LAC

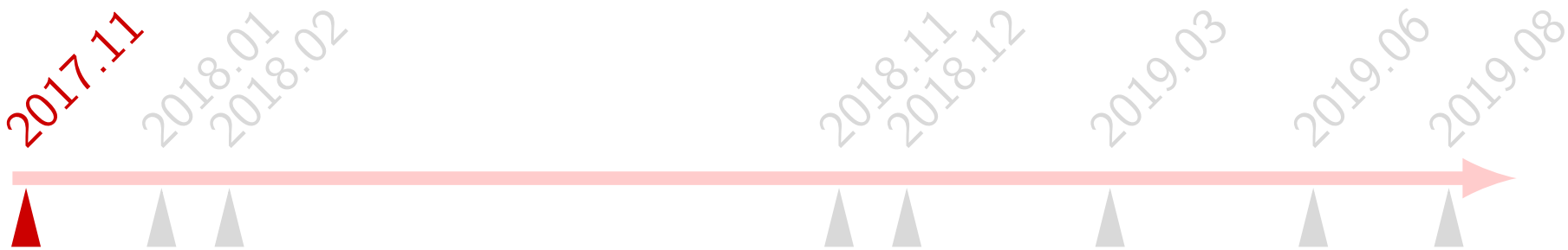
Xianhui Lu[1], Yamin Liu[1], Dingding Jia[1], Haiyang Xue[1], Jingnan He[1], Zhenfei Zhang[2], Zhe Liu[3], Hao Yang[3], Bao Li[1], Kunpeng Wang[1]

Algorand™

NIST Second PQC Standardization Conference

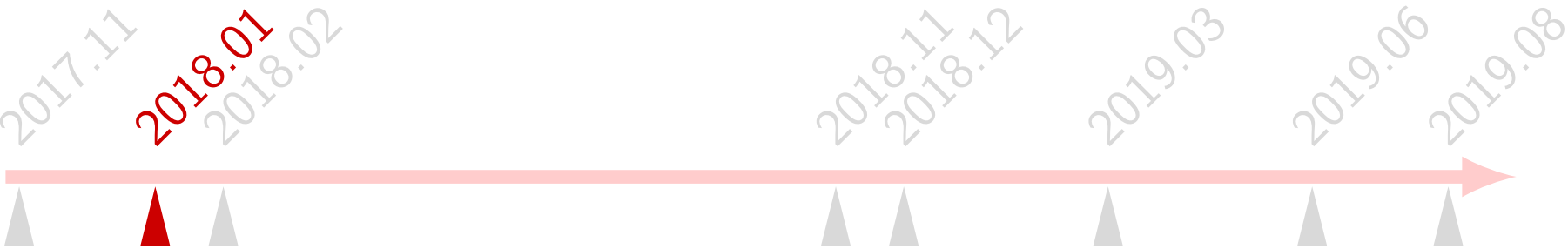
August 24, 2019

Timeline



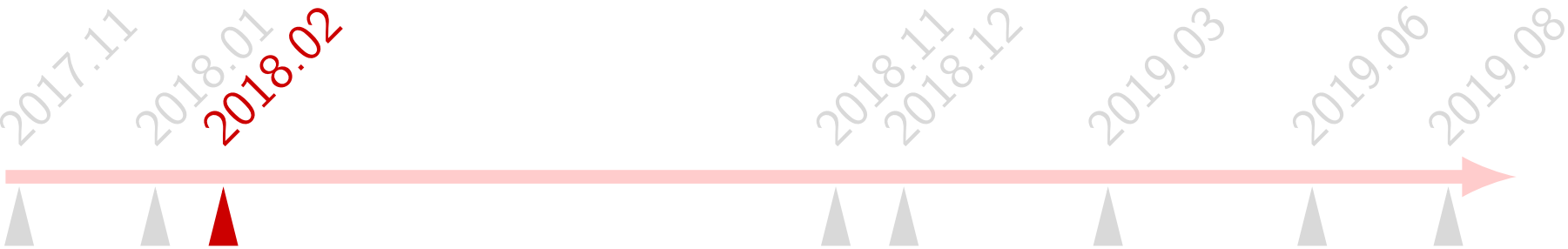
- Nov 2017: LAC round 1 submission

Timeline



- Nov 2017: LAC round 1 submission
- Jan 2018: Subfield attack

Timeline

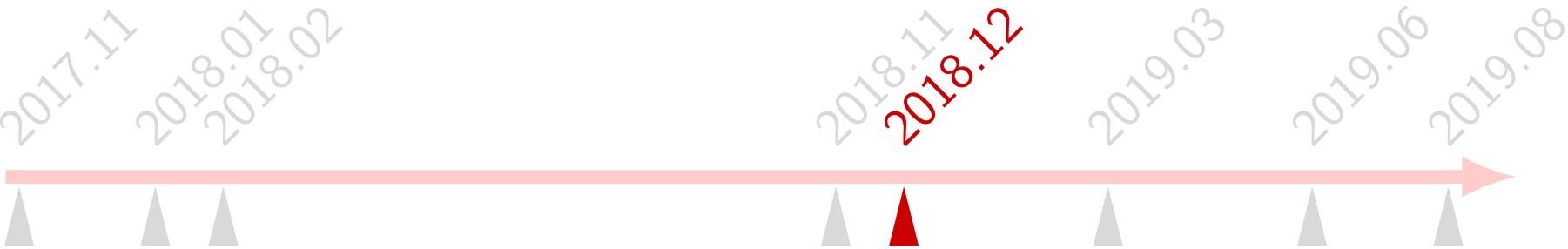


- Nov 2017: LAC round 1 submission
- Jan 2018: Subfield attack
- Feb 2018: High hamming weight attack (CCA)

Timeline

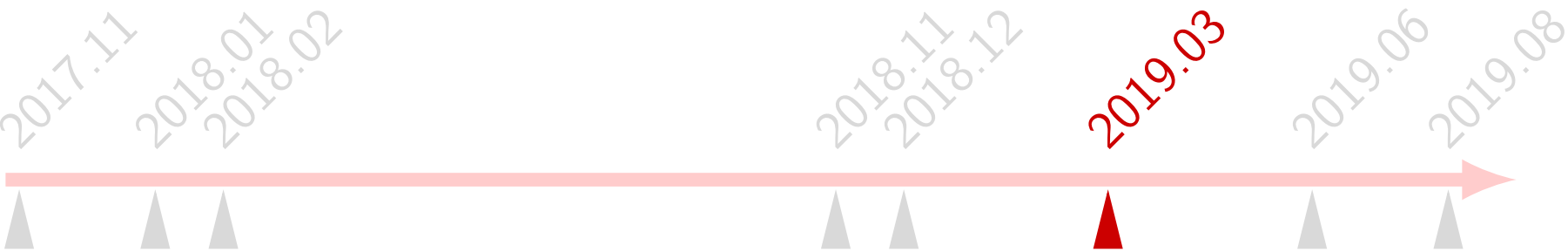
- Nov 2017: LAC round 1 submission
- Jan 2018: Subfield attack
- Feb 2018: High hamming weight attack (CCA)
- Nov 2018: Timing attack on ECC (CCA)

Timeline



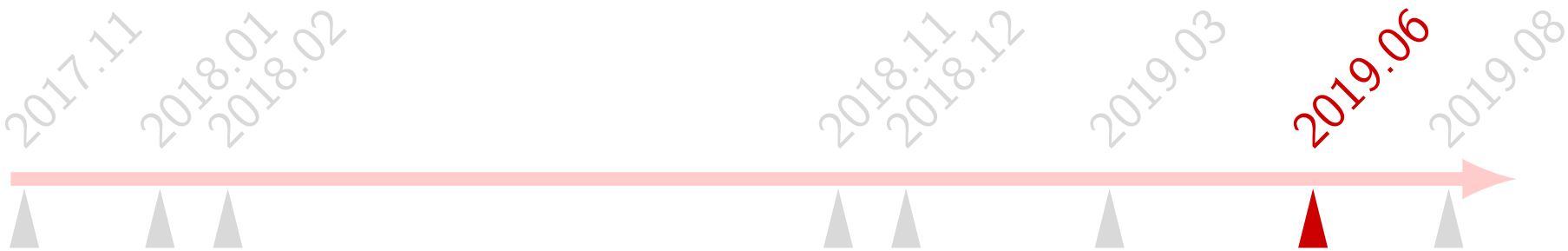
- Nov 2017: LAC round 1 submission
- Jan 2018: Subfield attack
- Feb 2018: High hamming weight attack (CCA)
- Nov 2018: Timing attack on ECC (CCA)
- Dec 2018: Error correlation (CCA)

Timeline



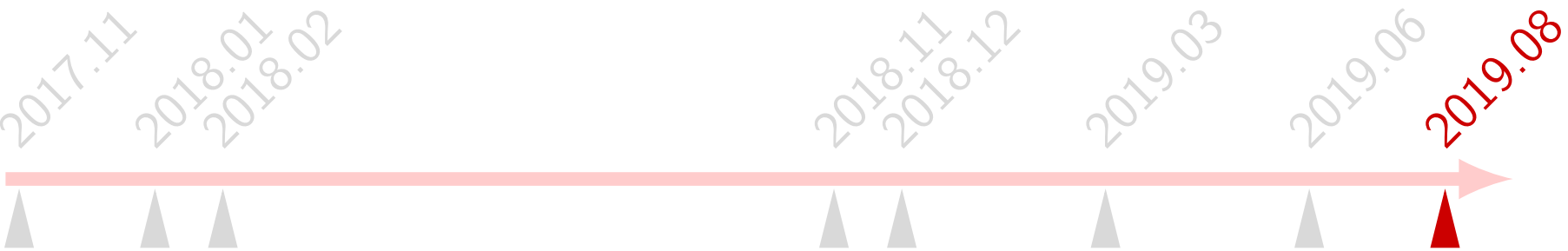
- Nov 2017: LAC round 1 submission
- Jan 2018: Subfield attack
- Feb 2018: High hamming weight attack (CCA)
- Nov 2018: Timing attack on ECC (CCA)
- Dec 2018: Error correlation (CCA)
- Mar 2019: LAC round 2 submission

Timeline



- Nov 2017: LAC round 1 submission
- Jan 2018: Subfield attack
- Feb 2018: High hamming weight attack (CCA)
- Nov 2018: Timing attack on ECC (CCA)
- Dec 2018: Error correlation (CCA)
- Mar 2019: LAC round 2 submission
- Jun 2019: Pattern attack (CCA)

Timeline



- Nov 2017: LAC round 1 submission
- Jan 2018: Subfield attack
- Feb 2018: High hamming weight attack (CCA)
- Nov 2018: Timing attack on ECC (CCA)
- Dec 2018: Error correlation (CCA)
- Mar 2019: LAC round 2 submission
- Jun 2019: Pattern attack (CCA)
- Aug 2019: Hybrid dual attack

A brief review

- $(pk, sk) \leftarrow \texttt{KeyGen}()$
  - $pk = (\mathbf{a}, \mathbf{b} := \mathbf{as} + \mathbf{e})$, $sk = \mathbf{s}$
- $c \leftarrow \texttt{Enc}(\texttt{msg}, \texttt{sk})$
  - $\tilde{\mathbf{m}} = \texttt{BCH\_encode}(\texttt{msg})$
  - $\mathbf{c}_1 = \mathbf{as}_1 + \mathbf{e}'$, $\mathbf{c}_2 = \mathbf{bs}_1 + \mathbf{e}'' + q/2\tilde{\mathbf{m}}$
  - $c = (\mathbf{c}_1, \mathbf{c}_2)$
- $msg \leftarrow \texttt{Dec}(\texttt{c}, \texttt{pk})$
  - $\ldots$
  - $msg = \texttt{BCH\_decode}(\tilde{\mathbf{m}})$

Motivation

- Want to use smallest modulus, $q = 251$

Motivation

- Want to use smallest modulus, $q = 251$
- Too many errors in the message

Motivation

- Want to use smallest modulus, $q = 251$
- Too many errors in the message
- Use ECC to handle the errors

Motivation

- Want to use smallest modulus, $q = 251$
- Too many errors in the message
- Use ECC to handle the errors
- The focus of the cryptanalysis

This talk

- A summary of the cryptanalysis on LAC;
- The updated parameter sets in Round 2;

This talk

- A summary of the cryptanalysis on LAC;
- The updated parameter sets in Round 2;
- And more cryptanalysis...

Subfield Attack [Alp18a]

Strategy

- $x^n + 1 = \mathbf{hg} := (x^{n/2} + 91x^{n/4} + 250)(x^{n/2} + 160x^{n/4} + 250) \bmod 251$
- Given $(\mathbf{a}, \mathbf{b} = \mathbf{as} + \mathbf{e})$, try to recover
  - $(\mathbf{s}_g, \mathbf{e}_g) := (\mathbf{s}, \mathbf{e}) \mod \mathbf{g}$
  - $(\mathbf{s}_h, \mathbf{e}_h) := (\mathbf{s}, \mathbf{e}) \mod \mathbf{h}$

Analysis

- $|\mathbf{s}_g, \mathbf{e}_g|_\infty = 25$ too large, c.f. RHF
- No impact on LAC parameters for Round 1 submission

High Hamming Weight Attack [Alp18b]

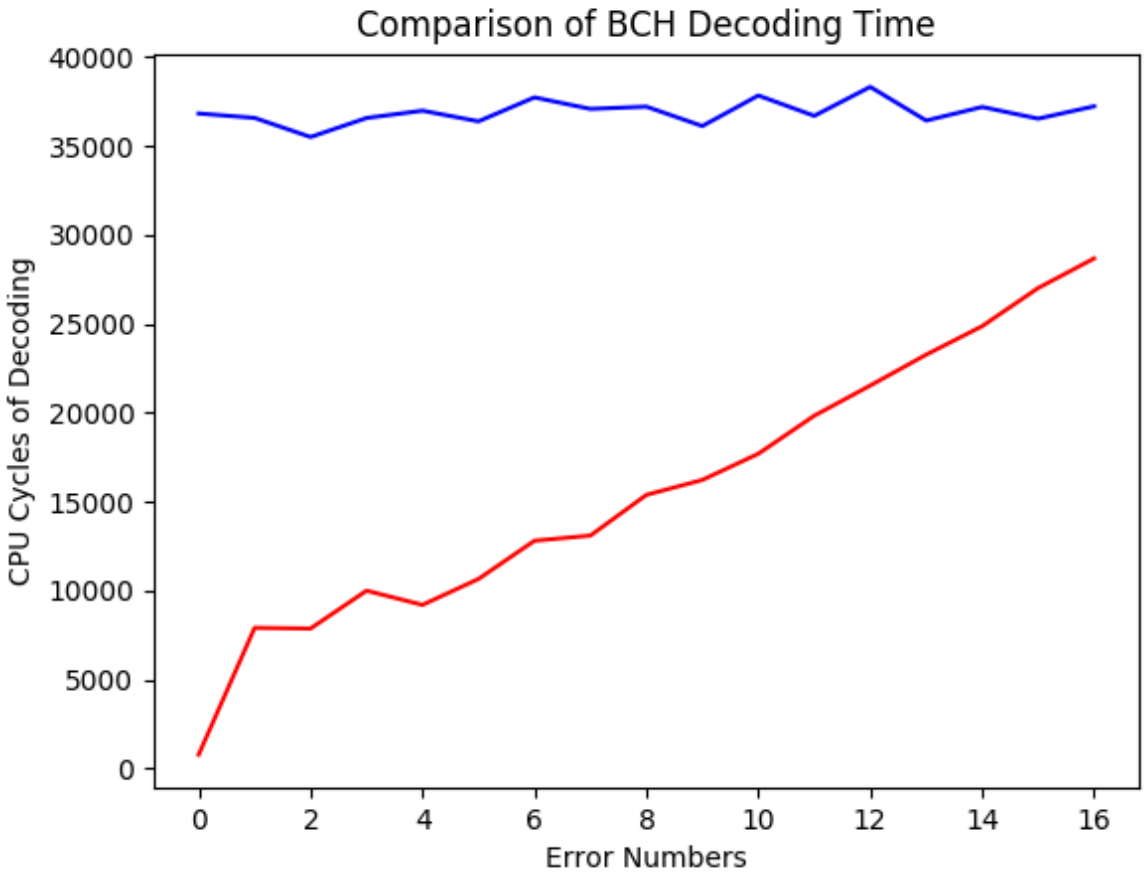
Strategy

- $\mathbf{s}_1, \mathbf{e}'$ follows binomial distribution
- Choose $\mathbf{s}_1, \mathbf{e}'$ with higher-then-normal Hamming weight
- Decryption error rate increased to $2^{-44.4}$
- Produce $2^{19.6}$ decryption failures with 2^{207} pre-computation and 2^{64} oracle queries for level 5.

Counter-measure

- Use binomial distribution with fixed Hamming weight.

Timing attack on ECC [DTVV19]



- Round 1 BCH: non-constant time, $O(err)$
- Round 2 BCH: *almost* constant time, $O(max(err))$

Error Correlation [DVV19]

Round 1 parameter

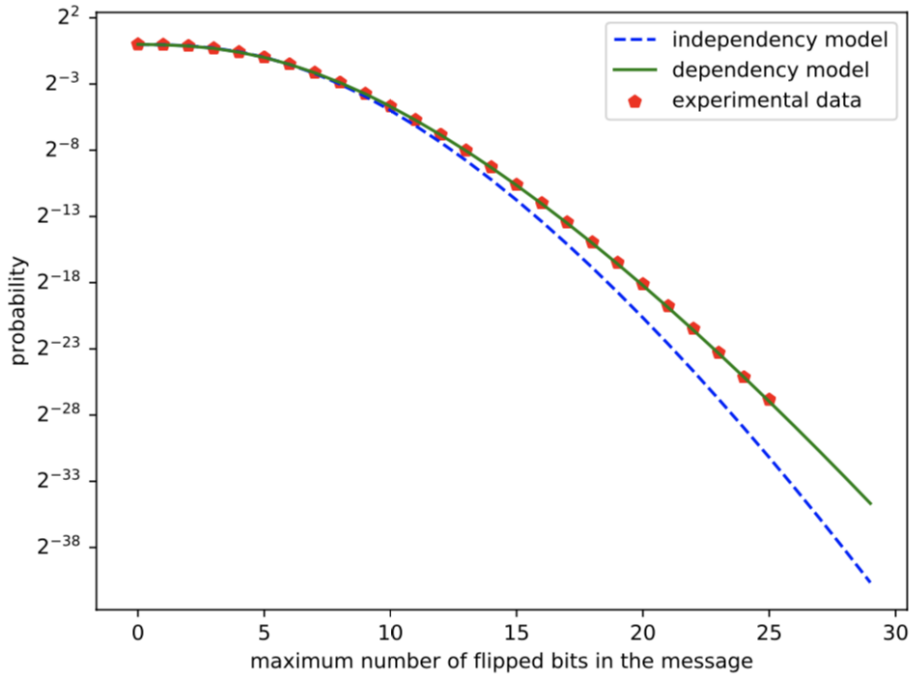
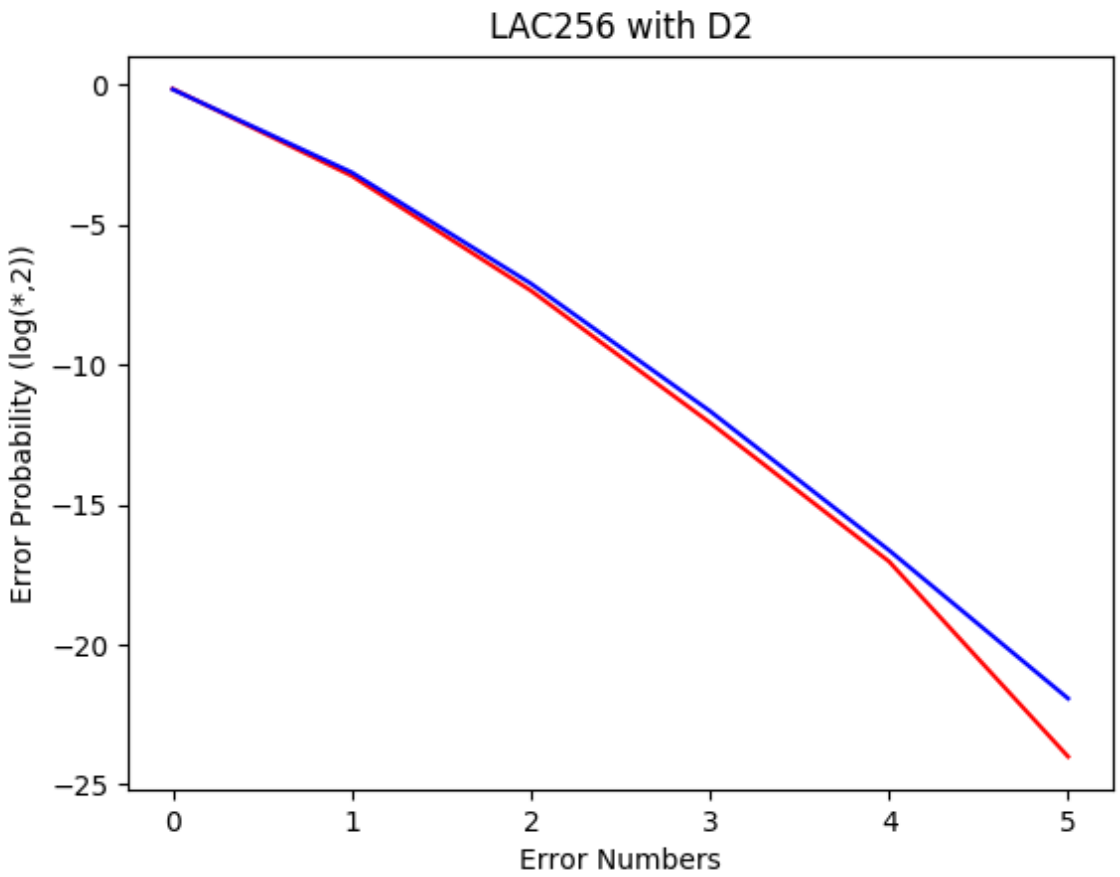


Figure 2: Probability of failure for various error correction capabilities of `ecc_enc`

- Dependency aware model: "*independence assumption is suitable for schemes without error correction, but that it might lead to under-estimating the failure probability of algorithms using error correcting codes*"

Error Correlation [DVV19], continued

Round 2 parameter



- Red line: Experimental data
- Blue line: Dependency aware model

Categories	n	q	**dis**	**ecc**	l_m	**pk**	**sk**	**ct**	**bit-er**	**dec-er**
LAC-128	512	251	$\Psi_1^n, \Psi_1^{n,\frac{n}{2}}$	[511, 256, 33]	256	544	512	712	$2^{-12.61}$	2^{-116}
LAC-192	1024	251	$\Psi_{\frac{1}{2}}^n, \Psi_{\frac{1}{2}}^{n,\frac{n}{4}}$	[511, 256, 17]	256	1056	1024	1188	$2^{-22.27}$	2^{-143}
LAC-256	1024	251	$\Psi_1^n, \Psi_1^{n,\frac{n}{2}}$	[511,256,33]+D2	256	1056	1024	1424	$2^{-12.96}$	2^{-122}

dis secret and noise distributions
ecc error correction code
l_m message length
sk secret key size (bytes)
pk public key size (bytes)
ct ciphertext size (bytes)
bit-er single bit error rate without BCH
dec-er decryption error rate

Table 2. Recommended parameter of LACv2

Major updates

	Round 1	Round 2
Message space	256, 384, 512	256
Noise dist.	binomial	fix-weight
ECC	BCH(511,264,29) BCH(511,392,13) BCH(1023,520,55)	BCH(511,256,16) BCH(511,256,8) BCH(511,256,16)+D2

Hybrid attacks, Round5 team and [Son19]

Hybrid primal attack

- Reduces security margin of LAC-192 from 286 to 278
- No impact on LAC-128/256

Hybrid dual attack

- Discovered by Round5 team and Son independently last week
- We are evaluating the impact
- Current thought: may affect security margin by a few bits

Pattern Attack [GJY19]

Strategy

- Assume $\mathbf{e}'$ has certain pattern
  - e.g., 33 consecutive $1, -1, \ldots$; happens with prob 2^{-122}
- $\mathbf{s}$ has certain distribution
  - e.g., $|\mathbf{s}_{odd}(1)| + |\mathbf{s}_{even}(1)| > 208$; happens with prob 2^{-70}
- A higher than normal error rate
  - e.g., $< 2^{-30}$, c.f., norm error rate 2^{-122}
- Repeat for enough errors to attack secret key
  - e.g., $\approx 2^{30}$ errors (?), with a total cost $2^{122+70+30+30} \approx 2^{252}$

Impact

- [GJY19] focused on LAC256 of round 1 parameter
- Our evaluation on round 2 parameter:
  - LAC128/192 remain intacct;
  - LAC256 needs a revision on error correct code.

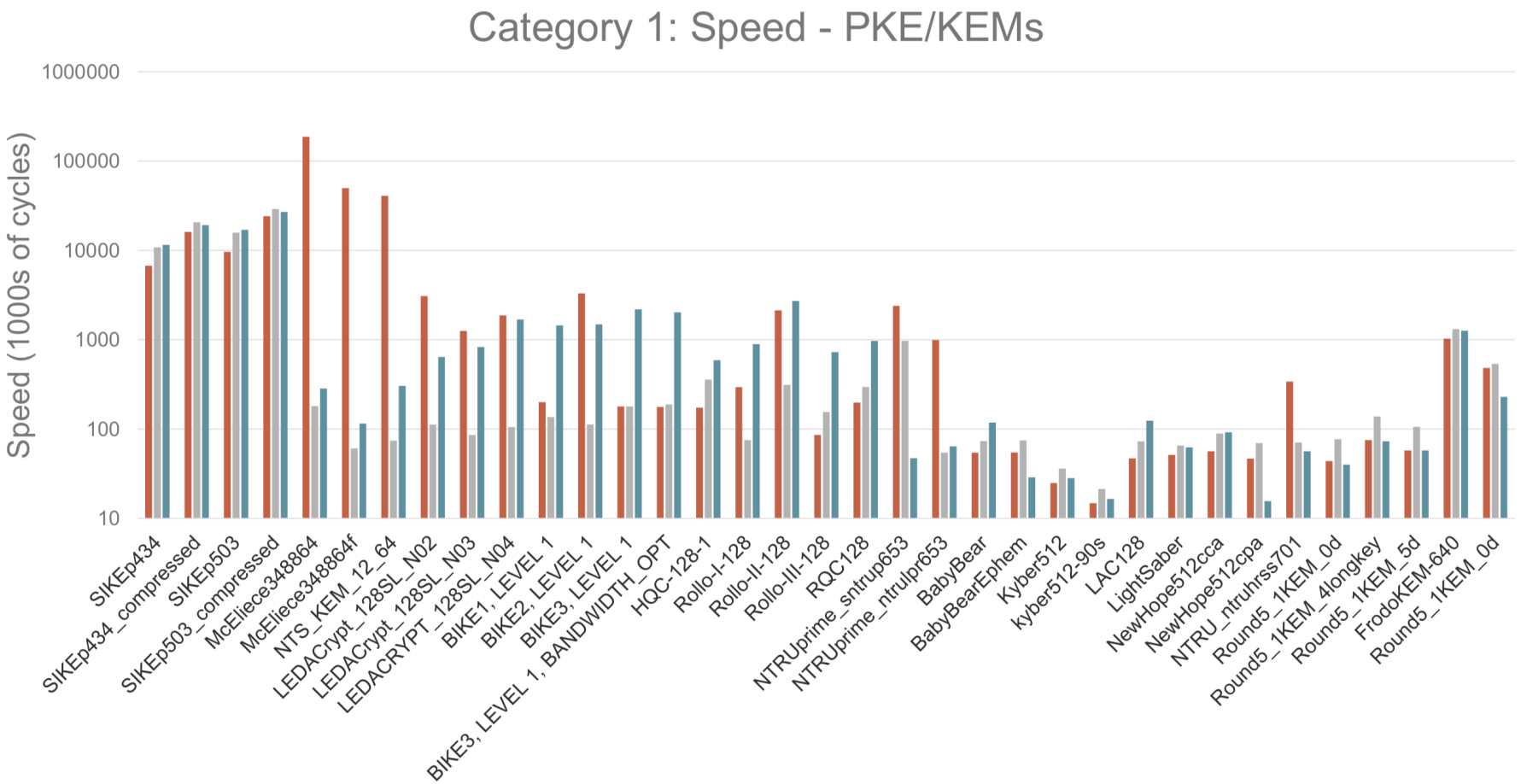
Performance

Scheme	Size (in Bytes)			AVX2 Cycles			Security
	sk	pk	ct	gen	enc	dec	
NewHope512	1888	928	1120	68,080	109,836	114,176	101
Kyber512	1632	800	736	33,428	49,184	40,564	100
LAC-128	1056	544	712	59,584	89,055	140,221	133
Kyber768	2400	1184	1088	62,396	83,748	70,304	164
LAC-192	2080	1056	1188	119,246	137,653	320,135	259
NewHope1024	3680	1824	2208	129,670	210,092	220,864	233
Kyber1024	3168	1568	1568	88,568	115,952	99,764	230
LAC-256	2080	1056	1424	135,780	207,938	359,209	290

sk secret key **pk** public key
ct ciphertext **gen** key generation
enc encryption or encapsulation **dec** decryption or decapsulation

Table 1. Comparison of NewHope, Kyber and LAC

Performance [Dus19]



A positive note

- LAC trials with a new direction to improve performance:
  - super small q + heavy error corrections;
  - c.f. different rings, lattice structures, etc.
- LAC has sparked a lot of new cryptanalysis technique.

Future work

- Improve error correction performance
- *Almost* constant time $\rightarrow$ constant-time implementation
- Re-write ring multiplication with Assembly
- Improve m4 and FPGA implementation


Alperin-Sheriff.
Official comment: Lac.
NIST PQC Forum, 2018.


Alperin-Sheriff.
Official comment: Lac.
NIST PQC Forum, 2018.


Jan-Pieter D'Anvers, Marcel Tiepelt, Frederik Vercauteren, and Ingrid Verbauwhede.
Timing attacks on error correcting codes in post-quantum secure schemes.
IACR Cryptology ePrint Archive, 2019:292, 2019.


Dustin Moody.
Opening remarks.
The 2nd Round of the NIST PQC Standardization Process, 2019.


Jan-Pieter D'Anvers, Frederik Vercauteren, and Ingrid Verbauwhede.
The impact of error dependencies on ring/mod-lwe/lwr based schemes.

In *Post-Quantum Cryptography - 10th International Conference, PQCrypto 2019, Chongqing, China, May 8-10, 2019 Revised Selected Papers*, pages 103–115, 2019.

Qian Guo, Thomas Johansson, and Jing Yang.
A novel cca attack using decryption errors against lac.
Asiacrypt, 2019.

Yongha Son.
A note on parameter choices of round5.
Cryptology ePrint Archive, Report 2019/949, 2019.
https://eprint.iacr.org/2019/949.