화이트 박스 블록 암호에 대한 최근 암호분석 기술 동향 연구

(Recent Trends in Cryptanalysis Techniques for White-box Block Ciphers)

오재린*, 임우상**, 김현일**, 서창호***
(Chae rin Oh, Woosang Im, Hyunil Kim, Changho Seo)

요 약

블랙박스 암호는 하드웨어로 구성된 암호화 장치를 기반으로 ‘디바이스와 사용자는 신뢰할 수 있다’는 가정하여 동작하는 암호이다. 그러나 공격자에게 내부 구조가 공개되는 순간 기 추출 등의 다양한 공격이 존재할 때, 동시에 최근 들어 신뢰할 수 없는 개발형 플랫폼에서 암호 알고리즘을 적용하는 경우가 증가하여 블랙 박스 암호 시스템에 대한 위협은 더욱 커져가고 있다. 그로 인해, 개발형 플랫폼에서 암호 알고리즘을 안전하게 동작하고자 암호화 과정에서 암호 키를 숨김으로써 공격자의 키 유출을 어렵게 하는 화이트 박스 암호화 기술이 제안되었다. 하지만, 이러한 화이트 박스 기반 암호는 기존의 암호화는 다르게 정해진 규칙이 존재하지 않아 구조적 안전성을 검증하는 것이 어렵다. 이에 CHES에서는 보다 안전한 화이트 박스 암호 활용을 위해 The Whibox Contest을 주기적으로 개최하여, 다양한 화이트 박스 암호에 대한 안전성 분석이 수행되었다. 이중 2016년 Bos가 제안한 Differential Computation Analysis(DCA) 공격법은 원래까지도 안전성 분석에 널리 활용되고 있는 강력한 화이트 박스 블록 암호에 대한 공격 기법에 해당한다. 이에 본 논문은 화이트 박스 암호에 대한 동향을 분석하고, 화이트 박스 블록 암호에 대한 부패리그 정보 기반 암호분석 기술인 DCA, HODCA 공격 분석 및 관련 대응 기술 동향을 정리한다.

■ 중심어 : 화이트 박스 암호 ; 암호분석 ; 부패리그 분석 ; 차분 개선 분석

Abstract

Black box cryptography is a cryptographic scheme based on a hardware encryption device, operating under the assumption that the device and the user can be trusted. However, with the increasing use of cryptographic algorithms on unreliable open platforms, the threats to black box cryptography systems have become even more significant. As a consequence, white box cryptography have been proposed to securely operate cryptographic algorithms on open platforms by hiding encryption keys during the encryption process, making it difficult for attackers to extract the keys. However, unlike traditional cryptography, white box-based encryption lacks established specifications, making it challenging to verify its structural security. To promote the safer utilization of white box cryptography, CHES organizes The Whibox Contest periodically, which conducts safety analyses of various white box cryptographic techniques. Among these, the Differential Computation Analysis (DCA) attack proposed by Bos in 2016 is widely utilized in safety analyses and represents a powerful attack technique against robust white box block ciphers. Therefore, this paper analyzes the research trends in white box block ciphers and provides a summary of DCA attacks and relevant countermeasures, adhering to the format of a research paper.

■ keywords : White-box cryptography ; Cryptanalysis ; Sidechannel analysis ; Differential Computation Analysis

1. 서 론

블랙박스 암호(Black-box Cryptography)는 하드웨어로 구성된 암호화 장치를 기반으로 작동
되는 암호 기술로, 암호화된 데이터와 관련된 모든 처리가 외부에서 알 수 없도록 구현된다. 즉, 내부 동작 및 알고리즘은 외부로부터의 접근이 차단되어 암호 알고리즘의 내부를 보호하여 동작한다. 그러나 블랙박스 내부가 공개되는 순간 암호 알고리즘과 암호키가 노출되어 안전하지 않고, 최근에는 신뢰할 수 없는 개발형 플랫폼에서 암호 알고리즘을 적용하는 경우가 증가하여 하드웨어 전적으로 의존하는 블랙박스의 경우 암호 보안이 취약해져 안전하게 암호 알고리즘을 동작하고 암호키를 보호하기 위해 화이트 박스 암호 기술(White-box Cryptography)이 제안 및 연구되고 있다([1, 2]).

화이트 박스 암호는 암호화 기술에 소프트웨어의 개념이 도입된 것으로 암호화 알고리즘의 내부의 상황에서 비밀키를 안전하게 보호할 수 있도록 설계되었으며, 공격자에 의한 키 유출을 어렵게 하기 위해 암호 알고리즘을 큰 규모로 분절로 만들고 그 안에 암호 키를 삽입하는 형태로 사용된다. 그러나 화이트 박스 암호는 기존의 블랙박스 암호와는 다르게 정해진 규격이 제한적이지 않아 보다 체계적인 안전성 검증을 필요로 한다. 이러한 문제점을 해결하기 위해 CHES(Workshop on Cryptographic Hardware and Embedded Systems, IACR)에서는 The Whibox Contest를 주기적으로 개최하고 있다. 특히 2017, 2019년도에 화이트 박스 AES에 대한 안전성을 분석하고 있으며, 그중 DCA(Differential Computation Analysis) 공격은 부채널 공격 기법에 기반한 것으로 현재 화이트 박스 AES(Advanced Encryption Standard) 안전성 분석에 많이 활용되고 있다. 이러한 DCA 공격은 부채널 공격에 대한 대응 기술 중 하나인 마스킹 기법을 활용하여 대응이 가능하나, 해당 마스킹 기법은 고도화된 공격의 HODCA(Higher Order DCA) 공격에 취약함이 발견되었다. 본 논문은 화이트 박스 암호에 대한 동향을 분석하고, 화이트 박스 블록암호에 대한 부채널 정보 기반 암호 분석 기술인 DCA, HODCA 공격 분석 및 관련 대응 기술 동향을 정리한다.

II. 화이트 박스 암호의 보안 분석

1. 화이트 박스 암호

기존의 암호 알고리즘은 암호 키가 믿을 수 있는 장차에서 안전하게 유지 관리되는 가정하에 동작되었지만, 화이트 박스 암호는 공격자가 내부에서 암호화 키를 알 수 있다는 가정하에 보안 대책을 마련한다. 따라서 화이트 박스 암호는 신뢰할 수 없는 환경에서 실행되는 소프트웨어 구현에서 암호 키가 노출되지 않도록 보호하여 공격자가 암호화 키를 쉽게 유출할 수 없도록 하는 기술로 암호화 키 정보를 소프트웨어 보안한 알고리즘에 삽입하는 방법이다. 그림 1-(a)는 블랙박스 암호 알고리즘을 그림 1-(b)는 화이트 박스 암호 알고리즘의 구현도를 나타낸다.

![화이트 박스 암호 구현](image)

그림 1. 화이트 박스 암호 구현

2. 화이트 박스 암호 구현

화이트 박스 암호 원리는 알고리즘을 큰 규모로 분절로 만들고 그 안에 암호 키를 암호 알고리즘과 뒤섞인 형태로 숨겨둔다. 따라서 테이블 전체가 복록이라 볼 수 있으며, 규모 웨이블과 결과 키를 숨
表 1. AES 라운드 연산 과정

Algorithm 1 AES 라운드 연산 과정

1: State ← plaintext
2: AddRoundKey(state, \( k^0 \))
3: for \( r = 1 \) to \( 9 \):
4:     SubBytes(state)
5:     ShiftRows(state)
6:     MixColumns(state)
7:     AddRoundKey(state, \( k^r \))
8: SubBytes(state)
9: ShiftRows(state)
10: AddRoundKey(state, \( k^{10} \))

表 2. 화이트 박스 AES 라운드 연산 과정

Algorithm 2 화이트 박스 AES 라운드 연산 과정

1: State ← plaintext
2: for \( r = 1 \) to \( 9 \):
3:     ShiftRows(state)
4:     AddRoundKey(state, \( k^{r-1} \))
5:     SubBytes(state)
6:     MixColumns(state)
7:     ShiftRows(state)
8: SubBytes(state)
9: ShiftRows(state)
10: AddRoundKey(state, \( k^{10} \))

이는 데 효율적이지만 실용적이지 못하게 된다. 본 절에서는 화이트 박스 AES를 예시로 기존원리와 구현 체계를 다룬다.

가. 화이트 박스 AES 구현

화이트 박스 AES는 암호 키를 숨기기 위해 다양한 방법으로 구현될 수 있지만, 본 절에서는 S.Chow[1]에서 제시된 화이트 박스 AES 구현 방법을 기술한다. 먼저 기존의 AES와 화이트 박스 AES의 라운드 연산 과정에 약간의 차이가 존재한다. 표 1은 기존의 AES 라운드 연산 과정을 나타내며 표 2는 화이트 박스 AES 라운드 연산 과정을 나타내고 있다. 표 1을 살펴보면 기존의 AES는 AddRoundKey 연산을 먼저 수행한 후 SubByte, ShiftRow, Mixcolumn, AddRoundKey 순서로 1 라운드부터 9라운드까지 수행하고, 마지막 10라운드에서 SubByte, ShiftRow, AddRoundKey 연산을 수행한다. 그러나 표 2를 보면 알 수듯이 화이트 박스 AES는 AddRoundKey 연산을 수행하지 않고 바로 라운드 연산을 수행한다. 또한, 화이트 박스 AES는 AES와 다르게 ShiftRow, AddRoundKey, SubByte, Mixcolumn 순서로 1 라운드부터 9라운드까지 수행하고, 마지막 10라운드에서 ShiftRow, AddRoundKey, SubByte, AddRoundKey 연산을 수행한다.

이러한 연산 과정을 테이블로 만들어 연산을 수행하게 되는데 화이트 박스 AES의 테이블은 크게 4가지로 구분할 수 있으며, 그림 2는 각 테이블의 구조를 나타낸다. 그림 2-(a)는 Type II 테이블로 암호 알고리즘 연산에서 화이트 박스 AES 라운드 연산이 포함되어있으며, 그림 2-(b)는 Type III 테이블로 화이트 박스 AES의 연산을 수행하는 테이블을 의미하며 Type II 테이블에서 제작된 테이블로, Type III 테이블의 연산을 수행할 수 있는 XOR 연산을 수행하고 그림 2-(c)는 Type V 테이블로 최종 라운드의 연산을 수행한다.

![그림 2. 화이트 박스 AES 테이블 구조](image-url)
이러한 백만을 화이트 백스 AES 연산에 적용할 
화이트 백스 AES의 연산 과정은 표 3과 같이 진행 
된다. 1라운드부터 9라운드까지 TypeII, TypeIV, 
TypeIII, TypeIV 테이블을 수행하고 마지막 10라운 
드에서 TypeV 테이블을 수행하게 된다.

표 3. 테이블이 적용된 화이트 백스 AES 연산 과정

<table>
<thead>
<tr>
<th>Round 1-9</th>
</tr>
</thead>
<tbody>
<tr>
<td>TypeII → TypeIV → TypeIII → TypeIV</td>
</tr>
<tr>
<td>Round 10</td>
</tr>
<tr>
<td>TypeV</td>
</tr>
</tbody>
</table>

화이트 백스 암호에서 테이블 연산은 특정 암호 
알고리즘의 라운드 연산을 구현하는 데 사용된다. 
화이트 백스 AES에서는 AES의 각 라운드 연산을 
테이블 연산을 통해 구현하였는데, 화이트 백스 
AES와 마찬가지로 DES 및 ARX 암호에서도 라운 
드 연산을 테이블 연산을 활용하여 암호 연산을 
구현한다[4,5].

3. 화이트 백스 암호 동향

화이트 백스 암호는 안전하고 효율적인 암호 기술 
을 개발하는 것에 초점을 맞춰 있다. 앞서 언급했 
듯이 화이트 백스 암호 구조에는 표준이 없는 보안 
수준을 평가하기 어렵기 때문에 보안 분석에 대한 연 
구가 진행되고 있고, 다양한 응용 분야에서 연구가 
수행되고 있다. 실제로, 화이트 백스 암호에 대한 보 
안 분석에 대한 연구가 진행되고 있는데, 구조적 보 
안 강화를 위해서 키 추출, 역공학, 변조와 같은 공격 
으로부터 보호하기 위한 새로운 방법을 개발하고 있 
으며, 난독화, 코드 변형, 데이터 다양화 같은 기술을 
활용하여 화이트 백스 암호의 보안성을 향상시키는 
연구가 진행되고 있다[6]. 또한, 암호화 키를 보호하 
기 위해 키 분할, 키 혼합, 키 섞기 같은 기술을 탐구 
하여 화이트 백스 시스템에서의 키 저장 및 관리의 
보안성을 향상시키는 연구가 진행되고 있다[3].

특히 Differential Computation Analysis(DCA) 
공격, 대수적 공격, 부채널 공격과 같은 강력한 공격 
에 대한 보안성을 분석하고 취약점을 식별하며 대응 
책을 개발하는 노력이 기울이고 있다[6-11]. 
마지막으로 다양한 응용 분야에서 활용할 수도 있 
록 연구가 수행되고 있다. 화이트 백스 암호는 은행 
및 디지털 지배권 보호와 같은 분야에서 활용될 수 
있으며 이와 같은 응용 연구는 IoT 장치의 보안 강 
화와 클라우드 보안과 같은 다양한 분야에서 진행되 
고 있다[2].

전반적으로 화이트 백스 암호의 지속적인 연구는 
화이트 백스 시스템에 대한 공격에 대응하고 개방적 
이고 신뢰할 수 있는 환경에서 민감한 암호 정보를 
보호하기 위한 안전하고 실용적인 솔루션을 개발하 
는 것을 목표로 하고 있다.

III. DCA 공격 및 관련 대응 기술 분석

2.3절에서 언급하였듯이, 화이트 백스 암호는 기존 
암호와는 다르게 알고리즘 구현에 대한 일련의 표준 
이 존재하지 않아 보안 수준을 평가하기 어렵다. 그 
리나, 화이트 백스 암호의 여러 장점으로 인해 매우 
높은 성능을 갖고 있어 이에 대한 다양한 보안 분 
석 연구가 진행되고 있다. 특히, 주기를 기준으로 개별되 
는 ‘The WhiBoX Contest’를 통해 화이트 백스 암 
호에 대한 안전성을 분석하고 있다. 그 중, DCA 기 
반 공격이 대표적인 화이트 백스 암호 분석 기술에 
해당하며, 본 장에서는 DCA 공격 기반 기술 및 관 
련 대응 기술에 대한 분석을 수행한다.

표 4. 응용 정리

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T_{v,i}^e$</td>
<td>SubByte 수행 결과</td>
</tr>
<tr>
<td>$T_{v,i}^m$</td>
<td>Mixcolumn 수행 결과</td>
</tr>
<tr>
<td>$T_{w}$</td>
<td>마스킹이 적용된 $T_{v,i}^m$</td>
</tr>
<tr>
<td>$m^T$</td>
<td>마스킹의 전치</td>
</tr>
<tr>
<td>$(e_1, ..., e_t)$</td>
<td>계산 trace</td>
</tr>
<tr>
<td>$Sec T$</td>
<td>$T_{w} ⊗ m^T$</td>
</tr>
<tr>
<td>$Non4(x)$</td>
<td>4비트 비선형 테이블 연산</td>
</tr>
<tr>
<td>$NSec T$</td>
<td>$Non4(T_{w}) ⊗ m^T$</td>
</tr>
</tbody>
</table>
1. DCA 공격

DCA 공격[6]은 화이트 박스 암호에 대한 공격 중 하나이다. DCA 공격은 DPA(Differential Power Analysis) 및 CPA(Correlation Power Analysis)와 같은 부채널 압호분석 기법을 화이트 박스 암호에 적용한 공격으로 화이트 박스 암호의 테이블을 알지 못하더라도 비밀 정보를 복원할 수 있다. DCA 공격은 바이너리 수집 도구를 사용하여 메모리 데이터 정보를 수집하며, 수집한 데이터 중 특정 비트의 연산 정보를 활용하여 공격자는 화이트 박스 암호의 비밀 정보를 추론할 수 있다. 따라서 특정 비트의 연산 정보를 활용하여 화이트 박스 암호의 키 후보군을 통해 연산 중간값을 계산하고, 이때 계산된 중간 값과 수집된 바이너리 메모리 데이터 사이의 상관관계 수가 높은 지점을 유도함으로써 정확한 키를 추출할 수 있다. 그러므로, DCA 공격은 통해 테이블은 알지 못하더라도 화이트 박스 암호의 비밀 정보를 복원할 수 있다. 그림 3은 DCA 공격 과정을 나타낸다.

![그림 3. DCA 공격](image)

2. DCA 공격 대응 기술

DCA 공격은 마스킹 기법을 통해 대응할 수 있다. 본 절에서는 3.2절에서 언급된 마스킹 기법을 화이트 박스 AES에 적용하여 대응하는 과정을 기술하고 있다.

마스킹 기법은 부채널 공격에 대한 대응 기술 중 하나이다. 암호화 중 생성된 민감한 정보에 무작위 값을 추가하고 관련 없는 보조 정보를 통합함으로써, 마스킹은 공격자가 민감한 정보를 보조 정보와 연관을 가지지 않도록 하는 대응 기술이다. 따라서, 암호 알고리즘 동작 중간에 무작위 값을 추가하기 위해서는 모든 연산에 대해 무작위 값을 생성하고 계산해야 한다. 그러나 화이트 박스 환경에서는 내부 구조가 드러나기 때문에 마스킹 기법의 실행 결과는 드러나게 되고 그로 인해 화이트 박스 압호분석에서는 이러한 무작위 값 생성 및 연산 과정이 노출된다. Lee 등은 마스킹 난수 지수의 테이블 설정에 포함하는 구현 방법을 고안하였는데[7], Chow의 화이트 박스 AES에서 Type II 테이블을 마스킹을 포함하기 위해 마스킹 함수 M이 Type II 테이블의 중간에 추가하였다. 마스킹 함수 M은 독립적으로 랜덤한 마스크를 생성한 후에 XOR하는 연산에 참여하도록 마스크를 랜덤하게 생성하는 과정을 수행한다. 따라서 기존 Type II 테이블의 2배에 해당하는 공간을 요한다.

그림 4-(a)는 기존 Type II 테이블 구조를 나타내며 그림 4-(b)는 마스킹 기법이 적용된 Type II 테이블 구조를 나타낸다.

![그림 4. Type-M 테이블](image)
3. Higher Order DCA(HODCA) 공격

본 절에서는 DCA가 고도화된 HODCA 공격[8] 기법에 대해 분석한다. HODCA 공격은 고차 부채널 분석 기법을 적용한 것으로 마스킹 대응 기술이 적용된 암호에 대해서, 획득한 부채널 정보의 두 개 이상의 시점을 조합하여 가려진 정보를 드러내는 분석 기법이다. 따라서 HODCA는 전처리 단계와 DCA로 구성되는데, \( (v_1, ..., v_P) \)를 계산 trace라고 할 때, 뇌차 DCA는 trace의 조합을 계산하여 뇌차 trace \( (v_{i1}, ..., v_{iP}) \)를 형성한다. 이때, \( v_{ij} \)는 \( 1 \leq i \leq P \)에 대한 \( (v_1, ..., v_P) \)의 \( n \)개의 노드 함이며, 계산된 뇌차 trace에 대하여 DCA 공격을 수행하게 된다. 그러나 HODCA 공격은 [8]에서 제안된 마스킹 기법에 대한 공격 기법으로 3.2절에서 언급된 마스킹 기법이 적용된 암호로부터 비밀 정보를 추출하지 못한다.

4. 개선된 Higher Order DCA(HODCA) 공격

본 절에서는 3.3절에서 언급된 HODCA를 개선한 HODCA 공격[9]에 대해 분석한다. 3.3절에서 언급했듯이 HODCA 공격은 획득한 정보의 두 개 이상의 시점을 조합하여 가려진 정보를 드러내는 분석 기법이다. 즉, 공격자는 조합 대상이 되는 연산 시점을 셀링하게 파악해야 한다. HODCA 공격은 단순 계산 분석(Simple Computation Analysis, SCA)을 통해 조합 지점을 결정하고, 결정된 지점의 연산 정보를 조합한 후 고차 분석 기법을 사용하여 공격을 수행한다. 마스킹이 적용된 화이트 백스 AES에서 공격 시점은 Type II-M 테이블의 출력 데이터가 해당되고, 이를 단순 계산 분석(SCA)를 통해 파악할 수 있다.

가. 단순 계산 분석(SCA)

본 절에서는 단순 계산 분석을 통해 공격자가 공격 시점을 파악하는 방법에 대해 기술한다. 그림 5-(a)는 바이너리 분석 도구를 통해 수집한 주소 바이너리 trace로 가로축은 암호의 연산 시간, 세로축은 메모리 주소값의 최하위 1바이트 값을 나타낸다. 그림 5-(a)에 보여지듯이, 화이트 백스 AES 연산으로 추측할 수 있는 9개의 서로 같은 패턴을 확인할 수 있다. 화이트 백스 AES의 경우, TypeII, Type IV, TypeIII, TypeIV 테이블 순서로 연산이 수행된다. 이때, TypeII 테이블 연산 이후 MixColumn 연산을 수행하기 위해 TypeIV 테이블이 수행되며, TypeIV 테이블이 가장 많은 테이블 참조 연산을 수행한다. 또한, 마지막 10라운드에서는 MixColumn 연산을 수행하지 않기 때문에 9개의 서로 같은 패턴이 화이트 백스 AES의 각 라운드를 의미한다. 동일한 9개의 패턴 중 한 라운드 연산을 의미하는 부분을 확대한 그림이 그림 5-(b)이다. 앞서 언급하였듯이 TypeIV 테이블이 가장 많은 연산을 차지하고 있다. TypeII-M 테이블 연산 후 XOR 연산을 위한 TypeIV 테이블을 TypeIV-2 테이블이라 표기하며,
Type III 테이블 연산 후 진행되는 Type IV 테이블 을 Type IV–III 테이블로 표기한다. 한 라운드 연산 과정을 보면 Type II–M 테이블 연산 이후 Type IV–II 테이블 연산이 수행되고, Type III 테이블 연산 이후 Type IV–III가 수행된다. 이때, Type II–M 테이블 출력은 Type III 테이블 출력보다 더 많은 비트 를 가져 Type IV–II 테이블에 Type IV–III 테이블보다 더 많은 연산을 수행하여 구분할 수 있다. 따라서 그림 5-(b)와 같이 각 테이블의 연산 시점은 특정할 수 있다.

나. 고차 분석 기법

(1) 생존 비트 조합 공격

단순 계산 분석(SCA)을 통해 Type II–M 테이블의 연산 시점은 파악한 것을 토대로 고차 분석 기법을 적용하여 공격할 수 있다. 먼저 Type II–M 출력 64비트 중 마스크에 해당하는 32비트 정보를 마스킹이 적용된 $T_k$ 양상 결과에 XOR하여 기존의 정보를 복원한다. 단순 계산 분석을 통해 공격자는 Type II–M 테이블의 연산 위치를 정확하게 파악할 수 있으며, Type II–M 테이블 연산 위치의 데이터 바이너리 trace를 획득하여 해당 비트들의 XOR 연산 과정 후 2차 trace를 생성할 수 있다. $T_k$의 결과 값에 마스크가 적용된 테이블의 출력은 $T_m$이라고 할 때 2차 trace는 다음 수식을 통해 생성할 수 있다.

$$N_{Sec} \cdot T = Non4(T_m) \oplus m^T$$ (2)

$Non4$은 테이블 출력값에 추가로 조합하는 4비트 비선형 테이블 연산을 의미하며, 적절한 임계점을 설정하여 그보다 높은 기 상관계수가 발생할 때까지 공격을 반복 수행한다. 생존 비트 조합 공격에서 $T_m$과 $m$에 대한 2차 trace는 연산 결과값과 같은 값을 가지며, 화이트 박스 AES 라운드 연산에서 Type II–M 테이블의 출력값을 의미한다. 그러나 4 비트 비선형 테이블을 조합하는 연산을 추가함으로써 분해 Type II–M 테이블 출력값에서 빠르게 나타낼 수 있고, 정확한 비밀 값 복원이 가능하다. 이때, 비트의 특성은
表 5. DCA 및 HODCA 관련 연구 동향

<table>
<thead>
<tr>
<th>Method</th>
<th>Objectives</th>
<th>Attack</th>
<th>Countermeasure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lee et al. [7]</td>
<td>마스킹 기법</td>
<td>X</td>
<td>○</td>
<td>- 기존 테이블 2배의 공간 요구</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- 고차 분석 기법에 취약</td>
</tr>
<tr>
<td>이예한 et al. [9]</td>
<td>개선된 HODCA</td>
<td>○</td>
<td>X</td>
<td>- 공격 시점 파해 가능</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- 비선형 인코딩 악화 가능</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- 개선된 마스킹 기법[7] 파해 가능</td>
</tr>
</tbody>
</table>

비선행 인코딩 이후에도 특정 비트가 화이트 박스 AES 연산 중간값의 성질과 유사한 경향을 나타내는 정도를 의미한다. 이러한 고차 분석 기법을 사용하여 공격을 수행할 경우 모든 비트의 키를 올바르게 찾아낼 수 있을 것으로 판단된다.

화이트 박스 AES는 DCA 공격 기법에 취약하며 [6] 이러한 공격에 대응하기 위해 마스킹 기법이 제안되었지만 기존 테이블보다 2배의 공간이 필요하며 고차 분석 기법에 취약하다[7]. 마스킹 기법이 적용된 화이트 박스 AES는 고차 분석 기법인 HODCA에 취약하여, 현재 이러한 HODCA 공격에 대응하기 위해 SEL 마스킹 및 서플링 기법이 제안되었지만, 효과적으로 공격에 대응하지 못한다. 따라서 HODCA 공격 기법에 대응하기 위한 연구가 필요하다. 그림 6은 화이트 박스 악호에 대한 공격과 관련 대응기법에 관한 도식을 도로에 따라 나타내고 있으며, 표 5는 공격 기법과 대응기법 관련 연구 동향 논문에 대한 분석을 나타내고 있다.

IV. 결론

본 논문에서는 화이트 박스 악호의 연구 동향을 분석하고 DCA, HODCA 공격 및 관련 대응 기술을 정리한다. 화이트 박스 악호는 안전하고 효율적인 악호 기술을 개발하는 것에 초점이 맞춰져 있다. 구조적 보안을 강화하여 화이트 박스 악호의 보안성과 악호화 기에 대한 보안성을 향상시키기 위한 연구가 수행되고 있으며, 다양한 공격에 대한 보안성을 분석하여 대응책을 개발하는 노력을 기울이고 있다. 따라서 화이트 박스 악호에 대한 공격에 대응하고 안전하고 성능적인 화이트 박스 악호를 개발하기 위한 지속적인 연구가 필요하다.

화이트 박스 악호는 DCA 공격에 취약하다고 할 수 있다. 화이트 박스 악호는 DCA 공격에 대응하기 위해 난수를 랜덤한 난수의 알려진 정보를 보호하는 마스킹 기법이 제안되었지만 기존 테이블을 2배의 공간이 요구되었으며, HODCA 공격 기법을 통해 추가적인 취약점이 발견되었다. 따라서 화이트 박스 악호는 HODCA 공격으로부터 안전하지 않으며, 화이트 박스 악호의 안전성을 개선하기 위한 연구가 필요하다. 즉, HODCA 공격에 대한 대응기법의 지속적인 연구가 필요하다.

또한, 최근 들어 인공지능 기반 악호 분석 기술이 다양하게 연구되고 있다[12-20]. 이들은 트레드있는 기반 블록 악호에 대해, 특정 차분 값을 갖는 평문 및 악호문 생성을 입력받아 이에 대해 데이터 분석을 수행하여 일련의 분류(classification) 모델에 해당하는 난수값
REFERENCES


[2] 김신호, 이윤경, 정병호. "화이트 박스 암호 및 응 용 기술 동향 분석" 『전자통신신문학분석』 제5권 제5호, 137-146쪽, 2010년 10월

[3] 화이트박스 암호화 - 앱 보안의 미래(2022), https://www.appsealing.com/kr/%ED%99%94%EC%9D%B4%ED%8A%B8%EB%B0%88%EC%8A%A4-%EC%98%94%ED%86%B8%ED%99%A4/ (accessed Jan., 11).


[21] 채정남, "VGGNet 을 활용한 식재분류 인공지능 알고리즘 구현," 스마트마더어치널 제10권 제1호 3 2-38쪽, 2021년

[22] 윤기하, 박성모, "LEA 암-복호화 블록 파이프라 인 구현 연구," 스마트마더어치널 제6권 제3호 9-1 4쪽 2017년

저 자 소 개

오채린(학생회원)

2022년 공주대학교 응용수학과 학사
2023년 공주대학교 응용수학과 석사과정

<주관심 분야> 인공지능, AI 기반 암호 분석, 부채널 분석 등

임우성(학생회원)

2021년 공주대학교 응용수학과 학사
2023년 공주대학교 융합과학과 공학석사
2023년 공주대학교 융합과학과 박사과정

<주관심 분야> 양자네임암호, 부채널 분석, 인공지능 등

김현일(정회원)

2014년 공주대학교 응용수학과 학사
2016년 공주대학교 융합과학과 공학석사
2019년 공주대학교 융합과학과 공학박사
2020년~2022년 대구경북과학기술원 박사후연 구원
2022년~2023년 공주대학교 연구교수
2023년~현재 조선대학교 정보통신공학부 조교수

<주관심 분야> 암호기술, 프라이버시 보존형 연합학습 기술, DID 인증 기술 등

서창호(정회원)

1990년 고려대학교 수학과 학사
1992년 고려대학교 수학과 박사학사
1996년 고려대학교 수학과 박사학사
1996년~1999년 국방과학연구소 신입연구원
1999년~2000년 한국전자통신연구원 신입연구원, 박상
2000년~현재 공주대학교 응용수학과 교수

<관심분야> 암호알고리즘, PKI, 무선인터넷 보안 등