PQC 부채널대응 성능 분석

송민호

유튜브: https://youtu.be/5Ywg1Uyfssw

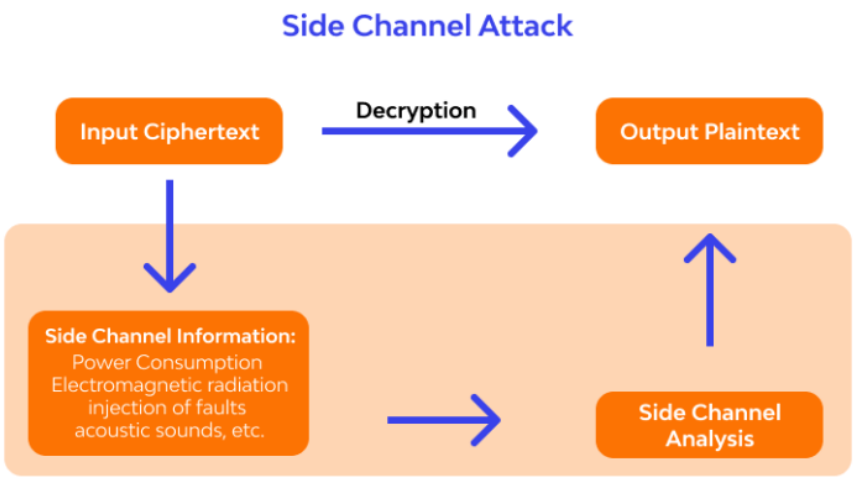
한성대학교 HANSUNG UNIVERSITY

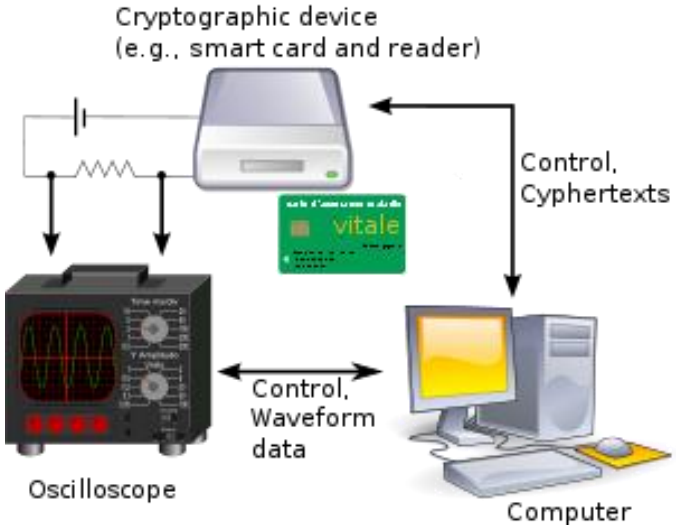
CryptoCraft LAB

부채널 공격

- **물리적으로 발생하는 정보를 이용하여 암호키를 탈취하는 공격**
  - 암호화 알고리즘의 취약점을 노리는 것이 아닌 구현된 환경의 취약점을 노림
  - **전력**, **전자파**, **연산 시간** 등을 이용하여 공격 가능

- **주요 공격 기법**
  - **Timing Attack**: 연산 동작 중 걸리는 시간을 토대로 암호를 유추
  - **Power Analysis**: 연산 이후, 장비의 매순간의 전력 사용량의 변화를 이용하여 분석
  - **Fault Analysis**: 오류 주입을 통해 비정상 동작을 유발하여 나온 연산 값을 정상 동작한 연산 값과 비교





부채널 공격

- **암호화 알고리즘들에 대해 유효한 부채널 공격 방법이 계속 연구 중**
  - 기존의 암호들은 부채널 공격으로부터 완전히 안전하지 않음

- **부채널 공격을 이용한 공격 사례가 존재**
  - 시차분석 공격(Portsmash)을 통해 인텔 마이크로프로세서에서 암호화된 데이터를 빼냄
  - 신용카드의 IC 칩의 전기 소모량을 분석해 새 IC 칩에 적용하여 PIN코드 우회
    - PQC 적용시 문제 발생 가능성 있음

부채널 공격에 저항할 수 있는 방안이 필요


ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

POLICY —

How a criminal ring defeated the secure chip-and-PIN credit cards

Over $680,000 stolen via a clever man-in-the-middle attack.

Using that information, the police were able to arrest a 25-year-old woman carrying a large number of cigarette packs and scratchers, which were apparently intended for resale on the black market. After her arrest, four more members of the fraud ring were identified and arrested. That number included the engineer who was able to put together the chip card hacking scheme that a group of French researchers call "the most sophisticated smart card fraud encountered to date."

25 stolen cards, specialized equipment, and €5,000 (approximately $5,660) in cash was seized. Ultimately police said about €600,000 (or $680,000) was stolen as a result of the card fraud scheme, spanning 7,000 transactions using 40 cards.


HOME · COMPUTING · NEWS

PortSmash attack exploits Intel's Hyper-Threading architecture to steal your data

By Chuong Nguyen
November 2, 2018

SHARE

Security researchers from Finland and Cuba have discovered a side-channel attack, known as PortSmash, that affects Intel chips and could allow attackers access to encrypted data processed from a computer's CPU. The vulnerability exists on chipsets that use simultaneous multithreading (SMT) architecture, so it could also affect AMD chips in addition to Intel chips with Hyper-Threading technology.

Kumar, Satyam, et al. "Side channel attack on stream ciphers: A three-step approach to state/key recovery." *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2022.2 (2022): 166-191

부채널 공격 대응기법

- **알고리즘의 연산 과정을 수정하여 물리적으로 발생하는 정보를 얻지 못하게 하는 것**

- **다양한 대응기법**
  - **무작위성**
    소비전력, 실행시간 등의 부채널 정보를 무작위로 생성하여 데이터 분석에 방해를 주는 방법
  - **블라인딩**
    연산 실행 전에 임의의 값을 암호화 데이터에 추가하여 원래의 데이터를 가리는 방법
  - **마스킹**
    연산에 쓰이는 정보를 임의의 값(마스크)로 변형하여 민감한 정보를 노출시키지 않는 방법
  - **노이즈**
    연산 과정에 노이즈를 추가, 연산 시간을 고의로 늘려 정확한 시간 측정에 혼란을 주는 방법
  - **Constant-time**
    암호화 연산이 입력 값에 따라 실행 시간이 달라지지 않도록 설계하는 방법

부채널 공격 대응기법 – PQC

- **Post-Quantuam Cryptograpy(PQC)도 부채널 대응기법이 필요**
  - 2023년 A.C.Canto가 제시한 논문에서 PQC는 기존의 고전 컴퓨터와 양자 컴퓨터의 공격으로부터 안전하지만 **부채널 공격에는 취약**

Algorithmic Security is Insufficient: A Comprehensive Survey on Implementation Attacks Haunting Post-Quantum Security

This survey is on forward-looking, emerging security concerns in post-quantum era, i.e., the implementation attacks for 2022 winners of NIST post-quantum cryptography (PQC) competition and thus the visions, insights, and discussions can be used as a step forward towards scrutinizing the new standards for applications ranging from Metaverse/Web 3.0 to deeply-embedded systems. The rapid advances in quantum computing have brought immense opportunities for scientific discovery and technological progress; however, it poses a major risk to today's security since advanced quantum computers are believed to break all traditional public-key cryptographic algorithms. This has led to active research on PQC algorithms that are believed to be secure against classical and powerful quantum computers. However, algorithmic security is unfortunately insufficient, and many cryptographic algorithms are vulnerable to side-channel attacks (SCA)

Canto, Alvaro Cintas, et al. "Algorithmic Security is Insufficient: A Comprehensive Survey on Implementation Attacks Haunting Post-Quantum Security." *arXiv preprint arXiv:2305.13544* (2023).

부채널 대응 기법 연구 현황 – Lattice

- **Lattice-based PQC**

유형	알고리즘	환경	논문	발표 년도
KEM	Kyber	FPGA	A masked pure-hardware implementation of Kyber cryptographic algorithm	2022
			Error detection architectures for hardware/software co-design approaches of number theoretic transform	2023
			Error detection schemes assessed on FPGA for multipliers in lattice-based key encapsulation mechanisms in post-quantum cryptography	2023
		ARM	High-speed masking for polynomial comparison in lattice-based KEMs	2020
			Masking Kyber: First-and higher-order implementations	2021
			Combined fault and DPA protection for lattice-based cryptography	2022
Signature	Dilithium	FPGA	Fault attack countermeasures for error samplers in lattice-based cryptography	2019
			Breaking and protecting the crystal: Side-channel analysis of Dilithium in hardware	2022
	FALOCN	FPGA	Efficient error detection architectures for post-quantum sig- nature FALCON’s Sampler and KEM Saber	2022
		ARM	The hidden parallelepiped is back again: Power analysis attacks on FALCON	2022
		Intel	BEARZ attack FALCON: implementation attacks with countermeasures on the FALCON signature scheme	2019

부채널 대응 기법 적용 시 성능 – Kyber

- **Power analysis에 관한 대응책**
  - FPGA Xilinx Virtex-7에서 구현
  - **하이딩 및 마스킹을 통해 PA에 저항**
    - 비밀 벡터 계수의 계산에 대한 회피(병렬 처리 및 파이프라인화 사용)
  - **Cycle Counts에 대한 성능**
    - Hiding - only : **8%** 오버헤드 발생
    - Hiding - plus - Masking : **17%** 오버헤드 발생

Implementation	Algorithm	Process	FPGA	Freq (MHz)	LUTs	Slices	DSPs	BRAMs	Div IPs	Cycle Counts
This work (Hiding-only)	Kyber-512	Encaps	Virtex7 VC707	100	153,939	107,804	53	264	0	88,176
		Decaps	Virtex7 VC707	100	143,112	81,746	60	294	0	126,619
This work (Hiding-plus-masking)	Kyber-512	Encaps	Virtex7 VC707	100	163,584	119,324	56	392	0	88,176
		Decaps	Virtex7 VC707	100	152,860	92,977	76	489.5	0	137,738
Huang et al. [3]	Kyber-512	Encaps	Artix7 AC701	155	80,322	141,825	54	200.5	2	49,015
		Decaps	Artix7 AC701	155	88,901	152,875	354	202	3	68,815
Huang et al. [3]	Kyber-768	Encaps	Artix7 AC701	155	97,085	153,867	36	200.5	2	77,481
		Decaps	Artix7 AC701	155	110,260	167,293	292	202	3	102,113
Huang et al. [3]	Kyber-1024	Encaps	Virtex7 VC707	192	119,189	162,636	36	200.5	2	107,054
		Decaps	Virtex7 VC707	192	132,918	172,489	548	202	3	135,553

T. Kamucheka, A. Nelson, D. Andrews, and M. Huang. A masked pure-hardware implementation of Kyber cryptographic algorithm. ICFPT. pp. 1-9, 2022.

부채널 대응 기법 적용 시 성능 – Lattice based

- **Fault attack에 관한 대응책**
  - FPGA Xilinx Artix-7에서 구현
  - Error Samplers에 대한 대응 기법 사용
    - 가우시안 및 이항 분포를 활용하여 Error Sampler가 제대로 작동하는지 확인

  - **하드웨어에서 가장 효율적인 Error Sampler와의 평가**
    - Low Cost
      - 3개의 추가 슬라이스 필요
      - **추가 Clock Cycles 필요 없음**
    - Standard
      - 22개의 추가 슬라이스 필요
      - **1개의 추가 Clock Cycles 필요**
    - Expensive
      - 96~116개의 추가 슬라이스 필요
      - **32개의 추가 Clock Cycles 필요**

Countermeasure Category	LUT/FF	Slices	DSP/ BRAM	Freq. (MHz)	Clock Cycles	Ops/sec ($\times 10^6$)
Plain CDT Sampler	115/81	33	0/0	297	6	49.5
Low Cost	6/10	3	0/0	-	$+0^{\dagger}$	-
CDT with Low Cost	123/91	36	0/0	297	6	49.5
Standard	74/58	24	0/0	-	$+1^{\dagger}$	-
CDT with Standard	182/139	55	0/0	297	6	49.5
Expensive	226/436	126	1/0	-	$+32^{\dagger}$	-
CDT with Expensive	315/517	149	1/0	297	6	49.5
CDT with Expensive	251/453	129	1/1	193	6	38.6

약 8%의 오버헤드 발생

J. Howe, A. Khalid, M. Martinoli, F. Regazzoni, and E. Oswald. Fault attack countermeasures for error samplers in lattice-based cryptography. ISCAS. pp. 1-5, 2019.

부채널 대응 기법 적용 시 성능 – Kyber

- **Fault attack에 관한 대응책**
  - FPGA Xilinx Virtex-7, Spartan-7에서 구현
  - NTT 가속기 아키텍처에 효과적인 재계산 방법
    - 연산에 negating 및 swapping 적용
  - **Architecture, Parameter에 따라 성능이 달라짐**
    - Virtex-7 : 최소 **9.32%**, 최대 **21.78%** 오버헤드 발생
    - Spartan-7 : 최소 **8.46%**, 최대 **15.88%** 오버헤드 발생

Architecture	Zynq UltraScale+ (xczu4eg-fbvb900-1LV-i)				Spartan-7 (xc7s100fgga676-1IL)			
	Area		Delay	Power	Area		Delay	Power
	LUT	FF	(ns)	(W)	LUT	FF	(ns)	(W)
Original (a)	277	235	15.78	1.27	429	398	13.07	1.03
RENO (a)	353	285	17.25	1.53	523	469	14.18	1.19
	(27.44%)	(21.28%)	(9.32%)	(20.47%)	(21.91%)	(17.84%)	(8.46%)	(15.62%)
Original (b)	265	212	19.87	1.13	376	344	17.39	0.96
RENO (b)	303	238	23.77	1.28	424	417	20.15	1.03
	(14.63%)	(12.26%)	(19.66%)	(13.27%)	(12.74%)	(21.22%)	(15.88%)	(7.62%)
Original (c)	389	345	40.31	7.82	318	293	30.12	6.33
RENO (c)	460	399	49.09	9.17	395	336	34.25	7.04
	(18.25%)	(15.65%)	(21.78%)	(17.26%)	(24.21%)	(14.68%)	(13.71%)	(11.22%)

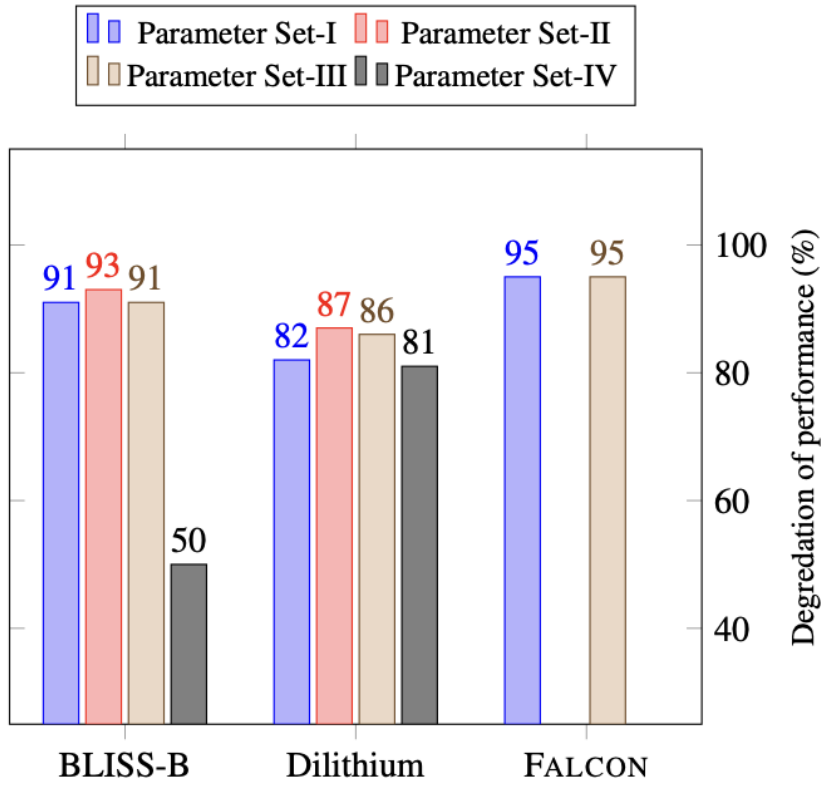
A. Sarker, A. Cintas-Canto, M. Mozaffari-Kermani, and R. Azarderakhsh. Error detection architectures for hardware/software co-design approaches of number theoretic transform. IEEE Transactions on Computer-Aided Design Integrated Circuits Systems, accepted, to appear 2023.

부채널 대응 기법 적용 시 성능 – Dilithium, Falcon

- **Fault attack에 관한 대응책**
  - Intel E5-1620 CPU에서 구현
  - verify-after-sign 구현
    - Verify-after-sign : 서명 후 서명을 확인하는 과정
    - 서명을 두 번 생성하는 것보다 실행시간이 효율적

- **Falcon의 키 생성 과정에서 최대 30%의 오버헤드가 발생하나 전체에 끼치는 영향은 미미함**

- **사용하는 Parameter에 따라 성능 감소율 다름**
  - Falcon 최대 **5%**의 오버헤드 발생
  - Dilithium 최대 **19%**의 오버헤드 발생



S. McCarthy, J. Howe, N. Smyth, S. Brannigan, and M. O'Neill. BEARZ attack FALCON: implementation attacks with countermeasures on the FALCON signature scheme. Cryptology ePrint Archiv, 2019.

부채널 대응 기법 적용 시 성능 – Falcon

- **Fault attack에 관한 대응책**
  - FPGA Xilinx ZYNQ에서 구현
  - Falcon은 Gaussian 샘플러 사용으로 Fault attack에 취약
  - 효율적인 오류 감지 방식 제안
    - Falcon 샘플러에 대한 재계산을 통해 에러 탐지

- **Architecture에 따라 성능이 달라짐**
  - Area 측면에서 최대 **22.59%** 오버헤드
  - Delay 측면에서 최대 **19.77%** 오버헤드
  - Power 측면에서 최대 **10.67%** 오버헤드

Architecture	Scheme	Area		Delay (ns)	Power (mW)
		LUTs	FFs		
Binomial sampling	Original	85	88	2.03	0.697
	RESwO	100 (17.64%)	105 (19.32%)	2.35 (15.76%)	0.745 (6.88%)
Polynomial multiplication	Original	17,352	5,171	2.959	1.724
	RENO	20,420 (17.68%)	6,346 (22.72%)	3.297 (11.42%)	1.908 (10.67%)
Hardware/software codesign	Original	14,277	1,025	3.764	2.097
	RENO	17,502 (22.59%)	1,206 (17.66%)	4.508 (19.77%)	2.295 (9.45%)

A. Sarker, M. Mozaffari-Kermani, and R. Azarderakhsh. Efficient error detection architectures for post-quantum sig- nature FALCON's Sampler and KEM Saber. IEEE Trans. VLSI Systems, vol. 30, no. 6, pp. 794-802, 2022.

부채널 대응 기법 적용 시 성능 정리

- **Lattice based PQC에 대응법 적용 시 성능**
  - 어떤 대응법을 적용하냐에 따라 오버헤드 수치가 크게 달라짐

- **Power analysis**
  - Kyber의 경우 **최소 8%, 최대 17%**의 오버헤드가 발생함

- **Fault attack 대응책**
  - Kyber의 경우 **최소 8%, 최대 21.78%**의 오버헤드가 발생함
  - Dilithium의 경우 **최소 8%, 최대 19%**의 오버헤드가 발생함
  - Falcon의 경우 **최소 5%, 최대 19.77%**의 오버헤드가 발생함

평균적으로 약 5% ~ 20%의 오버헤드 발생

부채널 대응 기법 연구 현황 – Hash

- **Hash-based PQC**
  - NIST PQC 공모전에서 선정된 해시 기반 스킴은 SPHINCS가 유일

유형	알고리즘	환경	논문	발표 년도
Signature	SPHINCS	ASIC	Reliable hash trees for post-quantum stateless cryptographic hash-based signatures	2015
			Fault detection architectures for post-quantum cryptographic stateless hash-based secure signatures benchmarked on ASIC	2016
		-	On protecting SPHINCS+ against fault attacks	2023

부채널 대응 기법 적용 시 성능 – SPHINCS

- Fault attack에 관한 대응책
  - ASIC에서 구현
  - fault detection 구현
    - 신뢰할 수 있는 해시 트리로 인한 오류 감지
    - SPHINCS 내부에서 사용하는 암호인 ChaCha에 대해 암호화된 피연산자(REEO)를 사용하여 재계산

  - Area 측면에서 최대 **15.5%**의 오버헤드 발생
  - Performance 측면에서 최소 **10.4%**, 최대 **14.6%**의 오버헤드 발생

Table IV. Area Overhead and Performance Degradations of the Proposed Schemes for ChaCha

Structure	Area (μm^2) (KGE)	Overhead	Frequency (MHz)	Throughput (Gbps)	Degradation
Original	79,772 (56.5)	—	307	9.6	—
Complementary	106,191 (75.3)	33.1%	538	8.2	14.5%
REEO[1]	87,012 (61.7)	**9.1%**	551	**8.6**	**10.4%**
REEO[2]	92,190 (65.3)	15.5%	**789**	8.2	14.6%

1 and 2: One- and two-stage sub-pipelined architectures.

M.Mozaffari-Kermani, R.Azarderakhsh, and A.Aghaie. Fault detection architectures for post-quantum cryptographic stateless hash-based secure signatures benchmarked on ASIC. ACM Transactions on Embedded Computing Systems, vol. 16, no. 2, pp. 59:1-19, 2016.

부채널 대응 기법 연구 현황 - Code

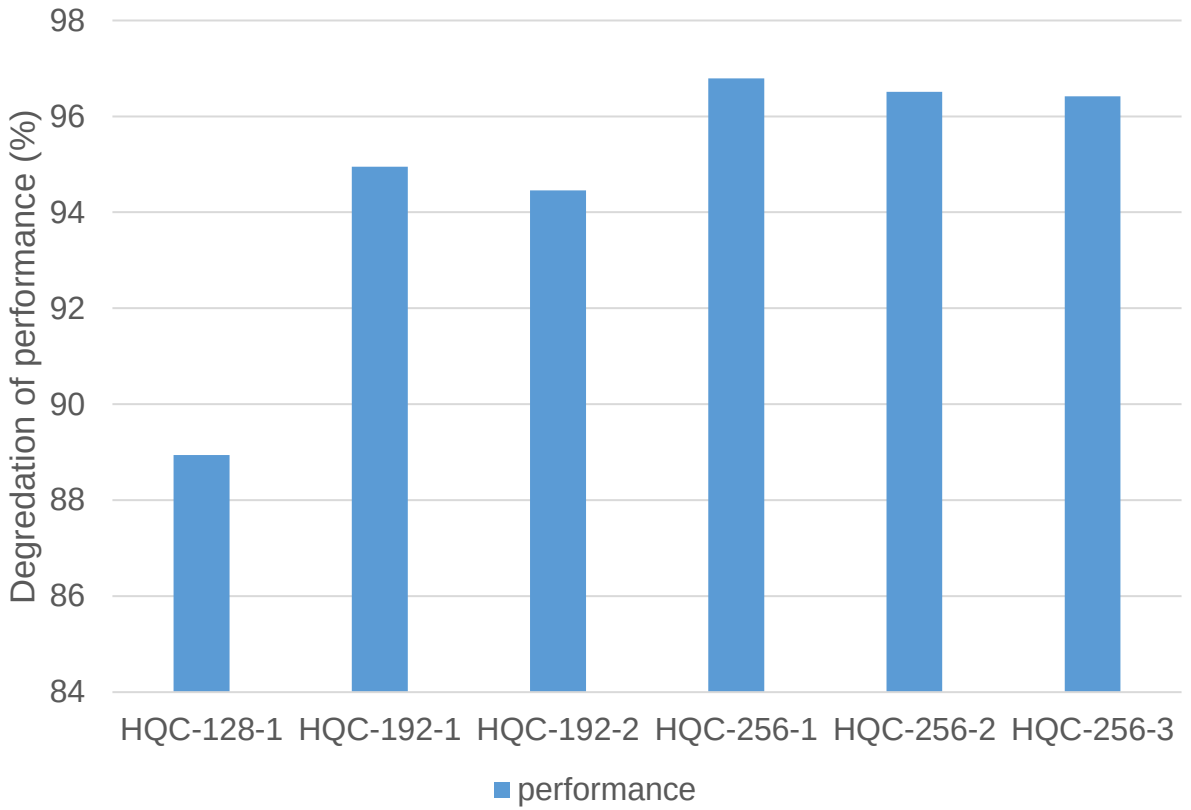
- **Code-based PQC**

유형	알고리즘	논문	발표 년도
KEM	McEliece	Reliable CRC-based error detection constructions for finite field multipliers with applications in cryptography	2021
		CRC-based error detection constructions for FLT and ITA finite field inversions over $GF\ (2^m)$	2021
		Reliable architectures for finite field multipliers using cyclic codes on FPGA utilized in classic and post-quantum cryptography	2023
		Reliable constructions for the key generator of code- based post-quantum cryptosystems on FPGA	2023
	BIKE	Secure sampling of constant-weight words–application to bike	2021
	HQC	A PRACTICABLE TIMING ATTACK AGAINST HQC AND ITS COUNTERMEASURE	2019
		A new key recovery side-channel attack on HQC with chosen ciphertext	2022

부채널 대응 기법 적용 시 성능 – HQC

- **Timing attack에 관한 대응책**
  - Intel core i7-7820X CPU에서 구현
  - constant-time 구현
    - BCH 디코딩에 대한 상수 시간 구현
  - HQC-128: **11.06%** 오버헤드 발생
  - HQC-192: 최대 **5.54%** 오버헤드 발생
  - HQC-256: 최대 **3.58%** 오버헤드 발생

	HQC.Decaps		Overhead
	Original BCH	Constant time BCH	
HQC-128-1	507285	563414	11.06%
HQC-192-1	947552	995272	5.05%
HQC-192-2	992057	1047054	5.54%
HQC-256-1	1490993	1538824	3.21%
HQC-256-2	1562207	1616673	3.49%
HQC-256-3	1617269	1675195	3.58%



Wafo-Tapa, G., Bettaieb, S., Bidoux, L., Gaborit, P., Marcatel, E.: A practicable timing attack against HQC and its countermeasure. Cryptology ePrint Archive, Report 2019/909 (2019)

부채널 대응 기법 적용 시 성능 – BIKE

- **Timing attack에 관한 대응책**
  - Intel arria10 FPGA에서 구현
  - Constant-time 구현
    - 상수 시간 디코더 구현
    - 계산을 파이프라인화하고 병렬화함
    - 다른 디코더에 비해 추가적인 1라운드 필요
    - h bits = 9801일 경우 약 200,000 Cycles 필요
    - 약 **12%** 오버헤드 발생

Table 1: Comparison to the literature

Author	SL	h bits	Platform	Cycles	LUTs	Clock speed	Cost/key^2
This work	128	65498	Arria 10	1,300,000	51,207	110MHz	15.54
Hu et. al.	64	19714	Virtex 6	99,396 avg	32,646	250MHz	8.35
Hu et. al.	40	9602	Virtex 6	35,539 avg	15,322	310 MHz	5.90

Reinders, Andrew H., et al. "Efficient BIKE hardware design with constant-time decoder." *2020 IEEE International Conference on Quantum Computing and Engineering (QCE)*. IEEE, 2020.

부채널 대응 기법 적용 시 성능 – Code based

- **Fault attack에 관한 대응책**
  - FPGA Kintex-7에서 구현
  - fault detection 구현
    - 순환 중복 검사(cyclic redundancy checks, CRC)를 통한 결함 탐지
- **McEliece에 적용한 실험 평가**
  - Horner block – **5.43%**의 오버헤드 발생
    이외에 20.03%의 Area overhead, 9.72%의 Power overhead
  - Inversion block – **7.99%**의 오버헤드 발생
    - 이외에 48.91%의 Area overhead, 11.88%의 Power overhead

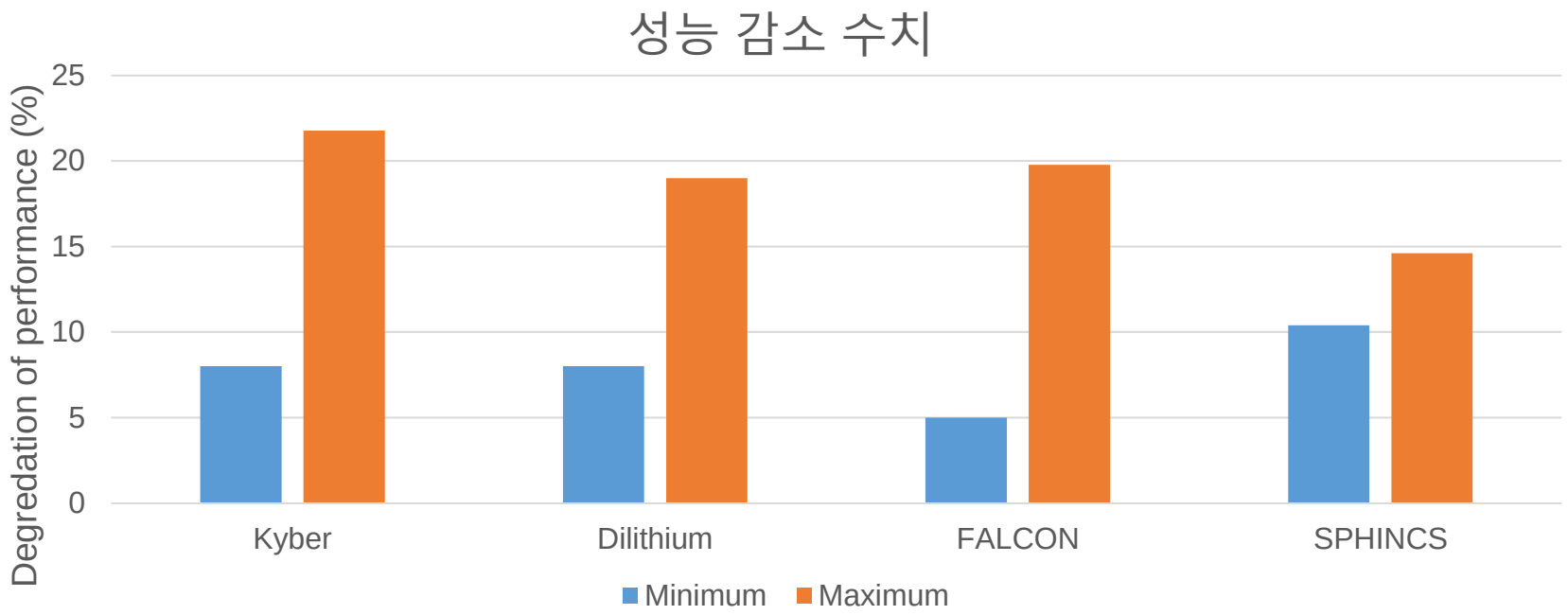
Architecture	Area (occupied slices)	Delay (ns)	Power (mW) @50 MHz	Throughput (Gbps)	Efficiency (Gbps/slices)
Original Horner block	2,976	28.267	0.144	0.460	1.54×10^{-4}
Horner Reg. Parity (predicted/actual/compressor)	3,138 (5.44%)	28.541 (Neg. over.)	0.147 (Neg. over.)	0.455 (Neg. over.)	1.45×10^{-4} (5.84%)
Horner Inter. Parity (predicted/actual/compressor)	3,402 (14.31%)	29.410 (Neg. over.)	0.157 (9.03%)	0.442 (Neg. over.)	1.30×10^{-4} (15.58%)
Horner CRC-2 (predicted/actual/compressor)	3,285 (10.38%)	28.850 (Neg. over.)	0.154 (6.94%)	0.451 (Neg. over.)	1.37×10^{-4} (11.04%)
Horner CRC-8 (predicted/actual/compressor)	3,572 (20.03%)	29.803 (5.43%)	0.158 (9.72%)	0.446 (Neg. over.)	1.25×10^{-4} (18.83%)
Original Inversion block	783	28.820	0.101	0.451	5.76×10^{-4}
Inversion Reg. Parity (predicted/actual/compressor)	976 (24.65%)	29.013 (Neg. over.)	0.108 (6.93%)	0.448 (Neg. over.)	4.59×10^{-4} (20.31%)
Inversion Inter. Parity (predicted/actual/compressor)	1,083 (38.31%)	28.995 (Neg. over.)	0.110 (8.91%)	0.448 (Neg. over.)	4.14×10^{-4} (28.12%)
Inversion CRC-2 (predicted/actual/compressor)	1,121 (43.17%)	28.720 (Neg. over.)	0.112 (10.89%)	0.453 (Neg. over.)	4.04×10^{-4} (29.86%)
Inversion CRC-8 (predicted/actual/compressor)	1,166 (48.91%)	31.124 (7.99%)	0.113 (11.88%)	0.418 (–7.31%)	3.58×10^{-4} (37.84%)

A. Cintas-Canto, M. Mozaffari-Kermani, and R. Azarderakhsh. Reliable constructions for the key generator of code- based post-quantum cryptosystems on FPGA. ACM Emerging Technologies in Computing Systems (special issue on CAD for Hardware Security), vol. 29, no. 1, pp. 5:1-5:20, 2023.

NIST PQC 표준안 성능 비교

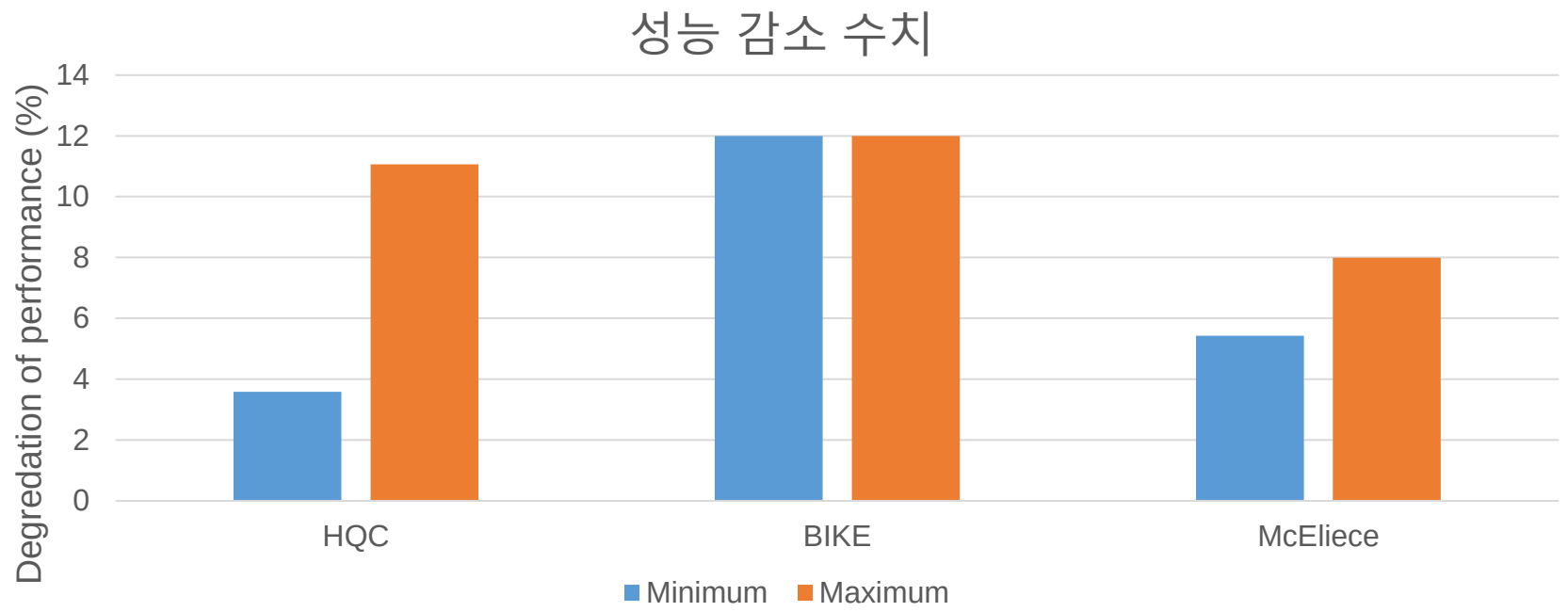
- **오버헤드 최소치 순위**
  - FALCON > Kyber ≥ Dilithium > SPHINCS

- **오버헤드 최대치 순위**
  - SPHINCS > Dilithium > FALCON > Kyber



NIST PQC 4-ROUND 성능 비교

- **오버헤드 최소치 순위**
  - HQC > McEliece > BIKE
- **오버헤드 최대치 순위**
  - McEliece > HQC > BIKE



Q & A