

Rose-Hulman Institute of Technology

Rose-Hulman Scholar

Mathematical Sciences Technical Reports
(MSTR)

Mathematics

5-23-2023

Human and Technical Factors in the Adoption of Quantum Cryptographic Algorithms

Alyssa Pinkston

Rose-Hulman Institute of Technology, PINKSTA1@rose-hulman.edu

Follow this and additional works at: https://scholar.rose-hulman.edu/math_mstr



Part of the [Graphics and Human Computer Interfaces Commons](#), [Information Security Commons](#), [Quantum Physics Commons](#), and the [Theory and Algorithms Commons](#)

Recommended Citation

Pinkston, Alyssa, "Human and Technical Factors in the Adoption of Quantum Cryptographic Algorithms" (2023). *Mathematical Sciences Technical Reports (MSTR)*. 183.

https://scholar.rose-hulman.edu/math_mstr/183

This Article is brought to you for free and open access by the Mathematics at Rose-Hulman Scholar. It has been accepted for inclusion in Mathematical Sciences Technical Reports (MSTR) by an authorized administrator of Rose-Hulman Scholar. For more information, please contact ligget@rose-hulman.edu.

Human and Technical Factors in the Adoption of Quantum Cryptographic Algorithms

Alyssa Pinkston

23 May 2023

Contents

1	Introduction	1
2	Background	1
3	List of Symbols	2
4	BB84	3
5	BB84 with noise	5
6	Technical Attacks	7
7	Key Infrastructures	9
8	Security Models	10
9	Human Error	13
10	Cybercrime	14
11	QKD Landscape	15
12	Research Methods	19
13	Conclusion	23
14	Appendix	26

Abstract

The purpose of this research is to understand what factors would cause users to choose quantum key distribution (QKD) over other methods of cryptography. An Advanced Encryption Standard (AES) key can be exchanged through communication using the Rivest, Shamir, Adleman (RSA) cryptographic algorithm, QKD, or post-quantum cryptography (PQC). QKD relies on quantum physics where RSA and PQC use complex mathematics to encrypt data. The BB84 quantum cryptographic protocol involves communication over a quantum channel and a public channel. The quantum channel can be technically attacked by beamsplitting or intercept/resend. QKD, like other forms of cryptography, is vulnerable to social attacks such as industrial espionage. QKD products can transmit over maximum distances ranging from 40 km up to 150 km with key rates as low as 1.4 kb/s up to at least 300 kb/s. A survey and focus group discussion with a defense contracting company revealed that while nobody fully trusts current security systems, they are more concerned about social engineering attacks before attacks on cryptography. The company is not interested in implementing QKD unless the range capabilities are improved or there is regulation requiring them to use it.

1 Introduction

From secret messages scribbled on scraps of paper, through world wars, to mechanical and digital systems, there has been an arms race between cryptographers and cryptanalysts surrounding the distribution of sensitive information. Cryptographers design and implement systems to encrypt data so that it would be difficult to decrypt by anyone who is not the intended recipient. Cryptanalysts intercept encrypted data and work to uncover the hidden information without having the necessary information to perform the intended conventional decryption. Cryptographers now are looking towards QKD as the next step in this arms race. QKD relies on quantum physics, making it resilient against immense computing power.

Two actors, Alice and Bob, want to exchange secret messages. To do so, they use quantum mechanics to share a key. If this QKD is successful, the key is privy to Alice and Bob alone. In this scenario, Alice is the transmitter and Bob is the receiver. During the transmission, there may be an eavesdropper, Eve. Eve is listening in with the hopes that she can glean some or all of the key and therefore make Alice and Bob's secret messages not so secret. Alice and Bob are wary of Eve, so they take steps to circumvent eavesdropping and ensure the privacy of their key.

2 Background

The current state of the cryptography arms race uses RSA, which is a method of public key asymmetric cryptography that allows two actors to encrypt their communication without having an established shared key [1]. In asymmetric cryptography, an individual has two keys that go together. Of these keys, the public key is available to everyone while the private key is only available to the owner of the key pair. Anyone can use the public key to encrypt a message to that individual, but the private key is required to decrypt the message. If Eve has a private key that is not hers, then she can decrypt messages that were not intended for her. Alice can use Bob's public key to encrypt a message to him, which he can then decrypt with his private key. Often, public key

communication is a tool to be used in combination with AES, where RSA is used initially to share an AES key [1].

AES is a method of symmetric cryptography where the two actors have an agreed upon secret key they use to encrypt and decrypt the data being sent between them [1]. As opposed to public key cryptography, symmetric key cryptography uses a single key, known only by the sender and recipient, to encrypt and decrypt data. To exchange information in this way, the users must have communicated beforehand to establish their shared secret key. RSA and QKD are both ways in which Alice and Bob can exchange an AES key.

Another way to exchange an AES key is by using PQC, which is another public key system with public key infrastructure. Using more complex ciphers make this method of cryptography safer against attacks by quantum computers [2]. Against regular computers, PQC is slower than RSA and requires more bandwidth, but provides the same level of security as RSA [2]. PQC does not require the use of any new hardware [2].

The purpose of this research is to consider advantages and disadvantages of these systems, and understand what factors would cause users to choose RSA, PQC, or QKD for the purpose of exchanging an AES key. Where other cryptographic systems rely on complex mathematics, quantum cryptography uses physics to encrypt data. Because of this, an AES encryption key exchanged using QKD is less susceptible to compromise from a technical attack by a malicious actor than one exchanged with RSA, depending on the decisions made by the humans using the system. Technical attacks are more successful against PQC than QKD. With the introduction of quantum computers capable of breaking RSA, the benefit of QKD becomes even more important.

To understand the advantages and disadvantages of these systems, this paper will cover the technical background behind QKD, including technical attacks against the system. With the quantum background established, there will be an explanation of public and quantum key infrastructures, followed by security tradeoffs and attack models, use cases for various systems, and a discussion of human error. Cybercrime statistics and an overview of QKD products on the market will be given. Next, there will be research methods, results, and conclusions, which will be related back to the hypothesis of this research.

3 List of Symbols

f is the fraction of the beam Eve diverts in a beamsplitting attack

k is the upper bound on the bits that Eve knows

λ is the probability that Eve has been eavesdropping on the transmission

m is the number of subsets of bit locations in the raw key

μ is the number of bits per pulse (pulse intensity)

N is the number of bits in the raw key after the first phase

n is the number of bits in reconciled string (after the third phase)

p is the error rate

ρ is the fraction of the raw key that Eve knows s is an arbitrary security parameter

t is the number of errors in the quantum transmission

4 BB84

Understanding the quantum cryptographic protocol invented by Bennett and Brassard in 1984, known as BB84, alone and with the introduction of noise is useful to determine how it can be attacked and where human actors may make mistakes. BB84 occurs in one phase over a quantum channel and two phases over a public channel. A quantum channel is a communication pathway over which quantum data can be transmitted, where Alice sends data and Bob reads out data. The medium for a quantum channel transmission may be fiber optic cable or free space [3]. A public channel can be any standard method of communication, such as the internet.

BB84 makes use of two quantum alphabets. A quantum alphabet is a system used to associate bit values with a particular quantum state [3]. BB84 uses both a circular polarization quantum alphabet and a linear polarization quantum alphabet [3]. In a circular polarization quantum alphabet, a 1 corresponds to a clockwise orientation $|\curvearrowright\rangle$ and a 0 corresponds to a counterclockwise orientation $|\curvearrowleft\rangle$. In a linear polarization quantum alphabet, a 1 is vertical $|\updownarrow\rangle$ and a 0 is horizontal $|\leftrightarrow\rangle$. The incompatibility of these quantum alphabets requires the recipient of the quantum transmission to choose a basis in which to measure the transmitted bit.

Symbol	Bit
$ \curvearrowright\rangle$	1
$ \curvearrowleft\rangle$	0

Table 1: Circular Polarization Quantum Alphabet A_{\odot} [3]

Symbol	Bit
$ \updownarrow\rangle$	1
$ \leftrightarrow\rangle$	0

Table 2: Linear Polarization Quantum Alphabet A_{\boxplus} [3]

4.1 Quantum Channel

Over the quantum channel, Alice transmits a string of bits, with each bit randomly encoded with either circular or linear polarization. For each of these bits, Bob chooses randomly to measure either circular or linear.

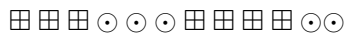
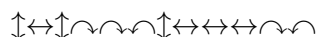
Alice's string:
101100101111

Alice encodes:

$\boxplus \odot \odot \boxplus \boxplus \odot \boxplus \boxplus \odot \odot \odot \boxplus$

Alice transmits:

$\updownarrow \curvearrowright \curvearrowright \updownarrow \leftrightarrow \updownarrow \leftrightarrow \curvearrowright \curvearrowright \updownarrow$

Bob measures:

 Bob decodes:

 Bob's string:
 101110100010

If Alice and Bob choose the same alphabet, Bob receives the correct bit. However if they choose opposing alphabets, based on the Heisenberg uncertainty principle, Bob has a fifty percent chance of receiving the correct bit. The Heisenberg uncertainty principle prevents Bob from predicting with any certainty the value of the bit [3].

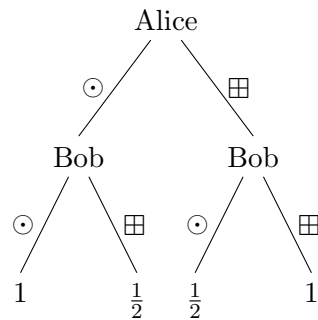


Figure 1: Probability of Bob receiving the correct bit

When Bob measures in the incorrect basis, he will receive randomly either a 1 or 0, which may or may not be the same bit Alice sent.

4.2 Public Channel

The public channel communication occurs in two phases. The purpose of this public channel communication is to eliminate errors between the string that Alice sent and what Bob received and to detect eavesdropping from Eve.

4.2.1 Phase 1

The first phase of communication on the public channel is for Alice and Bob to compare their measurement systems and remove any bits from the transmitted string where they used mismatching measurements [3]. The result from this is a string of with N bits, known as the raw key [3].

4.2.2 Phase 2

The second phase is to perform error detection to check for interference from Eve. Alice and Bob have an agreed subset of bit locations in their raw key that they select and compare. After they compare, all the bits from that subset are removed from the string since they have been broadcast publicly [3]. If any of the bits in these subsets do not agree, it can be concluded that Eve has been listening in on some of the transmission. In this case, they can choose to start over or move on

knowing that Eve knows some part of their shared bit string.

If the compared bits agree, then Eve may have been listening to the transmission and has avoided detection, or she may not have been listening to the transmission at all. Alice and Bob can predict the probability of Eve avoiding detection based on the odds that she is eavesdropping, λ , and the number of subsets of bit locations they choose to compare, m , for a probability of $(1 - \frac{\lambda}{4})^m$ [3]. They can manipulate the value of m until they determine the probability of eavesdropping is sufficiently low.

5 BB84 with noise

In practical application, realistic factors such as the equipment Alice and Bob are using may introduce error into the system that Eve is not responsible for. The communication over the quantum channel stays the same as in BB84 without noise.

With the introduction of noise, the public channel communication changes from two phases to four phases: extracting the raw key, estimating error, extracting the reconciled key, and performing privacy amplification.

5.1 Phase 1

The first phase on the public channel is the same as in BB84 without noise where Alice and Bob compare measurement systems and get rid of all bits from the string where their measurement systems do not agree.

5.2 Phase 2

The second phase involves error estimation. Alice and Bob agree on a maximum error rate to tolerate [3]. They compare a random sample from the string and determine the error rate in that sample, and then throw out all bits in the sample since they have been publicly broadcast [3]. If the error rate from the sample exceeds the maximum error rate, they choose to throw out the string entirely and start over.

5.3 Phase 3

The third phase tries to ensure Bob's bit string agrees with the bit string Alice sent and eliminate remaining errors. Alice and Bob choose blocks, which are subsets of a fixed length, to pull from the string and they compare the parity of each block [3]. The parity value they compare is either 0 or 1, determined by taking the sum of the bits in the string modulo two.

If the parities match, Alice and Bob throw out the last bit in the block to reintroduce ambiguity [3]. By removing a bit from the string, the parity will change if that bit is a 1. For example, if a string is 011001 the parity is 1; when the last bit is removed to make the string 01100 the parity is now 0. Otherwise if the bit removed is a 0 then the parity will not be changed. Now the parity of the block is no longer known.

If the parities disagree, Alice and Bob perform binary search on their blocks, comparing parities, still throwing out a bit after each comparison, until they find the bit that is the source of the error which can then be removed [3].

For example:

Alice's block is 01011001
Bob's block is 11011001

The parity of Alice's block is 0, and the parity of Bob's block is 1. When they compare, they realize that there is an error in one of their strings. They perform the first step of a binary search and split their strings in half:

Alice has 0101 and 1001
Bob has 1101 and 1001

They compare the second half of their strings and the parities match, so they know the error is not in that part of the block. They discard the last bit of this section so the parity is no longer known. On the first half of their strings, the parities do not match, so they bisect the string again:

Alice has 01 and 01
Bob has 11 and 01

They repeat the comparison of the second part of this section, and the parities match, so they discard the last bit. Then they compare the parities of the first part of this section and find that the parities do not agree. They split the string again:

Alice has 0 and 1
Bob has 1 and 1

They compare the second part and the parities match and since it is only one bit, that is the bit they discard. Finally they compare the final bit and find that is the bit causing the error, and they discard it as well. They repeat this process on other blocks they extract from the bit string. The final result from these comparisons is known as the reconciled key. In this example, the reconciled key is:

Alice's key 0100
Bob's key 0100

There is a possibility that the subset they choose will have matching parities despite containing errors. An example of this is a scenario where Alice has 0110 and Bob has 0000. In this case, the parities match, so the errors will get through undetected.

5.4 Phase 4

The fourth and final phase over the public channel is known as privacy amplification. If n is the number of bits in the reconciled key, k is an upper bound on the number of bits of information Eve knows as explained in section 6.3, and s is an arbitrary security parameter, $n - k - s$ random subsets are pulled out of the reconciled key [4]. So, if the reconciled key contains 100 bits and Eve knows up to 30 of those bits, and Alice and Bob have chosen a security parameter of 20, $100 - 30 - 20 = 50$, 50 subsets are chosen from the reconciled key. The parities of each of these subsets combine to become the final secret key.

6 Technical Attacks

To eavesdrop on Alice and Bob's communication over the quantum channel, there are two primary attack methods Eve can leverage. The attacks are known as beamsplitting and intercept/resend. When Alice transmits a bit, she sends a light pulse along the quantum channel which may be composed of multiple photons, generally up to two photons per pulse, and μ is the number of photons in each of these pulses of light [5].

6.1 Beamsplitting

Beamsplitting is an attack where Eve splits off part of the beam to herself, and allows the rest to go along to Bob. She can do so by using a device such as a partly-silvered mirror, causing her to receive a fraction f of the transmitted photon beam while the rest continues to Bob [5]. If there are multiple photons per pulse, Eve can successfully detect one with probability $f\mu$ and let the rest, $1 - f$, go on to Bob [5]. If there are N bits in the raw key and the conservative assumption is made that $f = 1$, and if μ is the probability of Eve detecting a photon, Eve learns $N\mu$ bits. To account for error, Alice and Bob include a 5σ standard deviation $5\sqrt{N\mu(1-\mu)}$ [5]. Combining these parts, Alice and Bob determine Eve learns fewer than $N\mu + 5\sqrt{N\mu(1-\mu)}$ of the transmitted bits [5].

If Eve splits off a large enough fraction of the beam that Bob no longer receives a photon, or if Bob receives a photon but measures incorrectly, it is detected when Alice and Bob perform their public channel communication, and the bit does not become a part of their shared string. If Bob does receive the remainder of the beam and measures correctly, then the bit remains in their string.

If Eve is capable of postponing measurement of her photon until after Alice tells Bob which polarization she sent the photon with, Eve can measure correctly and know the value of the bit. Otherwise, she must guess a measurement basis at the time of receiving the bit which may or may not be accurate, with fifty percent probability. So, with a total of seventy-five percent probability, Eve knows the value of the bit sent by Alice that ends up in Alice and Bob's shared string.

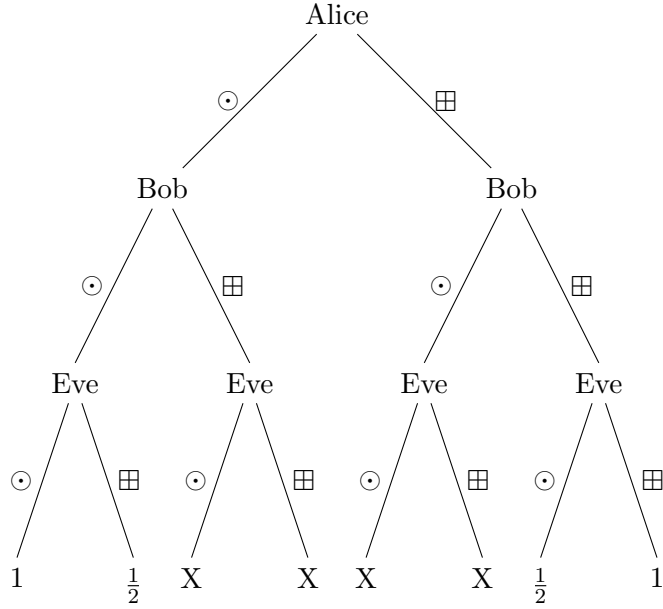


Figure 2: Possible outcomes of a beamsplitting attack

The $\frac{1}{2}$ denotes the fifty percent probability of Eve reading the correct value of the transmitted bit. The X represents the cases where the bit is discarded during the first phase on the public channel. The 1 showcases instances where Eve knows the value of the transmitted bit with one-hundred percent certainty.

6.2 Intercept/Resend

Eve can intercept a pulse on its way to Bob and send him one that she fabricates. The pulse she fabricates to send to Bob uses the same polarization in which she chooses to detect it, at an intensity enough to not cause any suspicion [5]. Assuming Alice and Bob catch twenty-five percent of Eve's fake pulses, it is estimated that Eve fakes four times the number of detected errors. If t is the number of errors in the quantum transmission, intercept/resend attacks affect fewer than $4t$ bits with an arbitrary 5σ error allowance of $5\sqrt{12t}$ bits, for an upper bound of $4t + 5\sqrt{12t}$ bits [5]. The number of bits Eve learns via this method is worth as much as if she learned $\frac{4}{\sqrt{2}}t$ with another 5σ allowance $5\sqrt{(4 + 4\sqrt{2})t}$ for a total of $\frac{4}{\sqrt{2}}t + 5\sqrt{(4 + 4\sqrt{2})t}$ bits from the transmission over the quantum channel [5]. With an intercept/resend attack the potential outcomes are as follows: Eve may learn the value of the transmitted bit and resend one that allows her interference to go undetected, the bit may be thrown out due to Alice and Bob using mismatched measurements, or Eve may disrupt the value of the bit and be detected.

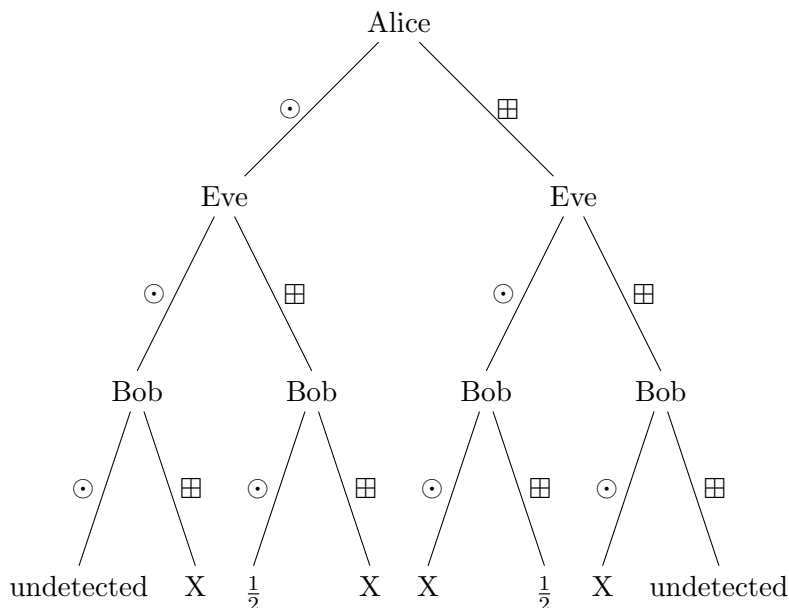


Figure 3: Possible outcomes of an intercept/resend attack

The $\frac{1}{2}$ denotes the fifty percent probability of Eve disrupting the value of the transmitted bit. Since she is using the opposite basis than both Alice and Bob, half of the time she causes the bit to flip and Bob to receive the incorrect value. The X represents the cases where the bit is discarded during the first phase on the public channel.

6.3 Combining Attacks

If both beamsplitting and intercept/resend are applied, the fraction of the string Eve learns is at most $\rho = \mu + \frac{4}{\sqrt{2}}p$ fraction of the key, where p is the bit error rate, μ is the fraction of bits Eve learns from beamsplitting, and $\frac{4}{\sqrt{2}}$ is the maximum fraction Eve learns through intercept/resend [5]. Combining the total number of bits sent, N , and the fraction leaked, $N\rho + 5\sqrt{N(\mu(1-\mu) + (4 + 2\sqrt{2})p)}$ is the estimated maximum total number of bits leaked to Eve [5]. This approximation includes a conservative 5σ allowance for uncaught errors.

7 Key Infrastructures

The commercial application of QKD must be compared with the current implementation of public key infrastructure to fully understand the workings of each approach, along with the risks involved and the magnitude of those risks. Understanding various attack models is crucial to decision making when it comes to the adoption of QKD.

7.1 Public Key Infrastructure

When Alice wants to send messages to Bob, a series of steps are followed. A certificate authority (CA) has a self-signed or root certificate [1]. Bob goes to the CA with identification such as a driver's license. The CA verifies Bob's identity and signs his certificate with their secret key [1]. Bob now has a signed public key certificate to prove the legitimacy of his public key. When Alice wants to communicate with Bob, she first checks Bob's public key certificate.

A legitimate Bob has been authenticated by a certificate authority and the certificate authority has signed his public key certificate [1]. When Alice sees the signed certificate, she trusts Bob's public key. Asymmetric cryptography is more computationally expensive than symmetric cryptography, so they want to exchange a symmetric key for the rest of their communications [1]. Alice sends Bob an AES key encrypted with his public key, which they then use to encrypt their communications.

Public key infrastructure is fast, convenient, and cost-effective, but because of the ease of spoofing and person-in-the-middle attacks, attackers are capable of accessing secret information that can be read out at their leisure [1]. On the security triangle discussed in section 8.2, public key infrastructure lands slightly above center, closer to convenience, but slower and less secure than the other systems being considered.

7.2 QKD Infrastructure

When Alice and Bob use QKD, they have a trusted courier deliver the physical QKD device and an initial key. They use message authentication codes (MAC) to authenticate on the classical channel [6]. Alice inputs the initial key along with her message in the MAC algorithm to generate the MAC she sends to Bob with her message [6]. When Bob receives Alice's message, he inputs it to the MAC algorithm along with the initial key to generate a MAC [6]. They compare the MAC they each generated and if they match, their classical channel is authenticated [6]. They now are set up for the public channel communications as explained in section 5. Since the quantum channel is set up with physical hardware, Alice trusts that Bob is at the other end of the line. The BB84 protocol is performed and the two land on a final shared secret binary string, which is what they then use as their AES key to communicate on a non-quantum channel [6]. To re-authenticate, Alice and Bob agree that the next key they establish using BB84 will replace the initial key they input to their MAC algorithms [6].

QKD infrastructure may require more work to set up than public key channels, and the cost of QKD hardware must be considered. Attackers are inconvenienced by having to constantly stay on the line for the exchange of information between Alice and Bob, as explained in section 8.1.2. The inconvenience of attacking QKD might discourage their attempts. The consideration of these factors play into business decisions surrounding whether to use QKD.

8 Security Models

An important consideration in deciding whether to choose QKD over other methods of cryptography is understanding the ways in which each of the options can be attacked. Another key factor is the

security and tradeoffs of each method relative to their alternatives. The resources available to an attacker also plays into the security model.

8.1 Attack Models

The ways in which tradeoffs between using QKD systems are assessed differ based on the attack model. In some cases, Eve is able to perform technical attacks including intercept/resend and beamsplitting. However, there are times when Eve may have other methods of getting information than technical attacks. One attack to consider is harvesting, which is a form of passive eavesdropping where attackers collect data as it is being transmitted in order to decrypt at a later time [1]. A short-term form of harvesting is a person-in-the-middle attack where Eve may run the connection all day and process the information overnight [1]. Other instances may require the information to be stored safely for much longer, especially in the case of governments where global secrets have value even after decades. Companies might worry about industrial espionage with competitors listening to private communications and learning trade secrets.

8.1.1 Public Key Infrastructure Attack Model

In public key infrastructure, an attack model of concern would be Eve listening in on conversations between Alice and Bob. The public key that Alice chooses to trust might actually belong to Eve and not Bob [1]. So, Alice sends a message encrypted with Eve's public key, then Eve decrypts the message and re-encrypts with Bob's public key before passing it along to Bob [1]. When Alice sends the AES key in the next step, Eve gets the key information, passes it along to Bob, and can now listen to any of Alice's communications with Bob. Eve can log the data being sent and analyze the amassed information at a later time if she so chooses. By storing the data for later decryption, Eve does not have to be involved real-time, making this attack more convenient for her.

Systems are sometimes under attack by multiple actors, which then makes it useful to consider how multiple attackers may disrupt one another. A disruption may occur by interfering with each other's attack, or by one of them getting caught thereby causing Alice and Bob to lose trust in the system. If a second attacker, Frank, is introduced, Alice now sends a message to Eve encrypted with Eve's public key. Eve thinks Frank is Bob so she sends Frank a message encrypted with Frank's private key, then Frank can send Bob the message encrypted with Bob's private key. In this case, Alice thinks Eve is Bob and Eve thinks Frank is Bob. If Frank is fooled by Eve's fake certificate where she is pretending to be Bob, he might reveal himself as another attacker to Eve by sending her a message that he intended to send to Bob.

8.1.2 Quantum Key Infrastructure Attack Model

In quantum key infrastructure, an attack model of concern on the QKD side looks similar to an attack on public key infrastructure, with an added step of complexity. If Eve is on both the quantum and public channels, she would be able to conduct a person-in-the-middle attack between Alice and Bob. In this attack model, Eve sits on the end of a quantum channel and a public channel with Alice, leading to a secret bit string shared between the two of them. Eve sets up the same exchange with Bob so she has channels to both parties. Eve must keep track of the key between herself and Alice and the key shared between herself and Bob. Since Alice cannot send

messages directly to Bob, Eve must be present on the line constantly and in real time decrypt the message from Alice then re-encrypt and send to Bob. Eve no longer has the luxury of letting the logs pile up and coming to decrypt them later. If a second attacker, Frank, is introduced, a more complex string of dependencies piles up where Alice and Eve share a key, Eve and Frank share a key, then Frank and Bob share a key along this message chain, all which must be handled real-time.

If the channels were set up with Bob on the public channel and Eve on the quantum channel, Eve would be able to facilitate an intercept/resend attack. Alternatively, if Bob is on the quantum channel and Eve is on the public channel, Eve cannot get any useful information but she can cause enough noise that the key is thrown out entirely.

8.2 Security Tradeoffs

An important consideration in deciding cryptographic systems is practicality. A user must assess the security tradeoffs to determine what fits their needs. What qualifies as good enough security? Will people use QKD? Where does QKD fall between security, convenience, and speed? The security triangle can be drawn between these three qualifications.

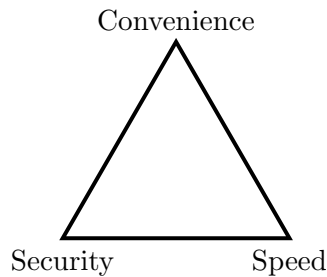


Figure 4: Security Triangle

On the security triangle, QKD falls slightly below center, being less convenient than systems that use existing infrastructure while providing good security at a moderate speed. AES can be found in the center of the triangle, a happy medium which contributes to it being the modern standard. RSA lives slightly closer to convenience, above AES. PQC provides the same security as RSA but is slower. However, the security triangle changes when considered in respect to quantum computers compared with normal computers.

With the involvement of attackers using large-scale quantum computers, RSA is no longer secure [7]. Depending on which tradeoff is chosen, either security or speed degrades for AES [2]. PQC takes the spot of RSA where it lands on the former security triangle. The position of QKD does not change in this scenario, where it is less convenient than PQC while providing more security.

8.3 Advantages of QKD

There are several reasons users could benefit from using QKD systems. QKD is protected against quantum computers because it is based on physics rather than mathematics, where RSA can easily

be broken by quantum computers [7]. Regardless of the involvement of quantum computers, there are still advantages to using QKD. Spoofing and person-in-the-middle attacks are more difficult to execute as outlined in the technical attacks section 6. As explained in section 5, QKD is capable of detecting any eavesdropping on the quantum information exchange.

8.4 Defense Options

Options to defend against malicious actors with a quantum computer would include implementing QKD, using PQC, or not using digital infrastructure at all. QKD provides the advantages discussed in section 8.3, but is more challenging to implement because of the hardware component and potential need to implement new infrastructure. Implementation and adoption may be too much of a barrier and outweigh the protection QKD provides. Rather than the quantum physics of QKD, PQC is based on complex mathematics. PQC algorithms are still in the research stages, with a few having been chosen for standardization [2]. Someone might choose to use PQC over QKD because it does not require any additional hardware and may be easier to implement in existing infrastructure. Choosing not to use digital infrastructure at all has its downfalls in convenience, where the use of couriers to deliver AES keys may take a long time and does not guarantee delivery. With the possibility of an attacker who has access to a quantum computer, it is important to already have one or more of these defense options implemented [2].

9 Human Error

Involving humans in this system has a vast potential to corrupt the security of the system. Humans may underestimate the eavesdropper, for example if Alice and Bob continue from their quantum channel communication to phase one of their public channel communication and Eve is able to keep her photon from decaying until after they openly share measurement systems, then Eve can correctly measure the photon she has kept. The system relies on Alice choosing randomly between circular and linear polarization alphabets, so there are privacy implications if Alice chooses predictably between quantum alphabets, allowing Eve to identify a pattern.

Alice and Bob may encounter calibration errors where even if they use the same measurement but their clocks are off or their measurement setup is not physically lined up, error will be introduced in the key string. If Bob's measurement system is slightly skewed, even if he chooses to measure in the same basis that Alice uses, he will never receive the bit with perfect certainty. If their clocks do not align, Bob may end up with a multitude of erasures, or a key that is shifted by a phase that induces error on many bits of the string.

Another potential for error is human nature. QKD secures the transmission of the shared secret key, but the key may be stored insecurely on their computer, leaving it vulnerable. Someone may walk away from their computer without locking it and a malicious actor can steal the key. Perhaps Bob trusts his partner Cindy and decides to tell her the key he shares with Alice. Maybe Bob gets phished and exposes his password which is then used to login as him and find his key. All of these are examples of social attacks that rely on the human factor. Vulnerabilities at the endpoints exist for any method of key exchange, particularly when humans are included.

10 Cybercrime

When comparing human versus technical attacks, consideration must be given to the size of the audience affected by each type as well as the monetary damage caused by each. The 2022 FBI Internet Crime Report provides data on types of cybercrime, including the number of victims and money lost to each [8]. These internet crimes have been sorted into human and technical attacks, with a third category for crimes that are unclear.

Human	Victims	Technical	Victims	Unclear	Victims
Phishing	300,497	Personal data breach	58,859	Credit Card/Check Fraud	22,985
Non-Payment/Non-Delivery	51,679	Spoofing	20,649	Business Email Compromise	21,832
Extortion	39,416	Data breach	2,795	Other	9,966
Tech Support	32,538	Ransomware	2,385		
Investment	30,529	Malware	762		
Identity Theft	27,922	Botnet	568		
Confidence/Romance	19,021				
Employment	14,946				
Harassment/Stalking	11,779				
Real Estate	11,727				
Government Impersonation	11,554				
Advanced Fee	11,264				
Overpayment	6,183				
Lottery/Sweepstakes/Inheritance	5,650				
Crimes Against Children	2,587				
Threats of Violence	2,224				
IPR/Copyright/Counterfeit	2,183				
SIM Swap	2,026				
Total	583,725	Total	86,018	Total	54,783

Table 3: Digital Crime Victims [8]

Human	Loss (\$)	Technical	Loss (\$)	Unclear	Loss (\$)
Investment	3,311,742,206	Personal data breach	742,438,136	Business Email Compromise	2,742,354,049
Tech Support	806,551,993	Data breach	459,321,859	Credit Card/Check Fraud	264,148,905
Confidence/Romance	735,882,192	Spoofing	107,926,252	Other	117,686,789
Real Estate	396,932,821	Ransomware	34,353,237		
Non-Payment/Non-Delivery	281,770,073	Botnet	17,099,378		
Government Impersonation	240,553,091	Malware	9,326,482		
Identity Theft	189,205,793				
Advanced Fee	104,325,444				
Lottery/Sweepstakes/Inheritance	83,602,376				
SIM Swap	72,652,571				
Extortion	54,335,128				
Employment	52,204,269				
Phishing	52,089,159				
Overpayment	38,335,772				
Harassment/Stalking	5,621,402				
Threats of Violence	4,972,099				
IPR/Copyright/Counterfeit	4,591,177				
Crimes Against Children	577,464				
Total	6,435,945,030	Total	1,370,465,344	Total	3,124,189,743

Table 4: Digital Crime Loss [8]

A metric was developed to calculate risk using the number of victims and money lost. For each crime, its risk is calculated as follows:

$$\text{risk} = \frac{\text{victims}}{\text{population}} * \frac{\text{victim loss}}{\text{victims}}$$

The first part determines the chance that someone will be a victim and multiplies that with the money lost by each victim. Some crimes may happen to a large group of people, but the damage is minimal, where other crimes may be very rare but have significant monetary repercussions. Since the FBI crime report is from 2022, the 2022 US population, 333,287,557, is used in the risk calculation [9]. Risk is measured in dollars per person in the population.

Human	Risk	Technical	Risk	Unclear	Risk
Investment	9.94	Personal data breach	2.23	Business Email Compromise	8.23
Tech Support	2.42	Data breach	1.38	Credit Card/Check Fraud	0.79
Confidence/Romance	2.21	Spoofing	0.32	Other	0.35
Real Estate	1.19	Ransomware	0.10		
Non-Payment/Non-Delivery	0.84	Botnet	0.05		
Government Impersonation	0.72	Malware	0.03		
Identity Theft	0.57				
Advanced Fee	0.31				
Lottery/Sweepstakes/Inheritance	0.25				
SIM Swap	0.22				
Extortion	0.163				
Employment	0.157				
Phishing	0.156				
Overpayment	0.12				
Harassment/Stalking	0.02				
Threats of Violence	0.015				
IPR/Copyright/Counterfeit	0.013				
Crimes Against Children	0.002				
Total	19.31	Total	4.11	Total	9.37

Table 5: Digital Crime Risk [8]

11 QKD Landscape

The theory of how to perform QKD has been solidified for years, but the implementation of the algorithms is more recent. There are QKD products available for commercial use, albeit with limited capabilities. There is also much research being done into ways to advance QKD products and combat those limitations.

11.1 Market

QKD hardware shares keys over optical fibre or free space. These systems have a range of capabilities, including estimating a maximum amount of information obtained by an eavesdropper. QKD products supplied by four different companies were studied for the purpose of this research: ID Quantique (IDQ), Quintessence Labs (QLabs), and Toshiba. IDQ has a number of QKD products,

including Clavis, Cerberis, XGR Series, Cerberis3, and Clavis300 [10]. Toshiba also provides multiple products, one multiplexed and one designed for long-distance communication [11].

Product	Range (km)	Key Rate (kb/s)
Clavis (IDQ)	up to 150	over 100
Cerberis (IDQ)	up to 90	2
Cerberis3 (IDQ)	50 (up to 70/80)	1.4
Clavis300 (IDQ)	up to 70	6
Multiplexed (Toshiba)	up to 70	40
Long-distance (Toshiba)	up to 120	300
qOptica (QLabs)	up to 40	4.3

Table 6: QKD Product Specifications [10] [12] [11]

Clavis is ideal for high key throughput and long range communication, Cerberis can be easily integrated into existing fiber optic network, the XGR Series is an open platform for research and development, Cerberis3 is designed for integration into data centers, and Clavis300 is ideal for testing quantum cryptography on different network configurations [10]. Since the XGR Series is for research, there are no specifications made publicly available. The target markets for these products include governments, finance, healthcare, critical infrastructure, and service providers. The cost of these devices likely scales with their capabilities where the more expensive devices have longer ranges and higher key rates. The products claim to be cost effective due to their compatibility with existing systems.

11.2 Research and Development

A prominent concern with the current products on the market is the range limitations. As explained in section 12.2.2, target customers are located much farther apart than the maximum ranges of QKD products can reach. Research is being done into methods of extending the range that quantum transmissions can span, including the use of satellites and quantum repeaters. Both of these approaches rely on quantum entanglement. Quantum entanglement causes multiple particles to share quantum states over any distance in a link that persists until one of the entangled particles is measured, at which point all particles collapse into the same distinct state [13].

One solution for the range limitations that come with current QKD products is the use of quantum repeaters. QKD can be performed by distributing pairs of entangled particles between endpoints [14].

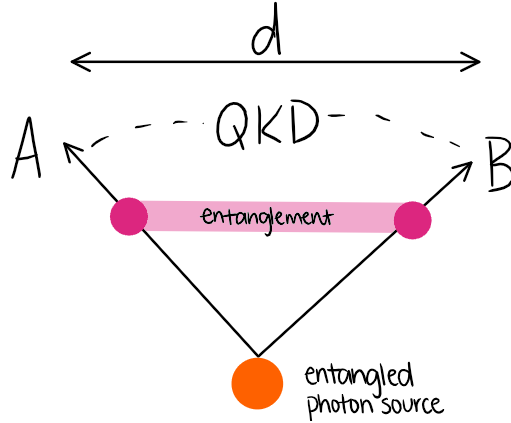


Figure 5: Quantum entanglement for QKD [14]

Quantum repeaters can be placed along the transmission path to boost the quantum data with a stronger signal before the photons degrade [14]. Quantum repeaters work using multiple pairs of entangled particles, sending one from each pair to each endpoint and the other to a measurement device between the endpoints [14]. If the particles are measured the same in the middle, then that means the outer particles are entangled [14].

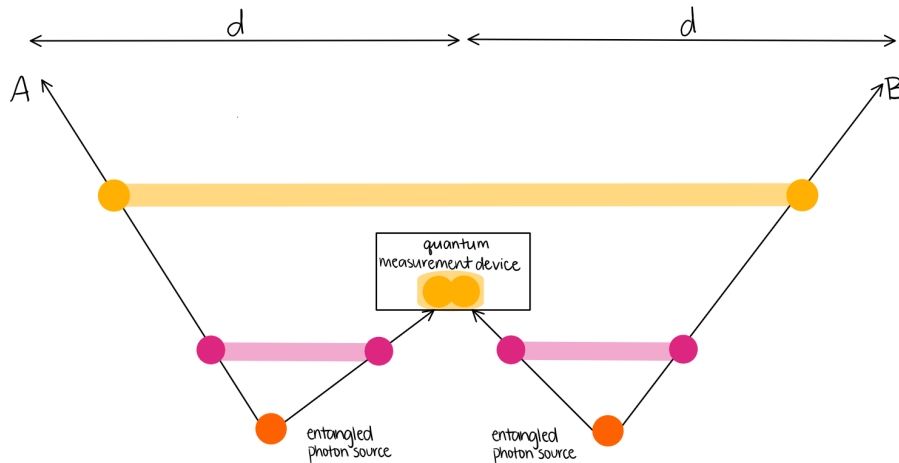


Figure 6: Quantum repeater [14]

Implementing repeater infrastructure would solve the range concerns with the existing products, but currently quantum repeater technology is not far enough along to make a difference. Repeaters have potential to be solutions to the range limitations of current QKD products, but since they are in experimental stages it is not yet possible to implement commercial quantum repeater infrastructure.

Quantum satellites use entangled particles to expand the distance over which quantum data can be transmitted. China has launched the satellite Micius and successfully tested the long-distance transmission of photons from the satellite to the ground [13]. Inside the satellite, photon pairs are entangled by sending a laser beam through a light-altering crystal [13]. The entangled photons are

then sent to the separate ground stations 1200 kilometers apart [13]. Previously, entangled particles had been measured at a maximum of 1.43 kilometers apart over fiber optic cable [13]. Regardless of distance, when the state of one of these photons is measured, the state of the other is known [13].

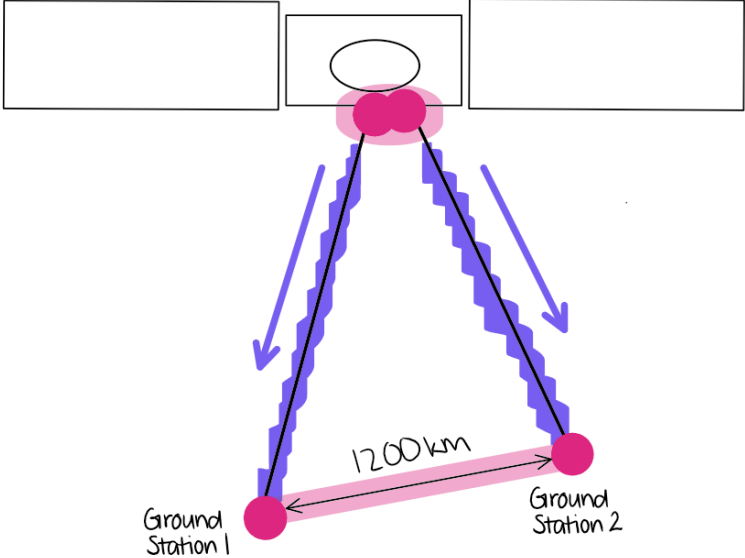


Figure 7: Photon pair being transmitted to ground stations [13]

Micius uses this fact to perform QKD by sending strings of entangled photons to the ground stations, generating their shared secret key [13]. Despite a transmission rate of 5.9 million entangled photon pairs per second, only 1 in 6 million photons successfully reached the ground stations [13]. QKD is not practical to implement with the rate of around 1 photon making it to the ground per second. The keys need to be long strings of photons, and it would take too long to transmit a key of reasonable length.

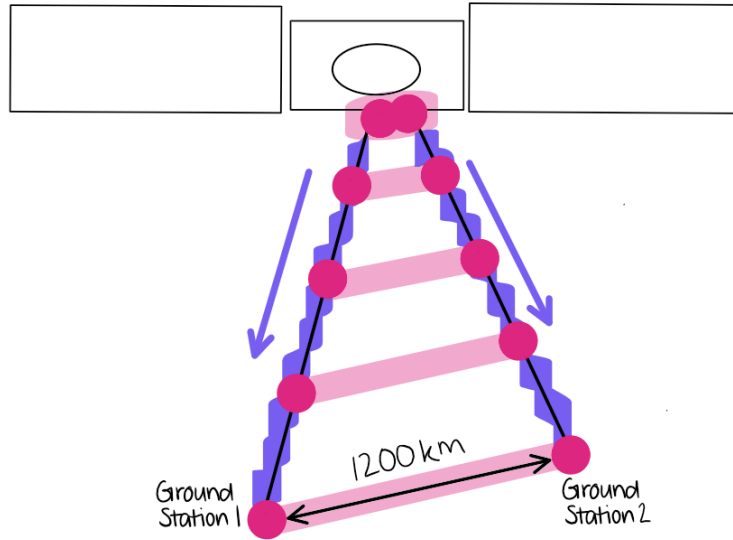


Figure 8: Sending strings of photon pairs [13]

A quantum internet could be created following the introduction of more satellites that perform the same operation as Micius [13]. The potential widespread distribution of quantum satellites poses a reasonable solution for the range concerns associated with current QKD products. Satellites could easily perform a complete beamsplitting attack, so to preserve the secrecy of their key, Alice and Bob would have to trust the satellites being used.

12 Research Methods

To learn about human trust in computers, research was conducted with a company that works in defense contracting. The employees take security seriously and have technical knowledge in the field.

12.1 Survey

A survey was distributed to the company to gather information about how individuals value security and trust existing measures. The survey consists of four questions, two of which are multiple choice and the other two Likert scale. The survey respondents have the following occupations:

- Cyber Software Engineer
- Software Engineer
- Program Manager
- Reverse Engineer
- Hardware Engineer
- Electrical Engineer

Half of the respondents have been at the company for two to four years, and the other half between zero and two years, as specified in 14.1. Alongside this demographic collection, participants were asked a series of questions regarding how much they value security and how much trust they have in current security systems.

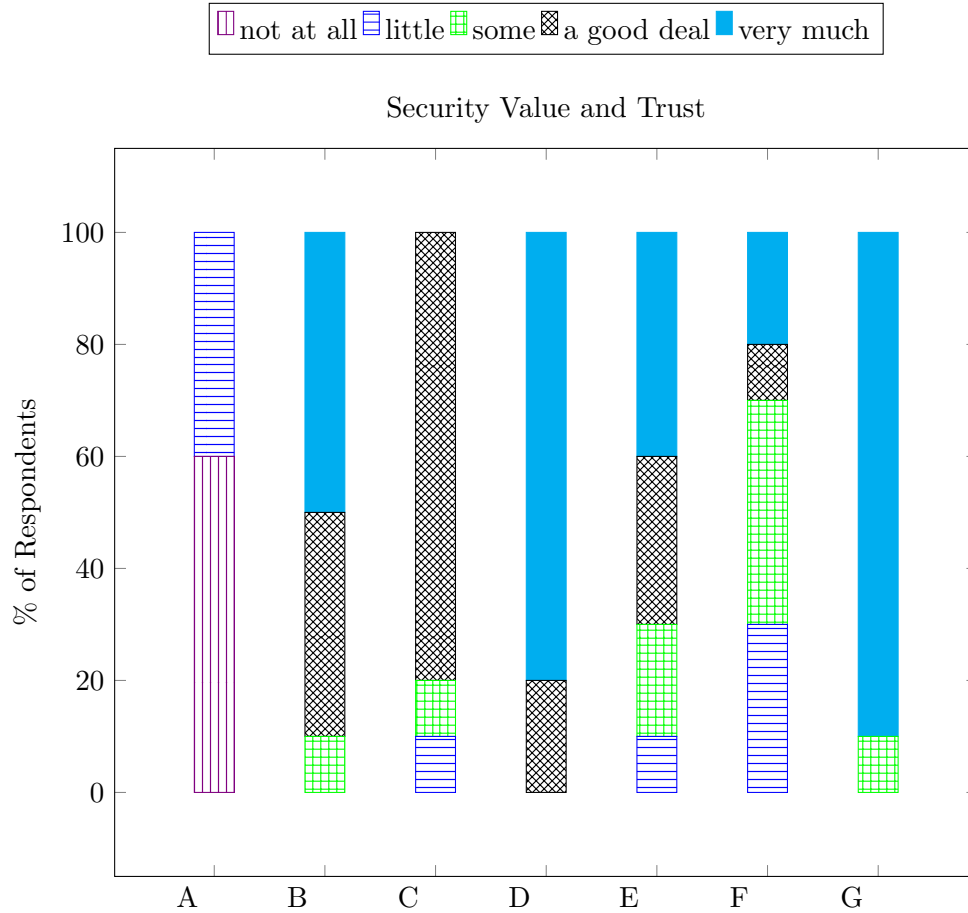
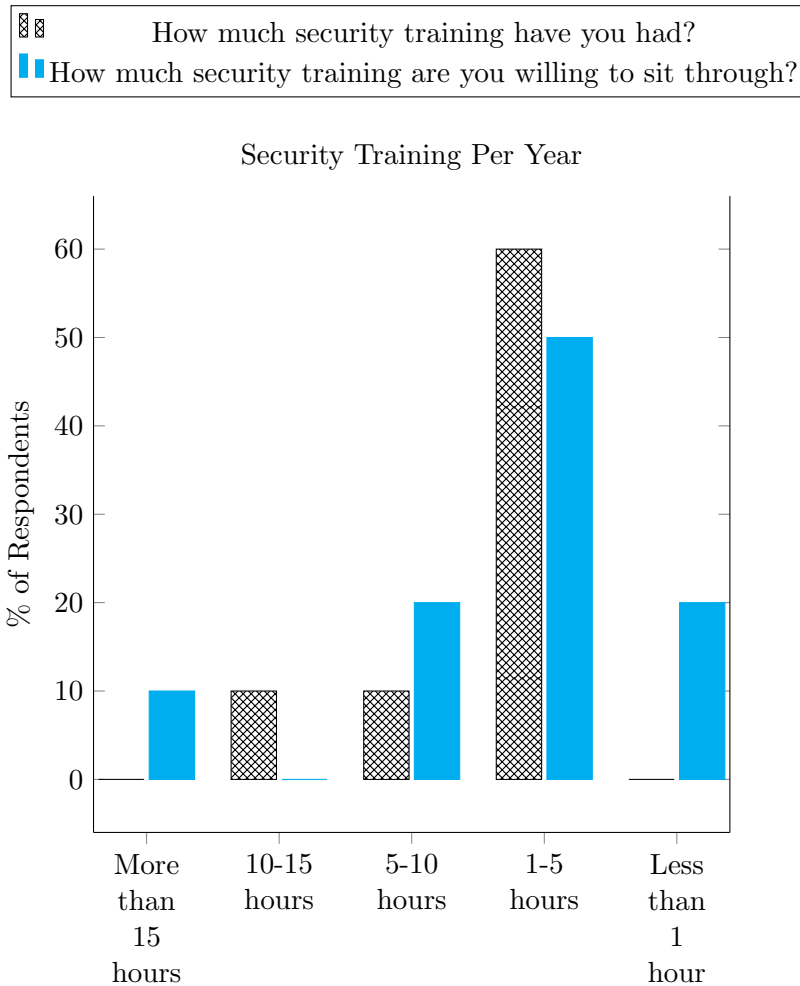


Figure 9:
 A: How much the individual is familiar with quantum cryptography
 B: How much the individual values protecting data
 C: How much the individual trusts current systems
 D: How much the company values security
 E: Importance of convenience in deciding security systems
 F: Importance of cost in deciding security systems
 G: Importance of protection in deciding security systems

Participants were asked about security training at their company, both how much they already have and how much they are willing to participate in.



Based on these survey results, the company makes security a top priority. Employees feel that protection is the most important factor when making decisions about security systems. None of the participants fully trust the security systems that are in place today, and all of them are willing to sit through at least one hour of security training. The survey results informed the determination of questions to be used as part of a follow-up focus group discussion.

12.2 Focus Group

As part of the survey, respondents had the option to volunteer to participate in a follow-up focus group discussion. For this discussion, the participants were given an overview of the research and background information on QKD products and key infrastructures. The Toshiba devices were not investigated until after the focus group, so the participants did not see their product specifications. The focus group touched on personal and corporate security concerns, including convenience issues. When asked about convenience, the participants brought up the convenience tradeoffs of using

multi-factor authentication (MFA). The participants were asked explicitly what attack model they might be worried about and what limits there are to what they are willing to give up for security. After the presentation of product research, participants were asked about how they would make decisions between the different QKD products. The discussion covered internal incentives and counter-incentives for using QKD.

12.2.1 Coding

The following codes are used to analyze the focus group discussion:

Threat Model	Tradeoffs	Quantum
Risk	Range	QKD products
Social engineering	Regulation	Quantum mechanics
Exfiltration	Convenience	
Password management	Cost	
Banking	Training	
MFA	Resources	
	Necessity	
	Subjectivity	

Table 7: Coding

Some categories came up more than others in the discussion. Despite tradeoffs encompassing a greater number of subtopics, the conversation brought up threat model more frequently.

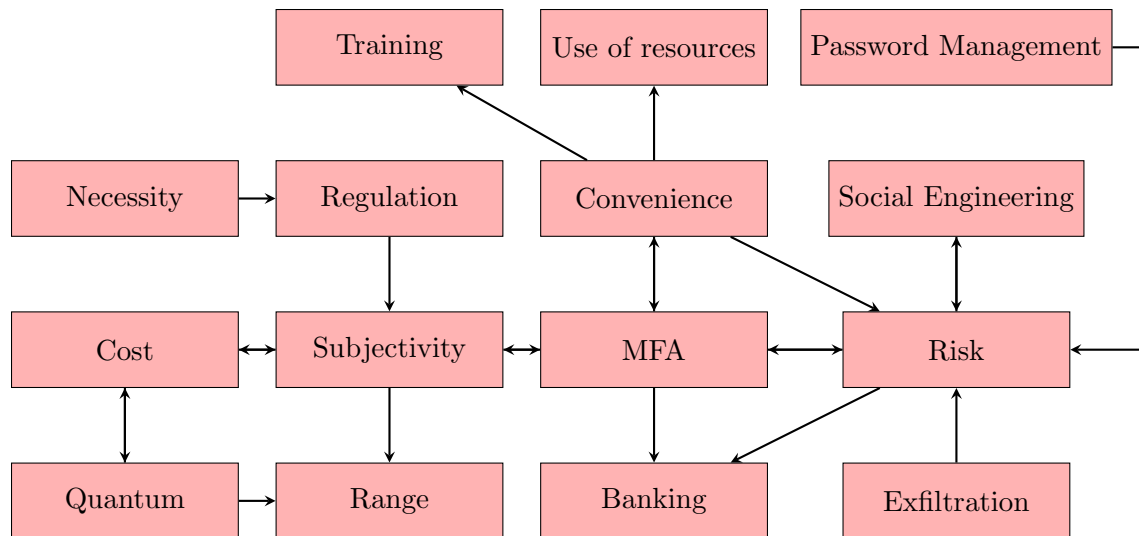
Code	Count
Threat Model	20
Tradeoffs	15
Quantum	8

Table 8: Frequency of Topics

These three codes are condensed into the general theme where the participants are more worried about vulnerabilities from a social attack before a technical attack. As a result, their incentives to adopt QKD come from the potential of government regulation requiring them to do so, rather than concern that their current methods of cryptography are vulnerable. These focus group takeaways contradict the survey results which indicate that nobody fully trusts existing security systems.

12.2.2 Conversation Flow

The conversation during the focus group reflected how the subcategory groupings of the codes did not necessarily influence the flow of conversation. The discussion centered around threat model, subjectivity, convenience, and MFA.



Regarding subjectivity, one participant made the insightful comment that “the accountants care about the cost, the users care about the convenience, and the lawyer cares about the security.” All of those groups would be involved in the decision to implement QKD in the company, so the feedback has potential to be varied. Range proved to be the most critical factor in the adoption of QKD, which is why conversations that led to range ended there.

Based on these focus group results, the company would switch to QKD if required by government, but it would be difficult to switch of their own volition. Contrary to the survey results, employees care more about practicality than protection.

13 Conclusion

The security arms race has led to QKD as a method of encrypting data using quantum physics, rather than the complex mathematics used in other algorithms. Technical attacks against the BB84 quantum cryptographic protocol require highly skilled attackers with access to expensive resources. Attacking quantum key infrastructure is an extra step of complexity beyond what is necessary for an attack on public key infrastructure. Such complications may dissuade some malicious entities from pursuing attacks against QKD.

Using QKD, the best case scenario for Alice and Bob is if Eve did not eavesdrop at all on the private channel. If this is the case, they can perform the public channel phases and realize Eve has not been at work, leaving them with a private key that is not only perfectly secret, but also perfectly correct [15]. If Eve is suspected to have eavesdropped on the private channel, then Alice and Bob will have to throw out a much greater portion of their string to get to the final secret key. They can manipulate how much information they are willing to let Eve know, knowing that they must choose between a longer key than Eve may have more information about and a shorter key that Eve has less information about.

The employees who participated in the research are security experts and emphasize the seriousness with which they and their employer want to protect the company data. Despite not fully trusting existing security systems, they trust them far enough that their concern for human attacks outweighs their worry of a technical attack against their cryptography. Their evaluation is valid, backed by the cybercrime statistics from the FBI report reinforcing the frequency, damage, and risk of both human and technical attacks. Couple this with the imbalance of opportunities for cybercrime that relies on a human factor as it vastly outnumbers technical cybercrime, and it makes sense for users to be less concerned about technical attacks. With government customers, a push for the company to implement QKD would be regulation requiring them to do so. On the same note, it would be difficult to make the switch to QKD before the government standardizes it. Current QKD products are limited by range, key rate, and the difficulty of implementing the infrastructure to support the hardware. If attackers were working with large-scale quantum computers, some method of quantum-resistant cryptography like QKD would be immediately necessary. PQC is a prominent competitor, and with standardization of PQC algorithms it has potential to be adopted by companies due to the ease of integration. Where QKD prevails over PQC is against technical attacks. The primary incentives for adoption of QKD as the next step in the cryptography arms race would be due to regulation and necessity. Currently, the adoption of QKD is viewed as more inconvenient than the security it provides is worth.

References

- [1] N. Daswani, C. Kern, and A. Kesavan, *Foundations of Security*. Apress Berkeley, CA., 2007.
- [2] “PQC standardization process,” July 2022. [Online]. Available: <https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4>
- [3] S. J. Lomonaco Jr., “A quick glance at quantum cryptography,” November 1998. [Online]. Available: <https://doi.org/10.48550/arXiv.quant-ph/9811056>
- [4] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, “Experimental quantum cryptography,” *Advances in Cryptology*, pp. 253–265, 1991. [Online]. Available: https://doi.org/10.1007/3-540-46877-3_23
- [5] C. H. Bennett, J. Smolin, F. Bessette, G. Brassard, and L. Salvail, “Experimental quantum cryptography,” *Journal of Cryptology*, pp. 3–28, 1992. [Online]. Available: <https://doi.org/10.1007/BF00191318>
- [6] J. Cederlof, “Authentication in quantum key growing,” June 2005. [Online]. Available: <https://www.lysator.liu.se/~jc/mthesis/mthesis.pdf>
- [7] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlmutter, and D. Smith-Tone, “Report on post-quantum cryptography,” April 2016. [Online]. Available: <https://doi.org/10.6028/NIST.IR.8105>
- [8] “Internet crime report,” 2022. [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
- [9] “Growth in u.s. population shows early indication of recovery amid covid-19 pandemic,” December 2022. [Online]. Available: <https://www.census.gov/newsroom/press-releases/2022/2022-population-estimates.html>
- [10] “Id quantique.” [Online]. Available: <https://www.idquantique.com/>
- [11] “Products.” [Online]. Available: <https://www.global.toshiba/ww/products-solutions/security-ict/qkd/products>
- [12] “Quintessence labs.” [Online]. Available: <https://www.quintessencelabs.com/>
- [13] G. Popkin, “China’s quantum satellite achieves ‘spooky action’ at record distance,” June 2017. [Online]. Available: <https://www.science.org/content/article/china-s-quantum-satellite-achieves-spooky-action-record-distance>
- [14] “Quantum repeaters,” 2010. [Online]. Available: <https://web.archive.org/web/20221109174252/http://quantumrepeaters.eu/quantumrepeaters.eu/index.php/qcomm/quantum-repeaters/>
- [15] C. H. Bennett, G. Brassard, and J.-M. Robert, “Privacy amplification by public discussion,” *Society for Industrial and Applied Mathematics*, vol. 17, no. 2, April 1988. [Online]. Available: <https://doi.org/10.1137/0217014>

14 Appendix

14.1 Raw data

The raw data from the survey.

Time Employed	Number of Employees
less than 1 year:	2
1-2 years:	3
2-4 years:	5

Table 9: How long employees have been at the company

Title	Number of Employees
Cyber Software Engineer:	2
Electrical Engineer:	1
Hardware Engineer:	1
Program Manager:	1
Reverse Engineer:	1
Software Engineer:	3

Table 10: Employee job titles

	less than 1 hour	1-5 hours	5-10 hours	10-15 hours	more than 15 hours
How much security training are you willing to sit through?	2	5	2	0	1
How much security training have you had?	0	6	1	1	0

Table 11: Security training per year

	not at all	little	some	a good deal	very much
How much familiarity do you have with quantum cryptography?	6	4	0	0	0
How much do you value protecting your data?	0	0	1	4	5
How much do you trust current systems?	0	1	1	8	0
How much does your company value security?	0	0	0	2	8
How important is convenience to a decision about security systems?	0	1	2	3	4
How important is cost to a decision about security systems?	0	3	4	1	2
How important is protection to a decision about security systems?	0	0	1	0	9

Table 12: Security risk and trust

14.2 Focus Group

The questions asked in the focus group:

- What are your security concerns? Personally, and for your company?
- What attack model are you worried about?
- What are some issues of convenience? For the individual and for the company?
- What is the limit of how much you are willing to give up for security?
- How does security, cost, and speed affect decisions between QKD products?
- What are some internal incentives and counter-incentives for using QKD?

How often each code came up:

Code	Count
Threat Model	20
Tradeoffs	15
Quantum	8

Table 13: Frequency of Topics