Aliro SECURITY™

Advanced Secure Networks and the Security Landscape

Aliro Security

www.alirosecurity.com

Summary **3**
Introduction **3**
Classical security today **3**
Symmetric encryption 3
Asymmetric encryption 5
Vulnerabilities of today's encryption algorithms **7**
RSA and Shor's Algorithm 7
AES and Grover's Algorithm 10
Post Quantum Cryptography **12**
Lattice-Based Cryptography 12
Information-theoretic Security **14**
The One Time Pad (OTP) 14
Advanced Secure Communication Protocols 15
The Evolving Security Landscape **22**
Integrating Entanglement-based Advanced Secure Networks **24**
References **26**

Summary

This white paper examines how organizations can address the urgent need for robust security measures as we stand on the brink of a new era marked by the advent of quantum computing. The objective of this white paper is to give you the information you need about the evolving security landscape, show how today's security measures are jeopardized by quantum computation, and how a security strategy that includes Advanced Secure Networking ensures resilience in the face of quantum advancements.

Introduction

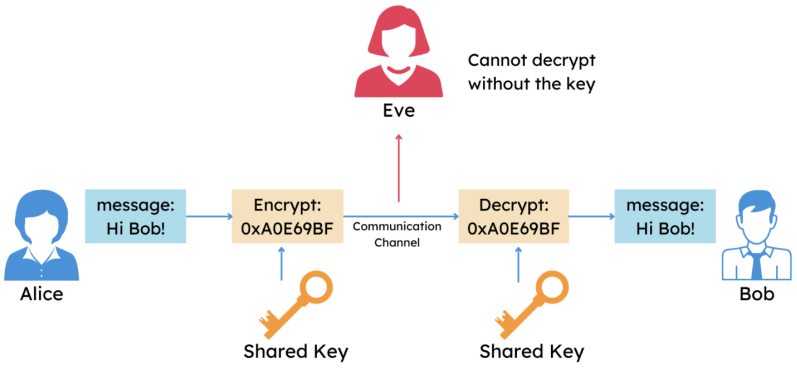
Organizations must continually navigate the protection of digital assets in an ever-evolving threat landscape. Classical encryption algorithms such as symmetric and asymmetric encryption form the cornerstone of cybersecurity, safeguarding everything from individual privacy to global financial transactions. Symmetric encryption relies on a single key for both encryption and decryption, making it fast and efficient for securing large volumes of data. Asymmetric encryption, on the other hand, uses a pair of keys — one public and one private — to facilitate secure data exchange over unsecured channels. While effective against classical computing threats, quantum computation is more powerful. Quantum computers, with their ability to solve complex mathematical problems at unprecedented speeds, will be able to break these cryptographic systems. Development and adoption of quantum-safe methods that can withstand the sophisticated computational capabilities of quantum technology are needed in order to ensure the continued protection of sensitive information.

Classical security today

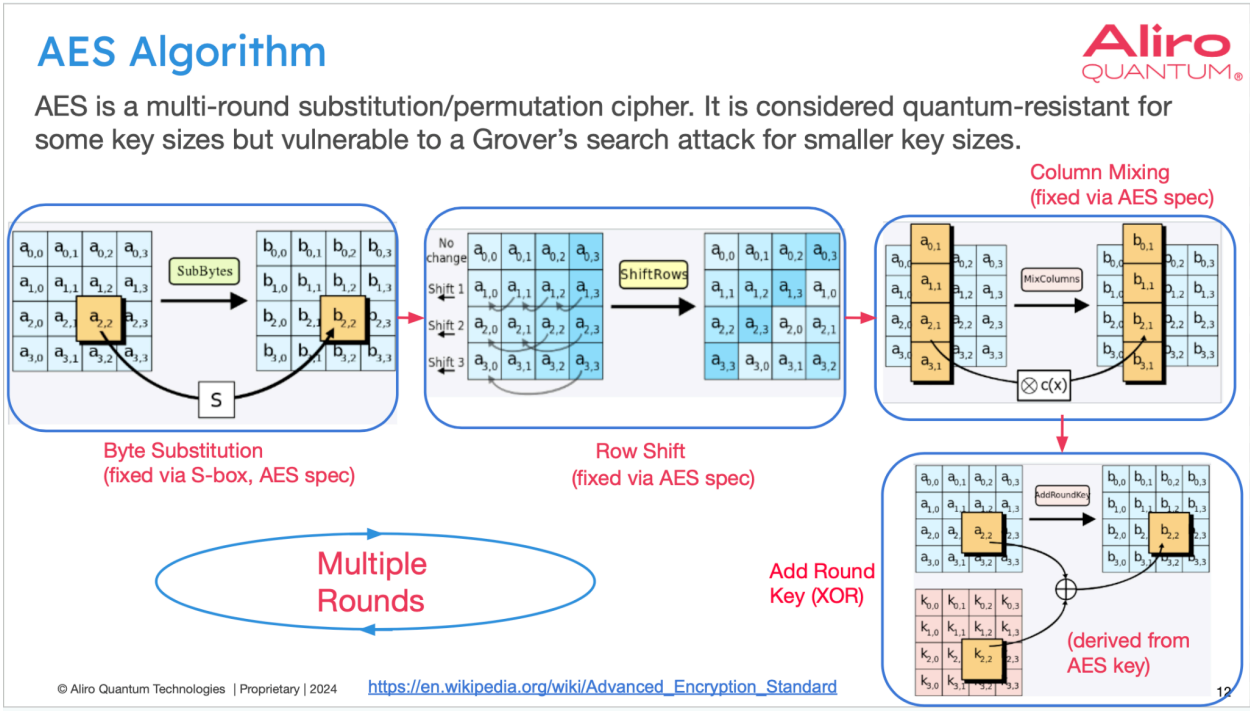
Today's security is underpinned by symmetric and asymmetric encryption algorithms.

Symmetric encryption

In symmetric encryption, a sender will encrypt information with a single pre-shared secret key that the receiver then uses to decrypt the message. This key must be kept secret between sender and receiver, or the information encrypted with the key could be compromised. Symmetric encryption is very efficient: it uses just one key and can encrypt large amounts of data quickly, and the resulting ciphertext is relatively small. Symmetric key schemes include AES, TDEA, and hash-based password systems..



AES (Advanced Encryption Standard) is a symmetric block cipher that encrypts data in fixed-size blocks. It's widely used to secure sensitive data due to its efficiency and strong security characteristics. AES is one of the most popular symmetric encryption algorithm in use today.



Here's how AES encryption works[AES]:

1. Key Generation
    - Key Selection: Start by choosing a key of appropriate length, typically 128, 192, or 256 bits.
    - Key Expansion: Expand the initial key into multiple sets of round keys using the Rijndael key schedule. This involves generating a series of round keys from the initial key. Each round key is used in one of the AES rounds during the encryption and decryption processes. The number of rounds (and thus the number of round keys) depends on the key size: 10 rounds (and keys) for 128 bits, 12 rounds for 192 bits, and 14 rounds for 256 bits.

2. Encryption
    - Initial Setup: Divide the plaintext into blocks of 128 bits each, as AES processes 128 bits (16 bytes) at a time in a 4x4 column-major order matrix called the state.
    - Round Process: Perform the following steps for each block of plaintext. The number of rounds varies based on key size:
        - SubBytes: Apply the Substitution box (S-box) to each byte of the state matrix, replacing the byte with another according to a predefined table, to introduce non-linearity.
        - ShiftRows: Cyclically shift the rows of the state matrix; the first row is not shifted, the second row is shifted left by one byte, the third row by two bytes, and the fourth row by three bytes, facilitating diffusion.
        - MixColumns (omitted in the final round): Combine the bytes in each column of the state matrix using a linear transformation, which mixes the data within each column.
        - AddRoundKey: XOR the state with the round key derived during the key expansion phase.

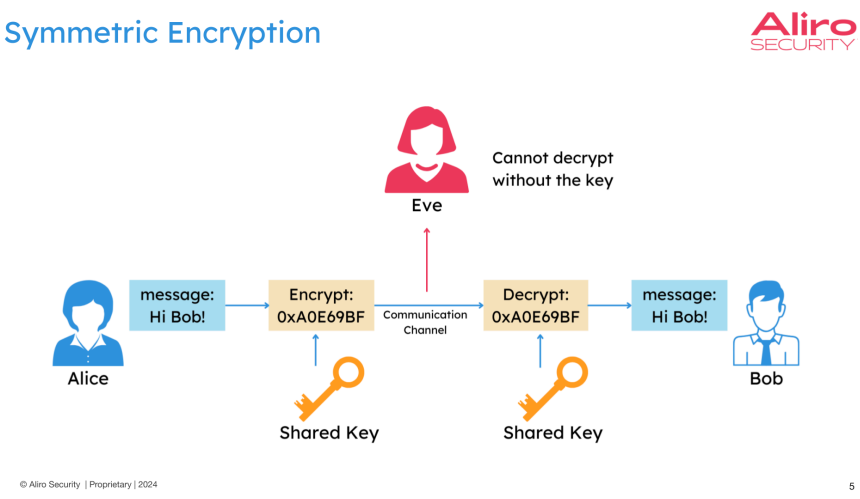
- Final Round: In the last round, perform the SubBytes, ShiftRows, and AddRoundKey steps, but omit the MixColumns step.

3. Decryption
   - Initial Setup: The decryption process uses the same initial key as encryption, with the key expansion process yielding the same set of round keys.
   - Round Process: Perform the inverse of each encryption step in reverse order to decrypt the ciphertext back into plaintext:
   - AddRoundKey: XOR the round key (starting from the last and moving backwards).
   - InvMixColumns (included in all but the final round during decryption): Apply the inverse of the MixColumns transformation.
   - InvShiftRows: Cyclically shift the rows of the state matrix in the opposite direction; the first row remains stationary, the second shifts right by one byte, the third by two, and the fourth by three.
   - InvSubBytes: Apply the inverse Substitution box (InvS-box) to each byte of the state matrix, reversing the substitution step.
   - Final Round of Decryption: In the final decryption round, perform the InvSubBytes, InvShiftRows, and AddRoundKey steps, omitting the InvMixColumns transformation.

The challenge with symmetric encryption algorithms like AES is sharing the key in a secure manner, so that the information it protects won't be compromised. For this reason, symmetric encryption is often used in combination with asymmetric encryption.

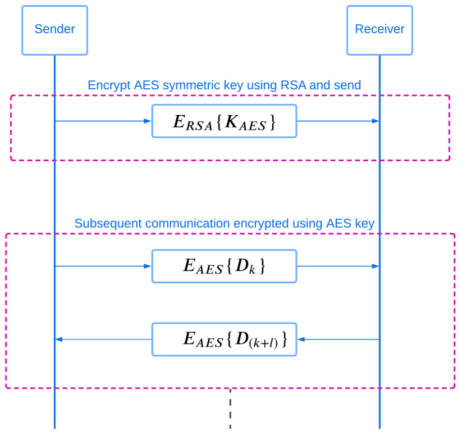
Asymmetric encryption

In asymmetric encryption, two keys are used to encrypt and decrypt information. One key is publicly available, and one key is private and known only to the receiver. In this scheme, the sender encrypts data with the public key of the receiver, and the receiver decrypts the message with the private key. The public keys can be shared with any potential sender, but the private key is owned only by the receiver. This provides a one-way communication of data, and any adversary intercepting the data wouldn't be able to decrypt it without the private key. Asymmetric encryption schemes include RSA, Elliptical Curve Cryptography, and Diffie-Hellman.



Asymmetric encryption, such as RSA, is commonly used along with a symmetric encryption algorithm, such as AES. An AES symmetric key is encrypted using an asymmetric RSA algorithm, and sent to the receiver. Subsequent secret data transmissions are then encrypted using the AES symmetric key.

Key Exchange Using Asymmetric & Symmetric Encryption



Asymmetric encryption (such as RSA) is commonly used along with a symmetric encryption algorithm such as AES:

- A symmetric key is encrypted using RSA and sent to the receiver
- Subsequent data transmissions are encrypted using the symmetric key
- Symmetric encryption is more computationally efficient

© Aliro Security | Proprietary | 2024

The underlying security of RSA is based on the computational hardness of factoring a large composite number into its prime factors.

RSA Algorithm

Encrypt

$$c = m^e mod\ N$$

Decrypt

$$m = c^d mod\ N$$

Public Key (N, e) Private Key (N, d)

(Asymmetric Keys)

https://en.wikipedia.org/wiki/RSA_(cryptosystem)

The RSA algorithm is based on the conjectured difficulty of integer factorization

$$N = pq$$

where N is known and p and q are unknown large prime numbers to determine.

Given the public key it is difficult to derive the corresponding private key.

$$d \cdot e = 1 \mod \phi(N)$$

$$\phi(N) = (p-1)(q-1)$$

Euler totient function

© Aliro Security | Proprietary | 2024

RSA relies on the practical difficulty of factoring the product of two large prime numbers, making it computationally infeasible to derive p and q from N. This ensures that while the public key (N, e) can be widely distributed and used for encrypting messages, the private key (N, d) remains secure and confidential, capable of decrypting the information. Hence, without access to the private key, it is extremely difficult to derive the plaintext from the ciphertext. Here's how RSA works[RSA]:

1. Key Generation:
   - Choose Primes: Select two large prime numbers, p and q.
   - Compute N: Calculate $N=p\times q$. This number N is used as the modulus for both the public and private keys.
   - Euler's Totient Function $\phi\ (N)$: Calculate $\phi(n)=(p-1)\times(q-1)$ which is used in determining the public and private exponents.
   - Choose Public Exponent e: Select an integer e such that $1<e<\phi(n)$ and e is coprime to $\phi(N)$. This e is part of the public key.
   - Determine Private Exponent d: Calculate d as the modular multiplicative inverse of e modulo $\phi(N)$, i.e, $d\times e\equiv 1 \pmod{\phi(N)}$ This d is part of the private key.

2. Encryption:
   - Public Key (N, e): The public key is composed of the modulus N and the public exponent e.
   - Encrypt Message: To encrypt a plaintext message m, interpret the message as a long binary number, then exponentiate that number with the public exponent e, compute mod n, to arrive at the ciphertext c: $c=m^e \bmod n$.

3. Decryption:
   - Private Key (N, d): The private key consists of the modulus N and the private exponent d.
   - Decrypt Message: To decrypt the ciphertext c, use the private key to compute $m=c^d \bmod n$. The result m is the original plaintext.

Vulnerabilities of today's encryption algorithms

Both symmetric and asymmetric algorithms are vulnerable to quantum attacks. Shor's algorithm enables quantum computers to factor large integers and compute discrete logarithms very quickly. Similarly, Grover's algorithm can significantly reduce the time required to brute-force symmetric keys, effectively halving the bit strength of algorithms like AES.

RSA and Shor's Algorithm

RSA encryption is based on the principle that it is easy to multiply large numbers together but difficult to factorize the product back into its original prime factors. The security of RSA depends on the computational difficulty of the integer factorization problem. Any cryptographic algorithm that relies on integer factorization for security is vulnerable to Shor's algorithm.

Shor's Algorithm: introduction

The integer factorization problem can be recast as an order-finding problem. This problem is related to other problems including the discrete logarithm, period-finding problem, and hidden-subgroup problem. **Shor's algorithm solves integer factorization exponentially faster than classical methods.**

$a^r = 1(mod\ N)$ ← Order-finding problem: $a\ is\ coprime\ to\ N,\ find\ r$

$a^r - 1 = 0(mod\ N)$

$(a^{r/2} + 1)(a^{r/2} - 1) = 0(mod\ N)$

$(a^{r/2} + 1)(a^{r/2} - 1) = mN$ Must be true due to mod N congruence

$gcd(a^{r/2} \pm 1, N)$ ← Factors: gcd can be efficiently calculated using Euclid's algorithm

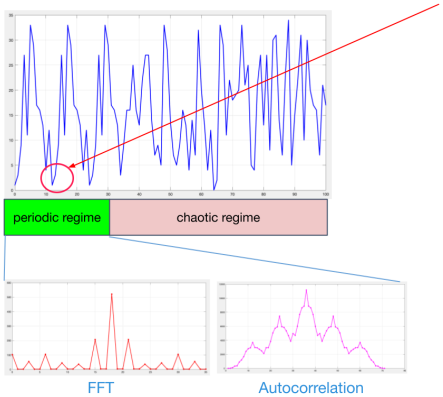
© Aliro Security | Proprietary | 2024

The integer factorization problem, discrete logarithm, period-finding problem, and hidden-subgroup problem are all vulnerable to Shor's algorithm. Shor's algorithm solves these problems exponentially faster than classical methods; any cryptographic system could be rendered insecure by a quantum computer capable of running this algorithm. Here's how Shor's algorithm works:

At the heart of Shor's algorithm lies the order-finding problem, which fundamentally transforms the approach to integer factorization. Traditional factorization involves breaking down a number, *N*, into its prime components, a task that grows exponentially harder as *N* increases. Shor's algorithm cleverly shifts this problem to finding the order of an element relative to *N*, which quantum algorithms can solve very efficiently.

Shor's Algorithm: classical intuition

Let's visualize the (chaotic) sequence $y_k = 3^k\ mod\ 35$ and find where $y_k = 1$



The index k where $y_k = 1$ is the solution! In this case the order is $r = 12$. We can now use Euclid's algorithm to get our greatest common divisors and find the factors:

$p = gcd(3^{\frac{12}{2}} - 1, 35) = 7$

$q = gcd(3^{\frac{12}{2}} + 1, 35) = 5$

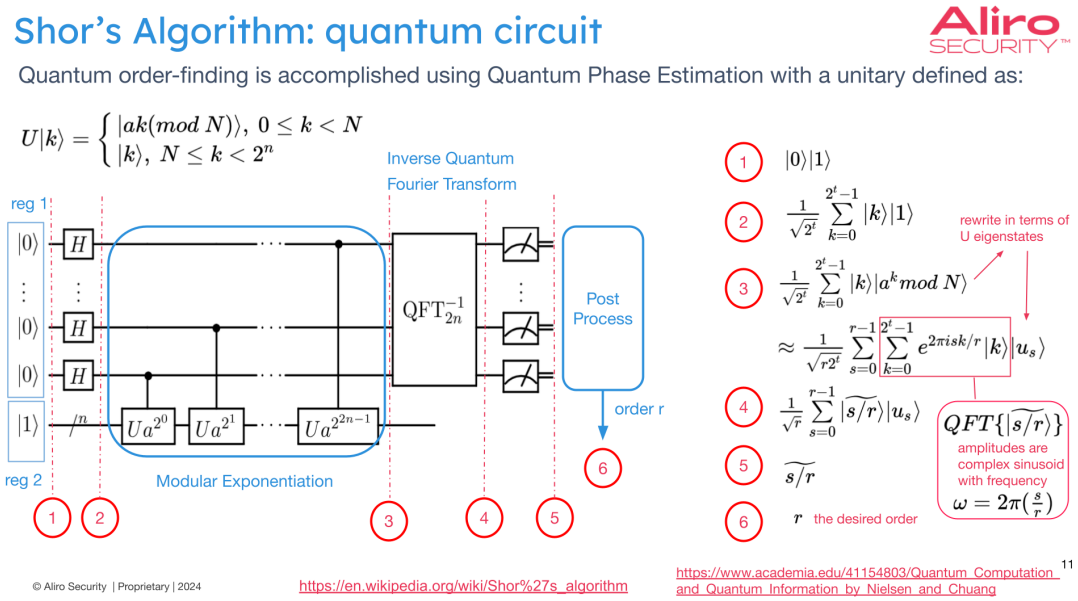
Factors

- Autocorrelation function shows period = 12
- FFT shows period is approximately: 1/(3/35) =12

© Aliro Security | Proprietary | 2024

Shor's algorithm uses properties of modular arithmetic, focusing on finding the period or order of a number. The task is to find the smallest positive integer *r* such that $a^r = 1(mod\ N)$, where *N* is the RSA modulus (product of two primes *p* and *q*), and *a* is a randomly chosen integer less than *N* that

shares no common factors with N. The integer r is referred to as the "order" of a modulo N. The use of quantum Fourier transform to efficiently compute the period r is a key component of Shor's algorithm. This quantum approach provides a significant speed advantage over classical methods, which do not have efficient means to determine r for large N, where N is the RSA modulus (product of two primes p and q). In summary, r is used in a process that exploits properties of modular arithmetic to find conditions under which the factors of N can be directly calculated.



Above is a quantum circuit for executing Shor's algorithm[QUANTUMCIRCUIT]

Shor's Algorithm leverages quantum phase estimation. Quantum phase estimation is used to estimate the phase (or eigenvalue) of an eigenstate of a unitary operator, which is a critical operation in the manipulation and utilization of quantum information. Here is an overview of how this works[SHOR]:

1. Define the Unitary Operator:

- Select a specific unitary operator U such that when it operates on the quantum state $|k\rangle$ by multiplying it by $a^k \ mod\ N$ where a is a chosen integer less than N which is the modulus (the product of two primes).

2. Setting Up the Quantum Circuit:

- The quantum circuit involves two registers:
  - **Index Register**: This is the top register, initialized in a state of superposition. It controls the application of the unitary operations.
  - **Target Register**: This is the lower register where the actual computation of $U^{2^j}|k\rangle$ occurs, representing the modular exponentiation $a^k \ mod\ N$

3. Controlled Unitary Operations:

- The algorithm leverages the index register to control the application of the unitary operations U^{2^j} on the target register. Each qubit in the index register determines the power of *U* applied, effectively encoding the value *k* in superposed states.

4. Quantum Fourier Transform:

- After processing through the unitary operations, an inverse Quantum Fourier Transform is performed on the index register. This transform is crucial as it decodes the phase information encoded in the amplitudes of the quantum states into a format that can be measured and interpreted.

5. Measurement and Phase Estimation:

- The state of the index register is measured, providing an output from which the phase θ can be deduced. This phase relates directly to the eigenvalue $e^{2\pi i\theta}$ of the unitary operator.

6. Interpreting the Output:

- The output from the measurement is used to estimate the order *r* of a modulo *N*. This involves classical post-processing techniques to convert the measured values into an estimate of *r*, which is critical for factorization.

7. Factorization of N:

- With *r* known, Shor's algorithm proceeds to calculate $a^{r/2}\pm 1$ and uses the greatest common divisor (gcd) method to find the factors of *N*, typically the primes *p* and *q* used in RSA encryption.

8. Post-Processing for Factorization:

- Classical computing methods finalize the factorization process by extracting p and q from the greatest common divisor calculations.

AES and Grover's Algorithm

Grover's algorithm is a method used in quantum computing to efficiently find a specific input for a function when only the output is known, which can be applied to cryptographic one-way functions. This is a critical vulnerability because a lot of cryptographic functions are one-way functions: they're easy to compute in one direction and difficult to compute in the other. Grover's algorithm is a quantum search algorithm that significantly impacts symmetric encryption algorithms like AES (Advanced Encryption Standard). Here's a brief explanation of how Grover's algorithm functions and its implications for AES[GROVER]:

1. Key Generation

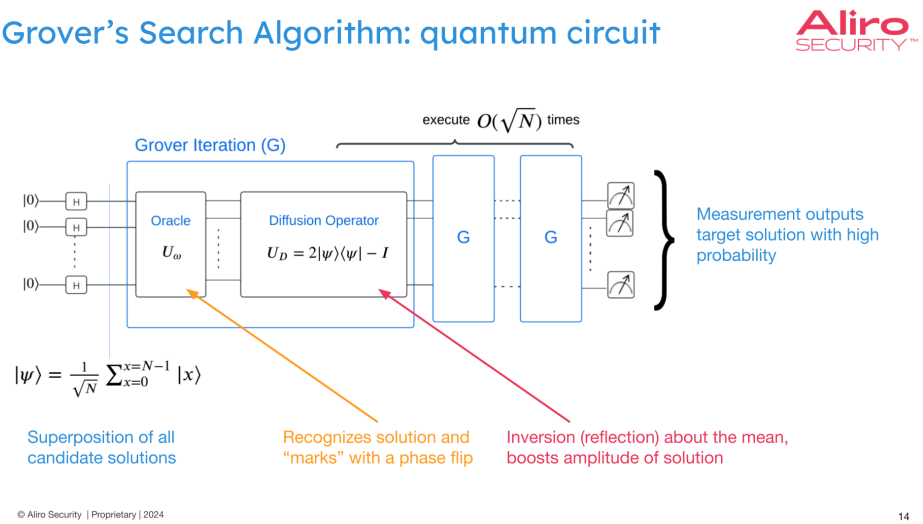
- Quantum Oracle Creation: The first step involves defining a "quantum oracle." This oracle is a quantum circuit that can recognize the correct input (or key) based on output values it generates. It's worth noting that recognizing a solution is much easier than finding a solution. In the context of AES, the oracle would discern if a guessed key is correct by reversing the encryption process.
- Setup of the Quantum System: The system begins with all possible candidate keys in a superposition. This means every possible key is simultaneously considered by the oracle in one quantum computation step.

2. Encryption (Grover's Search Mechanism)

- **Iteration Process:**
  - Oracle Function: Each iteration of Grover's search begins with the oracle function evaluating whether a given key in superposition correctly decrypts the ciphertext to its corresponding plaintext.
  - Amplitude Amplification (Diffusion): After the oracle marks the correct key, the diffusion process amplifies the probability amplitude of the correct key's quantum state. This step is crucial as it incrementally increases the likelihood that a measurement will result in the correct key.
- **Repeat Iterations:**
  - The Grover iteration (oracle evaluation and diffusion) is repeated approximately $\sqrt{N}$ times, where *N* is the number of possible keys. This square root relationship represents a significant speedup compared to classical search algorithms, which require *N* iterations in the worst case.

3. Decryption (Finding the AES Key)

- Measurement: After sufficient iterations, measuring the quantum state of the system will collapse it to a state that corresponds to the correct key with a high probability.



Grover's algorithm greatly reduces the effective security of AES. For example, AES-128, which classically would require 2^{128} operations to break, would need only about 2^{64} quantum operations[GROVER2]. This vulnerability makes AES-128 susceptible to quantum attacks using relatively modest-sized quantum computers.

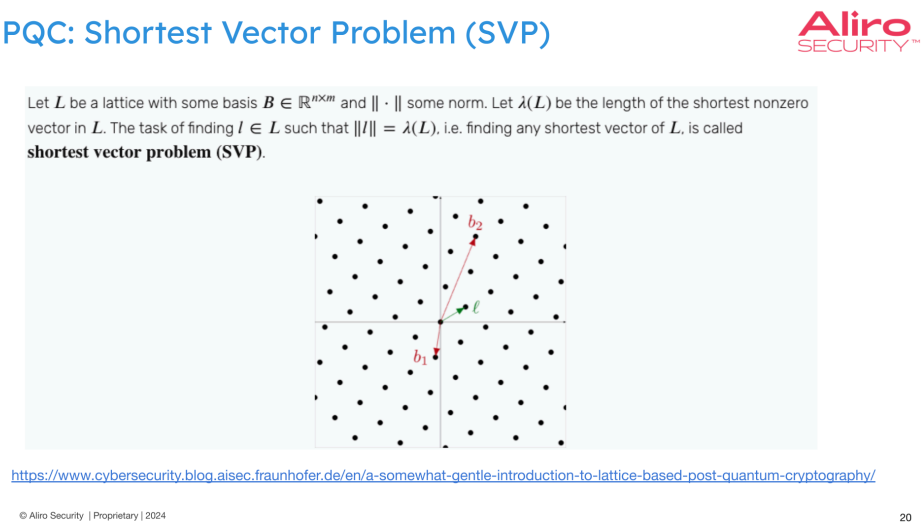
Post Quantum Cryptography

Post Quantum Cryptography (PQC) is an evolving field of classical cryptographic methods designed to secure communication against the potential threat posed by quantum computation. PQC protocols have been developed and continue to evolve in order to withstand attacks from quantum algorithms. While there are many different ways to approach PQC, here the focus is on those approaches that are most robust.

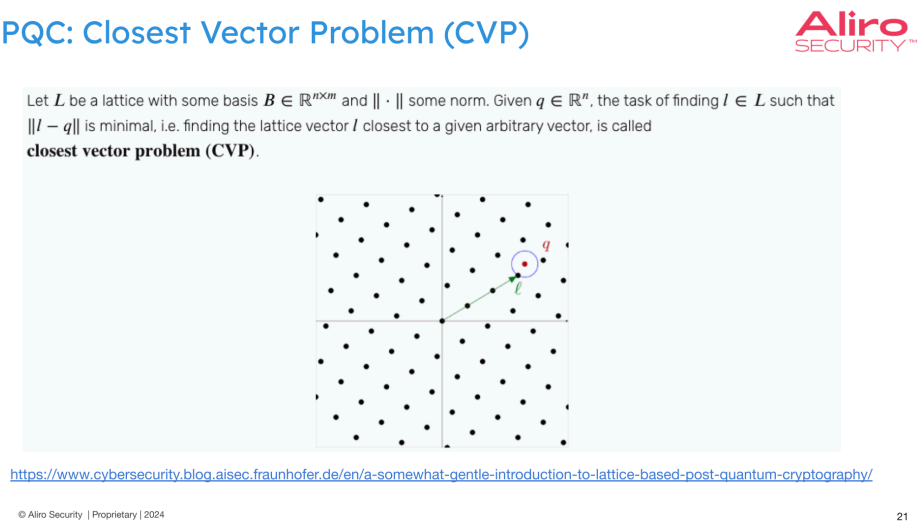
Lattice-Based Cryptography

Lattice-based cryptography is the cornerstone of many PQC methods due to its resistance to known quantum attacks, including those running Shor's algorithm. With lattice-based problems, the public key is derived from the definition of a lattice, while the private key is related to the problem solution. Some underlying mathematical challenges used in lattice-based cryptography include:

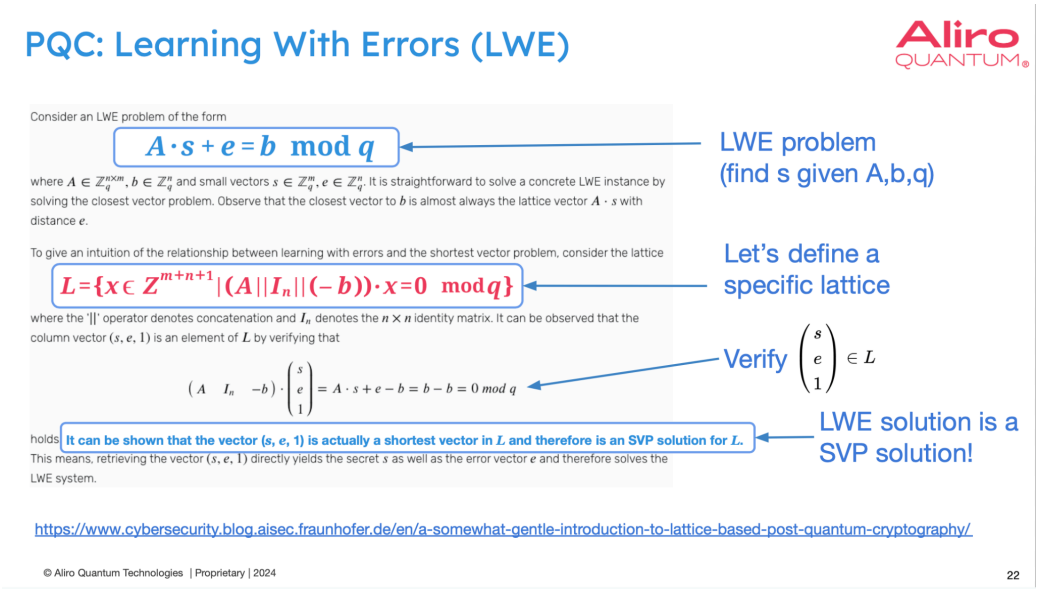
- **Shortest Vector Problem (SVP):** Assuming some lattice, which is like a periodic structure created by spanning basis vectors, b_1 and b_2. Generally, these are not orthogonal vectors. The spanning of these vectors creates a lattice. And the problem to solve is, what is the shortest vector in this lattice? The goal here is to find the shortest non-zero vector in the lattice, which is a grid-like structure formed by points in multidimensional space. This problem is computationally hard to solve, making it an ideal basis for cryptography.[SVP]



- **Closest Vector Problem (CVP):** This problem specifically deals with finding a lattice vector l that is closest to a given query vector q that is not on the lattice. In this case, there is a lattice defined by a basis, and the question is, what is the vector in the lattice that is closest to the query vector outside of the lattice?[CVP]



- **Learning With Errors (LWE):** LWE involves solving linear algebra equations with a unique twist—small random errors are added to the results of each equation. In this setup, the matrix A, vector b, and modulus q are publicly known, whereas the solution vector s and the error vector e remain private. These private vectors, s and e, are crucial to the secure setup and are never directly transmitted or shared. Decrypting the message requires accurately determining the original values of s before the errors encapsulated by e were introduced, a task that is challenging even for quantum computers due to the complexity introduced by these errors and the modular arithmetic constraints.[LWE]



In 2016, NIST initiated a challenge to identify viable post-quantum cryptography algorithms, leading to several years of competitive development. As a result, the field has been narrowed to four finalists, three of which are based on lattice cryptography—either for signature schemes or key encapsulation methods. The fourth finalist uses hash trees with collision-resistant functions. This composition underscores the significance of lattice-based solutions in post-quantum cryptography research. Notably, while traditional encryption methods like RSA and elliptic curve cryptography remain susceptible to quantum attacks, these post-quantum candidates are intended to offer quantum resistance, although their absolute long-term security remains unproven.

Information-theoretic Security

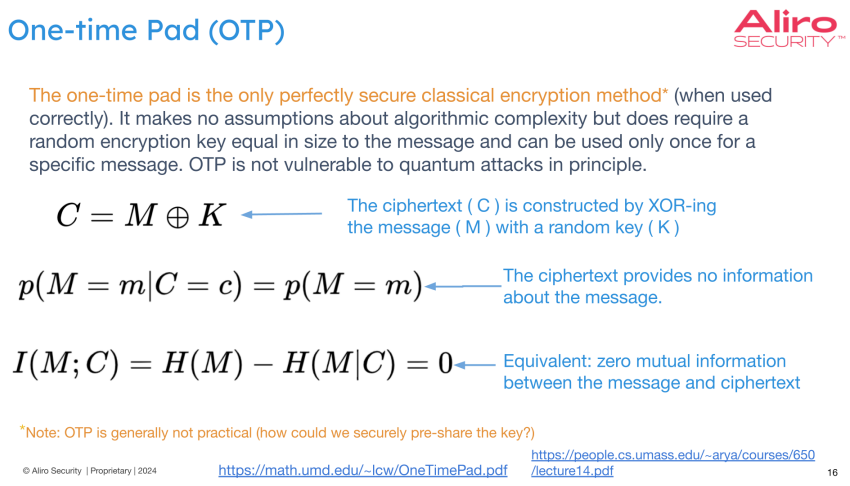
Information-theoretic security refers to a standard of cryptography that is impossible to break, even with unlimited computational power and time. A foundational principle of information-theoretic security is that the encryption process introduces a level of randomness and uncertainty such that the output (ciphertext) appears completely random to anyone who does not possess the decryption key. In other words, the ciphertext does not reveal any patterns or provide any information that could lead to deducing the plaintext or the encryption key, making the system secure against all conceivable forms of attack.

Information-theoretic security is desirable because it guarantees permanent security, unaffected by advances in mathematics or computing power. However, achieving this level of security in practice is quite challenging.

The One Time Pad (OTP)

The One Time Pad (OTP) is recognized as the only perfectly secure classical encryption method when applied correctly. This method requires that each encryption key be used exactly once and never reused. The OTP achieves what is known as information-theoretic security, making it immune to quantum attacks if implemented with a statistically unbiased key. The encryption process involves a straightforward operation where the

plaintext message is combined with a key using the XOR (exclusive or) operation to produce ciphertext. This method ensures that the ciphertext reveals no information about the plaintext, maintaining zero mutual information between the two. This characteristic means that the entropy—or uncertainty—of the original message remains unchanged after encryption, ensuring that any intercepted ciphertext gives no insight into the original message.[OTP]

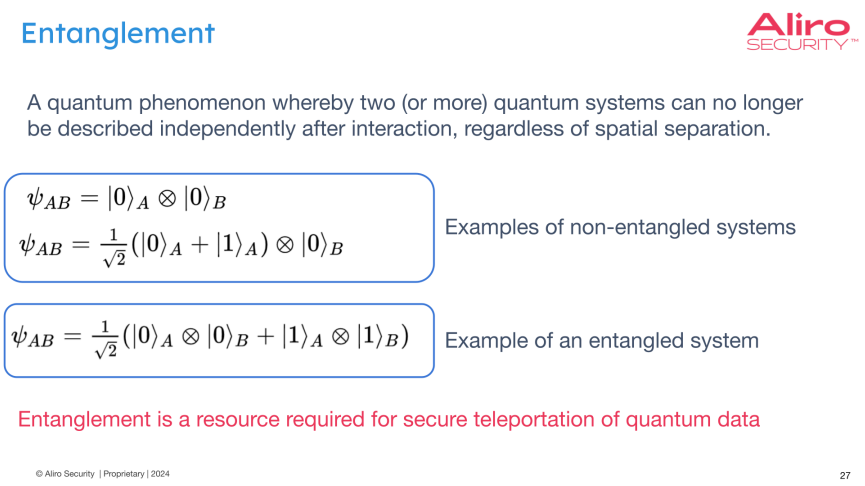


However, OTP's requirement for key uniqueness and length equal to the message makes practical application challenging. Key distribution poses a significant problem because a secure method to transmit the key without interception must already be in place. If that channel were in place, then creating a key might not be necessary to begin with; the secured channel would be used to send the data. Another practical challenge to using OTP is in the case of continuous secure communication: a new key of a length equivalent to the data must be continuously generated during transmission, which complicates the use of OTP in scenarios involving large data volumes or frequent communications.

Advanced Secure Communication Protocols

Communication protocols such as teleportation and quantum secure direct communication (QSDC) provide information-theoretic security, making them resistant to any computational power, including future quantum computers. This security stems from fundamental scientific principles:

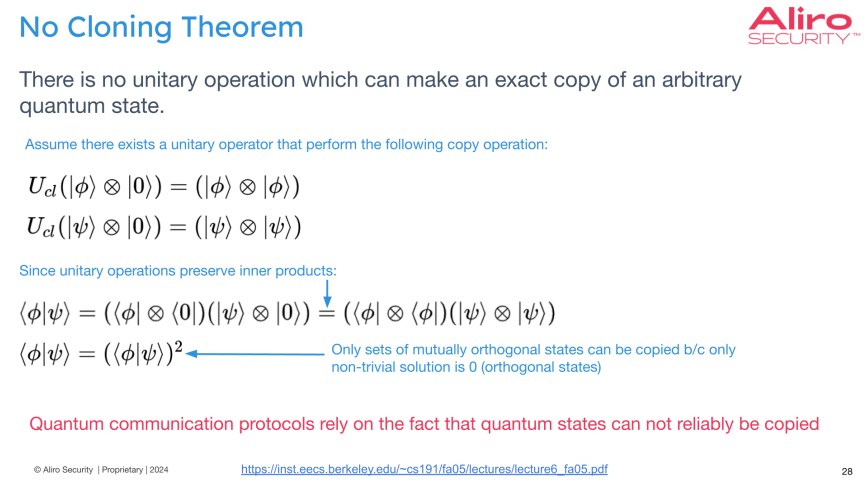
Entanglement. Entanglement is a phenomenon where quantum systems, such as a pair of photons used in quantum communication, become interconnected such that the state of one cannot be described without the other, regardless of the distance separating them. In quantum communication, entanglement is a valuable resource, especially for secure data transmission across entanglement-based Advanced Secure Networks because any attempt to eavesdrop on the quantum state alters the state itself, thereby revealing the presence of an eavesdropper.



In the example above, the first blue box shows two independent quantum systems, A and B, written as a tensor product. The measurement of A doesn't affect the measurement of B.

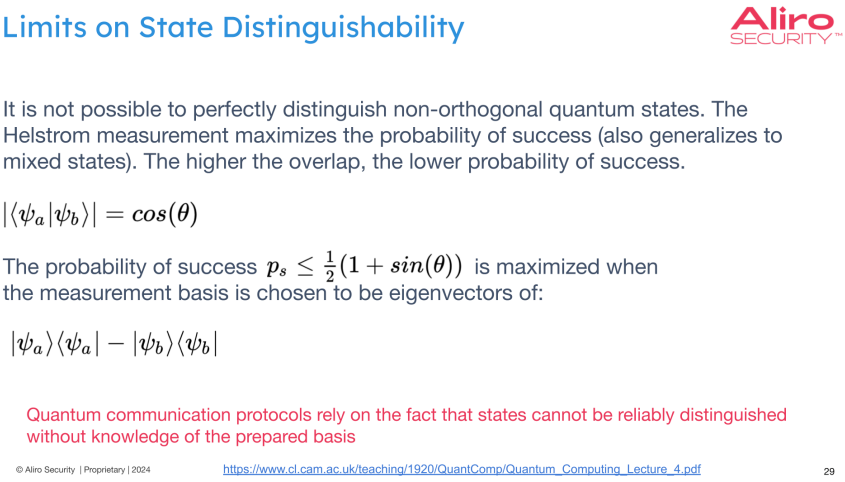
The equation in the second blue box describes an entangled system. In this case, the mathematical structure is not just a tensor product state. Once entangled, these systems cannot just be described by a simple tensor product. Instead, they exist in a state of superposition. In this state, any measurement of A immediately influences the state of B, reflecting a simultaneous collapse in the quantum state of both systems.

No-cloning Theorem. This theorem states that it is impossible to create an exact copy of an arbitrary unknown quantum state. This principle can be understood by considering a proposed unitary operation intended to clone quantum states.



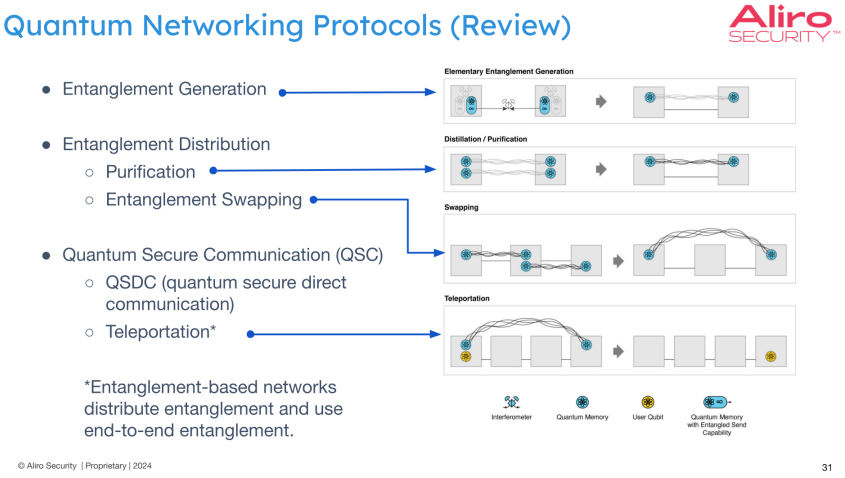
Unitary operations, which are a type of linear operation in quantum mechanics, preserve the inner product between states. This preservation implies that if an operation could clone quantum states, it could only clone states that are mutually orthogonal, as non-orthogonal states would not retain their inner product values post-operation[NOCLONING]. This principle guarantees that secure information passed through quantum states cannot be cloned or intercepted without detection.

State distinguishability. State distinguishability is a concept that delineates the limits of what can be known about a quantum state without prior knowledge of how it was prepared. The ability to distinguish quantum states depends significantly on their orthogonality. Non-orthogonal states, which do not lie at perpendicular angles in the state space, have a higher degree of overlap, making them more challenging to differentiate. In contrast, orthogonal states, positioned at right angles to each other, are readily distinguishable[DISTINGUISHABILITY]. By utilizing measurements that depend on the state preparations, any disturbances introduced by an interceptor change the system's statistical output, revealing their presence.



Quantum Networking Protocols

These protocols leverage the unique properties discussed previously to enhance security and communication capabilities across networks. The primary objective of these protocols is to distribute entanglement between nodes, allowing for complex processes like teleportation and quantum secure direct communication (QSDC).



There are three main processes / protocols involved in distributing entanglement for end user applications:

Elementary entanglement generation, or EEG, is used to distribute entanglement between nearby devices. Note that for local area entanglement-based Advanced Secure Networks, repeaters or other scaling technologies are not necessary. In this case, EEG alone can be used for entanglement distribution.

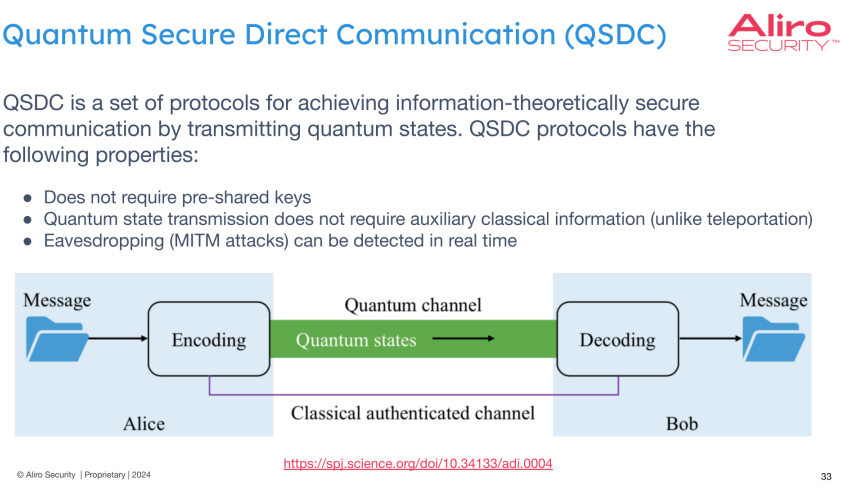
Entanglement purification, sometimes known as entanglement distillation, is used to ensure that the quality, or fidelity, of the entanglement is at a high enough level throughout the entire entanglement distribution process so it can be used for end user applications.

Entanglement swapping is used to extend the distance of the entanglement distributed by EEG. Using swapping and EEG together aids in distributed entanglement across far distances.

More on these protocols can be found in the Advanced Secure Networking 101 White Paper.

Teleportation. Teleportation is a protocol that enables transfer of quantum information (such as the quantum state of a particle) from one location to another, without physically moving the particle itself. Initially, two parties, Alice and Bob, share a pair of entangled qubits by using the protocols of EEG, entanglement purification, and entanglement swapping. Alice has a quantum state in a qubit that she wishes to teleport to Bob. Alice then performs a Bell-state measurement on the particle entangled with Bob's and the particle whose state is to be teleported. This measurement entangles these two particles and projects their combined state onto one of the four Bell states (a specific type of quantum state that involves entanglement). Once Bob applies the correct operations, his particle assumes the quantum state of Alice's original particle. The state has been "teleported" from Alice to Bob, without the original particle having traveled through space. ***More on teleportation can be found in the on-demand webinar.***

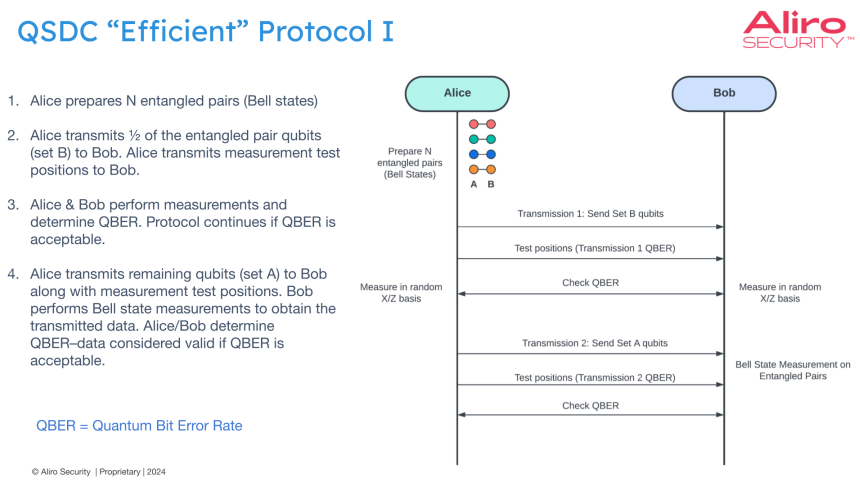
Quantum Secure Direct Communication (QSDC). QSDC protocols facilitate secure direct communication without the need for pre-shared keys, which differentiates them from traditional Quantum Key Distribution (QKD) methods like BB84, where keys are generated and then used for encrypting messages sent over a classical channel. In QSDC, the quantum states themselves carry the information, eliminating the need for an additional classical channel to reconstruct the state, unlike teleportation. QSDC protocols are also able to detect eavesdropping in real time[QSDC].



One of the core challenges in implementing QSDC is the inherent limitations in quantum state transmission over long distances. This includes issues like photon loss, which increases exponentially with the distance, and the need for high fidelity in state preparation and measurement. Protocols must manage these challenges while maintaining a low quantum bit error rate (QBER) to ensure the integrity and security of the communication.

The Efficient Protocol. The Efficient Protocol within QSDC frameworks is executed in two rounds.

ROUND 1



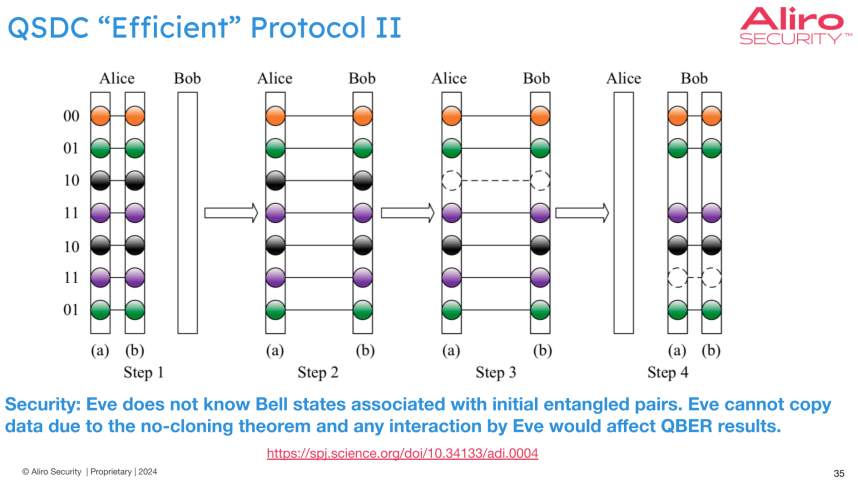
Step 1 - Preparation of Entangled States: Alice prepares a set of entangled quantum states, often Bell states, which are pairs of qubits entangled in such a way that the state of one (no matter the distance) instantly correlates with the state of the other upon measurement.

Step 2 - Transmission of Half of the Entangled Pairs: Alice sends one half of each entangled pair to Bob. This initial shipment of qubits sets the stage for establishing a secure communication link.

Step 3 - Initial Measurements and QBER Assessment: Upon receiving the first half of the entangled pairs, both Alice and Bob perform quantum measurements on their respective qubits. These measurements are used to calculate the Quantum Bit Error Rate (QBER). The QBER helps assess the integrity of the transmission up to this point, checking for any potential eavesdropping or interference.

Step 4 - Security Check: If the QBER is within acceptable limits—indicating no interference or eavesdropping—the protocol proceeds. This check is crucial as it confirms that the quantum channel is secure and that the initial part of the communication has not been compromised.

ROUND 2



Step 1 - Transmission of Remaining Qubits: Once the first round's security is confirmed, Alice sends the remaining half of the entangled pairs to Bob. This second transmission may also include additional test positions to further verify security during this phase.

Step 2 - Final Measurements and Re-Evaluation of QBER: After receiving the second set of qubits, Alice and Bob again perform measurements. These are needed for a second assessment of the QBER to ensure that no interference occurred during the second phase of transmission.

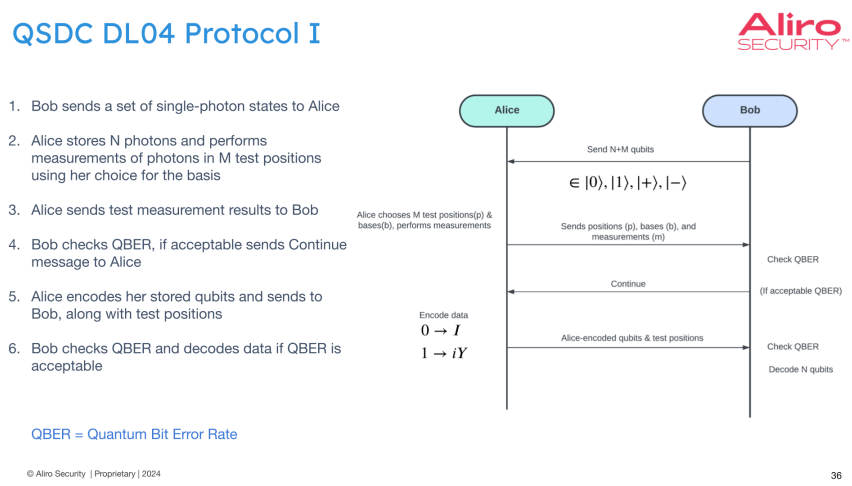
Step 3 - Decoding of Information: If the second QBER assessment also indicates a secure transmission, Bob then proceeds to use Bell state measurements to decode the information encoded in the states sent by Alice. This step effectively completes the secure communication process, as Bob can now retrieve the data transmitted by Alice.

Step 4 - Completion of Secure Communication: The protocol concludes with Bob having securely received and decoded the information sent by Alice, using the entangled states and ensuring through the QBER checks that the transmission was free from eavesdropping.

Each round in the Efficient protocol is designed to incrementally build and then confirm the security of the communication channel, using principles of quantum mechanics to safeguard the data against unauthorized access or interference. This staged approach allows for real-time monitoring and assurance of security before sensitive information is fully transmitted.

The DL04 Protocol. The DL04 Protocol within QSDC frameworks is executed using single photon states. Information is being sent from Alice to Bob, but in this protocol Bob initiates the protocol.

QSDC DL04 Protocol I



Step 1 - Initiation by Bob: The protocol begins with Bob sending a stream of single-photon states to Alice. These photons are encoded in a variety of bases, which could include both the standard computational bases (denoted as 0 or 1) and the superposition bases (denoted as + or -), also known as the X basis. This variety in encoding enhances the security of the transmission.

Step 2 - Selection and Measurement by Alice: Upon receiving the photons, Alice selects a subset of these photons to serve as test positions. She measures these selected photons using bases of her choice, which could vary between the computational and the X-basis. This step is critical as it determines the integrity and security of the transmission up to this point.

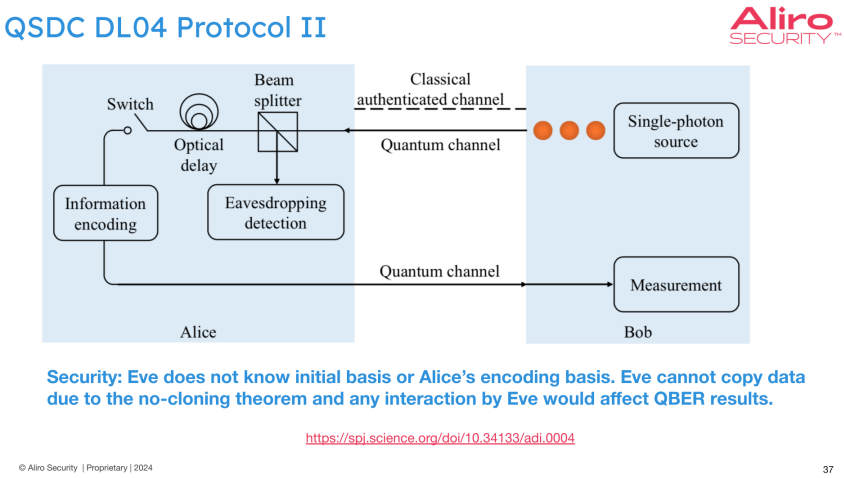
Step 3 - Communication of Results and Verification: Alice then communicates the results of her measurements back to Bob. Bob uses these results to calculate the Quantum Bit Error Rate (QBER), which is a critical measure of the integrity of the quantum state transmission. If the QBER is within acceptable limits, it suggests that the quantum states have not been tampered with, indicating no eavesdropping or interference.

Step 4 - Continuation of Protocol: If the QBER is acceptable, Bob sends a "Continue" command to Alice. This signals Alice to proceed with the encoding of her message onto the remaining stored qubits.

Step 5 - Final Transmission: Alice encodes her stored qubits and sends them to Bob, along with test positions.

Step 6 - Final Transmission Decoding: Bob performs a final check of the QBER with additional test positions to ensure that no interference occurred during the final transmission. If the QBER remains within acceptable limits, Bob proceeds to decode the data, thereby successfully receiving the message intended by Alice.

Below is a diagram of the physical setup for this protocol[DL04].

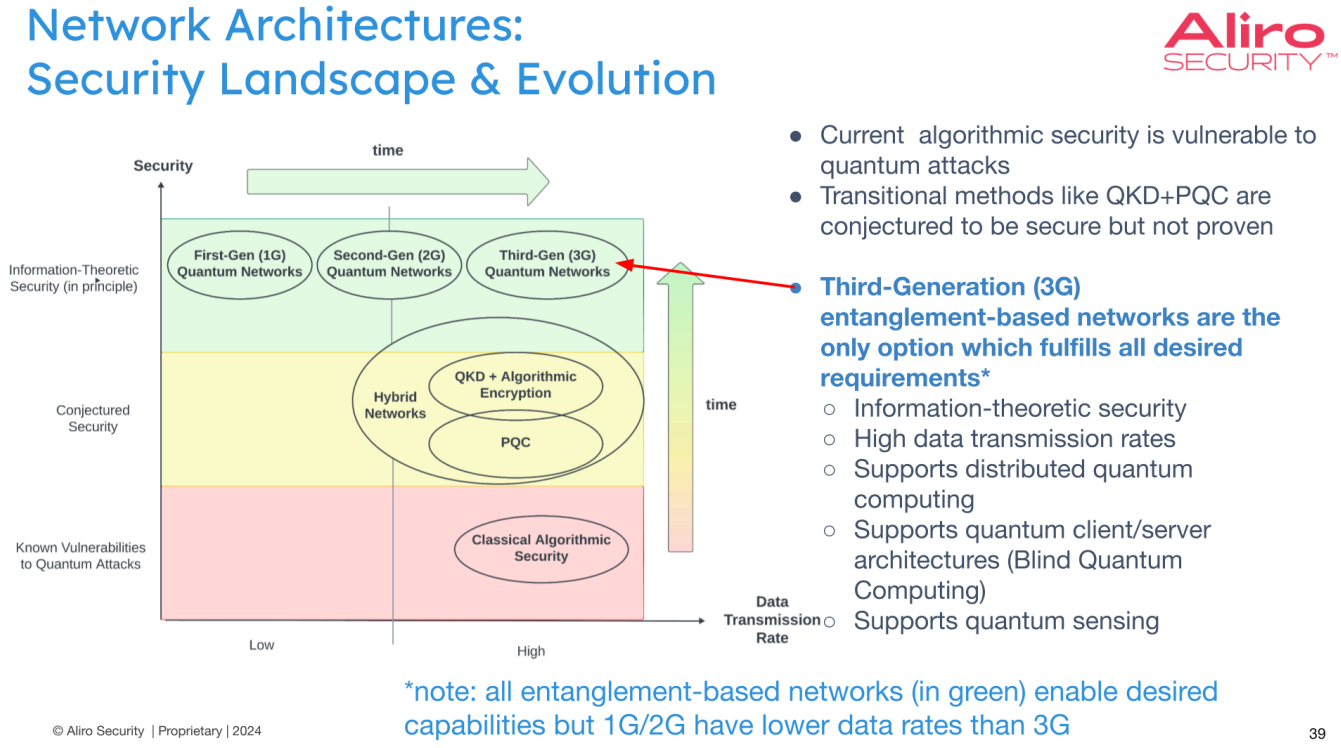


Bob is on the right, Alice is on the left, Bob sends a stream of photons across the channel. The beam splitter randomly selects a set of test positions and measures those, sending the results back over the classical channel to Bob. If Bob determines the error rate is acceptable, he sends the continue message back to Alice. Meanwhile, Alice stores the non-test positions in an optical delay. When she gets the continue message from Bob, she then flips the switch to use these qubits for information encoding, sends them back over to Bob, and then Alice and Bob perform the QBER test again on a subset of the qubits. Assuming no eavesdropping occurred, Bob will decode the remaining information from Alice.

The Evolving Security Landscape

Advanced Secure Networking technologies and their integration into network architectures signify a transformative shift in the security landscape. Classical networks, while offering high data rates, are increasingly susceptible to attacks by quantum computers due to the vulnerabilities of current encryption methods to Shor's algorithm and Grover's algorithm. These vulnerabilities can be addressed by Advanced Secure Networks, which promise to meet high-security standards through information-theoretic security by leveraging entanglement for a strong security foundation resistant to both quantum and classical attack.

The graphic below captures the evolution of the secure networking landscape.



At the bottom right is classical algorithmic security in use today. While these networks have high data transmission rates, there are critical known vulnerabilities to quantum attacks.

Just above classical algorithmic security are transitional methods such as QKD networks, which are vulnerable due to the required use of trusted nodes. Trusted nodes are not nodes that have proven to be trustworthy, but instead are nodes that are trusted regardless of whether they are secure or unsecure. Post Quantum Cryptography (PQC) is conjectured to be secure, but not proven. QKD can be used in combination with PQC to enhance security, which also prepares the infrastructure for a smoother transition to entanglement-based networks. However, QKD networks cannot be used to enable any applications beyond key exchange.

Another hybrid classical/entanglement-based network architecture could multiplex the classical/quantum data. This provides utility even when entanglement-based channel data rates are much lower than the classical data rates. Classical data could be time-division multiplexed with entangled data to detect eavesdropping using the concept of qubit error rate calculation from QKD and QSDC.

In the green area of the chart are entanglement-based Advanced Secure Networks. These networks achieve information-theoretic security, but 1G and 2G have lower data rates than 3G. The higher data transmission rates of 3G Advanced Secure Networks supports other capabilities beyond key exchange, including distributed quantum computing, quantum client/server architectures (such as

Blind Quantum Computing), and distributed quantum sensing. Entanglement provides a strong basis for security, however errors in the physical implementation of these networks can introduce vulnerabilities to side channel attacks. Implementing a layered security scheme with PQC requires attackers to break multiple systems in order to intercept the communication, strengthening the security posture.

Integrating Entanglement-based Advanced Secure Networks

It is evident that the landscape of security, especially in the context of Quantum Secure Communication advancements, is rapidly evolving. We stand on the brink of a significant transformation, where classical cryptographic techniques are giving way to the more robust protocols enabled by Advanced Secure Networks. Looking forward, Advanced Secure Networking promises not only enhanced protection but also a vast array of new applications. Preparing your cybersecurity infrastructure for the future involves proactive adaptation and thoughtful integration of these technologies into your existing frameworks to create a secure, resilient, and efficient networked world.

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 the capabilities of entanglement-based Advanced Secure Networking.

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

- Emerging hardware components necessary to build the entanglement-based network.
- The software necessary to design, simulate, run, and manage the entanglement-based Advanced Secure 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 Advanced Secure network. The steps you can take to ensure your organization is meeting the challenges and leveraging the benefits of the Advanced Secure Networking revolution are part of a clear, unified solution already at work in networks like the EPB Quantum Network℠ powered by Qubitekk in Chattanooga, Tennessee.

AliroNet™, the world's first full-stack entanglement-based Advanced Secure Network solution, consists of the software and services necessary to ensure customers will fully meet their secure networking goals. Each component within AliroNet™ is built from the ground up to be compatible with

entanglement-based Advanced Secure Networks of any scale and architecture. AliroNet™ is used to simulate, design, run, and manage entanglement-based 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 Advanced Secure 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 entanglement-based Advanced Secure Networks, (2) Pilot Mode for implementing a small-scale Advanced Secure Network testbed, and (3) Deployment Mode for scaling entanglement-based Advanced Secure 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 secure networking journey), reach out to the Aliro team for additional information on how AliroNet™ can enable your Advanced Secure Network.

info@alirosecurity.com www.alirosecurity.com

References

[AES] "Advanced Encryption Standard." Wikipedia, Wikimedia Foundation, 5 June 2024, en.wikipedia.org/wiki/Advanced_Encryption_Standard

[CVP] "A Somewhat Gentle Introduction to Lattice-Based Post-Quantum Cryptography." Cybersecurity Blog, Fraunhofer AISEC, 7 Feb. 2023, https://www.cybersecurity.blog.aisec.fraunhofer.de/en/a-somewhat-gentle-introduction-to-lattice-based-post-quantum-cryptography/

[DISTINGUISHABILITY] "Quantum Computing Lecture 4." University of Cambridge, www.cl.cam.ac.uk/teaching/1920/QuantComp/Quantum_Computing_Lecture_4.pdf

[DL04] "Free-Space Quantum Secure Direct Communication: Basics, Progress, and Outlook" Science.org, American Association for the Advancement of Science, 10.34133/adi.0004. https://spj.science.org/doi/10.34133/adi.0004

[GROVER] "Grover's Algorithm." *Wikipedia*, Wikimedia Foundation, 7 June 2024, en.wikipedia.org/wiki/Grover%27s_algorithm

[GROVER2] "Applying Grover's algorithm to AES: quantum resource estimates." arXiv, Cornell University, 16 Dec. 2015, arxiv.org/pdf/1512.04965.pdf

[LWE] "A Somewhat Gentle Introduction to Lattice-Based Post-Quantum Cryptography." Cybersecurity Blog, Fraunhofer AISEC, 7 Feb. 2023, www.cybersecurity.blog.aisec.fraunhofer.de/en/a-somewhat-gentle-introduction-to-lattice-based-post-quantum-cryptography/

[NOCLONING] "Lecture 6: Title of Lecture." University of California, Berkeley, Fall 2005, inst.eecs.berkeley.edu/~cs191/fa05/lectures/lecture6_fa05.pdf

[OTP] "One-Time Pad." *University of Maryland*, www.math.umd.edu/~lcw/OneTimePad.pdf

[QSDC] Pan, Dong, Xiao-Tian Song, and Gui-Lu Long. "Free-Space Quantum Secure Direct Communication: Basics, Progress, and Outlook." Advances in Data and Information Sciences, vol. 1, no. 1, 2024, American Association for the Advancement of Science, doi:10.34133/adi.0004. https://spj.science.org/doi/10.34133/adi.0004

[QUANTUMCIRCUIT] Quyen, Nguyen. "Quantum Computation and Quantum Information." Academia.edu, https://www.academia.edu/1537724/Quantum_computation_and_quantum_information

[RSA] "RSA (Cryptosystem)." Wikipedia, Wikimedia Foundation, 7 June 2024, en.wikipedia.org/wiki/RSA_(cryptosystem)

[SHOR] "Shor's Algorithm." Wikipedia, Wikimedia Foundation, 7 June 2024, en.wikipedia.org/wiki/Shor%27s_algorithm

[SVP] Fraunhofer AISEC. "A Somewhat Gentle Introduction to Lattice-Based Post-Quantum Cryptography." Cybersecurity Blog, 7 Feb. 2023, www.cybersecurity.blog.aisec.fraunhofer.de/en/a-somewhat-gentle-introduction-to-lattice-based-post-quantum-cryptography/