Aliro™

Quantum Keys in Action: Using BBM92 for Secure Communication Today

Aliro

www.alirotech.com

Quantum Keys in Action:
Using BBM92 for Secure Communication Today

Summary

Entanglement-based networking is a powerful technology. It can be used for many applications, but for this report the focus is on secure communication. In this white paper we explain the urgent need for Quantum Secure Communication, how BBM92 works, and the practical considerations organizations have about integrating entanglement-based quantum networks into their security posture.

The Vulnerability Problem

Imagine that all the messages containing sensitive data we're sending today can be intercepted and stored, then decrypted by an adversary or bad actor. This is no longer science fiction. Encrypted information and the keys protecting encrypted information may be subject to a whole new level of Harvest Now Decrypt Later attacks (HNDL), where the data is captured today and decrypted via quantum computation when the resources are available. Because the modern world relies heavily on the Internet for everyday activities and basic necessities, virtually everyone is impacted by this vulnerability. Financial information, medical records, and passwords all rely on encryption to stay private and secure. On a broader scale, our communities, our economy, all of our essential services and national security would be endangered without secure communications.

How can we continue to securely send sensitive information, given that no mathematical algorithm can guarantee long term security and secrecy?
The answer is critically important for protecting sensitive information, whether that's held by individuals, by companies, or even government organizations. Entanglement-based quantum networking has emerged as a way to protect the most targeted communications links, where sensitive data traverses the network at the highest volume. These networks solve the problem of HNDL attacks with protocols such as BBM92 and E91. The security of these protocols is not based on computational assumptions, and instead relies on the laws of quantum physics. These physical laws ensure that any attempt to intercept a key can be detected, because this kind of tampering inevitably leaves a trace. Entanglement-based quantum networks are able to protect sensitive communications so completely that no amount of future computing power can compromise its security.

How does it work?

Raw Key Generation: Entangled photon pairs are measured in randomly chosen bases by each party. The resulting outcomes form correlated raw key strings due to quantum entanglement.

Key Sifting: Remove uncorrelated bits from the raw key strings.

Eavesdropper Detection: Use the quantum bit error rate to identify the presence of eavesdropping.

Information Reconciliation: Fix errors in the sifted key. Also referred to as error correction

Privacy Amplification: Decouple the secret key from leaked information.

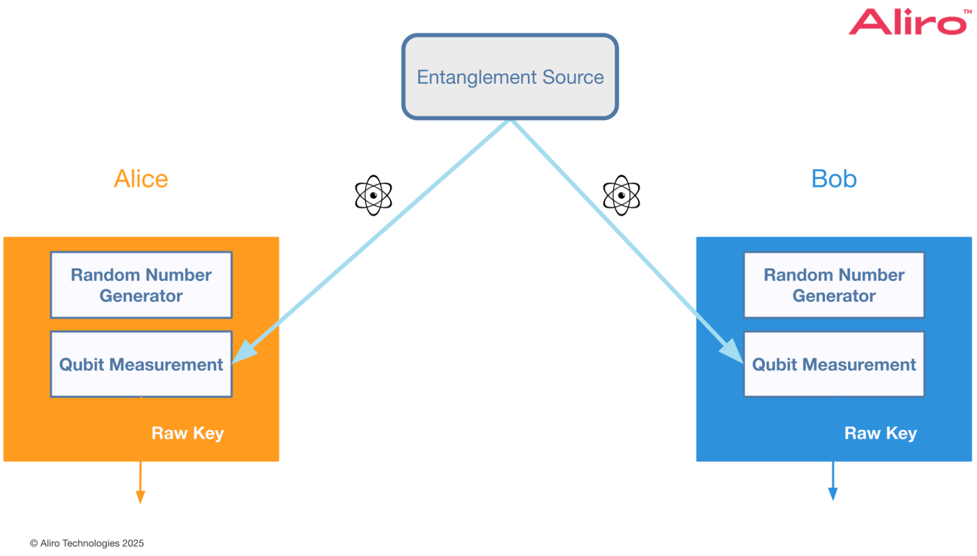
At a very high level, the process begins with creating entangled photon pairs, which are packets of light with a special correlation relationship. Those entangled photons are sent down optical fiber, one to each communication partner. When the photons arrive, at each end node, they are randomly measured in one of two different ways. After measurement, the communicating parties send each other messages about how they measured their photons: not what the results were, but the way in which the photons were measured. The measurements that don't happen to be done in the same way are thrown out, leaving only the photons that were measured the same way. The remaining measurements are then processed to make symmetric keys. Because of the special correlation relationship of entanglement, when entangled photons are measured in the same way, they'll give the same result no matter the distance between them. This measurement result is a truly random bit– not pseudo randomness from a complex equation, but true randomness from quantum physics. From this process a long, strong secret that only these two communicating partners know is created, and no adversary can calculate what that secret code is.

The details of how BBM92 works

Let’s take a closer look at how the BBM92 protocol works using the standard example of Alice and Bob as communicating parties at two different end nodes.

Step 1: Entanglement Distribution.

A source node generates a pair of maximally entangled photons. It sends one photon to one end node, Alice, and the other photon to the other node, Bob.



In quantum mechanics, degrees of freedom are the different ways in which a quantum particle like a photon can store or exhibit information. For photons, the most common degrees of freedom that can be used for encoding qubits (quantum bits) include:

- Polarization. Orientation of the photon's electric field.
- Frequency. The photon's color or energy.
- Time-bin. The time of arrival of the photon.

Each of these degrees can be used to create qubits, and photons can be entangled in any one (or more) of these dimensions.

For this example, consider that the two photons are maximally entangled in their polarization state. This means their qubit states are correlated such that when Alice and Bob measure each photon's polarization in the same basis, the outcomes are either always identical (perfect correlation) or always opposite (perfect anti-correlation), depending on the specific entangled state and the chosen basis—making it possible for them to know each other's measurement results with certainty and use those results to derive identical keys known only to the two of them.

Alice and Bob each receive an individual photon from an entangled pair, and now independently and randomly select basis for measurement. They pick from two difference bases:
- The Z basis, sometimes called the rectilinear basis, which will result in vertical or horizontal polarizations as outcomes.
- The X basis, which will result in diagonal or anti-diagonal polarizations as outcomes.

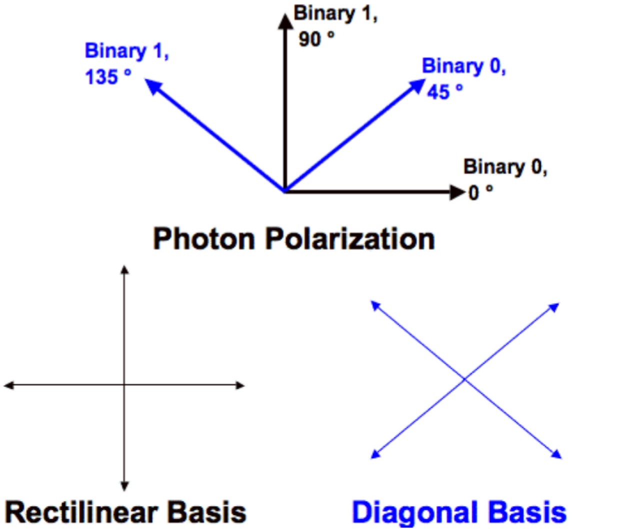


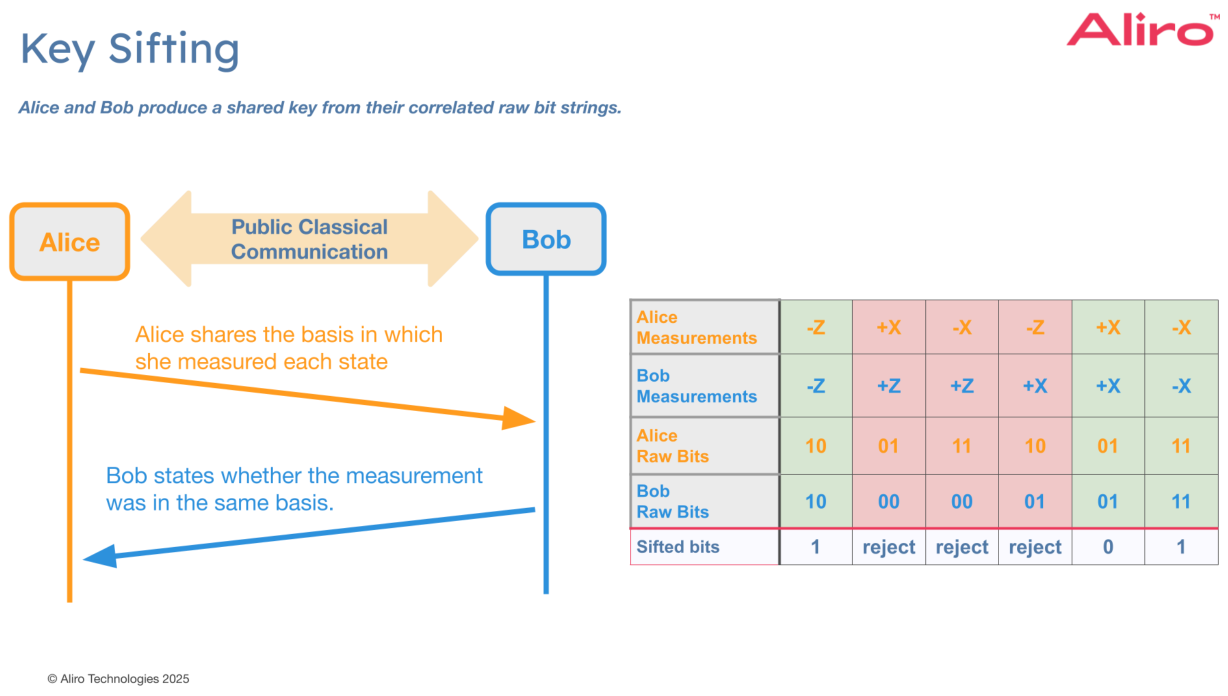
Image from Mart Haitjema https://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/

- If Alice and Bob measure in the same basis, then their measurement results are perfectly correlated.
- If Alice and Bob measure in different bases, then their measurement values are uncorrelated.

When Alice and Bob randomly choose the same basis, these measurement results will be perfectly correlated/anti-correlated, a direct consequence of the entanglement that they share. However, if they choose different bases, the outcomes will be random and uncorrelated.

Step 2: Key Sifting

The next step is called key sifting. To ensure that they only use correlated measurements to create a shared key, Alice and Bob communicate their measurement basis over a public channel. For this example, the measurement basis, Z or X, is said to be the public bit that is shared among the two end nodes. The measurement result, which is either horizontal, vertical, diagonal, or anti-diagonal, is said to be a private bit. The public bit is used in key sifting, and the private bit will contribute to the shared secret key.
When their bases match, Alice and Bob store the corresponding measurement result. When their bases don't match, the measurement result is discarded.



Key Sifting

Alice and Bob produce a shared key from their correlated raw bit strings.

Alice

Public Classical Communication

Bob

Alice shares the basis in which she measured each state

Bob states whether the measurement was in the same basis.

Alice Measurements	-Z	+X	-X	-Z	+X	-X
Bob Measurements	-Z	+Z	+Z	+X	+X	-X
Alice Raw Bits	10	01	11	10	01	11
Bob Raw Bits	10	00	00	01	01	11
Sifted bits	1	reject	reject	reject	0	1

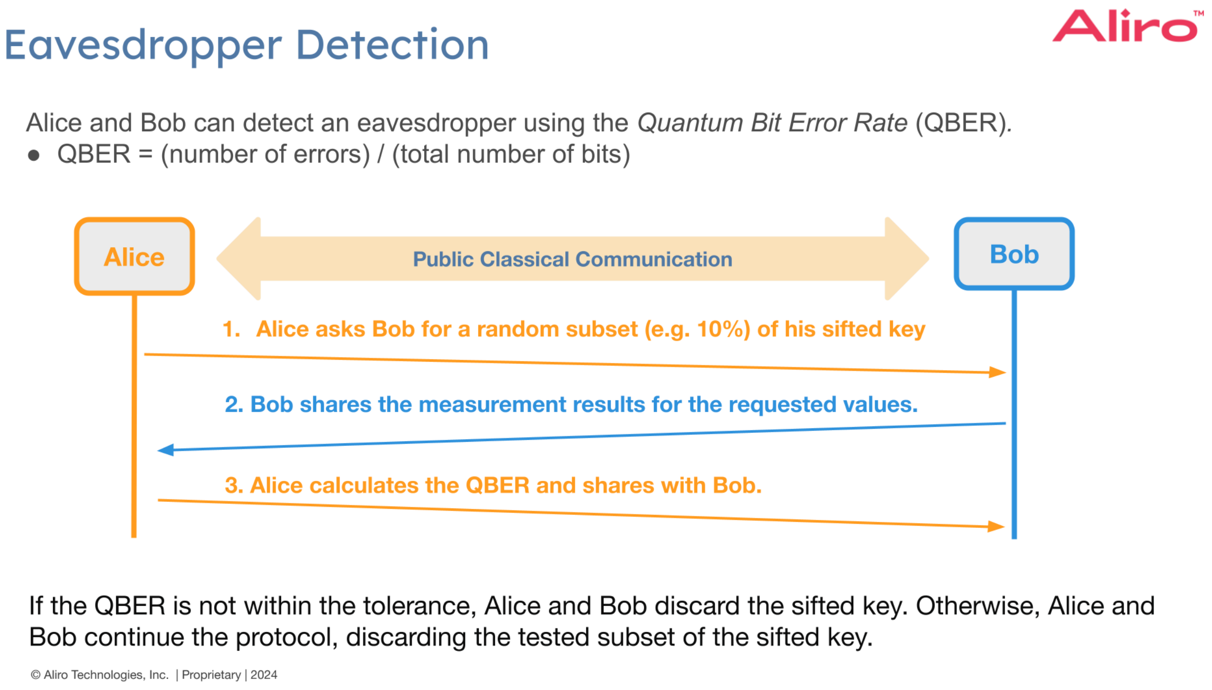
This process raises an important question: how do we prove that the system does all of this in a secure manner without compromising any cryptographic integrity? First, the classical channel used by Alice and Bob to exchange this information must be authenticated. If not authenticated, an adversary could perform a man-in-the-middle attack and manipulate the messages between Alice and Bob. The resulting key would be compromised and no longer secret in that case. Beyond this protection, Alice and Bob can use eavesdropper detection.

Step 3: Eavesdropper Detection

In classical communication, the data transmitted can be copied perfectly, bit by bit. In quantum mechanics, the No Cloning Theorem states that it is physically impossible to make an exact copy of an unknown quantum state. If an eavesdropper tries to intercept the qubits and tries to copy the qubit, they cannot copy them without disturbing them. That disturbance is detectable almost immediately by the legitimate users, Alice and Bob, through the Quantum Bit Error Rate, or QBER.

In the case of an attacker tampering with the quantum states in order to discover the secret key, the resulting interference with those entangled photons results in disturbances that show up in the measurements obtained by Alice and Bob. If the eavesdropper is injecting new photons or manipulating them in some way, the legitimate parties now discover this tampering because, even when measuring in the same basis, they will get differing measurement results that are caused by disturbances in the quantum state - also known as noise. The percentage of these errors is called the quantum bit error rate, or QBER, and above a certain threshold the QBER indicates high potential for an eavesdropper to be present. There might be some inherent noise that also impacts the level of QBER, such as physical imperfections, electrostatic fields, or temperature variations that disturb the quantum state as it's propagating to the devices, and it’s expected that a certain level of QBER will always be present. QBER rates above this expected level could be attributed to an eavesdropper. Essentially, if Alice and Bob have some sort of expectation on what the level of noise (QBER) normally is on the network, they can detect when higher levels of noise are introduced due to a potential adversary.

How does this work, practically speaking?
Once Alice and Bob have collected the measurements of their entangled photon pairs, the way they identify the QBER on their secret measurements is by performing something called parameter estimation.



Eavesdropper Detection

Aliro™

Alice and Bob can detect an eavesdropper using the *Quantum Bit Error Rate* (QBER).

- QBER = (number of errors) / (total number of bits)

Alice

Public Classical Communication

Bob

1. Alice asks Bob for a random subset (e.g. 10%) of his sifted key

2. Bob shares the measurement results for the requested values.

3. Alice calculates the QBER and shares with Bob.

If the QBER is not within the tolerance, Alice and Bob discard the sifted key. Otherwise, Alice and Bob continue the protocol, discarding the tested subset of the sifted key.

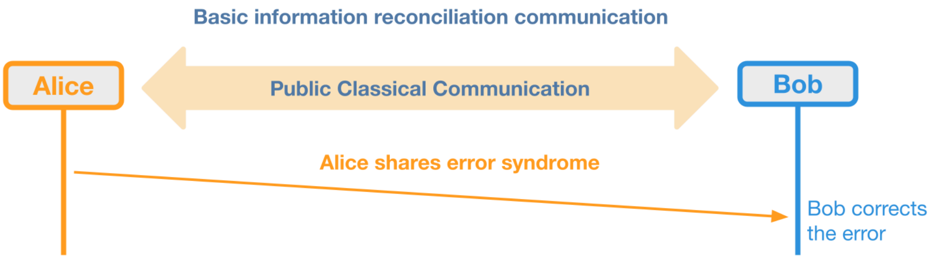
Alice will first determine some subset of her secret key bits that she wants to use for parameter estimation. Alice then requests Bob's measurement results over these specific bits in this specific sequence. Bob will then respond with the actual measurement outcomes. Alice can now compare the measurements from Bob against her own measurements and obtain an estimate of the expected QBER between the remainder of their secret key bits. Alice shares this QBER with Bob. If the QBER is too high, it's beyond the threshold of expected noise – either because of an eavesdropper or due to errors in the physical system, they discard the secret key bits and start the process again.

Step 4: Information Reconciliation

If the QBER is within acceptable limits, it indicates that no significant eavesdropping has occurred and that any disturbance present is small enough to allow secure key extraction. Alice and Bob now proceed to post-processing those measurements to extract secret keys.

As mentioned previously, there is noise that could be inherent in the quantum system. At this point, Alice and Bob's secret key bits might not actually be the same. In order to create symmetric keys that can be used for symmetric key cryptography, Alice and Bob need to ensure these key bits are actually the same. After parameter estimation provides an acceptable QBER, the next step is information reconciliation, where any errors that exist between Alice and Bob's secret key bits are fixed and minimizing any information that could leak about those secret key bits.

Information reconciliation **fixes the errors between Alice and Bob's sifted keys while trying to minimize the amount of leaked information.**


Basic information reconciliation communication
Alice
Public Classical Communication
Bob
Alice shares error syndrome
Bob corrects the error

In classical networking, error correction is used to ensure both parties share the same information, even if some bits get corrupted during transmission. Here's how it typically works: Alice takes a message and runs it through an error correction code, which produces additional "redundancy bits." She sends both her message and these redundancy bits to Bob over a classical channel. Bob then uses the redundancy bits to detect and fix any errors in the message bits he receives.

Usage of error correction in quantum communication works differently: Alice runs her secret key bits through an error correction code but sends Bob only the redundancy bits. This is what we call the error syndrome. Bob then uses his own version of the key bits, along with the error syndrome from Alice, to run the error correction code on his end. Bob now has corrected key bits that match Alice's original key bits exactly.

One challenge with information reconciliation is that sharing the error syndrome can still leak some information to an eavesdropper: only a limited number of key combinations could result in that specific error syndrome, and by intercepting the error syndrome the eavesdropper can narrow the search of possible secret keys.
The final step of BBM92, privacy amplification, addresses this potential leakage.

Step 5: Privacy Amplification

Privacy amplification takes the reconciled key and applies a transformation that reduces any partial information the eavesdropper might have gained, ensuring the final key is truly secret. In the BBM92 protocol, privacy amplification guarantees that the final shared key is secure, even if some information was unintentionally leaked earlier in the process.

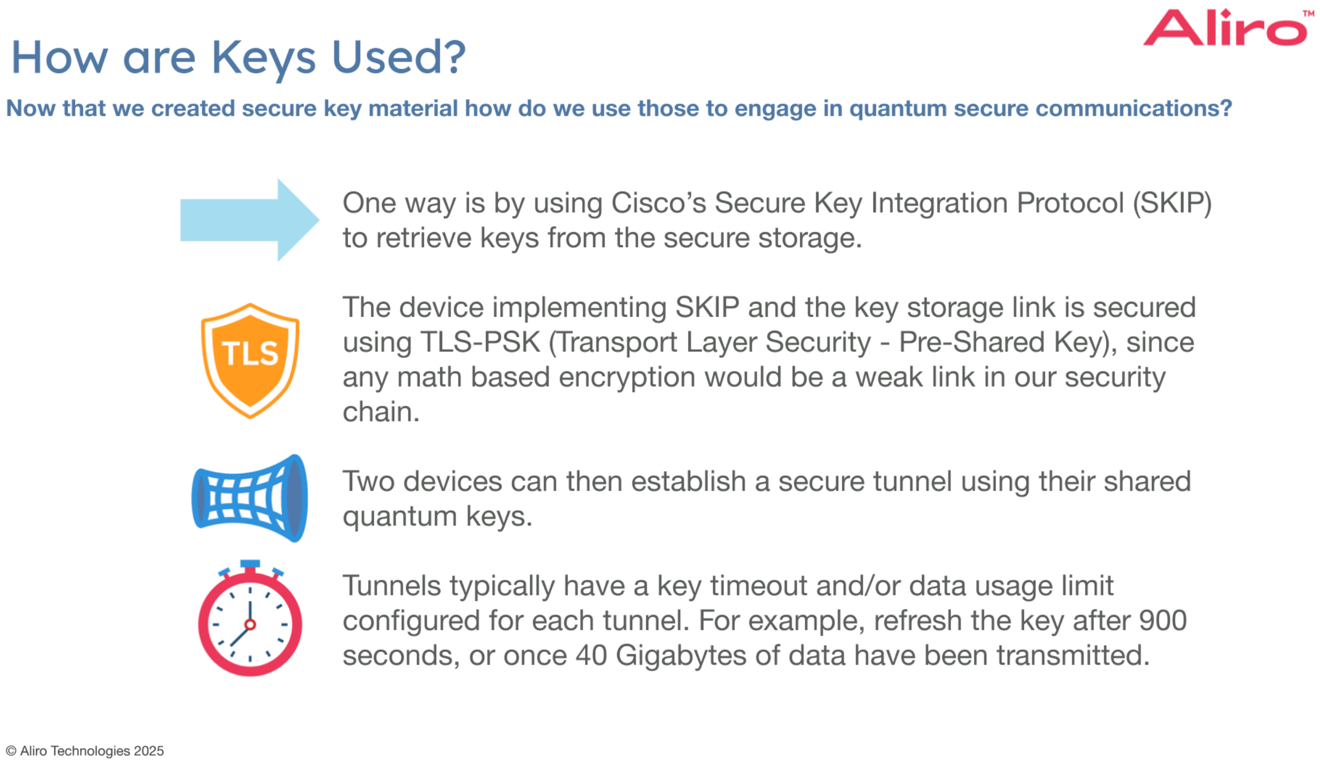
Alice and Bob extract a stronger set of secret key bits, decoupled from any of this leaked information that might have been collected by an eavesdropper. Typically this is done by using a randomness extractor, which takes those secret key bits and some additional seed (a short, random string that acts as an input to the randomness extractor) and outputs a set of stronger secret key bits. In the BBM92 protocol, this is implemented by Alice and Bob agreeing on the extractor in advance. Alice will determine the seed to use for the extractor, and share this with Bob over the classical communication channel. Then, in private, they'll run their secret key bits with that seed through the extractor. This results in a strongly secure secret key that was originally derived from the entangled photons.

What does this look like for end users?

For the end user of symmetric key encryption now sending and receiving encrypted information through the BBM92 protocol, everything would look exactly the same as it does now. The entanglement-based key generation that described here would work behind the scenes, providing keys to routers so that they can encrypt messages for all kinds of apps, just like they do now, but more securely. Network operators, on the other hand, would see some changes: they would use orchestration, control and management software to provision services of entanglement-based key generation, monitor their performance, and resolve any issues that arise. For a demonstration of what this looks like in practice, please see the webinar at timestamp 18:17, Quantum Networks in Action: How BBM92 is Delivering Future-Proof Security. https://www.brighttalk.com/webcast/19861/644059

Once generated, how are these keys used?

There are several ways to use the keys generated by the BBM92 protocol.
One approach is through the Cisco Secure Key Integration Protocol (SKIP). SKIP allows applications to retrieve quantum-generated keys and use them to establish secure communication.



How are Keys Used?

Now that we created secure key material how do we use those to engage in quantum secure communications?

One way is by using Cisco's Secure Key Integration Protocol (SKIP) to retrieve keys from the secure storage.

The device implementing SKIP and the key storage link is secured using TLS-PSK (Transport Layer Security - Pre-Shared Key), since any math based encryption would be a weak link in our security chain.

Two devices can then establish a secure tunnel using their shared quantum keys.

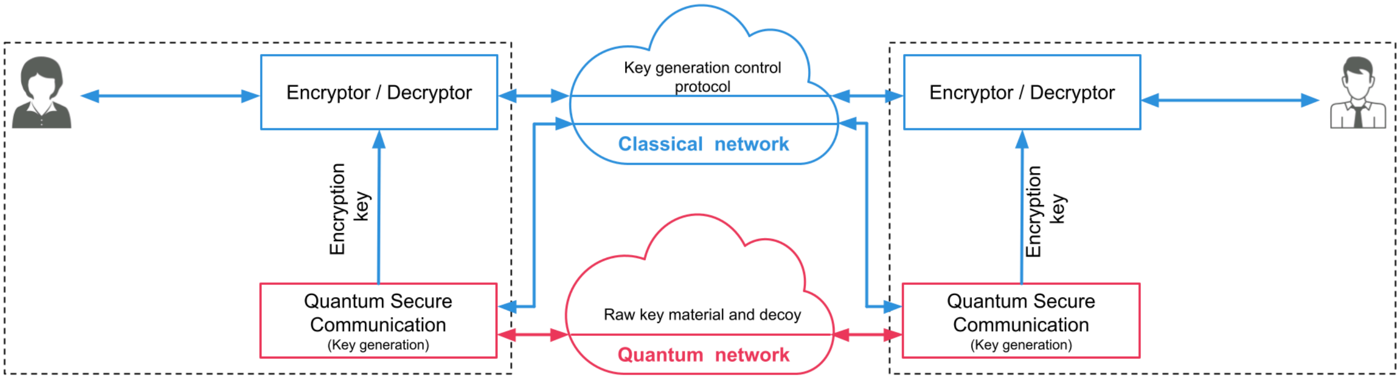
Tunnels typically have a key timeout and/or data usage limit configured for each tunnel. For example, refresh the key after 900 seconds, or once 40 Gigabytes of data have been transmitted.

Another approach follows the ETSI QKD 014 standard. Instead of using traditional TLS with pre-shared keys, it sets up multiple TLS connections in parallel. The basic concept remains the same: use quantum-generated keys to secure the communication channel. These keys can be used to set up secure tunnels, whether using MACsec, IPsec, or some other protocol. Once the tunnel is established, any type of data could be transmitted securely over it. Because generating quantum keys is resource-intensive, it's not practical to use a unique key for every bit of data. Instead, keys are periodically refreshed, ensuring ongoing security while maintaining efficiency.

How does quantum key generation get translated into usable outputs for classical systems?

After secure keys have been generated, some additional management of these keys between Alice and Bob can be done so the keys can be provided as needed. In principle, those secret key bits are just classical bits that can be directly used for any kind of symmetric key cryptography application. They might be pre-segmented into fixed-length keys. A stream of these secret key bits could be supplied to a higher layer application. For the purposes of something like the SKIP protocol, there's a discussion for agreeing on a key identifier, for selecting the key to be used: assigning key IDs to the fixed length keys so that an upper layer protocol like SKIP actually has that metadata for its coordination purposes and agreeing on the exact key that it's going to use.

How does the quantum layer handle traffic, and how does it integrate into the classical network?



There are a couple different ways to look at the quantum layer with regard to traffic. In one way, the quantum layer doesn't handle traffic in the way classical networks do, because the quantum layer is not sending messages. The quantum layer is establishing these entangled links and using them to generate ultra-secure keys. Those keys get passed up to a router via a key import protocol, where they are used to encrypt and decrypt classical messages. However, to achieve the highest level of security, those keys need to be used with a one time pad encryption technique: a system where the keys are never reused, so encrypting each bit of the message requires a new key bit. In this case, traffic management becomes incredibly important because you need to ensure that the quantum network is allocating resources very strategically to generate keys in proportion to the classical traffic. Even in more efficient methods such as rolling over the keys in the routers at regular time intervals, traffic optimization techniques are still needed to ensure the system is going to meet the demands imposed by the router's key consumption rates and prioritize appropriately so the network isn't overtaxed. In either case, either in the high-security setting or the high-efficiency setting, an orchestrator that is aware of the key consumption patterns of all the communicating endpoint node pairs is necessary to ensure resources are maintained in an appropriate way.

What's the first step in deploying BBM92?

A smart first step in building a BBM92 network is to use a quantum network simulator to model the network. This gives organizations the ability to design, validate, and optimize the network architecture before physical deployment. The BBM92 protocol, which relies on entangled photon pairs for secure quantum key distribution (QKD), requires precise configuration of quantum hardware, synchronization of entangled photon sources, and robust error handling mechanisms.

Quantum network simulation helps to de-risk your BBM92 deployment in a few ways:

- It aids in identifying the most efficient and effective hardware configurations, entanglement distribution strategies, and protocol parameters to align with the requirements of the BBM92 protocol before any costly hardware purchases need to be made.
- Simulation can determine the real-world practicality of establishing high-fidelity entanglement across desired distances with the accurate modeling of loss, noise, and error rates. While mathematical models exist for some of these parameters, many become intractable when the network grows beyond a few nodes.
- Simulation tools are a digital sandbox for exploring different topologies, routing algorithms, and quantum repeater placements to ensure network scalability.

Using simulation as a first step, organizations can mitigate the costs of trial-and-error physical setups and build internal fluency with quantum networking and how it integrates with classical networking.

How do simulations inform or validate real world deployments of entanglement-based protocols?

Quantum networks can integrate with existing classical networks, and quantum keys can be passed up to the same encryptors that are already in use today. However, at a physical level, the way that happens is very different from what's happening in a classical setting. Because of that, there's more that needs to be looked at when designing a quantum network. In classical networking, for example, under one type of encoding, many photons are sent along a fiber to represent a bit value of 1, and (still many) but fewer photons are sent represent a bit value of 0. Think of the optical fiber as a hose, and that hose is spraying a stream of water. Think of ones as being the pressure washer setting and the soaker hose setting as being zero.

Whereas in quantum networking, depending on the encoding being used, the entangled bits that are sent to Alice and Bob are a single photon: a single particle of light that is tiny and delicate, and there's only one. In the analogy, this photon is like a delicate little marble rolling down the hose. Sending and receiving a single photon is very different from sending classical bits. Single photons may be buried in noise by other photons, they may be lost along the way for other reasons, the information in the photon might shift along the way so that its state is different when it arrives than it was when it was sent. There are a lot of details that can be simulated to determine, given a specific set of equipment, if it is possible to achieve the necessary level performance needed for BBM92, over a certain distance and under certain conditions. Details that simulators are able to incorporate into this kind of analysis are things like noise and imperfections introduced based on:

- Whether the optical fibers are buried deep underground or strung up in the air
- How the optical fiber is shielded
- How close optical fibers are to each other
- The kinds of signals being carried on those adjacent optical fibers: is it a quantum networking channel or is it a super-high-bandwidth channel carrying classical communications?
- Temperature changes and other environmental factors

There are many details to track, and by simulating those carefully, it's possible to de-risk deployments: before the hardware is purchased and the network is built, there's already an understanding of how it's going to function. Simulation also allows organizations to use an iterative process and test different scenarios. Simulation can also aid in debugging unexpected issues with the physical network after it's built, making it a powerful tool for achieving high performance quantum networks.

What aspects of BBM92 can be reliably simulated, and what aspects require physical implementations to understand fully?

In the case of BBM92 protocol, all of the core aspects of the protocol can be reliably simulated: entanglement distribution, random basis selection, qubit measurements, calculation of QBER. Simulation tools can also help with modeling non-ideal scenarios such as errors, basis mismatches, eavesdropping strategies (e.g., intercept-resend or entanglement-based attacks).

However, for simulations to be realistic, they need to incorporate parameters derived from actual hardware in real-world environments. For example, accurately modeling dark counts, channel losses, polarization drift in fiber, and other sources of noise often requires empirical data. These variables can change depending on environmental factors such as temperature, vibration, and other operating conditions. Since these values can only be coarsely approximated from component specifications or estimated environmental fluctuations, accurate simulation often requires partial implementation and characterization of components in the network to obtain realistic parameters.

As the quantum network becomes more sophisticated, such as with more nodes, longer distances, or more sophisticated protocols, computational demands increase dramatically. Large entangled systems cause exponential growth in the state space and demand increasingly detailed models, especially when incorporating real-world physical effects such as noise and channel imperfections. Quantum network simulators may eventually benefit from quantum computation, or hybrid quantum-classical computation. Quantum network simulators are invaluable for guiding design choices, identifying potential bottlenecks, and optimizing performance.

While not addressed in this paper, many cybersecurity professionals have important questions about Quantum Secure Communications (QSC). QSC is a powerful solution to the growing real-world vulnerabilities in today's encryption systems. Please see our blog post, Five concerns cybersecurity pros raise about Quantum Secure Communication, https://www.aliroquantum.com/blog/five-concerns-cybersecurity-pros-raise-about-quantum-secure-communication *where we address some of the most common and critical questions we're asked about Quantum Secure Communication, particularly through protocols like BBM92.*

A full-stack solution for Quantum Networking

Entanglement-based secure networks are being built today by a variety of organizations for a variety of use cases, benefiting organizations internally as well as providing great value to an organization's customers. Telecommunications companies, national research labs, intelligence organizations, and systems integrators are just a few examples of the organizations Aliro is helping to leverage quantum networking.

Building entanglement-based quantum networks is no easy task. It requires:

- Emerging hardware components necessary to build the quantum network.
- The software necessary to design, simulate, run, and manage the quantum network.
- A team with expertise in quantum physics and classical networking.
- Years of hard work and development.

This may seem overwhelming, but Aliro is uniquely positioned to help you build your quantum network. The steps you can take to ensure your organization is meeting the challenges and leveraging the benefits of the quantum revolution are part of a clear, unified solution already at work in quantum networks like the EPB Quantum Network℠ in Chattanooga, Tennessee.

AliroNet™, the world's first full-stack entanglement-based quantum network solution, consists of the software and services necessary to ensure customers will fully meet their quantum networking goals. Each component within AliroNet™ is built from the ground up to be compatible and optimal with quantum networks of any scale and architecture. AliroNet™ is used to simulate, design, run, and manage quantum networks as well as test, verify, and optimize quantum hardware for network performance. AliroNet™ leverages the expertise of Aliro personnel in order to ensure that customers get the most value out of the software and their investment.

Depending on where customers are in their quantum networking journeys, AliroNet™ is available in three modes that create a clear path toward building full-scale entanglement-based secure networks: (1) Emulation Mode, for emulating, designing, and validating quantum networks, (2) Pilot Mode for implementing a small-scale quantum network testbed, and (3) Deployment Mode for scaling quantum networks and integrating end-to-end applications. AliroNet™ has been developed by a team of world-class experts in quantum physics and classical networking.

To get started (or continue on your quantum journey), reach out to the Aliro Quantum team for additional information on how AliroNet™ can enable your quantum network.

info@alirotech.com www.alirotech.com