KpqC 공모전 알고리즘 부채널 안전성 분석기술 연구

고려대학교 인공지능사이버보안학과

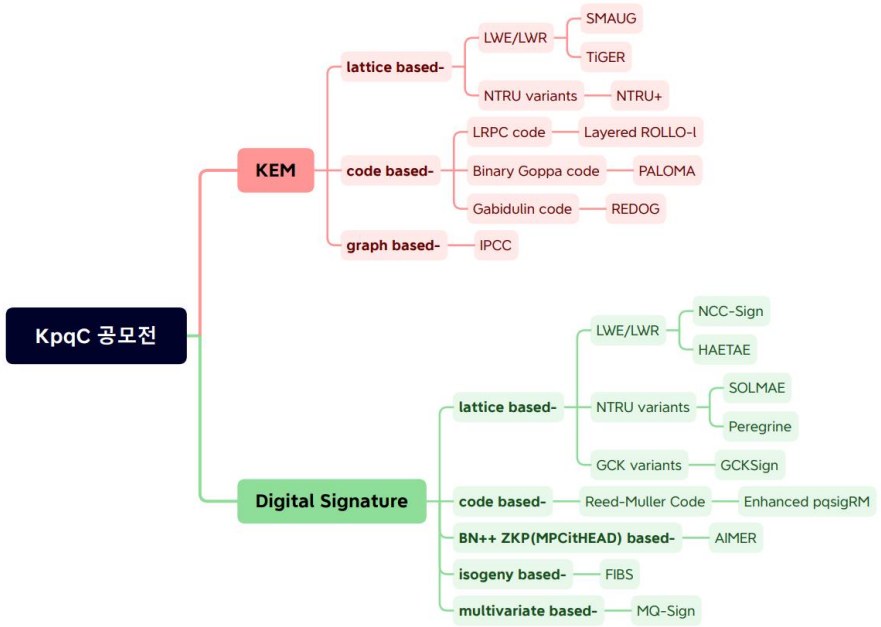
김 희 석

Contents

1. 과제 개요 및 추진 일정

IA&AI SecLab
Implementation Attacks & AI Security Laboratory

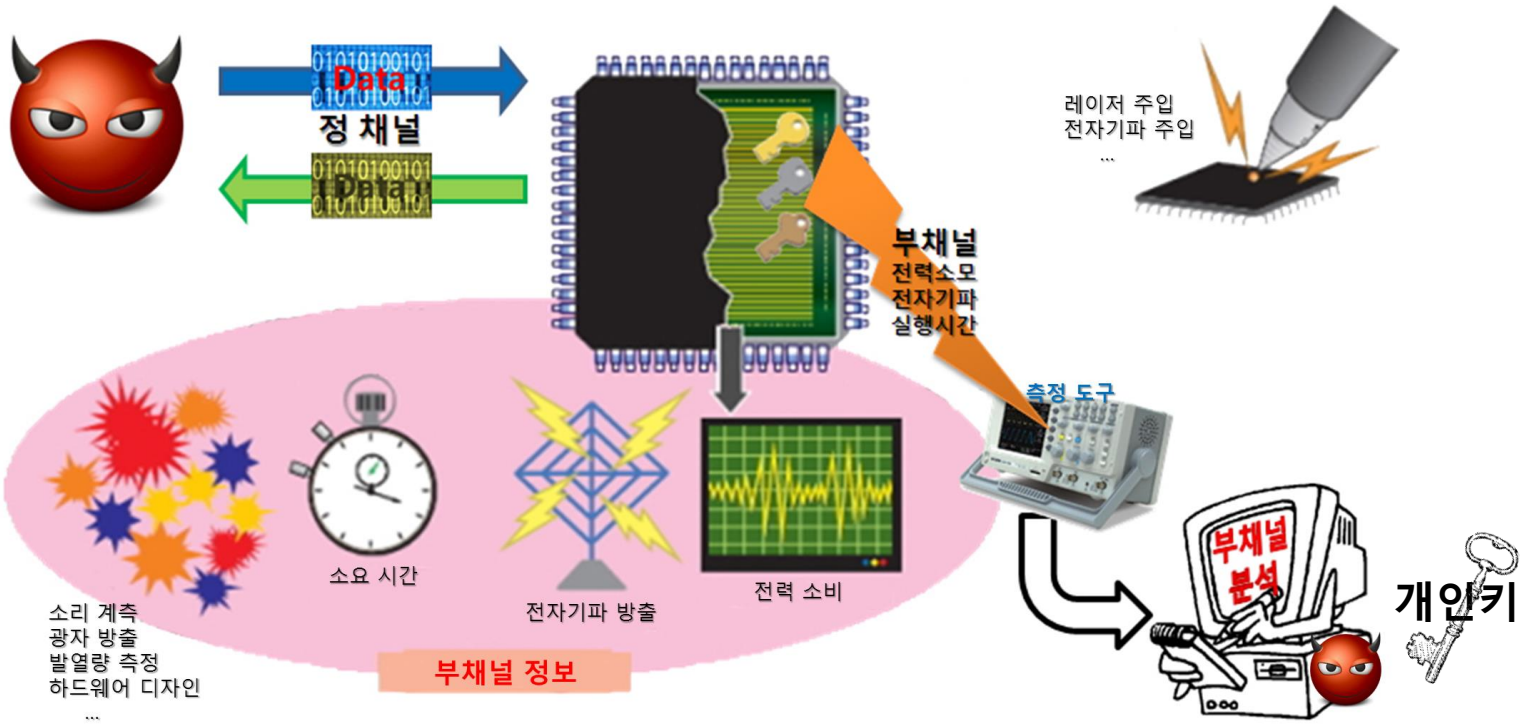
- **과제명**
  - KpqC 공모전 알고리즘 부채널 안전성 분석기술 연구
- **연구 과제 최종 목표**
  - 국내 KpqC 1라운드 공모 알고리즘에 대상 시간차 분석, 전력분석 취약성 연구



연구 내용	추진 일정(월)						
	4	5	6	7	8	9	10
o KpqC 공모전 1라운드 격자 기반 알고리즘에 대한 부채널 분석	→	→	→	→	(6차 워크숍, 완료)		
o KpqC 공모전 1라운드 코드 기반 알고리즘에 대한 부채널 분석	(7차 워크숍)			→	→	→	→
o KpqC 공모전 1라운드 기타 기반 알고리즘에 대한 부채널 분석					→	→	

2. 부채널 분석의 필요성

- **부채널 분석(SCA, Side Channel Analysis)**
  - 암호 알고리즘이 동작할 때 누출되는 전력, 전자파, 시간 등의 **부가적인 정보**를 이용하여 비밀정보를 추출하는 물리적 분석 기법
  - 시간차, 전력, 전자파 등을 이용하여 분석하는 **비침투 공격**과 레이저, 전자기파를 이용하여 오류를 주입하는 **침투 공격**으로 나뉨
  - **새로운 암호 알고리즘**이 제안될 경우 그에 대한 **부채널 분석**을 통한 **안전성 검증**은 **필수적**



2. 부채널 분석의 필요성


무선키보드 (국내)
FPGA 해킹
보안 USB 해킹
Researchers crack KeeLoq RFID technology - Again
by Steve Ragan - Apr 3 2008, 19:39
Tweet
자동차 스마트 키 해킹
Researchers from Ruhr University Bochum, Germany, have cracked the security on keyless entry systems based on KeeLoq RFID technology (IMG:J.Anderson)

2. 부채널 분석의 필요성

진수희 "IC카드 복제 가능...금융사고 위험 노출"

새로운 컴퓨터 프로세서 부채널 공격! RSA 알고리즘이 위험

좋아요 32개 | 입력 : 2018-08-20 10:39

CPU에서 발생하는 자기
RSA 알고리즘 자체의 작

FPGA 하

사파리 통해 애플 칩셋 공략할 수 있는 새로운 부채널 공격 기법 등장

2023-10-27 14:00

가 + 가 -

있는 모든 브라우저도 해당되는 문제

PadOS, 맥OS를 기반으로 하고 있는 시스템에 설치된 A시리즈 및 M시리즈 CPU들을
했다고 한다. 이 공격 기법에는 아이리키지(iLeakage)라는 이름이 붙었다. 사파리 브
약점을 발동시켜 익스플로잇 할 수 있게 되며, 이를 통해 사파리에 저장된 민감한 정
를 꼬드겨 특정 웹사이트로 접속하게 한다면, 피해자의 지메일이나 크리덴셜 등을 훔

ARTIFICIAL INTELLIGENCE

AI Helps Crack NIST-Recommended Post-Quantum Encryption Algorithm

The CRYSTALS-Kyber public-key encryption and key encapsulation mechanism recommended by NIST for post-quantum cryptography has been broken using AI combined with side channel attacks.

By Kevin Townsend
February 21, 2023

TRENDING

1. Okta Hack Blamed on Employee Using Personal Google Account on Company Laptop
2. Mortgage Giant Mr. Cooper Shuts Down Systems Following Cyberattack
3. Cyberattack Disrupts Ace Hardware's Operations
4. Atlassian Issues Second Warning on Potential Exploitation of Critical Confluence Flaw
5. Cisco Finds Second Zero-Day as Number of Hacked Devices Apparently Drops
6. In Other News: Airport Taxi Hacking, Post-Quantum Crypto Guidance, Stanford Breach
7. 'Looney Tunables' Glibc Vulnerability Exploited in Cloud Attacks
8. Industry Reactions to SEC Charging SolarWinds and Its CISO: Feedback Friday

The **CRYSTALS-Kyber** public-key encryption and key encapsulation mechanism recommended by NIST in July 2022 for post-quantum cryptography has been broken. Researchers from the KTH Royal Institute of Technology, Stockholm, Sweden, used recursive training AI combined with side channel attacks.

2. 부채널 분석의 필요성

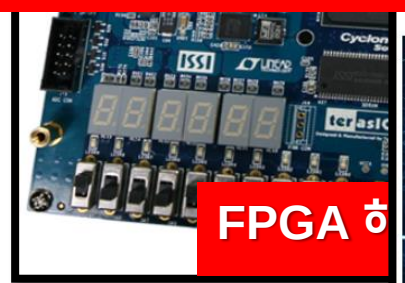
진수희 "IC카드 복제 가능...금융사고 위험 노출"

새로운 컴퓨터 프로세서 부채널 공격! RSA 알고리즘이 위험

좋아요 32개 | 입력 : 2018-08-20 10:39

사파리 통해 애플 칩셋 공략할 수 있는 새로운 부채널 공격 기법 등장

새로운 암호 알고리즘 및 보안 시스템에 대한 부채널 안정성 검증 필요



FPGA 하

The **CRYSTALS-Kyber** public-key encryption and key encapsulation mechanism recommended by NIST in July 2022 for post-quantum cryptography has been broken. Researchers from the KTH Royal Institute of Technology, Stockholm, Sweden, used recursive training AI combined with side channel attacks.

TRENDING

1. Okta Hack Blamed on Employee Using Personal Google Account on Company Laptop
2. Mortgage Giant Mr. Cooper Shuts Down Systems Following Cyberattack
3. Cyberattack Disrupts Ace Hardware's Operations
4. Atlassian Issues Second Warning on Potential Exploitation of Critical Confluence Flaw
5. Cisco Finds Second Zero-Day as Number of Hacked Devices Apparently Drops
6. In Other News: Airport Taxi Hacking, Post-Quantum Crypto Guidance, Stanford Breach
7. 'Looney Tunables' Glibc Vulnerability Exploited in Cloud Attacks
8. Industry Reactions to SEC Charging SolarWinds and Its CISO: Feedback Friday

있는 모든 브라우저도 해당되는 문제

PadOS, 맥OS를 기반으로 하고 있는 시스템에 설치된 A시리즈 및 M시리즈 CPU들을
했다고 한다. 이 공격 기법에는 아이리키지(iLeakage)라는 이름이 붙었다. 사파리 브
약점을 발동시켜 익스플로잇 할 수 있게 되며, 이를 통해 사파리에 저장된 민감한 정
를 꼬드겨 특정 웹사이트로 접속하게 한다면, 피해자의 지메일이나 크리덴셜 등을 훔

2. 부채널 분석의 필요성

- **양자내성암호와 부채널 분석 – 미국 국립표준기술연구소(NIST) pqc 표준화 작업**
  - 2016년, PQCrypto 컨퍼런스에서 NIST가 양자내성암호에 대한 미국 연방 표준 사업 계획을 발표
  - 현재 표준화 대상 KEM 1종, 전자서명 3종 선정, 추가적으로 KEM 4종에 대해 4라운드 진행중
  - NIST는 표준화 작업 시작부터 **선정 기준**으로 **부채널 공격 저항성**을 제시함

NIST에서 공표한 pqc 선정 기준 프레젠테이션

THE SELECTION CRITERIA

- Security - against both classical and quantum attacks
- Performance - measured on various "classical" platforms
- Other properties
  - Drop-in replacements - Compatibility with existing protocols and networks
  - Perfect forward secrecy
  - Resistance to side-channel attacks
  - Simplicity and flexibility
  - Misuse resistance, and
  - More

NIST에서 공표한 pqc 평가 기준 문서

Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process

Submitters can try to meet the requirements of categories 4 or 5, or they can specify some other level of security that demonstrates the ability of their cryptosystem to scale up beyond category 3.

4.A.6 Additional Security Properties While the previously listed security definitions cover many of the attack scenarios that will be used in the evaluation of the submitted algorithms, there are several other properties that would be desirable:

One such property is perfect forward secrecy.[7] While this property can be obtained through the use of standard encryption and signature functionalities, the cost of doing so may be prohibitive in some cases. In particular, public-key encryption schemes with a slow key generation algorithm, such as RSA, are typically considered unsuitable for perfect forward secrecy. This is a case where there is significant interaction between the cost, and the practical security, of an algorithm.

Another case where security and performance interact is resistance to side-channel attacks. Schemes that can be made resistant to side-channel attack at minimal cost are more desirable than those whose performance is severely hampered by any attempt to resist side-channel attacks. We further note that optimized implementations that address side-channel attacks (e.g., constant-time implementations) are more meaningful than those which do not.

A third desirable property is resistance to multi-key attacks. Ideally an attacker should not gain an advantage by attacking multiple keys at once, whether the attacker's goal is to compromise a single key pair, or to compromise a large number of keys.

2. 부채널 분석의 필요성

- **양자내성암호와 부채널 분석 – 미국 국립표준기술연구소(NIST) pqc 표준화 작업**
  - 2016년, PQCrypto 컨퍼런스에서 NIST가 양자내성암호에 대한 미국 연방 표준 사업 계획을 발표
  - 현재 표준화 대상 KEM 1종, 전자서명 3종 선정, 추가적으로 KEM 4종에 대해 4라운드 진행중
  - NIST는 표준화 작업 시작부터 **선정 기준**으로 **부채널 공격 저항성**을 제시함

NIST에서 공표한 pqc 선정 기준 프레젠테이션

THE SELECTION CRITERIA

- Security - against both classical and quantum attacks
- Performance - measured on various "classical" platforms
- Other properties
  - Drop-in replacements - Compat
  - Perfect forward secrecy
  - Resistance to side-channel attacks
  - Simplicity and flexibility
  - Misuse resistance, and
  - More

특히, **constant-time 구현**을 언급하며 **시간분석**에 대한 **저항성**을 역설함

NIST에서 공표한 pqc 평가 기준 문서

Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process

Submitters can try to meet the requirements of categories 4 or 5, or they can specify some other level of security that demonstrates the ability of their cryptosystem to scale up beyond category 3.

4.A.6 Additional Security Properties While the previously listed security definitions cover many of the attack scenarios that will be used in the evaluation of the submitted algorithms, there are several other properties that would be desirable:

One such property is perfect forward secrecy.[7] While this property can be obtained through the use of standard encryption and signature functionalities, the cost of doing so may be prohibitive in some cases. In particular, public-key encryption schemes with a slow key generation algorithm, such as RSA, are typically considered unsuitable for perfect forward secrecy. This is a case where there is significant interaction between the cost, and the practical security, of an algorithm.

Another case where security and performance interact is resistance to side-channel attacks. Schemes that can be made resistant to side-channel attack at minimal cost are more desirable than those whose performance is severely hampered by any attempt to resist side-channel attacks. We further note that optimized implementations that address side-channel attacks (e.g., constant-time implementations) are more meaningful than those which do not.

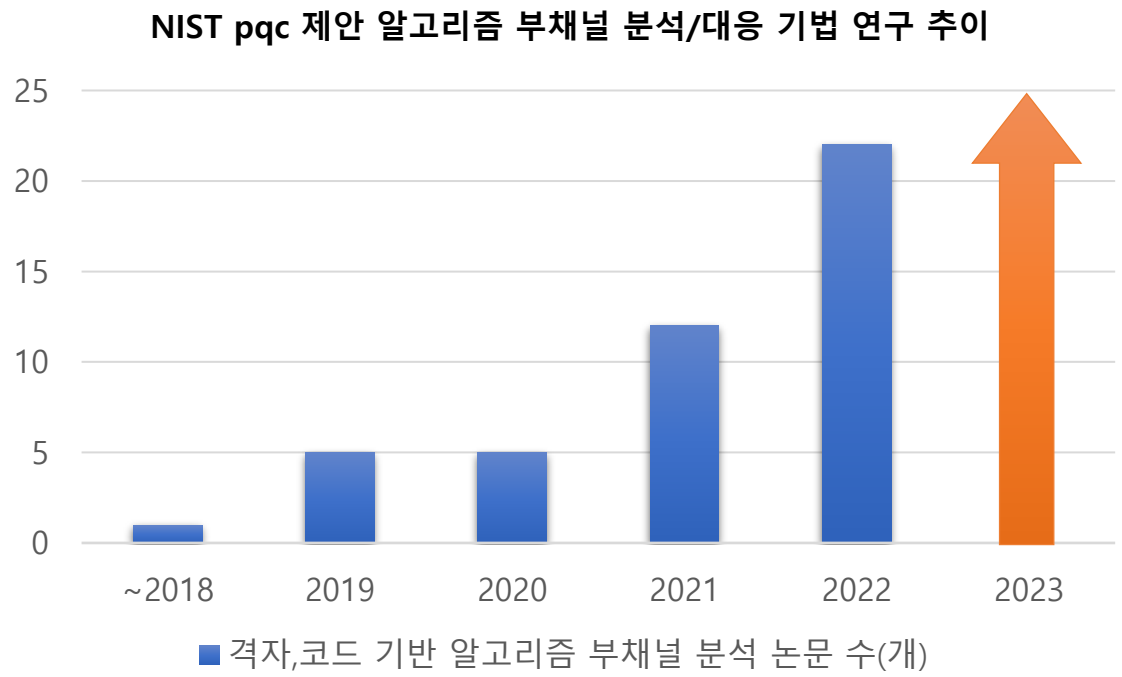
A third desirable property is resistance to multi-key attacks. Ideally an attacker should not gain an advantage by attacking multiple keys at once, whether the attacker's goal is to compromise a single key pair, or to compromise a large number of keys.

2. 부채널 분석의 필요성

- **양자내성암호와 부채널 분석 – 미국 국립표준기술연구소(NIST) pqc 표준화 작업**
  - 아래는 주요 기반 문제인 격자 기반과 코드 기반에 대한 부채널 분석/대응 기법 연구를 나타낸 표와 그래프임
  - NIST pqc 제안 알고리즘에 대한 부채널 분석/대응 기법 연구는 **해마다 증가**하고 있음
  - 2022 표준화 알고리즘 선정 및 4라운드 추가 진행됨에 따라 pqc 부채널 분석/대응 기법 연구는 **지속적으로 증가**될 예정
  - 이는 **KpqC** 제안 알고리즘에 대한 **부채널 분석/대응 연구의 필요성**을 시사함

연도	격자 기반	코드 기반	계
~2018	1,3,31,36,40,55,59	23	**8**
2019	14,39,44,47	52	**5**
2020	6,29,51,60	30	**4**
2021	2,7,9,10,24,34,38,43,58	12,13,45	**12**
2022	4,5,11,15,17,26,32,33,35, 37,42,50,53,54,57	16,18,19,20,21,46,48	**22**
~2023 10월	8,22,25,27,28,49,56,41, …	…	**???**

*** 참고문헌의 번호로 적혀있음**
**** 표준화 대상 또는 Round4 알고리즘에 대한 직접적인 부채널 분석만 조사함**

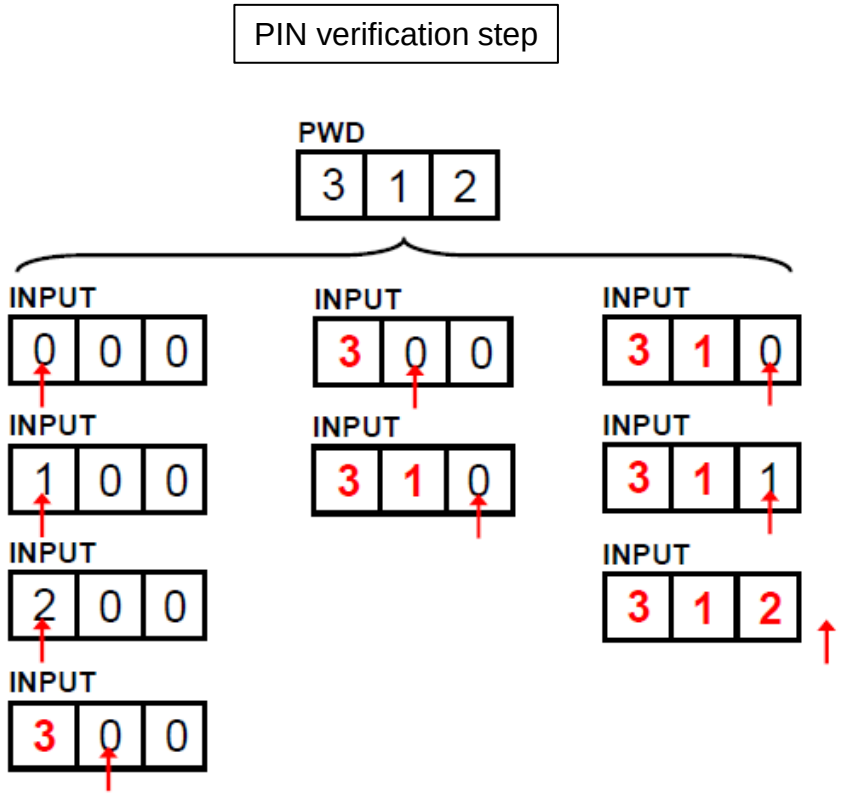


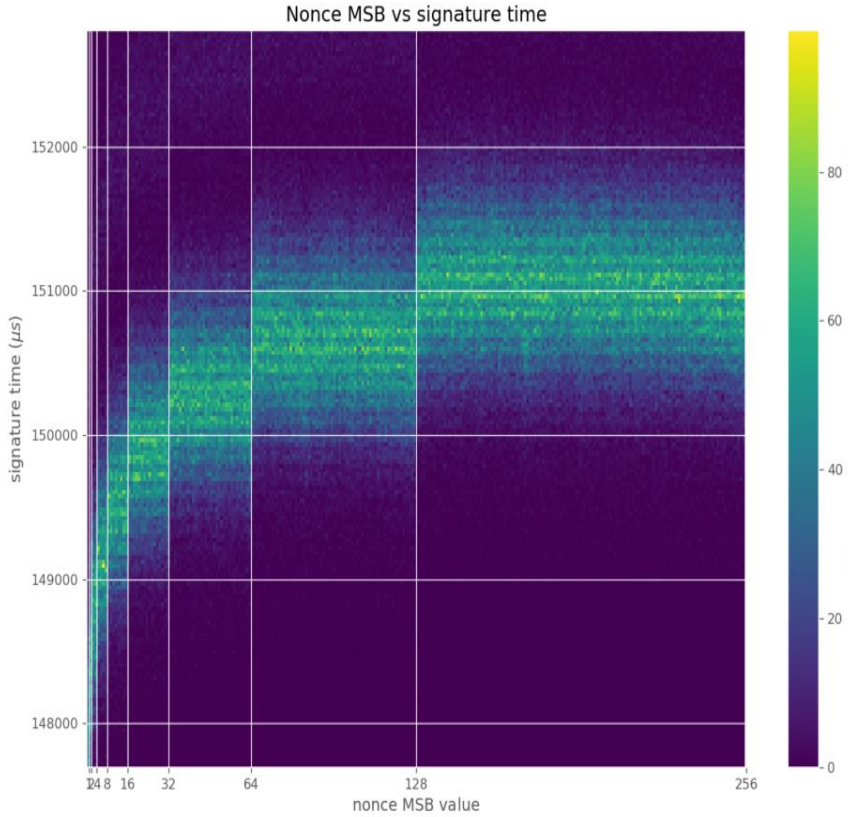
3. KpqC 알고리즘에 대한 부채널 분석

IA&AI SecLab
Implementation Attacks & AI Security Laboratory

- **부채널 취약점 – 동작 시간 차이**
  - 비밀정보와 연관된 데이터에 따라 암호의 **동작 시간의 차이**가 발생하는 경우
  - 부채널 분석에 대한 고려 없이 코딩을 하는 경우, 심각한 취약점 발생
  - 코드 작성 시, 분기문 없이 알고리즘을 구현하는 **Constant-time 구현**을 통해 대응 가능

```
for i = 0 to 2
    if (INPUT[i] ≠ PWD[i])
        return("REJECT")

return("ACCEPT")
```





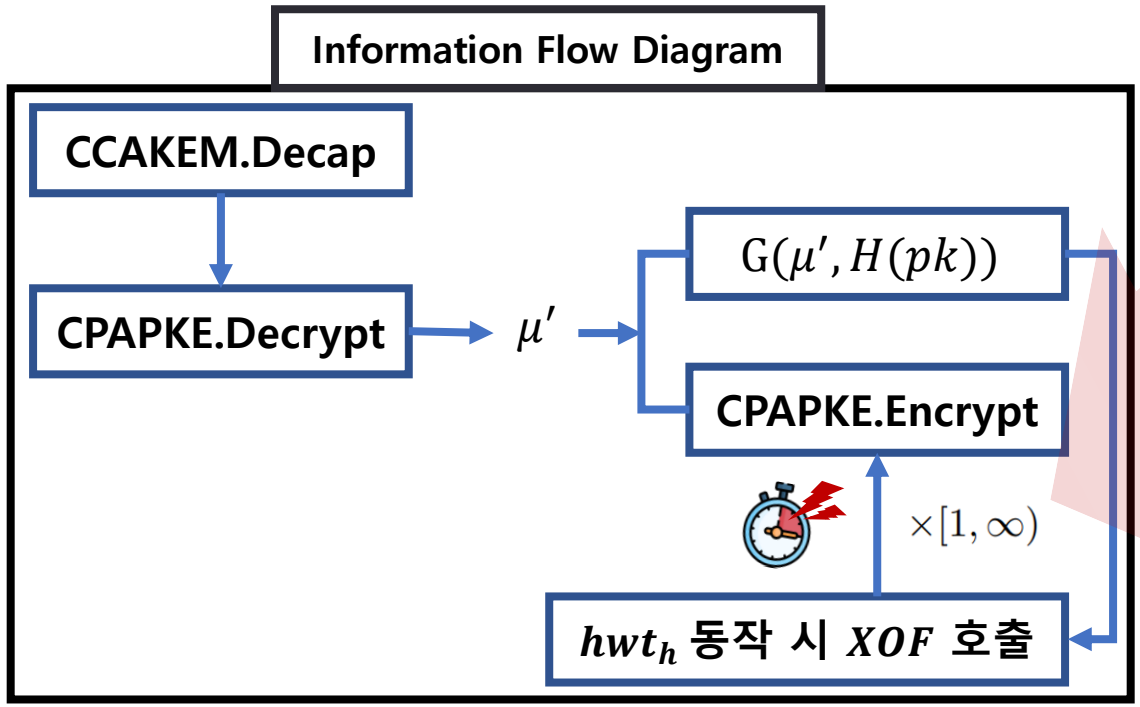
3. KpqC 알고리즘에 대한 부채널 분석

- **부채널 취약점 – 동작 시간 차이**
  - **예시 : SMAUG, TiGER 디캡슐화 과정**
    - hwt_h 함수에 대한 동작 시간 취약점
      - 재암호화 과정 중 hwt_h 함수는 임시키 r 생성을 위한 함수
      - $seed_r$에 따라 hwt_h 의 $XOF(shake256)$ 호출 횟수 차이 → 동작 시간 차이
      - 해당 부채널 정보를 통해 **선택 암호문 환경**에서 **개인키 복구** 가능[21][44][48]

Algorithm 2 SMAUG.PKE.Enc: encryption

Enc(pk, μ; $\text{seed}_\mathbf{r}$): ▷ pk = $(\text{seed}_\mathbf{A}, \mathbf{b})$, $\mu \in \mathcal{R}_t$

1: $\mathbf{A} = \text{expandA}(\text{seed}_\mathbf{A})$
2: **if** $\text{seed}_\mathbf{r}$ is not given **then** $\text{seed}_\mathbf{r} \leftarrow \{0,1\}^{256}$
3: $\mathbf{r} \leftarrow \text{HWT}_{h_r}(\text{seed}_\mathbf{r}) \in S_n^k$ **seed r = $G(\mu', H(pk))$**
4: $\mathbf{c}_1 = \lfloor p/q \cdot \mathbf{A} \cdot \mathbf{r} \rceil \in \mathcal{R}_p^k$
5: $c_2 = \lfloor p'/q \cdot \langle \mathbf{b}, \mathbf{r} \rangle + p'/t \cdot \mu \rceil \in \mathcal{R}_{p'}$
6: **return** $\text{ct} = (\mathbf{c}_1, c_2)$

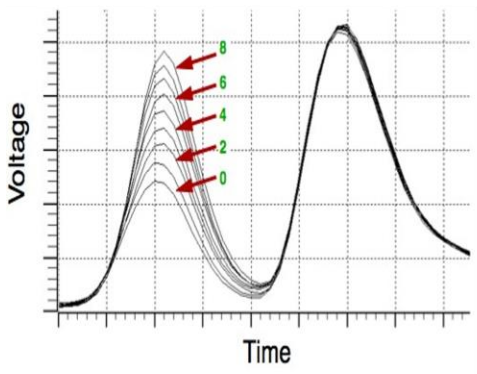


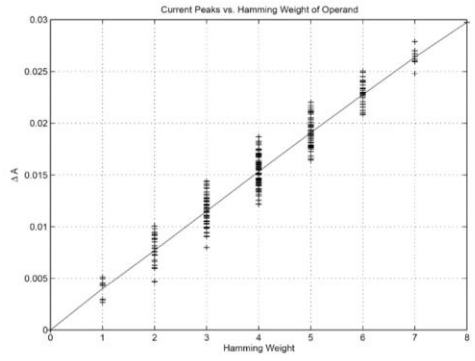

```
void hwt(uint8_t *res, uint8_t *cnt_arr, const uint8_t *input,
         const size_t input_size, const uint16_t hmwt) {

    ...

    for (i = 0; i < DIMENSION; ++i)
        res[i] = 0;

    for (i = DIMENSION - hmwt; i < DIMENSION; ++i) {
        do {
            if (pos >= SHAKE256_RATE / 2) {
                shake256_squeezeblocks((uint8_t *)buf, 1, &state);
                pos = 0;
            }

            deg = buf[pos++] & deg_mask;
        } while (deg > i);                    난수 충전 위한 XOF 추가 호출

        res[i] = res[deg];
        res[deg] = ((buf[pos - 1] >> 14) & 0x02) - 1;
    }

    ...

}
```

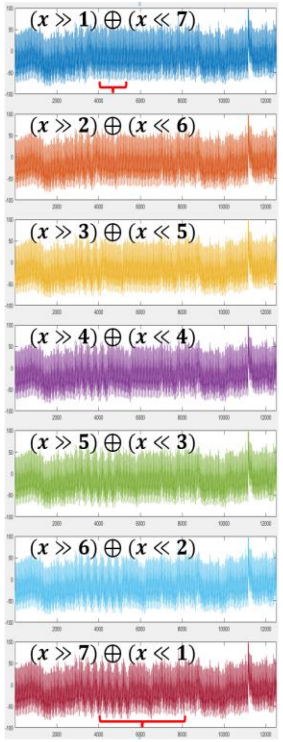
3. KpqC 알고리즘에 대한 부채널 분석

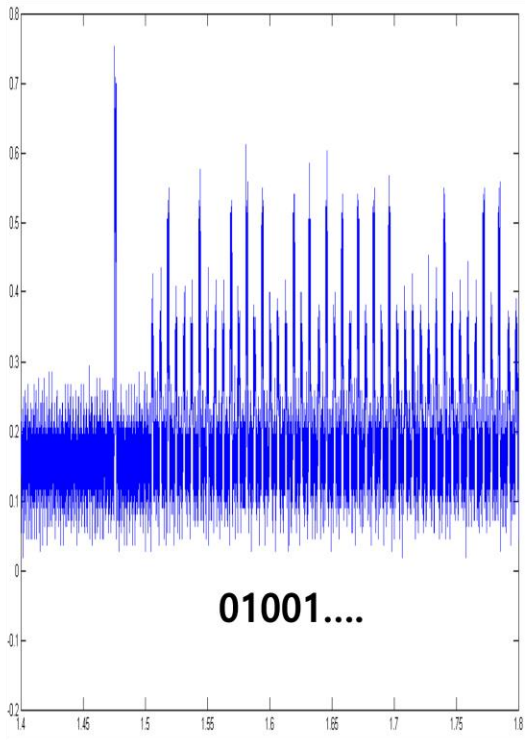
IA&AI SecLab
Implementation Attacks & AI Security Laboratory

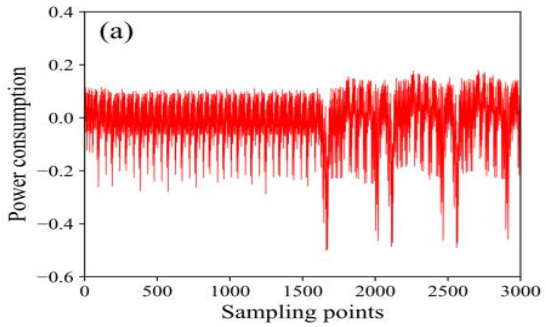
- **부채널 취약점 – 전력/전자파 소비량**
  - 장비 내부에서 연산되는 데이터 값, 연산코드 값에 의존해 전력/전자파 소비
  - 일반적으로 전력/전자파 소비가 데이터의 **해밍웨이트**에 비례한다는 관계를 이용하여 비밀정보를 복원하는 공격 기법
  - 난수값을 통해 비밀정보를 분할하여 연산하는 **마스킹 기법**을 통해 대응 가능

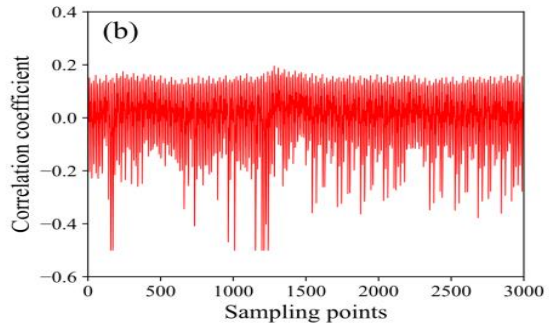




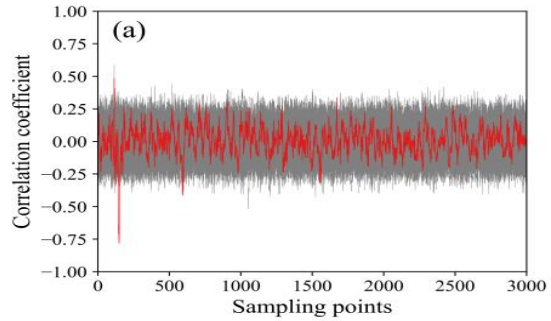


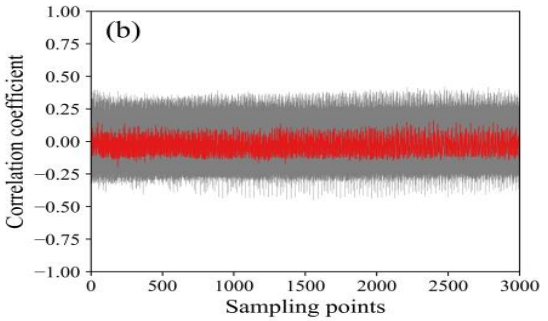






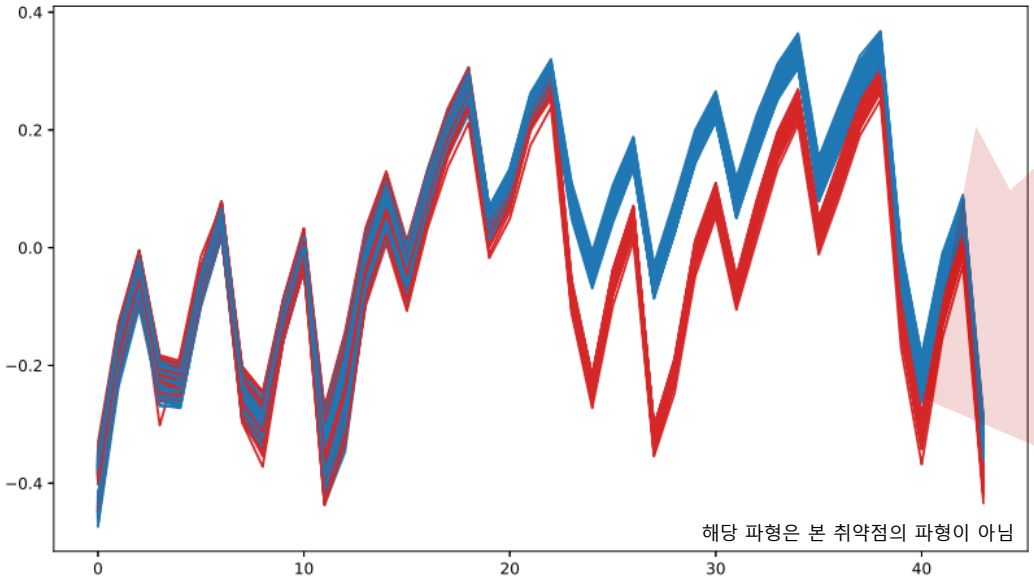
(a) 마스킹 기법 적용 전 AES, (b) 적용 후 AES





3. KpqC 알고리즘에 대한 부채널 분석

- **부채널 취약점 – 전력/전자파 소비량**
  - **예시 : NTRU+ 디캡슐화 과정**
    - ***crepmod3*** 함수에 대한 단순전력분석
      - 메시지 복호화 연산 중 $mod^{\pm}3$ 감산을 위한 함수
      - 복호화된 메시지는 $\{-1,0,1\}$을 계수로 가짐
      - **전력/전자파 상**으로 큰 HW 가진 **{-1}**과 작은 HW을 가진 **{0, 1}**으로 **구분됨**
      - 해당 부채널 정보를 활용하여 **디캡슐화 과정**에서 **메시지 일부 복구** 가능 개인키 복구 시나리오 존재 가능[64]



Algorithm 10 $\mathsf{Decap}(sk, c)$: decapsulation

Require: Secret key $sk \in \mathcal{B}^{\lceil \log_2 q \rceil \cdot n/4}$
Require: Ciphertext $c \in \mathcal{B}^{\lceil \log_2 q \rceil \cdot n/8}$
Ensure: Shared key $m \in \mathcal{B}^{32}$

1: $\hat{\mathbf{f}} = \mathsf{Decode}_q(sk)$
2: $\hat{\mathbf{c}} = \mathsf{Decode}_q(c)$
3: $\hat{\mathbf{h}}^{-1} = \mathsf{Decode}_q(sk + \lceil \log_2 q \rceil \cdot n/8)$
4: $\mathbf{m} = \mathsf{NTT}^{-1}(\hat{\mathbf{c}} \circ \hat{\mathbf{f}}) \mod^{\pm} 3$
5: $\hat{\mathbf{m}} = \mathsf{NTT}(\mathbf{m})$
6: $\hat{\mathbf{r}} = (\hat{\mathbf{c}} - \hat{\mathbf{m}}) \circ \hat{\mathbf{h}}^{-1}$
7: $m := \mathsf{Inv}(\mathbf{m}, \mathsf{G}(\mathsf{Encode}_q(\hat{\mathbf{r}})))$
8: $(K, \mathbf{r}) := \mathsf{H}(m)$
9: **if** $\mathbf{r} = \mathbf{r}'$
10: **return** K
11: **else**
12: **return** $\perp$

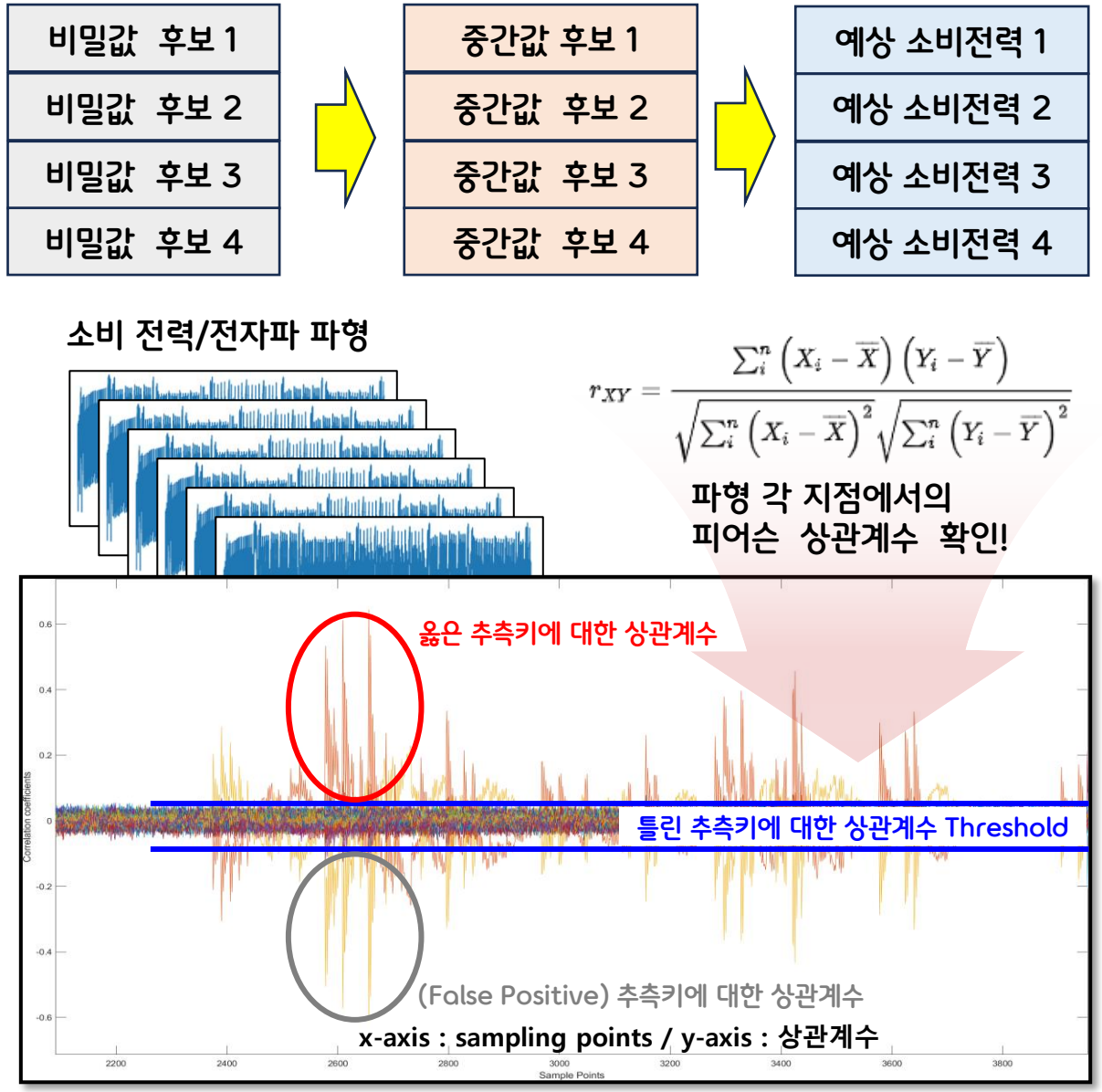
복호화된 메시지

```
static int16_t crepmod3(int16_t a) {
  a += (a >> 15) & NTRUPLUS_Q;
  a -= (NTRUPLUS_Q-1)/2;
  a += (a >> 15) & NTRUPLUS_Q;
  a -= (NTRUPLUS_Q+1)/2;

  a  = (a >> 8) + (a & 255);
  a  = (a >> 4) + (a & 15);
  a  = (a >> 2) + (a & 3);
  a  = (a >> 2) + (a & 3);
  a -= 3;
  a += ((a + 1) >> 15) & 3;   {-1, 0, 1}
  return a;
}
```

3. KpqC 알고리즘에 대한 부채널 분석

IA&AI SecLab
Implementation Attacks & AI Security Laboratory

- **부채널 취약점 – 전력/전자파 소비량**
  - **상관전력분석 (Correlation Power Analysis : CPA)**
    - 단순하면서도 강력한 효과적인 부채널 분석 방법
    - 공격 환경
      - 공격자가 암호문(또는 평문)을 암호 오라클에 입력할 수 있고 그에 대한 전력/전자파 파형을 수집할 수 있음
      - 오라클 동작 시 사용되는 개인키는 고정
    - 공격 방법
      ① 공격자는 암호 오라클에 입력할 암호문(또는 평문)을 다수 구성
      ② 암호문(또는 평문)을 입력하여 그에 대한 동작 전력/전자파 파형 수집
      ③ 개인키 일부를 추측하여 암호문(또는 평문)과 계산한 중간값의 해밍웨이트와 파형 간의 상관계수를 연산
      ④ 상관계수가 높게 나온 추측 개인키를 실제 개인키로 판단



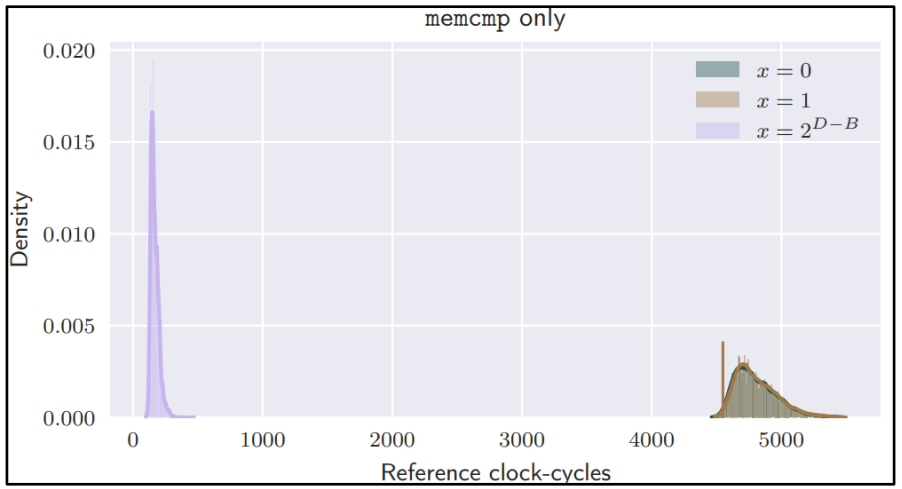
3. KpqC 알고리즘에 대한 부채널 분석

- **부채널 취약점 – <u>라이브러리 함수</u> 사용에 대하여**
  - 암호 구현 시, **라이브러리 함수**를 사용하면 **예상하지 못한 취약점 발생** 가능, 이에 대한 **대응 및 최적화**가 **어려움**.
    - **직접 구현**하여 취약점 대응 및 최적화하여야 함
  - 라이브러리 함수 취약점 예시
    - memcmp
      - 동작 시간 차이 취약점
        - memcmp가 입력된 두 배열을 비교할 때 동작 시간 차이 발생
        - 두 배열이 모두 같다면 동작 시간 상대적 느림
        - 두 배열이 다르다면 동작 시간 상대적 빠름
      - Guo, Q 등에 의해 memcmp를 통한 FrodoKEM 개인키 복구 시나리오가 제안됨[65]

A key-recovery timing attack on post-quantum primitives using the Fujisaki-Okamoto transformation and its application on FrodoKEM

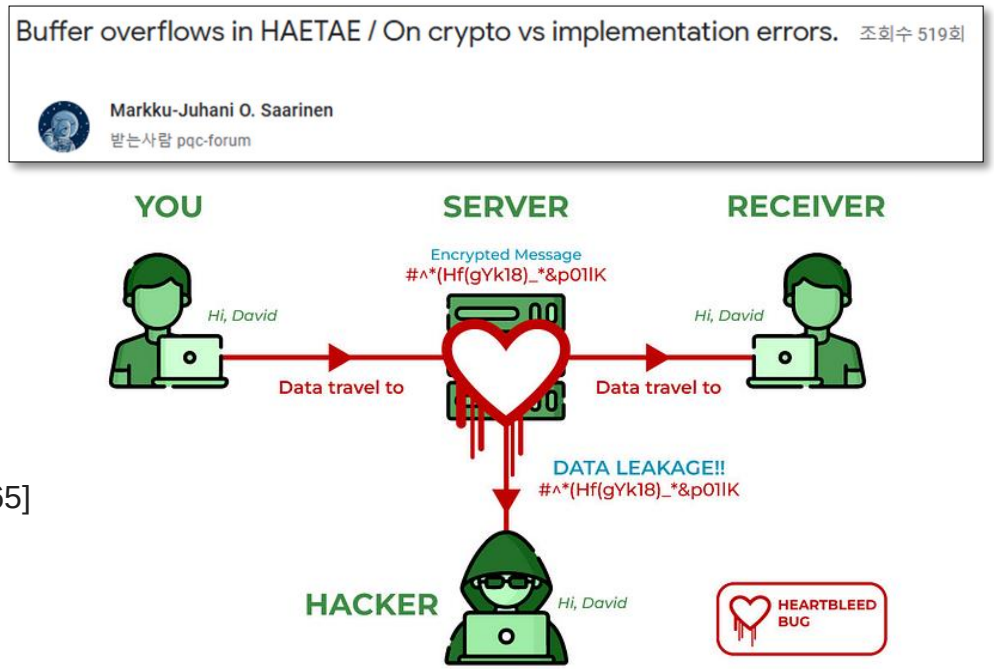
Qian Guo[1,2], Thomas Johansson[1], and Alexander Nilsson[1,3]

[1] Dept. of Electrical and Information Technology, Lund University, Lund, Sweden
{qian.guo,thomas.johansson,alexander.nilsson}@eit.lth.se
[2] Selmer Center, Department of Informatics, University of Bergen, Bergen, Norway
[3] Advenica AB, Malmö, Sweden



3. KpqC 알고리즘에 대한 부채널 분석

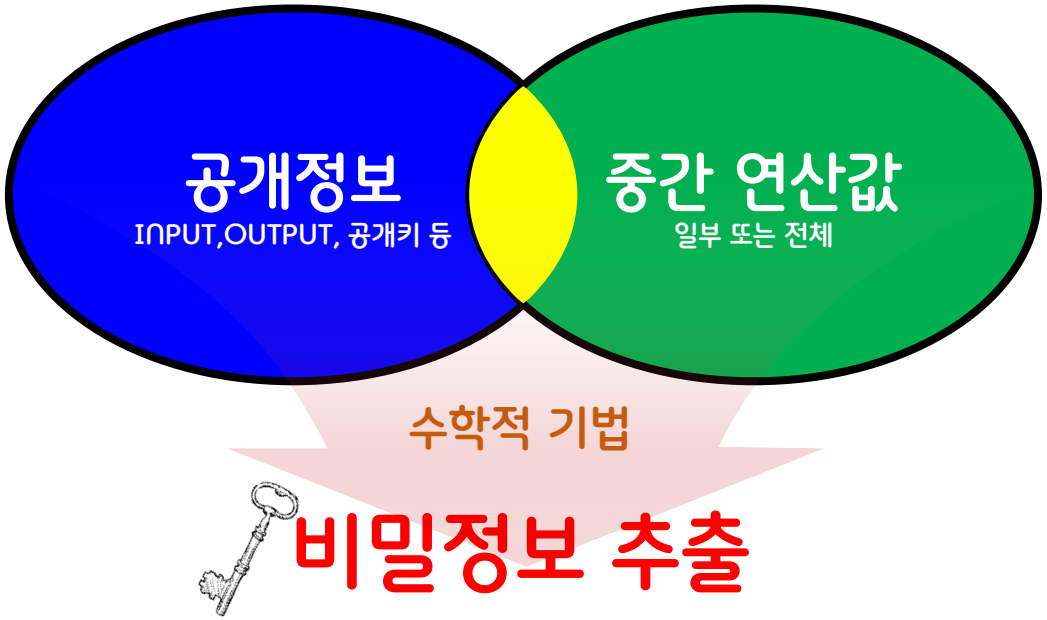
- **부채널 취약점 – <u>라이브러리 함수</u> 사용에 대하여**
  - 암호 구현 시, **라이브러리 함수**를 사용하면 **예상하지 못한 취약점 발생** 가능, 이에 대한 **대응 및 최적화**가 **어려움**.
    - **직접 구현**하여 취약점 대응 및 최적화하여야 함
  - 라이브러리 함수 취약점 예시
    - memcmp
      - 동작 시간 차이 취약점
        - memcmp가 입력된 두 배열을 비교할 때 동작 시간 차이 발생
        - 두 배열이 모두 같다면 동작 시간 상대적 느림
        - 두 배열이 다르다면 동작 시간 상대적 빠름
      - Guo, Q 등에 의해 memcmp를 통한 FrodoKEM 개인키 복구 시나리오가 제안됨[65]
    - memcpy
      - Heartbleed vulnerability
        1. memcpy(Destination, Source, Source_length)는 Source로부터 Destination에 Source_length 크기만큼 복사
        2. **공격자**가 **Source_length**에 **접근 가능하다면** Source 크기보다 큰 Source_length 입력 가능
        3. 함수는 Stack에 있는 **Source 버퍼 외에 정보**까지 포함하여 **Destination**에 **복사**
      - Markku-Juhani O. Saarinen에 의해 HAETAE의 Heartbleed 취약점 보고됨



3. KpqC 알고리즘에 대한 부채널 분석

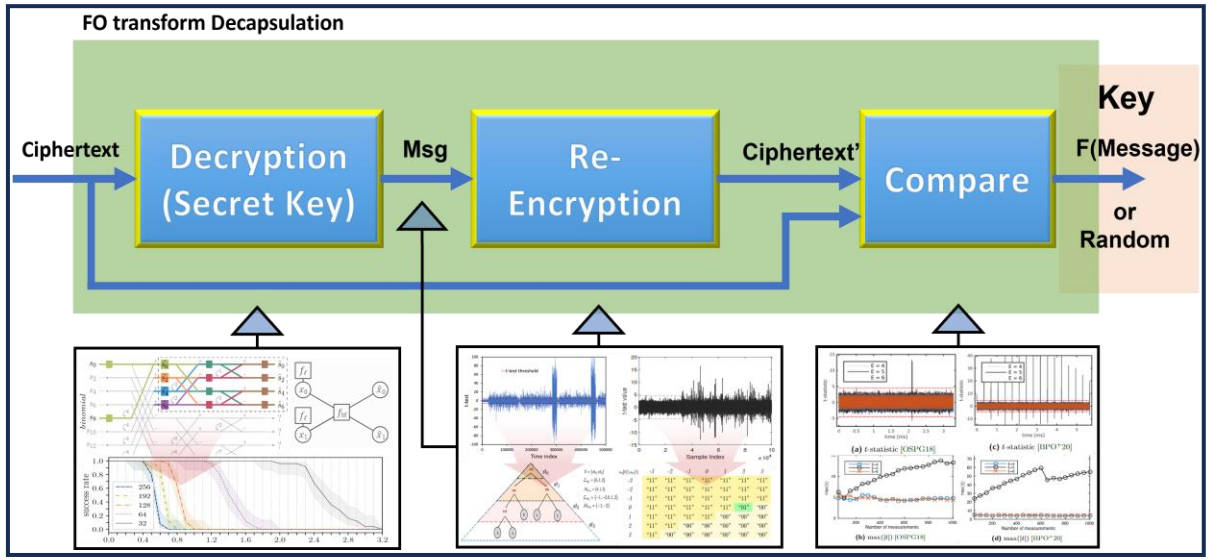
▪ 부채널 취약점을 사용한 공격 시나리오 개요

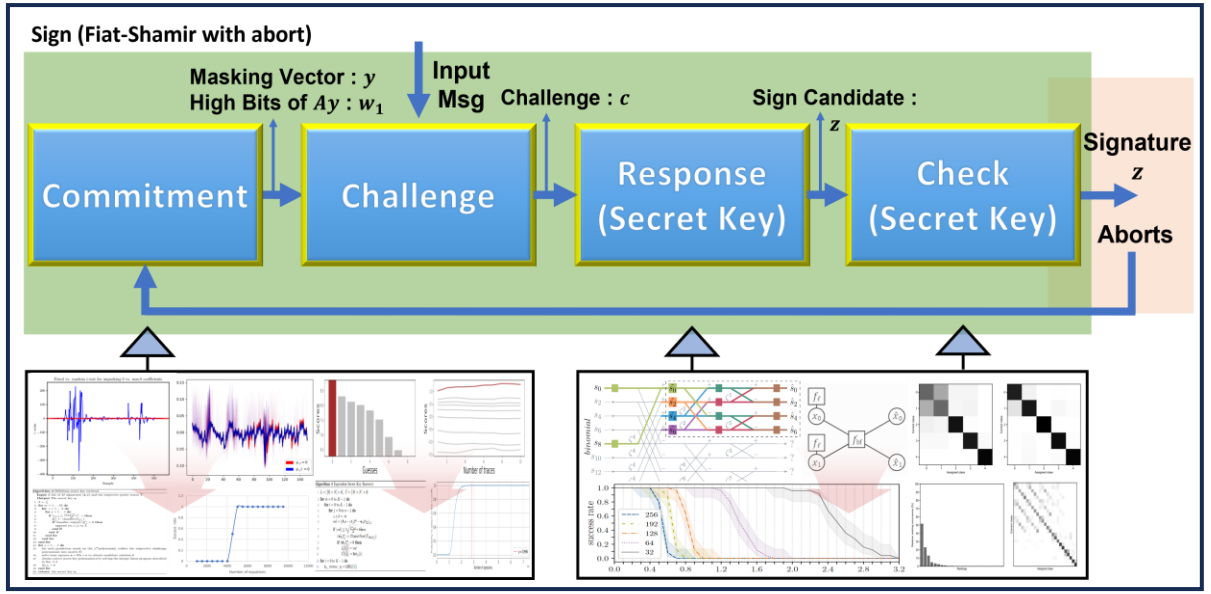
- **직접적** 공격
  - 비밀정보가 직접적으로 생성 또는 연산되는 지점의 부채널 정보를 획득하여 비밀정보를 추출하는 방법
- **간접적** 공격
  - 구분자(distinguisher) : 비밀정보와 연관된 **중간 연산값**이 **부채널 취약점**으로 인해 **일부 또는 전체 구분**됨
  - 구분자를 통해 중간 연산값 일부 또는 전체를 추측하고 **수학적 기법**을 사용하여 **비밀정보**를 **추출**
  - 다시 말해, **부채널 취약점**을 통해 블랙박스 환경의 **암호 안전성 가정**을 **깨트려** 다양한 공격을 가능하게 함



3. KpqC 알고리즘에 대한 부채널 분석

- **KpqC 알고리즘 부채널 취약점 분석 지점**
  - **직접적** 공격을 위한 부채널 취약점 분석 지점
    - 키 생성 중 개인키 생성 과정,
    - (KEM) 디캡슐화의 복호화 중 개인키 연산 과정
    - (전자서명) 서명의 개인키 연산 과정
  - **간접적** 공격을 위한 부채널 취약점 분석 지점
    - 키 생성 중 공개키 생성 과정
    - (KEM) 디캡슐화 전체 과정
    - (전자서명) 서명 전체 과정
  - **키 생성, 디캡슐화, 서명 과정**에 대한 부채널 취약점 **조사 필요**
  - 부채널 취약점 분석 **대상 함수**
    - 기반 연산 (예: 다항식 Toom-cook, Karatsuba연산 등)
    - 인코딩/디코딩 연산 (예: Vector-to/from-Bytes 함수, 압축 함수 등)
    - 비교 연산 (예: memcmp 사용 여부 등)

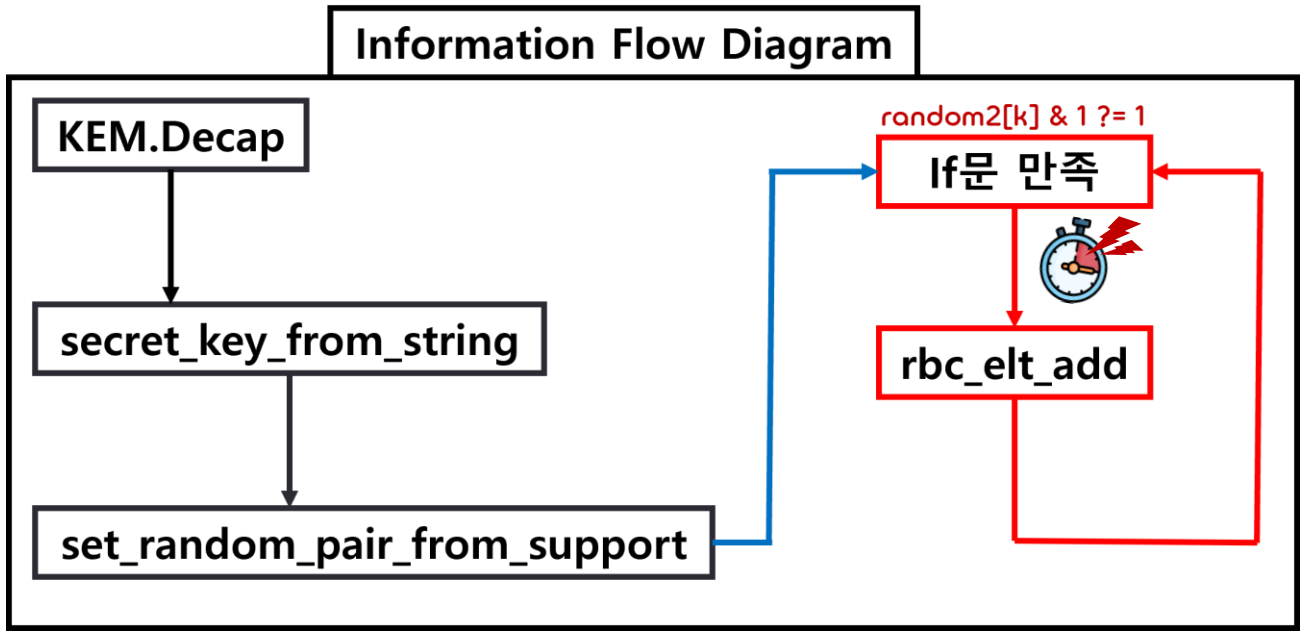




3. KpqC 알고리즘에 대한 부채널 분석

IA&AI SecLab
Implementation Attacks & AI Security Laboratory

- **KEM에 대한 부채널 취약점 분석 – Layered ROLLO-I**
  - **디캡슐화 과정**
    - **조건문**에 의한 동작 시간 발생 취약점
      - 디캡슐화 과정에서 개인키를 처리하는 부분에서 단순 **덧셈(XOR)연산** 수행
      - rbc_elt_add 함수 호출 횟수, if 조건문 차이 -> **동작 시간 차이** 발생
      - 해당 **시간차 부채널 정보**를 활용하여 **개인키 복구** 가능



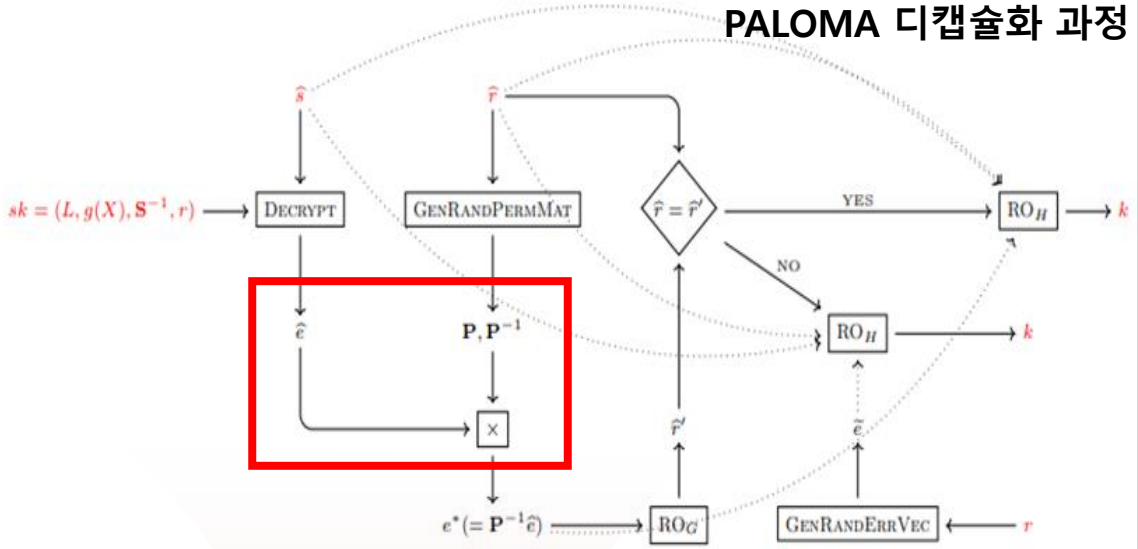

```c
random_get_bytes(ctx, random2, random2_size);

uint32_t k = 0;
uint32_t l = 0;

for(i = 0 ; i < size ; ++i) {
  if(rbc_67_elt_is_zero(o1[i])) {
    for(j = 0 ; j < support_size ; ++j) {
      if(random2[k] & 0x1) {
        rbc_67_elt_add(o1[i], support[j], o1[i]);
      }

      random2[k] = random2[k] >> 1;
      l++;
      if(l == 8) {
        l = 0;
        k++;
      }
    }
  }
}
```

```c
void rbc_67_elt_add(rbc_67_elt o, const rbc_67_elt e1, const rbc_67_elt e2) {
  for(uint8_t i = 0 ; i < RBC_67_ELT_SIZE ; i++) {
    o[i] = e1[i] ^ e2[i];
  }
}
```

3. KpqC 알고리즘에 대한 부채널 분석

- **KEM에 대한 부채널 취약점 분석 – PALOMA**
  - **디캡슐화 과정**
    - **역행렬 곱셈 과정**에서 발생하는 동작 시간 취약점
      - 치환 행렬의 역행렬을 곱하는 과정에서 조건문 사용
      - 두 비트가 다른 경우에만 코드를 수행하는 방식으로 코드 작성
      - 디캡슐화의 입력값에 따라 알고리즘 수행 시간 차이 발생
      - 각 **입력값**에 따라 발생하는 **동작 시간 정보**를 이용하여 $\hat{e}$ 추측 가능성 존재

PALOMA 디캡슐화 과정




```
/* decrypt */
Decrypt(e_hat, sk, s_hat, PALOMAParam);

/* randperm 복원 */
GenRandPermMat(P, n, r_hat);

/* ep ← P^{-1} ehat */
for (int i = 0; i < n / 64; i++) ep[i] = e_hat[i];

u64 One = 1;
for (int i = 0; i < n; i++) {          //P의 역행렬과 곱
    if (((ep[i / 64] >> (i % 64)) & 1) != ((ep[P[i] / 64] >> (P[i] % 64)) & 1)) {
        // 두 비트가 다른 경우에만 ^1 해서 바꾸기.
        ep[i / 64] ^= (One << (i % 64));
        ep[P[i] / 64] ^= (One << (P[i] % 64));
    }
}
```

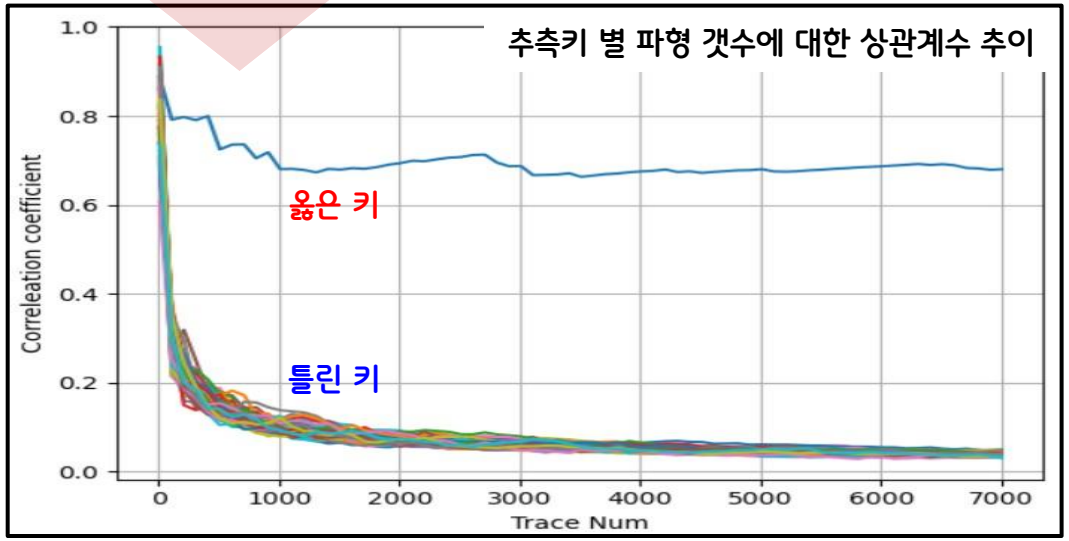
3. KpqC 알고리즘에 대한 부채널 분석

- **KEM에 대한 부채널 취약점 분석 – REDOG**
  - **복호화 과정**
    - 암호문과 개인키들의 **곱셈**에서 발생하는 **상관전력분석** 취약점
      - 공격 지점: 암호문 벡터의 원소와 개인키 벡터의 원소 **곱셈**의 **결과값**
      ① 공격자는 암호문을 구성 및 입력하여 그에 대한 동작 전력/전자파 파형 수집
      ② 개인키 P^{-1} (또는 S^{-1})의 원소 하나를 추측하여 중간값 c_1P^{-1}(또는 c_2P^{-1}) 의 해밍웨이트와 파형 간 상관계수를 계산
      ③ 가장 높은 상관계수를 가지는 P^{-1}(또는 S^{-1})의 원소 추측값을 실제값으로 판단
      - 분할-정복을 통하여 전체 P^{-1}, S^{-1} 복구
      - 같은 방법으로 개인키 H_1, H_2 까지 복구할 수 있음

$\mathsf{pk} = (G, F = GP^{-1}H_1^T[H_2^T]^{-1}S), \mathsf{sk} = (P, H, S, \Phi_H)$.

$\mathsf{Enc}(\mathsf{pk}, \mathbf{m})$: Let $\mathbf{m} \in \mathbb{F}_{q^m}^l$ be the plaintext message to be encrypted. Generate randomly vector $\mathbf{e} = (e_1, e_2) \in \mathbb{F}_{q^m}^{2n-k}$ such that $\mathrm{rk}(\mathbf{e})=t$, $e_1 \in \mathbb{F}_{q^m}^n$ and $e_2 \in \mathbb{F}_{q^m}^{n-k}$. Let $\mathbf{m}' = \mathbf{m} + \mathcal{H}(\mathbf{e})$. Compute $c_1 = \mathbf{m}'G + e_1, c_2 = \mathbf{m}'F + e_2$.
Output ciphertext $\mathbf{c} = (c_1, c_2)$.

$\mathsf{Dec}(\mathsf{sk}, c)$: Compute
$$\begin{aligned} c_1P^{-1}H_1^T - c_2S^{-1}H_2^T &= \mathbf{m}'GP^{-1}H_1^T + e_1P^{-1}H_1^T - \mathbf{m}'GP^{-1}H_1^T[H_2^T]^{-1}SS^{-1}H_2^T - e_2S^{-1}H_2^T \\ &= e_1P^{-1}H_1^T - e_2S^{-1}H_2^T \\ &= (e_1P^{-1}, -e_2S^{-1}) \begin{bmatrix} H_1^T \\ H_2^T \end{bmatrix} \end{aligned}$$
Let $\mathbf{e}' = (e_1P^{-1}, -e_2S^{-1})$. Since $\mathrm{rk}(\mathbf{e}') \leqslant r$, apply Φ_H to obtain $\mathbf{e}'$.
Compute $e_1 = e_1P^{-1}P$ and $e_2 = e_2S^{-1}S$ to obtain $\mathbf{e} = (e_1, e_2)$.
Finally, solve the system $\mathbf{m}'G = c_1 - e_1$ to recover $\mathbf{m} = \mathbf{m}' - \mathcal{H}(e)$.



3. KpqC 알고리즘에 대한 부채널 분석

IA&AI SecLab
Implementation Attacks & AI Security Laboratory

▪ 전자서명에 대한 부채널 취약점 분석 – Enhanced pqsigRM

• 서명 과정

◦ *y_init* 함수에 대한 **상관전력분석** 취약점

- 공격 지점 : 신드롬을 permutation 개인키 Q를 이용하여 치환하는 함수
  - ▸ 신드롬 $s \leftarrow h(m|i)$ 은 공격자가 자유롭게 생성할 수 있는 값

① 공격자는 메시지를 구성 및 입력하여 그에 대한 서명값 및 전력/전자파 파형 수집

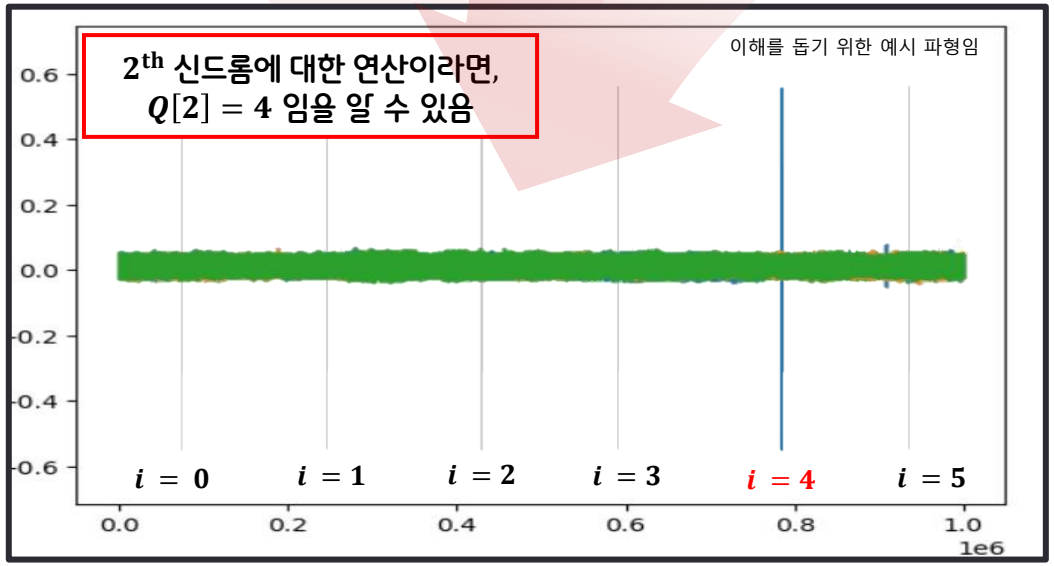
② 메시지와 서명값에 포함된 인덱스 i 를 통해 계산한 신드롬 s 의 i번째 원소의 해밍웨이트와 파형 간의 상관계수를 계산

③ 상관계수 파형 중 오른쪽 빨간 박스의 코드 구간에서 j 번째 인덱스 위치에서 상관계수가 높아졌다면 $Q[i] = j$ 라 판단

④ 1~3 단계를 반복하여 전체 Q 복구

- 같은 방식으로 개인키 σ_p^1, σ_p^2 복구 가능

```
void y_init(float *yc, float *yr, matrix* syndrome, uint16_t *Q){
        for(uint32_t i=0; i < CODE_N - CODE_K - 1; i++) {
            yc[i] = (get_element(syndrome, 0, i) == 0)? 1.:-1.;
        }
        for(uint32_t i=CODE_N-CODE_K - 1; i < CODE_N; i++) {
            yc[i] = 1.;
        }

        // yr first, yc next
        for(uint32_t i =0; i < CODE_N; i++) {
            yr[Q[i]] = yc[i];
        }
        for(uint32_t i =0; i < CODE_N; i++) {
            yc[i] = yr[i];
        }
}
```



3. KpqC 알고리즘에 대한 부채널 분석

IA&AI SecLab
Implementation Attacks & AI Security Laboratory

▪ 전자서명에 대한 부채널 취약점 분석 – AIMer

• 서명 과정

◦ *GF_add* 함수에 대한 **상관전력분석** 취약점

- 공격 지점 : 개인키 pt를 N share로 나누는 과정에서 사용되는 GF 덧셈 함수

① 공격자는 메시지를 구성 및 입력하여 그에 대한 서명값 및 전력/전자파 파형 수집

② $\bar{i}_k \neq 1$ 에 해당하는 서명값 중 $\{seeds_k\}_{k\in[\tau]}$를 통하여 $\{pk_k^i\}_{i\in[N]\setminus\{\bar{i}_k\}k\in[\tau]}$ 계산

③ pt의 부분 워드를 추측하여 $pt - pt_k^{(1)}$ 부분 워드의 해밍웨이트와 파형 간의 상관계수를 계산

④ 가장 높은 상관계수를 가지는 pt 의 부분 추측값을 실제값으로 판단

⑤ 1~3 단계를 반복하여 전체 pt 복구

▸ CISC-S'23 <KpqC 전자서명 후보 AIMer에 대한 부채널 및 오류주입 공격> 참고함

Algorithm 1: Sign$((\text{pt}, (\text{iv}, \text{ct})), m)$ - AIMer signature scheme, signing algorithm.

```
// Phase 1: Committing to the seeds and the execution views of the parties.
```

1 Sample a random salt salt $\xleftarrow{\$} \{0,1\}^{2\lambda}$.
2 Compute the first ℓ S-boxes' outputs $t_1, \ldots, t_\ell$.
3 Derive the binary matrix $A_{\text{iv}} \in (\mathbb{F}_2^{n\times n})^\ell$ and the vector $b_{\text{iv}} \in \mathbb{F}_2^n$ from the initial vector iv.
4 **for** *each parallel execution* $k \in [\tau]$ **do**
5 Sample a root seed : $\text{seed}_k \xleftarrow{\$} \{0,1\}^\lambda$.
6 Compute parties' seeds $\text{seed}_k^{(1)}, \ldots, \text{seed}_k^{(N)}$ as leaves of binary tree from seed_k.
7 **for** *each party* $i \in [N]$ **do**
8 Commit to the seed and expand random tape:
 $(\text{com}_k^{(i)}, \text{tape}_k^{(i)}) \leftarrow \text{CommitAndExpand}(\text{salt}, k, i, \text{seed}_k^{(i)})$.
9 Sample witness share: $\text{pt}_k^{(i)} \leftarrow \text{Sample}(\text{tape}_k^{(i)})$.
10 Compute witness offset and adjust first witness: $\Delta\text{pt}_k \leftarrow \text{pt} - \sum_i \text{pt}_k^{(i)}$, $\text{pt}_k^{(1)} \leftarrow \text{pt}_k^{(1)} + \Delta\text{pt}_k$.
11 **for** *each S-box with index* j **do**
12 **if** $j \le \ell$ **then**
13 For each party i, sample an S-box output: $t_{k,j}^{(i)} \leftarrow \text{Sample}(\text{tape}_k^{(i)})$.
14 Compute output offset and adjust first share: $\Delta t_{k,j} = t_j - \sum_i t_{k,j}^{(i)}$, $t_{k,j}^{(1)} \leftarrow t_{k,j}^{(1)} + \Delta t_{k,j}$.

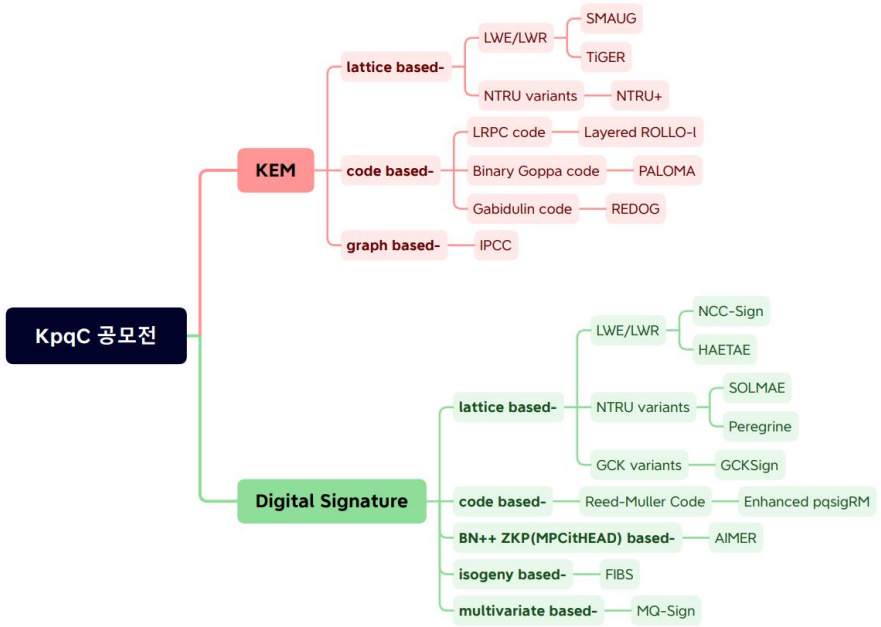
```
// Generate sharing of secret key
GF_copy(input_GF, i
```

개인키 pt에 난수값 $pt_k^{(i)}$가 for문을 통해 순차적으로 더해짐

```
for (size_t party = 0; party < N; party++)
{
    GF* shared_input =
        repetition_shared_inputs + (repetition * N + party);

    uint8_t* random_share =
        random_tapes->tape + (repetition * N + party) * random_tape_size;

    GF_from_bytes(random_share, shared_input[0]);
    GF_add(input_delta, shared_input[0], input_delta);
```

4. 향후 연구

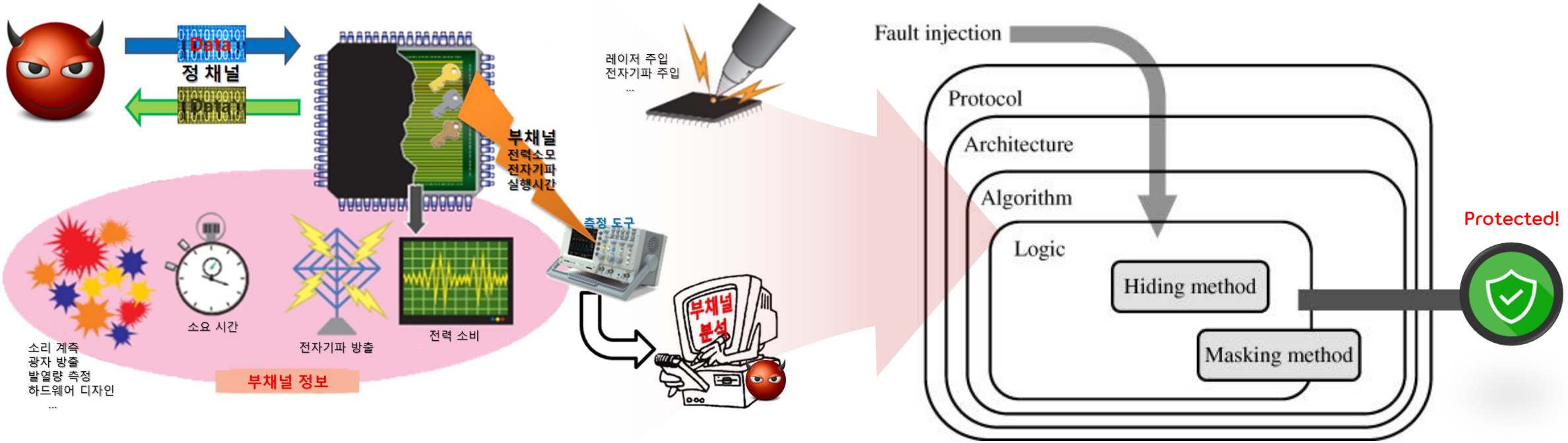
- **과제명**
  - KpqC 공모전 알고리즘 부채널 안전성 분석기술 연구
- **연구 과제 최종 목표**
  - 국내 KpqC 1라운드 공모 알고리즘에 대상 시간차 분석, 전력분석 취약성 연구



연구 내용	추진 일정(월) 4	5	6	7	8	9	10
o KpqC 공모전 1라운드 격자 기반 알고리즘에 대한 부채널 분석	(6차 워크숍, 완료)						
o KpqC 공모전 1라운드 코드 기반 알고리즘에 대한 부채널 분석	(7차 워크숍, 완료)						
o KpqC 공모전 1라운드 기타 기반 알고리즘에 대한 부채널 분석							

5. 결론

- KpqC 1라운드 **격자, 코드, 영지식 기반**에 대한 **부채널 취약점 조사**를 진행함
- **동작 시간** 및 **전력/전자파 분석**을 통한 취약점이 다수 발견됨
- KpqC 알고리즘에 대한 **완전한 constant-time 구현** 및 **마스킹 기법 개발**이 진행되어야 함
- 또한 프로파일링 공격, 오류 주입과 같은 **강한 부채널 공격**에 대한 **안전성 검증** 필요



참고 문헌

1. An, Soojung, Suhri Kim, Sunghyun Jin, HanBit Kim, and HeeSeok Kim. "Single trace side channel analysis on NTRU implementation." Applied Sciences 8, no. 11 (2018): 2014.
2. Askeland, Amund, and Sondre Rønjom. "A side-channel assisted attack on NTRU." Cryptology ePrint Archive (2021).
3. Atıcı, Ali C., Lejla Batina, Benedikt Gierlichs, and Ingrid Verbauwhede. "Power analysis on NTRU implementations for RFIDs: First results." In The 4th Workshop on RFID Security–RFIDSec. 2008.
4. Azouaoui, Melissa, Olivier Bronchain, Clément Hoffmann, Yulia Kuzovkova, Tobias Schneider, and François-Xavier Standaert. "Systematic study of decryption and re-encryption leakage: the case of kyber." In Constructive Side-Channel Analysis and Secure Design: 13th International Workshop, COSADE 2022, Leuven, Belgium, April 11-12, 2022, Proceedings, pp. 236-256. Cham: Springer International Publishing, 2022.
5. Azouaoui, Melissa, Yulia Kuzovkova, Tobias Schneider, and Christine van Vredendaal. "Post-quantum authenticated encryption against chosen-ciphertext side-channel attacks." Cryptology ePrint Archive (2022).
6. Bache, Florian, Clara Paglialonga, Tobias Oder, Tobias Schneider, and Tim Güneysu. "High-speed masking for polynomial comparison in lattice-based KEMs." IACR Transactions on Cryptographic Hardware and Embedded Systems (2020): 483-507.
7. Beirendonck, Michiel Van, Jan-Pieter D'anvers, Angshuman Karmakar, Josep Balasch, and Ingrid Verbauwhede. "A side-channel-resistant implementation of SABER." ACM Journal on Emerging Technologies in Computing Systems (JETC) 17, no. 2 (2021): 1-26.
8. Berzati, Alexandre, Andersson Calle Viera, Maya Chartouni, Steven Madec, Damien Vergnaud, and David Vigilant. "A Practical Template Attack on CRYSTALS-Dilithium." Cryptology ePrint Archive (2023).
9. Bhasin, Shivam, Jan-Pieter D'Anvers, Daniel Heinz, Thomas Pöppelmann, and Michiel Van Beirendonck. "Attacking and defending masked polynomial comparison for lattice-based cryptography." IACR Transactions on Cryptographic Hardware and Embedded Systems (2021): 334-359.
10. Bos, Joppe W., Marc Gourjon, Joost Renes, Tobias Schneider, and Christine Van Vredendaal. "Masking kyber: First-and higher-order implementations." IACR Transactions on Cryptographic Hardware and Embedded Systems (2021): 173-214.
11. Bronchain, Olivier, and Gaëtan Cassiers. "Bitslicing Arithmetic/Boolean Masking Conversions for Fun and Profit: with Application to Lattice-Based KEMs." IACR Transactions on Cryptographic Hardware and Embedded Systems (2022): 553-588.
12. Cayrel, Pierre-Louis, Brice Colombier, Vlad-Florin Drăgoi, Alexandre Menu, and Lilian Bossuet. "Message-recovery laser fault injection attack on the classic McEliece cryptosystem." In Advances in Cryptology–EUROCRYPT 2021: 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17–21, 2021, Proceedings, Part II, pp. 438-467. Cham: Springer International Publishing, 2021.

참고 문헌

13. Cayrel, Pierre-Louis, Brice Colombier, Vlad-Florin Drăgoi, Alexandre Menu, and Lilian Bossuet. "Message-recovery laser fault injection attack on the classic McEliece cryptosystem." In Advances in Cryptology–EUROCRYPT 2021: 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17–21, 2021, Proceedings, Part II, pp. 438-467. Cham: Springer International Publishing, 2021.

14. Chen, Cong, Oussama Danba, Jeffrey Hoffstein, Andreas Hülsing, Joost Rijneveld, John M. Schanck, Peter Schwabe, William Whyte, and Zhenfei Zhang. "Algorithm specifications and supporting documentation." Brown University and Onboard security company, Wilmington USA (2019).

15. Chen, Zhaohui, Yuan Ma, and Jiwu Jing. "Low-Cost Shuffling Countermeasures Against Side-Channel Attacks for NTT-Based Post-Quantum Cryptography." IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 42, no. 1 (2022): 322-326.

16. Colombier, Brice, Vlad-Florin Drăgoi, Pierre-Louis Cayrel, and Vincent Grosso. "Profiled Side-channel Attack on Cryptosystems based on the Binary Syndrome Decoding Problem." IEEE Transactions on Information Forensics and Security 17 (2022): 3407-3420.

17. D'Anvers, Jan-Pieter, Michiel Van Beirendonck, and Ingrid Verbauwhede. "Revisiting higher-order masked comparison for lattice-based cryptography: algorithms and bit-sliced implementations." IEEE Transactions on Computers 72, no. 2 (2022): 321-332.

18. Goy, Guillaume, Antoine Loiseau, and Philippe Gaborit. "A new key recovery side-channel attack on HQC with chosen ciphertext." In Post-Quantum Cryptography: 13th International Workshop, PQCrypto 2022, Virtual Event, September 28–30, 2022, Proceedings, pp. 353-371. Cham: Springer International Publishing, 2022.

19. Goy, Guillaume, Loiseau, Antoine, Gaborit, Philippe, "Estimating the Strength of Horizontal Correlation Attacks in the Hamming Weight Leakage Model: A Side-Channel Analysis on HQC KEM", wcc2022.uni-rostock.de

20. Guo, Qian, Andreas Johansson, and Thomas Johansson. "A key-recovery side-channel attack on classic mceliece." Cryptology ePrint Archive (2022).

21. Guo, Qian, Clemens Hlauschek, Thomas Johansson, Norman Lahr, Alexander Nilsson, and Robin Leander Schröder. "Don't reject this: Key-recovery timing attacks due to rejection-sampling in HQC and BIKE." IACR Transactions on Cryptographic Hardware and Embedded Systems (2022): 223-263.

22. Guo, Qian, Denis Nabokov, Alexander Nilsson, and Thomas Johansson. "SCA-LDPC: A Code-Based Framework for Key-Recovery Side-Channel Attacks on Post-Quantum Encryption Schemes." Cryptology ePrint Archive (2023).

23. Guo, Qian, Thomas Johansson, and Paul Stankovski. "A key recovery attack on MDPC with CCA security using decoding errors." In Advances in Cryptology–ASIACRYPT 2016: 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I 22, pp. 789-815. Springer Berlin Heidelberg, 2016.

24. Hamburg, Mike, Julius Hermelink, Robert Primas, Simona Samardjiska, Thomas Schamberger, Silvan Streit, Emanuele Strieder, and Christine van Vredendaal. "Chosen ciphertext k-trace attacks on masked CCA2 secure kyber." IACR Transactions on Cryptographic Hardware and Embedded Systems (2021): 88-113.

참고 문헌

25. Heinz, Daniel, and Gabi Dreo Rodosek. "Fast First-Order Masked NTTRU." In Constructive Side-Channel Analysis and Secure Design: 14th International Workshop, COSADE 2023, Munich, Germany, April 3–4, 2023, Proceedings, pp. 127-148. Cham: Springer Nature Switzerland, 2023.

26. Heinz, Daniel, and Thomas Pöppelmann. "Combined fault and DPA protection for lattice-based cryptography." IEEE Transactions on Computers (2022).

27. Hermelink, Julius, Silvan Streit, Emanuele Strieder, and Katharina Thieme. "Adapting Belief Propagation to Counter Shuffling of NTTs." IACR Transactions on Cryptographic Hardware and Embedded Systems (2023): 60-88.

28. Ji, Yanning, Ruize Wang, Kalle Ngo, and Elena Dubrova. "A Side-Channel Attack on a Hardware Implementation of CRYSTALS-Kyber." In 2023 IEEE European Test Symposium (ETS'23). 2023.

29. Kannwischer, Matthias J., Peter Pessl, and Robert Primas. 2020. "Single-Trace Attacks on Keccak". IACR Transactions on Cryptographic Hardware and Embedded Systems 2020 (3):243-68. https://doi.org/10.13154/tches.v2020.i3.243-268.

30. Lahr, Norman, Ruben Niederhagen, Richard Petri, and Simona Samardjiska. "Side channel information set decoding using iterative chunking: Plaintext recovery from the "Classic McEliece" hardware reference implementation." In Advances in Cryptology–ASIACRYPT 2020: 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7–11, 2020, Proceedings, Part I 26, pp. 881-910. Springer International Publishing, 2020.

31. Lee, Mun-Kyu, Jeong Eun Song, Dooho Choi, and Dong-Guk Han. "Countermeasures against power analysis attacks for the NTRU public key cryptosystem." IEICE transactions on fundamentals of electronics, communications and computer sciences 93, no. 1 (2010): 153-163.

32. Marzougui, Soundes, Vincent Ulitzsch, Mehdi Tibouchi, and Jean-Pierre Seifert. "Profiling side-channel attacks on dilithium: A small bit-fiddling leak breaks it all." Cryptology ePrint Archive (2022).

33. Mujdei, Catinca, Lennert Wouters, Angshuman Karmakar, Arthur Beckers, Jose Maria Bermudo Mera, and Ingrid Verbauwhede. "Side-channel analysis of lattice-based post-quantum cryptography: Exploiting polynomial multiplication." ACM Transactions on Embedded Computing Systems (2022).

34. Ngo, Kalle, Elena Dubrova, Qian Guo, and Thomas Johansson. "A side-channel attack on a masked IND-CCA secure saber KEM implementation." IACR Transactions on Cryptographic Hardware and Embedded Systems (2021): 676-707.

35. Ngo, Kalle, Ruize Wang, Elena Dubrova, and Nils Paulsrud. "Side-channel attacks on lattice-based KEMs are not prevented by higher-order masking." Cryptology ePrint Archive (2022).

36. Oder, Tobias, Tobias Schneider, Thomas Pöppelmann, and Tim Güneysu. "Practical CCA2-secure and masked ring-LWE implementation." Cryptology ePrint Archive (2016).

37. Paulsrud, Nils. "A Side Channel Attack on a Higher-Order Masked Software Implementation of Saber." (2022).

38. Pessl, Peter, and Lukas Prokop. "Fault attacks on CCA-secure lattice KEMs." IACR Transactions on Cryptographic Hardware and Embedded Systems (2021): 37-60.

참고 문헌

39. Pessl, Peter, and Robert Primas. "More practical single-trace attacks on the number theoretic transform." In Progress in Cryptology–LATINCRYPT 2019: 6th International Conference on Cryptology and Information Security in Latin America, Santiago de Chile, Chile, October 2–4, 2019, Proceedings 6, pp. 130-149. Springer International Publishing, 2019.

40. Primas, Robert, Peter Pessl, and Stefan Mangard. "Single-trace side-channel attacks on masked lattice-based encryption." In Cryptographic Hardware and Embedded Systems–CHES 2017: 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings, pp. 513-533. Springer International Publishing, 2017.

41. Rajendran, Gokulnath, Prasanna Ravi, Jan-Pieter D'Anvers, Shivam Bhasin, and Anupam Chattopadhyay. "Pushing the Limits of Generic Side-Channel Attacks on LWE-based KEMs-Parallel PC Oracle Attacks on Kyber KEM and Beyond." IACR Transactions on Cryptographic Hardware and Embedded Systems (2023): 418-446.

42. Ravi, Prasanna, Anupam Chattopadhyay, Jan Pieter D'Anvers, and Anubhab Baksi. "Side-channel and fault-injection attacks over lattice-based post-quantum schemes (Kyber, Dilithium): Survey and new results." Cryptology ePrint Archive (2022).

43. Ravi, Prasanna, Shivam Bhasin, Sujoy Sinha Roy, and Anupam Chattopadhyay. "On exploiting message leakage in (few) NIST PQC candidates for practical message recovery attacks." IEEE Transactions on Information Forensics and Security 17 (2021): 684-699.

44. Ravi, Prasanna, Sujoy Sinha Roy, Anupam Chattopadhyay, and Shivam Bhasin. "Generic Side-channel attacks on CCA-secure lattice-based PKE and KEM schemes." Cryptology ePrint Archive (2019).

45. Schamberger, Thomas, Julian Renner, Georg Sigl, and Antonia Wachter-Zeh. "A power side-channel attack on the CCA2-secure HQC KEM." In Smart Card Research and Advanced Applications: 19th International Conference, CARDIS 2020, Virtual Event, November 18–19, 2020, Revised Selected Papers 19, pp. 119-134. Springer International Publishing, 2021.

46. Schamberger, Thomas, Lukas Holzbaur, Julian Renner, Antonia Wachter-Zeh, and Georg Sigl. "A power side-channel attack on the reed-muller reed-solomon version of the HQC cryptosystem." In Post-Quantum Cryptography: 13th International Workshop, PQCrypto 2022, Virtual Event, September 28–30, 2022, Proceedings, pp. 327-352. Cham: Springer International Publishing, 2022.

47. Schamberger, Thomas, Oliver Mischke, and Johanna Sepulveda. "Practical evaluation of masking for NTRUEncrypt on ARM Cortex-M4." In Constructive Side-Channel Analysis and Secure Design: 10th International Workshop, COSADE 2019, Darmstadt, Germany, April 3–5, 2019, Proceedings 10, pp. 253-269. Springer International Publishing, 2019.

48. Schröder, Leander. "A novel timing side-channel assisted key-recovery attack against HQC." PhD diss., Wien, 2022.

49. Shen, Muyan, Chi Cheng, Xiaohan Zhang, Qian Guo, and Tao Jiang. "Find the Bad Apples: An efficient method for perfect key recovery under imperfect SCA oracles–A case study of Kyber." IACR Transactions on Cryptographic Hardware and Embedded Systems (2023): 89-112.

50. Sim, Bo-Yeon, 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, no. 21 (2022): 21382-21397.

참고 문헌

51. Sim, Bo-Yeon, Jihoon Kwon, Joohee Lee, Il-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 8 (2020): 183175-183191.

52. Sim, Bo-Yeon, Jihoon Kwon, Kyu Young Choi, Jihoon Cho, Aesun Park, and Dong-Guk Han. "Novel side-channel attacks on quasi-cyclic code-based cryptography." IACR Transactions on Cryptographic Hardware and Embedded Systems (2019): 180-212.

53. Steffen, Hauke Malte, Lucie Johanna Kogelheide, and Timo Bartkewitz. "In-depth Analysis of Side-Channel Countermeasures for CRYSTALS-Kyber Message Encoding on ARM Cortex-M4." In Smart Card Research and Advanced Applications: 20th International Conference, CARDIS 2021, Lübeck, Germany, November 11–12, 2021, Revised Selected Papers, pp. 169-188. Cham: Springer International Publishing, 2022.

54. Ueno, Rei, Keita Xagawa, Yutaro Tanaka, Akira Ito, Junko Takahashi, and Naofumi Homma. "Curse of re-encryption: A generic power/em analysis on post-quantum kems." IACR Transactions on Cryptographic Hardware and Embedded Systems (2022): 296-322.

55. Wang, An, Ce Wang, Xuexin Zheng, Weina Tian, Rixin Xu, and Guoshuang Zhang. "Random key rotation: side-channel countermeasure of NTRU cryptosystem for resource-limited devices." Computers & Electrical Engineering 63 (2017): 220-231.

56. Wang, Ruize, Kalle Ngo, and Elena Dubrova. "A message recovery attack on LWE/LWR-based PKE/KEMs using amplitude-modulated EM emanations." In Information Security and Cryptology–ICISC 2022: 25th International Conference, ICISC 2022, Seoul, South Korea, November 30–December 2, 2022, Revised Selected Papers, pp. 450-471. Cham: Springer Nature Switzerland, 2023.

57. Wang, Ruize, Kalle Ngo, and Elena Dubrova. "Side-channel analysis of saber kem using amplitude-modulated em emanations." In 2022 25th Euromicro Conference on Digital System Design (DSD), pp. 488-495. IEEE, 2022.

58. Xu, Zhuang, Owen Pemberton, Sujoy Sinha Roy, David Oswald, Wang Yao, and Zhiming Zheng. "Magnifying side-channel leakage of lattice-based cryptosystems with chosen ciphertexts: The case study of kyber." IEEE Transactions on Computers 71, no. 9 (2021): 2163-2176.

59. Zheng, Xuexin, An Wang, and Wei Wei. "First-order collision attack on protected NTRU cryptosystem." Microprocessors and Microsystems 37, no. 6-7 (2013): 601-609.

60. Guo, Qian, Thomas Johansson, and Alexander Nilsson. "A key-recovery timing attack on post-quantum primitives using the Fujisaki-Okamoto transformation and its application on FrodoKEM." In *Advances in Cryptology–CRYPTO 2020: 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17–21, 2020, Proceedings, Part II*, pp. 359-386. Cham: Springer International Publishing, 2020.

61. Karabulut, Emre, and Aydin Aysu. "Falcon down: Breaking falcon post-quantum signature scheme through side-channel attacks." In *2021 58th ACM/IEEE Design Automation Conference (DAC)*, pp. 691-696. IEEE, 2021.

62. Guerreau, Morgane, Ange Martinelli, Thomas Ricosset, and Mélissa Rossi. "The hidden parallelepiped is back again: power analysis attacks on falcon." *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2022): 141-164.

참고 문헌

63. Zhang, Shiduo, Xiuhan Lin, Yang Yu, and Weijia Wang. "Improved Power Analysis Attacks on Falcon." In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 565-595. Cham: Springer Nature Switzerland, 2023.

64. Ravi, Prasanna, Martianus Frederic Ezerman, Shivam Bhasin, Anupam Chattopadhyay, and Sujoy Sinha Roy. "Will you cross the threshold for me?-Generic side-channel assisted chosen-ciphertext attacks on NTRU-based KEMs." *Cryptology ePrint Archive* (2021).

65. Guo, Qian, Thomas Johansson, and Alexander Nilsson. "A key-recovery timing attack on post-quantum primitives using the Fujisaki-Okamoto transformation and its application on FrodoKEM." In *Annual International Cryptology Conference*, pp. 359-386. Cham: Springer International Publishing, 2020.