Frontiers of Quantum Complexity and Cryptography Spring 2022

Lecture 8 - Quantum Key Distribution

Lecturer: Henry Yuen *Scribes: Wei Zheng Teo*

1 Overview

In this lecture, we started on the topic of quantum cryptography. Similar to the classical setting, in quantum cryptography, we have two honest parties (typically denoted as Alice and Bob) trying to communicate with each other, and an adversary (typically denoted as Eve) which has access to the communication channels between Alice and Bob. At the start of the lecture, we went through different combinations of the honest parties and the adversary being classical or quantum. The table below summarizes the sub-areas of cryptography that deal with these different combinations. In particular, when both the honest parties and the adversary are classical, this falls under classical cryptography, which has been widely studied. When the honest parties are classical but the adversary is quantum, this is handled by post-quantum cryptography (PQC), which aims to develop *classical* cryptosystems that are difficult even for quantum computers to break. The case where the honest parties are quantum and the adversary is classical is generally not of significant interest, since we usually consider adversaries to at least be as powerful as the honest parties. Finally, when both honest parties and the adversary are quantum, we have "fully" quantum cryptography – this is where honest parties can use quantum information to perform cryptography in ways that are impossible in the classical setting.

		Adversary	
		Classical	Quantum
Honest parties	Classical	Classical cryptography	Post-quantum cryptography
	Quantum	Uninteresting case	"Fully" quantum cryptography

2 Post-Quantum Cryptography

Post-quantum cryptography (PQC) is definitely an essential area of research; once technology progresses to the point where we can build a fault-tolerant quantum computer, we can then execute Shor's algorithm [1], a quantum polynomial-time algorithm, to perform integer factoring efficiently. RSA [2] is a widely used public-key cryptography system that relies on the difficulty of factoring products of two large primes, and will be susceptible to being broken with a quantum computer running Shor's algorithm. It is therefore imperative that an alternative to RSA be developed before such a quantum computer can be built.

While not the main topic of this lecture, we still went through some remarks about PQC. The National Institute of Standards and Technology (NIST) is currently holding a competition where participants propose potential quantum-resistant cryptosystems. As of now, most of the promising candidates are based on the hardness of lattice problems, such as the shortest vector problem (SVP). In SVP, we are given a basis of a lattice (which is usually a finite subgroup of $\mathbb{Z}^n$ for some

choice of n), and we have to find the shortest non-zero vector in the lattice. There are usually several additional steps to make use of a lattice problem in a cryptosystem, but one of the steps can involve the reduction of SVP to the learning with errors (LWE) problem. Roughly speaking, in the LWE problem we have a matrix $A \in \mathbb{Z}_q^{m \times n}$, and a secret string $s \in \mathbb{Z}_q^n$. Given $As + e$ where e is a "small weight" error in $\mathbb{Z}_q^n$, we want to deduce s. It is conjectured that this is hard even for quantum computers. It has been shown that SVP is reducible to LWE [3].

3 Quantum Key Distribution

In this lecture, we are interested in the setting of "fully" quantum cryptography. We discussed quantum key distribution (QKD). Similar to key distribution in the classical setting, we have the two honest parties, Alice and Bob, wanting to establish a secret key $k \in \{0,1\}^m$ through shared (and usually public) channels, such that only Alice and Bob will know what k is and any adversaries (Eve) will only have a negligible probability of knowing k. In QKD, Alice and Bob both share a classical channel and a quantum channel, where we assume that the classical channel is an authenticated channel (meaning that Alice and Bob can trust that what they hear is what the other person really said). The adversary Eve has the ability to eavesdrop on the classical channel and also to tamper with the qubits being transmitted across the quantum channel. A solution to QKD would achieve the goal of sharing a key k with unconditional security, i.e. we are assured of security even if Eve has unlimited time and computational power.

3.1 BB84

The first QKD scheme ever proposed was BB84 [4], by Charles Bennett and Gilles Brassard in 1984. The BB84 protocol works as follows:

- Alice samples $x, b \in \{0,1\}^n$ uniformly at random.
- Alice sends $|\psi\rangle$ where, for $1 \leq i \leq n$, $|\psi_i\rangle = H^{b_i}|x_i\rangle$, i.e. if $b_i = 0$, Alice sends $|x_i\rangle$, and if $b_i = 1$, Alice sends $H|x_i\rangle$. Thus, for each i, Alice sends one of four states: $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$.
- Bob receives $|\psi\rangle$. Bob samples $b' \in \{0,1\}^n$ uniformly at random, and measures the state $H^{b'_i}|\psi_i\rangle$ for each qubit, i.e. if $b'_i = 0$, Bob measures $|\psi_i\rangle$ directly, and if $b'_i = 1$, Bob applies H to $|\psi_i\rangle$ before measuring. The outcome of the measurement of the i-th qubit is stored as x'_i.
  - Note that if $b'_i = b_i$, i.e. Bob "guessed" b_i correctly, then $x'_i = x_i$. Otherwise, Bob has a $\frac{1}{2}$ chance of measuring the correct value of x_i.
- Alice and Bob then send b and b' to each other in the clear over the classical channel.
- Both Alice and Bob discard coordinates in x and x' where $b_i \neq b'_i$. The expected number of coordinates left will be $\frac{n}{2}$. Let the resulting strings from removing these coordinates from x and x' be z and z' respectively.
- If no tampering or errors have occurred, Alice and Bob should have $z = z'$. However, we want to check if Eve has tampered with the qubits sent by Alice, e.g. performed a measurement on them. To detect this, Alice samples a subset I of the remaining coordinates (say, half of

the bits), and checks with Bob over the classical channel whether $z_i = z'_i$ for each $i \in I$. If Alice and Bob discover a difference, the entire procedure is restarted. Otherwise, Alice and Bob can be confident that most of the remaining bits in z and z' are identical.

- Alice and Bob then perform *information reconciliation* to correct the remaining differences in z and z', so that they agree on the *same* string z''. This involves communication over the classical channel.
- At this point, Eve may have gleaned some information about z'', so Alice and Bob perform a final step of *privacy amplification* to process z'' and obtain the final key k that Eve is completely ignorant of.

3.1.1 Security of BB84

It has been shown that, under very mild assumptions (e.g. the equipment of Alice and Bob are shielded from the adversary, the laws of quantum mechanics are correct, the classical channel between Alice and Bob is authenticated, etc), the BB84 protocol is secure. The full proof of security of BB84 can get rather involved, but we'll try to get some intuition for why it's plausibly secure. We'll think about a specific way that Eve can attack the scheme.

Measurment disturbance. We can consider attacks by Eve where Eve simply performs a measurement on some qubits in some basis, which has the potential of collapsing the wavefunction of affected qubits. Consider a simple case where for each qubit $|\psi_i\rangle$, Eve either decides to let the qubit pass, or measure it in a random basis (either the standard basis $\{|0\rangle, |1\rangle\}$ or the Hadamard basis $\{|+\rangle, |-\rangle\}$) before letting it pass. Note that when the qubits are sent, Eve does not yet know the correct basis of each qubit, which explains why Eve is choosing a random basis.

For example, suppose $|\psi_i\rangle = |+\rangle$ (i.e. $x_i = 0$ and $b_i = 1$), and Eve decides to measure $|\psi_i\rangle$ in the standard basis. Clearly Eve will measure either 0 or 1, i.e. $|\psi_i\rangle$ collapses to $|0\rangle$ or $|1\rangle$ each with $\frac{1}{2}$ probability. Now, if Bob had guessed b'_i correctly, i.e. $b'_i = b_i = 1$, Bob will apply H to the tampered $|\psi_i\rangle$ before measuring in the standard basis. However, now Bob will get either $|+\rangle$ or $|-\rangle$ before measuring, and in either case, Bob obtains $x'_i \neq x_i$ with $\frac{1}{2}$ probability. It can be shown that if Alice and Bob check $\frac{1}{2}$ of the bits in z and z' in a future step, there is a $\frac{1}{8}$ chance that a discrepancy shows up at the i-th bit.

We note that if Eve measures too many qubits, there is a high probability that a discrepancy will be discovered in z and z', and thus the attack will "fail" since Alice and Bob will restart the protocol. If Eve measures too few qubits, then we should expect to have a small enough number of errors that can be corrected in the information reconciliation stage.

No cloning. If Eve could make copies of $|\psi\rangle$ when it is being transmitted, then Eve could duplicate multiple copies of each qubit, and measure each qubit multiple times in each basis until Eve is very sure of the state of each qubit. However, as a result of the no-cloning theorem, this attack is not possible.

3.1.2 Drawbacks of BB84

Being the first ever QKD system proposed, it is not unusual for some downsides to exist for BB84. One drawback of BB84 is its inefficiency, as there are several steps required just to share a bit string. Also, if we want an m-bit shared key, the initial n typically has much larger than m, which can be impractical considering that we need to transmit n qubits. Another drawback of the BB84 – at least the way we described it – is that it is not noise-tolerant, meaning that if there's any noise in the system, the protocol will reject. However, noise is inevitable so the protocol should have a way of tolerating noise (e.g. allowing *some*, but not too many, mismatches to occur).

References

[1] P. W. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM Journal of Computing, 26(5):1484–1509, 1997.

[2] R. L. Rivest, A. Shamir, L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM, 21(2):120–126, 1978.

[3] O. Regev, *On lattices, learning with errors, random linear codes, and cryptography*, Journal of the ACM, 56(6):84-93, 2005.

[4] C. H. Bennett, G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, 175–179, 1984.