정 보 보 호 학 회 지
제 33 권 제6호, 2023. 12

물리적 복제 불가능 함수에 기반하는 양자 내성 암호의 암호키 관리 시스템

이 경 택*, 전 두 현*

요 약

현재 사용되고 있는 RSA, ECC 등 비대칭키 암호알고리즘은 앞으로 나올 양자컴퓨터와 양자알고리즘의 빠른 계산 속도로 알고리즘의 비가역성이 깨질 수 있음이 알려졌다. 이는 공개키로부터 비밀키를 계산할 수 있음을 의미한다. 이를 극복하기 위해 미국 국립표준기술연구소 (NIST)는 최근에 양자 내성 암호 (PQC) 알고리즘 선정과 표준화 작업을 진행해 왔으며, 4차 라운드에 진입해 있다. PQC 알고리즘에 필요한 PQC 비밀키는 PQC 알고리즘이 구현된 칩 외부에서 주입하거나 칩 내부에서 자체 생성을 하여 사용하는데, 이 비밀키를 비휘발성 메모리 (NVM) 등에 저장한다. 만약 시스템의 보안 취약성으로 인해 비밀키가 노출된다면 아무리 PQC 알고리즘이 강력해도 전체 시스템이 무너진다. 즉, 알고리즘의 수학적 능력과 무관하게 해당 보안 시스템은 무력화되는 것이다. 본 논문에서는 물리적 복제 방지 기능 (PUF)을 사용하여 PQC 비밀키를 안전하게 보호하고, 이를 기반으로 전체 시스템을 보호할 것을 제안한다. PQC 비밀키가 외부에서 주입되면 해당 키는 NVM에 저장되기 전에 PUF 키로 암호화 될 수 있다. PUF 값에서 파생되는 PUF 키는 필요할 때 마다 다시 만들어서 사용이 가능하므로 메모리에 저장할 필요가 없으며, 따라서 외부 공격에 PUF 키가 노출 되지 않는다. 반도체 수동소자로 이루어지는 Via PUF 기술은 최악의 환경 변화에도 그 특성이 유지되는 가장 최적의 PUF 기능을 제공한다.

Ⅰ. 서 론

현대 암호시스템의 구성은 암호학에 기반하는 암호알고리즘을 이용하고 있다. 이 때, 암호알고리즘이 어떻게 연산하는지에 대해서는 공개되어 있으며, 암호문은 공개적인 네트워크를 통해 전달되기 때문에 누구나 접근 가능하다고 볼 수 있다. 따라서, 암호키를 안전하게 보호하는 것이 암호시스템을 안전하게 보호하는 가장 핵심적인 요소이다. 특히, 공개키 암호 알고리즘 (PKI)은 암호화 키와 복호화 키가 서로 다르며, 공개키로 암호화하고 해당 비밀키로 복호화를 한다. 이 때 사용하는 암호 알고리즘은 수학적 난제를 기반으로 하며 현재까지 RSA와 ECC 등의 알고리즘이 널리 사용되고 있다. 수학적인 난제에 기반한 알고리즘의 핵심은 비가역성, 즉 비밀키를 알고 있다면 공개키를 쉽게 계산할 수 있지만, 그 반대는 현실적으로 불가능하다는 점에 있다. 여기에서 비가역성은 즉, 공개키 암호알고리즘, 평문-암호문 쌍, 공개키 정보를 알아도, 비밀키를 알아내는 것은 수학적으로 불가능해야 한다는 것을 의미한다.

그러나, 양자 컴퓨터의 발전으로 쇼어 알고리즘의 연산을 빠르게 처리할 수 있다면, 현재 사용 중인 RSA 및 ECC와 같은 비대칭 키 암호 알고리즘의 비가역성이 깨질 수 있다고 알려졌다 [1]. 즉, 양자 컴퓨팅의 빠른 연산능력을 이용하여 쇼어 알고리즘 방식으로 계산을 하면 고전 컴퓨터에서는 지수시간 문제였던 것이 이제는 다항 시간의 문제가 되어 계산이 가능하게 된다는 사실이다. 그렇다면 더 이상 기존 비대칭 키 암호화 알고리즘은 안전하지 않을 수 있다.

이 문제를 해결하기 위해서 미국 국립표준기술연구소 (NIST)는 최근에 양자 내성 암호 (PQC) 알고리즘 선정과 표준화 작업을 진행해 왔으며, 2022년에 표준화를 위해 제 3 라운드 경쟁이 종료되고 제 4 라운드로 나아가면서, 총 4개의 후보 알고리즘을 선정하였다. NIST는 CRYSTALS-KYBER (키생성과 암복호) 와 CRYSTALS- Dilithium (디지털 서명)이 강력한 보안

본 논문은 정부 (과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 해외우수과학자 유치사업 (Brain Pool)의 일환으로 수행되었습니다 (과제 번호 2021H1D3A2A02096391)
* 주식회사 ICTK 시스템반도체 개발실 (Chief Strategy Officer/SoC 그룹장, ktlee@ictk.com, 책임 연구원, dhjeon@ictk.com)

과 우수한 성능을 갖추어 선정되었다고 발표했다. 더불어, 서명 체계 FALCON과 SPHINCS+도 표준화될 예정이다. NIST 발표는 핵심 알고리즘 자체에 중점을 두었으며, 이는 암호 알고리즘의 수학적 난제를 더욱 강화하여, 양자컴퓨터를 이용한 비가역성을 깨기 위한 공격이 있다고 해도 비밀키가 계산되어 노출되지 않고 안전하게 보호될 수 있다는 것을 의미한다.

그러나 NIST는 비밀키 혹은 암호키가 안전하게 생성 및 저장되는 시스템 보안의 중요성은 다루지 않았다. 일단 비밀키가 만들어지면 이 비밀키는 시스템 어딘가에 저장 되어야 한다. 아무리 강력한 PQC 알고리즘이 구현되어도, 저장된 PQC 암호키가 유출되면 그 암호시스템은 더 이상 안전하지 않다. 제 4 라운드 알고리즘들은 양자컴퓨터의 공격에 대한 수학적 강도를 제공할 수는 있지만, 시스템 자체를 안전하게 만들기 위한 솔루션을 제공하지는 않는다.

따라서, PQC 알고리즘을 이용하여 암호키가 수학적 역계산을 통해 노출되지 않도록 보호하는 것도 중요하지만, 이 생성된 암호키를 안전하게 관리할 수 있는 방법 또한 매우 중요하다.

지금과 같은 초연결 시대에서 암호키를 안전하게 보호하기 위해서 하드웨어 보안 모듈 (HSM)의 적용 등의 여러가지 방법이 시도되고 있다. 특히 제로 트러스터 (Zero Trust) 환경 하에서 보안 개념을 보여주는 방식이 적용되고 있다. 여기에서 대부분은 생성된 암호키를 비휘발성 메모리 (NVM)에 저장하는 방식을 사용하고 있다. 그러나, 이러한 NVM을 대상으로 하는 각종 물리적 보안 공격 기술 수준이 발전하고 있으며, 암호키와 같은 비밀정보를 단순히 NVM에 저장하는 방법은 더 이상 안전하지 않다 [2]-[5].

본 논문에서 소개될 Via-PUF (Physically Unclonable Function) 기술은 이러한 물리적 보안 공격으로부터 암호키를 보호할 수 있는 강력한 보안 기술이다. PUF를 이용하면 암호키가 메모리에 저장되지 않고, 필요할 때에만 매번 생성되기 때문에, 기존의 메모리를 대상으로 하는 보안 공격에도 암호키를 안전하게 보호할 수 있다. 또한, 본 논문에서는 PQC 암호키를 외부에서 생성하여 주입하는 경우와 PUF를 이용하여 내부에서 생성하는 경우를 다루고 각각의 경우에 PUF 기술이 어떻게 사용될 수 있는지를 보여준다. PQC 칩에 PUF 기술을 통합하기 위한 여러가지 방식도 보여준다. 하드웨어 신뢰점 (Root of Trust)의 솔루션으로서 Via-PUF 기술을 설명하며 해당 기술이 PQC 암호키와 같은 비밀 정보를 보호할 수 있다는 것을 보여준다. 따라서 본 논문에서는 PQC 암호키의 안전한 관리를 위하여, PUF 기반의 암호키 보호 방법을 제안한다.

Ⅱ. Via-PUF 기술

Via-PUF는 일반적인 CMOS 반도체 제작 과정의 비아 또는 콘택이 랜덤하게 형성되는 기술에 기반하고 있다. 이 기술은 디자인 룰을 만족시키기보다는 오히려 비아 또는 콘택 크기를 요구 사항보다 작게 디자인하여 비아 또는 콘택의 형성이 예측할 수 없는 1 또는 0 값이 나오도록 유도하는 기술이다 [6][7]. 이 PUF 기술은 사람의 지문처럼 IC 칩의 지문으로 간주되는 " 고유한 Inborn ID" 속성을 제공한다. PUF ID를 메모

〔표 1〕 VIA-PUF 주요 특징

주요 특징	설명
Inborn ID	칩 고유의 “inborn ID”. 반도체 칩 지문 또는 DNA 역할을 하며, 별도의 ID 저장 과정이 불필요함.
제조 방법	일반적인 CMOS 공정으로 제조되며, PUF를 위한 별도의 반도체 공정이 추가되지 않음. PUF 특성을 위한 고전압 등의 환경이 불필요함..
랜덤성	디자인룰 위배를 통하여, 비아 또는 콘택이 랜덤하게 형성되게 하고, 한번 형성된 비아 또는 콘택을 기반으로 랜덤수를 형성함. 형성된 랜덤수는 NIST SP800-22의 랜덤 평가 기준을 모두 통과
고유성	평균 해밍거리는 0.4999로 이상적인 0.5에 매우 근접함. 3072 개의 비트셀을 이용하여 256비트 엔트로피를 형성
신뢰성	금속 구조를 사용하여, 한번 결정된 단락 여부는 변하지 않음. PUF 회로를 동작시킬 때마다 동일한 랜덤값이 생성됨. 에러율은 1.211E-11 이하로, 이는 4,587,520의 비아를 2000번 반복측정하는 동안 한번도 변하지 않았음을 의미함.
오류정정부호	별도의 오류정정부호 회로를 사용하지 않음
보안성	VIA 구조는 랜덤하게 배치되어, 역공학으로 그 위치 및 PUF 값을 파악하는 것이 현실적으로 불가능함

리에 저장할 필요가 없으며 외부로부터 주입도 필요하지 않다. Via-PUF 비트는 회로에 사용되는 수동소자 (Passive device)인 저항체의 구조이며 능동소자 (Active device)를 사용하는 다른 PUF (예를 들면 SRAM-PUF) 와는 다른 특성을 지닌다. 수동소자 이므로 환경적 스트레스 (전압 및 온도 변동과 같은 외부 변화나 노후화 등)에 민감하지 않기 때문에 오류 교정 코드 (Error Correction Code, ECC)나 헬퍼 데이터 (Helper Data)가 별도로 필요하지 않다. Via-PUF의 특성은 표 1에 나와 있다. 특히 반도체 ASIC 칩 디자인 과정에서 Via-PUF Cell은 Standard Cell의 형태로 제공되므로 Auto-Placement & Routing 시에 다른 로직 Cell들과 동일하게 다루어지는 점과 웨이퍼 제작 시에 추가 Mask가 필요치 않은 점은 Via-PUF만의 최대 강점이다.

Via-PUF에서 발생되는 비밀키 (PUF 키)는 각 반도체 칩마다 다른 값을 가지며 칩 외부로 노출이 안되도록 하드웨어로 디자인되어, 여러가지 보안 용도로 다양한 분야에서 사용된다. 신뢰점 (Root of Trust, RoT)의 핵심인 Secure Storage 기능도 Via-PUF를 이용하여 구현 된다.

Ⅲ. 수동소자 PUF와 능동소자 PUF 비교

"수동소자 PUF (Passive PUF)"라는 용어는 저항이나 커패시터와 같은 수동 소자를 사용한 PUF를 의미하며, "능동소자 PUF (Active PUF)"는 트랜지스터 또는 SRAM 셀과 같은 능동소자를 사용한 PUF를 의미한다.

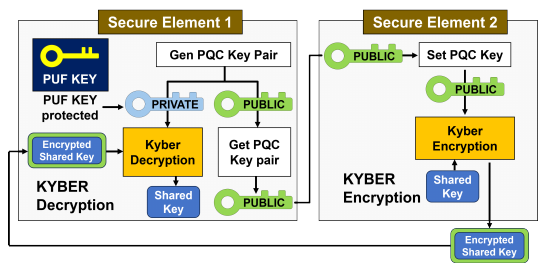
Via-PUF와 같은 수동소자 PUF는 극한의 운용조건에서도 탁월한 신뢰성을 제공한다. 이는 능동 소자에 비해서 수동 소자는 온도 및 전압 변동과 같은 외부요인의 영향을 거의 받지 않기 때문이다. Via-PUF는 표준 ASIC 공정 상에서 비아나 콘택과 같은 수동 성분의 무작위 형성을 기반으로 하므로 외부 요인의 영향이 거의 없다고 할 수 있다. 또한 14nm 혹은 그 이하의 최첨단 FinFET 공정에서 능동소자 PUF는 더욱이 기존에 없었던 어려운 점이 존재할 수 있는데, 웨이퍼 상의 다이 위치에 따른 바이어스 문제가 있어 랜덤성이 상실되는 문제가 그것이다. 그것을 극복하기 위하여 더 많은 ECC 로직과 헬퍼 데이터가 필요하다. 반면 Via-PUF는 수동소자의 특성을 가지므로 그런 문제로부터 상대적으로 자유롭다. 따라서 특히 산업용 IoT 애플리케이션과 같이 물리적 손상이나 환경적 스트레스가 존재하는 곳에서는 수동소자 PUF가 탁월한 선택이 된다.

Ⅳ. PQC 알고리즘과 Via-PUF의 중요성

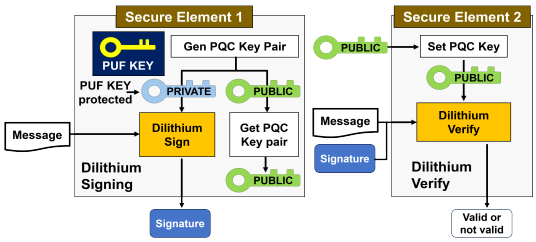
그렇다면 칩마다 고유한 값을 가지는 PUF 키가 양자 내성 암호 (PQC) 알고리즘에서 어떻게 사용될 수 있는지를 생각해보자.

NIST는 제로 트러스터 환경 (ZTE) 에서의 보안 개념을 정의하였는데, 이는 방화벽과 같은 기업 네트워크 전체를 하나의 보안대상으로 보는 개념이 아니라, 보안 주체를 개별 기기 레벨로 내려서 모든 통신 세션에 보안 검증을 요구하는 개념이다. ZTE 사이버 보안은 '신뢰하지 말고 항상 검증하라'라는 개념을 갖고 있다 [8]. 그렇다면 PQC 알고리즘을 운용하는 개별 기기에서의 보안은 PQC 개인키를 얼마나 안전하게 보호하는가의 문제로 귀결될 것이다. 기기의 NVM에 PQC 비밀키가 평문으로 저장되어 있다면 NVM의 데이터가 탈취당했을 때는 해당 키를 보호할 수 없다. PUF 기술은 여기에서 중요한 역할을 수행할 수 있다. 만약 공격자의 목표인 PQC 비밀키가 기기에 저장되지 않고 필요할 때마다 생성되고 그 후에는 사라진다면 어떨까? 공격자는 물리적인 대상이 없기 때문에 큰 어려움에 부딪힐 것이다.

CRYSTALS-Kyber 프로토콜은 격자 기반 암호학의 LWE (Learning with Error) 문제의 복잡성을 기반으로하며 Key Generation, Encrypt/Encapsulate, 그리고 Decrypt/Decapsulate 세 가지 핵심 함수로 구성되어 있다 [9]. 초기화는 Key Generation 함수로 시작되며 이 함수는 비밀키와 대응하는 공개키 한 쌍을 생성한다. 이때 생성된 비밀키를 PUF 키로 암호화해서 NVM에 저장할 수 있다 (그림 1). 여기에서 PUF 키는



〔그림 1〕 CRYSTALS Kyber 알고리즘에서 PUF를 이용한 비밀키 보호



〔그림 2〕 CRYSTALS Dilithium 알고리즘에서 PUF를 이용한 비밀키 보호

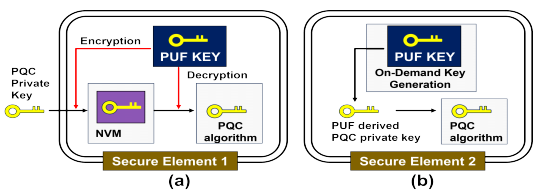
칩 어느 곳에도 저장이 되지 않고 세션에 필요할 때마다 만들어서 계산에 사용된다. PUF는 각 칩마다 고유한 비밀값이며 실제 연산에 사용되는 PUF 키는 그 PUF 값으로부터 계산된다.

한편, CRYSTALS-Dilithium은 키 생성, 서명 절차 및 이어지는 검증 과정으로 이루어진 디지털 서명 프로토콜이다 [10]. 비밀키를 입력으로 하여 공개키를 계산하는 키 생성 알고리즘을 사용한다. 이때 입력된 비밀키는 또한 PUF key로 암호화를 해서 NVM에 저장할 수 있다 (그림 2). 비밀키는 내부생성 혹은 외부주입으로 만들 수 있으며, 두가지 경우 모두 PUF 키를 이용하여 비밀키를 암호화하여 저장할 수 있다. PUF 기술은 PQC 비밀키를 보호하는 데 중요한 역할을 할 수 있다.

Ⅴ. PUF 기술을 활용한 PQC 비밀키 보호

키 생성 출처에 따라 PQC 알고리즘의 비밀키를 보호할 수 있는 방법에는 두 가지 예가 있다.

키가 칩 외부에서 만들어지는 경우에는 생성된 키가 칩 내부로 안전하게 주입되어야 하며, 이를 발급 혹은 Provisioning이라고 부른다. 여기에서 주입되는 키를 칩 메모리에 저장하기 전에 PUF 키를 이용하여 암호화하여 저장한다면 전체 시스템의 보안을 강화할 수 있다 (그림 3(a)). PQC알고리즘 수행 시에 NVM에 저장된 비밀키가 필요하다면 동일한 PUF 키로 복호화를 해서 PQC 알고리즘에 공급해준다.



〔그림 3〕 PQC의 비밀키 보호 방법 (a) 칩 외부에서 주입하는 비밀키를 PUF로 암호화 하는 방법 (b) 칩 내부의 PUF를 이용한 비밀키 직접 생성 방법

여기에서 중요한 점은 발급이 이루어지는 발급 환경의 보안성이다. 예를 들면 Joint Interpretation Working Group (JIWG)에서 발행된 Joint Interpretation Library (JIL)에 명시된 사이트 보안 요구사항 (MSSR)이 있는데 이것은 Common Criteria 인증서를 받기 위해서 필요한 요구사항으로서 물리적인 사이트나 시설의 안전을 보장하기 위해 수립된 지침, 표준 또는 명세서이다 [11]. 이때 발급환경의 보안수준은 수치로 표시될 수 있다. 이러한 요구 사항은 무단 접근, 도난, 야간 행위, 테러 등으로부터 발급사이트를 보호하기 위해 개발되고 시행된다. 그러나 이러한 보안 환경을 설치 유지하는 것은 많은 노력과 비용이 요구되는 것이 사실이다. PQC 비밀키의 발급은 이러한 보안환경에서 수행되는 것이 중요하다.

반면, PQC의 비밀키가 보안칩 내부에서 자체 생성이 되는 경우가 있다 (그림 3(b)). PQC의 비밀키가 PUF 기반 난수 생성기에서 내부적으로 생성될 때, 해당 키는 칩의 메모리에 반드시 저장할 필요는 없다. 이는 ZTE 환경에서 암호화 비밀키에 대한 더 강력한 보호 기능을 제공한다.

5.1. PQC 비밀키의 외부 주입

일반적으로 보안 시스템은 데이터를 암호화하고, 문서에 전자 서명을 하며, 인증서를 사용하여 자신을 인증할 수 있는 Public Key Infrastructure (PKI)를 사용한다. PQC 알고리즘을 운영하는 클라이언트 디바이스는 공개키와 비밀키 쌍을 생성하고 서명을 위해 공개키는 인증 기관 (Certification Authority, CA)에 전송하고 비밀키는 클라이언트 디바이스에 남겨진다. 클라이언트 디바이스는 CA로부터 받은 서명된 인증서와 디바이스에 남겨진 PQC 비밀키와 같은 보안 데이터를 메모리에 저장하는 발급과정을 거치게 된다. 디바이스는 보안 데이터가 전원이 꺼진 상황에서도 손실되지 않아야 하므로 주로 플래시 메모리와 같은 비휘발성 메모리 (NVM)에 저장을 한다. 이 발급 단계에서 해당 비밀 데이터가 발급기에서 칩 내부의 NVM으로 전달되는 과정 중에서 각종 환경적인 요인이나 발급기에 대한 공격 등으로 유출될 수 있는 잠재적인 위험이 있다. 비밀 데이터가 안전하게 NVM까지 전송되더라

도 NVM에 대한 공격으로 저장된 데이터가 노출될 수도 있다 [2]-[5]. 따라서 보호되지 않은 비밀 데이터를 NVM에 단순 저장하는 것은 보안 공격에 매우 취약하며, 저장되기 전에 암호화 등의 방법으로 보호해서 저장해야 한다.

이때 비밀 데이터를 암호화하기 위해서는 암호화 키가 사용된다. 이를 키 암호화 키 (Key Encryption Key, KEK)라고 부르며, 이 KEK를 안전하게 보호하는 것도 중요하다. KEK를 NVM에 단순 저장하면 같은 이유로 취약점이 나타날 수 있다. 만약 NVM에 저장되지 않으면서 비밀 데이터를 암호화할 수 있는 방법이 있다면 가장 근본적인 해결책이 될 수 있을 것이다. 이러한 조건을 만족시키는 방법으로는 PUF 기술을 사용하는 것이다.

그림 3(a)에 나타난 대로 PQC 알고리즘에 사용될 비밀키가 NVM에 저장되기 전에 PUF 키로 암호화된다면, 공격자에 의해 NVM 데이터가 노출되더라도 암호화된 이미지만 노출될 것이다. 디바이스마다 고유한 PUF 키 값을 알고 있지 않는 한 노출된 데이터는 무용지물이다. PUF 키 값은 각 보안칩 내부에서 생성되는 비밀값이며 저장되지 않고 필요할 때 마다 재생하여 사용한다.

5.2. PQC 비밀키의 칩 내부 생성

다른 방법으로 PQC 비밀키를 칩 내부에서 생성한다면 발급과정에서 발생할 수 있는 노출 위험도를 없앨 수 있을 것이다. 각 디바이스 내장된 고유의 비밀값인 PUF에서 파생된 비밀키를 생성하는 것이다. PUF가 제공하는 기본 속성은 PQC 알고리즘이 요구하는 속성과 같기 때문에 PUF값으로부터 PQC 비밀키를 파생시켜 사용할 수 있다.

그러나 PQC 비밀키에 대한 특별한 요구조건이 있어서 PUF값을 그대로 사용하기가 어렵다면, PQC 비밀키의 엔트로피가 필요로 하는 만큼의 PUF 비트를 생성하고 PUF 비트를 PQC 비밀키 생성 로직의 시드 값 (seed number)으로 사용할 수 있다 [12]. 이렇게하면 PUF를 사용하는 이점을 극대화하기 위해 고유한 비밀 키를 필요할 때마다 생성할 수 있기 때문에 플래시나 OTP와 같은 NVM 메모리에 해당 비밀키를 저장할 필요가 없다. 이는 PUF 기술이 지원하는 비밀키의 "온디맨드 (On-Demand)" 생성 기능이다.

Ⅵ. PQC 칩과 PUF 기술의 통합방법

6.1. PQC 칩과 PUF 칩의 오프칩 통합성

PQC 칩과 PUF 칩이 PCB 보드 상에서 오프칩 연결로 통신한다면, PUF 칩 내부에 암호화된 상태로 PQC 비밀키를 저장하고 필요할 때 해당 비밀키를 꺼내 사용하는 것이다. 여기에서 두 칩 간의 통신은 암호화 상태로 이루어져야 한다. 그렇지 않으면 두 칩 간의 전송 중에 키 유출의 위험이 있다. 두 칩 간의 보안 프로토콜을 적용하는 통신 보안을 먼저 만들고, PUF 칩의 디바이스 인증을 실행하여 진성임을 확인한 후, PUF 칩에 내장되어 있는 PQC 비밀키를 암호화하여 PQC칩으로 전송한다.

또한, 암호화된 PQC 비밀키가 전송된 후, PQC 칩 내에서는 암호화되어 있는 키를 복호화 해야 하며 칩 내에 있는 PQC 엔진으로 안전하게 전송되어야 한다.

PCB보드 상에서 두 칩 간에 이루어지는 오프칩 통신은 많은 취약점이 있을 수 밖에 없다. 그것을 보완하고자 통신보안이 필요하고 또한 PQC 비밀키의 암호화를 추가해야 하는 이중 보호 장치가 필요하다. 다음의 차선책으로 PCB 보드가 아니고 두 개의 다이를 하나의 칩으로 패키지를 하는 방법이다. 이것은 PCB 보드의 경우 보다는 보안상 좋은 방법이나 여전히 통신 보안 등의 추가 보안 장치가 필요하다.

6.2. PUF IP의 온 칩 통합

PUF IP의 형태로 PQC에 단일 칩으로 통합되는 경우, 두 가지의 PUF 활용 방법이 있다. PQC 비밀키를 외부에서 생성해서 주입하는 경우와 PUF에 의해서 자체 생성해서 사용하는 경우이다. 외부 주입의 경우에는 PUF key를 이용하여 암호화해서 메모리에 저장하는 방법은 앞서 기술한 바와 같다. 이 경우 한가지 고려해야 할 사항은 PQC 비밀키가 칩 내부의 시스템 버스를 통해서 이동한다면, 침투성 혹은 비침투성의 다양한 유형의 공격에 의해 그 값이 노출될 수 있다. 따라서 시스템 버스를 이동할 때는 전송을 위한 보안 프로토콜이 필요하다. 하드웨어 인증 프로토콜이나 시스템 버스 스크램블링 (scrambling)과 같은 것이 이에 해당한다.

민감한 비밀키의 이동은 시스템칩의 시스템 버스를 이용하기 보다는 전용 채널을 사용하는 것이 최근의

경향이다.

Ⅶ. 결 론

양자 컴퓨터의 등장에 대한 대응으로 NIST의 PQC 알고리즘들이 선정되었다. 이것은 양자컴퓨터로도 깨지기 힘든 수학적인 해결책을 제공할 수는 있다. 그러나, 이러한 알고리즘들이 PQC 비밀키 관리에 대한 보안성까지 보장할 수는 없다. 이에 본 논문에서는 PUF를 기반으로 하여 PQC 비밀키를 안전하게 관리하는 방법을 소개하였다. PUF 값은 각 칩마다 다른 고유의 비밀값이므로 이로부터 파생된 PUF 키를 만들어서 PQC 비밀키를 암호화해서 보호할 수가 있다. 다른 방법으로는 PUF값 자체로부터 PQC 비밀키를 만들어 내어 사용할 수 있는 방법이 있다. 이 경우에는 외부로부터 비밀키를 주입할 필요가 없으며 메모리에 그 키를 저장해 둘 필요도 없다. 필요할 때마다 PUF 값으로부터 PQC 비밀키를 생성시키면 된다. 메모리에 비밀키를 저장하지 않으므로 키 값을 알아내려는 외부 공격으로부터 안전하게 보호할 수 있다. 트렌지스터를 활용하는 능동소자 (Active device) 성격의 PUF 보다는 Via-PUF처럼 수동소자 (Passive device)의 성격을 지닌 PUF는 외부 환경의 영향에 민감하지 않고 안정적인 보안의 기능을 제공한다.

참 고 문 헌

[1] Peter Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,” *SIAM J. Comput*., 26 (5): 1484-1509, 1996.

[2] R. Anderson and M. Kuhn (2016), "Tamper Resistance: A Cautionary Note", presented at *the Proc. 2nd USENIX Workshop Electron. Commerce*, Berkeley, CA, USA

[3] Ross Anderson and Markus Kuhm (1997), "Low Cost Attacks on Tamper Resistant Devices", in *Proc. 5th Int.Workshop Secur. Protocols*, 1997, pp 125-136. doi: 10.1007/BFb0028165.

[4] S. P. Skorobogatov (2005), "Semi-invasive attacks: a new approach to hardware security analysis", PhD Thesis, University of Cambridge. Ph. D. dissertation, 2005.

[5] F. Courbon, S. Skorobogatov, and C. Woods (2016), "Reverse Engineering Flash EEPROM Memories Using Scanning Electron Microscopy", in *Proc. 15th Int. Conf. Smart Card Res. Adv. Appl. (CARDIS)*, Cham, 11 2016, vol 10146, pp 57-72. doi: 10.1007/978-3-319-54669-8_4.

[6] D. Jeon, et al. “A Physical Unclonable Function with Bit Error Rate < 2.3 × 10-8 based on Contact Formation Probability Without Error Correction Code,” *IEEE Journal of Solid-State Circuits*, vol. 55, no. 3, pp. 805-816, Mar. 2020.

[7] D. Jeon, D. Lee, D. K. Kim, and B.-D. Choi, “A 325 F2 Physical Unclonable Function Based on Contact Failure Probability with Bit Error Rate < 0.43 ppm after Preselection With 0.0177% Discard Ratio,” in *IEEE Journal of Solid-State Circuits*, July 2022.

[8] Alper Kerman, “Zero Trust Cybersecurity: ‘Never Trust, Always Verify”, Available at https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify

[9] Roberto Avanzi, Joppe Bos, Leo Ducas, Eike Kiltz, Tancrede Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, Damien Stehle, “CRYSTALS-KYBER Algorithm Specifications And Supporting Documentation (version 3.01)”

[10] Shi Bai, Leo Ducas, Eike Kiltz, Tancrede Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler and Damien Stehle (2021), "CRYSTALS-Dilithium Algorithm Specifications and Supporting Documentation (version 3.1)".

[11] https://www.sogis.eu/documents/cc/domains/sc/JIL-Minimum-Site-Security- Requirements-v3.0.pdf

[12] Bertrand Cambou, et. al. (2021), "Post Quantum Cryptographic Keys Generated with Physical Unclonable Functions". *Appl. Sci*. 2021, 11, 2801.

〈저 자 소 개〉

이 경 택 (Teddy Kyung Lee)
정회원
1993년 2월 : 서울대학교 전자공학과 졸업 학사
1996년 5월 : The University of Texas at Austin, Electrical and Computing Engineering 석사
1999년 12월 : The University of Texas at Austin, Electrical and Computing Engineering 박사
2000년~2007년 : Sun Microsystems, Sunnyvale, CA
2007년~2014년 : Altera Co., San Jose, CA
현재 : ICTK SoC 그룹장/전무이사/CSO
<관심분야> 전자공학, Post Quantum Cryptography, SoC Architecture and Low power design, Security Chip Development, PUF Technology

전 두 현 (Duhyun Jeon)
2011년 2월 : 한양대학교 전자통신컴퓨터공학부 졸업
2020년 8월 : 한양대학교 전자컴퓨터통신공학과 박사
2020년 2월~현재 : ICTK 책임
<관심분야> 전자공학, 정보보호, PUF, 보안회로