내는 암호 정보 c_2를 입력하고,

상기 키 벡터 기억부는, 수학식 44에 나타내는 키 벡터 $k^*_{L,\,dec}$를 기억하고,

상기 페어링 연산부는, 수학식 45에 나타내는 연산을 행하고, 상기 암호 벡터 c_1로부터 상기 평문 정보 m을 추출하는

것을 특징으로 하는 복호 장치.

[수학식 42]

$$c_1 := \sum_{t=1}^{h} \delta_t \left(\sum_{i=1}^{n} x_{t,i} b_i \right) + \zeta b_{n+1}$$

여기서,
$\left(\vec{x}_1,\ldots,\vec{x}_h\right) := \left(\left(x_{1,1},\ldots,x_{1,n}\right),\ldots,\left(x_{h,1},\ldots,x_{h,n}\right) \right)$: 속성 정보,

$\delta_1,\ldots,\delta_d,\zeta$: 난수치
이다.

[수학식 43]

$$c_2 := g_T^{\xi} m$$

여기서,
$g_T = e(a_i, a_i^*) \neq 1$,
$\mathbb{A}$는 공간 $\mathbb{V}$의 기저로서, $\mathbb{A} := (a_1, ..., a_N)$,
$\mathbb{A}^*$는 공간 $\mathbb{V}^*$의 기저로서, $\mathbb{A}^* := (a_1^*, ..., a_N^*)$
이다.

[수학식 44]

$$k_{L,\mathrm{dec}}^* := \sum_{t=1}^{L} \sigma_{\mathrm{dec},t} \left(\sum_{i=1}^{n} v_{t,i} b_i^* \right) + b_{n+1}^* + \sum_{h=1}^{r} \eta_{\mathrm{dec},h} b_{n+2+h}^*$$

여기서,
$\sigma_{\mathrm{dec},t}, \eta_{\mathrm{dec},h} \quad (t = 1, \ldots, L;\ h = 1, ..., r)$: 난수치,
$v_{t,i} \quad (t = 1, ..., L; i = 1, ..., n)$: 술어 정보,
r : 1이상의 정수로서, $n + 2 = R,\ n + 2 + r = S$
이다.

[수학식 45]

$$m := c_2 / e\left(c_1, k_{L,\mathrm{dec}}^*\right)$$

여기서,
$e(p,q) := \prod_{i=1}^{N} e(\chi_i b_i, \eta_i b_i^*)$,
$p := \sum_{i=1}^{N} \chi_i b_i$,
$q := \sum_{i=1}^{N} \eta_i b_i^*$,
χ_i, η_i : 계수
이다.

청구항 29

수학식 46에 나타내는 페어링 연산에 의해 관련지어진 쌍대 가군(dual modules)인 공간 V와 공간 V^*를 이용하여 술어 암호 처리를 행하는 암호 처리 시스템으로서,

상기 공간 V에 있어서의 소정의 기저 B를 구성하는 기저 벡터 b_i(i=1, …, n, …, S, …, N)(N은 3 이상의 정수, S는 n+1 이상 N-1 이하의 정수, n은 1 이상 N-2 이하의 정수) 중 기저 벡터 b_i(i=S+1, …, N)를 제외한 적어도 기저 벡터 b_i(i=1, …, n+1)를 갖는 기저 B^와, 소정의 속성 정보가 공개 키로서 주어지고, 상기 기저 B^의 기저 벡터 b_i(i=1, …, n) 중 적어도 일부의 기저 벡터에 대한 계수로서 속성 정보를 설정함과 아울러, 상기 기저 벡터 b_{n+1}에 대한 계수로서 소정의 정보를 설정한 벡터를 암호 벡터 c_1로서 처리 장치에 의해 생성하는 암호화 장치와,

상기 공간 V^*의 기저 B^*에 있어서의 벡터로서, 기저 B^*를 구성하는 기저 벡터 b^*_i(i=1, …, n, …, S, …, N)의 기저 벡터 b^*_i(i=1, …, n) 중 적어도 일부의 기저 벡터에 대한 계수로서 술어 정보를 설정함과 아울러, 상기 기저 B^*의 기저 벡터 b^*_{n+1}에 대한 계수로서 소정의 값을 설정한 벡터를 키 벡터 $k^*_{L,\,dec}$로 하여, 상기 암호화 장치가 생성한 암호 벡터 c_1과 상기 키 벡터 $k^*_{L,\,dec}$에 대하여, 처리 장치에 의해 수학식 46에 나타내는 페어링 연산

$e(c_1, k^*_{L, dec})$를 행하여 상기 암호 벡터 c_1을 복호하여 상기 소정의 정보에 관한 값을 추출하는 복호 장치

를 구비하는 것을 특징으로 하는 암호 처리 시스템.

[수학식 46]

$$e(p,q) := \prod_{i=1}^{N} e(\chi_i b_i, \eta_i b_i^*)$$

여기서,

$p := \sum_{i=1}^{N} \chi_i b_i$,

$q := \sum_{i=1}^{N} \eta_i b_i^*$,

χ_i, η_i : 계수

이다.

청구항 30

술어 암호에 있어서의 비밀 키인 키 벡터 $k^*_{L, dec}$를 생성하고, 수학식 47에 나타내는 페어링 연산에 의해 관련지어진 쌍대 가군인 공간 V와 공간 V^* 중 상기 공간 V에 있어서의 소정의 기저 B를 구성하는 기저 벡터 b_i(i=1, …, n, …, S, …, N)(N은 3 이상의 정수, S는 n+1 이상 N-1 이하의 정수, n은 1 이상 N-2 이하의 정수) 중 기저 벡터 b_i(i=S+1, …, N)를 제외한 적어도 기저 벡터 b_i(i=1, …, n+1)를 갖는 기저 B^가 공개 키로서 주어진 경우에 있어서의 비밀 키인 키 벡터 $k^*_{L, dec}$를 생성하는 키 생성 장치로서,

상기 공간 V^*에 있어서의 소정의 기저 B^*를 기억 장치에 기억하는 마스터 키 기억부와,

상기 마스터 키 기억부가 기억한 상기 기저 B^*를 구성하는 기저 벡터 b^*_i(i=1, …, n, …, S, …, N) 중, 기저 벡터 b^*_i(i=1, …, n)의 적어도 일부의 기저 벡터 b^*_i(i=1, …, μ_L)에 대한 계수로서 술어 정보를 설정함과 아울러, 기저 벡터 b^*_{n+1}에 대한 계수로서 소정의 값을 설정한 벡터를 키 벡터 $k^*_{L, dec}$로서 처리 장치에 의해 생성하는 키 벡터 생성부

를 구비하는 것을 특징으로 하는 키 생성 장치.

[수학식 47]

$$e(p,q) := \prod_{i=1}^{N} e(\chi_i b_i, \eta_i b_i^*)$$

여기서,

$p := \sum_{i=1}^{N} \chi_i b_i$,

$q := \sum_{i=1}^{N} \eta_i b_i^*$,

χ_i, η_i : 계수

이다.

청구항 31

술어 암호에 있어서의 비밀 키인 키 벡터 $k^*_{L, dec}$로 복호 가능한 암호 벡터 중 일부의 암호 벡터를 복호 가능한 키 벡터 $k^*_{L+1, dec}$를 생성하는 키 위양 장치로서, 수학식 48에 나타내는 페어링 연산에 의해 관련지어진 쌍대 가군인 공간 V와 공간 V^* 중 상기 공간 V에 있어서의 소정의 기저 B를 구성하는 기저 벡터 b_i(i=1, …, n, …, R,

…, S, …, N)(N은 4 이상의 정수, S는 n+2 이상 N-1 이하의 정수, R은 n+1 이상 S-1 이하의 정수, n은 1 이상 N-3 이하의 정수) 중 기저 벡터 b_i(i=S+1, …, N)를 제외한 적어도 기저 벡터 b_i(i=1, …, n+1)를 갖는 기저 B^가 공개 키로서 주어잔 경우에 있어서의 비밀 키인 키 벡터 $k^*_{L+1,\,dec}$를 생성하는 상기 키 위양 장치로서,

상기 기저 B^*를 구성하는 기저 벡터 b^*_i(i=1, …, n, …, R, …, S, …, N) 중, 기저 벡터 b^*_i(i=1, …, n)의 적어도 일부의 기저 벡터 b^*_i(i=1, …, μ_L)에 대한 계수로서 술어 정보가 설정되고, 기저 벡터 b^*_{n+1}에 대한 계수로서 소정의 값이 설정되고, 기저 벡터 b^*_i(i=R+1, …, S)에 대한 계수로서 난수치가 설정된 키 벡터 $k^*_{L,\,dec}$를 취득하는 키 벡터 취득부와,

적어도 j=μ_L+1, …, n의 각 j에 대하여, 기저 벡터 b^*_j에 대한 계수로서 난수치가 설정되는 것과 아울러, 기저 벡터 b^*_i(i=R+1, …, S)에 대한 계수로서 난수치가 설정된 적어도 n-μ_L개의 키 생성용 벡터 $k^*_{L,\,del,\,j}$를 취득하는 키 생성용 벡터 취득부와,

상기 키 생성용 벡터 취득부가 취득한 상기 키 생성용 벡터 $k^*_{L,\,del,\,j}$의 적어도 일부의 상기 키 생성용 벡터 $k^*_{L,\,del,\,j}$의 각 기저 벡터의 계수를 술어 정보로 승산하고, 상기 키 벡터 취득부가 취득한 상기 키 벡터 $k^*_{L,\,dec}$에 가산하여 키 벡터 $k^*_{L+1,\,dec}$를 생성하는 키 벡터 생성부

를 구비하는 것을 특징으로 하는 키 위양 장치.

[수학식 48]

$$e(p,q) := \prod_{i=1}^{N} e(\chi_i b_i, \eta_i b_i^*)$$

여기서,

$p := \sum_{i=1}^{N} \chi_i b_i$,

$q := \sum_{i=1}^{N} \eta_i b_i^*$,

χ_i, η_i : 계수

이다.

청구항 32

페어링 연산에 의해 관련지어진 쌍대 가군인 공간 V와 공간 V^*에 있어서 실현되는 술어 암호 처리에 있어서의 암호문인 암호 벡터 c_1을 생성하는 암호화 장치로서,

상기 공간 V에 있어서의 소정의 기저 B를 구성하는 기저 벡터 b_i(i=1, …, n, …, S, …, N)(N은 3 이상의 정수, S는 n+1 이상 N-1 이하의 정수, n은 1 이상 N-2 이하의 정수) 중 기저 벡터 b_i(i=S+1, …, N)를 제외한 적어도 기저 벡터 b_i(i=1, …, n+1)를 갖는 기저 B^를 취득함과 아울러, 소정의 속성 정보를 취득하는 공개 키 취득부와,

상기 공개 키 취득부가 취득한 기저 B^에 있어서의 벡터로서, 기저 벡터 b_{n+1}에 대한 계수로서 소정의 정보를 설정한 벡터를 송신 정보 벡터 ζ_v로서 처리 장치에 의해 생성하는 송신 정보 설정부와,

상기 기저 B^의 상기 기저 벡터 b_i(i=1, …, n) 중 적어도 일부의 기저 벡터에 대한 계수로서 상기 속성 정보를 설정한 속성 정보 벡터를, 상기 송신 정보 설정부가 생성한 송신 정보 벡터 ζ_v에 가산하여 암호 벡터 c_1을 처리 장치에 의해 생성하는 암호 벡터 생성부

를 구비하는 것을 특징으로 하는 암호화 장치.

청구항 33

수학식 49에 나타내는 페어링 연산에 의해 관련지어진 쌍대 가군인 공간 V와 공간 V^*에 있어서 실현되는 술어 암호 처리에 있어서의 암호문을 복호하는 복호 장치로서,

상기 공간 V에 있어서의 소정의 기저 B를 구성하는 기저 벡터 b_i(i=1, …, n, …, S, …, N)(N은 3 이상의 정수, S는 n+1 이상 N-1 이하의 정수, n은 1 이상 N-2 이하의 정수) 중 기저 벡터 b_i(i=S+1, …, N)를 제외한 적어도 기저 벡터 b_i(i=1, …, n+1)를 갖는 기저 B^가 공개 키로서 주어진 경우에 생성되는 암호문인 암호 벡터 c_1로서, 상기 기저 B^의 기저 벡터 b_i(i=1, …, n) 중 적어도 기저 벡터 b_i(i=1, …, μ_h)에 대한 계수로서 속성 정보가 설정되는 것과 아울러, 상기 기저 벡터 b_{n+1}에 대한 계수로서 소정의 정보가 설정된 벡터인 암호 벡터 c_1을 입력하는 벡터 입력부와,

상기 공간 V^*에 있어서의 소정의 기저 B^*의 기저 벡터 b^*_i(i=1, …, n, …, S, …, N) 중, 기저 벡터 b^*_i(i=1, …, n)의 적어도 기저 벡터 b^*_i(i=1, …, μ_L)($\mu_L \leq \mu_h$)에 대한 계수로서 술어 정보 v_i(i=1, …, μ_L)가 설정되고, 기저 벡터 b^*_{n+1}에 대한 계수로서 소정의 값이 설정된 키 벡터 $k^*_{L,\,dec}$를 기억 장치에 기억하는 키 벡터 기억부와,

상기 벡터 입력부가 입력한 암호 벡터 c_1과, 상기 키 벡터 기억부가 기억한 키 벡터 $k^*_{L,\,dec}$에 대하여 처리 장치에 의해 수학식 49에 나타내는 페어링 연산을 행하고, 상기 암호 벡터 c_1로부터 상기 소정의 정보에 관한 값을 추출하는 페어링 연산부

를 구비하는 것을 특징으로 하는 복호 장치.

[수학식 49]

$$e(p,q) := \prod_{i=1}^{N} e(\chi_i b_i, \eta_i b_i^*)$$

여기서,

$p := \sum_{i=1}^{N} \chi_i b_i$,

$q := \sum_{i=1}^{N} \eta_i b_i^*$,

χ_i, η_i : 계수

이다.

청구항 34

수학식 50에 나타내는 페어링 연산에 의해 관련지어진 쌍대 벡터 공간인 공간 V와 공간 V^*를 이용하여 술어 암호 처리를 행하는 암호 처리 방법으로서,

처리 장치가, 상기 공간 V에 있어서의 소정의 기저 B를 구성하는 기저 벡터 b_i(i=1, …, n, …, S, …, N)(N은 3 이상의 정수, S는 n+1 이상 N-1 이하의 정수, n은 1 이상 N-2 이하의 정수) 중 기저 벡터 b_i(i=S+1, …, N)를 제외한 적어도 기저 벡터 b_i(i=1, …, n+1)를 갖는 기저 B^와, 소정의 속성 정보가 공개 키로서 주어지고, 상기 기저 B^의 기저 벡터 b_i(i=1, …, n) 중 적어도 일부의 기저 벡터에 대한 계수로서 속성 정보를 설정함과 아울러, 상기 기저 벡터 b_{n+1}에 대한 계수로서 소정의 정보를 설정한 벡터를 암호 벡터 c_1로서 생성하는 암호화 단계와,

처리 장치가, 상기 공간 V^*의 기저 B^*에 있어서의 벡터로서, 기저 B^*를 구성하는 기저 벡터 b^*_i(i=1, …, n, …,

S, …, N)의 기저 벡터 b^*_i(i=1, …, n) 중 적어도 일부의 기저 벡터에 대한 계수로서 술어 정보를 설정함과 아울러, 상기 기저 B^*의 기저 벡터 b^*_{n+1}에 대한 계수로서 소정의 값을 설정한 벡터를 키 벡터 $k^*_{L,\,dec}$로 하여, 상기 암호 벡터 c_1과 상기 키 벡터 $k^*_{L,\,dec}$에 대하여, 수학식 50에 나타내는 페어링 연산 $e(c_1, k^*_{L,\,dec})$를 행하여 상기 암호 벡터 c_1을 복호하여 상기 소정의 정보에 관한 값을 추출하는 복호 단계

를 구비하는 것을 특징으로 하는 암호 처리 방법.

[수학식 50]

$$e(p,q) := \prod_{i=1}^{N} e(\chi_i b_i, \eta_i b_i^*)$$

여기서,

$p := \sum_{i=1}^{N} \chi_i b_i$,

$q := \sum_{i=1}^{N} \eta_i b_i^*$,

χ_i, η_i : 계수

이다.

청구항 35

수학식 51에 나타내는 페어링 연산에 의해 관련지어진 쌍대 벡터 공간인 공간 V와 공간 V^*를 이용하여 술어 암호 처리를 행하는 암호 처리 프로그램을 기록한 컴퓨터 판독 가능한 기록 매체로서,

처리 장치가, 상기 공간 V에 있어서의 소정의 기저 B를 구성하는 기저 벡터 b_i(i=1, …, n, …, S, …, N)(N은 3 이상의 정수, S는 n+1 이상 N-1 이하의 정수, n은 1 이상 N-2 이하의 정수) 중 기저 벡터 b_i(i=S+1, …, N)를 제외한 적어도 기저 벡터 b_i(i=1, …, n+1)를 갖는 기저 B^와, 소정의 속성 정보가 공개 키로서 주어지고, 상기 기저 B^의 기저 벡터 b_i(i=1, …, n) 중 적어도 일부의 기저 벡터에 대한 계수로서 속성 정보를 설정함과 아울러, 상기 기저 벡터 b_{n+1}에 대한 계수로서 소정의 정보를 설정한 벡터를 암호 벡터 c_1로서 생성하는 암호화 처리와,

처리 장치가, 상기 공간 V^*의 기저 B*에 있어서의 벡터로서, 기저 B^*를 구성하는 기저 벡터 b^*_i(i=1, …, n, …, S, …, N)의 기저 벡터 b^*_i(i=1, …, n) 중 적어도 일부의 기저 벡터에 대한 계수로서 술어 정보를 설정함과 아울러, 상기 기저 B^*의 기저 벡터 b^*_{n+1}에 대한 계수로서 소정의 값을 설정한 벡터를 키 벡터 $k^*_{L,\,dec}$로 하여, 상기 암호화 장치가 생성한 암호 벡터 c_1과 상기 키 벡터 $k^*_{L,\,dec}$에 대하여, 수학식 51에 나타내는 페어링 연산 $e(c_1, k^*_{L,\,dec})$를 행하여 상기 암호 벡터 c_1을 복호하여 상기 소정의 정보에 관한 값을 추출하는 복호 처리

를 구비하는 것을 특징으로 하는 암호 처리 프로그램을 기록한 컴퓨터 판독 가능한 기록 매체.

[수학식 51]

$$e(p,q) := \prod_{i=1}^{N} e(\chi_i b_i, \eta_i b_i^*)$$

여기서,

$p := \sum_{i=1}^{N} \chi_i b_i$,

$q := \sum_{i=1}^{N} \eta_i b_i^*$,

χ_i, η_i : 계수

이다.

명 세 서

기 술 분 야

[0001] 본 발명은, 계층적 술어 키 비닉 방식 및 계층적 술어 암호에 관한 것이다.

배 경 기 술

[0002] 비특허 문헌 18에는, 페어링 연산에 의해 관련지어진 쌍대 공간에 있어서 계층적 술어 키 비닉 방식 및 계층적 술어 암호를 실현하는 것이 기재되어 있다.

[0003] (선행 기술 문헌)

[0004] (비특허 문헌)

[0005] (비특허 문헌 1) Bethencourt, J., Sahai, A., Waters, B. : Ciphertext-policy attribute-based encryption. In : 2007 IEEE Symposium on Security and Privacy, pp. 321--334. IEEE Press(2007)

[0006] (비특허 문헌 2) Boneh, D., Boyen, X. : Efficient selective-ID secure identity based encryption without random oracles. In : Cachin, C., Camenisch, J.(eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223--238. Springer Heidelberg(2004)

[0007] (비특허 문헌 3) Boneh, D., Boyen, X. : Secure identity based encryption without random oracles. In : Franklin, M. K.(ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 443--459. Springer Heidelberg(2004)

[0008] (비특허 문헌 4) Boneh, D., Boyen, X., Goh, E. : Hierarchical identity based encryption with constant size ciphertext. In: Cramer, R.(ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 440--456. Springer Heidelberg(2005)

[0009] (비특허 문헌 5) Boneh, D., Franklin, M. : Identity-based encryption from the Weil pairing. In : Kilian, J.(ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213--229. Springer Heidelberg(2001)

[0010] (비특허 문헌 6) Boneh, D., Hamburg, M. : Generalized identity based and broadcast encryption scheme. In : Pieprzyk, J.(ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 455--470. Springer Heidelberg(2008)

[0011] (비특허 문헌 7) Boneh, D., Waters, B. : Conjunctive, subset, and range queries on encrypted data. In : Vadhan, S. P.(ed.) TCC 2007. LNCS, vol. 4392, pp. 535--554. Springer Heidelberg(2007)

[0012] (비특허 문헌 8) Boyen, X., Waters, B. : Anonymous hierarchical identity-based encryption(without random oracles). In : Dwork, C.(ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 290--307. Springer Heidelberg(2006)

[0013] (비특허 문헌 9) Cocks, C. : An identity based encryption scheme based on quadratic residues. In : Honary, B.(ed.) IMA Int. Conf. LNCS, vol. 2260, pp. 360--363. Springer Heidelberg(2001)

[0014] (비특허 문헌 10) Gentry, C. : Practical identity-based encryption without random oracles. In : Vaudenay, S.(ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 445--464. Springer Heidelberg(2006)

[0015] (비특허 문헌 11) Gentry, C., Halevi, S. : Hierarchical identity-based encryption with polynomially many levels. In : Reingold, O.(ed.) TCC 2009. LNCS, vol. 5444, pp. 437--456. Springer Heidelberg(2009)

[0016] (비특허 문헌 12) Gentry, C., Silverberg, A. : Hierarchical ID-based cryptography. In : Zheng, Y.(ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 548--566. Springer Heidelberg(2002)

[0017] (비특허 문헌 13) Goyal, V., Pandey, O., Sahai, A., Waters, B. : Attribute-based encryption for fine-grained access control of encrypted data. In : ACM Conference on Computer and Communication Security 2006, pp. 89--98, ACM(2006)

[0018] (비특허 문헌 14) Groth, J., Sahai, A. : Efficient non-interactive proof systems for bilinear groups. In : Smart, N. P.(ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 415--432. Springer Heidelberg(2008)

[0019] (비특허 문헌 15) Horwitz, J., Lynn, B. : Towards hierarchical identity-based encryption. In : Knudsen, L. R.(ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 466--481. Springer Heidelberg(2002)

[0020] (비특허 문헌 16) Katz, J., Sahai, A., Waters, B. : Predicate encryption supporting disjunctions, polynomial equations, and inner products. In : Smart, N. P.(ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 146--162. Springer Heidelberg(2008)

[0021] (비특허 문헌 17) Okamoto, T., Takashima, K. : Homomorphic encryption and signatures from vector decomposition. In : Galbraith, S. D., Paterson, K. G.(eds.) Pairing 2008. LNCS, vol. 5209, pp. 57--74. Springer Heidelberg(2008)

[0022] (비특허 문헌 18) Okamoto, T., Takashima, K. : A geometric approach on pairings and hierarchical predicate encryption. In : Poster session, EUROCRYPT 2009.(2009)

[0023] (비특허 문헌 19) Ostrovsky, R., Sahai, A., Waters, B. : Attribute-based encryption with non-monotonic access structures. In : ACM Conference on Computer and Communication Security 2007, pp. 195--203, ACM(2007)

[0024] (비특허 문헌 20) Pirretti, M., Traynor, P., McDaniel, P., Waters, B. : Secure attribute-based systems. In : ACM Conference on Computer and Communication Security 2006, pp. 99--112, ACM(2006)

[0025] (비특허 문헌 21) Sahai, A., Waters, B. : Fuzzy identity-based encryption. In : Cramer, R.(ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457--473. Springer Heidelberg(2005)

[0026] (비특허 문헌 22) Shi, E., Waters, B. : Delegating capability in predicate encryption systems. In : Aceto, L., Damgard, I., Goldberg, L. A., Halldorsson, M. M., Ingolfsdottir, A., Walukiewicz, I.(eds.) ICALP(2) 2008. LNCS, vol. 5126, pp. 560--578. Springer Heidelberg(2008)

[0027] (비특허 문헌 23) Takashima, K. : Efficiently computable distortion maps for super singular curves. In : van der Poorten, A. J., Stein, A.(eds.) ANTS VIII, LNCS, vol. 5011, pp. 88--101. Springer Heidelberg(2008)

[0028] (비특허 문헌 24) Waters, B. : Ciphertext-policy attribute-based encryption : an expressive, efficient, and provably secure realization. ePrint, IACR, http://eprint.iacr.org/2008/290

[0029] (비특허 문헌 25) T. Okamoto and K. Takashima, "Hierarchical predicate encryption for inner-products", Asiacrypt 2009, LNCS vol. 5912, pp. 214-231. Springer Heidelberg(2009)

[0030] (비특허 문헌 26) B. Waters, "Dual system encryption : Realizing fully secure IBE and HIBE under simple assumptions", CRYPTO 2009, LNCS vol. 5677, pp. 619-636. Springer Heidelberg(2009)

[0031] (비특허 문헌 27) A. Lewko and B. Waters, "New techniques for dual system encryption and fully secure HIBE with short ciphertexts", ePrint, IACR, http://eprint.iacr.org/2009/482

발명의 내용

해결하려는 과제

[0032] 비특허 문헌 18에서 제안되어 있는 계층적 술어 키 비닉 방식 및 계층적 술어 암호는, 이상화된 모델(Generic Model)에 있어서의 안전성이 증명되어 있다. 그러나, 비특허 문헌 18에서 제안되어 있는 계층적 술어 키 비닉 방식 및 계층적 술어 암호는, 표준의 모델(Standard Model)에 있어서의 안전성은 증명되어 있지 않다.

[0033] 본 발명은, 안전성이 높은 술어 암호 및 술어 키 비닉 방식을 제공하는 것을 목적으로 한다. 특히, 권한 위양을 가능하게 한 술어 암호 및 술어 키 비닉 방식을 제공하는 것을 목적으로 한다.

과제의 해결 수단

[0034] 본 발명에 따른 암호 처리 시스템은, 예컨대, 수학식 1에 나타내는 페어링 연산에 의해 관련지어진 쌍대 벡터 공간인 공간 V와 공간 V^*를 이용하여 술어 암호 처리를 행하는 암호 처리 시스템이며, 상기 공간 V에 있어서의 소정의 기저 B를 구성하는 기저 벡터 b_i(i=1, …, n, …, S, …, N)(N은 3 이상의 정수, S는 n+1 이상 N-1 이하의 정수, n은 1 이상 N-2 이하의 정수) 중 기저 벡터 b_i(i=S+1, …, N)를 제외한 적어도 기저 벡터 b_i(i=1, …, n+1)를 갖는 기저 B^와, 소정의 속성 정보가 공개 키로서 주어지고, 상기 기저 B^의 기저 벡터 b_i(i=1, …, n) 중 적어도 일부의 기저 벡터에 대한 계수로서 속성 정보를 설정함과 아울러, 상기 기저 벡터 b_{n+1}에 대한 계수로서 소정의 정보를 설정한 벡터를 암호 벡터 c_1로서 처리 장치에 의해 생성하는 암호화 장치와, 상기 공간 V^*의 기저 B^*에 있어서의 벡터로서, 기저 B^*를 구성하는 기저 벡터 b^*_i(i=1, …, n, …, S, …, N)의 기저 벡터 b^*_i(i=1, …, n) 중 적어도 일부의 기저 벡터에 대한 계수로서 술어 정보를 설정함과 아울러, 상기 기저 B^*의 기저 벡터 b^*_{n+1}에 대한 계수로서 소정의 값을 설정한 벡터를 키 벡터 $k^*_{L,\,dec}$로 하여, 상기 암호화 장치가 생성한 암호 벡터 c_1과 상기 키 벡터 $k^*_{L,\,dec}$에 대하여, 처리 장치에 의해 수학식 1에 나타내는 페어링 연산 $e(c_1, k^*_{L,\,dec})$를 행하여 상기 암호 벡터 c_1을 복호하여 상기 소정의 정보에 관한 값을 추출하는 복호 장치를 구비하는 것을 특징으로 한다.

[0035] [수학식 1]

$$e(p,q) := \prod_{i=1}^{N} e(\chi_i b_i, \eta_i b_i^*)$$

여기서,

$$p := \sum_{i=1}^{N} \chi_i b_i ,$$

$$q := \sum_{i=1}^{N} \eta_i b_i^* ,$$

χ_i, η_i : 계수

[0036] 이다.

발명의 효과

[0037] 본 발명에 따른 암호 시스템에 의하면, 안전성이 높은 술어 암호 및 술어 키 비닉 방식을 실현할 수 있다.

도면의 간단한 설명

[0038] 도 1은 「권한 위양(계층적인 권한 위양)」이라고 하는 개념을 설명하기 위한 도면.

도 2는 계층을 도외시한 권한 위양을 설명하기 위한 도면.

도 3은 속성 정보와 술어 정보의 계층 구조를 나타내는 도면.

도 4는 계층적 내적 술어 암호의 응용예인 계층적 ID 베이스 암호의 예를 나타내는 도면.

도 5는 기저와 기저 벡터를 설명하기 위한 도면.

도 6은 벡터 공간에 있어서의 계층 구조의 실현 방법의 일례를 설명하기 위한 도면.

도 7은 암호 처리 시스템(10)의 구성도.

도 8은 암호 처리 시스템(10)의 키 생성 장치(100)와 제 L 층째의 암호화 장치(200)와 복호 장치(300)의 동작을 나타내는 플로우차트.

도 9는 암호 처리 시스템(10)의 제 L 층째의 키 위양 장치(400)와 제 L+1 층째의 암호화 장치(200)와 복호 장치(300)의 동작을 나타내는 플로우차트.

도 10은 기저 변환 방법을 설명하기 위한 도면.

도 11은 실시의 형태 2에 따른 계층적 술어 암호를 실현하는 암호 처리 시스템(10)의 기능을 나타내는 기능 블록도.

도 12는 실시의 형태 2에 따른 키 생성 장치(100)의 동작을 나타내는 플로우차트.

도 13은 실시의 형태 2에 따른 암호화 장치(200)의 동작을 나타내는 플로우차트.

도 14는 실시의 형태 2에 따른 복호 장치(300)의 동작을 나타내는 플로우차트.

도 15는 실시의 형태 2에 따른 키 위양 장치(400)의 동작을 나타내는 플로우차트.

도 16은 실시의 형태 2에 따른 쌍대 페어링 벡터 공간의 기저의 구조를 나타내는 개념도.

도 17은 실시의 형태 2에 따른 계층적 술어 키 비닉 방식을 실현하는 암호 처리 시스템(10)의 기능을 나타내는 기능 블록도.

도 18은 실시의 형태 2에 따른 암호화 장치(200)의 동작을 나타내는 플로우차트.

도 19는 실시의 형태 2에 따른 복호 장치(300)의 동작을 나타내는 플로우차트.

도 20은 실시의 형태 3에 따른 권한 위양이 가능한 술어 암호를 실현하는 암호 처리 시스템(10)의 기능을 나타내는 기능 블록도.

도 21은 키 생성 장치(100), 암호화 장치(200), 복호 장치(300), 키 위양 장치(400)의 하드웨어 구성의 일례를 나타내는 도면.

발명을 실시하기 위한 구체적인 내용

[0039] 이하, 도면에 근거하여, 발명의 실시의 형태를 설명한다.

[0040] 이하의 설명에 있어서, 처리 장치는 후술하는 CPU(911) 등이다. 기억 장치는 후술하는 ROM(913), RAM(914), 자기 디스크(920) 등이다. 통신 장치는 후술하는 통신 보드(915) 등이다. 입력 장치는 후술하는 키보드(902), 통신 보드(915) 등이다. 출력 장치는 후술하는 RAM(914), 자기 디스크(920), 통신 보드(915), LCD(901) 등이다. 다시 말해, 처리 장치, 기억 장치, 통신 장치, 입력 장치, 출력 장치는 하드웨어이다.

[0041] 이하의 설명에 있어서의 기법(記法)에 대하여 설명한다.

[0042] A가 랜덤 변수 또는 분포일 때, 수학식 101은, A의 분포에 따라 A로부터 y를 랜덤 선택하는 것을 나타낸다. 다시 말해, 수학식 101에 있어서, y는 난수이다.

[0043] [수학식 101]

[0044] $$y \xleftarrow{R} A$$

[0045] A가 집합일 때, 수학식 102는, A로부터 y를 균등하게 선택하는 것을 나타낸다. 다시 말해, 수학식 102에 있어서, y는 균등 난수이다.

[0046] [수학식 102]

[0047] $$y \xleftarrow{U} A$$

[0048] 수학식 103은, y가 z에 의해 정의된 집합인 것, 또는 y가 z가 대입된 집합인 것을 나타낸다.

[0049] [수학식 103]

[0050] $$y := z$$

[0051] a가 상수일 때, 수학식 104는, 기계(알고리즘) A가 입력 x에 대하여 a를 출력하는 것을 나타낸다.

[0052] [수학식 104]

$$A(x) \rightarrow a$$

예컨대,

[0053] $$A(x) \rightarrow 1$$

[0054] 벡터 표기는, 유한체 F_q에 있어서의 벡터 표시를 나타낸다. 다시 말해, 수학식 105이다.

[0055] [수학식 105]

$\vec{x}$는,

$$(x_1,\ldots,x_n) \in \mathbb{F}_q$$

[0056] 를 나타낸다.

[0057] 수학식 106은, 수학식 107에 나타내는 2개의 벡터 $\vec{x}$와 $\vec{v}$의 수학식 108에 나타내는 내적을 나타낸다.

[0058] [수학식 106]

[0059] $$\vec{x} \cdot \vec{v}$$

[0060] [수학식 107]

$$\vec{x} = (x_1,\ldots,x_n)$$,

[0061] $$\vec{v} = (v_1,\ldots,v_n)$$

[0062] [수학식 108]

[0063] $$\sum_{i=1}^{n} x_i v_i$$

[0064] X^T는, 행렬 X의 전치 행렬을 나타낸다.

[0065] 또한, 이하의 설명에 있어서, 암호 처리란, 암호화 처리, 복호 처리, 키 생성 처리를 포함하는 것이며, 키 비닉 처리도 포함하는 것이다.

[0066] 실시의 형태 1.

[0067] 본 실시의 형태에서는, 이후의 실시의 형태에서 설명하는 「권한 위양을 갖는 술어 암호(Predicate Encryption with Delegation)」나 「권한 위양을 갖는 술어 키 비닉 방식(Predicate Key Encapsulation Mechanism with Delegation)」을 실현하는 기초가 되는 개념과, 권한 위양을 갖는 술어 암호(술어 키 비닉 방식)의 기본 구성에 대하여 설명한다.

[0068] 첫 번째로, 권한 위양을 갖는 술어 암호(술어 키 비닉 방식)의 일종인 「권한 위양을 갖는 내적 술어 암호(내적 술어 키 비닉 방식)」라고 하는 개념을 설명한다. 이후의 실시의 형태에서 설명하는 권한 위양을 갖는 술어 암호(술어 키 비닉 방식)는, 권한 위양을 갖는 내적 술어 암호(내적 술어 키 비닉 방식)이다. 권한 위양을 갖는 내적 술어 암호라고 하는 개념을 설명함에 있어서, 우선 「권한 위양」이라고 하는 개념을 설명한다. 또한, 아울러, 「계층적(Hierarchial)인 권한 위양」이라고 하는 개념을 설명한다. 다음으로, 「내적 술어 암호」를 설명한다. 그리고, 계층적인 권한 위양이라고 하는 개념을 내적 술어 암호에 더한 「계층적 내적 술어 암호(계층적 내적 술어 키 비닉 방식)」를 설명한다. 또한, 계층적 내적 술어 암호의 이해를 깊게 하기 위해, 계층적 내적 술어 암호의 응용예를 설명한다.

[0069] 두 번째로, 벡터 공간에 있어서의 계층적 내적 술어 암호를 설명한다. 본 실시의 형태 및 이하의 실시의 형태에서는, 계층적 술어 암호와 계층적 술어 키 비닉 방식을 벡터 공간에 있어서 실현한다. 여기에서는, 우선, 「기저」와 「기저 벡터」에 대하여 설명한다. 다음으로, 「벡터 공간에 있어서의 내적 술어 암호」에 대하여 설명한다. 그리고, 「벡터 공간에 있어서의 계층 구조의 실현 방법」에 대하여 설명한다. 또한, 이해를 깊게 하기 위해, 계층 구조의 실현예를 설명한다.

[0070] 세 번째로, 본 실시의 형태 및 이후의 실시의 형태에 따른 「계층적 술어 암호」와 「계층적 술어 키 비닉 방식」이라는 기본 구성을 설명한다. 아울러, 계층적 술어 암호와 계층적 술어 키 비닉 방식을 실행하는 「암호 처

리 시스템(10)」의 개요를 설명한다.

[0071] 네 번째로, 계층적 술어 키 비닉 방식이나 계층적 술어 암호를 실현하기 위한 개념을 설명한다. 여기에서는, 「쌍선형 페어링 그룹」, 「벡터 공간 V와 벡터 공간 V^*」, 「표준적인 쌍대 기저 A, A^*」, 「페어링 연산」, 「기저 변환」, 「디스토션 사상(distortion maps)」을 설명한다.

[0072] 다섯 번째로, 계층적 술어 키 비닉 방식과 계층적 술어 암호를 실현하기 위한 공간인 「쌍대 페어링 벡터 공간(Dual Pairing Vector Spaces, DPVS)」이라고 하는 풍부한 수학적 구조를 갖는 공간을 설명한다.

[0073] 그리고, 여섯 번째로, 이상의 설명을 근거로 하여, 이후의 실시의 형태에서 상세하게 설명하는 계층적 술어 암호와 계층적 술어 키 비닉 방식의 실현 방법을 간단하게 설명한다.

[0074] <제 1. 계층적 내적 술어 암호>

[0075] <제 1-1. 권한 위양(계층적인 권한 위양)이라고 하는 개념>

[0076] 도 1은 「권한 위양(계층적인 권한 위양)」이라고 하는 개념을 설명하기 위한 도면이다.

[0077] 권한 위양이란, 상위의 키를 갖는 이용자가, 그 키(상위의 키)보다 기능이 제한된 하위의 키를 생성하는 것이다.

[0078] 도 1에서는, Root(키 생성 장치)는, 마스터 비밀 키를 이용하여, 제 1 층째(Level-1)의 이용자에게 비밀 키를 생성한다. 다시 말해, Root는, 제 1 층째의 이용자 1, 2, 3 각각에 키 1, 2, 3을 생성한다. 그리고, 예컨대, 이용자 1이면, 키 1을 이용하여, 이용자 1의 하위(제 2 층째)의 이용자인 이용자 11, 12, 13 각각에 키 11, 12, 13을 생성할 수 있다. 여기서, 이용자 1이 갖는 키 1보다, 이용자 11, 12, 13이 갖는 키 11, 12, 13은 기능이 제한되어 있다. 기능이 제한되어 있다는 것은, 그 비밀 키에 의해 복호할 수 있는 암호문이 한정되어 있다고 하는 것이다. 다시 말해, 상위의 비밀 키로 복호할 수 있는 암호문의 일부의 암호문만 하위의 비밀 키로 복호할 수 있는 것을 의미한다. 즉, 이용자 1이 갖는 키 1로 복호할 수 있는 암호문 중, 일부의 암호문만 이용자 11, 12, 13이 갖는 키 11, 12, 13으로 복호할 수 있다. 또한, 통상, 키 11과 키 12와 키 13이 복호할 수 있는 암호문은 다르다. 한편, 키 11과 키 12와 키 13이 복호할 수 있는 암호문은, 키 1로 복호할 수 있다.

[0079] 또한, 도 1에 나타내는 바와 같이, 각 비밀 키가 계층(레벨)별로 나누어져 있는 것을 「계층적」이라고 한다. 다시 말해, 도 1에 나타내는 바와 같이, 계층적으로 하위의 키를 생성하는 것을 「계층적인 권한 위양」이라고 부른다.

[0080] 또, 도 1에서는, Root가 제 1 층째의 이용자에게 비밀 키를 생성하고, 제 1 층째의 이용자가 제 2 층째의 이용자에게 비밀 키를 생성하고, 제 2 층째의 이용자가 제 3 층째의 이용자에게 비밀 키를 생성하는 것으로 설명했다. 그러나, 도 2에 나타내는 바와 같이, Root는, 제 1 층째의 이용자에게 비밀 키를 생성할 뿐만 아니라, 제 2 층째 이하의 층의 이용자에게 비밀 키를 생성할 수도 있다. 마찬가지로, 제 1 층째의 이용자는, 제 2 층째의 이용자에게 비밀 키를 생성할 뿐만 아니라, 제 3 층째 이하의 층의 이용자에게 비밀 키를 생성할 수도 있다. 다시 말해, Root나 이용자는, 자신이 갖는 비밀 키보다 하위의 층의 비밀 키를 생성할 수 있다.

[0081] <제 1-2. 내적 술어 암호>

[0082] 다음으로, 「내적 술어 암호」에 대하여 설명한다.

[0083] 우선, 술어 암호란, 술어 정보 f_v에 속성 정보 x를 입력한 경우에 1(True)이 되는 경우($f_v(x)=1$이 되는 경우)에, 암호문을 복호할 수 있는 암호 방식이다. 통상, 암호문에 속성 정보 x가 삽입되고, 비밀 키에 술어 정보 f_v가 삽입된다. 다시 말해, 술어 암호에서는, 속성 정보 x에 근거하여 암호화된 암호문 c를, 술어 정보 f_v에 근거하여 생성된 비밀 키 SK_f에 의해 복호한다. 술어 암호는, 예컨대, 술어 정보 f_v가 조건식이며, 속성 정보 x가 그 조건식으로의 입력 정보이며, 입력 정보(속성 정보 x)가 조건식(술어 정보 f_v)을 만족시키면 ($f_v(x)=1$), 암호문을 복호할 수 있는 암호 방식이라고도 할 수 있다.

[0084] 또, 술어 암호에 대하여 자세하게는 비특허 문헌 16에 기재되어 있다.

[0085] 내적 술어 암호란, 속성 정보 x와 술어 정보 f_v의 내적이 소정의 값인 경우에, $f_v(x)=1$이 되는 술어 암호이다. 다시 말해, 속성 정보 x와 술어 정보 f_v의 내적이 소정의 값인 경우에만, 속성 정보 x에 의해 암호화된 암호문

c를, 술어 정보 f_v에 근거하여 생성된 비밀 키 SK_f에 의해 복호할 수 있다. 이하의 설명에서는, 속성 정보 x와 술어 정보 f_v의 내적이 0인 경우에, $f_v(x)=1$이 되는 것으로 한다.

[0086] <제 1-3. 계층적 내적 술어 암호>

[0087] 계층적 내적 술어 암호(계층적 내적 술어 키 비닉 방식)란, 상술한 「계층적인 권한 위양」이라고 하는 개념을 갖는 「내적 술어 암호」이다.

[0088] 계층적 내적 술어 암호는, 내적 술어 암호에 계층적인 권한 위양 시스템을 갖게 하기 위해, 속성 정보와 술어 정보에 계층 구조를 갖게 한다.

[0089] 도 3은 속성 정보와 술어 정보의 계층 구조를 나타내는 도면이다.

[0090] 도 3에 있어서, 부호가 대응하는 속성 정보와 술어 정보는 대응하는(다시 말해, 내적이 0이 되는) 것으로 한다. 다시 말해, 속성 1과 술어 1의 내적은 0이 되고, 속성 11과 술어 11의 내적은 0이 되고, 속성 12와 술어 12의 내적은 0이 되고, 속성 13과 술어 13의 내적은 0이 되는 것으로 한다. 즉, 속성 1에 의해 암호화된 암호문 c1은, 술어 1에 근거하여 생성된 비밀 키 k1이면 복호할 수 있다. 또한, 속성 11에 의해 암호화된 암호문 c11은, 술어 11에 근거하여 생성된 비밀 키 k11이면 복호할 수 있다. 속성 12와 술어 12, 속성 13과 술어 13에 대해서도 같다고 할 수 있다.

[0091] 상기한 바와 같이, 계층적 내적 술어 암호는 계층적인 권한 위양 시스템을 갖는다. 그 때문에, 술어 1에 근거하여 생성된 비밀 키 k1과, 술어 11에 근거하여, 비밀 키 k11을 생성할 수 있다. 다시 말해, 상위의 비밀 키 k1을 갖는 이용자는, 그 비밀 키 k1과 하위의 술어 11로부터, 비밀 키 k1의 하위의 비밀 키 k11을 생성할 수 있다. 마찬가지로, 비밀 키 k1과 술어 12로부터 비밀 키 k12를 생성할 수 있고, 비밀 키 k1과 술어 13으로부터 비밀 키 k13을 생성할 수 있다.

[0092] 또한, 하위의 비밀 키에 대응하는 키(공개 키)로 암호화된 암호문을 상위의 비밀 키로 복호할 수 있다. 한편, 상위의 비밀 키에 대응하는 키(공개 키)로 암호화된 암호문은, 하위의 비밀 키로 복호할 수 없다. 다시 말해, 속성 11, 속성 12, 속성 13에 의해 암호화된 암호문 c11, c12, c13은, 술어 1에 근거하여 생성된 비밀 키 k1이면 복호할 수 있다. 한편, 속성 1에 의해 암호화된 암호문 c1은, 술어 11, 술어 12, 술어 13에 근거하여 생성된 비밀 키 k11, k12, k13으로는 복호할 수 없다. 즉, 속성 11, 속성 12, 속성 13과 술어 1의 내적은 0이 된다. 한편, 속성 1과 술어 11, 술어 12, 술어 13의 내적은 0이 되지 않는다.

[0093] <제 1-4. 계층적 내적 술어 암호의 응용예>

[0094] 도 4는 후술하는 계층적 내적 술어 암호의 응용예인 계층적 ID 베이스 암호(Hierarchial Identifier Based Encryption, HIBE)의 예를 나타내는 도면이다. 또, 계층적 ID 베이스 암호란, ID 베이스 암호가 계층적으로 된 암호 처리이다. ID 베이스 암호는, 술어 암호의 일종이며, 암호문에 포함되는 ID와 비밀 키에 포함되는 ID가 일치하는 경우에 암호문을 복호할 수 있는 매칭 술어 암호이다.

[0095] 도 4에 나타내는 예에서는, Root(키 생성 장치)는, 마스터 비밀 키 sk와 A 회사의 ID인 「A」에 근거하여, ID 「A」에 대응하는 비밀 키(키 A)를 생성한다. 예컨대, A 회사의 보안 담당자는, 키 A와 각 부문의 ID에 근거하여, 그 ID에 대응하는 비밀 키를 생성한다. 예컨대, 보안 담당자는, 영업 부문의 ID인 「A-1」에 대응하는 비밀 키(키 1)를 생성한다. 다음으로, 예컨대, 각 부문의 관리자는, 그 부문의 비밀 키와 그 부문에 속하는 각 과의 ID에 근거하여, 그 ID에 대응하는 비밀 키를 생성한다. 예컨대, 영업 부문의 관리자는, 영업 1과의 ID인 「A-11」에 대응하는 비밀 키(키 11)를 생성한다.

[0096] 여기서, 영업 1과의 ID 「A-11」에 대응하는 비밀 키인 키 11에 의해, 영업 1과의 ID 「A-11」로 암호화된 암호문을 복호할 수 있다. 그러나, 키 11에 의해, 영업 2과나 영업 3과의 ID로 암호화된 암호문은 복호할 수 없다. 또한, 키 11에 의해, 영업 부문의 ID로 암호화된 암호문은 복호할 수 없다.

[0097] 영업 부문의 ID 「A-1」에 대응하는 비밀 키인 키 1에 의해, 영업 부문의 ID 「A-1」로 암호화된 암호문을 복호할 수 있다. 또한, 키 1에 의해, 영업 부문에 속하는 과의 ID로 암호화된 암호문을 복호할 수 있다. 다시 말해, 키 1에 의해, 영업 1과, 영업 2과, 영업 3과의 ID로 암호화된 암호문을 복호할 수 있다. 그러나, 키 1에 의해, 제조 부문(ID : A-2)이나 스태프 부문(ID : A-3)의 ID로 암호화된 암호문은 복호할 수 없다. 또한, 키 1에 의해, A 회사의 ID로 암호화된 암호문은 복호할 수 없다.

[0098] A 회사의 ID 「A」에 대응하는 비밀 키인 키 A에 의해, A 회사의 ID 「A」로 암호화된 암호문을 복호할 수

있다. 또한, A 회사에 속하는 각 부문이나, 그 부문에 속하는 과의 ID로 암호화된 암호문을 복호할 수 있다.

[0099] 계층적 내적 술어 암호는, ID 베이스 암호 이외에도 여러 가지 응용이 가능하다. 특히, 이하에 설명하는 암호 처리는, 등호 관계 테스트의 클래스로 한정된 것은 아니기 때문에, 매우 많은 응용이 가능하다. 예컨대, 내적 술어 암호의 일종인 검색 가능 암호 등에 대해서도, 계층마다 검색 가능한 범위를 AND 조건이나 OR 조건 등의 조건식을 이용하여 한정하는 등, 종래의 권한 위양 시스템을 갖는 술어 암호에서는 실현할 수 없었던 응용이 가능하다.

[0100] 다시 말해, 이후의 실시의 형태에서 설명하는 계층적 술어 키 비닉 방식과 계층적 술어 암호는, ID 베이스 암호나 검색 가능 암호 등에 폭넓은 응용이 가능하다.

[0101] <제 2. 벡터 공간에 있어서의 계층적 내적 술어 암호>

[0102] 계층적 술어 키 비닉 방식과 계층적 술어 암호는, 후술하는 쌍대 페어링 벡터 공간이라고 하는 고차원 벡터 공간에 있어서 실현된다. 그래서, 벡터 공간에 있어서의 계층적 내적 술어 암호를 설명한다.

[0103] <제 2-1. 기저와 기저 벡터>

[0104] 우선, 벡터 공간의 설명에 있어서 사용하는 「기저」와 「기저 벡터」에 대하여 간단하게 설명한다.

[0105] 도 5는 기저와 기저 벡터를 설명하기 위한 도면이다.

[0106] 도 5는 2차원 벡터 공간에 있어서의 벡터 v를 나타낸다. 벡터 v는, $c_1a_1+c_2a_2$이다. 또한, 벡터 v는, $y_1b_1+y_2b_2$이다. 여기서, a_1, a_2를 기저 A에 있어서의 기저 벡터라고 하고, 기저 A:=(a_1, a_2)로 나타낸다. 또한, b_1, b_2를 기저 B에 있어서의 기저 벡터라고 하고, 기저 B:=(b_1, b_2)로 나타낸다. 또한, c_1, c_2, y_1, y_2는, 각 기저 벡터에 대한 계수이다. 도 5에서는, 2차원 벡터 공간이었기 때문에, 각 기저에 있어서의 기저 벡터는 2개였다. 그러나, N차원 벡터 공간이면, 각 기저에 있어서의 기저 벡터는 N개이다.

[0107] <제 2-2. 벡터 공간에 있어서의 내적 술어 암호>

[0108] 다음으로, 벡터 공간에 있어서의 내적 술어 암호를 설명한다.

[0109] 상기한 바와 같이, 내적 술어 암호란, 속성 정보 x와 술어 정보 f_v의 내적이 소정의 값(여기에서는, 0)인 경우에, $f_v(x)=1$이 되는 술어 암호이다. 속성 정보 x와 술어 정보 f_v가 벡터인 경우, 다시 말해 속성 벡터 $\vec{x}$와 술어 벡터 $\vec{v}$인 경우, 내적 술어는 수학식 109와 같이 정의된다.

[0110] [수학식 109]

$$\vec{x}\cdot\vec{v}=\sum_{i=1}^{n}x_iv_i=0 \text{ 이면, } \quad f_{\vec{v}}(\vec{x})=1,$$

$$\vec{x}\cdot\vec{v}=\sum_{i=1}^{n}x_iv_i\neq 0 \text{ 이면, } \quad f_{\vec{v}}(\vec{x})=0$$

여기서,

$$\vec{x}=(x_1,\ldots,x_n)\ ,$$

$$\vec{v}=(v_1,\ldots,v_n)$$

[0111] 이다.

[0112] 다시 말해, 속성 벡터 $\vec{x}$와 술어 벡터 $\vec{v}$의 내적, 다시 말해 요소마다의 내적의 합이 0인 경우에, 술어 정보 f_v에 속성 정보 x를 입력한 결과가 1(True)이 된다. 또한, 속성 벡터 $\vec{x}$와 술어 벡터 $\vec{v}$의 내적이 0이 아닌 경우에, 술어 정보 f_v에 속성 정보 x를 입력한 결과가 0(False)이 되는 술어 암호이다.

[0113] <제 2-3. 벡터 공간에 있어서의 계층 구조의 실현 방법>

[0114] 다음으로, 벡터 공간에 있어서의 계층 구조의 실현 방법을 설명한다.

[0115] 도 6은 벡터 공간에 있어서의 계층 구조의 실현 방법의 일례를 설명하기 위한 도면이다.

[0116] 여기서 다루는 벡터 공간은, 고차원(N차원) 벡터 공간인 것으로 한다. 다시 말해, 벡터 공간에 있어서의 소정의 기저 C에는, 기저 벡터 c_i(i=1, …, N)의 N개의 기저 벡터가 존재한다.

[0117] N개의 기저 벡터 중 n개의 기저 벡터(기저 벡터 c_i(i=1, …, n))를 계층 구조를 나타내기 위해 사용한다. 또한, 기저 벡터 c_i(i=1, …, n)를, 기저 벡터 c_i(i=1, …, μ_1)와, 기저 벡터 c_i(i=μ_1+1, …, μ_2)와, …, 기저 벡터 c_i(i=μ_{d-1}+1, …, n)의 d개로 분할한다. 여기서, d는, 계층의 깊이를 나타내는 수가 된다.

[0118] 그리고, μ_1개의 기저 벡터 c_i(i=1, …, μ_1)를 제 1 층째의 속성 정보나 술어 정보를 나타내기 위해 할당한다. 또한, μ_2-μ_1개의 기저 벡터 c_i(i=μ_1+1, …, μ_2)를 제 2 층째의 속성 정보나 술어 정보를 나타내기 위해 할당한다. 이하 마찬가지로, μ_d-μ_{d-1}개의 기저 벡터 c_i(i=μ_{d-1}+1, …, μ_d(=n))를 제 d 층째의 속성 정보나 술어 정보를 나타내기 위해 할당한다.

[0119] 또한, 제 L 층째의 속성 정보에 의해 암호문을 생성하는 경우에는, 제 L 층째의 속성 정보뿐만이 아니라, 제 1 층째로부터 제 L 층째까지의 속성 정보를 이용하여 암호문을 생성한다. 마찬가지로, 제 L 층째의 술어 정보에 의해 비밀 키를 생성하는 경우에는, 제 L 층째의 술어 정보뿐만이 아니라, 제 1 층째로부터 제 L 층째까지의 술어 정보를 이용하여 비밀 키를 생성한다. 다시 말해, 제 L 층째의 속성 정보에 의해 암호문을 생성하는 경우나, 제 L 층째의 술어 정보에 의해 비밀 키를 생성하는 경우에는, 제 1 층째로부터 제 L 층째까지 할당된 μ_L개의 기저 벡터 c_i(i=1, …, μ_L)를 이용한다. 예컨대, 제 3 층째의 속성 정보에 의해 암호문을 생성하는 경우에는, 제 1 층째로부터 제 3 층째까지 할당된 μ_3개의 기저 벡터 c_i(i=1, …, μ_3)를 이용하여, 제 1 층째로부터 제 3 층째까지의 속성 정보를 이용하여 암호문을 생성한다. 마찬가지로, 제 3 층째의 술어 정보에 의해 비밀 키를 생성하는 경우에는, 제 1 층째로부터 제 3 층째까지 할당된 μ_3개의 기저 벡터 c_i(i=1, …, μ_3)를 이용하여, 제 1 층째로부터 제 3 층째까지의 술어 정보를 나타내어 비밀 키를 생성한다. 다시 말해, 하위의 층에서 사용되는 속성 정보나 술어 정보에는, 상위의 층에서 사용되는 속성 정보나 술어 정보가 포함된다. 이에 의해, 속성 정보와 술어 정보에 계층 구조를 갖게 한다. 그리고, 이 속성 정보와 술어 정보에 계층 구조를 이용하여, 내적 술어 암호에 권한 위양 시스템을 갖게 한다.

[0120] 또, 이하의 설명에 있어서는, 벡터 공간에 있어서의 계층적 구조를 나타내기 위해, 계층 정보 $\vec{\mu}$를 이용한다. 계층 정보 $\vec{\mu}$를 수학식 110에 나타낸다.

[0121] [수학식 110]

$$\vec{\mu} := (n, d; \mu_1, \ldots, \mu_d)$$

여기서,

$$\mu_0 = 0 < \mu_1 < \mu_2 < \cdots < \mu_d = n$$

[0122] 이다.

[0123] 다시 말해, 계층 정보 $\vec{\mu}$는, 계층 구조를 나타내기 위해 할당된 기저 벡터수(차원수)를 나타내는 n과, 계층의 깊이를 나타내는 d와, 각 계층에 할당된 기저 벡터를 나타내기 위한 μ_1, …, μ_d의 정보를 갖는다.

[0124] 다음으로, 벡터 공간에 있어서의 계층적 내적 술어 암호를 설명한다.

[0125] 속성 공간 Σ_L(L=1, …, d)을, 제 L 층째의 속성 정보를 나타내기 위해 할당된 공간인 것으로 한다. 여기서, 각 Σ_L은, 수학식 111이다.

[0126] [수학식 111]

[0127] $$\sum_L := \mathbb{F}_q^{\mu_L - \mu_{L-1}} \setminus \{\vec{0}\}$$

[0128] 계층적인 속성을 수학식 112에 나타내는 Σ로 한다. 여기서, 합집합은 서로소인 합집합이다.

[0129] [수학식 112]

[0130] $$\Sigma := \bigcup_{L=1}^{d} (\Sigma_1 \times \ldots \times \Sigma_L)$$

[0131] 그러면, 수학식 113에 나타내는 계층적인 속성에 있어서의 수학식 114에 나타내는 계층적인 술어는, 수학식 115와 같이 정의된다.

[0132] [수학식 113]

[0133] $$(\vec{x}_1, \ldots, \vec{x}_h) \in \Sigma$$

[0134] [수학식 114]

$$f(\vec{v}_1, \ldots, \vec{v}_L)$$

여기서,

$$\vec{v}_i \in \mathbb{F}_q{}^{\mu_i - \mu_{i-1}} \setminus \{\vec{0}\}$$

[0135] 이다.

[0136] [수학식 115]

$L \le h$ 이며,

모든 $1 \le i \le L$ 에 대하여, $\vec{x}_i \cdot \vec{v}_i = 0$ 일 때,

또한 그 때에 한하여,

[0137] $$f_{(\vec{v}_1, \ldots, \vec{v}_L)}(\vec{x}_1, \ldots, \vec{x}_h) = 1$$

[0138] 계층적인 술어 공간을 수학식 116에 나타내는 F로 한다.

[0139] [수학식 116]

[0140] $$\mathcal{F} := \left\{ f_{(\vec{v}_1, \ldots, \vec{v}_L)} \middle| \vec{v}_i \in \mathbb{F}_q{}^{\mu_i - \mu_{i-1}} \setminus \{\vec{0}\} \right\}$$

[0141] 또한, 수학식 117의 h와 수학식 118의 L을 계층이라고 부른다.

[0142] [수학식 117]

[0143] $$(\vec{x}_1, \ldots, \vec{x}_h)$$

[0144] [수학식 118]

[0145] $$(\vec{v}_1, \ldots, \vec{v}_L)$$

[0146] <제 2-4. 계층 구조의 실현예>

[0147] 여기서, 간단한 예를 이용하여 계층 구조를 설명한다. 여기에서는, 3개의 계층을 구비하고, 각 계층이 2차원으로 구성된 6차원 공간을 이용하여 설명한다. 다시 말해, $\vec{\mu}$:=(n, d; μ_1, …, μ_d)=(6, 3; 2, 4, 6)이다.

[0148] 제 1 층째의 술어 벡터 $\vec{v}_1$:=(v_1, v_2)에 근거하여 생성된 제 1 층째의 비밀 키 sk_1을 갖는 이용자는, 제 1 층째의 비밀 키 sk_1과 제 2 층째의 술어 벡터 $\vec{v}_2$:=(v_3, v_4)에 근거하여 제 2 층째의 비밀 키 sk_2를 생성할 수 있다. 다시 말해, 제 2 층째의 비밀 키 sk_2는, 술어 벡터 ($\vec{v}_1$, $\vec{v}_2$)에 근거하여 생성된다. 마찬가지로, 제 2 층째의 비밀 키 sk_2를 갖는 이용자는, 제 2 층째의 비밀 키 sk_2와 제 3 층째의 술어 벡터 $\vec{v}_3$:=(v_5, v_6)에 근거하여 제 3 층째의 비밀 키 sk_3을 생성할 수 있다. 다시 말해, 제 3 층째의 비밀 키 sk_3은, 술어 벡터 ($\vec{v}_1$, $\vec{v}_2$, $\vec{v}_3$)에 근거하여 생성된다.

[0149] 제 1 층째의 술어 벡터 $\vec{v}_1$에 근거하여 생성된 제 1 층째의 비밀 키 sk_1은, $(\vec{v}_1, (0, 0), (0, 0))$에 의해 생성된 비밀 키이다. 그 때문에, 제 1 층째의 비밀 키 sk_1은, 속성 벡터 $(\vec{x}_1, (*, *), (*, *)):=((x_1, x_2), (*, *), (*, *))$에 의해 암호화된 암호문을, $\vec{v}_1 \cdot \vec{x}_1=0$인 경우에는 복호할 수 있다. 왜냐하면, $(*, *) \cdot (0, 0)=0$이기 때문이다. 여기서, "*"는, 임의의 값을 나타낸다.

[0150] 마찬가지로, 제 2 층째의 술어 벡터 $(\vec{v}_1, \vec{v}_2)$에 근거하여 생성된 제 2 층째의 비밀 키 sk_2는, $(\vec{v}_1, \vec{v}_2, (0, 0))$에 의해 생성된 비밀 키이다. 그 때문에, 제 2 층째의 비밀 키 sk_2는, 속성 벡터 $(\vec{x}_1, \vec{x}_2, (*, *)):=((x_1, x_2), (x_3, x_4), (*, *))$에 의해 암호화된 암호문을, $\vec{v}_1 \cdot \vec{x}_1=0$ 또한 $\vec{v}_2 \cdot \vec{x}_2=0$인 경우에는 복호할 수 있다.

[0151] 그러나, 제 2 층째의 비밀 키 sk_2는, 제 1 층째의 속성 벡터 $\vec{x}_1:=(x_1, x_2)$(다시 말해, $(\vec{x}_1, (*, *), (*, *))$에 의해 암호화된 암호문을 복호할 수 없다. 왜냐하면, $\vec{v}_2=(0, 0)$이 아니면, $(*, *) \cdot \vec{v}_2 \neq 0$이며, $\vec{v}_2 \cdot \vec{x}_2 \neq 0$이기 때문이다. 그 때문에, 제 2 층째의 비밀 키 sk_2는, 부모인 비밀 키 sk_1보다 한정된 능력만을 갖고 있다고 할 수 있다.

[0152] <제 3. 계층적 술어 암호와 계층적 술어 키 비닉 방식의 구성>

[0153] <제 3-1. 계층적 술어 암호>

[0154] 계층적 술어 암호의 구성을 간단하게 설명한다.

[0155] 계층적 술어 암호는, Setup, GenKey, Enc, Dec, $Delegate_L$(L=1, …, d-1)의 5개의 확률적 다항식 시간 알고리즘을 구비한다.

[0156] (Setup)

[0157] Setup 알고리즘에서는, 보안 파라미터 1^λ와 계층 정보 $\vec{\mu}$가 입력되고, 마스터 공개 키 pk와 마스터 비밀 키 sk가 출력된다. 마스터 비밀 키 sk는 가장 상위의 키이다.

[0158] (GenKey)

[0159] GenKey 알고리즘에서는, 마스터 공개 키 pk와 마스터 비밀 키 sk와 수학식 119에 나타내는 술어 벡터가 입력되고, 수학식 120에 나타내는 제 L 층째의 비밀 키가 출력된다.

[0160] [수학식 119]

[0161] $$(\vec{v}_1, \ldots, \vec{v}_L)$$

[0162] [수학식 120]

[0163] $$sk_{(\vec{v}_1, \ldots, \vec{v}_L)}$$

[0164] (Enc)

[0165] Enc 알고리즘에서는, 마스터 공개 키 pk와 수학식 121에 나타내는 속성 벡터와 평문 정보 m이 입력되고, 암호문 c가 출력된다. 다시 말해, Enc 알고리즘에서는, 평문 정보 m을 삽입하고, 수학식 121에 나타내는 속성 벡터에 의해 암호화된 암호문 c가 출력된다.

[0166] [수학식 121]

$$(\vec{x}_1, \ldots, \vec{x}_h)$$

[0167] 여기서,
$1 \leq h \leq d$
이다.

[0168] (Dec)

[0169] Dec 알고리즘에서는, 마스터 공개 키 pk와 수학식 122에 나타내는 제 L 층째의 비밀 키와 암호문 c가 입력되고, 평문 정보 m 또는 식별 정보 ⊥가 출력된다. 식별 정보 ⊥란, 복호에 실패한 것을 나타내는 정보이다. 다시 말해, Dec 알고리즘에서는, 암호문 c를 제 L 층째의 비밀 키로 복호하여, 평문 정보 m을 추출한다. 또한, 복호에 실패한 경우에는 식별 정보 ⊥를 출력한다.

[0170] [수학식 122]

$$\mathsf{sk}_{(\vec{v}_1,\ldots,\vec{v}_L)}$$

여기서,

[0171] $1 \le L \le d$

이다.

[0172] ($\mathrm{Delegate}_L$)

[0173] $\mathrm{Delegate}_L$에서는, 마스터 공개 키 pk와 수학식 123에 나타내는 제 L 층째의 비밀 키와 수학식 124에 나타내는 제 L+1 층째의 술어 벡터가 입력되고, 수학식 125에 나타내는 제 L+1 층째의 비밀 키가 출력된다. 다시 말해, $\mathrm{Delegate}_L$ 알고리즘에서는, 하위의 비밀 키가 출력된다.

[0174] [수학식 123]

[0175] $$\mathsf{sk}_{(\vec{v}_1,\ldots,\vec{v}_L)}$$

[0176] [수학식 124]

[0177] $$\vec{v}_{L+1}$$

[0178] [수학식 125]

[0179] $$\mathsf{sk}_{(\vec{v}_1,\ldots,\vec{v}_{L+1})}$$

[0180] <제 3-2. 계층적 술어 키 비닉 방식>

[0181] 계층적 술어 키 비닉 방식의 구성을 간단하게 설명한다.

[0182] 계층적 술어 키 비닉 방식은, 계층적 술어 암호와 같이, Setup, GenKey, Enc, Dec, $\mathrm{Delegate}_L$(L=1, …, d-1)의 5개의 확률적 다항식 시간 알고리즘을 구비한다.

[0183] (Setup)

[0184] Setup 알고리즘에서는, 보안 파라미터 1^λ와 계층 정보 $\vec{\mu}$가 입력되고, 마스터 공개 키 pk와 마스터 비밀 키 sk가 출력된다. 마스터 비밀 키 sk는 가장 상위의 키이다.

[0185] (GenKey)

[0186] GenKey 알고리즘에서는, 마스터 공개 키 pk와 마스터 비밀 키 sk와 수학식 126에 나타내는 술어 벡터가 입력되고, 수학식 127에 나타내는 제 L 층째의 비밀 키가 출력된다.

[0187] [수학식 126]

[0188] $$(\vec{v}_1,\ldots,\vec{v}_L)$$

[0189] [수학식 127]

[0190] $$\mathsf{sk}_{(\vec{v}_1,\ldots,\vec{v}_L)}$$

[0191] (Enc)

[0192] Enc 알고리즘에서는, 마스터 공개 키 pk와 수학식 128에 나타내는 속성 벡터가 입력되고, 암호문 c와 세션 키 K가 출력된다. 다시 말해, Enc 알고리즘에서는, 소정의 정보(ρ)를 삽입하고, 수학식 128에 나타내는 속성 벡터

에 의해 암호화된 암호문 c와, 소정의 정보(ρ)로부터 생성한 세션 키 K가 출력된다.

[0193] [수학식 128]

$$(\vec{x}_1,\ldots,\vec{x}_h)$$

여기서,

[0194] $1 \le h \le d$ 이다.

[0195] (Dec)

[0196] Dec 알고리즘에서는, 마스터 공개 키 pk와 수학식 129에 나타내는 제 L 층째의 비밀 키와 암호문 c가 입력되고, 세션 키 K 또는 식별 정보 ⊥가 출력된다. 식별 정보 ⊥란, 복호에 실패한 것을 나타내는 정보이다. 다시 말해, Dec 알고리즘에서는, 암호문 c를 제 L 층째의 비밀 키로 복호하여, 소정의 정보(ρ)에 관한 정보를 추출하고, 세션 키 K를 생성한다. 또한, 복호에 실패한 경우에는 식별 정보 ⊥를 출력한다.

[0197] [수학식 129]

[0198] $\mathsf{sk}_{(\vec{v}_1,\ldots,\vec{v}_L)}$

[0199] ($\mathrm{Delegate}_L$)

[0200] $\mathrm{Delegate}_L$ 알고리즘에서는, 마스터 공개 키 pk와 수학식 130에 나타내는 제 L 층째의 비밀 키와 수학식 131에 나타내는 제 L+1 층째의 술어 벡터가 입력되고, 수학식 132에 나타내는 제 L+1 층째의 비밀 키가 출력된다. 다시 말해, $\mathrm{Delegate}_L$ 알고리즘에서는, 하위의 비밀 키가 출력된다.

[0201] [수학식 130]

[0202] $\mathsf{sk}_{(\vec{v}_1,\ldots,\vec{v}_L)}$

[0203] [수학식 131]

[0204] $\vec{v}_{L+1}$

[0205] [수학식 132]

[0206] $\mathsf{sk}_{(\vec{v}_1,\ldots,\vec{v}_{L+1})}$

[0207] <제 3-3. 암호 처리 시스템(10)>

[0208] 암호 처리 시스템(10)에 대하여 설명한다. 암호 처리 시스템(10)은, 상술한 계층적 술어 암호와 계층적 술어 키 비닉 방식의 알고리즘을 실행한다.

[0209] 도 7은 암호 처리 시스템(10)의 구성도이다.

[0210] 암호 처리 시스템(10)은, 키 생성 장치(100), 암호화 장치(200), 복호 장치(300), 키 위양 장치(400)를 구비한다. 또, 여기에서는, 복호 장치(300)는, 키 위양 장치(400)를 구비하는 것으로 한다. 또한, 상술한 것처럼, 암호 처리 시스템(10)은, 계층적인 암호 처리를 실행하는 것이기 때문에, 암호 처리 시스템(10)은, 복수의 암호화 장치(200), 복수의 복호 장치(300), 복수의 키 위양 장치(400)를 구비하는 것으로 한다.

[0211] 키 생성 장치(100)는, 계층적 술어 키 비닉 방식과 계층적 술어 암호의 Setup, GenKey 알고리즘을 실행한다.

[0212] 암호화 장치(200)는, 계층적 술어 키 비닉 방식과 계층적 술어 암호의 Enc 알고리즘을 실행한다.

[0213] 복호 장치(300)는, 계층적 술어 키 비닉 방식과 계층적 술어 암호의 Dec 알고리즘을 실행한다.

[0214] 키 위양 장치(400)는, 계층적 술어 키 비닉 방식과 계층적 술어 암호의 $\mathrm{Delegate}_L$ 알고리즘을 실행한다.

[0215] 도 8은 암호 처리 시스템(10)의 키 생성 장치(100)와 제 L 층째의 암호화 장치(200)와 복호 장치(300)의 동작을 나타내는 플로우차트이다. 다시 말해, 도 8은 마스터 키(마스터 공개 키와 마스터 비밀 키)의 생성, 제 L 층째의 비밀 키의 생성으로부터, 제 L 층째에 있어서의 암호화와 복호까지의 동작을 나타내는 플로우차트이다.

[0216] (S101 : 키 생성 단계)

[0217] 키 생성 장치(100)는, Setup 알고리즘을 실행하여 마스터 공개 키 pk와 마스터 비밀 키 sk를 생성한다. 또한, 키 생성 장치(100)는, 생성한 마스터 공개 키 pk와 마스터 비밀 키 sk와, 소정의 복호 장치(300)(제 L 층째의 복호 장치(300))에 대응하는 술어 벡터 $\vec{v}_L(\vec{v}_L=(v_1, \cdots, v_i)(i=\mu_L))$에 근거하여, GenKey 알고리즘을 실행하여 제 L 층째의 비밀 키를 생성한다. 그리고, 키 생성 장치(100)는, 생성한 마스터 공개 키 pk를 공개(배포)함과 아울러, 제 L 층째의 비밀 키를 상기 소정의 복호 장치(300)에 비밀리에 배포한다. 또, 키 생성 장치(100)는, 마스터 비밀 키를 비밀리에 유지한다.

[0218] (S102 : 암호화 단계)

[0219] 암호화 장치(200)는, (S101)에서 키 생성 장치(100)가 배포한 마스터 공개 키 pk와, 상기 복호 장치(300)의 속성 벡터 $\vec{x}_L(\vec{x}_L=(x_1, \cdots, x_i)(i=\mu_L))$에 근거하여, Enc 알고리즘을 실행하여 암호문 c를 생성한다. 또, 계층적 술어 키 비닉 방식이면, 암호화 장치(200)는, 세션 키 K도 아울러 생성한다. 그리고, 암호화 장치(200)는, 생성한 암호문 c를 상기 복호 장치(300)에 네트워크 등을 통해 송신한다. 또, 속성 벡터 $\vec{x}_L$은, 공개되어 있는 것으로 하더라도 좋고, 암호화 장치(200)가 키 생성 장치(100)나 복호 장치(300)로부터 취득하는 것으로 하더라도 좋다.

[0220] (S103 : 복호 단계)

[0221] 복호 장치(300)는, (S101)에서 키 생성 장치(100)가 배포한 마스터 공개 키 pk와 제 L 층째의 비밀 키에 근거하여, 알고리즘 Dec를 실행하여, 암호화 장치(200)로부터 수신한 암호문 c를 복호한다. 복호 장치(300)는, 암호문 c를 복호한 결과, 계층적 술어 키 비닉 방식이면 세션 키 K를 취득하고, 계층적 술어 암호이면 평문 정보 m을 취득한다. 복호 장치(300)는, 복호에 실패한 경우에는 식별 정보 $\perp$를 출력한다.

[0222] 도 9는 암호 처리 시스템(10)의 제 L 층째의 키 위양 장치(400)와, 제 L+1 층째의 암호화 장치(200)와 복호 장치(300)의 동작을 나타내는 플로우차트이다. 다시 말해, 도 9는 제 L+1 층째의 비밀 키의 생성으로부터, 제 L+1 층째에 있어서의 암호화와 복호까지의 동작을 나타내는 플로우차트이다.

[0223] (S201 : 키 위양 단계)

[0224] 제 L 층째의 키 위양 장치(400)(제 L 층째의 복호 장치(300)가 구비하는 키 위양 장치(400))는, (S101)에서 키 생성 장치(100)가 배포한 마스터 공개 키 pk와, 키 생성 장치(100) 또는 제 L-1 층째의 키 위양 장치(400)가 배포한 제 L 층째의 비밀 키와, 제 L+1 층째의 복호 장치(300)에 대응하는 술어 벡터 $\vec{v}_{L+1}(\vec{v}_{L+1}=(v_i, \cdots, v_j)(i=\mu_L+1, j=\mu_{L+1}))$에 근거하여, 알고리즘 $\mathrm{Delegate}_L$을 실행하여 제 L+1 층째의 비밀 키를 생성한다. 그리고, 제 L 층째의 키 위양 장치(400)는, 생성한 비밀 키를 제 L+1 층째의 복호 장치(300)에 비밀리에 배포한다.

[0225] (S202 : 암호화 단계)

[0226] 암호화 장치(200)는, (S101)에서 키 생성 장치(100)가 배포한 마스터 공개 키 pk와, 제 L+1 층째까지의 복호 장치(300)의 속성 벡터 $\vec{x}_1$로부터 속성 벡터 $\vec{x}_{L+1}(\vec{x}_i(i=1, \cdots, L+1)(=(x_1, \cdots, x_i)(i=\mu_{L+1})))$에 근거하여, Enc 알고리즘을 실행하여 암호문 c를 생성한다. 또, 계층적 술어 키 비닉 방식이면, 암호화 장치(200)는, 세션 키 K도 아울러 생성한다. 그리고, 암호화 장치(200)는, 생성한 암호문 c를 상기 복호 장치(300)에 네트워크 등을 통해 송신한다. 또, 속성 벡터 $\vec{x}_1$로부터 속성 벡터 $\vec{x}_{L+1}(\vec{x}_i(i=1, \cdots, L+1))$은, 공개되어 있는 것으로 하더라도 좋고, 암호화 장치(200)가 키 생성 장치(100)나 복호 장치(300)로부터 취득하는 것으로 하더라도 좋다.

[0227] (S203 : 복호 단계)

[0228] 복호 장치(300)는, (S101)에서 키 생성 장치(100)가 배포한 마스터 공개 키 pk와, (S201)에서 제 L 층째의 키 위양 장치(400)가 배포한 비밀 키에 근거하여, 알고리즘 Dec를 실행하여, 암호화 장치(200)로부터 수신한 암호문 c를 복호한다. 복호 장치(300)는, 암호문 c를 복호한 결과, 계층적 술어 키 비닉 방식이면 세션 키 K를 취득하고, 계층적 술어 암호이면 평문 정보 m을 취득한다.

[0229] <제 4. 계층적 술어 키 비닉 방식과 계층적 술어 암호를 실현하기 위한 개념>

[0230] 다음으로, 상술한 계층적 술어 암호와 계층적 술어 키 비닉 방식의 각 알고리즘을 실현하기 위해 필요한 개념을 설명한다.

[0231] 여기에서는, 비대칭 페어링 그룹의 직적(direct product)에 의해 후술하는 쌍대 페어링 벡터 공간을 구성하는 예를 이용하여, 암호 처리를 실현하는 방법을 설명한다. 그러나, 쌍대 페어링 벡터 공간은, 비대칭 페어링 그룹의 직적에 의해 실현되는 것으로 한정되지 않는다. 다시 말해, 다른 방법에 의해 구성된 쌍대 페어링 벡터 공간에 있어서도, 이하에 설명하는 암호 처리는 실현 가능하다. 또, 쌍대 페어링 벡터 공간의 전형적인 3개의 예가, 비특허 문헌 17에 기재되어 있다.

[0232] <제 4-1. 쌍선형 페어링 그룹>

[0233] 쌍선형 페어링 그룹(q, G_1, G_2, G_T, g_1, g_2, g_T)을 설명한다.

[0234] 쌍선형 페어링 그룹(q, G_1, G_2, G_T, g_1, g_2, g_T)은, 위수(order) q의 3개의 순회군 G_1, G_2, G_T의 그룹이다. g_1은 G_1의 생성원이며, g_2는 G_2의 생성원이다. 그리고, 쌍선형 페어링 그룹(q, G_1, G_2, G_T, g_1, g_2, g_T)은, 이하의 비퇴화 쌍선형 페어링의 조건을 만족시킨다.

[0235] (조건 : 비퇴화 쌍선형 페어링)

[0236] 다항식 시간으로 계산 가능한 수학식 133에 나타내는 비퇴화 쌍선형 페어링이 존재하는 것.

[0237] [수학식 133]

$$e:\mathbb{G}_1\times\mathbb{G}_2\to\mathbb{G}_T$$

다시 말해, 어떠한 $\xi\in\mathbb{G}_1$, $\eta\in\mathbb{G}_2$ 에 대해서도,

$e(s\xi,t\eta)=e(\xi,\eta)^{st}$ 이며,

[0238] $g_T=e(g_1,g_2)\neq 1$ 이다.

[0239] 여기서, G_1=G_2(=:G)인 경우, 대칭 쌍선형 페어링이라고 부른다. 한편, $G_1\neq G_2$인 경우, 비대칭 쌍선형 페어링이라고 부른다. 대칭 쌍선형 페어링은, 초특이 (초)타원 곡선을 이용하여 구축할 수 있다. 한편, 비대칭 쌍선형 페어링은, 어떤 (초)타원 곡선을 이용하더라도 구축할 수 있다. 비대칭 쌍선형 페어링은, 예컨대, 통상의 타원 곡선을 이용하여 구축할 수 있다.

[0240] <제 4-2. 벡터 공간 V와 벡터 공간 V^*>

[0241] 1차원 공간의 순회군을 고차원 공간(고차원 벡터 공간)에 확장한다. 다시 말해, 수학식 134에 나타내는 바와 같이, G_1과 G_2의 직적에 의해 N차원 벡터 공간 V와 N차원 벡터 공간 V_*를 구축한다.

[0242] [수학식 134]

$$\mathbb{V}:=\overbrace{\mathbb{G}_1\times\cdots\times\mathbb{G}_1}^{N},$$

$$\mathbb{V}^*:=\overbrace{\mathbb{G}_2\times\cdots\times\mathbb{G}_2}^{N}$$

여기서, 공간 $\mathbb{V}$의 요소 x는 N 차원 벡터에 의해 이하와 같이 나타낼 수 있다.

$$x:=(x_1g_1,\ldots,x_Ng_1),$$

마찬가지로, 공간 $\mathbb{V}^*$의 요소 y는 N 차원 벡터에 의해 이하와 같이 나타낼 수 있다.

$$y:=(y_1g_2,\ldots,y_Ng_2),$$

[0243] 또, $i=1,\ldots,N$에 대하여, $x_i,y_i\in\mathbb{F}_q$이다.

[0244] <제 4-3. 표준적인 쌍대 기저 A, A^*>

[0245] N차원 벡터 공간 V의 표준 기저 A와, N차원 벡터 공간 V^*의 표준 기저 A^*를 설명한다.

[0246] 수학식 135는, 표준 기저 A와 표준 기저 A^*를 나타낸다.

[0247] [수학식 135]

$$\mathbb{A} := (a_1,\ldots,a_N),$$

$$\mathbb{A}^* := (a_1^*,\ldots,a_N^*)$$

여기서,

$$a_1 := (g_1,0,\ldots,0), a_2 := (0,g_1,0,\ldots,0),\ldots,a_N := (0,\ldots,0,g_1)$$

$$a_1^* := (g_2,0,\ldots,0), a_2^* := (0,g_2,0,\ldots,0),\ldots,a_N^* := (0,\ldots,0,g_2)$$

[0248] 이다.

[0249] 표준 기저 A와 표준 기저 A^*는, 수학식 136에 나타내는 조건을 만족시킨다.

[0250] [수학식 136]

$$e(a_i,a_j^*) = g_T^{\delta_{i,j}} \qquad i,j \in \{1,\ldots,N\}$$

여기서,

δ: Kronecker δ 다시 말해, $\delta_{i,j} = 1$ if $i = j$ and $\delta_{i,j} = 0$ if $i \neq j$),

$$g_T := e(g_1,g_2) \neq 1$$

[0251] 이다.

[0252] 다시 말해, 표준 기저 A와 표준 기저 A^*는, 쌍대 정규 직교 기저이며, 공간 V와 공간 V^*는, 페어링 연산 e에 의해 관련지어진 쌍대 벡터 공간이다.

[0253] 표준 기저 A와 표준 기저 A^*가 수학식 136에 나타내는 조건을 만족시키는 것에 대하여 보충한다.

[0254] 우선, $e(a_i, a^*_i)=g_T$인 것에 대하여 설명한다. 일례로서, $e(a_1, a^*_1)$에 대하여 계산한다. 상기한 바와 같이, $a_1=(g_1, 0, \cdots, 0)$이며, $a^*_1=(g_2, 0, \cdots, 0)$이다. 따라서, $e(a_1, a^*_1)=e(g_1, g_2)\times e(0, 0)\times\cdots\times e(0, 0)$이다. 여기서, 상기한 바와 같이, $e(g_1, g_2)=g_T$이다. 또한, $e(0, 0)=e(0\cdot g_1, 0\cdot g_2)=e(g_1, g_2)^0$이기 때문에, $e(0, 0)=1$이다. 따라서, $e(a_1, a^*_1)=g_T$가 된다. 다른 $e(a_i, a^*_i)$에 대해서도 같은 계산이 성립하고, $e(a_i, a^*_i)=g_T$가 된다.

[0255] 다음으로, $e(a_i, a^*_j)=1(i\neq j)$인 것에 대하여 설명한다. 일례로서, $e(a_1, a^*_2)$에 대하여 계산한다. 상기한 바와 같이, $a_1=(g_1, 0, \cdots, 0)$이며, $a^*_2=(0, g_2, 0, \cdots, 0)$이다. 따라서, $e(a_1, a^*_2)=e(g_1, 0)\times e(0, g_2)\times e(0, 0)\times\cdots,\times e(0, 0)$이다. $e(g_1, 0)=e(g_1, 0\cdot g_2)=e(g_1, g_2)^0$이기 때문에, $e(g_1, 0)=1$이다. 마찬가지로, $e(0, g_2)=1$이다. 또한, 상기한 바와 같이, $e(0, 0)=1$이다. 따라서, $e(a_i, a^*_j)=1$이 된다. 다른 $e(a_i, a^*_j)$에 대해서도 같은 계산이 성립하고, $e(a_i, a^*_j)=1$이 된다.

[0256] 따라서, 표준 기저 A와 표준 기저 A^*에 있어서, $e(a_i, a^*_i)=g_T$이며, $e(a_i, a^*_j)=1(i\neq j)$이다.

[0257] <제 4-4. 페어링 연산>

[0258] N차원 벡터 공간 V, V^*에 있어서의 페어링 연산 e를 수학식 137에 나타내는 바와 같이 정의한다.

[0259] [수학식 137]

[0260] $$e(x,y) := \prod_{i=1}^{N} e(x_i g_1, y_i g_2)$$

[0261] 다시 말해, N차원 벡터 공간 V의 벡터 $x:=(x_1g_1, x_2g_1, \cdots, x_Ng_1)$과 N차원 벡터 공간 V^*의 벡터 $y:=(y_1g_2, y_2g_2, \cdots, y_Ng_2)$의 페어링 연산 e(x, y)는, 벡터 x와 벡터 y의 요소마다의 페어링 연산의 곱이라고 정의한다. 그러면, 상술한 비퇴화 쌍선형 페어링의 조건으로부터, 페어링 연산 e(x, y)는, 수학식 138에 나타내는 바와 같이 나타낼 수 있다.

[0262] [수학식 138]

[0263] $$e(x,y) := \prod_{i=1}^{N} e(x_i g_1, y_i g_2) = e(g_1, g_2)^{\sum_{i=1}^{N} x_i y_i} = g_T^{\vec{x}\cdot\vec{y}} \in \mathbb{G}_T$$

[0264] <제 4-5. 기저 변환>

[0265] 표준 기저 A와 표준 기저 A^*로 이루어지는 다른 기저 B와 기저 B^*로 변환하는 기저 변환 방법에 대하여 설명한다. 도 10은 기저 변환 방법을 설명하기 위한 도면이다.

[0266] 공간 V에 있어서의 표준 기저 A로부터 공간 V에 있어서의 다른 기저 $B:=(b_1, \cdots, b_N)$으로 변환한다. 여기에서는, 수학식 139에 나타내는 균등하게 선택된 선형 변환 X를 이용하여, 수학식 140에 나타내는 바와 같이 공간 V에 있어서의 표준 기저 A로부터 공간 V에 있어서의 다른 기저 B로 변환한다.

[0267] [수학식 139]

[0268] $$X := \left(x_{i,j}\right) \xleftarrow{\mathrm{U}} GL\left(N, \mathbb{F}_q\right)$$

[0269] [수학식 140]

$$b_i = \sum_{j=1}^{N} x_{i,j} a_j \qquad i = 1, \ldots, N$$

여기서,

$$\mathbb{B} := \left(b_1, \ldots, b_N\right)$$

[0270] 이다.

[0271] 여기서, GL은, General Linear을 의미한다. 다시 말해, GL은, 일반 선형군이며, 행렬식이 0이 아닌 정방 행렬의 집합이며, 곱셈에 관한 군이다.

[0272] X를 이용하는 것에 의해, 공간 V^*에 있어서의 표준 기저 A^*로부터 공간 V^*에 있어서의 기저 $B^*:=(b^*_1, \cdots, b^*_N)$을 효율적으로 계산할 수 있다. 여기에서는, 수학식 141에 나타내는 바와 같이 X를 이용하여, 공간 V^*에 있어서의 기저 B^*를 계산한다.

[0273] [수학식 141]

$$b_i^* = \sum_{j=1}^{N} v_{i,j} a_j^* \qquad i = 1, \ldots, N$$

여기서,

$$\left(v_{i,j}\right) := \left(X^T\right)^{-1}$$

$$\mathbb{B}^* := \left(b_1^*, \ldots, b_N^*\right)$$

[0274] 이다.

[0275] 여기서, 수학식 142가 성립한다.

[0276] [수학식 142]

$$e\left(b_i,b_j^*\right)=g_T^{\delta_{i,j}} \qquad i,j\in\{1,\ldots,N\}$$

여기서,

δ : Kronecker δ (다시 말해, $\delta_{i,j}=1$ if $i=j$ and $\delta_{i,j}=0$ if $i\neq j$),

$$g_T:=e\left(g_1,g_2\right)\neq 1$$

[0277] 이다.

[0278] 다시 말해, 기저 B와 기저 B^*는, 쌍대 공간 V와 V^*에 있어서의 쌍대 정규 직교 기저이다. 즉, X를 이용하여 표준 기저 A와 A^*를 변형한 경우이더라도, 쌍대 정규 직교 기저는 보존된다.

[0279] <제 4-6. 디스토션 사상>

[0280] 표준 기저 A에 있어서의 공간 V의 생성원 x에 대한 디스토션 사상이라고 하는 선형 변환에 대하여 설명한다.

[0281] 공간 V의 표준 기저 A에 있어서의 디스토션 사상 $\Phi_{i,j}$는, 수학식 143에 나타내는 사상이다.

[0282] [수학식 143]

$\phi_{i,j}\left(a_j\right)=a_i$ 이며,

[0283] $k\neq j$ 이면, $\phi_{i,j}\left(a_k\right)=0$ 이다.

[0284] 수학식 144가 성립하기 때문에, 디스토션 사상 $\Phi_{i,j}$는, 수학식 145의 변환을 행할 수 있다.

[0285] [수학식 144]

$$\phi_{i,j}(x)=\phi_{i,j}\left(x_1a_1+x_2a_2+\cdots+x_Na_N\right)=\phi_{i,j}\left(x_ja_j\right)$$

[0286] $$=x_j\phi_{i,j}\left(a_j\right)=x_ja_i$$

[0287] [수학식 145]

$x:=\left(x_1g_1,\ldots,x_jg_1,\ldots,x_Ng_1\right)$에 대하여,

[0288] $$\phi_{i,j}(x):=\left(\overbrace{0,\ldots,0}^{i-1},x_jg_1,\overbrace{0,\ldots,0}^{N-i}\right)$$

[0289] 다시 말해, 표준 기저 A의 벡터 x의 기저 벡터 j의 요소를 기저 벡터 i의 요소로 변환할 수 있다. 이때, 변환된 기저 벡터 j의 요소를 제외한 다른 요소는, 모두 0이 된다. 즉, 벡터 x의 기저 벡터 j의 요소가 기저 벡터 i의 요소가 되고, 그 외의 요소는 0이 된다.

[0290] 공간 V^*의 표준 기저 A^*에 있어서의 디스토션 사상 $\Phi^*_{i,j}$도, 공간 V의 표준 기저 A에 있어서의 디스토션 사상 $\Phi_{i,j}$와 같이 나타낼 수 있다.

[0291] 디스토션 사상 $\Phi_{i,j}$($\Phi^*_{i,j}$)를 이용하는 것에 의해, 수학식 146에 나타내는 N×N 행렬로서 나타내어지는 선형 변환 W로서, x∈V에 대한 어떠한 선형 변환 W도 수학식 147에 의해 효율적으로 계산할 수 있다.

[0292] [수학식 146]

[0293] $$\left(\gamma_{i,j}\right)\in\mathbb{F}_q{}^{N\times N}$$

[0294] [수학식 147]

[0295] $$W(x):=\sum_{i=1,j=1}^{N,N}\gamma_{i,j}\phi_{i,j}(x)$$

[0296] <제 5. 쌍대 페어링 벡터 공간>

[0297] 제 4에서 설명한 개념을 근거로 하여, 쌍대 페어링 벡터 공간에 대하여 설명한다. 후술하는 계층적 술어 암호와 계층적 술어 키 비닉 방식은, 쌍대 페어링 벡터 공간에 있어서 실현된다.

[0298] 쌍대 페어링 벡터 공간 (q, V, V^*, G_T, A, A^*)는, 소수 위수 q와, F_q상의 2개의 N차원 벡터 공간 V, V^*와, 위수 q의 순회군 G_T와, 공간 V의 표준 기저 A:=(a_1, …, a_{N-1})과, 공간 V^*의 표준 기저 A^*:=(a^*_1, …, a^*_{N-1})을 갖는 공간이다. 그리고, 쌍대 페어링 벡터 공간 (q, V, V^*, G_T, A, A^*)는, 이하의 (1) 비퇴화 쌍선형 페어링이 존재하는 것, (2) 표준 기저 A, A^*가 쌍대 정규 직교 기저인 것, (3) 디스토션 사상이 존재한다고 하는 것의 3개의 조건을 만족시키는 공간이다.

[0299] (1) 비퇴화 쌍선형 페어링(상기 제 4-1 참조)

[0300] 다항식 시간으로 계산 가능한 비퇴화 쌍선형 페어링 e가 존재하는 것.

[0301] 다시 말해, 수학식 148에 나타내는 비퇴화 쌍선형 페어링 e가 존재하는 것이 1번째의 조건이다.

[0302] [수학식 148]

$$e:\mathbb{V}\times\mathbb{V}^*\rightarrow\mathbb{G}_T$$

다시 말해, $e(sx,ty)=e(x,y)^{st}$ 이며,

[0303] 모든 $y\in\mathbb{V}$에 대하여, $e(x,y)=1$이면, $x=0$이다.

[0304] (2) 쌍대 정규 직교 기저(상기 제 4-2 참조)

[0305] 공간 V의 표준 기저 A와 공간 V^*의 표준 기저 A^*가 쌍대 정규 직교 기저인 것.

[0306] 다시 말해, 공간 V의 표준 기저 A와 공간 V^*의 표준 기저 A^*가, 수학식 149에 나타내는 조건을 만족시키는 것이 2번째의 조건이다.

[0307] [수학식 149]

모든 i, j에 대하여

$$e(a_i,a_j^*)=g_T^{\delta_{i,j}}$$

여기서,

δ : Kronecker δ (다시 말해, $\delta_{i,j}=1$ if $i=j$ and $\delta_{i,j}=0$ if $i\neq j$),

$g_T\neq 1\in\mathbb{G}_T$

[0308] 이다.

[0309] (3) 디스토션 사상(상기 제 4-6 참조)

[0310] 다항식 시간으로 계산 가능한 디스토션 사상 $\Phi_{i,j}$와 $\Phi^*_{i,j}$가 존재하는 것.

[0311] 다시 말해, 수학식 150에 나타내는 공간 V의 준동형 $\Phi_{i,j}$와 공간 V^*의 준동형 $\Phi^*_{i,j}$가 다항식 시간으로 계산 가능하다고 하는 것이 3번째의 조건이다.

[0312] [수학식 150]

$\phi_{i,j}\left(a_j\right)=a_i$ 이며,

$k\neq j$ 이면, $\phi_{i,j}\left(a_k\right)=0$ 이다.

$\phi^*_{i,j}\left(a^*_j\right)=a^*_i$ 이며,

[0313] $k\neq j$ 이면, $\phi^*_{i,j}\left(a^*_k\right)=0$ 이다.

[0314] 2번째의 조건을 만족시키는 것에 의해, 공간 V와 공간 V^*가 페어링 연산 e(상기 제 4-2 참조)에 의해 관련지어진 쌍대 공간이라고 하는 것도 말할 수 있다.

[0315] <제 6. 계층적 술어 암호와 계층적 술어 키 비닉 방식의 실현 방법의 개요>

[0316] 상술한 개념(상기 제 4 참조)과, 쌍대 페어링 벡터 공간(상기 제 5 참조)을 근거로 하여, 상술한 암호 처리 시스템(10)(상기 제 3 참조)이 계층적 술어 암호와 계층적 술어 키 비닉 방식을 실현하는 방법을 간단하게 설명한다.

[0317] 우선, 암호 처리 시스템(10)에 의해 실현되는 내적 술어 암호의 개요에 대하여 설명한다. 또, 설명을 간단하게 하기 위해, 여기에서는, 계층적이라고 하는 개념을 생략하고, 1계층만으로 구성되는 내적 술어 암호의 개요에 대하여 설명한다.

[0318] 암호 처리 시스템(10)은, 쌍대 페어링 벡터 공간 (q, V, V^*, G_T, A, A^*)에 있어서 내적 술어 암호를 실현한다. 또, 여기서, 공간 V, V^*는, 모두 n+4차원 공간이다.

[0319] 키 생성 장치(100)는, 제 4-5에서 설명한 기저 변환에 의해, 표준 기저 A, A^*로부터 정규 직교 기저 $B:=(b_1, \cdots, b_{n+4})$와, $B^*:=(b^*_1, \cdots, b^*_{n+4})$를 생성한다. 키 생성 장치(100)는, 기저 $B:=(b_1, \cdots, b_{n+4})$ 중 기저 벡터 $b_i(i=1, \cdots, n+2)$로 이루어지는 기저 $B\hat{}:=(b_1, \cdots, b_{n+2})$를 생성한다. 그리고, 기저 $B\hat{}$를 마스터 공개 키 pk로 하고, 기저 B^*를 마스터 비밀 키 sk로 한다. 또한, 키 생성 장치(100)는, 술어 벡터 $\vec{v}(\vec{v}=(v_1, \cdots, v_n))\in F^n_q$로부터 비밀 키 k^*를 수학식 151과 같이 생성하여 복호 장치(300)에 비밀리에 송신한다.

[0320] [수학식 151]

$$k^*:=\sigma\left(v_1b^*_1+\cdots+v_nb^*_n\right)+b^*_{n+1}+\eta b^*_{n+3}$$

여기서,

[0321] $\sigma,\eta\xleftarrow{U}\mathbb{F}_q$ 이다.

[0322] 암호화 장치(200)는, 속성 벡터 $\vec{x}(\vec{x}=(x_1, \cdots, x_n))\in F^n_q$와 평문 정보 m으로부터, 2개의 암호문 c_1과 c_2를 생성한다. 암호문 c_1과 c_2는 수학식 152와 같이 생성된다.

[0323] [수학식 152]

$$c_1:=\delta_1\left(x_1b_1+\cdots+x_nb_n\right)+\zeta b_{n+1}+\delta_2b_{n+2},$$

$$c_2:=g_T^{\zeta}m$$

여기서,

[0324] $\delta_1,\delta_2,\zeta\xleftarrow{U}\mathbb{F}_q$ 이다.

[0325] 복호 장치(300)는, 암호문 c_1, c_2와 비밀 키 k^*에 근거하여, 수학식 153을 계산하여, 평문 정보 m을 추출한다.

[0326] [수학식 153]

[0327] $$m := c_2 / e(c_1, k^*)$$

[0328] 여기서, $\vec{v} \cdot \vec{x}=0$이면, 수학식 154에 나타내는 바와 같이, 수학식 153을 계산하는 것에 의해, 복호 장치(300)는 평문 정보 m을 얻을 수 있다.

[0329] [수학식 154]

[0330] $$e(c_1, k^*)$$
$$= \left(\prod_{i=1}^{n} e(\delta_1 x_i b_i, \sigma v_i b_i^*) \cdot e(\zeta b_{n+1}, b_{n+1}^*) \cdot e(\delta_2 b_{n+2}, 0) \cdot e(0, \eta b_{n+3}^*)\right)$$
$$= g_T^{\delta_1 \sigma(\sum_{i=1}^{n} x_i v_i) + \zeta + 0 + 0}$$
$$= g_T^{\zeta}$$

[0331] 다음으로, 계층적인 권한 위양을 가능하게 한 내적 술어 암호, 다시 말해 계층적 내적 술어 암호의 개요에 대하여, 간단한 예를 이용하여 설명한다. 여기에서는, 3개의 계층을 구비하고, 각 계층이 2차원으로 구성된 6차원을 술어 벡터와 속성 벡터에 이용하고, 그 외에 4차원을 갖는 10차원 공간을 이용하여 설명한다. 다시 말해, 공간 V, V^*는, 10차원 공간이다. 따라서, 마스터 공개 키에 포함되는 기저 $B\hat{}:=(b_1, \cdots, b_6, b_7, b_8)$이다. 또한, 마스터 비밀 키에 포함되는 기저 $B^*:=(b^*1, \cdots, b^*10)$이다.

[0332] 또, 이하의 설명에 있어서, 첨자의 「dec」는 「decryption」을 의미하며, 첨자에 「dec」라고 되어 있는 것은, 암호문의 복호에 이용되는 키 벡터이다. 또한, 첨자의 「ran」은 「randomization」을 의미하며, 첨자에 「ran」이라고 되어 있는 것은, 하위의 키 벡터의 소정의 기저 벡터에 대한 계수를 랜덤화하기 위한 랜덤화 벡터이다. 또한, 첨자의 「del」은 「delegation」을 의미하며, 첨자에 「del」이라고 되어 있는 것은, 하위의 키 벡터를 생성하기 위한 키 생성용 벡터이다.

[0333] 여기서, 암호문 c_1, c_2는, 속성 벡터 $(\vec{x}_1, \vec{x}_2, \vec{x}_3):=((x_1, x_2), (x_3, x_4), (x_5, x_6))$과 평문 정보 m에 의해, 수학식 155와 같이 생성된다.

[0334] [수학식 155]

[0335] $$c_1 := \delta_1(x_1 b_1 + x_2 b_2) + \cdots + \delta_3(x_5 b_5 + x_6 b_6) + \zeta b_7 + \delta_4 b_8,$$
$$c_2 := g_T^{\zeta} m$$

여기서,

$$\delta_1, \ldots, \delta_4, \zeta \xleftarrow{U} \mathbb{F}_q$$

이다.

[0336] 만약, 속성 벡터가, $\vec{x}_1:=(x_1, x_2)$와 같이 높은 계층인 경우, 속성 벡터를 수학식 156과 같이 수정한다.

[0337] [수학식 156]

[0338] $$\vec{x}^+ := \left((x_1, x_2), \left(x_3^+, x_4^+\right), \left(x_5^+, x_6^+\right)\right)$$

여기서,

$$\left(x_3^+, x_4^+, x_5^+, x_6^+\right) \xleftarrow{U} \mathbb{F}_q^4$$

이다.

[0339] 다시 말해, 속성 벡터 $\vec{x}_1$에 의해 생성된 암호문 c_1은, 수학식 156에 나타내는 속성 벡터 $\vec{x}^+$에 의해 생성된 암

호문 c_1로서 생성된다.

[0340] 제 1 층째의 술어 벡터 $\vec{v}_1:=(v_1, v_2)\in F_q^2$에 근거하여 생성된 제 1 층째의 비밀 키 $\vec{k}^*_1:=(k^*_{1,dec}, k^*_{1,ran,1}, k^*_{1,ran,2}, k^*_{1,del,3}, \cdots, k^*_{1,del,6})$은, $k^*_{1,dec}$와, $(k^*_{1,ran,1}, k^*_{1,ran,2})$와, $(k^*_{1,del,3}, \cdots, k^*_{1,del,6})$의 3개의 요소로 이루어진다. 여기서, $k^*_{1,dec}$는, 암호문의 복호에 이용되는 키 벡터이다. $(k^*_{1,ran,1}, k^*_{1,ran,2})$는, 하위의 키 벡터의 소정의 기저 벡터에 대한 계수를 랜덤화하기 위한 랜덤화 벡터이다. $(k^*_{1,del,3}, \cdots, k^*_{1,del,6})$은, 하위의 키 벡터를 생성하기 위한 키 생성용 벡터이다. $k^*_{1,dec}$와, $(k^*_{1,ran,1}, k^*_{1,ran,2})$와, $(k^*_{1,del,3}, \cdots, k^*_{1,del,6})$은, 수학식 157과 같이 생성된다.

[0341] [수학식 157]

$$k^*_{1,\mathrm{dec}} := \sigma_{1,0}\left(v_1 b^*_1 + v_2 b^*_2\right) + b^*_7 + \eta_0 b^*_9,$$

$$k^*_{1,\mathrm{ran},j} := \sigma_{1,j}\left(v_1 b^*_1 + v_2 b^*_2\right) + \eta_j b^*_9 \qquad (j=1,2),$$

$$k^*_{1,\mathrm{del},j} := \sigma_{1,j}\left(v_1 b^*_1 + v_2 b^*_2\right) + \psi b^*_j + \eta_j b^*_9 \qquad (j=3,\ldots,6)$$

여기서,

$$\sigma_{1,j}, \eta_j, \psi \xleftarrow{U} \mathbb{F}_q \qquad (j=0,\ldots,6)$$

[0342] 이다.

[0343] 암호문 c_1을 생성할 때 이용된 속성 벡터가, $(x_1, x_2)\cdot(v_1, v_2)=0$이 되는 $((x_1, x_2), (*, *), (*, *))$이라면, 수학식 158이기 때문에, $k^*_{1,0}$은, 수학식 159를 계산하는 것에 의해, 암호문 c_1, c_2를 복호할 수 있다.

[0344] [수학식 158]

[0345] $$e\left(c_1, k^*_{1,\mathrm{dec}}\right) = g_T^{\xi}$$

[0346] [수학식 159]

[0347] $$c_2 / e\left(c_1, k^*_{1,0}\right)$$

[0348] 제 2 층째의 술어 벡터 $\vec{v}_2:=(v_3, v_4)$에 의해 제 2 층째의 비밀 키 $\vec{k}^*_2:=(k^*_{2,dec}, k^*_{2,ran,1}, k^*_{2,ran,2}, k^*_{2,ran,3}, k^*_{2,del,5}, k^*_{2,del,6})$을 생성한다.

[0349] 우선, $k^*_{2,dec}$를 생성하는 경우, $\sigma_{2,0}(v_3 k^*_{1,del,3}+v_4 k^*_{1,del,4})$를, $k^*_{1,dec}$에 더한다. $k^*_{2,ran,j}$를 생성하는 경우, $\sigma_{2,j}(v_3 k^*_{1,del,3}+v_4 k^*_{1,del,4})$를 0에 더한다(j=1, 2, 3). $k^*_{2,del,j}$를 생성하는 경우, $\sigma_{2,j}(v_3 k^*_{1,del,3}+v_4 k^*_{1,del,4})$를 $\psi^+ k^*_{1,del,j}$에 더한다(j=5, 6). 여기서, $\sigma_{2,j}$(j=0, 1, 2, 3, 5, 6)와, ψ^+는 균등하게 선택된 값이다.

[0350] 또한, 제 2 층째의 비밀 키의 $(v_1 b^*_1+v_2 b^*_2)$와 b^*_7과 b^*_8의 계수의 값을 랜덤화한다(균등하게 분포시킨다). 그래서, $k^*_{2,dec}$를 생성하는 경우, $(\alpha_{0,1} k^*_{1,ran,1}+\alpha_{0,2} k^*_{1,ran,2})$를 더 더한다. $k^*_{2,ran,j}$를 생성하는 경우, $(\alpha_{j,1} k^*_{1,ran,1}+\alpha_{j,2} k^*_{1,ran,2})$를 더한다(j=1, 2, 3). $k^*_{2,del,j}$를 생성하는 경우, $(\alpha_{j,1} k^*_{1,ran,1}+\alpha_{j,2} k^*_{1,ran,2})$를 더한다(j=5, 6). 여기서, $\alpha_{j,1}$과 $\alpha_{j,2}$(j=0, 1, 2, 3, 5, 6)는 균등하게 선택된 값이다.

[0351] 다시 말해, 제 2 층째의 비밀 키 $\vec{k}^*_2:=(k^*_{2,dec}, k^*_{2,ran,1}, k^*_{2,ran,2}, k^*_{2,ran,3}, k^*_{2,del,5}, k^*_{2,del,6})$이 수학식 160과 같이 생성된다.

[0352] [수학식 160]

$$k^*_{2,\mathrm{dec}} := k^*_{1,\mathrm{dec}} + \left(\alpha_{0,1}k^*_{1,\mathrm{ran},1} + \alpha_{0,2}k^*_{1,\mathrm{ran},2}\right) + \sigma_{2,0}\left(v_3 k^*_{1,\mathrm{del},3} + v_4 k^*_{1,\mathrm{del},4}\right),$$

$$k^*_{2,\mathrm{ran},j} := \left(\alpha_{j,1}k^*_{1,\mathrm{ran},1} + \alpha_{j,2}k^*_{1,\mathrm{ran},2}\right) + \sigma_{2,j}\left(v_3 k^*_{1,\mathrm{del},3} + v_4 k^*_{1,\mathrm{del},4}\right) \quad (j = 1,2,3),$$

$$k^*_{2,\mathrm{del},j} := \psi^+ k^*_{1,\mathrm{del},j} + \left(\alpha_{j,1}k^*_{1,\mathrm{ran},1} + \alpha_{j,2}k^*_{1,\mathrm{ran},2}\right) + \sigma_{2,j}\left(v_3 k^*_{1,\mathrm{del},3} + v_4 k^*_{1,\mathrm{del},4}\right) \quad (j = 5,6)$$

여기서,

$$\alpha_{j,1}, \alpha_{j,2}, \sigma_{2,j}, \psi^+ \xleftarrow{U} \mathbb{F}_q \quad (j = 0,1,2,3,5,6)$$

[0353] 이다.

[0354] 또, $k^*_{2,\mathrm{dec}}$는, 암호문의 복호에 이용되는 키 벡터이다. ($k^*_{2,\mathrm{ran},1}$, $k^*_{2,\mathrm{ran},2}$, $k^*_{2,\mathrm{ran},3}$)은, 하위의 키 벡터의 소정의 기저 벡터에 대한 계수를 랜덤화하기 위한 랜덤화 벡터이다. ($k^*_{2,\mathrm{del},5}$, $k^*_{2,\mathrm{del},6}$)은, 하위의 키의 생성에 이용된다.

[0355] 일반적으로, 제 L 층째의 비밀 키 $\vec{k}^*_L := (k^*_{L,\mathrm{dec}}, k^*_{L,\mathrm{ran},j}, k^*_{L,\mathrm{del},j})$에 있어서, $k^*_{L,\mathrm{dec}}$는, 암호문의 복호에 이용되는 키 벡터이다. $k^*_{L,\mathrm{ran},j}$는, 하위의 키 벡터의 소정의 기저 벡터에 대한 계수를 랜덤화하기 위한 랜덤화 벡터이다. $k^*_{L,\mathrm{del},j}$는, 하위의 키 벡터를 생성하기 위한 키 생성용 벡터이다.

[0356] 실시의 형태 2.

[0357] 본 실시의 형태에서는, 실시의 형태 1에서 설명한 개념에 근거하여, 계층적 술어 암호를 실현하는 암호 처리 시스템(10)에 대하여 설명한다.

[0358] 도 11로부터 도 16에 근거하여, 실시의 형태 2에 따른 암호 처리 시스템(10)의 기능과 동작에 대하여 설명한다.

[0359] 도 11은 계층적 술어 암호를 실현하는 암호 처리 시스템(10)의 기능을 나타내는 기능 블록도이다. 암호 처리 시스템(10)은, 상술한 것처럼, 키 생성 장치(100), 암호화 장치(200), 복호 장치(300), 키 위양 장치(400)를 구비한다. 또한, 여기에서도, 복호 장치(300)가 키 위양 장치(400)를 구비하는 것으로 한다.

[0360] 도 12는 키 생성 장치(100)의 동작을 나타내는 플로우차트이다. 도 13은 암호화 장치(200)의 동작을 나타내는 플로우차트이다. 도 14는 복호 장치(300)의 동작을 나타내는 플로우차트이다. 도 15는 키 위양 장치(400)의 동작을 나타내는 플로우차트이다.

[0361] 도 16은, 쌍대 페어링 벡터 공간의 기저의 구조를 나타내는 개념도이다.

[0362] 키 생성 장치(100)의 기능과 동작에 대하여 설명한다. 키 생성 장치(100)는, 마스터 키 생성부(110), 마스터 키 기억부(120), 키 벡터 생성부(130), 랜덤화 벡터 생성부(140), 키 생성용 벡터 생성부(150), 키 배포부(160)를 구비한다.

[0363] (S301 : 마스터 키 생성 단계)

[0364] 마스터 키 생성부(110)는, 수학식 161을 계산하여, 마스터 공개 키 pk와 마스터 비밀 키 sk를 처리 장치에 의해 생성하여 마스터 키 기억부(120)에 기억한다.

[0365] [수학식 161]

(1)

$$N := n+2+r+s,$$
$$\left(q,\mathbb{V},\mathbb{V}^*,\mathbb{G}_T,\mathbb{A},\mathbb{A}^*\right) \xleftarrow{R} \mathcal{G}_{\mathsf{dpvs}}\left(1^\lambda,N\right)$$

(2)

$$X := \left(\chi_{i,j}\right) \xleftarrow{U} GL\left(N,\mathbb{F}_q\right)$$

(3)

$$b_i = \sum_{j=1}^{N} \chi_{i,j} a_j,$$
$$\mathbb{B} := \left(b_1,\ldots,b_N\right)$$

(4)

$$\hat{\mathbb{B}} := \left(b_1,\ldots,b_n,b_{n+1},b_{n+2}\right)$$

(5)

$$\left(v_{i,j}\right) := \left(X^T\right)^{-1}$$

(6)

$$b_i^* = \sum_{j=1}^{N} v_{i,j} a_j^*,$$
$$\mathbb{B}^* := \left(b_1^*,\ldots,b_N^*\right)$$

(7)

$$\mathsf{sk} := \left(X,\mathbb{B}^*\right), \mathsf{pk} := \left(1^\lambda,q,\mathbb{V},\mathbb{V}^*,\mathbb{G}_T,\mathbb{A},\mathbb{A}^*,\hat{\mathbb{B}}\right)$$

[0366] return sk,pk

[0367] 다시 말해, (1) 마스터 키 생성부(110)는, 보안 파라미터 1^λ로, N(=n+2+s+r)차원의 쌍대 페어링 벡터 공간 (q, V, V^*, G_T, A, A^*)를 처리 장치에 의해 생성한다. 여기서, G_{dpvs}는, 1^λ와 N을 입력으로 하여, 보안 파라미터 1^λ와 N차원 공간에 대한 쌍대 페어링 벡터 공간 (q, V, V^*, G_T, A, A^*)를 출력하는 쌍대 페어링 벡터 공간 생성 알고리즘이다. 또한, n은 1 이상의 정수, s는 1 이상의 정수, r은 0 이상의 정수이다. 또한, n+2=R이며, n+2+r=S이다. 특히, (s, r)=(1, 0), (1, 1), (n, 1), (1, n), (n, n)의 경우가 중요하다. 여기서, n은 2 이상의 임의의 값이다. s나 r이 작은 값이면 효율이 좋아지고, s나 r이 큰 값이면 안전성이 높아진다.

[0368] (2) 마스터 키 생성부(110)는, 표준 기저 A로부터 기저 B를 생성하기 위한 선형 변환 X를 처리 장치에 의해 랜덤 선택한다.

[0369] (3) 마스터 키 생성부(110)는, 선택한 선형 변환 X에 근거하여, 기저 A:=(a_1, …, a_N)으로부터 기저 B:=(b_1, …, b_N)을 처리 장치에 의해 생성한다.

[0370] (4) 마스터 키 생성부(110)는, 기저 B에 있어서의 기저 벡터 b_i(i=1, …, n+2)를 갖는 기저 벡터 B^:=(b_1, …, b_n, b_{n+1}, b_{n+2})를 처리 장치에 의해 생성한다.

[0371] (5) 마스터 키 생성부(110)는, 기저 A^*:=(a^*_1, …, a^*_N)으로부터 기저 B^*:=(b^*_1, …, b^*_N)을 생성하기 위한 선형 변환 $(X^T)^{-1}$을 선형 변환 X로부터 처리 장치에 의해 생성한다.

[0372] (6) 마스터 키 생성부(110)는, 생성한 선형 변환 $(X^T)^{-1}$에 근거하여, 기저 A^*로부터 기저 B^*:=(b^*_1, …, b^*_N)을 처리 장치에 의해 생성한다.

[0373] (7) 마스터 키 생성부(110)는, 생성한 선형 변환 X와 기저 B^*를 마스터 비밀 키 sk로 하고, 생성한 기저 B^를 포함하는 (1^λ, q, V, V^*, G_T, A, A^*, B^)를 마스터 공개 키 pk로 한다. 그리고, 마스터 키 기억부(120)는, 마스터 키 생성부(110)가 생성한 마스터 공개 키 pk와 마스터 비밀 키 sk를 기억 장치에 기억한다.

[0374] 또, 쌍대 페어링 벡터 공간의 차원수는, N(=n+2+r+s)인 것으로 했다. 여기서, n은, 계층 정보 $\vec{\mu}$가 갖는 계층 구조를 나타내기 위해 할당되어 있는 기저수를 나타내는 n이다. 다시 말해, 여기에서는, 계층 구조를 나타내기 위해 할당되어 있는 기저수 n에 더하여, 2+r+s개의 기저 벡터가 마련되어 있다.

[0375] 도 16에 나타내는 바와 같이, N(=n+2+r+s)개의 기저 벡터 중, n개의 기저 벡터가 술어 벡터나 속성 벡터를 위해 할당되어 있다. 술어 벡터나 속성 벡터를 위해 할당되어 있는 기저 벡터의 구조는, 도 6에 나타내는 구조와 같다. 나머지 2+r+s개의 기저 벡터 중 n+1번째의 기저 벡터는, 세션 키를 생성하는 정보를 위한 기저 벡터이다. n+2번째의 기저 벡터는, 암호문 c_1을 랜덤화하기 위한 기저 벡터이다. n+3번째로부터 n+2+r번째까지의 기저 벡터는, 키 k^*_L을 랜덤화하기 위한 기저 벡터이다. n+2+r+1번째로부터 n+2+r+s번째까지의 기저 벡터는, 사용하지 않는다.

[0376] 즉, (S301)에 있어서, 마스터 키 생성부(110)는, 수학식 162에 나타내는 Setup 알고리즘을 실행하여, 마스터 공개 키 pk와 마스터 비밀 키 sk를 생성한다.

[0377] [수학식 162]

$$\mathsf{Setup}\left(1^\lambda, \vec{\mu} := (n, d; \mu_1, \ldots, \mu_d)\right):$$
$$\left(\mathsf{param}, \mathbb{B}, \mathbb{B}^*\right) \xleftarrow{R} \mathcal{G}_{\mathsf{ob}}\left(1^\lambda, n+2+r+s\right),$$
$$\hat{\mathbb{B}} := \left(b_1, \ldots, b_n, b_{n+1}, b_{n+2}\right),$$
$$\text{return } \mathsf{sk} := \left(X, \mathbb{B}^*\right),\ \mathsf{pk} := \left(1^\lambda, \mathsf{param}, \hat{\mathbb{B}}\right).$$

여기서,

$$\mathcal{G}_{\mathsf{ob}}\left(1^\lambda, N\right): \mathsf{param} := \left(q, \mathbb{V}, \mathbb{V}^*, \mathbb{G}_T, \mathbb{A}, \mathbb{A}^*\right) \xleftarrow{R} \mathcal{G}_{\mathsf{dpvs}}\left(1^\lambda, N\right),$$
$$X := \left(\chi_{i,j}\right) \xleftarrow{U} GL\left(N, \mathbb{F}_q\right),\ \left(v_{i,j}\right) := \left(X^{\mathrm{T}}\right)^{-1},$$
$$b_i = \sum_{j=1}^{N} \chi_{i,j} a_j,\ \mathbb{B} := \left(b_1, \ldots, b_N\right),$$
$$b_i^* = \sum_{j=1}^{N} v_{i,j} a_j^*,\ \mathbb{B}^* := \left(b_1^*, \ldots, b_N^*\right),$$
$$\text{return } \left(\mathsf{param}, \mathbb{B}, \mathbb{B}^*\right)$$

[0378] 이다.

[0379] (S302 : 키 벡터 $k^*_{L,\,dec}$ 생성 단계)

[0380] 키 벡터 생성부(130)는, 마스터 공개 키 pk와 마스터 비밀 키 sk와, 수학식 163에 나타내는 술어 벡터 ($\vec{v}_1$, …, $\vec{v}_L$)에 근거하여, 수학식 164를 계산하여, 제 L 층째(레벨 L)의 비밀 키의 선두 요소인 키 벡터 $k^*_{L,\,dec}$를 처리 장치에 의해 생성한다.

[0381] [수학식 163]

[0382] $$\left(\vec{v}_1, \ldots, \vec{v}_L\right) := \left(\left(v_1, \ldots, v_{\mu_1}\right), \ldots, \left(v_{\mu_{L-1}+1}, \ldots, v_{\mu_L}\right)\right)$$

[0383] [수학식 164]

(1)

$$\sigma_{0,i},\eta_{0,h} \xleftarrow{U} \mathbb{F}_q \qquad (i=1,\ldots,L;\ h=1,\ldots,r)$$

(2)

$$vv := \sum_{t=1}^{L}\sigma_{0,t}\left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b_i^*\right)$$

(3)

$$rv := \sum_{h=1}^{r}\eta_{0,h} b_{n+2+h}^*$$

(4)

$$k_{L,\mathrm{dec}}^* := vv + b_{n+1}^* + rv$$

$$:= \sum_{t=1}^{L}\sigma_{0,t}\left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b_i^*\right) + b_{n+1}^* + \sum_{h=1}^{r}\eta_{0,h} b_{n+2+h}^*$$

[0384]

[0385] 다시 말해, (1) 키 벡터 생성부(130)는, 난수 $\sigma_{0,i}$(i=1, …, L)와 난수 $\eta_{0,h}$(h=1, …, r)를 처리 장치에 의해 생성한다.

[0386] (2) 키 벡터 생성부(130)는, 기저 벡터 b^*_i(i=1, …, μ_L)에 대한 계수로서, 생성한 난수 $\sigma_{0,t}$로 랜덤화한 술어 벡터의 각 요소를 설정하여, 벡터 vv를 처리 장치에 의해 생성한다. 다시 말해, 기저 벡터 b^*_i(i=1, …, μ_L)에 대한 계수에는, 술어 벡터의 각 요소가 삽입된다.

[0387] (3) 키 벡터 생성부(130)는, 기저 벡터 b^*_i(i=n+2+1, …, n+2+r)에 대한 계수로서, 생성한 난수 $\eta_{0,h}$를 설정하여, 벡터 rv를 처리 장치에 의해 생성한다.

[0388] (4) 키 벡터 생성부(130)는, 생성한 벡터 vv와 벡터 rv를, 기저 벡터 b^*_{n+1}에 대한 계수로서 1을 설정한 벡터에 가산하여, 키 벡터 $k^*_{L,\mathrm{dec}}$를 생성한다.

[0389] (S303 : 랜덤화 벡터 $k^*_{L,\mathrm{ran},j}$ 생성 단계)

[0390] 랜덤화 벡터 생성부(140)는, 마스터 공개 키 pk와 마스터 비밀 키 sk와, 수학식 163에 나타내는 술어 벡터 ($\vec{v}_1$, …, $\vec{v}_L$)에 근거하여, 수학식 165를 계산하여, 랜덤화 벡터 $k^*_{L,\mathrm{ran},j}$(j=1, …, L+1)를 생성한다. 랜덤화 벡터 $k^*_{L,\mathrm{ran},j}$(j=1, …, L+1)는, 하위의 키 중, 술어 벡터의 각 요소가 삽입되는 기저 벡터에 대한 계수를 균등하게 분포시키기 위한 벡터이다. 또, 랜덤화 벡터 $k^*_{L,\mathrm{ran},j}$는, 제 L 층째의 비밀 키의 j번째의 요소이다.

[0391] [수학식 165]

(1)

$$\sigma_{j,i},\eta_{j,h} \xleftarrow{U} \mathbb{F}_q \qquad (j=1,\ldots,L+1;\ i=1,\ldots,L;\ h=1,\ldots,r)$$

(2)

$$vv_j := \sum_{t=1}^{L}\sigma_{j,t}\left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b_i^*\right) \qquad (j=1,\ldots,L+1)$$

(3)

$$rv_j := \sum_{h=1}^{r}\eta_{j,h} b_{n+2+h}^* \qquad (j=1,\ldots,L+1)$$

(4)

$$k_{L,\mathrm{ran},j}^* := vv_j + rv_j$$

$$:= \sum_{t=1}^{L}\sigma_{j,t}\left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b_i^*\right) + \sum_{h=1}^{r}\eta_{j,h} b_{n+2+h}^* \qquad (j=1,\ldots,L+1)$$

[0392]

[0393] 다시 말해, (1) 랜덤화 벡터 생성부(140)는, 난수 $\sigma_{j,i}$(j=1, …, L+1; i=1, …, L)와 난수 $\eta_{j,h}$(j=1, …, L+1; h=1, …, r)를 처리 장치에 의해 생성한다.

[0394] (2) 랜덤화 벡터 생성부(140)는, j=1, …, L+1의 각 j에 대하여, 기저 벡터 b^*_i(i=1, …, μ_L)에 대한 계수로서, 난수 $\sigma_{j,t}$로 랜덤화한 술어 벡터의 각 요소를 설정하여, 벡터 vv_j를 처리 장치에 의해 생성한다. 다시 말해, 기저 벡터 b^*_i(i=1, …, μ_L)에 대한 계수에는, 술어 벡터의 각 요소가 삽입된다.

[0395] (3) 랜덤화 벡터 생성부(140)는, j=1, …, L+1의 각 j에 대하여, 기저 벡터 b^*_i(i=n+2+1, …, n+2+r)에 대한 계수로서, 난수 $\eta_{j,h}$를 처리 장치에 의해 설정하여, 벡터 rv_j를 처리 장치에 의해 생성한다.

[0396] (4) 랜덤화 벡터 생성부(140)는, j=1, …, L+1의 각 j에 대하여, 생성한 벡터 vv_j와 벡터 rv_j를 가산하여, 랜덤화 벡터 $k^*_{L,ran,j}$(j=1, …, L+1)를 생성한다.

[0397] (S304 : 키 생성용 벡터 $k^*_{L,del,j}$ 생성 단계)

[0398] 키 생성용 벡터 생성부(150)는, 마스터 공개 키 pk와 마스터 비밀 키 sk와, 수학식 163에 나타내는 술어 벡터 ($\vec{v}_1$, …, $\vec{v}_L$)에 근거하여, 수학식 166을 계산하여, 키 생성용 벡터 $k^*_{L,del,j}$(j=μ_L+1, …, n)를 처리 장치에 의해 생성한다. 키 생성용 벡터 $k^*_{L,del,j}$(j=μ_L+1, …, n)는, 하위의 비밀 키(하위의 키 벡터)를 생성하기 위한 벡터이다. 또, 키 생성용 벡터 $k^*_{L,del,j}$는, 제 L 층째의 비밀 키의 j번째의 요소이다.

[0399] [수학식 166]

(1)

$$\sigma_{j,i},\psi,\eta_{j,h} \xleftarrow{U} \mathbb{F}_q \qquad (j=\mu_L+1,\ldots,n;\ i=1,\ldots,L;\ h=1,\ldots r)$$

(2)

$$vv_j := \sum_{t=1}^{L}\sigma_{j,t}\left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b_i^*\right) \qquad (j=\mu_L+1,\ldots,n)$$

(3)

$$\psi v_j := \psi b_j^* \qquad (j=\mu_L+1,\ldots,n)$$

(4)

$$rv_j := \sum_{h=1}^{r}\eta_{j,h}b_{n+2+h}^* \qquad (j=\mu_L+1,\ldots,n)$$

(5)

$$k_{L,\mathrm{del},j}^* := vv_j+\psi v_j+rv_j := \sum_{t=1}^{L}\sigma_{j,t}\left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b_i^*\right)+\psi b_j^*+\sum_{h=1}^{r}\eta_{j,h}b_{n+2+h}^* \qquad (j=\mu_L+1,\ldots,n)$$

[0400]

[0401] 다시 말해, (1) 키 생성용 벡터 생성부(150)는, 난수 $\sigma_{j,i}$(j=μ_L+1, …, n; i=1, …, L)와 난수 ψ와 난수 $\eta_{j,h}$(j=μ_L+1, …, n; h=1, …, r)를 처리 장치에 의해 생성한다.

[0402] (2) 키 생성용 벡터 생성부(150)는, j=μ_L+1, …, n의 각 j에 대하여, 기저 벡터 b^*_i(i=1, …, μ_L)에 대한 계수로서 난수 $\sigma_{j,t}$로 랜덤화한 술어 벡터의 각 요소를 설정하여, 벡터 vv_j를 처리 장치에 의해 생성한다. 다시 말해, 기저 벡터 b^*_i(i=1, …, μ_L)에 대한 계수에는, 술어 벡터의 각 요소가 삽입된다.

[0403] (3) 키 생성용 벡터 생성부(150)는, j=μ_L+1, …, n의 각 j에 대하여, 기저 벡터 b^*_j에 대한 계수로서 난수 ψ를 설정하고, 벡터 ψv_j를 처리 장치에 의해 생성한다.

[0404] (4) 키 생성용 벡터 생성부(150)는, $j=\mu_L+1, \cdots, n$의 각 j에 대하여, 기저 벡터 $b^*_i(i=n+2+1, \cdots, n+2+r)$에 대한 계수로서, 난수 $\eta_{j,h}$를 처리 장치에 의해 설정하여, 벡터 rv_j를 처리 장치에 의해 생성한다.

[0405] (5) 키 생성용 벡터 생성부(150)는, $j=\mu_L+1, \cdots, n$의 각 j에 대하여, 벡터 vv_j와, 벡터 ψv_j와, 벡터 rv_j를 가산하여, 키 생성용 벡터 $k^*_{L,del,j}(j=\mu_L+1, \cdots, n)$를 생성한다.

[0406] 즉, (S302)로부터 (S304)에 있어서, 키 벡터 생성부(130)와 랜덤화 벡터 생성부(140)와 키 생성용 벡터 생성부(150)는, 수학식 167에 나타내는 GenKey 알고리즘을 처리 장치에 의해 실행한다. 이에 의해, 키 벡터 $k^*_{L,dec}$와, 랜덤화 벡터 $k^*_{L,ran,j}(j=1, \cdots, L+1)$와, 키 생성용 벡터 $k^*_{L,del,j}(j=\mu_L+1, \cdots, n)$를 포함하는 제 L 층째의 비밀 키(키 정보 $\vec{k}^*_L$)가 생성된다.

[0407] [수학식 167]

$$\mathsf{GenKey}\left(\mathsf{pk},\mathsf{sk},\left(\vec{v}_1,\ldots,\vec{v}_L\right)\right) := \left(\left(v_1,\ldots,v_{\mu_1}\right),\ldots,\left(v_{\mu_{L-1}+1},\ldots,v_{\mu_L}\right)\right):$$

$$\sigma_{j,i},\psi,\eta_{j,h} \xleftarrow{U} \mathbb{F}_q$$

$$\text{for } j=0,\ldots,L+1,\mu_L+1,\ldots,n;\ i=1,\ldots,L;\ h=1,\ldots,r$$

$$k^*_{L,\mathsf{dec}} := \sum_{t=1}^{L}\sigma_{0,t}\left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b_i^*\right) + b^*_{n+1} + \sum_{h=1}^{r}\eta_{0,h}b^*_{n+2+h},$$

$$k^*_{L,\mathsf{ran},j} := \sum_{t=1}^{L}\sigma_{j,t}\left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b_i^*\right) + \sum_{h=1}^{r}\eta_{j,h}b^*_{n+2+h}$$

$$\text{for } j=1,\ldots,L+1,$$

$$k^*_{L,\mathsf{del},j} := \sum_{t=1}^{L}\sigma_{j,t}\left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b_i^*\right) + \psi b^*_j + \sum_{h=1}^{r}\eta_{j,h}b^*_{n+2+h}$$

$$\text{for } j=\mu_L+1,\ldots,n,$$

$$\text{return } \vec{k}^*_L := \left(k^*_{L,\mathsf{dec}},k^*_{L,\mathsf{ran},1},\ldots,k^*_{L,\mathsf{ran},L+1},k^*_{L,\mathsf{del},\mu_L+1},\ldots,k^*_{L,\mathsf{del},n}\right)$$

[0408]

[0409] (S305 : 키 배포 단계)

[0410] 키 배포부(160)는, 마스터 키 생성부(110)가 생성한 마스터 공개 키와, 키 벡터 생성부(130)와 랜덤화 벡터 생성부(140)와 키 생성용 벡터 생성부(150)가 생성한 키 정보 $\vec{k}^*_L$을 복호 장치(300)에 통신 장치를 통해 송신한다. 또한, 키 배포부(160)는, 마스터 공개 키를 암호화 장치(200)에 통신 장치를 통해 송신한다. 여기서, 키 정보 $\vec{k}^*_L$은 비밀리에 복호 장치(300)에 송신되지만, 키 정보 $\vec{k}^*_L$을 비밀리에 복호 장치(300)에 송신하는 방법에 관해서는, 어떠한 방법이더라도 상관없다. 예컨대, 종래의 암호 처리를 사용하여 송신하더라도 좋다.

[0411] 암호화 장치(200)의 기능과 동작에 대하여 설명한다. 암호화 장치(200)는, 송신 정보 설정부(210), 암호 벡터 생성부(220), 암호 정보 생성부(230), 데이터 송신부(240), 공개 키 취득부(250)를 구비한다.

[0412] 또, 이하의 처리 전에, 공개 키 취득부(250)는, 마스터 공개 키 pk와, 복호 장치(300)의 술어 정보 벡터에 대응하는 속성 정보 벡터를 취득하고 있는 것으로 한다.

[0413] (S401 : 송신 정보 설정 단계)

[0414] 송신 정보 설정부(210)는, 마스터 공개 키 pk에 근거하여, 수학식 168을 처리 장치에 의해 계산하여 송신 정보 벡터 ζv를 생성한다.

[0415] [수학식 168]

(1)

$$\zeta \xleftarrow{U} \mathbb{F}_q$$

(2)

$$\zeta v := \zeta b_{n+1}$$

[0416]

[0417] 다시 말해, (1) 송신 정보 설정부(210)는, 난수 ζ를 처리 장치에 의해 생성한다.

[0418] (2) 송신 정보 설정부(210)는, 마스터 공개 키 pk에 포함되는 기저 B^의 기저 벡터 b_{n+1}에 대한 계수로서 난수 ζ를 처리 장치에 의해 설정하여, 송신 정보 벡터 ζv를 생성한다.

[0419] (S402 : 암호 벡터 c_1 생성 단계)

[0420] 암호 벡터 생성부(220)는, 마스터 공개 키 pk와, 수학식 169에 나타내는 속성 벡터 ($\vec{x}_1$, …, $\vec{x}_L$)에 근거하여, 수학식 170을 처리 장치에 의해 계산하여 암호 벡터 c_1을 생성한다.

[0421] [수학식 169]

[0422] $$\left(\vec{x}_1,\ldots,\vec{x}_L\right) := \left(\left(x_1,\ldots,x_{\mu_1}\right),\ldots,\left(x_{\mu_{L-1}+1},\ldots,x_{\mu_L}\right)\right)$$

[0423] [수학식 170]

(1)

$$\left(\vec{x}_{L+1},\ldots,\vec{x}_d\right) := \left(\left(x_{\mu_L+1},\ldots,x_{\mu_{L+1}}\right),\ldots,\left(x_{\mu_{d-1}+1},\ldots,x_{\mu_d}\right)\right)$$

$$\xleftarrow{U} \mathbb{F}_q^{\mu_{L+1}-\mu_L}\times\cdots\times\mathbb{F}_q^{n-\mu_{d-1}},$$

$$\delta_1,\ldots,\delta_d,\delta_{n+2},\zeta \xleftarrow{U} \mathbb{F}_q$$

(2)

$$xv := \sum_{t=1}^{d}\delta_t\left(\sum_{i=\mu_{t-1}+1}^{\mu_t} x_i b_i\right)$$

(3)

$$rv := \delta_{n+2} b_{n+2}$$

(4)

$$c_1 := xv + \zeta v + rv$$

[0424] $$:= \sum_{t=1}^{d}\delta_t\left(\sum_{i=\mu_{t-1}+1}^{\mu_t} x_i b_i\right) + \zeta b_{n+1} + \delta_{n+2} b_{n+2}$$

[0425] 다시 말해, (1) 암호 벡터 생성부(220)는, 난수 ($\vec{x}_{L+1}$, …, $\vec{x}_d$)와, 난수 δ_i(i=1, …, d, n+2)를 처리 장치에 의해 생성한다.

[0426] (2) 암호 벡터 생성부(220)는, 마스터 공개 키 pk에 포함되는 기저 B의 기저 벡터 b_i(i=1, …, μ_L)에 대한 계수로서 속성 벡터의 각 요소를 처리 장치에 의해 설정한다. 다시 말해, 기저 벡터 b_i(i=1, …, μ_L)에 대한 계수에는, 속성 벡터의 각 요소가 삽입된다. 또한, 암호 벡터 생성부(220)는, 기저 벡터 b_i(i=μ_L+1, …, n)에 대한 계수로서 난수를 처리 장치에 의해 설정한다. 이에 의해, 암호 벡터 생성부(220)는, 벡터 xv를 생성한다.

[0427] (3) 암호 벡터 생성부(220)는, 마스터 공개 키 pk에 포함되는 기저 B의 기저 벡터 b_{n+2}에 대한 계수로서 난수 δ_{n+2}를 처리 장치에 의해 설정하여, 벡터 rv를 생성한다.

[0428] (4) 암호 벡터 생성부(220)는, 생성한 벡터 xv와 벡터 rv를, 송신 정보 설정부(210)가 생성한 송신 정보 벡터 ζv에 가산하여 암호 벡터 c_1을 처리 장치에 의해 생성한다.

[0429] 또, 벡터 rv는, 안전성을 높게 하기 위해 더해지는 것이며, 필수 요소는 아니다.

[0430] (S403 : 암호 정보 c_2 생성 단계)

[0431] 암호 정보 생성부(230)는, 평문 정보 m에 근거하여, 수학식 171을 처리 장치에 의해 계산하여 암호 정보 c_2를 생성한다.

[0432] [수학식 171]

$$c_2 := g_T^{\zeta} m$$

여기서,

$$g_T = e(a_i, a_i^*) \neq 1$$

[0433] 이다.

[0434] (S404 : 데이터 송신 단계)

[0435] 데이터 송신부(240)는, 암호 벡터 생성부(220)가 생성한 암호 벡터 c_1과, 암호 정보 생성부(230)가 생성한 암호 정보 c_2를 복호 장치(300)에 통신 장치를 통해 송신한다.

[0436] 즉, 암호화 장치(200)는, 수학식 172에 나타내는 Enc 알고리즘을 실행하여, 암호 벡터 c_1과 암호 정보 c_2를 생성한다.

[0437] [수학식 172]

$$\begin{aligned}
&\mathsf{Enc}\left(\mathsf{pk}, m \in \mathbb{G}_T, \left(\vec{x}_1, \ldots, \vec{x}_L\right) := \left(\left(x_1, \ldots, x_{\mu_1}\right), \ldots, \left(x_{\mu_{L-1}+1}, \ldots, x_{\mu_L}\right)\right)\right): \\
&\quad \left(\vec{x}_{L+1}, \ldots, \vec{x}_d\right) \xleftarrow{\mathrm{U}} \mathbb{F}_q^{\mu_{L+1}-\mu_L} \times \cdots \times \mathbb{F}_q^{n-\mu_{d-1}}, \\
&\quad \delta_1, \ldots, \delta_d, \delta_{n+2}, \zeta \xleftarrow{\mathrm{U}} \mathbb{F}_q, \\
&\quad c_1 := \sum_{t=1}^{d} \delta_t \left(\sum_{i=\mu_{t-1}+1}^{\mu_t} x_i b_i \right) + \zeta b_{n+1} + \delta_{n+2} b_{n+2}, \; c_2 := g_T^{\zeta} m, \\
&\quad \mathsf{return} \; (c_1, c_2)
\end{aligned}$$

[0438]

[0439] 복호 장치(300)의 기능과 동작에 대하여 설명한다. 복호 장치(300)는, 벡터 입력부(310), 키 벡터 기억부(320), 페어링 연산부(330)를 구비한다.

[0440] (S501 : 벡터 입력 단계)

[0441] 벡터 입력부(310)는, 암호화 장치(200)의 데이터 송신부(240)가 송신한 암호 벡터 c_1과 암호 정보 c_2를 통신 장치를 통해 수신하여 입력한다.

[0442] (S502 : 복호 단계)

[0443] 페어링 연산부(330)는, 마스터 공개 키 pk와 제 L 층째의 비밀 키의 선두 요소인 키 벡터 $k^*_{L,\,dec}$에 근거하여, 수학식 173을 처리 장치에 의해 계산하여 평문 정보 m'를 생성한다.

[0444] [수학식 173]

$$m' := c_2 / e\left(c_1, k^*_{L,\mathsf{dec}}\right)$$

[0445]

[0446] 다시 말해, 페어링 연산부(330)는, 벡터 입력부(310)가 입력한 암호 벡터 c_1과, 키 벡터 기억부(320)가 기억 장치에 기억한 키 벡터 $k^*_{L,\,dec}$에 대하여, 페어링 연산 e를 처리 장치에 의해 행한다. 이에 의해, 페어링 연산부(330)는, g^{ζ}_T를 계산한다. 그리고, 계산한 g^{ζ}_T로 암호 정보 $c_2(=g^{\zeta}_T m)$를 나누는 것에 의해, 평문 정보 m'(=m)를 계산한다. 또, 키 벡터 기억부(320)는, 키 생성 장치(100) 또는 상위의 키 위양 장치(400)로부터 키 벡터 $k^*_{L,\,dec}$가 배포되었을 때, 키 벡터 $k^*_{L,\,dec}$를 기억 장치에 기억하고 있다.

[0447] 여기서, 암호화 장치(200)가 암호화에 이용한 속성 벡터 $\vec{x}_i(i=1, \cdots, h)$와, 복호 장치(300)가 복호에 이용한 키 벡터의 술어 벡터 $\vec{v}_i(i=1, \cdots, L)$에 대하여, $L \leq h$이며, 모든 i(i=1, …, L)에 대하여 $\vec{x}_i \cdot \vec{v}_i = 0$이면, 수학식 174에 나타내는 바와 같이, 암호 벡터 c_1과 키 벡터 $k^*_{L,\,dec}$에 대하여 페어링 연산 e를 행하는 것에 의해, g^{ζ}_T

를 얻을 수 있다.

[0448] [수학식 174]

[0449] $$e\left(c_1,k^*_{L,\mathrm{dec}}\right)=g_T^{\sum_{1\le i\le L}\sigma_i\delta_i\vec{x}_i\cdot\vec{v}_i+\zeta}=g_T^{\zeta}$$

[0450] 다시 말해, 복호 장치(300)는, 수학식 175에 나타내는 Dec 알고리즘을 실행하여, 평문 정보 m'를 생성한다.

[0451] [수학식 175]

[0452] $$\mathrm{Dec}\left(\mathrm{pk},k^*_{L,\mathrm{dec}},c_1,c_2\right):m':=c_2/e\left(c_1,k^*_{L,\mathrm{dec}}\right),$$
$$\text{return } m'$$

[0453] 키 위양 장치(400)의 기능과 동작에 대하여 설명한다. 키 위양 장치(400)는, 키 벡터 취득부(410)(키 생성용 벡터 취득부), 키 벡터 생성부(420), 랜덤화 벡터 생성부(430), 키 생성용 벡터 생성부(440), 키 배포부(450)를 구비한다.

[0454] (S601 : 키 정보 k^*_L 취득 단계)

[0455] 키 벡터 취득부(410)는, 제 L 층째의 비밀 키의 선두 요소인 키 벡터 $k^*_{L,\,dec}$와, 랜덤화 벡터 $k^*_{L,\,ran,\,j}$(j=1, …, L+1)와, 키 생성용 벡터 $k^*_{L,\,del,\,j}$(j=μ_L+1, …, n)를 포함하는 제 L 층째의 비밀 키(키 정보 $\vec{k}^*_L$)를 통신 장치를 통해 취득한다.

[0456] (S602 : 키 벡터 $k^*_{L+1,\,dec}$ 생성 단계)

[0457] 키 벡터 생성부(420)는, 마스터 공개 키 pk와 키 정보 $\vec{k}^*_L$과 수학식 176에 나타내는 술어 벡터 $\vec{v}_{L+1}$에 근거하여, 수학식 177을 계산하여, 제 L+1 층째의 비밀 키의 선두 요소인 키 벡터 $k^*_{L+1,\,dec}$를 처리 장치에 의해 생성한다.

[0458] [수학식 176]

[0459] $$\vec{v}_{L+1}:=\left(v_{\mu_L+1},\ldots,v_{\mu_{L+1}}\right)$$

[0460] [수학식 177]

[0461] (1)
$$\alpha_{0,i},\sigma_0\xleftarrow{\mathrm{U}}\mathbb{F}_q\qquad(i=1,\ldots,L+1)$$
(2)
$$rv:=\sum_{i=1}^{L+1}\alpha_{0,i}k^*_{L,\mathrm{ran},i}$$
(3)
$$vv:=\sigma_0\left(\sum_{i=\mu_L+1}^{\mu_{L+1}}v_ik^*_{L,\mathrm{del},i}\right)$$
(4)
$$k^*_{L+1,\mathrm{dec}}:=k^*_{L,\mathrm{dec}}+rv+vv$$
$$:=k^*_{L,\mathrm{dec}}+\sum_{i=1}^{L+1}\alpha_{0,i}k^*_{L,\mathrm{ran},i}+\sigma_0\left(\sum_{i=\mu_L+1}^{\mu_{L+1}}v_ik^*_{L,\mathrm{del},i}\right)$$

[0462] 다시 말해, (1) 키 벡터 생성부(420)는, 난수 $\alpha_{0,\,i}$(i=1, …, L+1)와 난수 σ_0을 처리 장치에 의해 생성한다.

[0463] (2) 키 벡터 생성부(420)는, i=1, …, L+1의 각 i에 대하여, 랜덤화 벡터 $k^*_{L,\,ran,\,i}$의 계수를 난수 $\alpha_{0,\,i}$로 승산한 벡터를 가산하여, 벡터 rv를 처리 장치에 의해 생성한다. 또, 랜덤화 벡터 $k^*_{L,\,ran,\,i}$(i=1, …, L+1)에 있어서의 기저 벡터 b^*_i(i=1, …, μ_L)에 대한 계수에는, 술어 벡터의 각 요소가 삽입되어 있다. 그 때문에, 벡터

rv에 있어서의 기저 벡터 $b^*_i(i=1, \cdots, \mu_L)$에 대한 계수에는, 난수가 승산된 술어 벡터의 각 요소가 삽입된다.

[0464] (3) 키 벡터 생성부(420)는, 키 생성용 벡터 $k^*_{L, del, i}(i=\mu_L+1, \cdots, \mu_{L+1})$의 계수에 술어 벡터 $\vec{v}_{L+1}$의 각 요소를 설정한 벡터를 가산하고, 난수 σ_0로 승산하여 벡터 vv를 처리 장치에 의해 생성한다. 다시 말해, 기저 벡터 $b^*_i(i=\mu_L+1, \cdots, \mu_{L+1})$에 대한 계수에는, 술어 벡터의 각 요소가 삽입된다.

[0465] (4) 키 벡터 생성부(420)는, 키 벡터 $k^*_{L, dec}$와, 벡터 rv와 벡터 vv를 가산하여, 키 벡터 $k^*_{L+1, dec}$를 처리 장치에 의해 생성한다.

[0466] (S603 : 랜덤화 벡터 $k^*_{L+1, ran, j}$ 생성 단계)

[0467] 랜덤화 벡터 생성부(430)는, 마스터 공개 키 pk와 키 정보 $\vec{k}^*_L$과 수학식 176에 나타내는 술어 벡터 $\vec{v}_{L+1}$에 근거하여, 수학식 178을 계산하여, 랜덤화 벡터 $k^*_{L+1, ran, j}(j=1, \cdots, L+2)$를 생성한다. 랜덤화 벡터 $k^*_{L+1, ran, j}(j=1, \cdots, L+2)$는, 하위의 키 중, 술어 벡터의 각 요소가 삽입되는 기저 벡터에 대한 계수를 균등하게 분포시키기 위한 벡터이다. 또, 랜덤화 벡터 $k^*_{L+1, ran, j}$는, 제 L+1 층째의 비밀 키의 j번째의 요소이다.

[0468] [수학식 178]

(1)

$$\alpha_{j,i}, \sigma_j \xleftarrow{U} \mathbb{F}_q \qquad (j=1,\ldots,L+2;\ i=1,\ldots,L+1)$$

(2)

$$rv_j := \sum_{i=1}^{L+1} \alpha_{j,i} k^*_{L,\mathrm{ran},i} \qquad (j=1,\ldots,L+2)$$

(3)

$$vv_j := \sigma_j \left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^*_{L,\mathrm{del},i} \right) \qquad (j=1,\ldots,L+2)$$

(4)

$$k^*_{L+1,\mathrm{ran},j} := rv_j + vv_j$$
$$:= \sum_{i=1}^{L+1} \alpha_{j,i} k^*_{L,\mathrm{ran},i} + \sigma_j \left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^*_{L,\mathrm{del},i} \right)$$
$$(j=1,\ldots,L+2)$$

[0469]

[0470] 다시 말해, (1) 랜덤화 벡터 생성부(430)는, 난수 $\alpha_{j, i}(j=1, \cdots, L+2;\ i=1, \cdots, L)$와 난수 $\sigma_j(j=1, \cdots, L+2)$를 처리 장치에 의해 생성한다.

[0471] (2) 랜덤화 벡터 생성부(430)는, j=1, …, L+2의 각 j에 대하여, 랜덤화 벡터 $k^*_{L, ran, i}(i=1, \cdots, L+1)$의 계수를 난수 $\alpha_{j, i}(i=1, \cdots, L+1)$로 승산하여 벡터 rv_j를 처리 장치에 의해 생성한다. 상술한 것처럼, 랜덤화 벡터 $k^*_{L, ran, i}(i=1, \cdots, L+1)$에 있어서의 기저 벡터 $b^*_i(i=1, \cdots, \mu_L)$에 대한 계수에는, 술어 벡터의 각 요소가 삽입되어 있다. 그 때문에, 벡터 rv_j에 있어서의 기저 벡터 $b^*_i(i=1, \cdots, \mu_L)$에 대한 계수에는, 난수가 승산된 술어 벡터의 각 요소가 삽입된다.

[0472] (3) 랜덤화 벡터 생성부(430)는, j=1, …, L+2의 각 j에 대하여, 키 생성용 벡터 $k^*_{L, del, i}(i=\mu_L+1, \cdots, \mu_{L+1})$의 계수에 술어 벡터의 각 요소를 설정한 벡터를 가산하고, 난수 σ_j로 승산하여 벡터 vv_j를 처리 장치에 의해 생성한다. 다시 말해, 기저 벡터 $b^*_i(i=\mu_L+1, \cdots, \mu_{L+1})$에 대한 계수에는, 술어 벡터의 각 요소가 삽입된다.

[0473] (4) 랜덤화 벡터 생성부(430)는, j=1, …, L+2의 각 j에 대하여, 생성한 벡터 rv_j와 벡터 vv_j를 가산하여, 랜덤

화 벡터 $k^{*}_{L+1,\,ran,\,j}$를 처리 장치에 의해 생성한다.

[0474] (S604 : 키 생성용 벡터 $k^{*}_{L+1,\,del,\,j}$ 생성 단계)

[0475] 키 생성용 벡터 생성부(440)는, 마스터 공개 키 pk와 키 정보 $\vec{k}^{*}_{L}$과 수학식 176에 나타내는 술어 벡터 $\vec{v}_{L+1}$에 근거하여, 수학식 179를 계산하여, 키 생성용 벡터 $k^{*}_{L+1,\,del,\,j}$(j=μ_{L+1}+1, …, n)를 처리 장치에 의해 생성한다. 키 생성용 벡터 $k^{*}_{L+1,\,del,\,j}$(j=μ_{L+1}+1, …, n)는, 하위의 비밀 키(하위의 키 벡터)를 생성하기 위한 벡터이다. 또, 키 생성용 벡터 $k^{*}_{L+1,\,del,\,j}$는, 제 L+1 층째의 비밀 키의 j번째의 요소이다.

[0476] [수학식 179]

(1)

$$\alpha_{j,i},\sigma_j,\psi' \xleftarrow{U} \mathbb{F}_q \quad (j=\mu_{L+1}+1,\ldots,n;\ i=1,\ldots,L+1)$$

(2)

$$rv_j := \sum_{i=1}^{L+1}\alpha_{j,i}k^{*}_{L,\mathrm{ran},i} \qquad (j=\mu_{L+1}+1,\ldots,n)$$

(3)

$$vv_j := \sigma_j\left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^{*}_{L,\mathrm{del},i}\right) \qquad (j=\mu_{L+1}+1,\ldots,n)$$

(4)

$$\psi v_j := \psi' k^{*}_{L,\mathrm{del},j} \qquad (j=\mu_{L+1}+1,\ldots,n)$$

(5)

$$\begin{aligned} k^{*}_{L+1,\mathrm{del},j} &:= rv_j + vv_j + \psi v_j \\ &:= \sum_{i=1}^{L+1}\alpha_{j,i}k^{*}_{L,\mathrm{ran},i} + \sigma_j\left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^{*}_{L,\mathrm{del},i}\right) + \psi' k^{*}_{L,\mathrm{del},j} \\ &\qquad (j=\mu_{L+1}+1,\ldots,n) \end{aligned}$$

[0477]

[0478] 다시 말해, (1) 키 생성용 벡터 생성부(440)는, 난수 $\alpha_{j,\,i}$(j=μ_{L+1}+1, …, n; i=1, …, L+1)와, 난수 σ_j(j=μ_{L+1}+1, …, n)와, 난수 ψ'를 처리 장치에 의해 생성한다.

[0479] (2) 키 생성용 벡터 생성부(440)는, j=μ_{L+1}+1, …, n의 각 j에 대하여, 랜덤화 벡터 $k^{*}_{L,\,ran,\,i}$(i=1, …, L+1)의 계수를 난수 $\alpha_{j,\,i}$로 승산한 벡터 rv_j를 처리 장치에 의해 생성한다. 상술한 것처럼, 랜덤화 벡터 $k^{*}_{L,\,ran,\,i}$(i=1, …, L+1)에 있어서의 기저 벡터 b^{*}_{i}(i=1, …, μ_L)에 대한 계수에는, 술어 벡터의 각 요소가 삽입되어 있다. 그 때문에, 벡터 rv_j에 있어서의 기저 벡터 b^{*}_{i}(i=1, …, μ_L)에 대한 계수에는, 난수가 승산된 술어 벡터의 각 요소가 삽입된다.

[0480] (3) 키 생성용 벡터 생성부(440)는, j=μ_{L+1}+1, …, n의 각 j에 대하여, 키 생성용 벡터 $k^{*}_{L,\,del,\,i}$(i=μ_L+1, …, μ_{L+1})의 계수에 술어 벡터의 각 요소를 설정한 벡터를 가산하고, 난수 σ_j로 승산하여 벡터 vv_j를 처리 장치에 의해 생성한다. 다시 말해, 기저 벡터 b^{*}_{i}(i=μ_L+1, …, μ_{L+1})에 대한 계수에는, 술어 벡터의 각 요소가 삽입된다.

[0481] (4) 키 생성용 벡터 생성부(440)는, j=μ_{L+1}+1, …, n의 각 j에 대하여, 키 생성용 벡터 $k^{*}_{L,\,del,\,j}$의 계수를 난수 ψ'로 승산하여, 벡터 ψv_j를 처리 장치에 의해 생성한다. 또, 키 생성용 벡터 $k^{*}_{L,\,del,\,j}$에 있어서의 기저 벡터 b^{*}_{j}(j=μ_{L+1}+1, …, n)에 대한 계수에는, 술어 벡터의 요소가 삽입되어 있다. 그 때문에, 벡터 ψv_j(j=μ_{L+1}+1,

…, n)에 있어서의 기저 벡터 b^*_j에 대한 계수에는, 난수가 승산된 술어 벡터의 요소가 삽입된다.

[0482] (5) 키 생성용 벡터 생성부(440)는, $j=\mu_{L+1}+1$, …, n의 각 j에 대하여, 생성한 벡터 rv_j와, 벡터 vv_j와, 벡터 ψv_j를 가산하여, 키 생성용 벡터 $k^*_{L+1,\,del,\,j}$($j=\mu_{L+1}+1$, …, n)를 처리 장치에 의해 생성한다.

[0483] 즉, (S602)로부터 (S604)에 있어서, 키 벡터 생성부(420)와 랜덤화 벡터 생성부(430)와 키 생성용 벡터 생성부(440)는, 수학식 180에 나타내는 $Delegate_L$ 알고리즘을 실행하여, 키 벡터 $k^*_{L+1,\,dec}$와, 랜덤화 벡터 $k^*_{L+1,\,ran,\,j}$(j=1, …, L+2)와, 키 생성용 벡터 $k^*_{L+1,\,del,\,j}$($j=\mu_{L+1}+1$, …, n)를 포함하는 제 L+1 층째의 비밀 키(키 정보 $\vec{k}^*_{L+1}$)를 처리 장치에 의해 생성한다.

[0484] [수학식 180]

$$\mathrm{Delegate}_L\left(\mathsf{pk},\vec{k}^*_L,\vec{v}_{L+1}:=\left(v_{\mu_L+1},\ldots,v_{\mu_{L+1}}\right)\right):$$

$$\alpha_{j,i},\sigma_j,\psi' \xleftarrow{U} \mathbb{F}_q \quad \text{for } j=0,\ldots,L+2,\mu_{L+1}+1,\ldots,n;\ i=1,\ldots,L+1,$$

$$k^*_{L+1,\mathsf{dec}} := k^*_{L,\mathsf{dec}} + \sum_{i=1}^{L+1}\alpha_{0,i}k^*_{L,\mathsf{ran},i} + \sigma_0\left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^*_{L,\mathsf{del},i}\right),$$

$$k^*_{L+1,\mathsf{ran},j} := \sum_{i=1}^{L+1}\alpha_{j,i}k^*_{L,\mathsf{ran},i} + \sigma_j\left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^*_{L,\mathsf{del},i}\right)$$

$$\text{for } j=1,\ldots,L+2,$$

$$k^*_{L+1,\mathsf{del},j} := \sum_{i=1}^{L+1}\alpha_{j,i}k^*_{L,\mathsf{ran},i} + \sigma_j\left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^*_{L,\mathsf{del},i}\right) + \psi' k^*_{L,\mathsf{del},j}$$

$$\text{for } j=\mu_{L+1}+1,\ldots,n,$$

$$\text{return } \vec{k}^*_{L+1} := \begin{pmatrix} k^*_{L+1,\mathsf{dec}}, k^*_{L+1,\mathsf{ran},1},\ldots,k^*_{L+1,\mathsf{ran},L+2}, \\ k^*_{L+1,\mathsf{del},\mu_{L+1}+1},\ldots k^*_{L+1,\mathsf{del},n} \end{pmatrix}$$

[0485]

[0486] (S605 : 키 배포 단계)

[0487] 키 배포부(440)는, 키 벡터 생성부(420)와 랜덤화 벡터 생성부(430)와 키 생성용 벡터 생성부(440)가 생성한 키 정보 $\vec{k}^*_{L+1}$을 하위의 복호 장치(300)에 통신 장치를 통해 송신한다. 여기서, 키 정보 $\vec{k}^*_{L+1}$은 비밀리에 복호 장치(300)에 송신되지만, 키 정보 $\vec{k}^*_{L+1}$을 비밀리에 복호 장치(300)에 송신하는 방법에 관해서는, 어떠한 방법이더라도 상관없다. 예컨대, 종래의 암호 처리를 사용하여 송신하더라도 좋다.

[0488] 이상과 같이, 암호 처리 시스템(10)이 실현하는 암호 처리는, 비특허 문헌 18에서 제안되어 있는 암호 처리보다 안전성이 높아, 표준의 모델(Standard Model)에 있어서의 안전성을 증명할 수 있다.

[0489] 이 이유는, 주로 이하의 (1)로부터 (3)의 특징 때문이다.

[0490] (1) 암호 처리에 이용하고 있는 공간 V와 V^*는, N(=n+2+r+s)차원인데 비하여, 암호화 장치(200)가 암호 벡터 c_1을 생성하는데 이용하고 있는 기저 벡터는, 기저 벡터 b_i(i=1, …, n+2)의 n+2차원뿐이다. 또한, 복호 장치(300)가 복호에 이용하고 있는 기저 벡터는, 기저 벡터 b^*_i(i=1, …, n+2+r)의 n+2+r차원뿐이다. 다시 말해, 암호 처리에서는, 공간 V와 V^* 중, s차원(기저 벡터 $b_{n+2+r+1}$, …, $b_{n+2+r+s}$)을 사용하지 않는다. 바꿔 말하면, 암호 처리에서 사용하는 n+2+r차원의 공간보다 s차원만큼 차원수가 많은 공간에 있어서 마스터 비밀 키나 마스터 공개 키가 생성된다. 그 때문에, 암호 처리에서 사용하는 n+2+r차원의 공간에서 마스터 비밀 키나 마스터 공개 키를 생성하는 경우에 비하여, 마스터 비밀 키나 마스터 공개 키를 생성하는데 이용되는 선형 변환 X 등의 랜덤 요소가 s차원만큼 증가한다. 랜덤 요소가 증가하는 것에 의해 안전성이 높아진다.

[0491] (2) 키 생성 장치(100)가 생성하는 키 벡터 $k^*_{L,\,dec}$와, 랜덤화 벡터 $k^*_{L,\,ran,\,j}$(j=1, …, L+1)와, 키 생성용 벡터 $k^*_{L,\,del,\,j}$($j=\mu_L+1$, …, n)에 랜덤 요소가 더해지고 있다. 다시 말해, 키 벡터 $k^*_{L,\,dec}$와, 랜덤화 벡터 $k^*_{L,\,ran,}$

$_{j}$(j=1, …, L+1)와, 키 생성용 벡터 $k^{*}_{L,\,del,\,j}$(j=μ_L+1, …, n)의 각각에, 기저 벡터 b^{*}_{n+3}에 난수를 설정하고 있다. 키 벡터 $k^{*}_{L,\,dec}$와, 랜덤화 벡터 $k^{*}_{L,\,ran,\,j}$(j=1, …, L+1)와, 키 생성용 벡터 $k^{*}_{L,\,del,\,j}$(j=μ_L+1, …, n)에 랜덤 요소가 더해지는 것에 의해, 안전성이 높아진다.

[0492] (3) 키 위양 장치(400)가 하위의 키를 생성하는 경우에, 랜덤화 벡터를 이용하여 생성한다. 이에 의해, 하위의 키의 소정의 기저 벡터에 대한 계수를 랜덤화할 수 있어, 하위의 키를 생성하는 것에 의해, 키의 안전성이 열화되지 않는다.

[0493] 여기서, 랜덤화 벡터를 이용하지 않는 경우, 키 정보 $\vec{k}^{*}_{L}$로부터 생성되는 2개의 하위의 키 벡터 $k^{*}_{L+1,\,dec}$(A)와 키 벡터 $k^{*}_{L+1,\,dec}$(B)는, 수학식 181과 같이 된다.

[0494] [수학식 181]

$$k^{*}_{L+1,\mathrm{dec}}(\mathrm{A}) := k^{*}_{L,\mathrm{dec}} + \sigma_A\left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^{*}_{L,\mathrm{del},i}\right)$$
$$:= \sum_{t=1}^{L}\sigma_{0,t}\left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b^{*}_i\right) + \sigma_A\left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^{*}_{L,\mathrm{del},i}\right) + \eta_0 b^{*}_{n+1} + (1-\eta_0) b^{*}_{n+2}$$

$$k^{*}_{L+1,\mathrm{dec}}(\mathrm{B}) := k^{*}_{L,\mathrm{dec}} + \sigma_B\left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^{*}_{L,\mathrm{del},i}\right)$$
$$:= \sum_{t=1}^{L}\sigma_{0,t}\left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b^{*}_i\right) + \sigma_B\left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^{*}_{L,\mathrm{del},i}\right) + \eta_0 b^{*}_{n+1} + (1-\eta_0) b^{*}_{n+2}$$

[0495]

[0496] 다시 말해, 랜덤화 벡터를 이용하지 않는 경우, 키 벡터 $k^{*}_{L,\,dec}$에 포함되는 숨어 정보가 설정된 기저 벡터 b^{*}_{i}(i=1, …, μ_L)의 계수는, 키 벡터 $k^{*}_{L+1,\,dec}$(A)와 키 벡터 $k^{*}_{L+1,\,dec}$(B)의 사이에 공통이 되어 버린다.

[0497] 그러나, 랜덤화 벡터를 이용하는 경우, 키 정보 $\vec{k}^{*}_{L}$로부터 생성되는 2개의 하위의 키 벡터 $k^{*}_{L+1,\,dec}$(A)와 키 벡터 $k^{*}_{L+1,\,dec}$(B)는, 수학식 182와 같이 된다.

[0498] [수학식 182]

$$k^{*}_{L+1,\mathrm{dec}}(\mathrm{A}) := k^{*}_{L,\mathrm{dec}} + \sum_{i=1}^{L+1}\alpha_{A,i} k^{*}_{L,\mathrm{ran},i} + \sigma_A\left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^{*}_{L,\mathrm{del},i}\right)$$
$$:= \sum_{t=1}^{L}\sigma_{0,t}\left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b^{*}_i\right) + \sum_{i=1}^{L+1}\alpha_{A,i} k^{*}_{L,\mathrm{ran},i} + \sigma_A\left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^{*}_{L,\mathrm{del},i}\right) + \eta_0 b^{*}_{n+1} + (1-\eta_0) b^{*}_{n+2}$$

$$k^{*}_{L+1,\mathrm{dec}}(\mathrm{B}) := k^{*}_{L,\mathrm{dec}} + \sum_{i=1}^{L+1}\alpha_{B,i} k^{*}_{L,\mathrm{ran},i} + \sigma_B\left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^{*}_{L,\mathrm{del},i}\right)$$
$$:= \sum_{t=1}^{L}\sigma_{0,t}\left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b^{*}_i\right) + \sum_{i=1}^{L+1}\alpha_{A,i} k^{*}_{L,\mathrm{ran},i} + \sigma_B\left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^{*}_{L,\mathrm{del},i}\right) + \eta_0 b^{*}_{n+1} + (1-\eta_0) b^{*}_{n+2}$$

[0499]

[0500] 다시 말해, 랜덤화 벡터를 이용하는 경우, 키 벡터 $k^{*}_{L+1,\,dec}$(A)에는, 난수 $\alpha_{A,\,i}$로 계수의 값이 균등하게 분포된 랜덤화 벡터 $k^{*}_{L,\,ran,\,i}$가 더해지고, 키 벡터 $k^{*}_{L+1,\,dec}$(B)에는, 난수 $\alpha_{B,\,i}$로 계수의 값이 균등하게 분포된 랜덤화 벡터 $k^{*}_{L,\,ran,\,i}$가 더해진다. 여기서, 랜덤화 벡터 $k^{*}_{L,\,ran,\,i}$에는, 기저 벡터 b^{*}_{i}(i=1, …, μ_L)가 포함되어 있다. 따라서, 키 벡터 $k^{*}_{L+1,\,dec}$(A)와 키 벡터 $k^{*}_{L+1,\,dec}$(B)에 있어서의 기저 벡터 b^{*}_{i}(i=1, …, μ_L)의 계수의 값은 균등

하게 분포되어 있다. 다시 말해, 키 벡터 $k^{*}_{L+1,\,dec}(A)$와 키 벡터 $k^{*}_{L+1,\,dec}(B)$에 있어서, 술어 정보가 설정된 기저 벡터 $b^{*}_{i}(i=1, \cdots, \mu_L)$의 계수는 다르다.

[0501] 또한, 상기 설명에서는, N(=n+2+r+s)차원 벡터 공간에서 암호 처리를 실현했지만, 권한 위양이 없는 암호 처리이면, n은 1 이상의 정수이다. 또한, 권한 위양을 갖는 암호 처리이면, n은 2 이상의 정수이다. 또한, r은 0 이상의 정수이다. 또한, s는 1 이상의 정수이다.

[0502] r이 0인 경우에는, 키 벡터 $k^{*}_{L,\,dec}$와, 랜덤화 벡터 $k^{*}_{L,\,ran,\,j}(j=1, \cdots, L+1)$와, 키 생성용 벡터 $k^{*}_{L,\,del,\,j}(j=\mu_L+1, \cdots, n)$에 랜덤 요소가 더해지지 않는다.

[0503] 또, 상술한 것처럼, (S402)에 있어서, 암호화 장치(200)가 기저 벡터 b_{n+2}를 이용하여, 벡터 rv를 생성하는 것은 필수는 아니다. 벡터 rv를 생성하지 않는 것이면, N(=n+1+r+s)차원 벡터 공간에서 암호 처리를 실현할 수 있다.

[0504] 따라서, 권한 위양이 없는 암호 처리이면, N은 2 이상의 정수이며, 권한 위양을 갖는 암호 처리이면, N은 3 이상의 정수이다.

[0505] 또한, 상술한 암호 처리에서는, 쌍대 페어링 벡터 공간인 것의 조건에 포함되어 있던 디스토션 사상을 이용하고 있지 않다. 디스토션 사상에 대해서는, 암호 처리를 실현하는 알고리즘에서는 사용하지 않고, 암호 처리의 안전성을 증명하기 위해 사용한다. 따라서, 상술한 암호 처리는, 디스토션 사상이 없는 공간이더라도 성립한다고 할 수 있다. 즉, 상술한 암호 처리를 실현하는 공간에 디스토션 사상이 있는 것은, 필수는 아니다. 이하에 설명하는 암호 처리에 대해서도 같다.

[0506] 또한, 상기 설명에서는, 계층적 술어 암호에 대하여 설명했다. 다음으로, 계층적 술어 키 비닉 방식에 대하여 설명한다. 계층적 술어 키 비닉 방식에 대하여, 상술한 계층적 술어 암호와 다른 부분만을 설명한다.

[0507] 도 17은 계층적 술어 키 비닉 방식을 실현하는 암호 처리 시스템(10)의 기능을 나타내는 기능 블록도이다.

[0508] 여기서, 키 생성 장치(100)의 처리와 키 위양 장치(400)의 처리는, 상술한 계층적 술어 암호의 경우와 같다. 그래서, 여기에서는, 암호화 장치(200)의 처리와 복호 장치(300)의 처리만을 설명한다.

[0509] 도 18은 암호화 장치(200)의 동작을 나타내는 플로우차트이다. 도 19는 복호 장치(300)의 동작을 나타내는 플로우차트이다.

[0510] 암호화 장치(200)의 기능과 동작에 대하여 설명한다.

[0511] 도 17에 나타내는 암호화 장치(200)는, 도 11에 나타내는 암호화 장치(200)가 구비하는 기능에 더하여, 세션 키 생성부(260)를 구비한다. 또, 도 17에 나타내는 암호화 장치(200)는, 도 11에 나타내는 암호화 장치(200)가 구비하는 암호 정보 생성부(230)는 구비하고 있지 않다.

[0512] (S701)과 (S702)는, (S401)과 (S402)와 같다.

[0513] (S703 : 데이터 송신 단계)에서는, (S702)에서 암호 벡터 생성부(220)가 생성한 암호 벡터 c_1을 복호 장치(300)에 통신 장치를 통해 송신한다. 다시 말해, 계층적 술어 키 비닉 방식에서는, 평문 정보 m을 삽입한 암호 정보 c_2는 생성되지 않고, 복호 장치(300)에 송신되지 않는다.

[0514] (S704 : 세션 키 생성 단계)에서는, 세션 키 생성부(260)가 수학식 183을 처리 장치에 의해 계산하여 세션 키 K를 생성한다.

[0515] [수학식 183]

$$K := g_T^{\zeta}$$

여기서,

$$g_T = e(a_i, a_i^{*}) \neq 1$$

[0516] 이다.

[0517] 즉, 암호화 장치(200)는, 수학식 184에 나타내는 Enc 알고리즘을 실행하여, 암호 벡터 c_1과 세션 키 K를 생성한다.

[0518] [수학식 184]

$$\mathsf{Enc}\left(\mathsf{pk},\left(\vec{x}_1,\ldots,\vec{x}_L\right):=\left(\left(x_1,\ldots,x_{\mu_1}\right),\ldots,\left(x_{\mu_{L-1}+1},\ldots,x_{\mu_L}\right)\right)\right):$$
$$\left(\vec{x}_{L+1},\ldots,\vec{x}_d\right)\xleftarrow{\mathrm{U}}\mathbb{F}_q{}^{\mu_{L+1}-\mu_L}\times\cdots\times\mathbb{F}_q{}^{n-\mu_{d-1}},$$
$$\delta_1,\ldots,\delta_d,\delta_{n+3},\zeta\xleftarrow{\mathrm{U}}\mathbb{F}_q,$$
$$c_1:=\sum_{t=1}^{d}\delta_t\left(\sum_{i=\mu_{t-1}+1}^{\mu_t}x_i b_i\right)+\zeta d_{n+1}+\delta_{n+3}b_{n+3},\ K:=g_T^{\zeta},$$

[0519] return (c_1,K)

[0520] 복호 장치(300)의 기능과 동작에 대하여 설명한다.

[0521] 도 17에 나타내는 복호 장치(300)는, 도 11에 나타내는 복호 장치(300)와 같은 기능 구성이다.

[0522] (S801 : 벡터 입력 단계)

[0523] 벡터 입력부(310)는, 암호화 장치(200)의 데이터 송신부(240)가 송신한 암호 벡터 c_1을 통신 장치를 통해 수신하여 입력한다.

[0524] (S802 : 복호 단계)

[0525] 페어링 연산부(330)는, 마스터 공개 키 pk와 제 L 층째의 비밀 키의 선두 요소인 키 벡터 $k^*_{L,\,dec}$에 근거하여, 수학식 185를 처리 장치에 의해 계산하여 세션 키 K를 생성한다.

[0526] [수학식 185]

[0527] $$K':=e\left(c_1,k^*_{L,\mathsf{dec}}\right)$$

[0528] 다시 말해, 페어링 연산부(330)는, 벡터 입력부(310)가 입력한 암호 벡터 c_1과, 키 벡터 기억부(320)가 기억 장치에 기억한 키 벡터 $k^*_{L,\,dec}$에 대하여, 페어링 연산 e를 처리 장치에 의해 행한다. 이에 의해, 페어링 연산부(330)는, 암호화 장치(200)가 삽입한 ζ에 관한 값인 g_T^{ζ}(=K)를 계산한다.

[0529] 즉, 복호 장치(300)는, 수학식 186에 나타내는 Dec 알고리즘을 실행하여, 세션 키 K'(=K)를 생성한다.

[0530] [수학식 186]

$$\mathsf{Dec}\left(\mathsf{pk},k^*_{L,\mathsf{dec}},c_1\right):K':=e\left(c_1,k^*_{L,\mathsf{dec}}\right),$$

[0531] return K'

[0532] 이상과 같이, 계층적 술어 키 비닉 방식에 의하면, 암호화 장치(200)로부터 복호 장치(300)에, 세션 키 K를 비밀리에 송신할 수 있다. 다시 말해, 암호화 장치(200)와 복호 장치(300)의 사이에 세션 키를 공유할 수 있다.

[0533] 실시의 형태 3.

[0534] 실시의 형태 3에서는, 실시의 형태 2에서 설명한 계층적 술어 암호와 계층적 술어 키 비닉 방식보다 일반화된 권한 위양을 갖는 술어 암호에 대하여 설명한다.

[0535] 상술한 것처럼, 실시의 형태 2에서 설명한 계층적 술어 암호와 계층적 술어 키 비닉 방식에서는, 도 16에 나타내는 바와 같이 기저 벡터를 사용했다. 다시 말해, n+2+r+s개의 기저 벡터 중, n개의 기저 벡터를 속성 벡터나 술어 벡터를 위한 기저 벡터로서, 계층 구조를 나타내기 위해 사용했다. 특히, 처음의 μ_1개의 기저 벡터를 제 1 층째의 속성 벡터나 술어 벡터를 위한 기저 벡터로 하고, $\mu_2-\mu_1$개의 기저 벡터를 제 2 층째의 속성 벡터나 술어 벡터를 위한 기저 벡터로 하고, 이하 마찬가지로, $\mu_L-\mu_{L-1}$개의 기저 벡터를 제 L 층째의 속성 벡터나 술어 벡터를 위한 기저 벡터로 했다.

[0536] 그리고, 제 L 층째의 키 벡터 $k^{*}_{L,\ dec}$를 수학식 164에 나타내는 바와 같이 계산했다. 다시 말해, 제 L 층째의 키 벡터 $k^{*}_{L,\ dec}$는, 기저 벡터 b^{*}_{i}(i=1, …, L)에 대한 계수로서 술어 벡터의 각 요소가 할당되고, 기저 벡터 b^{*}_{i}(i=L+1, …, n)에 대한 계수로서 0이 할당되었다.

[0537] 또한, 제 L 층째의 암호 벡터 c_1을 수학식 170에 나타내는 바와 같이 계산했다. 다시 말해, 제 L 층째의 암호 벡터 c_1은, 기저 벡터 b_i(i=1, …, L)에 대한 계수로서 속성 벡터의 각 요소가 할당되고, 기저 벡터 b_i(i=L+1, …, n)에 대한 계수로서 난수가 할당되었다.

[0538] 이에 의해, 계층적으로 권한 위양하는 것이 실현되었다.

[0539] 실시의 형태 3에서 설명하는 술어 암호(술어 키 비닉 방식)에서는, 실시의 형태 2의 경우와 같이, n+2+r+s개의 기저 벡터 중, n개의 기저 벡터를 속성 벡터나 술어 벡터를 위한 기저 벡터로서 사용한다. 그러나, 어느 키이더라도(상위의 키이더라도, 하위의 키이더라도), n개의 기저 벡터 모두를 술어 벡터를 위한 기저 벡터로 한다. 다시 말해, n개의 기저 벡터 모두를 항상 속성 벡터나 술어 벡터를 위한 기저 벡터로 한다.

[0540] 그리고, 키 벡터 $k^{*}_{L,\ dec}$는, 기저 벡터 b^{*}_{i}(i=1, …, n)에 대한 계수로서 술어 벡터의 각 요소가 할당된다. 또한, 제 L 층째의 암호 벡터 c_1은, 기저 벡터 b_i(i=1, …, n)에 대한 계수로서 속성 벡터의 각 요소가 할당된다.

[0541] 다시 말해, n개의 기저 벡터에 대하여 계층 구조라고 하는 개념은 없다. 또한, 비밀 키가 계층적으로 권한 위양되는 개념은 없다. 그 때문에, 실시의 형태 2에서 설명한 암호 방식에 비하여, 보다 자유도가 높은 권한 위양이 가능해진다.

[0542] 우선, 권한 위양을 갖는 술어 암호를 실현하는 경우에 대하여 설명한다.

[0543] 도 20은 권한 위양을 갖는 술어 암호를 실현하는 암호 처리 시스템(10)의 기능을 나타내는 기능 블록도이다. 또, 도 20에 나타내는 암호 처리 시스템(10)이 구비하는 기능은, 도 11에 나타내는 암호 처리 시스템(10)이 구비하는 기능과 같다.

[0544] 권한 위양을 갖는 술어 암호를 실현하는 경우에 있어서의 실시의 형태 3에 따른 암호 처리 시스템(10)의 동작의 흐름은, 실시의 형태 2에 따른 암호 처리 시스템(10)의 동작의 흐름과 같다. 그래서, 도 20과, 도 12로부터 도 16에 근거하여, 실시의 형태 3에 따른 암호 처리 시스템(10)의 기능과 동작에 대하여 설명한다.

[0545] 키 생성 장치(100)의 기능과 동작에 대하여 설명한다.

[0546] (S301 : 마스터 키 생성 단계)

[0547] 실시의 형태 2에 있어서의 (S301)과 같이, 마스터 키 생성부(110)는, 수학식 187을 계산하여, 마스터 공개 키 pk와 마스터 비밀 키 sk를 처리 장치에 의해 생성하여 마스터 키 기억부(120)에 기억한다.

[0548] [수학식 187]

$$\mathrm{Setup}\left(1^{\lambda},\vec{\mu}:=n\right):\left(\mathrm{param},\mathbb{B},\mathbb{B}^{*}\right)\xleftarrow{R}\mathcal{G}_{\mathrm{ob}}\left(1^{\lambda},n+2+r+s\right),$$
$$\hat{\mathbb{B}}:=\left(b_1,\ldots,b_n,b_{n+1},b_{n+2}\right),$$
$$\text{return sk}:=\left(X,\mathbb{B}^{*}\right),\ \mathrm{pk}:=\left(1^{\lambda},\mathrm{param},\hat{\mathbb{B}}\right).$$

여기서,

$$\mathcal{G}_{\mathrm{ob}}\left(1^{\lambda},N\right):\mathrm{param}:=\left(q,\mathbb{V},\mathbb{V}^{*},\mathbb{G}_T,\mathbb{A},\mathbb{A}^{*}\right)\xleftarrow{R}\mathcal{G}_{\mathrm{dpvs}}\left(1^{\lambda},N\right),$$
$$X:=\left(\chi_{i,j}\right)\xleftarrow{U}GL\left(N,\mathbb{F}_q\right),\ \left(\upsilon_{i,j}\right):=\left(X^{\mathrm{T}}\right)^{-1},$$
$$b_i=\sum_{j=1}^{N}\chi_{i,j}a_j,\ \mathbb{B}:=\left(b_1,\ldots,b_N\right),$$
$$b_i^{*}=\sum_{j=1}^{N}\upsilon_{i,j}a_j^{*},\ \mathbb{B}^{*}:=\left(b_1^{*},\ldots,b_N^{*}\right),$$
$$\text{return}\ \left(\mathrm{param},\mathbb{B},\mathbb{B}^{*}\right)$$

[0549] 이다.

[0550] (S302 : 키 벡터 $k^{*}_{L,\,dec}$ 생성 단계)

[0551] 키 벡터 생성부(130)는, 마스터 공개 키 pk와 마스터 비밀 키 sk와, 수학식 188에 나타내는 술어 벡터 ($\vec{v}_1$, …, $\vec{v}_L$)에 근거하여, 수학식 189를 계산하여, 제 L 층째(레벨 L)의 비밀 키의 선두 요소인 키 벡터 $k^{*}_{L,\,dec}$를 처리 장치에 의해 생성한다.

[0552] [수학식 188]

[0553] $$\left(\vec{v}_1,\ldots,\vec{v}_L\right):=\left(\left(v_{1,1},\ldots,v_{1,n}\right),\ldots,\left(v_{L,1},\ldots,v_{L,n}\right)\right)$$

[0554] [수학식 189]

(1)

$$\sigma_{\mathrm{dec},t},\eta_{\mathrm{dec},h}\xleftarrow{U}\mathbb{F}_q\qquad\left(t=1,\ldots,L;\ h=1,\ldots,r\right)$$

(2)

$$vv:=\sum_{t=1}^{L}\sigma_{\mathrm{dec},t}\left(\sum_{i=1}^{n}v_{t,i}b_i^{*}\right)$$

(3)

$$rv:=\sum_{h=1}^{r}\eta_{\mathrm{dec},h}b_{n+2+h}^{*}$$

(4)

$$k_{L,\mathrm{dec}}^{*}:=vv+b_{n+1}^{*}+rv$$

[0555] $$:=\sum_{t=1}^{L}\sigma_{\mathrm{dec},t}\left(\sum_{i=1}^{n}v_{t,i}b_i^{*}\right)+b_{n+1}^{*}+\sum_{h=1}^{r}\eta_{\mathrm{dec},h}b_{n+2+h}^{*}$$

[0556] (S303 : 랜덤화 벡터 $k^{*}_{L,\,ran,\,j}$ 생성 단계)

[0557] 랜덤화 벡터 생성부(140)는, 마스터 공개 키 pk와 마스터 비밀 키 sk와, 수학식 188에 나타내는 술어 벡터 ($\vec{v}_1$, …, $\vec{v}_L$)에 근거하여, 수학식 190을 계산하여, 랜덤화 벡터 $k^{*}_{L,\,ran,\,j}$(j=1, …, L+1)를 생성한다.

[0558] [수학식 190]

(1)

$$\sigma_{\mathrm{ran},j,t},\eta_{\mathrm{ran},j,h} \xleftarrow{U} \mathbb{F}_q \qquad (j=1,\ldots,L+1;\ t=1,\ldots,L;\ h=1,\ldots,r)$$

(2)

$$vv_j := \sum_{t=1}^{L} \sigma_{\mathrm{ran},j,t}\left(\sum_{i=1}^{n} v_{t,i} b_i^*\right) \qquad (j=1,\ldots,L+1)$$

(3)

$$rv_j := \sum_{h=1}^{r} \eta_{\mathrm{ran},j,h} b_{n+2+h}^* \qquad (j=1,\ldots,L+1)$$

(4)

$$k_{L,\mathrm{ran},j}^* := vv_j + rv_j$$

$$:= \sum_{t=1}^{L} \sigma_{\mathrm{ran},j,t}\left(\sum_{i=1}^{n} v_{t,i} b_i^*\right) + \sum_{h=1}^{r} \eta_{\mathrm{ran},j,h} b_{n+2+h}^* \qquad (j=1,\ldots,L+1)$$

[0559]

[0560] (S304 : 키 생성용 벡터 $k^*_{L,\,del,\,j}$ 생성 단계)

[0561] 키 생성용 벡터 생성부(150)는, 마스터 공개 키 pk와 마스터 비밀 키 sk와, 수학식 188에 나타내는 숄어 벡터 ($\vec{v}_1$, …, $\vec{v}_L$)에 근거하여, 수학식 191을 계산하여, 키 생성용 벡터 $k^*_{L,\,del,\,j}$(j=1, …, n)를 처리 장치에 의해 생성한다.

[0562] [수학식 191]

(1)

$$\sigma_{\mathrm{del},j,t},\eta_{\mathrm{del},j,h},\psi \xleftarrow{U} \mathbb{F}_q \qquad (j=1,\ldots,n;\ t=1,\ldots,L;\ h=1,\ldots,r)$$

(2)

$$vv_j := \sum_{t=1}^{L} \sigma_{\mathrm{del},j,t}\left(\sum_{i=1}^{n} v_{t,i} b_i^*\right) \qquad (j=1,\ldots,n)$$

(3)

$$\psi v_j := \psi b_j^* \qquad (j=1,\ldots,n)$$

(4)

$$rv_j := \sum_{h=1}^{r} \eta_{\mathrm{del},j,h} b_{n+2+h}^* \qquad (j=1,\ldots,n)$$

(5)

$$k_{L,\mathrm{del},j}^* := vv_j + \psi v_j + rv_j$$

$$:= \sum_{t=1}^{L} \sigma_{\mathrm{del},j,t}\left(\sum_{i=1}^{n} v_{t,i} b_i^*\right) + \psi b_j^* + \sum_{h=1}^{r} \eta_{\mathrm{del},j,h} b_{n+2+h}^* \qquad (j=1,\ldots,n)$$

[0563]

[0564] 즉, (S302)로부터 (S304)에 있어서, 키 벡터 생성부(130)와 랜덤화 벡터 생성부(140)와 키 생성용 벡터 생성부(150)는, 수학식 192에 나타내는 GenKey 알고리즘을 처리 장치에 의해 실행한다. 이에 의해, 키 벡터 $k^*_{L,\,dec}$와, 랜덤화 벡터 $k^*_{L,\,ran,\,j}$(j=1, …, L+1)와, 키 생성용 벡터 $k^*_{L,\,del,\,j}$(j=1, …, n)를 포함하는 제 L 층째의 비밀 키(키 정보 $\vec{k}^*_L$)가 생성된다.

[0565] [수학식 192]

$$\mathsf{GenKey}(\mathsf{pk},\mathsf{sk},(\vec{v}_1,\ldots,\vec{v}_L)) := \left((v_{1,1},\ldots,v_{1,n}),\ldots,(v_{L,1},\ldots,v_{L,n})\right):$$

$$\sigma_{\mathsf{dec},t},\eta_{\mathsf{dec},\mathsf{h}},\sigma_{\mathsf{ran},j,t},\eta_{\mathsf{ran},j,h}\,(j=1,\ldots,L+1),$$

$$\sigma_{\mathsf{del},j,t},\eta_{\mathsf{del},j,h}\,(j=1,\ldots,n),\ \psi \xleftarrow{\mathrm{U}} \mathbb{F}_q$$

$$\text{for } t=1,\ldots,L;\ h=1,\ldots,r,$$

$$k^*_{L,\mathsf{dec}} := \sum_{t=1}^{L}\sigma_{\mathsf{dec},t}\left(\sum_{i=1}^{n}v_{t,i}b^*_i\right)+b^*_{n+1}+\sum_{h=1}^{r}\eta_{\mathsf{dec},h}b^*_{n+2+h},$$

$$k^*_{L,\mathsf{ran},j} := \sum_{t=1}^{L}\sigma_{\mathsf{ran},j,t}\left(\sum_{i=1}^{n}v_{t,i}b^*_i\right)+\sum_{h=1}^{r}\eta_{\mathsf{ran},j,h}b^*_{n+2+h}$$

$$\text{for } j=1,\ldots,L+1,$$

$$k^*_{L,\mathsf{del},j} := \sum_{t=1}^{L}\sigma_{\mathsf{del},j,t}\left(\sum_{i=1}^{n}v_{t,i}b^*_i\right)+\psi b^*_j+\sum_{h=1}^{r}\eta_{\mathsf{del},j,h}b^*_{n+2+h}$$

$$\text{for } j=1,\ldots,n,$$

[0566] $$\text{return } \vec{k}^*_L := \left(k^*_{L,\mathsf{dec}},k^*_{L,\mathsf{ran},1},\ldots,k^*_{L,\mathsf{ran},L+1},k^*_{L,\mathsf{del},1},\ldots,k^*_{L,\mathsf{del},n}\right)$$

[0567] (S305 : 키 배포 단계)

[0568] 실시의 형태 2에 있어서의 (S305)와 같이, 키 배포부(160)는, 마스터 키 생성부(110)가 생성한 마스터 공개 키와, 키 벡터 생성부(130)와 랜덤화 벡터 생성부(140)와 키 생성용 벡터 생성부(150)가 생성한 키 정보 $\vec{k}^*_L$을 복호 장치(300)에 통신 장치를 통해 송신한다. 또한, 키 배포부(160)는, 마스터 공개 키를 암호화 장치(200)에 통신 장치를 통해 송신한다.

[0569] 암호화 장치(200)의 기능과 동작에 대하여 설명한다.

[0570] (S401 : 송신 정보 설정 단계)

[0571] 실시의 형태 2에 있어서의 (S401)과 같이, 송신 정보 설정부(210)는, 마스터 공개 키 pk에 근거하여, 수학식 193을 처리 장치에 의해 계산하여 송신 정보 벡터 ζ_V를 생성한다.

[0572] [수학식 193]

(1)

$$\zeta \xleftarrow{\mathrm{U}} \mathbb{F}_q$$

(2)

[0573] $$\zeta v := \zeta b_{n+1}$$

[0574] (S402 : 암호 벡터 c_1 생성 단계)

[0575] 암호 벡터 생성부(220)는, 마스터 공개 키 pk와, 수학식 194에 나타내는 속성 벡터 ($\vec{x}_1$, …, $\vec{x}_L$)에 근거하여, 수학식 195를 처리 장치에 의해 계산하여 암호 벡터 c_1을 생성한다.

[0576] [수학식 194]

[0577] $$\left(\vec{x}_1,\ldots,\vec{x}_L\right) := \left((x_{1,1},\ldots,x_{1,n}),\ldots,(x_{L,1},\ldots,x_{L,n})\right)$$

[0578] [수학식 195]

(1)

$$\delta_1,\ldots,\delta_L,\delta_{n+2},\zeta \xleftarrow{U} \mathbb{F}_q$$

(2)

$$xv := \sum_{t=1}^{L}\delta_t\left(\sum_{i=1}^{n}x_{t,i}b_i\right)$$

(3)

$$rv := \delta_{n+2}b_{n+2}$$

(4)

$$c_1 := xv + \zeta v + rv$$

[0579] $$:= \sum_{t=1}^{L}\delta_t\left(\sum_{i=1}^{n}x_{t,i}b_i\right) + \zeta b_{n+1} + \delta_{n+2}b_{n+2}$$

[0580] (S403 : 암호 정보 c_2 생성 단계)

[0581] 실시의 형태 2에 있어서의 (S403)과 같이, 암호 정보 생성부(230)는, 평문 정보 m에 근거하여, 수학식 196을 처리 장치에 의해 계산하여 암호 정보 c_2를 생성한다.

[0582] [수학식 196]

[0583] $$c_2 := g_T^{\zeta}m$$

[0584] (S404 : 데이터 송신 단계)

[0585] 실시의 형태 2에 있어서의 (S404)와 같이, 데이터 송신부(240)는, 암호 벡터 생성부(220)가 생성한 암호 벡터 c_1과, 암호 정보 생성부(230)가 생성한 암호 정보 c_2를 복호 장치(300)에 통신 장치를 통해 송신한다.

[0586] 즉, 암호화 장치(200)는, 수학식 197에 나타내는 Enc 알고리즘을 실행하여, 암호 벡터 c_1과 암호 정보 c_2를 생성한다.

[0587] [수학식 197]

[0588] $$\mathsf{Enc}\left(\mathsf{pk}, m\in\mathbb{G}_T, \left(\vec{x}_1,\ldots,\vec{x}_L\right) := \left(\left(x_{1,1},\ldots,x_{1,n}\right),\ldots,\left(x_{L,1},\ldots,x_{L,n}\right)\right)\right):$$
$$\delta_1,\ldots,\delta_L,\delta_{n+2},\zeta \xleftarrow{U} \mathbb{F}_q,$$
$$c_1 := \sum_{t=1}^{L}\delta_t\left(\sum_{i=1}^{n}x_{t,i}b_i\right) + \zeta b_{n+1} + \delta_{n+2}b_{n+2},\ \ c_2 := g_T^{\zeta}m,$$
$$\mathsf{return}\ \left(c_1,c_2\right)$$

[0589] 복호 장치(300)의 기능과 동작에 대하여 설명한다.

[0590] (S501 : 벡터 입력 단계)

[0591] 실시의 형태 2에 있어서의 (S501)과 같이, 벡터 입력부(310)는, 암호화 장치(200)의 데이터 송신부(240)가 송신한 암호 벡터 c_1과 암호 정보 c_2를 통신 장치를 통해 수신하여 입력한다.

[0592] (S502 : 복호 단계)

[0593] 실시의 형태 2에 있어서의 (S502)와 같이, 페어링 연산부(330)는, 마스터 공개 키 pk와 제 L 층째의 비밀 키의 선두 요소인 키 벡터 $k^{*}_{L,\,dec}$에 근거하여, 수학식 198을 처리 장치에 의해 계산하여 평문 정보 m'를 생성한다.

[0594] [수학식 198]

[0595] $$m' := c_2 / e\left(c_1, k^{*}_{L,\mathsf{dec}}\right)$$

[0596] 여기서, 암호화 장치(200)가 암호화에 이용한 속성 벡터 $\vec{x}_i$(i=1, …, h)와, 복호 장치(300)가 복호에 이용한

키 벡터의 술어 벡터 $\vec{v}_j$(j=1, …, L)에 대하여, 모든 i(i=1, …, h), j(j=1, …, L)에 대하여 $\vec{x}_i \cdot \vec{v}_j=0$이면, 페어링 연산부(330)는, 평문 정보 m을 생성할 수 있다. 또, 평문 정보 $m \in G_T$인 것으로 한다.

[0597] 다시 말해, 복호 장치(300)는, 수학식 199에 나타내는 Dec 알고리즘을 실행하여, 평문 정보 m'를 생성한다.

[0598] [수학식 199]

$$\mathrm{Dec}\left(\mathrm{pk}, k^*_{L,\mathrm{dec}}, c_1, c_2\right): m' := c_2 / e\left(c_1, k^*_{L,\mathrm{dec}}\right),$$

[0599] return m'

[0600] 키 위양 장치(400)의 기능과 동작에 대하여 설명한다.

[0601] (S601 : 키 정보 $\vec{k}^*_L$ 취득 단계)

[0602] 실시의 형태 2에 있어서의 (S601)과 같이, 키 벡터 취득부(410)는, 제 L 층째의 비밀 키의 선두 요소인 키 벡터 $k^*_{L,\,dec}$와, 랜덤화 벡터 $k^*_{L,\,ran,\,j}$(j=1, …, L+1)와, 키 생성용 벡터 $k^*_{L,\,del,\,j}$(j=1, …, n)를 포함하는 제 L 층째의 비밀 키(키 정보 $\vec{k}^*_L$)를 통신 장치를 통해 취득한다.

[0603] (S602 : 키 벡터 $k^*_{L+1,\,dec}$ 생성 단계)

[0604] 키 벡터 생성부(420)는, 마스터 공개 키 pk와 키 정보 $\vec{k}^*_L$과 수학식 200에 나타내는 술어 벡터 $\vec{v}_{L+1}$에 근거하여, 수학식 201을 계산하여, 제 L+1 층째의 비밀 키의 선두 요소인 키 벡터 $k^*_{L+1,\,dec}$를 처리 장치에 의해 생성한다.

[0605] [수학식 200]

[0606] $$\vec{v}_{L+1} := \left(v_{L+1,1}, \ldots, v_{L+1,n}\right)$$

[0607] [수학식 201]

(1)

$$\alpha_{\mathrm{dec},t}, \sigma_{\mathrm{dec}} \xleftarrow{\mathrm{U}} \mathbb{F}_q \qquad (t = 1, \ldots, L+1)$$

(2)

$$rv := \sum_{t=1}^{L+1} \alpha_{\mathrm{dec},t} k^*_{L,\mathrm{ran},t}$$

(3)

$$vv := \sigma_{\mathrm{dec}} \left(\sum_{i=1}^{n} v_{L+1,i} k^*_{L,\mathrm{del},i} \right)$$

(4)

$$k^*_{L+1,\mathrm{dec}} := k^*_{L,\mathrm{dec}} + rv + vv$$

[0608] $$:= k^*_{L,\mathrm{dec}} + \sum_{t=1}^{L+1} \alpha_{\mathrm{dec},t} k^*_{L,\mathrm{ran},t} + \sigma_{\mathrm{dec}} \left(\sum_{i=1}^{n} v_{L+1,i} k^*_{L,\mathrm{del},i} \right)$$

[0609] (S603 : 랜덤화 벡터 $k^*_{L+1,\,ran,\,j}$ 생성 단계)

[0610] 랜덤화 벡터 생성부(430)는, 마스터 공개 키 pk와 키 정보 $\vec{k}^*_L$과 수학식 200에 나타내는 술어 벡터 $\vec{v}_{L+1}$에 근거하여, 수학식 202를 계산하여, 랜덤화 벡터 $k^*_{L+1,\,ran,\,j}$(j=1, …, L+2)를 생성한다.

[0611] [수학식 202]

(1)

$$\alpha_{\mathrm{ran},j,t},\sigma_{\mathrm{ran},j} \xleftarrow{\mathrm{U}} \mathbb{F}_q \qquad (j=1,\ldots,L+2;\ t=1,\ldots,L+1)$$

(2)

$$rv_j := \sum_{t=1}^{L+1} \alpha_{\mathrm{ran},j,t} k^*_{L,\mathrm{ran},t} \qquad (j=1,\ldots,L+2)$$

(3)

$$vv_j := \sigma_{\mathrm{ran},j}\left(\sum_{i=1}^{n} v_{L+1,i} k^*_{L,\mathrm{del},i}\right) \qquad (j=1,\ldots,L+2)$$

(4)

$$k^*_{L+1,\mathrm{ran},j} := rv_j + vv_j$$
$$:= \sum_{t=1}^{L+1} \alpha_{\mathrm{ran},j,t} k^*_{L,\mathrm{ran},t} + \sigma_{\mathrm{ran},j}\left(\sum_{i=1}^{n} v_{L+1,i} k^*_{L,\mathrm{del},i}\right)$$
$$(j=1,\ldots,L+2)$$

[0612]

[0613] (S604 : 키 생성용 벡터 $k^*_{L+1,\,del,\,j}$ 생성 단계)

[0614] 키 생성용 벡터 생성부(440)는, 마스터 공개 키 pk와 키 정보 $\vec{k}^*_L$과 수학식 200에 나타내는 술어 벡터 $\vec{v}_{L+1}$에 근거하여, 수학식 203을 계산하여, 키 생성용 벡터 $k^*_{L+1,\,del,\,j}$(j=1, …, n)를 처리 장치에 의해 생성한다.

[0615] [수학식 203]

(1)

$$\alpha_{\mathrm{del},j,t},\sigma_{\mathrm{del},j},\psi' \xleftarrow{\mathrm{U}} \mathbb{F}_q \quad (j=1,\ldots,n;\ i=1,\ldots,L+1)$$

(2)

$$rv_j := \sum_{t=1}^{L+1} \alpha_{\mathrm{del},j,t} k^*_{L,\mathrm{del},t} \qquad (j=1,\ldots,n)$$

(3)

$$vv_j := \sigma_{\mathrm{del},j}\left(\sum_{i=1}^{n} v_{L+1,i} k^*_{L,\mathrm{del},i}\right) \qquad (j=1,\ldots,n)$$

(4)

$$\psi v_j := \psi' k^*_{L,\mathrm{del},j} \qquad (j=1,\ldots,n)$$

(5)

$$k^*_{L+1,\mathrm{del},j} := rv_j + vv_j + \psi v_j$$
$$:= \sum_{t=1}^{L+1} \alpha_{\mathrm{del},j,t} k^*_{L,\mathrm{del},t} + \sigma_{\mathrm{del},j}\left(\sum_{i=1}^{n} v_{L+1,i} k^*_{L,\mathrm{del},i}\right)$$
$$+\psi' k^*_{L,\mathrm{del},j}$$
$$(j=1,\ldots,n)$$

[0616]

[0617] 즉, (S602)로부터 (S604)에 있어서, 키 벡터 생성부(420)와 랜덤화 벡터 생성부(430)와 키 생성용 벡터 생성부(440)는, 수학식 204에 나타내는 $\mathrm{Delegate}_L$ 알고리즘을 실행하여, 키 벡터 $k^*_{L+1,\,dec}$와, 랜덤화 벡터 $k^*_{L+1,\,ran,\,j}$(j=1, …, L+2)와, 키 생성용 벡터 $k^*_{L+1,\,del,\,j}$(j=1, …, n)를 포함하는 제 L+1 층째의 비밀 키(키 정보 $\vec{k}^*_{L+1}$)를 처리 장치에 의해 생성한다.

[0618] [수학식 204]

$$\mathsf{Delegate}_L\left(\mathsf{pk},\vec{k}^*_L,\vec{v}_{L+1}:=\left(v_{L+1,1},\ldots,v_{L+1,n}\right)\right):$$

$$\alpha_{\mathsf{dec},t},\sigma_{\mathsf{dec}},\alpha_{\mathsf{ran},j,t},\sigma_{\mathsf{ran},j}\left(j=1,\ldots,L+2\right),$$

$$\alpha_{\mathsf{del},j,t},\sigma_{\mathsf{del},j}\left(j=1,\ldots,n\right),\psi' \xleftarrow{\mathrm{U}} \mathbb{F}_q$$

$$\text{for } t=1,\ldots,L+1,$$

$$k^*_{L+1,\mathsf{dec}} := k^*_{L,\mathsf{dec}} + \sum_{t=1}^{L+1}\alpha_{\mathsf{dec},t}k^*_{L,\mathsf{ran},t} + \sigma_{\mathsf{dec}}\left(\sum_{i=1}^{n}v_{L+1,i}k^*_{L,\mathsf{del},i}\right),$$

$$k^*_{L+1,\mathsf{ran},j} := \sum_{t=1}^{L+1}\alpha_{\mathsf{ran},j,t}k^*_{L,\mathsf{ran},t} + \sigma_{\mathsf{ran},j}\left(\sum_{i=1}^{n}v_{L+1,i}k^*_{L,\mathsf{del},i}\right)$$

$$\text{for } j=1,\ldots,L+2,$$

$$k^*_{L+1,\mathsf{del},j} := \sum_{t=1}^{L+1}\alpha_{\mathsf{del},j,t}k^*_{L,\mathsf{del},t} + \sigma_{\mathsf{del},j}\left(\sum_{i=1}^{n}v_{L+1,i}k^*_{L,\mathsf{del},i}\right) + \psi' k^*_{L,\mathsf{del},j}$$

$$\text{for } j=1,\ldots,n,$$

$$\text{return } \vec{k}^*_{L+1} := \left(k^*_{L+1,\mathsf{dec}},k^*_{L+1,\mathsf{ran},1},\ldots,k^*_{L+1,\mathsf{ran},L+2},k^*_{L+1,\mathsf{del},1},\ldots k^*_{L+1,\mathsf{del},n}\right)$$

[0619]

[0620] (S605 : 키 배포 단계)

[0621] 실시의 형태 2에 있어서의 (S605)와 같이, 키 배포부(450)는, 키 벡터 생성부(420)와 랜덤화 벡터 생성부(430)와 키 생성용 벡터 생성부(440)가 생성한 키 정보 $\vec{k}^*_{L+1}$을 하위의 복호 장치(300)에 통신 장치를 통해 송신한다.

[0622] 상술한 것처럼, 암호화 장치(200)가 암호화에 이용한 속성 벡터 $\vec{x}_i$(i=1, …, h)와, 복호 장치(300)가 복호에 이용한 키 벡터 $k^*_{L,\,\mathsf{dec}}$의 술어 벡터 $\vec{v}_j$(j=1, …, L)에 대하여, 모든 i(i=1, …, h), j(j=1, …, L)에 대하여 $\vec{x}_i \cdot \vec{v}_j=0$이면, 복호 장치(300)는 복호할 수 있다. 다시 말해, 술어 벡터($\vec{v}_1$)에 근거하여 생성된 키 벡터 $k^*_{1,\,\mathsf{dec}}$로 복호하는 경우, $\vec{x} \cdot \vec{v}_1=0$이면, 복호 장치(300)는 복호할 수 있다. 또한, 술어 벡터 ($\vec{v}_1$, $\vec{v}_2$)에 근거하여 생성된 키 벡터 $k^*_{2,\,\mathsf{dec}}$로 복호하는 경우, $\vec{x} \cdot \vec{v}_1=0$ 또한 $\vec{x} \cdot \vec{v}_2=0$이면, 복호 장치(300)는 복호할 수 있다. 다시 말해, 실시의 형태 2에서 설명한 알고리즘과 같이, 하위의 키 벡터 $k^*_{2,\,\mathsf{dec}}$는, 상위의 키 벡터 $k^*_{1,\,\mathsf{dec}}$보다 기능이 제한되어 있다.

[0623] 또한, 실시의 형태 2와 같이, 암호화 장치(200)가 실행하는 Enc 알고리즘과, 복호 장치(300)가 실행하는 Dec 알고리즘을, 각각 수학식 205와 수학식 206과 같이 변경하는 것에 의해, 계층적 술어 키 비닉 방식을 실현하는 것도 가능하다.

[0624] [수학식 205]

$$\mathsf{Enc}\left(\mathsf{pk},\left(\vec{x}_1,\ldots,\vec{x}_L\right):=\left(\left(x_{1,1},\ldots,x_{1,n}\right),\ldots,\left(x_{L,1},\ldots,x_{L,n}\right)\right)\right):$$

$$\delta_1,\ldots,\delta_L,\delta_{n+2},\zeta \xleftarrow{\mathrm{U}} \mathbb{F}_q,$$

$$c_1 := \sum_{t=1}^{L}\delta_t\left(\sum_{i=1}^{n}x_{t,i}b_i\right) + \zeta b_{n+1} + \delta_{n+2}b_{n+2},\quad K := g_T^{\zeta},$$

$$\text{return } \left(c_1,K\right)$$

[0625]

[0626] [수학식 206]

$$\mathsf{Dec}\left(\mathsf{pk},k^*_{L,\mathsf{dec}},c_1\right):K' := e\left(c_1,k^*_{L,\mathsf{dec}}\right),$$

$$\text{return } K'$$

[0627]

[0628] 실시의 형태 4.

[0629] 이상의 실시의 형태에서는, 쌍대 벡터 공간에 있어서 암호 처리를 실현하는 방법에 대하여 설명했다. 본 실시의 형태에서는, 쌍대 가군에 있어서 암호 처리를 실현하는 방법에 대하여 설명한다.

[0630] 다시 말해, 이상의 실시의 형태에서는, 소수 위수 q의 순회군에 있어서 암호 처리를 실현했다. 그러나, 합성수 M을 이용하여 수학식 207과 같이 환 R을 나타낸 경우, 환 R을 계수로 하는 가군에 있어서도, 상기 실시의 형태에서 설명한 암호 처리를 적용할 수 있다.

[0631] [수학식 207]

$$\mathbb{R} := \mathbb{Z}/M\mathbb{Z}$$

여기서,
$\mathbb{Z}$: 정수
M : 합성수

[0632] 이다.

[0633] 예컨대, 실시의 형태 2에서 설명한 계층적 술어 암호를, 환 R을 계수로 하는 가군에 있어서 실현하면 수학식 208로부터 수학식 212와 같이 된다.

[0634] [수학식 208]

$$\begin{aligned}
&\mathsf{Setup}\left(1^{\lambda}, \vec{\mu} := (n, d; \mu_1, \ldots, \mu_d)\right):\\
&\quad \left(\mathsf{param}, \mathbb{B}, \mathbb{B}^*\right) \xleftarrow{\mathrm{R}} \mathcal{G}_{\mathsf{ob}}\left(1^{\lambda}, n+2+r+s\right),\\
&\quad \hat{\mathbb{B}} := \left(b_1, \ldots, b_n, b_{n+1}, b_{n+2}\right),\\
&\quad \text{return } \mathsf{sk} := \left(X, \mathbb{B}^*\right),\ \mathsf{pk} := \left(1^{\lambda}, \mathsf{param}, \hat{\mathbb{B}}\right)
\end{aligned}$$

여기서,

$$\begin{aligned}
&\mathcal{G}_{\mathsf{ob}}\left(1^{\lambda}, N\right): \mathsf{param} := \left(M, \mathbb{V}, \mathbb{V}^*, \mathbb{G}_T, \mathbb{A}, \mathbb{A}^*\right) \xleftarrow{\mathrm{R}} \mathcal{G}_{\mathsf{dpvs}}\left(1^{\lambda}, N\right),\\
&\quad X := \left(\chi_{i,j}\right) \xleftarrow{\mathrm{U}} GL(N, \mathbb{R}),\ \left(v_{i,j}\right) := \left(X^{\mathrm{T}}\right)^{-1},\\
&\quad b_i = \sum_{j=1}^{N} \chi_{i,j} a_j,\ \mathbb{B} := \left(b_1, \ldots, b_N\right),\\
&\quad b_i^* = \sum_{j=1}^{N} v_{i,j} a_j^*,\ \mathbb{B}^* := \left(b_1^*, \ldots, b_N^*\right),\\
&\quad \text{return } \left(\mathsf{param}, \mathbb{B}, \mathbb{B}^*\right)
\end{aligned}$$

[0635] 이다.

[0636] [수학식 209]

$$\begin{aligned}
&\mathsf{GenKey}\left(\mathsf{pk}, \mathsf{sk}, \left(\vec{v}_1, \ldots, \vec{v}_L\right)\right) := \left(\left(v_1, \ldots, v_{\mu_1}\right), \ldots, \left(v_{\mu_{L-1}+1}, \ldots, v_{\mu_L}\right)\right):\\
&\quad \sigma_{j,i}, \psi, \eta_{j,h} \xleftarrow{\mathrm{U}} \mathbb{R}\\
&\qquad \text{for } j = 0, \ldots, L+1, \mu_L+1, \ldots, n;\ i = 1, \ldots, L;\ h = 1, \ldots, r\\
&\quad k_{L,\mathsf{dec}}^* := \sum_{t=1}^{L} \sigma_{0,t} \left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b_i^*\right) + \sum_{h=1}^{r} \eta_{0,h} b_{n+2+h}^*,\\
&\quad k_{L,\mathsf{ran},j}^* := \sum_{t=1}^{L} \sigma_{j,t} \left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b_i^*\right) + \sum_{h=1}^{r} \eta_{j,h} b_{n+2+h}^*\\
&\qquad \text{for } j = 1, \ldots, L+1,\\
&\quad k_{L,\mathsf{del},j}^* := \sum_{t=1}^{L} \sigma_{j,t} \left(\sum_{i=\mu_{t-1}+1}^{\mu_t} v_i b_i^*\right) + \psi b_j^* + \sum_{h=1}^{r} \eta_{j,h} b_{n+2+h}^*\\
&\qquad \text{for } j = \mu_L+1, \ldots, n,\\
&\quad \text{return } \vec{k}_L^* := \left(k_{L,0}^*, \ldots, k_{L,L+1}^*, k_{L,\mu_L+1}^*, \ldots, k_{L,n}^*\right)
\end{aligned}$$

[0637]

[0638] [수학식 210]

$$\mathsf{Enc}\left(\mathsf{pk}, m \in \mathbb{G}_T, \left(\vec{x}_1,\ldots,\vec{x}_L\right) := \left(\left(x_1,\ldots,x_{\mu_1}\right),\ldots,\left(x_{\mu_{L-1}+1},\ldots,x_{\mu_L}\right)\right)\right):$$
$$\left(\vec{x}_{L+1},\ldots,\vec{x}_d\right) \xleftarrow{\mathrm{U}} \mathbb{R}^{\mu_{L+1}-\mu_L} \times \cdots \times \mathbb{R}^{n-\mu_{d-1}},$$
$$\delta_1,\ldots,\delta_d,\delta_{n+2},\zeta \xleftarrow{\mathrm{U}} \mathbb{R},$$
$$c_1 := \sum_{t=1}^{d} \delta_t \left(\sum_{i=\mu_{t-1}+1}^{\mu_t} x_i b_i\right) + \zeta b_{n+1} + \delta_{n+2} b_{n+2},\ \ c_2 := g_T^{\zeta} m,$$
$$\text{return } (c_1, c_2)$$

[0639]

[0640] [수학식 211]

$$\mathsf{Dec}\left(\mathsf{pk}, k^*_{L,\mathsf{dec}}, c_1, c_2\right): m' := c_2 / e\left(c_1, k^*_{L,\mathsf{dec}}\right),$$
$$\text{return } m'$$

[0641]

[0642] [수학식 212]

$$\mathsf{Delegate}_L\left(\mathsf{pk}, \vec{k}^*_L, \vec{v}_{L+1} := \left(v_{\mu_L+1},\ldots,v_{\mu_{L+1}}\right)\right):$$
$$\alpha_{j,i},\sigma_j,\psi' \xleftarrow{\mathrm{U}} \mathbb{R} \ \text{ for } j = 0,\ldots,L+2, \mu_{L+1}+1,\ldots,n;\ i = 1,\ldots,L+1,$$
$$k^*_{L+1,\mathsf{dec}} := k^*_{L,\mathsf{dec}} + \sum_{i=1}^{L+1} \alpha_{0,i} k^*_{L,\mathsf{ran},i} + \sigma_0 \left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^*_{L,\mathsf{del},i}\right),$$
$$k^*_{L+1,\mathsf{ran},j} := \sum_{i=1}^{L+1} \alpha_{j,i} k^*_{L,\mathsf{ran},i} + \sigma_j \left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^*_{L,\mathsf{del},i}\right) \ \text{ for } j = 0,\ldots,L+2,$$
$$k^*_{L+1,\mathsf{del},j} := \sum_{i=1}^{L+1} \alpha_{j,i} k^*_{L,\mathsf{ran},i} + \sigma_j \left(\sum_{i=\mu_L+1}^{\mu_{L+1}} v_i k^*_{L,\mathsf{del},i}\right) + \psi' k^*_{L,\mathsf{del},j}$$
$$\text{for } j = \mu_{L+1}+1,\ldots,n,$$
$$\text{return } \vec{k}^*_{L+1} := \left(k^*_{L+1,0},\ldots,k^*_{L+1,L+2}, k^*_{L+1,\mu_{L+1}+1},\ldots k^*_{L+1,n}\right)$$

[0643]

[0644] 여기에서는, 실시의 형태 2에서 설명한 계층적 술어 암호에 대해서만, 환 R을 계수로 하는 가군에 있어서 실현하는 방법을 나타냈다. 그러나, 원칙적으로 이상의 실시의 형태에서 체 F_q로서 설명한 처리를, 환 R로 치환하는 것에 의해, 이상의 실시의 형태에서 설명한 다른 암호 처리에 대해서도, 환 R을 계수로 하는 가군에 있어서 실현할 수 있다.

[0645] 다음으로, 실시의 형태에 있어서의 암호 처리 시스템(10)(키 생성 장치(100), 암호화 장치(200), 복호 장치(300), 키 위양 장치(400))의 하드웨어 구성에 대하여 설명한다.

[0646] 도 21은 키 생성 장치(100), 암호화 장치(200), 복호 장치(300), 키 위양 장치(400)의 하드웨어 구성의 일례를 나타내는 도면이다.

[0647] 도 21에 나타내는 바와 같이, 키 생성 장치(100), 암호화 장치(200), 복호 장치(300), 키 위양 장치(400)는, 프로그램을 실행하는 CPU(911)(Central Processing Unit, 중앙 처리 장치, 처리 장치, 연산 장치, 마이크로프로세서, 마이크로컴퓨터, 프로세서라고도 한다)를 구비하고 있다. CPU(911)는, 버스(912)를 통해 ROM(913), RAM(914), LCD(901)(Liquid Crystal Display), 키보드(902)(K/B), 통신 보드(915), 자기 디스크 장치(920)와 접속되고, 이러한 하드웨어 디바이스를 제어한다. 자기 디스크 장치(920)(고정 디스크 장치) 대신에, 광디스크 장치, 메모리 카드 판독/기입 장치 등의 기억 장치라도 좋다. 자기 디스크 장치(920)는, 소정의 고정 디스크 인터페이스를 통해 접속된다.

[0648] ROM(913), 자기 디스크 장치(920)는, 비휘발성 메모리의 일례이다. RAM(914)은, 휘발성 메모리의 일례이다. ROM(913)과 RAM(914)과 자기 디스크 장치(920)는, 기억 장치(메모리)의 일례이다. 또한, 키보드(902), 통신 보드(915)는, 입력 장치의 일례이다. 또한, 통신 보드(915)는, 통신 장치(네트워크 인터페이스)의 일례이다. 또한, LCD(901)는, 표시 장치의 일례이다.

[0649] 자기 디스크 장치(920) 또는 ROM(913) 등에는, 오퍼레이팅 시스템(921)(OS), 윈도우 시스템(922), 프로그램군(923), 파일군(924)이 기억되어 있다. 프로그램군(923)의 프로그램은, CPU(911), 오퍼레이팅 시스템(921), 윈도우 시스템(922)에 의해 실행된다.

[0650] 프로그램군(923)에는, 상기의 설명에 있어서 「마스터 키 생성부(110)」, 「마스터 키 기억부(120)」, 「키 벡

터 생성부(130)」, 「랜덤화 벡터 생성부(140)」, 「키 생성용 벡터 생성부(150)」, 「키 배포부(160)」, 「송신 정보 설정부(210)」, 「암호 벡터 생성부(220)」, 「암호 정보 생성부(230)」, 「데이터 송신부(240)」, 「공개 키 취득부(250)」, 「세션 키 생성부(260)」, 「벡터 입력부(310)」, 「키 벡터 기억부(320)」, 「페어링 연산부(330)」, 「키 벡터 취득부(410)」, 「키 벡터 생성부(420)」, 「랜덤화 벡터 생성부(430)」, 「키 생성용 벡터 생성부(440)」, 「키 배포부(450)」 등으로서 설명한 기능을 실행하는 소프트웨어나 프로그램이나 그 외의 프로그램이 기억되어 있다. 프로그램은, CPU(911)에 의해 판독되어 실행된다.

[0651] 파일군(924)에는, 상기의 설명에 있어서 「마스터 공개 키 pk」, 「마스터 비밀 키 sk」, 「암호 벡터 c」, 「키 벡터」 등의 정보나 데이터나 신호치나 변수치나 파라미터가, 「파일」이나 「데이터베이스」의 각 항목으로서 기억된다. 「파일」이나 「데이터베이스」는, 디스크나 메모리 등의 기록 매체에 기억된다. 디스크나 메모리 등의 기억 매체에 기억된 정보나 데이터나 신호치나 변수치나 파라미터는, 판독/기입 회로를 통해 CPU(911)에 의해 메인 메모리나 캐시 메모리에 판독되어, 추출・검색・참조・비교・연산・계산・처리・출력・인쇄・표시 등의 CPU(911)의 동작에 이용된다. 추출・검색・참조・비교・연산・계산・처리・출력・인쇄・표시의 CPU(911)의 동작 동안, 정보나 데이터나 신호치나 변수치나 파라미터는, 메인 메모리나 캐시 메모리나 버퍼 메모리에 일시적으로 기억된다.

[0652] 또한, 상기의 설명에 있어서의 플로우차트의 화살표의 부분은 주로 데이터나 신호의 입출력을 나타내고, 데이터나 신호치는, RAM(914)의 메모리, 그 밖의 광디스크 등의 기록 매체나 IC 칩에 기록된다. 또한, 데이터나 신호는, 버스(912)나 신호선이나 케이블 그 밖의 전송 매체나 전파에 의해 온라인 전송된다.

[0653] 또한, 상기의 설명에 있어서 「~부」로서 설명하는 것은, 「~회로」, 「~장치」, 「~기기」, 「~수단」, 「~기능」이더라도 좋고, 또한, 「~단계」, 「~순서」, 「~처리」이더라도 좋다. 또한, 「~장치」로서 설명하는 것은, 「~회로」, 「~기기」, 「~수단」, 「~기능」이더라도 좋고, 또한, 「~단계」, 「~순서」, 「~처리」이더라도 좋다. 또한, 「~처리」로서 설명하는 것은 「~단계」이더라도 상관없다. 즉, 「~부」로서 설명하는 것은, ROM(913)에 기억된 펌웨어로 실현되고 있더라도 상관없다. 혹은, 소프트웨어만, 혹은, 소자・디바이스・기판・배선 등의 하드웨어만, 혹은, 소프트웨어와 하드웨어의 조합, 또한, 펌웨어와의 조합으로 실시되어도 상관없다. 펌웨어와 소프트웨어는, 프로그램으로서, ROM(913) 등의 기록 매체에 기억된다. 프로그램은 CPU(911)에 의해 판독되어, CPU(911)에 의해 실행된다. 즉, 프로그램은, 상기에서 말한 「~부」로서 컴퓨터 등을 기능시키는 것이다. 혹은, 상기에서 말한 「~부」의 순서나 방법을 컴퓨터 등에 실행시키는 것이다.

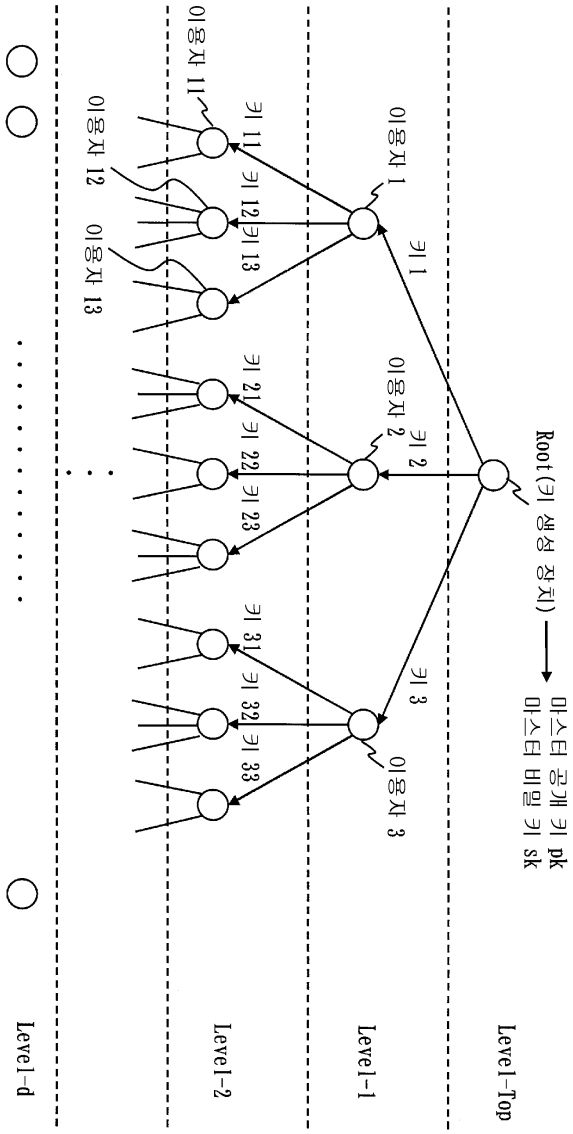
부호의 설명

[0654]

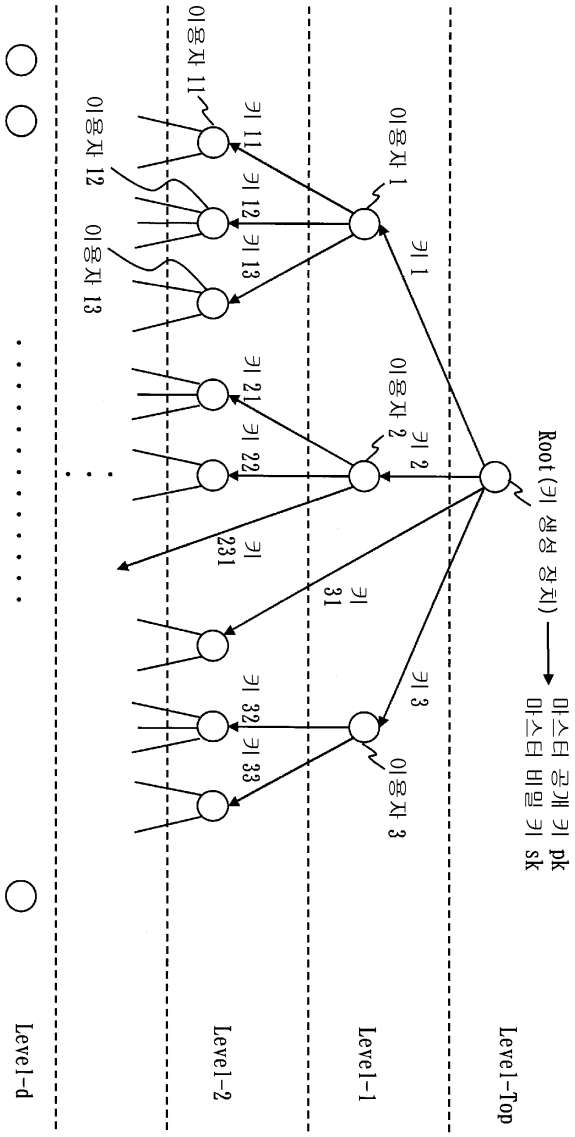
10 : 암호 처리 시스템
100 : 키 생성 장치
110 : 마스터 키 생성부
120 : 마스터 키 기억부
130 : 키 벡터 생성부
140 : 랜덤화 벡터 생성부
150 : 키 생성용 벡터 생성부
160 : 키 배포부
200 : 암호화 장치
210 : 송신 정보 설정부
220 : 암호 벡터 생성부
230 : 암호 정보 생성부
240 : 데이터 송신부
250 : 공개 키 취득부
260 : 세션 키 생성부
300 : 복호 장치
310 : 벡터 입력부
320 : 키 벡터 기억부
330 : 페어링 연산부
400 : 키 위양 장치
410 : 키 벡터 취득부
420 : 키 벡터 생성부
430 : 랜덤화 벡터 생성부
440 : 키 생성용 벡터 생성부
450 : 키 배포부

도면

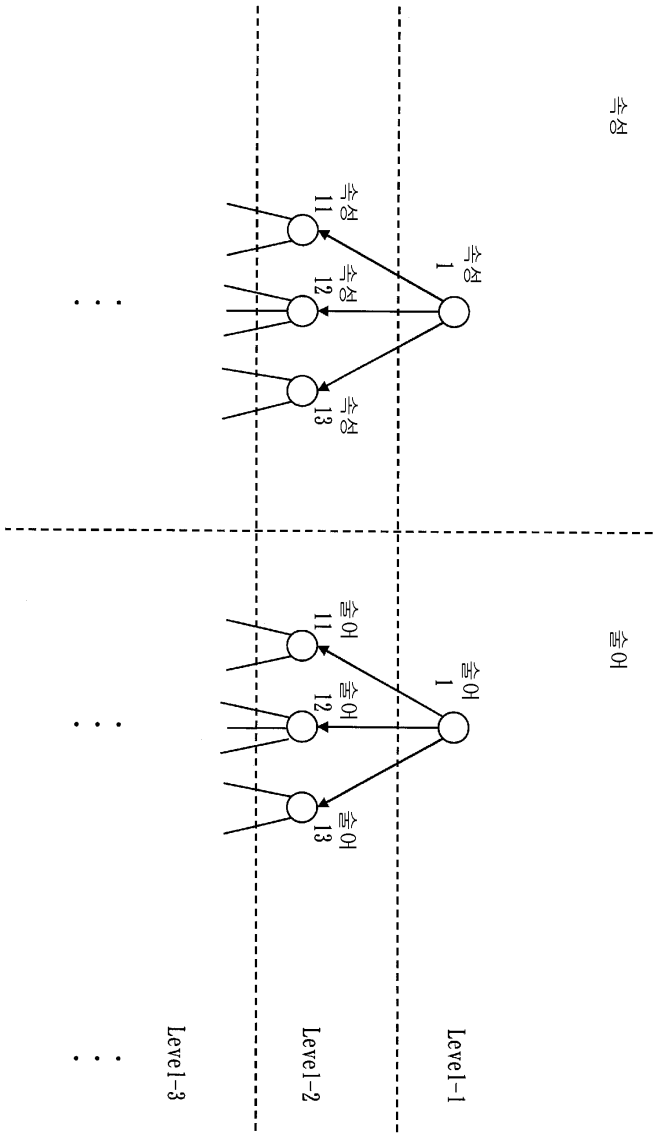
도면1


Root(키 생성 장치)
마스터 공개 키 pk
마스터 비밀 키 sk
Level-Top
키 1
키 2
키 3
이용자 1
이용자 2
이용자 3
Level-1
키 11
키 12
키 13
키 21
키 22
키 23
키 31
키 32
키 33
이용자 11
이용자 12
이용자 13
Level-2
Level-d

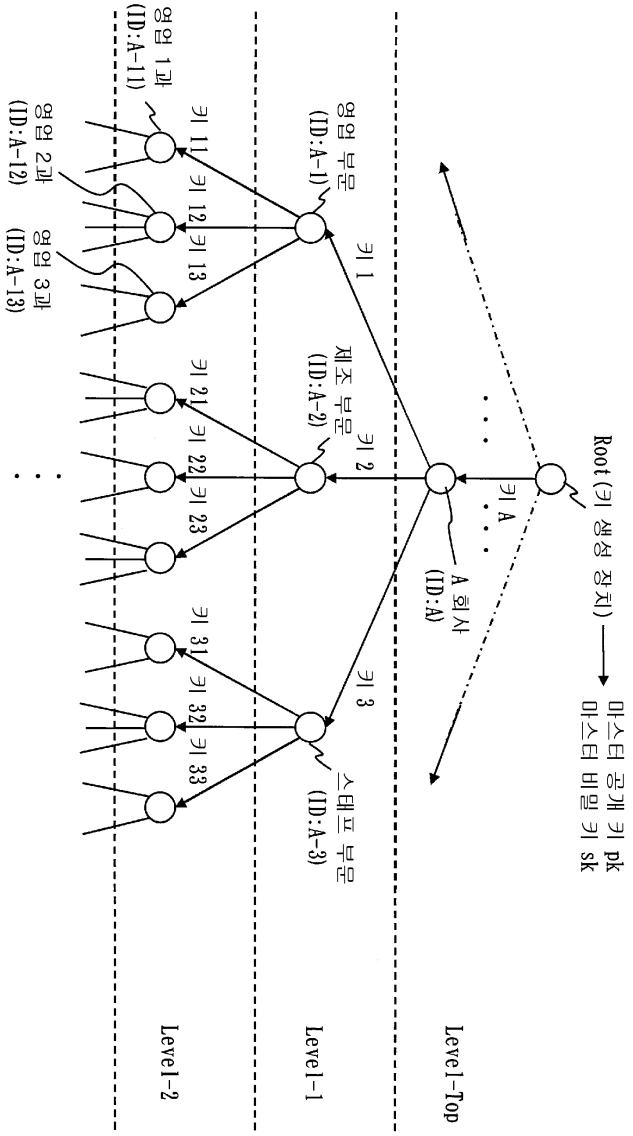
도면2


Root (키 생성 장치)
마스터 공개 키 pk
마스터 비밀 키 sk
Level-Top
키 1
키 2
키 3
이용자 1
이용자 2
이용자 3
Level-1
키 11
키 12
키 13
키 21
키 22
키 231
키 31
키 32
키 33
이용자 11
이용자 12
이용자 13
Level-2
Level-d

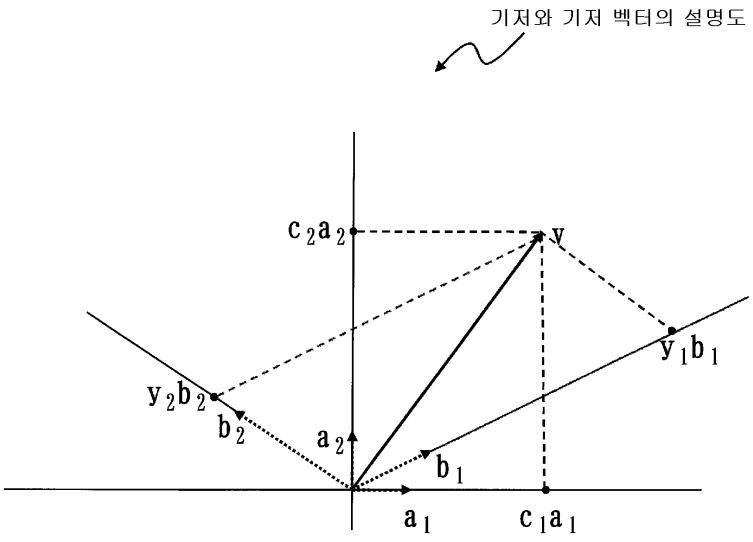
도면3


속성
출어
속성 1
속성 11
속성 12
속성 13
출어 1
출어 11
출어 12
출어 13
Level-1
Level-2
Level-3

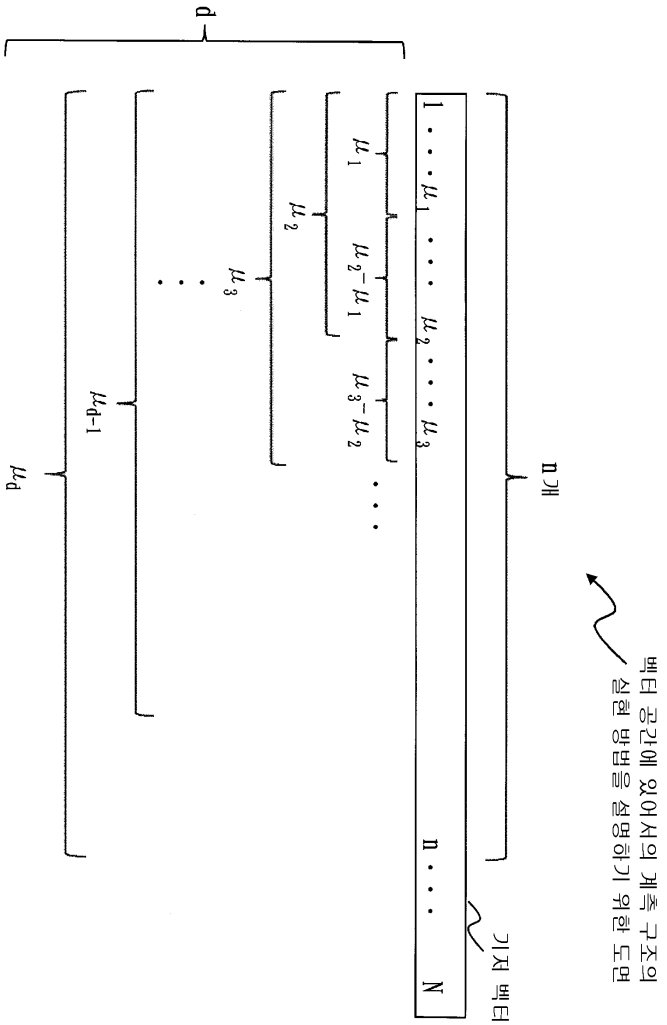
도면4


Root (키 생성 정지)
마스터 공개 키 pk
마스터 비밀 키 sk
키 A
A 회사
(ID:A)
키 1
키 2
키 3
영업 부문
(ID:A-1)
제조 부문
(ID:A-2)
스태프 부문
(ID:A-3)
키 11
키 12
키 13
키 21
키 22
키 23
키 31
키 32
키 33
영업 1과
(ID:A-11)
영업 2과
(ID:A-12)
영업 3과
(ID:A-13)
Level-Top
Level-1
Level-2

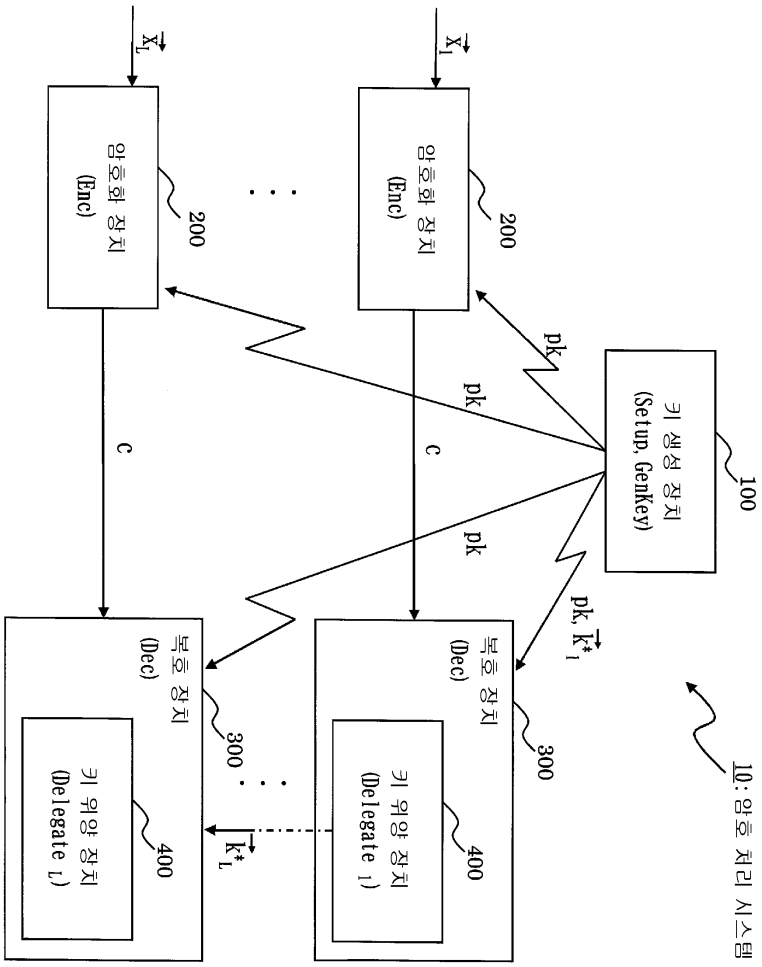
도면5


기저와 기저 벡터의 설명도
c 2a 2
v
y 1b 1
y 2b 2
b 2
a 2
b 1
a 1
c 1a 1

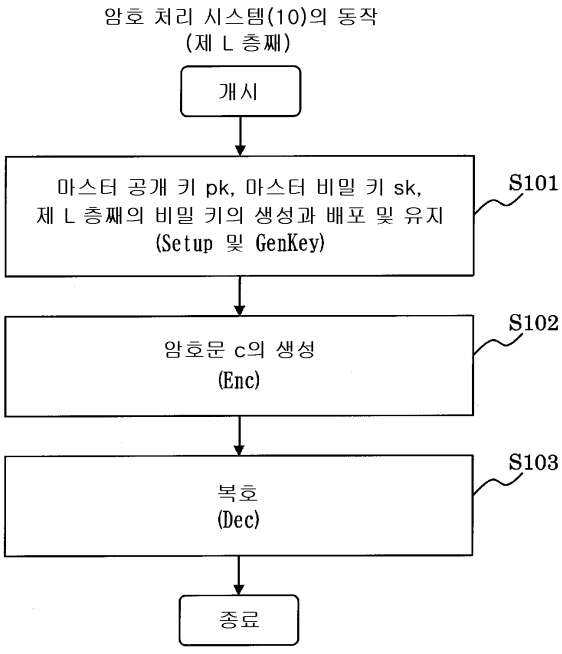
도면6


d
n개
1 · · · μ_1 · · · · μ_2 · · · μ_3 n · · · N
μ_1
$\mu_2-\mu_1$
$\mu_3-\mu_2$
μ_2
μ_3
μ_{d-1}
μ_d
기저 벡터
벡터 공간에 있어서의 계층 구조의 실현 방법을 설명하기 위한 도면

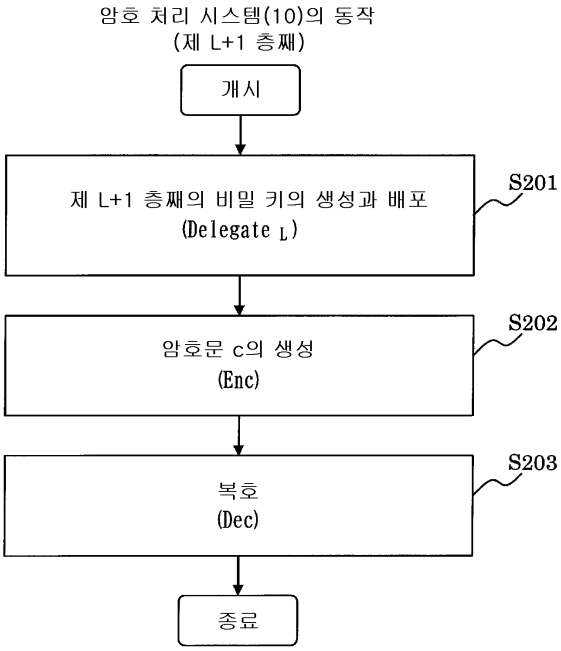
도면7


암호화 장치 (Enc)
200
암호화 장치 (Enc)
200
키 생성 장치 (Setup, GenKey)
100
pk
pk
pk
pk, $\vec{k}^*_1$
c
c
복호 장치 (Dec)
300
키 위양 장치 (Delegate 1)
400
복호 장치 (Dec)
300
키 위양 장치 (Delegate L)
400
$\vec{k}^*_L$
10: 암호 처리 시스템

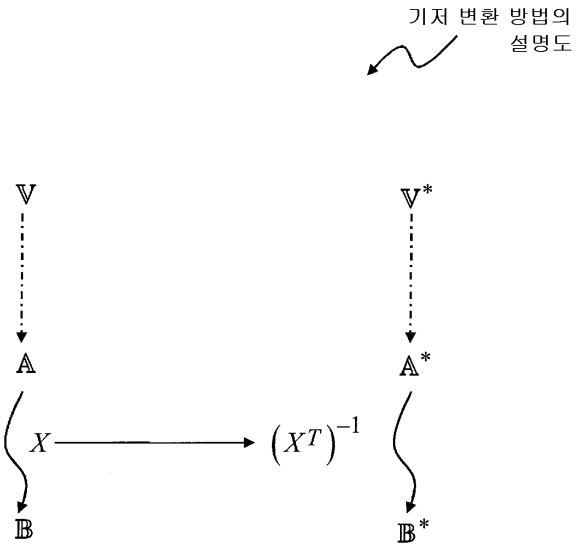
도면8


암호 처리 시스템(10)의 동작
(제 L 층째)
개시
마스터 공개 키 pk, 마스터 비밀 키 sk,
제 L 층째의 비밀 키의 생성과 배포 및 유지
(Setup 및 GenKey)
S101
암호문 c의 생성
(Enc)
S102
복호
(Dec)
S103
종료

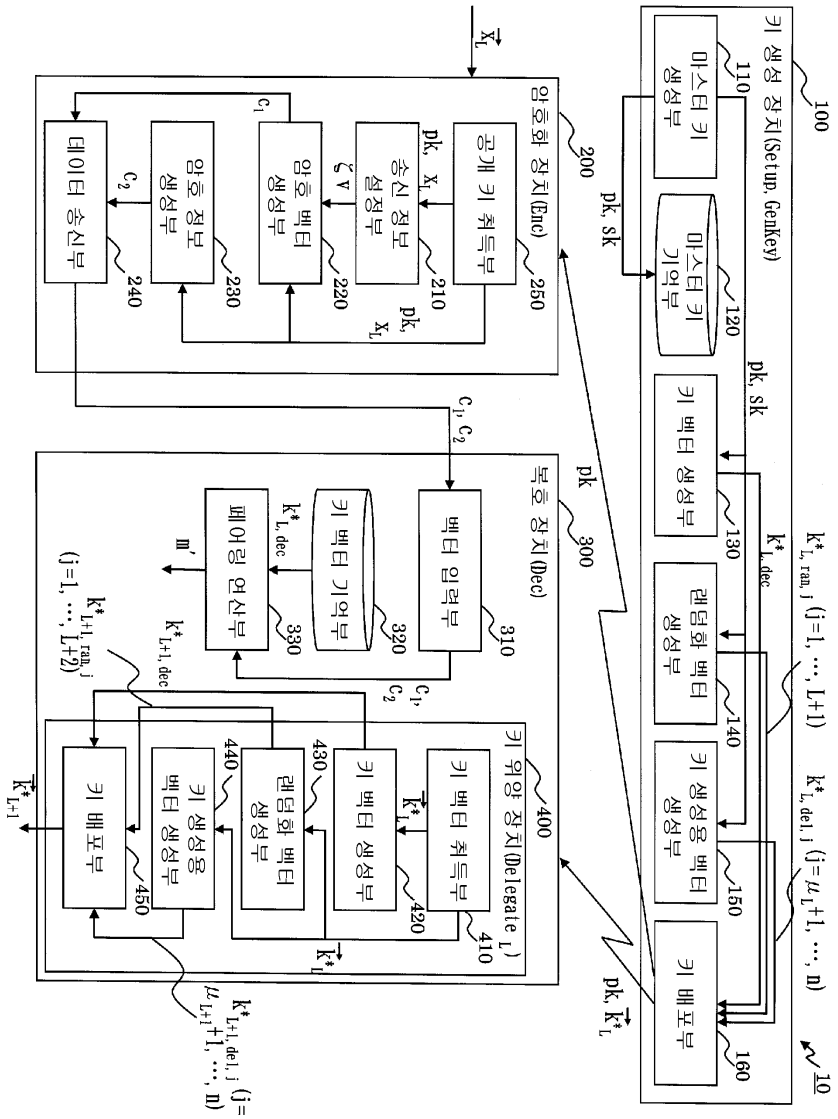
도면9


암호 처리 시스템(10)의 동작
(제 L+1 층째)
개시
제 L+1 층째의 비밀 키의 생성과 배포
(Delegate L)
S201
암호문 c의 생성
(Enc)
S202
복호
(Dec)
S203
종료

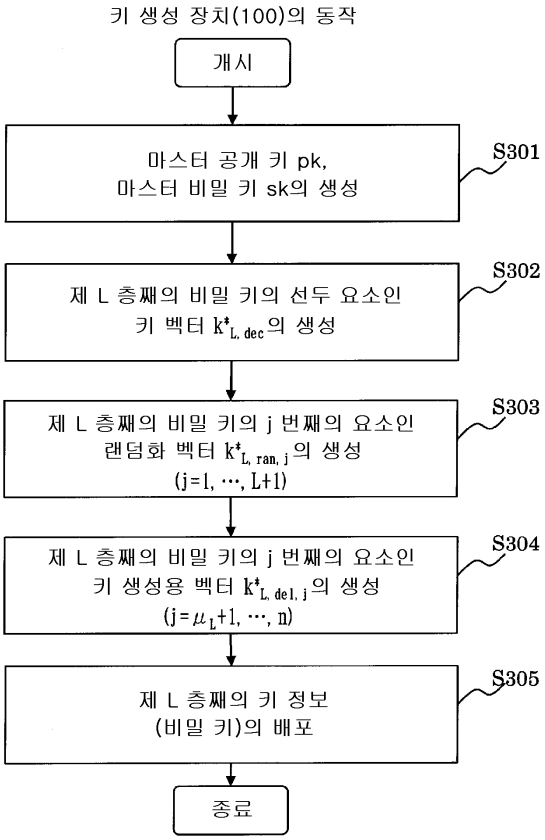
도면10


기저 변환 방법의
설명도
V
A
B
V*
A*
B*
X
$(X^T)^{-1}$

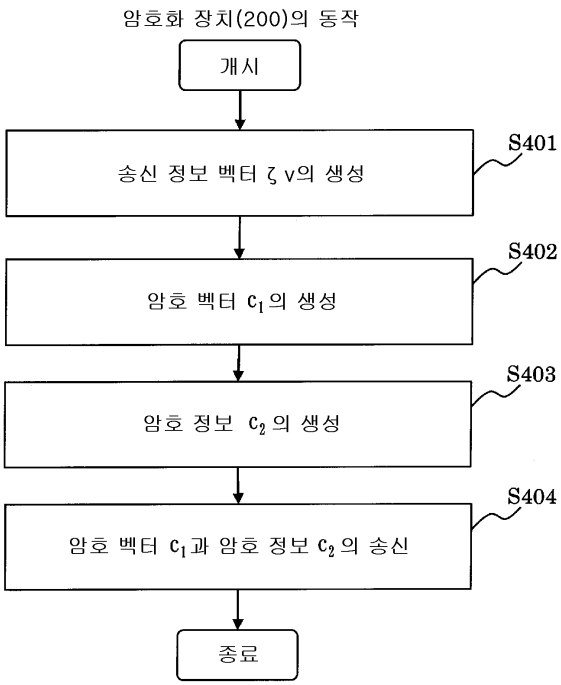
도면11


키 생성 장치(Setup, Genkey)
100
마스터 키 생성부
110
마스터 키 기억부
120
키 벡터 생성부
130
랜덤화 벡터 생성부
140
키 생성용 벡터 생성부
150
키 배포부
160
10
암호화 장치(Enc)
200
공개 키 취득부
250
210
송신 정보 설정부
220
암호 벡터 생성부
230
암호 정보 생성부
240
데이터 송신부
복호 장치(Dec)
300
벡터 입력부
310
키 벡터 기억부
320
패어링 연산부
330
키 위양 장치(Delegate)
400
키 벡터 취득부
410
420
키 벡터 생성부
430
랜덤화 벡터 생성부
440
키 생성용 벡터 생성부
450
키 배포부
pk, sk
pk
pk, $\vec{k}^*_L$
$\vec{x}_L$
c_1, c_2
$k^*_{L, ran, j}$ (j=1, …, L+1)
$k^*_{L, del, j}$ (j=μ_L+1, …, n)
$k^*_{L, dec}$
$\vec{k}^*_L$
$\vec{k}^*_{L+1}$
$k^*_{L+1, dec}$
$k^*_{L+1, ran, j}$ (j=1, …, L+2)
$k^*_{L+1, del, j}$ (j=μ_{L+1}+1, …, n)
m'

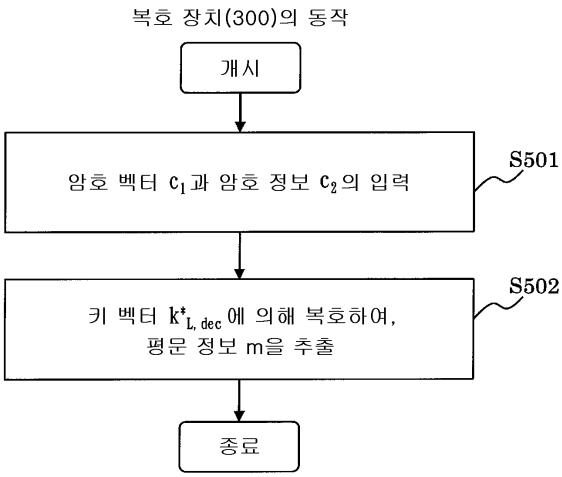
도면12


키 생성 장치(100)의 동작
개시
마스터 공개 키 pk,
마스터 비밀 키 sk의 생성
S301
제 L 층째의 비밀 키의 선두 요소인
키 벡터 $k^{*}_{L,dec}$의 생성
S302
제 L 층째의 비밀 키의 j 번째의 요소인
랜덤화 벡터 $k^{*}_{L,ran,j}$의 생성
(j=1, ···, L+1)
S303
제 L 층째의 비밀 키의 j 번째의 요소인
키 생성용 벡터 $k^{*}_{L,del,j}$의 생성
($j=\mu_L+1, \cdots, n$)
S304
제 L 층째의 키 정보
(비밀 키)의 배포
S305
종료

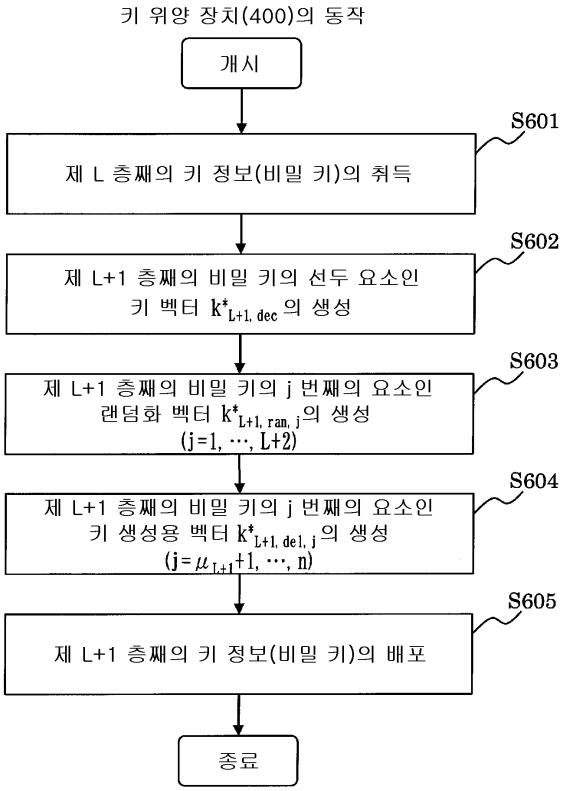
도면13


암호화 장치(200)의 동작
개시
송신 정보 벡터 ζ v의 생성
S401
암호 벡터 c_1의 생성
S402
암호 정보 c_2의 생성
S403
암호 벡터 c_1과 암호 정보 c_2의 송신
S404
종료

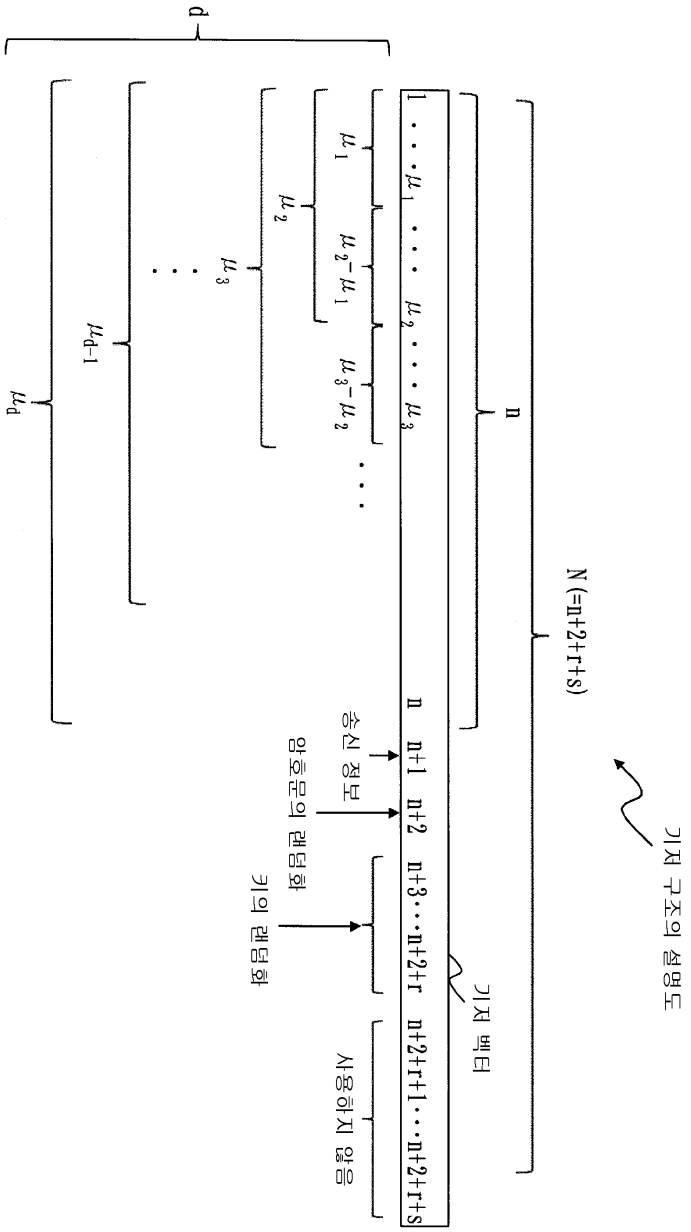
도면14


복호 장치(300)의 동작
개시
암호 벡터 c_1과 암호 정보 c_2의 입력
S501
키 벡터 $k^*_{L,dec}$에 의해 복호하여,
평문 정보 m을 추출
S502
종료

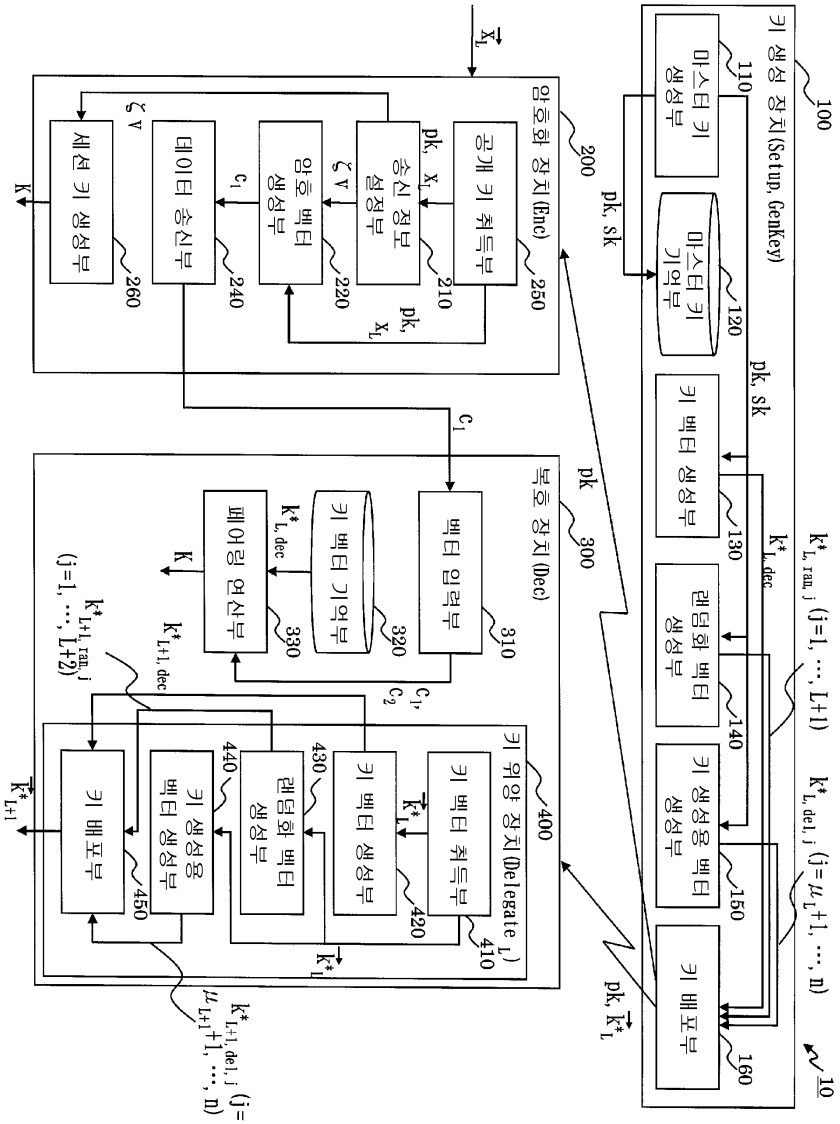
도면15


키 위양 장치(400)의 동작
개시
제 L 층째의 키 정보(비밀 키)의 취득
S601
제 L+1 층째의 비밀 키의 선두 요소인
키 벡터 $k^*_{L+1,dec}$의 생성
S602
제 L+1 층째의 비밀 키의 j 번째의 요소인
랜덤화 벡터 $k^*_{L+1,ran,j}$의 생성
(j=1, …, L+2)
S603
제 L+1 층째의 비밀 키의 j 번째의 요소인
키 생성용 벡터 $k^*_{L+1,del,j}$의 생성
($j=\mu_{L+1}+1, \cdots, n$)
S604
제 L+1 층째의 키 정보(비밀 키)의 배포
S605
종료

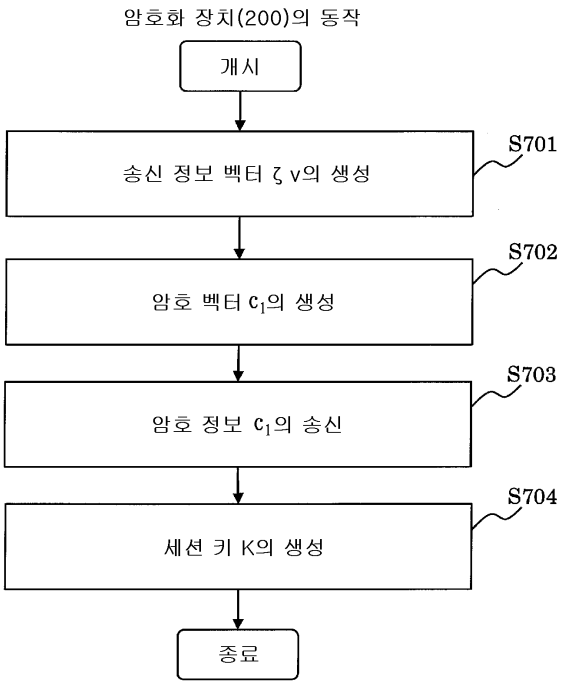
도면16


d
μ_d
μ_{d-1}
μ_3
μ_2
μ_1
$\mu_2-\mu_1$
$\mu_3-\mu_2$
1 · · · μ_1 · · · μ_2 · · · μ_3
n
N (=n+2+r+s)
n n+1 n+2 n+3···n+2+r n+2+r+1···n+2+r+s
송신 정보
암호문의 랜덤화
키의 랜덤화
사용하지 않음
기저 벡터
기저 구조의 설명도

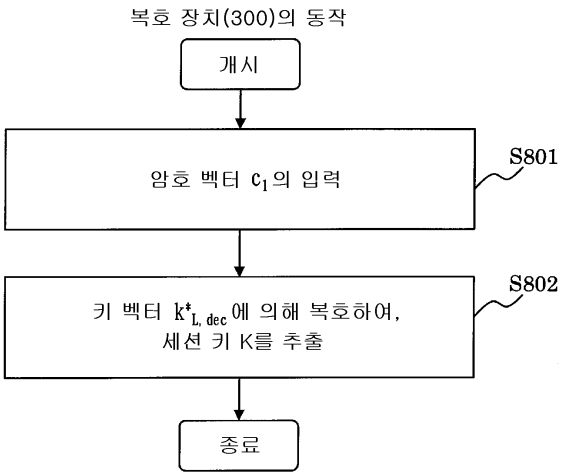
도면17


키 생성 장치(Setup, GenKey)
100
마스터 키 생성부
110
마스터 키 기억부
120
키 벡터 생성부
130
랜덤화 벡터 생성부
140
키 생성용 벡터 생성부
150
키 배포부
160
10
암호화 장치(Enc)
200
공개 키 취득부
210
송신 정보 설정부
220
암호 벡터 생성부
240
데이터 송신부
260
세션 키 생성부
250
복호 장치(Dec)
300
벡터 입력부
310
키 벡터 기억부
320
패어링 연산부
330
키 위양 장치(Delegate I)
400
키 벡터 취득부
410
키 벡터 생성부
420
랜덤화 벡터 생성부
430
키 생성용 벡터 생성부
440
키 배포부
450
pk, sk
pk
pk, $\vec{k}^*_L$
$k^*_{L,ran,j}$ (j=1, …, L+1)
$k^*_{L,del,j}$ (j=μ_L+1, …, n)
$k^*_{L,dec}$
$\vec{x}_L$
pk, x_L
c_1
c_1, c_2
K
$k^*_{L+1,dec}$
$k^*_{L+1,ran,j}$ (j=1, …, L+2)
$\vec{k}^*_{L+1}$
$k^*_{L+1,del,j}$ (j=μ_{L+1}+1, …, n)

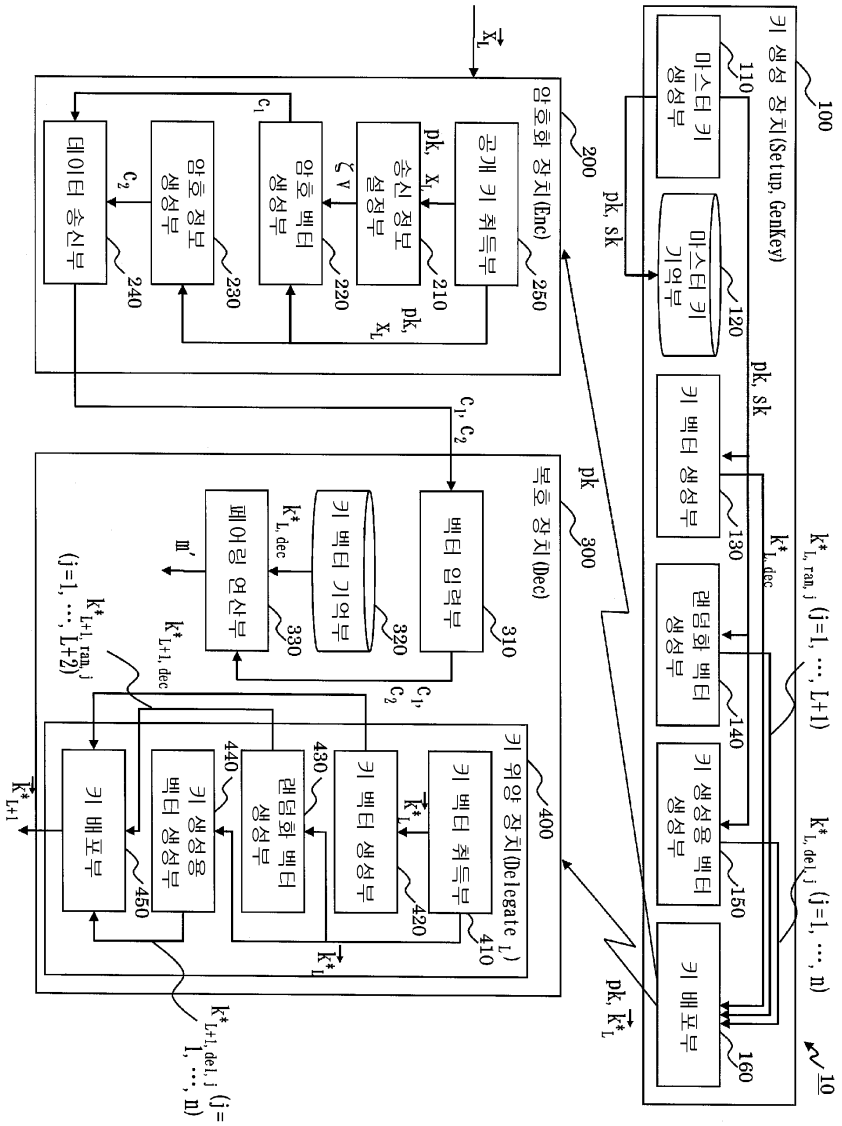
도면18


암호화 장치(200)의 동작
개시
송신 정보 벡터 ζ v의 생성
S701
암호 벡터 c1의 생성
S702
암호 정보 c1의 송신
S703
세션 키 K의 생성
S704
종료

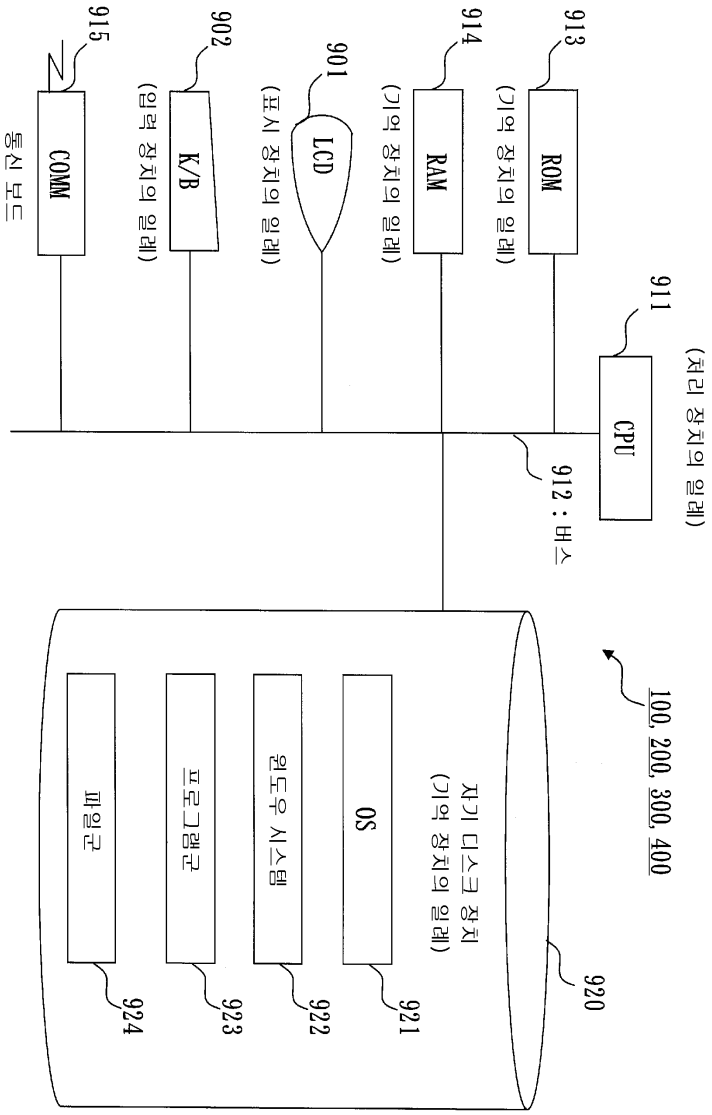
도면19


복호 장치(300)의 동작
개시
암호 벡터 c1의 입력
S801
키 벡터 k*L, dec에 의해 복호하여,
세션 키 K를 추출
S802
종료

도면20


키 생성 장치(Setup, GenKey)
100
마스터 키 생성부
110
마스터 키 기억부
120
키 벡터 생성부
130
랜덤화 벡터 생성부
140
키 생성용 벡터 생성부
150
키 배포부
160
10
pk, sk
$k^*_{L,ran,j}$ (j=1, …, L+1)
$k^*_{L,dec}$
$k^*_{L,del,j}$ (j=1, …, n)
암호화 장치(Enc)
200
공개 키 취득부
250
송신 정보 설정부
210
암호 벡터 생성부
220
암호 정보 생성부
230
데이터 송신부
240
pk, x_L
ζ, v
c_1
c_2
$\vec{x}_L$
pk
복호 장치(Dec)
300
벡터 입력부
310
키 벡터 기억부
320
패어링 연산부
330
$k^*_{L,dec}$
$k^*_{L+1,dec}$
m'
키 위양 장치(Delegate_L)
400
키 벡터 취득부
410
키 벡터 생성부
420
랜덤화 벡터 생성부
430
키 생성용 벡터 생성부
440
키 배포부
450
$\vec{k}^*_L$
$\vec{k}^*_{L+1}$
$k^*_{L+1,ran,j}$ (j=1, …, L+2)
$k^*_{L+1,del,j}$ (j=1, …, n)

도면21


915
통신 보드
902
(입력 장치의 일례)
K/B
901
(표시 장치의 일례)
LCD
914
(기억 장치의 일례)
RAM
913
(기억 장치의 일례)
ROM
911
(처리 장치의 일례)
CPU
912 : 버스
100, 200, 300, 400
920
자기 디스크 장치
(기억 장치의 일례)
921
OS
922
윈도우 시스템
923
프로그램군
924
파일군