Volume 21, 2024 http://www.esecurity.ch/communications.html

Contents

1 Editorial

During the year 2024, quantum computing and post-quantum cryptography (PQC) have been hotly debated topics that have been almost impossible to avoid. While companies like IBM have further pursued their plans to build constantly growing quantum computers (in terms of number of qubits), the U.S. National Institute of Standards and Technology (NIST) released the first three PQC standards in August. These standards include CRYSTALS-Kyber (standardized in FIPS 203 as ML-KEM, standing for module-lattice-based key encapsulation mechanism), CRYSTALS-Dilithium (standardized in FIPS 204 as ML-DSA, standing for module-lattice-based digital signature algorithm), and SPHINCS+ (standardized in FIPS 205 as SLH-DSA, standing for stateless hash-based digital signature algorithm). In addition, a fourth standard is built around FALCON and will be standardized in FIPS 206 as FN-DSA, standing for FFT (fast-Fourier transform) over NTRU-lattice-based digital signature algorithm.[1] This sums up to three digital signature standards and one single KEM standard. Nevertheless, the NIST has called for additional digital signature proposals to be considered in the PQC standardization process to diversify its post-quantum signature portfolio. Since two signature schemes based on structured lattices have already been standardized, NIST has expressed particular interest in additional general-purpose signature schemes based on a security assumption that do not use structured lattices as well as signature schemes with short signatures and fast verification. This work is still going on.

Against this background, many companies and software manufacturers are busily implementing ML-KEM, ML-DSA, SLH-DSA, and/or FN-DSA and upgrading their products accordingly. Instead of replacing traditional public key cryptography with PQC, it is best practice to implement PQC in addition to traditional public key cryptography, and to put in place a respective hybrid system. This has the advantage that a failure in either type of cryptography does not necessarily compromise the other, meaning that a failure in one may be compensated by the other. If somebody is able to build a cryptographically relevant quantum computer (CRQC), then traditional public key cryptography may fail but the failure may be compensated by PQC. On the other hand, if somebody finds a failure in a new PQC algorithm, then the overall security may still be maintained by traditional public key cryptography. Hibridity thus helps to improve resilience.

Following a hybrid design strategy, the developers of the Signal E2EE messenger have updated one of their core protocols to make it resistant against quantum computers. More specifically, the extended Triple Diffie-Hellman (X3DH) protocol (that is at the core of the Signal protocol) is complemented with ML-KEM in a hybrid protocol known as post-quantum extended Diffie-Hellman (PQXDH). Thus, PQXDH is one of the first cryptographic security protocols that is assumed to be able to withstand a CRQC. Meanwhile, many other protocols have followed a similar approach, such as iMessage from Apple (where iMessage even goes one step further in terms of resistance against quantum computers) as well as Transport Layer Security (TLS) 1.3.

The PQXDH protocol and its use of ML-KEM is also addressed in *Signal and Messaging Layer Security*—my new and upcoming book that is scheduled to appear in 2025 (see below). The book has given me the opportunity to dive deeply into lattice-based cryptography and its use in ML-KEM and PQXDH. As usual, this deep dive has been intellectually stimulating, but also more challenging than originally anticipated. Anyway, it has required a lot of time during summertime, and I hope that you can profit from this effort when you read the book. The topic is difficult and I have given my best to make it as accessible as possible. Anyway, I expect the hype around quantum computing and PQC to continue, before it will eventually die down and normalize.

2 News

As mentioned above, Rof Oppliger has written a draft for his new and upcoming book entitled *Signal and Messaging Layer Security* that is scheduled to appear in 2025.[2] The book is to explain in detail the Signal protocol and its ingredients, as well as the new Messaging Layer Security (MLS) protocol that has been standardized by the IETF working group of the same name. The respective RFC 9420 was officially released in July 2023. The main challenge addressed by MLS is to specify a protocol that provides forward secrecy (FS) and post-compromise security (PCS) in a way that scales to potentially very large groups. In contrast to the Signal protocol, the MLS protocol is not yet widely deployed

[1] FALCON is based on a well-known lattice-based public key cryptosystem known as NTRU, where the name stands for "N-th degree Truncated polynomial Ring Units."

[2] `https://rolf.esecurity.ch/?page_id=1284`

in the field and there are only a few real-world implementations and that use it. Unfortunately, the book cover has not been designed yet, so it cannot be revealed here.

In addition to the new book, eSECURITY Technologies Rolf Oppliger has also worked out a new service offering called eSECURITY Cryptographic Knowledge (Cryptoledge).[3] The respective website looks as follows:

In short, eSECURITY Cryptoledge refers to a service that aims to provide expert knowledge and expertise in contemporary and state of the art cryptography to support and help out in application design and development projects that employ cryptographic techniques, mechanisms, algorithms, and/or protocols in one way or another. If you are interested in this service, then please let us know so we can give it a try. We assume that the service meets a demand in the market, but this is only an assumption.

3 Publications

In 2024, Rolf Oppliger has continued his line of research on risk management as originally initiated with the publication of "Quantitative Risk Analysis in Information Security Management: A Modern Fairy Tale" (IEEE Security & Privacy, Volume 13, Issue 6, December 2015) and "How To Manage Cyber Risks – Lessons Learnt from Medical Science" (IEEE Computer, Volume 56, January 2013). For the second publication, Rolf Oppliger teamed up with Andreas Grünert from the Swiss NCSC. They also explored the use of heuristics as an alternative to quantitative risk analysis in "How To Measure Cybersecurity and Why Heuristics Matter" (IEEE Computer, Volume 57, February 2024), and tried to explain "Why Probabilities Cannot Be Used in Cyber Risk Management" (Computer, Volume 57, October 2024). In their latest publication, they have also been joined by Ruedi Rytz (also from Swiss NCSC) and James Bret Michael (from the Naval Postgraduate School in Monterey, CA).

In this new team configuration, they have also started to address a new topic, namely the measurability and testability of IT security, and are about to publish some preliminary results in a first article soon.

4 Information Security and Privacy Books

In 2024, *Learning and Experiencing Cryptography with CrypTool and SageMath* (ISBN 978-1-68569-017-5) written by Bernhard Esslinger and his colleagues and *Medical Device Cybersecurity for Engineers and Manufacturers, Second Edition* (978-1-63081-991-0) written by Axel Wirth, Christopher Gates, and Jason Smith were published in the book series. Furthermore, a few new book projects are currently in the queue, including *Signal and Messaging Layer Security* mentioned above.

Also, the process of contracting new authors is going on. If you are working in the field and you are interested to write and publish a book in the series, then you may contact either the Series Editor (Rolf Oppliger) or one of the Commissioning Editors at Artech House (refer to the book series' homepage[4] for their coordinates).

5 Announcements

There are a few announcements to make regarding university lectures, courses, invited talks, as well as international conferences and workshops.

5.1 University Lectures

In the spring semester, Rolf Oppliger held his annual lecture on "IT Security" at the University of Zurich (UZH).[5] Again, the lecture (including the final exam)

[3] `https://cryptoledge.esecurity.ch`

[4] `https://www.esecurity.ch/serieseditor.html`

[5] `http://www.esecurity.ch/Teaching/uni-zh-2024.shtml`

took place onsite and was partly recorded with MS Teams. It was attended by more than 120 students.

The lecture will take place again in the spring semester of 2025. A preliminary version of the lecture slides can be downloaded from the lecture website that is publicly accessible.[6] Please, feel free to download the slides and provide feedback at will.

5.2 Courses

In 2024, no eSECURITY Academy course took place. But for 2025, the following courses and bootcamps are scheduled:

- Kryptografie — Entstehungsgeschichte und Funktionsweise der modernen Verschlüsselungstechnik, January 16, 2025 (1 day)
- Tor & Darkweb, January 23, 2025 (1 day)
- SSL und TLS Sicherheit, February 6 – 7, 2025 (2 days)
- Signal-Protokoll — Moderne End-zu-End- Nachrichtenverschlüsselung für Messaging-Dienste wie WhatsApp, March 6, 2025 (1 day)
- Bitcoin & Blockchain — Kryptografische Grundlagen und Funktionsweise, March 7, 2025 (1 day)
- Crypto Bootcamp, July 7 – 11, 2025 (5 days)
- Cybersecurity Bootcamp, July 14 – 18, 2025 (5 days)

All courses are German-speaking and will take place in Bern. You may find descriptions of the public courses and download respective flyers from eSECURITY Academy's website.[7]

Also, if you want eSECURITY Academy to organize and put into effect a private event that meets your specific needs and requirements (with a topic of your choice), then you may contact us directly. A private event can be held onsite or online, e.g., using MS Teams. It can also be customized in terms of scope and content, and we are open in most regards.

5.3 Invited Talks

During 2024, Rolf Oppliger repeated his introductory talk at the SBB security champions onboarding events a couple of times.

On July 2, he also gave an invited talk entitled "Riskomanagement in der Informatiksicherheit: Was wir von der Medizin lernen können." at the ISSS Zürcher Tagung on risk management.[8] The talk was well received and started a discussion.

5.4 Conferences and Workshops

In 2024, Rolf Oppliger has served as a member of the program committee for the following events (in chronological order):

- 14th ACM Conference on Data and Application Security and Privacy (CODASPY 2024), Porto (Portugal), June 19 - 21, 2024
- 19th ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS 2024), Singapore, July 1 - 5, 2024
- 21st International Conference on Security and Cryptography (SECRYPT 2024), Dijon (France), July 8 - 10, 2024
- 19th International Conference on Availability, Reliability and Security (ARES 2024), Vienna (Austria), July 30 - August 2, 2024
- 2nd Annual IEEE International Conference on Metaverse Computing, Networking, and Applications (MetaCom 2024), Hong Kong (China), August 12 - 15, 2024
- 26th International Conference on Information and Communications Security (ICICS 2024), Mytilene (Greece), August 26 - 30, 2024
- 9th International Conference on e-Democracy (eDemocracy 2024), Athens (Greece), September 26 - 27, 2024

Rolf Oppliger has already agreed to serve as a member of the program committee for several international conferences and workshops that will take place in 2025.[9]

About the Company

eSECURITY Technologies Rolf Oppliger is an independent and privately owned company founded in October 1999 to provide scientific and state-of-the-art consulting, education, and engineering services related to information technology security. The company is registered in the commercial register of Bern-Mittelland and located in Muri b. Bern, Switzerland.

[6] http://www.esecurity.ch/Teaching/uni-zh-2025.shtml

[7] https://academy.esecurity.ch

[8] https://isss.ch/veranstaltungeb-kurse/isss-zuercher-tagung-risk-management/

[9] https://rolf.esecurity.ch/?page_id=16