



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2011-0109467
(43) 공개일자 2011년10월06일

(51) Int. Cl.

H04L 9/32 (2006.01) H04L 9/28 (2006.01)

(21) 출원번호 10-2010-0029227

(22) 출원일자 2010년03월31일

심사청구일자 2010년03월31일

(71) 출원인

고려대학교 산학협력단

서울 성북구 안암동5가 1

(72) 발명자

홍석희

서울특별시 도봉구 도봉2동 한신아파트 103-107

김성경

서울 성북구 안암동2가 118-2번지 SM빌딩 606호

(74) 대리인

특허법인충현

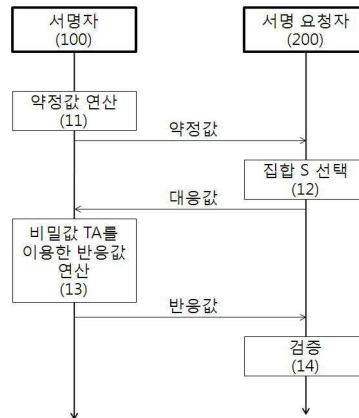
전체 청구항 수 : 총 12 항

(54) 오류주입 공격에 안전한 피아트 샤미르 개인 식별 장치, 방법 및 그 기록 매체

(57) 요약

오류주입 공격에 안전한 피아트 샤미르 개인 식별 장치, 방법 및 그 기록 매체가 개시된다. 본 발명의 일 실시예에 따른 오류주입 공격에 안전한 피아트 샤미르 개인 식별 장치는 비밀키 $s_1, s_2, \dots, s_t \bmod N$ 과 비밀값 T_A 를 저장하는 메모리부; 랜덤값 r 을 이용하여 $x = r^2 \bmod N$ 을 연산하고 상기 서명 요청자에 전송하는 약정값 전송부; 상기 서명 요청자에서 정수 l 이하의 자연수로 이루어진 집합 중 랜덤하게 선택된 부분 집합 S 를 수신하는 대응값 수신부; 및 상기 비밀값 T_A 및 상기 부분 집합 S 의 원소를 이용하여 반응값을 연산하고 상기 서명 요청자에 전송하는 반응값 전송부를 포함한다.

대표도 - 도2



특허청구의 범위

청구항 1

N을 공개값으로 하고, 알려진 정수 l, t ($1 \leq t$)에 대해 $PK_l = \{u_i | u_i = s_i^2 \bmod N, 1 \leq i \leq t\}$ 를 공개키로 하는 경우, 비밀키 $s_1, s_2, \dots, s_t \bmod N$ 과 비밀값 T_A 를 저장하는 서명자에서 랜덤값 r 을 이용하여 $x = r^2 \bmod N$ 을 연산하고 서명 요청자에 전송하는 단계;

상기 서명 요청자에서 정수 l 이하의 자연수로 이루어진 집합 중 랜덤하게 선택된 부분 집합 S 를 상기 서명자가 수신하는 단계;

상기 서명자에서 상기 비밀값 T_A 및 상기 부분 집합 S 의 원소를 이용하여 반응값을 연산하고 상기 서명 요청자에 전송하여, 상기 서명 요청자가 y^2 과 $x \cdot \prod_{i \in S} u_i \bmod N$ 을 비교하여 상기 서명자를 검증하게 하는 단계를 포함하는, 오류주입 공격에 안전한 피아트 샤미르 개인 식별 방법.

청구항 2

제 1 항에 있어서,

상기 비밀값 T_A 는 $\prod_{i=1}^t s_i$ 인 것을 특징으로 하는, 오류주입 공격에 안전한 피아트 샤미르 개인 식별 방법.

청구항 3

제 1 항에 있어서,

상기 반응값은 $y = r \frac{T_A}{\prod_{i=1, i \notin S}^t s_i} \bmod N$ 인 것을 특징으로 하는, 오류주입 공격에 안전한 피아트 샤미르 개인 식별 방법.

청구항 4

제 1 항에 있어서,

N은 비밀키 p 와 q 의 곱이고, p 와 q 는 서로 다른 소수인 것을 특징으로 하는, 오류주입 공격에 안전한 피아트 샤미르 개인 식별 방법.

청구항 5

제 1 항에 있어서,

s_i 와 N의 최대 공약수는 1인 것을 특징으로 하는, 오류주입 공격에 안전한 피아트 샤미르 개인 식별 방법.

청구항 6

N을 공개값으로 하고, $v_i = s_i^2 \bmod N$ ($1 \leq i \leq t$)를 공개키로 하는 경우, 비밀키 $s_1, s_2, \dots, s_t \bmod N$ 과 비밀값 $T_A = \prod_{i=1}^t s_i$ 을 저장하는 서명자에서 랜덤값 r 및 $s \in \{-1, 1\}$ 를 이용하여 $x = sr^2 \bmod N$ 을 연산하여 서명 요청자에 전송하는 단계;

상기 서명 요청자에서 선택된 집합 $S = \{a_i | a_i \in \{0, 1\}, 1 \leq i \leq t\}$ 를 상기 서명자가 수신하는 단계;

상기 서명자에서 상기 비밀값 T_A 및 상기 집합 S 의 원소를 이용하여 반응값을 연산하고 상기 서명 요청자에 전송

하여, 상기 서명 요청자에서 y^2 과 $\pm x(v_1^{a_1}v_2^{a_2}\cdots v_t^{a_t}) \bmod N$ 을 비교하여 상기 서명자를 검증하게 하는 단계

를 포함하는, 오류주입 공격에 안전한 피아트 샤미르 개인 식별 방법.

청구항 7

제 6 항에 있어서,

상기 비밀값 T_A 는 $\prod_{i=1}^t s_i$ 인 것을 특징으로 하는, 오류주입 공격에 안전한 피아트 샤미르 개인 식별 방법.

청구항 8

제 6 항에 있어서,

상기 반응값은 $y = rT_A/(s_1^{\bar{a}_1}s_2^{\bar{a}_2}\cdots s_t^{\bar{a}_t})$ 인 것을 특징으로 하는, 오류주입 공격에 안전한 피아트 샤미르 개인 식별 방법.

청구항 9

제 6 항에 있어서,

s_i 와 N 의 최대 공약수는 1인 것을 특징으로 하는, 오류주입 공격에 안전한 피아트 샤미르 개인 식별 방법.

청구항 10

제1항 내지 제9항 중 어느 한 항의 방법을 컴퓨터 시스템에서 실행하기 위한 프로그램이 기록된, 컴퓨터 시스템이 판독할 수 있는 기록매체.

청구항 11

서명자 요청자에 반응값을 전송하여 자신을 식별하게 하는 장치에 있어서,

N 을 공개값으로 하고, 알려진 정수 l, t ($1 \leq t$)에 대해 $PK_l = \{u_i | u_i = s_i^2 \bmod N, 1 \leq i \leq t\}$ 를 공개키로 하는 경우, 비밀키 $s_1, s_2, \cdots, s_t \bmod N$ 과 비밀값 T_A 를 저장하는 메모리부;

랜덤값 r 을 이용하여 $x = r^2 \bmod N$ 을 연산하고 상기 서명 요청자에 전송하는 약정값 전송부;

상기 서명 요청자에서 정수 l 이하의 자연수로 이루어진 집합 중 랜덤하게 선택된 부분 집합 S 를 수신하는 대응값 수신부; 및

상기 비밀값 T_A 및 상기 부분 집합 S 의 원소를 이용하여 반응값을 연산하고 상기 서명 요청자에 전송하는 반응값 전송부

를 포함하는, 오류주입 공격에 안전한 피아트 샤미르 개인 식별 장치.

청구항 12

서명자 요청자에 반응값을 전송하여 자신을 식별하게 하는 장치에 있어서,

N 을 공개값으로 하고, $v_i = s_i^2 \bmod N$ ($1 \leq i \leq t$)를 공개키로 하는 경우, 비밀키 $s_1, s_2, \cdots, s_t \bmod N$ 과 비밀값 T_A 를 저장하는 메모리부;

랜덤값 r 및 $s \in \{-1, 1\}$ 를 이용하여 $x = sr^2 \bmod N$ 을 연산하고 상기 서명 요청자에 전송하는 약정값 전송부;

상기 서명 요청자에서 선택된 집합 $S = \{a_i | a_i \in \{0, 1\}, 1 \leq i \leq t\}$ 를 수신하는 대응값 수신부; 및

상기 비밀값 T_A 및 상기 집합 S 의 원소를 이용하여 반응값을 연산하고 상기 서명 요청자에 전송하는 반응값 전송부

를 포함하는, 오류주입 공격에 안전한 피아트 샤미르 개인 식별 장치.

명세서

기술분야

[0001] 본 발명은 표준으로 권장하고 있는 개인 식별 (Identification) 프로토콜인 피아트 샤미르 기법 (Fiat-Shamir scheme)에 관한 것으로, 특히, 오류주입 공격에 안전한 피아트 샤미르 개인 식별 장치, 방법 및 그 기록 매체에 관한 것이다.

배경기술

[0002] 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.

[0003] 전송되는 내용을 암호화하여 전송하는 방식에는 대칭키 암호화 방식과 공개키 암호화 방식이 있고, 공개키 암호화 방식 중에서 현재 인터넷이나 금융계 등에서 표준으로 선택되어 널리 사용되고 있는 방식으로는 RSA(Rivest Shamir Adleman) 공개키 암호화 방식이 있다. RSA 공개키 암호화 방식은 Rivest, Shamir 및 Adleman에 의해 제안된 방식으로 암호문에 따른 데이터의 크기가 커질수록 소인수 분해가 어렵다는 점에 그 안전도의 기반을 두고 있다.

[0004] 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.

[0005] 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.

[0006] 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.

[0007] 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. 최근 Giraud가 처음으로 전력 분석 공격 방법 중 하나인 단순 전력 공격 분석과 오류 주입 공격에 안전한 방법을 제안하였다.

[0008] Giraud 방법에서의 지수승 알고리즘은 단순 전력 분석과 오류 주입 공격에 안전한 몽고메리 레더(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.

[0009] 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. 예를 들어, 개인키 d , 및 메시지 m 에 대한 RSA 서명값 s 는 $m^d \bmod n$ 이다. 여기서 n 은 공개 모듈라값이고, 비밀값인 큰 소수 p 와 q 의 곱으로 연산된다. 한편, 암호화 표준에서는 RSA 서명 생성과정의 속도를 향상하기 위하여 중국인의 나머지 정리(CRT)를 이용한 RSA 암호 시스템(CRT-RSA)을 사용하기를 권고하고 있다.

[0010] 최근 암호 알고리즘뿐 아니라 개인 식별 프로토콜인 피아트 샤미르 기법에도 오류 주입 공격 방법이 소개되었다. 하지만 현재 대응방법이 나와있지 않은 상태이다.

발명의 내용

해결하려는 과제

[0011] 본 발명이 이루고자 하는 첫 번째 기술적 과제는 악의적인 공격자의 분석을 어렵게 하는 비밀값을 반응 과정에 반영하는, 오류주입 공격에 안전한 피아트 샤미르 개인 식별 장치를 제공하는 데 있다.

[0012] 본 발명이 이루고자 하는 두 번째 기술적 과제는 상기의 피아트 샤미르 개인 식별 장치에 적용되는 오류주입 공격에 안전한 피아트 샤미르 개인 식별 방법을 제공하는 데 있다.

[0013] 본 발명이 이루고자 하는 세 번째 기술적 과제는 상기의 오류주입 공격에 안전한 피아트 샤미르 개인 식별 방법을 컴퓨터에서 실행시키기 위한 프로그램을 컴퓨터로 읽을 수 있는 기록매체를 제공하는 데 있다.

과제의 해결 수단

[0014] 본 발명의 일 실시 예에 따른 오류주입 공격에 안전한 피아트 샤미르 개인 식별 장치는 비밀키 $s_1, s_2, \dots, s_t \bmod N$ 과 비밀값 T_A 를 저장하는 메모리부; 랜덤값 r 을 이용하여 $x = r^2 \bmod N$ 을 연산하고 상기 서명 요청자에 전송하는 약정값 전송부; 상기 서명 요청자에서 정수 l 이하의 자연수로 이루어진 집합 중 랜덤하게 선택된 부분 집합 S 를 수신하는 대응값 수신부; 및 상기 비밀값 T_A 및 상기 부분 집합 S 의 원소를 이용하여 반응값을 연산하고 상기 서명 요청자에 전송하는 반응값 전송부를 포함한다.

[0015] 또한, 본 발명의 다른 실시 예에 따른 오류주입 공격에 안전한 피아트 샤미르 개인 식별 장치는 비밀키 $s_1, s_2, \dots, s_t \bmod N$ 과 비밀값 T_A 를 저장하는 메모리부; 랜덤값 r 및 $s \in \{-1, 1\}$ 을 이용하여 $x = sr^2 \bmod N$ 을 연산하고 상기 서명 요청자에 전송하는 약정값 전송부; 상기 서명 요청자에서 선택된 집합 $S = \{a_i | a_i \in \{0, 1\}, 1 \leq i \leq t\}$ 를 수신하는 대응값 수신부; 및 상기 비밀값 T_A 및 상기 집합 S 의 원소를 이용하여 반응값을 연산하고 상기 서명 요청자에 전송하는 반응값 전송부를 포함한다.

[0016] 또한, 본 발명의 일 실시 예에 따른 오류주입 공격에 안전한 피아트 샤미르 개인 식별 방법은 비밀키 $s_1, s_2, \dots, s_t \bmod N$ 과 비밀값 T_A 를 저장하는 서명자에서 랜덤값 r 을 이용하여 $x = r^2 \bmod N$ 을 연산하고 서명 요청자에 전송하는 단계; 상기 서명 요청자에서 정수 l 이하의 자연수로 이루어진 집합 중 랜덤하게 선택된 부분 집합 S 를 상기 서명자가 수신하는 단계; 상기 서명자에서 상기 비밀값 T_A 및 상기 부분 집합 S 의 원소를 이용하여 반응값을 연산하고 상기 서명 요청자에 전송하여, 상기 서명 요청자가 y^2 과 $x \cdot \prod_{i \in S} u_i \bmod N$ 을 비교하여 상기 서명자를 검증하게 하는 단계를 포함한다.

[0017] 또한, 본 발명의 다른 실시 예에 따른 오류주입 공격에 안전한 피아트 샤미르 개인 식별 방법은 비밀키 $s_1, s_2, \dots, s_t \bmod N$ 과 비밀값 $T_A = \prod_{i=1}^t s_i$ 을 저장하는 서명자에서 랜덤값 r 및 $s \in \{-1, 1\}$ 을 이용하여 $x = sr^2 \bmod N$ 을 연산하여 서명 요청자에 전송하는 단계; 상기 서명 요청자에서 선택된 집합 $S = \{a_i | a_i \in \{0, 1\}, 1 \leq i \leq t\}$ 를 상기 서명자가 수신하는 단계; 상기 서명자에서 상기 비밀값 T_A 및 상기 집합 S 의 원소를 이용하여 반응값을 연산하고 상기 서명 요청자에 전송하여, 상기 서명 요청자에서 y^2 과 $\pm x(v_1^{a_1} v_2^{a_2} \dots v_t^{a_t}) \bmod N$ 을 비교하여 상기 서명자를 검증하게 하는 단계를 포함한다.

발명의 효과

[0018] 본 발명의 실시 예들에 의하면, 피아트 샤미르 기법을 이용하여 개인 식별을 하는 경우, 큰 연산량의 증가없이, 비밀 정보의 값을 알아내지 못하게 공격자가 알지 못하는 값을 반응값에 반영하여 공격자의 분석을 어렵게 하여 오류 주입 공격에 안전하다.

도면의 간단한 설명

- [0019] 도 1은 본 발명의 오류주입 공격에 안전한 피아트 샤미르 개인 식별 장치의 블록도이다.
- 도 2는 본 발명의 오류주입 공격에 안전한 피아트 샤미르 개인 식별 방법의 흐름도이다.
- 도 3a는 피아트 샤미르 개인 식별 프로토콜을 도시한 것이다.
- 도 3b는 본 발명의 일 실시 예에 따른 오류주입 공격에 안전한 피아트 샤미르 개인 식별 방법을 도시한 것이다.
- 도 4a는 페이지(Feige) 피아트 샤미르 개인 식별 프로토콜을 도시한 것이다.
- 도 4b는 본 발명의 다른 실시 예에 따른 오류주입 공격에 안전한 피아트 샤미르 개인 식별 방법을 도시한 것이다.

발명을 실시하기 위한 구체적인 내용

- [0020] 이하에서는 도면을 참조하여 본 발명의 바람직한 실시 예를 설명하기로 한다. 그러나, 다음에 예시하는 본 발명의 실시 예는 여러 가지 다른 형태로 변형될 수 있으며, 본 발명의 범위가 다음에 상술하는 실시 예에 한정되는 것은 아니다.
- [0021] 이하에서 서명자는 스마트 카드 기타 인증 정보나 개인 정보를 저장하는 장치를 의미한다. 서명 요청자는 서명 자로부터 수신되는 정보를 이용하여 서명자를 검증하는 장치나 서버 등을 의미한다.
- [0022] 도 1은 본 발명의 오류주입 공격에 안전한 피아트 샤미르 개인 식별 장치(100)의 블록도이다. 이하에서, N 은 비밀키 p 와 q 의 곱이고, p 와 q 는 서로 다른 소수를 나타낸다. 본 발명의 실시 예들에서는 서명 요청자가 알 수 없는 비밀값 T_A 를 반응값 연산에 포함시켜 악의적인 공격자의 분석을 어렵게 만든다.
- [0023] 본 발명의 일 실시 예에 따른 오류주입 공격에 안전한 피아트 샤미르 개인 식별 장치는 서명자의 비밀값 $T_A = \prod_{i=1}^t s_i$, 서명자의 약정값 $x = r^2 \bmod N$, 서명자의 반응값 $y = r \frac{T_A}{\prod_{i=1, i \notin S} s_i} \bmod N$ 를 이용한다.
- [0024] 메모리부(110)는 공개값 N , 알려진 정수 l , t ($1 \leq t$)에 대한 공개키 $PK_l = \{u_i | u_i = s_i^2 \bmod N, 1 \leq i \leq t\}$, 비밀키 $s_1, s_2, \dots, s_t \bmod N$, 비밀값 T_A 등을 저장한다.
- [0025] 약정값 전송부(120)는 랜덤값 r 을 약정값을 연산하고 서명 요청자에 전송한다.
- [0026] 대응값 수신부(130)는 서명 요청자에서 정수 l 이하의 자연수로 이루어진 집합 중 랜덤하게 선택된 부분 집합 S 를 수신한다. 부분 집합 S 는 반응값을 계산하는데 사용되는 서명 요청자의 대응값이다.
- [0027] 반응값 전송부(140)는 메모리부(110)에 저장된 비밀값 T_A 및 부분 집합 S 의 원소를 이용하여 반응값을 연산하고 서명 요청자에 전송한다.
- [0028] 한편, 본 발명의 다른 실시 예에 따른 오류주입 공격에 안전한 피아트 샤미르 개인 식별 장치는 서명자의 비밀값 $T_A = \prod_{i=1}^t s_i$, 서명자의 약정값 $x = sr^2 \bmod N$, $s \in \{-1, 1\}$, 서명자의 반응값 $y = rT_A / (s_1^{\bar{a}_1} s_2^{\bar{a}_2} \dots s_t^{\bar{a}_t})$ 를 이용한다.
- [0029] 메모리부(110)는 공개값 N , 알려진 정수 l , t ($1 \leq t$)에 대한 공개키 $v_i = s_i^2 \bmod N$ ($1 \leq i \leq t$), 비밀키 $s_1, s_2, \dots, s_t \bmod N$, 비밀값 T_A 등을 저장한다.
- [0030] 약정값 전송부(120)는 랜덤값 r 와 $s \in \{-1, 1\}$ 을 약정값을 연산하고 서명 요청자에 전송한다.
- [0031] 대응값 수신부(130)는 서명 요청자에서 랜덤하게 선택된 부분 집합 S 를 수신한다. 부분 집합 S 는 반응값을 계산하는데 사용되는 서명 요청자의 대응값이다.

- [0032] 반응값 전송부(140)는 메모리부(110)에 저장된 비밀값 T_A 및 부분 집합 S 의 원소를 이용하여 반응값을 연산하고 서명 요청자에 전송한다.
- [0033] 도 2는 본 발명의 오류주입 공격에 안전한 피아트 샤미르 개인 식별 방법의 흐름도이다.
- [0034] 본 발명의 개인 식별 프로토콜은 크게 4개의 단계로 구성된다. 첫 번째 단계는 서명자가(100)가 랜덤값 등을 이용하여 약정값을 연산하고 이를 서명 요청자에게 전송하는 약정 과정(11)이다. 두 번째 단계는 서명 요청자(200)가 집합 S 를 랜덤하게 선택하여 서명자(100)에 전송하는 대응 과정(12)이다. 서명 요청자(200)에 의해 랜덤하게 선택된 집합 S 는 서명자가 반응값을 계산하는데 사용된다. 세 번째 단계는 서명자(100)가 새로운 비밀값 T_A 와 서명 요청자(200)의 대응값 등을 이용하여 반응값을 연산하고 서명 요청자(200)에 전송하는 반응 과정(13)이다. 마지막으로 네 번째 단계는 서명 요청자(200)가 약정 과정에서 수신한 약정값 등을 이용하여 계산한 값을 반응값과 비교하여 서명자(100)를 검증하는 검증 과정(14)이다.
- [0035] 도 3a 내지 4b에서, Alice는 서명자 측을 의미하고, Bob은 서명 요청자 측을 의미한다.
- [0036] 도 3a는 피아트 샤미르 개인 식별 프로토콜을 도시한 것이다. 도 3a에서, 서명자는 n 비트의 법(modulus) $N(=p \cdot q)$ 을 저장하고, 가역 원소 $s_1, s_2, \dots, s_t \bmod N$ 의 집합을 저장한다. 또한, 서명자는 공개키에 대한 집합 $PK_t = \{u_i | u_i = s_i^2 \bmod N, 1 \leq i \leq t\}$ 를 저장한다. 서명자와 서명 요청자는 보안 파라미터인 $1, t(1 \leq t)$ 의 값을 공유한다.
- [0037] 서명 요청자의 오류 주입 공격시에, 서명 요청자는 프로토콜의 네 번째 단계인 검증 과정에서 오류가 발생했음을 검출할 수 있다. $s_j \bmod N$ 에 오류가 발생한다고 가정하면, $s_j \bmod N$ 은 다음과 같이 유도될 수 있다.
- [0038] 즉, 단일 비트 플립(Single Bit Flip)이 발생하면, s_j 는 프로토콜의 세 번째 단계인 반응 과정에서 $s_j \pm 2^b$ 로 바뀌게 된다. 여기서, $b \in \{0, 1, \dots, n-1\}$ 이다. 여러 번의 시행 착오를 통해 서명 요청자는 다음의 정보를 수집할 수 있다. 즉, 프로토콜의 첫 번째 단계인 약정 과정에서 $r^2 \bmod N$, 프로토콜의 세 번째 단계인 반응 과정에서 $\hat{y} = r(s_j \pm 2^b) \prod_{k \in S - s_j} s_k \bmod N$ 의 값을 얻을 수 있다.
- [0039] 서명 요청자는 s_j 에 오류가 발생했다는 가정하에 다음의 수학식 1의 연산을 통해 s_j 의 값을 얻을 수 있다.

수학식 1

$$c_1 = \frac{\hat{y}^2}{r^2} \bmod N = (s_j \pm 2^b)^2 \prod_{k \in S - s_j} s_k^2 \bmod N$$

$$c = \frac{c_1}{\prod_{i \in S} u_i} \bmod N = \frac{u_j + 2^{2b} \pm 2^{b+1}s_j}{u_j} \bmod N$$

$$s_j = \pm \frac{u_j(c-1) - 2^{2b}}{2^{b+1}} \bmod N$$

[0040]

[0041] 여기서, 서명 요청자는 정확한 에러 위치 i 를 결정함으로써 정확한 s_j 의 값을 찾아야 서명자가 저장하고 있는 비밀 원소들을 알아낼 수 있다. 그런데, 서명 요청자가 1번의 시행착오를 거치면서 $s_1, \dots, s_t$ 의 모든 위치에 서 에러가 발생하는 상황을 만들면, 서명자의 비밀 값이나 비밀키들을 모두 찾아낼 수 있게 된다.

[0042] 도 3b는 본 발명의 일 실시 예에 따른 오류주입 공격에 안전한 피아트 샤미르 개인 식별 방법을 도시한 것이다.

[0043] 도 3b에서 서명자는 n 비트의 법 $N(=p \cdot q)$ 을 저장하고, 가역 원소 $s_1, s_2, \dots, s_t \bmod N$ 의 집합 및 비밀값

$T_A = \prod_{i=1}^t s_i$ 를 저장한다. 또한, 서명자는 공개키에 대한 집합 $PK_l = \{u_i | u_i = s_i^2 \bmod N, 1 \leq i \leq t\}$ 를 저장한다. 서명자와 서명 요청자는 보안 파라미터인 1, $t(1 \leq t)$ 의 값을 공유한다. 바람직하게는, s_i 와 N 의 최대 공약수 (greatest common divisor)가 1이 되도록 s_i 와 N 의 값을 정할 수도 있다.

[0044] 도 3b의 약정 과정에서, 서명자는 랜덤값 $r(r \in_R Z_N^*)$ 을 이용하여 $x = r^2 \bmod N$ 을 연산하고 서명 요청자에 전송한다. 대응 과정에서, 서명 요청자는 부분 집합 $S \subseteq_R \{1, 2, \dots, l\}$ 를 서명자에 전송한다. 반응 과정에서, 서명자는 반응값 $y = r \frac{T_A}{\prod_{i=1, i \notin S}^t s_i} \bmod N$ 를 서명 요청자에 전송한다. 마지막의 검증 과정에서, 서명 요청자는 y^2 과 $x \cdot \prod_{i \in S} u_i \bmod N$ 을 비교하여 서명자를 검증한다.

[0045] 이러한 프로토콜에서, $s_j \bmod N$ 에 오류가 발생한다고 가정하면, $s_j \bmod N$ 은 다음과 같이 유도될 수 있다. 즉, 단일 비트 플립이 발생하면, s_j 는 프로토콜의 세 번째 단계인 반응 과정에서 $s_j \pm 2^b$ 로 바뀌게 된다. 여기서, $b \in \{0, 1, \dots, n-1\}$ 이다. 여러 번의 시행 착오를 통해 서명 요청자는 다음의 정보를 수집할 수 있다. 즉, 프로토콜의 첫 번째 단계인 약정 과정에서 $r^2 \bmod N$, 프로토콜의 세 번째 단계인 반응 과정에서 $\hat{y} = r \frac{T_A}{(s_j \pm 2^b) \prod_{i=1, i \notin S, i \neq j}^t s_k} \bmod N$ 의 값을 얻을 수 있다. 서명 요청자는 수학식 2와 같은 연산을 수행할 수 있다.

수학식 2

$$c_1 = \frac{\hat{y}^2}{r^2} \bmod N = \frac{T_A^2}{(s_j \pm 2^b)^2 \prod_{i=1, i \notin S, i \neq j}^t s_k^2} \bmod N$$

$$c = c_1 \cdot \left(\prod_{i=1, i \notin S}^t u_i \right) \bmod N = \frac{u_j T_A^2}{(s_j \pm 2^b)^2} \bmod N$$

$$s_j = \left(\frac{u_j T_A^2}{c} - u_j - 2^{2b} \right) / 2^{b+1}$$

[0046]

[0047] 그러나, 서명 요청자는 서명자의 비밀 값 T_A 를 알 수 없기 때문에, $s_j \bmod N$ 의 값을 계산할 수 없다. 결국, 도 3b의 개인 식별 방법이 오류 주입 공격에 안전함이 증명된다.

[0048] 도 4a는 페이지(Feige) 피아트 샤미르 개인 식별 프로토콜을 도시한 것이다. 도 4a에서 서명자는 n 비트의 법 $N(=p \cdot q)$ 을 저장하고, 가역 원소 $s_1, s_2, \dots, s_t \bmod N$ 의 집합을 저장한다. 여기서, $\gcd(s_i, N) = 1$ 을 만족하는데, $\gcd$ 는 최대 공약수를 의미한다. 또한, 서명자는 공개키에 대한 집합 $PK_l = \{u_i | u_i = s_i^2 \bmod N, 1 \leq i \leq t\}$ 를 저장한다. 서명자와 서명 요청자는 보안 파라미터인 1, $t(1 \leq t)$ 의 값을 공유한다.

[0049] 위 프로토콜에서, 서명 요청자의 오류 주입 공격이 있는 경우, 프로토콜의 첫 번째 단계에서 $sr^2 \bmod N$, 세 번째 단계에서 $\hat{y} = r^2 s_1^{a_1} \dots (s_j \pm 2^i)^{a_j} s_t^{a_t} \bmod N$ 의 값을 얻을 수 있다. 서명 요청자는 수학식 3의 과정을 통해 s_j 의 값을 도출할 수 있다.

수학식 3

$$c_1 = \frac{\hat{y}^2}{x} = \pm s_1^{2a_1} s_2^{2a_2} \dots (s_j \pm 2^i)^{2a_j} \dots s_t^{2a_t} \bmod N$$

$$c = \frac{c_1}{v_1^{a_1} v_2^{a_2} \dots v_t^{a_t}} = \frac{(s_j \pm 2^i)^{2a_j}}{v_j} \bmod N$$

$$s_j = \frac{v_j(c \pm 1) + 2^{2i}}{\pm 2^i} \bmod N$$

[0050]

[0051]

도 4b는 본 발명의 다른 실시 예에 따른 오류주입 공격에 안전한 피아트 샤미르 개인 식별 방법을 도시한 것이다.

[0052]

도 4b에서 서명자는 n비트의 법 $N(p \cdot q)$ 을 저장하고, 가역 원소 $s_1, s_2, \dots, s_t \bmod N$ 의 집합 및 비밀값 $T_A = \prod_{i=1}^t s_i$ 를 저장한다. 여기서, $\gcd(s_i, N) = 1$ 을 만족한다. 또한, 서명자는 공개키 $v_i = s_i^2 \bmod N$ ($1 \leq i \leq t$)를 저장한다. 서명자와 서명 요청자는 보안 파라미터인 $1, t$ ($1 \leq t$)의 값을 공유한다.

[0053]

도 4b의 약정 과정에서, 서명자는 랜덤값 r ($r \in_R Z_N^*$)과 $s \in \{-1, 1\}$ 를 이용하여 $x = sr^2 \bmod N$ 을 연산하고 서명 요청자에 전송한다. 대응 과정에서, 서명 요청자는 집합 $S = \{a_i | a_i \in \{0, 1\}, 1 \leq i \leq t\}$ 를 서명자에 전송한다. 반응 과정에서, 서명자는 반응값 $y = rT_A / (s_1^{a_1} s_2^{a_2} \dots s_t^{a_t})$ 를 서명 요청자에 전송한다. 마지막의 검증 과정에서, 서명 요청자는 y^2 과 $\pm x(v_1^{a_1} v_2^{a_2} \dots v_t^{a_t}) \bmod N$ 을 비교하여 서명자를 검증한다.

[0054]

본 발명은 소프트웨어를 통해 실행될 수 있다. 바람직하게는, 본 발명의 실시 예들에 따른 오류주입 공격에 안전한 피아트 샤미르 개인 식별 방법을 컴퓨터에서 실행시키기 위한 프로그램을 컴퓨터로 읽을 수 있는 기록매체에 기록하여 제공할 수 있다. 소프트웨어로 실행될 때, 본 발명의 구성 수단들은 필요한 작업을 실행하는 코드 세그먼트들이다. 프로그램 또는 코드 세그먼트들은 프로세서 판독 가능 매체에 저장되거나 전송 매체 또는 통신 망에서 반송파와 결합된 컴퓨터 데이터 신호에 의하여 전송될 수 있다.

[0055]

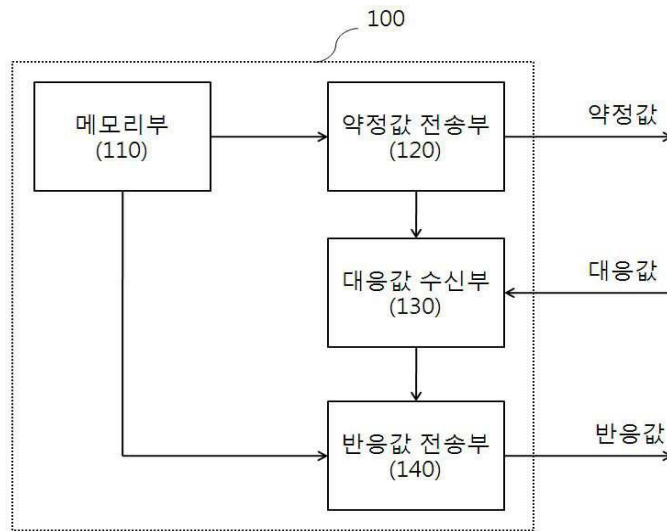
컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록 장치의 예로는 ROM, RAM, CD-ROM, DVD±ROM, DVD-RAM, 자기 테이프, 플로피 디스크, 하드 디스크(hard disk), 광데이터 저장장치 등이 있다. 또한, 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 장치에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

[0056]

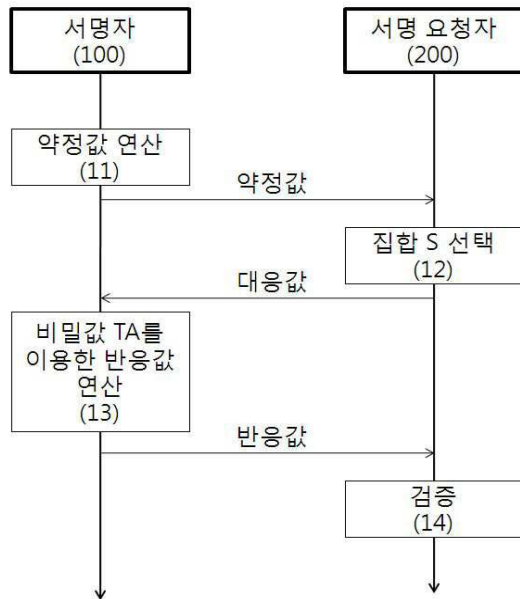
본 발명은 도면에 도시된 실시 예들을 참고로 하여 설명하였으나 이는 예시적인 것에 불과하며 당해 분야에서 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 실시 예의 변형이 가능하다는 점을 이해할 것이다. 그리고, 이와 같은 변형은 본 발명의 기술적 보호범위 내에 있다고 보아야 한다. 따라서, 본 발명의 진정한 기술적 보호범위는 첨부된 특허청구범위의 기술적 사상에 의해서 정해져야 할 것이다.

도면

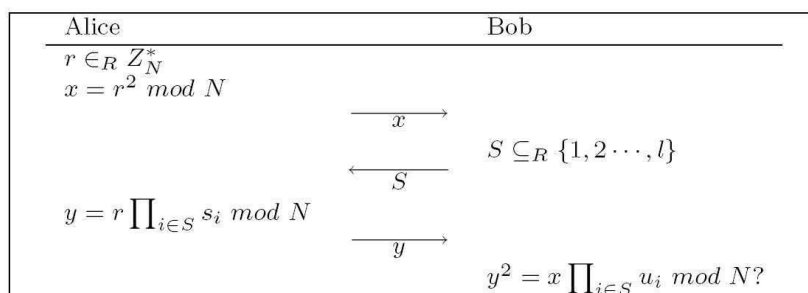
도면1



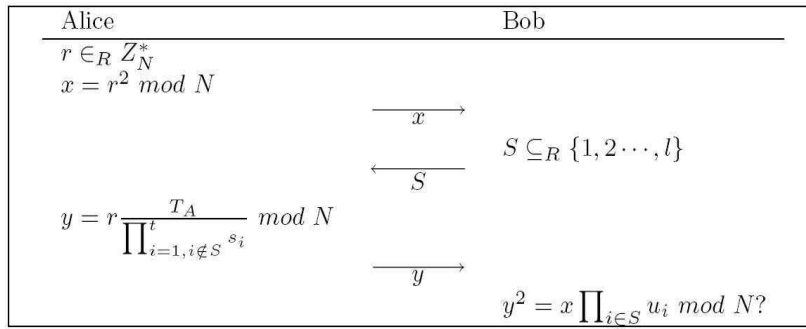
도면2



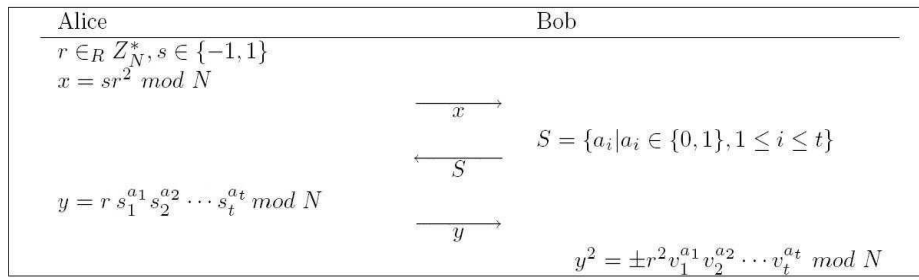
도면3a



도면3b



도면4a



도면4b

