(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0042905
(43) 공개일자 2024년04월02일

(51) 국제특허분류(Int. Cl.)
H04L 9/30 (2006.01) *H04L 9/32* (2006.01)
(52) CPC특허분류
H04L 9/3093 (2013.01)
H04L 9/3236 (2013.01)
(21) 출원번호 10-2022-0121755
(22) 출원일자 2022년09월26일
심사청구일자 2022년09월26일

(71) 출원인
조선대학교산학협력단
광주광역시 동구 필문대로 309 (서석동)
(72) 발명자
김찬기
광주광역시 서구 시청로 97 중흥에스-클래스스카이31 1420호
김영식
광주광역시 서구 풍암2로 66 금호타운 201동 1005호
(74) 대리인
김효성

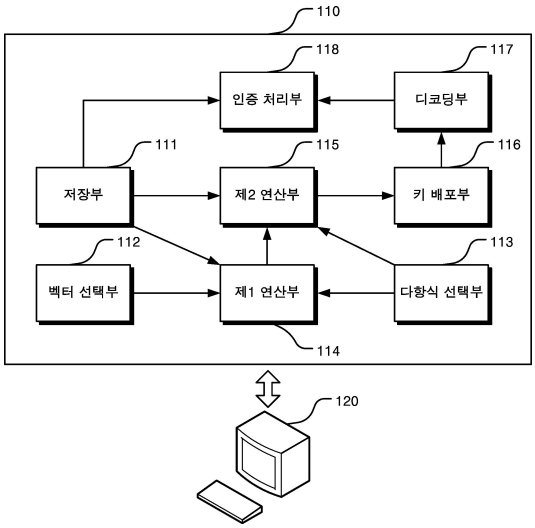
전체 청구항 수 : 총 8 항

(54) 발명의 명칭 **다항식 환을 이용한 비대칭키 기반의 보안 통신을 수행하기 위한 전자 장치 및 그 동작 방법**

(57) 요 약

본 발명은 다항식 환을 이용한 비대칭키 기반의 보안 통신을 수행하기 위한 전자 장치 및 그 동작 방법을 제시함으로써, 양자 내성을 갖는 보안 통신이 가능하도록 지원할 수 있다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/3273 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711152847
과제번호	2021-0-00400-002
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보보호핵심원천기술개발(정진기금)
연구과제명	저사양 디바이스 대상 고효율 PQC 안전성 및 성능 검증 기술 개발
기 여 율	1/1
과제수행기관명	조선대학교 산학협력단
연구기간	2022.01.01 ~ 2022.12.31

명 세 서

청구범위

청구항 1

다항식 환을 이용한 비대칭키 기반의 보안 통신을 수행하기 위한 전자 장치에 있어서,

사전 설정된 해시 함수인 Hash(·) 및, $\frac{n}{b}$ (n과 b는 정수임)차수의 사전 설정된 원시 다항식인 P가 저장되어 있는 저장부; - Hash(·)와 P는, 보안 통신을 수행하기로 사전 지정된 상대측 전자 단말에도 저장되어 있음 -

랭크 무게(rank weight) d(d는 정수임)를 갖는 $\frac{n}{b}$ -튜플 벡터들의 집합인 F로부터, 랜덤 벡터 x와 y를 랜덤하게 선택하는 벡터 선택부;

최대 차수가 $\frac{n}{b}$ 인 원시 다항식들의 집합으로 구성되는 다항식 환에서, (b-1)차수의 원시 다항식인 P_I를 랜덤하게 선택하고, 최대 차수가 n인 원시 다항식들의 집합으로 구성되는 다항식 환에서, n차수의 원시 다항식인 P_O, P_N을 랜덤하게 선택하는 다항식 선택부;

x, y, P_I를 기초로 $\frac{n}{b}$ -튜플 벡터 z($\mathbf{z} = P_I\mathbf{x}^{-1}\mathbf{y} \mod P$)를 연산하는 제1 연산부;

P_I, P_O를 기초로 공개키 다항식 P_P($P_P = P_O P_I \mod P^b$)를 연산하고, P_O, z, P_N을 기초로 공개키 벡터 h($\mathbf{h} = P_O\mathbf{z} + P_N P \mod P^b$)를 연산하는 제2 연산부; 및

P_P와 h를 공개키로 지정하고, x, y, P_I, P_O를 상기 공개키에 대응되는 개인키로 지정한 후, 상기 공개키로 지정된 P_P와 h를, 보안 통신을 수행할 상기 상대측 전자 장치로 전송하는 키 배포부

를 포함하는 전자 장치.

청구항 2

제1항에 있어서,

상기 상대측 전자 장치는

메모리 상에 Hash(·)와 P를 사전 저장하고 있고, 상기 전자 장치로부터 상기 공개키로 지정된 P_P와 h가 수신되면, 상기 메모리 상에 P_P와 h를 저장해 둔 후, 상기 전자 장치와의 상호 인증을 수행해야 하는 상황이 발생하는 경우, 최대 차수가 ($\frac{n}{b} - b$)이면서, 랭크 무게 r(r은 정수임)을 갖는 $\frac{n}{b}$ -튜플 벡터의 집합인 E로부터, 랜덤 벡터 e_1과 e_2를 랜덤하게 선택하고, e_1, e_2 및 h를 기초로 길이가 n인 벡터들인, $\mathbf{e}'_1 = [\mathbf{0}, \mathbf{e}_1]$, $\mathbf{e}'_2 = [\mathbf{0}, \mathbf{e}_2]$ 및 $\mathbf{h}' = [\mathbf{0}, \mathbf{h}]$ 를 생성한 후, e'$_1$, e'$_2$, h', P_P를 기초로 암호문 c($\mathbf{c} = P_P\mathbf{e}'_1 + \mathbf{h}'\mathbf{e}'_2 \mod P^b$)를 생성하고, Hash(·)에 E를 입력으로 인가하여 해시 값

K($K = Hash(E)$)를 연산한 후, 상기 전자 장치로 c와 K를 전송하는 것을 특징으로 하는 전자 장치.

청구항 3

제2항에 있어서,

상기 상대측 전자 장치로부터 c와 K가 수신되면, 상기 개인키로 지정된 x, P_I, P_0을 기초로 하기의 수학식 1의 연산을 수행하여 신드롬 벡터 $\mathbf{xc}_i''$를 생성한 후, $\mathbf{xc}_i''$에 대해 RSR(Rank Support Recovery) 디코딩을 수행하여 E를 재구축하는 디코딩부; 및

Hash(·)에, 재구축된 E를 입력으로 인가하여, 해시 값 K'($K' = Hash(E)$)을 생성한 후, K'과 K가 서로 일치하는지 비교하여, 서로 일치하는 것으로 확인되면, 상기 상대측 전자 장치에 대한 인증이 완료된 것으로 처리하는 인증 처리부

를 더 포함하는 전자 장치.

[수학식 1]

$$\mathbf{c}_i' = P_O^{-1}\mathbf{c} \mod P^b,$$

$$\mathbf{c}_i'' = P_I^{-1}\{\mathbf{c}_i' \mod P\} \mod P,$$

$$\mathbf{xc}_i'' = \mathbf{xe}_1 + \mathbf{ye}_2 \mod P$$

청구항 4

다항식 환을 이용한 비대칭키 기반의 보안 통신을 수행하기 위한 전자 장치의 동작 방법에 있어서,

사전 설정된 해시 함수인 Hash(·) 및, $\frac{n}{b}$(n과 b는 정수임)차수의 사전 설정된 원시 다항식인 P가 저장되어 있는 저장부를 유지하는 단계; - Hash(·)와 P는, 보안 통신을 수행하기로 사전 지정된 상대측 전자 단말에도 저장되어 있음 -

랭크 무게(rank weight) d(d는 정수임)를 갖는 $\frac{n}{b}$-튜플 벡터들의 집합인 F로부터, 랜덤 벡터 x와 y를 랜덤하게 선택하는 단계;

최대 차수가 $\frac{n}{b}$인 원시 다항식들의 집합으로 구성되는 다항식 환에서, (b-1)차수의 원시 다항식인 P_I를 랜덤하게 선택하고, 최대 차수가 n인 원시 다항식들의 집합으로 구성되는 다항식 환에서, n차수의 원시 다항식인 P_0, P_N을 랜덤하게 선택하는 단계;

x, y, P_I를 기초로 $\frac{n}{b}$-튜플 벡터 z($\mathbf{z} = P_I\mathbf{x}^{-1}\mathbf{y} \mod P$)를 연산하는 단계;

P_I, P_0를 기초로 공개키 다항식 P_P($P_P = P_O P_I \mod P^b$)를 연산하고, P_0, z, P_N을 기초로 공개키 벡터 h($\mathbf{h} = P_O\mathbf{z} + P_N P \mod P^b$)를 연산하는 단계; 및

P_P와 h를 공개키로 지정하고, x, y, P_I, P_0를 상기 공개키에 대응되는 개인키로 지정한 후, 상기 공개키로 지정된 P_P와 h를, 보안 통신을 수행할 상기 상대측 전자 장치로 전송하는 단계

를 포함하는 전자 장치의 동작 방법.

청구항 5

제4항에 있어서,

상기 상대측 전자 장치는

메모리 상에 Hash(·)와 P를 사전 저장하고 있고, 상기 전자 장치로부터 상기 공개키로 지정된 P_P와 h가 수신되면, 상기 메모리 상에 P_P와 h를 저장해 둔 후, 상기 전자 장치와의 상호 인증을 수행해야 하는 상황이 발생하는 경우, 최대 차수가 ($\frac{n}{b}-b$)이면서, 랭크 무게 r(r은 정수임)을 갖는 $\frac{n}{b}$-튜플 벡터의 집합인 E로부터, 랜덤 벡터 e_1과 e_2를 랜덤하게 선택하고, e_1, e_2 및 h를 기초로 길이가 n인 벡터들인, $\mathbf{e}'_1 = [\mathbf{0}, \mathbf{e}_1]$, $\mathbf{e}'_2 = [\mathbf{0}, \mathbf{e}_2]$ 및 $\mathbf{h}' = [\mathbf{0}, \mathbf{h}]$를 생성한 후, e'$_1$, e'$_2$, h', P_P를 기초로 암호문 c($\mathbf{c} = P_P\mathbf{e}'_1 + \mathbf{h}'\mathbf{e}'_2 \mod P^b$)를 생성하고, Hash(·)에 E를 입력으로 인가하여 해시 값 K($K = Hash(E)$)를 연산한 후, 상기 전자 장치로 c와 K를 전송하는 것을 특징으로 하는 전자 장치의 동작 방법.

청구항 6

제5항에 있어서,

상기 상대측 전자 장치로부터 c와 K가 수신되면, 상기 개인키로 지정된 x, P_I, P_0을 기초로 하기의 수학식 1의 연산을 수행하여 신드롬 벡터 $\mathbf{xc}''_i$를 생성한 후, $\mathbf{xc}''_i$에 대해 RSR(Rank Support Recovery) 디코딩을 수행하여 E를 재구축하는 단계; 및

Hash(·)에, 재구축된 E를 입력으로 인가하여, 해시 값 K'($K' = Hash(E)$)을 생성한 후, K'과 K가 서로 일치하는지 비교하여, 서로 일치하는 것으로 확인되면, 상기 상대측 전자 장치에 대한 인증이 완료된 것으로 처리하는 단계

를 더 포함하는 전자 장치의 동작 방법.

[수학식 1]

$$\mathbf{c}'_i = P_O^{-1}\mathbf{c} \mod P^b,$$

$$\mathbf{c}''_i = P_I^{-1}\{\mathbf{c}'_i \mod P\} \mod P,$$

$$\mathbf{xc}''_i = \mathbf{xe}_1 + \mathbf{ye}_2 \mod P$$

청구항 7

제4항 내지 제6항 중 어느 한 항의 방법을 컴퓨터와의 결합을 통해 실행시키기 위한 컴퓨터 프로그램을 기록한 컴퓨터 판독 가능 기록 매체.

청구항 8

제4항 내지 제6항 중 어느 한 항의 방법을 컴퓨터와의 결합을 통해 실행시키기 위한 저장매체에 저장된 컴퓨터 프로그램.

발명의 설명

기 술 분 야

[0001] 본 발명은 다항식 환을 이용한 비대칭키 기반의 보안 통신을 수행하기 위한 전자 장치 및 그 동작 방법에 대한 것이다.

배 경 기 술

[0002] 최근, 컴퓨터 시스템의 성능이 고도화됨에 따라, 보다 강화된 암호화 시스템에 대한 도입이 필요한 실정이다.

[0003] 특히, 양자 컴퓨터의 도입으로 인해서, 양자 컴퓨터를 통한 공격에 방어하기 위한 양자 내성 암호화 기술에 대한 관심이 증가하고 있다.

[0004] 이러한 양자 내성 암호화 기술 중 부호 기반 암호화 기술의 도입이 논의되고 있는데, 부호 기반 암호화 기술은 에러 정정에 사용하는 블록 부호를 활용하여 암호화를 수행하는 기술로서, 데이터 상에 소정의 에러 벡터를 임의로 삽입하여 데이터를 암호화하고, 에러 정정을 위한 디코딩을 통해 에러 벡터를 검출하는 방식으로 복호화를 수행하는 기술이라고 볼 수 있다.

[0005] 이러한 부호 기반 암호화 기술에서는 양자 컴퓨터를 통한 패턴 공격에 내성을 갖추기 위해서, 데이터 상에 랜덤한 에러 정보가 암호화 정보로서 삽입된다는 점에서, 소정의 부호화된 데이터로부터 에러를 검출하는 디코딩 기술에 대한 중요성이 크다고 볼 수 있다.

[0006] 이와 관련해서, 최근에는 부호화된 코드로부터 에러를 검출하기 위한 디코딩 기술로서, RSR(Rank Support Recovery)이 제안되었다. RSR은 LRPC(Low-Rank Parity-Check) 부호에 대한 신드롬(Syndrome)으로부터 랭크 무게 r을 갖는 에러 벡터들의 벡터 공간 E를 재구축할 수 있는 알고리즘이다. LRPC 부호를 이용한 부호 기반 암호화 기술은 랭크 메트릭(rank metric)에 기반한 암호화 시스템이기 때문에 작은 키 사이즈를 가지면서도 높은 보안성을 가지는 특징이 있다.

선행기술문헌

비특허문헌

[0007] (비특허문헌 0001) N. Aragon, P. gaborit, A. Hauteville, O. Ruatta, and G. Zemor, "Low rank parity check codes: New decoding algorithms and applications to cryptography," IEEE Trans. on Inf. Theo., vol. 65, no. 12, pp. 7697-7717(2019년 12월 공개)

발명의 내용

해결하려는 과제

[0008] 본 발명은 다항식 환을 이용한 비대칭키 기반의 보안 통신을 수행하기 위한 전자 장치 및 그 동작 방법을 제시함으로써, 양자 내성을 갖는 보안 통신이 가능하도록 지원하고자 한다.

과제의 해결 수단

[0009] 본 발명의 일실시예에 따른 다항식 환을 이용한 비대칭키 기반의 보안 통신을 수행하기 위한 전자 장치는 사전 설정된 해시 함수인 Hash(·) 및, $\frac{n}{b}$ (n과 b는 정수임)차수의 사전 설정된 원시 다항식인 P가 저장되어 있는 저장부 - Hash(·)와 P는, 보안 통신을 수행하기로 사전 지정된 상대측 전자 단말에도 저장되어 있음 - , 랭크 무

게(rank weight) d(d는 정수임)를 갖는 $\frac{n}{b}$-튜플 벡터들의 집합인 F로부터, 랜덤 벡터 x와 y를 랜덤하게 선택하는 벡터 선택부, 최대 차수가 $\frac{n}{b}$인 원시 다항식들의 집합으로 구성되는 다항식 환에서, (b-1)차수의 원시 다항식인 P_I를 랜덤하게 선택하고, 최대 차수가 n인 원시 다항식들의 집합으로 구성되는 다항식 환에서, n차수의 원시 다항식인 P_0, P_N을 랜덤하게 선택하는 다항식 선택부, x, y, P_I를 기초로 $\frac{n}{b}$-튜플 벡터 z($\mathbf{z} = P_I\mathbf{x}^{-1}\mathbf{y} \mod P$)를 연산하는 제1 연산부, P_I, P_0를 기초로 공개키 다항식 P_P($P_P = P_O P_I \mod P^b$)를 연산하고, P_0, z, P_N을 기초로 공개키 벡터 h($\mathbf{h} = P_O\mathbf{z} + P_N P \mod P^b$)를 연산하는 제2 연산부 및 P_P와 h를 공개키로 지정하고, x, y, P_I, P_0를 상기 공개키에 대응되는 개인키로 지정한 후, 상기 공개키로 지정된 P_P와 h를, 보안 통신을 수행할 상기 상대측 전자 장치로 전송하는 키 배포부를 포함한다.

[0010] 또한, 본 발명의 일실시예에 따른 다항식 환을 이용한 비대칭키 기반의 보안 통신을 수행하기 위한 전자 장치의 동작 방법은 사전 설정된 해시 함수인 Hash(·) 및, $\frac{n}{b}$ (n과 b는 정수임)차수의 사전 설정된 원시 다항식인 P가 저장되어 있는 저장부를 유지하는 단계 - Hash(·)와 P는, 보안 통신을 수행하기로 사전 지정된 상대측 전자 단말에도 저장되어 있음 - , 랭크 무게(rank weight) d(d는 정수임)를 갖는 $\frac{n}{b}$-튜플 벡터들의 집합인 F로부터, 랜덤 벡터 x와 y를 랜덤하게 선택하는 단계, 최대 차수가 $\frac{n}{b}$인 원시 다항식들의 집합으로 구성되는 다항식 환에서, (b-1)차수의 원시 다항식인 P_I를 랜덤하게 선택하고, 최대 차수가 n인 원시 다항식들의 집합으로 구성되는 다항식 환에서, n차수의 원시 다항식인 P_0, P_N을 랜덤하게 선택하는 단계, x, y, P_I를 기초로 $\frac{n}{b}$-튜플 벡터 z($\mathbf{z} = P_I\mathbf{x}^{-1}\mathbf{y} \mod P$)를 연산하는 단계, P_I, P_0를 기초로 공개키 다항식 P_P($P_P = P_O P_I \mod P^b$)를 연산하고, P_0, z, P_N을 기초로 공개키 벡터 h($\mathbf{h} = P_O\mathbf{z} + P_N P \mod P^b$)를 연산하는 단계 및 P_P와 h를 공개키로 지정하고, x, y, P_I, P_0를 상기 공개키에 대응되는 개인키로 지정한 후, 상기 공개키로 지정된 P_P와 h를, 보안 통신을 수행할 상기 상대측 전자 장치로 전송하는 단계를 포함한다.

발명의 효과

[0011] 본 발명은 다항식 환을 이용한 비대칭키 기반의 보안 통신을 수행하기 위한 전자 장치 및 그 동작 방법을 제시함으로써, 양자 내성을 갖는 보안 통신이 가능하도록 지원할 수 있다.

도면의 간단한 설명

[0012] 도 1은 본 발명의 일실시예에 따른 다항식 환을 이용한 비대칭키 기반의 보안 통신을 수행하기 위한 전자 장치의 구조를 도시한 도면이다.

도 2는 본 발명의 일실시예에 따른 다항식 환을 이용한 비대칭키 기반의 보안 통신을 수행하기 위한 전자 장치

의 동작 방법을 도시한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0013] 이하에서는 본 발명에 따른 실시예들을 첨부된 도면을 참조하여 상세하게 설명하기로 한다. 이러한 설명은 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였으며, 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 본 명세서 상에서 사용되는 모든 용어들은 본 발명이 속하는 기술분야에서 통상의 지식을 가진 사람에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다.

[0014] 본 문서에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있다는 것을 의미한다. 또한, 본 발명의 다양한 실시예들에 있어서, 각 구성요소들, 기능 블록들 또는 수단들은 하나 또는 그 이상의 하부 구성요소로 구성될 수 있고, 각 구성요소들이 수행하는 전기, 전자, 기계적 기능들은 전자회로, 집적회로, ASIC(Application Specific Integrated Circuit) 등 공지된 다양한 소자들 또는 기계적 요소들로 구현될 수 있으며, 각각 별개로 구현되거나 2 이상이 하나로 통합되어 구현될 수도 있다.

[0015] 한편, 첨부된 블록도의 블록들이나 흐름도의 단계들은 범용 컴퓨터, 특수용 컴퓨터, 휴대용 노트북 컴퓨터, 네트워크 컴퓨터 등 데이터 프로세싱이 가능한 장비의 프로세서나 메모리에 탑재되어 지정된 기능들을 수행하는 컴퓨터 프로그램 명령들(instructions)을 의미하는 것으로 해석될 수 있다. 이들 컴퓨터 프로그램 명령들은 컴퓨터 장치에 구비된 메모리 또는 컴퓨터에서 판독 가능한 메모리에 저장될 수 있기 때문에, 블록도의 블록들 또는 흐름도의 단계들에서 설명된 기능들은 이를 수행하는 명령 수단을 내포하는 제조물로 생산될 수도 있다. 아울러, 각 블록 또는 각 단계는 특정된 논리적 기능(들)을 실행하기 위한 하나 이상의 실행 가능한 명령들을 포함하는 모듈, 세그먼트 또는 코드의 일부를 나타낼 수 있다. 또, 몇 가지 대체 가능한 실시예들에서는 블록들 또는 단계들에서 언급된 기능들이 정해진 순서와 달리 실행되는 것도 가능함을 주목해야 한다. 예컨대, 잇달아 도시되어 있는 두 개의 블록들 또는 단계들은 실질적으로 동시에 수행되거나, 역순으로 수행될 수 있으며, 경우에 따라 일부 블록들 또는 단계들이 생략된 채로 수행될 수도 있다.

[0016] 도 1은 본 발명의 일실시예에 따른 다항식 환을 이용한 비대칭키 기반의 보안 통신을 수행하기 위한 전자 장치의 구조를 도시한 도면이다.

[0017] 도 1을 참조하면, 본 발명에 따른 전자 장치(110)는 저장부(111), 벡터 선택부(112), 다항식 선택부(113), 제1 연산부(114), 제2 연산부(115) 및 키 배포부(116)를 포함한다.

[0018] 저장부(111)에는 사전 설정된 해시 함수인 Hash(·) 및, $\frac{n}{b}$ (n과 b는 정수임)차수의 사전 설정된 원시 다항식인 P가 저장되어 있다.

[0019] 여기서, Hash(·)와 P는, 보안 통신을 수행하기로 사전 지정된 상대측 전자 단말(120)에도 저장되어 있다.

[0020] 벡터 선택부(112)는 랭크 무게(rank weight) d(d는 정수임)를 갖는 $\frac{n}{b}$ -튜플(tuple) 벡터들의 집합인 F로부터, 랜덤 벡터 x와 y를 랜덤하게 선택한다.

[0021] 다항식 선택부(113)는 최대 차수가 $\frac{n}{b}$ 인 원시 다항식들의 집합으로 구성되는 다항식 환에서, (b-1)차수의 원시 다항식인 P_I를 랜덤하게 선택하고, 최대 차수가 n인 원시 다항식들의 집합으로 구성되는 다항식 환에서, n차수의 원시 다항식인 P_0, P_N을 랜덤하게 선택한다.

[0022] 이때, P_I와 P_0, P_N은 하기의 수학식 1과 수학식 2를 만족하는 원시 다항식이다.

수학식 1

[0024] $$P_I \in \mathbb{F}_{q^m}[X]/ < P >$$

수학식 2

[0026] $$P_O, P_N \in \mathbb{F}_{q^m}[X]/ < P^b >$$

[0028] 여기서, $\mathbb{F}_{q^m}$ 는, 체(Field) $\mathbb{F}_q$ 의 확장에 의한 유한체(Finite Field)이다.

[0029] 제1 연산부(114)는 x, y, P_I를 기초로 하기의 수학식 3에 따라, $\frac{n}{b}$ -튜플 벡터 z를 연산한다.

수학식 3

[0031] $$\mathbf{z} = P_I \mathbf{x}^{-1} \mathbf{y} \mod P$$

[0033] 제2 연산부(115)는 P_I, P_0를 기초로 하기의 수학식 4에 따라, 공개키 다항식 P_P를 연산하고, P_0, z, P_N을 기초로 하기의 수학식 5에 따라, 공개키 벡터 h를 연산한다.

수학식 4

[0035] $$P_P = P_O P_I \mod P^b$$

수학식 5

[0037] $$\mathbf{h} = P_O \mathbf{z} + P_N P \mod P^b$$

[0039] 키 배포부(116)는 P_P와 h를 공개키로 지정하고, x, y, P_I, P_0를 상기 공개키에 대응되는 개인키로 지정한 후, 상

기 공개키로 지정된 P_P와 h를, 보안 통신을 수행할 상기 상대측 전자 장치(120)로 전송한다.

[0040] 이때, 본 발명의 일실시예에 따르면, 상대측 전자 장치(120)는 메모리 상에 Hash(·)와 P를 사전 저장하고 있고, 전자 장치(110)로부터 상기 공개키로 지정된 P_P와 h가 수신되면, 상기 메모리 상에 P_P와 h를 저장해 둘 수 있다.

[0041] 그 이후, 상대측 전자 장치(120)는 전자 장치(110)와의 상호 인증을 수행해야 하는 상황이 발생하는 경우, 상기 공개키로 지정된 P_P와 h를 기반으로 암호문을 생성해서 전자 장치(110)로 전송할 수 있다.

[0042] 구체적으로, 상대측 전자 장치(120)는 최대 차수가 ($\frac{n}{b}-b$)이면서, 랭크 무게 r(r은 정수임)을 갖는 $\frac{n}{b}$-튜플 벡터의 집합인 E로부터, 랜덤 벡터 e_1과 e_2를 랜덤하게 선택할 수 있다.

[0043] 그러고 나서, 상대측 전자 장치(120)는 e_1, e_2 및 h를 기초로 길이가 n인 벡터들인, $\mathbf{e}'_1 = [\mathbf{0}, \mathbf{e}_1]$, $\mathbf{e}'_2 = [\mathbf{0}, \mathbf{e}_2]$ 및 $\mathbf{h}' = [\mathbf{0}, \mathbf{h}]$ 를 생성할 수 있다.

[0044] 그 이후, 상대측 전자 장치(120)는 e'_1, e'_2, h', P_P를 기초로 하기의 수학식 6의 연산에 따라, 암호문 c를 생성할 수 있다.

수학식 6

[0046] $$\mathbf{c} = P_P\mathbf{e}'_1 + \mathbf{h}'\mathbf{e}'_2 \mod P^b$$

[0048] 이렇게, c가 생성되면, 상대측 전자 장치(120)는 Hash(·)에 E를 입력으로 인가하여 해시 값 K($K = Hash(E)$)를 연산한 후, 전자 장치(110)로 c와 K를 전송할 수 있다.

[0049] 이때, 본 발명의 일실시예에 따르면, 전자 장치(110)는 디코딩부(117) 및 인증 처리부(118)를 더 포함할 수 있다.

[0050] 디코딩부(117)는 상대측 전자 장치(120)로부터 c와 K가 수신되면, 상기 개인키로 지정된 x, P_I, P_O을 기초로 하기의 수학식 7의 연산을 수행하여 신드롬 벡터 $\mathbf{xc}''_i$ 를 생성한 후, $\mathbf{xc}''_i$ 에 대해 RSR(Rank Support Recovery) 디코딩을 수행하여 E를 재구축한다.

수학식 7

[0052] $$\mathbf{c}'_i = P_O^{-1}\mathbf{c} \mod P^b,$$
$$\mathbf{c}''_i = P_I^{-1}\{\mathbf{c}'_i \mod P\} \mod P,$$
$$\mathbf{xc}''_i = \mathbf{xe}_1 + \mathbf{ye}_2 \mod P$$

[0054] 관련해서, 상기 수학식 7의 연산으로부터 $\mathbf{xc}_i''$ 가 생성되는 과정을 구체적으로 설명하면 다음과 같다.

[0055] 먼저, 상기 수학식 7의 첫 번째 라인을 참조하면, $\{\mathbf{c}_i' \mod P\} = \{P_O^{-1}\mathbf{c} \mod P^b\} \mod P$ 로 표현할 수 있다.

[0056] 이때, $\{P_O^{-1}\mathbf{c} \mod P^b\} \mod P$ 은 $\mathbf{c} = P_P\mathbf{e}_1' + \mathbf{h}'\mathbf{e}_2' \mod P^b$ 이고, $P_P = P_O P_I \mod P^b$ 이므로, $\{P_I\mathbf{e}_1' \mod P^b\} + \{P_O^{-1}\mathbf{h}'\mathbf{e}_2' \mod P^b\} \mod P$ 으로 표현될 수 있다.

[0057] 이때, $\{P_I\mathbf{e}_1' \mod P^b\} \mod P$ 는 하기의 수학식 8과 같이 나타낼 수 있다.

수학식 8

[0059]
$$\{(\{P_I \mod P\}[\mathbf{0}, \mathbf{e}_1]) \mod P^b\} \mod P$$
$$= \{(P_I\mathbf{e}_1) \mod P\} \mod P$$

[0061] 그리고, $\{P_O^{-1}\mathbf{h}'\mathbf{e}_2' \mod P^b\} \mod P$ 는 하기의 수학식 9와 같이 나타낼 수 있다.

수학식 9

[0063]
$$\{P_O^{-1}\mathbf{h}'\mathbf{e}_2' \mod P^b\} \mod P$$
$$= \{(P_N P + [\mathbf{0}, \{P_I\mathbf{x}^{-1}\mathbf{y} \mod P\}])[\mathbf{0}, \mathbf{e}_2] \mod P^b\} \mod P$$
$$= \{P_I\mathbf{x}^{-1}\mathbf{y} \mod P\}\{\mathbf{e}_2 \mod P\}$$
$$= \{P_I\mathbf{x}^{-1}\mathbf{y}\mathbf{e}_2 \mod P\}$$

[0065] 결국, $\{\mathbf{c}_i' \mod P\} \mod P$ 는 $\{P_I\mathbf{e}_1' \mod P^b\} \mod P$ 와

$\{P_O^{-1}\mathbf{h}'\mathbf{e}_2' \mod P^b\} \mod P$ 가 결합된 것으로서, 하기의 수학식 10과 같이 정리될 수 있다.

수학식 10

[0067]
$$\{\mathbf{c}_i' \mod P\} \mod P$$
$$= \{(P_I\mathbf{e}_1) \mod P\} + \{P_I\mathbf{x}^{-1}\mathbf{y}\mathbf{e}_2 \mod P\}$$
$$= P_I\mathbf{e}_1 + P_I\mathbf{x}^{-1}\mathbf{y}\mathbf{e}_2 \mod P$$

[0069] 상기 수학식 10에서 나타낸 바와 같이, $\{\mathbf{c}_i' \mod P\} \mod P$ 는 $P_I\mathbf{e}_1 + P_I\mathbf{x}^{-1}\mathbf{y}\mathbf{e}_2 \mod P$ 로 정리될 수 있으므로, 상기 수학식 7에서 두 번째 라인에 따라 연산을 수행하게 되면, $\mathbf{c}_i''$ 는 $\mathbf{e}_1 + \mathbf{x}^{-1}\mathbf{y}\mathbf{e}_2 \mod P$ 로 연산될 수 있고, 이로 인해, 상기 수학식 8에서의 세 번째 라인에 따른 $\mathbf{x}\mathbf{c}_i''$ 가 연산될 수 있다.

[0070] 인증 처리부(118)는, 디코딩부(117)를 통해, E가 재구축 완료되면, Hash(·)에, 재구축된 E를 입력으로 인가하여, 해시 값 K'($K' = Hash(E)$)을 생성한 후, K'과 K가 서로 일치하는지 비교하여, 서로 일치하는 것으로 확인되면, 상대측 전자 장치(110)에 대한 인증이 완료된 것으로 처리한다.

[0071] 즉, 인증 처리부(118)는 양 해시 값의 비교를 수행함으로써, 디코딩부(117)에서 신드롬 벡터 $\mathbf{x}\mathbf{c}_i''$ 에 대해 RSR 디코딩을 수행하여 재구축한 E가, 상대측 전자 장치(120)에서 랜덤 벡터들을 선택하는데 사용된 E와 서로 일치하는지 여부를 확인할 수 있고, 서로 일치하는 것으로 확인되는 경우, 상대측 전자 장치(120)가 앞서 키 배포부(116)를 통해 배포된 공개키를 정상적으로 소지하고 있는 전자 장치가 맞음을 인증할 수 있게 된다.

[0072] 도 2는 본 발명의 일실시예에 따른 다항식 환을 이용한 비대칭키 기반의 보안 통신을 수행하기 위한 전자 장치의 동작 방법을 도시한 순서도이다.

[0073] 단계(S210)에서는 사전 설정된 해시 함수인 Hash(·) 및, $\frac{n}{b}$ (n과 b는 정수임)차수의 사전 설정된 원시 다항식인 P가 저장되어 있는 저장부를 유지한다.

[0074] 여기서, Hash(·)와 P는, 보안 통신을 수행하기로 사전 지정된 상대측 전자 단말에도 저장되어 있다.

[0075] 단계(S220)에서는 랭크 무게 d(d는 정수임)를 갖는 $\frac{n}{b}$ -튜플 벡터들의 집합인 F로부터, 랜덤 벡터 x와 y를 랜덤하게 선택한다.

[0076] 단계(S230)에서는 최대 차수가 $\frac{n}{b}$ 인 원시 다항식들의 집합으로 구성되는 다항식 환에서, (b-1)차수의 원시 다항식인 P_I를 랜덤하게 선택하고, 최대 차수가 n인 원시 다항식들의 집합으로 구성되는 다항식 환에서, n차수의 원시 다항식인 P_0, P_N을 랜덤하게 선택한다.

[0077] 단계(S240)에서는 x, y, P_I를 기초로 $\frac{n}{b}$-튜플 벡터 z($\mathbf{z} = P_I \mathbf{x}^{-1} \mathbf{y} \mod P$)를 연산한다.

[0078] 단계(S250)에서는 P_I, P_O를 기초로 공개키 다항식 P_P($P_P = P_O P_I \mod P^b$)를 연산하고, P_O, z, P_N을 기초로 공개키 벡터 h($\mathbf{h} = P_O \mathbf{z} + P_N P \mod P^b$)를 연산한다.

[0079] 단계(S260)에서는 P_P와 h를 공개키로 지정하고, x, y, P_I, P_O를 상기 공개키에 대응되는 개인키로 지정한 후, 상기 공개키로 지정된 P_P와 h를, 보안 통신을 수행할 상기 상대측 전자 장치로 전송한다.

[0080] 이때, 본 발명의 일실시예에 따르면, 상기 상대측 전자 장치는 메모리 상에 Hash(·)와 P를 사전 저장하고 있고, 상기 전자 장치로부터 상기 공개키로 지정된 P_P와 h가 수신되면, 상기 메모리 상에 P_P와 h를 저장해 둔 후, 상기 전자 장치와의 상호 인증을 수행해야 하는 상황이 발생하는 경우, 최대 차수가 ($\frac{n}{b} - b$)이면서, 랭크 무게 r(r은 정수임)을 갖는 $\frac{n}{b}$-튜플 벡터의 집합인 E로부터, 랜덤 벡터 e_1과 e_2를 랜덤하게 선택하고, e_1, e_2 및 h를 기초로 길이가 n인 벡터들인, $\mathbf{e}'_1 = [\mathbf{0}, \mathbf{e}_1]$, $\mathbf{e}'_2 = [\mathbf{0}, \mathbf{e}_2]$ 및 $\mathbf{h}' = [\mathbf{0}, \mathbf{h}]$를 생성한 후, e'_1, e'_2, h', P_P를 기초로 암호문 c($\mathbf{c} = P_P \mathbf{e}'_1 + \mathbf{h}' \mathbf{e}'_2 \mod P^b$)를 생성하고, Hash(·)에 E를 입력으로 인가하여 해시 값 K($K = Hash(E)$)를 연산한 후, 상기 전자 장치로 c와 K를 전송할 수 있다.

[0081] 이때, 본 발명의 일실시예에 따르면, 상기 전자 장치의 동작 방법은 상기 상대측 전자 장치로부터 c와 K가 수신되면, 상기 개인키로 지정된 x, P_I, P_O을 기초로 상기 수학식 7의 연산을 수행하여 신드롬 벡터 $\mathbf{xc}''_i$를 생성한 후, $\mathbf{xc}''_i$에 대해 RSR 디코딩을 수행하여 E를 재구축하는 단계 및 Hash(·)에, 재구축된 E를 입력으로 인가하여, 해시 값 K'($K' = Hash(E)$)을 생성한 후, K'과 K가 서로 일치하는지 비교하여, 서로 일치하는 것으로 확인되면, 상기 상대측 전자 장치에 대한 인증이 완료된 것으로 처리하는 단계를 더 포함할 수 있다.

[0082] 이상, 도 2를 참조하여 본 발명의 일실시예에 따른 전자 장치의 동작 방법에 대해 설명하였다. 여기서, 본 발명의 일실시예에 따른 전자 장치의 동작 방법은 도 1을 이용하여 설명한 전자 장치(110)의 동작에 대한 구성과 대응될 수 있으므로, 이에 대한 보다 상세한 설명은 생략하기로 한다.

[0083] 본 발명의 일실시예에 따른 전자 장치의 동작 방법은 컴퓨터와의 결합을 통해 실행시키기 위한 저장매체에 저장된 컴퓨터 프로그램으로 구현될 수 있다.

[0084] 또한, 본 발명의 일실시예에 따른 전자 장치의 동작 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.

[0085] 이상과 같이 본 발명에서는 구체적인 구성 요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되

었으나 이는 본 발명의 보다 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

[0086] 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

부호의 설명

[0087] 110: 전자 장치

111: 저장부 112: 벡터 선택부

113: 다항식 선택부 114: 제1 연산부

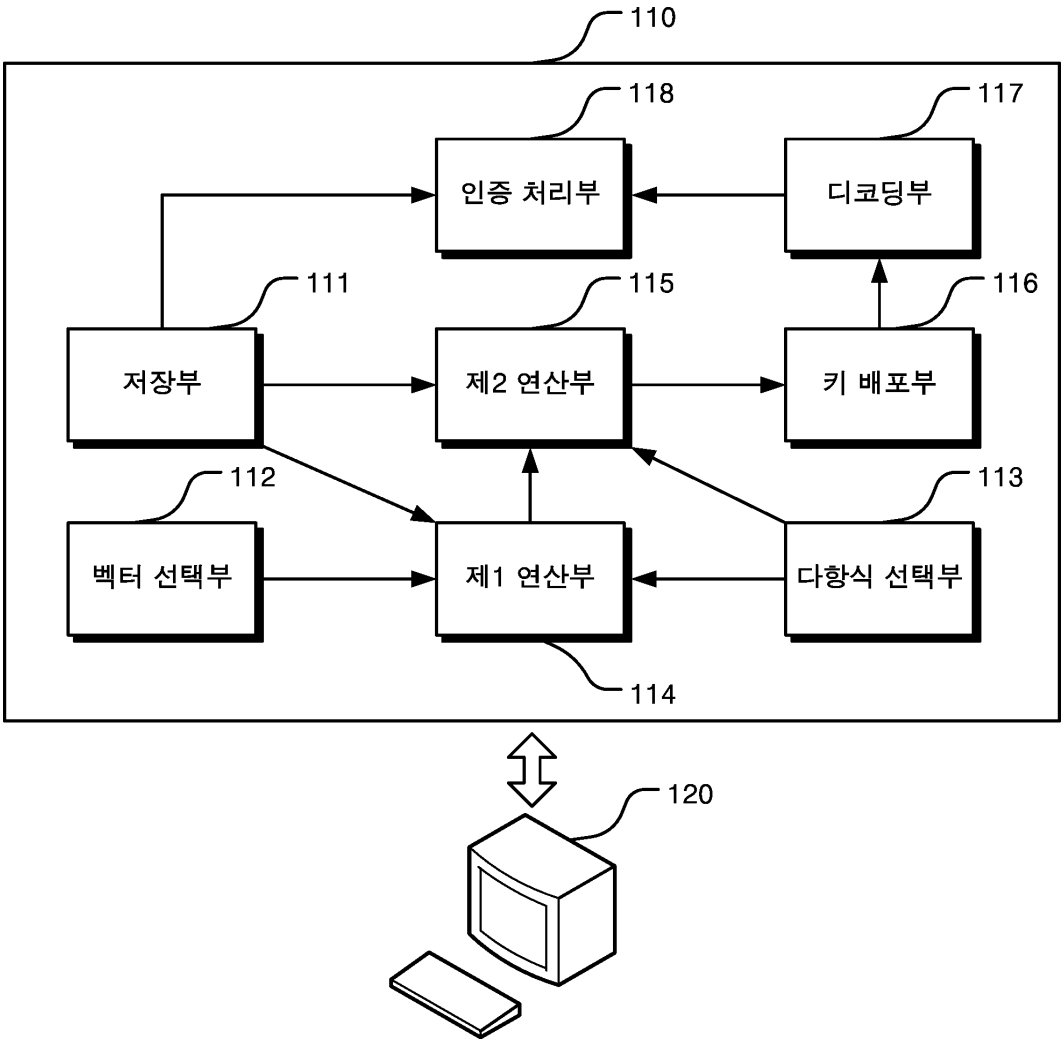
115: 제2 연산부 116: 키 배포부

117: 디코딩부 118: 인증 처리부

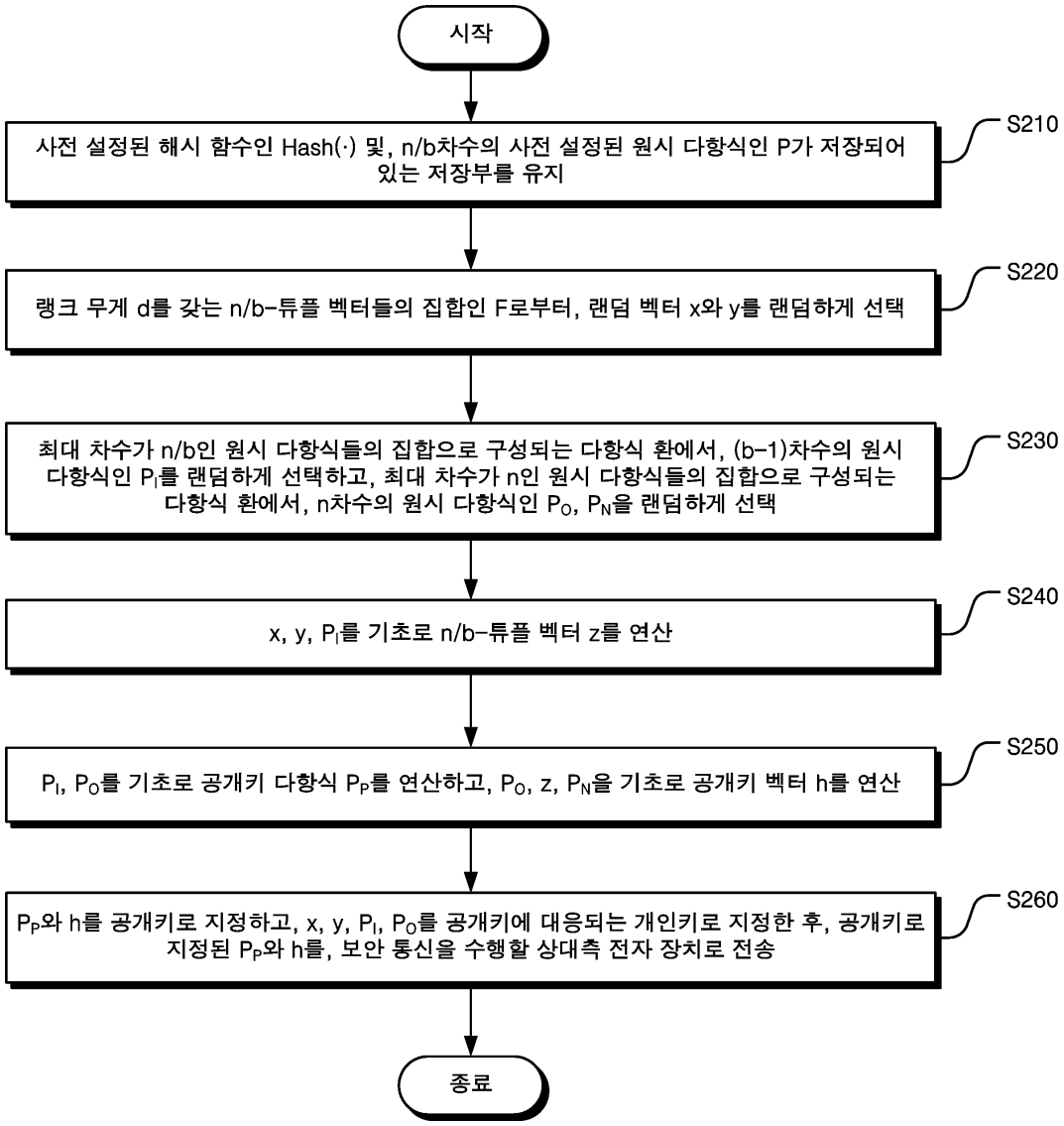
120: 상대측 전자 장치

도면

도면1



도면2


시작
사전 설정된 해시 함수인 Hash(·) 및, n/b차수의 사전 설정된 원시 다항식인 P가 저장되어 있는 저장부를 유지
S210
랭크 무게 d를 갖는 n/b-튜플 벡터들의 집합인 F로부터, 랜덤 벡터 x와 y를 랜덤하게 선택
S220
최대 차수가 n/b인 원시 다항식들의 집합으로 구성되는 다항식 환에서, (b-1)차수의 원시 다항식인 P_I를 랜덤하게 선택하고, 최대 차수가 n인 원시 다항식들의 집합으로 구성되는 다항식 환에서, n차수의 원시 다항식인 P_O, P_N을 랜덤하게 선택
S230
x, y, P_I를 기초로 n/b-튜플 벡터 z를 연산
S240
P_I, P_O를 기초로 공개키 다항식 P_P를 연산하고, P_O, z, P_N을 기초로 공개키 벡터 h를 연산
S250
P_P와 h를 공개키로 지정하고, x, y, P_I, P_O를 공개키에 대응되는 개인키로 지정한 후, 공개키로 지정된 P_P와 h를, 보안 통신을 수행할 상대측 전자 장치로 전송
S260
종료