제 8회 부채널정보분석경진대회 기업이 주는 우수 인재상

NIST PQC Dilithium의 부채널 공격 및 대응 기법 동향 분석

Kookmin University Sung-Hwan Yoo, Dong-Guk Han

I. Introduction

- 양자내성암호(PQC)의 수요에 따라 NIST PQC에서는 PKE/KEM과 Digital Signature 부분에서 표준 알고리즘을 선정하였다.

Table 1. NIST PQC Standard Algorithm

PKE/KEM		Digital Signature		
Kyber	HQC	Dilithium	Falcon	SPHINCS+

- 표준화로 인한 산업 활용도 측면에서 알고리즘의 안전성 분석 연구는 꾸준히 진행되며 이에 대한 동향 정리 역시 필요하다.
- 따라서 전자서명에서 표준으로 선정된 Dilithium의 부채널 공격 및 대응 기법 동향 분석을 진행한 후 향후 안전한 대응 기법에 대해 모색한다.

II. NIST PQC Dilithium

- Dilithium은 MLWE(Module Learning With Error)와 SIS(Short Integer Solution)을 기반으로 하는 격자 기반 전자서명 알고리즘이다.
- Keccak 기반 해시 함수를 통해 Uniform Sampling을 수행하며, NTT와 SampleBall 개념을 활용하여 연산 및 Challenge 값을 생성한다.

Input :
Output : $pk = (\rho, t_1), sk = (\rho, K, tr, s_1, s_2, t_0)$
1. $\zeta \leftarrow \{0,1\}^{256}$
2. $(\rho, \rho', K) \in \{0,1\}^{256} \times \{0,1\}^{512} \times \{0,1\}^{256} := H(\zeta)$
3. $A \in R_q^{k \times l} := \text{ExpandA}(\rho)$
4. $(s_1, s_2) \in S_\eta^l \times S_\eta^l := \text{ExpandS}(\rho')$
5. $t := As_1 + s_2$
6. $(t_1, t_0) := \text{Power2Round}_q(t, d)$
7. $tr \in \{0,1\}^{256} := H(\rho \,||\, t_1)$
8. return $(pk = (\rho, t_1), sk = (\rho, K, tr, s_1, s_2, t_0))$

Fig. 1. Key Generation Pseudocode

Input : $sk = (\rho, K, tr, s_1, s_2, t_0), m$ (공개 값 / 비밀 값)
Output : $\sigma = (\tilde{c}, z, h)$
1. $A \in R_q^{k \times l} := \text{ExpandA}(\rho)$
2. $\mu \in \{0,1\}^{512} := H(tr \,||\, m)$
3. $\kappa := 0, (z, h) := \perp$
4. $\rho' \in \{0,1\}^{512} := H(K \,||\, \mu)$
5. **while** $(z, h) = \perp$ ***do***
6. $\quad y \in \tilde{S}_{\gamma_1}^l := \text{ExpandMask}(\rho' \,||\, \kappa)$
7. $\quad w := Ay$
8. $\quad w_1 := \text{HighBits}(w, 2\gamma_2)$
9. $\quad \tilde{c} \in \{0,1\}^{256} := H(\mu \,||\, w_1)$
10. $\quad c \in B_\tau := \text{SampleBall}(\tilde{c})$
11. $\quad z := y + cs_1$
12. $\quad r_0 := \text{LowBits}_q(w - cs_2, 2\gamma_2)$
13. $\quad$ **if** $\|z\|_\infty \geq \gamma_1 - \beta$ **or** $\|r_0\|_\infty \geq \gamma_2 - \beta$, **then** $(z, h) := \perp$
14. $\quad$ **else**
15. $\quad\quad h := \text{MakeHint}_q(-ct_0, w - cs_2 + ct_0, 2\gamma_2)$
16. $\quad\quad$ **if** $\|ct_0\|_\infty \geq \gamma_2$ **or** the # of 1's in h in greater then ω, then $(z, h) := \perp$
17. $\quad \kappa := \kappa + l$
18. return $\sigma = (\tilde{c}, z, h)$

Fig. 2. Signature Generation Pseudocode

III. SCA Trends in Key Generation

- 키 생성은 통신 초기 과정 및 키 값 변경과 같이 수행되는 횟수가 제한적이다.
- 따라서 단일 수행 공격이 대부분이며, Factor Graph와 BP Algorithm을 사용하는 SASCA(Soft Analytical Side-Channel Attack)과 같은 공격이 다수 존재한다.

Table 2. Summary SCA Trends in Key Generation

Location	Target Function	Attack Method	Countermeasure	Reference
Fig. 1. line 2	H (Keccak)	SASCA (Factor Graph, BP Algorithm)	None	[1]
Fig. 1. line 5	Multiplication	SASCA (Factor Graph, BP Algorithm)	Shuffling	[2]

- Keccak로 구성되어 있는 H 함수 공격[1]은 Keccak-f 함수의 각 연산 값이 RAM의 저장될 시 발생하는 전력 정보를 사용하여 공격을 수행한다.
- NTT 곱셈 연산 공격[2]은 단일 Cooley-Turkey(CT) 연산을 대상으로 수행한다.

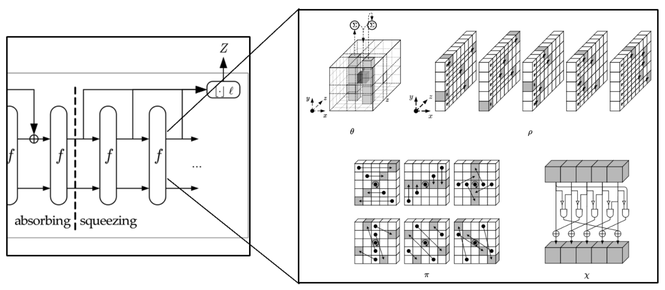

Fig. 3. Keccak-f Function Structure

Table 3. Get EM Data and Location

Location	Store Data
θ 입력	라운드 시작 전 전체 State
θ 출력, 패리티 평면	θ 계산 결과, θ 중간 XOR 결과
$\pi \cdot \rho$ 입력/출력	State 위치 이동 및 bit rotation
χ 입력/출력	State 논리 연산 연산 값

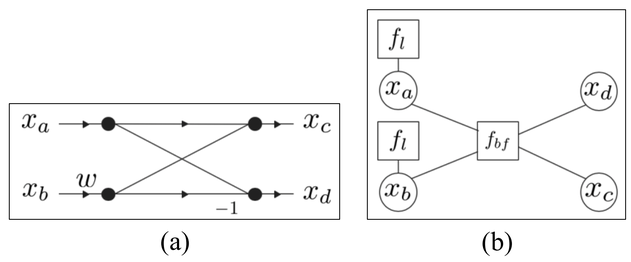

Fig. 4. (a) CT Structure, (b) Factor Graph of CT

Table 4. NTT Shuffling Countermeasure

구분	Coarse -Full	Coarse-In -Group	Fine
보안성	최대 엔트로피	그룹 내 무작위	Load/Store 무작위
엔트로피	$\frac{n}{2}!$	$\left(\frac{n}{2m}!\right)^m$	2^{2n}
사용기법	Knuth-Yates	그룹 shuffle	Arithmetic Conditional Swap

IV. SCA Trends in Signature Generation

- 서명 생성의 경우 키 생성과 다르게 동일한 키에 대해 반복적인 수행이 많다.
- 따라서 다중 수행 공격이 가능하며, 통계적 기법인 CPA나 Template Attack과 같은 공격이 존재한다.

Table 5. Summary SCA Trends in Signature Generation

Location	Target Function	Attack Method	Countermeasure	Reference
Fig. 2. line 11	Multiplication	CPA	Masking	[3]
Fig. 2. line 11 - 13	Rejection Sampling	Template with SASCA (Factor Graph, BP Algorithm)	Masking	[4]

- 서명 생성에서의 CPA 공격[3]은 비밀 값 s_1을 대상으로 수행되며, Mongomery Modular 곱셈 코드의 2가지 지점을 대상으로 수행된다.
- Rejection Sampling을 대상으로 수행된 Template with SASCA 공격[4]은 거부된 서명($\bar{c}$)과 유효한 서명 값(c)을 함께 사용하여 비밀 값 s_1을 복구한다.
- 대응 기법은 Masking의 대한 많은 연구[5, 6]가 진행되었으며 High-Order Masking의 Gadget을 제안하여 부채널 공격에 대응하였다.

Table 6. Summary Representative High-Order Masking Gadget

Representative Masking Gadget	Location	Role
ShiftMod	Fig. 2. line 6, line 13	Masking share bit shift in Sampling vector y
SecMult	Fig. 2. line 6, line 13	Masking share Multiplication
LMSwitch	Fig. 2. line 13	Larger Modular Switch

Input : t, c, s
Output :
1. unsigned int i
2. for(i = 0; i < 256; ++i){
3. int64_t a;
4. a = (int64_t)c[i]·s[i] Point 1
5. t = (int32_t)a·qinv
6. t[i] = (a – (int64_t)t·q) >> 32 Point 2
7. }

Fig. 5. Mongomery Modular Multiplication

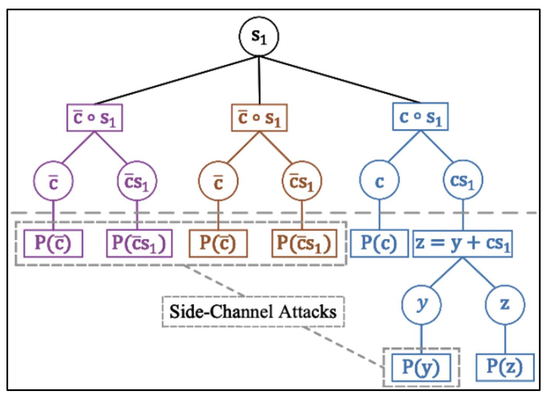

Fig. 6. Factor Graph from Rejection Sampling

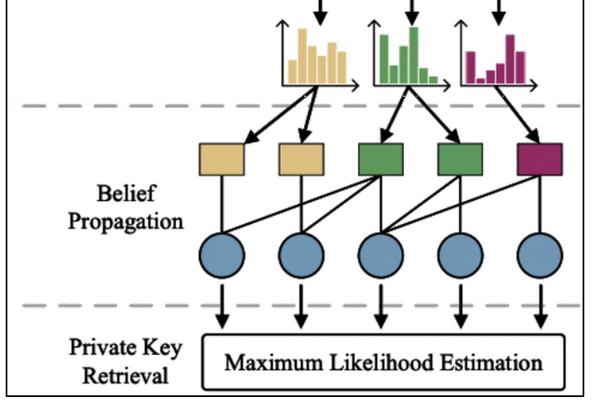

Fig. 7. Template with SASCA Process

V. Conclusion

- Dilithium은 표준으로 선정된 만큼 산업체에서 많은 활용이 요구되기에 부채널 안전성 검증 연구가 꾸준히 진행되고 있다.
- 특히, 대응 기법의 경우 수행 지점마다 요구되는 안전성이 다르며 키 생성의 경우 다소 오버헤드가 낮은 Shuffling을 서명 생성의 경우 안전성이 높은 Masking 대응 기법이 필요하다.
- 이에 따라, 두 대응 기법을 적절히 활용한 효율적인 대응 기법에 대한 연구가 지속적으로 필요하다.

[References]

[1] Matthias J. Kannwischer, et al, "Single-Trace Attacks on Keccak," in TCHES 2020.
[2] Prasanna Ravi, et al., "On Configurable SCA Countermeasures Against Single Trace Attacks for the NTT," in International Association for Cryptology Research - IACR 2020.
[3] Zhaohui Chen, et al, "An Efficient Non-Profiled Side-Channel Attack on the CRYSTALS-Dilithium Post-Quantum Signature," in Institute of Electrical and Electronics Engineers – IEEE 2021.
[4] Zheng Liu, et al, "Release the Power of Rejected Signatures: An Efficient Side-Channel Attack on Dilithium," in Cryptoeprint 2025.
[5] Jean-Sébastien Coron, et al, "Improved Gadgets for the High-Order Masking of Dilithium," in TCHES 2023.
[6] Jean-Sébastien, et al, "Improved High-Order Masked Generation of Maksing Vector and Rejection Sampling in Dilithium," in TCHES 2024.