Quantum computing and its impact on the field of cryptology

Martin Ekerå [1]

[1] Swedish NCSA, Swedish Armed Forces, SE-107 85 Stockholm, Sweden
Avdelningen för krypto och IT-säkerhet, MUST, Försvarsmakten

2018-10-23

SWEDISH ARMED FORCES

Motivation

Motivation

- We may be on the verge of a revolution that will transform the field of cryptology.

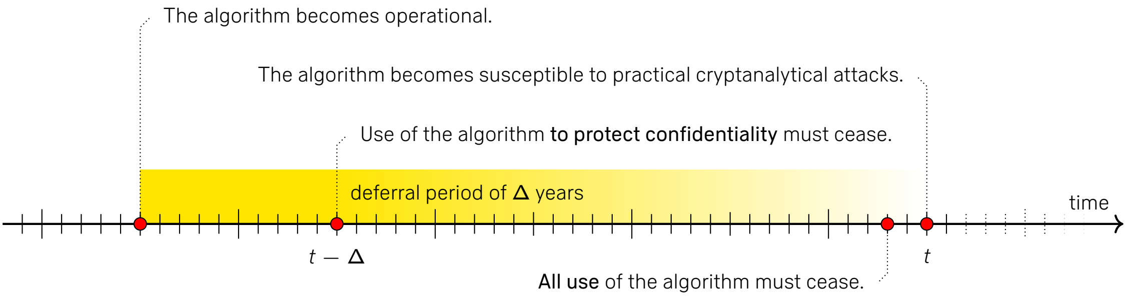
Immediate impact on asymmetric cryptology

- The two problems that underpin virtually all commercial asymmetric cryptography will become tractable if sufficiently capable quantum computers are built.

- It is conceivable that such computers may be built within the next 10-25 years.[a]

[a] It is very difficult to make predictions at this point in time. Opinions diverge in academia. As a cryptographer one must err on the side of caution and assume the above worst case scenario.

When do algorithms need to be replaced?



Deferral periods and confidentiality

- An algorithm that is used to provide confidentiality must resist cryptanalysis for as long as the data that it has been used to protect is to remain confidential.

Contents

1. Motivation

2. Quantum computing
   - The qubit
   - Quantum systems
   - Quantum circuits and operators
   - Are there quantum computers?

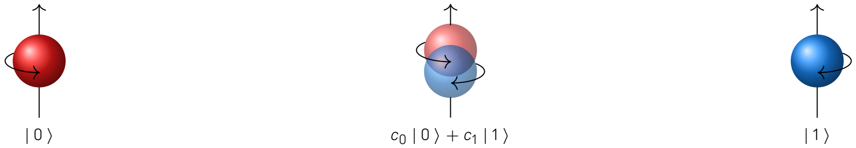
3. Impact of quantum computing
   - Shor’s algorithms
   - Ongoing standardization efforts
   - Summary and conclusion

The bit

The bit

- The smallest information-carrying classical unit is the *bit*.
- A bit may assume two discrete states denoted zero and one.

The qubit



The qubit

- The smallest information-carrying quantum unit is the *qubit*.

- A qubit is a normalized superposition of two basis states. More specifically

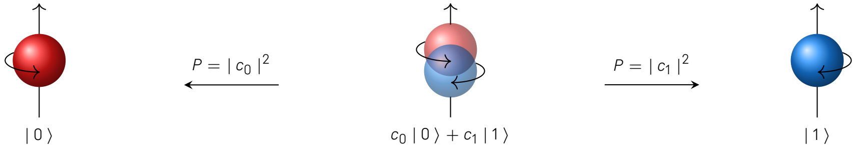
$$|\,\Psi\,\rangle = c_0\,|\,0\,\rangle + c_1\,|\,1\,\rangle \quad \text{where} \quad c_0,\, c_1 \in \mathbb{C} \quad \text{and} \quad |\,c_0\,|^2 + |\,c_1\,|^2 = 1.$$

Reading a bit

Reading a bit

- A bit may be read without side effects to yield zero or one.

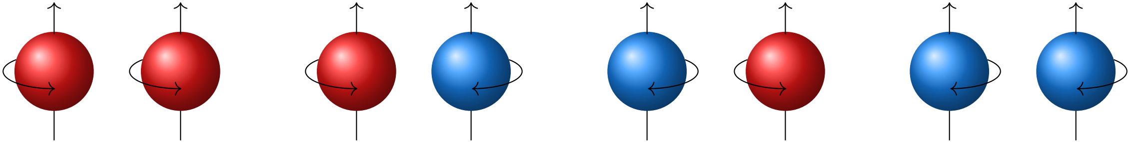
Observing a qubit



Observing a qubit

- Observing a qubit collapses the superposition to one of the basis states, yielding a single bit of classical information. The probability of collapsing to $|j\rangle$ is $|c_j|^2$.

Quantum systems

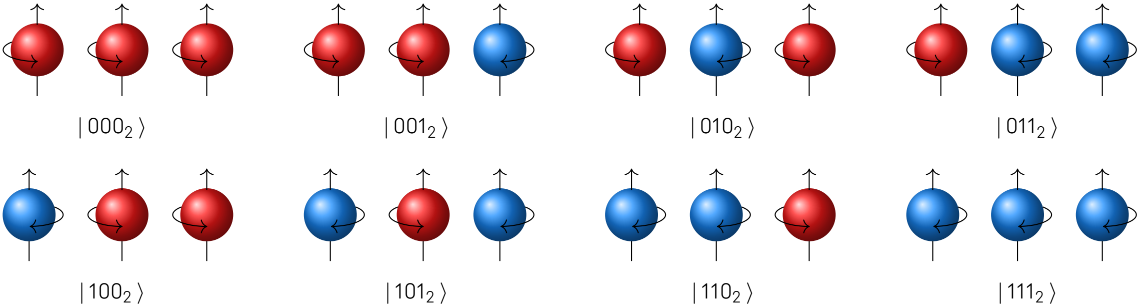


$|0 = 00_2\rangle$ $|1 = 01_2\rangle$ $|2 = 10_2\rangle$ $|3 = 11_2\rangle$

A system of two qubits

- A system of 2 qubits is in a superposition of $2^2 = 4$ basis states.

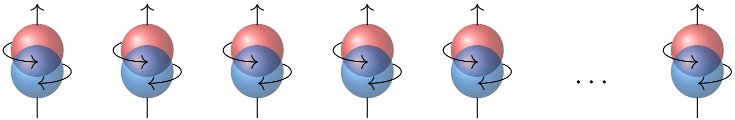
Quantum systems



A system of three qubits

- A system of 3 qubits is in a superposition of $2^3 = 8$ basis states.

Quantum systems



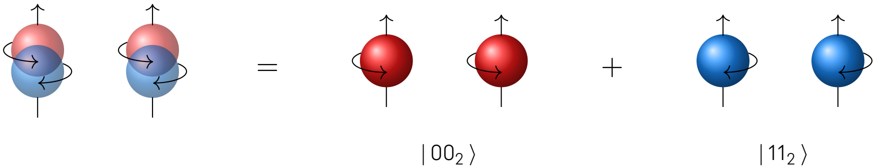
A system of m qubits

- A system of m qubits is in a superposition of 2^m basis states.

$$|\Psi\rangle = \sum_{j=0}^{2^m-1} c_j |j\rangle \qquad c_j \in \mathbb{C} \qquad \sum_{j=0}^{2^m-1} |c_j|^2 = 1$$

- When observed the probability of collapsing to $|j\rangle$ is $|c_j|^2$.

Quantum entanglement



$$|\,\Psi\,\rangle = \frac{1}{\sqrt{2}}\,|\,00_2\,\rangle + \frac{1}{\sqrt{2}}\,|\,11_2\,\rangle$$

Quantum entanglement

- Quantum systems that cannot be independently described are said to be *entangled*.

- The ability of quantum systems to be entangled gives rise to quantum speedups.

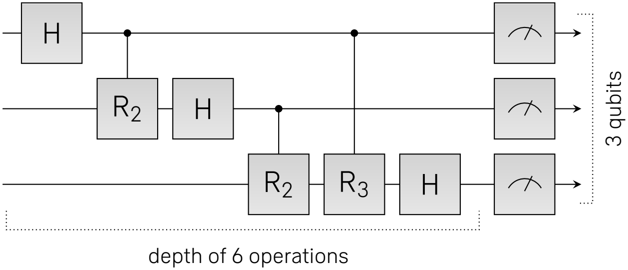
Quantum operators

Operating on qubits

- The quantum system is evolved by applying operators to qubits.

- Only unitary operators are admissible. There are universal sets of unitary operators using which any other unitary operator may be expressed up to precision.

Quantum algorithms and circuits

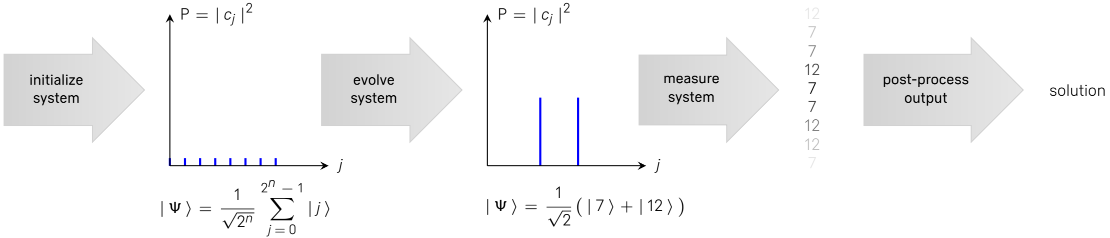


Quantum algorithms and circuits

- Quantum algorithms are compiled to quantum circuits. A circuit consists of a concrete sequence of operations and measurements.

- The circuit depth, and number and type of operations, determine the complexity.

Quantum computations



Quantum computations

- The goal of a quantum algorithm is to increase the amplitudes of some set of target states that provide information on the solution of a given problem.

- The quantum system must remain coherent from initialization to measurement.

Photo: IBM

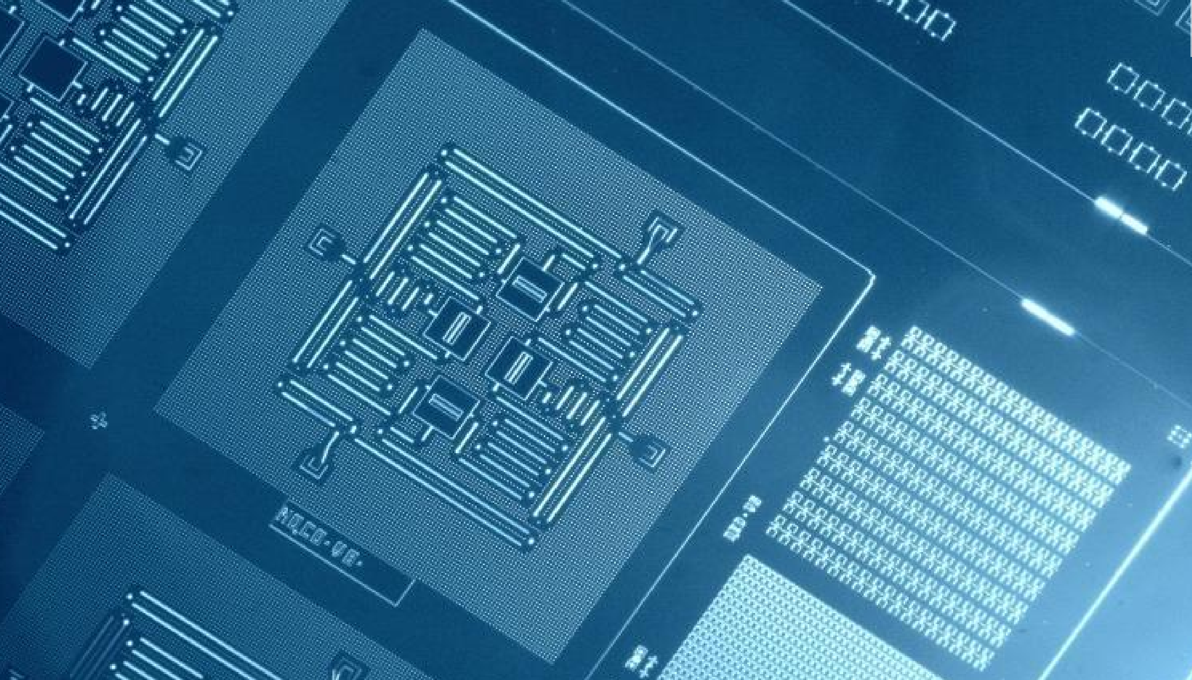
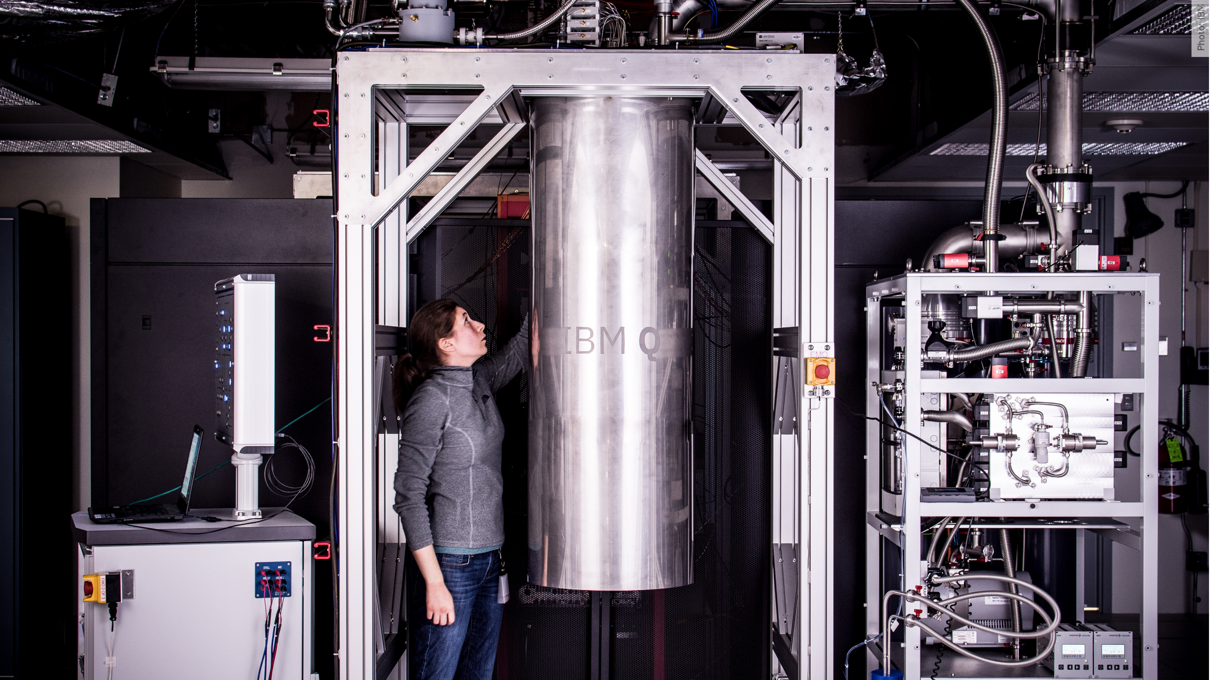


Photo: IBM


IBM Q
Photo: IBM

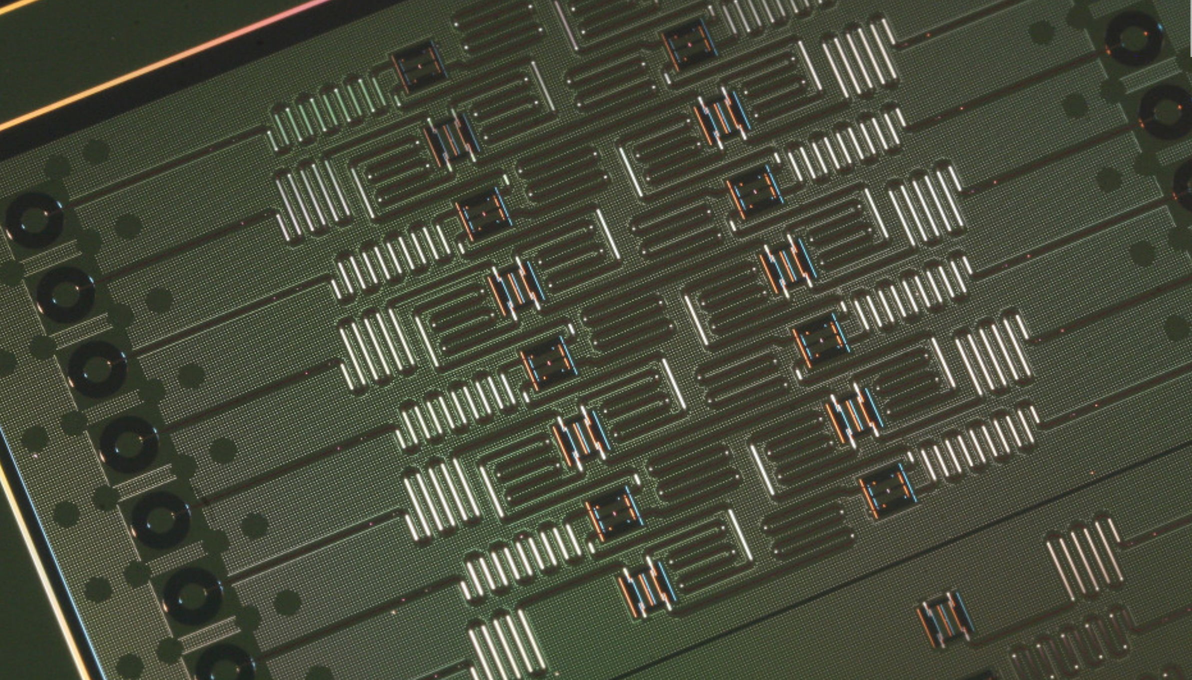


Photo: IBM

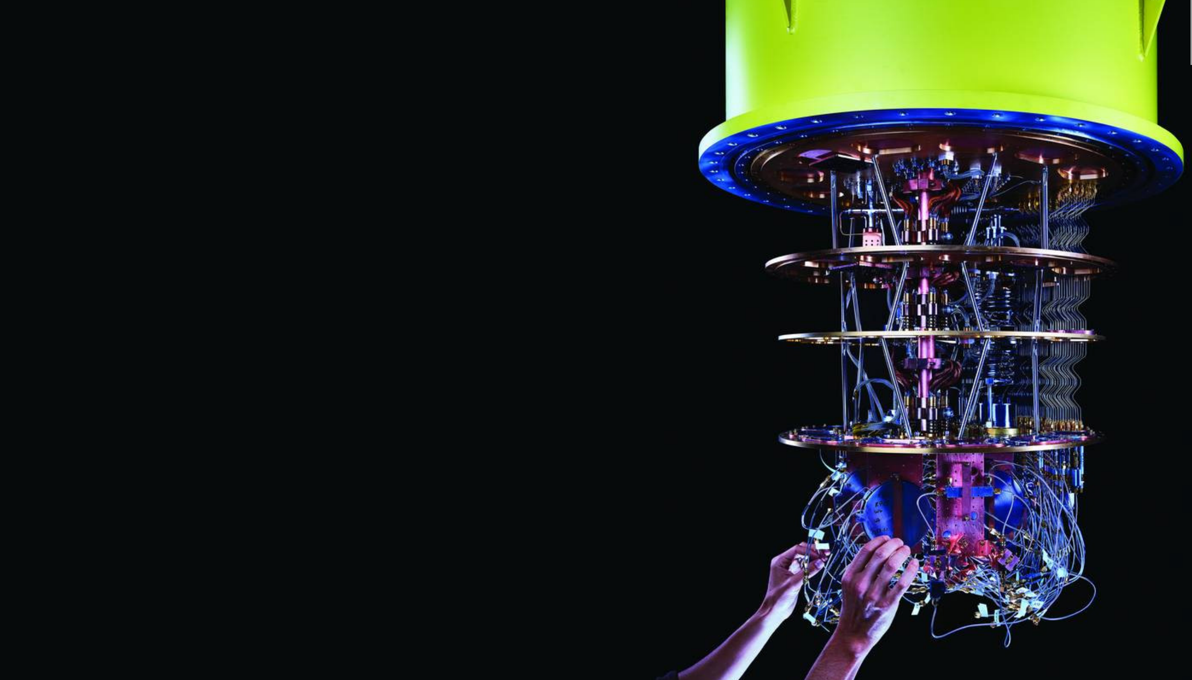


Photo: UCSB

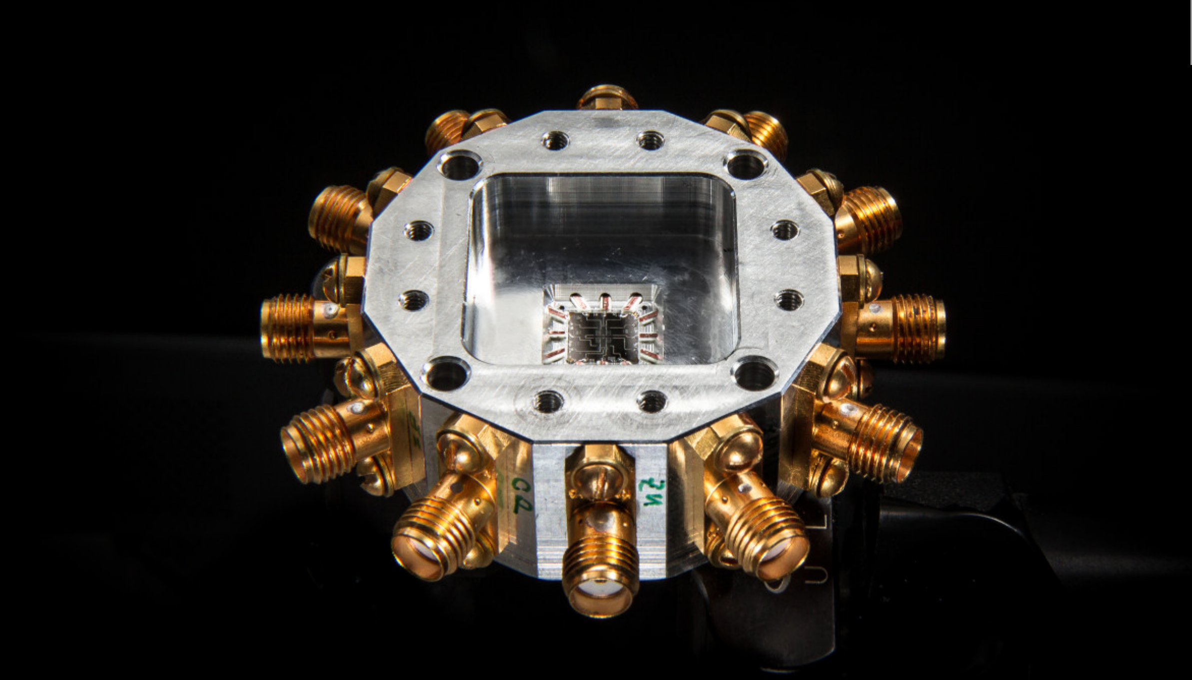
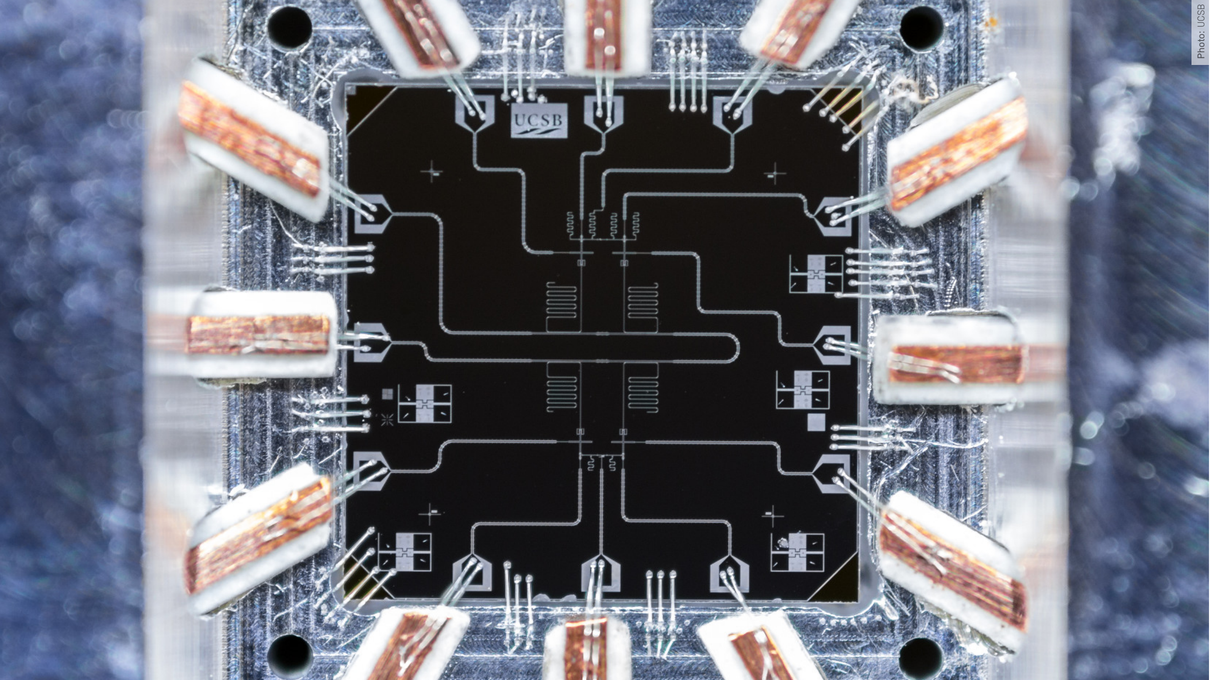


Photo: UCSB


UCSB
Photo: UCSB

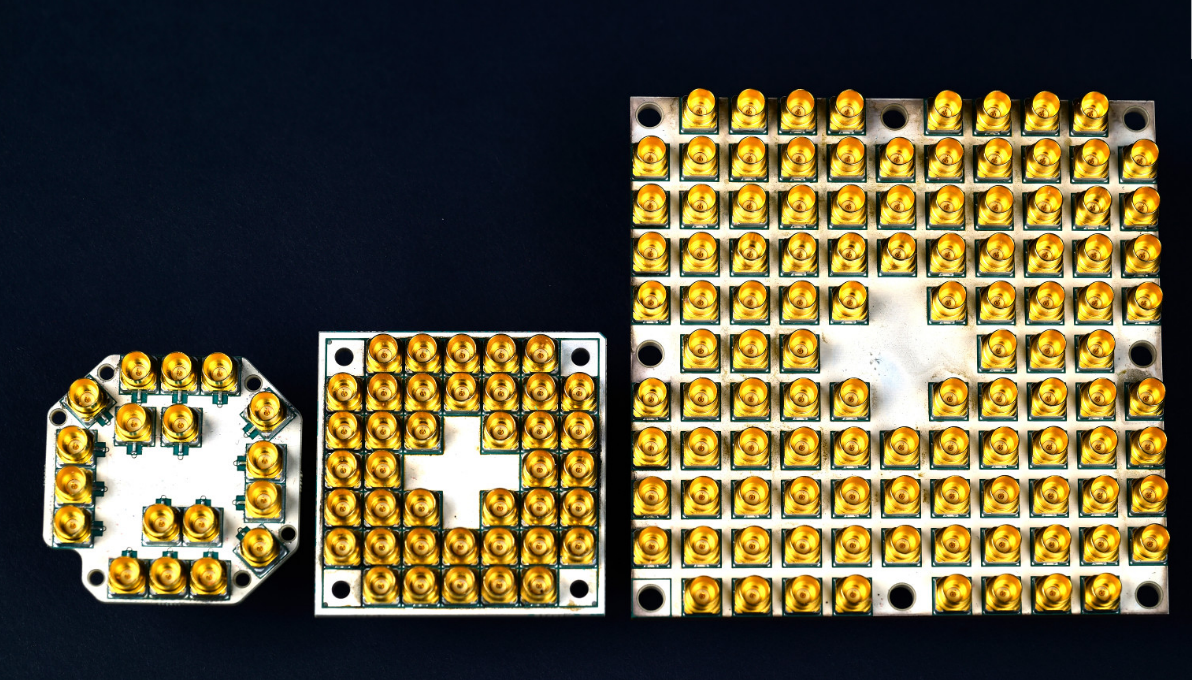


Photo: Intel

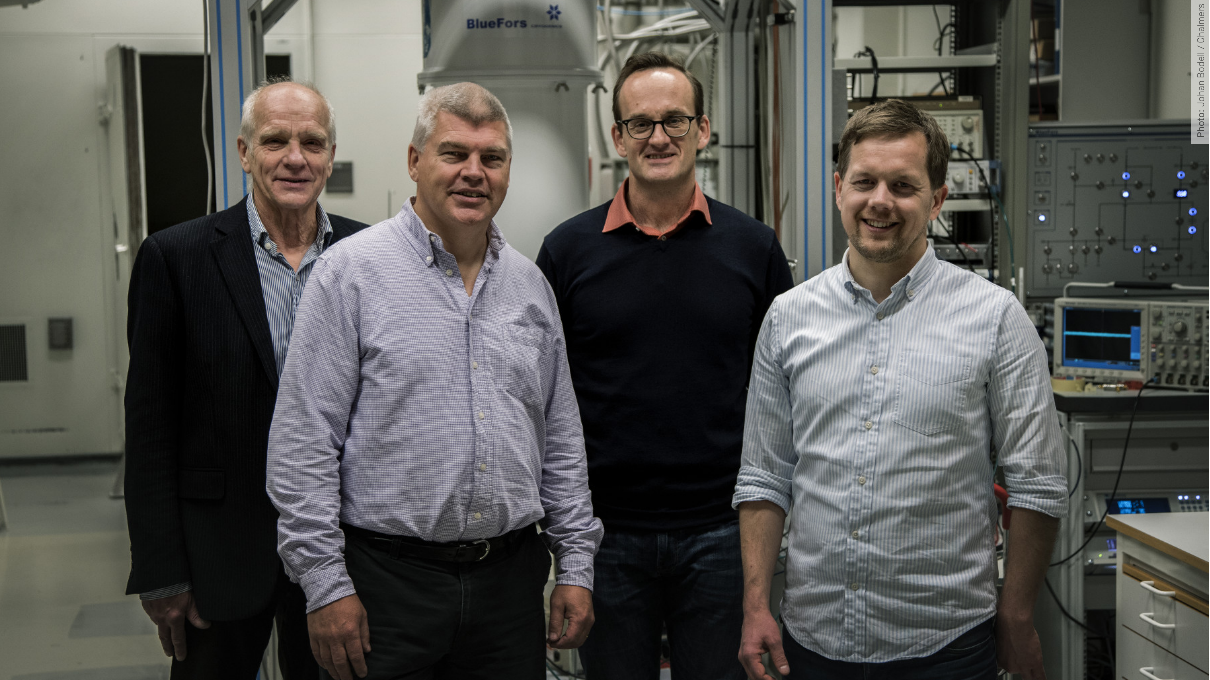


Photo: Johan Bodell / Chalmers

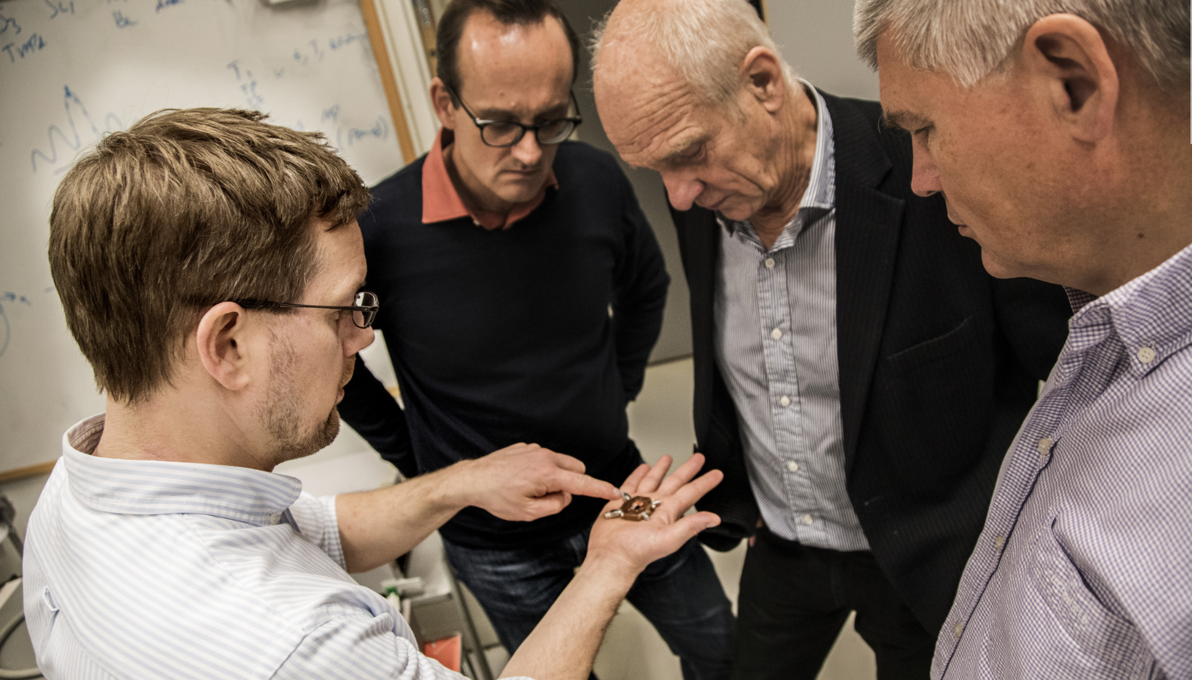


Photo: Johan Bodell / Chalmers

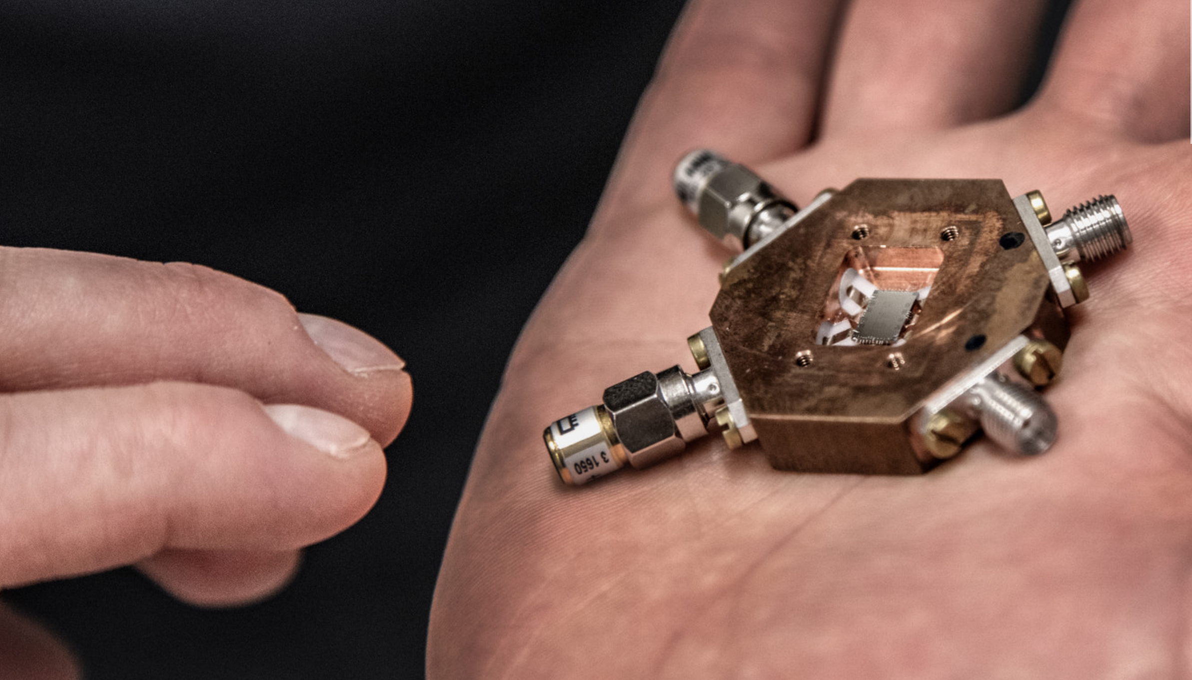


Photo: Johan Bodell / Chalmers

Contents

1. Motivation

2. Quantum computing
   - The qubit
   - Quantum systems
   - Quantum circuits and operators
   - Are there quantum computers?

3. Impact of quantum computing
   - Shor's algorithms
   - Ongoing standardization efforts
   - Summary and conclusion

Impact of quantum computing on cryptology

Quantum algorithms for cryptanalysis

- The current understanding of the implications of quantum computing is limited.

Grover's algorithm [Grover96]

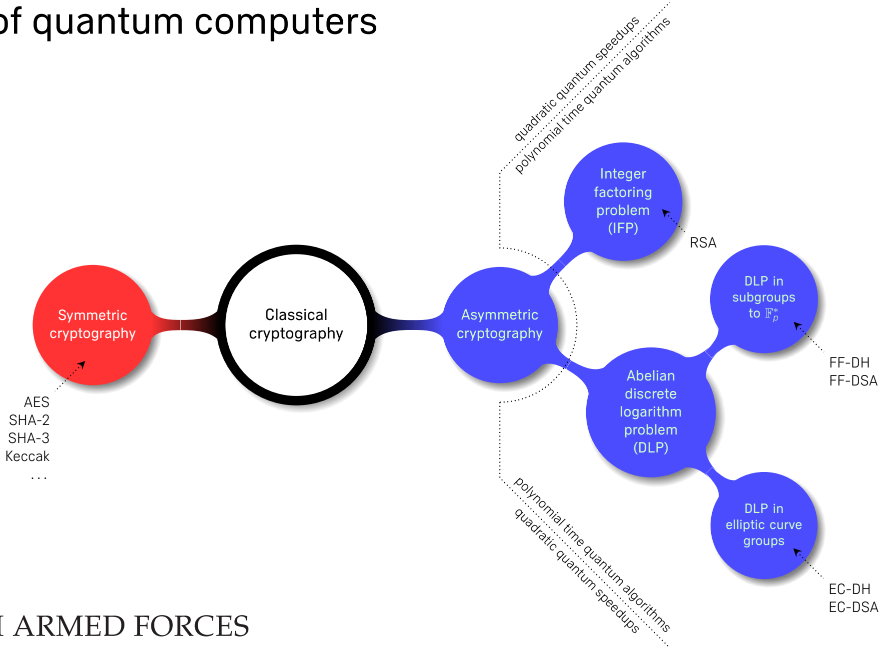
- Grover's algorithm provides a quadratic speedup for exhaustive search.

Shor's algorithms [Shor94]

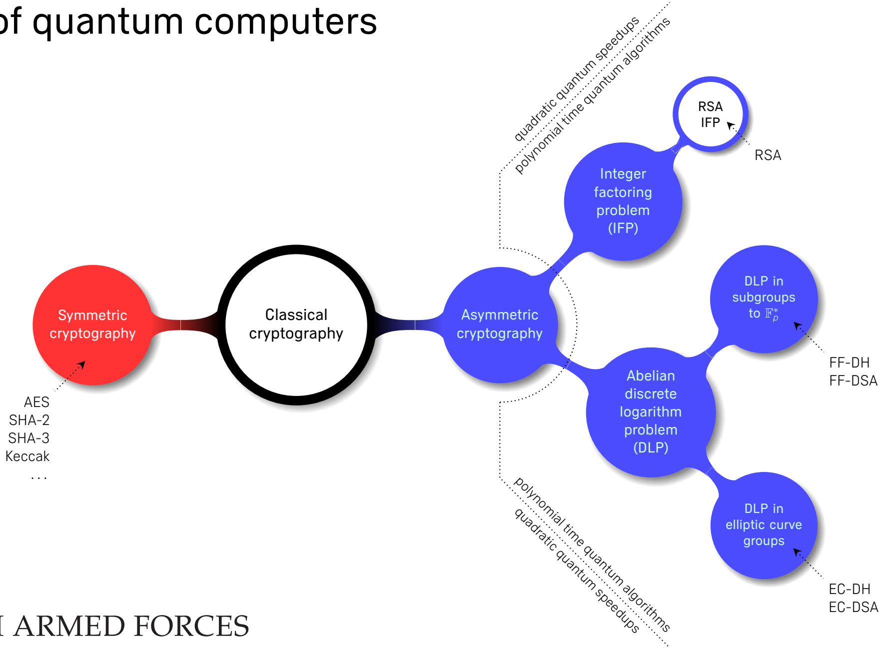
- Shor's algorithms solve the integer factoring and abelian discrete logarithm problems in polynomial time using only a polynomial number of qubits.

- Asymmetric algorithms based upon these problems must be replaced in time.

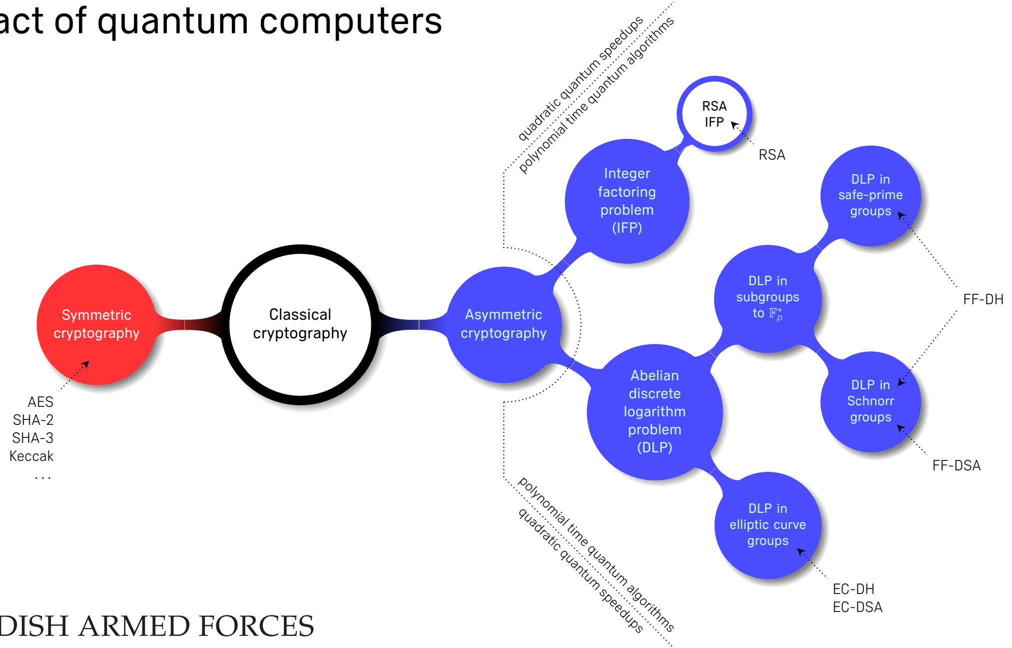
Impact of quantum computers



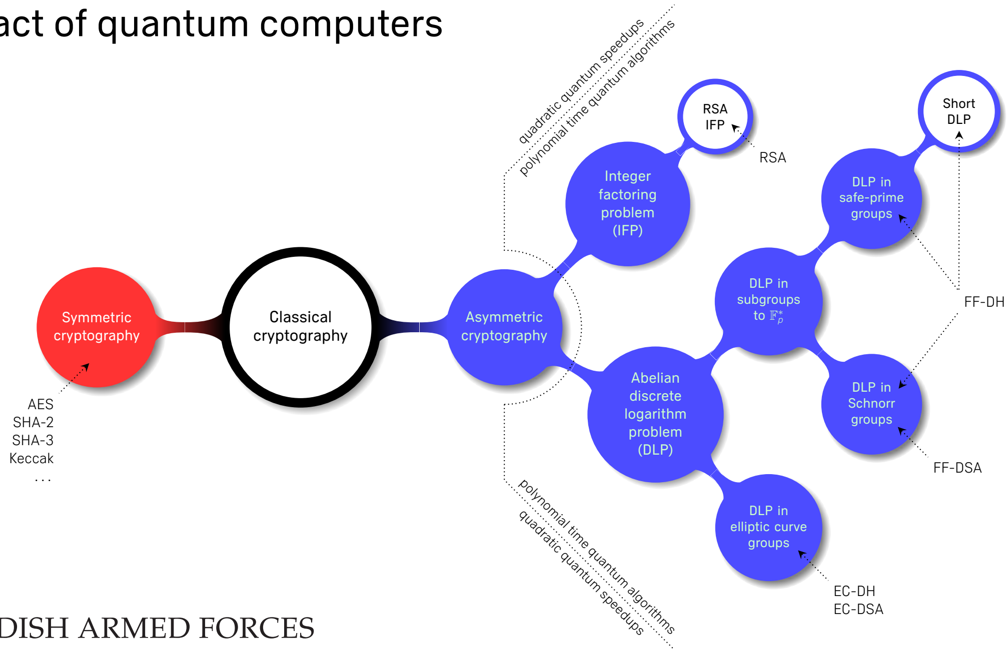
Impact of quantum computers



Impact of quantum computers

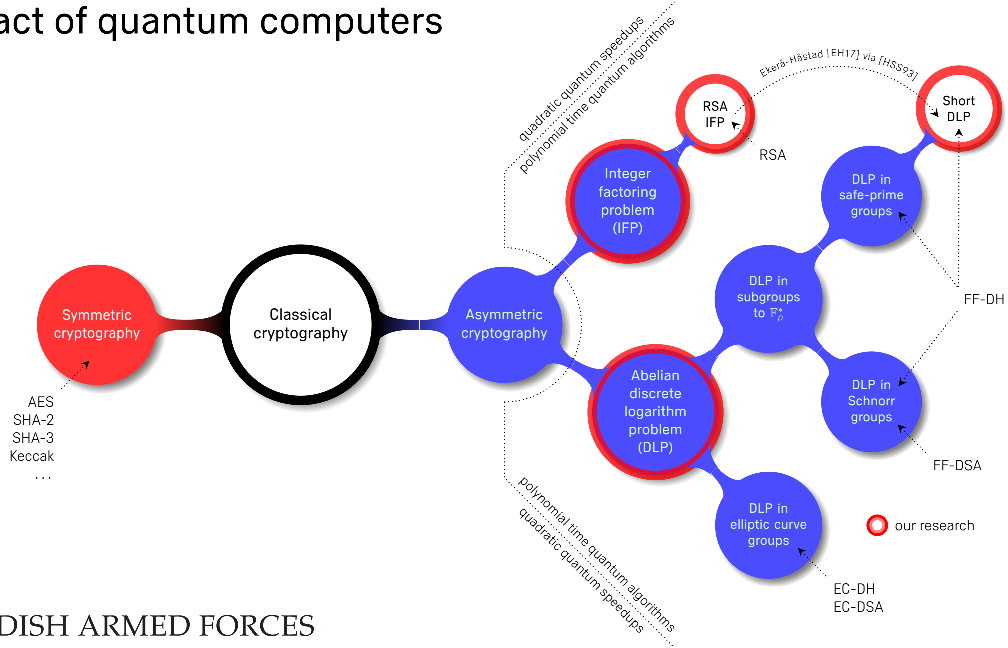


Impact of quantum computers



SWEDISH ARMED FORCES

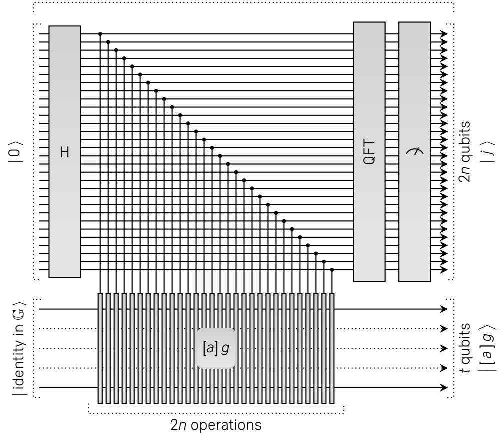
Impact of quantum computers



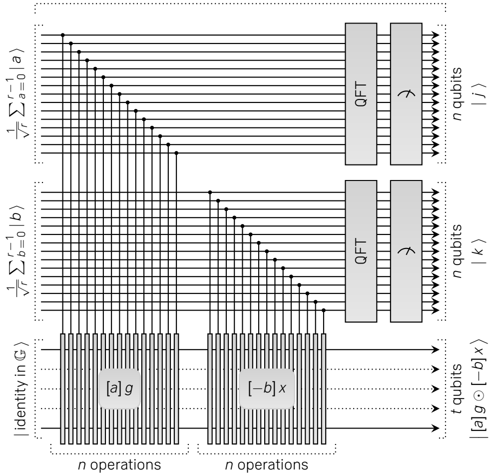
SWEDISH ARMED FORCES

Shor's algorithms

factoring n bit integer N via order finding in $\mathbb{G} = \langle g \rangle \subseteq \mathbb{Z}_N^*$



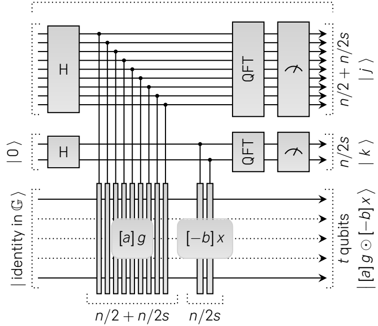
computing d given g and $x = [\,d\,]\, g$ in $\mathbb{G} = \langle g \rangle$ of order $r \sim 2^n$



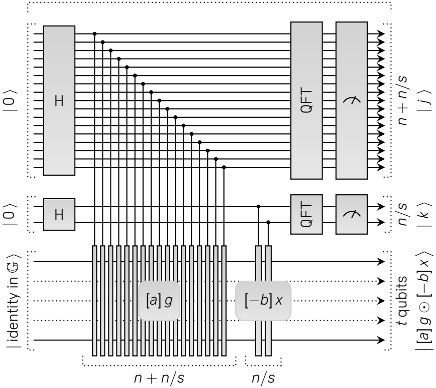
Shor's algorithms

Our specialized algorithms [EH17, Ekerå17, Ekerå18]

factoring n bit RSA integer N via short DLP in $\mathbb{G} = \langle g \rangle \subseteq \mathbb{Z}_N^*$



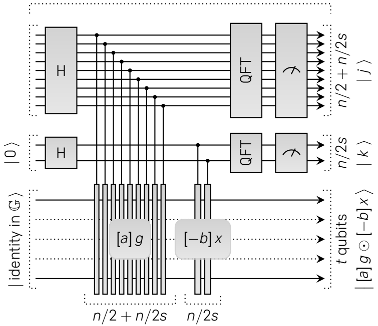
computing d given g and $x = [\, d \,]\, g$ in $\mathbb{G} = \langle g \rangle$ of order $r \sim 2^n$



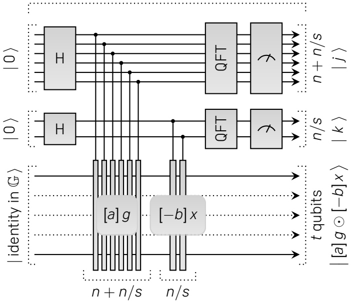
Shor's algorithms

Our specialized algorithms [EH17, Ekerå17, Ekerå18]

factoring n bit RSA integer N via short DLP in $\mathbb{G} = \langle g \rangle \subseteq \mathbb{Z}_N^*$



computing short $d \sim 2^n$ given g and $x = [\, d \,]\, g$ in $\mathbb{G} = \langle g \rangle$ of order r



Shor's algorithm

Solving EC-DLP on $E(\mathbb{F}_p)$

Size $\lceil \log_2 p \rceil$	Classical security in bits	Quantum operations in Toffoli operators	Circuit depth	Logical qubits
192	96	$1.85 \cdot 2^{34}$	$1.70 \cdot 2^{34}$	1754
256	128	$1.04 \cdot 2^{36}$	$1.91 \cdot 2^{35}$	2330
384	192	$1.86 \cdot 2^{37}$	$1.71 \cdot 2^{37}$	3484
521	260	$1.14 \cdot 2^{39}$	$1.05 \cdot 2^{39}$	4719

* Qubit count and operator count as given by Roetteler et al. [RNSL17] for $E(\mathbb{F}_p)$ on short Weierstrass form accounting for (a) qubit recycling by Mosca and Ekert [ME99] and (b) tradeoffs by Ekerå [Ekerå18]. The estimates assume an ideal quantum computer and do not account for the overheads caused by quantum error correction.

Shor's algorithm

Solving RSA IFP

Size $\lceil \log_2 pq \rceil$	Classical security in bits	Quantum operations in Toffoli operators	Logical qubits
1024	80	$1.16 \cdot 2^{37}$	2050
2048	110	$1.26 \cdot 2^{40}$	4098
3072	132	$1.13 \cdot 2^{42}$	6146
4096	150	$1.36 \cdot 2^{43}$	8194
8192	202	$1.48 \cdot 2^{46}$	16386

* Qubit count $2n + 2$ and operator count $2n^3(32.01 \log_2 n - 49.29)$ as extrapolated from Häner et al. [HRS17] accounting for optimization by (a) Mosca and Ekert [ME99] and (b) Ekerå and Håstad [EH17, Ekerå17]. The estimates assume an ideal quantum computer and do not account for error correction. Classical security estimated as in FIPS 140-2 IG.

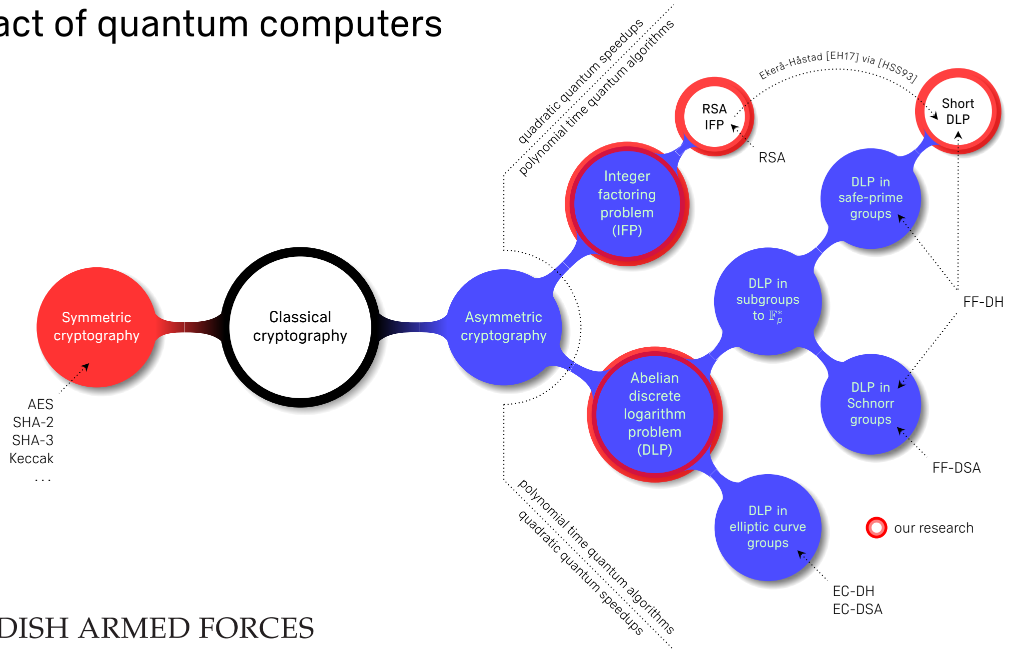
Shor’s algorithm

Solving FF-DLP

Size $n = \lceil \log_2 p \rceil$	Classical security in bits	Quantum operations: General DLP in Toffoli ops.	Quantum operations: Schnorr or short DLP in Toffoli operators	Logical qubits
1024	80	$1.13 \cdot 2^{38}$	$1.59 \cdot 2^{35}$	2050
2048	110	$1.23 \cdot 2^{41}$	$1.23 \cdot 2^{38}$	4098
3072	132	$1.10 \cdot 2^{43}$	$1.65 \cdot 2^{39}$	6146
4096	150	$1.35 \cdot 2^{44}$	$1.74 \cdot 2^{40}$	8194
8192	202	$1.47 \cdot 2^{47}$	$1.28 \cdot 2^{43}$	16386

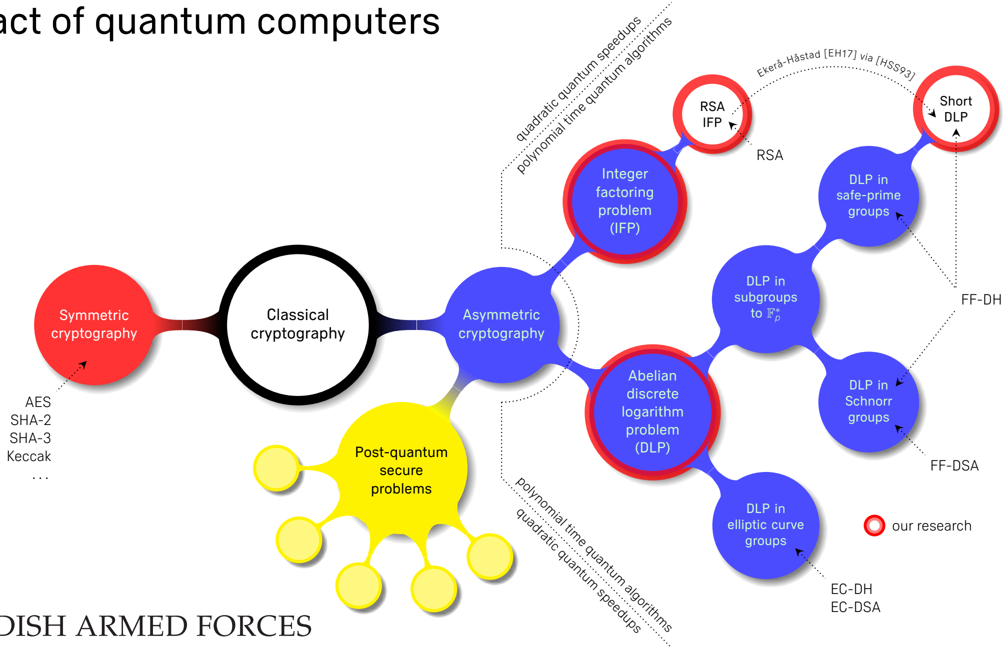
* Qubit count $2n + 2$ and operator count $2n^3(32.01 \log_2 n - 49.29)$ as extrapolated from Häner et al. [HRS17] accounting for optimizations by (a) Mosca and Ekert [ME99] and (b) Ekerå and Håstad [EH17, Ekerå17, Ekerå18]. The estimates assume an ideal quantum computer and do not account for error correction. Classical security estimated as in FIPS 140-2 IG.

Impact of quantum computers

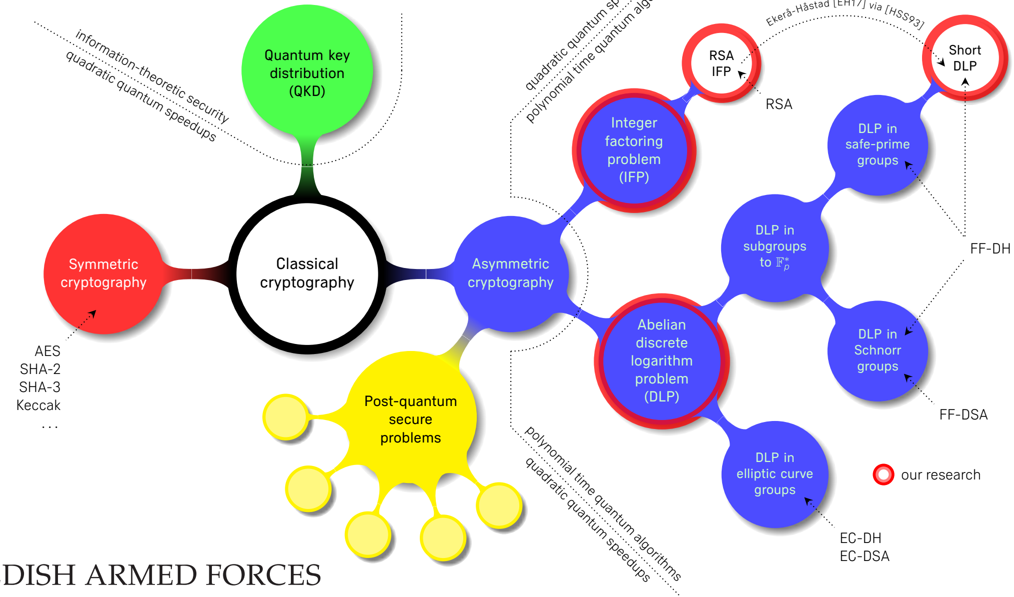


SWEDISH ARMED FORCES

Impact of quantum computers

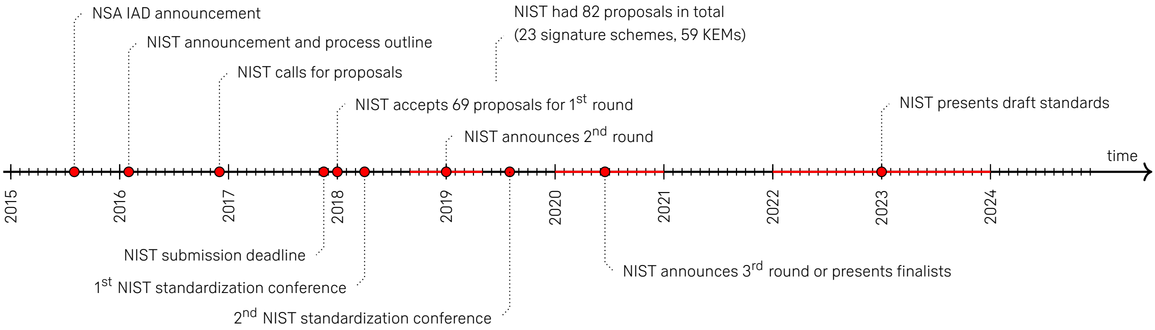


Impact of quantum computers



SWEDISH ARMED FORCES

Ongoing standardization efforts



Standardization efforts

- Standardization efforts are ongoing. It take time to develop and adopt standards.

Summary and conclusion

Summary and conclusion

- The two problems that underpin virtually all commercial asymmetric cryptography will become tractable if sufficiently capable quantum computers are built.

- It is conceivable that such computers may be built within the next 10-25 years.

Mitigating actions for asymmetric cryptology

- Prioritize taking mitigating actions for algorithms used to provide confidentiality.
- Migrate to a hybrid solution with a proven classically secure algorithm and a post-quantum secure algorithm. Adopt symmetric keying whenever feasible.

- Use approved COMSEC systems or seek expert advise from the Swedish NCSA.

Summary and conclusion

Swedish COMSEC and Swedish cyber defence

- Swedish COMSEC systems consitute an integral part of the Swedish cyber defence.

- COMSEC systems approved by the Swedish Armed Forces must be used to protect the confidentiality of information classified with respect to national security.