QUANTUM COMPUTERS -
STATE OF DEVELOPMENT FOR CRYPTANALYSIS

4.6.24 | PROF. DR. FRANK WILHELM-MAUCH, PGI-12
INHALT

• Motivation and some basic notions
• Why are errors so crucial?
• State of play in quantum error correction
• NISQ-algorithms for cryptanalysis?
• Status of various platforms
• New developments
MOTIVATION AND SOME BASIC NOTIONS
MOTIVATION

Why talk about quantum computers in crypto

• Decoding of RSA is the „killer app“ of quantum computing (Shor / Regev)
• Significant industrial and public activity - lots of news about some kind of progress
• What is real? What is hype? What should a cryptoanalyst look at for risk assessment?
• How much time do we have for moving to PQC?
WHAT IS QUANTUM SPEEDUP

What does it mean that quantum computers are faster than classical ones?

• Change of temporal complexity as problem size grows, e.g., polynomial instead of exponential

• e.g. RSA encryption: Known decryption method is superpolynomially hard, i.e., encryptor wins race for resources

• In some cases, changing the degree of the polynomial also makes a difference

• Clockspeed of quantum computer prototypes often quite slow - Trapped ions (100 kHz), superconducting chips (50 MHz)

Not clockspeed
THE ERA OF EARLY QUANTUM SUPREMACY

Meaning of the Google 2019 and later results

| Up to 50 qubits | Beyond 50 qubits | NISQ-Era | Beyond 1M Qubits |
|-----------------|------------------|----------|-----------------|
| Basic research in physics | Quantum advantage | Applied quantum advantage possible? | Provable quantum advantage |

- Quantum advantage based on exponential need for memory: **Most likely irreversible**
- N qubits correspond to $2^N$ floating point numbers - beyond large HPC at N>50
- Current goal: Better machines and more efficient algorithms: NISQ Era (NISQ: Noisy intermediate-scale quantum technologies)
- NISQ-Macines are **R&D infrastructure**
WHERE DOES SPEEDUP COME FROM

Classical Computer

- Binary data
- Single binary number pre register
- Sequential operations
- Parallel Operations require multiple cores

Quantum computer

- Binary data
- Quantum particles can sample multiple places / paths at once
- Quantum data can sample multiple calculations at once
- Computing along all allowed paths possible on one quantum core
POSTULATES OF QUANTUM COMPUTER PHYSICS

A peek into the black box

Quantum state $|\psi\rangle$: All possible information about the state
In general only statistical predictions about measurements
• Superposition of all evolutions
• All possible paths in mechanics - all possible calculations in informatics
USING QUANTUM SPEEDUP

Quantum parallelism

= Broad superposition + probability amplitudes

Parallel unitary operations

Challange

- Uncompute parallelism in the end
- Use quantum instruction set

Binary input

Only few known solutions

These are important primitives
• Note - a quantum gate needs to be the time evolution of a quantum system, hence it needs to be unitary, hence it needs to be invertible, hence the number of in-and output bits needs to be identical.
Single qubit gates

- Unitary maps on $\mathbb{C}^2$, global phase unimportant - Lie group

$$\text{SU}(2) = \{ U \in \mathbb{C}^{2 \times 2} : U^\dagger U = \mathbb{I}, \det(U) = 1 \}$$

- Identity: $|0\rangle \leftrightarrow |0\rangle, |1\rangle \leftrightarrow |1\rangle$ so $U = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

- NOT: $|0\rangle \leftrightarrow |1\rangle, |1\rangle \leftrightarrow |0\rangle$ so $U = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

- SET (0): $|0\rangle \leftrightarrow |0\rangle, |1\rangle \leftrightarrow |0\rangle$ not invertible, not unitary, not physical
The Hadamard gate

Define the Eigenstates of $\hat{X}$: $|\pm\rangle = \frac{1}{\sqrt{2}} (|0\rangle \pm |1\rangle)$: $\hat{X}|\pm\rangle = \pm |\pm\rangle$

Hadamard gate $H$: $|0\rangle \mapsto |+\rangle, |1\rangle \mapsto |-\rangle$ so $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

$H|+\rangle = \frac{1}{2} (|+\rangle + |-\rangle) = |0\rangle$ and $H|-\rangle = |1\rangle$ so $H^2 = \mathbb{I}$

- Turns computational basis states into even superpositions (tagged by a phase factor)

Key application: n-qubit Hadamard $H^\otimes n |0\rangle^\otimes n \equiv |H_n\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \otimes \cdots = \frac{1}{2^{n/2}} \sum_{s=0}^{2^n-1} |s\rangle$ e.g.

$n=2$: $HH|00\rangle = \frac{1}{2} \left( |00\rangle + |01\rangle + |10\rangle + |11\rangle \right)$
Rotation gates

Take a Pauli matrix $\sigma_k$. We have already shown that

$$ R_k^\alpha = \exp \left( -\frac{i}{2} \alpha \sigma_k \right) = \cos \frac{\alpha}{2} - i \sigma_k \sin \frac{\alpha}{2} $$

is a unitary matrix.

**Example**

$$ R_z^\alpha = \begin{pmatrix} e^{-i\alpha/2} & 0 \\ 0 & e^{i\alpha/2} \end{pmatrix} = e^{-i\alpha/2} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix} $$

**Example**

$$ R_x^\alpha = \begin{pmatrix} \cos \alpha/2 & -i \sin \alpha/2 \\ -i \sin \alpha/2 & \cos \alpha/2 \end{pmatrix} $$

**Example**

$$ R_{k}^\alpha \dagger = \cos \frac{\alpha}{2} + i \sigma_k \sin \frac{\alpha}{2} = \exp \left( \frac{i}{2} \alpha \sigma_k \right) = R_k^{-\alpha} $$
Geometric Interpretation

- $R^\alpha_k$ rotates the Bloch vector in around the $k$-axis by angle $\alpha$

- (Hence the name „single qubit rotations“)

- Structural background is the structure of the Levi-Civita symbol

- This allows to address the question of Universality
CONTROL BY RESONANCE

- 0 and 1 = lowest two energy levels
- Resonance to drive between states
- Needs uneven frequency splitting
Two qubit gates

- Set of all unitary matrices with irrelevant global phase
  \[ SU(4) = \left\{ U \in \mathbb{C}^{4 \times 4} : UU^\dagger = \mathbb{I}, \det(U) = 1 \right\} \]

- Trivial case: Two-qubit gate are just parallel one-qubit gates, \( SU(2) \otimes SU(2) \)

- Goal: describe useful gates, then also address universality

- Examples as intermediate steps
Controlled NOT (CNOT)

- As XOR can be used for universality in classical computers, let's make a unitary extension of XOR by carrying over one input qubit, \( |x,y\rangle \mapsto |x, x \oplus y\rangle \) with \( \oplus = \text{addition modulo 2} \)

- Perfect entangler \( (|0\rangle + |1\rangle)|0\rangle \mapsto |00\rangle + |11\rangle \)

- Voilà: A reversible gate with unitary matrix

\[
U = \begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0
\end{pmatrix}
\]

- Standard interpretation: First qubit = Control, second qubit = target: Apply NOT to target if control = 1

| In1 | In2 | Carry | XOR |
|-----|-----|-------|-----|
| 0   | 0   | 0     | 0   |
| 0   | 1   | 0     | 1   |
| 1   | 0   | 1     | 1   |
| 1   | 1   | 1     | 0   |

Diagram:
- Control input
- Target output
THE PHYSICAL COST OF TWO-QUBIT GATES

• Needs an interaction between qubits to make
  \[ U = \exp(-iH_{\text{int}} \tau) \]\n  where \( H_{\text{int}} \) describes the physical interaction between qubits and \( \tau \) the interaction time

• Interaction needs to be switchable (so the computer can be programmed) and is usually weaker than local terms

• Two qubit gates are the limiting resource in time and coherence

• To count the circuit depth, we count two-qubit layers!
ERRORS AS STRUCTURING ELEMENT
INTERFERENCE

Probability amplitudes vs. probability

- Classical random process described through probabilities: \( P(x) \geq 0 \) + Rules of probability theory
- Quantum physics: Wave character, interference of amplitudes \( \Psi(x, t) \) - Probability
  \[
P = |\Psi|^2
  \]
- Quantum laws are reversible and quantum superposition not just twice the same
DECOHERENCE AND THE CLASSICAL WORLD

Not a contradiction - but a technological challenge

• Analogous to going from a Laser to a Lightbulb (=Wave optics -> Geometric optics)
• Classical Physics emerges, when interference gets wiped out:
  • Phase of large objects cannot be resolved
    \[ \lambda = \frac{h}{p} \] (Wave lengths = Planck quantum / Momentum)
  • Resolution too coarse to see the phase
    (Light: \( \lambda = 400\ldots800\text{nm} \))
  • Phase blurred by noise (thermal light)
DECOHERENCE

The central dilemma of quantum technologies

- Strict quantum physics applies to closed systems
- Real Quantum Systems are *open* - coupled to a (makroskopic) Environment
- In particular relevant for quantum technologies with a human interface
- Decoherence (quantum-classical transition) emerges
- Interpretation I: Over time, system and environment merge into a single system - too large to be quantum
- Interpretation II: The complex environment executes a random process onto the phase, hence destroying the ability to interfere
- Both are equivalent!
ANALOG CHARACTER OF QUANTUM COMPUTERS

• Quantum algorithms have analogue elements

Example
Quantum Fourier-transform

\[
CR_n = \begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & e^{2\pi i/2^n}
\end{pmatrix}
\]

• Analogue Parameters (=Strength / time of interaction) control analogue gate

• Error stays digital: Born rule

\[
P_{\text{error}} = \left| \langle \psi_{\text{correct}} | \psi_{\text{real}} \rangle \right|^2
\]
HARDWARESTATUS

Fehler, nicht Anzahl!

• Dekohärenz wird eine Herausforderung bleiben - Quantencomputer haben analoge Komponenten
• Augenblicklich: 0.1% pro harter Operation - 1000 Schritte
• Angewandte Benchmarks nutzen einen kleinen Teil großer Chips
• Erste Ergebnisse die > 50 Qubits nutzbar machen
• Planung für 1000 Qubits braucht Fehler-Roadmap
• Schlüssel: Bessere Materialien
QUANTUM ERROR CORRECTION
The challenge

- Quantum bits are subject to decoherence
- Quantum gates contain analogue parameters (e.g. C-Rot with small rotation angles in QFT)
- In contrast, classical CMOS-logic is self-correcting
- Albeit hardware will get better, it is unlikely to ever use the low error rates of classical computers
Error correction / detection: Classical

- Simple example: Checksums - calculate sums of (generalizations) of your data to catch simple bit errors

- More advanced Example: Send multiple bits and compare

- Can catch few and uncorrelated errors - checksum errors can cancel - 3-bit comparison fails if two bits flip
The challenge of catching quantum errors

- Measurement destroys superpositions!

- Cannot just read out the bit values and check on the fly

- Coherent errors are quantum in nature, e.g., they occur with quantum probabilities:

\[
U_{\text{real}} = U_{\text{err}} U_{\text{ideal}} \quad \text{e.g. with}
\]

\[
U_{\text{err}} = \cos \alpha - iX \sin \alpha
\]

- For redundant encoding: Cannot get around no-cloning theorem

- Needs care - but can be done!
Remark: The error takes us out of the code space

\[ \text{span} \left\{ |0\rangle_L, |1\rangle_L \right\} \] and adds randomness - syndrome detection removes randomness but changes codewords - correction gets us into the codewords
Stabilizer generators for the Steane code

1. Stabilizer group \( S = \langle g_1, \ldots, g_6 \rangle \)

Take the parity check matrix of the Hamming [7,4] code to encode logical qubits: 

- \( g_1 = IIIIXXX \), \( g_2 = IXXIIXX \), \( g_3 = XIXIXIX \), 
- \( g_4 = IIIZZZZ \), \( g_5 = IZZIIZZ \), \( g_6 = ZIZIZIZ \)

2. Mutually commuting (even numbers of Xs and Zs colliding), six generators for seven qubits leave one qubit subspace open

3. Codewords (instructive but technically not needed):

   \[
   |0\rangle_L = \frac{1}{\sqrt{8}} \left( |0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle + |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle \right)
   \]

   \[
   |1\rangle_L = X^{\otimes 7} |0\rangle_L
   \]
QUANTUM ERROR CORRECTION

• Quantum error correction makes clever use of redundancy and syndrome detection

• Larger codes allow to reduce the logical error $p_L$ far below the physical error $p$, provided $p < p_{\text{threshold}}$

More Qubit error longer Algorithm $=$ more Overhead

Poly(n) $\times p^n$

overhead

uncorrelated errors

Useful

Harmful
FAULT TOLERANT QUANTUM ALGORITHMS

Clear quantum advantage - long trajectory
Clear roadmap and active community
Large Overhead
Surface code: 4-Qubit-Syndrome
STATE OF THE ART

Cosmic rates and other disasters

- Impressige Demonstration by Google
  - More Overhead reduces error further
  - More round of QEC improve the error
  - Fantastic 72 qubit chip
  - Detailed error budget
  - But not break even: Error budget does not match error correction model
A SMOKING GUN

Deep underground, far away from cosmic radiation (I. Pop, KIT)

"How often have I said to you that when you have eliminated the impossible, whatever remains, however improbable, must be the truth?“

Arthur Conan Doyle, The sign of four
Beyond shor

Shor Algorithm cannot be done without error correction

NISQ-Algorithms: Short subroutines as co-processor

New BSI-Evaluation scheme

No NISQ algorithms spelled out to the state where

But they are heuristics - adds uncertainty

Did China Break The Quantum Barrier?

Most likely not
STATUS OF HARDWARE
HOW DO THEY LOOK LIKE?

A Quantum system with knobs

A chip with quantum capabilities
NOT SO DIFFERENT FROM CLASSICAL COMPUTERS

1950s

- Plurality of platforms
- Hardly visible to consumers
- Important role in infrastructure
HARDWARE-STATUS

New dynamics and variation

A  B  Qualität  C  Fehlerkorrektur  D  Fehlertolerante Operationen  E

Donatoren
Halbleiter Quantenpunkte
2D-Transmonen (supraleitende Qubits)
Ionenfallen
Farbzentren
Rydberg-Atome
Andere supraleitende Qubits
Photonen
OUTLOOK SINCE THE LAST UPDATE

- IBM multi-processor roadmap: Less relevant
- IBM error reduction roadmap: Central
- Regev-Algorithm as improvement over Shor: Extremely important
- Bosonic Codes (Alice & Bob): Strong development
- Harvard /QuEra-Result: Enormous progress in quantum error correction - moves neutral atoms to eye-level with ions and superconductors
LDPC CODES
Low density parity check

- New development - novel error correction with low overhead
- Name: Flag qubits couple to very few neighbours
- Surface code and color code are the only completely worked out LDPC codes - but not very good ones
- New IBM results reduce overhead for quantum memory

High-threshold and low-overhead fault-tolerant quantum memory

https://doi.org/10.1038/s41586-024-07107-7
Received: 25 August 2023
Accepted: 23 January 2024

Sergey Bravyi, Andrew W. Cross, Jay M. Gambetta, Dmitri Maslov, Patrick Rall & Theodore J. Yoder

![Plot diagram](https://example.com/plot.png)

**Logical error rate, $p_L$**

- $\text{Surface }[[972,12,9]]$
- $\text{Surface }[[1452,12,11]]$
- $\text{Surface }[[2028,12,13]]$
- $\text{Surface }[[2700,12,15]]$
- $\text{LDPC }[[144,12,12]]$

**Physical error rate, $p$**
Hardware-adapted error correction

• Small superconducting qubit in large Al-cavity (3D-transmon)
• In standard operation the most coherent superconducting qubit - but too big
• New twist - use EM-Field to encode quantum information (infinite dimensional space, Bosons)
• So, one 3D-Transmon replaces a large patch of surface code for phase errors
• Extrapolation: this can reach appropriately low error rates
MS + QUANTINUUM

Reached break even

- Ion trap with Carbon Code
- Enormous experimental effort with pre- and post-selection and teleportation
- Large surcharge on overhead
- But shown: No principal obstacles

Demonstration of logical qubits and repeated error correction with better-than-physical error rates

M. P. da Silva,1 C. Ryan-Anderson,2 J. M. Bello-Rivas,1 A. Chernoguzov,2 J. M. Dreiling,2 C. Foltz,2 F. Frachon,1 J. P. Gaebler,2 T. M. Gatterman,2 L. Grans-Samuelsson,1 D. Hayes,2 N. Hewitt,2 J. Johansen,2 D. Lucchetti,2 M. Mills,2 S. A. Moses,2 B. Neyenhuis,2 A. Paz,1 J. Pino,2 P. Siegfried,2 J. Strabley,2 A. Sundaram,1 D. Tom,1 S. J. Wernli,1 M. Zanner,1 R. P. Stutz,2 and K. M. Svore1

1Microsoft Azure Quantum
2Quantinuum

(Dated: April 5, 2024)
• Primary axis of analysis: Error
• Cryptoanalytic algorithms with proof of overhead and convergence need error corrections
• NISQ-algorithms do not have that - neither do they have good heuristic tests
• Quantum error correction at break even point