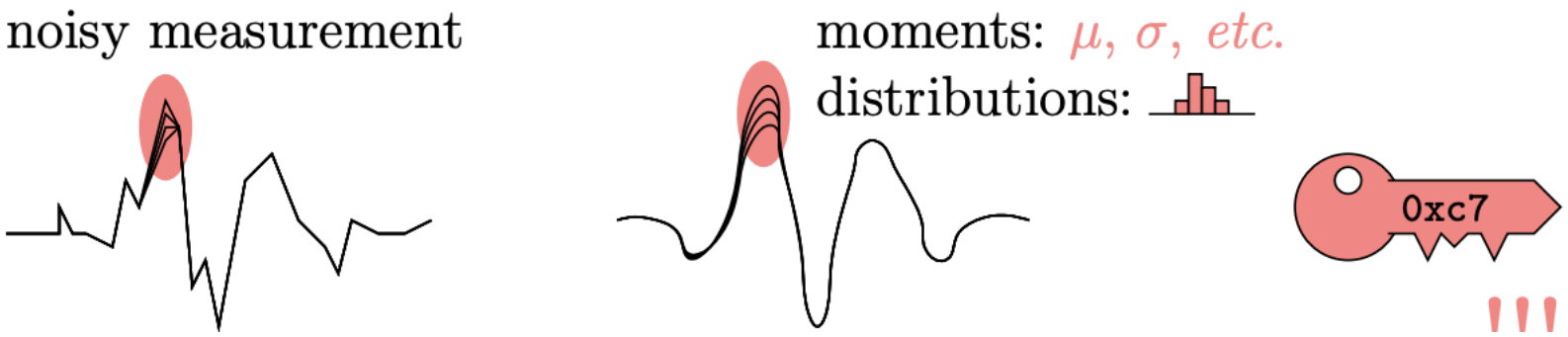
2차 부채널 분석 기법

부채널 대응책



- 외적
  노이즈 추가
  지연 추가

- 내적
  전력 감추기
  마스킹

마스킹

- 목표
  유출되는 값과 중간 값이 관계 없도록

- 방법
  무작위 값 사용

- 취약점
  고차 공격

1차 마스킹

$$P0 = Z \perp M , P1 = M$$

- 민감한 값 Z 를 두개의 값으로 분할
- P0은 마스킹 된 변수 ⊥ 반전 가능한 연산

- 부울 마스킹

$P0 = Z \oplus M , P1 = M$

2차 CPA

- 첫번째 누출과 두번째 누출의 결합

- 소프트웨어에서는 두 포인트은 순차적으로 실행됨

➢t0과 t1의 두 가지 다른 시간에 누출.

  ➢L (t0) 첫 번째 누출

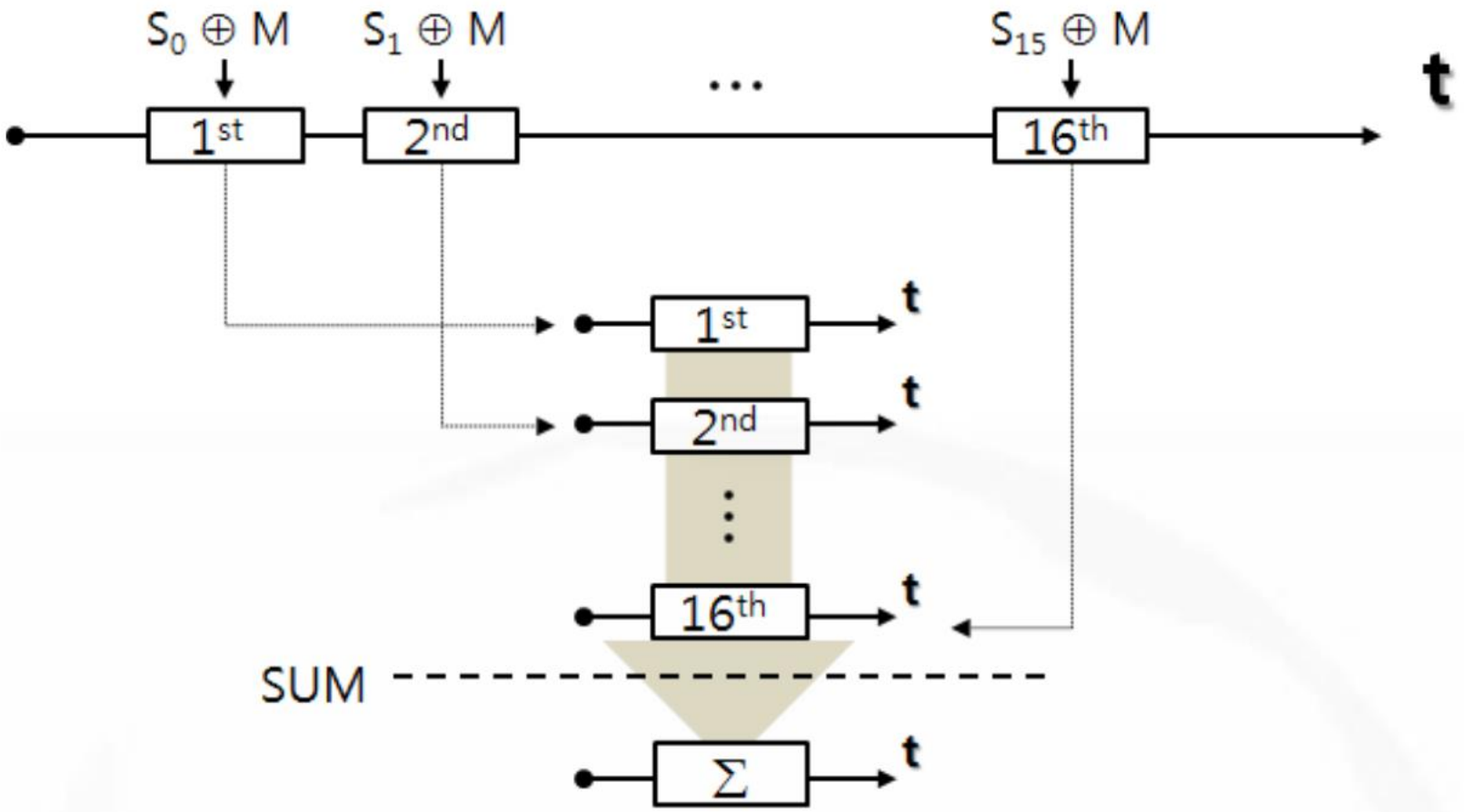
  ➢L (t1) 두 번째 누출

2차 CPA

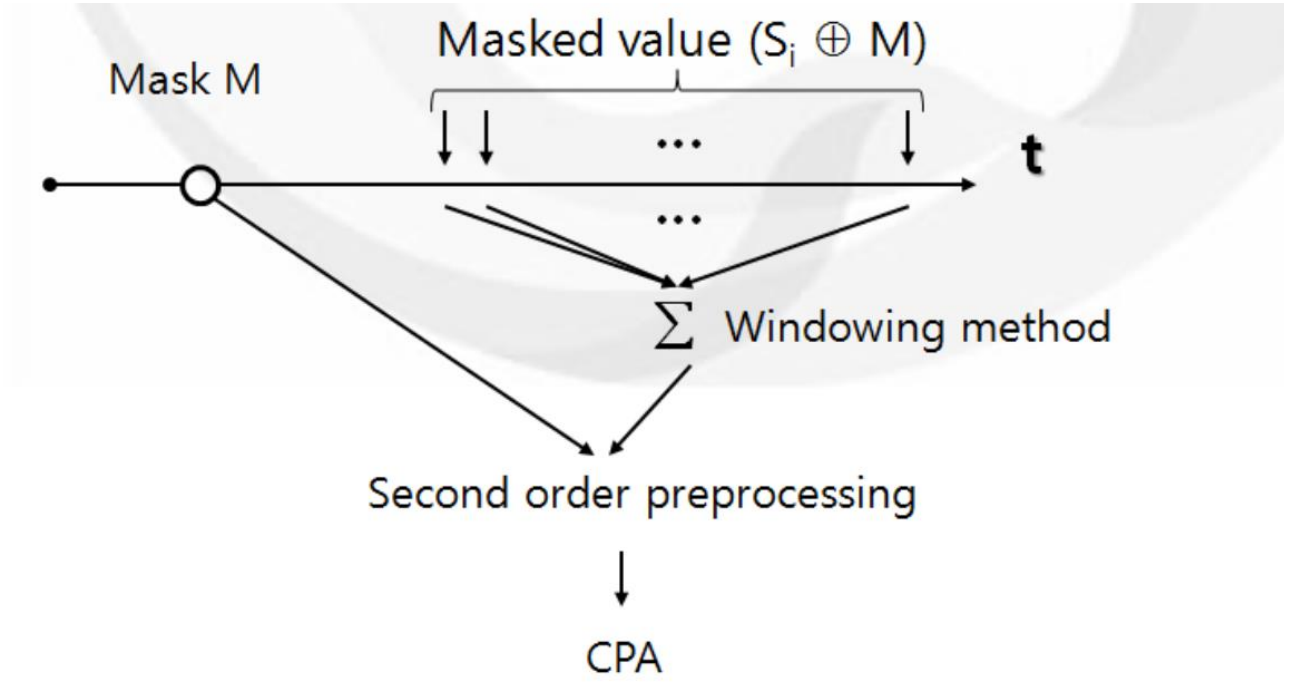
t0과 t1을 모르고 2O-CPA를 수행하는 방법?

- 전수조사
  가능한 모든 두 포인트에 공격 시도
  O(n ^ 2) CPA
- 좋은 포인트 찾기
- 전처리

Windowing 기법



Windowing 기법 + SOCPA



$$HW(a \oplus b) = |HW(a) - HW(b)|.$$

$$\begin{aligned} \mathrm{HW}(S) &\approx |\mathrm{HW}(M) - \mathrm{HW}(S \oplus M)| \\ &\approx |C(M) - C(S \oplus M)| \end{aligned}$$

두 지점의 Sbox 출력 공격

Practical Second-Order DPA Attacks for Masked Smart Card Implementations of Block Ciphers*

Elisabeth Oswald, Stefan Mangard, Christoph Herbst, and Stefan Tillich

Institute for Applied Information Processing and Communciations (IAIK),
Graz University of Technology, Inffeldgasse 16a, A–8010 Graz, Austria
{elisabeth.oswald, stefan.mangard, christoph.herbst,
stefan.tillich}@iaik.tugraz.at

Abstract. In this article we describe an improved concept for second-order differential-power analysis (DPA) attacks on masked smart card implementations of block ciphers. Our concept allows to mount second-order DPA attacks in a rather simple way: a second-order DPA attack consists of a pre-processing step and a DPA step. Therefore, our way of performing second-order DPA attacks allows to easily assess the number of traces that are needed for a successful attack. We give evidence on the effectiveness of our methodology by showing practical attacks on a masked AES smart card implementation. In these attacks we target inputs and outputs of the SubBytes operation in the first encryption round.

- 두가지 2차 cpa 공격 제안

하나의 마스크 사용

$$S'(X \oplus M) = S(X) \oplus M$$

$$S'(P \oplus K \oplus M) = S(P \oplus K) \oplus M$$

$$|C(S(P \oplus K) \oplus M) - C(P \oplus K \oplus M)|$$

$$HW(S(P \oplus K) \oplus (P \oplus K))$$

β	1	2	3	4	5	6
1 Bit	0.0861	0.0985	0.0950	0.0869	0.0775	0.0685
2 Bits	0.1119	0.1315	0.1283	0.1189	0.1080	0.0972
3 Bits	0.1415	0.1652	0.1604	0.1482	0.1341	0.1203
4 Bits	0.1723	0.1914	0.1834	0.1674	0.1496	0.1327
5 Bits	0.1936	0.2100	0.2003	0.1822	0.1623	0.1435
6 Bits	0.2092	0.2291	0.2186	0.1987	0.1767	0.1559
7 Bits	0.2278	0.2460	0.2341	0.2125	0.1887	0.1661
8 Bits	0.2405	0.2622	0.2501	0.2273	0.2021	0.1782

두개의 마스크 사용

$$S'(X \oplus M) = S(X) \oplus M'$$

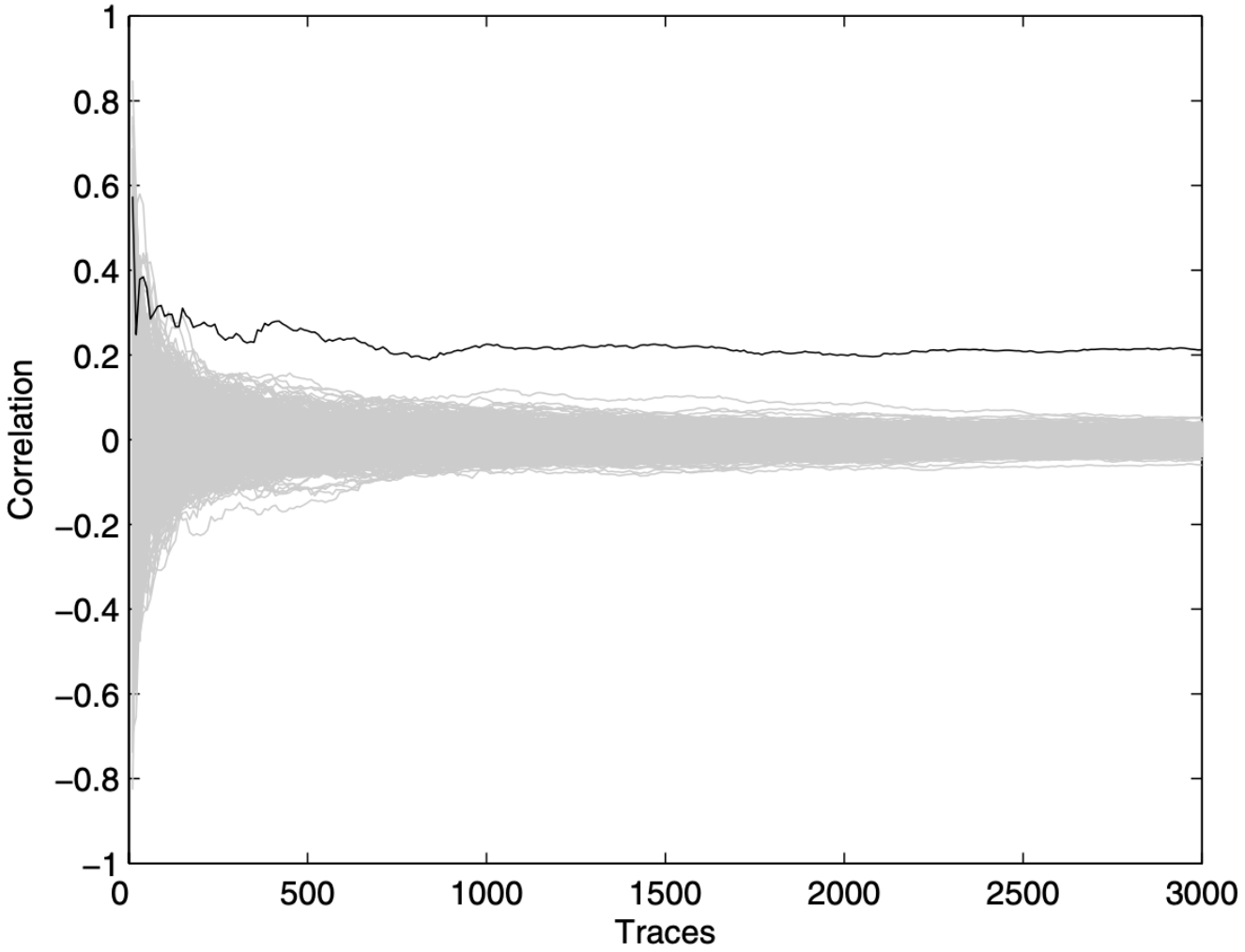
$$|C(S(P_1 \oplus K_1) \oplus M') - C(S(P_2 \oplus K_2) \oplus M')|$$

$$S(P_1 \oplus K_1) \oplus M' \qquad S(P_2 \oplus K_2) \oplus M'$$

$$HW(S(P_1 \oplus K_1) \oplus S(P_2 \oplus K_2))$$

β	1	2	3	4	5	6
1 Bit	0.0851	0.0894	0.0944	0.0788	0.0698	0.0587
8 Bits	0.2322	0.2563	0.2517	0.2265	0.2043	0.1755

결과


Correlation
Traces
1
0.8
0.6
0.4
0.2
0
−0.2
−0.4
−0.6
−0.8
−1
0
500
1000
1500
2000
2500
3000

Q & A