Software system security in the era of quantum computing

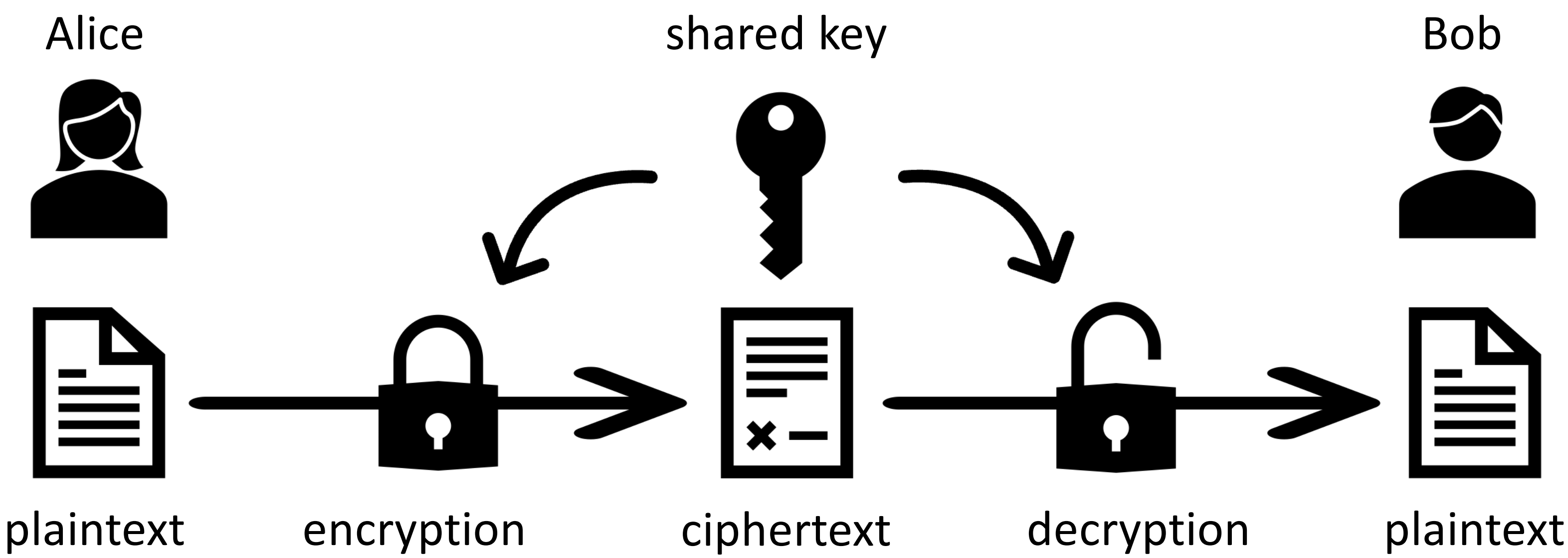
IS 471 Spring 2023

Lei Zhang

Classical Crypto

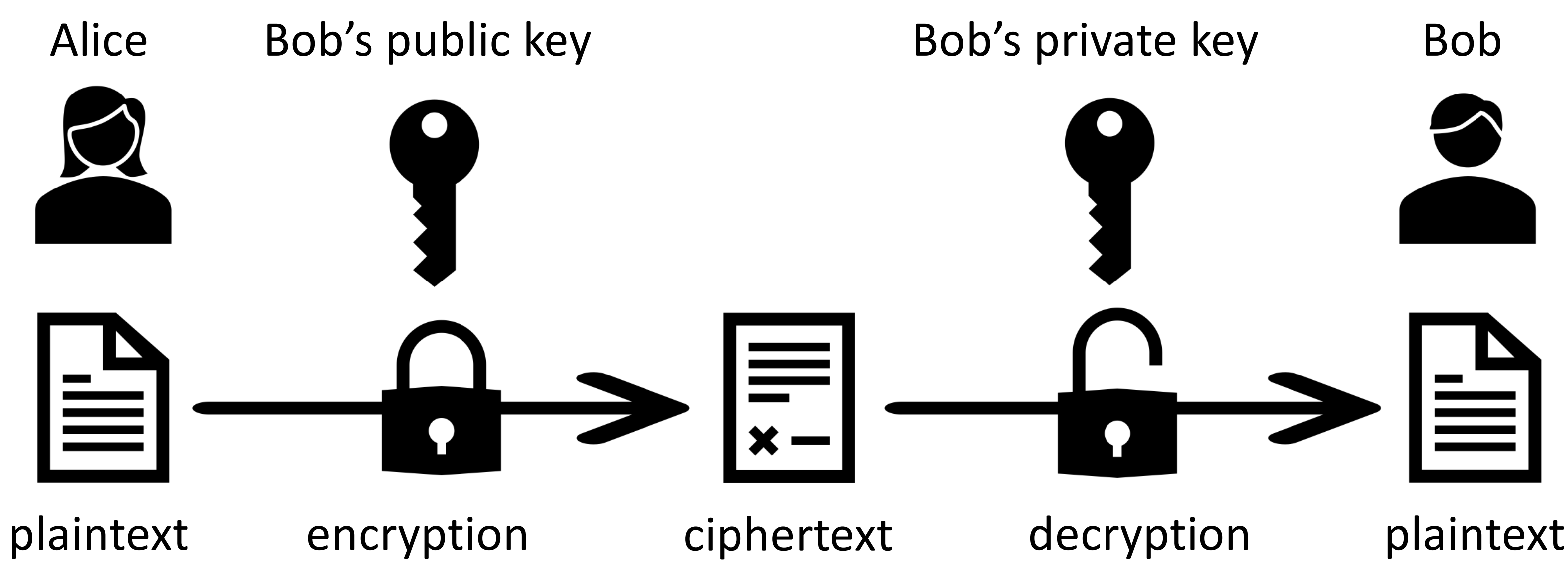
Private key (symmetric) encryption

(AES and 3DES)



Public key (asymmetric) encryption

(RSA, ECC and DH)



UMBC

Integer factorization

1459067680075833232301869393490706352924018723753571643995818710198734
3879900535893836957140267014980212181808629246742282815702292207674690
6543401224889672472407926969987100581290103199317858753663710862357656
5105078837142971156373427889114635351027120327651665184117268598379886
72111837205085526346618740053

- Problem: given an integer N, find its prime factors (**integer factorization**), e.g., $15 = 3 \times 5$.
- RSA scheme (public key -> private key)

Practice (5 min)

- https://github.com/zhangl64/qiskit-shor/blob/main/prime_factorization.py
- Download the code and test it with multiple numbers
  - 2,764,973 = 37 x 74,729
  - 5,436,949 = 29 x 187,481
  - 11,346,317 = 3,431 x 3,307
- Command: time python prime_factorization

UMBC

Shor's algorithm

14590676800758332323018693934907063529240187237535716439958187101987343879900535893836957140267014980212181808629246742282815702292207674690654340122488967247240792696998710058129010319931785875366371086235765651050788371429711563734278891146353510271203276516651841172685983798867211183720508552634661874005 3

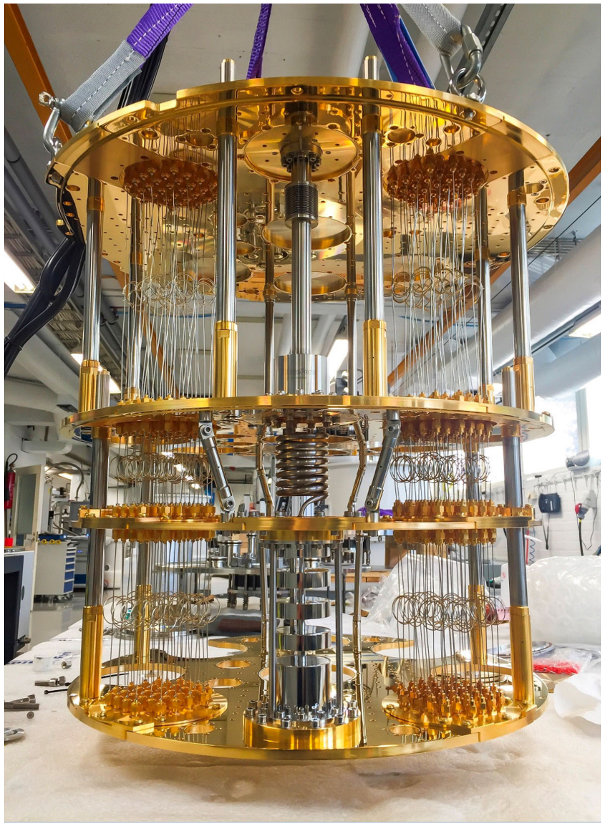
- The best classical algorithm has complexity $O(e^{1.9(logN)^{1/3}(loglogN)^{2/3}})$ – sub-exponential
- Shor's algorithm can solve it in quantum polynomial time $O((logN)^2(loglogN)(logloglogN))$


Peter Shor

Intro to Quantum

Fundamentals–what is quantum computing?

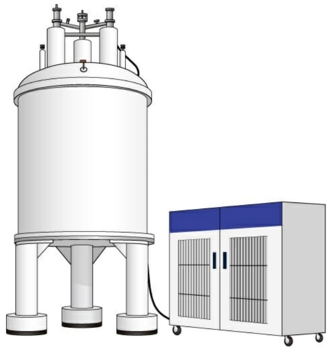
Quantum computing is the use of quantum mechanics (such as **superposition**, **entanglement**, and **interference**) to perform computation.

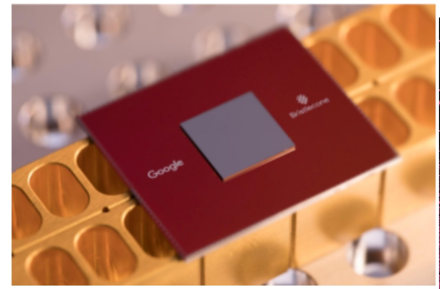


Source: Microsoft

UMBC

Timeline





1982 — First quantum computing model

1998 — First quantum computer (2-qubit)

← 18 years →

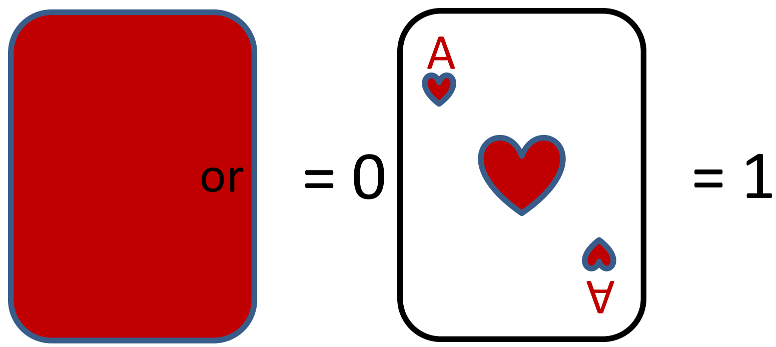
2016 — IBM: 5-qubit quantum computer

← 6 years →

2022 — IBM: 433-qubit quantum computer

? — Quantum Advantage

Qubits: a gentle introduction



A classical bit can only represent 0 or 1 at a time

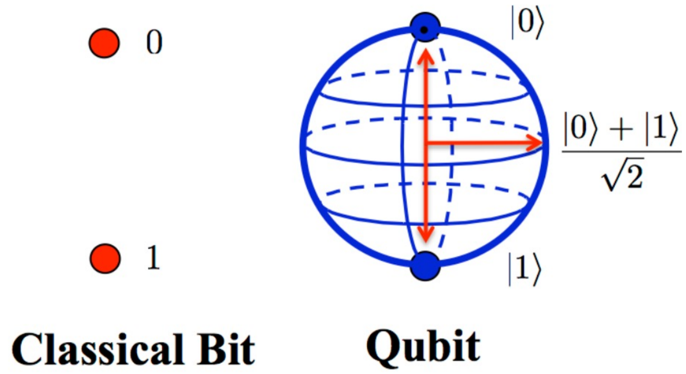
Qubits in superposition

= {0, 1}

1 qubit can represent 0 and 1 at the same time, i.e., "superposition".

Qubits

- A classical bit can take the value of 0 or 1.
  - A register of n bits can be one of 2^n states at a time.
- A qubit can be captured as a **superposition**
  - A register of n qubits can be 2^n different states.



Source: Poetry in Physics

“I think I can safely say that nobody really understands quantum mechanics,” Richard Feynman.

Scott Adams/Dilbert

Quantum Crypto

Motivation

The effective security strength of key encryption algorithms

Encryption type	Encryption algorithm	Key size (bits)	Effective security level on CCs (bits)	Effective security level on QCs (bits)
Public key	RSA 1024	1024	80	0
	RSA 2048	2048	112	0
	ECC 256	256	128	0
	ECC 384	384	256	0
Private key	AES 128	128	128	64
	AES 256	256	256	128

Shor's algorithm & Grover's algorithm on QCs

UMBC

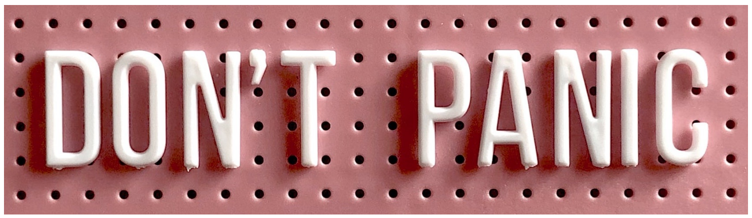
Factoring integers with sublinear resources on a superconducting quantum processor

Bao Yan,[1,2,*] Ziqi Tan,[3,*] Shijie Wei,[4,*] Haocong Jiang,[5] Weilong Wang,[1] Hong Wang,[1] Lan Luo,[1] Qianheng Duan,[1] Yiting Liu,[1] Wenhao Shi,[1] Yangyang Fei,[1] Xiangdong Meng,[1] Yu Han,[1] Zheng Shan,[1] Jiachen Chen,[3] Xuhao Zhu,[3] Chuanyu Zhang,[3] Feitong Jin,[3] Hekang Li,[3] Chao Song,[3] Zhen Wang,[3,†] Zhi Ma,[1,‡] H. Wang,[3] and Gui-Lu Long[2,4,6,7,§]

[1] *State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China*
[2] *State Key Laboratory of Low-Dimensional Quantum Physics and Department of Physics, Tsinghua University, Beijing 100084, China*
[3] *School of Physics, ZJU-Hangzhou Global Scientific and Technological Innovation Center, Interdisciplinary Center for Quantum Information, and Zhejiang Province Key Laboratory of Quantum Technology and Device, Zhejiang University, Hangzhou 310000, China*
[4] *Beijing Academy of Quantum Information Sciences, Beijing 100193, China*
[5] *Institute of Information Technology, Information Engineering University, Zhengzhou 450001, China*
[6] *Beijing National Research Center for Information Science and Technology and School of Information Tsinghua University, Beijing 100084, China*
[7] *Frontier Science Center for Quantum Information, Beijing 100084, China*

Shor's algorithm has seriously challenged information security based on public key cryptosystems. However, to break the widely used RSA-2048 scheme, one needs millions of physical qubits, which is far beyond current technical capabilities. Here, we report a universal quantum algorithm for integer factorization by combining the classical lattice reduction with a quantum approximate optimization algorithm (QAOA). The number of qubits required is $O(\log N/\log\log N)$, which is sublinear in the bit length of the integer N, making it the most qubit-saving factorization algorithm to date. We demonstrate the algorithm experimentally by factoring integers up to 48 bits with 10 superconducting qubits, the largest integer factored on a quantum device. We estimate that a quantum circuit with 372 physical qubits and a depth of thousands is necessary to challenge RSA-2048 using our algorithm. Our study shows great promise in expediting the application of current noisy quantum computers, and paves the way to factor large integers of realistic cryptographic significance.

Now or future?



- If it was true, are you ready?
- Take action now: replace public-key encryption with quantum-safe ones

UMBC

Emerging Software Technologies

Making your software quantum safe

May 4, 2022

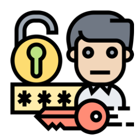
National Security Memo (NSM-10) on Mitigating Risks to Quantum Attacks

Sep 7, 2022

NSA: Commercial National Security Algorithm Suite 2.0 (CNSA 2.0)

Nov 18, 2022

OMB: Migrating to Post-Quantum Cryptography (PQC)



Dec 21, 2022

Law H.R.7535 Quantum Computing Cybersecurity Preparedness Act

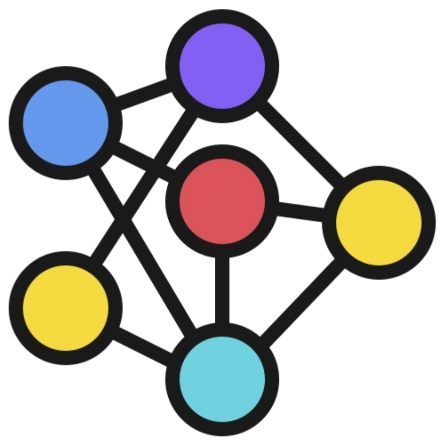
2024--2033

NIST PQC Standard; Migration to PQC

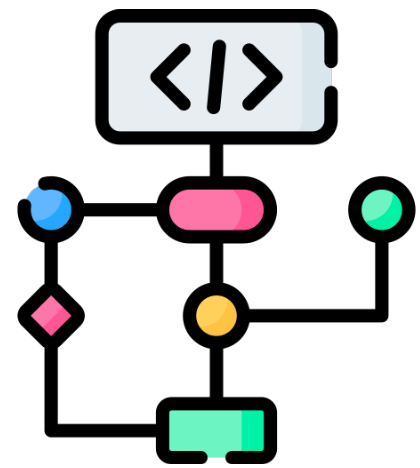
Icons credits: Xmind and Flaticon

What is PQC?

Classical
Algorithms



+



Classical
Computers

How to migrate to PQC?

1. Find Public-Key Encryption (PKE)

2. Replace PKE with PQC

PQC: Kyber

Kyber

Build Status coverage 93%

This repository contains the official reference implementation of the Kyber key encapsulation mechanism, and an optimized implementation for x86 CPUs supporting the AVX2 instruction set. Kyber has been selected for standardization in round 3 of the NIST PQC standardization project.

- https://github.com/pq-crystals/kyber

UMBC

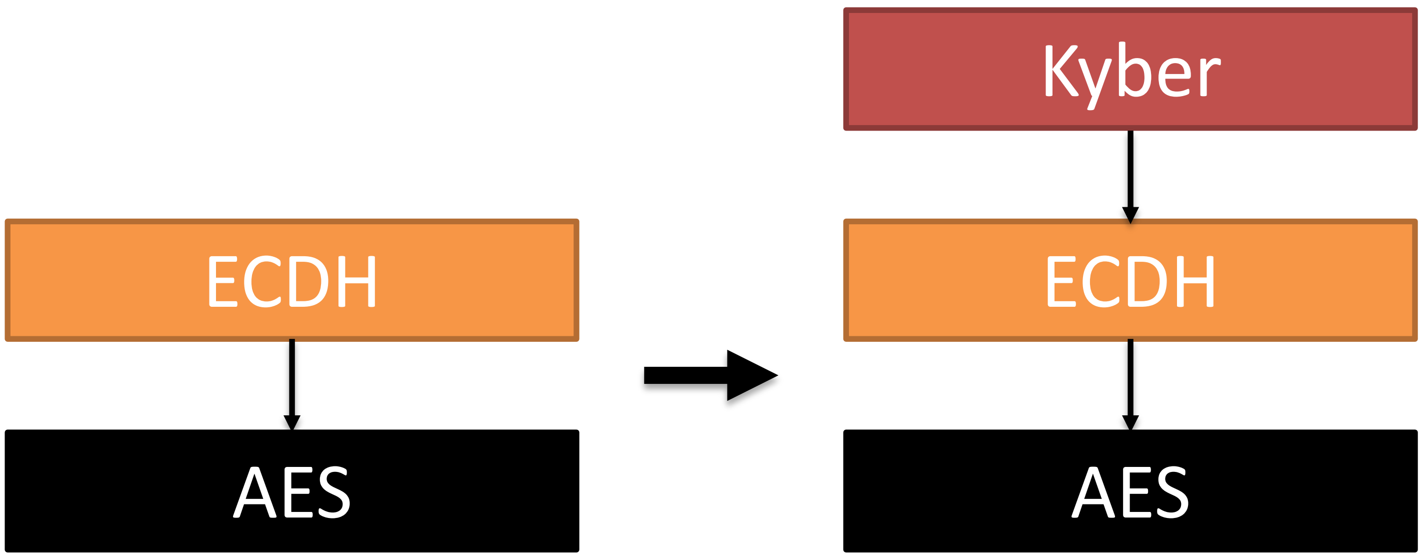
Challenge 1

- How to identify all the functions related to public key encryption?
  - OpenVPN has 168,090 lines of code and 500 files

```
     10 tests/unit_tests/plugins/auth-pam/Makefile.am
     92 tests/unit_tests/plugins/auth-pam/test_search_and_replace.c
     16 tests/update_t_client_ips.sh
     15 version.m4
 168090 total
(base) leizhang@Leis-MBP-14 openvpn %
```

Challenge 2

- What happens if Kyber is not secure in the future?

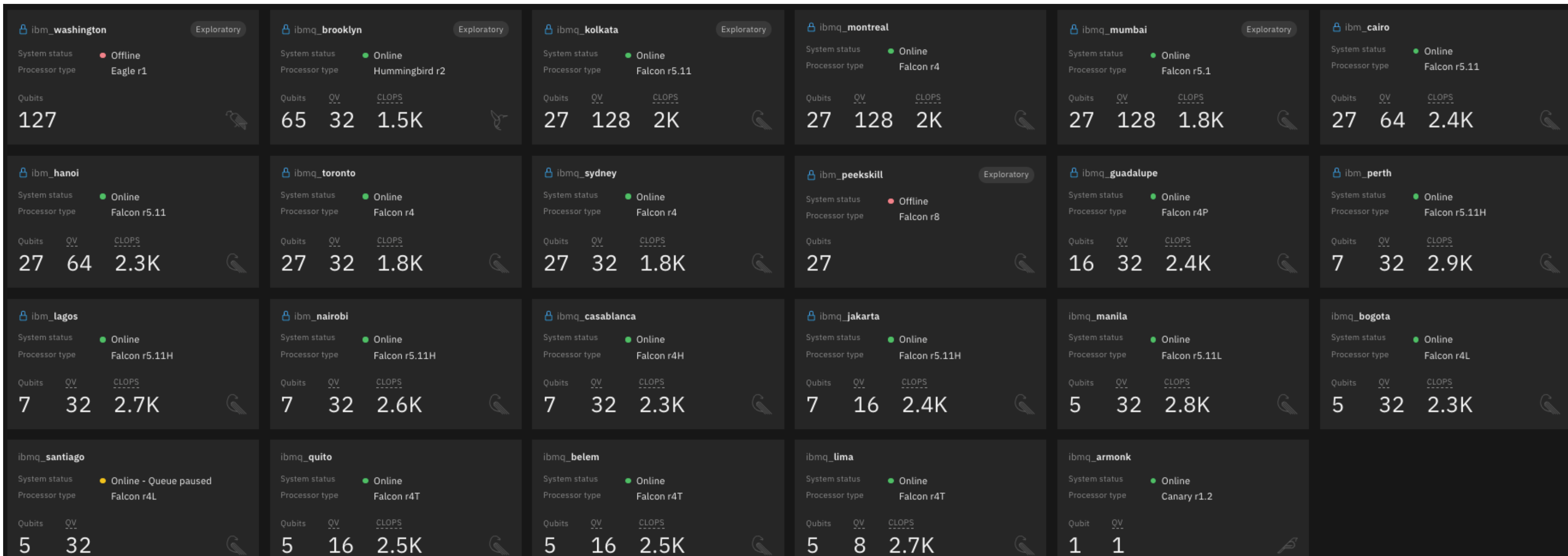


Classical Crypto

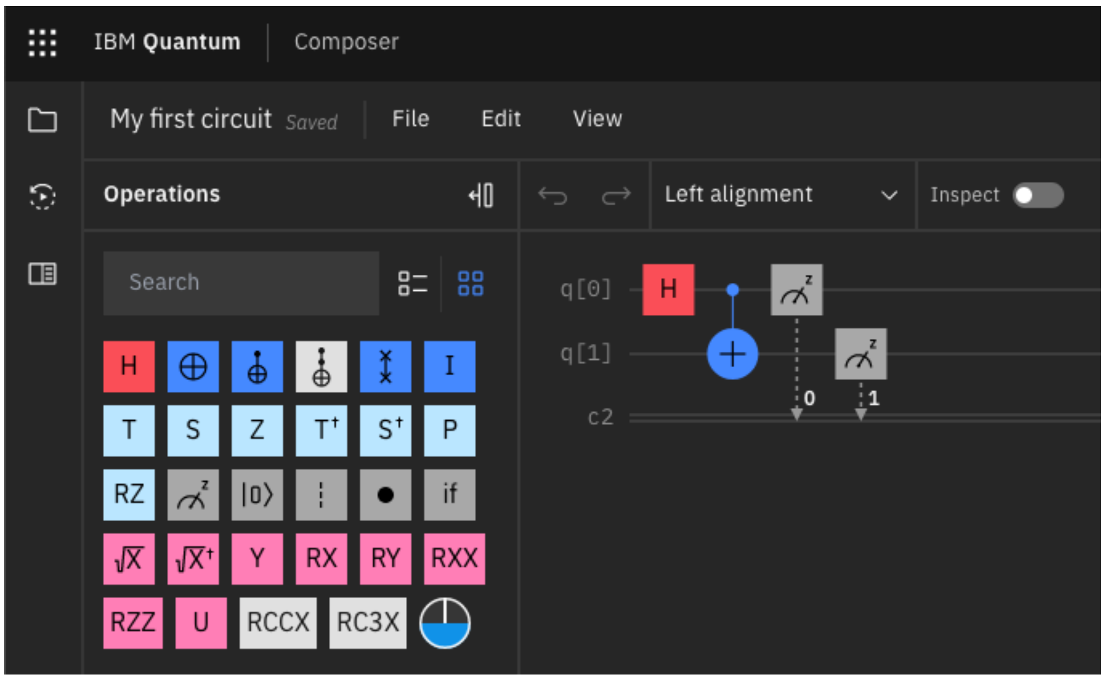
Hybrid Crypto

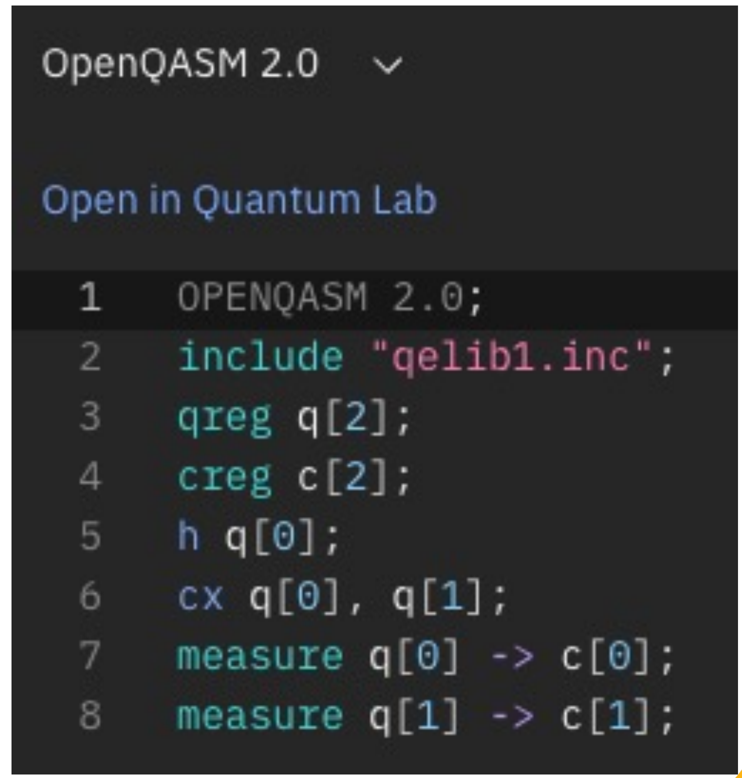
Beyond this lecture…

IBM quantum systems



IBM Q Experience





Quantum development platforms

Feature	Q#	Qiskit	Cirq	Quipper	Scaffold
Invocation	Standalone, usable from Python, C#, F#	Embedded into Python	Embedded into Python	Embedded into Haskell[a]	Standalone
Classical feedback	Yes	Yes[b]	No	Yes	Yes[c]
Adjoint generation	Yes	Yes	Yes	Yes	No
Resource estimation	Gate counts, number of qubits, depth and width, call graph profiling	Gate counts, number of qubits, depth and width	Gate counts, number of qubits	Gate counts, number of qubits, depth and width	Gate counts, number of qubits, depth[d]
Libraries	Standard, chemistry, numerics, ML	Standard, chemistry, optimization, finance, QCVV, ML	Standard, chemistry, ML	Standard, numerics	Standard[e]
Learning materials	Docs, tutorials, Katas	Docs, tutorials, textbook	Docs, tutorials	Docs[f], tutorials	Tutorials[g]

Kahoot!

- No need to sign up
- Any mobile devices with Internet
  - Phone, laptop, etc
- Just type the web link in your browser: **www.kahoot.it**
- Join with PIN on the screen

Thank you! Please take the survey.

https://forms.gle/fErS4QPubt9kFw6C8