(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2016-0042701
(43) 공개일자 2016년04월20일

(51) 국제특허분류(Int. Cl.)
H04L 9/12 (2006.01) *H04L 9/30* (2006.01)
(21) 출원번호 10-2014-0136966
(22) 출원일자 2014년10월10일
심사청구일자 없음

(71) 출원인
삼성전자주식회사
경기도 수원시 영통구 삼성로 129 (매탄동)
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
임정환
경기도 화성시 동탄중앙로 189, 334동 1802호 (반송동,
시범다은마을월드메르디앙반도유보라아파트)
박종환
서울특별시 종로구 홍지문2길 20 (홍지동)
(뒷면에 계속)
(74) 대리인
리앤목특허법인

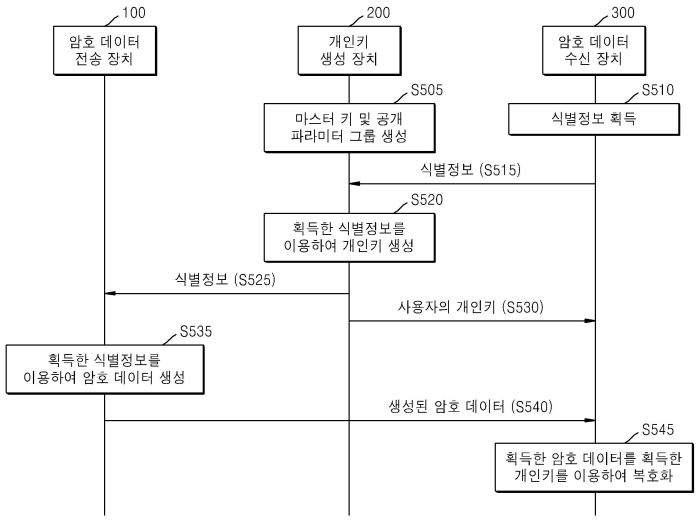
전체 청구항 수 : 총 14 항

(54) 발명의 명칭 **식별 정보 기반 암호화 방법 및 장치**

(57) 요 약

개인키 생성 장치가 복수의 파라미터가 포함된 마스터 키 및 복수의 공개 파라미터를 포함하는 공개 파라미터 그룹을 설정하는 단계, 상기 키 생성 장치가 암호 데이터 수신 장치의 식별 정보를 수신하여, 상기 마스터 키에 포함된 파라미터를 밑수로 포함하고, 상기 획득한 식별 정보를 이용하여 생성된 해쉬 함수값을 지수로 포함하는 승수 인자를 생성하며, 상기 생성된 승수 인자를 이용하여 개인키를 생성하고, 상기 생성된 개인키를 암호 데이터 수신 장치에 전송하는 단계, 암호 데이터 전송 장치가 상기 식별 정보를 수신하고, 상기 식별 정보에 기초하여 메시지를 암호화하여 암호 데이터를 생성하고, 상기 생성한 암호 데이터를 상기 암호 데이터 수신 장치에 전송하는 단계, 상기 암호 데이터 수신 장치가 상기 암호 데이터 및 상기 비밀키를 수신하여, 상기 수신한 비밀키에 기초하여 상기 암호 데이터를 복호화하여 상기 메시지를 획득하는 단계를 포함하는 암호 시스템이 개시된다.

대 표 도 - 도5



(72) 발명자

이동훈

서울특별시 성북구 안암로 145, 미래융합관 612호 (안암동5가)

이덕기

서울특별시 서초구 신반포로3길 19, 56동 505호 (반포동)

명 세 서

청구범위

청구항 1

암호 데이터 전송 방법에 있어서,

암호화 될 메시지 및 암호 데이터 수신 장치의 식별 정보를 획득하는 단계;

상기 획득한 메시지 및 임의의 수를 이용하여 제 1 암호 데이터를 생성하는 단계;

키생성 장치에 의해 설정된 공개 파라미터들중 하나를 밑수로 포함하고, 상기 획득한 식별 정보를 이용하여 생성된 해쉬 함수값을 지수에 포함하는 승수 인자를 생성하고, 상기 생성된 승수 인자에 기초하여 제 2 암호 데이터를 생성하는 단계;

상기 임의의 수를 이용하여 제 3 암호 데이터를 생성하는 단계;

상기 생성된 제 1 암호 데이터, 제 2 암호 데이터, 및 제 3 암호 데이터를 상기 암호 데이터 수신 장치에 전송하는 단계;

를 포함하는 암호 데이터 전송 방법.

청구항 2

제 1 항에 있어서,

상기 제 2 암호 데이터에 포함된 승수 인자들이 포함하는 밑수들은 동일한 곱셈군에 포함되는 것을 특징으로 하는 암호 데이터 전송 방법.

청구항 3

제 2 항에 있어서 상기 제 3 암호 데이터는

상기 곱셈군에 포함된 파라미터를 밑수로 포함하고, 상기 임의의 수를 지수에 포함하는 것을 특징으로 하는 암호 데이터 전송 방법.

청구항 4

암호화 될 메시지 및 암호 데이터 수신 장치의 식별 정보를 획득하는 정보 획득부;

상기 획득한 메시지 및 임의의 수를 이용하여 제 1 암호 데이터를 생성하고, 키생성 디바이스에 의해 설정된 공개 파라미터들중 하나를 밑수로 포함하고, 상기 식별 정보에 기초하여 생성된 해쉬 함수값을 지수에 포함하는 승수 인자를 생성하여, 상기 생성된 승수 인자를 포함하는 제 2 암호 데이터를 생성하고, 상기 임의의 수를 이용하여 제 3 암호 데이터를 생성하는 암호 데이터 생성부

상기 생성된 제 1 암호 데이터, 제 2 암호 데이터,및 제 3 암호 데이터를 상기 암호 데이터 수신 장치에 전송하는 암호 데이터 전송부;

를 포함하는 암호 데이터 전송 장치.

청구항 5

제 4 항에 있어서,

상기 제 2 암호 데이터에 포함된 승수 인자들이 포함하는 밑수들은 동일한 곱셈군에 포함되는 것을 특징으로 하는 암호 데이터 전송 장치.

청구항 6

제 5 항에 있어서 상기 제 3 암호 데이터는

상기 곱셈군에 포함된 파라미터를 밑수로 포함하고, 상기 임의의 수를 지수에 포함하는 것을 특징으로 하는 암호 데이터 전송 장치.

청구항 7

개인키 생성 방법에 있어서,

복수의 파라미터가 포함된 마스터 키 및 복수의 공개 파라미터를 포함하는 공개 파라미터 그룹을 생성하는 단계;

암호 데이터 수신 장치의 식별 정보를 획득하는 단계;

상기 마스터 키에 포함된 파라미터들중 하나를 밑수로 포함하고, 상기 식별 정보에 기초하여 생성된 해쉬 함수 값을 지수로 포함하는 승수 인자를 생성하고, 상기 생성된 승수 인자에 기초하여 제 1 개인키를 생성하는 단계;

를 포함하는 개인키 생성 방법.

청구항 8

제 7 항에 있어서 상기 개인키 생성 방법은,

상기 마스터 키에 포함된 파라미터, 및 임의의 수에 기초하여 제 2 개인키 및 제 3 개인키를 생성하는 단계;

를 더 포함하는 것을 특징으로 하는 개인키 생성 방법.

청구항 9

제 8 항에 있어서,

상기 제 1 개인키는 상기 제 2 개인키 및 제 3 개인키를 이용한 태그 함수 값에 기초하지 않는 것을 특징으로 하는 개인키 생성 방법.

청구항 10

개인키 생성 장치에 있어서,

복수의 파라미터가 포함된 마스터 키 및 복수의 공개 파라미터를 포함하는 공개 파라미터 그룹을 설정하는 파라미터 설정부;

암호 데이터 수신 장치로부터 식별 정보를 획득하는 정보 획득부;

상기 마스터 키에 포함된 파라미터를 밑수로 포함하고, 상기 획득한 식별 정보를 이용하여 생성된 해쉬 함수값을 지수로 포함하는 승수 인자를 생성하고, 상기 생성된 승수 인자를 포함하는 제 1 개인키를 생성하는 개인키 생성부;

를 포함하는 개인키 생성 장치.

청구항 11

제 10항에 있어서 상기 개인키 생성부는,

상기 마스터 키에 포함된 파라미터, 및 임의의 수를 이용하여 제 2 개인키 및 제 3 개인키를 더 생성하는 것을 특징으로 하는 개인키 생성 장치.

청구항 12

제 11 항에 있어서,

상기 제 1 개인키는 상기 제 2 개인키 및 제 3 개인키를 이용한 태그 함수 값을 이용하지 않는 것을 특징으로 하는 개인키 생성 장치.

청구항 13

개인키 생성 장치가 복수의 파라미터가 포함된 마스터 키 및 복수의 공개 파라미터를 포함하는 공개 파라미터

그룹을 설정하는 단계;

상기 키 생성 장치가 암호 데이터 수신 장치의 식별 정보를 수신하여, 상기 마스터 키에 포함된 파라미터를 밑수로 포함하고, 상기 획득한 식별 정보를 이용하여 생성된 해쉬 함수값을 지수로 포함하는 승수 인자를 생성하며, 상기 생성된 승수 인자를 이용하여 개인키를 생성하고, 상기 생성된 개인키를 암호 데이터 수신 장치에 전송하는 단계;

암호 데이터 전송 장치가 상기 식별 정보를 수신하고, 상기 식별 정보에 기초하여 메시지를 암호화하여 암호 데이터를 생성하고, 상기 생성한 암호 데이터를 상기 암호 데이터 수신 장치에 전송하는 단계;

상기 암호 데이터 수신 장치가 상기 암호 데이터 및 상기 비밀키를 수신하여, 상기 수신한 비밀키에 기초하여 상기 암호 데이터를 복호화하여 상기 메시지를 획득하는 단계;

를 포함하는 암호화 시스템.

청구항 14

제 1 항 내지 제 3 항, 및 제 7 항 내지 제 9 항중 어느 한 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

발명의 설명

기 술 분 야

[0001] 본 발명은 사용자의 식별 정보를 이용하여 개인키를 생성하고, 암호데이터를 생성하는 방법에 관한 것 이다.

배 경 기 술

[0002] 일반적으로 사용되는 공개키 시스템 기술은 비밀통신을 수행하고자 하는 각각의 사용자 단말이 자신의 비밀키와 공개키를 쌍으로 생성하고, 비밀통신을 수행하고자 하는 상대방 단말은 정당한 공개키를 획득해야만 통신이 이루어지도록 구성된다. 이때, 통신을 수행하고자 하는 상대방 단말의 공개키를 획득한 사용자는 자신이 획득한 공개키가 정당한지 여부를 입증하기 위해, 제 3 의 신뢰기관으로 획득한 공개키에 대한 서명을 받아 이를 공개키의 인증서로 사용한다.

[0003] 다만, 이와 같은 인증서 기반의 공개키 시스템은 공개키 인증서의 폐기 시, 인증서 폐기 목록을 일정 기간 동안 유지하거나, 지속적으로 관리해야 함에 따라, 관리에 따른 비용 및 시간 소모가 발생하는 문제점이 발생하였다.

[0004] 이를 해결하기 위해, 암호 데이터 수신 장치의 식별 정보(ID)기반 공개키 암호화 방법이 연구되어 왔다. 특히, 암호 데이터 수신 장치의 식별 정보(ID)를 이용하여 효율적으로 개인키를 생성하고, 암호 데이터를 생성하는 방법이 연구되고 있다.

발명의 내용

해결하려는 과제

[0005] 본 발명은 사용자의 식별 정보를 이용하여 효율적으로 개인키를 생성하고, 효율적으로 암호데이터를 생성하는 방법을 제공하고자 한다.

과제의 해결 수단

[0006] 상술한 기술적 과제를 달성하기 위한 기술적 수단으로서, 본 발명의 1 측면은 암호화 될 메시지 및 암호 데이터 수신 장치의 식별 정보를 획득하는 단계, 상기 획득한 메시지 및 임의의 수를 이용하여 제 1 암호 데이터를 생성하는 단계, 키생성 장치에 의해 설정된 공개 파라미터들중 하나를 밑수로 포함하고, 상기 획득한 식별 정보를 이용하여 생성된 해쉬 함수값을 지수에 포함하는 승수 인자를 생성하고, 상기 생성된 승수 인자에 기초하여 제 2 암호 데이터를 생성하는 단계, 상기 임의의 수를 이용하여 제 3 암호 데이터를 생성하는 단계, 상기 생성된 제 1 암호 데이터, 제 2 암호 데이터, 및 제 3 암호 데이터를 상기 암호 데이터 수신 장치에 전송하는 단계를 포함하는 암호 데이터 전송 방법을 제공 한다.

[0007] 또한, 상기 제 2 암호 데이터에 포함된 승수 인자들이 포함하는 밑수들은 동일한 곱셈군에 포함될 수 있다.

[0008] 또한, 상기 제 3 암호 데이터는 상기 곱셈군에 포함된 파라미터를 밑수로 포함하고, 상기 임의의 수를 지수에 포함할 수 있다.

[0009] 또한, 제 2 측면은 암호화 될 메시지 및 암호 데이터 수신 장치의 식별 정보를 획득하는 정보 획득부, 상기 획득한 메시지 및 임의의 수를 이용하여 제 1 암호 데이터를 생성하고, 키생성 디바이스에 의해 설정된 공개 파라미터들중 하나를 밑수로 포함하고, 상기 식별 정보에 기초하여 생성된 해쉬 함수값을 지수에 포함하는 승수 인자를 생성하여, 상기 생성된 승수 인자를 포함하는 제 2 암호 데이터를 생성하고, 상기 임의의 수를 이용하여 제 3 암호 데이터를 생성하는 암호 데이터 생성부, 상기 생성된 제 1 암호 데이터, 제 2 암호 데이터,및 제 3 암호 데이터를 상기 암호 데이터 수신 장치에 전송하는 암호 데이터 전송부를 포함하는 암호 데이터 전송 장치를 제공한다.

[0010] 또한, 상기 제 2 암호 데이터에 포함된 승수 인자들이 포함하는 밑수들은 동일한 곱셈군에 포함될 수 있다.

[0011] 또한, 상기 제 3 암호 데이터는 상기 곱셈군에 포함된 파라미터를 밑수로 포함하고, 상기 임의의 수를 지수에 포함할 수 있다.

[0012] 또한, 제 3 측면은, 개인키 생성 방법에 있어서, 복수의 파라미터가 포함된 마스터 키 및 복수의 공개 파라미터를 포함하는 공개 파라미터 그룹을 생성하는 단계, 암호 데이터 수신 장치의 식별 정보를 획득하는 단계, 상기 마스터 키에 포함된 파라미터들중 하나를 밑수로 포함하고, 상기 식별 정보에 기초하여 생성된 해쉬 함수값을 지수로 포함하는 승수 인자를 생성하고, 상기 생성된 승수 인자에 기초하여 제 1 개인키를 생성하는 단계를 포함하는 개인키 생성 방법을 제공할 수 있다.

[0013] 또한, 상기 개인키 생성 방법은 상기 마스터 키에 포함된 파라미터, 및 임의의 수에 기초하여 제 2 개인키 및 제 3 개인키를 생성하는 단계를 더 포함할 수 있다.

[0014] 또한, 상기 제 1 개인키는 상기 제 2 개인키 및 제 3 개인키를 이용한 태그 함수 값에 기초하지 않을 수 있다.

[0015] 또한, 제 4 측면은, 개인키 생성 장치에 있어서, 복수의 파라미터가 포함된 마스터 키 및 복수의 공개 파라미터를 포함하는 공개 파라미터 그룹을 설정하는 파라미터 설정부, 암호 데이터 수신 장치로부터 식별 정보를 획득하는 정보 획득부, 상기 마스터 키에 포함된 파라미터를 밑수로 포함하고, 상기 획득한 식별 정보를 이용하여 생성된 해쉬 함수값을 지수로 포함하는 승수 인자를 생성하고, 상기 생성된 승수 인자를 포함하는 제 1 개인키를 생성하는 개인키 생성부를 포함하는 개인키 생성 장치를 제공한다.

[0016] 또한, 상기 개인키 생성부는 상기 마스터 키에 포함된 파라미터, 및 임의의 수를 이용하여 제 2 개인키 및 제 3 개인키를 더 생성할 수 있다.

[0017] 또한, 상기 제 1 개인키는 상기 제 2 개인키 및 제 3 개인키를 이용한 태그 함수 값을 이용하지 않을 수 있다.

[0018] 또한, 제 5 측면은, 개인키 생성 장치가 복수의 파라미터가 포함된 마스터 키 및 복수의 공개 파라미터를 포함하는 공개 파라미터 그룹을 설정하는 단계, 상기 키 생성 장치가 암호 데이터 수신 장치의 식별 정보를 수신하여, 상기 마스터 키에 포함된 파라미터를 밑수로 포함하고, 상기 획득한 식별 정보를 이용하여 생성된 해쉬 함수값을 지수로 포함하는 승수 인자를 생성하며, 상기 생성된 승수 인자를 이용하여 개인키를 생성하고, 상기 생성된 개인키를 암호 데이터 수신 장치에 전송하는 단계, 암호 데이터 전송 장치가 상기 식별 정보를 수신하고, 상기 식별 정보에 기초하여 메시지를 암호화하여 암호 데이터를 생성하고, 상기 생성한 암호 데이터를 상기 암호 데이터 수신 장치에 전송하는 단계, 상기 암호 데이터 수신 장치가 상기 암호 데이터 및 상기 비밀키를 수신하여, 상기 수신한 비밀키에 기초하여 상기 암호 데이터를 복호화하여 상기 메시지를 획득하는 단계를 포함하는 암호화 시스템을 제공한다.

도면의 간단한 설명

[0019] 도 1 은 본 발명의 일 실시예에 따른 식별 정보 기반 공개키 암호화 방법을 구현한 시스템의 개략도이다.

도 2 는 본 발명의 일 실시예에 따른 암호 데이터 수신 장치의 식별 정보 기반 개인키 생성 방법을 설명하기 위한 순서도이다.

도 3 은 본 발명의 일 실시예에 따른 암호 데이터 전송 장치가 식별 정보 기반 암호 데이터를 생성하는 방법을 설명하기 위한 순서도이다.

도 4 는 본 발명의 일 실시예에 따른 암호 데이터 수신 장치가 암호 데이터 수신 장치의 식별 정보 기반 암호

데이터를 수신하여 복호화 하는 방법을 설명하기 위한 순서도이다.

도 5 는 본 발명의 일 실시예에 따른 식별 정보 기반 암호 시스템을 설명하기 위한 순서도이다.

도 6 은 본 발명의 일 실시예에 따른 암호 데이터 수신 장치의 식별 정보 기반 암호 시스템을 설명하기 위한 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0020] 아래에서는 첨부한 도면을 참조하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 본 발명의 실시예를 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 개시를 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0021] 명세서 전체에서, 어떤 부분이 다른 부분과 "연결"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 소자를 사이에 두고 "전기적으로 연결"되어 있는 경우도 포함한다. 또한 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다.

[0022] 이하 첨부된 도면을 참고하여 본 발명을 상세히 설명하기로 한다.

[0023] 도 1 은 본 발명의 일 실시예에 따른 식별 정보 기반 공개키 암호화 방법을 구현한 시스템의 개략도이다.

[0024] 도 1 에 도시된 바와 같이, 본 발명의 암호 데이터 수신 장치의 식별 정보에 기초한 암호화 방법을 구현하는 시스템은 개인키 생성 장치(200), 암호 데이터 전송 장치(100), 및 암호 데이터 수신 장치(300)를 포함한다.

[0025] 일 실시예에 따르면, 개인키 생성 장치(200)는 외부로부터 보안상수 k를 입력받아, 함수 생성 알고리즘을 이용하여, 타원 곡선군 G1 및 타원 곡선군 G2를 획득할 수 있다. 또한, 개인키 생성 장치(200)는 마스터 키를 생성할 수 있고, 복수의 파라미터가 포함된 공개 파라미터 그룹(PP)을 설정할 수 있다.

[0026] 일 실시예에 따르면, 개인키 생성 장치(200)는 암호 데이터 수신 장치(300)로부터 암호 데이터 수신 장치의 식별 정보를 수신할 수 있다. 또한, 개인키 생성 장치(200)는 수신한 식별 정보를 이용하여 개인키를 생성하고, 생성한 개인키를 암호 데이터 수신 장치(300)에 전송할 수 있다.

[0027] 일 실시예에 따르면, 암호 데이터 전송 장치(100)는 개인키 생성 장치(200)로부터 암호 데이터 수신 장치의 식별 정보를 획득할 수 있다. 또한, 획득한 식별 정보를 이용하여 암호 데이터를 생성하고, 생성한 암호 데이터를 암호 데이터 수신 장치(300)에 전송할 수 있다.

[0028] 일 실시예에 따르면, 암호 데이터 수신 장치(300)는 암호 데이터 수신 장치의 식별 정보를 획득하고, 획득한 암호 데이터 수신 장치의 식별 정보를 개인키 생성 장치(200)에 전송할 수 있다. 또한, 암호 데이터 수신 장치(300)는 암호 데이터 수신 장치의 식별 정보를 이용하여 생성된 개인키를 개인키 생성 장치(200)로부터 수신할 수 있다.

[0029] 일 실시예에 따르면, 암호 데이터 수신 장치(300)는 암호 데이터 전송 장치(100)로부터 암호 데이터를 수신할 수 있다. 암호 데이터 수신 장치(300)는 개인키 생성 장치(200)로부터 수신한 개인키를 이용하여 수신한 암호 데이터를 복호화할 수 있다.

[0030] 도 2 는 본 발명의 일 실시예에 따른 암호 데이터 수신 장치의 식별 정보 기반 개인키 생성 방법을 설명하기 위한 순서도이다.

[0031] 단계 S210에서, 개인키 생성 장치(200)는 마스터 키 및 공개 파라미터 그룹을 설정할 수 있다.

[0032] 일 실시예에 따르면, 개인키 생성 장치(200)는 외부로부터 보안상수 k를 입력받아, 함수 생성 알고리즘을 이용하여, 타원 곡선군 G1 및 타원 곡선군 G2를 획득할 수 있다. 또한, 개인키 생성 장치(200)는 타원 곡선군 G1에 속하는 생성원 중 임의의 제 1 생성원 g_1, 및 타원 곡선군 G2에 속하는 생성원중 임의의 제 2 생성원 g_2을 선택할 수 있다.

[0033] 일 실시예에 따르면, 개인키 생성 장치(200)는 마스터 키를 생성할 수 있다. 개인키 생성 장치(200)에 의해 생성된 마스터 키는 복수의 파라미터를 포함할 수 있다. 예를 들어, 개인키 생성 장치(200)가 생성한 마스터 키는 난수들(α , β , γ , δ) 및 제 2 곱셈군 G2에 속하는 제 2 생성원(g_2)을 포함할 수 있다.

[0034] 일 실시예에 따르면, 개인키 생성 장치(200)는 복수의 파라미터가 포함된 공개 파라미터 그룹(PP)을 설정할 수 있다. 공개 파라미터 그룹(PP)은 개인키 생성 장치(200), 암호 데이터 전송 장치(100), 및 암호 데이터 수신 장치(300)에 의해 사용되는 공개 파라미터들의 집합을 의미한다. 예를 들어, 공개 파라미터 그룹(PP)은 제 1 곱셈군에 속하는 생성원 g_1, u=(g_1)^α, v=(g_1)^β, w=(g_1)^ɣ, A=e(g_1,g_2)^β, 제 1 해쉬함수(H1), 제 2 해쉬함수(H2), 및 제 3 해쉬함수(H3)등을 포함할 수 있다.

[0035] 제 1 해쉬함수(H1), 제 2 해쉬함수(H2), 및 제 3 해쉬함수(H3)는 개인키 생성 장치(200)에 의해 선택된 암호학적 해쉬 함수를 의미한다. 개인키 생성 장치(200)는 기 설정된 제 1 해쉬함수(H1), 제 2 해쉬함수(H2), 및 제 3 해쉬함수(H3)를 외부의 디바이스로부터 수신할 수 있고, 제 1 해쉬함수(H1), 제 2 해쉬함수(H2), 및 제 3 해쉬함수(H3)를 생성할 수 있으며, 이에 한정되지 않고 다양한 방법으로 해쉬 함수들을 획득할 수 있다.

[0036] 일 실시예에 따르면, 개인키 생성 장치(200)는 획득한 공개 파라미터 그룹(PP)을 암호 데이터 전송 장치(100), 및 암호 데이터 수신 장치(300)에 전송할 수 있다. 예를 들어, 개인키 생성 장치(200)는 유선 통신 경로 또는 무선 통신 경로를 이용하여 획득한 공개 파라비터 그룹(PP)을 전송할 수 있다.

[0037] 단계 S220에서, 개인키 생성 장치(200)는 암호 데이터 수신 장치의 식별 정보를 획득할 수 있다.

[0038] 일 실시예에 따르면, 개인키 생성 장치(200)는 암호 데이터 수신 장치(300)로부터 암호 데이터 수신 장치의 식별 정보를 수신할 수 있다. 암호 데이터 수신 장치(300)의 식별 정보란, 암호 데이터 수신 장치(300)의 사용자 또는 암호 데이터 수신 장치를 나타내는 정보를 의미한다. 예를 들어, 암호 데이터 수신 장치의 식별 정보는, 사용자의 전화번호, 사용자의 주민등록 번호, 사용자의 이메일 주소등을 포함할 수 있으며, 이에 한정되지 않고 사용자를 나타내는 소정의 정보를 포함할 수 있다.

[0039] 또한, 암호 데이터 수신 장치의 식별 정보는, 암호 데이터 수신 장치의 제조 일자 또는 제조 번호등을 포함할 수 있으며, 이에 한정되지 않고 암호 데이터 수신 장치(300)를 나타내는 소정의 정보를 포함할 수 있다.

[0040] 단계 S230에서, 개인키 생성 장치(200)는 획득한 식별 정보를 이용하여 개인키를 생성할 수 있다.

[0041] 일 실시예에 따르면, 개인키 생성 장치(200)는 개인키를 생성하기 위해 복수의 난수를 생성할 수 있다. 예를 들어, 개인키 생성 장치(200)는 제 1 난수(r) 및 제 2 난수(Rid)를 생성할 수 있다.

[0042] $$D1=((g\_2)^{\alpha} * (g\_2)^{H1(ID)*\beta} * (g\_2)^{\gamma*Rid})^{r}$$ -- 수학식 (1)

[0043] 일 실시예에 따르면, 개인키 생성 장치(200)는 수학식(1)을 이용하여 제 1 개인키(D1)를 생성할 수 있다. 예를 들어, 개인키 생성 장치(200)는 마스터 키에 포함된 파라미터들(g_2, α, β, ɣ), 획득한 식별 정보의 제 1 해쉬 함수값(H1(ID)),제 1 난수(r), 및 제 2 난수(Rid)를 이용하여 제 1 개인키(D1)를 생성할 수 있다.

[0044] 일 실시예에 따르면, 개인키 생성 장치(200)는 제 1 개인키(D1)를 생성하기 위해, 마스터 키에 포함된 파라미터를 밑수로 포함하고, 획득한 암호 데이터 수신 장치의 식별 정보에 기초하여 생성된 제 1 해쉬 함수값(H1(ID))을 지수로 포함하는 승수 인자를 생성할 수 있다. 예를 들어, 개인키 생성 장치(200)는 마스터 키에 포함된 파라미터(g_2) 를 밑수로 포함하고, 제 1 해쉬 함수값(H1(ID))을 지수로 포함하는 승수 인자((g_2)^H1(ID))를 생성할 수 있다. 승수 인자란, 곱셈연산에서 곱해지는 인수에 곱하는 인수를 의미한다.

[0045] 또한, 개인키 생성 장치(200)는 마스터 키에 포함된 파라미터들을 이용하여 생성된 값((g_2)^β)을 밑수로 포함하고, 제 1 해쉬 함수값(H1(ID))을 지수로 포함하는 승수 인자((g_2)^β*H1(ID))를 생성할 수 있다.

[0046] 일 실시예에 따르면, 개인키 생성 장치(200)는 생성된 승수 인자((g_2)^H1(ID))를 이용하고, 수학식 (1)에 기초하여 제 1 개인키(D1)를 생성할 수 있다. 개인키 생성 장치(200)는 제 1 해쉬 함수값(H1(ID))을 지수 자리에 포함한 승수 인자를 사용함으로써, 제 1 해쉬 함수값(H1(ID))을 제1 곱셈군(G1) 또는 제2 곱셈군(G2)에 속하는 생성원중 하나로 매칭하는 과정을 생략할 수 있다. 그 결과, 개인키 생성 장치(200)는 종래 기술에 비해 개인키를 효율적으로 생성할 수 있다.

[0047] 일 실시예에 따르면, 개인키 생성 장치(200)는 제 2 개인키(D2) 및 제 3 개인키(D3)에 기초하여 생성된 제 2 해쉬함수값(H2(D2,D3))인 태그함수값의 이용을 생략하고 제 1 개인키를 생성할 수 있다. 예를 들어, 개인키 생성

장치(200)는 태그함수값 대신 제 2 난수(Rid)를 이용하여 제 1 개인키를 생성할 수 있다. 개인키 생성 장치(200)는 제 1 개인키를 생성하는 경우, 태그함수값 대신 난수(Rid)를 사용함으로써, 암호 데이터의 복호화시에 정확성 에러를 방지할 수 있다.

[0048] $D2=(g\_2)^{r}$ -- 수학식 (2)

[0049] 일 실시예에 따르면, 개인키 생성 장치(200)는 수학식(2)을 이용하여 제 2 개인키를 생성할 수 있다. 예를 들어, 개인키 생성 장치(200)는 마스터 키에 포함된 파라미터(g_2) 및 개인키 생성 장치(200)에의해 생성된 제 1 난수(r)를 수학식 (2)의 입력값으로 이용하여 제 2 개인키를 생성할 수 있다.

[0050] $D3=(g\_2)^{\delta+\gamma*r}$ -- 수학식 (3)

[0051] 일 실시예에 따르면, 개인키 생성 장치(200)는 수학식(3)을 이용하여 제 3 개인키를 생성할 수 있다. 예를 들어, 개인키 생성 장치(200)는 마스터 키에 포함된 파라미터들(g_2, δ, γ)및 개인키 생성 장치(200)에의해 생성된 제 1 난수(r)를 수학식 (3)의 입력값으로 이용하여 제 3 개인키를 생성할 수 있다.

[0052] 일 실시예에 따르면, 개인키 생성 장치(200)는 획득한 제 1 개인키, 제 2 개인키, 및 제 3 개인키를 암호 데이터 수신 장치(300)에 전송할 수 있다. 예를 들어, 개인키 생성 장치(200)는 제 1 개인키, 제 2 개인키, 및 제 3 개인키를 결합하여, 개인키 그룹을 생성하고, 생성된 개인키 그룹을 전송할 수 있다. 또한, 제 1 개인키, 제 2 개인키, 제 3 개인키를 각각 전송할 수 있으며, 이에 한정되지 않고 다양한 방법으로 제 1 개인키, 제 2 개인키,및 제 3 개인키를 전송할 수 있다.

[0053] 일 실시예에 따르면, 개인키 생성 장치(200)는 획득한 난수(Rid)를 암호 데이터 수신 장치(300)에 전송 할 수 있다. 예를 들어, 개인키 생성 장치(200)는 획득한 난수(Rid)를 개인키 그룹과 함께 전송할 수 있고, 독립적으로 전송할 수 있으며, 이에 한정되지 않고 다양한 방법으로 전송할 수 있다.

[0054] 도 3 은 본 발명의 일 실시예에 따른 암호 데이터 전송 장치가 식별 정보 기반 암호 데이터를 생성하는 방법을 설명하기 위한 순서도이다.

[0055] 단계 S310에서, 암호 데이터 전송 장치는 암호화될 메시지 및 암호 데이터 수신 장치의 식별 정보를 획득할 수 있다.

[0056] 일 실시예에 따르면, 암호 데이터 전송 장치(100)는 암호 데이터 수신 장치의 식별 정보를 획득할 수 있다. 예를 들어, 암호 데이터 전송 장치(100)는 암호 데이터 수신 장치 사용자의 전화번호, 주민등록 번호, 이메일 주소등을 획득할 수 있으며, 이에 한정되지 않고 사용자를 나타내는 소정의 정보를 획득할 수 있다.

[0057] 또한, 암호 데이터 전송 장치(100)는 암호 데이터 수신 장치의 제조 일자 또는 제조 번호등을 획득할 수 있으며, 이에 한정되지 않고 암호 데이터 수신 장치(300)를 나타내는 소정의 정보를 획득할 수 있다.

[0058] 일 실시예에 따르면, 암호 데이터 전송 장치(100)는 암호 데이터 수신 장치의 식별 정보를 개인키 생성 장치(200)로부터 수신할 수 있다. 또한, 암호 데이터 전송 장치(100)는 암호 데이터 수신 장치의 식별 정보를 암호 데이터 수신 장치(300)로부터 수신할 수 있다.

[0059] 일 실시예에 따르면, 암호 데이터 전송 장치(100)는 암호화 될 메시지(M)를 획득할 수 있다. 예를 들어, 암호 데이터 전송 장치(100)는 암호화 될 메시지(M)를 생성할 수 있고, 외부의 디바이스로부터 암호화 될 메시지를 수신할 수 있다.

[0060] 일 실시예에 따르면, 암호 데이터 전송 장치(100)는 개인키 생성 장치(200)에 의해 설정된 공개 파라미터 그룹(PP)을 획득할 수 있다. 예를 들어, 암호 데이터 전송 장치(100)는 개인키 생성 장치(200)로부터 공개 파라미터 그룹(PP)을 획득할 수 있으며, 이에 한정되지 않고 개인키 생성 장치(200)외부의 임의의 디바이스로부터 공개 파라미터 그룹(PP)을 획득할 수 있다.

[0061] 단계 S320에서, 암호 데이터 전송 장치(100)는 획득한 메시지 및 임의의 수를 이용하여 제 1 암호 데이터를 생

성할 수 있다.

[0062] 일 실시예에 따르면, 암호 데이터 전송 장치(100)는 소정의 난수(s)를 획득할 수 있다. 예를 들어, 암호 데이터 전송 장치(100)는 소정의 난수(s)를 생성할 수 있고, 외부의 디바이스로부터 수신할 수 있다.

[0063] $$C1 = H3(A^S) \oplus M$$ -- 수학식 (4-1)

[0064] 일 실시예에 따르면, 암호 데이터 전송 장치(100)는 수학식(4-1)을 이용하여 제 1 암호 데이터(C1)를 생성할 수 있다. 예를 들어, 암호 데이터 전송 장치(100)는 공개 파라미터 그룹(PP)에 포함된 공개 파라미터(A) 및 제 3 해쉬함수(H3), 획득한 난수(s), 획득한 메시지(M)를 이용하여 제 1 암호 데이터(C1)를 생성할 수 있다.

[0065] 단계 S330에서, 암호 데이터 전송 장치(100)는 개인키 생성 장치(200)에 의해 설정된 공개 파라미터 및 획득한 식별 정보를 이용하여 제 2 암호 데이터를 생성할 수 있다.

[0066] $$C2 = (uv^{H_1(ID)}w^{tagC})^s$$ -- 수학식 (4-2)

[0067] tagC=H2(C1,C2) -- 수학식 (5)

[0068] 일 실시예에 따르면, 암호 데이터 전송 장치(100)는 수학식(4-2)을 이용하여 제 2 암호 데이터(C2)를 생성할 수 있다. 예를 들어, 암호 데이터 전송 장치(100)는 공개 파라미터 그룹(PP)에 포함된 공개 파라미터들(u, v, w), 획득한 난수(s), 암호 데이터 수신 장치의 식별 정보에 기초하여 생성된 제 1 해쉬 함수 값(H1(ID)), 제 1 암호 데이터와 제 3 암호 데이터에 기초하여 생성된 태그 함수값(tagC)을 이용하여 제 2 암호 데이터(C2)를 생성할 수 있다. 암호 데이터 전송 장치(100)는 태그 함수값을 수학식 (5)를 이용하여 획득할 수 있다.

[0069] 일 실시예에 따르면, 암호 데이터 전송 장치(100)는 공개 파라미터 그룹(PP)에 포함된 공개 파라미터(v)를 밑수로 포함하고, 제 1 해쉬 함수 값(H1(ID))을 지수로 포함하는 승수 인자(v^(H1(ID)))를 생성할 수 있다.

[0070] 또한, 암호 데이터 전송 장치(100)는 생성한 승수 인자를 이용하여 제 2 암호 데이터를 생성할 수 있다. 암호 데이터 전송 장치(100)는 획득한 식별 정보의 제 1 해쉬 함수값(H1(ID))을 지수 자리에 포함한 승수 인자를 이용함으로써, 제 1 해쉬 함수값(H1(ID))을 제1 곱셈군(G1) 또는 제2 곱셈군(G2)에 속하는 생성원중 하나로 매칭하는 과정을 생략할 수 있다. 그 결과, 암호 데이터 전송 장치(100)는 종래 기술에 비해 암호 데이터를 효율적으로 생성할 수 있다.

[0071] 단계 S340에서, 암호 데이터 전송 장치(100)는 개인키 생성 장치(200)에 의해 설정된 공개 파라미터 및 임의의 수를 이용하여 제 3 암호 데이터를 생성할 수 있다.

[0072] C3=(g_1)^s -- 수학식(6)

[0073] 일 실시예에 따르면, 암호 데이터 전송 장치(100)는 획득한 난수(s)를 이용하여 제 3 암호 데이터를 생성할 수 있다. 예를 들어, 암호 데이터 전송 장치(100)는 공개 파라미터 그룹(PP)에 포함된 공개 파라미터(g_1) 및 획득한 난수(s)를 수학식(6)에 입력하여 제 3 암호 데이터를 생성할 수 있다.

[0074] 단계 S350에서, 암호 데이터 전송 장치(100)는 생성된 제 1 암호 데이터, 제 2 암호 데이터, 및 제 3 암호데이터를 암호 데이터 수신 장치(300)에 전송할 수 있다.

[0075] 일 실시예에 따르면, 암호 데이터 전송 장치(100)는 획득한 제 1 암호 데이터, 제 2 암호 데이터, 및 제 3 암호 데이터를 암호 데이터 수신 장치(300)에 전송할 수 있다. 예를 들어, 암호 데이터 전송 장치(100)는 제 1 암호 데이터, 제 2 암호 데이터, 및 제 3 암호 데이터를 결합하여, 하나의 암호 데이터 그룹을 생성하고, 생성된 암호 데이터 그룹을 전송할 수 있다. 또한, 제 1 암호 데이터, 제 2 암호 데이터, 제 3 암호 데이터를 각각 전송

할 수 있으며, 이에 한정되지 않고 다양한 방법으로 제 1 암호 데이터, 제 2 암호 데이터,및 제 3 암호 데이터를 전송할 수 있다.

[0076] 도 4 는 본 발명의 일 실시예에 따른 암호 데이터 수신 장치가 암호 데이터 수신 장치의 식별 정보 기반 암호 데이터를 수신하여 복호화 하는 방법을 설명하기 위한 순서도이다.

[0077] 단계 S410에서, 암호 데이터 수신 장치(300)는 사용자의 식별 정보를 획득할 수 있다.

[0078] 일 실시예에 따르면, 암호 데이터 수신 장치(300)는 사용자의 입력에 기초하여 식별 정보를 획득할 수 있다. 예를 들어, 암호 데이터 수신 장치(300)는 사용자가 입력한 ID, 사용자가 입력한 전화 번호, 사용자가 입력한 주민등록 번호등을 식별 정보로서 획득할 수 있다.

[0079] 일 실시예에 따르면, 암호 데이터 수신 장치(300)는 외부의 디바이스로부터 식별 정보를 수신할 수 있다. 예를 들어, 암호 데이터 수신 장치(300)는 암호 데이터 수신 장치(300)외부의 장치로부터 수신한 ID, 전화 번호, 주민등록번호등을 식별 정보로서 획득할 수 있다.

[0080] 일 실시예에 따르면, 암호 데이터 수신 장치(300)는 식별 정보를 생성할 수 있다. 예를 들어, 암호 데이터 수신 장치(300)는 기 입력된 제조 일자, 또는 제조 번호등을 이용하여 식별 정보를 생성할 수 있다.

[0081] 단계 S420에서, 암호 데이터 수신 장치(300)는 획득한 사용자의 식별 정보를 개인키 생성 장치(200)에 전송할 수 있다.

[0082] 일 실시예에 따르면, 암호 데이터 수신 장치(300)는 획득한 식별 정보를 개인키 생성 장치(200)에 전송할 수 있다. 예를 들어, 암호 데이터 수신 장치(300)는 획득한 식별 정보를 유선 통신 경로 또는 무선 통신 경로를 이용하여 전송할 수 있다.

[0083] 단계 S430에서, 암호 데이터 수신 장치(300)는 개인키 생성 장치(200)로부터 식별 정보에 기초한 개인키를 획득할 수 있다.

[0084] 일 실시예에 따르면, 암호 데이터 수신 장치(300)는 개인키 생성 장치(200)로부터 제 1 개인키(D1), 제 2 개인키(D2), 및 제 3 개인키(D3)를 수신할 수 있다. 예를 들어, 암호 데이터 수신 장치(300)는 개인키 그룹을 수신하고, 수신한 개인인키 그룹에 포함된 제 1 개인키(D1), 제 2 개인키(D2), 및 제 3 개인키(D3)를 획득할 수 있다. 또한, 암호 데이터 수신 장치(300)는 제 1 개인키(D1), 제 2 개인키(D2), 제 3 개인키(D3)를 각각 수신할 수 있으며, 이에 한정되지 않고 다양한 방법으로 제 1 개인키(D1), 제 2 개인키(D2),및 제 3 개인키(D3)를 수신할 수 있다.

[0085] 일 실시예에 따르면, 암호 데이터 수신 장치(300)는 개인키 생성 장치(200)로부터 공개 파라미터 그룹(PP)을 획득할 수 있다. 또한, 이에 한정되지 않고 암호 데이터 수신 장치(300)는 외부의 다양한 디바이스로부터 공개 파라미터 그룹(PP)을 획득할 수 있다.

[0086] 단계 S440에서, 암호 데이터 수신 장치(300)는 암호 데이터 전송 장치(100)로부터 암호 데이터 수신 장치의 식별 정보에 기초한 암호 데이터를 획득할 수 있다.

[0087] 일 실시예에 따르면, 암호 데이터 수신 장치(300)는 암호 데이터 전송 장치(100)로부터 제 1 암호 데이터(C1), 제 2 암호 데이터(C2), 및 제 3 암호 데이터(C3)를 수신할 수 있다. 예를 들어, 암호 데이터 수신 장치(300)는 암호 데이터 그룹을 수신하고, 수신한 암호 데이터 그룹에 포함된 제 1 암호 데이터(C1), 제 2 암호 데이터(C2), 및 제 3 암호 데이터(C3)를 획득할 수 있다.

[0088] 또한, 암호 데이터 수신 장치(300)는 제 1 암호 데이터(C1), 제 2 암호 데이터(C2), 제 3 암호 데이터(C3)를 각각 수신할 수 있으며, 이에 한정되지 않고 다양한 방법으로 제 1 암호 데이터(C1), 제 2 암호 데이터(C2),및 제 3 암호 데이터(C3)를 수신할 수 있다.

[0089] 단계 S450에서, 암호 데이터 수신 장치(300)는 획득한 개인키를 이용하여 획득한 암호 데이터를 복호화할 수 있다.

[0090] $$M = C1 \oplus H3\left(\frac{e(C3,\ D3,\ D1^{T})}{e(C2,\ D2^{T})}\right)$$ -- 수학식(7)

[0091] T=-1/(Rid - TagC) -- 수학식(8)

[0092] 일 실시예에 따르면, 암호 데이터 수신 장치(300)는 수신한 암호데이터를 복호화 하기 위해, T 를 획득할 수 있다. 예를 들어, 암호 데이터 수신 장치(300)는 수학식(5)을 이용하여 획득한 TagC 및 개인키 생성 장치(200)로부터 획득한 제 2 난수(Rid)를 수학식(8)의 입력값으로 이용하여, T를 생성할 수 있다.

[0093] 일 실시예에 따르면, 암호 데이터 수신 장치(300)는 획득한 암호 데이터들(C1, C2, C3)을 획득한 개인키들(D1, D2, D3)을 이용하여 복호화 하고, 복호화한 결과값인 메시지(M)를 획득할 수 있다. 예를 들어, 암호 데이터 수신 장치(300)는 획득한 암호 데이터들(C1,C2,C3) 및 획득한 개인키들(D1, D2, D3)을 수학식(7)에 입력하여, 메시지(M)를 획득할 수 있다.

[0094] 도 5 는 본 발명의 일 실시예에 따른 식별 정보 기반 암호 시스템을 설명하기 위한 순서도이다.

[0095] 단계 S505에서, 개인키 생성 장치(200)는 마스터 키 및 공개 파라미터 그룹(PP)을 생성할 수 있다.

[0096] 일 실시예에 따르면, 개인키 생성 장치(200)는 마스터 키를 생성할 수 있다. 개인키 생성 장치(200)에 의해 생성된 마스터 키는 복수의 파라미터를 포함할 수 있다. 예를 들어, 개인키 생성 장치(200)가 생성한 마스터 키는 난수들(α , β , γ , δ) 및 제 2 곱셈군 G2에 속하는 제 2 생성원(g_2)을 포함할 수 있다.

[0097] 일 실시예에 따르면, 개인키 생성 장치(200)는 복수의 파라미터가 포함된 공개 파라미터 그룹(PP)을 설정할 수 있다. 예를 들어, 공개 파라미터 그룹(PP)은 제 1 곱셈군에 속하는 생성원 g_1, u=g_1^α , v=(g_1)^β , w=(g_1)^γ , A=e(g_1,g_2)^β , 제 1 해쉬함수(H1), 제 2 해쉬함수(H2), 및 제 3 해쉬함수(H3)등을 포함할 수 있다.

[0098] 일 실시예에 따르면, 개인키 생성 장치(200)는 생성한 공개 파라미터 그룹을 암호 데이터 수신 장치(300) 및 암호 데이터 전송 장치(100)에 전송할 수 있다.

[0099] 단계 S510에서, 암호 데이터 수신 장치(300)는 암호 데이터 수신 장치의 식별 정보를 획득할 수 있다.

[0100] 일 실시예에 따르면, 암호 데이터 수신 장치(300)는 사용자의 입력에 기초하여 식별 정보를 획득할 수 있다. 또한, 외부의 디바이스로부터 식별 정보를 수신할 수 있다.

[0101] 단계 S515에서, 암호 데이터 수신 장치(300)는 획득한 식별 정보를 개인키 생성 장치(200)에 전송할 수 있다.

[0102] 일 실시예에 따르면, 암호 데이터 수신 장치(300)는 획득한 식별 정보를 개인키 생성 장치(200)에 전송할 수 있다. 예를 들어, 암호 데이터 수신 장치(300)는 획득한 식별 정보를 유선 통신 경로, 또는 무선 통신 경로를 이용하여 전송할 수 있으며, 이에 한정되지 않고 다양한 방법으로 식별 정보를 전송할 수 있다.

[0103] 일 실시예에 따르면, 암호 데이터 수신 장치(300)는 획득한 식별 정보를 암호 데이터 전송 장치(100)에 전송할 수 있다. 예를 들어, 암호 데이터 수신 장치(300)는 획득한 식별 정보를 유선 통신 경로, 또는 무선 통신 경로를 이용하여 전송할 수 있으며, 이에 한정되지 않고 다양한 방법으로 식별 정보를 전송할 수 있다..

[0104] 단계 S520에서, 개인키 생성 장치(200)는 회득한 식별 정보를 이용하여 개인키를 생성할 수 있다.

[0105] 일 실시예에 따르면, 개인키 생성 장치(200)는 개인키를 생성하기 위해 복수의 난수를 생성할 수 있다. 예를 들어, 개인키 생성 장치(200)는 제 1 난수(r) 및 제 2 난수(Rid)를 생성할 수 있다.

[0106] 일 실시예에 따르면, 개인키 생성 장치(200)는 수학식(1)을 이용하여 제 1 개인키(D1)를 생성할 수 있다. 예를 들어, 개인키 생성 장치(200)는 마스터 키에 포함된 파라미터들(g_2, α , β , γ), 획득한 식별 정보에 기초하여 생성된 제 1 해쉬 함수값(H1(ID)), 개인키 생성 장치(200)에의해 생성된 제 1 난수(r), 및 제 2 난수(Rid)를 이용하여 제 1 개인키(D1)를 생성할 수 있다.

[0107] 예를 들어, 개인키 생성 장치(200)는 마스터 키에 포함된 파라미터(g_2)를 밑수로 포함하고, 제 1 해쉬 함수값(H1(ID))을 지수로 포함하는 승수 인자(g_2^H1(ID))를 생성하고, 생성된 승수 인자 및 수학식 (1)에 기초하여 제 1 개인키(D1)를 생성할 수 있다.

[0108] 일 실시예에 따르면, 개인키 생성 장치(200)는 수학식(2)을 이용하여 제 2 개인키를 생성할 수 있다. 예를 들어, 개인키 생성 장치(200)는 마스터 키에 포함된 파라미터(g_2) 및 개인키 생성 장치(200)에의해 생성된 제 1 난수(r)를 수학식 (2)의 입력값으로 이용하여 제 2 개인키(D2)를 생성할 수 있다.

[0109] 일 실시예에 따르면, 개인키 생성 장치(200)는 수학식(3)을 이용하여 제 3 개인키를 생성할 수 있다. 예를 들어, 개인키 생성 장치(200)는 마스터 키에 포함된 파라미터들(g_2, δ, ɣ)및 개인키 생성 장치(200)에의해 생성된 제 1 난수(r)를 수학식 (3)의 입력값으로 이용하여 제 3 개인키(D3)를 생성할 수 있다.

[0110] 단계 S525에서, 암호 데이터 전송 장치(100)는 개인키 생성 장치(200)로부터 사용자의 식별 정보를 수신할 수 있다.

[0111] 일 실시예에 따르면, 암호 데이터 전송 장치(100)는 암호 데이터 수신 장치의 식별 정보를 개인키 생성 장치(200)로부터 수신할 수 있다. 또한, 암호 데이터 전송 장치(100)는 암호 데이터 수신 장치의 식별 정보를 암호 데이터 수신 장치(300)로부터 수신할 수 있다.

[0112] 단계 S530에서, 암호 데이터 수신 장치(300)는 개인키 생성 장치(200)로부터 사용자의 개인키를 수신할 수 있다.

[0113] 일 실시예에 따르면, 암호 데이터 수신 장치(300)는 개인키 생성 장치(200)로부터 사용자의 식별정보에 기초한 제 1 개인키(D1), 제 2 개인키(D2), 및 제 3 개인키(D3)를 수신할 수 있다. 예를 들어, 암호 데이터 수신 장치(300)는 사용자의 식별 정보에 기초한 개인키 그룹을 수신하고, 수신한 개인키 그룹에 포함된 제 1 개인키(D1), 제 2 개인키(D2), 및 제 3 개인키(D3)를 획득할 수 있다. 또한, 암호 데이터 수신 장치(300)는 제 1 개인키(D1), 제 2 개인키(D2), 제 3 개인키(D3)를 각각 수신할 수 있으며, 이에 한정되지 않고 다양한 방법으로 제 1 개인키(D1), 제 2 개인키(D2),및 제 3 개인키(D3)를 수신할 수 있다.

[0114] 단계 S535에서, 암호 데이터 전송 장치(100)는 획득한 사용자의 식별 정보를 이용하여 암호 데이터를 생성할 수 있다.

[0115] 일 실시예에 따르면, 암호 데이터 전송 장치(100)는 수학식(4-1)을 이용하여 제 1 암호 데이터(C1)를 생성할 수 있다. 예를 들어, 암호 데이터 전송 장치(100)는 공개 파라미터 그룹(PP)에 포함된 공개 파라미터(A) 및 제 3 해쉬함수(H3), 획득한 난수(s), 획득한 메시지(M)를 이용하여 제 1 암호 데이터(C1)를 획득할 수 있다.

[0116] 일 실시예에 따르면, 암호 데이터 전송 장치(100)는 수학식(4-2)을 이용하여 제 2 암호 데이터(C2)를 생성할 수 있다. 예를 들어, 암호 데이터 전송 장치(100)는 공개 파라미터 그룹(PP)에 포함된 공개 파라미터들(u, v, w), 획득한 난수(s), 암호 데이터 수신 장치(300)의 식별 정보에 기초하여 생성된 제 1 해쉬 함수 값(H1(ID)), 제 1 암호 데이터와 제 3 암호 데이터에 의해 결정되는 태그 함수값(tagC)을 이용하여 제 2 암호 데이터(C2)를 생성할 수 있다. 암호 데이터 전송 장치(100)는 태그 함수값을 수학식 (5)를 이용하여 획득할 수 있다.

[0117] 일 실시예에 따르면, 암호 데이터 전송 장치(100)는 공개 파라미터 그룹(PP)에 포함된 공개 파라미터(v)를 밑수로 포함하고, 획득한 암호 데이터 수신 장치의 식별 정보(H1(ID))를 지수로 포함하는 승수 인자(v^(H_1 (ID)))를 생성할 수 있다. 또한, 암호 데이터 전송 장치(100)는 생성한 승수 인자(v^(H_1 (ID)))를 이용하여 제 2 암호 데이터를 생성할 수 있다. 암호 데이터 전송 장치(100)는 획득한 암호 데이터 수신 장치의 식별 정보의 제 1 해쉬 함수값(H1(ID))을 지수 자리에 포함한 승수 인자를 이용함으로써, 제 1 해쉬 함수값(H1(ID))을 제1 곱셈군(G1) 또는 제2 곱셈군(G2)에 속하는 생성원중 하나로 매칭하는 과정을 생략할 수 있다. 그 결과, 암호 데이터 전송 장치(100)는 종래 기술에 비해 암호 데이터를 효율적으로 생성할 수 있다.

[0118] 일 실시예에 따르면, 암호 데이터 전송 장치(100)는 획득한 난수(s)를 이용하여 제 3 암호 데이터를 생성할 수 있다. 예를 들어, 암호 데이터 전송 장치(100)는 공개 파라미터 그룹(PP)에 포함된 공개 파라미터(g_1) 및 획득한 난수(s)를 수학식(6)에 입력하여 제 3 암호 데이터를 생성할 수 있다.

[0119] 단계 S540에서, 암호 데이터 전송 장치(100)는 생성한 암호 데이터를 암호 데이터 수신 장치(300)에 전송할 수 있다.

[0120] 일 실시예에 따르면, 암호 데이터 전송 장치(100)는 획득한 제 1 암호 데이터(C1), 제 2 암호 데이터(C2), 및 제 3 암호 데이터(C3)를 암호 데이터 수신 장치(300)에 전송할 수 있다. 예를 들어, 암호 데이터 전송 장치(100)는 제 1 암호 데이터(C1), 제 2 암호 데이터(C2), 및 제 3 암호 데이터(C3)를 결합하여, 하나의 암호 데이터 그룹을 생성하고, 생성된 암호 데이터 그룹을 전송할 수 있다. 또한, 제 1 암호 데이터(C1), 제 2 암호 데이터(C2), 제 3 암호 데이터(C3)를 각각 전송할 수 있으며, 이에 한정되지 않고 다양한 방법으로 제 1 암호 데이터(C1), 제 2 암호 데이터(C2),및 제 3 암호 데이터(C3)를 전송할 수 있다.

[0121] 단계 S545에서, 암호 데이터 수신 장치(300)는 획득한 암호 데이터를 획득한 사용자의 개인키를 이용하여 복호

화할 수 있다.

[0122] 일 실시예에 따르면, 암호 데이터 수신 장치(300)는 획득한 암호 데이터들(C1, C2, C3)을 획득한 개인키들(D1, D2, D3)을 이용하여 복호화 하고, 복호화한 결과값인 메시지(M)를 획득할 수 있다. 예를 들어, 암호 데이터 수신 장치(300)는 획득한 암호 데이터들(C1,C2,C3) 및 획득한 개인키들(D1, D2, D3)들을 수학식(7)에 입력하여, 메시지(M)를 획득할 수 있다.

[0123] 도 6 은 본 발명의 일 실시예에 따른 암호 데이터 수신 장치의 식별 정보 기반 암호 시스템을 설명하기 위한 블록도이다.

[0124] 일 실시예에 따르면, 개인키 생성 장치(200)는 정보 획득부(215), 파라미터 설정부(225), 개인키 생성부(235), 및 통신부(245)를 포함한다. 개인키 생성 장치(200)의 정보 획득부(215), 파라미터 설정부(225), 개인키 생성부(235),및 통신부(245)는 하나의 프로세서로 구현될 수 있으며, 복수의 프로세서로 구현될 수 있다.

[0125] 일 실시예에 따르면, 암호 데이터 전송 장치(100)는 정보 획득부(115), 암호 데이터 생성부(125),및 통신부(135)를 포함한다. 암호 데이터 전송 장치(100)의 정보 획득부(115), 파라미터 설정부(125),및 통신부(135)는 하나의 프로세서로 구현될 수 있으며, 복수의 프로세서로 구현될 수 있다.

[0126] 일 실시예에 따르면, 암호 데이터 수신 장치(300)는 정보 획득부(315), 암호 데이터 복호화부(325),및 통신부(335)를 포함한다. 암호 데이터 수신 장치(300)의 정보 획득부(315), 암호 데이터 복호화부(325),및 통신부(335)는 하나의 프로세서로 구현될 수 있으며, 복수의 프로세서로 구현될 수 있다.

[0127] 일 실시예에 따르면, 개인키 생성 장치(200)의 파라미터 설정부(225)는 마스터 키를 생성할 수 있다. 개인키 생성 장치(200)의 파라미터 설정부(225)에 의해 생성된 마스터 키는 파라미터 그룹을 포함할 수 있다. 예를 들어, 개인키 생성 장치(200)의 파라미터 설정부(225)는 난수들(α , β , ɣ , δ) 및 제 2 곱셈군 G2에 속하는 제 2 생성원(g_2)이 포함된 파라미터 그룹을 마스터키로서 설정할 수 있다.

[0128] 일 실시예에 따르면, 개인키 생성 장치(200)의 파라미터 설정부(225)는 복수의 파라미터가 포함된 공개 파라미터 그룹(PP)을 설정할 수 있다. 예를 들어, 공개 파라미터 그룹(PP)은 제 1 곱셈군에 속하는 생성원 g_1, u=(g_1)^α , v=(g_1)^β , w=(g_1)^ɣ , A=e(g_1,g_2)^β , 제 1 해쉬함수(H1), 제 2 해쉬함수(H2), 및 제 3 해쉬함수(H3)등을 포함할 수 있다.

[0129] 일 실시예에 따르면, 개인키 생성 장치(200)의 통신부(245)는 생성한 공개 파라미터 그룹을 암호 데이터 수신 장치(300) 및 암호 데이터 전송 장치(100)에 전송할 수 있다. 예를 들어, 개인키 생성 장치(200)의 통신부(245)는 생성한 공개 파라미터 그룹을 유선 통신 경로, 또는 무선 통신 경로를 이용하여 전송할 수 있으며, 이에 한정되지 않고 다양한 방법으로 공개 파라미터 그룹을 전송할 수 있다.

[0130] 일 실시예에 따르면, 암호 데이터 수신 장치(300)의 정보 획득부(315)는 사용자의 입력에 기초하여 식별 정보를 획득할 수 있다. 예를 들어, 암호 데이터 수신 장치(300)의 정보 획득부(315)는 사용자가 입력한 ID, 사용자가 입력한 전화 번호, 사용자가 입력한 주민등록 번호등을 식별 정보로서 획득할 수 있다. 또한, 암호 데이터 수신 장치(300)는 외부의 디바이스로부터 암호 데이터 수신 장치의 식별 정보를 수신할 수 있다.

[0131] 일 실시예에 따르면, 암호 데이터 수신 장치(300)의 통신부(335)는 획득한 식별 정보를 개인키 생성 장치(200)에 전송할 수 있다. 예를 들어, 암호 데이터 수신 장치(300)의 통신부(335)는 획득한 식별 정보를 유선 통신 경로, 또는 무선 통신 경로를 이용하여 획득한 사용자의 식별 정보를 전송할 수 있다.

[0132] 일 실시예에 따르면, 암호 데이터 수신 장치(300)의 통신부(335)는 획득한 식별 정보를 암호 데이터 전송 장치(100)에 전송할 수 있다. 예를 들어, 암호 데이터 수신 장치(300)의 통신부(335)는 획득한 식별 정보를 유선 통신 경로, 또는 무선 통신 경로를 이용하여 전송할 수 있다.

[0133] 일 실시예에 따르면, 개인키 생성 장치(200)의 파라미터 설정부(225)는 개인키를 생성하기 위해 복수의 난수를 생성할 수 있다. 예를 들어, 개인키 생성 장치(200)는 제 1 난수(r) 및 제 2 난수(Rid)를 생성할 수 있다.

[0134] 일 실시예에 따르면, 개인키 생성 장치(200)의 개인키 생성부(235)는 수학식(1)을 이용하여 제 1 개인키(D1)를 생성할 수 있다. 예를 들어, 개인키 생성 장치(200)의 개인키 생성부(235)는 마스터 키에 포함된 파라미터들(g_2, α , β , ɣ), 암호 데이터 수신 장치(300)의 식별 정보에 기초한 제 1 해쉬 함수값(H1(ID)), 개인키 생성 장치(200)의 파라미터 설정부(225)에의해 생성된 제 1 난수(r), 및 제 2 난수(Rid)를 이용하여 제 1 개인키(D1)를 생성할 수 있다.

[0135] 구체적으로, 개인키 생성 장치(200)의 개인키 생성부(235)는 마스터 키에 포함된 파라미터(g_2)를 밑수로 포함하고, 제 1 해쉬 함수값(H1(ID))을 지수로 포함하는 승수 인자((g_2)^H1(ID))를 생성하고, 생성된 승수 인자 및 수학식 (1)에 기초하여 제 1 개인키(D1)를 생성할 수 있다.

[0136] 일 실시예에 따르면, 개인키 생성 장치(200)의 개인키 생성부(235)는 수학식(2)을 이용하여 제 2 개인키를 생성할 수 있다. 예를 들어, 개인키 생성 장치(200)의 개인키 생성부(235)는 마스터 키에 포함된 파라미터(g_2) 및 개인키 생성 장치(200)의 파라미터 설정부(225)에 의해 생성된 제 1 난수(r)를 수학식 (2)의 입력값으로 이용하여 제 2 개인키(D2)를 생성할 수 있다.

[0137] 일 실시예에 따르면, 개인키 생성 장치(200)의 개인키 생성부(235)는 수학식(3)을 이용하여 제 3 개인키를 생성할 수 있다. 예를 들어, 개인키 생성 장치(200)의 개인키 생성부(235)는 마스터 키에 포함된 파라미터들(g_2, δ, ɣ)및 개인키 생성 장치(200)의 파라미터 설정부(225)에 의해 생성된 제 1 난수(r)를 수학식 (3)의 입력값으로 이용하여 제 3 개인키(D3)를 생성할 수 있다.

[0138] 일 실시예에 따르면, 암호 데이터 전송 장치(100)의 통신부(135)는 암호 데이터 수신 장치의 식별 정보를 개인키 생성 장치(200)로부터 수신하고, 암호 데이터 전송 장치(100)의 정보 획득부(115)는 수신한 암호 데이터 수신 장치의 식별 정보를 획득할 수 있다.

[0139] 또한, 암호 데이터 전송 장치(100)의 통신부(135)는 암호 데이터 수신 장치의 식별 정보를 암호 데이터 수신 장치(300)로부터 수신하고, 암호 데이터 전송 장치(100)의 정보 획득부(115)는 수신한 암호 데이터 수신 장치의 식별 정보를 획득할 수 있다.

[0140] 일 실시예에 따르면, 암호 데이터 수신 장치(300)의 통신부(335)는 개인키 생성 장치(200)의 통신부(245)로부터 사용자의 식별정보에 기초한 제 1 개인키(D1), 제 2 개인키(D2), 및 제 3 개인키(D3)를 수신하고, 암호 데이터 수신 장치(300)의 정보 획득부(315)는 수신한 개인키들을 획득할 수 있다.

[0141] 일 실시예에 따르면, 암호 데이터 전송 장치(100)의 암호 데이터 생성부(125)는 수학식(4-1)을 이용하여 제 1 암호 데이터(C1)를 생성할 수 있다. 예를 들어, 암호 데이터 전송 장치(100)의 암호 데이터 생성부(125)는 공개 파라미터 그룹(PP)에 포함된 공개 파라미터(A) 및 제 3 해쉬함수(H3), 획득한 난수(s), 획득한 메시지(M)를 이용하여 제 1 암호 데이터(C1)를 획득할 수 있다.

[0142] 일 실시예에 따르면, 암호 데이터 전송 장치(100)의 암호 데이터 생성부(125)는 수학식(4-2)을 이용하여 제 2 암호 데이터(C2)를 생성할 수 있다. 예를 들어, 암호 데이터 전송 장치(100)의 암호 데이터 생성부(125)는 공개 파라미터 그룹(PP)에 포함된 공개 파라미터들(u, v, w), 획득한 난수(s), 제 1 해쉬 함수 값(H1(ID)), 제 1 암호 데이터와 제 3 암호 데이터에 의해 결정되는 태그 함수값(tagC)을 이용하여 제 2 암호 데이터(C2)를 생성할 수 있다. 암호 데이터 전송 장치(100)의 암호 데이터 생성부(125)는 태그 함수값을 수학식 (5)를 이용하여 획득할 수 있다.

[0143] 일 실시예에 따르면, 암호 데이터 전송 장치(100)의 암호 데이터 생성부(125)는 공개 파라미터 그룹(PP)에 포함된 공개 파라미터(v)를 밑수로 포함하고, 획득한 암호 데이터 수신 장치의 식별 정보(H1(ID))를 지수로 포함하는 승수 인자(v^(H_1 (ID)))를 생성할 수 있다. 또한, 암호 데이터 전송 장치(100)의 암호 데이터 생성부(125)는 생성한 승수 인자(v^(H_1 (ID)))를 이용하여 제 2 암호 데이터를 생성할 수 있다. 암호 데이터 전송 장치(100)는 암호 데이터 수신 장치의 식별 정보에 기초하여 생성된 제 1 해쉬 함수값(H1(ID))을 지수 자리에 포함한 승수 인자를 이용함으로써, 제 1 해쉬 함수값(H1(ID))을 제1 곱셈군(G1) 또는 제2 곱셈군(G2)에 속하는 생성원중 하나로 매칭하는 과정을 생략할 수 있다. 그 결과, 암호 데이터 전송 장치(100)는 종래 기술에 비해 암호 데이터를 효율적으로 생성할 수 있다.

[0144] 일 실시예에 따르면, 암호 데이터 전송 장치(100)의 암호 데이터 생성부(125)는 획득한 난수(s)를 이용하여 제 3 암호 데이터를 생성할 수 있다. 예를 들어, 암호 데이터 전송 장치(100)의 암호 데이터 생성부(125)는 공개 파라미터 그룹(PP)에 포함된 공개 파라미터(g_1) 및 획득한 난수(s)를 수학식(6)에 입력하여 제 3 암호 데이터를 생성할 수 있다.

[0145] 일 실시예에 따르면, 암호 데이터 전송 장치(100)의 통신부(135)는 획득한 제 1 암호 데이터(C1), 제 2 암호 데이터(C2), 및 제 3 암호 데이터(C3)를 암호 데이터 수신 장치(300)에 전송할 수 있다.

[0146] 일 실시예에 따르면, 암호 데이터 수신 장치(300)의 통신부(335)는 암호 데이터 전송 장치(100)의 통신부로부터 제 1 암호 데이터(C1), 제 2 암호 데이터(C2), 및 제 3 암호 데이터(C3)를 수신하고, 암호 데이터 수신 장치

(300)의 정보 획득부(315)는 수신한 제 1 암호 데이터(C1), 제 2 암호 데이터(C2), 및 제 3 암호 데이터(C3)를 획득할 수 있다.

[0147] 일 실시예에 따르면, 암호 데이터 수신 장치(300)의 암호 데이터 복호화부(325)는 획득한 암호 데이터들(C1, C2, C3)을 획득한 개인키들(D1, D2, D3)을 이용하여 복호화 하고, 복호화한 결과값인 메시지(M)를 획득할 수 있다. 예를 들어, 암호 데이터 수신 장치(300)는 획득한 암호 데이터들(C1,C2,C3) 및 획득한 개인키들(D1, D2, D3)들을 수학식(7)에 입력하여, 메시지(M)를 획득할 수 있다.

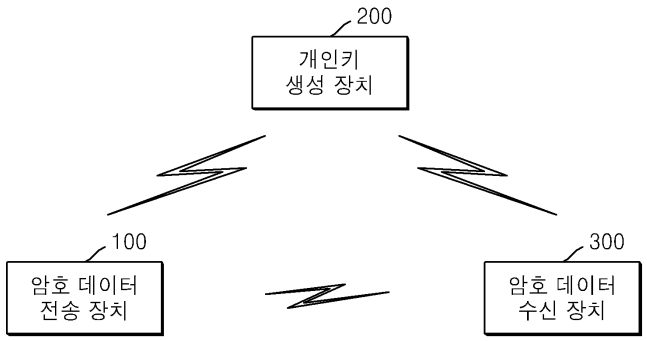
[0148] 일부 실시예는 컴퓨터에 의해 실행되는 프로그램 모듈과 같은 컴퓨터에 의해 실행가능한 명령어를 포함하는 기록 매체의 형태로도 구현될 수 있다. 컴퓨터 판독 가능 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 가용 매체일 수 있고, 휘발성 및 비휘발성 매체, 분리형 및 비분리형 매체를 모두 포함한다. 또한, 컴퓨터 판독가능 매체는 컴퓨터 저장 매체 및 통신 매체를 모두 포함할 수 있다. 컴퓨터 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술로 구현된 휘발성 및 비휘발성, 분리형 및 비분리형 매체를 모두 포함한다. 통신 매체는 전형적으로 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈, 또는 반송파와 같은 변조된 데이터 신호의 기타 데이터, 또는 기타 전송 메커니즘을 포함하며, 임의의 정보 전달 매체를 포함한다.

[0149] 전술한 본 개시의 설명은 예시를 위한 것이며, 본 개시가 속하는 기술분야의 통상의 지식을 가진 자는 본 개시의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.

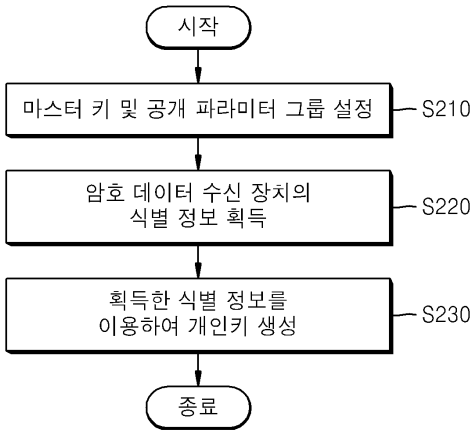
[0150] 본 개시의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 개시의 범위에 포함되는 것으로 해석되어야 한다.

도면

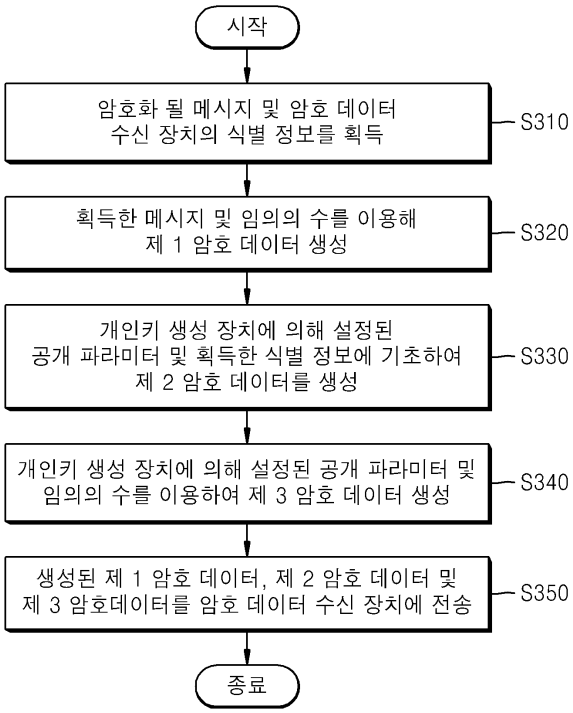
도면1



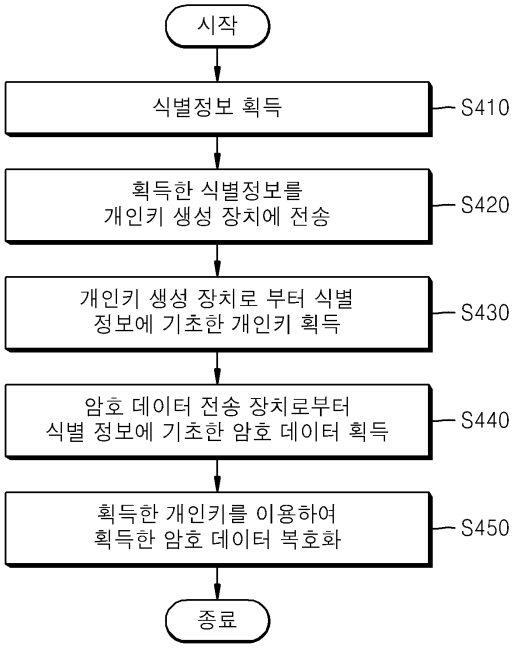
도면2


시작
마스터 키 및 공개 파라미터 그룹 설정
S210
암호 데이터 수신 장치의
식별 정보 획득
S220
획득한 식별 정보를
이용하여 개인키 생성
S230
종료

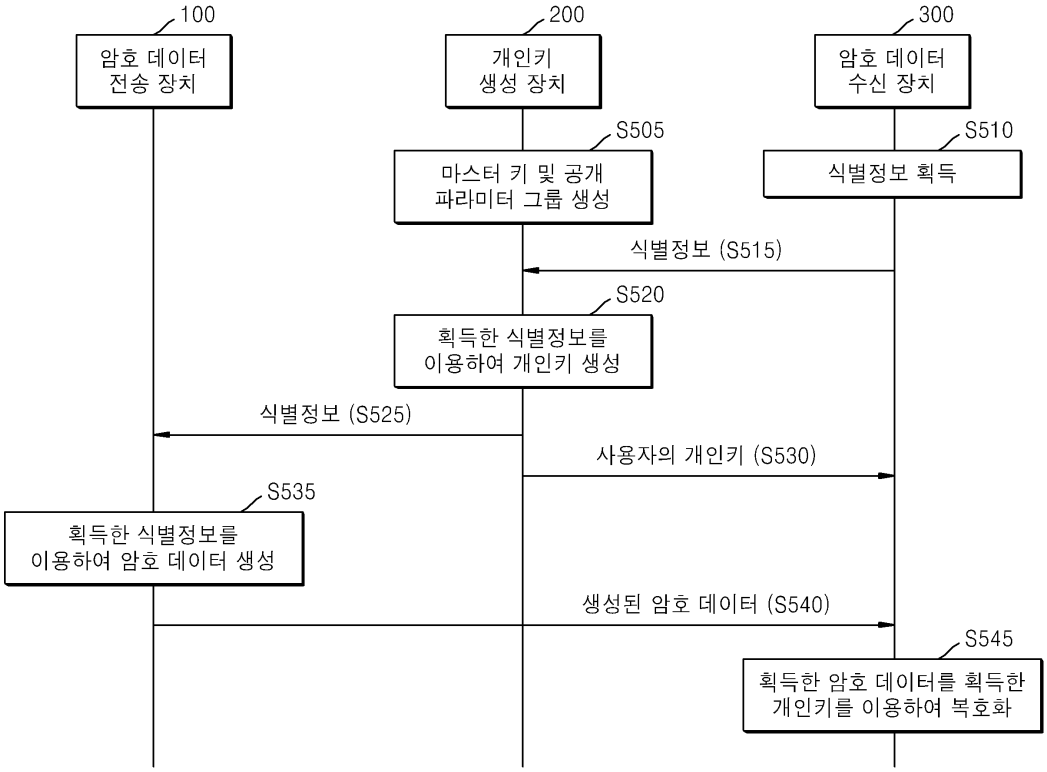
도면3


시작
암호화 될 메시지 및 암호 데이터
수신 장치의 식별 정보를 획득
S310
획득한 메시지 및 임의의 수를 이용해
제 1 암호 데이터 생성
S320
개인키 생성 장치에 의해 설정된
공개 파라미터 및 획득한 식별 정보에 기초하여
제 2 암호 데이터를 생성
S330
개인키 생성 장치에 의해 설정된 공개 파라미터 및
임의의 수를 이용하여 제 3 암호 데이터 생성
S340
생성된 제 1 암호 데이터, 제 2 암호 데이터 및
제 3 암호데이터를 암호 데이터 수신 장치에 전송
S350
종료

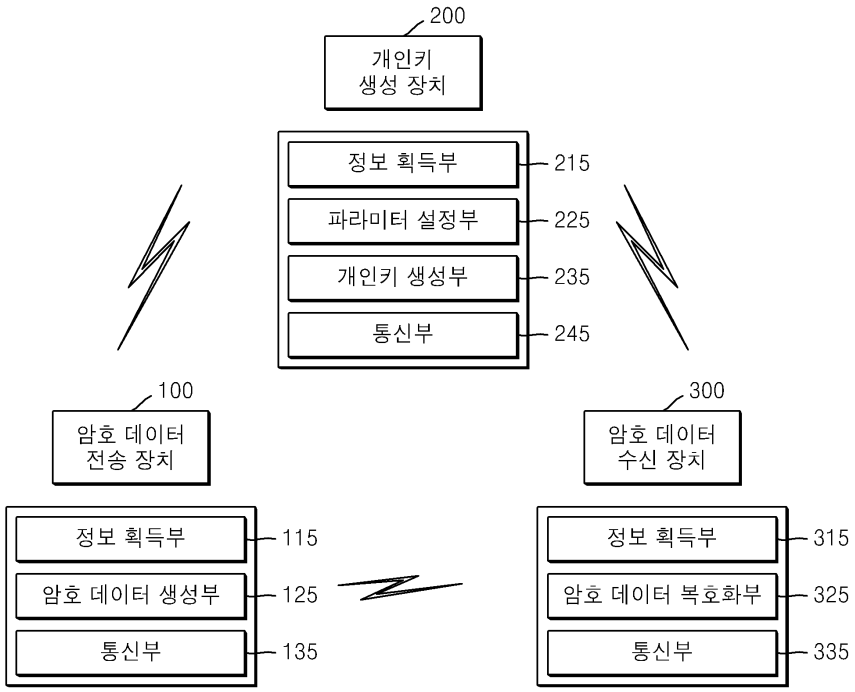
도면4


시작
식별정보 획득
S410
획득한 식별정보를
개인키 생성 장치에 전송
S420
개인키 생성 장치로 부터 식별
정보에 기초한 개인키 획득
S430
암호 데이터 전송 장치로부터
식별 정보에 기초한 암호 데이터 획득
S440
획득한 개인키를 이용하여
획득한 암호 데이터 복호화
S450
종료

도면5


100
암호 데이터
전송 장치
200
개인키
생성 장치
300
암호 데이터
수신 장치
S505
마스터 키 및 공개
파라미터 그룹 생성
S510
식별정보 획득
식별정보 (S515)
S520
획득한 식별정보를
이용하여 개인키 생성
식별정보 (S525)
사용자의 개인키 (S530)
S535
획득한 식별정보를
이용하여 암호 데이터 생성
생성된 암호 데이터 (S540)
S545
획득한 암호 데이터를 획득한
개인키를 이용하여 복호화

도면6


200
개인키
생성 장치
정보 획득부
215
파라미터 설정부
225
개인키 생성부
235
통신부
245
100
암호 데이터
전송 장치
정보 획득부
115
암호 데이터 생성부
125
통신부
135
300
암호 데이터
수신 장치
정보 획득부
315
암호 데이터 복호화부
325
통신부
335