*Journal of The Korea Institute of Information Security & Cryptology* ISSN 1598-3986(Print)
VOL.26, NO.5, Oct. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.5.1099

# 차분 전력 분석 공격에 대한 캐리 기반 랜덤 리코딩 방법의 취약성

하 재 철†‡
호서대학교

# Vulnerability of Carry Random Scalar Recoding Method against Differential Power Analysis Attack

Jaecheol Ha†‡
Hoseo University

요 약

정보보호용 임베디드 장치에 타원 곡선 암호 알고리듬을 구현할 경우 스칼라 곱셈 연산을 수행하게 되는데 이 연산 과정에서 발생하는 전력 소비 정보에 의해 비밀 키가 노출될 가능성이 있다. 최근에는 비밀 키 값을 리코딩하여 사용함으로써 단일 전력 분석과 차분 전력 분석 공격을 방어할 수 있도록 하는 캐리 랜덤 리코딩 방식이 제안되었다. 본 논문에서는 이 방식을 이용하면 차분 전력 분석을 방어할 수 있다는 원 논문의 주장과 달리 사용하는 리코딩 과정에서 발생하는 캐리 크기의 제한성으로 인해 차분 전력 분석에 여전히 취약함을 밝히고자 한다.

ABSTRACT

The user's secret key can be retrieved by the leakage informations of power consumption occurred during the execution of scalar multiplication for elliptic curve cryptographic algorithm which can be embedded on a security device. Recently, a carry random recoding method is proposed to prevent simple power and differential power analysis attack by recoding the secret key. In this paper, we show that this recoding method is still vulnerable to the differential power analysis attack due to the limitation of the size of carry bits, which is a different from the original claim.

**Keywords :** Carry Random Recoding, SPA, DPA, Scalar Multiplication

## I. 서 론

최근 센싱과 통신 기능이 향상된 사물 인터넷(Internet of Things, IoT)이 보급되면서 센서와 같은 단말 기기의 안전한 구현이 필수 요소로 대두되고 있다. 특히, 단말에서 인증이나 암호와 같은 정보보호 서비스를 제공하기 위해서는 사용되는 암호 알고리듬이 이론적 공격에도 안전해야 함은 물론 시스템 구현상에서 발생할 수 있는 부채널 분석(side channel analysis) 공격에도 안전하게 설계되어야 한다.

부채널 분석 공격은 1996년 Kocher에 의해 처음 제시된 공격 방법으로서 암호 알고리듬이 장치에서 동작할 때 발생하는 시간 정보, 전력 소비량 그리고 전자기파 방사 정보 등을 활용한다[1]. 이 중에서 전력 분석을 통한 공격이 가장 많이 연구되었으며 대표적인 공격 방법으로는 단순 전력 분석(Simple Power Analysis, SPA) 공격과 차분 전력 분석(Differential Power Analysis, DPA) 공격 등이 있다[2-3]. SPA는 단순히 하나의 소비 전력 파

Received(08. 03. 2016), Modified(09. 19. 2016), Accepted(09. 20. 2016)
† 주저자, jcha@hoseo.edu
‡ 교신저자, jcha@hoseo.edu(Corresponding author)

형을 관측함으로써 비밀 키를 추출하는 방법인 반면, DPA는 수십~수백 개의 전력 소비 파형을 수집한 후 통계적인 분석 기법을 이용하여 비밀 키를 추출한다.

한편, 타원 곡선 암호 시스템[4]의 스칼라 곱셈 시에도 SPA나 DPA와 같은 전력 분석 공격이 시도될 수 있다. 타원 곡선 암호 시스템에서 SPA를 방어하기 위해서는 Montgomery ladder 방법[5]이나 Double-and-add always 방법[2]과 같은 정규화 알고리듬을 사용하고 있다. 또한, DPA 공격을 방어하기 위해서는 스칼라 랜덤화, 점(point)의 랜덤화 그리고 좌표계(projective)의 랜덤화 기법 등을 사용하고 있다[2]. 이 외에도 스칼라 곱셈의 계산 효율성을 높이면서 랜덤성을 제공하기 위해 NAF(Non-Adjacent Form)에 기반한 스칼라 랜덤화 기법들이 제안되고 있다[6].

최근, 타원 곡선 암호 시스템에서 SPA와 DPA에 대응하기 위한 대응책으로 랜덤한 스칼라 리코딩 방법이 제안되었다[7]. 이 방법은 캐리(carry)를 랜덤하게 발생하여 스칼라 값을 랜덤하게 재부호화 하는 방법으로서, 이를 이용한 스칼라 곱셈은 SPA 및 DPA에 강인할 뿐만 아니라 기존 m-ary 방법보다 계산량이 약 11% 정도 줄어드는 것으로 분석되었다.

본 논문에서는 문헌 [7]에서 제시한 CRR (Carry Random Recoding) 방법을 재분석한 결과, 리코딩을 처리하는 캐리 비트 크기가 제한되는 약점으로 인해 DPA 공격에 여전히 취약함을 보이고자 한다.

## II. 최근 제안된 스칼라 리코딩 기법

타원 곡선 암호 시스템에서의 가장 중요한 연산은 스칼라 곱셈이며 이 연산은 타원 곡선위의 점 $P$를 $k$번 더하는 $Q=kP$로 표현된다. 스칼라 곱셈은 전자 서명 및 키 일치 암호 시스템에서 주로 수행되며 이 때 $k$는 비밀 키가 된다. 그러나 타원 곡선 암호 시스템에서의 스칼라 곱셈 시 이진 방식(binary method)과 같은 단순한 알고리듬을 사용하면 SPA나 DAP에 의해 비밀 키가 노출될 수 있다.

### 2.1 캐리 랜덤 리코딩 방법

최근 유효명 등은 부채널 공격에 대응하기 위해 CRR이라는 스칼라 리코딩 기법을 제안하였으며 이 방법을 통하여 SPA와 DPA를 방어할 수 있다고 주장하였다[7]. 이 방법에서는 비밀 키 $k$를 두 비트씩 묶어 하나의 디지트(digit)로 둔 4진수 표현 방법을 사용하고 있다. CRR 방법은 랜덤하게 발생한 캐리를 이용하여 디지트의 변환 여부를 선택하는 스칼라 변환 방식으로서 구체적인 변환 규칙은 Table 1과 같다.

리코딩은 하위 디지트로부터 상위 디지트로 진행하는데 생성된 랜덤 캐리에 의존하여 $k$값이 변환되게 된다. 이전 디지트에서 발생한 캐리는 다음 디지트에 영향을 주게 되는데 이 때 중요한 것은 캐리 발생이 연쇄적으로 상위 디지트에 영향을 미쳤을 때 한 디지트에는 최대 2까지의 캐리가 더해진다는 점이다. 그리고 최종적인 리코딩 결과는 원래 스칼라 값보다 한 자리 이상은 넘어가지 않는다.

Fig. 1은 $l$비트인 스칼라 $k$가 $(l+1)$비트인 $k'$으로 리코딩되는 알고리듬을 나타낸 것이다. 입력 스칼라 값은 0을 포함하여 4개 디지트 값을 갖지만 리

Table 1. Carry Random Recoding

| Digit | Carry | Recoded digit |
|---|---|---|
| 0 | 1 | -4 |
| 1 | 0 | 1 |
| | 1 | -3 |
| 2 | 0 | 2 |
| | 1 | -2 |
| 3 | 0 | 3 |
| | 1 | -1 |

Input: $k=(k_{l-1}, k_{l-2}, \ldots k_0)_4, k_i \in \{0,1,2,3\}$
Output: $k'=(k'_{t-1}, k'_{t-2}, \ldots k'_0)_4$,
$k'_i \in \{-4,-3,-2,-1,1,2,3\}$

1. $i \leftarrow 0$
2. for $i$ form 0 to $l-1$ do
   2.1 Generate random bit $R$
   2.2 if ($k \bmod 4 = 0$ ) then $R \leftarrow 1$
   2.3 $k' \leftarrow (k \bmod 4) - 4 \cdot R$
   2.4 $k \leftarrow k/4 + R$
3. $k'_l \leftarrow k$
4. if ($k'_l = 0$ ) then $t=l$ else $t=l+1$
5. Return$((k'_{t-1}, k'_{t-2}, \ldots k'_0)_4)$

Fig. 1. Carry Random Recoding

코딩된 값은 7개 값을 갖게 된다.

### 2.2 리코딩 기법을 활용한 타원 곡선 스칼라 곱셈

제안된 CRR 방법을 적용한 부채널 공격에 대응하는 타원 곡선 스칼라 곱셈을 나타낸 것이 Fig. 2 이다. 제안하는 알고리듬의 단계 4.2에서는 $P+Q$ 또는 $P-Q$ 연산을 수행하는데 두 점 $P$와 $Q$ 그리고 $Q$의 부호 정보를 Jacobian-affine coordinates ECADD 방식을 사용하여 처리하였다[8]. 또한, 정규적인 덧셈(addition)과 두 배(doubling) 연산을 이용하여 SPA 공격을 방어하고 랜덤 스칼라 리코딩을 이용하여 DPA를 방어할 수 있다고 분석하였다. 또한, CRR을 적용한 스칼라 곱셈의 경우 기존의 랜덤 m-ary 방법보다 약 11% 정도 연산량이 감소되는 것으로 분석하였다.

Input: $k=(k_{l-1}, k_{l-2}, \ldots k_0)_4$, $P \in E(F_p)$
Output: $kP$

1. Compute $k' = \sum_{i=0}^{t-1} k'_i 4^i$ using CRR alg.
2. Compute $P_i = iP$ for $i \in 1,2,3,4$
3. $Q \leftarrow O$
4. for $i$ from $t-1$ to 0 do
   4.1 $Q \leftarrow 4Q$
   4.2 $Q \leftarrow Q \pm P_{k'_i}$
5. Return(Q)

Fig. 2. Scalar multiplication using Carry Random Recoding algorithm

## III. CRR 방법의 DPA 대한 취약성

상기한 CRR 방법은 부호화된 디지트로 리코딩을 진행하면서 한 비트의 캐리를 사용한다. 여기서 스칼라 $k=\sum_{i=0}^{l-1} k_i 4^i$ 는 $k'=\sum_{i=0}^{l} k'_i 4^i$으로 부호화 된다고 가정한다. 그런데 하위의 디지트가 연속적으로 캐리를 발생시키면 다음과 같이 한 디지트에는 최대 2까지의 캐리가 발생하게 된다.

$$\sum_{j=0}^{i-1} k_j \cdot 4^j = \sum_{j=0}^{i-1} k'_j \cdot 4^j, \quad 4^i + \sum_{j=0}^{i-1} k'_j \cdot 4^j, \text{ or } 2 \cdot 4^i + \sum_{j=0}^{i-1} k'_j \cdot 4^j \quad .$$

또한, $kP = k'P$ 가 되므로 아래와 같은 등식이 성립한다.

$$\sum_{j=0}^{l-1} k_j \cdot 4^j = \sum_{j=0}^{l} k'_j \cdot 4^j$$

따라서 스칼라 곱셈이 진행되는 동안, 스칼라의 중간 값은 아래와 같이 표현할 수 있다.

$$\sum_{j=i}^{l-1} k_j \cdot 4^{j-i} = \sum_{j=i}^{l} k'_j \cdot 4^{j-i}, \ \sum_{j=i}^{l} k'_j \cdot 4^{j-i} - 1, \text{or } \sum_{j=i}^{l} k'_j \cdot 4^{j-i} - 2 \ .$$

따라서 공격자가 $k_{l-1}, k_{l-2}, .., k_{i+1}$ 를 알고 $k_i$비트를 공격한다고 가정하면 $(l-(i-1))$ 번째 반복문을 수행한 값은 $Q=(\sum_{j=i}^{l} k'_j \cdot 4^{j-i})P$ 가 되는데 $\sum_{j=i}^{l} k'_j \cdot 4^{j-i}$ 값은 다음 중 하나가 된다.

$$\sum_{j=i}^{l-1} k_j \cdot 4^{j-i}, \sum_{j=i}^{l-1} k_j \cdot 4^{j-i} + 1, \text{ or } \sum_{j=i}^{l-1} k_j \cdot 4^{j-i} + 2$$

즉, Fig. 2를 이용하여 스칼라 곱셈을 수행할 경우 단계 4.2에서 발생할 수 있는 값은 최대 3종류의 값만 가지게 된다. 결국, CRR을 이용한 리코딩 기법

| Index | | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|---|---|---|---|---|---|---|---|---|
| $k_i$ | | | 2 | 1 | 3 | 3 | 0 | 1 |
| $\sum_{j=i}^{l-1} k_i \cdot 4^{j-i}$ | | | 2 | 9 | 39 | 159 | 636 | 2545 |
| Case 1 | Carry | | 0 | 1 | 1 | 0 | 1 | 1 |
| | $k'_i$ | 1 | -1 | -1 | -3 | -4 | -3 | -3 |
| | $\sum_{j=i}^{l} k'_i \cdot 4^{j-i}$ | 1 | 3 | 11 | 41 | 160 | 637 | 2545 |
| Case 2 | Carry | | 1 | 1 | 0 | 1 | 1 | 0 |
| | $k'_i$ | 1 | -1 | -2 | 1 | -4 | -4 | 1 |
| | $\sum_{j=i}^{l} k'_i \cdot 4^{j-i}$ | 1 | 3 | 10 | 41 | 160 | 636 | 2545 |
| Case 3 | Carry | | 1 | 0 | 0 | 1 | 0 | 1 |
| | $k'_i$ | 1 | -2 | 3 | -4 | -1 | 1 | -3 |
| | $\sum_{j=i}^{l} k'_i \cdot 4^{j-i}$ | 1 | 2 | 11 | 40 | 159 | 637 | 2545 |

Fig. 3. The example of CRR algorithm

이 스칼라 값을 랜덤하게 만들 수 있지만 각 디지트 단위로 곱셈 연산을 수행할 경우에는 레지스터가 가질 수 있는 값이 제한적이므로 DPA 공격에 취약하다. Fig. 3은 $k=2{,}545$ 일 때 CRR 리코딩 방법과 스칼라 곱셈 과정의 중간 값을 표시한 예로서 CRR 알고리듬을 적용한 경우의 특정 디지트까지 계산한 스칼라 곱셈의 중간 값은 그렇지 않은 경우의 값과 같거나, 1 혹은 2를 더한 값이라는 것을 보여주고 있다.

상기한 CRR 알고리듬을 이용하여 스칼라 곱셈을 구현했을 경우 ZEMD(Zero-Exponent, Multiple-Data) 방식[3]을 이용한 DPA 공격 수행 절차를 나타낸 것이 Fig. 4이다.

여기서 공격에 필요한 파형 수를 예측하기 위해서 각 디지트에서 캐리가 발생할 확률을 계산할 필요가 있는데 이를 정리한 것이 Table 1이다. 먼저 캐리의 합이 2인 경우는 현재 디지트 값이 3인 상태에서 이전 디지트에서 캐리 $c_{i-1}$이 발생한 경우이므로 확률 1/4*1/2=1/8 로 발생한다. 그리고 캐리가 발생하지 않는 확률은 3/8이며 캐리 합이 1이 될 확률은 1/2이다. Table 1에서 $c_i$는 이전 캐리가 처리된 다음 상태에서 발생한 캐리를 의미한다.

Input: Random points, $\{P_1, P_2, .. P_s\}$
Output: Scalar exponent $k$

1. Choose random points $\{P_1, P_2, .. P_s\}$.
2. Compute $k \cdot P_v$ for $1 \le v \le s$, and obtain power trace $T^{(v)}$.
3. for $i = l-1$ to 0 by -1 do
   3.1 for $d = 0$ to 3 by 1 do
      3.1.1 Let $k_i = d$.
      3.1.2 Compute $(\sum_{j=i}^{l-1} k_j \cdot 4^{j-i}) P_v$ by simulation for $1 \le v \le s$.
      3.1.3 Divide $T^{(v)}$'s in to two set $S_0$, $S_1$ according to decision function, such as Hamming weight of the simulated values.
      3.1.4 Average the two sets and get the difference, $D = Avg(S_0) - Avg(S_1)$.
      3.1.5 If ($D$ has a spike) then break.
   3.2 Set $k_i = d$
4. Return($k$).

Fig. 4. The ZEMD attack on the scalar multiplication adopting CRR algorithm

Table 2. Probability of carry sum

| Current state | $c_{i-1}$ | Next state | $c_i$ | Carry sum | Probability |
|---|---|---|---|---|---|
| 0 | 0 | 0 | x | 1 | 1/8 |
| | 0 | 0 | x | 1 | |
| | 1 | 1 | 0 | 0 | 1/16 |
| | 1 | 1 | 1 | 1 | 1/16 |
| 1 | 0 | 1 | 0 | 0 | 1/16 |
| | 0 | 1 | 1 | 1 | 1/16 |
| | 1 | 2 | 0 | 0 | 1/16 |
| | 1 | 2 | 1 | 1 | 1/16 |
| 2 | 0 | 2 | 0 | 0 | 1/16 |
| | 0 | 2 | 1 | 1 | 1/16 |
| | 1 | 3 | 0 | 0 | 1/16 |
| | 1 | 3 | 1 | 1 | 1/16 |
| 3 | 0 | 3 | 0 | 0 | 1/16 |
| | 0 | 3 | 1 | 1 | 1/16 |
| | 1 | 0 | x | 2 | 1/8 |
| | 1 | 0 | x | 2 | |

따라서 Fig. 4의 공격 알고리듬에서 만약 $k_i$를 정확히 예측했다면 전체 $s$개의 파형 중에서 발생 확률에 비례한 파형 수 만큼 컴퓨터로 예측한 값과 실제 중간 값이 같을 것이다. 비밀 키를 정확히 예측하였지만 상태에서 캐리를 예측하지 못한 나머지 파형들은 차분 신호에 잡음처럼 작용하여 스파이크를 형성하는데 기여하지 않게 된다.

한편, DPA 공격에 필요한 파형 수 $n$은 예측 값과 실제 전력 파형의 상관 계수 $\rho$와 $n \approx 1/\rho^2$ 관계를 가지고 있다[9]. 공격에 필요한 상관 계수는 전력 파형수와 비례하므로, 만약 캐리 발생 확률이 $p$라면 원래 DPA 공격에 필요한 전력 파형 수보다 최소한 $1/p^2$ 배 정도의 파형이 필요하다. 따라서 Fig. 4의 공격에서 캐리가 1인 경우의 키를 찾아내기 위해서는 기존 공격에 필요한 파형보다 약 4배, 캐리가 0인 경우에는 약 7배 그리고 캐리가 2인 경우는 약 64배의 전력 파형을 수집하여야 한다. 그러나 캐리가 2인 경우는 캐리가 0이나 1이 아닌 경우로 예외 처리가 가능하므로 CRR 알고리듬을 이용하여 스칼라 곱셈을 구현할 경우 기존 공격보다 약 7배의 파형만 수집하면 DPA 공격이 가능할 것으로 분석된다.

이와 같이 CRR을 이용한 리코딩 기법을 이용한 스칼라 곱셈이 DPA에 취약한 이유는 리코딩을 이용해 무수히 많은 랜덤한 스칼라 값을 만들 수 있지만 각 디지트 단위로 끊어서 볼 때는 캐리가 최대 2까

지 제한되고 있어 스칼라 곱셈 시 특정 디지트의 자리에서 가질 수 있는 값은 최대 3종류 밖에 되지 않는다. 따라서 DPA 공격 대응책이 없을 경우 공격에 필요한 파형 수 보다 7배 정도 파형을 더 측정할 수 있다면 충분히 DPA 공격이 성공할 수 있다.

## IV. 결 론

본 논문에서는 타원 곡선 암호 시스템에서 이루어지는 스칼라 곱셈 연산 시 부채널 공격에 대응하기 위해 최근 제안된 캐리에 기반한 랜덤한 리코딩 기법을 적용하더라도 DPA 공격에 여전히 취약함을 증명하였다. 즉, 스칼라 값에 대한 랜덤화 기법은 비밀키 비트나 바이트를 순차적으로 탐색해 가는 DPA와 같은 형태의 공격에 의해 비밀 키가 노출될 수 있다.

따라서 스칼라 랜덤화 기법과 더불어 점의 랜덤화나 좌표계 랜덤화와 같은 다른 DPA 방어 대책을 동시에 적용하는 것 필요하다. 입력 점을 랜덤화 방식은 사전 계산 값을 저장 공간이 필요하고, 좌표계 랜덤화 기법은 좌표계 이동에 따른 추가 연산이 필요함에도 불구하고 저메모리, 저성능의 개발 환경에 적합한 DPA 방어 대책이 될 수 있다.

## References


[1] P. Kocher, "Timing Attacks on Implementation of Diffie-Hellman, RSA, DSS, and Other Systems," CRYPTO'96, LNCS 1109, pp. 104-113, 1996.

[2] J. Coron, "Resistance against differential power analysis for elliptic curve cryptosystems," CHES'99, LNCS 1717, pp. 292-302, 1999.

[3] T. Messerges, E. Dabbis, and R. Sloan, "Power analysis attacks of modular exponentiation in smartcard," CHES'99, LNCS 1717, pp. 144-157, 1999.

[4] N. Koblitz, "Elliptic curve cryptosystem," Mathematics of Computation, vol. 48, no. 177, pp. 203-209, 1987.

[5] M. Joye and S. M. Yen, "The Montgomery Powering Ladder," CHES'02, LNCS 2523, pp. 291-302, 2002.

[6] G. Reitwiesner, "Binary arithmetic," Advances in Computers, pp. 231-308, 1960.

[7] H. Ryu, S. Cho, T. Kim, C. Kim, and S. Hong, "A new scalar recoding method against side channel attacks," Journal of The Korea Institute of Information Security & Cryptology(JKIISC), 26(3), pp. 587-601, 2016.

[8] D. Hankerson, A. Menezes, and S. Vanstone, "Guide to elliptic curve cryptography," Springer Professional Computing, Springer-Verlag, New York, 2004.

[9] S. Mangard, E. Oswald, and T. Popp, Power Analysis attacks - Revealing the secrets of smart cards, Springer, pp. 136-150, 2007.


## 〈저자소개〉


하 재 철 (Jaecheol Ha) 종신회원
1989년 2월: 경북대학교 전자공학과 졸업
1993년 8월: 경북대학교 전자공학과 석사
1998년 2월: 경북대학교 전자공학과 박사
1998년 3월~2007년 2월: 나사렛대학교 정보통신학과 부교수
2007년 3월~현재: 호서대학교 컴퓨터정보공학부 정보보호전공 교수
2013년 1월~현재: 한국정보보호학회 부회장
2009년 1월~현재: 한국산학기술학회 이사
〈관심분야〉 암호 알고리듬, 네트워크 보안, 부채널 공격