JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 30 No. 8, pp. 147-154, August 2025
https://doi.org/10.9708/jksci.2025.30.08.147

Design and Evaluation of PUF-Based Embedded Module for Hybrid Post-Quantum Cryptographic Communication

Young-One Cho*, Yun-Seok Choi**, Sang-Hoon Han***

*Lecturer, School of Computer Engineering & Applied Mathematics, Hankyong National University, Pyeongtaek, Korea
**Director of Research, Dept. of Research and Development, DigitalNetset, Seoul, Korea
***Professor, School of Computer Engineering & Applied Mathematics, Hankyong National University, Pyeongtaek, Korea

[Abstract]

This study proposes a hybrid cryptographic communication system that integrates PUF-based device authentication and PQC encryption to address the vulnerabilities of conventional public-key cryptography in the quantum computing environment. The proposed system features a three-layer architecture that combines SRAM PUF-based unique device identification with the Kyber-768 key exchange mechanism. Implemented in an embedded environment, the system was evaluated in terms of performance and resistance against various attack scenarios, demonstrating its practicality and security. Comparative analysis with RSA and ECC-based schemes showed superior processing speed and resource efficiency. These results suggest that the proposed hybrid system combining PUF and PQC can serve as a emerging alternative for IoT security in the era of quantum computing.

▸ **Key words**: Post-Quantum Cryptography, Physically Unclonable Function, Embedded Security, Hybrid Cryptographic System, SRAM PUF

[요 약]

본 연구는 양자컴퓨팅 환경에서 기존 공개키 암호의 취약점을 보완하기 위해, PUF 기반 장치 인증과 PQC 암호화 기술을 통합한 하이브리드 암호통신 시스템을 제안한다. 제안된 시스템은 SRAM PUF를 통해 디바이스 고유 정보를 생성하고, Kyber-768 기반 키 교환 방식과 결합한 3계층 구조로 설계되었다. 임베디드 환경에서 구현된 시스템은 성능 분석 및 다양한 공격 시나리오에 대한 보안 저항성 평가를 통해 유효성과 신뢰성을 입증하였다. 또한 RSA 및 ECC 기반 기존 방식과 비교하여 처리 속도와 자원 효율성 면에서 우수한 결과를 보여주었다. 이를 통해 PUF와 PQC를 결합한 하이브리드 통신 시스템은 향후 양자컴퓨팅 시대의 IoT 보안 솔루션으로서 실질적인 대안이 될 수 있음을 확인하였다.

▸ **주제어**: 양자내성암호, 물리적복제 불가능함수, 임베디드 보안, 하이브리드 암호통신, IoT 보안

• First Author: Young-One Cho, Co-Author: Yun-Seok Choi, Corresponding Author: Sang-Hoon Han
*Young-One Cho (one2003@hanmail.net), School of Computer Engineering & Applied Mathematics, Hankyong National University
**Yun-Seok Choi (yacaeh@gmail.com), Dept. of Research and Development, DigitalNetset
***Sang-Hoon Han (hansh0903@hknu.ac.kr), School of Computer Engineering & Applied Mathematics, Hankyong National University
• Received: 2025. 07. 28, Revised: 2025. 08. 07, Accepted: 2025. 08. 18.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

양자 컴퓨팅 기술의 발전은 RSA, ECC 등 현재 공개키 암호 체계의 취약성을 드러내며 변화를 요구하고 있다. 1994년 Shor(쇼어) 알고리즘은 충분한 큐비트를 가진 양자 컴퓨터가 기존 공개키 암호시스템을 다항시간 내에 해독할 수 있음을 보여 주었다[1]. 2019년 Google의 양자 우월성 달성 발표 이후 양자 컴퓨팅 실용화가 생각보다 빠르게 현실적으로 다가오고 있으며[2], 미국 국가표준기술연구소(NIST)는 2022년 4개의 양자내성 암호 알고리즘을 표준으로 선정하였다[3,4].

양자내성 암호(PQC, Post-Quantum Cryptography)의 대표적인 키 교환과 디지털 서명 표준 알고리즘은 각각 CRYSTALS-Kyber, CRYSTALS-Dilithium 등으로 격자 문제, 코드 기반 문제 등 양자 컴퓨터로도 해독하기 어려운 수학적 문제를 기반으로 한다[5,6,7]. 또한 PQC는 기존 암호대비 큰 값의 키 크기(Kyber-768 공개키 1,184바이트 vs RSA-2048 256바이트), 높은 연산 복잡도, 빠른 메모리를 필요로 한다[8]. 이처럼 자원에 대한 높은 요구에도 불구하고, 사용이 지속적으로 증가하는 IoT 디바이스의 보안을 강화하기 위해, 키 생성 및 관리 부담을 줄일 수 있는 PUF와 PQC를 결합하려는 연구가 최근 활발히 이루어지고 있다.

물리적 복제 불가능 함수(PUF, Physically Unclonable Function)는 제조 과정의 물리적 변이를 이용해 디바이스마다 복제 불가능한 고유한 특성을 생성하는 기술이다[8]. 특히 SRAM PUF는 기존 하드웨어를 활용하므로 추가 비용이 필요 없고, 전원 인가시 SRAM 셀의 초기 상태 패턴이 디바이스마다 고유하게 결정된다[9]. 이처럼 PUF는 디바이스 키 정보를 미리 만들고 저장해 둘 필요가 없어 임베디드 환경에서 단순하고 효율적으로 키를 생성, 관리할 수 있다.

본 연구에서는 PUF 기반 하드웨어 신뢰성과 PQC의 양자내성 특성을 통합한 하이브리드 암호통신 시스템을 제안하고, 이를 임베디드 환경에 구현하여 유효성과 보안성을 평가하였다. 이를 위해 2장에서는 관련 연구를, 3장에서는 기반 기술을 살펴본 후, 4장에서는 PUF와 PQC를 계층적으로 결합한 시스템 구조를 설계하고 다양한 공격 시나리오를 제시하였다. 마지막으로 5장에서는 제안한 시스템의 성능과 시나리오별 보안성을 평가하고, 기존 보안 시스템과의 성능을 비교하였다.

II. Related works

국내에서는 한국전자통신연구원(ETRI), 한국표준과학연구원(KRISS) 등의 여러 연구기관들과, 한국과학기술원(KAIST), 한화시스템, 그리고 광주과학기술원(GIST) 등의 대학과 기업들 또한 연구와 투자에 집중하고 있다. SK 텔레콤과 KT는 양자 키 분배(QKD)와 관련된 제품을 출시하였고 LGU+도 PQC에 대한 제품 연구를 수행 중에 있다.

NIST는 지난 2025년 3월, PQC 표준 후보 4개에 대한 표준화를 마무리 하면서 기존 공개키 알고리즘은 2030년 이후 단계적으로 폐지하기로 계획하였다[10].

PUF와 PQC를 결합하는 기술에 대한 연구는 아직 초기 단계라고 볼 수 있다. Herder et al. [11]은 PUF와 양자내성 암호 PQC를 결합하기 위한 이론적인 프레임워크를 최초로 제시했으나 실제 구현은 없었다. Chatterjee et al. [12]은 Ring-LWE와 SRAM PUF 에 대한 통합 방안을 제시했지만 Helper Data에 대한 보안성 분석이 부족했다. Zhang et al. [13]은 Kyber와 Arbiter PUF가 결합된 IoT 시스템을 제안했으나 모델링의 공격에 대한 취약성 평가와 실제 성능 평가가 제한적이었다.

기존 연구는 대부분 이론적인 분석에 치중해 실증적인 측면에서의 평가가 부족했다고 볼 수 있다. 이들 기술의 보안 취약점으로 제시되고 있는 머신러닝 PUF 모델링 공격, Helper Data 탈취 공격, Side-channel 공격 등에 대한 체계적 분석이 미흡하며, 임베디드 환경에 적용 가능한 성능의 최적화에 대한 연구가 아직 충분하지 않다. 또한 PQC 알고리즘은 큰 값을 가지는 키의 크기와 높은 계산 복잡도를 요구하여 IoT 및 임베디드 환경에서 직접 활용하기 어렵다. 이러한 PQC의 한계를 보완하고 보안성을 실질적으로 검증하기 위한 연구가 더욱 요구된다.

III. Background

1. Post-Quantum Cryptography(PQC)

PQC는 양자 컴퓨터의 공격에도 안전한 암호 알고리즘들을 총칭한다. 기존의 RSA, ECC 등은 정수 인수분해 문제나 이산 로그 문제의 계산 복잡성에 의존하는데, 이들은 쇼어 알고리즘에 의해 양자 컴퓨터 환경에서 다항 시간 내에 해결될 수 있다. 이 때문에 기존의 공개키 알고리즘은 양자 컴퓨터에서 취약점을 가질 수밖에 없다. PQC는 양자 환경에 강한 수학적 구조에 기반하며 대표적으로 고차원 격자에서 벡터를 찾는 격자 기반(Lattice-based)의 방식

과 일방향 해시 함수의 역함수를 계산하는 해시 기반(Hash-based)의 방식이 있다.

NIST가 선정한 키 교환 메커니즘 CRYSTALS-Kyber는 격자 기반 Ring-LWE의 구조를 계승한 Module-LWE 기반의 암호 시스템으로, 다항식 링에서의 계산 구조를 활용하여 효율성과 보안성을 동시에 확보한다. 다음은 Ring-LWE 기반의 키 생성, 암호화, 복호화 과정을 간략하게 나타낸 것이다.

1) 키 생성과정
s1. 다항식 링 R_q, 잡음 벡터 x 에서 비밀키 s 생성
$s \leftarrow x^n \subset R_q$ where, $R_q = Z_q[X] / (X_n + 1)$
s2. 공개키 A와 에러 e를 이용하여 $t = As + e$ 계산
s3. 공개키 $pk = (A, t)$, 비밀키 $sk = s$

2) 암호화 과정
s1. 메시지 m 과 랜덤값 r 선택
s2. 암호문 c 계산
$c = (u, v) = (A^T r+e1, t^T r+e_2 + \lfloor q / 2 \rfloor m)$

3) 복호화 과정
s1. $m' = \lfloor 2 / q \rfloor (v - s^T u)$ 계산
s2. 반올림을 통해 원본 메시지 m 복원

2. Physically Unclonable Function(PUF)

PUF는 디바이스마다 고유한 응답을 생성하는 하드웨어 보안 프리미티브로, 챌린지(Challenge) C를 입력으로 받고 응답(Response) R을 출력하는 함수로 $R=PUF(C)$ 와 같이 모델링할 수 있다.

본 연구에서 사용하는 SRAM PUF는 키를 생성하는데 SRAM의 몇 가지 주요한 특징을 활용한다. 전원을 인가하면 SRAM 셀들은 무작위로 0 또는 1의 값을 갖는데 이들 각 셀의 초기 값은 제조 공정의 미세한 차이에 의해 결정된다. 이 때, 동일한 SRAM은 전원 재인가 시 초기 값과 유사한 패턴을 보이고, 서로 다른 SRAM의 경우 각자 다른 고유 패턴을 가진다. 이런 특성에 의해 SRAM 패턴은 하드웨어 보안 장치의 고유 지문처럼 활용될 수 있다.

그러나 SRAM PUF는 온도, 전압, 노화 등 환경 변화에 따라 노이즈가 발생할 수 있어, 동일 디바이스에서도 일부 비트 값이 불안정하게 변동되는 한계가 존재한다. 이를 해결하기 위해 주로 사용되는 기법에는 Helper Data, Fuzzy Extractor가 있다. Helper Data는 처음 비밀키를 추출하면서 생성, 저장되는 정보로 이후로도 동일한 비밀키를 복원하기 위해 활용되는 보조 데이터이다. Fuzzy Extractor는 PUF의 응답으로부터 Helper Data를 생성하고. 또 이를 활용해 동일한 비밀키를 복원해 내는 보안 메커니즘이다.

IV. The Proposed Scheme

본 연구에서는 PUF 기반의 디바이스 인증과 PQC 기반의 양자내성 통신을 결합하여 기존 시스템보다 안전하고 효율성이 높은 하이브리드 암호통신 시스템을 제안하고 이에 대한 유효성과 보안성을 분석하였다. 3개 계층으로 구성된 제안 시스템의 구조와, 시스템 보안성 분석에 활용될 세 가지 공격 시나리오를 살펴보도록 하겠다.

1. Layer 1: PUF Layer

하드웨어 계층에서는 전원을 인가하고 SRAM-PUF의 초기 응답 값을 추출한다. SRAM 셀들은 전원 인가 시 셀 트랜지스터의 최소 요구 값인 문턱 전압 차이에 따라 0 또는 1로 초기화된다. 이렇게 PUF의 응답으로 얻을 수 있는 셀의 초기값 R_i 의 수식은 (식 1)과 같고, 수식에 사용된 V_{th1}, V_{th2}는 문턱 전압을 의미한다. 이 초기 값에 대한 고유성은 (식 2)의 해밍 거리를 기반으로 측정하였다.

$$R_i = \begin{cases} 0, & V_{th1} > V_{th2} \\ 1, & V_{th1} \leq V_{th2} \end{cases} \quad \text{(식 1)}$$

$$Uniqueness = \frac{1}{n}\sum_{i=1}^{n}\frac{HD(R_i, R_j)}{l} \times 100\% \quad \text{(식 2)}$$

- $HD(R_i,R_j)$: 응답간 해밍 거리
- l : 응답 길이, n = 디바이스 쌍의 수

전통적인 Fuzzy Extractor 기반의 Helper Data 방식은 PUF 응답(R)의 유출 위험이 있을 뿐만 아니라 helper data(H)가 정적 형태로 존재하기 때문에 추측 공격이나 side-channel 공격에 상대적으로 취약할 수 있다. 이에 본 연구에서는 기존 Helper Data 구조에 내재된 정적 취약성과 노출 위험을 완화하기 위해 개선된 Helper Data 생성 알고리즘을 다음과 같이 제안한다.

mask ← GenerateRandomMask($|R|$)
$R' \leftarrow R \oplus mask$
(K, syndrome) ← BCH_Encode(R', t)
hash_chain ← Generate_Hash_Chain(K)
H ← (syndrome, mask, hash_chain, timestamp, temp)
output : (H, K)

- R : PUF의 응답 값, H : helper Data
- t : 오류 정정 파라미터
- K : 내부에서 사용되는 비밀키(seed)

제안된 알고리즘의 주요한 특징은 크게 세 가지이다. 첫 번째 랜덤 마스킹을 통한 외부 추정 방지, 두 번째 해시 체인을 통한 키 재사용 방지, 그리고 세 번째 타임스탬프 기반의 환경 적응성을 가진 Helper Data 생성이다. 이는 물리적 응답의 고유성과 BCH 인코딩의 에러 정정 능력을 유지하면서, Helper Data에 대한 보안성과 유연성을 확보하게 해준다.

2. Layer 2: PQC Layer

시스템 2계층에서는 PQC Kyber-768의 KeyGen()에 PUF를 결합하여 안전성이 보완된 키 생성 알고리즘을 제안한다. 이로부터 생성된 공개키와 비밀키는 캡슐화, 역캡슐화 알고리즘에 의해 암호화되어 안전하게 키를 교환하는데 활용된다.

1) Kyber-768 키 생성

KeyGen(R, H) : $\rho, \sigma \leftarrow$ Extract(R, H)
$A \leftarrow$ Parse(XOF(ρ))
$s, e \leftarrow \beta\_\eta(\sigma)$
$t := A \cdot s + e$
return ($pk = (A, t)$, $sk = s$)

- A : 공개 행렬, s, e : 비밀 잡음 벡터
- ρ, σ : 난수 시드

2) 캡슐화

Encaps(pk) : $m \leftarrow \{0, 1\}^{256}$
$(\bar{K}, r) \leftarrow G(m)$
$c \leftarrow$ Encrypt(pk, m, r)
$K \leftarrow$ KDF($\bar{K}$, $H(c)$)
return (c, K)

- m : 무작위 시드 값, r : 암호화를 위한 무작위 값
- $\bar{K}$: 임시 세션키, K : 최종 세션키
- c : 공개키의 암호문, H(c) : 암호문의 해쉬값

3) 역캡슐화

Decaps(sk,c) : $m' \leftarrow$ Decrypt(sk, c)
$(\bar{K}', r') \leftarrow G(m')$
$c' \leftarrow$ Encrypt(pk, m', r')
if $c = c'$ then $K \leftarrow$ KDF($\bar{K}'$, $H(c)$)
else $K \leftarrow$ KDF(s, $H(c)$)
return K

- c' : 암호문 후보

Kyber-758 키 생성 단계에서 KeyGen()은 입력 값으로 1계층에서 생성된 SRAM-PUF의 응답 R과 Helper Data H를 받아 디바이스 고유성이 결합된 난수 시드를 추출한다. 이를 활용해 공개 행렬과 비밀 잡음 벡터를 도출한 후 공개키(pk)와 비밀키(sk)를 생성하였다. 캡슐화 단계에서 Encaps()는 무작위 값들을 기반으로 앞 단계에서 생성된 공개키를 암호화한 후 암호문의 해시값과 후보 세션키에 KDF(키 도출 함수)를 적용해 최종 세션키를 얻는다. 역캡슐화 Decaps()에서는 암호문를 비밀키로 복호화하여 후보 세션키와 무작위 값을 추출하고 이들을 이용해 암호문 후보를 생성한 후 원본 암호문과의 비교를 통해 최종 세션키 K를 확정한다.

3. Layer 3: Hybrid Security Layer

3계층에서는 1계층의 디바이스 고유 PUF 응답과 2계층의 PQC 키 교환 메커니즘을 기반으로 세션 키와 보안 통신을 설정하는 하이브리드 키 교환 프로토콜을 제안한다. 이 과정은 아래와 같이 총 4단계로 이루어져 있다.

1) PUF 기반 상호 인증

Alice와 Bob은 각자의 PUF 응답을 이용해 상호 인증을 수행하며, 이 과정에서 디바이스 고유의 PUF 응답과 Challenge-Response 구조를 기반으로 신뢰성 있는 인증 토큰을 생성하고 상호 교환한다.

Alice → Bob : PUF_ID_A, $Challenge_A$
Bob → Alice : PUF_ID_B, $Challenge_B$, $Response_A$
Alice → Bob : $Response_B$, $Auth\_Token_A$
Bob → Alice : $Auth\_Token_B$

2) Kyber 기반 키 교환

상호 인증이 완료된 후, PUF의 고유 값을 입력으로 사용하여 Kyber-768 키 쌍을 생성하고 키 교환을 수행한다. Alice는 자신의 키 쌍을 생성한 뒤, 공개키를 Bob에게 전송하며, Bob은 해당 공개키를 기반으로 캡슐화를 수행하고 생성된 암호문을 다시 Alice에게 전송한다.

Alice : $(pk_A, sk_A) \leftarrow$ Kyber.KeyGen(PUF_Seed_A)
Alice → Bob : pk_A
Bob : $(ct, ss_B) \leftarrow$ Kyber.Encaps(pk_A, PUF_Seed_B)
Bob → Alice : ct
Alice : $ss_A \leftarrow$ Kyber.Decaps(ct, sk_A)

3) 세션 키 도출 과정

Kyber로부터 생성된 공유 비밀키 ss_A와 양측의 PUF 응답 값을 활용하여 HKDF(HMAC-based Key Derivation Function)를 기반으로 세션 키 K_Sess를 도출한다. 이 때 salt 값은 Alice와 Bob의 PUF 응답을 연결한 값으로 설정되며, 세션 키는 (식 3)를 통해 계산된다.

K_Sess= HKDF-Extract-Expand(salt, ikm, info, L) (식 3)

- salt : $PUF\_Response_A$ || $PUF\_Response_B$
- ikm : ss_A (Kyber shared secret)
- info : "HybridPQC-SessionKey-v1.0"
- L : 256 bits

4) 보안 통신 설정

도출된 세션 키를 바탕으로, 실제 통신에서 사용할 암호화 키 K_Comm을 파생한다. 이 키는 통신 방향성과 시퀀스 정보를 포함한 context 값을 입력으로 하여 (식 4)과 같이 계산된다. 이 과정을 통해 제안한 시스템은 PUF 기반 인증과 PQC 기반 키 교환을 통합함으로써, 고유하고 안전한 보안 통신 설정이 가능하다.

K_Comm = HKDF-Expand(K_Sess, context, 256) (식 4)

4. Security Evaluation Model

4.1. Overall System Security Strength

전체 시스템이 제공하는 보안 수준 Security_Strength는 (식 5)에서와 같이 가장 취약한 구성요소의 보안 강도로 결정되며 bits 단위로 측정된다. PUF_Entropy는 PUF의 고유성, 신뢰성, 엔트로피 및 모델링 공격 저항성과 같은 특성을 기반으로 실험 결과를 통해 평가될 수 있으며, Kyber_Security는 Kyber-768 알고리즘의 보안 등급기준에 따라 정의된다.

Security_Strength = min(PUF_Entropy, Kyber_Security) (식 5)

4.2. Resistance to ML-based Modeling Attacks

PUF 모델링 공격이란 공격자가 PUF의 Challenge-Response Pair(CRP)를 충분히 수집하고, PUF의 내부 동작을 모델링하여 응답을 예측하는 공격이다. 우리는 시스템의 보안성을 높이기 위해 응답의 불확실성과 무작위성을 적용해 모델이 정확하게 학습하지 못하게 하였다. 머신러닝 기반 PUF 모델링 공격에 대한 저항성은 (식 6)를 이용해 측정되며 저항성 평가 기준은 Table 1과 같다.

Modeling_Resistance = 1−max(Prediction_Accuracy) (식 6)

Table 1. Security Evaluation Based on Modeling Resistance and Prediction Accuracy

Resistance	Accuracy	Security Level
> 50%	< 50%	Highly unpredictable; considered secure
40~45%	55~60%	Partially predictable; relatively secure
< 40%	> 60%	Vulnerable to attacks; insecure level

4.3. Resistance of Helper Data Against Attacks

Helper Data 공격은 공격자가 Helper Data를 유출하고 그 정보를 활용해 키를 예측하는 방법이다. Helper Data 공격 저항성 측정 방법은 (식 7)과 같고 ϵ는 비밀키를 몇 비트 유추할 수 있는지의 척도로, ϵ 값이 작을수록 H(K | H)의 값이 H(K)에 가까워져 보안성이 높음을 의미한다. 본 시스템은 정보 유출량을 최소화함으로써 공격에 대한 저항성을 강화하였다.

$$H(K \mid H) \geq H(K) - \epsilon \quad \text{(식 7)}$$

- ε : 정보 유출량, H(K) : 키 자체의 무작위성
- H(K | H) : H가 주어졌을 때 K에 대한 조건부 불확실성

4.4. Resistance to Side-Channel Attacks

전력 분석 공격은 암호 연산 과정에서 발생하는 전력 소비 패턴을 분석하여 암호 키나 내부 데이터를 추출하는 대표적인 Side-channel 공격 기법이다. 이에 대한 저항성은

(식 8)과 같이 전력 소비량과 연산 과정에서 측정된 해밍 가중치 간 상관계수 ρ의 절대값을 이용하여 Table 2와 같이 평가한다. 상관계수가 높을수록 전력소비량과 해밍가중치의 변동 패턴이 뚜렷해 데이터 또는 키의 추출이 용이하며, 낮을수록 상호 의존성이 적어 보안성이 높아진다. PUF 기반 구조는 연산 복잡도가 낮아 전력 소비 편차가 작게 나타나므로 상관계수를 낮추는데 기여할 수 있다.

$$\rho = \frac{COV(P, H)}{\sigma_P \sigma_H} \quad \text{(식 8)}$$

- P : 전력 소비량, H : 연산 데이터의 해밍 가중치
- σ_P, σ_H : 각각의 표준편차, COV() = 공분산

Table 2. Power Analysis Resistance

$\|\rho\|$	Security Level	Interpretation
< 0.1	Very High	Key extraction is nearly impossible
0.1~0.2	High	Key extraction is difficult
0.2~0.4	Moderate	Key extraction is potentially feasible
> 0.4	Low	High probability of key leakage

V. Experiment Results

1. Experimental System Setup and Environment

제안한 시스템의 하드웨어 플랫폼은 Table 3과 같다.

Table 3. Experimental Environment Configuration

Category	Specification
platform	Raspberry Pi 4 Model B (ARM Cortex-A72 Quad-core 1.5GHz)
memory	4GB LPDDR4-3200 SDRAM
Storage	64GB microSD Card
Network	Gigabit Ethernet, 802.11ac Wi-Fi
PUF HW	99.68%
Sensors	Temperature: DS18B20 Voltage : INA219

시스템의 성능 및 보안성을 평가하기 위해, 총 50개의 장치를 사용하여 각 실험을 1000회 반복 수행하였다. 또한, 시스템의 안정성과 장기 운용 가능성을 검증하기 위해 동일 환경에서 30일간 연속 운용 테스트를 진행하였다.

2. Hybrid PQC-PUF System Performance

다음 Table 4는 PUF, PQC, 전체 하이브리드 시스템 관점에서 성능을 각각 평가하고 요약한 표이다.

Table 4. Evaluation Metrics of the Proposed Hybrid Cryptographic System

Metric	Result
PUF Uniqueness	49.7%
PUF Reliability	99.8%
PQC Performance	1.23ms
System Execution Time	9.7ms
System Stability	99.68%

1) PUF 고유성(Uniqueness)

PUF 고유성은 디바이스 식별과 복제 불가한 특성의 핵심 지표로 목표 수치는 50%이다. 50개 디바이스에서 측정한 PUF 고유성은 49.7%로 이상적인 값에 근접하였다.

2) PUF 신뢰성(Reliability)

PUF 신뢰성은 키 복원 가능성을 뒷받침하는 실용적인 지표로 온도의 변화에 따른 PUF 신뢰성을 측정한 결과 -10°C에서 70°C 범위에서 94.7% 이상으로 안정적이었다.

3) PQC 키 생성 성능(Performance)

PQC의 키 생성 속도는 실시간 통신이 가능할지를 판단하는 지표이다. 실험 결과 Kyber-768이 RSA 대비 37배 빠른 1.23ms로 높은 성능의 결과를 보여주었다.

4) 통합 프로토콜 전체 수행 시간(Time)

하이브리드 시스템의 세션키 생성과 인증을 수행하는 전체 소요시간으로 실험결과 9.7ms로 실시간 통신에 충분한 효율성과 속도를 입증하였다.

5) 장기 운용 성공률(System Stability)

시스템의 실용성과 신뢰성을 총괄하는 지표로 30일간 무결성을 테스트한 결과 99.68%의 안정성을 유지하였다.

3. System Security Evaluation and Analysis

앞에서 제시한 (식 5)의 하이브리드 시스템의 전체 보안 강도 Security_Strength는 아래 수치를 근거로 실험을 통해 얻은 값인 128 bits이다.

- PUF_Entropy ≈ 128 bits (실험으로 측정한 값)
- Kyber_Security = 192 bits (NIST Level 3)

추가적으로, 세 가지 공격 모델에 대한 시스템의 보안 저항성은 (식 6) ~ (식 8)을 기반으로 측정되었으며, 각 공격 시나리오별 보안 저항성을 평가한 정량적 결과는 Table 5에 제시되어 있다. ML 모델링 공격의 경우, 다섯 가지 머신러닝 알고리즘을 활용하여 예측 실험을 수행한 결과 예측 정확도 56.7%, 즉 저항성 43.3%가 도출되었으며, 이는 Table 1의 기준에 따라 안전한 수준으로 평가된다. Helper Data 유출에 대해서는 정보 이론 기반 분석을 기반으로 실험을 진행하였고, 정보 유출량이 0.1 bits 미만으로 측정되어 충분한 보안성을 확보한 것으로 판단된다. 마지막으로 Side-Channel 공격의 경우, 전력 및 타이밍 분석 기법을 적용한 결과, 상관계수의 절댓값이 0.15 미만으로 나타나 Table 2의 기준에 따라 안전성을 유지하는 것으로 분석된다.

그래프 Fig. 1은 Table 5에 정리된 정량적인 실험 결과를 바탕으로, 각 공격 유형에 대한 상대적 보안 수준을 백분율로 환산하여 시각적으로 표현한 것으로 모두 90% 이상의 높은 수준의 보안성을 나타내었다.

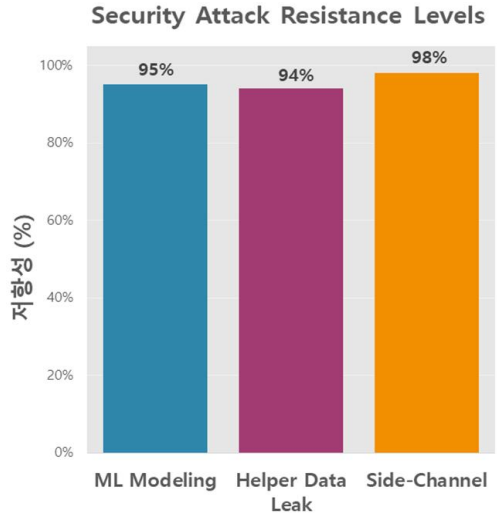

Fig. 1. Security Resistance Against Three Attack Models

Table 5. Security Evaluation Results Against Three Attack Models

Attack Type	Resistance Evaluation Result
ML Modeling	Prediction Accuracy : 56.7% → Resistance : 43.3%
Helper Data Leakage	Information Leakage : ε < 0.1 bits
Side-Channel	Correlation Coefficient : $\lvert\rho\rvert$ < 0.15

4. RSA/ECC System Performance Comparison

Table 6는 제안한 하이브리드 암호 시스템과 기존의 RSA-2048, ECC-P256 방식 간의 성능을 비교한 결과이다. 제안 시스템은 키 생성 시간(1.23ms) 및 키 교환 시간(3.1ms)에서 기존 방식 대비 월등히 빠른 성능을 보이며, 실시간 통신이 요구되는 임베디드 환경에 적합한 속도를 확보하였다. 비록 공개키 크기는 1,184B로 상대적으로 크지만, 전체 메모리 사용량(4.2KB)은 임베디드 장치에서도 효율적으로 운용 가능한 수준이다. 또한, RSA 및 ECC와 달리 양자 내성 및 하드웨어 기반 신뢰점(PUF)을 제공하여 보안성과 실용성을 모두 갖춘 구조임을 입증하였다.

Table 6. Performance Comparison : RSA-2048, ECC-P256, and the Proposed System

Metric	RSA -2048	ECC -P256	Proposed System
Key Generation Time	45.2ms	12.3ms	1.23ms
Key Exchange Time	8.9ms	3.4ms	3.1ms
Public Key Size	256B	64B	1,184B
Memory Usage	2.1KB	1.8KB	4.2KB
Quantum Resistance	-	-	√
Hardware Trust Anchor	-	-	√

VI. Conclusions

본 논문에서는 PUF 기반 하드웨어 신뢰성과 PQC 양자 내성 특성을 결합한 하이브리드 암호통신 시스템을 설계하고, 이를 임베디드 환경에 구현하여 유효성과 보안성을 검증하였다. 제안된 3계층 구조는 안정적인 키 생성 메커니즘과 향상된 Helper Data 처리 방식을 포함하고 있다.

실험 결과, 고유성 49.7%, 신뢰성 99.8%, 전체 프로토콜 수행 시간 9.7ms, 보안 저항성 90% 이상, 30일간 무결성 운용 성공률 99.68%를 기록하여 높은 안정성과 처리 성능을 입증하였다. 또한 RSA 및 ECC 기반 시스템 대비 최대 37배 빠른 키 생성 속도와 낮은 메모리 사용량으로 임베디드 환경에 효율적인 적용 가능성을 보여주었다. 이러한 결과를 바탕으로, 본 연구는 양자컴퓨팅 시대의 IoT 보안을 위한 기술적 대안을 제시하였으며, PUF와 PQC의 통합 구조를 실제로 구현하고 그 성능과 보안성을 직접 검증했다는 점에서 큰 의의를 갖는다.

향후 연구에서는 SRAM PUF의 극한 환경에서의 장기 운용 안정성을 확보하는 문제와, 대규모 IoT 환경에서의 확장성 및 키 관리 방법에 대한 심화 연구가 필요할 것으로 보인다. 더불어 다양한 공격유형에 대한 보안성을 점검하고, 서로 다른 하드웨어 환경에서도 전력 분석이나 타이

밍 공격과 같은 부채널 공격에 안전하도록 설계하는 연구가 지속적으로 수행되어야 할 것이다.

ACKNOWLEDGEMENT

This research was supported by Seoul R&BD Program(QR240018) through the Seoul Business Agency(SBA) funded by The Seoul Metropolitan Government.

REFERENCES

[1] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in Proceedings 35th Annual Symposium on Foundations of Computer Science, pp. 124-134, 1994.DOI: https://doi.org/10.1109/SFCS.1994.365700

[2] F. Arute et al., "Quantum supremacy using a programmable superconducting processor," Nature, Vol. 574, no. 7779, pp. 505-510, 2019.

[3] National Institute of Standards and Technology (NIST), "Post-Quantum Cryptography Standardization Project," NIST, https://csrc.nist.gov/projects/post-quantum-cryptography, 2022.

[4] Aghapour, S., et. al., "PUF-Kyber: Design of a PUF-Based Kyber Architecture Benchmarked on Diverse ARM Processors", IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. Vol. 16, No. 12, pp.4453-4462, Dec. 2024. DOI: https://doi.org/10.1109/TCAD.2024.3399669.

[5] J. Bos et al., "CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM," in 2018 IEEE European Symposium on Security and Privacy (EuroS&P), pp. 353-367, 2018. DOI: https://doi.org/10.1109/EuroSP.2018.00032.

[6] L. Ducas et al., "CRYSTALS-Dilithium: a lattice-based digital signature scheme," IACR Transactions on Cryptographic Hardware and Embedded Systems, Vol. 2018, no. 1, pp. 238-268, 2018. DOI: https://doi.org/10.13154/tches.v2018.i1.238-268

[7] D. J. Bernstein et al., "Post-quantum cryptography," Nature, Vol. 549, no. 7671, pp. 188-194, 2017. DOI: https://doi.org/10.1038/nature23461

[8] M. Kannwischer et al., "PQM4: Testing and Benchmarking NIST PQC on ARM Cortex-M4," IACR Cryptology ePrint Archive, 2019.

[9] D. E. Holcomb et al., "Initial SRAM state as a fingerprint and source of true random numbers for RFID tags," in Proceedings of the Conference on RFID Security, 2007.

[10] National Institute of Standards and Technology (NIST), "Post-Quantum Cryptography," NIST, 2022, https://csrc.nist.gov/projects/post-quantum-cryptography.

[11] C. Herder et al., "Trapdoor computational fuzzy extractors and stateless cryptographically-secure physical unclonable functions," IEEE Transactions on Dependable and Secure Computing, Vol. 14, no. 1, pp. 65-82, 2017. DOI: https://doi.org/10.1109/TDSC.2016.2536609.

[12] U. Chatterjee et al., "Building PUF based authentication and key exchange protocol for IoT without explicit CRPs in verifier database," IEEE Transactions on Dependable and Secure Computing, Vol. 16, no. 3, pp. 424-437, 2018. DOI: https://doi.org/10.1109/TDSC.2018.2832201.

[13] J. Zhang et al., "PUF-based secure communication protocol for IoT," ACM Transactions on Embedded Computing Systems, Vol. 19, no. 2, pp. 1-21, 2020.

Authors

Young-One Cho received the B.S. and M.S. degrees in 1994 and 1998, and was a Ph.D. candidate in 2012 in Computer Science and Engineering at Dongguk University, Korea.

Cho completed the Ph.D. coursework in Computer Engineering from Dongguk University. She has over 10 years at an IT company's R&D center. Since 2004, she has taught computer engineering courses at several universities. Her interests include artificial intelligence and computer security.

Yun-Seok Choi received the B.S., degrees in Computer Science and Engineering from Ulsan National Institute of Science and Technology, Korea, in 2018.

Choi joined Research and Development Department of DigitalNetset, Seoul, Korea, in 2021. He is currently a Director of Research at Department of Research and Development, DigitalNetset. He is interested in Information Security, Internet of Thing(IoT) and Computer Vision, and Brain Computer Interface.

Sang-Hoon Han received the B.S., M.S. and Ph.D. degrees in Computer Science and Engineering from Dongguk University, Korea, in 1990, 1995 and 2002, respectively.

Dr. Han joined the faculty of the Department of Computer Information Security at Korea National University of Welfare, Pyeongtaek, Korea, in 2003. Since 2023, he has been a professor at the School of Computer Engineering & Applied Mathematics, Hankyong National University. He is interested in Information Security, Internet of Thing(IoT) and Computer Vision, and multimedia computing.