(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년12월17일
(11) 등록번호 10-2192594
(24) 등록일자 2020년12월11일

(51) 국제특허분류(Int. Cl.)
H04L 9/06 (2006.01) *H04L 9/08* (2006.01)
(52) CPC특허분류
H04L 9/0618 (2013.01)
H04L 9/0643 (2013.01)
(21) 출원번호 10-2019-0006565
(22) 출원일자 2019년01월18일
심사청구일자 2019년01월18일
(65) 공개번호 10-2020-0089832
(43) 공개일자 2020년07월28일
(56) 선행기술조사문헌
US20140133651 A1*
(뒷면에 계속)
전체 청구항 수 : 총 12 항

(73) 특허권자
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
(72) 발명자
이광수
서울특별시 광진구 군자로 121, 229호
엄지은
서울특별시 성북구 인촌로22길 6-7, 215호
(74) 대리인
두호특허법인

심사관 : 최재귀

(54) 발명의 명칭 **신뢰기관이 없는 다중 클라이언트 환경의 순서 노출 암호화를 위한 장치 및 방법**

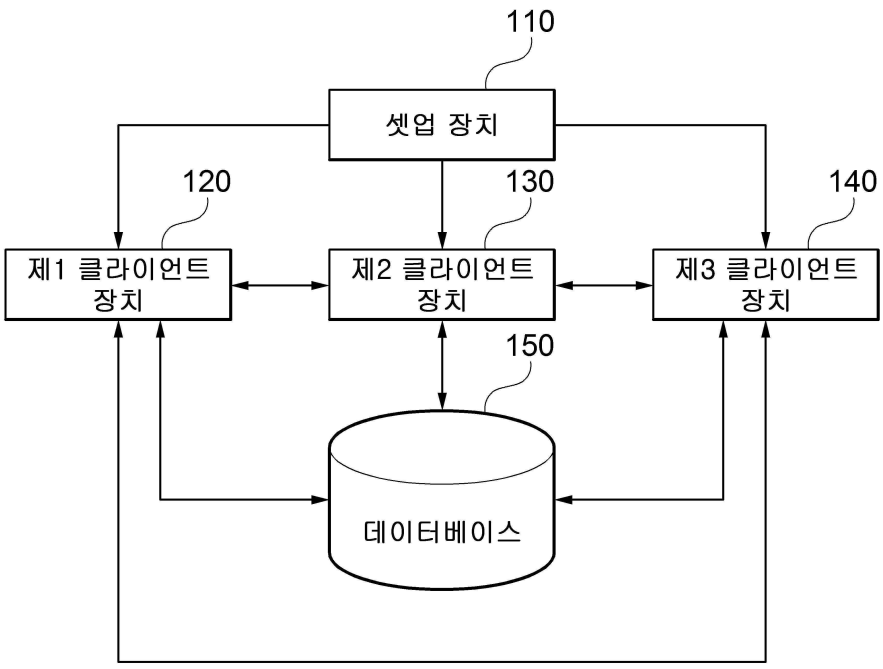
(57) 요 약

순서 노출 암호화를 위한 장치 및 방법이 개시된다. 본 발명의 일 실시예에 따른 순서 노출 암호화를 위한 방법은, 제1 사용자의 비밀키를 이용하여 제1 평문을 암호화한 제1 암호문 및 제2 사용자의 비밀키를 이용하여 제2 평문을 암호화한 제2 암호문을 획득하는 단계; 상기 제1 사용자에 의해 이용되는 제1 클라이언트 장치 및 제2 사

(뒷면에 계속)

대 표 도 - 도1

100



용자에 의해 이용되는 제2 클라이언트 장치로 상기 제1 사용자의 식별 정보 및 상기 제2 사용자의 식별 정보를 제공하는 단계; 상기 제1 클라이언트 장치로부터 상기 제1 사용자의 식별 정보, 상기 제2 사용자의 식별 정보 및 상기 제1 사용자의 비밀키를 이용하여 생성된 제1 비교키 엘리먼트를 수신하고, 상기 제2 클라이언트 장치로부터 상기 제1 사용자의 식별 정보, 상기 제2 사용자의 식별 정보 및 상기 제2 사용자의 비밀키를 이용하여 생성된 제2 비교키 엘리먼트를 수신하는 단계; 및 상기 제1 비교키 엘리먼트 및 상기 제2 비교키 엘리먼트를 포함하는 비교키를 이용하여 상기 제1 암호문 및 상기 제2 암호문을 암호화된 상태에서 비교하고, 상기 비교 결과에 기초하여 상기 제1 평문 및 상기 제2 평문 사이의 대소를 판단하는 단계를 포함한다.

(52) CPC특허분류
H04L 9/0816 (2013.01)

(56) 선행기술조사문헌
Mark Bun and Mark Zhandry, "Order-revealing encryption and the hardness of private learning", LNCS 9562, pp.176-206, 2016.
US20190007210 A1
US20160013933 A1
KR1020190133350 A
*는 심사관에 의하여 인용된 문헌

이 발명을 지원한 국가연구개발사업

과제고유번호	711076035
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기술진흥센터
연구사업명	정보보호핵심원천기술개발
연구과제명	(함수암호 1세부) 함수암호 기법 설계분석 및 구현기술 연구
기 여 율	1/1
과제수행기관명	상명대학교 산학협력단
연구기간	2018.06.01 ~ 2019.03.31

공지예외적용 : 있음

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 사용자의 비밀키를 이용하여 제1 평문을 암호화한 제1 암호문 및 제2 사용자의 비밀키를 이용하여 제2 평문을 암호화한 제2 암호문을 획득하는 단계;

상기 제1 사용자에 의해 이용되는 제1 클라이언트 장치 및 제2 사용자에 의해 이용되는 제2 클라이언트 장치로 상기 제1 사용자의 식별 정보 및 상기 제2 사용자의 식별 정보를 제공하는 단계;

상기 제1 클라이언트 장치로부터 상기 제1 사용자의 식별 정보, 상기 제2 사용자의 식별 정보 및 상기 제1 사용자의 비밀키를 이용하여 생성된 제1 비교키 엘리먼트를 수신하고, 상기 제2 클라이언트 장치로부터 상기 제1 사용자의 식별 정보, 상기 제2 사용자의 식별 정보 및 상기 제2 사용자의 비밀키를 이용하여 생성된 제2 비교키 엘리먼트를 수신하는 단계; 및

상기 제1 비교키 엘리먼트 및 상기 제2 비교키 엘리먼트를 포함하는 비교키를 이용하여 상기 제1 암호문 및 상기 제2 암호문을 암호화된 상태에서 비교하고, 상기 비교 결과에 기초하여 상기 제1 평문 및 상기 제2 평문 사이의 대소를 판단하는 단계를 포함하는, 방법.

청구항 2

청구항 1에 있어서,

상기 제1 비교키 엘리먼트는, 상기 제1 사용자의 식별 정보 및 상기 제2 사용자의 식별 정보에 대해 해시 함수(hash function)를 적용한 결과 값과 상기 제1 사용자의 비밀키를 이용하여 생성되고,

상기 제2 비교키 엘리먼트는, 상기 제1 사용자의 식별 정보 및 상기 제2 사용자의 식별 정보에 대해 상기 해시 함수를 적용한 결과 값과 상기 제2 사용자의 비밀키를 이용하여 생성되는, 방법.

청구항 3

청구항 2에 있어서,

상기 제1 비교키 엘리먼트는, 아래의 수학식 1

[수학식 1]

$$K_0 = \hat{H}(ID_j \parallel ID_k)^{s_j}$$

(이때, K_0는 상기 제1 비교키 엘리먼트, ID_j는 상기 제1 사용자의 식별 정보, ID_k는 상기 제2 사용자의 식별 정보, s_j는 상기 제1 사용자의 비밀키, $\hat{H}$는 $\hat{H}:\{0,1\}^* \rightarrow \hat{G}$를 만족하는 해시 함수, $\hat{G}$는 위수가 소수 p인 덧셈군)을 이용하여 생성되고,

상기 제2 비교키 엘리먼트는, 아래의 수학식 2

[수학식 2]

$$K_1 = \widehat{H}(ID_j \parallel ID_k)^{s_k}$$

(이때, K_1은 상기 제2 비교키 엘리먼트, s_k는 상기 제2 사용자의 비밀키)를 이용하여 생성되는, 방법.

청구항 4

청구항 1에 있어서,

상기 제1 암호문은, 상기 제1 평문의 각 비트 값에 대한 프리픽스(prefix) 비트 열 및 상기 제1 사용자의 비밀키를 이용하여 상기 제1 평문을 비트 단위로 암호화하여 생성되고,

상기 제2 암호문은, 상기 제2 평문의 각 비트 값에 대한 프리픽스 비트 열 및 상기 제2 사용자의 비밀키를 이용하여 상기 제2 평문을 비트 단위로 암호화하여 생성되는, 방법.

청구항 5

청구항 4에 있어서,

상기 제1 암호문은, 아래의 수학식 3 내지 5

[수학식 3]

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

[수학식 4]

$$C_{i,1} = H\left(prefix(m, i-1) \parallel (0x_i + 1)\right)^{s_j}$$

[수학식 5]

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

(이때, CT_j는 상기 1 암호문, m은 $m = x_1 x_2 \cdots x_n \in \{0,1\}^n$인 상기 제1 평문, x_i는 상기 제1 평문의 i 번째 비트 값, $prefix(m, i-1)$는 상기 제1 평문의 i 번째 비트 값에 대한 프리픽스 비트 열, s_j는 상기 제1 사용자의 비밀키, H는 $H: \{0,1\}^* \rightarrow G$를 만족하는 해시 함수, G는 위수가 소수 p인 덧셈 군)을 이용하여 생성되고,

상기 제2 암호문은, 아래의 수학식 6 내지 8

[수학식 6]

$$C'_{i,0} = H(prefix(m', i-1) \parallel 0x'_i)^{s_k}$$

[수학식 7]

$$C'_{i,1} = H(prefix(m', i-1) \parallel (0x'_i + 1))^{s_k}$$

[수학식 8]

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

CT_k $m = x'_1 x'_2 \cdots x'_n \in \{0,1\}^n$ x'_i

(이때, 는 상기 제2 암호문, m'은 인 상기 제2 평문, 는 상기 제2 평문의

$prefix(m', i-1)$ s_k

i 번째 비트 값, 는 상기 제2 평문의 i 번째 비트 값에 대한 프리픽스 비트 열, 는 상기 제2 사용자의 비밀키)을 이용하여 생성되는, 방법.

청구항 6

청구항 5에 있어서,

상기 판단하는 단계는,

$e(C_{i,0}, K_1)$ $e(C'_{i,0}, K_0)$ $e: G \times \hat{G} \rightarrow G_T$ $\hat{G}$

와 (이때, e는 를 만족하는 겹선형(bilinear) 함수, 는 위수가 소

G_T

수 p인 덧셈 군, 는 위수가 소수 p인 곱셈 군, K_0는 상기 제1 비교키 엘리먼트, K_1은 상기 제2 비교키 엘리먼트)가 일치하지 않는 i의 최소 값 i^*가 존재하는지 여부를 판단하는 단계; 및

$e(C_{i^*,1}, K_1)$ $e(C'_{i^*,0}, K_0)$

상기 최소 값 i^*이 존재하고, 와 가 일치하는 경우, 상기 제1 평문이 상기 제2 평문보

$e(C_{i^*,1}, K_1)$ $e(C'_{i^*,0}, K_0)$

다 작은 것으로 판단하고, 와 가 일치하지 않거나 상기 최소 값 i^*이 존재하지 않는 경우, 상기 제1 평문이 상기 제2 평문보다 크거나 같은 것으로 판단하는 단계를 포함하는, 방법.

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 사용자의 비밀키를 이용하여 제1 평문을 암호화한 제1 암호문 및 제2 사용자의 비밀키를 이용하여 제2 평문을 암호화한 제2 암호문을 획득하는 단계;

상기 제1 사용자에 의해 이용되는 제1 클라이언트 장치 및 제2 사용자에 의해 이용되는 제2 클라이언트 장치로 상기 제1 사용자의 식별 정보 및 상기 제2 사용자의 식별 정보를 제공하는 단계;

상기 제1 클라이언트 장치로부터 상기 제1 사용자의 식별 정보, 상기 제2 사용자의 식별 정보 및 상기 제1 사용자의 비밀키를 이용하여 생성된 제1 비교키 엘리먼트를 수신하고, 상기 제2 클라이언트 장치로부터 상기 제1 사용자의 식별 정보, 상기 제2 사용자의 식별 정보 및 상기 제2 사용자의 비밀키를 이용하여 생성된 제2 비교키 엘리먼트를 수신하는 단계; 및

상기 제1 비교키 엘리먼트 및 상기 제2 비교키 엘리먼트를 포함하는 비교키를 이용하여 상기 제1 암호문 및 상

기 제2 암호문을 암호화된 상태에서 비교하고, 상기 비교 결과에 기초하여 상기 제1 평문 및 상기 제2 평문 사이의 대소를 판단하는 단계를 실행하기 위한 명령어들을 포함하는, 장치.

청구항 8

청구항 7에 있어서,

상기 제1 비교키 엘리먼트는, 상기 제1 사용자의 식별 정보 및 상기 제2 사용자의 식별 정보에 대해 해시 함수(hash function)를 적용한 결과 값과 상기 제1 사용자의 비밀키를 이용하여 생성되고,

상기 제2 비교키 엘리먼트는, 상기 제1 사용자의 식별 정보 및 상기 제2 사용자의 식별 정보에 대해 상기 해시 함수를 적용한 결과 값과 상기 제2 사용자의 비밀키를 이용하여 생성되는, 장치.

청구항 9

청구항 8에 있어서,

상기 제1 비교키 엘리먼트는, 아래의 수학식 1

[수학식 1]

$$K_0 = \hat{H}(ID_j \parallel ID_k)^{s_j}$$

(이때, K_0는 상기 제1 비교키 엘리먼트, ID_j는 상기 제1 사용자의 식별 정보, ID_k는 상기 제2 사용자의 식별 정보, s_j는 상기 제1 사용자의 비밀키, $\hat{H}$는 $\hat{H}: \{0,1\}^* \rightarrow \hat{G}$를 만족하는 해시 함수, $\hat{G}$는 위수가 소수 p인 덧셈군)을 이용하여 생성되고,

상기 제2 비교키 엘리먼트는, 아래의 수학식 2

[수학식 2]

$$K_1 = \hat{H}(ID_j \parallel ID_k)^{s_k}$$

(이때, K_1은 상기 제2 비교키 엘리먼트, s_k는 상기 제2 사용자의 비밀키)를 이용하여 생성되는, 장치.

청구항 10

청구항 7에 있어서,

상기 제1 암호문은, 상기 제1 평문의 각 비트 값에 대한 프리픽스(prefix) 비트 열 및 상기 제1 사용자의 비밀키를 이용하여 상기 제1 평문을 비트 단위로 암호화하여 생성되고,

상기 제2 암호문은, 상기 제2 평문의 각 비트 값에 대한 프리픽스 비트 열 및 상기 제2 사용자의 비밀키를 이용하여 상기 제2 평문을 비트 단위로 암호화하여 생성되는, 장치.

청구항 11

청구항 10에 있어서,

상기 제1 암호문은, 아래의 수학식 3 내지 5

[수학식 3]

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

[수학식 4]

$$C_{i,1} = H\left(prefix(m,i-1) \parallel (0x_i+1)\right)^{s_j}$$

[수학식 5]

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

CT_j $m = x_1x_2\cdots x_n \in \{0,1\}^n$ x_i

(이때, 는 상기 1 암호문, m은 인 상기 제1 평문, 는 상기 제1 평문의 i 번

$prefix(m,i-1)$ s_j

째 비트 값, 는 상기 제1 평문의 i 번째 비트 값에 대한 프리픽스 비트 열, 는 상기 제1

$H: \{0,1\}^* \rightarrow G$ G

사용자의 비밀키, H는 를 만족하는 해시 함수, 는 위수가 소수 p인 덧셈 군)을 이용하여 생성되고,

상기 제2 암호문은, 아래의 수학식 6 내지 8

[수학식 6]

$$C'_{i,0} = H(prefix(m',i-1) \parallel 0x'_i)^{s_k}$$

[수학식 7]

$$C'_{i,1} = H(prefix(m',i-1) \parallel (0x'_i+1))^{s_k}$$

[수학식 8]

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

CT_k $m = x'_1x'_2\cdots x'_n \in \{0,1\}^n$ x'_i

(이때, 는 상기 제2 암호문, m'은 인 상기 제2 평문, 는 상기 제2 평문의

$prefix(m',i-1)$ s_k

i 번째 비트 값, 는 상기 제2 평문의 i 번째 비트 값에 대한 프리픽스 비트 열, 는 상기 제2 사용자의 비밀키)을 이용하여 생성되는, 장치.

청구항 12

청구항 11에 있어서,

상기 판단하는 단계는,

$e(C_{i,0}, K_1)$ $e(C'_{i,0}, K_0)$ $e: G \times \hat{G} \rightarrow G_T$ $\hat{G}$

와 (이때, e는 를 만족하는 겹선형(bilinear) 함수, 는 위수가 소

G_T

수 p인 덧셈 군, 는 위수가 소수 p인 곱셈 군, K_0는 상기 제1 비교키 엘리먼트, K_1은 상기 제2 비교키 엘리

먼트)가 일치하지 않는 i의 최소 값 i^*가 존재하는지 여부를 판단하는 단계; 및

상기 최소 값 i^*이 존재하고, $e(C_{i^*,1}, K_1)$ 와 $e(C'_{i^*,0}, K_0)$ 가 일치하는 경우, 상기 제1 평문이 상기 제2 평문보다 작은 것으로 판단하고, $e(C_{i^*,1}, K_1)$ 와 $e(C'_{i^*,0}, K_0)$ 가 일치하지 않거나 상기 최소 값 i^*이 존재하지 않는 경우, 상기 제1 평문이 상기 제2 평문보다 크거나 같은 것으로 판단하는 단계를 포함하는, 장치.

발명의 설명

기 술 분 야

[0001] 본 발명의 실시예들은 암호화 기술과 관련된다.

배 경 기 술

[0002] 순서 노출 암호화(Order-Revealing Encryption; ORE) 기술은 암호화된 상태에서 평문의 대소 비교를 가능하게 하는 기술이다. 기존의 ORE 기법은 모두 하나의 사용자로부터 생성된 즉, 하나의 비밀키로 암호화된 암호문 간의 비교만을 지원하였으나, 본 출원인의 한국특허출원 제10-2018-0058145호는 다중 클라이언트 환경에서 다수의 사용자로부터 생성된 즉, 서로 다른 비밀키로 암호화된 암호문 간의 비교를 통해 평문의 대소를 판단하기 위한 기법(이하, MC-ORE)을 제시하였다.

[0003] MC-ORE 기법에서는 전체 시스템을 셋업하고 각 사용자들에게 암호화를 위한 비밀키와 서로 다른 사용자의 암호문 비교를 위한 비교키를 발급하기 위한 센터가 존재한다. 이때, 센터는 모든 사용자의 비밀키를 알고 있으므로, 높은 신뢰도가 보장되어야 하며, 센터가 공격 당하는 경우에는 외부로 모든 사용자의 정보가 노출되는 위험이 발생할 수 있다.

[0004] 따라서, 센터의 신뢰도를 낮추면서도 사용자의 비밀 정보의 노출을 방지할 수 있는 방안이 요구된다.

선행기술문헌

특허문헌

[0005] (특허문헌 0001) 대한민국 공개특허공보 제10-2017-0103321호 (2017.09.13. 공개)

발명의 내용

해결하려는 과제

[0006] 본 발명의 실시예들은 다중 클라이언트 환경에서 복호화 과정 없이 서로 다른 비밀키로 암호화된 암호문 간의 비교를 가능하게 하는 순서 노출 암호화를 위한 장치 및 방법을 제공하기 위한 것이다.

과제의 해결 수단

[0007] 본 발명의 일 실시예에 따른 방법은, 하나 이상의 프로세서들 및 상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비한 컴퓨팅 장치에서 수행되는 방법으로서, 제1 사용자의 비밀키를 이용하여 제1 평문을 암호화한 제1 암호문 및 제2 사용자의 비밀키를 이용하여 제2 평문을 암호화한 제2 암호문을 획득하는 단계; 상기 제1 사용자에 의해 이용되는 제1 클라이언트 장치 및 제2 사용자에 의해 이용되는 제2 클라이언트 장치로 상기 제1 사용자의 식별 정보 및 상기 제2 사용자의 식별 정보를 제공하는 단계; 상기 제1 클라이언트 장치로부터 상기 제1 사용자의 식별 정보, 상기 제2 사용자의 식별 정보 및 상기 제1 사용자의 비밀키를 이용하여 생성된 제1 비교키 엘리먼트를 수신하고, 상기 제2 클라이언트 장치로부터 상기 제1 사용자의 식별 정보, 상기 제2 사용자의 식별 정보 및 상기 제2 사용자의 비밀키를 이용하여 생성된 제2 비교키 엘리먼트를 수신하는 단계; 및 상기 제1 비교키 엘리먼트 및 상기 제2 비교키 엘리먼트를 포함하는 비교키를 이용하여 상기 제1 암호문 및 상기 제2 암호문을 암호화된 상태에서 비교하고, 상기 비교 결과에 기초하여 상기 제1

평문 및 상기 제2 평문 사이의 대소를 판단하는 단계를 포함한다.

[0008] 상기 제1 비교키 엘리먼트는, 상기 제1 사용자의 식별 정보 및 상기 제2 사용자의 식별 정보에 대해 해시 함수(hash function)를 적용한 결과 값과 상기 제1 사용자의 비밀키를 이용하여 생성되고, 상기 제2 비교키 엘리먼트는, 상기 제1 사용자의 식별 정보 및 상기 제2 사용자의 식별 정보에 대해 상기 해시 함수를 적용한 결과 값과 상기 제2 사용자의 비밀키를 이용하여 생성될 수 있다.

[0009] 상기 제1 비교키 엘리먼트는, 아래의 수학식 1

[0010] [수학식 1]

$$K_0 = \hat{H}(ID_j \parallel ID_k)^{s_j}$$

[0011]

[0012] (이때, K_0는 상기 제1 비교키 엘리먼트, ID_j는 상기 제1 사용자의 식별 정보, ID_k는 상기 제2 사용자의 식별 정보, s_j는 상기 제1 사용자의 비밀키, $\hat{H}$는 $\hat{H}: \{0,1\}^* \rightarrow \hat{G}$를 만족하는 해시 함수, $\hat{G}$는 위수가 소수 p인 덧셈 군)을 이용하여 생성되고,

[0013] 상기 제2 비교키 엘리먼트는, 아래의 수학식 2

[0014] [수학식 2]

$$K_1 = \hat{H}(ID_j \parallel ID_k)^{s_k}$$

[0015]

[0016] (이때, K_1은 상기 제2 비교키 엘리먼트, s_k는 상기 제2 사용자의 비밀키)를 이용하여 생성될 수 있다.

[0017] 상기 제1 암호문은, 상기 제1 평문의 각 비트 값에 대한 프리픽스(prefix) 비트 열 및 상기 제1 사용자의 비밀키를 이용하여 상기 제1 평문을 비트 단위로 암호화하여 생성되고, 상기 제2 암호문은, 상기 제2 평문의 각 비트 값에 대한 프리픽스 비트 열 및 상기 제2 사용자의 비밀키를 이용하여 상기 제2 평문을 비트 단위로 암호화하여 생성될 수 있다.

[0018] 상기 제1 암호문은, 아래의 수학식 3 내지 5

[0019] [수학식 3]

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

[0020]

[0021] [수학식 4]

$$C_{i,1} = H\left(prefix(m, i-1) \parallel (0x_i + 1)\right)^{s_j}$$

[0022]

[0023] [수학식 5]

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

[0024]

[0025] (이때, CT_j는 상기 1 암호문, m은 $m = x_1 x_2 \cdots x_n \in \{0,1\}^n$인 상기 제1 평문, x_i는 상기 제1 평문의 i 번째 비트 값, $prefix(m, i-1)$는 상기 제1 평문의 i 번째 비트 값에 대한 프리픽스 비트 열, s_j는 상기 제1 사용자의 비밀키, H는 $H: \{0,1\}^* \rightarrow G$를 만족하는 해시 함수, G는 위수가 소수 p인 덧셈 군)을 이용하여 생성되고,

[0026] 상기 제2 암호문은, 아래의 수학식 6 내지 8

[0027] [수학식 6]

[0028] $$C'_{i,0} = H(prefix(m', i-1) \| 0x'_i)^{s_k}$$

[0029] [수학식 7]

[0030] $$C'_{i,1} = H(prefix(m', i-1) \| (0x'_i + 1))^{s_k}$$

[0031] [수학식 8]

[0032] $$CT_k = \left(\{C'_{i,0}, C'_{i,1}\}_{i\in[n]}\right)$$

[0033] (이때, CT_k는 상기 제2 암호문, m'은 $m = x'_1 x'_2 \cdots x'_n \in \{0,1\}^n$인 상기 제2 평문, x'_i는 상기 제2 평문의 $prefix(m', i-1)$ i 번째 비트 값, s_k는 상기 제2 평문의 i 번째 비트 값에 대한 프리픽스 비트 열, s_k는 상기 제2 사용자의 비밀키)을 이용하여 생성될 수 있다.

[0034] 상기 판단하는 단계는, $e(C_{i,0}, K_1)$와 $e(C'_{i,0}, K_0)$ (이때, e는 $e: G \times \hat{G} \rightarrow G_T$를 만족하는 겹선형(bilinear) 함수, $\hat{G}$는 위수가 소수 p인 덧셈 군, G_T는 위수가 소수 p인 곱셈 군, K_0는 상기 제1 비교키 엘리먼트, K_1은 상기 제2 비교키 엘리먼트)가 일치하지 않는 i의 최소 값 i^*가 존재하는지 여부를 판단하는 단계; 및 상기 최소 값 i^*이 존재하고, $e(C_{i^*,1}, K_1)$와 $e(C'_{i^*,0}, K_0)$가 일치하는 경우, 상기 제1 평문이 상기 제2 평문보다 작은 것으로 판단하고, $e(C_{i^*,1}, K_1)$와 $e(C'_{i^*,0}, K_0)$가 일치하지 않거나 상기 최소 값 i^*이 존재하지 않는 경우, 상기 제1 평문이 상기 제2 평문보다 크거나 같은 것으로 판단하는 단계를 포함할 수 있다.

[0035] 본 발명의 일 실시예에 따른 장치는, 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 사용자의 비밀키를 이용하여 제1 평문을 암호화한 제1 암호문 및 제2 사용자의 비밀키를 이용하여 제2 평문을 암호화한 제2 암호문을 획득하는 단계; 상기 제1 사용자에 의해 이용되는 제1 클라이언트 장치 및 제2 사용자에 의해 이용되는 제2 클라이언트 장치로 상기 제1 사용자의 식별 정보 및 상기 제2 사용자의 식별 정보를 제공하는 단계; 상기 제1 클라이언트 장치로부터 상기 제1 사용자의 식별 정보, 상기 제2 사용자의 식별 정보 및 상기 제1 사용자의 비밀키를 이용하여 생성된 제1 비교키 엘리먼트를 수신하고, 상기 제2 클라이언트 장치로부터 상기 제1 사용자의 식별 정보, 상기 제2 사용자의 식별 정보 및 상기 제2 사용자의 비밀키를 이용하여 생성된 제2 비교키 엘리먼트를 수신하는 단계; 및 상기 제1 비교키 엘리먼트 및 상기 제2 비교키 엘리먼트를 포함하는 비교키를 이용하여 상기 제1 암호문 및 상기 제2 암호문을 암호화된 상태에서 비교하고, 상기 비교 결과에 기초하여 상기 제1 평문 및 상기 제2 평문 사이의 대소를 판단하는 단계를 실행하기 위한 명령어들을 포함한다.

[0036] 상기 제1 비교키 엘리먼트는, 상기 제1 사용자의 식별 정보 및 상기 제2 사용자의 식별 정보에 대해 해시 함수(hash function)를 적용한 결과 값과 상기 제1 사용자의 비밀키를 이용하여 생성되고, 상기 제2 비교키 엘리먼트는, 상기 제1 사용자의 식별 정보 및 상기 제2 사용자의 식별 정보에 대해 상기 해시 함수를 적용한 결과 값과 상기 제2 사용자의 비밀키를 이용하여 생성될 수 있다.

[0037] 상기 제1 비교키 엘리먼트는, 아래의 수학식 1

[0038] [수학식 1]

$$K_0 = \hat{H}(ID_j \parallel ID_k)^{s_j}$$

[0039]

[0040] (이때, K_0는 상기 제1 비교키 엘리먼트, ID_j는 상기 제1 사용자의 식별 정보, ID_k는 상기 제2 사용자의 식별 정보, s_j는 상기 제1 사용자의 비밀키, $\hat{H}$는 $\hat{H}: \{0,1\}^* \rightarrow \hat{G}$를 만족하는 해시 함수, $\hat{G}$는 위수가 소수 p인 덧셈 군)을 이용하여 생성되고,

[0041] 상기 제2 비교키 엘리먼트는, 아래의 수학식 2

[0042] [수학식 2]

$$K_1 = \hat{H}(ID_j \parallel ID_k)^{s_k}$$

[0043]

[0044] (이때, K_1은 상기 제2 비교키 엘리먼트, s_k는 상기 제2 사용자의 비밀키)를 이용하여 생성될 수 있다.

[0045] 상기 제1 암호문은, 상기 제1 평문의 각 비트 값에 대한 프리픽스(prefix) 비트 열 및 상기 제1 사용자의 비밀키를 이용하여 상기 제1 평문을 비트 단위로 암호화하여 생성되고, 상기 제2 암호문은, 상기 제2 평문의 각 비트 값에 대한 프리픽스 비트 열 및 상기 제2 사용자의 비밀키를 이용하여 상기 제2 평문을 비트 단위로 암호화하여 생성될 수 있다.

[0046] 상기 제1 암호문은, 아래의 수학식 3 내지 5

[0047] [수학식 3]

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

[0048]

[0049] [수학식 4]

$$C_{i,1} = H\left(prefix(m, i-1) \parallel (0x_i + 1)\right)^{s_j}$$

[0050]

[0051] [수학식 5]

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

[0052]

[0053] (이때, CT_j는 상기 1 암호문, m은 $m = x_1 x_2 \cdots x_n \in \{0,1\}^n$인 상기 제1 평문, x_i는 상기 제1 평문의 i 번째 비트 값, $prefix(m, i-1)$는 상기 제1 평문의 i 번째 비트 값에 대한 프리픽스 비트 열, s_j는 상기 제1 사용자의 비밀키, H는 $H: \{0,1\}^* \rightarrow G$를 만족하는 해시 함수, G는 위수가 소수 p인 덧셈 군)을 이용하여 생성되고,

[0054] 상기 제2 암호문은, 아래의 수학식 6 내지 8

[0055] [수학식 6]

$$C'_{i,0} = H(prefix(m', i-1) \parallel 0x'_i)^{s_k}$$

[0056]

[0057] [수학식 7]

[0058] $$C'_{i,1} = H(prefix(m', i-1) \parallel (0x'_i + 1))^{s_k}$$

[0059] [수학식 8]

[0060] $$CT_k = \left(\{C'_{i,0}, C'_{i,1}\}_{i\in[n]}\right)$$

[0061] (이때, CT_k는 상기 제2 암호문, m'은 $m = x'_1 x'_2 \cdots x'_n \in \{0,1\}^n$인 상기 제2 평문, x'_i는 상기 제2 평문의 $prefix(m', i-1)$ i 번째 비트 값, s_k는 상기 제2 평문의 i 번째 비트 값에 대한 프리픽스 비트 열, k는 상기 제2 사용자의 비밀키)을 이용하여 생성될 수 있다.

[0062] 상기 판단하는 단계는, $e(C_{i,0}, K_1)$와 $e(C'_{i,0}, K_0)$ (이때, e는 $e: G \times \hat{G} \rightarrow G_T$를 만족하는 겹선형(bilinear) 함수, $\hat{G}$는 위수가 소수 p인 덧셈 군, G_T는 위수가 소수 p인 곱셈 군, K_0는 상기 제1 비교키 엘리먼트, K_1은 상기 제2 비교키 엘리먼트)가 일치하지 않는 i의 최소 값 i^*가 존재하는지 여부를 판단하는 단계; 및 상기 최소 값 i^*이 존재하고, $e(C_{i^*,1}, K_1)$와 $e(C'_{i^*,0}, K_0)$가 일치하는 경우, 상기 제1 평문이 상기 제2 평문보다 작은 것으로 판단하고, $e(C_{i^*,1}, K_1)$와 $e(C'_{i^*,0}, K_0)$가 일치하지 않거나 상기 최소 값 i^*이 존재하지 않는 경우, 상기 제1 평문이 상기 제2 평문보다 크거나 같은 것으로 판단하는 단계를 포함할 수 있다.

발명의 효과

[0063] 본 발명의 실시예들에 따르면, 각 사용자가 자신의 비밀 키를 직접 선택하여 암호문을 생성하고, 사용자들 간의 통신을 통해 비교키를 획득 가능하도록 함으로써, 기존 MC-ORE 기법의 센터와 같이 모든 사용자에게 비밀 키를 발급하기 위한 신뢰기관이 요구되지 않으며, 사용자의 비밀 정보의 노출을 방지할 수 있다.

도면의 간단한 설명

[0064] 도 1은 본 발명의 일 실시예에 따른 순서 노출 암호화 시스템의 구성도

도 2는 본 발명의 일 실시예에 따른 순서 노출 암호화 방법을 설명하기 위한 순서도

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

발명을 실시하기 위한 구체적인 내용

[0065] 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.

[0066] 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.

[0067] 도 1은 본 발명의 일 실시예에 따른 순서 노출 암호화 시스템의 구성도이다.

[0068] 도 1을 참조하면, 본 발명의 일 실시예에 따른 순서 노출 암호화 시스템(100)은 셋업(setup) 장치(110), 복수의 클라이언트 장치(120, 130, 140) 및 데이터베이스(150)를 포함한다.

[0069] 도 1에서는 설명의 편의를 위해 클라이언트 장치(110, 120, 130)가 3개인 것으로 예시하고 있으나, 실시예에 따라 클라이언트 장치의 개수는 변경될 수 있다.

[0070] 셋업 장치(110)는 후술할 셋업(setup) 알고리즘을 수행하여 공개 파라미터를 생성하고, 생성된 공개 파라미터를 순서 노출 암호화 시스템(100)을 이용하는 모든 사용자에게 공개한다.

[0071] 제1 클라이언트 장치(120), 제2 클라이언트 장치(130) 및 제3 클라이언트 장치(140)는 암호문 생성 및 암호문 비교를 위해 각 사용자에 의해 이용되는 장치이다. 이하에서는 설명의 편의를 위해 제1 클라이언트 장치(120)는 제1 사용자에 의해 이용되고, 제2 클라이언트 장치(130)는 제2 사용자에 의해 이용되며, 제3 클라이언트 장치(140)는 제3 사용자에 의해 이용되는 것으로 가정하여 설명하나, 실시예에 따라, 하나의 클라이언트 장치(120, 130, 140)가 2 이상의 사용자에 의해 이용될 수도 있다.

[0072] 데이터베이스(150)는 각 클라이언트 장치(120, 130, 140)에 의해 생성된 암호문을 저장하고, 각 클라이언트 장치(120, 130, 140)의 요청에 따라 기 저장된 암호문을 각 클라이언트 장치(120, 130, 140)로 제공할 수 있다.

[0073] 한편, 도 1에 도시된 순서 노출 암호화 시스템(100)에서 수행되는 순서 노출 암호화 기법은 다음과 같은 5개의 알고리즘과 1개의 프로토콜로 구성될 수 있다.

[0074] 셋업(setup) 알고리즘

[0075] 셋업 알고리즘은 보안 상수(Security Parameter) 1^{λ} 및 시스템에 참여할 사용자의 수(ℓ)을 입력받고, 공개 파라미터를 생성한다.

[0076] 구체적으로, 셋업 알고리즘은 각각 위수가 소수 p인 덧셈 군 G 및 $\hat{G}$, 위수가 소수 p인 곱셈 군 G_T, $e: G \times \hat{G} \rightarrow G_T$를 만족하는 겹선형(bilinear) 함수 e, $g \in G$를 만족하는 G의 생성원(generator) g, $\hat{g} \in \hat{G}$를 만족하는 $\hat{G}$의 생성원 $\hat{g}$, 해시 함수(hash function) H 및 $\hat{H}$를 생성하여, 공개 파라미터 $PP = ((p, G, \hat{G}, G_T, e), g, \hat{g}, H, \hat{H})$를 출력할 수 있다. 이때, H 및 $\hat{H}$는 각각 임의의 문자 열을 덧셈 군 G와 $\hat{G}$로 맵핑시키는 해시 함수(hash function)로서 각각 $H: \{0,1\}^* \rightarrow G$와 $\hat{H}: \{0,1\}^* \rightarrow \hat{G}$를 만족할 수 있다.

[0077] 한편, 본 발명의 실시예에서, 셋업 알고리즘은 셋업 장치(110)에 의해 수행될 수 있으며, 셋업 장치(110)는 셋업 알고리즘을 이용하여 생성한 공개 파라미터 PP를 순서 노출 암호화 시스템(100)의 모든 사용자에게 공개할 수 있다.

[0078] 비밀키 생성 알고리즘

[0079] 비밀키 생성 알고리즘은 $s_j \in Z_p$ (이때, j는 $j \in [\ell]$를 만족하는 사용자 인덱스, $Z_p = \{1, 2, \ldots, p-1\}$)를 만족하는 임의의 정수 s_j를 선택하여 사용자의 비밀키 $SK_j = s_j$를 생성한다.

[0080] 한편, 본 발명의 실시예에 있어서, 비밀키 생성 알고리즘은 각 사용자에 의해 이용되는 각 클라이언트 장치(120, 130, 140)에 의해 수행될 수 있다.

[0081] 암호화 알고리즘

[0082] 암호화 알고리즘은 비밀키 생성 알고리즘에 의해 생성된 사용자의 비밀키를 이용하여 평문을 암호화한다.

[0083] 구체적으로, 암호화 알고리즘은 암호화할 평문의 비트 열에 포함된 각 비트 값에 대한 프리픽스 비트 열 및 사용자의 비밀키를 이용하여 평문을 비트 단위로 암호화할 수 있다.

$$m = x_1 x_2 \cdots x_n \in \{0,1\}^n$$

[0084] 보다 구체적으로, 암호화 알고리즘은 평문 에 대해 i(이때, i∈[n])번째 비트마다 $C_{i,0} = H(prefix(m,i-1) \| 0x_i)^{s_j}$ 및 $C_{i,1} = H(prefix(m,i-1) \| (0x_i+1)^{s_j}$ 를 계산하여, 평문 m에 대한 암호문 $CT_j = (\{C_{i,0}, C_{i,1}\}_{i\in[n]})$ 을 생성할 수 있다. 이때, prefix(m, i-1)은 m의 i번째 비트 값(x_i)에 대한 프리픽스 비트 열(즉, prefix(m, i-1) = $x_1x_2\cdots x_{i-1}$)을 나타낸다. 또한, ‖ 는 두 비트 열 사이의 연결(concatenation)을 의미한다.

[0085] 한편, 본 발명의 실시예에 있어서, 암호화 알고리즘은 각 사용자에 의해 이용되는 각 클라이언트 장치(120, 130, 140)에 의해 수행될 수 있다.

[0086] 비교 알고리즘

[0087] 비교 알고리즘은 동일한 사용자의 비밀키를 이용하여 암호화된 암호문 사이의 비교를 수행하여 비교 결과를 출력한다.

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

[0088] 구체적으로, 비교 알고리즘은 사용자 j의 비밀키 s_j를 이용하여 암호화된 두 암호문 $CT'_j = (\{CT'_{i,0}, CT'_{i,1}\}_{i\in[n]})$ 및 을 암호화된 상태로 비교하여, 각 암호문에 대한 평문 사이의 대소를 판단할 수 있다.

[0089] 구체적으로, 비교 알고리즘은 비교 대상인 두 암호문을 최상위 비트(즉, i=1)부터 $C_{i,0}$ 와 $C'_{i,0}$ 를 비교하여, $C_{i,0} \neq C'_{i,0}$ 인 i의 최소 값 i^*가 존재하는지 여부를 판단할 수 있다.

[0090] 만약, i^*가 존재하는 경우, 비교 알고리즘은 $C_{i^*,1}$ 와 $C'_{i^*,0}$ 가 일치하는지 여부를 판단할 수 있다.

[0091] 이때, $C_{i^*,1}$ 와 $C'_{i^*,0}$ 가 일치하는 경우, 비교 알고리즘은 암호문 CT_j 에 대한 평문이 암호문 CT'_j 에 대한 평문보다 작은 것으로 판단할 수 있다.

[0092] 반면, $C_{i^*,1}$ 와 $C'_{i^*,0}$ 가 일치하지 않거나 i^*가 존재하지 않는 경우, 비교 알고리즘은 암호문 CT_j 에 대한 평문이 암호문 CT'_j 에 대한 평문보다 크거나 같은 것으로 판단할 수 있다.

[0093] 한편, 본 발명의 실시예에 있어서, 비교 알고리즘은 각 사용자에 의해 이용되는 각 클라이언트 장치(120, 130, 140)에 의해 수행될 수 있다.

[0094] 비교키 생성 프로토콜

[0095] 각각 상이한 사용자의 비밀키를 이용하여 암호화된 암호문 사이의 비교를 수행하고자 하는 클라이언트 장치(120, 130, 140)는 비교 대상인 각 암호문의 생성을 위해 이용된 사용자의 비밀키를 보유하고 있는 클라이언트 장치(120, 130, 140)와 안전한 채널을 통해 비교키 생성 프로토콜에 따른 정보를 교환하여 비교키를 획득한다.

[0096] 구체적으로, 사용자 j의 비밀키 s_j를 이용하여 암호화된 암호문 CT_j와 사용자 k(이때, k는 $k \in [\ell]$를 만족하는 사용자 인덱스)의 비밀키 s_k를 이용하여 암호화된 암호문 CT_k 사이의 비교를 위해 이용되는 비교키 $CK_{j,k}=(K_0, K_1)$은 다음과 같은 과정을 통해 획득할 수 있다.

[0097] ① 비교키를 요청하는 사용자 t(이때, t는 $t \in [\ell]$를 만족하는 사용자 인덱스)의 클라이언트 장치가 사용자 j의 클라이언트 장치로 사용자 j의 식별 정보 ID_j 및 사용자 k의 식별 정보 ID_k를 전달

[0098] ② 사용자 j의 클라이언트 장치가 ID_j, ID_k 및 사용자 j의 비밀키 s_j를 이용하여 제1 비교키 엘리먼트 K_0를 생성한 후, K_0를 사용자 t의 클라이언트 장치로 전달

[0099] ③ 사용자 t의 클라이언트 장치가 사용자 k의 클라이언트 장치로 ID_j 및 ID_k를 전달

[0100] ④ 사용자 k의 클라이언트 장치가 ID_j, ID_k 및 사용자 k의 비밀키 s_k를 이용하여 제2 비교키 엘리먼트 K_1을 생성한 후, K_1을 사용자 t의 클라이언트 장치로 전달

[0101] 한편, 상술한 비교키 획득 과정에서 사용자 j의 클라이언트 장치 및 사용자 k의 클라이언트 장치는 각각 ID_j 및 ID_k를 이용하여 특정한 군(Group)에 속하는 동일한 원소를 생성할 수 있다. 이후, 사용자 j의 클라이언트 장치는 생성된 원소 및 s_j를 이용하여 제1 비교키 엘리먼트 K_0를 생성하고, 사용자 k의 클라이언트 장치는 생성된 원소 및 s_k를 이용하여 제2 비교키 엘리먼트 K_1를 생성할 수 있다.

[0102] 보다 구체적으로, 사용자 j의 클라이언트 장치는 $\hat{G}$ 에 속하는 원소 $\tilde{H}(ID_j \| ID_k)$ 를 생성한 후, s_j를 이용하여 제1 비교키 엘리먼트 $K_0 = \tilde{H}(ID_j \| ID_k)^{s_j}$ 를 생성할 수 있다.

[0103] 또한, 사용자 j의 클라이언트 장치는 $\hat{G}$ 에 속하는 원소 $\tilde{H}(ID_j \| ID_k)$ 를 생성한 후, s_k를 이용하여 제2 비교키 엘리먼트 $K_1 = \tilde{H}(ID_j \| ID_k)^{s_k}$ 를 생성할 수 있다.

[0104] 다중 클라이언트 비교 알고리즘

[0105] 다중 클라이언트 비교 알고리즘은 각각 상이한 사용자의 비밀키를 이용하여 암호화된 두 암호문 및 두 암호문 사이의 비교를 위한 비교키를 이용하여 두 암호문 사이의 비교를 수행하여 비교 결과를 출력한다.

[0106] 구체적으로, 다중 클라이언트 비교 알고리즘은 사용자 j의 비밀키 s_j를 이용하여 암호화된 암호문 $CT_j = (\{C_{i,0}, C_{i,1}\}_{i \in [n]})$ 과 사용자 k의 비밀키 s_k를 이용하여 암호화된 암호문 $CT_k = (\{C'_{i,0}, C'_{i,1}\}_{i \in [n]})$ 을 비교키 생성 프로토콜을 통해 획득된 비교키 $CK_{j,k}$ 를 이용하여 암호화된 상태로 비교함으로써, 각 암호문에 대한 평문 사이의 대소를 판단할 수 있다.

[0107] 보다 구체적으로, 다중 클라이언트 비교 알고리즘은 비교 대상인 두 암호문 CT_j 및 CT_k의 최상위 비트(즉, i=1)부터 $e(C_{i,0},K_1)$와 $e(C'_{i,0},K_0)$를 비교하여, $e(C_{i,0},K_1) \neq e(C'_{i,0},K_0)$인 i의 최소 값 i^*가 존재하는지 여부를 판단할 수 있다.

[0108] 만약, i^*가 존재하는 경우, 다중 클라이언트 비교 알고리즘은 $e(C_{i^*,1},K_1)$와 $e(C'_{i^*,0},K_0)$가 일치하는지 여부를 판단할 수 있다.

[0109] 이때, $e(C_{i^*,1},K_1)$와 $e(C'_{i^*,0},K_0)$가 일치하는 경우, 다중 클라이언트 비교 알고리즘은 암호문 CT_j에 대한 평문이 암호문 CT_k에 대한 평문보다 작은 것으로 판단할 수 있다.

[0110] 반면, $e(C_{i^*,1},K_1)$와 $e(C'_{i^*,0},K_0)$가 일치하지 않거나 i^*가 존재하지 않는 경우, 다중 클라이언트 비교 알고리즘은 암호문 CT_j에 대한 평문이 암호문 CT_k에 대한 평문보다 크거나 같은 것으로 판단할 수 있다.

[0111] 한편, 본 발명의 실시예에 있어서, 다중 클라이언트 비교 알고리즘은 각 사용자에 의해 이용되는 각 클라이언트 장치(120, 130, 140)에 의해 수행될 수 있다.

[0112] 도 2는 본 발명의 일 실시예에 따른 순서 노출 암호화 방법을 설명하기 위한 순서도이다.

[0113] 도 2에 도시된 방법은 예를 들어, 도 1에 도시된 순서 노출 암호화 시스템(100)에 의하여 수행될 수 있다.

[0114] 도 2를 참조하면, 우선, 셋업 장치(110)는 셋업(set up) 알고리즘을 수행하여 순서 노출 암호화를 위한 공개 파라미터 $PP = ((p,G,\hat{G},G_T,e),g,\hat{g},H,\hat{H})$를 생성하고(201), 생성된 공개 파라미터 PP를 각 사용자에 의해 이용되는 클라이언트 장치(120, 130, 140)로 제공한다(202, 203, 204).

[0115] 이후, 제1 클라이언트 장치(120)는 $s_1 \in Z_p$를 만족하는 제1 사용자의 비밀키 s_1을 생성하고(205), 제2 클라이언트 장치(130)는 $s_2 \in Z_p$를 만족하는 제2 사용자의 비밀키 s_2을 생성한다(206).

[0116] 이후, 제1 클라이언트 장치(120)는 제1 사용자의 비밀키 s_1을 이용하여 평문 m_1에 대한 암호문 CT_1을 생성하고(207), 제2 클라이언트 장치(130)는 제2 사용자의 비밀키 s_2를 이용하여 평문 m_2에 대한 암호문 CT_2를 생성한다(208). 이때, 암호문 CT_1 및 CT_2는 각각 상술한 암호화 알고리즘을 통해 생성될 수 있다.

[0117] 이후, 제1 클라이언트 장치(120) 및 제2 클라이언트 장치(130)는 각각 생성된 암호문 CT_1 및 CT_2를 데이터베이스(150)에 저장한다(209, 210).

[0118] 이후, 제3 클라이언트 장치(140)는 데이터베이스(150)에 저장된 암호문 CT_1 및 CT_2 를 획득하고(211), 제1 클라이언트 장치(120)로 제1 사용자의 식별 정보 ID_1 및 제2 사용자의 식별 정보 ID_2를 제공하여 제1 비교키 엘리먼트 K_0를 요청한다(212).

[0119] 이후, 제1 클라이언트 장치(120)는 제1 사용자의 식별 정보 ID_1, 제2 사용자의 식별 정보ID_2 및 제1 사용자의 비밀키 s_1를 이용하여 제1 비교키 엘리먼트 K_0를 생성하고(213), 생성된 제1 비교키 엘리먼트 K_0를 제3 클라이언트 장치(140)로 제공한다(214).

[0120] 이때, 제1 클라이언트 장치(120)는 $\hat{H}(ID_1 \| ID_2)$ 를 계산한 후, s_1를 이용하여 제1 비교키 엘리먼트 $K_0 = \hat{H}(ID_1 \| ID_2)^{s_1}$ 를 생성할 수 있다.

[0121] 이후, 제3 클라이언트 장치(140)는 제2 클라이언트 장치(130)로 제1 사용자의 식별 정보 ID_1 및 제2 사용자의 식별 정보ID_2를 제공하여 제2 비교키 엘리먼트 K_1를 요청한다(215).

[0122] 이후, 제2 클라이언트 장치(130)는 제1 사용자의 식별 정보 ID_1, 제2 사용자의 식별 정보 ID_2 및 제2 사용자의 비밀키 s_2를 이용하여 제2 비교키 엘리먼트 K_1을 생성하고(216), 생성된 제2 비교키 엘리먼트 K_1을 제3 클라이언트 장치(140)로 제공한다(217).

[0123] 이때, 제2 클라이언트 장치(130)는 $\hat{H}(ID_1 \| ID_2)$ 를 계산한 후, s_2를 이용하여 제2 비교키 엘리먼트 $K_1 = \hat{H}(ID_1 \| ID_2)^{s_2}$ 를 생성할 수 있다.

[0124] 이후, 제3 클라이언트 장치(140)는 비교키 $CK_{1,2} = (K_0, K_1)$ 를 이용하여 암호문 CT_1 및 CT_2 를 암호화된 상태로 비교함으로써, 제1 평문 m_1과 제2 평문 m_2 사이의 대소를 판단한다(218). 이때, 대소 판단은 상술한 다중 클라이언트 비교 알고리즘을 통해 수행될 수 있다.

[0125] 한편, 도 2에 도시된 순서도에서는 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.

[0126] 도 3은 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.

[0127] 도시된 컴퓨팅 환경(10)은 컴퓨팅 장치(12)를 포함한다. 일 실시예에서, 컴퓨팅 장치(12)는 순서 노출 암호화 시스템(100)에 포함되는 하나 이상의 컴포넌트일 수 있다.

[0128] 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.

[0129] 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 자

기 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.

[0130] 통신 버스(18)는 프로세서(14), 컴퓨터 판독 가능 저장 매체(16)를 포함하여 컴퓨팅 장치(12)의 다른 다양한 컴포넌트들을 상호 연결한다.

[0131] 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.

[0132] 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

[0133] 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: 순서 노출 암호화 시스템

110: 셋업 장치

120: 제1 클라이언트 장치

130: 제2 클라이언트 장치

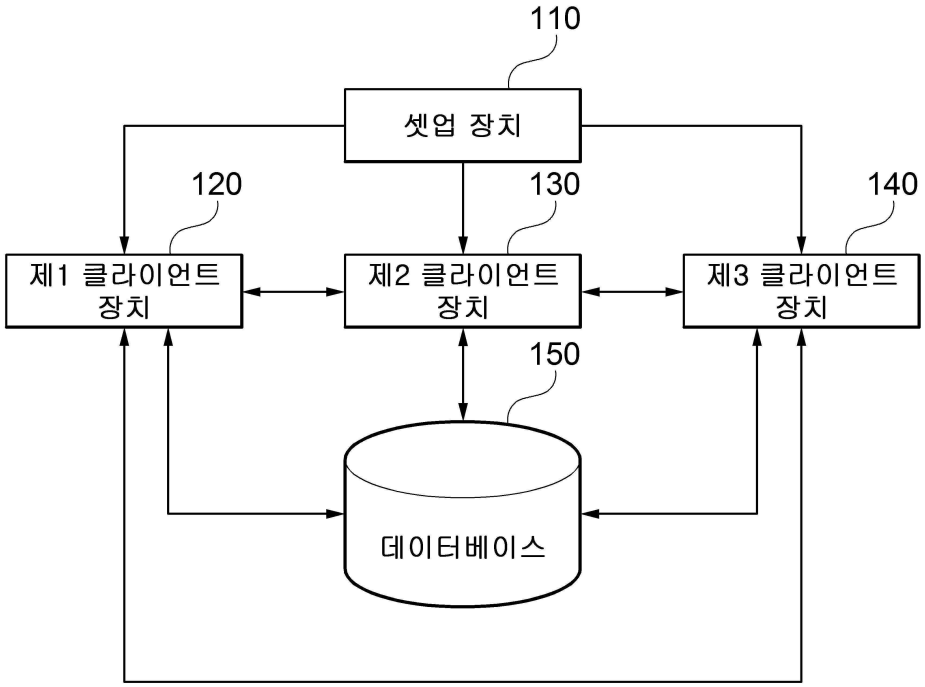
140: 제3 클라이언트 장치

150: 데이터베이스

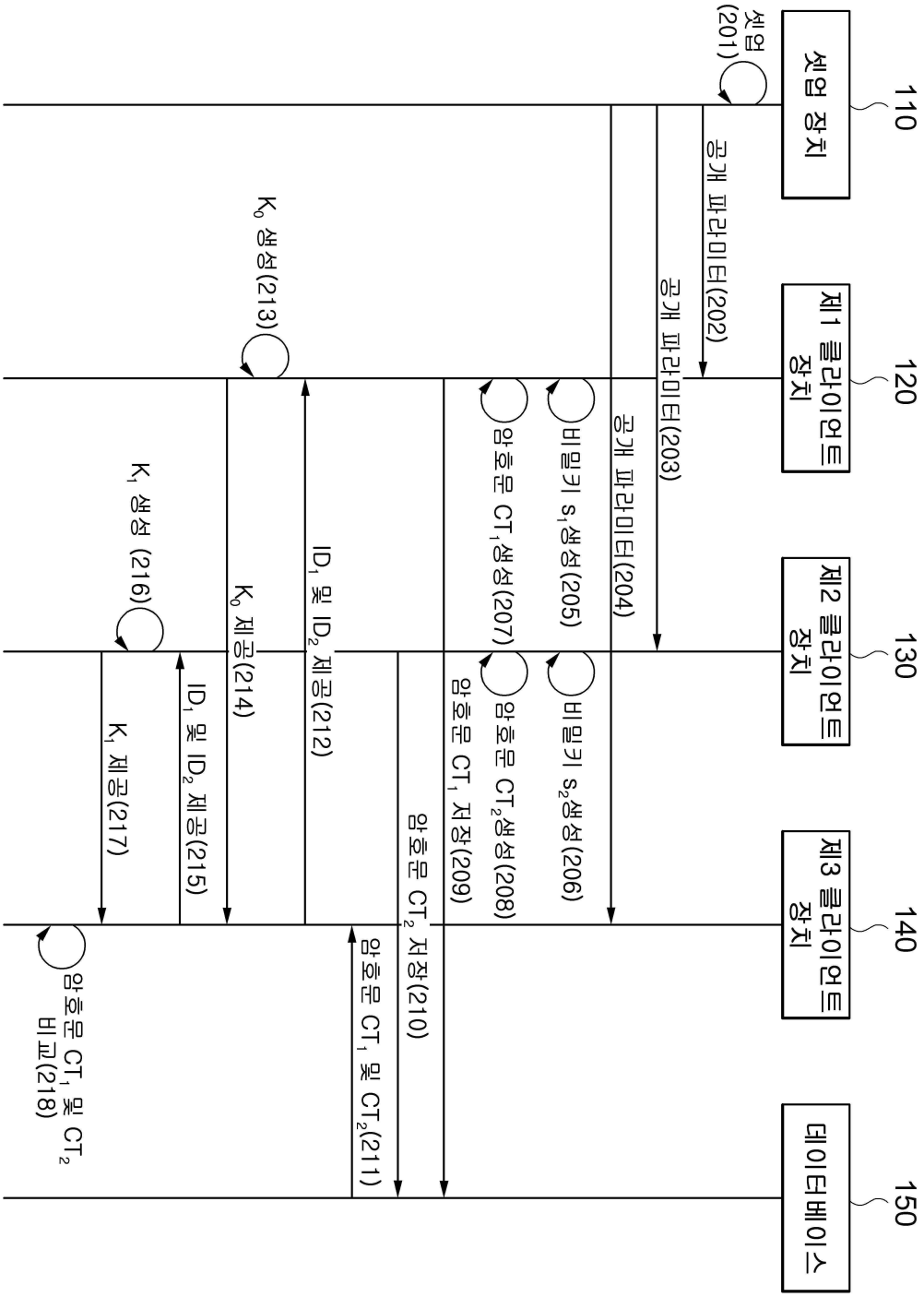
도면

도면1

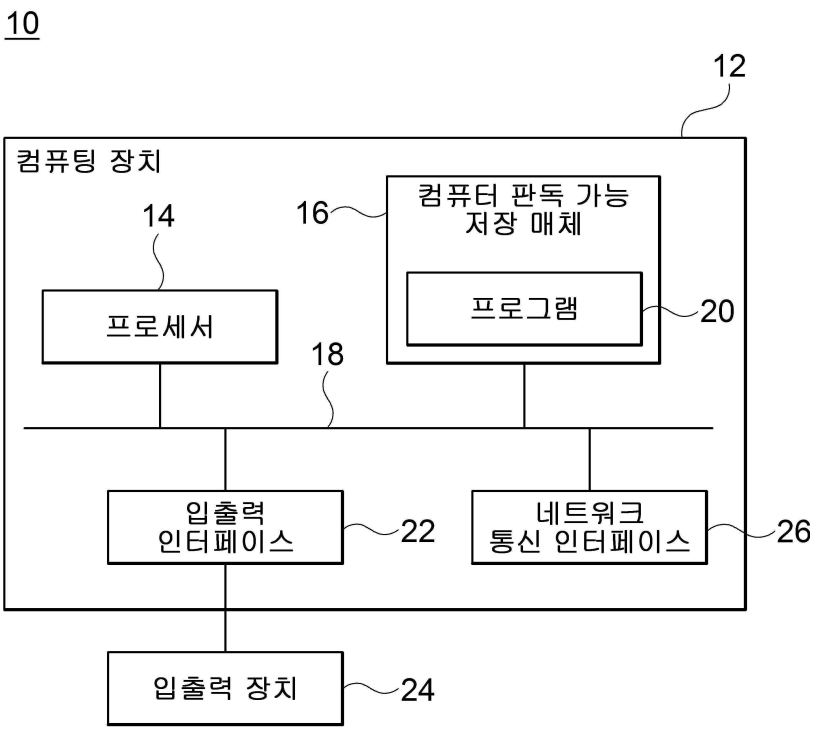
100


110
셋업 장치
120
130
140
제1 클라이언트 장치
제2 클라이언트 장치
제3 클라이언트 장치
150
데이터베이스

도면2


셋업 장치
110
제1 클라이언트 장치
120
제2 클라이언트 장치
130
제3 클라이언트 장치
140
데이터베이스
150
셋업 (201)
공개 파라미터(202)
공개 파라미터(203)
공개 파라미터(204)
비밀키 s_1생성(205)
암호문 CT_1생성(207)
비밀키 s_2생성(206)
암호문 CT_2생성(208)
암호문 CT_1 저장(209)
암호문 CT_2 저장(210)
암호문 CT_1 및 CT_2(211)
K_0 생성(213)
ID_1 및 ID_2 제공(212)
K_0 제공(214)
ID_1 및 ID_2 제공(215)
K_1 생성 (216)
K_1 제공(217)
암호문 CT_1 및 CT_2 비교(218)

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