NSR 국가보안기술연구소 National Security Research Institute

SICADA Side Channel Analysis Design Academy

[KpqC 연구단 9차 워크숍]

KpqC 알고리즘 부채널 안전성 분석

2024년 10월 22일 (화)

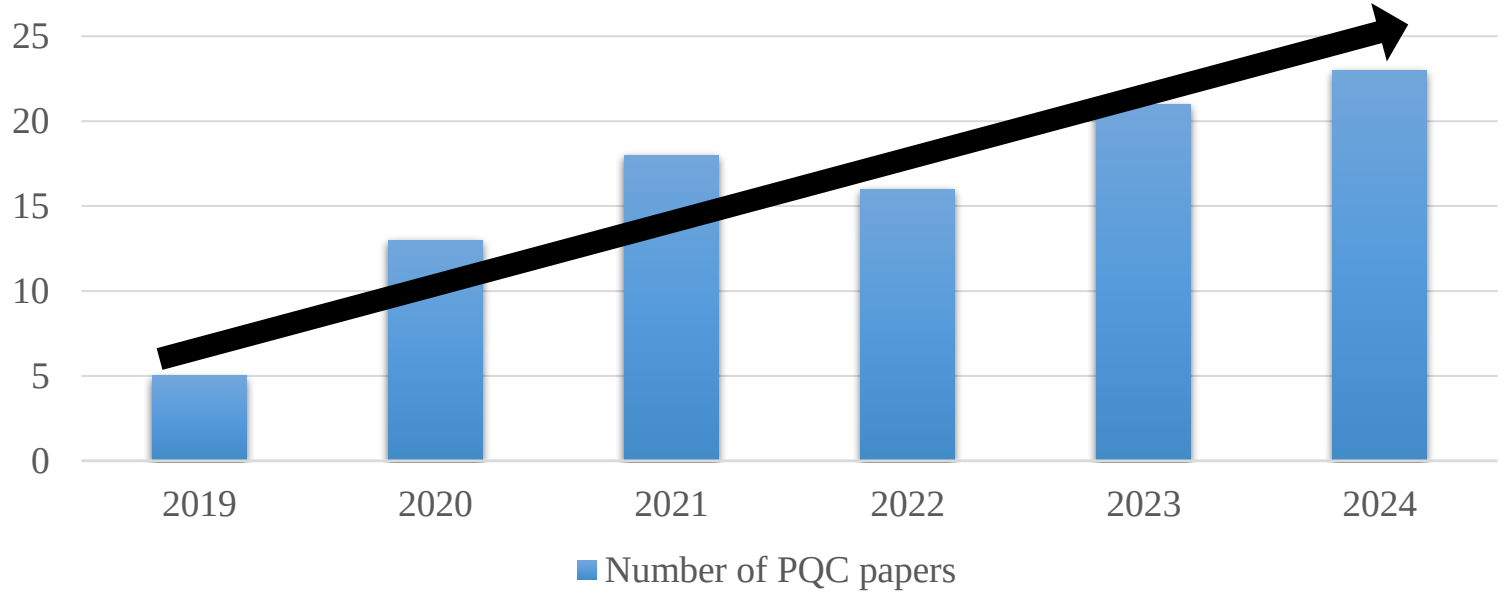
국민대학교 정보보안암호수학과

과제 책임 : 한동국 교수

과제 참여 : 한재승, 조홍래, 유성환 연구원

PQC in Hardware & Embedded Systems

PQC papers in CHES (Cryptographic Hardware and Embedded Systems)



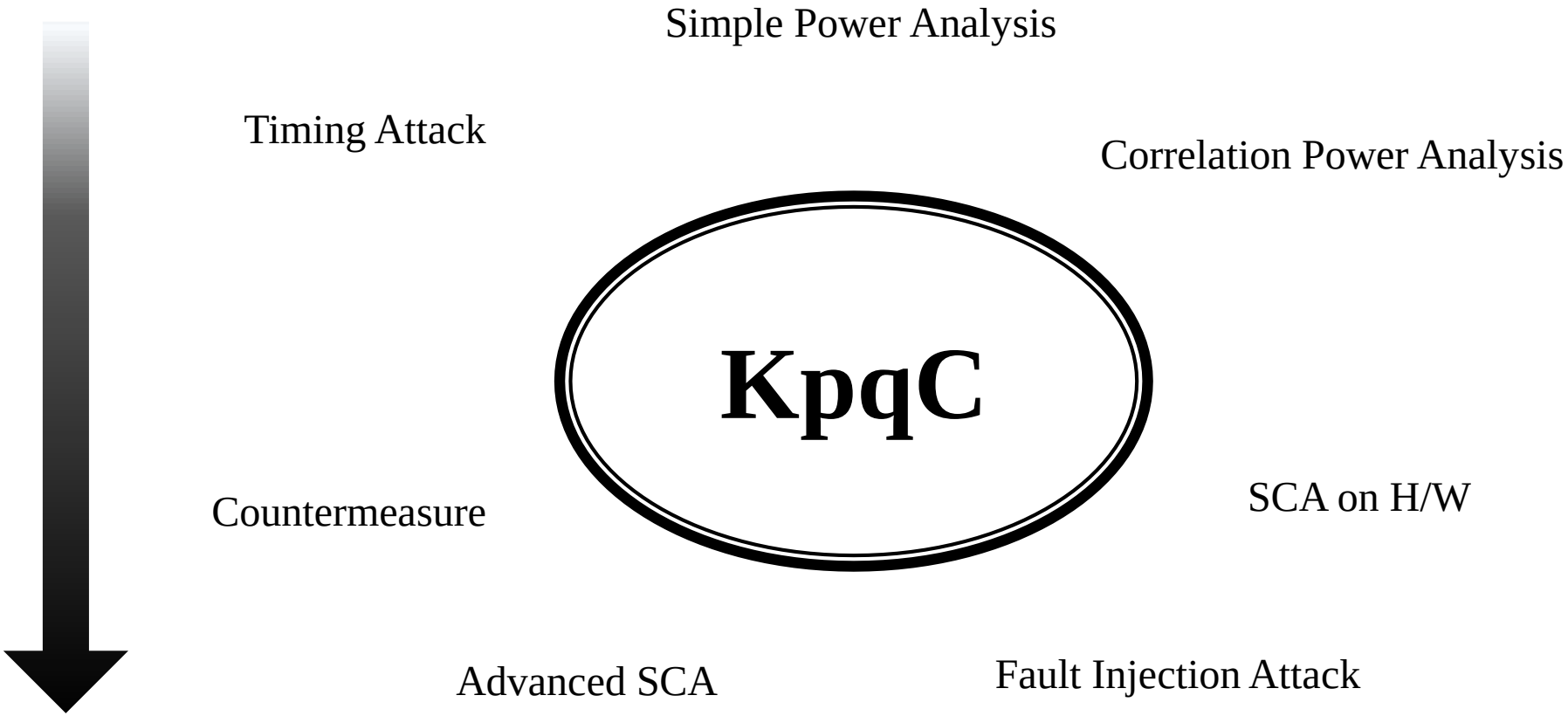
Main Subjects

SCA (Side-Channel Attacks)
S/W implementations

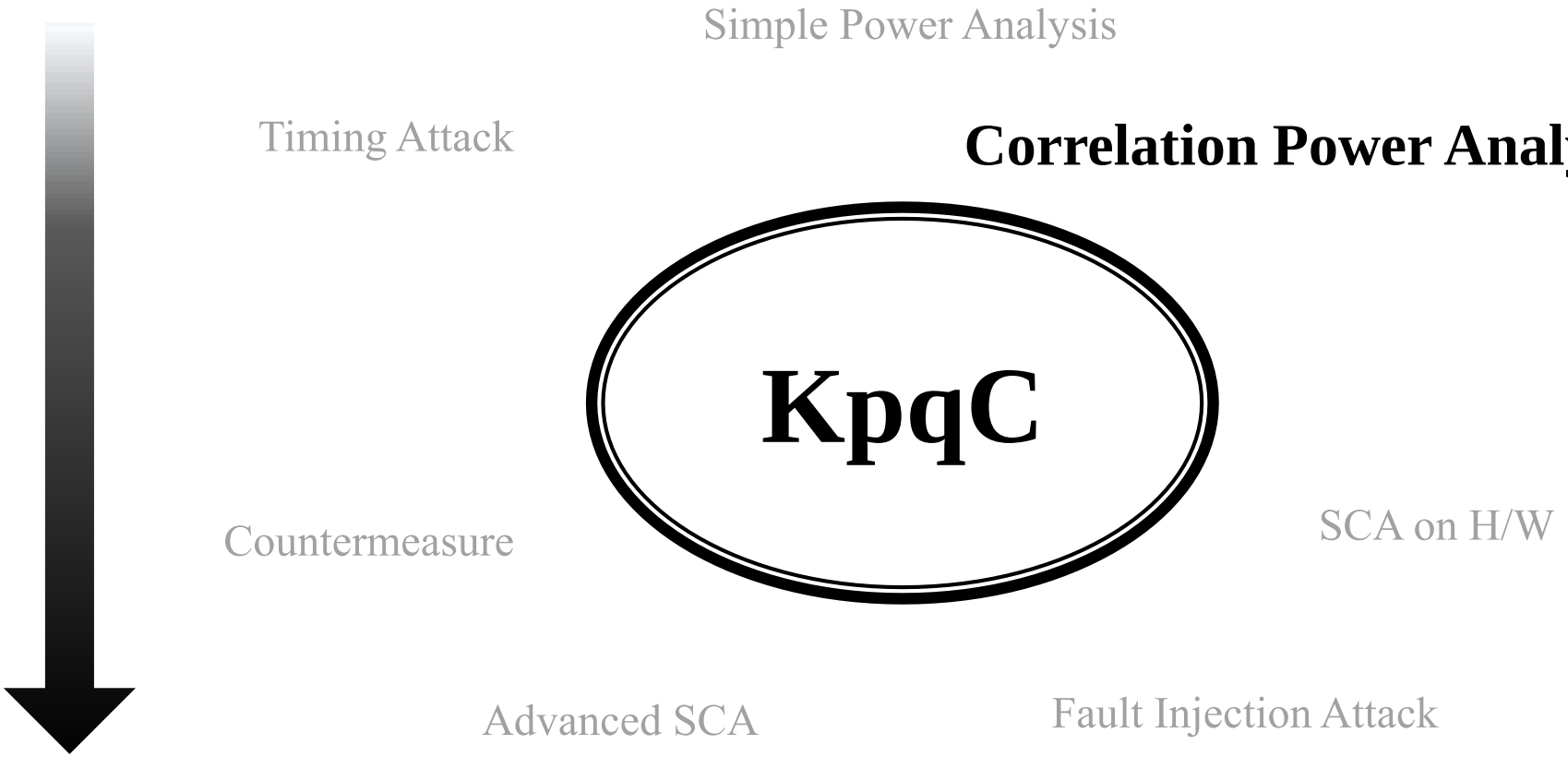
Masking
Advanced SCA
FIA (Fault Injection Attacks)
H/W implementation

in NIST PQC…

SCA on KpqC


Simple Power Analysis
Timing Attack
Correlation Power Analysis
KpqC
Countermeasure
SCA on H/W
Advanced SCA
Fault Injection Attack

SCA on KpqC


Simple Power Analysis
Timing Attack
Correlation Power Analysis!
KpqC
Countermeasure
SCA on H/W
Advanced SCA
Fault Injection Attack

▣ 신규 부채널 분석 결과

❖ 논문 실적 요약

연도	제출처	논문명	비고
2024	CISC-S'24	KpqC 2라운드 전자서명 HAETAE에 대한 상관전력분석	
2024	CISC-S'24	KpqC 2라운드 후보 SMAUG-T의 키종속 연산에 대한 단순전력분석	우수논문상 수상
2024	CISC-S'24	KpqC 2라운드 AIMer에 대한 비밀키 복구 부채널 분석 기법	우수논문상 수상
2024	국가암호공모전	KpqC 2라운드 전자서명에 대한 비밀키 복구 부채널 공격	우수상 수상
2024	JKIISC	SMAUG-T 곱셈 연산에 대한 단순전력분석 공격 및 대응기법	투고

❖ 부채널 분석 결과 요약

KpqC 알고리즘	식별 부채널 분석 대상 연산	부채널 분석 검증 실험
SMAUG-T	Polynomial ×	Simple Power Analysis
NTRU+	Polynomial ×	-
PALOMA	Matrix-vector ×	-
REDOG	Matrix-vector ×	-
HAETAE	Polynomial ×	Correlation Power Analysis
NCC-Sign	Polynomial ×	Correlation Power Analysis
MQ-Sign	Matrix-vector ×	Correlation Power Analysis
AIMer	Galois Field +,×	Correlation Power Analysis

Contents

1 연구 개요

2 국내·외 PQC 알고리즘 부채널 공격 동향

3 KpqC 알고리즘 부채널 분석

3.1 PKE/KEM

3.2 Signature

4 결론

Contents

1 연구 개요

2 국내·외 PQC 알고리즘 부채널 공격 동향

3 KpqC 알고리즘 부채널 분석

3.1 PKE/KEM

3.2 Signature

4 결론

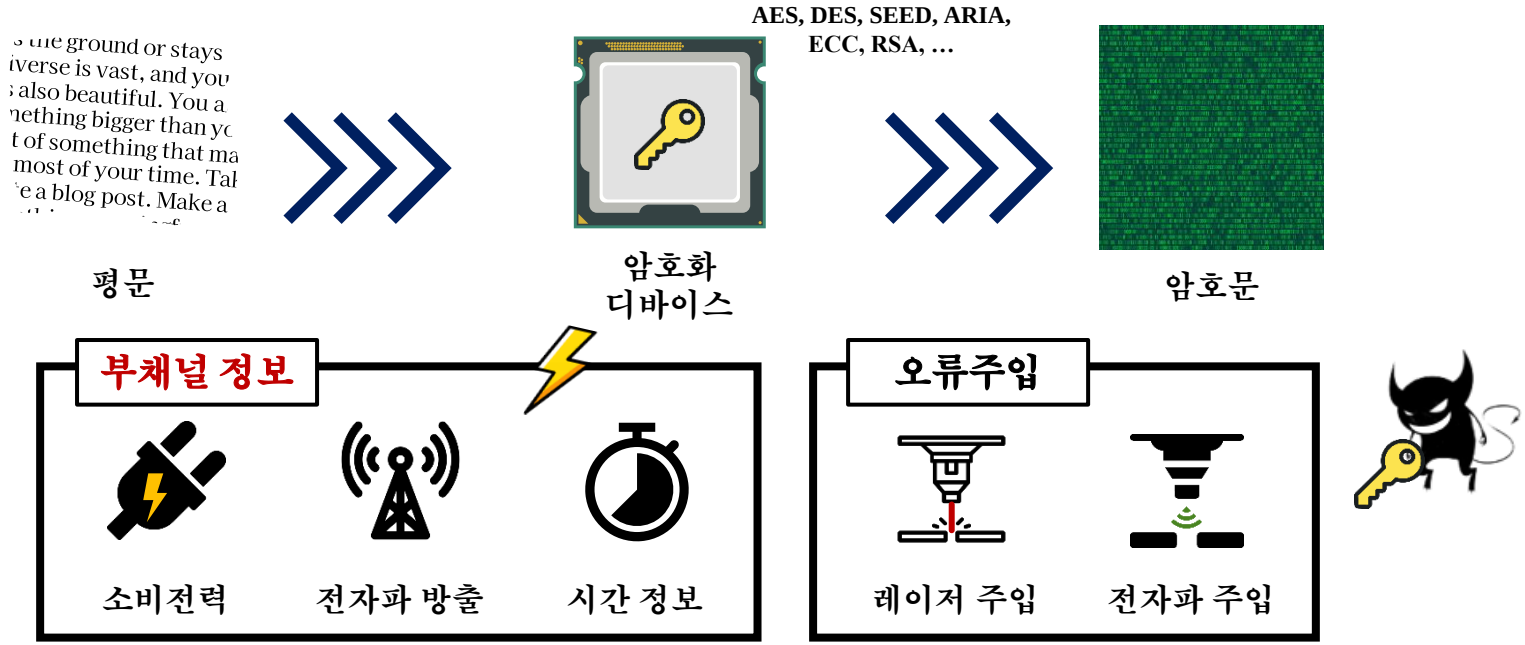
▣ 연구 목표

KpqC 공모전 2라운드 알고리즘 부채널 분석 및 암호전환 안전성 확보방안 연구	
기간	2024.04.01 - 2024.09.30(6개월)
목표	**국내·외 PQC 알고리즘에 대한 부채널 공격 동향 분석** ✓ 격자 기반 알고리즘 부채널 공격 동향 분석 ✓ 코드 기반 알고리즘 부채널 공격 동향 분석 ✓ 다변량 기반 알고리즘 부채널 공격 동향 분석 ✓ 영지식증명 기반 알고리즘 부채널 공격 동향 분석
	KpqC 공모전 2라운드 후보 알고리즘에 대한 부채널 취약성 연구 ✓ KpqC 2라운드 후보 8종 프로파일링 기반 부채널 취약성 연구 ✓ KpqC 2라운드 후보 8종 비프로파일링 기반 부채널 취약성 연구
	국내·외 양자내성암호 전환 동향 분석 ✓ 양자내성암호 표준화 동향 분석 ✓ 양자내성암호 전환을 위한 취약 요소 식별 기술 동향 분석

연구 내용	1	2	3	4	5	6	7	8	9	10	11	12
KpqC 2라운드 후보 알고리즘 구조 분석				→	→	→						
국내외 PQC 부채널 공격 동향 분석					→	→	→					
KpqC 2라운드 후보 부채널 취약성 연구						→	→	→	→			
국내외 양자내성암호 전환 동향 분석						→	→	→				

▣ 부채널 분석 (SCA, Side Channel Analysis)

❖ 암호 알고리즘이 동작할 때 발생하는 **부채널 정보**를 활용하여 비밀 값을 분석하는 방법



전자 주민등록증

전자 여권

전자 공무원증

Smart Car

USIM

금융IC카드

▣ 양자내성암호 부채널 분석 동향

❖ KpqC 2라운드 후보 알고리즘

	알고리즘	기반 문제	유사 NIST PQC 알고리즘
PKE/KEM	SMAUG-T	격자	CRYSTALS-KYBER, SABER
	NTRU+	격자	NTRU
	PALOMA	코드	Classic McEliece
	REDOG	코드	Classic McEliece
Signature	HAETAE	격자	CRYSTALS-DILITHIUM
	NCC-Sign	격자	CRYSTALS-DILITHIUM
	MQ-Sign	다변수	UOV, Rainbow
	AIMer	영지식증명	Picnic

❖ 국제 PQC 부채널 분석 주요 결과 (5년 이내)

	Signature			PKE/KEM	
	격자	다변수	영지식증명	격자	코드
국제 논문 수	**23**	**3**	**3**	**71**	**19**

➢ NIST PQC 주요 후보에 대한 부채널 분석 결과 ➔ **KpqC 후보에 대한 부채널 분석 논의 필요**

연구 추진 전략

STEP 1. 국내·외 PQC 알고리즘에 대한 부채널 공격 동향 분석

- 격자 기반 PQC 부채널 공격 동향 분석
- 코드 기반 PQC 부채널 공격 동향 분석
- 다변수 기반 PQC 부채널 공격 동향 분석
- 영지식증명 기반 PQC 부채널 공격 동향 분석

STEP 2. KpqC 2라운드 후보 알고리즘 분석

- 후보 8종에 대한 알고리즘 구조 분석
- 유사 NIST PQC 알고리즘과의 차이점 분석

STEP 3. KpqC 부채널 취약점 분석 연구

- 후보 8종에 대한 알고리즘 수준 부채널 분석
- 후보 8종에 대한 참조코드 수준 부채널 분석
- 후보 1종 이상 검증 보드 수준에서의 부채널 분석 및 검증

1 연구 개요

2 국내·외 PQC 알고리즘 부채널 공격 동향

3 KpqC 알고리즘 부채널 분석

3.1 PKE/KEM

3.2 Signature

4 결론

▣ PQC PKE/KEM 부채널 공격 동향

	알고리즘	유사 NIST PQC 알고리즘
PKE/KEM	SMAUG-T	CRYSTALS-KYBER, SABER
	NTRU+	NTRU
	PALOMA	Classic McEliece
	REDOG	Classic McEliece

대상 암호	논문	구현	공격 대상	대상 연산	공격
Lattice KEM (KYBER, NTRU, SABER,…)	[SAMOS 2020]	S/W	Decapsulation	Multiplication	Non-profiling
	[IEEE Trans 2020]	H/W	Key Generation	Multiplication	Profiling
	[IEEE ACCESS 2020]	S/W	Encapsulation (Message)	Message encoding	Profiling
	[IEEE IoT 2022]	S/W	Decapsulation	Barrett reduction	Profiling
	[IEEE Trans 2021]	S/W	Decapsulation	Inverse NTT, Message decoding	Non-profiling
	[ACNS 2024]	S/W (mask)	Decapsulation	Boolean to arithmetic masking	Profiling
	[SNCS 2024]	S/W	Decapsulation	Multiplication	Profiling
SMAUG	$[CISC\text{-}S\ 2023]_1$	S/W	Decapsulation	HWT sampling	Non-profiling
Classic McEliece	[CHES 2017]	S/W	Decapsulation	Multiplication	Non-profiling
	[TCHES 2022]	S/W H/W	Decapsulation	Additive FFT	Profiling
	[IEEE Trans 2022]	S/W	Encapsulation (Message)	Multiplication	Profiling
	[ICISC 2022]	-	Decapsulation	Multiplication	Profiling
	$[ePrint\ 2023]_1$	S/W	Decapsulation	Matrix vector multiplication	Non-profiling
	[AfricaCrypt 2023]	S/W	Decapsulation	Goppa polynomial loading function	Profiling
	$[ePrint\ 2023]_2$	-	Key generation	Gaussian elimination	Profiling

▣ PQC PKE/KEM 부채널 공격 동향

	알고리즘	유사 NIST PQC 알고리즘
PKE/KEM	SMAUG-T	CRYSTALS-KYBER, SABER
	NTRU+	NTRU
	PALOMA	Classic McEliece
	REDOG	Classic McEliece

대상 암호	논문	구현	공격 대상	대상 연산	공격
Lattice KEM (KYBER, NTRU, SABER,…)	[SAMOS 2020]	S/W	Decapsulation	Multiplication	Non-profiling
	[IEEE Trans 2020]	H/W	Key Generation	Multiplication	Profiling
	[IEEE ACCESS 2020]	S/W	Encapsulation (Message)	Message encoding	Profiling
	[IEEE IoT 2022]	S/W	Decapsulation	Barrett reduction	Profiling
	[IEEE Trans 2021]	S/W	Decapsulation	Inverse NTT, Message decoding	Non-profiling
	[ACNS 2024]	S/W (mask)	Decapsulation	Boolean to arithmetic masking	Profiling
	[SNCS 2024]	S/W	Decapsulation	Multiplication	Profiling
SMAUG	$[CISC\text{-}S\ 2023]_1$	S/W	Decapsulation	HWT sampling	Non-profiling
Classic McEliece	[CHES 2017]	S/W	Decapsulation	Multiplication	Non-profiling
	[TCHES 2022]	S/W H/W	Decapsulation	Additive FFT	Profiling
	[IEEE Trans 2022]	S/W	Encapsulation (Message)	Multiplication	Profiling
	[ICISC 2022]	-	Decapsulation	Multiplication	Profiling
	$[ePrint\ 2023]_1$	S/W	Decapsulation	Matrix vector multiplication	Non-profiling
	[AfricaCrypt 2023]	S/W	Decapsulation	Goppa polynomial loading function	Profiling
	$[ePrint\ 2023]_2$	-	Key generation	Gaussian elimination	Profiling

▣ PQC Signature 부채널 공격 동향

	알고리즘	유사 NIST PQC 알고리즘
Signature	HAETAE	CRYSTALS-DILITHIUM
	NCC-Sign	CRYSTALS-DILITHIUM
	MQ-Sign	UOV, Rainbow
	AIMer	Picnic

대상 암호	논문	구현	공격 대상	대상 연산	공격
DILITHIUM	[ICEA 2020]	S/W	Signature Generation	NTT	Profiling
	[SAMOS 2020]	S/W	Signature Generation	Multiplication	Non-profiling
	[HOST 2021]	S/W	Signature Generation	Sampling	Profiling
	[ICCD 2021]	S/W	Signature Generation	Multiplication	Non-profiling
	[IEEE ACCESS 2021]	S/W	Signature Generation Key Generation	NTT, Sampling, Addition, Rounding, Packing	Profiling
	[ePrint 2022]	S/W	Signature Generation	Sampling	Profiling
	[IEEE Trans 2022]	S/W	Signature Generation	Sampling, NTT, Addition	Non-profiling
	[PQCrypto 2023]	H/W	Signature Generation	NTT, Multiplication	Profiling, Non-profiling
	[TCHES 2023]$_1$	S/W	Signature Generation	Decompose	Profiling
UOV, Rainbow	[TCHES 2018]	S/W	Signature Generation	Multiplication	Non-profiling
	[DATE 2021]	S/W	Signature Generation	Multiplication	Non-profiling
	[TCHES 2023]$_2$	S/W	Signature Generation	Multiplication	Profiling
Picnic	[PQCrypto 2021]	S/W	Signature Generation	Core MPC operation (LowMC)	Non-profiling
	[TCHES 2021]	S/W	Signature Generation	Online phase of Preprocessing	Non-profiling
AIMer (Round 1)	[CISC-S 2023]$_2$	S/W	Signature Generation	GF Addition	Non-profiling

▣ PQC Signature 부채널 공격 동향

	알고리즘	유사 NIST PQC 알고리즘
Signature	HAETAE	CRYSTALS-DILITHIUM
	NCC-Sign	CRYSTALS-DILITHIUM
	MQ-Sign	UOV, Rainbow
	AIMer	Picnic

대상 암호	논문	구현	공격 대상	대상 연산	공격
DILITHIUM	[ICEA 2020]	S/W	Signature Generation	NTT	Profiling
	[SAMOS 2020]	S/W	Signature Generation	Multiplication	Non-profiling
	[HOST 2021]	S/W	Signature Generation	Sampling	Profiling
	[ICCD 2021]	S/W	Signature Generation	Multiplication	Non-profiling
	[IEEE ACCESS 2021]	S/W	Signature Generation Key Generation	NTT, Sampling, Addition, Rounding, Packing	Profiling
	[ePrint 2022]	S/W	Signature Generation	Sampling	Profiling
	[IEEE Trans 2022]	S/W	Signature Generation	Sampling, NTT, Addition	Non-profiling
	[PQCrypto 2023]	H/W	Signature Generation	NTT, Multiplication	Profiling, Non-profiling
	[TCHES 2023]$_1$	S/W	Signature Generation	Decompose	Profiling
UOV, Rainbow	[TCHES 2018]	S/W	Signature Generation	Multiplication	Non-profiling
	[DATE 2021]	S/W	Signature Generation	Multiplication	Non-profiling
	[TCHES 2023]$_2$	S/W	Signature Generation	Multiplication	Profiling
Picnic	[PQCrypto 2021]	S/W	Signature Generation	Core MPC operation (LowMC)	Non-profiling
	[TCHES 2021]	S/W	Signature Generation	Online phase of Preprocessing	Non-profiling
AIMer (Round 1)	[CISC-S 2023]$_2$	S/W	Signature Generation	GF Addition	Non-profiling

1 연구 개요

2 국내·외 PQC 알고리즘 부채널 공격 동향

3 KpqC 알고리즘 부채널 분석

3.1 PKE/KEM

3.2 Signature

4 결론

▣ KpqC 알고리즘 분석 결과 요약

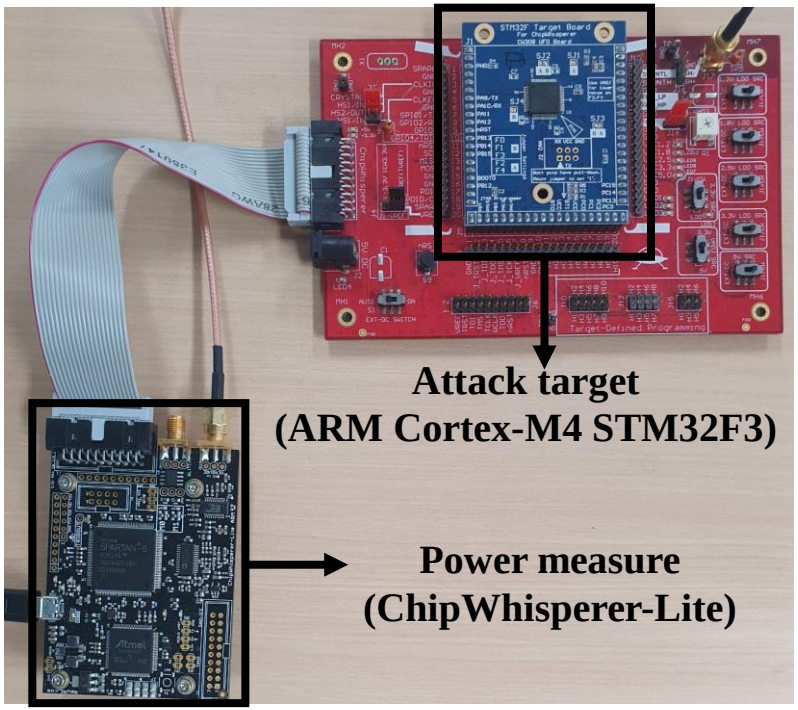
: 중간 : 최종

대상 KpqC 알고리즘		관련 공격 동향 분석	알고리즘 구조 분석	부채널 분석 취약점 식별
PKE/KEM	SMAUG-T	→	→	→
	NTRU+	→	➡	➡
	PALOMA	→	→	→
	REDOG	→	➡	➡
Signature	HAETAE	→	→	→
	NCC-Sign	→	➡	➡
	MQ-Sign	→	➡	➡
	AIMer	→	→	→

❖ **전체 8종에 대한 프로파일링, 비프로파일링 분석 위치 식별**

❖ **Signature 4종에 대한 비프로파일링 분석 실험 검증**

▣ KpqC 알고리즘 부채널 분석 검증 환경



Target Device	ARM Cortex-M4 MCU (STM32F303)
Target Implementation	KpqC round 2 reference code
Optimization Level	(arm-none-eabi-gcc 10.2.1) s
Number of Traces	5,000

- ❖ PKE/KEM 1종(SMAUG-T)에 대한 단순 전력 분석 실험 검증
- ❖ 전자서명 4종에 대한 상관 전력 분석 실험 검증

1 연구 개요

2 국내·외 PQC 알고리즘 부채널 공격 동향

3 KpqC 알고리즘 부채널 분석

3.1 PKE/KEM

3.2 Signature

4 결론

SMAUG-T 알고리즘 분석

Pink : Ephemeral Secret
red : Secret
green : Public

PKE/KEM			
SMAUG-T	NTRU+	PALOMA	REDOG

: 프로파일링 분석 대상
: 비프로파일링 분석 대상

❖ 부채널 분석 대상 위치 식별 (알고리즘)

SMAUG-T: PKE key generation

Input	-
Output	$pk = (A, b)$, $sk = s$

1: $\text{seed} \leftarrow \{0,1\}^{256}$
2: $(seed_A, seed_{sk}, seed_e) \leftarrow \text{XOF}(seed)$
3: $A \leftarrow \text{expandA}(seed_A) \in \mathcal{R}_q^{k \times k}$
4: $s \leftarrow \text{HWT}_{h_s}(seed_{sk}) \in S_\eta^k$
5: $e \leftarrow \text{D}_{\mathbb{Z},\sigma}(seed_e) \in \mathcal{R}_q^k$
6: $b = -A \cdot s + e \in \mathcal{R}_q^k$
7: **return** $pk = (A, b)$, $sk = s$

SMAUG-T: Encryption

Input	$pk = (A, b)$, m, $seed_r$
Output	$c = (c_1, c_2)$

1: $r \leftarrow \text{HWT}_{h_r}(seed_r) \in S_\eta^k$
2: $c_1 = \left\lfloor \frac{p}{q} \cdot A \cdot r \right\rceil \in \mathcal{R}_p^k$
3: $c_2 = \left\lfloor \frac{p'}{q} \cdot \langle b, r \rangle + \frac{p'}{t} \cdot m \right\rceil \in \mathcal{R}_{p'}$
4: **return** $c = (c_1, c_2)$

SMAUG-T: Decryption

Input	$sk = s$, $c = (c_1, c_2)$
Output	m

1: $m = \left\lfloor \frac{t}{p} \cdot \langle c_1, s \rangle + \frac{t}{p'} \cdot c_2 \right\rceil \in \mathcal{R}_t$
2: **return** m

SMAUG-T: KEM key generation

Input	-
Output	$pk = (A, b)$, $sk = (s, d, pk)$

1: $(A, b, s) \leftarrow \text{PKE_keygen}(\cdot)$
2: $d \leftarrow \{0,1\}^{256}$
3: **return** $pk = (A, b)$, $sk = (s, d, pk)$

SMAUG-T: Encapsulation

Input	$pk = (A, b)$
Output	c, K

1: $\mu \leftarrow \{0,1\}^{256}$
2: $(K, seed) \leftarrow \text{G}(\mu, \text{H}(pk))$
3: $c = \text{PKE_encrypt}(pk, \mu, seed)$
4: **return** c, K

SMAUG-T: Decapsulation

Input	$sk = (s, d, pk)$, c
Output	K'

1: $\mu' = \text{PKE_decrypt}(s, c)$
2: $(K', seed') \leftarrow \text{G}(\mu', \text{H}(pk))$
3: $c' = \text{PKE_encrypt}(pk, \mu', seed')$
4: $(\hat{K}, \cdot) \leftarrow \text{G}(d, \text{H}(c))$
5: **if** $c \neq c'$, **then** $K' = \hat{K}$
6: **return** K'

SMAUG-T 알고리즘 분석

Pink : Ephemeral Secret
red : Secret
green : Public

PKE/KEM			
SMAUG-T	NTRU+	PALOMA	REDOG

: 프로파일링 분석 대상
: 비프로파일링 분석 대상

❖ 통계 분석 대상 위치 식별 (참조 코드)

SMAUG-T: Decryption	
Input	$sk = s,\ c = (c_1, c_2)$
Output	m
1: $m = \left\lfloor \frac{t}{p} \cdot \langle c_1, s \rangle + \frac{t}{p'} \cdot c_2 \right\rceil \in \mathcal{R}_t$	
2: return m	

SMAUG-T: Decapsulation	
Input	$sk = (s, d, pk), c$
Output	K'
1: $\mu' = \text{PKE_decrypt}(s, c)$	
2: $(K', seed') \leftarrow G(\mu', H(pk))$	
3: $c' = \text{PKE_encrypt}(pk, \mu', seed')$	
4: $(\hat{K}, \cdot) \leftarrow G(d, H(c))$	
5: if $c \neq c'$, then $K' = \hat{K}$	
6: return K'	

```
void poly_mult_add(poly *res, const poly *op1, const sppoly *op2) {
    uint16_t temp[LWE_N * 2] = {0};

    for (size_t j = 0; j < op2->neg_start; ++j) {
        poly_add(temp, op1, (op2->sx)[j]);
    }

    for (size_t j = op2->neg_start; j < op2->cnt; ++j) {
        poly_sub(temp, op1, (op2->sx)[j]);
    }
    poly_reduce(res, temp);
}
```

```
void poly_add(uint16_t res[2 * LWE_N], const poly *op1, const uint8_t deg) {
    for (size_t i = 0; i < LWE_N; ++i)
        res[deg + i] += op1->coeffs[i];
```

CPA

deg + i (deg∈ {0,1, … , 255})

2^8개 추측 CPA

공격 결과 요약

➢ 계수가 1인 s의 항 (deg)
➔ 계수별 s의 모든 항
➔ 비밀 다항식 s

SMAUG-T 알고리즘 분석

Pink : Ephemeral Secret
red : Secret
green : Public

PKE/KEM			
SMAUG-T	NTRU+	PALOMA	REDOG

: 프로파일링 분석 대상
: 비프로파일링 분석 대상

❖ 단순 분석 대상 위치 식별 (참조 코드)

SMAUG-T: Decryption	
Input	$sk = s,\ c = (c_1, c_2)$
Output	m
1: $m = \left\lfloor \frac{t}{p} \cdot \langle c_1, s \rangle + \frac{t}{p'} \cdot c_2 \right\rceil \in \mathcal{R}_t$	
2: **return** m	

```
void poly_mult_add(poly *res, const poly *op1, const sppoly *op2) {
    uint16_t temp[LWE_N * 2] = {0};

    for (size_t j = 0; j < op2->neg_start; ++j) {
        poly_add(temp, op1, (op2->sx)[j]);
    }

    for (size_t j = op2->neg_start; j < op2->cnt; ++j) {
        poly_sub(temp, op1, (op2->sx)[j]);
    }
    poly_reduce(res, temp);
}
```

SMAUG-T: Decapsulation	
Input	$sk = (s, d, pk), c$
Output	K'
1: $\mu' = \text{PKE_decrypt}(s, c)$	
2: $(K', seed') \leftarrow \text{G}(\mu', \text{H}(pk))$	
3: $c' = \text{PKE_encrypt}(pk, \mu', seed')$	
4: $(\hat{K}, \cdot) \leftarrow \text{G}(d, \text{H}(c))$	
5: **if** $c \neq c'$, **then** $K' = \hat{K}$	
6: **return** K'	

SPA

1계수의 개수만큼 poly_add 반복

-1계수의 개수만큼 poly_sub 반복

SPA로 poly_add, poly_sub의 개수 파악

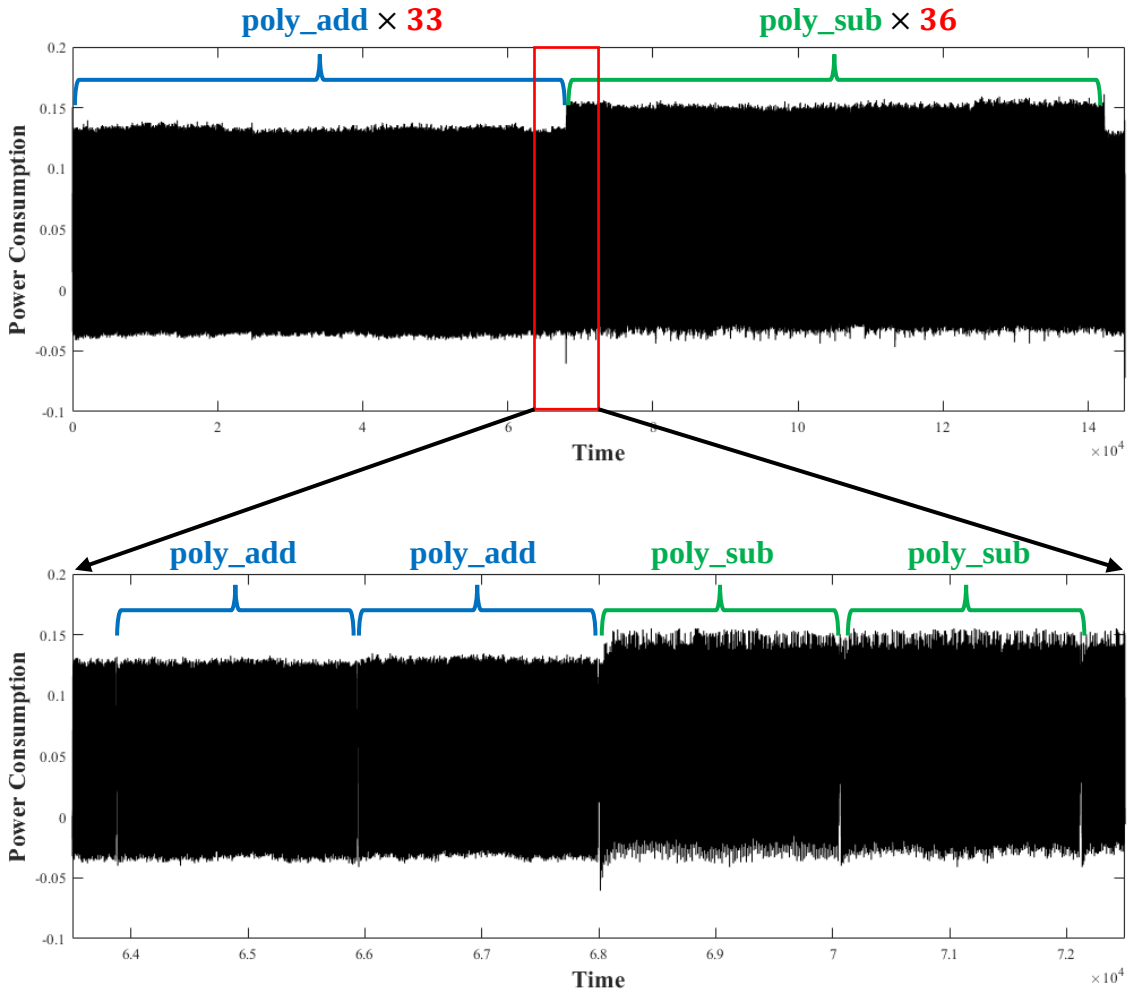
➔ 비밀키 다항식의 1, -1계수의 개수 복구

SMAUG-T SPA 결과

Pink : Ephemeral Secret
red : Secret
green : Public

PKE/KEM			
SMAUG-T	NTRU+	PALOMA	REDOG

poly_mult_add 전력 파형




```
void poly_mult_add(poly *res, const poly *op1, const sppoly *op2) {
    uint16_t temp[LWE_N * 2] = {0};

    for (size_t j = 0; j < op2->neg_start; ++j) {
        poly_add(temp, op1, (op2->sx)[j]);
    }

    for (size_t j = op2->neg_start; j < op2->cnt; ++j) {
        poly_sub(temp, op1, (op2->sx)[j]);
    }
    poly_reduce(res, temp);
}
```

공격 결과 요약

➢ 비밀 다항식 s의 1, -1 계수 항의 개수 복구

▣ NTRU+ 알고리즘 분석

Pink : Ephemeral Secret
red : Secret
green : Public

PKE/KEM			
SMAUG-T	NTRU+	PALOMA	REDOG

: 프로파일링 분석 대상
: 비프로파일링 분석 대상

❖ 부채널 분석 대상 위치 식별 (알고리즘)

NTRU+: KeyGen

Input	-
Output	$pk = h$, $sk = (f, h^{-1})$

1: $seed \leftarrow \{0,1\}^{256}$
2: $f', g' \leftarrow \mathrm{CBD}(seed) \in S_\eta$
3: $f = 3f' + 1$
4: **if** $\nexists f^{-1}, g^{-1} \in \mathcal{R}_q$, **then go to line 1**
5: $h = 3gf^{-1}$
6: **return** $pk = h, sk = (f, h^{-1})$

NTRU+ PKE: Encryption

Input	$pk = h$, $m \in \{0,1\}^{l_m}$
Output	c

1: $m' \leftarrow \{0,1\}^{l_r}$
2: $\widetilde{m} \leftarrow m \| m' \in \{0,1\}^{n=l_m+l_r}$
3: $R \leftarrow \mathrm{H}(\widetilde{m}, \mathrm{F}(h))$
4: $r \leftarrow \mathrm{CBD}(R) \in S_\eta$
5: $m' = \mathrm{SOTP}(\widetilde{m}, \mathrm{G}(r))$
6: $\boldsymbol{c = h \cdot r + m'}$
7: **return** $\boldsymbol{c}$

NTRU+ PKE: Decryption

Input	$sk = (f, h)$, $\boldsymbol{c}$
Output	$\widetilde{m}$

1: $m' = (c \cdot f) mod\ 3$
2: $r = (c - m')h^{-1}$
3: $\widetilde{m}, fail = \mathrm{InvSOTP}(m', \mathrm{G}(r))$
4: $R' \leftarrow \mathrm{H}(\widetilde{m}, \mathrm{F}(h))$
5: $r' \leftarrow \mathrm{CBD}(R') \in S_\eta$
6: **if** $r \neq r'$ **or** $fail = 1$, **then** $\widetilde{m} = 0$
7: **return** $\widetilde{m}$

NTRU+ KEM: Encapsulation

Input	$pk = h$
Output	c, K

1: $m \leftarrow \{0,1\}^n$
2: $(R, K) \leftarrow \mathrm{H}'(m, pk)$
3: $r \leftarrow \mathrm{CBD}(R) \in S_\eta$
4: $m' = \mathrm{SOTP}(m, \mathrm{G}(r))$
5: $c = h \cdot r + m'$
6: **return** $(\boldsymbol{c}, K)$

NTRU+ KEM: Decapsulation

Input	$sk = (f, h^{-1})$, c
Output	K

1: $m' = (c \cdot f) mod\ 3$
2: $r = (c - m')h^{-1}$
3: $m, fail = \mathrm{InvSOTP}(m', \mathrm{G}(r))$
4: $(R', K) \leftarrow \mathrm{H}'(m)$
5: $r' \leftarrow \mathrm{CBD}(R') \in S_\eta$
6: **if** $r \neq r'$ **or** $fail = 1$, **then** $K = 0$
7: **return** K

NTRU+ 알고리즘 분석

Pink : Ephemeral Secret
red : Secret
green : Public

PKE/KEM			
SMAUG-T	NTRU+	PALOMA	REDOG

: 프로파일링 분석 대상
: 비프로파일링 분석 대상

❖ 통계 분석 대상 위치 식별 (참조 코드)

NTRU+ PKE: Decryption	
Input	$sk = (f, h), c$
Output	$\tilde{m}$

1: $m' = (c \cdot f) mod\ 3$
2: $r = (c - m')h^{-1}$
3: $\tilde{m}, fail = \mathrm{InvSOTP}(m', \mathrm{G}(r))$
4: $R' \leftarrow \mathrm{H}(\tilde{m}, \mathrm{F}(h))$
5: $r' \leftarrow \mathrm{CBD}(R') \in S_\eta$
6: **if** $r \neq r'$ **or** $fail = 1$, **then** $\tilde{m} = 0$
7: **return** $\tilde{m}$

NTRU+ KEM: Decapsulation	
Input	$sk = (f, h^{-1}), c$
Output	K

1: $m' = (c \cdot f) mod\ 3$
2: $r = (c - m')h^{-1}$
3: $m, fail = \mathrm{InvSOTP}(m', \mathrm{G}(r))$
4: $(R', K) \leftarrow \mathrm{H}'(m)$
5: $r' \leftarrow \mathrm{CBD}(R') \in S_\eta$
6: **if** $r \neq r'$ **or** $fail = 1$, **then** $K = 0$
7: **return** K

```
void poly_basemul(poly *r, const poly *a, const poly *b)
{
    for(int i = 0; i < NTRUPLUS_N/6; i++)
    {
        basemul(r->coeffs + 6*i, a->coeffs + 6*i, b->coeffs + 6*i, zetas[96 + i]);
        basemul(r->coeffs + 6*i + 3, a->coeffs + 6*i + 3, b->coeffs + 6*i + 3, -zetas[96 + i]);
    }
}
```

```
void basemul(int16_t c[3], const int16_t a[3], const int16_t b[3], int16_t zeta)
{
    c[0]  = fqmul(a[2], b[1]);
    c[0] += fqmul(a[1], b[2]);
    c[0]  = fqmul(c[0], zeta);
    c[0] += fqmul(a[0], b[0]);

    c[1]  = fqmul(a[2], b[2]);
    c[1]  = fqmul(c[1], zeta);
    c[1] += fqmul(a[0], b[1]);
    c[1] += fqmul(a[1], b[0]);
    c[1]  = barrett_reduce(c[1]);

    c[2]  = fqmul(a[2], b[0]);
    c[2] += fqmul(a[1], b[1]);
    c[2] += fqmul(a[0], b[2]);
    c[2]  = barrett_reduce(c[2]);
}
```

CPA

$c_i f_i \quad (f_i \in \{0, 1, \dots, 3456\})$

약 2^{12}개 추측 CPA

공격 결과 요약

➢ 계수 f_i 12-bit 복구
➔ $f_0 \sim f_{n-1}$ 전체 ➔ 비밀 다항식 f

▣ PALOMA 알고리즘 분석

Pink : Ephemeral Secret
red : Secret
green : Public

PKE/KEM			
SMAUG-T	NTRU+	PALOMA	REDOG

: 프로파일링 분석 대상

: 비프로파일링 분석 대상

❖ 부채널 분석 대상 위치 식별 (알고리즘)

PALOMA: Key generation

Input	-
Output	pk, sk

$r_{\hat{c}}, L, g(X), H \leftarrow$ GenRandGoppaCode()
$r_{\hat{c}}, S^{-1}, \hat{H} \leftarrow$ GenScrambledCode(H)
$pk = \hat{H}_{[n-k:n]} \in \mathbb{F}_2^{(n-k)\times k}$
$r \xleftarrow{\$} \{0,1\}^{256}$
$sk = (L, g(X), S^{-1}, r_{\hat{c}}, r)$
return pk, sk

PALOMA: Encryption

Input	$pk = \hat{H}_{[n-k:n]}, \hat{e} \in \mathbb{F}_2^n \ \ (w_H(\hat{e}) = t)$
Output	$\hat{s} \in \mathbb{F}_2^{n-k}$

$\hat{H} = [I_{n-k} | \hat{H}_{[n-k:n]}] \in \mathbb{F}_2^{(n-k)\times n}$
$\hat{s} = \hat{H}\hat{e} \in \mathbb{F}_2^{n-k}$
return $\hat{s}$

PALOMA: Decryption

Input	$sk = (L, g(X), S^{-1}, r_{\hat{c}}, r), \hat{s} \in \mathbb{F}_2^{n-k}$
Output	$\hat{e} \in \mathbb{F}_2^n \ \ (w_H(\hat{e}) = t)$

$s = S^{-1}\hat{s}$
$e = \text{RecoverErrVec}(L, g(X), s)$
$\hat{e} = \text{PermInv}(e, r_{\hat{c}})$ $\quad //\hat{e} = P^{-1}e$
return $\hat{e}$

PALOMA: Encapsulation

Input	$pk = \hat{H}_{[n-k:n]} \in \mathbb{F}_2^{(n-k)\times k}$
Output	$c = (\hat{r}, \hat{s}) \in \{0,1\}^{256} \times \mathbb{F}_2^{n-k}, \kappa \in \{0,1\}^{256}$

$r^* \xleftarrow{\$} \{0,1\}^{256}$
$e^* \leftarrow \text{GenErrVec}(r^*)$ $\quad //e^* \in \mathbb{F}_2^n,\ w_H(e^*) = t$
$\hat{r} \leftarrow \text{RO}_G(e^*)$
$\hat{e} = \text{Perm}(e^*, \hat{r})$ $\quad //\hat{e} = Pe^*$
$\hat{s} = \text{PKE_encrypt}(pk, \hat{e})$
$\kappa \leftarrow \text{RO}_H(e^* || \hat{r} || \hat{s})$
return $c = (\hat{r}, \hat{s}), \kappa$

PALOMA: Decapsulation

Input	$sk = (L, g(X), S^{-1}, r_{\hat{c}}, r), c = (\hat{r}, \hat{s})$
Output	$\kappa \in \{0,1\}^{256}$

$\hat{e} = \text{PKE_decrypt}(sk, \hat{s})$
$e^* = \text{PermInv}(\hat{e}, \hat{r})$ $\quad //e^* = P^{-1}\hat{e}$
$\hat{r}' \leftarrow \text{RO}_G(e^*)$
$\tilde{e} \leftarrow \text{GenErrVec}(r)$
If $\hat{r}' \neq \hat{r}$ **then**
  $\kappa \leftarrow \text{RO}_H(\tilde{e} || \hat{r} || \hat{s})$
Else
  $\kappa \leftarrow \text{RO}_H(e^* || \hat{r} || \hat{s})$
return κ

PALOMA 알고리즘 분석

Pink : Ephemeral Secret
red : Secret
green : Public

PKE/KEM			
SMAUG-T	NTRU+	PALOMA	REDOG

: 프로파일링 분석 대상
: 비프로파일링 분석 대상

❖ 통계 분석 대상 위치 식별 (참조 코드)

PALOMA: Decryption	
Input	$sk = (L, g(X), S^{-1}, r_{\hat{c}}, r), \hat{s} \in \mathbb{F}_2^{n-k}$
Output	$\hat{e} \in \mathbb{F}_2^n \ (w_H(\hat{e}) = t)$
1: $s = S^{-1}\hat{s}$	
2: $e = \text{RecoverErrVec}(L, g(X), s)$	
3: $\hat{e} = \text{PermInv}(e, r_{\hat{c}})$ $\quad //\hat{e} = P^{-1}e$	
4: **return** $\hat{e}$	

PALOMA: Decapsulation	
Input	$sk = (L, g(X), S^{-1}, r_{\hat{c}}, r), c = (\hat{r}, \hat{s})$
Output	$\kappa \in \{0,1\}^{256}$
1: $\hat{e} = \text{PKE_decrypt}(sk, \hat{s})$	
2: $e^* = \text{PermInv}(\hat{e}, \hat{r})$ $\quad //e^* = P^{-1}\hat{e}$	
3: $\hat{r}' \leftarrow \text{RO}_G(e^*)$	
4: $\tilde{e} \leftarrow \text{GenErrVec}(r)$	
5: **If** $\hat{r}' \neq \hat{r}$ **then**	
6: $\quad \kappa \leftarrow \text{RO}_H(\tilde{e} \| \hat{r} \| \hat{s})$	
7: **Else**	
8: $\quad \kappa \leftarrow \text{RO}_H(e^* \| \hat{r} \| \hat{s})$	
9: **return** κ	

```
void matXvec(
        OUT Word* out_vec,
        IN const Word* in_mat,
        IN const Word* in_vec,
        IN int rownum,
        IN int colnum)
{
    int num_of_WORD_BITS_in_row = rownum / WORD_BITS;
    int col_index;

    for (int i = 0; i < colnum; i++)
    {
        col_index = (i * num_of_WORD_BITS_in_row);

        if ((in_vec[i / WORD_BITS] >> (i % WORD_BITS)) & 1)
        {
            xor_vec(out_vec, in_mat, col_index, num_of_WORD_BITS_in_row);
        }
    }
}

inline void xor_vec(
        OUT Word* out_vec,
        IN const Word* in_mat,
        IN int index,
        IN int num)
{
    for (int i = 0; i < num; i++)
    {
        out_vec[i] ^= in_mat[index + i];
    }
}
```

CPA

$S^{-1}\hat{s}$ ($S^{-1} \in \{0,1,\dots,255\}$)

$\hat{s}$ 고정시 약 2^8개 추측 CPA

공격 결과 요약

➢ S_0^{-1}의 8-bit 복구
➔ 비밀키 행렬 S_0^{-1}

▣ REDOG 알고리즘 분석

Pink : Ephemeral Secret
red : Secret
green : Public

PKE/KEM			
SMAUG-T	NTRU+	PALOMA	REDOG

: 프로파일링 분석 대상

: 비프로파일링 분석 대상

❖ 부채널 분석 대상 위치 식별 (알고리즘)

REDOG: Key generation	
Input	-
Output	$pk = (M, F), sk = (P, H, S, \Phi_H)$

1: $H, \Phi_H \leftarrow$ GenRandGabidulin()
2: $P, S, M \leftarrow$ GenScrambledCode(H)
3: $F = MP^{-1}H_1H_2^{-1}S$
4: $pk = (M, F)$
5: $sk = (P, H, S, \Phi_H)$
6: **return** pk, sk

REDOG: Encryption	
Input	$pk = (M, F) \in \mathbb{F}_{2^m}^{\ell \times n} \times \mathbb{F}_{2^m}^{\ell \times (n-k)}$, $m \in \mathbb{F}_{2^m}^{\ell}$
Output	$c = (c_1, c_2) \in \mathbb{F}_{2^m}^{n} \times \mathbb{F}_{2^m}^{n-k}$

1: $e_1 \leftarrow$ GenErrVec() //$e_1 \in \mathbb{F}_{2^m}^{n}$, $w_H(e_1) = t_1$
2: $e_2 \leftarrow$ GenErrVec() //$e_2 \in \mathbb{F}_{2^m}^{n-k}$, $w_H(e_2) = t_2$
3: $m' = m + \mathrm{H}(e_1, e_2)$
4: $c_1 = m'M + e_1$
5: $c_2 = m'F + e_2$
6: **return** $c = (c_1, c_2)$

REDOG: Decryption	
Input	$sk = (P, H, S, \Phi_H), c = (c_1, c_2)$
Output	$m \in \mathbb{F}_{2^m}^{\ell}$

1: $\hat{m} = c_1P^{-1}H_1 - c_2S^{-1}H_2$
2: $(e_1', e_2') = (e_1P^{-1}, e_2S^{-1}) = \Phi_H(\hat{m})$
3: $e_1 = e_1'P$; $e_2 = e_2'S$
4: $m' = \mathrm{Solve}(c_1 - e_1)$
5: $m = m' - \mathrm{H}(e_1, e_2)$
6: **return** m

CPA

$c_{2,0}S_0^{-1}$ $(S_0^{-1} \in \mathbb{F}_{2^n})$

2^n개 추측 CPA

공격 결과 요약

➢ S_0^{-1} n-bit 복구
➔ 비밀키 행렬 S_0^{-1}

1 연구 개요

2 국내·외 PQC 알고리즘 부채널 공격 동향

✓ 3 KpqC 알고리즘 부채널 분석

3.1 PKE/KEM

✓ 3.2 Signature

4 결론

▣ HAETAE 알고리즘 분석

Pink : Ephemeral Secret
red : Secret
green : Public

Signature			
HAETAE	**NCC-Sign**	**MQ-Sign**	**AIMer**

: 프로파일링 분석 대상

: 비프로파일링 분석 대상

❖ 부채널 분석 대상 위치 식별 (알고리즘)

HAETAE: KeyGen	
Input	-
Output	$pk = A, sk = (s, A)$

$A_0 \leftarrow \mathcal{R}_q^{k\times(l-1)}$
$(s_1, s_2) \leftarrow S_\eta^{l-1} \times S_\eta^k$
$b = -2(A_0 \cdot s_1 + s_2) \in \mathcal{R}_q^k$
$A = (b|2A_0)\ mod\ q \in \mathcal{R}_q^{k\times l}$
$s = (1|s_1|s_2) \in S_\eta^{l+k}$
if $\mathcal{N}(s) > \gamma^2 n$, **then go to line 2**
return $pk = A, sk = (s, A)$

HAETAE: Signature Generation	
Input	$sk = (s, A), m$
Output	$\sigma = (\lfloor z \rceil, c\ )$

$y = (y_1, y_2) \leftarrow$ SampleInHyperball() $\in \mathcal{R}^l \times \mathcal{R}^k$
$w = Ay_1 + 2y_2 \in \mathcal{R}_q^k$
$c = \mathrm{H}(w, m) \in \mathcal{R}_2$
$z = (z_1, z_2) = y + (-1)^b cs \in \mathcal{R}^l \times \mathcal{R}^k$
if $\|z\|_2 \geq B'$, **then go to line 1**
else if $\|2z - y\|_2 < B$, **then go to line 1**
return $\sigma = (\lfloor z \rceil, c\ )$

HAETAE 알고리즘 분석

Pink : Ephemeral Secret
red : Secret
green : Public

Signature			
HAETAE	NCC-Sign	MQ-Sign	AIMer

: 프로파일링 분석 대상
: 비프로파일링 분석 대상

❖ CPA 논리 식별

HAETAE: Signature Generation	
Input	$sk = (s, A), m$
Output	$\sigma = (\lfloor z \rceil, c)$

1: $y = (y_1, y_2) \leftarrow \text{SampleInHyperball}() \in \mathcal{R}^l \times \mathcal{R}^k$
2: $w = Ay_1 + 2y_2 \in \mathcal{R}_q^k$
3: $c = \text{H}(w, m) \in \mathcal{R}_2$
4: $z = (z_1, z_2) = y + (-1)^b cs \in \mathcal{R}^l \times \mathcal{R}^k$
5: **if** $\|z\|_2 \geq B'$, **then go to line 1**
6: **else if** $\|2z - y\|_2 < B$, **then go to line 1**
7: **return** $\sigma = (\lfloor z \rceil, c)$

CPA 1

$v = c_0 s_0 \bmod q$

$s_0 \in \{0, \ldots, q-1\}$

$q \approx 2^{16}$개 추측 CPA

CPA

$s_0 \in \{\alpha_0, \alpha_1\}$

$s_1 \in \{\beta_0, \beta_1\}$

…

CPA 2

$v = \zeta(c_0 s_0 - c_1 s_1) \bmod q$

$s_0 \in \{\alpha_0, \alpha_1\}, s_1 \in \{\beta_0, \beta_1\}$

2*2개 추측 CPA

CPA

(s_0, s_1)

$\in \{(\alpha_0, \beta_0), (\alpha_1, \beta_1)\}$

CPA 2*

$v = c_0 s_0 q^{-1}$

$s_0 \in \{\alpha_0, \alpha_1\}$

2개 추측 CPA

CPA

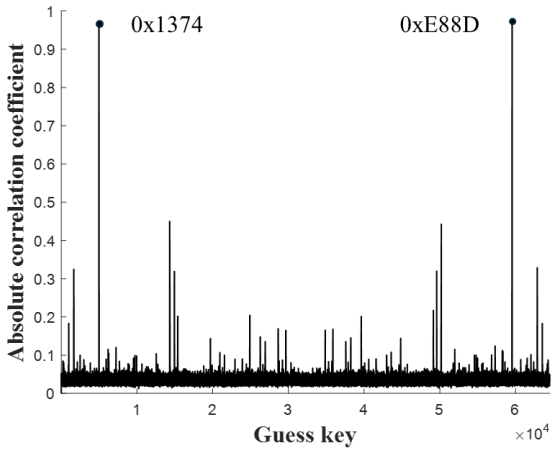
$s_0 = \alpha$

HAETAE CPA 결과

Pink : Ephemeral Secret
red : Secret
green : Public

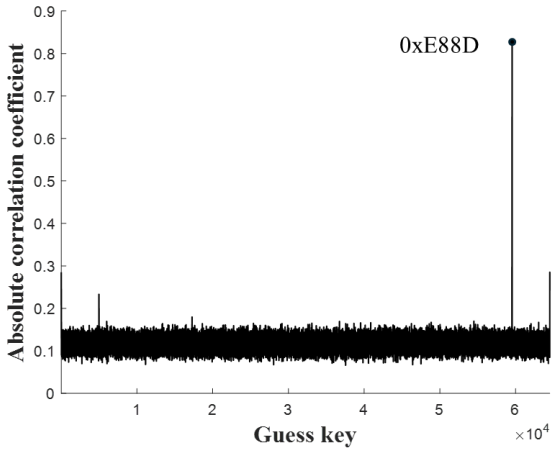
Signature			
HAETAE	NCC-Sign	MQ-Sign	AIMer

❖ **CPA 1)** $c_0 s_0 \bmod q$



➢ $s_0 = 0\text{x}1374$ or $0\text{xE}88\text{D}$

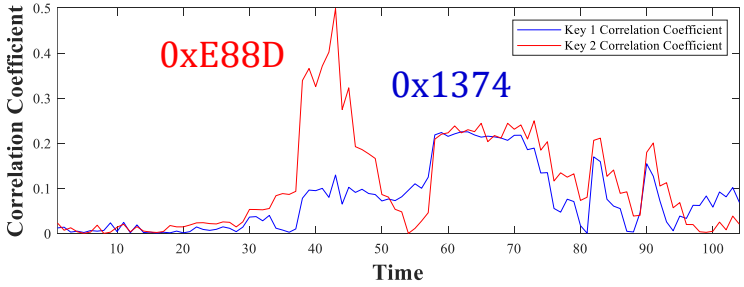
❖ **CPA 2)** $\zeta(c_0 s_0 - c_1 s_1) \bmod q$



➢ s_1 값 고정후 s_0 값 추측

➢ $(s_0, s_1) = (\beta_0, 0\text{xE}88\text{D})$ or $(\beta_1, 0\text{x}1374)$

❖ **CPA 2*)** $c_0 s_0 q^{-1}$



➢ $s_0 = 0\text{xE}88\text{D}$

공격 결과 요약

➢ 계수 s_0 16-bit 복구
➔ $s_0 \sim s_{255}$ 전체 ➔ 비밀 다항식 s

NCC-Sign 알고리즘 분석

Pink : Ephemeral Secret
red : Secret
green : Public

Signature			
HAETAE	NCC-Sign	MQ-Sign	AIMer

: 프로파일링 분석 대상

: 비프로파일링 분석 대상

❖ 부채널 분석 대상 위치 식별 (알고리즘)

NCC-Sign: KeyGen	
Input	-
Output	$pk = (a, t_1)$, $sk = (a, ph, t_0, s_1, s_2)$

1: $a \leftarrow \mathcal{R}_q$
2: $(s_1, s_2) \leftarrow S_\eta \times S_\eta$
3: $t = as_1 + s_2 \in \mathcal{R}_q$
4: $(t_1, t_0) = \text{Power2Round}(t)$
5: $ph = \text{H}(a, t_1)$
5: **return** $pk = (a, t_1)$, $sk = (a, ph, t_0, s_1, s_2)$

NCC-Sign: Signature Generation	
Input	$sk = (a, ph, t_0, s_1, s_2), m$
Output	σ

01: $\mu \leftarrow \text{H}(ph \| m) \in \{0,1\}^{512}$
02: $y \leftarrow S_{\gamma_1}$
03: $w = ay \in \mathcal{R}_q$
04: $c \leftarrow \text{SampleInBall}(\mu \| w) \in \mathcal{R}_q$
05: $z = y + cs_1 \in \mathcal{R}_q$
06: $r_0 = \text{LowBits}_q(w - cs_2, 2\gamma_2)$
07: **if** $\|z\|_\infty \geq \gamma_1 - \beta$ **or** $\|r_0\|_\infty \geq \gamma_2 - \beta$, **then**
08: **go to line 2**
09: $h = \text{MakeHint}_q(-ct_0, w - cs_2 + ct_0, 2\gamma_2)$
10: **if** $\|ct_0\|_\infty \geq \gamma_2$ **or** $\text{HW}(h) > \omega$, **then**
11: **go to line 2**
12: **return** $\sigma \leftarrow (c, z, h)$

NCC-Sign 알고리즘 분석

Pink : Ephemeral Secret
red : Secret
green : Public

Signature			
HAETAE	NCC-Sign	MQ-Sign	AIMer

: 프로파일링 분석 대상
: 비프로파일링 분석 대상

❖ CPA 논리 식별

NCC-Sign: Signature Generation	
Input	$sk = (a, ph, t_0, s_1, s_2), m$
Output	σ

01: $\mu \leftarrow \mathrm{H}(ph||m) \in \{0,1\}^{512}$
02: $y \leftarrow S_{\gamma_1}$
03: $w = ay \in \mathcal{R}_q$
04: $c \leftarrow \mathrm{SampleInBall}(\mu||w) \in \mathcal{R}_q$
05: $z = y + cs_1 \in \mathcal{R}_q$
06: $r_0 = \mathrm{LowBits}_q(w - cs_2, 2\gamma_2)$
07: **if** $\|z\|_\infty \geq \gamma_1 - \beta$ **or** $\|r_0\|_\infty \geq \gamma_2 - \beta$, **then**
08: **go to line 2**
09: $h = \mathrm{MakeHint}_q(-ct_0, w - cs_2 + ct_0, 2\gamma_2)$
10: **if** $\|ct_0\|_\infty \geq \gamma_2$ **or** $\mathrm{HW}(h) > \omega$, **then**
11: **go to line 2**
12: **return** $\sigma \leftarrow (c, z, h)$

CPA 1

$v = c_0 s_0 \bmod q$

$s_0 \in \{0, \ldots, q-1\}$

q개 추측 CPA

CPA ⇒

$s_0 \in \{\alpha_0, \alpha_1\}$

$s_1 \in \{\beta_0, \beta_1\}$

…

CPA 2

$v = \zeta(c_0 s_0 - c_1 s_1) \bmod q$

$s_0 \in \{\alpha_0, \alpha_1\}, s_1 \in \{\beta_0, \beta_1\}$

2*2개 추측 CPA

CPA ⇒

(s_0, s_1)

$\in \{(\alpha_0, \beta_0), (\alpha_1, \beta_1)\}$

CPA 2*

$v = c_0 s_0 q^{-1}$

$s_0 \in \{\alpha_0, \alpha_1\}$

2개 추측 CPA

CPA ⇒

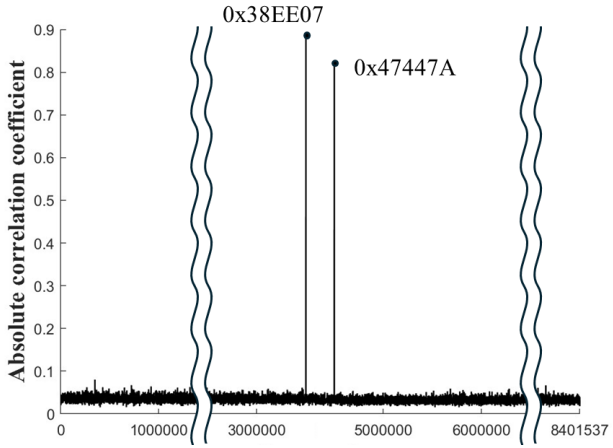
$s_0 = \alpha$

NCC-Sign CPA 결과

Pink : Ephemeral Secret
red : Secret
green : Public

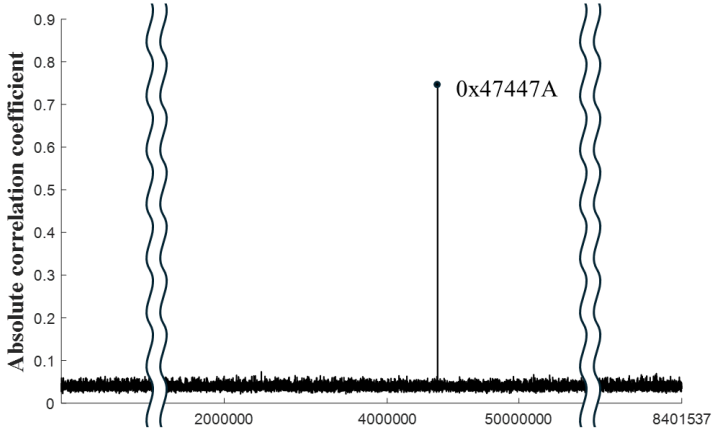
Signature			
HAETAE	NCC-Sign	MQ-Sign	AIMer

❖ **CPA 1)** $c_0 s_0 \bmod q$



➢ $s_0 = 0\text{x}38\text{EE}07$ or $0\text{x}47447\text{A}$

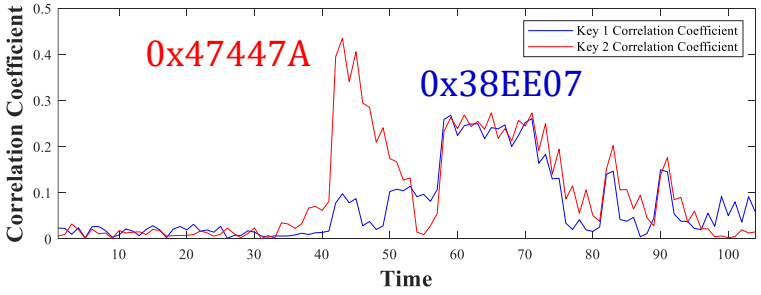
❖ **CPA 2)** $\zeta(c_0 s_0 - c_1 s_1) \bmod q$



➢ s_1 값 고정후 s_0 값 추측

➢ $(s_0, s_1) = (\beta_0, 0\text{x}47447\text{A})$ or $(\beta_1, 0\text{x}38\text{EE}07)$

❖ **CPA 2*)** $c_0 s_0 q^{-1}$



➢ $s_0 = 0\text{x}47447\text{A}$

공격 결과 요약

➢ 계수 s_0 23-bit 복구
➔ $s_0 \sim s_{n-1}$ 전체 ➔ 비밀 다항식 s

▣ MQ-Sign 알고리즘 분석

Pink : Ephemeral Secret
red : Secret
green : Public

Signature			
HAETAE	NCC-Sign	MQ-Sign	AIMer

: 프로파일링 분석 대상

: 비프로파일링 분석 대상

❖ 부채널 분석 대상 위치 식별 (알고리즘)

MQ-Sign: Key Generation	
Input	-
Output	$pk = P, sk = (F, T)$

1: $T \leftarrow GF(2^8)^{v \times o}$
2: $\mathcal{T} = \begin{pmatrix} I & T \\ 0 & I \end{pmatrix} \in GF(2^8)^{(v+o)\times(v+o)}$
3: $F \leftarrow GF(2^8)^{o\times(v\times(v+o))}$
4: $P = F \circ \mathcal{T}$
5: **return** $pk = P, sk = (F, T)$

MQ-Sign: Signature Generation	
Input	$sk = (F, T), m$
Output	σ

01: **while** $\exists A^{-1}, J$
02: $s_V = (s_1, \dots, s_v) \leftarrow GF(2^8)$
03: $R = \begin{pmatrix} A & B \\ C & D \end{pmatrix} = Coeffi(F^{(1)}(s_V), \dots, F^{(o)}(s_V))$
04: $c_V = (F_V^{(1)}(s_V), \dots, F_V^{(o)}(s_V)))$
05: $(G, I, J) = (CA^{-1}, CA^{-1}B, [D - CA^{-1}B]^{-1})$
06: **end while**
07: $K = A^{-1}B$
08: $r \leftarrow \{0,1\}^l$
09: $h \leftarrow H(m||r)$
10: $\xi = h - c_V$
11: $s_O = (s_{v+1}, \dots, s_{v+o}) = R^{-1} \cdot \xi$
12: $z = (s_V + T \cdot s_O, s_O)$
13: **return** $\sigma = (z, r)$

MQ-Sign 알고리즘 분석

Pink : Ephemeral Secret
red : Secret
green : Public

Signature			
HAETAE	NCC-Sign	MQ-Sign	AIMer

: 프로파일링 분석 대상
: 비프로파일링 분석 대상

❖ CPA 논리 식별

MQ-Sign: Signature Generation	
Input	$sk = (F, T), m$
Output	σ

01: **while** $\exists A^{-1}, J$
02: $s_V = (s_1, \dots, s_v) \leftarrow GF(2^8)$
03: $R = \begin{pmatrix} A & B \\ C & D \end{pmatrix} = Coeffi(F^{(1)}(s_V), \dots, F^{(o)}(s_V))$
04: $c_V = (F_V^{(1)}(s_V), \dots, F_V^{(o)}(s_V)))$
05: $(G, I, J) = (CA^{-1}, CA^{-1}B, [D - CA^{-1}B]^{-1})$
06: **end while**
07: $K = A^{-1}B$
08: $r \leftarrow \{0,1\}^l$
09: $h \leftarrow H(m||r)$
10: $\xi = h - c_V$
11: $s_O = (s_{v+1}, \dots, s_{v+o}) = R^{-1} \cdot \xi$
12: $z = (s_V + T \cdot s_O, s_O)$
13: **return** $\sigma = (z, r)$

CPA 1
CPA 2

CPA 1

$v = T_{1,1} \cdot s_{v+1}$ in $GF(2^8)$

$T_{1,1} \in GF(2^8)$

2^8개 추측 CPA

CPA ⇒ $T_{1,1} = \alpha$

CPA 2

$v = T_{1,1} \cdot s_{v+1} + T_{1,2} \cdot s_{v+2}$

in $GF(2^8)$

$T_{1,1} = \alpha,\ T_{1,2} \in GF(2^8)$

2^8개 추측 CPA

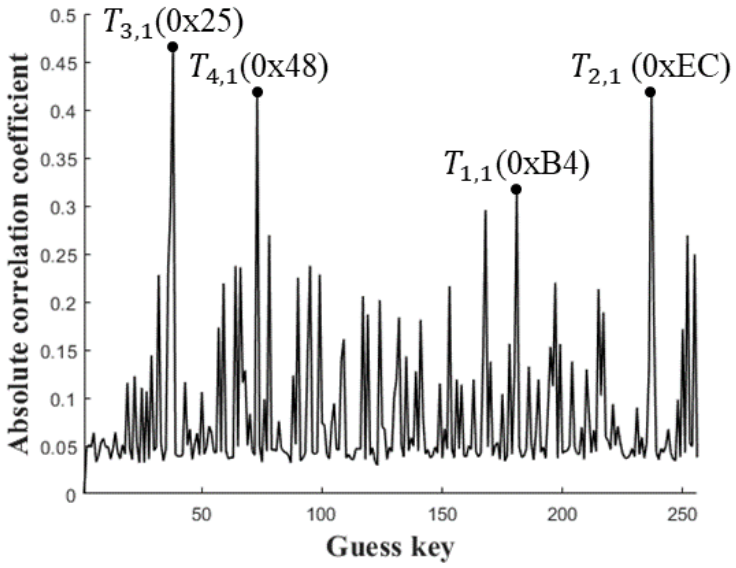
CPA ⇒ $T_{1,2} = \beta$

MQ-Sign CPA 결과

Pink : Ephemeral Secret
red : Secret
green : Public

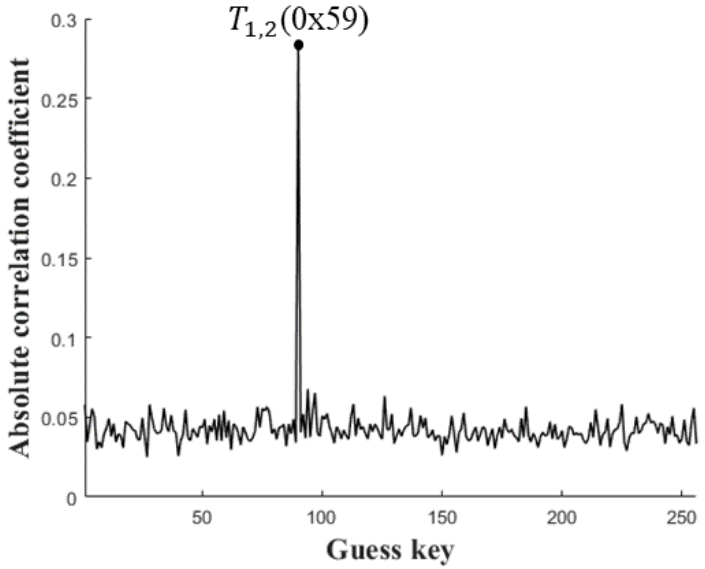
Signature			
HAETAE	NCC-Sign	MQ-Sign	AIMer

❖ **CPA 1)** $T_{1,1} \cdot s_{v+1}$ in $GF(2^8)$



➢ $T_{1,1} = 0$xB4

CPA 2) $T_{1,1} \cdot s_{v+1} + T_{1,2} \cdot s_{v+2}$ in $GF(2^8)$



➢ $T_{1,1}$ 값 고정후 $T_{1,2}$ 값 추측

➢ $T_{1,2} = 0$x59

공격 결과 요약

➢ $T_{1,1}, T_{1,2}$ 16-bit 복구
➔ $T_{1,1} \sim T_{v,o}$ 전체 ➔ 비밀키 행렬 T

AIMer 알고리즘 분석

Pink : Ephemeral Secret
red : Secret
green : Public

Signature			
HAETAE	NCC-Sign	MQ-Sign	AIMer

: 프로파일링 분석 대상

: 비프로파일링 분석 대상

❖ 부채널 분석 대상 위치 식별 (알고리즘)

AIMer: Key Generation	
Input	-
Output	$pk = (iv, ct)$, $sk = (iv, ct, pt)$

1: $pt \leftarrow \{0,1\}^{\lambda}$
2: $iv \leftarrow \{0,1\}^{\lambda}$
3: $ct = \text{AIM2}(iv, pt)$
4: **return** $pk = (iv, ct)$, $sk = pt$

AIMer: Signature Generation	
Input	$sk = (iv, ct, pt), m$
Output	σ

01: //phase 1 ~ 3: secret
02: $t_1 = \text{S}_1(pt + \gamma_1), \dots, t_l = \text{S}_l(pt + \gamma_l), y = pt$
03: $A_{iv}, b_{iv} = \text{Gen_Linear}(iv)$
04: **for** each repetition $k \in [\tau]$ **do**
05: $(a_k^{(1)}, \dots, a_k^{(N)}) \leftarrow GF(2^n)$
06: $(\Delta pt_k,\ pt_k^{(1)}, \dots, pt_k^{(N)}) \leftarrow \text{sharing}(pt)$
07: $c_k = \Sigma_i a_k^{(i)} \cdot pt$
08: $(\Delta c_k,\ c_k^{(1)}, \dots, c_k^{(N)}) \leftarrow \text{sharing}(c_k)$
09: **for** each S-box $j \in [l]$ **do**
10: $(\Delta t_{k,j},\ t_{k,j}^{(1)}, \dots, t_{k,j}^{(N)}) \leftarrow \text{sharing}\ (t_j)$
11: **endfor**
12: **for** each party $i \in [N]$ **do**
13: $\left(x_{k,j}^{(i)}, z_{k,j}^{(i)}\right)_{j\in[l+1]} = \text{AIM2_MPC}\left(A_{iv}, b_{iv}, ct, \left(t_{k,j}^{(i)}\right)_{j\in[l]}\right)$
14: **endfor**
15: **for** each $k \in \{1, \dots, \tau\},\ i \in \{1, \dots, N\}$ **do**
16: $\beta_k^{(i)} = \left(\Sigma_{j=1}^{l+1} \epsilon_{k,j} \cdot x_{k,j}^{(i)}\right) + a_k^{(i)}$
17: $v_k^{(i)} = \left(\Sigma_{j=1}^{l+1} \epsilon_{k,j} \cdot z_{k,j}^{(i)}\right) + \Sigma_i \beta_k^{(i)} \cdot pt_k^{(i)} + c_k^{(i)}$
18: **endfor**
19: **endfor**
20: //phase 4~5: public
21: **return** σ

AIMer 알고리즘 분석

Pink : Ephemeral Secret
red : Secret
green : Public

Signature			
HAETAE	NCC-Sign	MQ-Sign	AIMer

: 프로파일링 분석 대상
: 비프로파일링 분석 대상

❖ CPA 논리 식별

AIMer: Signature Generation

Input	$sk = (iv, ct, pt), m$
Output	σ

01: //phase 1 ~ 3: secret
02: $t_1 = \mathrm{S}_1(pt + \gamma_1), \dots, t_l = \mathrm{S}_l(pt + \gamma_l), y = pt$
03: $A_{iv}, b_{iv} = \mathrm{Gen_Linear}(iv)$
04: **for** each repetition $k \in [\tau]$ **do**
05: $(a_k^{(1)}, \dots, a_k^{(N)}) \leftarrow GF(2^n)$
06: $(\Delta pt_k,\ pt_k^{(1)}, \dots, pt_k^{(N)}) \leftarrow \mathrm{sharing}(pt)$
07: $c_k = \Sigma_i a_k^{(i)} \cdot pt$
08: $(\Delta c_k,\ c_k^{(1)}, \dots, c_k^{(N)}) \leftarrow \mathrm{sharing}(c_k)$
09: **for** each S-box $j \in [l]$ **do**
10: $(\Delta t_{k,j},\ t_{k,j}^{(1)}, \dots, t_{k,j}^{(N)}) \leftarrow \mathrm{sharing}\ (t_j)$
11: **endfor**
12: **for** each party $i \in [N]$ **do**
13: $\left(x_{k,j}^{(i)}, z_{k,j}^{(i)}\right)_{j\in[l+1]} = \mathrm{AIM2_MPC}\left(A_{iv}, b_{iv}, ct, \left(t_{k,j}^{(i)}\right)_{j\in[l]}\right)$
14: **endfor**
15: **for** each $k \in \{1, \dots, \tau\},\ i \in \{1, \dots, N\}$ **do**
16: $\beta_k^{(i)} = \left(\Sigma_{j=1}^{l+1} \epsilon_{k,j} \cdot x_{k,j}^{(i)}\right) + a_k^{(i)}$
17: $v_k^{(i)} = \left(\Sigma_{j=1}^{l+1} \epsilon_{k,j} \cdot z_{k,j}^{(i)}\right) + \Sigma_i \beta_k^{(i)} \cdot pt_k^{(i)} + c_k^{(i)}$
18: **endfor**
19: **endfor**
20: //phase 4~5: public
21: **return** σ

CPA 1

CPA 1

$v = \Delta t_{1,k} + t_1$ in $GF(2^{128})$

$t_1 \in GF(2^{128})$

XOR 이므로 8-bit 분석 가능

2^8개 추측 CPA

CPA ⇒ 8-bit of $t_1 = \alpha_0$ or α_1

CPA 2

CPA 2

$v = \gamma_1 \cdot (\Delta t_{1,k} + \cdots + t_1)$ in $GF(2^{128})$

$t_1 \in GF(2^{128})$

64-bit 단위 곱셈 분석 가능

$2^{64} \rightarrow 2^8$개 추측 CPA

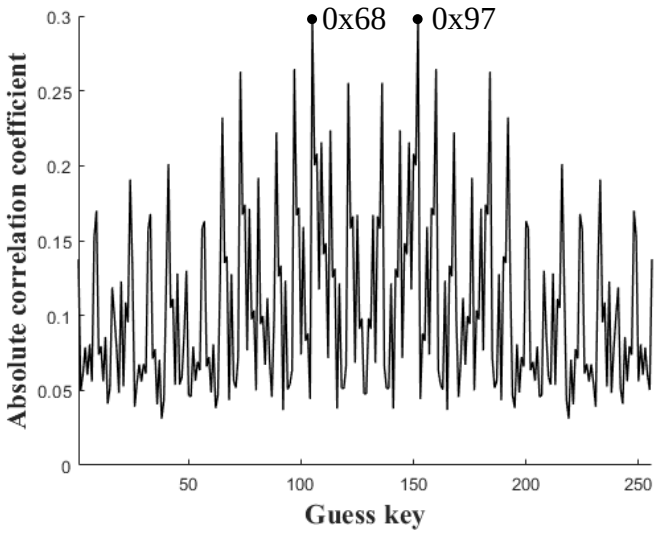
CPA ⇒ 64-bit of $t_1 = \alpha$

AIMer CPA 결과

Pink : Ephemeral Secret
red : Secret
green : Public

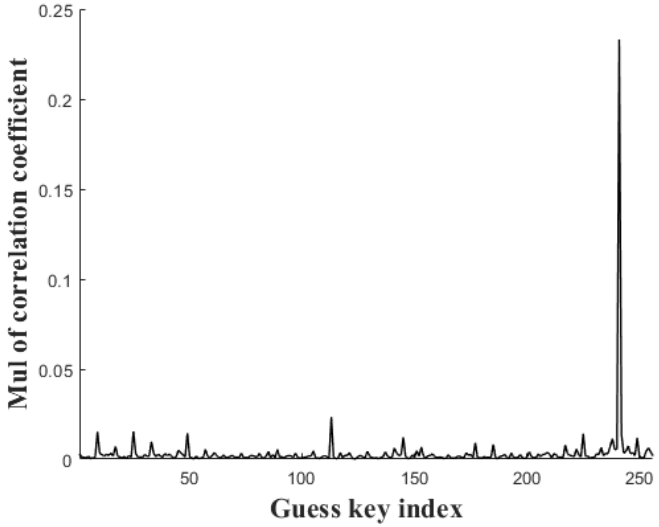
Signature			
HAETAE	NCC-Sign	MQ-Sign	AIMer

❖ **CPA 1)** $\Delta t_{1,k} + t_1$ in $GF(2^{128})$



➢ 8-bit of t_1 = 0x68 or 0x97

CPA 2) $\gamma_1 \cdot (\Delta t_{1,k} + \cdots + t_1)$ in $GF(2^{128})$



➢ 64-bit of t_1 높은 신뢰도로 분석

공격 결과 요약

➢ t_1 64-bit 복구
➔ t_1 전체 ➔ 비밀키 $pt = S_1^{-1}(t_1)$

➡ AIMer 팀에서 대응기법 설계 중

Contents

1 연구 개요

2 국내·외 PQC 알고리즘 부채널 공격 동향

3 KpqC 알고리즘 부채널 분석

3.1 PKE/KEM

3.2 Signature

✓ 4 결론

▣ 결론

- ❖ **PKE/KEM 4종에 대한 부채널 취약점 분석**

- ❖ **PKE/KEM 1종에 대한 단순 전력 분석 수행**
  - ➢ 비밀키의 일부 정보 획득
- ❖ **Signature 4종에 대한 부채널 취약점 분석**

- ❖ **Signature 4종에 대한 상관 전력 분석 수행**
  - ➢ 비밀키 획득

➡ KpqC 알고리즘에 대한 부채널 분석 대응기법 연구 필요

Q & A

References

[SAMOS 2020] Fournaris, A. P., Dimopoulos, C., & Koufopavlou, O. (2020, October). Profiling dilithium digital signature traces for correlation differential side channel attacks. In Embedded Computer Systems: Architectures, Modeling, and Simulation: 20th International Conference, SAMOS 2020, Samos, Greece, July 5–9, 2020, Proceedings (pp. 281-294). Cham: Springer International Publishing.

[IEEE Trans 2020] Kashyap, Priyank, et al. "2deep: Enhancing side-channel attacks on lattice-based key-exchange via 2-d deep learning." IEEE Transactions on Computer-Aided Design of Integrated Circuits

[IEEE ACCESS 2020] Bo-Yeon Sim, Jihoon Kwon, Joohee Lee, Ii-Ju Kim, Tae-Ho Lee, Jaeseung Han, Hyojin Yoon, Jihoon Cho, and Dong-Guk Han, “Single-Trace Attacks on Message Encoding in Lattice-Based KEMs”, IEEE ACCESS, 2020.

[IEEE IoT 2022] Bo-Yeon Sim, Aesun Park, and Dong-Guk Han. "Chosen-ciphertext clustering attack on CRYSTALS-KYBER using the side-channel leakage of Barrett reduction." IEEE Internet of Things Journal 9.21 (2022): 21382-21397.

[IEEE Trans 2021] Xu, Zhuang, et al. "Magnifying side-channel leakage of lattice-based cryptosystems with chosen ciphertexts: The case study of kyber." IEEE Transactions on Computers 71.9 (2021): 2163-2176.

[ACNS 2024] Wang, Ruize, Martin Brisfors, and Elena Dubrova. "A Side-Channel Attack on a Higher-Order Masked CRYSTALS-Kyber Implementation." International Conference on Applied Cryptography and Network Security. Cham: Springer Nature Switzerland, 2024.

[SNCS 2024] Rabas, Tomáš, Jiří Buček, and Róbert Lórencz. "Single-Trace Side-Channel Attacks on NTRU Implementation." SN Computer Science 5.2 (2024): 239.

[CISC-S 2023]$_1$ 이정환, 김규상, 김희석, 홍석희. “KpqC 1**라운드 SMAUG에 대한 개인키 복구 부채널 공격**”, **한국정보보호학회 하계학술대회**, pp. 535-538, 2023.

[CHES 2017] M. Rossi, M. Hamburg, M. Hutter, and M. E. Marson, “A side-channel assisted cryptanalytic attack against qcbits,” in Cryptographic Hardware and Embedded Systems (2017): 3–23.

[TCHES 2022] Guo, Qian, Andreas Johansson, and Thomas Johansson. "A key-recovery side-channel attack on Classic McEliece implementations." IACR Transactions on Cryptographic Hardware and Embedded Systems (2022): 800-827.

[IEEE Trans 2022] Colombier, Brice, et al. "Profiled side-channel attack on cryptosystems based on the binary syndrome decoding problem." IEEE Transactions on Information Forensics and Security 17 (2022): 3407-3420.

[ICISC 2022] Seck, Boly, et al. "Key-recovery by side-channel information on the matrix-vector product in code-based cryptosystems." International Conference on Information Security and Cryptology. Cham: Springer Nature Switzerland, 2022.

[ePrint 2023]$_1$ Colombier, Brice, et al. "Horizontal correlation attack on classic McEliece." Cryptology ePrint Archive (2023).

[AfricaCrypt 2023] Seck, Boly, et al. "A Side-Channel Attack Against Classic McEliece When Loading the Goppa Polynomial." International Conference on Cryptology in Africa. Cham: Springer Nature Switzerland, 2023.

[ePrint 2023]$_2$ Brinkmann, Marcus, et al. "Leaky McEliece: Secret Key Recovery From Highly Erroneous Side-Channel Information." Cryptology ePrint Archive (2023).

[ICEA 2020] Kim, I. J., Lee, T. H., Han, J., Sim, B. Y., & Han, D. G. (2020). Novel single-trace ML profiling attacks on NIST 3 round candidate Dilithium. Cryptology ePrint Archive. and Systems 40.6 (2020): 1217-1229.

References

[HOST 2021] Karabulut, E., Alkim, E., & Aysu, A. (2021, December). Single-trace side-channel attacks on ω-small polynomial sampling: with applications to NTRU, NTRU prime, and crystals-dilithium. In 2021 IEEE International Symposium on Hardware Oriented Security and Trust (HOST) (pp. 35-45). IEEE.

[ICCD 2021] Chen, Z., Karabulut, E., Aysu, A., Ma, Y., & Jing, J. (2021, October). An efficient non-profiled side-channel attack on the CRYSTALS-Dilithium post-quantum signature. In 2021 IEEE 39th International Conference on Computer Design (ICCD) (pp. 583-590). IEEE.

[IEEE ACCESS 2021] Han, J., Lee, T., Kwon, J., Lee, J., Kim, I. J., Cho, J., ... & Sim, B. Y. (2021). Single-trace attack on NIST round 3 candidate Dilithium using machine learning-based profiling. IEEE Access, 9, 166283-166292.

[ePrint 2022] Marzougui, S., Ulitzsch, V., Tibouchi, M., & Seifert, J. P. (2022). Profiling side-channel attacks on dilithium: A small bit-fiddling leak breaks it all. Cryptology ePrint Archive.

[IEEE Trans 2022] Qiao, Z., Liu, Y., Zhou, Y., Ming, J., Jin, C., & Li, H. (2022). Practical Public Template Attack Attacks on CRYSTALS-Dilithium With Randomness Leakages. IEEE Transactions on Information Forensics and Security, 18, 1-14.

[PQCrypto 2023] Steffen, Hauke, et al. "Breaking and protecting the crystal: Side-channel analysis of dilithium in hardware." International Conference on Post-Quantum Cryptography. Cham: Springer Nature Switzerland, 2023.

[TCHES 2023]$_1$ Berzati, Alexandre, et al. "Exploiting intermediate value leakage in dilithium: a template-based approach." IACR Transactions on Cryptographic Hardware and Embedded Systems 2023.4 (2023): 188-210.

[TCHES 2018] Park, Aesun, et al. "Side-channel attacks on post-quantum signature schemes based on multivariate quadratic equations:-rainbow and uov." IACR Transactions on Cryptographic Hardware and Embedded Systems (2018): 500-523.

[DATE 2021] Pokorný, David, Petr Socha, and Martin Novotný. "Side-Channel Attack on Rainbow Post-Quantum Signature. In 2021 Design, Automation & Test in Europe Conference & Exhibition (DATE)." (2021): 565-568.

[TCHES 2023]$_2$ Aulbach, Thomas, et al. "Separating Oil and Vinegar with a Single Trace: Side-Channel Assisted Kipnis-Shamir Attack on UOV." IACR Transactions on Cryptographic Hardware and Embedded Systems 2023.3 (2023): 221-245.

[PQCrypto 2021] Gellersen, Tim, Okan Seker, and Thomas Eisenbarth. "Differential power analysis of the picnic signature scheme." Post-Quantum Cryptography: 12th International Workshop, PQCrypto 2021, Daejeon, South Korea, July 20–22, 2021, Proceedings 12. Springer International Publishing, 2021.

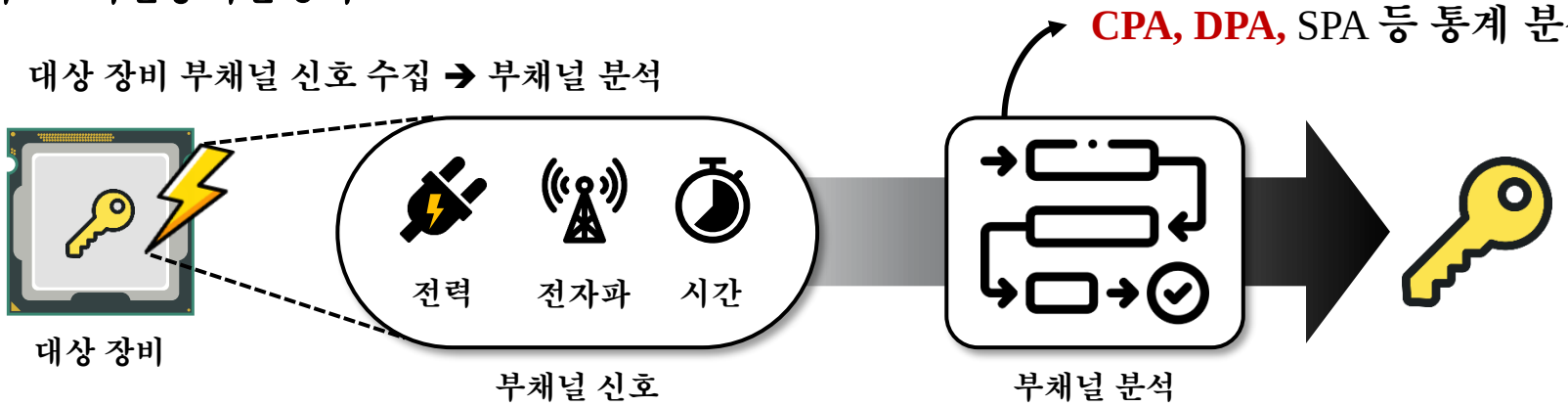
[TCHES 2021] Aranha, Diego F., et al. "Side-channel protections for Picnic signatures." IACR Transactions on Cryptographic Hardware and Embedded Systems (2021): 239-282.

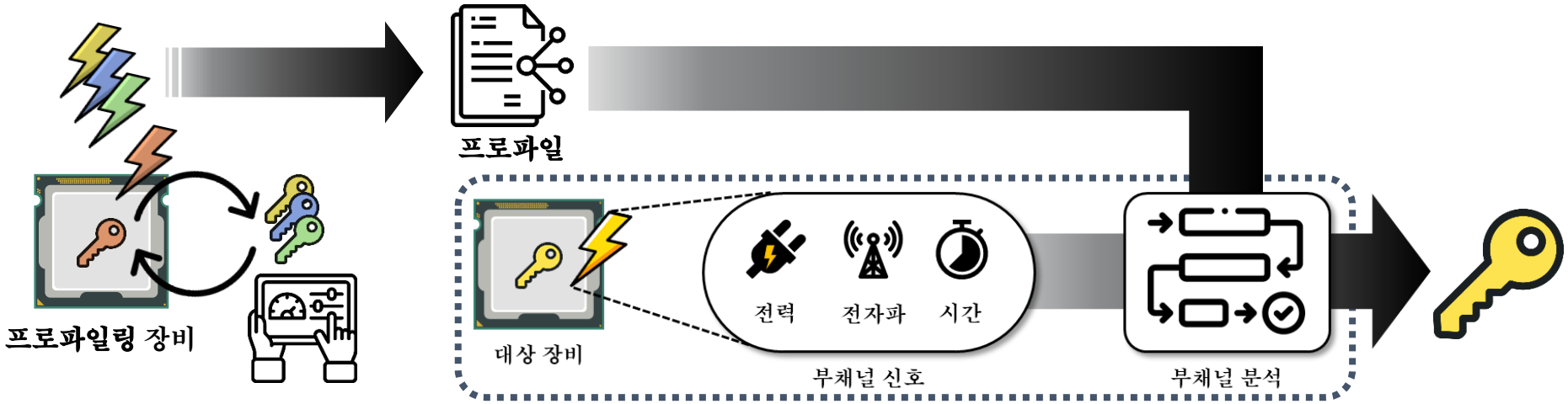
[CISC-S 2023]$_2$ 한재승, 허재원, 이상엽, 권지훈, 한동국. “KpqC **전자서명 후보** AIMer**에 대한 부채널 및 오류주입 공격**”, **한국정보보호학회 하계학술대회**, pp. 119-122, 2023.

▣ 부채널 분석 (SCA, Side Channel Analysis)

❖ 비프로파일링 기반 공격

➢ 대상 장비 부채널 신호 수집 ➔ 부채널 분석



❖ 프로파일링 기반 공격

➢ 제어 가능한 장비로 프로파일링 ➔ 대상 장비 부채널 신호 수집 ➔ 부채널 분석