



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0135371
(43) 공개일자 2017년12월08일

(51) 국제특허분류(Int. Cl.)

H04L 9/30 (2006.01)

(52) CPC특허분류

H04L 9/302 (2013.01)

H04L 2209/046 (2013.01)

(21) 출원번호 10-2016-0067173

(22) 출원일자 2016년05월31일

심사청구일자 2016년05월31일

(71) 출원인

고려대학교 산학협력단

서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)

(72) 발명자

홍석희

서울특별시 노원구 덕릉로73길 28, 206동 2304호 (중계동, 양지대림아파트)

김수리

강원도 춘천시 안마산로 214, 208동 1106호(퇴계동, 퇴계금호타운아파트)

(뒷면에 계속)

(74) 대리인

심경식, 홍성욱

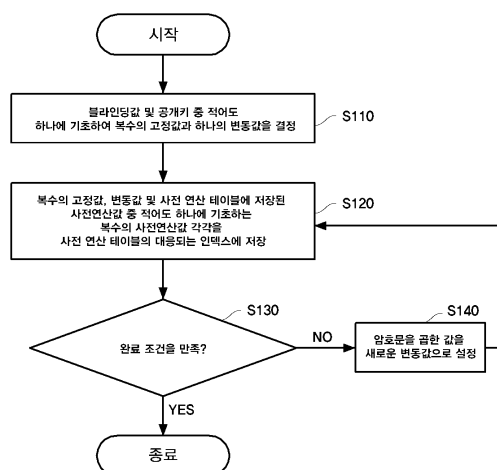
전체 청구항 수 : 총 15 항

(54) 발명의 명칭 RSA 암호시스템의 지수승 연산에 이용되는 사전 연산 테이블 생성 방법 및 그 장치

(57) 요약

RSA 암호시스템의 지수승 연산에 이용되는 사전 연산 테이블 생성 방법을 제공한다. 본 발명의 일 실시예에 따른 RSA 암호시스템의 지수승 연산에 이용되는 사전 연산 테이블 생성 방법은 RSA 암호문을 개인키 지수, 공개키, 랜덤 지수 및 랜덤한 블라인딩값을 기반으로 소정 비트 단위로 지수승 연산하여 복호화할 때 이용되는 사전 연산 테이블을 생성하는 방법에 있어서, 상기 블라인딩값 및 상기 공개키 중 적어도 하나에 기초하여 복수의 고정값과 하나의 변동값을 결정하는 단계; 상기 복수의 고정값, 상기 변동값 및 상기 사전 연산 테이블에 저장된 사전연산값 중 적어도 하나에 기초하는 복수의 사전연산값 각각을 상기 사전 연산 테이블의 대응되는 인덱스에 저장하는 단계; 및 상기 변동값과 상기 암호문을 곱한 값을 새로운 상기 변동값으로 하여, 소정의 완료 조건을 만족할 때까지, 상기 대응되는 인덱스에 저장하는 단계를 반복하여 수행하는 단계를 포함한다.

대표도 - 도1



(52) CPC특허분류

H04L 2209/08 (2013.01)

(72) 발명자

김태원

서울특별시 강동구 고덕로 315, 262동 503호(고덕동, 주공아파트)

김희석

대전광역시 유성구 지족북로66번길 33, 107동 1301호(지족동)

조성민

서울특별시 성북구 화랑로41길 9, 201호

이 발명을 지원한 국가연구개발사업

과제고유번호 NRF2014M3C4A7030649

부처명 미래창조과학부

연구관리전문기관 한국연구재단

연구사업명 차세대정보·컴퓨팅기술개발

연구과제명 암호 소프트웨어 안전성 연구

기 여 율 1/1

주관기관 고려대학교 산학협력단

연구기간 2015.07.01 ~ 2016.06.30

명세서

청구범위

청구항 1

RSA 암호문을 개인키 지수, 공개키, 랜덤 지수 및 랜덤한 블라인딩값을 기반으로 소정 비트 단위로 지수승 연산 하여 복호화할 때 이용되는 사전 연산 테이블을 생성하는 방법에 있어서,

상기 블라인딩값 및 상기 공개키 중 적어도 하나에 기초하여 복수의 고정값과 하나의 변동값을 결정하는 단계;

상기 복수의 고정값, 상기 변동값 및 상기 사전 연산 테이블에 저장된 사전연산값 중 적어도 하나에 기초하는 복수의 상기 사전연산값 각각을 상기 사전 연산 테이블의 대응되는 인덱스에 저장하는 단계; 및

상기 변동값과 상기 암호문을 곱한 값을 새로운 상기 변동값으로 하여, 소정의 완료 조건을 만족할 때까지, 상기 대응되는 인덱스에 저장하는 단계를 반복하여 수행하는 단계

를 포함하는 것을 특징으로 하는 RSA 암호시스템의 지수승 연산에 이용되는 사전 연산 테이블 생성 방법.

청구항 2

제1항에 있어서,

상기 지수승 연산이 w 비트(단, $w > 2$) 단위로 수행될 때,

상기 변동값을 결정하는 단계는 상기 복수의 고정값을 $(K-2)$ 개(단, $K = 2^w$) 결정하고,

상기 대응되는 인덱스에 저장하는 단계는 상기 $(K-2)$ 개의 고정값, 상기 변동값 및 상기 사전 연산 테이블에 저장된 사전연산값 중 적어도 하나에 기초하는 K 개의 상기 사전연산값 각각을 저장하는 것을 특징으로 하는 RSA 암호시스템의 지수승 연산에 이용되는 사전 연산 테이블 생성 방법.

청구항 3

제2항에 있어서,

상기 사전 연산 테이블의 대응되는 인덱스에 저장하는 단계는

상기 $(K-2)$ 개의 고정값 및 상기 변동값에 기초한 $(K-2)$ 개의 상기 사전연산값을 상기 사전 연산 테이블의 대응되는 인덱스에 저장하는 단계; 및

상기 사전 연산 테이블의 최초 2개의 인덱스에 저장되는 상기 사전연산값 및 상기 변동값에 기초한 2개의 상기 사전연산값을 상기 사전 연산 테이블의 대응되는 인덱스에 저장하는 단계

를 포함하는 것을 특징으로 하는 RSA 암호시스템의 지수승 연산에 이용되는 사전 연산 테이블 생성 방법.

청구항 4

제3항에 있어서,

상기 $(K-2)$ 개의 상기 사전연산값을 상기 사전 연산 테이블의 대응되는 인덱스에 저장하는 단계는 상기 $(K-2)$ 개의 고정값 각각과 상기 변동값을 곱한 $(K-2)$ 개의 상기 사전연산값을 저장하고,

상기 2개의 상기 사전연산값을 상기 사전 연산 테이블의 대응되는 인덱스에 저장하는 단계는 상기 사전 연산 테이블의 최초 2개의 인덱스에 저장되는 상기 사전연산값과 상기 변동값을 곱한 2개의 상기 사전연산값을 저장하는 것을 특징으로 하는 RSA 암호시스템의 지수승 연산에 이용되는 사전 연산 테이블 생성 방법.

청구항 5

제2항에 있어서,

상기 소정의 완료 조건은

상기 사전 연산 테이블에 저장된 상기 사전연산값이 총 $K*(2K-1)$ 개가 되는 것을 특징으로 하는 RSA 암호시스템의 지수승 연산에 이용되는 사전 연산 테이블 생성 방법.

청구항 6

제2항에 있어서,

상기 블라인딩값이 R이고, 상기 공개키가 N일 때,

상기 변동값을 결정하는 단계는

상기 (K-2)개의 고정값을 $\{R \bmod N, R^2 \bmod N, \dots, R^{K-2} \bmod N\}$ 으로 결정하는 단계; 및

상기 하나의 변동값을 $\{R^{K-2}\}$ 로 결정하는 단계

를 포함하는 것을 특징으로 하는 RSA 암호시스템의 지수승 연산에 이용되는 사전 연산 테이블 생성 방법.

청구항 7

제1항에 있어서,

상기 블라인딩값은

$R^{\Phi(N)} \equiv 1 \bmod N$ 을 만족하는 것을 특징으로 하는 RSA 암호시스템의 지수승 연산에 이용되는 사전 연산 테이블 생성 방법.

여기서, $R^{\Phi(N)}$ 은 상기 블라인딩값이고, $\Phi(N)$ 은 오일러-파이 함수이고, N은 상기 공개키이다.

청구항 8

제7항에 있어서,

상기 소정 비트 단위의 복호화는 수학적 식 1을 이용하여 수행되는 것을 특징으로 하는 RSA 암호시스템의 지수승 연산에 이용되는 사전 연산 테이블 생성 방법.

[수학적 식 1]

$$C = M^{r'_i} M^{\hat{d}'_i} R^{\Phi'_i} \bmod N$$

여기서, C는 복호화된 메시지이고, M은 상기 암호문이고, $R^{\Phi'_i}$ 은 상기 블라인딩값이고, r'_i 는 상기 랜덤

지수를 소정 비트 단위로 읽은 i번째 값이고, $\hat{d}'_i$ 는 상기 개인키 지수와 상기 랜덤 지수의 차이를 소정 비트

단위로 읽은 i번째 값이고, N은 상기 공개키이고, Φ'_i 는 상기 공개키에 대한 오일러-파이 함수값을 소정 비트 단위로 읽은 i번째 값이다.

청구항 9

제8항에 있어서,

상기 지수승 연산이 w비트(단, $w > 2$) 단위로 수행되어, 상기 r'_i , 상기 $\hat{d}'_i$ 및 상기 Φ'_i 가 각각 0부터 (K-1) (단, $K = 2^w$) 까지 총 K개의 값을 가질 때,

상기 복호화에 이용되는 상기 사전 연산 테이블은 총 $K*(2K-1)$ 개의 값을 가지는 것을 특징으로 하는 RSA 암호시스템의 지수승 연산에 이용되는 사전 연산 테이블 생성 방법.

청구항 10

RSA 암호문을 개인키 지수, 공개키, 랜덤 지수 및 랜덤한 블라인딩값을 기반으로 소정 비트 단위로 지수승 연산 하여 복호화할 때 이용되는 사전 연산 테이블을 생성하는 장치에 있어서,

상기 블라인딩값 및 상기 공개키 중 적어도 하나에 기초하여 복수의 고정값과 하나의 변동값을 결정하는 사전연산부;

상기 복수의 고정값, 상기 변동값 및 상기 사전 연산 테이블에 저장된 사전연산값 중 적어도 하나에 기초하는 복수의 상기 사전연산값을 연산하는 연산부;

상기 사전연산값 각각을 상기 사전 연산 테이블의 대응되는 인덱스에 저장하는 저장부; 및

상기 변동값과 상기 암호문을 곱한 값을 새로운 상기 변동값으로 하여, 소정의 완료 조건을 만족할 때까지, 상기 연산부 및 상기 저장부를 반복적으로 제어하여 상기 사전 연산 테이블을 생성하는 제어부

를 포함하는 것을 특징으로 하는 RSA 암호시스템의 지수승 연산에 이용되는 사전 연산 테이블 생성 장치.

청구항 11

제10항에 있어서,

상기 지수승 연산이 w 비트(단, $w > 2$) 단위로 수행될 때,

상기 사전연산부는 상기 복수의 고정값을 $(K-2)$ 개(단, $K = 2^w$) 결정하고,

상기 연산부는 상기 $(K-2)$ 개의 고정값, 상기 변동값 및 상기 사전 연산 테이블에 저장된 사전연산값 중 적어도 하나에 기초하는 K 개의 상기 사전연산값을 연산하는 것을 특징으로 하는 RSA 암호시스템의 지수승 연산에 이용되는 사전 연산 테이블 생성 장치.

청구항 12

제11항에 있어서,

상기 연산부는

상기 $(K-2)$ 개의 고정값 및 상기 변동값에 기초한 $(K-2)$ 개의 상기 사전연산값을 연산하고,

상기 사전 연산 테이블의 최초 2개의 인덱스에 저장되는 상기 사전연산값 및 상기 변동값에 기초한 2개의 상기 사전연산값을 연산하는 것을 특징으로 하는 RSA 암호시스템의 지수승 연산에 이용되는 사전 연산 테이블 생성 장치.

청구항 13

제12항에 있어서,

상기 $(K-2)$ 개의 사전연산값은 상기 $(K-2)$ 개의 고정값 각각과 상기 변동값을 곱한 $(K-2)$ 개의 값이고,

상기 2개의 사전연산값은 상기 사전 연산 테이블의 최초 2개의 인덱스에 저장되는 상기 사전연산값 각각과 상기 변동값을 곱한 2개의 값인 것을 특징으로 하는 RSA 암호시스템의 지수승 연산에 이용되는 사전 연산 테이블 생성 장치.

청구항 14

제11항에 있어서,

상기 소정의 완료 조건은

상기 사전 연산 테이블에 저장된 상기 사전연산값이 총 $K \cdot (2K-1)$ 개가 되는 것을 특징으로 하는 RSA 암호시스템의 지수승 연산에 이용되는 사전 연산 테이블 생성 장치.

청구항 15

제11항에 있어서,

상기 블라인딩값이 R이고, 상기 공개키가 N일 때,

상기 사전연산부는

상기 (K-2)개의 고정값을 $\{R \bmod N, R^2 \bmod N, \dots, R^{K-2} \bmod N\}$ 으로 결정하고,

상기 하나의 변동값을 $\{R^{K-2}\}$ 로 결정하는 것을 특징으로 하는 RSA 암호시스템의 지수승 연산에 이용되는 사전 연산 테이블 생성 장치.

발명의 설명

기술 분야

[0001] 본 발명은 RSA 암호시스템에서 지수승 연산에 이용되는 사전 연산 테이블을 생성하는 방법 및 그 장치에 관한 것이다.

배경 기술

[0002] RSA 암호시스템은 인수분해의 어려움으로 인해 그 안전성을 보장받고 있다. 즉, 계산을 통해 RSA 암호시스템의 개인키를 알아내기란 사실상 불가능하다. 그에 따라, RSA 암호시스템이 동작할 때 발생하는 전력 소비량을 이용하여 개인키를 복원하려는 시도가 행해지고 있다. 이렇듯 암호시스템이 동작할 때의 발생하는 부가적인 정보를 이용하여 비밀정보를 복원하는 공격을 부채널 공격(side-channel analysis attack)이라 한다. 1999년 Kocher 등이 처음 제안한 이후에 많은 관련연구가 진행되고 있다.

[0003] 이러한 부채널 공격 중에서도 단일 파형에서 동일한 연산에 대한 충돌쌍을 이용하는 공격법이 활발하게 연구되고 있다. 충돌쌍을 이용하는 단일 파형 공격에서 공격자는 곱셈 연산 시 동일한 피연산자를 사용하는 두 곱셈에 대하여 충돌이 발생하는 것을 알 수 있다.

[0004] 특히, 종래의 사전 연산 테이블을 생성하는 기술에서는, 사전 연산 테이블에 이미 포함된 사전연산값이 새로운 사전연산값을 산출하기 위한 곱셈 연산에서 반복적으로 재사용되어, 복호화에 이용되는 사전연산값 및 개인키의 정보가 누출될 가능성이 있어 왔다.

[0005] 따라서, 이와 같은 부채널 공격(특히, 충돌 공격)으로부터 보다 안전한 사전 연산 테이블의 생성 방법 및 장치에 대한 필요성이 대두되고 있다.

[0006] 관련 선행기술로는 한국등록특허 제10-1123729호(발명의 명칭: 역원 연산이 없는 RSA의 메시지 블라인딩 방법, 공개일자: 2012년 2월 28일)가 있다.

발명의 내용

해결하려는 과제

[0007] 본 발명은 RSA 암호시스템의 복호화 과정에서 사전 연산 테이블을 생성할 때, 부채널 공격(특히, 충돌 공격)으로부터 보다 안전한 사전 연산 테이블의 생성 방법 및 장치를 제공하고자 한다.

과제의 해결 수단

[0008] 상기 목적을 달성하기 위해, 본 발명에서 제공하는 RSA 암호시스템의 지수승 연산에 이용되는 사전 연산 테이블 생성 방법은 RSA 암호문을 개인키 지수, 공개키, 랜덤 지수 및 랜덤한 블라인딩값을 기반으로 소정 비트 단위로 지수승 연산하여 복호화할 때 이용되는 사전 연산 테이블을 생성하는 방법에 있어서, 상기 블라인딩값 및 상기 공개키 중 적어도 하나에 기초하여 복수의 고정값과 하나의 변동값을 결정하는 단계; 상기 복수의 고정값, 상기 변동값 및 상기 사전 연산 테이블에 저장된 사전연산값 중 적어도 하나에 기초하는 복수의 상기 사전연산값 각각을 상기 사전 연산 테이블의 대응되는 인덱스에 저장하는 단계; 및 상기 변동값과 상기 암호문을 곱한 값을 새로운 상기 변동값으로 하여, 소정의 완료 조건을 만족할 때까지, 상기 대응되는 인덱스에 저장하는 단계를 반

복하여 수행하는 단계를 포함한다.

[0009] 바람직하게는, 상기 지수승 연산이 w 비트(단, $w > 2$) 단위로 수행될 때, 상기 변동값을 결정하는 단계는 상기 복수의 고정값을 $(K-2)$ 개(단, $K = 2^w$) 결정하고, 상기 대응되는 인덱스에 저장하는 단계는 상기 $(K-2)$ 개의 고정값, 상기 변동값 및 상기 사전 연산 테이블에 저장된 사전연산값 중 적어도 하나에 기초하는 K 개의 상기 사전연산값 각각을 저장할 수 있다.

[0010] 바람직하게는, 상기 사전 연산 테이블의 대응되는 인덱스에 저장하는 단계는 상기 $(K-2)$ 개의 고정값 및 상기 변동값에 기초한 $(K-2)$ 개의 상기 사전연산값을 상기 사전 연산 테이블의 대응되는 인덱스에 저장하는 단계; 및 상기 사전 연산 테이블의 최초 2개의 인덱스에 저장되는 상기 사전연산값 및 상기 변동값에 기초한 2개의 상기 사전연산값을 상기 사전 연산 테이블의 대응되는 인덱스에 저장하는 단계를 포함할 수 있다.

[0011] 바람직하게는, 상기 $(K-2)$ 개의 상기 사전연산값을 상기 사전 연산 테이블의 대응되는 인덱스에 저장하는 단계는 상기 $(K-2)$ 개의 고정값 각각과 상기 변동값을 곱한 $(K-2)$ 개의 상기 사전연산값을 저장하고, 상기 2개의 상기 사전연산값을 상기 사전 연산 테이블의 대응되는 인덱스에 저장하는 단계는 상기 사전 연산 테이블의 최초 2개의 인덱스에 저장되는 상기 사전연산값과 상기 변동값을 곱한 2개의 상기 사전연산값을 저장할 수 있다.

[0012] 바람직하게는, 상기 소정의 완료 조건은 상기 사전 연산 테이블에 저장된 상기 사전연산값이 총 $K*(2K-1)$ 개가 되는 것일 수 있다.

[0013] 바람직하게는, 상기 블라인딩값이 R 이고, 상기 공개키가 N 일 때, 상기 변동값을 결정하는 단계는 상기 $(K-2)$ 개의 고정값을 $\{R \bmod N, R^2 \bmod N, \dots, R^{K-2} \bmod N\}$ 으로 결정하는 단계; 및 상기 하나의 변동값을 $\{R^{K-2}\}$ 로 결정하는 단계를 포함할 수 있다.

[0014] 바람직하게는, 상기 블라인딩값은 $R^{\Phi(N)} \equiv 1 \bmod N$ 을 만족할 수 있다.

[0015] 여기서, $R^{\Phi(N)}$ 은 상기 블라인딩값이고, $\Phi(N)$ 은 오일러-파이 함수이고, N 은 상기 공개키이다.

[0016] 바람직하게는, 상기 소정 비트 단위의 복호화는 수학식 1을 이용하여 수행될 수 있다.

[0017] [수학식 1]

$$C = M^{r'_i} M^{\hat{d}'_i} R^{\Phi'_i} \bmod N$$

[0019] 여기서, C 는 복호화된 메시지이고, M 은 상기 암호문이고, $R^{\Phi'_i}$ 은 상기 블라인딩값이고, r'_i 는 상기 랜덤 지수를 소정 비트 단위로 읽은 i 번째 값이고, $\hat{d}'_i$ 는 상기 개인키 지수와 상기 랜덤 지수의 차이를 소정 비트 단위로 읽은 i 번째 값이고, N 은 상기 공개키이고, Φ'_i 는 상기 공개키에 대한 오일러-파이 함수값을 소정 비트 단위로 읽은 i 번째 값이다.

[0020] 바람직하게는, 상기 지수승 연산이 w 비트(단, $w > 2$) 단위로 수행되어, 상기 r'_i , 상기 $\hat{d}'_i$ 및 상기 Φ'_i 는 각각 0부터 $(K-1)$ (단, $K = 2^w$) 까지 총 K 개의 값을 가질 때, 상기 복호화에 이용되는 상기 사전 연산 테이블은 총 $K*(2K-1)$ 개의 값을 가질 수 있다.

[0021] 또한, 상기 목적을 달성하기 위해, 본 발명에서 제공하는 RSA 암호시스템의 지수승 연산에 이용되는 사전 연산 테이블 생성 장치는 RSA 암호문을 개인키 지수, 공개키, 랜덤 지수 및 랜덤한 블라인딩값을 기반으로 소정 비트 단위로 지수승 연산하여 복호화할 때 이용되는 사전 연산 테이블을 생성하는 장치에 있어서, 상기 블라인딩값 및 상기 공개키 중 적어도 하나에 기초하여 복수의 고정값과 하나의 변동값을 결정하는 사전연산부; 상기 복수의 고정값, 상기 변동값 및 상기 사전 연산 테이블에 저장된 사전연산값 중 적어도 하나에 기초하는 복수의 상기 사전연산값을 연산하는 연산부; 상기 사전연산값 각각을 상기 사전 연산 테이블의 대응되는 인덱스에 저장하

는 저장부; 및 상기 변동값과 상기 암호문을 곱한 값을 새로운 상기 변동값으로 하여, 소정의 완료 조건을 만족할 때까지, 상기 연산부 및 상기 저장부를 반복적으로 제어하여 상기 사전 연산 테이블을 생성하는 제어부를 포함한다.

[0022] 바람직하게는, 상기 지수승 연산이 w 비트(단, $w > 2$) 단위로 수행될 때, 상기 사전연산부는 상기 복수의 고정값을 $(K-2)$ 개(단, $K = 2^w$) 결정하고, 상기 연산부는 상기 $(K-2)$ 개의 고정값, 상기 변동값 및 상기 사전 연산 테이블에 저장된 사전연산값 중 적어도 하나에 기초하는 K 개의 상기 사전연산값을 연산할 수 있다.

[0023] 바람직하게는, 상기 연산부는 상기 $(K-2)$ 개의 고정값 및 상기 변동값에 기초한 $(K-2)$ 개의 상기 사전연산값을 연산하고, 상기 사전 연산 테이블의 최초 2개의 인덱스에 저장되는 상기 사전연산값 및 상기 변동값에 기초한 2개의 상기 사전연산값을 연산할 수 있다.

[0024] 바람직하게는, 상기 $(K-2)$ 개의 사전연산값은 상기 $(K-2)$ 개의 고정값 각각과 상기 변동값을 곱한 $(K-2)$ 개의 값이고, 상기 2개의 사전연산값은 상기 사전 연산 테이블의 최초 2개의 인덱스에 저장되는 상기 사전연산값 각각과 상기 변동값을 곱한 2개의 값일 수 있다.

[0025] 바람직하게는, 상기 소정의 완료 조건은 상기 사전 연산 테이블에 저장된 상기 사전연산값이 총 $K*(2K-1)$ 개가 되는 것일 수 있다.

[0026] 바람직하게는, 상기 블라인딩값이 R 이고, 상기 공개키가 N 일 때, 상기 사전연산부는 상기 $(K-2)$ 개의 고정값을 $\{R \bmod N, R^2 \bmod N, \dots, R^{K-2} \bmod N\}$ 으로 결정하고, 상기 하나의 변동값을 $\{R^{K-2}\}$ 로 결정할 수 있다.

발명의 효과

[0027] 본 발명은 RSA 암호시스템의 복호화 과정에서 사전 연산 테이블을 생성할 때, 사전 연산 테이블에 포함되는 사전연산값이 곱셈 연산에서 재사용되는 경우가 최소화되도록 하여, 부채널 공격(특히, 충돌 공격)을 통해 사전연산값 및 개인키의 정보가 누출될 가능성을 최소화하는 효과가 있다.

도면의 간단한 설명

[0028] 도 1은 본 발명의 일실시예에 따른 RSA 암호시스템의 지수승 연산에 이용되는 사전 연산 테이블 생성 방법을 설명하기 위하여 도시한 흐름도이다.

도 2는 본 발명의 일실시예에 따른 RSA 암호시스템의 지수승 연산에 이용되는 사전 연산 테이블 생성 장치를 설명하기 위하여 도시한 도면이다.

도 3은 본 발명의 일실시예에 따른 사전 연산 테이블 생성 알고리즘을 설명하기 위하여 도시한 의사코드이다.

도 4는 종래 기술의 일실시예에 따른 사전 연산 테이블 생성 알고리즘을 설명하기 위하여 도시한 의사코드이다.

발명을 실시하기 위한 구체적인 내용

[0029] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였다.

[0030] 제1, 제2, A, B 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[0031] 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.

[0032] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가

아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 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.

[0033] 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 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0034] 이하, 본 발명에 따른 바람직한 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0035] 도 1은 본 발명의 실시예에 따른 RSA 암호시스템의 지수승 연산에 이용되는 사전 연산 테이블 생성 방법을 설명하기 위하여 도시한 흐름도이다.

[0036] 사전 연산 테이블은 아래의 수학적 식 1과 같이 RSA 암호문을 개인키 지수, 공개키, 랜덤 지수 및 랜덤한 블라인딩값을 기반으로 소정 비트 단위로 지수승 연산하여 복호화할 때 이용될 수 있다.

[0037] [수학적 식 1]

$$C = M^{r'_i} M^{\hat{d}'_i} R^{\Phi'_i} \bmod N$$

[0039] 여기서, C는 복호화된 메시지이고, M은 RSA 암호문이고, $R^{\Phi'_i}$ 은 블라인딩값이고, r'_i 는 랜덤 지수를 소정 비트 단위로 읽은 i번째 값이고, $\hat{d}'_i$ 는 개인키 지수와 랜덤 지수의 차이를 소정 비트 단위로 읽은 i번째 값이고, N 은 공개키이고, Φ'_i 는 공개키에 대한 오일러-파이 함수값을 소정 비트 단위로 읽은 i번째 값이다.

[0040] 여기서, RSA 암호문을 복호화할 때, DPA(differential power analysis) 공격을 막기 위하여 임의의 블라인딩값을 암호문에 곱하여 연산하는 메시지 블라인딩 기법(message blinding method)이 적용될 수 있다. 또한, SPA(simple power analysis)와 DPA 공격을 막기 위하여 지수승 연산 시 지수를 소정 비트 단위(예, w비트)로 스캔하여 연산하는 윈도우 기법(window method)이 적용될 수 있다. 또한, 공격 복잡도를 보다 높여 안전성을 보장하기 위해 랜덤 지수를 사용하여 개인키 지수(d)를 랜덤 지수(r)와 나머지 지수($\hat{d} = d - r$)인 개인키 지수와 랜덤 지수의 차이로 분할하여 $M^r M^{\hat{d}-r} R^{\Phi(n)} \bmod N$ 의 형태로 지수승 연산을 수행하는 지수 분할 기법(exponent splitting method)이 적용될 수 있다.

[0041] 단계 S110에서는, 사전 연산 테이블 생성 장치가 블라인딩값 및 공개키 중 적어도 하나에 기초하여 복수의 고정값과 하나의 변동값을 결정한다.

[0042] 고정값은 사전연산값의 연산에 이용되는 서로 다른 복수의 값일 수 있으며, 일단 그 값이 결정되면, 더 이상 그 값이 변경되지 않고 계속하여 사전연산값의 연산에 이용될 수 있다. 반면에, 변동값은 사전연산값의 연산에 이용되는 하나의 값이며, 최초에 그 값이 결정되고, 사전연산값의 연산이 수행되면서 그 값이 변경될 수 있다.

[0043] 즉, 사전 연산 테이블 생성 장치가 사전연산값을 연산하기 위한 준비 과정으로, 복수의 고정값과 하나의 변동값을 결정할 수 있다.

[0044] 단계 S120에서는, 사전 연산 테이블 생성 장치가 복수의 고정값, 하나의 변동값 및 사전 연산 테이블에 저장되는 사전연산값 중 적어도 하나에 기초하는 복수의 사전연산값 각각을 사전 연산 테이블의 대응되는 인덱스에 저장한다.

[0045] 예컨대, 사전 연산 테이블 생성 장치가 복수의 고정값과 하나의 변동값을 이용하여 일부의 사전연산값을 연산하여 사전 연산 테이블의 대응되는 인덱스에 저장할 수 있다. 또한, 사전 연산 테이블 생성 장치가 사전 연산 테

이블에 저장되는 사전연산값 중 일부와 하나의 변동값을 이용하여 일부의 사전연산값을 연산하여 사전 연산 테이블의 대응되는 인덱스에 저장할 수 있다.

- [0046] 단계 S130에서는, 사전 연산 테이블 생성 장치가 소정의 완료 조건이 충족되었는지 판단한다.
- [0047] 예컨대, 사전 연산 테이블 생성 장치가, 판단 결과에 따라, 완료 조건이 충족된 경우 사전 연산 테이블의 생성을 완료할 수 있다. 또한, 완료 조건이 충족되지 않은 경우, 단계 S140으로 이동하여 사전 연산 테이블 생성을 계속 진행할 수 있다.
- [0048] 마지막으로 단계 S140에서는, 사전 연산 테이블 생성 장치가 변동값과 암호문을 곱한 값을 새로운 변동값으로 하고, 단계 S120으로 이동하여 사전 연산 테이블 생성을 계속 진행한다.
- [0049] 즉, 사전 연산 테이블 생성 장치가 단계 S130에서 소정의 완료 조건이 충족될 때까지, 단계 S120을 반복하여 수행할 수 있다. 이때, 변동값은 기존의 변동값과 암호문을 곱한 값으로 갱신될 수 있다. 이와 같이, 변동값이 갱신됨으로 인하여, 사전연산값을 연산하는 과정에서 각 사전연산값이 서로 다른 값을 가질 수 있다.
- [0050] 다른 실시예에서는, 사전 연산 테이블 생성 장치가, 지수승 연산이 w 비트(단, $w > 2$) 단위로 수행될 때, 복수의 고정값을 $(K-2)$ 개(단, $K = 2^w$) 결정하고, 그 $(K-2)$ 개의 고정값, 하나의 변동값 및 사전 연산 테이블에 저장된 사전연산값 중 적어도 하나에 기초하는 K 개의 사전연산값 각각을 사전 연산 테이블의 대응되는 인덱스에 저장할 수 있다.
- [0051] 이때, 지수승 연산이 w 비트 단위로 수행된다는 것은, 윈도우 기법에서 윈도우 크기가 w 라는 것을 의미한다. 또한, 이로 인해, 윈도우 크기에 따라 지수승을 w 비트 단위로 읽은 값의 범위가 0에서 $K-1$ (즉, $2^w - 1$)의 사이로 결정될 수 있다.
- [0052] 또 다른 실시예에서는, 사전 연산 테이블 생성 장치가 $(K-2)$ 개의 고정값 및 변동값에 기초한 $(K-2)$ 개의 사전연산값을 사전 연산 테이블의 대응되는 인덱스에 저장하고, 사전 연산 테이블의 최초 2개의 인덱스에 저장되는 사전연산값 및 변동값에 기초한 2개의 사전연산값을 사전 연산 테이블의 대응되는 인덱스에 저장할 수 있다.
- [0053] 즉, 사전 연산 테이블 생성 장치가 $(K-2)$ 개의 고정값 및 변동값에 기초하여 $(K-2)$ 개의 사전연산값을 연산하고, 사전 연산 테이블의 최초 2개의 인덱스에 저장되는 사전연산값 및 변동값에 기초하여 2개의 사전연산값을 연산할 수 있다.
- [0054] 이와 같이, 사전연산값을 나누어서 연산하는 이유는 지수승 연산에서 사용되는 사전연산값의 개수가 변동값의 개수보다 2개 더 많기 때문일 수 있다. 보다 구체적으로, $w=5$ (즉, $K=32$)인 경우에, 사전 연산 테이블 생성 장치가 30개의 사전연산값과 2개의 사전연산값으로 나누어 연산하는 것은, 결정된 변동값이 30개이기 때문일 수 있다.
- [0055] 또한, 예컨대, 사전 연산 테이블의 인덱스는 0에서부터 시작할 수 있으며, 하나의 사전연산값이 사전 연산 테이블에 저장될 때마다, 인덱스가 1씩 증가할 수 있다.
- [0056] 또 다른 실시예에서는, 사전 연산 테이블 생성 장치가 $(K-2)$ 개의 고정값 각각과 하나의 변동값을 곱한 $(K-2)$ 개의 사전연산값과 사전 연산 테이블의 최초 2개의 인덱스에 저장되는 사전연산값과 하나의 변동값을 곱한 2개의 사전연산값을 사전 연산 테이블의 대응되는 인덱스에 저장할 수 있다.
- [0057] 예컨대, 고정값이 $\{T_1, T_2, T_3, \dots, T_{K-2}\}$ 이고, 변동값이 T 인 경우에, $(K-2)$ 개의 사전연산값은 $\{T_1 * T, T_2 * T, T_3 * T, \dots, T_{K-2} * T\}$ 이 될 수 있다. 또한, 사전 연산 테이블의 최초 2개의 인덱스에 저장되는 사전연산값이 $\{S_1, S_2\}$ 인 경우에, 2개의 사전연산값은 $\{S_1 * T, S_2 * T\}$ 이 될 수 있다.
- [0058] 이때, $\{T_1 * T, T_2 * T, T_3 * T, \dots, T_{K-2} * T\}$ 의 사전연산값은 이전에 연산된 사전연산값이 재사용되지 않고, 고정값과 변동값만을 이용하여 연산되고 있으므로, 부채널 공격으로부터 상대적으로 더 안전할 수 있다. 반면에, $\{S_1 * T, S_2 * T\}$ 의 사전연산값은 연산과정에서 이전에 연산된 $\{S_1, S_2\}$ 의 사전연산값이 이용되므로, 그 2개의 사전연산값은 부채널 공격으로부터 상대적으로 더 위험할 수 있다.
- [0059] 또 다른 실시예에서는, 소정의 완료 조건은 사전 연산 테이블에 저장된 사전연산값이 총 $K*(2K-1)$ 개가 되는 것일 수 있다.

- [0060] 예컨대, 사전 연산 테이블 생성 장치가 사전 연산 테이블에 저장된 사전연산값의 개수가 총 $K*(2K-1)$ 개가 되면, 사전 연산 테이블이 완성된 것으로 간주하여 사전 연산 테이블의 생성 과정을 종료할 수 있다.
- [0061] 한편, 사전연산값의 개수가 $K*(2K-1)$ 개일 때, 사전 연산 테이블이 완성된 것으로 볼 수 있는 이유에 대하여는 아래의 내용에서 구체적으로 후술한다.
- [0062] 또 다른 실시예에서는, 사전 연산 테이블 생성 장치가, 블라인딩값이 R 이고, 공개키가 N 일 때, $(K-2)$ 개의 고정값을 $\{R \bmod N, R^2 \bmod N, \dots, R^{K-2} \bmod N\}$ 으로 결정하고, 하나의 변동값을 $\{R^{K-2}\}$ 로 결정할 수 있다.
- [0063] 예컨대, 사전 연산 테이블 생성 장치가 랜덤한 블라인딩값 R 에 대하여, $(K-2)$ 개의 고정값을 $\{R, R^2, \dots, R^{K-2}\}$ 을 공개키 N 으로 mod 연산한 $\{R \bmod N, R^2 \bmod N, \dots, R^{K-2} \bmod N\}$ 으로 결정할 수 있다. 또한, 변동값을 $\{R^{K-2}\}$ 로 결정할 수 있다.
- [0064] 또 다른 실시예에서는, 블라인딩값은 $R^{\Phi(N)} \equiv 1 \bmod N$ 을 만족할 수 있다. $R^{\Phi(N)}$ 은 블라인딩값이고, $\Phi(N)$ 은 오일러-파이 함수이고, N 은 공개키이다.
- [0065] 여기서, 오일러-파이 함수가 임의의 정수 A 에 대하여 $A^{\Phi(N)} \equiv 1 \bmod N$ 을 만족하는 성질을 이용하면, 지수승의 최종 연산값이 $M R^{\Phi(N)} \bmod N$ 의 형태이고, $R^{\Phi(N)} \equiv 1 \bmod N$ 이므로, R 의 역원 연산을 수행할 필요가 없어 보다 효율적일 수 있다
- [0066] 또 다른 실시예에서는, 지수승 연산이 w 비트(단, $w > 2$) 단위로 수행되어, r'_i , $\widehat{d'_i}$ 및 Φ'_i 가 각각 0부터 $(K-1)$ (단, $K = 2^w$) 까지 총 K 개의 값을 가질 때, 수학식 1의 복호화에 이용되는 사전 연산 테이블은 총 $K*(2K-1)$ 개의 값을 가질 수 있다.
- [0067] 다시 말하면, 수학식 1에서, C 의 지수인 $r'_i + \widehat{d'_i}$ 는 0부터 $(2K-2)$ 까지 총 $(2K-1)$ 개의 값을 가질 수 있고, Φ'_i 는 0부터 $(K-1)$ 까지 총 K 개의 값을 가질 수 있으므로, C 의 지수와 R 의 지수가 가질 수 있는 값의 조합의 총 개수는 $K*(2K-1)$ 일 수 있다. 그리고, 이 총 개수가 사전 연산 테이블에 저장된 사전연산값의 개수일 수 있다.
- [0068] 보다 구체적으로, 윈도우 크기가 $w=3$ (즉, $K=8$)인 경우에, 사전 연산 테이블에 저장되는 사전연산값의 총 개수는 $8*(2*8-1)=120$ 개일 수 있다. 그 총 120개의 사전연산값 중에서 사전 연산 테이블의 최초 2개의 인덱스에 저장되는 사전연산값은 연산 과정에서 재사용되므로 부채널 공격으로부터 상대적으로 더 위험할 수 있으며, 나머지 118개는 연산 과정에서 재사용되지 않으므로 부채널 공격으로부터 상대적으로 더 안전할 수 있다.
- [0069] 이와 같이, 본 발명의 일실시예에 따른 RSA 암호시스템의 지수승 연산에 이용되는 사전 연산 테이블 생성 방법은, 사전 연산 테이블을 생성하는 과정에서 이미 저장된 사전연산값을 재사용하는 경우를 최소화함으로써 부채널 공격(특히, 충돌 공격(collision-based power analysis attack))으로부터 보다 안전하게 사전 연산 테이블을 생성할 수 있게 되는 효과가 있다.
- [0070] 도 3을 참조하면, 본 발명의 일실시예에 따른 사전 연산 테이블 생성 알고리즘을 설명하기 위한 의사코드이다.
- [0071] 4.1에서는 블라인딩값(R)을 공개키(n)로 mod 연산하여 복수의 고정값(T)을 결정한다.
- [0072] 4.2에서는 블라인딩값(R)에 기초하여 하나의 변동값(T')을 결정한다.
- [0073] 4.3에서는 사전연산값(S)을 연산한다.
- [0074] 4.3.1에서는 고정값(T)과 변동값(T')을 곱셈하여 사전연산값(S)을 연산한다.
- [0075] 4.3.2 및 4.3.3에서는 사전 연산 테이블에 저장된 최초 2개 인덱스의 사전연산값(S_v, S_{v+1})과 변동값(T')을 곱셈하여 사전연산값(S)을 연산한다.
- [0076] 4.3.4에서는 변동값(T')을 암호문(M)과 곱셈하여 갱신한다.

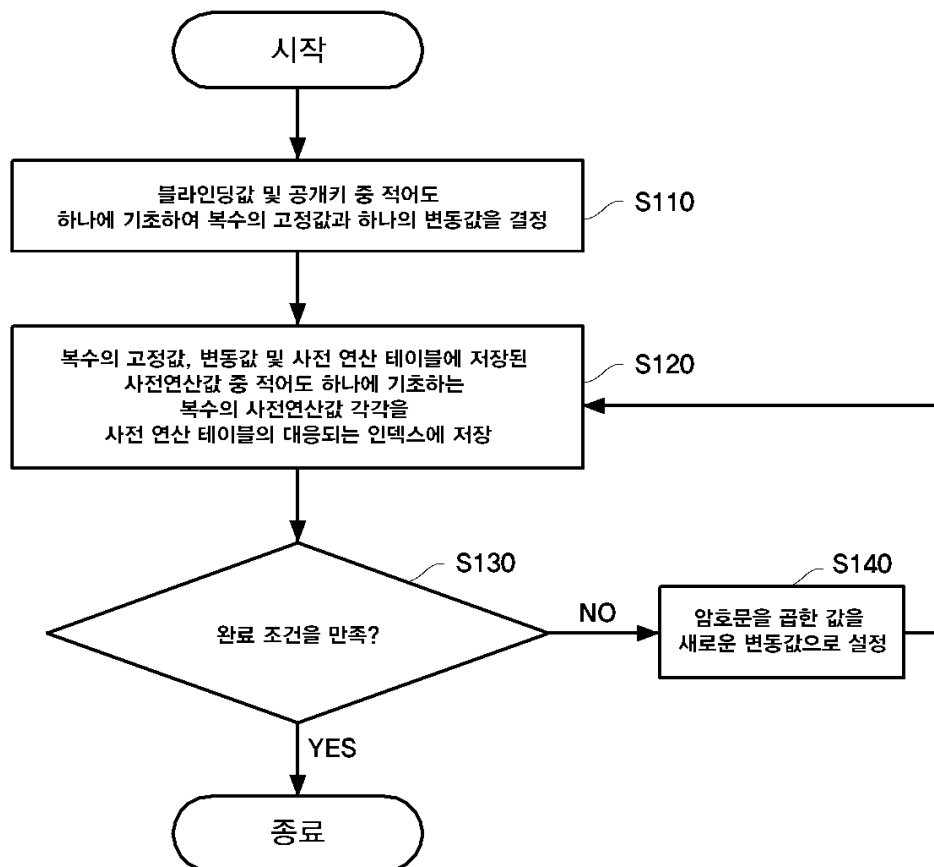
- [0077] 이와 같이, 4.3.1.1에서와 같이, 사전연산값을 연산하면서 다른 사전연산값을 재사용하는 횟수를 최소화(S_v , S_{v+1} 제외)하여, 사전 연산 테이블의 생성 시 부채널 공격으로 인한 정보 누출의 가능성이 최소화되는 효과를 얻을 수 있다.
- [0078] 예컨대, 본 발명의 일실시예에서, 사전연산값의 총 개수를 n 이라고 가정하면, 4.3.2 및 4.3.3에서 재사용되는 2개의 사전연산값(S_v , S_{v+1})은 악의의 공격자가 추측할 가능성이 있다. 그러나, 나머지 $(n-2)$ 개의 사전연산값에 대하여는 곱셈 연산 등을 통해 공격자에게 노출된 정보가 없으므로, 그 공격자는 나머지 $(n-2)$ 개의 사전연산값을 알아내기 위하여 $(n-2)!$ 회의 추측이 필요할 수 있다. 또한, 이미 계산된 사전연산값(S_v , S_{v+1}) 2개를 구별하는 것까지 고려할 때, 총 $2*(n-2)!$ 회의 추측이 필요할 수 있다. 보다 구체적으로, 윈도우 크기가 $w=5$ 라고 가정하면, 총 $2*1982!$ 회의 추측이 필요하게 되어, 사실상 추측이 불가능할 수 있다.
- [0079] 반면에, 도 4를 참조하면, 종래 기술의 일실시예에 따른 사전 연산 테이블 생성 알고리즘을 설명하기 위한 의사코드이다.
- [0080] 5.2.1.1에서는 이전에 연산된 사전연산값(S)과 암호문을 곱셈하여 사전연산값(S)을 연산한다.
- [0081] 이와 같이, 종래 기술에서는, 최초(5.1.1)를 제외하고는 반복적으로 이전에 연산된 사전연산값을 재사용하여 새로운 사전연산값을 연산하므로, 사전 연산 테이블의 생성 시 부채널 공격으로 인한 정보 누출이 발생할 가능성이 있다.
- [0082] 도 2는 본 발명의 일실시예에 따른 RSA 암호시스템의 지수승 연산에 이용되는 사전 연산 테이블 생성 장치를 설명하기 위하여 도시한 도면이다.
- [0083] 도 2를 참조하면, RSA 암호시스템의 지수승 연산에 이용되는 사전 연산 테이블 생성 장치(200)는 사전연산부(210), 연산부(220), 저장부(230) 및 제어부(240)를 포함할 수 있다. 한편, 사전 연산 테이블 생성 장치(200)는 컴퓨터, 스마트폰, 태블릿 및 웨어러블 장치 등에 탑재될 수 있다.
- [0084] 사전연산부(210)는 블라인딩값 및 공개키 중 적어도 하나에 기초하여 복수의 고정값과 하나의 변동값을 결정한다.
- [0085] 연산부(220)는 복수의 고정값, 변동값 및 사전 연산 테이블에 저장된 사전연산값 중 적어도 하나에 기초하는 복수의 사전연산값을 연산한다.
- [0086] 저장부(230)는 사전연산값 각각을 사전 연산 테이블의 대응되는 인덱스에 저장한다.
- [0087] 마지막으로 제어부(240)는 변동값과 암호문을 곱한 값을 새로운 변동값으로 하여, 소정의 완료 조건을 만족할 때까지, 연산부(220) 및 저장부(230)를 반복적으로 제어하여 사전 연산 테이블을 생성한다.
- [0088] 다른 실시예에서는, 지수승 연산이 w 비트(단, $w > 2$) 단위로 수행될 때, 사전연산부(210)는 복수의 고정값을 $(K-2)$ 개(단, $K = 2^w$) 결정하고, 연산부(220)는 $(K-2)$ 개의 고정값, 변동값 및 사전 연산 테이블에 저장된 사전연산값 중 적어도 하나에 기초하는 K 개의 사전연산값을 연산할 수 있다.
- [0089] 또 다른 실시예에서는, 연산부(220)는 $(K-2)$ 개의 고정값 및 변동값에 기초한 $(K-2)$ 개의 사전연산값을 연산하고, 사전 연산 테이블의 최초 2개의 인덱스에 저장되는 사전연산값 및 변동값에 기초한 2개의 사전연산값을 연산할 수 있다.
- [0090] 또 다른 실시예에서는, 그 $(K-2)$ 개의 사전연산값은 $(K-2)$ 개의 고정값 각각과 변동값을 곱한 $(K-2)$ 개의 값이고, 그 2개의 사전연산값은 사전 연산 테이블의 최초 2개의 인덱스에 저장되는 사전연산값 각각과 변동값을 곱한 2개의 값일 수 있다.
- [0091] 또 다른 실시예에서는, 소정의 완료 조건은 사전 연산 테이블에 저장된 사전연산값이 총 $K*(2K-1)$ 개가 되는 것일 수 있다.
- [0092] 또 다른 실시예에서는, 블라인딩값이 R 이고, 공개키가 N 일 때, 사전연산부(210)는 그 $(K-2)$ 개의 고정값을 $\{R \bmod N, R^2 \bmod N, \dots, R^{K-2} \bmod N\}$ 으로 결정하고, 그 하나의 변동값을 $\{R^{K-2}\}$ 로 결정할 수 있다.
- [0093] 한편, 상술한 본 발명의 실시예들은 컴퓨터에서 실행될 수 있는 프로그램으로 작성가능하고, 컴퓨터로 읽을 수 있는 기록매체를 이용하여 상기 프로그램을 동작시키는 범용 디지털 컴퓨터에서 구현될 수 있다.

[0094] 상기 컴퓨터로 읽을 수 있는 기록매체는 마그네틱 저장매체(예를 들면, 롬, 플로피 디스크, 하드디스크 등), 광학적 판독 매체(예를 들면, 시디롬, 디브이디 등)를 포함한다.

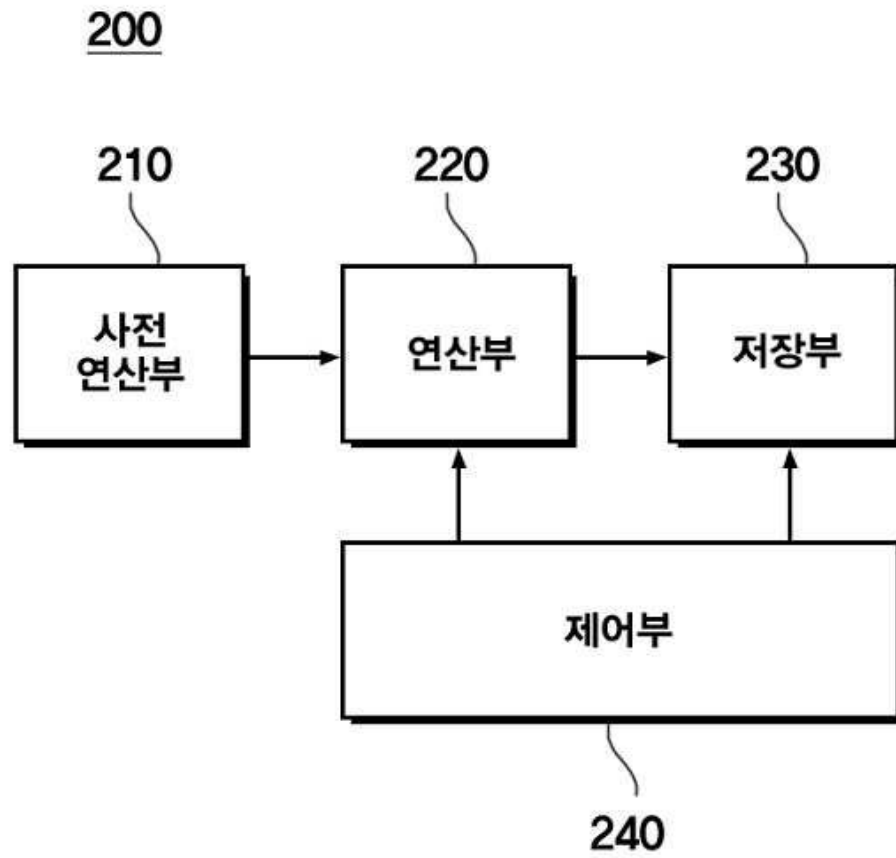
[0095] 이제까지 본 발명에 대하여 그 바람직한 실시예들을 중심으로 살펴보았다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

도면

도면1



도면2



도면3

입력	: $M, d = (d_{t-1} d_{t-2} \dots d_0)_2$
$\Phi(n)$	: $(\phi_{t-1} \phi_{t-2} \dots \phi_0)_2, \phi_{t-1} = 1$
RSA modulus	n
출력	: $M^e \bmod n$

1. If $M=1$, return 1; if $M=-1$, return $1-2d_0$
2. Generate random numbers $R \in \{1, 2, \dots, n-1\}$, r (t -length),
 $v \in \{0, 1, \dots, 2W^2 - W - 1\}$
 $v' \in \{0, 1, \dots, W-3\}$
3. Compute $\tilde{d} = d - r$
4. Pre-computation
 - 4.1 $i=0$ up to $W-3$
 - 4.1.1 $T_{v \oplus i} = R^{i+1} \bmod n$
 - 4.2 $T' = R^{W-2}$
 - 4.3 $i=-W$ up to $2W^2-3W$ by W
 - 4.3.1 $j=0$ up to $W-3$
 - 4.3.1.1

$$S_{v \oplus (i+j+W)} = T_{v' \oplus j} \times T'$$
 - 4.3.2

$$S_{v \oplus (i+2W-2)} = S_v \times T'$$
 - 4.3.3

$$S_{v \oplus (i+2W-1)} = S_{v \oplus 1} \times T'$$
 - 4.3.4

$$T' = T' \times M$$
5. For $i=k-1$ down to 1
 - 5.1 $S = S^W \bmod n$
 - 5.2 $S = S \times S_{v \oplus (W(d'_i + \tilde{d}'_i) + \phi_{t-1})} \bmod n$
6. Return $S \times S_{v \oplus (W(d'_k + \tilde{d}'_k) + \phi_{t-1})} \bmod n$

도면4

Input	$M, d = (d_{t-1} d_{t-2} \dots d_0)_2, \phi(N), N$
Output	$S = M^d \bmod N$
1. If $M=1$ then return 1 2. If $M=-1$ then return $1-2d_0$ 3. Generate random numbers $R \in \{1, 2, \dots, N-1\}, v \in \{0, 1, \dots, 2W^2 - W - 1\},$ $r(t\text{-length})$ 4. Compute $\tilde{d} = d - r$ 5. Pre-computation 5.1 For $(i=0; i < W; i++)$ 5.1.1 $S_{v \oplus i} = R^{\phi'_{v-i(W-1)+i}} \bmod N$ 5.2 For $(i=0; i < (2W^2 - W); i += W)$ 5.2.1 For $(j=0; j < W; j++)$ 5.2.1.1 $S_{v \oplus (i+j+W)} = S_{v \oplus (i+j)} \times M \bmod N$ 6. For $(i=k-1; i \geq 1; i--)$ 6.1 $S = S^W \bmod N$ 6.2 $S = S \times S_{v \oplus (W(r'_i + \tilde{d}'_i) + \phi'_{v-i})} \bmod N$ 7. Return $S^W \times S_{v \oplus (W(r'_0 + \tilde{d}'_0) + \phi'_{v-i})} \bmod N$	