SAMPLE

Quantum Cryptography

Unbreakable Codes

Aira Astralis

Free sample: Chapter 1

putrabooks.github.io

Buy the full book:

Gumroad

Payhip

Contents

Chapter 1: The Discovery of Quantum Cryptography

Chapter 2: Understanding Quantum Cryptography

Chapter 3: Key Characteristics of Quantum Cryptography

Chapter 4: The Science Behind Quantum Cryptography

Chapter 5: Observation and Measurement of Quantum Cryptography

Chapter 6: Important Features of Quantum Cryptography

Chapter 7: Quantum Cryptography in Context

Chapter 8: Modern Understanding of Quantum Cryptography

Chapter 9: Research and Exploration of Quantum Cryptography

Chapter 10: Challenges and Mysteries of Quantum Cryptography

Chapter 11: Future Directions in Quantum Cryptography Research

Chapter 12: Fun Facts and Trivia About Quantum Cryptography

Chapter 13: Conclusion: The Significance of Quantum Cryptography

Chapter 14: Conclusion: The Significance of Quantum Cryptography

Chapter 1: The Discovery of Quantum Cryptography

Independently, in 1991 Artur Ekert proposed to use Bell's inequalities to achieve secure key distribution. Ekert's protocol for the key distribution, as it was subsequently shown by Dominic Mayers and Andrew Yao, offers device-independent quantum key distribution. Companies that manufacture quantum cryptography systems include MagiQ Technologies, Inc. Cryptography is the strongest link in the chain of data security. However, interested parties cannot assume that cryptographic keys will remain secure indefinitely.

Quantum cryptography has the potential to encrypt data for longer periods than classical cryptography. Using classical cryptography, scientists cannot guarantee encryption beyond approximately 30 years, but some stakeholders could use longer periods of protection. Take, for example, the healthcare industry. As of 2017, 85.9% of office-based physicians are using electronic medical record systems to store and transmit patient data. Under the Health Insurance Portability and Accountability Act, medical records must be kept secret.

Quantum key distribution can protect electronic records for periods of up to 100 years. Also, quantum cryptography has useful applications for governments and militaries as, historically, governments have kept military data secret for periods of over 60 years. There also has been proof that quantum key distribution can travel through a noisy channel over a long distance and be secure. It can be reduced from a noisy quantum scheme to a classical noiseless scheme. This can be solved with classical probability theory.

This process of having consistent protection over a noisy channel can be possible through the implementation of quantum repeaters. Quantum repeaters have the ability to resolve quantum communication errors in an efficient way. Quantum repeaters, which are quantum computers, can be stationed as segments over the noisy channel to ensure the security of communication. Quantum repeaters do this by purifying the segments of the channel before connecting them creating a secure line of communication.

Sub-par quantum repeaters can provide an efficient amount of security through the noisy channel over a long distance. Quantum cryptography is a general subject that covers a broad range of cryptographic practices and protocols. While encryption techniques are widely recognized and understood, a significant challenge remains in the secure distribution of shared keys, often referred to as key establishment or key agreement. Quantum Key Distribution (QKD) aims to address this particular challenge.

Below, we explore various notable methodologies and applications currently employed in quantum cryptography.

The best-known and developed application of quantum cryptography is QKD, which is the process of using quantum communication to establish a shared key between two

parties (Alice and Bob, for example) without a third party (Eve) learning anything about that key, even if Eve can eavesdrop on all communication between Alice and Bob. If Eve tries to learn information about the key being established, discrepancies will arise causing Alice and Bob to notice.

Once the key is established, it is then typically used for encrypted communication using classical techniques. For instance, the exchanged key could be used for symmetric cryptography (e.g. The security of quantum key distribution can be proven mathematically without imposing any restrictions on the abilities of an eavesdropper, something not possible with classical key distribution.

This is usually described as "unconditional security", although there are some minimal assumptions required, including that the laws of quantum mechanics apply and that Alice and Bob are able to authenticate each other, i.e. Eve should not be able to impersonate Alice or Bob as otherwise a man-in-the-middle attack would be possible. While QKD is secure, its practical application faces some challenges. There are in fact limitations for the key generation rate at increasing transmission distances.

Recent studies have allowed important advancements in this regard.

In 2018, the protocol of twin-field QKD was proposed as a mechanism to overcome the limits of lossy communication. The rate of the twin field protocol was shown to overcome the secret key-agreement capacity of the lossy communication channel, known as repeater-less PLOB bound, at 340 km of optical fiber; its ideal rate surpasses this bound already at 200 km and follows the rate-loss scaling of the higher repeater-assisted secret key-agreement capacity (see figure 1 of and figure 11 of for more details).

The protocol suggests that optimal key rates are achievable on "550 kilometers of standard optical fibre", which is already commonly used in communications today. The theoretical result was confirmed in the first experimental demonstration of QKD beyond the PLOB bound which has been characterized as the first effective quantum repeater. Notable developments in terms of achieving high rates at long distances are the sending-not-sending (SNS) version of the TF-QKD protocol.

In mistrustful cryptography the participating parties do not trust each other. For example, Alice and Bob collaborate to perform some computation where both parties enter some private inputs. But Alice does not trust Bob and Bob does not trust Alice. Thus, a secure implementation of a cryptographic task requires that after completing the computation, Alice can be guaranteed that Bob has not cheated and Bob can be guaranteed that Alice has not cheated either.

Examples of tasks in mistrustful cryptography are commitment schemes and secure computations, the latter including the further examples of coin flipping and oblivious transfer. Key distribution does not belong to the area of mistrustful cryptography. Mistrustful quantum cryptography studies the area of mistrustful cryptography using quantum systems.

The goal of position-based quantum cryptography is to use the geographical location

of a player as its (only) credential.

The notion of using quantum effects for location verification first appeared in the scientific literature in 2010.

Currently, research is being conducted mainly in Japan and China: e.g. The principle of operation is as follows. Wyner is implemented.

The actual security provided by a QKD system is not the theoretical unconditional security from the laws of physics (as modeled and often suggested), but rather the more limited security that can be achieved by hardware and engineering designs.

Chapter 2: Understanding Quantum Cryptography

In contrast to quantum key distribution where unconditional security can be achieved based only on the laws of quantum physics, in the case of various tasks in mistrustful cryptography there are no-go theorems showing that unconditionally secure protocols cannot be built from quantum theory alone. However, some of these tasks can be implemented with unconditional security if the protocols not only exploit quantum mechanics but also special relativity.

For example, unconditionally secure quantum bit commitment was shown impossible by Mayers and by Lo and Chau. Unconditionally secure ideal quantum coin flipping was shown impossible by Lo and Chau. Moreover, Lo showed that there cannot be unconditionally secure quantum protocols for one-out-of-two oblivious transfer and other secure two-party computations. However, unconditionally secure relativistic protocols for coin flipping and bit-commitment have been shown by Kent.

Unlike quantum key distribution, quantum coin flipping is a protocol that is used between two participants who do not trust each other. The participants communicate via a quantum channel and exchange information through the transmission of qubits. But because Alice and Bob do not trust each other, each expects the other to cheat. Therefore, more effort must be spent on ensuring that neither Alice nor Bob can gain a significant advantage over the other to produce a desired outcome.

An ability to influence a particular outcome is referred to as a bias, and there is a significant focus on developing protocols to reduce the bias of a dishonest player, otherwise known as cheating. Quantum communication protocols, including quantum coin flipping, have been shown to provide significant security advantages over classical communication, though they may be considered difficult to realize in the practical world.

A coin flip protocol generally occurs like this: Alice chooses a basis (either rectilinear or diagonal) and generates a string of photons to send to Bob in that basis. Bob randomly chooses to measure each photon in a rectilinear or diagonal basis, noting which basis he used and the measured value. Bob publicly guesses which basis Alice used to send her qubits. Alice announces the basis she used and sends her original string to Bob. Bob confirms by comparing Alice's string to his table.

It should be perfectly correlated with the values Bob measured using Alice's basis and completely uncorrelated with the opposite. Cheating occurs when one player attempts to influence, or increase the probability of a particular outcome.

The protocol discourages some forms of cheating; for example, Alice could cheat at step 4 by claiming that Bob incorrectly guessed her initial basis when he guessed correctly, but Alice would then need to generate a new string of qubits that perfectly correlates with what Bob measured in the opposite table. Her chance of generating a matching string of qubits will decrease exponentially with the number of qubits sent, and if Bob notes a mismatch, he will know she was lying.

Alice could also generate a string of photons using a mixture of states, but Bob would easily see that her string will correlate partially (but not fully) with both sides of the table, and know she cheated in the process. There is also an inherent flaw that comes with current quantum devices. Errors and lost qubits will affect Bob's measurements, resulting in holes in Bob's measurement table. Significant losses in measurement will affect Bob's ability to verify Alice's qubit sequence in step 5.

One theoretically surefire way for Alice to cheat is to utilize the Einstein-Podolsky-Rosen (EPR) paradox. Two photons in an EPR pair are anticorrelated; that is, they will always be found to have opposite polarizations, provided that they are measured in the same basis. Alice could generate a string of EPR pairs, sending one photon per pair to Bob and storing the other herself.

When Bob states his guess, she could measure her EPR pair photons in the opposite basis and obtain a perfect correlation to Bob's opposite table. Bob would never know she cheated. However, this requires capabilities that quantum technology currently does not possess, making it impossible to do in practice. To successfully execute this, Alice would need to be able to store all the photons for a significant amount of time as well as measure them with near perfect efficiency.

This is because any photon lost in storage or in measurement would result in a hole in her string that she would have to fill by guessing. The more guesses she has to make, the more she risks detection by Bob for cheating. In addition to quantum coin-flipping, quantum commitment protocols are implemented when distrustful parties are involved.

A commitment scheme allows a party Alice to fix a certain value (to "commit") in such a way that Alice cannot change that value while at the same time ensuring that the recipient Bob cannot learn anything about that value until Alice reveals it. Such commitment schemes are commonly used in cryptographic protocols (e.g. Quantum coin flipping, Zero-knowledge proof, secure two-party computation, and Oblivious transfer).

Chapter 3: Key Characteristics of Quantum Cryptography

Quantum mechanics, remarkably, completes this toolkit: as Crépeau and Kilian demonstrated, an unconditionally secure protocol for oblivious transfer can be built from nothing more than a commitment scheme and a quantum channel, and Kilian had already established that oblivious transfer is the universal ingredient of distributed computing, since almost any secure multi-party computation can be implemented from it.

This is because the results do not guarantee "composability", that is, when plugging them together, one might lose security.) Early quantum commitment protocols were shown to be flawed. In fact, Mayers showed that (unconditionally secure) quantum commitment is impossible: a computationally unlimited attacker can break any quantum commitment protocol.

Yet, the result by Mayers does not preclude the possibility of constructing quantum commitment protocols (and thus secure multi-party computation protocols) under assumptions that are much weaker than the assumptions needed for commitment protocols that do not use quantum communication. The bounded quantum storage model described below is an example for a setting in which quantum communication can be used to construct commitment protocols.

A breakthrough in November 2013 offers "unconditional" security of information by harnessing quantum theory and relativity, which has been successfully demonstrated on a global scale for the first time. More recently, Wang et al., proposed another commitment scheme in which the "unconditional hiding" is perfect. Physical unclonable functions can be also exploited for the construction of cryptographic commitments. One possibility to construct unconditionally secure quantum commitment and quantum oblivious transfer (OT) protocols is to use the bounded quantum storage model (BQSM).

In this model, it is assumed that the amount of quantum data that an adversary can store is limited by some known constant Q. However, no limit is imposed on the amount of classical (i.e., non-quantum) data the adversary may store. In the BQSM, one can construct commitment and oblivious transfer protocols. The underlying idea is the following: The protocol parties exchange more than Q quantum bits (qubits).

Since even a dishonest party cannot store all that information (the quantum memory of the adversary is limited to Q qubits), a large part of the data will have to be either measured or discarded. Forcing dishonest parties to measure a large part of the data allows the protocol to circumvent the impossibility result, commitment and oblivious transfer protocols can now be implemented.

The protocols in the BQSM presented by Damgård, Fehr, Salvail, and Schaffner do not assume that honest protocol participants store any quantum information; the technical requirements are similar to those in quantum key distribution protocols. These protocols can thus, at least in principle, be realized with today's technology. The communication complexity is only a constant factor larger than the bound Q on the adversary's quantum memory.

The advantage of the BQSM is that the assumption that the adversary's quantum

memory is limited is quite realistic.

With today's technology, storing even a single qubit reliably over a sufficiently long time is difficult. By introducing an artificial pause in the protocol, the amount of time over which the adversary needs to store quantum data can be made arbitrarily large.) An extension of the BQSM is the noisy-storage model introduced by Wehner, Schaffner and Terhal.

Instead of considering an upper bound on the physical size of the adversary's quantum memory, an adversary is allowed to use imperfect quantum storage devices of arbitrary size. The level of imperfection is modelled by noisy quantum channels. For high enough noise levels, the same primitives as in the BQSM can be achieved and the BQSM forms a special case of the noisy-storage model.

In the classical setting, similar results can be achieved when assuming a bound on the amount of classical (non-quantum) data that the adversary can store. It was proven, however, that in this model also the honest parties have to use a large amount of memory (namely the square-root of the adversary's memory bound). This makes these protocols impractical for realistic memory bounds.

For example, one wants to send a message to a player at a specified position with the guarantee that it can only be read if the receiving party is located at that particular position.

In the basic task of position-verification, a player, Alice, wants to convince the (honest) verifiers that she is located at a particular point. It has been shown by Chandran et al. Under various restrictions on the adversaries, schemes are possible. Under the name of 'quantum tagging', the first position-based quantum schemes have been investigated in 2002 by Kent. A US-patent was granted in 2006.

Chapter 4: The Science Behind Quantum Cryptography

The idea of verifying a party's position by quantum effects entered the scientific literature in 2010, and the same year brought several further protocols for the task, after which Buhrman et al.

However, this result does not exclude the possibility of practical schemes in the bounded- or noisy-quantum-storage model (see above).

Later Beigi and König improved the amount of EPR pairs needed in the general attack against position-verification protocols to exponential. They also showed that a particular protocol remains secure against adversaries who controls only a linear amount of EPR pairs. It is argued in that due to time-energy coupling the possibility of formal unconditional location verification via quantum effects remains an open problem.

The study of position-based quantum cryptography also has connections with the

protocol of port-based quantum teleportation, which is a more advanced version of quantum teleportation, where many EPR pairs are simultaneously used as ports. A quantum cryptographic protocol is device-independent if its security does not rely on trusting that the quantum devices used are truthful. Thus the security analysis of such a protocol needs to consider scenarios of imperfect or even malicious devices.

Mayers and Yao proposed the idea of designing quantum protocols using "self-testing" quantum apparatus, the internal operations of which can be uniquely determined by their input-output statistics. Subsequently, Roger Colbeck in his Thesis proposed the use of Bell tests for checking the honesty of the devices. Since then, several problems have been shown to admit unconditional secure and device-independent protocols, even when the actual devices performing the Bell test are substantially "noisy", i.e., far from being ideal.

These problems include quantum key distribution, randomness expansion, and randomness amplification. In 2018, theoretical studies performed by Arnon- Friedman et al. Cryptographically-relevant quantum computers may become a technological reality; it is therefore important to study cryptographic schemes used against adversaries with access to a quantum computer.

The study of such schemes is often referred to as post-quantum cryptography. The need for post-quantum cryptography arises from the fact that many popular encryption and signature schemes, mainly those based on ECC and RSA, can be broken using Shor's algorithm for factoring and computing discrete logarithms on a quantum computer. Examples for schemes that are, as of today's knowledge, secure against quantum adversaries are McEliece and lattice-based schemes, as well as most symmetric-key algorithms. Surveys of post-quantum cryptography are available.

Additional research was made into how existing cryptographic techniques have to be modified to be able to cope with quantum adversaries. For example, when trying to develop zero-knowledge proof systems that are secure against quantum adversaries, new techniques need to be used: In a classical setting, the analysis of a zero-knowledge proof system usually involves "rewinding", a technique that makes it necessary to copy the internal state of the adversary.

In a quantum setting, copying a state is not always possible (no-cloning theorem); a variant of the rewinding technique has to be used. Post-quantum algorithms are also called "quantum resistant", because – unlike quantum key distribution – it is not known or provable that there will not be potential future quantum attacks against them. Even though they may possibly be vulnerable to quantum attacks in the future, the NSA is announcing plans to transition to quantum resistant algorithms.

The National Institute of Standards and Technology (NIST) believes that it is time to think of quantum-safe primitives. Historically, quantum cryptography has been closely associated with the development of quantum key distribution (QKD), which enables two distant parties to establish a shared secret key with information-theoretic security. While QKD addresses the fundamental problem of secure key establishment, it does not by itself provide solutions to many other important cryptographic tasks,

such as public-key encryption, digital signatures, authentication, or secure computation.

Moreover, in large communication networks, pairwise secret-key establishment and management may become increasingly demanding. These considerations have motivated the development of a broader range of quantum cryptographic primitives and protocols that extend quantum cryptography well beyond key distribution. Besides quantum commitment and oblivious transfer (discussed above), modern quantum cryptography encompasses a broad range of primitives beyond key distribution.

These include quantum message authentication, quantum digital signatures, quantum one-way functions, one-way state generators and public-key encryption, quantum key-exchange, quantum fingerprinting and entity authentication (for example, see Quantum readout of PUFs), etc. Some of these primitives derive their security from computational assumptions, while others exploit fundamental properties of quantum information, such as the no-cloning theorem, the Holevo bound, and the impossibility of perfectly distinguishing non-orthogonal quantum states. H. P.

Yuen presented Y-00 as a stream cipher using quantum noise around 2000 and applied it for the U.S. Defense Advanced Research Projects Agency (DARPA) High-Speed and High-Capacity Quantum Cryptography Project as an alternative to quantum key distribution. The review paper summarizes it well. Unlike quantum key distribution protocols, the main purpose of Y-00 is to transmit a message without eavesdrop-monitoring, not to distribute a key. Therefore, privacy amplification may be used only for key distributions.

Chapter 5: Observation and Measurement of Quantum Cryptography

Today the bulk of deployed QKD engineering comes out of Japan and China, and the operating principle of these systems is straightforward: legitimate users share a key and stretch it into a pseudo-random keystream with a common pseudo-random number generator. Then, the legitimate parties can perform conventional optical communications based on the shared key by transforming it appropriately.

For attackers who do not share the key, the wire-tap channel model of Aaron D. Wyner is implemented. The legitimate users' advantage based on the shared key is called "advantage creation". The goal is to achieve longer covert communication than the information-theoretic security limit (one-time pad) set by Shannon. The source of the noise in the above wire-tap channel is the uncertainty principle of the electromagnetic field itself, which is a theoretical consequence of the theory of laser described by Roy J.

C. George Sudarshan (coherent state). Therefore, existing optical communication technologies are sufficient for implementation that some reviews describes: e.g. Furthermore, since it uses ordinary communication laser light, it is compatible with

existing communication infrastructure and can be used for high-speed and long-distance communication and routing. Although the main purpose of the protocol is to transmit the message, key distribution is possible by simply replacing the message with a key.

Since it is a symmetric key cipher, it must share the initial key previously; however, a method of the initial key agreement was also proposed. On the other hand, it is currently unclear what implementation realizes information-theoretic security, and security of this protocol has long been a matter of debate. In theory, quantum cryptography seems to be a successful turning point in the information security sector. However, no cryptographic method can ever be absolutely secure.

In practice, quantum cryptography is only conditionally secure, dependent on a key set of assumptions. The theoretical basis for quantum key distribution assumes the use of single-photon sources. However, such sources are difficult to construct, and most real-world quantum cryptography systems use faint laser sources as a medium for information transfer. These multi-photon sources open the possibility for eavesdropper attacks, particularly a photon splitting attack. An eavesdropper, Eve, can split the multi-photon source and retain one copy for herself.

The other photons are then transmitted to Bob without any measurement or trace that Eve captured a copy of the data. Scientists believe they can retain security with a multi-photon source by using decoy states that test for the presence of an eavesdropper. However, in 2016, scientists developed a near perfect single photon source and estimate that one could be developed in the near future. In practice, multiple single-photon detectors are used in quantum key distribution devices, one for Alice and one for Bob.

These photodetectors are tuned to detect an incoming photon during a short window of only a few nanoseconds. Due to manufacturing differences between the two detectors, their respective detection windows will be shifted by some finite amount. An eavesdropper, Eve, can take advantage of this detector inefficiency by measuring Alice's qubit and sending a "fake state" to Bob. Eve first captures the photon sent by Alice and then generates another photon to send to Bob.

Eve manipulates the phase and timing of the "faked" photon in a way that prevents Bob from detecting the presence of an eavesdropper. The only way to eliminate this vulnerability is to eliminate differences in photodetector efficiency, which is difficult to do given finite manufacturing tolerances that cause optical path length differences, wire length differences, and other defects. Given the practical challenges raised below, several organizations recommend using "post-quantum cryptography (or quantum-resistant cryptography)" instead of quantum key distribution.

USA National Security Agency, European Union Agency for Cybersecurity of EU (ENISA), United Kingdom's National Cyber Security Centre, French Secretariat for Defense and Security (ANSSI), German Federal Office for Information Security (BSI)

Australia's ASD

Netherland National Communications Security Agency (NLNCSA) and Swedish National Communications Security Authority, Swedish Armed Forces For example, the US National Security Agency addresses five issues: Quantum key distribution is only a partial solution. QKD generates keying material for an encryption algorithm that provides confidentiality. Such keying material could also be used in symmetric key cryptographic algorithms to provide integrity and authentication if one has the cryptographic assurance that the original QKD transmission comes from the desired entity (i.e.

QKD does not provide a means to authenticate the QKD transmission source. Therefore, source authentication requires the use of asymmetric cryptography or pre-placed keys to provide that authentication. Moreover, the confidentiality services QKD offers can be provided by quantum-resistant cryptography, which is typically less expensive with a better understood risk profile. Quantum key distribution requires special purpose equipment. QKD is based on physical properties, and its security derives from unique physical layer communications.

This requires users to lease dedicated fiber connections or physically manage free-space transmitters. It cannot be implemented in software or as a service on a network, and cannot be easily integrated into existing network equipment. Since QKD is hardware-based it also lacks flexibility for upgrades or security patches. Quantum key distribution increases infrastructure costs and insider-threat risks. QKD networks frequently necessitate the use of trusted relays, entailing additional cost for secure facilities and additional security risk from insider threats.

This eliminates many use cases from consideration. Securing and validating quantum key distribution is a significant challenge.

Chapter 6: Important Features of Quantum Cryptography

In practice, a deployed QKD installation delivers less than the unconditional guarantee its physics suggests: what a customer actually buys is bounded by hardware and engineering, not by the laws of nature alone.

The tolerance for error in cryptographic security, however, is many orders of magnitude smaller than what is available in most physical engineering scenarios, making it very difficult to validate. The specific hardware used to perform QKD can introduce vulnerabilities, resulting in several well-publicized attacks on commercial QKD systems. Quantum key distribution increases the risk of denial of service. The sensitivity to an eavesdropper as the theoretical basis for QKD security claims also shows that denial of service is a significant risk for QKD.

In response to problem 1 above, proposals have appeared worldwide for delivering authentication keys with algorithms of the post-quantum, quantum-resistant class. On the other hand, quantum-resistant cryptography is cryptography belonging to the class of computational security.

ABOUT THE AUTHOR

Aira Astralis is a science writer specializing in astronomy and space exploration. Her work spans the full breadth of humanity's relationship with the cosmos -- from the earliest naked-eye observations to the engineering marvels of modern space missions.

Her books are built on a foundation of primary sources: peer-reviewed research, mission archives, and direct engagement with the scientific community. She writes for readers who want to understand not just what we know about the universe, but how we came to know it.

She believes that the most important frontier is not out there but in the gap between what scientists discover and what the public understands. Her books exist to close that gap.