제 7회 부채널정보분석경진대회 부채널분석연구회장상
KpqC 2라운드 후보 SMAUG-T의 키종속 연산에 대한 단순전력 분석

국민대학교 유성환, 한재승, 한동국

I. Introduction

- 양자내성암호(PQC)의 수요에 따라 부채널분석 저항성의 검증이 활발히 진행되고 있다.[1]
- KpqC 알고리즘에도 부채널분석 저항성 검증이 필요하다.
- KpqC 2라운드(2024.04) 후보에 대한 선행 연구가 존재하지 않는다.
  따라서 후보 중 SMAUG-T에 대한 단순전력분석(SPA)을 제안한다.

Challenges

- SMAUG-T 알고리즘에서 발생할 수 있는 취약점을 확인한다.
- 취약점과 부채널공격을 활용하여 SMAUG-T의 비밀 값을 유추한다.

Contribution

- 복호화 연산 과정에서 다항식 곱셈 함수에 대한 비 상수시간과 비밀키 값에 따라 달라지는 연산 과정의 취약점을 식별한다.
- 식별한 취약점과 단순전력분석 공격 기법을 활용하여 비밀키 정보를 유추한다.

II. KpqC SMAUG-T Feature

Sparse Ternary

- 1, 0, -1을 비밀키 계수로 사용하며, 다항식에서 사용되는 1과 -1의 총 개수는 파라미터인 sparse 값으로 주어진다.

Secret Key Architecture

- SMAUG-T128 기준으로 비밀키 다항식은 2개이며, 2개의 sparse 값은 140이다.
- 다항식 별 sparse 값은 랜덤으로 생성되고, 다항식에서의 1과 -1의 개수 역시 랜덤으로 생성된다.

Parameters sets Security level	SMAUG-T128 1
n	256
k	2
(q, p)	$(1024, 256)$
(p', t)	$(32, 2)$
(h_s, h_r)	$(140, 132)$
σ	1.0625

```
1번째 키 생성
poly1의 1과 -1의 총 개수 : 67
poly2의 1과 -1의 총 개수 : 73
poly 2개의 1과 -1의 총 개수 : 140
-----------------------------
2번째 키 생성
poly1의 1과 -1의 총 개수 : 71
poly2의 1과 -1의 총 개수 : 69
poly 2개의 1과 -1의 총 개수 : 140
-----------------------------
```

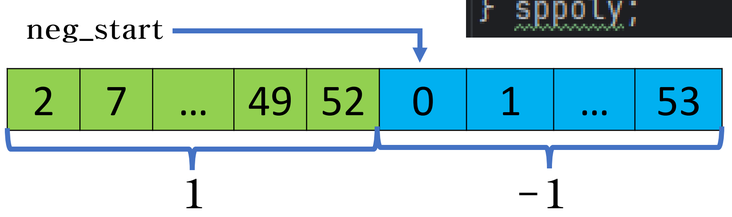
```
1번째 키 생성
poly1에서 1의 개수 : 34, -1의 개수 : 36
poly2에서 1의 개수 : 41, -1의 개수 : 29
-----------------------------------------
2번째 키 생성
poly1에서 1의 개수 : 39, -1의 개수 : 34
poly2에서 1의 개수 : 34, -1의 개수 : 33
```

SMAUG-T Key Store Mechanism

- 비밀키 저장 시 차수 값 만을 배열로 저장하며, 계수가 1인 차수 값을 먼저 저장한 뒤 -1이 계수인 차수 값을 저장한다.

sx	차수 값을 저장하는 배열
neg_start	-1의 차수가 저장되는 첫 인덱스
cnt	-1과 1의 총 sparse 값 (배열 길이)

```
typedef struct {
    uint8_t *sx;
    uint8_t neg_start;
    uint8_t cnt;
} sppoly;
```



III. Attack Target Function

- 복호화 연산에서 비밀키를 통해 다항식 곱셈을 수행하는 함수를 타겟 함수로 선택하였다.[2]

$$m = \left\lfloor \frac{t}{p} \cdot \langle c_1, s \rangle + \frac{t}{p'} \cdot c_2 \right\rfloor$$

- ①을 통해 입력 값 b에 대해 수행되는 반복 문 횟수가 다르다. (상수시간 만족 안함)
- ②을 통해 비밀키 계수에 따라 수행되는 연산자가 다르기에, 단순전력분석을 통해 계수 값을 유추할 수 있다.

Algorithm 1. poly_mult_add

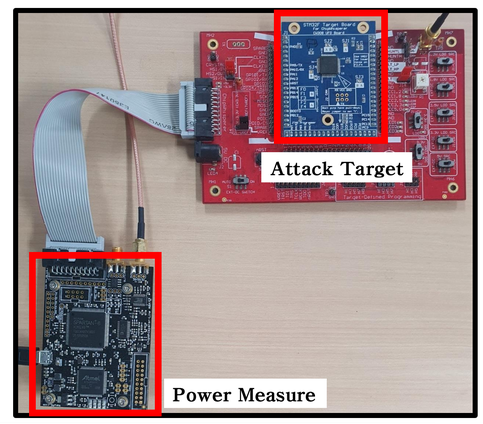
Input	a, b, neg_start
Output	c

```
c = 0,
for i = 0 to neg_start − 1 do
    degree = b[i]
    for j = neg_start to n − 1 do
        c[degree + j] = c[degree + j] + a[j]
for i = neg_start to len(b) − 1 do
    degree = b[i]
    for j = 0 to n − 1 do
        c[degree + j] = c[degree + j] − a[j]
for j = 0 to n − 1 do
    c[j] = c[j] − c[n + j]
return c
```

IV. Experimental Environment

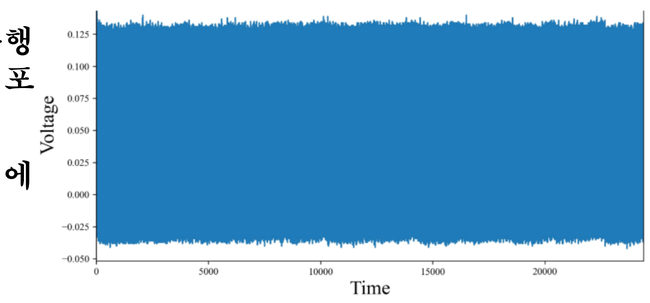
- 전자파 수집을 위해 타겟 보드에 3에서 소개한 poly_mult_add 함수를 탑재했다.
- 단순전력 분석이기에 단일 파형으로 공격이 가능하기에 파형은 1개만 수집하였다.

Attack Target	ARM Cortex-M4 STM32F3
Power Measure	ChipWhisperer-Lite

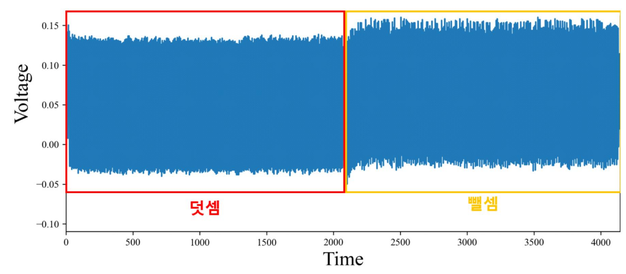


V. Experimental Result

- 한 개의 다항식의 곱셈 연산 수행 시 수집되는 전자파는 100,964 포인트가 수집되었다.
- 다항식 별 sparse 값은 랜덤이기에 매번 수집되는 포인트는 다르다.



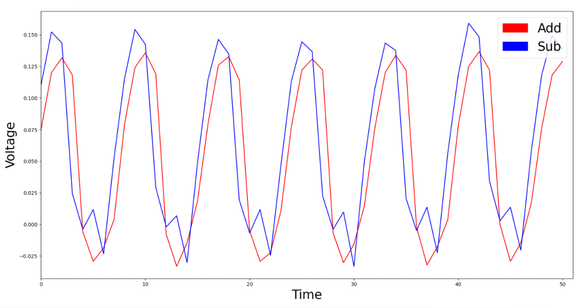
- 덧셈, 뺄셈 연산 시 수집되는 전자파는 2,050 포인트이다.
- 덧셈, 뺄셈 연산은 상수시간을 만족하기에 매번 동일한 포인트로 수집된다.



- 다항식 한 개의 곱셈 연산은 3에서 소개한 것처럼 덧셈과 뺄셈으로만 구성되기에 전체 포인트 수 100,964에서 2,050 포인트를 나눈 약 49가 덧셈과 뺄셈의 연산 횟수이다.
- 즉, 공격자는 랜덤으로 생성되는 다항식 별 sparse 값을 단순전력 분석을 통해 유추할 수 있다.
- 덧셈과 뺄셈의 전력차를 특이점으로 파형을 분석하고자 평균을 구한 결과 그래프와 다르게 뺄셈이 작게 계산된다.

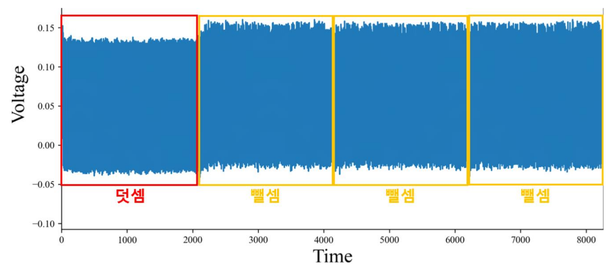
연산	소비전력 차이
덧셈	0.16324745
뺄셈	0.09461675

- 소비전력을 자세히 확인한 결과 뺄셈의 경우 ③과 같이 전력차가 매우 작게 형성되는 부분이 존재한다.
- 해당 부분으로 인해 소비전력 차이가 덧셈보다 작게 형성된다.



VI. Conclusion

- 전력차를 기반으로 파형을 분석한 결과 다음과 같이 덧셈과 뺄셈의 연산 횟수를 파악할 수 있다.
- 공격자는 랜덤으로 생성되는 1과 -1의 개수까지 파악할 수 있으며 비밀키 다항식의 정보를 유추할 수 있다.



- 본 논문은 KpqC 2라운드 후보 중 SMAUG-T 알고리즘에서 비밀키 정보를 유출할 수 있는 방법론을 제시하고 실험을 통해 비밀키에서 랜덤으로 생성되는 정보를 유출할 수 있음을 보인다.

References

- [1] Jeonghwan Lee, et al. "A key recovery side-channel attack on KpqC 1 round candidate SMAUG" 정보보호학회 2023
- [2] Jung Hee Cheon, et al. “SMAUG-T: the Key Exchange Algorithm based on Module-LWE and Module-LWR” KPQC 2024

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터사업의 연구결과로 수행되었음 (No. IITP-2024-RS-2022-0016480