(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0036727
(43) 공개일자 2020년04월07일

(51) 국제특허분류(Int. Cl.)
H04L 9/30 (2006.01) *H04L 9/06* (2006.01)
H04L 9/08 (2006.01)
(52) CPC특허분류
H04L 9/3033 (2013.01)
H04L 9/0618 (2013.01)
(21) 출원번호 10-2019-0102150
(22) 출원일자 2019년08월21일
심사청구일자 2019년08월21일
(30) 우선권주장
107134068 2018년09월27일 대만(TW)

(71) 출원인
네이셔널 치아오 텅 유니버시티
중화민국 대만 신츄 시티 타 슈에 로드 1001호
(72) 발명자
폰타자 로다스 리카르도 네프탈리
대만 타이페이 시티 다안 디스트릭트 지룽 로드 섹터 3 넘버 75 빌딩 에이 룸 626
린 잉-달
대만 타이페이 시티 중정 디스트릭트 헤티 리 진먼 스트리트 넘버 9-19 6층-1
(74) 대리인
리앤목특허법인

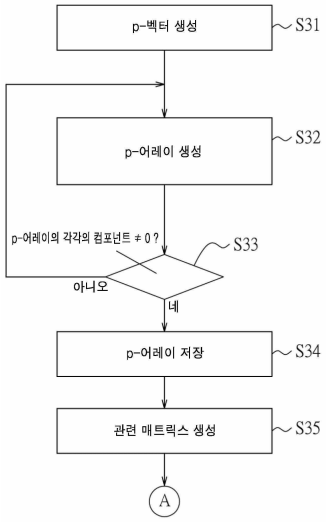
전체 청구항 수 : 총 16 항

(54) 발명의 명칭 **프라임 모듈로 이중 캡슐화에 기초한 일대다 분산 키 관리 기능을 갖춘 포스트 퀀텀 비대칭 키 암호 시스템**

(57) 요 약

포스트-퀀텀 비대칭 키 생성 방법 및 시스템에서, 처리 유닛은 프라임 및 산술 함수 또는 클래식 스트링에 기초하여, 무한한 개수의 성분들을 갖는 프라임 벡터를 생성하며(S31), 프라임 벡터에 기초하여 p-어레이를 생성하며(S32), 프라임 어레이에 기초하여 관련 매트릭스를 생성하며(S35), 관련 매트릭스 및 제1 기준 프라임에 기초하여, 개인키 역할을 하는 제1 기준 인버스 프라임 어레이를 획득하며(S38), 그리고 제2 기준 인버스 프라임 어레이에 기초하여 개인키와 쌍을 이루는 공개키를 획득한다(S40). 제2 기준 인버스 프라임 어레이는 관련 매트릭스, 제1 기준 프라임, 제2 기준 프라임 및 랜덤화 어레이에 기초하여 획득된다.

대 표 도 - 도3



(52) CPC특허분류
H04L 9/0825 (2013.01)
H04L 9/0852 (2013.01)
H04L 2209/08 (2013.01)

명 세 서

청구범위

청구항 1

처리 유닛에 의해 구현되는 포스트-퀀텀 비대칭 키 생성 방법으로서,

A) 프라임 p 그리고 시드 역할을 하는 클래식 스트링(classical string) 및 산술 함수 중 하나에 기초하여, 프라임 p와 관련되고 무한한 개수의 성분들을 갖는 p-벡터($\vec{f}_p$)를 생성하는 단계로서, 상기 p-벡터($\vec{f}_p$)는 $\vec{f}_p := [f(p^0), f(p^1), f(p^2), f(p^3), \ldots]$ 로 정의되는데, f는 상기 시드 역할을 하는 클래식 스트링 및 산술 함수 중 상기 하나를 나타내는, 단계;

B) p-벡터($\vec{f}_p$)에 기초하여, m 개의 성분들을 갖고 프라임 p와 관련되는 p-어레이($\overleftrightarrow{f}_p\big|_{s,t}^{m}$)를 생성하는 단계로서, 상기 p-어레이($\overleftrightarrow{f}_p\big|_{s,t}^{m}$)는 $\overleftrightarrow{f}_p\big|_{s,t}^{m} := \sum_{i=0}^{t}\left[f\left(p^{s+im}\right), \ldots, f\left(p^{s+im+(m-1)}\right)\right]$ 로 정의되며, 파라미터들 m, s 및 t 각각은 사용자-정의되는 양의 정수이며, 그리고 프라임 p 및 파라미터들 s, t는 협력하여 제1 파라미터 세트(I)를 구성하며, 상기 p-어레이($\overleftrightarrow{f}_p\big|_{s,t}^{m}$)는 $\overleftrightarrow{f}\big|^{m}$ 로도 표현되는, 단계;

C) 상기 p-어레이($\overleftrightarrow{f}\big|^{m}$)에 기초하여, 관련 매트릭스($\left[\overleftrightarrow{f}\big|^{m}\right]$)를 생성하는 단계로서, 상기 관련 매트릭스($\left[\overleftrightarrow{f}\big|^{m}\right]$)는 :

$$\left[\overleftrightarrow{f}\big|^{m}\right] = \begin{pmatrix} \overleftrightarrow{f}\big|^{m}(0) & \overleftrightarrow{f}\big|^{m}(1) & \cdots & \overleftrightarrow{f}\big|^{m}(m-1) \\ \overleftrightarrow{f}\big|^{m}(m-1) & \overleftrightarrow{f}\big|^{m}(0) & \cdots & \overleftrightarrow{f}\big|^{m}(m-2) \\ \vdots & \vdots & \ddots & \vdots \\ \overleftrightarrow{f}\big|^{m}(1) & \overleftrightarrow{f}\big|^{m}(2) & \cdots & \overleftrightarrow{f}\big|^{m}(0) \end{pmatrix}$$

로 정의되는데, $\overleftrightarrow{f}\big|^{m}$ (j)는 p-어레이의 m 개의 성분들 중 (j+1) 번째 성분을 나타내고, $0 \leq j \leq (m-1)$인, 단계;

D) 관련 매트릭스 $\left[\overleftrightarrow{f}\big|^{m}\right]$ 와 사용자-정의된 양의 정수인 모듈러스 ℓ 에 기초하여, 상기 모듈러스 ℓ 에 대하여 인버스 p-어레이($\overleftrightarrow{F}_\ell\big|^{m}$)를 생성하는 단계로서, 상기 인버스 p-어레이($\overleftrightarrow{F}_\ell\big|^{m}$)는 $\overleftrightarrow{F}_\ell\big|^{m} := \left(L_\ell[1, 0, \cdots, 0]\left[\overleftrightarrow{f}\big|^{m}\right]^*\right) \pmod{\ell}$ 로 정의되는데, L_ℓ 는 상기 모듈러스 ℓ 에 대한 관련 매트릭스 $\left[\overleftrightarrow{f}\big|^{m}\right]$ 의 행렬식(determinant)의 인버스 모듈러스를 나타내며, $L_\ell := \left(\det\left[\overleftrightarrow{f}\big|^{m}\right]\right)^{-1} \pmod{\ell}$ 로 정의되고, 그리고 $\left[\overleftrightarrow{f}\big|^{m}\right]^*$ 는 상기 관련 매트릭스 $\left[\overleftrightarrow{f}\big|^{m}\right]$ 의 수반 행렬(adjoint matrix)을 나타내는, 단계;

E) 제1 기준 프라임(p_1)을 임의로 선택하고, 그리고 상기 제1 기준 프라임(p_1), b로 표시되는 p-어레이 $\overleftrightarrow{f}\Big|^m$ 의 m 개의 성분들 중 가장 큰 것, 제1 기준 양의 정수($\tilde{a}$) 그리고 파라미터(m), 제2 기준 양의 정수($\tilde{b}$) 및 제3 기준 양의 정수(r)로 구성된 제2 파라미터 세트(S)와 관련된 미리 결정된 기준에 기초하여 제2 기준 프라임(p_2)을 결정하는 단계로서, 상기 미리 결정된 기준은 $p_2 > \max(p_1 m\tilde{a}\tilde{b}, mbr)$ 을 포함하는, 단계;

F) 제1 기준 프라임(p_1) 및 제2 기준 프라임(p_2) 각각이 인버스 p-어레이($\overleftrightarrow{F}_{\ell}\Big|^m$)의 모듈러스(modulus)($\ell$)로서 기능하게 함으로써, 제1 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_1}\Big|^m$) 및 제2 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_2}\Big|^m$)를 획득하는 단계로서, 상기 제1 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_1}\Big|^m$)는 $K_{\text{private}} = \left(\overleftrightarrow{f}\Big|^m, p_1, \tilde{a}\right)$ 로 정의되는 개인키(K_{private}) 역할을 하는, 단계; 및

G) 상기 제2 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_2}\Big|^m$), 상기 제1 기준 프라임($p_1$), 상기 제2 기준 프라임($p_2$) 및 상기 키-생성 랜덤화 어레이($\overleftrightarrow{R}\Big|^m_{(\tilde{a})}$)에 기초하여 키-생성 랜덤화 어레이 $\overleftrightarrow{R}\Big|^m_{(\tilde{a})}$ 와 관련하여 공개키(K_{public})를 생성하는 단계로서, 키-생성 랜덤화 어레이($\overleftrightarrow{R}\Big|^m_{(\tilde{a})}$)는 0과 제1 기준 양의 정수($\tilde{a}$) 사이의 m 개의 숫자 성분을 가지며, 그리고 공개키(K_{public})는 개인키(K_{private})와 쌍을 이루며, 그리고 m 개의 숫자 성분들을 포함하고 $\overleftrightarrow{K}_{\text{public}}\Big|^m := \text{Rand}\left(\overleftrightarrow{F}_{p_2}\Big|^m, p_1, \tilde{a}\right) \pmod{p_2}$ 를 나타내는 $K_{\text{public}} = \left(\overleftrightarrow{K}_{\text{public}}\Big|^m, p_2\right)$ 라고도 표시되는 어레이($\overleftrightarrow{K}_{\text{public}}\Big|^m$)이며, $\text{Rand}\left(\overleftrightarrow{F}_{p_2}\Big|^m, p_1, \tilde{a}\right)$ 는 키 생성 랜덤화 어레이($\overleftrightarrow{R}\Big|^m_{(\tilde{a})}$)에 대한 제2 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_2}\Big|^m$)의 키 생성 랜덤화 함수이며, 그리고 $\text{Rand}\left(\overleftrightarrow{F}_{p_2}\Big|^m, p_1, \tilde{a}\right) = p_1\left(\overleftrightarrow{F}_{p_2}\Big|^m \circledast \overleftrightarrow{R}\Big|^m_{(\tilde{a})}\right)$ 로 정의되며, 여기서 $\circledast$ 는 컨볼루션 곱셈 연산자를 나타내는, 단계를 포함하는, 포스트-퀀텀 비대칭 키 생성 방법.

청구항 2

프로세서에 의해 구현되는 암호화 방법으로서,

청구항 1에 따른 포스트-퀀텀 비대칭 키 생성 방법에 따라 생성되는 공개키(K_{public}), 상기 포스트-퀀텀 비대칭 키 생성 방법에서 사용되는 제2 기준 프라임(p_2), 그리고 0과 상기 포스트-퀀텀 비대칭 키 생성 방법에서 사용되는 제2 기준 양의 정수($\tilde{b}$) 사이의 m 개의 숫자 성분들을 갖는 암호화 랜덤화 어레이($\overleftrightarrow{R}\Big|^m_{(\tilde{b})}$)를 사용하여, 전송될 평문에 대응하고 m 개의 숫자 성분들을 갖는 데이터 어레이($\overleftrightarrow{M}\Big|^m$)에 대한 암호화 절차를 수행하고, 그리

고 상기 암호화 랜덤화 어레이($\overleftrightarrow{R}\big|_{(\tilde{b})}^{m}$)에 관한 암호문($\overleftarrow{Cipher}\big|^{m}$)을 획득하는 단계로서, 상기 암호문($\overleftarrow{Cipher}\big|^{m}$)은 m 개의 암호화된 숫자 성분들을 갖는, 단계를 포함하는, 암호화 방법.

청구항 3

청구항 2에 있어서,

상기 평문은 m 개의 문자들을 가지며,

상기 데이터 어레이($\overleftrightarrow{M}\big|^{m}$)의 m 개의 숫자 성분들 각각은 0과 상기 포스트-퀀텀 비대칭 키 생성 방법에서 사용되는 제1 기준 양의 정수($\tilde{a}$) 사이이며, 그리고 상기 평문의 m 개의 문자들 중 대응하는 문자를 나타내는, 암호화 방법.

청구항 4

청구항 2에 있어서,

상기 암호화 절차는 :

공개키(K_{public}) 및 암호화 랜덤화 어레이($\overleftrightarrow{R}\big|_{(\tilde{b})}^{m}$)에 기초하여, $\overleftrightarrow{R}\big|^{m} := \mathbf{Rand}\left(\overleftrightarrow{K}_{\text{public}}\big|^{m}, 1, \tilde{b}\right)$ 로 정의되는 암호화 랜덤화 함수($\overleftrightarrow{R}\big|^{m}$)를 생성하는 단계; 및

상기 데이터 어레이($\overleftrightarrow{M}\big|^{m}$)와 상기 암호화 랜덤화 함수($\overleftrightarrow{R}\big|^{m}$)의 합에 대해 제2 기준 프라임(p_2)으로 모듈로 연산(modulo operation)을 수행함으로써 암호문($\overleftarrow{Cipher}\big|^{m}$)을 획득하는 단계로서, 상기 암호문($\overleftarrow{Cipher}\big|^{m}$)은 $\overleftarrow{Cipher}\big|^{m} := \left(\overleftrightarrow{M}\big|^{m} + \overleftrightarrow{R}\big|^{m}\right) \pmod{p_2}$ 로 표현되는, 단계를 포함하는, 암호화 방법.

청구항 5

프로세서에 의해 구현되는 해독 방법으로서,

청구항 1에 따른 포스트-퀀텀 비대칭 키 생성 방법에서 사용되는 p-어레이($\overleftrightarrow{f}\big|^{m}$), 개인키(K_{private}), 제1 기준 프라임(p_1) 및 제2 기준 프라임(p_2)을 사용하여, 암호문($\overleftarrow{Cipher}\big|^{m}$)에 대해 해독 절차를 수행하고, m 개의 해독된 숫자 성분들을 갖는 평문 어레이($\overleftrightarrow{M_1}\big|^{m}$)를 획득하는 단계를 포함하며,

상기 암호문($\overleftarrow{Cipher}\big|^{m}$)은 :

상기 포스트-퀀텀 비대칭 키 생성 방법에 따라 생성되는 공개키, 상기 포스트-퀀텀 비대칭 키 생성 방법에서 사용되는 제2 기준 프라임(p_2), 그리고 0과 상기 포스트-퀀텀 비대칭 키 생성 방법에서 사용되는 제2 기준 양의 정수($\tilde{b}$) 사이의 m 개의 숫자 성분들을 갖는 암호화 랜덤화 어레이($\overleftrightarrow{R}\big|_{(\tilde{b})}^{m}$)를 사용하여, 전송될

평문에 대응하고 m 개의 숫자 성분들을 갖는 데이터 어레이($\overleftrightarrow{M}\Big|^{m}$)에 대한 암호화 절차를 수행하고, 그리고 상기 암호화 랜덤화 어레이($\overleftrightarrow{R}\Big|^{m}_{(b)}$)와 관련되고 m 개의 암호화된 숫자 성분들을 갖는 암호문($\overleftrightarrow{Cipher}\Big|^{m}$)을 획득함으로써 생성되는, 해독 방법.

청구항 6

청구항 5에 있어서,

상기 해독 절차는 :

상기 암호문($\overleftrightarrow{Cipher}\Big|^{m}$)과 상기 p-어레이($\overleftrightarrow{f}\Big|^{m}$)의 제1 컨볼루션 결과에 대해 제2 기준 프라임(p_2)으로 모듈로 연산을 수행하여 제1 모듈로 연산 결과를 획득하며, 그리고 상기 제1 모듈로 연산 결과에 대해 제1 기준 프라임(p_1)으로 모듈로 연산을 수행하여 제2 모듈로 연산 결과($\overleftrightarrow{M_0}\Big|^{m}$)를 획득하는 단계로서, 상기 제2 모듈로 연산 결과($\overleftrightarrow{M_0}\Big|^{m}$)는 $\overleftrightarrow{M_0}\Big|^{m} := \left[\left(\overleftrightarrow{Cipher}\Big|^{m} \circledast \overleftrightarrow{f}\Big|^{m}\right) \pmod{p_2}\right] \pmod{p_1}$ 로 정의되는, 단계; 및

제2 모듈로 연산 결과($\overleftrightarrow{M_0}\Big|^{m}$) 그리고 개인키(K_{private}) 역할을 하는 제1 기준 인버스 p-어레이($\overleftrightarrow{F_{p_1}}\Big|^{m}$)의 제2 컨볼루션 결과에 대해 제1 기준 프라임(p_1)으로 모듈로 연산을 수행하여 평문 어레이($\overleftrightarrow{M_1}\Big|^{m}$)를 획득하는 단계로서, 상기 평문 어레이($\overleftrightarrow{M_1}\Big|^{m}$)는 $\overleftrightarrow{M_1}\Big|^{m} := \overleftrightarrow{M_0}\Big|^{m} \circledast \overleftrightarrow{F}_{p_1}\Big|^{m} \pmod{p_1}$ 로 정의되는, 단계를 포함하는, 해독 방법.

청구항 7

포스트-퀀텀 비대칭 키 생성 시스템으로서,

프라임 p 그리고 시드 역할을 하는 클래식 스트링(classical string) 및 산술 함수 중 하나에 기초하여, 프라임 p와 관련되고 무한한 개수의 성분들을 갖는 p-벡터($\overrightarrow{f}_p$)를 생성하도록 구성된 p-벡터 생성 모듈로서, 상기 p-벡터($\overrightarrow{f}_p$)는 $\overrightarrow{f}_p := [f(p^0), f(p^1), f(p^2), f(p^3), \ldots]$ 로 정의되는데, f는 상기 시드 역할을 하는 클래식 스트링 및 산술 함수 중 상기 하나를 나타내는, p-벡터 생성 모듈;

상기 p-벡터 생성 모듈에 연결되고, 그리고 상기 p-벡터($\overrightarrow{f}_p$)에 기초하여, m 개의 성분들을 갖고 프라임 p와 관련되는 p-어레이($\overleftrightarrow{f}_p\Big|^{m}_{s,t}$)를 생성하도록 구성되는 p-어레이 생성 모듈로서, 상기 p-어레이($\overleftrightarrow{f}_p\Big|^{m}_{s,t}$)는 $\overleftrightarrow{f}_p\Big|^{m}_{s,t} := \sum_{i=0}^{t}\left[f\left(p^{s+im}\right), \ldots, f\left(p^{s+im+(m-1)}\right)\right]$ 로 정의되며, 파라미터들 m, s 및 t 각각은 사용자-정의되는 양의 정수이며, 그리고 프라임 p 및 파라미터들 s, t는 협력하여 제1 파라미터 세트(I)를 구성하며, 상기 p-어레이($\overleftrightarrow{f}_p\Big|^{m}_{s,t}$)는 $\overleftrightarrow{f}\Big|^{m}$ 로도 표현되는, p-어레이 생성 모듈;

상기 p-어레이 생성 모듈에 연결되고, 그리고 상기 p-어레이($\overleftrightarrow{f}\big|^m$)에 기초하여, 관련 매트릭스($\left[\overleftrightarrow{f}\big|^m\right]$)를 생성하도록 구성되는 관련 매트릭스 생성 모듈로서, 상기 관련 매트릭스($\left[\overleftrightarrow{f}\big|^m\right]$)는 :

$$\left[\overleftrightarrow{f}\big|^m\right]=\begin{pmatrix} \overleftrightarrow{f}\big|^m(0) & \overleftrightarrow{f}\big|^m(1) & \cdots & \overleftrightarrow{f}\big|^m(m-1) \\ \overleftrightarrow{f}\big|^m(m-1) & \overleftrightarrow{f}\big|^m(0) & \cdots & \overleftrightarrow{f}\big|^m(m-2) \\ \vdots & \vdots & \ddots & \vdots \\ \overleftrightarrow{f}\big|^m(1) & \overleftrightarrow{f}\big|^m(2) & \cdots & \overleftrightarrow{f}\big|^m(0) \end{pmatrix}$$

로 정의되는데, $\overleftrightarrow{f}\big|^m$ (j)는 p-어레이의 m 개의 성분들 중 (j+1) 번째 성분을 나타내며, 0 ≤ j ≤ (m-1)인, 관련 매트릭스 생성 모듈;

상기 관련 매트릭스 생성 모듈에 연결되고, 그리고 상기 관련 매트릭스 $\left[\overleftrightarrow{f}\big|^m\right]$와 사용자-정의된 양의 정수인 모듈러스 ℓ 에 기초하여, 상기 모듈러스 ℓ 에 대하여 인버스 p-어레이($\overleftrightarrow{F}_{\ell}\big|^m$)를 생성하도록 구성된 인버스 p-어레이 생성 모듈로서, 상기 인버스 p-어레이($\overleftrightarrow{F}_{\ell}\big|^m$)는

$$\overleftrightarrow{F}_{\ell}\big|^m := \left(L_{\ell}[1,0,\cdots,0]\left[\overleftrightarrow{f}\big|^m\right]^*\right) \pmod{\ell}$$

로 정의되는데, L_{ℓ} 는 상기 모듈러스 ℓ 에 대한 관련 매트릭스 $\left[\overleftrightarrow{f}\big|^m\right]$ 의 행렬식(determinant)의 인버스 모듈러스를 나타내며,

$$L_{\ell} := \left(\det\left[\overleftrightarrow{f}\big|^m\right]\right)^{-1} \pmod{\ell}$$

로 정의되고, 그리고 $\left[\overleftrightarrow{f}\big|^m\right]^*$ 는 상기 관련 매트릭스 $\left[\overleftrightarrow{f}\big|^m\right]$의 수반 행렬(adjoint matrix)을 나타내는, 인버스 p-어레이 생성 모듈;

제1 기준 프라임(p_1)을 임의로 선택하고, 그리고 상기 제1 기준 프라임(p_1), b로 표시되는 p-어레이 $\overleftrightarrow{f}\big|^m$ 의 m 개의 성분들 중 가장 큰 것, 제1 기준 양의 정수($\tilde{a}$) 그리고 파라미터(m), 제2 기준 양의 정수($\tilde{b}$) 및 제3 기준 양의 정수(r)로 구성된 제2 파라미터 세트(S)와 관련된 미리 결정된 기준에 기초하여 제2 기준 프라임(p_2)을 결정하도록 구성된 기준 프라임 결정 모듈로서, 상기 미리 결정된 기준은 $p_2 > \max(p_1 m\tilde{a}\tilde{b}, mbr)$ 을 포함하는, 기준 프라임 결정 모듈;

상기 인버스 p-어레이 생성 모듈 및 상기 기준 프라임 결정 모듈에 연결되고, 그리고 제1 기준 프라임(p_1)이 인버스 p-어레이($\overleftrightarrow{F}_{\ell}\big|^m$)의 모듈러스(modulus)(ℓ)로서 기능하게 함으로써, 제1 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_1}\big|^m$)를 획득하도록 구성된 개인키 생성 모듈로서, 상기 제1 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_1}\big|^m$)는

$$K_{\text{private}} = \left(\overleftrightarrow{f}\big|^m, p_1, \tilde{a}\right)$$

로 정의되는 개인키(K_{private}) 역할을 하는, 개인키 생성 모듈; 및

상기 인버스 p-어레이 생성 모듈 및 상기 기준 프라임 결정 모듈에 연결되고, 그리고 제2 기준 프라임(p_2)이 인버스 p-어레이($\overleftrightarrow{F}_{\ell}\big|^m$)의 모듈러스(modulus)(ℓ)로서 기능하게 함으로써, 제2 기준 인버스 p-어레이

($\overleftrightarrow{F}_{p_2}\big|^m$)를 획득하도록 구성되고, 상기 제2 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_2}\big|^m$), 상기 제1 기준 프라임($p_1$), 상기 제2 기준 프라임($p_2$) 및 상기 키-생성 랜덤화 어레이($\overleftrightarrow{R}\big|^m_{(\tilde{a})}$)에 기초하여 키-생성 랜덤화 어레이 $\overleftrightarrow{R}\big|^m_{(\tilde{a})}$와 관련하여 공개키($K_{\text{public}}$)를 생성하도록 구성되는 공개키 생성 모듈로서, 상기 키-생성 랜덤화 어레이($\overleftrightarrow{R}\big|^m_{(\tilde{a})}$)는 0과 제1 기준 양의 정수($\tilde{a}$) 사이의 m 개의 숫자 성분을 가지며, 그리고 공개키(K_{public})는 개인키(K_{private})와 쌍을 이루며, 그리고 m 개의 숫자 성분들을 포함하고 $\overleftrightarrow{K}_{\text{public}}\big|^m := \text{Rand}\left(\overleftrightarrow{F}_{p_2}\big|^m, p_1, \tilde{a}\right) \pmod{p_2}$를 나타내는 $K_{\text{public}} = \left(\overleftrightarrow{K}_{\text{public}}\big|^m, p_2\right)$라고도 표시되는 어레이($\overleftrightarrow{K}_{\text{public}}\big|^m$)인, 공개키 생성 모듈을 포함하며,

$\text{Rand}\left(\overleftrightarrow{F}_{p_2}\big|^m, p_1, \tilde{a}\right)$는 키 생성 랜덤화 어레이($\overleftrightarrow{R}\big|^m_{(\tilde{a})}$)에 대한 제2 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_2}\big|^m$)의 키 생성 랜덤화 함수이며, 그리고 $\text{Rand}\left(\overleftrightarrow{F}_{p_2}\big|^m, p_1, \tilde{a}\right) = p_1\left(\overleftrightarrow{F}_{p_2}\big|^m \circledast \overleftrightarrow{R}\big|^m_{(\tilde{a})}\right)$로 정의되며, 여기서 $\circledast$는 컨볼루션 곱셈 연산자를 나타내는, 포스트-퀀텀 비대칭 키 생성 방법.

청구항 8

청구항 7에 있어서,

상기 p-어레이 생성 모듈, 상기 기준 프라임 결정 모듈, 상기 개인키 생성 모듈 및 상기 공개키 생성 모듈에 연결된 저장 모듈을 더 포함하며,

상기 저장 모듈은 :

상기 p-어레이 생성 모듈로부터 수신된 p-어레이($\overleftrightarrow{f}\big|^m$), 상기 기준 프라임 결정 모듈로부터 수신된 상기 제1 기준 프라임(p_1) 및 상기 제2 기준 프라임(p_2), 상기 개인키 생성 모듈로부터 수신된 제1 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_1}\big|^m$), 그리고 상기 공개키 생성 모듈로부터 수신된 제2 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_2}\big|^m$)를 저장하는, 포스트-퀀텀 비대칭 키 생성 방법.

청구항 9

청구항 8에 있어서,

상기 공개키 생성 모듈은 :

상기 저장 모듈에 저장된 상기 제2 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_2}\big|^m$), 상기 제1 기준 프라임($p_1$) 및 상기 제2 기준 프라임($p_2$), 그리고 키-생성 랜덤화 어레이($\overleftrightarrow{R^*}\big|^m_{(\tilde{a})}$)와 상이한 다른 키-생성 랜덤화 어레

이($\overleftrightarrow{R^*}\big|_{(\tilde{a})}^{m}$)에 기초하여, 상기 다른 키-생성 랜덤화 어레이($\overleftrightarrow{R^*}\big|_{(\tilde{a})}^{m}$)와 관련하여 업데이트된 공개키(K^*_{public})를 생성하도록 더 구성되며,

상기 업데이트된 공개키(K^*_{public})는 개인키(K_{private})와 쌍을 이루며,

상기 다른 키-생성 랜덤화 어레이($\overleftrightarrow{R^*}\big|_{(\tilde{a})}^{m}$)는 0과 상기 제1 기준 양의 정수($\tilde{a}$) 사이의 m 개의 숫자 성분들을 가지며, 그리고

상기 공개키(K_{public})는 $\overleftrightarrow{K^*}_{\text{public}}\big|^{m} = \text{Rand}\left(\overleftrightarrow{F}_{p_2}\big|^{m}, p_1, \tilde{a}\right) \pmod{p_2} = p_1\left(\overleftrightarrow{F}_{p_2}\big|^{m} \circledast \overleftrightarrow{R^*}\big|_{(\tilde{a})}^{m}\right) \pmod{p_2}$ 를 나타내는 $K^*_{\text{public}} = \left(\overleftrightarrow{K^*}_{\text{public}}\big|^{m}, p_2\right)$ 라고도 표시되는, 포스트-퀀텀 비대칭 키 생성 방법.

청구항 10

암호화 통신 시스템으로서,

상기 암호화된 통신 시스템은 키 서버, 송신단 및 수신단을 포함하며,

상기 키 서버는 :

프라임 p 그리고 시드 역할을 하는 클래식 스트링(classical string) 및 산술 함수 중 하나에 기초하여, 프라임 p와 관련되고 무한한 개수의 성분들을 갖는 p-벡터($\vec{f}_p$)를 생성하도록 구성된 p-벡터 생성 모듈로서, 상기 p-벡터($\vec{f}_p$)는 $\vec{f}_p := [f(p^0), f(p^1), f(p^2), f(p^3), \ldots]$ 로 정의되는데, f는 상기 시드 역할을 하는 클래식 스트링 및 산술 함수 중 상기 하나를 나타내는, p-벡터 생성 모듈;

상기 p-벡터 생성 모듈에 연결되고, 그리고 상기 p-벡터($\vec{f}_p$)에 기초하여, m 개의 성분들을 갖고 프라임 p와 관련되는 p-어레이($\overleftrightarrow{f}_p\big|_{s,t}^{m}$)를 생성하도록 구성되는 p-어레이 생성 모듈로서, 상기 p-어레이($\overleftrightarrow{f}_p\big|_{s,t}^{m}$)는 $\overleftrightarrow{f}_p\big|_{s,t}^{m} := \sum_{i=0}^{t}\left[f\left(p^{s+im}\right), \ldots, f\left(p^{s+im+(m-1)}\right)\right]$ 로 정의되며, 파라미터들 m, s 및 t 각각은 사용자-정의되는 양의 정수이며, 그리고 프라임 p 및 파라미터들 s, t는 협력하여 제1 파라미터 세트(I)를 구성하며, 상기 p-어레이($\overleftrightarrow{f}_p\big|_{s,t}^{m}$)는 $\overleftrightarrow{f}\big|^{m}$ 로도 표현되는, p-어레이 생성 모듈;

상기 p-어레이 생성 모듈에 연결되고, 그리고 상기 p-어레이($\overleftrightarrow{f}\big|^{m}$)에 기초하여, 관련 매트릭스($\left[\overleftrightarrow{f}\big|^{m}\right]$)를 생성하도록 구성된 관련 매트릭스 생성 모듈로서, 상기 관련 매트릭스($\left[\overleftrightarrow{f}\big|^{m}\right]$)는 :

$$\left[\overleftrightarrow{f}\big|^{m}\right] = \begin{pmatrix} \overleftrightarrow{f}\big|^{m}(0) & \overleftrightarrow{f}\big|^{m}(1) & \cdots & \overleftrightarrow{f}\big|^{m}(m-1) \\ \overleftrightarrow{f}\big|^{m}(m-1) & \overleftrightarrow{f}\big|^{m}(0) & \cdots & \overleftrightarrow{f}\big|^{m}(m-2) \\ \vdots & \vdots & \ddots & \vdots \\ \overleftrightarrow{f}\big|^{m}(1) & \overleftrightarrow{f}\big|^{m}(2) & \cdots & \overleftrightarrow{f}\big|^{m}(0) \end{pmatrix}$$ 로 정의되는데, $\overleftrightarrow{f}\big|^{m}(j)$는 p-어레이의 m 개의 성분들 중 (j+1) 번째 성분을 나타내며, $0 \le j \le (m-1)$인, 관련 매트릭스 생성 모듈;

상기 관련 매트릭스 생성 모듈에 연결되고, 그리고 상기 관련 매트릭스 $\left[\overleftrightarrow{f}\right|^{m}]$와 사용자-정의된 양의 정수인 모듈러스 ℓ 에 기초하여, 상기 모듈러스 ℓ 에 대하여 인버스 p-어레이($\overleftrightarrow{F}_{\ell}\Big|^{m}$)를 생성하도록 구성된 인버스 p-어레이 생성 모듈로서, 상기 인버스 p-어레이($\overleftrightarrow{F}_{\ell}\Big|^{m}$)는

$$\overleftrightarrow{F}_{\ell}\Big|^{m} := \left(L_{\ell}[1,0,\cdots,0]\left[\overleftrightarrow{f}\Big|^{m}\right]^{*}\right) \pmod{\ell}$$

로 정의되는데, L_{ℓ} 는 상기 모듈러스 ℓ 에 대한 관련 매트릭스 $\left[\overleftrightarrow{f}\right|^{m}]$ 의 행렬식(determinant)의 인버스 모듈러스를 나타내며,

$$L_{\ell} := \left(\det\left[\overleftrightarrow{f}\Big|^{m}\right]\right)^{-1} \pmod{\ell}$$

로 정의되고, 그리고 $\left[\overleftrightarrow{f}\right|^{m}]^{*}$ 는 상기 관련 매트릭스 $\left[\overleftrightarrow{f}\right|^{m}]$의 수반 행렬(adjoint matrix)을 나타내는, 인버스 p-어레이 생성 모듈;

제1 기준 프라임(p_1)을 임의로 선택하고, 그리고 상기 제1 기준 프라임(p_1), b로 표시되는 p-어레이 $\overleftrightarrow{f}\Big|^{m}$ 의 m 개의 성분들 중 가장 큰 것, 제1 기준 양의 정수($\tilde{a}$) 그리고 파라미터(m), 제2 기준 양의 정수($\tilde{b}$) 및 제3 기준 양의 정수(r)로 구성된 제2 파라미터 세트(S)와 관련된 미리 결정된 기준에 기초하여 제2 기준 프라임(p_2)을 결정하도록 구성된 기준 프라임 결정 모듈로서, 상기 미리 결정된 기준은

$$p_2 > \max(p_1 m\tilde{a}\tilde{b}, mbr)$$

을 포함하는, 기준 프라임 결정 모듈;

상기 인버스 p-어레이 생성 모듈 및 상기 기준 프라임 결정 모듈에 연결되고, 그리고 제1 기준 프라임(p_1)이 인버스 p-어레이($\overleftrightarrow{F}_{\ell}\Big|^{m}$)의 모듈러스(modulus)(ℓ)로서 기능하게 함으로써, 제1 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_1}\Big|^{m}$)를 획득하도록 구성된 개인키 생성 모듈로서, 상기 제1 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_1}\Big|^{m}$)는

$$K_{\text{private}} = \left(\overleftrightarrow{f}\Big|^{m}, p_1, \tilde{a}\right)$$

로 정의되는 개인키(K_{private}) 역할을 하는, 개인키 생성 모듈; 및

상기 인버스 p-어레이 생성 모듈 및 상기 기준 프라임 결정 모듈에 연결되고, 그리고 제2 기준 프라임(p_2)이 인버스 p-어레이($\overleftrightarrow{F}_{\ell}\Big|^{m}$)의 모듈러스(modulus)(ℓ)로서 기능하게 함으로써, 제2 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_2}\Big|^{m}$)를 획득하도록 구성되고, 상기 제2 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_2}\Big|^{m}$), 상기 제1 기준 프라임(p_1), 상기 제2 기준 프라임(p_2) 및 상기 키-생성 랜덤화 어레이($\overleftrightarrow{R}\Big|^{m}_{(\tilde{a})}$)에 기초하여 키-생성 랜덤화 어레이 $\overleftrightarrow{R}\Big|^{m}_{(\tilde{a})}$ 와 관련하여 공개키(K_{public})를 생성하도록 구성되는 공개키 생성 모듈로서, 상기 키-생성 랜덤화 어레이($\overleftrightarrow{R}\Big|^{m}_{(\tilde{a})}$)는 0과 제1 기준 양의 정수($\tilde{a}$) 사이의 m 개의 숫자 성분을 가지며, 그리고 공개키(K_{public})는 개인키(K_{private})와 쌍을 이루며, 그리고 m 개의 숫자 성분들을 포함하고

$\overleftrightarrow{K}_{\text{public}}\Big|^{m} := \text{Rand}\left(\overleftrightarrow{F}_{p_2}\Big|^{m}, p_1, \tilde{a}\right) \pmod{p_2}$ 를 나타내는 $K_{\text{public}} = \left(\overleftrightarrow{K}_{\text{public}}\Big|^{m}, p_2\right)$ 라고도 표시되는 어레이($\overleftrightarrow{K}_{\text{public}}\Big|^{m}$)인, 공개키 생성 모듈을 포함하며,

$\text{Rand}\left(\overleftrightarrow{F}_{p_2}\Big|^{m}, p_1, \tilde{a}\right)$ 는 키 생성 랜덤화 어레이($\overleftrightarrow{R}\Big|^{m}_{(\tilde{a})}$)에 대한 제2 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_2}\Big|^{m}$)의 키 생성 랜덤화 함수이며, 그리고 $\text{Rand}\left(\overleftrightarrow{F}_{p_2}\Big|^{m}, p_1, \tilde{a}\right) = p_1\left(\overleftrightarrow{F}_{p_2}\Big|^{m} \circledast \overleftrightarrow{R}\Big|^{m}_{(\tilde{a})}\right)$ 로 정의되며, 여기서 $\circledast$ 는 컨볼루션 곱셈 연산자를 나타내며,

상기 송신단은 상기 공개키(K_{public}), 상기 제2 기준 프라임(p_2) 및 상기 제2 기준 양의 정수($\tilde{b}$)를 저장하는 제1 저장 유닛, 그리고 상기 제1 저장 유닛에 연결된 제1 프로세서를 포함하며,

상기 수신단은 상기 개인키(K_{private}), 상기 p-어레이($\overleftrightarrow{f}\Big|^{m}$), 상기 제1 기준 프라임($p_1$) 및 상기 제2 기준 프라임($p_2$)을 저장하는 제2 저장 유닛, 그리고 상기 제2 저장 유닛에 연결된 제2 프로세서를 포함하며,

상기 수신단에 전송될 평문에 대응하고 그리고 m 개의 숫자 성분들을 갖는 데이터 어레이($\overleftrightarrow{M}\Big|^{m}$)에 대해, 상기 제1 프로세서는 상기 제1 저장 유닛에 저장된 공개키(K_{public}) 및 제2 기준 프라임(p_2), 그리고 0과 상기 제2 기준 양의 정수($\tilde{b}$) 사이의 m 개의 숫자 성분들을 갖는 암호화 랜덤화 어레이($\overleftrightarrow{R}\Big|^{m}_{(\tilde{b})}$)를 사용하여, 상기 데이터 어레이($\overleftrightarrow{M}\Big|^{m}$)에 대한 암호화 절차를 수행하고, 그리고 상기 암호화 랜덤화 어레이($\overleftrightarrow{R}\Big|^{m}_{(\tilde{b})}$)에 관한 암호문($\overleftrightarrow{Cipher}\Big|^{m}$)을 획득하며, 그리고 상기 송신단은 제1 통신 채널을 통해 상기 수신단에 상기 암호문($\overleftrightarrow{Cipher}\Big|^{m}$)을 송신하며, 상기 암호문($\overleftrightarrow{Cipher}\Big|^{m}$)은 m 개의 암호화된 숫자 성분들을 가지며,

상기 제2 프로세서에 의한 상기 암호문($\overleftrightarrow{Cipher}\Big|^{m}$)의 수신시, 상기 제2 프로세서는 상기 제2 저장 유닛에 저장된 개인키(K_{private}), p-어레이($\overleftrightarrow{f}\Big|^{m}$), 제1 기준 프라임($p_1$) 및 제2 기준 프라임($p_2$)을 사용하여, 암호문($\overleftrightarrow{Cipher}\Big|^{m}$)에 대해 해독 절차를 수행하고, m 개의 해독된 숫자 성분들을 갖고 상기 데이터 어레이($\overleftrightarrow{M}\Big|^{m}$)와 동일한 평문 어레이($\overleftrightarrow{M_1}\Big|^{m}$)를 획득하는, 암호화 통신 시스템.

청구항 11

청구항 10에 있어서,

상기 평문은 m 개의 문자들을 가지며,

상기 제1 프로세서는 상기 평문을 상기 데이터 어레이($\overleftrightarrow{M}\Big|^{m}$)로 변환하기 위해 미리 결정된 문자-숫자 기술을

사용하도록 구성된 텍스트 변환 모듈을 가지며, 그리고

상기 데이터 어레이($\overleftrightarrow{M}\Big|^m$)의 m 개의 숫자 성분들 각각은 0과 상기 제1 기준 양의 정수($\tilde{a}$) 사이이며, 그리고 상기 평문의 m 개의 문자들 중 대응하는 문자를 나타내는, 암호화 통신 시스템.

청구항 12

청구항 11에 있어서,

상기 제1 프로세서는 암호화 랜덤화 함수 생성 모듈, 그리고 상기 텍스트 변환 모듈 및 상기 암호화 랜덤화 함수 생성 모듈에 연결된 암호문 생성 모듈을 가지며, 그리고

상기 암호화 절차에서, 상기 암호화 랜덤화 함수 생성 모듈은, 공개키(K_{public}) 및 암호화 랜덤화 어레이 ($\overleftrightarrow{R}\Big|^m_{(\tilde{b})}$)에 기초하여, $\overleftrightarrow{R}\Big|^m := \text{Rand}\left(\overleftrightarrow{K}_{\text{public}}\Big|^m, 1, \tilde{b}\right)$ 로 정의되는 암호화 랜덤화 함수($\overleftrightarrow{R}\Big|^m$)를 생성하고; 그리고 상기 암호문 생성 모듈은 상기 데이터 어레이($\overleftrightarrow{M}\Big|^m$)와 상기 암호화 랜덤화 함수($\overleftrightarrow{R}\Big|^m$)의 합에 대해 제2 기준 프라임(p_2)으로 모듈로 연산(modulo operation)을 수행함으로써 암호문($\overleftarrow{Cipher}\Big|^m$)을 획득하고, 상기 암호문($\overleftarrow{Cipher}\Big|^m$)은 $\overleftarrow{Cipher}\Big|^m := \left(\overleftrightarrow{M}\Big|^m + \overleftrightarrow{R}\Big|^m\right) \pmod{p_2}$ 로 표현되는, 암호화 통신 시스템.

청구항 13

청구항 10에 있어서,

상기 제2 프로세서는 제1 컨볼루션 모듈 및 상기 제1 컨볼루션 모듈에 연결된 제2 컨볼루션 모듈을 가지며,

상기 해독 절차에서, 상기 제1 컨볼루션 모듈은 상기 암호문($\overleftarrow{Cipher}\Big|^m$)과 상기 p-어레이($\overleftrightarrow{f}\Big|^m$)의 제1 컨볼루션 결과를 계산하고, 상기 제1 컨볼루션 결과에 대해 제2 기준 프라임(p_2)으로 모듈로 연산을 수행하여 제1 모듈로 연산 결과를 획득하며, 그리고 상기 제1 모듈로 연산 결과에 대해 제1 기준 프라임(p_1)으로 모듈로 연산을 수행하여 제2 모듈로 연산 결과($\overleftrightarrow{M_0}\Big|^m$)를 획득하며, 상기 제2 모듈로 연산 결과($\overleftrightarrow{M_0}\Big|^m$)는 $\overleftrightarrow{M_0}\Big|^m := \left[\left(\overleftarrow{Cipher}\Big|^m \circledast \overleftrightarrow{f}\Big|^m\right) \pmod{p_2}\right] \pmod{p_1}$ 로 정의되고; 그리고 상기 제2 컨볼루션 모듈은 제2 모듈로 연산 결과($\overleftrightarrow{M_0}\Big|^m$) 그리고 개인키(K_{private}) 역할을 하는 제1 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_1}\Big|^m$)의 제2 컨볼루션 결과를 계산하고, 상기 제2 컨볼루션 결과에 대해 제1 기준 프라임(p_1)으로 모듈로 연산을 수행하여 평문 어레이($\overleftrightarrow{M_1}\Big|^m$)를 획득하고, 상기 평문 어레이($\overleftrightarrow{M_1}\Big|^m$)는 $\overleftrightarrow{M_1}\Big|^m := \overleftrightarrow{M_0}\Big|^m \circledast \overleftrightarrow{F}_{p_1}\Big|^m \pmod{p_1}$ 로 정의되는, 암호화 통신 시스템.

청구항 14

청구항 10에 있어서,

상기 공개키(K_{public}) 전에, 상기 제2 기준 프라임(p_2) 및 상기 제2 기준 양의 정수($\tilde{b}$)는 상기 제1 저장 유닛에 저장되며, 상기 키 서버는 제2 통신 채널을 통해 상기 공개키(K_{public}), 상기 제2 기준 프라임(p_2) 및 상기 제2

기준 양의 정수($\tilde{b}$)를 상기 송신단에 송신하며, 그리고 상기 제1 프로세서는 상기 키 서버로부터 수신된 상기 공개키(K_{public}), 상기 제2 기준 프라임(p_2) 및 상기 제2 기준 양의 정수($\tilde{b}$)를 상기 제1 저장 유닛에 저장하며; 그리고

상기 개인키($K_{private}$)전에, 상기 p-어레이($\overleftrightarrow{f}\big|^m$), 상기 제1 기준 프라임($p_1$) 및 상기 제2 기준 프라임($p_2$)은 상기 제2 저장 유닛에 저장되며, 상기 키 서버는 제3 통신 채널을 통해 상기 개인키($K_{private}$), 상기 p-어레이($\overleftrightarrow{f}\big|^m$), 상기 제1 기준 프라임($p_1$) 및 상기 제2 기준 프라임($p_2$)을 상기 수신단에 송신하며, 그리고 상기 제2 프로세서는 상기 키 서버로부터 수신된 상기 개인키($K_{private}$), 상기 p-어레이($\overleftrightarrow{f}\big|^m$), 상기 제1 기준 프라임($p_1$) 및 상기 제2 기준 프라임($p_2$)을 상기 제2 저장 유닛에 저장하는, 암호화 통신 시스템.

청구항 15

청구항 14에 있어서,

상기 키 서버는 상기 p-어레이 생성 모듈, 상기 기준 프라임 결정 모듈, 상기 개인키 생성 모듈 및 상기 공개키 생성 모듈에 연결된 저장 모듈을 더 포함하며,

상기 저장 모듈은 상기 p-어레이 생성 모듈로부터 수신된 p-어레이($\overleftrightarrow{f}\big|^m$), 상기 기준 프라임 결정 모듈로부터 수신된 상기 제1 기준 프라임(p_1) 및 상기 제2 기준 프라임(p_2), 상기 개인키 생성 모듈로부터 수신된 제1 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_1}\big|^m$), 그리고 상기 공개키 생성 모듈로부터 수신된 제2 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_2}\big|^m$)를 저장하는, 암호화 통신 시스템.

청구항 16

청구항 15에 있어서,

상기 공개키 생성 모듈은 :

상기 제2 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_2}\big|^m$), 상기 제1 기준 프라임($p_1$), 상기 제2 기준 프라임($p_2$), 그리고 키-생성 랜덤화 어레이($\overleftrightarrow{R^*}\big|^m_{(\tilde{a})}$)와 상이한 다른 키-생성 랜덤화 어레이($\overleftrightarrow{R^*}\big|^m_{(\tilde{a})}$)에 기초하여, 상기 다른 키-생성 랜덤화 어레이($\overleftrightarrow{R^*}\big|^m_{(\tilde{a})}$)와 관련하여 업데이트된 공개키($K^*_{public}$)를 생성하도록 더 구성되며, 상기 업데이트된 공개키(K^*_{public})는 개인키($K_{private}$)와 쌍을 이루며, 상기 다른 키-생성 랜덤화 어레이($\overleftrightarrow{R^*}\big|^m_{(\tilde{a})}$)는 0과 상기 제1 기준 양의 정수($\tilde{a}$) 사이의 m 개의 숫자 성분들을 가지며, 그리고 상기 공개키(K_{public})는 $\overleftrightarrow{K^*}_{public}\big|^m = \mathrm{Rand}\left(\overleftrightarrow{F}_{p_2}\big|^m, p_1, \tilde{a}\right) \pmod{p_2} = p_1\left(\overleftrightarrow{F}_{p_2}\big|^m \circledast \overleftrightarrow{R^*}\big|^m_{(\tilde{a})}\right) \pmod{p_2}$ 를 나타내는 $K^*_{public} = \left(\overleftrightarrow{K^*}_{public}\big|^m, p_2\right)$ 라고도 표시되며;

상기 키 서버는 상기 제2 통신 채널을 통해 상기 송신단에 상기 업데이트된 공개키(K^*_{public})를 송신하며;

상기 키 서버로부터의 상기 업데이트된 공개키(K^{*}_{public})의 수신시, 상기 제1 프로세서는 상기 제1 저장 유닛에 저장된 상기 공개키(K_{public})가 상기 업데이트된 공개키(K^{*}_{public})가 되도록 업데이트하며;

상기 공개키(K_{public})가 상기 업데이트된 공개키(K^{*}_{public})가 되도록 업데이트한 후, 상기 제1 프로세서는 상기 업데이트된 공개키(K^{*}_{public}), 상기 제2 기준 프라임(p_2) 및 암호화 랜덤화 어레이($\overleftrightarrow{R}\big|^{m}_{(\tilde{b})}$)를 사용하여, 데이터 어레이($\overleftrightarrow{M}\big|^{m}$)에 대해 암호화 절차를 수행하며, 그리고 상기 업데이트된 공개키(K^{*}_{public}) 및 암호화 랜덤화 어레이($\overleftrightarrow{R}\big|^{m}_{(\tilde{b})}$)와 관련하여 다른 암호문($\overleftrightarrow{Cipher^{*}}$)을 획득하며, 그리고 상기 송신단은 상기 제1 통신 채널을 통해 상기 다른 암호문($\overleftrightarrow{Cipher^{*}}$)을 상기 수신단에 송신하며, 상기 다른 암호문($\overleftrightarrow{Cipher^{*}}$)은 m 개의 암호화된 숫자 성분들을 가지며; 그리고

상기 제2 프로세서에 의한 상기 다른 암호문($\overleftrightarrow{Cipher^{*}}$)의 수신시, 상기 제2 프로세서는 상기 제2 저장 유닛에 저장된 상기 개인키($K_{private}$), 상기 p-어레이($\overleftrightarrow{f}\big|^{m}$), 상기 제1 기준 프라임(p_1) 및 상기 제2 기준 프라임(p_2)을 사용하여 상기 다른 암호문($\overleftrightarrow{Cipher^{*}}$)에 대해 해독 절차를 수행하며, 그리고 평문 어레이($\overleftrightarrow{M_1}\big|^{m}$)를 획득하는, 암호화 통신 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 비대칭 키 생성 방법에 관한 것으로, 더 구체적으로는 격자 대수 기반의 포스트 퀀텀 비대칭 키 생성 방법(lattice algebra based post-quantum asymmetric key generation method) 및 시스템, 키-리프레시 방법, 암호화 방법, 복호화 방법 및 암호화 통신 시스템에 관한 것이다.

배 경 기 술

[0002] 고전적인 암호 시스템은 대칭 키 알고리즘과 비대칭 키 알고리즘의 두 가지 주요 카테고리들로 분류될 수 있다. 대칭 키 알고리즘(예를 들어, AES(Advanced Encryption Standard))은 공유 키를 사용하여 암호화 및 복호화를 수행한다. 비대칭 키 알고리즘은 서로 다른 키, 즉 쌍을 이루는 공개키와 개인키를 사용하여 암호화 및 복호화를 수행한다. 예를 들어, RSA는 최초의 공개키 암호 시스템들 중 하나이며, 그리고 보안 데이터 전송에 널리 사용되고; NTRU(number theory research unit)는 또 다른 비대칭 키 알고리즘이며; 그리고 ECC(elliptic curve cryptography)는 타원 곡선들의 대수 구조를 기반으로 하는 공개키 암호화에 대한 접근법이다. 대칭 키 알고리즘의 구현에는 두 당사자들 간의 키 교환을 위한 보안 채널이 필요하다. 비대칭 키 알고리즘의 구현에는 보안 채널이 필요하지 않지만, 비대칭 키 알고리즘은 쌍을 이루는 키의 생성, 암호화 및 복호화에 비교적 많은 양의 계산을 요구할 수 있다. RSA와 비교하여, ECC가 더 나은 보안을 제공할 수 있지만, 암호화 및 복호화에 더 많은 시간이 필요하다.

[0003] 전통적인 암호 시스템에는 다음과 같은 단점이 있을 수 있다 :

[0004] 1. 현재의 비대칭 키 알고리즘에 대한 프로토콜은 암호화 및 해독화가 한 번에 한 문자씩 처리되기 때문에 짧은 시간 내에 많은 양의 데이터를 전송할 수 없다.

[0005] 2. 현재의 비대칭키 알고리즘은 동일한 대수 그룹, 링 또는 벡터 공간에 속하는 것과 같은 수학적 특성을 가지

며 본질적으로 유사한 공개키 및 개인키를 사용하므로, 평문 공격(plaintext attack) 또는 무작위 대입 공격(brute force attack)을 받기 쉽다.

[0006] 3. 현재 비대칭 키 알고리즘의 경우, 사용자가 자신의 공개키를 새로운 공개키로 변경하면, 다른 모든 사용자는 자신의 개인키를 새로운 공개키와 쌍을 이루도록 업데이트해야 한다. 그렇지 않으면, 이전 개인키를 계속 사용하는 사용자로부터의 가능한 통신은 유효하지 않을 것이다.

[0007] 4. 시스템 설치시 모든 사용자가 키 리프레시를 수행해야 하는 경우, 키 리프레시 시간을 나타내는 중앙집중형 엔티티가 필요하다.

[0008] 5. 소인수 분해 기반 알고리즘(예를 들어, RSA, DSA) 또는 이산 로그 문제 기반 알고리즘(예를 들어, ECC)은 Shor 및 Grover의 알고리즘에 기초한 포스트 퀀텀 공격에 약하다.

[0009] 6. 분산 키 리프레시는 이러한 암호 시스템에 대한 프로토콜의 기본 정의의 일부가 아니기 때문에, RSA, AES 그리고 NTRU를 사용하는 네트워크에는 분산 키 리프레시가 존재하지 않는다.

[0010] 7. 전통적인 공개키 암호 시스템은 강하게 결합된 공개-개인키들을 갖는다(즉, 각각의 공개키는 유일한 개인키와 쌍을 이룬다). 쌍을 이룬 키들 중 하나에 대한 공격은 종종 다른 하나의 정보를 누설한다.

발명의 내용

해결하려는 과제

[0011] 따라서, 본 발명의 목적은 종래 기술의 결점들 중 적어도 하나를 완화할 수 있는 격자 대수 기반의 포스트 퀀텀 비대칭 키 생성 방법(lattice algebra based post-quantum asymmetric key generation method) 및 시스템, 키-리프레시 메커니즘, 암호화 방법, 복호화 방법 및 암호화 통신 시스템에 관한 것이다.

과제의 해결 수단

[0012] 본 개시서에 따르면, 포스트-퀀텀 비대칭 키 생성 방법은 처리 유닛에 의해 구현되며, 다음의 단계들을 포함한다 :

[0013] A) 프라임 p 그리고 시드 역할을 하는 클래식 스트링(classical string) 및 산술 함수 중 하나에 기초하여, p-벡터로 표시되고 프라임 p에 의존하는 $\vec{f}_p$ 로서 표기되는 벡터를 생성하는 단계로서, 상기 p-벡터($\vec{f}_p$)는 무한한 개수의 성분들을 가지며, 그리고 $\vec{f}_p := [f(p^0), f(p^1), f(p^2), f(p^3), \ldots]$ 로 정의되며, 여기서 f는 상기 시드 역할을 하는 클래식 스트링 및 산술 함수 중 상기 하나를 나타내는, 단계;

[0014] B) I = (p, s, t)로서 인스턴스의 개념을 정의하는 단계로서, p는 프라임이며, s 및 t는 사용자-정의되는 양의 정수들인, 단계;

[0015] C) p-벡터($\vec{f}_p$) 및 인스턴스 I = (p, s, t)에 기초하여, m 개의 성분들을 갖고 프라임 p와 관련되는 p-어레이($\overleftrightarrow{f}_p\big|_{s,t}^{m}$)를 생성하는 단계로서, 상기 p-어레이($\overleftrightarrow{f}_p\big|_{s,t}^{m}$)는 $\overleftrightarrow{f}_p\big|_{s,t}^{m} := \sum_{i=0}^{t}\left[f\left(p^{s+im}\right), \ldots, f\left(p^{s+im+(m-1)}\right)\right]$ 로 정의되며, I = (p, s, t)가 공지된 경우 상기 p-어레이($\overleftrightarrow{f}_p\big|_{s,t}^{m}$)는 $\overleftrightarrow{f}\big|^{m}$ 로도 표현되는, 단계;

[0016] D) 상기 p-어레이($\overleftrightarrow{f}\big|^{m}$)에 기초하여, 관련 매트릭스($\left[\overleftrightarrow{f}\big|^{m}\right]$)를 생성하는 단계로서, 상기 관련 매트릭스

($\left[\overleftrightarrow{f}\right|^{m}\right]$)는 :

$$\left[\overleftrightarrow{f}\right|^{m}\right]=\begin{pmatrix}\overleftrightarrow{f}\left|^{m}(0)\right. & \overleftrightarrow{f}\left|^{m}(1)\right. & \cdots & \overleftrightarrow{f}\left|^{m}(m-1)\right.\\ \overleftrightarrow{f}\left|^{m}(m-1)\right. & \overleftrightarrow{f}\left|^{m}(0)\right. & \cdots & \overleftrightarrow{f}\left|^{m}(m-2)\right.\\ \vdots & \vdots & \ddots & \vdots\\ \overleftrightarrow{f}\left|^{m}(1)\right. & \overleftrightarrow{f}\left|^{m}(2)\right. & \cdots & \overleftrightarrow{f}\left|^{m}(0)\right.\end{pmatrix}$$

[0017] 로 정의되며, 여기서 $\overleftrightarrow{f}\left|^{m}\right.(j)$는 p-어레이의 m 개의 성분들 중 (j+1) 번째 성분을 나타내는(0 ≤ j ≤ (m-1)), 단계;

[0018] E) 관련 매트릭스 $\left[\overleftrightarrow{f}\right|^{m}\right]$와 사용자-정의된 양의 정수인 모듈러스 ℓ에 기초하여, 상기 모듈러스 ℓ에 대하여 인버스 p-어레이($\overleftrightarrow{F}_{\ell}\left|^{m}\right.$)를 생성하는 단계로서, 상기 인버스 p-어레이($\overleftrightarrow{F}_{\ell}\left|^{m}\right.$)는

$$\overleftrightarrow{F}_{\ell}\left|^{m}\right.:=\left(L_{\ell}[1,0,\cdots,0]\left[\overleftrightarrow{f}\right|^{m}\right]^{*}\right)\ (\mathrm{mod}\ \ell)$$

로 정의되며, 여기서, L_{ℓ}는 상기 모듈러스 ℓ에 대한 관련 매트릭스 $\left[\overleftrightarrow{f}\right|^{m}\right]$의 행렬식(determinant)의 인버스 모듈러스를 나타내며, $L_{\ell}:=\left(\det\left[\overleftrightarrow{f}\right|^{m}\right]\right)^{-1}\ (\mathrm{mod}\ \ell)$로 정의되고, 그리고 $\left[\overleftrightarrow{f}\right|^{m}\right]^{*}$는 상기 관련 매트릭스 $\left[\overleftrightarrow{f}\right|^{m}\right]$의 수반 행렬(adjoint matrix)을 나타내는, 단계;

[0019] F) 제1 기준 프라임(p_1)을 임의로 선택하고, 그리고 상기 제1 기준 프라임(p_1), b로 표시되는 p-어레이 $\overleftrightarrow{f}\left|^{m}\right.$의 m 개의 성분들 중 가장 큰 것, 제1 기준 양의 정수($\tilde{a}$) 그리고 파라미터(m), 제2 기준 양의 정수($\tilde{b}$) 및 제3 기준 양의 정수(r)로 구성된 제2 파라미터 세트(S)와 관련된 미리 결정된 기준에 기초하여 제2 기준 프라임(p_2)을 결정하는 단계로서, 상기 미리 결정된 기준은 $p_2>\max(p_1m\tilde{a}\tilde{b},mbr)$을 포함하는, 단계;

[0020] G) 제1 기준 프라임(p_1) 및 제2 기준 프라임(p_2) 각각이 인버스 p-어레이($\overleftrightarrow{F}_{\ell}\left|^{m}\right.$)의 모듈러스(modulus)($\ell$)로서 기능하게 함으로써, 제1 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_1}\left|^{m}\right.$) 및 제2 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_2}\left|^{m}\right.$)를 획득하는 단계로서, 상기 제1 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_1}\left|^{m}\right.$)는

$$K_{\mathrm{private}}=\left(\overleftrightarrow{f}\left|^{m},p_1,\tilde{a}\right.\right)$$

로 정의되는 개인키(K_{private}) 역할을 하는, 단계; 및

[0021] H) 상기 제2 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_2}\left|^{m}\right.$), 상기 제1 기준 프라임($p_1$), 상기 제2 기준 프라임($p_2$) 및 상기 키-생성 랜덤화 어레이($\overleftrightarrow{R}\left|^{m}_{(\tilde{a})}\right.$)와 관련하여 공개키($K_{\mathrm{public}}$)를 생성하는 단계로서, 키-생성 랜덤화 어레이($\overleftrightarrow{R}\left|^{m}_{(\tilde{a})}\right.$)는 0과 제1 기준 양의 정수($\tilde{a}$) 사이의 m 개의 숫자 성분을 가지며, 그리고 공개키(K_{public})는 개인키(K_{private})와 쌍을 이루며, 그리고 m 개의 숫자 성분들을 포함하고 $K_{\mathrm{public}}=\left(\overleftrightarrow{K}_{\mathrm{public}}\left|^{m},p_2\right.\right)$라고도 표시

되는 어레이($\overleftrightarrow{K}_{\text{public}}\Big|^{m}$)이며, $\overleftrightarrow{K}_{\text{public}}\Big|^{m} := \text{Rand}\left(\overleftrightarrow{F}_{p_2}\Big|^{m}, p_1, \tilde{a}\right) \pmod{p_2}$ 를 나타내며, $\text{Rand}\left(\overleftrightarrow{F}_{p_2}\Big|^{m}, p_1, \tilde{a}\right)$ 는 키 생성 랜덤화 어레이($\overleftrightarrow{R}\Big|^{m}_{(\tilde{a})}$)에 대한 제2 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_2}\Big|^{m}$)의 키 생성 랜덤화 함수이며, 그리고 $\text{Rand}\left(\overleftrightarrow{F}_{p_2}\Big|^{m}, p_1, \tilde{a}\right) = p_1\left(\overleftrightarrow{F}_{p_2}\Big|^{m} \circledast \overleftrightarrow{R}\Big|^{m}_{(\tilde{a})}\right)$ 로 정의되며, 여기서 $\circledast$ 는 컨볼루션 곱셈 연산자를 나타내는, 단계.

[0022] 이 개시서에 따르면, 암호화 방법은 프로세서에 의해 구현되며, 상기 암호화 방법은 :

[0023] 이 개시서의 포스트-퀀텀 비대칭 키 생성 방법에 따라 생성되는 공개키(K_{public}), 이 개시서의 포스트-퀀텀 비대칭 키 생성 방법에서 사용되는 제2 기준 프라임(p_2), 그리고 0과 이 개시서의 포스트-퀀텀 비대칭 키 생성 방법에서 사용되는 제2 기준 양의 정수($\tilde{b}$) 사이의 m 개의 숫자 성분들을 갖는 암호화 랜덤화 어레이($\overleftrightarrow{R}\Big|^{m}_{(\tilde{b})}$)를 사용하여, 전송될 평문에 대응하고 m 개의 숫자 성분들을 갖는 데이터 어레이($\overleftrightarrow{M}\Big|^{m}$)에 대한 암호화 절차를 수행하고, 상기 암호화 랜덤화 어레이($\overleftrightarrow{R}\Big|^{m}_{(\tilde{b})}$)에 관한 암호문($\overrightarrow{Cipher}\Big|^{m}$)을 획득하는 단계로서, 상기 암호문($\overleftarrow{Cipher}\Big|^{m}$)은 m 개의 암호화된 숫자 성분들을 갖는, 단계를 포함한다.

[0024] 이 개시서에 따르면, 해독 방법은 프로세서에 의해 구현되며, 상기 해독 방법은 :

[0025] 이 개시서의 포스트-퀀텀 비대칭 키 생성 방법에서 사용되는 p-어레이($\overleftrightarrow{f}\Big|^{m}$), 개인키(K_{private}), 제1 기준 프라임(p_1) 및 제2 기준 프라임(p_2)을 사용하여, 암호문($\overrightarrow{Cipher}\Big|^{m}$)에 대해 해독 절차를 수행하고, m 개의 해독된 숫자성분들을 갖는 평문 어레이($\overleftrightarrow{M_1}\Big|^{m}$)를 획득하는 단계를 포함하며,

[0026] 여기서, 상기 암호문($\overrightarrow{Cipher}\Big|^{m}$)은 :

[0027] 이 개시서의 포스트-퀀텀 비대칭 키 생성 방법에 따라 생성되는 공개키, 이 개시서의 포스트-퀀텀 비대칭 키 생성 방법에서 사용되는 제2 기준 프라임(p_2), 그리고 0과 이 개시서의 포스트-퀀텀 비대칭 키 생성 방법에서 사용되는 제2 기준 양의 정수($\tilde{b}$) 사이의 m 개의 숫자 성분들을 갖는 암호화 랜덤화 어레이($\overleftrightarrow{R}\Big|^{m}_{(\tilde{b})}$)를 사용하여, 전송될 평문에 대응하고 m 개의 숫자 성분들을 갖는 데이터 어레이($\overleftrightarrow{M}\Big|^{m}$)에 대한 암호화 절차를 수행하고, 그리고 상기 암호화 랜덤화 어레이($\overleftrightarrow{R}\Big|^{m}_{(\tilde{b})}$)와 관련되고 m 개의 암호화된 숫자 성분들을 갖는 암호문($\overleftarrow{Cipher}\Big|^{m}$)을 획득함으로써 생성된다.

[0028] 이 개시서에 따르면, 포스트-퀀텀 비대칭 키 생성 시스템은 :

[0029] 프라임 p 그리고 시드 역할을 하는 클래식 스트링(classical string) 및 산술 함수 중 하나에 기초하여, 프라임 p와 관련되고 무한한 개수의 성분들을 갖는 p-벡터($\overrightarrow{f}_p$)를 생성하도록 구성된 p-벡터 생성 모듈로서, 상기 p-

벡터($\vec{f}_p$)는 $\vec{f}_p := [f(p^0), f(p^1), f(p^2), f(p^3), \ldots]$ 로 정의되며, 여기서 f는 상기 시드 역할을 하는 클래식 스트링 및 산술 함수 중 상기 하나를 나타내는, p-벡터 생성 모듈;

[0030] 상기 p-벡터 생성 모듈에 연결되고, 그리고 상기 p-벡터($\vec{f}_p$)에 기초하여, m 개의 성분들을 갖고 프라임 p와 관련되는 p-어레이($\overleftrightarrow{f}_p\big|_{s,t}^{m}$)를 생성하도록 구성되는 p-어레이 생성 모듈로서, 상기 p-어레이($\overleftrightarrow{f}_p\big|_{s,t}^{m}$)는

$$\overleftrightarrow{f}_p\Big|_{s,t}^{m} := \sum_{i=0}^{t}\left[f\left(p^{s+im}\right), \ldots, f\left(p^{s+im+(m-1)}\right)\right]$$

로 정의되며, 파라미터들 m, s 및 t 각각은 사용자-정의되는 양의 정수이며, 그리고 프라임 p 및 파라미터들 s, t는 협력하여 제1 파라미터 세트(I)를 구성하며, 상기 p-어레이($\overleftrightarrow{f}_p\big|_{s,t}^{m}$)는 $\overleftrightarrow{f}\big|^{m}$ 로도 표현되는, p-어레이 생성 모듈;

[0031] 상기 p-어레이 생성 모듈에 연결되고, 그리고 상기 p-어레이($\overleftrightarrow{f}\big|^{m}$)에 기초하여, 관련 매트릭스($\left[\overleftrightarrow{f}\big|^{m}\right]$)를 생성하도록 구성된 관련 매트릭스 생성 모듈로서, 상기 관련 매트릭스($\left[\overleftrightarrow{f}\big|^{m}\right]$)는 :

$$\left[\overleftrightarrow{f}\big|^{m}\right] = \begin{pmatrix} \overleftrightarrow{f}\big|^{m}(0) & \overleftrightarrow{f}\big|^{m}(1) & \cdots & \overleftrightarrow{f}\big|^{m}(m-1) \\ \overleftrightarrow{f}\big|^{m}(m-1) & \overleftrightarrow{f}\big|^{m}(0) & \cdots & \overleftrightarrow{f}\big|^{m}(m-2) \\ \vdots & \vdots & \ddots & \vdots \\ \overleftrightarrow{f}\big|^{m}(1) & \overleftrightarrow{f}\big|^{m}(2) & \cdots & \overleftrightarrow{f}\big|^{m}(0) \end{pmatrix}$$

[0032] 로 정의되며, 여기서 $\overleftrightarrow{f}\big|^{m}$ (j)는 p-어레이의 m 개의 성분들 중 (j+1) 번째 성분을 나타내는(0 ≤ j ≤ (m-1)), 관련 매트릭스 생성 모듈;

[0033] 상기 관련 매트릭스 생성 모듈에 연결되고, 그리고 상기 관련 매트릭스 $\left[\overleftrightarrow{f}\big|^{m}\right]$와 사용자-정의된 양의 정수인 모듈러스 ℓ 에 기초하여, 상기 모듈러스 ℓ 에 대하여 인버스 p-어레이($\overleftrightarrow{F}_\ell\big|^{m}$)를 생성하도록 구성된 인버스 p-어레이 생성 모듈로서, 상기 인버스 p-어레이($\overleftrightarrow{F}_\ell\big|^{m}$)는

$$\overleftrightarrow{F}_\ell\Big|^{m} := \left(L_\ell[1, 0, \cdots, 0]\left[\overleftrightarrow{f}\big|^{m}\right]^{*}\right) \pmod{\ell}$$

로 정의되며, 여기서, L_ℓ 는 상기 모듈러스 ℓ 에 대한 관련 매트릭스 $\left[\overleftrightarrow{f}\big|^{m}\right]$ 의 행렬식(determinant)의 인버스 모듈러스를 나타내며,

$$L_\ell := \left(\det\left[\overleftrightarrow{f}\big|^{m}\right]\right)^{-1} \pmod{\ell}$$

로 정의되고, 그리고 $\left[\overleftrightarrow{f}\big|^{m}\right]^{*}$ 는 상기 관련 매트릭스 $\left[\overleftrightarrow{f}\big|^{m}\right]$의 수반 행렬(adjoint matrix)을 나타내는, 인버스 p-어레이 생성 모듈;

[0034] 제1 기준 프라임(p_1)을 임의로 선택하고, 그리고 상기 제1 기준 프라임(p_1), b로 표시되는 p-어레이 $\overleftrightarrow{f}\big|^{m}$ 의 m 개의 성분들 중 가장 큰 것, 제1 기준 양의 정수($\tilde{a}$) 그리고 파라미터(m), 제2 기준 양의 정수($\tilde{b}$) 및 제3 기준 양의 정수(r)로 구성된 제2 파라미터 세트(S)와 관련된 미리 결정된 기준에 기초하여 제2 기준 프라임(p_2)을 결정하도록 구성된 기준 프라임 결정 모듈로서, 상기 미리 결정된 기준은 $p_2 > \max(p_1 m\tilde{a}\tilde{b}, mbr)$ 을

포함하는, 기준 프라임 결정 모듈;

[0035] 상기 인버스 p-어레이 생성 모듈 및 상기 기준 프라임 결정 모듈에 연결되고, 그리고 제1 기준 프라임(p_1)이 인버스 p-어레이($\overleftrightarrow{F}_{\ell}\Big|^{m}$)의 모듈러스(modulus)(ℓ)로서 기능하게 함으로써, 제1 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_1}\Big|^{m}$)를 획득하도록 구성된 개인키 생성 모듈로서, 상기 제1 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_1}\Big|^{m}$)는 $K_{\text{private}} = \left(\overleftrightarrow{f}\Big|^{m}, p_1, \tilde{a}\right)$ 로 정의되는 개인키(K_{private}) 역할을 하는, 개인키 생성 모듈; 및

[0036] 상기 인버스 p-어레이 생성 모듈 및 상기 기준 프라임 결정 모듈에 연결되고, 그리고 제2 기준 프라임(p_2)이 인버스 p-어레이($\overleftrightarrow{F}_{\ell}\Big|^{m}$)의 모듈러스(modulus)(ℓ)로서 기능하게 함으로써, 제2 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_2}\Big|^{m}$)를 획득하도록 구성되고, 상기 제2 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_2}\Big|^{m}$), 상기 제1 기준 프라임(p_1), 상기 제2 기준 프라임(p_2) 및 상기 키-생성 랜덤화 어레이($\overleftrightarrow{R}\Big|^{m}_{(\tilde{a})}$)에 기초하여 키-생성 랜덤화 어레이 $\overleftrightarrow{R}\Big|^{m}_{(\tilde{a})}$ 와 관련하여 공개키(K_{public})를 생성하도록 구성되는 공개키 생성 모듈로서, 상기 키-생성 랜덤화 어레이($\overleftrightarrow{R}\Big|^{m}_{(\tilde{a})}$)는 0과 제1 기준 양의 정수($\tilde{a}$) 사이의 m 개의 숫자 성분을 가지며, 그리고 공개키(K_{public})는 개인키(K_{private})와 쌍을 이루며, 그리고 m 개의 숫자 성분들을 포함하고 $K_{\text{public}} = \left(\overleftrightarrow{K}_{\text{public}}\Big|^{m}, p_2\right)$ 라고도 표시되는 어레이($\overleftrightarrow{K}_{\text{public}}\Big|^{m}$)이며, $\overleftrightarrow{K}_{\text{public}}\Big|^{m} := \text{Rand}\left(\overleftrightarrow{F}_{p_2}\Big|^{m}, p_1, \tilde{a}\right) \pmod{p_2}$ 를 나타내는, 공개키 생성 모듈을 포함하며,

[0037] 여기서, $\text{Rand}\left(\overleftrightarrow{F}_{p_2}\Big|^{m}, p_1, \tilde{a}\right)$ 는 키 생성 랜덤화 어레이($\overleftrightarrow{R}\Big|^{m}_{(\tilde{a})}$)에 대한 제2 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_2}\Big|^{m}$)의 키 생성 랜덤화 함수이며, 그리고 $\text{Rand}\left(\overleftrightarrow{F}_{p_2}\Big|^{m}, p_1, \tilde{a}\right) = p_1\left(\overleftrightarrow{F}_{p_2}\Big|^{m} \circledast \overleftrightarrow{R}\Big|^{m}_{(\tilde{a})}\right)$ 로 정의되며, 여기서 $\circledast$ 는 컨볼루션 곱셈 연산자를 나타낸다.

[0038] 이 개시서에 따르면, 암호화 통신 시스템은 키 서버, 송신단 및 수신단을 포함하며,

[0039] 상기 키 서버는 :

[0040] 프라임 p 그리고 시드 역할을 하는 클래식 스트링(classical string) 및 산술 함수 중 하나에 기초하여, 프라임 p와 관련되고 무한한 개수의 성분들을 갖는 p-벡터($\vec{f}_p$)를 생성하도록 구성된 p-벡터 생성 모듈로서, 상기 p-벡터($\vec{f}_p$)는 $\vec{f}_p := [f(p^0), f(p^1), f(p^2), f(p^3), \ldots]$ 로 정의되며, 여기서 f는 상기 시드 역할을 하는 클래식 스트링 및 산술 함수 중 상기 하나를 나타내는, p-벡터 생성 모듈;

[0041] 상기 p-벡터 생성 모듈에 연결되고, 그리고 상기 p-벡터($\vec{f}_p$)에 기초하여, m 개의 성분들을 갖고 프라임 p와

관련되는 p-어레이($\overleftrightarrow{f}_p\big|_{s,t}^m$)를 생성하도록 구성되는 p-어레이 생성 모듈로서, 상기 p-어레이($\overleftrightarrow{f}_p\big|_{s,t}^m$)는

$$\overleftrightarrow{f}_p\Big|_{s,t}^m := \sum_{i=0}^{t}\left[f\left(p^{s+im}\right),\ldots,f\left(p^{s+im+(m-1)}\right)\right]$$

로 정의되며, 파라미터들 m, s 및 t 각각은 사용자-정의되는 양의 정수이며, 그리고 프라임 p 및 파라미터들 s, t는 협력하여 제1 파라미터 세트(I)를 구성하며, 상기 p-어레이($\overleftrightarrow{f}_p\big|_{s,t}^m$)는 $\overleftrightarrow{f}\big|^m$ 로도 표현되는, p-어레이 생성 모듈;

[0042] 상기 p-어레이 생성 모듈에 연결되고, 그리고 상기 p-어레이($\overleftrightarrow{f}\big|^m$)에 기초하여, 관련 매트릭스($\left[\overleftrightarrow{f}\big|^m\right]$)를 생성하도록 구성된 관련 매트릭스 생성 모듈로서, 상기 관련 매트릭스($\left[\overleftrightarrow{f}\big|^m\right]$)는 :

[0043] $$\left[\overleftrightarrow{f}\big|^m\right] = \begin{pmatrix} \overleftrightarrow{f}\big|^m(0) & \overleftrightarrow{f}\big|^m(1) & \cdots & \overleftrightarrow{f}\big|^m(m-1) \\ \overleftrightarrow{f}\big|^m(m-1) & \overleftrightarrow{f}\big|^m(0) & \cdots & \overleftrightarrow{f}\big|^m(m-2) \\ \vdots & \vdots & \ddots & \vdots \\ \overleftrightarrow{f}\big|^m(1) & \overleftrightarrow{f}\big|^m(2) & \cdots & \overleftrightarrow{f}\big|^m(0) \end{pmatrix}$$

로 정의되며, 여기서 $\overleftrightarrow{f}\big|^m$ (j)는 p-어레이의 m 개의 성분들 중 (j+1) 번째 성분을 나타내는(0 ≤ j ≤ (m-1)), 관련 매트릭스 생성 모듈;

[0044] 상기 관련 매트릭스 생성 모듈에 연결되고, 그리고 상기 관련 매트릭스 $\left[\overleftrightarrow{f}\big|^m\right]$와 사용자-정의된 양의 정수인 모듈러스 ℓ 에 기초하여, 상기 모듈러스 ℓ 에 대하여 인버스 p-어레이($\overleftrightarrow{F}_\ell\big|^m$)를 생성하도록 구성된 인버스 p-어레이 생성 모듈로서, 상기 인버스 p-어레이($\overleftrightarrow{F}_\ell\big|^m$)는

$$\overleftrightarrow{F}_\ell\Big|^m := \left(L_\ell[1,0,\cdots,0]\left[\overleftrightarrow{f}\big|^m\right]^*\right) \pmod{\ell}$$

로 정의되며, 여기서, L_ℓ 는 상기 모듈러스 ℓ 에 대한 관련 매트릭스 $\left[\overleftrightarrow{f}\big|^m\right]$ 의 행렬식(determinant)의 인버스 모듈러스를 나타내며,

$$L_\ell := \left(\det\left[\overleftrightarrow{f}\big|^m\right]\right)^{-1} \pmod{\ell}$$

로 정의되고, 그리고 $\left[\overleftrightarrow{f}\big|^m\right]^*$ 는 상기 관련 매트릭스 $\left[\overleftrightarrow{f}\big|^m\right]$의 수반 행렬(adjoint matrix)을 나타내는, 인버스 p-어레이 생성 모듈;

[0045] 제1 기준 프라임(p_1)을 임의로 선택하고, 그리고 상기 제1 기준 프라임(p_1), b로 표시되는 p-어레이 $\overleftrightarrow{f}\big|^m$ 의 m 개의 성분들 중 가장 큰 것, 제1 기준 양의 정수($\tilde{a}$) 그리고 파라미터(m), 제2 기준 양의 정수($\tilde{b}$) 및 제3 기준 양의 정수(r)로 구성된 제2 파라미터 세트(S)와 관련된 미리 결정된 기준에 기초하여 제2 기준 프라임(p_2)을 결정하도록 구성된 기준 프라임 결정 모듈로서, 상기 미리 결정된 기준은 $p_2 > \max(p_1 m\tilde{a}\tilde{b}, mbr)$ 을 포함하는, 기준 프라임 결정 모듈;

[0046] 상기 인버스 p-어레이 생성 모듈 및 상기 기준 프라임 결정 모듈에 연결되고, 그리고 제1 기준 프라임(p_1)이 인버스 p-어레이($\overleftrightarrow{F}_\ell\big|^m$)의 모듈러스(modulus)(ℓ)로서 기능하게 함으로써, 제1 기준 인버스 p-어레이

($\overleftrightarrow{F}_{p_1}\big|^m$)를 획득하도록 구성된 개인키 생성 모듈로서, 상기 제1 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_1}\big|^m$)는 $K_{\text{private}} = \left(\overleftrightarrow{f}\big|^m, p_1, \tilde{a}\right)$ 로 정의되는 개인키(K_{private}) 역할을 하는, 개인키 생성 모듈; 및

[0047] 상기 인버스 p-어레이 생성 모듈 및 상기 기준 프라임 결정 모듈에 연결되고, 그리고 제2 기준 프라임(p_2)이 인버스 p-어레이($\overleftrightarrow{F}_{\ell}\big|^m$)의 모듈러스(modulus)(ℓ)로서 기능하게 함으로써, 제2 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_2}\big|^m$)를 획득하도록 구성되고, 상기 제2 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_2}\big|^m$), 상기 제1 기준 프라임(p_1), 상기 제2 기준 프라임(p_2) 및 상기 키-생성 랜덤화 어레이($\overleftrightarrow{R}\big|^m_{(\tilde{a})}$)에 기초하여 키-생성 랜덤화 어레이 $\overleftrightarrow{R}\big|^m_{(\tilde{a})}$ 와 관련하여 공개키(K_{public})를 생성하도록 구성되는 공개키 생성 모듈로서, 상기 키-생성 랜덤화 어레이($\overleftrightarrow{R}\big|^m_{(\tilde{a})}$)는 0과 제1 기준 양의 정수($\tilde{a}$) 사이의 m 개의 숫자 성분을 가지며, 그리고 공개키(K_{public})는 개인키(K_{private})와 쌍을 이루며, 그리고 m 개의 숫자 성분들을 포함하고 $K_{\text{public}} = \left(\overleftrightarrow{K}_{\text{public}}\big|^m, p_2\right)$ 라고도 표시되는 어레이($\overleftrightarrow{K}_{\text{public}}\big|^m$)이며, $\overleftrightarrow{K}_{\text{public}}\big|^m := \text{Rand}\left(\overleftrightarrow{F}_{p_2}\big|^m, p_1, \tilde{a}\right) \pmod{p_2}$ 를 나타내는, 공개키 생성 모듈을 포함하며,

[0048] $\text{Rand}\left(\overleftrightarrow{F}_{p_2}\big|^m, p_1, \tilde{a}\right)$ 는 키 생성 랜덤화 어레이($\overleftrightarrow{R}\big|^m_{(\tilde{a})}$)에 대한 제2 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_2}\big|^m$)의 키 생성 랜덤화 함수이며, 그리고 $\text{Rand}\left(\overleftrightarrow{F}_{p_2}\big|^m, p_1, \tilde{a}\right) = p_1\left(\overleftrightarrow{F}_{p_2}\big|^m \circledast \overleftrightarrow{R}\big|^m_{(\tilde{a})}\right)$ 로 정의되며, 여기서 $\circledast$ 는 컨볼루션 곱셈 연산자를 나타내며,

[0049] 상기 송신단은 상기 공개키(K_{public}), 상기 제2 기준 프라임(p_2) 및 상기 제2 기준 양의 정수($\tilde{b}$)를 저장하는 제1 저장 유닛, 그리고 상기 제1 저장 유닛에 연결된 제1 프로세서를 포함하며,

[0050] 상기 수신단은 상기 개인키(K_{private}), 상기 p-어레이($\overleftrightarrow{f}\big|^m$), 상기 제1 기준 프라임(p_1) 및 상기 제2 기준 프라임(p_2)을 저장하는 제2 저장 유닛, 그리고 상기 제2 저장 유닛에 연결된 제2 프로세서를 포함하며,

[0051] 상기 수신단에 전송될 평문에 대응하고 그리고 m 개의 숫자 성분들을 갖는 데이터 어레이($\overleftrightarrow{M}\big|^m$)에 대해, 상기 제1 프로세서는 상기 제1 저장 유닛에 저장된 공개키(K_{public}) 및 제2 기준 프라임(p_2), 그리고 0과 상기 제2 기준 양의 정수($\tilde{b}$) 사이의 m 개의 숫자 성분들을 갖는 암호화 랜덤화 어레이($\overleftrightarrow{R}\big|^m_{(\tilde{b})}$)를 사용하여, 상기 데이터 어레이($\overleftrightarrow{M}\big|^m$)에 대한 암호화 절차를 수행하고, 그리고 상기 암호화 랜덤화 어레이($\overleftrightarrow{R}\big|^m_{(\tilde{b})}$)에 관한 암호문

($\overleftrightarrow{Cipher}\Big|^m$)을 획득하며, 그리고 상기 송신단은 제1 통신 채널을 통해 상기 수신단에 상기 암호문 ($\overleftrightarrow{Cipher}\Big|^m$)을 송신하며, 상기 암호문($\overleftrightarrow{Cipher}\Big|^m$)은 m 개의 암호화된 숫자 성분들을 가지며,

[0052] 상기 제2 프로세서에 의한 상기 암호문($\overleftrightarrow{Cipher}\Big|^m$)의 수신시, 상기 제2 프로세서는 상기 제2 저장 유닛에 저장된 개인키($K_{private}$), p-어레이($\overleftrightarrow{f}\Big|^m$), 제1 기준 프라임(p_1) 및 제2 기준 프라임(p_2)을 사용하여, 암호문 ($\overleftrightarrow{Cipher}\Big|^m$)에 대해 해독 절차를 수행하고, m 개의 해독된 숫자 성분들을 갖고 상기 데이터 어레이($\overleftrightarrow{M}\Big|^m$) 와 동일한 평문 어레이($\overleftrightarrow{M_1}\Big|^m$)를 획득한다.

도면의 간단한 설명

[0053] 본 개시서의 다른 특징들 및 이점들은 첨부 도면을 참조하여 실시예(들)에 대한 다음의 상세한 설명에서 명백해질 것이다.

도 1은 본 발명에 따른 암호화된 통신 시스템의 일 실시예를 나타내는 블록도이다.

도 2는 암호화된 통신 시스템의 키 서버를 도시하는 블록도이다.

도 3 및 도 4는 본 발명에 따른 키 생성 절차의 단계들을 설명하는 흐름도를 협력적으로 형성한다.

도 5는 암호화된 통신 시스템의 송신단을 나타내는 블록도이다.

도 6은 암호화된 통신 시스템의 수신단을 나타내는 블록도이다.

도 7은 본 발명에 따른 암호화 절차의 단계들을 설명하는 흐름도이다.

도 8은 본 발명에 따른 해독 절차의 단계들을 설명하는 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0054] 본 개시서가 보다 상세하게 설명되기 전에, 적절한 것으로 고려되는 경우, 참조부호들 또는 참조부호들의 끝부분(terminal portion)은 옵션으로 유사한 특성을 가질 수 있는 대응하는 또는 유사한 요소들을 나타내기 위해 도면들 사이에서 반복되었다는 점에 유의해야 한다.

[0055] 도 1을 참조하면, 본 개시서에 따른 암호화된 통신 시스템(100)의 실시예는 키 서버(1)를 포함하고 다수의 사용자단(user end)을 포함하는 것으로 도시되어 있다. 각각의 사용자단은 암호화 절차 및 해독 절차를 사용하는 통신 프로토콜에 기초하여 다른 사용자단과 통신할 수 있다. 각각의 사용자단은 메시지를 송신할 때 송신단으로서 기능하고, 메시지를 수신할 때 수신단으로서 기능할 수 있다. 도 1은 2 개의 사용자단들을 간단히 예시하는데, 그 중 하나는 송신단(2)으로서 기능하고, 다른 하나는 수신단(3)으로서 기능하지만, 본 개시서는 이와 관련하여 제한되지 않는다. 송신단(2)은 저장 유닛(21), 그리고 저장 유닛(21)에 연결된 프로세서(22)를 포함한다. 수신단(3)은 저장 유닛(31), 그리고 저장 유닛(31)에 연결된 프로세서(32)를 포함한다. 이 실시예에서, 키 서버(1)는 송신단(2) 및 수신단(3)과 독립적이다. 그러나, 다른 실시예들에서 키 서버(1)는 송신단(2) 내에 통합될 수 있다.

[0056] 키 서버(1)는 포스트-퀀텀 비대칭 키 생성 시스템(10)으로 구성된다. 도 2를 참조하면, 포스트-퀀텀 비대칭 키 시스템(10)은 p-벡터(prime vector) 생성 모듈(11), 상기 p-벡터 생성 모듈(11)에 연결된 p-어레이(prime array) 생성 모듈(13), 상기 p-어레이 생성 모듈(13)에 연결된 관련 매트릭스 생성 모듈(14), 상기 관련 매트릭스 생성 모듈(14)에 연결된 인버스 p-어레이 생성 모듈(15), 기준(reference) 프라임 결정 모듈(16), 상기 인버스 p-어레이 생성 모듈(15)과 상기 기준 프라임 결정 모듈(16)에 연결된 개인키 생성 모듈(17), 상기 인버스 p-어레이 생성 모듈(15)과 상기 기준 프라임 결정 모듈(16)에 연결된 공개키 생성 모듈(18), 그리고 상기 p-어레이 생성 모듈(13), 상기 기준 프라임 결정 모듈(16), 상기 개인키 생성 모듈(17) 및 상기 공개키 생성 모듈(18)에 연결된 저장 모듈(19)을 포함한다. 상기 p-벡터 생성 모듈(11), 상기 p-어레이 생성 모듈(13), 상기 관련

매트릭스 생성 모듈(14), 상기 인버스 p-어레이 생성 모듈(15), 상기 기준 프라임 결정 모듈(16), 상기 개인키 생성 모듈(17) 및 상기 공개키 생성 모듈(18)은 프로세서(미도시) 내에 통합될 수 있지만, 본 발명은 이와 관련하여 한정되지 않는다는 것에 유의한다.

[0057] 암호화된 통신 시스템(100)을 사용하기 전에, 키 서버(1)는 암호화 및 복호화를 위해 비대칭 키들(예를 들어, 개인키, 그리고 상기 개인키와 쌍을 이루는 적어도 하나의 공개키)을 생성한다. 도 3 및 도 4는 도 2에 예시된 포스트-퀀텀 비대칭 키 생성 시스템(10)이 비대칭 키 생성 절차를 수행하는 방법을 협력적으로 예시한다.

[0058] 단계 S31에서, p-벡터 생성 모듈(11)은, 프라임 p 그리고 시드 역할을 하는 산술 함수 및 클래식 스트링(classical string)(예를 들어, 정수들의 시퀀스, 또는 ASCII 코드와 같은 정수로 매핑될 수 있는 문자들) 중 하나(즉, 산술 함수 또는 클래식 스트링 중 하나가 시드로서 역할함)에 기초하여, 프라임 p와 관련되고 무한한 개수의 성분을 갖는 p-벡터 $\vec{f}_p$ 를 생성한다. 이 실시예에서, p-벡터 $\vec{f}_p$ 는 다음과 같이 정의된다 :

[0059] $$\vec{f}_p := [f(p^0), f(p^1), f(p^2), f(p^3), \ldots]$$

[0060] 여기서, f는 시드 역할을 하는 산술 함수 또는 클래식 스트링이다(후자의 경우, $f(p^n)$는 클래식 스트링에서 n번째 문자를 나타낸다).

[0061] 일례에서, 시드는 다음의 산술 함수 $f(p^n)$로서 예시된다 :

[0062] n = 0인 경우, $f(p^n) = 1$; 그리고

[0063] n > 0인 경우, $f(p^n) = (-1)^n \times (\sqrt{p}$의 소수 부분의 n 번째 수) -----(1)

[0064] 단계 S32에서, p-어레이 생성 모듈(13)은, p-벡터 $\vec{f}_p$ 에 기초하여, m 개의 성분을 가지며 프라임 p와 관련되고 다음과 같이 정의되는 p-어레이 $\overleftrightarrow{f}_p\big|_{s,t}^{m}$ 를 생성한다 :

[0065] $$\overleftrightarrow{f}_p\big|_{s,t}^{m} := \sum_{i=0}^{t} \left[f\left(p^{s+im}\right), \ldots, f\left(p^{s+im+(m-1)}\right) \right]$$

[0066] 여기서, 파라미터들 m, s 및 t 각각은 사용자-정의되는 양의 정수이며, 그리고 프라임 p 및 파라미터들 s, t는 협력하여 제1 파라미터 세트 I를 구성한다(이하, I=(p, s, t) 라고도 지칭됨). p-어레이 $\overleftrightarrow{f}_p\big|_{s,t}^{m}$의 표현은 이후에 $\overleftrightarrow{f}\big|^{m}$ 로 간략화될 수 있다. 예를 들어, I=(3, *0*, *1*) 그리고 m = 5일 때, p-벡터 $\vec{f}_3$ 및 p-어레이 $\overleftrightarrow{f}_3\big|_{0,1}^{5}$ (또는 간단히 $\overleftrightarrow{f}\big|^{5}$)는 각각 다음의 방정식 (2) 및 방정식 (3)과 같이 구할 수 있다.

[0067] $\vec{f}_3$ = [1, -7, 3, -2, 0, -5, 0, -8, 0, -7, …] --- (2)

[0068] $$\begin{aligned} \overleftrightarrow{f}_3\big|_{0,1}^{5} &= [1-5, -7+0, 3-8, -2+0, 0-7] \\ &= [-4, -7, -5, -2, -7]. \end{aligned}$$ --- (3)

[0069] 다른 예로서, 비밀 함수 f와 비밀 인스턴스 I에 의해 $\overleftrightarrow{f}\big|^{5}$ 가 주어지게 한다 :

[0070] $$\overleftrightarrow{f}\Big|^{5} = [2, 81, 27, 9, 3] \quad \text{--- (4)}$$

[0071] 상기 2 개의 예들은 시드 및 제1 파라미터 세트 I에 기초하여 p-어레이가 생성되는 방법을 예시적으로 보여준다. 제1 파라미터 세트 I를 저장함으로써, 대응하는 p-어레이는 언제든지 시드에 기초하여 획득될 수 있다.

[0072] 단계 S33에서, p-어레이 생성 모듈(13)은 p-어레이 $\overleftrightarrow{f}\Big|^{m}$ 의 m 개의 성분들 각각이 0이 아닌지 여부를 판단한다. 판단이 긍정적일 때(즉, p-어레이 $\overleftrightarrow{f}\Big|^{m}$ 의 m 개의 성분들 모두가 0이 아닐 때), p-어레이 생성 모듈(13)은 p-어레이 $\overleftrightarrow{f}\Big|^{m}$ 를 관련 매트릭스 생성 모듈(14)에 출력하고, p-어레이 $\overleftrightarrow{f}\Big|^{m}$ 를 저장 모듈(19)에 저장한다(단계 S34). 예를 들어, 방정식 (3) 및 방정식 (4) 각각에 도시된 바와 같이 p-어레이 $\overleftrightarrow{f}\Big|^{m}$ 의 5 개의 성분들 모두가 0이 아니다. p-어레이 생성 모듈(13)이 p-어레이 $\overleftrightarrow{f}\Big|^{m}$ 의 m 개의 성분들 중 임의의 하나가 0이라고 판단할 때, 흐름도는 단계 S32로 되돌아가서, 사용자가 상이한 제1 파라미터 세트 I(즉, 새로운 제1 파라미터 세트 I에서의 프라임 p 및 파라미터들 s, t 중 적어도 하나는 원래의 제1 파라미터 세트 I에서의 것과 다르다)를 단계 S32에 적용할 수 있게 한다. 단계 S32는 단계 S33에서의 판단이 긍정적일 때까지 상이한 제1 파라미터 세트들 I로 반복될 수 있다.

[0073] 단계 S35에서, 관련 매트릭스 생성 모듈(14)은 p-어레이 생성 모듈(13)로부터 수신된 p-어레이 $\overleftrightarrow{f}\Big|^{m}$ 에 기초하여 관련 매트릭스 $\left[\overleftrightarrow{f}\Big|^{m}\right]$ 를 생성하며, 그리고 상기 관련 매트릭스 $\left[\overleftrightarrow{f}\Big|^{m}\right]$ 를 인버스 p-어레이 생성 모듈(15)에 출력한다. 관련 매트릭스 $\left[\overleftrightarrow{f}\Big|^{m}\right]$ 는 다음과 같이 정의된다 :

[0074] $$\left[\overleftrightarrow{f}\Big|^{m}\right] = \begin{pmatrix} \overleftrightarrow{f}\Big|^{m}(0) & \overleftrightarrow{f}\Big|^{m}(1) & \cdots & \overleftrightarrow{f}\Big|^{m}(m-1) \\ \overleftrightarrow{f}\Big|^{m}(m-1) & \overleftrightarrow{f}\Big|^{m}(0) & \cdots & \overleftrightarrow{f}\Big|^{m}(m-2) \\ \vdots & \vdots & \ddots & \vdots \\ \overleftrightarrow{f}\Big|^{m}(1) & \overleftrightarrow{f}\Big|^{m}(2) & \cdots & \overleftrightarrow{f}\Big|^{m}(0) \end{pmatrix}$$

[0075] 여기서, $\overleftrightarrow{f}\Big|^{m}(j)$ 는 p-어레이의 m 개의 성분들 중 (j+1) 번째 성분을 나타낸다(여기서, $0 \le j \le (m-1)$). 방정식 (4)에서의 p-어레이 $\overleftrightarrow{f}\Big|^{5}$ 에 이어, 관련 매트릭스 생성 모듈(14)에 의해 생성되는 관련 매트릭스는 방정식 (5)에 도시된 바와 같을 것이다 :

$$\left[\overleftrightarrow{f}\Big|^{5}\right]=\begin{pmatrix}2 & 81 & 27 & 9 & 3\\ 3 & 2 & 81 & 27 & 9\\ 9 & 3 & 2 & 81 & 27\\ 27 & 9 & 3 & 2 & 81\\ 81 & 27 & 9 & 3 & 2\end{pmatrix} \quad \text{--- (5)}$$

[0076]

[0077] 단계 S36에서, 관련 매트릭스 $\left[\overleftrightarrow{f}\Big|^{m}\right]$ 와 사용자-정의된 양의 정수인 모듈러스 ℓ 에 기초하여, 인버스 p-어레이 생성 모듈(15)은 모듈러스 ℓ 에 대하여 인버스 p-어레이 $\overleftrightarrow{F}_{\ell}\Big|^{m}$ 를 생성한다. 인버스 p-어레이 생성 모듈(15)은 개인키 생성 모듈(17) 및 공개키 생성 모듈(18)에 상기 인버스 p-어레이 $\overleftrightarrow{F}_{\ell}\Big|^{m}$ 를 출력한다. 인버스 p-어레이 $\overleftrightarrow{F}_{\ell}\Big|^{m}$ 는 다음과 같이 정의된다 :

$$\overleftrightarrow{F}_{\ell}\Big|^{m}:=\left(L_{\ell}[1,0,\cdots,0]\left[\overleftrightarrow{f}\Big|^{m}\right]^{*}\right)\ (\mathrm{mod}\ \ell)$$

[0078]

[0079] 여기서, L_{ℓ} 는 모듈러스 ℓ 에 대한 관련 매트릭스 $\left[\overleftrightarrow{f}\Big|^{m}\right]$ 의 행렬식(determinant)의 인버스 모듈러스를 나타내며, $L_{\ell}:=\left(\det\left[\overleftrightarrow{f}\Big|^{m}\right]\right)^{-1}\ (\mathrm{mod}\ \ell)$ 로 정의되고, 그리고 $\left[\overleftrightarrow{f}\Big|^{m}\right]^{*}$ 는 관련 매트릭스 $\left[\overleftrightarrow{f}\Big|^{m}\right]$의 수반 행렬(adjoint matrix)을 나타낸다.

[0080] 단계 S37에서, 기준 프라임 결정 모듈(16)은 제1 기준 프라임(p_1)을 임의로 선택하고, 그리고 상기 제1 기준 프라임(p_1), b로 표시되는 p-어레이 $\overleftrightarrow{f}\Big|^{m}$ 의 m 개의 성분들 중 가장 큰 것, 제1 기준 양의 정수($\tilde{a}$) 그리고 파라미터(m), 제2 기준 양의 정수($\tilde{b}$) 및 제3 기준 양의 정수(r)로 구성된 제2 파라미터 세트(S)와 관련된 미리 결정된 기준에 기초하여 제2 기준 프라임(p_2)을 결정한다. 상기 미리 결정된 기준은 $p_2>\max(p_1m\tilde{a}\tilde{b},mbr)$ 을 포함한다. 상기 기준 프라임 결정 모듈(16)은 개인키 생성 모듈(17)에 제1 기준 프라임(p_1)을 출력하며, 공개키 생성 모듈(18)에 제1 기준 프라임(p_1) 및 제2 기준 프라임(p_2)을 출력하며, 그리고 저장 모듈(19)에 제1 기준 프라임(p_1) 및 제2 기준 프라임(p_2)을 저장한다. 방정식 (4)의 예에 따르면, $b=\max\left(\overleftrightarrow{f}\Big|^{5}\right)=81$ 이 획득된다. 또한, S = (m, $\tilde{b}$, r) = (5, 120, 120) 및 $\tilde{a}$ = 120의 예시적인 조건 하에서, 기준 프라임 결정 모듈(16)이 p_1 = 251을 선택할 때, 미리 결정된 기준은 :

$$p_2>p_1m\tilde{a}\tilde{b}=251\times5\times120\times120=18072000,$$
$$p_2>mbr=5\times81\times120=48600,$$

[0081]

[0082] 을 포함할 것이며, 예를 들어, p_2 = 18072001인 것으로 결정될 수 있지만, 본 개시서는 미리 결정된 기준이 만족되는 한 이와 관련하여 제한되지 않는다.

[0083] 단계 S36 및 S37에 후속하는 단계 S38에서, 개인키 생성 모듈(17)은 제1 기준 인버스 p-어레이 $\overleftrightarrow{F}_{p_1}\Big|^m$ 를 획득하기 위해 제1 기준 프라임(p_1)이 인버스 p-어레이($\overleftrightarrow{F}_{\ell}\Big|^m$)의 모듈러스(modulus)($\ell$)로서 기능하게 한다. 제1 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_1}\Big|^m$)는 $K_{\text{private}} = \left(\overleftrightarrow{f}\Big|^m, p_1, \tilde{a}\right)$ 로 정의되는 개인키(K_{private}) 역할을 한다(즉, K_{private} = $\overleftrightarrow{F}_{p_1}\Big|^m$). 개인키 생성 모듈(17)은 저장 모듈(19)에 제1 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_1}\Big|^m$)를 저장한다. p_1 = 251 인 방정식(5)의 이전 예에 따르면, $\det\left(\left[\overleftrightarrow{f}\Big|^5\right]\right) \equiv 68 \pmod{251}$ 이기 때문에, L_{251} =$(68)^{-1}$(mod 251)=48이 획득될 수 있으며, 그리고 개인키(K_{private})는 다음과 같이 획득될 것이다 :

[0084] K_{private} = $\overleftrightarrow{F}_{251}\Big|^5$ = $\left(\overleftrightarrow{f}\Big|^5, 251, 120\right)$

[0085] = $\left(L_{251}[1,0,\ldots,0]\ \left[\overleftrightarrow{f}\Big|^5\right]^*\right) \pmod{251}$

[0086] = [164, 128, 92, 223, 74]

[0087] ---(6)

[0088] 단계 S36 및 S37에 후속하는 단계 S39에서, 공개키 생성 모듈(18)은 제2 기준 인버스 p-어레이 $\overleftrightarrow{F}_{p_2}\Big|^m$ 를 획득하기 위해 제2 기준 프라임(p_2)이 인버스 p-어레이($\overleftrightarrow{F}_{\ell}\Big|^m$)의 모듈러스(modulus)($\ell$)로서 기능하게 하며, 그리고 저장 모듈(19)에 제2 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_2}\Big|^m$)를 저장한다. m = 5, p = 3, p_2 = 18072001 및 $\det\left(\left[\overleftrightarrow{f}\Big|^5\right]\right) \equiv 16142697 \pmod{18072001}$ $\tilde{a}$ = 120의 이전 예에 따라, 및 $L_{18072001} = 16142697^{-1} \equiv 17712763 \pmod{18072001}$ 이기 때문에, 다음이 획득된다 :

[0089] $\overleftrightarrow{F}_{18072001}\Big|^5$ = $\left(\overleftrightarrow{f}\Big|^5, 18072001, 120\right)$ = $L_{18072001}[1, 0, \ldots, 0]\ \left[\overleftrightarrow{f}\Big|^5\right]^*\Big)$ = $[1287507, 11026277, 11798464, 16030112, 7407741]$ --- (7)

[0090] 단계 S40에서, 공개키 생성 모듈(18)은 제2 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_2}\big|^m$), 제1 기준 프라임(p_1), 제2 기준 프라임(p_2) 및 키-생성 랜덤화 어레이($\overleftrightarrow{R}\big|^m_{(\tilde{a})}$)에 기초하여 키-생성 랜덤화 어레이 $\overleftrightarrow{R}\big|^m_{(\tilde{a})}$와 관련하여 공개키($K_{\text{public}}$)를 생성한다. 키-생성 랜덤화 어레이($\overleftrightarrow{R}\big|^m_{(\tilde{a})}$)는 0과 제1 기준 양의 정수($\tilde{a}$) 사이의(0과 $\tilde{a}$ 포함) m 개의 숫자 성분을 갖는다(예를 들어, 0과 $\tilde{a}$ 사이의 m개의 임의의 정수). 공개키(K_{public})는 개인키(K_{private})와 쌍을 이룬다. 이 실시예에서, 공개키(K_{public})는 m 개의 숫자 성분들을 포함하고 $K_{\text{public}} = \left(\overleftrightarrow{K}_{\text{public}}\big|^m, p_2\right)$ 라고도 표시되는 어레이($\overleftrightarrow{K}_{\text{public}}\big|^m$)이며, $\overleftrightarrow{K}_{\text{public}}\big|^m := \text{Rand}\left(\overleftrightarrow{F}_{p_2}\big|^m, p_1, \tilde{a}\right) \pmod{p_2}$ 를 나타낸다. $\text{Rand}\left(\overleftrightarrow{F}_{p_2}\big|^m, p_1, \tilde{a}\right)$ 는 키 생성 랜덤화 어레이($\overleftrightarrow{R}\big|^m_{(\tilde{a})}$)에 대한 제2 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_2}\big|^m$)의 키 생성 랜덤화 함수이며, 그리고 $\text{Rand}\left(\overleftrightarrow{F}_{p_2}\big|^m, p_1, \tilde{a}\right) = p_1\left(\overleftrightarrow{F}_{p_2}\big|^m \circledast \overleftrightarrow{R}\big|^m_{(\tilde{a})}\right)$ 로 정의되며, 여기서 $\circledast$ 는 컨볼루션 곱셈 연산자를 나타낸다. 방정식 (7)에서 $m=5$, $p=3$, p_1 =251, p_2=18072001, $\tilde{a}$=120 및 $\overleftrightarrow{F}_{18072001}\big|^5$ 인 이전 예에 따르면, $\overleftrightarrow{R}\big|^5_{(120)} = [98, 83, 38, 114, 4]$ 라고 가정되는 예시적인 키-생성 랜덤화 어레이가 사용되는 경우, 공개키(K_{public})는 다음과 같이 방정식(6)의 개인키(K_{private})를 사용하여 획득된다 :

[0091]
$$\begin{aligned}\overleftrightarrow{K}_{\text{public}}\big|^5 &= \text{Rand}\left(\overleftrightarrow{F}_{18072001}\big|^5, 251, 120\right) \pmod{18072001}\\ &= 251\left(\overleftrightarrow{F}_{18072001}\big|^5, 251, 120 \circledast \overleftrightarrow{R}\big|^5_{(120)}\right) \pmod{18072001}\\ &= [13126654, 5728821, 15683333, 5171087, 12284834].\end{aligned} \quad \text{--- (8)}$$

[0092] 그러나, 방정식(6)에서 개인키(K_{private})를 사용하여 획득되는 공개키(K_{public})는 이에 한정되지는 않는다. $\overleftrightarrow{R^*}\big|^5_{(120)} = [58, 53, 77, 85, 90]$ 라고 가정되는 다른 예시적인 키 생성 랜덤화 어레이가 공개키 생성 모듈(18)에 의해 사용된다면, 다른 공개키(K^*_{public})는 다음과 같이 방정식(6)의 개인키(K_{private})를 사용하여 획득된다 :

[0093]
$$\overleftrightarrow{K^*}_{\text{public}}\big|^5 = [17687579, 12818350, 12426167, 13811533, 10953056] \quad \text{--(9)}$$

[0094] 즉, 공개키 생성 모듈(18)은 상이한 키-생성 랜덤화 어레이를 사용함으로써 동일한 개인키(K_{private})와 쌍을 이루는 상이한 공개키들을 생성할 수 있으며, 공개키를 리프레시할 때 키 서버(1)를 선호(favoring)한다.

[0095] 비대칭 키 생성 절차가 완료되면, 키 서버(1)는 키 서버(1)와 송신단(2) 사이의 통신 채널(도 1의 C2)을 통해 송신단(2)에 공개키(K_{public})(공개키(K_{public})가 생성된 경우), 제2 기준 프라임(p_2) 및 제2 기준 양의 정수($\tilde{b}$)를 송신하며, 그리고 키 서버(1)와 수신단(3) 사이의 통신 채널(도 1의 C3)을 통해 수신단(3)에 개인키(K_{private}),

p-어레이($\overleftrightarrow{f}\big|^{m}$), 제1 기준 프라임(p_1) 및 제2 기준 프라임(p_2)을 송신한다.

[0096] 도 5를 참조하면, 송신단(2)의 프로세서(22)는 키 서버(1)로부터 수신된 공개키(K_{public}), 제2 기준 프라임(p_2) 및 제2 기준 양의 정수($\tilde{b}$)를 저장 유닛(21)에 저장한다. 이 실시예에서, 프로세서(22)는 텍스트 변환 모듈(221), 암호화 랜덤화 함수 생성 모듈(encryption randomization function generation module)(222), 그리고 상기 텍스트 변환 모듈(221) 및 상기 암호화 랜덤화 함수 생성 모듈(222)에 연결된 암호문 생성 모듈(223)을 갖도록 구성된다.

[0097] 또한, 도 7을 참조하면, 송신단(2)에 의해 수행되는 암호화 절차가 도시되어 있다. 단계 S71에서, 텍스트 변환 모듈(221)은 ASCII 코드와 같은 미리 결정된 문자-숫자 기술을 사용하여, 암호화될 m 개의 문자들을 갖는 평문을 m 개의 숫자 성분을 갖는 데이터 어레이($\overleftrightarrow{M}\big|^{m}$)로 변환한다. 구체적으로, 데이터 어레이($\overleftrightarrow{M}\big|^{m}$)의 m 개의 숫자 성분들 각각은 0과 제1 기준 양의 정수($\tilde{a}$) 사이이며, 그리고 평문의 m 개의 문자들 중 대응하는 하나를 나타낸다. 예를 들어, 평문 "Hello"(즉, m = 5)의 경우, ASCII 코드에 기초하여 획득되는 데이터 어레이($\overleftrightarrow{M}\big|^{5}$)는 :

$$\overleftrightarrow{M}\big|^{5} = [72, 101, 108, 108, 111]$$

[0098] ---- (1)

[0099] 일 것이지만, 본 개시서는 임의의 특정 문자-숫자 기술로 제한되지 않는다.

[0100] 단계 S72에서, 암호화 랜덤화 함수 생성 모듈(222)은 공개키(K_{public}) 및 암호화 랜덤화 어레이($\overleftrightarrow{R}\big|^{m}_{(\tilde{b})}$)에 기초하여 암호화 랜덤화 함수($\overleftrightarrow{R}\big|^{m}$)를 생성한다. 암호화 랜덤화 어레이($\overleftrightarrow{R}\big|^{m}_{(\tilde{b})}$)는 0과 제2 기준 양의 정수($\tilde{b}$) 사이의 m 개의 숫자 성분들을 갖는다. 암호화 랜덤화 함수($\overleftrightarrow{R}\big|^{m}$)는 $\overleftrightarrow{R}\big|^{m} := \mathbf{Rand}\left(\overleftrightarrow{K}_{\mathbf{public}}\big|^{m}, 1, \tilde{b}\right)$ 로서 정의된다. 제2 파라미터 세트 S=(m, $\tilde{b}$, r)=(5, 120, 120)이고 공개키 K_{public} = $\overleftrightarrow{K}_{\mathbf{public}}\big|^{5}$ = $[13126654, 5728821, 15683333, 5171087, 12284834]$ 인 이전 예에 따라, 암호화 랜덤화 어레이가 $\overleftrightarrow{R}\big|^{5}_{(\tilde{b})} = \overleftrightarrow{R_{encrypt_1}}\big|^{5}_{(120)} = [52, 45, 91, 95, 22]$ 로 예시되는 경우, 결과물인 암호화 랜덤화 함수($\overleftrightarrow{R}\big|^{5}$)는 다음과 같을 것이다 :

$$\overleftrightarrow{R}\big|^{5} = \mathbf{Rand}\left(\overleftrightarrow{K}_{\mathbf{public}}\big|^{5}, 1, 120\right)$$
$$= [3321923152, 2842804607, 3548678919, 3013267698, 3131717969]$$

[0101]

[0102] ---------- (11)

[0103] 암호화 랜덤화 어레이가 $\overleftrightarrow{R}\big|^{5}_{(\tilde{b})} = \overleftrightarrow{R_{encrypt_2}}\big|^{5}_{(120)} = [17, 23, 45, 90, 2]$ 로 예시되는 다른 경우, 결과물인 암호화 랜덤화 함수 $\overleftrightarrow{R_1}\big|^{5}$ 는 다음과 같을 것이다 :

$$\overleftrightarrow{R_1}\Big|^5 = \mathrm{Rand}\left(\overleftrightarrow{K}_{\mathrm{public}}\Big|^5, 1, 120\right)$$
$$= [2161360827, 1448885025, 2105056208, 1912390611, 1575374362],$$

[0104]

[0105] --- (12)

[0106] 즉, 암호화 랜덤화 함수 생성 모듈(222)은 상이한 암호화 랜덤화 어레이들을 사용하여 상이한 암호화 랜덤화 함수들을 생성할 수 있다.

[0107] 단계 S71 및 S72에 후속하는 단계 S73에서, 암호문 생성 모듈(223)은 (텍스트 변환 모듈(221)로부터 수신된) 데이터 어레이($\overleftrightarrow{M}\Big|^m$)와 (암호화 랜덤화 함수 생성 모듈(222)로부터 수신된) 암호화 랜덤화 함수($\overleftrightarrow{R}\Big|^m$)의 합에 대해 제2 기준 프라임($p_2$)으로 모듈로 연산을 수행함으로써 암호화 랜덤화 함수와 관련하여 암호문($\overleftrightarrow{Cipher}\Big|^m$)을 획득한다. 암호문($\overleftrightarrow{Cipher}\Big|^m$)은 m 개의 암호화된 숫자 성분들을 가지며, 그리고 $\overleftrightarrow{Cipher}\Big|^m := \left(\overleftrightarrow{M}\Big|^m + \overleftrightarrow{R}\Big|^m\right) \pmod{p_2}$ 로 표현된다. 데이터 어레이($\overleftrightarrow{M}\Big|^5$) 및 암호화 랜덤화 함수($\overleftrightarrow{R_1}\Big|^5$)가 방정식 (10) 및 방정식 (11)으로 표시되는 예에서, 결과물인 암호문($\overleftrightarrow{Cipher}\Big|^5$)은 다음과 같을 것이다 :

$$\overleftrightarrow{Cipher}\Big|^5 = \left(\overleftrightarrow{M}\Big|^5 + \overleftrightarrow{R}\Big|^5\right) \pmod{18072001}$$

[0108]

$$= [14747041, 5500551, 6566831, 13315640, 5261907]$$

[0109] ---- (13)

[0110] 데이터 어레이($\overleftrightarrow{M}\Big|^5$) 및 암호화 랜덤화 함수($\overleftrightarrow{R_1}\Big|^5$)가 방정식 (10) 및 방정식 (12)에 도시된 예에서, 결과적인 암호문($\overleftrightarrow{Cipher}\Big|^5$)은 다음과 같을 것이다 :

$$\overleftrightarrow{Cipher_1}\Big|^5 = \left(\overleftrightarrow{M}\Big|^5 + \overleftrightarrow{R_1}\Big|^5\right) \pmod{18072001}$$

[0111]

$$= [10792780, 3125046, 8704200, 14830614, 3110386]$$

[0112] ---- (14)

[0113] 암호화 절차 완료 후에, 송신단(2)은 송신단(2)과 수신단(3) 사이의 통신 채널(도 1의 C1)을 통해 수신단(3)에 암호문($\overleftrightarrow{Cipher}\Big|^m$)을 송신한다. 통신 채널(C1)은 본 개시서에 따라 암호화 통신 시스템(100)에 의해 암호화되지 않은 채널일 수 있다.

[0114] 도 1 및 도 6을 참조하면, 송신단(3)의 프로세서(32)는 키 서버(1)로부터 수신되는 개인키(K_{private}), p-어레이($\overleftrightarrow{f}\Big|^m$), 제1 기준 프라임($p_1$) 및 제2 기준 프라임($p_2$)을 저장 유닛(31)에 저장한다. 이 실시예에서, 프로세서(32)는 제1 컨볼루션 모듈(321), 그리고 상기 제1 컨볼루션 모듈(321)에 연결된 제2 컨볼루션 모듈(322)을 갖도록 구성된다.

[0115] 도 8을 더 참조하면, 수신단(3)에 의해 수신되는 암호문($\overleftrightarrow{Cipher}\Big|^m$)에 수행될 해독 절차가 도시된다. 단계 S81에서, 제1 컨볼루션 모듈(321)은 암호문($\overleftrightarrow{Cipher}\Big|^m$)과 p-어레이($\overleftrightarrow{f}\Big|^m$)의 제1 컨볼루션 결과(즉,

$\left(\overleftarrow{Cipher}\right|^m \circledast \overleftrightarrow{f}\left|^m\right)$)를 계산하며, 상기 제1 컨볼루션 결과에 대해 제2 기준 프라임(p_2)으로 모듈로 연산을 수행하여 제1 모듈로 연산 결과(즉, $\left(\overleftarrow{Cipher}\right|^m \circledast \overleftrightarrow{f}\left|^m\right) \pmod{p_2}$)를 획득하며, 그리고 상기 제1 모듈로 연산 결과에 대해 제1 기준 프라임(p_1)으로 모듈로 연산을 수행하여 제2 모듈로 연산 결과($\overleftrightarrow{M_0}|^m$)를 획득한다. 제2 모듈로 연산 결과($\overleftrightarrow{M_0}|^m$)는

$$\overleftrightarrow{M_0}|^m := \left[\left(\overleftarrow{Cipher}\right|^m \circledast \overleftrightarrow{f}\left|^m\right) \pmod{p_2}\right] \pmod{p_1}$$

로 정의된다. p_1 = 251, p_2 = 18072001, p-어레이는 방정식 (4)의 $\overleftrightarrow{f}|^5$ 이며, 암호문은 방정식 (13)의 $\overleftarrow{Cipher}|^5$ 인 이전 예에 따라, 결과물인 제1 모듈로 연산 결과 및 제2 모듈로 연산 결과는 다음과 같을 것이다 :

[0116] $$\left(\overleftarrow{Cipher}\right|^5 \circledast \overleftrightarrow{f}\left|^5\right) \pmod{18072001} = [5305912, 5220083, 4408431, 6184511, 4741098]$$

[0117] $$\begin{aligned}\overleftrightarrow{M_0}|^5 &= [5305912, 5220083, 4408431, 6184511, 4741098] \pmod{251} \\ &= [23, 36, 118, 122, 210]\end{aligned}$$

--- (15)

[0118] p_1 = 251, p_2 = 18072001, p-어레이는 방정식 (4)의 $\overleftrightarrow{f}|^5$ 이며, 암호문은 방정식 (14)의 $\overleftarrow{Cipher_1}|^5$ 인 다른 예에 따라, 결과물인 제1 모듈로 연산 결과 및 제2 모듈로 연산 결과는 다음과 같을 것이다 :

[0119] $$\left(\overleftarrow{Cipher_1}\right|^5 \circledast \overleftrightarrow{f_3}\left|^5\right) \pmod{18072001} = [2642300, 3569758, 1907467, 3871797, 3041577]$$

[0120] $$\overleftrightarrow{M_{01}}\Big|^5 = [2642300, 3569758, 1907467, 3871797, 3041577] \pmod{251}$$

[0121] $$= [23, 36, 118, 122, 210]$$

--- (16)

[0122] 방정식 (15) 및 방정식 (16)으로부터, 제1 컨볼루션 모듈(321)은 상이한 암호문들 $\overleftarrow{Cipher}|^5$ 및 $\overleftarrow{Cipher_1}|^5$을 사용함으로써 동일한 제2 모듈로 연산 결과($\overleftrightarrow{M_0}|^5 = \overleftrightarrow{M_{01}}|^5 = [23, 36, 118, 122, 210]$)를 획득한다는 것에 유의한다.

[0123] 단계 S82에서, 제2 컨볼루션 모듈(322)은 제2 모듈로 연산 결과($\overleftrightarrow{M_0}|^m$) 그리고 개인키($K_{\text{private}}$) 역할을 하는 제1 기준 인버스 p-어레이($\overleftrightarrow{F_{p_1}}|^m$)의 제2 컨볼루션 결과를 계산하며, 상기 제2 컨볼루션 결과에 대해 제1 기준 프라임(p_1)으로 모듈로 연산을 수행하여 평문 어레이($\overleftrightarrow{M_1}|^m$)를 획득한다. 이 때, 평문 어레이($\overleftrightarrow{M_1}|^m$)는 m 개의 해독된 숫자 성분들을 가지며, 그리고 $\overleftrightarrow{M_1}|^m := \overleftrightarrow{M_0}|^m \circledast \overleftrightarrow{F_{p_1}}|^m \pmod{p_1}$로 정의된다. p_1

= 251인 이전 예에 따르면, 개인키($K_{private}$)는 방정식 (6)의 $\overleftrightarrow{F}_{251}\Big|^5$ 이며, 그리고 제2 모듈로 연산 결과는 방정식 (15)의 $\overleftrightarrow{M_0}\Big|^5$ 이며, 획득된 평문 어레이($\overleftrightarrow{M_1}\Big|^5$)는 다음과 같을 것이다 :

$$\begin{aligned}\overleftrightarrow{M_1}\Big|^5 &= \overleftrightarrow{M_0}\Big|^5 \circledast \overleftrightarrow{F}_{251}\Big|^5 \pmod{251}\\ &\equiv [23, 36, 118, 122, 210] \circledast [164, 128, 92, 223, 74] \pmod{251}\\ &\equiv [72, 101, 108, 108, 111] = Hello.\end{aligned}$$

[0124]

[0125] 획득된 평문 어레이($\overleftrightarrow{M_1}\Big|^5$)가 방정식 (10)의 데이터 어레이($\overleftrightarrow{M}\Big|^5$)와 동일한 것을 볼 수 있다. 따라서, 수신단(3)은 평문 어레이($\overleftrightarrow{M_1}\Big|^5$)의 해독된 숫자 성분들 모두를 문자들로 변환함으로써 평문 "Hello"를 성공적으로 획득할 수 있다.

[0126] 다시 도 1 및 도 2를 참조하면, 암호 통신 시스템(100)이 키 리프레시를 수행할 필요가 있을 때, 키 서버(1)의 공개키 생성 모듈(18)은 원래의 공개키(K_{public})를 생성하는데 사용되는 키-생성 랜덤화 어레이($\overleftrightarrow{R^*}\Big|^m_{(\tilde{a})}$)와 상이한 키-생성 랜덤화 어레이($\overleftrightarrow{R^*}\Big|^m_{(\tilde{a})}$)(예를 들어, $\overleftrightarrow{R^*}\Big|^5_{(120)}$)와 관련하여, 제2 기준 인버스 p-어레이($\overleftrightarrow{F}_{p_2}\Big|^m$), 제1 기준 프라임($p_1$), 제2 기준 프라임($p_2$) 및 키-생성 랜덤화 어레이($\overleftrightarrow{R^*}\Big|^m_{(\tilde{a})}$)에 기초하여, 개인키($K_{private}$)와 쌍을 이루는 업데이트된 공개키($K^*_{public}$)(예를 들어, 방정식 (9)의 $\overleftrightarrow{K^*}_{public}\Big|^5$)를 생성하기 위해 단계 S40(도 4 참조)을 수행하는데 사용될 수 있다. 이와 유사하게, 업데이트된 공개키(K^*_{public})는

$$K^*_{public} = \left(\overleftrightarrow{K^*}_{public}\Big|^5, 18072001\right)$$

로 표기되는

$$\overleftrightarrow{K^*}_{public}\Big|^m = \text{Rand}\left(\overleftrightarrow{F}_{p_2}\Big|^m, p_1, \tilde{a}\right) \pmod{p_2} = p_1\left(\overleftrightarrow{F}_{p_2}\Big|^m \circledast \overleftrightarrow{R^*}\Big|^m_{(\tilde{a})}\right) \pmod{p_2}$$

로 표현될 수 있다. 그 다음, 키 서버(1)는 통신 채널(C2)을 통해 송신단(2)에 업데이트된 공개키(K^*_{public})를 송신하며, 그리고 송신단(2)의 프로세서(22)는 저장부(21)에서 공개키(K_{public})를 업데이트된 공개키(K^*_{public})로 업데이트한다.

[0127] 저장 유닛(21)의 공개키를 업데이트한 후, 송신단(2)의 프로세서(22)는 업데이트된 공개키(K^*_{public}), 제2 기준 프라임(p_2) 및 암호화 랜덤화 어레이($\overleftrightarrow{R}\Big|^m_{(\tilde{b})}$)를 사용하여, 데이터 어레이($\overleftrightarrow{M}\Big|^m$)에 대해 암호화 절차를 수행할 수 있으며, 그리고 업데이트된 공개키(K^*_{public}) 및 암호화 랜덤화 어레이($\overleftrightarrow{R}\Big|^m_{(\tilde{b})}$)와 관련하여 다른 암호문($\overleftrightarrow{Cipher^*}$)을 획득할 수 있다. 암호문($\overleftrightarrow{Cipher^*}$)은 m 개의 암호화된 숫자 성분들을 가지며, 그리고 송신단(2)의 프로세서(22)에 의해 통신 채널(C1)을 통해 수신단(3)에 전송된다. m = 5, $\tilde{b}$ = 120인 이전 예에서, 데이터 어레이는 방정식(10)의 $\overleftrightarrow{M}\Big|^5$ 이며, 그리고 공개키는 방정식 (9)의 K^*_{public}이며,

$\overleftrightarrow{R}\Big|_{(\tilde{b})}^{5} = \overleftarrow{R_{encrypt_3}}\Big|_{(120)}^{5} = [33, 81, 78, 19, 14]$ 일 때, 결과물인 암호문($\overleftarrow{Cipher^*}\Big|^{5}$)은 다음과 같을 것이다 :

[0128] $$\overleftarrow{Cipher^*}\Big|^{5} = [18005199, 1895209, 12634479, 5802146, 12936752]$$

--- (17)

[0129] $\overleftrightarrow{R}\Big|_{(\tilde{b})}^{5} = \overleftarrow{R_{encrypt_4}}\Big|_{(120)}^{5} = [13, 25, 19, 92, 54]$ 인 다른 경우, 결과물인 암호문($\overleftarrow{Cipher^*}\Big|^{5}$)은 다음과 같을 것이다 :

[0130] $$\overleftarrow{Cipher_1^*}\Big|^{5} = [17286247, 11666092, 5342822, 6738991, 2816645]$$

--- (18)

[0131] 수신단(3)의 프로세서(32)가 송신단(2)으로부터 암호문($\overleftarrow{Cipher^*}$)을 수신할 때, 프로세서(32)는 개인키($K_{private}$), p-어레이($\overleftrightarrow{f}\Big|^{m}$), 제1 기준 프라임($p_1$) 및 제2 기준 프라임($p_2$)을 사용하여 암호문($\overleftarrow{Cipher^*}$)에 대해 해독 절차를 수행하며, 이로써 평문 어레이($\overleftrightarrow{M_1}\Big|^{m}$)를 획득한다. $p_1 = 251$, $p_2 = 18072001$인 이전 예에 따르면, p-어레이는 방정식(4)의 $\overleftrightarrow{f}\Big|^{5}$ 이며, 그리고 암호문은 방정식 (17)의 $\overleftarrow{Cipher^*}\Big|^{5}$이며, 결과물인 제1 모듈로 연산 결과 및 제2 모듈로 연산 결과($\overleftrightarrow{M_0^*}\Big|^{5}$)는 각각 다음과 같을 것이다 :

[0132] $$\left(\overleftarrow{Cipher^*}\Big|^{5} \circledast \overleftrightarrow{f}\Big|^{5}\right) \pmod{18072001} = [4541115, 4066487, 3590422, 3912710, 4450691]$$

[0133] $$\overleftrightarrow{M_0^*}\Big|^{5} = [4541115, 4066487, 3590422, 3912710, 4450691] \pmod{251}$$
$$= [23, 36, 118, 122, 210]$$

[0134] $p_1 = 251$, $p_2 = 18072001$, p-어레이가 방정식 (4)의 $\overleftrightarrow{f}\Big|^{5}$ 이며, 암호문이 방정식 (18)의 $\overleftarrow{Cipher_1^*}\Big|^{5}$인 다른 예에서, 결과물인 제1 모듈로 연산 결과 및 제2 모듈로 연산 결과는 각각 다음과 같을 것이다 :

[0135] $$\left(\overleftarrow{Cipher_1^*}\Big|^{5} \circledast \overleftrightarrow{f}\Big|^{5}\right) \pmod{18072001} = [3669141, 3982904, 4102462, 3585155, 3217277]$$

[0136] $$\overleftrightarrow{M_{0_1}^*}\Big|^{5} = [3669141, 3982904, 4102462, 3585155, 3217277] \pmod{251}$$
$$= [23, 36, 118, 122, 210].$$

[0137] 수신단(3)이 업데이트된 공개키(K^*_{public})를 사용하여 암호화된 상이한 암호문들(예를 들어, $\overleftarrow{Cipher^*}\Big|^{5}$ 및 $\overleftarrow{Cipher_1^*}\Big|^{5}$)을 수신하더라도, 개인키($K_{private}$)를 사용하여 동일한 제2 모듈로 연산 결과

($\overleftrightarrow{M_0^*}\Big|^5 = \overleftrightarrow{M_{0_1}^*}\Big|^5 = [23, 36, 118, 122, 210]$)가 획득될 수 있으며, 이에 따라 동일한 평문이 획득될 수 있다는 것이 유의되어야 한다.

[0138] 따라서, 상기 상세한 설명으로부터 다음과 같이 알려져 있다 :

[0139] 1. 포스트-퀀텀 비대칭 키 생성 시스템(10)은 제1 파라미터 세트(I), 제2 파라미터 세트(S), 제1 기준 프라임(p_1) 및 제2 기준 프라임(p_2)의 상이한 조합과 협력하여 단일 산술 함수 및 클래식 스트링(classical string)만을 사용함으로써 다수의 개인키들을 생성하기 위해 비대칭 키 생성 절차를 수행할 수 있다;

[0140] 2. 특정 개인키에 대해, 포스트-퀀텀 비대칭 키 생성 시스템(10)은 빠르고 개인키를 재계산할 필요가 없는 소프트 키 리셋 알고리즘을 사용하여 개인키와 각각 쌍을 이루는 다수의 공개키들을 생성할 수 있으며, 이에 따라 키 서버(1)는 키 리프레시를 더 쉽게 수행할 수 있다;

[0141] 3. p-어레이를 생성하는 독특한(unique) 방법이 존재하지 않는다. 패딩을 0으로 만들거나 p-어레이의 형성에 임의성을 추가하여 p-벡터에 임의성을 추가할 수 있다;

[0142] 4. 무작위 대입 공격(brute force attack)의 어려움을 높이기 위해 더 큰 파라미터 m을 선택하여 키 공간이 증가될 수 있다. 이 실시예에서, m = 5 그리고 p_1= 251의 선택은 설명의 편의를 위한 것일 뿐이다. m = 16이거나 심지어 m = 64인 경우, 가능한 키 공간이 너무 커져, 무차별 대입 공격이 성공하는데 시간이 오래 걸릴 것이다. 메시지 공간과 키 공간의 크기는 수많은 가능성을 포함할 것이며, 이는 무차별 대입 공격이 작동하지 않게 할 것이다.

[0143] 표 1은 옥타-코어 프로세서 및 32GB RAM(random access memory)의 하드웨어 사양 하에서 암호화 통신 시스템(100)을 사용하여 상이한 길이의 메시지들에 대한 암호화 및 복호화에 필요한 시간의 실험 결과를 나열한다.

표 1

[0144]

메시지 길이 (bytes)	암호화 시간 (ms)	해독 시간 (ms)
4	0.000193	0.001184
8	0.000225	0.001224
16	0.000279	0.000759
32	0.000399	0.001048
64	0.000687	0.001526
128	0.000886	0.002171
196	0.000997	0.002934

[0146] 표 1의 데이터에 기초하여, 본 개시서의 암호화 통신 시스템(100)의 사용은 메시지 길이에 상관 없이 종래의 AES 및 RSA 프로토콜에 비해 암호화 및 복호화에 필요한 시간을 수백배만큼 감소시킬 수 있다는 것이 알려져 있다. 분명히, 본 개시서의 암호화 통신 시스템(100)은 암호화 및 해독화의 속도를 상당히 증가시킬 수 있다.

[0147] 본 개시서의 실시예에서, 공개키 및 개인키는 산술 함수 또는 클래식 스트링, p-벡터, 그리고 본질적으로 벡터인 p-어레이에 기초하여 생성되어, 비교적 많은 양의 데이터에 대한 암호화 및 해독을 가능하게하며, 이로써, 암호화 및 해독화 속도가 향상되고 데이터 보안이 보장된다. 제안된 암호화 통신 시스템은 포스트-퀀텀 보안, 즉 포스트-퀀텀 컴퓨터들의 공격에 효과적으로 저항할 수 있는 보안을 보장할 수 있다. p-벡터 및 p-어레이의 특성으로 인해, 실시예의 구현을 위한 하드웨어 요건들은 저장 용량 및/또는 계산 능력면에서 상대적으로 낮다. 본 실시예는 개인키의 사용에 영향을 미치지 않으면서 공개키의 리프레시를 허용하여, 동일한 네트워크 내의 모든 사용자들에 대해 분산된 키 리프레시를 가능하게 한다. 또한, 개인키를 생성하는데 사용되는 산술 함수(f)가 무한한 양의 데이터를 생성할 수 있는 함수이기 때문에, 하나의 단일 함수만으로도 다수의 상이한 공개키들이 생성될 수 있다.

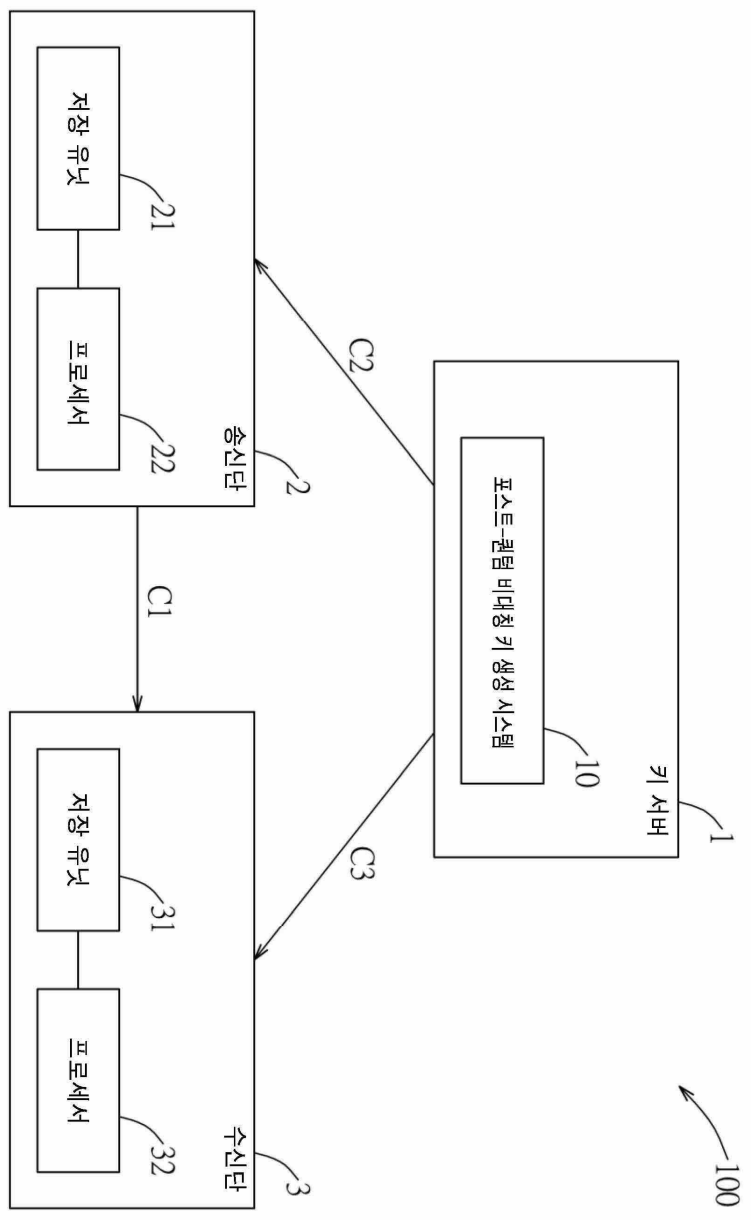
[0148] 상기 설명에서, 설명의 목적으로, 실시예(들)의 철저한 이해를 제공하기 위해 다수의 특정 세부사항들이 설명되었다. 그러나, 하나 이상의 다른 실시예들이 이들 특정 세부사항들 중 일부 없이 실시될 수 있다는 것이 당업자

에게 명백할 것이다. 또한, 본 명세서 전체에서 “일 실시예”, “실시예”, 서수를 나타내는 실시예 등을 언급한다는 것은 특정 특징, 구조, 또는 특성이 본 개시서의 실시에 포함될 수 있음을 의미한다는 것을 이해해야 한다. 상세한 설명에서, 본 개시서를 간소화하고 다양한 발명의 측면들의 이해를 돕기 위해 다양한 특징들은 하나의 실시예, 도면, 또는 그것의 설명에서 때때로 함께 그룹화된다는 것, 그리고 본 개시서의 실시에서 적절한 경우 하나의 실시예로부터의 하나 이상의 특징들 또는 특정 세부사항들은 다른 실시예의 하나 이상의 특징들 또는 특정 세부사항들과 함께 실시될 수 있다는 것 또한 이해되어야 한다.

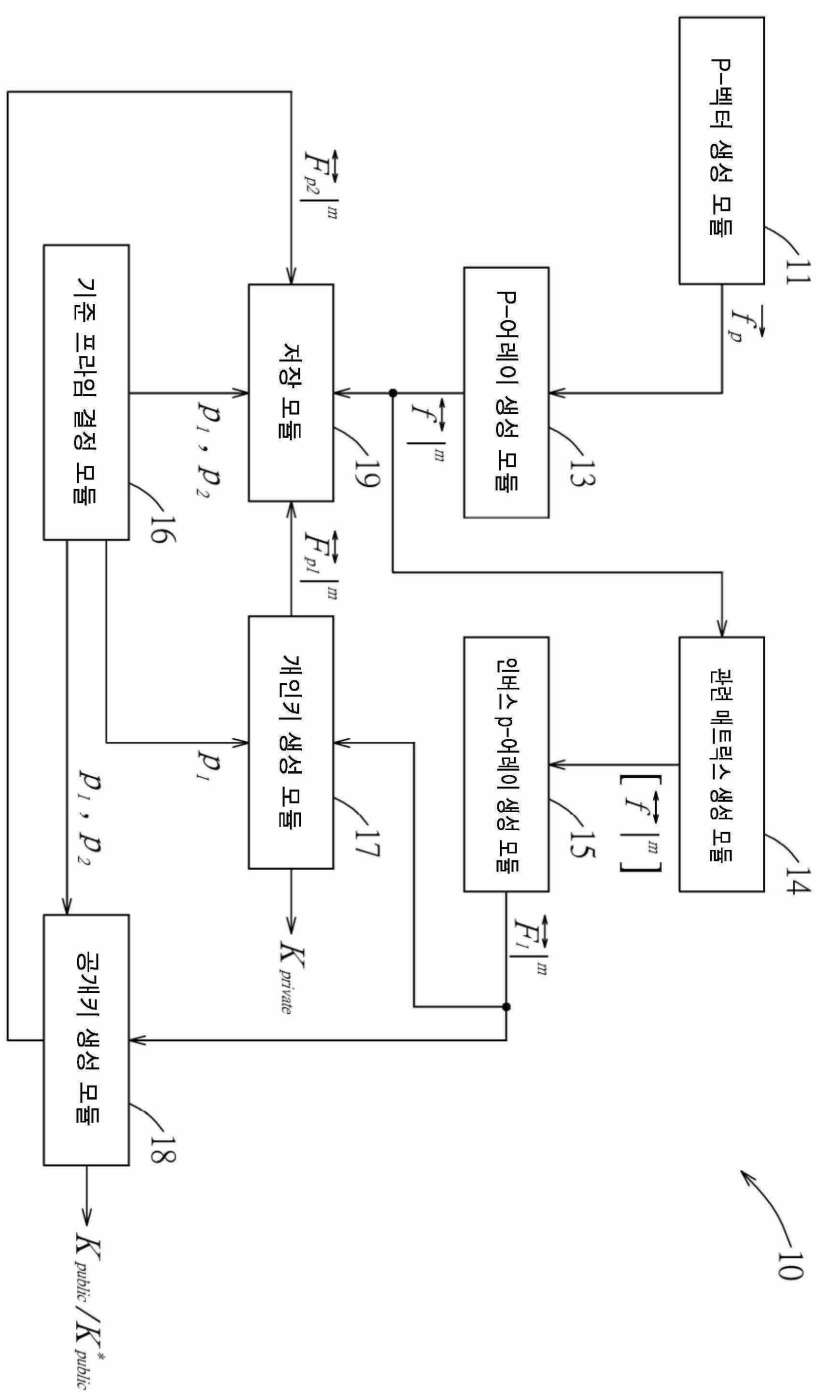
[0149] 본 개시서는 예시적인 실시예(들)로 간주되는 것과 관련하여 설명되었지만, 본 개시서는 개시된 실시예(들)로 제한되지 않으며, 모든 그러한 수정들 및 등가의 구성들을 포함하도록 가장 넓은 해석의 사상 및 범위 내에 포함되는 다양한 구성들을 포함하도록 의도된다는 것이 이해되어야 한다.

도면

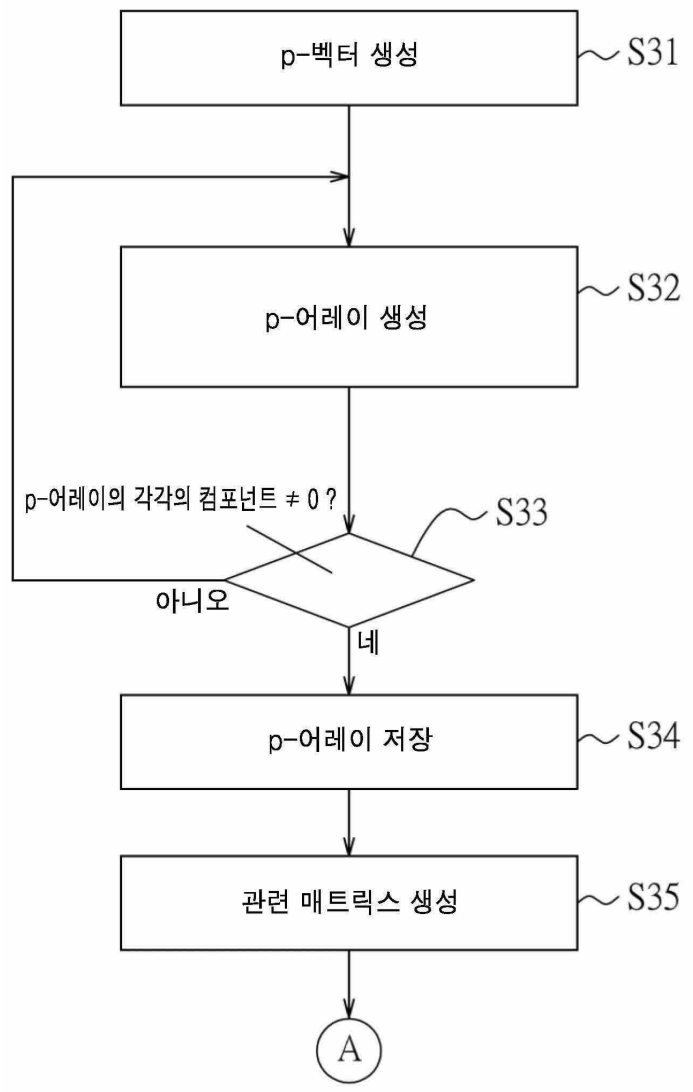
도면1


저장 유닛
21
프로세서
22
송신단
2
C2
C1
C3
포스트-퀀텀 비대칭 키 생성 시스템
10
키 서버
1
저장 유닛
31
프로세서
32
수신단
3
100

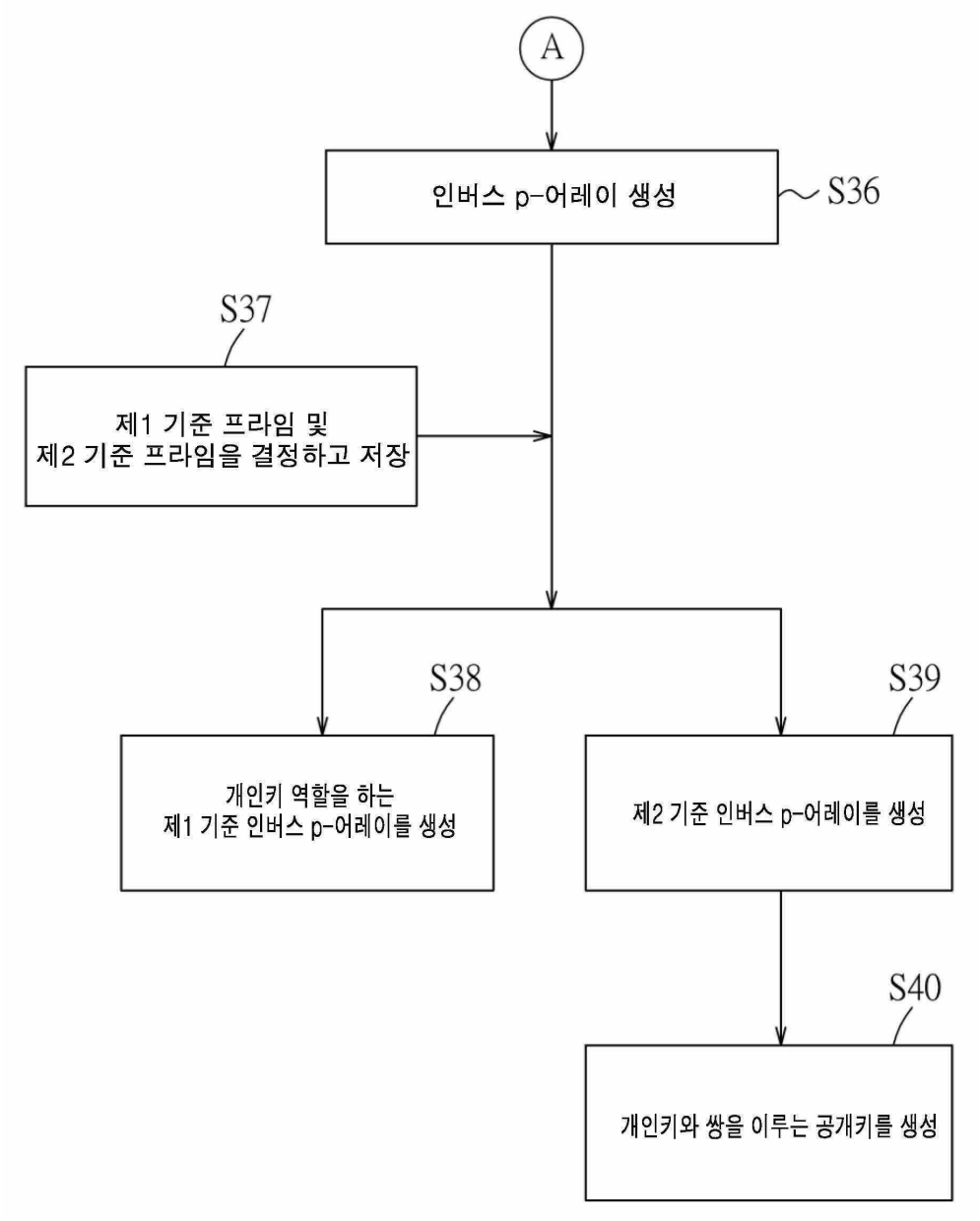
도면2


P-벡터 생성 모듈
11
P-어레이 생성 모듈
13
관련 메트릭스 생성 모듈
14
인버스 P-어레이 생성 모듈
15
기준 프라임 결정 모듈
16
개인키 생성 모듈
17
공개키 생성 모듈
18
저장 모듈
19
10

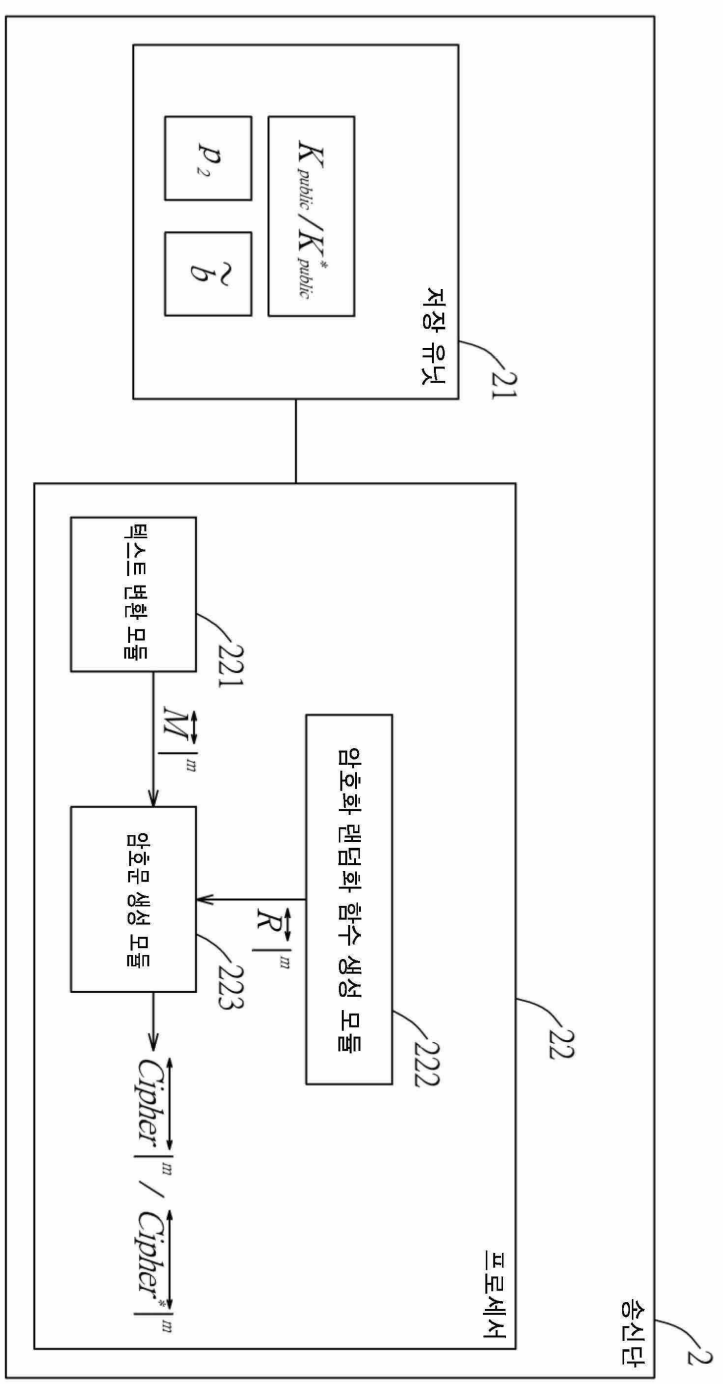
도면3


p-벡터 생성
S31
p-어레이 생성
S32
p-어레이의 각각의 컴포넌트 ≠ 0 ?
S33
아니오
네
p-어레이 저장
S34
관련 매트릭스 생성
S35
A

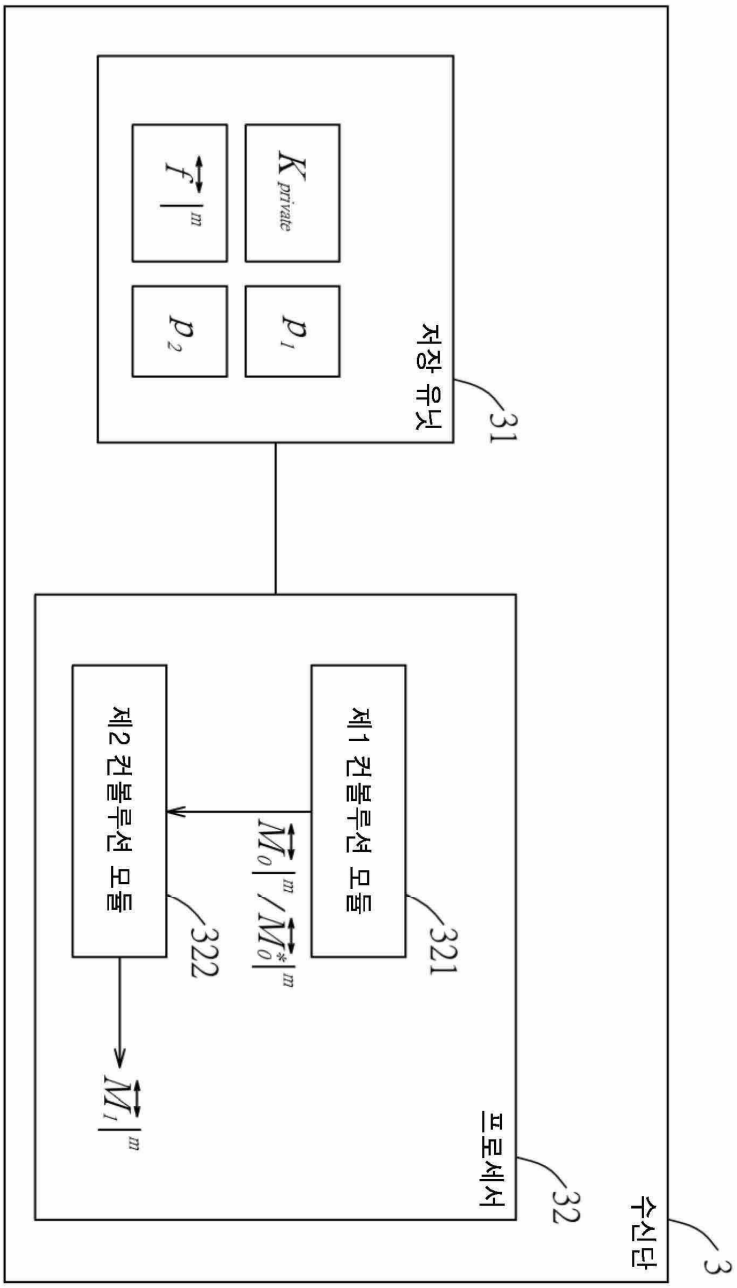
도면4


A
인버스 p-어레이 생성
S36
S37
제1 기준 프라임 및
제2 기준 프라임을 결정하고 저장
S38
개인키 역할을 하는
제1 기준 인버스 p-어레이를 생성
S39
제2 기준 인버스 p-어레이를 생성
S40
개인키와 쌍을 이루는 공개키를 생성

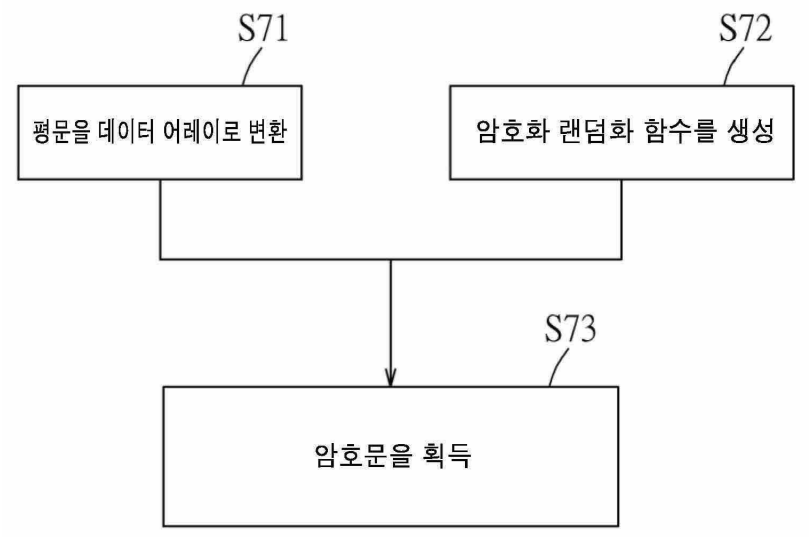
도면5


송신단
2
프로세서
22
암호화 랜덤화 함수 생성 모듈
222
암호문 생성 모듈
223
텍스트 변환 모듈
221
저장 유닛
21

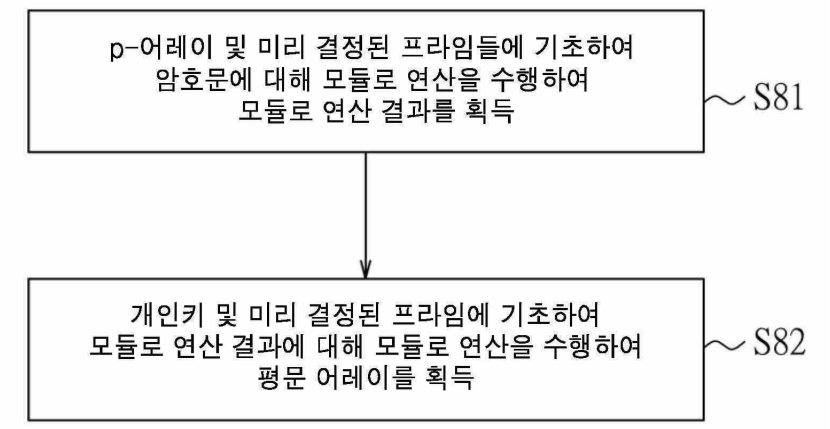
도면6


수신단
3
프로세서
32
제1 컨볼루션 모듈
321
제2 컨볼루션 모듈
322
저장 유닛
31
$K_{private}$
p_1
p_2

도면7


S71
S72
평문을 데이터 어레이로 변환
암호화 랜덤화 함수를 생성
S73
암호문을 획득

도면8


p-어레이 및 미리 결정된 프라임들에 기초하여
암호문에 대해 모듈로 연산을 수행하여
모듈로 연산 결과를 획득
S81
개인키 및 미리 결정된 프라임에 기초하여
모듈로 연산 결과에 대해 모듈로 연산을 수행하여
평문 어레이를 획득
S82