Quantum Cryptography

John Sipahioglu and Garrett Stallsmith

In conjunction with Dr. Younghun Chae

Abstract

The aim of this research is to provide its viewer a look into what quantum computers are, how they defeat modern cryptosystems, and what the future of cryptography may look like in the quantum age.

Classical Cryptographic Systems

We will use the traditional names Alice, Bob, and Eve for the actors throughout. Much of internet security lies in the Diffie-Hellman Key Exchange and the RSA algorithm.

These algorithms currently use the exponential time complexity of solving Discrete Logarithms in the case of Diffie-Hellman, or factoring products of large primes in the case of RSA[1].

Quantum algorithms, particularly Shor's Algorithm, can provide an exponential speed-up [2].

Quantum Computing

Normal computers operate with bits, 0 and 1. An n-bit processor can have 2n states at a time, from 00…0 to 11…1. A quantum bit, called a qubit, can also have two states, |0> and |1>.

Through a type of superposition called entanglement, quantum bits can take exponentially many states at once from |00…0> to |11…1>.

There are two counterintuitive properties of quantum physics to be considered:

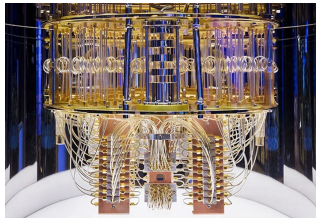
1. A system in a definite state can still behave randomly
2. Two systems that are too far apart to influence each other can behave in ways that, while individually random, are somehow strongly correlated

Quantum Decoherence is the phenomenon that occurs when the state of a quantum system breaks down due to outside noise and heat.

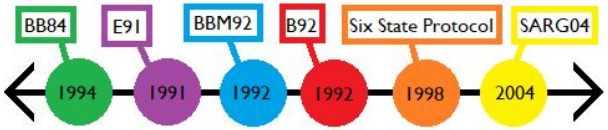
Currently, quantum processors must be cooled to near absolute zero temperatures and kept as isolated as possible from outside conditions. Additionally, quantum computers use materials such as Helium-3 which are not easily available

Figure1: IBM Quantum Computer at Cleveland Clinic. Source [5]

Figure2: IBM Quantum One Computer internals at Cleveland Clinic. Source [5]



Timeline of Quantum Key Distributions



Quantum Fourier Transform

In its simplest terms, the QFT is a change of basis from the Computational Basis to the Fourier Basis. The simplest QFT is the H-Gate applied to a single qubit. For n qubits, we have 2n = N basis states. The quantum state as a tensor product:

$$|x\rangle = |x_1 x_2 x_3 \dots x_{n-1} x_n\rangle = |x_1\rangle \otimes |x_2\rangle \otimes |x_3\rangle \otimes \cdots \otimes |x_{n-1}\rangle \otimes |x_n\rangle$$

From here we can derive the general QFT: $QFT|x\rangle = |\tilde{x}\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{\frac{2\pi i x y}{N}} |y\rangle =$

$$\frac{1}{\sqrt{N}} \left(|0\rangle + e^{\frac{2\pi i x}{2}}|1\rangle\right) \otimes \left(|0\rangle + e^{\frac{2\pi i x}{2^2}}|1\rangle\right) \otimes \left(|0\rangle + e^{\frac{2\pi i x}{2^3}}|1\rangle\right) \otimes \cdots \otimes \left(|0\rangle + e^{\frac{2\pi i x}{2^n}}|1\rangle\right)$$

From here we can design a circuit to implement this, using H-Gates and Unitary-Rotation Gates ($UROT_k$) with a controller on the $UROT_k$.

$$UROT_k|x\rangle = e^{\frac{2\pi i x_j}{2^k}}|x_j\rangle = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{bmatrix}$$

We can now build the quantum circuit to implement this[2].

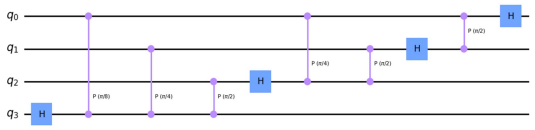


Figure3: Quantum circuit diagram to Implement QFT made using Qiskit Python API

Conclusion

While we are likely some time away from a true "quantum age" in computing, it is still important to always consider future risks and prepare for them. Technology will continue to advance, and it is necessary to understand these new technologies now before they are fully realized.

Future research should be done in the areas of improving quantum technology to make it more affordable and accessible, exploring weaknesses of QKDs, and continued development of Quantum Resistant algorithms for communication over a classical channel.

Symmetric Bernstein-Vazirani

Alice sends Bob a binary number x, and Bob applies a function fs(x) that maps to {0,1}, based on Bob's secret number s, and sends the result to Alice.

By sending numbers 100…0, 010…0, …, 000…1, Alice can recover s in n steps, which is the best case.

The Quantum Bernstein-Vazirani algorithm can solve this in one step. Now we will display an algorithm that uses this idea for a QKD.

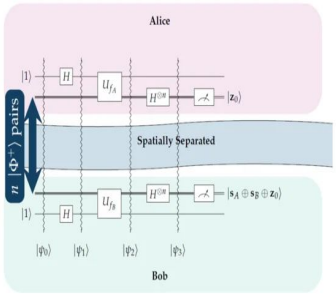
Both start with all bits in entangled state

Actions by Alice:

- Output register is set to |1>
- Apply H gate to output register
- Apply tentative key sA
- Apply H-Gate to input register
- Measure input register to get random binary string z0
- Receive Bob's tentative key sB
- Compute key $sA \oplus sB \oplus z0$

Actions by Bob:

- First 5 steps are the same (except using sB)
- Measure input register to find the key $sA \oplus sB \oplus z0$
- Share tentative key sB with Alice [7]



Attacks

Intercept and Resend

- Due to the No-Cloning Theorem and Wave-Collapse Function, qubits cannot be measured without the state being changed
- Eve must measure the intercepted qubit, then prepare a qubit in that state to pass to Bob
- Probability of detection is very high even with small key sizes [7]

Man-In-The-Middle (MITM)

- If Alice and Bob do not authenticate each other prior to transmission, Eve may tell Alice she is Bob and tell Bob that she is Alice
- In this case Eve is free to eavesdrop and manipulate information
- Authentication can be done through a secure classical channel, third-party, or by using Chaos Theory [7]

Other Attacks

- Photon-Number-Splitting (PNS)
- Trojan Horse
- Laser Pulse
- Denial of Service (DoS)

References

[1] M. Weismann, An Illustrated Theory of Numbers, 1st Edition, Providence, Rhode Island, American Mathematical Society, 2017
[2] A. Asfaw. (2020). Shor's Algorithm I: Understanding Quantum Fourier Transform, Quantum Phase Estimation. Available: https://learn.qiskit.org/summer-school/2020/shors-algorithm-i-fourier-transform-phase-estimation
[3] C. Bennett et. All, "Learn quantum computing: a field guide", IBM Quantum, https://quantum-computing.ibm.com/composer/docs/iqx/guide/, (accessed Jan 2022)
[4] J. Ledin, Modern Computer Architecture and Organization, 2nd Edition, Birmingham, Packt Publishing, 2022
[5] Cleveland Clinic, Discovery Accelerator, ClevelandClinic.org. https://ieeeauthorcenter.ieee.org/wp-content/uploads/IEEE-Reference-Guide.pdf (accessed Mar. 21, 2023)
[6] A. Kumar, S. Garhwal. "State-pf-the-Art Survey of Quantum Cryptography." Arch. Of Comp. Methods in Eng. Vol. 28. pp. 3831-3868. Aug 2021. doi: https://doi.org/10.1007/s11831-021-09561-2
[7] M. Ampatzis and T. Andronikos, "QKD Based on Symmetric Entangled Bernstein-Vazirani", Entropy, vol. 23, no. 7, pp. 870-886, July 2021 doi: 10.3390/e23070870
[8] Y. Chae, D. Mathews. "Quantum Cryptography"