KpqC 2라운드 후보 TiMER의 메시지 인코딩에 대한 단일파형공격

유성환*, 한재승**, 한동국***

*,**,***국민대학교 (학부생, 대학원생, 교수)

Single-trace attack on message encoding of KpqC round 2 candidate TiMER

Sung-Hwan Yoo*, Jae-Seung Han**, Dong-Guk Han***

*,**,***Kookmin University(Undergraduate, Graduate student, Professor)

요 약

최근 양자 컴퓨터와 양자 알고리즘의 성장으로 양자 내성 암호(Post-Quantum Cyptography, PQC)에 대한 공모전이 활발히 진행되고 있다. 국내에서는 2022년부터 KpqC 국가공모전(Korean Post-Quantum Cryptography)을 시작했으며, 2024년 11월 기준 총 8종의 알고리즘이 평가되고 있다. 본 논문에서는 2라운드 후보 중 SMAUG-T의 일종인 TiMER 알고리즘에 대한 부채널 취약점과 이를 이용한 메시지 값 복구 논리를 제안하고 실험을 통해 검증한다. 본 논문에서는 TiMER에서 사용되는 D2 인코딩에서 메시지 bit 값에 따라 소비전력 차이가 발생함을 조사하였다. 제안하는 공격 논리는 해당 특성을 사용하여 단일 전력 파형만으로도 메시지 값을 복구하는 방법이다. 실험은 ARM Cortex-M4 기반 MCU 환경에서 수행되었으며, 메시지 값이 단일 파형으로 복구 가능함을 실험적으로 검증하였다.

I. 서론

최근 양자 컴퓨터와 양자 알고리즘의 성장이 가속화 되고 있는 시점에서 RSA와 ECC와 같은 현대 암호의 안전성 문제가 대두되고 있다. 미국 NIST에서는 고수준의 양자 컴퓨터 개발 이후에도 안전한 암호 통신 체계를 구축하고자 2016년부터 양자 내성 암호 (Post Quantum Cryptograpy, PQC) 공모전을 시작하였다. 국내에서도 2022년부터 KpqC 공모전을 시작하였으며, 2024년 10월 기준 KpqC는 2라운드를 진행하고 있다. 2라운드에서는 PKE(Public Key Encryption)/KEM(Key Encapsulation Mechanism)에서 4종, 전자서명에서 4종이 평가되고 있다. 평가 과정에 있어 알고리즘에 대한 안전성에 대한 평가는 필수적이며 부채널 공격에 대한 안전성 연구 역시 활발히 이루어지고 있다.[1]

본 논문은 KpqC 2라운드 PKE/KEM 후보 중 TiMER 알고리즘의 부채널 분석을 진행한다. TiMER는 SMAUG-T 알고리즘의 모드 중 IoT 환경에서 주로 사용되는 모드로 NewHope과 같이 KEM 과정에서 D2 인코딩을 사용한다.[2] TiMER에 대한 부채널 분석을 수행한 결과 KEM에서 사용되는 D2 인코딩 연산의 단일 소비전력 파형만으로 메시지 값을 복구할 수 있음을 확인했다. 따라서 본 논문에서는 단일 소비전력 파형의 단순전력분석(Simple Power Analysis, SPA)를 통해 메시지 값을 복구하는 방법과 실험을 보인다.

[Contribution]

본 논문에서는 TiMER의 D2 인코딩 연산 중 메시지를 다항식으로 변환하는 과정에서 bit 별 소비전력 차이가 발생함을 보이고, 이를 기반으로 단순전력분석을 통해 메시지 값을 복구하는 공격을 제안한다. 그리고 제안한 공격을 ARM Cortex-M4 기반 STM32-F3 환경에서 실험하

여 메시지 값이 성공적으로 복구됨을 보인다.

II. 배경지식

본 절에서는 TiMER의 D2 인코딩 알고리즘과 기존 메시지 인코딩에 대한 단일파형 공격을 설명하고, SMAUG-T팀에서 제시한 대응기법을 소개한다.

2.1 기존 메시지 인코딩 공격

1장에서 설명했듯 TiMER는 SMAUG-T의 다른 모드와 다르게 D2 인코딩을 사용하며, 이는 복호 실패율을 낮추고, 암호문의 크기를 줄이는 장점을 가진다. 이로 인해 TiMER는 IoT와 같이 저수준 환경에 적합하게 사용되고 있다. [표 1]은 대응기법 전 D2 인코딩 의사코드이다.

[표 1] D2 인코딩 의사코드

Input : message = μ
Output : poly
1. $v \leftarrow R_q$
2. **for** i from 0 to message_len **do**
3. **for** j from 0 to 7 **do**
4. mask $\leftarrow -((\mu[i] \gg j)) \ \& \ 1$
5. $v_{8*i+j+0} \leftarrow$ mask & (q/2)
6. $v_{8*i+j+128} \leftarrow$ mask & (q/2)
7. return $v \in R_q$

line 4는 인코딩 과정에서 메시지 bit에 따라 0은 0, 1은 -1로 mask를 설정한다. mask의 unsigned int 자료형 특성상 0과 1은 32 만큼의 HW(Hamming Weight)차이를 가지며, 이를 통해 메시지를 복구하는 단일파형공격이 등장하였다.

2.2 SMAUG-T 팀의 대응기법

2.1에서 D2 인코딩에 대한 단일파형 공격이 소개되자 SMAUG-T 팀은 SMAUG와 TiGER를 결합하는 과정에서 대응기법을 적용하였다.[3] 0과 -1에 대한 HW 차이로 메시지 값이 복구되기에 인코딩 수행 시 mask 값을 0과 1로 설정하여 HW 차이를 줄였다. [표 2]는 대응기법을 적용한 D2 인코딩의 의사코드이다.

[표 2] 대응기법 적용된 D2 인코딩 의사코드

Input : message = μ
Output : poly
1. $v \leftarrow R_q$
2. **for** i from 0 to 15 **do**
3. **for** j from 0 to 7 **do**
4. mask $\leftarrow ((\mu[i] \gg j)) \ \& \ 1$
5. mask $\leftarrow$ (mask * (q/2)) & (q/2)
6. $v_{8*i+j+0} \leftarrow$ mask
7. $v_{8*i+j+128} \leftarrow$ mask
8. return $v \in R_q$

line 4에서 연산에 대한 부호를 제거하여 기존 0과 -1이 아닌 0과 1로 mask 값을 할당해 메시지 인코딩 공격에 대응하였다.

III. 메시지 복구에 대한 부채널 공격

본 절에서는 SMAUG-T 팀이 제시한 D2 인코딩 대응기법에서 여전히 bit별 소비전력 차이가 발생됨을 보이고 이를 활용해 단일파형 공격으로 메시지 값이 복구됨을 보인다.

3.1 부채널 공격 방법론

대응기법이 적용된 [표 2]의 의사코드는 mask 값을 0과 1로 할당하였지만 D2 인코딩 성질을 위해 line 5에서 $q/2$와의 곱셈 연산을 수행한다. SMAUG-T 팀은 해당 부분을 [그림 1]과 같이 구현했으며, 해당 코드는 SMAUG-T의 공식 Github 코드로 4.0.1 버전의 코드이다.[4]

```
mask = (msg[i] >> j) & 1;
mask = (mask * Modulus_Q_2) & Modulus_Q_2;
```

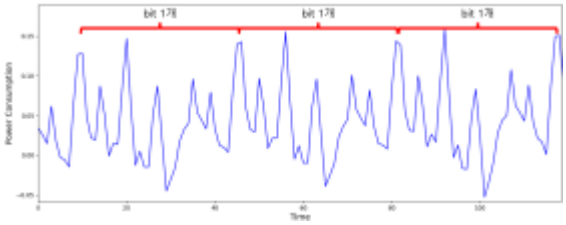
[그림 1] D2 인코딩 mask 구현

앞서 언급했듯 line 2에서 mask는 0x7fff 값을 가지는 Modulus_Q_2($q/2$)와 곱셈 연산을 수행한다. 즉, Modulus_Q_2 곱셈으로 mask 값은 0과 0x7fff을 가지며 HW 차이는 15만큼 발생된다. 따라서 곱셈 연산의 실제 소비전력을 측정하면 파형 분포에 따라 mask 값을 유추할 수 있고, 메시지 값을 복구할 수 있다. D2 인코딩이 사용되는 KEM은 암호화 통신 과정에서 세션키를 전달 때만 사용되기에 전체 통신에서 1

번만 수행된다. 즉 KEM을 대상으로 메시지 복구를 수행하기 위해서는 단일파형만으로 메시지 값을 복구해야 하며, 본 공격은 단일파형만으로 메시지 값을 복구할 수 있다.

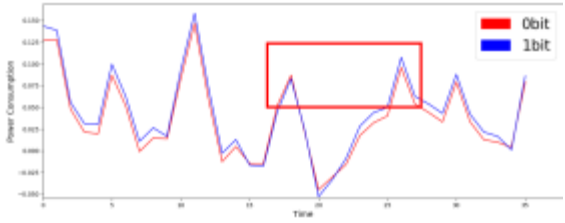
3.2 부채널 공격 실험

본 절에서는 3.1에서 소개한 단일파형 공격 방법론을 검증하기 위해 ARM Cortex-M4 기반 STM32F303 MCU 보드와 CW308UFO를 ChipWhisperer-Lite와 결합해 파형을 수집하였다. [그림 2]은 mask와 Modulus_Q_2의 bit별 곱셈 연산 소비전력이며, bit마다 반복되는 파형 개요를 나타낸다.



[그림 2] bit별 mask와 Modulus_Q_2의 곱셈 소비전력

메시지 bit값에 따라 소비전력 차이를 파악하기 위해서는 0과 1일 때의 파형을 비교해야 하며 [그림 3]은 두가지 파형을 함께 출력한 파형이다.



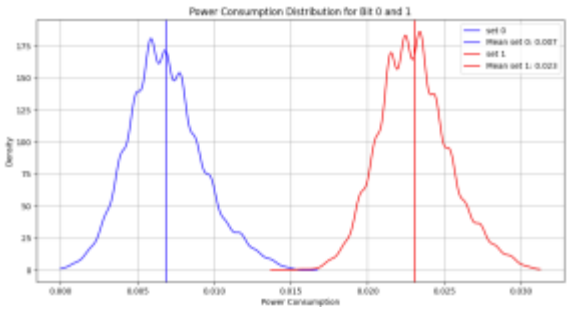
[그림 3] 메시지 bit가 0과 1bit에서의 파형 비교

출력된 파형에서 표시한 두 극점을 기준으로 12800개의 bit 파형을 분석한 결과 [표 2]와 같이 bit별 소비전력 차이가 식별된다.

[표 2] bit별 극점 사이의 평균 소비전력 차

bit	평균 소비전력 차
0	0.009765625
1	0.025390625

명확한 구분을 위해 소비전력 차이에 대한 분포를 확인한 결과 [그림 4]와 같이 0과 1에서의 분포도 차이가 명확히 들어난다.



[그림 4] bit별 소비전력 차에 대한 분포

해당 데이터를 기반으로 곱셈 연산의 파형을 단순전력분석한 결과 인코딩 되는 메시지 값을 복구할 수 있었다.

IV. 결론

본 논문은 KpqC 2라운드 PKE/KEM 후보 중 SMAUG-T의 TiMER 모드에 대한 단일파형 공격 방법을 제안하고 실험을 통해 메시지 값이 복구됨을 입증했다. SMAUG-T 팀에서 제안한 대응기법이 적용됨에도 불구하고, D2 인코딩에서 메시지 bit에 따라 소비전력 차이가 여전히 발생하며 이는 TiMER 알고리즘의 취약점으로 사용될 수 있음을 실험을 통해 검증하였다. 따라서 향후 본 논문에서 제안한 공격에 대응되는 대응기법에 대한 연구가 필요하다.

[사사] “본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터사업의 연구결과 수행되었음”(IITP-2024-RS-2022-00164800)

[참고문헌]

[1] BO-YEON SIM, et al. “Single-Trace Attacks on Message Encoding in Lattice-Based KEMs. IEEE 2020.
[2] Erdem Alkim, et al. “NewHope.” NIST PQC 2020.
[3] Jung Hee Cheon, et al. “SMAUG-T: the Key Exchange Algorithm based on Module-LWE and Module-LWR“ KPQC 2024. pp. 30.
[4] hmchoe0528(2024). SMAUG-T_public. https://github.com/hmchoe0528/SMAUG-T_public.git.