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

백 유 진,† 최 두 호‡
1우석대학교, 2한국전자통신연구원

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

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

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 이용하여 비밀 정보를 알아내는 공격 방법이다. 특히 전력분석 공격은 암호 연산 수행중 발생하는 전력 소비량의 변화를 측정함으로써 암호 기기 내부의 비밀 정보를 알아내는 공격법으로 이에 대한 여러 가지 대응 방법이 제안되었다. 본 논문에서는 불록 암호 알고리즘 구현시 전력분석 공격 및 글리치 공격을 방어할 수 있는 게이트 레벨 기법을 제안한다. 또한 본 논문에서 제안한 방법을 이용하여 AES 불록 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 information 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 반인간적인 접근과 같은 보안 위협이 상존하며 이를 방어하기 위하여 다양한 암호 알고리즘이 사용되고 있다. 따라서 효율적이고 안전한 암호 알고리즘의 구현에 대한 관심 및 중요성이 점점 더 증가하고 있다. 이러한 암호 알고리즘은 수학적 안전성뿐만 아니라 해당 알고리즘 구현시 부채널 공격
AND 게이트에 대한 2차 G-equivariant 로직 게이트 및 AES 구현에의 응용

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 방식이 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 전력 분석 공격 및 글리치 공격에 안전하게 구현할 수 있는 방법을 제시한다.


text:image

II. 사전 지식

2.1 부채널 공격

일반적으로 암호 공격법은 크게 수학적인 공격과 부채널 공격의 두 가지 방주로 분류된다. 먼저 수학적인 공격법은 암호 알고리즘을 비밀키를 인자로 가진 수학적인 변환 또는 함수로 간주하여 수학적인 관점에서 그 안전성에 평가한다. 이러한 공격법의 대표적인 예로는 차분 공격, 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 전력 분석 공격과 차분 전력 분석이 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 평론에 대한 암호화 연산을 수행한 후에 암호화 비밀키와 사용된 암호화 연산을 수행함으로써 외부에 노출된 전력소비 패턴과 내부 데이터와의 상관관계를 축소 또는 제거한다. 이러한 마스킹 기법은 암호의 함수에 적용 가능하지만 일반적으로 해당 함수가 블록 암호 알고리즘의 S-box와 같은 비선형 함수인 경우 그 적용이 쉽지 않는다는 난점이 있으며 이를 해결하기 위하여 게이트 레벨 마스킹 기법(gate-level masking method)이 연구되었다.


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 않으므로 그 출력값은 한 클록 사이를 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 \( n \)개이고 출력 신호가 1개인 게이트 \( g \)를 다음과 같은 불리안(Boolean) 함수로 간주한다:

\[
g : F_2^n \rightarrow F_2.
\]

여기서 \( F_2^n \)은 \( 0 \)과 \( 1 \)로 구성된 이진 필드(binary field)를 의미하며 \( F_2 \)상의 덧셈 연산은 \( \oplus \)로 표기된다.

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

\[
E_{g,i} : F_2 \times F_2 \times M_y \rightarrow V
\]

\[
((a, x, \phi)) \rightarrow E_{g}(k_n, k_n).
\]

여기서 \( M_y \)는 집합 \((1, \ldots, n)\)에서 자기 자신으로 가는 모든 함수로 구성된 집합을 나타내고, \( V \)는 선형 독립인 벡터 \( e_0, e_1, \ldots, e_i \)을 기저로 가지는 \( 2^n \)차원 클로저 공간을 의미하는데 여기서 \( e_i \)는 게이트의 신호가 \( i \)에서 \( j \)로 변화하는 경우 전력 소비량을 나타내는 심볼이다. 또한 \( \hat{b}_i = (b_1, \ldots, b_n) \in F_2^n \)은 다음과 같이 주어진 벡터를 의미한다: \( \hat{b}_i = a \cdot b_{n+1} = \hat{x} \)이고

\[
b_{i+1} = \begin{cases} x_j & \text{if } \phi(j) = i \\ b_{i,j} & \text{else} \end{cases}
\]

정의 1에서 \( \phi \in M_y \)는 실제 게이트의 입력 신호의 도착 순서를 나타내는 데다 \( i, j = 1, \ldots, n \)에 대하여 \( \phi(i) = j \)는 입력 신호의 \( j \)번째 벡터 원소가 \( i \)번째에 도착했음을 의미한다. 따라서 (부분) 에너지 함수는, 가령 \( g \)의 입력 신호가 \( \hat{a} \)에서 \( \hat{x} \)로 변화하고 신호의 도착 순서가 \( \phi \)에 의해서 정해지는 경우에 \( g \)가 소비하는 전력 소비량을 표시하게 된다.

정의 2. 게이트 \( g : F_2^n \rightarrow F_2 \)의 임의의 입력값 \( (a, b) \in F_2^n \)에 대하여 다음을 만족시키는 \( (a_n, a_{n+1}, b_n) \in F_2^n \)를 \( (a, b) \)의 (일차) 마스킹된 신호쌍이라고 한다:

1) \( a_n \oplus a_{n+1} \oplus b_n = a \)

2) \( a_n, a_{n+1}, b_n \)는 동분포(uniformly distributed)되어 있다.

3) \( i, j = 1, 2 \)에 대하여 랜덤 변수 \( a \)와 \( b \)는 서로 독립이다.

정의 3. 게이트 \( g : F_2^n \rightarrow F_2 \)에 대하여 \( g \)의 (일차) 마스킹된 게이트는 다음을 만족시키는 게이트 쌍 \( (g_1, g_2) \)을 의미한다:

1) \( g_1, g_2 : F_2^n \rightarrow F_2 \)

2) \( g \)의 입력의 입력값 \( (a, b) \in F_2^n \)의 입력의 (일차) 마스킹된 신호쌍 \( (a_n, a_{n+1}, b_n) \)을 \( (a, b) \)에 대하여 \( g_1(a_n, a_{n+1}, b_n) \oplus g_2(a_n, a_{n+1}, b_n) = g(a, b) \).

정의 4 ([7]). 만약 임의의 \( \phi \in M_y \)\((1, 2, 3, 4)\)와 \( i = 1, 2, 3, 4 \)에 대하여 다음과 같이 주어진 \( 16 \)개의 값을 동일하게 게이트 \( g : F_2^n \rightarrow F_2 \)을 G-equivariant 게이트라고 한다:

\[
\sum_{a_n, a_{n+1}, b_n} E_{g,i}((a_1, a_2, b_1, b_2), (x_1, x_2, y_1, y_2), \phi).
\]

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 강한 특성을 가진다. 그러나 하기 정리 1이 보여주듯이 AES 등의 같은 블락 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.

고 그 존재성을 증명한다. 그러나 semi-G-equivariant 게이트는 각 입력 신호의 (일차) 마스킹된 신호쌍이 동시에 게이트에 도착한다는 가정을 하고 있는데 이러한 가정은 실제 구현하기는 용이하지 않다. 따라서 본 논문에서는 이러한 가정을 대체하여 각 입력 신호가 각각 마스킹이 되었다고 가정을 하고 이러한 가정 하에서 정의 4의 G-equivariant 게이트가 존재한다는 것을 증명한다. 이를 위해서 본 논문에는 정의 2, 3, 4를 다음과 같이 했고 한다.

정의 2-1. 게이트 : \( F_2^n \rightarrow F_2^n \)의 입력의 입력값 \((a, b) \in F_2^n \)에 대하여 다음과 같은 만족시키는 \((a_1, a_2, a_3, b_1, b_2, b_3) \in F_2^6\)를 이차 랜덤화된 신호쌍이라고 한다.

1) \( a \in (a_1 \oplus a_2 \oplus a_3, b = b_1 \oplus b_2 \oplus b_3) \)
2) \( a_1, a_2, a_3, b_1, b_2, b_3 \)는 동분포(uniformly distributed) 되어 있다.
3) \( i, j = 1, 2, 3 \)에 대하여 랜덤 변수 \( a_i \)와 \( b_i \)는 서로 독립이다.

정의 3-1. 게이트 : \( F_2^6 \rightarrow F_2^n \)에 대하여 \( g \)의 이차 마스킹된 게이트는 다음과 같은 만족시키는 게이트쌍 \((g_1, g_2)\)를 의미한다.

1) \( g_1, g_2, g_3 : F_2^6 \rightarrow F_2^n \)
2) \( g \)의 입력의 입력값 \((a, b) \in F_2^n \) 및 \((a, b)\)의 입력의 이차 마스킹된 신호쌍
   \((a_1, a_2, a_3, b_1, b_2, b_3) \in F_2^6\)에 대하여
   \[ g(a_1, a_2, a_3, b_1, b_2, b_3) \oplus g_1(a_1, a_2, a_3, b_1, b_2, b_3) = g_2(a, b) \]

정의 4-1. 만약 입력의 \( \phi \in \text{Map}_{1, 2, 3, 4, 5, 6} \)와 \( i = 1, \ldots, 6 \)에 대하여 다음과 같은 16개의 값이 동일하다면 게이트 : \( F_2^6 \times F_2^6 \rightarrow F_2^n \)이 이차 G-equivariant 게이트라고 한다: \( a, b, x, y \in F_2^n \)에 대하여

\[
\sum_{a_i \oplus b_i \oplus x_i \oplus y_i = a \oplus b} F_{g_i}(\langle \vec{a}, \vec{b}, \langle \vec{x}, \vec{y} \rangle, \phi) \quad \text{(1)}
\]

여기서 \( \vec{a}, \vec{b}, \vec{x}, \vec{y} \)는 다음과 같이 주어진 벡터이다:

\[
\vec{a} = (a_1, a_2, a_3) \quad , \quad \vec{b} = (b_1, b_2, b_3) \\
\vec{x} = (x_1, x_2, x_3) \\
\vec{y} = (y_1, y_2, y_3)
\]

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

정리 2. 다음과 같이 정의된 게이트 \( g_1, g_2, g_3 : F_2^6 \times F_2^6 \rightarrow F_2^n \)는 이차 G-equivariant 게이트이며 AND 게이트의 이차 마스킹된 게이트이다.

\[
g_1(a_1, a_2, a_3, b_1, b_2, b_3) = a_1 b_1 + a_2 b_2 + a_3 b_3 \\
g_2(a_1, a_2, a_3, b_1, b_2, b_3) = a_1 b_1 + a_2 b_2 + a_3 b_3 \\
g_3(a_1, a_2, a_3, b_1, b_2, b_3) = a_1 b_1 + a_2 b_2 + a_3 b_3
\]

또한 \((a, b) \in F_2^6\)를 계산하기 위하여 \((a, b)\)의 이차 마스킹된 신호쌍을 이용하여 \(g_1, g_2, g_3\)을 계산하는 경우 그 중간 계산값의 확률 분포는 \((a, b)\)에 독립이며 따라서 \(g_1, g_2, g_3\)은 각각의 AND 게이트는 입력 전력분석 공격에 안전하다.

증명. 먼저 \((a, b) \in F_2^6\)를 계산하기 위하여 \((a, b)\)의 이차 마스킹된 신호쌍 \(a_1, a_2, a_3, b_1, b_2, b_3\)을 이용하여 \(g_1, g_2, g_3\)을 계산하는 경우 그 중간 계산값의 확률 분포는 \((a, b)\)에 독립이며 따라서 \(g_1, g_2, g_3\)은 각각의 AND 게이트는 입력 전력분석 공격에 안전하다.

이에 \( \alpha, \beta \in \{0, 1\} \)에 대하여

\[
\text{Pr}(a_1 b_1 + a_2 b_2 + a_3 b_3 = 0 | a = \alpha, b = \beta),
\]

\[
= \text{Pr}(a_1 b_2 + a_2 b_1 + a_3 b_3 = 0 | a = \alpha, b = \beta),
\]

\[
= \text{Pr}(a_1 b_3 + a_2 b_2 + a_3 b_1 = 0 | a = \alpha, b = \beta)
\]

\[
= \frac{5}{8}
\]

이기 때문에 \(a_1 b_2 + a_3 b_3 + a_2 b_1 + a_2 b_2 + a_1 b_3 + a_3 b_1 + a_1 b_3 + a_3 b_1\)의 확률 분포 역시 \(a, b\)에 독립이다.

따라서

\[
g_1(a, b, a_1, a_2, a_3, b_1, b_2, b_3) = a_1 b_1 + a_2 b_2 + a_3 b_3
\]

\[
= ab
\]
이기 때문에 $g_1, g_2, g_3$는 AND 게이트에 대한 이차 마스킹된 게이트가 된다.

마지막으로 $g_1, g_2, g_3$가 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

$$E_{g_i}(a, b, x, y, \phi) \in \mathbb{Z}_{g_{10}} + \mathbb{Z}_{g_{11}} + \mathbb{Z}_{c_{10}} + \mathbb{Z}_{c_{11}}$$

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

입력: $g : F_2^3 \times F_2^3 \rightarrow F_2$
$\phi \in \text{Map}(1, 2, 3, 4, 5, 6)$
$a, b, x, y \in \{0, 1\}$
$i = 1, \ldots, 6$

출력: $E_{g_i}(a, b, x, y, \phi)$
1. $E_{g_i}(a, b, x, y, \phi) = 0$
2. For $a_1, a_2 = 0 \text{ to } 1$
   For $b_1, b_2 = 0 \text{ to } 1$
   For $x_1, x_2 = 0 \text{ to } 1$
   For $y_1, y_2 = 0 \text{ to } 1$
      $a_3 = a_1 \oplus a_2 \oplus a_3$
      $b_3 = b_1 \oplus b_2 \oplus b_3$
      $x_3 = x_1 \oplus x_1 \oplus x_2$
      $y_3 = y_1 \oplus y_1 \oplus y_2$
      $E_{g_i}(a, b, x, y, \phi) = e_{g_i}(a, \phi, y_3, x_3, y), \text{ where}$
      $a = (a_1, a_2, a_3), \ b = (b_1, b_2, b_3), \ x = (x_1, x_2, x_3) \text{ and}$
      $y = (y_1, y_2, y_3)$

IV. AES S-Box 구현에의 응용

AES 알고리즘에 사용하는 함수는 AddRoundKey, MixColumns, ShiftRows, SubBytes가 있다[8]. 이 중에서 SubBytes를 제외하고는 모든 선형 또는 아핀(affine) 함수이기 때문에 마스킹 기법을 적용하는 것은 어렵지 않다. 따라서 이번 장에서는 3 장에서 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 함수를 주로 다룬다.

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

$$GF(2^2) = GF(2)[x]/(x^2 + x + 1),$$
$$GF((2^2)^2)^2 = GF(2)[x]/(x^2 + x + \lambda),$$
$$(\phi = (100), \lambda = (1100)) \in GF(2^8),$$
$$GF(2^8) = GF(2)[x]/(x^8 + x^4 + x^3 + x + 1)$$

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

\[
\begin{array}{cccccccc}
110000010 & 010010110 & 011111001 & 011000011 & 011101011 & 000110101 & 011110111 & 000000101
\end{array}
\]

Fig.1. Pictorial Illustration of $g_1, g_2, g_3$
\[
\sigma(h)^{-1} = \frac{1}{a^{2\lambda} + b(a+b)} (ax + a+b).
\]
즉 \(GF(2^2)\) 상의 역원 계산은 \(GF((2^2)^2)\) 상의 연산을 사용하여 구현 가능하여 이때 \(GF((2^2)^2)\) 상의 비선형 연산은 \(a^{2\lambda} + b(a+b)\)와 같은 곱셈 연산이 된다. 비슷하게
\[
a = a_1 x + a_2, b = b_1 x + b_2 \in GF((2^2)^2)
\]
에 대하여 \(a\)의 역원 및 \(a, b\)의 곱 \(ab\)는 다음과 같이 계산 가능하다(10):
\[
\begin{align*}
\sigma^{-1} &= (a_1 + r, (a_2 + a_1) x^2) (a_1 x + a_1 + a_2), \\
ab &= ((a_1 + r, b_1 + b_2), a_2 b_1 x + (a_1 b_1 + a_2 b_2)).
\end{align*}
\]
결국 \(\sigma^{-1}, ab\)계산은 \(GF((2^2)^2)\) 상의 연산을 사용하여 구현 가능하여 이때의 유일한 비선형 연산은 \(a b\)와 같은 곱셈 연산이다. 따라서 본 논문에서 제안한 AND 게이트에 대한 이차 G-equivariant 게이트를 이용하면 \(GF(2^2)\) 상의 곱셈 연산인 AND 게이트를 (일차) 전력분석 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 게이트레벨 마스킹 알고리즘을 제안하였으며 제안한 방법이 이차 G-equivariant함을 보임으로써 글리치 공격에 강화함을 보인다. 또한 본 논문에서 제안한 방법을 이용하여 AES 알고리즘을 전력분석 공격 및 글리치 공격에 안전하게 구현할 수 있는 방법을 제시하였다.

References

<저자소개>

백유진 (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

최두호 (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: 암호엔지니어링, 부채널 분석, IoT 보안