Chapter 1

Physical Security in Quantum Key Distribution

Contents

1 Cryptography in the Age of Quantum Computers

To do
Add citation on QKD origins

For a decade or two now, Quantum Computing has been creating a buzz that nobody in Computer Science and adjacent fields could evade. Originating in the 1980ies as a highly academic fusion applying concepts from Computer Science in Quantum Physics, its concepts have long found their way into popular science articles. Quantum Computing encompasses a model of computation that is fundamentally different from the *classical*[1] digital circuits that underly all of modern computing. While at first this might seem like a step backwards into the era of early 1900s analog computing, the capabilites of a future quantum computer promise to far outpace those of contemporary classical computers. Key to this improved processing capability is a property called *Quantum Parallelism*. What this refers to is the fact that a quantum computer's internal state can simultaneously represent a multitude of states of a classical, digital computer, and the quantum computer can operate on all those states at once using a single quantum operation.

To do
Add citation on early analog computing

Applying Quantum Parallelism to practical problems is far more complicated than, e.g., translating a digital circuit solving some equation to a quantum circuit, but for certain problems we already know *quantum algorithms* that for large inputs solve these problems much faster than any classical computer ever could. Two of these algorithms, one by Shor and one by Grover are what caused most of the buzz around the field of quantum computing, because they spell trouble for a large part of modern cryptography.

To do
Add citations on Shor's and Grover's algorithm

Besides the computational speed-up promised by Quantum Parallelism, there is one more interesting aspect of Quantum Computing where it radically deviates from classical computing. The reason modern cryptography exists is that when we transmit (or store!) classical information through some channel (or storage!) that we do not control, there is nothing we can do to prevent an attacker from reading this information. Even with cryptography we cannot prevent this, but cryptography gives us tools to very effectively make whatever information the attacker is able to read useless to them.

A basic principle of Quantum Physics is the *No-Cloning Theorem*, which

[1] In Quantum Computing, the term *classical* is used as the complement of *quantum*, and refers to the digital computers we know and (sometimes) love. This terminology stems from the distinction between classical and quantum physics.

states that it is impossible to create an identical, independent copy of an arbitrary, unknown quantum state. An implication of this theorem is that when we encode classical information into quantum states in just the right way, we can make it so that an attacker atttempting to eavesdrop on our quantum information can only actually read this information by destroying it in the process. This property can be exploited to replace a number of classical asymmetric primitives in interactive settings, the most popular application of which is replacing an asymmetric Diffie-Hellman key exchange with a quantum process called Quantum Key Distribution that yields much of the same properties.

To do
Add citation on No-Cloning Theorem

To do
Add citation on substitution, check if interactive only

To do
Add citation on DH-Kex

In the past decades, the field of cryptography has been fundamentally shaped by the development of Quantum Computing and Quantum Key Distribution. However, the popular conception that all of today's cryptography will be broken and that we have to start from scratch is not accurate. Quantum Computing poses an unique threat to modern cryptography, and Quantum Key Distribution is a promising new tool, but the practical implications of both are much more subtle than how they may be portrayed. In the remainder of this chapter, we will look into the practical implications of these quantum technologies, and we will come to two major conclusions: First, that while the underlying cryptographic primitives will change, apart from some minor engineering issues cryptography as a whole will remain largely the same. Second, that while Quantum Key Distribution is hailed as a revolution for network security, its practical advantages will remain far short of how it is usually conceptualized, and hardware security will assume a pivotal role in the practical security of Quantum Key Distribution systems that is a stark departure from its relative irrelevance in today's applied cryptography.

Building on these conclusions, we will end this chapter with a study of a use case that illustrates a practical design for a secure network employing Quantum Key Distribution. Relying on both established classical and quantum primitives with known security properties we will elaborate how one can construct a large-scale network from those primitives that provides practical security to its users that goes beyond the (surprisingly limited) extents of quantum security proofs.

1.1 Computational Assumptions and Information-Theoretic Security

In the past paragraphs we have briefly mentioned that Quantum Computing provides a significant speed-up that can be applied to solve many cryptographic problems fast enough for it to become a problem, but we have not elaborated on what that means in practice. In this section, we will attempt to provide concrete numbers to quantify the threat that both Shor's and Grover's algorithm pose to modern cryptography.

Shor's algorithm allows for the factorization of large numbers in polynomial time on a quantum computer, a problem whose hardness (or the hardness of variants of which) is the foundation for the vast majority of today's asymmetric cryptography.

While Shor's algorithm attacks the foundations of most modern asymmetric cryptography, Grover's algorithm can be applied to hash functionss and symmetric cryptography. Fundamentally, Grover's algorithm is a search algorithm that allows a quantum computer to find one target entry out of an *unstructured* list of N source entries in $\mathcal{O}\left(\sqrt{N}\right)$ time instead of the $\mathcal{O}(N)$ time that a classical computer would require for an exhaustive search. Applied to cryptography, we model the key space of a symmetric cipher as the unstructured list that is input to the algorithm, and set it to search for the key that results in the successful decryption of a given ciphtertext.

An important nuance applying these algorithms to cryptography is that while both provide significant speed-ups over classical computers, the speed-up of Shor's algorithm is exponential and effectively breaks most modern asymmetric cryptography as it erases the asymmetric nature of the underlying mathematical problem's computational complexity. That is, for an asymmetric cryptosystem susceptible to Shor's algorithm, there is no set of parameters that is large enough to be safe.

To do
definition, citation of security level

In contrast to this, while Grover's algorithm radically speeds up the breaking of a symmetric cryptosystem, this speed-up is only quadratic. In practice this means that it halves the security level of a given symmetric cipher. While this is bad news for applications that parameterize these symmetric primitives to a security level at the lower end of what is considered secure today, the advantage provided by Grover's algorithm can easily be compensated by doubling key size. Longer key sizes require more storage or bandwidth for the additional bits and result in slightly slower operation of the cipher, but this additional cost is easily manageable even without any

improvement in today's hardware.

Impagliazzo [7] provided a colloquial but useful analysis characterizing the implications of which kinds of hard problems are solvable in practice, based on the observation that the fact that an *average* problem out of a class like NP is solvable does not mean that most, or even many *practical* problems are solvable. Impagliazzo [7] was published after Shor's algorithm was discovered, and before Grover's algorithm was published. Impagliazzo foresaw that fast quantum algorithms could threaten public-key security, and their analysis remains relevant facing the outlook of quantum computing today.

Impagliazzo proposes a set of five scenarios that provide increasingly extensive computational hardness properies, dubbed *Algorithmica*, *Heuristica*, *Pessiland*, *Minicrypt*, and *Cryptomania*. In Algorithmica, $P = NP$. In Heuristica, $P \neq NP$, but NP problems are only intractable in the worst case, and tractable on average. In Pessiland, problems exist that are hard on average, but there are no one-way functions and thus there is no way to efficiently sample solved instances of hard problems.

The next scenario, Minicrypt is frequently cited in cryptographic works. In it, one-way functions exist, but there is no public key cryptography. Minicrypt aligns well with a world in which fast quantum algorithms exist that solve the computational problems underlying public-key cryptosystems. Impagliazzo's last scenario is Cryptomania, which extends Minicrypt with public-key cryptography and aligns with the world view that is commonly assumed in cryptography today.

In Mincrypt, we assume that all computational problems that are amenable to public key cryptography fall. However, it is not specified *how* specifically this fall will happen—whether it will be classically, or by quantum algorithms—leading to two sub-variants of the Minicrypt scenario. The pessimistic sub-variant is one where classical algorithms solving all those problems are discovered. This scenario leads to identical conclusions to those Impagliazzo drew. However, if we base our Minicrypt assumption instead on the availability of *quantum* algorithms for these problems, and thus on quantum computers being both powerful enough and generally available, we end up with an interesting spin on the original Minicrypt scenario that recently has garnered some academic attention, receiving the name Mini**Q**Crypt[6, 1]. In MiniQCrypt, on one hand, conventional public key cryptography falls before quantum computers, but the key observa-

tion is that on the other hand, we can then use those quantum computers to do *quantum* cryptography, re-gaining some of what we have lost. The (im)possibility results for MiniQCrypt are nuanced, and provide something between the intact conventional public-key cryptography in Cryptomania, and the total absence of it in classical Minicrypt.

In the discourse on quantum computing and its application to cryptography, it is important to be mindful of which security notion the authors of some source, or the implementors of some device base their work on. Especially in academic work, Pessiland assumptions are often implicitly made. In this model, we can use neither public-key nor symmetric cryptography. In this framework, secret key rate becomes paramount because it is assumed that QKD keys will be used with an information-theoretically secure encryption scheme, requiring a never-ending secret key stream. Key expansion functions are based on one-way-functions, which are unavailable here.

While in academic sources Pessiland assumptions are common, commercial systems usually are based on Minicrypt assumptions. That is, commercial systems propose QKD as an alternative to classical asymmetric cryptography for cryptographic key exchange, but then continue to use classical symmetric cryptography for purposes such as key derivation and secret-key encryption. Using a computationally secure key derivation function such as Argon 2, a small, fixed amount of precious QKD secret key bits can be expanded into a key of almost unbounded length. Similarly, a computationally secure symmetric cipher such as AES can be used to encrypt almost arbitrary amounts of data using a single, short key[2].

2 The Practical Security Implications of Quantum Computing

Given that as of yet, noone has claimed to have a quantum computer powerful enough to pose a threat to current cryptographic protocols, one may ask the fair question why the possible future development of such a machine

[2]We write that the amount of key bits that can be extracted from a computationally secure key derivation function and the amount of data that can be encrypted with a computationally secure cipher are only *almost* unbounded because both share that they operate on blocks of a fixed, short size and in most applications, collisions of two such blocks either at the primitve's output or inside of the primitive enables stochastic *Birthday Attacks*. Usually, for a primitive of block size n bit, an amount of $2^{\frac{n}{2}}$ extracted blocks is used as an upper bound for safe usage. For most modern primitives using a block size of 128 bit, this bound lies at 256 EB of data[3, 8].

would be consequential for today's cryptographic practice. The answer to this question lies in *Store-Now-Decrypt-Later* attacks. In such attacks, the attacker records all data transmitted between a cryptographic protocol's parties. The security of any key exchange protocol rests on a computational hardness assumption about some particular problem. When this assumption falls, for example because of a powerful quantum computer becoming available, the attacker can then retroactively break the security of those stored protocol instances and decrypt all traffic.

Modern cryptographic protocols such as TLS or the Signal messenger's key ratchet are designed with facilities to provide some degree of protection against key compromise called *(Perfect) Forward Secrecy*. Forward Secrecy means that a compromise of keys at one protocol step will not break the secrecy of past protocol steps. Forward Secrecy is achieved by repeatedly mixing fresh key material called *Ephemeral Keys* into the protocol's secret state. For a post-quantum attacker, this implies that to decrypt a run of a forward-secret cryptographic protocol, the quantum algorithm breaking the protocol's computational assumption must be run a number of times, but this results only in a linear increase of both protocol and attack complexity, which turns out to no advantage for the defender.

Store-Now-Decrypt-Later attacks are considered a serious threat today based on the stark discrepancy between the capacity of today's inexpensive storage media, and the comparatively tiny bandwidth of cryptographic protocols in applications such as *End-To-End-Encrypted* text messaging. A single hard drive can conceivably store years of a person's encrypted digital communications.

There has been ongoing work on quantum secure cryptographic algorithms, and standardization of several such algorithms is progressing. However, in the time frame of cryptosystems, these algorithms are still rather young and the recent discovery of a catastrophic key recovery attack against the Supersingular Isogeny Diffie-Hellman protocol (SIDH)[5] illustrates the risk in the use of immature cryptographic primitives. Thus, recommendations on the concrete steps that should be taken today to mitigate Store-Now-Decrypt-Later attacks vary. For instance, Google's under its threat model as laid out in Schmieg, Kölbl, and Endignoux [10] recommends a list of quantum secure counterparts to classically secure cryptographic algorithms, but recognizes the relative immaturity of these quantum secure algorithms and consequently recommends *Hybrid Deployment*, where a young,

quantum secure algorithm is paired with a mature classically secure algorithm such that *both* algorithms would have to be broken to compromise the composite protocol's security. Given that quantum secure public key cryptography tends to have both a much larger key and/or ciphertext size and worse performance compared to state-of-the-art Elliptic Curve-based key exchange or signature algorithms, pairing it with a classically secure alternative incurs only a negligible overhead in key storage, network communication and computation costs.

To do
research some more policies.

To do
missing

3 The Physics of Quantum Computing

4 Quantum Key Distribution

As we discussed in Section 1.1, quantum computers promise novel attacks on many contemporary cryptographic systems. At the same time, quantum technology also promises new cryptographic primitives that support security guarantees beyond what can be realized with the best classical computers. The core of this nascent field of Quantum Cryptography is a set of methods that are collectively called Quantum Key Distribution.

Informally speaking, a Quantum Key Distribution system is a system that distributes a secret key between two[3] parties such that after a successful execution of the protocol, each of the two parties holds a copy of a randomly generated secret key, and the probability that an attacker was able to extract some portion of the key during the protocol's execution can be bounded to some negligible ϵ by each of the parties.

Quantum Key Distribution provides a similar service as cryptographic key exchange protocols such as the classic Diffie-Hellman key exchange provide. The core difference between QKD and cryptographic key exchange protocols is that QKD provides information-theoretic security based on the No-Cloning Theorem, where cryptographic protocols provide only computational security based on the computational hardness assumption underlying some public-key cryptosystem.

QKD is attractive in that it gives practically useful security guarantees

[3] Although the key distribution problem can conceptually be framed for any number $n \geq 2$ of parties, practical treatment is almost always limited to the two-party case. In case of QKD, problem instances for $n > 2$ parties can trivially be reduced to $(n^2 - n)/2$ invocations of the two-party protocol, combined with any information-theoretically secure secret sharing scheme.

without relying on any computational hardness assumptions. This way, QKD would remain secure even in a scenario where a hybrid deployment of a classically secure but mature algorithm paired with a quantum secure but young algorithm as discussed in Section poses too much of a risk—a scenario where both large quantum computers arrive and a flaw in the quantum secure algorithm is found. Note that here, because we assume we have large quantum computers, the possibility of a flaw in the quantum secure algorithm extends beyond mathematical flaws leading to practical attacks with classical computers, and includes novel quantum algorithms.

4.1 Security assumptions in QKD

While QKD protocols provide information-theoretic security, part of these protocols is always an authenticated channel that is used by the protocol's parties to exchange information necessary to align both parties' quantum measurements so that they can reconstruct the same secret key bit stream. In the security model of QKD, this authenticated channel does some heavy lifting. While the QKD protocol provides key exchange–an asymmetric primitive–based on this authenticated channel–which in its most simple implementation requires only symmetric primitives, an implementation of QKD using symmetric primitives such as HMAC or CMAC for the authenticated channel would not achieve information-theoretic security. To acheive information-theoretic security, the authenticated channel itself must use an information-theoretically secure authentication method. The issue with that is that information-theoretically secure authentication methods are (provably) rather inefficient in their key use. While symmetric MACs can use a single, short key for a very long time, information-theoretically secure MACs need a continuous stream of fresh key bits.

To do
citation on "provably"

In QKD, the authenticated channel can be bootstrapped by taking these MAC key bits from the QKD channel itself. The disadvantage of doing that is that it consumes a fraction of the system's precious secure key rate. As a consequence, at this point there is ongoing research on both systems based on symmetric MACs and systems using information-theoretically secure MACs, with commercial systems often choosing the latter[4] owing to the low secure key rates that are the state of the art.

To do
citations on ongoing research

To do
Finish this section

4.2 The Technical Implementation of QKD

On the technical level, QKD must be distinguished from general Quantum Computing. While QKD systems employ the No-Cloning Theorem and sometimes quantum entanglement in their operation, the scope of their quantum operations is very limited. QKD systems always operate on photons, while general quantum computers use a variety of physical implementations for their qubits that include photons and squeezed light, but extend over atom nuclei, trapped ions, various aspects of currents in superconducters into phonons[2].

To do
I don't like this paragraph.

4.3 Practical Challenges

The central challenge in general quantum computers is extending the lifetime of the quantum state encoding a qubit. Quantum states are extremely sensitive to disturbances, and despite the best efforts to shield their quantum states against external influence, their lifetime is still inconveniently short compared to the timescales required for quantum computation, resulting in significant amounts of noise in the output of quantum algorithms run on contemporary quantum computers. Quantum Key Distribution systems use photons and only perform a handful of operations on each photonic state between generation and measurement, with the vast majority of the state's lifetime spent in transit between the two endpoints of the QKD protocol.

While QKD systems are easy to build and operationally robust compared to general quantum computers, at their core they still exchange information through quantum states that physically need to transit the distance from one endpoint to the other. For classical computer networks, bridging distances of several hundred kilometers is no big challenge. Using appropriate high-power transceivers, a single optical link can already bridge upwards of 100km. Longer ranges can easily be achieved by either logically chaining multiple links, or by using optical amplifiers.

To do
Citation on distance

In contrast, the quantum states at the core of QKD systems must necessarily be "weak". A single quantum state on the wire on average must consist of approximately a single photon. If the system's quantum states consisted of more than one photon carrying the same information, this would enable a *Photon Number Splitting Attack*, in which an attacker extracts one of the state's photons for later analysis, and forwards the remaining photons to the receiver. The attacker can then later measure the captured photon to

extract the same information that the receiver measured.

The practical implication of this is that the optical brightness of a QKD system is directly proportional to the rate at which the system can prepare, and later measure the individual quantum states. With today's electronics, rates up to a few GHz are feasible. Alas, this brightness limit interacts poorly with the reality of optical communication, especially through fibers. Even modern, high-quality fiber-optic cables have attenuation in the order of 0.5 $\frac{\text{dB}}{\text{km}}$, which corresponds to roughly half of the signal being lost every 5 km. In classical optical networks, this can be compensated by increasing transmit power–i.e. packing more photons into each bit–or by optically amplifying the signal partway through the fiber. In QKD systems however, the signal cannot be amplified, and the system's bit rate exponentially decreases with distance due to absorption. Some QKD systems can reach ranges of several hundred kilometer, but the useable data rate (here called *key rate*) of these systems usually is in the kilobits per second or worse.

QKD signals cannot be amplified because their security rests on the fact that each transmitted quantum state on average only contains on the order of one photon each. Security rests on the No-Cloning Theorem, which implies that not just attackers, but even the system's operators are unable to duplicate the quantum state in flight without destroying it.

When transmitted over a fiber, there are multiple effects that degrade the quantum-optical signal of a QKD system. We can coarsely classify these degrading effects into two categories: *Decoherence*, and *Absorption*. Decoherence effects result in the quantum state being changed in transit, which depending on the QKD implementation may mean destroying information contained within the state such as by disturbing the pulse's polarization, or destruction of entanglement between the in-flight state and another local state. In an optical channel affected by such decoherence effects, a quantum state enters the channel, and subsequently exits it at the other end changed. In contrast, absorption means the quantum state is not ever leaving the channel.

In practice, absorption limits the length of an individual fiber run, as it becomes problematic at short distances. Decoherence is less relevant for the distance limitation, and mostly limits which fiber-optic technologies can be utilized in the first place. Due to decoherence, QKD systems usually use Single-Mode (SM) fiber over Multi-Mode (MM) fiber, and makes it more difficult to utilize Wavelength Division Multiplexing (xWDM) to send

multiple either quantum or classical optical signals through a single fiber.

To do
go more into the details on xWDM, elaborate on decoherence mechanisms, especially crosstalk in the context of xWDM.

4.4 Relaying

The No-Cloning Theorem prevents us from using conventional optical amplifiers to extend the range of a single continuous QKD link. What remains as ways to extend the range of a QKD link are *relaying* methods, where one QKD link is terminated at the relay, and another is started, with the relay proxying information between the two. We can separate relay implementations into two broad categories.

To do
CV-QKD

To do
(one?) term of the art seems to be "repeater"

To do
mention that one MDI-QKD range doubling hack

Classical relays encompass the trivial implementation of a relay, where the QKD link is formed by simply stitching two QKD links together by connecting one link's receiver to the other link's transmitter. The key characteristic of classical relays is that inside the relay, the link's cryptographic payload information is handled in its classical plaintext form. Classical relays are practically feasible, but because they must handle the payload in plaintext form, they are security-critical.

Quantum relays are relays that forward the QKD payload information from one link to the other in the quantum realm, without translating it to classical information and back. QKD relays are currently not practically feasible, but if they become available in the future, they would allow range extension without compromising the QKD link's security as the same tamper-detecting properties that the QKD links provide can be extended to cover the quantum forwarding process inside the relay.

5 Quantum Networking

So far we have focused on the range limitation of a single QKD link with classical relays as the only practical solution at this point in time. Quantum Networks naturally follow from a relay-assisted QKD link, if we consider a type of "relay" that is connected to more than two links. Just like switches and routers can be meshed to construct complex topologies in classical wide-area networks (WANs), such multi-fanout relays, or *routers* can be used to provide QKD services over complex network topologies.

There exists a large corpus of academic research on the theory of such large-scale QKD networks ranging from the technical implementation of

management protocols to specialized QKD systems for QKD networks that improve on standard two-party QKD in areas such as complexity or performance. In the past decades, a number of proof-of-concept QKD networks have been put into practice. None of these systems provide any practical utility yet, and their raison d'être lies in the political realm more than it arises out of technical necessity considering that any of today's city-scale demonstrations can easily be simulated more compactly in a lab using a few spools of fiber as a near-perfect stand-in for long-range fiber links.

To do
lots of citations here

Many of the technical challenges in the deployment of QKD networks coincide with similar technical challenges in classical packet-switched networks. An unique challenge to QKD networks is how their routing problem is different to the one in classical computer networks. In a classical network, each link has a known, fixed capacity. A router decides which packet to send through which link, and when the rate of incoming packets momentarily exceeds the capacity of the outgoing links, packets must either be dropped, or put into a growing queue. QKD networks are different in that information is not exchanged through the network, but instead the network *generates* information in the form of secret key material. The measurement of individual pulses that underly key generation conform to a stochastic process, but amortized across the large time spans required for the subsequent selection and privacy amplification steps that converts these raw measurements into usable secret key bits, key generation rate is constant. Each node of a QKD network thus accumulates secret key bits for each of its links, storing them for later use. The routing problem in this scenario revolves around managing the levels of these key stores to avoid depletion.

6 Securing QKD Networks with Inertial HSMs

As we discussed above, when it comes down to practical, end-to-end security properties, Quantum Key Distribution removes trust in the hardness of particular mathematical problems (good!), but increases trust in the physical integrity of the transceivers of the QKD link (bad!). In scenarios where the communicating parties are all located within physical proximity–in QKD, meaning within at most a few hundred kilometers from each other depending on secret key rate requirements–this added trust is of no consequence because the communcating parties' hardware must be trusted in either QKD-assisted or purely classical setups. However, this trust requirement becomes

a burden as soon as at least one party is too far away (or higher secret key rates are required), as now physically trusted relays become necessary.

Extrapolating to practical deployments, we can make two predictions. First, as QKD only solves key distribution, but the actual data transfer still happens through normal off-the-shelf telecommunications components in QKD networks, there is no reason for a practical QKD setup to *not* also use classical cryptography as an additional layer for defense in depth, meaning the QKD setup will at worst degrade to the same security a purely classical system would provide, never less.

To do
citation on defense in depth, and on this hybrid scenario

The second prediction we can make is that any practical QKD network will have to use trusted relays to bridge large distances. While in certain specialized applications such as the proposed financial QKD network in Switzerland smaller, isolated networks are conceivable, in every telecommunication system from the telegraph through the telephone system and up to the internet it has been shown conclusively that there is a real demand for a global, interconnected network[4][9].

To do
citation on swiss deployment

To do
at least one more citation on historic networks

In this section, we will outline a solution that provides practical, end-to-end security in large-scale QKD networks by delegating the hardware trust issue of QKD relays to Inertial Hardware Security Modules. The primary design challenges we will address are the systems' overall envelope design, optical passthroughs, and matching the cryptographic assumptions behind the IHSM's heartbeat and alarm subsystem to those of the QKD application.

6.1 The anatomy of a QKD node

With the exception of special cases such as the middle node in a MDI-QKD system, a general QKD relay contains the same components that the endpoint of a QKD connection uses. Only in a QKD relay, two transceivers are connected back-to-back to one another. QKD provides physical security for the photons traversing the fiber that forms the systme's channel, and the security envelope of the system begins where this fiber is terminated in the power splitters, single-photon detectors, lasers, and interferometers of the QKD transmitter and receiver. To process the raw measurements of the

[4]In fact, history repeats, and the enthusiasm that Quantum Key Distribution networks have kindled parallels the one that the first trans-atlantic telegraph cables brought forth as described by Müller [9]. Both parallel not just in the extensive promises attributed to their respective technologies, but also in the facade of technological determinism that in both cases hides a number of social and political motivations.

QKD system into a usable stream of secret key bits, in addition to these components implementing the physics of the QKD system, a classical computer is needed. On top of the remote monitoring and management tasks that any piece of networking equipment is expected to perform nowadays, this computer is tasked with the information reconciliation and privacy amplification that form the information-theoretic part of the QKD system. Since this computer must necessarily handle secret key bits in their plain text form, it, too, must be inside the relay node's physical protection envelope.

6.2 Physical requirements of QKD transceivers

Putting a QKD relay node and associated machinery inside of an IHSM, we first need to answer two key questions. First, *will it fit?*, and second, *Can we hook it up?*. In the following paragraphs, we will go through several aspects of these general questions one by one.

Physical dimensions. At this point, a number of commercial systems promising QKD exist. Common QKD protocols do not require any particularly large or power-hungry components, and so commercial systems have generally adopted the 19 Inch rackmount enclosure standard that is common to modern telecommunications equipment, with a width of $\approx 50\,\mathrm{cm}$, a height between $\approx 4\,\mathrm{cm}$ to $30\,\mathrm{cm}$ and a depth below $\approx 100\,\mathrm{cm}$. While something of this size would be infeasible to protect with the security mesh of a traditional hardware security module, placed vertically, even without modifications any of these systems are well within an envelope that can be protected with a single IHSM cage.

To do
Re-check these numbers shortly before submission

Power supply. QKD systems do not contain any particularly power-hungry components. Unlike quantum computers, most of the signal path is optical, and as such can be implemented with room-temperature fiber-optic components. Only the single-photon detectors may require cooling in some systems, but unlike something like an ion trap quantum computer's processor, energy-intensive deep cryogenic cooling is not necessary. Most manufacturers don't quote the power requirements of their systems, but we were able to find that IDQuantique specifies their QKD systems to be able to run off a single 300 W power supply. In an intertial HSM, power up

to several kW can easily be transferred to the payload with through-axis cables.

Cooling. While the few hundred watt of power that QKD systems require could easily be transported through the mesh of a a traditional HSM as well, cooling that amount of thermal load purely by heat conduction through centimeters of epoxy resin would make implementation infeasible in traditional HSM. In an IHSM, on the other hand, up to several kW can easily be dissipated through forced-air cooling since the rotating security mesh can have an arbitrary amount of longitudinal slots or holes.

Data and signals. A QKD transceiver has a number of ports in addition the port for the fiber optic quantum channel. Depending on the system, one or more additional optical links may be necessary for clock distribution, allowing both endpoints to tune their lasers into precise alignment. QKD protocols require a classical link used for information reconciliation, which along with the key stream output and management links requires one or more classical network ports.

In a QKD relay node, the key stream never leaves the security envelope. The management and information reconciliation links can be combined into a single, classical network link, requiring a single fiber when using a standard wavelength division multiplexing transceiver. The QKD link's clock channel and the quantum channel require a dedicated fiber each, adding up to a total of five fibers for a uni-directional QKD relay, or nine fibers for a bidirectional one. Since fiber pigtails have an outer diameter of usually about 1 mm, this amount of fibers can be fed through an IHSM's axis of rotation. The mechanical challenge in such a multi-fiber signal and data feedthrough is to observe the fiber's minimum bending radius, which for common fibers is usually in the range of 5 mm to 10 mm .

To do
Provide citation on bend radius. Maybe a small table of products by a few vendors?

Concluding the above paragraphs, a QKD node is not a particularly challenging payload for an IHSM. The most problematic requirement is feeding through a number of fibers for its various input and output signals, but fundamentally it is no different from any server or other piece of IT equipment. In the following section, we will present a design that provides a combined power and multi-fiber passthrough that is sufficient for QKD applications.

6.3 Multi-fiber passthrough with active secondary mesh

7 Outlook

Bibliography

[1] Khashayar Barooti et al. "Public-Key Encryption with Quantum Keys". In: *Theory of Cryptography*. Ed. by Guy Rothblum and Hoeteck Wee. Cham: Springer Nature Switzerland, 2023, pp. 198–227. DOI: 10.1007/978-3-031-48624-1_8.

[2] Eduardo Berrios et al. "High Fidelity Quantum Gates with Vibrational Qubits". In: *The Journal of Physical Chemistry A* 116.46 (Nov. 26, 2012), pp. 11347–11354. DOI: 10.1021/jp3055729.

[3] Karthikeyan Bhargavan and Gaëtan Leurent. "On the Practical (In-)Security of 64-Bit Block Ciphers: Collision Attacks on HTTP over TLS and OpenVPN". In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. CCS'16: 2016 ACM SIGSAC Conference on Computer and Communications Security. Vienna Austria: ACM, Oct. 24, 2016, pp. 456–467. DOI: 10.1145/2976749.2978423.

[4] Khodakhast Bibak and Robert Ritchie. "Quantum Key Distribution with PRF(Hash, Nonce) Achieves Everlasting Security". In: *Quantum Information Processing* 20.7 (July 2021), p. 228. DOI: 10.1007/s11128-021-03164-3.

[5] Wouter Castryck and Thomas Decru. "An Efficient Key Recovery Attack on SIDH". In: *Advances in Cryptology – EUROCRYPT 2023*. Ed. by Carmit Hazay and Martijn Stam. Vol. 14008. Cham: Springer Nature Switzerland, 2023, pp. 423–447. DOI: 10.1007/978-3-031-30589-4_15.

[6] Alex B. Grilo et al. "Oblivious Transfer Is in MiniQCrypt". In: *Advances in Cryptology – EUROCRYPT 2021*. Ed. by Anne Canteaut and François-Xavier Standaert. Cham: Springer International Publishing, 2021, pp. 531–561. DOI: 10.1007/978-3-030-77886-6_18.

[7] R. Impagliazzo. “A Personal View of Average-Case Complexity”. In: *Proceedings of Structure in Complexity Theory. Tenth Annual IEEE Conference*. Structure in Complexity Theory. Tenth Annual IEEE Conference. Minneapolis, MN, USA: IEEE Comput. Soc. Press, 1995, pp. 134–147. DOI: 10.1109/SCT.1995.514853.

[8] Gaurav Kodwani, Shashank Arora, and Pradeep K. Atrey. “On Security of Key Derivation Functions in Password-based Cryptography”. In: *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*. 2021 IEEE International Conference on Cyber Security and Resilience (CSR). Rhodes, Greece: IEEE, July 26, 2021, pp. 109–114. DOI: 10.1109/CSR51186.2021.9527961.

[9] Simone Müller. *Wiring the World: The Social and Cultural Creation of Global Telegraph Networks*. Columbia University Press, Apr. 12, 2016. DOI: 10.7312/mlle17432.

[10] Sophie Schmieg, Stefan Kölbl, and Guillaume Endignoux. *Google's Threat Model for Post-Quantum Cryptography*. Google's Threat model for Post-Quantum Cryptography. Mar. 11, 2024. URL: https://bughunters.google.com/blog/5108747984306176/google-s-threat-model-for-post-quantum-cryptography (visited on 06/27/2024).