(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2014년05월12일
(11) 등록번호 10-1393899
(24) 등록일자 2014년05월02일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01)
(21) 출원번호 10-2013-7012670
(22) 출원일자(국제) 2011년12월06일
심사청구일자 2013년05월16일
(85) 번역문제출일자 2013년05월16일
(65) 공개번호 10-2013-0084669
(43) 공개일자 2013년07월25일
(86) 국제출원번호 PCT/JP2011/078164
(87) 국제공개번호 WO 2012/086405
국제공개일자 2012년06월28일
(30) 우선권주장
JP-P-2010-286511 2010년12월22일 일본(JP)
(56) 선행기술조사문헌
"News Analysis", THE JOURNAL OF THE INSTITUTE OF ELECTRONICS , INFORMATION AND COMMUCATION ENGINEERS,Vol. 93, no. 12, pages 1070 to 1071(December 1. 2010)
Dan Boneh et al., Functional Encryption : Definitions and Challenges, <http ://eprint.iacr.org/cgi-bin/versions.pi ?entry=2010/543>(November 1, 2010)
전체 청구항 수 : 총 8 항

(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

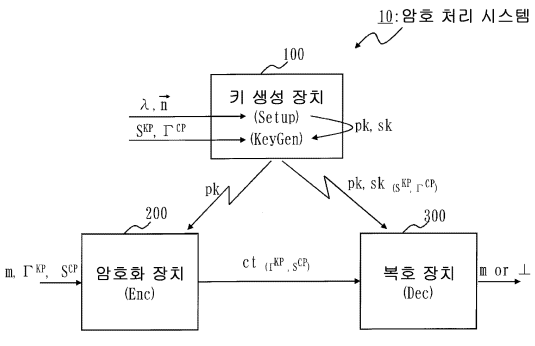
심사관 : 홍기완

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

(57) 요 약

많은 암호 기능을 갖는 안전한 함수형 암호 방식을 제공하는 것을 목적으로 한다. 스팬 프로그램에 속성 벡터의 내적을 적용하는 것에 의해, 액세스 스트럭쳐를 구성했다. 이 액세스 스트럭쳐는, 스팬 프로그램의 설계와, 속성 벡터의 설계에 자유도가 있고, 액세스 제어의 설계에 큰 자유도를 갖는다. 이 액세스 스트럭쳐를, 암호문과 복호 키의 각각에 갖게 하여 함수형 암호 처리를 실현했다.

대 표 도



10 암호 처리 시스템
100 키 생성 장치
200 암호화 장치
300 복호 장치

특허청구의 범위

청구항 1

키 생성 장치와 암호화 장치와 복호 장치를 구비하고, 기저 B_0 및 기저 B_0^*와, t=1, …, d^{KP}(d^{KP}는 1 이상의 정수)의 각 정수 t에 대한 기저 B_t^{KP} 및 기저 $B^*_t{}^{KP}$와, t=1, …, d^{CP}(d^{CP}는 1 이상의 정수)의 각 정수 t에 대한 기저 B_t^{CP} 및 기저 $B^*_t{}^{CP}$를 이용하여 암호 처리를 실행하는 암호 처리 시스템으로서,

상기 키 생성 장치는,

i=1, …, L^{KP}(L^{KP}는 1 이상의 정수)의 각 정수 i에 대한 변수 $\rho^{KP}(i)$로서, 식별 정보 t(t=1, …, d^{KP}의 어느 하나의 정수)와, 속성 벡터 $\vec{v}^{KP}_i:=(v_{i,i'}{}^{KP})(i'=1, \cdots, n_t^{KP}$, n_t^{KP}는 1 이상의 정수)의 긍정형의 조(tuple) $(t, \vec{v}^{KP}_i)$ 또는 부정형의 조 $\neg(t, \vec{v}^{KP}_i)$의 어느 하나인 변수 $\rho^{KP}(i)$와, L^{KP}행 r^{KP}열(r^{KP}는 1 이상의 정수)의 소정의 행렬 M^{KP}를 입력하는 제 1 KP 정보 입력부와,

t=1, …, d^{CP}의 적어도 1개 이상의 정수 t에 대하여, 식별 정보 t와, 속성 벡터 $\vec{x}^{CP}_t:=(x_{t,i'}{}^{CP})(i'=1, \cdots, n_t^{CP}$, n_t^{CP}는 1 이상의 정수)를 갖는 속성 집합 Γ^{CP}를 입력하는 제 1 CP 정보 입력부와,

기저 B^*_0의 기저 벡터 $b^*_{0,p}$(p는 소정의 값)의 계수로서 값 $-s_0^{KP}$($s_0^{KP}:=\vec{h}^{KP}\cdot(\vec{f}^{KP})^T$, $\vec{h}^{KP}$ 및 $\vec{f}^{KP}$는 r^{KP}개의 요소를 갖는 벡터)를 설정하고, 기저 벡터 $b^*_{0,p'}$(p'는 상기 p와는 다른 소정의 값)의 계수로서 난수 δ^{CP}를 설정하고, 기저 벡터 $b^*_{0,q}$(q는 상기 p 및 상기 p'와는 다른 소정의 값)의 계수로서 소정의 값 κ를 설정하여 요소 k^*_0을 생성하는 주 복호 키 생성부와,

상기 $\vec{f}^{KP}$와, 상기 제 1 KP 정보 입력부가 입력한 행렬 M^{KP}에 근거하여 생성되는 열 벡터 $(\vec{s}^{KP})^T:=(s_1^{KP}, \cdots, s_i^{KP})^T:=\vec{M}^{KP}\cdot(\vec{f}^{KP})^T(i=L^{KP})$와, 난수 $\Theta_i^{KP}(i=1, \cdots, L^{KP})$에 근거하여, i=1, …, L^{KP}의 각 정수 i에 대한 요소 $k^*_i{}^{KP}$를 생성하는 KP 복호 키 생성부로서, i=1, …, L^{KP}의 각 정수 i에 대하여, 변수 $\rho^{KP}(i)$가 긍정형의 조 $(t, \vec{v}^{KP}_i)$인 경우에는, 그 조의 식별 정보 t가 나타내는 기저 $B^*_t{}^{KP}$의 기저 벡터 $b^*_{t,1}{}^{KP}$의 계수로서 $s_i^{KP}+\Theta_i^{KP}v_{i,1}{}^{KP}$를 설정함과 아울러, 상기 식별 정보 t와 i'=2, …, n_t^{KP}의 각 정수 i'가 나타내는 기저 벡터 $b^*_{t,i'}{}^{KP}$의 계수로서 $\Theta_i^{KP}v_{i,i'}{}^{KP}$를 설정하여 요소 $k^*_i{}^{KP}$를 생성하고, 변수 $\rho^{KP}(i)$가 부정형의 조 $\neg(t, \vec{v}^{KP}_i)$인 경우에는, 그 조의 식별 정보 t와 i'=1, …, n_{tKP}의 각 정수 i'가 나타내는 기저 벡터 $b^*_{t,i'}{}^{KP}$의 계수로서 $s_i^{KP}v_{i,i'}{}^{KP}$를 설정하여 요소 $k^*_i{}^{KP}$를 생성하는 KP 복호 키 생성부와,

상기 제 1 CP 정보 입력부가 입력한 속성 집합 Γ^{CP}에 포함되는 각 식별 정보 t에 대한 요소 $k^*_t{}^{CP}$를 생성하는 CP 복호 키 생성부로서, 기저 $B^*_t{}^{CP}$의 기저 벡터 $b^*_{t,i'}{}^{CP}(i'=1, \cdots, n_{tCP})$의 계수로서 상기 난수 δ^{CP}배 한 $x_{t,i'}{}^{CP}$를 설정하여 요소 $k^*_t{}^{CP}$를 생성하는 CP 복호 키 생성부

를 구비하고,

상기 암호화 장치는,

t=1, …, d^{KP}의 적어도 1개 이상의 정수 t에 대하여, 식별 정보 t와, 속성 벡터 $\vec{x}^{KP}_t:=(x_{t,i'}{}^{KP})(i'=1, \cdots, n_t^{KP})$

를 갖는 속성 집합 Γ^{KP}를 입력하는 제 2 KP 정보 입력부와,

i=1, …, L^{CP}(L^{CP}는 1 이상의 정수)의 각 정수 i에 대한 변수 $\rho^{CP}(i)$로서, 식별 정보 t(t=1, …, d^{CP}의 어느 하나의 정수)와, 속성 벡터 $\vec{v}_i^{CP}:=(v_{i,i'}^{CP})(i'=1, \cdots, n_t^{CP})$의 긍정형의 조 $(t, \vec{v}_i^{CP})$ 또는 부정형의 조 $\neg(t, \vec{v}_i^{CP})$의 어느 하나인 변수 $\rho^{CP}(i)$와, L^{CP}행 r^{CP}열(r^{CP}는 1 이상의 정수)의 소정의 행렬 $\mathbb{M}^{CP}$를 입력하는 제 2 CP 정보 입력부와,

기저 B_0의 기저 벡터 $b_{0,p}$의 계수로서 난수 ω^{KP}를 설정하고, 기저 벡터 $b_{0,p'}$의 계수로서 값 $-s_0^{CP}(s_0^{CP}:=\vec{h}^{CP}\cdot(\vec{f}^{CP})^T$, $\vec{h}^{CP}$ 및 $\vec{f}^{CP}$는 r^{CP}개의 요소를 갖는 벡터)를 설정하고, 기저 벡터 $b_{0,q}$의 계수로서 난수 ζ를 설정하여 요소 c_0을 생성하는 주 암호화 데이터 생성부와,

상기 제 2 KP 정보 입력부가 입력한 속성 집합 Γ^{KP}에 포함되는 각 식별 정보 t에 대한 요소 c_t^{KP}를 생성하는 KP 암호화 데이터 생성부로서, 기저 B_t^{KP}의 기저 벡터 $b_{t,i'}^{KP}(i'=1, \cdots, n_t)$의 계수로서 상기 난수 ω^{KP}배 한 $x_{t,i'}^{KP}$를 설정하여 요소 c_t^{KP}를 생성하는 KP 암호화 데이터 생성부와,

상기 $\vec{f}^{CP}$와, 상기 제 2 CP 정보 입력부가 입력한 행렬 $\mathbb{M}^{CP}$에 근거하여 생성되는 열 벡터 $(\vec{s}^{CP})^T:=(s_1^{CP}, \cdots, s_i^{CP})^T:=\mathbb{M}^{CP}\cdot(\vec{f}^{CP})^T(i=L^{CP})$와, 난수 $\Theta_i^{CP}(i=1, \cdots, L^{CP})$에 근거하여, i=1, …, L^{CP}의 각 정수 i에 대한 요소 c_i^{CP}를 생성하는 CP 암호화 데이터 생성부로서, i=1, …, L^{CP}의 각 정수 i에 대하여, 변수 $\rho^{CP}(i)$가 긍정형의 조 $(t, \vec{v}_i^{CP})$인 경우에는, 그 조의 식별 정보 t가 나타내는 기저 B_t^{CP}의 기저 벡터 $b_{t,1}^{CP}$의 계수로서 $s_i^{CP}+\Theta_i^{CP}v_{i,1}^{CP}$를 설정함과 아울러, 상기 식별 정보 t와 i'=2, …, n_t^{CP}의 각 정수 i'가 나타내는 기저 벡터 $b_{t,i'}^{CP}$의 계수로서 $\Theta_i^{CP}v_{i,i'}^{CP}$를 설정하여 요소 c_i^{CP}를 생성하고, 변수 $\rho^{CP}(i)$가 부정형의 조 $\neg(t, \vec{v}_i^{CP})$인 경우에는, 그 조의 식별 정보 t와 i'=1, …, n_t^{CP}의 각 정수 i'가 나타내는 기저 벡터 $b_{t,i'}^{CP}$의 계수로서 $s_i^{CP}v_{i,i'}^{CP}$를 설정하여 요소 c_i^{CP}를 생성하는 CP 암호화 데이터 생성부

를 구비하고,

상기 복호 장치는,

상기 주 암호화 데이터 생성부가 생성한 요소 c_0과, 상기 KP 암호화 데이터 생성부가 생성한 요소 c_t^{KP}와, 상기 CP 암호화 데이터 생성부가 생성한 요소 c_i^{CP}와, 상기 속성 집합 Γ^{KP}와, 상기 변수 $\rho^{CP}(i)$를 포함하는 암호화 데이터 $ct_{(\Gamma KP,\ SCP)}$를 취득하는 데이터 취득부와,

상기 주 복호 키 생성부가 생성한 요소 k_0^*과, 상기 KP 복호 키 생성부가 생성한 요소 k_i^{*KP}와, 상기 CP 복호 키 생성부가 생성한 요소 k_t^{*CP}와, 상기 변수 $\rho^{KP}(i)$와, 상기 속성 집합 Γ^{CP}를 포함하는 복호 키 $sk_{(SKP,\ \Gamma CP)}$를 취득하는 복호 키 취득부와,

상기 데이터 취득부가 취득한 암호화 데이터 $ct_{(\Gamma KP,\ SCP)}$에 포함되는 속성 집합 Γ^{KP}와, 상기 복호 키 취득부가 취득한 복호 키 $sk_{(SKP,\ \Gamma CP)}$에 포함되는 변수 $\rho^{KP}(i)$에 근거하여, i=1, …, L^{KP}의 각 정수 i 중, 변수 $\rho^{KP}(i)$가 긍정형의 조 $(t, \vec{v}_i^{KP})$이고, 또한, 그 조의 $\vec{v}_i^{KP}$와, 그 조의 식별 정보 t가 나타내는 Γ^{KP}에 포함되는 $\vec{x}_t^{KP}$의 내적이 0이 되는 i와, 변수 $\rho^{KP}(i)$가 부정형의 조 $\neg(t, \vec{v}_i^{KP})$이고, 또한, 그 조의 $\vec{v}_i^{KP}$와, 그 조의 식별 정보 t

가 나타내는 Γ^{KP}에 포함되는 $\vec{x}_t^{KP}$의 내적이 0이 되지 않는 i의 집합 I^{KP}를 특정함과 아울러, 특정한 집합 I^{KP}에 포함되는 i에 대하여, $\alpha_i^{KP} M_i^{KP}$를 합계한 경우에 상기 $h^{\rightarrow KP}$가 되는 보완 계수 α_i^{KP}를 계산하는 KP 보완 계수 계산부와,

상기 암호화 데이터 $ct_{(\Gamma KP,\ SCP)}$에 포함되는 i=1, …, L^{CP}의 각 정수 i에 대한 변수 $\rho^{CP}(i)$와, 상기 복호 키 $sk_{(SKP,\ \Gamma CP)}$에 포함되는 속성 집합 Γ^{CP}에 근거하여, i=1, …, L^{CP}의 각 정수 i 중, 변수 $\rho^{CP}(i)$가 긍정형의 조 $(t, \vec{v}_i^{CP})$이고, 또한, 그 조의 $\vec{v}_i^{CP}$와, 그 조의 식별 정보 t가 나타내는 Γ^{CP}에 포함되는 $\vec{x}_t^{CP}$의 내적이 0이 되는 i와, 변수 $\rho^{CP}(i)$가 부정형의 조 $\neg(t, \vec{v}_i^{CP})$이고, 또한, 그 조의 $\vec{v}_i^{CP}$와, 그 조의 식별 정보 t가 나타내는 Γ^{CP}에 포함되는 $\vec{x}_t^{CP}$의 내적이 0이 되지 않는 i의 집합 I^{CP}를 특정함과 아울러, 특정한 집합 I^{CP}에 포함되는 i에 대하여, $\alpha_i^{CP} M_i^{CP}$를 합계한 경우에 상기 $h^{\rightarrow CP}$가 되는 보완 계수 α_i^{CP}를 계산하는 CP 보완 계수 계산부와,

상기 암호화 데이터 $ct_{(\Gamma KP,\ SCP)}$에 포함되는 요소 c_0과 요소 c_t^{KP}와 요소 c_i^{CP}와, 상기 복호 키 $sk_{(SKP,\ \Gamma CP)}$에 포함되는 요소 k^*_0과 요소 k^{*KP}_i와 요소 k^{*CP}_t에 대하여, 상기 KP 보완 계수 계산부가 특정한 집합 I^{KP}와, 상기 KP 보완 계수 계산부가 계산한 보완 계수 α_i^{KP}와, 상기 CP 보완 계수 계산부가 특정한 집합 I^{CP}와, 상기 CP 보완 계수 계산부가 계산한 보완 계수 α_i^{CP}에 근거하여, 수학식 1에 나타내는 페어링 연산을 행하여 값 K를 계산하는 페어링 연산부

를 구비하는 것을 특징으로 하는 암호 처리 시스템.

[수학식 1]

$$K := e(c_0, k_0^*) \cdot \prod_{i \in I^{KP} \wedge \rho^{KP}(i)=(t,\vec{v}_i^{KP})} e(c_t^{KP}, k_i^{*KP})^{\alpha_i^{KP}} \cdot \prod_{i \in I^{KP} \wedge \rho^{KP}(i)=\neg(t,\vec{v}_i^{KP})} e(c_t^{KP}, k_i^{*KP})^{\alpha_i^{KP}/(\vec{v}_i^{KP} \cdot \vec{x}_t^{KP})} \cdot \prod_{i \in I^{CP} \wedge \rho^{CP}(i)=(t,\vec{v}_i^{CP})} e(c_t^{CP}, k_i^{*CP})^{\alpha_i^{CP}} \cdot \prod_{i \in I^{CP} \wedge \rho^{CP}(i)=\neg(t,\vec{v}_i^{CP})} e(c_t^{CP}, k_i^{*CP})^{\alpha_i^{CP}/(\vec{v}_i^{CP} \cdot \vec{x}_t^{CP})}$$

청구항 2

제 1 항에 있어서,

상기 암호 처리 시스템은,

적어도 기저 벡터 $b_{0,i}$(i=1, 2, …, $2+u_0$, $2+u_0+1$, …, $2+u_0+1+w_0$, …, $2+u_0+1+z_0$)를 갖는 기저 B_0과,

적어도 기저 벡터 $b^*_{0,i}$(i=1, 2, …, $2+u_0$, $2+u_0+1$, …, $2+u_0+1+w_0$, …, $2+u_0+1+z_0$)를 갖는 기저 B^*_0과,

적어도 기저 벡터 $b_{t,i}^{KP}$(i=1, …, n_t^{KP}, …, $n_t^{KP}+u_t^{KP}$, …, $n_t^{KP}+u_t^{KP}+w_t^{KP}$, …, $n_t^{KP}+u_t^{KP}+w_t^{KP}+z_t^{KP}$)($u_t^{KP}$, w_t^{KP}, z_t^{KP}는 1 이상의 정수)를 갖는 기저 B_t^{KP}(t=1, …, d)와,

적어도 기저 벡터 $b^*_{t,i}{}^{KP}$(i=1, …, n_t^{KP}, …, $n_t^{KP}+u_t^{KP}$, …, $n_t^{KP}+u_t^{KP}+w_t^{KP}$, …, $n_t^{KP}+u_t^{KP}+w_t^{KP}+z_t^{KP}$)를 갖는 기저

B^{*KP}_t(t=1, …, d^{KP})와,

적어도 기저 벡터 $b^{CP}_{t,i}$(i=1, …, n^{CP}_t, …, $n^{CP}_t+u^{CP}_t$, …, $n^{CP}_t+u^{CP}_t+w^{CP}_t$, …, $n^{CP}_t+u^{CP}_t+w^{CP}_t+z^{CP}_t$)($u^{CP}_t$, w^{CP}_t, z^{CP}_t는 1 이상의 정수)를 갖는 기저 B^{CP}_t(t=1, …, d)와,

적어도 기저 벡터 $b^{*CP}_{t,i}$(i=1, …, n^{CP}_t, …, $n^{CP}_t+u^{CP}_t$, …, $n^{CP}_t+u^{CP}_t+w^{CP}_t$, …, $n^{CP}_t+u^{CP}_t+w^{CP}_t+z^{CP}_t$)를 갖는 기저 B^{*CP}_t(t=1, …, d_{CP})

를 이용하여 암호 처리를 실행하고,

상기 키 생성 장치에서는,

상기 주 복호 키 생성부는, 난수 δ^{CP}, $\eta_{0,i}$(i=1, …, w_0)와 소정의 값 κ에 근거하여 수학식 2에 나타내는 요소 k^*_0을 생성하고,

상기 KP 복호 키 생성부는, 상기 변수 ρ^{KP}(i)가 긍정형의 조 (t, $\vec{v}^{KP}_i$)인 경우에는, 난수 Θ^{KP}_i, $\eta^{KP}_{i,i'}$(i=1, …, L^{KP}, i'=1, …, w^{KP}_t)에 근거하여 수학식 3에 나타내는 요소 k^{*KP}_i를 생성하고, 변수 ρ^{KP}(i)가 부정형의 조 ㄱ(t, $\vec{v}^{KP}_i$)인 경우에는, 난수 $\eta^{KP}_{i,i'}$(i=1, …, L^{KP}, i'=1, …, w^{KP}_t)에 근거하여 수학식 4에 나타내는 요소 k^{*KP}_i를 생성하고,

상기 CP 복호 키 생성부는, 상기 난수 δ^{CP}와 난수 $\eta^{CP}_{t,i}$(i=1, …, w^{CP}_t)에 근거하여 수학식 5에 나타내는 요소 k^{*CP}_t를 생성하고,

상기 암호화 장치에서는,

상기 주 암호화 데이터 생성부는, 상기 난수 ω^{KP}와 난수 ζ, $\phi_{0,i}$(i=1, …, z_0)에 근거하여 수학식 6에 나타내는 요소 c_0을 생성하고,

상기 KP 암호화 데이터 생성부는, 상기 난수 ω^{KP}와 난수 $\phi^{KP}_{t,i}$(i=1, …, z^{KP}_t)에 근거하여 수학식 7에 나타내는 요소 c^{KP}_t를 생성하고,

상기 CP 암호화 데이터 생성부는, 상기 변수 ρ^{CP}(i)가 긍정형의 조 (t, $\vec{v}^{CP}_i$)인 경우에는, 난수 Θ^{CP}_i, $\phi^{CP}_{i,i'}$(i=1, …, L^{CP}, i'=1, …, z^{CP}_t)에 근거하여 수학식 8에 나타내는 요소 c^{CP}_i를 생성하고, 변수 ρ^{CP}(i)가 부정형의 조 ㄱ(t, $\vec{v}^{CP}_i$)인 경우에는, 난수 $\phi^{CP}_{i,i'}$(i=1, …, L^{CP}, i'=1, …, z^{CP}_t)에 근거하여 수학식 9에 나타내는 요소 c^{CP}_i를 생성하는

것을 특징으로 하는 암호 처리 시스템.

[수학식 2]

$$k^*_0 := (-s^{KP}_0, \delta^{CP}, \overbrace{0^{u_0}}^{u_0}, 1, \overbrace{\eta_{0,1},\ldots,\eta_{0,w_0}}^{w_0}, \overbrace{0^{z_0}}^{z_0})_{\mathbb{B}^*_0}$$

[수학식 3]

$$k_i^{*\mathsf{KP}} := (\overbrace{s_i^{\mathsf{KP}} + \theta_i^{\mathsf{KP}} v_{i,1}^{\mathsf{KP}}, \theta_i^{\mathsf{KP}} v_{i,2}^{\mathsf{KP}}, \ldots, \theta_i^{\mathsf{KP}} v_{i,n_t^{\mathsf{KP}}}^{\mathsf{KP}}}^{n_t^{\mathsf{KP}}}, \overbrace{0^{u_t^{\mathsf{KP}}},}^{u_t^{\mathsf{KP}}} \overbrace{\eta_{i,1}^{\mathsf{KP}}, \ldots, \eta_{i,w_t^{\mathsf{KP}}}^{\mathsf{KP}}}^{w_t^{\mathsf{KP}}}, \overbrace{0^{z_t^{\mathsf{KP}}}}^{z_t^{\mathsf{KP}}})_{\mathbb{B}_t^{*\mathsf{KP}}}$$

[수학식 4]

$$k_i^{*\mathsf{KP}} := (\overbrace{s_i^{\mathsf{KP}} v_{i,1}^{\mathsf{KP}}, \ldots, s_i^{\mathsf{KP}} v_{i,n_t^{\mathsf{KP}}}^{\mathsf{KP}}}^{n_t^{\mathsf{KP}}}, \overbrace{0^{u_t^{\mathsf{KP}}},}^{u_t^{\mathsf{KP}}} \overbrace{\eta_{i,1}^{\mathsf{KP}}, \ldots, \eta_{i,w_t^{\mathsf{KP}}}^{\mathsf{KP}}}^{w_t^{\mathsf{KP}}}, \overbrace{0^{z_t^{\mathsf{KP}}}}^{z_t^{\mathsf{KP}}})_{\mathbb{B}_t^{*\mathsf{KP}}}$$

[수학식 5]

$$k_t^{*\mathsf{CP}} := (\overbrace{\delta^{\mathsf{CP}} \vec{x}_t^{\mathsf{CP}},}^{n_t^{\mathsf{CP}}} \overbrace{0^{u_t^{\mathsf{CP}},}}^{u_t^{\mathsf{CP}}} \overbrace{\eta_{t,1}^{\mathsf{CP}}, \ldots, \eta_{t,w_t^{\mathsf{CP}}}^{\mathsf{CP}},}^{w_t^{\mathsf{CP}}} \overbrace{0^{z_t^{\mathsf{KP}}}}^{z_t^{\mathsf{KP}}})_{\mathbb{B}_t^{*\mathsf{CP}}}$$

[수학식 6]

$$c_0 := (\omega^{\mathsf{KP}}, -s_0^{\mathsf{CP}}, \overbrace{0^{u_0},}^{u_0} \zeta, \overbrace{0^{w_0},}^{w_0} \overbrace{\varphi_{0,1}, \ldots, \varphi_{0,z_0}}^{z_0})_{\mathbb{B}_0}$$

[수학식 7]

$$c_t^{\mathsf{KP}} := (\overbrace{\omega^{\mathsf{KP}} \vec{x}_t^{\mathsf{KP}},}^{n_t^{\mathsf{KP}}} \overbrace{0^{u_t^{\mathsf{KP}},}}^{u_t^{\mathsf{KP}}} \overbrace{0^{w_t^{\mathsf{KP}},}}^{w_t^{\mathsf{KP}}} \overbrace{\varphi_{t,1}^{\mathsf{KP}}, \ldots, \varphi_{t,z_t^{\mathsf{KP}}}^{\mathsf{KP}}}^{z_t^{\mathsf{KP}}})_{\mathbb{B}_t^{\mathsf{KP}}}$$

[수학식 8]

$$c_i^{\mathsf{CP}} := (\overbrace{s_i^{\mathsf{CP}} + \theta_i^{\mathsf{CP}} v_{i,1}^{\mathsf{CP}}, \theta_i^{\mathsf{CP}} v_{i,2}^{\mathsf{CP}}, \ldots, \theta_i^{\mathsf{CP}} v_{i,n_t^{\mathsf{CP}}}^{\mathsf{CP}}}^{n_t^{\mathsf{CP}}}, \overbrace{0^{u_t^{\mathsf{CP}},}}^{u_t^{\mathsf{CP}}} \overbrace{0^{w_t^{\mathsf{CP}},}}^{w_t^{\mathsf{CP}}} \overbrace{\varphi_{i,1}^{\mathsf{CP}}, \ldots, \varphi_{i,z_t^{\mathsf{CP}}}^{\mathsf{CP}}}^{z_t^{\mathsf{CP}}})_{\mathbb{B}_t^{\mathsf{CP}}}$$

[수학식 9]

$$c_i^{\mathsf{CP}} := (\overbrace{s_i^{\mathsf{CP}} v_{i,1}^{\mathsf{CP}}, \ldots, s_i^{\mathsf{CP}} v_{i,n_t^{\mathsf{CP}}}^{\mathsf{CP}}}^{n_t^{\mathsf{CP}}}, \overbrace{0^{u_t^{\mathsf{CP}},}}^{u_t^{\mathsf{CP}}} \overbrace{0^{w_t^{\mathsf{CP}},}}^{w_t^{\mathsf{CP}}} \overbrace{\varphi_{i,1}^{\mathsf{CP}}, \ldots, \varphi_{i,z_t^{\mathsf{CP}}}^{\mathsf{CP}}}^{z_t^{\mathsf{CP}}})_{\mathbb{B}_t^{\mathsf{CP}}}$$

청구항 3

제 1 항 또는 제 2 항에 있어서,

상기 암호화 장치는,

소정의 값 i에 대하여 $g_T=e(b_{0,i}, b^*_{0,i})$이고, t=1, …, d^{KP}의 각 정수 t와 소정의 값 i에 대하여 $g_T=e(b_{t,i}, b^*_{t,i})$이고, t=1, …, d^{CP}의 각 정수 t와 소정의 값 i에 대하여 $g_T=e(b_{t,i}, b^*_{t,i})$인 값 g_T를 이용하여, 메시지 m을 삽입한 요소 $c_{d+1}=g_T^{\zeta}m$을 생성하는 메시지 암호화 데이터 생성부

를 더 구비하고,

상기 복호 장치에서는,

상기 데이터 취득부는, 상기 요소 c_{d+1}을 포함하는 암호화 데이터 $ct_{(\Gamma^{KP}, SCP)}$를 더 취득하고,

상기 복호 장치는,

상기 암호화 데이터 $ct_{(\Gamma^{KP}, SCP)}$에 포함되는 상기 요소 c_{d+1}을, 상기 페어링 연산부가 계산한 값 K로 나누어, 상기 메시지 m을 계산하는 메시지 계산부

를 더 구비하는 것을 특징으로 하는 암호 처리 시스템.

청구항 4

기저 B_0 및 기저 B_0^*와, t=1, …, d^{KP}(d^{KP}는 1 이상의 정수)의 각 정수 t에 대한 기저 B_t^{KP} 및 기저 $B^*{}_t^{KP}$와, t=1, …, d^{CP}(d^{CP}는 1 이상의 정수)의 각 정수 t에 대한 기저 B_t^{CP} 및 기저 $B^*{}_t^{CP}$를 이용하여 암호 처리를 실행하는 암호 처리 시스템에 있어서, 복호 키 $sk_{(SKP, \Gamma CP)}$를 생성하는 키 생성 장치로서,

i=1, …, L^{KP}(L^{KP}는 1 이상의 정수)의 각 정수 i에 대한 변수 $\rho^{KP}(i)$로서, 식별 정보 t(t=1, …, d^{KP}의 어느 하나의 정수)와, 속성 벡터 $\vec{v}_i^{KP}:=(v_{i,i'}{}^{KP})$(i'=1, …, n_t^{KP}, n_t^{KP}는 1 이상의 정수)의 긍정형의 조 $(t, \vec{v}_i^{KP})$ 또는 부정형의 조 $\neg(t, \vec{v}_i^{KP})$의 어느 하나인 변수 $\rho^{KP}(i)$와, L^{KP}행 r^{KP}열(r^{KP}는 1 이상의 정수)의 소정의 행렬 M^{KP}를 입력하는 제 1 KP 정보 입력부와,

t=1, …, d^{CP}의 적어도 1개 이상의 정수 t에 대하여, 식별 정보 t와, 속성 벡터 $\vec{x}_t^{CP}:=(x_{t,i'}{}^{CP})$(i'=1, …, n_t^{CP}, n_t^{CP}는 1 이상의 정수)를 갖는 속성 집합 Γ^{CP}를 입력하는 제 1 CP 정보 입력부와,

기저 B^*_0의 기저 벡터 $b^*_{0,p}$(p는 소정의 값)의 계수로서 값 $-s_0^{KP}$($s_0^{KP}:=\vec{h}^{KP}\cdot(\vec{f}^{KP})_T$, $\vec{h}^{KP}$ 및 $\vec{f}^{KP}$는 r^{KP}개의 요소를 갖는 벡터)를 설정하고, 기저 벡터 $b^*_{0,p'}$(p'는 상기 p와는 다른 소정의 값)의 계수로서 난수 δ^{CP}를 설정하고, 기저 벡터 $b^*_{0,q}$(q는 상기 p 및 상기 p'와는 다른 소정의 값)의 계수로서 소정의 값 κ를 설정하여 복호 키 $sk_{(SKP, \Gamma CP)}$의 요소 k^*_0을 생성하는 주 복호 키 생성부와,

상기 $\vec{f}^{KP}$와, 상기 제 1 KP 정보 입력부가 입력한 행렬 M^{KP}에 근거하여 생성되는 열 벡터 $(\vec{s}^{KP})^T:=(s_1^{KP}, …, s_i^{KP})^T:=M^{KP}\cdot(\vec{f}^{KP})_T$(i=$L^{KP}$)와, 난수 Θ_i^{KP}(i=1, …, L^{KP})에 근거하여, i=1, …, L^{KP}의 각 정수 i에 대한 요소 $k^*_i{}^{KP}$를 생성하는 KP 복호 키 생성부로서, i=1, …, L^{KP}의 각 정수 i에 대하여, 변수 $\rho^{KP}(i)$가 긍정형의 조 $(t, \vec{v}_i^{KP})$인 경우에는, 그 조의 식별 정보 t가 나타내는 기저 $B^*{}_t^{KP}$의 기저 벡터 $b^*{}_{t,1}^{KP}$의 계수로서 $s_i^{KP}+\Theta_i^{KP}v_{i,1}^{KP}$를 설정함과 아울러, 상기 식별 정보 t와 i'=2, …, n_t^{KP}의 각 정수 i'가 나타내는 기저 벡터 $b^*{}_{t,i'}^{KP}$의 계수로서 $\Theta_i^{KP}v_{i,i'}^{KP}$를 설정하여 복호 키 $sk_{(SKP, \Gamma CP)}$의 요소 $k^*_i{}^{KP}$를 생성하고, 변수 $\rho^{KP}(i)$가 부정형의 조 $\neg(t, \vec{v}_i^{KP})$인 경우에는, 그 조의 식별 정보 t와 i'=1, …, n_t^{KP}의 각 정수 i'가 나타내는 기저 벡터 $b^*{}_{t,i'}^{KP}$의 계수로서 $s_i^{KP}v_{i,i'}^{KP}$를 설정하여 복호 키 $sk_{(SKP, \Gamma CP)}$의 요소 $k^*_i{}^{KP}$를 생성하는 KP 복호 키 생성부와,

상기 제 1 CP 정보 입력부가 입력한 속성 집합 Γ^{CP}에 포함되는 각 식별 정보 t에 대한 요소 $k^*_t{}^{CP}$를 생성하는 CP 복호 키 생성부로서, 기저 $B^*{}_t^{CP}$의 기저 벡터 $b^*{}_{t,i'}^{CP}$(i'=1, …, n_t^{CP})의 계수로서 상기 난수 δ^{CP}배 한 $x_{t,i'}^{CP}$를 설

정하여 복호 키 $sk_{(SKP,\ \Gamma CP)}$의 요소 k^{*CP}_t를 생성하는 CP 복호 키 생성부

를 구비하는 것을 특징으로 하는 키 생성 장치.

청구항 5

기저 B_0 및 기저 B_0^*와, t=1, …, d^{KP}(d^{KP}는 1 이상의 정수)의 각 정수 t에 대한 기저 B_t^{KP} 및 기저 B^{*KP}_t와, t=1, …, d^{CP}(d^{CP}는 1 이상의 정수)의 각 정수 t에 대한 기저 B_t^{CP} 및 기저 B^{*CP}_t를 이용하여 암호 처리를 실행하는 암호 처리 시스템에 있어서, 암호화 데이터 $ct_{(\Gamma KP,\ SCP)}$를 생성하는 암호화 장치로서,

t=1, …, d^{KP}의 적어도 1개 이상의 정수 t에 대하여, 식별 정보 t와, 속성 벡터 $\vec{x}^{KP}_t:=(x_{t,i'}{}^{KP})(i'=1,\ \cdots,\ n_t^{KP})$를 갖는 속성 집합 Γ^{KP}를 입력하는 제 2 KP 정보 입력부와,

i=1, …, L^{CP}(L^{CP}는 1 이상의 정수)의 각 정수 i에 대한 변수 $\rho^{CP}(i)$로서, 식별 정보 t(t=1, …, d^{CP}의 어느 하나의 정수)와, 속성 벡터 $\vec{v}^{CP}_i:=(v_{i,i'}{}^{CP})(i'=1,\ \cdots,\ n_t^{CP})$의 긍정형의 조 $(t,\ \vec{v}^{CP}_i)$ 또는 부정형의 조 $\neg(t,\ \vec{v}^{CP}_i)$의 어느 하나인 변수 $\rho^{CP}(i)$와, L^{CP}행 r^{CP}열(r^{CP}는 1 이상의 정수)의 소정의 행렬 $\mathbb{M}^{CP}$를 입력하는 제 2 CP 정보 입력부와,

기저 B_0의 기저 벡터 $b_{0,p}$의 계수로서 난수 ω^{KP}를 설정하고, 기저 벡터 $b_{0,p'}$의 계수로서 값 $-s_0^{CP}$($s_0^{CP}:=\vec{h}^{CP}\cdot(\vec{f}^{CP})^T$, $\vec{h}^{CP}$ 및 $\vec{f}^{CP}$는 r^{CP}개의 요소를 갖는 벡터)를 설정하고, 기저 벡터 $b_{0,q}$의 계수로서 난수 ζ를 설정하여 암호화 데이터 $ct_{(\Gamma KP,\ SCP)}$의 요소 c_0을 생성하는 주 암호화 데이터 생성부와,

상기 제 2 KP 정보 입력부가 입력한 속성 집합 Γ^{KP}에 포함되는 각 식별 정보 t에 대한 요소 c_t^{KP}를 생성하는 KP 암호화 데이터 생성부로서, 기저 B_t^{KP}의 기저 벡터 $b_{t,i'}{}^{KP}(i'=1,\ \cdots,\ n_t)$의 계수로서 상기 난수 ω^{KP}배 한 $x_{t,i'}{}^{KP}$를 설정하여 암호화 데이터 $ct_{(\Gamma KP,\ SCP)}$의 요소 c_t^{KP}를 생성하는 KP 암호화 데이터 생성부와,

상기 $\vec{f}^{CP}$와, 상기 제 2 CP 정보 입력부가 입력한 행렬 $\mathbb{M}^{CP}$에 근거하여 생성되는 열 벡터 $(\vec{s}^{CP})^T:=(s_1^{CP},\ \cdots,\ s_i^{CP})^T:=\mathbb{M}^{CP}\cdot(\vec{f}^{CP})^T(i=L^{CP})$와, 난수 $\Theta_i^{CP}(i=1,\ \cdots,\ L^{CP})$에 근거하여, i=1, …, L^{CP}의 각 정수 i에 대한 요소 c_i^{CP}를 생성하는 CP 암호화 데이터 생성부로서, i=1, …, L^{CP}의 각 정수 i에 대하여, 변수 $\rho^{CP}(i)$가 긍정형의 조 $(t,\ \vec{v}^{CP}_i)$인 경우에는, 그 조의 식별 정보 t가 나타내는 기저 B_t^{CP}의 기저 벡터 $b_{t,1}{}^{CP}$의 계수로서 $s_i^{CP}+\Theta_i^{CP}v_{i,1}{}^{CP}$를 설정함과 아울러, 상기 식별 정보 t와 i'=2, …, n_t^{CP}의 각 정수 i'가 나타내는 기저 벡터 $b_{t,i'}{}^{CP}$의 계수로서 $\Theta_i^{CP}v_{i,i'}{}^{CP}$를 설정하여 암호화 데이터 $ct_{(\Gamma KP,\ SCP)}$의 요소 c_i^{CP}를 생성하고, 변수 $\rho^{CP}(i)$가 부정형의 조 $\neg(t,\ \vec{v}^{CP}_i)$인 경우에는, 그 조의 식별 정보 t와 i'=1, …, n_t^{CP}의 각 정수 i'가 나타내는 기저 벡터 $b_{t,i'}{}^{CP}$의 계수로서 $s_i^{CP}v_{i,i'}{}^{CP}$를 설정하여 암호화 데이터 $ct_{(\Gamma KP,\ SCP)}$의 요소 c_i^{CP}를 생성하는 CP 암호화 데이터 생성부

를 구비하는 것을 특징으로 하는 암호화 장치.

청구항 6

기저 B_0 및 기저 B_0^*와, t=1, …, d^{KP}(d^{KP}는 1 이상의 정수)의 각 정수 t에 대한 기저 B_t^{KP} 및 기저 B^{*KP}_t와, t=1,

…, d^{CP}(d^{CP}는 1 이상의 정수)의 각 정수 t에 대한 기저 B_t^{CP} 및 기저 B^{*CP}_t를 이용하여 암호 처리를 실행하는 암호 처리 시스템에 있어서, 암호화 데이터 $ct_{(\Gamma^{KP},\ SCP)}$를 복호 키 $sk_{(SKP,\ \Gamma^{CP})}$로 복호하는 복호 장치로서,

t=1, …, d^{KP}의 적어도 1개 이상의 정수 t에 대하여, 식별 정보 t와, 속성 벡터 $\vec{x}_t^{KP}:=(x_{t,i'}^{KP})(i'=1, \cdots, n_t^{KP}$, n_t^{KP}는 1 이상의 정수)를 갖는 속성 집합 Γ^{KP}와,

i=1, …, L^{CP}(L^{CP}는 1 이상의 정수)의 각 정수 i에 대한 변수 $\rho^{CP}(i)$로서, 식별 정보 t(t=1, …, d^{CP}의 어느 하나의 정수)와, 속성 벡터 $\vec{v}_i^{CP}:=(v_{i,i'}^{CP})(i'=1, \cdots, n_t^{CP}$, n_t^{CP}는 1 이상의 정수)의 긍정형의 조 $(t, \vec{v}_i^{CP})$ 또는 부정형의 조 $\neg(t, \vec{v}_i^{CP})$의 어느 하나인 변수 $\rho^{CP}(i)$와,

L^{CP}행 r^{CP}열(r^{CP}는 1 이상의 정수)의 소정의 행렬 $\mathbb{M}^{CP}$와,

기저 B_0의 기저 벡터 $b_{0,p}$의 계수로서 난수 ω^{KP}가 설정되고, 기저 벡터 $b_{0,p'}$의 계수로서 값 $-s_0^{CP}$($s_0^{CP}:=\vec{h}^{CP}\cdot(\vec{f}^{CP})^T$, $\vec{h}^{CP}$ 및 $\vec{f}^{CP}$는 r^{CP}개의 요소를 갖는 벡터)가 설정되고, 기저 벡터 $b_{0,q}$의 계수로서 난수 ζ가 설정된 요소 c_0과,

상기 속성 집합 Γ^{KP}에 포함되는 각 식별 정보 t에 대하여, 기저 B_t^{KP}의 기저 벡터 $b_{t,i'}^{KP}(i'=1, \cdots, n_t)$의 계수로서 상기 난수 ω^{KP}배 한 $x_{t,i'}^{KP}$가 설정된 요소 c_t^{KP}와,

상기 $\vec{f}^{CP}$와, 상기 행렬 $\mathbb{M}^{CP}$에 근거하여 생성되는 열 벡터 $(\vec{s}^{CP})^T:=(s_1^{CP}, \cdots, s_i^{CP})^T:=\mathbb{M}^{CP}\cdot(\vec{f}^{CP})^T(i=L^{CP})$와, 난수 $\Theta_i^{CP}(i=1, \cdots, L^{CP})$에 근거하여, i=1, …, L^{CP}의 각 정수 i에 대하여 생성된 요소 c_i^{CP}로서, i=1, …, L^{CP}의 각 정수 i에 대하여, 변수 $\rho^{CP}(i)$가 긍정형의 조 $(t, \vec{v}_i^{CP})$인 경우에는, 그 조의 식별 정보 t가 나타내는 기저 B_t^{CP}의 기저 벡터 $b_{t,1}^{CP}$의 계수로서 $s_i^{CP}+\Theta_i^{CP}v_{i,1}^{CP}$가 설정됨과 아울러, 상기 식별 정보 t와 i'=2, …, n_t^{CP}의 각 정수 i'가 나타내는 기저 벡터 $b_{t,i'}^{CP}$의 계수로서 $\Theta_i^{CP}v_{i,i'}^{CP}$가 설정되고, 변수 $\rho^{CP}(i)$가 부정형의 조 $\neg(t, \vec{v}_i^{CP})$인 경우에는, 그 조의 식별 정보 t와 i'=1, …, n_t^{CP}의 각 정수 i'가 나타내는 기저 벡터 $b_{t,i'}^{CP}$의 계수로서 $s_i^{CP}v_{i,i'}^{CP}$가 설정된 요소 c_i^{CP}

를 포함하는 암호화 데이터 $ct_{(\Gamma^{KP},\ SCP)}$를 취득하는 데이터 취득부와,

i=1, …, L^{KP}(L^{KP}는 1 이상의 정수)의 각 정수 i에 대한 변수 $\rho^{KP}(i)$로서, 식별 정보 t(t=1, …, d^{KP}의 어느 하나의 정수)와, 속성 벡터 $\vec{v}_i^{KP}:=(v_{i,i'}^{KP})(i'=1, \cdots, n_t^{KP})$의 긍정형의 조 $(t, \vec{v}_i^{KP})$ 또는 부정형의 조 $\neg(t, \vec{v}_i^{KP})$의 어느 하나인 변수 $\rho^{KP}(i)$와,

L^{KP}행 r^{KP}열(r^{KP}는 1 이상의 정수)의 소정의 행렬 $\mathbb{M}^{KP}$와,

t=1, …, d^{CP}의 적어도 1개 이상의 정수 t에 대하여, 식별 정보 t와, 속성 벡터 $\vec{x}_t^{CP}:=(x_{t,i'}^{CP})(i'=1, \cdots, n_t^{CP})$를 갖는 속성 집합 Γ^{CP}와,

기저 B^*_0의 기저 벡터 $b^*_{0,p}$(p는 소정의 값)의 계수로서 값 $-s_0^{KP}$($s_0^{KP}:=\vec{h}^{KP}\cdot(\vec{f}^{KP})^T$, $\vec{h}^{KP}$ 및 $\vec{f}^{KP}$는 r^{KP}개의 요소를 갖는 벡터)가 설정되고, 기저 벡터 $b^*_{0,p'}$(p'는 상기 p와는 다른 소정의 값)의 계수로서 난수 δ^{CP}가 설정되고,

기저 벡터 $b^{*}_{0,q}$(q는 상기 p 및 상기 p'와는 다른 소정의 값)의 계수로서 소정의 값 κ가 설정된 요소 k^{*}_{0}과,

상기 $f^{\rightarrow KP}$와, 상기 행렬 M^{KP}에 근거하여 생성되는 열 벡터 $(s^{\rightarrow KP})^{T}:=(s_1^{KP}, \cdots, s_i^{KP})^{T}:=M^{KP}\cdot(f^{\rightarrow KP})^{T}(i=L^{KP})$와, 난수 $\Theta_i^{KP}(i=1, \cdots, L^{KP})$에 근거하여, i=1, …, L^{KP}의 각 정수 i에 대하여 생성된 요소 k^{*KP}_i로서, i=1, …, L^{KP}의 각 정수 i에 대하여, 변수 $\rho^{KP}(i)$가 긍정형의 조 $(t, v^{\rightarrow KP}_i)$인 경우에는, 그 조의 식별 정보 t가 나타내는 기저 B^{*KP}_t의 기저 벡터 $b^{*KP}_{t,1}$의 계수로서 $s_i^{KP}+\Theta_i^{KP}v_{i,1}^{KP}$가 설정됨과 아울러, 상기 식별 정보 t와 i'=2, …, n_t^{KP}의 각 정수 i'가 나타내는 기저 벡터 $b^{*KP}_{t,i'}$의 계수로서 $\Theta_i^{KP}v_{i,i'}^{KP}$가 설정되고, 변수 $\rho^{KP}(i)$가 부정형의 조 $\neg(t, v^{\rightarrow KP}_i)$인 경우에는, 그 조의 식별 정보 t와 i'=1, …, n_t^{KP}의 각 정수 i'가 나타내는 기저 벡터 $b^{*KP}_{t,i'}$의 계수로서 $s_i^{KP}v_{i,i'}^{KP}$가 설정된 요소 k^{*KP}_i와,

상기 속성 집합 Γ^{CP}에 포함되는 각 식별 정보 t에 대하여, 기저 B^{*CP}_t의 기저 벡터 $b^{*CP}_{t,i'}$(i'=1, …, n_t^{CP})의 계수로서 상기 난수 δ^{CP}배 한 $x_{t,i'}^{CP}$가 설정된 요소 k^{*CP}_t

를 포함하는 복호 키 $sk_{(SKP,\ \Gamma CP)}$를 취득하는 복호 키 취득부와,

상기 데이터 취득부가 취득한 암호화 데이터 $ct_{(\Gamma KP,\ SCP)}$에 포함되는 속성 집합 Γ^{KP}와, 상기 복호 키 취득부가 취득한 복호 키 $sk_{(SKP,\ \Gamma CP)}$에 포함되는 변수 $\rho^{KP}(i)$에 근거하여, i=1, …, L^{KP}의 각 정수 i 중, 변수 $\rho^{KP}(i)$가 긍정형의 조 $(t, v^{\rightarrow KP}_i)$이고, 또한, 그 조의 $v^{\rightarrow KP}_i$와, 그 조의 식별 정보 t가 나타내는 Γ^{KP}에 포함되는 $x^{\rightarrow KP}_t$의 내적이 0이 되는 i와, 변수 $\rho^{KP}(i)$가 부정형의 조 $\neg(t, v^{\rightarrow KP}_i)$이고, 또한, 그 조의 $v^{\rightarrow KP}_i$와, 그 조의 식별 정보 t가 나타내는 Γ^{KP}에 포함되는 $x^{\rightarrow KP}_t$의 내적이 0이 되지 않는 i의 집합 I^{KP}를 특정함과 아울러, 특정한 집합 I^{KP}에 포함되는 i에 대하여, $\alpha_i^{KP}M_i^{KP}$를 합계한 경우에 상기 $h^{\rightarrow KP}$가 되는 보완 계수 α_i^{KP}를 계산하는 KP 보완 계수 계산부와,

상기 암호화 데이터 $ct_{(\Gamma KP,\ SCP)}$에 포함되는 i=1, …, L^{CP}의 각 정수 i에 대한 변수 $\rho^{CP}(i)$와, 상기 복호 키 $sk_{(SKP,\ \Gamma CP)}$에 포함되는 속성 집합 Γ^{CP}에 근거하여, i=1, …, L^{CP}의 각 정수 i 중, 변수 $\rho^{CP}(i)$가 긍정형의 조 $(t, v^{\rightarrow CP}_i)$이고, 또한, 그 조의 $v^{\rightarrow CP}_i$와, 그 조의 식별 정보 t가 나타내는 Γ^{CP}에 포함되는 $x^{\rightarrow CP}_t$의 내적이 0이 되는 i와, 변수 $\rho^{CP}(i)$가 부정형의 조 $\neg(t, v^{\rightarrow CP}_i)$이고, 또한, 그 조의 $v^{\rightarrow CP}_i$와, 그 조의 식별 정보 t가 나타내는 Γ^{CP}에 포함되는 $x^{\rightarrow CP}_t$의 내적이 0이 되지 않는 i의 집합 I^{CP}를 특정함과 아울러, 특정한 집합 I^{CP}에 포함되는 i에 대하여, $\alpha_i^{CP}M_i^{CP}$를 합계한 경우에 상기 $h^{\rightarrow CP}$가 되는 보완 계수 α_i^{CP}를 계산하는 CP 보완 계수 계산부와,

상기 암호화 데이터 $ct_{(\Gamma KP,\ SCP)}$에 포함되는 요소 c_0과 요소 c_t^{KP}와 요소 c_i^{CP}와, 상기 복호 키 $sk_{(SKP,\ \Gamma CP)}$에 포함되는 요소 k^{*}_0과 요소 k^{*KP}_i와 요소 k^{*CP}_t에 대하여, 상기 KP 보완 계수 계산부가 특정한 집합 I^{KP}와, 상기 KP 보완 계수 계산부가 계산한 보완 계수 α_i^{KP}와, 상기 CP 보완 계수 계산부가 특정한 집합 I^{CP}와, 상기 CP 보완 계수 계산부가 계산한 보완 계수 α_i^{CP}에 근거하여, 수학식 10에 나타내는 페어링 연산을 행하여 값 K를 계산하는 페어링 연산부

를 구비하는 것을 특징으로 하는 복호 장치.

[수학식 10]

$$K := e(c_0, k_0^*) \cdot \prod_{i \in I^{KP} \wedge \rho^{KP}(i)=(t,\vec{v}_i^{KP})} e(c_t^{KP}, k_i^{*KP})^{\alpha_i^{KP}} \cdot \prod_{i \in I^{KP} \wedge \rho^{KP}(i)=\neg(t,\vec{v}_i^{KP})} e(c_t^{KP}, k_i^{*KP})^{\alpha_i^{KP}/(\vec{v}_i^{KP} \cdot \vec{x}_t^{KP})} \cdot \prod_{i \in I^{CP} \wedge \rho^{CP}(i)=(t,\vec{v}_i^{CP})} e(c_t^{CP}, k_i^{*CP})^{\alpha_i^{CP}} \cdot \prod_{i \in I^{CP} \wedge \rho^{CP}(i)=\neg(t,\vec{v}_i^{CP})} e(c_t^{CP}, k_i^{*CP})^{\alpha_i^{CP}/(\vec{v}_i^{CP} \cdot \vec{x}_t^{CP})}$$

청구항 7

기저 B_0 및 기저 B_0^*와, t=1, …, d^{KP}(d^{KP}는 1 이상의 정수)의 각 정수 t에 대한 기저 B_t^{KP} 및 기저 B_t^{*KP}와, t=1, …, d^{CP}(d^{CP}는 1 이상의 정수)의 각 정수 t에 대한 기저 B_t^{CP} 및 기저 B_t^{*CP}를 이용한 암호 처리 방법으로서,

키 생성 장치가, i=1, …, L^{KP}(L^{KP}는 1 이상의 정수)의 각 정수 i에 대한 변수 $\rho^{KP}(i)$로서, 식별 정보 t(t=1, …, d^{KP}의 어느 하나의 정수)와, 속성 벡터 $\vec{v}_i^{KP} := (v_{i,i'}^{KP})$(i'=1, …, n_t^{KP}, n_t^{KP}는 1 이상의 정수)의 긍정형의 조 $(t, \vec{v}_i^{KP})$ 또는 부정형의 조 $\neg(t, \vec{v}_i^{KP})$의 어느 하나인 변수 $\rho^{KP}(i)$와, L^{KP}행 r^{KP}열(r^{KP}는 1 이상의 정수)의 소정의 행렬 M^{KP}를 입력하는 제 1 KP 정보 입력 공정과,

상기 키 생성 장치가, t=1, …, d^{CP}의 적어도 1개 이상의 정수 t에 대하여, 식별 정보 t와, 속성 벡터 $\vec{x}_t^{CP} := (x_{t,i'}^{CP})$(i'=1, …, n_t^{CP}, n_t^{CP}는 1 이상의 정수)를 갖는 속성 집합 Γ^{CP}를 입력하는 제 1 CP 정보 입력 공정과,

상기 키 생성 장치가, 기저 B_0^*의 기저 벡터 $b_{0,p}^*$(p는 소정의 값)의 계수로서 값 $-s_0^{KP}$($s_0^{KP} := \vec{h}^{KP} \cdot (\vec{f}^{KP})^T$, $\vec{h}^{KP}$ 및 $\vec{f}^{KP}$는 r^{KP}개의 요소를 갖는 벡터)를 설정하고, 기저 벡터 $b_{0,p'}^*$(p'는 상기 p와는 다른 소정의 값)의 계수로서 난수 δ^{CP}를 설정하고, 기저 벡터 $b_{0,q}^*$(q는 상기 p 및 상기 p'와는 다른 소정의 값)의 계수로서 소정의 값 κ를 설정하여 요소 k_0^*을 생성하는 주 복호 키 생성 공정과,

상기 키 생성 장치가, 상기 $\vec{f}^{KP}$와, 상기 제 1 KP 정보 입력 공정에서 입력한 행렬 M^{KP}에 근거하여 생성되는 열벡터 $(\vec{s}^{KP})^T := (s_1^{KP}, \cdots, s_i^{KP})^T := M^{KP} \cdot (\vec{f}^{KP})^T$(i=$L^{KP}$)와, 난수 Θ_i^{KP}(i=1, …, L^{KP})에 근거하여, i=1, …, L^{KP}의 각 정수 i에 대한 요소 k_i^{*KP}를 생성하는 KP 복호 키 생성 공정으로서, i=1, …, L^{KP}의 각 정수 i에 대하여, 변수 $\rho^{KP}(i)$가 긍정형의 조 $(t, \vec{v}_i^{KP})$인 경우에는, 그 조의 식별 정보 t가 나타내는 기저 B_t^{*KP}의 기저 벡터 $b_{t,1}^{*KP}$의 계수로서 $s_i^{KP} + \Theta_i^{KP} v_{i,1}^{KP}$를 설정함과 아울러, 상기 식별 정보 t와 i'=2, …, n_t^{KP}의 각 정수 i'가 나타내는 기저 벡터 $b_{t,i'}^{*KP}$의 계수로서 $\Theta_i^{KP} v_{i,i'}^{KP}$를 설정하여 요소 k_i^{*KP}를 생성하고, 변수 $\rho^{KP}(i)$가 부정형의 조 $\neg(t, \vec{v}_i^{KP})$인 경우에는, 그 조의 식별 정보 t와 i'=1, …, n_t^{KP}의 각 정수 i'가 나타내는 기저 벡터 $b_{t,i'}^{*KP}$의 계수로서 $s_i^{KP} v_{i,i'}^{KP}$를 설정하여 요소 k_i^{*KP}를 생성하는 KP 복호 키 생성 공정과,

상기 키 생성 장치가, 상기 제 1 CP 정보 입력 공정에서 입력한 속성 집합 Γ^{CP}에 포함되는 각 식별 정보 t에 대한 요소 k_t^{*CP}를 생성하는 CP 복호 키 생성 공정으로서, 기저 B_t^{*CP}의 기저 벡터 $b_{t,i'}^{*CP}$(i'=1, …, n_t^{CP})의 계수로

서 상기 난수 δ^{CP}배 한 $x_{t,i'}{}^{CP}$를 설정하여 요소 $k^{*}_{t}{}^{CP}$를 생성하는 CP 복호 키 생성 공정과,

암호화 장치가, t=1, …, d^{KP}의 적어도 1개 이상의 정수 t에 대하여, 식별 정보 t와, 속성 벡터 $\vec{x}_{t}{}^{KP}:=(x_{t,i'}{}^{KP})(i'=1, \cdots, n_t{}^{KP})$를 갖는 속성 집합 Γ^{KP}를 입력하는 제 2 KP 정보 입력 공정과,

상기 암호화 장치가, i=1, …, L^{CP}(L^{CP}는1 이상의 정수)의 각 정수 i에 대한 변수 $\rho^{CP}(i)$로서, 식별 정보 t(t=1, …, d^{CP}의 어느 하나의 정수)와, 속성 벡터 $\vec{v}_{i}{}^{CP}:=(v_{i,i'}{}^{CP})(i'=1, \cdots, n_t{}^{CP})$의 긍정형의 조 (t, $\vec{v}_{i}{}^{CP}$) 또는 부정형의 조 ¬(t, $\vec{v}_{i}{}^{CP}$)의 어느 하나인 변수 $\rho^{CP}(i)$와, L^{CP}행 r^{CP}열(r^{CP}는 1 이상의 정수)의 소정의 행렬 M^{CP}를 입력하는 제 2 CP 정보 입력 공정과,

상기 암호화 장치가, 기저 B_0의 기저 벡터 $b_{0,p}$의 계수로서 난수 ω^{KP}를 설정하고, 기저 벡터 $b_{0,p'}$의 계수로서 값 $-s_0{}^{CP}$($s_0{}^{CP}:=\vec{h}^{CP}\cdot(\vec{f}^{CP})^{T}$, $\vec{h}^{CP}$ 및 $\vec{f}^{CP}$는 r^{CP}개의 요소를 갖는 벡터)를 설정하고, 기저 벡터 $b_{0,q}$의 계수로서 난수 ζ를 설정하여 요소 c_0을 생성하는 주 암호화 데이터 생성 공정과,

상기 암호화 장치가, 상기 제 2 KP 정보 입력 공정에서 입력한 속성 집합 Γ^{KP}에 포함되는 각 식별 정보 t에 대한 요소 $c_t{}^{KP}$를 생성하는 KP 암호화 데이터 생성 공정으로서, 기저 $B_t{}^{KP}$의 기저 벡터 $b_{t,i'}{}^{KP}$(i'=1, …, n_t)의 계수로서 상기 난수 ω^{KP}배 한 $x_{t,i'}{}^{KP}$를 설정하여 요소 $c_t{}^{KP}$를 생성하는 KP 암호화 데이터 생성 공정과,

상기 암호화 장치가, 상기 $\vec{f}^{CP}$와, 상기 제 2 CP 정보 입력 공정에서 입력한 행렬 M^{CP}에 근거하여 생성되는 열 벡터 $(\vec{s}^{CP})^{T}:=(s_1{}^{CP}, \cdots, s_i{}^{CP})^{T}:=M^{CP}\cdot(\vec{f}^{CP})^{T}(i=L^{CP})$와, 난수 $\Theta_i{}^{CP}$(i=1, …, L^{CP})에 근거하여, i=1, …, L^{CP}의 각 정수 i에 대한 요소 $c_i{}^{CP}$를 생성하는 CP 암호화 데이터 생성 공정으로서, i=1, …, L^{CP}의 각 정수 i에 대하여, 변수 $\rho^{CP}(i)$가 긍정형의 조 (t, $\vec{v}_{i}{}^{CP}$)인 경우에는, 그 조의 식별 정보 t가 나타내는 기저 $B_t{}^{CP}$의 기저 벡터 $b_{t,1}{}^{CP}$의 계수로서 $s_i{}^{CP}+\Theta_i{}^{CP}v_{i,1}{}^{CP}$를 설정함과 아울러, 상기 식별 정보 t와 i'=2, …, $n_t{}^{CP}$의 각 정수 i'가 나타내는 기저 벡터 $b_{t,i'}{}^{CP}$의 계수로서 $\Theta_i{}^{CP}v_{i,i'}{}^{CP}$를 설정하여 요소 $c_i{}^{CP}$를 생성하고, 변수 $\rho^{CP}(i)$가 부정형의 조 ¬(t, $\vec{v}_{i}{}^{CP}$)인 경우에는, 그 조의 식별 정보 t와 i'=1, …, $n_t{}^{CP}$의 각 정수 i'가 나타내는 기저 벡터 $b_{t,i'}{}^{CP}$의 계수로서 $s_i{}^{CP}v_{i,i'}{}^{CP}$를 설정하여 요소 $c_i{}^{CP}$를 생성하는 CP 암호화 데이터 생성 공정과,

복호 장치가, 상기 주 암호화 데이터 생성 공정에서 생성한 요소 c_0과, 상기 KP 암호화 데이터 생성 공정에서 생성한 요소 $c_t{}^{KP}$와, 상기 CP 암호화 데이터 생성 공정에서 생성한 요소 $c_i{}^{CP}$와, 상기 속성 집합 Γ^{KP}와, 상기 변수 $\rho^{CP}(i)$를 포함하는 암호화 데이터 $ct_{(\Gamma KP,\ SCP)}$를 취득하는 데이터 취득 공정과,

상기 복호 장치가, 상기 주 복호 키 생성 공정에서 생성한 요소 k^{*}_{0}과, 상기 KP 복호 키 생성 공정에서 생성한 요소 $k^{*}_{i}{}^{KP}$와, 상기 CP 복호 키 생성 공정에서 생성한 요소 $k^{*}_{t}{}^{CP}$와, 상기 변수 $\rho^{KP}(i)$와, 상기 속성 집합 Γ^{CP}를 포함하는 복호 키 $sk_{(SKP,\ \Gamma CP)}$를 취득하는 복호 키 취득 공정과,

상기 복호 장치가, 상기 데이터 취득 공정에서 취득한 암호화 데이터 $ct_{(\Gamma KP,\ SCP)}$에 포함되는 속성 집합 Γ^{KP}와, 상기 복호 키 취득 공정에서 취득한 복호 키 $sk_{(SKP,\ \Gamma CP)}$에 포함되는 변수 $\rho^{KP}(i)$에 근거하여, i=1, …, L^{KP}의 각 정수 i 중, 변수 $\rho^{KP}(i)$가 긍정형의 조 (t, $\vec{v}_{i}{}^{KP}$)이고, 또한, 그 조의 $\vec{v}_{i}{}^{KP}$와, 그 조의 식별 정보 t가 나타내는 Γ^{KP}에 포함되는 $\vec{x}_{t}{}^{KP}$의 내적이 0이 되는 i와, 변수 $\rho^{KP}(i)$가 부정형의 조 ¬(t, $\vec{v}_{i}{}^{KP}$)이고, 또한, 그 조의

$v_i^{\rightarrow KP}$와, 그 조의 식별 정보 t가 나타내는 Γ^{KP}에 포함되는 $x_t^{\rightarrow KP}$의 내적이 0이 되지 않는 i의 집합 I^{KP}를 특정함과 아울러, 특정한 집합 I^{KP}에 포함되는 i에 대하여, $\alpha_i^{KP}M_i^{KP}$를 합계한 경우에 상기 $h^{\rightarrow KP}$가 되는 보완 계수 α_i^{KP}를 계산하는 KP 보완 계수 계산 공정과,

상기 복호 장치가, 상기 암호화 데이터 $ct_{(\Gamma KP,\ SCP)}$에 포함되는 i=1, …, L^{CP}의 각 정수 i에 대한 변수 $\rho^{CP}(i)$와, 상기 복호 키 $sk_{(SKP,\ \Gamma CP)}$에 포함되는 속성 집합 Γ^{CP}에 근거하여, i=1, …, L^{CP}의 각 정수 i 중, 변수 $\rho^{CP}(i)$가 긍정형의 조 $(t, v_i^{\rightarrow CP})$이고, 또한, 그 조의 $v_i^{\rightarrow CP}$와, 그 조의 식별 정보 t가 나타내는 Γ^{CP}에 포함되는 $x_t^{\rightarrow CP}$의 내적이 0이 되는 i와, 변수 $\rho^{CP}(i)$가 부정형의 조 $\neg(t, v_i^{\rightarrow CP})$이고, 또한, 그 조의 $v_i^{\rightarrow CP}$와, 그 조의 식별 정보 t가 나타내는 Γ^{CP}에 포함되는 $x_t^{\rightarrow CP}$의 내적이 0이 되지 않는 i의 집합 I^{CP}를 특정함과 아울러, 특정한 집합 I^{CP}에 포함되는 i에 대하여, $\alpha_i^{CP}M_i^{CP}$를 합계한 경우에 상기 $h^{\rightarrow CP}$가 되는 보완 계수 α_i^{CP}를 계산하는 CP 보완 계수 계산 공정과,

상기 복호 장치가, 상기 암호화 데이터 $ct_{(\Gamma KP,\ SCP)}$에 포함되는 요소 c_0과 요소 c_t^{KP}와 요소 c_i^{CP}와, 상기 복호 키 $sk_{(SKP,\ \Gamma CP)}$에 포함되는 요소 k_0^*과 요소 k_i^{*KP}와 요소 k_t^{*CP}에 대하여, 상기 KP 보완 계수 계산 공정에서 특정한 집합 I^{KP}와, 상기 KP 보완 계수 계산 공정에서 계산한 보완 계수 α_i^{KP}와, 상기 CP 보완 계수 계산 공정에서 특정한 집합 I^{CP}와, 상기 CP 보완 계수 계산 공정에서 계산한 보완 계수 α_i^{CP}에 근거하여, 수학식 11에 나타내는 페어링 연산을 행하여 값 K를 계산하는 페어링 연산 공정

을 구비하는 것을 특징으로 하는 암호 처리 방법.

[수학식 11]

$$K := e(c_0, k_0^*) \cdot \prod_{i \in I^{KP} \wedge \rho^{KP}(i)=(t,\vec{v}_i^{KP})} e(c_t^{KP}, k_i^{*KP})^{\alpha_i^{KP}} \cdot \prod_{i \in I^{KP} \wedge \rho^{KP}(i)=\neg(t,\vec{v}_i^{KP})} e(c_t^{KP}, k_i^{*KP})^{\alpha_i^{KP}/(\vec{v}_i^{KP}\cdot\vec{x}_t^{KP})} \cdot \prod_{i \in I^{CP} \wedge \rho^{CP}(i)=(t,\vec{v}_i^{CP})} e(c_t^{CP}, k_i^{*CP})^{\alpha_i^{CP}} \cdot \prod_{i \in I^{CP} \wedge \rho^{CP}(i)=\neg(t,\vec{v}_i^{CP})} e(c_t^{CP}, k_i^{*CP})^{\alpha_i^{CP}/(\vec{v}_i^{CP}\cdot\vec{x}_t^{CP})}$$

청구항 8

키 생성 프로그램과 암호화 프로그램과 복호 프로그램을 구비하고, 기저 B_0 및 기저 B_0^*와, t=1, …, d^{KP}(d^{KP}는 1 이상의 정수)의 각 정수 t에 대한 기저 B_t^{KP} 및 기저 B_t^{*KP}와, t=1, …, d^{CP}(d^{CP}는 1 이상의 정수)의 각 정수 t에 대한 기저 B_t^{CP} 및 기저 B_t^{*CP}를 이용하여 암호 처리를 실행하는 암호 처리 프로그램을 기록한 컴퓨터 판독 가능한 기록 매체로서,

상기 키 생성 프로그램은,

i=1, …, L^{KP}(L^{KP}는 1 이상의 정수)의 각 정수 i에 대한 변수 $\rho^{KP}(i)$로서, 식별 정보 t(t=1, …, d^{KP}의 어느 하나의 정수)와, 속성 벡터 $v_i^{\rightarrow KP}:=(v_{i,i'}^{KP})$(i'=1, …, n_t^{KP}, n_t^{KP}는 1 이상의 정수)의 긍정형의 조 $(t, v_i^{\rightarrow KP})$ 또는 부정형의 조 $\neg(t, v_i^{\rightarrow KP})$의 어느 하나인 변수 $\rho^{KP}(i)$와, L^{KP}행 r^{KP}열(r^{KP}는 1 이상의 정수)의 소정의 행렬 M^{KP}를

입력하는 제 1 KP 정보 입력 처리와,

t=1, …, d^{CP}의 적어도 1개 이상의 정수 t에 대하여, 식별 정보 t와, 속성 벡터 $\vec{x}_t^{CP}:=(x_{t,i'}^{CP})(i'=1, \cdots, n_t^{CP}$, n_t^{CP}는 1 이상의 정수)를 갖는 속성 집합 Γ^{CP}를 입력하는 제 1 CP 정보 입력 처리와,

기저 B^*_0의 기저 벡터 $b^*_{0,p}$(p는 소정의 값)의 계수로서 값 $-s_0^{KP}(s_0^{KP}:=\vec{h}^{KP}\cdot(\vec{f}^{KP})^T$, $\vec{h}^{KP}$ 및 $\vec{f}^{KP}$는 r^{KP}개의 요소를 갖는 벡터)를 설정하고, 기저 벡터 $b^*_{0,p'}$(p'는 상기 p와는 다른 소정의 값)의 계수로서 난수 δ^{CP}를 설정하고, 기저 벡터 $b^*_{0,q}$(q는 상기 p 및 상기 p'와는 다른 소정의 값)의 계수로서 소정의 값 κ를 설정하여 요소 k^*_0을 생성하는 주 복호 키 생성 처리와,

상기 $\vec{f}^{KP}$와, 상기 제 1 KP 정보 입력 처리에서 입력한 행렬 M^{KP}에 근거하여 생성되는 열 벡터 $(\vec{s}^{KP})^T:=(s_1^{KP}$, …, $s_i^{KP})^T:=M^{KP}\cdot(\vec{f}^{KP})^T(i=L^{KP})$와, 난수 $\Theta_i^{KP}(i=1, \cdots, L^{KP})$에 근거하여, i=1, …, L^{KP}의 각 정수 i에 대한 요소 $k^*_i{}^{KP}$를 생성하는 KP 복호 키 생성 처리로서, i=1, …, L^{KP}의 각 정수 i에 대하여, 변수 $\rho^{KP}(i)$가 긍정형의 조 $(t, \vec{v}_i^{KP})$인 경우에는, 그 조의 식별 정보 t가 나타내는 기저 $B^*_t{}^{KP}$의 기저 벡터 $b^*_{t,1}{}^{KP}$의 계수로서 $s_i^{KP}+\Theta_i^{KP}v_{i,1}{}^{KP}$를 설정함과 아울러, 상기 식별 정보 t와 i'=2, …, n_t^{KP}의 각 정수 i'가 나타내는 기저 벡터 $b^*_{t,i'}{}^{KP}$의 계수로서 $\Theta_i^{KP}v_{i,i'}{}^{KP}$를 설정하여 요소 $k^*_i{}^{KP}$를 생성하고, 변수 $\rho^{KP}(i)$가 부정형의 조 $\neg(t, \vec{v}_i^{KP})$인 경우에는, 그 조의 식별 정보 t와 i'=1, …, n_t^{KP}의 각 정수 i'가 나타내는 기저 벡터 $b^*_{t,i'}{}^{KP}$의 계수로서 $s_i^{KP}v_{i,i'}{}^{KP}$를 설정하여 요소 $k^*_i{}^{KP}$를 생성하는 KP 복호 키 생성 처리와,

상기 제 1 CP 정보 입력 처리에서 입력한 속성 집합 Γ^{CP}에 포함되는 각 식별 정보 t에 대한 요소 $k^*_t{}^{CP}$를 생성하는 CP 복호 키 생성 처리로서, 기저 $B^*_t{}^{CP}$의 기저 벡터 $b^*_{t,i'}{}^{CP}(i'=1, \cdots, n_t^{CP})$의 계수로서 상기 난수 δ^{CP}배 한 $x_{t,i'}{}^{CP}$를 설정하여 요소 $k^*_t{}^{CP}$를 생성하는 CP 복호 키 생성 처리

를 컴퓨터에 실행시키고,

상기 암호화 프로그램은,

t=1, …, d^{KP}의 적어도 1개 이상의 정수 t에 대하여, 식별 정보 t와, 속성 벡터 $\vec{x}_t^{KP}:=(x_{t,i'}^{KP})(i'=1, \cdots, n_t^{KP})$를 갖는 속성 집합 Γ^{KP}를 입력하는 제 2 KP 정보 입력 처리와,

i=1, …, L^{CP}(L^{CP}는 1 이상의 정수)의 각 정수 i에 대한 변수 $\rho^{CP}(i)$로서, 식별 정보 t(t=1, …, d^{CP}의 어느 하나의 정수)와, 속성 벡터 $\vec{v}_i^{CP}:=(v_{i,i'}^{CP})(i'=1, \cdots, n_t^{CP})$의 긍정형의 조 $(t, \vec{v}_i^{CP})$ 또는 부정형의 조 $\neg(t, \vec{v}_i^{CP})$의 어느 하나인 변수 $\rho^{CP}(i)$와, L^{CP}행 r^{CP}열(r^{CP}는 1 이상의 정수)의 소정의 행렬 M^{CP}를 입력하는 제 2 CP 정보 입력 처리와,

기저 B_0의 기저 벡터 $b_{0,p}$의 계수로서 난수 ω^{KP}를 설정하고, 기저 벡터 $b_{0,p'}$의 계수로서 값 $-s_0^{CP}(s_0^{CP}:=\vec{h}^{CP}\cdot(\vec{f}^{CP})^T$, $\vec{h}^{CP}$ 및 $\vec{f}^{CP}$는 r^{CP}개의 요소를 갖는 벡터)를 설정하고, 기저 벡터 $b_{0,q}$의 계수로서 난수 ζ를 설정하여 요소 c_0을 생성하는 주 암호화 데이터 생성 처리와,

상기 제 2 KP 정보 입력 처리에서 입력한 속성 집합 Γ^{KP}에 포함되는 각 식별 정보 t에 대한 요소 c_t^{KP}를 생성하는 KP 암호화 데이터 생성 처리로서, 기저 B_t^{KP}의 기저 벡터 $b_{t,i'}{}^{KP}(i'=1, \cdots, n_t)$의 계수로서 상기 난수 ω^{KP}배

한 $x_{t,i'}^{KP}$를 설정하여 요소 c_t^{KP}를 생성하는 KP 암호화 데이터 생성 처리와,

상기 $f^{\rightarrow CP}$와, 상기 제 2 CP 정보 입력 처리에서 입력한 행렬 M^{CP}에 근거하여 생성되는 열 벡터 $(s^{\rightarrow CP})^T:=(s_1^{CP}, \cdots, s_i^{CP})^T:=M^{CP}\cdot(f^{\rightarrow CP})^T(i=L^{CP})$와, 난수 $\Theta_i^{CP}(i=1, \cdots, L^{CP})$에 근거하여, i=1, …, L^{CP}의 각 정수 i에 대한 요소 c_i^{CP}를 생성하는 CP 암호화 데이터 생성 처리로서, i=1, …, L^{CP}의 각 정수 i에 대하여, 변수 $\rho^{CP}(i)$가 긍정형의 조 $(t, v_i^{\rightarrow CP})$인 경우에는, 그 조의 식별 정보 t가 나타내는 기저 B_t^{CP}의 기저 벡터 $b_{t,1}^{CP}$의 계수로서 $s_i^{CP}+\Theta_i^{CP}v_{i,1}^{CP}$를 설정함과 아울러, 상기 식별 정보 t와 i'=2, …, n_t^{CP}의 각 정수 i'가 나타내는 기저 벡터 $b_{t,i'}^{CP}$의 계수로서 $\Theta_i^{CP}v_{i,i'}^{CP}$를 설정하여 요소 c_i^{CP}를 생성하고, 변수 $\rho^{CP}(i)$가 부정형의 조 $\neg(t, v_i^{\rightarrow CP})$인 경우에는, 그 조의 식별 정보 t와 i'=1, …, n_t^{CP}의 각 정수 i'가 나타내는 기저 벡터 $b_{t,i'}^{CP}$의 계수로서 $s_i^{CP}v_{i,i'}^{CP}$를 설정하여 요소 c_i^{CP}를 생성하는 CP 암호화 데이터 생성 처리

를 컴퓨터에 실행시키고,

상기 복호 프로그램은,

상기 주 암호화 데이터 생성 처리에서 생성한 요소 c_0과, 상기 KP 암호화 데이터 생성 처리에서 생성한 요소 c_t^{KP}와, 상기 CP 암호화 데이터 생성 처리에서 생성한 요소 c_i^{CP}와, 상기 속성 집합 Γ^{KP}와, 상기 변수 $\rho^{CP}(i)$를 포함하는 암호화 데이터 $ct_{(\Gamma KP,\ SCP)}$를 취득하는 데이터 취득 처리와,

상기 주 복호 키 생성 처리에서 생성한 요소 k_0^*과, 상기 KP 복호 키 생성 처리에서 생성한 요소 k_i^{*KP}와, 상기 CP 복호 키 생성 처리에서 생성한 요소 k_t^{*CP}와, 상기 변수 $\rho^{KP}(i)$와, 상기 속성 집합 Γ^{CP}를 포함하는 복호 키 $sk_{(SKP,\ \Gamma CP)}$를 취득하는 복호 키 취득 처리와,

상기 데이터 취득 처리에서 취득한 암호화 데이터 $ct_{(\Gamma KP,\ SCP)}$에 포함되는 속성 집합 Γ^{KP}와, 상기 복호 키 취득 처리에서 취득한 복호 키 $sk_{(SKP,\ \Gamma CP)}$에 포함되는 변수 $\rho^{KP}(i)$에 근거하여, i=1, …, L^{KP}의 각 정수 i 중, 변수 $\rho^{KP}(i)$가 긍정형의 조 $(t, v_i^{\rightarrow KP})$이고, 또한, 그 조의 $v_i^{\rightarrow KP}$와, 그 조의 식별 정보 t가 나타내는 Γ^{KP}에 포함되는 $x_t^{\rightarrow KP}$의 내적이 0이 되는 i와, 변수 $\rho^{KP}(i)$가 부정형의 조 $\neg(t, v_i^{\rightarrow KP})$이고, 또한, 그 조의 $v_i^{\rightarrow KP}$와, 그 조의 식별 정보 t가 나타내는 Γ^{KP}에 포함되는 $x_t^{\rightarrow KP}$의 내적이 0이 되지 않는 i의 집합 I^{KP}를 특정함과 아울러, 특정한 집합 I^{KP}에 포함되는 i에 대하여, $\alpha_i^{KP}M_i^{KP}$를 합계한 경우에 상기 $h^{\rightarrow KP}$가 되는 보완 계수 α_i^{KP}를 계산하는 KP 보완 계수 계산 처리와,

상기 암호화 데이터 $ct_{(\Gamma KP,\ SCP)}$에 포함되는 i=1, …, L^{CP}의 각 정수 i에 대한 변수 $\rho^{CP}(i)$와, 상기 복호 키 $sk_{(SKP,\ \Gamma CP)}$에 포함되는 속성 집합 Γ^{CP}에 근거하여, i=1, …, L^{CP}의 각 정수 i 중, 변수 $\rho^{CP}(i)$가 긍정형의 조 $(t, v_i^{\rightarrow CP})$이고, 또한, 그 조의 $v_i^{\rightarrow CP}$와, 그 조의 식별 정보 t가 나타내는 Γ^{CP}에 포함되는 $x_t^{\rightarrow CP}$의 내적이 0이 되는 i와, 변수 $\rho^{CP}(i)$가 부정형의 조 $\neg(t, v_i^{\rightarrow CP})$이고, 또한, 그 조의 $v_i^{\rightarrow CP}$와, 그 조의 식별 정보 t가 나타내는 Γ^{CP}에 포함되는 $x_t^{\rightarrow CP}$의 내적이 0이 되지 않는 i의 집합 I^{CP}를 특정함과 아울러, 특정한 집합 I^{CP}에 포함되는 i에 대하여, $\alpha_i^{CP}M_i^{CP}$를 합계한 경우에 상기 $h^{\rightarrow CP}$가 되는 보완 계수 α_i^{CP}를 계산하는 CP 보완 계수 계산 처리와,

상기 암호화 데이터 $ct_{(\Gamma KP,\ SCP)}$에 포함되는 요소 c_0과 요소 c_t^{KP}와 요소 c_i^{CP}와, 상기 복호 키 $sk_{(SKP,\ \Gamma CP)}$에 포함되는 요소 k_0^*과 요소 k_i^{*KP}와 요소 k_t^{*CP}에 대하여, 상기 KP 보완 계수 계산 처리에서 특정한 집합 I^{KP}와, 상기 KP 보완 계수 계산 처리에서 계산한 보완 계수 α_i^{KP}와, 상기 CP 보완 계수 계산 처리에서 특정한 집합 I^{CP}와, 상기 CP 보완 계수 계산 처리에서 계산한 보완 계수 α_i^{CP}에 근거하여, 수학식 12에 나타내는 페어링 연산을 행하여 값 K를 계산하는 페어링 연산 처리

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

[수학식 12]

$$K := e(c_0, k_0^*) \cdot \prod_{i \in I^{KP} \wedge \rho^{KP}(i)=(t,\vec{v}_i^{KP})} e(c_t^{KP}, k_i^{*KP})^{\alpha_i^{KP}} \cdot \prod_{i \in I^{KP} \wedge \rho^{KP}(i)=\neg(t,\vec{v}_i^{KP})} e(c_t^{KP}, k_i^{*KP})^{\alpha_i^{KP}/(\vec{v}_i^{KP} \cdot \vec{x}_t^{KP})} \cdot \prod_{i \in I^{CP} \wedge \rho^{CP}(i)=(t,\vec{v}_i^{CP})} e(c_t^{CP}, k_i^{*CP})^{\alpha_i^{CP}} \cdot \prod_{i \in I^{CP} \wedge \rho^{CP}(i)=\neg(t,\vec{v}_i^{CP})} e(c_t^{CP}, k_i^{*CP})^{\alpha_i^{CP}/(\vec{v}_i^{CP} \cdot \vec{x}_t^{CP})}$$

명 세 서

기 술 분 야

[0001] 본 발명은, 함수형 암호(Functional Encryption, FE) 방식에 관한 것이다.

배 경 기 술

[0002] 비특허 문헌 3-6, 10, 12, 13, 15, 18에는, 함수형 암호 방식의 하나의 클래스인 ID 베이스 암호(Identity-Based Encryption, IBE) 방식에 대한 기재가 있다.

[0003] (선행 기술 문헌)

[0004] (비특허 문헌)

[0005] (비특허 문헌 1) Beimel, A., Secure schemes for secret sharing and key distribution. PhD Thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996

[0006] (비특허 문헌 2) Bethencourt, J., Sahai, A., Waters, B. : Ciphertext policy attribute-based encryption. In : 2007 IEEE Symposium on Security and Privacy, pp. 321·34. IEEE Press (2007)

[0007] (비특허 문헌 3) 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. 223·38. Springer Heidelberg (2004)

[0008] (비특허 문헌 4) Boneh, D., Boyen, X. : Secure identity based encryption without random oracles. In : Franklin, M. K. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 443·59. Springer Heidelberg (2004)

[0009] (비특허 문헌 5) Boneh, D., Boyen, X., Goh, E. : Hierarchical identity based encryption with constant size ciphertext. In : Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 440·56. Springer Heidelberg (2005)

[0010] (비특허 문헌 6) Boneh, D., Franklin, M. : Identity-based encryption from the Weil pairing. In : Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213·29. Springer Heidelberg (2001)

[0011] (비특허 문헌 7) Boneh, D., Hamburg, M. : Generalized identity based and broadcast encryption scheme. In : Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 455·70. Springer Heidelberg (2008)

[0012] (비특허 문헌 8) Boneh, D., Katz, J., Improved efficiency for CCA-secure crypto systems built using identity based encryption. RSA-CT 2005, LNCS, Springer Verlag (2005)

[0013] (비특허 문헌 9) Boneh, D., Waters, B. : Conjunctive, subset, and range queries on encrypted data. In : Vadhan, S. P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 535·54. Springer Heidelberg (2007)

[0014] (비특허 문헌 10) Boyen, X., Waters, B. : Anonymous hierarchical identity-based encryption(without random oracles). In : Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 290·07. Springer Heidelberg (2006)

[0015] (비특허 문헌 11) Canetti, R., Halevi S., Katz J., Chosen-ciphertext security from identity-based encryption. EUROCRYPT 2004, LNCS, Springer-Verlag (2004)

[0016] (비특허 문헌 12) Cocks, C. : An identity based encryption scheme based on quadratic residues. In : Honary, B. (ed.) IMA Int. Conf. LNCS, vol. 2260, pp. 360·63. Springer Heidelberg (2001)

[0017] (비특허 문헌 13) Gentry, C. : Practical identity-based encryption without random oracles. In : Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 445·64. Springer Heidelberg (2006)

[0018] (비특허 문헌 14) Gentry, C., Halevi, S. : Hierarchical identity-based encryption with polynomially many levels. In : Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 437·56. Springer Heidelberg (2009)

[0019] (비특허 문헌 15) Gentry, C., Silverberg, A. : Hierarchical ID-based cryptography. In : Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 548·66. Springer Heidelberg (2002)

[0020] (비특허 문헌 16) 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. 89·8, ACM (2006)

[0021] (비특허 문헌 17) Groth, J., Sahai, A. : Efficient non-interactive proof systems for bilinear groups. In : Smart, N. P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 415·32. Springer Heidelberg (2008)

[0022] (비특허 문헌 18) Horwitz, J., Lynn, B. : Towards hierarchical identity-based encryption. In : Knudsen, L. R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 466·81. Springer Heidelberg (2002)

[0023] (비특허 문헌 19) 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. 146·62. Springer Heidelberg (2008)

[0024] (비특허 문헌 20) Lewko, A., Okamoto, T., Sahai, A., Takashima, K., Waters, B. : Fully secure functional encryption : Attribute-based encryption and (hierarchical) inner product encryption, In : Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 62-91. Springer, Heidelberg (2010)

[0025] (비특허 문헌 21) Lewko, A. B., Waters, B. : Fully secure HIBE with short ciphertexts. ePrint, IACR, http://eprint.iacr.org/2009/482

[0026] (비특허 문헌 22) 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. 57·4. Springer Heidelberg (2008)

[0027] (비특허 문헌 23) Okamoto, T., Takashima, K. : Hierarchical predicate encryption for Inner-Products, In : ASIACRYPT 2009, Springer Heidelberg (2009)

[0028] (비특허 문헌 24) Okamoto, T., Takashima, K. : Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption, In : CRYPTO 2010, LNCS vol. 6223, pp. 191-208. Springer Heidelberg (2010)

[0029] (비특허 문헌 25) Ostrovsky, R., Sahai, A., Waters, B. : Attribute-based encryption with non-monotonic access structures. In : ACM Conference on Computer and Communication Security 2007, pp. 195·03, ACM (2007)

[0030] (비특허 문헌 26) Pirretti, M., Traynor, P., McDaniel, P., Waters, B. : Secure attribute-based systems. In : ACM Conference on Computer and Communication Security 2006, pp. 99·12, ACM, (2006)

[0031] (비특허 문헌 27) Sahai, A., Waters, B. : Fuzzy identity-based encryption. In : Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457·73. Springer Heidelberg (2005)

[0032] (비특허 문헌 28) Shi, E., Waters, B. : Delegating capability in predicate encryption systems. In : Aceto, L., Damgard, I., Goldberg, L. A., Halldosson, M. M., Ingofsdotir, A., Walukiewicz, I. (eds.) ICALP (2) 2008. LNCS, vol. 5126, pp. 560·78. Springer Heidelberg (2008)

[0033] (비특허 문헌 29) Waters, B. : Efficient identity based encryption without random oracles. Eurocrypt 2005, LNCS No. 3152, pp. 443·59. Springer Verlag, 2005.

[0034] (비특허 문헌 30) Waters, B. : Ciphertext-policy attribute-based encryption : an expressive, efficient, and provably secure realization. ePrint, IACR, http://eprint.iacr.org/2008/290

[0035] (비특허 문헌 31) Waters, B. : Dual system encryption : Realizing fully secure IBE and HIBE under simple assumptions. In : Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 619·36. Springer Heidelberg (2009)

발명의 내용

해결하려는 과제

[0036] 본 발명은, 다기능의 암호 기능을 갖는 안전한 함수형 암호 방식을 제공하는 것을 목적으로 한다.

과제의 해결 수단

[0037] 본 발명에 따른 암호 처리 시스템은, 키 생성 장치와 암호화 장치와 복호 장치를 구비하고, 기저 B_0 및 기저 B_0^*와, t=1, …, d^{KP}(d^{KP}는 1 이상의 정수)의 각 정수 t에 대한 기저 B_t^{KP} 및 기저 $B^*{}_t^{KP}$와, t=1, …, d^{CP}(d^{CP}는 1 이상의 정수)의 각 정수 t에 대한 기저 B_t^{CP} 및 기저 $B^*{}_t^{CP}$를 이용하여 암호 처리를 실행하는 암호 처리 시스템이고, 상기 키 생성 장치는, i=1, …, L^{KP}(L^{KP}는 1 이상의 정수)의 각 정수 i에 대한 변수 $\rho^{KP}(i)$로서, 식별 정보 t(t=1, …, d^{KP}의 어느 하나의 정수)와, 속성 벡터 $\vec{v}_i^{KP}:=(v_{i,i'}{}^{KP})$(i'=1, …, n_t^{KP}, n_t^{KP}는 1 이상의 정수)의 긍정형의 조 $(t, \vec{v}_i^{KP})$ 또는 부정형의 조 $\neg(t, \vec{v}_i^{KP})$의 어느 하나인 변수 $\rho^{KP}(i)$와, L^{KP}행 r^{KP}열(r^{KP}는 1 이상의 정수)의 소정의 행렬 M^{KP}를 입력하는 제 1 KP 정보 입력부와, t=1, …, d^{CP}의 적어도 1개 이상의 정수 t에 대하여, 식별 정보 t와, 속성 벡터 $\vec{x}_t^{CP}:=(x_{t,i'}{}^{CP})$(i'=1, …, n_t^{CP}, n_t^{CP}는 1 이상의 정수)를 갖는 속성 집합 Γ^{CP}를 입력하는 제 1 CP 정보 입력부와, 기저 B^*_0의 기저 벡터 $b^*_{0,p}$(p는 소정의 값)의 계수로서 값 $-s_0^{KP}$($s_0^{KP}:=\vec{h}^{KP}\cdot(\vec{f}^{KP})^T$, $\vec{h}^{KP}$ 및 $\vec{f}^{KP}$는 r^{KP}개의 요소를 갖는 벡터)를 설정하고, 기저 벡터 $b^*_{0,p'}$(p'는 상기 p와는 다른 소정의 값)의 계수로서 난수 δ_C^P를 설정하고, 기저 벡터 $b^*_{0,q}$(q는 상기 p 및 상기 p'와는 다른 소정의 값)의 계수로서 소정의 값 κ를 설정하여 요소 k^*_0를 생성하는 주 복호 키 생성부와, 상기 $\vec{f}^{KP}$와, 상기 제 1 KP 정보 입력부가 입력한 행렬 M^{KP}에 근거하여 생성되는 열 벡터 $(\vec{s}^{KP})^T:=(s_1^{KP}, \cdots, s_i^{KP})^T:=M^{KP}\cdot(\vec{f}^{KP})^T$(i=$L^{KP}$)와, 난수 Θ_i^{KP}(i=1,

…, L^{KP})에 근거하여, i=1, …, L^{KP}의 각 정수 i에 대한 요소 k^{*KP}_i를 생성하는 KP 복호 키 생성부로서, i=1, …, L^{KP}의 각 정수 i에 대하여, 변수 $\rho^{KP}(i)$가 긍정형의 조 $(t, v^{\rightarrow KP}_i)$인 경우에는, 그 조의 식별 정보 t가 나타내는 기저 B^{*KP}_t의 기저 벡터 $b^{*KP}_{t,1}$의 계수로서 $s_i^{KP}+\Theta_i^{KP}v_{i,1}^{KP}$를 설정함과 아울러, 상기 식별 정보 t와 i'=2, …, n_t^{KP}의 각 정수 i'가 나타내는 기저 벡터 $b^{*KP}_{t,i'}$의 계수로서 $\Theta_i^{KP}v_{i,i'}^{KP}$를 설정하여 요소 k^{*KP}_i를 생성하고, 변수 $\rho^{KP}(i)$가 부정형의 조 $\neg(t, v^{\rightarrow KP}_i)$인 경우에는, 그 조의 식별 정보 t와 i'=1, …, n_t^{KP}의 각 정수 i'가 나타내는 기저 벡터 $b^{*KP}_{t,i'}$의 계수로서 $s_i^{KP}v_{i,i'}^{KP}$를 설정하여 요소 k^{*KP}_i를 생성하는 KP 복호 키 생성부와, 상기 제 1 CP 정보 입력부가 입력한 속성 집합 Γ^{CP}에 포함되는 각 식별 정보 t에 대한 요소 k^{*CP}_t를 생성하는 CP 복호 키 생성부로서, 기저 B^{*CP}_t의 기저 벡터 $b^{*CP}_{t,i'}$(i'=1, …, n_t^{CP})의 계수로서 상기 난수 δ^{CP}배 한 $x_{t,i'}^{CP}$를 설정하여 요소 k^{*CP}_t를 생성하는 CP 복호 키 생성부를 구비하고, 상기 암호화 장치는, t=1, …, d^{KP}의 적어도 1개 이상의 정수 t에 대하여, 식별 정보 t와, 속성 벡터 $\vec{x}^{KP}_t:=(x_{t,i'}^{KP})$(i'=1, …, n_t^{KP})를 갖는 속성 집합 Γ^{KP}를 입력하는 제 2 KP 정보 입력부와, i=1, …, L^{CP}(L^{CP}는 1 이상의 정수)의 각 정수 i에 대한 변수 $\rho^{CP}(i)$로서, 식별 정보 t(t=1, …, d^{CP}의 어느 하나의 정수)와, 속성 벡터 $\vec{v}^{CP}_i:=(v_{i,i'}^{CP})$(i'=1, …, n_t^{CP})의 긍정형의 조 $(t, v^{\rightarrow CP}_i)$ 또는 부정형의 조 $\neg(t, v^{\rightarrow CP}_i)$의 어느 하나인 변수 $\rho^{CP}(i)$와, L^{CP}행 r^{CP}열(r^{CP}는 1 이상의 정수)의 소정의 행렬 M^{CP}를 입력하는 제 2 CP 정보 입력부와, 기저 B_0의 기저 벡터 $b_{0,p}$의 계수로서 난수 ω^{KP}를 설정하고, 기저 벡터 $b_{0,p'}$의 계수로서 값 $-s_0^{CP}$($s_0^{CP}:=\vec{h}^{CP}\cdot(\vec{f}^{CP})^T$, $\vec{h}^{CP}$ 및 $\vec{f}^{CP}$는 r^{CP}개의 요소를 갖는 벡터)를 설정하고, 기저 벡터 $b_{0,q}$의 계수로서 난수 ζ를 설정하여 요소 c_0을 생성하는 주 암호화 데이터 생성부와, 상기 제 2 KP 정보 입력부가 입력한 속성 집합 Γ^{KP}에 포함되는 각 식별 정보 t에 대한 요소 c_t^{KP}를 생성하는 KP 암호화 데이터 생성부로서, 기저 B_t^{KP}의 기저 벡터 $b_{t,i'}^{KP}$(i'=1, …, n_t)의 계수로서 상기 난수 ω^{KP}배 한 $x_{t,i'}^{KP}$를 설정하여 요소 c_t^{KP}를 생성하는 KP 암호화 데이터 생성부와, 상기 $\vec{f}^{CP}$와, 상기 제 2 CP 정보 입력부가 입력한 행렬 M^{CP}에 근거하여 생성되는 열 벡터 $(\vec{s}^{CP})^T:=(s_1^{CP}, \cdots, s_i^{CP})^T:=M^{CP}\cdot(\vec{f}^{CP})^T$(i=$L^{CP}$)와, 난수 Θ_i^{CP}(i=1, …, L^{CP})에 근거하여, i=1, …, L^{CP}의 각 정수 i에 대한 요소 c_i^{CP}를 생성하는 CP 암호화 데이터 생성부로서, i=1, …, L^{CP}의 각 정수 i에 대하여, 변수 $\rho^{CP}(i)$가 긍정형의 조 $(t, v^{\rightarrow CP}_i)$인 경우에는, 그 조의 식별 정보 t가 나타내는 기저 B_t^{CP}의 기저 벡터 $b_{t,1}^{CP}$의 계수로서 $s_i^{CP}+\Theta_i^{CP}v_{i,1}^{CP}$를 설정함과 아울러, 상기 식별 정보 t와 i'=2, …, n_t^{CP}의 각 정수 i'가 나타내는 기저 벡터 $b_{t,i'}^{CP}$의 계수로서 $\Theta_i^{CP}v_{i,i'}^{CP}$를 설정하여 요소 c_i^{CP}를 생성하고, 변수 $\rho^{CP}(i)$가 부정형의 조 $\neg(t, v^{\rightarrow CP}_i)$인 경우에는, 그 조의 식별 정보 t와 i'=1, …, n_t^{CP}의 각 정수 i'가 나타내는 기저 벡터 $b_{t,i'}^{CP}$의 계수로서 $s_i^{CP}v_{i,i'}^{CP}$를 설정하여 요소 c_i^{CP}를 생성하는 CP 암호화 데이터 생성부를 구비하고, 상기 복호 장치는, 상기 주 암호화 데이터 생성부가 생성한 요소 c_0과, 상기 KP 암호화 데이터 생성부가 생성한 요소 c_t^{KP}와, 상기 CP 암호화 데이터 생성부가 생성한 요소 c_i^{CP}와, 상기 속성 집합 Γ^{KP}와, 상기 변수 $\rho^{CP}(i)$를 포함하는 암호화 데이터 $ct_{(\Gamma KP,\ SCP)}$를 취득하는 데이터 취득부와, 상기 주 복호 키 생성부가 생성한 요소 k^{*}_0과, 상기 KP 복호 키 생성부가 생성한 요소 k^{*KP}_i와, 상기 CP 복호 키 생성부가 생성한 요소 k^{*CP}_t와, 상기 변수 $\rho^{KP}(i)$와, 상기 속성 집합 Γ^{CP}를 포함하는 복호 키 $sk_{(SKP,\ \Gamma CP)}$를 취득하는 복호 키 취득부와, 상기 데이터 취득부가 취득한 암호화 데이터 $ct_{(\Gamma KP,\ SCP)}$에 포함되는 속성 집합 Γ^{KP}와, 상기 복호 키 취득부가 취득한 복호 키 $sk_{(SKP,\ \Gamma CP)}$에 포함되는 변수 $\rho^{KP}(i)$에 근거

하여, i=1, …, L^{KP}의 각 정수 i 중, 변수 $\rho^{KP}(i)$가 긍정형의 조 $(t, \vec{v}_i^{KP})$이고, 또한, 그 조의 $\vec{v}_i^{KP}$와, 그 조의 식별 정보 t가 나타내는 Γ^{KP}에 포함되는 $\vec{x}_t^{KP}$의 내적이 0이 되는 i와, 변수 $\rho^{KP}(i)$가 부정형의 조 $\neg(t, \vec{v}_i^{KP})$이고, 또한, 그 조의 $\vec{v}_i^{KP}$와, 그 조의 식별 정보 t가 나타내는 Γ^{KP}에 포함되는 $\vec{x}_t^{KP}$의 내적이 0이 되지 않는 i의 집합 I^{KP}를 특정함과 아울러, 특정한 집합 I^{KP}에 포함되는 i에 대하여, $\alpha_i^{KP} M_i^{KP}$를 합계한 경우에 상기 $\vec{h}^{KP}$가 되는 보완 계수 α_i^{KP}를 계산하는 KP 보완 계수 계산부와, 상기 암호화 데이터 $ct_{(\Gamma KP,\ SCP)}$에 포함되는 i=1, …, L^{CP}의 각 정수 i에 대한 변수 $\rho^{CP}(i)$와, 상기 복호 키 $sk_{(SKP,\ \Gamma CP)}$에 포함되는 속성 집합 Γ^{CP}에 근거하여, i=1, …, L^{CP}의 각 정수 i 중, 변수 $\rho^{CP}(i)$가 긍정형의 조 $(t, \vec{v}_i^{CP})$이고, 또한, 그 조의 $\vec{v}_i^{CP}$와, 그 조의 식별 정보 t가 나타내는 Γ^{CP}에 포함되는 $\vec{x}_{tCP}$의 내적이 0이 되는 i와, 변수 $\rho^{CP}(i)$가 부정형의 조 $\neg(t, \vec{v}_i^{CP})$이고, 또한, 그 조의 $\vec{v}_i^{CP}$와, 그 조의 식별 정보 t가 나타내는 Γ^{CP}에 포함되는 $\vec{x}_t^{CP}$의 내적이 0이 되지 않는 i의 집합 I^{CP}를 특정함과 아울러, 특정한 집합 I^{CP}에 포함되는 i에 대하여, $\alpha_i^{CP} M_i^{CP}$를 합계한 경우에 상기 $\vec{h}^{CP}$가 되는 보완 계수 α_i^{CP}를 계산하는 CP 보완 계수 계산부와, 상기 암호화 데이터 $ct_{(\Gamma KP,\ SCP)}$에 포함되는 요소 c_0과 요소 c_t^{KP}와 요소 c_i^{CP}와, 상기 복호 키 $sk_{(SKP,\ \Gamma CP)}$에 포함되는 요소 k_0^*과 요소 k_i^{*KP}와 요소 k_t^{*CP}에 대하여, 상기 KP 보완 계수 계산부가 특정한 집합 I^{KP}와, 상기 KP 보완 계수 계산부가 계산한 보완 계수 α_i^{KP}와, 상기 CP 보완 계수 계산부가 특정한 집합 I^{CP}와, 상기 CP 보완 계수 계산부가 계산한 보완 계수 α_i^{CP}에 근거하여, 수학식 1에 나타내는 페어링 연산을 행하여 값 K를 계산하는 페어링 연산부를 구비하는 것을 특징으로 한다.

[0038] [수학식 1]

$$K := e(c_0, k_0^*) \cdot \prod_{i \in I^{KP} \wedge \rho^{KP}(i) = (t, \vec{v}_i^{KP})} e(c_t^{KP}, k_i^{*KP})^{\alpha_i^{KP}} \cdot \prod_{i \in I^{KP} \wedge \rho^{KP}(i) = \neg(t, \vec{v}_i^{KP})} e(c_t^{KP}, k_i^{*KP})^{\alpha_i^{KP}/(\vec{v}_i^{KP} \cdot \vec{x}_t^{KP})} \cdot \prod_{i \in I^{CP} \wedge \rho^{CP}(i) = (t, \vec{v}_i^{CP})} e(c_t^{CP}, k_i^{*CP})^{\alpha_i^{CP}} \cdot \prod_{i \in I^{CP} \wedge \rho^{CP}(i) = \neg(t, \vec{v}_i^{CP})} e(c_t^{CP}, k_i^{*CP})^{\alpha_i^{CP}/(\vec{v}_i^{CP} \cdot \vec{x}_t^{CP})}$$

[0039]

발명의 효과

[0040] 본 발명에 따른 암호 처리 시스템은, 복호 키와 암호문의 양쪽에 액세스 스트럭처가 삽입되어 있고, 다기능의 암호 기능을 실현하고 있다.

도면의 간단한 설명

[0041] 도 1은 행렬 $\hat{M}$의 설명도.

도 2는 행렬 M_δ의 설명도.

도 3은 s_0의 설명도.

도 4는 $\vec{s}^T$의 설명도.

도 5는 Unified-Policy 함수형 암호 방식을 실행하는 암호 처리 시스템(10)의 구성도.

도 6은 키 생성 장치(100)의 기능을 나타내는 기능 블록도.

도 7은 암호화 장치(200)의 기능을 나타내는 기능 블록도.

도 8은 복호 장치(300)의 기능을 나타내는 기능 블록도.

도 9는 Setup 알고리즘의 처리를 나타내는 플로차트.

도 10은 KeyGen 알고리즘의 처리를 나타내는 플로차트.

도 11은 Enc 알고리즘의 처리를 나타내는 플로차트.

도 12는 Dec 알고리즘의 처리를 나타내는 플로차트.

도 13은 키 생성 장치(100), 암호화 장치(200), 복호 장치(300)의 하드웨어 구성의 일례를 나타내는 도면.

발명을 실시하기 위한 구체적인 내용

[0042] 이하, 도면에 근거하여, 발명을 실시의 형태를 설명한다.

[0043] 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. 다시 말해, 처리 장치, 기억 장치, 통신 장치, 입력 장치는 하드웨어이다.

[0044] 이하의 설명에 있어서의 기법에 대하여 설명한다.

[0045] A가 랜덤 변수 또는 분포일 때, 수학식 101은, A의 분포에 따라 A로부터 y를 랜덤 선택하는 것을 나타낸다. 다시 말해, 수학식 101에 있어서, y는 난수이다.

[0046] [수학식 101]

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

[0048] A가 집합일 때, 수학식 102는, A로부터 y를 균등하게 선택하는 것을 나타낸다. 다시 말해, 수학식 102에 있어서, y는 균등 난수이다.

[0049] [수학식 102]

[0050] $$y \xleftarrow{U} A$$

[0051] 수학식 103은, y가 z에 의해 정의된 집합인 것, 또는 y가 z가 대입된 집합인 것을 나타낸다.

[0052] [수학식 103]

[0053] $$y := z$$

[0054] a가 상수일 때, 수학식 104는, 기계(알고리즘) A가 입력 x에 대하여 a를 출력하는 것을 나타낸다.

[0055] [수학식 104]

$$A(x) \to a$$

예컨대,

[0056] $$A(x) \to 1$$

[0057] 수학식 105, 다시 말해 F_q는, 위수 q의 유한체를 나타낸다.

[0058] [수학식 105]

[0059] $$\mathbb{F}_q$$

[0060] 벡터 표기는, 유한체 F_q에 있어서의 벡터 표시를 나타낸다. 다시 말해, 수학식 106이다.

[0061] [수학식 106]

$\vec{x}$는

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

[0062] 를 나타낸다

[0063] 수학식 107은, 수학식 108에 나타내는 2개의 벡터 $\vec{x}$와 $\vec{v}$의 수학식 109에 나타내는 내적을 나타낸다.

[0064] [수학식 107]

[0065] $\vec{x}\cdot\vec{v}$

[0066] [수학식 108]

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

[0067] $\vec{v}=(v_1,\ldots,v_n)$

[0068] [수학식 109]

[0069] $\sum_{i=1}^{n}x_iv_i$

[0070] X^T는, 행렬 X의 전치 행렬을 나타낸다.

[0071] 수학식 110에 나타내는 기저 B와 기저 B^*에 대하여, 수학식 111이다.

[0072] [수학식 110]

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

[0073] $\mathbb{B}^*:=(b_1^*,\ldots,b_N^*)$

[0074] [수학식 111]

$(x_1,\ldots,x_N)_{\mathbb{B}}:=\sum_{i=1}^{N}x_ib_i,$

[0075] $(y_1,\ldots,y_N)_{\mathbb{B}^*}:=\sum_{i=1}^{N}y_ib_i^*$

[0076] $\vec{e}_{t,j}^{KP}$, $\vec{e}_{t,j}^{CP}$는, 각각 수학식 112에 나타내는 정규 기저 벡터를 나타낸다.

[0077] [수학식 112]

$\vec{e}_{t,j}^{KP}:(\overbrace{0\cdots0}^{j-1},1,\overbrace{0\cdots0}^{n_t-j})\in\mathbb{F}_q^{n_t^{KP}}\ \text{for}\ j=1,\ldots,n_t^{KP},$

[0078] $\vec{e}_{t,j}^{CP}:(\overbrace{0\cdots0}^{j-1},1,\overbrace{0\cdots0}^{n_t-j})\in\mathbb{F}_q^{n_t^{CP}}\ \text{for}\ j=1,\ldots,n_t^{CP}$

[0079] 또한, 이하의 설명에 있어서, F_q^{ntCP}에 있어서의 ntCP는 n_t^{CP}이다.

[0080] 마찬가지로, 복호 키 $sk_{(SKP,\ \Gamma CP)}$에 있어서의 SKP는 S^{KP}이고, ΓCP는 Γ^{CP}이다. 암호화 데이터 $ct_{(\Gamma KP,\ SCP)}$에 있어서의 ΓKP는 Γ^{KP}이고, SCP는 S^{CP}이다.

[0081] 마찬가지로, $param_{V0}$에 있어서의 V0은 V_0이다. $param_{VtKP}$에 있어서의 VtKP는 V_t^{KP}이다. $param_{VtCP}$에 있어서의 VtCP는 V_t^{CP}이다.

[0082] 마찬가지로, "δi,j"가 어깨 글자(superior letter)로 나타나 있는 경우, 이 δi,j는, $\delta_{i,j}$를 의미한다.

[0083] 또한, 벡터를 의미하는 "→"가 다리 글자(inferior letter) 또는 어깨 글자에 붙어 있는 경우, 이 "→"는 다리

글자 또는 어깨 글자에 어깨 글자로 붙어 있는 것을 의미한다.

[0084] 또한, 이하의 설명에 있어서, 암호 처리란, 키 생성 처리, 암호화 처리, 복호 처리를 포함하는 것이다.

[0085] 실시의 형태 1.

[0086] 본 실시의 형태에서는, 「함수형 암호(Functional Encryption) 방식」을 실현하는 기초가 되는 개념과, 함수형 암호의 구성에 대하여 설명한다.

[0087] 제 1에, 함수형 암호에 대하여 간단히 설명한다.

[0088] 제 2에, 함수형 암호를 실현하기 위한 공간인 「쌍대 페어링 벡터 공간(Dual Pairing Vector Spaces, DPVS)」이라고 하는 풍부한 수학적 구조를 갖는 공간을 설명한다.

[0089] 제 3에, 함수형 암호를 실현하기 위한 개념을 설명한다. 여기서는, 「스팬 프로그램(Span Program)」, 「속성 벡터의 내적과 액세스 스트럭쳐」, 「비밀 분산 방식(비밀 공유 방식)」에 대하여 설명한다.

[0090] 제 4에, 본 실시의 형태에 따른 「함수형 암호 방식」을 설명한다. 본 실시의 형태에서는, 「Unified-Policy 함수형 암호(Unified-Policy Functional Encryption, UP-FE) 방식」에 대하여 설명한다. 그래서, 우선, 「Unified-Policy 함수형 암호 방식」의 기본 구성에 대하여 설명한다. 다음으로, 이 「Unified-Policy 함수형 암호 방식」을 실현하는 「암호 처리 시스템(10)」의 기본 구성에 대하여 설명한다. 그리고, 본 실시의 형태에 따른 「Unified-Policy 함수형 암호 방식」 및 「암호 처리 시스템(10)」에 대하여 상세히 설명한다.

[0091] <제 1. 함수형 암호 방식>

[0092] 함수형 암호 방식은, 암호화 키(encryption-key, ek)와, 복호 키(decryption-key, dk)의 사이의 관계를 보다 고도화하고, 보다 유연하게 한 암호 방식이다.

[0093] 함수형 암호 방식에 있어서, 암호화 키와 복호 키는, 각각, 속성 x와 속성 v가 설정되어 있다. 그리고, 관계 R에 대하여 R(x, v)가 성립하는 경우에 한하여, 복호 키 $dk_v:=(dk, v)$는 암호화 키 $ek_x:=(ek, x)$로 암호화된 암호문을 복호할 수 있다.

[0094] 함수형 암호 방식에는, 데이터베이스의 액세스 컨트롤, 메일 서비스, 콘텐츠 배포 등의 다양한 어플리케이션이 존재한다(비특허 문헌 2, 7, 9, 16, 19, 25-28, 30 참조).

[0095] R이 등호 관계인 경우, 다시 말해, x=v인 경우에 한하여 R(x, v)가 성립하는 경우, 함수형 암호 방식은 ID 베이스 암호 방식이다.

[0096] ID 베이스 암호 방식보다 일반화된 함수형 암호 방식으로서, 속성 베이스 암호 방식이 있다.

[0097] 속성 베이스 암호 방식에서는, 암호화 키와 복호 키에 설정되는 속성이 속성의 조이다. 예컨대, 암호화 키와 복호 키에 설정되는 속성이, 각각, $X:=(x_1, \cdots, x_d)$와, $V:=(v_1, \cdots, v_d)$이다.

[0098] 그리고, 속성의 컴포넌트에 대하여, 컴포넌트마다의 등호 관계(예컨대, $\{x_t=v_t\}_{t\in\{1, \cdots, d\}}$)가 액세스 스트럭쳐 S에 입력된다. 그리고, 액세스 스트럭쳐 S가 입력을 수리한 경우에만, R(X, V)가 성립한다. 다시 말해, 암호화 키로 암호화된 암호문을 복호 키로 복호할 수 있다.

[0099] 액세스 스트럭쳐 S가 복호 키 dk_V에 삽입되어 있는 경우, 속성 베이스 암호(ABE) 방식은, Key-Policy ABE(KP-ABE)라고 불린다. 한편, 액세스 스트럭쳐 S가 암호문에 삽입되어 있는 경우, 속성 베이스 암호(ABE) 방식은, Ciphertext-Policy ABE(CP-ABE)라고 불린다. 그리고, 액세스 스트럭쳐 S가 복호 키 dk_V와 암호문의 양쪽에 삽입되어 있는 경우, 속성 베이스 암호(ABE) 방식은, Unified-Policy ABE(UP-ABE)라고 불린다.

[0100] 비특허 문헌 19에 기재된 내적 술어 암호(Inner-Product Encryption, IPE)도 함수형 암호의 하나의 클래스이다. 여기서는, 암호화 키와 복호 키에 설정되는 속성이 각각 체 또는 환상의 벡터이다. 예컨대, $\vec{x}:=(x_1, \cdots, x_n)\in F_q^n$과 $\vec{v}:=(v_1, \cdots, v_n)\in F_q^n$이 각각 암호화 키와 복호 키에 설정된다. 그리고, $\vec{x}\cdot\vec{v}=0$인 경우에 한하여, $R(\vec{x}, \vec{v})$가 성립한다.

[0101] <제 2. 쌍대 페어링 벡터 공간>

[0102] 우선, 대칭 쌍선형 페어링군(Symmetric Bilinear Pairing Groups)에 대하여 설명한다.

[0103] 대칭 쌍선형 페어링군(q, G, G^T, g, e)는, 소수 q와, 위수 q의 순회 덧셈군 G와, 위수 q의 순회 곱셈군 G^T와, g≠0∈G와, 다항식 시간에 계산 가능한 비퇴화 쌍선형 페어링(Nondegenerate Bilinear Pairing) e:G×G→G_T의 조이다. 비퇴화 쌍선형 페어링은, $e(sg, tg)=e(g, g)^{st}$이고, e(g, g)≠1이다.

[0104] 이하의 설명에 있어서, 수학식 113을, 1^{λ}를 입력으로 하여, 시큐리티 파라미터를 λ로 하는 쌍선형 페어링군의 파라미터 $param_G:=(q, G, G_T, g, e)$의 값을 출력하는 알고리즘으로 한다.

[0105] [수학식 113]

[0106] $\mathcal{G}_{bpg}$

[0107] 다음으로, 쌍대 페어링 벡터 공간에 대하여 설명한다.

[0108] 쌍대 페어링 벡터 공간 (q, V, G_T, A, e)는, 대칭 쌍선형 페어링군($param_G:=(q, G, G^T, g, e)$)의 직적에 의해 구성할 수 있다. 쌍대 페어링 벡터 공간 (q, V, G_T, A, e)는, 소수 q, 수학식 114에 나타내는 F_q상의 N차원 벡터 공간 V, 위수 q의 순회군 G_T, 공간 V의 표준 기저 $A:=(a_1, \cdots, a_N)$의 조이고, 이하의 연산 (1), (2)를 갖는다. 여기서, a_i는, 수학식 115에 나타내는 것과 같다.

[0109] [수학식 114]

[0110] $$\mathbb{V} := \overbrace{\mathbb{G} \times \cdots \times \mathbb{G}}^{N}$$

[0111] [수학식 115]

[0112] $$a_i := (\overbrace{0,\ldots,0}^{i-1}, g, \overbrace{0,\ldots,0}^{N-i})$$

[0113] 연산 (1) : 비퇴화 쌍선형 페어링

[0114] 공간 V에 있어서의 페어링은, 수학식 116에 의해 정의된다.

[0115] [수학식 116]

$$e(x,y) := \prod_{i=1}^{N} e(G_i, H_i) \in \mathbb{G}_T$$

여기서,

$$(G_1,\ldots,G_N) := x \in \mathbb{V},$$
$$(H_1,\ldots,H_N) := y \in \mathbb{V}$$

[0116] 이다.

[0117] 이것은, 비퇴화 쌍선형이다. 다시 말해, $e(sx, ty)=e(x, y)^{st}$이고, 모든 y∈V에 대하여, e(x, y)=1인 경우, x=0이다. 또한, 모든 i와 j에 대하여, $e(a_i, a_j)=e(g, g)^{\delta_{i,j}}$이다. 여기서, i=j이면, $\delta_{i,j}=1$이고, i≠j이면, $\delta_{i,j}=0$이다. 또한, $e(g, g)\neq 1 \in G_T$이다.

[0118] 연산 (2) : 디스토션 사상

[0119] 수학식 117에 나타내는 공간 V에 있어서의 선형 변환 $\phi_{i,j}$는, 수학식 118을 행할 수 있다.

[0120] [수학식 117]

$\phi_{i,j}(a_j) = a_i$이고,

[0121] $k \neq j$이면, $\phi_{i,j}(a_k) = 0$이다

[0122] [수학식 118]

$$\phi_{i,j}(x) := (\overbrace{0,\ldots,0}^{i-1}, g_j, \overbrace{0,\ldots,0}^{N-i})$$

여기서,

$$(g_1,\ldots g_N) := x$$

[0123] 이다

[0124] 여기서, 선형 변환 $\Phi_{i,j}$를 디스토션 사상이라고 부른다.

[0125] 이하의 설명에 있어서, 수학식 119를, 1^{λ}(λ∈자연수), N∈자연수, 쌍선형 페어링군의 파라미터 $param_G$:=(q, G, G_T, g, e)의 값을 입력으로 하여, 시큐리티 파라미터가 λ이고, N차원의 공간 V로 하는 쌍대 페어링 벡터 공간의 파라미터 $param_V$:=(q, V, G_T, A, e)의 값을 출력하는 알고리즘으로 한다.

[0126] [수학식 119]

[0127] $\mathcal{G}_{dpvs}$

[0128] 또, 여기서는, 상술한 대칭 쌍선형 페어링군에 의해, 쌍대 페어링 벡터 공간을 구성한 경우에 대하여 설명한다. 또, 비대칭 쌍선형 페어링군에 의해 쌍대 페어링 벡터 공간을 구성하는 것도 가능하다. 이하의 설명을, 비대칭 쌍선형 페어링군에 의해 쌍대 페어링 벡터 공간을 구성한 경우에 응용하는 것은 용이하다.

[0129] <제 3. 함수형 암호를 실현하기 위한 개념>

[0130] <제 3-1. 스팬 프로그램>

[0131] 도 1은, 행렬 $\hat{M}$의 설명도이다.

[0132] $\{p_1, \cdots, p_n\}$을 변수의 집합으로 한다. $\hat{M}$:=(M, ρ)는, 레이블링(labeling)된 행렬이다. 여기서, 행렬 M은, F_q 상의 (L행×r열)의 행렬이다. 또한, ρ는, 행렬 M의 각 행에 부여된 레이블이고, $\{p_1, \cdots, p_n, \neg p_1, \cdots, \neg p_n\}$의 어느 1개의 리터럴(literal)에 대응된다. 또, M의 모든 행에 부여된 레이블 ρ_i(i=1, …, L)가 어느 1개의 리터럴에 대응된다. 다시 말해, ρ:{1, …, L}→$\{p_1, \cdots, p_n, \neg p_1, \cdots, \neg p_n\}$이다.

[0133] 모든 입력열 $\delta \in \{0, 1\}^n$에 대하여, 행렬 M의 부분 행렬 M_δ는 정의된다. 행렬 M_δ는, 입력열 δ에 의해 레이블 ρ에 값 "1"이 대응된 행렬 M의 행으로 구성되는 부분 행렬이다. 다시 말해, 행렬 M_δ는, δ_i=1인 p_i에 대응된 행렬 M의 행과, δ_i=0인 $\neg p_i$에 대응된 행렬 M의 행으로 이루어지는 부분 행렬이다.

[0134] 도 2는, 행렬 M_δ의 설명도이다. 또, 도 2에서는, n=7, L=6, r=5로 하고 있다. 다시 말해, 변수의 집합은, $\{p_1, \cdots, p_7\}$이고, 행렬 M은 (6행×5열)의 행렬이다. 또한, 도 2에 있어서, 레이블 ρ는, ρ_1이 $\neg p_2$에, ρ_2가 p_1에, ρ_3이 p_4에, ρ_4가 $\neg p_5$에, ρ_5가 $\neg p_3$에, ρ_6이 p_5에 각각 대응되어 있는 것으로 한다.

[0135] 여기서, 입력열 $\delta \in \{0, 1\}^7$이, δ_1=1, δ_2=0, δ_3=1, δ_4=0, δ_5=0, δ_6=1, δ_7=1인 것으로 한다. 이 경우, 파선으로 둘러싼 리터럴 (p_1, p_3, p_6, p_7, $\neg p_2$, $\neg p_4$, $\neg p_5$)에 대응되어 있는 행렬 M의 행으로 이루어지는 부분 행렬이 행렬 M_δ이다. 다시 말해, 행렬 M의 1행째(M_1), 2행째(M_2), 4행째(M_4)로 이루어지는 부분 행렬이 행렬 M_δ이다.

[0136] 바꿔 말하면, 사상 γ:{1, …, L}→{0, 1}이, [ρ(j)=p_i]∧[δ_i=1] 또는 [ρ(j)=$\neg p_i$]∧[δ_i=0]인 경우, γ(j)=1이고, 다른 경우, γ(j)=0인 것으로 한다. 이 경우에, M_δ:=$(M_j)_{\gamma(j)=1}$이다. 여기서, M_j는, 행렬 M의 j번째의 행이다.

[0137] 다시 말해, 도 2에서는, 사상 γ(j)=1(j=1, 2, 4)이고, 사상 γ(j)=0(j=3, 5, 6)이다. 따라서, $(M_j)_{\gamma(j)=1}$은,

M_1, M_2, M_4이고, 행렬 M_δ이다.

[0138] 즉, 사상 $\chi(j)$의 값이 "0"인지 "1"인지에 따라, 행렬 M의 j번째의 행이 행렬 M_δ에 포함되는지 여부가 결정된다.

[0139] $\vec{1} \in \mathrm{span}\langle M_\delta \rangle$인 경우에 한해, 스팬 프로그램 $\hat{M}$는 입력열 δ를 수리하고, 다른 경우에는 입력열 δ를 거절한다. 다시 말해, 입력열 δ에 의해 행렬 $\hat{M}$로부터 얻어지는 행렬 M_δ의 행을 선형 결합하여 $\vec{1}$가 얻어지는 경우에 한해, 스팬 프로그램 $\hat{M}$는 입력열 δ를 수리한다. 또, $\vec{1}$란, 각 요소가 값 "1"인 행 벡터이다.

[0140] 예컨대, 도 2의 예이면, 행렬 M의 1, 2, 4행째로 이루어지는 행렬 M_δ의 각 행을 선형 결합하여 $\vec{1}$가 얻어지는 경우에 한해, 스팬 프로그램 $\hat{M}$는 입력열 δ를 수리한다. 다시 말해, $\alpha_1(M_1)+\alpha_2(M_2)+\alpha_4(M_4)=\vec{1}$가 되는 α_1, α_2, α_4가 존재하는 경우에는, 스팬 프로그램 $\hat{M}$는 입력열 δ를 수리한다.

[0141] 여기서, 레이블 ρ가 정의 리터럴 $\{p_1, \cdots, p_n\}$에만 대응되어 있는 경우, 스팬 프로그램은 모토톤이라고 불린다. 한편, 레이블 ρ가 리터럴 $\{p_1, \cdots, p_n, \neg p_1, \cdots, \neg p_n\}$에 대응되어 있는 경우, 스팬 프로그램은 논모토톤이라고 불린다. 여기서는, 스팬 프로그램은 논모토톤으로 한다. 그리고, 논모토톤 스팬 프로그램을 이용하여, 액세스 스트럭쳐(논모토톤 액세스 스트럭쳐)를 구성한다. 액세스 스트럭쳐란, 간단히 말하면 암호로의 액세스 제어를 행하는 것이다. 다시 말해, 암호문을 복호할 수 있는지 여부의 제어를 행하는 것이다.

[0142] 자세하게는 후술하지만, 스팬 프로그램이 모토톤이 아니고, 논모토톤인 것에 의해, 스팬 프로그램을 이용하여 구성하는 함수형 암호 방식의 이용 범위가 넓어진다.

[0143] <제 3-2. 속성 벡터의 내적과 액세스 스트럭쳐>

[0144] 여기서는, 속성 벡터의 내적을 이용하여 상술한 사상 $\chi(j)$를 계산한다. 다시 말해, 속성 벡터의 내적을 이용하여, 행렬 M의 어느 행을 행렬 M_δ에 포함시킬지를 결정한다.

[0145] U_t(t=1, …, d이고 $U_t \subset \{0, 1\}^*$)는, 부분 전체집합(sub-universe)이고, 속성의 집합이다. 그리고, U_t는, 각각 부분 전체집합의 식별 정보(t)와, n_t차원 벡터($\vec{v}$)를 포함한다. 다시 말해, U_t는, $(t, \vec{v})$이다. 여기서, $t \in \{1, \cdots, d\}$이고, $\vec{v} \in F_q^{nt}$이다.

[0146] $U_t := (t, \vec{v})$를 스팬 프로그램 $\hat{M} := (M, \rho)$에 있어서의 변수 p로 한다. 다시 말해, $p := (t, \vec{v})$이다. 그리고, 변수 $(p := (t, \vec{v}), (t', \vec{v'}), \cdots)$로 한 스팬 프로그램 $\hat{M} := (M, \rho)$를 액세스 스트럭쳐 S로 한다.

[0147] 다시 말해, 액세스 스트럭쳐 $S := (M, \rho)$이고, $\rho : \{1, \cdots, L\} \rightarrow \{(t, \vec{v}), (t', \vec{v'}), \cdots, \neg(t, \vec{v}), \neg(t', \vec{v'}), \cdots\}$이다.

[0148] 다음으로, Γ를 속성의 집합으로 한다. 다시 말해, $\Gamma := \{(t, \vec{x}_t) \mid \vec{x}_t \in Fq^{nt}, 1td\}$이다.

[0149] 액세스 스트럭쳐 S에 Γ가 주어진 경우, 스팬 프로그램 $\hat{M} := (M, \rho)$에 대한 사상 $\chi : \{1, \cdots, L\} \rightarrow \{0, 1\}$은, 이하와 같이 정의된다. i=1, …, L의 각 정수 i에 대하여, $[\rho(i) = (t, \vec{v}_i)] \wedge [(t, \vec{x}_t) \in \Gamma] \wedge [\vec{v}_i \cdot \vec{x}_t = 0]$, 또는, $[\rho(i) = \neg(t, \vec{v}_i)] \wedge [(t, \vec{x}_t) \in \Gamma] \wedge [\vec{v}_i \cdot \vec{x}_t \neq 0]$인 경우, $\chi(j)=1$이고, 다른 경우, $\chi(j)=0$으로 한다.

[0150] 다시 말해, 속성 벡터 $\vec{v}$와 $\vec{x}$의 내적에 근거하여, 사상 χ가 계산된다. 그리고, 상술한 바와 같이, 사상 χ에 의해, 행렬 M의 어느 행을 행렬 M_δ에 포함시킬지가 결정된다. 즉, 속성 벡터 $\vec{v}$와 $\vec{x}$의 내적에 의해, 행렬 M의 어느 행을 행렬 M_δ에 포함시킬지가 결정되고, $\vec{1} \in \mathrm{span}\langle (M_i)_{\chi(i)=1} \rangle$인 경우에 한해, 액세스 스트럭쳐 $S := (M,$

ρ)는 Γ를 수리한다.

[0151] <제 3-3. 비밀 분산 방식>

[0152] 액세스 스트럭쳐 S:=(M, ρ)에 대한 비밀 분산 방식에 대하여 설명한다.

[0153] 또, 비밀 분산 방식이란, 비밀 정보를 분산시키고, 의미가 없는 분산 정보로 하는 것이다. 예컨대, 비밀 정보 s를 10개로 분산시키고, 10개의 분산 정보를 생성한다. 여기서, 10개의 분산 정보 각각은, 비밀 정보 s의 정보를 갖고 있지 않다. 따라서, 어느 1개의 분산 정보를 손에 넣더라도 비밀 정보 s에 관하여 조금도 정보를 얻을 수는 없다. 한편, 10개의 분산 정보를 모두 손에 넣으면, 비밀 정보 s를 복원할 수 있다.

[0154] 또한, 10개의 분산 정보를 모두 손에 넣지 않더라도, 일부만(예컨대, 8개) 손에 넣으면 비밀 정보 s를 복원할 수 있는 비밀 분산 방식도 있다. 이와 같이, 10개의 분산 정보 중 8개로 비밀 정보 s를 복원할 수 있는 경우를, 8-out-of-10이라고 부른다. 다시 말해, n개의 분산 정보 중 t개로 비밀 정보 s를 복원할 수 있는 경우를, t-out-of-n이라고 부른다. 이 t를 임계치라고 부른다.

[0155] 또한, d_1, …, d_{10}의 10개의 분산 정보를 생성한 경우에, d_1, …, d_8까지의 8개의 분산 정보이면 비밀 정보 s를 복원할 수 있지만, d_3, …, d_{10}까지의 8개의 분산 정보이면 비밀 정보 s를 복원할 수 없다고 하는 비밀 분산 방식도 있다. 다시 말해, 손에 넣은 분산 정보의 수뿐만 아니라, 분산 정보의 조합에 따라 비밀 정보 s를 복원할 수 있는지 여부를 제어하는 비밀 분산 방식도 있다.

[0156] 도 3은, s_0의 설명도이다. 도 4는, $\vec{s}^{T}$의 설명도이다.

[0157] 행렬 M을 (L행×r열)의 행렬로 한다. $\vec{f}^{T}$를 수학식 120에 나타내는 열 벡터로 한다.

[0158] [수학식 120]

[0159] $$\vec{f}^{\mathrm{T}} := (f_1, \ldots f_r)^T \xleftarrow{U} \mathbb{F}_q^r$$

[0160] 수학식 121에 나타내는 s_0을 공유시키는 비밀 정보로 한다.

[0161] [수학식 121]

[0162] $$s_0 := \vec{1} \cdot \vec{f}^{\mathrm{T}} := \sum_{k=1}^{r} f_k$$

[0163] 또한, 수학식 122에 나타내는 $\vec{s}^{T}$를 s_0의 L개의 분산 정보의 벡터로 한다.

[0164] [수학식 122]

[0165] $$\vec{s}^{\mathrm{T}} := (s_1, \ldots s_L)^{\mathrm{T}} := M \cdot \vec{f}^{\mathrm{T}}$$

[0166] 그리고, 분산 정보 s_i를 ρ(i)에 속하는 것으로 한다.

[0167] 액세스 스트럭쳐 S:=(M, ρ)가 Γ를 수리하는 경우, 다시 말해 ɣ:{1, …, L}→{0, 1}에 대하여 $\vec{1} \in \mathrm{span}\langle (M_i)_{\gamma(i)=1} \rangle$인 경우, I⊆{i∈{1, …, L} | ɣ(i)=1}인 상수 $\{\alpha_i \in F_q \mid i \in I\}$가 존재한다.

[0168] 이것은, 도 2의 예에서, $\alpha_1(M_1)+\alpha_2(M_2)+\alpha_4(M_4)=\vec{1}$가 되는 α_1, α_2, α_4가 존재하는 경우에는, 스팬 프로그램 $\hat{M}$는 입력열 δ를 수리한다고 설명한 것으로부터도 분명하다. 다시 말해, $\alpha_1(M_1)+\alpha_2(M_2)+\alpha_4(M_4)=\vec{1}$가 되는 α_1, α_2, α_4가 존재하는 경우에는, 스팬 프로그램 $\hat{M}$가 입력열 δ를 수리하는 것이면, $\alpha_1(M_1)+\alpha_2(M_2)+\alpha_4(M_4)=\vec{1}$가 되는 α_1, α_2, α_4가 존재한다.

[0169] 그리고, 수학식 123이다.

[0170] [수학식 123]

[0171] $$\sum_{i\in I}\alpha_i s_i := s_0$$

[0172] 또, 상수 $\{\alpha_i\}$는, 행렬 M의 사이즈에 있어서의 다항식 시간에 계산 가능하다.

[0173] 본 실시의 형태 및 이하의 실시의 형태에 따른 함수형 암호 방식은, 상술한 바와 같이, 스팬 프로그램에 내적 술어와 비밀 분산 방식을 적용하여 액세스 스트럭쳐를 구성한다. 그 때문에, 스팬 프로그램에 있어서의 행렬 M이나, 내적 술어에 있어서의 속성 정보 x 및 속성 정보 v(술어 정보)를 설계하는 것에 의해, 액세스 제어를 자유롭게 설계할 수 있다. 다시 말해, 매우 높은 자유도로 액세스 제어의 설계를 행할 수 있다. 또, 행렬 M의 설계는, 비밀 분산 방식의 임계치 등의 조건 설계에 상당한다.

[0174] 예컨대, 상술한 속성 베이스 암호 방식은, 본 실시의 형태 및 이하의 실시의 형태에 따른 함수형 암호 방식에 있어서의 액세스 스트럭쳐에 있어서, 내적 술어의 설계를 어느 조건으로 한정한 경우에 상당한다. 다시 말해, 본 실시의 형태 및 이하의 실시의 형태에 따른 함수형 암호 방식에 있어서의 액세스 스트럭쳐에 비하여, 속성 베이스 암호 방식에 있어서의 액세스 스트럭쳐는, 내적 술어에 있어서의 속성 정보 x 및 속성 정보 v(술어 정보)가 설계의 자유도가 없는 만큼, 액세스 제어의 설계의 자유도가 낮다. 또, 구체적으로는, 속성 베이스 암호 방식은, 속성 정보 $\{\vec{x}_t\}_{t\in\{1,\cdots,d\}}$와 $\{\vec{v}_t\}_{t\in\{1,\cdots,d\}}$를, 등호 관계에 대한 2차원 벡터, 예컨대 $\vec{x}_t:=(1, x_t)$와 $\vec{v}_t:=(v_t, -1)$로 한정한 경우에 상당한다.

[0175] 또한, 상술한 내적 술어 암호 방식은, 본 실시의 형태 및 이하의 실시의 형태에 따른 함수형 암호 방식에 있어서의 액세스 스트럭쳐에 있어서, 스팬 프로그램에 있어서의 행렬 M의 설계를 어느 조건으로 한정한 경우에 상당한다. 다시 말해, 본 실시의 형태 및 이하의 실시의 형태에 따른 함수형 암호 방식에 있어서의 액세스 스트럭쳐에 비하여, 내적 술어 암호 방식에 있어서의 액세스 스트럭쳐는, 스팬 프로그램에 있어서의 행렬 M의 설계의 자유도가 없는 만큼, 액세스 제어의 설계의 자유도가 낮다. 또, 구체적으로는, 내적 술어 암호 방식은, 비밀 분산 방식을 1-out-of-1(혹은, d-out-of-d)로 한정한 경우이다.

[0176] 특히, 본 실시의 형태 및 이하의 실시의 형태에 따른 함수형 암호 방식에 있어서의 액세스 스트럭쳐는, 논모토톤 스팬 프로그램을 이용한 논모토톤 액세스 스트럭쳐를 구성한다. 그 때문에, 액세스 제어의 설계의 자유도가 보다 높아진다.

[0177] 구체적으로는, 논모토톤 스팬 프로그램에는, 부정형의 리터럴($\neg p$)을 포함하기 때문에, 부정형의 조건을 설정할 수 있다. 예컨대, 제 1 회사에는, A부와 B부와 C부와 D부의 4개의 부서가 있는 것으로 한다. 여기서, 제 1 회사의 B부 이외의 부서에 속하는 사용자에게만 액세스 가능(복호 가능)하다고 하는 액세스 제어를 하고 싶은 것으로 한다. 이 경우에, 부정형의 조건의 설정을 할 수 없는 것으로 하면, 「제 1 회사의 A부와 C부와 D부의 어느 하나에 속할 것」이라고 하는 조건을 설정할 필요가 있다. 한편, 부정형의 조건의 설정을 할 수 있는 것으로 하면, 「제 1 회사의 사원이고, B부 이외에 속할 것」이라고 하는 조건을 설정할 수 있다. 다시 말해, 부정형의 조건을 설정할 수 있는 것에 의해, 자연스러운 조건 설정이 가능하게 된다. 또, 여기서는 부서의 수가 적지만, 부서의 수가 많은 경우 등은 매우 유효한 것을 알 수 있다.

[0178] <제 4. 함수형 암호 방식의 기본 구성>

[0179] <제 4-1. Unified-Policy 함수형 암호 방식의 기본 구성>

[0180] Unified-Policy 함수형 암호 방식의 구성을 간단히 설명한다. 또, Unified-Policy란, 복호 키 및 암호문에 Policy가 삽입되는 것, 다시 말해 액세스 스트럭쳐가 삽입되는 것을 의미한다.

[0181] Unified-Policy 함수형 암호 방식은, Setup, KeyGen, Enc, Dec의 4개의 알고리즘을 구비한다.

[0182] (Setup)

[0183] Setup 알고리즘은, 시큐리티 파라미터 λ와, 속성의 포맷 $\vec{n}:=((d^{KP}; n_t^{KP}, u_t^{KP}, w_t^{KP}, z_t^{KP}(t=1, \cdots, d^{KP})), (d^{CP}; n_t^{CP}, u_t^{CP}, w_t^{CP}, z_t^{CP}(t=1, \cdots, d^{CP})))$가 입력되고, 공개 파라미터 pk와, 마스터 키 sk를 출력하는 확률적 알고리즘이다.

[0184] (KeyGen)

[0185] KeyGen 알고리즘은, 액세스 스트럭쳐 $S^{KP}:=(M^{KP}, \rho^{KP})$와, 속성의 집합인 $\Gamma^{CP}:=\{(t, \vec{x}_t^{CP}) \mid \vec{x}_t^{CP} \in F_q^{ntCP} \setminus \{\vec{0}\}, 1td^{CP}\}$와, 공개 파라미터 pk와, 마스터 키 sk를 입력으로 하여, 복호 키 $sk_{(SKP, \Gamma CP)}$를 출력하는 확률적 알고리즘이다.

[0186] (Enc)

[0187] Enc 알고리즘은, 메시지 m과, 속성의 집합인 $\Gamma^{KP}:=\{(t, \vec{x}_t^{KP}) \mid \vec{x}_t^{KP} \in F_q^{ntKP} \setminus \{\vec{0}\}, 1td^{KP}\}$와, 액세스 스트럭쳐 $S^{CP}:=(M^{CP}, \rho^{CP})$와, 공개 파라미터 pk를 입력으로 하여, 암호화 데이터 $ct_{(\Gamma KP, SCP)}$를 출력하는 확률적 알고리즘이다.

[0188] (Dec)

[0189] Dec 알고리즘은, 속성의 집합 및 액세스 스트럭쳐(Γ^{KP}, S^{CP})의 아래에서 암호화된 암호화 데이터 $ct_{(\Gamma KP, SCP)}$와, 액세스 스트럭쳐 및 속성의 집합(S^{KP}, Γ^{CP})에 대한 복호 키 $sk_{(SKP, \Gamma CP)}$와, 공개 파라미터 pk를 입력으로 하여, 메시지 m(평문 정보), 또는, 식별 정보 $\perp$를 출력하는 알고리즘이다.

[0190] Unified-Policy 함수형 암호 방식은, 수학식 124에 나타내는 모든 공개 파라미터 pk 및 마스터 키 sk와, 모든 액세스 스트럭쳐 S^{KP}와, 모든 속성의 집합 Γ^{CP}와, 수학식 125에 나타내는 모든 복호 키 $sk_{(SKP, \Gamma CP)}$와, 모든 메시지 m과, 모든 속성의 집합 Γ^{KP}와, 모든 액세스 스트럭쳐 S^{CP}와, 수학식 126에 나타내는 모든 암호화 데이터 $ct_{(\Gamma KP, SCP)}$에 대하여, 액세스 스트럭쳐 S^{KP}가 속성의 집합 Γ^{KP}를 수리하고, 또한, 액세스 스트럭쳐 S^{CP}가 속성의 집합 Γ^{CP}를 수리하는 경우, 압도적인 확률로 $m=Dec(pk, sk_{(SKP, \Gamma CP)}, ct_{(\Gamma KP, SCP)})$이다. 다시 말해, 공개 파라미터 pk와, 복호 키 $sk_{(SKP, \Gamma CP)}$와, 암호화 데이터 $ct_{(\Gamma KP, SCP)}$를 입력으로 하여 Dec 알고리즘을 실행하는 것에 의해, 메시지 m을 얻을 수 있다.

[0191] [수학식 124]

[0192] $$(pk, sk) \xleftarrow{R} Setup(1^{\lambda}, \vec{n})$$

[0193] [수학식 125]

[0194] $$sk_{(\mathbb{S}^{KP}, \Gamma^{CP})} \xleftarrow{R} KeyGen(pk, sk, \mathbb{S}^{KP}, \Gamma^{CP})$$

[0195] [수학식 126]

[0196] $$ct_{(\Gamma^{KP}, \mathbb{S}^{CP})} \xleftarrow{R} Enc(pk, m, \Gamma^{KP}, \mathbb{S}^{CP})$$

[0197] <제 4-2. 암호 처리 시스템(10)>

[0198] 상술한 Unified-Policy 함수형 암호 방식의 알고리즘을 실행하는 암호 처리 시스템(10)에 대하여 설명한다.

[0199] 도 5는, Unified-Policy 함수형 암호 방식을 실행하는 암호 처리 시스템(10)의 구성도이다.

[0200] 암호 처리 시스템(10)은, 키 생성 장치(100), 암호화 장치(200), 복호 장치(300)를 구비한다.

[0201] 키 생성 장치(100)는, 시큐리티 파라미터 λ와, 속성의 포맷 $\vec{n}:=((d^{KP}; n_t^{KP}, u_t^{KP}, w_t^{KP}, z_t^{KP}(t=1, \cdots, d^{KP})), (d^{CP}; n_t^{CP}, u_t^{CP}, w_t^{CP}, z_t^{CP}(t=1, \cdots, d^{CP})))$를 입력으로 하여 Setup 알고리즘을 실행하여, 공개 파라미터 pk와 마스터 키 sk를 생성한다. 그리고, 키 생성 장치(100)는, 생성한 공개 파라미터 pk를 공개한다. 또한, 키 생성 장치(100)는, 액세스 스트럭쳐 S^{KP}와, 속성의 집합 Γ^{CP}와, 공개 파라미터 pk와, 마스터 키 sk를 입력으로 하여

KeyGen 알고리즘을 실행하여, 복호 키 $sk_{(SKP,\ \Gamma CP)}$를 생성하여 복호 장치(300)에 비밀리에 배포한다.

[0202] 암호화 장치(200)는, 메시지 m과, 속성의 집합 Γ^{KP}와, 액세스 스트럭쳐 S^{CP}와, 공개 파라미터 pk를 입력으로 하여 Enc 알고리즘을 실행하여, 암호화 데이터 $ct_{(\Gamma KP,\ SCP)}$를 생성한다. 암호화 장치(200)는, 생성한 암호화 데이터 $ct_{(\Gamma KP,\ SCP)}$를 복호 장치(300)에 송신한다.

[0203] 복호 장치(300)는, 공개 파라미터 pk와, 복호 키 $sk_{(SKP,\ \Gamma CP)}$와, 암호화 데이터 $ct_{(\Gamma KP,\ SCP)}$를 입력으로 하여 Dec 알고리즘을 실행하여, 메시지 m 또는 식별 정보 $\perp$를 출력한다.

[0204] <제 4-3. Unified-Policy 함수형 암호 방식 및 암호 처리 시스템(10)의 상세>

[0205] 도 6으로부터 도 12에 근거하여, Unified-Policy 함수형 암호 방식, 및, Unified-Policy 함수형 암호 방식을 실행하는 암호 처리 시스템(10)의 기능과 동작에 대하여 설명한다.

[0206] 도 6은, 키 생성 장치(100)의 기능을 나타내는 기능 블록도이다. 도 7은, 암호화 장치(200)의 기능을 나타내는 기능 블록도이다. 도 8은, 복호 장치(300)의 기능을 나타내는 기능 블록도이다.

[0207] 도 9와 도 10은, 키 생성 장치(100)의 동작을 나타내는 플로차트이다. 또, 도 9는 Setup 알고리즘의 처리를 나타내는 플로차트이고, 도 10은 KeyGen 알고리즘의 처리를 나타내는 플로차트이다. 도 11은, 암호화 장치(200)의 동작을 나타내는 플로차트이고, Enc 알고리즘의 처리를 나타내는 플로차트이다. 도 12는, 복호 장치(300)의 동작을 나타내는 플로차트이고, Dec 알고리즘의 처리를 나타내는 플로차트이다.

[0208] 또, 여기서는, $x_{t,1}^{KP}$:=1, $x_{t,1}^{CP}$:=1로 정규화한다. 또, $x_{t,1}^{KP}$ 및 $x_{t,1}^{CP}$가 정규화되어 있지 않은 경우, $(1/x_{t,1}^{KP})\cdot x_{t,1}^{KP}$, 및, $(1/x_{t,1}^{CP})\cdot x_{t,1}^{CP}$로서 정규화하면 된다. 이 경우, $x_{t,i}^{KP}$ 및 $x_{t,i}^{CP}$는 0이 아닌 것으로 한다.

[0209] 키 생성 장치(100)의 기능과 동작에 대하여 설명한다.

[0210] 도 6에 나타내는 바와 같이, 키 생성 장치(100)는, 마스터 키 생성부(110), 마스터 키 기억부(120), 정보 입력부(130)(제 1 정보 입력부), 복호 키 생성부(140), 키 배포부(150)를 구비한다.

[0211] 또한, 정보 입력부(130)는, KP 정보 입력부(131)(제 1 KP 정보 입력부), CP 정보 입력부(132)(제 1 CP 정보 입력부)를 구비한다. 또한, 복호 키 생성부(140)는, f 벡터 생성부(141), s 벡터 생성부(142), 난수 생성부(143), 주 복호 키 생성부(144), KP 복호 키 생성부(145), CP 복호 키 생성부(146)를 구비한다.

[0212] 우선, 도 9에 근거하여, Setup 알고리즘의 처리에 대하여 설명한다.

[0213] (S101 : 정규 직교 기저 생성 단계)

[0214] 마스터 키 생성부(110)는, 처리 장치에 의해, 수학식 127을 계산하여, $param_{n\rightarrow}$와, 기저 B_0 및 기저 B^*_0과, t=1, …, d^{KP}의 각 정수 t에 대하여 기저 B_t^{KP} 및 기저 B^*_{tKP}와, t=1, …, d^{CP}의 각 정수 t에 대하여 기저 B_t^{CP} 및 기저 B^{*CP}_t를 랜덤 생성한다.

[0215] [수학식 127]

$$\mathcal{G}_{ob}^{up}(1^{\lambda},\vec{n}:=((d^{KP};n_t^{KP},u_t^{KP},w_t^{KP},z_t^{KP}\,(t=1,\ldots,d^{KP})),$$
$$(d^{CP};n_t^{CP},u_t^{CP},w_t^{CP},z_t^{CP}\,(t=1,\ldots,d^{CP}))):$$
$$\mathrm{param}_{\mathbb{G}}:=(q,\mathbb{G},\mathbb{G}_T,g,e)\xleftarrow{R}\mathcal{G}_{bpg}(1^{\lambda}),\quad \psi\xleftarrow{U}\mathbb{F}_q^{X},$$
$$N_0:=2+u_0+1+w_0+z_0,$$
$$N_t^{KP}:=n_t^{KP}+u_t^{KP}+w_t^{KP}+z_t^{KP}\ \text{ for } t=1,\ldots,d^{KP},$$
$$N_t^{CP}:=n_t^{CP}+u_t^{CP}+w_t^{CP}+z_t^{CP}\ \text{ for } t=1,\ldots,d^{CP},$$
$$\mathrm{param}_{\mathbb{V}_0}:=(q,\mathbb{V}_0,\mathbb{G}_T,\mathbb{A}_0,e):=\mathcal{G}_{dpvs}(1^{\lambda},N_0,\mathrm{param}_{\mathbb{G}}),$$
$$X_0:=(\chi_{0,i,j})_{i,j}\xleftarrow{U}GL(N_0,\mathbb{F}_q),\quad (v_{0,i,j})_{i,j}:=\psi\cdot(X_0^{\mathrm{T}})^{-1},$$
$$b_{0,i}:=(\chi_{0,i,1},\ldots,\chi_{0,i,N_0})_{\mathbb{A}_0},\ \mathbb{B}_0:=(b_{0,1},\ldots,b_{0,N_0}),$$
$$b_{0,i}^{*}:=(v_{0,i,1},\ldots,v_{0,i,N_0})_{\mathbb{A}_0},\ \mathbb{B}_0^{*}:=(b_{0,i}^{*},\ldots,b_{0,N_0}^{*}),$$
$$\text{for } t=1,\ldots,d^{KP},$$
$$\mathrm{param}_{\mathbb{V}_t^{KP}}:=(q,\mathbb{V}_t^{KP},\mathbb{G}_T,\mathbb{A}_t^{KP},e):=\mathcal{G}_{dpvs}(1^{\lambda},N_t^{KP},\mathrm{param}_{\mathbb{G}}),$$
$$X_t^{KP}:=(\chi_{t,i,j}^{KP})_{i,j}\xleftarrow{U}GL(N_t^{KP},\mathbb{F}_q),\quad (v_{t,i,j}^{KP})_{i,j}:=\psi\cdot((X_t^{KP})^{\mathrm{T}})^{-1},$$
$$b_{t,i}^{KP}:=(\chi_{t,i,1}^{KP},\ldots,\chi_{t,i,N_t^{KP}}^{KP})_{\mathbb{A}_t^{KP}},\ \mathbb{B}_t^{KP}:=(b_{t,1}^{KP},\ldots,b_{t,N_t^{KP}}^{KP}),$$
$$b_{t,i}^{*KP}:=(v_{t,i,1}^{KP},\ldots,v_{t,i,N_t^{KP}}^{KP})_{\mathbb{A}_t^{KP}},\ \mathbb{B}_t^{*KP}:=(b_{t,1}^{*KP},\ldots,b_{t,N_t^{KP}}^{*KP}),$$
$$\text{for } t=1,\ldots,d^{CP},$$
$$\mathrm{param}_{\mathbb{V}_t^{CP}}:=(q,\mathbb{V}_t^{CP},\mathbb{G}_T,\mathbb{A}_t^{CP},e):=\mathcal{G}_{dpvs}(1^{\lambda},N_t^{CP},\mathrm{param}_{\mathbb{G}}),$$
$$X_t^{CP}:=(\chi_{t,i,j}^{CP})_{i,j}\xleftarrow{U}GL(N_t^{CP},\mathbb{F}_q),\quad (v_{t,i,j}^{CP})_{i,j}:=\psi\cdot((X_t^{CP})^{\mathrm{T}})^{-1},$$
$$b_{t,i}^{CP}:=(\chi_{t,i,1}^{CP},\ldots,\chi_{t,i,N_t^{CP}}^{CP})_{\mathbb{A}_t^{CP}},\ \mathbb{B}_t^{CP}:=(b_{t,1}^{CP},\ldots,b_{t,N_t^{CP}}^{CP}),$$
$$b_{t,i}^{*CP}:=(v_{t,i,1}^{CP},\ldots,v_{t,i,N_t^{CP}}^{CP})_{\mathbb{A}_t^{CP}},\ \mathbb{B}_t^{*CP}:=(b_{t,1}^{*CP},\ldots,b_{t,N_t^{CP}}^{*CP}),$$
$$g_T:=e(g,g)^{\psi},$$
$$\mathrm{param}_{\vec{n}}:=(\mathrm{param}_{\mathbb{V}_0},\{\mathrm{param}_{\mathbb{V}_t^{KP}}\}_{t=1,\ldots,d^{KP}},\{\mathrm{param}_{\mathbb{V}_t^{CP}}\}_{t=1,\ldots,d^{CP}},g_T)$$
$$\text{return } (\mathrm{param}_{\vec{n}},\{\mathbb{B}_0,\mathbb{B}_0^{*}\},\{\mathbb{B}_t^{KP},\mathbb{B}_t^{*KP}\}_{t=1,\ldots,d^{KP}},\{\mathbb{B}_t^{CP},\mathbb{B}_t^{*CP}\}_{t=1,\ldots,d^{CP}})$$

[0216]

[0217] 다시 말해, 마스터 키 생성부(110)는 이하의 처리를 실행한다.

[0218] 우선, 마스터 키 생성부(110)는, 입력 장치에 의해, 시큐리티 파라미터 $\lambda(1^{\lambda})$와, 속성의 포맷 $\vec{n}:=((d^{KP};n_t^{KP},u_t^{KP},w_t^{KP},z_t^{KP}(t=1,\cdots,d^{KP})),(d^{CP};n_t^{CP},u_t^{CP},w_t^{CP},z_t^{CP}(t=1,\cdots,d^{CP})))$를 입력한다. 여기서, d^{KP}는 1 이상의 정수이고, t=1, …, d^{KP}까지의 각 정수 t에 대하여 n_t^{KP}, u_t^{KP}, w_t^{KP}, z_t^{KP}는 1 이상의 정수이다. 또한, d^{CP}는 1 이상의 정수이고, t=1, …, d^{CP}까지의 각 정수 t에 대하여 n_t^{CP}, u_t^{CP}, w_{tCP}, z_t^{CP}는 1 이상의 정수이다.

[0219] 다음으로, 마스터 키 생성부(110)는, 처리 장치에 의해, 수학식 128을 계산한다.

[0220] [수학식 128]

[0221] $$\mathrm{param}_{\mathbb{G}}:=(q,\mathbb{G},\mathbb{G}_T,g,e)\xleftarrow{R}\mathcal{G}_{bpg}(1^{\lambda})$$

[0222] 다시 말해, 마스터 키 생성부(110)는, 시큐리티 파라미터 $\lambda(1^{\lambda})$를 입력으로 하여 알고리즘 G_{bpg}를 실행하여, 쌍선형 페어링군의 파라미터 $\mathrm{param}_{\mathbb{G}}:=(q, G, G_T, g, e)$의 값을 생성한다.

[0223] 다음으로, 마스터 키 생성부(110)는, 처리 장치에 의해, 수학식 129를 계산한다.

[0224] [수학식 129]

$$\psi \xleftarrow{U} \mathbb{F}_q^X,$$
$$N_0 := 2+u_0+1+w_0+z_0,$$
$$N_t^{KP} := n_t^{KP}+u_t^{KP}+w_t^{KP}+z_t^{KP} \quad \text{for } t=1,\ldots,d^{KP},$$

[0225]
$$N_t^{CP} := n_t^{CP}+u_t^{CP}+w_t^{CP}+z_t^{CP} \quad \text{for } t=1,\ldots,d^{CP}$$

[0226] 다시 말해, 마스터 키 생성부(110)는, 난수 ψ를 생성한다. 또한, 마스터 키 생성부(110)는, N_0에 $2+u_0+1+w_0+z_0$을 설정하고, t=1, …, d^{KP}의 각 정수 t에 대하여 N_t^{KP}에 $n_{tKP}+u_{tKP}+w_t^{KP}+z_t^{KP}$를 설정하고, t=1, …, d^{CP}의 각 정수 t에 대하여 N_t^{CP}에 $n_t^{CP}+u_t^{CP}+w_{tCP}+z_t^{CP}$를 설정한다. 여기서, u_0, w_0, z_0은 1 이상의 정수이다.

[0227] 다음으로, 마스터 키 생성부(110)는, 처리 장치에 의해, 수학식 130을 계산한다.

[0228] [수학식 130]

$$\text{param}_{\mathbb{V}_0} := (q, \mathbb{V}_0, \mathbb{G}_T, \mathbb{A}_0, e) := \mathcal{G}_{\text{dpvs}}(1^\lambda, N_0, \text{param}_{\mathbb{G}}),$$
$$X_0 := (\chi_{0,i,j})_{i,j} \xleftarrow{U} GL(N_0, \mathbb{F}_q),$$
$$(\nu_{0,i,j})_{i,j} := \psi \cdot (X_0^{\mathrm{T}})^{-1},$$
$$b_{0,i} := (\chi_{0,i,1},\ldots,\chi_{0,i,N_0})_{\mathbb{A}_0},\ \mathbb{B}_0 := (b_{0,1},\ldots,b_{0,N_0}),$$

[0229]
$$b_{0,i}^* := (\nu_{0,i,1},\ldots,\nu_{0,i,N_0})_{\mathbb{A}_0},\ \mathbb{B}_0^* := (b_{0,i}^*,\ldots,b_{0,N_0}^*)$$

[0230] 다시 말해, 마스터 키 생성부(110)는, 입력한 시큐리티 파라미터 $\lambda(1^\lambda)$와, 설정한 N_0과, 생성한 $\text{param}_G := (q, G, G_T, g, e)$의 값을 입력으로 하여 알고리즘 G_{dpvs}를 실행하여, 쌍대 페어링 벡터 공간의 파라미터 $\text{param}_{V0} := (q, V_0, G_T, A_0, e)$의 값을 생성한다.

[0231] 또한, 마스터 키 생성부(110)는, 설정한 N_0과, F_q를 입력으로 하여, 선형 변환 $X_0 := (X_{0,i,j})_{i,j}$를 랜덤 생성한다. 또, GL은, General Linear의 약어이다. 다시 말해, GL은, 일반 선형군이고, 행렬식이 0이 아닌 정방행렬의 집합이고, 곱셈에 관한 군이다. 또한, $(X_{0,i,j})_{i,j}$는, 행렬 $X_{0,i,j}$의 첨자 i, j에 관한 행렬이라고 하는 의미이고, 여기서는, i, j=1, …, N_0이다.

[0232] 또한, 마스터 키 생성부(110)는, 난수 ψ와 선형 변환 X_0에 근거하여, $(v_{0,i,j})_{i,j} := \psi \cdot (X_0^{\mathrm{T}})^{-1}$을 생성한다. 또, $(v_{0,i,j})_{i,j}$도 $(X_{0,i,j})_{i,j}$와 같이, 행렬 $v_{0,i,j}$의 첨자 i, j에 관한 행렬이라고 하는 의미이고, 여기서는, i, j=1, …, N_0이다.

[0233] 그리고, 마스터 키 생성부(110)는, 선형 변환 X_0에 근거하여, 표준 기저 A_0으로부터 기저 B_0을 생성한다. 마찬가지로, 마스터 키 생성부(110)는, $(v_{0,i,j})_{i,j}$에 근거하여, 표준 기저 A_0으로부터 기저 B^*_0을 생성한다.

[0234] 다음으로, 마스터 키 생성부(110)는, 처리 장치에 의해, 수학식 131을 계산한다.

[0235] [수학식 131]

$$\text{for } t=1,\ldots,d^{KP},$$
$$\text{param}_{\mathbb{V}_t^{KP}} := (q, \mathbb{V}_t^{KP}, \mathbb{G}_T, \mathbb{A}_t^{KP}, e) := \mathcal{G}_{\text{dpvs}}(1^\lambda, N_t^{KP}, \text{param}_{\mathbb{G}}),$$
$$X_t^{KP} := (\chi_{t,i,j}^{KP})_{i,j} \xleftarrow{U} GL(N_t^{KP}, \mathbb{F}_q),$$
$$(\nu_{t,i,j}^{KP})_{i,j} := \psi \cdot ((X_t^{KP})^{\mathrm{T}})^{-1},$$
$$b_{t,i}^{KP} := (\chi_{t,i,1}^{KP},\ldots,\chi_{t,i,N_t^{KP}}^{KP})_{\mathbb{A}_t^{KP}},\ \mathbb{B}_t^{KP} := (b_{t,1}^{KP},\ldots,b_{t,N_t^{KP}}^{KP}),$$

[0236]
$$b_{t,i}^{*KP} := (\nu_{t,i,1}^{KP},\ldots,\nu_{t,i,N_t^{KP}}^{KP})_{\mathbb{A}_t^{KP}},\ \mathbb{B}_t^{*KP} := (b_{t,1}^{*KP},\ldots,b_{t,N_t^{KP}}^{*KP})$$

[0237] 다시 말해, 마스터 키 생성부(110)는, t=1, …, d^{KP}의 각 정수 t에 대하여 이하의 처리를 실행한다.

[0238] 마스터 키 생성부(110)는, 입력한 시큐리티 파라미터 $\lambda(1^{\lambda})$와, 설정한 N_t^{KP}와, 생성한 $param_G:=(q, G, G_T, g, e)$의 값을 입력으로 하여 알고리즘 G_{dpvs}를 실행하여, 쌍대 페어링 벡터 공간의 파라미터 $param_{VtKP}:=(q, V_t^{KP}, G_T, A_t^{KP}, e)$의 값을 생성한다.

[0239] 또한, 마스터 키 생성부(110)는, 설정한 N_t^{KP}와, F_q를 입력으로 하여, 선형 변환 $X_t^{KP}:=(X_{t,i,j}^{KP})_{i,j}$를 랜덤 생성한다. $(X_{t,i,j}^{KP})_{i,j}$는, 행렬 $X_{t,i,j}^{KP}$의 첨자 i, j에 관한 행렬이라고 하는 의미이고, 여기서는, i, j=1, …, N_{tKP}이다.

[0240] 또한, 마스터 키 생성부(110)는, 난수 ψ와 선형 변환 X_t^{KP}에 근거하여, $(v_{t,i,j}^{KP})_{i,j}:=\psi\cdot((X_t^{KP})^T)^{-1}$을 생성한다. 또, $(v_{t,i,j}^{KP})_{i,j}$도 $(X_{t,i,j}^{KP})_{i,j}$와 같이, 행렬 $v_{t,i,j}^{KP}$의 첨자 i, j에 관한 행렬이라고 하는 의미이고, 여기서는, i, j=1, …, N_t^{KP}이다.

[0241] 그리고, 마스터 키 생성부(110)는, 선형 변환 X_t^{KP}에 근거하여, 표준 기저 A_t^{KP}로부터 기저 B_t^{KP}를 생성한다. 마찬가지로, 마스터 키 생성부(110)는, $(v_{t,i,j}^{KP})_{i,j}$에 근거하여, 표준 기저 A_t^{KP}로부터 기저 B_{*t}^{KP}를 생성한다.

[0242] 다음으로, 마스터 키 생성부(110)는, 처리 장치에 의해, 수학식 132를 계산한다.

[0243] [수학식 132]

[0244]
$$\begin{aligned}
&\text{for } t=1,\ldots,d^{CP},\\
&\mathbf{param}_{\mathbb{V}_t^{CP}} := (q,\mathbb{V}_t^{CP},\mathbb{G}_T,\mathbb{A}_t^{CP},e) := \mathcal{G}_{\mathbf{dpvs}}(1^{\lambda},N_t^{CP},\mathbf{param}_{\mathbb{G}}),\\
&X_t^{CP} := (\chi_{t,i,j}^{CP})_{i,j} \xleftarrow{U} GL(N_t^{CP},\mathbb{F}_q),\\
&(\nu_{t,i,j}^{CP})_{i,j} := \psi\cdot((X_t^{CP})^{T})^{-1},\\
&b_{t,i}^{CP} := (\chi_{t,i,1}^{CP},\ldots,\chi_{t,i,N_t^{CP}}^{CP})_{\mathbb{A}_t^{CP}},\ \mathbb{B}_t^{CP} := (b_{t,1}^{CP},\ldots,b_{t,N_t^{CP}}^{CP}),\\
&b_{t,i}^{*CP} := (\nu_{t,i,1}^{CP},\ldots,\nu_{t,i,N_t^{CP}}^{CP})_{\mathbb{A}_t^{CP}},\ \mathbb{B}_t^{*CP} := (b_{t,1}^{*CP},\ldots,b_{t,N_t^{CP}}^{*CP})
\end{aligned}$$

[0245] 다시 말해, 마스터 키 생성부(110)는, t=1, …, d^{CP}의 각 정수 t에 대하여 이하의 처리를 실행한다.

[0246] 마스터 키 생성부(110)는, 입력한 시큐리티 파라미터 $\lambda(1^{\lambda})$와, 설정한 N_t^{CP}와, 생성한 $param_G:=(q, G, G_T, g, e)$의 값을 입력으로 하여 알고리즘 G_{dpvs}를 실행하여, 쌍대 페어링 벡터 공간의 파라미터 $param_{VtCP}:=(q, V_t^{CP}, G_T, A_t^{CP}, e)$의 값을 생성한다.

[0247] 또한, 마스터 키 생성부(110)는, 설정한 N_t^{CP}와, F_q를 입력으로 하여, 선형 변환 $X_t^{CP}:=(X_{t,i,j}^{CP})_{i,j}$를 랜덤 생성한다. $(X_{t,i,j}^{CP})_{i,j}$는, 행렬 $X_{t,i,j}^{CP}$의 첨자 i, j에 관한 행렬이라고 하는 의미이고, 여기서는, i, j=1, …, N_t^{CP}이다.

[0248] 또한, 마스터 키 생성부(110)는, 난수 ψ와 선형 변환 X_t^{CP}에 근거하여, $(v_{t,i,j}^{CP})_{i,j}:=\psi\cdot((X_t^{CP})^T)^{-1}$을 생성한다. 또, $(v_{t,i,j}^{CP})_{i,j}$도 $(X_{t,i,j}^{CP})_{i,j}$와 같이, 행렬 $v_{t,i,j}^{CP}$의 첨자 i, j에 관한 행렬이라고 하는 의미이고, 여기서는, i, j=1, …, N_t^{CP}이다.

[0249] 그리고, 마스터 키 생성부(110)는, 선형 변환 X_t^{CP}에 근거하여, 표준 기저 A_t^{CP}로부터 기저 B_t^{CP}를 생성한다. 마

찬가지로, 마스터 키 생성부(110)는, $(v_t^{CP}{}_{,i,j})_{i,j}$에 근거하여, 표준 기저 A_t^{CP}로부터 기저 B_t^{*CP}를 생성한다.

[0250] 다음으로, 마스터 키 생성부(110)는, 처리 장치에 의해, 수학식 133을 계산한다.

[0251] [수학식 133]

[0252]
$$g_T := e(g,g)^{\psi},$$
$$\mathrm{param}_{\vec{n}} := (\mathrm{param}_{\mathbb{V}_0}, \{\mathrm{param}_{\mathbb{V}_t^{KP}}\}_{t=1,\ldots,d^{KP}}, \{\mathrm{param}_{\mathbb{V}_t^{CP}}\}_{t=1,\ldots,d^{CP}}, g_T)$$

[0253] 다시 말해, 마스터 키 생성부(110)는, g_T에 $e(g, g)^{\psi}$를 설정한다.

[0254] 또한, 마스터 키 생성부(110)는, $\mathrm{param}_{\vec{n}}$에 param_{V0}과, t=1, …, d^{KP}의 각 정수 t에 대한 param_{VtKP}와, t=1, …, d^{CP}의 각 정수 t에 대한 param_{VtCP}와, g_T를 설정한다. 또, i=1, …, N_0의 각 정수 i에 대하여, $g_T=e(b_{0,i}, b^{*}_{0,i})$이다. 또한, t=1, …, d^{KP}와 i=1, …, N_t^{KP}의 각 정수 t, i에 대하여, $g_T=e(b_{t,i}, b^{*}_{t,i})$이다. 또한, t=1, …, d^{CP}와 i=1, …, N_t^{CP}의 각 정수 t, i에 대하여, $g_T=e(b_{t,i}, b^{*}_{t,i})$이다.

[0255] 그리고, 마스터 키 생성부(110)는, $\mathrm{param}_{\vec{n}}$와, $\{B_0, B^{*}_0\}$과, t=1, …, d^{KP}의 각 정수 t에 대한 $\{B_t^{KP}, B_t^{*KP}\}$와, t=1, …, d^{CP}의 각 정수 t에 대한 $\{B_t^{CP}, B_t^{*CP}\}$를 얻는다.

[0256] (S102 : 공개 파라미터 생성 단계)

[0257] 마스터 키 생성부(110)는, 처리 장치에 의해, 기저 B_0의 부분 기저 $\hat{B}_0$과, t=1, …, d^{KP}의 각 정수 t에 대하여, 기저 B_t^{KP}의 부분 기저 $\hat{B}_t^{KP}$와, t=1, …, d^{CP}의 각 정수 t에 대하여, 기저 B_t^{CP}의 부분 기저 $\hat{B}_t^{CP}$를 수학식 134에 나타내는 바와 같이 생성한다.

[0258] [수학식 134]

[0259]
$$\hat{\mathbb{B}}_0 := (b^*_{0,1}, b^*_{0,2}, b^*_{0,2+u_0+1}, b^*_{0,2+u_0+1+w_0+1}, \ldots, b^*_{0,2+u_0+1+w_0+z_0}),$$
$$\text{for } t = 1,\ldots,d^{KP},$$
$$\hat{\mathbb{B}}_t^{KP} := (b^{KP}_{t,1}, \ldots, b^{KP}_{t,n_t^{KP}}, b^{KP}_{t,n_t^{KP}+u_t^{KP}+w_t^{KP}+1}, \ldots, b^{KP}_{t,n_t^{KP}+u_t^{KP}+w_t^{KP}+z_t^{KP}}),$$
$$\text{for } t = 1,\ldots,d^{CP},$$
$$\hat{\mathbb{B}}_t^{CP} := (b^{CP}_{t,1}, \ldots, b^{CP}_{t,n_t^{CP}}, b^{CP}_{t,n_t^{CP}+u_t^{CP}+w_t^{CP}+1}, \ldots, b^{CP}_{t,n_t^{CP}+u_t^{CP}+w_t^{CP}+z_t^{CP}})$$

[0260] 마스터 키 생성부(110)는, 생성한 부분 기저 $\hat{B}_0$, 부분 기저 $\hat{B}_t^{KP}$, 부분 기저 $\hat{B}_t^{CP}$와, (S101)에서 입력된 시큐리티 파라미터 $\lambda(1^{\lambda})$와, (S101)에서 생성한 $\mathrm{param}_{\vec{n}}$를 합쳐, 공개 파라미터 pk로 한다.

[0261] (S103 : 마스터 키 생성 단계)

[0262] 마스터 키 생성부(110)는, 처리 장치에 의해, 기저 B_{*0}의 부분 기저 $\hat{B}^{*}_0$과, t=1, …, d^{KP}의 각 정수 t에 대하여, 기저 B_{*t}^{KP}의 부분 기저 $\hat{B}^{*KP}_t$와, t=1, …, d^{CP}의 각 정수 t에 대하여, 기저 B_t^{*CP}의 부분 기저 $\hat{B}^{*CP}_t$를 수학식 135에 나타내는 바와 같이 생성한다.

[0263] [수학식 135]

$$\hat{\mathbb{B}}_0^* := (b_{0,1}^*, b_{0,2}^*, b_{0,2+u_0+1}^*, b_{0,2+u_0+1+1}^*, \ldots, b_{0,2+u_0+1+w_0}^*),$$
$$\text{for } t = 1, \ldots, d^{KP},$$
$$\hat{\mathbb{B}}_t^{*KP} := (b_{t,1}^{*KP}, \ldots, b_{t,n_t^{KP}}^{*KP}, b_{t,n_t^{KP}+u_t^{KP}+1}^{*KP}, \ldots, b_{t,n_t^{KP}+u_t^{KP}+w_t^{KP}}^{*KP}),$$
$$\text{for } t = 1, \ldots, d^{CP},$$
$$\hat{\mathbb{B}}_t^{*CP} := (b_{t,1}^{*CP}, \ldots, b_{t,n_t^{CP}}^{*CP}, b_{t,n_t^{CP}+u_t^{CP}+1}^{*CP}, \ldots, b_{t,n_t^{CP}+u_t^{CP}+w_t^{CP}}^{*CP})$$

[0264]

[0265] 마스터 키 생성부(110)는, 생성한 부분 기저 $\hat{B}^*_0$, 부분 기저 $\hat{B}^{*KP}_t$, 부분 기저 $\hat{B}^{*CP}_t$를 마스터 키 sk로 한다.

[0266] (S104 : 마스터 키 기억 단계)

[0267] 마스터 키 기억부(120)는, (S102)에서 생성한 공개 파라미터 pk를 기억 장치에 기억한다. 또한, 마스터 키 기억부(120)는, (S103)에서 생성한 마스터 키 sk를 기억 장치에 기억한다.

[0268] 다시 말해, (S101)로부터 (S103)에 있어서, 키 생성 장치(100)는 수학식 136에 나타내는 Setup 알고리즘을 실행하여, 공개 파라미터 pk와 마스터 키 sk를 생성한다. 그리고, (S104)에서, 키 생성 장치(100)는 생성된 공개 파라미터 pk와 마스터 키 sk를 기억 장치에 기억한다.

[0269] 또, 공개 파라미터는, 예컨대, 네트워크를 통해 공개되고, 암호화 장치(200)나 복호 장치(300)가 취득 가능한 상태가 된다.

[0270] [수학식 136]

$$\mathsf{Setup}(1^\lambda, \vec{n} := ((d^{KP}; n_t^{KP}, u_t^{KP}, w_t^{KP}, z_t^{KP}\,(t = 1, \ldots, d^{KP})),$$
$$(d^{CP}; n_t^{CP}, u_t^{CP}, w_t^{CP}, z_t^{CP}\,(t = 1, \ldots, d^{CP}))):$$
$$(\mathsf{param}_{\vec{n}}, \mathbb{B}_0, \mathbb{B}_0^*, \{\mathbb{B}_t^{KP}, \mathbb{B}_t^{*KP}\}_{t=1,\ldots,d^{KP}},$$
$$\{\mathbb{B}_t^{CP}, \mathbb{B}_t^{*CP}\}_{t=1,\ldots,d^{CP}}) \xleftarrow{R} \mathcal{G}_{ob}(1^\lambda, \vec{n}),$$
$$\hat{\mathbb{B}}_0 := (b_{0,1}^*, b_{0,2}^*, b_{0,2+u_0+1}^*, b_{0,2+u_0+1+w_0+1}^*, \ldots, b_{0,2+u_0+1+w_0+z_0}^*),$$
$$\hat{\mathbb{B}}_0^* := (b_{0,1}^*, b_{0,2}^*, b_{0,2+u_0+1}^*, b_{0,2+u_0+1+1}^*, \ldots, b_{0,2+u_0+1+w_0}^*),$$
$$\text{for } t = 1, \ldots, d^{KP},$$
$$\hat{\mathbb{B}}_t^{KP} := (b_{t,1}^{KP}, \ldots, b_{t,n_t^{KP}}^{KP}, b_{t,n_t^{KP}+u_t^{KP}+w_t^{KP}+1}^{KP}, \ldots, b_{t,n_t^{KP}+u_t^{KP}+w_t^{KP}+z_t^{KP}}^{KP}),$$
$$\hat{\mathbb{B}}_t^{*KP} := (b_{t,1}^{*KP}, \ldots, b_{t,n_t^{KP}}^{*KP}, b_{t,n_t^{KP}+u_t^{KP}+1}^{*KP}, \ldots, b_{t,n_t^{KP}+u_t^{KP}+w_t^{KP}}^{*KP}),$$
$$\text{for } t = 1, \ldots, d^{CP},$$
$$\hat{\mathbb{B}}_t^{CP} := (b_{t,1}^{CP}, \ldots, b_{t,n_t^{CP}}^{CP}, b_{t,n_t^{CP}+u_t^{CP}+w_t^{CP}+1}^{CP}, \ldots, b_{t,n_t^{CP}+u_t^{CP}+w_t^{CP}+z_t^{CP}}^{CP}),$$
$$\hat{\mathbb{B}}_t^{*CP} := (b_{t,1}^{*CP}, \ldots, b_{t,n_t^{CP}}^{*CP}, b_{t,n_t^{CP}+u_t^{CP}+1}^{*CP}, \ldots, b_{t,n_t^{CP}+u_t^{CP}+w_t^{CP}}^{*CP}),$$
$$\mathsf{pk} := (1^\lambda, \mathsf{param}_{\vec{n}}, \hat{\mathbb{B}}_0, \{\hat{\mathbb{B}}_t^{KP}\}_{t=1,\ldots,d^{KP}}, \{\hat{\mathbb{B}}_t^{CP}\}_{t=1,\ldots,d^{CP}}),$$
$$\mathsf{sk} := (\hat{\mathbb{B}}_0^*, \{\hat{\mathbb{B}}_t^{*KP}\}_{t=1,\ldots,d^{KP}}, \{\hat{\mathbb{B}}_t^{*CP}\}_{t=1,\ldots,d^{CP}})$$
$$\mathsf{return}\ \mathsf{pk}, \mathsf{sk}$$

[0271]

[0272] 다음으로, 도 10에 근거하여, KeyGen 알고리즘의 처리에 대하여 설명한다.

[0273] (S201 : 정보 입력 단계)

[0274] 제 1 KP 정보 입력부(131)는, 입력 장치에 의해, 액세스 스트럭처 $S^{KP} := (M^{KP}, \rho^{KP})$를 입력한다. 또, 행렬 M^{KP}는, L^{KP}행×r^{KP}열의 행렬이다. L^{KP}, r^{KP}는, 1 이상의 정수이다.

[0275] 또한, 제 1 CP 정보 입력부(132)는, 입력 장치에 의해, 속성의 집합 $\Gamma^{CP} := \{(t, \vec{x}_t^{CP} := (x_{t,i}^{CP}\,(i=1, \cdots, n_t^{CP})) \in F_q^{n_t^{CP}} \setminus \{\vec{0}\}) \mid 1 t d^{CP}\}$를 입력한다. t는, 1 이상 d^{CP} 이하의 모든 정수는 아니고, 1 이상 d^{CP} 이하의 적어도 일부

의 정수이더라도 좋다.

[0276] 또, 액세스 스트럭쳐 S^{KP}의 행렬 $\mathbb{M}^{KP}$의 설정에 대해서는, 실현하고 싶은 시스템의 조건에 따라 설정되는 것이다. 또한, 액세스 스트럭쳐 S^{KP}의 ρ^{KP}나 속성의 집합 Γ^{CP}는, 예컨대, 복호 키 $sk_{(SKP,\ \Gamma CP)}$의 사용자의 속성 정보가 설정되어 있다.

[0277] (S202 : f 벡터 생성 단계)

[0278] f 벡터 생성부(141)는, 처리 장치에 의해, r^{KP}개의 요소를 갖는 벡터 $f^{\rightarrow KP}$를 수학식 137에 나타내는 바와 같이 랜덤 생성한다.

[0279] [수학식 137]

[0280] $$\vec{f}^{\mathsf{KP}} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{r^{\mathsf{KP}}}$$

[0281] (S203 : s 벡터 생성 단계)

[0282] s 벡터 생성부(142)는, 처리 장치에 의해, (S201)에서 입력한 액세스 스트럭쳐 S^{KP}에 포함되는 (L^{KP}행×r^{KP}열)의 행렬 $\mathbb{M}^{KP}$와, (S202)에서 생성한 r^{KP}개의 요소를 갖는 벡터 $f^{\rightarrow KP}$에 근거하여, 벡터 $(s^{\rightarrow KP})^{T}$를 수학식 138에 나타내는 바와 같이 생성한다.

[0283] [수학식 138]

[0284] $$(\vec{s}^{\mathsf{KP}})^{\mathrm{T}} := (s_1^{\mathsf{KP}}, \ldots, s_{L^{\mathsf{KP}}}^{\mathsf{KP}})^{\mathrm{T}} := M^{\mathsf{KP}} \cdot (\vec{f}^{\mathsf{KP}})^{\mathrm{T}}$$

[0285] 또한, s 벡터 생성부(142)는, 처리 장치에 의해, (S202)에서 생성한 벡터 $f^{\rightarrow KP}$에 근거하여, 값 s_0^{KP}를 수학식 139에 나타내는 바와 같이 생성한다. 또, $1^{\rightarrow}$는, 모든 요소가 값 1인 벡터이다.

[0286] [수학식 139]

[0287] $$s_0^{\mathsf{KP}} := \vec{1} \cdot (\vec{f}^{\mathsf{KP}})^{\mathrm{T}}$$

[0288] (S204 : 난수 생성 단계)

[0289] 난수 생성부(143)는, 처리 장치에 의해, 난수 δ^{CP}와, Γ^{CP}에 포함되는 (t, $x^{\rightarrow CP}_t$)의 각 정수 t에 대하여 난수 $\eta^{\rightarrow CP}_t$와, 난수 $\eta^{\rightarrow}_0$을 수학식 140에 나타내는 바와 같이 생성한다.

[0290] [수학식 140]

[0291] $$\delta^{\mathsf{CP}} \xleftarrow{\mathsf{U}} \mathbb{F}_q,$$
$$\vec{\eta}_t^{\mathsf{CP}} := (\eta_{t,1}^{\mathsf{CP}}, \ldots, \eta_{t,w_t^{\mathsf{CP}}}^{\mathsf{CP}}) \xleftarrow{\mathsf{U}} \mathbb{F}_q^{w_t^{\mathsf{CP}}} \quad \text{such that } (t, \vec{x}_t^{\mathsf{CP}}) \in \Gamma^{\mathsf{CP}},$$
$$\vec{\eta}_0 := (\eta_{0,1}, \ldots, \eta_{0,w_0}) \xleftarrow{\mathsf{U}} \mathbb{F}_q^{w_0}$$

[0292] (S205 : 주 복호 키 생성 단계)

[0293] 주 복호 키 생성부(144)는, 처리 장치에 의해, 복호 키 $sk_{(SKP,\ \Gamma CP)}$의 요소인 주 복호 키 k^{*}_0을 수학식 141에 나타내는 바와 같이 생성한다.

[0294] [수학식 141]

[0295] $$k_0^* := (-s_0^{\mathsf{KP}}, \delta^{\mathsf{CP}}, \overbrace{0^{u_0}}^{u_0}, 1, \overbrace{\eta_{0,1}, \ldots, \eta_{0,w_0}}^{w_0}, \overbrace{0^{z_0}}^{z_0})_{\mathbb{B}_0^*}$$

[0296] 또, 상술한 바와 같이, 수학식 110에 나타내는 기저 B와 기저 B^{*}에 대하여, 수학식 111이다. 따라서, 수학식

141은, 이하와 같이, 기저 B^*_0의 기저 벡터의 계수가 설정되는 것을 의미한다. 여기서는, 표기를 간략화하여, 기저 벡터 $b^*_{0,i}$ 중, i의 부분만으로 기저 벡터를 특정한다. 예컨대, 기저 벡터 1이면, 기저 벡터 $b^*_{0,1}$을 의미한다. 또한, 기저 벡터 1, …, 3이면, 기저 벡터 $b^*_{0,1}$, …, $b^*_{0,3}$을 의미한다.

[0297] 기저 B^*_0의 기저 벡터 1의 계수로서 $-s_0^{KP}$가 설정된다. 기저 벡터 2의 계수로서 난수 δ^{CP}가 설정된다. 기저 벡터 2+1, …, $2+u_0$의 계수로서 0이 설정된다. 기저 벡터 $2+u_0+1$의 계수로서 1이 설정된다. 기저 벡터 $2+u_0+1+1$, …, $2+u_0+1+w_0$의 계수로서 난수 $\eta_{0,1}$, …, $\eta_{0,w0}$(여기서, w0은 w_0이다)이 설정된다. 기저 벡터 $2+u_0+1+w_0+1$, …, $2+u_0+1+w_0+z_0$의 계수로서 0이 설정된다.

[0298] (S206 : KP 복호 키 생성 단계)

[0299] KP 복호 키 생성부(145)는, 처리 장치에 의해, i=1, …, L^{KP}의 각 정수 i에 대하여, 복호 키 $sk_{(SKP,\ \Gamma CP)}$의 요소인 KP 복호 키 k^{*KP}_i를 수학식 142에 나타내는 바와 같이 생성한다.

[0300] [수학식 142]

$$\text{for } i=1,\ldots,L^{KP},$$

$$\text{if } \rho^{KP}(i)=(t,\vec{v}_i^{KP}:=(v_{i,1}^{KP},\ldots,v_{i,n_t^{KP}}^{KP})\in\mathbb{F}_q^{n_t^{KP}}\setminus\{\vec{0}\}),$$

$$\theta_i^{KP}\xleftarrow{U}\mathbb{F}_q,\ \vec{\eta}_i^{KP}:=(\eta_{i,1}^{KP},\ldots,\eta_{i,w_t^{KP}}^{KP})\xleftarrow{U}\mathbb{F}_q^{w_t^{KP}},$$

$$k_i^{*KP}:=(\overbrace{s_i^{KP}\vec{e}_{t,1}^{KP}+\theta_i^{KP}\vec{v}_i^{KP}}^{n_t^{KP}},\overbrace{0^{u_t^{KP}}}^{u_t^{KP}},\overbrace{\vec{\eta}_i^{KP}}^{w_t^{KP}},\overbrace{0^{z_t^{KP}}}^{z_t^{KP}})_{\mathbb{B}_t^{*KP}},$$

$$\text{if } \rho^{KP}(i)=\neg(t,\vec{v}_i^{KP}),$$

$$\vec{\eta}_i^{KP}:=(\eta_{i,1}^{KP},\ldots,\eta_{i,w_t^{KP}}^{KP})\xleftarrow{U}\mathbb{F}_q^{w_t^{KP}},$$

$$k_i^{*KP}:=(\overbrace{s_i^{KP}\vec{v}_i^{KP}}^{n_t^{KP}},\overbrace{0^{u_t^{KP}}}^{u_t^{KP}},\overbrace{\vec{\eta}_i^{KP}}^{w_t^{KP}},\overbrace{0^{z_t^{KP}}}^{z_t^{KP}})_{\mathbb{B}_t^{*KP}}$$

[0301]

[0302] 다시 말해, 수학식 142는, 수학식 141과 같이, 이하와 같이, 기저 B^{*KP}_t의 기저 벡터의 계수가 설정되는 것을 의미한다. 또, 여기서는, 표기를 간략화하여, 기저 벡터 $b^{*KP}_{t,i}$ 중, i의 부분만으로 기저 벡터를 특정한다. 예컨대, 기저 벡터 1이면, 기저 벡터 $b^{*KP}_{t,1}$를 의미한다. 또한, 기저 벡터 1, …, 3이면, 기저 벡터 $b^{*KP}_{t,1}$, …, $b^{*KP}_{t,3}$를 의미한다.

[0303] $\rho^{KP}(i)$가 긍정형의 조 $(t, \vec{v}^{KP}_i)$인 경우에는, 기저 벡터 1의 계수로서 $s_i^{KP}+\Theta_i^{KP}v_{i,1}^{KP}$가 설정된다. 또, 상술한 바와 같이, $\vec{e}^{KP}_{t,j}$는, 수학식 112에 나타내는 정규 기저 벡터를 나타낸다. 또한, 기저 벡터 2, …, n_t^{KP}의 계수로서 $\Theta_i^{KP}v_{i,2}^{KP}$, …, $\Theta_i^{KP}v_{i,ntKP}^{KP}$(여기서, ntKP는 n_t^{KP}이다)가 설정된다. 기저 벡터 $n_t^{KP}+1$, …, $n_t^{KP}+u_t^{KP}$의 계수로서 0이 설정된다. 기저 벡터 $n_t^{KP}+u_t^{KP}+1$, …, $n_t^{KP}+u_t^{KP}+w_t^{KP}$의 계수로서 $\eta_{i,1}^{KP}$, …, $\eta_{i,wtKP}^{KP}$(여기서, wtKP는 w_t^{KP}이다)가 설정된다. 기저 벡터 $n_t^{KP}+u_t^{KP}+w_t^{KP}+1$, …, $n_t^{KP}+u_t^{KP}+w_t^{KP}+z_t^{KP}$의 계수로서 0이 설정된다.

[0304] 한편, $\rho^{KP}(i)$가 부정형의 조 $\neg(t, \vec{v}^{KP}_i)$인 경우에는, 기저 벡터 1, …, n_t^{KP}의 계수로서 $s_i^{KP}v_{i,1}^{KP}$, …, $s_i^{KP}v_{i,ntKP}^{KP}$(여기서, ntKP는 n_t^{KP}이다)가 설정된다. 기저 벡터 $n_t^{KP}+1$, …, $n_t^{KP}+u_t^{KP}$의 계수로서 0이 설정된다. 기저 벡터 $n_t^{KP}+u_t^{KP}+1$, …, $n_t^{KP}+u_t^{KP}+w_t^{KP}$의 계수로서 $\eta_{i,1}^{KP}$, …, $\eta_{i,wtKP}^{KP}$(여기서, wtKP는 w_t^{KP}이다)가 설정된다. 기

저 벡터 $n_t^{KP}+u_t^{KP}+w_t^{KP}+1$, …, $n_t^{KP}+u_t^{KP}+w_t^{KP}+z_{tKP}$의 계수로서 0이 설정된다.

[0305] 또, Θ_i^{KP} 및 $\eta_i^{\rightarrow KP}$는 난수 생성부(143)에 의해 생성되는 난수이다.

[0306] (S207 : CP 복호 키 생성 단계)

[0307] CP 복호 키 생성부(146)는, 처리 장치에 의해, Γ^{CP}에 포함되는 (t, $x_{\rightarrow t}^{CP}$)의 각 정수 t에 대하여, 복호 키 $sk_{(SKP,\ \Gamma CP)}$의 요소인 CP 복호 키 k_t^{*CP}를 수학식 143에 나타내는 바와 같이 생성한다.

[0308] [수학식 143]

[0309] $$k_t^{*CP} := (\overbrace{\delta^{CP}\vec{x}_t^{CP}}^{n_t^{CP}}, \overbrace{0^{u_t^{CP}},}^{u_t^{CP}} \overbrace{\vec{\eta}_t^{CP}}^{w_t^{CP}}, \overbrace{0^{z_t^{KP}}}^{z_t^{CP}})_{\mathbb{B}_t^{*CP}} \quad \text{for } (t,\vec{x}_t^{CP}) \in \Gamma^{CP}$$

[0310] 다시 말해, 수학식 143은, 수학식 141과 같이, 이하와 같이, 기저 B_t^{*CP}의 기저 벡터의 계수가 설정되는 것을 의미한다. 또, 여기서는, 표기를 간략화하여, 기저 벡터 $b_{t,i}^{*CP}$ 중, i의 부분만으로 기저 벡터를 특정한다. 예컨대, 기저 벡터 1이면, 기저 벡터 $b_{t,1}^{*CP}$를 의미한다. 또한, 기저 벡터 1, …, 3이면, 기저 벡터 $b_{t,1}^{*CP}$, …, $b_{t,3}^{*CP}$를 의미한다.

[0311] 기저 벡터 1, …, n_t^{CP}의 계수로서 $\delta^{CP}x_{t,1}^{CP}$, …, $\delta^{CP}x_{t,ntCP}^{CP}$(여기서, ntCP는 n_t^{CP}이다)가 설정된다. 기저 벡터 $n_t^{CP}+1$, …, $n_t^{CP}+u_t^{CP}$의 계수로서 0이 설정된다. 기저 벡터 $n_t^{CP}+u_t^{CP}+1$, …, $n_t^{CP}+u_t^{CP}+w_t^{CP}$의 계수로서 $\eta_{t,1}^{CP}$, …, $\eta_{t,wtCP}^{CP}$(여기서, wtCP는 w_t^{CP}이다)가 설정된다. 기저 벡터 $n_t^{CP}+u_t^{CP}+w_t^{CP}+1$, …, $n_t^{CP}+u_t^{CP}+w_t^{CP}+z_t^{CP}$의 계수로서 0이 설정된다.

[0312] (S208 : 키 배포 단계)

[0313] 키 배포부(150)는, 주 복호 키 k_0^*과, 액세스 스트럭처 S^{KP} 및 KP 복호 키 k_i^{*KP}(i=1, …, L^{KP})와, 속성의 집합 Γ^{CP} 및 CP 복호 키 k_t^{*CP}(t는 속성의 집합 Γ^{CP}에 포함되는 (t, $x_t^{\rightarrow CP}$)에 있어서의 t)를 요소로 하는 복호 키 $sk_{(SKP,\ \Gamma CP)}$를, 예컨대 통신 장치에 의해 네트워크를 통해 비밀리에 복호 장치(300)에 배포한다. 물론, 복호 키 $sk_{(SKP,\ \Gamma CP)}$는, 다른 방법에 의해 복호 장치(300)에 배포되더라도 좋다.

[0314] 다시 말해, (S201)로부터 (S207)에 있어서, 키 생성 장치(100)는 수학식 144에 나타내는 KeyGen 알고리즘을 실행하여, 복호 키 $sk_{(SKP,\ \Gamma CP)}$를 생성한다. 그리고, (S208)에서, 키 생성 장치(100)는 생성된 복호 키 $sk_{(SKP,\ \Gamma CP)}$를 복호 장치(300)에 배포한다.

[0315] [수학식 144]

$$\mathsf{KeyGen}(\mathsf{pk},\mathsf{sk},\mathbb{S}^{\mathsf{KP}}:=(M^{\mathsf{KP}},\rho^{\mathsf{KP}}),$$

$$\Gamma^{\mathsf{CP}}:=\{(t,\vec{x}_t^{\mathsf{CP}}:=(x_{t,1}^{\mathsf{CP}},\ldots,x_{t,n_t^{\mathsf{CP}}}^{\mathsf{CP}})\in\mathbb{F}_q^{n_t^{\mathsf{CP}}}\setminus\{\vec{0}\})$$

$$\left|1\le t\le d^{\mathsf{CP}},x_{t,1}^{\mathsf{CP}}:=1\right\})$$

$$\vec{f}^{\mathsf{KP}}\xleftarrow{\mathsf{U}}\mathbb{F}_q^{r^{\mathsf{KP}}},\quad(\vec{s}^{\mathsf{KP}})^{\mathrm{T}}:=(s_1^{\mathsf{KP}},\ldots,s_{L^{\mathsf{KP}}}^{\mathsf{KP}})^{\mathrm{T}}:=M^{\mathsf{KP}}\cdot(\vec{f}^{\mathsf{KP}})^{\mathrm{T}},$$

$$s_0^{\mathsf{KP}}:=\vec{1}\cdot(\vec{f}^{\mathsf{KP}})^{\mathrm{T}},$$

$$\delta^{\mathsf{CP}}\xleftarrow{\mathsf{U}}\mathbb{F}_q,\quad\vec{\eta}_t^{\mathsf{CP}}\xleftarrow{\mathsf{U}}\mathbb{F}_q^{w_t^{\mathsf{CP}}}\ \text{ such that }(t,\vec{x}_t^{\mathsf{CP}})\in\Gamma^{\mathsf{CP}},$$

$$\vec{\eta}_0\xleftarrow{\mathsf{U}}\mathbb{F}_q^{w_0},$$

$$k_0^*:=(-s_0^{\mathsf{KP}},\delta^{\mathsf{CP}},\overbrace{0^{u_0}}^{u_0},1,\overbrace{\eta_{0,1},\ldots,\eta_{0,w_0}}^{w_0},\overbrace{0^{z_0}}^{z_0})_{\mathbb{B}_0^*},$$

$$\text{for } i=1,\ldots,L^{\mathsf{KP}},$$

$$\text{if }\rho^{\mathsf{KP}}(i)=(t,\vec{v}_i^{\mathsf{KP}}:=(v_{i,1}^{\mathsf{KP}},\ldots,v_{i,n_t^{\mathsf{KP}}}^{\mathsf{KP}})\in\mathbb{F}_q^{n_t^{\mathsf{KP}}}\setminus\{\vec{0}\}),$$

$$\theta_i^{\mathsf{KP}}\xleftarrow{\mathsf{U}}\mathbb{F}_q,\quad\vec{\eta}_i^{\mathsf{KP}}\xleftarrow{\mathsf{U}}\mathbb{F}_q^{w_t^{\mathsf{KP}}},$$

$$k_i^{*\mathsf{KP}}:=(\overbrace{s_i^{\mathsf{KP}}\vec{e}_{t,1}^{\mathsf{KP}}+\theta_i^{\mathsf{KP}}\vec{v}_i^{\mathsf{KP}}}^{n_t^{\mathsf{KP}}},\overbrace{0^{u_t^{\mathsf{KP}}}}^{u_t^{\mathsf{KP}}},\overbrace{\vec{\eta}_i^{\mathsf{KP}}}^{w_t^{\mathsf{KP}}},\overbrace{0^{z_t^{\mathsf{KP}}}}^{z_t^{\mathsf{KP}}})_{\mathbb{B}_t^{*\mathsf{KP}}},$$

$$\text{if }\rho^{\mathsf{KP}}(i)=\neg(t,\vec{v}_i^{\mathsf{KP}}),\quad\vec{\eta}_i^{\mathsf{KP}}\xleftarrow{\mathsf{U}}\mathbb{F}_q^{w_t^{\mathsf{KP}}},$$

$$k_i^{*\mathsf{KP}}:=(\overbrace{s_i^{\mathsf{KP}}\vec{v}_i^{\mathsf{KP}}}^{n_t^{\mathsf{KP}}},\overbrace{0^{u_t^{\mathsf{KP}}}}^{u_t^{\mathsf{KP}}},\overbrace{\vec{\eta}_i^{\mathsf{KP}}}^{w_t^{\mathsf{KP}}},\overbrace{0^{z_t^{\mathsf{KP}}}}^{z_t^{\mathsf{KP}}})_{\mathbb{B}_t^{*\mathsf{KP}}},$$

$$\text{for }(t,\vec{x}_t^{\mathsf{CP}})\in\Gamma^{\mathsf{CP}},$$

$$k_t^{*\mathsf{CP}}:=(\overbrace{\delta^{\mathsf{CP}}\vec{x}_t^{\mathsf{CP}}}^{n_t^{\mathsf{CP}}},\overbrace{0^{u_t^{\mathsf{CP}}}}^{u_t^{\mathsf{CP}}},\overbrace{\vec{\eta}_t^{\mathsf{CP}}}^{w_t^{\mathsf{CP}}},\overbrace{0^{z_t^{\mathsf{KP}}}}^{z_t^{\mathsf{CP}}})_{\mathbb{B}_t^{*\mathsf{CP}}},$$

$$\text{return }\mathsf{sk}_{(\mathbb{S}^{\mathsf{KP}},\Gamma^{\mathsf{CP}})}:=$$

$$(k_0^*;\mathbb{S}^{\mathsf{KP}},k_1^{*\mathsf{KP}},\ldots,k_{L^{\mathsf{KP}}}^{*\mathsf{KP}};\Gamma^{\mathsf{CP}},\{k_t^{*\mathsf{CP}}\}_{(t,\vec{x}_t^{\mathsf{CP}})\in\Gamma^{\mathsf{CP}}})$$

[0316]

[0317] 암호화 장치(200)의 기능과 동작에 대하여 설명한다.

[0318] 도 7에 나타내는 바와 같이, 암호화 장치(200)는, 공개 파라미터 취득부(210), 정보 입력부(220)(제 2 정보 입력부), 암호화 데이터 생성부(230), 데이터 송신부(240)(데이터 출력부)를 구비한다.

[0319] 또한, 정보 입력부(220)는, KP 정보 입력부(221)(제 2 KP 정보 입력부), CP 정보 입력부(222)(제 2 CP 정보 입력부), 메시지 입력부(223)를 구비한다. 또한, 암호화 데이터 생성부(230)는, f 벡터 생성부(231), s 벡터 생성부(232), 난수 생성부(233), 주 암호화 데이터 생성부(234), KP 암호화 데이터 생성부(235), CP 암호화 데이터 생성부(236), 메시지 암호화 데이터 생성부(237)를 구비한다.

[0320] 도 11에 근거하여, Enc 알고리즘의 처리에 대하여 설명한다.

[0321] (S301 : 공개 파라미터 취득 단계)

[0322] 공개 파라미터 취득부(210)는, 예컨대, 통신 장치에 의해 네트워크를 통해, 키 생성 장치(100)가 생성한 공개 파라미터 pk를 취득한다.

[0323] (S302 : 정보 입력 단계)

[0324] KP 정보 입력부(221)는, 입력 장치에 의해, 속성의 집합 $\Gamma^{KP}:=\{(t,\ \vec{x}_t^{KP}:=(x_{t,i}^{KP}(i=1,\ \cdots,\ n_t^{KP}))\in F_q^{ntKP}\setminus\{0\vec{}\})\mid 1td^{KP}\}$를 입력한다. t는, 1 이상 d^{KP} 이하의 모든 정수는 아니고, 1 이상 d^{KP} 이하의 적어도 일부의 정수이더라도 좋다.

[0325] 또한, CP 정보 입력부(222)는, 입력 장치에 의해, 액세스 스트럭쳐 $S^{CP}:=(M^{CP},\ \rho^{CP})$를 입력한다. 또, 행렬

M^{CP}는, L^{CP}행×r^{CP}열의 행렬이다. L^{CP}, r^{CP}는, 1 이상의 정수이다.

[0326] 또한, 메시지 입력부는, 입력 장치에 의해, 복호 장치(300)에 송신하는 메시지 m을 입력한다.

[0327] 또, 액세스 스트럭쳐 S^{CP}의 행렬 M^{CP}의 설정에 대해서는, 실현하고 싶은 시스템의 조건에 따라 설정되는 것이다. 액세스 스트럭쳐 S^{CP}의 ρ^{CP}나 속성의 집합 Γ^{KP}는, 예컨대, 복호 가능한 사용자의 속성 정보가 설정되어 있다.

[0328] (S303 : 난수 생성 단계)

[0329] 난수 생성부(233)는, 처리 장치에 의해, 난수 ω^{KP}와, 난수 $\vec{\phi}_0$과, Γ^{KP}에 포함되는 $(t, \vec{x}_t^{KP})$의 각 정수 t에 대하여 $\vec{\phi}_t^{KP}$와, 난수 ζ를 수학식 145에 나타내는 바와 같이 생성한다.

[0330] [수학식 145]

[0331]
$$\omega^{KP}, \zeta \xleftarrow{U} \mathbb{F}_q,$$
$$\vec{\varphi}_0 := (\varphi_{0,1}, \ldots, \varphi_{0,z_0}) \xleftarrow{U} \mathbb{F}_q^{z_0},$$
$$\vec{\varphi}_t^{KP} := (\varphi_{t,1}^{KP}, \ldots, \varphi_{t,z_t^{KP}}^{KP}) \xleftarrow{U} \mathbb{F}_q^{z_t^{KP}} \text{ for } (t, \vec{x}_t^{KP}) \in \Gamma$$

[0332] (S304 : f 벡터 생성 단계)

[0333] f 벡터 생성부(231)는, 처리 장치에 의해, r^{CP}개의 요소를 갖는 벡터 $\vec{f}^{CP}$를 수학식 146에 나타내는 바와 같이 랜덤 생성한다.

[0334] [수학식 146]

[0335]
$$\vec{f}^{CP} \xleftarrow{R} \mathbb{F}_q^{r^{CP}}$$

[0336] (S305 : s 벡터 생성 단계)

[0337] s 벡터 생성부(232)는, 처리 장치에 의해, (S302)에서 입력한 액세스 스트럭쳐 S^{CP}에 포함되는 (L^{CP}행×r^{CP}열)의 행렬 M^{CP}와, (S304)에서 생성한 r^{CP}개의 요소를 갖는 벡터 $\vec{f}^{CP}$에 근거하여, 벡터 $(\vec{s}^{CP})^T$를 수학식 147에 나타내는 바와 같이 생성한다.

[0338] [수학식 147]

[0339]
$$(\vec{s}^{CP})^T := (s_1^{CP}, \ldots, s_{L^{CP}}^{CP})^T := M^{CP} \cdot (\vec{f}^{CP})^T$$

[0340] 또한, s 벡터 생성부(232)는, 처리 장치에 의해, (S304)에서 생성한 벡터 $\vec{f}^{CP}$에 근거하여, 값 s_0^{CP}를 수학식 148에 나타내는 바와 같이 생성한다. 또, $\vec{1}$는, 모든 요소가 값 1인 벡터이다.

[0341] [수학식 148]

[0342]
$$s_0^{CP} := \vec{1} \cdot (\vec{f}^{CP})^T$$

[0343] (S306 : 주 암호화 데이터 생성 단계)

[0344] 주 암호화 데이터 생성부(234)는, 처리 장치에 의해, 암호화 데이터 $ct_{(\Gamma^{KP}, SCP)}$의 요소인 주 암호화 데이터 c0을 수학식 149에 나타내는 바와 같이 생성한다.

[0345] [수학식 149]

[0346]
$$c_0 := (\omega^{KP}, -s_0^{CP}, \overbrace{0^{u_0}, \ldots}^{u_0}, \zeta, \overbrace{0^{w_0}, \ldots}^{w_0}, \overbrace{\varphi_{0,1}, \ldots, \varphi_{0,z_0}}^{z_0})_{\mathbb{B}_0}$$

[0347] 또, 상술한 바와 같이, 수학식 110에 나타내는 기저 B와 기저 B^*에 대하여, 수학식 111이다. 따라서, 수학식

149는, 이하와 같이, 기저 B_0의 기저 벡터의 계수가 설정되는 것을 의미한다. 여기서는, 표기를 간략화하여, 기저 벡터 $b_{0,i}$ 중, i의 부분만으로 기저 벡터를 특정한다. 예컨대, 기저 벡터 1이면, 기저 벡터 $b_{0,1}$을 의미한다. 또한, 기저 벡터 1, …, 3이면, 기저 벡터 $b_{0,1}$, …, $b_{0,3}$을 의미한다.

[0348] 기저 B_0의 기저 벡터 1의 계수로서 난수 ω^{KP}가 설정된다. 기저 벡터 2의 계수로서 $-s_0^{CP}$가 설정된다. 기저 벡터 2+1, …, 2+u_0의 계수로서 0이 설정된다. 기저 벡터 2+u_0+1의 계수로서 난수 ζ가 설정된다. 기저 벡터 2+u_0+1+1, …, 2+u_0+1+w_0의 계수로서 0이 설정된다. 기저 벡터 2+u_0+1+w_0+1, …, 2+u_0+1+w_0+z_0의 계수로서 난수 $\phi_{0,1}$, …, $\phi_{0,z0}$(여기서, z0은 z_0이다)이 설정된다.

[0349] (S307 : KP 암호화 데이터 생성 단계)

[0350] KP 암호화 데이터 생성부(235)는, 처리 장치에 의해, Γ^{KP}에 포함되는 (t, $\vec{x}_t^{KP}$)의 각 정수 t에 대하여, 암호화 데이터 $ct_{(\Gamma KP,\ SCP)}$의 요소인 KP 암호화 데이터 c_t^{KP}를 수학식 150에 나타내는 바와 같이 생성한다.

[0351] [수학식 150]

$$c_t^{KP} := (\overbrace{\omega^{KP}\vec{x}_t^{KP}}^{n_t^{KP}}, \overbrace{0^{u_t^{KP}},}^{u_t^{KP}} \overbrace{0^{w_t^{KP}},}^{w_t^{KP}} \overbrace{\vec{\varphi}_t^{KP}}^{z_t^{KP}})_{\mathbb{B}_t^{KP}}$$

[0352] $$\text{for } (t, \vec{x}_t^{KP}) \in \Gamma^{KP}$$

[0353] 다시 말해, 수학식 150은, 수학식 149와 같이, 이하와 같이, 기저 B_t^{KP}의 기저 벡터의 계수가 설정되는 것을 의미한다. 또, 여기서는, 표기를 간략화하여, 기저 벡터 $b_{t,i}^{KP}$ 중, i의 부분만으로 기저 벡터를 특정한다. 예컨대, 기저 벡터 1이면, 기저 벡터 $b_{t,1}^{KP}$를 의미한다. 또한, 기저 벡터 1, …, 3이면, 기저 벡터 $b_{t,1}^{KP}$, …, $b_{t,3}^{KP}$를 의미한다.

[0354] 기저 벡터 1, …, n_t^{KP}의 계수로서 $\omega^{KP}x_{t,1}^{KP}$, …, $\omega^{KP}x_{t,ntKP}^{KP}$(여기서, ntKP는 n_t^{KP}이다)가 설정된다. 기저 벡터 n_t^{KP}+1, …, n_t^{KP}+u_t^{KP}+w_t^{KP}의 계수로서 0이 설정된다. 기저 벡터 n_t^{KP}+u_t^{KP}+w_t^{KP}+1, …, n_t^{KP}+u_t^{KP}+w_t^{KP}+z_t^{KP}의 계수로서 $\phi_{t,1}^{KP}$, …, $\phi_{t,ztKP}^{KP}$(여기서, ztKP는 z_t^{KP}이다)가 설정된다.

[0355] (S308 : CP 암호화 데이터 생성 단계)

[0356] CP 암호화 데이터 생성부(236)는, 처리 장치에 의해, i=1, …, L^{CP}의 각 정수 i에 대하여, 암호화 데이터 $ct_{(\Gamma KP,\ SCP)}$의 요소인 CP 암호화 데이터 c_i^{CP}를 수학식 151에 나타내는 바와 같이 생성한다.

[0357] [수학식 151]

$$\text{for } i = 1,\ldots,L^{CP},$$

$$\text{if } \rho^{CP}(i) = (t, \vec{v}_i^{CP} := (v_{i,1}^{CP},\ldots,v_{i,n_t^{CP}}^{CP}) \in \mathbb{F}_q^{n_t^{CP}} \setminus \{\vec{0}\})(v_{i,n_t^{CP}}^{CP} := 1),$$

$$\theta_i^{CP} \xleftarrow{U} \mathbb{F}_q\ ,\vec{\varphi}_i^{CP} := (\varphi_{i,0}^{CP},\ldots,\varphi_{i,z_t^{CP}}^{CP}) \xleftarrow{U} \mathbb{F}_q^{z_t^{CP}},$$

$$c_i^{CP} := (\overbrace{s_i^{CP}\vec{e}_{t,1}^{CP} + \theta_i^{CP}\vec{v}_i^{CP}}^{n_t^{CP}}, \overbrace{0^{u_t^{CP}},}^{u_t^{CP}} \overbrace{0^{w_t^{CP}},}^{w_t^{CP}} \overbrace{\vec{\varphi}_i^{CP}}^{z_t^{CP}})_{\mathbb{B}_t^{CP}},$$

$$\text{if } \rho^{CP}(i) = \neg(t, \vec{v}_i^{CP}),$$

$$\vec{\varphi}_i^{CP} := (\varphi_{i,0}^{CP},\ldots,\varphi_{i,z_t^{CP}}^{CP}) \xleftarrow{U} \mathbb{F}_q^{z_t^{CP}},$$

$$c_i^{CP} := (\overbrace{s_i^{CP}\vec{v}_i^{CP}}^{n_t^{CP}}, \overbrace{0^{u_t^{CP}},}^{u_t^{CP}} \overbrace{0^{w_t^{CP}},}^{w_t^{CP}} \overbrace{\vec{\varphi}_i^{CP}}^{z_t^{CP}})_{\mathbb{B}_t^{CP}}$$

[0358]

[0359] 다시 말해, 수학식 151은, 수학식 150과 같이, 이하와 같이, 기저 B_t^{CP}의 기저 벡터의 계수가 설정되는 것을 의미한다. 또, 여기서는, 표기를 간략화하여, 기저 벡터 $b_{t,i}^{CP}$ 중, i의 부분만으로 기저 벡터를 특정한다. 예컨대, 기저 벡터 1이면, 기저 벡터 $b_{t,1}^{CP}$를 의미한다. 또한, 기저 벡터 1, …, 3이면, 기저 벡터 $b_{t,1}^{CP}$, …, $b_{t,3}^{CP}$를 의미한다.

[0360] $\rho_{CP}(i)$가 긍정형의 조 $(t, \vec{v}_i^{CP})$인 경우에는, 기저 벡터 1의 계수로서 $s_i^{CP}+\theta_i^{CP}v_{i,1}^{CP}$가 설정된다. 또, 상술한 바와 같이, $\vec{e}_{t,j}^{CP}$는, 수학식 112에 나타내는 정규 기저 벡터를 나타낸다. 또한, 기저 벡터 2, …, n_t^{CP}의 계수로서 $\theta_i^{CP}v_{i,2}^{CP}$, …, $\theta_i^{CP}v_{i,ntCP}^{CP}$(여기서, ntCP는 n_t^{CP}이다)가 설정된다. 기저 벡터 $n_t^{CP}+1$, …, $n_t^{CP}+u_t^{CP}+w_t^{CP}$의 계수로서 0이 설정된다. 기저 벡터 $n_t^{CP}+u_t^{CP}+w_t^{CP}+1$, …, $n_t^{CP}+u_t^{CP}+w_t^{CP}+z_t^{CP}$의 계수로서 $\phi_{i,1}^{CP}$, …, $\phi_{i,ztCP}^{CP}$(여기서, ztCP는 z_t^{CP}이다)가 설정된다.

[0361] 한편, $\rho^{CP}(i)$가 부정형의 조 $\neg(t, \vec{v}_i^{CP})$인 경우에는, 기저 벡터 1, …, n_t^{CP}의 계수로서 $s_i^{CP}v_{i,1}^{CP}$, …, $s_i^{CP}v_{i,ntCP}^{CP}$(여기서, ntCP는 n_t^{CP}이다)가 설정된다. 기저 벡터 $n_t^{CP}+1$, …, $n_t^{CP}+u_t^{CP}+w_t^{CP}$의 계수로서 0이 설정된다. 기저 벡터 $n_t^{CP}+u_t^{CP}+w_t^{CP}+1$, …, $n_t^{CP}+u_t^{CP}+w_t^{CP}+z_t^{CP}$의 계수로서 $\phi_{i,1}^{CP}$, …, $\phi_{i,ztCP}^{CP}$(여기서, ztCP는 z_t^{CP}이다)가 설정된다.

[0362] 또, θ_i^{CP} 및 $\vec{\phi}_i^{CP}$는 난수 생성부(233)에 의해 생성되는 난수이다.

[0363] (S309 : 메시지 암호화 데이터 생성 단계)

[0364] 메시지 암호화 데이터 생성부(237)는, 처리 장치에 의해, 암호화 데이터 $ct_{(\Gamma^{KP}, SCP)}$의 요소인 메시지 암호화 데이터 c_{d+1}을 수학식 152에 나타내는 바와 같이 생성한다.

[0365] [수학식 152]

[0366] $$c_{d+1} := g_T^{\zeta} m$$

[0367] 또, 상술한 바와 같이, 수학식 153이다.

[0368] [수학식 153]

[0369] $$g_T := e(g,g)^{\psi}$$

[0370] (S310 : 데이터 송신 단계)

[0371] 데이터 송신부(240)는, 주 암호화 데이터 c_0과, 속성의 집합 Γ^{KP} 및 KP 암호화 데이터 c_t^{KP}와, 액세스 스트럭처 S^{CP} 및 CP 암호화 데이터 c_i^{CP}와, 메시지 암호화 데이터 c_{d+1}을 요소로 하는 암호화 데이터 $ct_{(\Gamma^{KP}, SCP)}$를, 예컨대 통신 장치에 의해 네트워크를 통해 복호 장치(300)에 송신한다. 물론, 암호화 데이터 $ct_{(\Gamma^{KP}, SCP)}$는, 다른 방법에 의해 복호 장치(300)에 송신되더라도 좋다.

[0372] 다시 말해, (S301)로부터 (S309)에 있어서, 암호화 장치(200)는, 수학식 154에 나타내는 Enc 알고리즘을 실행하여, 암호화 데이터 $ct_{(\Gamma^{KP}, SCP)}$를 생성한다. 그리고, (S310)에서, 암호화 장치(200)는, 생성된 암호화 데이터 $ct_{(\Gamma^{KP}, SCP)}$를 복호 장치(300)에 송신한다.

[0373] [수학식 154]

$$
\begin{aligned}
&\mathsf{Enc}(\mathsf{pk}, m, \Gamma^{\mathsf{KP}} :=\\
&\quad \{(t, \vec{x}_t^{\mathsf{KP}} := (x_{t,1}^{\mathsf{KP}}, \ldots, x_{t,n_t^{\mathsf{KP}}}^{\mathsf{KP}}) \in \mathbb{F}_q^{n_t^{\mathsf{KP}}} \setminus \{\vec{0}\}) \,|\, 1 \le t \le d^{\mathsf{KP}}, x_{t,1}^{\mathsf{KP}} := 1\},\\
&\quad \mathbb{S}^{\mathsf{CP}} := (M^{\mathsf{CP}}, \rho^{\mathsf{CP}})):\\
&\qquad \omega^{\mathsf{KP}}, \zeta \xleftarrow{\mathsf{U}} \mathbb{F}_q, \vec{\varphi}_0 \xleftarrow{\mathsf{U}} \mathbb{F}_q^{z_0}, \vec{\varphi}_t^{\mathsf{KP}} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{z_t^{\mathsf{KP}}} \text{ for } (t, \vec{x}_t^{\mathsf{KP}}) \in \Gamma,\\
&\qquad \vec{f}^{\mathsf{CP}} \xleftarrow{\mathsf{R}} \mathbb{F}_q^{r^{\mathsf{CP}}}, (\vec{s}^{\mathsf{CP}})^{\mathrm{T}} := (s_1^{\mathsf{CP}}, \ldots, s_{L^{\mathsf{CP}}}^{\mathsf{CP}})^{\mathrm{T}} := M^{\mathsf{CP}} \cdot (\vec{f}^{\mathsf{CP}})^{\mathrm{T}},\\
&\qquad s_0^{\mathsf{CP}} := \vec{1} \cdot (\vec{f}^{\mathsf{CP}})^{\mathrm{T}},\\
&\qquad c_0 := (\omega^{\mathsf{KP}}, -s_0^{\mathsf{CP}}, \overbrace{0^{u_0}}^{u_0}, \zeta, \overbrace{0^{w_0}}^{w_0}, \overbrace{\varphi_{0,1}, \ldots, \varphi_{0,z_0}}^{z_0})_{\mathbb{B}_0},\\
&\qquad \text{for } (t, \vec{x}_t^{\mathsf{KP}}) \in \Gamma^{\mathsf{KP}},\\
&\qquad\quad c_t^{\mathsf{KP}} := (\overbrace{\omega^{\mathsf{KP}} \vec{x}_t^{\mathsf{KP}}}^{n_t^{\mathsf{KP}}}, \overbrace{0^{u_t^{\mathsf{KP}}}}^{u_t^{\mathsf{KP}}}, \overbrace{0^{w_t^{\mathsf{KP}}}}^{w_t^{\mathsf{KP}}}, \overbrace{\vec{\varphi}_t^{\mathsf{KP}}}^{z_t^{\mathsf{KP}}})_{\mathbb{B}_t^{\mathsf{KP}}},\\
&\qquad\quad \text{for } i = 1, \ldots, L^{\mathsf{CP}},\\
&\qquad\quad\quad \text{if } \rho^{\mathsf{CP}}(i) = (t, \vec{v}_i^{\mathsf{CP}} := (v_{i,1}^{\mathsf{CP}}, \ldots, v_{i,n_t^{\mathsf{CP}}}^{\mathsf{CP}}) \in \mathbb{F}_q^{n_t^{\mathsf{CP}}} \setminus \{\vec{0}\}),\\
&\qquad\quad\quad\quad \theta_i^{\mathsf{CP}} \xleftarrow{\mathsf{U}} \mathbb{F}_q, \vec{\varphi}_i^{\mathsf{CP}} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{z_t^{\mathsf{CP}}},\\
&\qquad\quad\quad\quad c_i^{\mathsf{CP}} := (\overbrace{s_i^{\mathsf{CP}} \vec{e}_{t,1}^{\mathsf{CP}} + \theta_i^{\mathsf{CP}} \vec{v}_i^{\mathsf{CP}}}^{n_t^{\mathsf{CP}}}, \overbrace{0^{u_t^{\mathsf{CP}}}}^{u_t^{\mathsf{CP}}}, \overbrace{0^{w_t^{\mathsf{CP}}}}^{w_t^{\mathsf{CP}}}, \overbrace{\vec{\varphi}_i^{\mathsf{CP}}}^{z_t^{\mathsf{CP}}})_{\mathbb{B}_i^{\mathsf{CP}}},\\
&\qquad\quad\quad \text{if } \rho^{\mathsf{CP}}(i) = \neg(t, \vec{v}_i^{\mathsf{CP}}), \vec{\varphi}_i^{\mathsf{CP}} \xleftarrow{\mathsf{U}} \mathbb{F}_q^{z_t^{\mathsf{CP}}},\\
&\qquad\quad\quad\quad c_i^{\mathsf{CP}} := (\overbrace{s_i^{\mathsf{CP}} \vec{v}_i^{\mathsf{CP}}}^{n_t^{\mathsf{CP}}}, \overbrace{0^{u_t^{\mathsf{CP}}}}^{u_t^{\mathsf{CP}}}, \overbrace{0^{w_t^{\mathsf{CP}}}}^{w_t^{\mathsf{CP}}}, \overbrace{\vec{\varphi}_i^{\mathsf{CP}}}^{z_t^{\mathsf{CP}}})_{\mathbb{B}_i^{\mathsf{CP}}},\\
&\qquad c_{d+1} := g_T^{\zeta} m,\\
&\qquad \text{return } \mathsf{ct}_{(\Gamma^{\mathsf{KP}}, \mathbb{S}^{\mathsf{CP}})} :=\\
&\qquad\quad (c_0; \Gamma^{\mathsf{KP}}, \{c_t^{\mathsf{KP}}\}_{(t, \vec{x}_t^{\mathsf{KP}}) \in \Gamma^{\mathsf{KP}}}; \mathbb{S}^{\mathsf{CP}}, c_1^{\mathsf{CP}}, \ldots, c_{L^{\mathsf{CP}}}^{\mathsf{CP}}; c_{d+1})
\end{aligned}
$$

[0374]

[0375] 복호 장치(300)의 기능과 동작에 대하여 설명한다.

[0376] 도 8에 나타내는 바와 같이, 복호 장치(300)는, 복호 키 취득부(310), 데이터 수신부(320)(데이터 취득부), 스팬 프로그램 계산부(330), 보완 계수 계산부(340), 페어링 연산부(350), 메시지 계산부(360)를 구비한다.

[0377] 또한, 스팬 프로그램 계산부(330)는, KP 스팬 프로그램 계산부(331), CP 스팬 프로그램 계산부(332)를 구비한다. 또한, 보완 계수 계산부(340)는, KP 보완 계수 계산부(341), CP 보완 계수 계산부(342)를 구비한다.

[0378] 도 12에 근거하여, Dec 알고리즘의 처리에 대하여 설명한다.

[0379] (S401 : 복호 키 취득 단계)

[0380] 복호 키 취득부(310)는, 예컨대, 통신 장치에 의해 네트워크를 통해, 키 생성 장치(100)로부터 배포된 복호 키 $sk_{(SKP,\ \Gamma CP)}$를 취득한다. 또한, 복호 키 취득부(310)는, 키 생성 장치(100)가 생성한 공개 파라미터 pk를 취득한다.

[0381] (S402 : 데이터 수신 단계)

[0382] 데이터 수신부(320)는, 예컨대, 통신 장치에 의해 네트워크를 통해, 암호화 장치(200)가 송신한 암호화 데이터 $ct_{(\Gamma KP,\ SCP)}$를 수신한다.

[0383] (S403 : 스팬 프로그램 계산 단계)

[0384] KP 스팬 프로그램 계산부(331)는, 처리 장치에 의해, (S401)에서 취득한 복호 키 $sk_{(SKP,\ \Gamma CP)}$에 포함되는 액세스 스트럭쳐 S^{KP}가, (S402)에서 수신한 암호화 데이터 $ct_{(\Gamma KP,\ SCP)}$에 포함되는 속성의 집합 Γ^{KP}를 수리할지 여부를

판정한다.

[0385] 또한, CP 스팬 프로그램 계산부(332)는, 처리 장치에 의해, (S402)에서 수신한 암호화 데이터 $ct_{(\Gamma KP,\ SCP)}$에 포함되는 액세스 스트럭쳐 S^{CP}가, (S401)에서 취득한 복호 키 $sk_{(SKP,\ \Gamma CP)}$에 포함되는 속성의 집합 Γ_{CP}를 수리할지 여부를 판정한다.

[0386] 또, 액세스 스트럭쳐가 속성의 집합을 수리하는지 여부의 판정 방법은, 「제 3. 함수형 암호를 실현하기 위한 개념」에서 설명한 바와 같다.

[0387] 스팬 프로그램 계산부(330)는, 액세스 스트럭쳐 S^{KP}가 속성의 집합 Γ^{KP}를 수리하고, 또한, 액세스 스트럭쳐 S^{CP}가 속성의 집합 Γ^{CP}를 수리하는 경우(S403에서 수리), 처리를 (S404)로 진행시킨다. 한편, 액세스 스트럭쳐 S^{KP}가 속성의 집합 Γ^{KP}를 거절하는 경우와, 액세스 스트럭쳐 S^{CP}가 속성의 집합 Γ^{CP}를 거절하는 경우의 적어도 하나의 경우(S403에서 거절), 암호화 데이터 $ct_{(\Gamma KP,\ SCP)}$를 복호 키 $sk_{(SKP,\ \Gamma CP)}$로 복호할 수 없는 것으로 하여, 식별 정보 $\perp$를 출력하여, 처리를 종료한다.

[0388] (S404 : 보완 계수 계산 단계)

[0389] KP 보완 계수 계산부(341)는, 처리 장치에 의해, 수학식 155가 되는 I^{KP}와, I^{KP}에 포함되는 각 정수 i에 대하여 상수(보완 계수) α_i^{KP}를 계산한다.

[0390] [수학식 155]

[0391]
$$\vec{1}=\sum_{i\in I}\alpha_i^{KP}M_i^{KP},\ \text{where } M_i^{KP} \text{ is the } i-\text{th row of } M^{KP}, \text{and}$$
$$I^{KP}\subseteq\{i\in\{1,\ldots,L^{KP}\}$$
$$\left|[\rho^{KP}(i)=(t,\vec{v}_i^{KP})\wedge(t,\vec{x}_t^{KP})\in\Gamma^{KP}\wedge\vec{v}_i^{KP}\cdot\vec{x}_t^{KP}=0]\right.$$
$$[\rho^{KP}(i)=\neg(t,\vec{v}_i^{KP})\wedge(t,\vec{x}_t^{KP})\in\Gamma^{KP}\wedge\vec{v}_i^{KP}\cdot\vec{x}_t^{KP}\neq 0]\}$$

[0392] 또한, CP 보완 계수 계산부(342)는, 처리 장치에 의해, 수학식 156이 되는 I^{CP}와, I^{CP}에 포함되는 각 정수 i에 대하여 상수(보완 계수) α_i^{CP}를 계산한다.

[0393] [수학식 156]

[0394]
$$\vec{1}=\sum_{i\in I}\alpha_i^{CP}M_i^{CP},\ \text{where } M_i^{CP} \text{ is the } i-\text{th row of } M^{CP}, \text{and}$$
$$I^{CP}\subseteq\{i\in\{1,\ldots,L^{CP}\}$$
$$\left|[\rho^{CP}(i)=(t,\vec{v}_i^{CP})\wedge(t,\vec{x}_t^{CP})\in\Gamma^{CP}\wedge\vec{v}_i^{CP}\cdot\vec{x}_t^{CP}=0]\right.$$
$$[\rho^{CP}(i)=\neg(t,\vec{v}_i^{CP})\wedge(t,\vec{x}_t^{CP})\in\Gamma^{CP}\wedge\vec{v}_i^{CP}\cdot\vec{x}_t^{CP}\neq 0]\}$$

[0395] (S405 : 페어링 연산 단계)

[0396] 페어링 연산부(350)는, 처리 장치에 의해, 수학식 157을 계산하여, 세션 키 $K=g_T^{\zeta}$를 생성한다.

[0397] [수학식 157]

$$K := e(c_0, k_0^*) \cdot \prod_{i \in I^{KP} \wedge \rho^{KP}(i) = (t, \vec{v}_i^{KP})} e(c_t^{KP}, k_i^{*KP})^{\alpha_i^{KP}} \cdot \prod_{i \in I^{KP} \wedge \rho^{KP}(i) = \neg(t, \vec{v}_i^{KP})} e(c_t^{KP}, k_i^{*KP})^{\alpha_i^{KP}/(\vec{v}_i^{KP} \cdot \vec{x}_t^{KP})} \cdot \prod_{i \in I^{CP} \wedge \rho^{CP}(i) = (t, \vec{v}_i^{CP})} e(c_t^{CP}, k_i^{*CP})^{\alpha_i^{CP}} \cdot \prod_{i \in I^{CP} \wedge \rho^{CP}(i) = \neg(t, \vec{v}_i^{CP})} e(c_t^{CP}, k_i^{*CP})^{\alpha_i^{CP}/(\vec{v}_i^{CP} \cdot \vec{x}_t^{CP})}$$

[0398]

[0399] 또, 수학식 158에 나타내는 바와 같이, 수학식 157을 계산하는 것에 의해 키$K=g_T^{\zeta}$가 얻어진다.

[0400] [수학식 158]

$$\begin{aligned} K &:= e(c_0, k_0^*) \cdot \prod_{i \in I^{KP} \wedge \rho^{KP}(i) = (t, \vec{v}_i^{KP})} e(c_t^{KP}, k_i^{*KP})^{\alpha_i^{KP}} \cdot \prod_{i \in I^{KP} \wedge \rho^{KP}(i) = \neg(t, \vec{v}_i^{KP})} e(c_t^{KP}, k_i^{*KP})^{\alpha_i^{KP}/(\vec{v}_i^{KP} \cdot \vec{x}_t^{KP})} \cdot \prod_{i \in I^{CP} \wedge \rho^{CP}(i) = (t, \vec{v}_i^{CP})} e(c_t^{CP}, k_i^{*CP})^{\alpha_i^{CP}} \cdot \prod_{i \in I^{CP} \wedge \rho^{CP}(i) = \neg(t, \vec{v}_i^{CP})} e(c_t^{CP}, k_i^{*CP})^{\alpha_i^{CP}/(\vec{v}_i^{CP} \cdot \vec{x}_t^{CP})} \\ &= g_T^{-\varpi^{KP} s_0^{KP} - \delta^{CP} s_0^{CP} + \zeta} \cdot \prod_{i \in I^{KP} \wedge \rho^{KP}(i) = (t, \vec{v}_i^{KP})} g_T^{\varpi^{KP} \alpha_i s_i^{KP}} \cdot \prod_{i \in I^{KP} \wedge \rho^{KP}(i) = \neg(t, \vec{v}_i^{KP})} g_T^{\varpi^{KP} \alpha_i s_i^{KP} (\vec{v}_i^{KP} \cdot \vec{x}_t^{KP})/(\vec{v}_i^{KP} \cdot \vec{x}_t^{KP})} \cdot \prod_{i \in I^{CP} \wedge \rho^{CP}(i) = (t, \vec{v}_i^{CP})} g_T^{\delta^{CP} \alpha_i s_i^{CP}} \cdot \prod_{i \in I^{CP} \wedge \rho^{CP}(i) = \neg(t, \vec{v}_i^{CP})} g_T^{\delta^{CP} \alpha_i s_i^{CP} (\vec{v}_i^{CP} \cdot \vec{x}_t^{CP})/(\vec{v}_i^{CP} \cdot \vec{x}_t^{CP})} \\ &= g_T^{-\varpi^{KP} s_0^{KP} - \delta^{CP} s_0^{CP} + \zeta + \varpi^{KP} s_0^{KP} + \delta^{CP} s_0^{CP}} \\ &= g_T^{\zeta} \end{aligned}$$

[0401]

[0402] (S406 : 메시지 계산 단계)

[0403] 메시지 계산부(360)는, 처리 장치에 의해, $m'=c_{d+1}/K$를 계산하여, 메시지 $m'(=m)$를 생성한다. 또, 메시지 암호화 데이터 c_{d+1}은 수학식 152에 나타내는 바와 같이 $g_T^{\zeta}m$이고, K는 g_T^{ζ}이므로, $m'=c_{d+1}/K$를 계산하면 메시지 m이 얻어진다.

[0404] 다시 말해, (S401)로부터 (S406)에 있어서, 복호 장치(300)는, 수학식 159에 나타내는 Dec 알고리즘을 실행하여, 메시지 $m'(=m)$를 생성한다.

[0405] [수학식 159]

$$
\begin{aligned}
&\mathrm{Dec}(pk,\\
&\quad \mathsf{sk}_{(\mathbb{S}^{\mathsf{KP}},\Gamma^{\mathsf{CP}})} := (k_0^*;\mathbb{S}^{\mathsf{KP}},k_1^{*\mathsf{KP}},\ldots,k_{L^{\mathsf{KP}}}^{*\mathsf{KP}};\Gamma^{\mathsf{CP}},\{k_t^{*\mathsf{CP}}\})_{(t,\vec{x}_t^{\mathsf{CP}})\in\Gamma^{\mathsf{CP}}},\\
&\quad \mathsf{ct}_{(\Gamma^{\mathsf{KP}},\mathbb{S}^{\mathsf{CP}})} := (c_0;\Gamma^{\mathsf{KP}},\{c_t^{\mathsf{KP}}\}_{(t,\vec{x}_t^{\mathsf{KP}})\in\Gamma^{\mathsf{KP}}};\mathbb{S}^{\mathsf{CP}},c_1^{\mathsf{CP}},\ldots,c_{L^{\mathsf{CP}}}^{\mathsf{CP}};c_{d+1})):\\
&\quad \text{If } \mathbb{S}^{\mathsf{KP}} := (M^{\mathsf{KP}},\rho^{\mathsf{KP}}) \text{ accepts } \Gamma^{\mathsf{KP}} := \{(t,\vec{x}_t^{\mathsf{KP}})\}\\
&\qquad \text{and } \mathbb{S}^{\mathsf{CP}} := (M^{\mathsf{CP}},\rho^{\mathsf{CP}}) \text{ accepts } \Gamma^{\mathsf{CP}} := \{(t,\vec{x}_t^{\mathsf{CP}})\},\\
&\qquad \text{then compute } (I^{\mathsf{KP}},\{\alpha_i^{\mathsf{KP}}\}_{i\in I^{\mathsf{KP}}}) \text{ and } (I^{\mathsf{CP}},\{\alpha_i^{\mathsf{CP}}\}_{i\in I^{\mathsf{CP}}}) \text{ such that}\\
&\qquad\quad \vec{1}=\textstyle\sum_{i\in I}\alpha_i^{\mathsf{KP}} M_i^{\mathsf{KP}}, \text{ where } M_i^{\mathsf{KP}} \text{ is the } i-\text{th row of } M^{\mathsf{KP}}, \text{and}\\
&\qquad\quad I^{\mathsf{KP}} \subseteq \{i\in\{1,\ldots,L^{\mathsf{KP}}\}\\
&\qquad\qquad \big|[\rho^{\mathsf{KP}}(i)=(t,\vec{v}_i^{\mathsf{KP}})\wedge(t,\vec{x}_t^{\mathsf{KP}})\in\Gamma^{\mathsf{KP}}\wedge\vec{v}_i^{\mathsf{KP}}\cdot\vec{x}_t^{\mathsf{KP}}=0]\\
&\qquad\qquad \vee[\rho^{\mathsf{KP}}(i)=\neg(t,\vec{v}_i^{\mathsf{KP}})\wedge(t,\vec{x}_t^{\mathsf{KP}})\in\Gamma^{\mathsf{KP}}\wedge\vec{v}_i^{\mathsf{KP}}\cdot\vec{x}_t^{\mathsf{KP}}\neq 0]\},\text{and}\\
&\qquad\quad \vec{1}=\textstyle\sum_{i\in I}\alpha_i^{\mathsf{CP}} M_i^{\mathsf{CP}}, \text{ where } M_i^{\mathsf{CP}} \text{ is the } i-\text{th row of } M^{\mathsf{CP}}, \text{and}\\
&\qquad\quad I^{\mathsf{CP}} \subseteq \{i\in\{1,\ldots,L^{\mathsf{CP}}\}\\
&\qquad\qquad \big|[\rho^{\mathsf{CP}}(i)=(t,\vec{v}_i^{\mathsf{CP}})\wedge(t,\vec{x}_t^{\mathsf{CP}})\in\Gamma^{\mathsf{CP}}\wedge\vec{v}_i^{\mathsf{CP}}\cdot\vec{x}_t^{\mathsf{CP}}=0]\\
&\qquad\qquad \vee[\rho^{\mathsf{CP}}(i)=\neg(t,\vec{v}_i^{\mathsf{CP}})\wedge(t,\vec{x}_t^{\mathsf{CP}})\in\Gamma^{\mathsf{CP}}\wedge\vec{v}_i^{\mathsf{CP}}\cdot\vec{x}_t^{\mathsf{CP}}\neq 0]\},\\
&\quad K := e(c_0,k_0^*)\cdot\\
&\qquad \prod_{i\in I^{\mathsf{KP}}\wedge\rho^{\mathsf{KP}}(i)=(t,\vec{v}_i^{\mathsf{KP}})} e(c_t^{\mathsf{KP}},k_i^{*\mathsf{KP}})^{\alpha_i^{\mathsf{KP}}}\cdot\\
&\qquad \prod_{i\in I^{\mathsf{KP}}\wedge\rho^{\mathsf{KP}}(i)=\neg(t,\vec{v}_i^{\mathsf{KP}})} e(c_t^{\mathsf{KP}},k_i^{*\mathsf{KP}})^{\alpha_i^{\mathsf{KP}}/(\vec{v}_i^{\mathsf{KP}}\cdot\vec{x}_t^{\mathsf{KP}})}\cdot\\
&\qquad \prod_{i\in I^{\mathsf{CP}}\wedge\rho^{\mathsf{CP}}(i)=(t,\vec{v}_i^{\mathsf{CP}})} e(c_t^{\mathsf{CP}},k_i^{*\mathsf{CP}})^{\alpha_i^{\mathsf{CP}}}\cdot\\
&\qquad \prod_{i\in I^{\mathsf{CP}}\wedge\rho^{\mathsf{CP}}(i)=\neg(t,\vec{v}_i^{\mathsf{CP}})} e(c_t^{\mathsf{CP}},k_i^{*\mathsf{CP}})^{\alpha_i^{\mathsf{CP}}/(\vec{v}_i^{\mathsf{CP}}\cdot\vec{x}_t^{\mathsf{CP}})},
\end{aligned}
$$

[0406] return $m' := c_{d+1}/K$

[0407] 이상과 같이, 암호 처리 시스템(10)은, 스팬 프로그램과 내적 술어와 비밀 분산을 이용하여 구성한 액세스 스트럭쳐 S^{KP} 및 S^{CP}를 이용하여, 암호 방식(함수형 암호 방식)을 실현한다. 따라서, 암호 처리 시스템(10)은, 매우 높은 자유도로 액세스 제어의 설계를 행하는 것이 가능한 암호 방식을 실현한다.

[0408] 특히, 암호 처리 시스템(10)은, 액세스 스트럭쳐 S^{KP}를 복호 키에 갖게 하고, 액세스 스트럭쳐 S^{CP}를 암호화 데이터에 갖게 하고 있다. 따라서, 암호 처리 시스템(10)은, 복호 키와 암호화 데이터의 양쪽으로 액세스 컨트롤을 행할 수 있다.

[0409] 또, 상기 설명에 있어서, u_t, w_t, z_t(t=0, …, d+1)의 차원은, 안전성을 높이기 위해 마련한 차원이다. 따라서, 안전성이 낮아져 버리지만, u_t, w_t, z_t(t=0, …, d+1)를 각각 0으로 하여, u_t, w_t, z_t(t=0, …, d+1)의 차원을 마련하지 않더라도 좋다.

[0410] 또한, 상기 설명에서는, (S101)에서 N_0에 $2+u_0+1+w_0+z_0$을 설정했다. 그러나, $2+u_0+1+w_0+z_0$을 2+2+1+2+1로 하여, N_0에 8을 설정하더라도 좋다.

[0411] 또한, 상기 설명에서는, (S101)에서 N_t^{KP}에 $n_t^{KP}+u_t^{KP}+w_t^{KP}+z_t^{KP}$를 설정했다. 그러나, $n_t^{KP}+u_t^{KP}+w_t^{KP}+z_t^{KP}$를 $n_t^{KP}+n_t^{KP}+n_t^{KP}+1$로 하여, N_t^{KP}에 $3n_t^{KP}+1$을 설정하더라도 좋다.

[0412] 마찬가지로, (S101)에서 N_t^{CP}에 $n_t^{CP}+u_t^{CP}+wt^{CP}+z_t^{CP}$를 설정했다. 그러나, $n_t^{CP}+u_t^{CP}+w_t^{CP}+z_t^{CP}$를 $n_t^{CP}+n_t^{CP}+n_t^{CP}+1$로 하여, N_t^{CP}에 $3n_t^{CP}+1$을 설정하더라도 좋다.

[0413] 이 경우, 수학식 136에 나타내는 Setup 알고리즘은, 수학식 160과 같이 고쳐 쓸 수 있다. 또, G_{ob}^{UP}는 수학식 161과 같이 고쳐 쓸 수 있다.

[0414] [수학식 160]

$$
\begin{aligned}
&\mathsf{Setup}(1^{\lambda},\vec{n} := ((d^{\mathsf{KP}};n_1^{\mathsf{KP}},\ldots,n_{d^{\mathsf{KP}}}^{\mathsf{KP}}),(d^{\mathsf{CP}};n_1^{\mathsf{CP}},\ldots,n_{d^{\mathsf{CP}}}^{\mathsf{CP}}))\colon\\
&\quad(\mathsf{param}_{\vec{n}},\mathbb{B}_0,\mathbb{B}_0^*,\{\mathbb{B}_t^{\mathsf{KP}},\mathbb{B}_t^{*\mathsf{KP}}\}_{t=1,\ldots,d^{\mathsf{KP}}},\\
&\quad\{\mathbb{B}_t^{\mathsf{CP}},\mathbb{B}_t^{*\mathsf{CP}}\}_{t=1,\ldots,d^{\mathsf{CP}}}) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{ob}}(1^{\lambda},\vec{n}),\\
&\quad\hat{\mathbb{B}}_0 := (b_{0,1},b_{0,2},b_{0,5},b_{0,8}),\ \ \hat{\mathbb{B}}_0^* := (b_{0,1}^*,b_{0,2}^*,b_{0,5}^*,b_{0,6}^*,b_{0,7}^*),\\
&\quad\text{for } t=1,\ldots,d^{\mathsf{KP}},\ \ \hat{\mathbb{B}}_t^{\mathsf{KP}} := (b_{t,1}^{\mathsf{KP}},\ldots,b_{t,n_t^{\mathsf{KP}}}^{\mathsf{KP}},b_{t,3n_t^{\mathsf{KP}}+1}^{\mathsf{KP}}),\\
&\qquad\qquad\hat{\mathbb{B}}_t^{*\mathsf{KP}} := (b_{t,1}^{*\mathsf{KP}},\ldots,b_{t,n_t^{\mathsf{KP}}}^{*\mathsf{KP}},b_{t,2n_t^{\mathsf{KP}}+1}^{*\mathsf{KP}},\ldots,b_{t,3n_t^{\mathsf{KP}}}^{*\mathsf{KP}}),\\
&\quad\text{for } t=1,\ldots,d^{\mathsf{CP}},\ \ \hat{\mathbb{B}}_t^{\mathsf{CP}} := (b_{t,1}^{\mathsf{CP}},\ldots,b_{t,n_t^{\mathsf{CP}}}^{\mathsf{CP}},b_{t,3n_t^{\mathsf{CP}}+1}^{\mathsf{CP}}),\\
&\qquad\qquad\hat{\mathbb{B}}_t^{*\mathsf{CP}} := (b_{t,1}^{*\mathsf{CP}},\ldots,b_{t,n_t^{\mathsf{CP}}}^{*\mathsf{CP}},b_{t,2n_t^{\mathsf{CP}}+1}^{*\mathsf{CP}},\ldots,b_{t,3n_t^{\mathsf{CP}}}^{*\mathsf{CP}}),\\
&\quad\mathsf{pk} := (1^{\lambda},\mathsf{param}_{\vec{n}},\hat{\mathbb{B}}_0,\{\hat{\mathbb{B}}_t^{\mathsf{KP}}\}_{t=1,\ldots,d^{\mathsf{KP}}},\{\hat{\mathbb{B}}_t^{\mathsf{CP}}\}_{t=1,\ldots,d^{\mathsf{CP}}}),\\
&\quad\mathsf{sk} := (\hat{\mathbb{B}}_0^*,\{\hat{\mathbb{B}}_t^{*\mathsf{KP}}\}_{t=1,\ldots,d^{\mathsf{KP}}},\{\hat{\mathbb{B}}_t^{*\mathsf{CP}}\}_{t=1,\ldots,d^{\mathsf{CP}}})
\end{aligned}
$$

[0415] return pk, sk

[0416] [수학식 161]

$$
\begin{aligned}
&\mathcal{G}_{\mathsf{ob}}^{\mathsf{up}}(1^{\lambda},\vec{n} := ((d^{\mathsf{KP}};n_1^{\mathsf{KP}},\ldots,n_{d^{\mathsf{KP}}}^{\mathsf{KP}}),(d^{\mathsf{CP}};n_1^{\mathsf{CP}},\ldots,n_{d^{\mathsf{CP}}}^{\mathsf{CP}}))\colon\\
&\quad\mathsf{param}_{\mathbb{G}} := (q,\mathbb{G},\mathbb{G}_T,g,e) \xleftarrow{\mathsf{R}} \mathcal{G}_{\mathsf{bpg}}(1^{\lambda}),\quad \psi \xleftarrow{\mathsf{U}} \mathbb{F}_q^{\times},\\
&\quad N_0 := 8,\ \ N_t^{\mathsf{KP}} := 3n_t^{\mathsf{KP}}+1 \ \text{ for } t=1,\ldots,d^{\mathsf{KP}},\\
&\quad N_t^{\mathsf{CP}} := 3n_t^{\mathsf{CP}}+1 \ \text{ for } t=1,\ldots,d^{\mathsf{CP}},\\
&\quad\mathsf{param}_{\mathbb{V}_0} := (q,\mathbb{V}_0,\mathbb{G}_T,\mathbb{A}_0,e) := \mathcal{G}_{\mathsf{dpvs}}(1^{\lambda},N_0,\mathsf{param}_{\mathbb{G}}),\\
&\quad X_0 := (\chi_{0,i,j})_{i,j} \xleftarrow{\mathsf{U}} GL(N_0,\mathbb{F}_q),\quad (v_{0,i,j})_{i,j} := \psi\cdot(X_0^{\mathrm{T}})^{-1},\\
&\quad b_{0,i} := (\chi_{0,i,1},\ldots,\chi_{0,i,N_0})_{\mathbb{A}_0},\ \ \mathbb{B}_0 := (b_{0,1},\ldots,b_{0,N_0}),\\
&\quad b_{0,i}^* := (v_{0,i,1},\ldots,v_{0,i,N_0})_{\mathbb{A}_0},\ \ \mathbb{B}_0^* := (b_{0,i}^*,\ldots,b_{0,N_0}^*),\\
&\quad\text{for } t=1,\ldots,d^{\mathsf{KP}},\\
&\qquad\mathsf{param}_{\mathbb{V}_t^{\mathsf{KP}}} := (q,\mathbb{V}_t^{\mathsf{KP}},\mathbb{G}_T,\mathbb{A}_t^{\mathsf{KP}},e) := \mathcal{G}_{\mathsf{dpvs}}(1^{\lambda},N_t^{\mathsf{KP}},\mathsf{param}_{\mathbb{G}}),\\
&\qquad X_t^{\mathsf{KP}} := (\chi_{t,i,j}^{\mathsf{KP}})_{i,j} \xleftarrow{\mathsf{U}} GL(N_t^{\mathsf{KP}},\mathbb{F}_q),\quad (v_{t,i,j}^{\mathsf{KP}})_{i,j} := \psi\cdot(X_t^{\mathsf{KP}})^{\mathrm{T}})^{-1},\\
&\qquad b_{t,i}^{\mathsf{KP}} := (\chi_{t,i,1}^{\mathsf{KP}},\ldots,\chi_{t,i,N_t^{\mathsf{KP}}}^{\mathsf{KP}})_{\mathbb{A}_t^{\mathsf{KP}}},\ \ \mathbb{B}_t^{\mathsf{KP}} := (b_{t,1}^{\mathsf{KP}},\ldots,b_{t,iN_t^{\mathsf{KP}}}^{\mathsf{KP}}),\\
&\qquad b_{t,i}^{*\mathsf{KP}} := (v_{t,i,1}^{\mathsf{KP}},\ldots,v_{t,i,N_t^{\mathsf{KP}}}^{\mathsf{KP}})_{\mathbb{A}_t^{\mathsf{KP}}},\ \ \mathbb{B}_t^{*\mathsf{KP}} := (b_{t,1}^{*\mathsf{KP}},\ldots,b_{t,N_t^{\mathsf{KP}}}^{*\mathsf{KP}}),\\
&\quad\text{for } t=1,\ldots,d^{\mathsf{CP}},\\
&\qquad\mathsf{param}_{\mathbb{V}_t^{\mathsf{CP}}} := (q,\mathbb{V}_t^{\mathsf{CP}},\mathbb{G}_T,\mathbb{A}_t^{\mathsf{CP}},e) := \mathcal{G}_{\mathsf{dpvs}}(1^{\lambda},N_t^{\mathsf{CP}},\mathsf{param}_{\mathbb{G}}),\\
&\qquad X_t^{\mathsf{CP}} := (\chi_{t,i,j}^{\mathsf{CP}})_{i,j} \xleftarrow{\mathsf{U}} GL(N_t^{\mathsf{CP}},\mathbb{F}_q),\quad (v_{t,i,j}^{\mathsf{CP}})_{i,j} := \psi\cdot(X_t^{\mathsf{CP}})^{\mathrm{T}})^{-1},\\
&\qquad b_{t,i}^{\mathsf{CP}} := (\chi_{t,i,1}^{\mathsf{CP}},\ldots,\chi_{t,i,N_t^{\mathsf{CP}}}^{\mathsf{CP}})_{\mathbb{A}_t^{\mathsf{CP}}},\ \ \mathbb{B}_t^{\mathsf{CP}} := (b_{t,1}^{\mathsf{CP}},\ldots,b_{t,N_t^{\mathsf{CP}}}^{\mathsf{CP}}),\\
&\qquad b_{t,i}^{*\mathsf{CP}} := (v_{t,i,1}^{\mathsf{CP}},\ldots,v_{t,i,N_t^{\mathsf{CP}}}^{\mathsf{CP}})_{\mathbb{A}_t^{\mathsf{CP}}},\ \ \mathbb{B}_t^{*\mathsf{CP}} := (b_{t,1}^{*\mathsf{CP}},\ldots,b_{t,N_t^{\mathsf{CP}}}^{*\mathsf{CP}}),\\
&\quad g_T := e(g,g)^{\psi},\\
&\quad\mathsf{param}_{\vec{n}} := (\mathsf{param}_{\mathbb{V}_0},\{\mathsf{param}_{\mathbb{V}_t^{\mathsf{KP}}}\}_{t=1,\ldots,d^{\mathsf{KP}}},\{\mathsf{param}_{\mathbb{V}_t^{\mathsf{CP}}}\}_{t=1,\ldots,d^{\mathsf{CP}}},g_T)
\end{aligned}
$$

[0417] return $(\mathsf{param}_{\vec{n}},\{\mathbb{B}_0,\mathbb{B}_0^*\},\{\mathbb{B}_t^{\mathsf{KP}},\mathbb{B}_t^{*\mathsf{KP}}\}_{t=1,\ldots,d^{\mathsf{KP}}},\{\mathbb{B}_t^{\mathsf{CP}},\mathbb{B}_t^{*\mathsf{CP}}\}_{t=1,\ldots,d^{\mathsf{CP}}})$

[0418] 또한, 수학식 144에 나타내는 KeyGen 알고리즘은, 수학식 162와 같이 고쳐 쓸 수 있다.

[0419] [수학식 162]

$$\mathsf{KeyGen}(\mathsf{pk},\mathsf{sk},\mathbb{S}^{\mathsf{KP}}:=(M^{\mathsf{KP}},\rho^{\mathsf{KP}}),$$

$$\Gamma^{\mathsf{CP}}:=\{(t,\vec{x}_t^{\mathsf{CP}}:=(x_{t,1}^{\mathsf{CP}},\ldots,x_{t,n_t^{\mathsf{CP}}}^{\mathsf{CP}})\in\mathbb{F}_q^{n_t^{\mathsf{CP}}}\setminus\{\vec{0}\})\,|\,1\le t\le d^{\mathsf{CP}},x_{t,1}^{\mathsf{CP}}:=1\})$$

$$\vec{f}^{\mathsf{KP}}\xleftarrow{\mathsf{U}}\mathbb{F}_q^{r^{\mathsf{KP}}},\quad(\vec{s}^{\mathsf{KP}})^{\mathrm{T}}:=(s_1^{\mathsf{KP}},\ldots,s_{L^{\mathsf{KP}}}^{\mathsf{KP}})^{\mathrm{T}}:=M^{\mathsf{KP}}\cdot(\vec{f}^{\mathsf{KP}})^{\mathrm{T}},$$

$$s_0^{\mathsf{KP}}:=\vec{1}\cdot(\vec{f}^{\mathsf{KP}})^{\mathrm{T}},$$

$$\delta^{\mathsf{CP}}\xleftarrow{\mathsf{U}}\mathbb{F}_q,\quad\vec{\eta}_t^{\mathsf{CP}}\xleftarrow{\mathsf{U}}\mathbb{F}_q^{n_t^{\mathsf{CP}}}\ \text{ such that }(t,\vec{x}_t^{\mathsf{CP}})\in\Gamma^{\mathsf{CP}},$$

$$(\eta_{0,1},\eta_{0,2})\xleftarrow{\mathsf{U}}\mathbb{F}_q^2,$$

$$k_0^*:=(-s_0^{\mathsf{KP}},\delta^{\mathsf{CP}},0,0,1,\eta_{0,1},\eta_{0,2},0)_{\mathbb{B}_0^*},$$

$$\text{for } i=1,\ldots,L^{\mathsf{KP}},$$

$$\text{if }\rho^{\mathsf{KP}}(i)=(t,\vec{v}_i^{\mathsf{KP}}:=(v_{i,1}^{\mathsf{KP}},\ldots,v_{i,n_t^{\mathsf{KP}}}^{\mathsf{KP}})\in\mathbb{F}_q^{n_t^{\mathsf{KP}}}\setminus\{\vec{0}\}),$$

$$\theta_i^{\mathsf{KP}}\xleftarrow{\mathsf{U}}\mathbb{F}_q,\quad\vec{\eta}_i^{\mathsf{KP}}\xleftarrow{\mathsf{U}}\mathbb{F}_q^{n_t^{\mathsf{KP}}},$$

$$k_i^{*\mathsf{KP}}:=(\overbrace{s_i^{\mathsf{KP}}\vec{e}_{t,1}^{\mathsf{KP}}+\theta_i^{\mathsf{KP}}\vec{v}_i^{\mathsf{KP}}}^{n_t^{\mathsf{KP}}},\overbrace{0^{n_t^{\mathsf{KP}}}}^{n_t^{\mathsf{KP}}},\overbrace{\vec{\eta}_i^{\mathsf{KP}}}^{n_t^{\mathsf{KP}}},\overbrace{0}^{1},\overbrace{1}^{1})_{\mathbb{B}_t^{*\mathsf{KP}}},$$

$$\text{if }\rho^{\mathsf{KP}}(i)=\neg(t,\vec{v}_i^{\mathsf{KP}}),\quad\vec{\eta}_i^{\mathsf{KP}}\xleftarrow{\mathsf{U}}\mathbb{F}_q^{n_t^{\mathsf{KP}}},$$

$$k_i^{*\mathsf{KP}}:=(\overbrace{s_i^{\mathsf{KP}}\vec{v}_i^{\mathsf{KP}}}^{n_t^{\mathsf{KP}}},\overbrace{0^{n_t^{\mathsf{KP}}}}^{n_t^{\mathsf{KP}}},\overbrace{\vec{\eta}_i^{\mathsf{KP}}}^{n_t^{\mathsf{KP}}},\overbrace{0}^{1},\overbrace{1}^{1})_{\mathbb{B}_t^{*\mathsf{KP}}},$$

$$\text{for }(t,\vec{x}_t^{\mathsf{CP}})\in\Gamma^{\mathsf{CP}},$$

$$k_t^{*\mathsf{CP}}:=(\overbrace{\delta^{\mathsf{CP}}\vec{x}_t^{\mathsf{CP}}}^{n_t^{\mathsf{CP}}},\overbrace{0^{n_t^{\mathsf{CP}}}}^{n_t^{\mathsf{CP}}},\overbrace{\vec{\eta}_t^{\mathsf{CP}}}^{n_t^{\mathsf{CP}}},\overbrace{0}^{1},\overbrace{1}^{1})_{\mathbb{B}_t^{*\mathsf{CP}}},$$

$$\text{return }\mathsf{sk}_{(\mathbb{S}^{\mathsf{KP}},\Gamma^{\mathsf{CP}})}:=$$

$$(k_0^*;\mathbb{S}^{\mathsf{KP}},k_1^{*\mathsf{KP}},\ldots,k_{L^{\mathsf{KP}}}^{*\mathsf{KP}};\Gamma^{\mathsf{CP}},\{k_t^{*\mathsf{CP}}\}_{(t,\vec{x}_t^{\mathsf{CP}})\in\Gamma^{\mathsf{CP}}})$$

[0420]

[0421] 또한, 수학식 154에 나타내는 Enc 알고리즘은, 수학식 163과 같이 고쳐 쓸 수 있다.

[0422] [수학식 163]

$$
\begin{aligned}
&\mathsf{Enc}(\mathsf{pk}, m, \Gamma^{\mathsf{KP}} :=\\
&\quad \{(t,\vec{x}_t^{\mathsf{KP}} := (x_{t,1}^{\mathsf{KP}},\ldots,x_{t,n_t^{\mathsf{KP}}}^{\mathsf{KP}}) \in \mathbb{F}_q^{n_t^{\mathsf{KP}}} \setminus \{\vec{0}\}) \,\middle|\, 1 \le t \le d^{\mathsf{KP}}, x_{t,1}^{\mathsf{KP}} := 1\},\\
&\quad \mathbb{S}^{\mathsf{CP}} := (M^{\mathsf{CP}}, \rho^{\mathsf{CP}})) :\\
&\qquad \omega^{\mathsf{KP}}, \varphi_0, \varphi_t^{\mathsf{KP}}, \zeta \xleftarrow{\mathsf{U}} \mathbb{F}_q \text{ for } (t,\vec{x}_t^{\mathsf{KP}}) \in \Gamma,\\
&\qquad \vec{f}^{\mathsf{CP}} \xleftarrow{\mathsf{R}} \mathbb{F}_q^{r^{\mathsf{CP}}}, (\vec{s}^{\mathsf{CP}})^{\mathrm{T}} := (s_1^{\mathsf{CP}},\ldots,s_{L^{\mathsf{CP}}}^{\mathsf{CP}})^{\mathrm{T}} := M^{\mathsf{CP}} \cdot (\vec{f}^{\mathsf{CP}})^{\mathrm{T}},\\
&\qquad s_0^{\mathsf{CP}} := \vec{1} \cdot (\vec{f}^{\mathsf{CP}})^{\mathrm{T}},\\
&\qquad c_0 := (\omega^{\mathsf{KP}}, -s_0^{\mathsf{CP}}, 0, 0, \zeta, 0, 0, \varphi_0)_{\mathbb{B}_0},\\
&\qquad \text{for } (t,\vec{x}_t^{\mathsf{KP}}) \in \Gamma^{\mathsf{KP}},\\
&\qquad\quad c_t^{\mathsf{KP}} := (\overbrace{\omega^{\mathsf{KP}}\vec{x}_t^{\mathsf{KP}}}^{n_t^{\mathsf{KP}}}, \overbrace{0^{n_t^{\mathsf{KP}}}}^{n_t^{\mathsf{KP}}}, \overbrace{0^{n_t^{\mathsf{KP}}}}^{n_t^{\mathsf{KP}}}, \overbrace{\varphi_t^{\mathsf{KP}}}^{1})_{\mathbb{B}_t^{\mathsf{KP}}},\\
&\qquad\quad \text{for } i = 1,\ldots,L^{\mathsf{CP}},\\
&\qquad\quad\quad \text{if } \rho^{\mathsf{CP}}(i) = (t,\vec{v}_i^{\mathsf{CP}} := (v_{i,1}^{\mathsf{CP}},\ldots,v_{i,n_t^{\mathsf{CP}}}^{\mathsf{CP}}) \in \mathbb{F}_q^{n_t^{\mathsf{CP}}} \setminus \{\vec{0}\})(v_{i,n_t^{\mathsf{CP}}}^{\mathsf{CP}} := 1),\\
&\qquad\quad\quad\quad \varphi_i^{\mathsf{CP}}, \theta_i^{\mathsf{CP}} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\\
&\qquad\quad\quad\quad c_i^{\mathsf{CP}} := (\overbrace{s_i^{\mathsf{CP}}\vec{e}_{t,1}^{\mathsf{CP}} + \theta_i^{\mathsf{CP}}\vec{v}_i^{\mathsf{CP}}}^{n_t^{\mathsf{CP}}}, \overbrace{0^{n_t^{\mathsf{CP}}}}^{n_t^{\mathsf{CP}}}, \overbrace{0^{n_t^{\mathsf{CP}}}}^{n_t^{\mathsf{CP}}}, \overbrace{\varphi_i^{\mathsf{CP}}}^{1})_{\mathbb{B}_t^{\mathsf{CP}}},\\
&\qquad\quad\quad \text{if } \rho^{\mathsf{CP}}(i) = \neg(t,\vec{v}_i^{\mathsf{CP}}), \varphi_i^{\mathsf{CP}} \xleftarrow{\mathsf{U}} \mathbb{F}_q,\\
&\qquad\quad\quad\quad c_i^{\mathsf{CP}} := (\overbrace{s_i^{\mathsf{CP}}\vec{v}_i^{\mathsf{CP}}}^{n_t^{\mathsf{CP}}}, \overbrace{0^{n_t^{\mathsf{CP}}}}^{n_t^{\mathsf{CP}}}, \overbrace{0^{n_t^{\mathsf{CP}}}}^{n_t^{\mathsf{CP}}}, \overbrace{\varphi_i^{\mathsf{CP}}}^{1})_{\mathbb{B}_t^{\mathsf{CP}}},\\
&\qquad c_{d+1} := g_T^{\zeta} m,\\
&\qquad \text{return } \mathsf{ct}_{(\Gamma^{\mathsf{KP}},\mathbb{S}^{\mathsf{CP}})} :=\\
&\qquad\quad (c_0; \Gamma^{\mathsf{KP}}, \{c_t^{\mathsf{KP}}\}_{(t,\vec{x}_t^{\mathsf{KP}}) \in \Gamma^{\mathsf{KP}}}; \mathbb{S}^{\mathsf{CP}}, c_1^{\mathsf{CP}},\ldots,c_{L^{\mathsf{CP}}}^{\mathsf{CP}}; c_{d+1})
\end{aligned}
$$

[0423]

[0424] 또, 수학식 159에 나타내는 Dec 알고리즘에는 변경은 없다.

[0425] 또한, 상기 설명에서는, (S101)에서 N_0에 8을 설정했다. 그러나, N_0은 8은 아니고, 3이상의 정수이면 된다. N_0이 3이면, 기저 B_0과 기저 B_{*0}이 2차원이 된다. N_0이 3인 경우, KeyGen 알고리즘에 있어서, $k^*_0 := (-s_0^{KP}, \delta^{CP}, 1)_{B*0}$으로 하고, Enc 알고리즘에 있어서, $c_0 := (\omega^{KP}, -s_0^{CP}, \zeta)_{B0}$으로 하면 된다. 여기서, B*0은 B_{*0}이고, B0은 B_0이다.

[0426] 또한, 상기 설명에서는, KeyGen 알고리즘에 있어서, $k^*_0 := (-s_0, \delta^{CP}, 0, 0, 1, \eta_{0,1}, \eta_{0,2}, 0)_{B*0}$으로 했다. 그러나, 암호화 장치(200)가 알 수 있는 소정의 값 κ를 이용하여, $k^*_0 := (-s_0, \delta^{CP}, 0, 0, \kappa, \eta_{0,1}, \eta_{0,2}, 0)_{B*0}$으로 하더라도 좋다. 여기서, B*0은 B^*_0이고, B0은 B_0이다. 이 경우, Dec 알고리즘으로 계산되는 $K := g_T^{\zeta\kappa}$가 되기 때문에, Enc 알고리즘에 있어서, $c_{d+1} := g_T^{\zeta\kappa} m$으로 하면 된다.

[0427] 또한, 상기 설명에서는, $v_{i,ntCP}^{CP}$(여기서 ntCP는 n_t^{CP}이다)의 값에 대하여 특별히 한정하지 않았다. 그러나, 안전성의 증명의 관점으로부터, $v_{i,ntCP}^{CP} := 1$인 한정으로 하더라도 좋다.

[0428] 또한, 안전성의 증명의 관점으로부터, i=1, …, L^{KP}의 각 정수 i에 대한 $\rho^{KP}(i)$는, 각각 다른 식별 정보 t에 대한 긍정형의 조 $(t, \vec{v}_i^{KP})$ 또는 부정형의 조 $\neg(t, \vec{v}_i^{KP})$인 것으로 한정하더라도 좋다.

[0429] 바꾸어 말하면, $\rho^{KP}(i)=(t, \vec{v}_i^{KP})$ 또는 $\rho^{KP}(i)=\neg(t, \vec{v}_i^{KP})$인 경우에, 함수 $\rho^{\sim KP}$를, $\rho^{\sim KP}(i)=t$인 $\{1, \cdots, L\}\rightarrow\{1, .., d^{KP}\}$의 사상인 것으로 한다. 이 경우, $\rho^{\sim KP}$가 단사인 것으로 한정하더라도 좋다. 또, $\rho^{KP}(i)$는, 상술한 액세스 스트럭쳐 $S^{KP}:=(M^{KP}, \rho^{KP}(i))$의 $\rho^{KP}(i)$이다.

[0430] 마찬가지로, $i=1, \cdots, L^{CP}$의 각 정수 i에 대한 $\rho^{CP}(i)$는, 각각 다른 식별 정보 t에 대한 긍정형의 조 $(t, \vec{v}_i^{CP})$ 또는 부정형의 조 $\neg(t, \vec{v}_i^{CP})$인 것으로 한정하더라도 좋다.

[0431] 바꾸어 말하면, $\rho^{CP}(i)=(t, \vec{v}_i^{CP})$ 또는 $\rho^{CP}(i)=\neg(t, \vec{v}_i^{CP})$인 경우에, 함수 $\rho^{\sim CP}$를, $\rho^{\sim CP}(i)=t$인 $\{1, \cdots, L\}\rightarrow\{1, .., d^{CP}\}$의 사상인 것으로 한다. 이 경우, $\rho^{\sim CP}$가 단사인 것으로 한정하더라도 좋다. 또, $\rho^{CP}(i)$는, 상술한 액세스 스트럭쳐 $S^{CP}:=(M^{CP}, \rho^{CP}(i))$의 $\rho^{CP}(i)$이다.

[0432] 또한, Setup 알고리즘은, 암호 처리 시스템(10)의 셋업시에 한 번 실행하면 되고, 복호 키를 생성할 때마다 실행할 필요는 없다. 또한, 상기 설명에서는, Setup 알고리즘과 KeyGen 알고리즘을 키 생성 장치(100)가 실행하는 것으로 했지만, Setup 알고리즘과 KeyGen 알고리즘을 각각 다른 장치가 실행하는 것으로 하더라도 좋다.

[0433] 또한, 상기 설명에서는, 스팬 프로그램 $\hat{M}$는, 입력열 δ에 의해 행렬 $\hat{M}$로부터 얻어지는 행렬 M_δ의 행을 선형 결합하여 $\vec{1}$가 얻어지는 경우에 한해, 입력열 δ를 수리하는 것으로 했다. 그러나, 스팬 프로그램 $\hat{M}$는, $\vec{1}$는 아니고, 다른 벡터 $\vec{h}$가 얻어지는 경우에 한해, 입력열 δ를 수리하는 것으로 하더라도 좋다.

[0434] 이 경우, KeyGen 알고리즘에 있어서, $s_0^{KP}:=\vec{1}\cdot(f^{\vec{\rightarrow}KP})^T$는 아니고, $s_0:=h^{\vec{\rightarrow}KP}\cdot(f^{\vec{\rightarrow}KP})^T$로 하면 된다. 마찬가지로, Enc 알고리즘에 있어서, $s_0^{CP}:=\vec{1}\cdot(f^{\vec{\rightarrow}CP})^T$는 아니고, $s_0:=h^{\vec{\rightarrow}CP}\cdot(f^{\vec{\rightarrow}CP})^T$로 하면 된다.

[0435] 실시의 형태 2.

[0436] 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.

[0437] 다시 말해, 이상의 실시의 형태에서는, 소수 위수 q의 순회군에 있어서 암호 처리를 실현했다. 그러나, 합성수 M을 이용하여 수학식 164와 같이 환 R을 나타낸 경우, 환 R을 계수로 하는 가군에 있어서도, 상기 실시의 형태에서 설명한 암호 처리를 적용할 수 있다.

[0438] [수학식 164]

$$\mathbb{R}:=\mathbb{Z}/M\mathbb{Z}$$

여기서,

$\mathbb{Z}$: 정수
M : 합성수

[0439] 이다

[0440] 예컨대, 실시의 형태 1에서 설명한 Unified-Policy 함수형 암호를, 환 R을 계수로 하는 가군에 있어서 실현하면 수학식 165로부터 수학식 169와 같이 된다.

[0441] [수학식 165]

$$\mathcal{G}_{\mathsf{ob}}{}^{\mathsf{up}}(1^{\lambda},\vec{n}:=((d^{\mathsf{KP}};n_t^{\mathsf{KP}},u_t^{\mathsf{KP}},w_t^{\mathsf{KP}},z_t^{\mathsf{KP}}\,(t=1,\ldots,d^{\mathsf{KP}})),$$
$$(d^{\mathsf{CP}};n_t^{\mathsf{CP}},u_t^{\mathsf{CP}},w_t^{\mathsf{CP}},z_t^{\mathsf{CP}}\,(t=1,\ldots,d^{\mathsf{CP}}))):$$
$$\mathsf{param}_{\mathbb{G}}:=(q,\mathbb{G},\mathbb{G}_T,g,e)\xleftarrow{\mathsf{R}}\mathcal{G}_{\mathsf{bpg}}(1^{\lambda}),\quad \psi\xleftarrow{\mathsf{U}}\mathbb{R}^{\mathsf{X}},$$
$$N_0:=2+u_0+1+w_0+z_0,$$
$$N_t^{\mathsf{KP}}:=n_t^{\mathsf{KP}}+u_t^{\mathsf{KP}}+w_t^{\mathsf{KP}}+z_t^{\mathsf{KP}}\ \text{ for } t=1,\ldots,d^{\mathsf{KP}},$$
$$N_t^{\mathsf{CP}}:=n_t^{\mathsf{CP}}+u_t^{\mathsf{CP}}+w_t^{\mathsf{CP}}+z_t^{\mathsf{CP}}\ \text{ for } t=1,\ldots,d^{\mathsf{CP}},$$
$$\mathsf{param}_{\mathbb{V}_0}:=(q,\mathbb{V}_0,\mathbb{G}_T,\mathbb{A}_0,e):=\mathcal{G}_{\mathsf{dpvs}}(1^{\lambda},N_0,\mathsf{param}_{\mathbb{G}}),$$
$$X_0:=(\chi_{0,i,j})_{i,j}\xleftarrow{\mathsf{U}}GL(N_0,\mathbb{R}),\quad (\nu_{0,i,j})_{i,j}:=\psi\cdot(X_0^{\mathrm{T}})^{-1},$$
$$b_{0,i}:=(\chi_{0,i,1},\ldots,\chi_{0,i,N_0})_{\mathbb{A}_0},\ \mathbb{B}_0:=(b_{0,1},\ldots,b_{0,N_0}),$$
$$b_{0,i}^*:=(\nu_{0,i,1},\ldots,\nu_{0,i,N_0})_{\mathbb{A}_0},\ \mathbb{B}_0^*:=(b_{0,i}^*,\ldots,b_{0,N_0}^*),$$
$$\text{for } t=1,\ldots,d^{\mathsf{KP}},$$
$$\mathsf{param}_{\mathbb{V}_t^{\mathsf{KP}}}:=(q,\mathbb{V}_t^{\mathsf{KP}},\mathbb{G}_T,\mathbb{A}_t^{\mathsf{KP}},e):=\mathcal{G}_{\mathsf{dpvs}}(1^{\lambda},N_t^{\mathsf{KP}},\mathsf{param}_{\mathbb{G}}),$$
$$X_t^{\mathsf{KP}}:=(\chi_{t,i,j}^{\mathsf{KP}})_{i,j}\xleftarrow{\mathsf{U}}GL(N_t^{\mathsf{KP}},\mathbb{F}_q),\quad (\nu_{t,i,j}^{\mathsf{KP}})_{i,j}:=\psi\cdot((X_t^{\mathsf{KP}})^{\mathrm{T}})^{-1},$$
$$b_{t,i}^{\mathsf{KP}}:=(\chi_{t,i,1}^{\mathsf{KP}},\ldots,\chi_{t,i,N_t^{\mathsf{KP}}}^{\mathsf{KP}})_{\mathbb{A}_t^{\mathsf{KP}}},\ \mathbb{B}_t^{\mathsf{KP}}:=(b_{t,1}^{\mathsf{KP}},\ldots,b_{t,N_t^{\mathsf{KP}}}^{\mathsf{KP}}),$$
$$b_{t,i}^{*\mathsf{KP}}:=(\nu_{t,i,1}^{\mathsf{KP}},\ldots,\nu_{t,i,N_t^{\mathsf{KP}}}^{\mathsf{KP}})_{\mathbb{A}_t^{\mathsf{KP}}},\ \mathbb{B}_t^{*\mathsf{KP}}:=(b_{t,1}^{*\mathsf{KP}},\ldots,b_{t,N_t^{\mathsf{KP}}}^{*\mathsf{KP}}),$$
$$\text{for } t=1,\ldots,d^{\mathsf{CP}},$$
$$\mathsf{param}_{\mathbb{V}_t^{\mathsf{CP}}}:=(q,\mathbb{V}_t^{\mathsf{CP}},\mathbb{G}_T,\mathbb{A}_t^{\mathsf{CP}},e):=\mathcal{G}_{\mathsf{dpvs}}(1^{\lambda},N_t^{\mathsf{CP}},\mathsf{param}_{\mathbb{G}}),$$
$$X_t^{\mathsf{CP}}:=(\chi_{t,i,j}^{\mathsf{CP}})_{i,j}\xleftarrow{\mathsf{U}}GL(N_t^{\mathsf{CP}},\mathbb{F}_q),\quad (\nu_{t,i,j}^{\mathsf{CP}})_{i,j}:=\psi\cdot((X_t^{\mathsf{CP}})^{\mathrm{T}})^{-1},$$
$$b_{t,i}^{\mathsf{CP}}:=(\chi_{t,i,1}^{\mathsf{CP}},\ldots,\chi_{t,i,N_t^{\mathsf{CP}}}^{\mathsf{CP}})_{\mathbb{A}_t^{\mathsf{CP}}},\ \mathbb{B}_t^{\mathsf{CP}}:=(b_{t,1}^{\mathsf{CP}},\ldots,b_{t,N_t^{\mathsf{CP}}}^{\mathsf{CP}}),$$
$$b_{t,i}^{*\mathsf{CP}}:=(\nu_{t,i,1}^{\mathsf{CP}},\ldots,\nu_{t,i,N_t^{\mathsf{CP}}}^{\mathsf{CP}})_{\mathbb{A}_t^{\mathsf{CP}}},\ \mathbb{B}_t^{*\mathsf{CP}}:=(b_{t,1}^{*\mathsf{CP}},\ldots,b_{t,N_t^{\mathsf{CP}}}^{*\mathsf{CP}}),$$
$$g_T:=e(g,g)^{\psi},$$
$$\mathsf{param}_{\vec{n}}:=(\mathsf{param}_{\mathbb{V}_0},\{\mathsf{param}_{\mathbb{V}_t^{\mathsf{KP}}}\}_{t=1,\ldots,d^{\mathsf{KP}}},\{\mathsf{param}_{\mathbb{V}_t^{\mathsf{CP}}}\}_{t=1,\ldots,d^{\mathsf{CP}}},g_T)$$
$$\text{return } (\mathsf{param}_{\vec{n}},\{\mathbb{B}_0,\mathbb{B}_0^*\},\{\mathbb{B}_t^{\mathsf{KP}},\mathbb{B}_t^{*\mathsf{KP}}\}_{t=1,\ldots,d^{\mathsf{KP}}},\{\mathbb{B}_t^{\mathsf{CP}},\mathbb{B}_t^{*\mathsf{CP}}\}_{t=1,\ldots,d^{\mathsf{CP}}})$$

[0442]

[0443] [수학식 166]

$$\mathsf{Setup}(1^{\lambda},\vec{n}:=((d^{\mathsf{KP}};n_t^{\mathsf{KP}},u_t^{\mathsf{KP}},w_t^{\mathsf{KP}},z_t^{\mathsf{KP}}\,(t=1,\ldots,d^{\mathsf{KP}})),$$
$$(d^{\mathsf{CP}};n_t^{\mathsf{CP}},u_t^{\mathsf{CP}},w_t^{\mathsf{CP}},z_t^{\mathsf{CP}}\,(t=1,\ldots,d^{\mathsf{CP}}))):$$
$$(\mathsf{param}_{\vec{n}},\mathbb{B}_0,\mathbb{B}_0^*,\{\mathbb{B}_t^{\mathsf{KP}},\mathbb{B}_t^{*\mathsf{KP}}\}_{t=1,\ldots,d^{\mathsf{KP}}},$$
$$\{\mathbb{B}_t^{\mathsf{CP}},\mathbb{B}_t^{*\mathsf{CP}}\}_{t=1,\ldots,d^{\mathsf{CP}}})\xleftarrow{\mathsf{R}}\mathcal{G}_{\mathsf{ob}}(1^{\lambda},\vec{n}),$$
$$\hat{\mathbb{B}}_0:=(b_{0,1}^*,b_{0,2}^*,b_{0,2+u_0+1}^*,b_{0,2+u_0+1+w_0+1}^*,\ldots,b_{0,2+u_0+1+w_0+z_0}^*),$$
$$\hat{\mathbb{B}}_0^*:=(b_{0,1}^*,b_{0,2}^*,b_{0,2+u_0+1}^*,b_{0,2+u_0+1+1}^*,\ldots,b_{0,2+u_0+1+w_0}^*),$$
$$\text{for } t=1,\ldots,d^{\mathsf{KP}},$$
$$\hat{\mathbb{B}}_t^{\mathsf{KP}}:=(b_{t,1}^{\mathsf{KP}},\ldots,b_{t,n_t^{\mathsf{KP}}}^{\mathsf{KP}},b_{t,n_t^{\mathsf{KP}}+u_t^{\mathsf{KP}}+w_t^{\mathsf{KP}}+1}^{\mathsf{KP}},\ldots,b_{t,n_t^{\mathsf{KP}}+u_t^{\mathsf{KP}}+w_t^{\mathsf{KP}}+z_t^{\mathsf{KP}}}^{\mathsf{KP}}),$$
$$\hat{\mathbb{B}}_t^{*\mathsf{KP}}:=(b_{t,1}^{*\mathsf{KP}},\ldots,b_{t,n_t^{\mathsf{KP}}}^{*\mathsf{KP}},b_{t,n_t^{\mathsf{KP}}+u_t^{\mathsf{KP}}+1}^{*\mathsf{KP}},\ldots,b_{t,n_t^{\mathsf{KP}}+u_t^{\mathsf{KP}}+w_t^{\mathsf{KP}}}^{*\mathsf{KP}}),$$
$$\text{for } t=1,\ldots,d^{\mathsf{CP}},$$
$$\hat{\mathbb{B}}_t^{\mathsf{CP}}:=(b_{t,1}^{\mathsf{CP}},\ldots,b_{t,n_t^{\mathsf{CP}}}^{\mathsf{CP}},b_{t,n_t^{\mathsf{CP}}+u_t^{\mathsf{CP}}+w_t^{\mathsf{CP}}+1}^{\mathsf{CP}},\ldots,b_{t,n_t^{\mathsf{CP}}+u_t^{\mathsf{CP}}+w_t^{\mathsf{CP}}+z_t^{\mathsf{CP}}}^{\mathsf{CP}}),$$
$$\hat{\mathbb{B}}_t^{*\mathsf{CP}}:=(b_{t,1}^{*\mathsf{CP}},\ldots,b_{t,n_t^{\mathsf{CP}}}^{*\mathsf{CP}},b_{t,n_t^{\mathsf{CP}}+u_t^{\mathsf{CP}}+1}^{*\mathsf{CP}},\ldots,b_{t,n_t^{\mathsf{CP}}+u_t^{\mathsf{CP}}+w_t^{\mathsf{CP}}}^{*\mathsf{CP}}),$$
$$\mathsf{pk}:=(1^{\lambda},\mathsf{param}_{\vec{n}},\hat{\mathbb{B}}_0,\{\hat{\mathbb{B}}_t^{\mathsf{KP}}\}_{t=1,\ldots,d^{\mathsf{KP}}},\{\hat{\mathbb{B}}_t^{\mathsf{CP}}\}_{t=1,\ldots,d^{\mathsf{CP}}}),$$
$$\mathsf{sk}:=(\hat{\mathbb{B}}_0^*,\{\hat{\mathbb{B}}_t^{*\mathsf{KP}}\}_{t=1,\ldots,d^{\mathsf{KP}}},\{\hat{\mathbb{B}}_t^{*\mathsf{CP}}\}_{t=1,\ldots,d^{\mathsf{CP}}})$$
$$\text{return } \mathsf{pk},\mathsf{sk}$$

[0444]

[0445] [수학식 167]

$$\mathsf{KeyGen}(\mathsf{pk},\mathsf{sk},\mathbb{S}^{\mathsf{KP}}:=(M^{\mathsf{KP}},\rho^{\mathsf{KP}}),$$

$$\Gamma^{\mathsf{CP}}:=\{(t,\vec{x}_t^{\mathsf{CP}}:=(x_{t,1}^{\mathsf{CP}},\ldots,x_{t,n_t^{\mathsf{CP}}}^{\mathsf{CP}})\in\mathbb{R}^{n_t^{\mathsf{CP}}}\setminus\{\vec{0}\})$$

$$\left|1\le t\le d^{\mathsf{CP}},x_{t,1}^{\mathsf{CP}}:=1\right\})$$

$$\vec{f}^{\mathsf{KP}}\xleftarrow{\mathsf{U}}\mathbb{R}^{r^{\mathsf{KP}}},\quad(\vec{s}^{\mathsf{KP}})^{\mathrm{T}}:=(s_1^{\mathsf{KP}},\ldots,s_{L^{\mathsf{KP}}}^{\mathsf{KP}})^{\mathrm{T}}:=M^{\mathsf{KP}}\cdot(\vec{f}^{\mathsf{KP}})^{\mathrm{T}},$$

$$s_0^{\mathsf{KP}}:=\vec{1}\cdot(\vec{f}^{\mathsf{KP}})^{\mathrm{T}},$$

$$\delta^{\mathsf{CP}}\xleftarrow{\mathsf{U}}\mathbb{R},\quad\vec{\eta}_t^{\mathsf{CP}}\xleftarrow{\mathsf{U}}\mathbb{R}^{w_t^{\mathsf{CP}}}\ \text{ such that }(t,\vec{x}_t^{\mathsf{CP}})\in\Gamma^{\mathsf{CP}},$$

$$\vec{\eta}_0\xleftarrow{\mathsf{U}}\mathbb{R}^{w_0},$$

$$k_0^*:=(-s_0^{\mathsf{KP}},\delta^{\mathsf{CP}},\overbrace{0^{u_0}}^{u_0},1,\overbrace{\eta_{0,1},\ldots,\eta_{0,w_0}}^{w_0},\overbrace{0^{z_0}}^{z_0})_{\mathbb{B}_0^*},$$

$$\text{for } i=1,\ldots,L^{\mathsf{KP}},$$

$$\text{if } \rho^{\mathsf{KP}}(i)=(t,\vec{v}_i^{\mathsf{KP}}:=(v_{i,1}^{\mathsf{KP}},\ldots,v_{i,n_t^{\mathsf{KP}}}^{\mathsf{KP}})\in\mathbb{R}^{n_t^{\mathsf{KP}}}\setminus\{\vec{0}\}),$$

$$\theta_i^{\mathsf{KP}}\xleftarrow{\mathsf{U}}\mathbb{R},\quad\vec{\eta}_i^{\mathsf{KP}}\xleftarrow{\mathsf{U}}\mathbb{R}^{w_t^{\mathsf{KP}}},$$

$$k_i^{*\mathsf{KP}}:=(\overbrace{s_i^{\mathsf{KP}}\vec{e}_{t,1}^{\mathsf{KP}}+\theta_i^{\mathsf{KP}}\vec{v}_i^{\mathsf{KP}}}^{n_t^{\mathsf{KP}}},\overbrace{0^{u_t^{\mathsf{KP}}}}^{u_t^{\mathsf{KP}}},\overbrace{\vec{\eta}_i^{\mathsf{KP}}}^{w_t^{\mathsf{KP}}},\overbrace{0^{z_t^{\mathsf{KP}}}}^{z_t^{\mathsf{KP}}})_{\mathbb{B}_t^{*\mathsf{KP}}},$$

$$\text{if } \rho^{\mathsf{KP}}(i)=\neg(t,\vec{v}_i^{\mathsf{KP}}),\quad\vec{\eta}_i^{\mathsf{KP}}\xleftarrow{\mathsf{U}}\mathbb{R}^{w_t^{\mathsf{KP}}},$$

$$k_i^{*\mathsf{KP}}:=(\overbrace{s_i^{\mathsf{KP}}\vec{v}_i^{\mathsf{KP}}}^{n_t^{\mathsf{KP}}},\overbrace{0^{u_t^{\mathsf{KP}}}}^{u_t^{\mathsf{KP}}},\overbrace{\vec{\eta}_i^{\mathsf{KP}}}^{w_t^{\mathsf{KP}}},\overbrace{0^{z_t^{\mathsf{KP}}}}^{z_t^{\mathsf{KP}}})_{\mathbb{B}_t^{*\mathsf{KP}}},$$

$$\text{for }(t,\vec{x}_t^{\mathsf{CP}})\in\Gamma^{\mathsf{CP}},$$

$$k_t^{*\mathsf{CP}}:=(\overbrace{\delta^{\mathsf{CP}}\vec{x}_t^{\mathsf{CP}}}^{n_t^{\mathsf{CP}}},\overbrace{0^{u_t^{\mathsf{CP}}}}^{u_t^{\mathsf{CP}}},\overbrace{\vec{\eta}_t^{\mathsf{CP}}}^{w_t^{\mathsf{CP}}},\overbrace{0^{z_t^{\mathsf{KP}}}}^{z_t^{\mathsf{CP}}})_{\mathbb{B}_t^{*\mathsf{CP}}},$$

$$\mathsf{return}\ \mathsf{sk}_{(\mathbb{S}^{\mathsf{KP}},\Gamma^{\mathsf{CP}})}:=$$

[0446] $$(k_0^*;\mathbb{S}^{\mathsf{KP}},k_1^{*\mathsf{KP}},\ldots,k_{L^{\mathsf{KP}}}^{*\mathsf{KP}};\Gamma^{\mathsf{CP}},\{k_t^{*\mathsf{CP}}\}_{(t,\vec{x}_t^{\mathsf{CP}})\in\Gamma^{\mathsf{CP}}})$$

[0447] [수학식 168]

$$
\begin{aligned}
&\mathsf{Enc}(\mathsf{pk}, m, \Gamma^{\mathsf{KP}} :=\\
&\quad \{(t, \vec{x}_t^{\mathsf{KP}} := (x_{t,1}^{\mathsf{KP}}, \ldots, x_{t,n_t^{\mathsf{KP}}}^{\mathsf{KP}}) \in \mathbb{R}^{n_t^{\mathsf{KP}}} \setminus \{\vec{0}\}) \,\middle|\, 1 \le t \le d^{\mathsf{KP}}, x_{t,1}^{\mathsf{KP}} := 1\},\\
&\quad \mathbb{S}^{\mathsf{CP}} := (M^{\mathsf{CP}}, \rho^{\mathsf{CP}})):\\
&\qquad \omega^{\mathsf{KP}}, \zeta \xleftarrow{\mathsf{U}} \mathbb{R},\ \vec{\varphi}_0 \xleftarrow{\mathsf{U}} \mathbb{R}^{z_0},\ \vec{\varphi}_t^{\mathsf{KP}} \xleftarrow{\mathsf{U}} \mathbb{R}^{z_t^{\mathsf{KP}}} \text{ for } (t, \vec{x}_t^{\mathsf{KP}}) \in \Gamma,\\
&\qquad \vec{f}^{\mathsf{CP}} \xleftarrow{\mathsf{R}} \mathbb{R}^{r^{\mathsf{CP}}}, (\vec{s}^{\mathsf{CP}})^{\mathrm{T}} := (s_1^{\mathsf{CP}}, \ldots, s_{L^{\mathsf{CP}}}^{\mathsf{CP}})^{\mathrm{T}} := M^{\mathsf{CP}} \cdot (\vec{f}^{\mathsf{CP}})^{\mathrm{T}},\\
&\qquad s_0^{\mathsf{CP}} := \vec{1} \cdot (\vec{f}^{\mathsf{CP}})^{\mathrm{T}},\\
&\qquad c_0 := (\omega^{\mathsf{KP}}, -s_0^{\mathsf{CP}}, \overbrace{0^{u_0}}^{u_0}, \zeta, \overbrace{0^{w_0}}^{w_0}, \overbrace{\varphi_{0,1}, \ldots, \varphi_{0,z_0}}^{z_0})_{\mathbb{B}_0},\\
&\qquad \text{for } (t, \vec{x}_t^{\mathsf{KP}}) \in \Gamma^{\mathsf{KP}},\\
&\qquad\quad c_t^{\mathsf{KP}} := (\overbrace{\omega^{\mathsf{KP}} \vec{x}_t^{\mathsf{KP}}}^{n_t^{\mathsf{KP}}}, \overbrace{0^{u_t^{\mathsf{KP}}}}^{u_t^{\mathsf{KP}}}, \overbrace{0^{w_t^{\mathsf{KP}}}}^{w_t^{\mathsf{KP}}}, \overbrace{\vec{\varphi}_t^{\mathsf{KP}}}^{z_t^{\mathsf{KP}}})_{\mathbb{B}_t^{\mathsf{KP}}}\\
&\qquad\quad \text{for } i = 1, \ldots, L^{\mathsf{CP}},\\
&\qquad\quad\quad \text{if } \rho^{\mathsf{CP}}(i) = (t, \vec{v}_i^{\mathsf{CP}} := (v_{i,1}^{\mathsf{CP}}, \ldots, v_{i,n_t^{\mathsf{CP}}}^{\mathsf{CP}}) \in \mathbb{R}^{n_t^{\mathsf{CP}}} \setminus \{\vec{0}\}),\\
&\qquad\quad\quad\quad \theta_i^{\mathsf{CP}} \xleftarrow{\mathsf{U}} \mathbb{R}, \vec{\varphi}_i^{\mathsf{CP}} \xleftarrow{\mathsf{U}} \mathbb{R}^{z_t^{\mathsf{CP}}},\\
&\qquad\quad\quad\quad c_i^{\mathsf{CP}} := (\overbrace{s_i^{\mathsf{CP}} \vec{e}_{t,1}^{\mathsf{CP}} + \theta_i^{\mathsf{CP}} \vec{v}_i^{\mathsf{CP}}}^{n_t^{\mathsf{CP}}}, \overbrace{0^{u_t^{\mathsf{CP}}}}^{u_t^{\mathsf{CP}}}, \overbrace{0^{w_t^{\mathsf{CP}}}}^{w_t^{\mathsf{CP}}}, \overbrace{\vec{\varphi}_i^{\mathsf{CP}}}^{z_t^{\mathsf{CP}}})_{\mathbb{B}_t^{\mathsf{CP}}},\\
&\qquad\quad\quad \text{if } \rho^{\mathsf{CP}}(i) = \neg(t, \vec{v}_i^{\mathsf{CP}}),\ \vec{\varphi}_i^{\mathsf{CP}} \xleftarrow{\mathsf{U}} \mathbb{R}^{z_t^{\mathsf{CP}}},\\
&\qquad\quad\quad\quad c_i^{\mathsf{CP}} := (\overbrace{s_i^{\mathsf{CP}} \vec{v}_i^{\mathsf{CP}}}^{n_t^{\mathsf{CP}}}, \overbrace{0^{u_t^{\mathsf{CP}}}}^{u_t^{\mathsf{CP}}}, \overbrace{0^{w_t^{\mathsf{CP}}}}^{w_t^{\mathsf{CP}}}, \overbrace{\vec{\varphi}_i^{\mathsf{CP}}}^{z_t^{\mathsf{CP}}})_{\mathbb{B}_t^{\mathsf{CP}}},\\
&\qquad c_{d+1} := g_T^{\zeta} m,\\
&\qquad \mathsf{return}\ \mathsf{ct}_{(\Gamma^{\mathsf{KP}}, \mathbb{S}^{\mathsf{CP}})} :=\\
&\qquad\quad (c_0; \Gamma^{\mathsf{KP}}, \{c_t^{\mathsf{KP}}\}_{(t, \vec{x}_t^{\mathsf{KP}}) \in \Gamma^{\mathsf{KP}}}; \mathbb{S}^{\mathsf{CP}}, c_1^{\mathsf{CP}}, \ldots, c_{L^{\mathsf{CP}}}^{\mathsf{CP}}; c_{d+1})
\end{aligned}
$$

[0448]

[0449] [수학식 169]

$$
\begin{aligned}
&\mathrm{Dec}(\mathrm{pk},\\
&\quad \mathrm{sk}_{(\mathbb{S}^{KP},\Gamma^{CP})} := (k_0^*;\mathbb{S}^{KP},k_1^{*KP},\ldots,k_{L^{KP}}^{*KP};\Gamma^{CP},\{k_t^{*CP}\})_{(t,\vec{x}_t^{CP})\in\Gamma^{CP}}),\\
&\quad \mathrm{ct}_{(\Gamma^{KP},\mathbb{S}^{CP})} := (c_0;\Gamma^{KP},\{c_t^{KP}\}_{(t,\vec{x}_t^{KP})\in\Gamma^{KP}};\mathbb{S}^{CP},c_1^{CP},\ldots,c_{L^{CP}}^{CP};c_{d+1})):\\
&\quad \text{If } \mathbb{S}^{KP} := (M^{KP},\rho^{KP}) \text{ accepts } \Gamma^{KP} := \{(t,\vec{x}_t^{KP})\}\\
&\quad\ \text{and } \mathbb{S}^{CP} := (M^{CP},\rho^{CP}) \text{ accepts } \Gamma^{CP} := \{(t,\vec{x}_t^{CP})\},\\
&\quad \text{then compute } (I^{KP},\{\alpha_i^{KP}\}_{i\in I^{KP}}) \text{ and } (I^{CP},\{\alpha_i^{CP}\}_{i\in I^{CP}}) \text{ such that}\\
&\qquad \vec{1}=\textstyle\sum_{i\in I}\alpha_i^{KP}M_i^{KP}, \text{ where } M_i^{KP} \text{ is the } i-\text{th row of } M^{KP}, \text{and}\\
&\qquad I^{KP}\subseteq\{i\in\{1,\ldots,L^{KP}\}\\
&\qquad\quad \big|[\rho^{KP}(i)=(t,\vec{v}_i^{KP})\wedge(t,\vec{x}_t^{KP})\in\Gamma^{KP}\wedge\vec{v}_i^{KP}\cdot\vec{x}_t^{KP}=0]\\
&\qquad\quad \vee[\rho^{KP}(i)=\neg(t,\vec{v}_i^{KP})\wedge(t,\vec{x}_t^{KP})\in\Gamma^{KP}\wedge\vec{v}_i^{KP}\cdot\vec{x}_t^{KP}\neq 0]\}, \text{and}\\
&\qquad \vec{1}=\textstyle\sum_{i\in I}\alpha_i^{CP}M_i^{CP}, \text{ where } M_i^{CP} \text{ is the } i-\text{th row of } M^{CP}, \text{and}\\
&\qquad I^{CP}\subseteq\{i\in\{1,\ldots,L^{CP}\}\\
&\qquad\quad \big|[\rho^{CP}(i)=(t,\vec{v}_i^{CP})\wedge(t,\vec{x}_t^{CP})\in\Gamma^{CP}\wedge\vec{v}_i^{CP}\cdot\vec{x}_t^{CP}=0]\\
&\qquad\quad \vee[\rho^{CP}(i)=\neg(t,\vec{v}_i^{CP})\wedge(t,\vec{x}_t^{CP})\in\Gamma^{CP}\wedge\vec{v}_i^{CP}\cdot\vec{x}_t^{CP}\neq 0]\},\\
&\quad K := e(c_0,k_0^*)\cdot\\
&\qquad \prod_{i\in I^{KP}\wedge\rho^{KP}(i)=(t,\vec{v}_i^{KP})} e(c_t^{KP},k_i^{*KP})^{\alpha_i^{KP}}\cdot\\
&\qquad \prod_{i\in I^{KP}\wedge\rho^{KP}(i)=\neg(t,\vec{v}_i^{KP})} e(c_t^{KP},k_i^{*KP})^{\alpha_i^{KP}/(\vec{v}_i^{KP}\cdot\vec{x}_t^{KP})}\cdot\\
&\qquad \prod_{i\in I^{CP}\wedge\rho^{CP}(i)=(t,\vec{v}_i^{CP})} e(c_t^{CP},k_i^{*CP})^{\alpha_i^{CP}}\cdot\\
&\qquad \prod_{i\in I^{CP}\wedge\rho^{CP}(i)=\neg(t,\vec{v}_i^{CP})} e(c_t^{CP},k_i^{*CP})^{\alpha_i^{CP}/(\vec{v}_i^{CP}\cdot\vec{x}_t^{CP})},
\end{aligned}
$$

[0450] return $m' := c_{d+1}/K$

[0451] 또한, 상기 설명에 있어서의 암호 처리는, 권한의 위양을 행하는 것도 가능하다. 권한의 위양이란, 복호 키를 갖는 자가 그 복호 키보다 권한이 약한 하위의 복호 키를 생성하는 것이다. 여기서, 권한이 약하다는 것은, 복호할 수 있는 암호화 데이터가 한정된다고 하는 의미이다.

[0452] 예컨대, 제 1 계층째(최상위)에 있어서는, t=1의 기저 B_t와 기저 B^*_t를 이용하고, 제 2 계층째에 있어서는, t=1, 2의 기저 B_t와 기저 B^*_t를 이용하고, …, 제 k 계층째에 있어서는, t=1, …, k의 기저 B_t와 기저 B^*_t를 이용한다. 이용하는 기저 B_t와 기저 B^*_t가 늘어나는 만큼, 속성 정보가 많이 설정되게 된다. 따라서, 보다 복호 키의 권한이 한정되게 된다.

[0453] 다음으로, 실시의 형태에 있어서의 암호 처리 시스템(10)(키 생성 장치(100), 암호화 장치(200), 복호 장치(300))의 하드웨어 구성에 대하여 설명한다.

[0454] 도 13은, 키 생성 장치(100), 암호화 장치(200), 복호 장치(300)의 하드웨어 구성의 일례를 나타내는 도면이다.

[0455] 도 13에 나타내는 바와 같이, 키 생성 장치(100), 암호화 장치(200), 복호 장치(300)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, 이들의 하드웨어 디바이스를 제어한다. 자기 디스크 장치(920)(고정 디스크 장치) 대신에, 광 디스크 장치, 메모리카드 읽기/쓰기 장치 등의 기억 장치라도 좋다. 자기 디스크 장치(920)는, 소정의 고정 디스크 인터페이스를 통해 접속된다.

[0456] 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 보

드(915)는, 입력 장치의 일례이다. 또한, 통신 보드(915)는, 통신 장치의 일례이다. 또한, LCD(901)는, 표시 장치의 일례이다.

[0457] 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.

[0458] 프로그램군(923)에는, 상기의 설명에 있어서 「마스터 키 생성부(110)」, 「정보 입력부(130)」, 「복호 키 생성부(140)」, 「키 배포부(150)」, 「공개 파라미터 취득부(210)」, 「정보 입력부(220)」, 「암호화 데이터 생성부(230)」, 「데이터 송신부(240)」, 「복호 키 취득부(310)」, 「데이터 수신부(320)」, 「스팬 프로그램 계산부(330)」, 「보완 계수 계산부(340)」, 「페어링 연산부(350)」, 「메시지 계산부(360)」 등으로서 설명한 기능을 실행하는 소프트웨어나 프로그램이나 기타 프로그램이 기억되어 있다. 프로그램은, CPU(911)에 의해 판독되어 실행된다.

[0459] 파일군(924)에는, 상기의 설명에 있어서 「공개 파라미터 pk」, 「마스터 키 sk」, 「암호화 데이터 $ct_{(\Gamma KP,\ SCP)}$」, 「복호 키 $sk_{(SKP,\ \Gamma CP)}$」, 「액세스 스트럭쳐 S^{KP}, S^{CP}」, 「속성의 집합 Γ^{KP}, Γ^{CP}」, 「메시지 m」 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, 읽기/쓰기 회로를 통해 CPU(911)에 의해 메인메모리나 캐시메모리에 판독되고, 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 중, 정보나 데이터나 신호치나 변수치나 파라미터는, 메인메모리나 캐시메모리나 버퍼메모리에 일시적으로 기억된다.

[0460] 또한, 상기의 설명에 있어서의 플로차트의 화살표의 부분은 주로 데이터나 신호의 입출력을 나타내고, 데이터나 신호치는, RAM(914)의 메모리, 기타 광 디스크 등의 기록 매체나 IC 칩에 기록된다. 또한, 데이터나 신호는, 버스(912)나 신호선이나 케이블 기타 전송 매체나 전파에 의해 온라인 전송된다.

[0461] 또한, 상기의 설명에 있어서 「~부」로서 설명하는 것은, 「~회로」, 「~장치」, 「~기기」, 「~수단」, 「~기능」이더라도 좋고, 또한, 「~단계」, 「~수순」, 「~처리」이더라도 좋다. 또한, 「~장치」로서 설명하는 것은, 「~회로」, 「~기기」, 「~수단」, 「~기능」이더라도 좋고, 또한, 「~단계」, 「~수순」, 「~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 실시되더라도 상관없다. 펌웨어와 소프트웨어는, 프로그램으로서, ROM(913)등의 기록 매체에 기억된다. 프로그램은 CPU(911)에 의해 판독되고, CPU(911)에 의해 실행된다. 즉, 프로그램은, 상기에서 말한 「~부」로서 컴퓨터 등을 기능시키는 것이다. 혹은, 상기에서 말한 「~부」의 수순이나 방법을 컴퓨터 등에 실행시키는 것이다.

부호의 설명

[0462]

10 : 암호 처리 시스템

100 : 키 생성 장치

110 : 마스터 키 생성부

120 : 마스터 키 기억부

130 : 정보 입력부

131 : KP 정보 입력부

132 : CP 정보 입력부

140 : 복호 키 생성부

141 : f 벡터 생성부

142 : s 벡터 생성부

143 : 난수 생성부

144 : 주 복호 키 생성부

145 : KP 복호 키 생성부

146 : CP 복호 키 생성부

150 : 키 배포부

200 : 암호화 장치

210 : 공개 파라미터 취득부

220 : 정보 입력부

221 : KP 정보 입력부

222 : CP 정보 입력부

223 : 메시지 입력부

230 : 암호화 데이터 생성부

231 : f 벡터 생성부

232 : s 벡터 생성부

233 : 난수 생성부

234 : 주 암호화 데이터 생성부

235 : KP 암호화 데이터 생성부

236 : CP 암호화 데이터 생성부

237 : 메시지 암호화 데이터 생성부

240 : 데이터 송신부

300 : 복호 장치

310 : 복호 키 취득부

320 : 데이터 수신부

330 : 스팬 프로그램 계산부

331 : KP 스팬 프로그램 계산부

332 : CP 스팬 프로그램 계산부

340 : 보완 계수 계산부

341 : KP 보완 계수 계산부

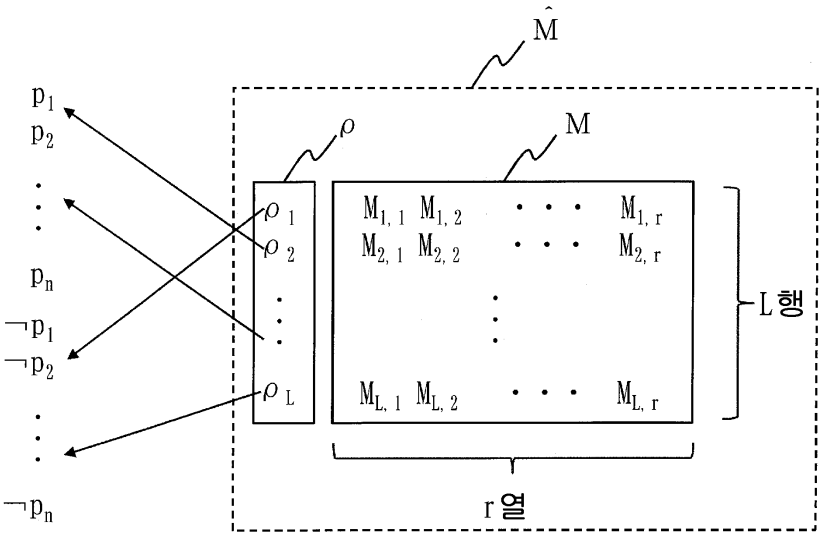
342 : CP 보완 계수 계산부

350 : 페어링 연산부

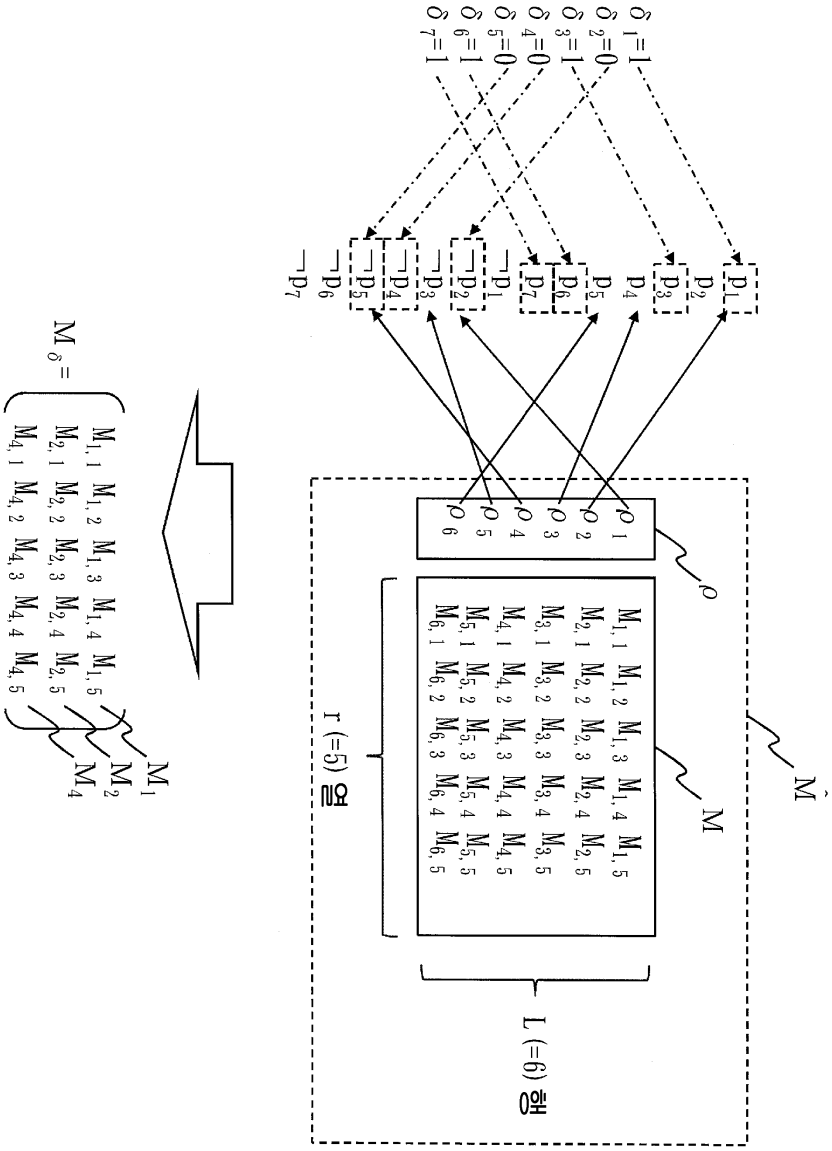
360 : 메시지 계산부

도면

도면1



도면2



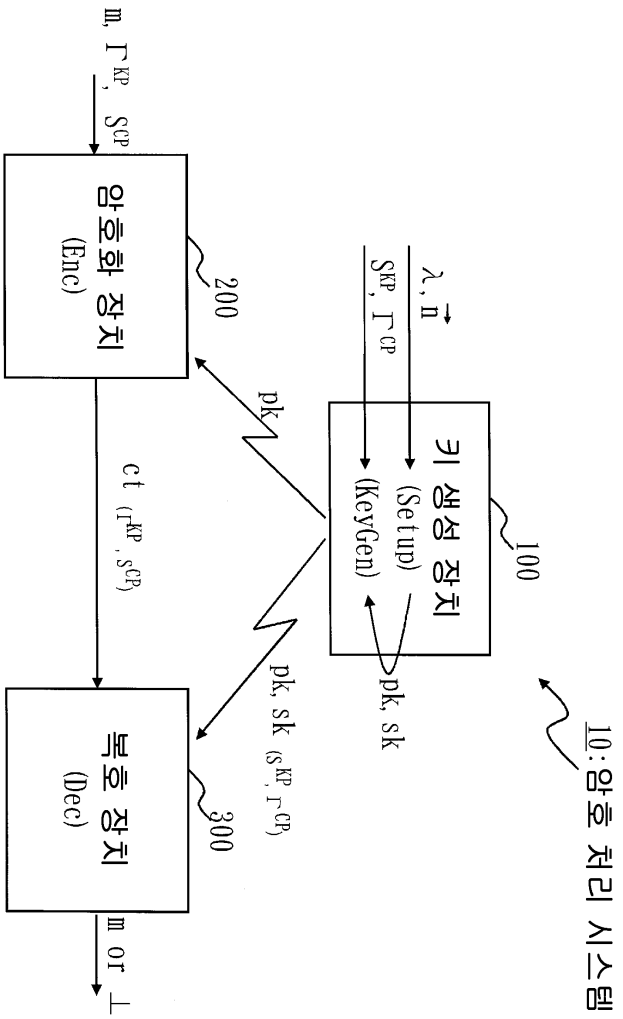
도면3

$$s_0 = \underbrace{(1, \ldots, 1)}_{\text{r 열}} \begin{pmatrix} f_1 \\ \cdot \\ \cdot \\ \cdot \\ f_r \end{pmatrix} = \sum_{k=1}^{r} f_k$$

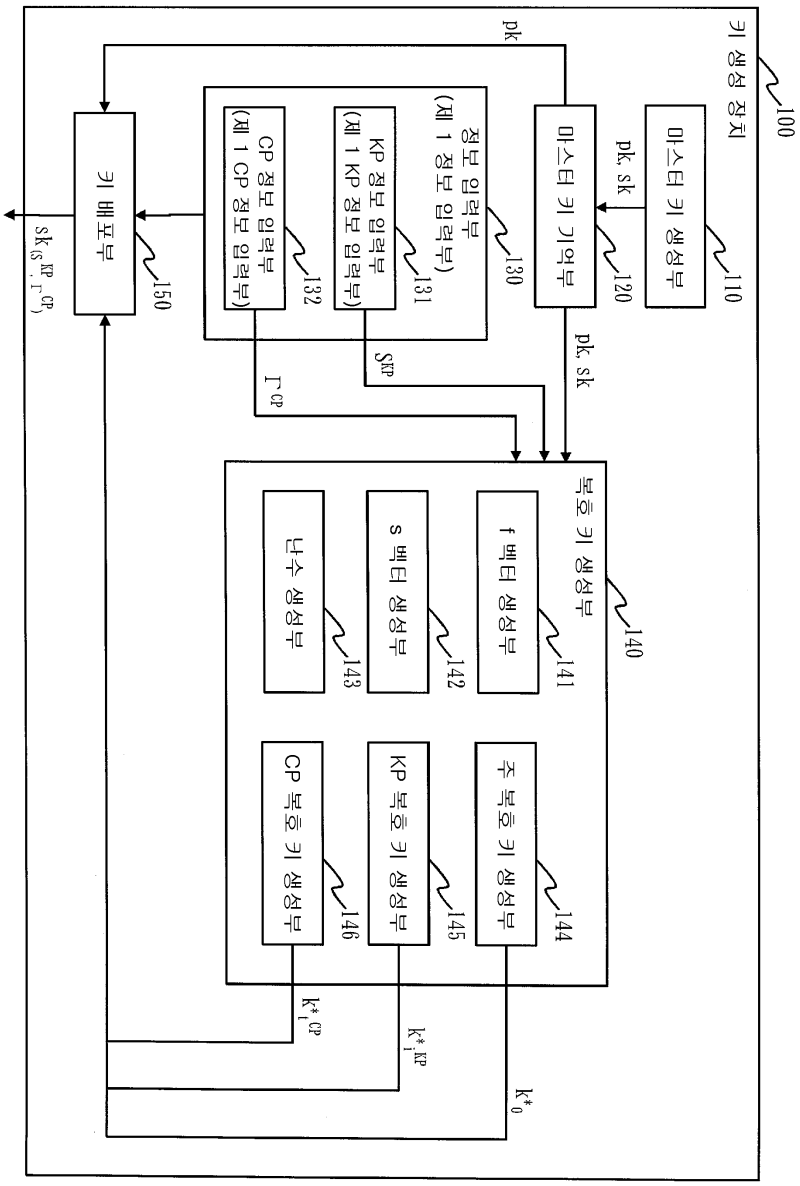
도면4

$$\vec{s}^{T} = \begin{pmatrix} M_{1,1} & M_{1,2} & \cdots & M_{1,r} \\ M_{2,1} & M_{2,2} & \cdots & M_{2,r} \\ & & \vdots & \\ M_{L,1} & M_{L,2} & \cdots & M_{L,r} \end{pmatrix} \begin{pmatrix} f_1 \\ \vdots \\ f_r \end{pmatrix} = \begin{pmatrix} s_1 \\ \vdots \\ s_r \end{pmatrix}$$

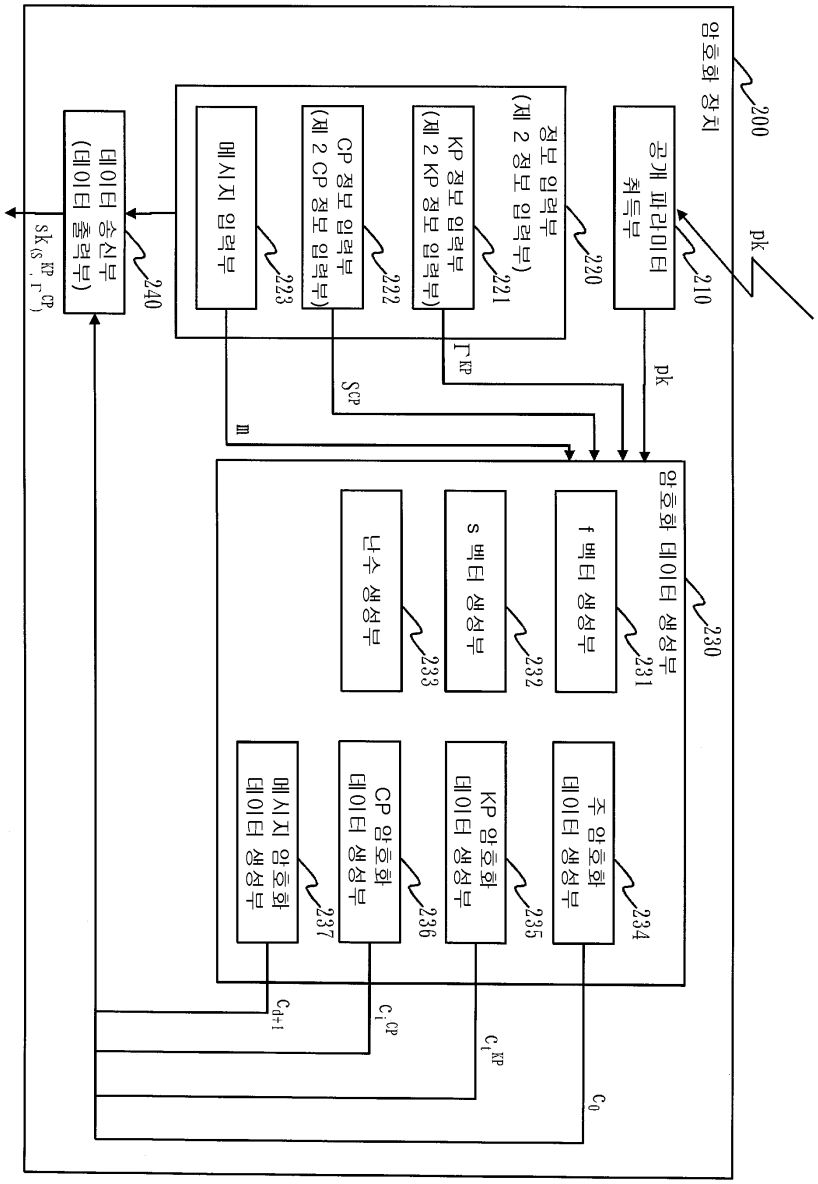
도면5



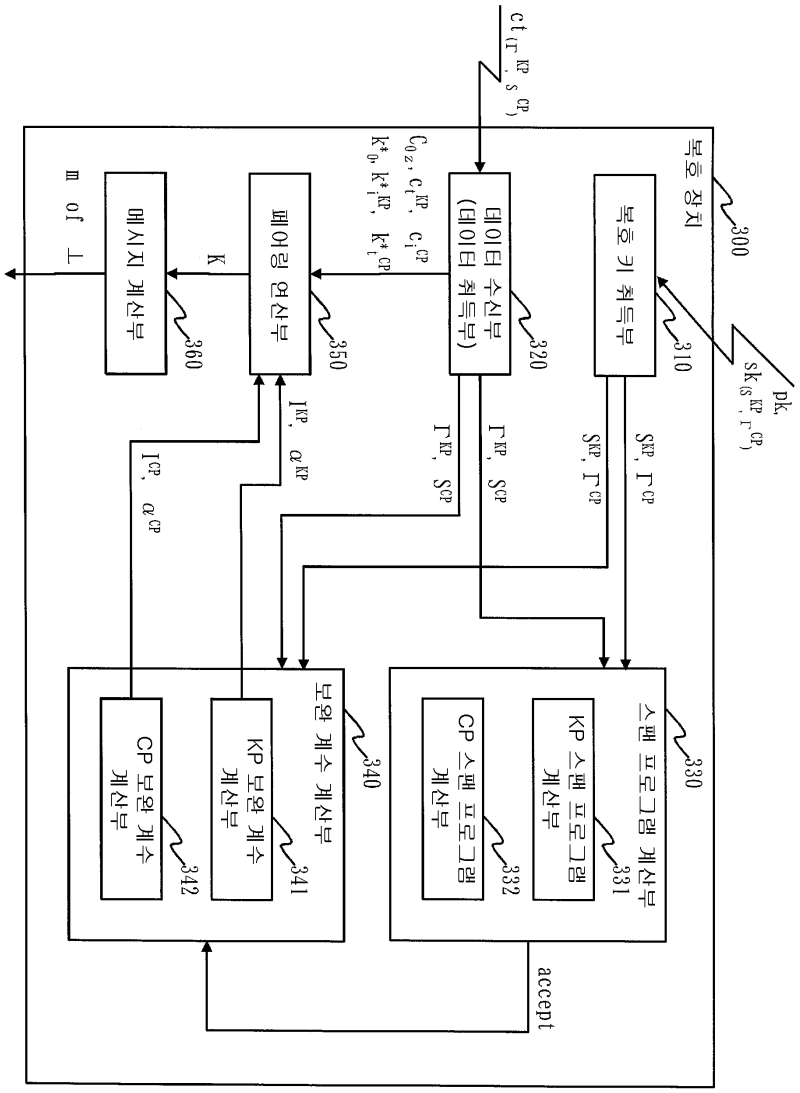
도면6


키 생성 장치
100
마스터 키 생성부
110
마스터 키 기억부
120
pk, sk
pk
정보 입력부
(제 1 정보 입력부)
130
KP 정보 입력부
(제 1 KP 정보 입력부)
131
CP 정보 입력부
(제 1 CP 정보 입력부)
132
키 배포부
150
$sk_{S^{KP}, \Gamma^{CP}}$
S^{KP}
Γ^{CP}
pk, sk
복호 키 생성부
140
f 벡터 생성부
141
s 벡터 생성부
142
난수 생성부
143
주 복호 키 생성부
144
KP 복호 키 생성부
145
CP 복호 키 생성부
146
k^{*}_{0}
$k^{*}_{1}{}^{KP}$
$k^{*}_{1}{}^{CP}$

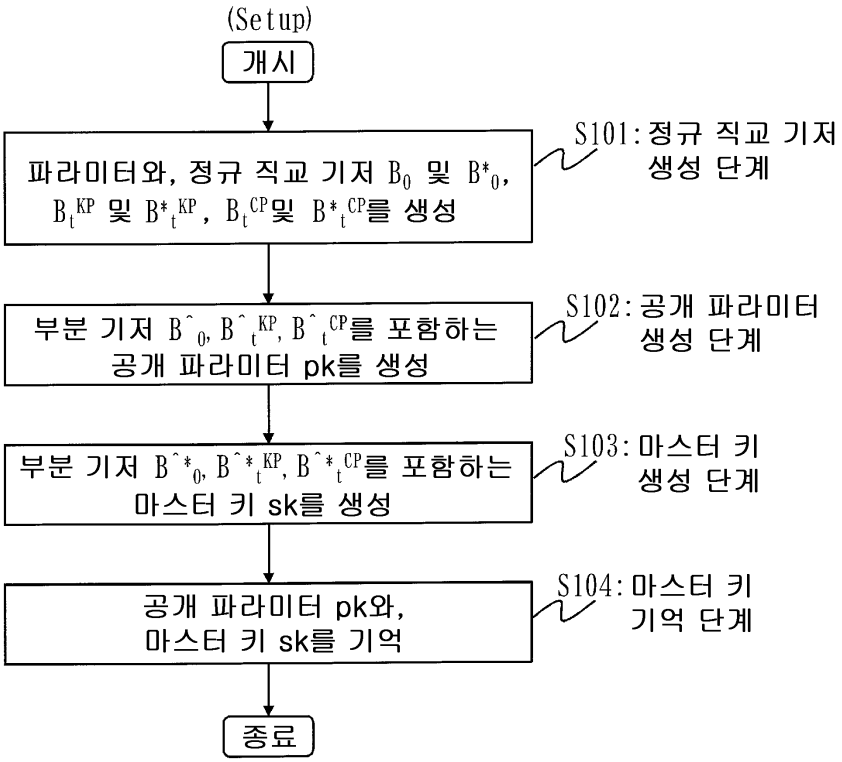
도면7


암호화 장치
200
공개 파라미터 취득부
210
pk
정보 입력부 (제 2 정보 입력부)
220
KP 정보 입력부 (제 2 KP 정보 입력부)
221
CP 정보 입력부 (제 2 CP 정보 입력부)
222
메시지 입력부
223
데이터 송신부 (데이터 출력부)
240
암호화 데이터 생성부
230
f 벡터 생성부
231
s 벡터 생성부
232
난수 생성부
233
주 암호화 데이터 생성부
234
KP 암호화 데이터 생성부
235
CP 암호화 데이터 생성부
236
메시지 암호화 데이터 생성부
237

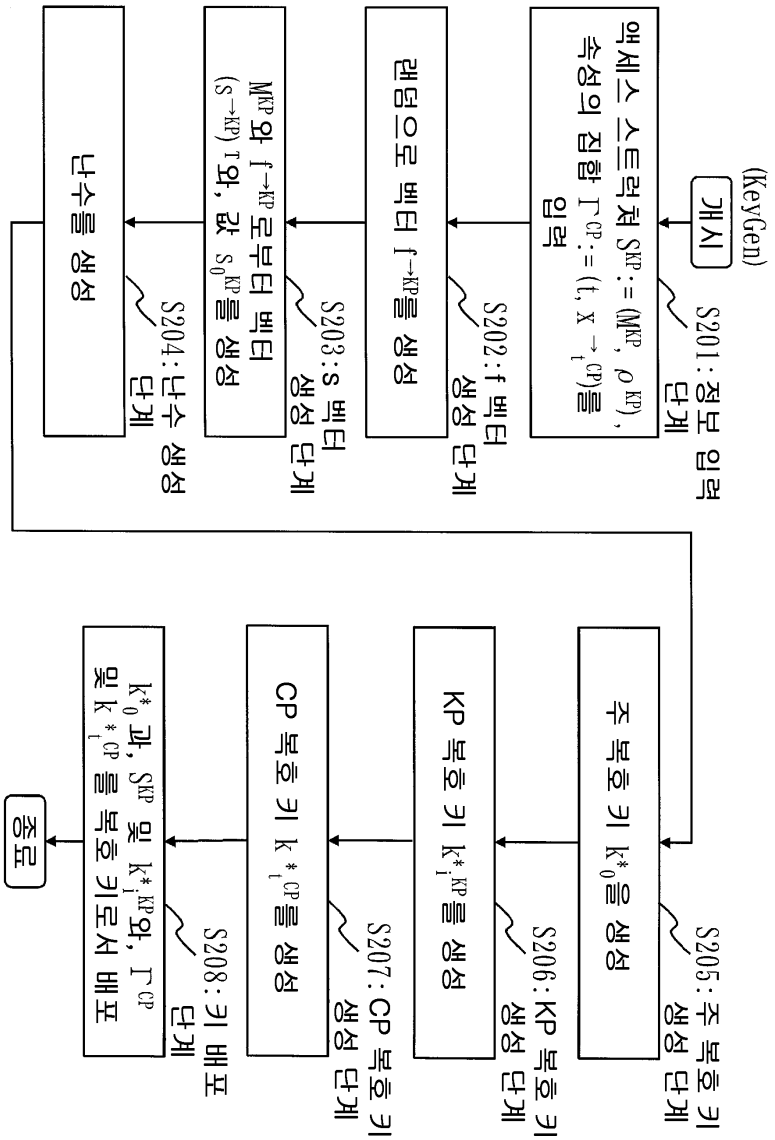
도면8


복호 장치
300
복호 키 취득부
310
데이터 수신부
(데이터 취득부)
320
페어링 연산부
350
메시지 계산부
360
스팸 프로그램 계산부
330
KP 스팸 프로그램
계산부
331
CP 스팸 프로그램
계산부
332
보완 계수 계산부
340
KP 보완 계수
계산부
341
CP 보완 계수
계산부
342
accept

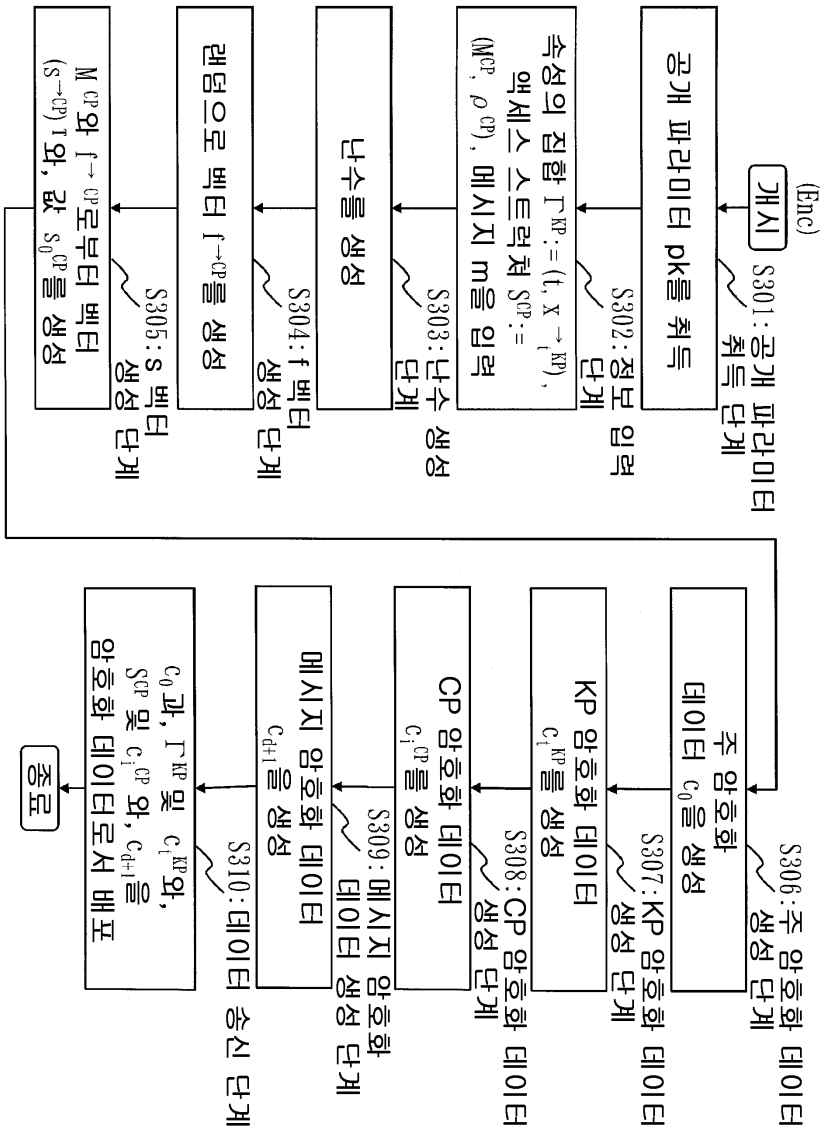
도면9


(Setup)
개시
파라미터와, 정규 직교 기저 B_0 및 B^*_0, B_t^{KP} 및 $B^{*}_t{}^{KP}$, B_t^{CP}및 $B^{*}_t{}^{CP}$를 생성
S101: 정규 직교 기저 생성 단계
부분 기저 $\hat{B}_0$, $\hat{B}_t^{KP}$, $\hat{B}_t^{CP}$를 포함하는 공개 파라미터 pk를 생성
S102: 공개 파라미터 생성 단계
부분 기저 $\hat{B}^*_0$, $\hat{B}^{*}_t{}^{KP}$, $\hat{B}^{*}_t{}^{CP}$를 포함하는 마스터 키 sk를 생성
S103: 마스터 키 생성 단계
공개 파라미터 pk와, 마스터 키 sk를 기억
S104: 마스터 키 기억 단계
종료

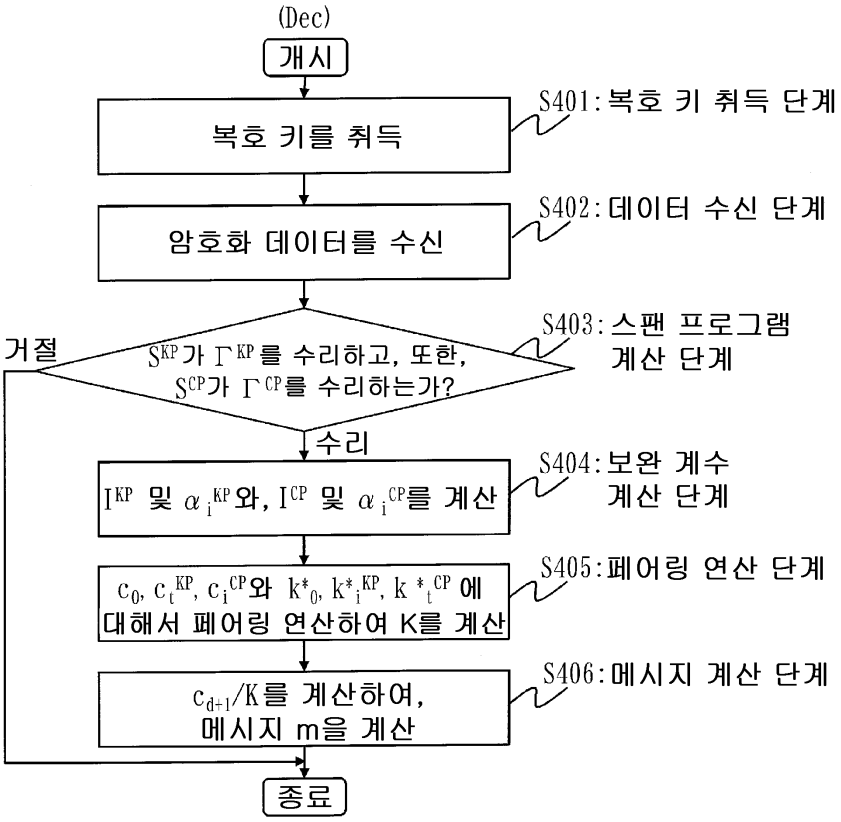
도면10


(KeyGen)
개시
S201 : 정보 입력 단계
액세스 스트럭쳐 $S^{KP} := (M^{KP}, \rho^{KP})$, 속성의 집합 $\Gamma^{CP} := (t, x \rightarrow {}_t{}^{CP})$를 입력
S202 : f 벡터 생성 단계
랜덤으로 벡터 $f^{\rightarrow KP}$를 생성
S203 : s 벡터 생성 단계
M^{KP}와 $f^{\rightarrow KP}$로부터 벡터 $(s^{\rightarrow KP})^T$와, 값 s_0^{KP}를 생성
S204 : 난수 생성 단계
난수를 생성
S205 : 주 복호 키 생성 단계
주 복호 키 k^*_0을 생성
S206 : KP 복호 키 생성 단계
KP 복호 키 k^{*KP}_i를 생성
S207 : CP 복호 키 생성 단계
CP 복호 키 k^{*CP}_t를 생성
S208 : 키 배포 단계
k^*_0과, S^{KP} 및 k^{*KP}_i와, Γ^{CP} 및 k^{*CP}_t를 복호 키로서 배포
종료

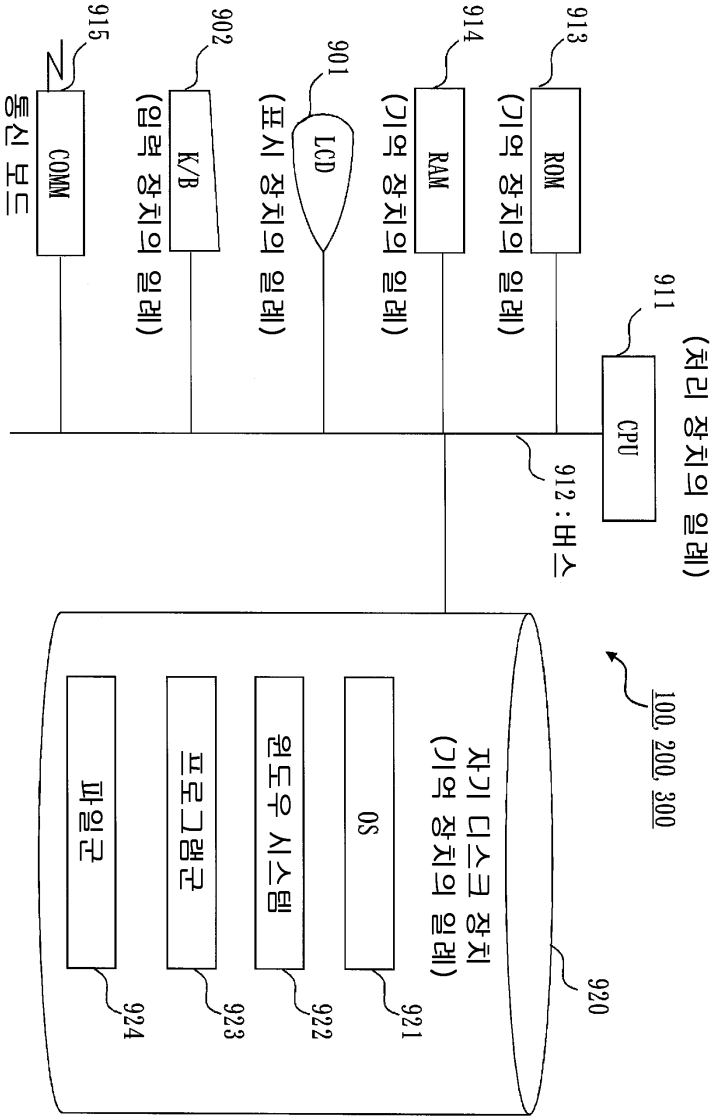
도면11


(Enc)
개시
S301 : 공개 파라미터 취득 단계
공개 파라미터 pk를 취득
S302 : 정보 입력 단계
속성의 집합 $\Gamma^{KP} := (t, X \rightarrow {}_{t}^{KP})$, 액세스 스트럭쳐 $S^{CP} :=$ (M^{CP}, ρ^{CP}), 메시지 m을 입력
S303 : 난수 생성 단계
난수를 생성
S304 : f 벡터 생성 단계
랜덤으로 벡터 $f \rightarrow {}^{CP}$를 생성
S305 : s 벡터 생성 단계
M^{CP}와 $f \rightarrow {}^{CP}$로부터 벡터 $(S \rightarrow {}^{CP})T$와, 값 $S_0{}^{CP}$를 생성
S306 : 주 암호화 데이터 생성 단계
주 암호화 데이터 C_0을 생성
S307 : KP 암호화 데이터 생성 단계
KP 암호화 데이터 C_t^{KP}를 생성
S308 : CP 암호화 데이터 생성 단계
CP 암호화 데이터 C_i^{CP}를 생성
S309 : 메시지 암호화 데이터 생성 단계
메시지 암호화 데이터 C_{d+1}을 생성
S310 : 데이터 송신 단계
C_0과, Γ^{KP} 및 C_t^{KP}와, S^{CP} 및 C_i^{CP}와, C_{d+1}을 암호화 데이터로서 배포
종료

도면12


(Dec)
개시
복호 키를 취득
S401: 복호 키 취득 단계
암호화 데이터를 수신
S402: 데이터 수신 단계
거절
S^{KP}가 Γ^{KP}를 수리하고, 또한,
S^{CP}가 Γ^{CP}를 수리하는가?
S403: 스팬 프로그램 계산 단계
수리
I^{KP} 및 α_i^{KP}와, I^{CP} 및 α_i^{CP}를 계산
S404: 보완 계수 계산 단계
c_0, c_t^{KP}, c_i^{CP}와 k^*_0, $k^*_i{}^{KP}$, $k^*_t{}^{CP}$ 에 대해서 페어링 연산하여 K를 계산
S405: 페어링 연산 단계
c_{d+1}/K를 계산하여, 메시지 m을 계산
S406: 메시지 계산 단계
종료

도면13


915
통신 보드
COMM
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
920
자기 디스크 장치
(기억 장치의 일례)
921
OS
922
윈도우 시스템
923
프로그램군
924
파일군