Literature Review On Quantum Cryptography

by

Mingke Wang

Bachelor

School of Electronic Information
and Electrical Engineering

Shanghai Jiao Tong University

Shanghai, China

2019

Acknowledgments

This thesis is the final project of class EE378, and the main topic I choose is quantum cryptography.

Abstract

In this artical, I mainly talk about what is quantum, how does it related to transmission cryptography, and the drawback of it.

Contents

1. Introduction

1.1 Overview

Rapid development of supercomputers and the prospect of quantum computers are posing increasingly serious threats to the security of communication. Using the principles of quantum cryptography, quantum communication offers provable security of communication and is a promising solution to counter such threats. Quantum cryptography that does not depend on the computer capacity of the adversary but is absolutely guaranteed by the laws of quantum physics, although it is in an initial stage, it is necessary to motivate the work for research purposes in the academic world, industry and society in general is taken as a solid alternative of security.

There is no doubt that QKD has taken the spotlight in terms of the use of quantum information for cryptography (in fact, so much that the term “quantum cryptography” is often equated with QKD—a misconception that we aim to rectify here!); yet there exist many other uses ofquantum information in cryptography. What ismore, quantum information opens up the cryptographic landscape to allow-functionalities that do not exist using classical1 information alone, for example uncloneable quantum money. We note, however, that the use of quantum information in cryptography has its limitations and challenges. For instance, we know that quantum information alone is insufficient to implement information-theoretically secure bit commitment; and that a proof technique called rewinding (which is commonly used in establishing a zero-knowledge property for a protocol) does not directly carry over to the quantum world and must re-visited in light of quantum information.

2. Quantum

2.1 State Space

The bit is the fundamental unit of information for classical information processing. In quantum information processing, the corresponding unit is the qubit, which is described mathematically by a vector of length one in a two-dimensional complex vector space. We use notation from physics to denote vectors that represent quantum states, enclosing vectors in a ket.

2.2 Unitary evolution and circuits

Basic evolutions of a quantum system are described by linear operations that preserve the norm; formally, these operations can be expressed as unitary complex matrices

Quantum algorithms are commonly described as circuits (rather than by quantum Turing matrix machines) consisting of basic quantum gates from a universal set

2.3 measurement

In addition to unitary evolution, we specify an operation called measurement, which, in the simplest case, takes a qubit and outputs a classical bit

We further specify that, after the process of measurement, the quantum system collapses to the measured outcome. Thus, the quantum state is disturbed and it becomes classical: any further measurements have a deterministic outcome. We have described measurement with respect to the standard basis; of course, a measurement can be described according to an arbitrary basis; the probabilities of the outcomes can be computed by first applying the corresponding change-of-basis, followed by the standard basis measurement. Measurements can actually be described much more generally: e.g. we can describe outcomes of measurements of a strict subset of a quantum system-the mathematical formalism to describe the outcomes uses the density matrix formalism, which we do not describe here.Broadbent and Schaffner (2016)

2.4 Quantum no-cloning

One of the most fundamental properties of quantum information is that it is not physically possible, in general, to clone a quantum system (i.e. there is no physical process that takes as input a single quantum system, and outputs two identical copies of its input). A simple proof follows from the linearity of quantum operations.5 At the intuitive level, this principle is present in almost all of quantum cryptography, since it prevents the classical reconstruction of the description of a given qubit system. For instance, given a single copy α and β, because measuring disturbs the state. At the formal level, however, we generally of a general qubit $\alpha|0\rangle+ \beta|1\rangle$, it is not possible to "extract" a full classical description of require more sophisticated tools to prove the security of quantum cryptography protocols

2.5 Quantum entanglement and nonlocality

Acrucial and rather counter-intuitive feature ofquantummechanics is quantum entanglement, a physical phenomenon that occurs when quantum particles behave in such a way that the quantum state of each particle cannot be described individually. A simple example of such an entangled state are two qubits in the state $\frac{(|00\rangle_{AB}+|11\rangle_{AB})}{\sqrt{2}}$. When Alice measures her qubit (in system A), she obtains a random bit $a \in \{0,1\}$ as outcome and her qubit collapses to the state $|a\rangle_A$ she observed. At the same time, Bob's qubit (in system B) also collapses to $|a\rangle_B$ and hence, a subsequent measurement by Bob yields the same outcome $b = a$. It is important to realize that this collapse of state at Bob's side occurs simultaneously with Alice's measurement, but it does not allow the players to send information from Alice to Bob.

It simply provides Alice and Bob with a shared random bit. In general, quantum entanglement does not contradict the fundamental non-signaling principle of the theory of relativity stating that no information can travel faster than the speed of light.

2.6 Quantum cryptographic constructions

Many of quantum cryptographic protocols share the remarkable feature of being based on a very simple pattern of quantum information called conjugate coding. Because of its paramount importance in quantum cryptography, we first present this notion. We then show how conjugate coding is the crucial ingredient in the quantum- cryptographic constructions for quantum money, QKD, a quantum reduction from oblivious transfer to bit commitment, the limited-quantum-storage model and delegated quantum computation. Further topics covered in this section are quantum coin-flipping and device-independent cryptography.

2.7 Essential properties of polarized photons

Polarized light can be produced by sending an ordinary light beam through a polarizing apparatus such as a Polaroid filter or calcite crystal; the beam's polarization axis is determined by the orientation of the polarizing apparatus in which the beam originates. Generating single polarized photons is also possible, in principle by picking them out of a polarized beam, and in practice by a variation of an experiment of Aspect Aspect, Grangier, and Roger (1982) et al.

Although polarization is a continuous variable, the uncertainty principle forbids measurements on any single photon from revealing more than one bit about its polarization. For example, if a light beam with polarization axis α is sent into a filter oriented at angle β, the individual photons behave dichotomously and probabilistically, sorbed with the complementary probability $\sin 2(\alpha\beta)$. being transmitted with probability $\cos 2(\alpha\beta)$ and ab The photons behave deterministically only when the two axes are parallel (certain transmission) or perpendicular (certain absorption).

If the two axes are not perpendicular, so that some photons are transmitted, one might hope to learn additional information about α by measuring the transmitted photons again with a polarizer oriented at some third angle; but this is to no avail, because the transmitted photons, in passing through the β polarizer, emerge with exactly β polarization, having lost all memory of their previous polarization α. Another way one might hope to learn more than one bit from a single photon would be not to measure it directly, but rather somehow amplify it into a clone of identically polarized photons, then perform measurements on these; but this hope is also vain, because such cloning can be shown to be inconsistent with the foundations of quantum mechanicsWootters and Zurek (1982).

3. Quantum Key Distribution

QKD is by far the most successful application of quantum information to cryptography. By now, QKD is the main topic of a large number of surveys.

3.1 Comparsion with Traditional Cryptography

In traditional public-key cryptography, trapdoor functions are used to conceal the meaning of messages between two users from a passive eavesdropper, despite the lack of any initial shared secret information between the two users.

In quantum public key distribution, the quantum channel is not used directly to send meaningful messages, but is rather used to transmit a supply of random bits between two users who share no secret information initially, in such a way that the users, by subsequent consultation over an ordinary non-quantum channel subject to passive eavesdropping, can tell with high probability whether the original quantum transmission has been disturbed in transit, as it would be by an eavesdropper (it is the quantum channel's peculiar virtue to compel eavesdropping to be active). If the transmission has not been disturbed, they agree to use these shared secret bits in the well-known way as a one-time pad to conceal the meaning of subsequent meaningful communications, or for other cryptographic applications (e.g. authentication tags) requiring shared secret random information. If transmission has been disturbed, they discard it and try again, deferring any meaningful communications until they have succeeded in transmitting enough random bits through the quantum channel to serve as a one-time pad.

3.2 Protocol

one user ('Alice') chooses a random bit string and a random sequence of polarization bases (rectilinear or diagonal). She then sends the other user ('Bob') a train of photons, each representing one bit of the string in the basis chosen for that bit position, a horizontal or 45-degree photon standing for a binary zero and a vertical or 135-degree photon standing for a binary 1.

As Bob receives the photons he decides, randomly for each photon and independently of Alice, whether to measure the photon's rectilinear polarization or its diagonal polarization, and interprets the result of the measurement as a binary zero or one. As explained in the previous section a random answer is produced and all information lost when one attempts to measure the rectilinear polarization of a diagonal photon, or vice versa. Thus Bob obtains meaningful data from only half the photons he detects—those for which he guessed the correct polarization basis. Bob's information is further degraded by the fact that, realistically, some of the photons would be lost in transit or would fail to be counted by Bob's imperfectly-efficient detectors.

Subsequent steps of the protocol take place over an ordinary public communications channel, assumed to be susceptible to eavesdropping but not to the injection or alteration of messages. Bob and Alice first determine, by public exchange of messages, which photons were successfully received and of these which were received with the correct basis. If the quantum transmission has been undisturbed, Alice and Bob should agree on the bits encoded by these photons, even though this data has never been discussed over the public channel. Each of these photons, in other words, presumably carries one bit of random information (e.g. whether a rectilinear photon was vertical or horizontal) known to Alice and Bob but to no one else.

Because of the random mix of rectilinear and diagonal photons in the quantum transmission, any eavesdropping carries the risk of altering the transmission in such a way as to produce disagreement between Bob and Alice on some of the bits on which they think they should agree. Specifically, it can be shown that no measurement on a photon in transit, by an eavesdropper who is informed of the photon's original basis only after he has performed his measurement, can yield more than $\frac{1}{2}$ expected bits of information about the key bit encoded by that photon; and that any such measurement yielding b bits of expected information ($b \leq \frac{1}{2}$) must induce a disagreement with probability at least $\frac{b}{2}$ if the measured photon, or an attempted forgery of it, is later re-measured in its original basis. (This optimum tradeoff occurs, for example, when the eavesdropper measures and retransmits all intercepted photons in the rectilinear basis, thereby learning the correct polarizations of half the photons and inducing disagreements in $\frac{1}{4}$ of those that are later re-measured in the original basis.)Bennett and Brassard (2014)

Alice and Bob can therefore test for eavesdropping by publicly comparing some of the bits on which they think they should agree, though of course this sacrifices the secrecy of these bits. The bit positions used in this comparison should be a random subset (say one third) of the correctly received bits, so that eavesdropping on more than a few photons is unlikely to escape detection. If all the comparisons agree, Alice and Bob can conclude that the quantum transmission has been free of significant eavesdropping, and those of the remaining bits that were sent and received with the same basis also agree, and can safely be used as a one-time pad for subsequent secure communications over the public channel. When this one-time pad is used up, the protocol is repeated to send a new body of random information over the quantum channel.

The need for the public (non-quantum) channel in this scheme to be immune to active eavesdropping can be relaxed if Alice and Bob have agreed beforehand on a small secret key, which they use to create Wegman– Carter authentication tags Goldreich, Micali, and Wigderson 1991 for their messages over the public channel. In more detail the Wegman–Carter multiple-message authentication scheme uses a small random key to produce a message-dependent 'tag' (rather like a check sum) for an arbitrarily large message, in such a way that an eavesdropper ignorant of the key has only a small probability of being able to generate any other valid message–tag pairs. The tag thus provides evidence that the message is legitimate, and was not generated or altered by someone ignorant of the key. (Key bits are gradually used up in the Wegman–Carter scheme, and cannot be reused without compromising the system's provable security; however, in the present application, these key bits can be replaced by fresh random bits successfully transmitted through the quantum channel.) The eavesdropper can still prevent communication by suppressing messages in the public channel, as of course he can by suppressing or excessively perturbing the photons sent through the quantum channel. However, in either case, Alice and Bob will conclude with high probability that their secret communications are being suppressed, and will not be fooled into thinking their communications are secure when in fact they're not.

3.3 Quantum Coin Tossing

Quantum coin tossing is a scheme involving classi- cal and quantum messages which is secure against traditional kinds of cheating, even by an opponent with unlimited computing power. Ironically, it can be subverted by a still subtler quantum phenomenon, the so-called Einstein– Podolsky–Rosen effect. This threat is merely theoretical, because it requires perfect efficiency of storage and detection of photons, which though not impossible in principle is far beyond the capabilities of current technology. The honestly-followed protocol, on the other hand, could be realized with current technology

1. Alice chooses randomly one basis (say rectilinear) and a sequence of random bits (one thousand should be sufficient). She then encodes her bits as a sequence of photons in this same basis, using the same coding scheme as

before. She sends the resulting train of polarized photons to Bob.

2. Bob chooses, independently and randomly for each photon, a sequence of reading bases. He reads the photons accordingly, recording the results in two tables, one of rectilinearly received photons and one of diagonally received photons. Because of losses in his detectors and in the transmission channel, some of the photons may not be received at all, resulting in holes in his tables. At this time, Bob makes his guess as to which basis Alice used, and announces it to Alice. He wins if he guessed correctly, loses otherwise.

3. Alice reports to Bob whether he won, by telling him which basis she had actually used. She certifies this information by sending Bob, over a classical channel, her entire original bit sequence used in step 1.

4. Bob verifies that no cheating has occurred by comparing Alice's sequence with both his tables. There should be perfect agreement with the table corresponding to Alice's basis and no correlation with the other table. In our example, Bob can be confident that Alice's original basis was indeed rectilinear as claimed.

4. limitations and challenges

4.1 Impossibility of quantum bit commitment

The 10-year period following the publication ofthe first QKD protocol Bennett and Brassard 2014 saw only a handful of cryptographers working in quantum cryptography. The main impossibility argument are listed below.

First, consider the following sketch of impossibility for perfectly secure classical bit commitment: suppose such a protocol exists. Then by the informationtheoretic security requirement, at the end ofthe commitment phase,Bob's viewofthe protocol must be independent of b (since, otherwise, the protocol would not be perfectly hiding). But phase, with both being accepted by Bob. Hence, the bit commitment cannot be binding. this independence implies that Alice can choose to reveal either b = 0or b = 1inthe reveal It is interesting that the same proof structure is applicable to the quantum case, albeit by invoking some slightly more technical tools. Namely, we first consider a purified version of the protocol, which consists in all parties acting at the quantum level (measurements are replaced by a unitary process via a standard technique). Next, by the information-theoretic hiding property, the reduced quantum state that Bob holds at the end of the commit phase must be identical, whether b = 0or b = 1. This condition is enough to break the binding her system in order to re-create a joint state consistent with either b = 0, or b = 1, at her choosing.13 Hence, she can chose to open either b = 0or b = 1 at a later time, and Bob will accept: the commitment scheme cannot be binding.

Going back to the original paper on quantum bit commitment, we note that a subtlety in the definition of the binding property is the origin of the false claim of security: while it is true that the protocol is such that Alice is unable to simultaneously hold messages that b = 0 and b = 1), this is insufficient to prove security, since in fact Alice is able to delay would unveil a commitment to b = 0 and as b = 1 (and thus, to be able to choose to open her choice of commitment until the very end of the protocol—at which point she can choose to open as either b = 0 or b = 1.

4.2 Impossibility of secure two-party computation using quantum communication

Given the impossibility of quantum bit commitment, the next question to ask is: are there any classical primitives that may be implemented securely using quantum communication? In fact, the possibility for OT was stated as a open problem in Montrdal and Centre-ville 1996. Unfortunately, this hope was shattered rather quickly, as impossibility results were given by Lo in Lo 2008 for one- sided computations (where only one party receives output). This result already shows the impossibility of 1-out-of-2 OT—the proof technique follows closely the technique developed for the impossibility of quantum bit commitment (see Sect. 4.1). It took almost 10years until Colbeck showed the first impossibility result for two-sided computations, namely that Alice can always obtain more information about Bob's input than what is implied by the value of the function. In a similar vein, Salvail, Schaffner and Sotakova proved in Salvail, Schaffner, and Sotáková 2015 that any quantum protocol for a non-trivial primitive leaks information to a dishonest player. What is worse, even with the help of a trusted party, the cryptographic power of any primitive cannot be "amplified" by a quantum-communication protocol. Buhrman, Christandl and Schaffner have strengthened the above impossibility results by showing that the leakage in any quantum protocol is essentially as bad as one can imagine: even in the case of approximate correctness and security, if a protocol is "secure" against Bob, then it is completely insecure against Alice (in the sense that she can compute the output of the computation for all of her possible inputs). For impossibility results in the universal composability (UC) framework.

4.3 Zero-knowledge against quantum adversaries: "quantum rewinding"

Zero-knowledge interactive proofs, as introduced by Goldwasser, Micali, and Rackoff are interactive proofs with the property that the verifier learns nothing from her interaction with the honest prover, beyond the validity ofthe statement being proved. These proofsystems play an important role in the foundations of cryptography, and are also fundamental building blocks to achieve cryptographic functionalities (see

Goldreich, Micali, and Wigderson 1991 for a survey). In zero-knowledge interactive proofs, the notion that the verifier "learns nothing" is for- malized via the simulation paradigm: if, for every cheating verifier (interacting in the protocol on a positive instance), there exists a simulator (who does not interact with the prover) such that the output of the verifier is indistinguishable from the output of the simulator, thenwe say that the zero-knowledge property holds. In the classical world, a common proof technique used for establishing the zero-knowledge property is rewinding: a simulator is typically built by executing the given verifier—except that some computation paths are culled if the ran- dom choices of the verifier are not consistent with the desired effect. This selection is done by keeping a trace of the interaction, thus, if the interaction is deemed to have followed an incorrect path, the simulation can simply reset the computation ("rewind") to an earlier part of the computation (see Goldreich, Micali, and Wigderson 1991 and references therein).

In the quantum setting, such a rewinding approach is impossible: the no-cloning theorem tells us that it is not possible, in general, to keep a secondary copy of the transcript in order to return to it later on. This problem is further aggravated by the fact that, in the most general case, the verifier starts with some auxiliary quantum information (which we do not, in general, know how to re-create)—thus even a "patch" that would emulate the rewinding approach in the simple case would appear to fail in the case of auxiliary quantum information. We emphasize that the above concerns about the zero-knowledge property are applicable to purely classical protocols: honest parties are completely classical, but we wish to establish the zero-knowledge property against a verifier that may receive, store and process quantum information.

Bibliography

Aspect, Alain, Philippe Grangier, and Gérard Roger (1982). “Experimental realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A new violation of Bell’s inequalities”. In: *Physical Review Letters* 49.2, pp. 91–94. ISSN: 00319007. DOI: 10.1103/PhysRevLett.49.91.

Bennett, Charles H. and Gilles Brassard (2014). “Quantum cryptography: Public key distribution and coin tossing”. In: *Theoretical Computer Science* 560.P1, pp. 7–11. ISSN: 03043975. DOI: 10.1016/j.tcs.2014.05.025. URL: http://dx.doi.org/10.1016/j.tcs.2014.05.025.

Broadbent, Anne and Christian Schaffner (2016). *Quantum cryptography beyond quantum key distribution*. Vol. 78. 1. Springer US, pp. 351–382. ISBN: 1062301501. DOI: 10.1007/s10623-015-0157-4. arXiv: 1510.06120.

Goldreich, Oded, Silvio Micali, and A V I Wigderson (1991). “Zero-Knowledge twenty years after its invention”. In: *Computing* 38.1, pp. 691–729.

Lo, Hoi-kwong (2008). “Insecurity of Quantum Secure Computations”. In: pp. 1–28. arXiv: 9611031v2 [arXiv:quant-ph].

Montrdal, Universitd De and Succursale Centre-ville (1996). “Cryptology Column 25 Years of Quantum Cryptography”. In: pp. 13–24.

Salvail, Louis, Christian Schaffner, and Miroslava Sotáková (2015). “Quantifying the leakage of quantum protocols for classical two-party cryptography”. In: *International Journal of Quantum Information* 13.4. ISSN: 02197499. DOI: 10.1142/S0219749914500415. arXiv: 1501.01549.

Wootters, W. K. and W H Zurek (Oct. 1982). “A single quantum cannot be cloned”. In: *Nature* 299.5886, pp. 802–803. ISSN: 0028-0836. DOI: 10.1038/299802a0. URL: http://www.nature.com/articles/246170a0%20http://www.nature.com/articles/299802a0.