Quantum Key-Exchange

JonLuca DeCaro

November 5, 2017

The information-theoretic secure one-time pad offers a mathematical guarantee of perfect security, with a few drawbacks - you are required to exchange keys that are at least as long as your message, and you can only use these keys once. The key exchange is a difficult, imperfect process, which is why the one-time pad is not commonly used. However, the fact that even with infinite computing power you cannot deduce anything besides previously held knowledge of the message makes a more secure key-exchange system an interesting avenue of research.

This is where the theory of quantum key-distribution arose. This is a cryptographic paradigm that is not only mathematically secure - it is also impervious to interception by eavesdroppers. It relies heavily on the no-cloning theorem, which states that "it is impossible to create an identical copy of an arbitrary unknown quantum state."[3] This methodology allows for a secure key exchange over insecure channels - where even the interception of the exchange fundamentally alters the communication itself. This is predicated upon the validity of the no-cloning theorem, which is outlined in the theorems and proofs section below.

Imagine Alice and Bob want to communicate with each other, and there is an eavesdropper Eve that is attempting to intercept their messages. Alice and Bob only have access to two **insecure** channels - a traditional one for bits, and a quantum one for qubits. Awn Umar has an excellent example, listed below [2]:

> Alice has the option of using two different polarization basis—rectilinear and diagonal—using which she can send either 0 or 1. She arbitrarily decides that a 1 encoded in the rectilinear basis will be vertically (0°) polarized, a 1 encoded in the diagonal basis will

> be polarized at 45°, and so on. She informs Bob of this scheme through the conventional channel, and now they are ready to exchange keys. This is summarized in the table :
>
> Table 1: w.l.o.g, arbitrary polarization basis
>
> | **Basis** | **0** | **1** |
> |---|---|---|
> | Rectilinear (+) | 90° | 0° |
> | Diagonal (x) | 135° | 45° |
>
> Alice begins by generating cryptographically-secure random pairings of bits and basis—huge amounts of them. For example,
>
> ```
> 1: diagonal,
> 0: diagonal,
> 0: rectilinear,
> 1: diagonal,
> ```
>
> One at a time, she encodes the bits in their associated basis and sends the resulting polarized photons to Bob through the quantum channel. Now, the way this works is that any party that wishes to read these incoming qubits cannot tell which basis they were encoded in—so they just guess. But there's another catch: if they measure the qubit in the wrong basis, the reading they get is purely random, and the qubit is destroyed in either case.

In the scenario above, **Eve cannot intercept the communication without altering it, thus exposing herself**. Any attempt to read the original data results in its destruction, thus preventing man-in-the-middle attacks or allowing Eve to reconstruct the original qubits.

After Alice has sent all the data, Bob uses the public bit channel to disclose his choices of basis for each bit sent. Alice then replies with the original, true basis and they both discard any bits where Bob guessed incorrectly. Statistically, Bob will guess correctly around 50% of the time. The verification that they weren't eavesdropped is now simple - they select a random subset of the message and compare it over the bit channel. If it matches, they can ascertain with a high degree of certainty that Eve did not intercept their message.

This is mathematically secure - however, it does not take into account the possibility of the regular channel being attacked by Eve in a MitM style attack. This issue is rectified with other common cryptographical tools, however, such as Wegman-Carter authentication.

I personally thought this topic was fascinating - the fact that a communication channel exists such that any data that is read is permanently destroyed/lost is unique and not commonly found elsewhere in information theory. I enjoyed reading about quantum mechanics, and about the opportunities afforded to us through quantum computing. I do not have a strong background in physics, so I must accept some of the proofs as fact without self verification.

Required Proofs and Equations

Schrodinger's Equation:

$$-\frac{\hbar^2}{2m}\frac{d^2\psi}{dx^2} + V\psi = E\psi$$

No-Cloning Proof (courtesy of Yoav Pollack)[1]:

$|\psi\rangle$ is the original state of particle A and $|Blank\rangle$ is some general state of a particle B which we shall use to copy particle A. The overall state is therefore $|\psi\rangle \otimes |Blank\rangle$. an operation on a particle should be unitary, and we wish it to copy the original state:

$$U(|\psi\rangle \otimes |Blank\rangle) = |\psi\rangle \otimes |\psi\rangle \tag{1}$$

This should of course work for any state, and we therefore choose without loss of generality another state which is neither the same nor orthogonal to the original one of particle A.

$$U(|\phi\rangle \otimes |Blank\rangle) = |\phi\rangle \otimes |\phi\rangle \tag{2}$$

Taking the inner product of the the two results we arrive at:

$$(\langle Blank| \otimes \langle\phi|)(U^\dagger U)(|\psi\rangle \otimes |Blank\rangle) = (\langle\phi| \otimes \langle\phi|)(|\psi\rangle \otimes |\psi\rangle) = (\langle\phi||\psi\rangle)^2 \tag{3}$$

on the one hand. On the other hand:

$$(\langle Blank| \otimes \langle\phi|)U^\dagger U(|\psi\rangle \otimes |Blank\rangle) = (\langle Blank| \otimes \langle\phi|)(|\psi\rangle \otimes |Blank\rangle) = \langle\phi||\psi\rangle \tag{4}$$

We arrive at a contradiction since we assumed the states are not identical or orthogonal.

References

[1] *Quantum Cryptography.* URL: http://physweb.bgu.ac.il/COURSES/QuantumMechCohen/Contributions/yoav.pdf.

[2] Awn Umar. *Quantum Key-Exchange.* July 2017. URL: https://cryptolosophy.io/quantum-key-exchange/.

[3] W. K. Wootters and W. H. Zurek. “A single quantum cannot be cloned”. In: *Nature* 299.5886 (Oct. 1982), pp. 802–803. DOI: 10.1038/299802a0.