Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.5, Oct. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.5.985

지수 분할 기법이 적용된 RSA 알고리듬에 대한 충돌 전력 분석 공격 안전성 평가*

하 재 철†‡
호서대학교

Security Evaluation Against Collision-based Power Analysis on RSA Algorithm Adopted Exponent Splitting Method*

Jaecheol Ha†‡
Hoseo University

요 약

정보보호용 임베디드 장치에 RSA 암호 알고리듬을 구현하여 연산을 수행할 경우, 동작 과정에서 발생하는 부채널 누설 정보에 의해 비밀 키가 노출될 가능성이 있다. 여러 부채널 공격 중에서 RSA 알고리듬을 수행하면서 발생한 하나의 전력 파형에서 전력 충돌 쌍을 찾아 공격하는 충돌 전력 분석 공격이 매우 위협적인 것으로 알려져 있다. 최근 이 공격에 대한 대응책으로 윈도우 기법에 기반하여 블라인딩과 지수 분할 기법을 적용한 RSA 멱승 알고리듬이 제안되었다. 본 논문에서는 윈도우 크기가 2일 때를 기준으로 이 대응책의 공격 복잡도가 2^{98}이라는 원 논문의 주장과 달리 2^{53}의 복잡도를 제공한다는 점을 밝히고자 한다.

ABSTRACT

The user's secret key can be retrieved by various side channel leakage informations occurred during the execution of cryptographic RSA exponentiation algorithm which is embedded on a security device. The collision-based power analysis attack known as a serious side channel threat can be accomplished by finding some collision pairs on a RSA power consumption trace. Recently, an RSA exponentiation algorithm was proposed as a countermeasure which is based on the window method adopted combination of message blinding and exponent splitting. In this paper, we show that this countermeasure provides approximately 2^{53} attack complexity, much lower than 2^{98} insisted in the original article, when the window size is two.

Keywords: Embedded Secure Module, Exponentiation Algorithm, Collision-based Power Analysis, Exponent Splitting, Efficiency-Security Evaluation

I. 서 론

스마트카드와 같은 정보보호 디바이스에서 데이터를 암·복호화 하거나 서명을 할 경우 RSA와 같은 암호 알고리듬을 소프트웨어 형태로 구현하여 사용한다. 그러나 알고리듬을 수행할 때 발생하는 누설 정보(전력, 전자기파, 시간 정보 등)를 이용하면 비밀 키 추출이 가능한데 이러한 공격을 부채널 공격(side channel attack)이라 한다. 부채널 공격은 1996년 Kocher에 의해 제안된 이후 많은 공격 기법과 그에 대한 대응책들이 제시되어 왔다[1-4]. 특히, 알고리듬 수행 시 발생하는 소비 전력을 분석하

접수일(2015년 7월 17일), 수정일(1차: 2015년 8월 31일, 2차: 2015년 9월 30일), 게재확정일(2015년 10월 2일)
* 이 논문은 2014년도 호서대학교의 재원으로 학술연구비 지원을 받아 수행된 연구임.(2014-0420)
† 주저자, jcha@hoseo.edu
‡ 교신저자, jcha@hoseo.edu(Corresponding author)

는 전력 분석 공격이 대표적인 부채널 공격이라 할 수 있다.

여러 가지 전력 분석 공격 방법 중, 최근에는 모듈라 곱셈의 입력이 같은 두 연산에서 소비 전력 충돌이 발생하는 점을 이용한 충돌 전력 분석 공격이 등장하게 되었다[5-6]. 따라서 논문 [7]에서는 기존 메시지 블라인딩 기법[8]과 윈도우 기법이 적용된 RSA 암호 알고리듬[9]에 지수 분할 기법[10]을 혼합한 충돌 분석 공격 대응 알고리듬을 제안하였다. 그리고 기존의 방식이 약 2^{44}의 공격 복잡도를 제공했던 것에 비해 지수 분할 기법을 도입하여 구현하면 2^{98}까지 복잡도를 제공할 수 있다고 분석하였다.

그러나 본 논문에서는 논문 [7]에서 제시한 RSA 멱승 알고리듬을 사용할 경우, 모듈라 곱셈에 사용된 사전 계산 테이블의 사용 빈도가 달라진다는 점을 이용하면 충돌 전력 분석 공격의 공격 복잡도가 기존의 분석 결과보다 낮아진다는 점을 밝히고자 한다. 결론적으로 지수 분할 기법을 적용한 RSA 멱승 알고리듬을 구현하여 사용할 경우, 추가되는 사전 저장 테이블은 약 두 배 정도 늘어나지만 충돌 전력 분석 공격에 대한 안전성은 2^{53} 정도까지 향상시킬 수 있음을 고려하여야 한다.

II. 기존 RSA 충돌 분석 공격 대응 방안

2.1 멱승 알고리듬 및 모듈라 곱셈

공개 키 암호 알고리듬인 RSA를 이용하여 메시지를 복호하거나 서명을 수행할 경우 메시지 M에 대해 $S = M^d \bmod N$ 과 같은 멱승 연산을 수행한다. 일반적으로 d는 t비트의 개인 키로서 비밀 정보에 해당하며 N은 두 소수 p와 q의 곱으로서 1024 비트 이상의 큰 정수를 사용한다.

멱승 연산을 위해서는 다양한 알고리듬들을 사용할 수 있는데 기존의 전력 분석 공격과 같은 부채널 공격에 대비하여 변형된 멱승 기법을 많이 사용한다[3, 4, 8]. 특히, 논문 [8]에서는 단순 전력 분석이나 차분 전력 분석 공격에 안전하도록 랜덤 값 R을 사용한 블라인딩 기법을 제안한 바 있다. 논문에서는 메시지 M에 대한 서명을 $S = M^d R^{2\phi(N)} \bmod N$과 같이 계산한다. 여기서$\phi(N)$은 Euler totient 함수이다.

논문 [8]에서 제시한 멱승 방법은 역원 계산이 없으면서도 부채널 공격에 안전하도록 설계되어 있는데 연산의 효율성을 높이기 위해 윈도우 기법과 같은 고속 처리 알고리듬을 동시에 적용할 수 있다. 실제로 논문 [7]에서는 메시지 블라인딩 기법과 윈도우 기법을 적용한 멱승 알고리듬을 구체적으로 제시하였다. 그럼에도 불구하고 이 멱승 알고리듬은 윈도우 w가 2일 경우 약 2^{44} 정도의 비교적 낮은 공격 복잡도를 제공하고 있다.

2.2 지수 분할 방법을 적용한 기법

논문 [7]에서는 충돌 분석 공격의 공격 복잡도를 높이기 위해 메시지 블라인딩 기법[8]과 윈도우 기법이 적용된 RSA 암호 알고리듬에 지수 분할 기법[10]을 혼용한 새로운 멱승 기법을 제안하였다. 충돌 전력 분석 공격은 이전 논문에서와 같이 특정한 모듈라 곱셈 연산에서 입력 데이터가 같은 경우 전력 파형의 충돌이 발생할 수 있으며 이를 공격자가 구분 가능하다는 가정을 기반으로 하였다[7]. 따라서 충돌 전력 분석 공격은 하나의 멱승 연산에 대한 전력 소비 파형을 수집한 다음 이를 모듈라 곱셈 연산 단위로 구분한 후 각 연산 단위별로 충돌 쌍을 찾아냄으로써 비밀 키를 찾아내는 매우 위협적인 공격 방법이다.

논문 [7]에서 제안하는 멱승 알고리듬에서는 윈도우 크기가 w이고 $W = 2^w$일 때 아래와 같이 서명 연산을 수행한다.

$$S = M^r M^{(d-r)} R^{W\phi(N)} \bmod N \qquad (1)$$

이때 $\hat{d} = d - r$라 두고 세 비밀 지수 r, $\hat{d}$ 그리고 $\phi(N)$값을 표현하면 아래와 같다. 여기서 $k = \lceil t/w \rceil$ 이다.

$$r = (r_{t-1} r_{t-2} \cdots r_0)_2 = (r'_{k-1} r'_{k-2} \cdots r'_0)_W$$
$$\hat{d} = (\hat{d}_{t-1} \hat{d}_{t-2} \cdots \hat{d}_0)_2 = (\hat{d}'_{k-1} \hat{d}'_{k-2} \cdots \hat{d}'_0)_W$$
$$\phi(N) = (\phi_{t-1} \cdots \phi_0)_2 = (\phi'_{k-1} \phi'_{k-2} \cdots \phi'_0)_W$$

결국, 세 비밀 지수 r, $\hat{d}$ 그리고 $\phi(N)$을 w비트씩 스캐닝한 값 r'_i, $\hat{d'}_i$ ϕ'_{i-1}에 따라 Table 1과 같이 랜덤 수 R로 블라인딩되어 있는 메시지 $M^{r'_i + \hat{d}'_i} R^{\tilde{\phi}'_{i-1}}$을 곱하면서 멱승을 수행하게 된다.

이 경우 사전 연산 값 $M^{r'_i+\hat{d}'_i}R^{\tilde{\phi}'_{i-1}}$은 지수인 $r'_i+\hat{d}'_i$와 $\hat{\phi}'_{i-1}$ 값의 가지 수에 의해 결정된다. $r'_i+\hat{d}'_i$ 값이 가지는 개수를 계산해 보면 아래와 같이 0에서 $2W-2$ 사이의 $2W-1$개임을 알 수 있다.

$$r'_i,\ \hat{d}'_i \in \{0,1,\cdots\ W-1\} \tag{2}$$

$$r'_i+\hat{d}'_i \in \{0,1,\cdots\ 2W-2\} \tag{3}$$

또한, ϕ'_{i-1}는 W개가 존재하게 된다. 따라서 사전 계산 테이블은 $n=2W^2-W$개가 필요하다.

여기서 주목할 점은 r'_i와 $\widehat{d'}_i$가 각각 W개의 값을 가질 때 이 두 값을 더하는 경우의 수는 W^2이지만 그 결과 값의 개수는 $2W-1$라는 것이다. 예로서 Table 1과 같이 $w=2$인 경우를 살펴보면 $W=2^w=4$가 되고 더하는 경우의 수는 16종류가 되며, ϕ'_{i-1} 가 4이므로 모두 64개의 경우가 발생한다. 하지만 $r'_i+\hat{d}'_i$ 값의 종류는 $2W-1=7$개 밖에 되지 않으므로 총 28개의 사전 계산 테이블만 필요하게 된다.

실제 예로서 Table 1을 살펴보면, $r'_i=0$와 $\widehat{d'}_i=1$일 때의 사전 계산 값이나 $r'_i=1$와 $\widehat{d'}_i=0$일 때의 사전 계산 값은 같은 값을 가지며 멱승 연산 시에는 동일한 사전 계산 테이블을 이용하게 된다. 여기서 주목할 점은 $r'_i+\hat{d}'_i$의 값의 종류는 7가지이지만 이 7가지가 동일한 발생 빈도를 가지지 않는다는 것이며, 이러한 사실이 누설 정보가 되며 공격을 더 용이하게 만드는 요인이 된다.

Table 1. Pre-computation values for combined exponentiation algorithm ($w=2$, $\phi'_{k-1}=1$)

r'_i	$\widehat{d}'_i$	ϕ'_{i-1}	$\tilde{\phi}'_{i-1}$	Pre-computation
0	0	0	3	R^3
0	0	1	4	R^4
0	0	2	5	R^5
0	0	3	6	R^6
0	1	0	3	MR^3
0	1	1	4	MR^4
0	1	2	5	MR^5
0	1	3	6	MR^6
1	0	0	3	MR^3
1	0	1	4	MR^4
:	:	:	:	:
3	3	3	6	M^6R^6

다음 Fig. 1은 논문 [7]에서 제안하는 윈도우에 기반한 블라인딩과 지수 분할 기법을 조합한 멱승 알고리듬을 나타낸 것이다. 이 알고리듬에서는 랜덤 수를 발생하는 과정, d를 분할하는 과정, 사전 계산 테이블을 만드는 과정 그리고 반복 루프 연산을 통해 실제 멱승 값을 계산하는 과정으로 나눌 수 있다.

논문의 저자들은 이 알고리듬을 사용할 경우 충돌 분석 공격에 대한 공격 복잡도가 $(2W-1)(W-1)\times(n-1)$로 향상된다고 주장하였다. 즉, $w=2$인 경우, 지수 분할 기법을 적용하지 않았을 때 2^{44}의 복잡도를 가지던 것을 2^{98}까지 증가시킬 수 있다고 분석하였다. 그러나 이 논문에서의 복잡도 분석은 28개의 사전 계산 값을 사용하는 빈도가 동일할 경우를 가정한 것으로서 지수의 덧셈 값인 $r'_i+\hat{d}'_i$이 서로 다른 빈도를 나타낸다는 점을

Input : M, d, $\phi(N)$, N

Output : $S=M^d \bmod N$

1. If $M=1$ then return 1
2. If $M=-1$ then return $1-2d_0$
3. Generate random numbers $R\in\{1,2,\cdots,N-1\}$, $r(t-bits)$
4. Compute $\widehat{d}=d-r$
5. Pre-computation
   5.1 for($i=0$; $i<W$; i++)
      5.1.1 $S_i=R^{\phi'_{k-1}(W-1)+i} \bmod N$
   5.2 for($i=0$; $i<(2W^2-W)$; i+= W)
      5.2.1 for($j=0$; $j<W$; j++)
         5.2.2.1 $S_{(i+j+W)}=S_{(i+j)}\times M \bmod N$
6. for($i=k-1$; $i\geq 1$; i--)
   6.1 $S=S^W \bmod N$
   6.2 $S=S\times S_{(W(r'_i+\widehat{d}'_i)+\phi'_{i-1})} \bmod N$
7. Return($S^W\times S_{(W(r'_0+\widehat{d}'_0)+\phi'_{k-1})} \bmod N$)

Fig. 1. The combined exponentiation algorithm message blinding and exponent splitting based on window method[7]

간과하였다. 따라서 이 멱승 알고리듬에 대한 충돌 전력 분석 공격 복잡도의 재분석이 필요하다.

III. 충돌 전력 분석 공격 복잡도 재분석

지수 분할을 이용한 멱승 기법은 차분 전력 분석 공격(Differential Power Analysis, DPA) 대응책으로 제시되었다. 즉, 비밀 지수 d를 r과 $d-r$의 두 부분으로 나누어 $S=M^r \cdot M^{(d-r)} \bmod N$과 같이 구현할 때 $S_1=M^r \bmod N$과 $S_2=M^{(d-r)} \bmod N$을 분리하여 계산한 후 $S=S_1 \cdot S_2 \bmod N$를 구한다면 DPA 공격에 안전하다. 그러나 이 두 연산을 Shamir의 기법[11]을 적용하여 동시에 처리하는 경우에는 분리된 두 지수를 다시 더하는 효과로 인해 DPA 공격에 취약하다는 것이 밝혀졌다[12].

그럼에도 논문 [7]에서는 DPA 방어책인 메시지 블라인딩 방법과 충돌 분석 공격에 대한 방어책으로 지수 분할 기법을 혼용하는 멱승 알고리듬을 제안하였다. 따라서 본 논문에서는 지수 분할 기법을 충돌 분석 공격 대응책으로 다른 멱승 기법들과 혼용할 경우 어느 정도 공격 복잡도를 증가시키는지 재분석하고자 한다.

앞 장에서 기술한 바와 같이 $r'_i+\hat{d}'_i$의 값은 0에서 $2W-2$의 범위에 존재하지만 이 값을 만드는 경우의 수는 다름을 알 수 있다. 구체적인 예로서 $w=2$일 때 $r'_i+\hat{d}'_i$는 0에서 6까지 7가지의 값을 가지지만 이 7가지의 결과를 갖는 빈도는 서로 차이가 있다. 이를 자세히 기술한 것이 Fig. 2이다.

그림에서 보는 바와 같이 $r'_i+\hat{d}'_i$가 발생할 수 있는 경우는 모두 16가지이고 결과 값은 모두 7가지이다. 이 중에서 하나의 덧셈 결과가 가장 많이 발생하는 것은 두 지수 값의 합이 3이 되는 경우로서 모두 4가지 경우이다(그림에서 회색 부분). 그리고 두 지수 값의 합이 2인 경우와 4인 경우가 동일한데 각각 3가지 경우이다. 그리고 두 지수 값의 합이 0이 되거나 6이 되는 경우는 각각 1번 정도로서 발생 빈도가 가장 낮다.

따라서 Fig. 1의 단계 6.2에서 수행되는 사전 계산 테이블과의 곱셈은 동일한 확률로 충돌을 발생시키는 것이 아니라 충돌이 많이 발생하는 경우도 있으며 적게 발생하는 경우도 발생하게 된다. 다시 말해서 단계 6.2는 모두 28종류의 곱셈이 이루어지지만

r'_i	0	0	0	0
$\hat{d}'_i$	0	1	2	3
$r'_i+\hat{d}'_i$	0	1	2	3

r'_i	1	1	1	1
$\hat{d}'_i$	0	1	2	3
$r'_i+\hat{d}'_i$	1	2	3	4

r'_i	2	2	2	2
$\hat{d}'_i$	0	1	2	3
$r'_i+\hat{d}'_i$	2	3	4	5

r'_i	3	3	3	3
$\hat{d}'_i$	0	1	2	3
$r'_i+\hat{d}'_i$	3	4	5	6

(a) Addition of two exponents

$r'_i+\hat{d}'_i$	0	1	2	3	4	5	6
Number of occurrence	1	2	3	4	3	2	1
Group	D	C	B	A	B	C	D

(b) Number of occurrence

Fig. 2. The number of occurrence for addition of two exponents

가장 충돌이 많이 일어나는 경우는 $r'_i+\hat{d}'_i$가 3이 되는 경우로서 모두 4가지 경우(ϕ'_{i-1}가 4종류 이므로)가 된다.

따라서 공격자는 단계 6.2에서 가장 많은 충돌 쌍을 나타내는 4가지를 그룹 A로 묶고 $r'_i+\hat{d}'_i$가 3이라고 가정한다. 동일한 방법으로 그 다음 충돌 쌍이 많은 8가지를 그룹 B로 묶고 $r'_i+\hat{d}'_i$은 2 혹은 4라고 가정한다. 그리고 그 다음 충돌 빈도수를 가지는 8가지를 다시 묶어 그룹 C라 하고 $r'_i+\hat{d}'_i$은 1 혹은 5라고 가정한다. 마지막으로 충돌 빈도수가 가장 적은 8가지를 그룹 D로 묶어 $r'_i+\hat{d}'_i$가 0이나 6이라고 가정하고 비밀 지수 값을 분석한다.

실제로 1024비트에 지수에 대해 $w=2$인 경우를 가정하여 1,000번을 시뮬레이션 분석을 해 본 결과, Table 2와 같이 512개의 $r'_i+\hat{d}'_i$ 값 중에서 가장

많은 빈도수를 나타내는 그룹 A에서 약 128개씩, 그 다음 빈도수는 그룹 B에서 약 96개씩, 그룹 C에서는 약 64개씩, 그룹 D에서는 약 32개씩의 발생 빈도수를 나타내었다. 따라서 그룹 A에 속하는 4개의 값은 각각 평균 128/4=32번 나타나며 그룹 B에 속하는 8개의 값은 각각 192/8=24번, 그룹 C에 속하는 8개의 값은 각각 128/8=16번 그룹 D에 속하는 8개의 값은 각각 64/8=8번씩 나타나게 된다.

본 논문에서 충돌 분석 공격이 성공하기 위한 중요한 요소는 수집된 전력 파형을 각 그룹으로 어떻게 잘 분류하는가 하는 문제이다. 즉, 한 번의 멱승 연산 시 수집된 전력 소비 파형을 곱셈 단위로 분리한 후 각 곱셈 파형간의 충돌 기준을 정하고 유사한 파형을 가장 많이 나타내는(약 32개 정도씩) 4가지 경우를 묶어 그룹 A로 가정한다. 또, 비슷한 방법으로 순차적으로 높은 유사도를 나타내는(약 24개 정도씩) 8개의 경우를 묶어 그룹 B로 가정하는 방식을 순차적으로 적용하여 모든 그룹을 분류한다.

그러나 전력 파형을 여러 그룹 분류하는 것이 각 파형의 충돌성이 잘 드러나는 디바이스인 경우에는 큰 문제가 되지 않지만 분류가 잘못되었을 경우에는 비밀 키를 제대로 추출할 수 없다. 즉, 공격 대상 디바이스의 물리적인 특성, 곱셈 세그먼트간의 충돌 기준, 파형 수집 장비 및 실험 환경 등에 의해 그룹 분류 오류가 발생할 가능성은 내재되어 있다. 곱셈 세그먼트 그룹이 정확하게 분류되었는지의 최종 판단은 후보 키 탐색 과정을 거친 후 도출된 비밀 키를 검증하는 과정에서 결정하게 된다.

따라서 충돌 분석 공격은 단지 한 개의 전력 파형만 이용하지만 각 곱셈 파형의 그룹 분류가 정확히 이루어지기 위해서는 여러 실험 과정을 통해 충돌 판단 기준을 조정하는 것과 같은 추가 작업이 필요할 수 있다.

Table 2. Simulation on additional result for two exponents($t=1024$, $w=2$)

Group	$r'_i+\hat{d}'_i$	Number of occurrence (avg.)	Percentage
A	3	128.0	25.0
B	2	95.9	18.7
	4	95.8	18.7
C	1	64.1	12.5
	5	63.8	12.5
D	0	32.4	6.3
	6	32.0	6.3

이러한 물리적 공격 요건으로 인해 논문 [7]에서는 충돌 분석 공격의 계산 복잡도를 정의함에 있어 수집된 전력 파형에 대한 그룹 분류를 마친 것을 전제로 키 예상되는 후보의 개수에 기반하여 계산 복잡도를 산출하였다. 본 논문에서는 원 논문과 동일 조건하에서의 비교를 위해 전력 파형의 분류 오류로부터 발생할 수 있는 비용은 계산 복잡도에 포함시키지 않았다. 즉, 본 논문에서의 계산 복잡도는 충돌 분석에 의해 멱승 연산에 사용된 28개의 사전 계산 테이블 값을 4개의 그룹 A, B, C, D로 정확히 분류하였다는 가정하에 산출되었다.

[정리 1] (충돌 분석 공격 복잡도) 윈도우 기법을 적용한 메시지 블라인딩과 지수 분할 기법을 혼합한 멱승 알고리듬에 대한 충돌 분석 공격의 복잡도는 윈도우 크기가 w일 때 최대 $W!\times(2W!)^{W-1}\times 2W$ 이다.

[증명] 모든 가능한 사전 계산 값이 단계 6.2에서 사용되지만 각각의 사전 계산 테이블을 곱하는 빈도수는 지수 값 $r'_i+\hat{d}'_i$ 에 따라 달라진다. 공격을 위해서는 먼저 가장 많은 충돌 빈도를 나타내는 W가지는 그룹 A에, 그 다음 충돌 빈도를 나타내는 $2W$가지는 그룹 B에, 다음 충돌 빈도를 나타내는 $2W$가지는 그룹 C에 분류하는 방식으로 충돌 쌍을 분류한다. 이때 그룹 A는 $W!$가지, 그리고 그룹 B, C 등과 같이 모두 $(W-1)$개의 그룹은 $2W!$개의 경우의 수가 발생한다. 그리고 단계 7에서는 가정한 충돌 그룹을 알 수 있으므로 그룹 내에서 최대 $2W$개의 경우의 수를 가지게 된다. 따라서 이 멱승 알고리듬에 대한 충돌 분석 공격 복잡도는 $W!\times(2W!)^{W-1}\times 2W$ 가 된다. □

기존의 방식들과 $w=2$인 경우를 가정하여 계산 복잡도를 계산해 보자. 논문 [7]에서 저자들은 지수 분할 기법을 적용하지 않았을 경우에는 2^{44}이었던 것을 지수 분할 방법을 적용하면 복잡도가 2^{98}으로 크게 향상된다고 하였다. 그러나 본 논문에서 재분석한 결과, 이 알고리듬은 약 2^{53}정도의 공격 복잡도를 가짐을 확인하였다. 따라서 윈도우 기법에 기반하여 메시지 블라인딩과 지수 분할 기법을 사용한 멱승에서는 사전 계산 테이블이 15개에서 28개로 두 배 정도

증가하는 반면 공격 복잡도는 2^{44}에서 2^{53}로 증가함을 알 수 있다.

본 논문에서 분석한 바와 같이 지수 분할 기법은 분할된 두 랜덤 지수를 독립적으로 사용하지 않으면 DPA 공격뿐만 아니라 충돌 분석 공격에도 취약한 특성을 갖는다. 그 이유는 두 랜덤 지수를 동시에 이용하는 것이 다시 결합하는 효과로 나타나고 이것이 분리 특성을 감쇄시키는 결과로 작용하게 되기 때문이다. 특히, 본 논문에서와 사전 계산 테이블을 이용하는 경우에는 두 랜덤 지수를 결합한 결과 값이 곱셈 연산의 발생 빈도수와 관련성을 가지고 있다는 점이 비밀 키를 누설할 수 있는 새로운 부채널 정보로 이용된다.

IV. 결 론

본 논문에서는 최근에 제안된 지수 분할과 블라인딩 기법을 혼합한 윈도우 기반 RSA 멱승 알고리듬에 대해 충돌 전력 분석 공격에 대한 안전성을 분석하였다. 분석 결과, 지수 분할 기법은 멱승 연산 시 나누어진 지수를 다시 합하는 과정에서 발생하는 덧셈 결과의 빈도수가 새로운 전력 분석을 위한 누설 정보가 되기 때문에 원 논문에서 주장하는 것과 같이 높은 안전성을 제공하기는 어렵다. 따라서 스마트카드와 같은 임베디드 장치에 RSA 알고리듬을 구현할 경우에는 충돌 전력 분석 공격에 충분히 대응할 수 있는지에 대해 심층적인 고려가 필요하다.

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] P. Kocher, J. Jae, and B. Jun, "Differential power analysis," CRYPTO'99, LNCS 1666, pp. 388-397, 1999.

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

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

[5] P. Fouque and F. Valette, "The doubling attack- why upwards is better than downwards," CHES'03, LNCS 2779, pp. 269-280, 2003.

[6] M. Witteman, J. Woudenberg, and F. Menarini, "Defeating RSA Multiply-Always and Message Blinding Countermeasures," CT- RSA'11, LNCS 6558, pp. 77-88, 2011.

[7] B. Sim, Y. Won and D. Han, "Study for improving attack complexity against RSA collision analysis," Journal of The Korea Institute of Information Security & Cryptology(JKIISC), Vol. 25, No. 2, pp. 261-270, 2015.

[8] H. Kim, D. Han, S. Hong, J. Ha, "Message blinding method requiring on multiplicative inversion for RSA," ACM Trans. on Embedded Computing Systems, Vol. 9, No. 4, article 39, Mar. 2011.

[9] R. Rivest, A Shamir, and L, Adelman, "A method for obtaining digital signature and public-key cryptosystems," Comm. of the ACM 21, pp. 120-126, 1978.

[10] C. Clavier and M. Joye, "Universal exponentiation algorithm - A first step towards provable SPA-Resistance," CHES'01, LNCS 2162, pp.300-308, 2001

[11] J. Solinas, "Low-weight binary representations for pairs of integers," Technical report CORR 2001-41, CACR, University of Waterloo, 2001.

[12] H. Kim, Y, Baek, S. Kim, and D. Won, "Power attack against an exponent blinding method," Proceedings of Conference on Information Security and Cryptology-Summer(CISC-S'06), Vol. 16, No. 1, pp. 164-168, 2006.

〈저자소개〉

하 재 철 (Jaecheol Ha) 종신회원
1989년 2월: 경북대학교 전자공학과 졸업
1993년 2월: 경북대학교 전자공학과 석사
1998년 2월: 경북대학교 전자공학과 박사
1998년 3월~2007년 2월: 나사렛대학교 정보통신학과 부교수
2007년 3월~현재: 호서대학교 컴퓨터정보공학부 정보보호전공 교수
1991년 1월~현재: 한국정보보호학회 부회장
2009년 1월~현재: 한국산학기술학회 이사
〈관심분야〉 암호 알고리듬, 네트워크 보안, 부채널 공격