Side-Channel Attacks on NIST PQC 3rd Round Candidates

James Howe
Independent Researcher
jameshoweee@gmail.com

TABLE OF CONTENTS

01

Introduction

Why do we care about attacks on PQC?

NIST PQC Timeline so far

- Feb 2016 – NIST PQC “Competition” announced; CFP posted.
- Dec 2017 – 1^{st} Round begins; 69 submissions accepted (5 withdraw).
- April 2018 – 1^{st} NIST PQC Standardization workshop (@ Florida Atlantic).
- Jan 2019 – Round 2 candidates announced (17 KEM/PKEs + 9 Signatures).
- Aug 2019 – 2^{nd} NIST PQC Standardization workshop (@ CRYPTO).
- July 2020 – Round 3 finalists announced (4 KEMs + 3 Signatures), plus 8 alternates.
- June 2021 – 3^{rd} NIST PQC Standardization workshop.
- October 2021 – Cut off point for any new results on candidates for NIST’s consideration.
- ~2022-2024 – Draft standards for public comment.

Welcome to PQC Side-Channel Attacks

This is a talk about side-channel attacks (SCA) against NIST Post-Quantum Cryptography candidates.

NIST has repeatedly stated the importance of SCA and countermeasures:

- From the original NIST PQC call for proposals in 2016:
  "Schemes that can be made resistant to side-channel attacks at minimal cost are more desirable than those whose performance is severely hampered by any attempt to resist side-channel attacks."

- To the latest PQC summary document (NISTIR 8309):
  "NIST hopes to see more and better data for performance in the third round. This performance data will hopefully include implementations that protect against side-channel attacks, such as timing attacks, power monitoring attacks, fault attacks, etc."

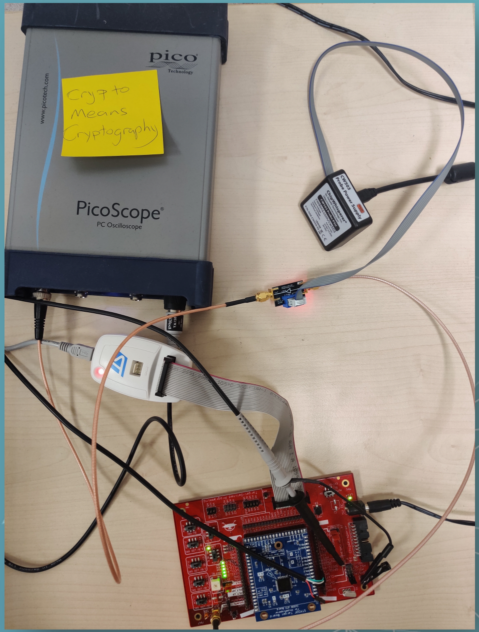
02

Attacks on NIST PQC Schemes

A survey of attacks on NIST PQC 3rd Round Candidates

Types of Attacks Considered

- **Classical cryptanalysis** mathematically analyzes a cryptosystem.
- **Timing analysis** exploits variable runtime of an algorithm.
- **Fault attacks** are semi-invasive methods to intentionally induce faults to reveal cryptographic internal states.
- **Simple**, **differential**, **correlation power analysis** non-invasively exploits variations in power consumption of a cryptographic algorithm.
- **Electromagnetic attacks** exploit radiation from a cryptographic algorithm.
- **Template attacks** profiles a sensitive device to gain access to the secret.
- **Cold-boot attacks** exploit memory remanence to read data out of a computer's memory after the computer has been powered off.
- **Countermeasures** protect/hinder attacks via hiding or masking methods.



A Disclaimer to the Survey

The purpose of this talk is to motivate more attacks.

By showing gaps in the state-of-the-art.

We try to remain as unbiased/neutral as possible:

- Presenting papers that directly attack a candidate.
- Thus, we only focus on KEMs and signatures.
- We try to assume implementations are correct.
- Oracle timings attacks [GJN20], etc., *should* be fixed by now.

A Summary of the Attacks on NIST PQC Candidates

Table1: Attacks on NIST PQC third round candidates categorized by classical cryptanalysis (CC), static timing analysis (STA), fault attacks (FA), simple power analysis (SPA), advanced (correlation/differential) power analysis (APA), electromagnetic (EM) attacks, template attacks (TA), cold-boot attacks (CB), and countermeasures (CM).

		PQC Scheme	CC	STA	FA	SPA	APA	EM	TA	CB	CM	References
Finalists	KEMs	Classic McEliece [BCL+19]			✓			✓		✓		[CCD+20][LNPS19][Pol18]
		Kyber [SAB+19]			✓	✓		✓	✓	✓		[RRB+19][XPRO20][RRCB20][RBRC20][PP19][ADP18]
		NTRU [ZCH+19]				✓				✓		[PV17][Pol18]
		Saber [DKRV19]						✓			✓	[RRCB20][RBRC20][Ver19][BDK+20]
	Signs	Dilithium [LDK+19]			✓			✓			✓	[BP18][RJH+19][RRB+19][MGTF19]
		Falcon [PFH+19]			✓							[MHS+19]
		Rainbow [DCP+19]	✓				✓			✓		[Beu20][PSKH18][Pol18]
Alternatives	KEMs	BIKE [ABB+19]		✓	✓							[GJN20][CCD+20]
		FrodoKEM [NAB+19]		✓		✓	✓	✓	✓	✓	✓	[GJN20][BFM+19][RRCB20][RRB+19][HMOR19][ATT+18]
		HQC [AAB+19]		✓			✓					[GJN20][CCD+20]
		NTRU Prime [BCLv19]					✓		✓		✓	[WZW13][HCY20]
		SIKE [JAC+19]	✓	✓								[CLN+20][GJN20]
	Signs	GeMSS [CFM+19]	✓				✓					[TPD20][PSKH18]
		Picnic [ZCD+19]	✓				✓					[DN19][LIM20][GSE20]
		SPHINCS+ [HBD+19]			✓							[CMP18]

General Observations on Attacks on PQC

Many candidates could have used inspections for secure coding practices.

- Lots of these were posted on the NIST PQC forum[1].

Things to be cautious of in code-based cryptography:

- Decoding *must* be implemented in constant-time.
- Be cautious of decoding methods that are insecure (e.g. Reed-Solomon).

What about hash-based signatures?

- Hash-based signatures are particularly sensitive to fault attacks.
- Stateful hash-based signatures need care in state management.
- SPHINCS+ has not had a lot of focus compared to others.

1. https://groups.google.com/a/list.nist.gov/g/pqc-forum

General Observations on Attacks on PQC

Things to be cautious of in lattice-based cryptography:

- Plenty of attacks found on schemes designed before the competition.
- No major cryptanalysis attacks on lattice hardness assumptions.
- Decryption failures need to be infeasible, even one is too many [DRV20].
- In general, masking schemes perform quite well.

What about isogeny-based cryptography?

- Unclear how effective attacks/countermeasures transfer from ECC.
- SIKE is the only NIST candidate, promising schemes designed since.
- CSIDH had a few damaging quantum attacks [Pei20, CSCDJRH20].
- New signature schemes proposed Wave [DST19] and SQISign [DFKL+20].

03

Recent Highlights

Some selected attacks relevant to the
NIST PQC standardization project.

New Classical Cryptanalysis of Rainbow and GeMSS in Round 3

Multivariate schemes in the 3rd Round:

- Rainbow (Finalist Signature)
- GeMSS (Alternate Signature)

Both substantially attacked near the start of the 3rd Round by new MinRank-style attacks [Beu20, TPD20]

- (Was not part of end-of-2nd-Round decision-making)

Rainbow loses ~16 bits of security at Level 1, and ~55 bits of security at Level 5

- (Rainbow team proposes new security analysis accounting for memory costs – correct?)

GeMSS loses up to 71 bits of security at Level 1, and up to 196 bits of security at Level 5

- Notably, there seems to be very little security gain between their Level 1 and Level 5 parameter sets now

LWE With Side Information

"When a side-channel attack fails, what can you still do with it?" – Léo Ducas.

- Lattice reduction (e.g. [ACD+18]) is a common method for deriving security levels.
- [DDGR20] propose a tool[1] to integrate "hints" from side-channels to use in lattice reduction.
- e.g. if you discover via side-channels HW$(s_0) = 2 \rightarrow s_0 \in \{3,5\}$, for $s_i \in \{-5, \dots, 5\}$.
- There are four types of hints:

Perfect:	Modular:	Approximate:	Short Vector Hints:
$\langle \boldsymbol{s}, \boldsymbol{v} \rangle = l$	$\langle \boldsymbol{s}, \boldsymbol{v} \rangle = l \bmod k$	$\langle \boldsymbol{s}, \boldsymbol{v} \rangle = l + \epsilon_\sigma$	$\boldsymbol{v} \in \boldsymbol{\Lambda}$

- These hints can reduce the BKZ block size, making attacks easier.

1. https://github.com/lducas/leaky-LWE-Estimator

LWE With Side Information

"When a side-channel attack fails, what can you still do with it?" – Léo Ducas.

This work may have impacts in the future:

- This could potentially affect certifications of cryptographic modules.
- Especially certifiers for Common Criteria, perhaps even FIPS 140-3 and more.
- Some certifiers (at least for symmetric) may require 2^{80}, or 2^{100} remaining keys **after** SCA.
- Thus, if this is unsatisfied, the implementation can 'fail'.

- **But** having this a priori knowledge could help certifications.
- One may now set cryptographic parameters with side channels in mind.

Masking Lattice-Based KEMs

Masked Ring-LWE (à la NewHope) [OSPG18] has large performance differences:

- Overheads in sampling and A2B conversion due to prime modulus.
- Overall, the performance for 1^{st} order protection is 5.7x slower than unprotected.
- Using Masked Comparison [BPO+20] this could be reduced further, but was broken.

The choice between Kyber and Saber may come down to side-channels and masking:

- Differences between these schemes is small, but their moduli differ.
- Masked Saber [Ver19,BDK+20] is 2.5x slower for 1^{st} order protection.
- Recent work [LS19,CHK+20] shows Saber and NTRU can benefit from using NTTs.

Masking Lattice-Based KEMs

We have seen attacks on Saber's 1st order masking scheme:

- In [NDJ21], session keys and secret keys are retrieved using deep neural networks (created at a profiling stage), but require 2.5k and 62k traces.
- They target multiple points in the masked logical shifting on arithmetic shares function, poly_A2A(), and its shuffled variant, poly_A2A_shuffled().

- In [NDGJ21] the session key and long-term secret-key are recovered from 16 traces using deep learning power analysis, without needing to profiling the scheme with masks deactivated.
- They target similar points-of-interest, poly_A2A() and POL2MSG(), for message recovery, and for the secret-key using maps from error-correcting codes using single and multiple traces.

- The target device is once more a very leaky Cortex M4, running at a lower frequency compared to [SKB21].

Masking Lattice-Based KEMs

Kyber have also designed a masked scheme [BGRSV21], for first-order as well as high-order protection. This is a relatively new publication so attacks have not been seen yet.

In [XPROYZ21] the unmasked Kyber is targeted to first find the secret key using EM, requiring 4 traces, on the reference implementation. The same attack is not viable for the assembly-optimised version, thus they target message recovery by also attacking the decoding function which requires profiling to find POIs.

More countermeasures are designed in [HP21] to protect against DPA and fault attacks. The DPA protection is realised in a RNR-protected NTT multiplier and achieves a relatively low overhead of 1.13x compared to unprotected.

Masking Lattice-Based Signatures

This issue is also seen in lattice-based signature schemes:

- Masked Dilithium [MGTF20] 7-9x faster using power-of-two modulus.
- Dilithium 1st order masking 5.6x slower compared to unprotected.
- Masking qTESLA [GR19] also gained efficiencies by changing modulus.

Masking Falcon will be slightly different:

- But now "isochronous" with constant runtime of Gaussian sampling [HPRR20].
- Its use of floating-point arithmetic makes masking an open problem.
- But has been considered before in MPC [ABZS13,GHK+20].
- Recent result called Mitaka: a simpler, parallelisable, maskable variant of Falcon.

Countermeasures are no Guarantee

But in general, we've only just begun protecting these schemes.

- There's many attack vectors to find and countermeasures need to be tested.

So far, we only have masked designs for Saber, Kyber and Dilithium.

- For first-order [MGT+19] and higher-order [BDK+19,BGR+21].

And obviously, countermeasures also not a guarantee.

- The masking scheme for the code-based scheme QcBits [RHH+17] was attacked [SKC+19].
- Masked comparison [BPO+20] used in lattice-based masked KEMs was attacked recently [BDH+21].
- As already discussed, Saber's masking has been broken by appropriate profiling and power analysis.

Active Side-Channel Attacks: QuantumHammer (LWEHammer?)

- QuantumHammer is a Rowhammer-style fault attack [MIS20] against LUOVß.
- Didn't have a large impact *on the process*, because of a concurrent work -- computational attack on LUOV [DDSVZ20].

- Intuition:
  1. Profile a victim device (e.g. in the cloud, like AWS) in an offline, pre-processing step.
  2. Online physical manipulation of the device while LUOV signature scheme is running.
     This causes the device to output malformed signatures that are secret key dependent.
  3. Computationally recover the secret key given enough malformed signatures.

- Is this more broadly applicable? (Upcoming work, joint NIST PQC + Univ of AR team – "LWEHammer").
- Rowhammer is an "old attack" (2014); modern cloud architectures *ought* to have defenses.
- Are the Rowhammer defenses enough in practice? Can Rowhammer be replaced by fault attacks, etc.?

Fault Attacks Against PQC

Determinism is generally considered preferrable from a security perspective.

Fault attacks have exploited determinism in SPHINCS+ [CMP18] and Dilithium [BP18,RJH+19].

- Many schemes counter this by adding random salt as an option or as standard.

Hedging [AOT+20] is an interesting alternative to mitigating these fault attacks (and randomness failures) is by deriving the per-signature randomness from a combination of the secret-key, message, and a nonce.

This is formalized for Fiat-Shamir signatures and apply the results to hedged versions of XEdDSA, a variant of EdDSA used in the Signal messaging protocol, and to Picnic2, and show hedging mitigates many of the possible fault attacks.

04

Takeaways for the Future

What can we learn from these attacks?

What can we learn from these attacks?

Implementation complexity will significantly increase with these standards.

- NIST set the focus on ARM Cortex M4 and Xilinx Artix-7.
- Will attacks or countermeasures we've seen be as effective on other devices?
- Will we see more attack vectors? Will we need more countermeasures?

Complexity also increased by the large number of fragile/sensitive operations.

- Past attacks highlight many sensitive/fragile operations that can break schemes.
- Even constant-time; e.g. how will *ctgrind* work with rejection sampling?

In order to learn the relevance of these attacks you should consider your use case.

- Some candidates will not fit on these devices, let alone smart cards.

Selecting the Correct Device

In order to learn the relevance of these attacks you should consider your use case.

Many of the attacks shown are on the ARM Cortex M4, a device NIST chose for benchmarking.

One recent research result looked at benchmarking Falcon and Dilithium on ARM Cortex M7.

- Similar to M4, except the M7 has a full 64-bit floating-point unit, needed by Falcon.

We wanted to benchmark, profile, and analyse Falcon on this embedded target using the FPU.

- Falcon signing ran more than 6x faster with the FPU, Dilithium had no improvements.
- Profiling Falcon we saw a 15-17x speed-up in many operations inside key gen and sign.

However, we saw some irregularities on the constant time performance of Falcon…

Selecting the Correct Device

We found a few subtle constant time issues with Falcon on Cortex M7 on STM32 development boards and ARMv7.

Firstly, 64-bit floating point operations are not fully constant-time on four STM32 development boards we tested that had ARM Cortex M7 CPUs.

For instance, $a \times b$ is much faster if $b = 0$. Worse, the timing of $a + b$ depends on relative sizes of the exponents of a and b.

We found constant-time issues with almost every operation on the four boards.

We did not investigate how to exploit these issues.

Selecting the Correct Device

Secondly, we discovered is an issue with Falcon on ARMv7.

When casting a double type to an int64_t, C prescribes to round towards zero.

There is no native instruction to do such a double→int64 truncation on ARMv7.
Instead, the compiler calls the runtime symbol __fixdfi, aka __aeabi_d2lz.

This might or might not be implemented in constant time.
In LLVM it is not – and it leaks the sign.

This is also the case for the Raspberry Pi 3, which they target in [6].
We reported this issue to the Falcon team and proposed a fix.

05

Conclusions

In Summary

We hope this survey will motivate further evaluations of NIST PQC candidates.

NIST will take these into consideration in their final decisions for standardization.

NIST PQC will add implementation complexities.

- We have seen many novel attacks due to the fragility of some operations.
- Many attacks were also enabled by implementation errors.

We discuss some open questions and implications of the attacks found.

Start your PQC transition now and consider the attacks that will affect your use cases.

Thanks

Does anyone have any questions?

jameshoweee@gmail.com

References

[AAB+19] Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean Christophe Deneuville, Philippe Gaborit, Edoardo Persichetti, and Gilles Zémor. HQC. Technical report, National Institute of Standards and Technology, 2019. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions.

[AASA+20] Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, et al. Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. NIST, Tech. Rep., July, 2020.

[ABB+19] Nicolas Aragon, Paulo Barreto, Slim Bettaieb, Loic Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Phillipe Gaborit, Shay Gueron, Tim Guneysu, Carlos Aguilar Melchor, Rafael Misoczki, Edoardo Persichetti, Nicolas Sendrier, Jean-Pierre Tillich, Gilles Zémor, and Valentin Vasseur. BIKE. Technical report, National Institute of Standards and Technology, 2019.

[ABZS13] Mehrdad Aliasgari, Marina Blanton, Yihua Zhang, and Aaron Steele. Secure computation on floating point numbers. In NDSS 2013. The Internet Society, February 2013.

[ACD+18] Martin R. Albrecht, Benjamin R. Curtis, Amit Deo, Alex Davidson, Rachel Player, Eamonn W. Postlethwaite, Fernando Virdia, and Thomas Wunderer. Estimate all the LWE, NTRU schemes! In Dario Catalano and Roberto De Prisco, editors, SCN 18, volume 11035 of LNCS, pages 351–367. Springer, Heidelberg, September 2018.

[ADP18] Martin R. Albrecht, Amit Deo, and Kenneth G. Paterson. Cold boot attacks on ring and module LWE keys under the NTT. IACR TCHES, 2018(3):173–213, 2018.

[ATT+18] Aydin Aysu, Youssef Tobah, Mohit Tiwari, Andreas Gerstlauer, and Michael Orshansky. Horizontal side-channel vulnerabilities of post-quantum key exchange protocols. In HOST, pages 81–88. IEEE, 2018.

References

[BCL+19] Daniel J. Bernstein, Tung Chou, Tanja Lange, Ingo von Maurich, Rafael Misoczki, Ruben Niederhagen, Edoardo Persichetti, Christiane Peters, Peter Schwabe, Nicolas Sendrier, Jakub Szefer, and Wen Wang. Classic McEliece. Technical report, National Institute of Standards and Technology, 2019.

[BCLv19] Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, and Christine van Vredendaal. NTRU Prime. Technical report, National Institute of Standards and Technology, 2019.

[BDK+20] Michiel Van Beirendonck, Jan-Pieter D'Anvers, Angshuman Karmakar, Josep Balasch, and Ingrid Verbauwhede. A side-channel resistant implementation of saber. Cryptology ePrint Archive, Report 2020/733, 2020.

[Beu20] Ward Beullens. Improved cryptanalysis of uov and rainbow. Cryptology ePrint Archive, Report 2020/1343, 2020. [BFM+19] Joppe W. Bos, Simon Friedberger, Marco Martinoli, Elisabeth Oswald, and Martijn Stam. Assessing the feasibility of single trace power analysis of Frodo. In Carlos Cid and Michael J. Jacobson Jr:, editors, SAC 2018, volume 11349 of LNCS, pages 216–234. Springer, Heidelberg, August 2019.

[BP18] Leon Groot Bruinderink and Peter Pessl. Differential fault attacks on deterministic lattice signatures. IACR TCHES, 2018(3):21–43, 2018.

[BPO+20] Florian Bache, Clara Paglialonga, Tobias Oder, Tobias Schneider, and Tim Güneysu. High-speed masking for polynomial comparison in lattice-based kems. IACR TCHES, 2020(3):483–507, 2020.

[CCD+20] Pierre-Louis Cayrel, Brice Colombier, Vlad-Florin Dragoi, Alexandre Menu, and Lilian Bossuet. Message-recovery laser fault injection attack on code-based cryptosystems. Cryptology ePrint Archive, Report 2020/900, 2020.

[CFM+19] A. Casanova, J.-C. Faugère, G. Macario-Rat, J. Patarin, L. Perret, and J. Ryckeghem. GeMSS. Technical report, National Institute of Standards and Technology, 2019.

References

[CHK+20] Chi-Ming Marvin Chung, Vincent Hwang, Matthias J. Kannwischer, Gregor Seiler, Cheng Jhih Shih, and Bo-Yin Yang. Ntt multiplication for ntt-unfriendly rings. Cryptology ePrint Archive, Report 2020/1397, 2020.

[CLN+20] Craig Costello, Patrick Longa, Michael Naehrig, Joost Renes, and Fernando Virdia. Improved classical cryptanalysis of SIKE in practice. In Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, editors, PKC 2020, Part II, volume 12111 of LNCS, pages 505–534. Springer, Heidelberg, May 2020.

[CMP18] Laurent Castelnovi, Ange Martinelli, and Thomas Prest. Grafting trees: A fault attack against the SPHINCS framework. In Tanja Lange and Rainer Steinwandt, editors, Post Quantum Cryptography - 9th International Conference, PQCrypto 2018, pages 165–184. Springer, Heidelberg, 2018.

[DCP+19] Jintai Ding, Ming-Shing Chen, Albrecht Petzoldt, Dieter Schmidt, and Bo-Yin Yang. Rainbow. Technical report, National Institute of Standards and Technology, 2019.

[DDGR20] Dana Dachman-Soled, Léo Ducas, Huijing Gong, and Mélissa Rossi. LWE with side information: Attacks and concrete security estimation. In Daniele Micciancio and Thomas Ristenpart, editors, CRYPTO 2020, Part II, volume 12171 of LNCS, pages 329–358. Springer, Heidelberg, August 2020.

[DKRV19] Jan-Pieter D'Anvers, Angshuman Karmakar, Sujoy Sinha Roy, and Frederik Vercauteren. SABER. Technical report, National Institute of Standards and Technology, 2019.

[DN19] Itai Dinur and Niv Nadler. Multi-target attacks on the Picnic signature scheme and related protocols. In Yuval Ishai and Vincent Rijmen, editors, EUROCRYPT 2019, Part III, volume 11478 of LNCS, pages 699–727. Springer, Heidelberg, May 2019.

[GHK + 20] Chuan Guo, Awni Hannun, Brian Knott, Laurens van der Maaten, Mark Tygert, and Ruiyu Zhu. Secure multiparty computations in floating-point arithmetic. arXiv preprint arXiv:2001.03192, 2020.

References

[GJN20] Qian Guo, Thomas Johansson, and Alexander Nilsson. A key-recovery timing attack on post-quantum primitives using the Fujisaki-Okamoto transformation and its application on FrodoKEM. In Daniele Micciancio and Thomas Ristenpart, editors, CRYPTO 2020, Part II, volume 12171 of LNCS, pages 359–386. Springer, Heidelberg, August 2020.

[GR19] François Gérard and Mélissa Rossi. An efficient and provable masked implementation of qtesla. In Sonia Belaïd and Tim Güneysu, editors, Smart Card Research and Advanced Applications - 18th International Conference, CARDIS 2019, Prague, Czech Republic, November 11-13, 2019, Revised Selected Papers, volume 11833 of Lecture Notes in Computer Science, pages 74–91. Springer, 2019.

[GSE20] Tim Gellersen, Okan Seker, and Thomas Eisenbarth. Differential power analysis of the picnic signature scheme. Cryptology ePrint Archive, Report 2020/267, 2020.

[HBD + 19] Andreas Hulsing, Daniel J. Bernstein, Christoph Dobraunig, Maria Eichlseder, Scott Fluhrer, Stefan-Lukas Gazdag, Panos Kampanakis, Stefan Kolbl, Tanja Lange, Martin M Lauridsen, Florian Mendel, Ruben Niederhagen, Christian Rechberger, Joost Rijneveld, Peter Schwabe, and Jean-Philippe Aumasson. SPHINCS+. Technical report, National Institute of Standards and Technology, 2019.

[HCY20] Wei-Lun Huang, Jiun-Peng Chen, and Bo-Yin Yang. Power Analysis on NTRU Prime. IACR TCHES, 2020(1), 2020.

[HMOR19] James Howe, Marco Martinoli, Elisabeth Oswald, and Francesco Regazzoni. Optimised Lattice-Based Key Encapsulation in Hardware. NIST's Second PQC Standardization Conference, 2019.

[HPRR20] James Howe, Thomas Prest, Thomas Ricosset, and Mélissa Rossi. Isochronous gaussian sampling: From inception to implementation. In Jintai Ding and Jean-Pierre Tillich, editors, Post-Quantum Cryptography - 11th International Conference, PQCrypto 2020, pages 53–71. Springer, Heidelberg, 2020.

References

[JAC + 19] David Jao, Reza Azarderakhsh, Matthew Campagna, Craig Costello, Luca De Feo, Basil Hess, Amir Jalali, Brian Koziel, Brian LaMacchia, Patrick Longa, Michael Naehrig, Joost Renes, Vladimir Soukharev, David Urbanik, and Geovandro Pereira. SIKE. Technical report, National Institute of Standards and Technology, 2019. [LDK + 19] Vadim Lyubashevsky, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Peter Schwabe, Gregor Seiler, and Damien Stehlé. CRYSTALS-DILITHIUM. Technical report, National Institute of Standards and Technology, 2019.

[LIM20] Fukang Liu, Takanori Isobe, and Willi Meier. Cryptanalysis of full lowmc and lowmc-m with algebraic techniques. Cryptology ePrint Archive, Report 2020/1034, 2020.

[LNPS19] Norman Lahr, Ruben Niederhagen, Richard Petri, and Simona Samardjiska. Side channel information set decoding. Cryptology ePrint Archive, Report 2019/1459, 2019.

[LS19] Vadim Lyubashevsky and Gregor Seiler. NTTRU: Truly fast NTRU using NTT. IACR TCHES, 2019(3):180–201, 2019.

[MGTF19] Vincent Migliore, Benoît Gérard, Mehdi Tibouchi, and Pierre-Alain Fouque. Masking Dilithium - efficient implementation and side-channel evaluation. In Robert H. Deng, Valérie Gauthier-Umaña, Martín Ochoa, and Moti Yung, editors, ACNS 19, volume 11464 of LNCS, pages 344–362. Springer, Heidelberg, June 2019.

[MHS+19] Sarah McCarthy, James Howe, Neil Smyth, Séamus Brannigan, and Máire O'Neill. BEARZ attack FALCON: implementation attacks with countermeasures on the FALCON signature scheme. In Proceedings of the 16th International Joint Conference on e-Business and Telecommunications, ICETE 2019 - Volume 2: SECRYPT, Prague, Czech Republic, July 26-28, 2019., pages 61–71, 2019.

[MIS20] Koksal Mus, Saad Islam, and Berk Sunar. QuantumHammer: A practical hybrid attack on the LUOV signature scheme. In Jay Ligatti, Xinming Ou, Jonathan Katz, and Giovanni Vigna, editors, ACM CCS 20, pages 1071–1084. ACM Press, November 2020.

References

[NAB+19] Michael Naehrig, Erdem Alkim, Joppe Bos, Léo Ducas, Karen Easterbrook, Brian LaMacchia, Patrick Longa, Ilya Mironov, Valeria Nikolaenko, Christopher Peikert, Ananth Raghunathan, and Douglas Stebila. FrodoKEM. Technical report, National Institute of Standards and Technology, 2019.

[OSPG18] Tobias Oder, Tobias Schneider, Thomas Pöppelmann, and Tim Güneysu. Practical CCA2-secure masked Ring-LWE implementations. IACR TCHES, 2018(1):142–174, 2018.

[PFH+19] Thomas Prest, Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang. FALCON. Technical report, National Institute of Standards and Technology, 2019.

[Pol18] Ricardo Luis Villanueva Polanco. Cold Boot Attacks on Post-Quantum Schemes. PhD thesis, Royal Holloway, University of London, 2018.

[PP19] Peter Pessl and Robert Primas. More practical single-trace attacks on the number theoretic transform. In Peter Schwabe and Nicolas Thériault, editors, LATINCRYPT 2019, volume 11774 of LNCS, pages 130–149. Springer, Heidelberg, 2019.

[PSKH18] Aesun Park, Kyung-Ah Shim, Namhun Koo, and Dong-Guk Han. Side-channel attacks on post-quantum signature schemes based on multivariate quadratic equations. IACR TCHES, 2018(3):500–523, 2018.

[PV17] Kenneth G. Paterson and Ricardo Villanueva-Polanco. Cold boot attacks on NTRU. In Arpita Patra and Nigel P. Smart, editors, INDOCRYPT 2017, volume 10698 of LNCS, pages 107–125. Springer, Heidelberg, December 2017.

[RBRC20] Prasanna Ravi, Shivam Bhasin, Sujoy Sinha Roy, and Anupam Chattopadhyay. Drop by drop you break the rock - exploiting generic vulnerabilities in lattice-based pke/kems using em-based physical attacks. Cryptology ePrint Archive, Report 2020/549, 2020.

References

[RJH+19] Prasanna Ravi, Mahabir Prasad Jhanwar, James Howe, Anupam Chattopadhyay, and Shivam Bhasin. Exploiting determinism in lattice-based signatures: Practical fault attacks on pqm4 implementations of NIST candidates. In Steven D. Galbraith, Giovanni Russello, Willy Susilo, Dieter Gollmann, Engin Kirda, and Zhenkai Liang, editors, ASIACCS 19, pages 427–440. ACM Press, July 2019.

[RRB+19] Prasanna Ravi, Debapriya Basu Roy, Shivam Bhasin, Anupam Chattopadhyay, and Debdeep Mukhopadhyay. Number "Not Used" Once-Practical Fault Attack on pqm4 Implementations of NIST Candidates. In International Workshop on Constructive Side-Channel Analysis and Secure Design, pages 232–250. Springer, 2019.

[RRCB20] Prasanna Ravi, Sujoy Sinha Roy, Anupam Chattopadhyay, and Shivam Bhasin. Generic side-channel attacks on CCA-secure lattice-based PKE and KEMs. IACR TCHES, 2020(3):307–335, 2020.

[SAB+19] Peter Schwabe, Roberto Avanzi, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Gregor Seiler, and Damien Stehlé. CRYSTALS-KYBER. Technical report, National Institute of Standards and Technology, 2019.

[TPD20] Chengdong Tao, Albrecht Petzoldt, and Jintai Ding. Improved key recovery of the hfev signature scheme. Cryptology ePrint Archive, Report 2020/1424, 2020.

[Ver19] Kasper Verhulst. Power Analysis and Masking of Saber. Master's thesis, KU Leuven, Belgium, 2019.

[WZW13] An Wang, Xuexin Zheng, and Zongyue Wang. Power analysis attacks and countermeasures on ntru-based wireless body area networks. KSII Transactions on Internet & Information Systems, 7(5), 2013.

[XPRO20] Zhuang Xu, Owen Pemberton, Sujoy Sinha Roy, and David Oswald. Magnifying side channel leakage of lattice-based cryptosystems with chosen ciphertexts: The case study of kyber. Cryptology ePrint Archive, Report 2020/912, 2020.

References

[ZCD+19] Greg Zaverucha, Melissa Chase, David Derler, Steven Goldfeder, Claudio Orlandi, Sebastian Ramacher, Christian Rechberger, Daniel Slamanig, Jonathan Katz, Xiao Wang, and Vladmir Kolesnikov. Picnic. Technical report, National Institute of Standards and Technology, 2019.

[ZCH+19] Zhenfei Zhang, Cong Chen, Jeffrey Hoffstein, William Whyte, John M. Schanck, Andreas Hulsing, Joost Rijneveld, Peter Schwabe, and Oussama Danba. NTRUEncrypt. Technical report, National Institute of Standards and Technology, 2019.