Jesse Mayer
Dr. Sukanya Manna
CSCI-10
21 February 2017

# Encryption & Quantum Computers

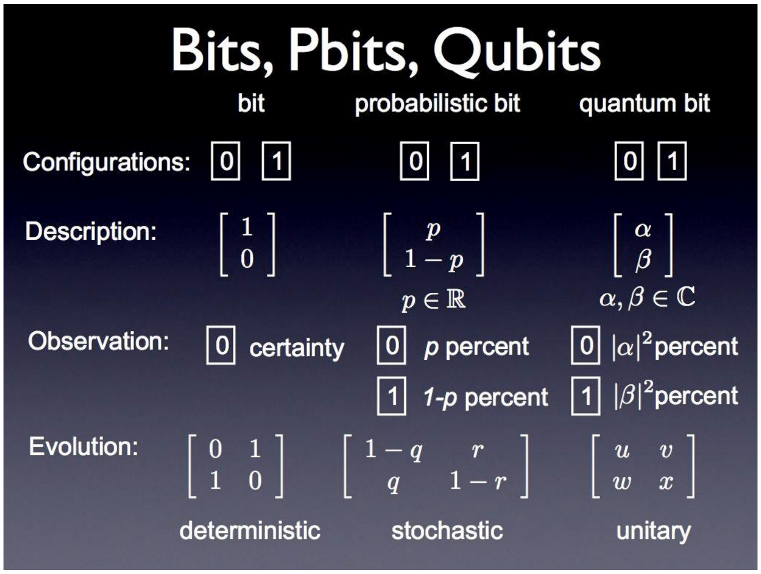
## Section 1: Introduction

Data encryption is the method of securing data so that it remains private. In this process data is encrypted through an encryption algorithm with an encryption key. The way this works is that the algorithm scrambles the information making it unreadable without the key. The goal is therefore to keep the key private so that only those allowed access can decipher the code using the key and makes it normal again. Despite requiring more resources for computation longer keys have a positive relationship with the security of the encryption. The primary way to break through encryptions is to try random keys until the right one is found, but the amount of time needed to discover the key randomly can make this unfeasible.

However, the advancement of quantum computers change this entire system. The most noticeable benefit of quantum computers is that they enable an exponential increase in computational power over today's computers. The problem with this is that our encryption methods are based on massively complex mathematical problems which were previously too complex to solve but now are becoming increasingly more attainable through the development of super-fast quantum computing.

## Section 2: Concept Description

Conventional computers store information using binary bits of 1's and 0's, while quantum computers store information through quantum bits called "qubits". The revolutionary thing about quantum computing is that quibits can simultaneously be a 1 and a 0 due to the phenomena of superposition. This enables quantum computers to be immensely more powerful than current computer systems and thus capable of completing extremely complex mathematical calculations that currently surpass our computational capabilities.



Bits, Pbits, Qubits

| | bit | probabilistic bit | quantum bit |
|---|---|---|---|
| Configurations: | $\boxed{0}$ $\boxed{1}$ | $\boxed{0}$ $\boxed{1}$ | $\boxed{0}$ $\boxed{1}$ |
| Description: | $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ | $\begin{bmatrix} p \\ 1-p \end{bmatrix}$<br>$p \in \mathbb{R}$ | $\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$<br>$\alpha, \beta \in \mathbb{C}$ |
| Observation: | $\boxed{0}$ certainty | $\boxed{0}$ $p$ percent<br>$\boxed{1}$ *1-p* percent | $\boxed{0}$ $\lvert\alpha\rvert^2$percent<br>$\boxed{1}$ $\lvert\beta\rvert^2$percent |
| Evolution: | $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ | $\begin{bmatrix} 1-q & r \\ q & 1-r \end{bmatrix}$ | $\begin{bmatrix} u & v \\ w & x \end{bmatrix}$ |
| | deterministic | stochastic | unitary |

## Section 3: Analysis

The proliferation of quantum computers will make most forms of encryption obsolete in the near future. As a result, currently secure data will inevitably soon be at risk of being decrypted through quantum computers. The prohibitive cost of quantum computers will make it so that initially they will be primarily operated by governments and corporations, thus meaning that quantum computers will not create a level playing field when they first start to roll out. Because of this trend, personal and corporate data will likely be at the mercy of government probing and corporate espionage for a time.

However, despite the dangers quantum computers pose to data security they will also enable significant advances in computational power. This heightened computation power will promote significant advancements in artificial intelligence, our understanding of human biology, and the development of advanced material sciences.

## Section 4: Discussion/Conclusion

Therefore quantum computers will fundamentally change our technological world forever in many ways, enabling new possibilities while also threatening current data security measures. As quantum computers continue to develop and get closer to being deployed, we must seek new security methods that are not susceptible to the nature of quantum computers. This would require the discovery of new ways of creating public keys for encryption that are quantum computer resistant, which fortunately is something already being worked on. Last year the NSA called out for a shift to quantum-resistant encryption but this is just the first step. What comes next will have to be standardization and widespread implementation of new quantum proof encryption methods. Fortunately we have awhile to develop these technologies, as quantum computers are another 15 or so years away, thus giving the industry a fair amount of time to prepare for these drastic changes. The answer therefore is to start research on new encryption methods now so that they will be perfected by the time quantum computers finally do arrive.

# Bibliography

Gent, Edd. "Quantum Computers Could Crush Today's Top Encryption in 15 Years."*Singularity Hub*. N.p., 12 Dec. 2016. Web. 21 Feb. 2017.

Kobie, Nicole. "The Quantum Clock Is Ticking on Encryption – and Your Data Is under Threat." *WIRED UK*. WIRED UK, 18 Oct. 2016. Web. 21 Feb. 2017.

Lord, Nate. "What Is Data Encryption?" *Digital Guardian*. N.p., 27 Jan. 2017. Web. 21 Feb. 2017.

Satell, Greg. "Here's How Quantum Computing Will Change The World." *Forbes*. Forbes Magazine, 12 Oct. 2016. Web. 21 Feb. 2017.