Quantum Computing & Cryptography

Richard Perry

Villanova University

Department of Electrical and Computer Engineering

richard.perry@villanova.edu

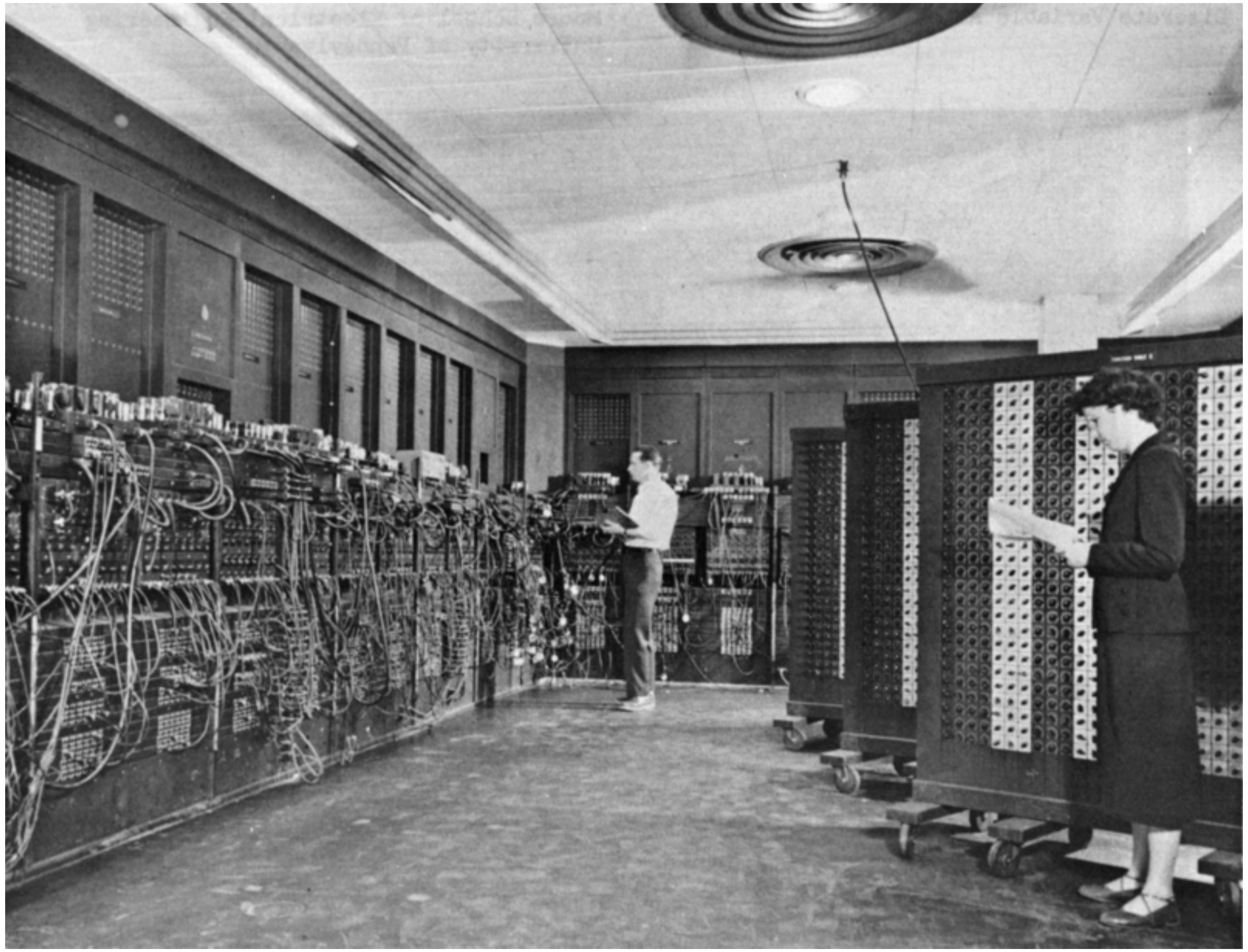
March 2020

0100001011100110101001111011011011101001101111110000101010001001101010011011101011011000101001111000001111110100101000011010001010111111111000101011001111111000001010111

Outline

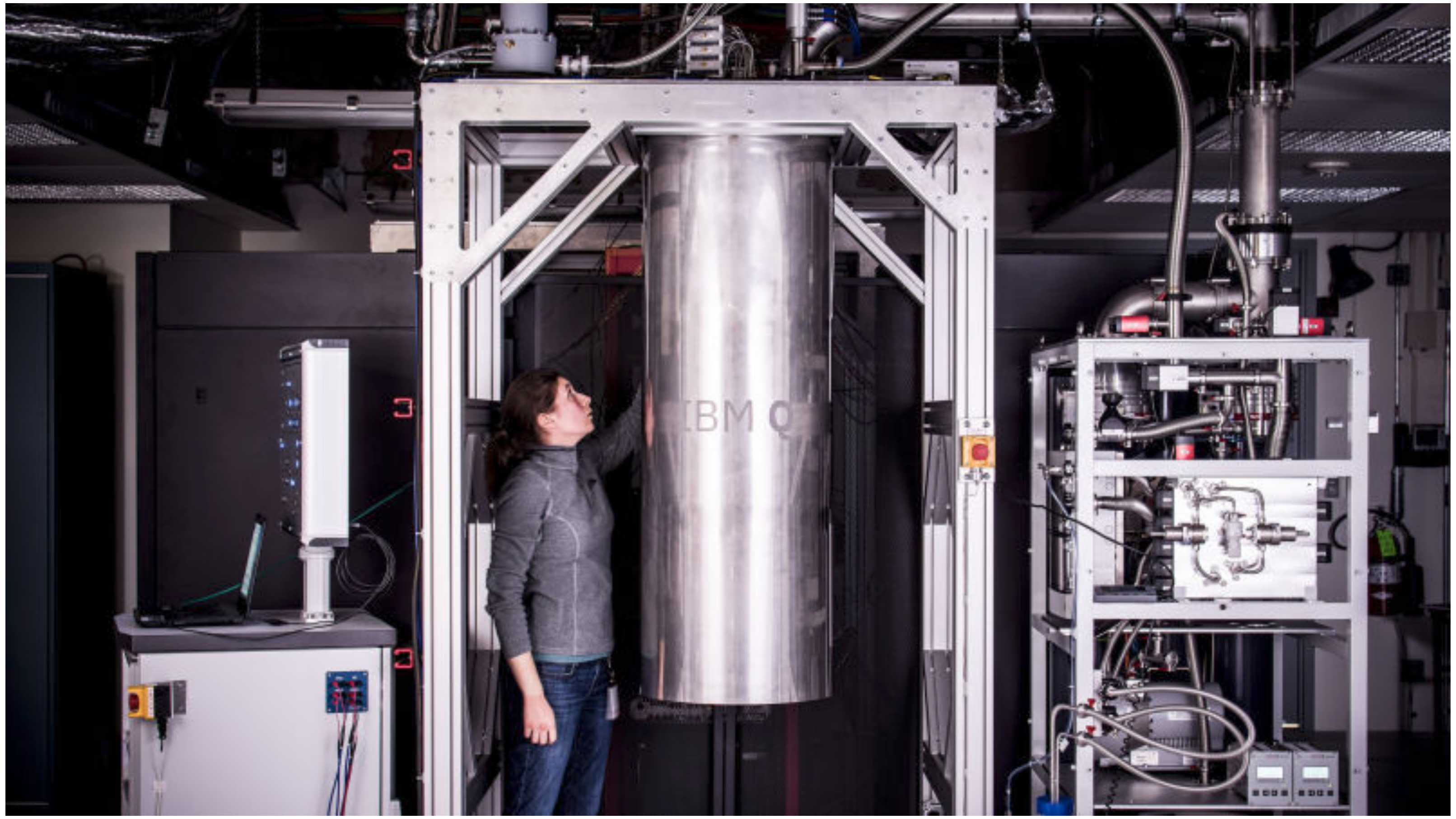
1. Background
2. Physics
3. Math
4. Simulation
5. Breaking Cryptography
6. Post-Quantum Cryptography

Eniac 1950: 30 tons, 150 KW, 1 KB, 100 KHz

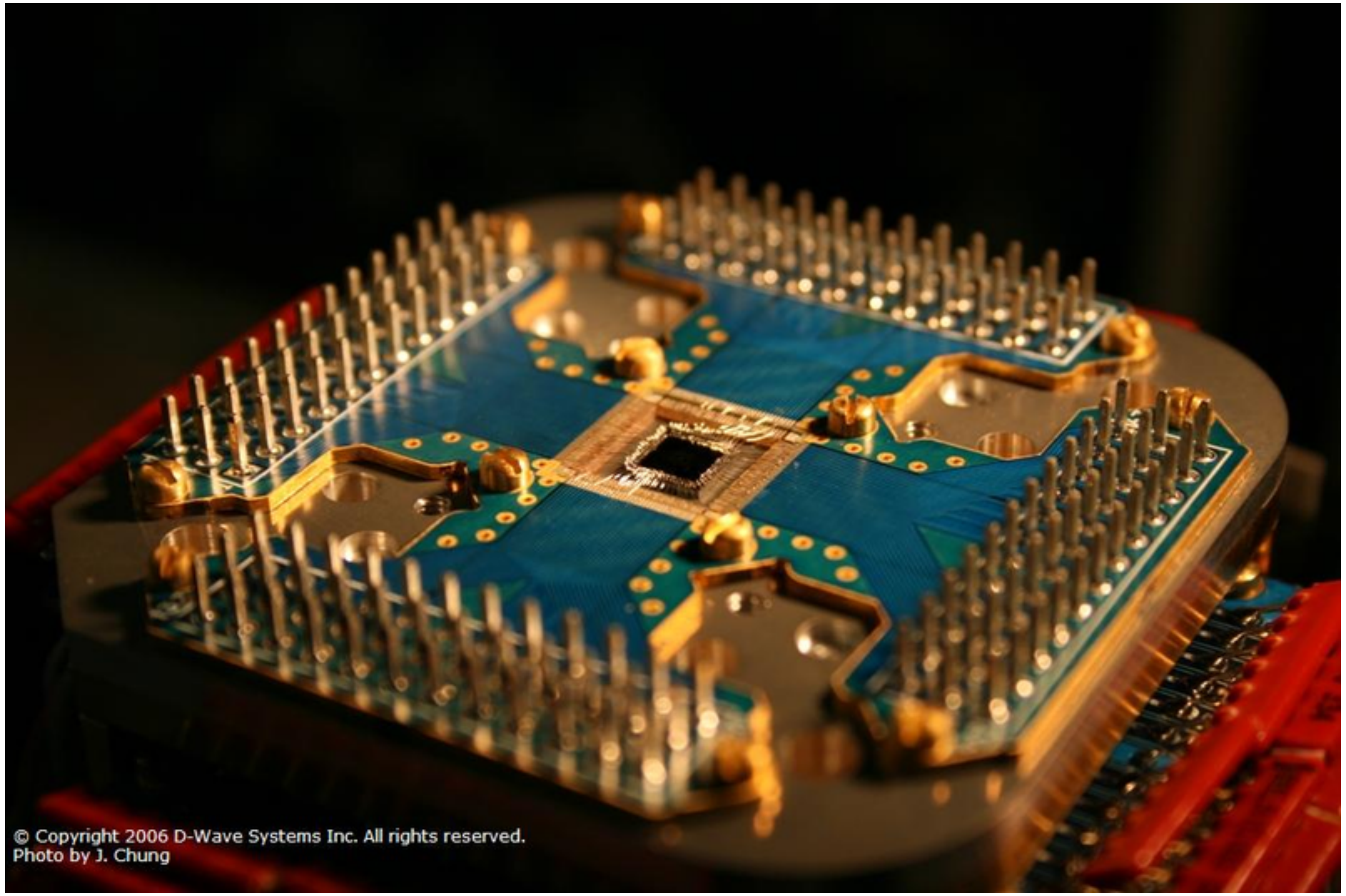


Phone 2020: 5 oz., 1 W, 4 GB, 2 GHz

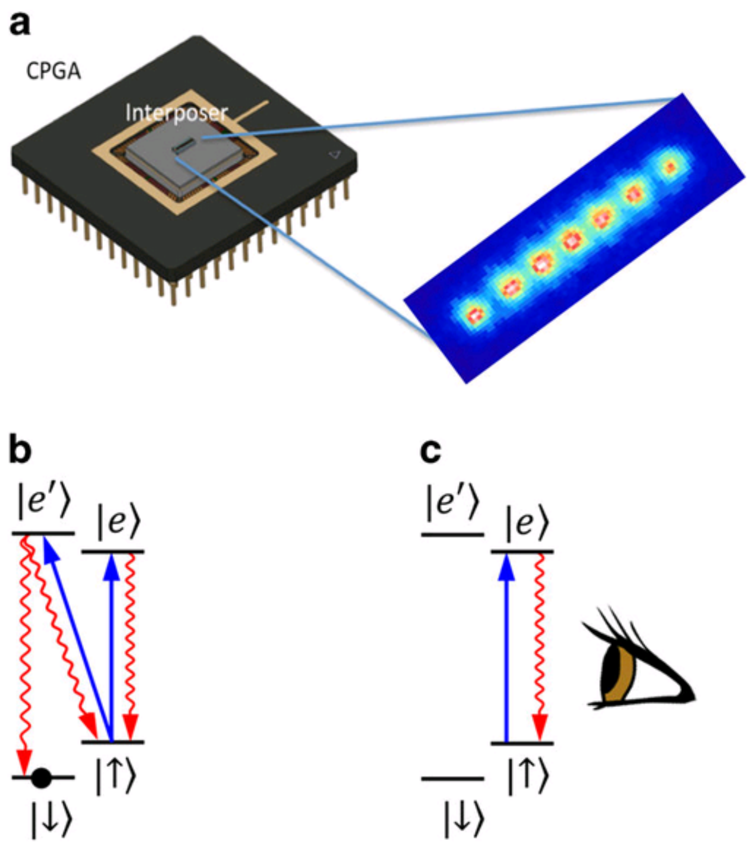
QC 2020: tons, KW, 50 qubits, 1 MHz



QC 2050: ???


© Copyright 2006 D-Wave Systems Inc. All rights reserved.
Photo by J. Chung

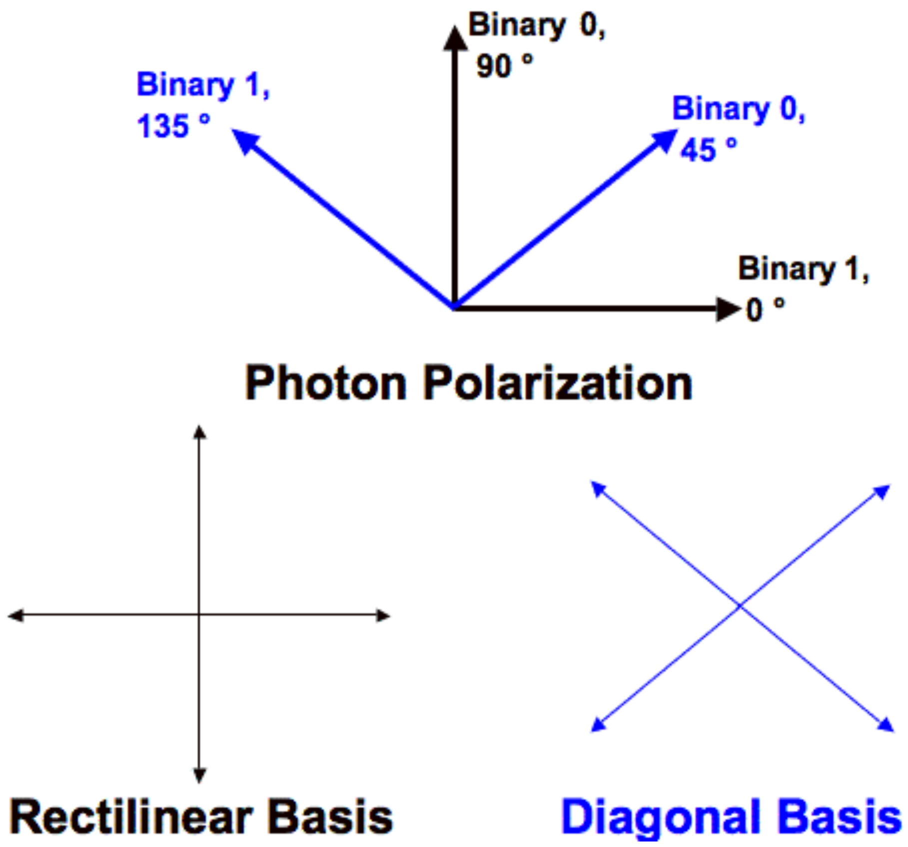
Ion Trap Quantum Device



(**a**) Schematic of silicon chip-trap mounted on a ceramic pin grid array carrier with raised interposer, confining atomic ions that hover ~75 µm above the surface. The inset is an image of 7 atomic ytterbium ($^{171}Yb^{+}$) ions arranged in a linear crystal and laser-cooled to be nearly at rest. The few-micrometre separation between ions is determined by a balance between the external confinement force and Coulomb repulsion. (**b**,**c**) Reduced energy level diagram of a single $^{171}Yb^{+}$ atomic ion, showing the atomic hyperfine levels $|\uparrow\rangle$ and $|\downarrow\rangle$ that represent a qubit. The electronic excited states $|e\rangle$ and $|e'\rangle$ are separated from the ground states by an energy corresponding to an optical wavelength of 369.53 nm, and applied laser radiation (blue arrows) drives these transitions for (**b**) initialisation to state $|\downarrow\rangle$, and (**c**) fluorescence detection of the qubit state ($|\uparrow\rangle$, fluorescence, $|\downarrow\rangle$, no fluorescence).

[Co-designing a scalable quantum computer with trapped atomic ions], Kenneth R Brown, Jungsang Kim & Christopher Monroe, Nature 2016.

Quantum Key Distribution



A Survey of the Prominent Quantum Key Distribution Protocols, Mart Haitjema. Figure 2, corrected.

Quantum Key Distribution

Alice's bit	0	1	1	0	1	0	0	1
Alice's basis	+	+	X	+	X	X	X	+
Alice's polarization	↑	→	↖	↑	↖	↗	↗	→
Bob's basis	+	X	X	X	+	X	+	+
Bob's measurement	↑	↗	↖	↗	→	↗	→	→
Public discussion								
Shared Secret key	0		1			0		1

Alice's bits:	**secret**
Alice's basis:	**initially secret, public later**
Alice's polarization:	**secret**
Bob's basis:	**public**
Bob's measurement:	**secret**

A Survey of the Prominent Quantum Key Distribution Protocols, Mart Haitjema. Figure 3.

Schrödinger Equation

$$i\hbar \frac{d|\psi\rangle}{dt} = H|\psi\rangle$$

Complex state vector Ψ: $|\Psi_i|^2$ = Prob(measure state i)

Hamiltonian matrix H, Hermitian: $H^\dagger = H$

$$|\psi(t_2)\rangle = \exp\left[\frac{-iH(t_2 - t_1)}{\hbar}\right]|\psi(t_1)\rangle = U(t_1, t_2)|\psi(t_1)\rangle$$

$$U(t_1, t_2) \equiv \exp\left[\frac{-iH(t_2 - t_1)}{\hbar}\right]$$

Unitary matrix U: $U^{-1} = U^\dagger$

Quantum Computation and Quantum Information, 10th Anniversary Edition, Michael A. Nielsen & Isaac L. Chuang, Cambridge University Press, 2010.

One Qubit

The standard basis for $\mathbb{C}^2$ *is denoted by* $|0\rangle_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. *The standard basis for* $(\mathbb{C}^2)^{\otimes q}$, *which has* 2^q *elements, is denoted by* $|0\rangle_q, |1\rangle_q, \ldots, |2^q - 1\rangle_q$.

If we pick the standard basis for $\mathbb{C}^2$, *then a single qubit* $(q = 1)$ *can be represented as* $\alpha|0\rangle + \beta|1\rangle = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ *where* $\alpha, \beta \in \mathbb{C}$ *and* $|\alpha|^2 + |\beta|^2 = 1$.

Superposition: $\alpha\ |0> + \beta\ |1>$

Complex Amplitudes: $\alpha,\ \beta$

Probabilities: $|\alpha|^2,\ |\beta|^2$

An Introduction to Quantum Computing, Without the Physics, Giacomo Nannicini, 2017 (2020).

Single Qubit Operations

Definition 11. *The four Pauli gates are the following single-qubit gates:*

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Proposition 5. *The Pauli gates form a basis for $\mathbb{C}^{2\times 2}$, they are Hermitian, and they satisfy the relationship $XYZ = iI$.*

The X, Y, Z gates all correspond to $90°$ rotations, around different axes. The X gate flips a qubit:

$$X|0\rangle = |1\rangle \qquad X|1\rangle = |0\rangle.$$

This is the equivalent of a NOT gate in classical computers. At the same time, the Z gate is also called a phase-flip gate: it leaves $|0\rangle$ unchanged, and maps $|1\rangle$ to $-|1\rangle$.

$$Z|0\rangle = |0\rangle \qquad Z|1\rangle = -|1\rangle.$$

A single-qubit gate that is used in many quantum algorithms is the *Hadamard* gate:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

The action of H is as follows:

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Superposition

An Introduction to Quantum Computing, Without the Physics, Giacomo Nannicini, 2017 (2020).

01000010111001101010011110110110111010011011111110000101010001001101010011011101011011000101001111000001111110100101000011010001010111111111100010101100111111100000101011011110011010101101111111

Two Qubits

Let us write the basis elements of $(\mathbb{C}^2)^{\otimes 2} = \mathbb{C}^2 \otimes \mathbb{C}^2$*:*

$$|0\rangle_2 = |0\rangle \otimes |0\rangle = |00\rangle = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} \qquad |1\rangle_2 = |0\rangle \otimes |1\rangle = |01\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$$

$$|2\rangle_2 = |1\rangle \otimes |0\rangle = |10\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \qquad |3\rangle_2 = |1\rangle \otimes |1\rangle = |11\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}.$$

$$|x\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$$
$$|y\rangle = \beta_0|0\rangle + \beta_1|1\rangle.$$

that taken as a whole will be in state:

$$|x\rangle \otimes |y\rangle = \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle, \tag{1}$$

with the normalization conditions $|\alpha_0|^2 + |\alpha_1|^2 = 1$ and $|\beta_0|^2 + |\beta_1|^2 = 1$. The general state of a 2-qubit register $|\psi\rangle$ is:

$$|\psi\rangle = \gamma_{00}|00\rangle + \gamma_{01}|01\rangle + \gamma_{10}|10\rangle + \gamma_{11}|11\rangle, \tag{2}$$

with normalization condition $|\gamma_{00}|^2 + |\gamma_{01}|^2 + |\gamma_{10}|^2 + |\gamma_{11}|^2 = 1$.

Entanglement

An Introduction to Quantum Computing, Without the Physics, Giacomo Nannicini, 2017 (2020).

CNOT: creating entangled states

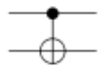


Figure 10: The CNOT, or controlled-NOT, gate.

The matrix description of the gate with control qubit 2 and target qubit 1 is as follows:

$$\mathrm{CNOT}_{21} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

initially a = |0>+|1>, b = |0>

q	a b	p	->	a b⊕a	
0	0 0	0.5		0 0	0.5
1	0 1			0 1	
2	1 0	0.5		1 0	
3	1 1			1 1	0.5

```
class TwoQubit:
  def cnot(self):
      '''Controlled NOT operation'''
      self.onezero, self.oneone = self.oneone, self.onezero
      return self
```

Using an array:

q[0], q[1], q[2], q[3]

swap q[2] and q[3]

Using names for the complex amplitudes:

zerozero, zeroone, onezero, oneone

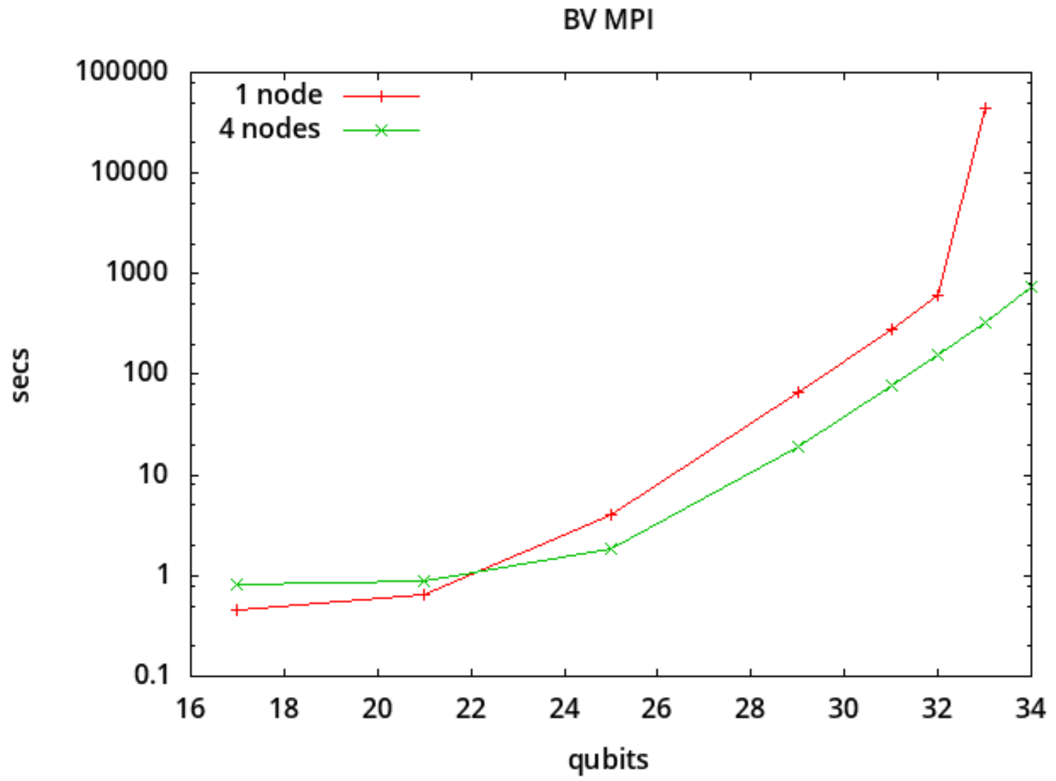
Python Quantum Computing simulator, Juliana Peña, 2011.

0100001011100110101001111011011011101001101111110000101010001001101010011011101011011000101001111000001111110100101000011010001010111111111000101011001111111000001010110111100110101011011111111

Simulation: n qubits -> 2^n complex state amplitudes

$$\begin{array}{c}1\\ \begin{bmatrix} q_0 \\ q_1 \end{bmatrix}\end{array} \quad \begin{array}{c}2\\ \begin{bmatrix} q_0 \\ q_1 \\ q_2 \\ q_3 \end{bmatrix}\end{array} \quad \begin{array}{c}3\\ \begin{bmatrix} q_0 \\ q_1 \\ q_2 \\ q_3 \\ q_4 \\ q_5 \\ q_6 \\ q_7 \end{bmatrix}\end{array} \quad \begin{array}{c}4\\ \begin{bmatrix} q_0 \\ q_1 \\ q_2 \\ q_3 \\ q_4 \\ q_5 \\ q_6 \\ q_7 \\ q_8 \\ q_9 \\ q_{10} \\ q_{11} \\ q_{12} \\ q_{13} \\ q_{14} \\ q_{15} \end{bmatrix}\end{array} \quad \begin{array}{c}5\\ \begin{bmatrix} q_0 \\ q_1 \\ q_2 \\ q_3 \\ q_4 \\ q_5 \\ q_6 \\ q_7 \\ q_8 \\ q_9 \\ q_{10} \\ q_{11} \\ q_{12} \\ q_{13} \\ q_{14} \\ q_{15} \\ q_{16} \\ q_{17} \\ q_{18} \\ q_{19} \\ q_{20} \\ q_{21} \\ q_{22} \\ q_{23} \\ q_{24} \\ q_{25} \\ q_{26} \\ q_{27} \\ q_{28} \\ q_{29} \\ q_{30} \\ q_{31} \end{bmatrix}\end{array}$$

Simulation: distributed computing



For n=33 qubits, 128 GB of memory is required just for the array of quantum amplitudes. On a single 128 GB node this causes swapping, and the run-time increases to 43832 seconds (about 12 hours) which is a factor of 36 times what would be expected following the exponential scaling (20 minutes). For n=34 qubits a single node has insufficient memory and can not perform the simulation.

Simulating Single Qubit Gate Operations in a Distributed Environment, R. Perry, 2019

Grover's Search (1996): Quadratic Speedup

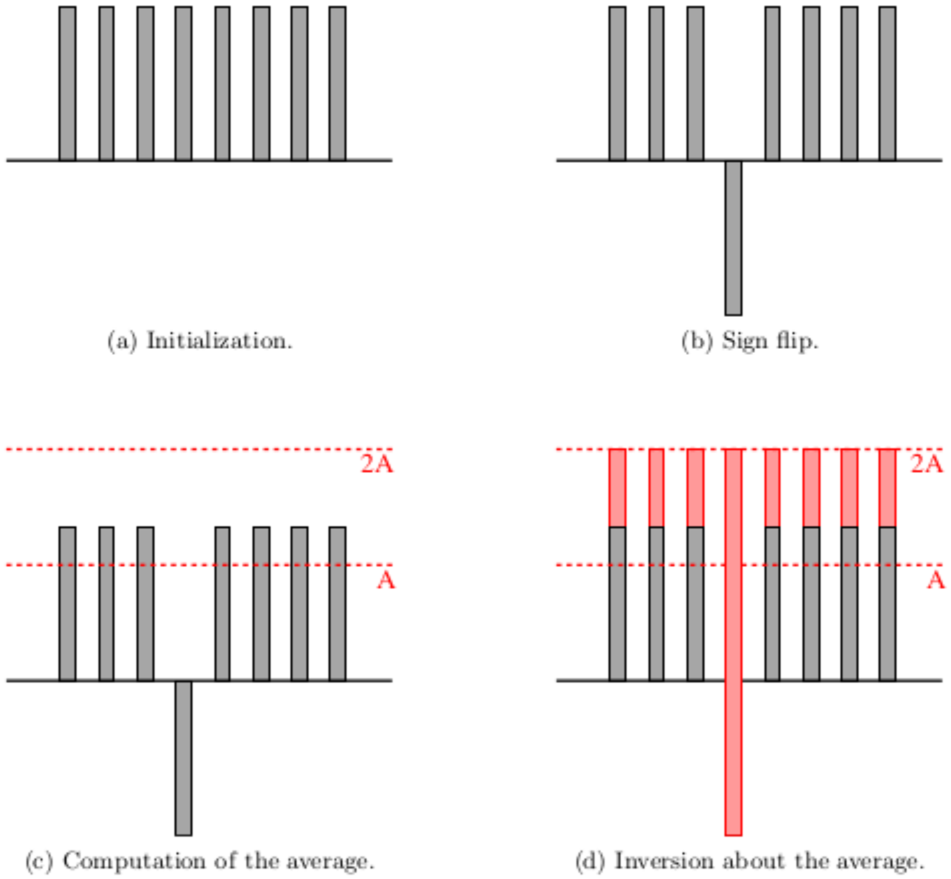
- **Search space of size 2^n using $2^{(n/2)}$ function evaluations vs. classical $(2^n)/2$**
- **Security implications: 256-bit key for ANY algorithm will have only 128-bit security level**
- **Simulation:**

```
for( iter = 1; iter <= k; ++iter)
{
 // apply f, i.e. flip sign of state m
 //
  q[m] = -q[m];

 // inversion about the average
 //
  avg = 0;  for( i = 0; i < N; ++i) avg += q[i];

  avg *= 2.0/N;  for( i = 0; i < N; ++i) q[i] = avg - q[i];
}
```

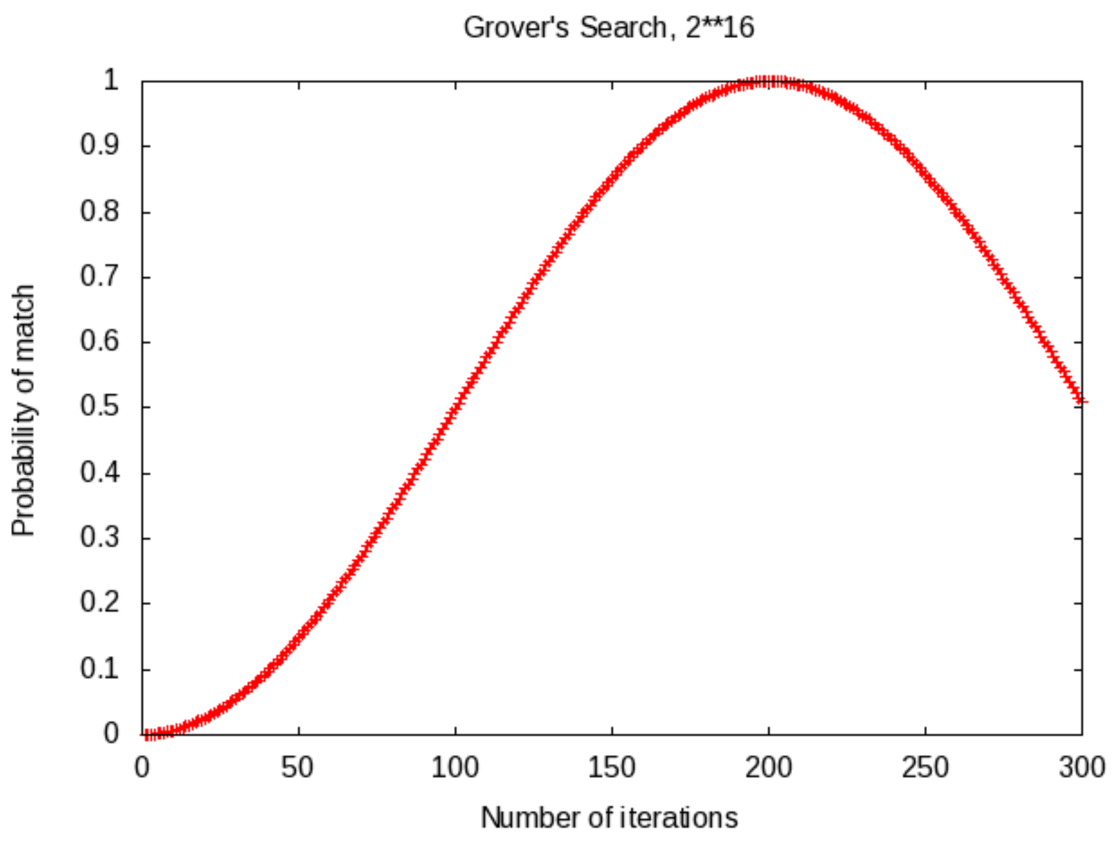
Grover's Search: inversion about the average



[An Introduction to Quantum Computing, Without the Physics](), Giacomo Nannicini, 2017 (2020).

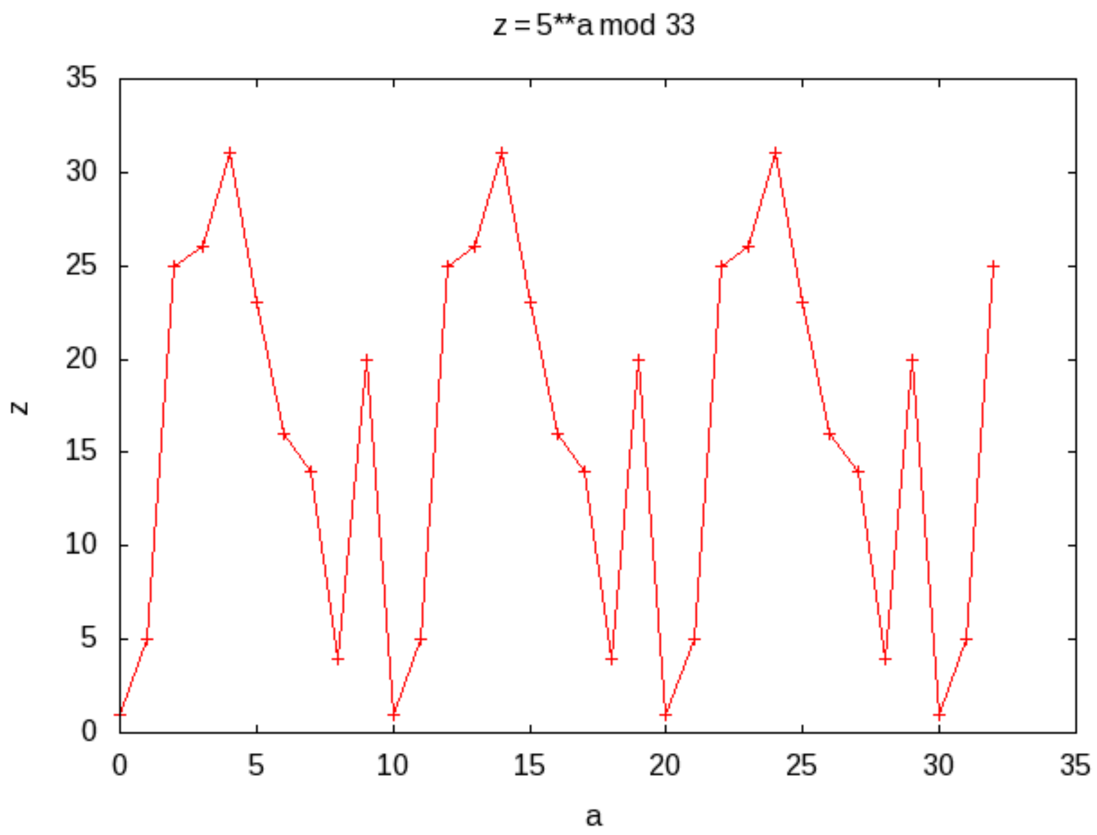
Grover's Search: 16-bit Example

- 2^{16} = 65536 possibilities, would take $(2^{16})/2$ = 32768 iterations on average classically
  - Takes only $(\pi/4)2^{(16/2)}$ = 201 quantum iterations optimally, success probability 0.999988



Shor factoring (1994): breaking RSA

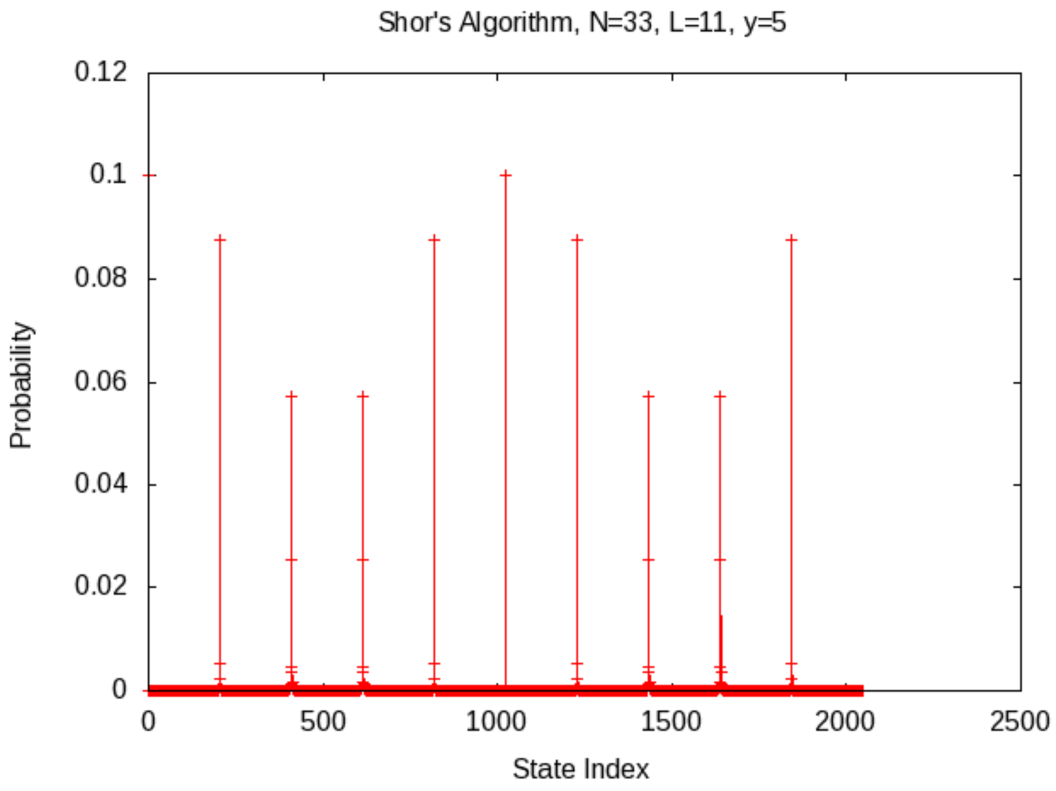
- Quantum evaluation of y^a `mod N` for random y, and ALL `a` at once
- Determine period r, mod N: $y^r = 1$, so $(y^{r/2} - 1)*(y^{r/2} + 1) = 0$ -> will share factor with N



0100001011100110101001111011011011101001101111111000010101000100110101001101110101101100010100111100000111111010010100001101000101011111111100010101100111111100000101011011110011010101101111111

Shor factoring example: N = 33

- **DFT probability peaks (205, 410, 614, 819, ...) produce period estimates (9.9902, 4.9951, 3.3355, 2.5006, ...)**
- **Using r = 10 ≈ 9.9902: $(5^{10/2} - 1)*(5^{10/2} + 1) = 22*24$**
  - **gcd(22,N) = 11, gcd(24,N) = 3, both factors of N**



Post-Quantum Cryptography

- **NIST = National Institute of Standards and Technology**
- **Standardizing one or more quantum-resistant public-key cryptographic algorithms**
- **For use on classical computers**
- **Must be resistant to classical and quantum computing attacks**
- **Second-round candidate algorithms include:**
  - **17 public-key encryption and key-establishment algorithms**
  - **9 algorithms for digital signatures**
- **"*A wide range of mathematical ideas are represented by these algorithms... to hedge against the possibility that if someone breaks one, we could still use another.*"**
- **pqcrypto.org - Dan Bernstein's post-quantum cryptography resources**

NIST Post-Quantum-Cryptography-Standardization

NIST Reveals 26 Algorithms Advancing to the Post-Quantum Crypto 'Semifinals'

01000010111001101010011110110110111010011011111100001010100010011010100110111010110110001010011110000011111101001010000110100010101111111110001010110011111100000101011

References

1. An Introduction to Quantum Computing, Without the Physics, Giacomo Nannicini, 2017 (2020). *arxiv.org/abs/1708.03684*
2. Python Quantum Computing simulator, Juliana Pena, 2011. Two qubits and superdense coding protocol example. *gist.github.com/limitedmage/945473*
3. Quantum Computing Emulation, R. Perry, 2018-2020. *fog.misty.com/perry/qce/notes.html*

Hackers of the Future

Already planning attacks on quantum computers:

4. An entangling-probe attack on Shor's algorithm for factorization, Hiroo Azuma, 2017. arxiv.org/abs/1705.00271 : *an attacker can steal an exact solution of Shor's algorithm outside an institute where the quantum computer is installed if he replaces its initialized quantum register with entangled qubits.*