(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년03월10일
(11) 등록번호 10-2224998
(24) 등록일자 2021년03월03일

(51) 국제특허분류(Int. Cl.)
G06F 21/62 (2013.01) *G06F 21/60* (2013.01)
H04L 9/08 (2006.01)
(52) CPC특허분류
G06F 21/6209 (2013.01)
G06F 21/602 (2013.01)
(21) 출원번호 10-2017-0062798
(22) 출원일자 2017년05월22일
심사청구일자 2020년05월15일
(65) 공개번호 10-2017-0142872
(43) 공개일자 2017년12월28일
(30) 우선권주장
15/185,575 2016년06월17일 미국(US)
(56) 선행기술조사문헌
EP2924911 A1
WO2016051591 A1

(73) 특허권자
팔로 알토 리서치 센터 인코포레이티드
미국 캘리포니아주 94304 팔로 알토 코요테 힐 로드 3333
(72) 발명자
배니쉬리, 라오
미합중국 94043 캘리포니아주 마운틴 뷰 유닛 266 사이프레스 포인트 드라이브 505
샨타누, 래인
미합중국 94025 캘리포니아주 멘로 파크 아파트먼트 201 사론 파크 드라이브 675
(뒷면에 계속)
(74) 대리인
장훈

전체 청구항 수 : 총 18 항 심사관 : 구대성

(54) 발명의 명칭 **데이터 재-암호화를 통하여 민감한 데이터를 보호하기 위한 컴퓨터-구현 시스템 및 방법**

(57) 요 약

데이터 재-암호화를 통하여 민감한 데이터를 보호하기 위한 컴퓨터-구현 방법이 제공된다. 암호화된 데이터는 유지된다. 데이터 질의는 공개 키 및 비밀 키와 연관된 사용자로부터 수신된다. 질의의 결과는 암호화된 데이터 중 적어도 일부를 식별함으로써 그리고 결과로서 암호화된 데이터 중 식별된 부분에 대한 평문을 더함으로써 컴퓨팅된다. 재-암호화 키는 사용자의 공개 키를 사용하여 결과에 대해 생성되고 그리고 결과는 재-암호화 키를 사용하여 재-암호화된다. 재-암호화된 결과는 그 후 사용자에 송신된다.

(52) CPC특허분류
H04L 9/0861 (2013.01)
(72) 발명자
에르신, 우준
미합중국 95008 캘리포니아주 캠벨 카프리 드라이브 1186
알레한드로, 이. 브리토
미합중국 94040 캘리포니아주 마운틴 뷰 오르테가 에비뉴 163

명 세 서

청구범위

청구항 1

데이터 재-암호화를 통하여 민감한 데이터를 보호하기 위한 컴퓨터-구현 시스템으로서,

데이터 소유자의 암호화된 데이터를 유지하기 위한 데이터베이스로서, 상기 암호화된 데이터는 상기 암호화된 데이터의 기저에 있는 평문의 덧셈을 지원하는 속성을 포함하고 상기 데이터 소유자의 공개 키를 통하여 암호화되는, 상기 데이터베이스;

사용자로부터 질의를 수신하고 상기 사용자로부터의 상기 질의를 충족하는 상기 암호화된 데이터의 적어도 일부를 식별하기 위한 프로세서;

중앙 처리 장치, 메모리, 상기 질의를 수신하기 위한 입력 포트, 및 출력 포트를 포함하는 서버로서, 상기 중앙 처리 장치는 상기 사용자의 공개 키를 사용하여 상기 암호화된 데이터의 식별된 부분에 대한 재-암호화 키, 상기 데이터 소유자의 비밀 키, 및 요소들의 군으로부터 선택되는 2개의 랜덤 요소들을 생성하도록 구성되는, 상기 서버; 및

중앙 처리 장치, 메모리, 상기 데이터베이스로부터 상기 암호화된 데이터의 상기 식별된 부분 및 상기 서버로부터 상기 재-암호화 키를 수신하기 위한 입력 포트, 및 출력 포트를 포함하는 추가적 서버로서, 상기 중앙 처리 장치는:

상기 재-암호화 키를 사용하여 상기 암호화된 데이터의 상기 식별된 부분을 재-암호화된 데이터로서 재-암호화하고;

상기 질의에 응답하여 상기 재-암호화된 데이터를 상기 사용자에 송신하도록 구성되는, 상기 추가적 서버를 포함하는, 컴퓨터-구현 시스템.

청구항 2

제1항에 있어서,

상기 사용자에 대한 공개 파라미터들을 생성하고 상기 공개 파라미터들 중 적어도 하나를 사용하여 상기 공개 키를 생성하기 위한 공개 키 생성기를 더 포함하는, 컴퓨터-구현 시스템.

청구항 3

제1항에 있어서,

상기 사용자에 대한 개인 파라미터들(private parameters)을 생성하고 상기 개인 파라미터들 중 적어도 하나를 사용하여 상기 사용자에 대한 비밀 키(secret key)를 컴퓨팅하기 위한 비밀 키 생성기를 더 포함하는, 컴퓨터-구현 시스템.

청구항 4

제1항에 있어서,

각각의 데이터 아이템을 세그먼트들로 분할하고, 각각의 세그먼트를 제1 블록 및 제2 블록을 포함하는 2개의 블록들로 더 분할하고, 상기 데이터 아이템에서 각각의 세그먼트로부터 상기 제1 블록을 수집하고 암호문을 생성하고, 상기 데이터 아이템에서 각각의 세그먼트로부터 상기 제2 블록을 수집하고 암호문을 생성하고, 당해 데이터 아이템의 암호화로서 상기 제1 블록 및 상기 제2 블록으로부터의 상기 암호문을 조합함으로써 상기 암호화된 데이터의 각각의 데이터 아이템을 암호화하기 위한 메시지 암호화기를 더 포함하는, 컴퓨터-구현 시스템.

청구항 5

제1항에 있어서,

상기 데이터 소유자와 연관된 상기 비밀 키 및 상기 사용자의 상기 공개 키의 각각을 2개의 섹션들로 파싱하고, 상기 2개의 랜덤 요소들을 선택하고, 상기 랜덤 요소들 중 하나, 상기 비밀 키의 제 1 섹션, 및 상기 공개 키의

제 1 섹션에 기초하여 상기 재-암호화 키의 제 1 부분을 컴퓨팅하고, 다른 랜덤 요소, 상기 비밀 키의 제 2 섹션, 및 상기 공개 키의 제 2 섹션에 기초하여 상기 재-암호화 키의 제 2 부분을 컴퓨팅하고, 상기 재-암호화 키로서 상기 제 1 및 제 2 부분들을 조합함으로써 상기 재-암호화 키를 계산하기 위한 재-암호화 키 생성기를 더 포함하는, 컴퓨터-구현 시스템.

청구항 6

제1항에 있어서,

상기 질의의 사용자를 식별하고 재-암호화를 위해 식별된 사용자와 연관된 상기 재-암호화 키를 액세스하기 위한 키 액세스 모듈을 더 포함하는, 컴퓨터-구현 시스템.

청구항 7

제1항에 있어서,

상기 암호화된 데이터 아이템을 2개의 부분들로 분할하고, 상기 재-암호화 키로부터의 요소들 및 상기 암호화된 데이터 아이템의 상기 제 1 부분을 사용하여 제 1 재-암호화 성분을 컴퓨팅하고, 상기 재-암호화 키로부터의 요소들 및 암호화된 데이터 아이템의 상기 제 2 부분을 사용하여 제 2 재-암호화 성분을 계산하고, 재-암호화된 데이터 아이템으로서 상기 제 1 및 제 2 재-암호화 성분들을 조합함으로써 상기 암호화된 데이터의 상기 식별된 부분의 하나의 상기 암호화된 데이터 아이템에 대해 상기 재-암호화를 수행하기 위한 재-암호화 모듈을 더 포함하는, 컴퓨터-구현 시스템.

청구항 8

제1항에 있어서,

상기 재-암호화된 결과들은 상기 암호화된 데이터의 암호문과는 다른 암호문을 포함하는, 컴퓨터-구현 시스템.

청구항 9

제8항에 있어서,

상기 재-암호화된 암호문을 2개의 부분들로 분할하고, 오라클 및 디코딩 알고리즘을 상기 제 1 부분에 적용하고 상기 디코딩 알고리즘을 상기 제 2 부분에 적용하고, 암호화된 데이터 아이템의 상기 암호문으로서 상기 제 1 및 제 2 부분들을 조합함으로써 하나의 상기 데이터 아이템의 상기 재-암호화된 암호문을 복호화하기 위한 복호화 모듈을 더 포함하는, 컴퓨터-구현 시스템.

청구항 10

데이터 재-암호화를 통하여 민감한 데이터를 보호하기 위한 컴퓨터-구현 방법으로서,

데이터 소유자의 암호화된 데이터를 유지하는 단계로서, 상기 암호화된 데이터는 상기 암호화된 데이터의 기저에 있는 평문의 덧셈을 지원하는 속성을 포함하고 상기 데이터 소유자의 공개 키를 통하여 암호화되는, 상기 암호화된 데이터를 유지하는 단계;

사용자로부터 질의를 수신하는 단계;

상기 사용자로부터의 질의를 충족하는 상기 암호화된 데이터의 적어도 일부를 식별하는 단계;

상기 사용자의 공개 키, 상기 데이터 소유자의 비밀 키, 및 요소들의 군으로부터 선택되는 2개의 랜덤 요소들을 사용하여 상기 암호화된 데이터의 식별된 부분에 대한 재-암호화 키를 생성하는 단계; 및

상기 재-암호화 키를 사용하여 상기 암호화된 데이터의 식별된 부분을 재-암호화된 데이터로서 재-암호화하는 단계; 및

상기 질의의 결과로서 상기 재-암호화된 데이터를 상기 사용자에 송신하는 단계를 포함하는, 컴퓨터-구현 방법.

청구항 11

제10항에 있어서,

상기 사용자에 대한 공개 파라미터들을 생성하는 단계; 및

상기 공개 파라미터들 중 적어도 하나를 사용하여 상기 공개 키를 생성하는 단계를 더 포함하는, 컴퓨터-구현 방법.

청구항 12

제10항에 있어서,

상기 사용자에 대한 개인 파라미터들을 생성하는 단계; 및

상기 개인 파라미터들 중 적어도 하나를 사용하여 상기 사용자에 대한 비밀 키를 컴퓨팅하는 단계를 더 포함하는, 컴퓨터-구현 방법.

청구항 13

제10항에 있어서,

상기 암호화된 데이터의 각각의 아이템을 암호화하는 단계를 더 포함하고, 상기 암호화하는 단계는:

각각의 데이터 아이템을 세그먼트들로 분할하는 단계;

각각의 세그먼트를 제1 블록 및 제2 블록을 포함하는 2개의 블록들로 더 분할하는 단계;

상기 데이터 아이템에서 각각의 세그먼트로부터 상기 제1 블록을 수집하고 암호문을 생성하는 단계;

상기 데이터 아이템에서 각각의 세그먼트로부터 상기 제2 블록을 수집하고 암호문을 생성하는 단계; 및

당해 데이터 아이템의 암호화로서 상기 제1 블록 및 상기 제2 블록으로부터의 상기 암호문을 조합하는 단계를 포함하는, 컴퓨터-구현 방법.

청구항 14

제10항에 있어서,

상기 재-암호화 키를 계산하는 단계를 더 포함하고, 상기 재-암호화 키를 계산하는 단계는:

상기 데이터 소유자와 연관된 상기 비밀 키 및 상기 사용자의 상기 공개 키의 각각을 2개의 섹션들로 파싱하는 단계;

상기 2개의 랜덤 요소들을 선택하는 단계;

상기 랜덤 요소들 중 하나, 상기 비밀 키의 제 1 섹션, 및 상기 공개 키의 제 1 섹션에 기초하여 상기 재-암호화 키의 제 1 부분을 컴퓨팅하는 단계;

다른 랜덤 요소, 상기 비밀 키의 제 2 섹션, 및 상기 공개 키의 제 2 섹션에 기초하여 상기 재-암호화 키의 제 2 부분을 컴퓨팅하는 단계; 및

상기 재-암호화 키로서 상기 제 1 및 제 2 부분들을 조합하는 단계를 포함하는, 컴퓨터-구현 방법.

청구항 15

제10항에 있어서,

상기 사용자를 식별하는 단계; 및

재-암호화를 위해 식별된 사용자와 연관된 상기 재-암호화 키를 액세스하는 단계를 더 포함하는, 컴퓨터-구현 방법.

청구항 16

제10항에 있어서,

상기 암호화된 데이터의 상기 식별된 부분의 하나의 상기 암호화된 데이터 아이템에 대해 상기 재-암호화를 수행하는 단계를 더 포함하고, 상기 재-암호화를 수행하는 단계는:

상기 암호화된 데이터 아이템을 2개의 부분들로 분할하는 단계;

상기 재-암호화 키로부터의 요소들 및 상기 암호화된 데이터 아이템의 상기 제 1 부분을 사용하여 제 1 재-암호화 성분을 컴퓨팅하는 단계;

상기 재-암호화 키로부터의 요소들 및 상기 암호화된 데이터 아이템의 상기 제 2 부분을 사용하여 제 2 재-암호화 성분을 계산하는 단계; 및

재-암호화된 데이터 아이템으로서 상기 제 1 및 제 2 재-암호화 성분들을 조합하는 단계를 포함하는, 컴퓨터-구현 방법.

청구항 17

제10항에 있어서,

상기 재-암호화된 결과들은 상기 암호화된 데이터의 암호문과는 다른 암호문을 포함하는, 컴퓨터-구현 방법.

청구항 18

제17항에 있어서,

하나의 상기 데이터의 아이템의 상기 재-암호화된 암호문을 복호화하는 단계; 및

상기 사용자의 비밀 키를 통하여 상기 재-암호화된 데이터를 복호화하는 단계 중 하나를 더 포함하고,

상기 재-암호화된 암호문을 복호화하는 단계는:

상기 재-암호화된 암호문을 2개의 부분들로 분할하는 단계;

오라클 및 디코딩 알고리즘을 상기 제 1 부분에 적용하고 상기 디코딩 알고리즘을 상기 제 2 부분에 적용하는 단계; 및

암호화된 데이터 아이템의 상기 암호문으로서 상기 제 1 및 제 2 부분들을 조합하는 단계를 포함하는, 컴퓨터-구현 방법.

발명의 설명

기 술 분 야

[0001] 본 출원은 일반적으로는 데이터 암호화에 관한 것이고, 그리고 구체적으로는 데이터 재-암호화를 통하여 민감한 데이터를 보호하기 위한 컴퓨터-구현 시스템 및 방법에 관한 것이다.

배 경 기 술

[0002] 회사는 정상적 사업 과정 동안 다량의 데이터를 수집하려는 경향이 있다. 데이터 중 적어도 일부는, 사회 보장 번호를 포함하여, 고객 식별, 의료 프로필, 및 금융 거래와 같은, 민감한 정보를 포함한다. 수집되고 나면, 회사는, 회사 정책에 의해 또는 정부 가이드라인 및 정책에 의해 요구되는 대로, 때로는 장기간의 시간 동안 데이터를 저장하여야 한다. 그렇지만, 과반수의 회사는 요구되는 상당량의 저장 공간에 기인하여 데이터를 자체 저장할 수 없고 그리하여 더 큰 회사로부터 저장 및 컴퓨팅 능력을 임차하는 것에 의존한다. 데이터를 저장하도록 더 큰 회사에 의해 사용되는 서버는 공중 및 보통은 클라우드 기반이다.

[0003] 부가적으로, 비즈니스 인텔리전스 분야는 동향을 식별하고, 전략을 이끌고, 그리고 성공적 사업 실시를 지원하기 위해 분석론에 의존한다. 분석은 공통적으로는 회사에 의해 고용된 분석가에 의해 수행된다. 이들 분석가에게는, 분석 이전에 저장된 데이터를 복호화하기 위한 복호화 키를 포함하여, 중요한 툴이 맡겨져 있다. 그렇지만, 적과 같은 권한 없는 개인이 복호화 키를 획득하면, 데이터를 저장하고 있는 데이터베이스 전체로의 액세스가 승인된다. 불행하게도, 분석가의 모바일 디바이스는 보통은 강력한 침입 방지 메커니즘을 구비하고 있지 않아서, 분석가를 적에 의한 공격에 대한 약한 링크가 되게 한다.

[0004] 권한 없는 개인으로부터 데이터 소유자의 민감한 정보를 보호하는 것은 데이터의 부정유용을 방지하는데 극도로 중요하다. 현재, 민감한 데이터는 서버가 데이터에 관심 있는 당사자와 우선 맞물리고 그 후 관심 있는 당사자가 데이터에 액세스하기 전에 액세스 제어 메커니즘에 의해 확립된 인증 프로토콜을 통과하기 위해 필요한 크리

덴셜을 입력할 것을 요구하도록 데이터가 저장되어 있는 서버에서 액세스 제어 메커니즘을 통하여 보호될 수 있다. 불행하게도, 권한 부여된 사용자에 대한 크리덴셜의 권한 없는 액세스에 기인하여 여러 보안 위반이 최근 증가되었다.

[0005] 사용자가 크리덴셜을 입력할 것을 요구하는 것에 부가하여, 저장되는 데이터는 데이터 콘텐츠로의 액세스를 방지함으로써 위반 효과를 감축하도록 부가적 보안 계층으로서 저장 이전에 암호화될 수 있다. 그렇지만, 암호화 자체는 일반적으로는 데이터 콘텐츠의 누설을 방지하기에 충분한 보안은 아니다. 예를 들면, 데이터를 암호화하기 위해, 회사는 일반적으로는 저장 이전에 데이터를 암호화하도록 공개 키를 이용한다. 후속하여, 회사와 연관된 사용자는 데이터에 액세스할 필요가 있지만, 그렇게 하기 위해, 암호화된 데이터를 복호화하도록 회사의 비밀 키(secret key)를 획득하여야 한다. 회사의 다수의 사용자가 비밀 키로의 액세스를 가능하게 하는 것은 사용자가 키를 권한 없는 사용자에게 제공할 수 있으므로 데이터를 취약한 위치에 둔다. 부가적으로, 비밀 키에는 권한 없는 사용자가 직접 액세스할 수 있어, 데이터 콘텐츠로의 액세스를 초래할 수 있다. 불행하게도, 인간은 보통은 단순한 사회 공학적 공격에 의해 쉽게 속으므로 비밀 키를 획득하는 것은 꽤 쉬울 수 있다.

[0006] 그래서, 개선된 데이터 보호 및 위반 방지에 대한 접근법이 필요하다. 바람직하게는, 데이터 보호 및 위반 방지는 데이터에 액세스하도록 권한 부여된 개인을 통한 또는 데이터 자체로의 권한 없는 액세스의 효과를 감축하도록 다량의 평문 데이터에 대한 재-암호화 기법을 포함할 것이다.

발명의 내용

[0007] 보안 클라우드-컴퓨팅 아키텍처는 관용적 보안 방법에 비해 위반 기회를 감축하고 그리고 민감한 데이터의 보안을 증가시키도록 사용될 수 있다. 공개 및 비밀 암호화 키는 클라우드 기반 서버 상에 민감한 데이터를 저장하는 데이터 소유자에 대해 그리고 데이터에 액세스하도록 권한 부여된 각각의 개인에 대해 생성될 수 있다. 저장 이전에, 데이터는 데이터 소유자의 공개 키를 사용하여 암호화된다. 사용자는 암호화된 데이터에 액세스하도록 질의를 제출할 수 있고 그리고 질의의 결과는 저장된 암호화된 데이터에 기반하여 결정된다. 재-암호화 키는 요청하는 사용자에 대해 그의 공개 키를 사용하여 생성된다. 암호문 형태인 암호화된 데이터 결과는 그 후, 재-암호화 키를 사용하여, 다른 암호문 형태로 재-암호화된다. 재-암호화된 결과는 요청하는 개인에 제공되고 그 후 분석 및 추가적 사용을 위해 복호화된다. 구체적으로, 재-암호화된 암호문의 복호화는 기저 평문, 즉, 질의 결과를 드러낸다.

[0008] 일 실시형태는 데이터 재-암호화를 통하여 민감한 데이터를 보호하기 위한 컴퓨터-구현 방법을 제공한다. 암호화된 데이터는 유지된다. 데이터 질의는 공개 키 및 비밀 키와 연관된 사용자로부터 수신된다. 질의의 결과는 암호화된 데이터 중 적어도 일부를 식별함으로써 그리고 결과로서 암호화된 데이터 중 식별된 부분에 대한 평문을 더함으로써 컴퓨팅된다. 재-암호화 키는 사용자의 공개 키를 사용하여 결과에 대해 생성되고 그리고 결과는 재-암호화 키를 사용하여 재-암호화된다. 재-암호화된 결과는 그 후 사용자에 송신된다.

[0009] 본 발명의 또 다른 실시형태는, 본 발명을 수행하도록 고려되는 최상 모드를 예시하는 것에 의해 본 발명의 실시형태가 설명되는, 이하의 상세한 설명으로부터 당업자에게는 쉽게 분명하게 될 것이다. 인식될 바와 같이, 본 발명은 다른 그리고 상이한 실시형태가 가능하고 그리고 그 수 개의 상세는 다양한 자명한 관점에서 수정이 가능하며, 전부 본 발명의 취지 및 범위로부터 벗어나지 않는다. 따라서, 도면 및 상세한 설명은 본질이 예시적인 것으로 그리고 제한적이지 않은 것으로 간주되어야 한다.

도면의 간단한 설명

[0010] 도 1은, 일 실시형태에 따라, 데이터 재-암호화를 통하여 민감한 데이터를 보호하기 위한 컴퓨터-구현 시스템을 도시하는 블록 선도,

도 2는, 일 실시형태에 따라, 데이터 재-암호화를 통하여 민감한 데이터를 보호하기 위한 컴퓨터-구현 방법을 도시하는 순서도,

도 3은, 예로서, 암호화 셋업을 수행하기 위한 프로세스를 도시하는 순서도,

도 4는, 예로서, 공개 키 및 비밀 키를 생성하기 위한 프로세스를 도시하는 순서도,

도 5는, 예로서, 도 4의 공개 키를 사용하여 데이터를 암호화하기 위한 프로세스를 도시하는 순서도,

도 6은, 예로서, 재-암호화 키를 생성하기 위한 프로세스를 도시하는 순서도,

도 7은, 예로서, 도 6의 재-암호화 키를 사용하여 암호문을 재-암호화하기 위한 프로세스를 도시하는 순서도, 및

도 8은, 예로서, 암호문을 복호화하기 위한 프로세스를 도시하는 순서도.

발명을 실시하기 위한 구체적인 내용

[0011] 회사는 다량의 데이터를 수집 및 저장한다. 고용된 분석가는, 비즈니스 인텔리전스에서의 사용을 위해서와 같이, 수집된 데이터를 분석할 수 있다. 그렇지만, 분석가는 각각, 분석 이전에 암호화된 데이터를 복호화하기 위한 복호화 키와 같은, 극도로 중요한 툴을 맡고 있으므로 보통은 약한 링크라고 생각된다. 불행하게도, 분석가의 대부분은 강력한 침입 방지 메커니즘을 구비하고 있지 않고, 그리하여 공격이 흔하다. 별개로 각각의 데이터 소유자에 대한 데이터를 암호화하고 데이터 소유자에 의해 권한 부여된 특정 사용자에 대한 데이터를 재-암호화하는 것은 서버로의 권한 없는 액세스, 신뢰할 수 없는 사용자, 또는 데이터의 보안 정보에 대한 비밀 공유가 허용된 사용자에 대한 공격에 기인하는 데이터의 위반을 방지하는 것을 돕는다.

[0012] 재-암호화는 암호화된 데이터베이스를 복호화하도록 사용되는 복호화 키가 더 이상 종단점에 거처하지 않는 것을 용이하게 한다. 도 1은, 일 실시형태에 따라, 데이터 재-암호화를 통하여 민감한 데이터를 보호하기 위한 컴퓨터-구현 시스템(10)을 도시하는 블록 선도이다. 시간의 흐름에 따라, 데이터 소유자는 정상적 사업 과정 동안, 소유자와 연관된 서버(11)에 상호접속되는 로컬 데이터베이스(15) 상에 원래 저장될 수 있는, 다량의 데이터(16)를 수집할 수 있다. 데이터(16)는 문서, 메시지, 음성 녹음, 비디오 클립, 의료 기록, 금융 거래, 및 위치 데이터는 물론, 다른 유형의 데이터도 포함할 수 있다. 데이터베이스(15)는 또한 데이터 소유자에 대한 비밀 키(18) 및 공개 키(17)를 포함할 수 있다.

[0013] 서버(11)는 암호화기(12), 셋업 모듈(13), 및 키 생성기(14)를 포함한다. 암호화기(12)는 데이터베이스(15) 상에 저장된 데이터(16)를 암호화하도록 데이터 소유자의 공개 키를 이용한다. 암호화되고 나면, 데이터(23)는 클라우드 기반 서버(19)와 연관된 데이터베이스(22)에 저장을 위해 송신된다. 클라우드 기반 저장소는 극도로 다량의 저장 공간을 제공하여, 데이터 소유자가 모든 데이터를 로컬 저장하는 부담을 덜어준다. 클라우드 기반 서버로부터의 암호화된 데이터(23)에 액세스하기 위해, 권한 부여된 사용자는 각각 공개 키(29) 및 비밀 키(30)와 연관되되, 공개 키는 그 사용자의 컴퓨팅 디바이스(24)와 연관된 데이터베이스(28)에 유지되어 있을 수 있다. 대안으로, 공개 키(29)는 클라우드 기반 서버의 데이터베이스에 저장될 수 있다. 사용자의 공개 키(29) 및 비밀 키(30)는, 도 3을 참조하여 아래에서 더 설명되는 바와 같이, 데이터(23)에 액세스하도록 권한 부여된 각각의 사용자에 대한 키를 생성하도록 키 생성기(14)에 의해 사용될 수 있는 파라미터를 출력하는, 셋업 모듈(13)을 통하여 소유자의 서버(11)에 의해 생성될 수 있다.

[0014] 각각의 권한 부여된 사용자는 데이터에 관한 분석론을 수행하도록, 데스크톱 또는 랩톱 컴퓨터는 물론, 또한 모바일 디바이스와 같은, 컴퓨팅 디바이스(24)를 통하여 소유자의 암호화된 데이터(23)에 액세스할 수 있다. 구체적으로, 컴퓨팅 디바이스(24)는 복호화기(27) 및 질의를 생성하기 위한 질의 생성기(26)를 갖는 서버(25)와 연관된다. 질의는, 질의를 수신 및 파싱하기 위한 질의 수신기(20), 및 질의에 응답하여 암호화된 데이터(23)를 프로세싱하고 하나 이상의 암호화된 결과를 생성하는 결과 파인더(21)를 포함하는, 클라우드 기반 서버(19)에 송신된다. 질의의 결과는 결과의 기저 평문을 더함으로써 컴퓨팅된다. 그렇지만, 암호화된 결과를 사용자에 제공하기 이전에, 결과는, 키 생성기(32) 및 재-암호화기(33)를 포함하는, 프록시 재-암호화 서버(31)에 송신된다. 키 생성기(32)는, 도 6에 대해 더 상세히 아래에서 설명되는 바와 같이, 그 요청하는 사용자의 공개 키 및 데이터 소유자의 비밀 키에 기반하여 각각의 권한 부여된 사용자에 대한 재-암호화 키(35)를 생성한다. 사용자에 대한 재-암호화 키(35)는 암호문 영역에서 덧셈 준동형 연산을 지원할 수 있고 그리고 프록시 재-암호화기(31)와 연관된 데이터베이스(34)에 저장된다. 재-암호화기(33)는 데이터 소유자의 공개 키에 따라서로부터 요청하는 사용자의 공개 키로 암호화된 데이터 결과의 암호문을 재-암호화하고 그리고 재-암호화된 결과를 요청하는 사용자에 송신한다. 요청하는 사용자에 의해 수신되고 나면, 재-암호화된 데이터 결과는 복호화기(27)에 의해 요청하는 사용자의 비밀 키를 사용하여 복호화될 수 있다. 재-암호화된 암호문의 복호화는 기저 평문, 즉 질의 결과를 드러낸다.

[0015] 모바일 컴퓨팅 디바이스 및 서버는 각각 여기에서 개시된 실시형태를 수행하기 위한 하나 이상의 모듈을 포함할 수 있다. 모듈은 관용적 프로그래밍 언어로 소스 코드로서 기록된 컴퓨터 프로그램 또는 프로시저로서 구현될 수 있고 그리고 객체 또는 바이트 코드로서 중앙 처리 장치에 의한 실행을 위해 제시된다. 대안으로, 모듈은 또한, 집적 회로로서, 하드웨어로 구현될 수 있고 그리고 서버 및 클라이언트의 각각은 전문 컴퓨터로서 역할할

수 있다. 소스 코드 및 객체 및 바이트 코드의 다양한 구현은, 플로피 디스크, 하드 드라이브, 디지털 비디오 디스크(DVD), 램(RAM), 롬(ROM) 및 유사한 저장 매체와 같은, 컴퓨터-판독가능한 저장 매체 상에 유지될 수 있다. 다른 유형의 모듈 및 모듈 기능은 물론, 다른 물리적 하드웨어 컴포넌트도 가능하다.

[0016] 암호문을 재-암호화하는 것은, 복호화 키의 공유를 방지하고 부가적 레벨의 보안을 더함으로써, 데이터 위반을 방지하는 것은 물론, 일어나는 어느 위반의 효과도 최소화하는 것도 돕는다. 구체적으로, 재-암호화 키가 도용되면, 권한 없는 사용자가 그 키로 할 수 있는 전부는 암호문을 하나의 공개 키로부터 다른 하나로 변환하는 것이다. 환언하면, 권한 없는 사용자는 암호문을 복호화할 수 없다. 도 2는, 일 실시형태에 따라, 데이터 재-암호화를 통하여 민감한 데이터를 보호하기 위한 컴퓨터-구현 방법(40)을 도시하는 순서도이다. 데이터 소유자는, 데이터 소유자 자신 및 소유자의 데이터에 액세스하도록 권한 부여된 사용자에 대한 공개 및 비밀 키를 생성(블록(42))하기 위한 파라미터를 식별하는 것을 포함하여, 셋업을 수행한다(블록(41)). 파라미터를 생성하는 것은 도 3에 대해 상세히 아래에서 더 설명되는 한편, 데이터 소유자 및 사용자에 대한 공개 및 비밀 키를 생성하는 것은 도 4를 참조하여 아래에서 더 설명된다. 셋업과 동시에 또는 후속하여, 권한 부여된 사용자 중 하나 이상에 대한 재-암호화 키는, 도 6을 참조하여 아래에서 더 설명되는 바와 같이, 그 사용자의 공개 키를 사용하여 생성될 수 있다(블록(43)).

[0017] 소유자에 의해 수집된 데이터는, 도 5를 참조하여 아래에서 더 설명되는 바와 같이, 소유자의 공개 키를 사용하여 암호화되고(블록(44)) 그리고 하나 이상의 클라우드 기반 서버 상에 저장될 수 있다. 하나 이상의 권한 부여된 사용자는 데이터의 적어도 하나의 부분집합에 대한 질의를 제출(블록(45))함으로써 암호화된 데이터에 관한 분석론을 수행할 수 있다. 덧셈 준동형 알고리즘을 사용하여 그리고 암호화된 데이터에 기반하여, 질의의 결과는 질의를 충족하는 암호화된 결과의 기저 평문을 더함으로써 컴퓨팅된다(블록(46)). 요청하는 사용자에 결과를 제공하기 이전에, 암호화된 및 평문 결과를 포함하는 결과는, 도 7을 참조하여 아래에서 더 설명되는 바와 같이, 재-암호화 키를 사용하여 재-암호화된다(블록(47)). 그 후, 재-암호화된 결과는, 도 8을 참조하여 아래에서 더 설명되는 바와 같이, 요청하는 사용자에 제공되고(블록(48)) 그리고 사용자에 의한 사용을 위해 복호화될 수 있다(블록(49)).

[0018] 소유자의 데이터에 액세스하도록 권한 부여된 각각의 사용자는 공개 키 및 비밀 키와 연관된다. 사용자의 키는 데이터 소유자와의 그들 공통 관계에 기반하여 관련되어야 한다. 셋업 단계는, 모든 권한 부여된 사용자의 키가 파라미터의 공통 집합에 기반하여 함께 묶이게 되도록, 키를 생성하기 위한 파라미터를 결정한다. 도 3은, 예로서, 암호화 셋업을 수행하기 위한 프로세스(50)를 도시하는 순서도이다. 셋업 동안, 각각 차수 $N = p_1^k p_2^k p_3$의, 2개의 곱셈 순환군 G 및 G_T을 식별하도록 이중선형 군 생성기 알고리즘이 실행된다(블록(51)). p_1, p_2, 및 p_3의 각각은 $\dot{g}$, G의 생성기, 및 이중선형 사상 e: $G \times G \rightarrow G_T$과 함께, 이중선형 군 생성기 알고리즘을 통하여 또한 출력되는 구별되는 소수이고, 그리고 k는 N보다 작은 양의 정수이다. 그리하여, 실행되고 나면, 이중선형 군 생성기는 이하의 파라미터의 각각을 식별한다: $(\mathbb{G}, \mathbb{G}_T, e, N, \dot{g}, p_1, p_2, p_3)$, 여기서 $\dot{g}$는 군 생성기이다.

[0019] 요소의 집합 $Z_N = \{0, 1, \ldots N-1\}$이 액세스되고(블록(53)) 그리고 집합 Z_N으로부터 요소의 2개의 부분집합이 랜덤 선택된다(블록(54)). 각각의 랜덤 선택된 요소는 요소의 2개의 계산된 집합을 생성하도록 지수화를 통해 프로세싱된다(블록(55)). 예컨대, 집합 Z_N으로부터 요소의 2개의 부분집합 $\alpha_0, \alpha_1, \ldots \alpha_{k-1}$ 및 $\beta_0, \beta_1, \ldots \beta_{k-1}$이 랜덤 선택되고, 그리고 다음의 등식:

[0020] $$h_i = \left(\dot{g}^{p_2^k p_3}\right)^{\alpha_i p_1^i}$$

[0021] $$f_i = \left(\dot{g}^{p_1^k p_2}\right)^{\beta_i p_2^i}$$

[0022] 에서 별개로 채용되어 파라미터 $h_0, \ldots, h_{k-1}, f_0, \ldots, f_{k-1}$를 생성할 수 있다.

[0023] 또한, 셋업 단계 동안, 도 8을 참조하여 아래에서 더 설명되는 바와 같이, 소수 중 하나를 사용하여 암호화된 및 재-암호화된 암호문을 복호화하도록 디코딩 알고리즘과의 사용을 위해 복호화 오라클이 구축된다(블록(56)).

마지막으로, 파라미터 G, G_T, N, g, e, 및 파라미터의 계산된 군 $h_0, \ldots, h_{k-1}, f_0, \ldots, f_{k-1}$은 공개 파라미터로서 출력되는 한편(블록(57)), p_1, p_2, 및 p_3는 개인 파라미터(private parameter)로서 데이터 소유자에 의해 저장된다(블록(58)).

[0024] 셋업이 수행되고 나면, 데이터 소유자 및 하나 이상의 사용자에 대한 비밀 키 및 공개 키가 생성될 수 있다. 예컨대, 새로운 종업원을 고용시, 종업원이 고용주에 의해 소유되고 클라우드 기반 서버 상에 저장된 암호화된 데이터에 액세스하도록 공개 및 비밀 키가 생성될 수 있다. 도 4는, 예로서, 공개 키 및 비밀 키를 생성하기 위한 프로세스(60)를 도시하는 순서도이다. 군 G은 공개 셋업 파라미터로부터 액세스되고 그리고 군으로부터의 2개의 요소는 랜덤 선택된다(블록(61)). 일 실시형태에서, 요소는 다른 공개 셋업 파라미터, 군 Z_N으로부터의 γ 및 $\tilde{\gamma}$를 샘플링하고, 그리고 그 후 셋업 단계로부터의 군 생성기 g를 사용함으로써 다음과 같이 결정될 수 있다, $g = \dot{g}^{\gamma}, \tilde{g} = \dot{g}^{\tilde{\gamma}}$.

[0025] 부가적으로, 2개의 요소의 2개의 군은 각각 집합 Z_N으로부터 랜덤 선택된다(블록(62)). 예컨대, $a, \tilde{a} \leftarrow \mathbb{Z}_N$ 및 $b, \tilde{b} \leftarrow \mathbb{Z}_N$. 공개 키는 Z_N에 대한 랜덤 요소의 2개의 군 및 G로부터의 랜덤 요소를 사용하여 컴퓨팅된다(블록(63)). 구체적으로, G로부터의 및 Z_N 으로부터의 랜덤 요소는 $g^a, g^b, \tilde{g}^{\tilde{a}}$, 및 $\tilde{g}^{\tilde{b}}$를 생성하도록 컴퓨팅된다. 그 후, 공개 키는 $\mathrm{pk} = \left((g, g^a, g^b), (\tilde{g}, \tilde{g}^{\tilde{a}}, \tilde{g}^{\tilde{b}})\right)$로서 출력된다(블록(65)).

[0026] 그러는 동안, 비밀 키는 개인 파라미터 중 하나 및 Z_N으로부터 선택된 랜덤 요소의 군 양자에 기반하여 컴퓨팅된다(블록(64)). 일 실시형태에서, p_1은 개인 파라미터에 사용된다; 그렇지만, 개인 파라미터 중 다른 하나가 사용될 수 있다. 그 후, 비밀 키는 $sk = ((a, b, g), (\tilde{a}, \tilde{b}, \tilde{g}), p_1)$로서 출력된다(블록(65)). 출력시(블록(65)), 공개 키 및 비밀 키는 데이터 소유자에 의해 유지되는 것은 물론, 또한 저장된 데이터에 액세스하도록 연관된 사용자에 제공될 수 있다. 셋업 단계로부터의 파라미터의 사용은 또한 위의 식별된 프로세스를 사용하여 데이터 소유자에 대한 공개 및 비밀 키를 생성하도록 사용될 수 있다.

[0027] 데이터, 특히 민감한 데이터를 클라우드 기반 서버 상에 저장하기 이전에, 데이터 소유자는 위반을 방지하는 것은 물론, 위반이 일어나면 데이터로의 액세스를 감축하는 것도 돕도록 데이터를 암호화할 수 있다. 도 5는, 예로서, 도 4의 공개 키를 사용하여 데이터를 암호화하기 위한 프로세스(70)를 도시하는 순서도이다. 암호화될, 메시지와 같은, 데이터는 데이터 소유자의 공개 키와 수신된다(블록(71)). 각각의 메시지는 세그먼트 M_i로 분할되고(블록(72)) 그리고 각각의 세그먼트는 그 후 2개의 블록, $M_i^{[1]}$ 및 $M_i^{[2]}$으로 분할된다(블록(73)). 일 실시형태에서, 메시지 세그먼트는 비밀 공유를 사용하여 분할된다; 그렇지만, 메시지 세그먼트를 분할하기 위한 다른 프로세스가 가능하다.

[0028] 각각의 메시지에 대해, 제1 메시지 블록 $M_i^{[1]}$ 전부가 수집되고(블록(74)) 그리고 제2 메시지 블록 $M_i^{[2]}$ 전부가 수집된다(블록(77)). 후속하여, 제1 블록 집합 및 제2 블록 집합 상에 별개로 인코딩 알고리즘이 실행된다(블록(75, 78)). 각각의 블록 군에 대한 알고리즘은 동시에 또는 비동기식으로 실행될 수 있다. 인코딩 알고리즘은 입력으로서 데이터 소유자의 공개 키 $pk = \left((g, g^a, g^b), (\tilde{g}, \tilde{g}^{\tilde{a}}, \tilde{g}^{\tilde{b}})\right)$ 및 메시지를 수신한다. 일 실시형태에서, 인코딩 알고리즘은 다음과 같다:

$$Encode\left(\{g_i\}_{i=0}^{k-1}, (m_0, \ldots m_{k-1})\right) = \prod_{i=0}^{k-1} g_i^{m_i}$$

[0029]

[0030] 인코딩 알고리즘의 실행 동안, 2개의 요소의 2개의 군은 Z_N으로부터 샘플링되고, $r, s \leftarrow Z_N$ 및 $\tilde{r}, \tilde{s} \leftarrow Z_N$ 그리

고 메시지를 인코딩하도록 사용된다. 구체적으로, 제1 메시지 블록의 군은 다음의 등식에 따라 암호문 C_1을 생성하도록 암호화된다(블록(76)).

[0031] $$C_1 = ((g^a)^r, (g^b)^s, g^{r+s} \cdot Encode\left(\{h_i\}_{I=0}^{k-1}, (m_0[1], \ldots, m_{k-1}[1])\right))$$

[0032] 여기서 h_i는, 도 3을 참조하여 위에서 설명된 바와 같이, 셋업 단계 동안 식별된 공개 파라미터 중 일부를 표현한다. 그러는 동안, 제2 메시지 블록의 군은 다음의 등식에 따라 암호문 C_2을 생성하도록 암호화된다(블록(79)).

[0033] $$C_2 = ((\tilde{g}^{\tilde{a}})^{\tilde{r}}, (\tilde{g}^{\tilde{b}})^{\tilde{s}}, \tilde{g}^{\tilde{r}+\tilde{s}} \cdot Encode\left(\{f_i\}_{I=0}^{k-1}, (m_0[2], \ldots, m_{k-1}[2])\right))$$

[0034] 여기서 f_i는, 도 3을 참조하여 위에서 설명된 바와 같이, 셋업 단계 동안 식별된 공개 파라미터 중 일부를 표현한다. 그 후, 제1 메시지 블록 C_1 및 제2 메시지 블록 C_2에 대한 암호문은, 후에 암호화된 메시지로서 출력되는(블록(81)), 메시지에 대한 암호문 C = (C_1, C_2)으로서 조합된다(블록(80)).

[0035] 암호화된 데이터가 저장되고 나면, 사용자는 질의를 제출함으로써 데이터를 분석할 수 있다. 질의의 결과는, 예컨대, 클라우드 기반 서버를 통하여 식별될 수 있다. 그렇지만, 요청하는 사용자에 결과를 제공하기 이전에, 암호화된 결과는 데이터 소유자의 공개 키에 따라서로부터 사용자의 공개 키에 따라서로 재-암호화된다. 도 6은, 예로서, 재-암호화 키를 생성하기 위한 프로세스(90)를 도시하는 순서도이다. 데이터 소유자의 비밀 키 $sk = ((a,b,g),(\tilde{a},\tilde{b},\tilde{g}),p_1)$ 및 사용자의 공개 키 $pk = ((g,g^a,g^b),(\tilde{g},\tilde{g}^{\tilde{a}},\tilde{g}^{\tilde{b}}))$는 입력으로서 수신된다(블록(91)). 데이터 소유자의 비밀 키 및 사용자의 공개 키의 각각은 파싱되고(블록(92)), 그리고 2개의 요소는 집합 Z_N으로부터 랜덤 선택된다(블록(93)), $z,\tilde{z} \leftarrow Z_N$. 재-암호화 키 r_k는 다음과 같이 2개의 부분으로 컴퓨팅된다.

[0036] $rk_{S\to R} = ((Z_1,Z_2,Z_3),(\tilde{Z}_1,\tilde{Z}_2,\tilde{Z}_3))$, 여기서:

[0037] $$(Z_1,Z_2,Z_3) = ((g_R^{a_R})^{\frac{z}{a_s}}, (g_R^{b_R})^{\frac{z}{b_s}}, g_R^{z})$$

[0038] $$(\tilde{Z}_1,\tilde{Z}_2,\tilde{Z}_3) = ((\tilde{g}_R^{\tilde{a}_R})^{\frac{\tilde{z}}{\tilde{a}_s}}, (\tilde{g}_R^{\tilde{b}_R})^{\frac{\tilde{z}}{\tilde{b}_s}}, \tilde{g}_R^{\tilde{z}})$$

[0039] 구체적으로, 재-암호화 키의 제1 절반은 집합 Z_N으로부터 선택된 제1 랜덤 요소 z, 데이터 소유자의 비밀 키의 제1 부분 (a,b,g), 및 사용자의 공개 키의 제1 부분 (a,g^a,g^b)을 사용하여 컴퓨팅된다(블록(94)). 또한, 재암호화 키의 제2 절반은 집합 Z_N으로부터 선택된 제2 랜덤 요소 $\tilde{z}$, 데이터 소유자의 비밀 키의 제2 부분 $(\tilde{a},\tilde{b},\tilde{g})$, 및 사용자의 공개 키의 제2 부분 $(\tilde{g},\tilde{g}^{\tilde{a}},\tilde{g}^{\tilde{b}})$을 사용하여 컴퓨팅된다(블록(95)). 계산되고 나면, 재암호화 키의 2개의 부분은 조합되고(블록(96)) 그리고 암호화된 데이터 결과를 재암호화하도록 출력된다(블록(97)).

[0040] 암호화된 데이터의 암호문을 재-암호화하는 것은 사용자가, 데이터 소유자의 비밀 키보다는, 그의 비밀 키를 사용하여 데이터를 복호화할 수 있게 하고, 그리고 부가적 레벨의 보안을 제공한다. 도 7은, 예로서, 도 6의 재-암호화 키를 사용하여 암호문을 재-암호화하기 위한 프로세스(100)를 도시하는 순서도이다. 요청하는 사용자에 대한 재-암호화 키 $rk_{S\to R} = \left((Z_1,Z_2,Z_3),(\tilde{Z}_1,\tilde{Z}_2,\tilde{Z}_3)\right)$ 및 암호화된 데이터 결과의 암호문 $C = (C_1,C_2)$은 입력으로서 수신된다(블록(101)). 일 실시형태에서, $C_1 = (W,X,Y)$, 여기서:

[0041] $$W = (g^a)^r$$

[0042] $$X = (g^b)^s$$

[0043] $$Y = g^{r+s} \cdot Encode\left(\{h_i\}_{i=0}^{k-1}, (m_0[1], \ldots, m_{k-1}[1])\right)$$

[0044] 그리고 $C_2 = (\tilde{W}, \tilde{X}, \tilde{Y})$, 여기서:

[0045] $$\tilde{W} = (\tilde{g}^{\tilde{a}})^{\tilde{r}}$$

[0046] $$\tilde{X} = (\tilde{g}^{\tilde{b}})^{\tilde{s}}$$

[0047] $$\tilde{Y} = \tilde{g}^{\tilde{r}+\tilde{s}} \cdot Encode\left(\{f_i\}_{i=0}^{k-1}, (m_0[2], \ldots, m_{k-1}[2])\right)$$

[0048] 재-암호화 키의 제1 절반과 암호문의 제1 절반의 성분별 페어링은 재-암호화된 암호문의 제1 부분으로서 다음과 같이 컴퓨팅된다(블록(102)):

[0049] $$E = e(W, Z_1)$$

[0050] $$F = e(X, Z_2)$$

[0051] $$G = e(Y, Z_3)$$

[0052] 재-암호화 키의 제2 절반과 암호문의 제2 절반의 성분-별 페어링은 재-암호화된 암호문의 제2 부분으로서 다음과 같이 컴퓨팅된다(블록(103)):

[0053] $$\tilde{E} = e(\tilde{W}, \tilde{Z}_1)$$

[0054] $$\tilde{F} = e(\tilde{X}, \tilde{Z}_2)$$

[0055] $$\tilde{G} = e(\tilde{Y}, \tilde{Z}_3)$$

[0056] 재-암호화된 암호문의 제1 부분과 제2 부분은 $C_R = \left((E,F,G),(\tilde{E}, \tilde{F},\tilde{G})\right)$로서 조합되고(블록(104)) 그리고 재-암호화된 데이터로서 출력된다(블록(105)).

[0057] 사용자가 재-암호화된 데이터 결과를 수신하고 나면, 사용자의 비밀 키는 재-암호화된 데이터를 복호화하도록 사용될 수 있다. 부가적으로, 데이터 소유자는 암호화된 데이터를, 필요하면, 데이터 소유자의 비밀 키를 사용하여 복호화할 수 있다. 도 8은, 예로서, 암호문을 복호화하기 위한 프로세스(110)를 도시하는 순서도이다. 암호문 및 복호화 키는 입력으로서 수신된다(블록(111)). 암호문은 데이터 소유자에 의해 암호화된 데이터와 같은 프레시 암호문 $C = (C_1, C_2)$이거나, 또는, 재-암호화된 암호문 $C_R = \left((E,F,G),(\tilde{E}, \tilde{F},\tilde{G})\right)$을 포함하는, 프레시 암호문의 합일 수 있다. 또한, 복호화 키는, 복호화될 암호문에 종속하여, 데이터 소유자의 비밀 키 $sk = \left((a,b,g),(\tilde{a},\tilde{b},\tilde{g}),p_1\right)$ 또는 사용자의 비밀 키를 포함할 수 있다. 사용자 또는 데이터 소유자는 암호문의 복호화 요청을 제출하고(블록(112)) 그리고 디코딩 알고리즘이 액세스된다(블록(113)). 암호문이 프레시인지 또는, 재-암호화된 암호문과 같은, 프레시 암호문의 합인지를 포함하는, 암호문 유형의 결정이 이루어진다. 일 실시형태에서, 암호문은 자동으로 분류될 수 있거나, 대안으로, 분류 유형은 개인 또는 다른 사용자에 의해 입력될 수 있다.

[0058] 암호문이 프레시이면, 셋업 동안 생성된 오라클이 액세스되고(블록(114)) 그리고 프레시 암호문의 제1 부분은 오라클 및 디코딩 알고리즘을 통하여 프로세싱된다(블록(115)). 구체적으로, 프레시 암호문의 제1 부분 $C_1 = (W, X, Y)$ 은 다음을 컴퓨팅하도록 사용된다:

[0059] $\frac{Y}{W^{1/a} X^{1/b}}$, 여기서 a 및 b는 비밀 키로부터 획득된다.

[0060] 도 5에 대해 위에서 제공되는 W, X, 및 Y의 값이 입력되고 나면, 등식은 다음과 같이 보인다:

[0061] $$\frac{g^{r+s} \cdot Encode\left(\{h_i\}_{i=0}^{k-1}, (m_0[1], \ldots, m_{k-1}[1])\right)}{g^r \cdot g^s} = Encode\left(\{h_i\}_{i=0}^{k-1}, (m_0[1], \ldots, m_{k-1}[1])\right)$$

[0062] 오라클은 인코딩 알고리즘을 통하여 질의되고 그리고 $\frac{Y}{W^{1/a} X^{1/b}}$ 은 오라클에 입력되어, 아래에서 디코딩 알고리즘을 사용하여 암호문의 제1 부분과 연관된 제1 메시지 블록 $M_i^{[1]}$을 출력한다(블록(116)).

[0063] $Decode\left(0, 2^{\omega} - 1, p_1, \{h_i\}_{i=0}^{k-1}, inp\right)$,

[0064] 여기서 p_1은 개인 파라미터이고 그리고 h_i는 공개 파라미터를 포함하며, 그 양자는 도 3에 대해 위에서 논의되어 있다. 더욱, 디코딩 알고리즘의 최소 i = 0 및 최대 k-1 파라미터는 원래 평문 값의 예상된 범위, 2^{k(w-1)}를 표현한다. 오라클의 출력은 메시지 세그먼트의 제1 블록 $(m_0[1], \ldots, m_{k-1}[1])$ 의 평문을 포함한다.

[0065] 평문의 제1 부분의 프로세싱과 동시에 또는 비동기식으로, 암호문의 제2 부분 $C_2 = (\tilde{W}, \tilde{X}, \tilde{Y})$ 의 프로세싱(블록(117))은, 오라클 없이, 디코딩 알고리즘을 통하여 일어날 수 있다. 구체적으로, 다음과 같이, 암호문의 제2 부분을 사용하여 다음이 컴퓨팅된다:

[0066] $\frac{\tilde{Y}}{\tilde{W}^{\tilde{a}-1} \tilde{X}^{\tilde{b}-1}}$

[0067] 도 5에 대해 위에서 제공되는 W~, X~, 및Z~ 의 값이 입력되고 나면, 등식은 다음과 같이 보인다:

[0068] $$\frac{\tilde{g}^{\tilde{r}+\tilde{s}} \cdot Encode\left(\{f_i\}_{i=0}^{k-1}, (m_0[2], \ldots, m_{k-1}[2])\right)}{\tilde{g}^{\tilde{r}} \cdot \tilde{g}^{\tilde{s}}} = Encode\left(\{f_i\}_{i=0}^{k-1}, (m_0[2], \ldots, m_{k-1}[2])\right)$$

[0069] 후속하여, 디코딩 알고리즘은 아래에서 제공되는 바와 같이 실행된다:

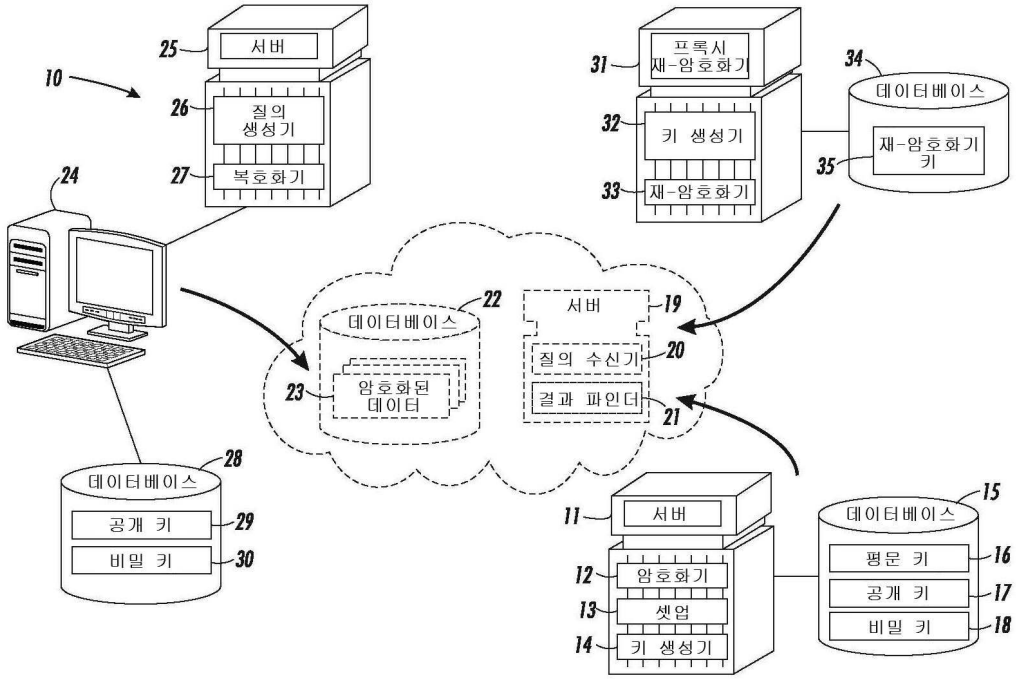
[0070] $Decode\left(0, 2^{\omega} - 1, p_2, \{f_i\}_{i=0}^{k-1}\right), Encode\left(\{f_i\}_{i=0}^{k-1}, (m_0[2], \ldots, m_{k-1}[2])\right)$

[0071] 디코딩 알고리즘의 결과는 메시지 세그먼트의 제2 블록 $(m_0[2], \ldots, m_{k-1}[2])$ 의 평문을 포함한다(블록(118)). 마지막으로, 메시지 세그먼트의 제1 블록과 제2 블록의 평문은 복호화된 메시지로서 조합되어(블록(119)), 시장 조사를 수행하거나 거동 동향 및 패턴을 식별하기 위해서와 같이, 프로세싱 및 분석을 위해 사용자에 출력된다(블록(120)).

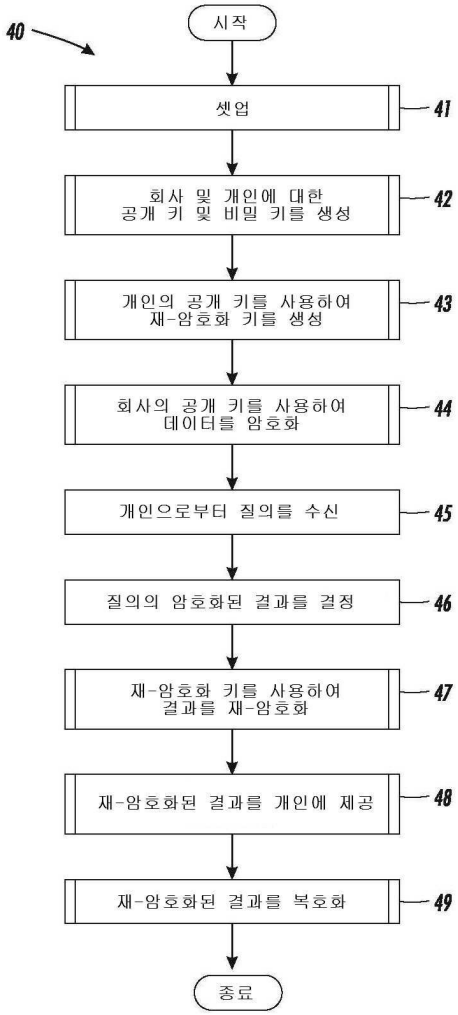
[0072] 암호문이, 재-암호화된 암호문과 같은, 프레시 생성된 암호문의 합이라고 결정되면, 복호화는, 디코딩 알고리즘에서의 최소 및 최대 파라미터가 원래 프레시 암호문에서의 평문 메시지의 예상된 범위 및 더해진 그러한 프레시 암호문의 총 수에 기반하여 컴퓨팅된다는 것을 제외하고는, 위에서 제공된 바와 같이 수행될 수 있다.

도면

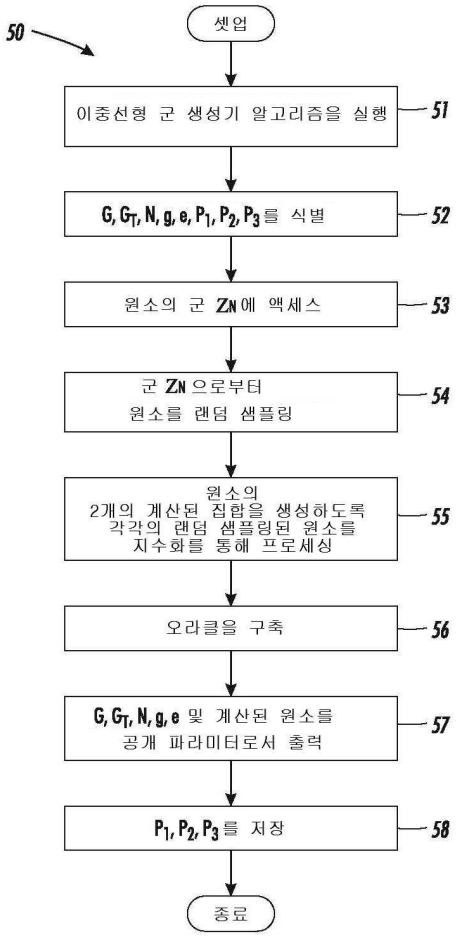
도면1


10
25
서버
26
질의
생성기
27
복호화기
24
31
프록시
재-암호화기
32
키 생성기
33
재-암호화기
34
데이터베이스
재-암호화기
키
35
22
데이터베이스
23
암호화된
데이터
19
서버
20
질의 수신기
21
결과 파인더
28
데이터베이스
공개 키
29
비밀 키
30
11
서버
12
암호화기
13
셋업
14
키 생성기
15
데이터베이스
평문 키
16
공개 키
17
비밀 키
18

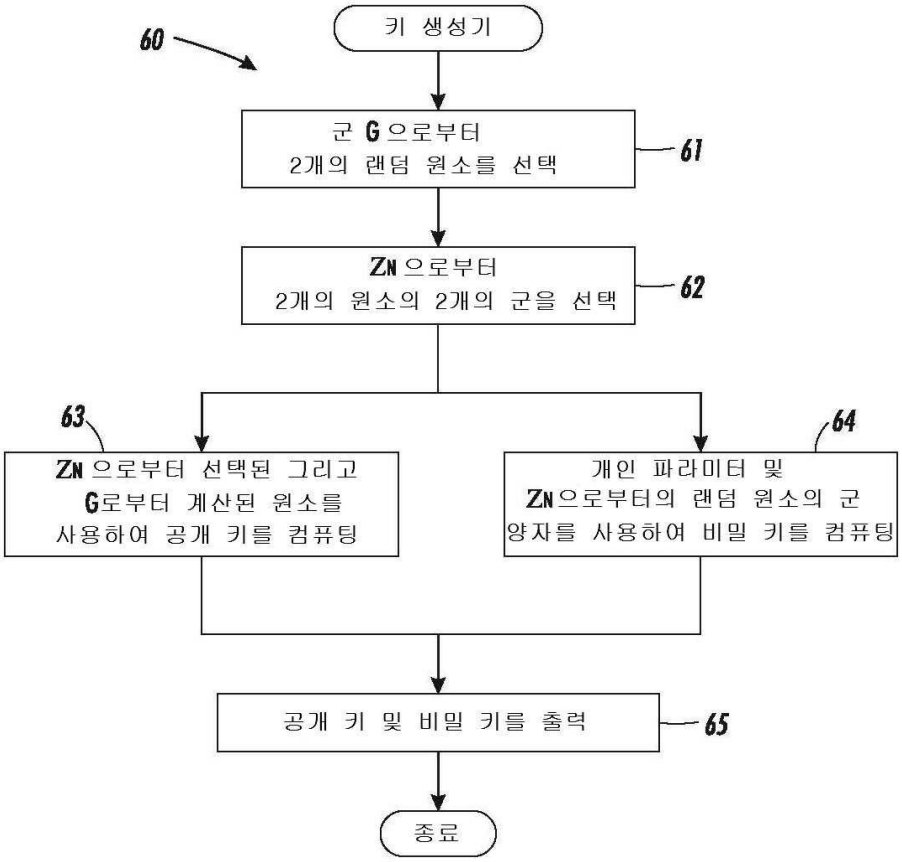
도면2


40
시작
셋업
41
회사 및 개인에 대한
공개 키 및 비밀 키를 생성
42
개인의 공개 키를 사용하여
재-암호화 키를 생성
43
회사의 공개 키를 사용하여
데이터를 암호화
44
개인으로부터 질의를 수신
45
질의의 암호화된 결과를 결정
46
재-암호화 키를 사용하여
결과를 재-암호화
47
재-암호화된 결과를 개인에 제공
48
재-암호화된 결과를 복호화
49
종료

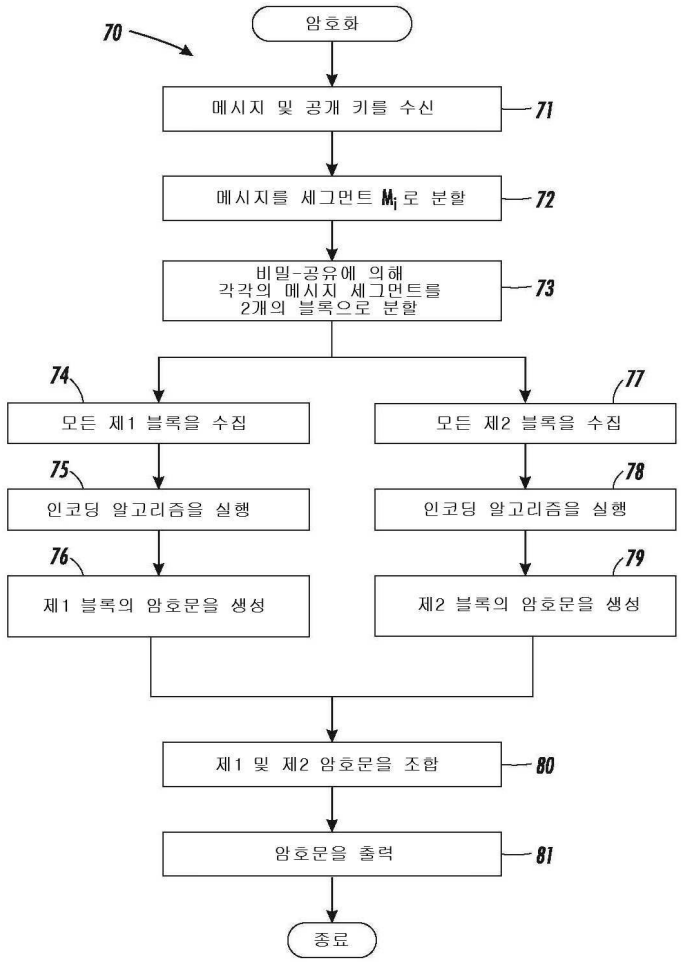
도면3


50
셋업
이중선형 군 생성기 알고리즘을 실행
51
G, G_T, N, g, e, P_1, P_2, P_3를 식별
52
원소의 군 Z_N에 액세스
53
군 Z_N으로부터
원소를 랜덤 샘플링
54
원소의
2개의 계산된 집합을 생성하도록
각각의 랜덤 샘플링된 원소를
지수화를 통해 프로세싱
55
오라클을 구축
56
G, G_T, N, g, e 및 계산된 원소를
공개 파라미터로서 출력
57
P_1, P_2, P_3를 저장
58
종료

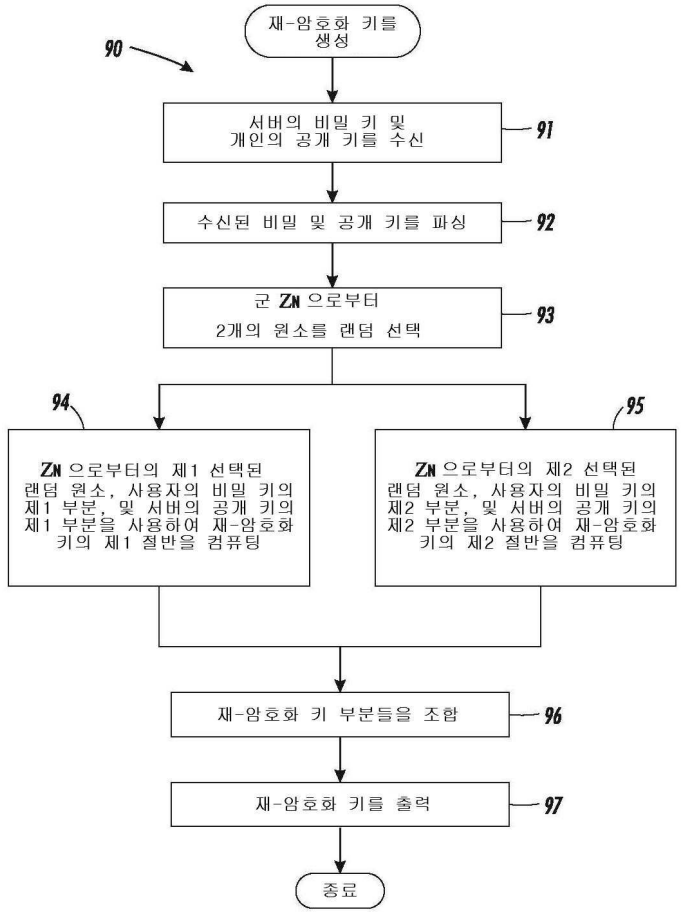
도면4


60
키 생성기
군 G으로부터
2개의 랜덤 원소를 선택
61
ZN으로부터
2개의 원소의 2개의 군을 선택
62
63
ZN으로부터 선택된 그리고
G로부터 계산된 원소를
사용하여 공개 키를 컴퓨팅
64
개인 파라미터 및
ZN으로부터의 랜덤 원소의 군
양자를 사용하여 비밀 키를 컴퓨팅
공개 키 및 비밀 키를 출력
65
종료

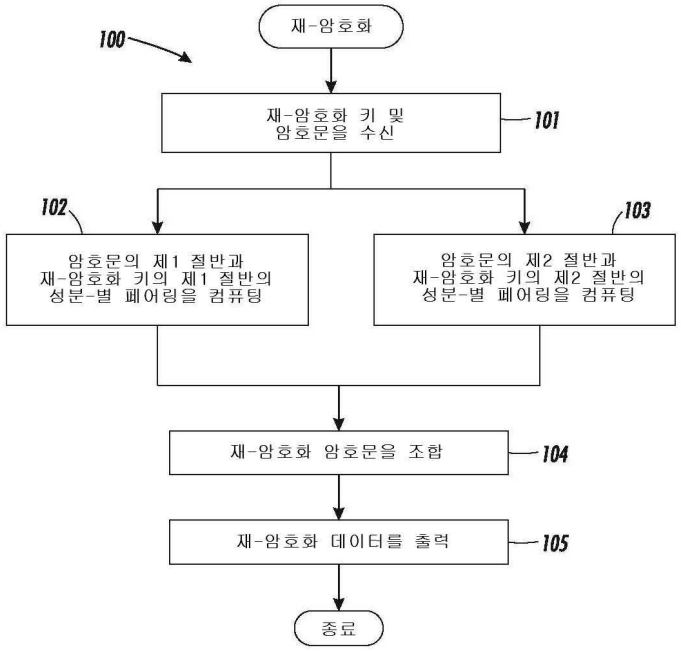
도면5


70
암호화
메시지 및 공개 키를 수신
71
메시지를 세그먼트 M_i로 분할
72
비밀-공유에 의해
각각의 메시지 세그먼트를
2개의 블록으로 분할
73
74
모든 제1 블록을 수집
77
모든 제2 블록을 수집
75
인코딩 알고리즘을 실행
78
인코딩 알고리즘을 실행
76
제1 블록의 암호문을 생성
79
제2 블록의 암호문을 생성
제1 및 제2 암호문을 조합
80
암호문을 출력
81
종료

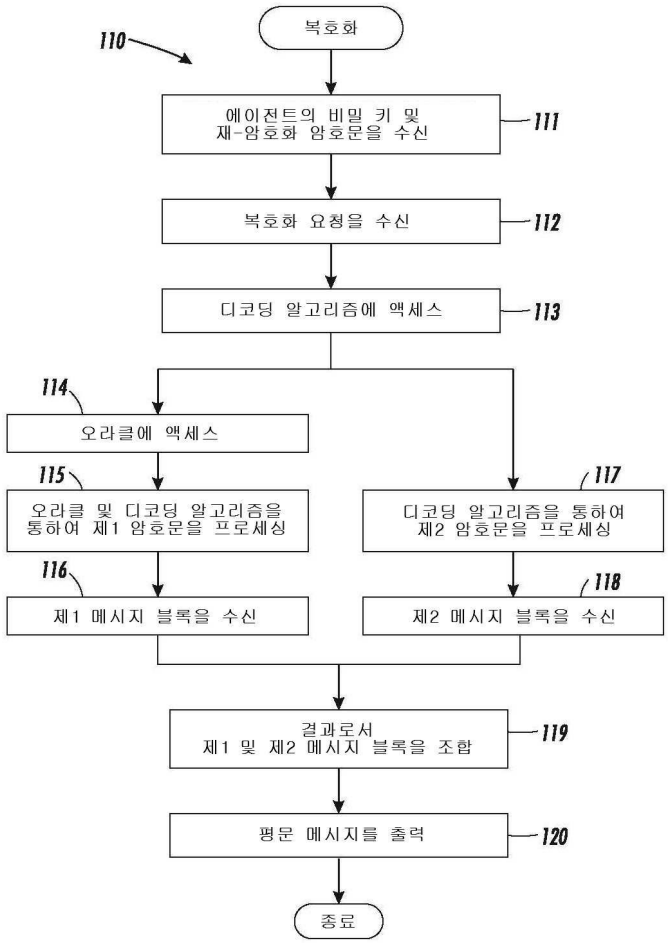
도면6


재-암호화 키를 생성
90
서버의 비밀 키 및 개인의 공개 키를 수신
91
수신된 비밀 및 공개 키를 파싱
92
군 ZN 으로부터 2개의 원소를 랜덤 선택
93
94
ZN 으로부터의 제1 선택된 랜덤 원소, 사용자의 비밀 키의 제1 부분, 및 서버의 공개 키의 제1 부분을 사용하여 재-암호화 키의 제1 절반을 컴퓨팅
95
ZN 으로부터의 제2 선택된 랜덤 원소, 사용자의 비밀 키의 제2 부분, 및 서버의 공개 키의 제2 부분을 사용하여 재-암호화 키의 제2 절반을 컴퓨팅
재-암호화 키 부분들을 조합
96
재-암호화 키를 출력
97
종료

도면7


재-암호화
100
재-암호화 키 및 암호문을 수신
101
102
암호문의 제1 절반과 재-암호화 키의 제1 절반의 성분-별 페어링을 컴퓨팅
103
암호문의 제2 절반과 재-암호화 키의 제2 절반의 성분-별 페어링을 컴퓨팅
재-암호화 암호문을 조합
104
재-암호화 데이터를 출력
105
종료

도면8


110
복호화
에이전트의 비밀 키 및
재-암호화 암호문을 수신
111
복호화 요청을 수신
112
디코딩 알고리즘에 액세스
113
114
오라클에 액세스
115
오라클 및 디코딩 알고리즘을
통하여 제1 암호문을 프로세싱
116
제1 메시지 블록을 수신
117
디코딩 알고리즘을 통하여
제2 암호문을 프로세싱
118
제2 메시지 블록을 수신
결과로서
제1 및 제2 메시지 블록을 조합
119
평문 메시지를 출력
120
종료