An Introduction to Key Quantum Distribution

While the word "quantum" has only started trending in the technology space during the last decade, many past technologies already relied on our understanding of the quantum world, from lasers to MRI imaging, electronic transistors, and nuclear power. The reason quantum has become so popular lately is that researchers have become increasingly better at manipulating individual quantum particles (light photons, electrons, atoms) in ways that weren't possible before. These advances allow us to harness more explicitly the unique and weird properties of the quantum world. They could launch yet another quantum technology revolution in areas like sensing, computation, and communication.

What is a quantum computer?

The power of quantum computers comes chiefly from the superposition principle. A *classical* bit can only be in a 0 or 1 state, while a *quantum bit (qubit)* can exist in several 0 and 1 state combinations. When one measures and observes the qubit, it will *collapse* into just one of these combinations. Each combination has a specific probability of occurring when the qubit collapses.

While two classical bits can only exist in one out of four combinations, two quantum bits can exist in all these combinations simultaneously before being observed. Therefore, these qubits can hold more information than a classical bit, and the amount of information they can hold grows exponentially with each additional qubit. Twenty qubits can already hold a million values simultaneously (2^{20}), and 300 qubits can store as many particles as there are in the universe (2^{300}).

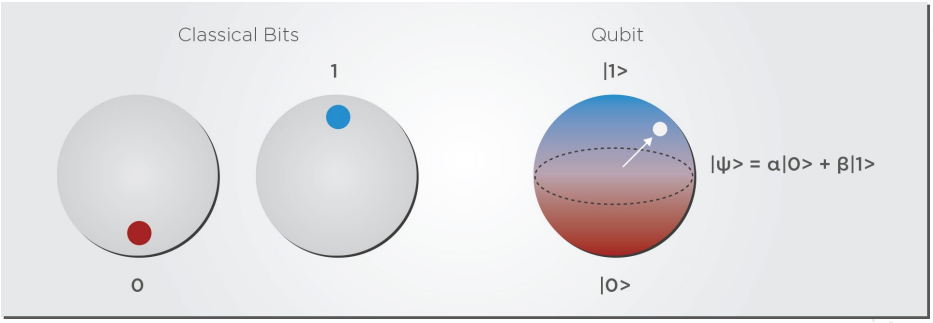

Figure 1: Classical bits in 0 or 1 state vs a qubit in a superposition of |0⟩ *and* |1⟩ *states.*

However, to harness this potential processing power, we must understand that probabilities in quantum mechanics do not work like conventional probabilities. The probability we learned about in school allowed only for numbers between 0 and 1. On the other hand, probabilities in quantum mechanics behave as waves with *amplitudes* that can be positive or negative. And just like waves, quantum probabilities can interfere, reinforcing each other or cancelling each other out.

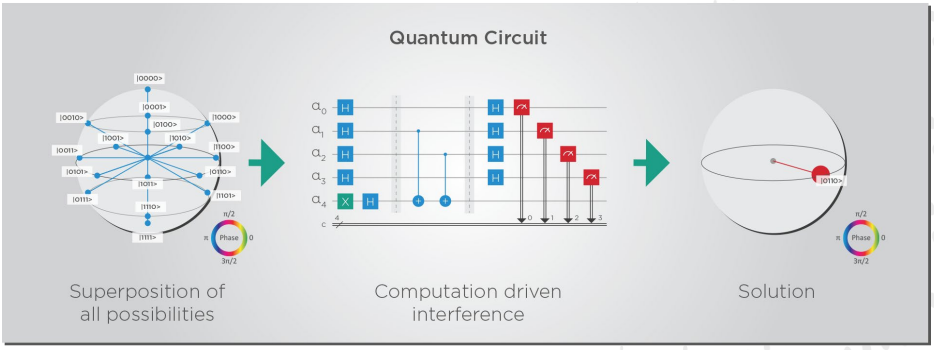

Figure 2: Quantum computation as an interference process. The quantum circuit processes all the potential possibilities, cancelling out the wrong solution and reinforcing the correct solution. [Source: Qiskit]

Quantum computers solve computational problems by harnessing such interference. The quantum algorithm choreographs a pattern of interference where the combinations leading to a wrong answer cancel each other out. In contrast, the combinations leading to the correct answer reinforce each other. This process gives the computer a massive speed boost. We only know how to create such interference patterns for particular computational problems, so for most problems, a quantum computer will only be as fast as a conventional computer. However, one problem where quantum computers are much faster than classical ones is finding the prime factors of very large numbers.

How quantum computers threaten conventional cryptography

Today's digital society depends heavily on securely transmitting and storing data. One of the oldest and most widely used methods to encrypt data is called RSA (Rivest-Shamir-Adleman – the surnames of the algorithm's designers). RSA protocols encrypt messages with a key that results from the multiplication of two very large numbers. Only someone who knows the values of these two numbers can decode the message.

RSA security relies on a mathematical principle: multiplying two large numbers is computationally easy, but the opposite process—figuring out what large numbers were multiplied—is extremely hard, if not practically impossible, for a conventional computer. However, in 1994 mathematician Peter Shor proved that an ideal quantum computer could find the prime factors of large numbers exponentially more quickly than a conventional computer and thus break RSA encryption within hours or days.

While practical quantum computers are likely decades away from implementing Shor's algorithm with enough performance and scale to break RSA or similar encryption methods, the potential implications are terrifying for our digital society and our data safety.

In combination with private key systems like AES, RSA encrypts most of the traffic on the Internet. Breaking RSA means that emails, online purchases, medical records, company data, and military information, among many others, would all be more susceptible to attacks from malicious third parties. Quantum computers could also crack the digital signatures that ensure the integrity of updates to apps, browsers, operating systems, and other software, opening a path for malware.

This security threat has led to heavy investments in new *quantum-resistant* encryption. Besides, existing private key systems used in the enterprise telecom sector like AES-256 are already quantum resistant. However, even if these methods are secure now, there is no guarantee that they will remain secure in the future. Someone might discover a way to crack them, just as it happened with RSA.

Quantum Key Distribution and its impact on the telecom world

Given these risks, arguably the most secure way to protect data and communications is by **fighting quantum with quantum:** protect your data from quantum computer hacking by using security protocols that harness the power of quantum physics laws. That's what *quantum key distribution (QKD)* does: QKD uses qubits to generate a secret cryptographic key protected by the phenomenon of *quantum state collapse*. If an attacker tries to eavesdrop and learn information about the key, they will distort the qubits irreversibly. The sender and receiver will see this distortion as errors in their qubit measurements and know that their key has been compromised.

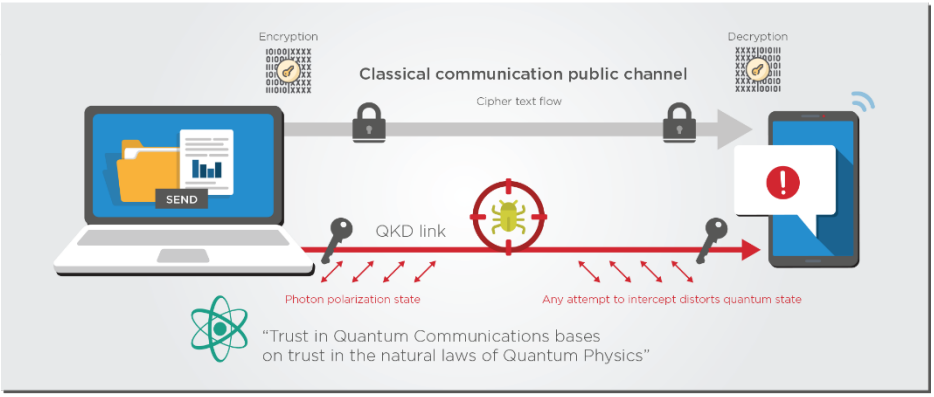

Figure 3: Example of a communications link encrypted via QKD. [Source: TU Eindhoven]

Quantum-safe encryption will take part in people's day-to-day lives through upgrades to laptops, phones, browsers, and other consumer products. However, most of the burden for quantum-safe communication will be handled by businesses, governments, and cloud service providers that must design and install these systems. It's a hugely complex change that's on par with upgrading internet communications from IPv4 to IPv6.

Even if practical quantum computers are not yet available, it's essential to begin investing in these changes, as explained by Toshiba Chief Digital Officer Taro Shimada: *"Sectors such as finance, health and government are now realizing the need to invest in technology that will prepare and protect them for the quantum economy of the future. Our business plan goes far deeper and wider than selling quantum cryptographic hardware. We are developing a quantum platform and services that will not only deliver quantum keys and a quantum network but ultimately enable the birth of a quantum internet".* Toshiba expects the QKD market to grow to approximately $20 billion worldwide in FY 2035.

How Photonics Impacts QKD

Qubits can be photons, electrons, atoms, or any other system that can exist in a quantum state. However, using photons as qubits will likely dominate the quantum communications and QKD application space. We have decades of experience manipulating the properties of photons, such as polarization and phase, to encode qubits. Thanks to optical fiber, we also know how to send photons over long distances with relatively little loss. Besides, optical fiber is already a fundamental component of modern telecommunication networks, so future quantum networks can run on that existing fiber infrastructure. All these signs point towards a new era of *quantum photonics*.

Photonic QKD devices have been, in some shape or form, commercially available for over 15 years. Still, factors such as the high cost, large size, and the inability to operate over longer distances have slowed their widespread adoption. Many R&D efforts regarding quantum photonics aim to address the size, weight, and power (SWaP) limitations. One way to overcome these limitations and reduce the cost per device would be to integrate every QKD function—generating, manipulating, and detecting photonic qubits—into a single chip. The further development of the integrated quantum photonics (IQP) chip is considered by many as a critical step in building the platform that will unlock quantum applications in much the same way as integrated circuits transformed microelectronics.

In the coming articles, we will discuss more how to combine photonic integration with quantum technologies to address the challenges in quantum communications.