(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2018년06월08일
(11) 등록번호 10-1865703
(24) 등록일자 2018년06월01일

(51) 국제특허분류(Int. Cl.)
H04L 9/08 (2006.01) *H04L 9/32* (2006.01)
(52) CPC특허분류
H04L 9/0861 (2013.01)
H04L 9/0869 (2013.01)
(21) 출원번호 10-2016-0142251
(22) 출원일자 2016년10월28일
심사청구일자 2016년11월09일
(65) 공개번호 10-2018-0046720
(43) 공개일자 2018년05월09일
(56) 선행기술조사문헌
KR101460541 B1
KR101329007 B1
KR1020070096014 A
KR1020140057134 A

(73) 특허권자
삼성에스디에스 주식회사
서울특별시 송파구 올림픽로35길 125 (신천동)
(72) 발명자
최규영
서울특별시 송파구 올림픽로35길 125 (신천동, 삼성SDS타워 West Campus)
문덕재
서울특별시 송파구 올림픽로35길 125 (신천동, 삼성SDS타워 West Campus)
조지훈
서울특별시 송파구 올림픽로35길 125 (신천동, 삼성SDS타워 West Campus)
(74) 대리인
두호특허법인

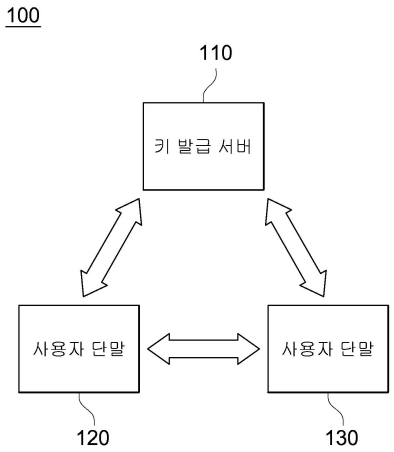
전체 청구항 수 : 총 20 항 심사관 : 양종필

(54) 발명의 명칭 **키 생성 방법 및 장치, 암호화 장치 및 방법**

(57) 요 약

본 발명의 일 실시예에 따른 키 생성 장치는, 키 요청 단말로부터 기 설정된 아이디 제약 조건에 따라 생성된 아이디를 포함하는 키 생성 요청을 수신하는 수신부, 상기 아이디 제약 조건에 따라 이용 가능한 모든 심볼들 각각에 대한 아이디 내 위치별 비밀 파라미터 값을 포함하는 비밀 파라미터 테이블로부터 상기 수신된 아이디에 포함된 각 심볼들의 상기 수신된 아이디 내 위치에 대응하는 비밀 파라미터 값들을 추출하고, 추출된 비밀 파라미터 값들을 이용하여, 상기 수신된 아이디에 대응하는 비밀키를 생성하는 비밀키 생성부 및 상기 비밀키를 상기 키 요청 단말로 제공하는 키 정보 제공부를 포함한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/3247 (2013.01)

명 세 서

청구범위

청구항 1

키 요청 단말로부터 기 설정된 아이디 제약 조건에 따라 생성된 아이디를 포함하는 키 생성 요청을 수신하는 수신부;

상기 아이디 제약 조건에 따라 이용 가능한 모든 심볼들 각각에 대한 아이디 내 위치별 비밀 파라미터 값을 포함하는 비밀 파라미터 테이블로부터 상기 수신된 아이디에 포함된 각 심볼들의 상기 수신된 아이디 내 위치에 대응하는 비밀 파라미터 값들을 추출하고, 추출된 비밀 파라미터 값들을 이용하여, 상기 수신된 아이디에 대응하는 비밀키를 생성하는 비밀키 생성부; 및

상기 비밀키를 상기 키 요청 단말로 제공하는 키 정보 제공부를 포함하는 키 생성 장치.

청구항 2

청구항 1에 있어서,

상기 비밀키 생성부는, 상기 추출된 비밀 파라미터 값들의 합을 이용하여 상기 비밀키를 생성하는 키 생성 장치.

청구항 3

청구항 1에 있어서,

상기 비밀키는, 아래의 수학식

$$Sk = \sum_{i=1}^{n} S_i \cdot R$$

(이때, Sk는 상기 비밀키, n은 상기 수신된 아이디의 자릿수, S_i는 상기 수신된 아이디 내 i 번째 위치의 심볼에 대응하는 비밀 파라미터 값, R은 임의의 난수)

에 의해 생성되는 키 생성 장치.

청구항 4

청구항 1에 있어서,

상기 아이디 내 위치는, 아이디를 복수의 블록으로 분할하였을 때, 분할된 각 블록 내 위치이며,

상기 비밀키 생성부는, 상기 추출된 비밀 파라미터 값들을 상기 각 블록별로 합한 값들을 이용하여 상기 비밀키를 생성하는 키 생성 장치.

청구항 5

청구항 4에 있어서,

상기 비밀키는, 아래의 수학식

$$Sk = \sum_{k=1}^{m}(B_k) \cdot R_k$$

(이때, Sk는 비밀키, m은 상기 분할된 블록의 수, B_k는 k번째 블록에 대한 상기 추출된 비밀 파라미터 값들의 합, R_k는 임의의 난수)

에 의해 생성되는 키 생성 장치.

청구항 6

청구항 5에 있어서,

상기 R_k는, 상기 B_k가 가질 수 있는 최대 비트 수의 k배 크기의 비트 수를 가지는 임의의 난수인 키 생성 장치.

청구항 7

키 요청 단말로부터 기 설정된 아이디 제약 조건에 따라 생성된 아이디를 포함하는 키 생성 요청을 수신하는 단계;

상기 아이디 제약 조건에 따라 이용 가능한 모든 심볼들 각각에 대한 아이디 내 위치별 비밀 파라미터 값을 포함하는 비밀 파라미터 테이블로부터 상기 수신된 아이디에 포함된 각 심볼들의 상기 수신된 아이디 내 위치에 대응하는 비밀 파라미터 값들을 추출하는 단계;

상기 추출된 비밀 파라미터 값들을 이용하여, 상기 수신된 아이디에 대응하는 비밀키를 생성하는 단계; 및

상기 비밀키를 상기 키 요청 단말로 제공하는 단계를 포함하는 키 생성 방법.

청구항 8

청구항 7에 있어서,

상기 비밀키를 생성하는 단계는, 상기 추출된 비밀 파라미터 값들의 합을 이용하여 상기 비밀키를 생성하는 키 생성 방법.

청구항 9

청구항 7에 있어서,

상기 비밀키는, 아래의 수학식

$$Sk = \sum_{i=1}^{n} S_i \cdot R$$

(이때, Sk는 상기 비밀키, n은 상기 수신된 아이디의 자릿수, S_i는 상기 수신된 아이디 내 i 번째 위치의 심볼에 대응하는 비밀 파라미터 값, R은 임의의 난수)

에 의해 생성되는 키 생성 방법.

청구항 10

청구항 7에 있어서,

상기 아이디 내 위치는, 아이디를 복수의 블록으로 분할하였을 때, 분할된 각 블록 내 위치이며,

상기 비밀키를 생성하는 단계는, 상기 추출된 비밀 파라미터 값들을 상기 각 블록별로 합한 값들을 이용하여 상기 비밀키를 생성하는 키 생성 방법.

청구항 11

청구항 10에 있어서,

상기 비밀키는, 아래의 수학식

$$Sk = \sum_{k=1}^{m}(B_k) \cdot R_k$$

(이때, Sk는 비밀키, m은 상기 분할된 블록의 수, B_k는 k번째 블록에 대한 상기 추출된 비밀 파라미터 값들의 합, R_k는 임의의 난수)

에 의해 생성되는 키 생성 방법.

청구항 12

청구항 11에 있어서,

상기 R_k는, 상기 B_k가 가질 수 있는 최대 비트 수의 k배 크기의 비트 수를 가지는 임의의 난수인 키 생성 방법.

청구항 13

기 설정된 아이디 제약 조건에 따라 생성된 암호화 장치의 사용자 아이디를 포함한 키 생성 요청을 키 발급 서버로 전송하여, 상기 키 발급 서버로부터 상기 기 설정된 아이디 제약 조건에 따라 생성 가능한 모든 심볼들에 대한 아이디 내 위치별 공개 파라미터 값을 포함하는 공개 파라미터 테이블 및 상기 암호화 장치의 사용자 아이디에 대응되는 비밀키를 획득하는 키 정보 획득부;

상기 공개 파라미터 테이블을 공유하는 외부 단말로부터 상기 아이디 제약 조건에 따라 생성된 상기 외부 단말의 사용자 아이디를 수신하는 아이디 수신부;

상기 공개 파라미터 테이블로부터 상기 외부 단말의 사용자 아이디에 포함된 각 심볼의 아이디 내 위치에 대응되는 공개 파라미터 값들을 추출하고, 상기 추출된 공개 파라미터 값들을 이용하여 상기 외부 단말의 사용자 아이디에 대응되는 공개키를 생성하는 공개키 생성부; 및

상기 공개키를 이용하여 상기 외부 단말로 전송할 데이터를 암호화 하거나, 상기 비밀키를 이용하여 상기 전송할 데이터에 대한 전자 서명을 수행하는 암호화부를 포함하는 암호화 장치.

청구항 14

청구항 13에 있어서,

상기 공개키 생성부는, 상기 추출된 공개 파라미터들의 곱을 이용하여 상기 사용자 아이디에 대응되는 공개키를 생성하는 암호화 장치.

청구항 15

청구항 13에 있어서,

상기 아이디 내 위치는, 상기 외부 단말의 사용자 아이디를 복수의 블록으로 분할하였을 때, 분할된 각 블록 내

위치이며,

상기 공개키 생성부는, 상기 추출된 공개 파라미터 값들을 상기 각 블록별로 곱한 값들을 이용하여 상기 사용자 아이디에 대응되는 공개키를 생성하는 암호화 장치.

청구항 16

청구항 13에 있어서,

상기 외부 단말로 상기 암호화 장치의 사용자 아이디를 제공하는 아이디 제공부;

상기 외부 단말로부터 상기 암호화 장치의 사용자 아이디에 대응되는 공개키를 이용하여 암호화된 데이터 또는 상기 외부 단말의 비밀키를 이용하여 전자 서명된 데이터를 수신하는 데이터 수신부; 및

상기 암호화 장치의 사용자 아이디에 대응되는 비밀키를 이용하여 상기 암호화된 데이터를 복호화하거나, 상기 외부 단말의 사용자 아이디에 대응되는 공개키를 이용하여 상기 전자 서명된 데이터에 대한 검증을 수행하는 복호화부를 더 포함하는 암호화 장치.

청구항 17

기 설정된 아이디 제약 조건에 따라 생성된 암호화 장치의 사용자 아이디를 포함한 키 생성 요청을 키 발급 서버로 전송하는 단계;

상기 키 발급 서버로부터 상기 기 설정된 아이디 제약 조건에 따라 생성 가능한 모든 심볼들에 대한 아이디 내 위치별 공개 파라미터 값을 포함하는 공개 파라미터 테이블 및 상기 암호화 장치의 사용자 아이디에 대응되는 비밀키를 획득하는 단계;

상기 공개 파라미터 테이블을 공유하는 외부 단말로부터 상기 아이디 제약 조건에 따라 생성된 상기 외부 단말의 사용자 아이디를 수신하는 단계;

상기 공개 파라미터 테이블로부터 상기 외부 단말의 사용자 아이디에 포함된 각 심볼의 아이디 내 위치에 대응되는 공개 파라미터 값들을 추출하는 단계;

상기 추출된 공개 파라미터 값들을 이용하여 상기 외부 단말의 사용자 아이디에 대응되는 공개키를 생성하는 단계; 및

상기 공개키를 이용하여 상기 외부 단말로 전송할 데이터를 암호화 하거나, 상기 비밀키를 이용하여 상기 전송할 데이터에 대한 전자 서명을 수행하는 단계를 포함하는 암호화 방법.

청구항 18

청구항 17에 있어서,

상기 공개키를 생성하는 단계, 상기 추출된 공개 파라미터들의 곱을 이용하여 상기 사용자 아이디에 대응되는 공개키를 생성하는 암호화 방법.

청구항 19

청구항 17에 있어서,

상기 아이디 내 위치는, 상기 외부 단말의 사용자 아이디를 복수의 블록으로 분할하였을 때, 분할된 각 블록 내 위치이며,

상기 공개키를 생성하는 단계는, 상기 추출된 공개 파라미터 값들을 상기 각 블록별로 곱한 값들을 이용하여 상기 사용자 아이디에 대응되는 공개키를 생성하는 암호화 방법.

청구항 20

청구항 17에 있어서,

상기 외부 단말로 상기 암호화 장치의 사용자 아이디를 제공하는 단계;

상기 외부 단말로부터 상기 암호화 장치의 사용자 아이디에 대응되는 공개키를 이용하여 암호화된 데이터 또는 상기 외부 단말의 비밀키를 이용하여 전자 서명된 데이터를 수신하는 단계; 및

상기 암호화 장치의 사용자 아이디에 대응되는 비밀키를 이용하여 상기 암호화된 데이터를 복호화하거나, 상기 외부 단말의 사용자 아이디에 대응되는 공개키를 이용하여 상기 전자 서명된 데이터에 대한 검증을 수행하는 단계를 더 포함하는 암호화 방법.

발명의 설명

기 술 분 야

[0001] 본 발명의 실시예들은 암호화 및 암호화를 위한 키 생성 기술과 관련된다.

배 경 기 술

[0002] 최근 컴퓨터 기술의 발달과 통신망의 급속한 확장으로 인해 컴퓨터 관련 자원과 전송되는 데이터들에 대한 보안 문제가 큰 이슈로 부각되고 있다. 이러한 문제를 해결할 수 있는 하나의 대안으로 암호 기반 시스템이 이용되고 있다. 현재까지 가장 크게 기여한 암호 시스템은 공개키 암호 시스템인데, 이와 같은 전통적 공개키 시스템에서는 사용자의 공개키를 미리 인증해야 하고 문제가 발생한 인증서는 유효기간 종료 전이라도 폐기해야 하므로 공개키의 인증서 관리에 관한 어려움이 발생한다. 따라서 개인의 아이디(identity, ID)를 기반으로 하는 아이디(ID) 기반 암호 시스템이 제안되었다.

[0003] 공개키 기반 암호 시스템은 비밀키를 먼저 정하고 공개키를 계산하는 방식을 따른다. 반면, 아이디 기반 암호 시스템은 아이디를 먼저 선택하고 이로부터 비밀키를 계산하며, 비밀키 발급은 키 발행 기관(PKG, private key generator)이 아이디로부터 계산하여 안전한 채널을 통해 발급한다.

[0004] 이와 관련하여, 선행 특허 문헌인 한국등록특허 제10-1301609호는 아이디 기반 암호 시스템에서 사전계산 테이블을 이용한 이산대수 계산 방법을 적용하여 아이디와 비밀키 간의 일대일로 대응하는 관계를 보장할 수 있는 비밀키를 계산하는 방법을 제안하고 있다. 그러나, 해당 선행 특허 문헌에서 제안하는 방법은 사전계산으로 인해 사용자들의 아이디에 대한 비밀키 생성을 위해 많은 시간과 많은 비용(Amazon EC2 기준 100 core로 100일)이 요구된다. 따라서 제공하는 서비스에 따라 별도의 키 생성이 필요한 경우 시간과 비용적으로 비효율적인 문제점이 있다

선행기술문헌

특허문헌

[0005] (특허문헌 0001) 한국등록특허 제10-1301609호 (2013.8.29. 공고)

발명의 내용

해결하려는 과제

[0006] 본 발명의 실시예들은 암호화를 위한 키 생성 장치 및 방법과 암호화 장치 및 방법을 제공하기 위한 것이다.

과제의 해결 수단

[0007] 본 발명의 일 실시예에 따른 키 생성 장치는, 키 요청 단말로부터 기 설정된 아이디 제약 조건에 따라 생성된

아이디를 포함하는 키 생성 요청을 수신하는 수신부, 상기 아이디 제약 조건에 따라 이용 가능한 모든 심볼들 각각에 대한 아이디 내 위치별 비밀 파라미터 값을 포함하는 비밀 파라미터 테이블로부터 상기 수신된 아이디에 포함된 각 심볼들의 상기 수신된 아이디 내 위치에 대응하는 비밀 파라미터 값들을 추출하고, 추출된 비밀 파라미터 값들을 이용하여, 상기 수신된 아이디에 대응하는 비밀키를 생성하는 비밀키 생성부 및 상기 비밀키를 상기 키 요청 단말로 제공하는 키 정보 제공부를 포함한다.

[0008] 상기 비밀키 생성부는, 상기 추출된 비밀 파라미터 값들의 합을 이용하여 상기 비밀키를 생성할 수 있다.

[0009] 상기 비밀키는, 아래의 수학식

$$Sk = \sum_{i=1}^{n} S_i \cdot R$$

[0010]

[0011] (이때, Sk는 상기 비밀키, n은 상기 수신된 아이디의 자릿수, S_i는 상기 수신된 아이디 내 i 번째 위치의 심볼에 대응하는 비밀 파라미터 값, R은 임의의 난수)에 의해 생성될 수 있다.

[0012] 상기 아이디 내 위치는, 아이디를 복수의 블록으로 분할하였을 때, 분할된 각 블록 내 위치이며, 상기 비밀키 생성부는, 상기 추출된 비밀 파라미터 값들을 상기 각 블록별로 합한 값들을 이용하여 상기 비밀키를 생성할 수 있다.

[0013] 상기 비밀키는, 아래의 수학식

$$Sk = \sum_{k=1}^{m} (B_k) \cdot R_k$$

[0014]

[0015] (이때, Sk는 비밀키, m은 상기 분할된 블록의 수, B_k는 k번째 블록에 대한 상기 추출된 비밀 파라미터 값들의 합, R_k는 임의의 난수)에 의해 생성될 수 있다.

[0016] 상기 R_k는, 상기 B_k가 가질 수 있는 최대 비트 수의 k배 크기의 비트 수를 가지는 임의의 난수일 수 있다.

[0017] 본 발명의 일 실시예에 따른 키 생성 방법은, 키 요청 단말로부터 기 설정된 아이디 제약 조건에 따라 생성된 아이디를 포함하는 키 생성 요청을 수신하는 단계, 상기 아이디 제약 조건에 따라 이용 가능한 모든 심볼들 각각에 대한 아이디 내 위치별 비밀 파라미터 값을 포함하는 비밀 파라미터 테이블로부터 상기 수신된 아이디에 포함된 각 심볼들의 상기 수신된 아이디 내 위치에 대응하는 비밀 파라미터 값들을 추출하는 단계, 상기 추출된 비밀 파라미터 값들을 이용하여, 상기 수신된 아이디에 대응하는 비밀키를 생성하는 단계 및 상기 비밀키를 상기 키 요청 단말로 제공하는 단계를 포함한다.

[0018] 상기 비밀키를 생성하는 단계는, 상기 추출된 비밀 파라미터 값들의 합을 이용하여 상기 비밀키를 생성할 수 있다.

[0019] 상기 비밀키는, 아래의 수학식

$$Sk = \sum_{i=1}^{n} S_i \cdot R$$

[0020]

[0021] (이때, Sk는 상기 비밀키, n은 상기 수신된 아이디의 자릿수, S_i는 상기 수신된 아이디 내 i 번째 위치의 심볼에 대응하는 비밀 파라미터 값, R은 임의의 난수)에 의해 생성될 수 있다.

[0022] 상기 아이디 내 위치는, 아이디를 복수의 블록으로 분할하였을 때, 분할된 각 블록 내 위치이며, 상기 비밀키를 생성하는 단계는, 상기 추출된 비밀 파라미터 값들을 상기 각 블록별로 합한 값들을 이용하여 상기 비밀키를 생성할 수 있다.

[0023] 상기 비밀키는, 아래의 수학식

$$Sk = \sum_{k=1}^{m} (B_k) \cdot R_k$$

[0024]

[0025] (이때, Sk는 비밀키, m은 상기 분할된 블록의 수, B_k는 k번째 블록에 대한 상기 추출된 비밀 파라미터 값들의

합, R_k는 임의의 난수)에 의해 생성될 수 있다.

[0026] 상기 R_k는, 상기 B_k가 가질 수 있는 최대 비트 수의 k배 크기의 비트 수를 가지는 임의의 난수일 수 있다.

[0027] 본 발명의 일 실시예에 따른 암호화 장치는, 기 설정된 아이디 제약 조건에 따라 생성된 암호화 장치의 사용자 아이디를 포함한 키 생성 요청을 키 발급 서버로 전송하여, 상기 키 발급 서버로부터 상기 기 설정된 아이디 제약 조건에 따라 생성 가능한 모든 심볼들에 대한 아이디 내 위치별 공개 파라미터 값을 포함하는 공개 파라미터 테이블 및 상기 암호화 장치의 사용자 아이디에 대응되는 비밀키를 획득하는 키 정보 획득부, 상기 공개 파라미터 테이블을 공유하는 외부 단말로부터 상기 아이디 제약 조건에 따라 생성된 상기 외부 단말의 사용자 아이디를 수신하는 아이디 수신부, 상기 공개 파라미터 테이블로부터 상기 외부 단말의 사용자 아이디에 포함된 각 심볼의 아이디 내 위치에 대응되는 공개 파라미터 값들을 추출하고, 상기 추출된 공개 파라미터 값들을 이용하여 상기 외부 단말의 사용자 아이디에 대응되는 공개키를 생성하는 공개키 생성부 및 상기 공개키를 이용하여 상기 외부 단말로 전송할 데이터를 암호화 하거나, 상기 비밀키를 이용하여 상기 전송할 데이터에 대한 전자 서명을 수행하는 암호화부를 포함한다.

[0028] 상기 공개키 생성부는, 상기 추출된 공개 파라미터들의 곱을 이용하여 상기 사용자 아이디에 대응되는 공개키를 생성할 수 있다.

[0029] 상기 아이디 내 위치는, 상기 외부 단말의 사용자 아이디를 복수의 블록으로 분할하였을 때, 분할된 각 블록 내 위치이며, 상기 공개키 생성부는, 상기 추출된 공개 파라미터 값들을 상기 각 블록별로 곱한 값들을 이용하여 상기 사용자 아이디에 대응되는 공개키를 생성할 수 있다.

[0030] 상기 암호화 장치는, 상기 외부 단말로 상기 암호화 장치의 사용자 아이디를 제공하는 아이디 제공부, 상기 외부 단말로부터 상기 암호화 장치의 사용자 아이디에 대응되는 공개키를 이용하여 암호화된 데이터 또는 상기 외부 단말의 비밀키를 이용하여 전자 서명된 데이터를 수신하는 데이터 수신부 및 상기 암호화 장치의 사용자 아이디에 대응되는 비밀키를 이용하여 상기 암호화된 데이터를 복호화하거나, 상기 외부 단말의 사용자 아이디에 대응되는 공개키를 이용하여 상기 전자 서명된 데이터에 대한 검증을 수행하는 복호화부를 더 포함할 수 있다.

[0031] 본 발명의 일 실시예에 따른 암호화 방법은, 기 설정된 아이디 제약 조건에 따라 생성된 암호화 장치의 사용자 아이디를 포함한 키 생성 요청을 키 발급 서버로 전송하는 단계, 상기 키 발급 서버로부터 상기 기 설정된 아이디 제약 조건에 따라 생성 가능한 모든 심볼들에 대한 아이디 내 위치별 공개 파라미터 값을 포함하는 공개 파라미터 테이블 및 상기 암호화 장치의 사용자 아이디에 대응되는 비밀키를 획득하는 단계, 상기 공개 파라미터 테이블을 공유하는 외부 단말로부터 상기 아이디 제약 조건에 따라 생성된 상기 외부 단말의 사용자 아이디를 수신하는 단계, 상기 공개 파라미터 테이블로부터 상기 외부 단말의 사용자 아이디에 포함된 각 심볼의 아이디 내 위치에 대응되는 공개 파라미터 값들을 추출하는 단계, 상기 추출된 공개 파라미터 값들을 이용하여 상기 외부 단말의 사용자 아이디에 대응되는 공개키를 생성하는 단계 및 상기 공개키를 이용하여 상기 외부 단말로 전송할 데이터를 암호화 하거나, 상기 비밀키를 이용하여 상기 전송할 데이터에 대한 전자 서명을 수행하는 단계를 포함한다.

[0032] 상기 공개키를 생성하는 단계는, 상기 추출된 공개 파라미터들의 곱을 이용하여 상기 사용자 아이디에 대응되는 공개키를 생성할 수 있다.

[0033] 상기 아이디 내 위치는, 상기 외부 단말의 사용자 아이디를 복수의 블록으로 분할하였을 때, 분할된 각 블록 내 위치이며, 상기 공개키를 생성하는 단계는, 상기 추출된 공개 파라미터 값들을 상기 각 블록별로 곱한 값들을 이용하여 상기 사용자 아이디에 대응되는 공개키를 생성할 수 있다.

[0034] 상기 암호화 방법은, 상기 외부 단말로 상기 암호화 장치의 사용자 아이디를 제공하는 단계, 상기 외부 단말로부터 상기 암호화 장치의 사용자 아이디에 대응되는 공개키를 이용하여 암호화된 데이터 또는 상기 외부 단말의 비밀키를 이용하여 전자 서명된 데이터를 수신하는 단계 및 상기 암호화 장치의 사용자 아이디에 대응되는 비밀키를 이용하여 상기 암호화된 데이터를 복호화하거나, 상기 외부 단말의 사용자 아이디에 대응되는 공개키를 이용하여 상기 전자 서명된 데이터에 대한 검증을 수행하는 단계를 더 포함할 수 있다.

발명의 효과

[0035] 본 발명의 실시예들에 따르면, 사용자의 아이디를 구성하는 심볼의 위치에 1:1 대응되는 비밀 파라미터를 이용하여 비밀키를 생성함으로써, 종래 기술에서 요구되는 사전계산이 요구되지 않으며, 이에 따라 키 생성을 위해

요구되는 처리 시간과 비용을 현저하게 줄일 수 있게 된다.

도면의 간단한 설명

[0036] 도 1은 본 발명의 일 실시예에 따른 암호화 시스템의 구성도

도 2는 본 발명의 일 실시예에 따른 키 생성 장치의 구성도

도 3은 본 발명의 추가적인 실시예에 따른 키 생성 장치의 구성도

도 4는 비밀 파라미터 테이블의 일 예를 나타낸 예시도

도 5는 비밀 파라미터 테이블의 다른 예를 나타낸 예시도

도 6은 공개 파라미터 테이블의 일 예를 나타낸 예시도

도 7은 공개 파라미터 테이블의 다른 예를 나타낸 예시도

도 8은 본 발명의 일 실시예에 따른 암호화 장치의 구성도

도 9는 본 발명의 일 실시예에 따른 키 생성 방법의 순서도

도 10은 본 발명의 추가적인 실시예에 따른 키 생성 방법의 순서도

도 11은 본 발명의 일 실시예에 따른 암호화 과정을 나타낸 순서도

도 12는 본 발명의 일 실시예에 따른 복호화 과정을 나타낸 순서도

도 13은 본 발명의 일 실시예에 따른 전자 서명 수행 과정을 나타낸 순서도

도 14는 본 발명의 일 실시예에 따른 전자 서명된 데이터에 대한 검증 과정을 나타낸 순서도

발명을 실시하기 위한 구체적인 내용

[0037] 이하, 도면을 참조하여 본 발명의 구체적인 실시형태를 설명하기로 한다. 이하의 상세한 설명은 본 명세서에서 기술된 방법, 장치 및/또는 시스템에 대한 포괄적인 이해를 돕기 위해 제공된다. 그러나 이는 예시에 불과하며 본 발명은 이에 제한되지 않는다.

[0038] 본 발명의 실시예들을 설명함에 있어서, 본 발명과 관련된 공지기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략하기로 한다. 그리고, 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다. 상세한 설명에서 사용되는 용어는 단지 본 발명의 실시예들을 기술하기 위한 것이며, 결코 제한적이어서는 안 된다. 명확하게 달리 사용되지 않는 한, 단수 형태의 표현은 복수 형태의 의미를 포함한다. 본 설명에서, "포함" 또는 "구비"와 같은 표현은 어떤 특성들, 숫자들, 단계들, 동작들, 요소들, 이들의 일부 또는 조합을 가리키기 위한 것이며, 기술된 것 이외에 하나 또는 그 이상의 다른 특성, 숫자, 단계, 동작, 요소, 이들의 일부 또는 조합의 존재 또는 가능성을 배제하도록 해석되어서는 안 된다.

[0039] 도 1은 본 발명의 일 실시예에 따른 암호화 시스템의 구성도이다.

[0040] 도 1을 참조하면, 본 발명의 일 실시예에 따른 암호화 시스템(100)은 키 발급 서버(110) 및 사용자 단말(12, 130)을 포함한다.

[0041] 키 발급 서버(110)는 예를 들어, 신뢰할 수 있는 기관이나 암호화 서비스 제공자 등에 의해 운영되는 서버로서, 사용자 단말(120, 130)의 키 생성 요청에 따라 암호화를 위한 키 정보를 생성할 수 있다. 또한, 키 발급 서버(110)는 생성된 키 정보를 안전한 채널을 통해 각 사용자 단말(120, 130)로 제공할 수 있다.

[0042] 이때, 키 정보는 후술할 바와 같이 각 사용자 단말(120, 130)의 사용자 아이디에 대응되는 비밀키와 사용자 아이디를 이용하여 공개키를 생성할 수 있는 공개 파라미터 테이블을 포함할 수 있다.

[0043] 각 사용자 단말(120, 130)은 키 발급 서버(110)로부터 키 정보를 제공받아 암복호화 내지는 데이터에 대한 전자 서명 및 검증을 수행하기 위한 장치일 수 있다. 예를 들어, 각 사용자 단말(120, 130)은 스마트폰, PDA, 패블릿(pablet), 데스크톱 PC, 랩톱 PC, 태블릿 PC, 서버, 센서 등과 같이 정보 처리 기능, 데이터 저장 기능 및 유선

또는 무선 네트워크를 통한 데이터 통신 기능을 구비한 다양한 형태의 컴퓨팅 장치일 수 있다.

[0044] 각 사용자 단말(120, 130)은 사용자 아이디를 키 발급 서버(110)로 전송하여 키 생성을 요청할 수 있다. 또한, 각 사용자 단말(120, 130)은 키 발급 서버(110)로부터 공개 파라미터 테이블과 사용자 아이디에 대응되는 비밀키를 수신할 수 있다.

[0045] 이때, 키 발급 서버(110)로부터 각 사용자 단말(120, 130)로 전송되는 비밀키는 각 사용자 단말(120, 130)로부터 전송된 사용자 아이디에 따라 상이한 값을 가질 수 있다. 반면, 키 발급 서버(110)로부터 각 사용자 단말(120, 130)로 전송되는 공개 파라미터 테이블은 각 사용자 단말(120, 130)로부터 전송된 사용자 아이디와 무관하게 동일할 수 있으며, 이에 따라, 각 사용자 단말(120, 130)은 동일한 공개 파라미터 테이블을 공유할 수 있다.

[0046] 한편, 키 발급 서버(110)로부터 비밀키 및 공개 파라미터 테이블을 수신한 각 사용자 단말(120, 130)은 수신된 비밀키 및 공개 파라미터 테이블을 이용하여 암복호화를 수행하거나, 전송될 데이터에 대한 전자 서명 및 전자 서명된 데이터에 대한 검증을 수행할 수 있다.

[0047] 예를 들어, 사용자 단말(120)은 사용자 단말(130)의 사용자 아이디를 수신하고, 공개 파라미터 테이블을 이용하여 수신된 사용자 아이디에 대응되는 공개키를 생성할 수 있다. 또한, 사용자 단말(120)은 생성된 공개키를 이용하여 데이터를 암호화한 후 사용자 단말(130)로 전송할 수 있다.

[0048] 이때, 사용자 단말(120)로부터 암호화된 데이터를 수신한 사용자 단말(130)은 키 발급 서버(110)로부터 수신된 비밀키를 이용하여 암호화된 데이터를 복호화할 수 있다.

[0049] 마찬가지로, 사용자 단말(130)은 사용자 단말(120)의 사용자 아이디를 수신하고, 공개 파라미터 테이블을 이용하여 수신된 사용자 아이디에 대응되는 공개키를 생성할 수 있다. 또한, 사용자 단말(130)은 생성된 공개키를 이용하여 데이터를 암호화한 후 사용자 단말(120)로 전송할 수 있다.

[0050] 이때, 사용자 단말(130)로부터 암호화된 데이터를 수신한 사용자 단말(120)은 키 발급 서버(110)로부터 수신된 비밀키를 이용하여 암호화된 데이터를 복호화할 수 있다.

[0051] 다른 예로, 사용자 단말(120)은 키 발급 서버(110)로부터 수신된 비밀키를 이용하여 데이터에 대한 전자 서명을 수행하고, 전자 서명된 데이터 및 사용자 단말(120)의 사용자 아이디를 사용자 단말(130)로 제공할 수 있다.

[0052] 이때, 사용자 단말(120)로부터 전자 서명된 데이터와 사용자 단말(120)의 사용자 아이디를 수신한 사용자 단말(130)은 공개 파라미터 테이블을 이용하여 수신된 사용자 아이디에 대응되는 공개키를 생성할 수 있다. 이후, 사용자 단말(130)은 생성된 공개키를 이용하여 수신된 전자 서명된 데이터에 대한 검증을 수행할 수 있다.

[0053] 마찬가지로, 사용자 단말(130)은 키 발급 서버(110)로부터 수신된 비밀키를 이용하여 데이터에 대한 전자 서명을 수행하고, 전자 서명된 데이터 및 사용자 단말(130)의 사용자 아이디를 사용자 단말(120)로 제공할 수 있다.

[0054] 이때, 사용자 단말(130)로부터 전자 서명된 데이터와 사용자 단말(130)의 사용자 아이디를 수신한 사용자 단말(120)은 공개 파라미터 테이블을 이용하여 수신된 사용자 아이디에 대응되는 공개키를 생성할 수 있다. 이후, 사용자 단말(120)은 생성된 공개키를 이용하여 수신된 전자 서명된 데이터에 대한 검증을 수행할 수 있다.

[0055] 도 2는 본 발명의 일 실시예에 따른 키 생성 장치의 구성도이다.

[0056] 도 2를 참조하면, 본 발명의 일 실시예에 따른 키 생성 장치(200)는 수신부(210), 비밀키 생성부(220) 및 키 정보 제공부(230)를 포함한다.

[0057] 본 발명의 일 실시예에서, 키 생성 장치(200)는 예를 들어, 도 1에 도시된 키 발급 서버(110)의 일 구성으로 구현될 수 있다.

[0058] 수신부(210)는 키 요청 단말(예를 들어, 도 1의 사용자 단말(120, 130))로부터 기 설정된 아이디 제약 조건에 따라 생성된 아이디를 포함하는 키 생성 요청을 수신한다.

[0059] 이때, 아이디 제약 조건은 아이디 생성 시 아이디가 만족하여야 하는 하나 이상의 규칙을 포함할 수 있으며, 암호화 서비스의 제공자에 의해 미리 설정될 수 있다. 구체적으로, 아이디 제약 조건은 예를 들어, 아이디를 구성하기 위해 이용할 수 있는 심볼의 종류(예를 들어, 영문 대문자, 영문 소문자, 숫자, 특수 문자 등) 및 아이디의 최대 자릿수를 포함할 수 있다. 그러나, 아이디 제약 조건은 반드시 상술한 예에 한정되는 것은 아니며, 예를 들어, 아이디의 최소 자릿수, 상이한 종류의 심볼들의 조합(예를 들어, 영문 대문자와 숫자의 조합) 등과 같

이 암호화 서비스의 정책에 따라 다양한 조건들이 추가될 수 있다.

[0060] 한편, 심볼은 컴퓨팅 장치를 이용하여 입력 가능한 모든 형태의 문자, 숫자, 기호, 특수 문자 등을 의미할 수 있다.

[0061] 키 요청 단말로부터 키 생성 요청이 수신된 경우, 비밀키 생성부(220)는 비밀 파라미터 테이블로부터, 수신된 아이디에 포함된 각 심볼들의 수신된 아이디 내 위치에 대응하는 비밀 파라미터 값들을 추출한다. 또한, 비밀키 생성부(220)는 추출된 비밀 파라미터 값들을 이용하여, 수신된 아이디에 대응하는 비밀키를 생성한다.

[0062] 이때, 비밀 파라미터 테이블은 아이디 제약 조건에 따라 이용 가능한 모든 심볼들 각각에 대한 아이디 내 위치별 비밀 파라미터 값을 포함할 수 있다. 비밀 파라미터 테이블에 대한 상세한 설명은 후술하기로 한다.

[0063] 한편, 본 발명의 일 실시예에 따르면, 수신된 아이디에 대응하는 비밀키는 추출된 비밀 파라미터 값들의 합을 이용하여 생성될 수 있다.

[0064] 구체적으로, 비밀키는 예를 들어, 아래의 수학식 1에 따라 생성될 수 있다.

[0065] [수학식 1]

$$Sk = \sum_{i=1}^{n} S_i \cdot R$$

[0066]

[0067] 이때, Sk는 비밀키, n은 수신된 아이디의 자릿수, S_i는 수신된 아이디 내 i 번째 위치의 심볼에 대응하는 비밀 파라미터 값, R은 임의의 난수를 나타낸다.

[0068] 한편, 본 발명의 다른 실시예에 따르면, 키 요청 단말로부터 키 생성 요청이 수신된 경우, 비밀키 생성부(220)는 수신된 아이디를 복수의 블록으로 분할하고, 비밀 파라미터 테이블로부터 수신된 아이디 내 각 심볼들의 각 블록 내 위치에 대응하는 비밀 파라미터 값들을 추출한다. 또한, 비밀키 생성부(220)는 추출된 비밀 파라미터 값들을 이용하여, 수신된 아이디에 대응하는 비밀키를 생성한다.

[0069] 이때, 수신된 아이디에 대응하는 비밀키는 추출된 비밀 파라미터 값들을 각 블록별로 합한 값들을 이용하여 생성될 수 있다.

[0070] 구체적으로, 비밀키는 예를 들어, 아래의 수학식 2에 따라 생성될 수 있다.

[0071] [수학식 2]

$$Sk = \sum_{k=1}^{m} (B_k) \cdot R_k$$

[0072]

[0073] 이때, Sk는 비밀키, m은 분할된 블록의 수, B_k는 k번째 블록에 대해 추출된 비밀 파라미터 값들의 합, R_k는 임의의 난수를 나타낸다.

[0074] 한편, 본 발명의 일 실시예에 따르면, 수학식 2에서, R_k는 B_k가 가질 수 있는 최대 비트 수의 k배 크기의 비트 수를 가지는 임의의 난수일 수 있다.

[0075] 구체적으로, 수학식 2에 따라 비밀키를 생성하는 경우, 비밀 파라미터 테이블에 포함된 비밀 파라미터들이 모두 상이한 값을 가지더라도, 상이한 아이디에 대해 추출된 비밀 파라미터들의 합이 동일한 경우가 발생할 수 있으며, 이 경우, 상이한 아이디에 대해 동일한 비밀키가 생성될 수 있다.

[0076] 반면, 수학식 2에서 R_k가 B_k가 가질 수 있는 최대 비트 수의 k배 크기의 비트 수를 가지는 임의의 난수인 경우, 상이한 아이디에 대해 동일한 비밀키가 생성되는 것을 방지할 수 있다.

[0077] 구체적으로, 비밀 파라미터 테이블에 포함된 각 비밀 파라미터 값들이 128 bit 크기를 가지며, 아이디를 4자리의 블록들로 분할하는 것으로 가정하면, 비밀 파라미터 테이블에서 추출된 비밀 파라미터 값들을 각 블록별로 합한 값(즉, B_k)들의 크기는 최대 130 bit가 된다. 따라서, Bk에 곱해지는 Rk는 130ㅅk의 비트 수를 가지는 임의의 난수가 된다.

[0078] 이 경우, 수학식 2에서 B_1에 곱해지는 난수인 R_1은 130 bit 크기의 난수이며, B_2에 곱해지는 난수인 R2는 260

bit 크기의 난수가 된다. 또한, Rk가 곱해짐에 따라 B_k 값이 k에 따라 상이한 bit 크기를 가지는 값이 되므로, 상이한 아이디에 대해 추출된 비밀 파라미터들의 합이 동일한 경우라도, 수학식 2에 따라 생성되는 비밀키는 상이하게 된다.

[0079] 한편, 키 정보 제공부(230)는 키 요청 단말로부터 수신된 아이디에 대한 비밀키가 생성된 경우, 생성된 비밀키를 키 요청 단말로 제공한다.

[0080] 한편, 일 실시예에서, 도 2에 도시된 수신부(210), 비밀키 생성부(220) 및 키 정보 제공부(230)는 하나 이상의 프로세서 및 그 프로세서와 연결된 컴퓨터 판독 가능 기록 매체를 포함하는 하나 이상의 컴퓨팅 장치 상에서 구현될 수 있다. 컴퓨터 판독 가능 기록 매체는 프로세서의 내부 또는 외부에 있을 수 있고, 잘 알려진 다양한 수단으로 프로세서와 연결될 수 있다. 컴퓨팅 장치 내의 프로세서는 각 컴퓨팅 장치로 하여금 본 명세서에서 기술되는 예시적인 실시예에 따라 동작하도록 할 수 있다. 예를 들어, 프로세서는 컴퓨터 판독 가능 기록 매체에 저장된 명령어를 실행할 수 있고, 컴퓨터 판독 가능 기록 매체에 저장된 명령어는 프로세서에 의해 실행되는 경우 컴퓨팅 장치로 하여금 본 명세서에 기술되는 예시적인 실시예에 따른 동작들을 수행하도록 구성될 수 있다.

[0081] 도 3은 본 발명의 추가적인 실시예에 따른 키 생성 장치의 구성도이다.

[0082] 도 3을 참조하면, 본 발명의 일 실시예에 따른 키 생성 장치(300)는 수신부(210), 비밀키 생성부(220), 키 정보 제공부(230), 비밀 파라미터 생성부(240), 비밀 파라미터 테이블 생성부(250), 공개 파라미터 생성부(260) 및 공개 파라미터 테이블 생성부(270) 를 포함한다.

[0083] 도 3에 도시된 실시예에서, 키 생성 장치(300)는 예를 들어, 도 1에 도시된 키 발급 서버(110)의 일 구성으로 구현될 수 있다.

[0084] 비밀 파라미터 생성부(240)는 기 설정된 아이디 제약 조건에 따라 아이디 생성을 위해 이용 가능한 모든 심볼(symbol)들에 대하여, 각 심볼의 아이디 내 위치별 비밀 파라미터 값을 생성한다. 본 발명의 일 실시예에 따르면, 비밀 파라미터 생성부(240)는 아이디 제약 조건에 따라 아이디 생성을 위해 이용 가능한 모든 심볼(symbol)들에 대하여, 각 심볼의 아이디 내 위치별로 대응되는 비밀 파라미터 값을 생성할 수 있다.

[0085] 예를 들어, 비밀 파라미터 생성부(240)는 아이디 제약 조건에 따라 이용 가능한 각 심볼에 대하여, 아이디 내 위치에 따라 임의의 값을 생성하고, 생성된 임의의 값을 AES 알고리즘으로 암호화하여 각 심볼의 아이디 내 특정 위치에 대응하는 비밀 파라미터를 생성할 수 있다.

[0086] 이때, 본 발명의 일 실시예에 따르면, 비밀 파라미터 생성부(240)는 아이디 제약 조건에 따라 생성 가능한 아이디의 최대 자릿수를 복수의 블록으로 분할한 후, 아이디 제약 조건에 따라 이용 가능한 모든 심볼들에 대하여, 각 심볼의 분할된 각 블록 내 위치별로 대응되는 비밀 파라미터 값을 생성할 수 있다.

[0087] 예를 들어, 아이디 제약 조건에 따른 아이디의 최대 자릿수가 24자리인 경우, 비밀 파라미터 생성부(240)는 24자리를 4개 자리씩 6개의 블록으로 분할할 수 있다. 또한, 비밀 파라미터 생생부(210)는 아이디 제약 조건에 따라 생성 가능한 모든 심볼들 각각에 대해 분할된 6개의 각 블록 내 위치에 대응되는 비밀 파라미터 값을 생성할 수 있다.

[0088] 한편, 본 발명의 일 실시예에 따르면, 비밀 파라미터 생성부(240)에 의해 생성되는 비밀 파라미터 값은 모두 상이할 수 있다.

[0089] 구체적으로, 비밀 파라미터 생성부(240)는 예를 들어, 아래 수학식 1에 따른 맵핑 함수를 이용하여, 각 심볼의 블록 내 위치에 따른 임의의 값을 생성할 수 있다.

[0090] [수학식 3]

$$\text{Mapping function} = [(x \parallel p) \ll ((i-1)*16) + r]$$

[0091]

[0092] 수학식 3은 분할된 블록 중 i번째 블록에서 특정 심볼(x)의 p번째 위치에 대한 맵핑 함수를 나타내며, r은 임의의 난수를 나타낸다.

[0093] 한편, 수학식 3에 따라 각 심볼의 블록 내 위치에 따른 임의의 값이 생성된 경우, 비밀 파라미터 생성부(240)는 생성된 각 임의의 값을 AES 알고리즘으로 암호화하여 각 심볼의 블록 내 위치에 따른 비밀 파라미터 값을 생성

할 수 있다.

[0094] 한편, 비밀 파라미터 생성부(240)에 의한 비밀 파라미터 값 생성 방식은 반드시 상술한 예에 한정되는 것은 아니며, 아이디 제약 조건에 따라 생성 가능한 각 심볼의 아이디 내 위치에 따라 상이한 값들을 생성할 수 있다면, 어떠한 방식이라도 이용 가능함을 유의하여야 한다.

[0095] 한편, 비밀 파라미터 테이블 생성부(250)는 비밀 파라미터 생성부(240)에서 생성된 비밀 파라미터 값들을 포함하는 비밀 파라미터 테이블을 생성한다.

[0096] 구체적으로, 비밀 파라미터 테이블 생성부(250)는 비밀 파라미터 생성부(240)에 의해 생성된 각 비밀 파라미터 값을 대응되는 심볼의 아이디 내 위치로 인덱싱하여 비밀 파라미터 테이블을 생성할 수 있다.

[0097] 구체적인 예로, 도 4는 비밀 파라미터 테이블의 일 예를 나타낸 예시도이다.

[0098] 도 4에 도시된 예에서, 아이디 제약 조건에 따라 사용자 아이디 생성을 위해 영문 대문자만이 이용 가능하며, 아이디의 최대 자릿 수는 i개인 것으로 가정한다.

[0099] 도시된 예에서, P_i는 아이디 내 심볼의 위치를 나타낸다. 구체적으로, P_1은 아이디 내 첫 번째 위치를 나타내며, P_2는 아이디 내 두 번째 위치를 나타낸다.

[0100] 또한, A_i 내지 Z_i는 각 심볼의 아이디 내 i 번째 위치에 대응되는 비밀 파라미터 값을 나타낸다. 예를 들어, A_1은 심볼 A가 아이디 내 첫 번째 자리에 위치한 경우에 대한 비밀 파라미터 값이며, B_1은 심볼 B가 아이디 내 첫 번째 자리에 위치한 경우에 대한 비밀 파라미터 값이다.

[0101] 도 5는 비밀 파라미터 테이블의 다른 예를 나타낸 예시도이다.

[0102] 도 5에 도시된 예에서, 아이디 제약 조건에 따라 사용자 아이디 생성을 위해 영문 대문자만이 이용 가능하며, 아이디의 최대 자릿수를 i개 자리씩 k개 블록으로 분할한 것으로 가정한다.

[0103] 도시된 예에서, P_i는 각 블록(Block 1 내지 Block k) 내 심볼의 위치를 나타낸다. 구체적으로, Block 1에서 P_1은 Block 1 내 첫 번째 위치를 나타내며, P_2는 Block 1 내 두 번째 위치를 나타낸다. 또한, Block 2에서 P_1은 Block 2 내 첫 번째 위치를 나타내며, P_2는 Block 2 내 두 번째 위치를 나타낸다.

[0104] 또한, A_{ki} 내지 Z_{ki}는 k 번째 블록 내에서 각 심볼의 i 번째 위치에 대응되는 비밀 파라미터 값을 나타낸다. 예를 들어, A_{11}은 심볼 A가 Block 1 내 첫 번째 자리에 위치한 경우에 대한 비밀 파라미터 값이며, B_{21}은 심볼 B가 Block 2 내 첫 번째 자리에 위치한 경우에 대한 비밀 파라미터 값이다.

[0105] 한편, 공개 파라미터 생성부(260)는 비밀 파라미터 생성부(240)에 의해 생성된 비밀 파라미터 값을 이용하여, 아이디 제약 조건에 따라 이용 가능한 모든 심볼에 대한 각 심볼의 아이디 내 위치별 공개 파라미터 값을 생성한다.

[0106] 구체적으로, 공개 파라미터 생성부(260)는 예를 들어, 아래의 수학식 4에 따라 각 심볼의 아이디 내 위치별 공개 파라미터 값을 생성할 수 있다.

[0107] [수학식 4]

$$P_{Xi} = g^{Xi \cdot R} (\mathrm{mod}\, N)$$

[0108]

[0109] 이때, P_{Xi}는 아이디 제약 조건에 따라 이용 가능한 특정 심볼의 아이디 내 i 번째 위치에 대응되는 공개 파라미터 값, Xi는 특정 심볼의 아이디 내 i 번째 위치에 대응되는 비밀 파라미터 값, R은 임의의 난수, g는 유한한 군 Z_N = {0, 1, 2, ..., N-1}의 최대 순환 부분군 G의 생성원, N은 N=pq를 만족하는 정수, p 및 q는 각각 $p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$를 만족하는 소수를 나타낸다. 이하, g, R 및 N은 동일한 의미로 사용된다.

[0110] 다른 예로, 비밀 파라미터 생성부(240)에서 생성되는 비밀 파라미터 값이 각 심볼의 분할된 블록 내 위치별 비밀 파라미터 값인 경우, 공개 파라미터 생성부(260)는 아래의 수학식 5에 따라 각 심볼의 분할된 블록 내 위치별 공개 파라미터 값을 생성할 수 있다.

[0111] [수학식 5]

$$P_{X_{ki}} = g^{X_{ki} \cdot R_k} (\mathrm{mod}\ N)$$

[0112]

[0113] 이때, $P_{X_{ki}}$ 는 아이디 제약 조건에 따라 이용 가능한 특정 심볼의 k번째 블록 내 i 번째 위치에 대응되는 공개 파라미터 값, X_{ki}는 특정 심볼의 k번째 블록 내 i 번째 위치에 대응되는 비밀 파라미터 값, R_k는 임의의 난수를 나타낸다.

[0114] 한편, 공개 파라미터 테이블 생성부(270)는 공개 파라미터 생성부(260)에서 생성된 공개 파라미터 값들을 포함하는 공개 파라미터 테이블을 생성한다.

[0115] 구체적으로, 공개 파라미터 테이블 생성부(270)는 공개 파라미터 생성부(260)에 의해 생성된 각 공개 파라미터 값을 대응되는 심볼의 아이디 내 위치로 인덱싱하여 공개 파라미터 테이블을 생성할 수 있다.

[0116] 구체적인 예로, 도 6은 공개 파라미터 테이블의 일 예를 나타낸 예시도이다.

[0117] 도 6에 도시된 예에서, 아이디 제약 조건에 따라 사용자 아이디 생성을 위해 영문 대문자만이 이용 가능하며, 아이디의 최대 자릿 수는 i개인 것으로 가정한다.

[0118] 도시된 예에서, P_i는 아이디 내 심볼의 위치를 나타낸다. 구체적으로, P_1은 아이디 내 첫 번째 위치를 나타내며, P_2는 아이디 내 두 번째 위치를 나타낸다.

[0119] 또한, $g^{Ai \cdot R}$ 내지 $g^{Zi \cdot R}$ 은 각 심볼의 i 번째 위치에 대응되는 공개 파라미터 값을 나타낸다. 예를 들어, $g^{A1 \cdot R}$ 은 심볼 A가 아이디 내 첫 번째 자리에 위치한 경우에 대한 공개 파라미터 값이며, $g^{B1 \cdot R}$ 은 심볼 B가 아이디 내 첫 번째 자리에 위치한 경우에 대한 공개 파라미터 값이다.

[0120] 도 7은 공개 파라미터 테이블의 다른 예를 나타낸 예시도이다.

[0121] 도 7에 도시된 예에서, 아이디 제약 조건에 따라 사용자 아이디 생성을 위해 영문 대문자만이 이용 가능하며, 아이디의 최대 자릿수를 i개 자리씩 k개 블록으로 분할한 것으로 가정한다.

[0122] 도시된 예에서, P_i는 각 블록(Block 1 내지 Block k) 내 심볼의 위치를 나타낸다. 구체적으로, Block 1에서 P_1은 Block 1 내 첫 번째 위치를 나타내며, P_2는 Block 1 내 두 번째 위치를 나타낸다. 또한, Block 2에서 P_1은 Block 2 내 첫 번째 위치를 나타내며, P_2는 Block 2 내 두 번째 위치를 나타낸다.

[0123] 또한, $g^{Aki \cdot Rk}$ 내지 $g^{Zki \cdot Rk}$ 는 k 번째 블록 내에서 각 심볼의 i 번째 위치에 대응되는 공개 파라미터 값을 나타낸다. 예를 들어, $g^{A11 \cdot R1}$ 은 심볼 A가 Block 1 내 첫 번째 자리에 위치한 경우에 대한 공개 파라미터 값이며, $g^{B21 \cdot R2}$는 심볼 B가 Block 2 내 첫 번째 자리에 위치한 경우에 대한 공개 파라미터 값이다.

[0124] 한편, 수신부(210)는 키 요청 단말(예를 들어, 도 1의 사용자 단말(120, 130))로부터 아이디 제약 조건에 따라 생성된 아이디를 포함하는 키 생성 요청을 수신한다.

[0125] 한편, 키 요청 단말로부터 키 생성 요청이 수신된 경우, 비밀키 생성부(220)는 비밀 파라미터 테이블로부터 수신된 아이디에 포함된 각 심볼들의 수신된 아이디 내 위치에 대응하는 비밀 파라미터 값들을 추출한다. 또한, 비밀키 생성부(220)는 추출된 비밀 파라미터 값들을 이용하여, 수신된 아이디에 대응하는 비밀키를 생성한다.

[0126] 이때, 본 발명의 일 실시예에 따르면, 수신된 아이디에 대응하는 비밀키는 추출된 비밀 파라미터 값들의 합을 이용하여 생성될 수 있다.

[0127] 구체적으로, 비밀키는 예를 들어, 상술한 수학식 1에 따라 생성될 수 있다.

[0128] 예를 들어, 비밀 파라미터 테이블 생성부(250)에 의해 생성된 비밀 파라미터 테이블이 도 4와 같다고 가정하면, 키 요청 단말로부터 수신된 아이디가 'ABCDEFGH'인 경우, 비밀 파라미터 테이블로부터 추출되는 비밀 파라미터 값들은 A_1, B_2, C_3, D_4, E_5, F_6, G_7, H_8이 된다.

[0129] 또한, 수신된 아이디 'ABCDEFGH'에 대한 비밀키(Sk)는 수학식 1에 따라 $(A_1+B_2+C_3+D_4+E_5+F_6+G_7+H_8)\times R$이 된다.

[0130] 한편, 본 발명의 다른 실시예에 따르면, 키 요청 단말로부터 키 생성 요청이 수신된 경우, 비밀키 생성부(220)는 수신된 아이디를 복수의 블록으로 분할하고, 비밀 파라미터 테이블로부터 수신된 아이디 내 각 심볼들의 각 블록 내 위치에 대응하는 비밀 파라미터 값들을 추출한다. 또한, 비밀키 생성부(220)는 추출된 비밀 파라미터 값들을 이용하여, 수신된 아이디에 대응하는 비밀키를 생성한다.

[0131] 이때, 수신된 아이디에 대응하는 비밀키는 추출된 비밀 파라미터 값들을 각 블록별로 합한 값들을 이용하여 생성될 수 있다.

[0132] 구체적으로, 비밀키는 예를 들어, 상술한 수학식 2에 따라 생성될 수 있다.

[0133] 예를 들어, 비밀 파라미터 테이블 생성부(250)에 의해 생성된 비밀 파라미터 테이블이 도 5와 같고 각 블록의 자릿수가 4(즉, i=4)인 것으로 가정하면, 키 요청 단말로부터 수신된 아이디가 'ABCDEFGH'인 경우, 비밀 파라미터 테이블로부터 추출되는 비밀 파라미터 값들은 A_{11}, B_{12}, C_{13}, D_{14}, E_{21}, F_{22}, G_{23}, H_{24}가 된다.

[0134] 즉, 비밀키 생성부(220)는 수신된 아이디'ABCDEFGH'를 4자리씩 분할하여 'ABCD'와 'EFGH'두 개의 블록으로 분할한 후, 비밀 파라미터 테이블의 Block 1으로부터 첫 번째 블록인'ABCD'에 대응되는 비밀 파라미터 값 A_{11}, B_{12}, C_{13}, D_{14}를 추출한다. 또한, 비밀키 생성부(220)는 비밀 파라미터 테이블의 Block 2으로부터 두 번째 블록인'EFGH'에 대응되는 비밀 파라미터 값 E_{21}, F_{22}, G_{23}, H_{24}를 추출한다.

[0135] 이 경우, 수신된 아이디 'ABCDEFGH'에 대한 비밀키(Sk)는 수학식 2에 따라 $(A_{11}+B_{12}+C_{13}+D_{14})R_1+(E_{21}+F_{22}+G_{23}+H_{24})R_2$이 된다.

[0136] 한편, 키 정보 제공부(230)는 키 요청 단말로부터 수신된 아이디에 대한 비밀키가 생성된 경우, 생성된 비밀키 및 공개 파라미터 테이블을 키 요청 단말로 제공한다.

[0137] 한편, 일 실시예에서, 도 3에 도시된 수신부(210), 비밀키 생성부(220), 키 정보 제공부(230), 비밀 파라미터 생성부(240), 비밀 파라미터 테이블 생성부(250), 공개 파라미터 생성부(260) 및 공개 파라미터 테이블 생성부(270)는 하나 이상의 프로세서 및 그 프로세서와 연결된 컴퓨터 판독 가능 기록 매체를 포함하는 하나 이상의 컴퓨팅 장치 상에서 구현될 수 있다. 컴퓨터 판독 가능 기록 매체는 프로세서의 내부 또는 외부에 있을 수 있고, 잘 알려진 다양한 수단으로 프로세서와 연결될 수 있다. 컴퓨팅 장치 내의 프로세서는 각 컴퓨팅 장치로 하여금 본 명세서에서 기술되는 예시적인 실시예에 따라 동작하도록 할 수 있다. 예를 들어, 프로세서는 컴퓨터 판독 가능 기록 매체에 저장된 명령어를 실행할 수 있고, 컴퓨터 판독 가능 기록 매체에 저장된 명령어는 프로세서에 의해 실행되는 경우 컴퓨팅 장치로 하여금 본 명세서에 기술되는 예시적인 실시예에 따른 동작들을 수행하도록 구성될 수 있다.

[0138] 도 8은 본 발명의 일 실시예에 따른 암호화 장치의 구성도이다.

[0139] 도 8을 참조하면, 본 발명의 일 실시예에 따른 암호화 장치(800)는 키 정보 획득부(810), 아이디 수신부(820), 공개키 생성부(830), 암호화부(840), 아이디 제공부(850), 데이터 수신부(860) 및 복호화부(870)를 포함한다.

[0140] 본 발명의 일 실시예에서, 암호화 장치(800)는 예를 들어, 도 1에 도시된 사용자 단말(120, 130)의 일 구성으로 구현될 수 있다.

[0141] 키 정보 획득부(810)는 아이디 제약 조건에 따라 생성된 암호화 장치(800)의 사용자 아이디를 포함한 키 생성 요청을 키 발급 서버(110)로 전송한다. 또한, 키 정보 획득부(810)는 키 발급 서버(110)로부터 공개 파라미터 테이블 및 암호화 장치(800)의 사용자 아이디에 대응되는 비밀키를 획득한다.

[0142] 이때, 키 발급 서버(110)로부터 획득되는 공개 파라미터 테이블 및 비밀키는 키 생성 장치(200)와 관련하여 이미 상술하였으므로, 이에 대한 상세한 설명은 생략한다.

[0143] 아이디 수신부(820)는 키 발급 서버(110)로부터 획득된 공개 파라미터 테이블을 공유하는 외부 단말로부터 아이디 제약 조건에 따라 생성된 외부 단말의 사용자 아이디를 수신한다.

[0144] 예를 들어, 도 1에 도시된 예에서, 각 사용자 장치(210, 220)는 키 발급 서버(110)로부터 동일한 공개 파라미터 테이블을 획득할 수 있다. 이 경우, 암호화 장치(800)가 사용자 장치(210)의 일 구성으로 구현된 경우, 외부 장

치는 사용자 장치(130)일 수 있다.

[0145] 공개키 생성부(830)는 키 발급 서버(110)로부터 획득된 공개 파라미터 테이블에서 외부 단말의 사용자 아이디에 포함된 각 심볼의 아이디 내 위치에 대응되는 공개 파라미터 값들을 추출한다. 또한, 공개키 생성부(830)는 추출된 공개 파라미터 값들을 이용하여 외부 단말의 사용자 아이디에 대응되는 공개키를 생성한다.

[0146] 이때, 본 발명의 일 실시예에 따르면, 공개키 생성부(830)는 추출된 공개 파라미터들의 곱을 이용하여 외부 단말의 사용자 아이디에 대응되는 공개키를 생성할 수 있다.

[0147] 예를 들어, 외부 단말의 사용자 아이디가 'ABCDEFGH'이고, 공개 파라미터 테이블이 도 6과 같다면, 공개 파라미터 테이블로부터 추출되는 공개 파라미터 값들은 $g^{A1\cdot R}$, $g^{B2\cdot R}$, $g^{C3\cdot R}$, $g^{D4\cdot R}$, $g^{E5\cdot R}$, $g^{F6\cdot R}$, $g^{G7\cdot R}$, $g^{H8\cdot R}$ 이 된다.

[0148] 또한, 추출된 공개 파라미터 값들로부터 생성되는 공개키(Pk)는 다음과 같다.

[0149] $Pk=g^{A1\cdot R}\times g^{B2\cdot R}\times g^{C3\cdot R}\times g^{D4\cdot R}\times g^{E5\cdot R}\times g^{F6\cdot R}\times g^{G7\cdot R}\times g^{H8\cdot R}$

[0150] $= g^{(A1+B2+C3+D4+E5+F6+G7+H8)\cdot R}$

[0151] 한편, 본 발명의 일 실시예에 따르면, 공개 파라미터 테이블이 도 7에 도시된 예와 같은 경우, 공개키 생성부(830)는 외부 단말의 사용자 아이디를 복수의 블록으로 분할하고, 공개 파라미터 테이블로부터 분할된 각 블록에 포함된 각 심볼의 블록 내 위치에 대응되는 공개 파라미터 값들을 추출한다.

[0152] 예를 들어, 도 7에 도시된 예에서, i가 4인 것으로 가정하면, 외부 단말의 사용자 아이디가 'ABCDEFGH'인 경우, 공개 파라미터 테이블로부터 추출되는 비밀 파라미터 값들은 $g^{A11\cdot R1}$, $g^{B12\cdot R1}$, $g^{C13\cdot R1}$, $g^{D14\cdot R1}$, $g^{E21\cdot R2}$, $g^{F22\cdot R2}$, $g^{G23\cdot R2}$, $g^{H24\cdot R2}$ 가 된다.

[0153] 즉, 공개키 생성부(830)는 외부 단말의 사용자 아이디 'ABCDEFGH'를 4자리씩 분할하여 'ABCD'와 'EFGH'두 개의 블록으로 분할한 후, 공개 파라미터 테이블의 Block 1으로부터 첫 번째 블록인'ABCD'에 대응되는 비밀 파라미터 값 $g^{A11\cdot R1}$, $g^{B12\cdot R1}$, $g^{C13\cdot R1}$, $g^{D14\cdot R1}$를 추출한다. 또한, 공개키 생성부(830)는 공개 파라미터 테이블의 Block 2으로부터 두 번째 블록인'EFGH'에 대응되는 비밀 파라미터 값 $g^{E21\cdot R2}$, $g^{F22\cdot R2}$, $g^{G23\cdot R2}$, $g^{H24\cdot R2}$ 를 추출한다.

[0154] 이 경우, 외부 단말의 사용자 아이디'ABCDEFGH'에 대한 공개키(Pk)는 다음과 같다.

[0155] $Pk=g^{A11\cdot R1}\times g^{B12\cdot R1}\times g^{C13\cdot R1}\times g^{D14\cdot R1}\times g^{E21\cdot R2}\times g^{F22\cdot R2}\times g^{G23\cdot R2}\times g^{H24\cdot R}$

[0156] $= g^{(A11+B12+C13+D14)\cdot R1+(E21+F22+G23+H24)\cdot R2}$

[0157] 암호화부(840)는 공개키 생성부(830)에서 생성된 외부 단말의 사용자 아이디에 대한 공개키를 이용하여 외부 단말로 전송할 데이터를 암호화한다.

[0158] 예를 들어, 암호화부(840)는 임의의 난수 t를 선택하고, 전송할 데이터 M에 대하여 다음과 같은 암호문 (C1, C2)를 계산할 수 있다.

[0159] $C1= g^{t} \pmod N$

[0160] $C2= Pk^{t} \pmod N \text{ XOR } M$

[0161] 한편, 실시예에 따라, 암호화부(840)는 키 정보 획득부(810)에서 획득된 비밀키를 이용하여 외부 단말로 전송할 데이터에 대한 전자 서명을 수행할 수 있다.

[0162] 아이디 제공부(850)는 아이디 제약 조건에 따라 생성된 암호화 장치(800)의 사용자 아이디를 외부 단말로 제공한다.

[0163] 데이터 수신부(860)는 외부 단말로부터 암호화 장치(800)의 사용자 아이디에 대응되는 공개키를 이용하여 암호화된 데이터 또는 외부 단말의 비밀키를 이용하여 전자 서명된 데이터를 수신한다.

[0164] 구체적으로, 암호화 장치(800)의 사용자 아이디를 수신한 외부 단말은 암호화 장치(800)와 공유하는 공개 파라미터 테이블을 이용하여 상술한 방식과 동일한 방식으로 공개키를 생성할 수 있으며, 생성된 공개키를 이용하여

데이터를 암호화한 후 암호화 장치(800)로 전송할 수 있다.

[0165] 복호화부(870)는 외부 단말로부터 암호화 장치(800)의 사용자 아이디에 대응되는 공개키를 이용하여 암호화된 데이터를 수신한 경우, 키 정보 획득부(810)에 의해 획득된 비밀키를 이용하여 암호화된 데이터를 복호화한다.

[0166] 예를 들어, 수신된 암호문이 C1, C2인 경우, 복호화부(870)는 키 정보 획득부(810)에 의해 획득된 비밀키(Sk)를 이용하여 다음과 같이 복호화할 수 있다.

[0167] $M= C1^{Sk} (mod\ N)\ XOR\ C2$

[0168] 한편, 복호화부(870)는 외부 단말의 비밀키를 이용하여 전자 서명된 데이터를 수신한 경우, 공개키 생성부(830)에서 생성된 외부 단말의 사용자 아이디에 대한 공개키를 이용하여 수신된 데이터에 대한 검증을 수행할 수 있다.

[0169] 한편, 일 실시예에서, 도 7에 도시된 키 정보 획득부(810), 아이디 수신부(820), 공개키 생성부(830), 암호화부(840), 아이디 제공부(850), 데이터 수신부(860) 및 복호화부(870)는 하나 이상의 프로세서 및 그 프로세서와 연결된 컴퓨터 판독 가능 기록 매체를 포함하는 하나 이상의 컴퓨팅 장치 상에서 구현될 수 있다. 컴퓨터 판독 가능 기록 매체는 프로세서의 내부 또는 외부에 있을 수 있고, 잘 알려진 다양한 수단으로 프로세서와 연결될 수 있다. 컴퓨팅 장치 내의 프로세서는 각 컴퓨팅 장치로 하여금 본 명세서에서 기술되는 예시적인 실시예에 따라 동작하도록 할 수 있다. 예를 들어, 프로세서는 컴퓨터 판독 가능 기록 매체에 저장된 명령어를 실행할 수 있고, 컴퓨터 판독 가능 기록 매체에 저장된 명령어는 프로세서에 의해 실행되는 경우 컴퓨팅 장치로 하여금 본 명세서에 기술되는 예시적인 실시예에 따른 동작들을 수행하도록 구성될 수 있다.

[0170] 도 9는 본 발명의 일 실시예에 따른 키 생성 방법의 순서도이다.

[0171] 도 9에 도시된 방법은 예를 들어, 도 2에 도시된 키 생성 장치(200)에 의해 수행될 수 있다.

[0172] 도 9를 참조하면, 키 생성 장치(200)는 우선, 키 요청 단말로부터 아이디 제약 조건에 따라 생성된 아이디를 포함하는 키 생성 요청을 수신한다(910).

[0173] 이후, 키 생성 장치(200)는 비밀 파라미터 테이블로부터 수신된 아이디에 포함된 각 심볼들의 수신된 아이디 내 위치에 대응하는 비밀 파라미터 값들을 추출한다(920).

[0174] 이후, 키 생성 장치(200)는 추출된 비밀 파라미터 값들을 이용하여 수신된 아이디에 대응하는 비밀키를 생성한다(930).

[0175] 이후, 키 생성 장치(200)는 생성된 비밀키를 키 요청 단말로 제공한다(940).

[0176] 도 10은 본 발명의 추가적인 실시예에 따른 키 생성 방법의 순서도이다.

[0177] 도 10에 도시된 방법은 예를 들어, 도 3에 도시된 키 생성 장치(300)에 의해 수행될 수 있다.

[0178] 도 10을 참조하면, 키 생성 장치(300)는 우선, 기 설정된 아이디 제약 조건에 따라 이용 가능한 모든 심볼들에 대하여, 각 심볼의 아이디 내 위치별 비밀 파라미터 값을 생성한다(1010).

[0179] 이후, 키 생성 장치(300)는 생성된 비밀 파라미터 값이 대응되는 심볼의 아이디 내 위치로 인덱싱된 비밀 파라미터 테이블을 생성한다(1020).

[0180] 이후, 키 생성 장치(300)는 생성된 비밀 파라미터 값을 이용하여, 아이디 제약 조건에 따라 이용 가능한 모든 심볼들에 대한 각 심볼의 아이디 내 위치별 공개 파라미터 값을 생성한다(1030).

[0181] 이후, 키 생성 장치(300)는 생성된 공개 파라미터 값이 대응되는 심볼의 아이디 내 위치로 인덱싱된 공개 파라미터 테이블을 생성한다(1040).

[0182] 이후, 키 생성 장치(300)는 키 요청 단말로부터 아이디 제약 조건에 따라 생성된 아이디를 포함하는 키 생성 요청을 수신한다(1050).

[0183] 이후, 키 생성 장치(300)는 비밀 파라미터 테이블로부터 수신된 아이디에 포함된 각 심볼들의 수신된 아이디 내 위치에 대응하는 비밀 파라미터 값들을 추출한다(1060).

[0184] 이후, 키 생성 장치(300)는 추출된 비밀 파라미터 값들을 이용하여 수신된 아이디에 대응하는 비밀키를 생성한다(1070).

[0185] 이후, 키 생성 장치(300)는 생성된 비밀키 및 공개 파라미터 테이블을 키 요청 단말로 제공한다(1080).

[0186] 도 11은 본 발명의 일 실시예에 따른 암호화 과정을 나타낸 순서도이다.

[0187] 도 11에 도시된 방법은 예를 들어, 도 8에 도시된 암호화 장치(800)에 의해 수행될 수 있다.

[0188] 도 11을 참조하면, 암호화 장치(800)는 우선, 기 설정된 아이디 제약 조건에 따라 생성된 암호화 장치(800)의 사용자 아이디를 포함한 키 생성 요청을 키 발급 서버(110)로 전송한다(1110).

[0189] 이후, 암호화 장치(800)는 키 발급 서버(110)로부터 아이디 제약 조건에 따라 생성 가능한 모든 심볼들에 대한 아이디 내 위치별 공개 파라미터 값을 포함하는 공개 파라미터 테이블 및 암호화 장치(800)의 사용자 아이디에 대응되는 비밀키를 획득한다(1120).

[0190] 이후, 암호화 장치(800)는 공개 파라미터 테이블을 공유하는 외부 단말로부터 아이디 제약 조건에 따라 생성된 외부 단말의 사용자 아이디를 수신한다(1130).

[0191] 이후, 암호화 장치(800)는 공개 파라미터 테이블로부터 외부 단말의 사용자 아이디에 포함된 각 심볼의 아이디 내 위치에 대응되는 공개 파라미터 값들을 추출한다(1140).

[0192] 이후, 암호화 장치(800)는 추출된 공개 파라미터 값들을 이용하여 외부 단말의 사용자 아이디에 대응되는 공개키를 생성한다(1150).

[0193] 이후, 암호화 장치(800)는 생성된 공개키를 이용하여 외부 단말로 전송할 데이터를 암호화한다(1160).

[0194] 도 12는 본 발명의 일 실시예에 따른 복호화 과정을 나타낸 순서도이다.

[0195] 도 12에 도시된 방법은 예를 들어, 도 8에 도시된 암호화 장치(800)에 의해 수행될 수 있다.

[0196] 도 12를 참조하면, 암호화 장치(800)는 우선, 기 설정된 아이디 제약 조건에 따라 생성된 암호화 장치(800)의 사용자 아이디를 포함한 키 생성 요청을 키 발급 서버(110)로 전송한다(1210).

[0197] 이후, 암호화 장치(800)는 아이디 제약 조건에 따라 생성 가능한 모든 심볼들에 대한 아이디 내 위치별 공개 파라미터 값을 포함하는 공개 파라미터 테이블 및 암호화 장치(800)의 사용자 아이디에 대응되는 비밀키를 획득한다(1220).

[0198] 이후, 암호화 장치(800)는 공개 파라미터 테이블을 공유하는 외부 단말로 암호화 장치(800)의 사용자 아이디를 제공한다(1230).

[0199] 이후, 암호화 장치(800)는 외부 단말로부터 암호화 장치(800)의 사용자 아이디에 대응되는 공개키를 이용하여 암호화된 데이터를 수신한다(1240).

[0200] 이후, 암호화 장치(800)는 1220 단계에서 획득된 비밀키를 이용하여 수신된 암호화된 데이터를 복호화한다(1250).

[0201] 도 13은 본 발명의 일 실시예에 따른 전자 서명 수행 과정을 나타낸 순서도이다.

[0202] 도 13에 도시된 방법은 예를 들어, 도 8에 도시된 암호화 장치(800)에 의해 수행될 수 있다.

[0203] 도 13을 참조하면, 암호화 장치(800)는 우선, 기 설정된 아이디 제약 조건에 따라 생성된 암호화 장치(800)의 사용자 아이디를 포함한 키 생성 요청을 키 발급 서버(110)로 전송한다(1310).

[0204] 이후, 암호화 장치(800)는 아이디 제약 조건에 따라 생성 가능한 모든 심볼들에 대한 아이디 내 위치별 공개 파라미터 값을 포함하는 공개 파라미터 테이블 및 암호화 장치(800)의 사용자 아이디에 대응되는 비밀키를 획득한다(1320).

[0205] 이후, 암호화 장치(800)는 획득된 비밀키를 이용하여 공개 파라미터 테이블을 공유하는 외부 장치로 전송할 데이터에 대한 전자 서명을 수행한다(1330).

[0206] 도 14는 본 발명의 일 실시예에 따른 전자 서명된 데이터에 대한 검증 과정을 나타낸 순서도이다.

[0207] 도 14에 도시된 방법은 예를 들어, 도 8에 도시된 암호화 장치(800)에 의해 수행될 수 있다.

[0208] 도 14를 참조하면, 암호화 장치(800)는 우선, 기 설정된 아이디 제약 조건에 따라 생성된 암호화 장치(800)의 사용자 아이디를 포함한 키 생성 요청을 키 발급 서버(110)로 전송한다(1410).

[0209] 이후, 암호화 장치(800)는 아이디 제약 조건에 따라 생성 가능한 모든 심볼들에 대한 아이디 내 위치별 공개 파라미터 값을 포함하는 공개 파라미터 테이블 및 암호화 장치(800)의 사용자 아이디에 대응되는 비밀키를 획득한다(1420).

[0210] 이후, 암호화 장치(800)는 공개 파라미터 테이블을 공유하는 외부 단말로부터 아이디 제약 조건에 따라 생성된 외부 단말의 사용자 아이디를 수신한다(1430).

[0211] 이후, 암호화 장치(800)는 공개 파라미터 테이블로부터 외부 단말의 사용자 아이디에 포함된 각 심볼의 아이디 내 위치에 대응되는 공개 파라미터 값들을 추출한다(1440).

[0212] 이후, 암호화 장치(800)는 추출된 공개 파라미터 값들을 이용하여 외부 단말의 사용자 아이디에 대응되는 공개키를 생성한다(1450).

[0213] 이후, 암호화 장치(800)는 외부 단말로부터 외부 단말의 비밀키를 이용하여 전자 서명된 데이터를 수신한다(1460).

[0214] 이후, 암호화 장치(800)는 외부 단말의 사용자 아이디에 대응되는 공개키를 이용하여 수신된 전자 서명된 데이터에 대한 검증을 수행한다(1470).

[0215] 한편, 도 9 내지 도 14에 도시된 순서도에서는 상기 방법을 복수 개의 단계로 나누어 기재하였으나, 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 부가되어 수행될 수 있다.

[0216] 한편, 본 발명의 실시예는 본 명세서에서 기술한 방법들을 컴퓨터상에서 수행하기 위한 프로그램을 포함하는 컴퓨터 판독 가능 기록매체를 포함할 수 있다. 상기 컴퓨터 판독 가능 기록매체는 프로그램 명령, 로컬 데이터 파일, 로컬 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체는 본 발명을 위하여 특별히 설계되고 구성된 것들이거나, 또는 컴퓨터 소프트웨어 분야에서 통상적으로 사용 가능한 것일 수 있다. 컴퓨터 판독 가능 기록매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD와 같은 광 기록 매체, 플로피 디스크와 같은 자기-광 매체, 및 롬, 램, 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 포함할 수 있다.

[0217] 이상에서 본 발명의 대표적인 실시예들을 상세하게 설명하였으나, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 상술한 실시예에 대하여 본 발명의 범주에서 벗어나지 않는 한도 내에서 다양한 변형이 가능함을 이해할 것이다. 그러므로 본 발명의 권리범위는 설명된 실시예에 국한되어 정해져서는 안 되며, 후술하는 특허청구범위뿐만 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

부호의 설명

[0218] 100: 암호화 시스템

110: 키 발급 서버

120, 130: 사용자 단말

200, 300: 키 생성 장치

210: 수신부

220: 비밀키 생성부

230: 키 정보 제공부

240: 비밀 파라미터 생성부

250: 비밀 파라미터 테이블 생성부

260: 공개 파라미터 생성부

270: 공개 파라미터 테이블 생성부

800: 암호화 장치

810: 키 정보 획득부

820: 아이디 수신부

830: 공개키 생성부

840: 암호화부

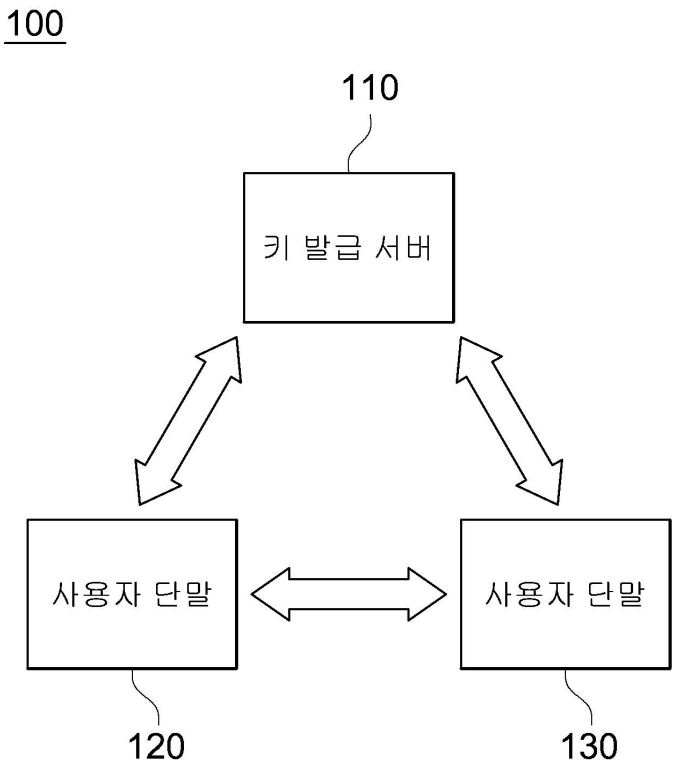
850: 아이디 제공부

860: 데이터 수신부

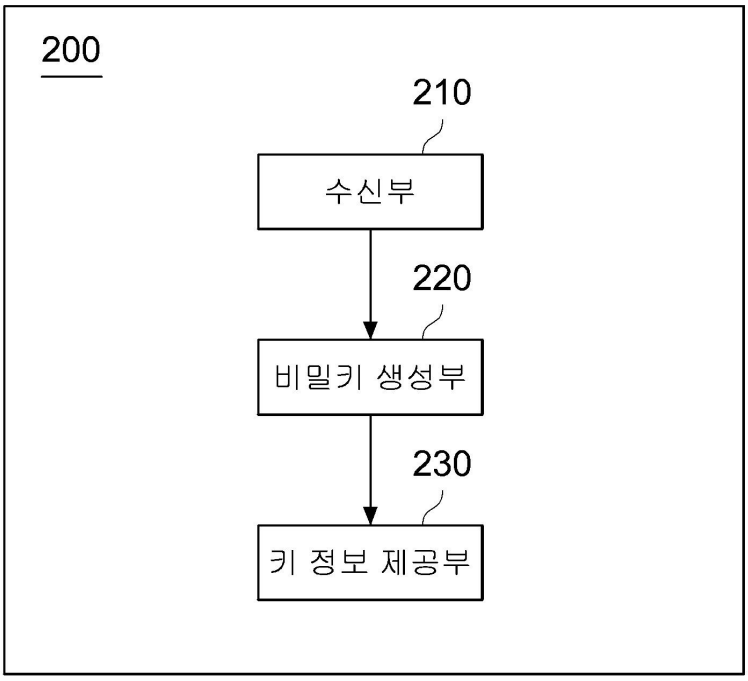
870: 복호화부

도면

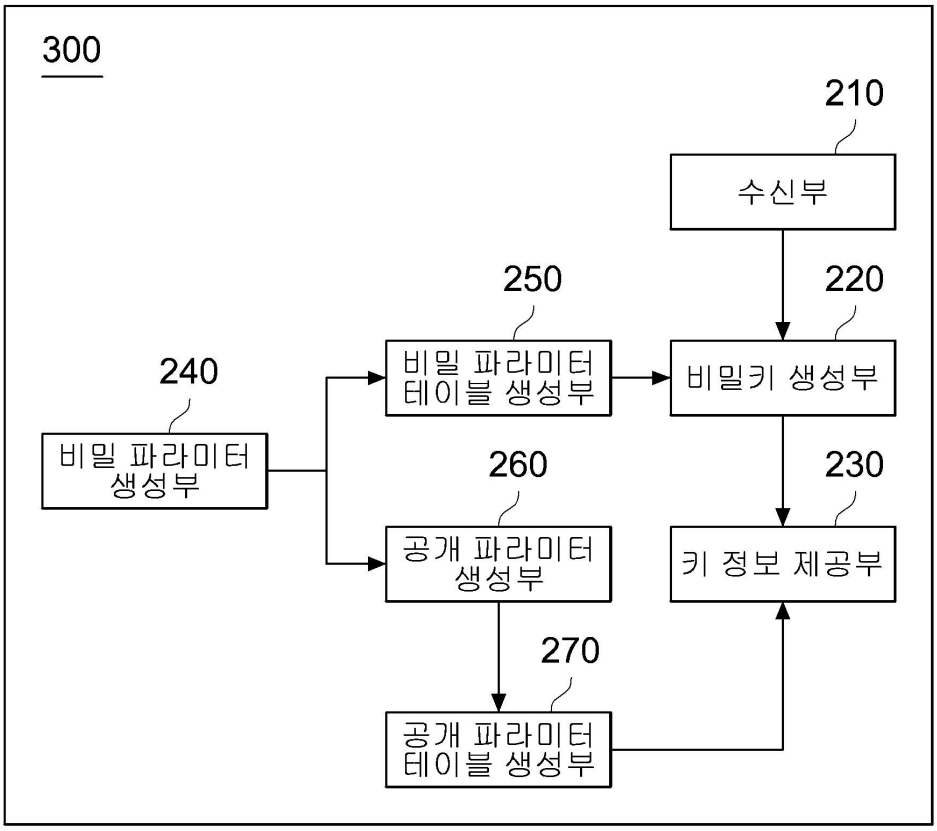
도면1



도면2



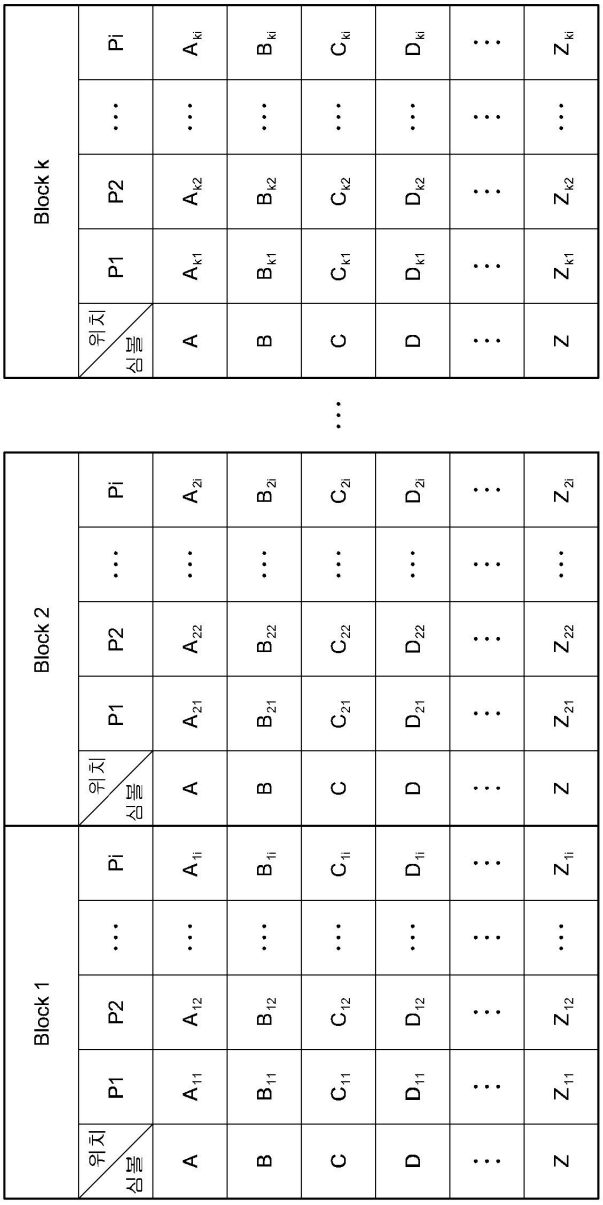
도면3


300
210
수신부
250
220
240
비밀 파라미터 테이블 생성부
비밀키 생성부
비밀 파라미터 생성부
260
230
공개 파라미터 생성부
키 정보 제공부
270
공개 파라미터 테이블 생성부

도면4

위치 / 심볼	P1	P2	P3	P3	···	P_i
A	A_1	A_2	A_3	A_4	···	A_i
B	B_1	B_2	B_3	B_4	···	B_i
C	C_1	C_2	C_3	C_4	···	C_i
D	D_1	D_2	D_3	D_4	···	D_i
⋮	⋮	⋮	⋮	⋮	⋮	⋮
Z	Z_1	Z_2	Z_3	Z_4	···	Z_i

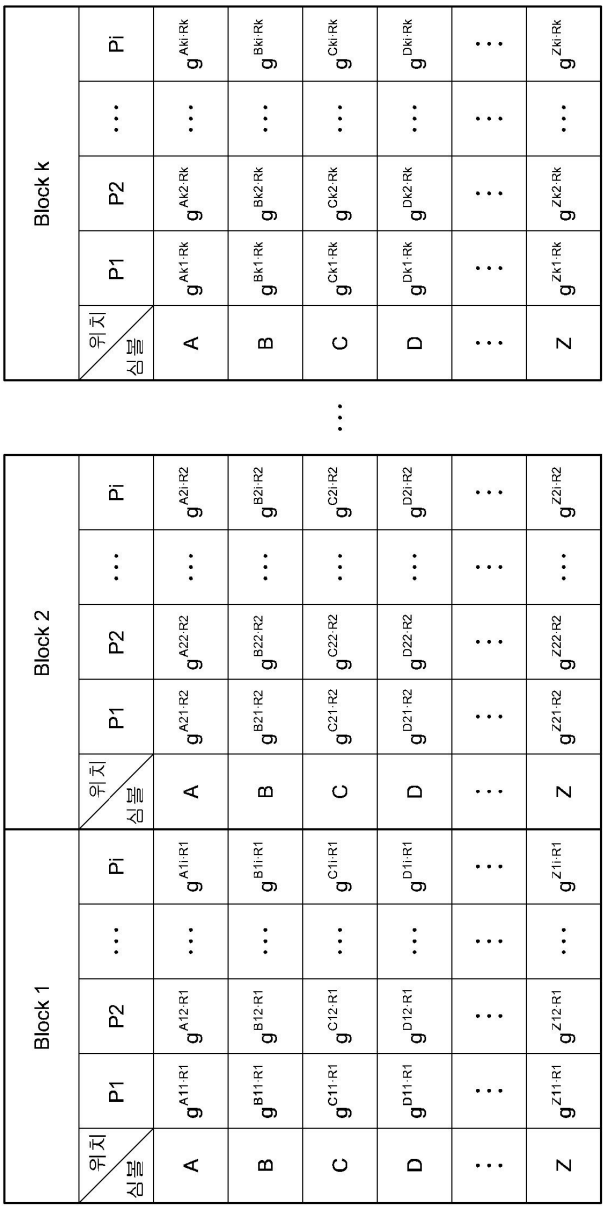
도면5



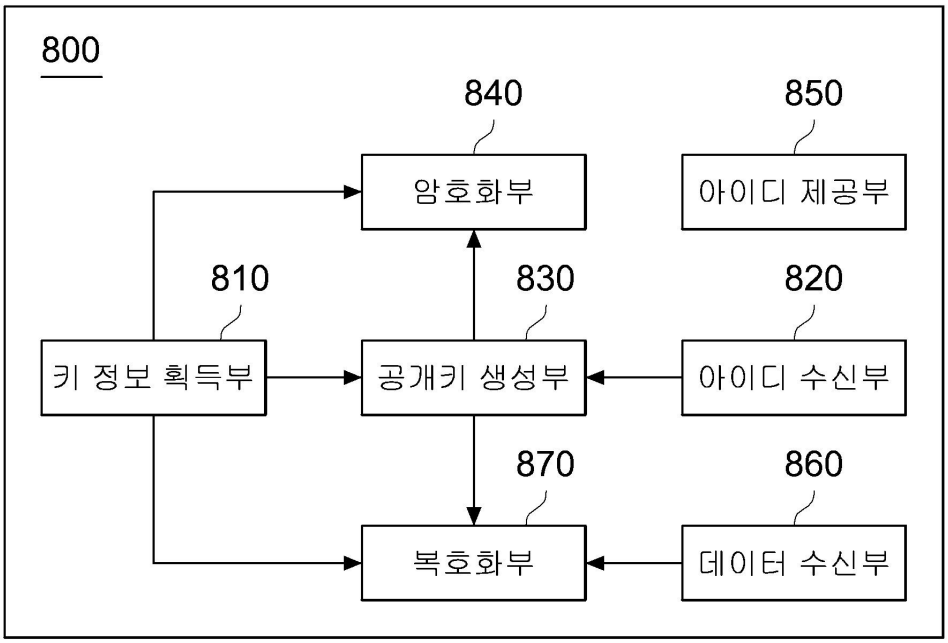
도면6

위치 / 심볼	P1	P2	P3	P3	···	P_i
A	$g^{A1\cdot R}$	$g^{A2\cdot R}$	$g^{A3\cdot R}$	$g^{A4\cdot R}$	···	$g^{Ai\cdot R}$
B	$g^{B1\cdot R}$	$g^{B2\cdot R}$	$g^{B3\cdot R}$	$g^{B4\cdot R}$	···	$g^{Bi\cdot R}$
C	$g^{C1\cdot R}$	$g^{C2\cdot R}$	$g^{C3\cdot R}$	$g^{C4\cdot R}$	···	$g^{Ci\cdot R}$
D	$g^{D1\cdot R}$	$g^{D2\cdot R}$	$g^{D3\cdot R}$	$g^{D4\cdot R}$	···	$g^{Di\cdot R}$
⋮	⋮	⋮	⋮	⋮	⋮	⋮
Z	$g^{Z1\cdot R}$	$g^{Z2\cdot R}$	$g^{Z3\cdot R}$	$g^{Z4\cdot R}$	···	$g^{Zi\cdot R}$

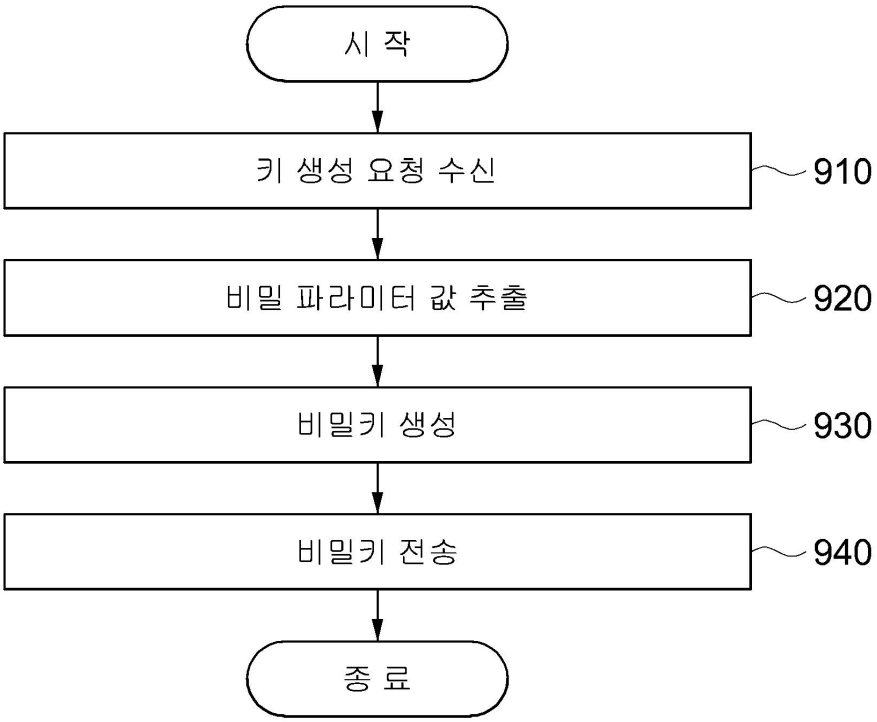
도면7



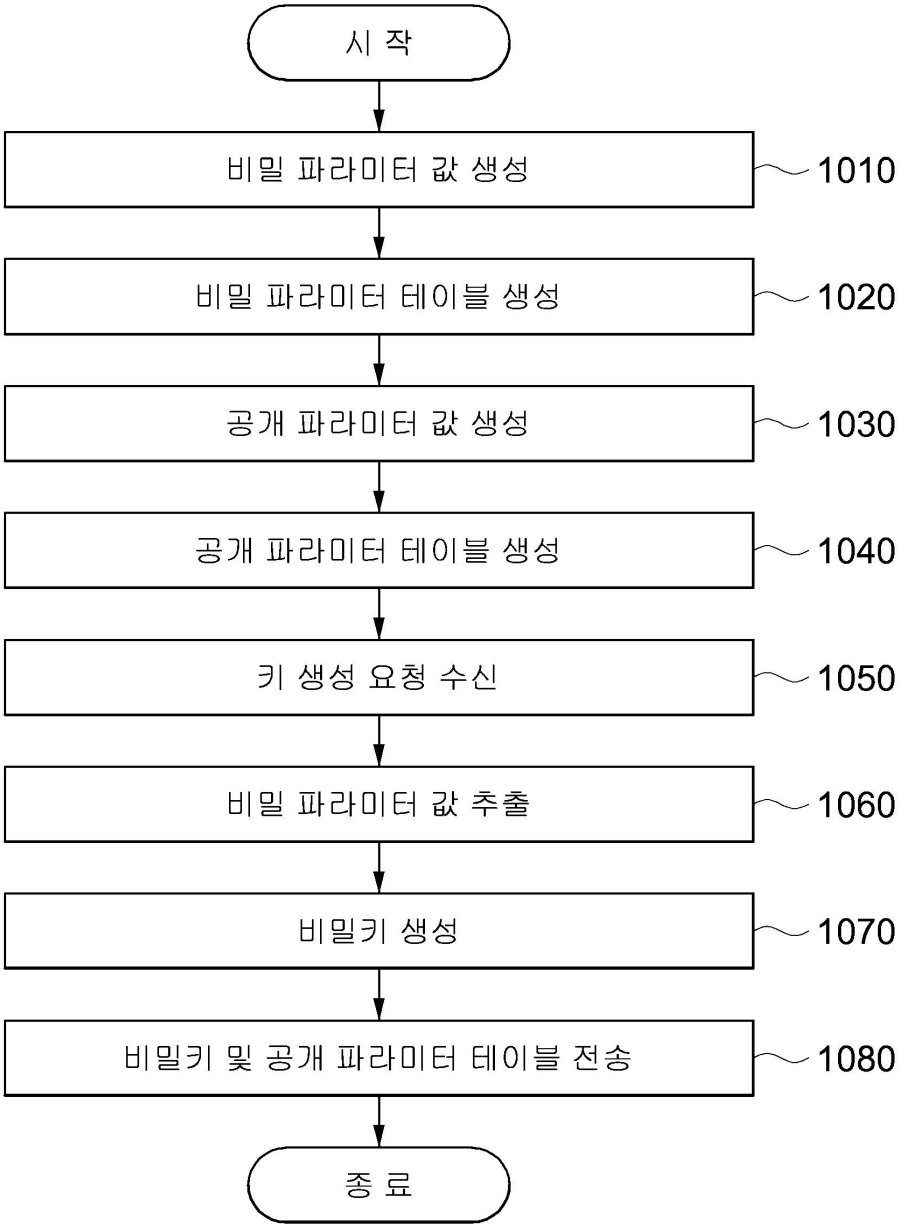
도면8


800
840
850
암호화부
아이디 제공부
810
830
820
키 정보 획득부
공개키 생성부
아이디 수신부
870
860
복호화부
데이터 수신부

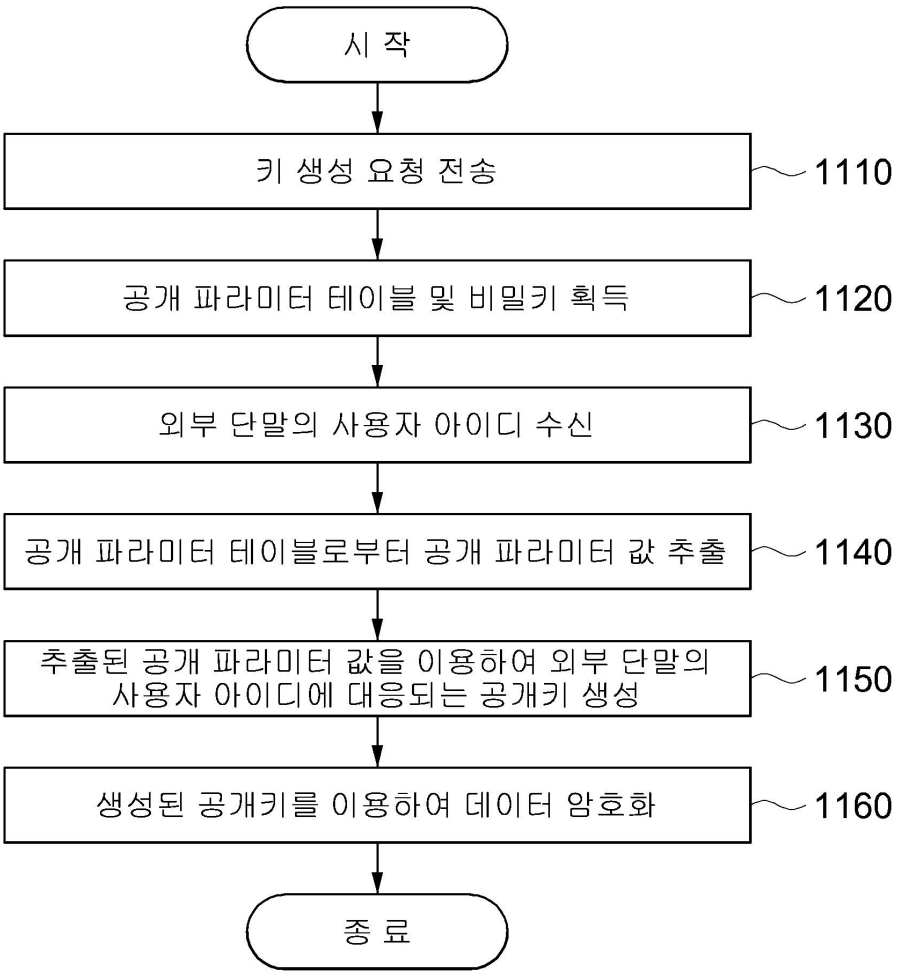
도면9


시 작
키 생성 요청 수신
910
비밀 파라미터 값 추출
920
비밀키 생성
930
비밀키 전송
940
종 료

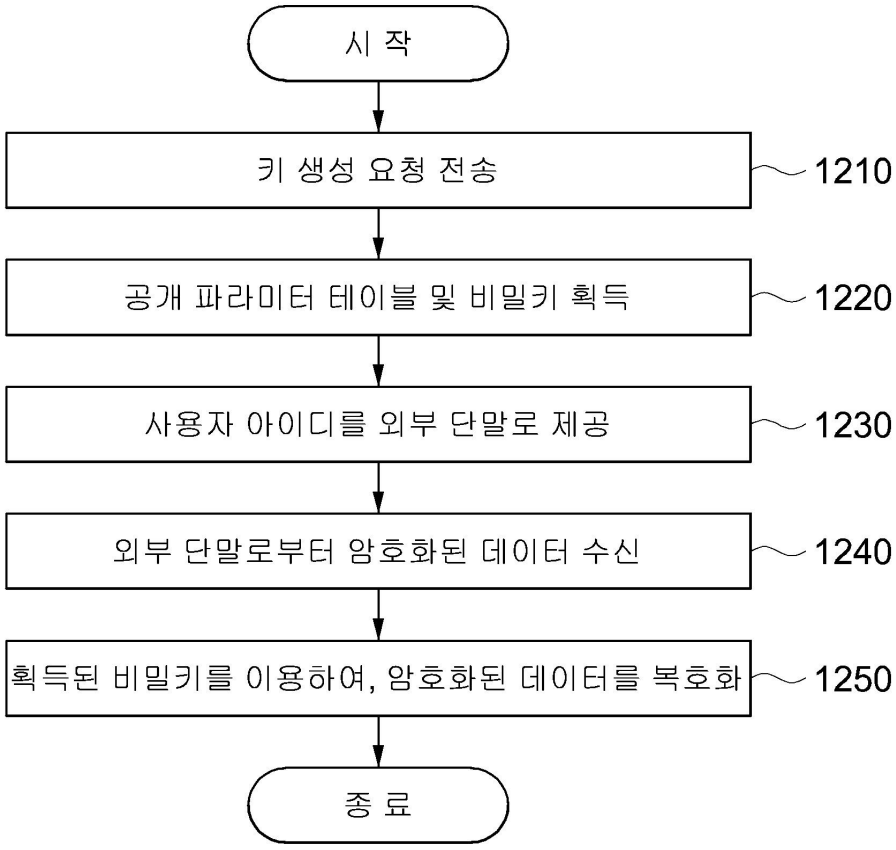
도면10


시 작
비밀 파라미터 값 생성
1010
비밀 파라미터 테이블 생성
1020
공개 파라미터 값 생성
1030
공개 파라미터 테이블 생성
1040
키 생성 요청 수신
1050
비밀 파라미터 값 추출
1060
비밀키 생성
1070
비밀키 및 공개 파라미터 테이블 전송
1080
종 료

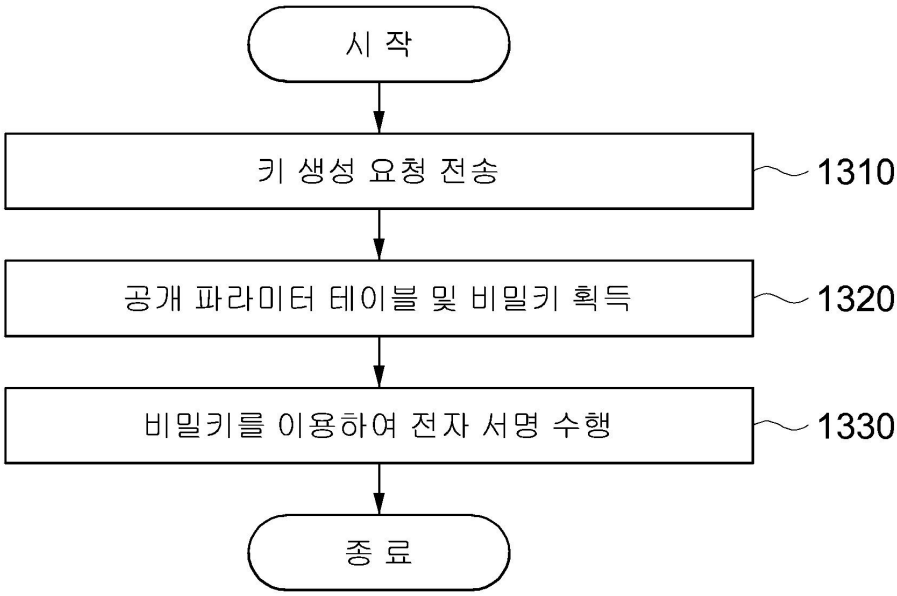
도면11


시 작
키 생성 요청 전송
1110
공개 파라미터 테이블 및 비밀키 획득
1120
외부 단말의 사용자 아이디 수신
1130
공개 파라미터 테이블로부터 공개 파라미터 값 추출
1140
추출된 공개 파라미터 값을 이용하여 외부 단말의 사용자 아이디에 대응되는 공개키 생성
1150
생성된 공개키를 이용하여 데이터 암호화
1160
종 료

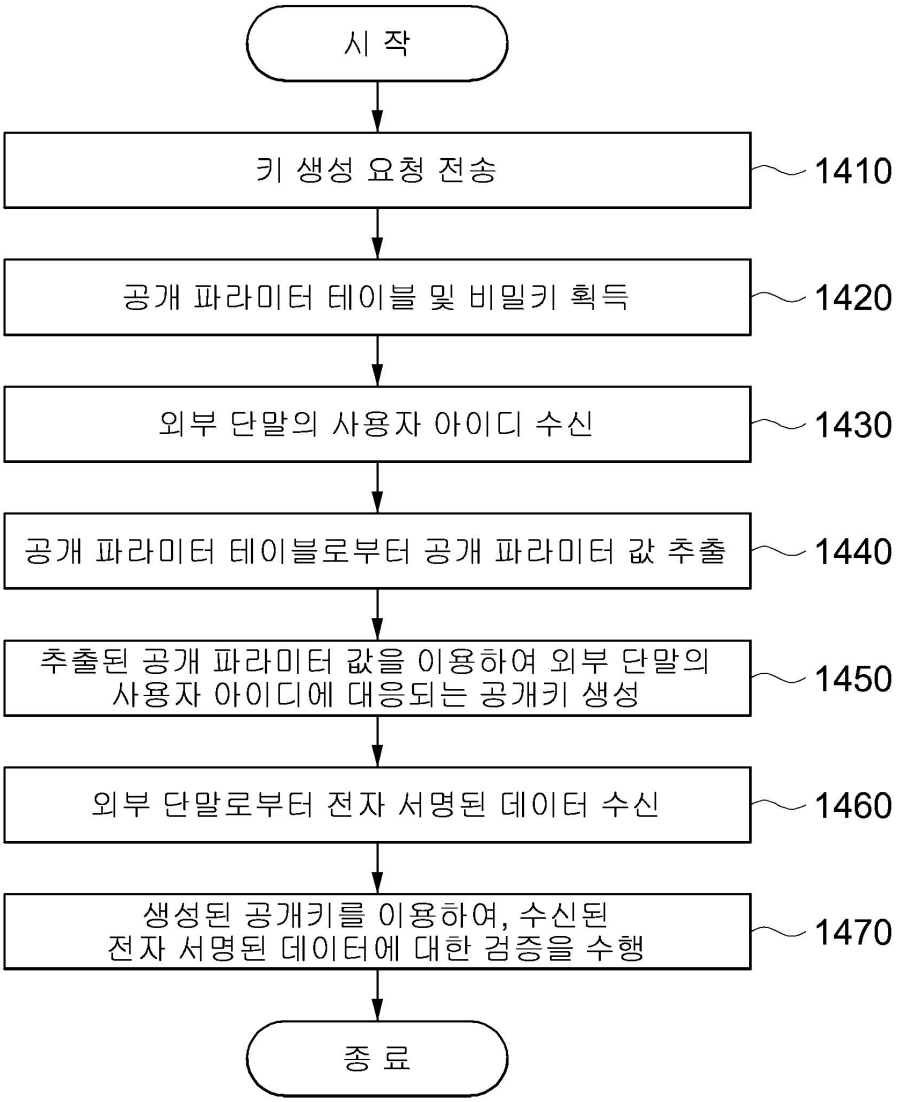
도면12


시 작
키 생성 요청 전송
1210
공개 파라미터 테이블 및 비밀키 획득
1220
사용자 아이디를 외부 단말로 제공
1230
외부 단말로부터 암호화된 데이터 수신
1240
획득된 비밀키를 이용하여, 암호화된 데이터를 복호화
1250
종 료

도면13


시 작
키 생성 요청 전송
1310
공개 파라미터 테이블 및 비밀키 획득
1320
비밀키를 이용하여 전자 서명 수행
1330
종 료

도면14


시 작
키 생성 요청 전송
1410
공개 파라미터 테이블 및 비밀키 획득
1420
외부 단말의 사용자 아이디 수신
1430
공개 파라미터 테이블로부터 공개 파라미터 값 추출
1440
추출된 공개 파라미터 값을 이용하여 외부 단말의 사용자 아이디에 대응되는 공개키 생성
1450
외부 단말로부터 전자 서명된 데이터 수신
1460
생성된 공개키를 이용하여, 수신된 전자 서명된 데이터에 대한 검증을 수행
1470
종 료