



POSTQUANTUM
SHIELD

Make it more Secure

#하드웨어해킹 #양자내성암호

암호 제품 개발사가 공공기관(항공, 금융, 교통, 국방) 납품 앞에서 마주하는
하드웨어 해킹 인증의 벽을 넘게 해주는 서비스 (B2B)



PACL@DGIST
Privacy and Applied Cryptography Lab.



대구경북과학기술원
Daegu Gyeongbuk
Institute of Science & Technology



Background

대한민국에서 자주 발생하는 보안 사고



POSTQUANTUM
SHIELD

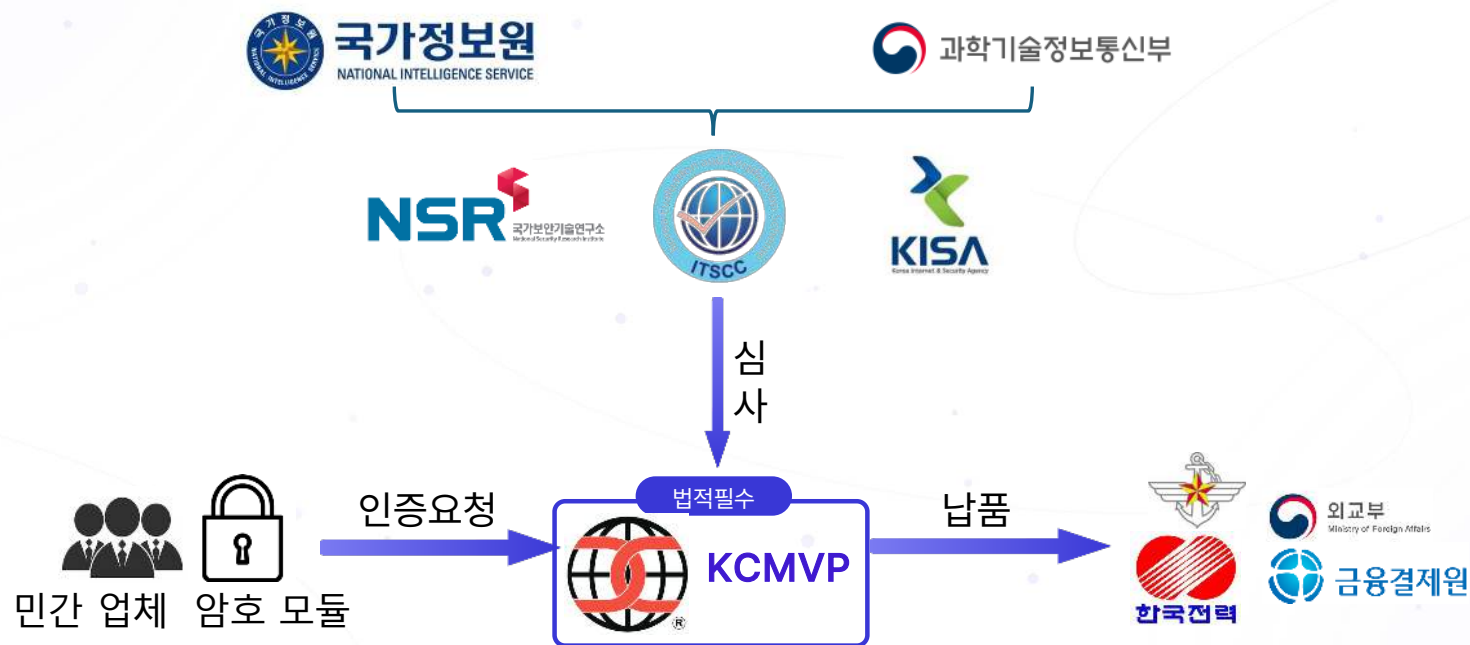


몰라서 뚫린 게 아니라, 안 막아서 뚫렸음
그래서 국가는 '인증'이라는 최소한의 방어선을 둬

Background

공공기관 납품에 보안 인증은 법적 필수 조건

국가정보원은 '검증필 암호모듈 탑재'를 국가·공공기관 도입 기준으로 필수 요구한다.



공공기관은 전 국민의 중요한 정보를 들고 있음
따라서 민간업체는 보안제품을 납품하려면 인증을 받아야 함

Problem



보안 인증을 받는 것은 어려운 과정

1 인증 기간

KCMVP ~1년

국가보안기술연구소 기준

- 시험·검증에만 최대 1년이 걸림
- 사설 업체 이용 시 3천~1억 소모

2 어려운 난이도

낮은 등급 vs 높은 등급

KCMVP 비침습 영역 적용 유무, CC AVA_VAL.5유무

- 높은 보안 등급에서는 고도화된 실험을 요구함
- SW뿐 아니라 HW에 대한 지식 필요

3 리스크

엄격한 인증

허술한 인증은 심각한 문제 초래

- 인증 실패시, 추가 기간 소요
- 지연된 만큼 납품 일정도 밀림

이러한 보안 인증은 민간 업체 입장에서 어려운 과정임
따라서, 높은 보안 등급 보다는 **낮은 보안 등급을 선호함**



POSTQUANTUM
SHIELD

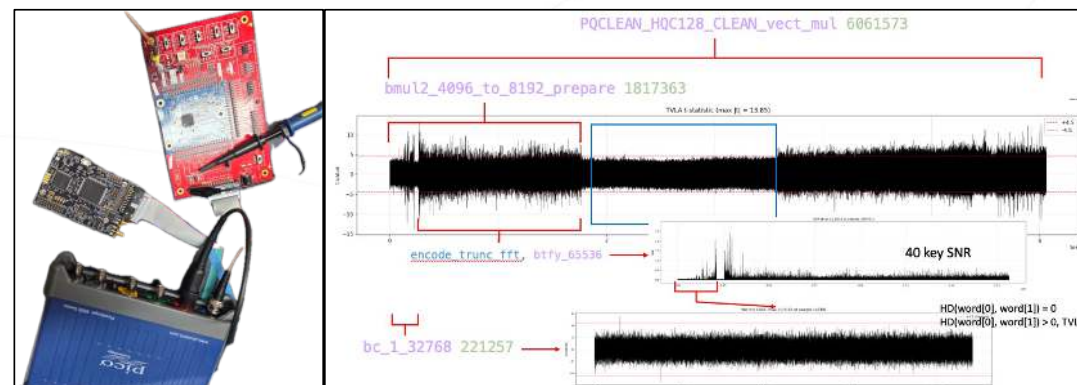
Problem

보안 인증을 받는 것은 어려운 과정

소프트웨어 검증 (KCMVP 비침습공격 X, CC AVA_VAN.5 X)

```
void expand_and_sum(rm_expanded_cdw *dest, rm_codeword_t src[]) {  
    // start with the first copy  
    for (int32_t part = 0; part < 4; part++) {  
        for (int32_t bit = 0; bit < 32; bit++) {  
            (*dest)[part * 32 + bit] = src[0].u32[part] >> bit & 1;  
        }  
    }  
    // sum the rest of the copies  
    for (int32_t copy = 1; copy < MULTIPLICITY; copy++) {  
        for (int32_t part = 0; part < 4; part++) {  
            for (int32_t bit = 0; bit < 32; bit++) {  
                (*dest)[part * 32 + bit] += src[copy].u32[part] >> bit & 1;  
            }  
        }  
    }  
}
```

하드웨어 해킹 대응 (KCMVP 비침습공격 O, CC AVA_VAN.5 O)



보안 모듈 개발 업체

장비도, 사람도, 노하우도 없기 때문에
낮은 보안 레벨인 소프트웨어 검증을 선호함

※ 비침습 공격(부채널) — 하드웨어 해킹의 일종. 칩을 뜯지 않고 전력·전자파·시간의 미세한 변화만으로 암호키를 알아낸다.
AVA_VAN.5 — 평가기관이 직접 그 공격을 수행해, 고도의 공격자에게도 안 뚫림을 실험으로 입증하는 최고 등급 시험.

Problem

국내 하드웨어 해킹 대응은 거의 없다

KCMVP (보안수준 + 비침습 옵션)

등급	전체 인증	비침습 고려
L1	104	5
L2	5	2
L3·L4	0	0
합계	109	7

KCMVP 최고등급 0건

CC (AVA_VAN.5 = 부채널 시험 옵션)

등급	전체 인증	AVA_VAN.5
EAL2	83	0
EAL4	141	0
EAL5	0	0
EAL5+	5	5

CC 인증 5건 = 전자여권 · 전자카드
국가가 꼭 필요한 곳에만 적용됐다(민간제품 X)



POSTQUANTUM
SHIELD

338건 중 12건

CC+KCMVP 338건 중 하드웨어 해킹을 고려한 것은 12건 — 3.6%

부채널 미검증

부채널 미검증

SK텔레콤

롯데카드

쿠팡

티빙

2025.04

2025.08

2025.11

2026.06

202n. ??

부채널 분석은 표준에서 요구하는 알려진 공격 방식
알려진 공격 안 막은 것 = '잠재적 대한민국 보안의 허점'

Why now?

이것은 시장의 신호다

1 국가 양자내성암호 전환 마스터플랜

2023.7.12 국가정보원 · 과학기술정보통신부



양자컴퓨팅으로 인한 기존 암호 붕괴
'제12회 정보보호의날'에서 발표.
2035년까지 국가 기반시설의 암호를 전면 교체한다.

→ 모든 인증을 다시 받아야 한다

2 양자내성암호 시범전환 착수 · 45억

2025.12.03 과학기술정보통신부 · KISA



통신 · 금융 · 교통
국방 · 우주
5개 핵심 인프라 우선 전환

→ 고신뢰 영역부터 먼저 바뀐다

3 해외는 이미 하고 있다

	프랑스	네덜란드	독일	스페인	한국
전체 CC 인증	435	314	246	75	229
AVA_VAN.5 (부채널)	318	146	72	11	5
비율	73%	47%	29%	15%	2.2%

그리고 — 해외는 '꼭 필요한 곳'에만 쓰지 않음

모빌리티 · 네트워크 · 운영체제 · 시스템 · 전자서명 · 디바이스
— 공공기관 뿐 아니라 민간 분야에 하드웨어 해킹 대응을 적용함

반면에 한국은 전자여권과 전자카드, 단 두 종류뿐임

암호를 전부 갈아엮고 있으며, 해외에는 이미 하드웨어 보안을 일상에 적용하고 있습니다.

시장에 대한 PostQuantumShield의 분석

01

암호 인증 개수가 늘어남

Classic	PQC
AES RSA ECC	ML-KEM · ML-DSA SLH-DSA · Falcon HQC · McEliece FrodoKEM ...
3종	10종+

NIST · ISO가 각각 다른 알고리즘을 표준화함

02

양자내성암호는
하드웨어 해킹에 더 취약함

NIST 공식 발표
"PQC의 부채널 대응이 가장 큰 과제"

- **Falcon** 샘플링에서 구조적 취약
- **HQC** 최근 5년 16건 보고
- **ML-KEM/DSA · McEliece** IACR · CCS 등 최상위 학회에 다수 발표

03

고신뢰 영역에는
더 높은 보안 수준의 요구 예상

통신 · 금융 · 교통 · 국방 · 우주

(정부 지침)

→ 하드웨어 해킹이 실제 위협인
영역부터 전환된다

Our Vision

양자내성암호가 도입되면서 하드웨어 해킹의 수요가 예상됨

하드웨어 해킹 보안 시장이 열리기 전에, 미리 선점한다

* HQC 부채널 건수는 자체 집계(최근 5년) | PQC 표준: NIST FIPS 203/204/205, ISO/IEC 18033-2 Am.2(McEliece-FrodoKEM), 14888-4

** NIST IR 8413 (3라운드 보고서, 2022) — "NIST표준은 경량화 디바이스에서의 성능과, 특히 부채널 공격 방어가 고려되어야 한다."; *국보연 기간과 인증 병목 현상은 드림시큐리티 신** 인터뷰 바탕으로 조사됨



POSTQUANTUM
SHIELD

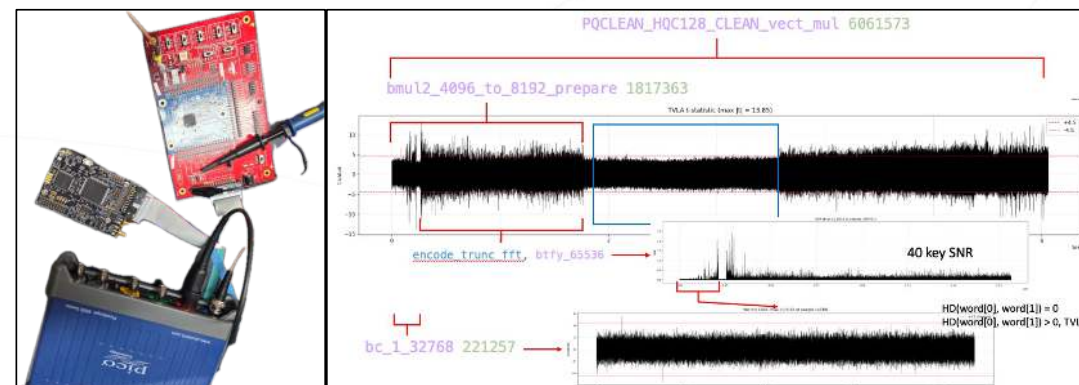
Our solution

보안 인증을 받는 것은 어려운 과정

소프트웨어 검증 (KCMVP 비침습공격 X, CC AVA_VAN.5 X)

```
void expand_and_sum(rm_expanded_cdw *dest, rm_codeword_t src[]) {  
    // start with the first copy  
    for (int32_t part = 0; part < 4; part++) {  
        for (int32_t bit = 0; bit < 32; bit++) {  
            (*dest)[part * 32 + bit] = src[0].u32[part] >> bit & 1;  
        }  
    }  
    // sum the rest of the copies  
    for (int32_t copy = 1; copy < MULTIPLICITY; copy++) {  
        for (int32_t part = 0; part < 4; part++) {  
            for (int32_t bit = 0; bit < 32; bit++) {  
                (*dest)[part * 32 + bit] += src[copy].u32[part] >> bit & 1;  
            }  
        }  
    }  
}
```

하드웨어 해킹 대응 (KCMVP 비침습공격 O, CC AVA_VAN.5 O)



보안 모듈 개발 업체

대부분 왼쪽을 선호한다 -> 이제 오른쪽 길도 열린다
장비, 사람, 노하우 없다 -> 우리가 제공한다
보안 개발 업체 대상 인증 컨설팅 서비스 (B2B)

Our solution & Roadmap

인증 컨설팅



POSTQUANTUM
SHIELD

Appendix-Exit 사례 참고

하드웨어 해킹 진단



취약점 보완



인증 대응



유지보수

한 번 통과하면 국내 납품 + 해외 수출이 동시에 열린다 (AVA_VAN.5 = 국제 공통 언어)

우리의 로드맵 | 정부 PQC 전환 일정에 맞춰 움직인다

2026

준비 · 검증

정부: 시범전환 (45억)

- 부채널 진단 파이프라인 구축
- PQC 구현 부채널 취약점 연구
- 레퍼런스 1호 고객 확보

2027

첫 인증 통과

정부: 전환 준비·기준 정립

- 국내 첫 민간업체 부채널 인증 지원 성공
- KCMVP 비침습 L3 / CC AVA_VAN.5
- 진단 툴 제품화 시작

2028-2030

본격 확장

정부: 본격 전환 착수

- 기존 모듈 재인증 대응 (326건 대상)
- 유지보수 리테이너 확대
- 국방·금융 레퍼런스 확보

2031-2035

해외 진출

정부: 전면 전환 완료

- 유럽 CC 스킴 대응 (BSI-ANSSI)
- 국내 벤더의 해외 수출 지원
- 글로벌 부채널 평가 파트너

정부가 2035년까지 바꾼다. 우리는 2026년부터 **인증 병목의 길**에 서있다

예상 시장 규모


326건

 기존 KCMVP 102 + CC 224
(부채널 미보유)

×3

PQC 암호 3배

978건

PQC 전환 대상 인증

×40%

부채널 채택률

391건

부채널 인증 대상

+ 연 신규 80건/년

신규 인증 66.6건 × 3 × 40%

건당 단가 (하드웨어 해킹 옵션)

L1	L2	L3	L4	CC AVA_VAN.5
2,500만	3,000만	5,000만	8,000만	4,000만

유지보수 500~2,000만/년

일회성

초기 시장 — PQC 전환
220 억

- 전환 391건 × 건당 단가 = 138억
- 신규 80건/년 × 5년 = 84억
- PQC 전환기(~2035)에 집중되는 수요

전환기 초기 시장

반복

유지보수 시장 — ARR
67 (+신규유입 10억) 억 / 년 (2032~)

- 5년 누적 200억 · 설치 기반 791건
- 새로운 공격이 나올 때마다 방어책 갱신
- 신규 유입 25%로 잡으면 매년 10억 추가 인증

전환기가 끝나도 남는다

Why Us

얼마나 어려운가?

암호 이해

+

하드웨어 이해

+

AI/통계 기법

PQC 알고리즘군
(Lattice · Code · Hash · MQ · Isogeny)



SPHINCS+



Fast-Fourier Lattice-based
Compact Signatures over NTRU

HQC

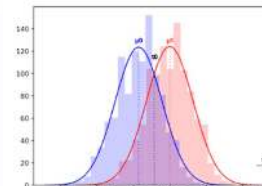
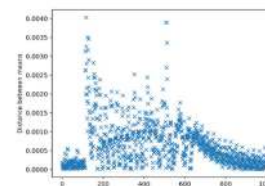
외 11종

Classic McEliece

실측 장비 운용
(오실로스코프 · 프로브 · 타겟 보드)



누출 판정 · TVLA · AI 딥러닝 분석
(수만 회 측정 · 상관분석)



AI Agent에 대체될 수 없는
인간 노하우의 영역

물리 계측 — 장비 · 프로브 · 측정 세팅



POSTQUANTUM
SHIELD

암호이해 + 하드웨어 이해 + AI/통계기법 **삼위일체**를 갖추는 데는 **수년**이 걸림

Why Us

우리는 이 기술을 이미 가졌다



전재호

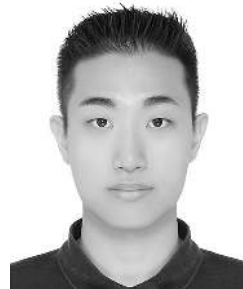
CEO

- 양자내성암호 전환 기술 공모전 최우수상
- 한국통신학회 추계 논문 최우수상
- DGIST 대학원 학생회 대표
- 前) NEX (블록체인) 수석개발자
스마트컨트랙트 자산 80억 운용, (2022~2024)
- 前) 티클 (핀테크) — 로보어드바이저 운용, (2021~2022)
- 前) 삼성SDI 차량 전지 리서처, (2018~2019)
- DGIST 석사(전기전자컴퓨터공학) / DGIST 학사(컴퓨터공학)

Our team,
Make it more Secure



POSTQUANTUM
SHIELD



박용성

CTO

Power · EM · Timing · Fault 등
하드웨어 해킹 실험 전 영역 총괄

핵심 역량 · 수상

- EKC 2025 AI-Assisted Society Challenge
Gold Prize

경력 · 학력

- DGIST EECS 석사과정
- 충북대 소프트웨어학과 학사



김명준

PQC Researcher

PQC 알고리즘 분석 · 양자 알고리즘 기반
양자내성암호 안전성 연구

핵심 역량 · 수상

- 삼성전자 시스템LSI — NIST PQC HW 가속기 개발 참여
- 2025 암호분석 경진대회 수상

경력 · 학력

- DGIST 인공지능전공 석사과정 · 전남대 수학 학사



이수성

Side-Channel Engineer

NIST 표준 PQC 부채널 실험 담당
계측 · 분석 실험 전문

핵심 역량 · 수상

- Stable Diffusion 기반 로고 UGRP 장려상

경력 · 학력

- 삼성전자 시스템LSI NIST PQC HW 가속기 개발
- DGIST EECS 통합과정
- 한국과학영재학교 졸업



조승현

Business Development

기술 사업화 · 스타트업 경험 기반 사업개발 총괄

핵심 역량 · 수상

- 2025 국가암호공모전 / 암호분석 경진대회 수상
- 2024 부산미래과학자상 — IoT PQC 구현·벤치마크

경력 · 학력

- Saksaha — Rust 기반 ZKP 메신저 개발 (R&D · 1년)
- Nethermind 암호연구팀 인턴 · Reth 컨트리뷰터
- DGIST EECS 석사과정

Advisor



POSTQUANTUM
SHIELD



김영식 교수 · 고문



2024 국무총리표창
과학기술·정보통신의 날 (정보통신유공)

- KpqC 연구단 기술자문위원/운영위원
- DGIST 전기전자컴퓨터공학과 학과장
- DGIST 인공지능전공 책임교수
- KCMVP 평가위원, 개인정보보호위원회 위원
- 前 삼성전자 반도체부문 (2007-2010)
- 서울대 전기공학 학·석·박사
- 한국연구재단(NRF) RB

HW

하드웨어 보안 IP 설계

- **삼성전자 전략산학** 초고성능 하이브리드 PQC Security IP · 시스템 아키텍처 ('25-'30, 연구책임자)
- **삼성전자 시스템LSI** NIST PQC 서명 연산 HW 가속기 / 부호기반 암호 Accelerator ('24-'26)
- **前 삼성전자 반도체** 스마트카드용 보안 하드웨어 IP 개발 ('07-'10)

PQC

양자내성암호 — 표준 제안 및 국가 전환 총괄

- **NIST PQC 공모전** 알고리즘 제출자 — pqsigRM (서명) · McNie (암호)
- **범국가 PQC 전환** PQC-QKD 결합 도메인 간 양자보안 시스템 ('26-'29, 총괄책임자)
- **범국가 PQC 전환** DevOps 기반 PQC 전환 자동화·오픈플랫폼 ('26-'29, 기관책임자)

검증

암호 안전성 검증

- **IITP 총괄** 양자내성암호 전환기술 · 대양자 복합 안전성 검증 ('24-'27) — **90억 / 4년**
- **IITP 총괄** 자율주행 V2X 무선통신 인프라 보안 ('24-'26) — **41.25억 / 3년**
- **IITP 총괄 · 국보연** 저사양 디바이스 PQC 안전성·성능 검증 ('21-'24) / 잡음원 엔트로피 테스트



POSTQUANTUM
SHIELD

Make it more
Secure

Appendix

Exit 사례

최근 2년, 계측 장비와 반도체 EDA의 거인이 각각 부채널 회사를 인수했다.

Riscure

네덜란드 · 델프트

Secure-IC

프랑스 · 렌

설립

2001년 · 업력 23년

2010년 · 업력 15년

사업

독립 보안 시험소 — 부채널 · 오류주입 테스트

임베디드 보안 IP + 부채널 평가 솔루션

규모

약 150~175명 (외부 집계)

140명+ · 8개국 거점

인수 시점

2024. 2

2025. 10 완료

인수자

Keysight (계측 장비)

Cadence (반도체 EDA)

인수 금액

\$78M

약 1,000억 원

\$139.6M

약 2,000억 원



POSTQUANTUM
SHIELD

Appendix

국가 PQC 전환 마스터 플랜

		2025	2026	2027	2028	2029	2030	2031-2035
전략 1	과제 1 기술 확보	가. 한국형 양자내성암호 활용기반 확보 및 실용화 여건 조성						
		(과제1-가-①) 암호 알고리즘 활용 방안 정립 및 신뢰성 강화						
		(과제1-가-②) 암호 알고리즘 실용화 및 암호 이용 활성화						
		나. 안전성 검증 및 암호체계 전환 대비 원천·응용기술 확보						
		(과제1-나-①) 양자내성암호 적용 암호모듈 시험·검증 기술 개발						
	과제 2 제도 정비	가. 양자 후 암호기술 사용기준 마련 및 가이드·안내서 개발·보급						
		(과제2-가-①) 보안강도 재정립 및 PQC의 단계적 적용 방법론 도출						
		(과제2-가-②) 암호 사용기준·안내서 시리즈 개발·정비 및 보급						
		나. 암호모듈 검증제도(KCMVP) 양자내성암호 도입 기반 마련·시행						
		(과제2-나-①) 암호모듈 검증제도 적용 체계 구축						
	과제 3 절차정립	가. 암호체계 전환 이행·관리체계 수립						
		(과제3-가-①) 종합 추진계획 현행화 및 정기 개편						
		(과제3-가-②) 외국가 암호체계 전환 추진 체계 정립 및 조직운영						
		나. 기관·분야 맞춤형 「전환 준비」 계획 수립 토대 마련						
		(과제3-나-①) 암호자산 식별기준 및 준비사항 정립						
전략 2	과제 4 PKI 고도화	가. 민간·행정·국방·금융·교육 등 수부문 PKI 전환 얼라이언스 구축						
		(과제4-가-①) 외부처 통합 대응·협력 체계 구축·운영						
		나. PKI 운용기준 및 실용기술 개발 등 기술·정책적 기반 마련						
		(과제4-나-①) (1단계) PKI 특화기술·정책 연구						
		(과제4-나-②) (2단계) 이용기준 마련 및 PQC 기반 PKI 실용기술 확보						
	과제 5 전환지원	다. 단계적 운용 안정성 확보						
		(과제4-다-①) (1단계) PKI 암호체계 보안강도 상황						
		(과제4-다-②) (2단계) 실증 및 단계적 전환을 통한 안정적 PKI 구축						
		가. 「전환 시행」 가이드라인 개발 등 전환지원 체계 마련						
		(과제5-가-①) 암호체계 전환 실증 및 취약점·미비점 보완체계 마련						
	과제 6 인적/산업 기반구축	(과제5-가-②) 전환 실무가이드 및 인증제도 개발 등 전환 유도·가속화						
		나. 양자내성암호 전환 통합 지원 서비스 구축·운영						
		(과제5-나-①) 암호체계 전환 지원 인프라 구축·지원						
		(과제5-나-②) 원소통 지원 서비스 운영						
		가. 양자내성암호 및 암호전환 분야 인재 육성						
		(과제6-가-①) 원천기술 연구 활성화·교육 및 기술 공유·전수 행사 확대						
		나. 기업 육성·지원 등 산업기반 공고화						
		(과제6-나-①) 전문 컨설팅 기업 양성 및 지원						
		(과제6-나-②) 관련 신기술 특성화 및 기업 경쟁력 제고						
		다. 암호전환 필요성 대국민 인식확산 및 기초체력 강화						
		(과제6-다-①) 양자내성암호 체계 전환 인식 제고						
		(과제6-다-②) 핵심 원천기술 학술연구 지원 및 분야 개척 강화						



POSTQUANTUM
SHIELD

양자내성암호, Post-Quantum Cryptography

양자컴퓨팅이 상용화되면, 기존 암호 RSA, DSA, ECDSA는 해독됨
따라서, 양자컴퓨팅에 내성이 있는 양자내성암호를 미리 도입해야함



IBM Q System One

Security against
Quantum Computation

RSA Shor's algorithm
DSA
ECDSA

New Cryptographic Primitives
= Post-Quantum Cryptography (PQC)
= Quantum Safe Cryptography

Lattice Code

Post-Quantum
Cryptography

Hash MQ

Isogeny MPC

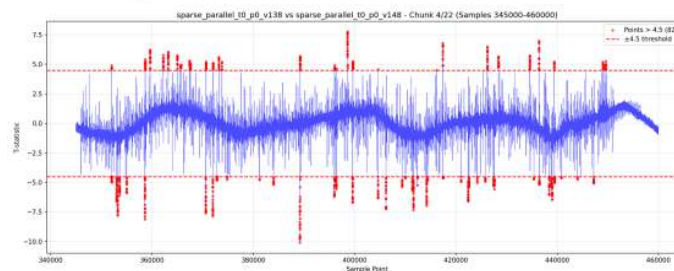
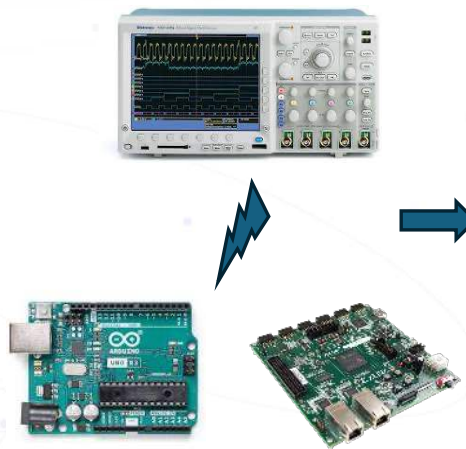
Appendix

하드웨어 해킹 그리고 부채널 분석

암호 알고리즘은 이론적으로 안전함

하지만, 구현 레벨에서는 하드웨어로 부터 관련 정보를 가져오면 비밀키를 해독할 수 있음

Algorithmic security $\neq$ Implementation security




=
0x8F

Appendix

하드웨어 해킹 사례

21년, 테슬라 모델 X 키를 2초만에 해킹하여 문을 여는 연구

IACR Transactions on Cryptographic Hardware and Embedded Systems
ISSN 2569-2925, Vol. 2021, No. 4, pp. 149–172. DOI:10.46586/tches.v2021.i4.149-172

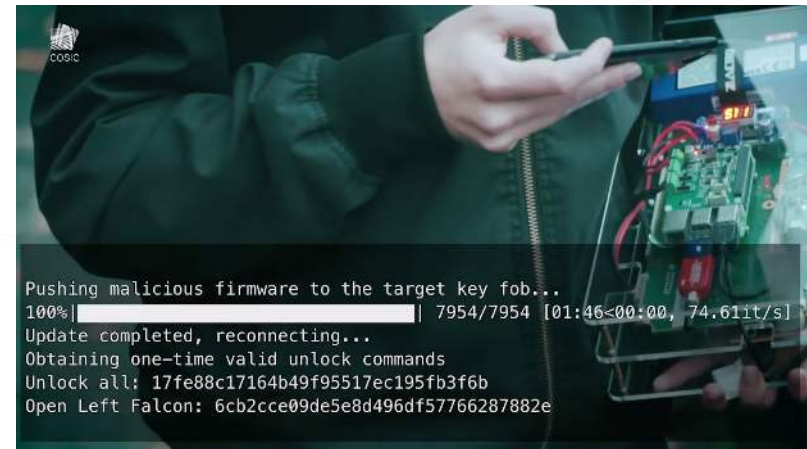
My other car is *your car*: compromising the Tesla Model X keyless entry system

Lennert Wouters, Benedikt Gierlichs and Bart Preneel

imec-COSIC, KU Leuven, Kasteelpark Arenberg 10, B-3001 Leuven-Heverlee, Belgium
firstname.lastname@esat.kuleuven.be



POSTQUANTUM
SHIELD



Appendix

하드웨어 해킹 사례



꾸준히 나오는 PQC 부채널 분석 논문들, 작년 TCHES25에서 6개 발표

9. OT-PCA: New Key-Recovery Plaintext-Checking Oracle Based Side-Channel Attacks on HQC with Offline Templates

Haiyue Dong, Qian Guo

Independent Researcher; Lund University

TCHES

PDF

4. Leaky McEliece: Secret Key Recovery From Highly Erroneous Side-Channel Information

Marcus Brinkmann, Chitchanok Chuengsatiansup, Alexander May, Julian Nowakowski, Yuval Yarom

Ruhr University Bochum; University of Klagenfurt

TCHES

PDF

8. Multi-Value Plaintext-Checking and Full-Decryption Oracle-Based Attacks on HQC from Offline Templates

Haiyue Dong, Qian Guo

Lund University

TCHES

PDF

2. MulLeak: Exploiting Multiply Instruction Leakage to Attack the Stack-optimized Kyber Implementation on Cortex-M4

Fan Huang, Xiaolin Duan, Chengcong Hu, Mengce Zheng, Honggang Hu

University of Science and Technology of China; Zhejiang Wanli University

TCHES

PDF

13. Full Key-Recovery Cubic-Time Template Attack on Classic McEliece Decapsulation

Vlad-Florin Drăgoi, Brice Colombier, Nicolas Vallet, Pierre-Louis Cayrel, Vincent Grosso

Aurel Vlaicu University of Arad; Université Jean Monnet Saint-Etienne; Centre National de la Recherche Scientifique

TCHES

PDF

27. Rejected Signatures' Challenges Pose New Challenges: Key Recovery of CRYSTALS-Dilithium via Side-Channel Attacks

Yuanyuan Zhou, Weijia Wang, Yiteng Sun, Yu Yu

Synopsys; Shandong University; Shanghai Jiao Tong University

TCHES

PDF

하드웨어 해킹 사례

Downfall (2023) — Intel Core 6~11세대 (Skylake~Tiger Lake), CVE-2022-40982
gather 명령이 투기적 실행 중 SIMD 벡터 레지스터(AVX)에 남은 값을 흘린다
OpenSSL AES 키 복구 — AES-128 100%, AES-256 86%

Downfall (security vulnerability)

[Add languages](#)[Article](#) [Talk](#)[Read](#) [Edit](#) [View history](#)

From Wikipedia, the free encyclopedia

See also: [Transient execution CPU vulnerability](#)

Downfall, known as **Gather Data Sampling (GDS)** by Intel,^[1] is a [computer security vulnerability](#) found in 6th through 11th generations of consumer and 1st through 4th generations of Intel [Xeon Scalable x86-64](#) microprocessors.^[2] It is a [transient execution CPU vulnerability](#) which relies on [speculative execution](#) of [Advanced Vector Extensions](#) (AVX) instructions to reveal the content of [vector registers](#).^{[3][4]}

Vulnerability [\[edit \]](#)

Intel's [Software Guard Extensions](#) (SGX) security subsystem is also affected by this bug.^[4]

The Downfall vulnerability was discovered by the security researcher [Daniel Moghimi](#), who publicly released information about the vulnerability in August 2023, after a year-long embargo period.^{[5][6]}

Downfall

CVE identifier	CVE-2022-40982
Affected hardware	6-11th gen Intel Core CPUs, 1-4th gen Intel Xeon Scalable CPUs
Website	downfall.page

Appendix

하드웨어 해킹 사례

21년 구글 타이탄키 (하드웨어 키)를 EM공격 방식으로 키 탈취

IDENTITY & ACCESS

Researchers Show Google's Titan Security Keys Can Be Cloned

Researchers have found a way to clone [Google's Titan Security Keys](#) through a side-channel attack, but conducting an attack requires physical access to a device for several hours, as well as technical skills, custom software, and relatively expensive equipment.



By [Eduard Kovacs](#) | January 11, 2021 (12:33 PM ET)



POSTQUANTUM
SHIELD



KCMVP, CC



KCMVP

암호모듈 검증 (한국)

ISO/IEC 19790 암호모듈 보안 요구사항 — 등급 L1~L4

ISO/IEC 24759 위 요구사항의 시험 방법

§7.8 비침습 보안 부채널 대응을 별도 항목으로 규정 (옵션)

CC

정보보호제품 평가 (한국)

ISO/IEC 15408 평가 기준 (보증등급 EAL)

ISO/IEC 18045 평가 방법 — 취약점 분석 AVA_VAN

AVA_VAN.5 High 공격자 대응 = 부채널 침투시험

원문이 말하는 것 — 부채널은 '옵션이지만, 고등급에선 실측 시험'이다

ISO 19790 §7.8: “vendor가 비침습 대응을 주장하지 않으면 적용 안 됨” — 즉 선택 항목. 단, L1~L2 = 문서 심사, L3~L4 = 실제 시험 (Annex F → **ISO/IEC 17825**, TVLA 기반).

ISO 18045 AVA_VAN.5: “High 공격 잠재력을 가진 공격자가 악용 가능한 취약점 판정” — 부채널이 여기 포함. EAL5 이하는 기본 미포함, 상향(augmentation) 필요.

같은 ISO 표준 위에서 각국이 운영한다

한국

KCMVP · CC

ISO 19790/24759 · 15408/18045

미국 · 캐나다

CMVP (FIPS 140-3)

FIPS 140-3 = ISO 19790 채택

일본

JCMVP

ISO 19790 기반 (IPA 운영)

유럽

SOG-IS · EUCC

ISO 15408/18045 (CC)

국제

CCRA 상호인정

CC 인증 국가 간 상호 인정

Appendix

고객 군 정의

우리 고객 — 보안 모듈 개발 업체

광범위한 타깃 대신, 수요가 절박하고 마진이 높은 순으로 좁힌다

Tier 1

공공 · 국방 · 방산 벤더

국가 정보보안 제품 제조사 · 방산 업체 — KCMVP 상위 등급 검증이 필수

국보연이 하던 부채널 검증이 민간으로 넘어온다.

KCMVP가 PQC로 확대되며 알고리즘 종류·수요가 폭증 — 국보연 단독 감당 불가

Tier 2

암호 원천기술 · IP 기업

PQC 알고리즘을 칩·모듈로 구현해 라이선스 사업을 하려는 기업

KpqC HAETAE · SMAUG-T 등

NIST PQC ML-KEM · ML-DSA · HQC 등



POSTQUANTUM
SHIELD



드림시큐리티

HANCOM

한컴위드

AhnLab

SECUI

한국 전자인증

KSIGN (주) 케이사인

삼성 시스템LSI
Samsung System LSI

SMAUG-T & HAETAE