(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0039979
(43) 공개일자 2020년04월17일

(51) 국제특허분류(Int. Cl.)
G06F 21/60 (2013.01) *H04L 9/06* (2006.01)
H04L 9/08 (2006.01)
(52) CPC특허분류
G06F 21/602 (2013.01)
H04L 9/0618 (2013.01)
(21) 출원번호 10-2018-0119632
(22) 출원일자 2018년10월08일
심사청구일자 2018년10월08일

(71) 출원인
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

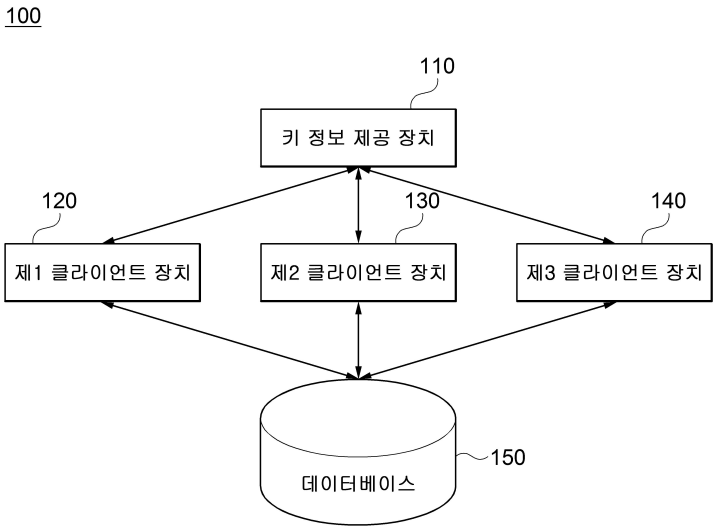
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 **순서 노출 암호화를 위한 장치 및 방법**

(57) 요 약

순서 노출 암호화를 위한 장치 및 방법이 개시된다. 본 발명의 일 실시예에 따른 방법은, 사용자에 대한 사용자 비밀키를 획득하는 단계; 상기 사용자 비밀키를 이용하여 평문 데이터를 비트 단위로 암호화하여 제1 암호문을 생성하는 단계; 및 임의의 정수를 이용하여 상기 제1 암호문을 공개키 암호화 기반으로 암호화하여 제2 암호문을 생성하는 단계를 포함한다.

대 표 도 - 도1



(52) CPC특허분류
H04L 9/0861 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711076035
부처명 과학기술정보통신부
연구관리전문기관 정보통신기술진흥센터
연구사업명 정보보호핵심원천기술개발(정진)
연구과제명 (함수암호 1세부) 함수암호 기법 설계·분석 및 구현기술 연구
기 여 율 1/1
주관기관 상명대학교산학협력단
연구기간 2018.06.01 ~ 2019.03.31

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,

사용자에 대한 사용자 비밀키를 획득하는 단계;

상기 사용자 비밀키를 이용하여 평문 데이터를 비트 단위로 암호화하여 제1 암호문을 생성하는 단계; 및

임의의 정수를 이용하여 상기 제1 암호문을 공개키 암호화 기반으로 암호화하여 제2 암호문을 생성하는 단계를 포함하는, 방법.

청구항 2

청구항 1에 있어서,

상기 제1 암호문을 생성하는 단계는, 상기 평문 데이터의 각 비트 값에 대한 프리픽스(prefix) 비트 열 및 상기 사용자 비밀키를 이용하여 상기 평문 데이터를 비트 단위로 암호화하는, 방법.

청구항 3

청구항 2에 있어서,

상기 제1 암호문은, 아래의 수학식 1 내지 3

[수학식 1]

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

[수학식 2]

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

[수학식 3]

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

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

을 이용하여 생성되는, 방법.

청구항 4

청구항 3에 있어서,

상기 제2 암호문은, 아래의 수학식 4 내지 6

[수학식 4]

$$C_{i,b,0} = F_{i,b} h_j^t$$

[수학식 5]

$$C_{i,b,1} = g^t$$

[수학식 6]

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

CT_j $t \in \{1,2,\cdots,p-1\}$

(이때, 는 상기 제2 암호문, g는 상기 덧셈 군 G의 생성원(generator), t는 를 만

h_j $h_j = g^{a_j}$ a_j $a_j \in \{1,2,\cdots,p-1\}$

족하는 상기 임의의 정수, 는 를 만족하는 공개 파라미터, 는 를 만족하는 임의의 정수)

을 이용하여 생성되는, 방법.

청구항 5

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,

사용자에 대한 사용자 비밀키를 획득하는 단계;

상기 사용자 비밀키를 이용하여 평문 데이터를 비트 단위로 암호화하여 제1 암호문을 생성하는 단계; 및

임의의 정수를 이용하여 상기 제1 암호문을 공개키 암호화 기반으로 암호화하여 제2 암호문을 생성하는 단계를 실행하기 위한 명령어들을 포함하는, 장치.

청구항 6

청구항 5에 있어서,

상기 제1 암호문을 생성하는 단계는, 상기 평문 데이터의 각 비트 값에 대한 프리픽스(prefix) 비트 열 및 상기 사용자 비밀키를 이용하여 상기 평문 데이터를 비트 단위로 암호화하는, 장치.

청구항 7

청구항 6에 있어서,

상기 제1 암호문은, 아래의 수학식 1 내지 3

[수학식 1]

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

[수학식 2]

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

[수학식 3]

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

(F_j 이때, 는 상기 1 암호문, m은 $m = x_1 x_2 \cdots x_n \in \{0,1\}^n$ 인 상기 제1 평문 데이터, x_i 는 상기 제1 평문 데이터의 i 번째 비트 값, $prefix(m, i-1)$ 는 상기 i 번째 비트 값에 대한 프리픽스 비트 열, s_j 는 상기 사용자 비밀키, H는 $H: \{0,1\}^* \rightarrow G$ 를 만족하는 해시 함수, G 는 위수가 소수 p인 덧셈 군)

을 이용하여 생성되는, 장치.

청구항 8

청구항 7에 있어서,

상기 제2 암호문은, 아래의 수학식 4 내지 6

[수학식 4]

$$C_{i,b,0} = F_{i,b} h_j^t$$

[수학식 5]

$$C_{i,b,1} = g^t$$

[수학식 6]

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

(CT_j 이때, 는 상기 제2 암호문, g는 상기 덧셈 군 G의 생성원(generator), t는 $t \in \{1, 2, \cdots, p-1\}$ 를 만족하는 상기 임의의 정수, h_j 는 $h_j = g^{a_j}$ 를 만족하는 공개 파라미터, a_j 는 $a_j \in \{1, 2, \cdots, p-1\}$ 를 만족하는 임의의 정수)

을 이용하여 생성되는, 장치.

청구항 9

하나 이상의 프로세서들, 및

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

제1 사용자 비밀키를 이용하여 제1 평문 데이터를 비트 단위로 암호화한 제1 암호문을 제1 임의의 정수를 이용하여 공개키 암호화 기반으로 암호화한 제2 암호문, 및 제2 사용자 비밀키를 이용하여 제2 평문 데이터를 비트 단위로 암호화한 제3 암호문을 제2 임의의 정수를 이용하여 상기 공개키 암호화 기반으로 암호화한 제4 암호문을 획득하는 단계;

상기 제1 사용자 비밀키 및 상기 제2 사용자 비밀키를 이용하여 생성된 비교키를 획득하는 단계; 및

상기 비교키를 이용하여 제2 암호문 및 상기 제4 암호문을 암호화된 상태에서 비교하여, 상기 제1 평문 데이터와 상기 제2 평문 데이터 사이의 대소를 판단하는 단계를 포함하는, 방법.

청구항 10

청구항 9에 있어서,

상기 제1 암호문은, 상기 제1 평문 데이터의 각 비트 값에 대한 프리픽스(prefix) 비트 열 및 상기 제1 사용자 비밀키를 이용하여 상기 제1 평문 데이터를 비트 단위로 암호화하여 생성되고,

상기 제3 암호문은, 상기 제2 평문 데이터의 각 비트 값에 대한 프리픽스 비트 열 및 상기 제2 사용자 비밀키를 이용하여 상기 제2 평문 데이터를 비트 단위로 암호화하여 생성되는, 방법.

청구항 11

청구항 10에 있어서,

상기 제1 암호문은, 아래의 수학식 1 내지 3

[수학식 1]

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

[수학식 2]

$$F_{i,1} = H\big(prefix(m, i-1) \parallel (0x_i + 1)\big)^{s_l}$$

[수학식 3]

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

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

을 이용하여 생성되고,

상기 제3 암호문은, 아래의 수학식 4 내지 6

[수학식 4]

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

[수학식 5]

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

[수학식 6]

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

(이때, F_k 는 상기 제3 암호문, m'은 $m = x'_1 x'_2 \cdots x'_n \in \{0,1\}^n$ 인 상기 제2 평문 데이터, x'_i 는 상기 제2 평문 데이터의 i 번째 비트 값, $prefix(m', i-1)$ 는 상기 제2 평문 데이터의 i 번째 비트 값에 대한 프리픽스 비트 열, s_k 는 상기 제2 사용자 비밀키)

을 이용하여 생성되는, 방법.

청구항 12

청구항 11에 있어서,

상기 제2 암호문은, 아래의 수학식 7 내지 9

[수학식 7]

$$C_{i,b,0} = F_{i,b} h_l^t$$

[수학식 8]

$$C_{i,b,1} = g^t$$

[수학식 9]

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

(이때, CT_l 는 상기 제2 암호문, g는 상기 덧셈 군 G 의 생성원(generator), t는 $t \in \{1,2,\cdots,p-1\}$ 를 만족하는 상기 제1 임의의 정수, h_l 는 $h_l = g^{a_l}$ 를 만족하는 공개 파라미터, a_l 는 $a_l \in \{1,2,\cdots,p-1\}$ 를 만족하는 임의의 정수)

를 이용하여 생성되고,

상기 제4 암호문은, 아래의 수학식 10 내지 12

[수학식 10]

$$C'_{i,b,0} = F'_{i,b} h_k^{t'}$$

[수학식 11]

$$C'_{i,b,1} = g^{t'}$$

[수학식 12]

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

CT_k $t' \in \{1,2,\cdots,p-1\}$ h_k

(이때, 는 상기 제4 암호문, t'는 를 만족하는 상기 제2 임의의 정수, 는 $h_k = g^{a_k}$ a_k $a_k \in \{1,2,\cdots,p-1\}$ 를 만족하는 공개 파라미터, 는 를 만족하는 임의의 정수)

를 이용하여 생성되는, 방법.

청구항 13

청구항 12에 있어서,

상기 비교키는, 아래의 수학식 13 내지 17

[수학식 13]

$$K_{0,0} = \hat{g}^{rs_l}$$

[수학식 14]

$$K_{0,1} = \hat{h}_k^{rs_l} = (\hat{g}^{a_k})^{rs_l}$$

[수학식 15]

$$K_{1,0} = \hat{g}^{rs_k}$$

[수학식 16]

$$K_{1,1} = \hat{h}_l^{rs_k} = (\hat{g}^{a_l})^{rs_k}$$

[수학식 17]

$$C_{l,k} = \left(\{K_{b,0}, K_{b,1}\}_{b\in\{0,1\}}\right)$$

$C_{l,k}$ $\hat{g}$ $\hat{G}$ $r \in \{1,2,\cdots,p-1\}$

(이때, 는 상기 비교키, 는 위수가 소수 p인 덧셈 군 의 생성원, r은 를 만족하는 임의의 정수)

을 이용하여 생성되는, 방법.

청구항 14

청구항 13에 있어서,

상기 판단하는 단계는,

$e(C_{i,0,0}, K_{1,0})/e(C_{i,0,1}, K_{1,1})$ 와 $e(C'_{i,0,0}, K_{0,0})/e(C'_{i,0,1}, K_{0,1})$ (이때, e는 $e: G \times \hat{G} \rightarrow G_T$ 를 만족하는 겹선형(bilinear) 함수, G_T 는 위수가 소수 p인 곱셈 군)가 일치하지 않는 i의 최소 값 i^*가 존재하는지 여부를 판단하는 단계; 및

상기 최소 값 i^*이 존재하고, $e(C_{i^*,1,0}, K_{1,0})/e(C_{i^*,1,1}, K_{1,1})$ 와 $e(C'_{i^*,0,0}, K_{0,0})/e(C'_{i^*,0,1}, K_{0,1})$ 가 일치하는 경우, 상기 제1 평문 데이터가 상기 제2 평문 데이터보다 작은 것으로 판단하고, $e(C_{i^*,1,0}, K_{1,0})/e(C_{i^*,1,1}, K_{1,1})$ 와 $e(C'_{i^*,0,0}, K_{0,0})/e(C'_{i^*,0,1}, K_{0,1})$ 가 일치하지 않거나 상기 최소 값 i^*이 존재하지 않는 경우, 상기 제1 평문 데이터가 상기 제2 평문 데이터보다 같거나 큰 것으로 판단하고 단계를 포함하는, 방법.

청구항 15

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 사용자 비밀키를 이용하여 제1 평문 데이터를 비트 단위로 암호화한 제1 암호문을 제1 임의의 정수를 이용하여 공개키 암호화 기반으로 암호화한 제2 암호문, 및 제2 사용자 비밀키를 이용하여 제2 평문 데이터를 비트 단위로 암호화한 제3 암호문을 제2 임의의 정수를 이용하여 상기 공개키 암호화 기반으로 암호화한 제4 암호문을 획득하는 단계;

상기 제1 사용자 비밀키 및 상기 제2 사용자 비밀키를 이용하여 생성된 비교키를 획득하는 단계; 및

상기 비교키를 이용하여 제2 암호문 및 상기 제4 암호문을 암호화된 상태에서 비교하여, 상기 제1 평문 데이터와 상기 제2 평문 데이터 사이의 대소를 판단하는 단계를 실행하기 위한 명령어들을 포함하는, 장치.

청구항 16

청구항 15에 있어서,

상기 제1 암호문은, 상기 제1 평문 데이터의 각 비트 값에 대한 프리픽스(prefix) 비트 열 및 상기 제1 사용자 비밀키를 이용하여 상기 제1 평문 데이터를 비트 단위로 암호화하여 생성되고,

상기 제3 암호문은, 상기 제2 평문 데이터의 각 비트 값에 대한 프리픽스 비트 열 및 상기 제2 사용자 비밀키를 이용하여 상기 제2 평문 데이터를 비트 단위로 암호화하여 생성되는, 장치.

청구항 17

청구항 16에 있어서,

상기 제1 암호문은, 아래의 수학식 1 내지 3

[수학식 1]

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

[수학식 2]

$$F_{i,1} = H\big(prefix(m, i-1) \parallel (0x_i + 1)\big)^{s_l}$$

[수학식 3]

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

(F_l 이때, $m = x_1 x_2 \cdots x_n \in \{0,1\}^n$ 는 상기 1 암호문, m은 x_i 인 상기 제1 평문 데이터, 는 상기 제1 평문 $prefix(m, i-1)$ 데이터의 i 번째 비트 값, 는 상기 제1 평문 데이터의 i 번째 비트 값에 대한 프리픽스 비 s_l $H: \{0,1\}^* \rightarrow G$ G 트 열, 는 상기 제1 사용자 비밀키, H는 를 만족하는 해시 함수, 는 위수가 소수 p인 덧셈 군)

을 이용하여 생성되고,

상기 제3 암호문은, 아래의 수학식 4 내지 6

[수학식 4]

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

[수학식 5]

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

[수학식 6]

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

(F_k 이때, $m = x'_1 x'_2 \cdots x'_n \in \{0,1\}^n$ 는 상기 제3 암호문, m'은 x'_i 인 상기 제2 평문 데이터, 는 상기 제2 평문 데이터의 i 번째 비트 값, $prefix(m', i-1)$ 는 상기 제2 평문 데이터의 i 번째 비트 값에 대한 프리픽스 비트 열, s_k 는 상기 제2 사용자 비밀키)

을 이용하여 생성되는, 장치.

청구항 18

청구항 17에 있어서,

상기 제2 암호문은, 아래의 수학식 7 내지 9

[수학식 7]

$$C_{i,b,0} = F_{i,b} h_l^t$$

[수학식 8]

$$C_{i,b,1} = g^t$$

[수학식 9]

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

CT_l G $t \in \{1,2,\cdots,p-1\}$

(이때, 는 상기 제2 암호문, g는 상기 덧셈 군 의 생성원(generator), t는 를 만

h_l $h_l = g^{a_l}$ a_l $a_l \in \{1,2,\cdots,p-1\}$

족하는 상기 제1 임의의 정수, 는 를 만족하는 공개 파라미터, 는 를 만족하는 임의의 정수)

를 이용하여 생성되고,

상기 제4 암호문은, 아래의 수학식 10 내지 12

[수학식 10]

$$C'_{i,b,0} = F'_{i,b} h_k^{t'}$$

[수학식 11]

$$C'_{i,b,1} = g^{t'}$$

[수학식 12]

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

CT_k $t' \in \{1,2,\cdots,p-1\}$ h_k

(이때, 는 상기 제4 암호문, t'는 를 만족하는 상기 제2 임의의 정수, 는

$h_k = g^{a_k}$ a_k $a_k \in \{1,2,\cdots,p-1\}$

를 만족하는 공개 파라미터, 는 를 만족하는 임의의 정수)

를 이용하여 생성되는, 장치.

청구항 19

청구항 18에 있어서,

상기 비교키는, 아래의 수학식 13 내지 17

[수학식 13]

$$K_{0,0} = \hat{g}^{rs_l}$$

[수학식 14]

$$K_{0,1} = \hat{h}_k^{rs_l} = (\hat{g}^{a_k})^{rs_l}$$

[수학식 15]

$$K_{1,0} = \hat{g}^{rs_k}$$

[수학식 16]

$$K_{1,1} = \hat{h}_l^{rs_k} = (\hat{g}^{a_l})^{rs_k}$$

[수학식 17]

$$C_{l,k} = \left(\{K_{b,0}, K_{b,1}\}_{b\in\{0,1\}}\right)$$

$C_{l,k}$ $\hat{g}$ $\hat{G}$ $r \in \{1,2,\cdots,p-1\}$

(이때, 는 상기 비교키, 는 위수가 소수 p인 덧셈 군 의 생성원, r은 를 만족하는 임의의 정수)

을 이용하여 생성되는, 장치.

청구항 20

청구항 19에 있어서,

상기 판단하는 단계는,

$e(C_{i,0,0}, K_{1,0})/e(C_{i,0,1}, K_{1,1})$ $e(C'_{i,0,0}, K_{0,0})/e(C'_{i,0,1}, K_{0,1})$ $e: G \times \hat{G} \rightarrow G_T$

와 (이때, e는 를 만족하는 겹선형(bilinear) 함수, G_T 는 위수가 소수 p인 곱셈 군)가 일치하지 않는 i의 최소 값 i^*가 존재하는지 여부를 판단하는 단계; 및

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

상기 최소 값 i^*이 존재하고, 와 가 일치하는 경우, 상기 제1 평문 데이터가 상기 제2 평문 데이터보다 작은 것으로 판단하고,

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

와 가 일치하지 않거나 상기 최소 값 i^*이 존재하지 않는 경우, 상기 제1 평문 데이터가 상기 제2 평문 데이터보다 같거나 큰 것으로 판단하고 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 수행하기 위한 기법(이하, MC-ORE)을 제시하였다.

[0003] MC-ORE 기법은 메시지를 비트 단위로 암호화하고, 최상위 비트부터 순차적으로 비트 단위의 비교를 수행한다. 따라서, 암호문 비교를 통해 대소 결과 이외에 처음으로 차이가 발생하는 비트 위치(most significant differing bit, MSDB)에 대한 정보가 추가적으로 노출되며, 하나의 암호문으로 동일 사용자의 다른 암호문과의 비교와 서로 다른 사용자의 암호문과의 비교를 모두 수행하므로, 두 비교 결과 모두 MSDB 정보를 노출시킨다는 문제점이 있다.

선행기술문헌

특허문헌

[0004] (특허문헌 0001) 대한민국 공개특허공보 제10-2017-0103321호 (2017.09.13. 공개)

발명의 내용

해결하려는 과제

[0005] 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

[0006] 본 발명의 일 실시예에 따른 방법은, 하나 이상의 프로세서들, 및 상기 하나 이상의 프로세서들에 의해 실행되는 하나 이상의 프로그램들을 저장하는 메모리를 구비한 컴퓨팅 장치에서 수행되며, 사용자에 대한 사용자 비밀키를 획득하는 단계; 상기 사용자 비밀키를 이용하여 평문 데이터를 비트 단위로 암호화하여 제1 암호문을 생성하는 단계; 및 임의의 정수를 이용하여 상기 제1 암호문을 공개키 암호화 기반으로 암호화하여 제2 암호문을 생성하는 단계를 포함한다.

[0007] 상기 제1 암호문을 생성하는 단계는, 상기 평문 데이터의 각 비트 값에 대한 프리픽스(prefix) 비트 열 및 상기 사용자 비밀키를 이용하여 상기 평문 데이터를 비트 단위로 암호화할 수 있다.

[0008] 상기 제1 암호문은, 아래의 수학식 1 내지 3

[0009] [수학식 1]

[0010] $$F_{i,0} = H(prefix(m, i-1) \,\|\, 0x_i)^{s_j}$$

[0011] [수학식 2]

[0012] $$F_{i,1} = H\big(prefix(m, i-1) \,\|\, (0x_i + 1)\big)^{s_j}$$

[0013] [수학식 3]

[0014] $$F_j = \left(\{F_{i,0}, F_{i,1}\}_{i\in[n]}\right)$$

[0015] (이때, F_j는 상기 1 암호문, m은 $m = x_1 x_2 \cdots x_n \in \{0,1\}^n$인 상기 제1 평문 데이터, x_i는 상기 제1 평문 데이터의 i 번째 비트 값, $prefix(m, i-1)$는 상기 i 번째 비트 값에 대한 프리픽스 비트 열, s_j는 상기

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

사용자 비밀키, H는 를 만족하는 해시 함수, 는 위수가 소수 p인 덧셈 군)을 이용하여 생성될 수 있다.

[0016] 상기 제2 암호문은, 아래의 수학식 4 내지 6

[0017] [수학식 4]

[0018] $$C_{i,b,0} = F_{i,b} h_j^t$$

[0019] [수학식 5]

[0020] $$C_{i,b,1} = g^t$$

[0021] [수학식 6]

[0022] $$CT_j = \left(\{C_{i,b,0}, C_{i,b,1}\}_{i\in[n], b\in\{0,1\}}\right)$$

CT_j $t \in \{1,2,\cdots,p-1\}$

[0023] (이때, 는 상기 제2 암호문, g는 상기 덧셈 군 G의 생성원(generator), t는 를 만족하는 상기 임의의 정수, h_j $h_j = g^{a_j}$ a_j $a_j \in \{1,2,\cdots,p-1\}$ 는 를 만족하는 공개 파라미터, 는 를 만족하는 임의의 정수)을 이용하여 생성될 수 있다.

[0024] 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, 사용자에 대한 사용자 비밀키를 획득하는 단계; 상기 사용자 비밀키를 이용하여 평문 데이터를 비트 단위로 암호화하여 제1 암호문을 생성하는 단계; 및 임의의 정수를 이용하여 상기 제1 암호문을 공개키 암호화 기반으로 암호화하여 제2 암호문을 생성하는 단계를 실행하기 위한 명령어들을 포함한다.

[0025] 상기 제1 암호문을 생성하는 단계는, 상기 평문 데이터의 각 비트 값에 대한 프리픽스(prefix) 비트 열 및 상기 사용자 비밀키를 이용하여 상기 평문 데이터를 비트 단위로 암호화할 수 있다.

[0026] 상기 제1 암호문은, 아래의 수학식 1 내지 3

[0027] [수학식 1]

[0028] $$F_{i,0} = H(prefix(m, i-1) \,\|\, 0x_i)^{s_j}$$

[0029] [수학식 2]

[0030] $$F_{i,1} = H\left(prefix(m, i-1) \,\|\, (0x_i + 1)\right)^{s_j}$$

[0031] [수학식 3]

[0032] $$F_j = \left(\{F_{i,0}, F_{i,1}\}_{i\in[n]}\right)$$

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

[0033] (이때, 는 상기 1 암호문, m은 인 상기 제1 평문 데이터, 는 상기 제1 평문 데이터의 i 번째 비트 값, $prefix(m, i-1)$ 는 상기 i 번째 비트 값에 대한 프리픽스 비트 열, s_j 는 상기

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

사용자 비밀키, H는 를 만족하는 해시 함수, 는 위수가 소수 p인 덧셈 군)을 이용하여 생성될 수 있다.

[0034] 상기 제2 암호문은, 아래의 수학식 4 내지 6

[0035] [수학식 4]

[0036] $$C_{i,b,0} = F_{i,b} h_j^t$$

[0037] [수학식 5]

[0038] $$C_{i,b,1} = g^t$$

[0039] [수학식 6]

[0040] $$CT_j = \left(\{C_{i,b,0}, C_{i,b,1}\}_{i\in[n], b\in\{0,1\}}\right)$$

CT_j $t \in \{1,2,\cdots,p-1\}$

[0041] (이때, 는 상기 제2 암호문, g는 상기 덧셈 군 G의 생성원(generator), t는 를 만족하는 상기 임의의 정수, h_j $h_j = g^{a_j}$ a_j $a_j \in \{1,2,\cdots,p-1\}$ 는 를 만족하는 공개 파라미터, 는 를 만족하는 임의의 정수)을 이용하여 생성될 수 있다.

[0042] 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 사용자 비밀키를 이용하여 제1 평문 데이터를 비트 단위로 암호화한 제1 암호문을 제1 임의의 정수를 이용하여 공개키 암호화 기반으로 암호화한 제2 암호문, 및 제2 사용자 비밀키를 이용하여 제2 평문 데이터를 비트 단위로 암호화한 제3 암호문을 제2 임의의 정수를 이용하여 상기 공개키 암호화 기반으로 암호화한 제4 암호문을 획득하는 단계; 상기 제1 사용자 비밀키 및 상기 제2 사용자 비밀키를 이용하여 생성된 비교키를 획득하는 단계; 및 상기 비교키를 이용하여 제2 암호문 및 상기 제4 암호문을 암호화된 상태에서 비교하여, 상기 제1 평문 데이터와 상기 제2 평문 데이터 사이의 대소를 판단하는 단계를 포함한다.

[0043] 상기 제1 암호문은, 상기 제1 평문 데이터의 각 비트 값에 대한 프리픽스(prefix) 비트 열 및 상기 제1 사용자 비밀키를 이용하여 상기 제1 평문 데이터를 비트 단위로 암호화하여 생성되고, 상기 제3 암호문은, 상기 제2 평문 데이터의 각 비트 값에 대한 프리픽스 비트 열 및 상기 제2 사용자 비밀키를 이용하여 상기 제2 평문 데이터를 비트 단위로 암호화하여 생성될 수 있다.

[0044] 상기 제1 암호문은, 아래의 수학식 1 내지 3

[0045] [수학식 1]

[0046] $$F_{i,0} = H(prefix(m, i-1) \,\|\, 0x_i)^{s_l}$$

[0047] [수학식 2]

[0048] $$F_{i,1} = H\left(prefix(m, i-1) \,\|\, (0x_i + 1)\right)^{s_l}$$

[0049] [수학식 3]

[0050] $$F_l = \left(\{F_{i,0}, F_{i,1}\}_{i\in[n]}\right)$$

[0051] (F_l, $m = x_1 x_2 \cdots x_n \in \{0,1\}^n$, x_i) (이때, F_l는 상기 1 암호문, m은 $m = x_1 x_2 \cdots x_n \in \{0,1\}^n$인 상기 제1 평문 데이터, x_i는 상기 제1 평문 데이터의 i 번째 비트 값, $prefix(m, i-1)$는 상기 제1 평문 데이터의 i 번째 비트 값에 대한 프리픽스 비트 열, s_l는 상기 제1 사용자 비밀키, H는 $H: \{0,1\}^* \rightarrow G$를 만족하는 해시 함수, G는 위수가 소수 p인 덧셈 군)을 이용하여 생성되고, 상기 제3 암호문은, 아래의 수학식 4 내지 6

[0052] [수학식 4]

[0053] $$F'_{i,0} = H(prefix(m', i-1) \parallel 0x'_i)^{s_k}$$

[0054] [수학식 5]

[0055] $$F'_{i,1} = H(prefix(m', i-1) \parallel (0x'_i + 1))^{s_k}$$

[0056] [수학식 6]

[0057] $$F_k = \left(\{F'_{i,0}, F'_{i,1}\}_{i \in [n]}\right)$$

[0058] (F_k, $m = x'_1 x'_2 \cdots x'_n \in \{0,1\}^n$, x'_i) (이때, F_k는 상기 제3 암호문, m'은 $m = x'_1 x'_2 \cdots x'_n \in \{0,1\}^n$인 상기 제2 평문 데이터, x'_i는 상기 제2 평문 데이터의 i 번째 비트 값, $prefix(m', i-1)$는 상기 제2 평문 데이터의 i 번째 비트 값에 대한 프리픽스 비트 열, s_k는 상기 제2 사용자 비밀키)을 이용하여 생성될 수 있다.

[0059] 상기 제2 암호문은, 아래의 수학식 7 내지 9

[0060] [수학식 7]

[0061] $$C_{i,b,0} = F_{i,b} h_l^t$$

[0062] [수학식 8]

[0063] $$C_{i,b,1} = g^t$$

[0064] [수학식 9]

[0065] $$CT_l = \left(\{C_{i,b,0}, C_{i,b,1}\}_{i \in [n], b \in \{0,1\}}\right)$$

[0066] (CT_l, G, $t \in \{1,2,\cdots,p-1\}$) (이때, CT_l는 상기 제2 암호문, g는 상기 덧셈 군 G의 생성원(generator), t는 $t \in \{1,2,\cdots,p-1\}$를 만족하는 상기 제1 임의의 정수, h_l는 $h_l = g^{a_l}$를 만족하는 공개 파라미터, a_l는 $a_l \in \{1,2,\cdots,p-1\}$를 만족하는 임의의 정수)를 이용하여 생성되고, 상기 제4 암호문은, 아래의 수학식 10 내지 12

[0067] [수학식 10]

[0068] $$C'_{i,b,0} = F'_{i,b} h_k^{t'}$$

[0069] [수학식 11]

$$C'_{i,b,1} = g^{t'}$$

[0070]

[0071] [수학식 12]

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

[0072]

[0073] (이때, CT_k는 상기 제4 암호문, t'는 $t' \in \{1,2,\cdots,p-1\}$를 만족하는 상기 제2 임의의 정수, h_k는 $h_k = g^{a_k}$를 만족하는 공개 파라미터, a_k는 $a_k \in \{1,2,\cdots,p-1\}$를 만족하는 임의의 정수)를 이용하여 생성될 수 있다.

[0074] 상기 비교키는, 아래의 수학식 13 내지 17

[0075] [수학식 13]

$$K_{0,0} = \hat{g}^{rs_l}$$

[0076]

[0077] [수학식 14]

$$K_{0,1} = \hat{h}_k^{rs_l} = (\hat{g}^{a_k})^{rs_l}$$

[0078]

[0079] [수학식 15]

$$K_{1,0} = \hat{g}^{rs_k}$$

[0080]

[0081] [수학식 16]

$$K_{1,1} = \hat{h}_l^{rs_k} = (\hat{g}^{a_l})^{rs_k}$$

[0082]

[0083] [수학식 17]

$$C_{l,k} = \left(\{K_{b,0}, K_{b,1}\}_{b\in\{0,1\}}\right)$$

[0084]

[0085] (이때, $C_{l,k}$는 상기 비교키, $\hat{g}$는 위수가 소수 p인 덧셈 군 $\hat{G}$의 생성원, r은 $r \in \{1,2,\cdots,p-1\}$를 만족하는 임의의 정수)을 이용하여 생성될 수 있다.

[0086] 상기 판단하는 단계는, $e(C_{i,0,0}, K_{1,0})/e(C_{i,0,1}, K_{1,1})$와 $e(C'_{i,0,0}, K_{0,0})/e(C'_{i,0,1}, K_{0,1})$(이때, e는 $e: G \times \hat{G} \rightarrow G_T$를 만족하는 겹선형(bilinear) 함수, G_T는 위수가 소수 p인 곱셈 군)가 일치하지 않는 i의 최소 값 i^*가 존재하는지 여부를 판단하는 단계; 및 상기 최소 값 i^*이 존재하고, $e(C_{i^*,1,0}, K_{1,0})/e(C_{i^*,1,1}, K_{1,1})$와 $e(C'_{i^*,0,0}, K_{0,0})/e(C'_{i^*,0,1}, K_{0,1})$가 일치하는 경우, 상기 제1 평문 데이터가

$e(C_{i^*,1,0}, K_{1,0})/e(C_{i^*,1,1}, K_{1,1})$

상기 제2 평문 데이터보다 작은 것으로 판단하고, 와 $e(C'_{i^*,0,0}, K_{0,0})/e(C'_{i^*,0,1}, K_{0,1})$ 가 일치하지 않거나 상기 최소 값 i^*이 존재하지 않는 경우, 상기 제1 평문 데이터가 상기 제2 평문 데이터보다 같거나 큰 것으로 판단하고 단계를 포함할 수 있다.

[0087] 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 사용자 비밀키를 이용하여 제1 평문 데이터를 비트 단위로 암호화한 제1 암호문을 제1 임의의 정수를 이용하여 공개키 암호화 기반으로 암호화한 제2 암호문, 및 제2 사용자 비밀키를 이용하여 제2 평문 데이터를 비트 단위로 암호화한 제3 암호문을 제2 임의의 정수를 이용하여 상기 공개키 암호화 기반으로 암호화한 제4 암호문을 획득하는 단계; 상기 제1 사용자 비밀키 및 상기 제2 사용자 비밀키를 이용하여 생성된 비교키를 획득하는 단계; 및 상기 비교키를 이용하여 제2 암호문 및 상기 제4 암호문을 암호화된 상태에서 비교하여, 상기 제1 평문 데이터와 상기 제2 평문 데이터 사이의 대소를 판단하는 단계를 실행하기 위한 명령어들을 포함한다.

[0088] 상기 제1 암호문은, 상기 제1 평문 데이터의 각 비트 값에 대한 프리픽스(prefix) 비트 열 및 상기 제1 사용자 비밀키를 이용하여 상기 제1 평문 데이터를 비트 단위로 암호화하여 생성되고, 상기 제3 암호문은, 상기 제2 평문 데이터의 각 비트 값에 대한 프리픽스 비트 열 및 상기 제2 사용자 비밀키를 이용하여 상기 제2 평문 데이터를 비트 단위로 암호화하여 생성될 수 있다.

[0089] 상기 제1 암호문은, 아래의 수학식 1 내지 3

[0090] [수학식 1]

[0091] $$F_{i,0} = H(prefix(m, i-1) \parallel 0x_i)^{s_l}$$

[0092] [수학식 2]

[0093] $$F_{i,1} = H\big(prefix(m, i-1) \parallel (0x_i + 1)\big)^{s_l}$$

[0094] [수학식 3]

[0095] $$F_l = \left(\{F_{i,0}, F_{i,1}\}_{i\in[n]}\right)$$

[0096] (F_l이때, 는 상기 1 암호문, m은 $m = x_1 x_2 \cdots x_n \in \{0,1\}^n$인 상기 제1 평문 데이터, x_i는 상기 제1 평문 데이터의 i 번째 비트 값, $prefix(m, i-1)$는 상기 제1 평문 데이터의 i 번째 비트 값에 대한 프리픽스 비트 열, s_l는 상기 제1 사용자 비밀키, H는 $H: \{0,1\}^* \to G$를 만족하는 해시 함수, G는 위수가 소수 p인 덧셈 군)을 이용하여 생성되고, 상기 제3 암호문은, 아래의 수학식 4 내지 6

[0097] [수학식 4]

[0098] $$F'_{i,0} = H(prefix(m', i-1) \parallel 0x'_i)^{s_k}$$

[0099] [수학식 5]

[0100] $$F'_{i,1} = H(prefix(m', i-1) \parallel (0x'_i + 1))^{s_k}$$

[0101] [수학식 6]

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

[0102]

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

[0103] (이때, 는 상기 제3 암호문, m'은 인 상기 제2 평문 데이터, 는 상기 제2 평문 데이터의 i 번째 비트 값, $prefix(m', i-1)$ 는 상기 제2 평문 데이터의 i 번째 비트 값에 대한 프리픽스 비트 열, s_k 는 상기 제2 사용자 비밀키)을 이용하여 생성될 수 있다.

[0104] 상기 제2 암호문은, 아래의 수학식 7 내지 9

[0105] [수학식 7]

$$C_{i,b,0} = F_{i,b} h_l^t$$

[0106]

[0107] [수학식 8]

$$C_{i,b,1} = g^t$$

[0108]

[0109] [수학식 9]

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

[0110]

CT_l G $t \in \{1,2,\cdots,p-1\}$

[0111] (이때, 는 상기 제2 암호문, g는 상기 덧셈 군 의 생성원(generator), t는 를 만족하는 상기 제1 임의의 정수, h_l 는 $h_l = g^{a_l}$ 를 만족하는 공개 파라미터, a_l 는 $a_l \in \{1,2,\cdots,p-1\}$ 를 만족하는 임의의 정수)를 이용하여 생성되고, 상기 제4 암호문은, 아래의 수학식 10 내지 12

[0112] [수학식 10]

$$C'_{i,b,0} = F'_{i,b} h_k^{t'}$$

[0113]

[0114] [수학식 11]

$$C'_{i,b,1} = g^{t'}$$

[0115]

[0116] [수학식 12]

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

[0117]

CT_k $t' \in \{1,2,\cdots,p-1\}$ h_k

[0118] (이때, 는 상기 제4 암호문, t'는 를 만족하는 상기 제2 임의의 정수, 는 $h_k = g^{a_k}$ a_k $a_k \in \{1,2,\cdots,p-1\}$ 를 만족하는 공개 파라미터, 는 를 만족하는 임의의 정수)를 이용하여 생성될 수 있다.

[0119] 상기 비교키는, 아래의 수학식 13 내지 17

[0120] [수학식 13]

$$K_{0,0} = \hat{g}^{rs_l}$$

[0121]

[0122] [수학식 14]

$$K_{0,1} = \hat{h}_k^{rs_l} = (\hat{g}^{a_k})^{rs_l}$$

[0123]

[0124] [수학식 15]

$$K_{1,0} = \hat{g}^{rs_k}$$

[0125]

[0126] [수학식 16]

$$K_{1,1} = \hat{h}_l^{rs_k} = (\hat{g}^{a_l})^{rs_k}$$

[0127]

[0128] [수학식 17]

$$C_{l,k} = \left(\{K_{b,0}, K_{b,1}\}_{b\in\{0,1\}}\right)$$

[0129]

$C_{l,k}$ $\hat{g}$ $\hat{G}$ $r \in \{1,2,\cdots,p-1\}$

[0130] (이때, 는 상기 비교키, 는 위수가 소수 p인 덧셈 군 의 생성원, r은 를 만족하는 임의의 정수)을 이용하여 생성될 수 있다.

$e(C_{i,0,0}, K_{1,0})/e(C_{i,0,1}, K_{1,1})$ $e(C'_{i,0,0}, K_{0,0})/e(C'_{i,0,1}, K_{0,1})$

[0131] 상기 판단하는 단계는, 와 (이때, e는 $e: G \times \hat{G} \rightarrow G_T$ G_T 를 만족하는 겹선형(bilinear) 함수, 는 위수가 소수 p인 곱셈 군)가 일치하지 않는 i의 최소 값 i^*가 존재하는지 여부를 판단하는 단계; 및 상기 최소 값 i^*이 존재하고, $e(C_{i^*,1,0}, K_{1,0})/e(C_{i^*,1,1}, K_{1,1})$ $e(C'_{i^*,0,0}, K_{0,0})/e(C'_{i^*,0,1}, K_{0,1})$ 와 가 일치하는 경우, 상기 제1 평문 데이터가 $e(C_{i^*,1,0}, K_{1,0})/e(C_{i^*,1,1}, K_{1,1})$ 상기 제2 평문 데이터보다 작은 것으로 판단하고, 와 $e(C'_{i^*,0,0}, K_{0,0})/e(C'_{i^*,0,1}, K_{0,1})$ 가 일치하지 않거나 상기 최소 값 i^*이 존재하지 않는 경우, 상기 제1 평문 데이터가 상기 제2 평문 데이터보다 같거나 큰 것으로 판단하고 단계를 포함할 수 있다.

발명의 효과

[0132] 본 발명의 실시예들에 따르면, 사용자 비밀키를 이용하여 평문 데이터를 암호화한 암호문을 공개키 암호 기술을 이용하여 추가적으로 암호화함으로써, 동일 사용자에 의해 생성된 암호문 사이의 비교가 불가능하도록 함과 동시에 비교키가 제공되기 전까지 다른 사용자에 의해 생성된 암호문 사이의 비교가 불가능하도록 할 수 있으며, 이에 따라 비교키가 제공되기 전까지 암호문에서 어떠한 정보도 노출되지 않는다.

[0133] 또한, 본 발명의 실시예들에 따르면, 동일한 사용자의 암호문 사이의 비교를 위해 기존의 ORE 기법들 중에서 추가 노출 정보량이 MSDB보다 적은 기법을 사용하고, 다른 사용자의 암호문 사이의 비교를 위해 본 발명의 실시예에 따라 생성된 암호문을 이용하는 경우, 비교키가 제공되기 전까지는 추가 노출 정보량이 기존 ORE 기법의 추가 노출 정보량과 동일하기 때문에 MSDB 보다 적은 양의 정보가 노출되고, 비교키가 제공되더라도 최대 기존의

MC-ORE 기법만큼 추가 정보가 노출되도록 할 수 있다.

도면의 간단한 설명

[0134] 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

[0135] 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.

[0136] 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.

[0137] 도 1은 본 발명의 일 실시예에 따른 순서 노출 암호화 시스템의 구성도이다.

[0138] 도 1을 참조하면, 본 발명의 일 실시예에 따른 순서 노출 암호화 시스템(100)은 키 정보 제공 장치(110) 및 복수의 클라이언트 장치(120, 130, 140)를 포함한다.

[0139] 도 1에서는 설명의 편의를 위해 클라이언트 장치(110, 120, 130)가 3개인 것으로 예시하고 있으나, 실시예에 따라 클라이언트 장치의 개수는 변경될 수 있다.

[0140] 키 정보 제공 장치(110)는 신뢰할 수 있는 기관에 의해 운영되는 장치로서 복수의 사용자에게 평문 데이터 암호화를 위한 사용자 비밀키 및 복수의 사용자 중 서로 다른 사용자에 의해 생성된 암호문 사이의 비교를 위한 비교키를 발급한다.

[0141] 클라이언트 장치(120, 130, 140)는 암호문 생성 및 암호문 비교를 위해 각 사용자에 의해 이용되는 장치이다. 이하에서는 설명의 편의를 위해 각 클라이언트 장치(120, 130, 140)가 상이한 사용자에 의해 이용되는 것으로 가정하여 설명하나, 실시예에 따라, 하나의 클라이언트 장치(120, 130, 140)가 2 이상의 사용자에 의해 이용될 수도 있다.

[0142] 한편, 각 클라이언트 장치(120, 130, 140)는 키 정보 제공 장치(110)로부터 각 클라이언트 장치(120, 130, 140)를 이용하는 사용자에 대한 사용자 비밀키를 발급받을 수 있다. 사용자 비밀키를 발급받은 각 클라이언트 장치(120, 130, 140)는 발급받은 사용자 비밀키를 이용하여 사용자의 평문 데이터를 비트 단위로 암호화한 후, 각 클라이언트 장치(120, 130, 140)에 의해 선택된 임의의 정수를 이용하여 추가 암호화함으로써 암호문을 생성할 수 있다.

[0143] 구체적으로, 각 클라이언트 장치(120, 130, 140)는 평문 데이터의 비트 열 중 각 비트 값에 대한 프리픽스(prefix) 비트 열 및 사용자 비밀키를 이용하여 평문 데이터를 비트 단위로 암호화할 수 있다. 이후, 각 클라이언트 장치(120, 130, 140)는 사용자 비밀키를 이용하여 암호화된 암호문을 임의의 정수를 이용하여 공개키 암호화 기반으로 추가 암호화할 수 있다.

[0144] 한편, 상이한 사용자에 의해 생성된 암호문 사이의 비교를 위해 각 클라이언트 장치(120, 130, 140)는 키 정보 제공 장치(110)로부터 비교키를 발급받을 수 있다. 이후, 각 클라이언트 장치(120, 130, 140)는 상이한 사용자에 의해 생성된 암호문을 발급받은 비교키를 이용하여 암호화된 상태로 비교함으로써 각 암호문에 대한 평문 데

이터 사이의 대소를 판단할 수 있다.

[0145] 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.

[0146] 한편, 도 1에 도시된 순서 노출 암호화 시스템(100)에서 수행되는 순서 노출 암호화 기법의 구체적인 과정은 아래와 같이 구성될 수 있다.

[0147] 셋업(setup)

[0148] 키 정보 제공 장치(110)는 보안 상수(Security Parameter) 1^{λ} 및 시스템에 참여할 수 있는 사용자 수(N)을 입력받고, 공개 파라미터 및 각 사용자에 대한 마스터 비밀키를 생성할 수 있다.

[0149] 구체적으로, 키 정보 제공 장치(110)는 각각 위수가 소수 p인 덧셈 군 G 및 $\hat{G}$, 위수가 소수 p인 곱셈 군 G_T $e: G \times \hat{G} \rightarrow G_T$, $g \in G$를 만족하는 겹선형(bilinear) 함수 e, g를 만족하는 G의 생성원(generator) $\hat{g} \in \hat{G}$, $\hat{G}$의 생성원 $\hat{g}$를 생성할 수 있다.

[0150] 이후, 키 정보 제공 장치(110)는 모든 사용자에 대해 $s_j \in Z_p$(이때, j는 j∈[N]를 만족하는 사용자 인덱스, $Z_p = \{1,2,\ldots,p-1\}$)를 만족하는 임의의 정수 s_j 및 $a_j \in Z_p$를 만족하는 임의의 정수 a_j를 선택하여, $h_j = g^{a_j}$ 및 $\hat{h}_j = \hat{g}^{a_j}$를 생성할 수 있다.

[0151] 이후, 키 정보 제공 장치(110)는 각 사용자에 대한 마스터 비밀키 $MK = \{s_j, \hat{h}_j\}_{j\in[N]}$와 공개 파라미터 $PP = ((p, G, \hat{G}, G_T, e), g, \hat{g}, \{h_j\}_{j\in[N]}, H)$를 출력할 수 있다. 이때, H는 임의의 비트 열을 덧셈 군 G로 맵핑시키는 해시 함수(hash function)로서 $H: \{0,1\}^* \rightarrow G$를 만족한다.

[0152] 한편, 키 정보 제공 장치(110)는 공개 파라미터 PP는 공개하고, 마스터 비밀키 MK는 안전하게 저장할 수 있다.

[0153] 비밀키 발급

[0154] 키 정보 제공 장치(110)는 각 사용자에 의해 이용되는 클라이언트 장치(120, 130, 140)로 각 사용자의 사용자 비밀키 $SK_j = a_j$를 안전하게 발급한다.

[0155] 암호화

[0156] 키 정보 제공 장치(110)로부터 사용자 비밀키 SK_j를 발급받은 각 클라이언트 장치(120, 130, 140)는 사용자 비밀키 SK_j 및 각 클라이언트 장치(120, 130, 140)에 의해 선택된 임의의 정수를 이용하여 평문 데이터를 암호화할 수 있다.

[0157] 구체적으로, 각 클라이언트 장치(120, 130, 140)는 평문 데이터의 비트 열 중 각 비트 값에 대한 프리픽스 비트

SK_j

열 및 사용자 비밀키 를 이용하여 평문 데이터를 비트 단위로 암호화할 수 있다. 보다 구체적으로, 각 클라

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

이언트 장치(120, 130, 140)는 평문 데이터 에 대해 i(이때, i∈[n])번째 비트마다

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

및 를 계산하여, 암호문

$F_j = (\{F_{i,0}, F_{i,1}\}_{i \in [N]})$

을 생성할 수 있다. 이때, prefix(m, i-1)은 m의 i번째 비트 값(x_i)에 대한 프리픽스 비

$\|$

트 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.

$$t \in Z_p$$

[0158] 이후, 각 클라이언트 장치(120, 130, 140)는 를 만족하는 임의의 정수 t를 선택한 후, 선택된 임의의

F_j

정수 t를 이용하여 암호문 를 공개키 암호화 기반으로 암호화할 수 있다. 구체적으로, 각 클라이언트 장치

$F_{i,b}$ $b \in \{0,1\}$ $C_{i,b,0} = F_{i,b} h_j^t$ $C_{i,b,1} = g^t$

(120, 130, 140)는 (이때,)에 대해 와 를 계산하여 암호문

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

를 생성할 수 있다.

[0159] 비교키 생성

$r \in Z_p$

[0160] 키 정보 제공 장치(110)는 를 만족하는 임의의 정수 r을 선택한 후, 사용자 인덱스가 l (즉, j=l)인

s_l s_k

제1 사용자의 사용자 비밀키 및 사용자 인덱스가 k (즉, j=k)인 제2 사용자의 사용자 비밀키 를 이용하

$C_{l,k} = (\{K_{b,0}, K_{b,1}\}_{b \in \{0,1\}})$

여 비교키 를 생성할 수 있다.

$K_{b,0}$

[0161] 이때, 는 아래의 수학식 1 및 2에 의해 생성될 수 있다.

[0162] [수학식 1]

$$K_{0,0} = \hat{g}^{rs_l}$$

[0163]

[0164] [수학식 2]

$$K_{0,1} = \hat{h}_k^{rs_l} = (\hat{g}^{a_k})^{rs_l}$$

[0165]

$K_{b,1}$

[0166] 또한, 는 아래의 수학식 3 및 4에 의해 생성될 수 있다.

[0167] [수학식 3]

$$K_{1,0} = \hat{g}^{rs_k}$$

[0168]

[0169] [수학식 4]

$$K_{1,1} = \hat{h}_l^{rs_k} = (\hat{g}^{a_l})^{rs_k}$$

[0170]

[0171] 한편, 비교키가 생성된 경우, 키 정보 제공 장치(110)는 생성된 비교키 $C_{l,k}$ 를 허가된 사용자에 의해 이용되는 클라이언트 장치(120, 130, 140)로 안전하게 발급할 수 있다.

[0172] 암호문 비교

[0173] 비교키 $C_{l,k}$ 를 발급받은 클라이언트 장치(120, 130, 140)는 비교키 $C_{l,k}$ 를 이용하여 제1 사용자의 암호문 $CT_l = \left(\{C_{i,b,0}, C_{i,b,1}\}_{i\in[N],b\in\{0,1\}}\right)$ 과 제2 사용자의 암호문 $CT_k = \left(\{C'_{i,b,0}, C'_{i,b,1}\}_{i\in[N],b\in\{0,1\}}\right)$ 을 암호화된 상태로 비교함으로써, 각 암호문에 대한 평문 데이터의 대소를 판단할 수 있다.

[0174] 구체적으로, 클라이언트 장치(120, 130, 140)는 각 암호문의 최상위 비트(즉, i=1)부터 $e(C_{i,0,0},K_{1,0})/e(C_{i,0,1},K_{1,1})$ 와 $e(C'_{i,0,0},K_{0,0})/e(C'_{i,0,1},K_{0,1})$ 를 비교하여, $e(C_{i,0,0},K_{1,0})/e(C_{i,0,1},K_{1,1}) \neq e(C'_{i,0,0},K_{0,0})/e(C'_{i,0,1},K_{0,1})$ 인 i의 최소 값 i^*가 존재하는지 여부를 판단할 수 있다.

[0175] 만약, i^*가 존재하는 경우, 클라이언트 장치(120, 130, 140)는 $e(C_{i^*,1,0},K_{1,0})/e(C_{i^*,1,1},K_{1,1})$ 와 $e(C'_{i^*,0,0},K_{0,0})/e(C'_{i^*,0,1},K_{0,1})$ 가 일치하는지 여부를 판단할 수 있다.

[0176] 이때, $e(C_{i^*,1,0},K_{1,0})/e(C_{i^*,1,1},K_{1,1})$ 와 $e(C'_{i^*,0,0},K_{0,0})/e(C'_{i^*,0,1},K_{0,1})$ 가 일치하는 경우, 클라이언트 장치(120, 130, 140)는 암호문 CT_l 에 대한 평문 데이터 m이 암호문 CT_k 에 대한 평문 데이터 m'보다 작은 것으로 판단할 수 있다.

[0177] 반면, $e(C_{i^*,1,0},K_{1,0})/e(C_{i^*,1,1},K_{1,1})$ 와 $e(C'_{i^*,0,0},K_{0,0})/e(C'_{i^*,0,1},K_{0,1})$ 가 일치하지 않거나 i^*가 존재하지 않는 경우, 클라이언트 장치(120, 130, 140)는 m이 m'보다 크거나 같은 것으로 판단할 수 있다.

[0178] 도 2는 본 발명의 일 실시예에 따른 순서 노출 암호화 방법을 설명하기 위한 순서도이다.

[0179] 도 2에 도시된 방법은 예를 들어, 도 1에 도시된 순서 노출 암호화 시스템(100)에 의하여 수행될 수 있다.

[0180] 도 2를 참조하면, 우선 키 정보 생성 장치(110)는 상술한 셋업(set up) 과정을 통해 순서 노출 암호화를 위한 공개 파라미터 및 각 사용자에 대한 마스터 비밀키를 생성한다(201).

[0181] 이후, 키 정보 제공 장치(110)는 제1 클라이언트 장치(120)로 사용자 인덱스가 1인 제1 사용자의 사용자 비밀키

s_l

를 발급한다(202).

s_l

[0182] 비밀키 를 발급받은 제1 클라이언트 장치(120)는 제1 사용자에 의해 생성된 제1 평문 데이터에 대한 암호문 CT_l CT_l CT_l 을 생성한 후(203), 생성된 암호문 을 데이터베이스(150)에 저장한다(204). 이때, 암호문 은 상술한 암호화 과정을 통해 생성될 수 있다.

[0183] 이후, 키 정보 제공 장치(110)는 제2 클라이언트 장치(130)로 사용자 인덱스가 k인 제2 사용자의 사용자 비밀키 s_k 를 발급한다(205).

s_k

[0184] 비밀키 를 발급받은 제2 클라이언트 장치(130)는 제2 사용자에 의해 생성된 제2 평문 데이터에 대한 암호문 CT_k CT_k CT_k 을 생성한 후(206), 생성된 암호문 을 데이터베이스(150)에 저장한다(207). 이때, 암호문 은 상술한 암호화 과정을 통해 생성될 수 있다.

CT_l CT_k

[0185] 이후, 제3 클라이언트 장치(140)는 데이터베이스(150)에 저장된 암호문 및 를 획득하고(208), 키 정보 제공 장치(110)로 암호문 CT_l 및 CT_k 의 비교를 위한 비교키 $C_{l,k}$ 의 발급을 요청한다(209).

$C_{l,k}$ $C_{l,k}$

[0186] 이후, 키 정보 제공 장치(110)는 비교키 를 생성한 후(210), 생성된 비교키 를 제3 클라이언트 장치(140)로 발급한다(211). 이때, 비교키 $C_{l,k}$ 는 상술한 비교키 생성 과정을 통해 생성될 수 있다.

$C_{l,k}$ CT_l CT_k

[0187] 이후, 제3 클라이언트 장치(140)는 비교키 를 이용하여 암호문 CT_l 및 CT_k 를 암호화된 상태로 비교함으로써, 제1 평문 데이터와 제2 평문 데이터 사이의 대소를 판단한다(212). 이때, 대소 판단은 상술한 암호문 비교 과정을 통해 수행될 수 있다.

[0188] 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.

[0189] 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.

[0190] 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 컴포넌트(예를 들어, 키 정보 제공 장치(110), 제1 클라이언트 장치(120), 제2 클라이언트 장치(130), 제3 클라이언트 장치(140))일 수 있다.

[0191] 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 동작

들을 수행하도록 구성될 수 있다.

[0192] 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.

[0193] 통신 버스(18)는 프로세서(14), 컴퓨터 판독 가능 저장 매체(16)를 포함하여 컴퓨팅 장치(12)의 다른 다양한 컴포넌트들을 상호 연결한다.

[0194] 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.

[0195] 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

[0196] 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: 키 정보 제공 장치

120: 제1 클라이언트 장치

130: 제2 클라이언트 장치

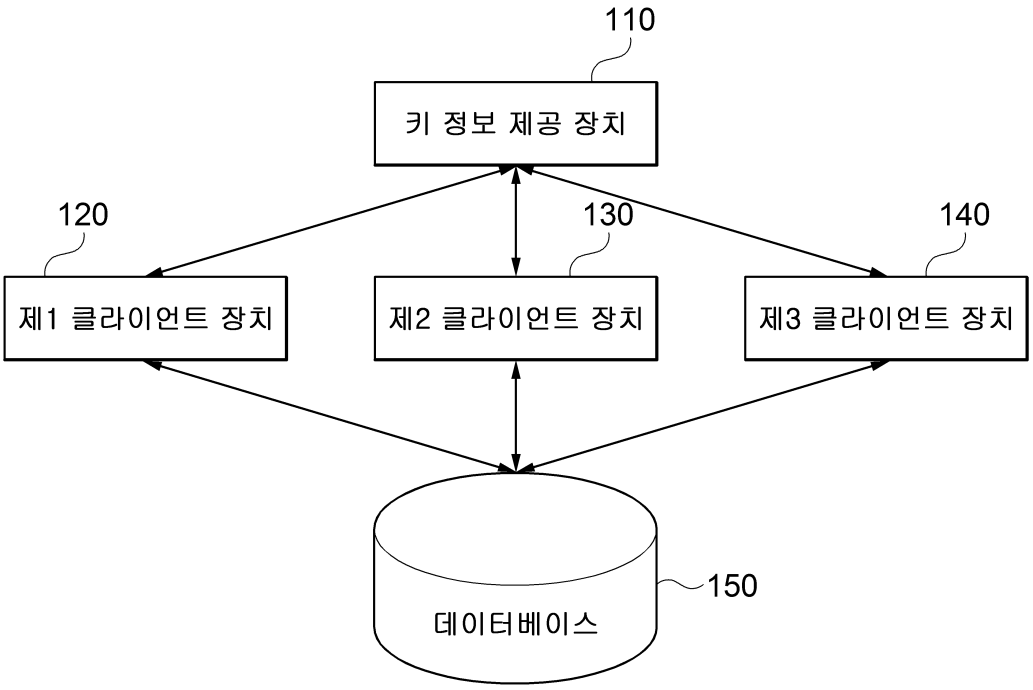
140: 제3 클라이언트 장치

150: 데이터베이스

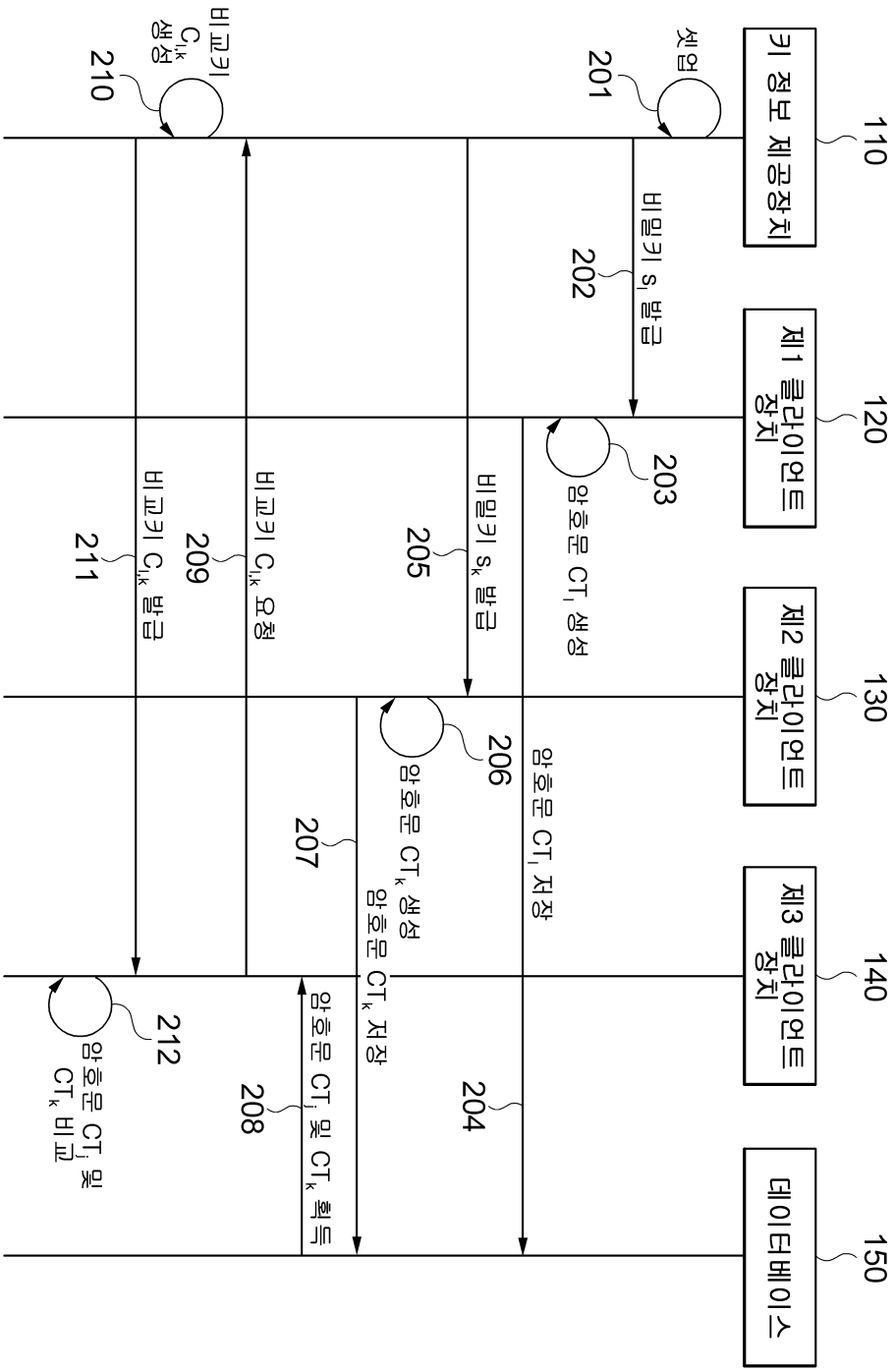
도면

도면1

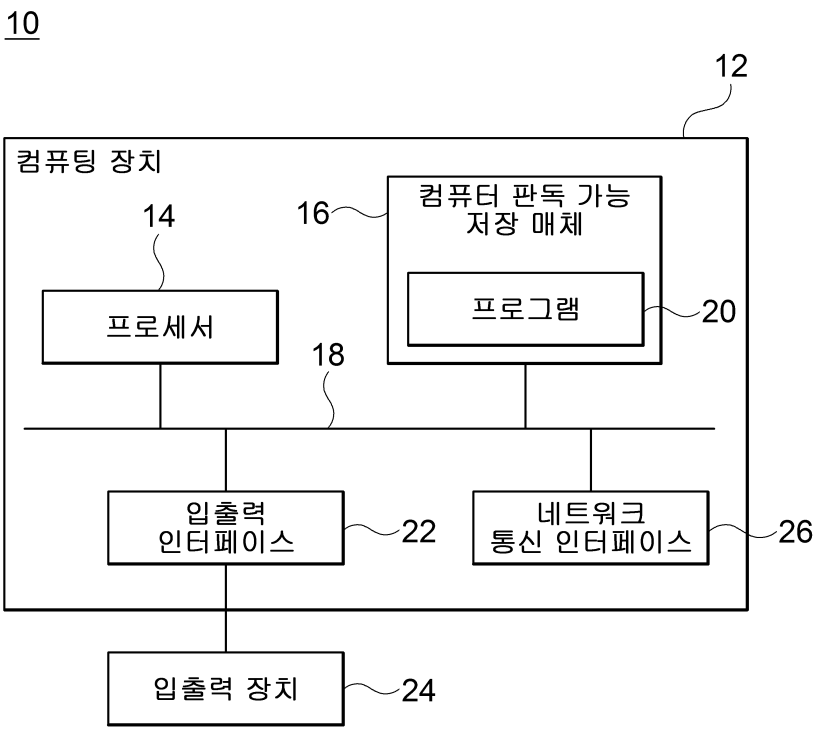
100


110
키 정보 제공 장치
120
130
140
제1 클라이언트 장치
제2 클라이언트 장치
제3 클라이언트 장치
150
데이터베이스

도면2


키 정보 제공장치
110
제1 클라이언트 장치
120
제2 클라이언트 장치
130
제3 클라이언트 장치
140
데이터베이스
150
셋업
201
비밀키 s_i 발급
202
암호문 CT_j 생성
203
비밀키 s_k 발급
205
암호문 CT_j 저장
암호문 CT_k 생성
206
암호문 CT_k 저장
207
비교키 $C_{i,k}$ 요청
209
비교키 $C_{i,k}$ 발급
211
암호문 CT_j 및 CT_k 획득
208
암호문 CT_j 및 CT_k 비교
212
비교키 $C_{i,k}$ 생성
210
204

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