INFORMATIVE REPORT

ASC X9 IR 01–2019

Quantum Computing Risks to the Financial Services Industry

By the ASC X9 Quantum Computing Risk Study Group

An Informative Report approved and released by:
Accredited Standards Committee X9, Incorporated

Date Released: February 14, 2019
First edition

Table of Contents

Page

Foreword

This Informative Report has been approved and released by the Accredited Standards Committee X9, Incorporated, 275 West Street, Suite 107, Annapolis, MD 21401. This document is copyrighted by X9 and is not an American National Standard and the material contained herein is not normative in nature. Comments on the content of this document should be sent to: Attn: Executive Director, Accredited Standards Committee X9, Inc., 275 West Street, Suite 107, Annapolis, MD 21401,

This Informative Report is a product of the Accredited Standards Committee X9 Financial Industry Standards and was generated by the Quantum Computing Risk Study Group created by the X9 Board of Directors in December of 2017 to research the state of quantum computing and to generate a report summarizing the findings of the group.

Suggestions for the improvement or revision of this report are welcome. They should be sent to the X9 Committee Secretariat, Accredited Standards Committee X9, Inc., Financial Industry Standards, 275 West Street, Suite 107, Annapolis, MD 21401 USA.

Published by

Accredited Standards Committee X9, Incorporated
Financial Industry Standards
275 West Street, Suite 107
Annapolis, MD 21401 USA
X9 Online http://www.x9.org

X9 Board of Directors:

At the time this Informative Report was published, the ASC X9 Board of Directors had the following member companies and company representatives and X9 had the following staff:

Roy C. DeCicco, X9 Board Chairperson
Angela Hendershott, X9 Board Vice Chairperson
Steve Stevens, X9 Executive Director
Janet Busch, X9 Senior Program Manager
Ambria Frazier, X9 Program Manager

Organization Represented on the X9 Board	*Representative*
ACI Worldwide	Doug Grote
Amazon	John Britton
American Bankers Association	Diane Poole
American Express Company	David Moore
Bank of America	Daniel Welch
BDO	Jeffrey Ward
Bloomberg LP	Corby Dear
Capital One	Marie LaQuerre
Citigroup, Inc.	Karla McKenna
Conexxus, Inc.	Gray Taylor
CUSIP Global Services	Gerard Faulkner
Delap LLP	Andrea Beatty
Deluxe Corporation	Angela Hendershott
Diebold Nixdorf	Bruce Chapa
Dover Fueling Solutions	Henry Fieglein
eCurrency	David Wen
Federal Reserve Bank	Mary Hughes
First Data Corporation	Lisa Curry
FIS	Stephen Gibson-Saxty
Fiserv	Dan Otten
FIX Protocol Ltd - FPL	James Northey
Futurex	Ryan Smith
Gilbarco	Bruce Welch
Harland Clarke	John McCleary
Hyosung TNS Inc.	Joe Militello
IBM Corporation	Todd Arnold
ISARA Corporation	Alexander Truskovsky
ISITC	Lisa Iagatta
ITS, Inc. (SHAZAM Networks)	Manish Nathwani
J.P. Morgan Chase	Roy DeCicco
MagTek, Inc.	Mimi Hart
MasterCard Europe Sprl	Mark Kamers
NACHA The Electronic Payments Association	George Throckmorton
National Security Agency	Mike Boyle
NCR Corporation	Kevin Spengler
Office of Financial Research, U.S. Treasury Department	Thomas Brown Jr.
PCI Security Standards Council	Troy Leach
RouteOne	Chris Irving
SWIFT/Pan Americas	Karin DeRidder
Symcor Inc.	Debbi Fitzpatrick
TECSEC Incorporated	Ed Scheidt
The Clearing House	Sharon Jablon
U.S. Bank	Michelle Wright
U.S. Commodity Futures Trading Commission (CFTC)	Robert Stowsky

USDA Food and Nutrition Service	Lisa Gifaldi
VeriFone, Inc.	Dave Faoro
Viewpointe	Richard Luchak
VISA	Kim Wagner
Wells Fargo Bank	Mark Schaffer

X9 Study Group:

At the time this informative report was published, the X9F Quantum Computing Risk Study Group had the following officers and members:

Steve Stevens, Chairperson
Tim Hollebeek, Vice Chairperson
John Barrowman, Editor

Organization Represented	*Representative*
American Express Company	Gail Chapman
American Express Company	David Moore
BlackBerry Limited	Daniel Brown
Capital One	Johnny Lee
Capital One	Dustin Rogers
Cisco	Scott Fluhrer
Conexxus, Inc.	David Ezell
Delap LLP	Andrea Beatty
Delap LLP	Spencer Giles
Digicert	Tim Hollebeek
Digicert	Steve Medin
Envieta	Roberta Faux
Envieta	Rino Sanchez
Federal Reserve Bank	Ray Green
Federal Reserve Bank	Pinkaj Klokkenga
Federal Reserve Bank	Francois Leclerc
Federal Reserve Bank	Daniel Littman
First Data Corporation	Lisa Curry
First Data Corporation	Vinayak Desai
First Data Corporation	Prince Duodu
First Data Corporation	Timothy Horton
FIX Protocol Ltd - FPL	James Northey
Gilbarco	Bruce Welch
IBM Corporation	Todd Arnold
IBM Corporation	Richard Kisley
IBM Corporation	Michael Osborne
ISARA Corporation	Mike Brown
ISARA Corporation	Philip Lafrance
ISARA Corporation	Alexander Truskovsky
J.P. Morgan Chase	Jackie Pagán
Level 10	Allan Elder
Member Emeritus	Bill Poletti
Member Emeritus	Richard Sweeney
National Institute of Standards and Technology (NIST)	Carl Miller
National Security Agency	Mike Boyle
National Security Agency	Austin Calder
Office of Financial Research, U.S. Treasury Department	Jennifer Bond-Caswell

PCI Security Standards Council	John Markh
PCI Security Standards Council	Ralph Poore
RSA, The Security Division of EMC	Steve Schmalz
SafeNet Infotech Pvt. Ltd.	Amit Sinha
TECSEC Incorporated	Ed Scheidt
TECSEC Incorporated	Jay Wack
Thales UK Limited	Larry Hines
TokenEx	Ulf Mattsson
University of Maryland	Jonathan Katz
University of Waterloo	Chin Lee
University of Waterloo	Michele Mosca
VeriFone, Inc.	John Barrowman
VeriFone, Inc.	Joachim Vance
VISA	Eric Le Saint
VISA	Johan ("Hans") Van Tilburg
VISA	Kim Wagner
Wells Fargo Bank	Allen Ausec
Wells Fargo Bank	Peter Bordow
Wells Fargo Bank	Robert Carter
Wells Fargo Bank	David Cooper
Wells Fargo Bank	Phillip Griffin
Wells Fargo Bank	Jeff Stapleton
Whitebox Advisors	Kerry Manaster

ASC X9 IR-01-2019
Quantum Computing Risks to the Financial Services Industry
Informative Report

1. Introduction

It is fascinating to think about the power in our pockets—today's smartphone has the computing power of a military computer from 50 years ago whose size filled an entire room. As the size of the switching elements used within computers, known as transistors, has shrunk to nearly that of an atom, the overall capacity and capability of the computer has grown unimaginably, and has changed the world.

Now there is a new switching element on the block called the qubit. Born out of the strange world of quantum physics, the qubit possesses traits and abilities that both defy logic and inspire the imagination. In fact, the startling abilities of the qubit have spawned an entirely new way of thinking about computers and their capabilities. It appears that quantum computers will eventually be able to solve some of the mathematical problems previously thought to be unsolvable.

The advent of the quantum computer evokes consternation in the secure payment industry since most encryption in practice today is based on unsolvable mathematic problems. This paper was written to inform the stakeholders in the greater secure payment industry about the issues associated with the advent of the quantum computing age.

1.1. Classical vs Quantum Computing

Even though classical computers can do many amazing things, they are really just calculators executing prewritten instructions based on binary bits (i.e. bits that can equal 0 or 1). One significant trait of a classical computer is that all functionality could be performed by a person, albeit much more slowly. Quantum computers differ in this regard, for they can perform functions that are well beyond human ability. In fact, today's largest classical computers can only simulate very simple quantum computers.

Quantum computers are not intended to and will ***not*** replace classical computers. They are expected to be a different tool we will use to solve specific types of complex problems that are beyond the capabilities of classical computers. For the most part, classical computers are limited to doing one thing at a time, so the more complex the problem, the longer it takes. A problem estimated to require more power and memory than today's computers can accommodate and that have a computational time that is estimated to take years is called an intractable problem. Intractable problems are the foundation of many of the cryptographic algorithms the financial industry relies upon to keep data safe. The very fact that they are intractable is what allows them to keep data secure. Unfortunately, some of these are the same types of problems that quantum computers can solve relatively easily. Predictions vary, but some intractable problems that could take a classical computer thousands to even millions of years could be solved by a quantum computer in seconds.

Quantum computing takes advantage of the strange phenomena of subatomic particles to exist in more than one state at any time and to be entangled with other particles. Einstein used the adjective "Spooky" to describe

> the actions of these particles. Due to the way these tiniest of particles behave, one quantum operation can modify the state of many qubits simultaneously. Harnessing the unusual phenomena of subatomic particles

allows a quantum computer to solve some problems much more quickly and use less energy than classical computers.

Instead of using bits to store and process data as does a classical computer, a quantum computer uses quantum bits—known as qubits. To illustrate the difference, imagine a sphere as shown in Figure 1. A classical computer bit can only be at either of the two poles of the z-axis, that is a bit can be a "0" or a "1". However, a qubit can exist at any point on the surface of the sphere. Using a quantum phenomenon called superposition, a qubit can also simultaneously represent any point on the surface of the sphere. So, this means that a computer using qubits can store an enormous amount of information and uses less energy doing so than a classical computer. In the era of quantum computing, we will be able to create processors that are significantly faster at certain tasks (a million or more times) than what we use today.

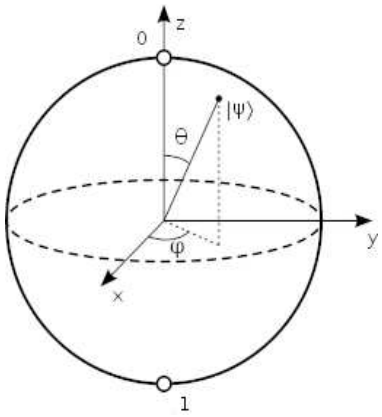


Figure 1 – A Bloch Sphere Showing Values for Classical Bits (0, 1)

It is difficult to predict how quantum computing will change our world. We are venturing into an entirely new realm of computation, and there will be new applications that we cannot possibly foresee at this time. Considering how classical computers revolutionized our world in a very short period of time using only binary bits, you can imagine the extraordinary capabilities possible when we utilize the processing power of qubits. The unsolvable becomes solvable.

The following is just one example of the potential power of a quantum computer. Cryptography based on RSA technology is common and used to secure data moving across the Internet. Unique keys are used when an Internet browser connects to a secure server. The keys can have different lengths and keys of length 2048 bits are among the longest and most secure keys in use today. It is so secure that a classical computer is estimated to take 6 quadrillion years to break a 2048-bit key encryption code. However, some researcher estimated a large quantum computer with approximately 4000 logical qubits could break the code in minutes.[1]

1.2. Overview

This document provides a basic background on quantum computers and the risk they are expected to pose to cryptography—specifically the cryptography used by the financial industry. The quantum computing landscape is currently undergoing an increasing rate of change as more research and money is dedicated to its development. In just the last 12 months, over $20 billion (world-wide) in funding for additional quantum

[1] Digicert, "The Math Behind Estimations to Break a 2048-bit Certificate", https://www.digicert.com/TimeTravel/math.htm

computing research has been announced. X9 is committed to tracking the ongoing evolution in quantum computing and will periodically revise this document. X9 also maintains a quantum computing risk web page on its public web site that tracks major developments and has links to relevant documents from other sites. Please contact X9 staff if you have information you would like referenced on this page.

This document provides information tailored towards management and technical people. The High-Level Review provides a shorter and less technical description of quantum computing, what it can and cannot do, and the expected risks that it poses. While it is not possible to avoid all discussions of technical issues, the review is written for people with a non-technical background. The remaining sections of this document provide a much more in-depth description and background of the software and hardware that make up a quantum computer. This includes a discussion of the algorithms specifically written for quantum computers to crack cryptographic systems. This section also discusses some of the hurdles that must still be overcome to create a general purpose, fault tolerant, large scale quantum computer. The last section covers recommendations for steps that can be taken now to defend against such a computer and a discussion on the steps that may be required in the future.

1.3. Purpose

The purpose of this report is:

- To provide basic information about quantum computers and how they function
- To identify how quantum computers will attack cryptography
- To provide a snap shot of the current state of quantum computing
- To inform financial services management of the risks posed by quantum computers
- To provide guidance for mitigating this risk, despite the uncertainty
- To identify next steps for X9 to address the risks

1.4. Scope

This report will provide:

- A description of how quantum computers work, and the different architectures being experimented with today
- A description of the technological hurdles remaining that are thwarting advancement to a large-scale quantum computer
- A list of the major companies, agencies and states participating in the race to create a stable, large scale, general purpose quantum computer
- An estimate of when a large scale, general purpose quantum computer (QC) will be operational
- Methods a quantum computer could use to break encryption, and how these attacks will specifically affect the different cryptographic methods used today
- Updates on the work being done by NIST to identify post-quantum algorithms
- Guidance for financial services organizations to mitigate quantum computing risk
- Steps that X9, as a standards body, needs to take over the next few years to prepare for the post-quantum world

2. Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

2.1 NIST NISTIR 8105, "Report on Post-Quantum Cryptography", published April 2016, http://dx.doi.org/10.6028/NIST.IR.8105

3. Management Level Review of Quantum Computing and Its Risks

This section provides a high-level management review of quantum computing. A minimum amount of math and science is used in its review. A more detailed review follows this section, and a conclusion section is provided at the end of the paper.

3.1. Classical vs Quantum Computers

Most classical computers in use today are digital computers that perform basic functions like adding, subtracting and comparing numbers. A classical computer performs functions that could be performed by a person, just much faster. A classical computer uses bits to store and process data. A bit can store either a one or zero. In the early days of classical computers, vacuum tubes were used to construct storage elements that would store bits. Those systems sometimes broke down after less than one hour of operation. Later, very small iron donut cores were used to store bit information. The cores would be magnetized to store either a one or a zero. Today, transistors created on silicon substrates are used to store and process bit data. Each subsequent technology has increased the speed, density, and reliability of classical computers and their storage and processing power. While classical computers are used to control just about everything, we have today that is computerized, there are a number of problems that classical computers either cannot solve or are extremely inefficient at solving. (E.g. Solving some of these problems would take longer than the lifetime of the universe.)

A quantum computer uses specific physical phenomena of quantum mechanics to perform certain mathematical operations far more efficiently that a classical computer—in some cases, exponentially faster. The phenomena are a natural byproduct of the behavior of matter at the subatomic level. Harnessing the interactions of subatomic particles allows a quantum computer to process data in a completely different way than a classical computer. Unlike classical computers, the quantum processes cannot be performed mentally by a person. As such, classical computers have limited ability to simulate quantum computers. The largest classical computer can only simulate a 40-qubit quantum computer.

A quantum computer uses a quantum bit or qubit to store and process data. A qubit employs two quantum phenomena called superposition and entanglement. Like a classical bit, a qubit can store either a one or zero, but by using superposition it can store a one or zero or any value in between all at the same time. Entanglement allows one qubit to be in a state which depends on the state of one or more other qubits. For a computer to be true quantum computer, the qubits must use both quantum characteristics.

In a classical computer that uses N bits to store and process a number, adding one additional bit (for a total of N+1) simply doubles the size of the largest number that can be stored and processed. The extra bit does not increase the processing power of the computer. In a quantum computer that harnesses quantum phenomena, adding a qubit not only doubles the processing power of the computer, but also doubles the number of states it can process.

The quantum phenomena used by a quantum computer yield exponential speedups in problem solving but only for a relatively small group of problems. These problems are found, for example, in the areas of physics simulation, number theory, and topology. Very important to the goals of this document is the fact that some

types of cryptographic problems fall into this same group of problems as well. Other groups of problems executed on quantum computers experience only modest speed gain, while others may experience no performance improvement at all.

3.2. Logical Functions

In classical computers, a program comprised of a series of computer instructions or commands is executed by the computer, causing the computer to perform the requested functions (e.g., adding, subtracting, comparing, or shifting the bits of numbers). Classical computers execute commands serially. These commands are combined to create high-level functions that can control, for example, cell phones or implement applications such as word processors or databases.

A quantum computation can be thought of as a series of gates that process and transform quantum-based information stored in qubits. In contrast to the likes of a classical computer program, a quantum algorithm resembles an electrical circuit diagram, and this algorithm enables the quantum computer to process qubit data in parallel. This explains why adding one qubit to a quantum computer doubles its processing power rather than just doubling the size of a number that can be stored, as in a classical computer. Some common types of quantum logic gates are: Hadamard, Pauli, Swap, and Toffoli. It should be noted that unlike most logic gates in classical computers, quantum logic gates are reversible. Moreover, since qubits can become entangled with each other in complicated ways, performing an operation on two or three qubits may also change the state of a large number of other qubits.

When a qubit is in superposition it can store all possible values, so the quantum program that is acting on that qubit is not just acting on a single value, but all possible values at the same time. A classical computer must examine every possible value one at a time, but a quantum computer can act on all possible values simultaneously. Therefore, quantum computers can execute instructions faster and be far more powerful than classical computers.

However, it is important to note that when a measurement is made, only one of the many possible values is returned. This means that it is not possible to read out the complete state of a qubit, nor can a qubit be copied. This is what prevents quantum computing from being a practical means of doing parallel computation for every math problem. However, certain clever algorithms, like Grover's Algorithm and Shor's Algorithm can carefully manipulate quantum states in such a way that the information returned by a measurement is information that would take much longer, or even would be impractical to find, using a classical computer.

3.3. Types of Qubits

Quantum computing is based on harnessing certain characteristics of subatomic particles to process data. Therefore, for a qubit to harness these characteristics, it must to be based on the direct behavior of a subatomic particle. There are many types of subatomic particles that can be used as building blocks for qubits. For example, a photon of light, an electron, and an atom all exhibit a quantum characteristic called spin which can be harnessed to make a qubit. There are a number of different technologies used to harness the different particles. (A detailed description of the major technologies is listed below.)

Most current technologies require the hardware to operate at just a few thousandths of a degree above absolute zero. This is necessary to reduce interaction between the subatomic particle that makes up the qubit and its surrounding environment. Such interactions cause errors in the qubits. The goal is to isolate the particle to assure that any transformation of the subatomic particle (qubit data) is due to the quantum program acting on the qubit and not due to influences from the surrounding environment. Ergo, the topic of error correction (or a fault-tolerance) is extremely important in quantum computing.

The ability of a quantum computer to solve worthwhile problems depends on its effective size. As of 2018, quantum computers were based on a variety of technologies, and all of these technologies are hobbled with issues of scalability. The state-of-the-art technology present in 2018 has yielded computers with fewer than 100 qubits. To achieve a 1,000-qubit computer, the technologies have to scale by factors of 10 or more. Some technologies are better at scaling than others, but none so far can easily scale to the large number of qubits that are presently sought by researchers.

3.4. What Problems are Quantum Computers Best Suited to Solve and Why

Quantum computers exploit certain characteristics of quantum mechanics to solve specific problems like factoring large integers or solving massive matrix-based math problems far faster than classical computers can. In some cases, a quantum computer can solve a problem a billion times faster than a classical computer. Nature-based systems (or natural systems) are, at their core, based on quantum mechanics. It stands to reason that such natural systems provide the types of problems that quantum computers may be best adapted to solve.

One example of a natural system is the simulation of how a molecule (a drug) will interact in the human body. The largest molecule that a classical computer can simulate has fewer than 10 atoms. For comparison, the human DNA has approximately 204 billion atoms.

Weather prediction is another area that a quantum computer should be able to improve. Weather prediction involves solving a huge number of differential equations simultaneously. Because classical computers are ill-suited to solve these types of systems, the equations are simplified to reduce the number of operations that must be resolved. This speeds up the time required for calculation but, also reduces the accuracy of the results. In contrast, quantum computers are well-suited for this type of problem. Eventually they will be able to handle the un-simplified differential equations and yield more accurate weather predictions much more efficiently than classical computers.

Cryptography is based on one-way functions. A one-way function can be solved easily in one direction but is nearly impossible to solve in the reverse direction. Depending on the one-way function, classical computers spend weeks, years, or even eons trying to solve cryptographic functions in reverse. In the absence of quantum technology, any data encrypted will be safe for the time it takes to solve the problem in reverse. Unfortunately, quantum computers are much better equipped to solve some of the cryptographic functions than are classical computers.

A quantum computer could be a billion times faster than a classical computer at solving some problems. In particular, quantum computers can break certain cryptographic systems in a fraction of the time it would take a classical computer. The cryptographic systems most at risk from attack by a quantum computer are those based on asymmetric technology. This type of technology is used extensively on the Internet for example in key exchange. Symmetric based encryption, such as AES, is not immune from attack but experts believe the protection time of these system can be preserved by doubling the length of the key. For example, a 256-bit symmetric key will have at least as much security against a Quantum Computer as a 128-bit symmetric key has against a classical computer, and is hence believed to be intractable to attack. In contrast, an asymmetric based system may be vulnerable to an attack by a quantum computer.

3.5. Logical Qubits vs Physical Qubits

All of today's quantum computers use only physical qubits. Physical qubits, essentially, store and operate on data. By their very nature, qubits are fragile and highly susceptible to environmental influences that introduce errors. To reduce these influences, most qubit hardware operates at a fraction of a degree above absolute zero, which increases the operating cost and complexity and negatively affects scalability. Research is being conducted to create more stable qubits with longer coherence times and to create better error correction technology.

One solution is to group multiple physical qubits in a way that creates a single logical qubit. Logical qubits will have better error correction, longer coherent times, and will be able to be entangled with other logical qubits. Logical qubits can be arranged to form quantum algorithms that will solve problems. A working logical qubit is currently the goal of researchers but has not yet been achieved (or at least has not been published).

3.6. Four Major Issues with Creating a Large Stable Quantum Computer

Coherence

Coherence (as in coherent operation) is the amount of time a qubit can operate without external influences corrupting its data. The externally induced errors occur when a qubit interacts with its surrounding environment. The source of these interactions can be thermal or electromagnetic or a combination of the two. Long duration coherent operation is the goal of research. Most quantum computers today operate coherently for a second or less. Although, there are a number of problems that can be solved in less than a second, a quantum computer must be able to operate coherently for hours or days in order to achieve its full potential. Solving the coherence problem is a major hurdle and one that is receiving a large portion of the research dollars.

Gate Fidelity

A quantum gate is a circuit that operates on one or more qubits. The quantum gates in use today are imperfect in that they may not exactly realize the intended implementation. This introduces additional errors every time a gate operation is performed, on top of the errors introduced by decoherence.

Error correction

One method of extending the coherent operation of a quantum computer uses technology that corrects both environmentally induced errors and errors introduced during gate operation in a qubit. There is significant research in this area.

Scaling

To achieve a general-purpose fault-tolerant large-scale quantum computer, experts believe such a system will need one to two thousand stable qubits. Some solutions that use physical qubits would need 10,000 or more qubits to reach this goal. Today's quantum computers have 50 to 70 qubits so major scaling must take place before a system with the required number of qubits can be created. Not all technologies used to manufacture qubits are scalable to this level and none have been proven to scale to this level. The qubit technology that is needed may not even be in use today. This is a significant hurdle that must be overcome.

3.7. What Size Quantum Computer Will Pose a Risk to Current Cryptographic Systems

The possibility of performing mathematical computations using quantum phenomena was first postulated in the 1950s, and technology to create a quantum computer based on these phenomena has been under development for over 40 years. In 1994 Peter Shor, a mathematician working for Bell Labs, developed a quantum algorithm for integer factorization. Word quickly spread that a quantum computer executing this algorithm could compromise asymmetric cryptographic systems. Shortly after this revelation, research to develop a working quantum computer surged. Four years later in 1998, the first working 2-qubit quantum computer was demonstrated. By late 2017, the largest known working quantum computer had 50 qubits. Recently, the number of qubits in a quantum computer has been increasing at about 35% per year. At that rate, a 300-qubit quantum computer could be achieved in 5 to 6 years. A 300-qubit quantum computer can process numbers as large as 2^{300}. For comparison, it is estimated that there are only 2^{266} atoms in the entire known universe.

Some cryptographic systems use keys with a length of 2048 bits. That is 2^{2048} possible keys, which is far more than the number of atoms in the universe. These large keys are used to avoid certain attacks with a classical computer. However, because elliptic curve cryptography uses smaller key sizes which speeds processing, it could be more vulnerable to quantum computer-based attacks.

It is tempting to view qubit counts for existing quantum computers as a useful metric for tracking the progress of quantum computing. For some problems that quantum computing can potentially solve, it is a very important metric. However, it is only part of the picture. Temporarily restricting our scope to a quantum

computer that can threaten RSA or ECC via Shor's Algorithm, there are a number of obstacles that must simultaneously be overcome:

1. The quantum computer must have at least twice as many logical qubits as the key has bits
2. The stability of the qubits must be long enough that the computer gets the right answer with non-negligible probability
3. The gate fidelity must be high enough that gate errors do not overwhelm the correct answer
4. The total number of physical qubits and related infrastructure necessary to achieve all three of the above simultaneously must be feasible to construct and operate (for example, it cannot require terawatts of power, or produce enough waste heat to make it impossible to keep cool)

Exactly how many physical qubits this will take depends on how much error correction is needed to overcome the errors. This is why it is not possible to name the exact number of physical qubits required to threaten RSA and ECC at this time.

If a 300-qubit quantum computer is at least 5 years away, a 2000 qubit computer would be 10 to 15 years away. These estimates are based on quantum computers that use physical qubits only, and assumes that a scaling projections similar to Moore's Law will emerge over time. Currently, there are too few data points over too short a time period to reliably assess whether this expectation will occur, or what the qubit doubling time really is. Current types of quantum computers based on physical qubit would still exhibit stability issues that would limit the time they could operate error free. However, a 2000 qubit quantum computer would still pose a significant risk to cryptographic systems if the qubits and quantum gates are sufficiently stable. Otherwise, systems based on logical qubits will probably require 10,000 or more physical qubits because it will require multiple physical qubits to create each logic qubit.

There is a risk that the technology used to develop quantum computers will be similar to or derived from existing technologies used to fabricate integrated circuits. If such a qubit technology is developed, existing fabrication processes and techniques could be quickly leveraged to mass-produce qubits, and large numbers of qubits may be achievable fairly quickly after such qubits are invented [reference ETSI QSC paper].

While there still are significant problems to be overcome before quantum computers appear that can threaten RSA or ECC, the pace of recent progress in this area is impressive, and the amount of effort being expended makes it reasonable to assume that the rate of innovation will probably continue to be rapid.

3.8. Risk Assessment and Time Line Actions

To assist in assessing the risks posed by quantum computers to an organization, that organization must analyze the type of data under consideration to determine the sensitivity of the data and the length of time the data must be kept confidential. This data may include, but is not limited to:

- Financial Data (including PIN and bank card account data)
- Financial Transaction Data (including purchase information)
- Personnel / Human Resources Records
- Confidential Communications (including VPN-based communication)
- Patient Medical Records
- Wage / Salary / Bonus History
- Corporate Strategy (e.g. Board of Director's confidential discussions
- Personal Identification Information
- Financial Account Information
- Product Design and Development Information
- Intellectual Properties
- Legally Privileged Information
- Email and other forms of electronic communication

The data listed above has varying "confidentiality life spans". Another way of describing confidentiality life span is to define the useful life of the data. For example, the compromise of some financial data associated with a bank transaction or bank card activity may only be valuable during the active lifecycle of the data.

The protection period, the confidentiality life span, of certain data has no expiration date. Patient medical records and Personal Identification Information (see table above for additional data types) must be kept confidential at all times, the confidentiality life span of that data has no expiration date.

In assessing the time sensitivity of confidential data, the methods of securing the data are critical to maintaining the confidentiality of the data during that timeframe. This can include data that is important to business, personal identity information, or data that, for regulatory reasons, must be kept confidential. For example, certain intellectual properties or medical records that were protected using single DES when it was considered safe are no longer adequately protected from exposure based on modern attacks that exist against DES. That data must be protected with improved cryptographic tools that would not be vulnerable to attack in the current or anticipated environments. Once that data is protected by more robust mechanisms, the prior records and archives that were protected by weaker means must be deleted so as to remove the possibility of exposure.

If confidential data is transmitted from one point to another, even in encrypted form, that data is subject to interception and recording. At a later date when that cryptographic protection is vulnerable to attack, the cryptographic tools used to protect that data can be compromised and the data exposed. If the data has value to the exchanging parties or the relying parties, then exposure would constitute a breach of confidentiality.

Now we can place cryptographic data protection in the context of Quantum Computing Risk.

As noted elsewhere in this document, it is projected by some experts that in 10 to 15 years quantum computing may advance to the point of being able to compromise major asymmetric / public key cryptographic schemes. Quantum computing is expected to reduce the secure key length of symmetric cryptography.

To put this in perspective, if data, for example a bank card magnetic stripe image has a useful life of five years (until the card expires), then any cryptographic protection scheme must be able to protect that data for at least five years. If it is expected that by 2028 a quantum computer capable of successfully attacking the protection will be developed, then the cryptography used to protect that data must be discontinued and converted to quantum-resistant cryptography at least five years before the potential for attack.

Additional considerations must be made for the time required to convert from a vulnerable cryptographic protection scheme to a more robust scheme that will be resistant to quantum computing attacks and other future anticipated advancements in processing technology.

Data sensitivity, cryptographic protection critical period and conversion period can be expressed in a variation of a formula developed by Michele Mosca, Ph.D., a quantum researcher and developer. His formula was developed to help understand the security evaluation process. Mosca's XYZ Theorem can be summarized as follows:

How long will the data or cryptographic keys protecting the data be required to remain secure? (X = period expressed in years)

How much time will be required to convert the infrastructure and / or cryptography to a more robust and secure scheme? (Y = period expressed in years)

How long will it take to develop a large-scale Quantum Computer capable of successfully attacking the cryptography associated with the data protection scheme or advances in technology occur which renders that scheme insecure? (Z = period expressed in years.)

It is possible to compute the latent period and timeline for commencing change where:

X + Y < Z indicates that there is some latent time before conversion needs to begin. (Begin tracking to conversion time.)

X + Y = Z indicates that it is currently time for conversion to begin (Now.)

X + Y > Z indicates that conversion should already be underway. Delays will result in the potential exposure of security data. (Time to worry.)

To put this into the context of the larger discussion, let's assume that in 10 years a large-scale Quantum Computer can be developed which is capable of successfully attacking our existing public key systems and reducing the attack time of our symmetric key cryptography.

If bank card transaction data is being protected, then the life of the card, typically 5 years or so, would determine how long that data must be protected. If it takes 2 years to convert to a new infrastructure and protection scheme, then conversion to a new infrastructure and protection scheme needs to begin in 3 years.

This can be expressed where X = 5, Y = 2, and Z = 10.

$$5 + 3 < 10$$

That data is currently secure, but conversion needs to begin in 2 years or 10 – (5 + 3). Tracking to the time of conversion should be considered.

If some corporate communication, bank account information, mortgage records, credit reporting data or similar data requires 8 years of confidentiality, and it will take 2 years to complete conversion, then this can be expressed where X = 8, Y = 2, and Z = 10.

$$8 + 2 = 10$$

In this example, conversion should start immediately to meet the confidentiality requirements of the data.

If data contains information that is permanently sensitive such as containing PIN information, certain personnel data or medical records are involved with no expiration on their sensitivity, then other variables don't matter, conversion must begin as soon as possible, old records must be converted to new protection and records protected under the old cryptographic scheme must be purged.

In any major system change such as what is outlined in this discussion, it is imperative to have strong audit controls. These controls should, at a minimum, include a complete identification and analysis of the data, associated regulatory and reputational risks of that data exposure, timelines associated with conversion, verification of the protection over the converted data. As an audit follow-up, there needs to be a confirmation of the destruction of any data protected using vulnerable schemes from backups and archives. Procedures and conversion records should be recorded to allow for future confirmation as determined by management. These records could be used to verify the conversions in the event of a regulatory review or for purposes of forensic contribution in the event of a data breach.

To continue this discussion, certain data will not fit this evaluation. This data has indefinite time sensitivity for business and / or regulatory purposes. This data includes, but is not limited to Personally Identifying Information, Medical Records and Health History, Legally Privileged Communication, Business Strategy, and similar data. For this data, it is necessary to begin converting that data to stronger protection schemes. Management should make a special risk determination against this data to determine how it will be protected, the timeframe needed for conversion and the disposition of archived data that could be exposed using an attack against the archive protection scheme.

4. Terms and definitions

For the purposes of this document, the following terms and definitions apply:

4.1. Advanced encryption standard (AES)

AES is a symmetric encryption algorithm defined by FIPS PUB 197. With an appropriate mode of operation, it can provide privacy (encryption) and integrity validation. It is believed that, assuming a random 256 bit key, AES encrypted texts are secure against Quantum Computers.

4.2. Block cipher

A block cipher is a symmetric encryption method that applies an algorithm along with a symmetric key to encrypt a block of text, rather than encrypting one bit at a time as in stream ciphers. For example, a common block cipher, AES, encrypts 128 bit blocks with a key of predetermined length: 128, 192, or 256 bits. Used in an appropriate mode of operation, it is able to encrypt arbitrary length messages, and provide other security guarantees, such as integrity.

4.3. Brute force attack

A trial-and-error method used to obtain information such as an encryption key, user password, or personal identification number (PIN); the attacker simply tries all possible values of the key/password/PIN until he finds the correct one. In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data.

4.4. Cipher

A secret code, usually one that was created using a mathematical algorithm.

4.5. Encryption

The process of using algorithmic schemes to transform plain text information into a non-readable form called ciphertext. A key (or algorithm) is required to decrypt the information and return it to its original plain text format.

4.6. Factor

A whole number greater than 1 that can be divided evenly into another number.

4.7. Feistel cipher (a.k.a. Feistel network)

A symmetric structure used in the construction of block ciphers, named after the German IBM cryptographer Horst Feistel and commonly known as the Feistel network. Many block ciphers use the scheme, including the Data Encryption Standard.

4.8. Integer

A whole number that can be written without a fractional component. For example, 21, 4, 0, and −2048 are integers, while 9.75, 5½, and √2 are not.

4.9. Permutations

A specific shuffling of a list of values; for example, if we have 6 values (a, b, c, d, e, f), one permutation exchanges the values a and b, leaves c alone, and sets d to e, e to f, and f to d. If we have n values, there are n! = n(n-1)(n-2)(n-3)…(3)(2)(1) possible permutations on that list.

4.10. Prime number

A prime number is a whole number greater than one that can only be divided by one and itself. For example, the first few prime numbers are 2, 3, 5, 7, 11, 13, 17, 19, 23 and 29.

4.11. Stream Cipher

A stream cipher is a symmetric encryption method in which a cryptographic key and algorithm are applied to each binary digit in a data stream, one bit at a time.

5. Symbols and abbreviated terms

For the purposes of this document, the following symbols and abbreviated terms apply:

5.1. 3DES

Triple Data Encryption Algorithm; defined in ANSI X9.52-1998, this is the DES algorithm applied three times, with two or three different keys. Considered obsolete.

5.2. AES

Advanced Encryption Standard; defined in FIPS PUB 197

5.3. DEA

Data encryption algorithm

5.4. DES

Data Encryption Standard; defined in FIPS PUB 46. Known to be insecure.

5.5. TDEA

Triple Data Encryption Algorithm

5.6. TDES

Triple Data Encryption Standard; another term for 3DES

6. Software

6.1. Overview of Encryption Principles

We are more digitally connected now than at any other time in history. Anyone sending an e-mail, using a mobile phone, or updating their social media profile is benefiting from innovations brought about largely by cryptography. Anyone using a card or smart phone to pay at a retail store or withdrawing cash from an ATM has cryptography to thank for it. Any business accepting online payments for products and services is indebted to developments in cryptography for making this possible. Cryptography is all around us, and it is the foundation of security for financial services.

To understand the threats posed by quantum computers, it is necessary to provide an overview of some basic principles of encryption and how encryption standards have evolved as technical computing capabilities continue to improve.

All encryption algorithms have a key exhaustion strength, which is the expected amount of computation needed to try every possible key value to determine which one is correct. Continued technology advances, increases in computational capabilities, and mathematical analysis of encryption algorithms have necessitated ongoing increases key size in order to resist brute force (guessing) attacks.

Following is a high-level description of the two types of encryption algorithms in use today and how they have evolved:

- Symmetric algorithms (single key/"shared secret")
- Asymmetric algorithms (two key: public key + private key) a.k.a. "Public Key Cryptography"

6.1.1. Symmetric algorithms (single key)

Until the 1970s all ciphers were symmetric. In symmetric encryption, the key is a shared secret used to both encrypt and decrypt the data. This could be compared to the lock on a door, where one key can both lock and unlock the door (see Figure 1). In a payment processing environment, the key used to encrypt the data can also decrypt it. In this type of a system, it is very important to protect the key, because if the key is compromised all the data is compromised. Key management and key exchange vulnerabilities are often exploited as a means to attack the encrypted message.

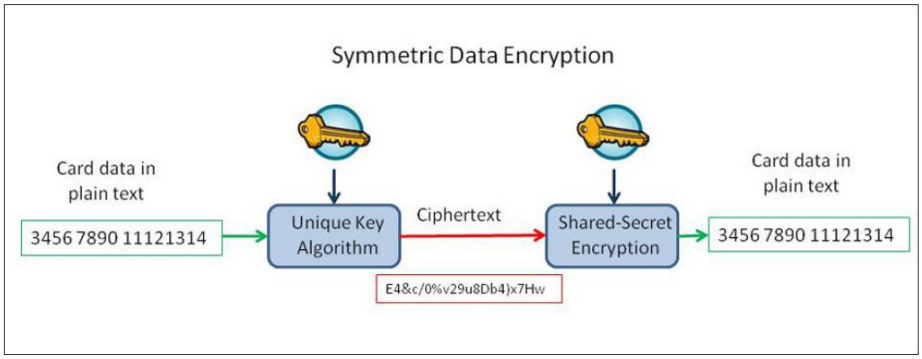


Figure 2: Symmetric Data Encryption

6.1.1.1. Data Encryption Standard (DES)

Data Encryption Standard (DES) is a symmetric-key algorithm for the encryption of electronic data. It was jointly developed in 1974 by IBM and the U.S. government (US patent 3,962,539) to set a standard everyone could use to securely communicate with each other. The Data Encryption Standard was published as an official Federal Information Processing Standard (FIPS-46) for the United States in 1977. DES was later adopted as the American National Standard (ANS) X3.32 Data Encryption Algorithm (DEA) in 1981 and DES became the standard cryptographic algorithm for the financial services industry in the United States and worldwide.

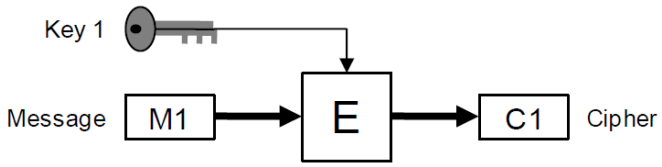


Figure 3: Single Data Encryption Standard

The length of the symmetric key used to encrypt/decrypt data is 56-bits. Because classical computing is binary, and each bit can have only two possible values, namely 0 or 1, this yields 2^56, or 72,057,594,037,927,936 possible keys. In 1976, when DES was new, it was estimated that a machine fast enough to test that many possibilities in a day would cost about $20 million. "Guessing" a 56-bit key with 72 quadrillion possible values was considered an intractable problem.

Advances in computing power over the next twenty years changed the scenario significantly. Beginning in January 1997, RSA Security initiated the DES Challenge, a series of brute force attack contests designed to highlight the lack of security provided by the Data Encryption Standard:

- The first winner to break a DES encrypted message relied on thousands of volunteers to run software in the background on their own machines, connected by the Internet. This group announced their success in June 1997, just 96 days after the challenge was announced.
- The second cipher was solved by Distributed.Net, a worldwide coalition of computer enthusiasts, in just 39 days in early 1998.
- The third challenge was solved in just 56 hours in July 1998, by the Electronic Frontier Foundation (EFF), using "Deep Crack", a specially designed supercomputer that cost EFF $250,000 to build. "Deep Crack" could generate 245 billion DES calculations per second.
- The final DES encrypted cipher was cracked in less than 24 hours through a joint effort between Distributed.Net and EFF, in January of 1999.

The contests demonstrated how quickly a rich corporation or government agency, having built a similar machine, could decrypt ciphertexts encrypted with DES.

Beginning in 1997, NIST worked with industry and the cryptographic community to develop an Advanced Encryption Standard (AES). The overall goal was to develop a Federal Information Processing Standard (FIPS) specifying an encryption algorithm capable of protecting sensitive government information well into the 21st century. The algorithm was expected to be used by the U.S. Government and, on a voluntary basis, by the private sector.

6.1.1.2. Triple Data Encryption Standard (Triple DES)

Triple DES (3DES), officially the Triple Data Encryption Algorithm (TDEA or Triple DEA), is a symmetric key cipher. The key is broken into three sub-keys or data blocks of 64 bits each (56 bits plus 8 parity bits). The DES algorithm is applied three times – once to each data block. The procedure for encryption is exactly the same as regular DES, but it is repeated three times, hence the name Triple DES. Triple DES employs three ordered instances of DES for encrypting data: encryption (E), decryption (D) and encryption (E); and three ordered instances of DES for decryption: decryption (D), encryption (E), and decryption (D). Triple DES (TDES) offers two keying options called Two Key (128-bit) or Three Key (192-bit).

6.1.1.3. Two Key Triple DES (128 bit)

Two Key Triple DES uses two keys: one key (Key 1) with the first (E) and third (E) instances and the other key for the second (D) instance. The intermediate results (C1 and C2) are intended to be internal to the Triple DES algorithm and not accessible by any system or application process:

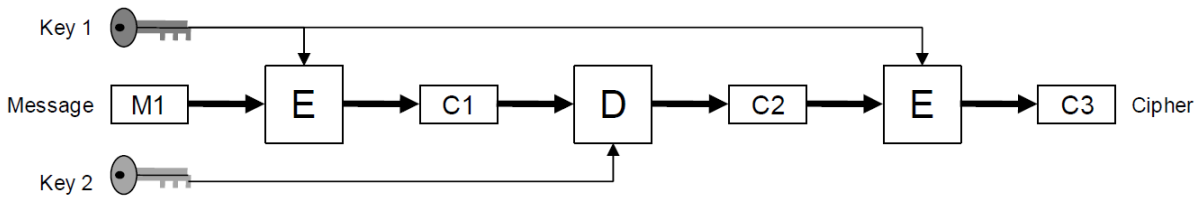


Figure 4: Two Key Triple DES

Two Key Triple DES has a medium security strength, higher than single DES but less than Three Key TDES.

6.1.1.4. Three Key Triple DES (192 bit)

Three Key Triple DES shows the plaintext message (M1) being encrypted (E, D, E) using three keys (Key 1, Key 2 and Key 3) with three instances of DES producing the final ciphertext (C4). This keying option of Triple DES uses a different key for each DES instance. As with Two Key Triple DES, the intermediate results (C1 and C2) are intended to be internal to the Triple DES algorithm and not accessible by any system or application process.

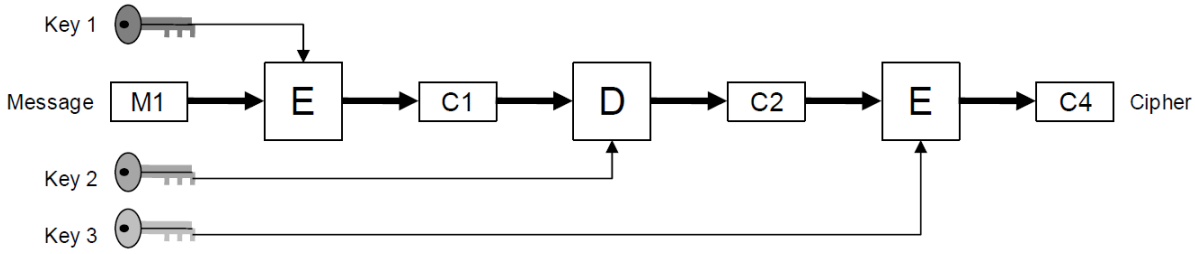


Figure 5: Three Key Triple DES

Three key Triple DES has higher security strength than single DES and Two Key TDES.

6.1.1.5. AES

Recognizing the limitations of both DES and Triple DES in light of rapid advances in computing power, in 1997 the National Institute of Science and Technology (NIST) set a goal to develop an unclassified, publicly disclosed encryption algorithm capable of protecting sensitive government information well into the 21st century. In September 1997, NIST put out a call to solicit candidate AES algorithms from the public, academic/research communities, manufacturers, voluntary standards organizations, and federal, state, and local government organizations. As a result of these efforts, The Advanced Encryption Standard (AES) was published as FIPS 197 on November 26, 2001.

AES is a symmetric block cipher capable of using three different keys sizes (128-bit, 192-bit and 256-bit cryptographic keys) to encrypt and decrypt data in 128-bit blocks; the key sizes are referred to as AES-128, AES-192 and AES-256 respectively.

6.1.2. Asymmetric algorithms (public key + private key)

In asymmetric cryptography, there are two keys: a public key and a private key. The keys are different, yet mathematically related. Only the combination of private and public keys makes the message readable. For example:

- The sender of a message could encrypt a message with the recipient's public key and the recipient could decrypt it with their private key.
- Similarly, a sender could digitally sign a message using their private key. The recipient could verify that specific message was signed by the sender using the sender's public key.

The mathematics behind RSA, the most commonly used public key cryptosystem, relies on prime numbers. While it is easy to multiply two random 300-digit prime numbers together, it is difficult and time-consuming to reverse the operation knowing only the product, even for today's advanced computers.

6.1.2.1. SSL/TLS

Transport Layer Security (TLS), originally known as SSL (Secure Sockets Layer), is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures the privacy and integrity of all data passed between the web server and browsers. TLS is an industry standard used by millions of websites in the protection of their online transactions with their customers.

6.1.2.2. RSA

Capable of providing both data encryption and digital signature functionality, crypto systems based on the RSA algorithms are perhaps the most widely deployed and deeply studied of all cryptographic systems in use today. Named after its inventors Rivest, Shamir, and Adleman, who developed it in 1978 while working at MIT, the security of RSA is based on the difficulty of factoring very large numbers. For example, it takes about an hour to factor the number 29,083 by hand. Of course, it only takes a minute to confirm the factors are 127 and 229. The disparity between the effort required to compute the factors and that required to confirm those factors are correct widens as the size of the numbers is increased.

6.2. Methods quantum computers can use to break encryption

6.2.1. Grover's Algorithm

Grover's Algorithm allows a quantum computer to find a value that has a certain property much faster than is possible on a classical computer. For example, secure hash functions rely on the problem "given Y, find X such that Hash(X) = Y" being difficult. Classically, for secure hash functions, the only known solution is to simply guess values for X until one is found that hashes to Y. This takes, on average, 2^n tries, where n is the number of bits needed to represent X. A similar argument can be made about finding an AES key when at least one plaintext/ciphertext pair is known.

A quantum computer can find the value X with high probability in the square root of the number of classical operations, or 2^(n/2). For large values of n, this is significantly faster. The number of required qubits is relatively modest; roughly the same number as the size of the key or hash being searched for.

However, a simple application of Grover's algorithm requires that all 2^(n/2) operations must be performed sequentially on the entangled qubits. For values of n that are suitable for cryptographic applications, this is an extremely large number of operations and thus this attack would require an impractical amount of time. It is possible to accelerate the attack by parallelizing the operation (for example, by using independent Quantum Computers each running Grover's algorithm to search disjoint parts of the search space); however, this reduces the efficiency gain of Grover's algorithm. An analysis of this in (Fluhrer, 2017) shows that, given a bound on the search time, Grover's algorithm effectively reduced the required time by a large constant factor, making it 2^{n-c} (assuming n > 2c). The paper further argues, based on plausible guesses on the likely performance of Quantum Computers, that c in the range 60 to 65 are reasonably conservative estimates.

In any event, attacks using Grover's algorithm can be completely mitigated by doubling the key size, restoring the original work factor. For example, AES-256 would require at least 2^128 quantum operations

to be performed. It is widely believed that performing 2^128 quantum operations is at least as infeasible as performing 2^128 classical operations.

Because of the ease of mitigating the attack by moving to larger keys, the recommended approach is to simply do so at the next available opportunity. The performance difference between AES-128 and AES-256 is typically small and may be negligible with hardware acceleration.

6.2.2.Shor's Algorithm

Shor's Algorithm is an integer factorization algorithm formulated by Peter Shor in 1994 which solves the following problem: given integer (whole number) "N", find its prime factors. If a quantum computer with a sufficient number of qubits could operate without succumbing to noise and other quantum decoherence phenomena, Shor's algorithm could be used to break public-key cryptosystems such as the widely used RSA scheme. RSA is based on the assumption that factoring large numbers is computationally infeasible. So far as is known, this assumption is valid only for classical (non-quantum) computers. Shor's algorithm shows that factoring is efficient on an ideal quantum computer, so it may be feasible to defeat RSA by using a quantum computer.

6.2.3. Shor's Algorithm – Problem Background

How long does it take to factor a large product of two primes? How long does it take to solve the discrete logarithm problem for a particular elliptic curve? These are the problems that determine the strength of RSA and ECC, respectively.

For classical computers, the answers are as follows: the fastest known classical factoring algorithms take roughly 2^(n^(1/3)) steps, where n is the number of bits in the number to be factored. This fast factoring algorithm is known as the number field sieve (NFS). The complexity of the NFS is sub-exponential, but it grows fast enough that factoring 2048-bit numbers is not currently feasible.

For discrete log problems using elliptic curves, the best-known algorithms have exponential runtime, allowing the use of smaller keys for an equivalent strength against classical computers. If an elliptic public key in compressed form has n bits, then the best ECC attacks take about 2^(n/2) steps. A 224-bit elliptic curve key is generally considered to have similar strength to a 2048-bit RSA key.

As can be seen from the graph below, exponentials grow quickly, and increases in the capability of classical computers can fairly readily be mitigated simply by moving to larger elliptic keys. The performance of RSA gets much worse as key sizes get larger, and this is why ECC is often recommended instead of RSA for providing the same security strength at a much lower computational cost.

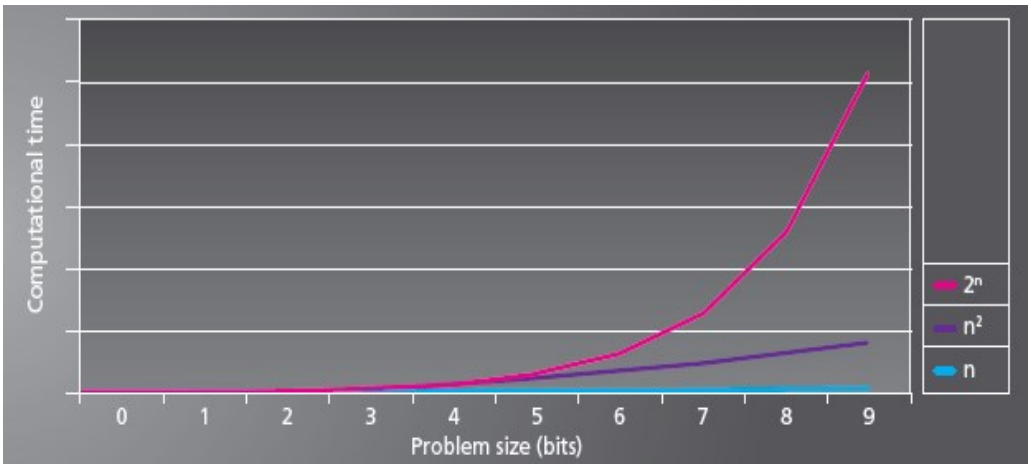


Figure 6: Numerical Strength Comparison: Exponential, Quadratic, and Linear

Shor's Algorithm takes advantage of entanglement to reduce the time needed to factor integers to polynomial scale (a similar algorithm works for discrete logs). The real importance of his work is the implication that quantum computers can in fact outperform classical computers (in this case exponentially) for specific types of problems. So far, Shor's algorithm has only been implemented using a small number of qubits, and therefore scaling has not been fully observed. Full verification is going to require a quantum computer with many more qubits than have been implemented so far, however there is no known physical or mathematical reason to expect it would not work.

Importantly, the work necessary to solve either problem (factoring or calculating discrete logs) depends on the size of the key, so although ECC is stronger than RSA against classical computers, it is actually weaker against quantum computers. This has caused some organizations to recommend not moving to ECC, and going directly to post-quantum cryptography instead.

Inside Shor's Algorithm

Shor's solution breaks the problem down into two parts. The first part, which can run on a classical computer, is a reduction of the factoring problem to a period finding problem. The second part, which runs on a quantum computer, does the job of searching for the period.

Before we dive into the details of Shor's algorithm, full credit must go to Dr. Scott Aaronson from the University of Texas for the explanation and analogy we're about to cover. There are many "poorly executed", analogies that attempt to explain how quantum algorithms work. Scott does a great job of staying true to the actual mechanics involved. (http://www.scottaaronson.com/blog/?p=208)

What is this period thing we're talking about? Let's start with the "powers of 2" series. 2, 4, 8, 16, … etc. If we then apply modulus 15 to each of these we get a series that repeats every 4 numbers, 2, 4, 8, 1, 2, 4, 8, 1, and so on. Note that modulus or mod is simply the integer remainder of the division. So, for example 16 mod 15 is 1.

Now, while there is no periodic pattern to the prime factors that we're interested in finding there is a period to a related set of numbers that is created by the series x mod n, x^2 mod n, x^3 mod n, and so on. As it turns out, this series repeats with a period that divides quantity (p-1)(q-1) evenly. As an example, if n=15 with prime factors p=3 and q=5 we can take x=2 like we did with the example series above to arrive at a period of 4 which is a factor of (p-1)(q-1) = (3-1)(5-1) = 2*4 = 8.

2^k: 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, …

2^k Mod 15: 2, 4, 8, 1, 2, 4, 8, 1, 2, 4, …

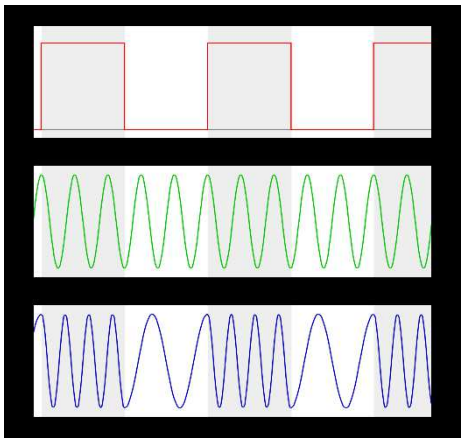
The period is 4 as the series 2, 4, 8, 1 repeats every 4 operations

So, the idea is to try random values of x to obtain a factor of (p-1)(q-1). With a few more math tricks you can get p and q with high probability.

This is where quantum computation is needed because the period of x^k mod N can be just as large as N and searching for this period on a conventional computer would not provide a speed up.

The first requirement of our quantum computer to find this period is to create a superposition over all the numbers in the repeating series and we'll need some sort of transformation or operation on those superpositions that will reveal the period.

Enter the Quantum Fourier Transform or QFT for short. A QFT works a lot like a normal FT that you may have seen for radio signal manipulations to separate out data from frequency encoded signals. For instance, below you'll see how Frequency Shift Keying or FSK encoding works. The data stream on top is used to change the carrier signal in the middle to a FSK wave where changes in frequency encode the bits. To get the original bit stream back you run an inverse FT that shows you where within the signal the 1's and 0's are located.



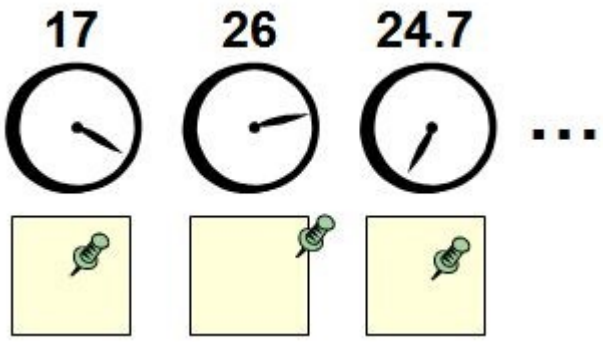
What makes the Quantum FT special is that it can operate on all the qubits simultaneously whereas a normal FT would have to operate on each bit individually. And, of course, a QFT gate can be built using the primitive quantum gates we discussed earlier.

But, how does a QFT actually find the period we're looking for? This is the part that requires quite a bit of Quantum Mechanics, Linear Algebra, and Quantum Circuit knowledge. Graduate level courses that discuss this algorithm step by step may take multiple days. But, here's a great analogy that gets the core of the idea across…

There's a famous experiment where researchers isolated people in sealed rooms for a few weeks. These rooms were clock and window free. Over the course of several days the subjects of the study began to shift their usual 24 hour clock to a 25, 26, and in some cases even a 28 hour clock. In the case of a 26 hour clocked person, he would wake up at 8am one day, then 10am the next, then 12 noon the following day. Over the course of 12 days this person would loop all the way around to waking up at 8am again.

Now, what if we couldn't observe the person directly to determine his biological clock and instead had to rely on the following rather odd measurement system.

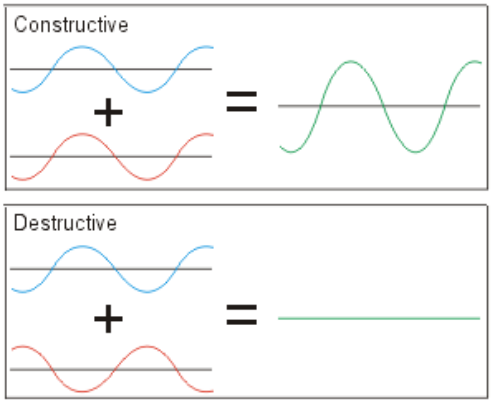
On the bedroom walls of our subject are many clocks. Each clock has only a single hand for the hour that is laid out like a military clock where the hand goes around one time for each day. However, each clock has a different number of hours in the day, one has the normal 24 hours, but there also a 23 hour clock, a 25 hour clock, a 26 hour clock and so on. Also, below each clock is a bulletin board with a thumbtack at the center of the board. Now, each time our sun deprived subject wakes up, he moves the thumbtacks under each clock one inch in the direction of the hour hand.



Here's the question… by examining the thumbtacks in the room, is it possible to determine the biological clock this person is operating under?

In fact, it is. Say this person is on a 26-hour clock. On the bulletin board below the 24 hour clock you would see the pin moving around in a cyclical fashion and, every 12th, day it would return to the center. The same would happen to all the other clocks with their respective periods. However, our exception is the 26-hour clock where the pin would move an inch in the same direction every morning eventually leading to the pin going off the poster-board.

What's going on here is the miracle of interference. Quantum states are described as waves whose amplitudes, when squared, result in real world probabilities. However, before the amplitudes are measured all the possible states of the superposition, using entangled qubits, are free to interact with each other using quantum gates like our Quantum Fourier Transform. The QFT causes all the states that are carrying the incorrect period to destructively interfere with each other leaving the state representing the right answer with the only large amplitude that when squared gives the largest probability of being correct.



Now, once we have the period of x^k Mod N from the quantum computer we are free to calculate the factors of N using a little math trick called the Chinese Remainder Theorem. This theorem tells us that if we know the period, r, of the series x^k Mod N (which we obtained from our quantum computer) we can get the factors of N by finding the greatest common divisor (GCD) of $x^{r/2}+1$ and N as well as the GCD of $x^{r/2}+1$ and N.

N=15, pick x=2, send to QC, receive period=4 then…

$$\gcd(2^{\frac{4}{2}}+1, 15) = 5$$

$$\gcd(2^{\frac{4}{2}}-1, 15) = 3$$

So, going back to our example of N=15 if we choose at random x=2 then the greatest common divisor (GCD) of $2^2+1=5$ and 15 is 5 and of course the GCD of 2^2-1 and 15 is 3. And, sure enough, 3 and 5 are prime factors of 15.

This explanation may leave the reader wondering why you can't simply have the quantum computer try every possible divisor of N. The answer is that you need some common property of all the possible divisors that can be used to calculate probabilities...something that allows for the creation of a superposition of states that is governed by a shared equation. You could setup a superposition of linear states that represents all possible answers for the direct calculation of the factors, but any operation you would perform on this system would just result in a single one of the answers, chosen at random. This is no better than performing the same calculation on a classical computer.

So, when you see an explanation stating that quantum computers do what they do by simply trying every possible answer simultaneously, just know that there's much more to it than that. You still need some clever mathematicians looking for insights into the way the possible results are related. This is also why some problems will probably remain difficult even for quantum computers. Its problems like these, in fact, that post-quantum cryptography is based upon.

6.3. Quantum Error Correction

If no errors occur, Shor's algorithm can factor RSA-2048 public keys as soon as a computer with 4,096 qubits is available. However, it is impossible to completely isolate a quantum system, even at temperatures near absolute zero. This inevitably leads to the probability that the qubit has interacted with its environment and is no longer entangled with the rest of the computer or has a state which is slightly different from the intended state. The time after which the state is likely to no longer still be coherent is called the decoherence time, and is an important measure of the quality of a qubit.

The quantum gates in use today aren't perfect. Imperfect gates may produce states that are not the intended states. In a complex quantum circuit, these errors build up and will eventually cause the computer to give the wrong answer.

Assuming the error per operation is about the same, these errors essentially put a limit on the depth of a quantum circuit that can be built with a particular set of qubits. For Shor's algorithm, this can equivalently be seen either as a limit on the largest number that can be factored with a particular qubit technology, or a maximum error allowed in order to factor a number of a given size. Existing and foreseeable techniques for making qubits do not have error rates that are low enough so that a straightforward implementation of Shor's algorithm is feasible.

In the early days after Shor's algorithm was published, there was a great degree of scepticism about whether the algorithm would ever be feasible in practice. However, it was soon discovered that quantum error correcting codes exist and could be used to correct errors that had accumulated in a qubit, at the cost of requiring many physical qubits to be used together to create a single logical qubit. The original quantum error correction code published by Shor required nine physical qubits to implement a single logical qubit.

When a qubit becomes corrupted, it has a non-zero probability of having the wrong state or wrong phase. It turns out that by using the additional qubits, it is possible to measure what kind of error (if any) has affected the qubit, without measuring the value of the qubit. That measurement either forces the original qubit either back into its

original “no error” state or forces it into a known error state (bit flip or phase flip) that can then be corrected. Either way, the qubit ends up in the intended state.

6.4. Requirements for breaking RSA-2048

4700 logical qubits, circuit depth ≈ 8 10^9.

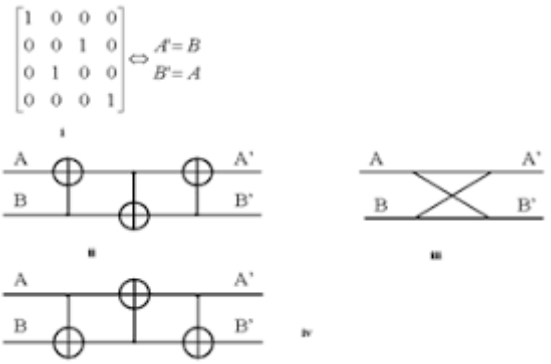
6.5. Requirements for breaking ECC NIST P-256

2330 logical qubits, circuit depth 1.3 10^11 [2]

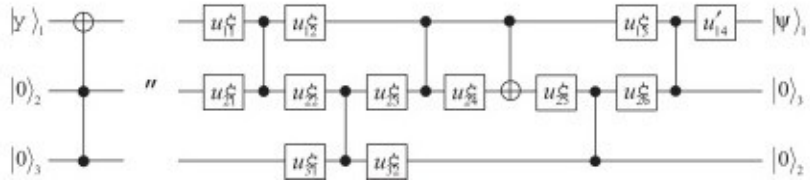
6.6. Example of Quantum Circuits

Quantum computer design is in very primitive state, as evidenced by the few elementary gates available today. To design a quantum computer capable of performing a given task, the design approach is limited to fixed-purpose (as opposed to general-purpose) paradigms.

The design and programming of a quantum are one in the same since the arrangement of the gates determine the functionality.



Reversible Arithmetic Logic Gate



Quantum circuit implementation of three-qubit Toffoli Gate.

[2] https://eprint.iacr.org/2017/598.pdf

7. Hardware Requirements to Implement a Quantum Computer

This section discusses the basic hardware elements of a quantum computer, the principles of operation, and what external hardware is required to create the environment necessary for a quantum computer to operate.

7.1. What is a Qubit?

A qubit is the fundamental unit of quantum information. They are similar to bits in the classical setting, but they use a few phenomena unique to quantum mechanics. These phenomena include superposition and entanglement. In a classical computer, a bit is represented by a voltage in a transistor. A low voltage represents a 0 and a higher voltage represents a 1. A qubit is formed by harnessing quantum features such as the spin of an electron or an atom or the polarization of a photon. Using electrons to create a qubit is the most commonly used method, at this time.

A qubit has two computational basis states which are analogous to the 0's and 1's of a classical computer. The 0 state is represented as |0> and the 1 state is represented as |1>. This is where quantum computers take a radical divergence from classical computers. The states of qubits are actually represented as two-dimensional complex vectors. The |0> state is a unit vector along the horizontal axis and the |1> state is a unit vector along the vertical axis. In between the two computational basis states are an infinite number of quantum states each represented by a two-dimensional complex vector. These vectors are in the form of $\alpha|0> + \beta|1> = |\Psi>$ and are of unit length (1). There is a constraint to all vectors called the normalization constraint. It requires that all vectors that represent the state of a qubit satisfy the following constraint: $|\alpha|^2 + |\beta|^2 = 1$. Therefore, the quantum state of a qubit is a vector of unit length in a two-dimensional complex space.

Another difference between a qubit and a classical bit occurs when one tries to read the state of a qubit. No matter what state the qubit is in when it is read, the result of the reading will be exactly one of the two computational basis states; even if the qubit was in a state between the basis states prior to reading. However, the chances of returning either of the computational basis states is proportional to the distance the actual complex vector was to either of the two basis states. Reading a qubit actually creates a quantum gating function. Reading a qubit is called a measurement gate and will only produce one of the two computational states, |1> or |0>. Some of the other quantum gates are: swap gate (swaps two qubits), the Pauli-X not gate (rotates the vector value of a qubit 180° about the x-axis), and several others. There are also control gates. See the software section for more details on programming a quantum computer.

7.1.1. Quantum Superposition

The spin of a particle is a measurement of the particle's angular momentum. The spin of an electron is "up" or "down" or in multiple states between "up" and "down". The "up" state is referred to as +1 (|1>)) and the down state as -1 (|0>). Being in more than one state at the same time is known as quantum superposition. Superposition state is a combination of the computational basis states. Another way to think about superposition is that the electron (qubit) has not determined which state it will end up in but it can have a bias toward one of the basis states. Most quantum computations start with a qubit in superposition and then the value of the qubit moves to a final state of a |1> or a |0> after being operated on by a magnetic field encoded with the quantum program being run.

7.1.2. Quantum Entanglement

Quantum entanglement is a physical phenomenon which occurs when pairs of electrons interact in ways such that the quantum state of each electron cannot be described independently of the state of the other electron or electrons, even when the electrons are separated by a large distance. Measurements of physical properties such as position, momentum, spin and polarization, performed on entangled particles are found to be correlated.

7.1.3. **Quantum Decoherence**

In a perfect world, the qubits of a quantum computer are completely isolated from their surrounding environment and each of the qubits operate in a pure quantum state where they interact as a waveform with each other. This type of operation is said to be coherent and the system is in coherence. Coherence in a system is a fundamental property of quantum mechanics and it is necessary for the proper functioning of a quantum computer. A lack of coherence means the computer can only operate in the classical world and not in the quantum world. It also means errors are introduced into the system and the results are likely incorrect.

In reality, the qubits are not perfectly isolated from their surrounding environment and over time they begin to communicate with the outside environment. This is sometimes referred to as the sharing or loss of quantum information. At some point, the quantum wave function collapses and the quantum computer can no longer function. This is called quantum decoherence. It has been found that the use of superconducting circuits operating at extremely low temperatures (~15° milli-kelvin) will increase the time that a quantum system is coherent. Companies are experimenting with different materials and methods that could extend the time the system is in coherence. Today, most quantum computers will lose coherence in less than a 1 µsec. The best quantum computers today cannot remain coherent for 1 msec. The issue of decoherence is a major hurdle that must be overcome before stable large-scale, stable quantum computers can be built.

In a recent article in IEEE Spectrum, they state:

> "Now scientists at Tsinghua University in Beijing have achieved a coherence time of more than 10 minutes for a single qubit consisting of a magnetically trapped, positively charged ytterbium-171 ion."[3]
>
> If this is true, it represents a major step forward in the stability of qubits.

7.2. Operating Environment of a Qubit

7.2.1. Temperature Requirements for a Quantum Computer

Research on quantum computation has been ongoing for about forty years, but companies are still exploring different technologies that can be used to build a physical qubit. Most of the technologies being used at this time require that the hardware implementing the physical qubit be maintained at temperatures within a fraction of one degree from absolute zero. For example, the latest generation D-Wave 2000Q system has an operating temperature of about 15 milli-Kelvin. Absolute zero is the lowest temperature that can be attained by matter and corresponds to a point where almost all motion in an atom stops. Depending on the temperature scale used, absolute zero is 0° Kelvin, -273.15° C or -459.67° F. The key reasons for operating at such a low temperature are that is removes influences from random thermal noise, slows movement within an atom which allows for measurement of quantum characteristic and increases the coherent working time of quantum computers.

Technology for achieving and operating near absolute zero is well known but is very expensive. That is one reason researchers continue to look for ways to operate the hardware for a physical qubit at higher temperatures. At present, no technology has been successful at operating a physical qubit, with *full* quantum features, above 1° K, but research continues.

Providing the required low temperature environment for the hardware that implements physical qubits is usually a multistep process. Conventional processes can be used to achieve temperatures around 4° K (which is the temperature of liquid helium). The last step that cools the hardware environment from approximately 4° K to 15° milli-Kelvin uses dilution refrigeration.

---

[3] IEEE Spectrum, "Long-Lasting Qubits Share Vibrations to Stay Cool" by Charles Q. Choi, Sept. 15, 2017: https://spectrum.ieee.org/tech-talk/computing/hardware/longlasting-qubits

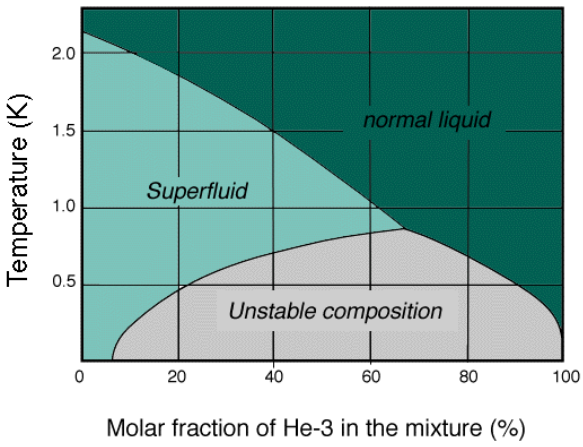
7.2.2. Methods to Achieve Low Temperature Operation

7.2.2.1. Dilution Refrigerator

[4]The dilution refrigerator was first proposed by Heinz London in the early 1950s and was realized experimentally in 1964 at Leiden University. In 1965, Henry Hall built the first ^{3}He-^{4}He dilution refrigerator at University of Manchester. The first commercial dilution refrigerator was developed in collaboration with Heinz London at the Oxford Instruments factory in Osney Mead, Oxford in 1967. The achieved 200° milli-Kelvin base temperature enabled dilution cooling beyond known ^{3}He temperatures. The dilution refrigerator has evolved over its 50 years with improved performance, reliability and ^{3}He efficiency. Today, temperatures below 4° milli-Kelvin can be achieved with the push of a button and without the use of any external liquid helium cooling.

How it works:

[5]This process relies on certain thermodynamic characteristics of ^{3}He (a rare helium isotope with 1 neutron) and ^{4}He (the most abundant helium isotope, which has 2 neutrons). The ^{3}He-^{4}He dilution has the phase diagram to the left.



At temperatures below the triple point, the ^{3}He-^{4}He mixture will separate into two liquid phases, divided by a phase boundary.

One phase we'll call the ^{3}He rich phase, because it contains mostly ^{3}He. This corresponds to a point in the diagram below and to the right of the triple point, along the equilibrium line.

The second phase we'll call the ^{4}He rich phase, because it is mostly ^{4}He -- it will, however, always be composed of at least 6% ^{3}He, no matter what temperature. This corresponds to a point in the diagram below and to the left of the triple point, along the equilibrium line.

The two phases are maintained in liquid-vapor form. Since there is a boundary between both phases, extra energy is required for particles to go from one phase to another.

A good example of this state would be what happens when you mix together oil and water. If you maintain the mixture at a high temperature they will stay mixed. But, if you were to lower the temperature (this effect can be seen at room temperature) the oil would separate from the water and float to the top, giving you two different phases in the liquid mixture. Not only that, but if you were to take a sample of the oil you would find a small amount of water present and vice-versa.

When you pump (in this case, a rotary pump is used) on the ^{4}He rich phase you will remove mostly ^{3}He (a move to the left off the equilibrium line in the diagram), destroying the equilibrium. To restore equilibrium, ^{3}He will have to cross the phase boundary from the ^{3}He rich side to the ^{4}He rich side. However, it needs energy to get past the boundary. The ^{3}He rich phase will provide the ^{3}He and get the energy in the form of heat, from the walls of the mixing chamber; the walls are in thermal contact with whatever you're trying to cool. Then the ^{3}He will cross the

---

[4] Graham Batey and Gustav Teleberg, “Principles of dilution refrigeration” (2015), http://www.oxford-instruments.cn/OxfordInstruments/media/nanoscience/Priciples-of-dilution-refrigeration_v14.pdf

[5] Geoffrey Nunes Jr., and Keith A. Earle, “Cooling and Cryogenic Equipment.” Page 45. http://cdms.berkeley.edu/UCB/75fridge/inxsrc/dilution/

phase boundary and join the ^{4}He rich phase, restoring equilibrium. Finally, the atoms lost by the ^{3}He rich phase are replenished by a constantly circulating flow of ^{3}He.

Another way of thinking about this process is in terms of expansion. ^{4}He is inert, in that it does not react with other molecules and thermodynamically can be thought of as a vacuum in some situations. Thus, when the ^{3}He moves from the ^{3}He rich phase to the ^{4}He rich phase, it expands into an almost vacuum. This expansion takes heat out of the walls of the mixing chamber, reducing the temperature of whatever you're trying to cool.

8. Methods of Communicating with Qubits

No matter what technology is used to create the physical qubits of a quantum computer, for the computer to function, the qubits have to communicate with the outside world and with classical computer electronics. However, due to the nature of quantum effects, almost any direct communication with the qubit will alter or destroy the state of the qubit. Much research has and is being conducted on methods to determine the state of a qubit without changing the state. Research is being conducted into special phenomenon of quantum physical. For example, a fluxon directed to pass near a qubit will change speed depending on the state of qubit and that change in speed can be measured. One key restriction on the method used to communicate with a qubit is based on the heat the method introduces into the quantum computer. The qubit hardware must operate at just a few thousands of a degree above absolute zero. Any method of communicating with a qubit must minimize the injection of thermal energy into the system and not overwhelm the cooling systems ability to reject it. This is an area that is still undergoing change and research continues.

9. Physical Qubits

A qubit is the smallest unit of information in a quantum computer. It can represent a 1 or 0 or when in superposition any value in between. In addition, a qubit can be entangled with another qubit. A qubit can be physically implemented in many different ways as long as the implementation harnesses the quantum effects of subatomic particles. For example, the energy levels and quantum characteristic of an electron in orbit around an atom can be used to create a qubit as can the polarization of photon. In most cases, the intrinsic angular momentum or spin is used to create the qubit. Therefore, elementary particles and composite particles, which have measurable spin, are possible candidates for technology that implements a qubit.

9.1.1. Types of Physical Qubits

9.1.1.1. Superconducting Loop

A qubit based on this technology is constructed using a superconducting metal loop with near zero resistance where a current oscillates back and forth on the loop. Microwave signals directed into the circuit excites the current into superposition states.

Companies that use this technology: Google, IBM and Quantum Circuits

Longevity (seconds): 0.00005

Logic Success Rate: 99.4%

Number Entangles: 9

Pros: Built on existing semiconductor technology and processes. Relatively mature technology.

Cons: Must operate a near absolute zero. Low coherence times

9.1.1.2. Trapped Ions

This technology is based on the manipulation of ions to create a qubit. An ion is an atom that has had an electron removed making the atom electrically charged which means electromagnetic fields can be used to confine or trap the ion. Heat is typically applied to strip electrons from atoms to create ions. Then specially tuned lasers are used to cool and move the ions to a trap. Once trapped, qubit information is stored in stable electronic states of an ion. In March of 2018, researchers at Oxford University set a new speed record for logic gates based on trapped ion technology.[6]

Companies that use this technology: ionQ

Longevity (seconds): >1000

Logic Success Rate: 99.9%

Number Entangles: 14

Pros: Very stable. Highest achieved gate fidelities

Cons: Slow operation. Many lasers are needed[7]

9.1.1.3. Silicon Quantum Dots

Quantum dots are "artificial atoms" made by adding an electron to a small piece of pure silicon. Microwaves are used to control the electron's quantum state.

Companies that use this technology: Intel

Longevity (seconds): 0.03

Logic Success Rate: 99%

Number Entangles: 2

Pros: Stable. Built on existing semiconductor technology

Cons: Must operate at near absolute zero and has limited entanglements[8]

9.1.1.4. Topological

This is a newer less investigated technology that is based on quasiparticles. These are particle-like objects that emerge from the interactions inside of matter. They are called non-abelian anyons. Using

---

[6] University of Oxford, "New speed record for trapped-ion 'building blocks' of quantum computers" https://phys.org/news/2018-03-trapped-ion-blocks-quantum.html

[7] Gabriel Popkin, Science Magazine, "Scientists are close to building a quantum computer that can beat a conventional one", Dec. 1, 2016, https://www.sciencemag.org/news/2016/12/scientists-are-close-building-quantum-computer-can-beat-conventional-one

[8] Gabriel Popkin, Science Magazine, "Scientists are close to building a quantum computer that can beat a conventional one", https://www.sciencemag.org/news/2016/12/scientists-are-close-building-quantum-computer-can-beat-conventional-one

quasiparticles, quantum states can be created that are very robust and can withstand external interference.[9]

Companies that use this technology: Microsoft

Longevity (seconds): N/A

Logic Success Rate: N/A

Number Entangles: N/A

Pros: Greatly reduces errors

Cons: Still experimental. Yet to be fully confirmed[10]

9.1.1.5. Quantum Annealing

Annealing involves a series of magnets that are arranged on a grid. The magnetic field of each magnet influences all the other magnets—together, they flip orientation to arrange themselves to minimize the amount of energy stored in the overall magnetic field. You can use the orientation of the magnets to solve problems by controlling how strongly the magnetic field from each magnet affects all the other magnets. This was first demonstrated on a 16-qubit quantum device on February 13, 2007.[11]

Companies that use this technology: D-Wave

Longevity (seconds): N/A

Logic Success Rate: N/A

Number Entangles: N/A

Pros: Has a large number of qubits, >512

Cons: Has low entanglement. Not considered a fully capable quantum computer[12]

---

[9] Elizabeth Gibney, Nature Magazine, "Inside Microsoft's quest for a topological quantum computer", https://www.nature.com/news/inside-microsoft-s-quest-for-a-topological-quantum-computer-1.20774

[10] Gabriel Popkin, Science Magazine, "Scientists are close to building a quantum computer that can beat a conventional one", https://www.sciencemag.org/news/2016/12/scientists-are-close-building-quantum-computer-can-beat-conventional-one

[11] Chris Lee, Ars Technica Magazine, "Explaining the upside and downside of D-Wave's new quantum computer", 1/26/2017, https://arstechnica.com/science/2017/01/explaining-the-upside-and-downside-of-d-waves-new-quantum-computer/

[12] Gabriel Popkin, Science Magazine, "Scientists are close to building a quantum computer that can beat a conventional one", https://www.sciencemag.org/news/2016/12/scientists-are-close-building-quantum-computer-can-beat-conventional-one

9.1.1.6. Diamond Vacancies

Diamond vacancies qubits result from the combination of "vacancies," which are locations in the diamond's crystal lattice where there should be a carbon atom but there isn't one, and "dopants," which are atoms of materials other than carbon that have found their way into the lattice. Together, the dopant and the vacancy create a dopant-vacancy "center," which has free electrons associated with it. The electrons' magnetic orientation, or "spin," which can be in superposition, constitutes the qubit.

A perennial problem in the design of quantum computers is how to read information out of qubits. Diamond defects present a simple solution, because they are natural light emitters. In fact, the light particles emitted by diamond defects can preserve the superposition of the qubits, so they could move quantum information between quantum computing devices. [13]

Companies that use this technology: Quantum Diamond Technologies

Longevity (seconds): 10

Logic Success Rate: 99.2%

Number Entangles: 6

Pros: Can operate at room temperature

Cons: Difficult to entangle[14]

9.1.2. Stability of a physical Qubit

Using current technology, physical qubits are required to operate as close to absolute zero (459.67 degrees Fahrenheit) as possible to stop or slow the movement of atoms. Refrigeration systems can cool the hardware of a quantum computer to a few thousands of a degree above absolute zero. However, this still allows for thermal noise to enter the system. In addition, electro-magnetic noise can also enter the system. These sources of noise negatively affect the stability of a physical qubit. With current technology, external noise will cause a physical qubit to become unstable and loss coherence in less than a second. Once unstable, a physical qubit cannot be used for computation and must be reset. If the technology used for physical qubits cannot be improved to create long term stable qubits then logical qubits must be developed that exhibit long term stability.

9.1.3. Maximum Number of Physical Qubits Currently Available

The largest quantum computer currently has 72 physical qubits. Google has developed this computer. This is the largest published computer. It is believed that larger quantum computers exist but their information has not been published. It is believed that quantum computers with around 100 physical qubits may exist.

9.2. Logical Qubits

A logical qubit is a stable qubit that can be used for programming and that exhibits all the quantum phenomena of a physical qubit including superposition and entanglement. A logical qubit has long term coherence times that are at least measured in hours if not days.

---

[13] Larry Hardesty, MIT News Office, "Toward mass-producible quantum computers", May 26, 2017, http://news.mit.edu/2017/toward-mass-producible-quantum-computers-0526

[14] Gabriel Popkin, Science Magazine, "Scientists are close to building a quantum computer that can beat a conventional one", https://www.sciencemag.org/news/2016/12/scientists-are-close-building-quantum-computer-can-beat-conventional-one

10. An Overview of Current Quantum Computer Programs

The follow table includes information on current efforts to develop a quantum computer.

Company	IBM	Google	Microsoft	D-Wave
Qubit Type	Super-conducting	Super-conducting	Majorana Fermions	Quantum Annealing
Operating Temp	10-15 mK	NA	10-15 mK	15 mK
Max. # of Qubit	50	72	NA	>2000
Coherence Time	90 µsec	NA	NA	NA
Error Correction	NO	NA	NA	NO
Qubit Entanglements	NA	NA	NA	NA

Note: D-Wave is not considered a full quantum computer. It does use certain features of a quantum computer but not all.

11. Problems to be solved before a large-scale, fault-tolerant QC can be created

Introduction:

A central goal of today's research into quantum computing is the development of a quantum computer with a large number of physical qubits. The definition of the term "large" varies but it is generally thought to be a number between several thousand qubits and tens of thousands of qubits. As long as the coherence time of a physical qubit is measured in seconds or fractions of a second, some type of error correction will be required to extend the continuous operating time of a qubit to at least minutes with a goal of hours or days. Research is current looking at creating stable logic qubits that would have coherence times measured in hours and possible days. Multiple physical qubits will be needed to create a single logical qubit. Therefore, there is a need to scale today's technology for creating a qubit by a factor of as much as 100.

11.1. Cooling Issues

As already discussed in this paper, most of the technology used today to create a qubit must operate at near absolute zero to function. The hardware to create 70 to 80 qubits (today's largest computer) will fit in a container that would hold approximately 100-200 gallons of water. Current cooling technology is adequate to lower a volume of this size to near absolute zero. However, as the computer powers up and operates, maintaining a temperature near absolute zero is difficult or impossible. A linear scaling of the electronics by a factor of 100 would require a volume of space that would hold 10,000 to 20,000 gallons of water. Today's cooling systems cannot cool a volume of this size to near absolute zero. The good news is that volume of space to be cooled to create a computer with thousands of qubits will not go up by a factor of 100 because the electronics to create a qubit will shrink in size. However, the volume will increase and cooling technology must improve in both the volume of space that can be cooled and uniformity of the temperature across the volume of space. This is an issue that must be solved.

11.2. Scaling of Electronics

Numerous technologies are in use today to create a physical qubit. Some can be created using the same manufacturing processes that are used to create a standard silicon wafer. Additionally, some of these technologies can be reduced in size and scaled up while using the same size footprint. However, the heat generated will increase and thus put an additional load on the cooling system. There is a believe that the technology that will allow large numbers of physical qubit to be created and packaged in a very small volume of space has not yet to be identified. This is a major problem to solved.

11.3. Error Correction (Logical Qubit)

A logical qubit must be stable, have a coherence time measured in hours or days and operate error free with all the quantum features of a physical qubit. Research into how create such a logical qubit is ongoing but the goals have not been achieved. This is a problem that must be solved if large scale quantum computers are to be created.

12. Quantum computing research Centers

The follow companies, universities or countries have research centers or are conducting research into quantum computing technology. There may by others but these are the one we know about.

12.1. China - National Laboratory for Quantum Information Sciences

12.2. Google

12.3. Holland (Intel) - Quantum Research Institute of Delft University of Technology

12.4. IBM

12.5. Intel

12.6. Microsoft

12.7. Russia - Russian Quantum Center

12.8. United States – Los Alamos National Laboratory

12.9. University of Maryland

12.10. University of Waterloo

13. NIST Work on Quantum-Resistant Cryptography

Cryptographic primitive (such as those from section 6.1) make the assumption that certain mathematical problems (such as factoring numbers) are hard. A primitive is only as strong as its “hardness assumption.” The problem is that, as we have seen in subsection 6.2.2, factoring a number N is *not* hard for a quantum computer. Briefly, this is because a quantum computer can find the period of any number under multiplication mod N, and that allows us to factor N. More generally, any cryptographic primitive that can be broken by *period-finding* (i.e., by determining

the size of the set $\{x^k\}$ for a given multiplicative element x) is a primitive that is gravely vulnerable to quantum computers. Both RSA and ECC are examples of such primitives.

Post-quantum cryptography is the study of cryptographic primitives that are believed to be secure against quantum computers. In order to construct such primitives, we have to identify mathematical problems that are hard not only for classical computers, but for quantum computers as well.

One potential example of a hard problem is the **shortest-vector problem.** Suppose that we have a small collection of long binary strings of the same length:

```
001101001001110110100010001 … 01100
110100101101111000101011110 … 00101
001010111010100010111111001 … 11010
      …
111110010111000100011101000 … 01010
```

Suppose that we choose a subset of these strings and add them, mod 2, using the rules 0+0=0, 0+1=1+0=1, and 1+1=0. Can we find such a subset whose sum contains only a very small number of 1's (in other words, a subset whose sum is a vector of small "weight")? Problems such as this underlie **code-based cryptography. Lattice-based cryptography** is similar, except that a larger modulus is typically used (i.e., we consider strings of remainders mod n) and the notion of weight is more complicated.

Another type of problem is solving multivariate polynomial systems. Suppose that we have a function, e.g.,

F (x, y, z) = (xy + yz , x + z, xz , x + y + 1).

which takes binary strings of length *n* to binary strings of length *m* using polynomials mod 2. *Inverting* this function would mean solving for x, y, and z given all of the values on the righthand side of the equation. When multivariate functions such as this are moderately complicated – such as having hundreds or thousands of terms – they are believed to be very hard to invert. **Multivariate cryptography** is based on this type of hardness assumption.

13.1. NIST Post-Quantum Cryptography Standardization

The goal of the NIST Post-Quantum Cryptography project[15] is to standardize new cryptography primitives that can replace RSA and that are resistant to attacks by quantum computers. This is a global effort that began at the end of 2016. Proposals were invited from the cryptography community for new public-key cryptography primitives, specifically addressing three tasks: **encryption, digital signing,** and **key exchange.**

The deadline for receipt of proposals for the NIST PQC was in December 2017. About 70 of the proposals were judged to be "complete and proper," and were placed on NIST's website for public comment. A conference was held by NIST in April 2018 in which all authors were invited to present their work.[16] Another such conference will be held in late 2019.

Candidate protocols are being evaluated based on the cryptographic community's confidence that they will be secure in the long term, and also based on performance (key size, ciphertext size, speed). The goal of the PQC project is to standardize a small number of cryptographic protocols for public use. The projected timeline for the project is 4-6 years.

[15] https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization

[16] https://csrc.nist.gov/events/2018/first-pqc-standardization-conference

In parallel, NIST is also looking to standardize stateful hash-based signatures[17]. Hash-based signatures are an old and very well understood idea that are resistant to quantum computers because they only rely on the non-invertibility of secure hash functions. The downside is that only a finite number of signatures can be made with a particular private key, and the private keys are very large. The advantage is that such schemes are more mature and can be deployed today. They are particularly well suited for code signing use cases, and for root and intermediate certificates that need to be embedded in devices with long lifetimes. There are two very similar systems, based on eXtended Merkle Signature Scheme (XMSS) and Leighton-Micali Signature (LMS)[18]. These specifications will be completed much earlier and can be used to deploy more advanced quantum safe algorithms once they are available.

13.1.1. NIST Post-Quantum Cryptography Standardization Timeline

Feb 24-26, 2016 NIST Presentation at PQCrypto 2016: Announcement and outline of NIST's Call for Submissions (Fall 2016), Dustin Moody

April 28, 2016 NIST releases NISTIR 8105, Report on Post-Quantum Cryptography

Dec 20, 2016 Formal Call for Proposals

Nov 30, 2017 Deadline for submissions

Dec 4, 2017 NIST Presentation at AsiaCrypt 2017: The Ship Has Sailed: The NIST Post-Quantum Crypto "Competition", Dustin Moody

Dec 21, 2017 Round 1 algorithms announced (69 submissions accepted as "complete and proper")

Apr 11, 2018 NIST Presentation at PQCrypto 2018: Let's Get Ready to Rumble - The NIST PQC "Competition", Dustin Moody

April 11-13, 2018 First PQC Standardization Conference - Submitter's Presentations

2018/2019 Round 2 begins

August 2019 Second PQC Standardization Conference

2020/2021 Round 3 begins for select algorithms

2022/2024 Draft Standards Available[19]

13.2. NIST Announces Second Round Candidate (1/30/2019)

On January 30, 2019, NIST issued an announcement that it had selected 26 algorithms that would advance to the post-quantum crypto Semifinals evaluation[20]. NIST also published an article about candidates and the process[21]. See the footnote for more details on the NIST Post-Quantum Project[22]. A part of the announcement is listed below.

After over a year of evaluation, NIST would like to announce the candidates that will be moving on to the 2nd round of the NIST PQC Standardization Process.

---

[17] https://groups.google.com/a/list.nist.gov/d/msg/pqc-forum/WN3MJoe1RKQ/q0f462p9BgAJ

[18] https://eprint.iacr.org/2017/349.pdf

[19] NIST web site. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Workshops-and-Timeline

[20] NIST web site, https://csrc.nist.gov/news/2019/pqc-standardization-process-2nd-round-candidates

[21] NIST web site, https://www.nist.gov/news-events/news/2019/01/nist-reveals-26-algorithms-advancing-post-quantum-crypto-semifinals

[22] NIST web site, https://csrc.nist.gov/projects/post-quantum-cryptography

The 17 Second-Round Candidate public-key encryption and key-establishment algorithms are:

- BIKE
- Classic McEliece
- CRYSTALS-KYBER
- FrodoKEM
- HQC
- LAC
- LEDAcrypt (merger of LEDAkem/LEDApkc)
- NewHope
- NTRU (merger of NTRUEncrypt/NTRU-HRSS-KEM)
- NTRU Prime
- NTS-KEM
- ROLLO (merger of LAKE/LOCKER/Ouroboros-R)
- Round5 (merger of Hila5/Round2)
- RQC
- SABER
- SIKE
- Three Bears

The 9 Second Round Candidates for digital signatures are:

- CRYSTALS-DILITHIUM
- FALCON
- GeMSS
- LUOV
- MQDSS
- Picnic
- qTESLA
- Rainbow
- SPHINCS+

14. Standardization Process for Post-Quantum Cryptography

- 3 years for NIST to complete review of quantum safe algorithms (started in November 2017)
- 4-6 year from now for NIST Standards to be released.
- 3-5 years to produce new industry standards based on NIST algorithms from NIST Standards
- 5-7 years for the industry to fully implement the new industry standards
- Full industry adoption could take 20 years from now.

15. Guidelines for Immediate Steps that can be taken

- Upgrade to AES, preferably AES-256
- Use SHA-512 for hashing
- Use stateful hash-based signatures for signing, especially for protecting upgrades of firmware/cryptographic software
- Use hybrid cryptography to protect against both weaknesses in RSA/ECC and potential weaknesses in post-quantum algorithms

15.1. Protecting Data in Transit

As of 2018, there were no large-scale quantum computers capable of cryptographic attacks. However, the lack of a quantum computer does not imply that bad actors cannot prepare to mount quantum-aided attacks. While the attacks themselves may not be possible to launch as of 2018, preparations can be made to more easily launch them when a large-scale quantum-computer becomes available. For example, attackers can copy data

in transit and store it until they can use a quantum computer to decrypt it. This is often referred to as “harvest & decrypt”. Such attacks are viable against many of the most commonly used secure communication protocols including: TLS, IPsec/IKEv2, SSH, CMS[23], and Signal. These vulnerabilities then affect applications such as VPN, secure internet communication, or secure voice/video. Attacks such as these are especially damaging in situations where the obligation of confidentiality extends past the time when large-scale quantum computers become available.

At present, the future harvest & decrypt style attacks may be mitigated by deploying hybrid classical/quantum-safe cryptosystems. The idea behind hybrid cryptosystems is to combine a classical cryptographic algorithm with a quantum-safe cryptographic algorithm in the same system or subsystem. Hybridization is particularly attractive for key establishment and digital signatures. A hybrid signature scheme might combine a classical and a quantum-safe signature algorithm so that both signatures must be verified for the signature to be accepted. A hybrid key establishment protocol might derive a key from secret materials produced by both a classical and a quantum-safe algorithm.

Hybrid-derived keys can be used to encrypt data before it is transmitted. This way a successful attacker would need to break both the quantum and classical key establishment protocols to recover the key. Signed data for which the signature must be valid for a long period of time can be signed today with a hybrid signature scheme. This way, even if the classical portion is broken by a quantum computer later on, the quantum-safe portion remains secure and valid.

Moreover, as noted in FAQ 001 of the NIST PQC Call For Proposals, if a NIST approved, FIPS validated classical key establishment algorithm or signature scheme is combined with a quantum-safe algorithm the FIPS validation on the classical component remains valid. This is then a reasonable initial step to migrate systems to use quantum-safe cryptographic primitives.

Working Groups within the Internet Engineering Task Force (IETF) have been making proposals to modify existing standards to allow some form of hybrid construction. Examples include using (Post-Quantum) Pre-Shared Keys in CMS (18) and IKEv2 (19).

15.2. Protecting Software Updates

Upgrading systems to use quantum-safe cryptography can be a major challenge. While some of the urgency to upgrade systems comes from the immediate threat of harvest & decrypt, other urgency comes from the costs and complexity of upgrading systems now versus later. Many of the systems we rely upon today, including critical systems like infrastructure, medical, automobile or financial systems, rely on software updates to maintain security. Long-lived systems are sold with embedded roots of trust which are used to authenticate software updates and are going to be in-field beyond the time large scale quantum computers are expected to arrive. If we don’t start embedding quantum-safe roots of trust today, we will have to manually update each system later in order to update these roots of trust—this may involve physically visiting and updating the systems. In most cases this will be logistically impossible or financially prohibitive.

There exist mature digital signature options that we can start using today. The stateful hash-based signature scheme XMSS has been recently approved by the Internet Research Task Force (IRTF) Crypto Forum Research Group (CFRG) and published as RFC 8391 (21), and the hierarchical LMS scheme is well on its way to RFC publication as well (22)**Error! Reference source not found.**. Although they are not ideal for high-f requency, high-throughput use cases, both of these schemes are quantum-safe and either of them can be used for signing updates or roots of trust in these long-lived systems.

Of particular concern to the financial services industry are Point of Sale (POS) terminals. One study estimates that the POS terminal industry will be worth over 116 billion USD by 2025 (20). These devices are relatively long lived, serve an indispensable service, and require interoperability with a range of payment options. As the

[23] Technically CMS is not a protocol. Nonetheless, Harvest-and-Decrypt attacks can still be carried out against CMS messages.

desired functionality of these devices increases—such as for tap payment or payment via mobile applications—users will experience less and less interoperability between their payment methods and POS terminals unless the terminals are upgraded.

The technical limitations of current generation POS terminals might prohibit the use of hybrid or quantum-safe cryptography. In particular, these devices might not be able to support larger public-key certificates—which will be needed to support quantum-safe authentication. This may be due to memory limitations as well as processing speed requirements. As public-key roots of trust come embedded into these devices, redesign and redeployment may be necessary sooner rather than later.

15.3. Crypto-agility

Crypto-agility is a term used to describe the ability of a system or subsystem to incorporate more than one cryptographic method and quickly switch between them. In this manner, if one method is found to be broken or obsolete at some future time, the system may rely on the additional method or methods. Crypto-agility enables systems to migrate to quantum-safe cryptographic primitives quickly once a large-scale quantum computer is readily available. It is nevertheless difficult to predict when such a quantum computer would be widely available, due to many factors, including impending scientific breakthroughs that may accelerate the process. This means that systems should be prepared to make this migration on short notice. This need for a speedy migration implies that a large, system-wide overhaul might not be a viable upgrade strategy. Instead, systems should be prepared to simply remove broken legacy components and have drop-in quantum-safe components ready to replace them.

Hybrid systems should be made crypto-agile because the security of the quantum-safe components is generally less well understood than that of the classical components. Of special interest to the financial services industry is the concept of hybrid PKI. While public-key key establishment algorithms are typically negotiated between peers and are generally fairly straightforward to update, authentication systems generally rely on a single digital signature algorithm which is more difficult to update. This difficulty is largely because of the dependency between PKI-based identity systems and communication protocols.

The International Telecommunications Union Telecommunications Sector (ITU-T) has recently approved the addition of an optional feature to the next version of the existing X.509 standard enabling the use of “Multiple Cryptographic Algorithms Public-Key Certificates” (23). These certificates would allow classical and quantum-safe signatures to be used in parallel while simultaneously enabling a seamless transition to completely quantum-safe systems. Furthermore, PKIs conforming to this updated standard will be interoperable with legacy infrastructures. This is because certificates will support both quantum-safe and legacy algorithms at the same time.

PKIs can be upgraded today to use crypto-agile certificates with stateful hash-based signatures used in parallel with classic ones. These PKIs will be fully backward compatible with legacy systems, and when suitable quantum-safe primitives have been standardized by NIST, they will be ready for their dependent systems to begin migration as well. With the race to build a quantum computer and the standardize process for quantum-safe algorithms ongoing, steps like PKI migration can be done to ensure that systems are secured against quantum enabled attackers by the time a quantum computer arrives.

16. Summary of Risks from Quantum Computing

16.1. Quotes from Industry Leaders and Government Agencies

As the threat posed by quantum computing becomes more widely understood, industry and government leaders are beginning to make public comments. These are just a few of the more recent comments.

16.1.1. Arvind Krishna – Director of IBM Research

The following quote was made by Arvind Krishna while speaking at a meeting of The Churchill Club in San Francisco on a panel discussion about quantum computers in business. "Anyone that wants to make sure that their data is protected for longer than 10 years should move to alternate forms of encryption now," said Arvind Krishna, Director of IBM Research… "Quantum computers can solve some types of problems near-instantaneously compared with billions of years of processing using conventional computers." [24]

16.1.2. National Institute of Standards and Technology (NIST)

"For public key cryptography, the damage from quantum computers will be catastrophic. We must look for quantum-resistant counterparts for these cryptosystems."[25]

Dr. Lily Chen, head of the National Institute of Standards and Technology's Cryptographic Technology Group, as reported by Gizmodo[26] from the American Association for the Advancement of Science 2018 Conference.

16.1.3. Institute for Quantum Computing University of Waterloo, CA

Dr. Michele Mosca, cofounder of the Institute for Quantum Computing at the University of Waterloo, Canada, entrepreneur and contributor to this paper, argues that it isn't too early [to act now] for companies handling data that remains valuable for many years, such as medical or financial records.

Such companies need to consider the risk that an adversary could capture encrypted data and store it until the day a quantum computer can decrypt it, says Mosca. Unless some companies start engaging now with the complicated process of upgrading society's encryption, the industry won't be ready to deploy quantum-secure encryption quickly when standards bodies and governments do sign off on it, he says.

Mosca estimates a one in seven chance that by 2026 someone, likely a nation state, will have a quantum computer able to crack encryption used for critical data today. "The industry's usual recipe of waiting for catastrophe and then fixing it is very risky," he says.[27]

From academics to the National Security Agency, there is widespread agreement that quantum computers will rock current security protocols that protect global financial markets and the inner workings of government.

16.1.4. Wired online Web Site

"Already, intelligence agencies around the world are archiving intercepted communications transmitted with encryption that's currently all but unbreakable, in the hopes that in the future computing advances will turn

---

[24] **https://www.zdnet.com/article/ibm-warns-of-instant-breaking-of-encryption-by-quantum-computers-move-your-data-today/**

[25] GIZMODO, "Quantum Hacking Could be 'Catastrophic' if We Don't Develop Better Cryptography", by Ryan F. Mandelbaum, February 16, 2018. https://gizmodo.com/u-s-government-has-69-proposed-candidates-for-quantum-1823084809

[26] https://gizmodo.com/u-s-government-has-69-proposed-candidates-for-quantum-1823084809

[27] MIT Technology Review, "Quantum Computing Paranoia Creates a New Industry" by Tom Simonite, January 30, 2017. https://www.technologyreview.com/s/603424/quantum-computing-paranoia-creates-a-new-industry/

what's gibberish now into potentially valuable intelligence. Rogue states may also be able to leverage the power of quantum to attack the banking and financial systems at the heart of western capitalism."

"Everyone has seen the damage individual hackers can do when they infiltrate a system.[28] Imagine a nation-state intercepting the encrypted financial data that flows across the globe and being able to read it as easily as you are reading this. Quantum computers are so big and expensive that—outside of global technology companies and well-funded research universities—most will be owned and maintained by nation-states. That means the first" quantum attacks are likely to be organized by countries hostile to the US and our allies. Rogue states could read military communiques the way the United States and its allies did after cracking the Nazi Enigma codes."

"The window is closing, fast. It took more than five years and nearly half a trillion dollars for companies and governments to prepare for Y2K, which resulted in a non-event for most people. But, the US is not ready for what experts call Y2Q (Years to Quantum), and the time to prepare is now. Even in a pre-quantum era, the need for quantum-safe encryption is real. Banks, government agencies, insurers, hospitals, utilities, and airlines all need to be thinking now about how to implement security and encryption that will withstand a quantum attack." [29]

16.1.5. National Security Agency (NSA)

"Currently, Suite B cryptographic algorithms are specified by the National Institute of Standards and Technology (NIST) and are used by NSA's Information Assurance Directorate in solutions approved for protecting classified and unclassified National Security Systems (NSS). Below, we announce preliminary plans for transitioning to quantum resistant algorithms."

"IAD will initiate a transition to quantum resistant algorithms in the not too distant future. Based on experience in deploying Suite B, we have determined to start planning and communicating early about the upcoming transition to quantum resistant algorithms."

"Until this new suite is developed and products are available implementing the quantum resistant suite, we will rely on current algorithms. For those partners and vendors that have not yet made the transition to Suite B elliptic curve algorithms, we recommend not making a significant expenditure to do so at this point but instead to prepare for the upcoming quantum resistant algorithm transition."

"Unfortunately, the growth of elliptic curve use has bumped up against the fact of continued progress in the research on quantum computing, which has made it clear that elliptic curve cryptography is not the long term solution many once hoped it would be. Thus, we have been obligated to update our strategy."

"For those customers who are looking for mitigations to perform while the new algorithm suite is developed and implemented into products, there are several things they can do. First, it is prudent to use larger key sizes in algorithms (see the table below) in many systems (especially, smaller scale systems). Additionally, IAD customers using layered commercial solutions to protect classified national security information with a long intelligence life should begin implementing a layer of quantum resistant protection. Such protection may be implemented today through the use of large symmetric keys and specific secure protocol standards." [30]

[28] https://www.wired.com/story/russian-hackers-attack-ukraine/

[29] Wired, Quantum Computing is the Next Big Security Risk", by Will Hurd, December 7,2017, https://www.wired.com/story/quantum-computing-is-the-next-big-security-risk/

[30] Information Assurance by the National Security Agency, "Commercial National Security Algorithm Suite" https://www.iad.gov/iad/programs/iad-initiatives/cnsa-suite.cfm

16.1.6. Popular Science – China's Investment in Quantum Computing)

"On 37 hectares (nearly 4 *million* square feet) in Hefei, Anhui Province, China is building a $10 billion research center for quantum applications. This news comes on the heels of the world's first video call made via quantum-encrypted communications and the completion of a quantum-encrypted fiber optic trunk cable."

"The National Laboratory for Quantum Information Sciences, slated to open in 2020, has two major research goals: quantum metrology and building a quantum computer. Both efforts would support military and national defense efforts, as well civilian innovators. "[31]

16.1.7. The Hill Online – America's Enigma Problem with China

"In August 2016, China launched the first quantum satellite called Micius[32]. The satellite conducted the first two-way video call using physics — not math — to secure the conversation[33] in August 2017. The conversation was secured by a secret key generated by quantum entanglement[34]."

"This isn't Skype on Steroids. This is much worse. It's about physics. And really big and powerful computers. And lots of money."

"There is no way to "eavesdrop" and listen in. No way to siphon off the message traffic by tapping the line. We will be completely blind. And with quantum encryption, our adversaries will absolutely know we're trying to listen in."[35]

---

[31] Popular Science Online, "China is Opening a New Quantum Research Supercenter" by Jeffrey Lin and P.W. Singer, October 10, 2017. https://www.popsci.com/chinas-launches-new-quantum-research-supercenter

[32] http://www.bbc.com/news/science-environment-40294795

[33] https://www.cnbc.com/2017/08/10/china-uses-quantum-satellite-to-transmit-potentially-unhackable-data.html

[34] https://www.technologyreview.com/s/610106/chinese-satellite-uses-quantum-cryptography-for-secure-video-conference-between-continents/

[35] The Hill, "America's Enigma Problem with China: The Threat of Quantum Computing", by Morgan Wright, March 5, 2018, http://thehill.com/opinion/national-security/376676-americas-enigma-problem-with-china-the-threat-of-quantum-computing

17. Conclusions

Quantum computing was first postulated in the 1950s. For the first 35 years research was slow, but after Dr. Peter Shor published a quantum algorithm that would break certain types of cryptography, research into the development of quantum computers started to accelerate. Nations such as China are now spending billions of dollars developing quantum computers and related technology. Large multinational companies like Google and IBM are developing quantum computing technology and have built working, small-scale quantum computers. All known quantum computers that exist in the world today have fewer than 100 physical qubits. Some of these may be able to perform limited work towards solving real world problems, however, most of these computers support coherent operations that are measured in fractions of a second. Work is progressing to realize a stable logical qubit that will have coherent operations that are measured in hours or days. These logical qubits will comprise multiple physical qubits. Therefore, the technology that will support thousands of stable logical qubits may need to be able to scale to 10,000 physical qubits or more.

For decades, the central question was whether the physics and engineering hurdles surrounding the development of a quantum computer could even be overcome. In recent years, the question has changed from “if a large-scale quantum computer can be created” to “when such a computer will be created”. The general feeling is that it could take fifteen to twenty years, at current funding levels, to develop a stable multi-thousand qubit quantum computer. At least one industry leader believes that a World War II style Manhattan Project could reduce the time to five to ten years. Such a project would have a cost in the range of $25 billion dollars. The probability of such a project is small but projects with lower funding levels are likely. China has recently allocated approximately $15 billion to the development of large quantum computers. It is more likely than not that other countries or commercial entities not wanting to be left behind will also increase their spending. These economic factors should reduce the time to develop a working large-scale quantum computer.

It is common to see headlines about quantum computing that focus on the number of qubits in a new quantum computer. This would lead one to think the only race is to create quantum computers with more and more qubits. While the number of qubits is an important metric for judging the capabilities of a quantum computer, and perhaps many thousands of them will be needed, the stability of the qubits is as, or even more, important at this time. There are a number of technologies used to create a qubit today but they all suffer stability issues. Most have stability (coherence) times that are less than a second. That means the qubits lose their entangled state and return to being independent in less than a second; after which the computer has to be reset. One second of stable computing time is not a sufficient period of time to solve most of the problems that quantum computers are expected to solve. In most cases, minutes or hours of stable computing time will be required. It should be noted that the qubit technology that will enable the creation of a large-scale, stable quantum computer probably has not yet been invented or identified for investigation. A key future headline will be one stating a breakthrough in qubit stability. If the technology used to create a stable qubit is based on or similar to existing chip fabrication techniques, it may be possible to create large numbers of qubits very rapidly once the method of constructing such a qubit is perfected.

The key take-a-way is that a large-scale, stable quantum computer is coming, probably in the next 10-15 years. As research into quantum computing expands, the number of problems not solvable by conventional computers but believed to be solvable by quantum computers is growing and creating an ever-larger demand for quantum computers. This pent-up demand is fueling the research necessary to create a large-scale, stable quantum computer.

Work has begun by government agencies and commercial companies to identify what cryptographic algorithms are jeopardized by quantum computers and to identify quantum-resistant algorithms that can replace them. NIST is almost two years into a three-year program to vet quantum-resistant algorithms. Standards organizations, like ASC X9, are ready to update current standards and/or create new standards based on quantum-resistant algorithms as soon as they are properly vetted by NIST. Examples of standards that will need to be updated to include quantum-resistant algorithms include those dealing with key blocks, PIN blocks, key derivation functions, key agreement and key transport protocols, PKIs and digital certificates, and digital signatures techniques. Companies that rely on quantum compromised algorithms should identify products that are based on quantum-resistant algorithms and make plans to migrate to them as soon as the new algorithms have successfully completed the review process.

Final standards based on quantum-resistant algorithms are an expected five to seven years away from being released to the public. In the interim period, there are some steps that companies can take. At present, it is believed that quantum computers are not exponentially faster than a classical computer in breaking symmetric cryptography

based on AES. Therefore, if AES based symmetric cryptography is not being used, upgrading to AES should be performed. This has been a recommendation for years because older symmetric algorithms, like DES, may not be sufficiently strong against future classical computers or improved mathematical techniques. If AES algorithms are being used, the current recommendation is to double the key length to account for a quantum computer's increased ability to break these algorithms.

Companies tend to think in terms of real-time hacking of the data. At some point when large scale, stable quantum computers are in play, this will be possible. However, it should be remembered that the cost to store data today is cheap. If encrypted data stored today could be decrypted by a quantum computer in ten years, and if the data, or at least some of it, will still be sensitive in ten years, then there is a problem.

X9 will continue to update this whitepaper as major milestones in the development of a large-scale quantum computer occurs. You can follow work on quantum computing and the work on quantum-resistant standards at the following X9 web site: https://x9.org/quantum-computing.

Annex A

Bibliography

1. A Primer of Payment Security Technologies: Encryption and Tokenization, First Data Corporation, 2011. https://www.firstdata.com/downloads/thought-leadership/primer-on-payment-security-technologies.pdf
2. Cryptography in the Age of Quantum Computing, Joyrene Thomas on January 2, 2018 Daily News, Issuing & Acquiring, http://www.paymentscardsandmobile.com/cryptography-age-quantum-computing-2/
3. IBM Q, presentation by Ingolf Whittman, Technical Director, to Accredited Standards Committee X9 – Financial Services on February X, 2018.
4. Six Things Everyone Should Know about Quantum Physics, Forbes, 2008, https://www.forbes.com/sites/chadorzel/2015/07/08/six-things-everyone-should-know-about-quantum-physics/#7fac4f2a7d46
5. The Bloch Sphere, Ian Glendinning, EUROPEAN CENTRE FOR PARALLEL COMPUTING AT VIENNA, QIA meeting , TechGate, February 16, 2005
6. https://www.hudson.org/
7. https://www.economist.com/technology-quarterly/2017-03-09/quantum-devices#s-3
8. https://www.hudson.org/research/13969-the-computer-that-could-rule-the-world
9. ASC X9 TR-37-2010, Migration from DES, https://webstore.ansi.org/RecordDetail.aspx?sku=ASC+X9+TR-37-2010
10. Brute Force: Cracking the Data Encryption Standard, Matt Curtin, ISBN 0-387-20109-2 ©2005
11. X3.32 Data Encryption Algorithm (DEA) in 1981
12. TG-24-1999 Technical Guideline #24: Managing Risk and Migration Planning: Withdrawal of ANSI X9.9, Financial Institution Message Authentication Codes (MAC) Wholesale
13. TG-25-1999 Technical Guideline #25: Managing Risk and Migration Planning: Withdrawal of ANSI X9.23, Encryption of Wholesale Financial Messages
14. TG-26-1999 Technical Guideline #26: Managing Risk and Migration Planning: Withdrawal of ANSI X9.17, Financial Institution Key Management (Wholesale)
15. FIPS 46-3 Data Encryption Standard
16. What Is Quantum Computing? A Super-Easy Explanation For Anyone – Forbes, July 4, 2017 http://www.forbes.com/sites/bernardmarr/2017/07/04/what-is-quantum-computing-a-super-easy-explanation-for-anyone/#55ace3941d3b
17. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/faqs
18. https://datatracker.ietf.org/doc/draft-housley-cms-mix-with-psk/
19. https://datatracker.ietf.org/doc/draft-ietf-ipsecme-qr-ikev2/
20. https://www.grandviewresearch.com/press-release/global-point-of-sale-terminals-market
21. https://datatracker.ietf.org/doc/rfc8391/
22. https://datatracker.ietf.org/doc/draft-mcgrew-hash-sigs/
23. https://datatracker.ietf.org/liaison/1541/