PhD Defence of **Alexander Nilsson**:

“Decryption Failure Attacks on Post-Quantum Cryptography”

Introduction by Opponent
Dr. Markku-Juhani O. Saarinen, Professor of Practice [1,2]

[1]PQShield Ltd, Oxford, UK [2]Tampere University, Finland

May 11, 2023 | LTH, Lund University
Department of Electrical and Information Technology

Subject Matter of The Thesis:

Encryption Algorithms and Protocols

- **Enablers of everyday electronic commerce and remote working.** (TLS, SSH, VPNs.)

  End-to-end security allows us to buy things from Amazon, handle our bank or tax affairs from home, operate computers remotely, and to handle company data with our laptops.

Post-Quantum Cryptography (PQC)

- **Newer algorithms designed to be secure against attacks with quantum computers**.

  PQC Will replace older, vulnerable RSA and Elliptic Curve cryptography in browsers, etc.

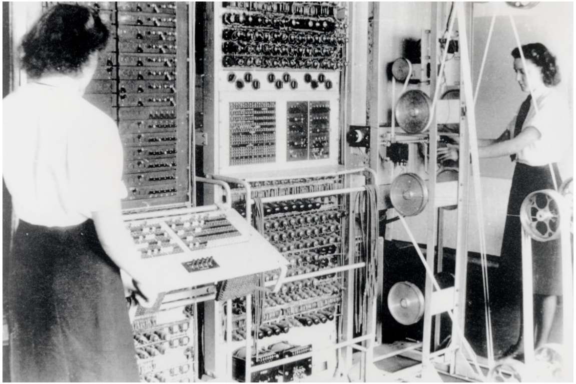
Cryptanalysis and Side-Channel Attacks (SCA)

- **Security is refined via adversarial analysis.** Vulnerabilities can be mathematical (cryptanalytic), or they can reside in the implementation of cryptosystems.

  The adversary can intercept, replay, or adaptively manipulate messages. High-precision observations about the behavior of systems may help to reveal secret information.

Quantum Computers: Why Cryptographers are Preparing

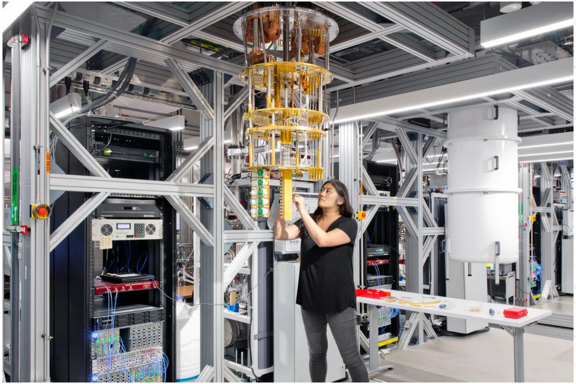
Bletchley Park (GC&CS), UK, 1943



Colossus Mark 2 codebreaking computer being operated by Dorothy Du Boisson and Elsie Booker.

Secret development of the Colossus digital computer during WW2 allowed the British to break the Lorentz cipher and read high-level German army messages.

IBM T. J. Watson, NY, USA, 2022



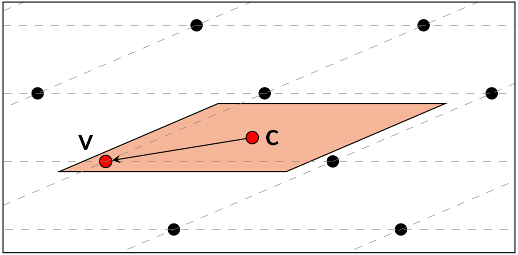
IBM Quantum System being worked on by Principal Research Scientist Maika Takita.

Sufficiently powerful quantum computers can break RSA and Elliptic Curve cryptography, on which much of the trust and security in the Internet is based on.

Designing Post-Quantum Cryptography Algorithms

While Factoring and Discrete Logarithm problems can be solved efficiently with quantum computers, there are mathematical problems that appear to be fundamentally hard.

Examples: Lattice problems (e.g., Learning With Errors) or problems from Coding Theory.



It is a complex challenge of cryptographic design to (provably!) translate such a problem into a practical public-key cryptosystem. One also needs to carefully model attacks to select suitable parameters so that the desired level of security against attacks holds.

PQC Development: The Context for This Thesis

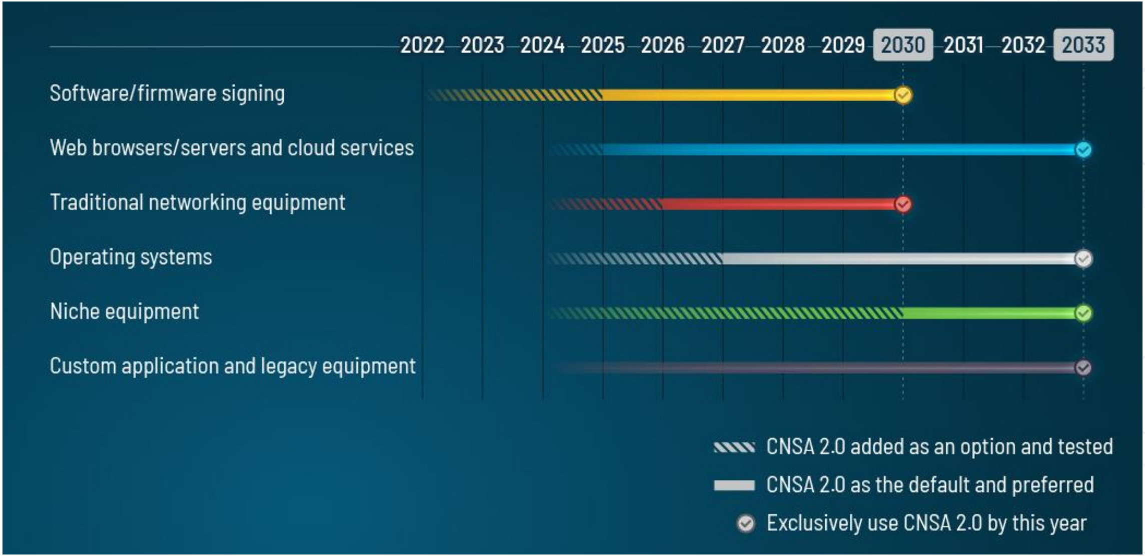
- → **1994:** Peter Shor shows that factoring (RSA) and Discrete Logarithm (Elliptic Curve) problems can be solved (in polynomial time) if a large quantum computer is built.
- → **2015:** National Security Agency (NSA) CNSS Advisory Memorandum 02-15. Indicates a long-term requirement for quantum-resistant cryptography standards.
- → **2016:** National Institute for Standards and Technology (NIST) starts an open, international standardization and evaluation process for PQC algorithms.

Many proposals were submitted to NIST, including the code-based schemes McEliece, BIKE, HQC and lattice-based schemes NTRU, FrodoKEM, Kyber discussed in Alexander's thesis.

- → **2022:** Crystals-Kyber selected as the primary PQC key establishment scheme by NIST.
- → **2024:** Ratification of official standards. Evaluation of McEliece, BIKE, HQC continuing.

Similar developments have been made with PQC Digital Signature (Authentication) algorithms: Crystals-Dilithium is the primary selection, with Falcon, SPHINCS+ also being standardized.

Adoption Timeframe Example: U.S. National Security Systems



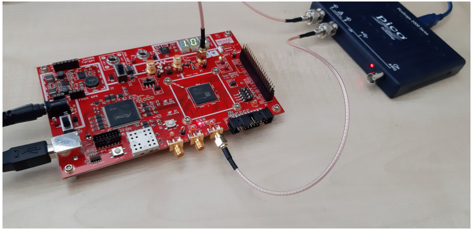
“Announcing the Commercial National Security Algorithm Suite 2.0.” U/OO/194427-22 | SEP 2022 https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

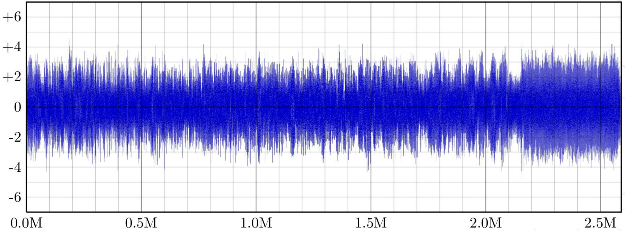
.. but you can also attack the implementation!

- Post-Quantum Cryptography will be used everywhere where classical cryptography is used: Web servers, Mobile Phones, Authentication Tokens, Payment cards, etc.

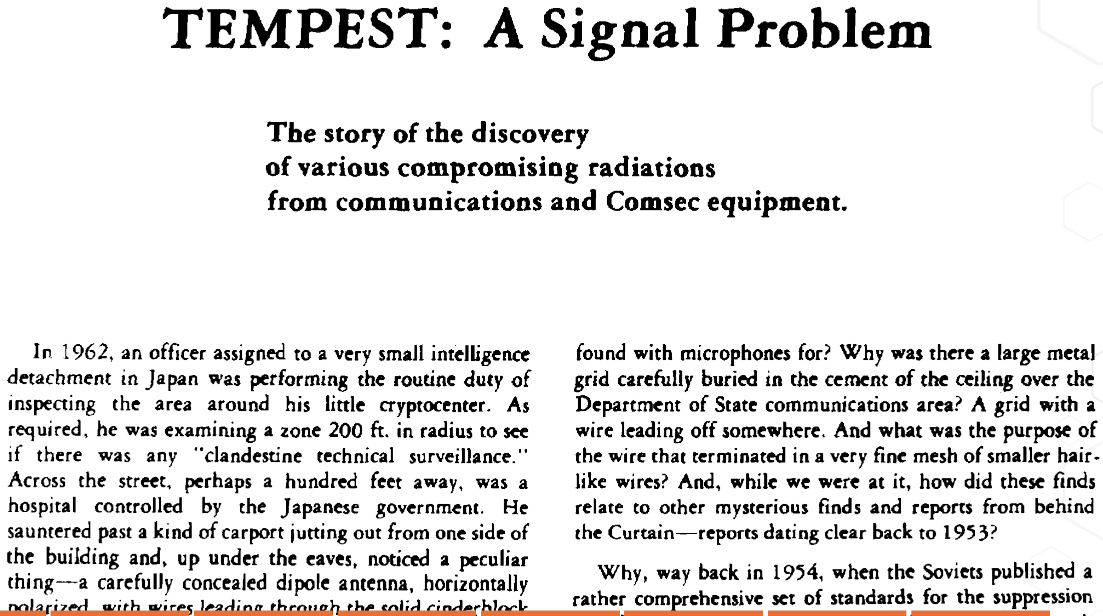
An example of a countermeasure against side-channel attacks:

- **Masking** is a *provable countermeasure* against side-channel leakage. Secret data $[\![\mathbf{s}]\!]$ is processed in d = **order** + 1 randomized shares $\mathbf{s}_i$. $[\![\mathbf{s}]\!] = \sum_{i=1}^{d} \mathbf{s}_i \pmod{q}$.
- You need all d shares $\mathbf{s}_i$ to learn $[\![\mathbf{s}]\!]$. If you only have partial observations (traces), the number needed grows *exponentially* in relation to d – and the masking order.





[Jerry Friedman, NSA Cryptologic Spectrum, Summer 1972.]



TEMPEST: A Signal Problem

The story of the discovery of various compromising radiations from communications and Comsec equipment.

In 1962, an officer assigned to a very small intelligence detachment in Japan was performing the routine duty of inspecting the area around his little cryptocenter. As required, he was examining a zone 200 ft. in radius to see if there was any "clandestine technical surveillance." Across the street, perhaps a hundred feet away, was a hospital controlled by the Japanese government. He sauntered past a kind of carport jutting out from one side of the building and, up under the eaves, noticed a peculiar thing—a carefully concealed dipole antenna, horizontally polarized, with wires leading through the solid cinderblock

found with microphones for? Why was there a large metal grid carefully buried in the cement of the ceiling over the Department of State communications area? A grid with a wire leading off somewhere. And what was the purpose of the wire that terminated in a very fine mesh of smaller hair-like wires? And, while we were at it, how did these finds relate to other mysterious finds and reports from behind the Curtain—reports dating clear back to 1953?

Why, way back in 1954, when the Soviets published a rather comprehensive set of standards for the suppression

The Devil is in The Details

“Don’t try to build a cryptosystem before you have broken at least a dozen.”

– A Wise Cryptography Professor

- **“Reaction attack”** refers to the reaction of a decryption oracle (attack target) to ciphertexts that have been specially crafted or modified by the attacker.
- The cryptosystem may respond with a special error code, delay, or other indicators that reveal information about the secret state of the target.
- Since both parties are computers (e.g., a web server and client), the attacker may perform thousands or millions of queries, with ciphertexts adapted dynamically based on responses, to ultimately derive secret keys. **Quantum computer not required.**