Estimate all the {LWE, NTRU} schemes!

Martin R. Albrecht[1], Benjamin R. Curtis[1], Amit Deo[1], Alex Davidson[1], Rachel Player[1,2], **Eamonn W. Postlethwaite**[1], Fernando Virdia[1], Thomas Wunderer[3],

August 26, 2018

[1]Royal Holloway, University of London, UK
[2]Sorbonne Université, CNRS, INRIA, LIP6, Équipe PolSys, France
[3]Technische Universität Darmstadt, Germany

Motivation

NIST “Competition”

This call for proposals aims to standardise post quantum {PKE, KEM, SIG} schemes.

Of 69 valid submissions, 23[1] approximate LWE or NTRU.

Type	LWE or NTRU	Code based	Multivariate	Hash based	Other	Total
#	26	24	13	4	15	82

[1] based on `https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/asiacrypt-2017-moody-pqc.pdf`

NIST “Competition”

This call for proposals aims to standardise post quantum {PKE, KEM, SIG} schemes.

Of 69 valid submissions, 23[1] approximate LWE or NTRU.

Type	LWE or NTRU	Code based	Multivariate	Hash based	Other	Total
#	23	—	—	—	—	69

[1] based on `https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/asiacrypt-2017-moody-pqc.pdf`

Requirements

Submitters were required by NIST[2] to

- give at least one parameter set
- target at least one (NIST defined) security category
- provide some form of cryptanalysis

[2] https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf

Cryptanalysis and Security

In {LWE, NTRU} cryptanalysis and bit security estimation

- there are a variety of attacks
- lattice reduction (i.e. BKZ) is ubiquitous
- many different cost models exist

Cost Models

$$\{\text{quantum, not quantum}\}$$
$$\times$$
$$\{\text{complexity of solving SVP in dimension } \beta\}$$
$$\times$$
$$\{\text{number of SVP calls required for given reduction quality}\}$$

Cost Models II

{complexity of solving SVP in dimension β}

Type	$\log_2$(Time complexity)
Sieving[3]	$O(s_0\beta + s_1)$
Enumeration I	$O(e_0\beta \log \beta + e_1\beta + e_2)$
Enumeration II	$O(e'_0\beta^2 + e'_1\beta + e'_2)$

[3] Also requires exponential memory.

Cost Models II

{complexity of solving SVP in dimension β}

Type	$\log_2$(Time complexity)
Sieving[3]	$O(s_0\beta + s_1)$
Enumeration I	$O(e_0\beta \log \beta + e_1\beta + e_2)$
Enumeration II	$O(e'_0\beta^2 + e'_1\beta + e'_2)$

{number of SVP calls required for given reduction quality}

Name	Number of SVP calls
Core	1
—	β
—	$8d$

[3] Also requires exponential memory.

Cost Models III

Model	Cost	Schemes
Core-Sieve Q-Core-Sieve	$2^{0.292\beta}$ $2^{0.265\beta}$	CRYSTALS [LDK+17,SAB+17] Falcon [PFH+17] HILA5 [Saa17] KINDI [Ban17] LAC [LLJ+17] New Hope [PAA+17] SABER [DKRV17] ThreeBears [Ham17] Titanium [SSZ17] NTRU HRSS [SHRS17] NTRUEncrypt [ZCHW17a] pqNTRUSign [ZCHW17b]
Core-Sieve+$O(1)$ Q-Core-Sieve+$O(1)$	$2^{0.292\beta+16.4}$ $2^{0.265\beta+16.4}$	LIMA [SAL+17]
Core-Sieve (min. space) Q-Core-Sieve (min. space)	$2^{0.368\beta}$ $2^{0.2975\beta}$	NTRU HRSS [SHRS17]
β-Sieve Q-β-Sieve	$\beta\, 2^{0.292\beta}$ $\beta\, 2^{0.265\beta}$	Frodo [NAB+17] Lizard [CPL+17] KCL [ZjGS17] Round2 [GMZB+17]
$8d$-Sieve+$O(1)$	$8d\, 2^{0.292\beta+16.4}$	Ding Key Exchange [DTGW17] EMBLEM [SPL+17]
Q-$8d$-Sieve+$O(1)$	$8d\, 2^{0.265\beta+16.4}$	qTESLA [BAA+17]
Core-Enum+$O(1)$	$2^{0.187\beta \log \beta - 1.019\beta + 16.1}$	NTRU HRSS [SHRS17] NTRUEncrypt [ZCHW17a] pqNTRUSign [ZCHW17b]
Q-Core-Enum+$O(1)$	$2^{(0.187\beta \log \beta - 1.019\beta + 16.1)/2}$	NTRU HRSS [SHRS17]
$8d$-Enum (quadratic fit)+$O(1)$	$8d\, 2^{0.000784\beta^2 + 0.366\beta - 0.9}$	NTRU Prime [BCLvV17]
LOTUS-Enum	$2^{0.125\beta \log \beta - 0.755\beta + 2.25}$	LOTUS [PHAM17]

Our Work

What?

Using the LWE estimator we estimated the security

- of every parameter set
- of every scheme
- against[4] all relevant attacks
- under each cost model included in a NIST submission

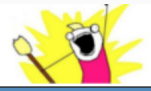
and made a human friendly[5] table which generates code snippets to repeat each experiment.

[4] almost

[5] `https://estimate-all-the-lwe-ntru-schemes.github.io/`

Website

Estimate all the {LWE, NTRU} schemes!



Complexity estimates for running the primal-uSVP and dual attacks against all LWE-based, and t
process run by NIST. We make use of the [APS15] estimator. The code for generating this table
provide with stand-alone Sagemath code for reproducing the estimate.

Below, we provide LWE-equivalent parameters, where n = LWE secret dimension, k = MLWE rank
schemes we provide ‖f‖, ‖g‖ = lengths of the short polynomials. If you spot a mistake in a param

We stress that the columns under "Proposed BKZ cost models" give different cost estimates for
these estimates explicitly are lower bounds (under some assumptions). Thus, a relatively small nu
scheme given in the corresponding row. Given that the numbers in different columns diverge gre

BabyBear – 0.265 β

```
# To reproduce the estimate run this snippet on
http://aleph.sagemath.org/
# Ring ops: 153
# Block size: 577
# Dimension: 1164
load('https://bitbucket.org/malb/lwe-
estimator/raw/HEAD/estimator.py')
n = 624
sd = 1
q = 1024
alpha = sqrt(2*pi)*sd/RR(q)
m = n
secret_distribution = "normal"
success_probability = 0.99
reduction_cost_model =  lambda beta, d, B: ZZ(2)**RR(0.265*beta)
primal_usvp(n, alpha, q, secret_distribution=secret_distribution,
m=m, success_probability=success_probability,
```

LWE n samples | LWE 2n samples | NTRU | 14 selected

Scheme	Assumption	Primitive	Parameters	Claimed security	NIST Category	Attack	0.265 β	0.265 β + 16.4	0.2975 β	0.265 β + log β	0.265 β + 16.4 + log (8d)	0.292 β	29 +
BabyBear	ILWE	KEM	n = 624, k =	152	2	primal	153	170	172	163	183	169	
BabyBear	ILWE	KEM	n = 624, k =	152	2	dual	193	206	211	202	218	207	
BabyBear	ILWE	KEM	n = 624, k =	141	2	primal	143	159	160	152	172	157	
BabyBear	ILWE	KEM	n = 624, k =	141	2	dual	180	192	197	186	205	193	
CRYSTALS-Dilithium	MLWE	SIG	n = 768, k =	91	1	primal	92	109	104	101	122	102	

Why?

We wanted to

- offer a meaningful comparison between schemes
- protect against a cost model becoming obsolete
- find {mistakes, intuition, unexpected results}
- display discrepancies in the estimation space

Disclaimers

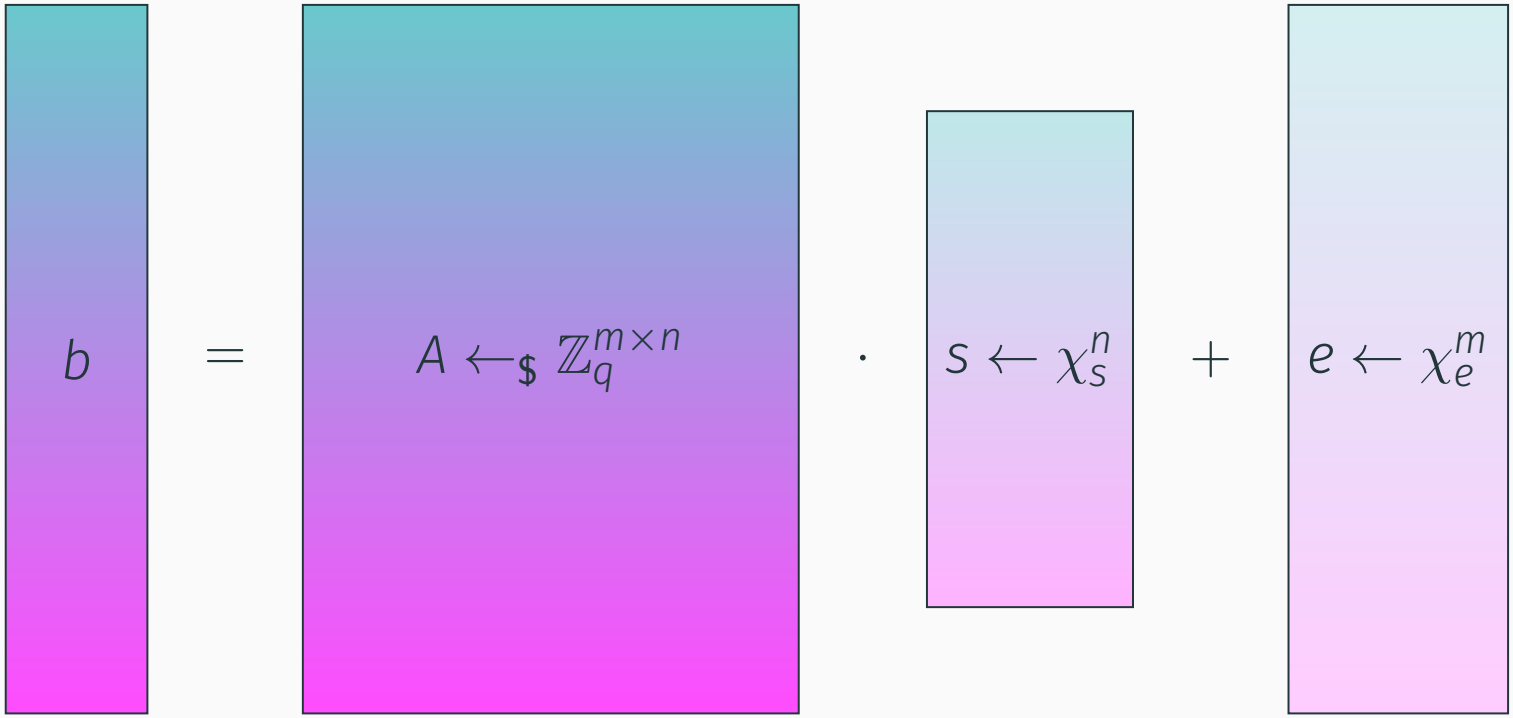
- Not a promotion of any {scheme, cost model}!
- The estimator is not perfect!

In particular we encourage code review of the estimator[6].

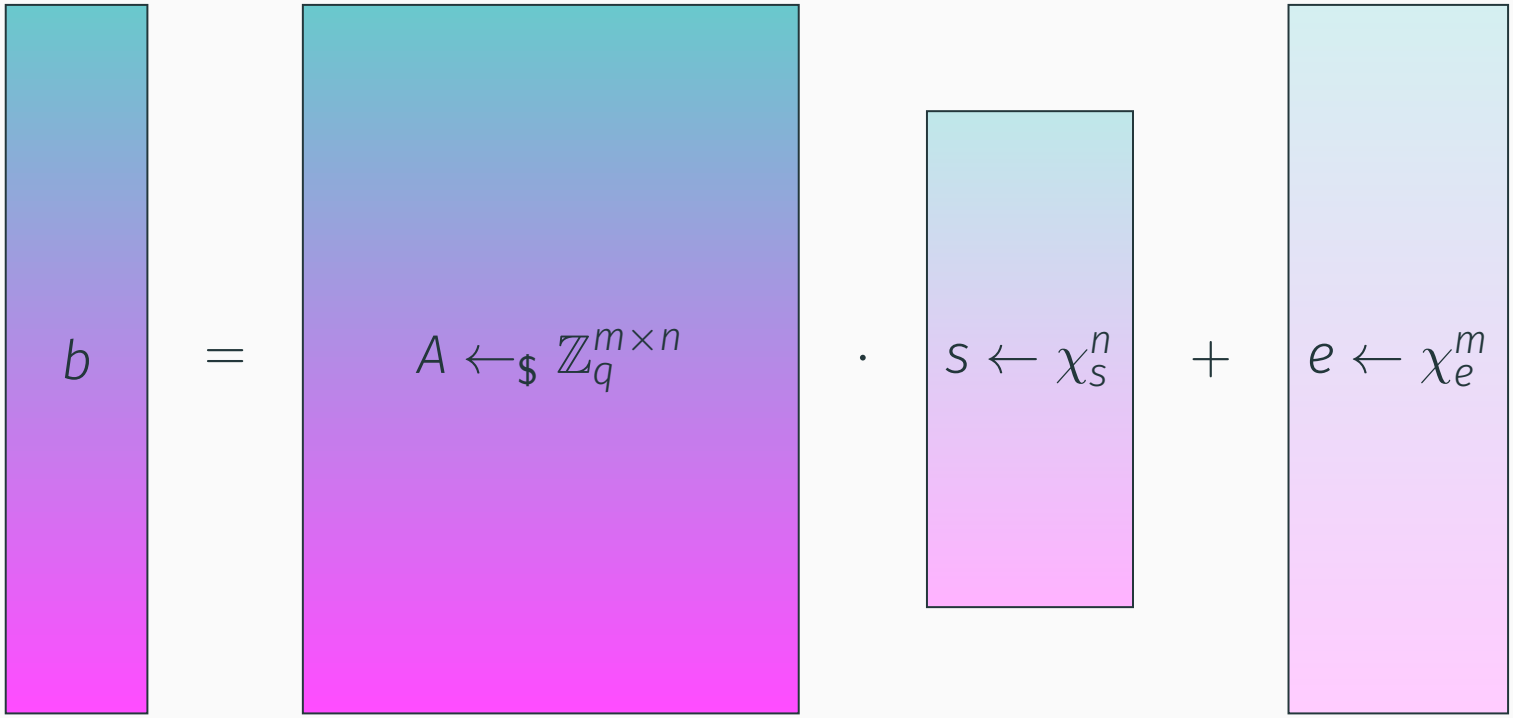
[6] `https://bitbucket.org/malb/lwe-estimator`

LWE and NTRU

LWE


b
$=$
$A \leftarrow_{\$} \mathbb{Z}_q^{m \times n}$
$\cdot$
$s \leftarrow \chi_s^n$
$+$
$e \leftarrow \chi_e^m$

LWE



LWE/Secret dimension	Modulus	# samples	Error distribution	Secret Distribution
n	q	$m \in \{n, 2n\}$	χ_e	χ_s

Notes

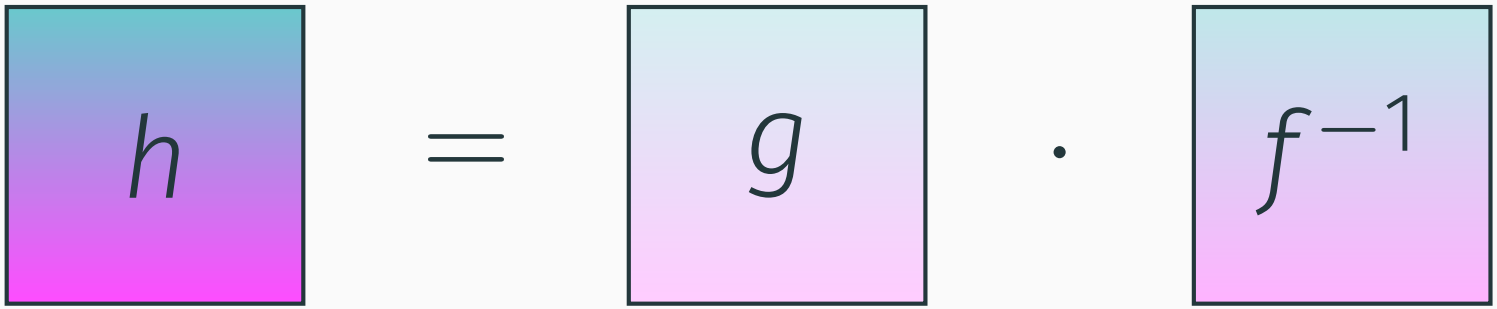
For LWE problems we

- consider the dual and primal attacks
- transform {LWR, RLWE, MLWE} to appropriate LWE
- deal with a variety of distributions for χ_e and χ_s

NTRU

Ring	Secrets (short)	Public
$\mathcal{R}_q = \frac{\mathbb{Z}_q[X]}{(\phi)}$	$f \in \mathcal{R}_q^\times, g \in \mathcal{R}_q$	$h \in \mathcal{R}_q$

Ring	Secrets (short)	Public
$\mathcal{R}_q = \frac{\mathbb{Z}_q[X]}{(\phi)}$	$f \in \mathcal{R}_q^\times, g \in \mathcal{R}_q$	$h \in \mathcal{R}_q$



Notes

We convert an NTRU instance into an LWE instance

- $n = \deg(\phi)$
- q modulus of $\mathcal{R}_q$
- χ_e takes variance $\|g\|/\sqrt{n}$
- $m = n$
- χ_s takes the distribution of f

Findings

Cost Swaps

Let P_1, P_2 be parameter sets for two schemes, and C_1, C_2 be two cost models. There are occurrences[7] of

$$C_1(P_1) > C_1(P_2) \wedge C_2(P_1) < C_2(P_2).$$

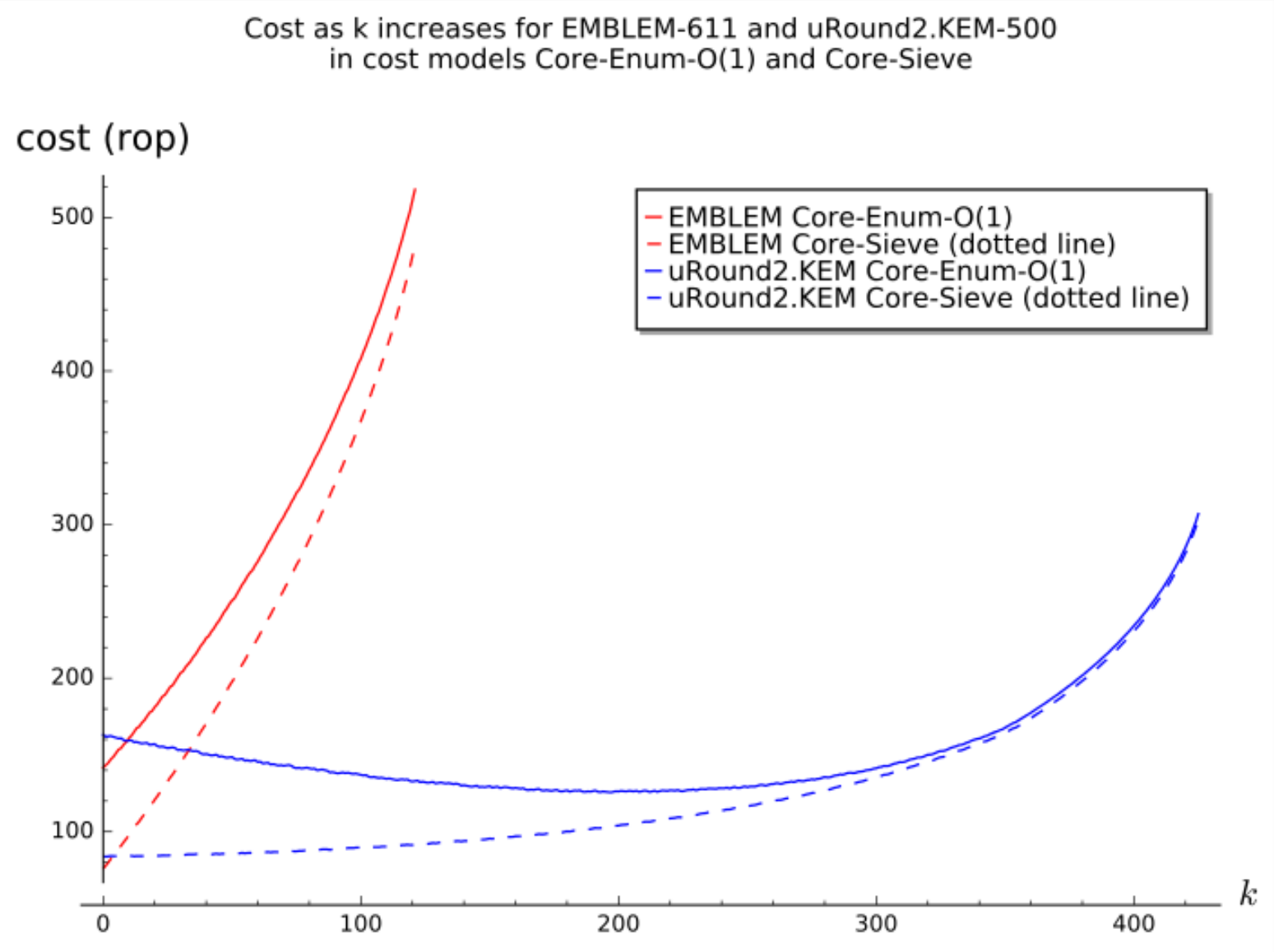
[7] Bernstein via pqc-forum mailing list `https://groups.google.com/a/list.nist.gov/forum/i#!msg/pqc-forum/1lDNio0sKq4/xjqy4K6SAgAJ`.

Cost Swaps II

If χ_s is small or sparse a hybird strategy is to guess entries as 0 and solve smaller dimensional instances.

Regime	$\log_2$(Time complexity)	Guessing effect
Enumeration	$O(e_0\beta \log \beta + e_1\beta + e_2)$	Stronger
Sieving	$O(s_0\beta + s_1)$	Weaker

Cost Swaps III



“Quantum Security”

NIST recommended a maximum quantum circuit depth.
Instead, many submissions focussed on asymptotic Q- model.

Security Category I: As hard as AES-128 key recovery. Does this mean

“Quantum Security”

NIST recommended a maximum quantum circuit depth.
Instead, many submissions focussed on asymptotic Q- model.

Security Category I: As hard as AES-128 key recovery. Does this mean

- Aim for Q- cost $\geq 2^{128}$, i.e. given “perfect Grover” as hard to break as as AES-128 classically?

“Quantum Security”

NIST recommended a maximum quantum circuit depth.
Instead, many submissions focussed on asymptotic Q- model.

Security Category I: As hard as AES-128 key recovery. Does this mean

- Aim for Q- cost $\geq 2^{128}$, i.e. given “perfect Grover” as hard to break as as AES-128 classically?
- Aim for Q- cost $\geq 2^{64}$, i.e. as hard to break as AES-128 given “perfect Grover’?’

“Quantum Security”

NIST recommended a maximum quantum circuit depth.
Instead, many submissions focussed on asymptotic Q- model.

Security Category I: As hard as AES-128 key recovery. Does this mean

- Aim for Q- cost $\geq 2^{128}$, i.e. given “perfect Grover” as hard to break as as AES-128 classically?
- Aim for Q- cost $\geq 2^{64}$, i.e. as hard to break as AES-128 given “perfect Grover’?’

Difficult to compare two schemes aiming for Security Category I under these two distinct definitions!

Conclusions

Further work I

The cost swap example implies more understanding is needed of the

- crossover point between enumeration and sieving
- accurate behaviour of BKZ in low block sizes

Further work II

The quantum cost example implies the need for

- agreement on how to interpret Q- cost
- concrete estimates of the quantum resources Grover requires
- collaboration with people who understand Q- circuit depth!

Thanks!