KU LEUVEN

How Dangerous are Decryption Failures in Lattice-based Encryption?

Jan-Pieter D'Anvers

20 november 2019

1 Outline

1. Introduction
2. How to find 1st failure
3. How to find next failure
4. Recovering the secret
5. Conclusion

KU LEUVEN

1 LWE hard problem

- LWE problem
- $\boldsymbol{A} \leftarrow \mathcal{U}(\mathbb{Z}_q^{n \times n})$
- $\boldsymbol{s}, \boldsymbol{e} \leftarrow \mathsf{small}(\mathbb{Z}_q^{n \times k})$

1 LWE hard problem

- LWE problem
- $\boldsymbol{A} \leftarrow \mathcal{U}(\mathbb{Z}_q^{n\times n})$
- $\boldsymbol{s}, \boldsymbol{e} \leftarrow \mathsf{small}(\mathbb{Z}_q^{n\times k})$
- $(\boldsymbol{A}, \boldsymbol{b} = \boldsymbol{A}\cdot\boldsymbol{s} + \boldsymbol{e})$

1 LWE based encryption

Alice Bob

$$\boldsymbol{A} \leftarrow \mathcal{U}(\mathbb{Z}_q^{n \times n})$$

$$\boldsymbol{s}, \boldsymbol{e} \leftarrow \mathsf{small}(\mathbb{Z}_q^{n \times k})$$

$$\boldsymbol{b} = \boldsymbol{A} \cdot \boldsymbol{s} + \boldsymbol{e} \qquad \xrightarrow{\boldsymbol{b}, \boldsymbol{A}}$$

KU LEUVEN

1 LWE based encryption

Alice		Bob
$\boldsymbol{A} \leftarrow \mathcal{U}(\mathbb{Z}_q^{n\times n})$		
$\boldsymbol{s}, \boldsymbol{e} \leftarrow \mathsf{small}(\mathbb{Z}_q^{n\times k})$		
$\boldsymbol{b} = \boldsymbol{A} \cdot \boldsymbol{s} + \boldsymbol{e}$	$\xrightarrow{\boldsymbol{b}, \boldsymbol{A}}$	$\boldsymbol{s}', \boldsymbol{e}', \boldsymbol{e}'' \leftarrow \mathsf{small}(\mathbb{Z}_q^{n\times k})$
		$\boldsymbol{b}' = \boldsymbol{A}^T \cdot \boldsymbol{s}' + \boldsymbol{e}'$
	$\xleftarrow{\boldsymbol{b}', v'}$	

1 LWE based encryption

Alice		Bob
$\boldsymbol{A} \leftarrow \mathcal{U}(\mathbb{Z}_q^{n\times n})$		
$\boldsymbol{s}, \boldsymbol{e} \leftarrow \mathsf{small}(\mathbb{Z}_q^{n\times k})$		
$\boldsymbol{b} = \boldsymbol{A} \cdot \boldsymbol{s} + \boldsymbol{e}$	$\xrightarrow{\boldsymbol{b}, \boldsymbol{A}}$	$\boldsymbol{s}', \boldsymbol{e}', \boldsymbol{e}'' \leftarrow \mathsf{small}(\mathbb{Z}_q^{n\times k})$
		$\boldsymbol{b}' = \boldsymbol{A}^T \cdot \boldsymbol{s}' + \boldsymbol{e}'$
	$\xleftarrow{\boldsymbol{b}', v'}$	$v' = \boldsymbol{b}^T \cdot \boldsymbol{s}' + \boldsymbol{e}'' + \lfloor \frac{q}{2} \rceil m$

1 LWE based encryption

$$
\begin{array}{lcl}
\text{Alice} & & \text{Bob} \\
 & & \\
\boldsymbol{A} \leftarrow \mathcal{U}(\mathbb{Z}_q^{n \times n}) & & \\
\boldsymbol{s}, \boldsymbol{e} \leftarrow \mathsf{small}(\mathbb{Z}_q^{n \times k}) & & \\
\boldsymbol{b} = \boldsymbol{A} \cdot \boldsymbol{s} + \boldsymbol{e} & \xrightarrow{\boldsymbol{b}, \boldsymbol{A}} & \boldsymbol{s}', \boldsymbol{e}', \boldsymbol{e}'' \leftarrow \mathsf{small}(\mathbb{Z}_q^{n \times k}) \\
 & & \boldsymbol{b}' = \boldsymbol{A}^T \cdot \boldsymbol{s}' + \boldsymbol{e}' \\
v = \boldsymbol{b}'^T \cdot \boldsymbol{s} & \xleftarrow{\boldsymbol{b}', v'} & v' = \boldsymbol{b}^T \cdot \boldsymbol{s}' + \boldsymbol{e}'' + \lfloor \frac{q}{2} \rceil m \\
m' = \lfloor \lfloor \frac{2}{q} \rceil (v' - v) \rceil & &
\end{array}
$$

1 LWE based encryption

Alice		Bob
$\boldsymbol{A} \leftarrow \mathcal{U}(\mathbb{Z}_q^{n\times n})$		
$\boldsymbol{s}, \boldsymbol{e} \leftarrow \mathsf{small}(\mathbb{Z}_q^{n\times k})$		
$\boldsymbol{b} = \boldsymbol{A}\cdot\boldsymbol{s} + \boldsymbol{e}$	$\xrightarrow{\boldsymbol{b}, \boldsymbol{A}}$	$\boldsymbol{s}', \boldsymbol{e}', \boldsymbol{e}'' \leftarrow \mathsf{small}(\mathbb{Z}_q^{n\times k})$
		$\boldsymbol{b}' = \boldsymbol{A}^T\cdot\boldsymbol{s}' + \boldsymbol{e}'$
$v = \boldsymbol{b}'^T\cdot\boldsymbol{s}$	$\xleftarrow{\boldsymbol{b}', v'}$	$v' = \boldsymbol{b}^T\cdot\boldsymbol{s}' + \boldsymbol{e}'' + \lfloor \frac{q}{2}\rceil m$
$m' = \lfloor\lfloor \frac{2}{q}\rceil(v' - v)\rceil$		

$$m' = \lfloor \frac{2}{q}(\boldsymbol{s}'^T\boldsymbol{A}\boldsymbol{s} + \boldsymbol{e}^T\boldsymbol{s}' + \boldsymbol{e}'' + \lfloor\frac{q}{2}\rceil m - \boldsymbol{s}'^T\boldsymbol{A}\boldsymbol{s} - \boldsymbol{e}'^T\boldsymbol{s})\rceil$$

KU LEUVEN

1 LWE based encryption

Alice		Bob
$\boldsymbol{A} \leftarrow \mathcal{U}(\mathbb{Z}_q^{n\times n})$		
$\boldsymbol{s}, \boldsymbol{e} \leftarrow \mathsf{small}(\mathbb{Z}_q^{n\times k})$		
$\boldsymbol{b} = \boldsymbol{A} \cdot \boldsymbol{s} + \boldsymbol{e}$	$\xrightarrow{\boldsymbol{b}, \boldsymbol{A}}$	$\boldsymbol{s}', \boldsymbol{e}', \boldsymbol{e}'' \leftarrow \mathsf{small}(\mathbb{Z}_q^{n\times k})$
		$\boldsymbol{b}' = \boldsymbol{A}^T \cdot \boldsymbol{s}' + \boldsymbol{e}'$
$v = \boldsymbol{b}'^T \cdot \boldsymbol{s}$	$\xleftarrow{\boldsymbol{b}', v'}$	$v' = \boldsymbol{b}^T \cdot \boldsymbol{s}' + \boldsymbol{e}'' + \lfloor \frac{q}{2} \rceil m$
$m' = \lfloor \lfloor \frac{2}{q} \rceil (v' - v) \rceil$		

$$m' = \lfloor \frac{2}{q} (\cancel{\boldsymbol{s}'^T \boldsymbol{A}\boldsymbol{s}} + \boldsymbol{e}^T \boldsymbol{s}' + \boldsymbol{e}'' + \lfloor \frac{q}{2} \rceil m - \cancel{\boldsymbol{s}'^T \boldsymbol{A}\boldsymbol{s}} - \boldsymbol{e}'^T \boldsymbol{s}) \rceil$$

1 Failures

- failure if: $||\boldsymbol{e}^T\boldsymbol{s}' + \boldsymbol{e}'' - \boldsymbol{e}'^T\boldsymbol{s}||_\infty \geq \frac{q}{4}$
- typically small failure probability $\delta \approx 2^{-128}$

1 How calculated

- calculate some bounds
- assume Gaussian and calculate σ and μ
- calculate pdf exhaustively

1 Variations

- polynomials, vectors/matrices of polynomials $\mathbb{Z}_q[X]/(X^n+1)$
- learning with rounding
- NTRU version, Mersenne prime, Threebears

1 Chosen ciphertext attacks

- Easy to attack with chosen ciphertexts
- We can not check the adversary

1 FO-transform

Alice		Bob
$\boldsymbol{A} \leftarrow \mathcal{U}(\mathbb{Z}_q^{n\times n})$		
$\boldsymbol{s}, \boldsymbol{e} \leftarrow \mathsf{small}(\mathbb{Z}_q^{n\times k})$		$m \leftarrow \mathcal{U}(\{0,1\}^{256})$
$\boldsymbol{b} = \boldsymbol{A} \cdot \boldsymbol{s} + \boldsymbol{e}$	$\xrightarrow{\boldsymbol{b}, \boldsymbol{A}}$	

KU LEUVEN

1 FO-transform

Alice		Bob
$\boldsymbol{A} \leftarrow \mathcal{U}(\mathbb{Z}_q^{n\times n})$		
$\boldsymbol{s}, \boldsymbol{e} \leftarrow \mathsf{small}(\mathbb{Z}_q^{n\times k})$		$m \leftarrow \mathcal{U}(\{0,1\}^{256})$
$\boldsymbol{b} = \boldsymbol{A} \cdot \boldsymbol{s} + \boldsymbol{e}$	$\xrightarrow{\boldsymbol{b}, \boldsymbol{A}}$	$\boldsymbol{s}', \boldsymbol{e}', \boldsymbol{e}'' \leftarrow \mathsf{small}(\mathbb{Z}_q^{n\times k}; \mathcal{H}(m))$
		$\boldsymbol{b}' = \boldsymbol{A}^T \cdot \boldsymbol{s}' + \boldsymbol{e}'$
	$\xleftarrow{\boldsymbol{b}', v'}$	

1 FO-transform

Alice		Bob
$\boldsymbol{A} \leftarrow \mathcal{U}(\mathbb{Z}_q^{n \times n})$		
$\boldsymbol{s}, \boldsymbol{e} \leftarrow \mathsf{small}(\mathbb{Z}_q^{n \times k})$		$m \leftarrow \mathcal{U}(\{0,1\}^{256})$
$\boldsymbol{b} = \boldsymbol{A} \cdot \boldsymbol{s} + \boldsymbol{e}$	$\xrightarrow{\boldsymbol{b}, \boldsymbol{A}}$	$\boldsymbol{s}', \boldsymbol{e}', \boldsymbol{e}'' \leftarrow \mathsf{small}(\mathbb{Z}_q^{n \times k}; \mathcal{H}(m))$
		$\boldsymbol{b}' = \boldsymbol{A}^T \cdot \boldsymbol{s}' + \boldsymbol{e}'$
	$\xleftarrow{\boldsymbol{b}', v'}$	$v' = \boldsymbol{b}^T \cdot \boldsymbol{s}' + \boldsymbol{e}'' + \lfloor \frac{q}{2} \rceil m$

1 FO-transform

Alice		Bob
$\boldsymbol{A} \leftarrow \mathcal{U}(\mathbb{Z}_q^{n\times n})$		
$\boldsymbol{s}, \boldsymbol{e} \leftarrow \mathsf{small}(\mathbb{Z}_q^{n\times k})$		$m \leftarrow \mathcal{U}(\{0,1\}^{256})$
$\boldsymbol{b} = \boldsymbol{A} \cdot \boldsymbol{s} + \boldsymbol{e}$	$\xrightarrow{\boldsymbol{b}, \boldsymbol{A}}$	$\boldsymbol{s}', \boldsymbol{e}', \boldsymbol{e}'' \leftarrow \mathsf{small}(\mathbb{Z}_q^{n\times k}; \mathcal{H}(m))$
		$\boldsymbol{b}' = \boldsymbol{A}^T \cdot \boldsymbol{s}' + \boldsymbol{e}'$
$v = \boldsymbol{b}'^T \cdot \boldsymbol{s}$	$\xleftarrow{\boldsymbol{b}', v'}$	$v' = \boldsymbol{b}^T \cdot \boldsymbol{s}' + \boldsymbol{e}'' + \lfloor \frac{q}{2} \rceil m$
$m' = \lfloor \lfloor \frac{2}{q} \rceil (v' - v) \rceil$		
$\mathsf{check}(m', \boldsymbol{b}', v')$		

KU LEUVEN

1 Error term

- let's group secret and ciphertext terms:

$$\boldsymbol{S} = \begin{pmatrix} -\boldsymbol{s} \\ \boldsymbol{e} \end{pmatrix} \quad \boldsymbol{C} = \begin{pmatrix} \boldsymbol{e}' \\ \boldsymbol{s}' \end{pmatrix}$$

1 Error term

- let's group secret and ciphertext terms:
  $\boldsymbol{S} = \begin{pmatrix} -\boldsymbol{s} \\ \boldsymbol{e} \end{pmatrix} \quad \boldsymbol{C} = \begin{pmatrix} \boldsymbol{e}' \\ \boldsymbol{s}' \end{pmatrix}$
- failure if:
  $||\boldsymbol{S}^T \boldsymbol{C} + \boldsymbol{e}''||_\infty \geq \frac{q}{4}$

2 Outline

1. Introduction
2. How to find 1st failure
3. How to find next failure
4. Recovering the secret
5. Conclusion

KU LEUVEN

2 Attack model

- precomputation: Grover's algorithm

2 Attack model

- precomputation: Grover's algorithm
- only classical access to decryption oracle

2 Failure boosting

- find weak ciphertexts
- query weak ciphertexts

2 Failure boosting

- find weak ciphertexts
  - generate ciphertext
  - estimate failure probability
  - accept if higher than f_t
- query weak ciphertexts

2 Failure boosting

- find weak ciphertexts α
  - generate ciphertext
  - estimate failure probability
  - accept if higher than f_t
- query weak ciphertexts β

2 Failure boosting

- find weak ciphertexts α
  - generate ciphertext
  - estimate failure probability
  - accept if higher than f_t
- query weak ciphertexts β

- **general model for schemes with decryption failures**
- works if:
  - can estimate failure probability of ciphertexts
  - estimated failure probability of ciphertexts is different

2 Failure boosting technical

- $\alpha = P[p_e(c) > f_t]$
- probability of finding weak ciphertext

2 Failure boosting technical

- $\alpha = P[p_e(c) > f_t]$
- probability of finding weak ciphertext

- $\beta = P[c \text{ fails} | p_e(c) > f_t]$
- failure probability of weak ciphertext

2 Lattice based schemes: simple case

- $||\boldsymbol{S}^T\boldsymbol{C} + \boldsymbol{e}''||_\infty \geq \frac{q}{4}$

2 Lattice based schemes: simple case

- $|\boldsymbol{S}^T\boldsymbol{C}| \geq \frac{q}{4}$
- $||\boldsymbol{S}^T||_2||\boldsymbol{C}||_2|\cos(\theta)| \geq \frac{q}{4}$

2 Lattice based schemes: matrices

- $||\boldsymbol{S}^T\boldsymbol{C}||_\infty \geq \frac{q}{4}$

2 Lattice based schemes: matrices

- $||\boldsymbol{S}^T\boldsymbol{C}||_\infty \geq \frac{q}{4}$

- Gaussian assumption
- $\mu = 0$
- σ

$$\begin{aligned} Var(\,(\boldsymbol{S}^T\boldsymbol{C})_{ij}\,) &= Var(\,\sum_k \boldsymbol{S}_{kj}\boldsymbol{C}_{ki}\,) \\ &= \sum_k \boldsymbol{C}_{ki}^2 \cdot Var(\boldsymbol{S}_{kj}) \\ &= ||\boldsymbol{C}_{k:}||_2^2 \cdot \sigma_s^2 \end{aligned}$$

2 How to calculate

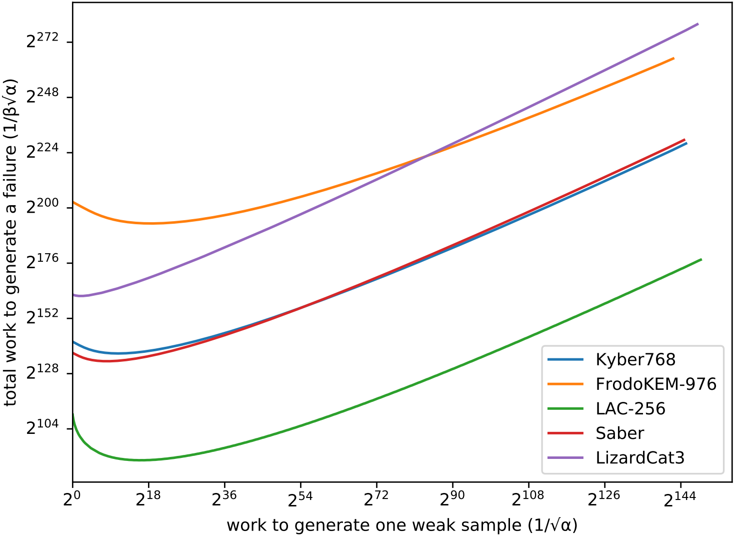
l	$P[\|\|\boldsymbol{C}\|\|_2 = l]$	$P[fail\|\|\|\boldsymbol{C}\|\|_2 = l]$
100	2^{-30}	2^{-100}
101	2^{-30}	2^{-99}
102	2^{-29}	2^{-98}
103	2^{-29}	2^{-97}

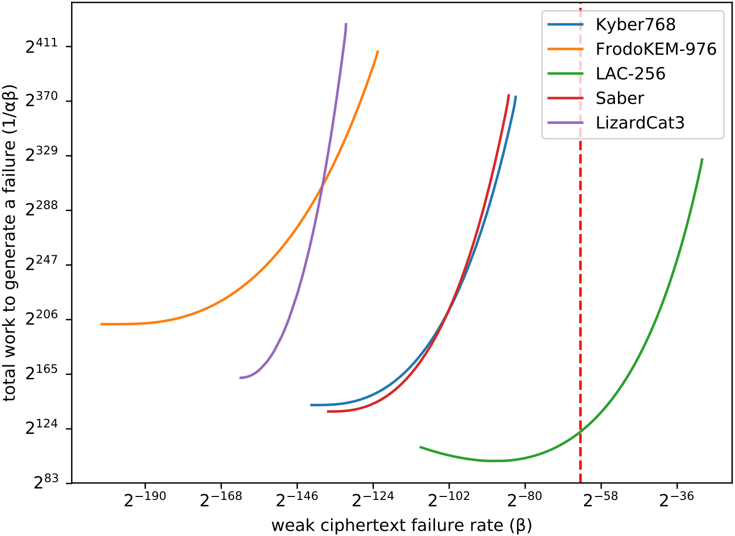
2 How to calculate

l	$P[\|\|\boldsymbol{C}\|\|_2 = l]$	$P[fail\|\|\|\boldsymbol{C}\|\|_2 = l]$
100	2^{-30}	2^{-100}
101	2^{-30}	2^{-99}
102	2^{-29}	2^{-98}
103	2^{-29}	2^{-97}
	α	β

2 How to calculate

l	$P[\|\|\boldsymbol{C}\|\|_2 = l]$	$P[fail\|\|\|\boldsymbol{C}\|\|_2 = l]$
100	2^{-30}	2^{-100}
101	2^{-30}	2^{-99}
102	2^{-29}	2^{-98}
103	2^{-29}	2^{-97}
	α	β


total work to generate a failure (1/β√α)
work to generate one weak sample (1/√α)
2^{272}
2^{248}
2^{224}
2^{200}
2^{176}
2^{152}
2^{128}
2^{104}
2^{0}
2^{18}
2^{36}
2^{54}
2^{72}
2^{90}
2^{108}
2^{126}
2^{144}
Kyber768
FrodoKEM-976
LAC-256
Saber
LizardCat3


Kyber768
FrodoKEM-976
LAC-256
Saber
LizardCat3
total work to generate a failure (1/αβ)
2^{411}
2^{370}
2^{329}
2^{288}
2^{247}
2^{206}
2^{165}
2^{124}
2^{83}
2^{-190}
2^{-168}
2^{-146}
2^{-124}
2^{-102}
2^{-80}
2^{-58}
2^{-36}
weak ciphertext failure rate (β)

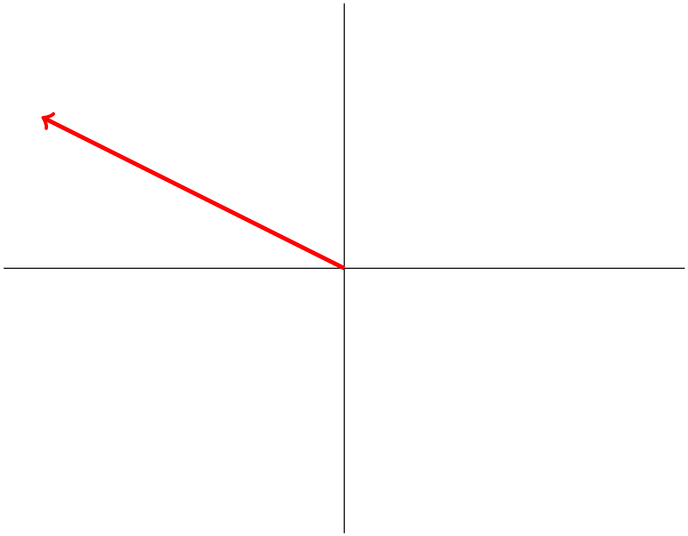
3 Outline

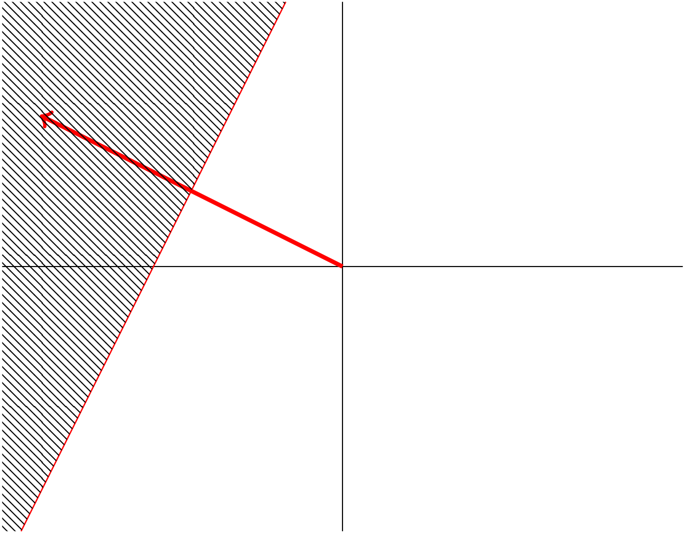
1. Introduction
2. How to find 1st failure
3. How to find next failure
4. Recovering the secret
5. Conclusion

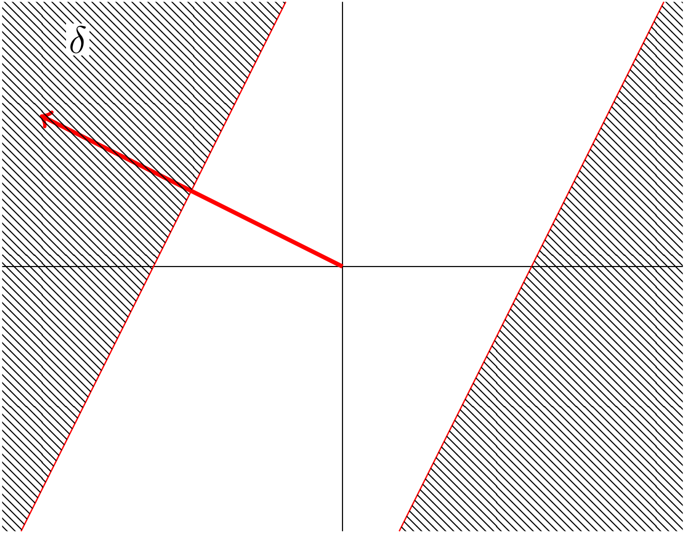
KU LEUVEN

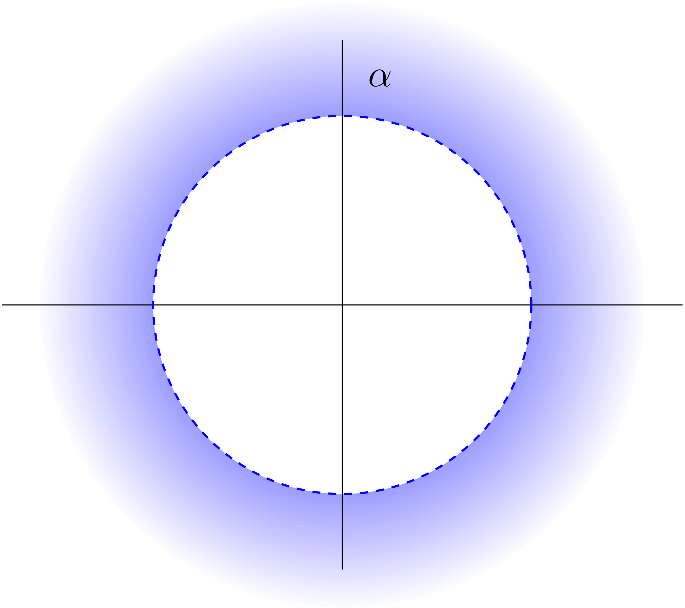
3 Failure boosting

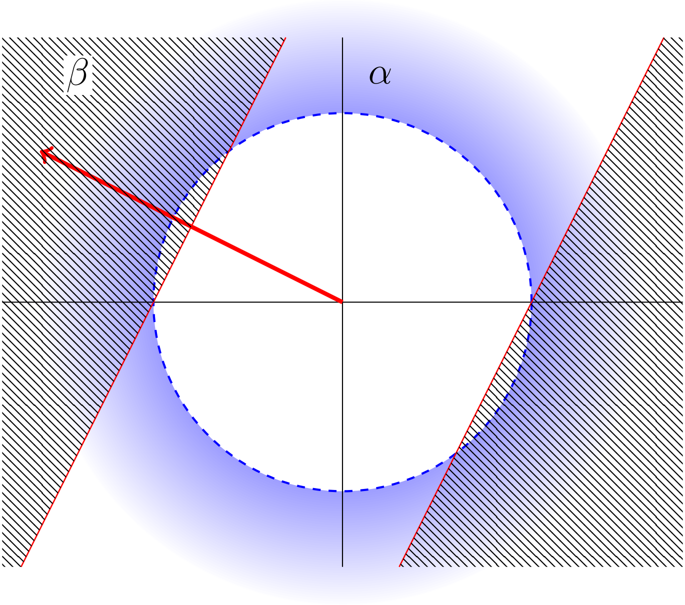
- $\boldsymbol{S}^T\boldsymbol{C} = ||\boldsymbol{S}||_2 \cdot ||\boldsymbol{C}||_2 \cos\theta$



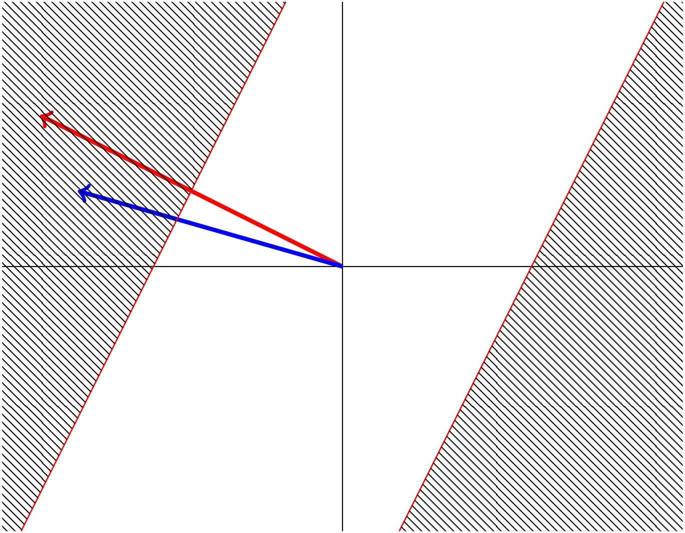


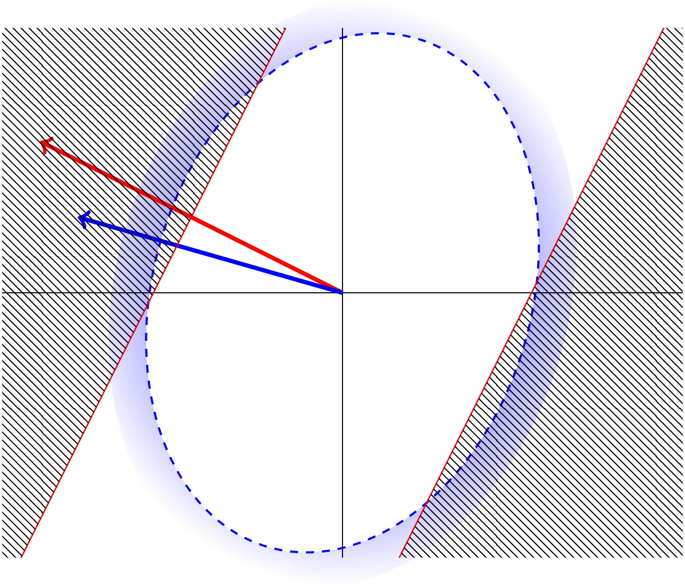

δ


α



β
α





3 Find next failures

- $|\boldsymbol{S}^T \boldsymbol{C}| \geq \frac{q}{4}$
- $\boldsymbol{E}$

3 Find next failures

- $|\boldsymbol{S}^T\boldsymbol{C}| \geq \frac{q}{4}$
- $\boldsymbol{E}$

- $|\boldsymbol{S}_{\parallel}^T\boldsymbol{C}_{\parallel} + \boldsymbol{S}_{\perp}^T\boldsymbol{C}_{\perp} + \boldsymbol{S}_{\parallel}^T\boldsymbol{C}_{\perp} + \boldsymbol{S}_{\perp}^T\boldsymbol{C}_{\parallel}| \geq \frac{q}{4}$

3 Find next failures

- $|\boldsymbol{S}^T\boldsymbol{C}| \geq \frac{q}{4}$
- $\boldsymbol{E}$

- $|\boldsymbol{S}_{\parallel}^T\boldsymbol{C}_{\parallel} + \boldsymbol{S}_{\perp}^T\boldsymbol{C}_{\perp} + \boldsymbol{S}_{\parallel}^T\boldsymbol{C}_{\perp} + \boldsymbol{S}_{\perp}^T\boldsymbol{C}_{\parallel}| \geq \frac{q}{4}$
- $|\boldsymbol{S}_{\parallel}^T\boldsymbol{C}_{\parallel} + \boldsymbol{S}_{\perp}^T\boldsymbol{C}_{\perp}| \geq \frac{q}{4}$

3 Find next failures

- $|\boldsymbol{S}^T\boldsymbol{C}| \geq \frac{q}{4}$
- $\boldsymbol{E}$

- $|\boldsymbol{S}_{\|}^T\boldsymbol{C}_{\|} + \boldsymbol{S}_{\perp}^T\boldsymbol{C}_{\perp} + \boldsymbol{S}_{\|}^T\boldsymbol{C}_{\perp} + \boldsymbol{S}_{\perp}^T\boldsymbol{C}_{\|}| \geq \frac{q}{4}$
- $|\boldsymbol{S}_{\|}^T\boldsymbol{C}_{\|} + \boldsymbol{S}_{\perp}^T\boldsymbol{C}_{\perp}| \geq \frac{q}{4}$
- $\left|\begin{array}{c} ||\boldsymbol{S}_{\|}||_2 \cdot ||\boldsymbol{C}_{\|}||_2 + \\ ||\boldsymbol{S}_{\perp}||_2 \cdot ||\boldsymbol{C}_{\perp}||_2 \cos(t) \end{array}\right| \geq \frac{q}{4}$

3 Find next failures

- $|\boldsymbol{S}^T\boldsymbol{C}| \geq \frac{q}{4}$
- $\boldsymbol{E}$

- $|\boldsymbol{S}_{\|}^T\boldsymbol{C}_{\|} + \boldsymbol{S}_{\perp}^T\boldsymbol{C}_{\perp} + \boldsymbol{S}_{\|}^T\boldsymbol{C}_{\perp} + \boldsymbol{S}_{\perp}^T\boldsymbol{C}_{\|}| \geq \frac{q}{4}$
- $|\boldsymbol{S}_{\|}^T\boldsymbol{C}_{\|} + \boldsymbol{S}_{\perp}^T\boldsymbol{C}_{\perp}| \geq \frac{q}{4}$
- $\left| \begin{array}{c} ||\boldsymbol{S}_{\|}||_2 \cdot ||\boldsymbol{C}_{\|}||_2 + \\ ||\boldsymbol{S}_{\perp}||_2 \cdot ||\boldsymbol{C}_{\perp}||_2 \cos(t) \end{array} \right| \geq \frac{q}{4}$
- $\left| \begin{array}{c} ||\boldsymbol{S}||_2 \cdot ||\boldsymbol{C}||_2 \cos(\theta_{SE}) \cos(\theta_{CE}) + \\ ||\boldsymbol{S}||_2 \cdot ||\boldsymbol{C}||_2 \sin(\theta_{SE}) \sin(\theta_{CE}) \cos(t) \end{array} \right| \geq \frac{q}{4}$

3 Find next failures

- $$\left| \begin{array}{c} ||\boldsymbol{S}||_2 \cdot ||\boldsymbol{C}||_2 \cos(\theta_{SE}) \cos(\theta_{CE}) + \\ ||\boldsymbol{S}||_2 \cdot ||\boldsymbol{C}||_2 \sin(\theta_{SE}) \sin(\theta_{CE}) \cos(t) \end{array} \right| \geq \frac{q}{4}$$
- $P[\cos(t) \geq \frac{q/4 - ||\boldsymbol{S}||_2 \cdot ||\boldsymbol{C}||_2 \cos(\theta_{SE}) \cos(\theta_{CE})}{||\boldsymbol{S}||_2 \cdot ||\boldsymbol{C}||_2 \sin(\theta_{SE}) \sin(\theta_{CE})}]$

3 Find next failures

- $P[\cos(t) \geq \frac{q/4 - ||\boldsymbol{S}||_2 \cdot ||\boldsymbol{C}||_2 \cos(\theta_{SE}) \cos(\theta_{CE})}{||\boldsymbol{S}||_2 \cdot ||\boldsymbol{C}||_2 \sin(\theta_{SE}) \sin(\theta_{CE})}]$

- $||\boldsymbol{S}||_2$: independent of ciphertext

3 Find next failures

- $P[\cos(t) \geq \frac{q/4 - ||\boldsymbol{S}||_2 \cdot ||\boldsymbol{C}||_2 \cos(\theta_{SE}) \cos(\theta_{CE})}{||\boldsymbol{S}||_2 \cdot ||\boldsymbol{C}||_2 \sin(\theta_{SE}) \sin(\theta_{CE})}]$

- $||\boldsymbol{S}||_2$: independent of ciphertext
- $\cos(\theta_{SE})$: independent of ciphertext, depends on how good $\boldsymbol{E}$ is

3 Find next failures

- $P[\cos(t) \geq \frac{q/4 - ||\boldsymbol{S}||_2 \cdot ||\boldsymbol{C}||_2 \cos(\theta_{SE}) \cos(\theta_{CE})}{||\boldsymbol{S}||_2 \cdot ||\boldsymbol{C}||_2 \sin(\theta_{SE}) \sin(\theta_{CE})}]$

- $||\boldsymbol{S}||_2$: independent of ciphertext
- $\cos(\theta_{SE})$: independent of ciphertext, depends on how good $\boldsymbol{E}$ is
- $\cos(t)$: independent of ciphertext

KU LEUVEN

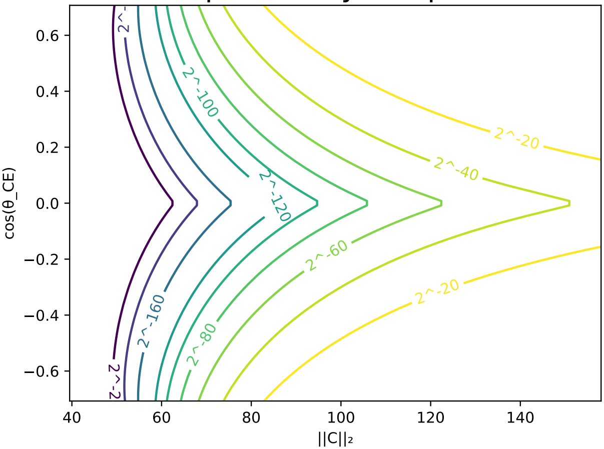
3 Find next failures

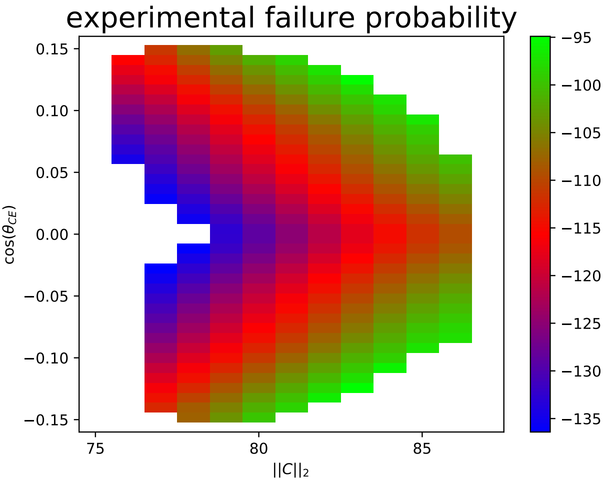
- $P[\cos(t) \geq \frac{q/4 - ||\boldsymbol{S}||_2 \cdot ||\boldsymbol{C}||_2 \cos(\theta_{SE}) \cos(\theta_{CE})}{||\boldsymbol{S}||_2 \cdot ||\boldsymbol{C}||_2 \sin(\theta_{SE}) \sin(\theta_{CE})}]$

- $||\boldsymbol{S}||_2$: independent of ciphertext
- $\cos(\theta_{SE})$: independent of ciphertext, depends on how good $\boldsymbol{E}$ is
- $\cos(t)$: independent of ciphertext

- $||\boldsymbol{C}||_2, \cos(\theta_{CE})$: ciphertext dependent

failure probability of ciphertexts




experimental failure probability
0.15
0.10
0.05
0.00
−0.05
−0.10
−0.15
cos(θ_CE)
75
80
85
||C||₂
−95
−100
−105
−110
−115
−120
−125
−130
−135

KU LEUVEN

3 problem with matrices/polynomials

- $||\boldsymbol{S}^T\boldsymbol{C}||_\infty \geq \frac{q}{4}$
- how to use this vector notation?
- what coefficient/position failed?

3 problem with matrices/polynomials

- $||\boldsymbol{S}^T\boldsymbol{C}||_\infty \geq \frac{q}{4}$
- how to use this vector notation?
- what coefficient/position failed?

KU LEUVEN

3 problem with matrices/polynomials

$$\boldsymbol{S} = \begin{bmatrix} s_{0,0} + s_{0,1}X + s_{0,2}X^2 \\ s_{1,0} + s_{1,1}X + s_{1,2}X^2 \end{bmatrix}, \quad \boldsymbol{C} = \begin{bmatrix} c_{0,0} + c_{0,1}X + c_{0,2}X^2 \\ c_{1,0} + c_{1,1}X + c_{1,2}X^2 \end{bmatrix} \quad (1)$$

for a ring $\mathbb{Z}_q[X]/(X^n + 1)$

3 problem with matrices/polynomials

$$\boldsymbol{S} = \begin{bmatrix} s_{0,0} + s_{0,1}X + s_{0,2}X^2 \\ s_{1,0} + s_{1,1}X + s_{1,2}X^2 \end{bmatrix}, \quad \boldsymbol{C} = \begin{bmatrix} c_{0,0} + c_{0,1}X + c_{0,2}X^2 \\ c_{1,0} + c_{1,1}X + c_{1,2}X^2 \end{bmatrix} \tag{1}$$

for a ring $\mathbb{Z}_q[X]/(X^n + 1)$

$$\overline{\boldsymbol{S}} = \begin{bmatrix} s_{0,0} \\ s_{0,1} \\ s_{0,2} \\ s_{1,0} \\ s_{1,1} \\ s_{1,2} \end{bmatrix}, \quad \overline{\boldsymbol{C}^{(0)}} = \begin{bmatrix} c_{0,0} \\ -c_{0,2} \\ -c_{0,1} \\ c_{1,0} \\ -c_{1,2} \\ -c_{1,1} \end{bmatrix} \quad \overline{\boldsymbol{C}^{(1)}} = \begin{bmatrix} c_{0,1} \\ c_{0,0} \\ -c_{0,2} \\ c_{1,1} \\ c_{1,0} \\ -c_{1,2} \end{bmatrix} \quad \overline{\boldsymbol{C}^{(3)}} = \begin{bmatrix} -c_{0,0} \\ c_{0,2} \\ c_{0,1} \\ -c_{1,0} \\ c_{1,2} \\ c_{1,1} \end{bmatrix}$$

$C \rightarrow X^r C(X^{-1})$

3 problem with matrices/polynomials

- $\overline{\boldsymbol{S}}^T \overline{\boldsymbol{C}^{(r)}} \geq q/4$
- for $r \in [0, 2N-1]$

3 problem with matrices/polynomials

- $\overline{\boldsymbol{S}}^T \overline{\boldsymbol{C}^{(r)}} \geq q/4$
- for $r \in [0, 2N-1]$

- what r value is responsible for the failure
- how to construct $\boldsymbol{E}$?

KU LEUVEN

3 problem with matrices/polynomials

- $\overline{\boldsymbol{S}}^T \overline{\boldsymbol{C}^{(r)}} \geq q/4$
- for $r \in [0, 2N-1]$

- what r value is responsible for the failure
- how to construct $\boldsymbol{E}$?

- for 1 ciphertext: does not matter
  - $\boldsymbol{C}$ fails at $r = 5$
  - we think $r = 0$
  - now we find a $\boldsymbol{C}$ such that:
  - $\overline{\boldsymbol{C}^{(0)}}$ is aligned with $\overline{\boldsymbol{C}_*^{(0)}}$

3 problem with matrices/polynomials

- $\overline{\boldsymbol{S}}^T \overline{\boldsymbol{C}^{(r)}} \geq q/4$
- for $r \in [0, 2N-1]$

- what r value is responsible for the failure
- how to construct $\boldsymbol{E}$?

- for 2 ciphertexts: does matter!
  - we need relative position

KU LEUVEN

3 finding relative positions

- fix $r_1 = 0$ and thus $\overline{\boldsymbol{C}_1^{(0)}}$

3 finding relative positions

- fix $r_1 = 0$ and thus $\overline{\boldsymbol{C}_1^{(0)}}$

- we know $\overline{\boldsymbol{S}}^T \overline{\boldsymbol{C}_1^{(0)}} \geq q/4$
- and $\overline{\boldsymbol{S}}^T \overline{\boldsymbol{C}_2^{(r_2)}} \geq q/4$

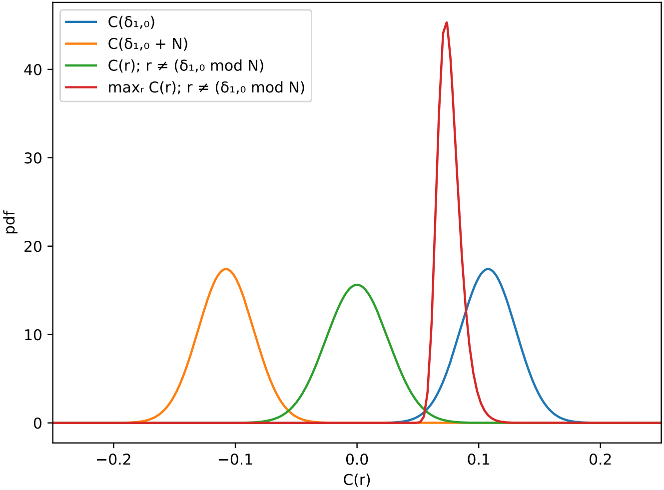
3 finding relative positions

- fix $r_1 = 0$ and thus $\overline{\boldsymbol{C}_1^{(0)}}$

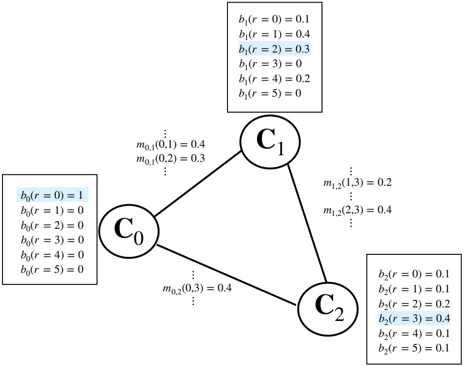
- we know $\overline{\boldsymbol{S}}^T \overline{\boldsymbol{C}_1^{(0)}} \geq q/4$
- and $\overline{\boldsymbol{S}}^T \overline{\boldsymbol{C}_2^{(r_2)}} \geq q/4$
- both $\overline{\boldsymbol{C}_1^{(0)}}$ and $\overline{\boldsymbol{C}_2^{(r_2)}}$ are correlated with $\overline{\boldsymbol{S}}$

KU LEUVEN

3 finding relative positions

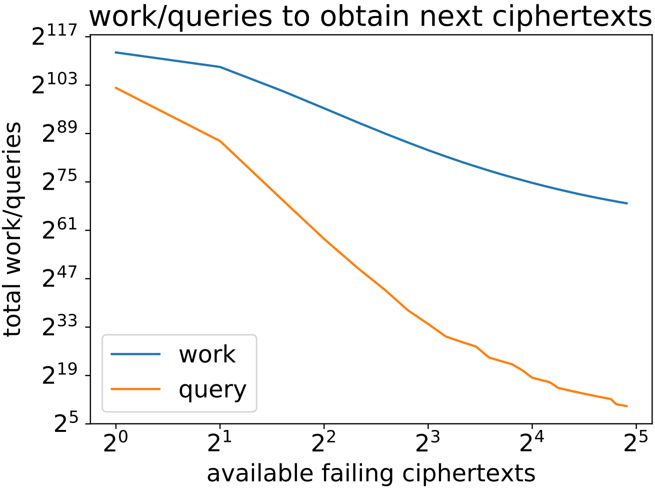


3 finding relative positions

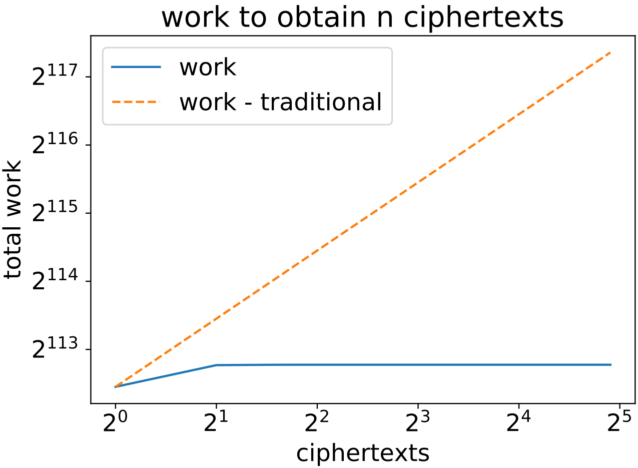


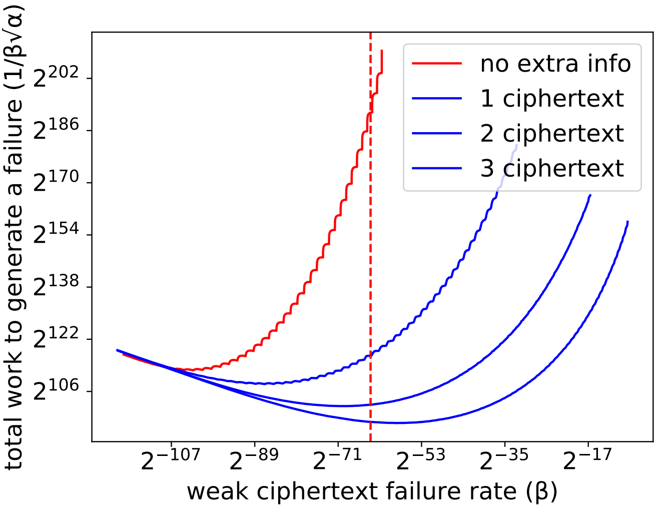
3 finding relative positions

	2 ciphertexts	3 ciphertexts	4 ciphertexts	5 ciphertexts
$P[success]$	84.0%	95.6%	$> 99.0\%$	$> 99.0\%$

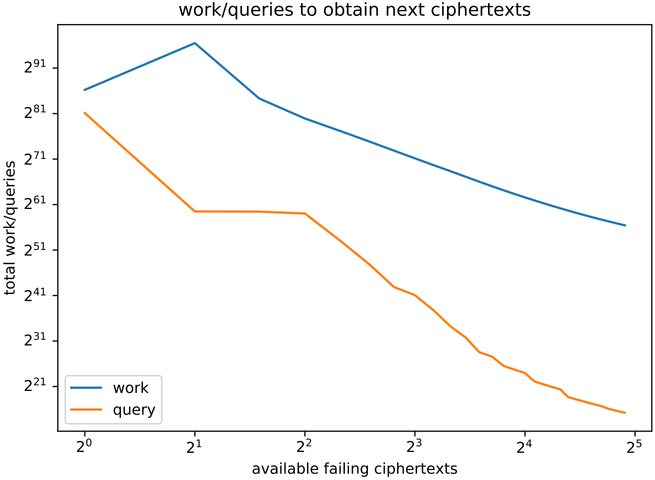


work/queries to obtain next ciphertexts
total work/queries
2^{117}
2^{103}
2^{89}
2^{75}
2^{61}
2^{47}
2^{33}
2^{19}
2^{5}
2^{0}
2^{1}
2^{2}
2^{3}
2^{4}
2^{5}
available failing ciphertexts
work
query


work to obtain n ciphertexts
work
work - traditional
total work
2^{117}
2^{116}
2^{115}
2^{114}
2^{113}
2^0
2^1
2^2
2^3
2^4
2^5
ciphertexts



total work to generate a failure (1/β√α)
2^{202}
2^{186}
2^{170}
2^{154}
2^{138}
2^{122}
2^{106}
no extra info
1 ciphertext
2 ciphertext
3 ciphertext
2^{-107}
2^{-89}
2^{-71}
2^{-53}
2^{-35}
2^{-17}
weak ciphertext failure rate (β)


work/queries to obtain next ciphertexts
total work/queries
2^{91}
2^{81}
2^{71}
2^{61}
2^{51}
2^{41}
2^{31}
2^{21}
2^0
2^1
2^2
2^3
2^4
2^5
available failing ciphertexts
work
query

4 Outline

1. Introduction
2. How to find 1st failure
3. How to find next failure
4. Recovering the secret
5. Conclusion

KU LEUVEN

4 Recovering the secret

- we have an estimate $\boldsymbol{E}$ of $\boldsymbol{S}$
- $\boldsymbol{E} = \begin{pmatrix} -\boldsymbol{s}_* \\ \boldsymbol{e}_* \end{pmatrix}$

4 Recovering the secret

- we have an estimate $\boldsymbol{E}$ of $\boldsymbol{S}$
- $\boldsymbol{E} = \begin{pmatrix} -\boldsymbol{s}_* \\ \boldsymbol{e}_* \end{pmatrix}$
- LWE problem $(\boldsymbol{A}, \boldsymbol{b} = \boldsymbol{A} \cdot \boldsymbol{s} + \boldsymbol{e})$
- simplify $\boldsymbol{b}_* = (\boldsymbol{A} \cdot \boldsymbol{s} + \boldsymbol{e}) - (\boldsymbol{A} \cdot \boldsymbol{s}_* + \boldsymbol{e}_*)$
- $\boldsymbol{b}_* = \boldsymbol{A} \cdot (\boldsymbol{s} - \boldsymbol{s}_*) + (\boldsymbol{e} - \boldsymbol{e}_*)$

5 Outline

1. Introduction
2. How to find 1st failure
3. How to find next failure
4. Recovering the secret
5. Conclusion

KU LEUVEN