Journal of Korea Society of Industrial Information Systems Vol.29 No.3, Jun. 2024 :23-40
http://dx.doi.org/10.9723/jksiis.2024.29.3.023 ISSN:1229-3741

e-Cryptex: 물리적으로 복제 불가능한 기능을 활용한 역공학 방지 기법

(e-Cryptex: Anti-Tampering Technology using Physically Unclonable Functions)

최 지 원[1], 박 선 용[2], 이 중 희[3]*, 이 형 규[4], 이 규 호[5], 장 우 현[5], 최 준 호[5]
(Jione Choi, Seonyong Park, Junghee Lee, Hyung Gyu Lee, Gyuho Lee, Woo Hyun Jang, and Junho Choi)

요 약 하드웨어 공격은 암호화 키 혹은 회로 설계와 같은 민감한 정보를 훔치기 위해 물리적인 역공학 작업을 수반한다. 암호화와 난독화는 대표적인 대응책이지만, 공격자가 키를 알아내면 무력화된다. 이 문제를 해결하기 위해 본 연구에서는 물리적으로 복제할 수 없는 기능 (Physically Unclonable Function)을 위변조 방지 방패로 활용하는 e-Cryptex를 제안한다. PUF는 난수 생성기 역할을 하며 복제나 복원할 수 없는 고유한 물리적 변형을 사용해 변조 방지 메커니즘을 강화한다. e-Cryptex는 시스템 구조를 보호하고 키를 생성하기 위해 PUF를 실드로 사용한다. 실드를 변조하면 키가 파괴된다. 본 논문은 e-Cryptex가 PUF 보안 요구 사항을 충족하며 실드를 뚫거나 완전히 파괴하는 변조 시도를 탐지하는 데 효과적임을 입증한다. 각 보드는 정상적인 조건에서 일관되게 같은 키를 생성하는 동시에 여러 보드에서 키 고유성을 보여준다.

핵심주제어: 보안, PUF, Shield, 안티템퍼링

Abstract Hardware attacks involve physical reverse engineering efforts to steal sensitive information, such as encryption keys and circuit designs. Encryption and obfuscation are representative countermeasures, but they are nullified if adversaries manage to find the key. To address this issue, we propose e-Cryptex, which utilizes a Physically Unclonable Function (PUF) as an anti-tampering shield. PUF acts as a random number generator and relies on unique physical variants that cannot be replicated or restored to enhance anti-tampering mechanisms. e-Cryptex uses PUF as a shield to protect the system's structure and generate the key. Tampering with the shield will result in the destruction of the key. This paper demonstrates that e-Cryptex meets PUF security requirements and is effective in detecting of tampering attempts that pierce or completely destroy the shield. Each board consistently generates the same key under normal conditions, while also showing key uniqueness across different boards.

Keywords: Security, PUF, Shield, Anti-tampering

* Corresponding Author: j_lee@korea.ac.kr
Manuscript received March 29, 2024 / revised May 02, 2024 / accepted June 02, 2024
1) 고려대학교 정보보호대학원, 제1저자
2) 고려대학교 사이버국방학과, 제2저자
3) 고려대학교 정보보호대학원, 교신저자
4) 덕성여자대학교 소프트웨어전공
5) LIG 넥스원

1. 서 론

오늘날의 상황에서 글로벌 분쟁이 증폭되면서 특히 하드웨어 시스템 영역에서 위변조 방지 기술의 중요성이 더욱 강조되고 있다. 공격자가 역공학을 성공적으로 수행하면 최첨단 기술이 오용될 뿐만 아니라 보안 기능이 손상되어 기기를 무단으로 조작할 수 있게 된다. 하드웨어 소유자는 막대한 개발 비용으로 제품을 연구하였지만, 공격자는 이러한 비용 없이도 역공학을 통해 대량의 위조 제품을 만들 수 있다. 이러한 위협은 상당한 자원과 강력한 동기로 무장한 국가 지원 공격자들이 취약점을 악용하도록 유도하는 무기 시스템에서 특히 더 심각한 결과를 초래한다 (IISS, 2021).

공격자들의 역량이 계속 발전함에 따라 공격의 초점이 소프트웨어에서 하드웨어로 눈에 띄게 이동하고 있다 (DarkReading, 2022). 하드웨어 기반 공격은 표적이 되는 하드웨어의 복잡한 동작을 포괄적으로 이해하는 것을 목표로 하므로 이미징, 프로빙, 사이드 채널 공격과 같은 비침입적 방법과 지연 및 주사 전자 현미경과 같은 보다 침습적인 기술을 사용한다. 이러한 방법은 표적이 되는 장치의 물리적 무결성을 변경할 필요 없이 정보를 추출하는데 능숙하다. 디지털 통합이 만연한 시대에 역공학 공격으로부터 하드웨어를 보호해야 할 필요성이 그 어느 때보다 강조되고 있다. 강력한 암호화 메커니즘, 하드웨어 난독화, 변조 방지 구성 요소의 배포는 하드웨어 보안을 강화하기 위한 핵심적인 대응책으로 부상하고 있다.

이러한 다각적인 문제에 대응하기 위해 용접, 코팅, 캡슐화, 센서 통합과 같은 물리적 방법과 보안 프로세서, 명령어 세트 무작위화, 암호화, 난독화, 워터마킹과 같은 정교한 하드웨어 및 소프트웨어 기술을 아우르는 다양한 위변조 방지 기술이 고안되었다 (Suh et al., 2003; Boyd et al., 2010; Zuo et al., 2022). 이러한 광범위한 조치에도 불구하고 역공학 시도에 취약한 소프트웨어는 특정 장치의 전체 기능을 이해하려는 공격자의 주요 표적이 되는 경우가 많다. 암호화되어 있더라도 소프트웨어와 암호화 키는 메모리나 레지스터에 저장되므로 안전한 저장 방법이 아니다. 한 가지 제안된 해결책은 전용 하드웨어를 사용하는 것이다. 대표적인 기술이 신뢰 플랫폼 모듈(Trusted Platform Module)로, 키를 하드웨어에 저장하고 내부에 암호화 및 복호화 회로를 갖추고 있어 키가 TPM을 벗어나지 않는다. 그러나 Choi and Kim(2012)의 연구에 의하면 TPM은 소프트웨어 공격에는 안전하지만, 물리적 공격에는 안전하지 않은 것으로 알려져 있다. 즉, 물리적 공격자 TPM 내부에 직접 액세스하면 키를 읽을 수 있다.

또한, 많은 연구에서 하드웨어 보안을 위한 보호 수단으로 실드를 사용하는 방법을 모색했다 (Kash et al., 1962; Kaul et al., 2002; Sarto et al., 2002; Lee et al., 2009; Cruciani et al., 2019). 그러나 이러한 연구에서 강조된 중요한 우려 사항은 이러한 실드의 잠재적 취약성이다. 변조 방지 센서나 장치가 장착된 액티브 실드를 배치했음에도 불구하고 여전히 중요한 문제가 남아 있는데, 바로 실드가 손상되기 쉽다는 것이다. 특히, Shi et al.(2018)에 의하면 공격자가 전원이 차단된 후 실드를 분리했다가 다시 부착하면 실드가 원활하게 기능을 재개하는 경우가 많다. 이는 하드웨어 변조에 대한 강력한 방어 수단으로서 실드의 효과에 대한 의구심을 불러일으킨다. 따라서 하드웨어 보안의 최첨단 기술을 발전시키고 정교한 공격에 대한 탄력적인 보호를 보장하기 위해서는 이러한 한계를 해결하는 것이 중요하다.

이 문제를 해결하기 위해 물리적으로 복제 불가능한 기능(PUF)을 활용하여 암호화 키 생성기와 물리적 역공학 공격에 대한 강력한 대응책이라는 두 가지 목적을 달성하는 혁신적인 접근 방식인 e-Cryptex를 소개한다. Cryptex는 영화 다빈치 코드에 등장하는 장치로 비밀 지시를 전달하는 역할을 한다. 올바른 비밀번호로 열면 그 내용을 확인할 수 있지만, 강제로 열면 Cryptex 내부의 화학 물질이 흘러나와 내용물을 파괴한다. 본 연구에서는 Cryptex와 유사한 아이디어를 착안하여 이름을 e-Cryptex로 정했다. e-Cryptex는 물리적 변조에 취약한 기존 키 저장 방식에 대한 보호 장치로 PUF를 활용한

다. PUF의 일부는 방패로 사용된다. 공격자가 실드를 뚫지 않는 한 시스템 내부에 접근할 수 없다. 그러나 실드를 파괴하면 키를 생성하는 PUF가 파괴되기 때문에 키를 다시 생성할 수 없다. PUF는 동일한 값을 갖는 저항-커패시터 회로(RC 회로) 두 개 사이의 충전 속도 차이를 활용한다. 이 방식은 프로세스의 자연스러운 변화를 기반으로 개발자가 예측할 수 없으므로 시스템의 복원력을 보장한다. e-Cryptex는 실드의 일부를 파괴하거나 다시 부착하는 물리적 역공학 공격에 대해 탐지하는 데 효과적이다. 이는 PUF가 손상되면 키가 변경되기 때문이다. 다음으로, 키 생성기로서 e-Cryptex를 사용하는 고유성과 견고성을 증명한다. 이는 일반적인 상황에서 동일한 보드에서 일관성을 유지하면서 각기 다른 보드에서는 고유한 키를 생성함으로써 달성할 수 있다.

본 논문의 기여는 다음과 같다.

- 물리적 역공학 공격에 대한 선구적인 PUF 기반 대응책인 e-Cryptex를 소개한다.
- e-Cryptex에서 PUF가 실드 역할을 할 수 있음을 입증한다.
- 실험을 통해 암호화 키 생성기로서 e-Cryptex의 견고성과 고유성을 포괄적으로 증명한다.
- 물리적 변조에 대응하여 e-Cryptex에서 생성된 값의 변화를 탐지 가능함을 입증하는 경험적 증거를 제시한다.

본 논문의 1장에서는 연구의 배경과 필요성, 다음 2장에서는 여러 PUF를 비교 분석하고 하드웨어 역공학의 이론적 토대를 살펴본 후 3장에서는 실드를 활용한 역공학 방지 기법에 대한 관련 학술 동향에 관해 설명한다. 4장에서는 e-Cryptex의 개념과 설계에 관해 설명하고 5장에서는 e-Cryptex의 보안 측면 평가와 물리적 공격에 대한 실험 결과를 정리한다. 이 논문은 6장으로 마무리되며, 6장에서는 하드웨어 보안에 대한 e-Cryptex의 연구 결과를 종합하고 향후 연구 방향을 제시하는 포괄적인 결론을 제시한다.

2. 배경 지식

이 장에서는 e-Cryptex에 대해 수행한 배경 지식에 대한 포괄적인 개요를 설명한다. 우선, PUF의 핵심 개념을 설명하고 다양한 PUF를 비교 분석한다. 그다음에는 다양한 물리적 공격 방법과 하드웨어 보안에 미치는 잠재적 파급 효과에 관해 설명한다.

2.1 Physically Unclonable Funtions (PUFs)

PUF는 하드웨어 제조 과정의 자연스러운 변화로 인해 복제할 수 없는 고유한 특성이다. PUF는 지원하는 특정 기능에 따라 다양한 형태로 나타나며, 흔히 하드웨어 지문이라고도 한다(Maes, 2013). PUF는 카드 내 난수 생성기(TRNG) 및 집적 회로(IC) 칩을 비롯한 다양한 영역에 걸쳐 적용되고 있다.

이전의 PUF에 대한 국제 표준은 주로 견고성(robustness)과 고유성(uniqueness)만을 보안 요구 사항으로 강조했지만, 현재 ISO/IEC 20897-1 (2022) 표준은 6가지 주요 보안 요구 사항을 제시한다.: 견고성(robustness), 무작위성(randomness), 고유성(uniqueness), 변조 방지(tamper-resistance), 수학적 복제 불가능성(mathematical unclonability), 물리적 복제 불가능성(physical unclonability). 견고성은 주어진 장치에 대해 일관된 출력을 보장하고, 무작위성은 여러 도전에 대해 충분히 무작위화된 응답을 보장하며, 고유성은 동일한 디자인 간에도 고유한 값을 생성한다. 변조 방지 기능은 사이드 채널 및 역공학 분석을 포함한 물리적 공격으로부터 안전하다. 수학적 복제 불가능성은 PUF 동작을 단방향 함수로 만들어 역공학 공격을 어렵게 만든다. 물리적 복제 불가능성은 장치의 고유하고 예측할 수 없는 물리적 특성에 의존하여 PUF 응답을 복제하거나 복제하려는 시도에 대한 저항을 강화한다. 이 속성은 특정 장치에 직접 액세스하지 않고 복제본을 만들려는 시도를 어렵게 한다(Mall, 2022).

Table 1은 4가지 주요 PUF에 관해 설명하고 표준에서 정의한 6가지 보안 요구 사항과 비교하여 실드로 사용할 수 있는지를 분석한다 . 또

Table 1 Comparative Analysis of PUFs.

	RO PUF	SRAM PUF	Optical PUF	VIA PUF	e-Cryptex's PUF
Measurement	Delay	Memory	Optical	VIA	Time constant
Robustness	△	○	○	△	○
Randomness	○	○	○	○	Not applicable
Uniqueness	○	○	○	○	○
Tamper-resistance	○	Untested	Untested	○	○
Unpredictability	Conditional	○	○	○	○
Mathematical Unclonability	X	X	○	X	○
Physical Unclonability	○	○	○	○	○
Can be used as a shield	X	X	○	X	○

한, e-Cryptex의 PUF에 대한 6가지 보안 요구 사항의 만족도를 평가한다.

2.1.1 Ring Oscillator PUF

링 오실레이터 PUF(RO-PUF)는 제조 변형을 활용하여 암호화 애플리케이션에 고유하고 예측할 수 없는 응답을 생성하는 하드웨어 보안 기본 요소로 설계되었다. 이 설계는 폐쇄 루프를 형성하는 상호 연결된 링 오실레이터로 구성되며, 각각 고유한 지연을 활용한다. 작동 중에 문제가 발생하고 오실레이터의 특정 지연에 따라 응답이 결정되며, 고유한 가변성을 암호화 키로 전환한다. RO-PUF의 보안 분석은 복제 시도 및 공격에 대한 저항성에 중점을 둔다. 제조 과정에서 발생하는 변동성은 암호화 강도를 위한 강력한 기반을 제공하지만, 공격자가 수학적 모델을 통해 PUF 동작을 복제하려는 모델링 공격과 링 오실레이터의 안정성에 대한 노후화 효과와 같은 취약성은 문제를 일으킬 수 있다. 또한, RO-PUF는 물리적 실드 적용을 위한 것이 아니다. 오류 수정 기술과 신중한 설계 고려 사항을 포함한 완화 전략은 이러한 취약성을 해결하고 RO-PUF의 전반적인 보안을 강화하는 데 필수적이다. RO-PUF는 물리적 실드 역할을 하지는 않지만 고유한 식별 및 인증 메커니즘을 통해 전자 시스템의 보안을 강화하는 데 활용된다 (Maiti et al., 2009; Maiti et al., 2011; Gao et al., 2014).

2.1.2 SRAM PUF

정적 랜덤 액세스 메모리(Static Random Access Memory) PUF는 암호화 애플리케이션을 위해 SRAM 셀의 고유한 변형을 활용하는 하드웨어 기반 보안 기본 요소이다. 이 설계에는 SRAM 셀 배열이 포함되며, 이러한 셀 내의 트랜지스터 불일치로 인해 발생하는 고유한 불안정성에서 챌린지-응답 쌍이 파생된다. SRAM PUF는 읽기 작업 중 SRAM 셀에 내재한 전이 불안정성을 활용하여 작동한다. 문제가 발생하면 SRAM 셀의 특정 준안정 상태에 따라 응답이 결정되므로 예측할 수 없는 독특한 출력이 발생한다. SRAM PUF의 보안 분석은 복제 시도에 대한 저항성과 다양한 공격에 대한 견고성을 강조한다. 트랜지스터 불일치에서 파생되는 고유한 응답은 SRAM PUF의 암호화 강도에 이바지한다. 그러나 반복적인 판독이 SRAM 셀의 상태를 변경할 수 있는 읽기 방해 효과와 같은 취약점은 문제가 될 수 있다(Gordon et al., 2021). 오류 수정 및 챌린지-응답 프로토콜을 포함한 전략은 이러한 취약성을 해결하고 SRAM PUF의 전반적인 보안을 강화하는 데 필수적이다 (Böhm et al., 2013; Jang et al., 2015). SRAM PUF 자체는 물리적 실드가 아니지만 인증 및 검증 목적으로 고유 식별자와 암호화 키를 제공함으로써 시스템의 물리적 보안을 강화하는 데 중요한 역할을 할 수 있다.

2.1.3 Optical PUF

Optical PUF는 암호화 애플리케이션을 위해 광학 구성 요소의 변형을 이용하도록 설계된 하드웨어 보안 요소이다. 이 설계에는 반사율 또는 투과율과 같은 광학적 특성의 변화가 각 광학 PUF 인스턴스의 고유성에 이바지하는 발광체 및 감지기 같은 요소를 통합하는 작업이 포함된다. 입사광 패턴이나 파장과 같은 챌린지에 대한 반응을 측정하여 작동하는 Optical PUF는 광학 특성의 고유한 변화로부터 고유한 챌린지-응답 쌍을 도출한다 (Geis et al., 2017; Silvério et al., 2021). Optical PUF에 대한 보안 분석은 공격에 대한 저항성과 대응의 고유성에 중점을 둔다. 연구원들은 입사광 패턴이나 파장을 변경하려는 조작 공격 등 잠재적인 취약점을 면밀히 조사하여 PUF의 예측 불가능성을 손상시킬 수 있는 취약점을 찾아낸다. 보안을 강화하기 위해 중복성 및 오류 수정 메커니즘과 같은 대응책을 모색하여 잠재적 위협에 대한 Optical PUF의 신뢰성과 견고성을 보장한다 (Lu et al., 2018; Shamsoshoara et al., 2020). 또한, Optical PUF는 물리적 실드로 사용될 수 있는 잠재력이 있지만, 아직 이러한 목적으로 연구되지는 않았다. 지금까지의 연구는 Optical PUF를 다른 보안 조치와 함께 물리적 장치 또는 시스템에 통합하여 포괄적인 보안 솔루션을 제공함으로써 Optical PUF가 인증 및 통신 채널 보안 역할을 하는 방식으로 진행되었다.

2.1.4 VIA PUF

수직 상호 연결 액세스(Vertical Interconnect Access) PUF는 집적 회로에 내장된 하드웨어 보안 기술이다. 반도체층의 VIA 제조 공정 변화를 활용하여 강력한 장치 인증과 안전한 키 생성을 제공한다. 챌린지 입력에 대한 독특하고 예측할 수 없는 반응은 칩의 여러 층을 연결하는 VIA의 전기적 특성에서 비롯된다(Jeon and Choi, 2016). PUF에 관한 다양한 연구가 진행되고 있지만, 현재 대량 생산 및 활용되고 있는 것은 VIA PUF가 유일하다 (Kim et al., 2014; solvitsystem, 2024). VIA PUF의 보안성은 사소한 제조 변형에 매우 민감한 반응을 생성할 수 있으므로 공격자가 원본 칩에 물리적으로 접근하지 않고는 복제하거나 예측하기가 매우 어렵다. 그러나 VIA PUF는 모델링 및 시뮬레이션 기반 공격과 같은 특정 공격에 취약하며, 이는 수학적 모델이나 시뮬레이션을 사용하여 VIA PUF의 동작을 복제하여 보안을 약화하려고 시도한다 (Kumar et al., 2014; Vijayakumar et al., 2015). 또한, 노후화 효과와 환경 변화는 시간이 지남에 따라 VIA PUF의 신뢰성을 저하할 수 있다. VIA PUF는 보호하는 하드웨어 구성 요소의 무결성과 신뢰성을 보장함으로써 시스템의 전반적인 보안에 간접적으로 이바지할 수 있다. 또한, 특정 유형의 공격에 대해 일정한 형태의 보호를 제공할 수 있는 물리적 특성을 가진 VIA PUF 구현도 있지만, 이것이 주된 목적은 아니며 전용 물리적 실드를 대체할 수 있는 신뢰할 방법도 아니다.

2.1.5 e-Cryptex's PUF

본 연구에서는 e-Cryptex의 PUF로 resistor와 capacitor로 구성된 RC 회로를 PUF로 활용하여 키 생성기로 사용하고 회로의 일부를 실드로 사용한다. e-Cryptex의 PUF에 대한 설계와 보안 요구 사항은 4장과 5장에서 평가한다.

2.2 Physical Attacks

이 장에서는 하드웨어에 대한 물리적 공격 방법인 비 침투 공격, 침투 공격, 반 침투 공격 중 모의 침투 공격에 대해 중점적으로 설명한다. 비 침투 공격은 물리적 피해를 주지 않고 하드웨어가 작동하는 방식을 분석하는 반면, 침투 공격은 장치 내부의 구성 요소를 대상으로 한다. 반 침투 공격은 표적을 공격하는 데 사용되는 방법에 따라 비 침투 공격과 침투 공격 사이에 속한다. 침투 공격에는 일반적으로 역공학과 프로빙이 포함된다. 이 장에서는 두 가지 유형의 공격에 관해 설명한다.

2.2.1 Reverse Engineering

복잡한 하드웨어 보안 분야에서는 역공학 공격의 유형이 크게 다가오고 있어 더욱 주의가

요구된다. 따라서 하드웨어 시스템 내의 취약점을 철저히 조사할 필요가 있다. 역공학은 물리적 장치의 내부 작동을 분석하여 독점적인 설계를 밝히고 확인된 취약점을 악용하는 정교한 프로세스이다. 공격자는 학문적 호기심, 지적 재산 도용, 위조, 악의적인 의도를 가진 변조된 하드웨어 제작 등 다양한 이유로 이러한 공격을 수행한다. 역공 공격으로부터의 방어는 장치의 펌웨어, 암호화 키 또는 중요한 기능에 대한 무단 액세스로부터 보호하는 것이 중요하다. 하드웨어 보안이 침해되면 하드웨어의 무결성이 손상될 뿐만 아니라 시스템 데이터의 기밀성과 신뢰성에 직접적인 위협이 되므로 강력한 하드웨어 보안 조치의 중요성이 강조된다 (Fyrbiak et al., 2017; Gordon et al., 2019).

기술이 계속 발전함에 따라 하드웨어 역공학과 관련된 위험은 점점 더 정교해지고 널리 퍼지고 있다. 잠재적인 취약점을 사전에 파악하고 완화하는 것은 종합적인 보안 전략의 중요한 요소이다. 이러한 문제를 해결하려면 하드웨어 제조업체, 사이버 보안 전문가, 규제 기관 간의 협업을 통해 엄격한 표준과 모범 사례를 수립해야 한다. 또한, 진화하는 위협에 한발 앞서 대응하고 역공학 공격에 대한 하드웨어 시스템의 복원력을 강화하기 위해서는 지속적인 연구와 개발이 필수적이다. 하드웨어 보안에 대한 공동의 노력을 통해 업계는 중요한 시스템과 데이터의 기밀성, 무결성, 가용성을 손상할 수 있는 광범위한 위협으로부터 더 효과적으로 보호할 수 있다.

2.2.2 Probing Attack

프로빙 공격은 심각한 위협이 되고 있으며, 잠재적인 취약성에 대비해 시스템을 강화하기 위한 철저한 검사가 필요하다. 프로빙은 데이터의 기밀성과 무결성에 위험을 초래하는 민감한 정보를 얻기 위해 하드웨어 구성 요소를 고의로 은밀하게 탐색하는 것을 말한다. 이러한 공격은 비침습적이거나 침습적일 수 있다. 비침습적 기술에는 전자기 프로빙 또는 전력 분석이 포함되며, 침습적 기술에는 장치의 구조를 물리적으로 조작하는 Focused Ion Beam(FIB) 공격이 포함된다. 프로빙 공격은 암호화 키, 중요한 시스템 매개변수 또는 민감한 데이터를 추출하여 전체 보안 인프라를 위태롭게 할 수 있으므로 특히 우려되는 공격이다 (Ling et al., 2012).

공격자는 하드웨어 설계의 특정 취약점을 악용하기 위해 다양한 프로빙 방법을 사용할 수 있다. 하드웨어 시스템이 더욱 복잡해짐에 따라 프로빙 공격에 대한 이해와 보호가 무엇보다 중요해졌다. 하드웨어 기반 암호화 및 키 관리를 포함한 고급 암호화 기술은 정보 추출 시도에 대한 복원력을 제공한다. 또한, 변조 방지 인클로저 및 보호 코팅과 같은 물리적 보안 조치를 구현하면 침입 프로빙 공격을 차단할 수 있다 (Ishai et al., 2003; Manich et al., 2012; Lee et al., 2020).

3. 관련 연구

연구자들은 하드웨어를 보호하기 위해 실드를 사용하는 다양한 방법을 연구하고 있다. 이러한 방법에는 파릴렌 기반 소재와 같은 flexible PCB (Sarto et al., 2002; Lee et al., 2009; Wang et al., 2020; Selbmann et al., 2021)를 유전체 및 캡슐화 재료로 사용하는 실드, 센서를 통해 실시간으로 변조를 감지하는 액티브 실드 (Kash and Tooper, 1962; Kaul et al., 2002; Cruciani et al., 2019), 소프트웨어 기반 실드 (Patel and Parameswaran, 2008; Chhabra et al., 2009; Lee and Shin, 2016; Lin and Chen, 2016; Gardikis et al., 2017)등이 있다. 이 모든 방법은 아직 연구 단계에 있으며 아직 널리 구현되지 않았다.

Immler et al.(2018)가 제안한 변조 방지 커버로 물리적 인클로저 보호에서는 기존 배터리로 작동하는 변조 방지 커버의 단점을 해결하기 위해 상업적으로 이용할 수 있고 확장 가능하며 검증된 기술인 flexible PCB 기술을 사용하여 제작된 배터리 없는 변조 방지 커버를 소개한다. 커버는 미세한 전극 메쉬로 구성되어 있으며, 커버 아래의 평가 장치는 단락과 개방 회로를 감지하고 메쉬 전극 사이의 커패시턴스를 측

정하여 무결성을 검증한다. 예비 무결성이 확인되면 PUF를 나타내는 정전용량 측정값에서 암호화 키를 도출하여 폐쇄형 시스템에서 민감한 데이터를 해독하고 인증한다. 제안된 PUF는 실드에 대한 변조 시도를 탐지하는 데 효과적이지만 전체 실드를 분리했다가 다시 부착할 수 있어 이러한 공격은 탐지할 수 없다. 실드가 실제로 사용되기 위해서는 이 문제를 해결해야 한다. 본 논문에서는 PUF의 일부를 실드로 사용하여 실드의 일부를 제거하면 키가 복구할 수 없는 손상을 입도록 함으로써 이 위협을 해결한다.

Cioranesco et al.(2014)와 Wang et al.(2019)가 제안한 암호화 보안 실드는 하드웨어 보안을 강화하기 위한 새로운 접근 방식을 도입한다. 제안된 실드 구조는 SIMON 경량 블록 암호와 독립적인 메쉬 라인을 활용하여 집적 회로에 대한 프로빙 공격으로부터 보호하는 것을 목표로 한다. 실드의 설계는 각 라인이 암호 메시지를 전달하도록 하여 공격자가 두 개 이상의 라인을 우회하는 것을 방지하고 잠재적인 공격 범위를 줄인다. 또한, 간단한 애플리케이션 프로그래밍 인터페이스(API)를 통해 실드를 제어할 수 있어 키 및 초기화 벡터(IV) 구성, 실드 활성화/비활성화, 알람 레지스터의 수정 여부를 모니터링할 수 있다. 이 연구는 침입 공격으로부터 암호화 IP를 보호하는 것의 중요성을 강조하고 실드의 비용, 전력 소비, CPU와의 연결성에 대한 종합적인 분석을 제시하며 금융, 신분증, 의료, 군사 애플리케이션과 같은 중요한 분야에서 이 기술의 잠재적 이점을 강조한다. 이 연구에서는 실드 제거에 대해 명시적으로 언급하지 않았다. 또한, 제거 과정에는 제공된 API를 통해 실드 기능을 비활성화하고 집적 회로를 물리적으로 수정하여 실드 구조를 제거하는 방법이 포함될 수 있다고 유추할 수 있다.

Shahrjerdi et al.(2014)가 제안한 센서를 이용한 집적 회로 차폐 및 보안에서는 광학 및 기계적 공격과 같은 위협의 탐지 및 예방에 중점을 두고 집적 회로(IC)를 물리적 공격으로부터 보호하기 위해 센서를 사용하는 방법에 관해 설명한다. 이 논문에서는 악의적인 활동을 감지하고 방어 메커니즘을 트리거하기 위해 광 검출기 및 NEMS/MEMS 캔틸레버와 같은 센서의 필요성을 강조한다. 이 논문은 집적 회로(IC)에 대한 물리적 공격을 탐지하고 방지하기 위해 센서를 사용하는 방법을 제안한다. 이 논문은 광 검출기, NEMS/MEMS 캔틸레버와 같은 센서를 IC에 내장함으로써 광학 및 기계적 공격을 포함한 다양한 유형의 물리적 공격을 감지하고 대응할 수 있다고 제안한다. 제안된 방어 메커니즘은 공격이 감지되면 IC에 저장된 기밀 정보를 파괴하기 위해 삭제 장치를 작동시키는 것을 포함한다. 그러나 실제 시나리오에서 이러한 센서 기반 방어 메커니즘의 효과는 충분히 검토되지 않았으며, 이 논문에서는 이러한 메커니즘의 구현에 대한 구체적인 세부 사항을 제공하지 않는다. 따라서 이 논문에서는 중요한 개념을 소개하지만, IC에 대한 물리적 공격을 방지하는 데 있어 제안된 방어 메커니즘의 실용성과 효과를 확인하려면 추가 연구와 실험이 필요하다.

4. e-Cryptex

이 장에서는 구현 과정과 실제 적용 시나리오를 포함하여 e-Cryptex에 대해 설명한다. e-Cryptex에서 활용하는 PUF를 설명하고 이를 어떻게 보호막으로 사용할 수 있는지 설명한다. 다음으로, e-Cryptex의 설계 및 운영 프레임워크와 함께 주요 특징과 기능을 설명한다. 또한 실제 시나리오에서 e-Cryptex를 어떻게 사용할 수 있는지 설명하여 실제 배포에 대한 통찰력과 강력한 하드웨어 보안 솔루션을 찾는 사용자에게 강력한 보안 방법을 제공한다.

4.1 e-Cryptex의 개념

Fig. 1은 e-Cryptex 개념을 보여준다. 두 개의 RC 회로로 구성된 PUF가 사용된다. RC 회로는 이 PUF의 중요한 구성 요소로, 신호가 물리적으로 보드 밖으로 나갔다가 다시 보드 안으로 들어와서 후 처리된다. 이 신호는 실드로 사용되며, e-Cryptex에서 후 처리하여 키를 생성

한다.

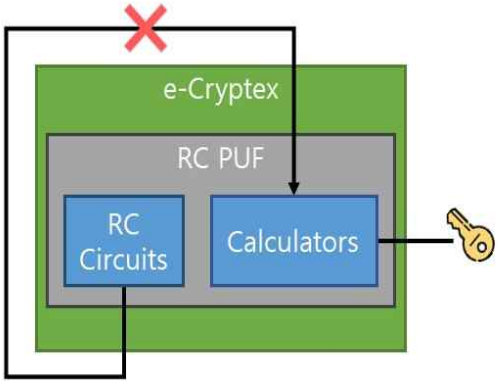


Fig. 1 The overview of the e-Cryptex operation.

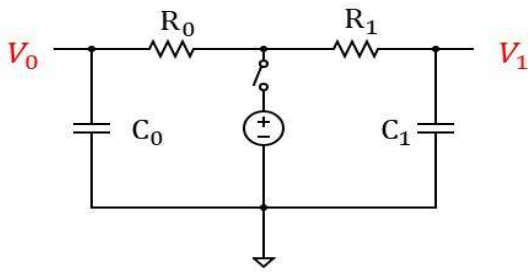


Fig. 2 The RC circuit used in e-Cryptex.

새로운 PUF를 설계할 때 시간 상수를 PUF로 활용하는 선택은 이러한 접근 방식이 제공하는 유연성과 적응성에 기반을 두고 있다. 칩에 구현된 PUF는 일반적으로 전기 소자로 제한되는 반면, PCB에 통합된 PUF는 더 광범위한 재료를 활용할 수 있다. 장치를 PUF로 활용하기 위해 핵심 기준은 특정 특성을 보유하는 데 있다. 크기와 두께와 같은 통제된 요소가 사양을 준수하는 대량 생산에서는 부품 재료의 균일성 변화와 같은 통제되지 않은 요소가 존재하면 본질적인 고유성이 발생한다 (Choi et al., 2022). 특히, 이 PUF 방법론은 광학적 특성을 통합하거나 자기 또는 전자기파를 사용하는 PUF를 고려하는 등 추가 탐색의 길을 열어 제안된 접근 방식의 다양성과 적용 가능성이 증가한다 (Dolev et al., 2015; Geis et al., 2017). 대량 생산에서도 제품마다 달라지는 통제되지 않은 요소는 절연율을 형성하는 데 중요한 역할을 하며 PUF 설계의 필수적인 측면을 형성한다. 결정적으로, 이렇게 선택된 비 제어 요인은 온도 및 습도와 같은 환경 변수의 영향을 받지 않아야 한다.

Sarjeant(1989)에 의하면 저항과 커패시터를 필수 구성 요소로 사용하여 시간 상수 차이를 활용하는 e-Cryptex의 PUF 설계는 장기간 사용 시 환경 변화와 성능 저하에 강한 탄력적인 방안으로 부상하고 있다. Fig. 2의 설계는 전략적으로 배치된 같은 커패시터와 같은 값을가진 같은 저항 두 쌍을 e-Cryptex에서 PUF로 사용한다. RC 회로의 시간 상수(τ)는 저항값과 커패시터값의 곱으로 계산된다. 식 1과 2는 시간 상수 차이의 수학적 식을 보여준다. V를 입력 전압, t를 시간, τ_0을 첫 번째 RC 회로의 시간 상수, τ_1을 두 번째 회로의 시간 상수로 정의한다. RC 회로의 자연적으로 발생한 서로 다른 처리 속도로 인해 발생하는 전압 차이인 식 3 S는 고안된 e-Cryptex 시스템 내에서 고유 식별자 즉, PUF가 된다. 이러한 τ 값은 프로세스에서 자연스러운 변화로 발생한다.

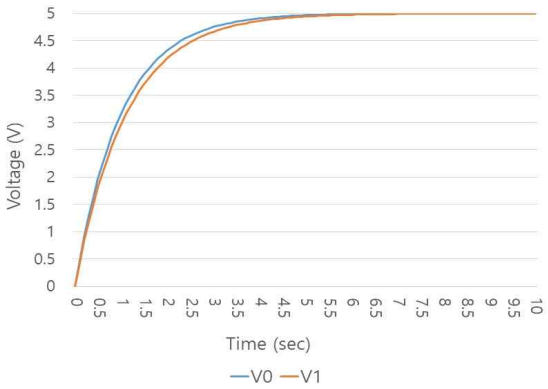
$$V_0(t) = V \cdot e^{-\frac{t}{\tau_0}} \quad (1)$$

$$V_1(t) = V \cdot e^{-\frac{t}{\tau_1}} \quad (2)$$

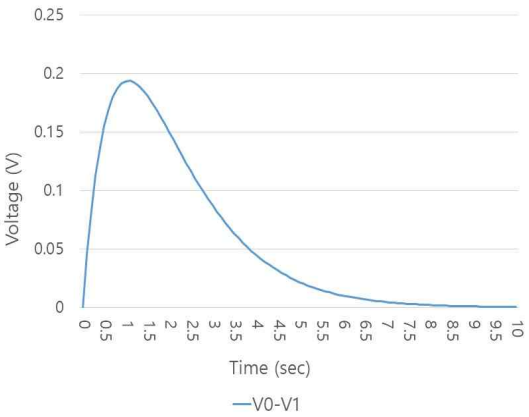
$$S = V_0(t) - V_1(t) \quad (3)$$

Fig. 3은 식 1과 2에서 계산한 τ의 두 값에서 10%의 공정 변동이 발생할 때 두 RC 회로의 전하 곡선과 그 차이를 표시하며, V는 5V, t는 10초, 저항은 10000Ω, 커패시터는 0.0001F로 설정했다. 실제로 두 τ값의 오차는 무작위이므로 PUF로서의 적합성을 확인할 수 있다. 역공학 방지 기술에서 RC 회로의 시간 상수를 PUF의 기초로 활용하는 것은 역공학 시도 중에 발생하는 저항값의 변화를 정확하게 반영할 수 있는가에서 비롯된다. 이러한 신호를 키 생성 메커니즘에 통합하면 시스템을 변조하려는 모든 시도가 기존과 다른 키값을 생성하여 손상된 키를

사용할 수 없게 된다. 이 혁신적인 PUF 방법론은 두 개의 저항과 두 개의 커패시터를 포함하는 시간 상수의 고유한 안정성과 견고성을 활용할 뿐만 아니라 하드웨어 보안 연구에 관한 추가 탐구의 길을 열어준다.



(a) The simulation involves charging at 5V with a process rate of 100% for V_0 and 90% for V_1 when τ is 1.



(b) The simulation of V_0 - V_1.

Fig. 3 Simulated results for two RC circuits with a τ of 1, where the process rates differ by 10%.

4.2 e-Cryptex 회로 설계와 구현

4.1장에서 RC 회로의 충·방전 속도 차이가 PUF 역할을 할 수 있음을 설명했다. 두 값 사이의 차이인 S는 시간이 지남에 따라 0으로 수렴한다. S값을 활용하는 방법에는 피크 감지기 또는 적분 두 가지가 있다. 피크 감지기의 경우 회로 구성을 최소화하기 위해 S는 항상 양수여야 한다. 음수 피크 검출기는 양수 피크 검출기보다 구성이 더 복잡하며, 이를 사용하려면 음수 및 양수 피크 검출기가 모두 필요하다. 그러나 S의 값은 무작위이므로 양수인지 음수인지 예측할 수 없다. 따라서 e-Cryptex에서는 랜덤 요소를 최대한 활용하기 위해 V_0과 V_1의 차이인 S를 적분하여 활용한다. S의 적분 값인 I는 식 4를 사용하여 계산한다. S가 적분 되면 시간이 지남에 따라 단조롭게 증가하거나 감소하여 특정 값으로 수렴한다. 수렴된 값을 결정하기 위해 0에서 무한대까지 적분한다. 이 식은 적분기의 출력이 두 RC 회로의 시간 상수 차이에 정비례한다는 것을 보여준다.

$$I = \int_0^{\infty} (S)dt \tag{4}$$
$$= [-\tau_0 V \bullet e^{-\frac{t}{\tau_0}} + \tau_1 V \bullet e^{-\frac{t}{\tau_1}}]_0^{\infty}$$
$$= (\tau_1 - \tau_0) V$$

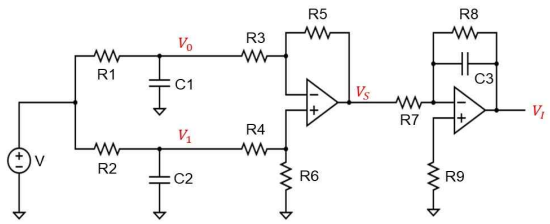


Fig. 4 Abstract e-Cryptex circuit.

Fig. 4 는 두 개의 RC 회로(V_0 및 V_1)의 출력 전압(V_S) 차이를 통합한 e-Cryptex의 회로도를 보여준다. e-Cryptex는 연산 증폭기(OP-amp)를 사용하여 각각 식 5와 식 6으로 V_S와 V_I를 계산하는 4계층 PCB이다.

Table 2 The value used in the e-Cryptex.

Reference	Value	Tolerance	Temperature Coefficient
C1, C2	47nF	20%	C0G
R1, R2, R5, R6	10MegaΩ	5%	±100ppm/℃
C3	0.1uF	5%	X7R
R7, R9	100Ω	0.1%	±50ppm/℃
R8	1KΩ	0.1%	±50ppm/℃
Op-amp	OP07CPZ	X	X

$$V_S = -V_0(\frac{R_5}{R_3}) + V_1(\frac{R_6}{R_4+R_6})(\frac{R_3+R_5}{R_3}) \quad (5)$$

$$V_I = -\frac{1}{R_7C_3}\int_0^t V_S dt = -\int_0^t V_S \frac{dt}{R_7C_3} \quad (6)$$

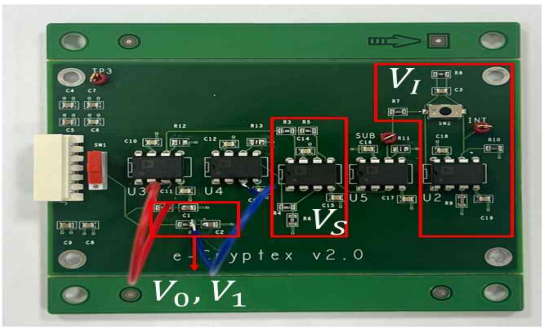


Fig. 5 The actual e-Cryptex Printed Circuit Board.

Fig. 5 는 실제 제작한 e-Cryptex 보드이다. Table 2에는 보드 제작에 사용된 값이 표시되어 있다. RC 회로 구성 요소는 높은 허용 오차와 낮은 온도 계수를 가져야 한다. 따라서 이러한 특성을 가진 소자를 선택했다. 보드 구성에는 이전 회로에 사용된 소자 값에 미치는 영향을 최소화하기 위해 버퍼 역할을 하는 3개의 전압 팔로워가 포함되어 있다. e-Cryptex는 2개의 RC 회로, 실제 PUF에서 사용되는 연산을 수행하는 저항, 커패시터, 2개의 OP 앰프, 전압 팔로워로 사용되는 3개의 OP 앰프로 구성된다. V_S를 계산하기 위해 차동 증폭기가 사용된다. 이 유형의 증폭기는 연산에 사용되는 저항값에 따라 하나의 회로에서 감산과 증폭을 수행할 수 있다. PUF로 사용되는 RC 회로는 실드 역할을 한다. 두 개의 RC 회로에서 작은 변화일지라도 원래 값에서 큰 변화로 보이도록 RC 회로의 변조를 증폭하는 것이 중요하다. 이를 위해 실험을 수행한 결과, 현재 사용되는 값으로 V_0과 V_1의 차이를 12배 증폭하면 많은 경우 V_S와 적분 된 V_I가 포화 한곗값에 도달한다는 사실을 발견했다. 특히 포화 경계가 있는 경우 변조로 인한 V_I값의 변화를 확인하는 것이 중요하다. V_I를 계산하는 회로는 역 적분기로 시간에 따른 V_S를 적분한 결과와 절댓값은 같지만, 부호는 반대이다. R_8은 V_I를 계산하고 포화 상태를 방지하는 데 사용된다. 그러나 V_S가 너무 크면 V_I가 포화한다. 현재 e-Cryptex 구성 값은 V_I가 ±3.0V에서 포화한다.

4.3 e-Cryptex 사용 시나리오

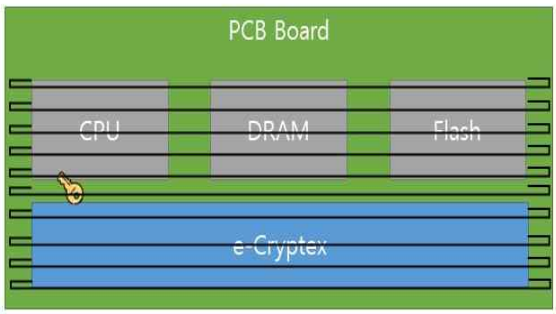


Fig. 6 When e-Cryptex is substantially added to the board, the entire board can be shield.

e-Cryptex는 다음과 같이 사용할 수 있다. Fig. 6 은 키 생성 과정과 그 이후의 적용을 보여주는 e-Cryptex의 실제 사용 모습을 보여준다. 보드 내부를 보여주기 위해 전선(실드)가 드

문드문 그려져 있다. 그러나 실제로는 전선 사이에 공간이 없이 촘촘하게 배치된다. 또한 전선을 겹겹이 쌓을 수도 있다. 전선이 여러 겹으로 겹쳐져 있는 경우, 공격자는 전선을 모두 끊어야만 보드 내부에 접근할 수 있다. e-Cryptex에서 생성된 키는 암호화 및 복호화 작업을 위해 프로세서로 전송되어 보드 전체를 보호하는 e-Cryptex로 효과적으로 보호된다. 이러한 전략적 통합은 잠재적 공격자에게 엄청난 도전 과제를 제시하는데, e-Cryptex 실드를 제거하지 않고는 보드 내부를 역공학하는 것이 사실상 불가능해진다.

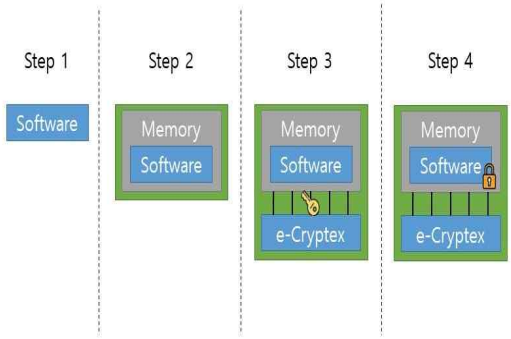


Fig. 7 The process of encrypting software using e-Cryptex.

소프트웨어 보안을 강화하고 역공학을 방지하기 위해 e-Cryptex는 소프트웨어 코드를 암호화하고 메모리에 안전하게 저장하는 혁신적인 접근 방식을 제공한다. Fig. 7 에 설명된 프로세스를 통해 소프트웨어에 대한 무단 접근을 방어할 수 있다. 각 프로세스에 대한 설명은 다음과 같다.

1. 암호화되지 않은 소프트웨어 개발.

암호화되지 않은 상태에서 소프트웨어 개발 프로세스를 시작하면 유연하고 쉽게 코딩할 수 있다.

2. 암호화되지 않은 프로그램을 메모리에 저장.

개발 단계를 완료한 후 암호화되지 않은 프로그램을 장치의 메모리에 저장하여 원래 상태를 유지한다.

3. 보드에 e-Cryptex를 설치.

e-Cryptex 시스템을 보드에 통합하여 후속 암호화 프로세스를 위한 안전한 환경을 구축한다.

4. 최초 부팅 암호화.

보드의 전원을 처음 켜면 e-Cryptex 시스템이 작동하여 메모리에 저장된 프로그램을 암호화한다. 그런 다음 암호화된 버전이 메모리에 다시 안전하게 저장된다. 이후 프로그램의 작동은 암호화된 상태로 작동하므로 잠재적인 위협에 대한 보안이 강화된다.

e-Cryptex를 소프트웨어 개발 및 실행 프로세스에 원활하게 통합하여 고급 암호화 및 실드를 통해 민감한 정보를 보호하고 소프트웨어 및 하드웨어에 대한 무단 액세스를 방지하는 다계층 방어 메커니즘을 제공한다.

5. 실 험

이 장에서는 위변조 방지 및 키 생성 영역에서 e-Cryptex의 효율성을 확인하기 위해 수행한 실험에서 얻은 종합적인 방법론과 그에 따른 결과를 설명한다. 이러한 실험의 주요 목적은 물리적 공격으로부터 보호하는 e-Cryptex의 성능을 검증하는 동시에 신뢰할 수 있는 키 생성기로서의 기능을 평가하는 것이다. 결과의 신뢰성을 보장하기 위해 기계로 대량 생산을 통해 20개의 e-Cryptex를 제작하는 방식을 택했다. 이러한 방법론적 선택은 인적 변이의 영향을 완화하여 e-Cryptex가 PUF로 역할할 것이라는 기대감을 조성하는 것을 목표로 한다.

실험은 τ의 경우 0.47, Voltage의 경우 5V, t의 경우 5초 동안 20개의 e-Cryptex 각각에 대해 수행되며, 두 RC 회로 사이의 뚜렷한 속도 차이로 인해 생성되는 결과 출력 전압을 오실로스코프를 사용하여 측정한다. 초기 측정은 20개의 보드에서 출력 전압 변화를 검증하여 강력한 키 생성기의 기능을 확인하는 데 중점을 둔다.

이 검증 단계에 이어, 실험에서는 사전 정의된 매개변수를 준수하는 고의적인 물리적 공격이 포함되어 출력 전압에 대한 물리적 역공학이 미치는 영향을 실험한다. 이러한 다각적인 접근 방식은 키 생성에 있어 e-Cryptex의 고유한 견고성뿐만 아니라 물리적 역공학 공격 시도를 탐지하고 대응하는 능력도 밝혀내는 것을 목표로

한다. 이러한 체계적인 프로세스를 통해 실험은 e-Cryptex가 출력 전압의 변화를 식별하여 물리적 변조를 탐지할 수 있는 기능을 가지고 있음을 입증한다. 이러한 결과는 키 생성 및 변조 방지 기능 모두에 다각적인 하드웨어 보안 솔루션으로서 e-Cryptex의 실질적인 효율성을 강조한다.

5.1 Trustworthy Evaluation

신뢰성 평가의 목표는 신뢰할 수 있는 키 생성기로서 e-Cryptex의 효율성을 확인하는 것이다. 이를 위해서는 고유성과 견고성을 강조하면서 e-Cryptex가 PUF의 고유 속성을 준수하는지 여부를 확인하기 위한 철저한 검사가 필요하다. PUF는 난수 발생기 역할을 하므로, e-Cryptex는 PUF 속성을 충족함으로써 효과적인 키 생성기로서의 역할을 한다.

반복되는 작업에서 일관된 출력을 보장하는 견고성의 속성은 e-Cryptex에 대해 실험되었다. 그 결과, e-Cryptex는 반복 실행 후에도 매우 좁은 범위(±5mV) 내에서 일관되게 동일한 출력을 생성한다. 이는 e-Cryptex의 핵심 원리인 두 개의 동일한 RC 회로 사이의 속도 차이가 임의로 결정되는 것이 아니라 제조 과정에서 미리 결정되고 안정적으로 유지된다는 것을 의미한다. 노화의 영향을 받았을 때 동일한 출력이 유지되는지에 대한 별도의 실험은 진행하지 않았지만, 저항, 커패시터, Op-amp 등 e-Cryptex의 대부분의 부품이 노화에 안정적이라는 점을 고려하면 노화로 인한 변화가 견고성에 영향을 미치지는 않을 것으로 예상된다.

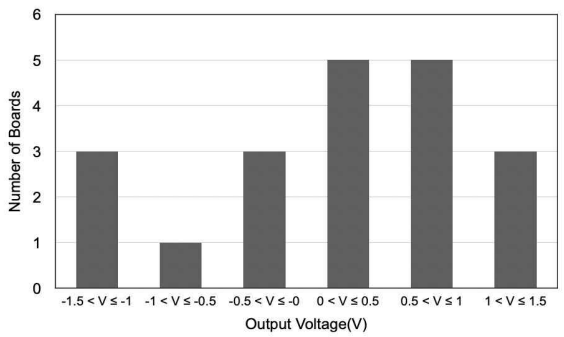


Fig. 8 Result of the uniqueness experiments.

고유성의 관점에서 볼 때, Fig. 8 과 같이 e-Cryptex는 -2V에서 2V에 이르는 광범위한 출력 값을 생성한다. Table 2는 실험에 사용된 RC 회로 요소의 허용 오차가 표시되어 있다. 이 결과는 PUF에 기대되는 특성과 일치하며 키 생성에 중요한 시사점을 제공한다. 출력이 아날로그-디지털 컨버터(ADC)를 통해 키 생성을 위한 입력으로 사용된다고 가정하면, Fig. 8.을 통해 여러 e-Cryptex 간의 고유성을 보장하기 위해 ADC의 해상도가 최소 6개의 부분으로 나눌 수 있음을 보여준다.

수학적 및 물리적 복제 불가능성 측면에서 볼 때, e-Cryptex의 PUF 특성은 정확히 같은 RC 회로의 속도 차이를 활용하기 때문에 수학적 복제를 불가능하게 한다. 마찬가지로, PCB 보드의 값과 회로에 대한 지식이 있어도 같은 출력을 생성하는 e-Cryptex를 제작하는 것은 불가능하다. 추가로, e-Cryptex는 같은 입력 전압에서 일관되게 작동하므로 기능의 무작위성을 고려할 필요가 없다.

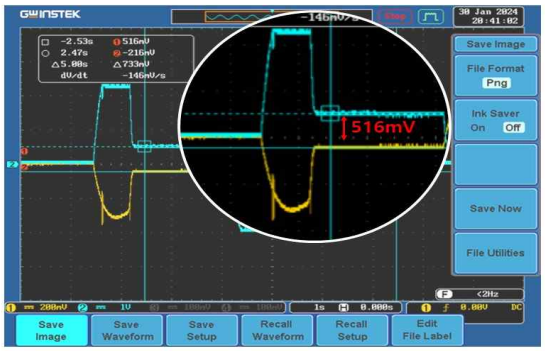
5.2 Tapmering Evaluation

이 장에서는 e-Cryptex의 역공학 방지 기능에 대한 실험적 평가에 관해 설명한다. e-Cryptex가 물리적 공격에 대한 신뢰할 수 있는 보호막으로 기능하고 신뢰점 역할을 하려면 공격자가 공격을 시작할 때 암호화 키를 신속하게 탐지하고 숨길 수 있어야 한다. 주요 목표는 역공학 공격 시도가 감지되면 e-Cryptex의 PUF 값이 변경되어 키 생성 프로세스를 신뢰할 수 없게 만들고 시스템의 무결성을 보호하는 것이다. 우리가 관심 있는 변화는 궁극적으로 키로 사용되는 e-Cryptex가 출력하는 값의 변화이므로, 물리적 공격 시 실드로 사용되는 PUF가 변조되고 이것이 e-Cryptex 출력에 영향을 미치는지 평가한다.

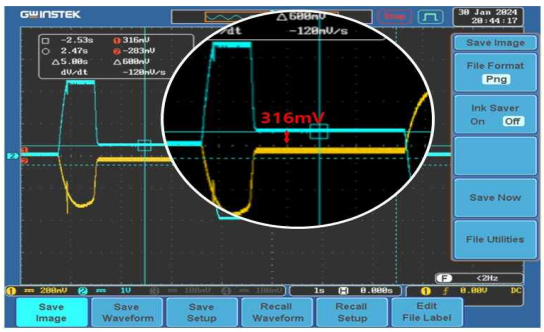
이 가설을 테스트하기 위해 실험을 설계했다. 공격자가 기판을 감싸는 실드로 e-Cryptex를 공격한다고 가정하여, 전선을 실드로 활용하여 전선을 물리적으로 조작하는 두 가지 공격 시나

리오를 제시한다. 첫 번째 시나리오에서 공격자는 시스템의 보호막인 e-Cryptex의 전선을 물리적으로 절단한 후 다시 연결하는 작업을 수행한다. 두 번째 시나리오에서는 공격자가 실드를 완전히 제거하고 새로운 실드로 교체한다. 이러한 시나리오는 일반적으로 기존 전자 장치의 동작에는 영향을 미치지 않을 수 있지만, e-Cryptex에는 영향을 미칠 수 있다. 이는 e-Cryptex가 두 RC 회로 간의 미묘한 차이에 의존하기 때문이다. 두 공격 시나리오 모두 출력에 차이가 발생한다.

물리적으로 공격당한 출력이 원래 출력에서 100mV 이상 차이가 나면 공격 탐지에 성공한 것으로 간주한다. 선택한 임곗값 100mV는 이전 e-Cryptex의 견고성 측정에서 관찰된 5mV 범위를 고려할 때 물리적 공격 감지를 위한 충분한 값임을 확인한다.



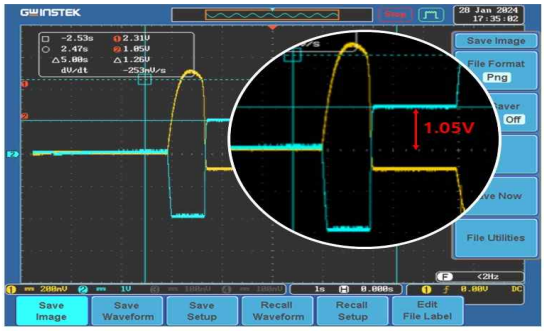
(a) Before Tampering (516mV).



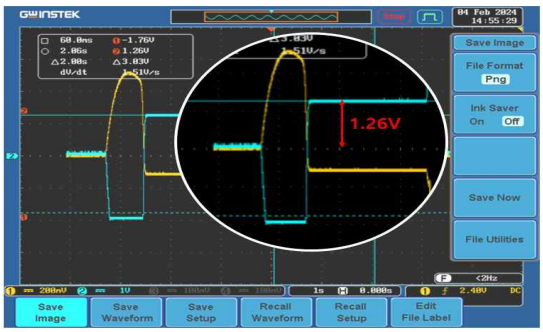
(b) After Tampering (316mV).

Fig. 9 A tampering experiment with breaking and restoring the shield in the middle.

전선 절단 후 다시 복원하는 첫 번째 공격 시나리오에서는 20개의 e-Cryptex 보드 중 3개에서 값의 변화를 확인했다. 이 물리적 공격 실험 후 결괏값은 원래 보드와 비교하여 최소 100mV에서 최대 200mV까지 변화의 값은 다양했다. Fig. 9는 오실로스코프 측정값을 보여주며, 물리적 공격 이후 출력 전압에 눈에 띄는 변화가 있음을 보여준다. 이 시나리오의 한 예로, 처음에 516mV로 측정된 V_I 의 값이 전선 중간이 공격당한 후 200mV가 변경되어 V_I 값이 316mV로 변경됨을 확인할 수 있다.



(a) Before Tampering (1.05V).



(b) After Tampering (1.26V).

Fig. 10 Tampering experiments with removing and reattaching the whole shield.

전선을 제거하고 새로 연결하는 두 번째 공격 시나리오에서는 20개의 e-Cryptex 보드 중 4개에서 물리적 공격 후 값의 변화를 확인했다. 물리적 공격 후 결괏값은 공격 전의 보드와 최소 120mV 이상 차이가 나거나 심지어 값의 변화가 아예 기존과는 다른 양상으로 나타났다. Fig.

10 은 물리적 변조가 출력 전압에 미치는 영향을 시각적으로 나타내며, e-Cryptex가 실드 자체를 통째로 제거 후 다시 부착하는 물리적 공격을 탐지하는 데에도 효과적임을 확인할 수 있다.

6. 결 론

본 연구에서는 악용 가능한 하드웨어 물리적 공격을 효과적으로 완화하도록 설계된 e-Cryptex를 소개했다. e-Cryptex는 2개의 RC 회로와 2개의 Op-amp를 통합하여 저항과 커패시터의 시간 상수를 PUF로 활용한다. 이는 PUF의 모든 보안 요구 사항을 충족하는 간단하면서도 견고한 설계를 제공한다. 이번 연구에 따르면 e-Cryptex는 PUF의 일부를 실드로 사용하는 효율적인 방법으로, 실드 자체를 제거하고 다시 부착하는 것을 목표로 하는 공격에 대한 효과적인 방어 메커니즘을 제공하며, 이는 이전의 실드 기반 연구 노력에서 해결하지 못했던 문제이다. 전반적으로 e-Cryptex는 다양한 물리적 공격으로부터 보호할 수 있는 실용적인 솔루션을 제공하는 하드웨어 보안의 유망한 발전이다.

References

Böhm, C. and Hofer, M. (2013). Using the Sram of a Microcontroller as a PUF, Springer, New York, NY.

Boyd, S. W., Kc, G. S., Locasto, M. E., Keromytis, A. D. and Prevelakis, V. (2010). *On the General Applicability of Instruction-set Randomization, IEEE Transactions on Dependable and Secure Computing,* 7(3), 255 - 270.

Chhabra, S., Rogers, B. and Solihin, Y. (2009). Shieldstrap: Making Secure Processors Truly Secure, *IEEE International Conference on Computer Design,* Oct, 4-7, Lake Tahoe, CA, USA, pp. 289 - 296.

Choi, J. O., Kim, B. J., Lee, H. G., Lee, J. H., Park, A. R., Lee, G. H. and Jang, W. H. (2022). A Physically Unclonable Function Based on RC Circuit with a Confidence Signal, Journal of Korea Society of Industrial Information Systems, 27(4), 11-18.

Choi, P. J. and Kim, D. K. (2012). Design of Security Enhanced Tpm Chip against Invasive Physical Attacks, *IEEE International Symposium on Circuits and Systems (ISCAS)*, May, 20-23, Seoul, Korea (South), pp. 1787 - 1790.

Cioranesco, J. M., Danger, J. L., Graba, T., Guilley, S., Mathieu, Y., Naccache, D. and Ngo, X. T. (2014). Cryptographically Secure Shields, *HOST-IEEE International Symposium on Hardware-Oriented Security and Trust,* May, 6-7, Washington, United States, pp. 25 - 31.

Cruciani, S., Campi, T., Maradei, F. and Feliziani, M. (2019). Active Shielding Design for Wireless Power Transfer Systems, *IEEE Transactions on Electromagnetic Compatibility,* 61(6), 1953 - 1960.

DarkReading. (2022). Secure Systems Need Hardware-Enhanced Tools Intel Says, https://www.darkreading.com/cyberattacks-data-breaches/secure-systems-need-hardware-enhanced-tools-intel-says (Accessed on May. 20th, 2024)

Dolev, S., Krzywiecki, L., Panwar, N. and Segal, M. (2015). Optical Puf for Non Forwardable Vehicle Authentication, *IEEE 14th International Symposium on Network Computing and Applications,* Sep, 28-30, Cambridge, MA, USA, pp. 204 - 207, 2015.

Fyrbiak, M., Strauß, S., Kison, C., Wallat, S., Elson, M., Rummel, N. and Paar, C. (2017). Hardware Reverse Engineering: Overview and Open Challenges, *IEEE 2nd International Verification and Security Workshop (IVSW)*,

Jul, 3-5, Thessaloniki, Greece, pp. 88-94.

Gao, M., Lai, K. and Qu, G. (2014). A Highly Flexible Ring Oscillator Puf, *51st ACM/EDAC/IEEE Design Automation Conference (DAC)*, Jun, 1-5, San Francisco, CA, USA, pp. 1 - 6.

Gardikis, G., Tzoulas, K., Tripolitis, K., Bartzas, A., Costicoglou, S., Lioy, A., Gastón, B., Fernández, C., Dávila, C., Litke, A., Papadakis, N., Papadopoulos, D., Pastor, A., Núñez, J., Jacquin, L., Attak, H., Davri, N., Xylouris, G., Kafetzakis, M., Katsianis, D., Neokosmidis, I., Terranova, M., Giustozzi, C., Batista, T., Preto, R., Trouva, E., Angelopoulos, Y. and Kourtis, A. (2017). Shield: A Novel Nfv-based Cybersecurity Framework, *IEEE Conference on Network Softwarization (NetSoft)*, Jul, 3-7, Bologna, Italy, pp. 1 - 6.

Geis, M., Gettings, K. and Vai, M. Optical Physical Unclonable Function, *IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS),* pages 1248 - 1251, 2017.

Gordon, H., Edmonds, J., Ghandali, S., Yan, W., Karimian, N. and Tehranipoor, F. (2021). Flashbased Security Primitives: *Evolution, Challenges and Future Directions, Cryptography,* https://doi.org/10.3390/cryptography5010007.

Gordon, T., Kilgore, E., Wylds, N. and Nowatkowski, M. (2019). Hardware Reverse Engineering Tools and Techniques, *2019 SoutheastCon,* Apr, 11-14, Huntsville, AL, USA, pp. 1 - 6.

Immler, V., Obermaier, J., Ng, K. K., Ke, F. X., Lee, J. Y., Lim, Y. P., Oh, W. K., Wee, K. H. and Sigl, G. (2018). Secure Physical Enclosures from Covers with Tamper-resistance, IACR Transactions on Cryptographic Hardware and Embedded Systems, https://doi.org/10.13154/tches.v2019.i1. 51-96.

International Institue for Strategic Studies (IISS), (2021), Cyber Capabilities and National Power: A Net Assessment, International Institute for Strategic Studies.

Ishai, Y., Sahai, A. and Wagner, D. (2003). Private Circuits: Securing Hardware against Probing Attacks, *Advances in Cryptology-CRYPTO 2003,* Springer Berlin Heidelberg.

ISO. (2020). Iso/iec 20897-1:2020 Information security, Cybersecurity and Privacy Protection Physically Unclonable Functions, https://www.iso.org/standard/76353.html (Accessed on May. 20th, 2024)

Jang, J. D. and Ghosh, S. (2015). Design and Analysis of Novel Sram Pufs with Embedded Latch for Robustness, 16*th International Symposium on Quality Electronic Design*, Mar, 2-4, Santa Clara, CA, USA, pp. 298 - 302.

Jeon, D. H. and Choi, B. D. (2016). Circuit Design of Physical Unclonable Function for Security Applications in Standard CMOS Technology, *IEEE International Conference on Electron Devices and Solid-State Circuits (EDSSC),* Aug, 3-5, Hong Kong, China, pp. 86 - 90.

Kash, S. W. and Tooper, R. F. (1962). Active Shielding for Manned Spacecraft, Astronautics, 7(9), 68-75.

Kaul, H., Sylvester, D. and Blaauw, D. (2002). Active shields: A New Approach to Shielding Global Wires, *ACM Great Lakes Symposium on VLSI,* Apr, 18-19, New York, NY, USA, pp. 112-117.

Kim, T. W., Choi, B. D. and Kim, D. K. (2014). Zero Bit Error Rate Id Generation Circuit Using via Formation Probability in 0.18 m Cmos Process, *Electronics Letters*, 50(12), 876 - 877.

Kumar, R. and Burleson, W. P. (2014). Hybrid Modeling Attacks on Current-based Pufs,

International Conference on Computer Design (ICCD), Oct, 19-22, Seoul, Korea (South), pp. 493 - 496.

Lee, C. H. and Shin, S. W. (2016). Shield: An Automated Framework for Static Analysis of Sdn Applications, *ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization*, https://doi.org/10.1145/2876019.2876026.

Lee, S. K., Kim, B. H. and Yoo, H. J. (2009). Planar Fashionable Circuit Board Technology and Its Applications, *Journal of Semiconductor Technology and Science,* 9(3), 174 - 180.

Lee, Y. W., Lim, H. C., Lee, Y. K. and Kang, S. H. (2020). Robust Secure Shield Architecture for Detection and Protection against Invasive Attacks, *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 39(10), 3023 - 3034.

Lin, C. W. and Chen, C. H. (2016). A Processor Shield for Software-based On-line Self-test, *Asia Pacific Conference on Circuits and Systems (APCCAS),* Oct, 25-28, Jeju, Korea (South), pp. 149 - 152.

Ling, M., Wu, L., Li, X., Zhang, X., Hou, J. and Wang, Y. (2012). Design of Monitor and Protect Circuits against Fib Attack on Chip Security, *8th International Conference on Computational Intelligence and Security, Nov, 17-18, Guangzhou, China, pp.* 530 - 533.

Lu, X., Hong, L. and Sengupta, K. (2021). Cmos Optical Pufs Using Noise-immune Process-sensitive Hotonic Crystals Incorporating Passive Variations for Robustness, *IEEE Journal of Solid-State Circuits,* 53(9), 2709 - 2721.

Maes, R. (2013). Physically Unclonable Functions: Properties, *Springer Berlin Heidelberg,* Berlin, Heidelberg.

Maiti, A. and Schaumont, P. (2009). Improving the Quality of a Physical Unclonable Function Using Configurable Ring Oscillators, *2009 International Conference on Field Programmable Logic and Applications*, Aug-Sep, 31-2, Prague, Czech Republic, pp. 703 - 707.

Maiti, A. and Schaumont, P. (2011). Improved Ring Oscillator Puf: An Fpga-friendly Secure Primitive, *Cryptology*, https://doi.org/10.1007/s00145-010-9088-4.

Mall, P., Amin, R., Das, A. K., Leung, M. T. and Choo, K. K. R. (2022) Puf-based Authentication and Key Agreement Protocols for Iot, Wsns, and Smart Grids: *A Comprehensive Survey, IEEE Internet of Things Journal,* 9(11), 8205 - 8228.

Manich, S., Wamser, M. S. and Sigl, G. (2012). Detection of Probing Attempts in Secure ICs, *IEEE International Symposium on Hardware-Oriented Security and Trust,* Jun, 3-4, San Francisco, CA, USA, pp. 134 - 139.

Patel, K. and Parameswaran, S. (2008). Shield: A Software Hardware Design Methodology for Security and Reliability of Mpsocs, Jun, 8-13, *2008 45th ACM/IEEE Design Automation Conference,* Anaheim, CA, USA, pp. 858 - 861.

Sarjeant, W. J. (1989). Capacitor Fundamentals, *19th Electrical Electronics Insulation Conference*, Sep, 25-28, Chicago, IL, USA, pp. 1 - 51.

Sarto, M. S., Di Michele, S. and Leerkamp, P. (2002). Electromagnetic Performance of Innovative Lightweight Shields to Reduce Radiated Emissions from Pcbs, *IEEE Transactions on Electromagnetic Compatibility,* 44(2), 353 - 363.

Selbmann, F., Roscher, F., de Souza Tortato, F., Wiemer, M., Otto, T. and Joseph, Y. (2021). An Ultra-thin and Highly Flexible Multilayer Printed Circuit Board Based on Parylene, *Smart Systems Integration (SSI),*

Apr, 27-29, Grenoble, France, pp. 1 - 4.

Shamsoshoara, A., Korenda, A., Afghah, F. and Zeadally, S. (2020). A Survey on Physical Unclonable Function (Puf)-based Security Solutions for Internet of Things, *Computer Networks*, https://doi.org/10.1016/j.comnet.2020.107593.

Shahrjerdi, D., Rajendran, J., Garg, S., Koushanfar, F. and Karri, R. (2014). Shielding and Securing Integrated Circuits with Sensors, *IEEE/ACM International Conference on ComputerAided Design (ICCAD),* Nov, 2-6, San Jose, CA, USA, pp. 170 - 174.

Shi, Q., Wang, H., Asadizanjani, N., Tehranipoor, M. M. and Forte, D. (2018). A Comprehensive Analysis on Vulnerability of Active Shields to Tilted Microprobing Attacks, *Asian Hardware Oriented Security and Trust Symposium (AsianHOST),* Dec, 17-18, Hong Kong, China, pp. 98 - 103.

Silvério, T., Dias, L., Ferreira, R. A. S. and André, P. S. (2021). Optical Authentication of Physically Unclonable Functions Using Flexible and Versatile Organicinorganic Hybrids, *SBMO/IEEE MTT-S International Microwave and Optoelectronics Conference (IMOC),* Oct, 24-27, Fortaleza, Brazil, pp. 1 - 3.

Solvitsystem. (2024). Ictk Holdings via Puf, https://www.solvitsystem.co.kr/product/product_040300.html (Accessed on May. 20th, 2024)

Suh, G. E., Clarke, D., Gasend, B., Van Dijk, M. and Devadas, S. (2003). Efficient Memory Integrity Verification and Encryption for Secure Processors, *36th Annual IEEE/ACM International Symposium on Microarchitecture,* Dec 05, San Diego, CA, USA, pp. 339 - 350.

Vijayakumar, A. and Kundu, S.. (2015). A Novel Modeling Attack Resistant Puf Design Based on Non-linear Voltage Transfer Characteristics, *2015 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Mar. 9-13, Grenoble, France, pp. 653 - 658.

Wang, H., Shi, Q., Forte, D. and Mark M. Tehranipoor. (2019). Probing Assessment Framework and Evaluation of Antiprobing Solutions, *IEEE Transactions on Very Large Scale Integration (VLSI) Systems,* 27(6), 1239 - 1252.

Wang, Y., Wang, H., Liu, F., Wu, X., Xu, J., Cui, H., Wu, Y. J., Xue, R. Tian, C. Zheng, B. and Yao, W. (2020). Flexible Printed Circuit Board Based on Graphene/Polyimide Composites with Excellent Thermal Conductivity and Sandwich Structure, *Composites Part A: Applied Science and Manufacturing, https://doi.org/10.1016/j.compositesa.2020.106075.*

Zuo, S., Zhuang, J., Liu, Y., Wang, M. and Yu, Z. (2022). Hardware Based RISC-V Instruction Set Randomization, *IEEE International Conference on Integrated Circuits, Technologies and Applications (ICTA)*, Oct, 28-30, Xi'an, China, pp. 96 - 97.

최 지 원 (Jione Choi)

- 정회원
- 동덕여자대학교 컴퓨터학과 공학학사
- (현재) 고려대학교 정보보호대학원 정보보호학과 석사 박사 통합과정
- 관심분야: 파일시스템 보안, 하드웨어 보안

박 선 용 (Seonyong Park)

- 고려대학교 사이버국방학과 공학학사
- 관심분야: 하드웨어 보안

이 중 희 (Junghee Lee)

- 정회원
- 서울대학교 컴퓨터공학과 공학학사
- 서울대학교 컴퓨터공학과 공학석사
- 조지아공과대학교 전자공학과 공학박사
- (현재) 고려대학교 정보보호대학원 부교수
- 관심분야: 하드웨어 보안

이 형 규 (Hyung Gyu Lee)

- 정회원
- 서울대학교 전기컴퓨터공학부 공학석사
- 서울대학교 전기컴퓨터공학부 공학박사
- (현재) 덕성여자대학교 소프트웨어전공 부교수
- 관심분야: 저전력 시스템 설계, 에너지 하베스팅, 저전력 메모리, 엣지 컴퓨팅

이 규 호 (Gyuho Lee)

- 인하대학교 컴퓨터공학과 공학학사
- 인하대학교 정보통신공학과 공학석사
- (현재) LIG넥스원 사이버전자전개발단 수석연구원
- 관심분야: 무기체계 사이버보안, 하드웨어 보안, 안티탬퍼링

장 우 현 (Woo Hyun Jang)

- 서강대학교 컴퓨터학과 공학학사
- 서강대학교 컴퓨터공학과 공학석사
- (현재) LIG넥스원 사이버전자전개발단 수석연구원
- 관심분야: 무기체계 사이버보안, 안티탬퍼링, 사이버 훈련

최 준 호 (Junho Choi)

- 인하대학교 정보통신공학과 공학학사
- 인하대학교 정보통신공학과 공학석사
- (현재) LIG넥스원 사이버전자전개발단 선임연구원
- 관심분야: 무기체계 사이버보안, 하드웨어 보안, 안티탬퍼링