Cryptography in a Post-Quantum World

Off to the Races

Mason Ballard

CNT 5412, Fall 2023

Abstract

Quantum computing is advancing. Promising speed and power, it has great potential to advance the world we live in while also introducing some new threats. The modern world has become increasing intertwined with the digital world including means of communication, employment, education, public health, commerce, and more. One of the main threats of post-quantum computing is its ability to break current public-key cryptography which in turn could endanger the private information of a great number of people and organizations, important critical infrastructure sectors, and critical infrastructure functions. Though NIST's updated standards are not expected to be completed and released until 2024, NIST currently has been conducting conferences and calls for papers, choosing algorithms to be standardized and recommended for use as well as collaborating with the NSA and DHS to solicit ideas and research, document decisions, and disseminate recommendations for the public and private sector. The first part of this paper will discuss what quantum computing is with particular attention it's power within cryptography. Second, we will go over the threats that such increased power will have. Third, we will go over the standards, recommendations, and guidelines in place currently. Because the standardization process is still ongoing we will discuss issues still present to address, the most recent updates gained from research or conferences, and the predicted next steps in this process and it's forward-looking impact on our world.

Summary

Information is everywhere. It is nearly a currency in our day in age. It covers the frivolous as well as the national critical, and quantum computers have the power to break the systems that currently secure it. In this paper we will discuss the background of quantum computers, the theories on which current work in the field is based, and the current and most recent developments in the field. At the end, we hope you will have a solid foundation and background to join this new "quantum movement", following the continued updates and discoveries as they come out.

Contents

1 Introduction

1.1 It's an information revolution

Information is everything. Information is ubiquitous. Information is a name, an email address, an IP address (a digital address), where you live (a physical address), a place of employment, a birthday, a file, a password, a text message, a credit card number, votes in an election, military deployment plans, and more. Information is created everyday, and it is exchanged everyday. It is interwoven with, provides guidelines for, and supports fields and domains that are simultaneously specific and private, owned and affected by the collective, as well as broadly applicable. Information science is a well-established field, and records proving its existence go as far back as the Library of Mesopotamia [29] even though the area of study did not receive its official name until about 1955 [34]. Alan Turing sought to define information science as a "universal, hardware-independent notion of computation"; whereas, Claude Shannon sought to define information science as a "universal, meaning-independent notion of communication". Oxford Languages defines **information science** as:

> "a broad and interdisciplinary field that studies how information is created, collected, organized, stored, retrieved, and used by humans and machines. It also examines the social, ethical, legal, and cultural aspects of information and its impact on society." [6]

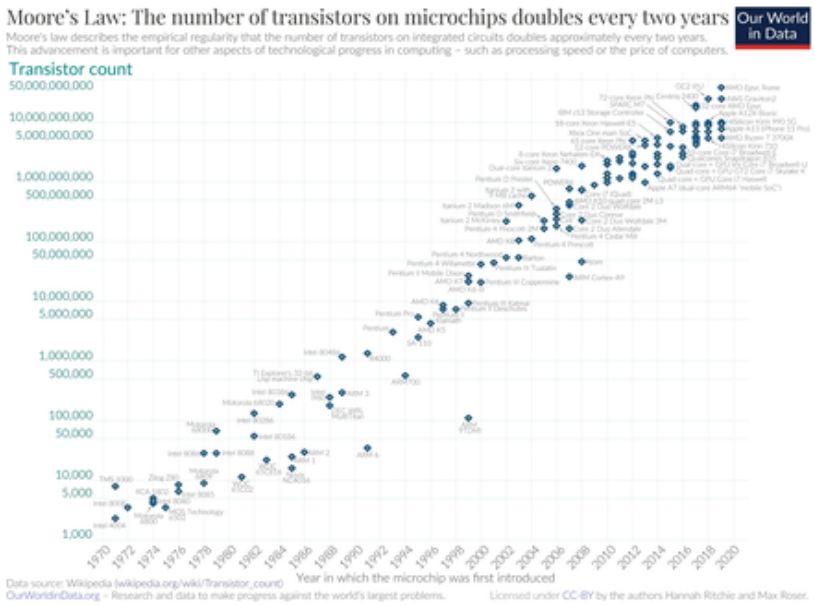

Figure 1: Moore's law is the observation and subsequent prediction the number of transistors per microchip will double every two years

The **information revolution** brought about by the advent of computers and the speed of its growth is quickly summarized using **Moore's law**. Originally published in Electronics Magazine in 1965, Gordon Moore predicted "the number of transistors per square inch on a microchip would double each year while the manufacturing cost per component would halve" [3]. This was revised a decade later to state "chip density would...double every two years for at least the next decade " [3].

Up until now, Moore's law has quite faithfully remained true, much to Moore's own surprise, made possible because engineers were able to continually develop smaller and smaller transistors. Well-known and regarded as a general rule rather than just a theorem in information science, its veracity has exceeded the predicted ten-year lifetime by more than thirty years as illustrated in Figure 1, but all good things must come to an end. As of 2016, the smallest transistor yet is roughly the same thickness as a single layer of carbon atoms [75]. Sarah Yang from the Berkeley National Lab remarked in "Smallest transistor ever made by Berkeley Lab" that transistors reaching the atomic scale may be the end of Moore's law as we know it, but maybe the end of one chapter is just the beginning of another.

1.2 Time for a quantum revolution: The future is... now?

The study of quantum mechanics goes all the way back to the early 1800s [87]. Essentially the physics of small things [82], the field of quantum mechanics paved the way for the field of quantum computing. When Stephen Wiesner invented conjugate coding in 1965 [85], this marked the beginning of quantum communication and computation and, arguably, a brand new information revolution. Whereas the invention of the classical computer spurred on the growth of the field of information science and provided the foundation for areas of study such as classical communication, computation, and cryptography, the invention of the quantum computer (**QC**) has great promise to do the same.

In an article as recent as October 2023, a quantum computer boasting a record-breaking 1,180 qubits was build by tech startup Atom Computing [71]. This broke IBM's standing record with their quantum computer, Osprey, having a, what now seems small, 433 qubits (as recent as 2022) [33]. In a vein that seems vaguely familiar to Moore's law, this innovation is notable not only because it represents a rapid level of innovation in an unexpectedly short amount of time, this recent news may indicate that quantum computing has the power to usher in new eras of quantum communication, computation, and cryptography in much the same fashion that classical computers kick-started the information revolution beginning in the early 1980s. With quantum computers promising to be more powerful and better at solving complex problems, increased power means great potential to be used for good or bad.

As an example, Shor's 1994 algorithm promises to be able to effectively do prime factorization with "strong evidence of super-polynomial speedup" [96]. This is significant because the security

of many public-key protocols is built on the premise that multiplying two primes is very easy, but given the their product, it is difficult to find it's prime factors especially if these primes were very large. In general, an ideal property for any cryptography scheme to have is that is it easy to compute but difficult to reverse unless you know a secret piece of information, and Shor's algorithm tells us that, backed by the power of quantum computers, public-key protocols used every day by individuals, companies, and world governments for encrypting sensitive and critical data as well as providing digital signatures may be at risk of being broken, leaving the information they protect vulnerable to stealing and exploitation.

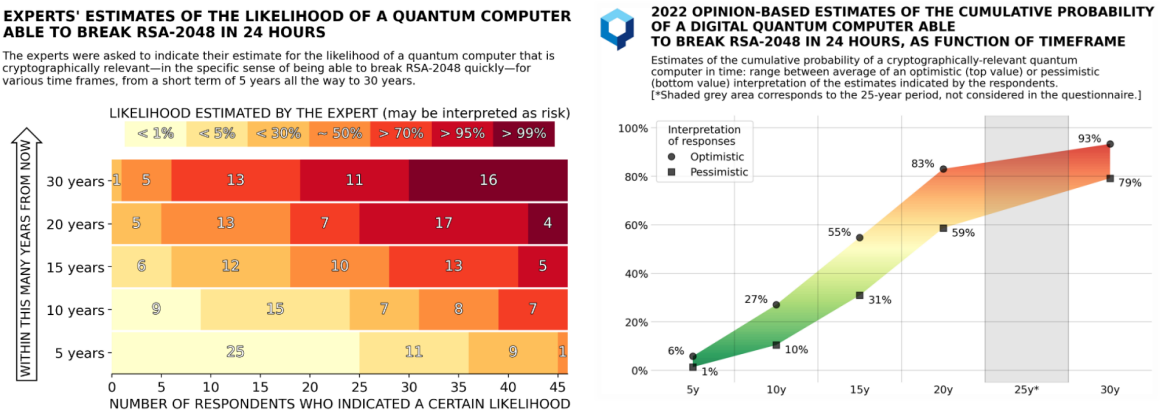

Figure 2: Mosca and Piani's 2022 survey shows estimates for when a cryptographically-relevant quantum computer may be made range from 5 to 30 years

We have already seen evidence that the quantum field is growing at a rapid pace to say the least. The threat this poses to the current security infrastructure as we illustrated is palpable. If recent developments are any indicator of where the field is going and the cadence it will maintain going forward, it is essential that developments on the defensive security side are worked concurrently, and they must try to keep pace. So far it seems that cryptographers are up to the challenge, and several exciting and interesting discoveries have come out as a byproduct of this work and research. The only question left weighing on many people minds is "how much time do we have?" which snowballs into other questions such as "do we have enough time?", "what can we reasonably expect to accomplish in the time we have?", and "if we don't have time to do everything we want, what should we prioritize?".

These very questions have received a certain amount of research of their own. Something that may cause anxiety due to the uncertainty of it all or may provide some relief is that computers capable of such computations do not yet exist; however, different researchers have tried to predict when such a computer could be expected, but have come up with answers that range from 5 to 30 years (Figure 2) [41]. Meanwhile, the US government believes that "adversarial nation-states are currently investing billions of dollars to weaponize quantum computers" [78]. In other words, we

aren't entirely sure, but doesn't mean we're clueless.

Mosca's theorem, named after renowned mathematician and computer scientist Michele Mosca, gives us a formula by which to judge such questions. More specifically it gives us a formula for us to judge how long we have to find a quantum-safe, -resistant, or -resilient solution and implement it before critical information and systems will be at risk (Figure 3).

Given:

$x \leftarrow$ shelf-life time or how long we need encryption to be secure

$z \leftarrow$ threat timeline or time until large-scale quantum computer is built

We have:

$y \leftarrow$ migration time or time we have to find a quantum-safe solution and retool existing architecture

Which tells us:

If $x + y > z$, then it's time to worry!

So we need to make sure $y < z - x$

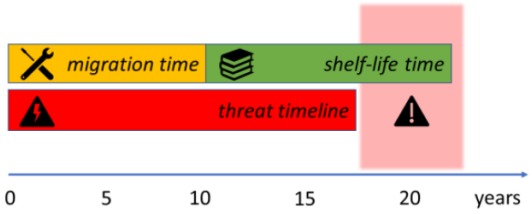

Figure 3: Mosca's theorem gives a mathematical method for conceptualizing the amount of time before quantum resistant/resilient cryptography will be necessary

Mosca's theorem goes hand in hand with a concept becoming increasingly well-known and referenced called a catch-and-exploit attack. In "Preparing Critical Infrastructure for Post-Quantum Cryptography" written and released by the Cybersecurity and Infrastructure Security Agency **CISA** (an operational component of DHS), a catch-and-exploit campaign is defined as an attack in which "adversaries capture data that has been encrypted using current encryption algorithms and hold onto such data with the intention of decrypting it when a quantum computer capable of breaking the encryption is available" [13]. This concept is important because it indicates the possibility that once a cryptographically-relevant quantum computer (**CRQC**) is made and available data assets may be at risk almost immediately, and it emphasizes the importance of updating the systems that protect and transmit this data as soon as possible.

The stakes are high, and it is under these circumstances that the US government has banded together to find a solution. While the National Security Agency (**NSA**) searches for possible solutions to protect US National Security Systems (**NSS**), the National Institute for Science and Technology (**NIST**) has been given the task finding, vetting, and standardizing quantum-safe protocols that could be used to phase out and replace systems currently in use that are most likely to be broken first once quantum computers are widely available. Meanwhile, the Department of Homeland Security (**DHS**) has been tasked with writing and disseminating recommendations for other public sector organizations (**FCEB** agencies, **SLTT** government organizations) and private sector organizations that provide any of the National Critical Functions (**NCF**s) or support the critical infrastructure (**CI**).

1.3 Cryptography in a Post-Quantum World

In this paper, we will discuss how the world of cryptography may be affected by the invention and development of quantum computers. This is an introductory discussion; therefore, we will aim to explain broad concepts using simple language. As such, the discussion will not be overly technical, but there are vast resources online which discuss the underlying implementation details, mechanics, and more taught by a variety of individual and organizations ranging from hobbyists to the inventors themselves. We will begin with an explanation of some background topics (Section 2) important to understanding the benefits and limitations of quantum computers. We will then discuss how these basic concepts backed the invention of some foundational systems in quantum cryptography (Section 3). We will briefly explain Shor's Algorithm and Grover's Algorithm to understand what they are, why they are important, and how they affect current work in the cryptographic field (Section 4). To provide a broad picture of how such work is affecting significant change in our world, we will talk about how the NSA, NIST, and DHS have been working together to secure our future (Section 5). Post-quantum cryptography standardization is an area of research still very much alive, and there is no better illustration of this than NIST's Post-Quantum Cryptography (**PQC**) Standardization Competition which we will close with in order to give readers the latest update of where the world stands in this development process, what we currently know, and where we predict it will head next (Section 6). This discussion will go back and forth between the conceptual and the tangible, leaning more and more heavily on the tangible side of things as we progress. As the discussion becomes more and more tangible and of the moment, we will try to use more and more real life examples to illustrate concepts while remaining introductory friendly. With that, it should be noted that this report cannot with any level of certainty know for sure where and how this industry and this process will conclude or when. We have sourced as many sources as possible within the given time frame to paint a picture of the work and how it currently stands as of the time of writing for the reader. It is our hope is that this paper will provide a good foundation, arming the reader with the knowledge base necessary follow this movement after the

writing of this paper, past the initial stages of standardization, and into the growth of the wider industry. Thank you for taking the time, and welcome to the quantum revolution.

2 The Basics of Quantum

In its most general form, a quantum computer is a device that stores quantum particles in a controlled environment that is controlled in a such a way that these particles can be made to do what we want [83]. QCs take advantage of fact that very small particles have unique rules and properties set out by quantum mechanics and quantum physics. In comparison with the properties of larger atoms, quantum particles seem as if they bend the rules of space and time. Acting in a seemingly random manner provable and made a little bit more predictable with mathematical properties and proofs, we use controlled environments with low temperatures, superconducting circuits, fiber optic cables, and more [39] to control quantum particles like photons in such a way that allows us to do computations on them and use them to solve problems. Where classical computers use bits in distinct zero or one states to store information and use mathematical transformations to do computations and solve problems, quantum computers use quantum bits, referred to as **qubits**. Some defining properties of qubits that make quantum computers distinct from classical computers are explained below.

2.1 Entanglement

The first unique property that quantum particles follow is that of entanglement. It is defined as thus:

> **Entanglement** is where the quantum state of each particle within a set cannot be described independently of the state of the other particles even when the particles are separated by a large distance. It has been found that position, momentum, spin, and polarization can all be perfectly correlated [95].

If we imagine qubits as particles that spin, we can compare traditional bits of zeroes and ones to qubits in a spin down state (which correlates to a natural-state of zero) and a spin up state (where this change in energy corresponds to a state of one). Entanglement tells us that given two entangled qubits, if one is spin up, and the relation between them is that they are inverses of each other, the other will be spin down, and if one changes its spin direction the other will automatically change accord to their relation. Additionally, observational research has also shown that entangled qubits are ”monogamous” [67], meaning the more entangled they are with each other, the less they will be with other qubits.

2.2 Superposition

Imagining qubits in the directly opposing spin up and spin down states, opens the door to discuss in-between states. Schrödinger's cat is a thought experiment by Edwin Schrödinger introduced in 1935, and it is commonly referenced to explain the idea of superposition:

> "A cat, a flask of poison, and a radioactive source are placed in a sealed box. If an internal radiation monitor (e.g. a Geiger counter) detects radioactivity (i.e. a single atom decaying), the flask is shattered releasing the poison which skills the cat. The Copenhagen interpretation [of quantum mechanics] implies that, after a while, the cat is simultaneously alive and dead. Yet, when one looks in the box, one sees the cat either alive or dead, but not both alive and dead." (See Figure 4) [76]

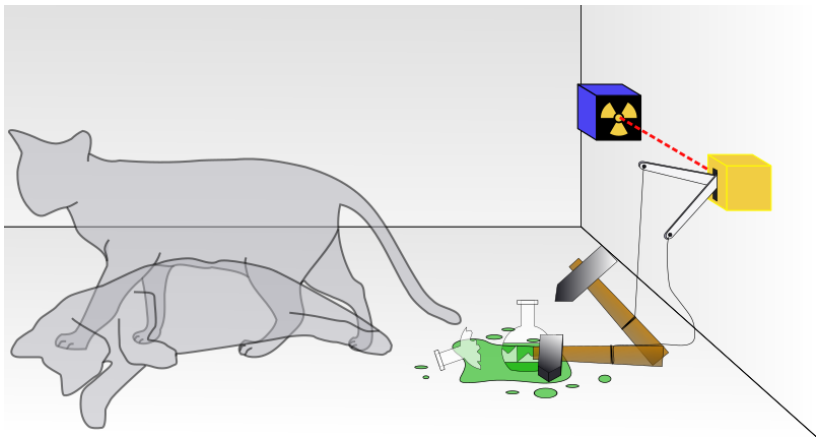

Figure 4: "Schrödinger's cat: a cat, a flask of poison, and a radioactive source connected to a Geiger counter are placed in a sealed box. As illustrated, the objects are in a state of superposition: the cat is both alive and dead." [76]

Originally intended as a criticism of how insensible the idea of superposition was, it went on to be used as a popular analogy for describing the exact principle it sought to criticize. It then went on to inspire further work that would build upon this premise. Charles Bennett explains the idea of superposition more directly:

> "Between any two reliably distinguishable states in the physical system - not all states or pairs of states are reliably distinguishable - there are intermediate states that are not distinguishable from either one, and they correspond to intermediate directions in space, and the two states are reliably distinguishable if their directions are perpendicular. Any two perpendicular directions correspond to reliably distinguishable states, and any two directions that are not perpendicular correspond to a pair of states that are different but not reliably distinguishable." [69]

Explained as simply as possible, superposition tells us that where a classical computer's bits must be a zero or one, qubits can be many things in between. Not only can it be more than two binary states, superposition tells us that in fact a qubit may be in all possible states at the same time. This increased complexity means that qubit states are often expressed using probabilities in something called **bra-ket notation** (sometimes referred to as Dirac notation).

2.3 What this means

Superposition is the main property that makes quantum computers the ideal tool to evaluate high variable, high complexity problems especially when the problem involves trying to find the best solution from a series of possible sources (an example is the traveling salesman problem) because this property allows us to store and on some level track and represent collective states rather than singular binary states. The one caveat is that reading the state of a quantum system will destroy the superposition information. This is what makes quantum computers not very good at problems that require sorting, possibly performing worse than classical computers.

Entanglement is the main property that enabled, inspired, and currently supports the field of quantum communication and its research. It is has inspired schemes such as Bennett and Brassard's BB84 communication protocol, and the way that entangled particles reliably react across long distances has enabled communication schemes that utilize this property to have near instantaneous communication across very large distances.

Beyond the basic properties of entanglement and superposition, there are a few more basic principles that limit quantum computers. The first property states that no quantum states can be cloned referred to as the no-cloning theorem. Secondly and somewhat relatedly, the exact polarization of a quantum particle or qubit or quantum state cannot be measured. Logically, being able to do one would enable the other and vice versa. These properties have posed issues when it comes to error checking and information transmission fidelity (i.e. what is sent is the same as what is received). Classical computers utilize many different schemes for error checking including parity bits, redundancy checks, and Hamming codes, and many of these involve some level of cloning. As it stands right now, quantum computers are still quite error prone due to the need to created adapted error checking schemes that don't rely on cloning. Multiple schemes have been suggested to combat this, but they have not yet been able to be implemented in a large scale way that would allow us to rigorously test their effectiveness [70].

3 Quantum Communication and Cryptography

If cryptography is the "art of secret writing" [37], then **quantum cryptography** is cryptography that takes advantage of the unique properties of quantum computers to provide confidentiality, integrity, non-repudiation, authenticity, and availability (see the CIA triad in the glossary). If

classical computers use mathematical operations to mangle and obscure data, quantum computers use quantum mechanics and physics to do the same. In this way, quantum computers' unique properties allow quantum cryptography to have built in security in ways not possible and more reliable than for cryptography done with classical computers. For example, the no-cloning theorem makes error checking and correction difficult, but it also makes quantum communication more secure. More generally, cryptography is:

> "the ability to send information between participants in a way that prevents others from reading it." [37]

To illustrate how cryptography can be made more secure using quantum computers rather than classical computers, we will introduce two common attack vectors that affect both classical and quantum cryptography, then we will use a basic quantum communication protocol to show how quantum computing can be more effective at defending against these vectors.

3.1 Common Attack Vectors

An **attack vector** is:

> "the method or combination of methods that cybercriminals use to breach or infiltrate a victim's network" [5]

Attack vectors may be individual means of accessing a network or it may be a set of tools and techniques combined to do so. Many attack vectors may be used as introductory or intermediary steps of getting into a system which means they may provide a means of compromising more security objectives than the immediate attack vector itself does.

3.1.1 Eavesdropping

Eavesdropping describes an attack where an adversary may intercept communication. It is a passive attack meaning that the information stream is not modified in any way. However, such an attack does violate the security objective of confidentiality.

3.1.2 Man-In-The-Middle (MITM)

A man-in-the-middle attack (or meddler-in-the-middle attack) is the active form of eavesdropping wherein an adversary may alter the information stream. They may "transmit their own messages, replay old messages, modify messages in transit, or delete or delay selected messages in transit" [37]. Because this attack involves an adversary reading and altering information not meant for them, it violates the security objectives of confidentiality and integrity.

3.2 Quantum Key Distribution (QKD)

The quantum key distribution method is a secure cryptographic communication protocol which allows participants to generate a shared key. This shared key may be used to privately negotiate an encryption scheme or as a one-time pad (see glossary **OTP**). Similar to the previously mentioned BB84, it is based on two principles: the Heisenberg uncertainty principle (see glossary) and the quantum property of entanglement. It works in this way:

Given:
$A \leftarrow$ the sender of some secret information
$B \leftarrow$ the receiver of some secret information

Algorithm 1 The QKD Procedure is as follows:

1: **procedure** QKD(A, B)
2: $bits_{sent} \leftarrow$ SENDBITS($bits_A, Filter_A$)
3: $Filter_B \leftarrow$ RAND($Filters$) ▷ where $Filters$ is a set of filters
4: $bits_B \leftarrow$ RECEIVEBITS($bits_sent, Filter_B$)
5: $key_{AB} \leftarrow$ COMPARE($Filter_A, Filter_B$)
6: **end procedure**

In this procedure, A sends some bits through a polarizing filter (see Appendix 8.3) to B. Because B doesn't know which polarizing filters A used, they use a random set of filters to receive these bits through. Once A has finished sending these bits and B has finished receiving them, they compare the polarizing filters they used. They keep the bits sent/received that match and discard those that do not. This set of matching bits becomes the shared key. Now, how does this protect against eavesdropping or MITM attacks?

3.2.1 Protecting Against Eavesdropping and MITM Attacks

An adversary could try to listen in on the communication between A and B, but reading a state destroys the superposition information which effectively changes the state. An adversary could try to use their own polarizing filter to read and/or pass on the information transmitted, but without being to compare (step 5), any information they collect is somewhat useless. Even better than the fact that an outsider is not able to effectively listen in or manipulate information communicated using this protocol is the way that doing so alters the information stream in a way that very quickly alerts the communicating parties that there is some interfering force that is not supposed to be there. This ability to protect against and detect any attempted meddling means that communicating parties can quickly and effectively respond (i.e. starting over), and they can rest assured that future communication will be secure from having been breached at this initial stage.

4 Breaking Classical Cryptography

Just as quantum communication and cryptography developed to utilize quantum computers for better communication and security, the offensive side of computer security was able to take advantage of the unique properties of quantum computers to perform better as well[1]. Two algorithms that exemplify this growth and how it can cause a domino effect on the industry and the world by extension are **Shor's algorithm** and **Grover's algorithm**.

4.1 Shor's Algorithm

Shor's algorithm was made by Peter Shor in 1994. Inspired by Dan Simon's research discussing an oracle function[2] capable of finding a period[3] as well as taking advantage of the observation that Fourier transformations[4] are good at find periodicity, Shor was able to devise an algorithm capable of breaking the discrete log problem and later developed this algorithm further to accomplish prime factorization with a super-polynomial speedup (when compared with classical algorithms; previously mentioned in Section 1.2) [70].

4.2 Grover's Algorithm

Grover's algorithm was made by Lov Grover in 1996. It is a search algorithm designed for use on unstructured datasets. Given a black box that produces a unique output, Grover's algorithm can find the unique input that produced this output with high probability. If the function's domain size is N, Grover's algorithm can find such an input with only $O(\sqrt{N})$ evaluations.

4.3 Why does this matter?

As previously discussed, Shor's algorithm can be used to break many if not nearly all public-key cryptography systems. This includes:

- the Diffie-Hellman key exchange
- ElGamal public-key encryption

[1] Defensive cryptography typically refers to systems, protocols, and schemes used to protect sensitive information from outside forces while the term offensive security is typically used to refer to cryptographic systems, protocols, and schemes that attack, break, or take advantage of weaknesses in systems to gain access to valuable and sensitive information. Though it may sound like one is a good thing and one is a bad thing, both work together and are equally important to make sure the systems that protect information grow with the industry that surround them.

[2] a "black box" function that when given an input gives an output; the implementation of how such a task might be done may not be known, but such a concept is often in proofs to provide abstract concepts not yet realized that may allow other discoveries

[3] a point at which a cyclical group repeats

[4] a function capable of decomposing a waveform; implementation not relevant to this discussion

- the Digital Signature Algorithm (**DSA**)
- Elliptic Curve Cryptography (**ECC** which includes Elliptic Curve Diffie-Hellman)
- the Rivest-Shamir-Adleman (**RSA**) encryption protocol

While Grover's algorithm could:

- optimize **brute-force attacks**
- find collisions in hash-based systems, acting as a precursor for **pre-image attack**

Currently Grover's algorithm has several restrictions that limit its implementation and use. One of these is that it is designed for use on unstructured datasets. The second is that it only provides a quadratic search speedup rather than, for example, an exponential one. When applied to structured datasets or smaller datasets, this algorithm may actually be less efficient or slower than other schemes such as the parallel rho algorithm[5] [28][79].

Neither algorithm has a quantum computer in existence able to run them with a low enough margin of error to be useful.

As you can see quantum computing, communication, and cryptography are growing on both the defensive and offensive side, and we know that Mosca's theorem put together with current predictions for when a cryptographically-relevant quantum computer could be expected tells us that now is as good a time as any to start preparing and strengthening current systems for its arrival.

5 Collaborating for Public Reform

In 2015, the NSA's Information Assurance Directorate (IAD) announced that they would "initiate a transition to quantum resistant algorithms in the not too distant future" [43]. Ditching their current initiative at the time called Suite B, they stated that they would be searching for "cost-effective security against a potential quantum computer" [78]. Stating that it must be cost-effective indicated that this new solution must be compatible with a wide variety of systems already in use. It is also one of the reasons that the NSA recommended pursuing research and searching for solutions in Post-Quantum Cryptography (PQC) rather than Quantum Key Distribution QKD systems[6].

This is the announcement that inspired NIST to kick off their Post-Quantum Cryptography Standardization Competition which we will discuss in the next section.

[5] used to solve the elliptic curve discrete log problem

[6] post-quantum cryptography is cryptography not weakened or completely broken by Shor or Grover's algorithm while being suitable for a wide range of applications; quantum key distribution in comparison is best for point-to-point communication [27]

The original plan was that the NSA would work to secure the National Security Systems (NSS) since they fell under the NSA's domain of responsibilities while NIST would work toward standardizing protocols and schemes that could be used and recommended to other government organizations and broader industry. However, because President Biden's January 2022 National Security Memorandum (**NSM**-8) gave the NSA 180 days to "identify instances of encryption used on NSS not in compliance with NSA-approved quantum resistant algorithms, as well as provide a plan and timeline to transition those systems to quantum resistant standards" [78], this plan had to pivot to accommodate this shortened timeline.

As a result NIST continued to pursue their PQC Standardization Competition, while the NSA joined forces with DHS to find an intermediary solution as well as draft and disseminate a plan that could be recommended to FCEB, SLTT, CI, and some private industry organizations and vendors.

Fulfilling their part of the deal, DHS's CISA has released multiple white papers[7] that educate, make recommendations, and update industry leaders as well as the public. Recommendations in these papers (specifically "Preparing Critical Infrastructure for Post-Quantum Cryptography" released in 2022) include things like:

- creating a "post-quantum readiness roadmap" and encouraging vendors and service providers that work with the organization to do the same
- putting together a project management team to "plan and scope the organization's migration to PQC" , including the organizations "cybersecurity and privacy risk managers who can prioritize assets that would be most impacted by a CRQC and/or would expose the organization to greater risk"
- developing an inventory of vulnerable and dependent systems with the cooperation of information technology and operational technology procurement experts, engaging with supply chain vendors to identify these technologies (much in the same mentality as developing a Software Bill of Materials (see **SBOM** in glossary))
- prioritizing high impact systems, industrial control systems (**ICSs**), and systems with long-term confidentiality/secrecy needs
- identifying data reliant on quantum vulnerable technologies, either updating these systems or coming up with plans and/or timelines to phase them out
- engaging with vendors on their roadmap to clarify when and how each commercial-off-the-shelf (**COTS**) vendor "plans to deliver updates or upgrades to enable the use of PQC, as well as the expected cost associated with" such a migration

[7] refers to an information publication made available to the public, i.e. it is not confidential or restricted

- engaging with cloud service providers to "understand the provider's quantum-readiness roadmap"

This quantum revolution, its increased capabilities as well as its increased threats has encouraged cross collaboration on every level. We have illustrated how the collaboration between the NSA and DHS has enacted change, and next we will discuss the last piece of the puzzle: how NIST is using their PQC Standardization Competition to find algorithms to standardize for use in both the private and public sector.

6 NIST's PQC Standardization Competition

In 2009, NIST published a PQC survey, but it wasn't until 2012 that they announced the PQC competition. Spurred on by the announcement made by the NSA that the US government systems would be pursuing quantum-safe solutions, NIST published a report on PQC (**NISTIR** 8105), devised a timeline, a series of submissions criteria, as well criteria by which to judge and test submissions. The rules and guidelines of the competition were presented at the PQCrypto Conference in 2016 in Japan with the caveat that such standards and rules may shift and change with input from the community. No stranger to competitions, NIST has successfully used similar competitions to standardize the Diffie-Hellman and Elliptic Curve Diffie-Hellman protocol (**ECDH**)(which resulted in **SP** 800-56A), the RSA encryption scheme (SP 800-56B, **FIPS** 186), DSA and Elliptic Curve DSA (**ECDSA**)(FIPS 186), and more. All of these past standards however were liable to be vulnerable to attack should a CRQC become available, and despite the familiarity of the process of standardizing new algorithms or updating standards for algorithms already in existence, the task of finding post-quantum algorithms to standardize and recommend was a much larger task that before because (1) post-quantum cryptography was going to be more complicated than the cryptography required for past competitions, (2) there would be no "silver bullet" because all algorithms would have benefits and weaknesses (NIST stated in addition they'd ideally like to choose more than one "winner"), (3) the algorithms chosen must be able to work on a wide variety of systems, and (4) they must be able to be run and be tested on classical systems while being quantum-safe.

Level	Security Description
I	At least as hard to break as AES128 (exhaustive key search)
II	At least as hard to break as SHA256 (collision search)
III	At least as hard to break as AES192 (exhaustive key search)
IV	At least as hard to break as SHA384 (collision search)
V	At least as hard to break as AES256 (exhaustive key search)

Figure 5: NIST's levels of security on which algorithms would be graded

Included in this announcement, they stated that they would be looking for digital signature,

encryption, and key exchange algorithms (**KEMs**) (while not being part of the official competition, they later announced that they would be looking for proposals for stateful hash-based signature algorithms as well). They expressed the desire for algorithms that would cover these three bases while being based on a variety of different types of quantum algorithms. In their solicitation for proposals and papers, they stated that submissions should be publicly disclosed and freely available, having signed statements with patent information disclosed, having "theoretical and empirical evidence providing justification for security claims", and including "concrete...parameters for meeting target security levels" (see Figure 5) [32].

In addition to security, they stated that algorithms would be judged on performance. Algorithm capable of additional features would be considered even better. Examples of additional features that NIST was looking for included:

- "drop-in replacements - compatibility with existing protocols and networks,
- perfect **forward secrecy**,
- resistance to **side-channel attacks**,
- simplicity and flexibility,
- misuse resistance" [20],
- and any other additional features similar to those already stated

In a presentation given by Dustin Moody (NIST Fed) at the AsiaCrypt conference in 2017, NIST described their role as "managing a process of achieving community consensus in a transparent and timely manner" [32].

6.1 Off to the Races

In the initial set of submissions, NIST received 82 papers with 69 papers meeting the minimal submissions criteria, being considered "complete and proper" [43]. Round over round and year after year, progress marked by continued presentations, workshops, and conferences whittled the number of algorithms in the running down quickly. Algorithms were eliminated for a variety of reasons such as being broken, significantly attacked, NIST lacking full confidence in their security, or the algorithms being deemed too inefficient. There were small alterations to submissions criteria and judging criteria made to incorporate feedback from the community and introduce a bit more flexibility. Some submissions were added in later rounds while other similar ones were merged, and some submissions were given suggestions to make improvements into order to move forward in the competition. As is illustrated in Figures 7 and 6, there were a variety of algorithms for encryption and key exchange as well as signatures which were split into several categories based on the type of

	Signatures	KEM/Encryption	Overall
Lattice-based	5	21	26
Code-based	2	17	19
Multi-variate	7	2	9
Symmetric/Hash-based	3		3
Other	2	5	7
Total	**19**	**45**	**64**

Figure 6: The breakdown of algorithms submitted in the first round. The majority were lattice-based encryption/key exchange protocols [43]

Encryption/KEMs					**Signatures**		
Crystals-Kyber	Lattice	MLWE			CRYSTALS-Dilithium	Lattice	Fiat-Shamir
Saber	Lattice	MLWR			qTesla	Lattice	Fiat-Shamir
FrodoKEM	Lattice	LWE			Falcon	Lattice	Hash then sign
Round 5	Lattice	LWR/RLWR					
LAC	Lattice	RLWE			SPHINCS+	Symm	Hash
NewHope	Lattice	RLWE			Picnic	Symm	ZKP
Three Bears	Lattice	IMLWE					
NTRU	Lattice	NTRU			LUOV	MultVar	UOV
NTRUprime	Lattice	NTRU			Rainbow	MultVar	UOV
					GeMMS	MultVar	HFEv-
SIKE	Isogeny	Isogeny			MQDSS	MultVar	Fiat-Shamir
Classic McEliece	Codes	Goppa					
~~NTS-KEM~~	~~Codes~~	~~Goppa~~	(merged)				
BIKE	Codes	short Hamming					
HQC	Codes	short Hamming					
LEDAcrypt	Codes	short					
ROLLO	Codes	low rank					
RQC	Codes	low rank					

Figure 7: The list of second round candidates sorted by algorithm type [22]

quantum algorithm they utilized. By the end of the third round in 2022, four algorithms had been chosen for standardization: one lattice-based encryption/key exchange protocol, two lattice-based[8] [9] digital signature schemes, and one hash-based digital signature scheme. A quick summary of each is given as follows:

6.2 CRYSTALS-Kyber

The only public-key encryption/key exchange protocol chosen for standardization at the end of the third round was CRYSTALS-Kyber which was based on structured lattices and the module

[8] refers to the type of quantum algorithm used, namely, it refers the quantum physics property or scheme that allows an algorithm built on it to be secure

[9] types of quantum algorithms include: (structured and unstructured) lattice-based (module learning with errors, module learning with rounding), isogeny based, code-based (Goppa, short Hamming, low rank), symmetric-based, hash-based, multivariate-based schemes, and more.

learning with errors problem. Designed to have IND-CCA2[10] base level security when used for key exchange and IND-CPA[11] base level security when used for encryption, it was chosen for its "strong security and performance" [20]. NIST stated they would standardize sub-schemes Kyber-768 (providing level 3 security, see Figure 5) and Kyber-1024 (providing level 4 security), and they were considering standardizing Kyber-512 as well (at the time of the fourth round they stated that this was just barely meeting level 1 security but it could be advantageous to standardize due to the current cost, stating it would be offered as a smaller alternative). This culminated in Draft FIPS 203 released August 24, 2023 which closed its public comment period on November 22, 2023.

6.3 CRYSTALS-Dilithium

One of the two structured lattice-based digital signature schemes chosen for standardization was from the same team as CRYSTALS-Kyber. CRYSTALS-Dilithium used a "Schnorr-like" [77] lattice-based scheme, supported by the module learning with errors problem. It was chosen for its "strong security and performance", and NIST stated that they planned to standardize the parameter sets that corresponded with "security categories 2, 3, and 5" [20]. This culminated in Draft FIPS 204 released August 24, 2023 which also closed its public comment period on November 22, 2023.

6.4 Falcon

Falcon is the second of the two structured lattice-based digital signature schemes and third of the overall schemes chosen for standardization. It was chosen for standardization as a possible alternative for applications where the CRYSTALS-Dilithium signature was too large. When the team behind Falcon were tasked with presenting their scheme they laid out how their scheme is different, its strengths, its weakness, as well as some ideal applications. Falcon is the only scheme that uses floating point arithmetic and as such must be run on systems with floating point units (**FPU**). This could pose a limitation on its adoption in the case of devices without FPUs, with FPU emulators, or variable-time FPUs. Where systems use emulators or variable-time FPUs, the performance of Falcon may be slower or less reliable, and for companies trying to keep the scheme they use secret, Falcon would not be the best choice because of its unique implementation. The team described vehicle-to-vehicle communications, TLS certificates, systems that don't have a lot of resources for verification, and DNSSEC[12] as ideal applications. NIST announced that they would write the draft standard document for Falcon after completing those for Kyber, Dilithium, and SPHINCS+ which means that despite not having been published yet, such a draft document for which a public comments period will open is due any day now.

[10] indistinguishability under adaptive chose ciphertext attack
[11] indistinguishability under chosen plaintext attack
[12] Domain Name System Security Extensions

6.5 SPHINCS+

SPHINCS+ is the final scheme chosen for standardization thus far, and it is the only hash-based digital signature scheme chosen for standardization. Chosen for its "solid security", it was originally listed as an alternate when the finalists were announced during the third round; however, the premise which its security is based has existed long enough to have made SPHINCS+ a safe bet. As such, this resulted in Draft FIPS 205 which closed its period for public comments November 22, 2023.

6.6 The Fourth Round...

As it currently stands, the PQC Standardization Competition is technically in its fourth round. As mentioned before three draft FIPS documents have been released, and we are awaiting a fourth for Falcon. NIST announced additional public key encryption/key exchange protocols BIKE, Classic McEliece, HQC, and SIKE will be candidates further considered for standardize. They have also released a call for proposals for digital signature algorithms with short signatures and fast verification [53].

6.7 ... Moving Forward

The fifth PQC standardization conference is scheduled to be held April 10-12, 2024. On their website they state the purpose will be to "discuss various aspects of the algorithms (both those selected and those being evaluated) and to obtain valuable feedback for informing decisions on standardization" [14] where representative from all teams creating algorithms under consideration will present. When the competition was initially announced, NIST stated that they would like to release standard by 2023. Halfway through the competition they received recommendation that they take their time to ensure a thoughtful and thorough evaluation process. When this decision was made, they amended their statement to say that standards would be available sometime in 2024. The process of not only finding solutions but making sure that the solution found are diverse and robust is an ongoing process which NIST is taking very serious. Coordinating a process in which scientists, mathematicians, physicists, as well as many other types of researchers from all over the world are participating in is a large task to take on, but it has been redeeming to see the ways in which people have come together to create solutions. The process of post-quantum standardization is likely to be an ongoing task that will not end very soon and may not end necessarily when quantum computers arrive. It is much more likely that the coming of a CQRC will create as much if not more excitement, presenting new challenge, we have seen from the discussion of the possibility of one which prompted the PQC competition. It is unclear where this timeline will end, but there have been many promising development to have come out of it.

7 Conclusion

Information makes up the threads that tie us together in this world and supports us as we move forward; therefore, the threat of a quantum computer capable of breaking the system that protect this information was a cause of great concern. Its unclear when such a computer will exist, and the power that a quantum computer may provide is only just started to be uncovered. With great potential and also posing great risk, we have seen individuals as well as government come together to find solutions that cross countries and backgrounds. This initial standardization phases is not over. We do not yet have a quantum computer to effectively test if they are fully secure and if they are, how long they will be so. Its too early in this "quantum revolution" to be able to tell how rapidly the field will grow. There is a whole world cryptography that could developed with quantum computers yet untapped. Beyond the codification and standards, it is yet to be delved into the possible applications for quantum computers though theoretical ideas do exist. Uncertainty can invite fear, but there is also a very high ceiling for potential which we are only just beginning to explore. Healthy curiosity and teamwork has brought us here, and maybe these pieces are exactly what we need to keep moving forward.

8 Appendix

8.1 Glossary

Acronyms

attack vector - "the method or combination of methods that cybercriminals use to breach or infiltrate a victim's network" [5]. 12

authenticity - an entity is who they say they are; data has come from a trusted source. 11, 23

availability - a system is available for use when needed and requested; can refer to timeliness and reliability. 11, 23

bra-ket notation - sometimes referred to as Dirac notation, this is a special notation used in quantum mechanics to describe quantum states; its unique representation allows us to "compute probabilities, transition amplitudes, and other important quantities in quantum mechanics" [99]. 11

brute-force attack - an attack where an adversary tries all possible inputs to try to break into a system; on average, they must try about fifty percent before (i.e. passwords) before succeeding. 15

CI - critical infrastructure. 8

CIA triad - the CIA triad defines the three key security objectives in cryptography; these are confidentiality, glsintegrity, and availability; additional objectives of non-repudiation and authenticity are often considered sub-objective of integrity. 11

CISA - Cybersecurity and Infrastructure Security Agency; an operational component of DHS. 7

confidentiality - information should not be divulged to unauthorized parties; only entities with express or explicit permission should be able to access information. 11, 23

COTS - commercial-off-the-shelf. 16

CRQC - a cryptographically relevant quantum computer; a computer "capable of actually attacking real world cryptographic systems that would be infeasible to attack with a normal computer" [55]. 7

cryptography - the ability to send information between participants in a way that prevents others from reading it. 12

DHS - Department of Homeland Security. 8

DSA - Digital Signature Algorithm. 15

eavesdropping - a passive attack where an adversary listens in on a information stream. 2, 12

ECC - Elliptic Curve Cryptography. 15

ECDH - Elliptic Curve Diffie-Hellman. 17

ECDSA - Elliptic Curve Digital Signature Algorithm. 17

entanglement - the quantum state of each particle within a set cannot be described independently of the state of the other particles even when the particles are separated by a large distance; position, momentum, spin, and polarization may be all perfectly correlated [95]. 9

FCEB - Federal Civilian Executive Branch; often used to refer to ".gov" agencies. 8

FIPS - Federal Information Processing Standards. 17

forward secrecy - "session keys will not be compromised even if long-term secrets used in the session key exchange are compromised" [90]. 18

FPU - floating point unit. 20

Grover's algorithm - an algorithm devised by Lov Grover in 1996 capable of finding a unique input that was given to black box function when given its unique output, searching unstructured datasets with a polynomial speedup. 14

Heisenberg uncertainty principle - sometimes called the indeterminacy principles, it states "there is a limit to the precision with which certain pairs of physical properties, such as position and momentum, can be simultaneously known' [98]. 13

ICS - industrial control systems. 16

information revolution - "the radical changes wrought by computer technology on the storage of and access to information since the mid-1980s" [100]. 5

information science - the study and practice of how to "collect, store, retrieve, and use information effectively"; explores the "social, ethical and cultural aspects of information"; combining "concepts and methods from various disciplines such as library science, computer science, linguistics, and psychology" [7]. 4

integrity - information must not be modified or destroyed by outside parties or without authorization; sender and receivers of information should be able to trust the information sent or received has not and will not be tampered with or altered. 11

KEM - key encapsulation method; a method used "to secure symmetric key material for transmission using asymmetric (public-key) algorithms" [93]. 18

MITM - a man-in-the-middle attack; an active attack where an adversary may "transmit their own messages, replay old messages, modify messages in transit, or delete or delay selected messages in transit" [37]. 2, 12

Moore's law - "the observation that the number of transistors in an integrated circuit... doubles about every two years" [50]. 5

Mosca's theorem - a theorem created by Michele Mosca that gives a "quantum threat timeline [to determine] whether a cyber-system is already at risk, well before the quantum threat has become concrete, because one has also to consider the needed migration time and the desired or required (e.g. by regulations) shelf-life time" [42]. 7

NCF - national critical functions; "functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof" [12]. 8

NIST - National Institute for Standards and Technology. 8, 15

NISTIR - NIST Interagency Report. 17

non-repudiation - actions should be uniquely traceable to the person or entity that did it. 11, 23

NSA - National Security Agency. 8, 15

NSM - National Security Memorandum. 16

NSS - National Security Systems; "systems that contain classified information or are otherwise critical to military or intelligence operations" [66]. 8, 16

OTP - one-time pad; a "single-use pre-shared key larger than or equal to size of the message being sent" that provides perfect secrecy, meaning it is technically impossible to crack [94]. 13

PQC - post-quantum cryptography. 8, 15

pre-image attack - an attack where an attack tries to find a message which hashes to a specific value. 15

QC - quantum computer. 5

QKD - quantum key distribution. 2, 13, 15

quantum cryptography - cryptography that uses quantum mechanical phenomena to secure communication [72]. 11

qubit - a quantum bit. 9

RSA - Rivest-Shamir-Adleman; an asymmetric encryption algorithm. 15

SBOM - Software Bill of Materials; likened to a ingredients list on a food label or receipt from the grocery store, this is an itemized and nested list of items that make up a software component that could be maintained for a vendor or given to potential consulting and contracting customers when building products, tools, and systems. 16

Shor's algorithm - an algorithm devised by Peter Shoe in 1994 that is able to break the discrete log problem as well as the prime factorization problem. 14

side-channel attack - "any attack based on extra information that can be gathered because of the fundamental way a computer protocol or algorithm is implemented, rather than flaws in the design of the protocol or algorithm itself (e.g. flaws found in a cryptanalysis of a cryptographic algorithm)" [97]. 18

SLTT - State/Local/Tribal/Territorial. 8

SP - Special Publication. 17

8.2 A Timeline

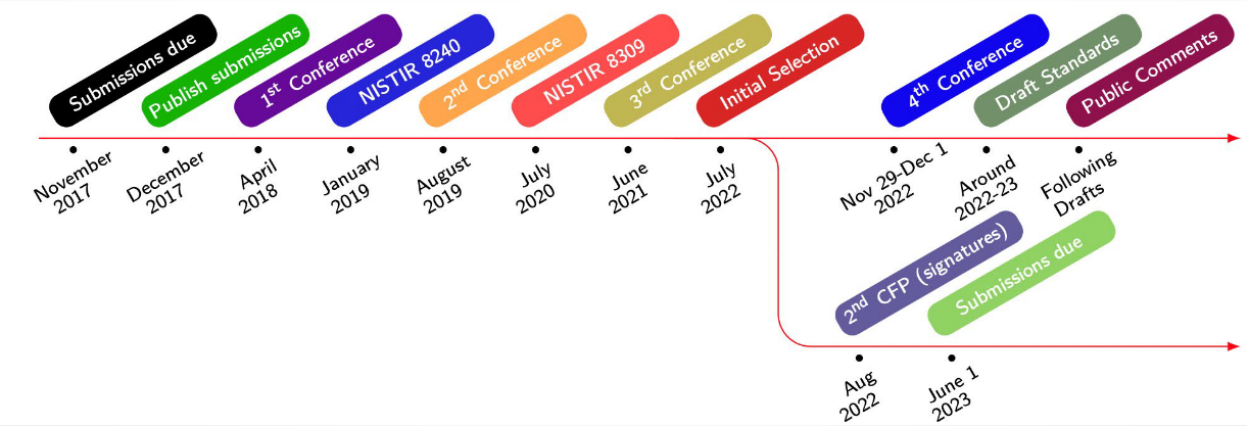

Figure 8: The latest timeline announced at the 4th PQC Standardization Workshop in 2023 [20]

1801	Thomas Young's double-slit experiment kicks off field of quantum mechanics
1935	Quantum entanglement discovered
1935	Schrödingers cat
1955	Information science receives its name
1965	Moore's law introduced
1965	Stephen Weisner introduced conjugate coding
1984	The BB84 protocol
1994	Shor's algorithm
1996	Grover's algorithm
2015	NSA announcement
2016	NIST announces PQC competition at PQCrypto
2016	NIST releases NISTIR 8105, Report on PQC
2016	NIST formal call for proposal
2017	NIST deadline for submissions
2017	IBM's 50-qubit quantum computer made
2017	Round 1 algorithms announced
2018	Intel's 49-qubit chip "Tangle-Lake" made
2018	Google's 72-qubit chip "Bristlecone" made
2018	NIST's first PQC standardization conference
2019	Second round candidates announced
2019	Deadline for updated packages for second round
2019	Second PQC standardization conference
2020	Third round candidates announced
2020	Deadline for updated packages for third round
2021	Third PQC standardization conference
2022	Announcement of candidates to be standardized and fourth round candidates
2022	Fourth PQC standardization conference
2022	President of US releases NSM-8
2023	Atom's 1180-qubit quantum computer made
2023	President of US releases NSM-10
2023	Three draft FIPS released for public comment
2024	Fifth PQC standardization conference

Table 1: A general timeline of quantum computing and NIST PQC standardization developments

8.3 A Note on Polarizing Filters

We have conceptualized qubits as photons with a spin in a particular direction or all possible directions in the case of superposition. If we were to compare a polarizing filter to a sieve, we might say that only photons with the same angle (or polarization) as the filter can get through the filter. But this is quantum physics, and in the case of qubits, it would be more accurate to say that if the polarization of the photon and filter match, all photons will get through; if they are opposite, none will get through; and if they are mismatch but not opposite (see Charles Bennett's definition

of “reliably distinguishable” in section 2.2), then a random number will get through the filter with the polarization possibly changed.

8.4 A Note on Symmetric Encryption

This paper has primarily focused on public key cryptography systems which are sometimes referred to as asymmetric key systems. An alternate type of encryption scheme is symmetric encryption. Research has indicated that these will be threatened by the development of a CRQC but not broken in the same way as public key systems, and as such, the increasing the length of keys for schemes such as AES and SHA-1/2/3 would be sufficient on the short term.

References

Alagic et al.: Status report on the first round of the NIST post-quantum cryptography standardization process **alagic_status_2019**

Gorjan Alagic et al. *Status report on the first round of the NIST post-quantum cryptography standardization process*. en. Tech. rep. NIST IR 8240. Gaithersburg, MD: National Institute of Standards and Technology, Jan. 2019, NIST IR 8240. DOI: 10.6028/NIST.IR.8240. URL: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8240.pdf (visited on 11/26/2023).

Annotations: The National Institute of Standards and Technology is in the process of selecting one or more public-key cryptographic algorithms through a public competition-like process. The new publickey cryptography standards will specify one or more additional digital signature, public-key encryption, and key-establishment algorithms to augment FIPS 186-4, Digital Signature Standard (DSS), as well as special publications SP 800-56A Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, and SP 800-56B, Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization. It is intended that these algorithms will be capable of protecting sensitive information well into the foreseeable future, including after the advent of quantum computers.

Alagic et al.: Status report on the third round of the NIST Post-Quantum Cryptography Standardization process **alagic_status_2022**

Gorjan Alagic et al. *Status report on the third round of the NIST Post-Quantum Cryptography Standardization process*. en. Tech. rep. NIST IR 8413-upd1. Gaithersburg, MD: National Institute of Standards and Technology (U.S.), Sept. 2022, NIST IR 8413–upd1. DOI: 10.6028/NIST.IR.8413-upd1. URL: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413-upd1.pdf (visited on 11/26/2023).

Annotations: The National Institute of Standards and Technology is in the process of selecting publickey cryptographic algorithms through a public, competition-like process. The new publickey cryptography standards will specify additional digital signature, public-key encryption, and key-establishment algorithms to augment Federal Information Processing Standard (FIPS) 186-4, Digital Signature Standard (DSS), as well as NIST Special Publication (SP) 800-56A Revision 3, Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography, and SP 800-56B Revision 2, Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography. It is intended that these algorithms will be capable of protecting sensitive information well into the foreseeable future, including after the advent of quantum computers.

Arcuri et al.: Moore's Law and Its Practical Implications **arcuri_moores**

Gregory Arcuri and Sujai Shivakumar. "Moore's Law and Its Practical Implications". en. In: (Oct. 2022). URL: https://www.csis.org/analysis/moores-law-and-its-practical-implications (visited on 11/27/2023).

Annotations: With competition for leadership in the semiconductor industry heating up, an understanding of the economic and policy significance of Moore's Law is critical to supporting policies that advance the international competitiveness of the United States.

Barker et al.: Getting Ready for Post-Quantum Cryptography barker_getting_2021

William Barker, William Polk, and Murugiah Souppaya. *Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms*. en. Tech. rep. National Institute of Standards and Technology, Apr. 2021. DOI: 10.6028/NIST.CSWP.04282021. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04282021.pdf (visited on 11/18/2023).

Bart Lenaerts-Bergmans: What are Attack Vectors attackvectors

Bart Lenaerts-Bergmans. *What are Attack Vectors: Definition & Vulnerabilities - CrowdStrike*. en. Apr. 2023. URL: https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/attack-vector/ (visited on 12/03/2023).

Annotations: Attack vectors are the method that adversaries use to breach a network. Recognizing and tracking them is key for cybersecurity. Learn more!

Bing: Information Science bing_is_def

Bing. *Information Science*. en. URL: https://www.bing.com:9943/search?q=define+information+science&toWww=1&redig=DBFC8BC5D6294429953E6F0FC25EC38C (visited on 11/27/2023).

Annotations: Used Bing to define information science. Bing's dictionary is backed by Oxford Languages, and when trying to figure out Bing's source, it cited itself, indicating it has in house data it can use to answer questions directly.

Bing AI: information science bing_info_science

Bing AI. *information science*. en. URL: %5Cxurl%7Bhttps://www.bing.com/search?pglt=163&q=information+science&cvid=6943ebe2cb8d4a659a2d77c36e1ef906&gs_lcrp=EgZjaHJvbWUqBggAEAAYQDIGCAAQABhAMgYIARAuGEAyBggCEEUYOzIGCAMQABhAMgYIBBAAGEAyBggFEAAYQDIGCAYQABhAMgYIBxBFGDwyBggIEEUYPNIBCDI5ODJqMGoxqAIAsAIA&FORM=ANNTA1&PC=W099%7D.

Annotations: Bing's AI sourced a comprehensive definition of what information science is and cited using 6 different sources for this aggregation including Britannica, Indeed, UNT's Department of Information Science, the Information Sciences journal available from Science Direct, asis&t, and the University of Van Pretoria's page on Information Science.

Cambridge Quantum delivers first quantum encryption keys | TechTarget noauthor_cambridge_nodate

Cambridge Quantum delivers first quantum encryption keys | TechTarget. en. URL: https://www.t

echtarget.com/searchdatacenter/news/252510605/Cambridge-Quantum-delivers-first-quantum-encryption-keys (visited on 11/25/2023).

Annotations: Cambridge Quantum has debuted a cloud-based cryptographic key generator platform that works across classical computing and quantum computing environments.

Cetin Kaya Ko: Dicrete Logarithm Problem **cetin_kaya_ko_dicrete_2017**

Cetin Kaya Ko. *Dicrete Logarithm Problem*. 2017.

Annotations: Note set on the discrete logarithm program for a class on index calculus.

Chen: Cryptography Standards in Quantum Time **chen_cryptography_2017**

Lidong Chen. "Cryptography Standards in Quantum Time: New Wine in an Old Wineskin?" en. In: *IEEE Security & Privacy* 15.4 (2017), pp. 51–57. ISSN: 1540-7993, 1558-4046. DOI: 10.1109/MSP.2017.3151339. URL: https://ieeexplore.ieee.org/document/8012315/ (visited on 11/21/2023).

Chen et al.: Report on Post-Quantum Cryptography **chen_report_2016**

Lily Chen et al. *Report on Post-Quantum Cryptography*. en. Tech. rep. NIST IR 8105. National Institute of Standards and Technology, Apr. 2016, NIST IR 8105. DOI: 10.6028/NIST.IR.8105. URL: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf (visited on 11/26/2023).

Annotations: In recent years, there has been a substantial amount of research on quantum computers –machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere. The goal of post-quantum cryptography (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks. This Internal Report shares the National Institute of Standards and Technology (NIST)'s current understanding about the status of quantum computing and post-quantum cryptography, and outlines NIST's initial plan to move forward in this space. The report also recognizes the challenge of moving to new cryptographic infrastructures and therefore emphasizes the need for agencies to focus on crypto agility.

CISA: National Critical Functions **ncfs**

CISA. *National Critical Functions*. en. 2023. URL: https://www.cisa.gov/topics/risk-management/national-critical-functions (visited on 12/02/2023).

Annotations: Definition of NCFs.

CISA Insights: Preparing Critical Infrastructure for Post-Quantum Cryptography
cisa_prep4pqc

CISA Insights. *Preparing Critical Infrastructure for Post-Quantum Cryptography*. Tech. rep. CISA, Aug. 2022. (Visited on 11/21/2023).

Annotations: quantum mechanics, quantum computer, critical infrastructure, post-quantum cryptography, cryptographic standards, public key encryption, digital signatures, national critical functions, catch-and-exploit.

Computer Security Division: Fifth PQC Standardization Conference | CSRC
announcingfifth

Information Technology Laboratory Computer Security Division. *Fifth PQC Standardization Conference | CSRC*. EN-US. Aug. 2023. URL: `https://csrc.nist.gov/events/2024/fifth-pqc-standardization-conference` (visited on 12/04/2023).

Annotations: NIST plans to hold the 5th NIST PQC Standardization Conference from April 10-12, 2024, in Rockville, Maryland.

Computer Security Division: Fourth PQC Standardization Conference | CSRC
computer_security_division_fourth_2022

Information Technology Laboratory Computer Security Division. *Fourth PQC Standardization Conference | CSRC*. EN-US. Nov. 2022. URL: `https://csrc.nist.gov/events/2022/fourth-pqc-standardization-conference` (visited on 11/27/2023).

Annotations: Agenda of events/presentations for the Fourth PQC Standardization Conference held by NIST including session links, downloadable presentation slide decks, and presentation recording links.

Computer Security Division: Post-Quantum Cryptography | CSRC | CSRC
computer_security_division_post-quantum_2017

Information Technology Laboratory Computer Security Division. *Post-Quantum Cryptography | CSRC | CSRC*. EN-US. Jan. 2017. URL: `https://csrc.nist.gov/Projects/post-quantum-cryptography/publications` (visited on 11/27/2023).

Annotations: Draft FIPS 203, FIPS 204 and FIPS 205, which specify algorithms derived from CRYSTALS-Dilithium, CRYSTALS-KYBER and SPHINCS+, were published August 24, 2023. The public comment period will close November 22, 2023. PQC Seminars Next Talk: November 28, 2023 Additional Digital Signature Schemes - Round 1 Submissions PQC License Summary & Excerpts Background NIST initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. Full details can be found in the Post-Quantum Cryptography Standardization page. In recent years, there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenom-

ena to solve mathematical problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital...

Computer Security Division: Workshops and Timeline - Post-Quantum Cryptography | CSRC | CSRC **computer_security_division_workshops_2017**

Information Technology Laboratory Computer Security Division. *Workshops and Timeline - Post-Quantum Cryptography | CSRC | CSRC*. EN-US. Jan. 2017. URL: https://csrc.nist.gov/Projects/post-quantum-cryptography/workshops-and-timeline (visited on 11/26/2023).

Annotations: Resource page on NIST's website with timeline of the PQC competition as well as the workshops.

D'Anvers et al.: Multitarget decryption failure attacks and their application to Saber and Kyber **danvers_multitarget_2021**

Jan-Pieter D'Anvers and Senne Batsleer. *Multitarget decryption failure attacks and their application to Saber and Kyber*. Publication info: Published by the IACR in PKC 2022. 2021. URL: https://eprint.iacr.org/2021/193 (visited on 11/26/2023).

Annotations: Definition of a multitarget decryption failure attack.

Differential fault analysis **noauthor_differential_2023**

Differential fault analysis. en. Page Version ID: 1145572426. Mar. 2023. URL: https://en.wikipedia.org/w/index.php?title=Differential_fault_analysis&oldid=1145572426 (visited on 11/26/2023).

Annotations: Definition of fault inject/fault injection attack.

Dustin Moody: Fourth PQC Standardization Conference (virtual) – Day 1 Part 1 **moody_fourth**

Dustin Moody. *Fourth PQC Standardization Conference (virtual) – Day 1 Part 1*. en. Publication Title: NIST. Dec. 2022. URL: https://www.nist.gov/video/fourth-pqc-standardization-conference-virtual-day-1-part-1 (visited on 11/26/2023).

Annotations: The video version of the lastest presentation given by NIST's Dustin Moody regarding the status of the PQC Standardization Process. This is a video recording of the Fourth PQC Standardization Conference with presentations from Dustin Moody, Matt Scholl (NIST's Computer Security Division Chief), Peter Schwabe (CRYSTALS-Kyber), Thomas Prest (FLACON), Vadim Lyubashevsky (CRYSTALS-Dilithium), Andreas Hulsing and Eyal Ronin (SPHINCS+).

Dustin Moody: Post-Quantum Cryptography: NIST's Plan for the Future **dustin_moody_post-quantum_2016**

Dustin Moody. *Post-Quantum Cryptography: NIST's Plan for the Future*. English. Feb. 2016.

Annotations: First presentation presented at PQ Crypto 2016 Conference announcing the PQC "competition".

Dustin Moody: Round 2 of the NIST PQC "Competition" - What was NIST Thinking? **moody_round2**

Dustin Moody. "Round 2 of the NIST PQC "Competition" - What was NIST Thinking?" en. In: (May 2019).

Annotations: fourth presentation given by Dustin Moody at the PQ Crypto Conference in 2019 in Chongqing, China.

Dustin Moody: The Beginning of the End: The First NIST PQC Standards **moody_begin**

Dustin Moody. "The Beginning of the End: The First NIST PQC Standards". In: (Mar. 2022).

Annotations: PQC standardization update.

Ekert: Quantum cryptography based on Bell's theorem **ekert_quantum_1991**

Artur K. Ekert. "Quantum cryptography based on Bell's theorem". en. In: *Physical Review Letters* 67.6 (Aug. 1991), pp. 661–663. ISSN: 0031-9007. DOI: 10.1103/PhysRevLett.67.661. URL: https://link.aps.org/doi/10.1103/PhysRevLett.67.661 (visited on 11/26/2023).

Eye on Tech: What is Quantum Cryptography? **eye_on_tech_what_2022**

Eye on Tech. *What is Quantum Cryptography? An Introduction*. May 2022. URL: https://www.youtube.com/watch?v=_5NQf8k3Jo0 (visited on 11/25/2023).

Annotations: Goes over the very general definition of what quantum cryptography is with a very general example.

Fouque et al.: Falcon - What's next? **falcon**

Pierre-Alain Fouque et al. "Falcon - What's next?" en. In: (Nov. 2022).

Annotations: Thomas Prest presents on behalf of PQShield the FALCON scheme, selected by NIST as one of the digital signature schemes that it will standardize based on structured lattices.

Gasman: Two Roads to Quantum-Safe Networks **ee_web**

Lawrence Gasman. *Two Roads to Quantum-Safe Networks*. en-US. Nov. 2020. URL: https://www.eeweb.com/two-roads-to-quantum-safe-networks/ (visited on 12/04/2023).

Annotations: Article comparing PQC and QKD.

Gill: Solving Elliptic Curve Discrete Logarithm Problem Using Parallelized Pollard's Rho and Lambda Methods **gill_ecc**

Puneet Gill. "Solving Elliptic Curve Discrete Logarithm Problem Using Parallelized Pollard's Rho and Lambda Methods". en. In: ().

Annotations: Describes what the parallel rho algorithm does.

Hartel: The History of Information Science in 30 Seconds? **30s_history_of_info_science**

Jenna Hartel. *The History of Information Science in 30 Seconds? - Information Matters*. en-US. Jan. 2022. URL: https://informationmatters.org/2022/01/the-history-of-information-science-in-30-seconds/,%20https://informationmatters.org/2022/01/the-history-of-information-science-in-30-seconds/.

Annotations: Where did Information Science come from? What are its theoretical, conceptual, and institutional precedents?

Hartel: The History of Information Science in 30 Seconds? **hartel_history_2022**

Jenna Hartel. *The History of Information Science in 30 Seconds? - Information Matters*. en-US. Jan. 2022. URL: https://informationmatters.org/2022/01/the-history-of-information-science-in-30-seconds/,%20https://informationmatters.org/2022/01/the-history-of-information-science-in-30-seconds/ (visited on 11/27/2023).

Annotations: Where did Information Science come from? What are its theoretical, conceptual, and institutional precedents?

IACR: PKC 2022: Session 4: Invited Talk with Dustin Moody **iacr_pkc_2022**

IACR. *PKC 2022: Session 4: Invited Talk with Dustin Moody*. Mar. 2022. URL: https://www.youtube.com/watch?v=DcwupScEaOQ (visited on 11/26/2023).

Annotations: Video version of presentation given by NIST's Dustin Moody on where NIST was at the time regarding PQC Standardization process choosing the algorithms which NIST had chosen to standardize given at PKC2022.

IACR: The ship has sailed **moody_ship_sailed**

IACR. *The Ship has Sailed: the NIST Post-Quantum Cryptography "competition"*. Jan. 2018. URL: https://www.youtube.com/watch?v=3doS6joRYTE (visited on 11/25/2023).

Annotations: the second presentation deck that accompanied the presentation given by Dustin Moody (NIST) at AsiaCrypt 2017.

IBM Unveils 400 Qubit-Plus Quantum Processor and Next-Generation IBM Quantum System Two **osprey**

IBM Unveils 400 Qubit-Plus Quantum Processor and Next-Generation IBM Quantum System Two. en-us. URL: https://newsroom.ibm.com/2022-11-09-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two (visited on 12/01/2023).

Annotations: IBM kicked off the IBM Quantum Summit 2022, announcing new breakthrough advancements in quantum hardware and software and outlining its pioneering vision for quantum-centric supercomputing.

Information science **wiki_info_science**

Information science. en. Nov. 2023. URL: https://en.wikipedia.org/w/index.php?title=Information_science&oldid=1185129590.

Institut quantique de l'Université de Sherbrooke: The Quantum Enigmas - Grover's Algorithm **enigmas_grover**

Institut quantique de l'Université de Sherbrooke. *The Quantum Enigmas - Grover's Algorithm*. Feb. 2023. URL: https://www.youtube.com/watch?v=TcA4ek4ePDc (visited on 12/03/2023).

Annotations: Grover's algorithm taught using storytelling from The Quantum Library.

Jean-Philippe Aumasson et al.: SPHINCS+ **sphincs**

Jean-Philippe Aumasson et al. *SPHINCS+*. Nov. 2023.

Annotations: Andreas Husling from Eindhoven University of Technology presents an update on the SPINCS+ scheme selected by NIST as a digital signature protocol that they will standardize. It is a hash-based scheme.

Kaufman et al.: Network security **netsec**

Charlie Kaufman et al. *Network security: private communication in a public world*. eng. Third edition. Pearson series in computer networking and distributed systems. Boston Amsterdam London: Addison-Wesley, 2023. ISBN: 978-0-13-664360-9.

Annotations: Textbook for this course, provided formal definitions.

Key encapsulation mechanism **noauthor_key_2023**

Key encapsulation mechanism. en. Page Version ID: 1185330307. Nov. 2023. URL: https://en.wikipedia.org/w/index.php?title=Key_encapsulation_mechanism&oldid=1185330307 (visited on 11/26/2023).

Annotations: In cryptographic protocols, a key encapsulation mechanism (KEM) or key encapsulation method is used to secure symmetric key material for transmission using asymmetric (public-key) algorithms. It is commonly used in hybrid cryptosystems. In practice, public key systems are clumsy to use in transmitting long messages. Instead they are often used to exchange symmetric keys, which are relatively short. The symmetric key is then used to encrypt the longer message. The traditional approach to sending a symmetric key with public key systems is to first generate a random symmetric key and then encrypt it using the chosen public key algorithm. The recipient then decrypts the public key message to recover the symmetric key. As the symmetric key is generally short, padding is required for full security and proofs of security for padding schemes are often less than complete. KEMs simplify the process by generating a random element in the finite group underlying the public key system and deriving the symmetric key by hashing that element, eliminating the need for padding.

Liu: Introduction to Quantum Computers **unc_qc**

Shubin Liu. "Introduction to Quantum Computers". en. In: (June 2021).

Annotations: UNC Information Technology Services presentation by Shubin Liu on "Introduction to Quantum Computers".

Michele Mosca: Cryptographically Relevant Quantum Computers (CRQCs) & The Quantum Threat | Splunk **mosca2**

Michele Mosca. *Cryptographically Relevant Quantum Computers (CRQCs) & The Quantum Threat | Splunk*. URL: https://www.splunk.com/en_us/blog/learn/crqcs-cryptographically-relevant-quantum-computers.html (visited on 12/04/2023).

Michele Mosca et al.: Quantum Threat Timeline Report- 2021: Executive Summary **mosca_piani_howsoon**

Michele Mosca and Marco Piani. *Quantum Threat Timeline Report- 2021: Executive Summary*. Tech. rep. Jan. 2022.

Michele Mosca et al.: Quantum Threat Timeline Report- 2021: Executive Summary **quantum_threat_timeline**

Michele Mosca and Marco Piani. *Quantum Threat Timeline Report- 2021: Executive Summary*. Tech. rep. Jan. 2022.

Annotations: Mosca and Piani provide more visuals for how soon we have until a CRQC.

Moody: Let's Get Ready to Rumble- The NIST PQC "Competition" **moody_lets_2018**

Dustin Moody. "Let's Get Ready to Rumble- The NIST PQC "Competition"". en. In: (Apr. 2018).

Annotations: the third presentation given by Dustin Moody at the PQ Crypto Conference 2018.

Moody: Module-Lattice-Based Digital Signature Standard **moody_module-lattice-based_2023-1**

Dustin Moody. *Module-Lattice-Based Digital Signature Standard*. en. Tech. rep. NIST FIPS 204 ipd. Gaithersburg, MD: National Institute of Standards and Technology, 2023, NIST FIPS 204 ipd. DOI: 10.6028/NIST.FIPS.204.ipd. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.ipd.pdf (visited on 11/27/2023).

Annotations: Draft FIP 204 CRYSTALS-Dilithium.

Moody: Module-Lattice-Based Key-Encapsulation Mechanism Standard **moody_module-lattice-based_2023**

Dustin Moody. *Module-Lattice-Based Key-Encapsulation Mechanism Standard*. en. Tech. rep. NIST FIPS 203 ipd. Gaithersburg, MD: National Institute of Standards and Technology, 2023, NIST FIPS 203 ipd. DOI: 10.6028/NIST.FIPS.203.ipd. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.ipd.pdf (visited on 11/27/2023).

Annotations: Draft FIPS 203 - CRYSTALS-Kyber.

Moody: NIST PQC Standardization Update - Round 2 and Beyond **moody_pqc_update_2+**

Dustin Moody. "NIST PQC Standardization Update - Round 2 and Beyond". en. In: (Sept. 2020).

Annotations: PQC standardization update.

Moody: NIST Status Update on the 3rd Round **moody_3rdroundupdate**

Dustin Moody. "NIST Status Update on the 3rd Round". en. In: (June 2021).

Annotations: Dustin Moody from NIST gives a presentation regarding status updates as of the 3rd round of the PQC Competition at the 3rd PQC Standardization Conference in 2021.

Moody et al.: Status report on the second round of the NIST post-quantum cryptography standardization process **moody_status_2020**

Dustin Moody et al. *Status report on the second round of the NIST post-quantum cryptography standardization process*. en. Tech. rep. NIST IR 8309. Gaithersburg, MD: National Institute of Standards and Technology, July 2020, NIST IR 8309. DOI: 10.6028/NIST.IR.8309. URL: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8309.pdf (visited on 11/21/2023).

Annotations: The National Institute of Standards and Technology is in the process of selecting one or more public-key cryptographic algorithms through a public, competition-like process. The new publickey cryptography standards will specify one or more additional digital signatures, public-key encryption, and key-establishment algorithms to augment Federal Information Processing Standard (FIPS) 186-4, Digital Signature Standard (DSS), as well as NIST Special Publication (SP) 800-56A Revision 3, Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography, and SP 800-56B Revision 2, Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography. It is intended that these algorithms will be capable of protecting sensitive information well into the foreseeable future, including after the advent of quantum computers.

Moody: The 2nd Round of the NIST PQC Standardization Process **moody_2ndround**

Dustin (Fed) Moody. "The 2nd Round of the NIST PQC Standardization Process". en. In: (Aug. 2019).

Annotations: Fifth presentation give by Dustin Moody representing NIST in the opening remarks at PQC 2019 in Santa Barbara.

Moore's law **moore**

Moore's law. en. Page Version ID: 1185981128. Nov. 2023. URL: https://en.wikipedia.org/w/index.php?title=Moore%27s_law&oldid=1185981128 (visited on 12/01/2023).

Annotations: Wikipedia definition of Moore's law.

National Institute of Standards and Technology: Post-Quantum Cryptography **national_institute_of_standards_and_technology_post-quantum_2021**

National Institute of Standards and Technology. *Post-Quantum Cryptography: the Good, the Bad, and the Powerful*. Oct. 2021. URL: https://www.youtube.com/watch?v=uE_Y1C4QPU8 (visited on 11/26/2023).

Annotations: This video featuring NIST's Matthew Scholl emphasizes how NIST is working with the brightest minds in government, academia, and industry from around the world to develop a new set of encryption standards that will work with our current classical computers—while being resistant to the quantum machines of the future. Quantum computers will be incredibly powerful and will have the potential to provide tremendous societal benefits; however, there are concerns related to how quantum computers could be used by our adversaries, competitors, or criminals. This video explores these scenarios and explains how we are staying ahead of this potential cybersecurity threat.

National Institute of Standards and Technology: The Cybersecurity Framework **national_institute_of_standards_and_technology_cybersecurity_2016**

National Institute of Standards and Technology. *The Cybersecurity Framework*. Sept. 2016. URL: https://www.youtube.com/watch?v=J9ToNuwmyF0 (visited on 11/25/2023).

Annotations: Learn more about why organizations of all sizes and types should be using NIST's voluntary Cybersecurity Framework, which is based on existing standards, guidelines, and best practices. Created through collaboration between industry, academia and government, the flexible Framework helps organizations manage their cybersecurity-related risk.

NIST: Announcing PQC Candidates to be Standardized, Plus Fourth Round Candidates | CSRC **announcingfourth**

NIST. *Announcing PQC Candidates to be Standardized, Plus Fourth Round Candidates | CSRC*. EN-US. Mar. 2022. URL: https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4 (visited on 12/04/2023).

Annotations: NIST is announcing four Post-Quantum Cryptography candidates for standardization, plus candidates for a fourth round of analysis.

NIST Post-Quantum Cryptography Standardization **noauthor_nist_2023**

NIST Post-Quantum Cryptography Standardization. en. Page Version ID: 1184502030. Nov. 2023. URL: https://en.wikipedia.org/w/index.php?title=NIST_Post-Quantum_Cryptography_Standardization&oldid=1184502030#Finalists (visited on 11/25/2023).

Annotations: Up to date tabular representation of which algorithms have made it to which stages of the competition.

NSA: Quantum Computing and Post-Quantum Cryptography **nsa_pqc_faq**

NSA. *Quantum Computing and Post-Quantum Cryptography*. Aug. 2021.

Annotations: Comparing quantum computing and post-quantum cryptography.

NSA Releases Future Quantum-Resistant (QR) Algorithm Requirements for National Security Sy **noauthor_nsa_nodate**

NSA Releases Future Quantum-Resistant (QR) Algorithm Requirements for National Security Sy. en-US. URL: https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3148990/nsa-releases-future-quantum-resistant-qr-algorithm-requirements-for-national-se/http%3A%2F%2Fwww.nsa.gov%2FPress-Room%2FPress-Releases-Statements%2FPress-Release-View%2FArticle%2F3148990%2Fnsa-releases-future-quantum-resistant-qr-algorithm-requirements-for-national-se%2F (visited on 11/29/2023).

Annotations: The National Security Agency (NSA) released the "Announcing Commercial National Security Algorithm Suite 2.0" (CNSA 2.0) Cybersecurity Advisory (CSA) today to notify National Security Systems (NSS).

PBS Space Time: Why Quantum Computing Requires Quantum Cryptography
pbs_space_time_why_2019

PBS Space Time. *Why Quantum Computing Requires Quantum Cryptography*. May 2019. URL: https://www.youtube.com/watch?v=pi7YwxxZQ5A (visited on 11/25/2023).

Annotations: Quantum theory may seem like an obscure subject of questionable relevance to the average person. But in fact much of our technological world depends on our understanding of the quantum properties of the subatomic universe. And soon, perhaps very soon, we'll be interacting with the weirdness of quantum mechanics even more directly – with the coming of quantum computing and the quantum internet. Quantum computing is a topic that's that has been well covered, so we're going to be talking about the quantum internet. Specifically quantum cryptography and quantum key distribution – the foundations of the prospective quantum internet. We may come back to quantum computer in detail – but for now let me show you why their advent will demand a quantum internet.

Perimeter Institute for Theoretical Physics: Quantum 101 Episode 5
perimeter_institute_for_theoretical_physics_quantum_2023

Perimeter Institute for Theoretical Physics. *Quantum 101 Episode 5: Quantum Entanglement Explained*. Aug. 2023. URL: https://www.youtube.com/watch?v=rqmIVeheTVU (visited on 11/28/2023).

Annotations: Quantum entanglement is one of the most intriguing and perplexing phenomena in quantum physics. It allows physicists to create connections between particles that seem to violate our understanding of space and time.

Perlner et al.: Quantum Resistant Public Key Cryptography: A Survey
perlner_quantum_2009

Ray A. Perlner and David A. Cooper. "Quantum Resistant Public Key Cryptography: A Survey". en. In: (Apr. 2009).

Annotations: Public key cryptography is widely used to secure transactions over the Internet. However, advances in quantum computers threaten to undermine the security assumptions upon which currently used public key cryptographic algorithms are based. In this paper, we provide a survey of some of the public key cryptographic algorithms that have been developed that, while not currently in widespread use, are believed to be resistant to quantum computing based attacks and discuss some of the issues that protocol designers may need to consider if there is a need to deploy these algorithms at some point in the future.

Perlner et al.: Quantum Resistant Public Key Cryptography: A Survey nist_survey

Ray A. Perlner and David A. Cooper. "Quantum Resistant Public Key Cryptography: A Survey". en. In: (Apr. 2015).

Annotations: Public key cryptography is widely used to secure transactions over the Internet. However, advances in quantum computers threaten to undermine the security assumptions upon which currently used public key cryptographic algorithms are based. In this paper, we provide a survey of some of the public key cryptographic algorithms that have been developed that, while not currently in widespread use, are believed to be resistant to quantum computing based attacks and discuss some of the issues that protocol designers may need to consider if there is a need to deploy these algorithms at some point in the future.

Peter Schwabe et al.: CRYSTALS-Kyber kyber

Peter Schwabe et al. *CRYSTALS-Kyber*. Nov. 2022. URL: https://pq-crystals.org/kyber.

Annotations: Peter Schwabe gives a presentation on the (only) KEM protocol chosen by NIST, CRYSTALS-Kyber based on structured lattices, for standardization (thus far).

Post-Quantum Cryptography noauthor_post-quantum_nodate

Post-Quantum Cryptography. URL: https://www.dhs.gov/quantum (visited on 11/21/2023).

Post-Quantum Cryptography noauthor_post-quantum_nodate-1

Post-Quantum Cryptography: CISA, NIST, and NSA Recommend How to Prepare Now. en-US. URL: https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3498776/post-quantum-cryptography-cisa-nist-and-nsa-recommend-how-to-prepare-now/http%3A%2F%2Fwww.nsa.gov%2FPress-Room%2FPress-Releases-Statements%2FPress-Release-View%2FArticle%2F3498776%2Fpost-quantum-cryptography-cisa-nist-and-nsa-recommend-how-to-prepare-now%2F (visited on 11/26/2023).

Annotations: The National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), and National Institute of Standards and Technology (NIST) warned that cyber actors could target our.

Post-Quantum Cryptography noauthor_post-quantum_nodate-2

Post-Quantum Cryptography: CISA, NIST, and NSA Recommend How to Prepare Now. en-US. URL: https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3498776/post-quantum-cryptography-cisa-nist-and-nsa-recommend-how-to-prepare-now/http%3A%2F%2Fwww.nsa.gov%2FPress-Room%2FPress-Releases-Statements%2FPress-Release-View%2FArticle%2F3498776%2Fpost-quantum-cryptography-cisa-nist-and-nsa-recommend-how-to-prepare-now%2F (visited on 11/29/2023).

Annotations: Article from the NSA's official website about how CISA, NIST, and the NSA are working together and what they are advising for government organizations and the industry to do to prepare now.

PQCrypto 2020: PQCrypto 2020 | LIVE SESSION • Day 3 pqcrypto_2020_pqcrypto_2020

PQCrypto 2020. *PQCrypto 2020 | LIVE SESSION • Day 3*. Sept. 2020. URL: https://www.youtube.com/watch?v=CBGX1OMzN1o (visited on 11/26/2023).

Annotations: PQCrypto 2020 - live session - day 3 - Wednesday, September 23.

President Biden Signs Memo to Combat Quantum Computing Threat nsm_10

President Biden Signs Memo to Combat Quantum Computing Threat. en-US. URL: https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3020175/president-biden-signs-memo-to-combat-quantum-computing-threat/http%3A%2F%2Fwww.nsa.gov%2FPress-Room%2FNews-Highlights%2FArticle%2FArticle%2F3020175%2Fpresident-biden-signs-memo-to-combat-quantum-computing-threat%2F (visited on 11/29/2023).

Annotations: FORT MEADE, Md. — The White House announced today that President Joe Biden has signed a National Security Memorandum (NSM).

Qiskit: Information is Quantum - Charlie Bennett Lecture info_is_quantum

Qiskit. *Information is Quantum - Charlie Bennett Lecture*. July 2020. URL: https://www.youtube.com/watch?v=rslt-LwtDK4 (visited on 11/25/2023).

Annotations: Information is Quantum: How physics helped explain the nature of information and what can be done with it. The Quantum Computing Seminar Series is a deep dive into various academic and research topics within the quantum community. It will feature community members and leaders every Friday, 12 PM EDT.

Qiskit: Information is Quantum - Charlie Bennett Lecture qiskit_information_2020

Qiskit. *Information is Quantum - Charlie Bennett Lecture*. July 2020. URL: https://www.youtube.com/watch?v=rslt-LwtDK4 (visited on 11/25/2023).

Annotations: Information is Quantum: How physics helped explain the nature of information and what can be done with it.

Qiskit: Quantum Information's Revolutionary Origins | Charles Bennett charles_b

Qiskit. *Quantum Information's Revolutionary Origins | Charles Bennett*. July 2021. URL: https://www.youtube.com/watch?v=B5BUhzBlO-U (visited on 11/24/2023).

Annotations: Quantum information? Charles Bennett discusses the physicality of information, and the revolutionary ideas and thinkers that led up to the fusion of physics and computer science that eventually gave birth to the field of quantum information. Charles Bennett is widely considered to be one of the founding fathers of quantum cryptography for his discovery of the BB84 protocol.

Qiskit: The Story of Shor's Algorithm, Straight From the Source | Peter Shor shor

Qiskit. *The Story of Shor's Algorithm, Straight From the Source | Peter Shor*. July 2021. URL: https://www.youtube.com/watch?v=6qD9XElTpCE (visited on 11/23/2023).

Annotations: Hear the story of Shor's Algorithm, straight from the source, Peter Shor. Peter Shor talks about the key events, people, and discoveries that resulted in Shor's algorithm for quantum factorization.

Quantum computer startup first to break 1,000-qubit milestone atom_computing

Quantum computer startup first to break 1,000-qubit milestone. en-US. Section: Computers. Oct. 2023. URL: https://newatlas.com/computers/quantum-computer-startup-1-000-qubits/ (visited on 11/29/2023).

Annotations: A startup called Atom Computing has announced the first quantum computer to pass the 1,000-qubit milestone. The prototype, due to become available for use in 2024, leapfrogs IBM's announcement of its new quantum computer platform expected in the next few weeks.

Quantum cryptography wiki_qcrypto

Quantum cryptography. en. Page Version ID: 1184097474. Nov. 2023. URL: https://en.wikipedia.org/w/index.php?title=Quantum_cryptography&oldid=1184097474 (visited on 12/03/2023).

Annotations: Quantum cryptography is the science of exploiting quantum mechanical properties to perform cryptographic tasks. The best known example of quantum cryptography is quantum key distribution, which offers an information-theoretically secure solution to the key exchange problem. The advantage of quantum cryptography lies in the fact that it allows the completion of various cryptographic tasks that are proven or conjectured to be impossible using only classical (i.e. non-quantum) communication. For example, it is impossible to copy data encoded in a quantum state. If one attempts to read the encoded data, the quantum state will be changed due to wave function collapse (no-cloning theorem). This could be used to detect eavesdropping in quantum key distribution (QKD).

Quantum Readiness noauthor_quantum_2023

Quantum Readiness: Migration to Post-Quantum Cryptography. Aug. 2023. URL: https://media.defense.gov/2023/Aug/21/2003284212/-1/-1/0/CSI-QUANTUM-READINESS.PDF (visited on 11/29/2023).

Regenscheid: NIST Cryptographic Standards and Guidelines Development Process **regenscheid_nist_2016**

Andrew R. Regenscheid. *NIST Cryptographic Standards and Guidelines Development Process*. en. Tech. rep. NIST IR 7977. National Institute of Standards and Technology, Mar. 2016, NIST IR 7977. DOI: 10.6028/NIST.IR.7977. URL: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7977.pdf (visited on 11/26/2023).

Annotations: This document describes the principles, processes and procedures that drive cryptographic standards and guidelines development efforts at the National Institute of Standards and Technology (NIST). This document reflects public comments received on two earlier versions, and will serve as the basis to guide NIST's future cryptographic standards and guidelines development efforts. It will be reviewed and updated every five years, or more frequently if a need arises, to help ensure that NIST fulfills its role and responsibilities for producing robust, effective cryptographic standards and guidelines.

Sarah Yang et al.: Smallest transistor ever made by Berkeley Lab **yang_transistor**

Sarah Yang and Lawrence Berkley National Laboratory. *Smallest transistor ever made by Berkeley Lab*. en-US. Oct. 2016. URL: https://www.universityofcalifornia.edu/news/smallest-transistor-ever-made-berkeley-lab (visited on 12/01/2023).

Annotations: Berkeley Lab-led research breaks major barrier in transistor size by creating gate only 1 nanometer long.

Schrödinger's cat **schrodinger**

Schrödinger's cat. en. Page Version ID: 1185282962. Nov. 2023. URL: https://en.wikipedia.org/w/index.php?title=Schr%C3%B6dinger%27s_cat&oldid=1185282962 (visited on 11/27/2023).

Annotations: Definition of Schrodinger's cat.

Shi Bai et al.: CRYSTALS-Dilithium **dilithium**

Shi Bai et al. *CRYSTALS-Dilithium*. Nov. 2022.

Annotations: A presentation given on one of the digital signature schemes chosen by NIST for standardization. Presented at the Fourth PQC Standardization Conference (Day 1, Pt 1). The CRYSTALS-Dilithium team was represented by Vadim Lyubashevsky.

Shore: How the NSA Is Moving Toward a Quantum-Resilient Future **2022_nsa**

Patrick Shore. *How the NSA Is Moving Toward a Quantum-Resilient Future*. en. Text. Publisher: The Center for the National Interest. July 2022. URL: https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/how-nsa-moving-toward-quantum (visited on 11/29/2023).

Annotations: The NSA has consistently held its door open for collaboration with the private sector which will be critical as the United States moves forward into a new generation of cybersecurity.

Stoudenmire et al.: Grover's Algorithm Offers No Quantum Advantage **grover_no_adv**

E. M. Stoudenmire and Xavier Waintal. "Grover's Algorithm Offers No Quantum Advantage". In: (2023). Publisher: arXiv Version Number: 1. DOI: 10.48550/ARXIV.2303.11317. URL: https://arxiv.org/abs/2303.11317 (visited on 11/29/2023).

Annotations: Grover's algorithm is one of the primary algorithms offered as evidence that quantum computers can provide an advantage over classical computers. It involves an "oracle" (external quantum subroutine) which must be specified for a given application and whose internal structure is not part of the formal scaling of the quantum speedup guaranteed by the algorithm. Grover's algorithm also requires exponentially many steps to succeed, raising the question of its implementation on near-term, non-error-corrected hardware and indeed even on error-corrected quantum computers. In this work, we construct a quantum inspired algorithm, executable on a classical computer, that performs Grover's task in a linear number of call to the oracle - an exponentially smaller number than Grover's algorithm - and demonstrate this algorithm explicitly for boolean satisfiability problems (3-SAT). Our finding implies that there is no a priori theoretical quantum speedup associated with Grover's algorithm. We critically examine the possibility of a practical speedup, a possibility that depends on the nature of the quantum circuit associated with the oracle. We argue that the unfavorable scaling of the success probability of Grover's algorithm, which in the presence of noise decays as the exponential of the exponential of the number of qubits, makes a practical speedup unrealistic even under extremely optimistic assumptions on both hardware quality and availability.

Technology: Stateless Hash-Based Digital Signature Standard **technology_stateless_2023**

National Institute of Standards and Technology. *Stateless Hash-Based Digital Signature Standard*. en. Tech. rep. Federal Information Processing Standard (FIPS) 205 (Draft). U.S. Department of Commerce, Aug. 2023. DOI: 10.6028/NIST.FIPS.205.ipd. URL: https://csrc.nist.gov/pubs/fips/205/ipd (visited on 11/27/2023).

Annotations: Draft FIPS 205 for SPHINCS+.

The First Ever Quantum Computer - What Was it Used for? **noauthor_first_2019**

The First Ever Quantum Computer - What Was it Used for? en. Section: Quantum Science Article. Sept. 2019. URL: https://www.azoquantum.com/Article.aspx?ArticleID=143 (visited on 11/25/2023).

Annotations: Quantum computing is believed by many researchers to be the next step forward in information technology.

TheUnlockr: Quantum Computers Explained in a Way Anyone Can Understand **qc_explained**

TheUnlockr. *Quantum Computers Explained in a Way Anyone Can Understand*. Sept. 2021. URL: https://www.youtube.com/watch?v=zhQItO6_WoI (visited on 11/22/2023).

Annotations: Everything I've seen trying to answer what quantum computers are or how quantum computers work seems to always give me annote answers and just leaves me with more questions. So in this Decodr episode, I bugged the hell out of some quantum scientists and think I can give you a better understanding of what quantum computing is, how it works, and what it will help us with (and what it won't).

TheUnlockr: Quantum Computers Explained in a Way Anyone Can Understand **theunlockr**

TheUnlockr. *Quantum Computers Explained in a Way Anyone Can Understand*. Sept. 2021. URL: https://www.youtube.com/watch?v=zhQItO6_WoI (visited on 11/22/2023).

Annotations: Everything I've seen trying to answer what quantum computers are or how quantum computers work seems to always give me annote answers and just leaves me with more questions. So in this Decodr episode, I bugged the hell out of some quantum scientists and think I can give you a better understanding of what quantum computing is, how it works, and what it will help us with (and what it won't).

Third PQC Standardization Conference - Session I Welcome/Candidate Updates **noauthor_third_2021**

Third PQC Standardization Conference - Session I Welcome/Candidate Updates. en. Publication Title: NIST. June 2021. URL: https://www.nist.gov/video/third-pqc-standardization-conference-session-i-welcomecandidate-updates (visited on 11/26/2023).

Annotations: Video version of NIST Status Update on the 3rd Round at the 3rd PQC Standardization Conference.

Timeline of quantum computing and communication **qc_timeline**

Timeline of quantum computing and communication. en. Page Version ID: 1186184124. Nov. 2023. URL: https://en.wikipedia.org/w/index.php?title=Timeline_of_quantum_computing_and_communication&oldid=1186184124 (visited on 11/27/2023).

Annotations: Timeline of quantum computing.

Timeline of quantum computing and communication **noauthor_timeline_2023**

Timeline of quantum computing and communication. en. Page Version ID: 1186184124. Nov. 2023. URL: https://en.wikipedia.org/w/index.php?title=Timeline_of_quantum_computing_and_communication&oldid=1186184124 (visited on 11/27/2023).

Annotations: Timeline of quantum computing.

Timeline of quantum mechanics **q_mech_timeline**

Timeline of quantum mechanics. en. Nov. 2023. URL: https://en.wikipedia.org/w/index.php?title=Timeline_of_quantum_mechanics&oldid=1187393636 (visited on 12/01/2023).

Annotations: The timeline of quantum mechanics is a list of key events in the history of quantum mechanics, quantum field theories and quantum chemistry.

What is Open Source Software (OSS)? **noauthor_what_nodate**

What is Open Source Software (OSS)? en. URL: https://resources.github.com/open-source/what-is-open-source-software/ (visited on 11/29/2023).

Annotations: Get an overview of open source software (OSS) with this introductory guide—and explore recommendations for getting started.

Wikipedia: Bra–ket notation **braket**

Wikipedia. *Bra–ket notation*. en. Page Version ID: 1185285238. Nov. 2023. URL: https://en.wikipedia.org/w/index.php?title=Bra%E2%80%93ket_notation&oldid=1185285238 (visited on 12/03/2023).

Annotations: Definition of Bra-ket notation.

Wikipedia: Forward secrecy **wiki_forward**

Wikipedia. *Forward secrecy*. en. Page Version ID: 1186463564. Nov. 2023. URL: https://en.wikipedia.org/w/index.php?title=Forward_secrecy&oldid=1186463564 (visited on 12/04/2023).

Annotations: Definition of forward secrecy.

Wikipedia: Grover's algorithm **wiki_grover**

Wikipedia. *Grover's algorithm*. en. Page Version ID: 1182007968. Oct. 2023. URL: https://en.wikipedia.org/w/index.php?title=Grover%27s_algorithm&oldid=1182007968 (visited on 11/29/2023).

Annotations: Definition of Grover's algorithm.

Wikipedia: Grover's algorithm **wikipedia_grovers_2023**

Wikipedia. *Grover's algorithm*. en. Page Version ID: 1182007968. Oct. 2023. URL: https://en.wikipedia.org/w/index.php?title=Grover%27s_algorithm&oldid=1182007968 (visited on 11/29/2023).

Annotations: Definition of Grover's algorithm.

Wikipedia: Key encapsulation mechanism **wiki_kem**

Wikipedia. *Key encapsulation mechanism*. en. Page Version ID: 1185330307. Nov. 2023. URL: https://en.wikipedia.org/w/index.php?title=Key_encapsulation_mechanism&oldid=1185330307 (visited on 12/04/2023).

Annotations: Definition of KEM.

Wikipedia: One-time pad **wiki_otp**

Wikipedia. *One-time pad*. en. Page Version ID: 1184117794. Nov. 2023. URL: https://en.wikipedia.org/w/index.php?title=One-time_pad&oldid=1184117794 (visited on 12/03/2023).

Annotations: Definition of one-time pad.

Wikipedia: Quantum entanglement **entanglement**

Wikipedia. *Quantum entanglement*. en. Page Version ID: 1185961536. Nov. 2023. URL: https://en.wikipedia.org/w/index.php?title=Quantum_entanglement&oldid=1185961536 (visited on 12/03/2023).

Annotations: Definition of quantum entanglement.

Wikipedia: Shor's algorithm **wiki_shor**

Wikipedia. *Shor's algorithm*. en. Page Version ID: 1184979778. Nov. 2023. URL: https://en.wikipedia.org/w/index.php?title=Shor%27s_algorithm&oldid=1184979778 (visited on 11/29/2023).

Annotations: Shor's algorithm is a quantum algorithm for finding the prime factors of an integer. It was developed in 1994 by the American mathematician Peter Shor. It is one of the few known quantum algorithms with compelling potential applications and strong evidence of superpolynomial speedup compared to best known classical (that is, non-quantum) algorithms. On the other hand, factoring numbers of practical significance requires far more qubits than available in the near future. Another concern is that noise in quantum circuits may undermine results, requiring additional qubits for quantum error correction. Shor proposed multiple similar algorithms solving the factoring problem, the discrete logarithm problem, and the period finding problem. "Shor's algorithm" usually refers to his algorithm solving factoring, but may also refer to each of the three. The discrete logarithm algorithm and the factoring algorithm are instances of the period finding algorithm, and all three are instances of the hidden subgroup problem.

Wikipedia: Side-channel attack **wiki_sidechannel**

Wikipedia. *Side-channel attack*. en. Page Version ID: 1187795463. Dec. 2023. URL: https://en.wikipedia.org/w/index.php?title=Side-channel_attack&oldid=1187795463 (visited on 12/04/2023).

Annotations: Definition of side-channel attack.

Wikipedia: Uncertainty principle **uncertainty**

Wikipedia. *Uncertainty principle*. URL: `https://en.wikipedia.org/wiki/Uncertainty_principle` (visited on 12/03/2023).

Annotations: Definition of the Heisenberg uncertainty principle.

Wikiversity: Dirac's notation **dirac**

Wikiversity. *Dirac's notation*. en. URL: `https://en.wikiversity.org/wiki/Dirac%27s_notation` (visited on 12/03/2023).

Annotations: Dirac notation definition has more detail that bra-ket notation definition.

Wright: The Desk Encyclopedia of World History **info_rev**

Edmund Wright, ed. *The Desk Encyclopedia of World History*. eng. OCLC: 85485736. Oxford [England]: Oxford University Press, 2006. ISBN: 978-0-7394-7809-7.

Annotations: Encyclopedia entry defining the information revolution.

Wright: The Desk Encyclopedia of World History **wright_desk_2006**

Edmund Wright, ed. *The Desk Encyclopedia of World History*. eng. OCLC: 85485736. Oxford [England]: Oxford University Press, 2006. ISBN: 978-0-7394-7809-7.

Annotations: Encyclopedia entry defining the information revolution.

Yehia et al.: Hash-based Signatures Revisited **yehia_hash-based_2020**

Mahmoud Yehia, Riham AlTawy, and T. Aaron Gulliver. *Hash-based Signatures Revisited: A Dynamic FORS with Adaptive Chosen Message Security*. Publication info: Published elsewhere. Africacrypt 2020. 2020. URL: `https://eprint.iacr.org/2020/564` (visited on 11/27/2023).

Annotations: Definition of FORS scheme used as basis for SPINCS+.