Quantum-resistant digital signatures schemes for low-power IoT

H. Hattenbach
Freie Universität Berlin

Seminar Internet of Things, 2021

Outline

Motivation
- Quantum Computing
- Internet of Things

Outline

Motivation

- Quantum Computing
- Internet of Things

Quantum Resistant Signature Schemes

- Performance Metrics
- different types
  - HBS
  - LBS

Outline

Motivation
- Quantum Computing
- Internet of Things

Quantum Resistant Signature Schemes
- Performance Metrics
- different types
  - HBS
  - LBS

Comparison
- FALCON
- Dilithium

Outline

Motivation
- Quantum Computing
- Internet of Things

Quantum Resistant Signature Schemes
- Performance Metrics
- different types
  - HBS
  - LBS

Comparison
- FALCON
- Dilithium

Conclusion

Outline

Quantum Computing breaks ordinary Cryptography

- sufficiently sized Quantum Computers (explained later) on the horizon
- They can break most of the cryptography in current use
  - RSA
  - ECDSA / ECDH
  - $\rightarrow$ Signal, WhatsApp, PGP, SSH, TLS/HTTPS, ...
- not everything equally effected
  - schemes in standardization to replace current cryptography
  - some are rather computationally intense
  - that is why i have a deeper look on which are feasable for IoT

Outline

Shors algorithm poses threat against asymmetric cryptography

- Quantum Computers operate on Qubits instead of normal Bits

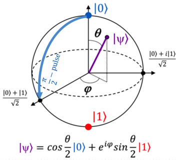


Figure: Model of a qubit [3]

- Algorithms can leverage those mechanics
  - up to exponential speed up in some cases
  - Shors algorithm completely breaks common asymmetric cryptography
    - can derive private key from public key
    - for everything based on Number-Theory (like RSA, ECDSA, ..)
  - Grovers algorithm poses threat against symmetric crypto and hash-functions
    - only quadratic speed-up
    - doubling length restores security (e.g. AES128 $\mapsto$ AES256)

Shors and Grovers algorithms

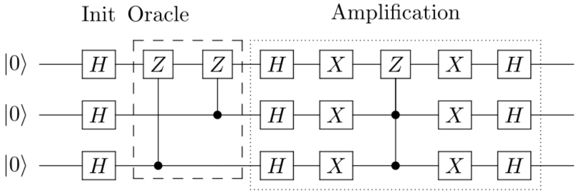


Figure: Grovers Algorithm [4]

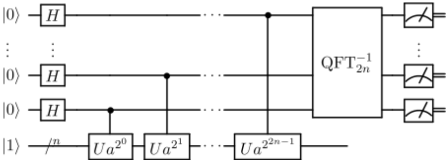


Figure: Shors Algorithm[5]

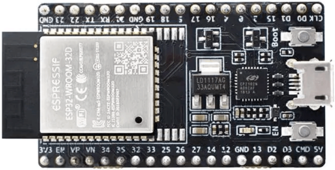
Outline

Many ressource constrained devices

- Internet of Things
- Smart-devices that are actually pretty dumb
  - little memory (kilobytes to megabytes)
  - low computing power (slow clock, small cache, etc.)
  - limited energy ressources (battery or solar operated)
- NIST classified into 3 classes:

Table: IETF IoT Classes

Class	RAM	Flash
C0	<< 10 KiB	<< 100 KiB
C1	10 KiB	100 KiB
C2	50 KiB	250 KiB



Outline

What makes a signature scheme better than any other?

- length of:
  - signature
  - public key
  - private key
- time and space needed to:
  - generate keys (GEN)
  - sign a message (SIGN)
  - verify a message (VER)
- security against quantum computers and traditional attackers

Table: QR Security classes and their traditional counterparts as classified by the NIST

Class	security comparable to
1	AES-128
2	SHA256
3	AES-192
4	SHA384
5	AES-256

Outline

Multiple types of underlying mathematica problems

- Super-singular isogeny based
  - SIKE
  - not well studied
- Multivariate polynomial based
  - Rainbow
  - not well studied
  - involves guessing work $\rightarrow$ not suited for low power devices
- Code based
  - McEliece
  - no finalist
- Hash based
  - SPHINCS+
  - big signatures (see next slide)
  - very well studied
- Lattice based
  - FALCON, Dilithium
  - most promising
  - most NIST finalists
  - most efficient
  - not as proofed as HBS

Hash Based Signatures

- Bases security upon Pre-Image resistance (of hash-functions) $\rightarrow$Well-Studied
- most simple form Lamport OTS:
  - private key: $2n$ random strings (two for each bit in digest)
  - public key: hash of these strings
  - sign by publishing one string for every bit in digest (either first or second)
- only useable one-time $\rightarrow$ publish x keys for x private keys
  - greatly improved by use of Merkle tree (no need for x keys, only one public)
  - but increases signature size by $\log(x)$

Lattice Based Signatures

- Bases security upon hardness ov CVP
  - find closest vector in a (High-d) Lattice
  - private key: short basis (red)
  - public key: long basis (black)
  - sign by providing a lattice vector close to a point on which the message would be mapped
  - hard with long basis but easy to verify
- keys are giant since high d requires $\mathcal{O}(d^2)$ scalars.
- reduce by introducing symmetries (NTRU[1])
- every signature leaks information about private key
  - don't give closest vector, but a close enough one
  - best to use gauss-sampling, but cryptographically hard

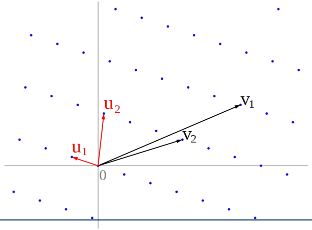


Table: Stack usage

Implementation name	GEN (bytes)	SIGN (bytes)	VER (bytes)
Dilithium-3 [21]	50k	86k	54k
2021 Dilithium(dyn)[10]	-	52k	36k
2021 Dilithium(sta)[10]	/ [2]	35k	19k
qTESLA-1 [21]	22k	29k	23k
qTESLA-3 [21]	43k	28k	45k
Falcon-5 [21]	120k	120k	120k
2021 FALCON [10]	-	42k	4.7k

Table: clock cycles

Implementation name	GEN	SIGN	VER
Dilithium-3 [21]	2.3	8.3	2.3
Dilithium-3 [23]	2.1	7.2	2.1
2021 Dilithium(dyn)[10]	-	29	3.4
2021 Dilithium(sta)[10]	-	8	1.5
qTESLA-3 [21]	30	11	2.2
Falcon-5 [21]	365	165	1
2021 Falcon [10]	-	75	1 [3]

Table: Flash sizes

Scheme	Size
FALCON	57KB
2021 Dilithium (Dyn)	11KB
2021 Dilithium (Sta)	26KB

Table: key and signature sizes

Scheme	public key	signature
SPHINCS	1KB	43KB
Dilithium-3	1.4KB	2.7KB
FALCON-1	900B	690B
FALCON-5	1.7KB	1.3KB
ECDSA	64B	64B

[2] precomputed key and directly stored in flash
[3] after optimizations these could be improved by further 43% [24]

Outline

FALCON is the fastest verifier

- most efficient by far for verification
  - smallest public key
  - smallest signature
  - fastest to verify
- great for verification only actors
- signing takes very long (1s)
  - since gauss sampling is used
  - also vulnerable to timing / side channel attacks (shown effective)

Outline

Dilithium is the best allrounder

- also great signing efficiency
- ditched gauss sampling
  - no FFT or FPA
  - everything in constant time $\rightarrow$ no timing attacks

QR IoT is possible

- two viable contenders for QR signatures in IOT:
  - Dilithium
  - FALCON
- already implemented with some kind of optimization
- still probably a little way up to key-length of ECDSA
- but already feasable for C2 devices and FALCON VER on C1

Ressources I

- https://github.com/PQClean/PQClean.
- https://github.com/mupq/.
- https://upload.wikimedia.org/wikipedia/commons/thumb/6/6b/Shor%27s_algorithm.svg/450px-Shor%27s_algorithm.svg.png.
- https://qiskit.org/textbook/ch-algorithms/images/grover_circuit_3qubits.png.
- https://www.researchgate.net/publication/335028508/figure/fig1/AS:789466423762944@1565234871365/The-Bloch-sphere-provides-a-useful-means-of-visualizing-the-s
ppm.
- https://www.mouser.de/images/espressifsystems/lrg/ESP32-DevKitC-32D_t.jpg.

Ressources II

- https://upload.wikimedia.org/wikipedia/commons/thumb/2/27/Lattice-reduction.svg/1200px-Lattice-reduction.svg.png.

- Erdem Alkim, Paulo S. L. M. Barreto, Nina Bindel, Juliane Krämer, Patrick Longa, and Jefferson E. Ricardini.
  The lattice-based digital signature scheme qtesla.
  In Mauro Conti, Jianying Zhou, Emiliano Casalicchio, and Angelo Spognardi, editors, *Applied Cryptography and Network Security*, pages 441–460, Cham, 2020. Springer International Publishing.

- IRIS ANSHEL, DEREK ATKINS, DORIAN GOLDFELD, and PAUL E. GUNNELLS.
  Walnutdsatm: A quantum-resistant digital signature algorithm.
  https://veridify.com/wp-content/uploads/2018/12/WP-walnutdsa-08-2018.pdf, 2018.

Ressources III

Gustavo Banegas, Koen Zandberg, Adrian Herrmann, Emmanuel Baccelli, and Benjamin Smith.
Quantum-resistant security for software updates on low-power networked embedded devices.
Cryptology ePrint Archive, Report 2021/781, 2021.
https://eprint.iacr.org/2021/781.

U. Banerjee, A. Pathak, and A. P. Chandrakasan.
2.3 an energy-efficient configurable lattice cryptography processor for the quantum-secure internet of things.
In *2019 IEEE International Solid- State Circuits Conference - (ISSCC)*, pages 46–48, 2019.

Ressources IV

PQShield The PQ Blog.
Falcon – a post-quantum signature scheme.
https://pqshield.com/falcon-a-post-quantum-signature-scheme/.
accessed june 2021.

C. Cheng, R. Lu, A. Petzoldt, and T. Takagi.
Securing the internet of things in a quantum world.
IEEE Communications Magazine, 55(2):116–120, 2017.

Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé.
Crystals-dilithium: A lattice-based digital signature scheme.
IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018(1):238–268, Feb. 2018.

Ressources V

T. M. Fernández-Caramés.
From pre-quantum to post-quantum iot security: A survey on quantum-resistant cryptosystems for the internet of things.
IEEE Internet of Things Journal, 7(7):6457–6480, 2020.

Pierre-Alain Fouque, François Gérard, Mélissa Rossi, and Yang Yu.
Zalcon: An alternative fpa-free ntru sampler for falcon.

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*, pages 74–91, Cham, 2020. Springer International Publishing.

Michael Heigl, Laurin Doerr, Martin Schramm2, and Dalibor Fiala1.
On the energy consumption of quantum-resistant cryptographic software implementations suitable for wireless sensor networks.
`https://www.scitepress.org/Papers/2019/78356/78356.pdf`, 2019.

Ressources VI

- Panos Kampanakis and Dimitrios Sikeridis.
  Two post-quantum signature use-cases: Non-issues, challenges and potential solutions.
  11 2019.
- Emre Karabulut and Aydin Aysu.
  Falcon down: Breaking falcon post-quantum signature scheme through side-channel attacks.
- A. Khalid, S. McCarthy, M. O'Neill, and W. Liu.
  Lattice-based cryptography for iot in a quantum world: Are we ready?
  In *2019 IEEE 8th International Workshop on Advances in Sensors and Interfaces (IWASI)*, pages 194–199, 2019.

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 - SECRYPT,*, pages 61–71. INSTICC, SciTePress, 2019.

M. J. O. Saarinen.
Mobile energy requirements of the upcoming nist post-quantum cryptography standards.
In *2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, pages 23–30, 2020.

Ressources VIII

- Tobias Oder, Julian Speith, Kira Höltgen, and Tim Güneysu.
  Towards practical microcontroller implementation of the signature scheme falcon.
  In Jintai Ding and Rainer Steinwandt, editors, *Post-Quantum Cryptography*, pages 65–80, Cham, 2019. Springer International Publishing.

- José Ignacio Escribano Pablos, María Isabel González Vasco, Misael Enrique Marriaga, and Ángel Luis Pérez del Pozo.
  The cracking of walnutdsa: A survey.
  2019.

- Ray A. Perlner and David A. Cooper.
  Quantum resistant public key cryptography: A survey.
  In *Proceedings of the 8th Symposium on Identity and Trust on the Internet*, IDtrust '09, page 85–93, New York, NY, USA, 2009. Association for Computing Machinery.

Ressources IX

Manohar Raavi, Simeon Wuthier, Pranav Chandramouli, Yaroslav Balytskyi, Xiaobo Zhou, and Sang-Yoon Chang.
Security comparisons and performance analyses of post-quantum signature algorithms.
In *International Conference on Applied Cryptography and Network Security*, pages 424–447. Springer, 2021.

S. Suhail, R. Hussain, A. Khan, and C. S. Hong.
On the role of hash-based signatures in quantum-safe internet of things: Current solutions and future directions.
IEEE Internet of Things Journal, 8(1):1–17, 2021.