Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.2, Apr. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.2.261

RSA 충돌 분석 공격 복잡도 향상을 위한 연구*

심 보 연,† 원 유 승, 한 동 국‡
국민대학교

Study for improving attack Complexity against RSA Collision Analysis*

Bo-Youn Sim,† Yoo-Seung Won, Dong-Guk Han‡
Kookmin University

요 약

스마트카드와 같은 정보보호 디바이스에서 데이터를 보호하기 위해 사용되는 RSA 암호 알고리즘은 부채널 분석에 취약함이 밝혀졌다. 특히 암호 알고리즘이 수행되는 동안 소비되는 전력 패턴을 관찰하여 분석에 활용하는 전력 분석 공격에 취약하다. 전력 분석 공격은 대표적으로 단순 전력 분석과 차분 전력 분석이 있고, 이 외 충돌 분석 등이 있다. 그 중에서 충돌 분석은 단순 전력 분석 및 차분 전력 분석에 안전하게 설계된 RSA 암호 알고리즘이라도 단일 파형을 이용하여 비밀 키 값을 찾을 수 있는 매우 강력한 공격기법이다. 따라서 기존 메시지 블라인딩 기법에 윈도우 기법을 적용한 대응기법이 고려되었지만, 이는 윈도우 크기가 작은 환경에서 충분히 큰 안전도를 제공하지 못한다. 이에 본 논문에서는 메시지 블라인딩 기법과 윈도우 기법이 적용된 RSA 암호 알고리즘에 지수 분할 기법을 혼합 적용하여 충돌 분석에 더 높은 안전도를 제공하는 대응기법을 제시한다. 실험을 통해 본 논문에서 제시하는 대응기법이 윈도우 크기가 작은 환경에서 메시지 블라인딩 기법과 윈도우 기법만 적용된 기존 RSA 암호 알고리즘 보다 공격 복잡도가 약 124% 향상되어 더 높은 안전도를 제공함을 보였다.

ABSTRACT

In information security devices, such as Smart Cards, vulnerabilities of the RSA algorithm which is used to protect the data were found in the Side Channel Analysis. The RSA is especially vulnerable to Power Analysis which uses power consumption when the algorithm is working. Typically Power Analysis is divided into SPA(Simple Power Analysis) and DPA(Differential Power Analysis). On top of this, there is a CA(Collision Analysis) which is a very powerful attack. CA makes it possible to attack using a single waveform, even if the algorithm is designed to secure against SPA and DPA. So Message blinding, which applies the window method, was considered as a countermeasure. But, this method does not provide sufficient safety when the window size is small. Therefore, in this paper, we propose a new countermeasure that provides higher safety against CA. Our countermeasure is a combination of message and exponent blinding which is applied to the window method. In addition, through experiments, we have shown that our countermeasure provides approximately 124% higher attack complexity when the window size is small. Thus it can provide higher safety against CA.

Keywords: RSA, Side Channel Analysis, Collision Analysis, Countermeasure, Message Blinding, Exponent Blinding

접수일(2015년 1월 9일), 수정일(2015년 3월 12일), 게재확정일(2015년 3월 13일)

* 본 연구는 2014년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(NRF-2013R1A1A2A10062137).

† 주저자, qjdusls@kookmin.ac.kr
‡ 교신저자, christa@kookmin.ac.kr(Corresponding author)

I. 서 론

스마트카드와 같은 임베디드 장치를 사용하여 데이터를 암·복호화 하거나 디지털 서명을 수행하는 경우, RSA와 같은 수학적으로 안전성이 증명된 암호 알고리즘을 사용한다. 그러나 수학적으로 안전한 것으로 알려진 암호 알고리즘이라도, 구현 단계에서 고려되지 못한 부가적인 정보의 누출을 이용한 공격에 취약함이 밝혀졌다. 부가적인 정보로는 스마트카드와 같은 정보보호 디바이스가 동작하는 동안 발생하는 전력 소비량이나 전자기파 등이 있다. 이러한 정보를 활용하여 디바이스 내부에 저장된 비밀 키를 찾아내는 공격 기법을 부채널 분석이라고 하며, 1996년 Paul Kocher[4]가 최초로 제안하였다.

부채널 분석으로는 시간 공격[1], 오류주입 공격[2], 전자기 분석 공격[3], 전력 분석 공격[5] 등이 있으며, 그 중 전력 분석 공격은 가장 강력한 공격 기법으로 알려져 있다. 전력 분석 공격은 암호 알고리즘이 수행되는 동안 소비되는 전력 패턴을 관찰하여 분석에 활용하는 공격 기법으로, 대표적으로 단순 전력 분석과 차분 전력 분석으로 나누어진다. 이 외에도 알고리즘 연산 과정에서 발생하는 정보의 충돌 존재 여부를 전력 소모량을 통해 관측하여 비밀 키를 찾는 충돌 분석 등이 있다.

충돌 분석[6][7][8][9][10][11]은 단순 전력 분석 및 차분 전력 분석에 안전하도록 설계된 암호 알고리즘일지라도 단일 파형을 이용하여 비밀 키 값을 찾을 수 있는 매우 강력한 공격 기법이다. 따라서 충돌 분석에 안전한 대응기법 설계에 대한 연구가 활발히 이루어져 왔다. 그리하여 RSA 암호 알고리즘의 경우 기존 메시지 블라인딩 기법[12]에 윈도우 기법을 적용하여 전력 충돌 공격 복잡도를 향상시키는 대응기법을 고려해왔다. 하지만 이는 윈도우 크기가 작은 환경에서 충분히 큰 공격 복잡도를 제공하지 못한다. 이에 본 논문에서는 기존 메시지 블라인딩 기법[12]과 윈도우 기법이 적용된 RSA 암호 알고리즘에 지수 분할 기법[13]을 혼합 적용하여 충돌 분석 공격 복잡도를 향상시키는 대응기법을 제시한다. 또한 실험을 통해 본 논문에서 제시하는 대응기법이 윈도우 크기가 작은 환경에서 기존 윈도우 기법이 적용된 메시지 블라인딩 알고리즘과 비교하여 공격 복잡도가 약 124% 향상되어 더 높은 안전도를 제공함을 보였다.

본 논문의 구성은 다음과 같다. 2장에서는 RSA 암호 알고리즘에 대한 대표적인 충돌 분석 공격을 설명한다. 3장에서는 기존 메시지 블라인딩 기법과 이에 윈도우 기법을 적용한 대응기법을 설명한다. 그리고 본 논문에서 수행하는 충돌 분석을 정의하고 공격 복잡도를 계산한다. 4장에서는 본 논문에서 제시하는 기존 메시지 블라인딩 기법과 윈도우 기법이 적용된 RSA 암호 알고리즘에 지수 분할 기법을 혼합 적용한 대응기법을 소개한다. 또한 실험을 통해 기존 RSA 부채널 분석 대응기법과의 차이점을 비교 설명한다. 마지막으로 5장에서 결론으로 본 논문을 마무리 한다.

II. 기존 RSA 충돌 분석 공격

본 장에서는 RSA 암호 알고리즘에 대한 대표 충돌 분석 공격인 더블링 공격(DA, Doubling Attack)을 설명한다. 더블링 공격은 두 개의 같은 데이터에 대하여 동일 연산을 수행할 때 발생하는 전력 소모량은 같지만 서로 다른 데이터에 대하여 동일 연산을 수행할 때 발생하는 전력소모량은 다르다는 가정을 기반으로 공격을 수행한다.

Table 1. Squaring and Multiply Always Algorithm

Input	$M, d=(d_{t-1}d_{t-2}\cdots d_0)_2, N$
Output	$S=M^d \bmod N$
1. $S=1$ 2. For $(i=t-1; i\geq 0; i--)$ 2.1 $S_0=S^2 \bmod N$ 2.2 $S_1=S_0\times M \bmod N$ 2.3 $S=S_{d_i}$ 3. Return S	

Table 2. Compute input Message M, M^2

k	d_{n-k}	M	S_{d_i}	M^2	S_{d_i}
1	1	$(M^0)^2$		$(M^0)^2$	
		$M^0\times M$	M	$M^0\times M^2$	M^2
2	0	$(M)^2$		$(M^2)^2$	
		$M^2\times M$	M^2	$M^4\times M^2$	M^4
3	0	$(M^2)^2$		$(M^4)^2$	
		$M^4\times M$	M^4	$M^8\times M^2$	M^8
4	1	$(M^4)^2$		$(M^8)^2$	
		$M^8\times M$	M^9	$M^{16}\times M^2$	M^{18}

Table 1. 알고리즘에 선택 평문 M과 M^2을 입력하면 Table 2.와 같이 $d_i=0$ 일 때 중간 값의 충돌이 발생한다. 따라서 M에 대한 $k+1$번째 연산 파형과 M^2에 대한 k번째 연산 파형을 비교하여 충돌이 발생하면 $d_{n-k}=0$, 발생하지 않으면 $d_{n-k}=1$ $(1 \le k \le n-1)$임을 통해 비밀 키를 찾는다.

III. 기존 RSA 부채널 분석 대응기법 및 충돌 분석 공격 복잡도 계산

본 장에서는 기존 RSA 부채널 분석 대응기법으로 역원 연산이 필요 없는 메시지 블라인딩 기법[12]과 이에 윈도우 기법을 적용한 알고리즘을 소개한다. 그리고 본 논문에서 다루는 충돌 분석과 공격 복잡도를 정의하고 각 알고리즘의 충돌 분석 공격 복잡도를 계산한다. 또한 본 논문에서 기존 RSA 부채널 분석 대응기법에 혼합 적용하는 지수 분할 기법[13]을 소개한다. 본 논문에서는 아래 Table 3.과 같은 기호들이 사용된다.

Table 3. Notations

Notation	Description
N	Modulus
d	Secret Key
t	Bit length of Secret Key d
$\phi(N)$	The positive integers less than or equal to N that are relatively prime to N
M	Message
v	Random value for address randomization
R	Random value for Message Blinding
r	Random value for Exponent Blinding
w	Window size
W	2^w
k	$\lceil t/w \rceil$
S	Signature

3.1 역원 연산이 필요 없는 메시지 블라인딩 기법

[12]에서 제안된 메시지 블라인딩 기법은 알고리즘이 실행될 때마다 랜덤 값으로 메시지 M을 감춰 공격자가 예상한 중간 값에 독립적인 전력 소비가 발생하게 하여 차분 전력 분석에 안전하도록 설계하는 방법이다. 기존의 RSA 암호 알고리즘의 지수승 연산 $S=M^d \bmod N$ 처럼 수행되는 것과 달리 메시지 블라인딩 기법을 적용한 지수승 연산은 랜덤 값 R과 $\phi(N)$ 값을 활용하여 $S=M^d R^{2\phi(N)} \bmod N$ 과 같이 수행된다. 단순 전력 분석에도 안전하게 설계하기 위해 비트 표현을 {0,1} 에서 {1,2} 로 바꿔 표현하는 리코딩 기법이 지수 $2\phi(N)$에 적용되어 있으며, 아래 식 (1)을 기반으로 구성된 방법이다.

$$2^{t-1}=(2^{t-2}+2^{t-3}+\cdots+2^0)+1 \quad (1)$$

위 식 (1)에 따라서 $\phi(N)=(\phi_{t-1}\phi_{t-2}\cdots\phi_0)_2$, $\phi_{t-1}=1$ 이고, $\tilde{\phi}_i=\phi_i+1\in\{1,2\}$ 일 때 식 (2)가 성립한다.

$$2\phi(N)=\sum_{i=1}^{t}\phi_{i-1}2^i=\left\{\sum_{i=1}^{t-1}\tilde{\phi}_{i-1}2^i+1\right\}+1$$
$$=\sum_{i=1}^{t-1}\tilde{\phi}_{i-1}2^i+2=(\tilde{\phi}_{t-2}\tilde{\phi}_{t-3}\cdots\tilde{\phi}_0 2)_2 \quad (2)$$

식 (2)를 기반으로 지수승 연산 수행 시 사전에 지수 $2\phi(N)$에 대한 리코딩 작업을 수행할 필요가 없다. Table 4.와 같이 사전에 지수 비트 d_i와 ϕ_{i-1}에 따라 연산해 놓은 값을 불러와 사용함으로써, 지수승 연산과 동시에 리코딩 기법을 적용할 수 있는 효율적인 기법이다.

따라서 두 비밀 지수 $d=(d_{t-1}d_{t-2}\cdots d_0)_2$ 의 i번째 비트 d_i와 $\phi(N)=(\phi_{t-1}\phi_{t-2}\cdots\phi_0)_2$ 의 $i-1$번째 비트 ϕ_{i-1}를 동시에 스캐닝 하여 비트에 따라 Table 4.와 같이 사전에 연산한, 랜덤 값 R로 블라인딩 되어 있는 메시지 $M^{d_i}R^{\tilde{\phi}_{i-1}}$ 를 곱한다. 이 메

Table 4. Pre-computation for Message Blinding

d_i	ϕ_{i-1}	$\tilde{\phi}_{i-1}$	Pre-computation value
0	0	1	R
0	1	2	R^2
1	0	1	MR
1	1	2	MR^2

시지 블라인딩 알고리즘은 식 (3)과 같이 오일러 정리에 따라 올바른 서명 값을 반환한다. 따라서 추가적인 역원 연산 없이 올바른 서명 값을 얻을 수 있는 메시지 블라인딩 기법이며, Table 5.와 같이 연산을 수행한다.

$$S = M^d R^{2\phi(N)} \bmod N = M^d \bmod N \quad (3)$$

역원 연산이 필요 없는 메시지 블라인딩 기법이 적용된 알고리즘의 경우 사전 연산 값 $M^{d_i} R^{\tilde{\phi}_{i-1}}$의 개수는 d_i와 ϕ_{i-1}이 각각 두 가지씩 존재하기 때문에 $n_1 = 4$ 개 이다.

Table 5. Message Blinding Algorithm

Input	$M, d = (d_{t-1} d_{t-2} \cdots d_0)_2, \phi(N), N$
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 $R \in \{1, 2, \cdots, N-1\}$, $v \in \{0, 1, 2, 3\}$ 4. Pre-computation $S = 1, S_v = R, S_{v\oplus 1} = R^2, S_{v\oplus 2} = MR, S_{v\oplus 3} = MR^2$ 5. For $(i = t-1; i \geq 1; i--)$ 5.1 $S = S^2 \bmod N$ 5.2 $S = S \times S_{v\oplus(2d_i + \phi_{i-1})} \bmod N$ 6. Return $S^2 \times S_{v\oplus(2d_0+1)} \bmod N$	

3.2 역원 연산이 필요 없는 메시지 블라인딩 알고리즘에 대한 충돌 분석 공격 복잡도 계산

본 절에서는 역원 연산이 필요 없는 메시지 블라인딩 알고리즘의 충돌 분석 공격 복잡도를 계산한다. 본 논문에서 충돌 분석은 동일 연산에 대한 입력 데이터가 같을 경우 전력 파형의 충돌이 발생하며, 이를 공격자가 구분 가능하다는 가정을 기반으로 한다.

그리고 본 논문에서는 지수승 연산 시 사전 연산 값을 불러와 곱하는 연산 파형에 대한 충돌 분석을 고려한다. 각 곱셈 연산 파형의 충돌 여부는 상관도를 통해 확인한다. 동일한 사전 연산 값이 사용될 경우 전력 파형의 충돌이 발생하기 때문에 이를 통해 각 사전 연산 값에 대한 집합으로 파형을 분류할 수 있다. 따라서 동일한 사전 연산 값에 대한 곱셈 파형으로 분류된 집합들의 비밀 지수를 각각 추측하여 평문-암호문 검증을 통해 올바른 비밀 키 값을 찾는다. 이 때 검증해야 하는 후보 키의 개수를 본 논문에서는 공격 복잡도로 정의한다.

[12]에서 제안된 역원 연산이 필요 없는 메시지 블라인딩 알고리즘에 대한 충돌 분석은 Table 5.에서 사전 연산 값을 사용하는 5.2단계와 6단계의 곱셈 연산 파형을 대상으로 수행한다. 그 결과 충돌 분석 공격 복잡도는 아래 정리 1.과 같다.

정리 1. [충돌 분석 공격 복잡도 정리 1] 모든 가능한 사전 연산 값이 사용될 경우 역원 연산이 필요 없는 메시지 블라인딩 알고리즘에 대한 충돌 분석 공격 복잡도는 12이다.

증명. 모든 가능한 사전 연산 값이 사용되었기 때문에 6단계와 5.2단계의 곱셈 연산 파형은 4개의 집합으로 분류된다. 이 때 6단계 곱셈 연산 파형이 속한 집합은 d_0에 따라 사용되는 사전 연산 값이 결정된다. 즉, $\phi_{t-1} = 1$이기 때문에 $d_0 = 0$ 일 때 R^2, $d_0 = 1$ 일 때 MR^2 에 대한 곱셈 연산 파형이다.

따라서 충돌 분석 수행 시 6단계 곱셈 연산 파형이 속한 집합의 사전 연산 값은 두 가지 경우의 수가 존재한다. 그리고 나머지 3개의 각 집합의 사전 연산 값을 추측할 때, 총 3! 가지 경우의 수가 존재한다. 그 결과 모든 가능한 사전 연산 값이 사용될 경우 d와 $\phi(N)$의 후보군의 개수는 각 집합의 사전 연산 값의 경우의 수에 따라 $2 \times 3! = 12$ 개다. 즉 충돌 분석 공격 복잡도는 12이다. □

3.3 역원 연산이 필요 없는 메시지 블라인딩 기법에 윈도우 기법의 적용

역원 연산이 필요 없는 메시지 블라인딩 기법[12]에 윈도우 기법을 적용하면 전력 충돌 분석 공격 복잡도를 향상시킬 수 있다. 따라서 전력 충돌 분석 대응 기법으로의 적용이 고려되어 왔다. 지수승 연산은 윈도우 크기가 w 일 때 $S = M^d R^{W\phi(N)} \bmod N$ 과 같이 수행된다. 단순 전력 분석에도 안전하게 설계하기 위해 비트 ϕ'_i 표현을 $\tilde{\phi}'_i$로 아래와 같이 바꿔 표현하는 리코딩 기법이 지수 $W\phi(N)$에 적용되어 있다.

$$\phi'_i \in \{0, 1, \cdots, W-1\}$$
$$\tilde{\phi}'_i \in \{\phi'_{k-1}(W-1), \phi'_{k-1}(W-1)+1, \cdots, \phi'_{k-1}(W-1)+(W-1)\}$$

아래 식 (4)를 기반으로 메시지 블라인딩 알고리즘에 윈도우 기법을 적용한다.

$$W^{k-1}=(W-1)\sum_{i=0}^{k-2}W^i+1 \tag{4}$$

위 식 (4)에 따라서 $\phi(N)=(\phi_{t-1}\phi_{t-2}\cdots\phi_0)_2$ $=(\phi'_{k-1}\phi'_{k-2}\cdots\phi'_0)_W$, $\phi'_{k-1}\neq 0$ 이고 다음 $\widetilde{\phi'}_i=\phi'_{k-1}(W-1)+\phi'_i$ 을 만족할 때 식 (5)가 성립한다.

$$\begin{aligned}W\phi(N)&=\sum_{i=1}^{k}\phi'_{i-1}W^i\\&=\phi'_{k-1}\left\{(W-1)\sum_{i=1}^{k-1}W^i+W\right\}+\sum_{i=1}^{k-1}\phi'_{i-1}W^i\\&=\sum_{i=1}^{k-1}\{\phi'_{k-1}(W-1)+\phi'_{i-1}\}W^i+W\phi'_{k-1}\\&=\sum_{i=1}^{k-1}\widetilde{\phi'}_{i-1}W^i+W\phi'_{k-1}\end{aligned} \tag{5}$$

식 (5)를 기반으로 지수승 연산 수행 시 사전에 지수 $W\phi(N)$ 에 대한 리코딩 작업을 수행할 필요가 없다. Table 6.과 같이 사전에 d'_i와 ϕ'_{i-1}에 따라 연산해 놓은 값을 불러와 사용함으로써, 지수승 연산과 동시에 리코딩 기법을 적용할 수 있는 효율적인 기법이다.

따라서 두 비밀 지수 d와 $\phi(N)$ 각각 w 개의 비트씩 동시에 스캐닝한 값 d'_i와 ϕ'_{i-1}에 따라 Table 6.과 같이 사전에 연산한, 랜덤 값 R로 블라인딩 되어있는 메시지 $M^{d'_i}R^{\widetilde{\phi}'_{i-1}}$ 을 곱한다. 비밀 지수 $d=(d_{t-1}d_{t-2}\cdots d_0)_2=(d'_{k-1}d'_{k-2}\cdots d'_0)_W$ 이며 w개의 비트 값 $d'_i=(d_{wi+w-1}d_{wi+w-2}\cdots d_{wi})_2$ 이다. 이와 유사하게 $\phi(N)=(\phi_{t-1}\phi_{t-2}\cdots\phi_0)_2=(\phi'_{k-1}\phi'_{k-2}\cdots\phi'_0)_W$ 이고 w개의 비트 값 $\phi'_{i-1}=(\phi_{wi-1}\phi_{wi-2}\ \phi_{w(i-1)})_2$이다. 윈도우 기법을 적용한 메시지 블라인딩 알고리즘은 Table 7.과 같이 연산을 수행한다.

윈도우 기법을 적용한 메시지 블라인딩 알고리즘의 경우 사전 연산 값 $M^{d'_i}R^{\widetilde{\phi}'_{i-1}}$ 개수는 d'_i와 ϕ'_{i-1}이 각각 W 가지씩 존재하기 때문에 $n_2=W^2$ 개 이며, 윈도우 크기 w에 따라 변한다.

Table 6. Pre-computation for Message Blinding with Window Method ($w=2, \phi'_{k-1}=1$)

d'_i	ϕ'_{i-1}	$\widetilde{\phi}'_{i-1}$	Pre-computation value
0	0	3	R^3
0	1	4	R^4
0	2	5	R^5
0	3	6	R^6
1	0	3	MR^3
⋮	⋮	⋮	⋮
3	2	5	M^3R^5
3	3	6	M^3R^6

3.4 역원 연산이 필요 없는 메시지 블라인딩 기법과 윈도우 기법을 적용한 알고리즘에 대한 충돌 분석 공격 복잡도 계산

본 절에서는 2.2절과 동일한 가정을 기반으로 역원 연산이 필요 없는 메시지 블라인딩 기법과 윈도우 기법을 적용한 알고리즘에 대한 충돌 분석 공격 복잡도를 계산한다. Table 7.에서 사전 연산 값을 사용하는 5.2단계와 6단계의 곱셈 연산 파형을 대상으로 충돌 분석을 수행한다. 그 결과 Table 7.의 Algorithm 1에 대한 충돌 분석 공격 복잡도는 아

Table 7. Message Blinding with Window Method (Algorithm 1)

Input	$M, d=(d_{t-1}d_{t-2}\cdots d_0)_2, \phi(N), N$
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 $R\in\{1,2,\cdots,N-1\}$, $v\in\{0,1,\cdots,W^2-1\}$ 4. Pre-computation 4.1 For $(i=0;i<W;i++)$ 4.1.1 $S_{v\oplus i}=R^{\phi'_{k-1}(W-1)+i} \bmod N$ 4.2 For $(i=0;i<W^2;i+=W)$ 4.2.1 For $(j=0;j<W;j++)$ 4.2.1.1 $S_{v\oplus(i+j+W)}=S_{v\oplus(i+j)}\times M \bmod N$ 5. For $(i=k-1;i\geq 1;i--)$ 5.1 $S=S^W \bmod N$ 5.2 $S=S\times S_{v\oplus(Wd'_i+\phi'_{i-1})} \bmod N$ 6. Return $S^W\times S_{v\oplus(Wd'_0+\phi'_{k-1})} \bmod N$	

래 정리 2.와 같다.

정리 2. [충돌 분석 공격 복잡도 정리 2] 모든 가능한 사전 연산 값이 사용될 경우 역원 연산이 필요 없는 메시지 블라인딩과 윈도우 기법이 적용된 알고리즘에 대한 충돌 분석 공격 복잡도는 윈도우 크기가 w일 때 $W\times(W-1)\times(n_2-1)!$이다.

증명. 모든 가능한 사전 연산 값이 사용되었기 때문에 6단계와 5.2단계의 곱셈 연산 파형은 $n_2 = W^2$개의 집합으로 분류된다. 이 때 6단계 곱셈 연산 파형이 속한 집합은 d'_0와 ϕ'_{k-1}에 따라 사용되는 사전 연산 값이 결정된다.

d'_0은 W가지, ϕ'_{k-1}은 $W-1$가지 존재하기 때문에 6단계 곱셈 연산 파형이 속한 집합의 사전 연산 값은 총 $W\times(W-1)$ 가지 경우의 수가 존재한다. 그리고 나머지 n_2-1개의 각 집합에 대한 사전 연산 값을 추측할 때, 총 $(n_2-1)!$가지 경우의 수가 존재한다.

그 결과 모든 가능한 사전 연산 값이 사용될 경우 d와 $\phi(N)$의 후보군의 개수는 각 집합의 사전 연산 값의 경우의 수에 따라 $W\times(W-1)\times(n_2-1)!$ 개다. 즉 충돌 분석 공격 복잡도는 $W\times(W-1)\times(n_2-1)!$이다. □

따라서 윈도우 크기 w가 커질수록 d와 $\phi(N)$ 의 후보군의 개수도 증가하여 충돌 분석 수행 시 공격 복잡도가 증가한다. 하지만 윈도우 크기 w가 2와 같이 작은 환경에서 공격 복잡도가 약 2^{44}(44비트)으로 충분히 큰 공격 복잡도를 제공하지 못한다.

3.5 지수 분할 기법

지수 분할 기법[13]은 랜덤 값 r을 이용하여 비밀 키 d를 감춰 공격자가 중간 값을 추측하지 못하도록 하는 대응기법이다. 매 암호 알고리즘 연산 시 새로운 랜덤 값 r을 생성하여 비밀 키 d를 감추기 때문에 차분 전력 분석에 안전하다. 지수 분할 기법은 비밀 키 d를 r과 $d-r$ 두 부분으로 나누어 $S = M^r M^{(d-r)} \bmod N$ 과 같이 지수승 연산을 수행한다. $M^r M^{(d-r)} \bmod N = M^d \bmod N$ 이기 때문에 지수승 연산 후 별도의 보정 연산이 필요 없다. 지수 분할 기법 적용 시 비밀 키 d의 상위 비트 노출 방지 및 공격 복잡도 향상을 위해 랜덤 값 r의 길이가 비밀 키 d의 길이와 같도록 생성하여 적용한다.

IV. 부채널 분석에 안전한 지수 분할 기법의 혼합 적용

기존 부채널 분석 대응기법은 단순 전력 분석 및 차분 전력 분석에 안전하지만, 충돌 분석에 취약하다. 충돌 분석은 단일 파형을 이용해 비밀 키 값을 찾을 수 있는 매우 강력한 기법이다. 따라서 충돌 분석에 안전한 대응기법 설계에 대한 연구가 활발히 이루어져 왔다. 그리하여 RSA 암호 알고리즘의 경우 기존 메시지 블라인딩 기법[12]과 윈도우 기법을 적용하여 충돌 분석 공격 복잡도를 향상시킨 대응기법이 고려되었다.

하지만 이는 윈도우 크기가 작은 환경에서 충분히 큰 공격 복잡도를 제공하지 못한다. 이에 본 논문에서는 기존 메시지 블라인딩 기법과 윈도우 기법이 적용된 RSA 암호 알고리즘에 지수 분할 기법[13]을 혼합 적용한 대응기법을 제안한다. 본 장에서 제안하는 대응기법은 충돌 분석 공격 복잡도를 향상시켜 더 높은 안전도를 제공한다.

4.1 기존 윈도우 기법을 적용한 메시지 블라인딩 알고리즘에 지수 분할 기법 적용

본 논문에서 제안하는 기존 메시지 블라인딩 기법[12]과 윈도우 기법이 적용된 RSA 암호 알고리즘에 지수 분할 기법[13]을 혼합 적용한 지수승 연산은 윈도우 크기가 w일 때 아래 식 (6)과 같이 수행된다.

$$S = M^r M^{(d-r)} R^{W\phi(N)} \bmod N \tag{6}$$

$M^r M^{(d-r)} R^{W\phi(N)} \bmod N = M^d \bmod N$ 이기 때문에 지수승 연산 후 별도의 보정 연산이 필요 없다. 윈도우 기법을 적용한 메시지 블라인딩과 지수 분할은 3.3에서와 같이 식 (4)와 식 (5)를 기반으로 구성된 방법이다. 또한 단순 전력 분석에도 안전하게 설계하기 위해 비트 ϕ'_i 표현을 $\tilde{\phi}'_i$ 로 3.3에서와 같이 바꿔 표현하는 리코딩 기법이 지수 $W\phi(N)$에 적용되어 있다. $\hat{d} = d-r$ 일 때 세 비밀 지수 $r, \hat{d}$ 그리고 $\phi(N)$은 아래와 같다.

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

식 (5)를 기반으로 지수승 연산 수행 시 사전에 지수 $W\phi(N)$에 대한 리코딩 작업을 수행할 필요가 없다. Table 8.과 같이 사전에 $r'_i, \hat{d}'_i$ 와 ϕ'_{i-1}에 따라 연산해 높은 값을 불러와 사용함으로써, 지수승 연산과 동시에 리코딩 기법을 적용할 수 있는 효율적인 기법이다. 따라서 세 비밀 지수 $r, \hat{d}$ 그리고 $\phi(N)$을 각각 w개의 비트씩 동시에 스캐닝한 값 $r'_i, \hat{d}'_i$ 그리고 ϕ'_{i-1}에 따라 Table 8.과 같이 사전에 연산한, 랜덤 값 R로 블라인딩 되어있는 메시지 $M^{r'_i+\hat{d}'_i}R^{\tilde{\phi}'_{i-1}}$ 을 곱한다.

윈도우 기법을 적용한 메시지 블라인딩 기법과 지수 분할 기법 혼합 알고리즘의 경우 사전 연산 값 $M^{r'_i+\hat{d}'_i}R^{\tilde{\phi}'_{i-1}}$ 의 개수는 $r'_i+\hat{d}'_i$와 ϕ'_{i-1} 값의 가지 수에 따라 결정된다. $r'_i+\hat{d}'_i$ 값의 범위는 아래와 같다.

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

따라서 $r'_i+\hat{d}'_i$ 가 $2W-1$ 가지, ϕ'_{i-1} 가 W 가지 존재하기 때문에 $n_3=2W^2-W$ 개 이며, 윈도우 크기 w에 따라 변한다. 윈도우 기법을 적용한 메시지 블라인딩 기법과 지수 분할 기법 혼합 알고리즘은 Table 9.와 같이 연산을 수행한다.

Table 8. Pre-computation for the Combination of Message Blinding and Exponent Splitting with Window Method ($w=2, \phi'_{k-1}=1$)

r'_i	$\hat{d}'_i$	ϕ'_{i-1}	$\tilde{\phi}'_{i-1}$	Pre-computation value
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
⋮	⋮	⋮	⋮	⋮
3	3	3	6	M^6R^6

Table 9. Combination of Message Blinding and Exponent Splitting with Window Method (Algorithm 2)

Input	$M, d=(d_{t-1}d_{t-2}\cdots d_0)_2, \phi(N), N$
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
   $R\in\{1,2,\cdots,N-1\}$, $v\in\{0,1,\cdots,2W^2-W-1\}$, $r(t\text{-length})$
4. Compute $\hat{d}=d-r$
5. Pre-computation
   5.1 For $(i=0; i<W; i++)$
      5.1.1 $S_{v\oplus i}=R^{\phi'_{k-1}(W-1)+i} \bmod N$
   5.2 For $(i=0; i<(2W^2-W); i+=W)$
      5.2.1 For $(j=0; j<W; j++)$
         5.2.1.1 $S_{v\oplus(i+j+W)}=S_{v\oplus(i+j)}\times M \bmod N$
6. For $(i=k-1; i\geq 1; i--)$
   6.1 $S=S^W \bmod N$
   6.2 $S=S\times S_{v\oplus(W(r'_i+\hat{d}'_i)+\phi'_{i-1})} \bmod N$
7. Return $S^W\times S_{v\oplus(W(r'_0+\hat{d}'_0)+\phi'_{k-1})} \bmod N$

4.2 윈도우 기법을 적용한 메시지 블라인딩과 지수 분할 기법 혼합 알고리즘에 대한 충돌 분석 공격 복잡도 계산

본 절에서는 3.2절과 동일한 가정을 기반으로 윈도우 기법을 적용한 메시지 블라인딩과 지수 분할 기법 혼합 알고리즘에 대한 충돌 분석 공격 복잡도를 계산한다. Table 9.에서 사전 연산 값을 사용하는 6.2단계와 7단계의 곱셈 연산 파형을 대상으로 충돌 분석을 수행한다. 그 결과 Table 9.의 Algorithm 2에 대한 충돌 분석 공격 복잡도는 아래 정리 3.과 같다.

정리 3. [충돌 분석 공격 복잡도 정리 3] 모든 가능한 사전 연산 값이 사용될 경우 윈도우 기법을 적용한 메시지 블라인딩 기법과 지수 분할 기법 혼합 알고리즘에 대한 충돌 분석 공격 복잡도는 윈도우 크기가 w일 때 $(2W-1)\ (W-1)\times(n_3-1)!$이다.

증명. 모든 가능한 사전 연산 값이 사용되었기 때문

에 7단계와 6.2단계의 곱셈 연산 파형은 모두 $n_3 = 2W^2 - W$ 개의 집합으로 분류된다. 이 때 7단계 곱셈 연산 파형이 속한 집합은 $r'_0 + \hat{d}'_0$와 ϕ'_{k-1}에 따라 사용되는 사전 연산 값이 결정된다.

$r'_0 + \hat{d}'_0$은 $2W-1$가지, ϕ'_{k-1}은 $W-1$가지 존재하기 때문에 7단계 곱셈 연산 파형이 속한 집합의 사전 연산 값은 총 $(2W-1)(W-1)$가지 경우의 수가 존재한다. 그리고 나머지 n_3-1개의 각 집합에 대한 사전 연산 값을 추측할 때, 총 $(n_3-1)!$가지 경우의 수가 존재한다. 그 결과 모든 가능한 사전 연산 값이 사용될 경우 d와 $\phi(N)$의 후보군의 개수는 각 집합의 사전 연산 값의 경우의 수에 따라 $(2W-1)(W-1)(n_3-1)!$ 개다. □

결과적으로 윈도우 크기 w가 커질수록 d와 $\phi(N)$의 후보군의 개수도 증가하여 충돌 분석 수행 시 공격 복잡도가 증가한다. 이는 기존 윈도우 기법을 적용한 메시지 블라인딩 알고리즘의 후보군의 개수 $W\times(W-1)\times(n_2-1)!$ 보다 더 많다. 그 이유는, 윈도우 기법을 적용한 메시지 블라인딩 알고리즘의 경우 하나의 비밀 지수 d의 비트 값에 따라 곱해지는 메시지 M의 횟수가 결정되는 것과 달리 본 논문에서 제시하는 알고리즘의 경우 분할된 두 비밀 지수 r과 $\hat{d}$의 비트 값의 합에 따라 곱해지는 메시지 M의 횟수가 결정되기 때문이다. 따라서 사전 연산 값의 개수가 증가하여 충돌 분석 수행 시 d와 $\phi(N)$의 후보군의 개수도 증가한다.

그러므로 본 논문에서 제시하는 윈도우 기법을 적용한 메시지 블라인딩 기법과 지수 분할 기법 혼합 알고리즘은 기존 윈도우 기법을 적용한 메시지 블라인딩 알고리즘 보다 충돌 분석에 더 높은 안전도를 제공한다.

4.3 비교 결과

본 논문에서는 Table 7.과 Table 9.같이 두 가지 종류로 구현된 RSA 암호 알고리즘을 CodeWarriror for ARM Development Suit을 이용하여 Table 10.과 같은 환경에서의 연산 속도 및 메모리를 측정하였다.

1024비트 RSA 연산에 대한 실험을 실시하였으며, 실험 비교 결과는 Table 11.과 같다. 이를 통해

Table 10. Test Board

	Processor	Clock
Target	ARM7TDMI	Real-Time

윈도우 크기가 3이하인 경우 Algorithm 1을 기준으로 Algorithm 2의 속도는 평균 1.02배로 거의 변화가 없음을 알 수 있다. 대응기법의 적용으로 인한 연산 오버헤드를 최소화하기 위해 Algorithm 3에서 지수 r과 $\hat{d}$에 대한 연산을 동시에 수행하기 때문에 속도가 두 배 이상 느려지지 않는다. 또한 사전 계산 값을 저장하기 위해 필요한 메모리가 Algorithm 1을 기준으로 Algorithm 2가 평균 1.12배로 증가함을 알 수 있다. 따라서 메모리 관점에서는 Algorithm 1이 Algorithm 2보다 좀 더 효율적이다.

하지만 윈도우 크기가 1일 때 Algorithm 1의 공격 복잡도는 약 4비트로 약 $2^4 = 16$ 개의 d와 $\phi(N)$의 후보군이 존재하고, Algorithm 2의 공격 복잡도는 약 9비트로 약 $2^9 = 512$ 개의 d와 $\phi(N)$의 후보군이 존재함을 통해 Algorithm 2가 약 125% 더 높은 공격 복잡도를 제공함을 알 수 있다. 또한 윈도우 크기가 2일 때는 알고리즘 1의 공격 복잡도가 약 44비트, 알고리즘 2의 공격 복잡도가 약 98비트로 약 123% 더 높은 공격 복잡도를 제공한다. 마찬가지로 윈도우 크기가 3일 때는 알고리즘 1의 공격 복잡도가 약 296비트, 알고리즘 2의 공격 복잡도가 661비트로 약 123% 더 높은 공격 복잡도를 제공한다. 결과적으로 알고리즘 2의 공격 복잡도가 알고리즘 1의 공격 복잡도보다 평균 124% 향상됨을 알 수 있다.

따라서 윈도우 크기가 1, 2, 3과 같이 작은 환경에서 Algorithm 2가 Algorithm 1보다 메모리 소모량은 높지만 유사한 속도로 충돌 분석에 더 높은 안전도를 제공함을 알 수 있다. 그러므로 만약 메모리를 어느 정도 감내할 수 있는 환경에서 RSA 암호

Table 11. Algorithm 1 and 2 test results

w	Speed ($\times 10^6$ Cycles)		Memory (KB)		Attack Complexity (bits)	
	1	2	1	2	1	2
1	249	256	0.64	0.66	4	9
2	184	194	0.71	0.77	44	98
3	169	178	0.89	1.13	296	661

알고리즘을 사용한다면, 적절한 윈도우 크기를 선택한 후 지수분할 기법을 혼합 적용하여 안전도를 향상시키는 방안을 고려해야 한다.

V. 결 론

본 논문에서는 충돌 분석에 더 높은 안전도를 제공하기 위해 기존 메시지 블라인딩 기법과 윈도우 기법이 적용된 RSA 암호 알고리즘에 지수 분할 기법을 혼합 적용하여 설계 및 구현한다. 그리고 실험을 통해 기존 윈도우 기법을 적용한 메시지 블라인딩 알고리즘과의 효율성 및 안전도를 비교 분석한다. 그 결과 윈도우 기법을 적용한 메시지 블라인딩 기법과 지수 분할 기법 혼합 알고리즘이 윈도우 크기가 작은 환경에서 윈도우 기법을 적용한 메시지 블라인딩 알고리즘 보다 메모리 소모량은 평균 1.12배로 증가하지만 유사한 속도로 충돌 분석 공격 복잡도가 평균 약 124% 향상됨을 보였다. 그러므로 만약 메모리를 어느 정도 감내할 수 있는 환경이라면 적절한 윈도우 크기를 선택한 후 지수 분할 기법을 혼합 적용하여 충돌 분석에 대한 안전도를 향상시키는 방안을 고려해야 한다.

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] D. Boneh, R. Demillo, and R. Lipton, "On the importance of checking cryptographic protocols for faults," EUROCRYPTO'97, LNCS 1233, pp. 37-51, 1997.

[3] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis : concrete results," CHES 2001, LNCS 2162, pp. 251-261, 2001.

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

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

[6] K. Okeya and K. Sakurai, "A second-order DPA attack breaks a window-method based countermeasure against side channel attacks," ISC 2002, LNCS 2433 pp. 389-401, 2002.

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

[8] N. Homma, A. Miyamoto, T. Aoki, A. Satoh, and A. Shamir, "Collision-based power analysis of modular exponentiation using chosen-message pairs," CHES 2008, LNCS 5154, pp. 15-29, 2008.

[9] HeeSeok Kim, Tae Hyun Kim, Joong Chul Yoon, and Seokhie Hong, "Practival second-order correlation power analysis on the message blinding method and its novel countermeasure for RSA," ETRI Journal, vol. 32, no. 1, pp. 102-111, Feb. 2010.

[10] M.F. Witteman, J.G.J. Woudenberg, and F. Menarini, "Defeating RSA multiply-always and message blinding countermeasures," CT-RSA 2011, LNCS 6558, pp. 77-88, 2011.

[11] T. Sugawara, D. Suzuki, M. Saeki, "Internal collision attack on RSA under closed EM measurement," SCIS 2014, pp. 1-8, Jan. 2014.

[12] HeeSeok Kim, Dong-Guk Han, Seokhie Hong, and JaeCheol Ha, "Message blinding method requiring no multiplicative inversion for RSA," ACM Transactions on Embedded Computing Systems, vol. 9, no. 4, article 39, Mar. 2011.

[13] C. Clavier and M. Joye, "Universal exponentiation algorithm a first step towards provable SPA-resistance," CHES 2001, LNCS 2162, pp. 300-308, 2001.

[14] RSA Laboratories, "PKCS #1 v2.2 : RSA cryptography standard," Oct. 2012.

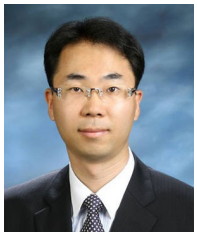
[15] Bo-Youn Sim, Yoo-Seung Won and

Dong-Guk Han, "Study on the combination of message and exponent blinding for countermeasure against RSA power collision analysis," CISC-S'14, pp. 119, Jun. 2014.

〈저자소개〉

심 보 연 (Bo-Youn Sim) 학생회원
2013년 2월: 국민대학교 수학과 학사
2015년 2월: 국민대학교 일반대학원 금융정보보안학과 석사
2015년 3월~현재: 국민대학교 일반대학원 수학과 박사과정
〈관심분야〉 공개키 암호 시스템, 부채널 분석 및 대응기법 설계, 경량·저전력 정보보호 기술

원 유 승 (Yoo-Seung Won) 학생회원
2012년 2월: 국민대학교 수학과 학사
2014년 2월: 국민대학교 일반대학원 수학과 석사
2014년 3월~현재: 국민대학교 일반대학원 금융정보보안학과 박사과정
〈관심분야〉 블록 암호 알고리즘, 경량 암호 알고리즘, 공개키 암호 알고리즘, 부채널 분석 및 대응기법 설계



한 동 국 (Dong-Guk Han) 종신회원
1999년 2월: 고려대학교 수학과 학사
2002년 2월: 고려대학교 수학과 석사
2005년 2월: 고려대학교 정보보호대학원 박사
2004년 4월~2005년 4월: 일본 Kyushu Univ. 방문연구원
2005년 4월~2006년 4월: 일본 Future Univ.-Hakodate Post.Doc.
2006년 6월~2009년 2월: 한국전자통신연구원 정보보호연구단 선임연구원
2009년 3월~현재: 국민대학교 수학과 부교수
〈관심분야〉 공개키 암호시스템 안전성 분석 및 고속 구현, 부채널 분석 및 대응법 설계, IoT 정보보호 기술