Sander Dorigo, sander.dorigo@fox-it.com

Sources

These are the main sources for information and photos that I used during my SECCON 22 presentation. Each reference is linked at the bottom of this PDF file.

- Fox Crypto website [Crypto(2022)]
- Huawei blocked from core 5G networks of major Dutch providers [Times(2022)]
- Modern quantum computer [Leprince-Ringuet(2021)]
- Shor's algorithm [Shor(1997)]
- Factoring 15 back into 3*5 [Vandersypen et al.(2001)Vandersypen, Steffen, Breyta, Yannoni, Sherwood, and Chuang]
- Post quantum efforts by NIST [NIST(2016)]
- Mosca's theorem [Mosca(2015)]
- Dueling over Dual_EC_DRGB [Kostyuk and Landau(2022)]
- BSI's quantum update from 2020 [BSI(2020)]
- Status of the quantum landscape [Jaques(2021)]
- Quantum Threat Timeline report [Institute(2021)]
- NIST logo [NIST(2007)]
- Results of NIST round 3 [NIST(2022)]
- 3.5 seconds vs 26 nanoseconds [Dridi and Alghassi(2017)]
- Breaking SPHINCS+ [Perlner et al.(2022)Perlner, Kelsey, and Cooper]
- Breaking SIKE [Castryck and Decru(2022)]
- Cloudflare TLS experiment [Kwiatkowski(2019)]

- OpenSSH 9.0 [OpenSSH(2022)]
- Cloudflare experiments in August 2022 [Westerbaan(2022)]
- Signal's double ratchet protocol [Marlinspike and Perrin(2016)]
- FrodoKEM by Microsoft [Microsoft(2022a)]
- McKinsey's quantum research [McKinsey(2019)] [McKinsey(2021)] [McKinsey(2022)]
- 1.8 Miljoen voor onderzoek naar quantum veiligheid publieke sleutelinfrastructuur [Welling(2021)]
- 10 million euros awarded for solving cyber security issues [NWO(2021)]
- Post-quantum cryptography according to TNO [TNO(2022)]
- Post-quantum cryptography according to AIVD [AIVD(2021)]
- Post-quantum cryptography according to BSI [BSI(2022)]
- Post-quantum cryptography according to ANSSI [ANSSI(2022)]
- Improving OpenVPN security [van Heesch et al.(2019)van Heesch, van Adrichem, Attema, and Veugen]
- Post Quantum SSH [Microsoft(2022b)]
- Stack Exchange [bbosak(2020)]
- Quantum in chemistry [Lee et al.(2022)Lee, Lee, Zhai, Tong, Dalzell, Kumar, Helms, Gray, Cui, Liu, Kastoryano, Babbush, Preskill, Reichman, Campbell, Valeev, Lin, and Chan]
- The quantum computing bubble [Gourianov(2022)]

Further reading

IF you're interested in reading more, check out these links. They refer to single tweets that inspired me, useful groups or pages, or other interesting tidbits.

- https://twitter.com/sejaques/status/1554482507399237634
- https://arstechnica.com/information-technology/2022/08/sike-once-a-post-quantum-encryption-contender-is-koed-in-nist-smackdown/
- https://martijn-dekker.medium.com/quantum-technology-is-a-blessing-for-information-security-5b25772618ac
- https://openquantumsafe.org/
- https://www.sanderdorigo.nl/stream (kind of an obvious plug)

References

[AIVD(2021)] AIVD. Bereid je voor op de komst van quantumcomputers, 2021. URL https://www.aivd.nl/binaries/aivd_nl/documenten/publicaties/2021/09/23/bereid-je-voor-op-de-dreiging-van-quantumcomputers/Bereid+je+voor+op+de+dreiging+van+quantumcomputers.pdf.

[ANSSI(2022)] ANSSI. Anssi views on the post-quantum cryptography transition, 2022. URL https://www.ssi.gouv.fr/en/publication/anssi-views-on-the-post-quantum-cryptography-transition/.

[bbosak(2020)] bbosak. Stack exchange - now that quantum computers have been out for a while, has rsa been cracked?, 2020. URL https://crypto.stackexchange.com/a/439.

[BSI(2020)] BSI. Status of quantum computer development, 2020. URL https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/P283_QC_Studie-V_1_2.html?nn=459758.

[BSI(2022)] BSI. Quantum-safe cryptography – fundamentals, current developments and recommendations, 2022. URL https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html?nn=433196.

[Castryck and Decru(2022)] Wouter Castryck and Thomas Decru. An efficient key recovery attack on sidh (preliminary version). Cryptology ePrint Archive, Paper 2022/975, 2022. URL https://eprint.iacr.org/2022/975. https://eprint.iacr.org/2022/975.

[Crypto(2022)] Fox Crypto. Fox crypto website, 2022. URL https://foxcrypto.com.

[Dridi and Alghassi(2017)] Raouf Dridi and Hedayat Alghassi. Prime factorization using quantum annealing and computational algebraic geometry. *Scientific Reports*, 7(1), feb 2017. doi: 10.1038/srep43048. URL https://doi.org/10.1038%2Fsrep43048.

[Gourianov(2022)] Dr Nikita Gourianov. The quantum computing bubble, 2022. URL https://www.ft.com/content/6d2e34ab-f9fd-4041-8a96-91802bab7765.

[Institute(2021)] Global Risk Institute. 2021 quantum threat timeline report, 2021. URL https://globalriskinstitute.org/publications/2021-quantum-threat-timeline-report/.

[Jaques(2021)] Samuel Jaques. Landscape of quantum computing in 2021, 2021. URL https://sam-jaques.appspot.com/quantum_landscape.

[Kostyuk and Landau(2022)] Nadiya Kostyuk and Susan Landau. Dueling over dual_ec_drgb the consequences of corrupting a cryptographic standardization process, 2022. URL https://harvardnsj.org/2022/06/dueling-over-dual_ec_drgb-the-consequences-of-corrupting-a-cryptographic-standardization-process/.

[Kwiatkowski(2019)] Kris Kwiatkowski. Tls post-quantum experiment, Oct 2019. URL https://blog.cloudflare.com/the-tls-post-quantum-experiment/.

[Lee et al.(2022)Lee, Lee, Zhai, Tong, Dalzell, Kumar, Helms, Gray, Cui, Liu, Kastoryano, Babbus
Seunghoon Lee, Joonho Lee, Huanchen Zhai, Yu Tong, Alexander M.

Dalzell, Ashutosh Kumar, Phillip Helms, Johnnie Gray, Zhi-Hao Cui, Wenyuan Liu, Michael Kastoryano, Ryan Babbush, John Preskill, David R. Reichman, Earl T. Campbell, Edward F. Valeev, Lin Lin, and Garnet Kin-Lic Chan. Is there evidence for exponential quantum advantage in quantum chemistry?, 2022. URL https://arxiv.org/abs/2208.02199.

[Leprince-Ringuet(2021)] Daphne Leprince-Ringuet. What is quantum computing? everything you need to know about the strange world of quantum computers, 2021. URL https://www.zdnet.com/article/what-is-quantum-computing-everything-you-need-to-know-about-the-strange-world-of-quantum-computers/.

[Marlinspike and Perrin(2016)] Moxie Marlinspike and Trevor Perrin. Specifications of the double ratchet algorithm, 2016. URL https://signal.org/docs/specifications/doubleratchet/.

[McKinsey(2019)] McKinsey. The next big thing? quantum computing's potential impact on chemicals, 2019. URL https://www.mckinsey.com/industries/chemicals/our-insights/the-next-big-thing-quantum-computings-potential-impact-on-chemicals.

[McKinsey(2021)] McKinsey. Pharma's digital rx: Quantum computing in drug research and development, 2021. URL https://www.mckinsey.com/industries/life-sciences/our-insights/pharmas-digital-rx-quantum-computing-in-drug-research-and-development.

[McKinsey(2022)] McKinsey. When - and how - to prepare for post-quantum cryptography, 2022. URL https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/when-and-how-to-prepare-for-post-quantum-cryptography.

[Microsoft(2022a)] Microsoft. Frodokem: Learning with errors key encapsulation, 2022a. URL https://github.com/microsoft/PQCrypto-LWEKE.

[Microsoft(2022b)] Microsoft. Post-quantum ssh, 2022b. URL https://www.microsoft.com/en-us/research/project/post-quantum-ssh/.

[Mosca(2015)] Michele Mosca. Cybersecurity in a quantum world: will we be ready?, 2015. URL https://csrc.nist.gov/csrc/media/events/workshop-

on-cybersecurity-in-a-post-quantum-world/documents/presentations/session8-mosca-michele.pdf.

[NIST(2007)] NIST. Nist logo, 2007. URL https://commons.wikimedia.org/wiki/File:NIST_logo.svg.

[NIST(2016)] NIST. Announcing request for nominations for public-key post-quantum cryptographic algorithms, 2016. URL https://csrc.nist.gov/news/2016/public-key-post-quantum-cryptographic-algorithms.

[NIST(2022)] NIST. Round 3 submissions - post-quantum cryptography: Csrc, 2022. URL https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions.

[NWO(2021)] NWO. 10 million euros awarded for solving cyber security issues, Apr 2021. URL https://www.nwo.nl/en/news/10-million-euros-awarded-solving-cyber-security-issues.

[OpenSSH(2022)] OpenSSH. Openssh 9.0 release notes, 2022. URL https://www.openssh.com/txt/release-9.0.

[Perlner et al.(2022)Perlner, Kelsey, and Cooper] Ray Perlner, John Kelsey, and David Cooper. Breaking category five sphincs+ with sha-256. Cryptology ePrint Archive, Paper 2022/1061, 2022. URL https://eprint.iacr.org/2022/1061. https://eprint.iacr.org/2022/1061.

[Shor(1997)] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, oct 1997. doi: 10.1137/s0097539795293172. URL https://doi.org/10.1137%2Fs0097539795293172.

[Times(2022)] NL Times. Huawei blocked from core 5g networks of major dutch providers, 2022. URL https://nltimes.nl/2021/05/21/huawei-blocked-core-5g-networks-major-dutch-providers.

[TNO(2022)] TNO. Well-prepared for the quantum age, 2022. URL https://www.tno.nl/en/focus-areas/information-communication-technology/roadmaps/trusted-ict/quantum/quantum-safe-crypto/.

[van Heesch et al.(2019)van Heesch, van Adrichem, Attema, and Veugen] Maran van Heesch, Niels van Adrichem, Thomas Attema, and Thijs Veugen. Towards quantum-safe vpns and internet. Cryptology ePrint Archive, Paper 2019/1277, 2019. URL https://eprint.iacr.org/2019/1277. https://eprint.iacr.org/2019/1277.

[Vandersypen et al.(2001)Vandersypen, Steffen, Breyta, Yannoni, Sherwood, and Chuang] Lieven M. K. Vandersypen, Matthias Steffen, Gregory Breyta, Costantino S. Yannoni, Mark H. Sherwood, and Isaac L. Chuang. Experimental realization of shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature*, 414(6866):883–887, dec 2001. doi: 10.1038/414883a. URL https://doi.org/10.1038%2F414883a.

[Welling(2021)] Rogier Welling. 1.8 miljoen voor onderzoek naar quantum veiligheid publieke sleutelinfrastructuur, Nov 2021. URL https://zynyo.com/blog-nieuws/hapkido-quantum-veiligheid/.

[Westerbaan(2022)] Bas Westerbaan. Experiment with post-quantum cryptography today, Aug 2022. URL https://blog.cloudflare.com/experiment-with-pq/.