(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2016-0042702
(43) 공개일자 2016년04월20일

(51) 국제특허분류(Int. Cl.)
H04L 9/06 (2006.01)
(21) 출원번호 10-2014-0136967
(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

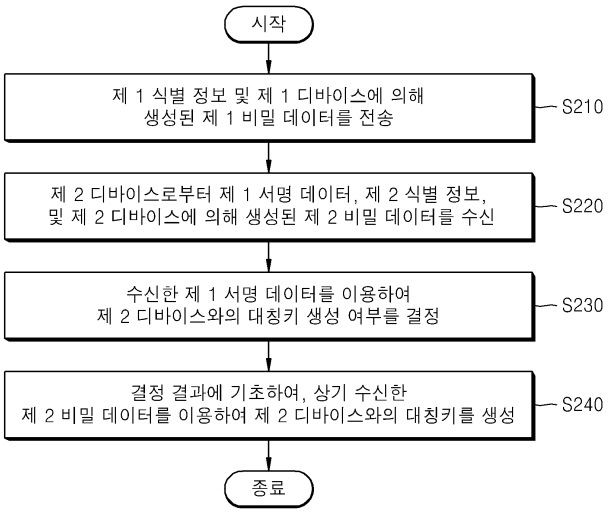
전체 청구항 수 : 총 13 항

(54) 발명의 명칭 **식별 정보를 이용하여 대칭키를 생성하는 방법 및 장치**

(57) 요 약

제 1 디바이스의 식별 정보 및 상기 제 1 디바이스에 의해 생성된 제 1 비밀 데이터를 전송하는 단계, 상기 제 2 디바이스로부터 제 1 서명 데이터, 상기 제 2 디바이스의 식별 정보, 및 상기 제 2 디바이스에 의해 생성된 제 2 비밀 데이터를 수신하는 단계, 상기 수신한 제 1 서명 데이터에 기초하여 상기 제 2 디바이스와의 대칭키 생성 여부를 결정하는 단계, 및 상기 결정하는 단계의 결과에 기초하여, 상기 수신한 제 2 비밀 데이터를 이용하여 제 2 디바이스와의 대칭키를 생성하는 단계를 포함하는 대칭키 생성 방법이 개시된다.

대 표 도 - 도2



(72) 발명자

이동훈

서울특별시 성북구 안암로 145, 미래융합관 612호 (안암동5가)

이덕기

서울특별시 서초구 신반포로3길 19, 56동 505호 (반포동)

명 세 서

청구범위

청구항 1

제 1 디바이스가 제 2 디바이스와의 대칭키를 생성하는 방법에 있어서,

상기 제 1 디바이스의 식별 정보 및 상기 제 1 디바이스에 의해 생성된 제 1 비밀 데이터를 전송하는 단계;

상기 제 2 디바이스로부터 제 1 서명 데이터, 상기 제 2 디바이스의 식별 정보, 및 상기 제 2 디바이스에 의해 생성된 제 2 비밀 데이터를 수신하는 단계;

상기 수신한 제 1 서명 데이터에 기초하여 상기 제 2 디바이스와의 대칭키 생성 여부를 결정하는 단계; 및

상기 결정하는 단계의 결과에 기초하여, 상기 수신한 제 2 비밀 데이터를 이용하여 제 2 디바이스와의 대칭키를 생성하는 단계;

를 포함하는 대칭키 생성 방법.

청구항 2

제 1 항에 있어서, 상기 대칭키 생성 방법은

상기 결정하는 단계의 결과에 기초하여, 상기 수신한 제 2 디바이스의 식별 정보, 상기 제 1 비밀 데이터, 및 상기 제 2 비밀 데이터에 상기 제 1 디바이스의 개인키로 각각 서명하여 제 2 서명 데이터를 생성하고, 상기 생성된 제 2 서명 데이터를 상기 제 2 디바이스에 전송하는 단계;

를 더 포함하는 대칭키 생성 방법.

청구항 3

제 1 항에 있어서,

상기 제 1 비밀 데이터는 상기 제 1 디바이스가 선택한 제 1 난수에 기초하여 생성되고, 상기 제 2 비밀 데이터는 상기 제 2 디바이스가 선택한 제 2 난수에 기초하여 생성된 것을 특징으로 하는 대칭키 생성 방법.

청구항 4

제 1 항에 있어서 상기 대칭키를 생성하는 단계는,

상기 제 2 비밀 데이터 및 상기 제 1 디바이스가 선택한 제 1 난수에 기초하여 대칭키를 생성하는 것을 특징으로 하는 대칭키 생성 방법.

청구항 5

제 1 항에 있어서 상기 결정하는 단계는

상기 수신한 제 2 디바이스의 식별 정보를 이용하는 것을 특징으로 하는 대칭키 생성 방법.

청구항 6

제 1항에 있어서 상기 결정하는 단계는,

상기 수신한 제 1 서명 데이터에 상기 제 2 디바이스의 개인키에 의해 각각 서명된 상기 제 1 디바이스의 식별 정보 및 상기 제 1 비밀 데이터가 포함되어 있는지 여부에 기초하여 결정하는 것을 특징으로 하는 대칭키 생성 방법.

청구항 7

제 2 디바이스와의 대칭키를 생성하는 제 1 디바이스에 있어서,

상기 제 1 디바이스의 식별 정보 및 상기 제 1 디바이스에 의해 생성된 제 1 비밀 데이터를 전송하고, 상기 제 2 디바이스로부터 제 1 서명 데이터, 상기 제 2 디바이스의 식별 정보, 및 상기 제 2 디바이스에 의해 생성된 제 2 비밀 데이터를 수신하는 통신부;

상기 수신한 제 1 서명 데이터에 기초하여 상기 제 2 디바이스와의 대칭키 생성 여부를 결정하는 결정부; 및

상기 결정 결과에 기초하여, 상기 수신한 제 2 비밀 데이터를 이용하여 제 2 디바이스와의 대칭키를 생성하는 대칭키 생성부;

를 포함하는 대칭키 생성 디바이스.

청구항 8

제 7 항에 있어서, 상기 대칭키 생성 디바이스는

상기 결정 결과에 기초하여, 상기 수신한 제 2 디바이스의 식별 정보, 상기 제 1 비밀 데이터, 및 상기 제 2 비밀 데이터에 상기 제 1 디바이스의 개인키로 각각 서명하여 제 2 서명 데이터를 생성하는 서명 데이터 생성부를 더 포함하고,

상기 통신부는 상기 생성된 제 2 서명 데이터를 상기 제 2 디바이스에 전송하는 것을 특징으로 하는 대칭키 생성 디바이스.

청구항 9

제 7 항에 있어서,

상기 제 1 비밀 데이터는 상기 제 1 디바이스가 선택한 제 1 난수에 기초하여 생성되고, 상기 제 2 비밀 데이터는 상기 제 2 디바이스가 선택한 제 2 난수에 기초하여 생성된 것을 특징으로 하는 대칭키 생성 디바이스.

청구항 10

제 7 항에 있어서 상기 대칭키 생성부는,

상기 제 2 비밀 데이터 및 상기 제 1 디바이스가 선택한 제 1 난수에 기초하여 대칭키를 생성하는 것을 특징으로 하는 대칭키 생성 디바이스.

청구항 11

제 7 항에 있어서 상기 결정부는

상기 수신한 제 2 디바이스의 식별 정보를 이용하는 것을 특징으로 하는 대칭키 생성 디바이스.

청구항 12

제 7항에 있어서 상기 결정부는,

상기 수신한 제 1 서명 데이터에 상기 제 2 디바이스의 개인키에 의해 각각 서명된 상기 제 1 디바이스의 식별 정보 및 상기 제 1 비밀 데이터가 포함되어 있는지 여부에 기초하여 결정하는 것을 특징으로 하는 대칭키 생성 디바이스.

청구항 13

제 1 항 내지 제 6 항중 어느 한 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

발명의 설명

기 술 분 야

[0001] 본 발명은 식별 정보를 이용하여 대칭키를 생성하는 방법에 관한 것이다.

배 경 기 술

[0002] 식별 정보(ID)기반 암호 기법은 암호문 생성자가 암호문 수신자의 공개키 인증서가 없이도 수신자의 이메일과 같은 공개된 정보를 식별 정보(ID)로 이용하여 암호문을 생성할 수 있는 시스템이다.

[0003] 다만, 이와 같은 식별 정보(ID)기반 암호 기법은 암호문을 생성하는데 많은 시간 지연이 발생하는 문제점이 있어, 다량의 데이터를 교환하는데 적합하지 않다. 이에 반해, 대칭키 기반 암호 기법은 암호문을 생성하는데 시간 지연이 발생하지 않아 다량의 데이터를 교환하는데 적합하다.

[0004] 따라서, 식별 정보(ID)기반 암호 기법을 이용하여 대칭키를 생성하는 방법이 연구되고 있다.

발명의 내용

해결하려는 과제

[0005] 본 발명은 식별 정보(ID)를 이용하여 효율적으로 대칭키를 생성하는 방법을 제공하고자 한다.

과제의 해결 수단

[0006] 상술한 기술적 과제를 달성하기 위한 기술적 수단으로서, 본 발명의 1 측면은 상기 제 1 디바이스의 식별 정보 및 상기 제 1 디바이스에 의해 생성된 제 1 비밀 데이터를 전송하는 단계, 상기 제 2 디바이스로부터 제 1 서명 데이터, 상기 제 2 디바이스의 식별 정보, 및 상기 제 2 디바이스에 의해 생성된 제 2 비밀 데이터를 수신하는 단계, 상기 수신한 제 1 서명 데이터에 기초하여 상기 제 2 디바이스와의 대칭키 생성 여부를 결정하는 단계, 및 상기 결정하는 단계의 결과에 기초하여, 상기 수신한 제 2 비밀 데이터를 이용하여 제 2 디바이스와의 대칭키를 생성하는 단계를 포함하는 대칭키 생성 방법을 제공 한다.

[0007] 또한, 상기 대칭키 생성 방법은 상기 결정하는 단계의 결과에 기초하여, 상기 수신한 제 2 디바이스의 식별 정보, 상기 제 1 비밀 데이터, 및 상기 제 2 비밀 데이터에 상기 제 1 디바이스의 개인키로 각각 서명하여 제 2 서명 데이터를 생성하고, 상기 생성된 제 2 서명 데이터를 상기 제 2 디바이스에 전송하는 단계를 더 포함할 수 있다.

[0008] 또한, 상기 제 1 비밀 데이터는 상기 제 1 디바이스가 선택한 제 1 난수에 기초하여 생성되고, 상기 제 2 비밀 데이터는 상기 제 2 디바이스가 선택한 제 2 난수에 기초하여 생성될 수 있다.

[0009] 또한, 상기 대칭키를 생성하는 단계는, 상기 제 2 비밀 데이터 및 상기 제 1 디바이스가 선택한 제 1 난수에 기초하여 대칭키를 생성할 수 있다.

[0010] 또한, 상기 결정하는 단계는 상기 수신한 제 2 디바이스의 식별 정보를 이용할 수 있다.

[0011] 또한, 상기 결정하는 단계는 상기 수신한 제 1 서명 데이터에 상기 제 2 디바이스의 개인키에 의해 각각 서명된 상기 제 1 디바이스의 식별 정보 및 상기 제 1 비밀 데이터가 포함되어 있는지 여부에 기초하여 제 2 디바이스와의 대칭키 생성 여부를 결정할 수 있다.

[0012] 또한, 제 2 측면은 상기 제 1 디바이스의 식별 정보 및 상기 제 1 디바이스에 의해 생성된 제 1 비밀 데이터를 전송하고, 상기 제 2 디바이스로부터 제 1 서명 데이터, 상기 제 2 디바이스의 식별 정보, 및 상기 제 2 디바이스에 의해 생성된 제 2 비밀 데이터를 수신하는 통신부, 상기 수신한 제 1 서명 데이터가 상기 전송한 제 1 디바이스의 식별 정보 및 상기 제 1 비밀 데이터에 기초하여 생성되었는지 여부를 결정하는 결정부, 및 상기 결정 결과에 기초하여, 상기 수신한 제 2 비밀 데이터를 이용하여 제 2 디바이스와의 대칭키를 생성하는 대칭키 생성부를 포함하는 대칭키 생성 디바이스를 제공한다.

[0013] 또한, 상기 대칭키 생성 디바이스는 상기 결정결과에 기초하여, 상기 수신한 제 2 디바이스의 식별 정보, 상기 제 1 비밀 데이터, 및 상기 제 2 비밀 데이터에 상기 제 1 디바이스의 개인키로 각각 서명하여 제 2 서명 데이터를 생성하는 서명 데이터 생성부를 더 포함하고, 상기 통신부는 상기 생성된 제 2 서명 데이터를 상기 제 2 디바이스에 전송할 수 있다.

[0014] 또한, 상기 제 1 비밀 데이터는 상기 제 1 디바이스가 선택한 제 1 난수에 기초하여 생성되고, 상기 제 2 비밀 데이터는 상기 제 2 디바이스가 선택한 제 2 난수에 기초하여 생성될 수 있다.

[0015] 또한, 상기 대칭키 생성부는 상기 제 2 비밀 데이터 및 상기 제 1 디바이스가 선택한 제 1 난수에 기초하여 대칭키를 생성할 수 있다.

[0016] 또한, 상기 결정부는 상기 수신한 제 2 디바이스의 식별 정보를 이용할 수 있다.

[0017] 또한, 상기 결정부는 상기 수신한 제 1 서명 데이터에 상기 제 2 디바이스의 개인키에 의해 각각 서명된 상기 제 1 디바이스의 식별 정보 및 상기 제 1 비밀 데이터가 포함되어 있는지 여부에 기초하여 제 2 디바이스와의 대칭키 생성 여부를 결정할 수 있다.

도면의 간단한 설명

[0018] 도 1 은 본 발명의 일 실시예에 따른, 대칭키를 생성하는 시스템을 설명하기 위한 개략도이다.

도 2 는 본 발명의 일 실시예에 따라, 제 1 디바이스가 대칭키를 생성하는 방법을 설명하기 위한 순서도이다.

도 3 은 본 발명의 일 실시예에 따라, 제 2 디바이스가 대칭키를 생성하는 방법을 설명하기 위한 순서도이다.

도 4 는 본 발명의 일 실시예에 따라, 대칭키를 생성하는 시스템을 설명하기 위한 순서도 이다.

도 5 는 본 발명의 일 실시예에 따라 식별 정보에 기반하여 대칭키를 생성하는 시스템을 설명하기 위한 순서도이다.

도 6 은 다른 실시예에 따라 식별 정보에 기반하여 대칭키를 생성하는 시스템을 설명하기 위한 순서도이다.

도 7 은 다른 실시예에 따라, 대칭키를 생성하는 시스템을 설명하기 위한 블록도이다.

도 8은 본 발명의 일 실시예에 따라, 대칭키를 생성하는 디바이스를 설명하기 위한 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0019] 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.

[0020] 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.

[0021] 명세서 전체에서, 제 1 디바이스(100)는 통신이 가능한 디바이스를 포함할 수 있다. 예를 들어, 핸드폰, 테블릿 컴퓨터,및 컴퓨터등을 포함할 수 있으며, 이에 한정되지 않고 통신이 가능한 모든 디바이스를 포함할 수 있다.

[0022] 명세서 전체에서, 제 2 디바이스(200)는 통신이 가능한 디바이스를 포함할 수 있다. 예를 들어, 핸드폰, 테블릿 컴퓨터,및 컴퓨터등을 포함할 수 있으며, 이에 한정되지 않고 통신이 가능한 모든 디바이스를 포함할 수 있다.

[0023] 이하 첨부된 도면을 참고하여 본 발명을 상세히 설명하기로 한다.

[0024] 도 1 은 본 발명의 일 실시예에 따른, 대칭키를 생성하는 시스템을 설명하기 위한 개략도이다.

[0025] 도 1 에 도시된 바와 같이, 본 발명의 사용자 식별정보에 기초한 암호화 방법을 구현하는 시스템은 개인키 생성 장치(300), 제 1 디바이스(100), 및 제 2 디바이스(200)를 포함한다.

[0026] 일 실시예에 따르면 제 1 디바이스(100)는 제 1 식별 정보를 획득할 수 있다. 또한, 제 2 디바이스(200)는 제2 식별 정보를 획득할 수 있다. 제 1 디바이스(100) 및 제 2 디바이스(200)는 제 1 식별정보와 제 2 식별정보를 개인키 생성 장치(300)에 전송하고, 각각의 식별정보에 대응되는 개인키를 개인키 생성 장치(300)로부터 획득할 수 있다.

[0027] 제 1 디바이스(100)는 제 1 비밀 데이터를 생성할 수 있다. 또한, 획득한 제 1 식별 정보 및 제 1 비밀 데이터를 제 2 디바이스(200)에 전송할 수 있다.

[0028] 제 2 디바이스(200)는 수신한 제 1 비밀 데이터 및 제 1 식별 정보에 제 2 디바이스(200)의 개인키로 서명하여 제 1 서명 데이터를 생성할 수 있다. 또한, 제 2 비밀 데이터를 생성할 수 있다.

[0029] 제 2 디바이스(200)는 제 1 서명 데이터, 제 2 비밀 데이터, 및 제 2 식별 정보를 제 1 디바이스(100)에 전송할

수 있다.

[0030] 제 1 디바이스(100)는 수신한 제 2 식별정보를 공개키로 이용하여 제 1 서명 데이터를 분석 함으로써, 제 2 디바이스(200)와의 대칭키 생성 여부를 결정할 수 있다. 제 1 디바이스(100)는 대칭키를 생성한다고 결정한 경우, 제 2 디바이스(200)로부터 수신한 제 2 비밀 데이터를 이용하여 대칭키를 생성할 수 있다.

[0031] 제 1 디바이스(100)는 생성된 대칭키를 이용하여 데이터를 암호화 하고, 암호화된 데이터를 제 2 디바이스(200)와 교환할 수 있다.

[0032] 도 2 는 본 발명의 일 실시예에 따라, 제 1 디바이스가 대칭키를 생성하는 방법을 설명하기 위한 순서도이다.

[0033] 단계 S210에서, 제 1 디바이스는 제 1 식별 정보 및 제 1 디바이스에 의해 생성된 제 1 비밀 데이터를 전송할 수 있다.

[0034] 일 실시예에 따르면, 제 1 디바이스(100)는 제 1 식별 정보를 획득할 수 있다. 제 1 식별 정보는 제 1 디바이스(100)를 나타내는 정보 또는 제 1 디바이스(100)의 사용자를 나타내는 정보를 포함할 수 있다. 예를 들어,제 1 식별 정보는 제 1 디바이스(100) 사용자의 전화번호, 사용자의 주민등록 번호, 사용자의 이메일 주소등을 포함할 수 있다. 또한, 제 1 식별 정보는 제 1 디바이스(100)의 제품 번호, 제 1 디바이스(100)의 제조 일자 등을 포함할 수 있으며, 이에 한정되지 않고 제 1 디바이스(100) 또는 제 1 디바이스(100)의 사용자를 나타내는 소정의 정보를 포함할 수 있다. 제 1 디바이스(100)는 제 1 식별 정보를 생성할 수 있고, 사용자의 입력에 기초하여 획득할 수 있으며, 외부의 디바이스로부터 수신할 수 있다.

[0035] 일 실시예에 따르면, 제 1 디바이스(100)는 제 1 비밀 데이터를 생성할 수 있다. 예를 들어, 제 1 디바이스(100)는 제 1 비밀 데이터를 생성하기 위해 난수(a)를 선택할 수 있다. 또한, 선택한 난수(a)를 이용하여 제 1 비밀 데이터를 생성할 수 있다.

[0036] 제 1 비밀데이터 = G^a - 수학식(1)

[0037] 일 실시예에 따르면, 제 1 디바이스(100)는 수학식(1)을 이용하여 제 1 비밀데이터를 생성할 수 있다. 예를 들어, 제 1 디바이스(100)는 개인키 생성 장치(300)에 의해 설정된 공개 파라미터 그룹(PP)에 포함된 파라미터(G) 및, 선택한 난수(a)를 수학식(1)에 입력하여 제 1 비밀데이터를 생성할 수 있다.

[0038] 일 실시예에 따르면, 제 1 디바이스(100)는 획득한 제 1 디바이스의 식별정보 및 제 1 비밀데이터를 제 2 디바이스(200)에 전송할 수 있다. 제 1 디바이스(100)는 유선 통신 경로, 또는 무선 통신 경로를 이용하여 전송할 수 있다.

[0039] 단계 S220에서, 제 1 디바이스는 제 2 디바이스로부터 제 1 서명 데이터, 제 2 식별 정보, 및 제 2 디바이스에 의해 생성된 제 2 비밀 데이터를 수신할 수 있다.

[0040] 일 실시예에 따르면, 제 2 디바이스(200)는 제 2 식별 정보를 획득할 수 있다. 제 2 식별 정보는 제 2 디바이스(200)를 나타내는 정보 또는 제 2 디바이스(200)의 사용자를 나타내는 정보를 포함할 수 있다. 예를 들어,제 2 식별 정보는 제 2 디바이스(200) 사용자의 전화번호, 사용자의 주민등록 번호, 사용자의 이메일 주소등을 포함할 수 있다. 또한, 제 2 식별 정보는 제 2 디바이스(200)의 제품 번호, 제 2 디바이스(200)의 제조 일자 등을 포함할 수 있으며, 이에 한정되지 않고 제 2 디바이스(200) 또는 제 2 디바이스(200)의 사용자를 나타내는 소정의 정보를 포함할 수 있다. 제 2 디바이스(200)는 제 2 식별 정보를 생성할 수 있고, 사용자의 입력에 기초하여 획득할 수 있으며, 외부의 디바이스로부터 수신할 수 있다.

[0041] 일 실시예에 따르면, 제 2 디바이스(200)는 제 2 비밀 데이터를 생성할 수 있다. 예를 들어, 제 2 디바이스(200)는 제 2 비밀 데이터를 생성하기 위해 난수(b)를 선택할 수 있다. 또한, 선택한 난수(b)를 이용하여 제 2 비밀 데이터를 생성할 수 있다.

[0042] 제 2 비밀데이터 = G^b - 수학식(2)

[0043] 일 실시예에 따르면, 제 2 디바이스(200)는 수학식(2)을 이용하여 제 2 비밀 데이터를 생성할 수 있다. 예를 들어, 제 2 디바이스(200)는 개인키 생성 장치(300)에 의해 설정된 공개 파라미터 그룹(PP)에 포함된 파라미터(G) 및, 선택한 난수(b)를 수학식(2)에 입력하여 제 2 비밀데이터를 생성할 수 있다.

[0044] 일 실시예에 따르면, 제 2 디바이스(200)는 수신한 제 1 식별 정보에 제 2 디바이스(200)의 개인키로 서명할 수 있다. 예를 들어, 제 2 디바이스(200)는 소정의 알고리즘에 제 1 식별 정보 및 제 2 디바이스(200)의 개인키를 입력하여, 제 1 식별 정보의 서명 데이터를 획득할 수 있다.

[0045] 일 실시예에 따르면, 제 2 디바이스(200)는 수신한 제 1 비밀 데이터에 제 2 디바이스(200)의 개인키로 서명할 수 있다. 예를 들어, 제 2 디바이스(200)는 소정의 알고리즘에 제 1 비밀 데이터 및 제 2 디바이스(200)의 개인키를 입력하여, 제 1 비밀 데이터의 서명 데이터를 획득할 수 있다.

[0046] 일 실시예에 따르면, 제 2 디바이스(200)는 제 1 서명 데이터를 획득할 수 있다. 예를 들어, 제 2 디바이스(200)는 제 1 식별 정보에 제 2 디바이스(200)의 개인키로 서명하여 생성된 제 1 식별 정보의 서명 데이터 및 제 1 비밀 데이터에 제 2 디바이스(200)의 개인키로 서명하여 생성된 제 1 비밀 데이터의 서명 데이터를 결합하여 제 1 서명 데이터를 획득할 수 있다. 제 2 디바이스(200)는 획득한 제 1 서명 데이터를 제 1 디바이스(100)에 전송할 수 있다.

[0047] 일 실시예에 따르면, 제 1 디바이스(100)는 제 2 식별 정보, 제 2 디바이스(200)에 의해 생성된 제 1 서명데이터,및 제 2 비밀 데이터를 수신할 수 있다. 예를 들어, 제 1 디바이스(100)는 유선 통신 경로를 통하여 제 1 서명 데이터, 제 2 식별 정보, 및 제 2 비밀 데이터를 획득할 수 있고, 무선 통신 경로를 이용하여 획득할 수 있다.

[0048] 단계 S230에서, 제 1 디바이스(100)는 수신한 제 1 서명 데이터를 이용하여 제 2 디바이스(200)와의 대칭키 생성여부를 결정할 수 있다.

[0049] 일 실시예에 따르면, 제 1 디바이스(100)는 수신한 제 1 서명 데이터를 분석할 수 있다. 예를 들어, 제 1 디바이스(100)는 수신한 제 1 서명 데이터를 수신한 제 2 식별 정보를 이용하여 분석할 수 있다. 구체적으로, 제 1 디바이스(100)는 제 2 식별 정보를 공개키로 이용하여, 수신한 제 1 서명 데이터에 제 2 디바이스의 개인키로 서명된 제 1 식별 정보가 포함되어 있는지 여부를 판단할 수 있다.

[0050] 또한, 제 1 디바이스(100)는 제 2 식별 정보를 공개키로 이용하여, 수신한 제 1 서명 데이터에 제 2 디바이스의 개인키로 서명된 제 1 비밀데이터가 포함되어 있는지 여부를 판단할 수 있다.

[0051] 제 1 디바이스(100)는 수신한 제 1 서명 데이터에 서명된 제 1 식별 정보 및 2 디바이스의 개인키로 서명된 제 1 비밀데이터가 포함되어 있는 경우, 제 2 디바이스(200)와의 대칭키를 생성한다고 결정할 수 있다.

[0052] 또한, 제 1 디바이스(100)는 수신한 제 1 서명 데이터에 제 2 디바이스의 개인키로 서명된 제 1 식별 정보 또는 제 2 디바이스의 개인키로 서명된 제 1 비밀 데이터가 포함되어 있지 않은 경우, 제 2 디바이스와의 대칭키를 생성하지 않는다고 결정할 수 있다.

[0053] 단계 S240에서, 제 1 디바이스(100)는 결정하는 단계의 결과에 기초하고, 수신한 제 2 비밀데이터를 이용하여 제 2 디바이스와의 대칭키를 생성할 수 있다.

[0054] 일 실시예에 따르면, 제 1 디바이스(100)는 대칭키를 생성한다고 결정한 경우, 제 2 디바이스와의 대칭키를 생성할 수 있다.

[0055] 대칭키 = $(G^b)^a$ - 수학식(3)

[0056] 예를 들어, 제 1 디바이스(100)는 수학식(3), 제 2 비밀 데이터(G^b), 제 1 디바이스(100)에 의해 선택된 난수(a)를 이용하여 대칭키를 생성할 수 있다. 또한, 제 1 디바이스(100)는 소정의 알고리즘에 제 2 비밀 데이터(G^b) 및 난수(a)를 입력하여 대칭키를 생성할 수 있다.

[0057] 제 1 디바이스(100)는 대칭키를 생성하지 않는다고 결정한 경우, 제 2 디바이스와의 대칭키를 생성하지 않고, 수신한 제 1 서명 데이터, 제 2 식별 정보, 및 제 2 비밀 데이터를 삭제할 수 있다.

[0058] 도 3 은 본 발명의 일 실시예에 따라, 제 2 디바이스가 대칭키를 생성하는 방법을 설명하기 위한 순서도이다.

[0059] 단계 S310에서, 제 2 디바이스는 제 1 식별 정보 및 제 1 디바이스에 의해 생성된 제 1 비밀 데이터를 수신할 수 있다.

[0060] 일 실시예에 따르면, 제 2 디바이스(200)는 제 1 디바이스로부터 제 1 식별 정보 및 제 1 비밀데이터를 수신할 수 있다. 예를 들어, 제 2 디바이스(200)는 제 1 식별 정보 및 제 1 비밀데이터를 유선 통신 경로를 이용하여 획득할 수 있고, 무선 통신 경로를 이용하여 획득할 수 있다.

[0061] 단계 S320에서, 제 2 디바이스는 제 1 서명 데이터 및 제 2 비밀 데이터를 생성할 수 있다.

[0062] 일 실시예에 따르면, 제 2 디바이스(200)는 수신한 제 1 식별 정보에 제 2 디바이스(200)의 개인키로 서명할 수 있다. 예를 들어, 제 2 디바이스(200)는 소정의 알고리즘에 제 1 식별 정보 및 제 2 디바이스(200)의 개인키를 입력하여, 서명 데이터를 획득할 수 있다.

[0063] 일 실시예에 따르면, 제 2 디바이스(200)는 수신한 제 1 비밀 데이터에 제 2 디바이스(200)의 개인키로 서명할 수 있다. 예를 들어, 제 2 디바이스(200)는 소정의 알고리즘에 제 1 비밀 데이터 및 제 2 디바이스(200)의 개인키를 입력하여, 서명 데이터를 획득할 수 있다.

[0064] 일 실시예에 따르면, 제 2 디바이스(200)는 제 1 서명 데이터를 획득할 수 있다. 예를 들어, 제 2 디바이스(200)는 제 1 식별 정보를 이용하여 생성된 서명 데이터 및 제 1 비밀 데이터를 이용하여 생성된 서명 데이터를 결합하여 제 1 서명 데이터를 획득할 수 있다.

[0065] 일 실시예에 따르면, 제 2 디바이스(200)는 제 2 비밀 데이터를 생성할 수 있다. 예를 들어, 제 2 디바이스(200)는 제 2 비밀 데이터를 생성하기 위해 난수(b)를 선택할 수 있다. 또한, 선택한 난수(b)를 이용하여 제 2 비밀 데이터를 생성할 수 있다. 예를 들어, 제 2 디바이스(200)는 개인키 생성 장치(300)에 의해 설정된 공개 파라미터 그룹(PP)에 포함된 파라미터(G) 및, 선택한 난수(b)를 수학식(2)에 입력하여 제 2 비밀데이터를 생성할 수 있다.

[0066] 단계 S330에서, 제 2 디바이스는 제 1 서명 데이터, 제 2 식별 정보,및 제 2 비밀 데이터를 전송할 수 있다.

[0067] 일 실시예에 따르면, 제 2 디바이스(200)는 제 1 서명데이터, 제 2 식별 정보, 및 제 2 비밀 데이터를 제 1 디바이스(100)에게 전송할 수 있다. 예를 들어, 제 2 디바이스(200)는 제 1 서명 데이터, 제 2 식별 정보, 및 제 2 비밀 데이터를 함께 전송할 수 있고, 각각 전송할 수 있다.

[0068] 단계 S340에서, 제 2 디바이스(200)는 제 2 서명 데이터를 제 1 디바이스(100)로부터 수신할 수 있다.

[0069] 일 실시예에 따르면, 제 1 디바이스(100)는 제 2 서명 데이터를 생성할 수 있다. 예를 들어, 제 1 디바이스(100)는 제 2 디바이스(200)와의 대칭키를 생성한다고 결정한 경우, 제 2 서명 데이터를 획득할 수 있다.

[0070] 일 실시예에 따르면, 제 1 디바이스(100)는 수신한 제 2 식별 정보에 제 1 디바이스(100)의 개인키로 서명할 수 있다. 예를 들어, 제 1 디바이스(100)는 소정의 알고리즘에 제 2 식별 정보 및 제 1 디바이스(100)의 개인키를 입력하여, 제 2 식별 정보의 서명 데이터를 획득할 수 있다.

[0071] 일 실시예에 따르면, 제 1 디바이스(100)는 수신한 제 2 비밀 데이터에 제 1 디바이스(100)의 개인키로 서명할 수 있다. 예를 들어, 제 1 디바이스(100)는 소정의 알고리즘에 제 2 비밀 데이터 및 제 1 디바이스(100)의 개인키를 입력하여, 제 2 비밀 데이터의 서명 데이터를 획득할 수 있다.

[0072] 일 실시예에 따르면, 제 1 디바이스(100)는 생성한 제 1 비밀 데이터에 제 1 디바이스(100)의 개인키로 서명할 수 있다. 예를 들어, 제 1 디바이스(100)는 소정의 알고리즘에 제 1 비밀 데이터 및 제 1 디바이스(100)의 개인키를 입력하여, 제 1 비밀 데이터의 서명 데이터를 획득할 수 있다.

[0073] 일 실시예에 따르면, 제 1 디바이스(100)는 제 2 서명 데이터를 생성할 수 있다. 예를 들어, 제 1 디바이스(100)는 제 2 식별 정보를 이용하여 생성된 서명 데이터, 제 1 비밀 데이터를 이용하여 생성된 서명 데이터, 및 제 2 비밀 데이터를 이용하여 생성된 서명 데이터를 결합하여 제 2 서명 데이터를 획득할 수 있다.

[0074] 일 실시예에 따르면, 제 2 디바이스(200)는 제 1 디바이스(100)에 의해 생성된 제 2 서명 데이터를 수신할 수 있다. 예를 들어, 제 2 디바이스(200)는 유선 통신 경로 또는 무선 통신 경로를 이용하여, 제 1 디바이스(100)로부터 제 2 서명 데이터를 수신할 수 있다.

[0075] 단계 S350에서, 제 2 디바이스(200)는 수신한 제 2 서명 데이터에 기초하여 제 1 디바이스(100)와의 대칭키 생성 여부를 결정할 수 있다.

[0076] 일 실시예에 따르면, 제 2 디바이스(200)는 수신한 제 2 서명 데이터를 분석할 수 있다. 예를 들어, 제 1 디바이스(100)는 수신한 제 2 서명 데이터를 제 1 식별 정보를 이용하여 분석할 수 있다. 구체적으로, 제 2 디바이스(200)는 제 1 식별 정보를 공개키로 이용하여, 수신한 제 2 서명 데이터에 제 1 디바이스의 개인키로 서명된 제 2 식별 정보가 포함되어 있는지 여부를 판단할 수 있다.

[0077] 또한, 제 2 디바이스(200)는 제 1 식별 정보를 공개키로 이용하여, 수신한 제 2 서명 데이터에 제 1 디바이스의 개인키로 서명된 제 2 비밀데이터가 포함되어 있는지 여부를 판단할 수 있다.

[0078] 또한, 제 2 디바이스(200)는 제 1 식별 정보를 공개키로 이용하여, 수신한 제 2 서명 데이터에 제 1 디바이스의 개인키로 서명된 제 1 비밀데이터가 포함되어 있는지 여부를 판단할 수 있다.

[0079] 제 2 디바이스(200)는 수신한 제 2 서명 데이터에 제 1 디바이스의 개인키로 서명된 제 1 식별 정보, 제 1 디바이스의 개인키로 서명된 제 1 비밀 데이터,및 제 1 디바이스의 개인키로 서명된 제 2 비밀데이터가 포함되어 있는 경우, 제 1 디바이스(100)와의 대칭키를 생성한다고 결정할 수 있다.

[0080] 또한, 제 2 디바이스(200)는 수신한 제 2 서명 데이터에 제 1 디바이스의 개인키로 서명된 제 2 식별 정보, 제 1 디바이스의 개인키로 서명된 제 1 비밀 데이터, 또는 제 1 디바이스의 개인키로 서명된 제 2 비밀 데이터가 포함되어 있지 않은 경우, 제 1 디바이스(100)와의 대칭키를 생성하지 않는다고 결정할 수 있다.

[0081] 단계 S360에서, 제 2 디바이스(200)는 결정하는 단계의 결과에 기초하여, 제 1 디바이스와의 대칭키를 생성할 수 있다.

[0082] 일 실시예에 따르면, 제 2 디바이스(200)는 제 1 디바이스(100)와의 대칭키를 생성한다고 결정한 경우, 제 1 디바이스와의 대칭키를 생성할 수 있다.

[0083] 대칭키 = (G^a)^b - 수학식(4)

[0084] 예를 들어, 제 2 디바이스(200)는 수학식(4)에, 제 1 비밀 데이터(G^a) 및 난수(b)를 입력하여 대칭키를 생성할 수 있다. 또한, 제 2 디바이스(200)는 소정의 알고리즘에 제 1 비밀 데이터(G^a) 및 난수(b)를 입력하여 대칭키를 생성할 수 있다.

[0085] 제 2 디바이스(200)는 제 1 디바이스(100)와의 대칭키를 생성하지 않는다고 결정한 경우, 제 1 디바이스와의 대칭키를 생성하지 않고, 수신한 제 2 서명 데이터를 삭제할 수 있다.

[0086] 도 4 는 본 발명의 일 실시예에 따라, 대칭키를 생성하는 시스템을 설명하기 위한 순서도 이다.

[0087] 단계 s405에서, 제 1 디바이스(100)는 제 1 식별 정보를 획득할 수 있다. 예를 들어,제 1 디바이스(100)는 제 1 디바이스(100) 사용자의 전화번호, 사용자의 주민등록 번호, 사용자의 이메일 주소 또는 제 1 디바이스(100)의 제품 번호, 제 1 디바이스(100)의 제조 일자 등을 획득할 수 있으며, 이에 한정되지 않고 제 1 디바이스(100) 또는 제 1 디바이스(100)의 사용자를 나타내는 소정의 정보를 획득할 수 있다.

[0088] 단계 s410에서, 제 2 디바이스(200)는 제 2 식별 정보를 획득할 수 있다. 예를 들어, 제 2 디바이스(200)는 제 2 디바이스(200) 사용자의 전화번호, 사용자의 주민등록 번호, 사용자의 이메일 주소 또는 제 2 디바이스(200)의 제품 번호, 제 2 디바이스(200)의 제조 일자 등을 획득할 수 있으며, 이에 한정되지 않고 제 2 디바이스(200) 또는 제 2 디바이스(200)의 사용자를 나타내는 소정의 정보를 획득할 수 있다.

[0089] 단계 s415에서 개인키 생성 장치(300)는 제 1 식별 정보 및 제 2 식별 정보를 수신하여, 식별 정보들 각각에 대응되는 개인키를 생성할 수 있다.

[0090] 일 실시예에 따르면, 개인키 생성 장치(300)는 복수의 파라미터가 포함된 공개 파라미터 그룹(PP)을 설정할 수 있다. 공개 파라미터 그룹(PP)은 제 1 디바이스(100), 제 2 디바이스(200), 및 개인키 생성 장치(300)에 의해 사용되는 공개 파라미터들의 집합을 의미한다. 개인키 생성 장치(300)는 공개 파라미터 그룹(PP)을 생성하고, 생성된 파라미터 그룹(PP)을 제 1 디바이스(100)및 제 2 디바이스(200)에 전송할 수 있다.

[0091] 일 실시예에 따르면, 개인키 생성 장치(300)는 제 1 식별 정보 및 제 2 식별 정보에 각각 대응되는 개인키를 생성할 수 있다. 예를 들어, 개인키 생성 장치(300)는 제 1 식별 정보 및 공개 파라미터 그룹(PP)에 포함된 파라미터들을 소정의 알고리즘에 입력하여, 제 1 디바이스(100)의 개인키를 생성할 수 있다. 또한, 개인키 생성 장치(300)는 공개 파라미터 그룹(PP)에 포함된 파라미터들 및 제 2 식별 정보를 소정의 알고리즘에 입력하여, 제 2 디바이스(200)의 개인키를 생성할 수 있다.

[0092] 일 실시예에 따르면, 개인키 생성 장치(300)는 생성한 제 1 디바이스(100)의 개인키를 제 1 디바이스(100)에 전송할 수 있다. 또한, 개인키 생성 장치(300)는 생성한 제 2 디바이스(200)의 개인키를 제 2 디바이스(200)에 전송할 수 있다.

[0093] 단계 s420에서, 제 1 디바이스(100)는 제 1 비밀 데이터를 생성할 수 있다. 예를 들어, 제 1 디바이스(100)는 개인키 생성 장치(300)에 의해 설정된 공개 파라미터 그룹(PP)에 포함된 파라미터(G) 및, 선택한 난수(a)를 수학식(1)에 입력하여 제 1 비밀데이터를 생성할 수 있다.

[0094] 일 실시예에 따르면, 제 1 디바이스(100)는 획득한 제 1 식별 정보 및 생성한 제 1 비밀 데이터를 제 2 디바이스(200)에게 전송할 수 있다. 예를 들어, 제 1 디바이스(100)는 무선 통신 경로 또는 유선 통신 경로를 이용하여 획득한 제 1 식별 정보 및 생성한 제 1 비밀 데이터를 제 2 디바이스(200)에게 전송할 수 있다.

[0095] 단계 s425 에서, 제 2 디바이스(200)는 제 1 서명 데이터 및 제 2 비밀 데이터를 생성할 수 있다. 예를 들어, 제 2 디바이스(200)는 수신한 제 1 식별 정보에 제 2 디바이스(200)의 개인키로 서명하여 생성한 서명 데이터, 및 수신한 제 1 비밀 데이터에 제 2 디바이스(200)의 개인키로 서명하여 생성한 서명 데이터를 결합하여 제 1 서명 데이터를 획득할 수 있다.

[0096] 또한, 제 2 디바이스(200)는 개인키 생성 장치(300)에 의해 설정된 공개 파라미터 그룹(PP)에 포함된 파라미터(G) 및, 선택한 난수(b)를 수학식(2)에 입력하여 제 2 비밀데이터를 생성할 수 있다.

[0097] 일 실시예에 따르면, 제 2 디바이스(200)는 생성된 제 1 서명 데이터, 생성된 제 2 비밀데이터, 획득한 제 2 식별 정보를 제 1 디바이스에 전송할 수 있다. 예를 들어, 제 2 디바이스(200)는 무선 통신 경로를 이용하여 생성된 제 1 서명 데이터, 생성된 제 2 비밀데이터, 획득한 제 2 식별 정보를 전송할 수 있으며, 유선 통신 경로를 이용하여 전송할 수 있다.

[0098] 단계 s430 에서, 제 1 디바이스(100)는 수신한 제 1 서명 데이터를 이용하여 제 2 디바이스(200)와의 대칭키 생성 여부를 결정할 수 있다.

[0099] 예를 들어, 제 1 디바이스(100)는 제 2 식별 정보를 공개키로 이용하여, 수신한 제 1 서명 데이터에 제 2 디바이스의 개인키로 서명된 제 1 식별 정보가 포함되어 있는지 여부를 판단할 수 있다. 또한, 제 1 디바이스(100)는 제 2 식별 정보를 공개키로 이용하여, 수신한 제 1 서명 데이터에 제 2 디바이스의 개인키로 서명된 제 1 비밀데이터가 포함되어 있는지 여부를 판단할 수 있다.

[0100] 제 1 디바이스(100)는 수신한 제 1 서명 데이터에 제 2 디바이스의 개인키로 서명된 제 1 식별 정보 및 제 2 디바이스의 개인키로 서명된 제 1 비밀데이터가 포함되어 있는 경우, 제 2 디바이스(200)와의 대칭키를 생성한다고 결정할 수 있다.

[0101] 또한, 제 1 디바이스(100)는 수신한 제 1 서명 데이터에 제 2 디바이스의 개인키로 서명된 제 1 식별 정보 또는 제 2 디바이스의 개인키로 서명된 제 1 비밀 데이터가 포함되어 있지 않은 경우, 제 2 디바이스(200)와의 대칭키를 생성하지 않는다고 결정할 수 있다.

[0102] 단계 s435 에서, 제 1 디바이스(100)는 결정하는 단계의 결과에 기초하여 제 2 서명 데이터를 생성할 수 있다.

[0103] 예를 들어, 제 1 디바이스(100)는 제 2 디바이스(200)와의 대칭키를 생성한다고 결정한 경우, 제 2 식별 정보, 수신한 제 2 비밀데이터, 생성한 제 1 비밀 데이터에 제 1 디바이스(100)의 개인키로 각각 서명하여 생성한 서명 데이터들을 결합하여, 제 2 서명 데이터를 생성할 수 있다.

[0104] 제 1 디바이스(100)는 생성한 제 2 서명 데이터를 제 2 디바이스(200)에 전송할 수 있다.

[0105] 단계 s440 에서, 제 2 디바이스(200)는 수신한 제 2 서명 데이터를 이용하여 제 1 디바이스(100)와의 대칭키 생성 여부를 결정할 수 있다.

[0106] 예를 들어, 제 2 디바이스(200)는 제 1 식별 정보를 공개키로 이용하여, 수신한 제 2 서명 데이터에 제 1 디바

이스의 개인키로 서명된 제 2 식별 정보가 포함되어 있는지 여부를 판단할 수 있다. 또한, 제 2 디바이스(200)는 제 1 식별 정보를 공개키로 이용하여, 수신한 제 2 서명 데이터에 제 1 디바이스의 개인키로 서명된 제 2 비밀데이터가 포함되어 있는지 여부를 판단할 수 있고, 수신한 제 2 서명 데이터에 제 1 디바이스의 개인키로 서명된 제 1 비밀 데이터가 포함되어 있는지 여부를 판단할 수 있다.

[0107] 제 2 디바이스(200)는 수신한 제 2 서명 데이터에 제 1 디바이스의 개인키로 서명된 제 2 식별 정보, 제 1 디바이스의 개인키로 서명된 제 1 비밀 데이터,및 제 1 디바이스의 개인키로 서명된 제 2 비밀데이터가 포함되어 있는 경우, 제 1 디바이스(100)와의 대칭키를 생성한다고 결정할 수 있다.

[0108] 단계 s450 에서, 제 1 디바이스(100)는 제 2 디바이스(200)와의 대칭키를 생성할 수 있다. 예를 들어, 제 1 디바이스(100)는 제 2 디바이스(200)와의 대칭키를 생성한다고 결정한 경우, 수학식 (3)을 이용하여 제 2 디바이스와의 대칭키를 생성할 수 있다.

[0109] 단계 s455 에서, 제 2 디바이스(200)는 제 1 디바이스(100)와의 대칭키를 생성할 수 있다. 예를들어, 제 2 디바이스(200)는 제 1 디바이스(100)와의 대칭키를 생성한다고 결정한 경우, 수학식 (4)을 이용하여 제 1 디바이스와의 대칭키를 생성할 수 있다.

[0110] 도 5 는 본 발명의 일 실시예에 따라 식별 정보에 기반하여 대칭키를 생성하는 시스템을 설명하기 위한 순서도이다.

[0111] 일 실시예에 따르면, 제 1 디바이스(100)는 제 1 식별정보(ID1)를 획득할 수 있다. 제 1 디바이스(100)는 획득한 제 1 식별정보(ID1)를 개인키 생성 장치(300)에 전송하고, 제 1 식별 정보(ID1)에 대응되는 개인키(SK1)를 획득할 수 있다.

[0112] 일 실시예에 따르면, 제 2 디바이스(200)는 제 2 식별정보(ID2)를 획득할 수 있다. 제 2 디바이스(200)는 획득한 제 2 식별정보(ID2)를 개인키 생성 장치(300)에 전송하고, 제 2 식별 정보(ID2)에 대응되는 개인키(SK2)를 획득할 수 있다.

[0113] 일 실시예에 따르면, 제 1 디바이스(100)는 난수(x1)를 선택하고, 선택한 난수(x1)를 이용하여 제 1 비밀 데이터(g^x1)를 생성할 수 있다. 제 1 디바이스(100)는 제 2 디바이스(200)에게 제 1 식별정보(ID1), 및 제 1 비밀 데이터(g^x1)를 전송할 수 있다(510).

[0114] 일 실시예에 따르면, 제 2 디바이스(200)는 수신한 제 1 식별정보(ID1), 및 제 1 비밀 데이터(g^x1)에 제 2 디바이스(200)의 개인키(SK2)로 각각 서명하여, 제 1 서명 데이터(IBS(SK2, ID1∥g^x1))를 생성할 수 있다. 또한, 제 2 디바이스(200)는 난수(x2)를 선택하고, 선택한 난수(x2)를 이용하여 제 2 비밀 데이터(g^x2)를 생성할 수 있다. 제 2 디바이스(200)는 제 1 디바이스(100)에게 제 2 식별 정보(ID2), 제 2 비밀 데이터(g^x2), 및 제 1 서명 데이터(IBS(SK2, ID1∥g^x1)를 전송할 수 있다(520).

[0115] 일 실시예에 따르면, 제 1 디바이스(100)는 수신한 제 1 서명 데이터(IBS(SK2, ID1∥g^x1))를 이용하여 제 1 디바이스(100)와의 대칭키 생성 여부를 결정할 수 있다.

[0116] 예를 들어, 제 1 디바이스(100)는 제 2 식별 정보(ID2)를 공개키로 이용하여, 수신한 제 1 서명 데이터에 제 2 디바이스의 개인키로 서명된 제 1 식별 정보가 포함되어 있는지 여부를 판단할 수 있다. 또한, 제 1 디바이스(100)는 제 2 식별 정보(ID2)를 공개키로 이용하여, 수신한 제 1 서명 데이터에 제 2 디바이스의 개인키로 서명된 제 1 비밀데이터가 포함되어 있는지 여부를 판단할 수 있다.

[0117] 제 1 디바이스(100)는 수신한 제 1 서명 데이터에 제 2 디바이스의 개인키로 서명된 제 1 식별 정보 및 제 2 디바이스의 개인키로 서명된 제 1 비밀데이터가 포함되어 있는 경우, 제 1 디바이스(100)와의 대칭키를 생성한다고 결정할 수 있다.

[0118] 일 실시예에 따르면, 제 1 디바이스(100)는 결정하는 단계의 결과에 기초하여 제 2 서명 데이터를 생성할 수 있다.

[0119] 예를 들어, 제 1 디바이스(100)는 제 2 디바이스(200)와의 대칭키를 생성한다고 결정한 경우, 제 2 식별 정보(ID2), 수신한 제 2 비밀 데이터(g^x2), 생성한 제 1 비밀 데이터(g^x1)에 제 1 디바이스(100)의 개인키로 각각 서명하여 생성된 서명 데이터들을 결합하여, 제 2 서명 데이터(IBS(SK1, ID2∥g^x1∥g^x2))를 생성할 수 있다.

[0120] 제 1 디바이스(100)는 생성한 제 2 서명 데이터를 제 2 디바이스(200)에 전송할 수 있다.(530)

[0121] 일 실시예에 따르면, 제 1 디바이스(100)는 결정하는 단계의 결과에 기초하여 대칭키를 생성할 수 있다. 예를 들어, 제 1 디바이스(100)는 수신한 제 2 비밀 데이터(g^x2) 및 난수(x1)를 이용하여 대칭키(K)를 생성할 수 있다. 제 1 디바이스(100)는 생성된 대칭키(K)를 이용하여 제 2 디바이스(200)와 데이터를 교환할 있다(540).

[0122] 일 실시예에 따르면, 제 2 디바이스(200)는 수신한 제 2 서명 데이터 IBS(SK2, ID2∥g^x1∥g^x2)를 이용하여 제 1 디바이스(100)와의 대칭키 생성 여부를 결정할 수 있다. 예를 들어, 제 2 디바이스(200)는 수신한 제 2 서명 데이터에 제 1 디바이스의 개인키로 서명된 제 2 식별 정보, 제 1 디바이스의 개인키로 서명된 제 1 비밀 데이터,및 제 1 디바이스의 개인키로 서명된 제 2 비밀데이터가 포함되어 있는 경우, 제 1 디바이스(100)와의 대칭키를 생성한다고 결정할 수 있다.

[0123] 일 실시예에 따르면, 제 2 디바이스(200)는 제 1 디바이스(100)와의 대칭키를 생성할 수 있다. 예를들어, 제 2 디바이스(200)는 제 1 디바이스(100)와의 대칭키를 생성한다고 결정한 경우, 제 1 비밀 데이터(g^x1), 및 난수(x2)를 이용하여 대칭키(K)를 생성할 수 있다. 제 2 디바이스(200)는 생성된 대칭키(K)를 이용하여 제 1 디바이스(100)와 데이터를 교환할 수 있다(540).

[0124] 도 6 은 다른 실시예에 따라 식별 정보에 기반하여 대칭키를 생성하는 시스템을 설명하기 위한 순서도이다.

[0125] 일 실시예에 따르면, 제 1 디바이스(100)는 제 1 식별정보(ID1)를 획득할 수 있다. 제 1 디바이스(100)는 획득한 제 1 식별정보(ID1)를 개인키 생성 장치(300)에 전송하고, 개인키 생성 장치(300)로부터 제 1 식별 정보(ID1)에 대응되는 개인키(SK1)를 획득할 수 있다.

[0126] 일 실시예에 따르면, 제 2 디바이스(200)는 제 2 식별정보(ID2)를 획득할 수 있다. 제 2 디바이스(200)는 획득한 제 2 식별정보(ID2)를 개인키 생성 장치(300)에 전송하고, 개인키 생성 장치(300)로부터 제 2 식별 정보(ID2)에 대응되는 개인키(SK2)를 획득할 수 있다.

[0127] 일 실시예에 따르면, 제 1 디바이스(100)는 제 2 식별정보(ID2)를 획득할 수 있다. 예를 들어, 제 1 디바이스(100)는 제 2 디바이스(200)로부터 제 2 식별 정보(ID2)를 수신할 수 있고, 개인키 생성 장치(300)로부터 제 2 식별 정보(ID2)를 수신할 수 있다.

[0128] 일 실시예에 따르면, 제 1 디바이스(100)는 제 1 난수(K1), 및 제 2 난수(R1)를 획득할 수 있다. 예를 들어, 제 1 디바이스(100)는 제 1 난수(K1) 및 제 2 난수(R1)를 생성할 수 있고, 외부의 디바이스로부터 수신할 수 있다.

[0129] 일 실시예에 따르면, 제 1 디바이스(100)는 획득한 제 1 난수(K1) 및 제 2 난수(R1)를 암호화 하여 제 1 암호 데이터(IBE(PP,ID2,K1∥R1))를 생성할 수 있다. 예를 들어, 제 1 디바이스(100)는 제 2 식별정보(ID2)를 공개키로 이용 하여 제 1 난수(K1) 및 제 2 난수(R1)를 암호화 함으로써, 제 1 암호 데이터(IBE(PP,ID2,K1∥R1))를 생성할 수 있다. 구체적으로, 제 1 디바이스(100)는 개인키 생성 장치에 의해 설정된 공개 파라미터 그룹(PP)에 포함된 파라미터들, 제 1 난수(K1), 제 2 난수(K2),및 제 2 식별 정보(ID2)를 소정의 알고리즘에 입력하여, 제 1 암호 데이터(IBE(PP,ID2,K1∥R1))를 획득할 수 있다.

[0130] 일 실시예에 따르면, 제 1 디바이스(100)는 획득한 제 1 식별 정보(ID1) 및 제 1 암호 데이터(IBE(PP,ID2,K1∥R1))를 제 2 디바이스(200)에 전송할 수 있다(610).

[0131] 일 실시예에 따르면, 제 2 디바이스(200)는 획득한 제 1 암호 데이터((IBE(PP,ID2,K1∥R1))를 복호화할 수 있다. 예를 들어, 제 2 디바이스(200)는 획득한 제 1 암호 데이터(IBE(PP,ID2,K1∥R1))를 제 2 디바이스의 개인키(SK2)를 이용하여 복호화 함으로써, 제 1 난수(K1) 및 제 2 난수(R1)를 획득할 수 있다.

[0132] 일 실시예에 따르면, 제 2 디바이스(200)는 제 3 난수(K2), 및 제 4 난수(R2)를 획득할 수 있다. 예를 들어, 제 2 디바이스(200)는 제 3 난수(K2) 및 제 4 난수(R2)를 생성할 수 있고, 외부의 디바이스로부터 수신할 수 있다.

[0133] 일 실시예에 따르면, 제 2 디바이스(200)는 획득한 제 3 난수(K2), 제 4 난수(R2), 및 제 2 난수(R1)를 암호화 하여 제 2 암호 데이터(IBE(PP,ID1,K2∥R1∥R2))를 생성할 수 있다. 예를 들어, 제 1 디바이스(100)는 제 1 식별정보(ID1)를 공개키로 이용 하여 제 3 난수(K2), 제 4 난수(R2), 및 제 2 난수(R1)를 암호화 함으로써, 제 2 암호 데이터(IBE(PP,ID1, K2∥R1∥R2))를 생성할 수 있다. 구체적으로, 제 1 디바이스(100)는 개인키 생성 장치에 의해 설정된 공개 파라미터 그룹(PP)에 포함된 파라미터들, 제 3 난수(K2), 제 4 난수(R2), 제 2 난수(R1), 및 제 2 식별 정보(ID2)를 소정의 알고리즘에 입력하여, 제 2 암호 데이터(IBE(PP,ID1,K1∥R1∥R2))를 획득할 수 있다.

[0134] 일 실시예에 따르면, 제 2 디바이스(200)는 획득한 제 2 암호 데이터(IBE(PP,ID1,K1∥R1∥R2))를 제 1 디바이스

(100)에 전송할 수 있다(620).

[0135] 일 실시예에 따르면, 제 1 디바이스(100)는 획득한 제 2 암호 데이터(IBE(PP,ID1,K1‖R1‖R2))를 복호화할 수 있다. 예를 들어, 제 1 디바이스(100)는 획득한 제 2 암호 데이터(IBE(PP,ID1,K1‖R1‖R2))를 제 1 디바이스의 개인키(SK1)를 이용하여 복호화 함으로써, 제 3 난수(K2), 제 4 난수(R2), 및 제 2 난수(R1)를 획득할 수 있다.

[0136] 일 실시예에 따르면, 제 1 디바이스(100)는 생성한 제 1 난수(K1) 및 제 3 난수(K2)를 이용하여 제 2 디바이스(200)와의 대칭키를 생성할 수 있다. 예를 들어, 제 1 디바이스(100)는 제 1 난수(K1) 및 제 3 난수(K2)를 해쉬 함수의 입력값으로 이용하여 대칭키를 생성할 수 있다. 또한, 제 1 디바이스(100)는 제 1 난수(K1) 및 제 3 난수(K2)를 소정의 알고리즘에 입력하여, 대칭키(K)를 생성할 수 있으며, 대칭키(K)를 생성하는 방법은 전술한 방법에 한정되지 않는다.

[0137] 일 실시예에 따르면, 제 1 디바이스(100)는 획득한 제 4 난수(R2)를 생성된 대칭키(K)로 암호화 하여, 제 3 암호 데이터(SKE(R2))를 획득할 수 있다, 또한, 획득한 제 3 암호 데이터(SKE(R2))를 제 2 디바이스(200)에 전송할 수 있다(630).

[0138] 일 실시예에 따르면, 제 2 디바이스(200)는 제 1 디바이스(100)와의 대칭키를 생성할 수 있다. 제 2 디바이스(200)는 제 1 난수(K1) 및 제 3 난수(K2)를 해쉬 함수의 입력값으로 이용하여 대칭키를 생성할 수 있다. 또한, 제 2 디바이스(200)는 제 1 난수(K1) 및 제 3 난수(K2)를 소정의 알고리즘에 입력하여, 대칭키(K)를 생성할 수 있으며, 대칭키(K)를 생성하는 방법은 전술한 방법에 한정되지 않는다.

[0139] 일 실시예에 따르면, 제 2 디바이스(200)는 제 3 암호 데이터(SKE(R2))를 획득할 수 있다. 또한, 제 2 디바이스(200)는 생성한 대칭키(K)를 이용하여 제 3 암호 데이터(SKE(R2))를 복호화 하고, 제 4 난수(R2)를 획득할 수 있다. 제 2 디바이스(200)는 제 4 난수(R2)를 획득함으로써, 제 2 디바이스(200)가 생성한 대칭키와 제 1 디바이스(100)가 생성한 대칭키가 일치함을 확인할 수 있다.

[0140] 일 실시예에 따르면, 제 1 디바이스(100)와 제 2 디바이스(200)는 생성한 대칭키를 이용하여 데이터를 교환할 수 있다(640).

[0141] 일 실시예에 따르면, 개인키 생성 디바이스(300)는 제 1 암호 데이터 및 제 2 암호 데이터를 획득한 경우, 대칭키를 생성할 수 있다. 예를 들어, 개인키 생성 디바이스(300)는 개인키들을 발급하는 과정에서 사용된 마스터키를 보유하고 있기에, 제 1 암호 데이터를 복호화 하여 제 1 난수(K1)를 획득할 수 있다. 또한, 개인키 생성 디바이스(300)는 제 2 암호 데이터를 복호하 하여 제 3 난수(K2)를 획득할 수 있다. 개인키 생성 디바이스(300)는 소정의 알고리즘에 획득한 제 1 난수(K1) 및 제 3 난수(K2)를 입력함으로써, 대칭키를 생성할 수 있다.

[0142] 일 실시예에 따르면, 개인키 생성 디바이스(300)는 제 1 디바이스(100)와 제 2 디바이스(200)가 교환하는 데이터를 감청할 수 있다. 예를 들어, 제 1 디바이스(100)와 제 2 디바이스(200)가 대칭키를 이용하여 암호화된 데이터를 교환하는 경우, 개인키 생성 디바이스(300)는 암호화된 데이터를 획득하고, 대칭키를 이용하여 암호화된 데이터를 복호화할 수 있다.

[0143] 도 7 은 다른 실시예에 따라, 대칭키를 생성하는 시스템을 설명하기 위한 블록도이다.

[0144] 일 실시예에 따르면, 제 1 디바이스(100)는 제 1 식별정보(ID1)를 획득할 수 있다. 제 1 디바이스(100)는 획득한 제 1 식별정보(ID1)를 개인키 생성 장치(300)에 전송하고, 개인키 생성 장치(300)로부터 제 1 식별 정보(ID1)에 대응되는 개인키(SK1)를 획득할 수 있다.

[0145] 일 실시예에 따르면, 제 2 디바이스(200)는 제 2 식별정보(ID2)를 획득할 수 있다. 제 2 디바이스(200)는 획득한 제 2 식별정보(ID2)를 개인키 생성 장치(300)에 전송하고, 개인키 생성 장치(300)로부터 제 2 식별 정보(ID2)에 대응되는 개인키(SK2)를 획득할 수 있다.

[0146] 일 실시예에 따르면, 제 1 디바이스(100)는 제 2 식별정보(ID2)를 획득할 수 있다. 예를 들어, 제 1 디바이스(100)는 제 2 디바이스(200)로부터 제 2 식별 정보(ID2)를 수신할 수 있고, 개인키 생성 장치(300)로부터 제 2 식별 정보(ID2)를 수신할 수 있다.

[0147] 일 실시예에 따르면, 제 1 디바이스(100)는 난수(x1)를 획득할 수 있다. 예를 들어, 제 1 디바이스(100)는 난수(x1)를 생성할 수 있고, 외부의 디바이스로부터 수신할 수 있다.

[0148] 일 실시예에 따르면, 제 1 디바이스(100)는 획득한 난수(x1)를 이용하여, 제 1 비밀 데이터(g^x1)를 획득할 수 있다. 예를 들어, 제 1 디바이스(100)는 획득한 난수(x1)를 소정의 알고리즘에 입력하여, 제 1 비밀 데이터

(g^x1)를 획득할 수 있다.

[0149] 일 실시예에 따르면, 제 1 디바이스(100)는 제 1 비밀 데이터(g^x1)를 암호화 하여 제 1 암호 데이터(IBE(PP,ID2, g^x1))를 생성할 수 있다. 예를 들어, 제 1 디바이스(100)는 제 2 식별정보(ID2)를 공개키로 이용 하여 제 1 비밀 데이터(g^x1)를 암호화 함으로써, 제 1 암호 데이터(IBE(PP,ID2, g^x1))를 생성할 수 있다. 구체적으로, 제 1 디바이스(100)는 개인키 생성 장치에 의해 설정된 공개 파라미터 그룹(PP)에 포함된 파라미터들, 제 1 비밀 데이터(g^x1),및 제 2 식별 정보(ID2)를 소정의 알고리즘에 입력하여, 제 1 암호 데이터(IBE(PP,ID2, g^x1))를 획득할 수 있다.

[0150] 일 실시예에 따르면, 제 1 디바이스(100)는 획득한 제 1 식별 정보(ID1) 및 제 1 암호 데이터(IBE(PP,ID2, g^x1))를 제 2 디바이스(200)에 전송할 수 있다(710).

[0151] 일 실시예에 따르면, 제 2 디바이스(200)는 획득한 제 1 암호 데이터(IBE(PP,ID2, g^x1))를 복호화할 수 있다. 예를 들어, 제 2 디바이스(200)는 제 2 디바이스의 개인키(SK2)를 이용하여 제 1 암호 데이터(IBE(PP,ID2, g^x1))를 복호화 함으로써, 제 1 비밀 데이터(g^x1)를 획득할 수 있다.

[0152] 일 실시예에 따르면, 제 2 디바이스(200)는 난수(x2)를 획득할 수 있다. 예를 들어, 제 2 디바이스(200)는 난수(x2)를 생성할 수 있고, 외부의 디바이스로부터 수신할 수 있다.

[0153] 일 실시예에 따르면, 제 2 디바이스(200)는 획득한 난수(x2)를 이용하여, 제 2 비밀 데이터(g^x2)를 획득할 수 있다. 예를 들어, 제 2 디바이스(200)는 획득한 난수(x2)를 소정의 알고리즘에 입력하여, 제 2 비밀 데이터(g^x2)를 획득할 수 있다.

[0154] 일 실시예에 따르면, 제 2 디바이스(200)는 제 1 비밀 데이터(g^x1) 및 제 2 비밀 데이터(g^x2)를 암호화 하여 제 2 암호 데이터(IBE(PP,ID1, g^x1‖g^x2))를 생성할 수 있다. 예를 들어, 제 1 디바이스(100)는 제 1 식별정보(ID1)를 공개키로 이용 하여 1 비밀 데이터(g^x1) 및 제 2 비밀 데이터(g^x2)를 암호화 함으로써, 제 2 암호 데이터(IBE(PP,ID1, g^x1‖g^x2))를 생성할 수 있다. 구체적으로, 제 1 디바이스(100)는 개인키 생성 장치에 의해 설정된 공개 파라미터 그룹(PP)에 포함된 파라미터들, 제 1 비밀 데이터(g^x1), 제 2 비밀 데이터(g^x2),및 제 2 식별 정보(ID2)를 소정의 알고리즘에 입력하여, 제 2 암호 데이터(IBE(PP,ID1, g^x1‖g^x2))를 획득할 수 있다.

[0155] 일 실시예에 따르면, 제 2 디바이스(200)는 획득한 제 2 암호 데이터(IBE(PP,ID1, g^x1‖g^x2))를 제 1 디바이스(100)에 전송할 수 있다(720).

[0156] 일 실시예에 따르면, 제 1 디바이스(100)는 획득한 제 2 암호 데이터(IBE(PP,ID1, g^x1‖g^x2))를 복호화할 수 있다. 예를 들어, 제 1 디바이스(100)는 획득한 제 2 암호 데이터(IBE(PP,ID1, g^x1‖g^x2))를 제 1 디바이스의 개인키(SK1)를 이용하여 복호화 함으로써, 제 1 비밀 데이터(g^x1) 및 제 2 비밀 데이터(g^x2)를 획득할 수 있다.

[0157] 일 실시예에 따르면, 제 1 디바이스(100)는 획득한 제 2 비밀 데이터(g^x2) 및 난수(x1)를 이용하여 제 2 디바이스(200)와의 대칭키를 생성할 수 있다. 예를 들어, 제 1 디바이스(100)는 제 2 비밀 데이터(g^x2)에 난수(x1)를 지수승하여 대칭키(K=(g^x2)^x1)를 획득할 수 있다. 또한, 제 1 디바이스(100)는 제 2 비밀 데이터(g^x2) 및 난수(x1)를 소정의 알고리즘에 입력하여, 대칭키(K)를 생성할 수 있으며, 대칭키(K)를 생성하는 방법은 전술한 방법에 한정되지 않는다.

[0158] 일 실시예에 따르면, 제 1 디바이스(100)는 획득한 제 2 비밀 데이터(g^x2)를 생성된 대칭키(K)로 암호화 하여, 제 3 암호 데이터(SKE(g^x2))를 획득할 수 있다, 또한, 획득한 제 3 암호 데이터(SKE(g^x2))를 제 2 디바이스(200)에 전송할 수 있다(730).

[0159] 일 실시예에 따르면, 제 2 디바이스(200)는 제 1 디바이스(100)와의 대칭키를 생성할 수 있다. 예를 들어, 제 2 디바이스(200)는 제 1 비밀 데이터(g^x1)에 난수(x2)를 지수승하여 대칭키(K=(g^x1)^x2)를 획득할 수 있다. 또한, 제 2 디바이스(200)는 제 1 비밀 데이터(g^x1) 및 난수(x2)를 소정의 알고리즘에 입력하여, 대칭키(K)를 생성할 수 있으며, 대칭키(K)를 생성하는 방법은 전술한 방법에 한정되지 않는다.

[0160] 일 실시예에 따르면, 제 2 디바이스(200)는 제 3 암호 데이터(SKE(g^x2))를 획득할 수 있다. 또한, 제 2 디바이스(200)는 생성한 대칭키(K)를 이용하여 제 3 암호 데이터(SKE(g^x2)) 복호화 하고, 제 2 비밀 데이터(g^x2)를 획득할 수 있다. 제 2 디바이스(200)는 제 2 비밀 데이터(g^x2)를 획득함으로써, 제 2 디바이스(200)가 생성한

대칭키와 제 1 디바이스(100)가 생성한 대칭키가 일치함을 확인할 수 있다.

[0161] 일 실시예에 따르면, 제 1 디바이스(100)와 제 2 디바이스(200)는 생성한 대칭키를 이용하여 데이터를 교환할 수 있다(740).

[0162] 일 실시예에 따르면, 개인키 생성 디바이스(300)는 제 1 암호 데이터 및 제 2 암호 데이터를 획득하더라도, 대칭키를 생성할 수 없다. 예를 들어, 개인키 생성 디바이스(300)는 개인키들을 발급하는 과정에서 사용된 마스터 키를 보유하고 있기에, 제 1 암호 데이터를 복호화 하여 제 1 비밀 데이터(g^x1)를 획득할 수 있다. 또한, 개인키 생성 디바이스(300)는 제 2 암호 데이터를 복호하 하여 제 2 비밀 데이터(g^x2)를 획득할 수 있다. 다만, 개인키 생성 디바이스(300)는 난수(x1) 및 난수(x2)를 획득할 수 없으므로, 개인키 생성 디바이스(300)는 대칭키를 생성할 수 없다.

[0163] 일 실시예에 따라, 제 1 디바이스(100)와 제 2 디바이스(200)가 도 7에서 설명된 방법을 이용하여 대칭키를 생성하는 경우, 개인키 생성 디바이스(300)는 제 1 디바이스(100)와 제 2 디바이스(200)가 교환하는 데이터를 감청할 수 없다. 예를 들어, 제 1 디바이스(100)와 제 2 디바이스(200)가 대칭키를 이용하여 암호화된 데이터를 교환하는 경우, 개인키 생성 디바이스(300)는 암호화된 데이터를 획득하더라도 암호화된 데이터를 복호화할 수 없다.

[0164] 도 8은 본 발명의 일 실시예에 따라, 대칭키를 생성하는 디바이스를 설명하기 위한 블록도이다.

[0165] 제 1 디바이스(100)는 정보 획득부(115), 통신부(125), 결정부(135), 대칭키 생성부(145), 및 서명 데이터 생성부(155)를 포함한다. 정보 획득부(115), 통신부(125), 결정부(135), 대칭키 생성부(145), 및 서명 데이터 생성부(155)는 하나의 프로세서에 의해 구현될 수 있고, 복수의 프로세서에 의해 구현될 수 있다.

[0166] 제 2 디바이스(200)는 정보 획득부(215), 통신부(225), 결정부(235), 대칭키 생성부(245), 및 서명 데이터 생성부(255)를 포함한다. 정보 획득부(215), 통신부(225), 결정부(235), 대칭키 생성부(245), 및 서명 데이터 생성부(255)는 하나의 프로세서에 의해 구현될 수 있고, 복수의 프로세서에 의해 구현될 수 있다.

[0167] 제 1 디바이스(100)의 정보 획득부(115)는 제 1 식별 정보를 획득할 수 있다. 예를 들어,제 1 디바이스(100)의 정보 획득부(115)는 제 1 디바이스(100) 사용자의 전화번호, 사용자의 주민등록 번호, 사용자의 이메일 주소 또는 제 1 디바이스(100)의 제품 번호, 제 1 디바이스(100)의 제조 일자 등을 획득할 수 있으며, 이에 한정되지 않고 제 1 디바이스(100) 또는 제 1 디바이스(100)의 사용자를 나타내는 소정의 정보를 획득할 수 있다.

[0168] 제 2 디바이스(200)의 정보 획득부(215)는 제 2 식별 정보를 획득할 수 있다. 예를 들어, 제 2 디바이스(200)의 정보 획득부(215)는 제 2 디바이스(200) 사용자의 전화번호, 사용자의 주민등록 번호, 사용자의 이메일 주소 또는 제 2 디바이스(200)의 제품 번호, 제 2 디바이스(200)의 제조 일자 등을 획득할 수 있으며, 이에 한정되지 않고 제 2 디바이스(200) 또는 제 2 디바이스(200)의 사용자를 나타내는 소정의 정보를 획득할 수 있다.

[0169] 개인키 생성 장치(300)는 제 1 식별 정보 및 제 2 식별 정보를 수신하여, 식별 정보들 각각에 대응되는 개인키를 생성할 수 있다.

[0170] 일 실시예에 따르면, 개인키 생성 장치(300)는 복수의 파라미터가 포함된 공개 파라미터 그룹(PP)을 설정할 수 있다. 개인키 생성 장치(300)는 공개 파라미터 그룹(PP)을 설정하고, 설정된 파라미터 그룹(PP)을 제 1 디바이스(100)의 통신부(125) 및 제 2 디바이스(200)의 통신부(225)에 전송할 수 있다.

[0171] 일 실시예에 따르면, 개인키 생성 장치(300)는 제 1 식별 정보 및 제 2 식별 정보에 각각 대응되는 개인키를 생성할 수 있다. 예를 들어, 개인키 생성 장치(300)는 제 1 식별 정보 및 공개 파라미터 그룹(PP)에 포함된 파라미터들을 소정의 알고리즘에 입력하여, 제 1 디바이스(100)의 개인키를 생성할 수 있다. 또한, 개인키 생성 장치(300)는 공개 파라미터 그룹(PP)에 포함된 파라미터들 및 제 2 식별 정보를 소정의 알고리즘에 입력하여, 제 2 디바이스(200)의 개인키를 생성할 수 있다.

[0172] 일 실시예에 따르면, 개인키 생성 장치(300)는 생성한 제 1 디바이스(100)의 개인키를 제 1 디바이스(100)의 통신부(125)에 전송할 수 있다. 또한, 개인키 생성 장치(300)는 생성한 제 2 디바이스(200)의 개인키를 제 2 디바이스(200)의 통신부(225)에 전송할 수 있다.

[0173] 제 1 디바이스(100)는 제 1 비밀 데이터를 생성할 수 있다. 예를 들어, 제 1 디바이스(100)는 개인키 생성 장치(300)에 의해 설정된 공개 파라미터 그룹(PP)에 포함된 파라미터(G) 및, 선택한 난수(a)를 수학식(1)에 입력하여 제 1 비밀데이터를 생성할 수 있다.

[0174] 일 실시예에 따르면, 제 1 디바이스(100)의 통신부(125)는 획득한 제 1 식별 정보 및 생성한 제 1 비밀 데이터를 제 2 디바이스(200)에게 전송할 수 있다. 예를 들어, 제 1 디바이스(100)의 통신부(125)는 무선 통신 경로 또는 유선 통신 경로를 이용하여 획득한 제 1 식별 정보 및 생성한 제 1 비밀 데이터를 제 2 디바이스(200)에게 전송할 수 있다.

[0175] 제 2 디바이스(200)는 제 1 서명 데이터 및 제 2 비밀 데이터를 생성할 수 있다. 예를 들어, 제 2 디바이스(200)의 서명 데이터 생성부(255)는 수신한 제 1 식별 정보에 제 2 디바이스(200)의 개인키로 서명하여 생성한 서명 데이터, 및 수신한 제 1 비밀 데이터에 제 2 디바이스(200)의 개인키로 서명하여 생성한 서명 데이터를 결합하여 제 1 서명 데이터를 획득할 수 있다.

[0176] 또한, 제 2 디바이스(200)는 개인키 생성 장치(300)에 의해 설정된 공개 파라미터 그룹(PP)에 포함된 파라미터(G) 및, 선택한 난수(b)를 수학식(2)에 입력하여 제 2 비밀데이터를 생성할 수 있다.

[0177] 일 실시예에 따르면, 제 2 디바이스(200)의 통신부(225)는 생성된 제 1 서명 데이터, 생성된 제 2 비밀데이터, 획득한 제 2 식별 정보를 제 1 디바이스에 전송할 수 있다. 예를 들어, 제 2 디바이스(200)의 통신부(225)는 무선 통신 경로를 이용하여 생성된 제 1 서명 데이터, 생성된 제 2 비밀데이터, 획득한 제 2 식별 정보를 전송할 수 있으며, 유선 통신 경로를 이용하여 전송할 수 있다.

[0178] 제 1 디바이스(100)의 결정부(135)는 수신한 제 1 서명 데이터를 이용하여 제 1 디바이스(100)와의 대칭키 생성 여부를 결정할 수 있다.

[0179] 예를 들어, 제 1 디바이스(100)의 결정부(135)는 제 2 식별 정보를 공개키로 이용하여, 수신한 제 1 서명 데이터에 제 2 디바이스의 개인키로 서명된 제 1 식별 정보가 포함되어 있는지 여부를 판단할 수 있다. 또한, 제 1 디바이스(100)의 결정부(135)는 제 2 식별 정보를 공개키로 이용하여, 수신한 제 1 서명 데이터에 제 2 디바이스의 개인키로 서명된 제 1 비밀데이터가 포함되어 있는지 여부를 판단할 수 있다.

[0180] 제 1 디바이스(100)의 결정부(135)는 수신한 제 1 서명 데이터에 제 2 디바이스의 개인키로 서명된 제 1 식별 정보 및 제 2 디바이스의 개인키로 서명된 제 1 비밀데이터가 포함되어 있는 경우, 제 1 디바이스(100)와의 대칭키를 생성한다고 결정할 수 있다.

[0181] 또한, 제 1 디바이스(100)의 결정부(135)는 수신한 제 1 서명 데이터에 제 2 디바이스의 개인키로 서명된 제 1 식별 정보 또는 제 2 디바이스의 개인키로 서명된 제 1 비밀 데이터가 포함되어 있지 않은 경우, 제 2 디바이스(200)와의 대칭키를 생성하지 않는다고 결정할 수 있다.

[0182] 제 1 디바이스(100)의 서명 데이터 생성부(155)는 결정하는 단계의 결과에 기초하여 제 2 서명 데이터를 생성할 수 있다.

[0183] 예를 들어, 제 1 디바이스(100)의 서명 데이터 생성부(155)는 제 2 디바이스(200)와의 대칭키를 생성한다고 결정한 경우, 제 2 식별 정보, 수신한 제 2 비밀데이터, 생성한 제 1 비밀 데이터에 제 1 디바이스(100)의 개인키로 각각 서명하여 생성한 서명 데이터들을 결합하여, 제 2 서명 데이터를 생성할 수 있다.

[0184] 제 1 디바이스(100)의 통신부(125)는 생성한 제 2 서명 데이터를 제 2 디바이스(200)에 전송할 수 있다.

[0185] 제 2 디바이스(200)의 결정부(235)는 수신한 제 2 서명 데이터를 이용하여 제 1 디바이스(100)와의 대칭키 생성 여부를 결정할 수 있다.

[0186] 예를 들어, 제 2 디바이스(200)의 결정부(235)는 제 1 식별 정보를 공개키로 이용하여, 수신한 제 2 서명 데이터에 제 1 디바이스의 개인키로 서명된 제 2 식별 정보가 포함되어 있는지 여부를 판단할 수 있다. 또한, 제 2 디바이스(200)의 결정부(235)는 제 1 식별 정보를 공개키로 이용하여, 수신한 제 2 서명 데이터에 제 1 디바이스의 개인키로 서명된 제 2 비밀데이터가 포함되어 있는지 여부를 판단할 수 있고, 수신한 제 2 서명 데이터에 제 1 디바이스의 개인키로 서명된 제 1 비밀데이터가포함되어 있는지 여부를 판단할 수 있다.

[0187] 제 2 디바이스(200)의 결정부(235)는 수신한 제 2 서명 데이터에 제 1 디바이스의 개인키로 서명된 제 2 식별 정보, 제 1 디바이스의 개인키로 서명된 제 1 비밀 데이터,및 제 1 디바이스의 개인키로 서명된 제 2 비밀데이터가 포함되어 있는 경우, 제 1 디바이스(100)와의 대칭키를 생성한다고 결정할 수 있다.

[0188] 제 1 디바이스(100)의 대칭키 생성부(145)는 제 2 디바이스(200)와의 대칭키를 생성할 수 있다. 예를 들어, 제 2 디바이스(200)와의 대칭키를 생성한다고 결정한 경우 제 1 디바이스(100)의 대칭키 생성부(145)는 수학식

(3)을 이용하여 제 2 디바이스와의 대칭키를 생성할 수 있다.

[0189] 제 2 디바이스(200)의 대칭키 생성부(245)는 제 1 디바이스(100)와의 대칭키를 생성할 수 있다. 예를들어, 제 1 디바이스(100)와의 대칭키를 생성한다고 결정한 경우 제 2 디바이스(200)의 대칭키 생성부(245)는 수학식 (4)을 이용하여 제 1 디바이스와의 대칭키를 생성할 수 있다.

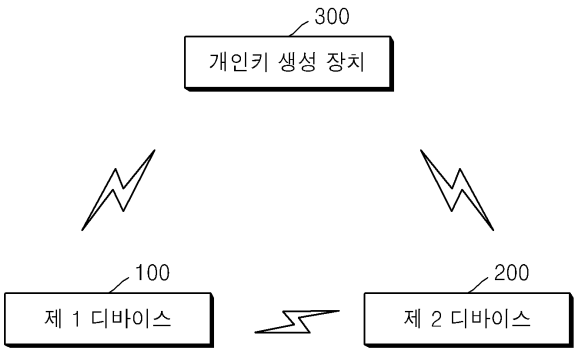
[0190] 일부 실시예는 컴퓨터에 의해 실행되는 프로그램 모듈과 같은 컴퓨터에 의해 실행가능한 명령어를 포함하는 기록 매체의 형태로도 구현될 수 있다. 컴퓨터 판독 가능 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 가용 매체일 수 있고, 휘발성 및 비휘발성 매체, 분리형 및 비분리형 매체를 모두 포함한다. 또한, 컴퓨터 판독가능 매체는 컴퓨터 저장 매체 및 통신 매체를 모두 포함할 수 있다. 컴퓨터 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술로 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.

[0191] 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.

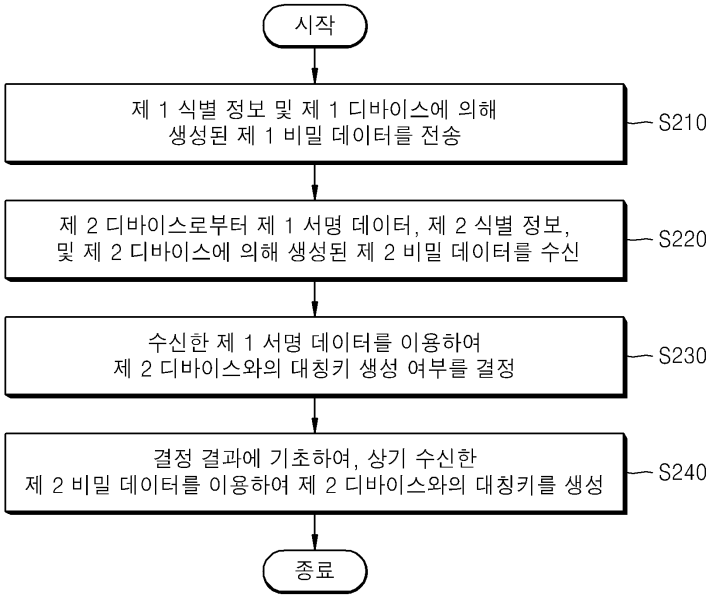
[0192] 본 개시의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 개시의 범위에 포함되는 것으로 해석되어야 한다.

도면

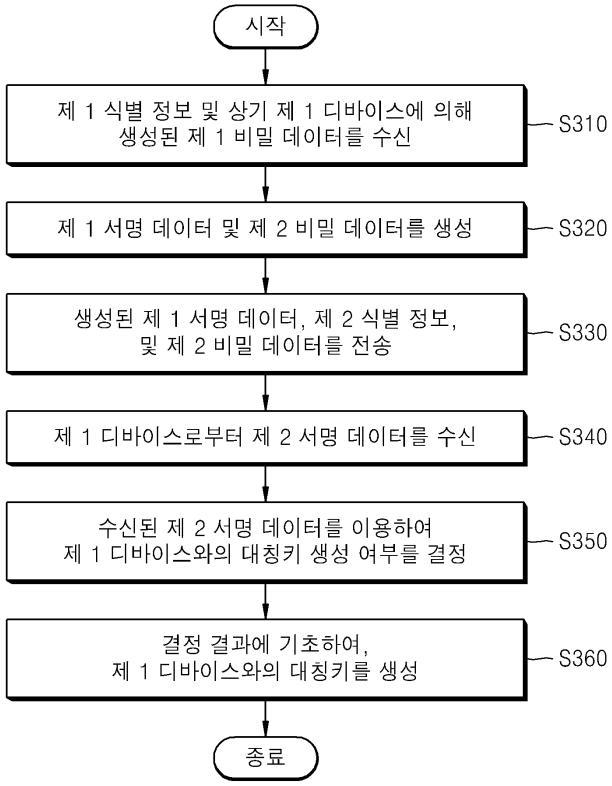
도면1



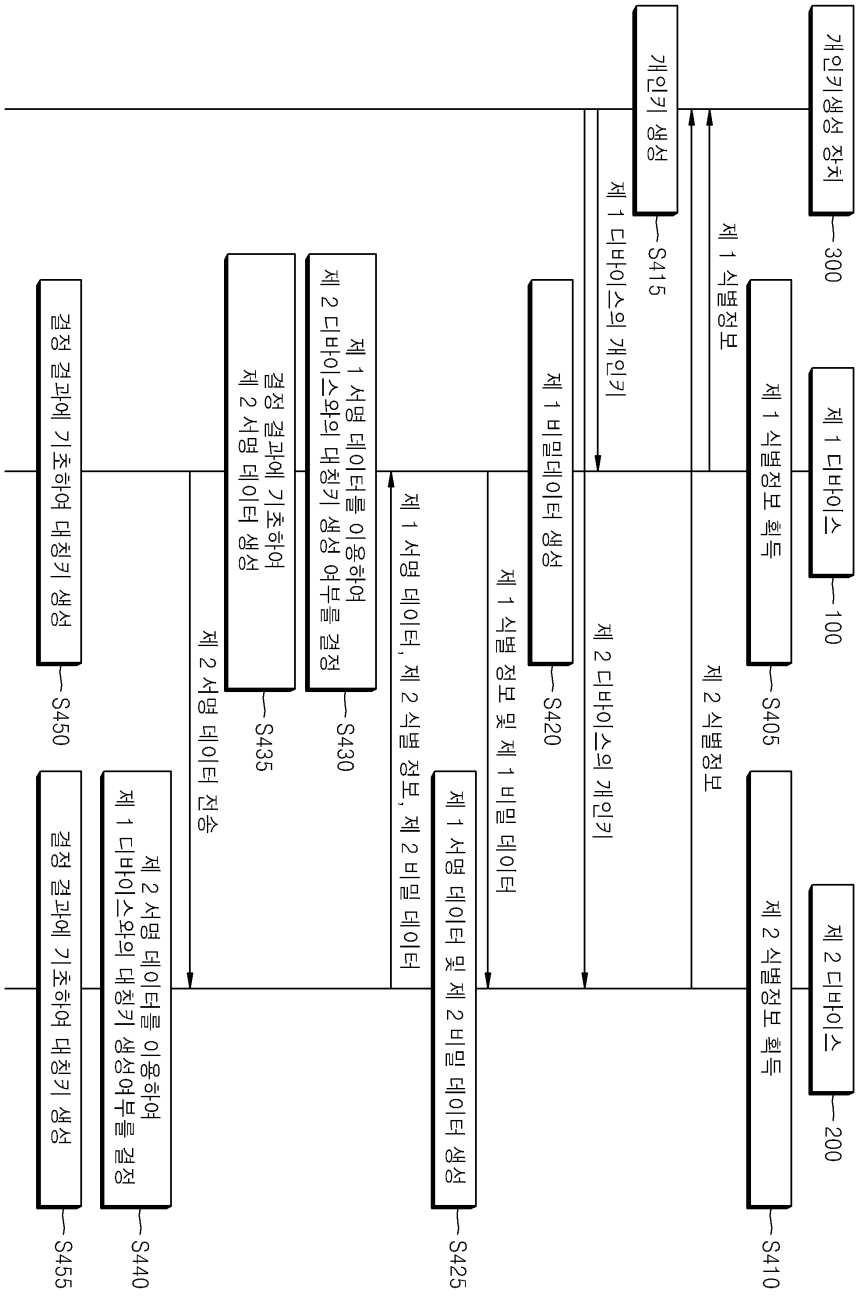
도면2


시작
제 1 식별 정보 및 제 1 디바이스에 의해
생성된 제 1 비밀 데이터를 전송
S210
제 2 디바이스로부터 제 1 서명 데이터, 제 2 식별 정보,
및 제 2 디바이스에 의해 생성된 제 2 비밀 데이터를 수신
S220
수신한 제 1 서명 데이터를 이용하여
제 2 디바이스와의 대칭키 생성 여부를 결정
S230
결정 결과에 기초하여, 상기 수신한
제 2 비밀 데이터를 이용하여 제 2 디바이스와의 대칭키를 생성
S240
종료

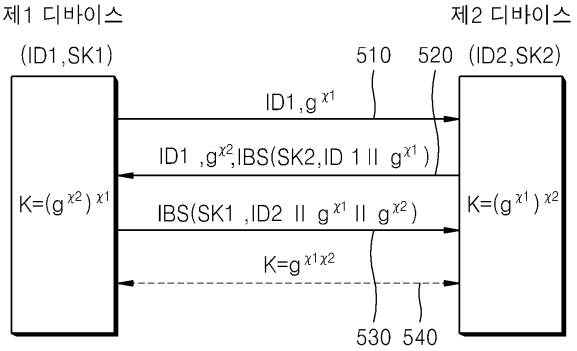
도면3


시작
제 1 식별 정보 및 상기 제 1 디바이스에 의해
생성된 제 1 비밀 데이터를 수신
S310
제 1 서명 데이터 및 제 2 비밀 데이터를 생성
S320
생성된 제 1 서명 데이터, 제 2 식별 정보,
및 제 2 비밀 데이터를 전송
S330
제 1 디바이스로부터 제 2 서명 데이터를 수신
S340
수신된 제 2 서명 데이터를 이용하여
제 1 디바이스와의 대칭키 생성 여부를 결정
S350
결정 결과에 기초하여,
제 1 디바이스와의 대칭키를 생성
S360
종료

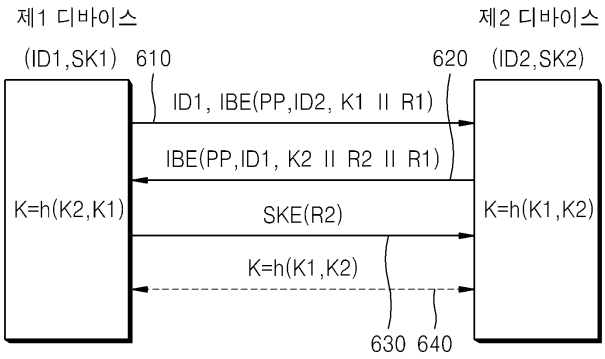
도면4


개인키생성 장치
300
개인키 생성
S415
제 1 디바이스의 개인키
제 1 식별정보
제 1 디바이스
100
제 1 식별정보 획득
S405
제 1 비밀데이터 생성
S420
제 2 디바이스의 개인키
제 2 식별정보
제 2 디바이스
200
제 2 식별정보 획득
S410
제 1 서명 데이터를 이용하여
제 2 디바이스와의 대칭키 생성 여부를 결정
S430
결정 결과에 기초하여
제 2 서명 데이터 생성
S435
결정 결과에 기초하여 대칭키 생성
S450
제 1 서명 데이터, 제 2 식별 정보, 제 2 비밀 데이터
제 1 서명 데이터 및 제 2 비밀 데이터 생성
S425
제 2 서명 데이터 전송
제 2 서명 데이터를 이용하여
제 1 디바이스와의 대칭키 생성여부를 결정
S440
결정 결과에 기초하여 대칭키 생성
S455

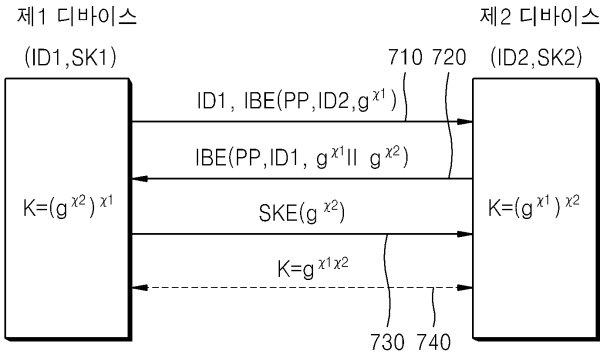
도면5


제1 디바이스
(ID1,SK1)
제2 디바이스
(ID2,SK2)
510
520
ID1,g^χ1
ID1 ,g^χ2,IBS(SK2,ID 1 II g^χ1)
K=(g^χ2)^χ1
IBS(SK1 ,ID2 II g^χ1 II g^χ2)
K=(g^χ1)^χ2
K=g^χ1χ2
530
540

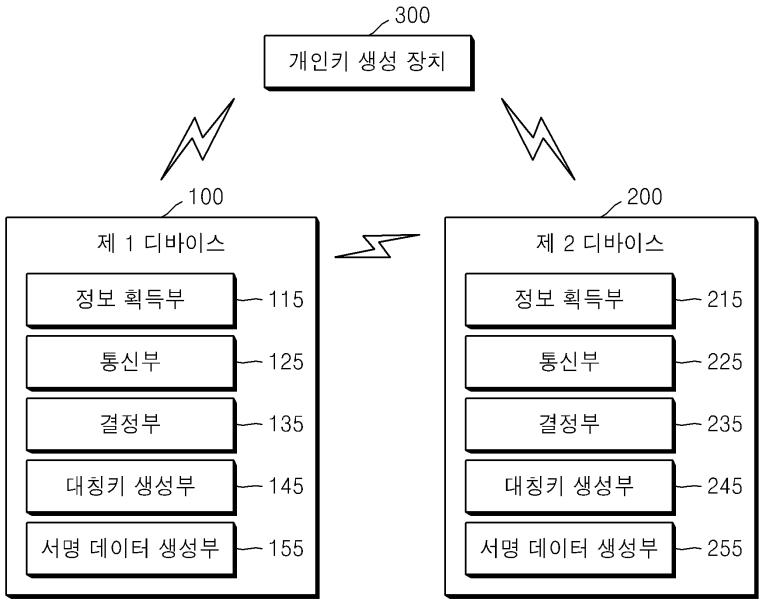
도면6


제1 디바이스
(ID1,SK1)
610
620
제2 디바이스
(ID2,SK2)
ID1, IBE(PP,ID2, K1 II R1)
IBE(PP,ID1, K2 II R2 II R1)
K=h(K2,K1)
SKE(R2)
K=h(K1,K2)
K=h(K1,K2)
630
640

도면7


제1 디바이스
(ID1,SK1)
710
720
제2 디바이스
(ID2,SK2)
ID1, IBE(PP,ID2,g^x1)
IBE(PP,ID1, g^x1II g^x2)
K=(g^x2)^x1
SKE(g^x2)
K=(g^x1)^x2
K=g^x1x2
730
740

도면8


300
개인키 생성 장치
100
제 1 디바이스
정보 획득부
115
통신부
125
결정부
135
대칭키 생성부
145
서명 데이터 생성부
155
200
제 2 디바이스
정보 획득부
215
통신부
225
결정부
235
대칭키 생성부
245
서명 데이터 생성부
255