(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2018년02월14일
(11) 등록번호 10-1829267
(24) 등록일자 2018년02월08일

(51) 국제특허분류(Int. Cl.)
H04L 9/00 (2006.01) *H04L 9/06* (2006.01)
H04L 9/08 (2006.01) *H04L 9/14* (2006.01)
(52) CPC특허분류
H04L 9/008 (2013.01)
H04L 9/0631 (2013.01)
(21) 출원번호 10-2016-0051432
(22) 출원일자 2016년04월27일
심사청구일자 2016년04월27일
(65) 공개번호 10-2017-0122458
(43) 공개일자 2017년11월06일
(56) 선행기술조사문헌
김세환, 윤현수, "클라우드 컴퓨팅 환경에서의 개인정보보호를 위한 완전 동형 암호 적용 방안 고찰", 정보보호학회논문지 VOL.24, NO.5 (2014.10.)*
Abhishek Banerjee, Chris Peikert and Alon Rosen, "Pseudorandom functions and lattices" (2011.08.10.)*
Jean-Sébastien Coron, Tancrède Lepoint and Mehdi Tibouchi, "Scale-Invariant Fully Homomorphic Encryption over the Integers", Public Key Cryptography, Vol.8383 (2014.)*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
서울대학교산학협력단
서울특별시 관악구 관악로 1 (신림동)
(72) 발명자
천정희
서울특별시 관악구 관악로 1 (신림동)
송용수
서울특별시 관악구 관악로 1 (신림동)
(74) 대리인
백도현

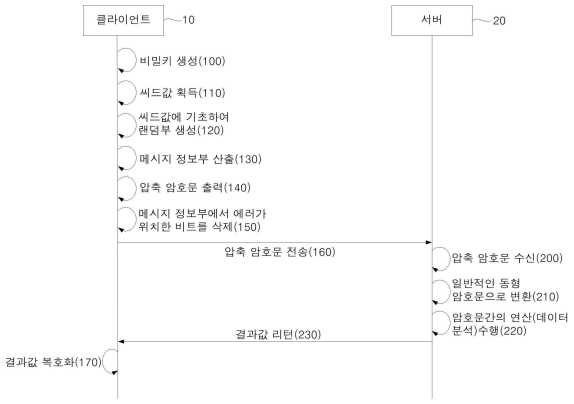
전체 청구항 수 : 총 1 항 심사관 : 박보미

(54) 발명의 명칭 **암호문의 크기가 감소되는 동형 암호화 방법**

(57) 요 약

본 발명은 컴퓨터가 수행하는 동형 암호화 알고리즘을 이용한 암호화 및 복호화 방법에 관한 것으로서 대칭키를 생성하는 제1 단계와; 상기 대칭키를 이용하여 데이터에 대해서 동형 암호화를 수행하는 제2 단계와; 상기 제2 단계의 결과물인 암호화 데이터를 암호화 데이터에 대한 연산이 위임된 서버에 전송하는 제3 단계와; 상기 서버가 수행한 연산 결과를 수신하는 제4 단계와; 상기 제4 단계에서 수신한 연산 결과에 대해서 상기 대칭키로 복호화하는 제5 단계를 포함한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/0869 (2013.01)
H04L 9/14 (2013.01)

명 세 서

청구범위

청구항 1

삭제

청구항 2

컴퓨터가 수행하는 동형 암호화 알고리즘을 이용한 암호화 방법에 있어서,

대칭키(s)를 획득하는 제1 단계와,

시드값(seed)을 획득하는 제2 단계와,

시드값을 의사난수생성기에 입력하여 동형 암호문의 랜덤부(A)를 산출하는 제3 단계와,

제3 단계에서 산출된 랜덤부와 대칭키를 이용하여 메시지 정보부($b = As + \frac{q}{2}m + E(mod\ q)$; m은 메시지)를 산출하는 제4 단계와,

상기 시드값과 상기 메시지 정보부로 구성되는 축약 암호문($c = (seed, b')$; $b' = \lfloor pb/q \rfloor$)을 출력하는 제5 단계를 포함하는,

동형 암호화 방법.

청구항 3

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은 동형 암호화 방법에 관한 것으로서 더 자세하게는 동형 암호화 알고리즘에 의해서 암호화되는 암호문의 크기를 획기적으로 감소시켜서 암호문 전송속도와 효율성 그리고 전송 부하를 감소시키고 보안성도 고양시키는 동형 암호화 방법에 관한 것이다.

배 경 기 술

[0003] 최근에는 서버에 개인 정보 내지 자료를 저장하고 필요한 경우에 사용자가 사용자 단말기를 통해서 서버에 저장되어 있는 데이터를 이용하도록 하는 클라우드 컴퓨팅 환경이 날로 늘어나고 있다. 개인 정보 내지 데이터를 서버에 보관할 때에는 데이터 유출을 방지하는 등 개인 정보 보호를 위해 데이터를 암호화하여 보관하게 된다. 이처럼 암호화된 데이터가 서버에 보관되어 있는 경우 해당 데이터를 검색하거나 연산을 통한 소정의 작업을 할 때에 암호화된 데이터를 일일이 복호화한 후에 원하는 검색 또는 연산을 수행하여야 하기 때문에 매우 비효율적이고, 연산을 위해 일시적으로 복호화된 개인 정보 내지 자료가 제3자에게 유출될 가능성이 증대되는 단점이 존재한다.

[0004] 이러한 문제를 해결하기 위해 동형 암호화 방법이 널리 연구되고 있다. 동형 암호화에 의하면, 암호화된 정보나 자료를 복호화하지 않고 암호문 자체에 대해서 연산을 해도 평문에 대해 동일한 연산을 수행한 후 암호화한 결과와 동일한 결과를 얻기 때문에 암호문을 복호화하지 않고도 소정의 연산을 수행할 수 있다.

[0005] (R)LWE((Ring) Learning With Errors) 기반 동형 암호화 방법과 정수 기반 동형 암호화(Approximate Greatest Common Divisor; AGCD) 방법에서 공개키를 이용하는 경우 안전성을 위해 매우 큰 암호문이 필요하다. 위 이론

에 기반한 동형 암호화를 수행하면 암호문 하나당 수십만 비트까지 크기가 증대하기 때문에 암호문 전송 부하 및 속도가 커다란 문제로 대두되고 있다.

[0006] 또한, 공개키를 이용한 비대칭 암호화 방법에 의해서 데이터를 동형 암호화하고 암호화된 데이터를 연산한 결과를 복호화하는 과정에서 사용자 이외의 자가 복호화키를 소유할 수 있기 때문에 보안성이 저하되는 문제가 있다.

발명의 내용

해결하려는 과제

[0008] 본 발명은 동형 암호화에 있어서 암호문의 크기를 현저하게 감소시킬 수 있는 대칭키를 이용한 동형 암호화 방법을 제시함으로써 전술한 종래 기술의 문제점을 해결할 수 있으며, 나아가 서버 등에 저장된 암호화 데이터에 대해서 연산을 수행한 결과를 사용자가 수신하여 대칭키로 직접 복호화함으로써 종래 기술에 의한 보안성 저하를 방지할 수 있는 대칭키 동형 암호화 방법을 제공하는 것을 목적으로 한다.

과제의 해결 수단

[0010] 본 발명은 컴퓨터가 수행하는 동형 암호화 알고리즘을 이용한 암호화 및 복호화 방법에 관한 것으로서 대칭키를 생성하는 제1 단계와; 상기 대칭키를 이용하여 데이터에 대해서 동형 암호화를 수행하는 제2 단계와; 상기 제2 단계의 결과물인 암호화 데이터를 암호화 데이터에 대한 연산이 위임된 서버에 전송하는 제3 단계와; 상기 서버가 수행한 연산 결과를 수신하는 제4 단계와; 상기 제4 단계에서 수신한 연산 결과에 대해서 상기 대칭키로 복호화하는 제5 단계를 포함한다.

[0011] 본 발명에 의한, 컴퓨터가 수행하는 동형 암호화 알고리즘을 이용한 암호화 방법은 대칭키를 획득하는 제1 단계와; 시드값(seed)을 획득하는 제2 단계와; 시드값을 의사난수생성기에 입력하여 동형 암호문의 랜덤부를 산출하는 제3 단계와; 제2 단계에서 산출된 랜덤부와 대칭키를 이용하여 메시지 정보부를 산출하는 제3 단계와; 상기 시드값과 상기 메시지 정보부로 구성되는 축약 암호문을 출력하는 제4 단계를 포함한다.

[0012] 본 발명의 바람직한 실시 형태에 의하면, 암호문의 메시지 정보부에서 에러가 위치한 비트를 삭제하는 제5 단계를 더 포함할 수 있다.

발명의 효과

[0014] 종래의 동형 암호화 방법에 따라 생성된 암호문이 수십만 비트의 크기를 가지는 것에 반해 본 발명에 의한 동형 암호화 방법에 의하면 그 크기를 수백 비트 수준까지 현저하게 감소시킬 수 있어서 처리 속도와 전송 데이터양이 획기적으로 감소하므로 실제로 구현할 수 있는 동형 암호화 방법을 제공할 수 있다.

[0015] 또한, 동형 암호화 및 복호화에 필요한 키를 사용자만 보유하면 되므로 공개키를 이용한 동형 암호화에 비해서 보안성이 고양되는 효과가 있다.

도면의 간단한 설명

[0017] 도 1은 본 발명에 의한 동형 암호화 방법의 흐름도.

발명을 실시하기 위한 구체적인 내용

[0018] 이하에서는 첨부 도면을 참조하여 본 발명에 대해서 자세하게 설명한다.

[0019] 본 명세서에서 수행되는 정보(데이터) 전송 과정은 필요에 따라서 암호화/복호화가 적용될 수 있으며, 본 명세서 및 특허청구범위에서 정보(데이터) 전송 과정을 설명하는 표현은 별도로 언급되지 않더라도 모두 암호화/복호화하는 경우도 포함하는 것으로 해석되어야 한다. 본 명세서에서 "A로부터 B로 전송(전달)" 또는 "A가 B로부터 수신"과 같은 형태의 표현은 중간에 다른 매개체가 포함되어 전송(전달) 또는 수신되는 것도 포함하며, A로부터 B까지 직접 전송(전달) 또는 수신되는 것만을 표현하는 것은 아니다. 본 발명의 설명에 있어서 각 단계의 순서는 선행 단계가 논리적 및 시간적으로 반드시 후행 단계에 앞서서 수행되어야 하는 경우가 아니라면 각 단계의 순서는 비제한적으로 이해되어야 한다. 즉 위와 같은 예외적인 경우를 제외하고는 후행 단계로 설명된 과정이 선행 단계로 설명된 과정보다 앞서서 수행되더라도 발명의 본질에는 영향이 없으며 권리범위 역시 단계의 순서에 관계없이 정의되어야 한다. 그리고 본 명세서에서 “A 또는 B”은 A와 B 중 어느 하나를 선택적으로 가

리키는 것 뿐만 아니라 A와 B 모두를 포함하는 것도 의미하는 것으로 정의된다. 또한, 본 명세서에서 "포함"이라는 용어는 포함하는 것으로 나열된 요소 이외에 추가로 다른 구성요소를 더 포함하는 것도 포괄하는 의미를 가진다.

[0020] 도 1에는 본 발명에 의한 대칭키를 이용한 동형 암호화 방법의 과정이 도시되어 있다.

[0021] 본 발명에 의한 동형 암호화 방법은 동형 암호화를 수행하는 클라이언트(10)와, 동형 암호화된 암호문에 대해서 연산을 수행하는 서버(20)를 포함하는 환경에서 수행된다. 클라이언트(10)와 서버(20)는 전자적 연산과 데이터 처리가 가능한 컴퓨터 장치일 수 있으며 본 발명에 의한 동형 암호화 및 복호화, 그리고 연산 내지 데이터 분석 등의 처리가 가능한 데스크탑 컴퓨터, 노트북 컴퓨터 등의 개인용 컴퓨터 내지 모바일 장치, 태블릿PC 또는 서버 컴퓨터 장치가 될 수 있다.

[0022] 본 명세서에서는 LWE에 기반한 동형 암호화 방법에서 메시지가 메시지 정보부의 최상위 비트에 위치하는 경우에 대한 구체적인 실시예를 자세히 설명하는데 이 실시예에 대한 설명은 RLWE 와 AGCD에 기반한 동형 암호화 방법에도 대동소이하게 적용될 수 있다. 그리고 아래에서 제시하는 수학식은 비제한적인 의미로만 해석되어야 하며, 아래에 제시된 수학식과 방식에 본 발명의 권리범위가 제한되는 것으로 해석되어서는 아니된다.

[0023] 클라이언트(10)는 대칭키 암호화에 사용할 비밀키를 생성한다(100). 비밀키 생성은 공지된 방법을 사용할 수 있는데 예를 들어 주어진 시큐리티 파라미터(security parameter) λ에 대해서, 충분히 큰 소수 q, p와, 시큐리티 파라미터 λ를 제공하는 n을 결정한 후에, 아래와 같이 비밀키 s를 생성한다. 시큐리티 파라미터(λ)는 80 내지 128 비트로 설정하는 것이 바람직하다. 그러나 이 비트수에 제한이 있는 것은 아니므로 이 범위는 비제한적인 의미로만 해석되어야 한다.

$$\mathbf{s} \leftarrow \mathbb{Z}_q^n$$

[0024]

[0025] 다음으로 랜덤한 시드값(seed)을 획득한다(110). 랜덤한 시드값을 획득하고 이 시드값을 서버(20)와 공유하는 의사난수생성기(Pseudo Random Number Generator; PRNG)에 아래와 같이 입력하여 랜덤 매트릭스 A(랜덤부)를 생성한다. 의사난수생성기는 작은 시드값으로부터 크기가 큰 난수를 생성하는 함수로서 후술하는 바와 같이 비교적 작은 랜덤 시드값을 동형 암호화에서의 큰(수십만 비트 수준의) 난수값을 대체할 수 있게 한다.

$$\mathrm{A} \leftarrow \mathrm{PRNG}(\mathrm{seed})\ in\ \mathbb{Z}_q^{l \times n}$$

[0026]

[0027] 다음으로 동형 암호화에 사용할 에러값을 다음과 같이 산출한다.

$$\mathrm{e} \leftarrow D^l$$

[0028]

[0029] 단계(130)에서는 앞서 산출한 랜덤 매트릭스(랜덤부) A와 대칭키, 그리고 메시지 및 에러 등을 이용하여 동형 암호화에서 사용하는 메시지 정보부를 다음과 같이 산출한다. 이 메시지 정보부 산출 공식은 종래에 알려진 다른 공식으로 대체되어도 무방하다.

$$\mathrm{b} = \mathrm{As} + \frac{q}{2}m + E(mod\ q)$$

[0030]

[0031] 위에서 산출된 랜덤부(A)와 메시지 정보부(b)를 이용하여 축약 암호문(c)을 다음과 같이 출력한다.

$$\mathrm{c} = (\mathrm{seed}, \mathrm{b}') \quad \mathrm{b}' = \lfloor \mathrm{pb}/\mathrm{q} \rceil$$

[0032] ,

[0033] q/p의 크기를 에러 E의 크기와 일치시키거나 유사하게 설정하는 것이 바람직한데 그 이유는 다음과 같다.

[0034] LWE에 기반한 동형 암호화 방법에 의해 암호화된 암호문을 복호화할 때에는 암호문과 비밀키 s로부터

$\frac{q}{2}m + E(mod\ q)$ 값을 계산하고 여기에서 메시지가 위치한 최상위 비트를 추출하여 메시지 벡터 $\overrightarrow{m}$ 을 복구한다. 그런데 메시지 정보부에서 에러가 위치한 비트들은 삭제하더라도 복호화 과정에 영향이 없다. 따라서 전송하는 암호문 데이터의 용량을 줄이기 위해서 단계(150)에서는 메시지 정보부에서 에러가 위치한 비트를 삭제해서 에러의 비트수만큼 줄어든 벡터(b')를 전송할 수 있다. 그러나 b'이 아니라 b를 이용하여 축약 암호문을 (seed, b)로 구성하더라도 무방하다. 본 명세서에서는 b 뿐만 아니라 b로부터 도출되는 b' 역시 메시지 정보부로 정의된다.

[0035] 단계(160)에서 클라이언트(10)는 축약 암호문을 서버(20)로 전송한다. 서버(20)는 축약 암호문을 수신하고(200), 클라이언트(10)와 공유하는 의사난수생성부(PRNG)를 이용하여 다음과 같이 축약 암호문을 온전한 동형 암호문 형태로 변환한다. b'이 아니라 b를 축약 암호문으로 전송했다면 b를 산출하는 과정은 불필요하다.

[0036] $$Conv(c) = (A, b)\ where\ A = PRNG(seed)\ and\ b = qb'/p$$

[0037] 서버(20)는 이 암호문에 대해서 연산이나 데이터 분석을 수행하고(220) 그 결과값을 클라이언트(10)에 리턴한다(230). 클라이언트(10)는 리턴받은 결과값을 전술한 대칭키로 복호화하여(170) 소정의 결과값을 획득할 수 있다.

[0038] 본 발명에 의하면 대칭키를 이용한 동형 암호화 방법에 의해서 암호화된 데이터는 연산 위임을 받은 서버(20)로 전송되며, 서버(20)는 요청받은 연산을 암호화된 데이터에 대해서 수행한다. 서버(20)가 암호화된 데이터에 연산을 수행하고 산출된 결과는 클라이언트(10)로 전송되며, 클라이언트(10)는 전술한 바와 같은 대칭키로 수신한 결과값을 복호화하여 최종 결과값을 산출한다. 이와 같은 본 발명의 방법에 따르면 오로지 사용자만 암호화 및 복호화에 필요한 대칭키(비밀키)를 보유하기 때문에 사용자가 아닌 제3자가 키를 보유할 수 있는 공개키 방식에 의한 동형 암호화 방법에 비해서 보안성이 증대되는 효과가 있다. 그리고 대칭키 방식에 따른 동형 암호화이기 때문에 암호문의 크기도 공개키 방식에 의한 것보다 훨씬 저감되어 데이터 용량이 줄어드는 효과도 있다.

[0039] AGCD 기반의 동형 암호화 방법에서는 암호문이 다음과 같은 정수 형태로 표시될 수 있다.

[0040] $$x = pq + 2e + m$$

[0041] 여기서 p는 비밀키, q는 랜덤한 정수, e는 작은 에러, m은 메시지이다.

[0042] 본 방식에서는 x를 p로 나눈 나머지가 2e+m 이 되는 랜덤해 보이는 정수를 생성하는 것이 스킴(scheme)의 목적이므로 큰 난수 a를 먼저 생성하고, a+b를 p로 나눈 나머지가 2e+m이 되는 p와 같은 비트수의 정수 b를 선택하여 x = a+b를 도출하는 방법과 통계적으로 차이가 없다.

[0043] 이렇게 되면 AGCD 기반의 동형 암호화 방법에서도 암호문을 랜덤부(a)와 메시지 정보부(b)로 표시할 수 있게 된다. 이 방식에서도 축약 암호문은 랜덤부 a를 생성할 수 있는 시드값(seed)과 메시지 정보부(b 또는 b')로 구성할 수 있게 된다. 다른 과정은 전술한 LWE 방식과 대동소이하다.

[0044] 이상 첨부 도면을 참고하여 본 발명에 대해서 설명하였지만 본 발명의 권리범위는 후술하는 특허청구범위에 의해 결정되며 전술한 실시예 및/또는 도면에 제한되는 것으로 해석되어서는 아니된다. 그리고 특허청구범위에 기재된 발명의, 당업자에게 자명한 개량, 변경 및 수정도 본 발명의 권리범위에 포함된다는 점이 명백하게 이해되어야 한다.

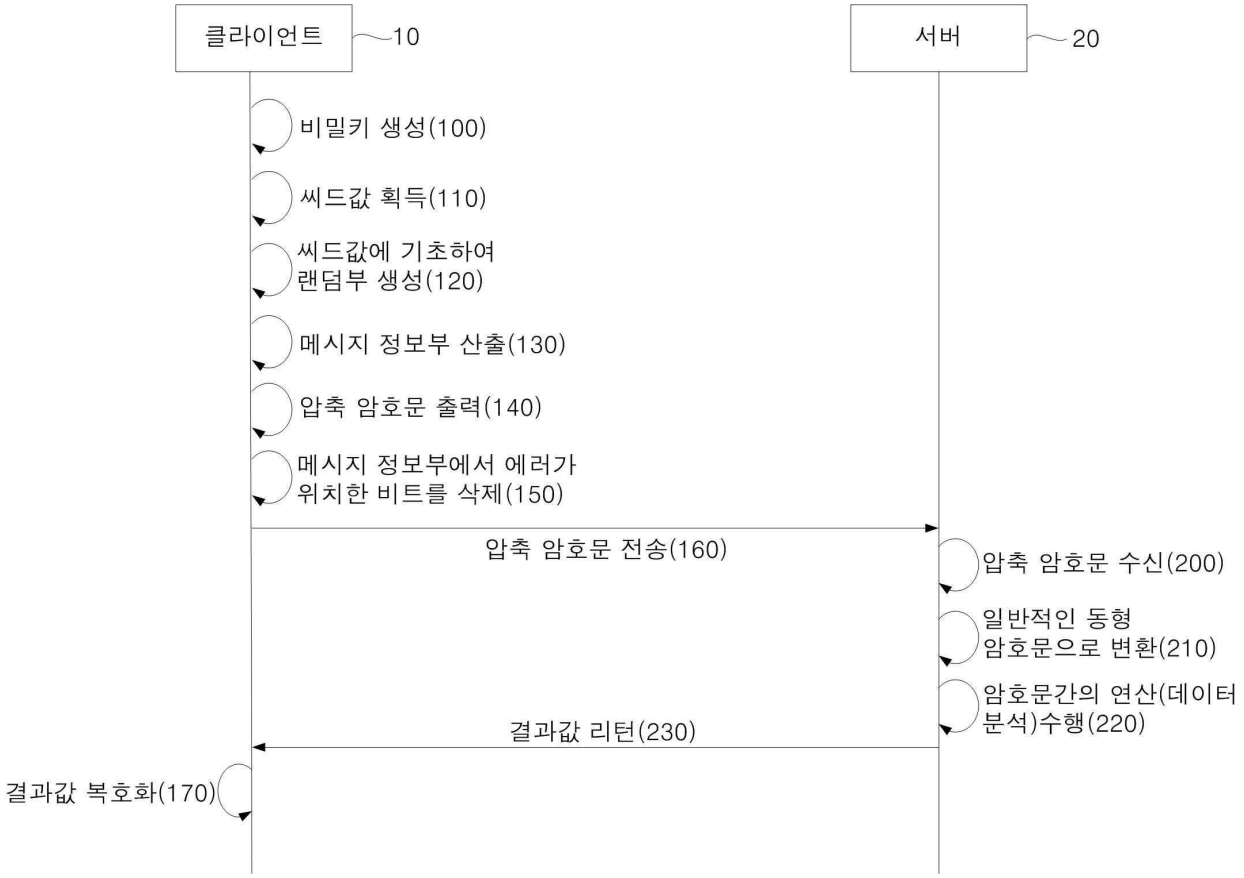
부호의 설명

[0046] 10: 클라이언트

20: 서버

도면

도면1


클라이언트
10
서버
20
비밀키 생성(100)
씨드값 획득(110)
씨드값에 기초하여
랜덤부 생성(120)
메시지 정보부 산출(130)
압축 암호문 출력(140)
메시지 정보부에서 에러가
위치한 비트를 삭제(150)
압축 암호문 전송(160)
압축 암호문 수신(200)
일반적인 동형
암호문으로 변환(210)
암호문간의 연산(데이터
분석)수행(220)
결과값 리턴(230)
결과값 복호화(170)