情報保護學會論文誌
第14券 第4號, 2004. 8

전력 분석 공격과 ID 기반 암호 시스템의 안전성*

양 연 형[a)†‡], 박 동 진[a)], 이 필 중[b)]
포항공과대학교[a)], 포항공과대학교/KT 기술연구소[b)]

On the Security of ID-Based Cryptosystem against Power Analysis Attacks*

Yeon Hyeong YANG[a)†‡], Dong Jin PARK[a)], Pil Joong LEE[b)]
POSTECH[a)], POSTECH/KT Research Center[b)]

요 약

ID 기반 암호 시스템과 전력 분석 공격(Power Analysis Attack)은 모두 각각의 분야에서 활발한 연구가 진행되는 주제이다. 특히 DPA(Differential Power Analysis) 공격[2]은 스마트카드와 같은 저전력 장치에 대한 가장 강력한 공격방식으로 취급되어 왔다. 그러나 ID 기반 암호 시스템과 전력 분석 공격은 각기 독립적으로 연구되고 있다. 본 논문에서는 전력 분석 공격이 ID 기반 암호 시스템의 안전도에 미치는 영향에 대해 분석한다. 그 결과로, pairing을 사용하는 ID 기반 암호 시스템의 경우 DPA에 대한 대응책 없이 SPA에 대한 대응책만으로도 충분히 안전하다는 것을 보인다.

ABSTRACT

The ID-based cryptosystem and Power Analysis Attack are attracting many researchers and have been developed aggressively to date. Especially, DPA (Differential Power Analysis) attack has been considered to be the most powerful attack against low power devices, such as smart cards. However, these two leading topics are researched independently and have little known relations with each other. In this paper, we investigate the effect of power analysis attack against ID based cryptosystem. As a result, we insist that ID-based cryptosystem is secure against DPA and we only need to defend against SPA (Simple Power Analysis).

Keywords : *ID-based cryptosystem, bilinear pairing, power analysis, DPA, SPA*

Ⅰ. 서 론

Boneh와 Franklin[1]이 Weil pairing을 사용한 ID 기반 암호 시스템을 제안한 이후로 ID 기반 암호 시스템에 대한 활발한 연구가 진행되고 있다. 지금까지 이러한 연구들은 주로 수학적으로 안전성을 증명할 수 있으면서 실용적인 시스템을 개발하는 데에 치중해 왔다.

그러나 현재까지 제안된 ID 기반 암호 시스템들이 부가 채널 공격(side-channel attack)에 대해 안전한지 그렇지 않은지에 관한 연구는 이루어지지 않고 있다. 부가 채널 공격은 스마트카드와 같은 저전력 장치가 암호학적 계산을 수행할 때 발생하는 전력 변화나 방출되는 전자기파, 계산의 소요 시간 등을 분석하는 공격으로, 암호 시스템의 안전성이 수학적으로 증명 가능하더라도 여전히 적용할 수 있다.

접수일 : 2004년 5월 6일 ; 채택일 : 2004년 6월 28일
* 본 연구는 대학 IT 연구센터 육성·지원사업, 교육부 두뇌한국 21사업의 지원으로 수행되었음.
† 주저자, ‡ 교신저자 : yhyang@oberon.postech.ac.kr

이러한 이유로 암호 시스템의 개발자들에게 있어서 부가 채널 공격은 현재 가장 위협적인 공격으로 취급되고 있다.

이에, 본 논문에서는 부가 채널 공격 중 전력 분석 공격[2]과 ID 기반 암호 시스템의 안전성의 관계를 논하고자 한다.

Ⅱ절에서 대표적인 전력 분석 공격인 SPA (Simple Power Analysis)와 DPA(Differential Power Analysis)의 특성에 대해 간단히 살펴본 후, Ⅲ절에서 SPA와 DPA에 모두 취약한 RSA와 ElGamal 암호 시스템을 살펴보고, Ⅳ절에서는 ID 기반 암호 시스템과 서명 시스템에 대해서 알아본다. Ⅴ절에서는 ID 기반 암호 시스템의 전력 분석 공격에 대한 안전도에 대해서 RSA나 ElGamal 시스템과 비교하도록 한다. Ⅵ절에서는 ID 기반 암호 시스템을 보다 안전하게 사용할 수 있는 방법에 대해서 설명한다.

Ⅱ. 전력 분석 공격(Power Analysis Attack)

전력 분석 공격[2]은 부가 채널(side-channel) 공격의 일종이다. 부가 채널 공격이란, 암호 시스템이 기반하고 있는 수학적 문제를 직접 풀지 않으면서, 암호 장치가 연산을 수행하는 동안에 부가 채널을 통해 유출되는 정보를 분석하여 암호 시스템을 공격하는 방식이다. 이 중에서 전력 분석 공격은 암호 장치가 연산을 수행하는 동안 소모하는 전력의 추이를 관찰함으로써 암호 시스템을 공격한다.

최근에 연구되고 있는 전력 분석 공격은 크게 두 가지이다. 하나는 SPA 공격이고, 또 하나는 DPA 공격이다. 많은 암호 시스템에서 $g^x \bmod p$와 같은 modular exponentiation, 혹은 xG와 같은 scalar multiplication이 사용되는데, SPA나 DPA는 이 때 사용되는 secret exponent인 x의 정보를 얻기 위해서 주로 사용된다.

1. SPA (Simple Power Analysis)

SPA는 한번의 power trace로부터 secret exponent의 정보를 얻는 방식이다. SPA는 서로 다른 계산을 수행할 때의 power trace가 서로 다르게 보이며 공격자가 이들을 서로 구별할 만큼의 측정 능력을 갖는다는 가정에서 출발하였다. 이러한 가정을 하게 되면, 하나의 power trace의 sample을 관찰함으로써 어느 부분에서 어떠한 연산이 수행중인지 알 수 있게 된다. SPA는 한 번의 power trace의 측정에서도 secret exponent의 정보 전부 또는 일부를 알아낼 수가 있다.

Exponentiation에 사용되는 exponent는 대개 0과 1로 이진 전개하여 exponentiation 알고리즘에 입력된다. 기본적인 square-and-multiply 방식의 exponentiation 알고리즘의 경우에, 한 개의 exponent 비트마다 0일 경우는 제곱, 1일 경우는 제곱과 곱셈을 수행한다. 만약 exponentiation을 수행하는 동안의 power trace를 본 공격자가 제곱만을 수행하는지, 혹은 제곱과 곱셈을 수행하는지 구별할 수 있다면 결과적으로 해당 exponent의 비트가 0이었는지 1이었는지를 구별할 수가 있게 된다. 이러한 방법으로 exponent의 일부 또는 모든 비트가 알려질 수 있다.

SPA를 막기 위해서는 exponent 비트의 값이 0일 경우에도 제곱과 곱셈을 수행하도록 exponentiation 알고리즘을 수정할 수 있다.

2. DPA (Differential Power Analysis)

DPA는 여러 개의 power trace로부터 secret exponent의 정보를 얻는 방식이다. DPA도 SPA와 같은 가정에서 출발하였으나, SPA처럼 개개의 power trace를 관찰하는 것이 아니라 여러 개의 표본으로부터 secret exponent와 power trace의 통계적 상관관계를 찾음으로써 secret exponent의 정보를 얻게 된다. DPA는 SPA에 대해 안전하게 만들어진 암호 시스템의 공격에도 사용될 수 있다. 그러나 동일한 secret exponent에 대한 여러 개의 power trace를 얻어야 하고, 통계정보를 얻기 위해서 공격자의 계산 능력이 뛰어나야 한다.

Exponentiation에 사용되는 특정 exponent 비트를 알고자 할 경우에, 해당 비트가 0일지 1일지를 먼저 추정한다. 그 후에 0이라고 추정한 경우의 power trace들과 1이라고 추정한 경우의 power trace들을 통계적으로 분석하여 뚜렷한 상관관계가 있는지를 알아본다. 추정이 옳았다면 상관관계가 보일 것이고 추정이 옳지 않았다면 상관관계가 전혀 없을 것이다. 이러한 방법으로 모든 exponent 비트의 값들을 알아낼 수가 있다. SPA는 기본적으로 한 개의 power trace로부터 exponent 비트의 값을 알아내는 것이기 때문에 각 비트의 값에 따른 power

trace의 모양에 차이가 많아야 한다. 그러나 DPA는 통계적인 상관관계를 측정하는 보다 진화된 방법을 사용하기 때문에 power trace의 모양에 차이가 작거나 또는 한 개의 power trace로는 구분 할 수 없는 경우에도 사용할 수 있다.

Ⅲ. 기존 PKI에 기반을 둔 암호 시스템

기존 PKI에 기반을 둔 암호 시스템에 사용되는 modular exponentiation이나 scalar multiplication에는 SPA와 DPA에 대한 대응책을 모두 사용해야 한다. RSA와 ElGamal 암호 시스템이 SPA와 DPA에 어떠한 취약점을 갖는지 알아보도록 한다.

1. RSA 암호 시스템

RSA 암호 시스템[3]의 기본 구조는 다음과 같다.

- **KeyGen.** 공개정보인 $n=pq$를 선택한다. 이 때, p와 q는 큰 소수이다. 사용자의 비밀키로 $d<\phi(n)$인 d를 선택하고 공개키로 $ed\equiv 1 \bmod \phi(n)$인 e를 선택하여 공개한다.
- **Encryption.** 평문 M에 대해서 암호문 C를 $C=M^e \bmod n$으로 계산한다.
- **Decryption.** 암호문 C에 대해서 평문 M을 $M=C^d \bmod n$으로 계산한다.

이 때 전력 분석 공격에 취약한 연산은 $M=C^d \bmod n$이다. 복호화 할 때마다 동일한 사용자에 대해서 동일한 비밀키 d가 사용된다. 따라서 이 연산이 SPA에 취약하면 d의 값을 추출할 수 있게 되고, SPA에 대한 대응책을 사용한 후에도 매번 동일한 exponent가 사용되기 때문에 DPA에 대한 대응책도 마련해야 한다.

2. ElGamal 암호 시스템

ElGamal 암호 시스템[4]의 기본 구조는 다음과 같다.

- **KeyGen.** 위수 n인 곱셈 순환군 G의 생성자 g를 생성하여 공개한다. 사용자의 비밀키로 $x<n$인 x를 선택한 후 공개키 $y=g^x$를 계산하여 공개한다.
- **Encryption.** $k<n$인 난수 k를 생성하여, $r=g^k$를 계산한다. 평문 M에 대해서 $v=M\cdot y^k$를 계산하여 암호문을 $C=(r, v)$로 한다.
- **Decryption.** 암호문 $C=(r, v)$에 대해서, 평문 M을 $M=r^{-x}\cdot v$, 또는 $M=(r^x)^{-1}\cdot v$로 계산한다.

이 때 전력 분석 공격에 취약한 연산은 $r=g^k$와 y^k, r^{-x}(또는 r^x)이다. 난수 k가 알려지면 정직한 사용자가 생성한 암호문으로부터 평문을 알아 낼 수가 있다. 그러나 k는 매번 다르게 생성되어야 하기 때문에 k를 알기 위해서 DPA를 적용할 수는 없다.

더욱 취약한 것은 r^x이다. 매번 같은 비밀키가 exponent로 사용되기 때문에 사용자의 비밀키를 보호하기 위해서는 SPA와 DPA에 대한 대응책을 모두 사용해야 한다.

Ⅳ. ID 기반 암호 시스템

1. Boneh-Franklin의 IBE (BF-IBE)

Boneh-Franklin의 ID 기반 암호 시스템[1]은 modified Weil pairing을 사용한다. 여기서 modified Weil pairing $\hat{e}$ 대신에 임의의 admissible bilinear map[1]을 사용할 수도 있다. Bilinear map $\hat{e}: G_1\times G_1\rightarrow G_2$는 다음과 같은 특징을 가진다.

- $\hat{e}(P, P)=g$인 g는 순환군 G_2의 생성자이다. (Non-degeneracy)
- $\hat{e}(aP, bP)=g^{ab}$. (Bilinearity)
- $\hat{e}(P, Q)$를 계산하기 위한 효율적인 알고리즘이 존재한다. (Computability)

Modified Weil pairing의 경우에는 $G_1=E(F_q)$, $G_2=F_{q^k}$이다.

BF-IBE의 기본 구조는 다음과 같다.

- **KeyGen.** 사용자의 ID에 대해서 공개키 $Q_{ID}=H_1(ID)\in\langle P\rangle$를 계산한다. 이 공개키

는 누구나 계산할 수가 있다. 여기서 P는 특정 타원곡선 위의 점이며 공개된 정보이다. H_1은 $H_1:\{0,1\}^* \rightarrow \langle P \rangle$인 해시 함수이다. 순환군 $\langle P \rangle$의 위수는 소수 q이다. 비밀키 생성 기관(PKG, Private Key Generator)이 사용자의 비밀키 $d_{ID}=sQ_{ID}$를 계산하여 사용자에게 전달한다. 여기서 s는 PKG의 master key이고 비밀 정보이다. PKG의 공개키는 $P_{pub}=sP$이다.

- **Encryption**. 난수 $r \in Z_q$를 선택한다. 평문 M에 대해서 암호문 $C=\langle U, V \rangle$를 다음과 같이 계산한다. $U=rP$, $V=M \oplus H_2(g_{ID}^r)$, 여기서 $g_{ID}=\hat{e}(Q_{ID}, P_{pub})$이고, $P_{pub}=sP$ 이다. H_2는 암호학적으로 안전한 해시 함수이다.
- **Decryption**. 암호문 C에 대해서 $M=V \oplus H_2(\hat{e}(d_{ID}, U))$와 같이 평문을 계산한다.

여기서 전력 분석 공격에 취약한 연산은 rP와 g_{ID}^r이다. 전력 분석 공격을 통해서 정보가 유출되는 것은 r이다. 그러나 여기서 r은 매번 같게 선택될 확률은 무시할 만하기 때문에 r을 알기 위해서 DPA를 적용할 수 없다. 따라서 BF-IBE에 사용되는 scalar multiplication이나 modular multiplication은 DPA 예방책을 꼭 적용할 필요는 없다. r이 유출되면 정상적인 암호문에서 평문을 알아낼 수가 있지만 이것은 SPA에 대한 대응책으로 충분히 막을 수 있다.

2. Cha-Cheon의 IBS (CC-IBS)

Cha-Cheon의 ID 기반 서명 시스템[5]의 기본 구조는 다음과 같다.

- **KeyGen**. Cha-Cheon IBS의 키 생성 과정은 BF-IBE와 같다.
- **Signature**. 난수 $r \in Z_q$를 선택한다. 메시지 M에 대해서 서명 $\sigma=\langle U, V \rangle$를 다음과 같이 계산한다. $U=rQ_{ID}$, $V=(r+h)d_{ID}$, 여기서 $h=H_2(M, U)$이고, H_2는 암호학적으로 안전한 해시 함수이다.
- **Verification**. 서명 $\sigma=\langle U, V \rangle$에 대해서 $\hat{e}(P, V)=\hat{e}(P_{pub}, U+hQ_{ID})$이 만족하면 서명을 받아들인다. 여기에서 $h=H_2(M, U)$이다.

이 경우에 전력 분석 공격에 취약한 연산은 rQ_{ID}이다. r이 알려질 경우에 사용자의 비밀키가 노출되게 된다. 그러나 BF-IBE에서와 마찬가지로 r은 매번 다르게 생성되기 때문에 DPA를 적용할 수는 없다. 따라서 사용자의 비밀키를 보호하기 위해서 SPA에 대한 대응책만을 사용해도 충분하다.

V. 분 석

이상에서 살펴본 바와 같이, RSA 암호 시스템이나 ElGamal 암호 시스템과 같이 복호화 (또는 서명) 과정에서 사용자의 비밀키가 secret exponent로 사용되는 경우에는 DPA 공격에 취약하다. 그러나 ID 기반 암호 시스템의 경우에는 사용자의 비밀키가 secret exponent로 사용되지 않기 때문에 DPA 공격에 취약하지 않다. 현재 DPA는 저 전력 암호 장치에서 가장 위협적인 공격으로 취급되었으나, 살펴본 바와 같이 ID 기반 암호 시스템에서는 그렇지 않다는 것을 알 수 있다.

그러나 지금까지 살펴본 것은 전력 분석 공격이 secret exponent의 정보를 추출하는 데에만 사용한다는 가정 하에서였다. BF-IBE와 CC-IBS에서 매번 같은 secret information이 연산에 사용되는 것은, BF-IBE의 복호화 과정에서 $\hat{e}(d_{ID}, U)$ 연산과 CC-IBS의 서명 과정에서 $(r+h)d_{ID}$ 연산이었다. CC-IBS의 서명과정의 경우 $(r+h)d_{ID}$ 연산에서 secret base인 d_{ID}의 정보를 얻는 공격이나 BF-IBE의 복호화 과정의 경우 $\hat{e}(d_{ID}, U)$ 연산에서 secret operand인 d_{ID}의 정보를 얻는 공격이 있다면 ID 기반 암호 시스템도 취약점을 갖게 될 것이다. 하지만, 아직까지 그런 공격은 소개되지 않았으며 open problem으로 남아 있다.

$\hat{e}(d_{ID}, U)$ 연산에 대한 미래의 공격에 대해서는 VI절에서 소개하는 방법으로 어느 정도 안전을 강화할 수 있다.

VI. ID 기반 암호 시스템의 안전도 강화

ID 기반 암호 시스템에서 $\hat{e}(d_{ID}, U)$ 연산에서

d_{ID}의 정보를 얻을 가능성은 여전히 남아 있다. $\hat{e}$가 $\hat{e}: G_1 \times G_1 \rightarrow G_2$의 modified Weil 혹은 Tate pairing[6, 7]이라면 이 연산을 $\hat{e}(U, d_{ID})$로 수정하여 보다 안전하게 만들 수가 있다. 이는 pairing 연산에 사용되는 Miller's algorithm의 특성에 기인한다. 여기에서 Miller's algorithm [8]에 대해서 간단히 살펴보도록 한다. 아래 알고리즘에서 m은 pairing의 order이다.

Miller's Algorithm for $e_m(P, Q)$

Input : $P, Q \in E(F_q)$

1) Choose a random point $S \in E(F_{q^k})$ and compute $Q' = Q + S \in E(F_{q^k})$.
2) Set $n \leftarrow |m|$, $T_1 \leftarrow P$, $f_1 \leftarrow 1$.
3) While $n \geq 1$ do :
3.1) Calculate the equations of lines l_1 and l_2 arising in doubling T_1.
3.2) Set $T_1 \leftarrow [2]T_1$, and
$$f_1 \leftarrow f_1^2 \frac{l_1(Q')l_2(S)}{l_2(Q')l_1(S)}.$$
3.3) If the n-th bit of m is 1, then
3.3.1) Calculate the equations of the lines l_1 and l_2 arising in adding T_1 and P.
3.3.2) Set $T_1 \leftarrow T_1 + P$, and
$$f_1 \leftarrow f_1 \frac{l_1(Q')l_2(S)}{l_2(Q')l_1(S)}.$$
3.4) Decrement n.
4) Return f_1.

여기에서 P가 보호되어야 하는 operand라면 미지수이긴 하지만 여전히 전력 분석 공격의 여지가 남아 있다. 그러나 Q가 보호되어야 하는 operand라면 step 1)에서 Q'를 계산한 후에 Q가 더 이상 계산에 포함되지 않는다. 이 Q'는 일종의 point randomization이라고 볼 수가 있다. $Q+S$의 operation에서 Q의 정보를 추출하는 공격이 가능하지 않다고 가정하면, Q'는 random point이므로 전력 분석 공격으로 얻는 정보가 없게 된다. 이 가정은 충분히 설득력이 있다. 왜냐하면 이러한 point addition 연산에서 Q의 정보를 추출하는 것이 가능하다면 다른 모든 암호 시스템들도 역시 안전하지 않게 되기 때문이다.

Ⅶ. 결 론

본 논문에서는 ID 기반 암호 시스템의 전력 분석 공격에 대한 안전도에 대해서 검토해 보았다. 또한 아직 알려지지 않은 pairing에 대한 공격을 미연에 방지하는 방법에 대해서 간단히 살펴보았다.

지금까지 가장 위협적인 공격이라고 알려진 DPA 공격이 ID 기반 암호 시스템에 적용될 가능성은 희박하다. 따라서 ID 기반 암호 시스템의 경우 DPA를 고려하지 않아도 되기 때문에 다른 DLP 기반의 암호 시스템들에 비해 성능상의 이점을 갖게 된다. 그러나 아직도 SPA에 대해서는 취약하기 때문에 SPA에 대한 대응책은 계속 연구해야 할 필요가 있다.

참 고 문 헌

[1] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," Crypto 2001, LNCS 2139, pp. 213-229.

[2] P. C. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," Crypto 1999, LNCS 1666, pp. 388-397.

[3] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, 21(2):120-126, 1978.

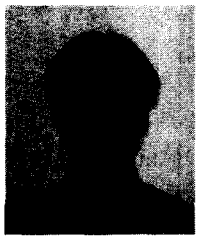
[4] T. ElGamal, "A Public-Key Cryptosystem and a Sinature Scheme Based on Discrete Logarithms," IEEE Trans. Information Theory, vol. 31, no. 4, pp. 469-472, 1985.

[5] J. Cha and J. Cheon, "An Identity-Based Signature from Gap Diffie-Hellman Groups," PKC 2003, LNCS 2567, pp. 18-30.

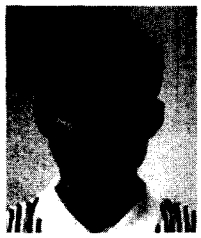
[6] A. J. Menezes, T. Okamoto, and S. A. Vanstone, "Reducing Elliptic Curve Logarithms to Logarithms in a Finite

Field," IEEE Trans. Information Theory, vol. 39, no. 5, pp. 1639-1646.
[7] G. Frey and H.-G. Rück, "A Remark Concerning m-Divisibility and the Discrete Logarithm in the Divisor Class Group of Curves," Math. Comp., vol. 62, no. 206 (1994), pp. 865-874.
[8] V. Miller, "Short Programs for Functions on Curves," unpublished manuscript, 1986.

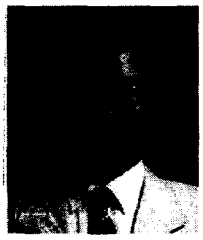
〈著者紹介〉



양 연 형 (Yeon Hyeong Yang) 학생회원
2002년 2월 : 포항공과대학교 전자전기공학과 학사
2002년 3월~현재 : 포항공과대학교 전자전기공학과 박사과정
〈관심분야〉 정보보호, 암호이론, Ubiquitous Computing



박 동 진 (Dong Jin Park) 학생회원
2000년 2월 : 포항공과대학교 전자전기공학과 학사
2000년 3월~현재 : 포항공과대학교 전자전기공학과 박사과정
〈관심분야〉 정보보호, 암호이론, 알고리즘 구현



이 필 중 (Pil Joong Lee) 정회원
1974년 2월 : 서울대학교 전자공학과 학사
1977년 2월 : 서울대학교 전자공학과 석사
1982년 6월 : U.C.L.A System Science, Engineer
1985년 6월 : U.C.L.A Electrical Engineering, Ph.D.
1980년 6월~1985년 8월 : Jet Propulsion Laboratory, Senior Engineer
1985년 8월~1990년 2월 : Bell Communications Research, M.T.S.
1990년 2월~현재 : 포항공과대학교 전자전기공학과 교수
1996년 2월~1997년 2월 : NEC Research Institute 방문 연구원
2000년 9월~2003년 8월 : 포항공과대학교 정보통신연구소 연구소장(정보통신대학원장 겸임)
2004년 1월~2004년 12월 : 한국정보보호학회 회장
2004년 1월~2004년 12월 : 한국통신 연구소 방문 연구원
〈관심분야〉 정보보호전반