(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년06월24일
(11) 등록번호 10-2126295
(24) 등록일자 2020년06월18일

(51) 국제특허분류(Int. Cl.)
G06F 21/60 (2013.01) *H04L 9/08* (2006.01)
(52) CPC특허분류
G06F 21/602 (2013.01)
H04L 9/0861 (2013.01)
(21) 출원번호 10-2018-0058145
(22) 출원일자 2018년05월23일
심사청구일자 2018년05월23일
(65) 공개번호 10-2019-0133350
(43) 공개일자 2019년12월03일
(56) 선행기술조사문헌
US20140133651 A1*
WO2014132552 A1
WO2015052957 A1
WO2012157279 A1
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
(72) 발명자
이광수
서울특별시 성북구 길음로 119, 221동 9층 902호 (길음동, 길음뉴타운)
(74) 대리인
두호특허법인

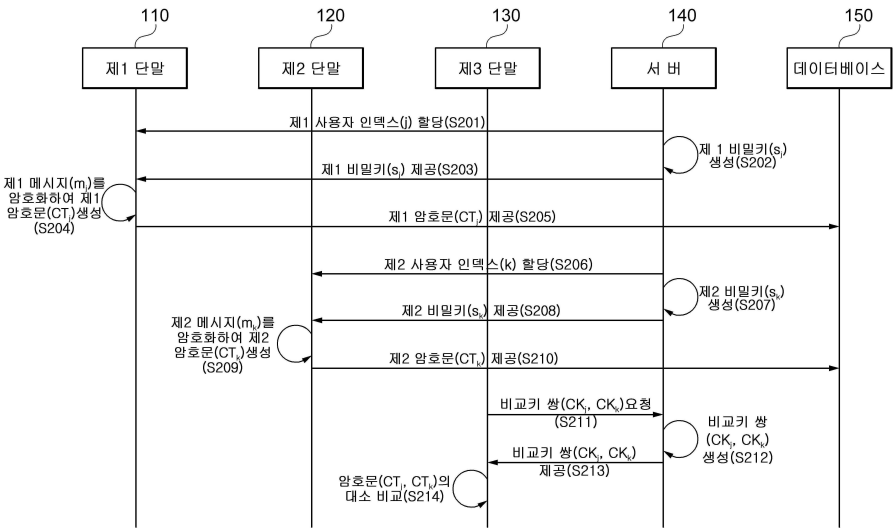
전체 청구항 수 : 총 9 항 심사관 : 구대성

(54) 발명의 명칭 **암호문 비교 방법 및 이를 수행하기 위한 장치**

(57) 요 약

암호문 비교 방법 및 이를 수행하기 위한 장치가 개시된다. 본 발명의 일 실시예에 따른 암호문 비교 방법은, 제1 메시지를 제1 비밀키로 암호화하여 생성된 제1 암호문 및 제2 메시지를 제2 비밀키로 암호화하여 생성된 제2 암호문을 획득하는 단계; 상기 제1 비밀키 및 상기 제2 비밀키를 기초로 생성된 비교키 쌍을 획득하는 단계; 및 상기 제1 암호문, 상기 제2 암호문 및 상기 비교키 쌍을 이용하여 상기 제1 메시지와 상기 제2 메시지의 크기를 비교하는 단계를 포함한다.

대 표 도



(52) CPC특허분류
H04L 9/088 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711058854
부처명 과학기술정보통신부
연구관리전문기관 정보통신기술진흥센터
연구사업명 정보보호핵심원천기술개발
연구과제명 (함수암호 1세부) 함수암호 기법 설계·분석 및 구현기술 연구
기 여 율 1/1
주관기관 상명대학교산학협력단
연구기간 2017.08.01 ~ 2018.05.31

명 세 서

청구범위

청구항 1

하나 이상의 프로세서들, 및

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

제1 메시지(m_j)를 제1 비밀키(s_j)로 암호화하여 생성된 제1 암호문(CT_j) 및 제2 메시지(m_k)를 제2 비밀키(s_k)로 암호화하여 생성된 제2 암호문(CT_k)을 획득하는 단계;

상기 제1 비밀키(s_j) 및 상기 제2 비밀키(s_k)를 기초로 생성된 비교키 쌍(CK_j, CK_k)을 획득하는 단계; 및

상기 제1 암호문(CT_j), 상기 제2 암호문(CT_k) 및 상기 비교키 쌍(CK_j, CK_k)을 이용하여 상기 제1 메시지(m_j)와 상기 제2 메시지(m_k)의 크기를 비교하는 단계를 포함하고,

상기 비교키 쌍(CK_j, CK_k)은, 제1 비교키(CK_j) 및 제2 비교키(CK_k)를 포함하며, 상기 제1 비교키(CK_j) 및 상기 제2 비교키(CK_k)는, 다음의 수학식

$$CK_j = \hat{g}^{r \times s_j}$$

$$CK_k = \hat{g}^{r \times s_k}$$

(이때, g는 위수가 p인 겹선형 군(bilinear group) G의 생성원($g \in G$), $\hat{g}$는 위수가 p인 겹선형 군(bilinear group) $\hat{G}$의 생성원($\hat{g} \in \hat{G}$), e는 위수가 p인 겹선형 군 G, $\hat{G}$, G_T에 대하여 $G \times \hat{G} \rightarrow G_T$의 관계를 만족하는 겹선형 함수, r은 난수)

에 의하여 계산되는, 암호문 비교 방법.

청구항 2

청구항 1에 있어서,

상기 제1 암호문(CT_j) 및 상기 제2 암호문(CT_k)은, 다음의 수학식

$$CT = (\{C_{i,0}, C_{i,1}\})_{i \in [n]}$$

$$C_{i,0} = H(prefix(m, i-1) \| 0x_i)^s$$

$$C_{i,1} = H(prefix(m, i-1) \| 0x_i + 1)^s$$

(이때, m은 $m = x_1x_2 \cdots x_n \in \{0,1\}^n$의 관계를 가지는 메시지, CT는 m에 대응되는 암호문, $prefix(m, i-1) = x_1x_2 \cdots x_{i-1}$, s는 비밀키, H는 해시함수)

에 의하여 생성되는, 암호문 비교 방법

청구항 3

삭제

청구항 4

청구항 2에 있어서,

상기 제1 메시지(m_j)와 상기 제2 메시지(m_k)의 크기를 비교하는 단계는,

$e(C_{i,0}, CK_k)$와 $e(C'_{i,0}, CK_j)$가 일치하지 않는 i의 최소값(i^*)을 계산하는 단계;

$e(C_{i*,1}, CK_k)$와 $e(C'_{i*,0}, CK_j)$가 일치하는지 여부를 판단하는 단계; 및

상기 판단 결과 일치하는 경우, 상기 제1 메시지(m_j)의 크기가 상기 제2 메시지(m_k)의 크기보다 더 작다고 판단하는 단계를 포함하는, 암호문 비교 방법.

청구항 5

청구항 4에 있어서,

상기 판단 결과 일치하지 않는 경우, 상기 제1 메시지(m_j)의 크기가 상기 제2 메시지(m_k)의 크기보다 더 크다고 판단하는 단계를 더 포함하는, 암호문 비교 방법.

청구항 6

청구항 1, 청구항 2, 청구항 4 및 청구항 5 중 어느 한 항에 기재된 암호문 비교 방법을 컴퓨터상에서 수행하기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 7

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,

제1 메시지(m_j)를 제1 비밀키(s_j)로 암호화하여 생성된 제1 암호문(CT_j) 및 제2 메시지(m_k)를 제2 비밀키(s_k)로 암호화하여 생성된 제2 암호문(CT_k)을 획득하는 단계;

상기 제1 비밀키(s_j) 및 상기 제2 비밀키(s_k)를 기초로 생성된 비교키 쌍(CK_j, CK_k)을 획득하는 단계; 및

상기 제1 암호문(CT_j), 상기 제2 암호문(CT_k) 및 상기 비교키 쌍(CK_j, CK_k)을 이용하여 상기 제1 메시지(m_j)와 상기 제2 메시지(m_k)의 크기를 비교하는 단계를 실행하기 위한 명령어들을 포함하고,

상기 비교키 쌍(CK_j, CK_k)은 제1 비교키(CK_j) 및 제2 비교키(CK_k)를 포함하며, 상기 제1 비교키(CK_j) 및 상기 제2 비교키(CK_k)는, 다음의 수학식

$$CK_j = \hat{g}^{r \times s_j}$$

$$CK_k = \hat{g}^{r \times s_k}$$

(이때, g는 위수가 p인 겹선형 군(bilinear group) G의 생성원($g \in G$), $\hat{g}$는 위수가 p인 겹선형 군(bilinear group) $\hat{G}$의 생성원($\hat{g} \in \hat{G}$), e는 위수가 p인 겹선형 군 G, $\hat{G}$, G_T에 대하여 $G \times \hat{G} \rightarrow G_T$의 관계를 만족하는 겹선형 함수, r은 난수)

에 의하여 계산되는, 암호문 비교 장치.

청구항 8

청구항 7에 있어서,

상기 제1 암호문(CT_j) 및 상기 제2 암호문(CT_k)은, 다음의 수학식

$$CT = (\{C_{i,0}, C_{i,1}\})_{i \in [n]}$$

$$C_{i,0} = H(prefix(m, i-1) \| 0x_i)^s$$

$$C_{i,1} = H(prefix(m, i-1) \| 0x_i + 1)^s$$

(이때, m은 $m = x_1x_2 \cdots x_n \in \{0,1\}^n$의 관계를 가지는 메시지, CT는 m에 대응되는 암호문, $prefix(m, i-1) = x_1x_2 \cdots x_{i-1}$, s는 비밀키, H는 해시함수)

에 의하여 생성되는, 암호문 비교 장치

청구항 9

삭제

청구항 10

청구항 8에 있어서,

상기 제1 메시지(m_j)와 상기 제2 메시지(m_k)의 크기를 비교하는 단계는,

$e(C_{i,0}, CK_k)$와 $e(C'_{i,0}, CK_j)$가 일치하지 않는 i의 최소값(i^*)을 계산하는 단계;

$e(C_{i^*,1}, CK_k)$와 $e(C'_{i^*,0}, CK_j)$가 일치하는지 여부를 판단하는 단계; 및

상기 판단 결과 일치하는 경우, 상기 제1 메시지(m_j)의 크기가 상기 제2 메시지(m_k)의 크기보다 더 작다고 판단하는 단계를 실행하기 위한 명령어들을 더 포함하는, 암호문 비교 장치.

청구항 11

청구항 10에 있어서,

상기 판단 결과 일치하지 않는 경우, 상기 제1 메시지(m_j)의 크기가 상기 제2 메시지(m_k)의 크기보다 더 크다고 판단하는 단계를 실행하기 위한 명령어들을 더 포함하는, 암호문 비교 장치.

발명의 설명

기 술 분 야

[0001] 본 발명의 실시예들은 네트워크 상에서의 보안 기술과 관련된다.

배 경 기 술

[0003] 순서 노출 암호(Order-Revealing Encryption; ORE)란 암호화된 상태에서 암호화되기 전 평문의 대소 비교를 가능하게 하는 암호 기술이다. 기존의 ORE 기법은 모두 하나의 키로 암호화된 즉, 한 사용자의 데이터 간의 비교만을 지원하였다. 그러나, 경우에 따라 다수의 사용자로부터 생성된 즉, 서로 다른 비밀키로 암호화된 암호문 간의 비교가 필요한 상황이 있을 수 있다. 이에 따라 서로 다른 비밀키로 암호화된 암호문 간의 대소 비교를 수행하기 위한 방법이 필요하게 되었다.

발명의 내용

해결하려는 과제

[0005] 본 발명의 실시예들은 복호화 과정 없이 서로 다른 비밀키로 암호화된 암호문 간의 비교를 가능하게 하기 위한 암호문 비교 방법을 제공하기 위한 것이다.

과제의 해결 수단

[0007] 개시되는 실시예들에 따르면, 하나 이상의 프로세서들, 및 상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비한 컴퓨팅 장치에서 수행되는 방법으로서, 제1 메시지(m_j)를 제1 비밀키(s_j)로 암호화하여 생성된 제1 암호문(CT_j) 및 제2 메시지(m_k)를 제2 비밀키(s_k)로 암호화하여 생성된 제2 암호문(CT_k)을 획득하는 단계; 상기 제1 비밀키(s_j) 및 상기 제2 비밀키(s_k)를 기초로 생성된 비교키 쌍(CK_j, CK_k)을 획득하는 단계; 및 상기 제1 암호문(CT_j), 상기 제2 암호문(CT_k) 및 상기 비교키 쌍(CK_j, CK_k)을 이용하여 상기 제1 메시지(m_j)와 상기 제2 메시지(m_k)의 크기를 비교하는 단계를 포함하는, 방법이 제공된다.

[0008] 상기 제1 암호문(CT_j) 및 상기 제2 암호문(CT_k)은, 다음의 수학식

$$CT = (\{C_{i,0}, C_{i,1}\})_{i\in[n]}$$

[0009]

$$C_{i,0} = H(prefix(m, i-1) \| 0x_i)^s$$

[0010]

$$C_{i,1} = H(prefix(m, i-1) \| 0x_i + 1)^s$$

[0011]

[0012] (이때, m은 $m = x_1x_2\cdots x_n \in \{0,1\}^n$의 관계를 가지는 메시지, CT는 m에 대응되는 암호문, $prefix(m, i-1) = x_1x_2\cdots x_{i-1}$, s는 비밀키, H는 해시함수)

[0013] 에 의하여 생성될 수 있다.

[0014] 상기 비교키 쌍(CK_j, CK_k)은, 제1 비교키(CK_j) 및 제2 비교키(CK_k)를 포함하며, 상기 제1 비교키(CK_j) 및 상기 제2 비교키(CK_k)는, 다음의 수학식

$$CK_j = \hat{g}^{r \times s_j}$$

[0015]

$$CK_k = \hat{g}^{r \times s_k}$$

[0016]

[0017] (이때, g는 위수가 p인 겹선형 군(bilinear group) G의 생성원($g \in G$), $\hat{g}$는 위수가 p인 겹선형 군(bilinear group) $\hat{G}$의 생성원($\hat{g} \in \hat{G}$), e는 위수가 p인 겹선형 군 G, $\hat{G}$, G_T에 대하여 $G \times \hat{G} \rightarrow G_T$의 관계를 만족하는 겹선형 함수, r은 난수)

[0018] 에 의하여 계산될 수 있다.

[0019] 상기 제1 메시지(m_j)와 상기 제2 메시지(m_k)의 크기를 비교하는 단계는, $e(C_{i,0}, CK_k)$와 $e(C'_{i,0}, CK_j)$가 일치하지 않는 i의 최소값(i^*)을 계산하는 단계; $e(C_{i^*,1}, CK_k)$와 $e(C'_{i^*,0}, CK_j)$가 일치하는지 여부를 판단하는 단계; 및 상기 판단 결과 일치하는 경우, 상기 제1 메시지(m_j)의 크기가 상기 제2 메시지(m_k)의 크기보다 더 작다고 판단하는 단계를 포함할 수 있다.

[0020] 상기 방법은, 상기 판단 결과 일치하지 않는 경우, 상기 제1 메시지(m_j)의 크기가 상기 제2 메시지(m_k)의 크기보다 더 크다고 판단하는 단계를 더 포함할 수 있다.

[0021] 다른 예시적인 실시예에 따르면, 상기 방법을 컴퓨터상에서 수행하기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체가 제공된다.

[0022] 다른 예시적인 실시예에 따르면, 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, 제1 메시지(m_j)를 제1 비밀키(s_j)로 암호화하여 생성된 제1 암호문(CT_j) 및 제2 메시지(m_k)를 제2 비밀키(s_k)로 암호화하여 생성된 제2 암호문(CT_k)을 획득하는 단계; 상기 제1 비밀키(s_j) 및 상기 제2 비밀키(s_k)를 기초로 생성된 비교키 쌍(CK_j, CK_k)을 획득하는 단계; 및 상기 제1 암호문(CT_j), 상기 제2 암호문(CT_k) 및 상기 비교키 쌍(CK_j, CK_k)을 이용하여 상기 제1 메시지(m_1)와 상기 제2 메시지(m_2)의 크기를 비교하는 단계를 실행하기 위한 명령어들을 포함하는 장치가 제공된다.

[0023] 상기 제1 암호문(CT_j) 및 상기 제2 암호문(CT_k)은, 다음의 수학식

$$CT = (\{C_{i,0}, C_{i,1}\})_{i \in [n]}$$

[0024]

$$C_{i,0} = H(prefix(m, i-1) \| 0x_i)^s$$

[0025]

$$C_{i,1} = H(prefix(m, i-1) \| 0x_i + 1)^s$$

[0026]

[0027] (이때, m은 $m = x_1x_2 \cdots x_n \in \{0,1\}^n$의 관계를 가지는 메시지, CT는 m에 대응되는 암호문, $prefix(m, i-1) = x_1x_2 \cdots x_{i-1}$, s는 비밀키, H는 해시함수)

[0028] 에 의하여 생성될 수 있다.

[0029] 상기 비교키 쌍(CK_j, CK_k)은 제1 비교키(CK_j) 및 제2 비교키(CK_k)를 포함하며, 상기 제1 비교키(CK_j) 및 상기 제2 비교키(CK_k)는, 다음의 수학식

$$CK_j = \hat{g}^{r \times s_j}$$

[0030]

$$CK_k = \hat{g}^{r \times s_k}$$

[0031]

[0032] (이때, g는 위수가 p인 겹선형 군(bilinear group) G의 생성원(g ∈ G), $\hat{g}$ 는 위수가 p인 겹선형 군(bilinear group) $\hat{G}$ 의 생성원($\hat{g} \in \hat{G}$), e는 위수가 p인 겹선형 군 G, $\hat{G}$, G_T에 대하여 $G \times \hat{G} \rightarrow G_T$의 관계를 만족하는 겹선형 함수, r은 난수)

[0033] 에 의하여 계산될 수 있다.

[0034] 상기 제1 메시지(m_j)와 상기 제2 메시지(m_k)의 크기를 비교하는 단계는, $e(C_{i,0}, CK_k)$와 $e(C'_{i,0}, CK_j)$가 일치하지 않는 i의 최소값(i^*)을 계산하는 단계; $e(C_{i^*,1}, CK_k)$와 $e(C'_{i^*,0}, CK_j)$가 일치하는지 여부를 판단하는 단계; 및 상기 판단 결과 일치하는 경우, 상기 제1 메시지(m_j)의 크기가 상기 제2 메시지(m_k)의 크기보다 더 작다고 판단하는 단계를 포함할 수 있다.

[0035] 상기 프로그램들은, 상기 판단 결과 일치하지 않는 경우, 상기 제1 메시지(m_j)의 크기가 상기 제2 메시지(m_k)의 크기보다 더 크다고 판단하는 단계를 실행하기 위한 명령어들을 더 포함할 수 있다.

발명의 효과

[0037] 개시되는 실시예들에 따를 경우, 서로 다른 비밀키로 암호화된 암호문에 대한 별도의 복호화 과정 없이도 암호화되기 전의 평문에 대한 대소 비교가 가능하게 된다.

도면의 간단한 설명

[0039] 도 1은 일 실시예에 따른 암호문 비교 시스템을 설명하기 위한 블록도이다.

도 2는 일 실시예에 따른 암호문 비교 알고리즘을 설명하기 위한 순서도이다.

도 3은 예시적인 실시예들에서 사용되기에 적합한 컴퓨팅 장치를 포함하는 컴퓨팅 환경을 예시하여 설명하기 위한 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0040] 이하, 첨부된 도면을 참조하여 본 명세서에 개시된 실시예를 상세히 설명하되, 도면 부호에 관계없이 동일하거나 유사한 구성요소는 동일한 참조 번호를 부여하고 이에 대한 중복되는 설명은 생략하기로 한다. 이하의 설명에서 사용되는 구성요소에 대한 접미사 "모듈" 및 "부"는 명세서 작성의 용이함만이 고려되어 부여되거나 혼용되는 것으로서, 그 자체로 서로 구별되는 의미 또는 역할을 갖는 것은 아니다. 또한, 본 명세서에 개시된 실시예를 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 본 명세서에 개시된 실시 예의 요지를 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다. 또한, 첨부된 도면은 본 명세서에 개시된 실시 예를 쉽게 이해할 수 있도록 하기 위한 것일 뿐, 첨부된 도면에 의해 본 명세서에 개시된 기술적 사상이 제한되지 않으며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.

[0041] 제1, 제2 등과 같이 서수를 포함하는 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되지는 않는다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다.

[0042] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0043] 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다.

[0044] 본 출원에서, "포함한다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계,

동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0045] 이하, 도면들을 참조하여 본 발명의 실시 예에 대해 상세히 설명하기로 한다. 본 발명은 본 발명의 정신 및 필수적 특징을 벗어나지 않는 범위에서 다른 특정한 형태로 구체화될 수 있음은 당업자에게 자명하다.

[0047] 도 1은 일 실시예에 따른 암호문 비교 시스템(100)을 설명하기 위한 블록도이다. 도 1에 도시된 바와 같이, 본 발명의 일 실시예에 따른 암호문 비교 시스템(100)은 단말(110, 120, 130) 및 서버(140)를 포함한다. 도 1에는 본 발명을 쉽게 설명하기 위한 편의상 단말(110, 120, 130)을 제1 단말(110), 제2 단말(120) 및 제3 단말(130)로 나누어 도시하였을 뿐, 실제 본 발명을 구현함에 있어 단말의 개수 및 각각의 기능은 이에 한정되지 않는다. 서버(140) 또한 하나인 것처럼 도시되었으나, 복수의 서버가 후술하는 서버(140)의 복수의 기능을 각각 나누어 구현할 수 있다.

[0048] 제1 단말(110) 및 제2 단말(120)은 서로 다른 사용자가 사용하는 단말일 수 있다. 제1 단말(110)은 제1 메시지(m_j)를 제1 비밀키(s_j)를 기초로 암호화하여 제1 암호문(CT_j)를 생성하며, 제2 단말(120)은 제2 메시지(m_k)를 제2 비밀키(s_k)를 기초로 암호화하여 제2 암호문(CT_k)을 생성할 수 있다.

[0049] 제3 단말(130)은 서로 다른 비밀키(s_j, s_k)를 기초로 생성된 비교키 쌍(CK_j, CK_k)을 이용하여 제1 암호문(CT_j) 및 제2 암호문(CT_k)을 비교할 수 있다. 구체적으로, 제3 단말(130)은 제1 암호문(CT_j) 및 제2 암호문(CT_k)을 비교함으로써, 제1 암호문(CT_j) 및 제2 암호문(CT_k) 각각에 내재된 제1 메시지(m_j) 및 제2 메시지(m_k)의 대소를 비교할 수 있다

[0050] 서버(140)는 제1 단말(110)로 제1 암호문(CT_j)의 생성에 기초가 되는 제1 비밀키(s_j)를 제공하며, 제2 단말(120)로 제2 암호문(CT_k)의 생성의 기초가 되는 제2 비밀키(s_k)를 제공하고, 제3 단말(130)로 제1 암호문(CT_j) 및 제2 암호문(CT_k)의 비교에 기초가 되는 비교키 쌍(CK_j, CK_k)을 제공할 수 있다.

[0051] 데이터베이스(150)는 서버(140)로부터 제공되는 비밀키에 의하여 암호화된 암호문이 저장되는 저장 장치이다. 데이터베이스(150)는 제1 단말(110) 및 제2 단말(120)로부터 생성되는 제1 암호문(CT_j) 및 제2 암호문(CT_k)을 저장하고, 제3 단말(130)의 요청시 기 저장된 제1 암호문(CT_j) 및 제2 암호문(CT_k)을 제공할 수 있다.

[0052] 한편, 제1 단말(110), 제2 단말(120) 및 제3 단말(130)은 모두 하나의 동일한 단말일 수 있으며, 각각의 동작을 구현하도록 명령하는 사용자만이 상이할 수 있다. 그 밖에도, 단말(110, 120, 130)과 서버(140) 간의 역할 분담은 실시예에 따라 다양하게 구성될 수 있다.

[0054] 도 2는 일 실시예에 따른 암호문 비교 방법을 설명하기 위한 순서도이다. 도시된 방법은 하나 이상의 프로세서들, 및 상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비한 컴퓨팅 장치, 예컨대 전술한 제1 단말(110), 제2 단말(120) 및 제3 단말(130)에 의하여 수행될 수 있다. 도시된 흐름도에서는 상기 방법을 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.

[0055] 제1 단말(110)은 서버(140)로부터 제1 사용자 인덱스(j)를 할당받을 수 있다(S201). 서버(140)는 제1 단말(110)에 할당한 제1 사용자 인덱스(j)를 기초로 제1 비밀키(s_j)를 생성하고(S202), 제1 단말(110)로 제1 비밀키(s_j)를 제공할 수 있다(S203). 제1 단말(110)은 제1 비밀키(s_j)를 기초로 제1 메시지(mj)를 암호화하여 제1 암호문(CT_j)을 생성하고(S204), 생성된 제1 암호문(CT_j)을 별도의 암호문 저장 데이터베이스(150)에 저장할 수 있다(S205).

[0056] 제2 단말(120)은 서버(140)로부터 제1 단말(110)과 상이한 제2 사용자 인덱스(k)를 할당받을 수 있다(S206). 서버(140)는 제2 단말(120)에 할당한 제2 사용자 인덱스(k)를 기초로 제2 비밀키(s_k)를 생성하고(S207), 제2 단말(120)로 제2 비밀키(s_k)를 제공할 수 있다(S208). 제2 단말(120)은 제2 비밀키(s_k)를 기초로 제2 메시지(m_k)를 암호화하여 제2 암호문(CT_k)을 생성하고(S209), 생성된 제2 암호문(CT_k)을 별도의 암호문 저장 데이터베이스(150)에 저장할 수 있다 (S210).

[0057] 제3 단말(130)은 서버(140)로 비교키 쌍(CK_j, CK_k)을 요청할 수 있다(S211). 예를 들어, 제3 단말(130)은 비교하고자 하는 제1 암호문(CT_j) 및 제2 암호문(CT_k)을 서버(140)로 제공함으로써, 비교키 쌍(CK_j, CK_k)을 요청할 수 있다. 다만, 제3 단말(130)이 서버(140)로 비교키 쌍(CK_j, CK_k)을 요청하는 방법은 이에 한정되는 것은 아니다.

[0058] 서버(140)는 두 개의 사용자 인덱스(j, k)에 각각 대응되는 두 개의 비밀키(s_j, s_k)를 기초로 비교키 쌍(CK_j, CK_k)을 생성하고(S212), 제3 단말(130)로 비교키 쌍(CK_j, CK_k)을 제공할 수 있다(S213). 제3 단말(130)은 비교키 쌍(CK_j, CK_k)을 기초로 제1 암호문(CT_j) 및 제2 암호문(CT_k)을 비교함으로써 두 개의 메시지(m_j, m_k)간의 대소를 비교할 수 있다(S214).

[0059] 이러한 환경을 구성하기 위한 알고리즘은 다음과 같이 5개의 알고리즘으로 구성될 수 있다.

[0060] 첫 번째, 셋업(Setup) 알고리즘은 보안 상수(Security Parameter, 1^λ) 및 시스템에 참여할 수 있는 사용자 수(ℓ)을 입력받고, 마스터 비밀키(Master secret Key, MK)와 공개 파라미터(Public Parameters, PP)를 출력하는 알고리즘이다. 서버(140)는 Setup(1^λ, ℓ) 알고리즘을 통해 생성한 공개 파라미터(PP)는 공개하고, 마스터 비밀키(MK)는 안전하게 저장할 수 있다.

[0061] 구체적으로, 서버(140)는 보안 상수(1^λ) 및 시스템에 참여할 수 있는 사용자 수(ℓ)를 입력받고, 위수가 p인 겹선형 군(bilinear group) G, $\hat{G}$, G_T, 겹선형 함수(bilinear map) e: $G \times \hat{G} \rightarrow G_T$, 및 겹선형 군 G의 생성원인 g($g \in G$) 및 겹선형 군 $\hat{G}$의 생성원인 $\hat{g}$ ($\hat{g} \in \hat{G}$)를 출력할 수 있다. 여기서, p는 소수(prime number)일 수 있으나, 반드시 이에 한정되는 것은 아니다.

[0062] 그리고, 서버(140)는 모든 $j \in [\ell]$에 대해 임의의 $s_j \in Z_p$를 선택하여 마스터 비밀키 $MK = \{s_j\}_{j\in[\ell]}$ 와 공개 파라미터 $PP = ((p, G, \hat{G}, G_T, e), g, \hat{g}, H)$를 출력한다. 여기서, 해시함수 $H: \{0,1\}^* \rightarrow G$는 임의의 문자열을 군으로 맵핑시키는 함수이다. 또한, Z_p는 $Z_p = \{1, 2, \ldots, p-1\}$의 관계를 만족하는 집합이다.

[0063] 두 번째, 비밀키 생성(GenKey) 알고리즘은 사용자 인덱스(index, j), 마스터 비밀키(MK) 및 공개 파라미터(PP)를 입력받고 비밀키(s_j)를 출력하는 알고리즘이다. 서버(140)는 GenKey(j, MK, PP) 알고리즘을 통해 제1 비밀키(s_j)를 생성할 수 있으며, GenKey(2, MK, PP) 알고리즘을 통해 제2 비밀키(s_j)를 생성할 수 있다.

[0064] 세 번째, 암호화(Encrypt) 알고리즘은 메시지(m), 비밀키(s) 및 공개 파라미터(PP)를 입력받고, 암호문(CT)를 출력하는 알고리즘이다. Encrypt(m, s, PP) 알고리즘을 통해, 제1 단말(110)은 제1 메시지(m_j) 및 제1 비밀키(s_j)를 기초로 제1 암호문(CT_j)을 생성하고, 제2 단말(120)은 제2 메시지(m_k) 및 제2 비밀키(s_k)를 기초로 제2 암호문(CT_k)을 생성할 수 있다.

[0065] 이때, 제1 단말(110)은 제1 메시지(m_j)를 대칭키 방식으로 암호화하여 제1 암호문(CT_j)을 생성하고, 제2 단말(120)은 제2 메시지(m_k)를 대칭키 방식으로 암호화하여 제2 암호문(CT_k)을 생성할 수 있다. 제1 암호문(CT_j) 및 제2 암호문(CT_k)은, 구체적으로, 하기의 수학식에 의하여 생성될 수 있다.

[0066] [수학식 1]

$$CT = (\{C_{i,0}, C_{i,1}\})_{i\in[n]}$$

[0067]

$$C_{i,0} = H(prefix(m, i-1) \parallel 0x_i)^s$$

[0068]

$$C_{i,1} = H(prefix(m, i-1) \| 0x_i + 1)^s$$

[0069]

[0070] 이때, m은 $m = x_1x_2\cdots x_n \in \{0,1\}^n$의 관계를 가지는 메시지, CT는 m에 대응되는 암호문, prefix(m, i-1)은 m의 첫 번째 비트부터 i-1번째 비트까지의 부분 문자열($prefix(m, i-1) = x_1x_2\cdots x_{i-1}$), s는 비밀키, H는 해시함수이다.

[0071] 상기 수학식에 의하여 계산된 제1 암호문(CT_j) 및 제2 암호문(CT_k)은 다음과 같다.

[0072] 제1암호문:

$$CT_j = (\{C_{i,0}, C_{i,1}\})_{i\in[n]}$$

[0073]

$$C_{i,0} = H(prefix(m_j, i-1) \| 0x_i)^{s_j}$$

[0074]

$$C_{i,1} = H(prefix(m_j, i-1) \| 0x_i + 1)^{s_j}$$

[0075]

[0076] 제2암호문:

$$CT_k = (\{C'_{i,0}, C'_{i,1}\})_{i\in[n]}$$

[0077]

$$C'_{i,0} = H(prefix(m_k, i-1) \| 0x_i)^{s_k}$$

[0078]

$$C'_{i,1} = H(prefix(m_k, i-1) \| 0x_i + 1)^{s_k}$$

[0079]

[0080] 네 번째, 비교키 생성(GenCmpKey) 알고리즘은 두 개의 사용자 인덱스(j, k), 마스터 비밀키(MK) 및 공개 파라미터(PP)를 입력받고 비교키 쌍(CK_j, CK_k)을 출력하는 알고리즘이다. 서버(140)는 GenCmpKey(j, k, MK, PP) 알고리즘을 통해 비교키 쌍(CK_j, CK_k)을 생성할 수 있다.

[0081] 구체적으로, 서버(140)는 두 개의 사용자 인덱스(j, k)에 대응되는 비밀키(s_j, s_k)를 이용하여 비교키 쌍(CK_j, CK_k)을 계산할 수 있다. 상기 비교키 쌍(CK_j, CK_k)은 제1 비교키(CK_j) 및 제2 비교키(CK_k)를 포함하며, 상기 제1 비교키(CK_j) 및 상기 제2 비교키(CK_k)는, 다음의 수학식 2에 의하여 계산될 수 있다.

[0082] [수학식 2]

$$CK_j = \hat{g}^{r\times s_j}$$

[0083]

$$CK_k = \hat{g}^{r\times s_k}$$

[0084]

[0085] 이때, g는 위수가 p인 겹선형 군(bilinear group) G의 생성원($g \in G$), $\hat{g}$는 위수가 p인 겹선형 군(bilinear group) $\hat{G}$의 생성원($\hat{g} \in \hat{G}$), e는 위수가 p인 겹선형 군 G, $\hat{G}$, G_T에 대하여 $G\times\hat{G}\rightarrow G_T$의 관계를 만족하는 겹선형 함수, r은 $r\in Z_p$인 관계를 만족하는 난수일 수 있다. 여기서, 난수(r)를 곱한 이유는 새로운 비교키 쌍의 생성을 막기 위함이다.

[0086] 다섯 번째, 다중 비교(CompareMC) 알고리즘은 두 개의 암호문(CT_j, CT_k)과, 두 개의 사용자 인덱스(j, k)에 대응되는 비교키 쌍(CK_j, CK_k) 및 공개 파라미터(PP)를 입력받고 비교값을 출력할 수 있다. 제3 단말(130)은

CompareMC(CT_j, CT_k, CK_j, CK_k, PP) 알고리즘을 통해 데이터(m_j, m_k)를 비교할 수 있다.

[0087] 예를 들어, 제3 단말(130)은 CompareMC(CT_j, CT_k, CK_j, CK_k, PP) 알고리즘을 이용하여 최상위 비트(i=1)부터 $e(C_{i,0}, CK_k)$와 $e(C'_{i,0}, CK_j)$를 계산해 나가면서 $e(C_{i,0}, CK_k)$와 $e(C'_{i,0}, CK_j)$가 일치하지 않는 i의 최소값(i^*)을 계산할 수 있다.

[0088] 제3 단말(130)은 $e(C_{i,0}, CK_k)$와 $e(C'_{i,0}, CK_j)$가 일치하지 않는 i의 최소값(i^*)을 구한 경우, 다음으로 $e(C_{i*,1}, CK_k)$와 $e(C'_{i*,0}, CK_j)$를 비교할 수 있다. 상기 비교 결과 $e(C_{i*,1}, CK_k)$와 $e(C'_{i*,0}, CK_j)$가 일치하지 않는 경우, 제3 단말(130)은 제1 메시지(m_j)의 크기가 제2 메시지(m_k)의 크기보다 더 크다고 판단할 수 있다. 이와 달리 제3 단말(130)은 $e(C_{i*,1}, CK_k)$와 $e(C'_{i*,0}, CK_j)$가 일치하는 경우, 제1 메시지(m_j)의 크기가 상기 제2 메시지(m_k)의 크기보다 더 작다고 판단할 수 있다.

[0090] 도 3은 예시적인 실시예들에서 사용되기에 적합한 컴퓨팅 장치를 포함하는 컴퓨팅 환경(10)을 예시하여 설명하기 위한 블록도이다.

[0091] 도시된 실시예에서, 각 컴포넌트들은 이하에 기술된 것 이외에 상이한 기능 및 능력을 가질 수 있고, 이하에 기술되는 것 이외에도 추가적인 컴포넌트를 포함할 수 있다.

[0092] 도시된 컴퓨팅 환경(10)은 컴퓨팅 장치(12)를 포함한다. 일 실시예에서, 컴퓨팅 장치(12)는 단말(예를 들어, 제1 단말(110), 제2 단말(120), 제3 단말(130))일 수 있다. 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.

[0093] 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.

[0094] 통신 버스(18)는 프로세서(14), 컴퓨터 판독 가능 저장 매체(16)를 포함하여 컴퓨팅 장치(12)의 다른 다양한 컴포넌트들을 상호 연결한다.

[0095] 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.

[0097] 이상의 상세한 설명은 모든 면에서 제한적으로 해석되어서는 아니되고 예시적인 것으로 고려되어야 한다. 본 발명의 범위는 첨부된 청구항의 합리적 해석에 의해 결정되어야 하고, 본 발명의 등가적 범위 내에서의 모든 변경은 본 발명의 범위에 포함된다.

부호의 설명

[0099] 100: 암호문 비교 시스템

110: 제1 단말

120: 제2 단말

130: 제3 단말

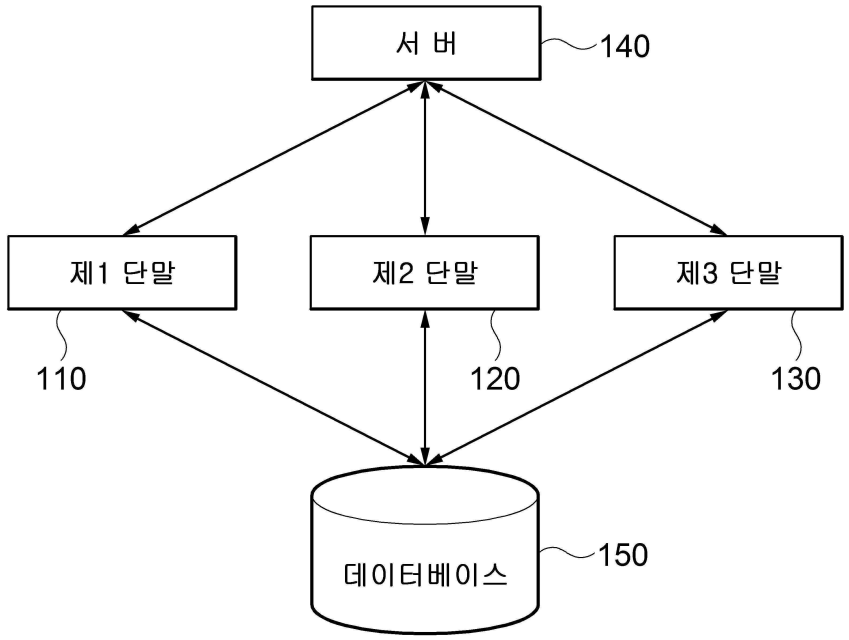
140: 서버

150: 데이터베이스

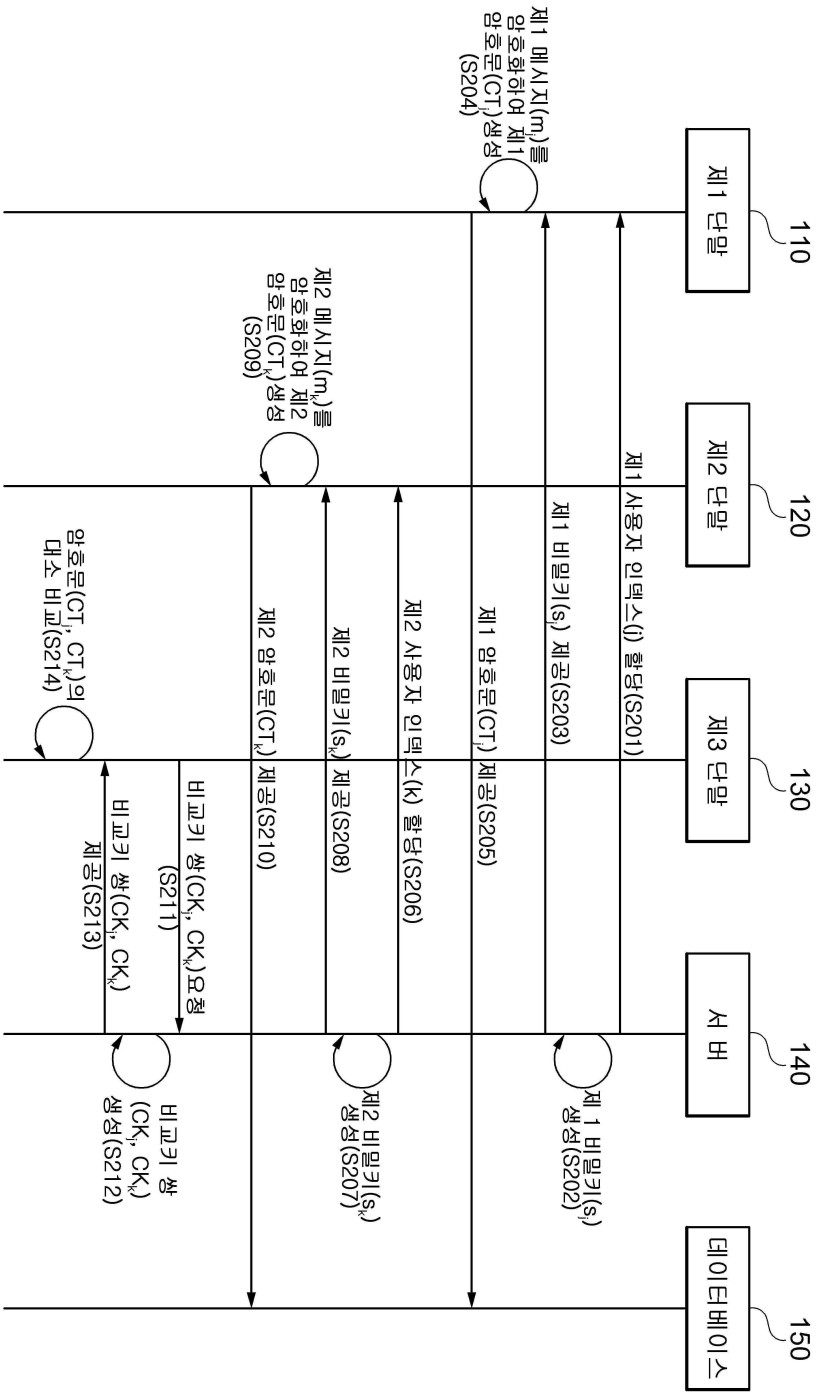
도면

도면1

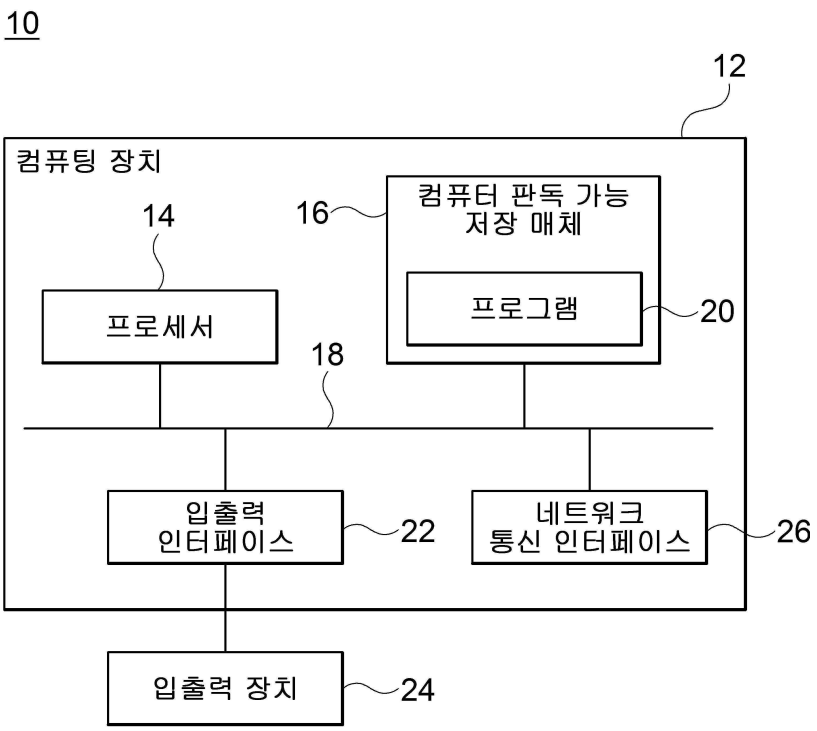
100



도면2


제1 단말
110
제2 단말
120
제3 단말
130
서 버
140
데이터베이스
150
제1 메시지(m_i)를 암호화하여 제1 암호문(CT_i)생성 (S204)
제1 사용자 인덱스(j) 할당(S201)
제1 비밀키(s_j) 제공(S203)
제1 암호문(CT_i) 제공(S205)
제1 비밀키(s_j) 생성(S202)
제2 메시지(m_k)를 암호화하여 제2 암호문(CT_k)생성 (S209)
제2 사용자 인덱스(k) 할당(S206)
제2 비밀키(s_k) 제공(S208)
제2 암호문(CT_k) 제공(S210)
제2 비밀키(s_k) 생성(S207)
암호문(CT_i, CT_k)의 대소 비교(S214)
비교키 쌍(CK_i, CK_k)요청 (S211)
비교키 쌍(CK_i, CK_k) 제공(S213)
비교키 쌍 (CK_i, CK_k) 생성(S212)

도면3


10
12
컴퓨팅 장치
14
프로세서
16
컴퓨터 판독 가능
저장 매체
프로그램
20
18
입출력
인터페이스
22
네트워크
통신 인터페이스
26
입출력 장치
24