

	(19) 대한민국특허청(KR) (12) 공개특허공보(A)	(11) 공개번호 10-2010-0098017 (43) 공개일자 2010년09월06일
(51) Int. Cl. <i>H04L 9/28</i> (2006.01) <i>G06F 7/38</i> (2006.01) (21) 출원번호 10-2009-0016972 (22) 출원일자 2009년02월27일 심사청구일자 2009년02월27일	(71) 출원인 고려대학교 산학협력단 서울 성북구 안암동5가 1 (72) 발명자 홍석희 서울특별시 도봉구 도봉동 한신아파트 103동 107호 조성민 서울특별시 성북구 장위3동 6-104 2층 201호 (뒷면에 계속) (74) 대리인 특허법인충현	

전체 청구항 수 : 총 15 항

(54) 확장된 몽고메리 레더를 이용한 스칼라 곱셈 방법

(57) 요약

본 발명은 확장된 몽고메리 레더를 이용한 스칼라 곱셈 방법에 관한 것으로, 본 발명의 일 실시 예에 따른 확장된 몽고메리 레더를 이용한 스칼라 곱셈 방법은 타원 곡선 암호 시스템에서 몽고메리 레더의 키 값을 3진수(ternary)로 표현하는 단계; 및 상기 몽고메리 레더에 복합 연산에 대해 x좌표만을 이용한 연산식을 적용하고, 상기 3진수의 키 값에 대해 상기 몽고메리 레더에 따른 스칼라 곱셈을 수행하는 단계를 포함한다. 본 발명에 의하면, $GF(2^m)$ 상에서 단순전력분석에 대한 안전성을 유지하면서, 기존의 타원곡선 스칼라 곱셈 알고리즘보다 연산 속도를 향상시킬 수 있다.

대표도 - 도5

1. INPUT: 상수 $d = d_{n-1}3^{n-1} + \dots + d_0$ ($d_{n-1} = 1$ 또는 2), 점 P
2. OUTPUT: dP
3. $Q[0] = d_{n-1}P$, $Q[0] = (d_{n-1} + 1)P$
4. for $i \leftarrow n-2$ downto 0
5. $Q[2] = ECDA^x(Q[d_i^H], Q[\overline{d_i^H}])$,
6. $Q[d_i^H \vee d_i^L] = atomicECDA^x(Q[d_i^H \vee d_i^L], Q[d_i^H])$,
7. $Q[\overline{d_i^H \vee d_i^L}] = Q[2]$.

(72) 발명자

김태현

서울 강서구 화곡2동 846-19

서석충

서울 중랑구 망우1동 153-60호

특허청구의 범위

청구항 1

$GF(2^m)$ 상의 비 초특이 타원 곡선(non-supersingular elliptic curve)에서 스칼라 곱셈을 수행하는 방법에 있어서,

타원 곡선 암호 시스템에서 몽고메리 레더의 키 값을 3진수 (ternary)로 표현하는 단계; 및

상기 몽고메리 레더에 복합 연산에 대해 x좌표만을 이용한 연산식을 적용하고, 상기 3진수의 키 값에 대해 상기 몽고메리 레더에 따른 스칼라 곱셈을 수행하는 단계

를 포함하는, 확장된 몽고메리 레더를 이용한 스칼라 곱셈 방법.

청구항 2

제1항에 있어서,

상기 스칼라 곱셈을 수행하는 단계는,

상기 x좌표만을 이용한 연산식을 위한 유한체 역원연산에 몽고메리 트릭 (Montgomery trick)을 적용하는 단계를 포함하는 것을 특징으로 하는, 확장된 몽고메리 레더를 이용한 스칼라 곱셈 방법.

청구항 3

제1항에 있어서,

상기 스칼라 곱셈을 수행하는 단계는,

상기 x좌표만을 이용한 연산식을 위한 원자블록들 중 적어도 하나에 더미 연산을 추가하여 부채널 원자성 (Side-channel atomicity)을 적용하는 단계를 포함하는 것을 특징으로 하는, 확장된 몽고메리 레더를 이용한 스칼라 곱셈 방법.

청구항 4

제1항에 있어서,

상기 x좌표만을 이용한 연산식은,

상기 타원 곡선 상의 서로 다른 두 점을 더하는 ECADD (Elliptic curve point addition) 및 상기 타원 곡선 상의 같은 점을 더하는 ECDBL (Elliptic curve point doubling)을 기반으로 변형된 연산식인 것을 특징으로 하는, 확장된 몽고메리 레더를 이용한 스칼라 곱셈 방법.

청구항 5

제4항에 있어서,

상기 x좌표만을 이용한 연산식은,

상기 타원 곡선 상의 임의의 두 점을 각각 $P_1=(x_1, y_1)$, $P_2=(x_2, y_2)$ ($P_1 \neq P_2$)라 하고, b는 타원 곡선 방정식의 계수이며, $3P_1$ 의 연산을 ECTPL (Elliptic curve point tripling)라 할 때, 하기의 수학식 (1)에 따른 연산식을 포함하는 것을 특징으로 하는, 확장된 몽고메리 레더를 이용한 스칼라 곱셈 방법.

$$ECTPL^x (P_3=3P_1=(x_3, y_3)), \quad x_3=x_1+\left(\frac{x_1^3}{x_1^4+x_1^3+b}\right)+\left(\frac{x_1^3}{x_1^4+x_1^3+b}\right)^2 \quad (1)$$

청구항 6

제4항에 있어서,

상기 x좌표만을 이용한 연산식은,

상기 타원 곡선 상의 임의의 두 점을 각각 $P_1=(x_1, y_1)$, $P_2=(x_2, y_2)$ ($P_1 \neq P_2$)라 하며, $2P_1+P_2$ 의 연산을 ECDA (Elliptic curve point double-and-add)라 할 때, 하기의 수학식 (2)에 따른 연산식을 포함하는 것을 특징으로 하는, 확장된 몽고메리 레더를 이용한 스칼라 곱셈 방법.

$$ECDA^x (P_4=2P_1+P_2=(x_4, y_4)), \quad x_4=x_2+\left(\frac{x_1(x_1+x_2)^2}{(x+x_1)(x_1+x_2)^2+x_1x_2}\right)+\left(\frac{x_1(x_1+x_2)^2}{(x+x_1)(x_1+x_2)^2+x_1x_2}\right)^2 \quad (2)$$

청구항 7

$GF(2^m)$ 상의 비 초특이 타원 곡선(non-supersingular elliptic curve)에서 스칼라 곱셈을 수행하는 방법에 있어서,

타원 곡선 암호 시스템에서 몽고메리 레더의 키 값을 4진수 (quaternary)로 표현하는 단계; 및

상기 몽고메리 레더에 x좌표만을 이용한 복합 연산에 대한 연산식을 적용하고, 상기 4진수의 키 값에 대해 상기 몽고메리 레더에 따른 스칼라 곱셈을 수행하는 단계

를 포함하는, 확장된 몽고메리 레더를 이용한 스칼라 곱셈 방법.

청구항 8

제7항에 있어서,

상기 스칼라 곱셈을 수행하는 단계는,

상기 x좌표만을 이용한 연산식을 위한 유한체 역원연산에 몽고메리 트릭 (Montgomery trick)을 적용하는 단계를 포함하는 것을 특징으로 하는, 확장된 몽고메리 레더를 이용한 스칼라 곱셈 방법.

청구항 9

제7항에 있어서,

상기 스칼라 곱셈을 수행하는 단계는,

상기 x좌표만을 이용한 연산식을 위한 원자블록들 중 적어도 하나에 더미 연산을 추가하여 부채널 원자성 (Side-channel atomicity)을 적용하는 단계를 포함하는 것을 특징으로 하는, 확장된 몽고메리 레더를 이용한 스칼라 곱셈 방법.

청구항 10

제7항에 있어서,

상기 x좌표만을 이용한 연산식은,

상기 타원 곡선 상의 임의의 두 점을 각각 $P_1=(x_1, y_1)$, $P_2=(x_2, y_2)$ ($P_1 \neq P_2$)라 하고, b는 타원 곡선 방정식의 계수이며, $4P_1$ 의 연산을 ECQPL (Elliptic curve point quadrupling)이라 할 때, 하기의 수학식 (3)에 따른 연산식을 포함하는 것을 특징으로 하는, 확장된 몽고메리 레더를 이용한 스칼라 곱셈 방법.

$$ECQPL^x (P_5=4P_1=(x_5, y_5)), \quad x_5=x_1+\frac{b^2(x_1^4+b)^2+bx_1^8}{x_1^4(x_1^4+b)^2} \quad (3)$$

청구항 11

제7항에 있어서,

상기 x좌표만을 이용한 연산식은,

상기 타원 곡선 상의 임의의 두 점을 각각 $P_1=(x_1, y_1)$, $P_2=(x_2, y_2)$ ($P_1 \neq P_2$)라 하고, $2P_1+2P_2$ 의 연산을 ECDAD (Elliptic curve point double-add-double)라 할 때, 하기의 수학식 (4)에 따른 연산식을 포함하는 것을 특징으로 하는, 확장된 몽고메리 레더를 이용한 스칼라 곱셈 방법.

$$ECDAD^x (P_6=2P_1+2P_2=(x_6, y_6)), \quad x_6=x_0+\left(\frac{x_1^2(x_2^4+b)}{(x_1^2x_2^2+b)(x_1^2+x_2^2)}\right)+\left(\frac{x_1^2(x_2^4+b)}{(x_1^2x_2^2+b)(x_1^2+x_2^2)}\right)^2 \quad (4)$$

청구항 12

제7항에 있어서,

상기 x좌표만을 이용한 연산식은,

상기 타원 곡선 상의 임의의 두 점을 각각 $P_1=(x_1, y_1)$, $P_2=(x_2, y_2)$ ($P_1 \neq P_2$)라 하고, $3P_1+P_2$ 의 연산을 ECTA (Elliptic curve point triple-and-add)라 할 때, 하기의 수학식 (5)에 따른 연산식을 포함하는 것을 특징으로 하는, 확장된 몽고메리 레더를 이용한 스칼라 곱셈 방법.

$$ECTA^x (P_7=3P_1+P_2=(x_7, y_7)), \quad x_7=x+\left(\frac{(x_1^4+b)(x_1+x_2)^2}{x_1^2\{x(x_1+x_2)^2+x_1x_2\}+(x_1^4+b)(x_1+x_2)^2}\right)+\left(\frac{(x_1^4+b)(x_1+x_2)^2}{x_1^2\{x(x_1+x_2)^2+x_1x_2\}+(x_1^4+b)(x_1+x_2)^2}\right)^2 \quad (5)$$

청구항 13

$GF(2^m)$ 상의 비 초특이 타원 곡선(non-supersingular elliptic curve)에서 스칼라 곱셈을 수행하는 방법에 있어서,

타원 곡선 암호 시스템에서 몽고메리 레더의 키 값을 3진수 (ternary)로 표현하는 단계; 및

상기 몽고메리 레더에 복합 연산에 대해 x좌표만을 이용한 연산식을 적용하고, 상기 3진수의 키 값에 대해 상기 몽고메리 레더에 따른 스칼라 곱셈을 두 개의 레지스터를 사용하여 수행하는 단계

를 포함하는, 확장된 몽고메리 레더를 이용한 스칼라 곱셈 방법.

청구항 14

$GF(2^m)$ 상의 비 초특이 타원 곡선(non-supersingular elliptic curve)에서 스칼라 곱셈을 수행하는 방법에 있어서,

타원 곡선 암호 시스템에서 몽고메리 레더의 키 값을 4진수 (quaternary)로 표현하는 단계; 및

x좌표만을 이용한 복합 연산에 대한 연산식을 상기 몽고메리 레더에 적용하고, 상기 4진수의 키 값에 대해 상기 몽고메리 레더에 따른 스칼라 곱셈을 두 개의 레지스터를 사용하여 수행하는 단계

를 포함하는, 확장된 몽고메리 레더를 이용한 스칼라 곱셈 방법.

청구항 15

제 1 항 내지 제 14 항 중 어느 한 항에 따른 확장된 몽고메리 레더를 이용한 스칼라 곱셈 방법을 컴퓨터 시스템에서 실행하기 위한 프로그램이 기록된 컴퓨터 시스템이 판독할 수 있는 기록매체.

명 세 서

발명의 상세한 설명

기술 분야

[0001] 본 발명은 스칼라 곱셈 연산에 관한 것으로, 특히, 타원 곡선 암호 시스템에서 스칼라 곱셈 연산을 단순전력분석에 안전하게 하면서 연산속도를 향상시킬 수 있는 방법에 관한 것이다.

배경 기술

[0002] 정보화 사회의 도래와 함께 암호 알고리즘 및 암호 프로토콜(Protocol)을 이용한 정보의 보호는 그 중요성을 더해가고 있다. 정보를 보호하는데 사용되는 암호 알고리즘 중에서 RSA(Rivest Shamir Adleman) 암호시스템 및 타원 곡선 암호 시스템(Elliptic Curve Cryptography)에서 사용하는 공개키(open key) 암호 알고리즘은, 비밀키(Secret Key) 암호 알고리즘의 단점인 키(Key) 분배 문제, 전자서명 문제 등을 해결하면서 인터넷이나 금융망과 같은 여러 분야의 응용에 빠르게 적용되고 있다.

[0003] 타원 곡선 암호 시스템은 기존의 RSA와 엘가말(ElGamal) 공개키 암호시스템과 비교하여 훨씬 짧은 길이의 키로도 비슷한 보안성을 제공한다는 장점을 가지고 있다. 키의 길이가 짧다는 장점 때문에 저전력을 사용하는 스마트카드나 PDA 등에 많이 사용된다.

[0004] 타원 곡선 암호 시스템의 안전성과 효율성에 가장 큰 영향을 주는 연산은 타원곡선 스칼라 곱셈이다. d 를 양의 정수라 하고, P 를 타원곡선 위의 한 점이라고 할 때, P 를 d 번 더하는 연산을 타원곡선 스칼라 곱셈이라 한다. 타원곡선 스칼라 곱셈은 타원곡선 암호 시스템의 안전성과 효율성에 가장 큰 영향을 주는 연산이다. 스칼라 곱셈을 구현하는 가장 일반적이고 기본적인 방법으로 레프트-투-라이트 바이너리 방법(Left-to-right binary method)이 있다.

[0005] 전력분석은 타원곡선 스칼라 곱셈 알고리즘에 대한 강력한 공격방법으로 스마트카드와 같은 모바일 장치에서 암호알고리즘이 동작할 때 소모되는 전력정보를 이용한 공격 방법이다. 전력분석은 단순전력분석과 차분전력분석으로 나눌 수 있다. 단순전력분석은 한 번의 알고리즘 수행에 의한 전력 소모량을 가지고 분석하는 방법으로 비밀키에 의존하는 공개키 암호 연산에 적용된다. 차분전력분석은 고정된 비밀키에 대한 암호 연산의 서로 다른 데이터에 대한 다수의 수행과정에서 비밀키의 특정 비트 값에 의존하는 중간 계산 값과 해당 전력소모량 사이의 상관관계를 통계적으로 분석하는 공격 방법이다. 타원곡선 스칼라 곱셈에 사용되는 연산들은 서로 다른 연산량과 연산순서를 가지고, 키 비트에 의존해서 실행되는 연산에 차이가 생기기 때문에 단순전력분석에 의한 분석이 많이 진행 되었다.

[0006] 타원곡선 스칼라 곱셈 알고리즘에 대한 단순전력분석이 진행되면서 이를 방어하기 위한 많은 대응방법들이 제안되었다. 이즈-타카기(Izu-Takagi)들은 키 값을 이진법으로 표현하고 두 개의 레지스터를 이용하는 몽고메리 레더(Montgomery ladder) 방법을 제안하고 효율성을 높이기 위하여 확장 바이너리 방법(extended binary method)을 이용한 변형된 몽고메리 레더 알고리즘을 제안하였다. 변형된 몽고메리 레더 방법은 한 번의 타원곡선 배증(doubling)과 세 번의 타원곡선 덧셈(addition)을 이용하며 모두 병렬적으로 연산이 가능하다. 그러나 이 방법은 네 개의 레지스터를 사용한다는 단점을 가지고 있다. 그리고, 추가적인 연산을 최소화 되고, 단순전력분석에 안전하도록 하는 부채널 원자성(Side-channel atomicity) 방법이 제안되기도 하였다. 레프트-투-라이트 바이너리 방법(Left-to-right binary method)에 유한체 덧셈만을 추가하는 부채널 원자 배증 및 덧셈(Side-channel atomic double and add) 알고리즘은 몽고메리 레더 방법보다 연산속도가 빠르다. 그리고 사전테이블을 이용하는 콤(comb) 방법과 윈도우(window) 방법 등 단순전력분석에 안전하면서 연산속도를 향상시키는 많은 알고리즘이 제안되었다.

발명의 내용

해결 하고자하는 과제

[0007] 본 발명이 이루고자 하는 기술적 과제는 $GF(2^m)$ 상에서 단순전력분석에 대한 안전성을 유지하면서, 기존의 타원곡선 스칼라 곱셈 알고리즘보다 연산속도를 향상시킬 수 확장된 몽고메리 레더를 이용한 스칼라 곱셈 방법을 제공하는 데 있다.

과제 해결수단

[0008] 상기의 기술적 과제를 이루기 위하여, 본 발명의 일 실시 예에 따른 확장된 몽고메리 레더를 이용한 스칼라 곱셈 방법은 타원 곡선 암호 시스템에서 몽고메리 레더의 키 값을 3진수(ternary)로 표현하는 단계; 및 상기 몽고메리 레더에 복합 연산에 대해 x 좌표만을 이용한 연산식을 적용하고, 상기 3진수의 키 값에 대해 상기 몽고메리

리 레더에 따른 스칼라 곱셈을 수행하는 단계를 포함한다.

- [0009] 바람직하게는, 상기 스칼라 곱셈을 수행하는 단계에서, 상기 x좌표만을 이용한 연산식을 위한 유한체 역원연산에 몽고메리 트릭(Montgomery trick)을 적용할 수 있다.
- [0010] 바람직하게는, 상기 스칼라 곱셈을 수행하는 단계에서, 상기 x좌표만을 이용한 연산식을 위한 원자블록들 중 적어도 하나에 더미 연산을 추가하여 부채널 원자성을 적용할 수 있다.
- [0011] 바람직하게는, 상기 x좌표만을 이용한 연산식은 상기 타원 곡선 상의 서로 다른 두 점을 더하는 ECADD(Elliptic curve point addition) 및 상기 타원 곡선 상의 같은 점을 더하는 ECDBL(Elliptic curve point doubling)을 기반으로 변형된 연산식일 수 있다.
- [0012] 상기의 기술적 과제를 이루기 위하여, 본 발명의 다른 실시 예에 따른 확장된 몽고메리 레더를 이용한 스칼라 곱셈 방법은 타원 곡선 암호 시스템에서 몽고메리 레더의 키 값을 4진수(quaternary)로 표현하는 단계; 및 상기 몽고메리 레더에 x좌표만을 이용한 복합 연산에 대한 연산식을 적용하고, 상기 4진수의 키 값에 대해 상기 몽고메리 레더에 따른 스칼라 곱셈을 수행하는 단계를 포함한다.
- [0013] 바람직하게는, 상기 스칼라 곱셈을 수행하는 단계에서, 상기 x좌표만을 이용한 연산식을 위한 유한체 역원연산에 몽고메리 트릭을 적용할 수 있다.
- [0014] 바람직하게는, 상기 스칼라 곱셈을 수행하는 단계에서, 상기 x좌표만을 이용한 연산식을 위한 원자블록들 중 적어도 하나에 더미 연산을 추가하여 부채널 원자성을 적용할 수 있다.
- [0015] 상기의 기술적 과제를 이루기 위하여, 본 발명의 또 다른 실시 예에 따른 확장된 몽고메리 레더를 이용한 스칼라 곱셈 방법은 $GF(2^m)$ 상의 비 초특이 타원 곡선(non-supersingular elliptic curve)에서, 타원 곡선 암호 시스템에서 몽고메리 레더의 키 값을 3진수로 표현하는 단계; 및 상기 몽고메리 레더에 복합 연산에 대해 x좌표만을 이용한 연산식을 적용하고, 상기 3진수의 키 값에 대해 상기 몽고메리 레더에 따른 스칼라 곱셈을 두 개의 레지스터를 사용하여 수행하는 단계를 포함한다.
- [0016] 상기의 기술적 과제를 이루기 위하여, 본 발명의 또 다른 실시 예에 따른 확장된 몽고메리 레더를 이용한 스칼라 곱셈 방법은 $GF(2^m)$ 상의 비 초특이 타원 곡선에서, 타원 곡선 암호 시스템에서 몽고메리 레더의 키 값을 4진수로 표현하는 단계; 및 x좌표만을 이용한 복합 연산에 대한 연산식을 상기 몽고메리 레더에 적용하고, 상기 4진수의 키 값에 대해 상기 몽고메리 레더에 따른 스칼라 곱셈을 두 개의 레지스터를 사용하여 수행하는 단계를 포함한다.

효 과

- [0017] 본 발명에 의하면, $GF(2^m)$ 상에서 단순전력분석에 대한 안전성을 유지하면서, 기존의 타원곡선 스칼라 곱셈 알고리즘보다 연산속도를 향상시킬 수 있다.

발명의 실시를 위한 구체적인 내용

- [0018] 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.

- [0019] 도 1 및 2는 몽고메리 레더 방법에서의 키 값을 3진수 또는 4진수로 표현했을 때의 새로운 덧셈체인을 나타낸 것이다.

- [0020] 비밀키인 양의 정수 d 를 $d = d_{n-1}3^{n-1} + \dots + d_0 (d_{n-1} = 1, 2)$ 와 같이 3진수로 표현하는 경우를 설명한다. 몽고메리 레더의 특성을 유지하도록 i 번째 비트까지의 합을 $Q[0]_i = \left(\sum_{k=1}^i d_{n-k} 3^{i-k} \right) P$ 와 같이 정의하고, $Q[1]_i = Q[0]_i + P$ 라고 정의하면, d_{n-i+1} 의 값에 의존하여 $Q[0]_{i+1}, Q[1]_{i+1}$ 와 $Q[0]_i, Q[1]_i$ 의 관계를 다음과 같이 나타낼 수 있고, $Q[1]_{i+1} = Q[0]_{i+1} + P$ 의 관계를 유지함을 알 수 있다.

[0021] 즉, $d_{n-i-1}=0$ 이면, $Q[0]_{i+1}=3Q[0]_i, Q[1]_{i+1}=2Q[0]_i+Q[1]_i, d_{n-i-1}=1$ 이면, $Q[0]_{i+1}=2Q[0]_i+Q[1]_i, Q[1]_{i+1}=2Q[1]_i+Q[0]_i, d_{n-i-1}=2$ 이면, $Q[0]_{i+1}=2Q[1]_i+Q[0]_i, Q[1]_{i+1}=3Q[1]_i$ 의 관계를 갖는다.

[0022] 이와 같이 비밀키 d 를 3진수로 표현했을 때, $Q[0]_{i+1}$ 과 $Q[1]_{i+1}$ 은 d_{n-i-1} 의 값에 따라서 이전에 계산된 $Q[0]_i$ 와 $Q[1]_i$ 를 이용하여 $3P$ 또는 $2P+Q$ 의 형태로 계산된다. $3P$ 와 $2P+Q$ 의 연산은 기존의 복합 연산 (composite operation)이 적용가능하다. 서로 다른 두 점을 $2P+Q$ 하는 연산을 ECDA (Elliptic curve point double-and-add)라 하고, 같은 점을 $3P$ 하는 연산을 ECTPL (Elliptic curve point tripling)이라고 한다. 그러면, d 를 3진수로 표현했을 때의 확장된 몽고메리 레더는 도 1로 나타낼 수 있다. 도 1에서의 ECTPL과 ECDA는 각각 타원곡선 상의 두 점 P, Q 에 대한 $3P$ 와 $2P+Q$ 연산을 의미한다.

[0023] 확장된 3진수 몽고메리 레더는 매 루프마다 $Q[0]$ 와 $Q[1]$ 의 차이가 P 를 유지하는 성질을 가지고 있다. 이 특성을 이용하여 x좌표만을 이용하는 몽고메리 레더를 구성할 수 있다.

[0024] 다음으로, 비밀키인 양의 정수 d 값을 $d=d_{n-1}4^{n-1}+\dots+d_0(d_{n-1}=1,2,3)$ 와 같이 4진수로 표현하는 경우를 설명한다. 마찬가지로 i 번째 비트까지의 합을 $Q[0]_i=(\sum_{k=1}^i d_{n-k}4^{i-k})P$ 와 같이 정의하고 $Q[1]_i=Q[0]_i+P$ 이라고 정의하면, d_{n-i-1} 의 값에 의존하여 $Q[0]_{i+1}, Q[1]_{i+1}$ 와 $Q[0]_i, Q[1]_i$ 의 관계를 다음과 같이 나타낼 수 있고, $Q[1]_{i+1}=Q[0]_{i+1}+P$ 의 관계를 유지함을 알 수 있다.

[0025] 즉, $d_{n-i-1}=0$ 이면, $Q[0]_{i+1}=4Q[0]_i, Q[1]_{i+1}=3Q[0]_i+Q[1]_i, d_{n-i-1}=1$ 이면, $Q[0]_{i+1}=3Q[0]_i+Q[1]_i, Q[1]_{i+1}=2Q[0]_i+2Q[1]_i, d_{n-i-1}=2$ 이면, $Q[0]_{i+1}=2Q[0]_i+2Q[1]_i, Q[1]_{i+1}=3Q[1]_i+Q[0]_i, d_{n-i-1}=3$ 이면, $Q[0]_{i+1}=3Q[1]_i+Q[0]_i, Q[1]_{i+1}=4Q[1]_i$ 의 관계를 갖는다.

[0026] 이와 같이 비밀키 d 를 4진수로 표현했을 때, $Q[0]_{i+1}$ 과 $Q[1]_{i+1}$ 은 d_{n-i-1} 의 값에 따라서 이전에 계산된 $Q[0]_i$ 와 $Q[1]_i$ 를 이용하여 $2P+2Q, 3P+Q$ 또는 $4P$ 의 복합 연산의 형태로 계산된다. 서로 다른 두 점의 $2P_1+2P_2$ 형태의 연산을 ECDAD (Elliptic curve point double-add-double), $3P_1+P_2$ 형태의 연산을 ECTA (Elliptic curve point triple-and-add)라 하고 같은 점을 $4P_1$ 하는 연산을 ECQPL (Elliptic curve point quadrupling)이라고 한다. 그러면, d 를 4진수로 표현했을 때의 확장된 몽고메리 레더는 도 2와 같이 나타낼 수 있다. 도 2에서의 ECQPL, ECDAD와 ECTA는 각각 $4P, 2P+2Q, 3P+Q$ 연산을 의미한다.

[0027] 확장된 4진수 몽고메리 레더 또한 매 루프마다 $Q[0]$ 와 $Q[1]$ 의 차이가 P 를 유지하는 성질을 가지고 있다. 이 특성을 이용하여 x좌표만을 이용하는 확장된 4진수 몽고메리 레더를 구성할 수 있다.

[0028] 이하에서는 알고리즘의 효율적인 연산을 위해, 복합 연산에 대해서 x좌표만을 이용하는 새로운 연산식들을 설명한다.

[0029] 본 발명의 일 실시 예에 따른 덧셈체인에서는 연산을 효율적으로 하기 위해서 $GF(2^m)$ 상에서 x좌표만을 이용하는 새로운 연산식들을 사용한다.

[0030] 서로 다른 두 점을 더하는 연산을 ECADD (Elliptic curve point addition)라 하고 같은 점을 더하는 연산을

ECDBL (Elliptic curve point doubling)이라고 한다. ECADD와 ECDBL은 모두 두 번의 유한체 곱셈, 한 번의 유한체 제곱과 한 번의 유한체 역원연산이 필요하다.

[0031] 이하에서 설명하는, x좌표만을 이용하는 새로운 연산식은 $ECADD^x$ 와 $ECDBL^x$ 에 기반을 두고 식을 변형한 형태이다. 타원곡선상의 임의의 두 점을 각각 $P_1=(x_1, y_1)$, $P_2=(x_2, y_2)$ 라 하고, 두 점의 차를 $P=P_2-P_1=(x_3, y_3)$ ($P_1 \neq P_2$)라 가정한다. 그리고 $2P=2(P_2-P_1)=(x_0, y_0)$ 라 가정한다.

[0032] 먼저 확장된 3진수 몽고메리 레더 방법에서의 ECTPL과 ECDA연산에 대한 x좌표만을 이용하는 방법은 각각 다음의 수학식 1 및 2와 같다. 이하에서, 상수 b는 타원 곡선 방정식의 계수를 나타낸다.

수학식 1

[0033] $ECTPL^x$ ($P_3=3P_1=(x_3, y_3)$),

$$x_3=x_1+\left(\frac{x_1^3}{x_1^4+x_1^3+b}\right)+\left(\frac{x_1^3}{x_1^4+x_1^3+b}\right)^2$$

[0034]

수학식 2

[0035] $ECDA^x$ ($P_4=2P_1+P_2=(x_4, y_4)$),

$$x_4=x_2+\left(\frac{x_1(x_1+x_2)^2}{(x+x_1)(x_1+x_2)^2+x_1x_2}\right)+\left(\frac{x_1(x_1+x_2)^2}{(x+x_1)(x_1+x_2)^2+x_1x_2}\right)^2$$

[0036]

[0037] 마찬가지로 확장된 4진수 몽고메리 레더 방법에서의 ECQPL, ECDAD와 ECTA연산에 대한 x좌표만을 이용하는 방법은 각각 다음의 수학식 3, 4, 5와 같다.

수학식 3

[0038] $ECQPL^x$ ($P_5=4P_1=(x_5, y_5)$),

$$x_5=x_1+\frac{b^2(x_1^4+b)^2+bx_1^8}{x_1^4(x_1^4+b)^2}$$

[0039]

수학식 4

[0040] $ECDAD^x$ ($P_6=2P_1+2P_2=(x_6, y_6)$),

$$x_6=x_0+\left(\frac{x_1^2(x_2^4+b)}{(x_1^2x_2^2+b)(x_1^2+x_2^2)}\right)+\left(\frac{x_1^2(x_2^4+b)}{(x_1^2x_2^2+b)(x_1^2+x_2^2)}\right)^2$$

[0041]

수학식 5

[0042] $ECTA^x$ ($P_7=3P_1+P_2=(x_7, y_7)$),

$$x_7=x+\left(\frac{(x_1^4+b)(x_1+x_2)^2}{x_1^2\{x(x_1+x_2)^2+x_1x_2\}+(x_1^4+b)(x_1+x_2)^2}\right)+\left(\frac{(x_1^4+b)(x_1+x_2)^2}{x_1^2\{x(x_1+x_2)^2+x_1x_2\}+(x_1^4+b)(x_1+x_2)^2}\right)^2$$

[0043]

- [0044] 본 발명의 일 실시 예에 따른 확장된 몽고메리 레더 방법은 단순전력분석에 취약함을 보완하기 위하여 부채널 원자성을 적용할 수 있다.
- [0045] 도 3a, 3b, 4a 및 4c는 부채널 원자성을 적용한 원자블록 (atomic block)을 도시한 것이다.
- [0046] 도 3a는 $GF(2^m)$ 상에서 $ECDA^x$ 와 $ECTPL^x$ 알고리즘의 연산순서와 연산량을 같게하는 것을 나타내고, 도 3b는 부채널 원자성이 적용된 $ECDA^x$ 또는 $ECTPL^x$ 을 출력하는 블록을 나타낸다.
- [0047] 도 3a 및 3b를 참고로, 확장된 3진수 몽고메리 레더 알고리즘의 경우에 대한 부채널 원자성을 적용하는 방법에 대하여 설명한다. 이 알고리즘은 키의 값에 의존해서 $ECTPL^x$, $ECDA^x$ 또는 $ECDA^x$, $ECDA^x$ 가 연산되는 문제점이 있다. 한 번의 루프에서 연되는 $ECTPL^x$, $ECDA^x$ 또는 $ECDA^x$, $ECDA^x$ 를 두 개의 원자블록인 γ_1 과 γ_2 로 나눈다. 여기서 γ_1 을 공통으로 연산되는 $ECDA^x$, γ_2 를 서로 다른 연산인 $ECTPL^x$ 와 $ECDA^x$ 로 한다. γ_1 은 같은 $ECDA^x$ 연산이므로 연산순서나 더미 연산이 불필요하다. 반면에 γ_2 는 $ECTPL^x$ 또는 $ECDA^x$ 를 연산해 주어야 하므로 원자블록을 만들어 줄 필요가 있다. 본 발명의 일 실시 예에서는 원자블록들 중 적어도 하나에 더미 연산을 추가하여 부채널 원자성을 적용할 수 있다.
- [0048] 도 4a는 $GF(2^m)$ 상에서 $ECDAD^x$ 와 $ECQPL^x$ 알고리즘의 연산순서와 연산량을 같게하는 것을 나타내고, 도 4b는 부채널 원자성이 적용된 $ECDAD^x$ 또는 $ECQPL^x$ 을 출력하는 블록을 나타낸다.
- [0049] 도 4a 및 4b는 타원곡선상의 임의의 두 점을 각각 $P_1=(x_1, y_1), P_2=(x_2, y_2)$ 라 하고, $2P=2(P_2-P_1)=(x_0, y_0)$ ($P_1 \neq -P_2$)라 가정하여 도출된 결과이다.
- [0050] 도 4a 및 도 4b를 참고로, 확장된 4진수 몽고메리 레더 알고리즘의 경우에 대한 부채널 원자성을 적용하는 방법에 대하여 설명한다. 확장된 4진수 몽고메리 레더 알고리즘의 경우에도 키의 값에 의존해서 $ECQPL^x$, $ECTA^x$ 또는 $ECDAD^x$, $ECTA^x$ 가 연산되므로 연산의 차이에 의한 단순전력분석에 의한 공격이 가능하다. 한 번의 루프에서 연산되는 $ECQPL^x$, $ECTA^x$ 또는 $ECDAD^x$, $ECTA^x$ 를 두 개의 원자블록인 γ_1 과 γ_2 로 나눈다. 여기서 γ_1 을 공통으로 연산되는 $ECTA^x$, γ_2 를 서로 다른 연산인 $ECQPL^x$ 와 $ECDAD^x$ 로 한다. γ_1 은 연산이 같으므로 추가 연산이 필요하지 않다. 반면에 γ_2 는 서로 다른 연산을 출력하기 위한 원자블록의 구성이 필요하다. 본 발명의 일 실시 예에서는 원자블록들 중 적어도 하나에 더미 연산을 추가하여 부채널 원자성을 적용할 수 있다.
- [0051] 도 5 및 도 6은 상술한 원자블록을 적용한 단순전력분석에 안전한 확장된 몽고메리 레더 방법의 알고리즘을 도시한 것이다.
- [0052] 도 5에서, d_i 값인 0,1,2를 비트정보로 각각 00, 01, 10으로 나타내고, 상위 비트를 d_i^H , 하위 비트를 d_i^L 으로 나타낸다. 도 6에서, d_i 값인 0,1,2,3을 비트정보로 각각 00, 01, 10, 11으로 나타내고, 상위 비트를 d_i^H , 하위 비트를 d_i^L 으로 나타낸다.
- [0053] 본 발명의 다른 실시 예에 따른 확장된 몽고메리 레더 방법은 연산속도를 높이기 위해서 유한체 역원연산에 몽고메리 트릭 (Montgomery trick)을 적용할 수 있다. 도 5 및 도 6은 병렬로 동작 가능하다. 즉, 병렬 동작 가능한 환경에서는 두 개의 저장공간을 이용해서 연산 속도를 높일 수 있다. 그러나 병렬동작이 불가능한 환경에서는 매 루프마다 유한체 역원이 두 번 연산되어야 한다. 따라서, 두 번의 유한체 역원연산의 효율성을 높이기 위해 몽고메리 트릭을 이용할 수 있다.

- [0054] 몽고메리 트릭은 n 개의 원소에 대한 유한체 역원을 한 번의 유한체 역원 연산과 $3(n-1)$ 번의 유한체 곱셈연산으로 구하는 방법이다. 예를 들어 a 와 b 를 $GF(2^m)$ 의 두 원소라 하면, 두 원소의 유한체 역원인 a^{-1} 와 b^{-1} 는 $a^{-1}=(a \cdot b)^{-1} \cdot b$ 와 $b^{-1}=(a \cdot b)^{-1} \cdot a$ 와 같이 계산할 수 있다. 이 때 연산량은 한 번의 유한체 역원과 세 번의 유한체 곱셈이 필요하다. 즉, 한 번의 유한체 역원을 세 번의 유한체 곱셈으로 나타낸다. 그러나, 도 1 및 도 2에 몽고메리 트릭을 사용할 경우에도 단순전력분석에 의한 키 정보 노출이 생길 수 있다.
- [0055] 본 발명의 또 다른 실시예에서는 몽고메리 트릭을 적용했을 경우에도 단순전력분석에 안전하도록 부채널 원자성을 적용할 수 있다.
- [0056] 도 7a 내지 8b는 타원곡선상의 임의의 두 점을 각각 $P_1=(x_1, y_1), P_2=(x_2, y_2)$ 라 하고, 두 점의 차를 $P=(P_2-P_1)=(x, y)$ ($P_1 \neq -P_2$)라고 가정하여 도출된 결과이다.
- [0057] 도 7a는 $GF(2^m)$ 상에서 몽고메리 트릭을 적용한 $ECDA^x$ 와 $ECTPL^x$ 또는 $ECDA^x$ 와 $ECDA^x$ 알고리즘의 연산순서와 연산량을 같게하는 것을 나타내고, 도 7b는 부채널 원자성이 적용된 몽고메리 트릭을 적용한 $ECDA^x$ 와 $ECTPL^x$ 또는 $ECDA^x$ 와 $ECDA^x$ 을 출력하는 $ECDDA^x$ 블록을 나타낸다. 여기서, $ECDDA^x$ 는 "Elliptic curve point double double-and-add"를 나타낸다.
- [0058] 도 8a는 $GF(2^m)$ 상에서 몽고메리 트릭을 적용한 $ECTA^x$ 와 $ECQPL^x$ 또는 $ECTA^x$ 와 $ECDAD^x$ 알고리즘의 연산순서와 연산량을 같게하는 것을 나타내고, 도 8b는 부채널 원자성이 적용된 몽고메리 트릭을 적용한 $ECTA^x$ 와 $ECQPL^x$ 또는 $ECTA^x$ 와 $ECDAD^x$ 을 출력하는 $ECTADAD^x$ 블록을 나타낸다. 여기서, $ECTADAD^x$ 는 "Elliptic curve point triple-and-add and double-add-double"을 나타낸다.
- [0059] 도 9 및 도 10은 몽고메리 트릭을 적용한 단순전력분석에 안전한 확장된 몽고메리 리더 알고리즘을 도시한 것이다. 도 9에는 $ECDDA^x$ 에 대한 원자블록이 사용되고, 도 10에는 $ECTADAD^x$ 에 대한 원자블록이 사용된다.
- [0060] 도 11과 도 12는 일반적으로 비밀키가 160 비트 정수라 할 때, 기존의 단순전력분석에 안전한 알고리즘들과 손익 분기점 (break even point)을 구한 것이다.
- [0061] 도 11의 결과처럼 몽고메리 트릭을 적용한 단순전력분석에 안전한 확장된 3진수 몽고메리 리더 알고리즘은 $I>6M$ 일 경우에는 기존에 제안된 방법들보다 빠른 연산속도를 가지는 것을 알 수 있다. 마찬가지로 도 12의 결과처럼 몽고메리 트릭을 적용한 단순전력분석에 안전한 확장된 4진수 몽고메리 리더 알고리즘은 $I>4M$ 일 경우에 기존의 방법들보다 연산속도가 빨라지는 것을 알 수 있다.
- [0062] 도 13은 일반적으로 비밀키가 160 비트 정수라 하고, $I/M=8$ 이라고 가정했을 때의 정확한 연산량을 비교한 것이다. 도 9의 알고리즘은 윈도우 방법과 콤팩트 방법에 비해서는 약 9%정도 연산속도가 빨라지고, 코론 방법 (Coron's method), 이즈-타카기 방법 (Izu-Takagi method)과 부채널 원자 배증 및 덧셈 (Side-channel atomic double and add)에 비해서 각각 41%, 35%, 23%의 연산속도 향상을 보였다. 도 10의 알고리즘은 윈도우 방법과 콤팩트 방법에 비해서는 약 26%의 연산속도 향상을 보였고, 코론 방법 (Coron's method), 이즈-타카기 방법 (Izu-Takagi method)과 부채널 원자 배증 및 덧셈 (Side-channel atomic double and add)에 비해서 각각 52%, 46%, 36%의 연산속도 향상을 보였다. 게다가 콤팩트 방법, 윈도우 방법의 경우는 사전테이블을 저장해야하는 단점이 있다. 비교되는 방법의 윈도우 크기는 가장 효율적이라고 할 수 있는 4로 했을 때의 연산량이다. 즉 사전테이블에 사용되는 저장공간이 8개 이상이 된다는 것을 알 수 있다. 반면에 본 발명에 따른 방법의 경우는 입력 P 와 $2P$ 의 값을 사전저장해서 사용하므로 콤팩트 방법, 윈도우 방법에 비해서 저장공간을 적게 사용한다. 즉, 저장공간을 적게 사용하면서 기존의 방법보다 빠른 연산속도를 가진다.
- [0063] 본 발명에 따른 몽고메리 리더 방법에서 비밀키 값을 3진수 또는 4진수로 표현했을 때, 두 개의 레지스터만을 사용할 수 있고, 이 경우 빠른 연산이 가능하다.
- [0064] 본 발명은 소프트웨어를 통해 실행될 수 있다. 바람직하게는, 본 발명의 일 실시 예에 따른 확장된 몽고메리 레

터를 이용한 스칼라 곱셈 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 통신망에서 반송파와 결합된 컴퓨터 데이터 신호에 의하여 전송될 수 있다.

[0065] 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.

[0066] 본 발명은 도면에 도시된 일 실시 예를 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.

산업이용 가능성

[0067] 본 발명은 타원 곡선 암호 시스템에서 스칼라 곱셈 연산을 단순전력분석에 안전하게 하면서 연산속도를 향상시킬 수 있는 방법에 관한 것으로, 저전력을 사용하는 스마트카드나 PDA 등에 적용될 수 있다.

도면의 간단한 설명

[0068] 도 1 및 2는 몽고메리 레더 방법에서의 키 값을 3진수 또는 4진수로 표현했을 때의 새로운 덧셈체인을 나타낸 것이다.

[0069] 도 3a, 3b, 4a 및 4c는 부채널 원자성을 적용한 원자블록을 도시한 것이다.

[0070] 도 5 및 도 6은 부채널 원자성을 적용한 단순전력분석에 안전한 확장된 몽고메리 레더 방법의 알고리즘을 도시한 것이다.

[0071] 도 7a 및 7b는 부채널 원자성과 몽고메리 트릭을 적용한 ECDDA^x에 대한 원자블록을 나타낸다.

[0072] 도 8a 및 8b는 부채널 원자성과 몽고메리 트릭을 적용한 ECTADAD^x에 대한 원자블록을 도시한 것이다.

[0073] 도 9 및 도 10은 몽고메리 트릭을 적용한 단순전력분석에 안전한 확장된 몽고메리 레더 알고리즘을 도시한 것이다.

[0074] 도 11과 도 12는 비밀키를 160 비트 정수라 할 때, 기존의 단순전력분석에 안전한 알고리즘들과 손익 분기점(break even point)을 나타낸 것이다.

[0075] 도 13은 일반적으로 비밀키가 160 비트 정수라 하고, I/M=8이라고 가정했을 때의 정확한 연산량을 비교한 것이다.

도면

도면1

```

1. INPUT: 상수  $d = d_{n-1}3^{n-1} + \dots + d_0 (d_{n-1} = 1, 2)$ ,
점  $P$ 
2. OUTPUT:  $dP$ 


---


3.  $Q[0] = d_{n-1}P, Q[0] = (d_{n-1} + 1)P$ 
4. for  $i \leftarrow n-2$  downto 0
5.   if  $d_i = 0$  then
6.      $Q[2] = ECTPL(Q[0]),$ 
7.      $Q[1] = ECDA(Q[0], Q[1]),$ 
8.   if  $d_i = 1$  then
9.      $Q[2] = ECDA(Q[0], Q[1]),$ 
10.     $Q[1] = ECDA(Q[1], Q[0]),$ 
11.   if  $d_i = 2$  then
12.     $Q[2] = ECDA(Q[1], Q[0]),$ 
13.     $Q[1] = ECTPL(Q[1]),$ 
14.     $Q[0] = Q[2].$ 
15. Return ( $Q[0]$ )

```

도면2

```

1. INPUT: 상수  $d = d_{n-1}4^{n-1} + \dots + d_0 (d_{n-1} = 1, 2, 3)$ ,
점  $P$ 
2. OUTPUT:  $dP$ 


---


3.  $Q[0] = d_{n-1}P, Q[0] = (d_{n-1} + 1)P$ 
4. for  $i \leftarrow n-2$  downto 0
5.   if  $d_i = 0$  then
6.      $Q[2] = ECQPL(Q[0]),$ 
7.      $Q[1] = ECTA(Q[0], Q[1]),$ 
8.   if  $d_i = 1$  then
9.      $Q[2] = ECTA(Q[0], Q[1]),$ 
10.     $Q[1] = ECDAD(Q[0], Q[1]),$ 
11.   if  $d_i = 2$  then
12.     $Q[2] = ECDAD(Q[0], Q[1]),$ 
13.     $Q[1] = ECTA(Q[1], Q[0]),$ 
14.   if  $d_i = 3$  then
15.     $Q[2] = ECTA(Q[1], Q[0]),$ 
16.     $Q[1] = ECQPL(Q[1]),$ 
17.     $Q[0] = Q[2].$ 
18. Return ( $Q[0]$ )

```

도면3a

Input : $P_1 = T_1, P_2 = T_2, P_1 - P_2 = T_3$ Output : $2P_1 + P_2$ 또는 $3P_1$	
$ECDA^x : P_1 \leftarrow 2P_1 + P_2$	$ECTPL^x : P_1 \leftarrow 3P_1$
$T_4 \leftarrow T_1 + T_2 (= x_1 + x_2)$ $T_4 \leftarrow T_4^2 (= (x_1 + x_2)^2)$ $T_5 \leftarrow T_1 \cdot T_4 (= B)$ $T_3 \leftarrow T_3 + T_1 (= x + x_1)$ $T_3 \leftarrow T_3 \cdot T_4 (= (x + x_1)(x_1 + x_2)^2)$ $T_4 \leftarrow T_1 \cdot T_2 (= x_1 x_2)$ $T_2 \leftarrow b$ (dummy) $T_3 \leftarrow T_3 + T_4 (= A)$ $T_5 \leftarrow T_5 / T_3 (= B/A)$ $T_1 \leftarrow T_1 + T_5 (= x_1 + B/A)$ $T_5 \leftarrow T_5^2 (= (B/A)^2)$ $T_1 \leftarrow T_1 + T_5 (= x_1 + B/A + (B/A)^2)$ <i>where</i> $A = (x + x_1)(x_1 + x_2)^2 + x_1 x_2$ $B = x_1(x_1 + x_2)^2$	$T_4 \leftarrow T_1 + T_2$ (dummy) $T_3 \leftarrow T_1^2 (= x_1^2)$ $T_5 \leftarrow T_1 \cdot T_3 (= B)$ $T_3 \leftarrow T_3 + T_1 (= x_1^2 + x_1)$ $T_3 \leftarrow T_3 \cdot T_1 (= x_1(x_1^2 + x_1))$ $T_4 \leftarrow T_1 \cdot T_3 (= x_1(x_1(x_1^2 + x_1)))$ $T_2 \leftarrow b$ ($= b$) $T_3 \leftarrow T_3 + T_2 (= A)$ $T_5 \leftarrow T_5 / T_3 (= B/A)$ $T_1 \leftarrow T_1 + T_5 (= x_1 + B/A)$ $T_5 \leftarrow T_5^2 (= (B/A)^2)$ $T_1 \leftarrow T_1 + T_5 (= x_1 + B/A + (B/A)^2)$ <i>where</i> $A = x_1(x_1(x_1^2 + x_1)) + b,$ $B = x_1(x_1^2)$

도면3b

Input: $Q[a] = T_1, Q[b] = T_2, P = T_3$ Output: $2Q[a] + Q[b]$ 또는 $3Q[a]$
$k = a \oplus b$ $T_4 \leftarrow T_1 + T_2$ $T_{3+k} \leftarrow T_{1+3k}^2$ $T_5 \leftarrow T_1 \cdot T_{3+k}$ $T_3 \leftarrow T_3 + T_1$ $T_3 \leftarrow T_3 \cdot T_{1+3k}$ $T_4 \leftarrow T_1 \cdot T_{3-k}$ $T_2 \leftarrow b$ $T_3 \leftarrow T_3 + T_{2+2k}$ $T_5 \leftarrow T_5 / T_3$ $T_1 \leftarrow T_1 + T_5$ $T_5 \leftarrow T_5^2$ $T_1 \leftarrow T_1 + T_5$ return T_1

도면4a

input: $P_1 = T_1, P_2 = T_2, 2(P_1 - P_2) = T_3$ output: $2P_1 + 2P_2$ or $4P_1$	
<i>ECMDDA</i> : $P_1 \leftarrow 2P_1 + 2P_2$	<i>ECMQPL</i> : $P_1 \leftarrow 4P_1$
$T_1 \leftarrow T_1^2 \quad (= x_1^2)$ $T_2 \leftarrow T_2^2 \quad (= x_2^2)$ $T_6 \leftarrow b \quad (= b)$ $T_4 \leftarrow T_1 + T_2 \quad (= (x_1^2 + x_2^2))$ $T_5 \leftarrow T_2^2 \quad (= x_2^4)$ $T_2 \leftarrow T_1 \cdot T_2 \quad (= x_1^2 x_2^2)$ $T_6 \leftarrow T_6^2 \quad (dummy)$ $T_6 \leftarrow b \quad (= b)$ $T_2 \leftarrow T_2 + T_6 \quad (= x_1^2 x_2^2 + b)$ $T_4 \leftarrow T_4 \cdot T_2 \quad (= A)$ $T_5 \leftarrow T_5 + T_6 \quad (= x_2^4 + b)$ $T_5 \leftarrow T_1 \cdot T_5 \quad (= B)$ $T_5 \leftarrow T_5 / T_4 \quad (= B/A)$ $T_2 \leftarrow T_3 + T_5 \quad (= x_0 + B/A)$ $T_6 \leftarrow T_5^2 \quad (= (B/A)^2)$ $T_1 \leftarrow T_2 + T_6 \quad (= x_0 + B/A + (B/A)^2)$ $A = (x_1^2 x_2^2 + b)(x_1^2 + x_2^2),$ $B = x_1^2(x_2^4 + b)$	$T_1 \leftarrow T_1^2 \quad (= x_1^2)$ $T_1 \leftarrow T_1^2 \quad (= x_1^4)$ $T_4 \leftarrow b \quad (= b)$ $T_2 \leftarrow T_1 + T_4 \quad (= x_1^4 + b)$ $T_5 \leftarrow T_2^2 \quad (= (x_1^4 + b)^2)$ $T_2 \leftarrow T_4 \cdot T_5 \quad (= b(x_1^4 + b)^2)$ $T_6 \leftarrow T_1^2 \quad (= x_1^8)$ $T_4 \leftarrow b \quad (= b)$ $T_2 \leftarrow T_2 + T_6 \quad (= b(x_1^4 + b)^2 + x_1^8)$ $T_4 \leftarrow T_4 \cdot T_2 \quad (= B)$ $T_2 \leftarrow T_5 + T_6 \quad (dummy)$ $T_5 \leftarrow T_1 \cdot T_5 \quad (= A)$ $T_5 \leftarrow T_4 / T_5 \quad (= B/A)$ $T_2 \leftarrow T_3 + T_5 \quad (dummy)$ $T_6 \leftarrow T_5^2 \quad (dummy)$ $T_1 \leftarrow T_1 + T_5 \quad (= x_1^4 + B/A)$ $A = x_1^4(x_1^4 + b)^2,$ $B = b(b(x_1^4 + b)^2 + x_1^8)$

도면4b

input: $Q[a] = T_1, Q[b] = T_2, P = T_3$ output: $2Q[a] + 2Q[b]$ or $4Q[a]$
$k = a \oplus b$ $T_1 \leftarrow T_1^2$ $T_{1+k} \leftarrow T_{1+k}^2$ $T_{4+2k} \leftarrow b$ $T_{2+2k} \leftarrow T_1 + T_{4-2k}$ $T_5 \leftarrow T_2^2$ $T_2 \leftarrow T_{4-3k} \cdot T_{5-3k}$ $T_6 \leftarrow T_{1+5k}^2$ $T_{4+2k} \leftarrow b$ $T_2 \leftarrow T_2 + T_6$ $T_4 \leftarrow T_4 \cdot T_2$ $T_{2+3k} \leftarrow T_5 + T_6$ $T_5 \leftarrow T_1 \cdot T_5$ $T_5 \leftarrow T_{4+k} / T_{5-k}$ $T_2 \leftarrow T_3 + T_5$ $T_6 \leftarrow T_5^2$ $T_1 \leftarrow T_{1+k} + T_{5+k}$ return T_1

도면5

1. INPUT: 상수 $d = d_{n-1}3^{n-1} + \dots + d_0$ ($d_{n-1} = 1$ 또는 2), 점 P
2. OUTPUT: dP

3. $Q[0] = d_{n-1}P$, $Q[0] = (d_{n-1} + 1)P$
4. for $i \leftarrow n-2$ downto 0
5. $Q[2] = ECDA^x(Q[d_i^H], Q[\overline{d_i^H}])$,
6. $Q[d_i^H \vee d_i^L] = atomicECDA^x(Q[d_i^H \vee d_i^L], Q[d_i^H])$,
7. $Q[\overline{d_i^H \vee d_i^L}] = Q[2]$.

도면6

1. INPUT: 상수 $d = d_{n-1}4^{n-1} + \dots + d_0$ ($d_{n-1} = 1, 2, 3$), 점 P
2. OUTPUT: dP

3. $Q[0] = d_{n-1}P$, $Q[0] = (d_{n-1} + 1)P$
4. for $i \leftarrow n-2$ downto 0
5. $Q[2] = ECTA^x(Q[d_i^H], Q[\overline{d_i^H}])$,
6. $Q[d_i^L] = atomicECDAD^x(Q[d_i^H], Q[d_i^L])$,
7. $Q[\overline{d_i^L}] = Q[2]$.
8. Return ($Q[0]$)

도면7a

input : $P_1 = T_1, P_2 = T_2, P_2 - P_1 = T_3$ output : $(3P_1, 2P_1 + P_2)$ or $(2P_1 + P_2, 2P_2 + P_1)$	
$(3P_1, 2P_1 + P_2)$	$(2P_1 + P_2, 2P_2 + P_1)$
$T_4 \leftarrow T_1^2 \quad (= x_1^2)$ $T_5 \leftarrow T_4 \cdot T_1 \quad (= x_1^3)$ $T_4 \leftarrow T_4^2 \quad (= x_1^4)$ $T_6 \leftarrow T_1 + T_2 \quad (= x_1 + x_2)$ $T_6 \leftarrow T_6^2 \quad (= (x_1 + x_2)^2)$ $T_7 \leftarrow T_1 + T_3 \quad (dummy)$ $T_3 \leftarrow T_1 + T_3 \quad (= x + x_1)$ $T_3 \leftarrow T_3 \cdot T_6 \quad (= (x + x_1)(x_1 + x_2)^2)$ $T_7 \leftarrow T_1 \cdot T_2 \quad (= x_1 x_2)$ $T_6 \leftarrow T_1 \cdot T_6 \quad (= x_1(x_1 + x_2)^2)$ $T_3 \leftarrow T_3 + T_7 \quad (= A)$ $T_7 \leftarrow T_2 \cdot T_6 \quad (dummy)$ $T_4 \leftarrow T_4 + T_5 \quad (= x_1^4 + x_1^3)$ $T_7 \leftarrow b \quad (= b)$ $T_4 \leftarrow T_4 + T_7 \quad (= B)$ $T_7 \leftarrow T_3 \cdot T_4 \quad (= AB)$ $T_7 \leftarrow T_7^{-1} \quad (= (AB)^{-1})$ $T_4 \leftarrow T_7 \cdot T_4 \quad (= A^{-1})$ $T_3 \leftarrow T_7 \cdot T_3 \quad (= B^{-1})$ $T_6 \leftarrow T_6 \cdot T_3 \quad (= x_1(x_1 + x_2)^2 A^{-1})$ $T_5 \leftarrow T_5 \cdot T_3 \quad (= x_1^3 B^{-1})$ $T_1 \leftarrow T_1 + T_5$ $T_5 \leftarrow T_5^2$ $T_1 \leftarrow T_1 + T_5 \quad (= 3P)$ $T_2 \leftarrow T_2 + T_6$ $T_6 \leftarrow T_6^2$ $T_2 \leftarrow T_2 + T_6 \quad (= 2P + Q)$ $A = (x + x_1)(x_1 + x_2)^2 + x_1 x_2,$ $B = x_1^4 + x_1^3 + b$	$T_4 \leftarrow T_1^2 \quad (dummy)$ $T_5 \leftarrow T_2 \cdot T_1 \quad (= x_1 x_2)$ $T_4 \leftarrow T_4^2 \quad (dummy)$ $T_6 \leftarrow T_1 + T_2 \quad (= x_1 + x_2)$ $T_6 \leftarrow T_6^2 \quad (= (x_1 + x_2)^2)$ $T_7 \leftarrow T_1 + T_3 \quad (= x + x_1)$ $T_3 \leftarrow T_2 + T_3 \quad (= x + x_2)$ $T_3 \leftarrow T_3 \cdot T_6 \quad (= (x + x_2)(x_1 + x_2)^2)$ $T_7 \leftarrow T_7 \cdot T_6 \quad (= (x + x_1)(x_1 + x_2)^2)$ $T_4 \leftarrow T_1 \cdot T_6 \quad (= x_1(x_1 + x_2)^2)$ $T_7 \leftarrow T_7 + T_5 \quad (= A)$ $T_6 \leftarrow T_2 \cdot T_6 \quad (= x_2(x_1 + x_2)^2)$ $T_3 \leftarrow T_3 + T_5 \quad (= B)$ $T_5 \leftarrow b \quad (dummy)$ $T_5 \leftarrow T_4 + T_6 \quad (dummy)$ $T_5 \leftarrow T_3 \cdot T_7 \quad (= AB)$ $T_5 \leftarrow T_5^{-1} \quad (= (AB)^{-1})$ $T_3 \leftarrow T_5 \cdot T_3 \quad (= A^{-1})$ $T_7 \leftarrow T_5 \cdot T_7 \quad (= B^{-1})$ $T_4 \leftarrow T_3 \cdot T_4 \quad (= x_1(x_1 + x_2)^2 A^{-1})$ $T_5 \leftarrow T_7 \cdot T_6 \quad (= x_2(x_1 + x_2)^2 B^{-1})$ $T_1 \leftarrow T_1 + T_5$ $T_5 \leftarrow T_5^2$ $T_1 \leftarrow T_1 + T_5 \quad (= 2Q + P)$ $T_2 \leftarrow T_2 + T_4$ $T_6 \leftarrow T_4^2$ $T_2 \leftarrow T_2 + T_6 \quad (= 2P + Q)$ $A = (x + x_1)(x_1 + x_2)^2 + x_1 x_2,$ $B = (x + x_2)(x_1 + x_2)^2 + x_1 x_2$

도면7b

input: $Q[a] = T_1, Q[b] = T_2, P = T_3, d_i$ output: $3Q[a], 2Q[a] + Q[b]$ or $2Q[a] + Q[b], 2Q[b] + Q[a]$
$k = d_i^L$ $T_4 \leftarrow T_1^2$ $T_5 \leftarrow T_1 \cdot T_{4-2k}$ $T_4 \leftarrow T_4^2$ $T_6 \leftarrow T_1 + T_2$ $T_6 \leftarrow T_6^2$ $T_7 \leftarrow T_1 + T_3$ $T_3 \leftarrow T_3 + T_{1+k}$ $T_3 \leftarrow T_3 \cdot T_6$ $T_7 \leftarrow T_{1+6k} \cdot T_{2+4k}$ $T_{6-2k} \leftarrow T_1 \cdot T_6$ $T_{3+4k} \leftarrow T_7 + T_{3+2k}$ $T_{7-k} \leftarrow T_2 \cdot T_6$ $T_{4-k} \leftarrow T_5 + T_{4-k}$ $T_{7-2k} \leftarrow b$ $T_{4+k} \leftarrow T_4 + T_{7-k}$ $T_{7-2k} \leftarrow T_3 \cdot T_{4+3k}$ $T_{7-2k} \leftarrow T_{7-2k}^{-1}$ $T_{4-k} \leftarrow T_{7-2k} \cdot T_{4-k}$ $T_{3+4k} \leftarrow T_7 \cdot T_{3+2k}$ $T_5 \leftarrow T_{5+2k} \cdot T_{3+3k}$ $T_{6-2k} \leftarrow T_{6-2k} \cdot T_3$ $T_1 \leftarrow T_1 + T_5$ $T_5 \leftarrow T_5^2$ $T_5 \leftarrow T_1 + T_5$ $T_2 \leftarrow T_2 + T_{6-2k}$ $T_6 \leftarrow T_{6-2k}^2$ $T_6 \leftarrow T_2 + T_6$ $T_1 \leftarrow T_5 + (d_i^H \vee d_i^L)$ $T_2 \leftarrow T_{6-2k} - (d_i^H \vee d_i^L)$ return (T_1, T_2)

도면9

1. INPUT: 상수 $d = d_{n-1}3^{n-1} + \dots + d_0 (d_{n-1} = 1, 2)$, 점 P
2. OUTPUT: dP

3. $Q[0] = d_{n-1}P, Q[1] = (d_{n-1} + 1)P$
4. for $i \leftarrow n-2$ downto 0
5. $(Q[0], Q[1]) = atomicECDDA^x(Q[d_i^H], Q[\overline{d_i^H}])$
6. Return ($Q[0]$)

도면10

1. INPUT: 상수 $d = d_{n-1}4^{n-1} + \dots + d_0 (d_{n-1} = 1, 2, 3)$, 점 P
2. OUTPUT: dP

3. $Q[0] = d_{n-1}P, Q[1] = (d_{n-1} + 1)P$
4. for $i \leftarrow n-2$ downto 0
5. $(Q[0], Q[1]) = atomicECTADAD^x(Q[d_i^H], Q[\overline{d_i^H}])$
6. Return ($Q[0]$)