



NTNU

Norwegian University of
Science and Technology

The quantum (in-)secure future of the financial sector

Tjerand Silde – Cyber security in 20 minutes

Introduction

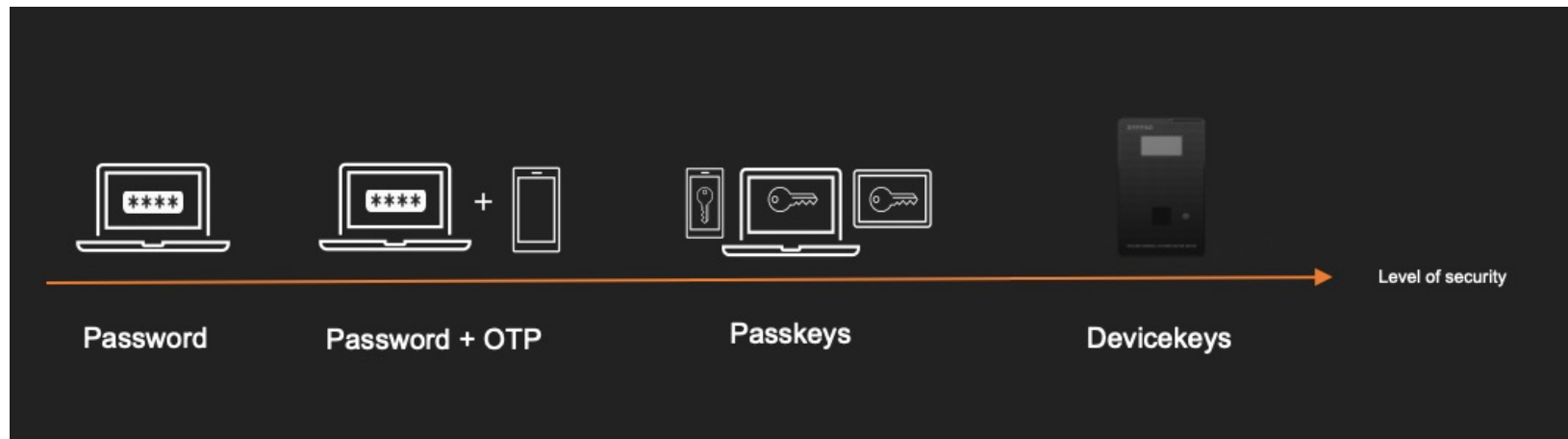
Associate Professor, Department
of Information Security and
Communication Technology, NTNU

Security and Cryptography Expert
at Pone Biometrics

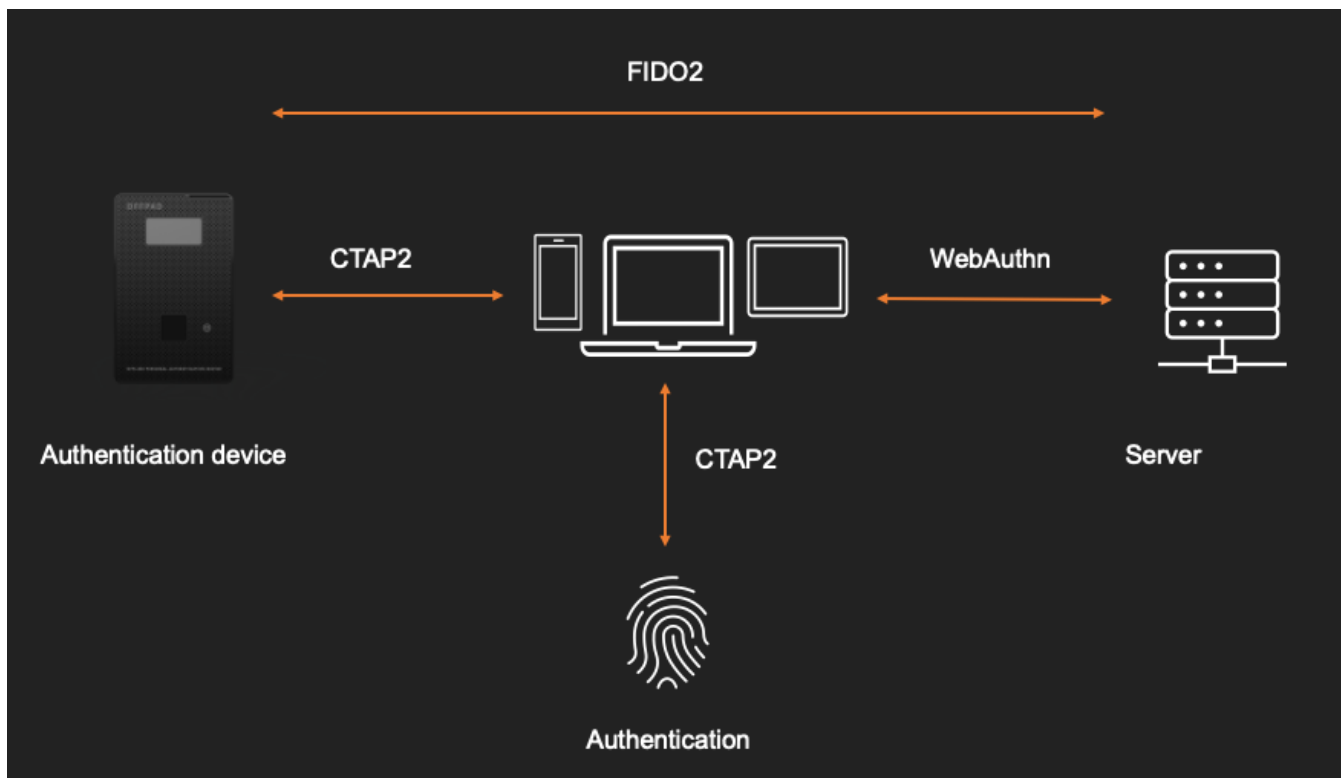
Researching privacy applications
and post-quantum cryptography



Secure Authentication



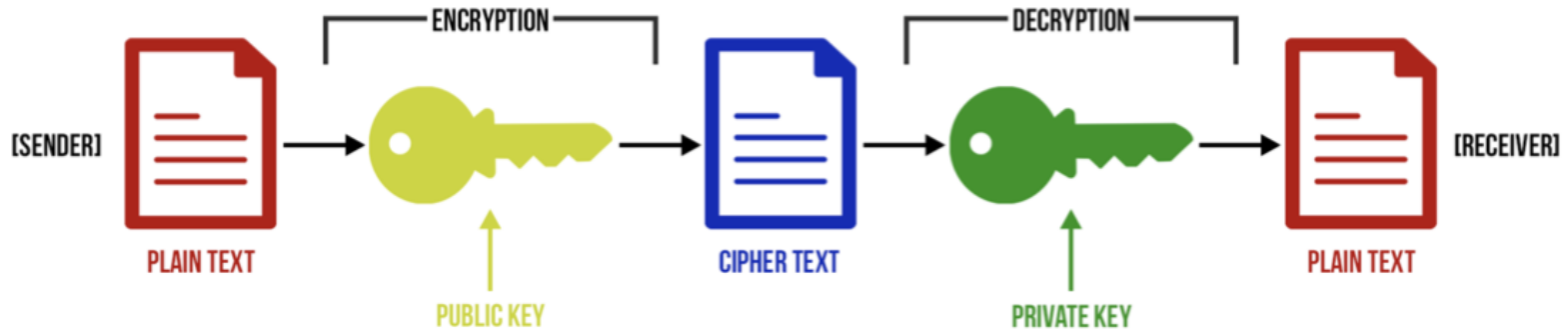
The FIDO Ecosystem



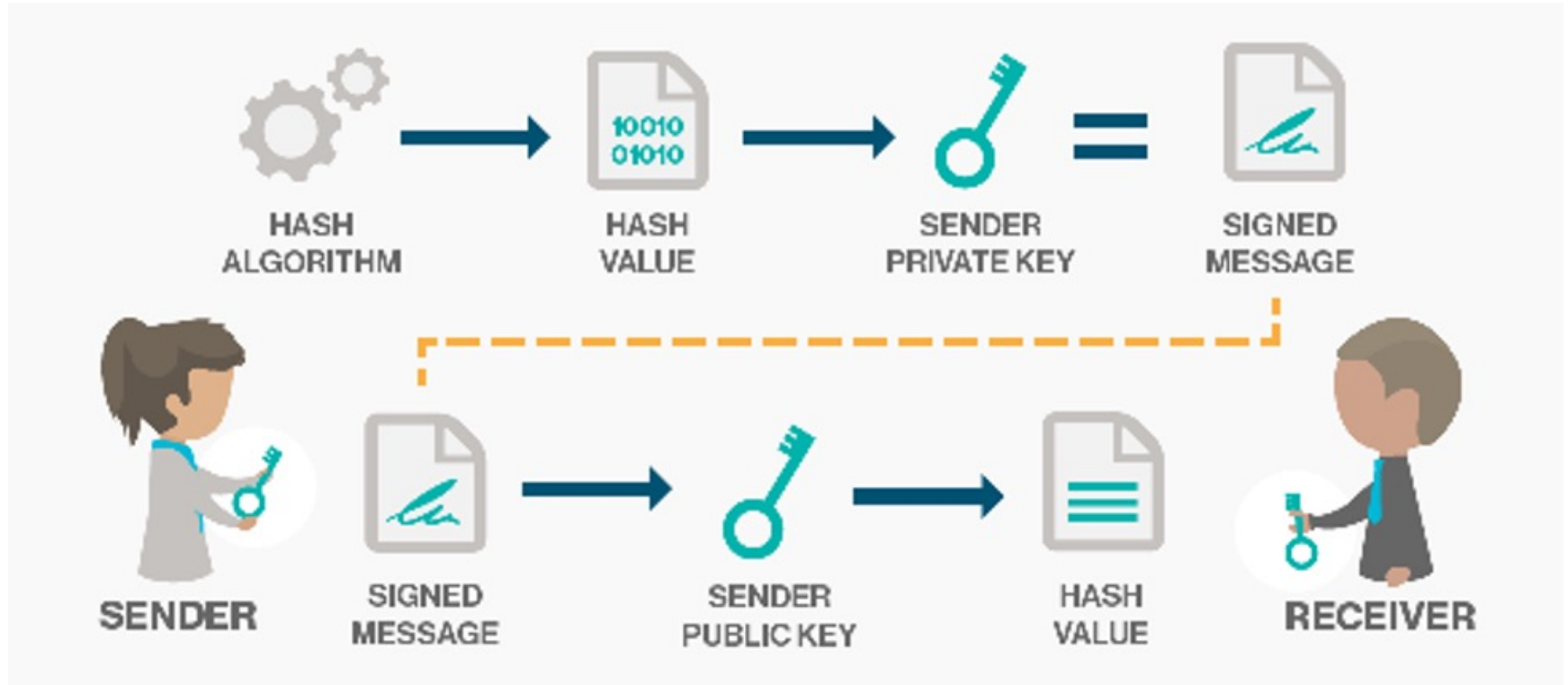
Symmetric Key Encryption



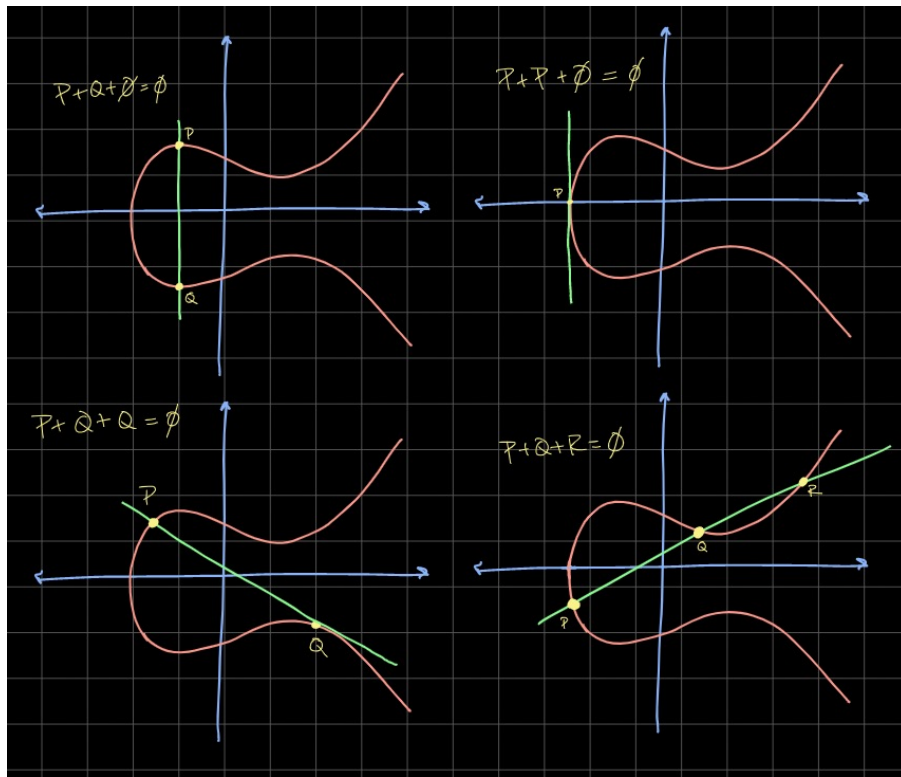
Public Key Encryption



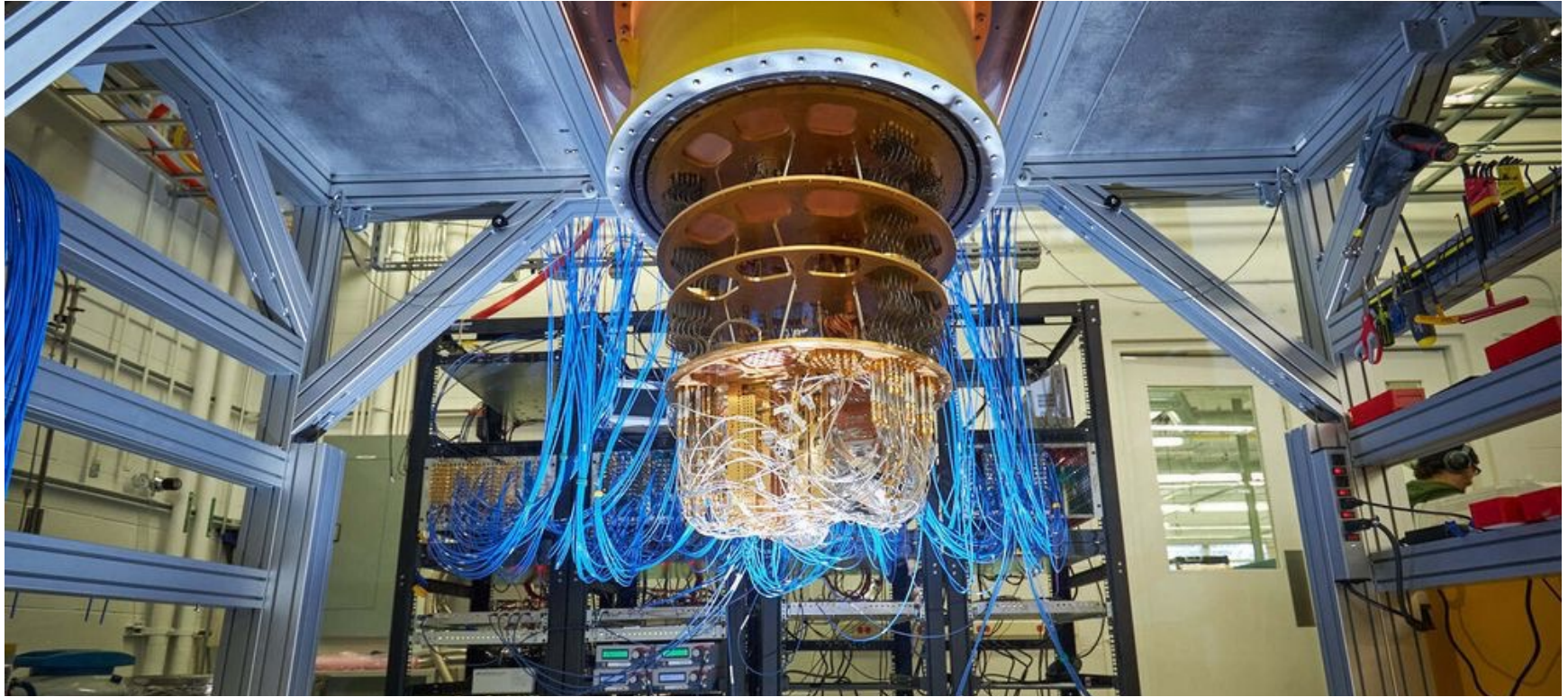
Digital Signatures



Today: Elliptic Curves



Quantum Computers are Coming!



Using Cryptography Online



Scott Hanselman ✓

@shanselman

Follow



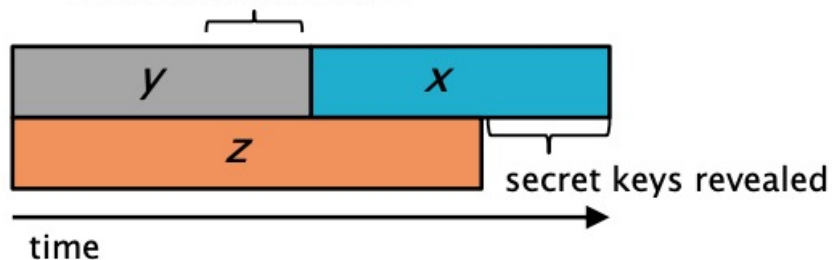
HTTPS & SSL doesn't mean "trust this." It means "this is private." You may be having a private conversation with Satan.



Lifetime of Data Protection

Theorem (Mosca): If $x + y > z$, then problem

What do we do here??



x – how long data needs to be safe

y – time for standardization and adoption

z – time until quantum computers

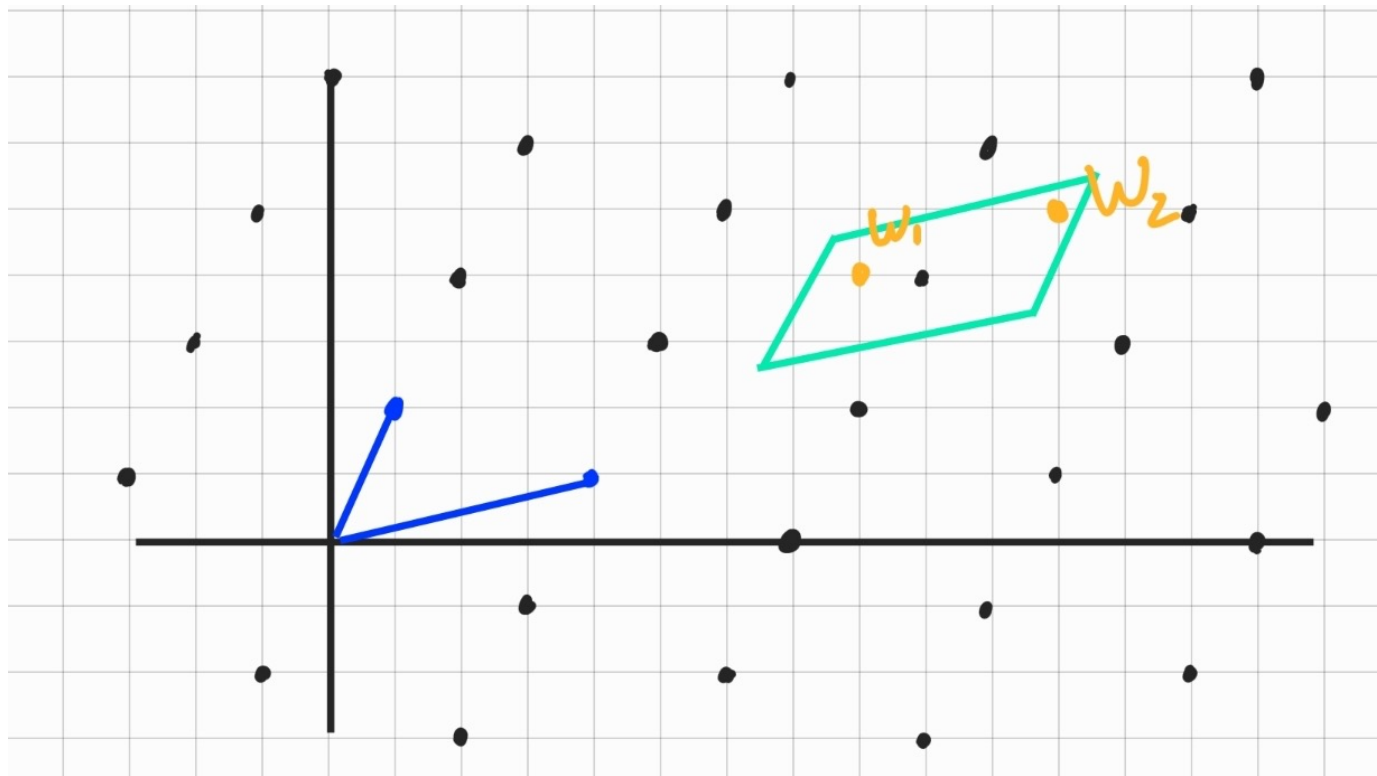
PQC Standardization

The Beginning of the End: The First NIST PQC Standards

Dustin Moody
Post-Quantum Cryptography Team



Tomorrow: Lattices



Thank you! Questions?

Email: tjerand.silde@ntnu.no

Web: tjerandsilde.no