(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2009-0080842
(43) 공개일자 2009년07월27일

(51) Int. Cl.
H04L 9/28 (2006.01) *H04L 9/32* (2006.01)
(21) 출원번호 10-2008-0006827
(22) 출원일자 2008년01월22일
심사청구일자 2008년01월22일

(71) 출원인
고려대학교 산학협력단
서울 성북구 안암동5가1 고려대학교 내
(72) 발명자
김성경
서울 성북구 안암동2가 118-2번지
김태현
서울 강서구 화곡2동 846-19
(뒷면에 계속)
(74) 대리인
현종철

전체 청구항 수 : 총 14 항

(54) C R T-R S A 모듈라 지수승 알고리즘을 이용한 디지털서명 방법, 그 장치 및 이를 기록한 컴퓨터 판독가능 저장매체

(57) 요 약

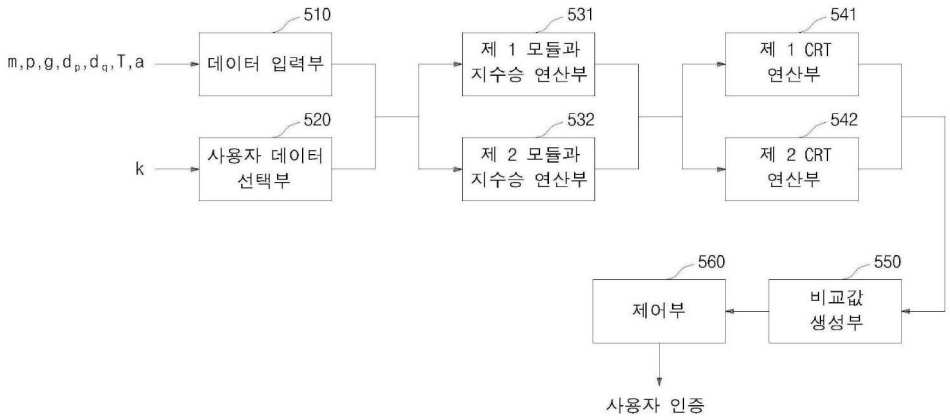
CRT-RSA 모듈라 지수승 알고리즘을 이용한 디지털 서명 방법, 그 장치 및 이를 기록한 컴퓨터 판독가능 저장 매체가 개시된다.

본 발명에 따른 CRT-RSA 모듈라 지수승 알고리즘을 이용한 디지털 서명 방법은 서로 다른 소수 p, q를 비밀키로, $n = pq$를 만족하는 n을 공개키로 euler totient 함수 $\Phi(n)$과 서로 소인 소정의 정수 e를 공개키로, $ed = 1 \bmod \Phi(n)$을 만족하는 d를 비밀키로 이용하는 CRT-RSA 모듈라 지수승 알고리즘을 이용한 디지털 서명 방법에 있어서, 인증된 수신자에게 전송하고자 하는 메시지 m, 상기 서로 다른 소수 p, q, 상기 d를 $p-1$로 모듈라 연산한 d_p, 상기 d를 $q-1$로 모듈라 연산한 d_q, 상기 d_p와 d_q의 합인 T, 상기 p^{-1}을 q로 모듈라 연산한 a 및 암호화하고자 하는 송신자에 의해 선택된 랜덤한 정수 k를 수신하는 단계; 상기 T와 d_q의 차에 따라 d_p'를 생성하고, 상기 메시지 m에 d_p'승한 값을 상기 p와 상기 정수 k를 곱한 값으로 모듈러 연산하여 s_p값을 산출하며, 상기 메시지 m에 $d_p'-1$승한 값을 상기 p와 상기 정수 k를 곱한 값으로 모듈러 연산하여 s_p'값을 산출하는 단계; 상기 T와 d_p의 차에 따라 d_q'를 생성하고, 상기 메시지 m에 d_q'승한 값을 상기 q와 상기 정수 k를 곱한 값으로 모듈러 연산하여 s_q값을 산출하고, 상기 메시지 m에 $d_q'-1$승한 값을 상기 q와 상기 정수 k를 곱한 값으로 모듈러 연산하여 s_q'값을 산출하는 단계; 상기 연산된 s_p 및 s_p'로 이루어진 제 1 데이터 쌍을 이용하여 s를 생성하고, 상기 연산된 s_q 및 s_q'로 이루어진 제 2 데이터 쌍을 이용하여 s'를 생성하는 단계; 상기 T의 비트 길이인 α와 모듈러 n의 비트 길이에 따라 생성되는 제 1 출력값과, d_p와 d_q'의 합에 상기 T의 보

수 $\overline{T}$ 를 제 1 논리 연산을 수행한 제 2 출력값을 합하여 제 1 총합값을 생성하고, 상기 메시지 m과 s'를 곱한 값을 n으로 모듈라 연산하여 제 3 출력값을 생성하여, 상기 제 1 총합값과 제 3 출력값을 입력으로 제 2 논리 연산을 수행하여 논리합 연산의 결과값을 생성하는 단계; 및 상기 논리합 연산의 결과값과 상기 s의 동일 여부에 따라 서명 인증값을 생성하는 단계를 포함한다.

본 발명에 의하면, 단순한 레지스터의 추가에 의해 단순한 암호화 방법을 제공하며, 연산량 역시 종래의 암호화 방법에 비해 증가하지 않으면서도 최근 제시된 새로운 단순 전력 분석 및 오류 주입 공격에 안전성을 제공함으로써 스마트카드와 같은 내장형 장치에서도 효율적이고 안전한 디지털 서명 기법을 제공할 수 있는 효과가 있다.

대 표 도



(72) 발명자

한동국

인천 계양구 작전2동 772번지 타임빌라 가동 201호

홍석희

서울 은평구 응암2동 451-12 202호

특허청구의 범위

청구항 1

서로 다른 소수 p, q를 비밀키로, $n = pq$를 만족하는 n을 공개키로 euler totient 함수 $\Phi(n)$과 서로 소인 소정의 정수 e를 공개키로, $ed = 1 \bmod \Phi(n)$을 만족하는 d를 비밀키로 이용하는 CRT-RSA 모듈라 지수승 알고리즘을 이용한 디지털 서명 방법에 있어서,

인증된 수신자에게 전송하고자 하는 메시지 m, 상기 서로 다른 소수 p, q, 상기 d를 $p-1$로 모듈라 연산한 d_p, 상기 d를 $q-1$로 모듈라 연산한 d_q, 상기 d_p와 d_q의 합인 T, 상기 p^{-1}을 q로 모듈라 연산한 a 및 암호화하고자 하는 송신자에 의해 선택된 랜덤한 정수 k를 수신하는 단계;

상기 T와 d_q의 차에 따라 d_p'를 생성하고, 상기 메시지 m에 d_p'승한 값을 상기 p와 상기 정수 k를 곱한 값으로 모듈러 연산하여 s_p값을 산출하며, 상기 메시지 m에 $d_p'-1$승한 값을 상기 p와 상기 정수 k를 곱한 값으로 모듈러 연산하여 s_p'값을 산출하는 단계;

상기 T와 d_p의 차에 따라 d_q'를 생성하고, 상기 메시지 m에 d_q'승한 값을 상기 q와 상기 정수 k를 곱한 값으로 모듈러 연산하여 s_q 값을 산출하고, 상기 메시지 m에 $d_q'-1$승한 값을 상기 q와 상기 정수 k를 곱한 값으로 모듈러 연산하여 s_q'값을 산출하는 단계;

상기 연산된 s_p 및 s_p'로 이루어진 제 1 데이터 쌍을 이용하여 s를 생성하고, 상기 연산된 s_q 및 s_q'로 이루어진 제 2 데이터 쌍을 이용하여 s'를 생성하는 단계;

상기 T의 비트 길이인 α와 모듈러 n의 비트 길이에 따라 생성되는 제 1 출력값과, d_p와 d_q'의 합에 상기 T의 보수 $\overline{T}$를 제 1 논리 연산을 수행한 제 2 출력값을 합하여 제 1 총합값을 생성하고, 상기 메시지 m과 s'를 곱한 값을 n으로 모듈라 연산하여 제 3 출력값을 생성하여, 상기 제 1 총합값과 제 3 출력값을 입력으로 제 2 논리 연산을 수행하여 논리합 연산의 결과값을 생성하는 단계; 및

상기 논리합 연산의 결과값과 상기 s의 동일 여부에 따라 서명 인증값을 생성하는 단계를 포함하는 CRT-RSA 모듈라 지수승 알고리즘을 이용한 디지털 서명 방법.

청구항 2

제 1 항에 있어서,

상기 논리합 연산의 결과값인 s'는

$\wedge$가 AND 연산이며 $\oplus$가 XOR 연산을 의미할 때, 하기의 식 1에 의해 생성되는 것을 특징으로 하는 CRT-RSA 모듈라 지수승 알고리즘을 이용한 디지털 서명 방법.

$$s' \leftarrow (m \cdot s' \bmod n) \wedge \left(\sum_{i=a}^{b-1} 2^i + (\overline{T} \oplus (d_p + d_q')) \right) \quad (1)$$

청구항 3

제 1 항에 있어서,

상기 제 1 논리 연산은 AND 연산이며, 상기 제 2 논리 연산은 XOR 연산인 것을 특징으로 하는 CRT-RSA 모듈라 지수승 알고리즘을 이용한 디지털 서명 방법.

청구항 4

제 1 항에 있어서,

상기 서명 인증값을 생성하는 단계는

상기 논리합 연산의 결과값과 상기 s가 동일하면 서명 인증값을 출력하고,

상기 논리합 연산의 결과값과 상기 s가 동일하지 않으면 오류 메시지를 출력하는 단계를 포함하는 것을 특징으로 하는 CRT-RSA 모듈라 지수승 알고리즘을 이용한 디지털 서명 방법.

청구항 5

제 1 항에 있어서,

상기 s와 s'는

각각 병렬로 CRT 연산에 따라 생성되는 것을 특징으로 하는 CRT-RSA 모듈라 지수승 알고리즘을 이용한 디지털 서명 방법.

청구항 6

서로 다른 소수 p, q를 비밀키로, $n = pq$를 만족하는 n을 공개키로 euler totient 함수 $\Phi(n)$과 서로소인 소정의 정수 e를 공개키로, $ed = 1 \bmod \Phi(n)$을 만족하는 d를 비밀키로 이용하는 CRT-RSA 모듈라 지수승 알고리즘을 이용한 디지털 서명 장치에 있어서,

인증된 수신자에게 전송하고자 하는 메시지 m, 상기 서로 다른 소수 p, q, 상기 d를 $p-1$로 모듈라 연산한 d_p, 상기 d를 $q-1$로 모듈라 연산한 d_q, 상기 d_p와 d_q의 합인 T 및 상기 p^{-1}을 q로 모듈라 연산한 a가 입력되는 데이터 입력부;

상기 메시지 m을 암호화하고자 하는 송신자에 의해 랜덤한 정수 k 가 선택되는 사용자 데이터 선택부;

상기 T와 d_q의 차에 따라 d_p'를 생성하고, 상기 메시지 m에 d_p'승한 값을 상기 p와 상기 정수

k를 곱한 값으로 모듈러 연산하여 s_p값을 산출하며, 상기 메시지 m에 $d_p'-1$승한 값을 상기 p와 상기 정수 k를 곱한 값으로 모듈러 연산하여 s_p' 값을 산출하는 제 1 모듈라 지수승 연산부;

상기 T와 d_p의 차에 따라 d_q'를 생성하고, 상기 메시지 m에 d_q'승한 값을 상기 q와 상기 정수 k를 곱한 값으로 모듈러 연산하여 s_q 값을 산출하고, 상기 메시지 m에 $d_q'-1$승한 값을 상기 q와 상기 정수 k를 곱한 값으로 모듈러 연산하여 s_q' 값을 산출하는 제 2 모듈라 지수승 연산부;

상기 연산된 s_p 및 s_p'로 이루어진 제 1 데이터 쌍을 이용하여 CRT 연산에 따라 s를 생성하는 제 1 CRT 연산부;

상기 연산된 s_q 및 s_q'로 이루어진 제 2 데이터 쌍을 이용하여 CRT 연산에 따라 s'를 생성하는 제 2 CRT 연산부;

상기 T의 비트 길이인 α와 모듈러 n의 비트 길이에 따라 생성되는 제 1 출력값과, d_p와 d_q'의 합에 상기 T의 보수 $\overline{T}$를 제 1 논리 연산을 수행한 제 2 출력값을 합하여 제 1 총합값을 생성하고, 상기 메시지 m과 s'를 곱한 값을 n으로 모듈라 연산하여 제 3 출력값을 생성하여, 상기 제 1 총합값과 제 3 출력값을 입력으로 제 2 논리 연산을 수행하여 논리합 연산의 결과값을 생성하는 비교값 생성부; 및

상기 논리합 연산의 결과값과 상기 s의 동일 여부에 따라 서명 인증값을 생성하는 제어부를 포함하는 CRT-RSA 모듈라 지수승 알고리즘을 이용한 디지털 서명 장치.

청구항 7

제 6 항에 있어서,

상기 논리합 연산의 결과값은

$\wedge$가 AND 연산이며 $\oplus$가 XOR 연산을 의미할 때, 하기의 식 2에 의해 생성되는 것을 특징으로 하는 CRT-RSA 모듈라 지수승 알고리즘을 이용한 디지털 서명 장치.

$$s' \leftarrow (m \cdot s' \bmod n) \wedge \left(\sum_{i=a}^{p-1} 2^i + (\overline{T} \oplus (d_p + d_q')) \right) \quad (2)$$

청구항 8

제 6 항에 있어서,

상기 제 1 논리 연산은 AND 연산이며, 상기 제 2 논리 연산은 XOR 연산인 것을 특징으로 하는 CRT-RSA 모듈라 지수승 알고리즘을 이용한 디지털 서명 장치.

청구항 9

제 6 항에 있어서,

상기 제어부는

상기 논리합 연산의 결과값과 상기 s가 동일하면 서명 인증값을 출력하고,

상기 논리합 연산의 결과값과 상기 s가 동일하지 않으면 오류 메시지를 출력하는 것을 특징으로 하는 CRT-RSA 모듈라 지수승 알고리즘을 이용한 디지털 서명 장치.

청구항 10

컴퓨터 판독 가능 저장 매체에 서로 다른 소수 p, q를 비밀키로, $n = pq$를 만족하는 n을 공개키로 euler totient 함수 $\Phi(n)$과 서로 소인 소정의 정수 e를 공개키로, $ed = 1 \bmod \Phi(n)$을 만족하는 d를 비밀키로 이용하는 CRT-RSA 모듈라 지수승 알고리즘을 이용한 디지털 서명을 생성하는 프로그램이 기록되어 있고, 상기 프로그램은,

인증된 수신자에게 전송하고자 하는 메시지 m, 상기 서로 다른 소수 p, q, 상기 d를 $p-1$로 모듈라 연산한 d_p, 상기 d를 $q-1$로 모듈라 연산한 d_q, 상기 d_p와 d_q의 합인 T, 상기 p^{-1}을 q로 모듈라 연산한 α 및 암호화하고자 하는 송신자에 의해 선택된 랜덤한 정수 k에 따라 상기 T와 d_q의 차에 따라 d_p'를 생성하고, 상기 메시지 m에 d_p'승한 값을 상기 p와 상기 정수 k를 곱한 값으로 모듈러 연산하여 s_p값을 산출하며, 상기 메시지 m에 $d_p'-1$승한 값을 상기 p와 상기 정수 k를 곱한 값으로 모듈러 연산하여 s_p'값을 산출하도록 하는 코드;

상기 T와 d_p의 차에 따라 d_q'를 생성하고, 상기 메시지 m에 d_q'승한 값을 상기 q와 상기 정수 k를 곱한 값으로 모듈러 연산하여 s_q 값을 산출하고, 상기 메시지 m에 $d_q'-1$승한 값을 상기 q와 상기 정수 k를 곱한 값으로 모듈러 연산하여 s_q'값을 산출하도록 하는 코드;

상기 연산된 s_p 및 s_p'로 이루어진 제 1 데이터 쌍을 이용하여 s를 생성하고, 상기 연산된 s_q 및 s_q'로 이루어진 제 2 데이터 쌍을 이용하여 s'를 생성하도록 하는 코드;

상기 T의 비트 길이인 α와 모듈러 n의 비트 길이에 따라 생성되는 제 1 출력값과, d_p와 d_q'의 합에 상기 T의 보수 $\overline{T}$를 제 1 논리 연산을 수행한 제 2 출력값을 합하여 제 1 총합값을 생성하고, 상기 메시지 m과 s'를 곱한 값을 n으로 모듈라 연산하여 제 3 출력값을 생성하여, 상기 제 1 총합값과 제 3 출력값을 입력으로 제 2 논리 연산을 수행하여 논리합 연산의 결과값을 생성하도록 하는 코드; 및

상기 논리합 연산의 결과값과 상기 s의 동일 여부에 따라 서명 인증값을 생성하도록 하는 코드를 포함하는 컴

퓨터 판독 가능 저장 매체.

청구항 11

제 10 항에 있어서,

상기 논리합 연산의 결과값은

$\wedge$가 AND 연산이며 $\oplus$가 XOR 연산을 의미할 때, 하기의 식 3에 의해 생성되는 것을 특징으로 하는 컴퓨터 판독 가능 저장 매체.

$$s' \leftarrow (m \cdot s' \bmod n) \wedge \left(\sum_{i=a}^{p-1} 2^i + (\overline{T} \oplus (d_p + d_q')) \right) \quad (3)$$

청구항 12

제 10 항에 있어서,

상기 제 1 논리 연산은 AND 연산이며, 상기 제 2 논리 연산은 XOR 연산인 것을 특징으로 하는 컴퓨터 판독 가능 저장 매체.

청구항 13

제 10 항에 있어서,

상기 서명 인증값을 생성하도록 하는 코드는

상기 논리합 연산의 결과값과 상기 s가 동일하면 서명 인증값을 출력하고,

상기 논리합 연산의 결과값과 상기 s가 동일하지 않으면 오류 메시지를 출력하도록 하는 코드를 포함하는 것을 특징으로 하는 컴퓨터 판독 가능 저장 매체.

청구항 14

제 10 항에 있어서,

상기 s와 s'는

각각 병렬로 CRT 연산에 따라 생성되는 것을 특징으로 하는 컴퓨터 판독 가능 저장 매체.

명 세 서

발명의 상세한 설명

기 술 분 야

<1> 본 발명은 암호화에 관한 것으로서, 특히 암호화의 표준인 중국인의 나머지 정리(Chinese Remainder Theorem:CRT)를 이용한 RSA 암호화 시스템에 오류 주입에 대한 안전성을 가질 뿐만 아니라, 전력 분석 공격 방법 중 단순 전력 공격 방법에도 안전한 CRT-RSA 모듈라 지수승 알고리즘을 이용한 디지털 서명 방법, 그 장치 및 이를 기록한 컴퓨터 판독가능 저장 매체를 제공하는 것이다.

배 경 기 술

<2> 정보화 사회의 도래와 함께 암호 알고리즘 및 암호 프로토콜을 이용한 정보의 보호는 그 중요성을 더해가고 있다. 이러한 암호 알고리즘 중에서 공개키 암호 알고리즘은 개선된 암호화 표준(Advanced Encryption Standard:AES)을 포함하는 비밀키 암호 알고리즘의 단점인 키 분배 문제, 전자 서명 문제 등을 해결하면서 인터넷이나 금융 망과 같은 여러 분야의 응용에 빠르게 적용이 되어 가고 있다.

<3> 전송되는 내용을 암호화하여 전송하는 방식에는 대칭키 암호화 방식과 공개키 암호화 방식이 있고, 공개키 암호화 방식 중에서 현재 인터넷이나 금융계 중에서 표준으로 선택되어 널리 사용되고 있는 방식으로는 RSA(Rivest Shamir Adleman) 공개키 암호화 방식이 있다.

<4> RSA 공개키 암호화 방식은 Rivest, Shamir 및 Adleman에 의해 제안된 방식으로 암호화문에 따른 데이터의 크기가 커질수록 소인수 분해가 어렵다는 점에 그 안전도의 기반을 두고 있다.

<5> 한편, 1996년 Kocher에 의하여 부채널 공격이 소개된 후, 내장형 장치(embedded device)의 암호 알고리즘에 대한 다양한 공격 방법이 소개되었다. 수동적인 공격 방법으로 분류되는 부채널 공격은 공격자가 알고리즘 수행 시간, 알고리즘의 동작 중에 사용되는 전력량, 그리고 전자파를 이용하여 공격하며 이를 각 시간 공격(Timing Attack:TA), 단순 전력 분석(Simple Power Analysis:SPA), 차분 전력 분석(Differential Power Analysis:DPA), 전자파 분석(Electro-Magnetic Analysis:EMA)이라고 한다.

<6> 능동적인 공격은 변형된 외부 클럭을 주입하거나, 온도를 변화시키거나 장치에 X-ray와 같은 레이저를 이용하여 공격하며, 이와 같이 능동적인 공격 방법을 오류 주입 공격(Fault Attack:FA)이라고 한다.

<7> 1996년 Bellcore에 의해 중국인의 나머지 정리(Chinese Remainder Theorem:CRT)를 이용한 RSA 암호 시스템(CRT-RSA)에서의 오류 주입 공격 방법이 제시된 후, 최근 DES, RSA, ElGamal, ECC, AES 등 다양한 암호 알고리즘이 오류 주입 공격 방법에 의해 공격되었다.

<8> 한편, CRT-RSA에서의 오류 주입 공격 방법에 대해서 스마트 카드의 사용이 증가하면서 효율적인 부채널 공격과 오류 주입 공격에 안전한 대응 방법이 요구되고, 스마트 카드와 같은 내장형 장치에는 연산 능력과 메모리가 제한적이기 때문에 적은 메모리와 연산량을 사용하는 효율적인 대응 방법이 요구되며 이에 대한 연구가 많이 진행되었다.

<9> 최근 2005년 Giraud가 처음으로 전력 분석 공격 방법 중 하나인 단순 전력 공격 분석과 오류 주입 공격에 안전한 방법을 제안하였다.

<10> Giraud 방법에서의 지수승 알고리즘은 단순 전력 분석과 오류 주입 공격에 안전한 Montgomery Ladder 방법을 이용하여 연산되고, 개인키만을 이용하여 오류 주입을 확인하게 된다. 따라서 개인키 만을 사용할 수 있는 자바 카드(Java card)의 공개키 환경에서도 안전하게 사용될 수 있다.

<11> 전술한 바와 같이, RSA 공개키 암호화 방식에서는 일반 공개키 암호화 방식에서와 같이 일반인도 알 수 있는 공개키와 암호화를 시키는 본인만이 알 수 있는 비밀키가 있다.

<12> 상기 RSA 암호화에 방식에서의 암호화 알고리즘은 하기와 같다.

<13> 우선, 암호문 작성자는 두 소수 p 및 q를 생성하여 비밀키로 지정하고, 상기 두 소수 p 및 q를 이용하여 $n(=p\times q)$ 을 공개키로 일반에게 공개한다.

<14> 그런 다음, Euler totient 함수 $\Phi(n)\,(=(p\text{-}1)(q\text{-}1))$과 서로 소(Relatively Prime)인 임의의 정수 e 를 선택하여 공개키로 지정하고, $e\cdot d=1 \bmod \Phi(n)$을 만족하는 정수 d를 Elucid 알고리즘을 이용하여 생성한 다음 이를 비밀키로 지정한다.

<15> 이와 같이, RSA 공개키 암호화 방식은 비밀키로 p, q, d를 지정하고, 공개키로 n, e를 지정하여, 전송하고자 하는 메시지를 자신의 비밀키 또는 상대방의 공개키 등을 이용하여 암호화하고, 수신자는 이와 반대로 전송자의 공개키 또는 자신의 비밀키 등을 이용하여 복호화한다.

<16> 여기서, 수신자에게 전송하고자하는 메시지를 M이라고 할 때, 메시지 전송자는 암호문 $C(=M^e \bmod n)$ 를 수신자에게 전송하게 되고, 수신자는 수신된 암호문 C로부터 메시지 $M(=C^d \bmod n)$의 과정을 통하여 복호화하여 복호화된 메시지를 확인한다.

<17> 한편, 수신자에게 전송하는 메시지에 디지털 서명을 하기 위하여 전송자는 $S = M^{d} \bmod n$의 과정을 거쳐 생성된 서명문 S와 메시지 M을 수신자에게 전송하며, 수신자는 $M' = S^{e} \bmod n$의 연산 과정을 거쳐 복호화한 후, 수신된 M과 연산된 M'를 비교하여 양자가 동일하면 진정한 서명으로 인증을 하게 된다.

<18> RSA 시스템은 공개 정보로부터 비밀키 d를 알아내는 것이 암호문을 해독하는 키가 되며, 공개 정보로부터 비밀키 d를 알아내는 공격이 성공하기 위해서는 $\Phi(n)$을 알아야 하고, 이는 공개키 n을 소인수 분해하여 p와 q를 구하는 문제로 귀결된다.

<19> 암호화하는 전송자는 타인이 암호문을 해독하는 것을 방지하기 위하여 p와 q를 일정크기 이상, 바람직하게는 384비트 이상의 수를 사용하여 n이 소인수 분해되는 것을 방지한다.

<20> 이와 같이, RSA 시스템에서 암호 및 서명을 하기 위해서는 큰 수에 대한 연산을 수행하여야 하고, 암호문을 복호화할 경우, 서명에 대한 많은 연산이 불가피하다.

<21> 이러한 단점을 보완하기 위하여 많은 고속 알고리즘이 개발되었는데, 그 중 중국인의 나머지 정리(Chinese Remainder Theorem:CRT)에 기초한 방법은 비밀키 d에 대한 멱승 연산을 효과적으로 처리하기 때문에 CRT를 이용한 RSA 암호 시스템에서 널리 사용되고 있다.

<22> 한편, CRT를 이용한 RSA 암호 시스템에서 사용되는 파라미터들은 RSA 모듈러 값인 $n = p \times q$, 공개키 e 및 개인키 d이다.

<23> CRT 기반의 RSA 암호 시스템에서 $m^{d} \bmod n$의 연산은 하기의 수학식 1을 통하여 연산된다.

수학식 1

<24> $$s_p \equiv m^{d \bmod (p-1)} \bmod p$$

<25> $$s_q \equiv m^{d \bmod (q-1)} \bmod q$$

<26> 그런 다음, 상기 수학식 1에 의거하여 $s = CRT(s_p, s_q)$ 연산을 수행한다.

<27> 그러나, 이에 대하여 오류 주입 공격을 수행하면, CRT 기반의 RSA 암호시스템은 안전하지 않다는 지적이 제시되었다.

<28> 오류 주입 공격이란, IC 카드나 프로세서의 동작 과정에서 과전류를 흘려보내는 등의 방식으로 하드웨어 도는 소프트웨어 상에 의도적으로 오류가 발생하도록 하여 출력된 오류값을 이용하여 원하는 비밀 정보를 알아내는 방법으로서 최근 주목을 받고 있는 공격 방법이다.

<29> 만약, s_p(또는 s_q) 연산에서 오류가 발생하고, s_q(또는 s_p) 는 오류가 발생하지 않는 값이라고 할 경우, 하기의 수학식 2과 같은 연산을 통하여 비밀 정보인 q(또는 p)의 값을 공격자가 알 수 있다.

수학식 2

<30> $$q = \gcd(s'^{e} - m, n) \quad \text{if} \quad s_p \ is \ error$$

<31> $$p = \gcd(s'^{e} - m, n) \quad \text{if} \quad s_q \ is \ error$$

<32> Shamir에 따른 CRT 기반의 RSA 암호 시스템에 대한 오류 주입 공격에 대한 대응 방법은 32비트 정도의 랜덤한 값 r을 선택한 후 하기의 수학식 3에 의거하여 s_p 또는 s_q를 연산한다.

수학식 3

<33> $$s_p \equiv m^{d \bmod (p-1)(r-1)} \bmod pr$$

<34> $$s_q \equiv m^{d \bmod (q-1)(r-1)} \bmod qr$$

<35> 그런 다음, CRT 연산 전에 $s_p \equiv s_q \bmod r$을 확인한다. 만약 s_p(또는 s_q) 연산에서 오류가 발생하였을 경우 $s_p \equiv s_q \bmod r$의 연산 단계를 통과하지 못하기 때문에 오류 주입 여부를 확인할 수 있다. 그러나, Shamir의 방법에는 여러 가지 문제점이 제안되었고, 그 후로 많은 대응 방안이 제시되었다.

<36> 최근 2005년에 Ciet와 Joye, 그리고 Giraud가 새로운 대응 방법을 제시하였다. Ciet와 joye는 Shamir의 대응 방법을 일반화하였고, Giraud는 Montgomery Ladder를 이용하여 오류 주입 공격에 안전한 방법을 제안하였다.

<37> Giraud의 방법은 전력 분석 공격 중 하나인 단순 전력 분석 공격에도 안전한 방법이다.

<38> Giraud의 방법은 Joye와 Yen이 제안하였던 단순 전력 분석 대응 방법의 Montgomery Ladder 모듈러 지수성 알고리즘의 결과 값인 m^{a-1}, m^{a}를 이용하며, Giraud는 Joye와 Yen의 모듈러 지수승 알고리즘을 단순전력 분석과 오류 주입 공격에 모두 안전한 모듈러 지수승으로 바꾸어 제안하였고, 이는 도 1에 도시된 바와 같다.

<39> 한편, 도 1에 따른 알고리즘 1을 이용하여 연산되는 Giraud의 CRT-RSA 방법은 도 2에 따른 알고리즘 2과 같다.

<40> 도 2에 따른 Giraud가 제안한 CRT-RSA 방법은 공개키 e를 요구하지 않으므로 자바 카드의 공개키 환경에서처럼 오직 개인키 d만 요구하는 경우에도 사용가능하다. 공개키 e를 이용하여 CRT-RSA 연산을 사용하는 경우, 공개키의 길이가 커질수록 속도 역시 늦어지게 되는 단점이 있어 Giraud가 제안한 CRT-RSA 방법은 유용하게 사용된다.

<41> Giraud가 제안하는 CRT-RSA 방법을 도 2를 참조하여 상술하면, Giraud가 제안하는 CRT-RSA 방법은 두 번의 CRT 연산을 수행하게 된다.

<42> 첫 번째 단계로, 입력값 m, p, q, d_p, d_q, a가 주어졌을 때, 먼저 랜덤한 k를 선택한다.

<43> 그 다음 단계로, m, d_p, q, k를 사용하여 s_p', s_p를 연산한다. 여기서, $s_p' = m^{d_p - 1} \bmod k \cdot p$이고, $s_p = m^{d_p} \bmod k \cdot p$의 값을 가지게 된다. 이와 같이 그 다음 단계인 s_q', s_q의 값도 마찬가지로 연산 된다.

<44> 그 다음 단계 4 및 단계 5에서는 두 번의 CRT 연산을 통하여 $s' = m^{d-1} \bmod n, s = m^{d} \bmod n$ 값을

연산하고, 단계 6에서 s' 값에 m을 곱하여 s와 동일한 값을 만들어 단계 7에서 s값과 비교한다.

<45> $CRT_{blinded}(s_p, s_q) = (((s_q - s_p) \bmod (k \cdot q)) \cdot a \bmod (k \cdot q)) \cdot p + s_p \bmod p \cdot q$ 이고, 만약 그 전 단계에서 오류가 주입되었을 경우, 단계 7에서의 $s' = s$를 통과하지 못하게 된다. 또한, 연산에 사용되는 각 변수들에 대한 변경 역시 단계 7에서 확인하게 된다.

<46> Giraud에 의해 제시된 모듈러 지수승 알고리즘에 대한 안전성은 하기와 같다. 그리고, 여기서 오류가 주입되어 변경된 값을 햇(hat, ^)을 사용하여 표현한다.

<47> 즉, x에 오류가 주입된 경우, $\hat{x}$로 표현할 수 있다.

<48> 첫 번째로, (s_q', s_q)의 연산 중에 m에 오류가 주입되었을 경우에는 $(s_p', \hat{s_q'})$를 이용하여 s'를 연산하고, $(s_p, \hat{s_q})$를 이용하여 s를 연산한다. 여기서, $\hat{s_q'}$, $\hat{s_q}$의 값은 하기의 수학식 4와 같다.

수학식 4

<49> $$\hat{s}_{q'} = \hat{m}^{d_p - 1} \bmod k \cdot q, \quad \hat{s}_q = \hat{m}^{d_p} \bmod k \cdot q$$

<50> 따라서, 상기 도 2의 단계 7에서의 $s' = s$의 비교 단계는 하기의 수학식 5에 의한다.

수학식 5

$$\begin{aligned} \hat{s} - m \cdot \hat{s'} &= ((\hat{s}_p - s_p) \cdot a \bmod q) \cdot p + s_p \\ &\quad - m \cdot (((\hat{s}_q - s'_p) \cdot a \bmod q) \cdot p + s'_p) \bmod n \\ &= ((\hat{m}^{d_q} - m \cdot \mu \cdot q - m^{d_p} + m \cdot \lambda \cdot p) \cdot a + a_0 \cdot q) \cdot p \\ &\quad + m^{d_q} - m \cdot \lambda \cdot p \\ &\quad - ((m \cdot \hat{m}^{d_p - 1} - m \cdot \mu \cdot q - m^{d_p} + m \cdot \lambda \cdot p) \cdot a \\ &\quad + m \cdot a_1 \cdot q) \cdot p \end{aligned}$$

<51> $$= a \cdot p \cdot \hat{m}^{d_q - 1} \cdot (\hat{m} - m) \bmod n$$

<52> 상기 수학식 5에서 λ와 μ는 유일한 정수 값이다. 이때, $\hat{m} - m$은 q로 나눠지지 않고, '0'의 값도 아니기 때문에 상기 도 2의 단계 7을 통과하지 못한다.

<53> 그러므로, 공격자는 송신자의 메시지에 대한 비밀 정보를 알아낼 수 없다.

<54> 두 번째로, s'(또는 s)의 연산과정에서 오류가 주입되었을 경우, 즉 s'(또는 s)의 연산을 위해 CRT 연산시 오류가 주입 되었을 경우에는 $s = m \cdot s' \bmod n$의 관계가 성립되지 않으므로 상기 도 2의 단계 7을 통과하지 못하여 공격자는 비밀 정보를 알아낼 수 없다.

<55> 세 번째로, (s_p', s_p)(또는, (s_q', s_q))의 연산 과정에 오류가 주입되었을 경우이다.

<56> 이는, $(\hat{s_p'}, \hat{s_p})$의 경우 상기 도 2의 단계 7은 하기의 수학식 6으로 표현될 수 있다.

수학식 6

$$
\begin{aligned}
\hat{s}-m\cdot\hat{s}' &= ((s_q-\hat{s}_p)\cdot a \bmod q)\cdot p+s_p \\
&\quad -m\cdot(((s'_q-\hat{s}'_p)\cdot a \bmod q)\cdot p+\hat{s}'_p) \bmod n \\
&= ((m^{d_q}-m\cdot\mu\cdot q-\hat{s}_p)\cdot a+\zeta_0\cdot q)\cdot p+\hat{s}_p \\
&\quad -(((m^{d_p}-m\cdot\mu\cdot q-m\cdot\hat{s}'_p)\cdot a+m\cdot\zeta_1\cdot q)\cdot p \\
&\quad -m\cdot\hat{s}'_p) \bmod (p\cdot q), \quad (\zeta_0,\zeta_1\in Z) \\
&= (m\cdot\hat{s}'_p-\hat{s}_p)\cdot(a\cdot p-1) \bmod n
\end{aligned}
$$

<57>

<58> 여기서, $a=p^{-1} \bmod q$ 이므로, $a\cdot p=1 \bmod p$ 이고, $a\cdot p=1+\zeta\cdot p$ 이므로, $\hat{s}-m\cdot\hat{s}'=(m\cdot\hat{s}'_p-\hat{s}_p)\cdot\zeta\cdot q \bmod n$ 을 만족한다. 이는 $m\cdot\hat{s}'_p\neq\hat{s}_p \bmod p$ 이기 때문에 '0'의 값도 아니고, p 로 나누어 지지도 않는다.

<59> 상술한 오류 주입에 대한 검증은, 서명의 생성시 S_p, S_q 를 두 번 연산하거나 검증함수를 통하여 오류가 발생하였는지를 검사하여 오류가 발생한 경우에는 서명을 다시 수행하여 공격자가 공격을 할 수 없도록 하는 방법이다.

<60> 이러한 방법은 암호 연산 자체가 많은 연산량을 요구하므로 비효율적이고, 또한 영구적인 결함을 가지고 있는 시스템의 경우에 오류가 생성되었는지를 검증할 방법이 없어 적절하지 못하며, 연산 과정이 복잡하고 계산량이 증가하는 단점이 있고, 비밀리에 관리해야 할 파라미터가 추가로 발생한다는 점에서 기존의 시스템과 호환적이지 않다는 문제점이 있다.

발명의 내용

해결 하고자하는 과제

<61> 본 발명이 해결하고자 하는 첫 번째 과제는 연산 과정이 단순하고 연산량이 추가적으로 증가하지 않으면서도 단순 전력 분석 및 오류 주입 공격에도 안전하여 스마트 카드와 같은 내장형 장치에서도 효율적이고 안전하게 사용할 수 있는 CRT-RSA 모듈라 지수승 알고리즘을 이용한 디지털 서명 방법을 제공하는 것이다.

<62> 본 발명이 해결하고자 하는 두 번째 과제는 상기 CRT-RSA 모듈라 지수승 알고리즘을 이용한 디지털 서명 방법을 이용한 CRT-RSA 모듈라 지수승 알고리즘을 이용한 디지털 서명 장치를 제공하는 것이다.

<63> 본 발명이 해결하고자 하는 세 번째 과제는 상기 CRT-RSA 모듈라 지수승 알고리즘을 이용한 디지털 서명 방법을 컴퓨터에서 수행할 수 있도록 프로그램으로 기록된 컴퓨터 판독 가능 저장 매체를 제공하는 것이다.

과제 해결수단

<64> 상기 첫 번째 과제를 해결하기 위하여 본 발명은,

<65> 서로 다른 소수 p, q 를 비밀키로, $n=pq$ 를 만족하는 n 을 공개키로 euler totient 함수 $\Phi(n)$ 과 서로소인 소정의 정수 e 를 공개키로, $ed=1 \bmod \Phi(n)$ 을 만족하는 d 를 비밀키로 이용하는 CRT-RSA 모듈라 지수승 알고리즘을 이용한 디지털 서명 방법에 있어서, 인증된 수신자에게 전송하고자 하는 메시지 m, 상기 서로 다른 소수 p, q, 상기 d 를 $p-1$ 로 모듈라 연산한 d_p, 상기 d 를 $q-1$ 로 모듈라 연산한 d_q, 상기 d_p 와 d_q 의 합인 T, 상기 p^{-1} 을 q 로 모듈라 연산한 a 및 암호화하고자 하는 송신자에 의해 선택된

랜덤한 정수 k 를 수신하는 단계; 상기 T와 d_q의 차에 따라 d_p'를 생성하고, 상기 메시지 m에 d_p' 승한 값을 상기 p와 상기 정수 k를 곱한 값으로 모듈러 연산하여 s_p값을 산출하며, 상기 메시지 m에 $d_p'-1$ 승한 값을 상기 p와 상기 정수 k를 곱한 값으로 모듈러 연산하여 s_p'값을 산출하는 단계;

<66> 상기 T와 d_p의 차에 따라 d_q'를 생성하고, 상기 메시지 m에 d_q'승한 값을 상기 q와 상기 정수 k를 곱한 값으로 모듈러 연산하여 s_q 값을 산출하고, 상기 메시지 m에 $d_q'-1$승한 값을 상기 q와 상기 정수 k를 곱한 값으로 모듈러 연산하여 s_q'값을 산출하는 단계; 상기 연산된 s_p 및 s_p'로 이루어진 제 1 데이터 쌍을 이용하여 s를 생성하고, 상기 연산된 s_q 및 s_q'로 이루어진 제 2 데이터 쌍을 이용하여 s'를 생성하는 단계; 상기 T의 비트 길이인 α와 모듈러 n의 비트 길이에 따라 생성되는 제 1 출력값과, d_p와 d_q'의 합에 상기 T의 보수 $\overline{T}$를 제 1 논리 연산을 수행한 제 2 출력값을 합하여 제 1 총합값을 생성하고, 상기 메시지 m과 s'를 곱한 값을 n으로 모듈라 연산하여 제 3 출력값을 생성하여, 상기 제 1 총합값과 제 3 출력값을 입력으로 제 2 논리 연산을 수행하여 논리합 연산의 결과값을 생성하는 단계; 및 상기 논리합 연산의 결과값과 상기 s의 동일 여부에 따라 서명 인증값을 생성하는 단계를 포함하는 CRT-RSA 모듈라 지수승 알고리즘을 이용한 디지털 서명방법을 제공한다.

<67> 여기서, 상기 논리합 연산의 결과값은 수학식 $s' \leftarrow (m \cdot s' \bmod n) \wedge (\sum_{i=\alpha}^{\rho-1} 2^i + (\overline{T} \oplus (d_p + d_q')))$ 에 의해 생성되는 것을 특징으로 한다.

<68> 그리고, 상기 제 1 논리 연산은 AND 연산이며, 상기 제 2 논리 연산은 XOR 연산인 것을 특징으로 한다.

<69> 한편, 상기 서명 인증값을 생성하는 단계는 상기 논리합 연산의 결과값과 상기 s가 동일하면 서명 인증값을 출력하고, 상기 논리합 연산의 결과값과 상기 s가 동일하지 않으면 오류 메시지를 출력하는 단계를 포함하는 것을 특징으로 한다.

<70> 아울러, 상기 s와 s'는 각각 병렬로 CRT 연산에 따라 생성되는 것을 특징으로 한다.

<71> 상기 두 번째 과제를 해결하기 위하여 본 발명은,

<72> 서로 다른 소수 p, q를 비밀키로, $n = pq$를 만족하는 n을 공개키로 euler totient 함수 $\Phi(n)$과 서로소인 소정의 정수 e를 공개키로, $ed = 1 \bmod \Phi(n)$을 만족하는 d를 비밀키로 이용하는 CRT-RSA 모듈라 지수승 알고리즘을 이용한 디지털 서명 장치에 있어서, 인증된 수신자에게 전송하고자 하는 메시지 m, 상기 서로 다른 소수 p, q, 상기 d를 $p-1$로 모듈라 연산한 d_p, 상기 d를 $q-1$로 모듈라 연산한 d_q, 상

기 d_p와 d_q의 합인 T, 상기 p^{-1}을 q로 모듈라 연산한 a가 입력되는 데이터 입력부; 상기 메시지 m을 암호화하고자 하는 송신자에 의해 랜덤한 정수 k가 선택되는 사용자 데이터 선택부; 상기 T와 d_q의 차에 따라 d_p'를 생성하고, 상기 메시지 m에 d_p'승한 값을 상기 p와 상기 정수 k를 곱한 값으로 모듈러 연산하여 s_p값을 산출하며, 상기 메시지 m에 $d_p'-1$승한 값을 상기 p와 상기 정수 k를 곱한 값으로 모듈러 연산하여 s_p'값을 산출하는 제 1 모듈라 지수승 연산부; 상기 T와 d_p의 차에 따라 d_q'를 생성하고, 상기 메시지 m에 d_q'승한 값을 상기 q와 상기 정수 k를 곱한 값으로 모듈러 연산하여 s_q 값을 산출하고, 상기 메시지 m에 $d_q'-1$승한 값을 상기 q와 상기 정수 k를 곱한 값으로 모듈러 연산하여 s_q'값을 산출하는 제 2 모듈라 지수승 연산부; 상기 연산된 s_p 및 s_p'로 이루어진 제 1 데이터 쌍을 이용하여 CRT 연산에 따라 s를 생성하는 제 1 CRT 연산부; 상기 연산된 s_q 및 s_q'로 이루어진 제 2 데이터 쌍을 이용하여 CRT 연산에 따라 s'를 생성하는 제 2 CRT 연산부; 상기 T의 비트 길이인 α와 모듈러 n의 비트 길이에 따라 생성되는 제 1 출력값과, d_p와 d_q'의 합에 상기 T의 보수 $\overline{T}$를 제 1 논리 연산을 수행한 제 2 출력값을 합하여 제 1 총합값을 생성하고, 상기 메시지 m과 s'를 곱한 값을 n으로 모듈라 연산하여 제 3 출력값을 생성하여, 상기 제 1 총합값과 제 3 출력값을 입력으로 제 2 논리 연산을 수행하여 논리합 연산의 결과값을 생성하는 비교값 생성부; 및 상기 논리합 연산의 결과값과 상기 s의 동일 여부에 따라 서명 인증값을 생성하는 제어부를 포함하는 CRT-RSA 모듈라 지수승 알고리즘을 이용한 디지털 서명 장치를 제공한다.

<73> 여기서, 상기 논리합 연산의 결과값은 수학식 $s' \leftarrow (m \cdot s' \bmod n) \wedge (\sum_{i=a}^{\alpha-1} 2^i + (\overline{T} \oplus (d_p + d_q')))$에 의해 생성되는 것을 특징으로 한다.

<74> 그리고, 상기 제 1 논리 연산은 AND 연산이며, 상기 제 2 논리 연산은 XOR 연산인 것을 특징으로 한다.

<75> 한편, 상기 제어부는 상기 논리합 연산의 결과값과 상기 s가 동일하면 서명 인증값을 출력하고, 상기 논리합 연산의 결과값과 상기 s가 동일하지 않으면 오류 메시지를 출력하는 것을 특징으로 한다.

<76> 상기 세 번째 과제를 해결하기 위하여 본 발명은, 상기 CRT-RSA 모듈라 지수승 알고리즘을 이용한 디지털 서명 방법을 컴퓨터에서 수행할 수 있는 프로그램으로 기록된 컴퓨터 판독 가능 저장 매체를 제공한다.

효 과

<77> 상술한 바와 같이 본 발명에 의하면, 단순한 레지스터의 추가에 의해 단순한 암호화 방법을 제공하며, 연산량 역시 종래의 암호화 방법에 비해 증가하지 않으면서도 최근 제시된 새로운 단순 전력 분석 및 오류 주입 공격에 안전성을 제공함으로써 스마트카드와 같은 내장형 장치에서도 효율적이고 안전한 디지털 서명 기법을 제공할 수 있는 효과가 있다.

발명의 실시를 위한 구체적인 내용

<78> 상술한 Giraud의 대응 방법에 대하여 새로운 오류 주입 공격 방법을 제시할 수 있다.

<79> 전술한 도 2에서 기존의 Giraud의 대응 방법에 대하여 d_p와 d_q에 오류가 주입되었을 때에도 안전하다고 주장되었으나, 도 2의 단계 2 또는 단계 3에서 d_p또는 d_q에 오류가 주입된 경우에는 안전하지 않다.

<80> d_p에 오류가 일시적으로 주입되었을 경우를 예를 들면 하기와 같다.

<81> 우선, 도 2의 단계 2에서 $(\hat{s_p}', s_p)$를 구하는 과정에서 d_p에 오류가 주입되었을 경우를 가정하면, 각 단계의 값은 하기의 수학식 7과 같다.

수학식 7

<82> $$(\hat{s}_p', \hat{s}_p) = (m^{\hat{d}_p - 1} \bmod k \cdot p, m^{\hat{d}_p} \bmod k \cdot p)$$

<83> 그리고, 도 2의 단계 3은 하기의 수학식 8과 같다.

수학식 8

<84> $$(s_q', s_q) = (m^{d_q - 1} \bmod k \cdot q, m^{d_q} \bmod k \cdot q)$$

<85> 그리고, 도 2의 단계 4에서는 $\hat{s}' = CRT(\hat{s}_p', s_q')$이고, 단계 5는 $\hat{s} = CRT(\hat{s}_p, s_q)$으로 연산 된다.

<86> 여기서, 상기 도 2의 알고리즘의 확인 과정은 $m\hat{s}' = \hat{s} \bmod n$이 되고 이는 하기의 수학식 9로 표현할 수 있다.

수학식 9

<87> $$m\hat{s}' = m_p \hat{s}_p' \bmod p$$
$$m\hat{s}' = m_q s_q' \bmod q$$

<88> 상기 수학식 9를 달리 표현하면 하기의 수학식 10으로 표현할 수 있다.

수학식 10

<89> $$\hat{s} = \hat{s}_p \bmod p$$
$$\hat{s} = s_q \bmod q$$

<90> 여기서, $m_p \hat{s}_p' \equiv \hat{s}_p \bmod p$이고, $m_q s_q' \equiv s_q \bmod q$ 이기 때문에 $m\hat{s}' \equiv \hat{s} \bmod n$을 만족하게 된다.

<91> 그리고, p, q, a역시 변경되지 않았기 때문에 상기 도 2의 단계 7을 통과하게 된다.

<92> 동일한 방법으로 d_q에서 오류가 발생하더라도 상기 도 2의 단계 7을 통과하게 된다. 즉, 두 번의 CRT 연산

과정에서 같은 오류의 값으로 연산되기 때문에 비교 과정에서 p, q, a에서의 오류 주입만 발생하지 않았다면 이에 대한 공격이 가능하게 된다.

<93> 따라서, Giraud가 제안한 대응 방법은 d_p와 d_q에서의 오류 주입에 대하여 공격이 가능하게 된다.

<94> 이에 따라 본 발명은, 상기 d_p와 d_q에서의 오류 주입에 대해서도 안전한 CRT-RSA 알고리즘을 제안하며, 이를 정리하면 도 3에 도시된 바와 같다.

<95> 본 발명에서는 전술한 상기 d_p와 d_q에서의 오류 주입에 대해서도 안전하게 구현될 수 있는 CRT-RSA 알고리즘을 제안한다.

<96> 종래의 CRT-RSA 알고리즘에 대하여 오류 주입에 따른 공격이 가능한 이유가 상기 도 2의 단계 2 또는 단계 3에서의 연산시 오류가 발생하더라도 (s_p', s_q')또는 (s_p, s_q)에 있어서 두 값 사이에 연결성이 유지되어 있기 때문이다.

<97> 따라서, 본 발명에서 제안하는 대응 방법은 (s_p', s_q')또는 (s_p, s_q)를 연산할 때의 오류를 확인하는 과정을 추가하여, 상기 도 2의 단계 7의 $s' = s$를 통과하지 못하게 된다.

<98> 본 발명은 종래의 CRT-RSA 방법과는 달리 입력 값이 $T(=d_p+d_q), d_p, d_q$이다.

<99> 도 4는 본 발명에 따른 CRT-RSA 모듈라 지수승 알고리즘을 이용한 디지털 서명 방법의 흐름도를 도시한 것이다.

<100> 우선, 서로 다른 소수 p, q를 비밀키로, $n = pq$를 만족하는 n을 공개키로 euler totient 함수 $\Phi(n)$과 서로 소인 소정의 정수 e를 공개키로, $ed = 1 \bmod \Phi(n)$을 만족하는 d를 비밀키로 이용하는 CRT-RSA 모듈라 지수승 알고리즘을 이용한 디지털 서명방법에 있어서, 인증된 수신자에게 전송하고자 하는 메시지 m, 상기 서로 다른 소수 p, q, 상기 d를 $p-1$로 모듈라 연산한 d_p, 상기 d를 $q-1$로 모듈라 연산한 d_q, 상기 d_p와 d_q의 합인 T, 상기 p^{-1}을 q로 모듈라 연산한 a 및 암호화하고자 하는 송신자에 의해 선택된 랜덤한 정수 k 를 수신한다(410 과정). 이는 암호화 파라미터들을 입력받는 과정으로, 상기 파라미터를 이용하여 CRT-RSA 모듈라 지수승 알고리즘에 따라 암호화가 수행되게 된다.

<101> 그 다음, 상기 T와 d_q의 차에 따라 d_p'를 생성하고, 상기 메시지 m에 d_p'승한 값을 상기 p와 상기 정수 k를 곱한 값으로 모듈러 연산하여 s_p값을 산출하며, 상기 메시지 m에 $d_p'-1$승한 값을 상기 p와 상기 정수 k를 곱한 값으로 모듈러 연산하여 s_p'값을 산출한다(420 과정).

<102> 이는, 도 1의 알고리즘에 따라 m, d_p', p, k와 $T-d_q$에 따른 d_p'을 입력으로 하여 s_p, s_p'를 산출하는 과정으로 본 발명은 T 및 d_p'를 사용하여 공격자의 오류 주입 공격과 단순 전력 분석 공격으로부터 안전한 CRT-RSA 모듈라 지수승 알고리즘을 제공할 수 있다.

<103> 그 다음, 상기 T와 d_p의 차에 따라 d_q'를 생성하고, 상기 메시지 m에 d_q'승한 값을 상기 q와 상기 정수 k를 곱한 값으로 모듈러 연산하여 s_q 값을 산출하고, 상기 메시지 m에 $d_q'-1$승한 값을 상기 q와 상기 정수 k를 곱한 값으로 모듈러 연산하여 s_q'값을 산출한다(430 과정).

<104> 마찬가지로, 도 1의 알고리즘에 따라 m, d_q', q, k와 $T-d_p$에 따른 d_q'을 입력으로 하여 s_q, s_q'를 산출하는 과정으로 본 발명은 T 및 d_q'를 사용하여 공격자의 오류 주입 공격과 단순 전력 분석 공격으로부터 안전한 CRT-RSA 모듈라 지수승 알고리즘을 제공할 수 있다.

<105> 즉, 이는 상기 420 과정에서 입력 값은 $m,\ d_p'(=T-d_p),\ p,\ k$가 되고, 단계 430 과정에서 입력 값은 $m,\ d_q'(=T-d_p'),\ q,\ k$ 이다.

<106> 그 다음, 상기 연산된 s_p 및 s_p'로 이루어진 제 1 데이터 쌍을 이용하여 s를 생성하고, 상기 연산된 s_q 및 s_q'로 이루어진 제 2 데이터 쌍을 이용하여 s'를 생성한다(440 과정).

<107> 여기서, s는 상기 연산된 s_p 및 s_q로 이루어진 제 1 데이터 쌍을 이용하여 하기의 수학식 11에 의하여 생성될 수 있고, s'는 상기 연산된 s_p' 및 s_q'로 이루어진 제 2 데이터 쌍을 이용하여 하기의 수학식 12에 의하여 생성될 수 있다.

수학식 11

<108> $$s' = CRT_{blinded}(s_p', s_q') = (((s_q' - s_p') \bmod kq)) \cdot (a \bmod kq)) \cdot p + s_p' \bmod pq$$

수학식 12

<109> $$s = CRT_{blinded}(s_p, s_q) = (((s_q - s_p) \bmod kq)) \cdot (a \bmod kq)) \cdot p + s_p \bmod pq$$

<110> 본 $CRT_{blinded}(s_p, s_q)$연산은 기존의 CRT 연산과 유사한 방법으로 계산되며, $\bmod kp$와 $\bmod kq$의 결과값을 $\bmod pq$로 수정하는 과정이 추가된 것이다.

<111> 그 다음, 상기 T의 비트 길이인 α와 모듈러 n의 비트 길이에 따라 생성되는 제 1 출력값과, d_p와 d_q'의 합에 상기 T의 보수 $\overline{T}$를 제 1 논리 연산을 수행한 제 2 출력값을 합하여 제 1 총합값을 생성하고, 상기 메시지 m과 s'를 곱한 값을 n으로 모듈라 연산하여 제 3 출력값을 생성하여, 상기 제 1 총합값과 제 3 출력값을 입력으로 제 2 논리 연산을 수행하여 논리합 연산의 결과값을 생성한다(450 과정).

<112> 이는, $m \cdot s' \bmod n$의 값과 $(\sum_{i=\alpha}^{\rho-1} 2^i + (\overline{T} \oplus (d_p + d_q')))$의 값을 AND 연산하게 된다.

<113> 이때, $\overline{T}$의 값은 T의 보수 값이고, α는 T의 비트 길이, ρ는 모듈러 n의 비트 길이이다.

<114> 또한, $\sum_{i=\alpha}^{\rho-1} 2^i$은 AND 연산을 위한 비트 길이를 맞추는 패딩 연산이다. $m \cdot s' \bmod n$의 결과 값에 대한 비트 길이는 모듈러 n의 비트 길이인 ρ이고, $(\sum_{i=\alpha}^{\rho-1} 2^i + (\overline{T} \oplus (d_p + d_q')))$의 결과 값에 대한 비트 길이는 T의 비트 길이인 α이다.

<115> 따라서, $\rho \leq \alpha$이므로, 상기 논리합 연산의 결과 값을 생성하는 연산은 비트 차이만큼 '1'이 채워지는 연산에 해당한다.

<116> 여기서, 오류가 주입되지 않았을 경우는 $T(d_p + d_q)$ 값과 $d_p + d_q'$의 값이 동일하므로, $\oplus\,(XOR)$연산의 결과 $2^{\alpha} - 1$이고, 패딩 연산 후의 결과 값은 $\sum_{i=\alpha}^{\rho-1} 2^i + 2^{\alpha} - 1 = 2^{\rho} - 2^{\alpha} + 2^{\alpha} - 1 = 2^{\rho} - 1$이 된다.

<117> 따라서, $m \cdot s' \bmod n$ 값과 비트 길이가 $\rho - 1$인 $2^{\rho}-1 (=111\cdots1)$을 AND 연산을 하게 되면, 그 결과 값은 기존의 $m \cdot s' \bmod n$ 값이 된다.

<118> 한편, 450 과정에서의 상기 논리합 연산의 결과값 s'는 하기의 수학식 13에 의해 생성될 수 있다.

수학식 13

<119> $$s' \leftarrow (m \cdot s' \bmod n) \wedge (\sum_{i=\alpha}^{\rho-1} 2^i + (\overline{T} \oplus (d_p + d_q')))$$

<120> 상기 수학식 13의 각각의 변수는 전술한 바와 동일하므로 중복된 상술은 생략하기로 하며, 상기 수학식 13에서 $\oplus$는 논리 연산 중 XOR 연산을 의미하며, $\wedge$는 논리 연산 중 AND 연산을 의미한다.

<121> 마지막으로, 상기 논리합 연산의 결과값과 상기 s의 동일 여부에 따라 서명 인증값을 생성한다(460 과정).

<122> 여기서, 상기 논리합 연산의 결과값 s'는 상기 440 과정의 CRT 연산에 의한 s'에 m을 곱한 값이므로, 공격자의 공격에 의하여 오류가 발생하지 않았을 경우에는 상기 논리합 연산의 결과값 s'와 상기 s는 동일하여야 한다.

<123> 따라서, 상기 논리합 연산의 결과값 s'와 s가 동일한 경우에는 공격자에 의한 공격을 받지 않은 것으로 판단할 수 있고, 이에 따른 사용자의 서명 인증값을 생성하게 되고, 상기 논리합 연산의 결과값 s'와 s가 동일하지 않을 경우에는 공격자에 의한 공격을 받은 것이므로 사용자의 서명 인증값을 생성하지 않고 오류 메시지를 출력하게 된다.

<124> 이와 같이, 상기 오류가 발생하지 않은 경우는 본 발명의 160 과정을 통과하게 되어 올바른 서명 값을 출력하게 된다. 오류가 발생할 수 있는 경우는 입력 값과 중간 연산 결과 값이다. 즉, 이는

$m, p, q, T, d_p, d_q, a, s_p', s_p, s_q', s_q, s', s, k$ 이다.

<125> 여기서 오류가 발생할 수 있는 경우를 살펴보면 하기와 같다.

<126> 첫 번째는 , 상기 420 과정의 연산시 d_q에 오류가 발생하였을 경우이다.

<127> 이는 $\widehat{d_q}$의 경우 d_p'의 값도 오류가 발생하게 되고, 430 과정에서의 입력 값 d_p'에 오류가 주입되었기 때문에 s_p, s_p', s_q, s_q' 모두 오류가 주입된 값이므로 공격자가 올바르지 않는 값을 이용하여 p또는 q를 얻을 수 없다.

<128> 두 번째는, 상기 430 과정에서의 d_p 의 메모리에 오류가 발생하였을 경우이다.

<129> 이와 같은 경우는, 상기 첫 번째의 경우와 동일하게 s_p, s_p', s_q, s_q' 모두 오류가 주입된 값이므로 공격자가 올바르지 않는 값을 이용하여 p또는 q를 얻지 못한다.

<130> 세 번째는, 상기 430 과정에서의 연산시에 d_p'에 오류가 발생하였을 경우이다.

<131> 이는 첫 번째 오류와는 달리 d_p'에 오류가 발생하는 경우 $\widehat{d_p'}$가 되며, 첫 번째 경우와는 달리 오류 확산이 일어나지 않는다. 따라서 별도로 확인하는 과정이 필요하다.

<132> 이는 450 과정에서 $(\sum_{i=a}^{p-1} 2^i + (\overline{T} \oplus (d_p + d'_q)))$를 연산하는 것이다. $(\overline{T} \oplus (d_p + \widehat{d}_q'))$의 값의 모든 비트가 '1'이 아니기 때문에 상기 450 연산의 결과 값인 s'가 s와 달라지기 때문에 상기 460 과정을 통과하지 못한다.

<133> 그 다음 네 번째는, 일시적인 T 의 오류이다.

<134> 이는 일시적으로 T에 오류가 발생하였을 경우에는 첫 번째 분석과 동일하게 오류 확산이 일어나기 때문에 공격이 불가능하다. 또한 430 과정에서의 T 의 일시적 오류인 경우에도 두 번째 분석과 동일하게 460 과정을 통과하지 못한다.

<135> 그 다음 다섯 번째는 지속적인 T 의 오류이다.

<136> 이는 지속적으로 T에 오류가 발생하였을 경우 d_p'는 오류가 주입된 값이 되지만, d_q'의 값은 올바른 값이 된다. 따라서, T 의 오류를 확인하는 과정이 없다면 공격자는 공격을 성공하게 된다. T의 오류 확인 과정도 상기 450 과정에서 $(\overline{T} \oplus (d_p + d'_q))$을 이용한다. $(d_p + d'_q)$는 기존의 오류가 주입되지 않은 T 값과 동일하지만, 오류가 주입된 $\overline{T}$와 달라지므로 상기 460 과정을 통과하지 못하게 된다.

<137> 다른 오류가 주입되었을 경우에는, 기존의 Giraud의 방법의 분석과 동일하게 된다. 따라서 본 발명에서 제안하는 대응 방법은 상기 420 과정 및 430 과정에서의 입력 값에 대한 일시적인 오류까지 안전한 방법이다.

<138> 본 대응 방법은 기존의 방법보다 세 개의 레지스터 d_p', d_q', T를 추가 사용하고, 상기 420 과정 및 430 과정에서의 두 번의 뺄셈 연산, 450 과정에서의 두 번의 덧셈 연산, AND 연산과 XOR 연산 만을 추가하여 공격자의 오류 주입에 대응하게 된다.

<139> 따라서, 본 발명에서는 오류 주입 공격과 단순 전력 분석 공격에 안전하다고 제안된 Giraud의 대응 방법에 대한 장점을 모두 취하며, 세 개의 레지스터를 더 요구하며 추가적인 연산으로 덧셈, 뺄셈 연산 그리고 XOR, AND 연산을 사용한다.

<140> 모듈러 지수성 연산에 필요한 연산량에 비교하면, 크게 고려하지 않아도 되는 추가 연산량이다. 따라서, 본 발명에 따르면 연산 능력과 메모리가 제안된 모든 환경에서 안전하게 이용될 수 있는 장점이 있다.

<141> 도 5는 본 발명에 따른 CRT-RSA 모듈라 지수승 알고리즘을 이용한 디지털 서명 장치의 블록도를 도시한 것이다.

<142> 도 5를 참조하면, 본 발명에 따른 CRT-RSA 모듈라 지수승 알고리즘을 이용한 디지털 서명 장치는, 데이터 입력부(510), 사용자 데이터 선택부(520), 제 1 모듈라 지수승 연산부(531), 제 2 모듈라 지수승 연산부(532), 제 1 CRT 연산부(541), 제 2 CRT 연산부(542), 비교값 생성부(550) 및 제어부(560)으로 이루어질 수 있다.

<143> 서로 다른 소수 p, q를 비밀키로, $n = pq$를 만족하는 n을 공개키로 euler totient 함수 $\Phi(n)$과 서로소인 소정의 정수 e를 공개키로, $ed = 1 \bmod \Phi(n)$을 만족하는 d를 비밀키로 이용하는 CRT-RSA 모듈라 지수승 알고리즘을 이용한 디지털 서명 장치에 있어서, 데이터 입력부(510)는 인증된 수신자에게 전송하고자 하는 메시지 m, 상기 서로 다른 소수 p, q, 상기 d를 $p-1$로 모듈라 연산한 d_p, 상기 d를 $q-1$로 모듈라 연산한 d_q, 상기 d_p와 d_q의 합인 T, 상기 p^{-1}을 q로 모듈라 연산한 a가 사용자에 의해 입력된다.

<144> 그리고, 사용자 데이터 선택부(520)는 상기 메시지 m을 암호화하고자 하는 송신자에 의해 랜덤한 정수 k가 선택되어 진다.

<145> 제 1 모듈라 지수승 연산부(531)는 상기 T와 d_q의 차에 따라 d_p'를 생성하고, 상기 메시지 m에 d_p'승한 값을 상기 p와 상기 정수 k를 곱한 값으로 모듈러 연산하여 s_p값을 산출하며, 상기 메시지 m에 $d_p'-1$승한 값을 상기 p와 상기 정수 k를 곱한 값으로 모듈러 연산하여 s_p'값을 산출한다.

<146> 제 2 모듈라 지수승 연산부(532)는 상기 T와 d_p의 차에 따라 d_q'를 생성하고, 상기 메시지 m에 d_q'승한 값을 상기 q와 상기 정수 k를 곱한 값으로 모듈러 연산하여 s_q값을 산출하고, 상기 메시지 m에 $d_q'-1$승한 값을 상기 q와 상기 정수 k를 곱한 값으로 모듈러 연산하여 s_q'값을 산출한다.

<147> 여기서, 상기 제 1 모듈라 지수승 연산부(531)와 제 2 모듈라 지수승 연산부(532)는 병렬 연결되어 연산되므로 병렬 연산에 의해 연산 속도를 향상시킬 수 있다.

<148> 한편, 제 1 CRT 연산부(541)는 상기 연산된 s_p 및 s_p'로 이루어진 제 1 데이터 쌍을 이용하여 CRT 연산에

따라 s를 생성한다.

<149> 그리고, 제 2 CRT 연산부(542)는 상기 연산된 s_q 및 $s_q{}'$로 이루어진 제 2 데이터 쌍을 이용하여 CRT 연산에 따라 s'를 생성한다.

<150> 비교값 생성부(550)는 상기 T의 비트 길이인 α와 모듈러 n의 비트 길이에 따라 생성되는 제 1 출력값과, d_p와 $d_q{}'$의 합에 상기 T의 보수 $\overline{T}$를 제 1 논리 연산을 수행한 제 2 출력값을 합하여 제 1 총합값을 생성하고, 상기 메시지 m과 s'를 곱한 값을 n으로 모듈라 연산하여 제 3 출력값을 생성하여, 상기 제 1 총합값과 제 3 출력값을 입력으로 제 2 논리 연산을 수행하여 논리합 연산의 결과값을 생성한다.

<151> 여기서, 상기 논리합 연산의 결과값은 상기 수학식 11에 의해 생성되며, 상기 제 1 논리 연산은 AND 연산이며, 상기 제 2 논리 연산은 XOR 연산일 수 있다.

<152> 그리고, 제어부(560)는 상기 논리합 연산의 결과값과 상기 s의 동일 여부에 따라 서명 인증값을 생성한다.

<153> 상기 제어부(560)는 상기 논리합 연산의 결과값과 상기 s가 동일하면 서명 인증값을 출력하고, 상기 논리합 연산의 결과값과 상기 s가 동일하지 않으면 오류 메시지를 출력할 수 있다.

<154> 이와 같이, 본 발명은 기존의 암호화 장치보다 세 개의 레지스터 $d_p{}'$, $d_q{}'$, T만을 추가적으로 사용함으로써, 제 1 모듈라 지수승 연산부(531)와 제 2 모듈라 지수승 연산부(532)에서 수행되는 두 번의 뺄셈 연산, 비교값 생성부(550)에서의 두 번의 덧셈 연산, AND 연산 및 XOR 연산 만을 추가하여 공격자의 오류 주입 공격과 단순 전력 분석 공격에 모두 안전한 CRT-RSA 모듈라 지수승 알고리즘을 이용한 디지털 서명 장치를 제공할 수 있다.

<155> 본 발명에 따른 CRT-RSA 모듈라 지수승 알고리즘을 이용한 디지털 서명 방법은 컴퓨터 판독 가능 저장 매체를 통하여 실행될 수 있다.

<156> 컴퓨터 판독 가능 저장 매체로 실행될 때, 본 발명의 구성 수단들은 필요한 작업을 수행하는 코드 세그먼트(code segment)들이다.

<157> 상기 코드 세그먼트들은 프로세서 판독 가능 매체에 저장되거나 전송 매체 또는 통신망에서 반송파와 결합된 컴퓨터 데이터 신호에 의하여 전송될 수 있다.

<158> 컴퓨터가 읽을 수 있는 저장 매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 저장 매체의 예로는 ROM, RAM, CD-ROM, DVD±ROM, DVD-RAM, 자기 테이프, 플로피 디스크, 하드 디스크(hard disk), 광데이터 저장장치 등이 있다.

<159> 또한, 컴퓨터가 읽을 수 있는 저장 매체는 네트워크로 연결된 컴퓨터 장치에 분산되어 분산방시으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

<160> 본 발명은 도면에 도시된 일 실시예를 참고로 하여 설명하였으나 이는 예시적인 것에 불과하며, 당해 분야에서 통상의 지식을 가진 자라면 이로부터 다양한 변형적인 것에 불과하며 당해 분야에서 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 실시예의 변형이 가능하다는 점을 이해할 것이다.

<161> 그러나, 이와 같은 변형은 본 발명의 기술적 보호범위 내에 있다고 보아야 한다.

<162> 따라서, 본 발명의 진정한 기술적 보호범위는 첨부된 특허청구범위의 기술적 사상에 의해서 정해져야 할 것이다.

도면의 간단한 설명

<163> 도 1은 종래의 모듈러 지수승 알고리즘을 도시한 것이다.

<164> 도 2는 Giraud의 종래의 단순 전력 분석 및 오류 주입 공격에 안전한 모듈러 지수승 알고리즘을 도시한 것이다.

<165> 도 3은 본 발명에 따른 모듈러 지수승 알고리즘을 도시한 것이다.

<166> 도 4는 본 발명에 따른 CRT-RSA 모듈라 지수승 알고리즘을 이용한 디지털 서명 방법의 흐름도를 도시한 것이다.

<167> 도 5는 본 발명에 따른 CRT-RSA 모듈라 지수승 알고리즘을 이용한 디지털 서명 장치의 블록도를 도시한 것이다.

도면

도면1

Algorithm1. Giraud의 모듈러 지수승 알고리즘

INPUT $m, d, oddN, k$

OUTPUT $(m^{d-1} \bmod kN, m^{d} \bmod kN)$

1. $a_0 \leftarrow m$
2. $a_1 \leftarrow a_0^2 \bmod kN$
3. for i from $n-2$ to 1 do
   - 3.1. $a_{\overline{d_i}} \leftarrow a_{\overline{d_i}} \cdot a_{d_i} \bmod kN$
   - 3.2. $a_{d_i} \leftarrow a_{d_i}^2 \bmod kN$
4. $a_1 \leftarrow a_1 \cdot a_0 \bmod kN$
5. $a_1 \leftarrow a_0^2 \bmod kN$
6. if (Loop Counter i not disturbed) & (Exponent d not disturbed) then return (a_0, a_1) else return(error)

도면2

Algorithm2. Giraud의 대응방법

INPUT $m, p, q, d_p, d_q, a(=p^{-1} \bmod q)$;

OUTPUT $m^{d} \bmod n$;

1. random integer k
2. $(s_p', s_p) \leftarrow Algorithm\,1(m, d_p, p, k)$
3. $(s_q', s_q) \leftarrow Algorithm\,1(m, d_q, q, k)$
4. $s' \leftarrow CRT_{blinded}(s_p', s_q')$
5. $s \leftarrow CRT_{blinded}(s_p, s_q)$
6. $s' \leftarrow m \cdot s' \bmod n$
7. if ($s' = s$) and (parameters p, q, a not modified) then return s else return (error)

도면3

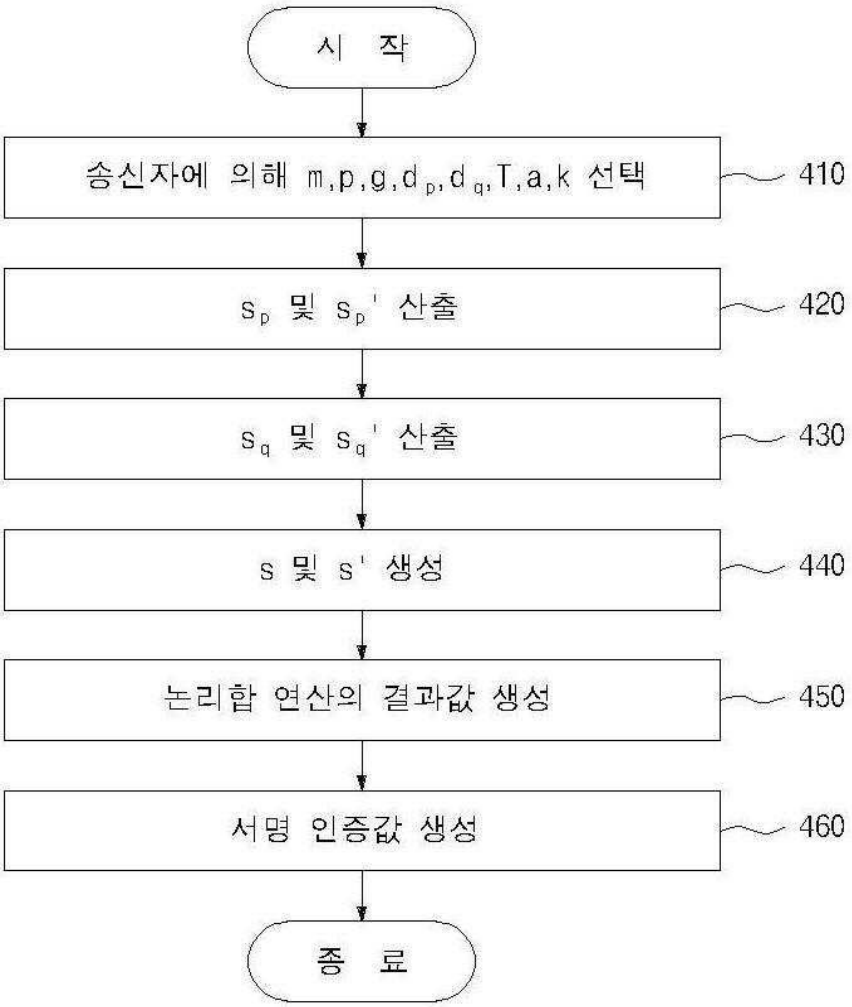
Algorithm3. 본 발명에 따른 대응 방법

INPUT $m, p, q, T(=d_p+d_q), d_p, d_q, a(=p^{-1} \bmod q)$;

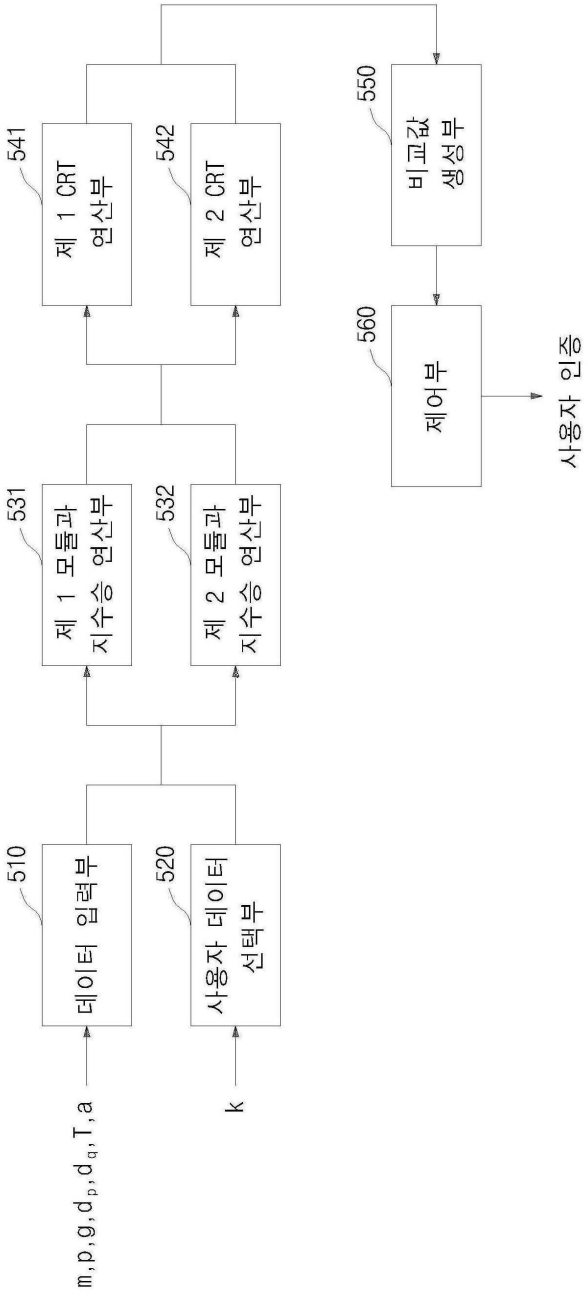
OUTPUT $m^d \bmod n$;

1. random integer k
2. $(s_p', s_p) \leftarrow Algorithm1(m, d_p', p, k),\ d_p' = T - d_q$
3. $(s_q', s_q) \leftarrow Algorithm1(m, d_q', q, k),\ d_q' = T - d_p'$
4. $s' \leftarrow CRT_{blinded}(s_p', s_q')$
5. $s \leftarrow CRT_{blinded}(s_p, s_q)$
6. $s' \leftarrow (m \cdot s' \bmod n) \wedge (\sum_{i=a}^{\rho-1} 2^i + (\overline{T} \oplus (d_p + d_q')))$
7. if ($s' = s$) and (parameters p, q, a not modified) then return s else return (error)

도면4



도면5


510
데이터 입력부
520
사용자 데이터 선택부
531
제 1 모듈과 지수승 연산부
532
제 2 모듈과 지수승 연산부
541
제 1 CRT 연산부
542
제 2 CRT 연산부
550
비교값 생성부
560
제어부
사용자 인증
m,p,g,d_p,d_q,T,a
k