



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2017-0101596
(43) 공개일자 2017년09월06일

(51) 국제특허분류(Int. Cl.)
H04L 9/00 (2006.01) H04L 9/06 (2006.01)
H04L 9/12 (2006.01)
(52) CPC특허분류
H04L 9/003 (2013.01)
H04L 9/0662 (2013.01)
(21) 출원번호 10-2016-0024356
(22) 출원일자 2016년02월29일
심사청구일자 2016년02월29일

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
홍석희
서울특별시 노원구 덕릉로71길 30, 102동 1701호 (중계동, 양지대림아파트)
김창한
서울특별시 강남구 삼성로 212, 21동 507호(대치동, 은마아파트)
(뒷면에 계속)
(74) 대리인
특허법인충정

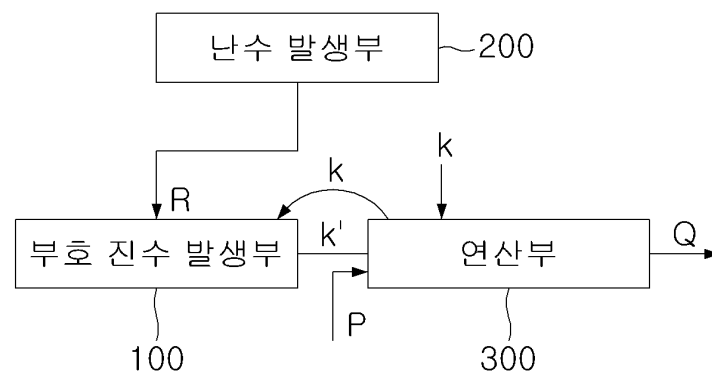
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 전력분석공격을 방지할 수 있는 타원 곡선 암호화 장치 및 그 방법

(57) 요약

본 발명은 단순전력분석(SPA : Simple Power Analysis)과 차분전력분석(DPA : Differential Power Analysis)에 안전하도록 두 공격 모두에 대응하는 전력분석공격을 방지할 수 있는 타원 곡선 암호화 장치 및 그 방법에 관한 것으로, 난수를 발생시키는 난수 발생부; 비밀 정보를 입력받고, 난수 발생부에서 난수를 입력받아 비밀 정보와 동일한 값을 가지는 부호화된 사진수를 발생시키는 부호 진수 발생부; 및 상기 부호 진수 발생부에서 부호화된 사진수를 참조하여 타원곡선상의 한 점을 네 배하는 연산과 두 점을 더하는 연산을 수행하여 스칼라 곱셈 결과값을 생성하는 연산부를 포함하는 전력분석공격을 방지할 수 있는 타원 곡선 암호화 장치 및 그 방법이 제공된다.

대표도 - 도1



(52) CPC특허분류

H04L 9/12 (2013.01)

H04L 2209/12 (2013.01)

H04L 2209/34 (2013.01)

(72) 발명자

조성민

서울특별시 성북구 월곡로14길 26, 14동 902호

유효명

경기도 용인시 기흥구 금화로11번길 9, 601동 210호(상갈동, 금화마을주공6단지아파트)

이 발명을 지원한 국가연구개발사업

과제고유번호 NRF-2014M3C4A7030649

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

난수를 발생시키는 난수 발생부;

비밀 정보를 입력받고, 난수 발생부에서 난수를 입력받아 비밀 정보와 동일한 값을 가지는 부호화된 사진수를 발생시키는 부호 진수 발생부; 및

상기 부호 진수 발생부에서 부호화된 사진수를 참조하여 타원곡선상의 한 점을 네 배하는 연산과 두 점을 더하는 연산을 수행하여 스칼라 곱셈 결과값을 생성하는 연산부를 포함하는 전력분석공격을 방지할 수 있는 타원 곡선 암호화 장치.

청구항 2

청구항 1항에 있어서,

상기 난수 발생부에서 발생시키는 난수는 상기 비밀 정보 k 의 $1/2$ 의 길이를 가진 비트로 구성되어 있는 전력분석공격을 방지할 수 있는 타원 곡선 암호화 장치.

청구항 3

청구항 2항에 있어서,

상기 부호 진수 발생부는 i 번째 디지털 위치에서의 비밀 정보 k 의 디지털의 부호화된 사진수를 상기 난수의 i 번째 비트 R 을 참조하여 생성하는 전력분석공격을 방지할 수 있는 타원 곡선 암호화 장치.

청구항 4

청구항 1항에 있어서,

상기 부호 진수 발생부는 비밀 정보를 최하위비트에서부터 시작하여 최상위 비트로 이동하면서 부호화된 사진수를 발생시키는 전력분석공격을 방지할 수 있는 타원 곡선 암호화 장치.

청구항 5

청구항 1항에 있어서,

상기 부호 진수 발생부는 비밀 정보를 입력받아 최하위 디지털을 선택한 후에 난수의 해당 비트를 참조하여 올림수 변환을 수행하고 올림수를 반영하거나, 유지한 후에 다음 상위 디지털을 선택하여 위의 과정을 최상위 비트까지 반복하여 부호화된 사진수를 생성하는 전력분석공격을 방지할 수 있는 타원 곡선 암호화 장치.

청구항 6

청구항 5항에 있어서,

상기 부호 진수 발생부는 난수가 1이면 올림수 변환을 수행하고, 난수가 0이면 유지하는 전력분석공격을 방지할 수 있는 타원 곡선 암호화 장치.

청구항 7

청구항 5항에 있어서,

상기 부호 진수 발생부는 디지털이 이진수 10일 경우 올림수 변환을 할 때에는 디지털을 0(-2)로 부호화하고 다음 디지털에 올림수를 더하며, 올림수 변환을 하지 않을 때에도 디지털을 유지하여 사진수 02로 부호화하며,

상기 부호 진수 발생부는 디지털이 이진수 01일 경우 올림수 변환을 할 때에는 디지털을 0(-3)로 부호화하고 다음 디지털에 올림수를 더하며, 올림수 변환을 하지 않을 때에도 디지털을 유지하여 사진수 01로 부호화하며,

상기 부호 진수 발생부는 디지털이 이진수 11일 경우 올림수 변환을 할 때에는 디지털을 0(-1)로 부호화하고 다음 디지털에 올림수를 더하며, 올림수 변환을 하지 않을 때에도 디지털을 유지하여 사진수 03로 부호화하며, 상기 부호 진수 발생부는 이진수 00의 경우에는 항상 사진수 0(-4)로 부호화하는 전력분석공격을 방지할 수 있는 타원 곡선 암호화 장치.

청구항 8

청구항 1항에 있어서,

상기 연산부는 부호 진수 발생부에서 부호화된 사진수를 참조하여 왼쪽에서 오른쪽으로 타원곡선상의 한 점을 네 배하는 연산과 두 점을 더하는 연산을 수행하여 스칼라 곱셈 결과값을 생성하는 전력분석공격을 방지할 수 있는 타원 곡선 암호화 장치.

청구항 9

청구항 8항에 있어서,

상기 연산부는 상기 부호 진수 발생부에서 부호화된 사진수 k' 를 입력받고, 타원 곡선상의 한점 P 를 입력받고, P , $2P$, $3P$ 및 $4P$ 를 사전 연산하여 사전 연산 테이블에 저장한 후에, 상위 디지털에서부터 각 디지털에 대해 네 배 연산과 두 점을 더하는 연산을 최하위 디지털에 이르도록 수행하여 스칼라 곱셈 결과값을 생성하는 전력분석공격을 방지할 수 있는 타원 곡선 암호화 장치.

청구항 10

청구항 9항에 있어서,

상기 연산부는 사전연산을 부호가 음인 디지털에 대한 연산까지 고려하여 $(x, y, -y)$ 와 같은 아핀 좌표를 저장하는 전력분석공격을 방지할 수 있는 타원 곡선 암호화 장치.

청구항 11

(A) 난수 발생부가 난수를 발생시키는 단계;

(B) 부호 진수 발생부가 상기 난수 발생부에서 난수를 입력받아 비밀 정보와 동일한 값을 가지는 부호화된 사진수를 발생시키는 단계; 및

(C) 연산부가 상기 부호 진수 발생부에서 부호화된 사진수를 참조하여 타원곡선상의 한 점을 네 배하는 연산과 두 점을 더하는 연산을 수행하여 스칼라 곱셈 결과값을 생성하는 단계를 포함하는 전력분석공격을 방지할 수 있는 타원 곡선 암호화 방법.

청구항 12

청구항 11항에 있어서,

상기 (B) 단계는

(B-1) 상기 부호 진수 발생부가 비밀 정보를 입력받아 최하위 디지털을 선택하는 단계;

(B-2) 상기 부호 진수 발생부가 난수의 해당 비트를 참조하여 상기 최하위 디지털을 올림수 변환을 수행하고 올림수를 반영하거나, 상기 최하위 디지털을 유지하여 부호화하는 단계; 및

(B-3) 상기 부호 진수 발생부가 다음 상위 디지털을 선택하여 난수의 해당 비트를 참조하여 상기 다음 상위 디지털을 올림수 변환을 수행하고 올림수를 반영하거나, 상기 다음 상위 디지털을 유지하여 부호화하는 과정을 최상위 비트까지 반복하여 부호화된 사진수를 생성하는 단계를 포함하는 전력분석공격을 방지할 수 있는 타원 곡선 암호화 방법.

청구항 13

청구항 11항에 있어서,

상기 난수 발생부에서 발생시키는 난수는 상기 비밀 정보 k 의 $1/2$ 의 길이를 가진 비트로 구성되어 있는 전력분

석공격을 방지할 수 있는 타원 곡선 암호화 방법.

청구항 14

청구항 13항에 있어서,

상기 부호 진수 발생부는 i 번째 디지털 위치에서의 비밀 정보 k 의 디지털의 부호화된 사진수를 상기 난수의 i 번째 비트 R 을 참조하여 생성하는 전력분석공격을 방지할 수 있는 타원 곡선 암호화 방법.

청구항 15

청구항 11항에 있어서,

상기 부호 진수 발생부는 비밀 정보를 최하위비트에서부터 시작하여 최상위 비트로 이동하면서 부호화된 사진수를 발생시키는 전력분석공격을 방지할 수 있는 타원 곡선 암호화 방법.

청구항 16

청구항 13항에 있어서,

상기 (C) 단계는

(C-1) 상기 연산부가 입력받은 k 를 상기 부호 진수 발생부에 입력하여 부호화된 사진수 k' 을 반환받는 단계;

(C-2) 상기 연산부가 입력받은 타원 곡선상의 한 점에 대한 사전 연산 테이블을 생성하는 단계; 및

(C-3) 상기 연산부가 최상위 디지털부터 각 디지털에 해당하는 네 배 연산과 두 점을 더하는 연산을 최하위 디지털까지 수행하여 스칼라 곱셈 결과 값을 생성하는 단계를 포함하는 전력분석공격을 방지할 수 있는 타원 곡선 암호화 방법.

청구항 17

청구항 16항에 있어서,

상기 (C-2) 단계는

상기 연산부가 타원 곡선상의 한점 P 를 입력받는 과정과,

상기 연산부가 P , $2P$, $3P$ 및 $4P$ 를 사전 연산하여 사전 연산 테이블에 저장하는 단계를 포함하는 전력분석공격을 방지할 수 있는 타원 곡선 암호화 방법.

청구항 18

청구항 17항에 있어서,

상기 연산부는 사전연산을 부호가 음인 디지털에 대한 연산까지 고려하여 $(x, y, -y)$ 와 같은 아핀 좌표를 저장하는 전력분석공격을 방지할 수 있는 타원 곡선 암호화 방법.

청구항 19

청구항 17항에 있어서,

상기 (C-3) 단계는,

상기 연산부가 최상위 디지털부터 네배 연산을 수행하는 과정과,

상기 연산부가 최상위 디지털에 대하여 두점을 더하는 연산을 수행하는 과정과,

상기 연산부가 다음 하위 디지털로 네배 연산을 수행하는 과정과,

상기 연산부가 다음 하위 디지털에 대하여 두 점을 더하는 연산을 수행하는 과정과,

상기 연산부가 다음 하위 디지털이 최하위 디지털인지를 판단하는 과정과,

상기 연산부가 판단 결과 최하위 디지털이 아니면 상기 다음 하위 디지털로 네배 연산을 수행하는 과정부터 반복하고, 최하위 디지털이면 네배 연산과 두 점을 더하는 연산을 수행하고 종료하는 과정을 포함하는 전력분석공

격을 방지할 수 있는 타원 곡선 암호화 방법.

청구항 20

청구항 16항에 있어서,

상기 (C-3) 단계의 두 점을 더하는 연산은

상기 연산부는 중간 연산 결과인 점 Q를 $P=(X_1, Y_1, Z_1)$ 로 입력받고, 해당 디지털에 상응하는 사전연산 테이블의 한 점을 $Q=(x_2, y_2, -y_2)$ 로 입력받고, 상기 연산부가 부호화된 사진수의 해당 디지털을 참조하여 해당 디지털가 음의 수이면 1을, 양의 수이면 0을 할당받은 사인비트 s를 입력으로 받는 과정과,

상기 연산부는 두 점을 더하는 연산을 수행할 때에 사인 비트 s가 1이면 점 Q의 x_2 와 $-y_2$ 를 이용하여 $P-Q$ 를 연산하는 과정과,

상기 연산부는 두 점을 더하는 연산을 수행할 때에 사인 비트 s가 0이면 점 Q의 x_2 와 y_2 를 이용하여 $P+Q$ 를 연산하는 과정을 포함하는 전력분석공격을 방지할 수 있는 타원 곡선 암호화 방법.

여기에서, X_1, Y_1, Z_1 는 타원 곡선의 한 점의 야코비안 좌표의 X축, Y축 및 Z축의 좌표 값이며, $x_2, y_2, -y_2$ 는 타원 곡선의 한 점의 아핀 좌표의 x축, y축 및 y축의 좌표 값임.

발명의 설명

기술 분야

[0001] 본 발명은 단순전력분석(SPA : Simple Power Analysis)과 차분전력분석(DPA : Differential Power Analysis)에 안전하도록 두 공격 모두에 대응하는 전력분석공격을 방지할 수 있는 타원 곡선 암호화 장치 및 그 방법에 관한 것이다.

배경 기술

[0002] 전력분석공격은 암호 장비가 연산을 수행하는 동안의 전력소비량과 해당 연산에 대한 데이터 간에 상관관계가 있다는 사실을 기반으로 한다.

[0003] 전력분석공격은 오롯이 암호 장비의 연산 수행 시 사용되는 전력량만을 이용하는 공격방법이다.

[0004] 전력분석을 통한 대표적인 공격방법은 단순전력분석(SPA : Simple Power Analysis)과 차분전력분석(DPA : Differential Power Analysis)이 있다.

[0005] SPA는 단순히 하나의 전력 소비 파형을 관찰하여 수행 연산을 구분하는 공격이다. 비밀 정보와 수행 연산이 밀접한 관계가 있는 경우 수행 연산의 구분만으로 비밀 정보를 추출해 낼 수 있기 때문에 SPA 공격이 가능하다.

[0006] DPA는 다수의 전력 소비 파형을 사용하여 통계적인 분석법을 통해 비밀 정보를 알아내는 방법이다. DPA는 연산의 중간값을 추측하고 통계치 계산을 통해 추측이 옳은지 판단하여 비밀 정보를 알아낸다.

[0007] SPA에 대응하기 위해서는 연산 패턴이 비밀 정보와 무관하도록 하여 연산 패턴의 구분을 통해 비밀 정보를 알 수 없게 해야 한다.

[0008] DPA를 막기 위해서는 고정된 비밀 정보로 여러 번 연산을 수행하더라도 중간 값이 모두 달라 추측하지 못하도록 연산의 중간 값을 랜덤화 해야 한다.

[0009] 한편, 타원곡선 군은 유한체 $GF(p)$ 상에서의 Weierstrass 방정식을 만족하는 타원곡선 위의 점들과 무한원점 0를 원소로 가지며 덧셈 연산에 대한 아벨군을 이룬다.

[0010] 타원곡선 암호는 타원곡선 군의 원소에 대한 스칼라 곱셈 연산($Q=kP=P+P+\dots P(k \text{ times})$)을 기본 연산으로 한다.

[0011] 타원곡선 스칼라 곱셈 연산은 타원곡선 덧셈 연산(ECADD : Elliptic Curve Addition)과 두 배 연산(ECDBL : Elliptic Curve Doubling)을 통해 수행된다.

[0012] 이 때 일반적으로 사용하는 타원곡선 스칼라 곱셈 연산 방법은 타원곡선 덧셈 연산 및 두 배 연산의 수행 순서가 비밀 정보인 스칼라와 밀접한 관계가 있어 SPA에 안전하지 않다. 또한 고정된 비밀 정보를 이용하여 반복적

으로 연산을 수행하게 되면 DPA를 통해 비밀 정보가 노출될 수 있다.

- [0013] 다음으로, 스칼라 레코딩은 비밀 정보인 스칼라를 이진수 표현이 아닌 음수 표현, 2^b 진수 표현 등의 표현 방식을 사용하여 레코딩하는 것이다.
- [0014] 스칼라의 레코딩을 통해 해밍 웨이트(Hamming weight)를 줄여 타원곡선 덧셈 연산의 수를 줄일 수도 있고, 모든 디지트(digit)가 0이 아니도록 레코딩하여 항상 타원곡선 덧셈 연산을 수행하도록 할 수도 있다.
- [0015] 이와 같은 스칼라 레코딩을 통해 타원곡선 스칼라 곱셈 연산의 효율을 향상시킬 수 있으며 전력분석공격으로부터 안전하도록 할 수도 있다.
- [0016] 기존의 스칼라 레코딩은 타원곡선 스칼라 곱셈 연산의 효율 향상을 목적으로 연구되었다. 연산의 효율 향상을 위한 대표적인 스칼라 레코딩 방법으로는 NAF(Non-adjacent form)이 있다. NAF는 이진수 11을 이진수 10(-1)와 같이 음수 표현을 사용하여 스칼라 비트열의 해밍 웨이트(Hamming weight)를 줄이는 방법이다.

선행기술문헌

특허문헌

- [0017] (특허문헌 0001) 국내공개특허번호 2006-0069177호
- (특허문헌 0002) 미국특허 7159115호
- (특허문헌 0003) 일본공개특허번호 2004-163687호
- (특허문헌 0004) 일본특허등록번호 4825199호
- (특허문헌 0005)

비특허문헌

- [0018] (비특허문헌 0001) [1] P. Kocher, J. Jaffe, and B. Jun, Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Others Systems. CRYPTO, LNCS 1109, pp. 104-113, 1996.
- (비특허문헌 0002) [2] P. Kocher, J. Jaffe, and B. Jun, Power Analysis, CRYPTO, LNCS 1666, pp. 388-397, 1999.
- (비특허문헌 0003) [3] D. Hankerson, A. Menezes, and S. Vanstone, to elliptic curve cryptography, Springer Professional Computing. Springer-Verlag, New York, 2004.
- (비특허문헌 0004) [4] M. Joye, M. Tunstall, recoding and regular exponentiation algorithms. Africacrypt 2003, ed. by M. Joye. LNCS, vol.5580, pp. 334-349
- (비특허문헌 0005) [5] J.-S. Coron, Against Differential Analysis for Elliptic Curve Cryptography., Advances in Cryptology CHES, volume 1717 of LNCS, pages 292-302. Springer-Verlag, 1999.
- (비특허문헌 0006) [6] B.C. Mames, M. Ciet, and M. Joye, solutions for preventing simple side-channel analysis: Side-channel atomicity, IEEE Transactions on Computers, vol. 53, no. 6, pp. 760-768, June 2004.
- (비특허문헌 0007) [7] Liping Wang, Weike Wang, Rong, Zhang, and Xiang Wang, New ECC scalar Multiplication Algorithm with Randomized Power Consumption, ICSICT2014, Guilin, China, 2014.
- (비특허문헌 0008) [8] E. Guerrini, L. Imbert, and T. Winterhalter, scalar multiplication using exact covering systems of congruences. Cryptology ePrint Archive, Report 2015/475, 2015.
- (비특허문헌 0009) [9] Peng LUO, Dengguo FENG, Yongbin Zhou, New Anti-SPA Algorithm of NAF scalar Multiplication used in ECC, International Journal of Advancements in Computing Technology, Nov2012, Vol.4 Issue 20, p692, 2012.
- (비특허문헌 0010) [10] JaeCheol Ha, SangJae Moon, signed-scalar multiplication of ECC to resist power

attacks., in Pre-Proceedings of Workshop on Cryptographic Hardware and Embedded Systems CHES, Springer-Verlag, pp.553-565, 2002.

(비특허문헌 0011) [11] MahnKi Ahn, JaeCheol Ha, HoonJae Lee, SangJae Moon, Random M-ary Method-Based Countermeasure against Power Analysis Attacks on ECC, Journal of the Korean Institute of Information Security and Cryptology v.13 no.3, pp.35 - 43, 2003

발명의 내용

해결하려는 과제

[0019] 본 발명이 해결하고자 하는 과제는 비밀 정보와 타원곡선 연산 순서간의 상관관계를 없애고 고정된 스칼라에 대한 레코딩 결과를 항상 다르게 생성하는 전력분석공격을 방지할 수 있는 타원 곡선 암호화 장치 및 그 방법을 제공하는 데 있다.

과제의 해결 수단

[0020] 본 발명의 장치는 난수를 발생시키는 난수 발생부; 비밀 정보를 입력받고, 난수 발생부에서 난수를 입력받아 비밀 정보와 동일한 값을 가지는 부호화된 사진수를 발생시키는 부호 진수 발생부; 및 상기 부호 진수 발생부에서 부호화된 사진수를 참조하여 타원곡선상의 한 점을 네 배하는 연산과 두 점을 더하는 연산을 수행하여 스칼라 곱셈 결과값을 생성하는 연산부를 포함한다.

[0021] 또한, 본 발명의 장치의 상기 난수 발생부에서 발생시키는 난수는 상기 비밀 정보 k 의 $1/2$ 의 길이를 가진 비트로 구성되어 있다.

[0022] 또한, 본 발명의 장치의 상기 부호 진수 발생부는 i 번째 디지털 위치에서의 비밀 정보 k 의 디지털의 부호화된 사진수를 상기 난수의 i 번째 비트 R 을 참조하여 생성한다.

[0023] 또한, 본 발명의 장치의 상기 부호 진수 발생부는 비밀 정보를 최하위비트에서부터 시작하여 최상위 비트로 이동하면서 부호화된 사진수를 발생시킨다.

[0024] 또한, 본 발명의 장치의 상기 부호 진수 발생부는 비밀 정보를 입력받아 최하위 디지털을 선택한 후에 난수의 해당 비트를 참조하여 올림수 변환을 수행하고 올림수를 반영하거나, 유지한 후에 다음 상위 디지털을 선택하여 위의 과정을 최상위 비트까지 반복하여 부호화된 사진수를 생성한다.

[0025] 또한, 본 발명의 장치의 상기 부호 진수 발생부는 난수가 1이면 올림수 변환을 수행하고, 난수가 0이면 유지한다.

[0026] 또한, 본 발명의 장치의 상기 부호 진수 발생부는 디지털이 이진수 10일 경우 올림수 변환을 할 때에는 디지털을 $0(-2)$ 로 부호화하고 다음 디지털에 올림수를 더하며, 올림수 변환을 하지 않을 때에도 디지털을 유지하여 사진수 02로 부호화하며, 상기 부호 진수 발생부는 디지털이 이진수 01일 경우 올림수 변환을 할 때에는 디지털을 $0(-3)$ 로 부호화하고 다음 디지털에 올림수를 더하며, 올림수 변환을 하지 않을 때에도 디지털을 유지하여 사진수 01로 부호화하며, 상기 부호 진수 발생부는 디지털이 이진수 11일 경우 올림수 변환을 할 때에는 디지털을 $0(-1)$ 로 부호화하고 다음 디지털에 올림수를 더하며, 올림수 변환을 하지 않을 때에도 디지털을 유지하여 사진수 03로 부호화하며, 상기 부호 진수 발생부는 이진수 00의 경우에는 항상 사진수 $0(-4)$ 로 부호화한다.

[0027] 또한, 본 발명의 장치의 상기 연산부는 부호 진수 발생부에서 부호화된 사진수를 참조하여 왼쪽에서 오른쪽으로 타원곡선상의 한 점을 네 배하는 연산과 두 점을 더하는 연산을 수행하여 스칼라 곱셈 결과값을 생성한다.

[0028] 또한, 본 발명의 장치의 상기 연산부는 상기 부호 진수 발생부에서 부호화된 사진수 k' 를 입력받고, 타원 곡선상의 한점 P 를 입력받고, P , $2P$, $3P$ 및 $4P$ 를 사전 연산하여 사전 연산 테이블에 저장한 후에, 상위 디지털에서부터 각 디지털에 대해 네배 연산과 두 점을 더하는 연산을 최하위 디지털에 이르도록 수행하여 스칼라 곱셈 결과값을 생성한다.

[0029] 또한, 본 발명의 장치의 상기 연산부는 사전연산을 부호가 음인 디지털에 대한 연산까지 고려하여 $(x, y, -y)$ 와 같은 아핀 좌표를 저장한다.

[0030] 한편, 본 발명의 방법은 (A) 난수 발생부가 난수를 발생시키는 단계; (B) 부호 진수 발생부가 상기 난수 발생부

에서 난수를 입력받아 비밀 정보와 동일한 값을 가지는 부호화된 사진수를 발생시키는 단계; 및 (C) 연산부가 상기 부호 진수 발생부에서 부호화된 사진수를 참조하여 타원곡선상의 한 점을 네 배하는 연산과 두 점을 더하는 연산을 수행하여 스칼라 곱셈 결과값을 생성하는 단계를 포함한다.

[0031] 또한, 본 발명의 방법의 상기 (B) 단계는 (B-1) 상기 부호 진수 발생부가 비밀 정보를 입력받아 최하위 디지털을 선택하는 단계; (B-2) 상기 부호 진수 발생부가 난수의 최하위 비트의 해당 비트값을 참조하여 상기 최하위 디지털을 올림수 변환을 수행하고 올림수를 반영하거나, 상기 최하위 디지털을 유지하여 부호화하는 단계; 및 (B-3) 상기 부호 진수 발생부가 다음 상위 디지털을 선택하여 난수의 다음 상위 비트의 해당 비트값을 참조하여 상기 다음 상위 디지털을 올림수 변환을 수행하고 올림수를 반영하거나, 상기 다음 상위 디지털을 유지하여 부호화하는 과정을 최상위 디지털까지 반복하여 부호화된 사진수를 생성하는 단계를 포함한다.

[0032] 또한, 본 발명의 방법의 상기 난수 발생부에서 발생시키는 난수는 상기 비밀 정보 k 의 $1/2$ 의 길이를 가진 비트로 구성되어 있다.

[0033] 또한, 본 발명의 방법의 상기 부호 진수 발생부는 i 번째 디지털 위치에서의 비밀 정보 k 의 디지털의 부호화된 사진수를 상기 난수의 i 번째 비트 R 을 참조하여 생성한다.

[0034] 또한, 본 발명의 방법의 상기 부호 진수 발생부는 비밀 정보를 최하위비트에서부터 시작하여 최상위 비트로 이동하면서 부호화된 사진수를 발생시킨다.

[0035] 또한, 본 발명의 방법의 상기 (C) 단계는 (C-1) 상기 연산부가 입력받은 k 를 상기 부호 진수 발생부에 입력하여 부호화된 사진수 k' 를 반환받는 단계; (C-2) 상기 연산부가 입력받은 타원 곡선상의 한점에 대한 사전 연산 테이블을 생성하는 단계; 및 (C-3) 상기 연산부가 최상위 디지털부터 각 디지털에 해당하는 네배 연산과 두점을 더하는 연산을 최하위 디지털까지 수행하여 스칼라 곱셈 결과값을 생성하는 단계를 포함한다.

[0036] 또한, 본 발명의 방법의 상기 (C-2) 단계는 상기 연산부가 타원 곡선상의 한점 P 를 입력받는 과정과, 상기 연산부가 P , $2P$, $3P$ 및 $4P$ 를 사전 연산하여 사전 연산 테이블에 저장하는 단계를 포함한다.

[0037] 또한, 본 발명의 방법의 상기 연산부는 부호가 음인 디지털에 대한 연산까지 고려하여 $(x, y, -y)$ 와 같은 아핀 좌표를 저장한다.

[0038] 또한, 본 발명의 방법의 상기 (C-3) 단계는, 상기 연산부가 최상위 디지털부터 네배 연산을 수행하는 과정과, 상기 연산부가 최상위 디지털에 대하여 두점을 더하는 연산을 수행하는 과정과, 상기 연산부가 다음 하위 디지털로 네배 연산을 수행하는 과정과, 상기 연산부가 다음 하위 디지털에 대하여 두 점을 더하는 연산을 수행하는 과정과, 상기 연산부가 다음 하위 디지털이 최하위 디지털인지를 판단하는 과정과, 상기 연산부가 판단 결과 최하위 디지털이 아니면 상기 다음 하위 디지털로 네배 연산을 수행하는 과정부터 반복하고, 최하위 디지털이면 네 배 연산과 두 점을 더하는 연산을 수행하고 종료하는 과정을 포함한다.

[0039] 또한, 본 발명의 방법의 상기 (C-3) 단계의 두 점을 더하는 연산은 상기 연산부는 중간 연산 결과인 점 Q 를 $P=(X_1, Y_1, Z_1)$ 로 입력받고, 해당 디지털에 상응하는 사전연산 테이블의 한 점을 $Q=(x_2, y_2, -y_2)$ 로 입력받고, 상기 연산부가 부호화된 사진수의 해당 디지털을 참조하여 해당 디지털이 음의 수이면 1을, 양의 수이면 0을 할당 받은 사인비트 s 를 입력으로 받는 과정과, 상기 연산부는 두 점을 더하는 연산을 수행할 때에 사인 비트 s 가 1이면 점 Q 의 x_2 와 $-y_2$ 를 이용하여 $P-Q$ 를 연산하는 과정과, 상기 연산부는 두 점을 더하는 연산을 수행할 때에 사인 비트 s 가 0이면 점 Q 의 x_2 와 y_2 를 이용하여 $P+Q$ 를 연산하는 과정을 포함하며, 여기에서, X_1, Y_1, Z_1 은 타원 곡선의 한 점의 야코비안 좌표의 X 축, Y 축 및 Z 축의 좌표 값이며, $x_2, y_2, -y_2$ 는 타원 곡선의 한 점의 아핀 좌표의 x 축, y 축 및 y 축의 좌표 값이다.

발명의 효과

[0040] 본 발명에 의하면, 타원곡선 스칼라 곱셈 연산에 대한 SPA 및 DPA 공격에 효율적으로 대응할 수 있다.

[0041] 실험을 통해 위 사실을 확인한 결과 타원곡선 연산 패턴이 비밀 정보와 무관하며 일정하게 반복되어 SPA 공격이 무의미하다.

[0042] 또한 고정된 비밀 정보로 여러 번 연산을 수행하더라도 항상 다른 레코딩 결과 값으로 연산이 이뤄지기 때문에 중간 값이 모두 달라 중간 값의 추측이 불가능하다.

[0043] 따라서 DPA 공격 역시 불가능하다. 실험은 ARM 보드(CPU : S3C2410(ARM920 T), Boot Flash 1MB, NAND Flash 8MB, SDRAM 64MB, 5V 전원, USB 인터페이스(115200bps))를 사용하여 진행했으며 Linux 환경에서 컴파일하였다.

[0044] 또한 본 발명은 SPA 및 DPA에 대응하는 기존의 다른 방법들에 비해 연산 효율이 우수하다.

도면의 간단한 설명

[0045] 도 1은 본 발명의 일 실시예에 따른 전력 분석 공격을 방지할 수 있는 타원 곡선 암호화 장치의 구성도이다.

도 2는 도 1의 부호 진수 발생부를 이용하여 다양한 난수에 대한 부호화된 사진수를 보여주는 도면이다.

도 3은 본 발명의 일 실시예에 따른 전력분석공격을 방지할 수 있는 타원 곡선 암호화 방법의 부호화된 사진수 발생 과정의 흐름도이다.

도 4는 본 발명의 일 실시예에 따른 전력분석공격을 방지할 수 있는 타원 곡선 암호화 방법의 부호화된 사진수 발생 과정의 알고리즘이다.

도 5는 본 발명의 일 실시예에 따른 전력 분석 공격을 방지할 수 있는 타원 곡선 암호화 방법의 흐름도이다.

도 6은 본 발명의 일 실시예에 따른 전력 분석 공격을 방지할 수 있는 타원 곡선 암호화 방법의 알고리즘이다.

도 7은 도 5의 두 점을 더하는 연산을 설명하기 위한 흐름도이다.

도 8은 도 7의 알고리즘이다.

발명을 실시하기 위한 구체적인 내용

[0046] 본 발명은 다양한 변환을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 이하에서는 특정 실시예들을 첨부된 도면을 기초로 상세히 설명하고자 한다.

[0047] 본 발명을 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다.

[0048] 제1, 제2 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되는 것은 아니며, 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다.

[0049] 이하 첨부되는 도면을 참조하여 상세히 설명한다.

[0050] 도 1은 본 발명의 일 실시예에 따른 전력분석공격을 방지할 수 있는 타원 곡선 암호화 장치의 구성도이다.

[0051] 도 1을 참조하면, 본 발명의 일 실시예에 따른 전력 분석 공격을 방지할 수 있는 타원 곡선 암호화 장치는 부호 진수 발생부(100)와, 난수 발생부(200) 및 연산부(300)로 이루어져 있다.

[0052] 상기 부호 진수 발생부(100)는 연산부(300)에서 비밀 정보 $k=(k_{l-1}, \dots, k_1, k_0)_4$ 를 양의 정수(Positive integer)로 입력받고, 난수 발생부(200)에서 난수(Random number)를 입력받아 난수의 각 비트 R값을 참조하여 비밀 정보 k와 동일한 값을 가지는 부호화된 사진수(또는 레코딩된 스칼라 recoded scalar) k'를 발생시킨다. 여기에서, k_{l-1} 는 최상위 디지털을 나타낸다.

[0053] 다음으로, 난수 발생부(200)는 k값 변환시에 참조할 난수를 발생시킨다. 상기 난수 발생부(200)에서 발생된 난수의 길이는 상기 비밀 정보의 길이의 1/2을 갖는다.

[0054] 한편, 연산부(300)는 비밀 정보 k를 입력받아 상기 부호 진수 발생부(100)에 제공하고, 상기 부호 진수 발생부(100)에서 부호화된 사진수를 참조하여 왼쪽에서 오른쪽으로 타원곡선상의 한 점 P를 네 배하는 연산(4Q)과 두 점을 더하는 연산($Q+P_{k'}$)을 수행하여 스칼라 곱셈 결과값 Q를 생성한다.

[0055] 이와 같은 구성의 본 발명의 일 실시예에 따른 전력분석공격을 방지할 수 있는 타원 곡선 암호화 장치의 동작을 살펴보면 다음과 같다.

[0056] 상기 부호 진수 발생부(100)는 앞서 생성한 난수의 한 비트 값 R과 비밀 정보 k를 이용하여 비밀 정보 k와 동일한 값을 가지는 부호화된 사진수 k'를 발생시킨다.

- [0057] 부호화된 사진수 k' 를 발생시키는 과정은 생성한 난수에 따라 다양한 결과를 생성할 수 있다.
- [0058] 먼저 부호 진수 발생부(100)는 비밀 정보 k 에서 두 비트를 한 디지털(digit)로 하여 하위 디지털에서부터 Right-to-left 방식으로(즉 오른쪽에서부터 왼쪽으로 진행하면서, 낮은 차수부터 높은 차수로 진행하면서) 부호화된 사진수를 발생시킨다.
- [0059] 상기 부호 진수 발생부(100)는 난수 발생부(200)에서 입력받은 난수의 비트 값에 따라 각 디지털에 대하여 선택적으로 수행한다.
- [0060] 따라서 부호 진수 발생부(100)에서 발생된 부호화된 사진수는 생성한 난수에 의존하여 항상 다르게 나타난다. 상기 난수는 상기 비밀 정보 k 의 $1/2$ 의 길이를 가진 비트로 구성되어 있고, i 번째 디지털 위치에서의 비밀 정보 k 의 디지털의 부호화된 사진수는 상기 난수의 i 번째 비트 값 R 에 의존한다.
- [0061] 즉, 상기 부호 진수 발생부(100)는 상기 i 번째 디지털 위치에서의 비밀 정보 k 의 값을 부호화된 사진수로 변환하는 경우에 난수의 i 번째 비트 값 R 이 1이면 올림수를 발생시키고(즉 올림수 변환을 하고), 난수의 i 번째 비트 값 R 이 0이면 올림수를 발생시키지 않을 수 있다(즉 유지할 수 있다).
- [0062] 물론 이와 반대로 상기 부호 진수 발생부(100)는 상기 i 번째 디지털 위치에서의 비밀 정보 k 의 값을 부호화된 사진수로 변환하는 경우에 난수의 i 번째 비트 값 R 이 0이면 올림수를 발생시키고, 난수의 i 번째 비트 값 R 이 1이면 올림수를 발생시키지 않을 수 있다. 다만, 00의 경우에는 항상 10(-4)로 부호화된 사진수를 생성한 후 다음 디지털에 올림수를 더하여 타원곡선 스칼라 곱셈 연산에서 모든 디지털에 대해 예외 없이 ECADD 연산이 수행되도록 부호화된 사진수를 생성할 수 있다.
- [0063] 상기 부호 진수 발생부(100)에서 앞 디지털에서의 올림수 발생 여부가 다음 디지털에 영향을 준다.
- [0064] 이와 같은 상황에서 올림수 발생이 연쇄적으로 영향을 미쳤을 때 한 디지털은 최대 2까지의 올림수를 받게 된다.
- [0065] 한 디지털은 최대 일곱 가지의 경우로 부호화 사진수를 생성할 수 있어 아주 랜덤한 부호화된 사진수가 생성된다.
- [0066] 상기 부호 진수 발생부(100)는 디지털이 이진수 10일 경우 올림수 변환을 할 때에는 이진수 1(-1)0이고 부호화된 사진수 변환인 경우에는 10(-2)이므로 디지털을 0(-2)로 부호화하고 다음 디지털에 올림수를 더한다.
- [0067] 그리고 부호 진수 발생부(100)는 올림수 변환을 하지 않을 때에도 이진수 10이 사진수 02이므로 디지털을 유지하여 사진수 02로 부호화한다.
- [0068] 마찬가지로 부호 진수 발생부(100)는 이진수 01을 사진수 0(-3)으로 부호화한 후에 다음 디지털에 올림수를 더하거나 유지하여 사진수 01로 부호화한다.
- [0069] 또한, 부호 진수 발생부(100)는 이진수 11을 사진수 0(-1)로 부호화한 후에, 다음 디지털에 올림수를 더하거나 유지하여 사진수 03으로 부호화한다.
- [0070] 그리고 부호 진수 발생부(100)는 이진수 00의 경우에는 항상 사진수 0(-4)로 부호화한 후에 다음 디지털에 올림수를 더하여 타원곡선 스칼라 곱셈 연산에서 모든 디지털에 대해 예외 없이 ECADD 연산이 수행되도록 부호화한다.
- [0071] 이와 같이 변환하므로 연산부(300)에서 스칼라 곱셈 연산의 경우에 올림수 변환 여부와 디지털의 값에 관계없이 항상 ECQPL(Elliptic Curve Quadrupling), ECADD 패턴의 연산을 수행하게 된다. 따라서 본 발명은 연산 패턴을 통한 비밀정보의 노출을 막는다.
- [0072] 추가적으로 모든 변환과정은 조건문 없이 수식 연산으로 구성할 수 있어 조건문에 따른 부채널 공격에도 안전하도록 할 수 있다.
- [0073] 이로 인해 부호 진수 발생부(100)에서 생성된 부호화된 사진수를 적용한 연산부(300)의 타원곡선 스칼라 곱셈 연산은 같은 비밀 정보 k 에 대해 여러 번 연산을 수행하더라도 항상 다른 부호화 사진수를 사용하게 된다.
- [0074] 따라서 연산부(300)에서 수행된 타원곡선 스칼라 곱셈 연산은 DPA에 대응할 수 있다.
- [0075] 또한 부호 진수 발생부(100)는 SPA에 대응하기 위해 모든 디지털에서 같은 패턴의 연산이 수행되도록 부호화된 사진수를 생성한다.

[0076] 상기 부호 진수 발생부(100)의 부호화는 길이가 1인 디지털의 스칼라에 대해 올림수 발생 여부와 관계없이 1-1 번째 디지털까지만 수행한다. 즉, 올림수로 인해 발생한 디지털은 변환을 수행하지 않는다. 이로써 변환 결과는 자리가 증가하더라도 최대 한 자리까지만에 증가하지 않는다.

[0077] 상기 부호 진수 발생부(100)에서 수행되는 부호화된 사진수의 생성 예가 아래 표 1에 도시되어 있다.

표 1

i	10	9	8	7	6	5	4	3	2	1	0
k		1	0	0	0	0	1	1	1	0	1
R		1			1		1		0		0
올림수	1		1		1						
k'	1	0	-1	0	-3	0	-3	0	3	0	1

[0079] 그리고, 도 2는 가장 윗줄에 있는 비밀 정보 k를 서로 다른 난수를 사용하여 부호화된 사진수를 형성하는 과정을 보여주는 도면이다.

[0080] 한편, 연산부(300)는 왼쪽에서 오른쪽으로 타원곡선상의 한 점 P를 네 배하는 연산(4Q)과 두 점을 더하는 연산($Q+P_{k'}$)을 수행하여 스칼라 곱셈 결과값 Q를 생성한다.

[0081] 이를 위하여 연산부(300)는 비밀 정보 k를 입력받아 부호 진수 발생부(100)에 제공하고, 부호 진수 발생부(100)에서 부호화된 사진수 k'를 입력받는다.

[0082] 그리고, 연산부(300)는 타원 곡선상의 한점 P를 입력받고, 양수 디지털값들의 타원곡선 스칼라 곱셈 결과인 P, 2P, 3P 및 4P를 사전 연산하여 사전 연산 테이블에 저장한다.

[0083] 본 발명은 자체적으로 DPA에 대응하기 때문에 DPA 대응책인 랜덤 투영 좌표(Random projective coordinates)를 사용할 필요가 없다.

[0084] 따라서, 아핀 좌표(affine coordinates)를 사용하여 저장하며, 이로써 다른 대응책들을 사용하는 것에 비해 메모리 및 연산 속도의 효율을 향상시킬 수 있다.

[0085] 사전 연산 테이블은 본 연산에서 디지털 값에 해당하는 ECADD 연산을 수행할 때 사용된다. 음수 디지털 값에 대한 ECADD 연산은 일반적으로 사전 연산 테이블에 저장된 점의 y좌표(coordinate)로부터 -y 좌표를 계산하여 수행된다.

[0086] 하지만 -y 좌표를 계산하는 추가연산이 발생함에 따라 부채널 정보를 통해 디지털의 부호 정보가 노출됨이 연구된 바 있다[8].

[0087] 이를 좀더 구체적으로 살펴보면, 연산부(300)는 최상위 디지털부터 네 배 연산을 수행하고, 이후에 두 점을 더하는 연산을 수행한다.

[0088] 그리고, 연산부(300)는 다음 하위 디지털로 네배 연산을 수행하고 두 점을 더하는 연산을 수행하며 이러한 과정을 최하위 디지털에 이르도록 수행한다.

[0089] 이를 아래 표 2를 참조하여 설명하면 연산부(300)는 Q를 무한 원점으로 설정한다(통상적으로 0으로 생각할 수 있다).

[0090] 그리고, 최상위 디지털을 확인하여 1이기 때문에 Q+P를 수행한다(최상위 디지털은 항상 양수이다).

[0091] 이후에, 연산부(300)는 다음 하위 디지털을 확인하여 -1이기 때문에 $Q-P=4P-P=3P$ 를 산출한다. 이러한 과정을 반복하여 최하위 디지털까지 수행하면 스칼라 곱셈 연산 결과값을 얻을 수 있다.

표 2

i	10	9	8	7	6	5	4	3	2	1	0
k'	1	0	-1	0	-3	0	-3	0	3	0	1
결과값	P	$Q(4P)-P=3P$		$Q(12P)-3P=9P$		$Q(36P)-3P=33P$		$Q(132)+3P=135P$		$Q(540P)+P=541P$	

- [0093] 도 3은 본 발명의 일 실시예에 따른 전력분석공격을 방지할 수 있는 타원 곡선 암호화 방법의 부호화된 사진수 발생 과정의 흐름도이다.
- [0094] 도 3을 참조하면, 본 발명의 일 실시예에 따른 전력 분석 공격을 방지할 수 있는 타원 곡선 암호화 방법의 부호화된 사진수 발생 과정은 상기 부호 진수 발생부가 비밀 정보 k 를 입력받는다(S100). 그리고, 난수 발생부가 난수를 발생시킨다(S102). 다음으로, 부호 진수 발생부는 난수의 최하위 비트를 선택하여(S104) 해당 비트 R 이 1인지 여부를 판단한다(S106).
- [0095] 상기 부호 진수 발생부는 판단 결과 해당 비트 R 이 1이면 올림수 변환을 수행하고(S108), 올림수를 상위 디지털에 반영한다(S110).
- [0096] 이와 달리 상기 부호 진수 발생부는 판단 결과 해당 비트 R 이 1이 아니면 유지하여 사진수로 부호화한다(S112).
- [0097] 한편, 부호 진수 발생부는 해당 디지털이 최상위 디지털인지를 판단하여(S114), 최상위 디지털이 아니면 다음 상위 디지털을 선택하여 상기 S106부터 반복하여 수행하며, 최상위 디지털이면 해당 디지털까지 부호화 과정을 실시한 후에 종료한다. 이때, 사용되는 알고리즘이 도 4에 도시되어 있다.
- [0098] 다음으로, 도 5는 본 발명의 일 실시예에 따른 전력 분석 공격을 방지할 수 있는 타원 곡선 암호화 방법의 흐름도이다.
- [0099] 도 5를 참조하면, 본 발명의 일 실시예에 따른 전력 분석 공격을 방지할 수 있는 타원 곡선 암호화 방법은 연산부는 비밀 정보 k 를 입력받고, 타원곡선상의 한 점 P 를 입력받는다(S200, S201).
- [0100] 그리고, 연산부는 부호 진수 발생부에 비밀 정보 k 를 제공한 후에 부호화된 사진수 k' 를 반환받는다(S202). 이 때, k' 은
$$\sum_{i=0}^{l-1} k'_i 4^i$$
로 표현될 수 있다.
- [0101] 그리고, 연산부는 사전 연산 테이블 P , $2P$, $3P$, $4P$ 를 준비한다(S204).
- [0102] 사전 연산 테이블은 본 연산에서 디지털 값에 해당하는 ECADD 연산을 수행할 때 사용된다. 음수 디지털 값에 대한 ECADD 연산은 일반적으로 사전 연산 테이블에 저장된 점의 y 좌표(coordinate)로부터 $-y$ 좌표를 계산하여 수행된다.
- [0103] 하지만 $-y$ 좌표를 계산하는 추가연산이 발생함에 따라 부채널 정보를 통해 디지털의 부호 정보가 노출됨이 연구된 바 있다[8].
- [0104] 따라서 사전연산은 부호가 음인 디지털에 대한 연산까지 고려하여 $(x, y, -y)$ (affine coordinates)와 같이 좌표를 저장한다.
- [0105] 이후에, 연산부는 최상위 디지털부터 네배 연산을 수행하고(S206), 이후에 두 점을 더하는 연산을 수행한다(S208).
- [0106] 그리고, 연산부는 다음 하위 디지털로 네배 연산을 수행하고(S210) 두 점을 더하는 연산을 수행하며(S212) 이러한 과정을 최하위 디지털에 이르도록 수행한다(S214). 이때, 최하위 디지털인지 판단하여(S214) 최하위 디지털이면 네 배 연산을 수행하고(S216), 두점을 더하는 연산을 수행한 후에(S218) 종료한다. 이와 같은 방법의 알고리즘이 도 6에 도시되어 있다.
- [0107] 도 7은 도 5의 두 점을 더하는 연산을 설명하기 위한 흐름도이다.
- [0108] 도 7을 참조하면, 도 5의 두 점을 더하는 연산은 상기 연산부의 중간 연산 결과인 점 Q 를 $P=(X_1, Y_1, Z_1)$ 로 입력받고, 해당 디지털에 상응하는 사전연산 테이블의 한 점을 $Q=(x_2, y_2, -y_2)$ 로 입력받고, 상기 연산부가 부호화된 사진수의 해당 디지털을 참조하여 해당 디지털이 음의 수이면 1을, 양의 수이면 0을 할당받은 사인비트 s 를 입력으로 받고(S300), 상기 연산부는 두 점을 더하는 연산을 수행할 때에 사인 비트 s 가 1이면(S302) 점 Q 의 x_2 와 $-y_2$ 를 이용하여 $P-Q$ 를 연산하는 과정과(S304), 상기 연산부는 두 점을 더하는 연산을 수행할 때에 사인 비트 s 가 0이면(S302) 점 Q 의 x_2 와 y_2 를 이용하여 $P+Q$ 를 연산하는 과정(S306)을 포함한다.
- [0109] 여기에서, X_1, Y_1, Z_1 은 타원 곡선의 한 점의 야코비안 좌표의 X 축, Y 축 및 Z 축의 좌표 값이며, $x_2, y_2, -y_2$ 는 타

원 곡선의 한 점의 아핀 좌표의 x 축, y 축 및 y 축의 좌표 값이다.

이와 관련하여 도 8은 도 7의 알고리즘을 나타낸다.

도 8은 ECADD 연산이 SPA로부터 디지털의 부호 정보가 노출되지 않도록 변형했다. 변형한 알고리즘은 ECADD 연산을 수행할 두 값인 스칼라 곱셈의 중간 값과 테이블 값을 입력으로 받고 추가적으로 해당 디지털의 부호 값을 입력받는다.

ECADD 연산은 입력으로 받은 부호 값에 따라 연산에 점 Q의 y 또는 -y를 적용하도록 하여 디지털의 부호에 관계 없이 같은 과정의 연산을 수행한다.

이 과정 역시 조건문을 사용하지 않고 입력받은 부호 값을 이용한 수식 연산으로 처리하여 조건문을 통한 부채널 공격에도 안전하도록 하였다.

상기와 같은 본 발명에 의하면, 타원곡선 스칼라 곱셈 연산에 대한 SPA 및 DPA 공격에 효율적으로 대응할 수 있다.

실험을 통해 위 사실을 확인한 결과 타원곡선 연산 패턴이 비밀 정보와 무관하며 일정하게 반복되어 SPA 공격이 무의미하다.

또한 고정된 비밀 정보로 여러 번 연산을 수행하더라도 항상 다른 레코딩 결과 값으로 연산이 이뤄지기 때문에 중간 값이 모두 달라 중간 값의 추측이 불가능하다. 따라서 DPA 공격 역시 불가능하다.

실험은 ARM 보드(CPU : S3C2410(ARM920 T), Boot Flash 1MB, NAND Flash 8MB, SDRAM 64MB, 5V 전원, USB 인터페이스(115200bps))를 사용하여 진행했으며 Linux 환경에서 컴파일 하였다.

또한 본 발명은 SPA 및 DPA에 대응하는 기존의 다른 방법들에 비해 연산 효율이 우수하다. 다른 방법들과의 연산효율 비교는 표 3과 표 4를 통해 제시한다.

II 3

타원곡선 스칼라 곱셈 연산량 비교

알고리즘	SPA 대응 여부	DPA 대응 여부	ECADD	ECDBL
Ha-Moonmethod [10]	○	○	n+1	n+1
Random m-ary method [11] (2, 4, 8-ary)	○	○	0.43n+3	1.29n+3
본 발명	○	○	0.5n+1	n+2

丑 4

256비트 비밀 정보에 대한 타원곡선 스칼라 곱셈 연산량 비교

256bit	ECADD	ECDBL
Ha-Moon's method [10]	257	257
Random m-ary method [11] (2, 4, 8-ary)	113.08	333.24
본 발명	129	258

상기에서는 본 발명의 바람직한 실시 예를 참조하여 설명하였지만, 해당 기술 분야에서 통상의 지식을 가진 자라면 하기의 특허 청구범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

부호의 설명

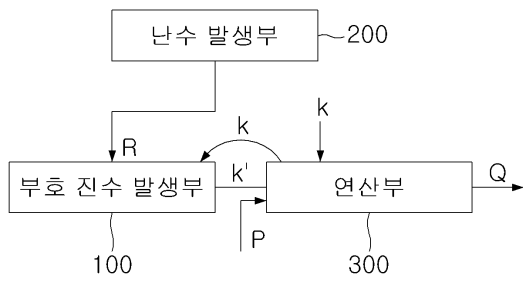
100 : 부호 진수 발생부

200 : 난수 발생부

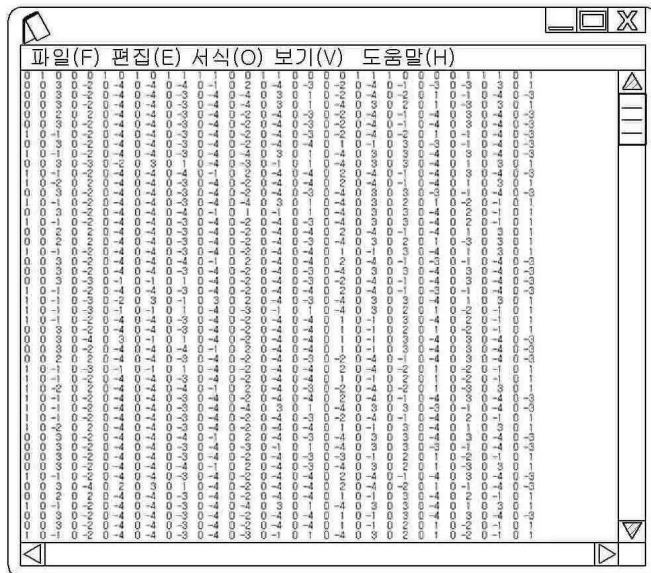
300 : 연산부

도면

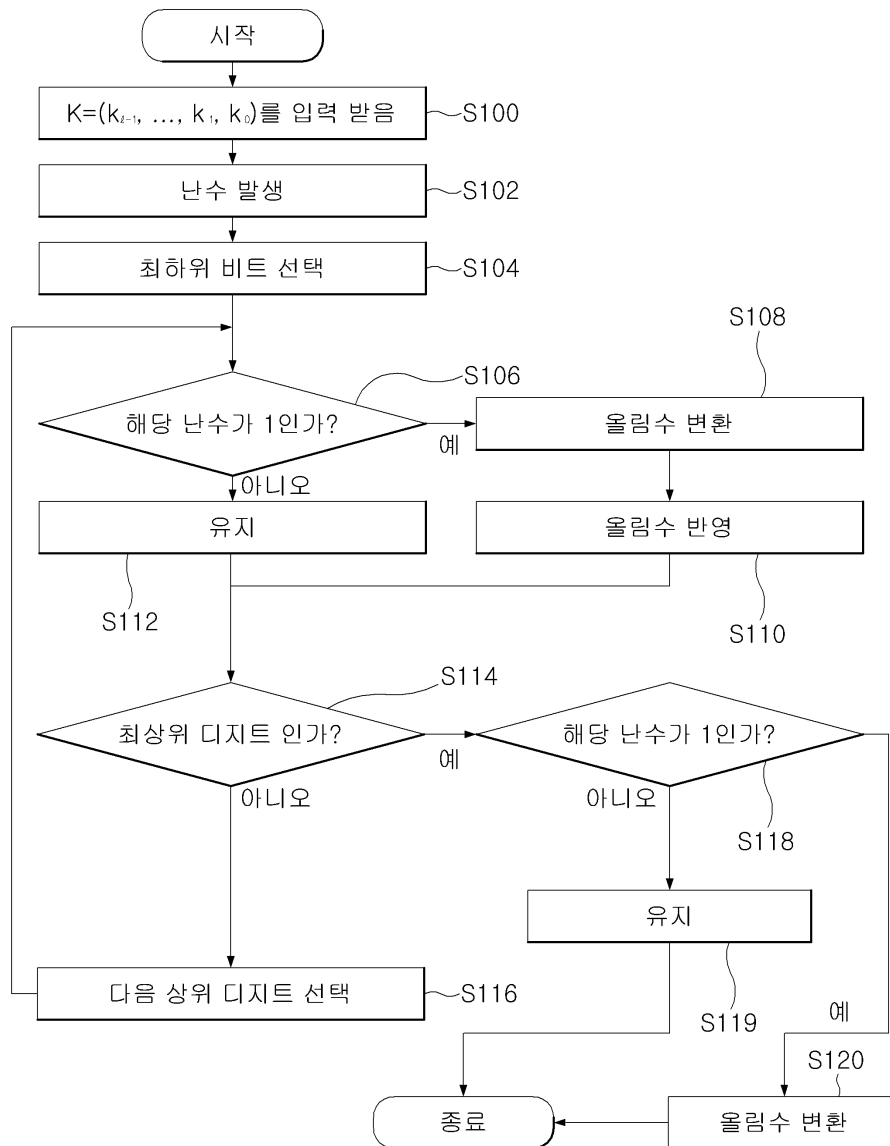
도면1



도면2



도면3



도면4

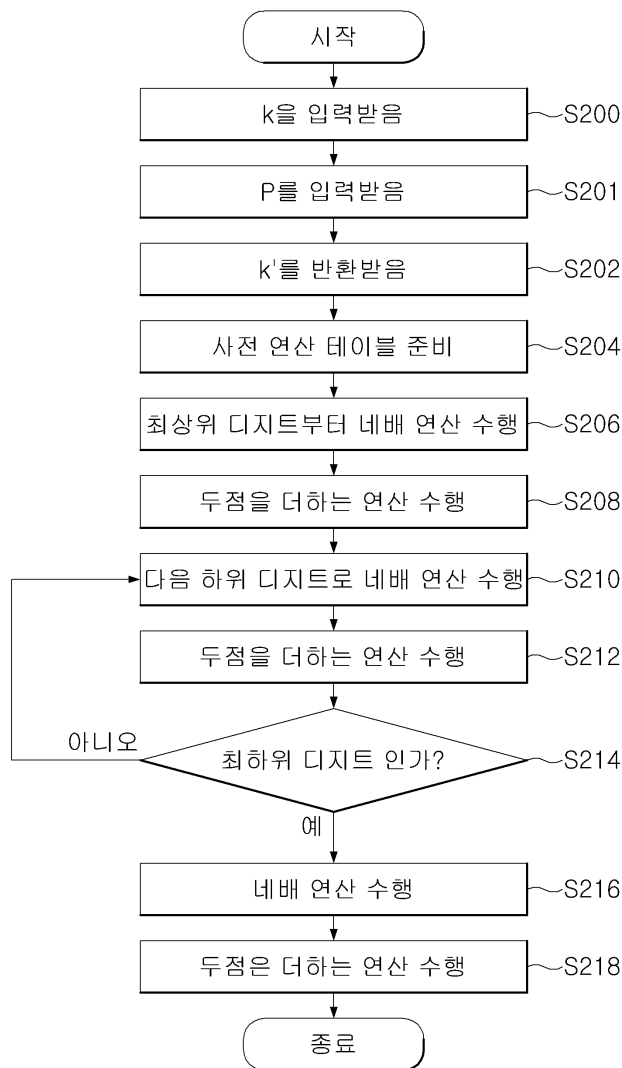
Algorithm1. Carry random recoding

INPUT : positive integer $k = (k_{l-1}, \dots, k_1, k_0)_4$.

OUTPUT : recoded scalar $k' = (k'_{t-1}, \dots, k'_1, k'_0)_4$

1. $i \leftarrow 0$
2. for i from 0 to $l-1$ do
 - 2.1 Judge the hit bit R of random number
 - 2.2 if $k \bmod 4 = 0$, then $R \leftarrow 1$.
 - 2.3 $k'_i \leftarrow (k \bmod 4) - 4 \cdot R$
 - 2.4 $k \leftarrow k/4 + R$
3. $t \leftarrow l + R$
4. Return $k' = (k'_{t-1}, \dots, k'_1, k'_0)_4$

도면5



도면6

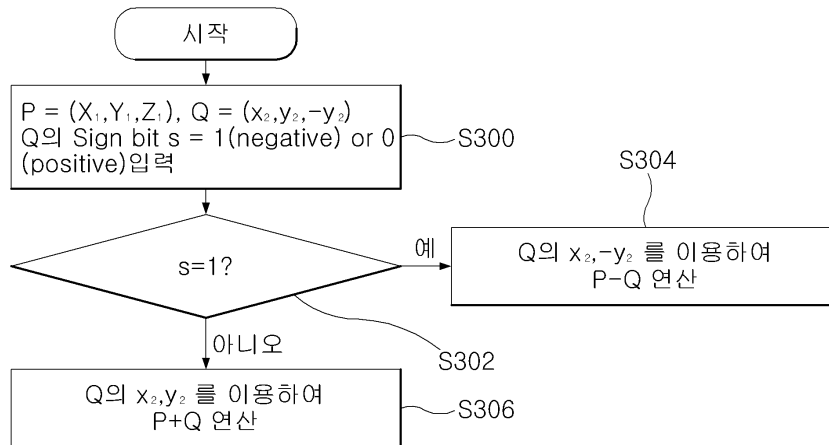
Algorithm2. Carry random recoding for point multiplication

INPUT : positive integer $k, P \in E(\mathbb{F}_q)$.

OUTPUT : kP .

1. Use Algorithm1 to compute $k' = \sum_{i=0}^{l-1} k'_i 4^i$,
2. Compute $P_i = iP$ for $i \in \{1, 2, 3, 4\}$
3. $Q \leftarrow \infty$
4. For i from $l-1$ downto 0 do
 - 4.1 $Q \leftarrow 4Q$.
 - 4.2 $Q \leftarrow Q + P_{k'_i}$.
5. Return(Q).

도면7



도면8

Algorithm3. Signed point addition using affine-Jacobian coordinates on Weierstrass curves.

INPUT : $P, Q \in E(\mathbb{F}_q)$ such that $P = (X_1, Y_1, Z_1)$ is in Jacobian coordinates,

$Q = (x_2, y_2, -y_2)$ is in affine coordinates,

$s = 1$ (negative) or 0 (positive) is sign bit of operand Q .

OUTPUT : $P + Q = (X_3, Y_3, Z_3) \in E(\mathbb{F}_q)$ in Jacobian coordinates.

- | | |
|--|--------------------------------------|
| 1. if $P = O$ then return Q | 14. $t_3 = t_1^2$ |
| 2. if $Q = O$ then return P | 15. $t_4 = t_3 \times t_1$ |
| 3. $t_1 = Z_1^2$ | 16. $t_3 = t_3 \times X_1$ |
| 4. $t_2 = t_1 \times Z_1$ | 17. $t_1 = 2t_3$ |
| 5. $t_1 = t_1 \times x_2$ | 18. $X_3 = t_2^2$ |
| 6. $t_2 = \{(1-s)y_2 - s(-y_2)\} \times t_2$ | 19. $X_3 = X_3 - t_1$ |
| 7. $t_1 = t_1 - X_1$ | 20. $X_3 = X_3 - t_4$ |
| 8. $t_2 = t_2 - Y_1$ | 21. $t_3 = t_3 - X_3$ |
| 9. if $t_1 = 0$ then | 22. $t_3 = t_3 \times t_2$ |
| 10. if $t_2 = 0$ then | 23. $t_4 = t_4 \times Y_1$ |
| 11. Use point doubling algorithm | 24. $Y_3 = t_3 - t_4$ |
| 12. else return O | 25. Return $P - Q = (X_3, Y_3, Z_3)$ |
| 13. $Z_3 = Z_1 \times t_1$ | |