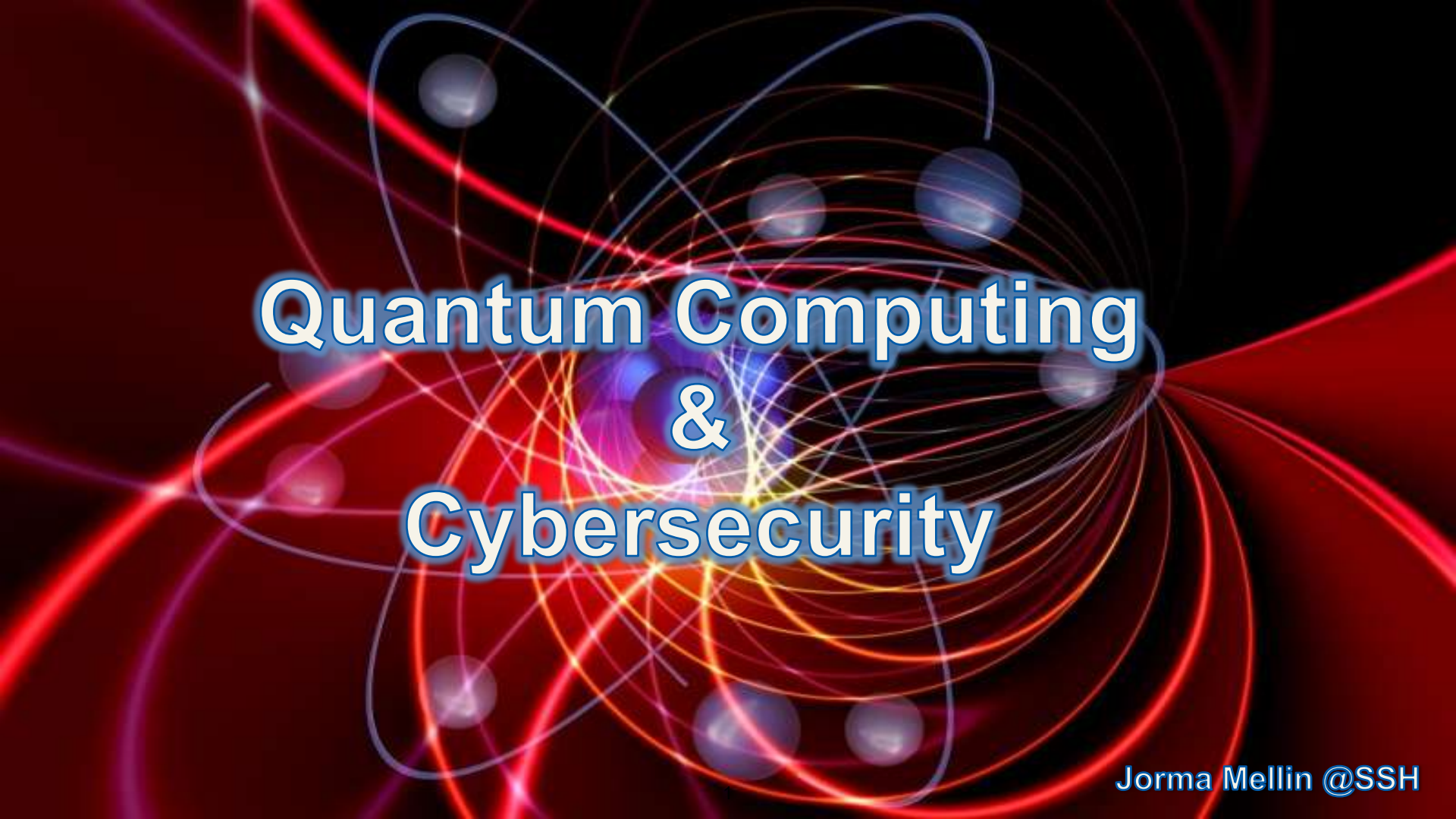

Quantum Computing
&
Cybersecurity
Jorma Mellin @SSH

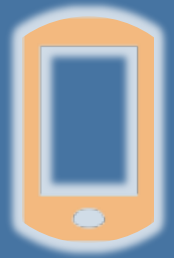
QUANTUM COMPUTING IN BRIEF

- Quantum runs qubits that can hold any position, not just 0 or 1
- Number of qubits is essential
- Measurement of qubic state is the key

- Quantum computers are programmed like legacy computers
- Quantum does not increase computing power
- Result of Quantum operation is not accurate

- Quantum algorithms will break cryptography
- Quantum safe algorithms are needed
- All digital societies rely on trust to algorithms

WHAT WILL COLLAPSE IF WE FAIL ON ENCRYPTION



Mobile networks

IoT systems

Cloud security

Secure browsing (HTTPS / TLS)

Secure email

VPN’s

Authentication

Digital Signatures

ID card security

Banking and Finance

Online accounts

Stock Market

Payment Systems


Quantum Threat

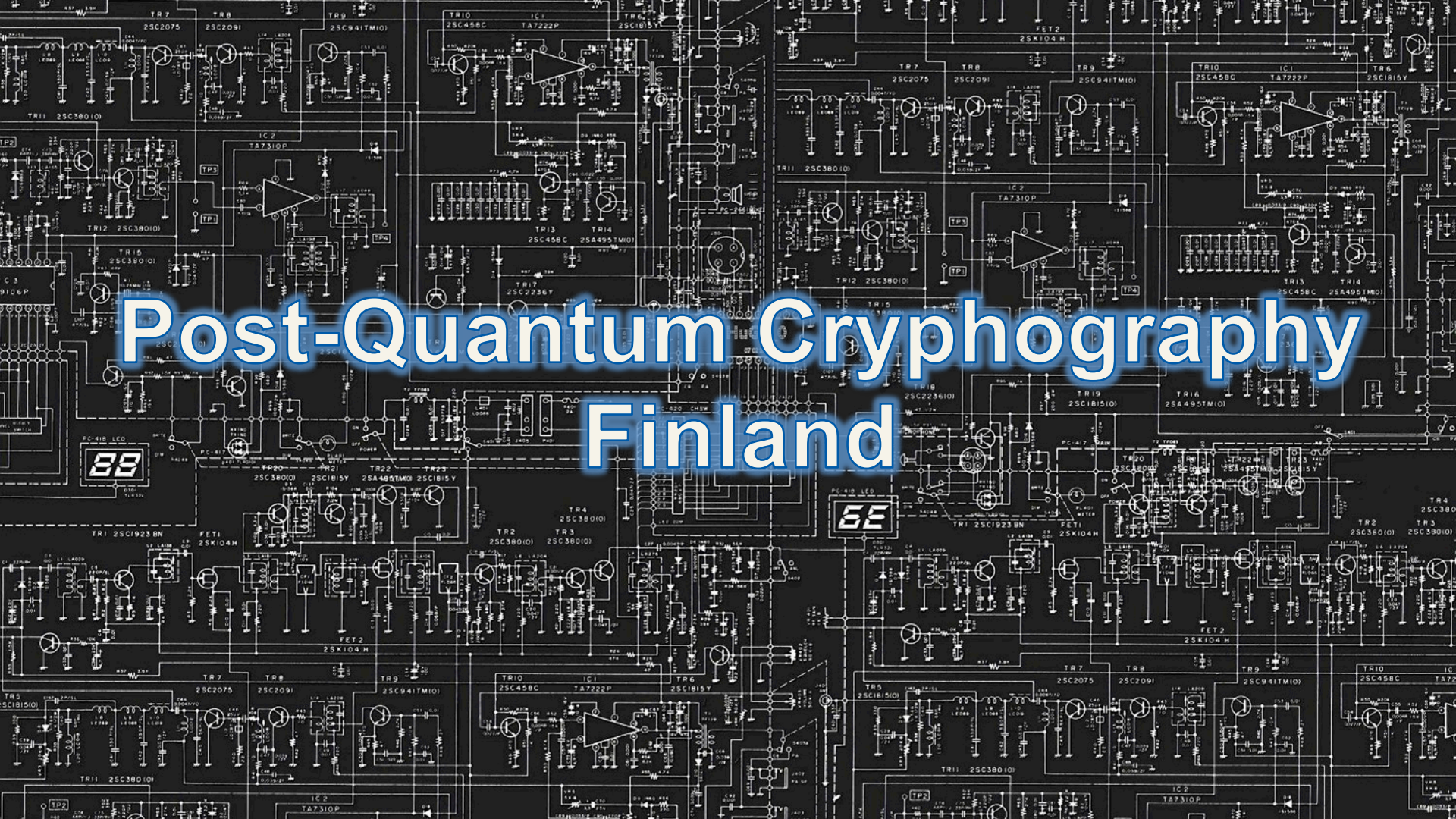
THREAT OF QUANTUM COMPUTER – AN EXAMPLE

- Asymmetric keys are multiples of two prime numbers
  - Easy to multiply two numbers together
  - Impossible to calculate which two numbers were multiplied (in legacy)

- With **Shor** algorithm ran in Quantum Computer, against an asymmetric key
  - Outcomes the range where the two original numbers exists
  - Reveals the two most likely prime numbers that were multiplied

- Outcome from Quantum Computer is a “best guess” and need to be verified with a legacy computer to get proof

- Key-length influence to number of qubits required to be efficient


Post-Quantum Cryphography
Finland

BUSINESS FINLAND -- DIGITAL TRUST PROJECT PQC--

- **Project targets (initially 2 year timeframe)**
  - Develop Finnish cryptography knowhow and skills further
  - Gain understanding how Finland can prepare for Quantum era
  - Strengthen national cybersecurity networks and forums in cryptology and in quantum technology
  - Prepare interfaces (API) for Quantum Safe algorithms
  - Create criteria and practices for certification of post-quantum products and services
  - Improve Finnish technology sector vendors in export struggles
  - Improving international cooperation also outside of academica

BUSINESS FINLAND -- DIGITAL TRUST PROJECT PQC--

- **Project in practise**
  - VTT act as project manager
  - Project steering group is formed
  - Three streams that share information
    - Quantum Computers, status, development and possibilities
    - Requirements for Quantum Safe in public key cryptography
    - Quantum Safe algorithms, theoretical models
  - Post-Quantum Cryptography pilots (proof of concept, evaluations)
    - Cryptolibraries, API, power consumption, effectiveness …)
  - Certification of PQC products and services
  - State of national crypto and Quantum strategy
  - Development areas towards 2030

SSH.COM

VTT

BUSINESS FINLAND

Puolustusvoimat
The Finnish Defence Forces

INSTA

advenica

TRAFICOM

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

TOSIBOX®

SECTRA

DIGI- JA VÄESTÖTIETO-VIRASTO

Bittium

Aalto-yliopisto

Encryption is Our Last Line of Defense