

Review

Not peer-reviewed version

How to Address the Threat Quantum Computing Poses to Cybersecurity

Jiya Goswami , Venkata A. Nimmagadda , Atria Datta , Joel Olora , [Mesut Yurukcu](#) *

Posted Date: 8 October 2026

Keywords: quantum computing; quantum physics; cryptography; quantum gates; cybersecurity



Preprints.org is a free multidisciplinary platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC, OpenAlex.

Copyright: This open access article is published under a [Creative Commons CC BY 4.0 license](#), which permit the free download, distribution, and reuse, provided that the author and preprint are cited in any reuse.

Disclaimer/Publisher's Note: The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.

Review

How to Address the Threat Quantum Computing Poses to Cybersecurity

Jiya Goswami ¹, Venkata A. Nimmagadda ¹, Atria Datta ¹, Joel Olora ¹ and Mesut Yurukcu ^{2,*}

¹ BASIS Cedar Park Ed.
² Mina AI Labs, LLC.
* Correspondence: mxyurukcu@ualr.edu

Abstract

Quantum computing represents a fundamental shift in computational capability, using quantum mechanical principles, such as superposition, entanglement, and interference, in order to process information exponentially faster than classical systems. Unlike traditional computers that manipulate bits as 0s and 1s, quantum computers harness qubits that exist in probabilistic superposition states, enabling exploration of multiple solutions at the same time. While this advancement promises transformative applications in molecular modeling, optimization, and machine learning, it also threatens the cryptographic foundations securing modern digital infrastructure. The security of modern day systems relies on mathematical problems that are not easily solvable for classical computers. Quantum algorithms, particularly Shor's Algorithm and Grover's Algorithm, render current asymmetric and symmetric encryption protocols computationally vulnerable; critically, the "Harvest Now, Decrypt Later" strategy transforms present day communications into long term security liabilities affecting government, financial, healthcare, and critical infrastructure sectors. To address this threat, this paper evaluates post-quantum cryptographic defenses and proposes Quantum Key Distribution (QKD) as the optimal security framework. Unlike mathematical approaches vulnerable to algorithmic advances, QKD anchors security in the No-Cloning theorem and wave-function collapse ensure that eavesdropping attempts introduce detectable anomalies, enabling real-time threat detection. Through comparative analysis of scalability, deployment feasibility, and cost efficiency, this paper demonstrates that QKD provides the most robust, future-proof mechanism for protecting sensitive data transmission in the quantum era, offering a critical blueprint for resilient network defense against emerging computational threats.

Keywords: quantum computing; quantum physics; cryptography; quantum gates; cybersecurity

1. Introduction

The introduction should briefly place the study in a broad context and highlight why it is important. The accelerating development of quantum computing represents one of the most consequential technological shifts of the twenty-first century. While quantum computation promises almost incomprehensible capabilities across fields such as optimization, materials science, and cryptography, it simultaneously poses some serious risks to global cybersecurity infrastructures. Modern digital systems rely fundamentally on classical cryptographic assumptions. Specifically, the computational hardness of problems such as integer factorization and discrete logarithms. These assumptions are part of nearly all secure communication protocols used today, including TLS, SSL, RSA, and elliptic curve cryptography. The emergence of scalable quantum computers threatens to circumnavigate these assumptions entirely. As a result, the security guarantees that sustain global commerce, governmental communication, financial systems, and personal privacy may be rendered obsolete. This paper examines the nature of this threat and argues that Quantum Key Distribution (QKD) represents the most robust and physically grounded solution for securing communication in a post quantum world [1,2].

To understand the scale of the challenge quantum computing poses, it is necessary to distinguish clearly between the realms of classical and quantum computing. Classical computation is built upon permutations of binary logic, where information is encoded in bits that take the values of 0 or 1. The scaling of this classical computational power has historically followed Moore's Law, driven by the miniaturization of transistors on integrated circuits. However, the miniaturization that follows Moore's Law has certain constraints due to the scale and size of atoms, because current computer architecture cannot take advantage of the behaviors of quantum particles, or matter at quantum scales. Quantum computing, by contrast, operates on qubits, which can exist in superpositions of classical states and become entangled with one another. These properties allow quantum computers to perform certain operations, such as factoring large integers using Shor's algorithm or speeding up search using Grover's algorithm, at speeds that are unseen in classical machines [2,3].

Therefore, there is a clear distinction between classical and quantum computing that is deeply rooted in physical principle and speed, which paints a picture as to the power quantum has over traditional. The implications of this distinction extend directly into cybersecurity. In modern times, cybersecurity is one of the most core facets that provides security and stability to the entire world, being the "glue" that holds the world wide web together. In other words, it's the failsafe that upholds digital society. These secure communication protocols govern nearly every aspect of contemporary life, like banking, cloud computing, governmental and medical records, personal messages, and many more. Said protocols rely on encryption whose security is derived from mathematical hardness, like how Rivest-Shamir-Adleman (RSA) depends on the difficulty of factoring large composite numbers, and elliptic-curve cryptography (ECC) depends on the hardness of discrete logarithms on elliptical curves. Symmetric key encryption algorithms such as Advanced Encryption Standard (AES) rely on how impractical brute forcing large key spaces is. Classical cybersecurity therefore assumes that adversaries are limited to classical computational resources, which is a key fallacy in the face of quantum [1,4,5].

Quantum disrupts this assumption which once lied as a key part of classical cybersecurity. A powerful enough quantum computer can most certainly factor large integers as well as compute discrete logarithms efficiently, severely stripping down the security and credibility of RSA and ECC as we advance in technology. Along with this, Grover's algorithm reduces the true security of symmetric encryption by establishing a quadratic speedup for the brute-force key search. Although symmetric methods can be strengthened using larger key sizes, public key cannot, and it along with its underlying hardness assumptions die with the introduction of quantum [2,3].

Taking in all of this surface level information presented above, it can be firmly concluded that the confidentiality, integrity, and authenticity of digital communications are at risk. In fact, the prominence of the threat has led many nations and corporations to invest in harvesting encrypted data for future decryption once quantum computers become available for commercial use. The cybersecurity landscape must therefore evolve from reliance on computational hardness to reliance on physical principles, so that this key flaw might be circumvented [6,7].

This paper argues that Quantum Key Distribution (QKD) is the most promising and fundamentally secure method for addressing this threat. QKD leverages quantum mechanical phenomena to enable two parties to generate shared secret keys with security guaranteed by the laws of physics rather than the aforementioned assumptions. QKD has many perks aside from how it bypasses the problems of classical methods, including impenetrable eavesdropping detection and guaranteed longevity. Once the key is established through this method, classical symmetric encryption like AES can be used for data transmission, with the assurance that the key exchange process is quantum secure. The significance of QKD becomes even clearer when compared to alternative approaches. Some of the most prominently studied methods to solve the problem discussed, like Post quantum cryptography (PQC), pale in comparison to the many guarantees QKD provides. Whilst these methods might be viable and plausible for the short run, they do not uphold the same safety and standard QKD promises to, and so it is clear as crystal that QKD should reign supreme [8,9].

Of course, QKD is not without its fallacies despite its many strengths. Practical implementations for QKD face challenges such as photon loss, limited transmission distance, susceptibility to side channel attacks, and the need for specialized hardware. However, ongoing research in satellite based QKD, entanglement based protocols, measurement device independent QKD, and quantum repeaters continues to expand the feasibility and scalability of quantum communication networks. These advancements suggest that QKD can be improved to meet the demands of global communication infrastructure, making it not only the most secure option but also the most adaptable. Therefore in this paper, we plan to explore ways to improve upon QKD as well [8,10–12].

This introduction establishes the framework used for the rest of the paper, with the next section further diving into the differences between classical and quantum computation, emphasizing the physical principles that enable quantum advantage. Following this, the paper will examine the structure and importance of modern cyber security systems, showing how deeply rooted they are within society once again. The next section will then analyze the specific threats quantum computing poses to classical cryptography, including the mathematics of Shor's and Grover's Algorithms. The core of the paper will then present Quantum Key Distribution as the most robust solution to these threats, explaining its mechanisms, security guarantees, and practical implementations. A further analysis will demonstrate why QKD surpasses all other proposed methods for securing communication in a post quantum world. Finally, as said before, the paper will attempt to show ways to improve upon this promising method.

Essentially, the frontier of quantum computing necessitates the need for a fundamental restructuring of our society's cybersecurity. Classical cryptography systems cannot withstand quantum attack, and computationally based defenses are not much better. Quantum Key Distribution offers a way forward that circumvents said problems due to its uniqueness in principle and design, and as years pass, QKD will prove to be a key and necessary part of cybersecurity.

2. Comparing Between Quantum, Classical Computing, and Cybersecurity

2.1. How does Quantum Computing Differ from Traditional Computing?

Traditional computers operate using bits, represented as either 0s or 1s. Quantum computers, in contrast, use quantum bits, or qubits, which exploit the principle of quantum mechanics to exist in a state of 0, 1, or both simultaneously. This phenomenon is known as superposition. Qubits can also experience entanglement, meaning that the state of one qubit directly correlates with the state of another. The physical distance between them does not affect this relationship. This allows quantum computers to process a large number of possibilities simultaneously rather than sequentially, thus making them much faster than standard computers. A third principle, quantum interference, is a fundamental phenomenon in quantum mechanics where the probability amplitudes of quantum states combine, allowing quantum computers to amplify correct answers and cancel out incorrect ones. Together, these properties give quantum computers computational power that dwarfs most things achievable by even the most powerful classical supercomputers in existence today [13,14].

In order to understand how quantum computers pose a threat to cybersecurity, it is important to understand the foundational mathematics upon which modern encryption is built upon. The majority of today's internet security relies on public key cryptographic systems. These systems are secure because they are based on mathematical problems that are computationally infeasible for standard computers to solve in a reasonable timeframe. For example, Rivest–Shamir–Adleman (RSA) encryption depends on the extreme difficulty of factoring very large numbers, numbers that are the product of two enormous prime numbers. Elliptic Curve Cryptography (ECC) similarly to RSA is an asymmetric encryption method used to secure digital communications. It relies on the algebraic structures of elliptic curves to create faster, smaller, and highly efficient cryptographic keys compared to older standards like RSA. A classical computer would take millions of years to factor a 2048 bit RSA key. However, a sufficiently powered quantum computer running Shor's Algorithm could theoretically factor that same number in a matter of hours or even minutes. ECC relies on the

difficulty of solving the discrete logarithm problem, however, due to Shor's algorithm's ability to efficiently solve both the integer factorization problem and the discrete logarithm problem found in the ECC encryption method, it is rendered futile in the face of quantum computing. Quantum computers are capable of rendering RSA and ECC encryption obsolete [1,2].

Symmetric Encryption algorithms, such as the Advanced Encryption Standard (AES), the global industry standard used to secure sensitive electronic data, are also susceptible, although to a smaller degree. Another quantum algorithm, Grover's Algorithm, can search through unsorted data quadratically faster than standard methods. This halves the security strength of symmetric keys, meaning AES-128 would offer only the equivalent protection of a 64-bit classical key, which is considered breakable. While this isn't as much of a risk as Shor's algorithm is to RSA keys, it still demands that organizations upgrade symmetric key lengths to maintain adequate protection. Beyond encryption, quantum attacks can compromise digital signatures, certificate authorities, VPNs, and virtually all other secure communication channels [1,3].

An alarming strategy that is already being used by many nation states and sophisticated threats is known as the "harvest now, decrypt later" (HNDL) strategy. In this attack model, encrypted data is harvested and stored today, even though it cannot be decrypted with current technology. The attackers are hoping that in the future, a sufficiently powerful quantum computer can be created that is able to decrypt the harvested data to release sensitive secrets. This makes quantum computing a threat not just in the future, but in the present as well. Classified government communications, intellectual property, financial data, and military intelligence being transmitted today could all become compromised the moment quantum computing becomes easily accessible. Intelligence agencies including the NSA have publicly recognized this risk and have begun urging organizations to turn to quantum resistant solutions [6,7,15].

3. Cybersecurity in Market Sectors

Across all sectors, the financial toll of cybersecurity breaches is large and rapidly increasing. Global cybercrime costs were recorded to be \$8 trillion dollars in 2023 increasing to \$10.1 trillion in 2025 [16]. The arrival of capable quantum computers threatens to make the figure look modest in comparison. The economic, social, and geopolitical consequences of a world unprepared for quantum enabled cyberattacks demand that every market sector treat post-quantum cryptographic readiness as a strategic imperative.

3.1. Financial Services and Banking

Financial services and banking are intensely reliant on cyber security. The financial sector is one of the most heavily targeted industries in the world. This is where money, data, and power intersect. Cybersecurity breaches in this sector manifest as bank fraud, unauthorized wire transfers, theft of customer financial records, and the collapse of trading platforms. The 2016 Bangladesh Bank heist, for example, illustrated how embedded digital vulnerabilities are in global finance as hackers exploited the SWIFT interbank messaging system to steal \$81 million. Beyond direct theft, breaches erode consumer confidence, trigger regulatory penalties, and cause catastrophic reputational damage that can take years to repair. Stock prices of breached financial institutions typically drop 4 - 7% immediately aftermath of a disclosed attack.

Modern banks rely on RSA and ECC encryption to secure transactions, authenticate identities, and protect customer data in transit. When quantum computers capable of running Shor's algorithm are operational, every encrypted financial transaction becomes theoretically decryptable. Even more alarming is the "harvest now, decrypt later" threat. People may already be archiving encrypted financial communications today, positioning themselves to expose decades of transaction data the moment quantum decryption matures. Central Banks and financial regulators, such as the Bank for International Settlements (BIS), have already begun issuing guidance urging institutions to assess their cryptographic exposure and accelerate migration toward post-quantum cryptographic standards.

3.2. Healthcare

Healthcare is arguably the sector with the highest human cost attached to cyber security breaches. Hospitals, insurance providers, and pharmaceutical companies store extraordinarily sensitive personal data, all of which being highly valued on the dark web, often exceeding the value of stolen credit card numbers. The 2015 Anthem Health breach exposed nearly 79 million patient records, while ransomware attacks on hospital networks have, in documented cases, contributed to patient deaths by disabling critical care systems. Beyond patient data, pharmaceutical companies are prime targets for intellectual property theft. Years of drug research and clinical trial data can be stolen in a single intrusion.

Quantum computing amplifies each of these risks. Medical research institutes increasingly share encrypted genomic data, trial results, and patented compound structures across global networks. These communications, secured today by classical encryption, are vulnerable to harvest-now-decrypt-later attacks by nation-state actors seeking to leapfrog years of pharmaceutical R&D. Furthermore, as healthcare systems rely more on AI driven diagnostics and connected medical devices, the attack surface grows exponentially and each device that relies on classical cryptographic handshakes becomes a potential quantum era vulnerability. The consequences extend past the simple financial loss, compromised drug formulation data or manipulated patient records in a quantum-breached environment could directly endanger lives.

3.3. National Security

Quantum computing also poses significant challenges to national security as well. The ability of quantum computers to break through encryption methods, like RSA and ECC, could lead to catastrophic data breaches, exposing classified information, and compromising national security. In addition to this, the potential for malicious actors to utilize quantum technology to launch cyber attacks on critical infrastructure, including power grids and transportation systems, poses severe risks to public safety and national stability. The enhanced data processing capabilities of quantum computing could also facilitate more effective surveillance and intelligence gathering, enabling adversaries to predict and counter national defense strategies.

4. Ways to Alleviate These Threats

4.1. Established Ways to Alleviate Quantum Computing Threats to Cybersecurity

The emergence of fault-tolerant quantum computers threatens to render the most widely deployed public-key cryptographic systems, such as RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC), obsolete. All of these systems derive their security from the computational hardness of integer factorization and the discrete logarithm problem. Shor's algorithm, when executed on a sufficiently powerful quantum computer, can solve problems in polynomial time, meaning a hacker could easily decrypt intercepted ciphertext, forge digital signatures, and impersonate trusted individuals across banking, healthcare, and military networks. A second quantum threat comes from Grover's algorithm, which provides a quadratic speedup for extensive key searches, effectively halving the security level of any symmetric cipher or hash function (e.g., reducing AES-256 to an equivalent of 128 bits of security) [1–3].

Currently, the cryptographic community, led by the National Institute of Standards and Technology (NIST) and academic researchers worldwide, has developed and standardized several classes of solutions. This section surveys five established approaches. (1) Post-Quantum Cryptography (PQC) standardized by NIST, (2) Quantum Key Distribution (QKD), (3) Symmetric-Key and Hash-Function Hardening, (4) Crypto-Agility Frameworks, and (5) Harvest-Now-Decrypt-Later (HDNL) Mitigations. Each method will be examined in terms of its mathematical foundation, current maturity, deployment considerations, and limitations [6,7,18].

4.2. Quantum Key Distribution (QKD)

4.2.1. Principles and Physics

Quantum Key Distribution (QKD) utilizes the laws of quantum mechanics to distribute cryptographic keys information theoretic security, a stronger guarantee than the computational security of PQC. The most important property exploited is the no-cloning theorem: an unknown quantum state that cannot be copied exactly. Anything trying to attempt to measure quantum-encoded key bits necessarily disturbs the quantum states, introducing detectable errors [8,9].

The first and most widely analyzed QKD protocol is BB84, a step-by-step procedure for securely exchanging cryptographic keys, proposed by Bennett and Brassard in 1984. In BB84, Alice and Bob, the standard fictional characters used in cryptography to represent the 2 communicating parties, work together to establish a shared secret key. Alice encodes random key bits onto individual photons using one of two conjugate bases chosen at random; Bob measures each photon in a randomly chosen basis. They publicly compare basis choices (but not bit values) and retain only their bits where their choices matched the sifted key. A subset of sifted bits sacrificed to estimate the Quantum Bit Error Rate (QBER). If the QBER exceeds approximately 11%, the channel is presumed compromised and the key is discarded. Otherwise, classical error correction and privacy amplification distill a secure final key [8,9].

Later protocols extend the BB84 framework. E91, a method proposed by Artur Ekert in 1991, uses entangled photon pairs and Bell inequality tests to certify security. Continuous Variable QKD (CV-QKD) encodes information on the quadrature amplitudes of coherent light states, enabling the use of standard telecom detectors [8,19].

4.2.2. Physical Implementation

Commercial QKD systems have been deployed by Quantique (Switzerland), Toshiba (United Kingdom), QuantumCTek (CHina), and magiQ Technologies (USA). Implementation modalities include:

Fiber-Optic QKD — Single photons or weak coherent pulses are transmitted over standard telecom single-mode fiber (attenuation ~ 0.2 dB/km). Practical ranges are limited to ~ 100 – 150 km due to photon loss, beyond which secure key rates approach zero. Quantum repeaters—which extend range via entanglement swapping—remain largely experimental [10,20].

Free Space and Satellite QKD — Photons are transmitted through open air or space. China's Micius satellite has demonstrated intercontinental QKD distances over 1,200 km by exploiting the low attenuation of space (above the dense atmosphere). Ground station networks and LEO satellite constellations represent the emerging architecture for global QKD [11,12].

Integrated Photonic QKD — Chip-scale implementations using silicon photonics reduce device size and cost, enabling future integration into network equipment [21–23].

4.2.3. Security Caveats and Side-Channel Attacks

The theoretical security of QKD is information-theoretic, but practical implementations are vulnerable to side-channel attacks exploiting deviations from the ideal quantum model. One of the attacks is a Photon Number Splitting (PNS) Attack. This attack occurs when a weak coherent pulse source occasionally emits multi-photon pulses. An eavesdropper can split off one photon and measure it after basis reconciliation, leaking key information without disturbing Bob's single-photon measurements. Decoy-state protocols statistically bound this attack by transmitting pulses of varying intensities [8,24].

Another attack is a Detector Blinding Attack. By illuminating single-photon detectors with bright classical light, an attacker can force them into a linear operating mode, controlling their responses and defeating the quantum channel entirely [25].

Lastly, the Trojan-Horse Attack. An adversary probes the sending apparatus with optical pulses to learn Alice's basis settings, exploiting information leaked by the physical device rather than the quantum channel [26,27].

4.2.4. Current Deployments and Limitations

Notable real-world QKD deployments include the Chinese national QKD backbone spanning over 2,000 km from Beijing to Shanghai, the EU Quantum Flagship network, and various financial institution pilots in Europe and Asia. Despite these advances, QKD faces fundamental limitations that preclude near-term replacement of PQC at internet scale [10,12].

Firstly, the distance factor. Fiber QKD is practically limited to ~100–150 km without quantum repeaters. Trusted relay nodes extend range but reintroduce classical security assumptions at each intermediate node.

Achievable secure key rates at 100 km are typically in the kilobits-per-second range—far below modern data-rate requirements. QKD keys refresh symmetric cipher keys rather than directly encrypting bulk data.

QKD requires an authenticated classical channel for basis reconciliation, creating a circular dependency on pre-shared keys or classical signatures.

Dedicated QKD hardware and fiber runs remain expensive, currently limiting deployment to high-security government and financial applications [10,15].

5. Comparing QKD and Other Methods

Although cybersecurity challenges introduced by quantum computing can be approached from multiple angles, not all solutions offer the same level of reliability or longevity. Every single problem has multiple approaches, and this problem is no exception, so why focus on just one such solution to a problem? In most technical problems, one method is usually the most accepted in that it is the most effective in the long run and works most thoroughly. The problem posed in this paper, that of quantum computing's threat to cybersecurity, is no different. Approaches like post quantum cryptography (PQC), hybrid systems, and strengthened classical methods might appear to fix the aforementioned problem, but they all have a glaring flaw: they rely on assumptions of mathematical hardness. These assumptions might not hold up forever, and are therefore liabilities that might hold these methods back from being completely effective [1,7].

In contrast to the methods mentioned, QKD or quantum key distribution is not based on such assumptions. It is based on the laws of physics, which are absolute when directly confronted. In this distinction lies what makes a world of difference between QKD and other methods. Because of this nature, QKD offers stronger fault tolerance, built in eavesdropping, and resilience to future developments in technology with a security that does not degrade over time. These key reasons prove why QKD is one of the most promising solutions to this threat of quantum computing on cybersecurity [8].

5.1. Fault Tolerance

Most cryptographic systems, regardless of if they are classical or post quantum, are built on assumptions about what operations are computationally difficult. With today's level of computing, these assumptions are reasonable, as said before. However, these assumptions can still be broken. If some new algorithms, mathematical principles, or hardware capable of breaking these assumptions is invented, all of these will be for naught. For example, PQC is designed to resist quantum attacks, yet it still depends on the idea that certain lattice or code based problems remain intractable. This shows that these do not account for multiple cases in order to make sure encryption works regardless of impasse, showing the lack of fault tolerance [1,6].

QKD avoids this fallacy, because its security is not tied to how hard it is to solve an equation but to how quantum states behave, which cannot be measured without disturbance. Again, because this

principle is rooted in physics, it does not rely on the mathematical hardness of a problem surviving. So, QKD could protect against many possible attack scenarios allowed by the laws of nature. It is then a fact that QKD cannot be broken in the ways presented, and is therefore the most fault tolerant [8,9].

5.2. Built in Detection for Threats

QKD has another big advantage over other methods, and it is that it exposes eavesdropping innately, without having to design measures to counter it by hand. In quantum key distribution, most attempts to intercept the data by intercepting the transmitted photons alters their quantum state, making them not convey the intended information anymore. This alteration is noticeable and can be recorded, or in other words is almost unavoidable. This not only works as an extra layer of security but also as this built-in way to detect eaves dropping, as it "notifies" when someone is observing the photons via "self-destruction". It also makes recorded information unusable as the disruption of the quantum state renders the conveyed information unreadable to eavesdroppers. This is not prevalent in algorithms like PQC or any other classical algorithm, and the possibilities to use this for threat counter measures and safety are vast. As a result, systems that include QKD can detect interception attempts as they happened, and prevent most of the interceptions from working by garbling the signal due to the disruption of quantum state [8,9].

This is fundamentally different from other systems like those of classical computing or PQC, which only make interception hard to carry out, but not impossible or detectable. In other words, the people conveying information cannot tell if anyone else has intercepted the message, and the interception itself can be successful, both of which are problems QKD mostly avoids. Again, QKD provides a physics-based guarantee of safety, while the others do not. The quantum collapse of the system acts as a built-in alarm that comes with transparency that other systems cannot replicate [1,8].

5.3. Security Regardless of Foreseeable Future Developments

One prominent problem in designing cybersecurity systems that are built for long term use is the unpredictable evolution of future mathematics, cypher breaking, and technology. Newer algorithms, technology, equations, and methodologies might be used in the future to undermine whatever cybersecurity system someone tries to set up that relies on computational hardness. Classical methods all rely on this, and so are also inevitably prone to being broken in the future. PQC is undeniably strong in computational hardness, beyond others proposed, but still is rooted in the same principle and is therefore also doomed to the same fate [1].

With the future holding many different possibilities that might disrupt the current state of cybersecurity due to the same reasons as quantum (as said in this paper), a solution to this problem is most effective not only by protecting from currently predicted short term threats, but also securing safety for the long run. QKD does just this; It is one of the methods that has no viable threats that might pop up in the long run. Of course this is limited by our human foreseeability, as we cannot account for some far off solution that is out of our scope right now, but it is still better than a method that could be broken within the bounds of our foreseeable scope.

Basically, QKD stands practically alone as a method that, again due to its rooting in physics principle and lack of mathematical hardness, is an exception to this problem. As long as the principles of quantum mechanics remain valid, the protections provided by QKD remain intact. This gives QKD a unique resilience to future developments that is not only unprecedented, but unseen in other upcoming methods. Few other systems can claim the same level of guarantee QKD has on this matter [8].

Conversely, things like hybrid cryptographic systems just provide security for now by integrating future mechanisms slowly. This is a good idea for the short term, but for true long-term security, a hybrid approach has value but does not completely work. QKD, with how it appears to be "unbreakable" for now, is a much better option in regards to the future [29].

Taken together, these characteristics make QKD one of the strongest available responses to the cybersecurity challenges posed by quantum computing. Its foundation in physics, rather than

mathematics, gives it a level of guarantee and reliability that few other approaches can match. It detects eavesdropping inherently, remains secure regardless of future computational developments, and does not degrade over time. While PQC and hybrid systems play important roles in the transition period, QKD stands out as one of the only methods that offers long term, physics-based security. As quantum technologies continue to advance, the stability and transparency provided by QKD make it a very compelling solution for safeguarding information in the foreseeable future [6,8].

6. Ways to Improve Upon Quantum Key Distribution

6.1. Common Criticisms of Quantum Key Distribution

Quantum Key Distribution (QKD) is often acclaimed due to the idea that it prevents interception and data theft through the laws of physics rather than mathematical formulas. However, some believe that QKD is not a reliable encryption method, citing its inability to perform authentication, its vulnerability to insider threats, its compromising reliance on hardware, its infrastructure costs, and its vulnerability to denial of service (DoS) attacks as reasons that QKD should be overlooked in favor of other methods of post-quantum cryptography.

6.2. Authentication and Hybrid Security

Organizations such as the National Security Administration argue that the need for classical authentication undermines the efficiency of QKD, requiring other forms of quantum-resistant cryptography to be developed alongside it in order for it to function. The figure below shows how QKD is vulnerable without authentication [15].

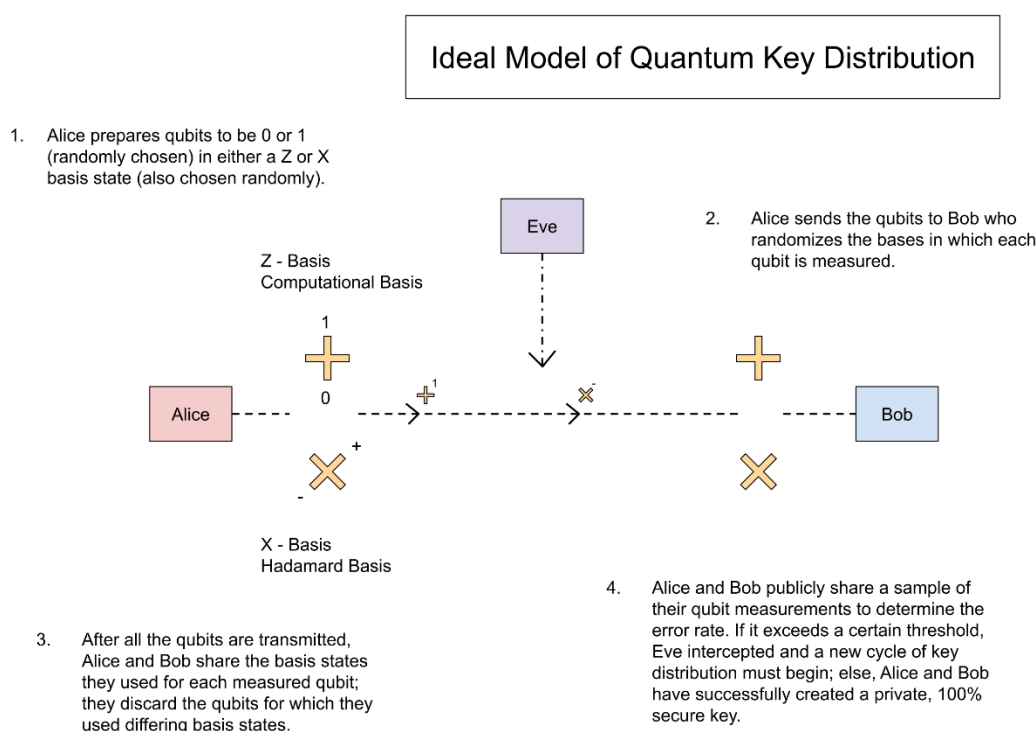


Figure 1. Ideal Model of Quantum Key Distribution.

Quantum Key Distribution Without Authentication

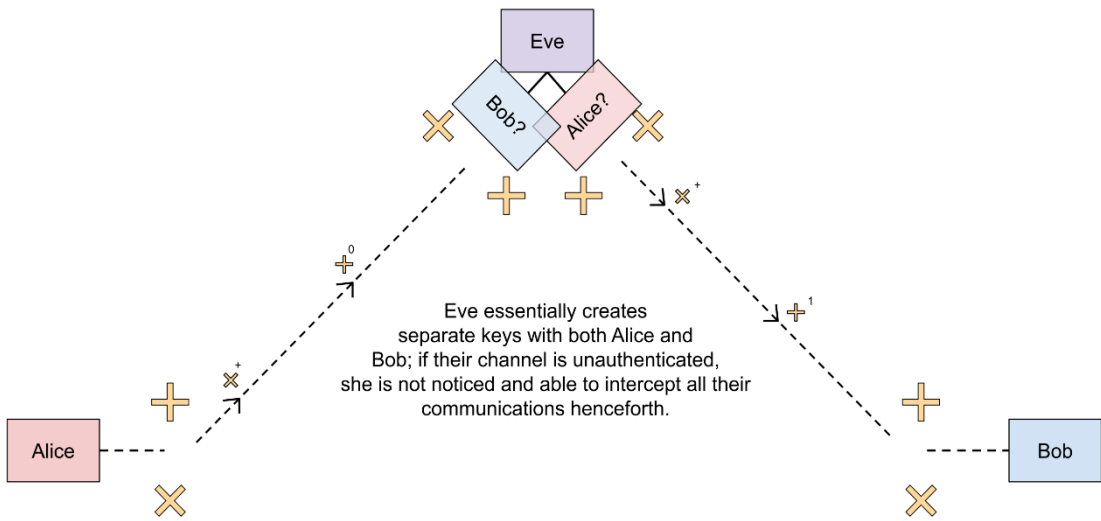


Figure 2. Quantum Key Distribution Without Authentication.

Why then, is quantum key distribution a viable candidate for future encryption?

First, it must be established that QKD and post-quantum cryptography (PQC) are not necessarily competing forms of cryptography. There is no need to choose between one or the other when striving to make the future resistant to quantum hacking. Secondly, quantum key distribution was never meant to be a method for authentication; it is meant to create an undecodable symmetric encryption key, focusing on confidentiality rather than identification. While the absence of authentication is concerning, one must consider that public key infrastructure (PKI) can be combined with PQC methods such as the lattice-structure-based ML-DSA and the hash-based SLH-DSA to authenticate the connection between sender and receiver before QKD is initiated [17,18].

Notably, QKD authentication is usually performed using Wegman-Carter Message Authentication Code (WC-MAC) [28]. First, the sender and receiver (commonly referred to as Alice and Bob respectively) use a predetermined secret key to derive a universally strong hash function and a one-time pad. Then Alice hashes the message she intends to send and proceeds to XOR the hashed message with the one-time pad, creating an authentication tag. Bob creates a tag in the same manner, and if it matches Alice’s, their connection is authenticated. It should be noted that this authentication is done at the end of the QKD process, when Alice and Bob classically exchange information about matching basis states, qubit measurements, and etcetera to verify any eavesdroppers (commonly referred to as Eve) did not intercept their correspondence [28].

One can argue that since such authentication only allows verification at the end of a QKD cycle, WC-MAC increases susceptibility to denial of service attacks, causing problems when urgent information needs to be conveyed securely through a quantum network. However, if tags can be reused without hurting the integrity of security, Alice and Bob can simply authenticate each individual transmission; any qubit transmissions that cannot be authenticated would be deemed invalid, and all others are theoretically guaranteed to be secure [28].

Finally, once an initial successful round of QKD has been achieved and authenticated, Alice and Bob can take a section of the newly generated key and use that as their predetermined secret key when they need to communicate once more. Using this approach and considering that QKD will likely only be used in high security connections, and that the complex infrastructure requires established senders and receivers, QKD networks have the capacity to be majorly independent in

their authentication as long as an initial Wegman-Carter MAC goes well and Alice and Bob stock up on shared secret keys [28].

6.3. Mitigating Reliance on Trusted Nodes Through Quantum Repeaters

Opponents of QKD often point to the fact that while it is a theoretically secure process by the laws of physics, the trusted relays needed to transfer qubits over long distances allow opportunities for insider threats, minimizing security and greatly reducing viable use cases. Due to attenuation, qubits can only travel through optic cables for a couple hundred kilometers at maximum before the signal becomes too weak to read or noise renders the information unreliable [20].

This problem was intended to be solved through trusted nodes. Trusted nodes allow a way to extend the reach of QKD and create quantum networks, making QKD more feasible for large-scale implementation [10].

However, trusted nodes introduce a new fundamental problem of their own. The security of Quantum Key Distribution is attributed to the fact that interception guarantees disruption, so an eavesdropping attempt will always be detected. Since trusted nodes involve classical computing and outsider involvement, the threats it introduces to security cannot be overlooked [29,30]. Listed below are examples of these threats, detailing what aspects of trusted nodes make them inadvisable to implement.

Intentional Insider Threats

Administrators: Their physical access, software access, and monitoring access allow copying of key material, alteration of logging systems, and creation of backdoors – vulnerabilities/imperfections in hardware and equipment functioning that can be exploited by attackers.

Employees: They can possibly leak stored keys & system configurations or install monitoring software to make communications insecure and open up side-channels for attackers.

Supply-Chain: Equipment can be modified before usage to be more susceptible toward hardware attacks.

Unintentional Insider Threats

Accidental Exposure of Key Material: Poor security and data handling procedures can leak the backlog of generated keys, compromising all communications encrypted by them.

In lieu of vulnerable trusted nodes, many proponents of Quantum Key Distribution turn to quantum repeaters as a solution. Quantum repeaters are a concept involving entanglement swapping, in which entangled connections between particles over short distances can be linked in order to create entanglement over longer distances, directly from sender to receiver (A Link Layer Protocol for Quantum Networks). Entanglement swapping is done through Bell State Measurements, working to transfer information over longer distances (MDI-QKD) without needing to trust third party quantum repeaters which relay the message. The connection is theoretically secure even if Eve is the one who performs the Bell State Measurement. This node can also be established through satellites for across ocean communication. Fully Device Independent QKD (DI-QKD) is the final goal, where no piece of machinery in the system needs to be trusted in order for the connection to be secure. This however, requires high-quality entanglement and quantum memories, concepts that cannot be realized in the near future [10,20,31].

6.4. Protecting the Theoretic Security of QKD Against Imperfect Hardware

One of the greatest threats to quantum key distribution is that it relies on hardware. While the theoretically absolute security built on physics rather than math is why many gravitate toward QKD, in actuality, manufacturing and design flaws can allow eavesdroppers to find creative ways to take advantage of practical implementation [8]. These imperfections are often referred to as side-channels, allowing Eve to gain information about the secret key without disturbing the quantum mechanics in play. While there are many proposed methods of quantum key distribution that help eliminate certain side-channels, (e.g. MDI-QKD, DI-QKD, etc.), BB84 protocol is the most widely used and

viable for implementation in current times. This is why it is important to focus on closing these loopholes rather than attempting a complete overhaul of the protocol itself.

This section discusses how to protect against hardware vulnerabilities in QKD, from source, to encoder, to detector.

6.4.1. Source

The main cause of side-channels in the source is imperfect photon generation. In order for QKD to be completely secure, all photon pulses must be random and indistinguishable and Eve must be unable to make a reliable copy of the transmitted photon's state. At high pulse emission rate, the laser doesn't always fully empty between pulses; this means that if photons remain, they can impact subsequent pulses, decreasing randomness and weakening security. Eve can take advantage of this idea so that even if a laser fully empties of the original light source, she can inject a strong laser into the space, causing future photon phases to become correlated to her own phase. This is known as a Laser Injection Attack [36].

Additionally, a strong enough outside laser can damage the functioning of the source laser (Laser Damage Attack), causing optical pulses to have more power and making Alice and Bob's connection vulnerable to Photon Number Splitting (PNS) Attacks; though Eve can't make a copy of the photons Alice sends, she can take advantage of multi-photon pulses enabled by the damaged attenuation to intercept the extra photons without disturbing the Quantum Bit Error Rate (QBER) [37]. Further emphasizing the importance of pulse indistinguishability, QKD systems that use multiple lasers to determine their bases & states of photons are almost guaranteed to have slight differences between the properties of their light pulses, giving Eve more information [51].

In order to ensure a random phase and protect against photon number splitting attacks, the source of a QKD system should have a singular laser paired with phase modulators, be equipped with true random number generation, optical power monitoring, optical isolators, and wavelength filters, and use precisely calibrated decoy states [36,37]. Using a singular laser prevents pulse distinguishability through laser imperfections, and when the phase modulators used to determine bases and states in this situation are coupled with a true RNG, there isn't the problem of nonrandom phase since the phase of leftover photons would be reset with each pulse [36,37]. Optical isolators prevent light from reaching the source, and wavelength filters block certain spectrums of light; together they work to greatly mitigate Laser Injection/Damage Attacks, and optical power monitoring alerts the QKD system when an abnormal amount of light does manage to pass through [36]. Decoy states are created when Alice randomly varies pulse intensity between signal and decoy pulses. The PNS Attack affects these pulses differently, so Alice and Bob will detect unusual statistics and Eve's presence will be revealed [8]. As long as decoy states are precisely calibrated so that they only differ in intensity, Eve will not know which pulse type she is attacking [8,37].

6.4.2. Encoder

Other than simply generating the light pulses needed for communication, it is also essential that the encoder determines pulse phases so that they cannot be intercepted by Eve. BB84 is based on the fact that certain quantum states are difficult to distinguish; this is why the standard bases used are the Computational and Hadamard Bases. The more that a polarization state is shifted from the target state (such as being off base by a couple degrees), the easier it is for Eve to identify them [38]. Eve can induce this vulnerability by changing when a photon reaches the phase modulator, changing the resultant phase by a certain factor δ (known as a Phase Remapping Attack); Eve knows this factor, and using the information she gains, Eve can measure and resend information to Bob without greatly changing the QBER, evading detection [32]. Rather than risk affecting the QBER through this method however, Eve can also opt to gain information about Alice's system through a Trojan Horse Attack, sending light toward Alice's encoding apparatus and analyzing the reflected light for equipment information [26,27].

While small imperfections in bases are unavoidable, as long as the possibility for imperfections is accounted for in security calculations measures can be put in place to set parameters for data privacy. Security proofs demonstrate that cryptographic systems meet their security requirements; as long as quantum state imperfections and outside interference is accounted for in these security calculations, they aren't much of a threat. The approaches to fight against phase-remapping and trojan horse attacks are fairly simple as well, with timing monitoring needed so that Alice and Bob are alerted when a photon has an incorrectly modulated phase and the optical power monitoring and optical isolators discussed previously [26,32,38].

6.4.3. Decoder/Detector

If messing with the preparation and deployment of Alice's quantum states doesn't work, Eve can turn her attention to Bob's receiving setup instead. Since detectors are one of the most complex components in a QKD system, they are often most heavily targeted.

The Trojan Horse Attack can be used on Bob's decoder and the same precautions listed for the encoder should be taken (i.e. optical power monitoring, optical filters), and this is also where we see the effects of the Phase-Remapping attack. Though the Phase-Remapping attack is not directly aimed at Bob's apparatus, one should install timing monitoring to the decoder as well to further security.

BB84 security relies upon Eve being unable to predict Bob's basis measuring states; however, beam splitting is usually used so that these states are measured randomly, and slight variations in pulse properties can bias Bob's system toward a certain detector. For example, a slightly higher or lower wavelength can make the photon prefer measurement of one basis state over the other [33]. Eve can use this to her advantage, manipulating the wavelength of a photon she sends out so that Bob's beam splitter is biased toward the same basis state she used to measure. Efficiency Mismatch Attacks depend on detectors being biased toward a particular quality of the signals Alice sends, such as pulse timing in Time-Shift Attacks and incidence angles when dealing with polarized states [34,35]. By manipulating these properties, Eve can increase the likelihood that Bob measures states in the same basis she did, decreasing the QBER and hiding her interference. Eve can also induce detector bias through Dead-Time attacks and After-Gate attacks, where she uses the inactive time after one of Bob's detectors has gone off to her advantage. QKD systems commonly use avalanche photodiodes (APDs) or single photon avalanche detectors (SPADs) in order for Bob to receive Alice's signals; since a detector can't process signals for a couple microseconds after being activated, Eve can take advantage of this reset period to resend her intercepted photons to Bob at a time that almost guarantees only one of the detectors will be working (the Dead-Time attack) [39]. After-Gate attacks involve Eve's faked states reaching Bob's detector(s) during dead-time, at an intensity so that Bob can only receive the photon if he is measuring in the same way Eve did [40]. APDs can also be saturated with photons in a Detector Blinding attack, turning them into classical detectors, unable to detect individual photons; Eve can then ensure she knows the secret key by measuring in a random basis state and resending the signal at an intensity for which Bob's detector will only "click" (detect the photon) if it measures in the same basis Eve did [25]. All these attacks are based on ensuring that Eve's basis states match with Bob's so that the QBER isn't noticeably affected and Eve can safely intercept the secret key information.

In order to prevent manipulation of detectors by Eve, one must remove beam splitters and the capability of bias they introduce. What better way to do this than removing the need for beam splitters as a whole and preventing Eve from having access to detector choice? Rather than using beam splitters, there are proposed methods of QKD that instead compel Bob to utilize a private Quantum RNG (QRNG) and mirror to determine which basis received photons are directed to [41]. This system eliminates much of the danger of Eve manipulating detectors, making wavelength-based attacks, efficiency mismatch attacks, time-shift attacks, dead-time attacks, after-gate attacks, and detector blinding attacks largely ineffective. The remaining susceptibility can be accounted for in the security proof.

Not all problems can be solved by simply redesigning an aspect of the system however. Superlinearity attacks happen when Eve capitalizes on the non-linear nature of detectors — the fact that detector probability of clicking increases exponentially with number of photons — so that she can resend her measurement of Alice's photons with a few photons per pulse, increasing the likelihood that a detector will click only if Bob's detector measured in the same basis as her [42]. Not many solutions for this are proposed except for creating detectors which have more linear click rates, installing optical power monitoring to judge pulse intensity, and simply accounting for superlinear tendencies in security proofs.

APDs themselves are not perfectly efficient, so some energy is released through photons, enabling Backflash Attacks. If detectors differ in the properties of their photon backflash, Eve may be able to differentiate which detector clicked, gaining some knowledge about the key [43]. Detectors can also differ in the properties of their response times, giving Eve a similar amount of knowledge on the key composition [45]. Backflash Attacks can be counteracted through optical filters and optical circulators that work to block and reabsorb the excess light and the timing side-channel can be dealt with by equalizing detector timing and rounding detection timestamps before transmitting them across classic channels [44,45].

To manage the majority of these attacks, these are all the precautions that should be taken against hardware flaws in classic QKD:

6.4.4.1. Source Security:

- single-laser system
- active phase randomization (through phase modulator)
- true QRNG
- indistinguishable decoy states
- optical power monitoring
- cascaded optical isolators
- wavelength filters

6.4.4.2. Encoder Security:

- electro-optic modulators for active state preparation and basis selection
- timing monitoring
- precise calibration of optical components

6.4.4.3. Detector/Decoder Security:

- optical circulators (mitigates detector backflash)
- precise calibration of components (specifically equalizing detector timing)
- reduced timestamp precision in classical channels

6.4.4.4 Security Proof Considerations:

- imperfect polarization/state preparation
- imperfect phase randomization
- detector efficiency mismatch
- superlinearity of detectors
- preciseness of calibration (influence on creation of decoy states, detector differences, etc.)
- electro-optic modulator timing (effectiveness of phase-remapping attack)

6.4.4.5 Important in Design:

- avoid multiple lasers during state preparation
- avoid beam splitters; create systems with active, randomized basis selection

- attempt identical detectors through careful calibration

Relying on physical devices for basis randomization is one of the most targeted flaws of QKD systems. For QKD in the near future, utilizing true quantum random number generators and electro-optic modulators instead of beam splitters and separate lasers eliminates a large number of side channel attacks [38,41].

Though it is of course more preferable to prevent attacks rather than mitigate them; this is why Measurement Device Independent QKD is the ideal long term goal and research into entanglement swapping devices should be prioritized [8,31].

6.5. Prioritizing Scalability and Addressing the Costs of QKD

Even after solving the weak security points of quantum key distribution, the cost it would take to implement this technology is often alleged to be greater than the benefit it affords. But this scenario assumes that QKD is adopted as the main form of encryption across the world. QKD is not currently realistic for an entire network overhaul; it instead aims to offer critical infrastructure a long term, safe way to encrypt their data that is not based on currently unsolved math problems. These critical sectors include national security, finance, and healthcare, where data is too powerful to be guarded only by difficult math; the safety guaranteed when quantum key distribution and post-quantum cryptography work in tandem outweighs the cost of implementation [10,15].

The current concerns about costs stem mainly from the specialized detectors, dedicated fibers, trusted-node infrastructure, need for maintenance, and installation of all hardware components.

For some concrete examples from the Austrian Institute of Technology (AIT):

- Discrete Variable QKD when distributed from AIT costs roughly \$140,000–\$220,000 per fiber link [46].
- Continuous Variable QKD is expected to drop from roughly \$180,000–\$200,000 per fiber link
- One AIT deployment involving entangled photon communication costed around \$275,000
- When asked about an MDI-QKD system they worked on, it was quoted to cost around \$410,000

When presented with just the numbers, it seems like QKD is far too expensive for its worth, but one must consider how much nations spend on average for their security. The U.S. planned to spend \$75 billion on Information Technology and Cybersecurity Funding in 2025, showing that when it comes to government security, cost should not be considered a larger factor than effectiveness. If countries and businesses are willing to spend millions and billions on security, they should invest in the best security available [47].

Governing bodies like the European Union and countries like South Korea have already started putting money toward implementation of quantum technology into their communication systems; with the EU's EuroOCI initiative having 193 million euro invested and South Korea projected to spend 2.6 billion dollars on quantum infrastructure by 2035. Though QKD may currently be pricey, investment into advancing infrastructure and deploying QKD systems in the real world is essential for it to move toward a reasonable price over time [48,49].

As quantum computers become more advanced and previously unsolvable math problems like prime factorization gain polynomial time quantum solutions, organizations begin to see the danger their data is in and more efforts are made to cheapen the cost of QKD without compromising its effectiveness.

One of the most promising avenues to explore when considering scalability is the prospect of integrated photonics. Integrated photonics offers the possibility of encoding QKD systems into microchips, allowing simpler and less costly installation. Most proposed chip structures are silicon-based and, notably, prefer time bins to distinguish qubits rather than polarization; this works by dividing one pulse into two qubits with differing time slots and modulating the phase of both bits —

from then on, the detecting and decoding process is similar. However, classic BB84 protocol and MDI-QKD can also be carried out using chips [21,50].

Currently, no chips have been confirmed to successfully encompass all of a QKD system (source, encoder, detector, and decoder), but multiple have managed to combine some of these components, creating transmitter chips and receiving chips [22,23].

Approaching QKD with silicon chips and novel protocols, though it invites new security concerns we have not covered, also invites new opportunities for mass manufacturing and market competition which will ultimately push QKD to optimization, convenience, and practical implementation.

6.6. Creating a Feasible Framework for Quantum-Secure Communication Systems

Though people often criticize quantum key distribution for its lack of authentication, implementation costs, transmission distance, and hardware vulnerabilities, these flaws lie in current technological limitations and misunderstanding of QKD's purpose rather than in the underlying principles themselves. Authentication is a challenge QKD was never meant to solve; classical post-quantum cryptography is meant to handle authentication when sharing a key, and while it does not replace quantum key distribution, it does allow a guarantee that the secure key is between the right sender and receiver. The implementation costs are projected to decrease with time, market competition, and integrated photonics, and transmission distance is lengthened by improved attenuation, trusted nodes, and quantum repeaters. Hardware vulnerabilities already have many documented fixes as discussed in Section 6.4, and new QKD protocols and set-ups are constantly being created so that the future of these systems seems to be malleable. So where should we go from here? [17,18,20,21].

Rather than replacing all network infrastructure right away, it makes more sense to first replace critical infrastructure for which the added cost of early QKD implementation is outweighed by the danger of "Harvest Now, Decrypt Later" attacks compromising important data. Sectors such as healthcare, finance, and national security fit in this category since data breaches can lead to patient injuries, financial insecurity leads to fraud, and leaking national secrets risks diplomatic relationships. These early QKD deployments should take the precautions listed near the end of Section 6.4, as BB84 QKD is currently the most feasible way to implement quantum infrastructure. Looking toward the future however, the current systems handling quantum key distribution should be evolved through integrated photonics, with much focus placed on refining detectors on receiving chips since their complex structure and many vulnerabilities require extra attention. As quantum networking and the efficiency of QKD chips improves, quantum key distribution can gradually become commercially available, with the chips potentially allowing integration through existing wiring networks without necessitating an overhaul of web architecture. The technology needed for Measurement Device Independent QKD and Device Independent QKD (e.g. devices capable of keeping reliable quantum memories, entanglement assurance, etc.) should be researched and tested in the meantime, but the ability to carry out QKD without trusted devices is better viewed as a long term goal rather than a necessity for QKD adoption [20,21,31,41].

The emergence of quantum computers brought about a new era of data processing in society — it also brought about a new era of hacking. The field of cryptography especially was completely upended, with secure protocols like RSA, used for years of encrypting, being rendered insecure by quantum algorithms. Now, cryptography must also enter the quantum realm. While no one technology can ensure perfect security, quantum key distribution's information-theoretic security working in tandem with post-quantum cryptography's computationally secure authentication is most likely the closest option. Though progress will take time, developing and adopting quantum key distribution is an important step to a truly secure society [2,8,17,18].

5. Conclusions

The emergence of quantum computers brought about a new era of data processing in society — it also brought about a new era of hacking. The difficult mathematical problems that common encryption algorithms such as RSA, ECC, and symmetric encryption rely on are often threatened by quantum computing. Despite the fact that quantum computers are still developmental and not yet widespread, "harvest now, decrypt later" strategies show how data today is already at risk of this quantum threat; if sectors such as health, finance, and national security are compromised, the effect on society would be devastating. Considering this, cybersecurity must stop relying solely on computational difficulty and instead enter the quantum realm itself.

Quantum Key Distribution is the most viable foundation for the transition into physics-based security. Since it is built on quantum phenomena such as the no-cloning theorem and measurement disturbance, it can detect eavesdropping and establish secure shared keys. Without the restraints of purely mathematical encryption, QKD offers a higher level of long-term security. That being said, QKD is complex, and its theoretical absolute security cannot be perfectly put into practice; factors such as authentication, transmission distance, hardware vulnerabilities, infrastructure costs, and scalability still hinder its widespread adoption. Regardless, these imperfections can be accounted for through continued development in QKD technologies (e.g. quantum repeaters, integrated photonics, etc.), physical countermeasures (e.g. optical isolators, single-laser transmission, etc.), and collaboration with post-quantum cryptography. In the long term, Measurement Device Independent QKD and similar protocols may be capable of mitigating almost all the security risks caused through hardware limitations, and chip-based QKD would allow many more opportunities for scalability if it were implemented.

The research concludes that the most realistic path toward quantum-secure communication is not a complete overhaul of existing infrastructure, but a gradual transition that considers practicality and hybrid implementation to protect against HNDL strategies while still moving toward the goal of completely quantum-secure communication. Initial deployment of quantum-resistant technologies should consist of post-quantum cryptography, which can provide authentication and protection while scalable QKD is in development and the current form of QKD is implemented into facilities that need the most sensitive communications, meaning national security, healthcare, and finance, where long-term data compromise is most dangerous. As QKD chips develop, becoming more efficient and affordable, quantum-secure networks can extend their reach past high-security applications, using existing networks of fiber-optic cable to provide safer communications for everyone. In the long term, protocols like Measurement Device Independent QKD and possibly even Device Independent QKD could develop to the point where the need for trusted nodes is eliminated, and insider attacks aren't a significant threat. Though progress will take time, developing and adopting quantum key distribution early is an essential step to a secure society.

Abbreviations

The following abbreviations are used in this manuscript:

QKD	Quantum Key Distribution
RSA	Rivest-Shamir-Adleman
ECC	Elliptic-curve cryptography
AES	Advanced Encryption Standard
PQC	Post quantum cryptography
HNDL	Harvest now, Decrypt later
NIST	National Institute of Standards and Technology
APDs	Avalanche photodiodes
SPADs	Single photon avalanche detectors

References

- Bernstein, D.J.; Lange, T. Post-quantum cryptography. *Nature* 2017, 549, 188–194.
- Shor, P.W. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*; 1994; pp. 124–134.
- Grover, L.K. A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*; 1996; pp. 212–219.
- Mahajan, P. A study of encryption algorithms AES, DES and RSA for security. *Glob. J. Comput. Sci. Technol.* 2013, 13, 1–9.
- Mahalle, V.S.; Shahade, A.K. Enhancing the data security in cloud by implementing hybrid (RSA & AES) encryption algorithm. In *Proceedings of the 2014 International Conference on Power, Automation and Communication (INPAC)*; 2014; pp. 146–149.
- National Institute of Standards and Technology. Post-quantum cryptography | CSRC. n.d.
- Vaishnavi, A.; Pillai, S. Cybersecurity in the quantum era—A study of perceived risks in conventional cryptography and discussion on post-quantum methods. *J. Phys. Conf. Ser.* 2021, 1964, 042002.
- Pirandola, S.; Andersen, U.L.; Banchi, L.; et al. Advances in quantum cryptography. *Adv. Opt. Photonics* 2020, 12, 1012–1236.
- Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*; 1984; pp. 175–179.
- Mehic, M.; Niemiec, M.; Rass, S.; et al. Quantum key distribution: A networking perspective. *ACM Comput. Surv.* 2020, 53, 96.
- Liao, S.K.; Cai, W.Q.; Liu, W.Y.; et al. Satellite-based entanglement distribution over 1200 kilometers. *Science* 2017, 356, 1140–1144.
- Chen, Y.A.; Zhang, Q.; Chen, T.Y.; et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature* 2021, 589, 214–219.
- Horodecki, M.; Horodecki, P. Detecting quantum entanglement. *Phys. Lett. A* 2002, 283, 1–7.
- Deng, D.-L.; Li, X.; Das Sarma, S. Quantum entanglement in neural network states. *Phys. Rev. X* 2017, 7, 021021.
- National Security Agency. Quantum key distribution (QKD) and quantum cryptography (QC). n.d.
- Khalil, M. Compromised devices statistics 2024–2025: Costs, attacks, trends. *DeepStrike*, 18 December 2025.
- National Institute of Standards and Technology. Module-Lattice-Based Digital Signature Standard; FIPS PUB 204; U.S. Department of Commerce, National Institute of Standards and Technology, 2024.
- National Institute of Standards and Technology. Stateless Hash-Based Digital Signature Standard; FIPS PUB 205; U.S. Department of Commerce, National Institute of Standards and Technology, 2024.
- Ekert, A.K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* 1991, 67, 661–663.
- Huttner, B.; Alléaume, R.; Diamanti, E.; et al. Long-range QKD without trusted nodes is not possible with current technology. *npj Quantum Inf.* 2022, 8, 108.
- Liu, Q.; Huang, Y.; Du, Y.; et al. Advances in chip-based quantum key distribution. *Entropy* 2022, 24, 1334.
- Paraíso, T.K.; De Marco, I.; Roger, T.; et al. A modulator-free quantum key distribution transmitter chip. *npj Quantum Inf.* 2019, 5, 42.
- Beutel, F.; Gehring, H.; Wolff, M.A.; Schuck, C.; Pernice, W. Detector-integrated on-chip QKD receiver for GHz clock rates. *npj Quantum Inf.* 2021, 7, 40.
- Huttner, B.; Imoto, N.; Gisin, N.; Mor, T. Quantum cryptography with coherent states. *Phys. Rev. A* 1995, 51, 1863–1869.
- Lydersen, L.; Wiechers, C.; Wittmann, C.; Elser, D.; Skaar, J.; Makarov, V. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photonics* 2010, 4, 686–689.
- Gisin, N.; Fasel, S.; Kraus, B.; Zbinden, H.; Ribordy, G. Trojan-horse attacks on quantum-key-distribution systems. *Phys. Rev. A* 2006, 73, 022320.
- Jain, N.; Anisimova, E.; Khan, I.; et al. Trojan-horse attacks threaten the security of practical quantum cryptography. *New J. Phys.* 2014, 16, 123030.

28. Price, A.B.; Rarity, J.G.; Erven, C. A quantum key distribution protocol for rapid denial of service detection. *EPJ Quantum Technol.* 2020, 7, 8.
29. Piétri, Y.; Verdier, P.-E.; Lacour, B.; et al. Quantum key distribution with efficient post-quantum cryptography-secured trusted node on a quantum network. *arXiv* 2025, arXiv:2504.01454.
30. International Telecommunication Union. Recommendation ITU-T X.1710: Security Framework for Quantum Key Distribution Networks; International Telecommunication Union, 2020.
31. Dahlberg, A.; Skrzypczyk, M.; Coopmans, T.; et al. A link layer protocol for quantum networks. In *Proceedings of the ACM Special Interest Group on Data Communication (SIGCOMM '19)*; 2019; pp. 159–173.
32. Fung, C.-H.F.; Qi, B.; Tamaki, K.; Lo, H.-K. Phase-remapping attack in practical quantum-key-distribution systems. *Phys. Rev. A* 2007, 75, 032314.
33. Li, H.-W.; Wang, S.; Huang, J.-Z.; et al. Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources. *Phys. Rev. A* 2011, 84, 062308.
34. Zhao, Y.; Fung, C.-H.F.; Qi, B.; Chen, C.; Lo, H.-K. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Phys. Rev. A* 2008, 78, 042333.
35. Sajeed, S.; Chaiwongkhot, P.; Bourgoin, J.-P.; Jennewein, T.; Lütkenhaus, N.; Makarov, V. Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch. *Phys. Rev. A* 2015, 91, 062301.
36. Lovic, V.; Marangon, D.G.; Smith, P.R.; Woodward, R.I.; Shields, A.J. Quantified effects of the laser-seeding attack in quantum key distribution. *Phys. Rev. Appl.* 2023, 20, 044005.
37. Huang, A.; Li, R.; Egorov, V.; Tchouragoulov, S.; Kumar, K.; Makarov, V. Laser-damage attack against optical attenuators in quantum key distribution. *Phys. Rev. Appl.* 2020, 13, 034017.
38. Xu, F.; Wei, K.; Sajeed, S.; et al. Experimental quantum key distribution with source flaws. *Phys. Rev. A* 2015, 92, 032305.
39. Weier, H.; Krauss, H.; Rau, M.; Fürst, M.; Nauerth, S.; Weinfurter, H. Quantum eavesdropping without interception: An attack exploiting the dead time of single-photon detectors. *New J. Phys.* 2011, 13, 073024.
40. Wiechers, C.; Lydersen, L.; Wittmann, C.; et al. After-gate attack on a quantum cryptosystem. *New J. Phys.* 2011, 13, 013043.
41. Stipčević, M. Enhancing the security of the BB84 quantum key distribution protocol against detector-blinding attacks via the use of an active quantum entropy source in the receiving station. *Entropy* 2023, 25, 1518.
42. Lydersen, L.; Jain, N.; Wittmann, C.; et al. Superlinear threshold detectors in quantum cryptography. *Phys. Rev. A* 2011, 84, 032320.
43. Kurtsiefer, C.; Zarda, P.; Mayer, S.; Weinfurter, H. The breakdown flash of silicon avalanche photodiodes—Back door for eavesdropper attacks? *J. Mod. Opt.* 2001, 48, 2039–2047.
44. Meda, A.; Degiovanni, I.P.; Tosi, A.; Yuan, Z.; Brida, G.; Genovese, M. Quantifying backflash radiation to prevent zero-error attacks in quantum key distribution. *Light Sci. Appl.* 2016, 6, e16261.
45. Lamas-Linares, A.; Kurtsiefer, C. Breaking a quantum key distribution system through a timing side channel. *Opt. Express* 2007, 15, 9388–9393.
46. Piller, E.; Schölnast, H. QKD. In *Data Encryption at the Intersection of Mathematics and Physics*; Springer, 2026.
47. Executive Office of the President of the United States, Office of Management and Budget. Research and Development; U.S. Government Publishing Office, 2024.
48. European Commission. Quantum communication infrastructure (EuroQCI). European Health and Digital Executive Agency, n.d.
49. Kim, J.-W. S. Korea to invest \$2.6 bn in quantum technology by 2035. *KED Global* 2023.
50. Wang, J.; Hanel, J.; Jiang, Z.; et al. Time-bin encoded quantum key distribution over 120 km with a telecom quantum dot source. *Light Sci. Appl.* 2026, 15, 126.
51. Ko, H.; Choi, B.-S.; Choe, J.-S.; Kim, K.-J.; Kim, J.-H.; Youn, C.J. Critical side channel effects in random bit generation with multiple semiconductor lasers in a polarization-based quantum key distribution system. *Opt. Express* 2017, 25, 20045–20055.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.