Eric Sciberras 761250

Quantum Cryptography

Charles H. Bennett, Gilles Brassard and Artur K. Ekert

Introduction

Cryptographic tasks such as sharing private keys is extremely difficult (if not impossible) to securely implement, but with Quantum mechanics we can develop better cryptographic systems.

Vernman Cipher

The Vernman cipher (one time pad) is theoretically unbreakable if implemented correctly. It requires three things:

1. A private key that is shared between both parties
2. That the key be longer than or equal to the size of the message
3. A new key to be used for each message sent

```
      H       E       L       L       O  message
    7 (H)   4 (E)  11 (L)  11 (L)  14 (O) message
+ 23 (X)  12 (M)   2 (C)  10 (K)  11 (L) key
= 30      16      13      21      25     message + key
=  4 (E)  16 (Q)  13 (N)  21 (V)  25 (Z) (message + key) mod 26
      E       Q       N       V       Z  → ciphertext
```

Figure 1: Vernman cipher encryption [1]

In this example the each number in the key is used to move a letter across the alphabet.
Note: the first 'L' in HELLO is changed to 'N' and the second 'L' to 'V' (this makes cryptanalysis difficult)

```
      E       Q       N       V       Z  ciphertext
    4 (E)  16 (Q)  13 (N)  21 (V)  25 (Z) ciphertext
-  23 (X)  12 (M)   2 (C)  10 (K)  11 (L) key
= -19       4      11      11      14     ciphertext - key
=   7 (H)   4 (E)  11 (L)  11 (L)  14 (O) ciphertext - key (mod 26)
      H       E       L       L       O  → message
```

Figure 2: Vernman cipher decryption [1]

Unfortunately sending a private key securely is difficult as it requires the use of some other encryption scheme such as RSA which is theoretically crackable. Alternatively both parties can meet face-to-face to exchange the key, but this is sometimes unfeasible. Luckily quantum key distribution (QKD) proposes a solution for this.

Photon Polarisation

Below are figures of various polarised photons entering a Calcite crystal.

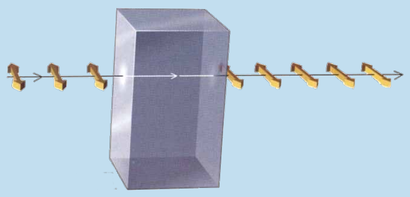


Figure 3: Horizontally polarised photons [2]

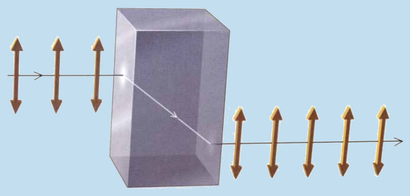


Figure 4: Vertically polarised photons [2]

As we can see from the two figures above both the horizontal and vertical polarised photons are unaltered as they pass through the crystal but go through different channels.

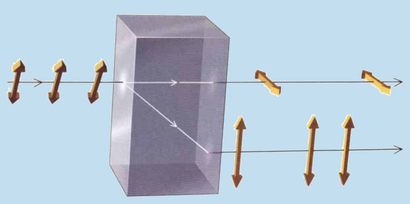


Figure 5: Diagonally polarised photons [2]

In the case of the diagonally polarised photon (45° or 135°), it will be measured as either vertical or horizontal (not both), with a 50/50 chance (this process is random which is vital for quantum key distribution).

References

[1] https://en.wikipedia.org/wiki/One-time_pad

[2] Bennett, C. H., Brassard, G., & Ekert, A. K. (1992). Quantum cryptography. Scientific American, (4), 50.

[3] https://en.wikipedia.org/wiki/Oblivious_transfer

Quantum Key Distribution

Quantum Key distribution is a method of securely sending private keys between two parties (Alice and Bob in the example below). This is useful for implementation of the Vernman cipher.

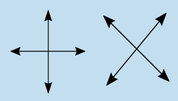


Figure 6: Polarisation filters (rectilinear and diagonal)

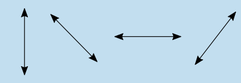
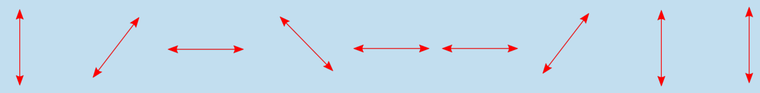
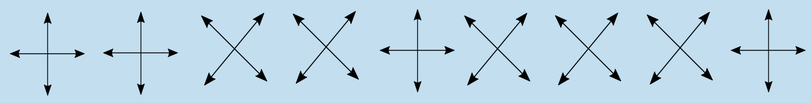


Figure 7: Polarised photons

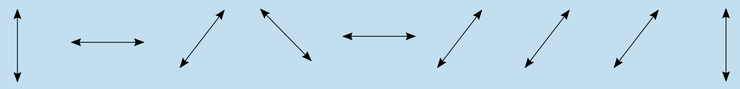
1. Alice prepares a set of polarised photons using a random sequence of rectilinear and diagonal polarising filters (The sequence is only known to Alice)



2. Bob receives the photons and uses another random sequence of polarising filters to measure the photons

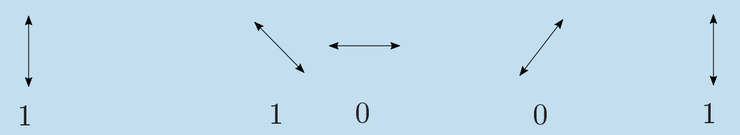


3. Bob gets these measurements.



4. Bob now communicates with Alice (can be through an open channel) the polarisation filters used and Alice tells him which were correct. All the incorrect measurements are thrown out and a subset of the measurements are also thrown out to check for any tempering in the quantum channel (this can also be done by checking the parity of multiple subsets).

5. The correct remaining polarisations can now be used as binary which make up the private key.



Note: Figures above are adapted from [2]

A third party observing the channel:

- Cannot clone the photons due to the no cloning theorem.
- Can measure the polarisations of the photons (would then be detected by Alice and Bob).
- Can use a beam splitter so that Alice and Bob are less likely to detect a third party (reducing the intensity of the beam can remedy this).

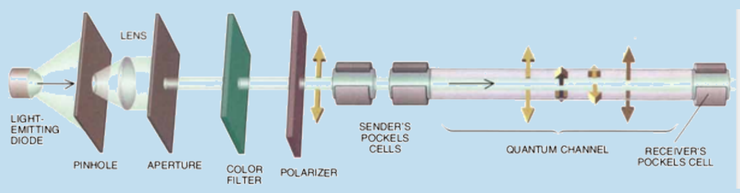


Figure 8: Apparatus for Quantum key distribution [2]

Quantum Decision Making

Imagine two parties wish to make a decision that depends on confidential information, but neither party wishes to disclose that information.

- Classically, an intermediary can take the confidential information from both parties and make the decision for them, but this situation isn't ideal as the intermediary may be untrustworthy.
- Apparatus similar to the one used in QKD can be used to make joint decisions discretely. This requires using many iterations of a process called 'oblivious transfer' where information is sent out (can be one or many pieces), but the sender doesn't know which piece the receiver has. [3]

Quantum Authentication

Wegman-Carter authentication which requires a shared secret key to authenticate messages can be used in conjunction with quantum key distribution (QKD).

1. QKD provides the shared secret key (this initial step must be authenticated by other means).
2. Wegman-Carter authentication can now be used for any successive QKD attempts.

Quantum Key Storage

Another weak point with implementing the Vernman cipher is the secure storage of keys. This can be solved thanks to the EPR effect where a spherically symmetric atom emits two photons in opposite directions (both containing opposite polarisations)

1. Alice prepares EPR photon pairs, keeping one of each pair for herself and giving the other to Bob.
2. Some of the photons are measured immediately to check for eavesdropping.
3. Once Alice and Bob need to communicate they can measure a subset of the photons (using the same polarisation filter type) and if the storage hasn't been disturbed Alice and Bob will always get opposite measurements of all the pairs.
4. The remaining photons are measured to retrieve the private key.

Importance

The results of this article are extremely important for cryptography as quantum key distribution, quantum key storage and quantum decision making have properties that classically, cannot be replicated (EPR effect and Heisenberg uncertainty principle). Combining these quantum processes with the Vernman cipher and Wegman-Carter authentication can help with implementing secure communications.