Secure Quantum Computing

Syllab.io

SylLab Systems

Secure quantum computing

Introduction

Quantum computing has been a futuristic technology for many years. While the theory behind quantum physics and quantum computing has been around for decades, implementations have lagged behind. For several years, quantum computing has been "just around the corner" but has never arrived.

In the last few years, this has changed, and the development of quantum computing has accelerated rapidly. Today, IBM has a 127-qubit quantum computer and plans to reach over 4,158 qubits by 2025. Since quantum computers' capabilities grow exponentially with the number of qubits, these systems are rapidly outpacing the capabilities of classical computers.

The emergence of quantum computing has significant implications for technology. Quantum computers work very differently from the classical ones today, making previously infeasible computations possible. While this has its benefits, it also has its downsides, especially in the areas of cryptography and cybersecurity.

How Does Quantum Computing Differ from Classical Computing?

At its core, traditional computing boils down to bits. A bit can hold the values 0 or 1, and collections of bits can be used to store various types of information. By manipulating and performing calculations with these bits, it is possible to build the IT infrastructure that exists today.

Quantum computers don't use bits. Instead, they use quantum bits or "qubits", which work very differently from the bits used in quantum computers. Instead of always storing a value of 0 or 1, a qubit can store a superposition of the two states, simultaneously holding the values of both 0 and 1.

Qubits can be used in calculations just like bits, but their ability to simultaneously store the values 0 and 1 means that these calculations can work very differently than on classical computers. For example, consider the case where a computer needs to test which two-bit value — 00, 01, 10, or 11 — achieves the desired result in an equation. In a classical computer, this would require four executions of the equation, one with each of the four values.

With a quantum computer, on the other hand, quantum superposition means that two qubits can store all four possible values simultaneously. This enables the quantum computer to complete the calculation in a single run, much more quickly than a classical computer.

With quantum computing, each additional qubit doubles the number of values that can be stored and used in computations. This makes quantum algorithms much better at solving certain problems than classical ones.

Quantum computers will be used for numerous important tasks, such as medical research and cybersecurity. Ensuring the security of these computers is essential to the validity of their computations and results.

The Impacts of the Rise of Quantum Computing

Quantum computers are fundamentally different from classical computers, and these differences can have significant impacts. Once large-scale quantum computing is available, quantum computing can revolutionize research in fields such as medicine. While a classical computer may have to grind through each possible input to a function to find valid solutions, a quantum computer can take advantage of quantum superposition to test many options at once.

However, the most famous and wide-reaching impact of quantum computing comes in the field of cryptography. Quantum computing has the potential to dramatically improve the security of encryption key creation and exchange. However, it poses a significant threat to the security of public key cryptographic algorithms.

Securing Encryption Keys with Quantum Physics

Symmetric encryption algorithms, such as AES, depend on a shared secret key. The security of the encryption process depends on this key being randomly generated and securely shared between the two parties. If an attacker can guess an encryption key or eavesdrop on the communications where it is exchanged between the two parties, then encryption provides no benefit for data security.

Quantum physics can help secure both phases of this process. Quantum computers can generate more random encryption keys than classical computers and can provide stronger security guarantees for key exchange.

Quantum Random Number Generation

Ideally, the secret keys used for data encryption and decryption should be completely random. In practice, encryption keys are usually generated using a pseudorandom number generator (PRNG) that is seeded with a random value.

This means that encryption keys are less random and secure that they otherwise could be. For example, a PRNG could be seeded with a non-random number or tampered with by an attacker to produce more predictable values.

Quantum random number generators (QRNGs) use the laws of quantum physics to generate provably random values. By using quantum sources of randomness, such as observing the state of a quantum particle, it is possible to generate encryption keys that are much more random and secure than ones created by classical computers.

Secure Quantum Key Distribution

The primary difference between symmetric and asymmetric cryptography is that symmetric algorithms use the same key for encryption and decryption while asymmetric algorithms use a pair of related keys. Symmetric algorithms need this shared key to be shared between two parties over a shared channel in some way.

Often, the generation of a shared secret key for symmetric encryption algorithms is performed using asymmetric cryptographic algorithms. However, symmetric algorithms used in this way become vulnerable to quantum computers when the asymmetric cryptography that they use becomes insecure.

Quantum key distribution (QKD) provides an alternative that renders it impossible for an attacker to eavesdrop on the transmission of a shared secret key between two parties.

In a QKD system, one party randomly selects one of two orthagonal quantum states and polarizes a photon in that state, encoding it as a 0 or 1, before transmitting it to the recipient. At the other end, the recipient measures the polarization of the photon in a randomly-selected state. After comparing the list of selected states and discarding the bits for which mismatched states were used, the two parties calculate their error rate by revealing a portion of their measured bits.

Under normal circumstances, the quantum bit error rate (QBER) will be under a certain threshold that accounts for interference due to random noise. However, if an attacker attempts to eavesdrop on a connection by intercepting photons, measuring them in a randomly-selected state, and transmitting appropriately-polarized photons, the photons for which they incorrectly guessed the state used will introduce additional errors. This enables the parties to detect the eavesdropping and discard the shared key as insecure.

Breaking Public Key Cryptography

Many modern IT systems rely on public-key or asymmetric cryptography to ensure the confidentiality, integrity, and authenticity of data. Asymmetric encryption enables confidential communications between parties without a preshared encryption key. Key exchange protocols allow the creation of shared secrets over a public channel. Digital signatures prove the integrity and authenticity of the signed data.

Public Key Cryptography and "Hard" Problems

The security of public-key cryptography relies on the asymmetric complexity of an underlying mathematical function. For example, the complexity of multiplying two large, prime numbers together has polynomial complexity; however, factoring the result has exponential complexity. In the factoring problem, the complexity of multiplication grows relatively slowly with the length of the values being multiplied. For example, multiplying two 257-bit numbers is only marginally more difficult than multiplying two 256-bit numbers.

Factoring, on the other hand, is much harder because the best-known algorithms for factoring the product of two prime numbers on a classical computer aren't much better than a brute-force search. If the size of the values being multiplied increases by a single bit, the number of potential factors to search doubles.

Public key cryptography's asymmetric complexity makes it possible to develop usable, secure systems. Legitimate users can perform "easy" calculations (like multiplication), while an attacker must perform a "hard" calculation (like factoring). By selecting a key length where the "easy" operation is possible but the "hard" one is not, these algorithms are made both usable and secure.

Quantum Computing Breaks Classical Asymmetric Cryptography

Classical asymmetric cryptography's security depends on the fact that the factoring and discrete logarithm problems can't be solved in polynomial time. This is true because a brute force search for factors by a classical computer quickly becomes infeasible as the length of the factors increases.

However, quantum computers work fundamentally differently than classical ones, and these differences have a significant impact on the security of classical asymmetric cryptography. Shor's algorithm is a quantum computing algorithm that is capable of solving the factoring problem in polynomial — rather than exponential — time when run on a sufficiently large quantum computer.

The existence of Shor's algorithm means that classical public-key cryptography based on the factoring and discrete logarithm problems has an expiration date. A

transition to post-quantum algorithms before quantum computers capable of running Shor's algorithm for the key lengths used in modern cryptography is essential to protecting data privacy and security.

Why the Quantum Threat Isn't a Reality Yet

Quantum computers have been "on the horizon" for many years now. Today, real quantum computers exist, and rapid progress is being made. In 2021 , IBM unveiled a quantum computer with 127 qubits. In 2023, the company's quantum roadmap includes a 1,000-qubit quantum computer.

However, today's quantum computers still lag behind modern classical computers, and they have a long ways to go before they pose a serious threat to the security of classical asymmetric cryptography. The reason for this is that large quantum computers are very difficult to build.

Two types of qubits exist: physical and logical qubits. A physical qubit is something capable of achieving quantum superposition, such as a trapped ion or a photon. A logical qubit is created using physical qubits and actually allows quantum computations. Ideally, every physical qubit would be a logical qubit, but this is not always the case.

The reason for this is that physical qubits are extremely unstable. To maintain the superposition that makes quantum computing so powerful, they need to be kept in a very stable, isolated environment. Any interference in this environment, such as a nearby atom vibrating, can cause the qubit to lose its superposition, resolving to a value of 0 or 1.

This loss of superposition by a qubit can cause an error in the calculations being run on a quantum computer using it. As a result, quantum computers need a means of detecting and correcting these errors. However, due to the vagaries of quantum physics, observing the state of a qubit — which can be helpful for identifying and fixing errors — also causes it to lose its superposition.

The biggest challenge in building a quantum computer is ensuring that it is stable for long enough to perform the necessary calculations and that the result of those calculations is correct. The complexity of doing this is why quantum computers large enough to threaten the security of classical asymmetric cryptography are still several years off, providing an opportunity to develop and deploy post-quantum cryptographic algorithms before quantum computing and Shor's algorithm pose a significant threat to data privacy and security.

Preparing for the Post-Quantum Future

Quantum computers capable of performing useful computations and posing a threat to the security of classical asymmetric cryptography are still years away. However, the existence of these quantum computers in the future still poses a threat to data security today.

With large-scale quantum computing on the horizon, “store now, decrypt later” attacks have become a serious threat. Organizations that collect and store communications protected with quantum-vulnerable classical encryption algorithms can decrypt these messages in the future when the necessary technology becomes available. While this data may be “stale” by then, it might also contain sensitive information.

The looming threat of quantum computing has inspired the National Institute of Standards and Technology (NIST) to initiate a Post-Quantum Cryptography Standardization Process and has spurred the development of post-quantum algorithms and implementations. The goal of these initiatives is to ensure that post-quantum cryptography is available and deployed before large-scale quantum computing is available.

However, the post-quantum threat is real today. “Store now, decrypt later” attacks threaten the decryption of data encrypted today once quantum computers become available. While some data may be “stale” by the time quantum computers are available, other data may remain sensitive. Additionally, the process of transitioning to post-quantum algorithms is a complex and time-consuming process, making it difficult for companies to transition rapidly once the quantum threat becomes a reality. Making the change as soon as possible is essential to minimizing the risk and impact on an organization’s data security.

SylLab Systems is helping organizations to start the transition to post-quantum today, improving not only data security but also the speed and efficiency of post-quantum algorithms. To learn more about the solutions and services that SylLab Systems can offer to support your organization’s post-quantum transition, schedule a meeting today or contact us at contact@syllab.io.