Decryption Failure is More Likely After Success

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

PQCrypto 2020
September 2020

Nina Bindel
John M. Schanck

Security of lattice-based encryption schemes

Security reduction from a computationally hard assumption & Estimated hardness of this assumption

Probability of finding decryption failures

Example: Learning With Errors (LWE) Problem

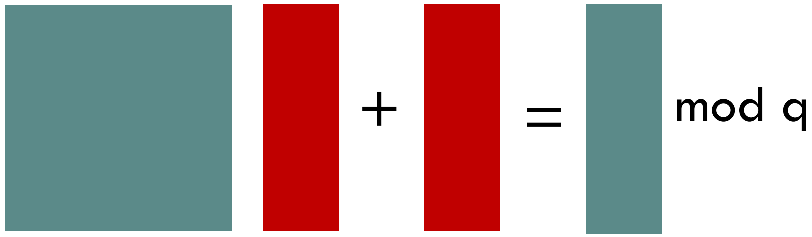
Given: (A,b) with

$A \leftarrow_{\$} \mathbb{Z}_q^{m\times n}$

$s \leftarrow_{\sigma} \mathbb{Z}^n$, $e \leftarrow_{\sigma} \mathbb{Z}^n$

$b = As + e \bmod q$

Find: s



This talk!

Contribution:

Consider adaptively chosen queries in theoretical and practical analysis

Encryption of LWE-based encryption schemes

$$A \cdot S + E = B \mod q$$

Encryption of LWE-based encryption schemes

Inputs

A , B , m

Algorithm

$$A \cdot S + E = B \mod q$$

$$A \cdot S' + E' = C \mod q$$

$$B \cdot S' + E'' + [q/4]\, m = C' \mod q$$

Decryption of LWE-based encryption schemes

Inputs

A, B, m

S, C, C'

Algorithm

$$A \cdot S + E = B \mod q$$

$$A \cdot S' + E' = C \mod q$$

$$\underbrace{B \cdot S' + E''}_{\approx V \approx A \cdot S \cdot S'} + \lfloor q/4 \rceil m = C' \mod q$$

$$\lfloor (C' - \overbrace{C \cdot S}) 4/q \rceil = m$$

Example statement: Frodo NIST submission, Section 2.2.7

The next lemma states bounds on the size of errors that can be handled by the decoding algorithm.

Lemma 2.18. *Let* $q = 2^D$, $B \leq D$. *Then* $\mathrm{dc}(\mathrm{ec}(k) + e) = k$ *for any* $k, e \in \mathbb{Z}$ *such that* $0 \leq k < 2^B$ *and* $-q/2^{B+1} \leq e < q/2^{B+1}$.

$$\lfloor (C' - C \cdot S) 4/q \rceil$$

$$= \underbrace{E \; S' + E'' + E' \; S}_{e} + \lfloor q/4 \rceil \underbrace{m}_{k}$$

Impact of decryption errors

Every decryption error tells us…

$$\boxed{E}\,\boxed{S'} + \boxed{E''} + \boxed{E'}\,\boxed{S} \geq q/2^{B+1}$$

or

$$\boxed{E}\,\boxed{S'} + \boxed{E''} + \boxed{E'}\,\boxed{S} < -q/2^{B+1}$$

State-of-the-art attacks

Original *failure boosting* attack
D'Anvers, Guo, Johansson, Nilsson, Vercauteren, Verbauwhede: Decryption failure attacks on IND-CCA secure lattice-based schemes. PKC 2019

Cost estimation of searching for decryption failure
D'Anvers, Rossie, Virdia: (One) failure is not an option – Bootstrapping the search for failures in lattice-based encryption schemes. EuroCrypt 2020

Impact of decryption errors

Every decryption error tells us…

$$E \; S' + E'' + E' \; S \geq q/2^{B+1}$$

or

$$E \; S' + E'' + E' \; S < -q/2^{B+1}.$$

Every successful decryption tells us…

$$-q/2^{B+1} \leq E \; S' + E'' + E' \; S < q/2^{B+1}.$$

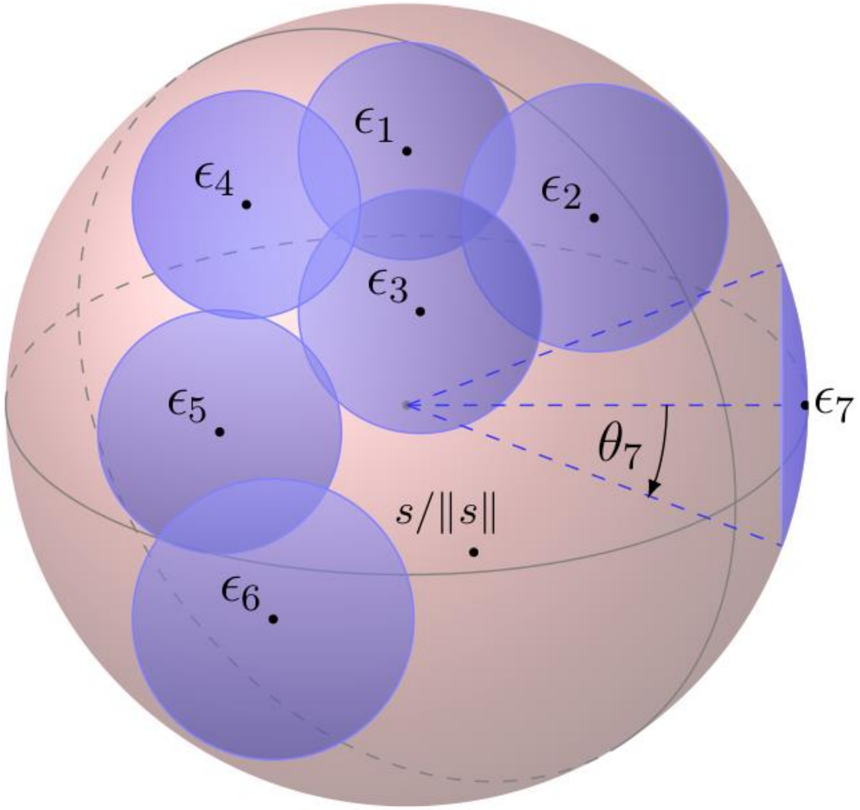
Even gather information from successful decryption.

1st contribution:

Refinement of the failure boosting attack:

Consider **adaptively** collected information of the secret

Idea of our attack



Recall:

$\mathrm{sk} = \mathrm{s}, \mathrm{e}$

$\mathrm{C}_1 = \mathrm{s}'\mathrm{a} + e'\mathrm{mod}\ 16$

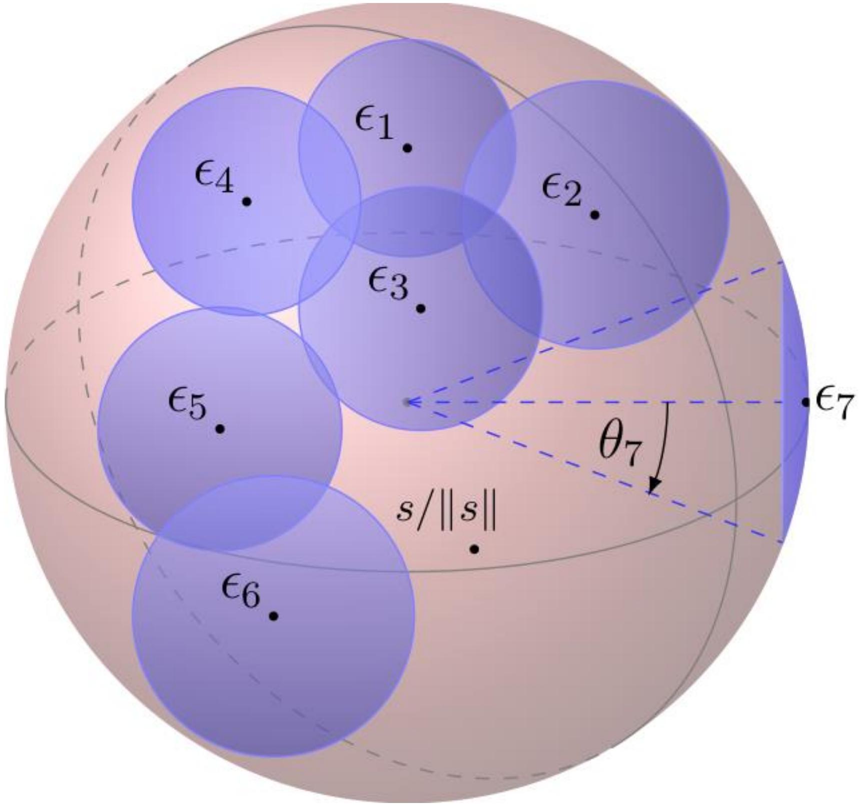
$\mathrm{C}_2 = \mathrm{v} + \mathrm{Encode}(\mathrm{m})$

$\epsilon_i = \epsilon_i(s', e')$ randomness used in encryption queried to decryption oracle

Adversary learns from succesfull decryptions:

- s is not in blue region
- To trigger decryption error with higher probability, choose ϵ_8 in red region

Efficacy of a query set



$\mathrm{E} = \{\epsilon_1, \ldots, \epsilon_7, \ldots\}$

Efficacy of E = fraction of the sphere covered by caps

$$= \frac{\text{blue area}}{\text{area of sphere}}$$

Intelligent adversary:

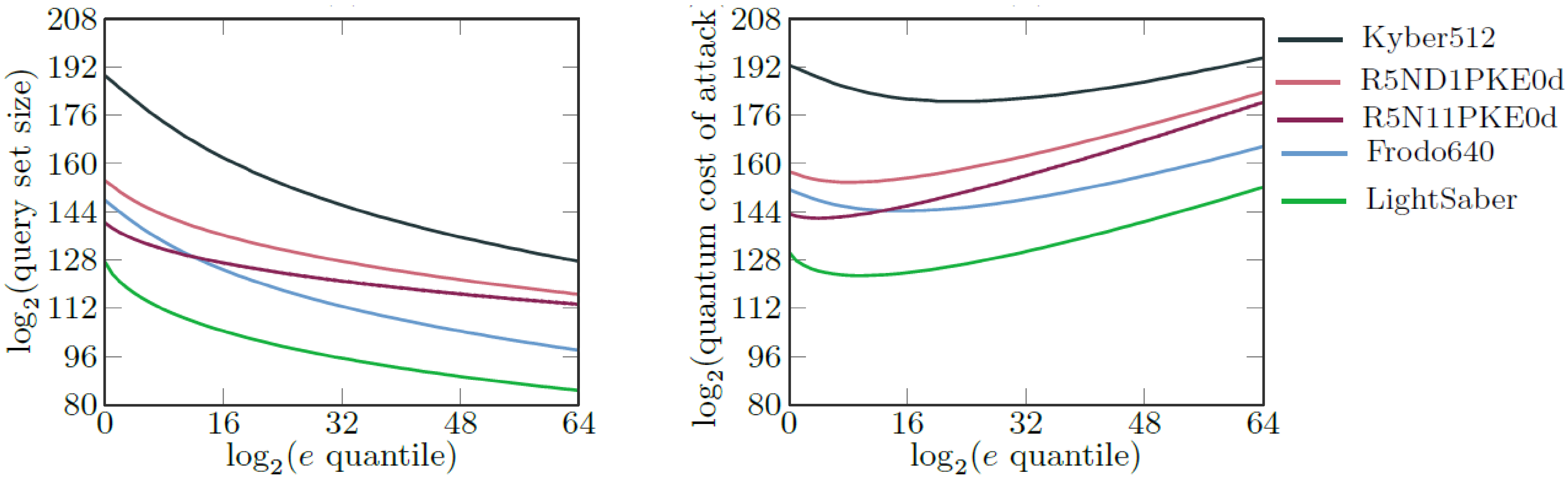
Efficacy ⇧ and #E ⇩

Cost of adversary:

- Cost of generation efficient query set
- Cost of asking queries: $\leq 2^{64}$ (NIST CfS)

Experimental results

Predicted size of a query set of unit efficacy and quantum cost of producing such a query set



Analyzing decryption failure probability

State-of-the-art failure attacks

Security reductions

Passively secure **randomized δ-correct** PKE rP

[FO99]
[HHK17]

$\mathrm{dP} = \mathrm{T}[\mathrm{rP}, \mathrm{G}]$

$\mathbf{Encr_{dP}(pk, m)} = \mathrm{Encr_{rP}}(\mathrm{pk}, \mathrm{m}; \mathrm{G}(\mathrm{m}))$

Passively secure **de-randomized $(\mathbf{q_G} \cdot \boldsymbol{\delta})$-correct** PKE dP

- New attack requires re-evaluation of parameters

+ Smallest parameters

+ Independent of attacks

- Leads to larger parameters

Reality check: Frodo

2.2.7 Correctness of IND-CPA PKE

The next lemma states bounds on the size of errors that can be handled by the decoding algorithm.

Lemma 2.18. *Let* $q = 2^D$, $B \leq D$. *Then* $\mathrm{dc}(\mathrm{ec}(k) + e) = k$ *for any* $k, e \in \mathbb{Z}$ *such that* $0 \leq k < 2^B$ *and* $-q/2^{B+1} \leq e < q/2^{B+1}$.

Proof. This follows directly from the fact that $\mathrm{dc}(\mathrm{ec}(k) + e) = \lfloor k + e2^B/q \rceil \bmod 2^B$. □

2.2.10 Correctness of IND-CCA KEM

The failure probability δ of FrodoKEM is the same as the failure probability of the underlying FrodoPKE as computed in Section 2.2.7.

2nd contribution:

New correctness definition tailored for de-randomized encryption schemes:

Consider **adaptively** asked decryption queries

Correctness definition

Hofheinz-Hövelmanns-Kiltz 2017:

$\underline{\mathrm{Expt}_{\mathsf{P}}^{\mathsf{COR}}(\mathcal{A}):}$

1 $(\mathrm{pk}, \mathrm{sk}) \leftarrow \mathsf{Keygen}()$
2 $\mathsf{m} \leftarrow \mathsf{A}(sk, pk)$
3 $c \leftarrow \mathsf{Encr}(\mathrm{pk}, \mathsf{m})$
4 return $[\mathsf{Dec}(sk, c) = \mathsf{m}]$

P is **δ-correct**

if $\Pr[\mathrm{COR}_{\mathrm{P}}^{\mathrm{A}}] \leq \delta$

$\Leftrightarrow E_{pk,sk}\left[\boxed{\max_{m} \Pr}[\mathrm{Dec}(c, sk) \neq m : c \leftarrow \mathrm{Enc}(m, pk)]\right] \leq \delta$

$\Leftrightarrow \Pr[\mathrm{Dec}(c, sk) \neq m : c \leftarrow Enc(m, pk), (pk, sk) \leftarrow Gen] \leq \delta$

if no depency on m

“One-shot probability“

This paper:

$\underline{\mathrm{Expt}_{\mathsf{P}}^{\mathsf{COR\text{-}ad}}}$

1 $(\mathrm{pk}, \mathrm{sk}) \leftarrow \mathsf{Keygen}()$
2 $\mathsf{m} \leftarrow \mathcal{A}^{H,D}(\mathrm{pk}, c^*)$
3 $c \leftarrow \mathsf{Encr}(\mathrm{pk}, \mathsf{m})$
4 return $[\mathsf{Decr}(sk, c) = \mathsf{m}]$

P is $\boldsymbol{\delta(q_D, t)}$**-correct**

if $\Pr[\mathrm{COR}-\mathrm{ad}_{\mathrm{P}}^{\mathrm{A}}] \leq \boxed{\delta(q_D, t)}$

#queries to oracle D

A‘s computational time

Different correctness definitions – Example Frodo640

One-shot probability δ		2^{-144}
FO-theorem #hash queries $\cdot\ \delta$	#hash queries $= 128$	2^{-16}
Our def. $\delta(\#\mathrm{decr.\,queries}, \mathrm{time})$	#decryption queries $= 64$, Time $= 2^{128}$	2^{-34}

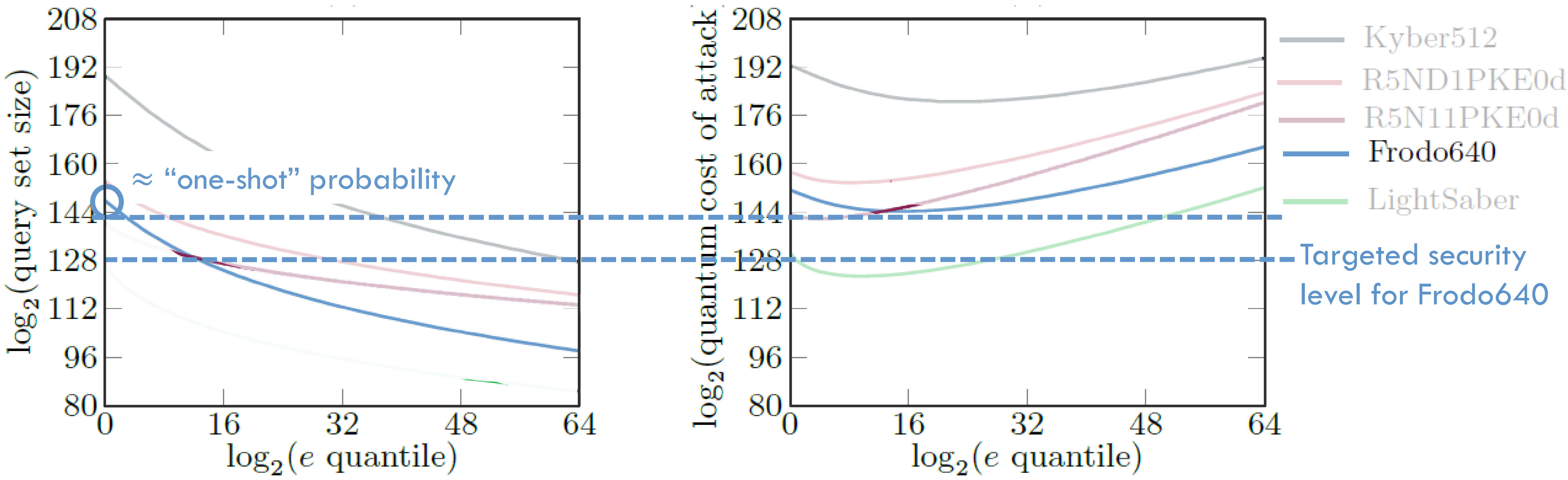
Concern:

CPA secure de-randomized δ-correct PKE $\Longrightarrow$ CCA secure δ-correct KEM

δ is multiplied with large terms, leading to less tight bounds

Experimental results

Predicted size of a query set of unit efficacy and quantum cost of producing such a query set



Summary

- Refinement of failure boosting attack
- New correctness definition tailored for de-randomized encryption schemes
- Experimental Results:
  - Do not ask for revision of parameters of NIST candidates
  - Show that one-shot probability is not reliable

Full paper: IACR eprint 2019/590

Acknowledgments

Special thanks to
Kathrin Hövelmanns
for insights on the correctness definition,
Jan-Pieter D'Anvers
for helpful discussions, and
Steve Weiss
for computer systems support.

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

THANKS