격자 기반 암호 부채널 공격 논문 리뷰

https://youtu.be/GHBeZfqH1O0

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB
https://crypto.modoo.at

논문

- **마스크 된 비대칭 격자 기반 암호화의 단일 트레이스 SCA**
- 템플릿 공격 (TA)과 다음의 조합 :

  신념 전파

  격자 디코딩

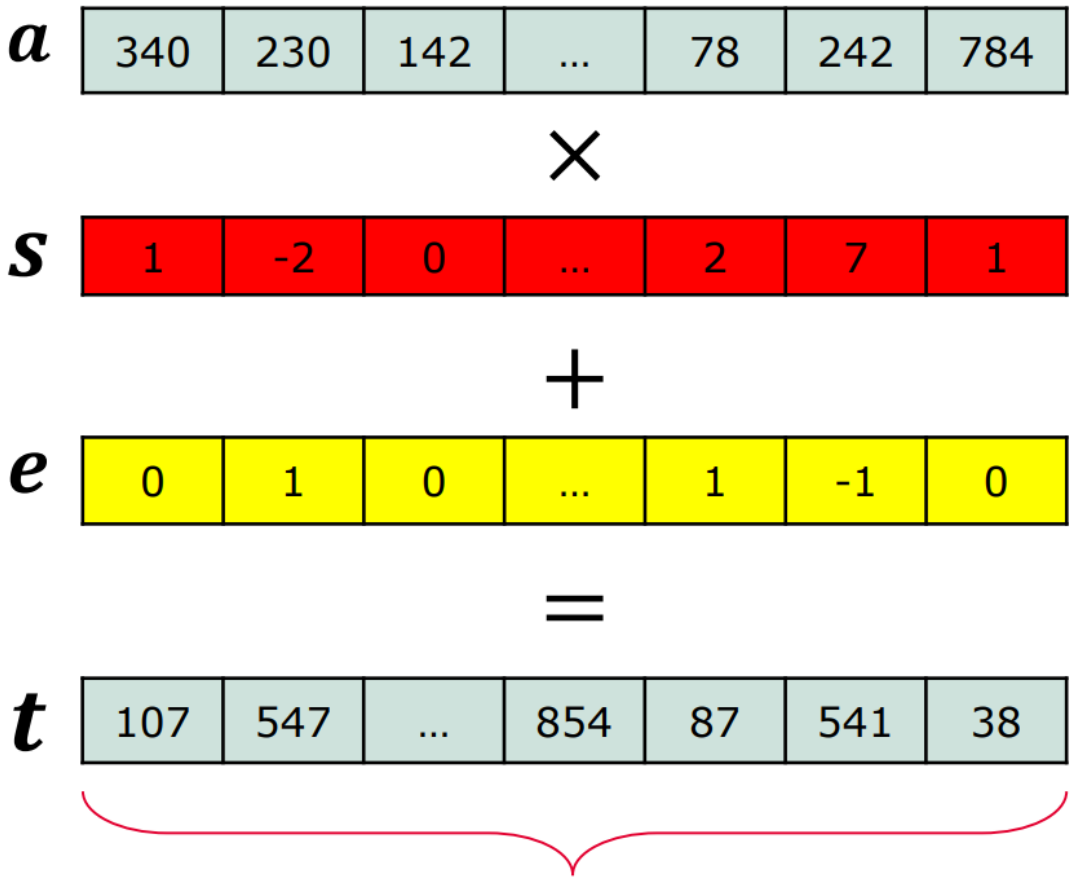
⇒ 전체 개인 키 복구

- **CCA 보안 격자 기반 PKE 및 KEM 체계에 대한 일반 사이드 채널 공격**
- NIST 표준화 과정의 두 번째 라운드에 있는 격자 기반 PKE / KEM에 적용

⇒ 격자 기반 방식과 FO 변환 내에서 사용되는 오류 수정 코드 내에서 EM 측 채널 취약성을 식별

⇒ 디코딩 알고리즘의 출력에 대한 정보를 통하여 전체 키 복구 함

Ring-LWE(Ring learning with errors)



다항식 $t(x) = (a(x) \cdot s(x)) + e(x)$

$a(x)$와 $t(x)$가 주어졌을 때

$s(x)$를 복구하는 것이 어렵다는 것을 사용

Encryption

$$\mathcal{R}_q = \mathbb{Z}_q[x]/\langle x^n + 1\rangle$$

r2
(private key)

(a,p) p = r1 − a x r2
(public key)

m
(encoded message)
e1,e2,e3 ← X n

c1 = a x e1 + e2 (cipher text 1)

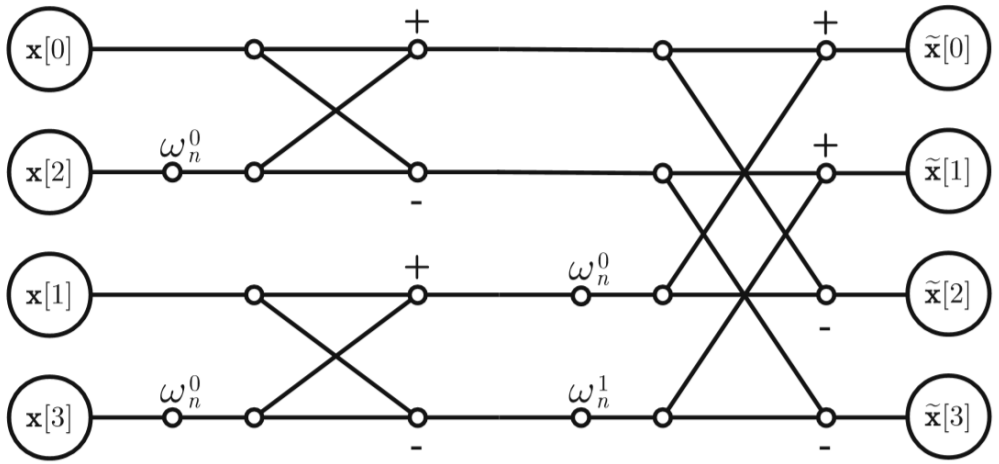
c2 = p x e1 + e3 + m ← (cipher text 2)

alice ⟵ **bob**

m = c1r2 + c2

Number Theoretic Transform

- m = c1 x r2 + c2
- 비효율적 > $\mathcal{O}(n^2)$
- a * b = INTT(NTT(a) ∗ NTT(b))



Number Theoretic Transform

m = c1 x r2 + c2

$$\overline{\mathbf{m}} = \mathrm{INTT}(\ \tilde{\mathbf{c}}_1 * \tilde{\mathbf{r}}_2 \ + \ \tilde{\mathbf{c}}_2\ )$$

⇒ Faster: $\mathcal{O}(n \log n)$

$$\overline{\mathbf{m}} = \mathrm{INTT}(\underbrace{\tilde{\mathbf{c}}_1 * \tilde{\mathbf{r}}_2 + \tilde{\mathbf{c}}_2}_{\mathcal{I}_{\mathrm{INTT}}}) \mod q$$

$$\tilde{\mathbf{r}}_2 = (\mathcal{I}_{\mathrm{INTT}} - \tilde{\mathbf{c}}_2) * \tilde{\mathbf{c}}_1^{-1} \mod q$$

공격

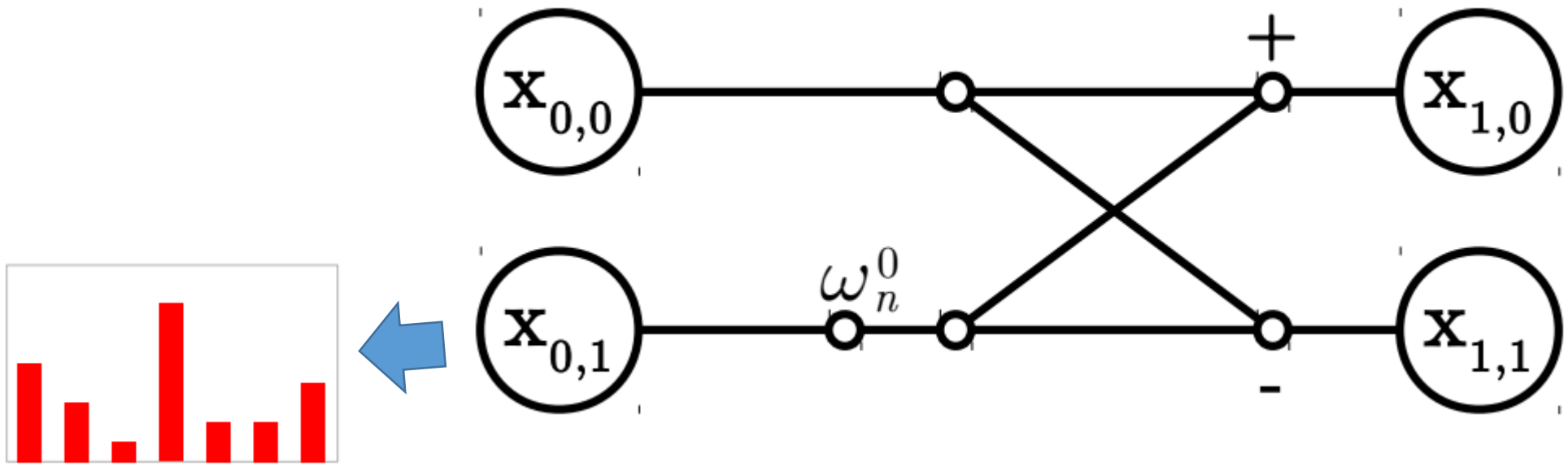
1. INTT 동작의 단일 트레이스 TA

2. 신뢰 전파 (Belief Propagation)를 통한 누출 조합

3. 격자 디코딩을 통한 키 복구

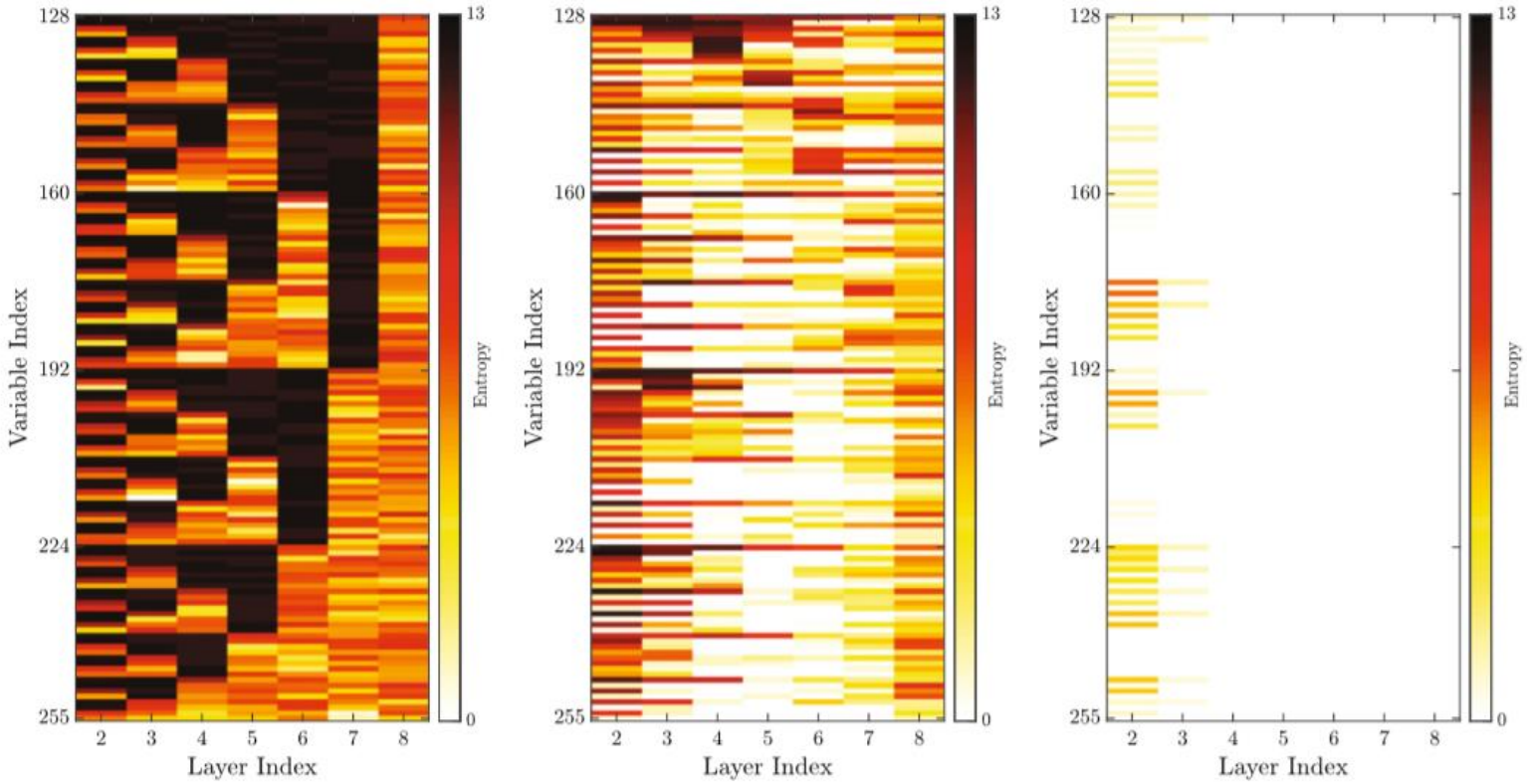
INTT 동작의 단일 트레이스 TA

- 먼저 프로파일링을 수행 한 다음 실제 공격에 대해 각 모듈 식 연산에서 기록 된 템플릿을 일치시켜 각 계수에 대한 확률 분포 획득



신뢰 전파 (Belief Propagation)를 통한 누출 조합

- 그래프 모델상에서 메시지 전달 알고리즘. 관측한 노드의 상태를 토대로 아직 관측하지 않은 노드의 주변분포를 각각 계산
- 모든 (I)NTT에 대하여 반복 조건부 확률을 사용하여 모든 누출 지점의 정보를 효율적으로 결합, 반복
- 네트워크가 수렴되었으며 거의 모든 중간값이 매우 높은 확률로 결정됨.



격자 디코딩을 통한 키 복구

- r2는 위의 시스템과 공개 키에 포함 된 정보 (a, p)를 결합하여 최종적으로 복구

- 격자 디코딩 성공률은 1
- ⇒ 공격 성공률은 1

- 마스크 구현에 대해서도 동일

논문 Results

- 충분한 누출이 발생하면 단일 암호 디코딩의 사이드 채널 관찰만으로 개인 키를 복구 할 수 있는 격자 기반 암호화에 대한 새로운 사이드 채널 공격을 제시
- 공격은 거의 모든 효율적인 격자 기반 암호화 구현을 위한 필수 구성 요소 인 NTT (Number Theoretic Transform)의 계산을 목표
- NTT 전체에서 모든 작업의 정보 (중간 가능성)를 결합합니다. NTT의 FFT와 유사한 구조를 그래프로 표현한 다음 신념 전파 알고리즘 (BP)을 적용
- 비밀 중간 값에 대한 지식을 공개 키와 결합하여 공격
- 마스킹을 사용하더라도 공격의 성능이 비슷하게 나타남

논문 Results

- NTT의 규칙적인 구조는 전체 암호 디코딩 프로세스의 누출을 효율적으로 결합 할 수 있습니다.
- NTT를 사용하는 격자 기반 암호화의 다른 구현에 적용 할 수 있습니다.
- 마스킹은 DPA에 효과적이지만 공격을 막지는 못합니다.
- 따라서 추가 대책이 구현되어야 한다.

Generic Side-channel attacks on CCA-secure lattice-based PKE and KEM schemes

- LWE / LWR 기반 체계에 사용 된 ECC (Error Correcting Code) 사이드 채널 취약성을 식별하여 암호 디코딩 작업에서 출력되는 코드 워드의 값을 구별 할 수 있었음

- ECC를 사용하지 않는 후지사키-오카모토 (Fujisaki-Okamoto) 변환에서 암호 디코딩 된 메시지에 대한 채널 정보를 제공하는 다중 격자 기반에서도 유사한 취약점을 발견

- NIST 표준화 과정의 두 번째 라운드에 있는 약 6 개의 CCA 보안 격자 기반 공개키에 적용됨

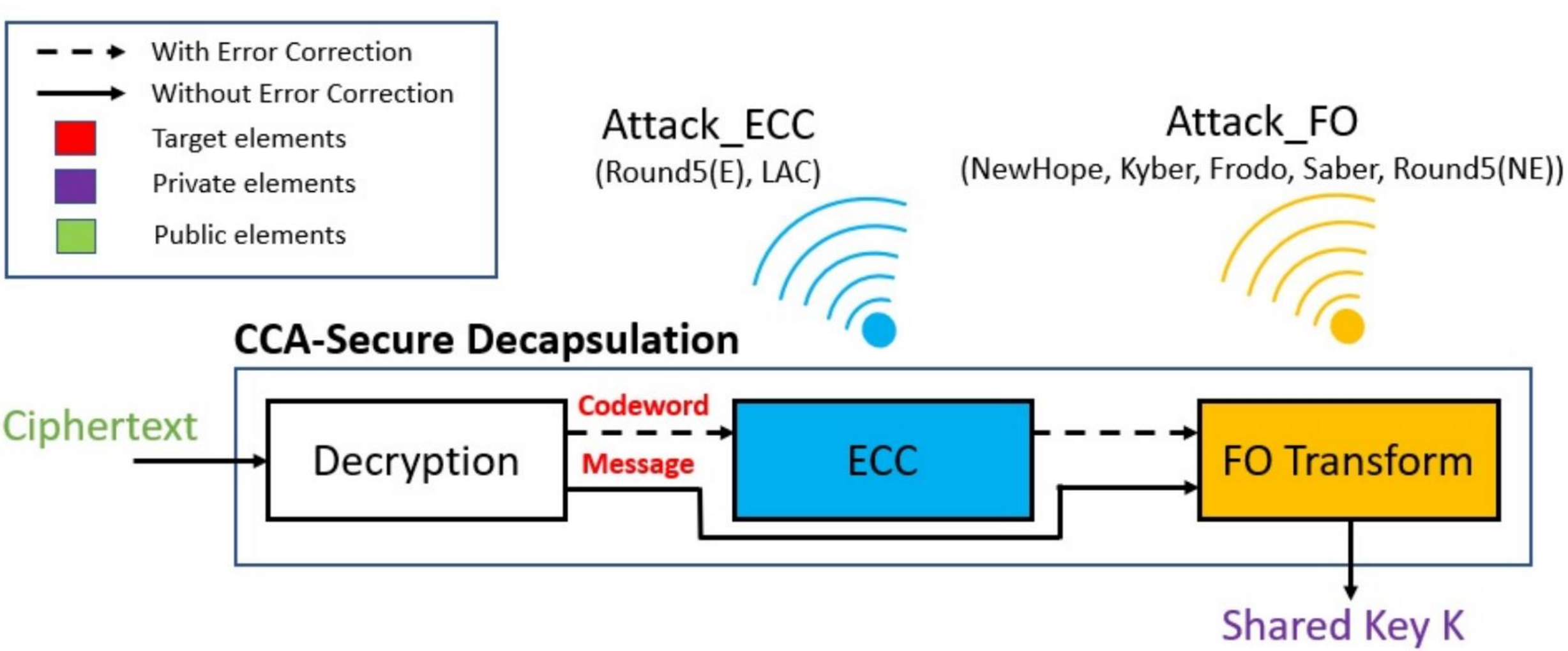
Generic Side-channel attacks on CCA-secure lattice-based PKE and KEM schemes

- 공개키 체계는 관련된 두 당사자가 공유 비밀 키를 설정하지 못할 때 실패 이벤트가 발생할 수 있습니다.

- 이러한 점을 설계자들은 CCA에 대한 보안을 달성하기위한 핵심 요구 사항으로 작용하고 있음

- LAC 및 Round5와 같은 특정 LWE / LWR 기반 체계는 디코딩 된 메시지의 오류를 수정하여 디코딩 실패를 인위적으로 줄이기 위해 ECC (오류 수정 코드) 사용을 선택

Generic Side-channel attacks on CCA-secure lattice-based PKE and KEM schemes



논문 Results

- 격자 기반 방식과 FO 변환 내에서 사용되는 오류 수정 코드 내에서 EM 측 채널 취약성을 식별
- 디코딩 알고리즘의 출력에 대한 정보를 유출하여 전체 키 복구 함
- ECC를 대상으로 하는 공격, ECC를 사용하지 않는 체계에서 FO 변환은 부채널 보호 구현을 통해 보호 할 수 있습니다.
- 격자 기반 암호화에 사용되는 ECC를 위한 효율적인 마스킹 기법은 아직 발명되지 않았다.
- CCA 보안 LWE / LWR 기반 PKE 및 KEM을 보호하기위한 효율적인 마스킹 전략과 함께 오류 수정 코드의 사이드 채널 내성 구현에 대한 관심이 필요

Q & A