(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0048760
(43) 공개일자 2020년05월08일

(51) 국제특허분류(Int. Cl.)
H04L 9/30 (2006.01) *H04L 9/14* (2006.01)
(52) CPC특허분류
H04L 9/3033 (2013.01)
H04L 9/14 (2013.01)
(21) 출원번호 10-2018-0131205
(22) 출원일자 2018년10월30일
심사청구일자 2018년10월30일

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
허준범
경기도 용인시 기흥구 보정로 30, 119동 201호(보정동, 동아솔레시티아파트)
한창희
인천광역시 남동구 호구포로 924, 109동 2204호 (만수동, 햇빛마을벽산아파트)
(74) 대리인
김홍석

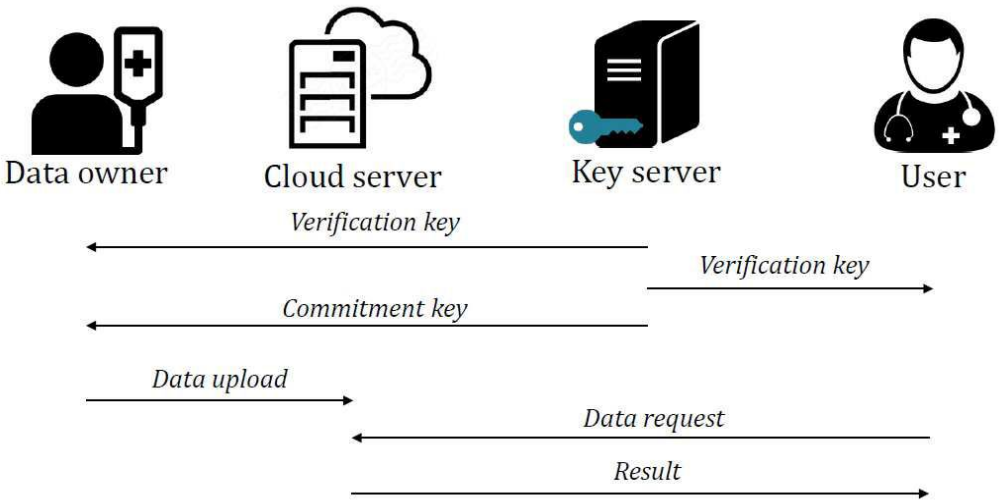
전체 청구항 수 : 총 14 항

(54) 발명의 명칭 **모바일 헬스케어를 위한 가상 물리 시스템에서 안전한 연산 위임 방법**

(57) 요 약

암호 시스템이 개시된다. 상기 암호 시스템은 키 서버, 제1 단말, 제2 단말, 및 클라우드 서버를 포함하고, 상기 키 서버는 제1 마스터키, 제2 마스터키, 제1 공개키, 및 제2 공개키를 생성하고, 비밀키, 변환키, 및 확약키를 생성하고, 상기 확약키를 상기 제1 단말로 송신하고, 상기 비밀키를 상기 제2 단말로 송신하고, 상기 변환키를 상기 클라우드 서버로 송신하고, 상기 제1 단말은 메시지를 암호화하여 암호문을 생성하고, 상기 확약키를 이용하여 확약값을 생성하고, 상기 암호문과 상기 확약값을 상기 클라우드 서버로 송신하고, 상기 클라우드 서버는 상기 암호문을 부분 복호화하여 부분 복호화된 암호문을 생성하고, 상기 부분 복호화된 암호문과 상기 확약값을 상기 제2 단말로 송신하고, 상기 제2 단말은 상기 비밀키를 이용하여 상기 부분 복호화된 암호문을 복호화한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 2209/26 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 2018-0-00269
부처명 과학기술정보통신부
연구관리전문기관 정보통신기술진흥센터
연구사업명 정보통신방송 기술개발사업
연구과제명 개인정보를 안전하고 편리하게 빅데이터 처리할수 있는 방법
기 여 율 1/2
주관기관 고려대학교 산학협력단
연구기간 2018.04.01 ~ 2020.12.31
이 발명을 지원한 국가연구개발사업
과제고유번호 2017-0-00184
부처명 과학기술정보통신부
연구관리전문기관 정보통신기술진흥센터
연구사업명 사이버자가방어기술개발
연구과제명 자기학습형 사이버 면역 기술 개발
기 여 율 1/2
주관기관 한국인터넷진흥원
연구기간 2017.03.01 ~ 2020.12.31

명 세 서

청구범위

청구항 1

키 서버, 제1 단말, 제2 단말, 및 클라우드 서버를 포함하는 암호 시스템에 있어서,

상기 키 서버는 제1 마스터키, 제2 마스터키, 제1 공개키, 및 제2 공개키를 생성하고, 비밀키, 변환키, 및 확약키를 생성하고, 상기 확약키를 상기 제1 단말로 송신하고, 상기 비밀키를 상기 제2 단말로 송신하고, 상기 변환키를 상기 클라우드 서버로 송신하고,

상기 제1 단말은 메시지를 암호화하여 암호문을 생성하고, 상기 확약키를 이용하여 확약값을 생성하고, 상기 암호문과 상기 확약값을 상기 클라우드 서버로 송신하고,

상기 클라우드 서버는 상기 암호문을 부분 복호화하여 부분 복호화된 암호문을 생성하고, 상기 부분 복호화된 암호문과 상기 확약값을 상기 제2 단말로 송신하고,

상기 제2 단말은 상기 비밀키를 이용하여 상기 부분 복호화된 암호문을 복호화하는,

암호 시스템

청구항 2

제1항에 있어서,

상기 키 서버는 ABE(Attribute-based encryption, 속성 기반 암호)의 셋업 알고리즘($ABE.Setup$)을 수행하여 상기 제1 마스터키와 상기 제1 공개키를 생성하고,

상기 키 서버는 보안 상수(λ)를 입력으로 받는 셋업 알고리즘($Setup$)을 수행하여 수학식 1과 수학식 2로 표현되는 상기 제2 마스터키(MK)와 상기 제2 공개키(VK)를 생성하고,

상기 수학식 1은 $MK = \gamma$ ($\gamma \in \mathbb{Z}_p^*$)이고,

상기 수학식 2는 $VK = (g_1, g_2, g_2^{\gamma})$ ($g_1 \in \mathbb{G}_1$, $g_2 \in \mathbb{G}_2$)이고,

상기 $\mathbb{G}_1$과 상기 $\mathbb{G}_2$는 소수 위수(prime order) p의 곱셈 순환군(multiplicative cyclic group)인,

암호 시스템.

청구항 3

제2항에 있어서,

상기 키 서버는 ABE의 키 생성 알고리즘($ABE.KeyGen$)을 수행하여 상기 비밀키와 상기 변환키를 생성하고,

상기 키 서버는 상기 제2 마스터키와 상기 제2 공개키를 입력으로 받는 확약키 생성 알고리즘($KeyGen$)을 수행하여 수학식 3으로 표현되는 상기 확약키(CK)를 생성하고,

상기 수학식 3은 $CK = (A, B)$ ($A = g_1^{\frac{1}{\gamma+x}}$, $B = x$, $x \in \mathbb{Z}_p^*$)인,

암호 시스템.

청구항 4

제3항에 있어서,

상기 제1 단말은 ABE의 암호화 알고리즘($ABE.Enc$)을 수행하여 상기 암호문을 생성하고,

상기 제1 단말은 상기 제2 공개키(VK), 상기 확약키(CK), 및 상기 메시지(M)를 입력으로 받는 확약값 생성 알고리즘을 수행하여 수학식 4로 표현되는 상기 확약값(σ)을 생성하고,

상기 수학식 4는 $\sigma = \left(A^B, g_2^{\gamma} \cdot g_2^B, C\right)$ ($C = H(e(g_1, g_2)^B, M)$)인,

암호 시스템.

청구항 5

제4항에 있어서,

상기 클라우드 서버는 ABE의 부분 복호화 알고리즘($ABE.PDec$)을 수행하여 상기 부분 복호화된 암호문을 생성하는,

암호 시스템.

청구항 6

제5항에 있어서,

상기 제2 단말은 ABE의 복호화 알고리즘($ABE.FDec$)을 수행하여 상기 부분 복호화된 암호문을 복호화하고,

상기 제2 단말은 상기 제2 공개키(VK), 상기 메시지(M), 및 상기 확약값(σ)을 입력으로 하는 검증 알고리즘($Vrfy$)을 수행하여 상기 부분 복호화된 암호문 또는 복호화된 암호문의 정확성을 검증하는,

암호 시스템.

청구항 7

제6항에 있어서,

상기 제2 단말은 수학식 5의 성립 여부에 따라 상기 부분 복호화된 암호문 또는 복호화된 암호문의 정확성을 검증하고,

상기 수학식 5는 $H\left(e(A^B, D), M\right) \stackrel{?}{=} C$ ($D = g_2^{\gamma} \cdot g_2^B$)인,

암호 시스템.

청구항 8

(a) 키 서버는 제1 마스터키, 제2 마스터키, 제1 공개키, 및 제2 공개키를 생성하고, 비밀키, 변환키, 및 확약키를 생성하고, 상기 확약키를 상기 제1 단말로 송신하고, 상기 비밀키를 상기 제2 단말로 송신하고, 상기 변환키를 상기 클라우드 서버로 송신하는 단계;

(b) 제1 단말이 메시지를 암호화하여 암호문을 생성하고, 상기 확약키를 이용하여 확약값을 생성하고, 상기 암호문과 상기 확약값을 클라우드 서버로 송신하는 단계;

(c) 상기 클라우드 서버가 상기 암호문을 부분 복호화하여 부분 복호화된 암호문을 생성하고, 상기 부분 복호화된 암호문과 상기 확약값을 제2 단말로 송신하는 단계; 및

(d) 상기 제2 단말이 상기 비밀키를 이용하여 상기 부분 복호화된 암호문을 복호화하는 단계를 포함하는 연산 위임 방법.

청구항 9

제8항에 있어서,

상기 (a) 단계에서, 상기 키 서버는 ABE(Attribute-based encryption, 속성 기반 암호)의 셋업 알고리즘($ABE.Setup$)을 수행하여 상기 제1 마스터키와 상기 제1 공개키를 생성하고, ABE의 키 생성 알고리즘($ABE.KeyGen$)을 수행하여 상기 비밀키와 상기 변환키를 생성하고,

상기 (b) 단계에서, 상기 제1 단말은 ABE의 암호화 알고리즘($ABE.Enc$)을 수행하여 상기 암호문을 생성하고,

상기 (c) 단계에서, 상기 클라우드 서버는 ABE의 부분 복호화 알고리즘($ABE.PDec$)을 수행하여 상기 부분 복호화된 암호문을 생성하고,

상기 (d) 단계에서, 상기 제2 단말은 ABE의 복호화 알고리즘($ABE.FDec$)을 수행하여 상기 부분 복호화된 암호문을 복호화하는,

연산 위임 방법.

청구항 10

제9항에 있어서,

상기 (a) 단계에서, 상기 키 서버는 보안 상수(λ)를 입력으로 받는 셋업 알고리즘($Setup$)을 수행하여 수학식 1과 수학식 2로 표현되는 상기 제2 마스터키(MK)와 상기 제2 공개키(VK)를 생성하고,

상기 수학식 1은 $MK = \gamma$ ($\gamma \in \mathbb{Z}_p^*$)이고,

상기 수학식 2는 $VK = (g_1, g_2, g_2^{\gamma})$ ($g_1 \in \mathbb{G}_1$, $g_2 \in \mathbb{G}_2$)이고,

상기 $\mathbb{G}_1$과 상기 $\mathbb{G}_2$는 소수 위수(prime order) p의 곱셈 순환군(multiplicative cyclic group)인,

연산 위임 방법.

청구항 11

제10항에 있어서,

상기 (a) 단계에서, 상기 키 서버는 상기 제2 마스터키와 상기 제2 공개키를 입력으로 받는 확약키 생성 알고리즘($KeyGen$)을 수행하여 수학식 3으로 표현되는 상기 확약키(CK)를 생성하고,

상기 수학식 3은 $CK = (A, B)$ ($A = g_1^{\frac{1}{\gamma + x}}$, $B = x$, $x \in \mathbb{Z}_p^*$)인,

연산 위임 방법.

청구항 12

제11항에 있어서,

상기 (b) 단계에서, 상기 제1 단말은 상기 제2 공개키(VK), 상기 확약키(CK), 및 상기 메시지(M)를 입력으로 받는 확약값 생성 알고리즘을 수행하여 수학식 4로 표현되는 상기 확약값(σ)을 생성하고,

상기 수학식 4는 $\sigma = \left(A^B, g_2^{\gamma} \cdot g_2^B, C\right)$ ($C = H(e(g_1, g_2)^B, M)$)인,

연산 위임 방법.

청구항 13

제12항에 있어서,

상기 연산 위임 방법은 상기 제2 단말이 상기 제2 공개키(VK), 상기 메시지(M), 및 상기 확약값(σ)을 입력으로 하는 검증 알고리즘($Vrfy$)을 수행하여 상기 부분 복호화된 암호문 또는 복호화된 암호문의 정확성을 검증하는 단계를 더 포함하는,

연산 위임 방법.

청구항 14

제13항에 있어서,

상기 검증하는 단계에서, 상기 제2 단말은 수학식 5의 성립 여부에 따라 상기 부분 복호화된 암호문 또는 복호화된 암호문의 정확성을 검증하고,

상기 수학식 5는 $H\left(e(A^B, D), M\right) \stackrel{?}{=} C$ ($D = g_2^{\gamma} \cdot g_2^B$)인,

연산 위임 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 안전한 연산 위임 방법에 관한 것으로, 특히 복호 연산의 일부를 클라우드 서버에 위임하는 ABE(attribute-based encryption)에서 부분 복호 또는 복호의 정확성을 검증할 수 있는 안전한 연산 위임 방법에 관한 것이다.

배 경 기 술

[0003] 모바일 헬스케어 시스템(mobile healthcare systems)에서, 의료 기기들(medical devices)은 임상 데이터(clinical data)를 수집하고 진단 정보(diagnostic information)를 보고하기 위하여 환자와 근접하여 위치한다. 이러한 장치들은 반도체가 내장된(semiconductor-embedded) 스마트 인텔리전트 센서들(smart intelligent sensors)일 수 있으며, 스마트 인텔리전트 센서들은 환자의 몸 속에 이식되어 병리적 증상(pathological symptoms)의 실시간 정량(real-time quantification)을 위해 동작할 수 있다. 진단 보고(diagnostic report)를 위하여, 개인 헬스 디바이스들(personal health devices)은 EHR(electronic health record) 형태로 데이터를 처리하는 스토리지 센터(storage centers)로 개인 의료 정보(medical information)를 전송한다. 최근, 다양한 클라우드 서비스 제공자들은 IMB Cloud Solutions for Healthcare, Google Cloud 및 Azure for health와 같은 의료 정보 서비스(medical information services)를 상용화하여 제공하고 있다. 그러나, 잠재적으로 신뢰할 수 없는 클라우드 서버에 민감 정보(sensitive information)를 위임(delegating)하는 것은 환자의 프라이버시와 관련하여 염려를 일으킨다.

[0004] ABE(attribute-based encryption, 속성 기반 암호)는 이러한 문제를 해결할 수 있는 암호 기법이다. 데이터 소유자(예컨대, 환자)는 접근 정책(access plocicy)을 생성하고, 암호화된 메시지(의료 데이터)를 첨부하며, 암호문을 클라우드 서버로 전송한다. 데이터 소유자가 생성한 접근 정책에 부합하는 속성이 할당된 사용자(의료 종사자)는 암호문으로부터 메시지를 복호화할 수 있다. 그러나, ABE는 사용자에게 과도한 복호화 연산을 요구한다.

[0005] Green 등은 사용자를 위하여 암호문뿐만 아니라 부분적으로 복호화할 수 있는 능력을 클라우드에 위임함으로써 이러한 이슈를 해결하고자 하였다(Green, M., Hohenberger, S., and Waters, B. “Outsourcing the decryption of abe ciphertexts”, *In USENIX Security Symposium*, Vol. 2011, No. 3, 2011.). 클라우드가 부분 복호화한 결과를 사용자에게 전송하면, 사용자는 암호문의 나머지 부분을 복호화할 수 있다. 따라서, 상당량의 연산 부담이 사용자로부터 클라우드로 이전될 수 있다. 그러나, 이와 같은 복호화 위임은 클라우드에 의해 수행된 연산의 정확성(correctness of the computation)에 대한 검증이 불가능하다는 문제점이 있다.

선행기술문헌

특허문헌

[0007] (특허문헌 0001) 대한민국 등록특허 제1575681호 (2015.12.02. 등록)

(특허문헌 0002) 대한민국 공개특허 제2014-0062745호 (2014.05.26. 공개)

비특허문헌

[0008] (비특허문헌 0001) Green, M., Hohenberger, S., and Waters, B. “Outsourcing the decryption of abe ciphertexts”, In USENIX Security Symposium, Vol. 2011, No. 3, 2011.

발명의 내용

해결하려는 과제

[0009] 본 발명이 이루고자 하는 기술적인 과제는 ABE 기법에서 부분 복호화 또는 복호화의 연산 정확성을 검증할 수 있는 안전한 연산 위임 방법을 제공하는 것이다.

과제의 해결 수단

[0011] 본 발명의 실시 예에 따른 암호 시스템은 키 서버, 제1 단말, 제2 단말, 및 클라우드 서버를 포함하고, 상기 키 서버는 제1 마스터키, 제2 마스터키, 제1 공개키, 및 제2 공개키를 생성하고, 비밀키, 변환키, 및 확약키를 생

성하고, 상기 확약키를 상기 제1 단말로 송신하고, 상기 비밀키를 상기 제2 단말로 송신하고, 상기 변환키를 상기 클라우드 서버로 송신하고, 상기 제1 단말은 메시지를 암호화하여 암호문을 생성하고, 상기 확약키를 이용하여 확약값을 생성하고, 상기 암호문과 상기 확약값을 상기 클라우드 서버로 송신하고, 상기 클라우드 서버는 상기 암호문을 부분 복호화하여 부분 복호화된 암호문을 생성하고, 상기 부분 복호화된 암호문과 상기 확약값을 상기 제2 단말로 송신하고, 상기 제2 단말은 상기 비밀키를 이용하여 상기 부분 복호화된 암호문을 복호화한다.

[0012] 또한, 본 발명의 일 실시 예에 따른 연산 위임 방법은 (a) 키 서버는 제1 마스터키, 제2 마스터키, 제1 공개키, 및 제2 공개키를 생성하고, 비밀키, 변환키, 및 확약키를 생성하고, 상기 확약키를 상기 제1 단말로 송신하고, 상기 비밀키를 상기 제2 단말로 송신하고, 상기 변환키를 상기 클라우드 서버로 송신하는 단계, (b) 제1 단말이 메시지를 암호화하여 암호문을 생성하고, 상기 확약키를 이용하여 확약값을 생성하고, 상기 암호문과 상기 확약값을 클라우드 서버로 송신하는 단계, (c) 상기 클라우드 서버가 상기 암호문을 부분 복호화하여 부분 복호화된 암호문을 생성하고, 상기 부분 복호화된 암호문과 상기 확약값을 제2 단말로 송신하는 단계; 및 (d) 상기 제2 단말이 상기 비밀키를 이용하여 상기 부분 복호화된 암호문을 복호화하는 단계를 포함한다.

발명의 효과

[0014] 본 발명의 실시 예에 따른 암호 시스템 및 연산 위임 방법에 의할 경우, 신뢰할 수 없는 서버에서 수행한 암호화된 데이터의 부분 복호 결과의 정확성을 검증할 수 있는 효과가 있다.

[0015] 또한, 본 발명에 의할 경우, 디지털 서명(digital signature) 기법과 동일한 수준의 안전성을 제공할 수 있다.

[0016] 또한, 본 발명은 ABE뿐만 아니라, 연산 위임을 지원하는 어떠한 정책 기반 암호(policy-based encryption)에 적용이 가능하다.

도면의 간단한 설명

[0018] 본 발명의 상세한 설명에서 인용되는 도면을 보다 충분히 이해하기 위하여 각 도면의 상세한 설명이 제공된다.

도 1은 본 발명의 일 실시 예에 따른 연산 위임 방법을 설명하기 위한 개략도이다.

도 2는 본 발명의 일 실시 예에 따른 시스템을 도시한다.

도 3은 도 2에 도시된 시스템 상에서 수행되는 연산 위임 방법을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0019] 본 명세서에 개시되어 있는 본 발명의 개념에 따른 실시 예들에 대해서 특정한 구조적 또는 기능적 설명들은 단지 본 발명의 개념에 따른 실시 예들을 설명하기 위한 목적으로 예시된 것으로서, 본 발명의 개념에 따른 실시 예들은 다양한 형태들로 실시될 수 있으며 본 명세서에 설명된 실시 예들에 한정되지 않는다.

[0020] 본 발명의 개념에 따른 실시 예들은 다양한 변경들을 가할 수 있고 여러 가지 형태들을 가질 수 있으므로 실시 예들을 도면에 예시하고 본 명세서에서 상세하게 설명하고자 한다. 그러나, 이는 본 발명의 개념에 따른 실시 예들을 특정한 개시 형태들에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물, 또는 대체물을 포함한다.

[0021] 제1 또는 제2 등의 용어는 다양한 구성 요소들을 설명하는데 사용될 수 있지만, 상기 구성 요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성 요소를 다른 구성 요소로부터 구별하는 목적으로만, 예컨대 본 발명의 개념에 따른 권리 범위로부터 벗어나지 않은 채, 제1 구성 요소는 제2 구성 요소로 명명될 수 있고 유사하게 제2 구성 요소는 제1 구성 요소로도 명명될 수 있다.

[0022] 어떤 구성 요소가 다른 구성 요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성 요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성 요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성 요소가 다른 구성 요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는 중간에 다른 구성 요소가 존재하지 않는 것으로 이해되어야 할 것이다. 구성 요소들 간의 관계를 설명하는 다른 표현들, 즉 "~사이에"와 "바로 ~사이에" 또는 "~에 이웃하는"과 "~에 직접 이웃하는" 등

도 마찬가지로 해석되어야 한다.

[0023] 본 명세서에서 사용한 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로서, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 명세서에서, "포함하다" 또는 "가지다" 등의 용어는 본 명세서에 기재된 특징, 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0024] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 갖는 것으로 해석되어야 하며, 본 명세서에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0025] 이하, 본 명세서에 첨부된 도면들을 참조하여 본 발명의 실시 예들을 상세히 설명한다. 그러나, 특허출원의 범위가 이러한 실시 예들에 의해 제한되거나 한정되는 것은 아니다. 각 도면에 제시된 동일한 참조 부호는 동일한 부재를 나타낸다.

[0027] 우선, 본 발명에서 이용하는 ABE(Attribute-based encryption, 속성 기반 암호)는 아래와 같이 5 개의 알고리즘으로 구성되어 있다.

[0028] - $\mathbf{Setup}(\lambda, U)$. 셋업 알고리즘은 보안 상수(security parameter) λ와 속성 집합(attribute universe description) U를 입력으로 받고, 공개 상수(public parameters) PK와 마스터키(master key) MK를 출력한다.

[0029] - $\mathbf{Encrypt}(\mathrm{PK}, M, I_{enc})$. 암호화 알고리즘은 공개 상수 PK, 메시지 M, 및 액세스 스트럭처(access structure, ABE의 방식에 따라 속성 집합(attribute set)이 될 수도 있음) I_{enc}을 입력으로 받고, 암호문 CT를 출력한다.

[0030] - $\mathbf{KeyGen}_{out}(\mathrm{MK}, I_{key})$. 키 생성 알고리즘은 마스터키 MK, 속성 집합(ABE의 방식에 따라 액세스 스트럭처가 될 수도 있음) I_{key}을 입력으로 받고, 비밀키(private key) SK와 변환키(transformation key) TK를 출력한다.

[0031] - $\mathbf{Transform}(\mathrm{TK}, \mathrm{CT})$. 암호문 변환 알고리즘(부분 복호화 알고리즘이라고 명명될 수도 있음)은 변환키 TK와 암호문 CT를 입력으로 받고, 부분적으로 복호화된 암호문(또는 부분 복호화된 암호문) CT'를 출력한다.

[0032] - $\mathbf{Decrypt}_{out}(\mathrm{SK}, \mathrm{CT}')$. 복호화 알고리즘은 비밀키 SK와 부분 복호화된 암호문 CT'을 입력으로 받고, 메시지 M을 출력한다.

[0033] 본 발명은 ABE 자체에 관한 발명이 아니므로, ABE에 관한 상세한 설명은 생략하기로 한다. ABE의 보다 구체적인 내용에 관하여는 Green 등의 논문(Green, M., Hohenberger, S., and Waters, B. “Outsourcing the decryption of abe ciphertexts”, *In USENIX Security Symposium*, Vol. 2011, No. 3, 2011.)이 참조될 수 있다. 또한, 상술한 ABE는 다양한 변형 예들이 존재할 수 있고, 본 발명의 권리범위가 이러한 변형 예들에 의해 제한되지 않음을 인지하여야 한다.

[0035] 도 1은 본 발명의 일 실시 예에 따른 연산 위임 방법을 설명하기 위한 개략도이다.

[0036] 우선, 키 서버(Key server)는 검증키(verification key, 실시 예에 따라 공개키(public key)로 명명될 수도 있

음)를 데이터 소유자(data owner, 상기 데이터 소유자의 단말기를 의미할 수 있음)와 사용자(user, 상기 사용자의 단말기를 의미할 수 있음)에게 발급한다. 또한, 상기 데이터 소유자는 상기 키 서버로부터 확약키(commitment key)를 할당받는다. 상기 데이터 소유자에게 업로드할 데이터가 있는 경우, 상기 데이터 소유자는 상기 확약키를 이용하여 확약값(comitment value)을 생성함으로써 데이터를 확약할 수 있다. 평문 데이터(plaintext data)를 암호화한 후, 상기 데이터 소유자는 상기 확약값과 암호문(ciphertext)을 클라우드 서버(cloud server)로 전송한다. 상기 사용자가 특정 데이터에 대한 액세스를 요청하는 경우, 상기 클라우드 서버는 부분 복호화를 수행하고, 수행 결과를 상기 사용자에게 전송한다. 상기 사용자는 평문 데이터를 복구하고 정확성을 검증할 수 있다.

[0038] 이하에서는 본 발명에서 사용되는 알고리즘에 대해 설명한다. 본 발명에 의한 연산 위임 방법은 아래와 같이 4개의 알고리즘으로 구성되어 있다.

[0039] 1) $(VK, MK) \leftarrow Setup(\lambda)$ **by key server.** 셋업 알고리즘(setup algorithm, 또는 셋업 단계)은 보안 파라미터(security parameter) λ를 입력으로 받고, 공개 검증키(public verification key) VK와 마스터 비밀키(master secret key) MK를 출력한다.

[0040] 2) $CK \leftarrow KeyGen(VK, MK)$ **by key server.** 확약키 생성 알고리즘(commitment key generation algorithm, 또는 확약키 생성 단계)은 공개 검증키 VK와 마스터 비밀키 MK를 입력으로 받고, 비밀 확약키(secret commitment key) CK를 출력한다.

[0041] 3) $\sigma \leftarrow Commit(VK, CK, M)$ **by data owner.** 확약(값) 생성 알고리즘(commitment generation algorithm, 또는 확약 생성 단계)은 공개 검증키 VK, 비밀 확약키 CK, 및 메시지 M을 입력으로 받고, 확약(commitment) σ을 출력한다.

[0042] 4) $y \leftarrow Vrfy(VK, M, \sigma)$ **by user.** 검증 알고리즘(verification algorithm, 또는 검증 단계)은 공개 검증키 VK, 메시지 M, 및 확약 σ를 입력으로 받고, 검증 결과 $y \in \{0,1\}$를 출력한다. 여기서, 0과 1은 각각 검증 실패(또는 검증 성공)와 검증 성공(또는 검증 실패)을 의미할 수 있다.

[0044] 본 발명에서 사용되는 알고리즘에 대한 구체적인 설명은 다음과 같다.

[0045] $H : \{0,1\}^* \rightarrow \mathbb{Z}_p$가 암호학적 해쉬 함수(cryptographic hash function)이고, $\mathbb{G}_1$, $\mathbb{G}_2$, 및 $\mathbb{G}_T$가 소수 위수(prime order) p의 곱셈 순환군(multiplicative cyclic groups)이고, $\mathbb{Z}_p^*$가 곱셈 모듈로(multiplication modulo) p의 군이고, $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$가 겹선형 함수(bilinear map)일 때, 본 발명에서 제안하는 기법은 아래와 같다.

[0046] 1) $(VK, MK) \leftarrow Setup(\lambda)$. 셋업 알고리즘(설정 알고리즘 또는 설정 단계)은 보안 상수(security parameter) λ를 입력으로 받는다. 또한, 셋업 알고리즘은 생성원 $g_1 \in \mathbb{G}_1$, $g_2 \in \mathbb{G}_2$와 임의의 값(random value) $\gamma \in \mathbb{Z}_p^*$를 선택한다. 셋업 알고리즘은 다음과 같은 검증키(VK)와 마스터 비밀키(MK)를 출력한다.

[0047] $$VK = (g_1, g_2, g_2^{\gamma}),\ MK = \gamma$$

[0048] 2) $CK \leftarrow KeyGen(VK, MK)$. 확약키 생성 알고리즘(확약키 생성 단계)은 검증키 VK와 마스터 비

밀키 MK를 입력으로 받는다. 또한, 확약키 생성 알고리즘은 임의의 값 $x \in \mathbb{Z}_p^*$를 선택하고, $A = g_1^{\frac{1}{\gamma+x}}$를 계산하고, $B = x$를 설정한다. 확약키 생성 알고리즘은 다음과 같은 확약키(CK)를 출력한다.

[0049] $$CK = (A, B)$$

[0050] 3) $\sigma \leftarrow Commit(VK, CK, M)$. 확약 생성 알고리즘(확약 생성 단계)은 검증키 VK, 확약키 CK, 및 메시지 M을 입력으로 받는다. 확약 생성 알고리즘은 $C = H(e(g_1, g_2)^B, M)$를 계산하고, 다음과 같은 확약(또는 확약값)을 생성한다.

[0051] $$\sigma = \left(A^B, g_2^{\gamma} \cdot g_2^B, C\right)$$

[0052] 4) $y \leftarrow Vrfy(VK, M, \sigma)$. 검증 알고리즘(검증 단계)은 검증키 VK, 메시지 M, 및 확약키 σ를 입력으로 받고, $D = g_2^{\gamma} \cdot g_2^B$를 설정(또는 연산)한다. 검증 알고리즘은 아래 수학식의 성립 여부에 따라 검증을 수행한다.

[0053] $$H\left(e(A^B, D), M\right) \stackrel{?}{=} C$$

[0054] 상기 수학식이 성립하는 경우, 검증 알고리즘은 $y = 1$을 출력하고, 이는 σ가 메시지 M에 대한 유효한 확약임을 의미한다. 그렇지 않은 경우, 알고리즘은 $y = 0$을 출력한다.

[0056] 상술한 검증의 정확성은 다음과 같이 증명될 수 있다. $\sigma = (A, B, C)$가 메시지 M에 대한 유효한 확약임을 가정하면 검증 알고리즘은 아래 수학식을 연산한다.

[0057]
$$\begin{aligned} H\left(e(A^B, D), M\right) &= H\left(e(g_1^{\frac{B}{\gamma+x}}, g_2^{\gamma} \cdot g_2^B), M\right) \\ &= H\left(e(g_1, g_2)^{\frac{B}{\gamma+x} \cdot (\gamma+B)}, M\right) \\ &= H\left(e(g_1, g_2)^B, M\right) \\ &= C. \end{aligned}$$

[0059] 상술한 기법은 어떠한 ABE(attribute-based encryption) 기법에도 적용이 가능하다. $ABE.Setup$(설정 알고리즘), $ABE.KeyGen$(키 생성 알고리즘), $ABE.Enc$(암호화 알고리즘), $ABE.PDec$(부분 복호화 알고리즘, 실시 예에 따라 암호문 변환 알고리즘이라 명명될 수도 있음), 및 $ABE.FDec$(최종 복호화 알고리즘, 실시 예에 따라 복호화 알고리즘이라 명명될 수도 있음) 각각이 공개 상수들(public parameters)을 설정하고, 비밀키(secret key)를 생성하고, 데이터를 암호화하고, 부분 복호화를 수행하고, 최종 복호화를 수행하는 ABE 알고리즘이라고 가정하자. 상술한 기법을 이용하여 아래와 같이 6 단계를 포함하는 검증 가능한 위탁 복호화 기법의 설계가 가능하다.

[0060] · System setup(시스템 설정 단계). 키 서버는 마스터 비밀키(master secret key)와 공개키들(public keys)을 생성하기 위하여 ABE의 셋업 알고리즘($ABE.Setup$)과 셋업 알고리즘($Setup$)을 수행한다. 상기 키 서버는 상기 마스터 비밀키를 안전하게 저장하고, 상기 공개키들을 공개한다.

[0061] ·Key issuance(키 발급 단계). 상기 키 서버는 ABE의 키 생성 알고리즘($ABE.KeyGen$)을 수행하여 비밀 복호화키(secret decryption key)를 생성하고 이를 허가된 사용자에게 발급한다. 또한, 상기 키 서버는 키 생성 알고리즘($KeyGen$)을 수행하고 허가된 데이터 소유자에게 확약키(commitment key)를 발급한다.

[0062] ·Data upload(데이터 업로드 단계). 상기 데이터 소유자는 메시지를 암호화하기 위하여 ABE의 암호화 알고리즘($ABE.Enc$)을 수행한다. 또한, 상기 데이터 소유자는 확약값(commitment value)을 생성하기 위하여 확약 알고리즘($Commit$)을 수행한다. 암호문과 확약값은 클라우드 서버(cloud server)에 업로드된다.

[0063] ·Partial decryption(부분 복호화 단계). 상기 클라우드 서버는 부분 복호화를 수행하기 위하여 ABE의 부분 복호화 알고리즘($ABE.PDec$)을 실행하고, 결과물은 사용자에게 전달된다.

[0064] ·Final decryption(최종 복호화 단계). 상기 사용자는 최종 복호화를 수행하기 위하여 ABE의 최종 복호화 알고리즘($ABE.FDec$)을 실행한다.

[0065] ·Verification(검증 단계). 상기 사용자는 최종 복호화 알고리즘($ABE.FDec$) 결과의 정확성을 검증하기 위하여 검증 알고리즘($Vrfy$)을 수행한다.

[0067] 도 2는 본 발명의 일 실시 예에 따른 시스템을 도시한다. 도 2에 도시된 시스템은 암호 시스템, 연산 위임 시스템, 데이터 제공 시스템, 클라우드 시스템 등과 같은 다양한 명칭으로 명명될 수도 있다.

[0068] 도 2를 참조하면, 시스템(10)은 키 서버(100), 제1 단말(300), 제2 단말(500), 및 클라우드 서버(700)를 포함한다.

[0069] 키 서버(100)는 시스템 설정 단계와 키 발급 단계를 수행한다.

[0070] 구체적으로, 키 서버(100)는 ABE의 셋업 알고리즘($ABE.Setup$)을 수행하여 제1 마스터키(또는 제1 마스터 비밀키)와 제1 공개키(또는 제1 공개 파라미터)를 생성하고, 셋업 알고리즘($Setup$)을 수행하여 제2 마스터키(또는 제2 마스터 비밀키)와 제2 공개키(또는 제2 공개 파라미터)를 생성할 수 있다. 상기 제2 공개키는 검증키를 의미할 수도 있다. 키 서버(100)는 상기 제1 마스터키와 상기 제2 마스터키를 안전하게 저장하고, 상기 제1 공개키와 상기 제2 공개키를 공개할 수 있다.

[0071] 또한, 키 서버(100)는 ABE의 키 생성 알고리즘($ABE.KeyGen$)을 수행하여 비밀키(또는 복호화키)와 변환키(또는 부분 복호화키)를 생성하고, 키 생성 알고리즘($KeyGen$)을 수행하여 확약키를 생성할 수 있다. 생성된 키들은 허가된 사용자(또는 단말)에게 발급될 수 있다. 즉, 상기 확약키는 제1 단말(300)로 송신되고, 상기 비밀키는 제2 단말(500)로 송신되고, 상기 변환키는 클라우드 서버(700)로 송신될 수 있다.

[0073] 데이터 소유자의 단말인 제1 단말(300)은 데이터 업로드 단계를 수행할 수 있다. 구체적으로, 제1 단말(300)은 ABE의 암호화 알고리즘($ABE.Enc$)을 수행하여 메시지를 암호화하여 암호문을 생성하고, 확약 알고리즘($Commit$)을 수행하여 확약값을 생성할 수 있다. 상기 암호문과 상기 확약값은 클라우드 서버(700)로 송신된다.

[0075] 클라우드 서버(700)는 제2 단말(500)의 요청에 응답하여 부분 복호화 단계(또는 암호문 변환 단계)를 수행한다. 즉, 클라우드 서버(700)는 ABE의 부분 복호화 알고리즘($ABE.PDec$, 또는 암호문 변환 알고리즘)을 수행하여 부분 복호화된 암호문을 생성하고, 상기 부분 복호화된 암호문을 제1 단말(300)로부터 수신한 확약값과 함께 제2 단말(500)로 송신한다.

[0077] 데이터 사용자의 단말인 제2 단말(500)은 최종 복호화 단계(또는 복호화 단계)와 검증 단계를 수행할 수 있다.

[0078] 구체적으로, 제2 단말(500)은 ABE의 최종 복호화 알고리즘($ABE.FDec$)을 수행하여 메시지를 생성할 수 있다. 또한, 제2 단말은 검증 알고리즘($Vrfy$)을 수행하여 최종 복호화 복호화 알고리즘(또는 부분 복호화 알고리즘) 결과의 정확성을 검증할 수 있다.

[0080] 도 3은 도 2에 도시된 시스템 상에서 수행되는 연산 위임 방법을 설명하기 위한 흐름도이다. 도 3에 도시된 방법은 암호화 방법, 데이터 제공 방법 등과 같은 다양한 명칭으로 명명될 수도 있다. 연산 위임 방법을 설명함에 있어 앞선 기재와 중복되는 내용에 관하여는 그 기재를 생략하기로 한다.

[0081] 도 3을 참조하면, 키 서버(100)는 시스템 설정 단계를 수행하여, 제1 및 제2 마스터키와 제1 및 제2 공개키를 생성한다(S100). 상기 제1 마스터키와 상기 제2 마스터키는 키 서버(100)에 의해 안전하게 저장되고, 상기 제1 공개키와 상기 제2 공개키를 공개할 수 있다.

[0082] S200 단계에서, 키 서버(100)는 비밀키, 변환키, 및 확약키를 생성할 수 있다. 생성된 키들은 허가된 사용자(또는 단말)에게 발급될 수 있다. 즉, 상기 확약키는 제1 단말(300)로 송신되고, 상기 비밀키는 제2 단말(500)로 송신되고, 상기 변환키는 클라우드 서버(700)로 송신될 수 있다.

[0083] S300 단계에서, 제1 단말(300)은 암호문과 확약값을 생성할 수 있다. 상기 암호문과 상기 확약값은 클라우드 서버(700)로 송신될 수 있다.

[0084] S400 단계에서, 클라우드 서버(700)는 제2 단말(500)의 요청(데이터 송신 요청)에 응답하여 부분 복호화된 암호문을 생성하고, 상기 부분 복호화된 암호문을 제1 단말(300)로부터 수신한 확약값과 함께 제2 단말(500)로 송신한다.

[0085] S500 단계에서, 제2 단말은 복호화 알고리즘을 수행하여 메시지를 생성(추출)할 수 있다. 또한, 제2 단말은 검증 알고리즘을 수행하여 복호화 알고리즘 또는 부분 복호화 알고리즘 결과의 정확성을 검증할 수 있다.

[0087] 이상에서 설명된 장치들은 하드웨어 구성 요소, 소프트웨어 구성 요소, 및/또는 하드웨어 구성 요소 및 소프트웨어 구성 요소의 집합으로 구현될 수 있다. 예를 들어, 실시 예들에서 설명된 장치 및 구성 요소는, 예를 들어, 프로세서, 콘트롤러, ALU(Arithmetic Logic Unit), 디지털 신호 프로세서(Digital Signal Processor), 마이크로컴퓨터, FPA(Field Programmable array), PLU(Programmable Logic Unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(Operation System, OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술 분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(Processing Element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(Parallel Processor)와 같은, 다른 처리 구성(Processing Configuration)도 가능하다.

[0088] 소프트웨어는 컴퓨터 프로그램(Computer Program), 코드(Code), 명령(Instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(Collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성 요소(Component), 물리적 장치, 가상 장치(Virtual Equipment), 컴퓨터 저장 매체 또는 장치, 또는 전송되는 신호 파(Signal Wave)에 영구적으로, 또는 일시적으로 구체화(Embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

[0089] 실시 예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판

독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 좋ㅂ하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시 예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(Magnetic Media), CD-ROM, DVD와 같은 광기록 매체(Optical Media), 플롭티컬 디스크(Floptical Disk)와 같은 자기-광 매체(Magneto-optical Media), 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 실시 예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0091] 본 발명은 도면에 도시된 실시 예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시 예가 가능하다는 점을 이해할 것이다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성 요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

부호의 설명

[0093] 10 : 시스템

100 : 키 서버

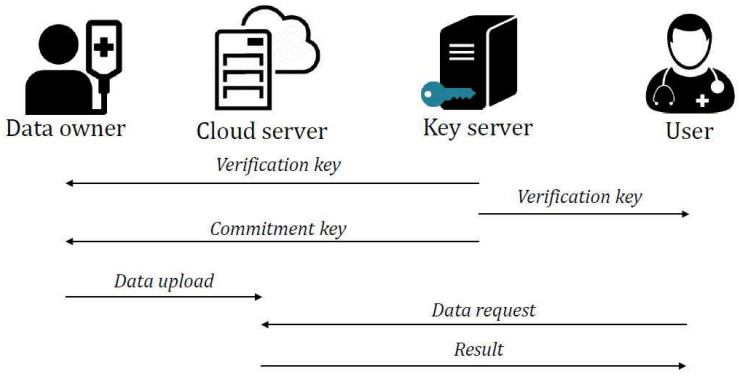
300 : 제1 단말

500 : 제2 단말

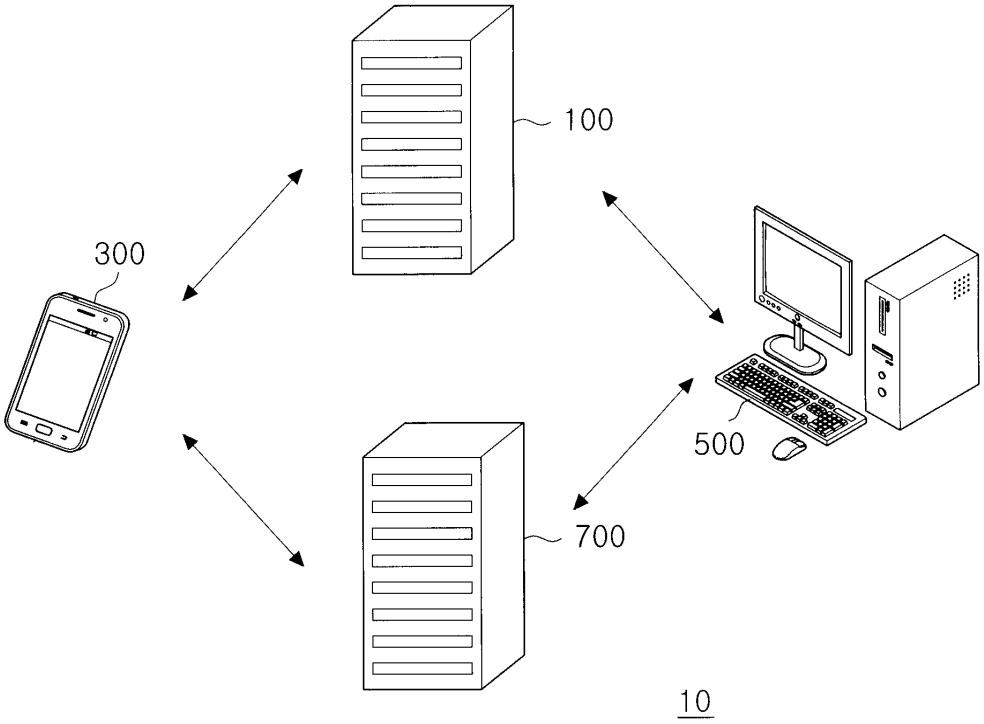
700 : 클라우드 서버

도면

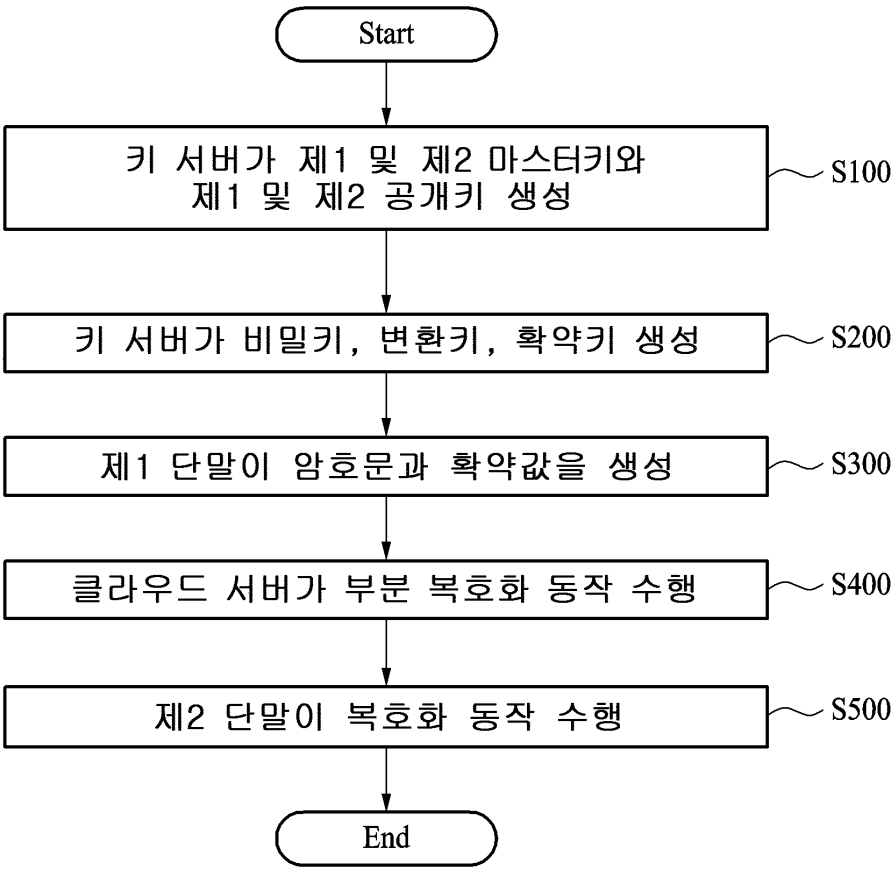
도면1



도면2


100
300
500
700
10

도면3


Start
키 서버가 제1 및 제2 마스터키와 제1 및 제2 공개키 생성
S100
키 서버가 비밀키, 변환키, 확약키 생성
S200
제1 단말이 암호문과 확약값을 생성
S300
클라우드 서버가 부분 복호화 동작 수행
S400
제2 단말이 복호화 동작 수행
S500
End