Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.1, Feb. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.1.221

AND 게이트에 대한 2차 G-equivariant 로직 게이트 및 AES 구현에의 응용*

백 유 진,[1†] 최 두 호[2‡]
[1]우석대학교, [2]한국전자통신연구원

Second-Order G-equivariant Logic Gate for AND Gate and its Application to Secure AES Implementation*

Yoo-Jin Baek,[1†] Doo-ho Choi[2‡]
[1]Woosuk University, [2]ETRI

요 약

스마트카드 등과 같은 모바일 기기에 구현된 암호 알고리즘은 수학적 안전성뿐만 아니라 부채널 공격에 대한 안전성도 함께 고려되어야 한다. 부채널 공격이란 구현된 암호 알고리즘의 연산 과정 중에 발생하는 부채널 정보를 이용해서 비밀 정보를 알아내는 공격 방법이다. 특히 전력분석 공격은 암호 연산 수행시 발생하는 전력 소비량의 변화를 측정함으로써 암호 기기 내부의 비밀 정보를 알아내는 공격법으로 이에 대한 여러 가지 대응 방법이 제안되었다. 본 논문에서는 블록 암호 알고리즘 구현시 전력분석 공격 및 글리치 공격을 방어할 수 있는 게이트 레벨 기법을 새롭게 제안한다. 또한 본 논문에서 제안한 방법을 이용하여 AES 블록 암호 알고리즘을 전력분석 공격 및 글리치 공격에 안전하게 구현할 수 있는 방법을 제시한다.

ABSTRACT

When implementing cryptographic algorithms in mobile devices like smart cards, the security against side-channel attacks should be considered. Side-channel attacks try to find critical information from the side-channel infromation obtained from the underlying cryptographic devices' execution. Especially, the power analysis attack uses the power consumption profile of the devices as the side-channel information. This paper proposes a new gate-level countermeasure against the power analysis attack and the glitch attack and suggests how to apply the measure to securely implement AES.

Keywords: Smart Card, Side-Channel Attack, Power Analysis Attack, Glitch Attack, Countermeasure, AES

I. 서 론

스마트카드 등과 같은 모바일 기기는 금융 정보 등과 같은 개인 비밀 정보를 저장하고 있기 때문에 불법적인 정보 유출과 비인가된 접근과 같은 보안 위험성이 상존하며 이를 방어하기 위하여 다양한 암호 알고리즘이 사용되고 있다. 따라서 효율적이고 안전한 암호 알고리즘의 구현에 대한 관심 및 중요성은 점점 더 증가하고 있다. 이러한 암호 알고리즘은 수학적 안전성뿐만 아니라 해당 알고리즘 구현시 부채널 공격

접수일(2013년 12월 26일), 수정일(2014년 1월 21일), 게재확정일(2014년 1월 29일)
* 본 연구는 ETRI의 연구개발과제인 K-SCARF 프로젝트로 수행하였음 (암호키 누출 검증 및 방지 원천 기술 연구)
† 주저자, yoojin.baek@gmail.com
‡ 교신저자, dhchoi@etri.re.kr (Corresponding author)

(side-channel attack)에 대한 안전성도 함께 고려되어야 한다.

부채널 공격이란 암호 알고리즘 구현시 연산 과정 중에 발생하는 부채널 정보를 이용해서 비밀 정보를 알아내는 공격 방법을 의미한다[1]. 특히 전력분석 공격은 암호 연산 수행시 발생하는 전력 소비량의 변화를 측정함으로써 암호 기기 내부의 비밀 정보를 알아내는 공격법으로 이에 대한 여러 가지 대응 방법이 제안되었다.

본 논문에서는 전력분석 공격 및 전력분석 공격의 일종인 글리치 공격에 대한 게이트 레벨에서의 새로운 방어 기법을 제시한다. 또한 제안된 방법을 응용하여 AES(Advanced Encryption Standard)를 전력분석 공격 및 글리치 공격에 안전하게 구현할 수 있는 방법을 제시한다.

II. 사전 지식

2.1 부채널 공격

일반적으로 암호 공격법은 크게 수학적인 공격과 부채널 공격의 두 가지 범주로 분류가 된다. 먼저 수학적인 공격법은 암호 알고리즘을 비밀키를 인자로 가지는 수학적인 변환 또는 함수로 간주하며 수학적인 관점에서 그 안전성을 평가한다. 이러한 공격법의 대표적인 예로는 차분 공격법, 선형 공격법 그리고 대수적인 공격법 등이 있다. 반면에 부채널 공격법은 암호 알고리즘을 물리적인 기기에서 동작하는 실제 프로그램으로 간주하며 해당 기기의 암호 연산 과정 중에 발생하는 부채널 정보를 이용하여 기기 내부에 저장된 비밀 정보를 알아내는 공격방법이다. 이러한 부채널 정보의 예로는 연산 시간, 전력 소비 패턴, 전자기장 패턴 및 의도된 혹은 의도되지 않은 오류 주입으로부터 생성된 잘못된 암호 연산값 등이 있다. 부채널 공격법은 Kocher 등에 의해 스마트카드에 대한 시간 분석 공격법이 제안된 이후로 현재까지 여러 가지 다양한 공격법과 그에 대한 대응 기법이 제시되었다[1].

부채널 공격법 중에서 전력 분석 공격법은 암호 기기의 전력 소비 패턴으로부터 기기 내에 저장된 비밀 정보를 추출해 내는 공격법으로 대표적으로 단순 전력분석 공격과 차분 전력분석 공격이 있다[2]. 먼저 단순 전력분석 공격은 암호 연산 자체의 전력 소비 패턴을 이용하여 다양한 원시 암호 연산을 구별해 내는 공격법으로 더미 연산을 삽입하는 것과 같은 다양한 방어기법이 제안되었다. 차분 전력분석 공격은 암호기기의 전력소비 패턴을 다양한 신호처리 기법을 이용하여 분석한 후 기기 내에 저장된 비밀 정보를 알아내는 공격법으로 이에 대한 대응 방법으로는 마스킹 기법(masking method)을 포함한 다양한 랜덤화 기법이 있다[3].

2.2 마스킹 기법과 글리치 공격

블록 암호 알고리즘을 차분 전력분석 공격에 안전하게 구현하기 위해서 제안된 대표적인 방법으로는 마스킹 기법이 있다. 마스킹 기법은 평문에 대한 암호화 연산을 수행하기 전에 난수를 이용하여 평문을 마스킹하고 마스킹된 데이터와 사용된 난수를 이용하여 암호 연산을 수행함으로써 외부에 노출된 전력소비 패턴과 내부 데이터와의 상관관계를 축소 또는 제거한다. 이러한 마스킹 기법은 임의의 함수에 적용 가능하지만 일반적으로 해당 함수가 블록 암호 알고리즘의 S-box와 같은 비선형 함수인 경우 그 적용이 쉽지 않다는 난점이 있으며 이를 해결하기 위하여 게이트 레벨 마스킹 기법(gate-level masking method)이 연구되었다.

게이트 레벨 마스킹 기법에서는 먼저 임의의 함수를 기본 게이트로 분해한 후 기본 게이트에 대하여 마스킹 방법을 적용한다. 특히 기본 게이트 중에서AND 및 OR 게이트가 비선형 함수의 역할을 하기 때문에 이러한 게이트에 대하여 마스킹 기법을 효율적으로 적용하는 방식에 대한 연구가 많이 진행되었다. 예를 들어 E. Trichina[4]는 여분의 랜덤 신호를 이용하여 AND 게이트에 대한 게이트 레벨 마스킹 기법을 제안하였으며 J. Golić 등[5]은 MUX 게이트에 먼저 마스킹 기법을 적용한 후 이를 이용하여 AND 게이트 및 OR 게이트에 적용 가능한 새로운 마스킹 기법을 제안하였다.

그러나 이러한 게이트 레벨 마스킹 기법 대부분은 해당 게이트의 모든 입력 신호가 동일하게 도착한다는 가정에 기반하였으며 이러한 가정에 기반한 마스킹 기법은 글리치 공격(glitch attack)에 취약함이 알려져 있다[6]. 즉, 게이트의 입력 신호는 동일한 시간에 도착하지 않고 따라서 그 출력값은 한 클록 싸이클 내에서 안정화되기 전까지 여러 번 전이하게 되는 글리치 특성을 보여주게 되는데 이러한 글리치 특성은 실제로 회로의 전력 소모에 많은 영향을 미치게 된다. 이러한 글리치 특성을 이용한 공격을 글리치 공격이라

고 하며 이전에 제안된 대부분의 게이트 레벨 마스킹 기법은 글리치 공격에 취약하다고 알려져 있다. 본 논문에서는 이러한 글리치 특성을 고려한 게이트 레벨 마스킹 방법을 제안하며 제안된 방법은 1차 전력 분석 공격 및 글리치 공격에 안전함을 보인다.

III. G-equivariant 로직 게이트

이번 장에서는 입력 신호가 n개이고 출력 신호가 1개인 게이트 g를 다음과 같은 불리안(Boolean) 함수로 간주한다:

$$g: F_2^n \to F_2.$$

여기서 F_2는 0과 1로 구성된 이진 필드(binary field)를 의미하며 F_2상에서의 덧셈 연산은 $\oplus$로 표기된다.

정의 1 ([7]). 게이트 $g: F_2^n \to F_2$ 및 $i=1,...,n$에 대하여 g의 (부분) 에너지 함수 $E_{g,i}$는 다음과 같이 정의된다:

$$E_{g,i}: F_2^n \times F_2^n \times Map_{\{1,...,n\}} \to V$$
$$(\tilde{a}, \tilde{x}, \phi) \mapsto e_{g(\tilde{b}_i), g(\tilde{b}_{i+1})}.$$

여기서 $Map_{\{1,...,n\}}$은 집합 $\{1,...,n\}$에서 자기 자신으로 가는 모든 함수로 구성된 집합을 나타내고, V는 선형 독립인 벡터 $e_{0,0}, e_{0,1}, e_{1,0}, e_{1,1}$를 기저로 가지는 4차원 실벡터 공간을 의미하는데 여기서 $e_{i,j}$는 게이트의 신호가 i에서 j로 변화하는 경우 전력 소비량을 나타내는 심볼이다. 또한 $\tilde{b}_i = (b_{i1}, ..., b_{in}) \in F_2^n$은 다음과 같이 주어진 벡터를 의미한다: $\tilde{b}_1 = \tilde{a}$, $\tilde{b}_{n+1} = \tilde{x}$이고

$$b_{(i+1)j} = \begin{cases} x_j & \text{if } \phi(j) = i \\ b_{ij} & else \end{cases}.$$

정의 1에서 $\phi \in Map_{\{1,...,n\}}$는 실제 게이트의 입력 신호의 도착 순서를 나타내게 되는데 가령 $i, j = 1, ..., n$에 대하여 $\phi(i) = j$는 입력 신호의 i번째 벡터 원소가 j번째에 도착했음을 의미한다. 따라서 (부분) 에너지 함수는, 가령 g의 입력 신호가 $\tilde{a}$에서 $\tilde{x}$로 변화하고 신호의 도착 순서가 ϕ에 의해서 정해지는 경우에 g가 소비하는 전력 소비량을 표시하게 된다.

정의 2. 게이트 $g: F_2^2 \to F_2$의 임의의 입력값 $(a,b) \in F_2^2$에 대하여 다음을 만족시키는 $(a_1, a_2, b_1, b_2) \in F_2^4$를 (a,b)의 (일차) 마스킹된 신호쌍이라고 한다:

1) $a = a_1 \oplus a_2, b = b_1 \oplus b_2$
2) a_1, a_2, b_1, b_2는 등분포(uniformly distributed) 되어 있다.
3) $i, j = 1, 2$에 대하여 랜덤 변수 a_i와 b_j는 서로 독립이다.

정의 3. 게이트 $g: F_2^2 \to F_2$에 대하여 g의 (일차) 마스킹된 게이트는 다음을 만족시키는 게이트 쌍 (g_1, g_2)를 의미한다:

1) $g_1, g_2 : F_2^2 \times F_2^2 \to F_2$
2) g의 임의의 입력값 $(a,b) \in F_2^2$ 및 (a,b)의 임의의 (일차) 마스킹된 신호쌍 $(a_1, a_2, b_1, b_2) \in F_2^4$에 대하여 $g_1(a_1, a_2, b_1, b_2) \oplus g_2(a_1, a_2, b_1, b_2) = g(a,b)$ 이다.

정의 4 ([7]). 만약 임의의 $\phi \in Map_{\{1,2,3,4\}}$와 $i = 1, 2, 3, 4$에 대하여 다음과 같이 주어진 16개의 값이 동일하면 게이트 $g: F_2^2 \times F_2^2 \to F_2$를 G-equivariant 게이트라고 한다: $a, b, x, y \in F_2$에 대하여

$$\sum_{\substack{a_1 \oplus a_2 = a \\ b_1 \oplus b_2 = b \\ x_1 \oplus x_2 = x \\ y_1 \oplus y_2 = y}} E_{g,i}((a_1, a_2, b_1, b_2), (x_1, x_2, y_1, y_2), \phi).$$

참고. 상기 정의 4는 논문 [7]의 Definition 5와 Lemma 1의 2)번 항을 결합한 정의이다.

G-equivariant 게이트는 게이트의 입력 신호가 동일하게 도착하지 않더라도 해당 게이트의 전력소비 패턴은 변하지 않으며 따라서 글리치 공격에 강인한 특성을 가진다. 그러나 하기 정리 1이 보여주듯이 AES 등과 같은 블록 암호 알고리즘의 구현을 위한 AND 게이트 및 OR 게이트의 마스킹에 사용될 수 있는 G-equivariant 게이트는 존재하지 않는다.

정리 1 ([7]). AND 및 OR 게이트의 마스킹에 사용될 수 있는 G-equivariant 게이트는 존재하지 않는다.

정리 1의 G-equivariant 게이트의 부존재성 때문에 논문 [7]에서는 G-equivariant 게이트보다 조건을 완화한 semi-G-quivariant 게이트를 정의하

고 그 존재성을 증명한다. 그러나 semi-G-quivariant 게이트는 각 입력 신호의 (일차) 마스킹된 신호 쌍들이 동시에 게이트에 도착한다는 가정을 하고 있는데 이러한 가정을 실제 구현하기는 용이하지 않다. 따라서 본 논문에서는 이러한 가정을 대신하여 각 입력 신호가 이차 마스킹이 되었다고 가정을 하고 이러한 가정 하에서 정의 4의 G-equivariant 게이트가 존재한다는 것을 증명할 것이다. 이를 위해서 본 논문은 정의 2, 3, 4를 다음과 같이 이차 마스킹으로 확장한다.

정의 2-1. 게이트 $g: F_2^2 \rightarrow F_2$의 임의의 입력값 $(a,b) \in F_2^2$에 대하여 다음을 만족시키는 $(a_1,a_2,a_3,b_1,b_2,b_3) \in F_2^6$를 (a,b)의 이차 랜덤화된 신호 쌍이라고 한다:

1) $a = a_1 \oplus a_2 \oplus a_3, b = b_1 \oplus b_2 \oplus b_3$
2) a_1,a_2,a_3,b_1,b_2,b_3는 등분포(uniformly distributed) 되어 있다.
3) $i,j = 1,2,3$에 대하여 랜덤 변수 a_i와 b_j는 서로 독립이다.

정의 3-1. 게이트 $g: F_2^2 \rightarrow F_2$에 대하여 g의 이차 마스킹된 게이트는 다음을 만족시키는 게이트 쌍 (g_1,g_2,g_3)를 의미한다:

1) $g_1,g_2,g_3 : F_2^3 \times F_2^3 \rightarrow F_2$
2) g의 임의의 입력값 $(a,b) \in F_2^2$ 및 (a,b)의 임의의 이차 마스킹된 신호쌍 $(a_1,a_2,a_3,b_1,b_2,b_3) \in F_2^6$에 대하여 $g_1(a_1,a_2,a_3,b_1,b_2,b_3) \oplus g_2(a_1,a_2,a_3,b_1,b_2,b_3) = g(a,b)$ 이다.

정의 4-1. 만약 임의의 $\phi \in Map_{\{1,2,3,4,5,6\}}$와 $i = 1,\ldots,6$에 대하여 다음과 같은 16개의 값이 동일하면 게이트 $g: F_2^3 \times F_2^3 \rightarrow F_2$를 이차 G-equivariant 게이트라고 한다: $a,b,x,y \in F_2$에 대하여

$$\sum_{\substack{a_1 \oplus a_2 \oplus a_3 = a \\ b_1 \oplus b_2 \oplus b_3 = b \\ x_1 \oplus x_2 \oplus x_3 = x \\ y_1 \oplus y_2 \oplus y_3 = y}} E_{g,i}((\bar{a},\bar{b}),(\bar{x},\bar{y}),\phi) \quad . \tag{1}$$

여기서 $\bar{a},\bar{b},\bar{x},\bar{y}$는 다음과 같이 주어진 벡터이다:

$\bar{a} := (a_1,a_2,a_3)$.
$\bar{b} := (b_1,b_2,b_3)$
$\bar{x} := (x_1,x_2,x_3)$
$\bar{y} := (y_1,y_2,y_3)$

이차 G-equivariant 게이트 역시 G-equivariant 게이트와 동일하게 게이트의 입력 신호가 동일하게 도착하지 않더라도 해당 게이트의 전력소비 패턴은 변하지 않으며 따라서 글리치 공격에 강인하다. 그러나 G-equvariant 게이트와는 다르게 AND 게이트의 마스킹에 사용될 수 있는 이차 G-equivariant 게이트가 존재함을 다음과 같이 보여줄 수 있다.

정리 2. 다음과 같이 정의된 게이트 $g_1,g_2,g_3 : F_2^3 \times F_2^3 \rightarrow F_2$는 이차 G-equivariant 게이트이며 AND 게이트의 이차 마스킹된 게이트이다:

$$g_1(a_1,a_2,a_3,b_1,b_2,b_3) = a_1b_1 \oplus a_3b_3 \oplus a_3b_1$$
$$g_2(a_1,a_2,a_3,b_1,b_2,b_3) = a_1b_2 \oplus a_2b_3 \oplus a_1b_3$$
$$g_3(a_1,a_2,a_3,b_1,b_2,b_3) = a_2b_2 \oplus a_2b_1 \oplus a_3b_2$$

또한 $(a,b) \in F_2^2$를 계산하기 위하여 (a,b)의 이차 마스킹된 신호쌍을 이용하여 g_1,g_2,g_3를 계산하는 경우 그 중간 계산값의 확률 분포는 (a,b)에 독립이며 따라서 g_1,g_2,g_3로 마스킹한 AND 게이트는 일차 전력분석 공격에 안전하다.

증명. 먼저 $(a,b) \in F_2^2$를 계산하기 위하여 (a,b)의 이차 마스킹된 신호쌍 a_1,a_2,a_3,b_1,b_2,b_3을 이용하여 g_1,g_2,g_3를 계산하는 경우 그 중간 계산값은 하기 Fig. 1.이 보여주듯이 다음과 같다: a_1b_1, a_3b_3, a_3b_1, a_1b_2, a_2b_3, a_1b_3, a_2b_2, a_2b_1, a_3b_2, $a_1b_2 \oplus a_2b_3 \oplus a_1b_3$, $a_2b_2 \oplus a_2b_1 \oplus a_3b_2$, $a_1b_1 \oplus a_3b_3 \oplus a_3b_1$. 이 중에서 a_1b_1, a_3b_3, a_3b_1, a_1b_2, a_2b_3, a_1b_3, a_2b_2, a_2b_1, a_3b_2의 확률 분포가 $a = a_1 \oplus a_2 \oplus a_3, b = b_1 \oplus b_2 \oplus b_3$와 독립이라는 것은 정의 2-1의 조건 2)번과 3)번에 의해서 자명하다. 또한 임의의 $\alpha,\beta \in \{0,1\}$에 대하여

$$\begin{aligned} &\Pr(a_1b_1 \oplus a_3b_3 \oplus a_3b_1 = 0 | a = \alpha, b = \beta), \\ &= \Pr(a_1b_2 \oplus a_2b_3 \oplus a_1b_3 = 0 | a = \alpha, b = \beta) \\ &= \Pr(a_2b_2 \oplus a_2b_1 \oplus a_3b_2 = 0 | a = \alpha, b = \beta) \\ &= \frac{5}{8} \end{aligned}$$

이기 때문에 $a_1b_2 \oplus a_2b_3 \oplus a_1b_3$, $a_2b_2 \oplus a_2b_1 \oplus a_3b_2$, $a_1b_1 \oplus a_3b_3 \oplus a_3b_1$의 확률 분포 역시 a,b와 독립이다.

다음으로

$$\begin{aligned} &g_1(a_1,a_2,a_3,b_1,b_2,b_3) \oplus \\ &g_2(a_1,a_2,a_3,b_1,b_2,b_3) \oplus \\ &g_3(a_1,a_2,a_3,b_1,b_2,b_3) \\ &= (a_1 \oplus a_2 \oplus a_3) \oplus (b_1 \oplus b_2 \oplus b_3) \\ &= ab \end{aligned}$$

이기 때문에 g_1, g_2, g_3는 AND 게이트에 대한 이차 마스킹된 게이트가 된다.

마지막으로 g_1, g_2, g_3가 이차 G-equivariant라는 증명을 위해서는 다음과 같은 표기법이 필요하다. 먼저 주어진 $a, b, x, y \in \{0,1\}$에 대하여 정의 4-1의 식 (1)에 해당하는 에너지 함수를 $E_{g,i}(a,b,x,y,\phi)$로 표기하면

$$E_{g,i}(a,b,x,y,\phi) \in Ze_{00} + Ze_{01} + Ze_{20} + Ze_{11}$$

가 되며 (여기서 Z는 정수의 집합을 의미한다.) 다음 코드는 실제로 $E_{g,i}(a,b,x,y,\phi)$를 계산하는 프로그램이 된다:

입력: $g: F_2^3 \times F_2^3 \to F_2$
$\phi \in Map_{\{1,2,3,4,5,6\}}$
$a, b, x, y \in \{0,1\}$
$i = 1, \ldots, 6$

출력: $E_{g,i}(a,b,x,y,\phi)$

1. $E_{g,i}(a,b,x,y,\phi) = 0$;
2. For $a_1, a_2 = 0$ to 1 do
   For $b_1, b_2 = 0$ to 1 do
   For $x_1, x_2 = 0$ to 1 do
   For $y_1, y_2 = 0$ to 1 do
   $a_3 = a \oplus a_1 \oplus a_2$;
   $b_3 = b \oplus b_1 \oplus b_2$;
   $x_3 = x \oplus x_1 \oplus x_2$;
   $y_3 = y \oplus y_1 \oplus y_2$;
   $E_{g,i}(a,b,x,y,\phi)$ += $e_{g(\bar{a},\bar{b}),g(\bar{x},\bar{y})}$, where $\bar{a} = (a_1,a_2,a_3)$, $\bar{b} = (b_1,b_2,b_3)$, $\bar{x} = (x_1,x_2,x_3)$ and $\bar{y} = (y_1,y_2,y_3)$.
   end loop
   end loop
   end loop
   end loop
3. Return $E_{g,i}(a,b,x,y,\phi)$.

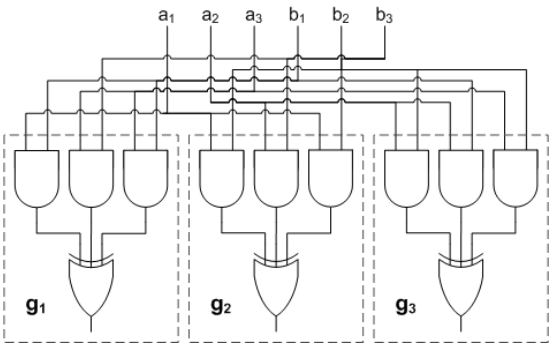

Fig.1. Pictorial Illustration of g_1, g_2, g_3

g_1, g_2, g_3에 대하여 상기 프로그램을 적용하면 임의의 ϕ 및 i에 대하여 $E_{g,i}(a,b,x,y,\phi)$가 동일함을 알 수 있으며 따라서 g_1, g_2, g_3가 이차 G-equivariant함을 증명할 수 있다. □

IV. AES S-Box 구현에의 응용

AES 알고리즘이 사용하는 함수는 AddRoundKey, MixColumns, ShiftRows, SubBytes가 있다[8]. 이 중에서 SubBytes를 제외하고는 모두 선형 또는 아핀(affine) 함수이기 때문에 마스킹 기법을 적용하는 것은 어렵지 않다. 따라서 이번 장에서는 3장에서 제안한 방법을 이용하여 AES SubBytes 함수를 전력분석 공격에 안전하게 구현하는 방법을 설명한다. 특히 AES SubBytes 함수는 유한체 $GF(2^8)$ 상에서의 역원 연산 및 아핀 함수의 합성 함수로 구성되어 있기 때문에 이번 장에서는 $GF(2^8)$상에서의 역원 연산을 주로 다룬다.

먼저 $GF(2^8)$의 각 원소는 다음과 같은 표기법 및 동형 사상 σ에 의해서 $GF(((2^2)^2)^2)$의 원소로 간주될 수 있다[9, 10]:

$$\begin{aligned} GF(2^2) &\simeq GF(2)[x]/(x^2+x+1), \\ GF((2^2)^2) &\simeq GF(2^2)[x]/(x^2+x+\phi), \\ &\quad (\phi = (10)_2 \in GF(2^2)), \\ GF(((2^2)^2)^2) &\simeq GF((2^2)^2)[x]/(x^2+x+\lambda), \\ &\quad (\lambda = (1100)_2 \in GF((2^2)^2)), \\ GF(2^8) &\simeq GF(2)[x]/(x^8+x^4+x^3+x+1) \end{aligned}$$

$$\sigma = \begin{pmatrix} 1&1&0&0&0&0&1&0 \\ 0&1&0&0&1&0&1&0 \\ 0&1&1&1&1&0&0&1 \\ 0&1&1&0&0&0&1&1 \\ 0&1&1&1&0&1&0&1 \\ 0&0&1&1&0&1&0&1 \\ 0&1&1&1&1&0&1&1 \\ 0&0&0&0&0&1&0&1 \end{pmatrix}$$

따라서 $h \in GF(2^8)$가 주어지면 어떤 $a, b \in GF((2^2)^2)$에 대하여 $\sigma(h) = ax+b$와 같이 표기 가능하고 따라서 $\sigma(h)^{-1}$는 다음과 같이 계산 가능하다[10]:

$$\sigma(h)^{-1} = \frac{1}{a^2\lambda + b(a+b)}(ax + a + b).$$

즉 $GF(2^8)$ 상의 역원 계산은 $GF((2^2)^2)$상의 연산을 사용하여 구현 가능하며 이때 $GF((2^2)^2)$상의 비선형 연산은 $\frac{1}{a^2\lambda + b(a+b)}$와 같은 역원 연산과 $a^2\lambda$와 같은 곱셈 연산이 된다. 비슷하게 $a = a_1x + a_2, b = b_1x + b_2 \in GF((2^2)^2)$에 대하여 a의 역원 및 a, b의 곱 ab는 다음과 같이 계산 가능하다[10]:

$$a^{-1} = (a_1\phi + a_2(a_1 + a_2))^2(a_1x + a_1 + a_2),$$
$$ab = ((a_1 + a_2)(b_1 + b_2) + a_2b_2)x + (a_1b_1\phi + a_2b_2).$$

결국 a^{-1}, ab계산은 $GF(2^2)$상의 연산을 사용하여 구현 가능하며 이때의 유일한 비선형 연산은 a_1b_1와 같은 곱셈 연산이 된다. 마지막으로 $GF(2^2)$상의 곱셈 연산은 다음과 같이 구현 가능하며 이때의 유일한 비선형 연산은 $GF(2)$상의 곱셈, 즉 AND 게이트가 된다[10]: $a = a_1x + a_2, b = b_1x + b_2 \in GF(2^2)$에 대하여

$$ab = (a_1b_1 \oplus a_1b_2 \oplus a_2b_1)x \oplus (a_1b_1 \oplus a_2b_2).$$

따라서 본 논문에서 제안한 AND 게이트에 대한 이차 마스킹된 G-equivariant 게이트를 이용하면 $GF(2)$상의 곱셈 연산인 AND 게이트를 (일차) 전력 분석 공격 및 글리치 공격에 안전하게 구현할 수 있으며 이는 다시 AES SubBytes 함수 및 AES 전체 알고리즘을 안전하게 구현할 수 있는 방법을 제공하게 된다.

V. 결 론

본 논문에서는 전력분석 공격에 안전하게 블록 암호 알고리즘을 구현하는 방법에 관한 새로운 게이트 레벨 마스킹 기법을 제안하였으며 제안한 방법이 이차 G-equivariant함을 보임으로써 글리치 공격에 강인함을 보일 수 있었다. 또한 본 논문에서 제안한 방법을 이용하여 AES 알고리즘을 전력분석 공격 및 글리치 공격에 안전하게 구현할 수 있는 방법을 제시하였다.

References

[1] P. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," Advances in Cryptology, CRYPTO '96, LNCS 1109, pp. 104-113, 1996.

[2] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," Advances in Cryptology, Crypto '99, LNCS 1666, pp. 388-397, 1999.

[3] T. Messerges, "Securing the AES finalists against power analysis attacks," Fast Software Encryption, FSE 2000, LNCS 1978, pp. 150-165, 2000.

[4] E. Trichina, "Combinational Logic Design for AES Subbyte Transformation on Masked Data," IACR ePrint 2003-236, 2003.

[5] J. Golić and R. Menicocci, "Universal Masking on Logic Gate Level," Electronics Letters, vol. 40, no. 9, pp. 526-527, Apr. 2004.

[6] S. Mangard, T. Popp, and B.M. Gammel, "Side-Channel Leakage of Masked CMOS Gates," RSA Conference 2005, Cryptographer's Track, CR-RSA 2005, LNCS 3376, pp. 351-365, 2005.

[7] W. Fischer and B.M. Gammel, "Masking at Gate Level in the Presence of Glitches," 7th Workshop on Cryptographic Hardware and Embedded Systems, CHES 2005, LNCS 3659, pp. 187-200, 2005.

[8] National Institute of Standards and Technology, "Anouncing the Advanced Encryption Standard(AES)," FIPS 197, 2001.

[9] A. Satoh, S. Morioka, K. Takano, and S. Munetoh, "A Compact Rijndael Hardware Architecture with S-Box Optimization," Asiacrypt 2001, LNCS 2248, pp. 239 - 254, 2001.

[10] Yoo-Jin Baek and Mi-Jung Noh, "DPA-Resistant Finite Field Multipliers and Secure AES Design," 2nd Information Security Practice and Experience, ISPEC 2006, LNCS 3903, pp. 1 - 12, 2006.

〈저자소개〉

백 유 진 (Yoo-Jin Baek) 종신회원
1997년 2월: 서울대학교 수학과 졸업
1999년 2월: 서울대학교 수학과 이학석사
2003년 2월: 서울대학교 수리과학부 이학박사
2003년 3월~2003년 6월: KAIST 박사후 연구원
2003년 7월~2013년 3월: 삼성전자 책임 연구원
2013년 3월~현재: 우석대학교 정보보안학과 조교수
〈관심분야〉 부채널 공격, 정보 보안

최 두 호 (Doo-ho Choi) 정회원
1994년 2월: 성균관대학교 수학과 졸업
1996년 2월: KAIST 수학과 석사
2002년 2월: KAIST 수학과 박사
2002년 1월~현재: 한국전자통신연구원 책임연구원
〈관심분야〉 암호 엔지니어링, 부채널 분석, IoT 보안