情報保護學會論文誌
第13券 第5號, 2003. 10

전력분석공격을 효율적으로 방어하는 타원곡선 비밀키의 랜덤화*

장 상 운**, 정 석 원**, 박 영 호***

Randomization of Elliptic Curve Secret Key to Efficiently Resist Power Analysis

Sang-Woon Jang**, Seok Won Jung**, Young-Ho Park***

요 약

본 논문에서는 DPA[2]와 Goubin의 공격[3]을 동시에 방어하도록 하는 타원곡선 스칼라 곱셈 알고리듬의 일반적인 조건을 제시하며, 제시된 조건을 만족하면 두 공격 모두를 방지할 수 있음을 보인다. 이러한 조건을 만족하는 것으로는 Ha-Moon의 재부호화 방법[5]을 이용한 랜덤 스칼라 곱셈 알고리듬이 있음을 보이고, 또한 Ha-Moon의 재부호 방법을 변형하여 두 공격을 방지하는 새로운 재부호화 알고리듬을 제안한다. 효율성 면에서 제안하는 스칼라 곱셈 방식은 Izu-Takagi의 스칼라 곱셈방법(y-좌표를 계산하지 않고 Montgomery-ladder를 사용)[6]과 비교될 만큼 효율적이다. 제안하는 스칼라 곱셈은 랜덤화된 사영좌표와 기저점 은닉(bsae point blinding) 또는 isogeny 함수를 결합한 방법보다 빠르다. 또한 Izu-Takagi의 경우 은닉 또는 isogeny 함수 방법을 이용하면 상당량의 시스템 파라미터를 EEPROM에 저장해야 하는 단점이 있지만 이것은 제안하는 스칼라 곱셈 방법에는 해당되지 않는다.

ABSTRACT

We establish the security requirements and derive a generic condition of elliptic curve scalar multiplication to resist against DPA[2] and Goubin's attack.[3] Also we show that if a scalar multiplication algorithm satisfies our generic condition, then both attacks are infeasible. Showing that the randomized signed scalar multiplication using Ha-Moon's recoding algorithm[5] satisfies the generic condition, we recommend the randomized signed scalar multiplication using Ha-Moon's recoding algorithm to be protective against both attacks. Also we newly design a random recoding method to prevent two attacks. Finally, in efficiency comparison, it is shown that the recommended method is a bit faster than Izu-Takagi's method[6] which uses Montgomery-ladder without computing y-coordinate combined with randomized projective coordinates and base point blinding or isogeny method. Moreover, Izu-Takagi's method uses additional storage, but it is not the case of ours.

keyword : *타원곡선, SPA, DPA, 랜덤 스칼라 곱셈*

Ⅰ. 서 론

암호시스템의 이론적 안전성과 별도로, 전력 소모량과 알고리즘의 수행시간과 같은 부가 정보는 스마트 카드, 모바일 폰, PAD 등의 내장된 하드웨어에서 암호 알고리즘의 구현에 대한 실질적인 위협이 되고

* 본연구는 한국전자통신연구원 위탁연구과제(0701-2003-0020) 지원으로 수행하였습니다.
** 고려대학교 정보보호 대학원({jangsw, jsw}@cist.korea.ac.kr)
*** 세종 사이버 대학교 컴퓨터 공학부(youngho@cybersejong.ac.kr)

있다. 1996년 Kocher가 암호 프리미티브에 대한 시간공격(timing attack)을 도입하고 1999년에 DPA(differential power analysis, 차분전력분석) 소개한 이후, 부가채널공격(side channel attack)에 안전하고 효율적인 타원곡선 스칼라 곱셈을 고안하는 것은 ECC(elliptic curve crytosystem) 구현 연구의 주요 주제 중 하나가 되었다.

1.1 타원곡선 스칼라 곱셈과 전력분석 공격

타원곡선 $E(F_q)$와 두 점 P_1, $P_2 \in E(F_q)$에 대하여, $P_1 \neq P_2$인 경우 P_1과 P_2의 타원곡선 덧셈을 $ECADD(P_1, P_2)$으로 나타내자. $P_1 = P_2$인 경우, 즉 P_1의 2배 연산을 $ECDBL(P_1)$으로 표기한다. 타원곡선 위의 점 P와 정수 k에 대하여, 타원곡선 스칼라 곱셈은 다음과 같이 정의된다.

$$k \cdot P = P + \cdots + P \ (k\text{-times})$$

비밀키 $k = \sum_{i=0}^{n-1} k_i 2^i$ ($k_i \in \{0,1\}$)에 대하여, 타원곡선 스칼라 곱셈은 $ECADD$와 $ECDBL$연산을 반복적으로 수행한다. 알고리듬 1, 2는 일반적인 이진 스칼라 곱셈 알고리즘을 나타내며, 알고리듬 1은 최상위부터 비트(Most significant bit(MSB) first)를 스캔하며, 알고리듬 2는 최하위부터 비트(Least significant bit (LSB) first)를 스캔한다.

알고리듬 1, 2는 비밀키 k_i에 의존하여 $ECADD$이 선택적으로 수행되도록 하는 조건 분기문이 포함되어 있다. 따라서 스칼라 곱셈의 전력 소모량이 $k_i = 1$인지 아닌지에 의존하여 다르게 나타나므로 SPA(simple power analysis, 단순전력분석)에 취약하다. Coron이 제시한 알고리듬 3에서 비밀키에 대한 스칼라 곱셈의 실행 의존성이 제거되었으며,[2] 알고리듬 4는 알고리듬 3의 LSB 버전이다. 알고리듬 3, 4는 비밀키에 상관없이 항상 $ECADD$을 실행하며, 따라서 알고리듬 1, 2에 비하여 상당량의 추가 연산을 필요로 한다.

알고리듬 3, 4는 SPA에는 강하지만, Coron은 DPA을 이용하여 알고리듬 3을 분석하였다. 일반적으로 DPA는 비밀키에 의존하여 발생하는 특정 값과 전력 소모량과의 상관관계를 이용한 공격이다. 공격자는 사전에 알려진 값으로부터 특정 값을 예측한 후, 특정 값의 출현 여부로부터 비밀키를 비트별로 찾아낸다. 따라서 스칼라 곱셈이 DPA에 강하기 위해서는 계산되는 값을 랜덤화 시켜서 고정된 값의 출현을 막아야 한다.

Algorithm 1 **: MSB-first binary**	**Algorithm 2** **: LSB-first binary**
Input k(binary secret key), P(basepoint), $n(=\|k\|)$ **Output** $k \cdot P$	

$Q[0] \leftarrow P$
for $i = n-2$ down to 0
  $Q[0] \leftarrow ECDBL(Q[0])$
  if(k_i == 1)
  $Q[0] \leftarrow ECADD(Q[0], P)$
return($Q[0]$)
	$Q[0] \leftarrow P$, $Q[1] \leftarrow O$
	for $i = 0$ up to $n-1$
	  if (k_i == 1)
	  $Q[1] \leftarrow ECADD(Q[0], Q[1])$
	  $Q[0] \leftarrow ECDBL(Q[0])$
	return($Q[1]$)

Algorithm 3[2] **: SPA-Resistant MSB-first binary**	**Algorithm 4** **: SPA-Resistant LSB-first binary**
Input k(binary secret key), P(basepoint), $n(=\|k\|)$ **Output** $d \cdot P$	

$Q[0] \leftarrow P$
for $i = n-2$ down to 0
  $Q[0] \leftarrow ECDBL(Q[0])$
  $Q[1] \leftarrow ECADD(Q[0], P)$
  $Q[0] \leftarrow Q[k_i]$
return($Q[0]$)
	$Q[0] \leftarrow P$, $Q[1] \leftarrow O$
	for $i = 0$ up to $n-1$
	  $Q[2] \leftarrow ECADD(Q[0], Q[1])$
	  $Q[0] \leftarrow ECDBL(Q[0])$
	  $Q[1] \leftarrow Q[k_i + 1]$
	return($Q[1]$)

Remark 1. 알고리듬 4에서 $(\pm P) + O$ 과정은 반드시 실제 덧셈의 절차를 통해 처리되어야 한다. 이 과정이 단순한 데이터 할당에 의하여 처리된다면 알고리즘에 대한 전력 파형을 분석하여 비밀키의 최초 1-비트가 출현하기 전 연속된 최하위 0-비트가 노출될 수 있다.

1.2 논문의 동기

1996년 Coron[2]은 타원곡선에 대하여 DPA를 처음으로 일반화하였으며, Coron의 DPA를 **C-DPA**라고 부르자. 동시에 그는 세 가지 DPA 대응방법을 제시하였다. 즉, (1) 비밀키의 랜덤화, (2) 기저점 은닉, (3) 랜덤화된 사영좌표계 (randomized projective coordinates)을 말한다. 2000년 Okeya와 Sakurai[11]는 Coron의 첫 번째와 두 번째 DPA 대응방법의 취약점을 지적하였다. Joye와 Tymen[8]이 랜덤한 타원곡선 동형사상(random elliptic curve isomorphisms)과 랜덤한 유한체 동형사상(random fields isomorphisms)의 두 가지 DPA 대응책을 제시한 이후, Goubin[3]은 2003년 남아있는 세 가지 DPA 대응방법(두 가지 랜덤한 동형사상과 랜덤한 사영좌표)에 대한 공격을 제시하였다. Goubin의 공격을 **G-DPA**으로, C-DPA와 G-DPA의 결합을 **CG-**

DPA라고 명하자. Goubin은 G-DPA에 대한 대응책으로서 단순히 기저점 은닉기법을 제시하였다. [14]에서 Smart는 G-DPA에 대한 방어책을 제안하였으나, 위수가 큰 특수점 (special point)의 경우 상당량의 메모리를 사용한다는 단점이 있다. C-DPA 대응방법과 Goubin 또는 Smart의 대응방법의 결합을 **기존의 CG-DPA 대응법**이라고 부른다.

남아있는 세 가지 DPA 대응방법에 비해서 기존의 CG-DPA 대응법은 더 많은 계산과 저장공간을 필요로 하며, 이것은 스마트카드와 같은 제한된 환경에서 분명히 단점이 된다. 본 논문은 다음의 동기로부터 출발한다.

- 첫째, 기존의 CG-DPA 대응법을 사용하지 않고 CG-DPA를 어떻게 대응할 수 있는가 ?
- 둘째, CG-DPA을 방어하는 스칼라 곱셈의 일반적인 조건은 무엇인가 ?

1.3 논문의 기여

본 논문의 기여와 결과는 다음과 같다.

- CG-DPA에 대응하는 타원곡선 스칼라 곱셈의 안전성 요구사항을 확립한다. 안전성 요구사항으로부터 CG-DPA의 공격특성을 제거하기 위한 타원곡선 스칼라 곱셈의 조건을 이끌어 내며, 알고리듬이 유도된 일반적인 조건을 만족하면 CG-DPA에 안전함을 증명한다.
- Ha-Moon의 재부호화 알고리듬[5]을 이용한 랜덤화된 스칼라 곱셈은 일반적인 조건을 만족함을 보인다. 또한 Ha-Moon의 재부호화 알고리듬의 변형으로 다른 재부호화 알고리듬을 제안하여 제안방법 또한 CG-DPA를 방어함을 보인다. 이를 기초로 두 가지 재부호화 알고리듬을 이용한 랜덤화된 스칼라 곱셈을 CG-DPA에 안전한 알고리듬으로 추천한다.
- 효율성 면에서 제안한 스칼라 곱셈은 Izu와 Takagi의 스칼라 곱셈방법(y-좌표를 계산하지 않고 Montgomery-ladder를 사용)[6]과 비교된다. 제안하는 스칼라 곱셈은 Izu-Takagi 방식 중에서 사영좌표와 기저점 은닉기법을 결합한 방법보다 빠르다. 또한 메모리 사용면에서 제안하는 스칼라 곱셈방식이 Izu-Takagi 방식보다 효율적이다.

II. 기존의 DPA 대응방법과 분석방법

이진 스칼라 $d=\sum_{j=0}^{n-1} d_j 2^j$에 대하여, 최상위 $(n-i)$ 비트를 $d^{(i)}=\sum_{j=i}^{n-1} d_j 2^{j-i}$ $(i=0,\cdots,n-1)$라고 표기하자.

2.1 일반적인 DPA (C-DPA)[2]

알고리듬 3에 대한 C-DPA의 절차에 대해 간략히 살펴보자. 공격자가 최상위 t 비트, 즉 $d^{(n-t)}$ 을 안다고 가정하자. 그러면 반복문의 t 번째 단계의 마지막에서, $Q[0]=d^{(n-(t+1))}\cdot P$ 이 얻어지면, 다음의 두 가지 경우중 하나가 발생한다.

- $d_{n-(t+1)}=0$이면, $(t+1)$-번째 단계에서 나타나는 값은 다음과 같다.

$$(2\cdot d^{(n-t)})\cdot P\ ,\quad (2\cdot d^{(n-t)}+1)\cdot P \tag{1}$$

- $d_{n-(t+1)}=1$이면, $(t+1)$-번째 단계에서 나타나는 값은 다음과 같다.

$$(2\cdot d^{(n-t)}+2)\cdot P,\quad (2\cdot d^{(n-t)}+3)\cdot P \tag{2}$$

$d_{n-(t+1)}=0$이면, $(2\cdot d^{(n-t)})\cdot P$이 알고리듬 3에서 계산이 되며, 전력 소모량은 $(2\cdot d^{(n-t)})\cdot P$의 임의의 특정 비트와 상관관계를 이루게 된다. $d_{n-(t+1)}=1$ 이면 $(2\cdot d^{(n-t)})\cdot P$은 계산되지 않으며 따라서 어떤 상관관계도 일어나지 않는다.

특정 비트와 전력 소모량사이의 상관관계를 명확히 관찰하기 위해서 통계적인 방법이 필요하다. 알고리듬 3을 k개의 서로 다른 점 $P_1,\cdots,P_k$에 대해 적용하여 $Q_1=dP_1$,$\cdots$, $Q_k=dP_k$를 계산한다. $1\le i\le k$에 대하여 $C_i(t)$은 시각 t에서 알고리듬의 i번째 실행에 해당하는 전력 소모량이라고 하자. s_i는 $(2\cdot d^{(n-t)})\cdot P_i$ $(1\le i\le k)$을 이진 표현했을 때 나타나는 특정 비트라고 하자. s_i와 $C_i(t)$사이의 상관관계 함수 $g(t)$는 다음과 같이 계산된다.

$$g(t)=\langle C_i(t)\rangle_{i=1,\cdots,k|s_i=1}-\langle C_i(t)\rangle_{i=1,\cdots,k|s_i=0}$$

시각 $t=t_1$에서 점 $(2\cdot d^{(n-t)})\cdot P_i$이 실행된다고 가정하면, 전력 소모량 $C_i(t_1)$은 $(2\cdot d^{(n-t)})\cdot P_i$의 이진표현에 의한 특정 비트 s_i와 상관관계가 발생할 것이다. 따라서 $s_i=1$ 일때 $(2\cdot d^{(n-t)})\cdot P_i$에 해당하는 전력 소모량은 $s_i=0$일 때의 전력 소모량과 차이가 생길 것이며, 시각 $t=t_1$에서 상관관계함수 $g(t)$

는 첨점을 보일 것이다. 만약 $(2 \cdot d^{(n-t)}) \cdot P_i$이 계산되지 않는다면, 함수 $g(t)$에서 첨점이 생기지 않게 된다.

2.2 기존의 DPA 대응방법

Coron의 대응방법[2]. Coron은 타원곡선 암호시스템에 DPA를 확장하였으며 C-DPA에 대한 대응책으로서 다음의 세 가지 방법을 제시하였다 : (1)비밀키의 랜덤화 방법, (2)기저점 은닉 방법, (3)랜덤화된 사영좌표계 방법.

Oswald의 대응방법[13]. Coron은 이진 스칼라 알고리듬에 입력이 되는 파라미터를 랜덤화하거나 은닉시키는 DPA 대응책을 고안한 반면, Oswald는 이진 스칼라 알고리듬 자체를 랜덤화 하는 DPA 대응방법을 제시하였다. 두 개의 랜덤화된 오토마타는 Morain과 Olivos[10]가 제안한 랜덤한 덧셈-뺄셈 연쇄(addition-subtraction chains)에 기인하다.

Joye-Tymen의 대응방법[8]. Joye와 Tymen은 기저점을 랜덤화하기 위한 두 가지 대수적인 방법을 제안하였다. 즉, (1) 랜덤한 타원곡선 동형사상과 (2) 랜덤한 유한체 동형사상이 그것인데, 그들의 아이디어는 랜덤한 동형사상을 통해서 스칼라 곱셈 계산을 다른 유한체나 타원곡선 상에서 이루어지도록 하는 것이다.

2.3 기존의 DPA 대응방법에 대한 분석

본 소절에서는 기존의 DPA 대응방법에 대한 공격 특성을 분석하고, DPA에 의해서 스칼라 곱셈 알고리즘이 분석되지 않기 위한 안전성 요구사항을 특성화한다.

Okeya-Sakurai의 공격[11]. Okeya와 Sakurai는 Coron의 첫 번째와 두 번째 대응방법을 분석하였다. Okaya와 Sakurai는 첫 번째 대응방법의 경우 SPA 대응법이 부주의 할 경우, 스칼라 곱셈의 실행되는 절차가 비밀키에 의존한다고 주장하였다. 두 번째, $d \cdot P$를 계산하는 데에 덧셈 $R+P$와 뺄셈 $d(P+R)-S$을 추가적으로 계산하는 이른바 기저점 P의 은닉기법이다. 여기서 R은 타원곡선상의 랜덤한 점이며 $S=d \cdot R$이다. 사전에 저장된 두 점 R, S와 난수 b에 대하여, R과 S는 각각 $R \leftarrow (-1)^b 2R$, $S \leftarrow (-1)^b 2S$와 같이 갱신된다. Okeya, Sakurai는 Coron의 은닉기법에서 두 점을 갱신하는 방법이 R, S를 제대로 랜덤화하지 못한다고 지적하였다.

Okeya-Sakurai의 공격[11]과 Han의 공격[4]. Okeya-Sakurai와 Han은 각각 Oswald의 랜덤화된 오토마타 1, 2를 분석하였다. 그들은 공통적으로 랜덤화된 오토마타 1, 2의 수행 중에 나타나는 덧셈 A와 2배 연산 D로 이루어진 AD-열 중 특정한 연산패턴 $DAAD$를 주요하게 이용하였다. 랜덤화된 오토마타 1, 2는 SPA와 DPA를 모두 방어하기 위한 대응책이었으나 결국 SPA를 이용한 분석으로 공격되었다.

Goubin의 공격 (G-DPA)[3]. G-DPA는 스칼라 곱셈에서 덧셈과 2배 연산을 항상 계산하는 방법이나 Mogomery-ladder와 같은 SPA 대응책이 사용하는 환경하에서, 랜덤 사영좌표나 랜덤 동형사상을 이용한 DPA 대응방법을 분석하였다. G-DPA는 타원곡선 $E(K)$가 특수점 $P_0 \neq O$(아핀 좌표나 사영좌표에서 하나의 성분이 0인 점)을 포함한다는 특성을 이용하였는데, 세 가지 DPA 대응방법이 이용되더라도 P_0의 특성을 제거하지 못한다는 것이 공격의 핵심이다.

알고리듬 3에 대하여 G-DPA를 적용하여 보자. C-DPA의 경우와 같이 비밀키에 대한 똑같은 가정과 수식(1), (2)하에서, 공격자는 점 P_1를 다음과 같이 선택한다.

- $d_{n-(t+1)}=0$으로 추측한 경우,

$$P_1 = [\ (2 \cdot d^{(n-t)}+1)^{-1} \bmod \#E(K)\ ] \cdot P_0\ ,$$

- $d_{n-(t+1)}=1$으로 추측한 경우,

$$P_1 = [\ (2 \cdot d^{(n-t)}+3)^{-1} \bmod \#E(K)\ ] \cdot P_0 \quad (4)$$

알고리듬 3이 $Q_1 = d \cdot P_1$을 계산하기 위해서 디바이스에 같은 점 P_1을 k번 입력한다고 가정하자. 전력 소모량에 대한 평균 곡선을 다음과 같이 정의한다.

$$M_{P_1}(t) = \frac{1}{k} \sum_{i=1}^{k} C_i(t) \quad (5)$$

$d_{n-(t+1)}$을 옳게 추측하면, 평균 곡선 $M_{P_1}(t_1)$은 첨점을 보일 것이다. 여기서 t_1은 루프의 $(t+1)$-번째 단계에서 특수한 점 P_0의 0 성분이 다루어질 때의 시각을 말한다. 반대로 $d_{n-(t+1)}$의 추측이 틀리면, $(t+1)$-번째 단계에서 나타나는 값이 랜덤화 되기 때문에 평균 곡선 $M_{P_1}(t_1)$은 첨점을 보이지 않을 것이다.

Remark 2. G-DPA는 기저점이 고정되는 ECDSA나 ECDH에서는 적용되지 않는다. G-DPA는 선택 평문 공격이다.

■ G-DPA에 대한 대응방법

1) Goubin은 G-DPA 에 대응하기 위해서 기저점 은닉 기법을 제안하였다. 이 방법은 두 번의 덧셈과 두 번의 2배 연산을 필요로 하므로 Jacobian 좌표계를 사용하면 48번의 유한체 곱셈이 소요된다[14].
2) [14] 에서 Smart는' 타원곡선 isogeny 함수를 이용한 G-DPA에 대한 대응방법을 제안하였다. 그의 대응방법은 특수점의 위수에 따라 두가지로 구분되는데, 특히 위수가 큰 경우에는 기저점 P를 isogeny 함수를 이용하여 특수점이 없는 타원곡선으로 변환하는 것이 그의 아이디어이다. ℓ을 isogeny 함수의 차수(degree)라고 할 때, isogeny 함수에 의한 변환과 역변환은 3ℓ번의 유한체 곱셈을 필요로 한다. Smart에 의해 지적되었듯이 isogeny 함수를 이용한 대응방법의 단점은 많은 양의 시스템 파라미터를 스마트 카드가 저장해야 한다는 것이다. 구체적으로 isogeny 함수를 정의하는 다항식의 계수를 저장하는 데에 $3\ell n$ 비트, isogeny 타원곡선을 저장하는 데에 $2n$ 비트정도의 메모리가 필요하다[14]. 이것은 저장공간이 제한된 환경에서 간과될 수 없는 문제점으로 남게 된다.

■ 안전성 요구사항

전력 소모량에 의한 공격에 대하여 스칼라 곱셈 알고리듬이 안전하기 위한 요구사항을 다음과 같이 요약할 수 있다.

1) 알고리듬의 수행되는 절차가 비밀키에 의존하지 않도록 한다.
2) 계산되는 객체를 랜덤화 한다.
3) 스칼라 곱셈 중간 단계에서 발생하는 특수점의 성질을 제거한다.

첫 번째 요구사항은 기본적으로 SPA를 방지하기 위한 것이며, 두 번째와 세 번째는 CG-DPA를 방어하기 위한 요구사항이다.

Ⅲ. CG-DPA를 어떻게 방어할 것인가?

본 절에서는 CG-DPA를 방어하기 위한 타원곡선 스칼라 곱셈의 조건을 제시한다. 다음의 정리 1은 스칼라 곱셈 알고리즘이 CG-DPA에 의한 분석 가능성 여부의 기준이 된다.

정리 1. MSB-first 스칼라 곱셈에 대하여, 공격자가 비밀키 d의 최상위 부분비트 $d^{(n-t)}$을 알고 있다는 가정 하에, 다음 비트 $d_{n-(t+1)}$을 추측하고자 한다. 루프의 t번째 단계에서 나타나는 중간 결과 값이 결정론적인 공식[1]을 갖지 않으면, 스칼라 곱셈이 CG-DPA에 대하여 안전하다.

(증명)

C-DPA case. 루프의 t번째 단계에서 나타나는 중간 값이 결정론적이지 않으면, $d_{n-(t+1)}$의 추측에 의존하는 중간 계산 값은 알고리즘 상에서 항상 계산되지 않는다. 따라서 중간 값의 어떤 특정 비트 s_i도 전력 소모량과 상관관계가 발생하지 않는다. 이것은 $d_{n-(t+1)}$의 모든 추측에 대하여 상관관계 함수 $g(t)$가 첨점이 발생하지 않음을 의미한다.

G-DPA case. $d_{n-(t+1)}$의 추측에 의존하여, 수식(4)의 P_1이 선택된다. $d \cdot P_1$의 계산에서 루프의 t번째 단계가 끝난 후의 값은 반드시 특수한 점 P_0이 아니다. 따라서 특수한 점의 0 성분에 대한 전력 소모량이 항상 발생되지 않기 때문에 평균 곡선 $M_{P_1}(t_1)$은 $d_{n-(t+1)}$의 추측에 무관하게 첨점이 발생하지 않게 된다.

Remark 3. 정리 1은 LSB-first 스칼라 곱셈 알고리즘에도 마찬가지로 적용되며, 덧셈과 2배 연산을 항상 계산하는 방법에 제한되지 않는다.

Remark 4. 기존의 CG-DPA 대응법은 다음과 같다.

1) 랜덤화된 사영 좌표계 + 기저점 은닉.
2) 랜덤한 타원곡선 동형사상 + 기저점 은닉.
3) 랜덤화된 사영 좌표계 + isogeny 함수.
4) 랜덤한 타원곡선 동형사상 + isogeny 함수.

Ⅳ. ±1 부호가 있는 랜덤화된 스칼라 곱셈 알고리듬

본 절에서는 Ha-Moon의 재부호화 방법[5]과 본 논

1) 예를 들어 G-DPA에서, '서로 다른 결정론적인 공식'이라 함은 두 중간 값이 논리적으로 서로 다름을 의미한다. 즉, $d(1)^{(n-(t+1))} \cdot P \neq d(2)^{(n-(t+1))} \cdot P$이다. 여기서 $d(1)$, $d(2)$는 비밀키 d에 대한 서로 다른 표현이다.

문에서 제안하는 또 다른 재부호화 방법을 소개한다. 두 재부호화 방법은 이진 스칼라 $k=\sum_{i=0}^{n-1} k_i 2^i$를 새로운 ±1 이진 스칼라 $d=\sum_{i=0}^{n-1} d_i 2^i$으로 변환한다. 여기서 $k_i \in \{0,1\}$, $d_i \in \{-1,0,1\}$, $k \cdot P = d \cdot P$이다. 두 재부호화 방법은 정리 1의 조건을 만족하며, 따라서 이들을 이용한 랜덤 스칼라 곱셈 알고리즘은 CG-DPA에 안전한 알고리즘이다.

4.1 Ha-Moon의 재부호화 방법[5]

초기값이 $c_0=0$인 $(i+1)$-번째 보조 캐리 c_{i+1}를 이용하여, 비트열 $c_{i+1}d_i$은 $c_{i+1}2^1+d_i2^0$의 값을 갖는다. 따라서 두 값 $c_{i+1}d_i=01$, $c_{i+1}d_i=1\bar{1}$은 표현상 다르지만 논리적으로 같은 값을 갖는다. 재부호화 알고리듬은 랜덤 비트 r_i를 생성하여 위의 두 표현이 랜덤하게 선택된다. 즉, AF(Adjacent Form)와 NAF (Non Adjacent form) 표현 방식이 랜덤하게 채택된다. 이것이 랜덤 재부호화 알고리듬의 핵심 아이디어이다. 그들의 분석결과에 의하면, 재부호화 알고리듬에 의해 생성된 ±1 이진 스칼라는 평균적으로 ±1 이진 스칼라 길이의 절반이 된다.

Ha-Moon 재부호화 방법에 의한 랜덤 스칼라 곱셈 알고리듬이 정리 1의 조건에 대한 만족 여부는 다음과 같이 쉽게 확인할 수 있다.

■ 안전성 확인

1) SPA에 대한 안전성
   2절에서 언급한 안전성 요구사항으로부터, 알고리듬 5를 적용하거나 Jacobi[9] 또는 Hessian[7] 형태 타원곡선에서 덧셈과 2배 연산의 통합된 공식을 적용하면 SPA를 방어할 수 있다.
2) CG-DPA에 대한 안전성
   k와 d는 각각 이진 비밀키와 ±1 이진 스칼라라고 할 때, 공격자는 비밀키 k의 최상위 부분비트 $k^{(n-t)}$을 알고 있으며, 다음 비트 $k_{n-(t+1)}$을 추측하고자 한다. 루프의 t번째 단계에서 나타나는 중간 계산 값은 $Q[0]=d^{(n-(t+1))} \cdot P$이다. 스칼라 곱셈이 실행될 때마다, ±1 이진 스칼라는 랜덤화 된다. 따라서 d의 랜덤화에 의해서 $d^{(n-(t+1))} \cdot P$ 또한 랜덤화 되므로 중간 계산 값 $Q[0]$에 대한 결정론적인 공식을 이끌어 내는 것이 매우 어렵다.

따라서 Ha-Moon 재부호화 방법에 의한 랜덤 스칼라 곱셈은 G-DPA를 막기 위해서 은닉기법과 같은 추가적인 대응책을 요구하지 않는다.

4.2 제안하는 재부호화 방법

정수의 ±1 이진 스칼라 표현이 유일하지 않다는 특성에 기초하여, 다음의 불변관계식을 이용한 랜덤한 재부호화 방법 (right-to-left)을 제안한다.

$$c_{i+1} \cdot 2 + (c_i + k_i) = c_{i+2} \cdot 2^2 + c'_{i+1} \cdot 2 + d_i \quad (6)$$

■ 제안하는 재부호화 방법의 설명

1) 입력 변수
- $k_i \in \{0,1\}$, $i=0,1,\cdots,n-1$: 이진스칼라 비트.
- $c_{i+1}, c_i \in \{\bar{1},0,1\}$, $c_0=c_1=0$: 입력 캐리 비트. 초기 두 개의 보조 캐리 c_0, c_1 은 0으로 설정되며 이후 비트는 재부호화 알고리즘에 의해 생성된다.
- $u_i, r_i \in \{0,1\}$, $i=0,1,\cdots,n$: 두 개의 독립적인 랜덤 비트.
- S_i : i 번째 상태. 5개의 성분 $(k_i, c_{i+1}, c_i, u_i, r_i)$은 하나의 상태를 결정한다.

〔표 1〕 새로운 랜덤 재부호화 알고리듬

상태	입 력					출 력		
s_i	k_i	c_{i+1}	c_i	u_i	r_i	c_{i+2}	c'_{i+1}	d_i
0	0	0	0	0	-	0	0	0
1	0	0	0	1	0	0	0	0
2	0	0	0	1	1	0	0	0
3	0	0	1	0	-	0	0	1
4	0	0	1	1	0	0	1	$\bar{1}$
5	0	0	1	1	1	1	$\bar{1}$	$\bar{1}$
6	0	1	$\bar{1}$	0	-	0	0	1
7	0	1	$\bar{1}$	1	0	0	1	$\bar{1}$
8	0	1	$\bar{1}$	1	1	1	$\bar{1}$	$\bar{1}$
9	1	0	0	0	-	0	0	1
10	1	0	0	1	0	0	1	$\bar{1}$
11	1	0	0	1	1	1	$\bar{1}$	$\bar{1}$
12	1	0	1	0	-	0	1	0
13	1	0	1	1	0	1	$\bar{1}$	0
14	1	0	1	1	1	1	$\bar{1}$	0
15	1	1	$\bar{1}$	0	-	0	1	0
16	1	1	$\bar{1}$	1	0	1	$\bar{1}$	0
17	1	1	$\bar{1}$	1	1	1	$\bar{1}$	0

2) 출력 변수

· $c_{i+2}, c'_{i+1} \in \{\bar{1}, 0, 1\}$: 출력 캐리 비트.
입력 캐리 비트 c_{i+1}은 출력 캐리 비트 c'_{i+1}으로 갱신된다.

· $d_i \in \{\bar{1}, 0, 1\}$, $i = 0, \cdots, n$: ±1 이진스칼라 비트

출력 비트열 $c_{i+2}c'_{i+1}d_i$은 두 가지 방식으로 랜덤화 된다. 첫째, 랜덤 비트열 $u_i r_i$ =0-[2], 10, 11에 따라서 각각 다른 출력 비트열 $c_{i+2}c'_{i+1}d_i$ = 001, 01$\bar{1}$, 1$\bar{1}\bar{1}$이 생성되며 이들의 논리적인 값은 모두 1로서 같다. 둘째, $u_i r_i$ =0-, 1- 에 따라서 각각 $c_{i+2}c'_{i+1}d_i$ = 010 또는 1$\bar{1}$0으로 랜덤하게 생성된다. 재부호화 된 스칼라는 본래의 이진 스칼라보다 많아야 한 비트 더 길 수도 있으며 이것은 Ha-Moon의 결과와 같다.

예제 1. $k = (1001101101)_2 = 2^9 + 2^6 + 2^5 + 2^3 + 2^2 + 1 = 621$ 에 대하여 두 개의 서로 다른 난수를 사용하였을 경우 d의 출력을 계산해 본다.

case 1. $u = (0001110101)_2$, $r = (1010110001)_2$

$d = (10100\bar{1}0\bar{1}1\bar{1})_{SD2} = 2^9 + 2^7 - 2^4 - 2^2 + 2^1 - 1 = 621$

case 2. $u = (1010111100)_2$, $r = (1111000001)_2$

$d = (11\bar{1}00\bar{1}0\bar{1}01)_{SD2} = 2^9 + 2^8 - 2^7 - 2^4 - 2^2 + 1 = 621$

알고리듬 5는 n비트 ±1 이진 스칼라를 입력으로 하며 SPA를 방어한다. CG-DPA를 방어하기 위하여 이진 스칼라 k를 d으로 변환하여 알고리듬이 수행된다.

마코프 연쇄 모델(Markov Chains Model)에 의한 분석에 의하면, 제안하는 재부호화 알고리듬에 의해 생성된 ±1 이진 스칼라의 Hamming weight는 평균적으로 전체 길이의 절반이 됨을 쉽게 알 수 있다.

Algorithm 5[5] : SPA-Resistant MSB-first signed-digit binary	
Input	d(sigined-binary secret key), P(basepoint), $n(=\|d\|)$
Output	$d \cdot P$
$Q[0] \leftarrow P$, $P[0] \leftarrow P$, $P[1] \leftarrow P$, $P[-1] \leftarrow -P$ for $i = n-2$ down to 0 $Q[0] \leftarrow ECDBL(Q[0])$ $Q[1] \leftarrow ECADD(Q[0], P[d_i])$ $Q[0] \leftarrow Q[\|d_i\|]$ return($Q[0]$)	

2) '-' 은 ±1 에 무관함을 의미한다.

■ **안전성.** Ha-Moon의 랜덤 스칼라 곱셈과 마찬가지로 제안하는 재부호화 알고리듬을 이용한 랜덤 스칼라 곱셈은 정리 1의 조건을 만족하므로 CG-DPA 에 안전하다.

V. 효율성 고려 및 비교

±1 이진 스칼라의 Hamming weight는 효율성과 관련이 있는데, 앞에서 언급한 바와 같이 두 재부호화 알고리듬에 의해 생성된 ±1 이진 스칼라의 Hamming weight는 평균적으로 전체 길이의 절반이 된다. Jacobi[9] 또는 Hessian[7] 형태 타원곡선에서 덧셈과 2배 연산의 통합된 공식을 적용하면, n 비트 ±1 이진 스칼라에 대하여 평균적으로 $(n-1)/2$회의 덧셈과 $(n-1)$회의 2배 연산을 통해 스칼라 곱셈이 이루어진다. 타원곡선 뺄셈 또한 Jacobi 와 Hessian 형태 타원곡선에서 다른 연산과 동일한 계산량과 절차에 이루어 질 수 있기 때문에 SPA에 안전한다.

Remark 5. Brier-Joye[1] 에 의한 Weierstraß 형태 타원곡선에서의 덧셈과 2배 연산의 통합된 공식은 고려하지 않는다. 왜냐하면 그들의 공식은 예외적인 점들에 대해 적용되지 않기 때문이다. 즉, $y_1 + y_2 = 0$을 만족하는 무한원점(point at infinity)이 아닌 두 개의 점 $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$은 유한체 $GF(p)^*$에서 0^{-1} 때문에 오류를 발생시킨다.

랜덤 재부호화 알고리듬의 비용은 전체 스칼라 곱셈 알고리듬의 계산량과 비교하여 무시할 만한 비용이 소요되므로 재부호화 알고리듬의 비용은 계산량 비교시 고려하지 않는다. 유한체의 제곱과 역원 계산량은 $1S$=0.8M, $1I$=30M 으로 추정하였다. 제안하는 스칼라 곱셈 방식은 알고리듬 5을 이용한다. 제안하는 방식의 효율성을 최적화하기 위해서 Jacobian 좌표계에서 연산을 수행한다. 알고리듬 5의 경우 반복문내에서 고정된 점이 더해지기 때문에 기저점 P을 Z=1 으로 설정할 수 있어서 효율성이 증대된다. Izu와 Takagi는 Mogomery-ladder를 이용하여 스칼라 곱셈을 2개, 4개의 프로세서로 처리하는 병렬처리 구조를 제안하였다. 그들의 방법은 DPA와 SPA를 동시에 막는 가장 빠른 알고리듬으로 알려져 있다. 스마트카드와 같은 제한적인 환경을 고려할 때, 본 논문의 비

〔표 2〕 제안하는 MSB-first CG-DPA 방어 알고리즘의 연산량 및 메모리 사용 비교, n은 소수 p의 비트크기. isogeny 함수를 이용하는 대응방법의 연산량 $3\ell M$이 기저점 은닉의 연산량 $2A + 2D$ (≒ $48M$) 보다 같거나 작게 되는 ℓ〈16인 경우를 고려한다.

algorithms		addition	subtraction	doubling	blinding or isogeny	# mul./bit	EEPROM(system parameters)
proposed signed-scalar	Hessian-type	12M	12M	12M	·	18 M/bit	7 n
	Jacobian coor. ECADDJ,Z=1	8M + 3S (Z=1)	8M + 3S (Z=1)	4M + 6S	·	19.2 M/bit	7 n
Izu-Takagi[6] (no parallel)	rand. proj. coor. + blinding	9M + 2S	·	6M + 3S	2A + 2D	19.55 M/bit	8 n + 6 n
	rand. isom. + blinding	8M + 2S (Z=1)	·	6M + 3S	2A + 2D	18.61 M/bit	8 n + 6 n
	rand. proj. coor. + isogeny	9M + 2S	·	6M + 3S	$3\ell M$	19.55 M/bit	8 n + 3 ℓn + 2 n
	rand. isom. + isogeny	8M + 2S (Z=1)	·	6M + 3S	$3\ell M$	18.61 M/bit	8 n + 3 ℓn + 2 n

교에서는 1개의 프로세서만을 이용하는 비병렬처리 구조만을 비교 대상에 포함시킨다. 제안하는 랜덤 스칼라 곱셈 알고리듬은 Izu-Takagi의 방법 중, 랜덤화된 사영좌표계 방법과 은닉 또는 isogeny를 결합한 방법보다 약간 더 빠르다.

스마트 카드의 RAM은 스칼라 곱셈 중간의 임시 변수를 저장한다. 반면 고정된 시스템 파라미터는 E-EPROM에 저장된다. 또한 EEPROM은 사용자 응용데이터와 실행파일을 보관하며 보통 16Kbyte로 제한되어 있다. 따라서 RAM뿐만 아니라 EEPROM의 메모리 사용을 줄이는 것 또한 중요한 문제가 된다. 모든 비교대상 알고리듬에서 공통적인 시스템 파라미터로서(소수, 타원곡선군 위수, 코펙터, 타원곡선 방정식의 계수, 기저점)이 포함된다. 기저점 은닉기법은 초기에 두 개의 타원곡선상의 점이 저장되기 때문에 $6n$ 비트의 메모리가 필요하며, isogeny 함수를 이용한 방법은 2절에서 언급되었듯이 $(3\ell+2)n$ 비트가 필요하다. 결과적으로 제안하는 스칼라 곱셈 방식은 기존의 CG-DPA 대응방법들 보다 적은 EEPROM을 사용한다.

참 고 문 헌

[1] É. Brier, M. Joye, "*Weierstraß Elliptic Curves and Side-Channel Attacks*", PKC 2002, LNCS 2274, pp.335~345, 2002.

[2] J.S. Coron, "*Resistance against Differential Power Analysis for Elliptic Curve Crypto-systems*", CHES 1999, LNCS 1717, pp.292~302, 1999.

[3] Louis Goubin, "*A Refined Power-Analysis Attack on Elliptic Curve Cryptosystems*", PKC 2003, LNCS 2567, pp.199~211, 2003.

[4] D-G. Han, N. S. Chang, S. W. Jung, Y.-H. Park, C.H. Kim, H. Ryu, "*Cryptanalysis of the Full version Randomized Addition-Subtraction Chains*", will be published in ACISP 2003.

[5] J. C. Ha, S. J. Moon, "*Randomized Signed-Scalar Multiplication of ECC to Resist Power Attacks*", CHES 2002, LNCS 2523, pp.551~563, 2002.

[6] T. Izu, T. Takagi, "*A Fast Parallel Elliptic Curve Multiplication Resistant against Side Channel Attack*", PKC 2002, LNCS 2274, pp.280~296, 2002.

[7] M. Joye, J.J. Quisquater, "*Hessian elliptic curves and side-channel attacks*", CHES 2001, LNCS 2162, pp.402~410, 2001.

[8] M. Joye, C. Tymen, "*Protections against differential analysis for elliptic curve cryptography : An algebraic approach*", CHES 2001, LNCS 2162, pp.377~390, 2001.

[9] P.Y. Liardet, N.P. Smart, "*Preventing SPA/DPA in ECC systems using the Jacobi form*", CHES 2001, LNCS 2162, pp.391~401, 2001.

[10] F. Morain, J. Olivos, "*Speeding up the computation on an elliptic curve using addition-subtraction chains*", Inform. Theory Appl. 24, pp.531~543, 1990.

[11] K. Okeya, K. Sakurai, "*Power analysis breaks elliptic curve cryptosystems even secure against the*

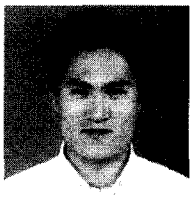
timing attack", Indocrypt 2000, LNCS 1977, pp.178~190, 2000.

[12] K. Okeya, K. Sakurai, "*On insecurity of the side channel attack countermeasure using addition-subtraction chains under distinguishablility between addition and doubling*", ACISP 2002, LNCS 2834, pp.420~435, 2002.

[13] E. Oswald, M. Aigner, "*Randomized Addition-Subtraction Chains as a Count-ermeasure against Power Attacks*", CHES 2001, LNCS 2162, pp.39~50, 2001.

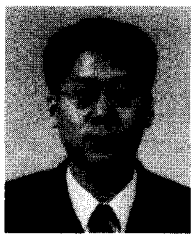
[14] N.P. Smart, "*An Analysis of Goubin;s Refined Power Analysis Attack*", to be published in CHES 2003.

〈著者紹介〉



장 상 운 (Sang-Woon Jang) 학생회원
2002년 2월 : 고려대학교 수학과 학사
2003년 3월 : 고려대학교 정보보호대학원 석사과정
<관심분야> 공개키 암호 알고리즘, 부채널 공격 방법론, 암호 프로토콜

정 석 원 (Seok Won Jung) 정회원
1991년 2월 : 고려대학교 수학과 학사
1993년 2월 : 고려대학교 수학과 석사
1997년 2월 : 고려대학교 수학과 박사
1997년 5월~1997년 11월 : 한국전자통신연구원 박사후연구원
1999년 2월~2001년 2월 : (주)텔리맨 책임연구원
2002년 3월~현재 : 고려대학교 정보보호대학원 조교수
<관심분야> 암호칩 설계, 부채널 공격 방법론, 공개키 암호알고리즘, 디지털 방송 보안



박 영 호 (Young-Ho Park) 정회원
1990년 2월 : 고려대학교 수학과 학사
1993년 2월 : 고려대학교 수학과 석사
1997년 2월 : 고려대학교 수학과 박사
2002년 3월~현재 : 세종 사이버 대학교 조교수
<관심분야> 정수론, 공개키 암호, 암호 프로토콜