



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0045820
(43) 공개일자 2020년05월06일

(51) 국제특허분류(Int. Cl.)
H04L 9/06 (2006.01) H04L 9/00 (2006.01)
(52) CPC특허분류
H04L 9/0618 (2013.01)
H04L 9/008 (2013.01)
(21) 출원번호 10-2018-0126802
(22) 출원일자 2018년10월23일
심사청구일자 없음

(71) 출원인
삼성에스디에스 주식회사
서울특별시 송파구 올림픽로35길 125 (신천동)
(72) 발명자
김은경
서울특별시 송파구 올림픽로35길 125 (신천동, 삼성SDS West Campus)
윤효진
서울특별시 송파구 올림픽로35길 125 (신천동, 삼성SDS West Campus)
(74) 대리인
두호특허법인

전체 청구항 수 : 총 24 항

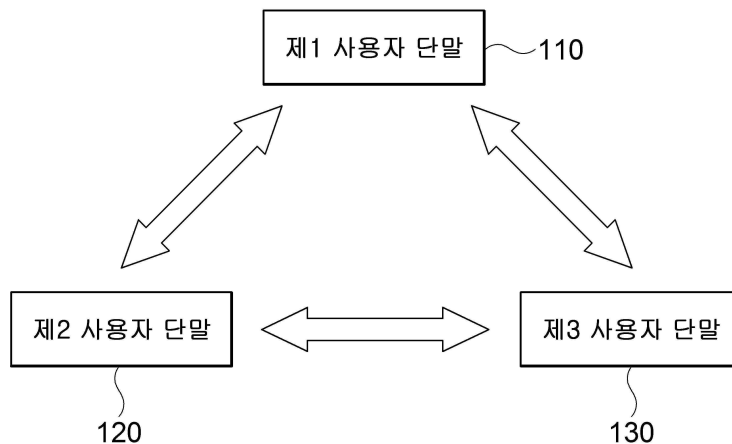
(54) 발명의 명칭 암호화 및 복호화를 위한 장치 및 방법

(57) 요약

암호화 및 복호화를 위한 장치 및 방법이 개시된다. 본 발명의 일 실시예에 따른 암호화 방법은, 사용자의 공개 키 지분을 생성하는 단계; 하나 이상의 타 사용자의 단말 각각으로부터 상기 하나 이상의 타 사용자 각각의 공개 키 지분을 수신하는 단계; 상기 사용자의 공개키 지분 및 상기 하나 이상의 타 사용자 각각의 공개키 지분을 이용하여 공개키를 생성하는 단계; 및 상기 공개키를 이용하여 평문 데이터를 암호화하는 단계를 포함한다.

대표도 - 도1

100



명세서

청구범위

청구항 1

하나 이상의 프로세서들, 및

상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비한 컴퓨팅 장치에서 수행되는 방법으로서,

사용자의 공개키 지분을 생성하는 단계;

하나 이상의 타 사용자의 단말 각각으로부터 상기 하나 이상의 타 사용자 각각의 공개키 지분을 수신하는 단계;

상기 사용자의 공개키 지분 및 상기 하나 이상의 타 사용자 각각의 공개키 지분을 이용하여 공개키를 생성하는 단계; 및

상기 공개키를 이용하여 평문 데이터를 암호화하는 단계를 포함하는, 암호화 방법.

청구항 2

청구항 1에 있어서,

상기 공개키 지분을 생성하는 단계는, 상기 사용자의 개인키 지분을 생성하는 단계; 및

상기 사용자의 개인키 지분을 이용하여 상기 사용자의 공개키 지분을 생성하는 단계를 포함하는, 암호화 방법.

청구항 3

청구항 2에 있어서,

상기 하나 이상의 타 사용자 각각의 공개키 지분은, 각각 상기 각 타 사용자 각각의 개인키 지분을 이용하여 생성되는, 암호화 방법.

청구항 4

청구항 1에 있어서,

상기 생성된 공개키 지분을 상기 하나 이상의 타 사용자의 단말 각각으로 제공하는 단계를 더 포함하는, 암호화 방법.

청구항 5

하나 이상의 프로세서;

메모리; 및

하나 이상의 프로그램을 포함하는 장치로서,

상기 하나 이상의 프로그램은 상기 메모리에 저장되고 상기 하나 이상의 프로세서에 의해 실행되도록 구성되며,

상기 프로그램은,

사용자의 공개키 지분을 생성하는 단계;

하나 이상의 타 사용자의 단말 각각으로부터 상기 하나 이상의 타 사용자 각각의 공개키 지분을 수신하는 단계;
 상기 사용자의 공개키 지분 및 상기 하나 이상의 타 사용자 각각의 공개키 지분을 이용하여 공개키를 생성하는 단계; 및
 상기 공개키를 이용하여 평문 데이터를 암호화하는 단계를 실행하기 위한 명령어들을 포함하는, 암호화 장치.

청구항 6

청구항 5에 있어서,
 상기 공개키 지분을 생성하는 단계는, 상기 사용자의 개인키 지분을 생성하는 단계; 및
 상기 사용자의 개인키 지분을 이용하여 상기 사용자의 공개키 지분을 생성하는 단계를 포함하는, 암호화 장치.

청구항 7

청구항 6에 있어서,
 상기 하나 이상의 타 사용자 각각의 공개키 지분은, 각각 상기 각 타 사용자 각각의 개인키 지분을 이용하여 생성되는, 암호화 장치.

청구항 8

청구항 5에 있어서,
 상기 프로그램은, 상기 생성된 공개키 지분을 상기 하나 이상의 타 사용자의 단말 각각으로 제공하는 단계를 실행하기 위한 명령어들을 더 포함하는, 암호화 장치.

청구항 9

하나 이상의 프로세서들, 및
 상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비한 컴퓨팅 장치에서 수행되는 방법으로서,
 사용자의 개인키 지분을 이용하여, 공개키를 이용하여 암호화된 암호문에 대한 부분 복호화 결과를 생성하는 단계;
 하나 이상의 타 사용자의 단말로 상기 암호문에 대한 부분 복호화를 요청하는 단계;
 상기 하나 이상의 타 사용자 단말 각각으로부터 상기 하나 이상의 타 사용자 각각의 개인키 지분을 이용한 상기 암호문에 대한 부분 복호화 결과를 수신하는 단계; 및
 상기 생성된 부분 복호화 결과 및 상기 하나 이상의 타 사용자 각각으로부터 수신된 부분 복호화 결과를 이용하여 상기 암호문에 대한 평문 데이터를 생성하는 단계를 포함하는, 복호화 방법.

청구항 10

청구항 9에 있어서,
 상기 공개키는, 상기 사용자의 공개키 지분 및 상기 하나 이상의 타 사용자 각각의 공개키 지분을 이용하여 생성되는, 복호화 방법.

청구항 11

청구항 10에 있어서,

상기 사용자의 공개키 지분은, 상기 사용자의 개인키 지분을 이용하여 생성되고,

상기 하나 이상의 타 사용자 각각의 공개키 지분은, 상기 하나 이상의 타 사용자 각각의 개인키 지분을 이용하여 생성되는, 복호화 방법.

청구항 12

청구항 9에 있어서,

상기 암호문은, 각각 상기 공개키를 이용하여 암호화된 복수의 암호문을 암호화된 상태로 연산하여 생성된 암호문인, 복호화 방법.

청구항 13

청구항 12에 있어서,

상기 평문 데이터는, 상기 복수의 암호문 각각에 대한 평문 데이터 사이의 연산 결과인, 복호화 방법.

청구항 14

청구항 12에 있어서,

상기 암호문은, 각각 상기 공개키를 이용하여 암호화된 복수의 암호문을 암호화된 상태로 더하여 생성된 암호문인, 복호화 방법.

청구항 15

청구항 14에 있어서,

상기 평문 데이터는, 상기 복수의 암호문 각각에 대한 평문 데이터를 더한 결과인, 복호화 방법.

청구항 16

청구항 15에 있어서,

상기 평문 데이터를 생성하는 단계는, 상기 생성된 부분 복호화 결과 및 상기 하나 이상의 타 사용자 각각으로부터 수신된 부분 복호화 결과를 더하여 상기 암호문에 대한 평문 데이터를 생성하는 복호화 방법.

청구항 17

하나 이상의 프로세서;

메모리; 및

하나 이상의 프로그램을 포함하는 장치로서,

상기 하나 이상의 프로그램은 상기 메모리에 저장되고 상기 하나 이상의 프로세서에 의해 실행되도록 구성되며,

상기 프로그램은,

사용자의 개인키 지분을 이용하여, 공개키를 이용하여 암호화된 암호문에 대한 부분 복호화 결과를 생성하는 단

계;

하나 이상의 타 사용자의 단말로 상기 암호문에 대한 부분 복호화를 요청하는 단계;

상기 하나 이상의 타 사용자 단말 각각으로부터 상기 하나 이상의 타 사용자 각각의 개인키 지분을 이용한 상기 암호문에 대한 부분 복호화 결과를 수신하는 단계; 및

상기 생성된 부분 복호화 결과 및 상기 하나 이상의 타 사용자 각각으로부터 수신된 부분 복호화 결과를 이용하여 상기 암호문에 대한 평문 데이터를 생성하는 단계를 실행하기 위한 명령어들을 포함하는, 복호화 장치.

청구항 18

청구항 17에 있어서,

상기 공개키는, 상기 사용자의 공개키 지분 및 상기 하나 이상의 타 사용자 각각의 공개키 지분을 이용하여 생성되는, 복호화 장치.

청구항 19

청구항 18에 있어서,

상기 사용자의 공개키 지분은, 상기 사용자의 개인키 지분을 이용하여 생성되고,

상기 하나 이상의 타 사용자 각각의 공개키 지분은, 상기 하나 이상의 타 사용자 각각의 개인키 지분을 이용하여 생성되는, 복호화 장치.

청구항 20

청구항 17에 있어서,

상기 암호문은, 각각 상기 공개키를 이용하여 암호화된 복수의 암호문을 암호화된 상태로 연산하여 생성된 암호문인, 복호화 장치.

청구항 21

청구항 20에 있어서,

상기 평문 데이터는, 상기 복수의 암호문 각각에 대한 평문 데이터 사이의 연산 결과인, 복호화 장치.

청구항 22

청구항 20에 있어서,

상기 암호문은, 각각 상기 공개키를 이용하여 암호화된 복수의 암호문을 암호화된 상태로 더하여 생성된 암호문인, 복호화 장치.

청구항 23

청구항 22에 있어서,

상기 평문 데이터는, 상기 복수의 암호문 각각에 대한 평문 데이터를 더한 결과인, 복호화 장치.

청구항 24

청구항 23에 있어서,

상기 평문 데이터를 생성하는 단계는, 상기 생성된 부분 복호화 결과 및 상기 하나 이상의 타 사용자 각각으로부터 수신된 부분 복호화 결과를 더하여 상기 암호문에 대한 평문 데이터를 생성하는, 복호화 장치.

발명의 설명**기술 분야**

[0001] 본 발명의 실시예들은 암호화 및 복호화를 위한 기술과 관련된다.

배경 기술

[0002] 미국 등록특허 US 9,252,942를 포함한 종래기술에서는 동형암호를 이용해 다수의 사용자 간의 안전한 데이터 융합 서비스를 제공하기 위해, 신뢰할 수 있는 한 사용자(비밀키 관리자)가 공개키와 비밀키를 생성하고 모든 사용자에게 공개키를 분배한다. 이 경우, 사용자들은 각자의 데이터를 분배받은 공개키를 이용해 암호화한 후, 암호화된 데이터의 동형연산을 수행하게 된다. 또한, 일반 사용자들이 비밀키 관리자에게 복호화 요청을 하면, 비밀키 관리자가 복호화된 평문 연산 결과를 일반 사용자들에게 전송한다.

[0003] 이러한 종래기술의 경우, 비밀키를 비밀키 관리자가 관리하고 있으므로, 전체 시스템의 안전성이 비밀키 관리자의 안전성에 전적으로 의존하게 되는 문제가 발생한다. 즉, 비밀키 관리자를 통해 비밀키가 유출되면 모든 사용자의 데이터가 복구가능하고 전체 시스템의 안전성이 훼손된다. 뿐만 아니라, 상호 신뢰하기 어려운 사용자들의 경우에는 모든 사용자가 신뢰할 수 있는 단 하나의 비밀키 관리자를 설정하는 것은 불가능하다는 문제점이 존재한다.

선행기술문헌**특허문헌**

[0004] (특허문헌 0001) 미국 등록특허 US 9,252,942 (2016.02.02. 등록)

발명의 내용**해결하려는 과제**

[0005] 본 발명의 실시예들은 암호화 및 복호화를 위한 장치 및 방법을 제공하기 위한 것이다.

과제의 해결 수단

[0006] 본 발명의 일 실시예에 따른 암호화 방법은, 하나 이상의 프로세서들, 및 상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비한 컴퓨팅 장치에서 수행되는 방법으로서, 사용자의 공개키 지분을 생성하는 단계; 하나 이상의 타 사용자의 단말 각각으로부터 상기 하나 이상의 타 사용자 각각의 공개키 지분을 수신하는 단계; 상기 사용자의 공개키 지분 및 상기 하나 이상의 타 사용자 각각의 공개키 지분을 이용하여 공개키를 생성하는 단계; 및 상기 공개키를 이용하여 평문 데이터를 암호화하는 단계를 포함한다.

[0007] 상기 공개키 지분을 생성하는 단계는, 상기 사용자의 개인키 지분을 생성하는 단계; 및 상기 사용자의 개인키 지분을 이용하여 상기 사용자의 공개키 지분을 생성하는 단계를 포함할 수 있다.

[0008] 상기 하나 이상의 타 사용자 각각의 공개키 지분은, 각각 상기 각 타 사용자 각각의 개인키 지분을 이용하여 생성될 수 있다.

[0009] 상기 생성된 공개키 지분을 상기 하나 이상의 타 사용자의 단말 각각으로 제공하는 단계를 더 포함할 수 있다.

[0010] 본 발명의 일 실시예에 따른 암호화 장치는, 하나 이상의 프로세서; 메모리; 및 하나 이상의 프로그램을 포함하

는 장치로서, 상기 하나 이상의 프로그램은 상기 메모리에 저장되고 상기 하나 이상의 프로세서에 의해 실행되도록 구성되며, 상기 프로그램은, 사용자의 공개키 지분을 생성하는 단계; 하나 이상의 타 사용자의 단말 각각으로부터 상기 하나 이상의 타 사용자 각각의 공개키 지분을 수신하는 단계; 상기 사용자의 공개키 지분 및 상기 하나 이상의 타 사용자 각각의 공개키 지분을 이용하여 공개키를 생성하는 단계; 및 상기 공개키를 이용하여 평문 데이터를 암호화하는 단계를 실행하기 위한 명령어들을 포함한다.

- [0011] 상기 공개키 지분을 생성하는 단계는, 상기 사용자의 개인키 지분을 생성하는 단계; 및 상기 사용자의 개인키 지분을 이용하여 상기 사용자의 공개키 지분을 생성하는 단계를 포함할 수 있다.
- [0012] 상기 하나 이상의 타 사용자 각각의 공개키 지분은, 각각 상기 각 타 사용자 각각의 개인키 지분을 이용하여 생성될 수 있다.
- [0013] 상기 프로그램은, 상기 생성된 공개키 지분을 상기 하나 이상의 타 사용자의 단말 각각으로 제공하는 단계를 실행하기 위한 명령어들을 더 포함할 수 있다.
- [0014] 본 발명의 일 실시예에 따른 복호화 방법은, 하나 이상의 프로세서들, 및 상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비한 컴퓨팅 장치에서 수행되는 방법으로서, 사용자의 개인키 지분을 이용하여, 공개키를 이용하여 암호화된 암호문에 대한 부분 복호화 결과를 생성하는 단계; 하나 이상의 타 사용자의 단말로 상기 암호문에 대한 부분 복호화를 요청하는 단계; 상기 하나 이상의 타 사용자 단말 각각으로부터 상기 하나 이상의 타 사용자 각각의 개인키 지분을 이용한 상기 암호문에 대한 부분 복호화 결과를 수신하는 단계; 및 상기 생성된 부분 복호화 결과 및 상기 하나 이상의 타 사용자 각각으로부터 수신된 부분 복호화 결과를 이용하여 상기 암호문에 대한 평문 데이터를 생성하는 단계를 포함한다.
- [0015] 상기 공개키는, 상기 사용자의 공개키 지분 및 상기 하나 이상의 타 사용자 각각의 공개키 지분을 이용하여 생성될 수 있다.
- [0016] 상기 사용자의 공개키 지분은, 상기 사용자의 개인키 지분을 이용하여 생성되고, 상기 하나 이상의 타 사용자 각각의 공개키 지분은, 상기 하나 이상의 타 사용자 각각의 개인키 지분을 이용하여 생성될 수 있다.
- [0017] 상기 암호문은, 각각 상기 공개키를 이용하여 암호화된 복수의 암호문을 암호화된 상태로 연산하여 생성된 암호문일 수 있다.
- [0018] 상기 평문 데이터는, 상기 복수의 암호문 각각에 대한 평문 데이터 사이의 연산 결과일 수 있다.
- [0019] 상기 암호문은, 각각 상기 공개키를 이용하여 암호화된 복수의 암호문을 암호화된 상태로 더하여 생성된 암호문일 수 있다.
- [0020] 상기 평문 데이터는, 상기 복수의 암호문 각각에 대한 평문 데이터를 더한 결과일 수 있다.
- [0021] 상기 평문 데이터를 생성하는 단계는, 상기 생성된 부분 복호화 결과 및 상기 하나 이상의 타 사용자 각각으로부터 수신된 부분 복호화 결과를 더하여 상기 암호문에 대한 평문 데이터를 생성할 수 있다.
- [0022] 본 발명의 일 실시예에 따른 복호화 방법은, 하나 이상의 프로세서; 메모리; 및 하나 이상의 프로그램을 포함하는 장치로서, 상기 하나 이상의 프로그램은 상기 메모리에 저장되고 상기 하나 이상의 프로세서에 의해 실행되도록 구성되며, 상기 프로그램은, 사용자의 개인키 지분을 이용하여, 공개키를 이용하여 암호화된 암호문에 대한 부분 복호화 결과를 생성하는 단계; 하나 이상의 타 사용자의 단말로 상기 암호문에 대한 부분 복호화를 요청하는 단계; 상기 하나 이상의 타 사용자 단말 각각으로부터 상기 하나 이상의 타 사용자 각각의 개인키 지분을 이용한 상기 암호문에 대한 부분 복호화 결과를 수신하는 단계; 및 상기 생성된 부분 복호화 결과 및 상기 하나 이상의 타 사용자 각각으로부터 수신된 부분 복호화 결과를 이용하여 상기 암호문에 대한 평문 데이터를 생성하는 단계를 실행하기 위한 명령어들을 포함한다.
- [0023] 상기 공개키는, 상기 사용자의 공개키 지분 및 상기 하나 이상의 타 사용자 각각의 공개키 지분을 이용하여 생성될 수 있다.
- [0024] 상기 사용자의 공개키 지분은, 상기 사용자의 개인키 지분을 이용하여 생성되고, 상기 하나 이상의 타 사용자 각각의 공개키 지분은, 상기 하나 이상의 타 사용자 각각의 개인키 지분을 이용하여 생성될 수 있다.
- [0025] 상기 암호문은, 각각 상기 공개키를 이용하여 암호화된 복수의 암호문을 암호화된 상태로 연산하여 생성된 암호문일 수 있다.

- [0026] 상기 평문 데이터는, 상기 복수의 암호문 각각에 대한 평문 데이터 사이의 연산 결과일 수 있다.
- [0027] 상기 암호문은, 각각 상기 공개키를 이용하여 암호화된 복수의 암호문을 암호화된 상태로 더하여 생성된 암호문일 수 있다.
- [0028] 상기 평문 데이터는, 상기 복수의 암호문 각각에 대한 평문 데이터를 더한 결과일 수 있다.
- [0029] 상기 평문 데이터를 생성하는 단계는, 상기 생성된 부분 복호화 결과 및 상기 하나 이상의 타 사용자 각각으로부터 수신된 부분 복호화 결과를 더하여 상기 암호문에 대한 평문 데이터를 생성할 수 있다.

발명의 효과

- [0030] 본 발명의 실시예들에 따르면, 비밀키 관리 권한을 공개키 생성을 위해 협력한 모든 사용자에게 동일하게 분산시켜 줄 뿐만 아니라, 복호화 역시 모든 사용자가 동의한 경우에만 가능하게 함으로써, 개인키 유출로 인한 부정확한 데이터 유출을 방지할 수 있으며, 상호 신뢰가 부족한 사용자 간에서도 안전한 개인키 관리가 가능하도록 할 수 있다

도면의 간단한 설명

- [0031] 도 1은 본 발명의 일 실시예에 따른 암호화 시스템의 구성도
- 도 2는 본 발명의 일 실시예에 따른 공개키 생성 과정을 나타낸 순서도
- 도 3은 본 발명의 일 실시예에 따른 복호화 과정을 나타낸 순서도
- 도 4는 예시적인 실시예들에서 사용되기에 적합한 컴퓨팅 장치를 포함하는 컴퓨팅 환경을 예시하여 설명하기 위한 블록도

발명을 실시하기 위한 구체적인 내용

- [0032] 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.
- [0033] 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.
- [0034] 도 1은 본 발명의 일 실시예에 따른 암호화 시스템의 구성도이다.
- [0035] 도 1을 참조하면, 본 발명의 일 실시예에 따른 암호화 시스템(100)은 복수의 사용자 단말(110, 130, 150)을 포함한다.
- [0036] 암호화 시스템(100)은 복수의 사용자가 협력하여 생성한 공개키를 이용하여 암호문을 생성하고, 모든 사용자가 동의한 경우에만 공개키를 이용하여 생성된 암호문 또는 공개키를 이용하여 생성된 암호문들 사이의 연산 결과에 대한 복호화를 가능케 하기 위한 것이다.
- [0037] 복수의 사용자 단말(110, 120, 130)은 각각 상이한 사용자에게 의해 이용되는 단말로서, 예를 들어, 데스크톱 PC, 랩톱 PC, 태블릿 PC, 스마트폰, 페블릿(phablet) 등일 수 있으나, 유/무선 네트워크를 이용한 통신 기능 및 데이터 연산 기능을 구비한 장치라면 반드시 특정한 형태의 장치로 한정되는 것은 아니다.
- [0038] 한편, 이하에서는 설명의 편의를 위해 도 1에 도시된 예와 같이 사용자 단말(110, 120, 130)이 3개인 것으로 가정하여 설명하나, 단말의 개수는 실시예에 따라 2개이거나 4개 이상이 될 수 있다.
- [0039] 또한, 이하에서는, 제1 사용자 단말(110)은 사용자 1에 의해 이용되고, 제2 사용자 단말(120)은 사용자 2에 의

해 이용되며, 제3 사용자 단말(130)은 사용자 3에 의해 이용되는 것으로 가정한다.

[0040] 한편, 본 발명의 일 실시예에 따르면, 각 사용자 단말(110, 120, 130)에 의해 수행되는 암호화 및 복호화 과정은 아래와 같이 수행될 수 있다.

[0041] 키 생성

[0042] 각 사용자 단말(110, 120, 130)은 각 사용자 단말(110, 120, 130)의 사용자에게 대한 개인키 지분 및 공개키 지분을 생성하고, 생성된 공개키 지분을 다른 사용자 단말(110, 120, 130)로 전송한다.

[0043] 또한, 다른 사용자의 공개키 지분을 수신한 각 사용자 단말(110, 120, 130)은 수신된 다른 사용자의 공개키 지분과 생성한 사용자의 공개키 지분을 이용하여 동일한 공개키를 생성한다.

[0044] 암호화 및 동형 연산

[0045] 공개키가 생성된 경우, 각 사용자 단말(110, 120, 130)은 생성된 공개키를 이용하여 평문 데이터에 대한 암호문을 생성한다.

[0046] 이때, 생성된 암호문은 각 사용자 단말(110, 120, 130)에 저장될 수 있으나, 실시예에 따라, 각 사용자 단말(110, 120, 130)에서 접근 가능한 별도의 데이터베이스(미도시) 내지 서버(미도시)에 저장될 수도 있다.

[0047] 한편, 각 사용자 단말(110, 120, 130)에 의해 생성되는 암호문은 동일한 공개키를 이용하여 암호화된 복수의 암호문을 암호화된 상태로 연산하여 각 암호문에 대한 평문 데이터 사이의 연산 결과에 대한 암호문을 생성 가능하도록 하는 다양한 방식의 동형 암호 (homomorphic encryption) 기술을 이용하여 생성될 수 있다.

[0048] 이 경우, 각 사용자 단말(110, 120, 130)은 암호문들 사이의 연산을 수행하여 각 암호문에 대한 평문 데이터 사이의 연산 결과에 대한 암호문을 생성할 수 있다. 이때, 암호문 사이의 연산을 위해 이용되는 각 암호문은 동일한 사용자 단말(110, 120, 130)에 의해 생성되거나, 상이한 사용자 단말(110, 120, 130)에 의해 생성된 암호문일 수 있다.

[0049] 한편, 암호문 사이의 연산은 상술한 바와 같이 각 사용자 단말(110, 120, 130)에 의해 수행될 수 있다. 그러나, 실시예에 따라, 각 사용자 단말(110, 120, 130)에 의해 생성된 암호문이 별도의 서버(미도시)에 저장되는 경우, 해당 서버에서 저장된 암호문들 사이의 연산을 수행한 후 그 결과를 각 사용자 단말(110, 120, 130)로 제공할 수 있다.

[0050] 복호화

[0051] 각 사용자 단말(110, 120, 130)은 각 사용자 단말(110, 120, 130)의 사용자에게 대한 개인키 지분을 이용하여 암호문에 대한 부분 복호화를 수행하고, 각 사용자 단말(110, 120, 130)에서 수행된 부분 복호화 결과들을 이용하여 암호문에 대한 평문 데이터를 생성한다. 이때, 암호문은 공개키를 이용하여 암호화된 암호문 또는 공개키를 이용하여 암호화된 복수의 암호문 사이의 연산을 통해 생성된 암호문일 수 있다.

[0052] 한편, 상술한 암호화 및 복호화 과정을 근사 계산이 가능한 동형 암호 기술에 적용한 구체적인 적용 예는 아래와 같다.

[0053] 키 생성

[0054] 우선, 각 사용자 단말(110, 120, 130)은 각 사용자의 개인키 지분 및 공개키 지분을 생성할 수 있다. 이때, 사용자 i (이때, i 는 $1 \leq i \leq 3$ 인 사용자 인덱스)에 대한 개인키 지분 sk_i 및 공개키 지분 pk_i 는 각각 아래의 수학적식 1 및 2를 만족할 수 있다.

[0055] [수학적식 1]

$$sk_i = (1, s_i)$$

[0056]

[0057] [수학적식 2]

$$pk_i = (b_i, a)$$

[0058]

[0059] 이때, s_i , b_i 및 a 는 각각 다항식 환(polynomial ring)의 원소이며, $b_i = -a \cdot s_i + e$ (이때, e 는 아주 작은 임의의

에러 값)를 만족할 수 있다. 또한, a 는 모든 사용자의 공개키 지분에 공통적으로 포함되는 값일 수 있다.

[0060] 이후, 각 사용자 단말(110, 120, 130)은 생성된 공개키 지분을 다른 사용자 단말(110, 120, 130)로 전송할 수 있다. 또한, 다른 사용자 단말(110, 120, 130)로부터 공개키 지분을 수신한 각 사용자 단말(110, 120, 130)은 수신한 공개키 지분 및 자신이 생성한 공개키 지분을 이용하여 공개키 pk 를 생성할 수 있다. 이때, 공개키 pk 는 예를 들어, 아래의 수학적 식 3을 이용하여 생성될 수 있다.

[0061] [수학적 식 3]

[0062]
$$pk = (b_1 + b_2 + b_3, a) = (b, a)$$

[0063] 암호화

[0064] 공개키를 생성한 각 사용자 단말(110, 120, 130)은 생성된 공개키를 이용하여 평문 데이터 m 에 대한 암호문 C 를 생성할 수 있다. 이때, 암호문 생성은 예를 들어, 아래의 수학적 식 4를 이용하여 생성될 수 있다.

[0065] [수학적 식 4]

[0066]
$$C = (c_0, c_1) = (v \cdot b + m + e_0, v \cdot a + e_1)$$

[0067] 이때, 평문 데이터 m 과 v 는 다항식환의 원소이며, e_0 및 e_1 은 아주 작은 임의의 에러 값을 나타낸다.

[0068] 한편, 생성된 암호문은 각 사용자 단말(110, 120, 130)에 저장될 수 있으나, 실시예에 따라, 각 사용자 단말(110, 120, 130)이 접속 가능한 별도의 데이터베이스(미도시) 또는 서버(미도시)에 저장될 수도 있다.

[0069] 동형 연산

[0070] 각 사용자 단말(110, 120, 130)은 상술한 암호화 과정을 통해 생성된 평문 데이터 m_1 에 대한 암호문 C_1 및 평문 데이터 m_2 에 대한 암호문 C_2 에 대하여, $C_1 + C_2$ 를 계산하여 $m_1 + m_2$ 에 대한 암호문 C_3 를 생성할 수 있다. 구체적으로, 암호문 C_1 및 C_2 가 각각 아래의 수학적 식 5 및 6과 같은 경우, C_3 는 아래의 수학적 식 7을 이용하여 생성될 수 있다.

[0071] [수학적 식 5]

[0072]
$$C_1 = (c_{1,0}, c_{1,1}) = (v_1 \cdot b + m_1 + e_{0,1}, v_1 \cdot a + e_{1,1})$$

[0073] [수학적 식 6]

[0074]
$$C_2 = (c_{2,0}, c_{2,1}) = (v_2 \cdot b + m_2 + e_{0,2}, v_2 \cdot a + e_{1,2})$$

[0075] [수학적 식 7]

[0076]
$$C_3 = C_1 + C_2 = (c_{3,0}, c_{3,1}) = (v_3 \cdot b + m_3 + e_{0,3}, v_3 \cdot a + e_{1,3})$$

[0077] 이때, $v_3 = v_1 + v_2$, $e_{0,3} = e_{0,1} + e_{0,2}$, $e_{1,3} = e_{1,1} + e_{1,2}$ 를 만족한다.

[0078] 한편, 실시예에 따라, 암호문 C_3 의 생성은 상술한 예와 달리 암호문 C_1 및 C_2 를 저장하고 있는 서버(미도시)에서 수행될 수 있으며, 이 경우, 서버(미도시)는 생성된 암호문 C_3 를 각 사용자 단말(110, 120, 130)로 제공할 수 있다.

[0079] 복호화

[0080] 각 사용자 단말(110, 120, 130)은 각 사용자 단말(110, 120, 130)의 사용자에게 대한 개인키 지분 sk_i 를 이용하여, 암호문 $C' = (c'_0, c'_1)$ 에 대한 부분 복호화를 수행할 수 있다. 이때, 암호문 C' 는 상술한 암호화 과정을 통해 생성된 암호문(예를 들어, C_1 또는 C_2) 또는 상술한 동형 연산 과정을 통해 생성된 암호문(예를 들어, C_3)일 수 있다.

[0081] 한편, 암호문 C'에 대한 부분 복호화는 예를 들어, 아래의 수학식 8을 이용하여 수행될 수 있다.

[0082] [수학식 8]

$$p_i = c'_1 \cdot s_i + e'_4 = v' \cdot a \cdot s_i + e'_1 \cdot s_i + e'_4$$

[0084] 이때, e'_4 는 아주 작은 임의의 에러 값을 나타낸다.

[0085] 한편, 암호문 C'에 대한 평문 데이터 m'는 예를 들어, 아래의 수학식 9를 이용하여 생성될 수 있다.

[0086] [수학식 9]

$$\begin{aligned} c'_0 + (p_1 + p_2 + p_3) &= \left(v' \cdot \sum_{i=1}^3 b_i + m' + e'_0 \right) + \sum_{i=1}^3 (v' \cdot a \cdot s_i + e'_1 \cdot s_i + e'_4) \\ &= m' + v' \cdot \sum_{i=1}^3 (b_i + a \cdot s_i) + \sum_{i=1}^3 (e'_1 \cdot s_i + e'_4) + e'_0 \\ &= m' + e'_5 \approx m' \end{aligned}$$

[0087]

[0088] 한편, 수학식 3에서, $e'_5 = v' \cdot \sum_{i=1}^3 (b_i + a \cdot s_i) + \sum_{i=1}^3 (e'_1 \cdot s_i + e'_4) + e'_0$ 를 만족하며, m'보다 매우 작은 값으로 설정될 수 있다.

[0089] 도 2는 본 발명의 일 실시예에 따른 공개키 생성 과정을 나타낸 순서도이다.

[0090] 도 2를 참조하면, 우선, 제1 사용자 단말(110)은 제1 사용자에 대한 공개키 지분 pk₁을 생성한다(201).

[0091] 이후, 제1 사용자 단말(110)은 공개키 지분 pk₁을 제2 사용자 단말(120) 및 제3 사용자 단말(130)로 전송한다(202, 203).

[0092] 이후, 제2 사용자 단말(120)은 제2 사용자에 대한 공개키 지분 pk₂을 생성한다(204).

[0093] 이후, 제2 사용자 단말(120)은 공개키 지분 pk₂을 제1 사용자 단말(110) 및 제3 사용자 단말(130)로 전송한다(205, 206).

[0094] 이후, 제3 사용자 단말(130)은 제3 사용자에 대한 공개키 지분 pk₃을 생성한다(207).

[0095] 이후, 제3 사용자 단말(130)은 공개키 지분 pk₃을 제1 사용자 단말(110) 및 제2 사용자 단말(120)로 전송한다(208, 209).

[0096] 이후, 제1 사용자 단말(110), 제2 사용자 단말(120) 및 제3 사용자 단말(130)은 각각 pk₁, pk₂ 및 pk₃를 이용하여 공개키 pk를 생성한다(210, 211, 212).

[0097] 한편, 도 2에서는 공개키 생성 과정을 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.

[0098] 도 3은 본 발명의 일 실시예에 따른 복호화 과정을 나타낸 순서도이다.

[0099] 도 3을 참조하면, 우선 제1 사용자 단말(110)은 제1 사용자의 개인키 지분 sk₁을 이용하여 암호문 C에 대한 부분 복호화 결과 p₁을 생성한다(301).

[0100] 이때, 암호문 C는 예를 들어, 도 2에 도시된 공개키 생성 과정을 이용하여 생성된 공개키 pk를 이용하여 암호화된 암호문 또는 각각 공개키 pk를 이용하여 암호화된 복수의 암호문 사이의 연산 결과일 수 있다.

[0101] 이후, 제1 사용자 단말(110)은 제2 사용자 단말(120) 및 제3 사용자 단말(130)로 암호문 C에 대한 부분 복호화를 요청한다(302, 303).

- [0102] 이때, 예를 들어, 암호문 C가 제1 사용자 단말(110)에 저장되어 있는 경우, 제1 사용자 단말(110)은 암호문 C를 제2 사용자 단말(120) 및 제3 사용자 단말(130)로 전송하여 암호문 C에 대한 부분 복호화를 요청할 수 있다.
- [0103] 다른 예로, 암호문 C가 제1 사용자 단말(110), 제2 사용자 단말(120) 및 제3 사용자 단말(130)에서 접근 가능한 별도의 데이터베이스(미도시) 또는 서버(미도시)에 저장되어 있는 경우, 제1 사용자 단말(110)은 제2 사용자 단말(120) 및 제3 사용자 단말(130)로 해당 데이터베이스(미도시) 또는 서버(미도시)에 저장된 암호문 C에 대한 부분 복호화를 요청할 수 있다.
- [0104] 한편, 제1 사용자 단말(110)로부터 암호문 C에 대한 부분 복호화를 요청받은 제2 사용자 단말(120)은 각각 제2 사용자의 개인키 지분 sk_2 를 이용하여 암호문 C에 대한 부분 복호화 결과 p_2 를 생성한다(304).
- [0105] 또한, 제1 사용자 단말(110)로부터 암호문 C에 대한 부분 복호화를 요청받은 제3 사용자 단말(130)은 각각 제3 사용자의 개인키 지분 sk_3 를 이용하여 암호문 C에 대한 부분 복호화 결과 p_3 를 생성한다(305).
- [0106] 이후, 제2 사용자 단말(120) 및 제3 사용자 단말(130)은 각각 생성한 부분 복호화 결과 p_2 및 p_3 를 제1 사용자 단말(110)로 전송한다(306, 307).
- [0107] 이후, 제1 사용자 단말(110)은 부분 복호화 결과 p_1 , p_2 및 p_3 를 이용하여 암호문 C에 대한 평문 데이터를 생성한다(308).
- [0108] 한편, 도 3에 도시된 순서도에서는 상기 복호화 과정을 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 추가되어 수행될 수 있다.
- [0109] 도 4는 예시적인 실시예들에서 사용되기에 적합한 컴퓨팅 장치를 포함하는 컴퓨팅 환경을 예시하여 설명하기 위한 블록도이다. 도시된 실시예에서, 각 컴포넌트들은 이하에 기술된 것 이외에 상이한 기능 및 능력을 가질 수 있고, 이하에 기술되지 것 이외에도 추가적인 컴포넌트를 포함할 수 있다.
- [0110] 도시된 컴퓨팅 환경(10)은 컴퓨팅 장치(12)를 포함한다. 일 실시예에서, 컴퓨팅 장치(12)는 각 사용자 단말(110, 120, 130)에 포함되는 하나 이상의 컴포넌트일 수 있다.
- [0111] 컴퓨팅 장치(12)는 적어도 하나의 프로세서(14), 컴퓨터 판독 가능 저장 매체(16) 및 통신 버스(18)를 포함한다. 프로세서(14)는 컴퓨팅 장치(12)로 하여금 앞서 언급된 예시적인 실시예에 따라 동작하도록 할 수 있다. 예컨대, 프로세서(14)는 컴퓨터 판독 가능 저장 매체(16)에 저장된 하나 이상의 프로그램들을 실행할 수 있다. 상기 하나 이상의 프로그램들은 하나 이상의 컴퓨터 실행 가능 명령어를 포함할 수 있으며, 상기 컴퓨터 실행 가능 명령어는 프로세서(14)에 의해 실행되는 경우 컴퓨팅 장치(12)로 하여금 예시적인 실시예에 따른 동작들을 수행하도록 구성될 수 있다.
- [0112] 컴퓨터 판독 가능 저장 매체(16)는 컴퓨터 실행 가능 명령어 내지 프로그램 코드, 프로그램 데이터 및/또는 다른 적합한 형태의 정보를 저장하도록 구성된다. 컴퓨터 판독 가능 저장 매체(16)에 저장된 프로그램(20)은 프로세서(14)에 의해 실행 가능한 명령어의 집합을 포함한다. 일 실시예에서, 컴퓨터 판독 가능 저장 매체(16)는 메모리(랜덤 액세스 메모리와 같은 휘발성 메모리, 비휘발성 메모리, 또는 이들의 적절한 조합), 하나 이상의 자기 디스크 저장 디바이스들, 광학 디스크 저장 디바이스들, 플래시 메모리 디바이스들, 그 밖에 컴퓨팅 장치(12)에 의해 액세스되고 원하는 정보를 저장할 수 있는 다른 형태의 저장 매체, 또는 이들의 적합한 조합일 수 있다.
- [0113] 통신 버스(18)는 프로세서(14), 컴퓨터 판독 가능 저장 매체(16)를 포함하여 컴퓨팅 장치(12)의 다른 다양한 컴포넌트들을 상호 연결한다.
- [0114] 컴퓨팅 장치(12)는 또한 하나 이상의 입출력 장치(24)를 위한 인터페이스를 제공하는 하나 이상의 입출력 인터페이스(22) 및 하나 이상의 네트워크 통신 인터페이스(26)를 포함할 수 있다. 입출력 인터페이스(22) 및 네트워크 통신 인터페이스(26)는 통신 버스(18)에 연결된다. 입출력 장치(24)는 입출력 인터페이스(22)를 통해 컴퓨팅 장치(12)의 다른 컴포넌트들에 연결될 수 있다. 예시적인 입출력 장치(24)는 포인팅 장치(마우스 또는 트랙패드 등), 키보드, 터치 입력 장치(터치패드 또는 터치스크린 등), 음성 또는 소리 입력 장치, 다양한 종류의 센서 장치 및/또는 촬영 장치와 같은 입력 장치, 및/또는 디스플레이 장치, 프린터, 스피커 및/또는 네트워크 카드와 같은 출력 장치를 포함할 수 있다. 예시적인 입출력 장치(24)는 컴퓨팅 장치(12)를 구성하는 일 컴포넌트로서 컴퓨팅 장치(12)의 내부에 포함될 수도 있고, 컴퓨팅 장치(12)와는 구별되는 별개의 장치로 컴퓨팅 장치(12)와

연결될 수도 있다.

[0115] 이상에서 대표적인 실시예를 통하여 본 발명에 대하여 상세하게 설명하였으나, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 전술한 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.

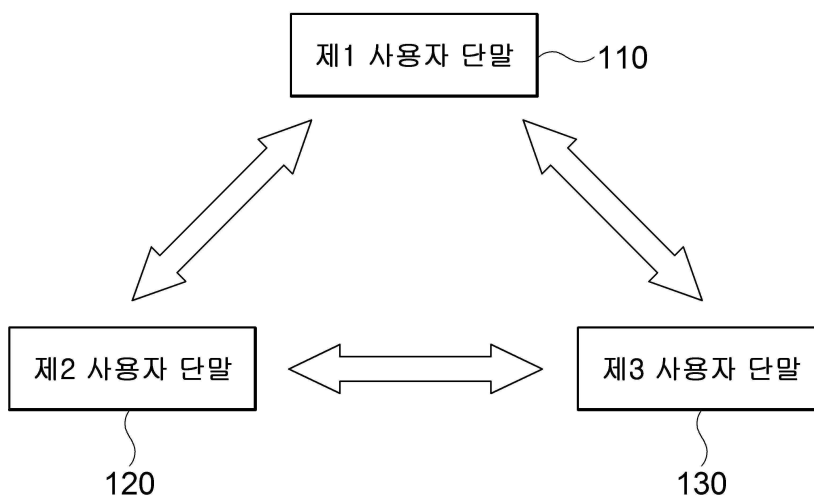
부호의 설명

[0116] 10: 컴퓨팅 환경
12: 컴퓨팅 장치
14: 프로세서
16: 컴퓨터 판독 가능 저장 매체
18: 통신 버스
20: 프로그램
22: 입출력 인터페이스
24: 입출력 장치
26: 네트워크 통신 인터페이스
100: 암호화 시스템
110: 제1 사용자 단말
120: 제2 사용자 단말
130: 제3 사용자 단말

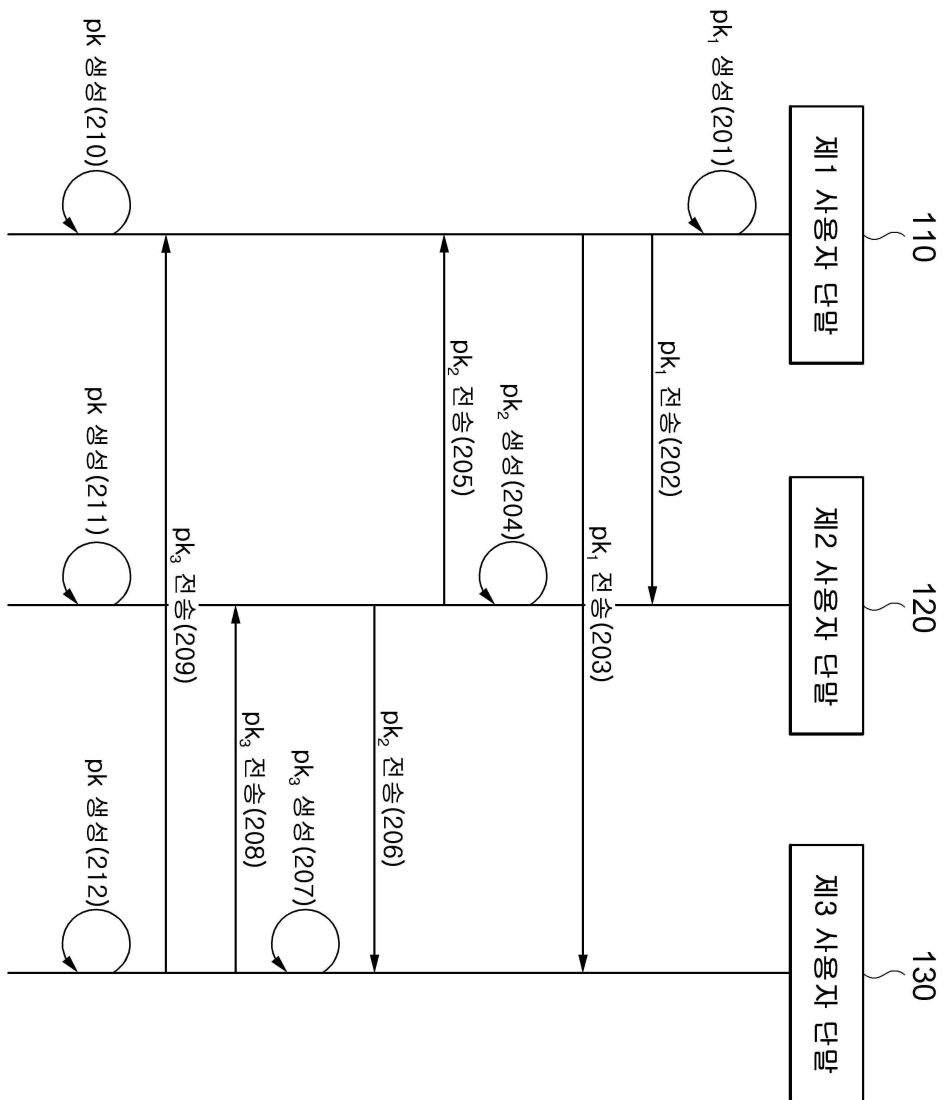
도면

도면1

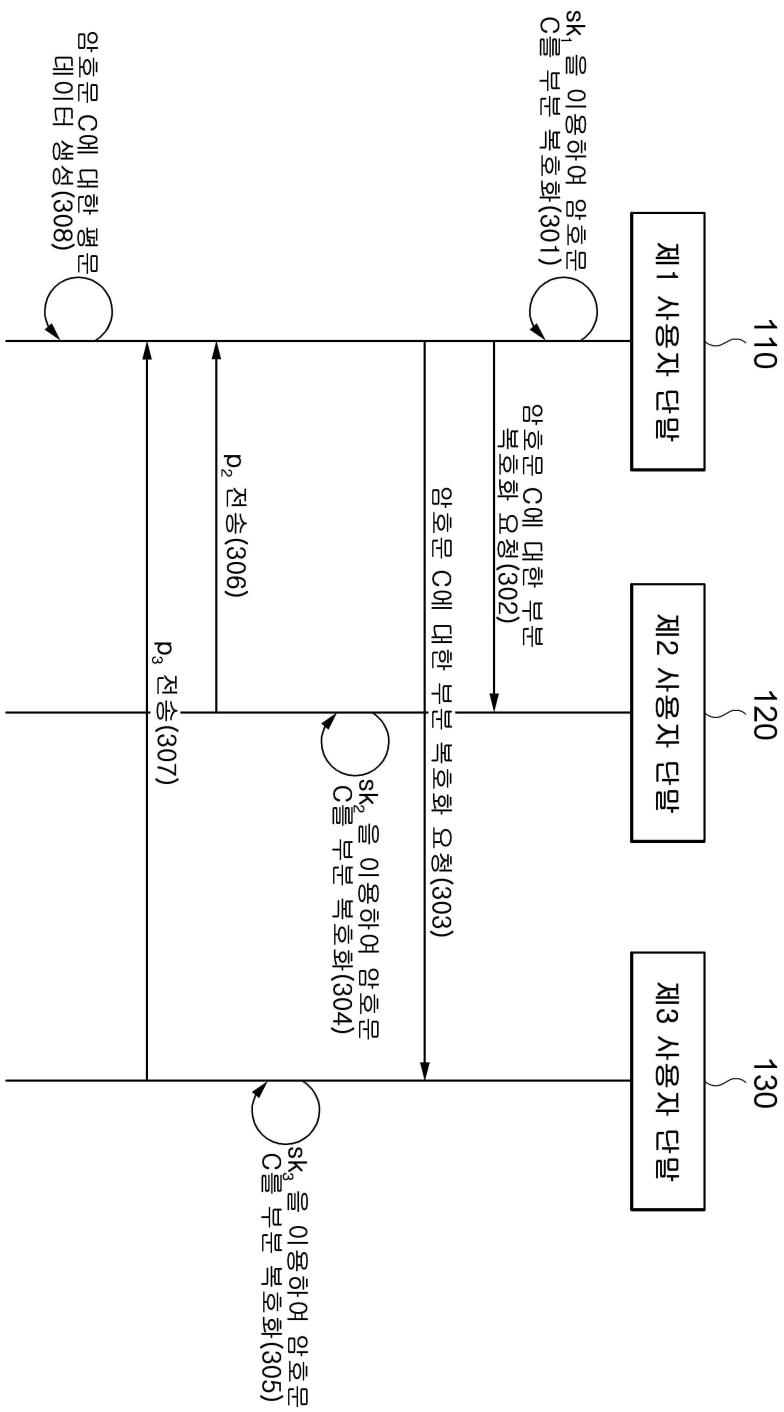
100



도면2



도면3



도면4

10

