

Quantum-resistant digital signatures schemes for low-power IoT

H. Hattenbach
Freie Universität Berlin

Seminar Internet of Things, 2021

Motivation

Motivation

Structure

- Skeleton
- Width-Coverage
- Depth-Coverage
- Ressources
- Schedule

- ▶ Quantum Computers operate on Qubits instead of normal Bits
- ▶ Qubits are Quantum-Mechanical
 - ▶ using spin of an electrons
 - ▶ Entanglement and Superposition
- ▶ Algorithms can leverage those mechanics
 - ▶ up to exponential speed up in some cases
 - ▶ Shors algorithm completely breaks common Encryption
 - ▶ everything based on Number-Theory (like RSA, ECDSA, ..)
 - ▶ (Qubits are currently rather unstable → not broken yet)

- ▶ There are a few proposed solutions
- ▶ mostly based on Lattice-Based hard Problems
 - ▶ Frodo-Kem (Encryption)
 - ▶ FALCON (Signature)
- ▶ IOT also needs to be secured
 - ▶ additional challenge of being low power/memory

Motivation

Structure

- Skeleton

- Width-Coverage

- Depth-Coverage

- Ressources

- Schedule

- ▶ Introduction
- ▶ Internet of Things
- ▶ Quantum Resistant Security
 - ▶ Quantum Computing
 - ▶ QR Algorithms
 - ▶ Performance Metrics
 - ▶ Encryption
 - ▶ Signatures
- ▶ QR Signatures in IoT
 - ▶ Performance Metrics in IoT
 - ▶ Failed Signatures
 - ▶ WalnutDSA
 - ▶ qTESLA
 - ▶ FALCON
- ▶ Conclusion

Motivation

Structure

Skeleton

Width-Coverage

Depth-Coverage

Ressources

Schedule

- ▶ Skimming multiple Quantum Resistant (QR) algorithms [15, 1] that focus on IoT [6, 12, 10, 5, 8]
- ▶ Deeper research about signature Schemes [16]
- ▶ and having a slightly more detailed look at two failed schemes [3, 14, 2, 7]

Motivation

Structure

Skeleton

Width-Coverage

Depth-Coverage

Ressources

Schedule

- ▶ having a deeper look at a NIST QR finalist with the most compact implementation:
FALCON [9, 13, 11]
- ▶ maybe having an outlook in the end on a Hardware-Accelerated QR chip [4]

Motivation

Structure




Skeleton


Width-Coverage


Depth-Coverage


Ressources

Schedule

-  <https://github.com/PQClean/PQClean>.
-  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.

- 

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.
- 

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.
- 



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.

- 



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.
- 

Panos Kampanakis and Dimitrios Sikeridis.
 Two post-quantum signature use-cases: Non-issues, challenges and potential solutions.
 11 2019.

-  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 - SECRIPT,, 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.
-  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.
-  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.

Motivation

Structure

- Skeleton
- Width-Coverage
- Depth-Coverage
- Ressources
- Schedule**

- ▶ 7.5. : skim breadth coverage literature
- ▶ 15.5.: write until signatures (at least bullet point comments)
- ▶ 30.5.: finish breadth (at least bullet point comments)
- ▶ α : skim and bullet point Depth
- ▶ 30.6.: finish