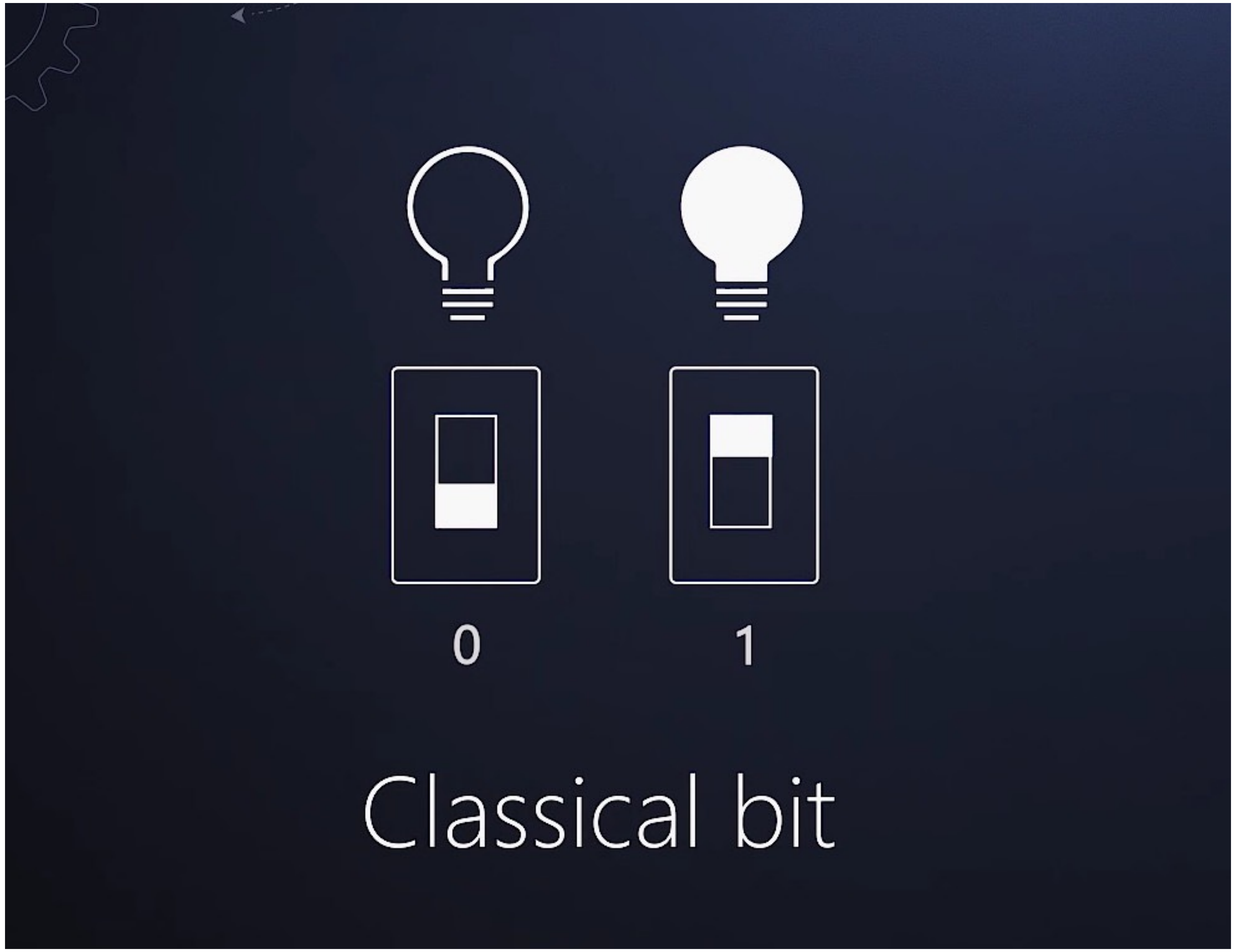
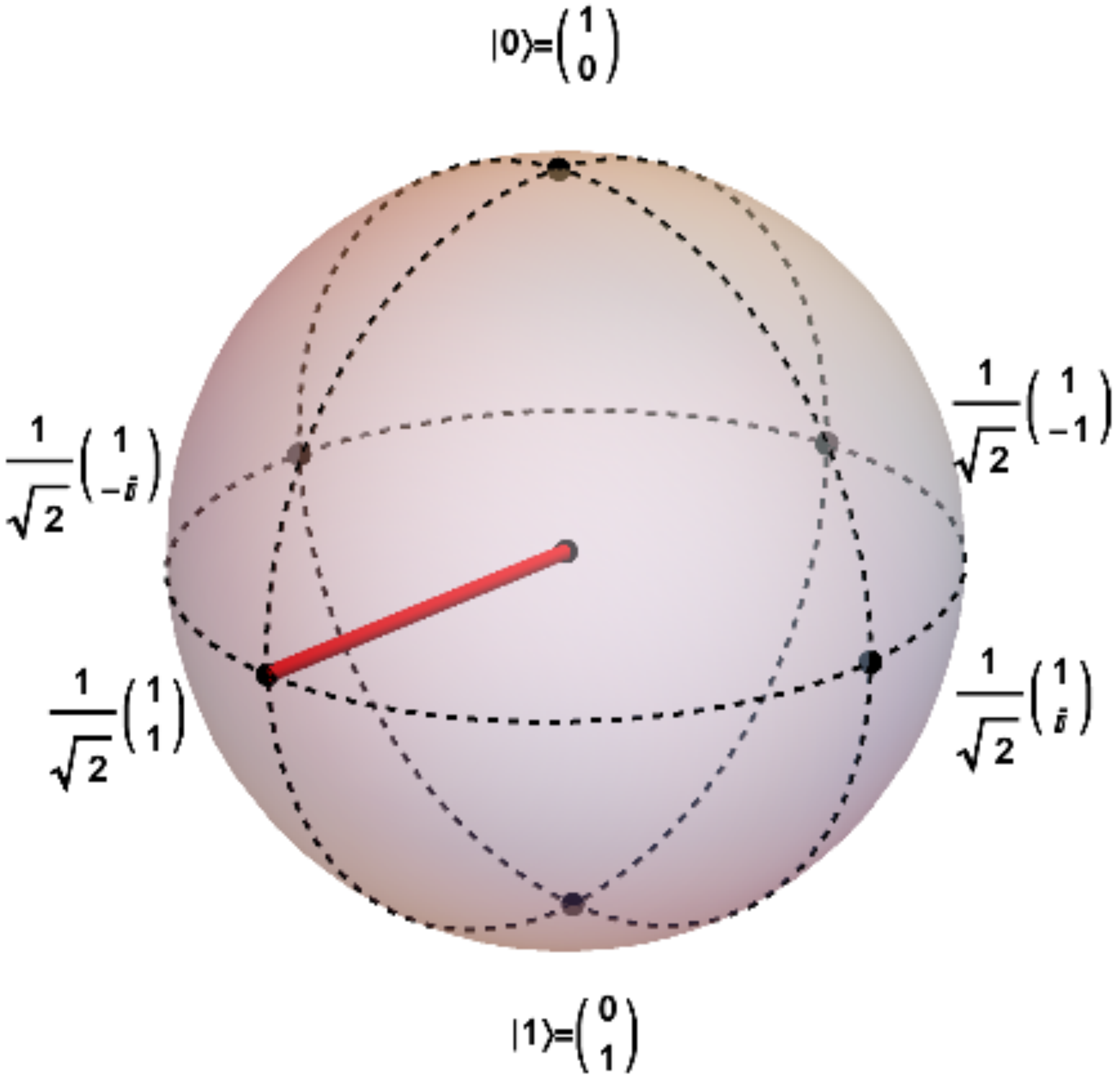
Emerging Security Revolution as a Response to the Quantum Mechanics Threats

Tomáš Rosa, Ph.D.
Cryptology and Biometrics Competence Centre & Quantum Computations Innovation Lab
Raiffeisen BANK International

Classical Computer - Classical Bit

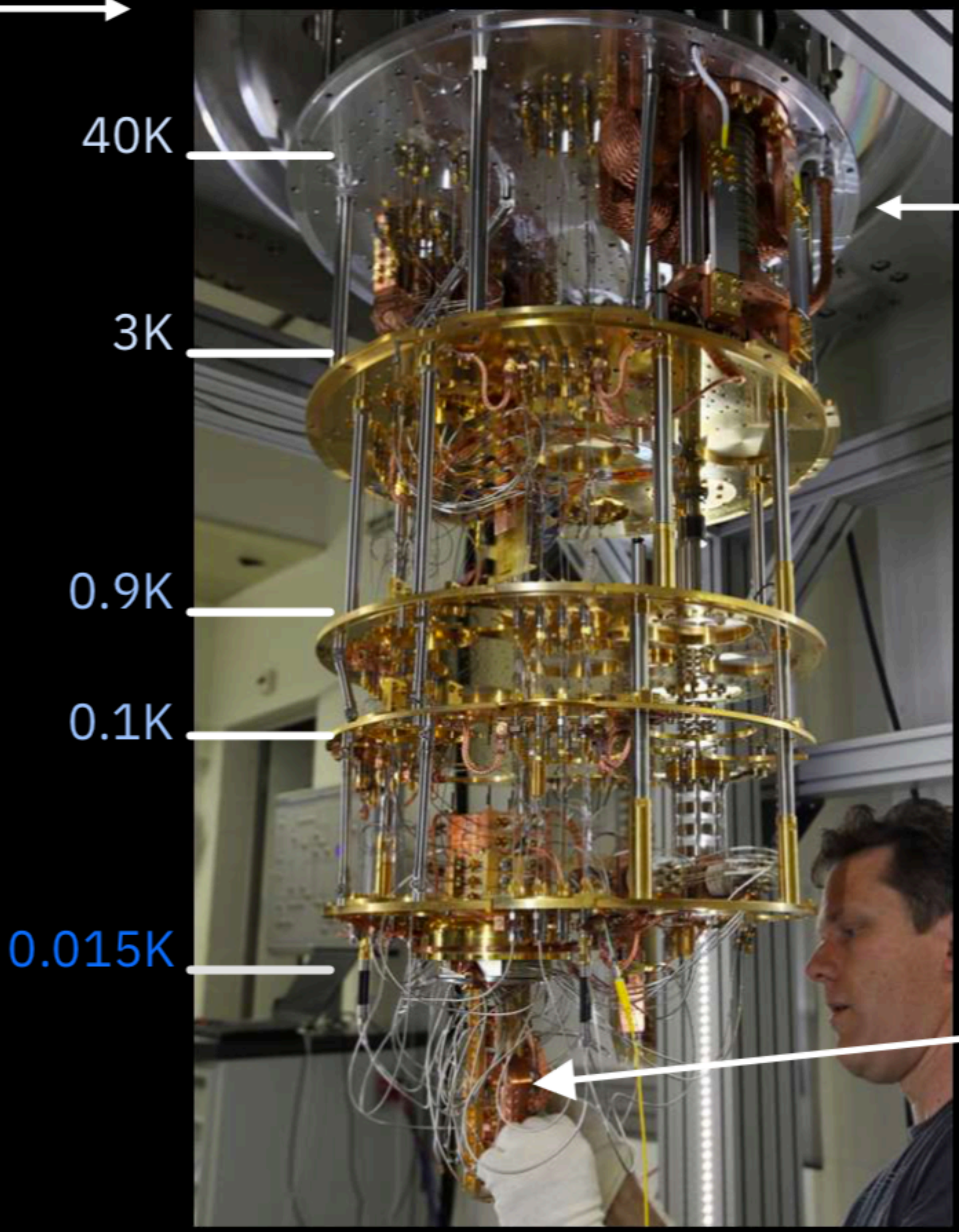


Quantum Computer - Quantum Bit (Qubit)


$|0\rangle=\begin{pmatrix}1\\0\end{pmatrix}$
$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix}$
$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$
$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$
$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}$
$|1\rangle=\begin{pmatrix}0\\1\end{pmatrix}$

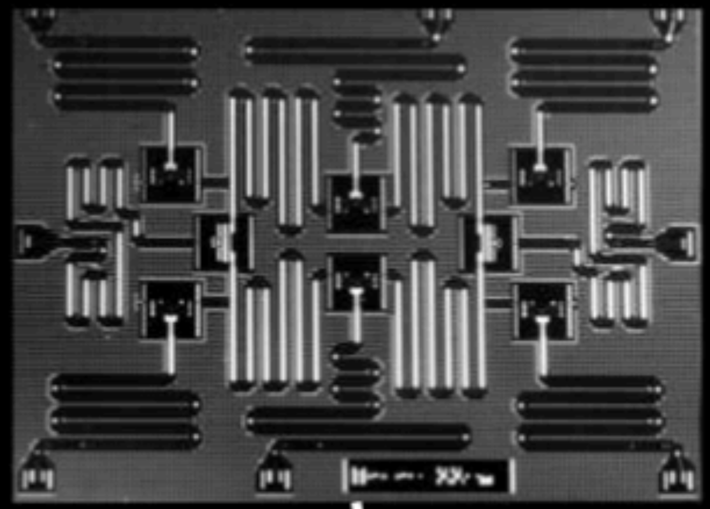
IBM Q quantum computing systems

Microwave electronics

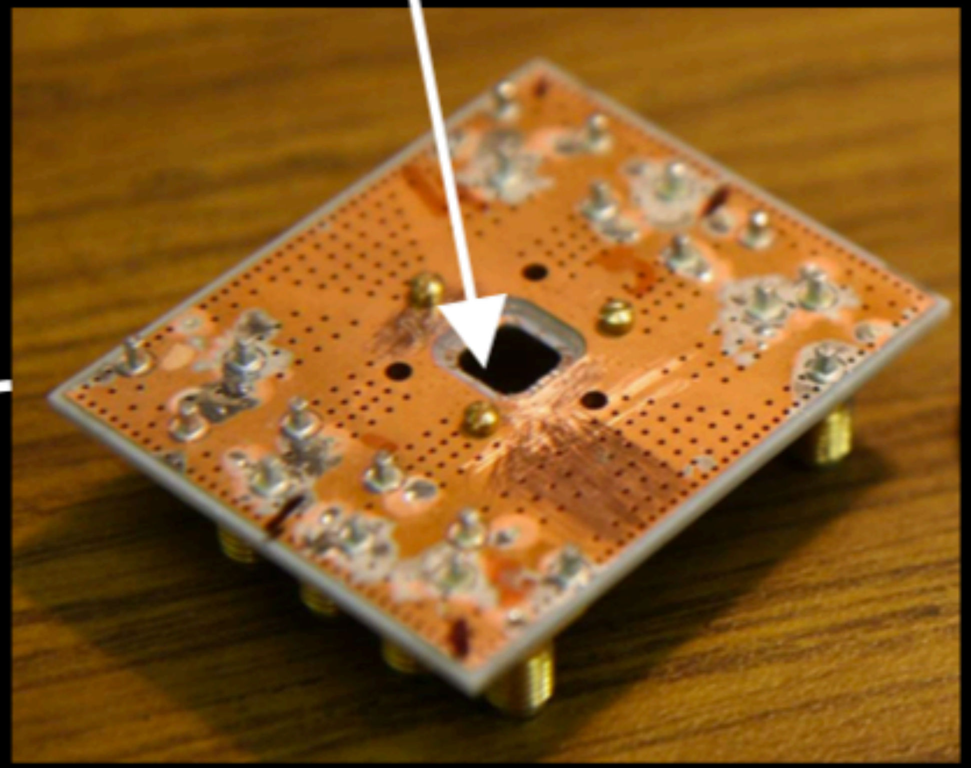


Refrigerator to cool qubits to 10 - 15 mK with a mixture of ^{3}He and ^{4}He

8-qubit PCB



Chip with superconducting qubits and resonators



PCB with the qubit chip at 15 mK
Protected from the environment by multiple shields

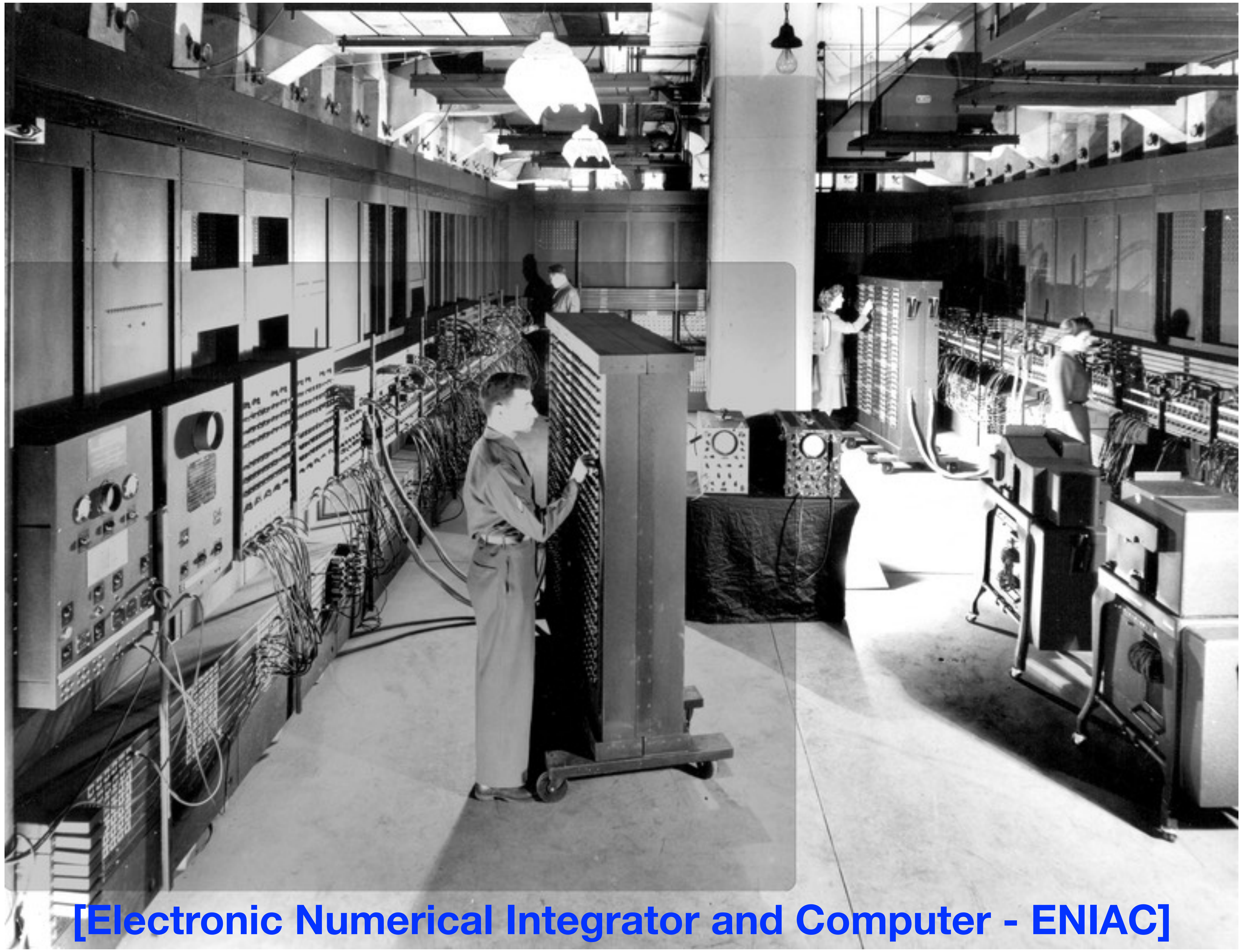
based on [Sutor, 2018]

Main Challenges for Quantum Computers Today

- We have a Noisy **Intermediate-Scale Quantum** (NISQ) technology

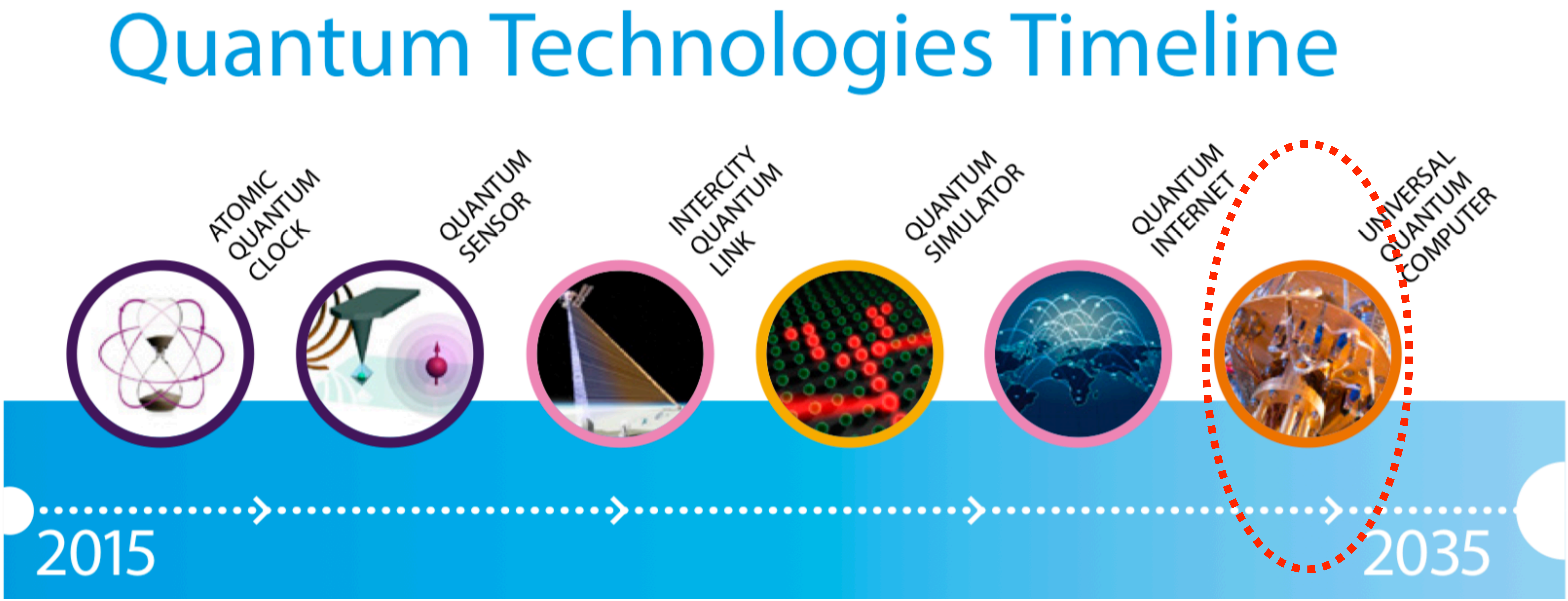
  - coherence time

  - scalability

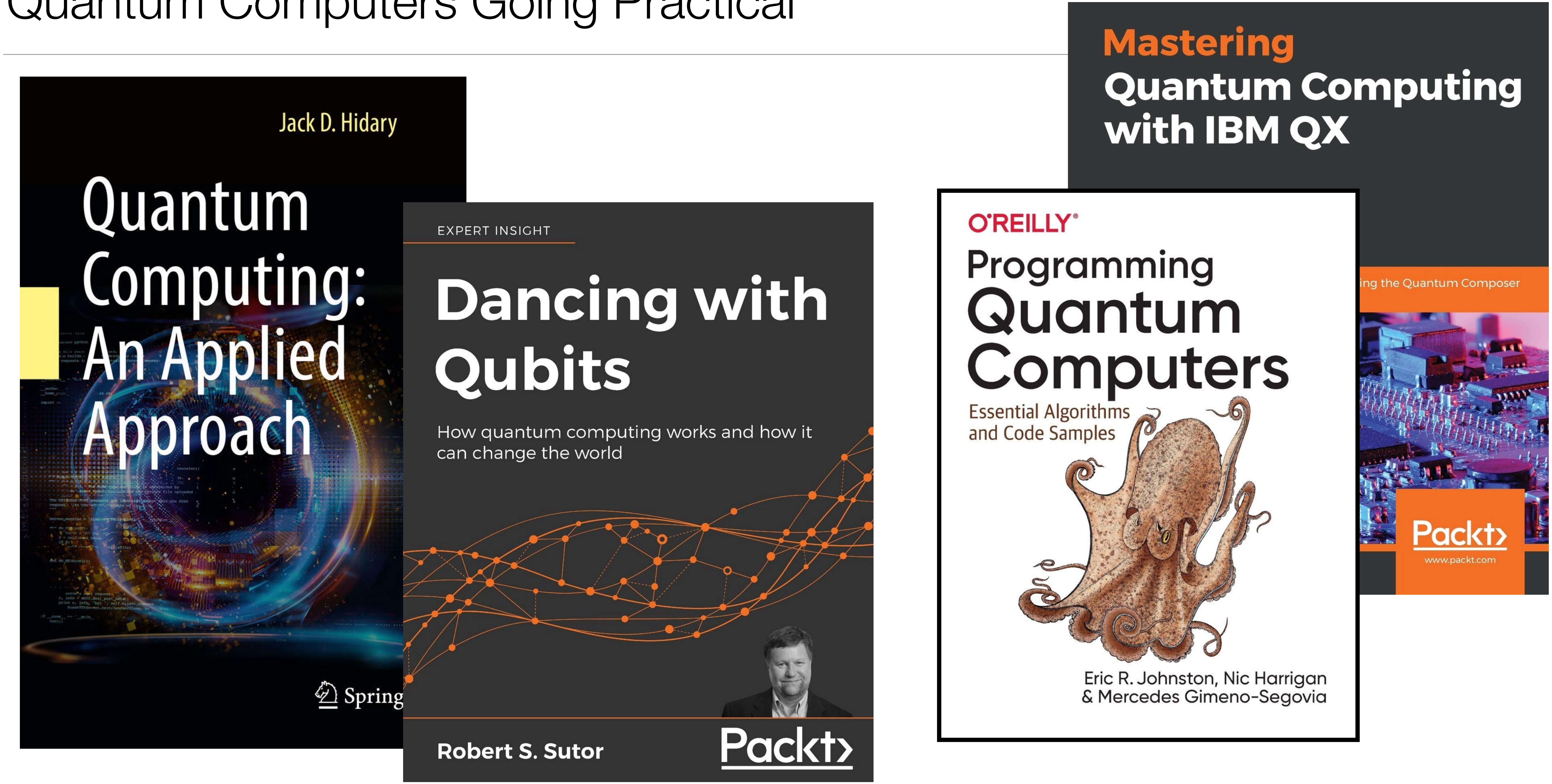


[Electronic Numerical Integrator and Computer - ENIAC]

EU Commission Roadmap (Quantum Manifesto)



Quantum Computers Going Practical



Jack D. Hidary

Quantum Computing: An Applied Approach

Spring

EXPERT INSIGHT

Dancing with Qubits

How quantum computing works and how it can change the world

Robert S. Sutor

Packt

O'REILLY®

Programming Quantum Computers

Essential Algorithms and Code Samples

Eric R. Johnston, Nic Harrigan & Mercedes Gimeno-Segovia

Mastering Quantum Computing with IBM QX

ing the Quantum Composer

Packt

www.packt.com

Another Viewpoint

> **“I estimate a 1/7 chance of breaking RSA-2048 by 2026 and a 1/2 chance by 2031.”**

— Michele Mosca, November 2015

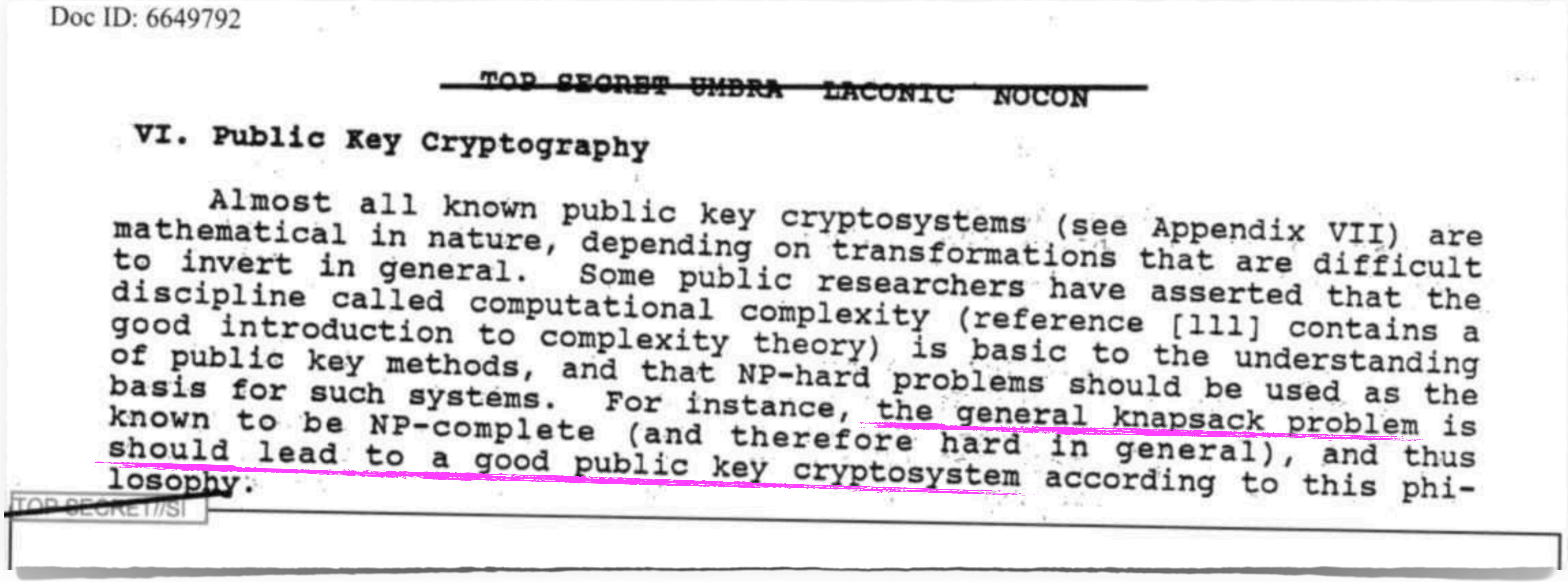
Post-Quantum Cryptography - Or Making It Quantum Resistant

—legend has it, this was the Schrödinger’s cat planning its revenge

Retroactive Cryptanalysis

- Despite powerful quantum computers are not here, yet, we shall **react today to be safe when they come**
- For encryption: start using **post-quantum cryptography**
- For signatures: start using **LTV process**
- For biometrics: **stop blindly assuming** inherent non-invertibility of clients' templates

Searching For the Right Problems
(can be tricky… 😉)



Doc ID: 6649792

~~TOP SECRET UMBRA LACONIC NOCON~~

VI. Public Key Cryptography

Almost all known public key cryptosystems (see Appendix VII) are mathematical in nature, depending on transformations that are difficult to invert in general. Some public researchers have asserted that the discipline called computational complexity (reference [111] contains a good introduction to complexity theory) is basic to the understanding of public key methods, and that NP-hard problems should be used as the basis for such systems. For instance, the general knapsack problem is known to be NP-complete (and therefore hard in general), and thus should lead to a good public key cryptosystem according to this philosophy.

~~TOP SECRET//SI~~

— Fifty Years of Mathematical Cryptanalysis (Fort Meade), Md. NSA, 1988

Diffie-Hellman and Its Generalization

$$(\alpha, g) \mapsto (g^{\alpha} \bmod p)$$

- This is the well-known cornerstone equation of the Diffie-Hellman protocol.
- In its direct interpretation, this is just **an exponentiation of integers modulo *p***, right?
- In general, we can recast this as **an action of the invertible integers modulo *p*-1 on the set of integers modulo *p*, as well**. Still fine?

Group Action in General

$$G \times S \to S$$

$$(\alpha, s) \mapsto \alpha * s$$

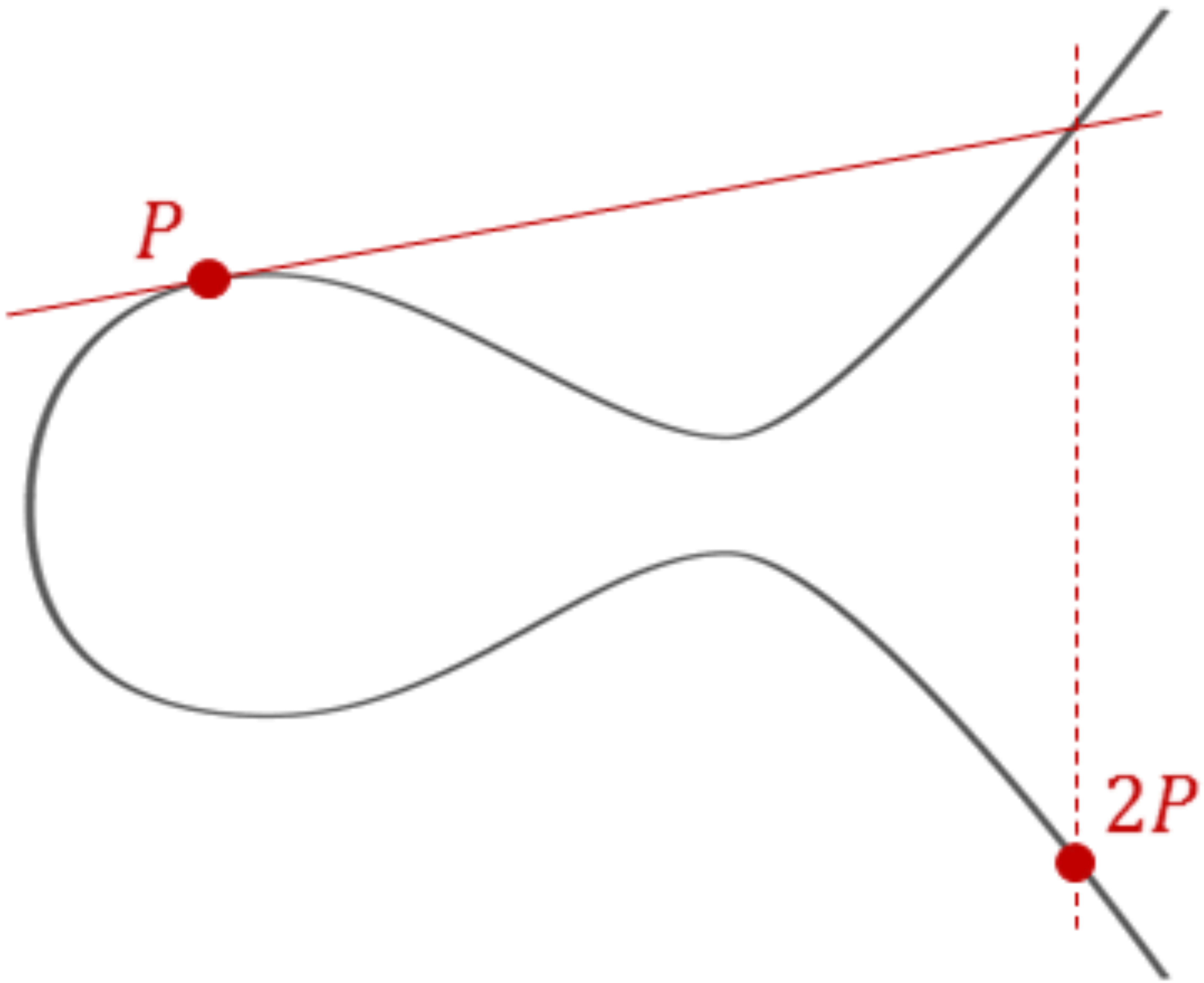
$$e * s = s,\ (\alpha \cdot \beta) * s = \alpha * (\beta * s)$$

- Vectorization problem: Given s and $\alpha \star s$, find α.
- Parallelization problem: Given s, $\alpha \star s$, and $\beta \star s$, find $\alpha\beta \star s$.
- We want a **hard homogeneous space *S***.

In Search for the Action

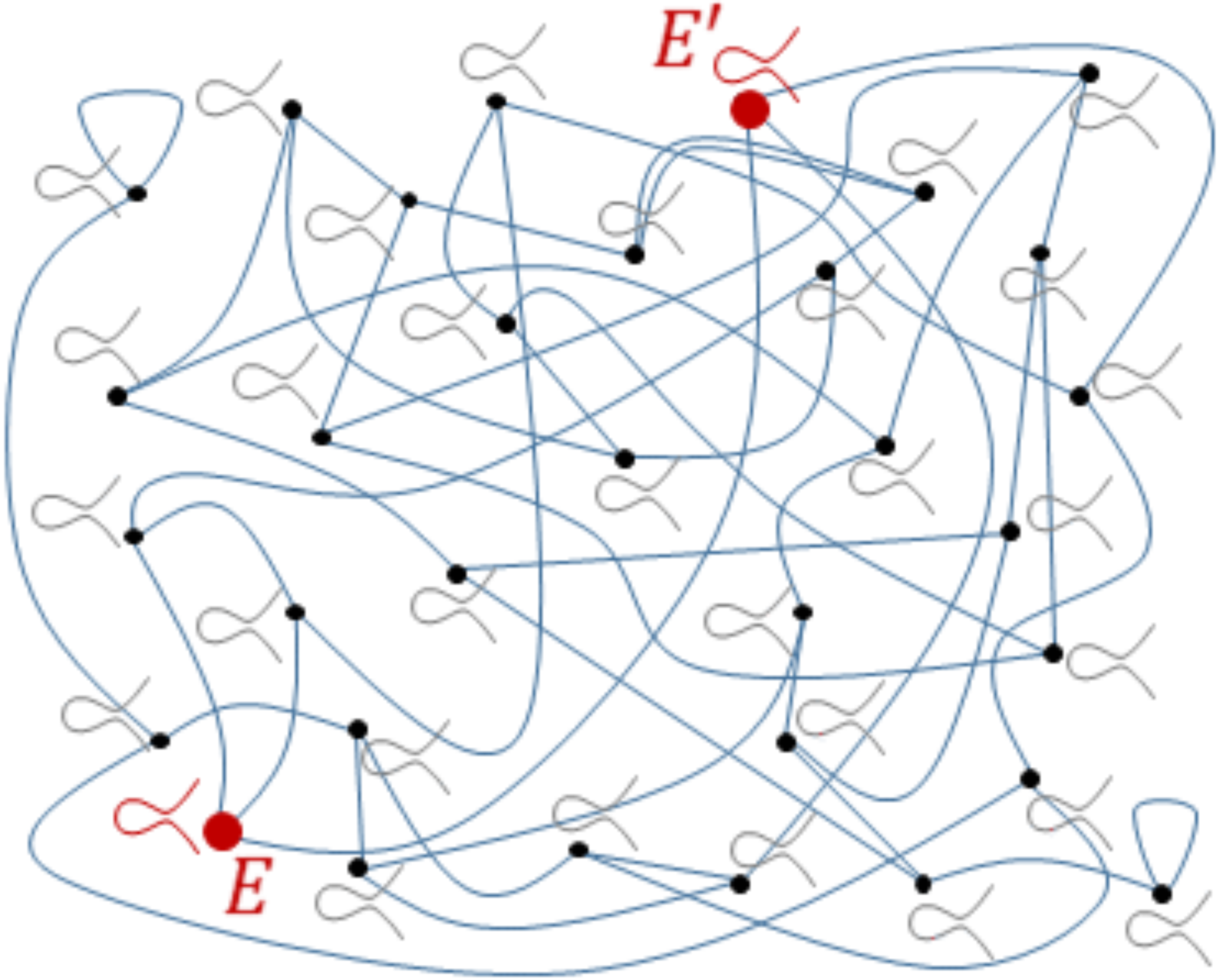
- Classical Diffie-Hellman: $\boldsymbol{Z}_{p\text{-}1}^{*}$ acting on $\boldsymbol{Z}_{p}^{*}$
- Elliptic curve DH (ECDH): $\boldsymbol{Z}_{n}^{*}$ acting on a subgroup of $E(\boldsymbol{F}_{q})$ of order n
- Isogeny DH by Couveignes and Rostovtsev and Stolbunov: class group $Cl(\mathcal{O})$ acting on a certain set of ordinary elliptic curves over $\boldsymbol{F}_{q}$
- SIDH / SIKE: a very special algebraic action (not even an Abelian group action) on a certain set of supersingular elliptic curves over $\boldsymbol{F}_{p\wedge 2}$
- CSIDH: a blend of the last two schemes, reintroducing the class group action for a supersingular setup

Classical ECDH Group Action



— Castryck, W.: Elliptic Curves are Quantum Dead, Long Live Elliptic Curves

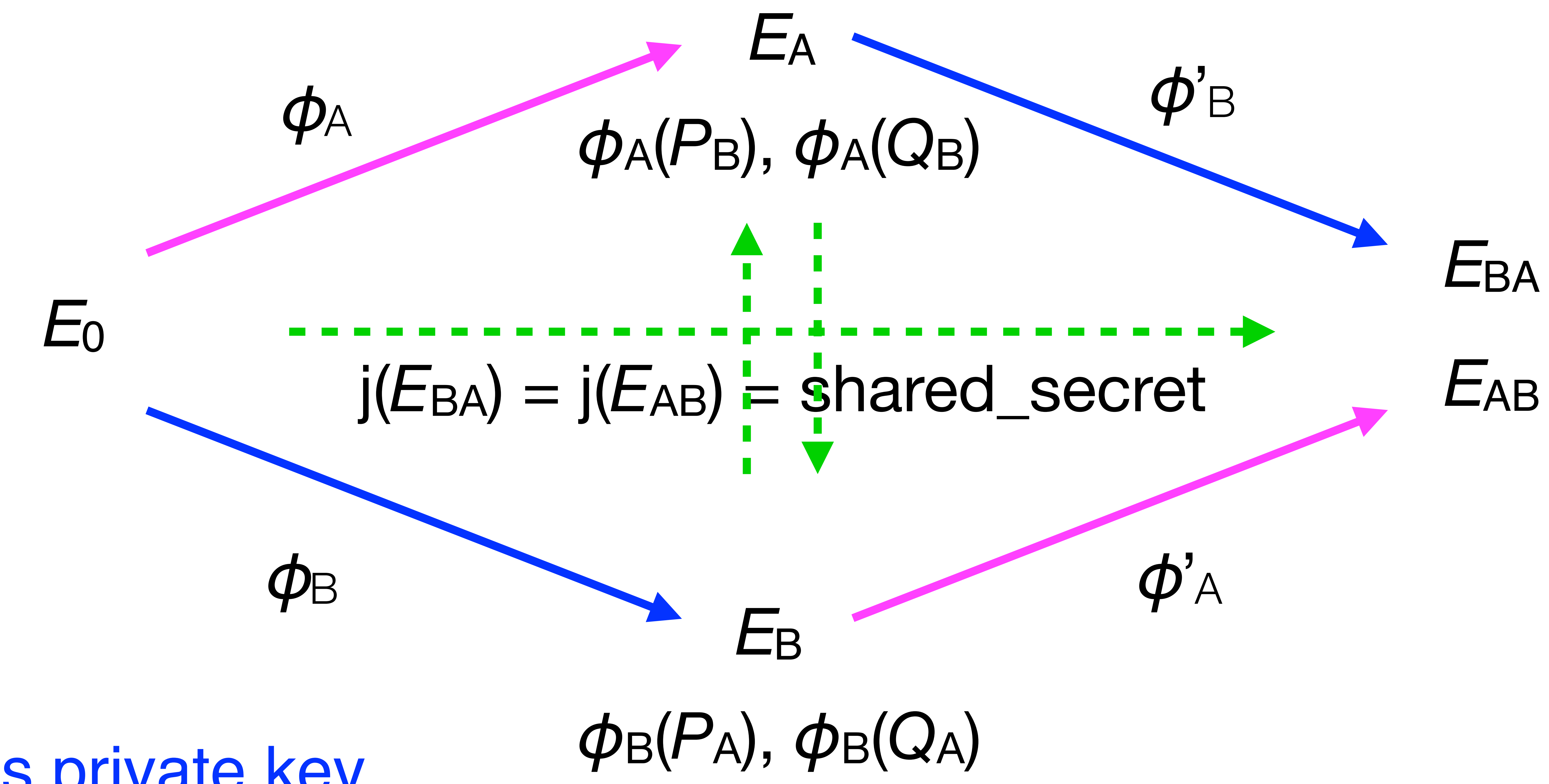
Isogeny Graphs



— Castryck, W.: Elliptic Curves are Quantum Dead, Long Live Elliptic Curves

Supersingular Isogeny-Based Diffie Hellman Protocol

ker(ϕ_A) ~ Alice’s private key



E_A

ϕ_A

ϕ'_B

$\phi_A(P_B)$, $\phi_A(Q_B)$

E_0

E_{BA}

E_{AB}

j(E_{BA}) = j(E_{AB}) = shared_secret

ϕ_B

ϕ'_A

E_B

$\phi_B(P_A)$, $\phi_B(Q_A)$

ker(ϕ_B) ~ Bob’s private key

Making It Practical

[https://medium.com/wultra-blog/quantum-resistant-cryptography-introducing-sike-for-java-376d201afa6e]

Conclusion

- Quantum computing is real
  - we are facing technological and technical issues, but not principal ones
  - we already went a similar way with all the classical computing machinery
- Retroactive cryptanalysis
  - the question of opening today’s communication is not *if*, but *when*
- Post-quantum readiness can be seen as a significant market differentiator
  - it will become necessity anyway, but the winner takes the applause