Post-Quantum cryptography refers to cryptographic algorithms that are secure both classically and against attacks using quantum computers, when they arrive. Governments and high-tech companies are spending large sums of money building these quantum computers with some success from companies like Google, IBM, and others. The large-scale quantum computers needed to break internet encryption are not available today, but that day is fast approaching.

NIST PQC Standardization

NIST, the National Institute of Standards and Technology is currently in the middle of a multiyear standardization process for post-quantum cryptography[i]. The result of this process will be standardized algorithms that will replace current algorithms in use today which are not quantum-safe. This includes algorithms such as RSA, ECDH, ECDSA, and the Diffie-Hellman key exchange. These algorithms account for more than 95% of public-key cryptography currently in use on the internet.

Round 3 of this process is expected to start as early as April 2020. As seen in Figure 1, there are currently 17 Key Encapsulation Mechanisms (KEMs) and 9 Digital Signature Algorithms (DSAs) remaining out of an initial 82 total submissions.

NIST has not quantified how many algorithms it plans to standardize of each category, other than a statement of most likely “more than one”. This is primarily due to that fact that previous (i.e. classical) standardization efforts have always found a single solution that was optimal in each category. In this case there are many trade-offs to consider. Additionally, standardizing multiple post-quantum algorithms will give additional options incase mathematical advances render classical algorithms and/or these post-quantum algorithms broken even before quantum computers are available. By having multiple options, we allow ourselves choices when it comes to migration and hybrid schemes.

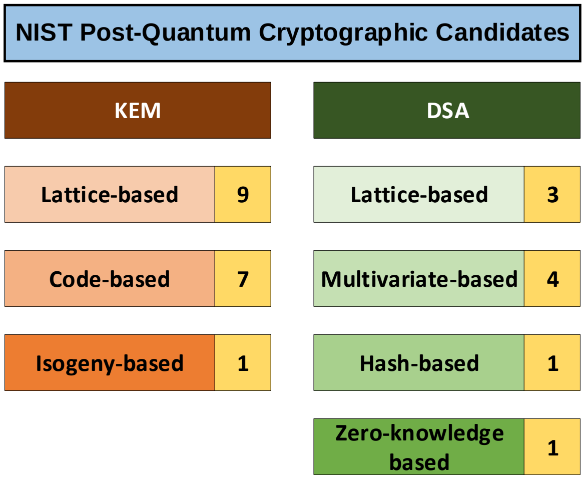


Figure 1: 17 KEM and 9 DSA algorithms still in Round 2 of the NIST standardization process.

NIST has already begun the standardization of two stateful hash-based signature schemes. These are the eXtended Merkle Signature Scheme (XMSS) and the Leighton-Micali Signature system (LMS). These schemes cannot be universally used in all situations but offer some options for situations where the need for post-quantum solutions arises before this standardization process is complete.

KEM vs DSA

The difference between KEMs and DSAs is mostly in their purpose. They are both public-key algorithms and are both used when sending encrypted messages. KEMs are designed to create a public and private key between two parties so information can be encrypted, sent, and decrypted once received.

While transmitted messages are usually encrypted using a symmetric key algorithm (i.e. AES) because of their efficiency, these algorithms cannot be used to generate the secret key they require. Therefore, a different type of algorithm is needed. This is where asymmetric cryptographic algorithms (or public-key algorithms) are used. A KEM incorporates a specific public-key algorithm but simplifies, and encapsulates the entire process, making it faster and more secure. KEMs generate a public and private key pair. Anyone can use the public key to encrypt, but only the receiver has the private key to decrypt.

DSAs are public-key algorithms that work a bit in reverse. When a message is received it could have been tampered with during transmission, come from a false source, or the person sending it could argue he/she ever sent it. DSAs are used to verify the source and the contents much in the same way a wax stamp seal was/is used on important documents.

Classical key exchange schemes are already at risk because of fears of retroactive decryption of highly sensitive data. This type of attack is known as a 'harvest and decrypt' attack because huge databases of encrypted data are currently being stored (harvested), and waiting for the day it can be broken (decrypted). This means we need quantum-safe KEMs in place years before quantum computers are available.

Digital signature schemes are not in the same immediate danger and have a few more years of leeway. Retroactively breaking authentication is mostly pointless since verification is done upon immediate receival. Without access to a quantum computer, we assume these current signature algorithms are secure.

Other Standards

NIST is not the only standardizing body studying quantum-safe algorithms and releasing guidelines. In 2015, the National Security Agency (NSA) publicly stated that this transition needs to happen, and we "Must act now". Since then, (some even before) many standardizing bodies have made this one of their top priorities.

ETSI, the European Telecommunications Standards Institute, has a working group, TC Cyber, or Technical Committee Cyber, that has been focused on the practical implementation of quantum-safe primitives since 2015 and has published an ETSI Guide that discusses the transition to post-quantum cryptography and some of the challenges. ETSI has also partnered with the Institute for Quantum Computing (IQC) and held yearly workshops in the area of post-quantum cryptography since 2013.

The Internet Engineering Task Force (IETF) is also focused on promoting voluntary internet standards and has a dedicated Crypto Forum Research Group (CFRG). This working group is currently developing Request for comment (RFC) protocols compatible with post-quantum cryptography.

ANSI, the American National Standards Institute, is the leading provider of U.S. standards and conformity assessment system. The Accredited Standards Committee X9F is the subcommittee of ANSI responsible for data and information security. This working group has already made some recommendations on lattice-based algorithms as far back as 2010.

IEEE, the Institute of Electrical and Electronics Engineers is a leading developer of international standards. The IEEE P1363 standardization project has been providing specifications for public-key cryptography dating back to 2008.

IETF, the Internet Engineering Task Force and the Internet Research Task Force (IRTF) have their own standards process and working groups. Specifically, the Crypto Forum Research Group (CFRG) is working to ease the transition from theory to practice by keeping the internet community aware of what is going on.

ISO, the International Organization for Standardization, is the largest international standards organization and has teamed with the International Electrotechnical Commission (IEC) for a Joint Technical Committee called ISO/IEC JTC 1. This committee is focused on adopting standards and protocols dedicated to post-quantum cryptography.

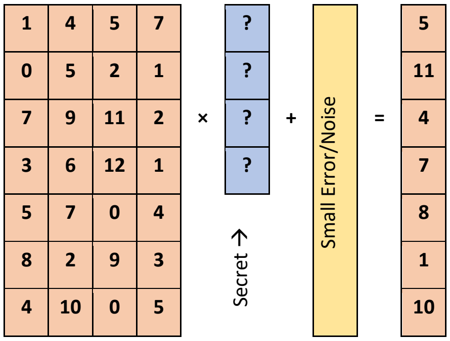
BSI, The German Federal Office for Information Security also released technical guidelines that recommend algorithms and key-lengths and makes specific recommendations of Merkle based signature schemes and XMSS.

China as well has begun its post-quantum standardization process similar to NISTs. This process received submissions in 2019 and has since begun investigating these candidates.

Other organizations are also making suggestions as well as testing and evaluating these proposed solutions. Choosing which solution (and when) to adopt will be a difficult choice so the suggestions from these bodies will be needed.

Mathematical Categories

While the exact details of each algorithm submitted to NIST and/or recommended by other bodies are different, there is a small subset of mathematical foundations they mostly seem to rely on.



$$\begin{bmatrix} 1 & 4 & 5 & 7 \\ 0 & 5 & 2 & 1 \\ 7 & 9 & 11 & 2 \\ 3 & 6 & 12 & 1 \\ 5 & 7 & 0 & 4 \\ 8 & 2 & 9 & 3 \\ 4 & 10 & 0 & 5 \end{bmatrix} \times \underbrace{\begin{bmatrix} ? \\ ? \\ ? \\ ? \end{bmatrix}}_{\text{Secret} \rightarrow} + \text{Small Error/Noise} = \begin{bmatrix} 5 \\ 11 \\ 4 \\ 7 \\ 8 \\ 1 \\ 10 \end{bmatrix}$$

Figure 2: Lattice based cryptography uses a random matrix along with the secret vector and some small error to compute the resultant vector. All operations are done modulo a prime number.

Lattice-based solutions are based on a set of defined basis vectors (think distance and direction) that generate a whole set. The security of lattice-based solutions relies on the difficulty of computing the Shortest Vector Problem (SVP). As in Figure 2, a small amount of noise is added into the computations to make it extremely difficult to recover the secret even if one was given the random matrix and resultant vector. This is called learning with errors (LWE). Variants of this problem included Ring-LWE, Module-LWE, and LWR or Learning with Rounding.

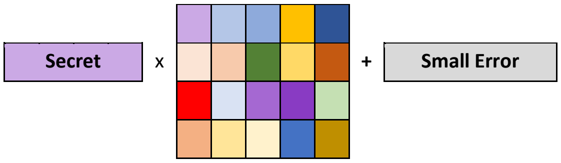


Figure 3: Code-based cryptography multiplies the secret by a public generator matrix and adds a small error that can be corrected. The public matrix is generated by scrambling and permuting the private matrix.

Code-based solutions use error-correcting codes that will "correct" to the closest code word in a given set. For an outsider or a hacker, finding this set of code words is extremely difficult, and thus correcting to the closest code word is nearly impossible. This type of post-quantum solution is the oldest and dates back to 1978 (McEliece). Because the public and private keys are large matrices (the private key is three large matrices), their key sizes tend to be quite large. However, encryption and decryption are faster than traditional RSA. Code-based cryptography does share many similarities with lattice-based cryptography but also has less restrictions.

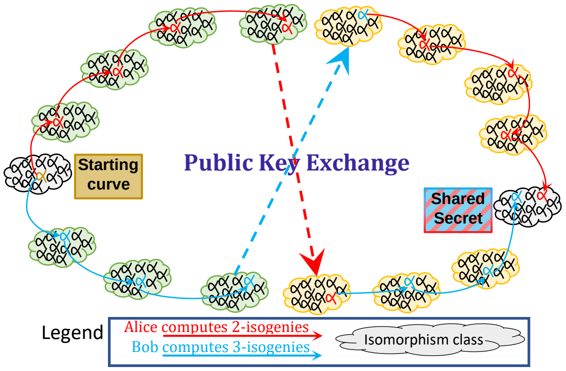


Figure 4: Example of an isogeny-based key exchange. The final curves may be different, but they are isomorphic and thus share a common number called the j-invariant which is used as the shared secret.

Isogeny-based solutions can be thought of as maps from one elliptic curve to another[ii]. This map can resemble the virtual 'handshake' seen in Diffie-Hellman. Isogenies of large degree are infeasible to compute in one step, so many tiny steps are taken. In Figure 4, Alice takes more smaller steps and Bob takes less larger steps. Once they reach their respective images, they swap curve information and repeat the process from each other's curve. Alice and Bob do not always end on the exact same graph, but their graphs will be isomorphic. Isogenies are the youngest but are also the most studied since the NIST PQC process began.

Multivariate-based solutions are based on a system of equation with 'multiple variables'. The polynomials are usually only of degree two, however, solving this system is still quite complicated without the secret key. These solutions are fast and offer the shortest signatures of all post quantum candidates.

Hash-based solutions use a pseudo-random function to turn any size input into an encrypted, specific size output. Hash functions are also called one-way functions as they are not easily (i.e. computationally complex) computed in reverse. This is what makes them very useful in authenticating signatures.

Zero-knowledge based solutions use the idea of zero-knowledge proofs where one party proves to another party, they know the answer without exchanging information that would give away the answer or help determine the answer for anyone eavesdropping. Also, no one other than the two parties involved would be able to prove either of them do in fact, know the answer.

Market

As talks of quantum computers increase, so does the market for post-quantum solutions. Currently, companies are testing out these proposed solutions on cloud servers, but another potential and growing market is IoT. With connected cars, smart homes, smart cities, connected health and more, the need for securing these devices will be vital as our digital world continues to incorporate into every aspect of our daily lives.

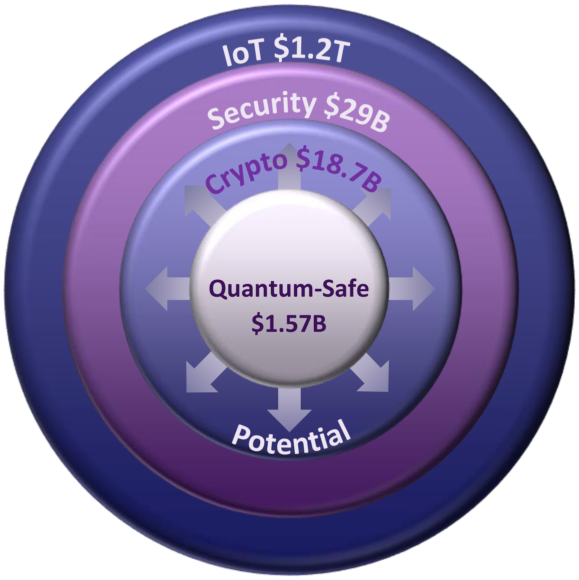


Figure 5: Markets related to IoT and IoT security

Cars can take up to 15 years from concept to market. Similarly, medical devices can take over 10 years of testing and research before they are brought to market. In both of these cases, consumers expect the devices themselves to last decades to come. For these reasons and more, companies are hoping to find working solutions sooner rather than later.

There are currently more than 10 billion IoT connected devices in use today and that number is expected to more than double in just five years. With each of these devices not only being under threat themselves, but also gateways into someone's home network, bank accounts, hospital records, as well as city and government infrastructures, we see the quantum-safe security market for IoT devices alone growing rapidly as seen in Figure 5.

Post-Quantum Candidates

Each mathematical category offers its own unique type of solution with its own pros and cons. A lengthier discussion of post-quantum cryptography and candidates can be found here[iii] but for KEM algorithms, the takeaway is code-

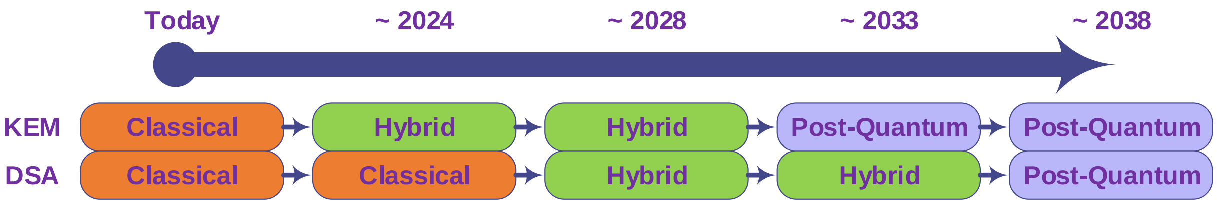


Figure 6: Transition from classical to post-quantum cryptography will need a hybrid period that is different for KEM and DSA.

based algorithms (e.g. McEliece) are fast but have large key sizes while isogeny-based solutions (SIKE) have very small key sizes but are relatively slow. Lattice-based solutions offer a middle ground of these two extremes, and more subdivisions within this category as well with additional tradeoffs. However, with so many KEM candidates remaining, it is hard to see what direction NIST will go. Since McEliece is the oldest and most studied, it is likely to be standardized. However, because of its large key size, it is also not ideal for most situations.

There are more categories for DSAs, but less candidates. While results of Round 2 are still uncertain it is looking like finalists for DSAs will be chosen only from the lattice-based and hash-based algorithms as these are the ones currently being studied in depth and thus, better understood.

Once Round 3 of the NIST PQC process is underway, the field will be narrowed to a select few finalists which all will have a high chance of being standardized. It is still possible for some candidates to merge for a single submission, but that window of opportunity is closing quickly.

It is expected that once the Round 3 candidates are announced, there will be surge of commercialization efforts taking place. Similarly, research will be consolidated into mostly these finalists and hopefully any potential weaknesses are completely explored.

Hybrid Schemes

Figure 6 illustrates the anticipated transition to quantum-safe schemes. Before we can move to quantum-safe only schemes, there will be a phase using hybrid cryptosystems where two or more cryptosystems are involved to exchange keys or create a signature[iv]. The benefit to using more than one cryptosystem is that now an attacker must break each individual system to break a key exchange or digital signature. The main drawbacks, of course, are that now we have additional computations, communication overhead, and storage.

Currently, we are not ready to adapt the current infrastructure to a post-quantum infrastructure as many complex design and security questions are left unexplored.

There are multiple ways of constructing the hybrid algorithms, but the main takeaway is that the combined system must have security at least as secure as each individual system. For example, you could run each system individually and concatenate the keys before they are sent, or one algorithm run first and its output used as input to the second algorithm.

Hybrid KEM algorithms are expected to be rolled out and put in place first as the current internet integrity relies on post-quantum algorithms being adopted quickly. As DSAs are only required once large-scale quantum computers are available, they are expected to begin the transition later, closer to the anticipated date of large-scale quantum computers being available. Once these algorithms have been put in place and thoroughly vetted, the removal of classical cryptographic algorithms will be beneficial to increase performance and speed.

There is one post-quantum candidate that offers a potential unique solution to this hybrid problem. Not only do isogeny-based solutions offer the smallest key size (but are also the slowest) they offer a unique hybrid solution with classical elliptic curve cryptography such as ECDH. Isogenies, in essence, are maps between elliptic curves, and since point arithmetic is already part of isogeny computations, very little additional hardware/software would be required to implement say Curve25519 or Curve448 to construct a secure hybrid scheme.

Even more interesting, an ECDH scheme could be designed to work directly on the primes used in SIKE, say p434, further reducing the overhead to almost no additional architecture required.

Key Size

Key size of submitted post-quantum algorithms is one of the biggest points of contention. While most of these post-quantum algorithms have key sizes larger than classical algorithms and performance speeds that are slower, this does not mean they are not still practical. Especially on servers and cloud computing that is already done by super computers. However, on smaller devices like embedded devices and IoT devices where power, energy, and even bandwidth are at a premium, there are concerns for some of the candidates. Some code-based candidates have key sizes of up to 1MB. Not only must this entire key be stored on a device, it must also be constructed/transferred over an unsecure channel usually requiring this amount of data being transmitted as well.

Communication overhead is generally more expensive (power consumption and energy usage) than computational overhead. Similarly, smaller bandwidths reduce power consumption and can increase the range of transmissions. This does, however, increase in the number of packets needed to be sent and potentially lost.

A small key and limited computations would be ideal, but no single post-quantum candidate fits this description. So, a choice must be made. When resources are at a premium, it seems logical to focus on key size as a means to decrease power and energy consumption and increase efficiently of data transfer.

The smallest of the key sizes comes from Isogeny-based solutions (SIKE) which ranges from about 200 bytes in a compressed version of its lowest security level to 560 bytes in its highest security uncompressed version. To put this in perspective, the recommend key size of RSA is 384 bytes. The next smallest post-quantum key sizes are from lattice-based solutions which range from 1-10KB for the smallest security level, making them at least 5-10 times larger.

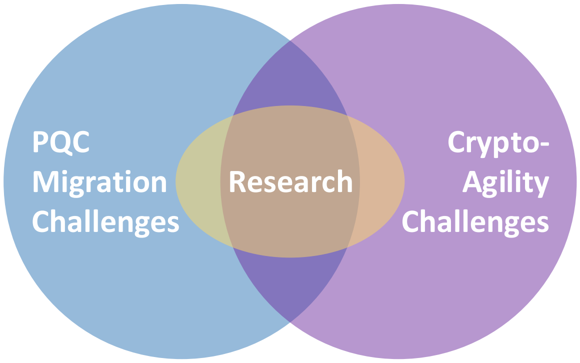


Figure 7: More research is needed before adoption[iv].

Implementation Challenges

Transitioning to new internet standards has always been a challenge and the transition from classical to post-quantum cryptography will probably be the most challenging yet. It has taken over 15 years for the majority of the internet to switch from RSA to ECC and many still haven't. Similarly, some that have, created footguns into the code while trying to implement a modified version. Lack of a strong understanding of the underlying mathematics is probably one of the leading factors, along with resistance to change. Since post-quantum solutions won't have a 'one size fits all' solution, the resistance to change will be even stronger.

In classical cryptography the choices were very simple. The key size directly related to the security level, and once that was determined, so was your choice. With lattice-based schemes and code-based schemes for example, there are multiple parameter choices that must be completed and implemented properly for the solution to be secure. These parameters are chosen by the designers of the scheme and are expected to be secure choices, but they will need to be implemented in the way they were designed.

Hardware implementations versus software implementations will also be a challenge as these costs (ex. monetarily, speed, power, ease of change, etc.) will also be exaggerated in this new set of solutions. While it is still early in the process, there is a lot of work to be done to make sure these algorithms are market ready before the standardization efforts are complete. Redesigning hardware architectures and making sure the software code not only functions properly but is compatible with the current internet will be a challenge itself.

Similarly, as hybrid solutions seem inevitable, trying to preserve the current classical solutions alongside the new post-quantum solutions (and then eventually removing the classical solutions) will be a challenge.

Even when all this is said and done, formal verification and testing will need to be done. As the technology becomes increasingly sophisticated it becomes out of the scope of most companies' IT department and they will either need to hire outside assistance for this, or hope they followed the complicated standardizations exactly. Even in the instances that companies plan to hire outside assistance, there are very few specialists worldwide working on this currently. Luckily many experts are professors and are attracting graduate students to work on these problems, paving the way for more industry experts than ever before.

[i] NIST - https://csrc.nist.gov/Projects/post-quantum-cryptography/round-2-submissions
[ii] Isogeny Explorer - https://isogenies.enricflorit.com/
[iii] Nature, Post-Quantum Cryptography - https://doi.org/10.1038/nature23461
[iv] Computing Community Consortium - https://cra.org/ccc/events/identifying-research-challenges-in-pqc-migration-and-cryptographic-agility/