# Quantum Key Distribution

Name: Eduard Korotkihs K-number: K2200500

## Executive Summary

This report will talk about quantum key distribution (QKD), how it works and how interceptor can be detected, its implementation and how it can be used in a large financial institution such as, international banks. In addition, an example will be provided on how to know if communication is compromised. At the end the conclusion will be given if large financial institutions should use QKD for secure communication.

## Introduction

The main purpose of classical cryptography is to transform original information (plain text) into a cipher text that becomes unreadable. To transform the text there are two type of algorithms that are used, symmetrical and asymmetrical algorithms. Symmetrical algorithms contain only one key to perform both encryption and decryption, it needs to be shared between both parties. It is 1000 times faster than asymmetric algorithm but its less secure as the key needs to be shared and if it intercepted it can be used for decryption (Yassein, Aljawarneh, Qawasmeh, Mardini and Khamayseh, 2017). Therefore, asymmetrical algorithms preferred more. It has two keys public for encryption and private for decryption. One of the algorithms that us mostly used is RSA. Classical cryptography has some advantages like there is no limit to the distance between two parties, and it may easily be implemented into software and hardware (Vignesh, Sudharssun and Kumar, 2009). However, classical cryptography has some major drawbacks. The first one is that hackers can exploit loopholes to interrupt systems security (Vignesh, Sudharssun and Kumar, 2009). Another drawback is that most of secure algorithms like RSA and ECC requires higher quantities of computational power to be effective.

With the development of quantum computing, classical cryptography became vulnerable to Shor's algorithm a polynomial time algorithm for factoring large prime numbers on a quantum computer (Hayward, 2005). This is because the significant part of cryptographic algorithms security depends directly or indirectly on the difficulty of factoring or extracting discrete logarithms (Brassard, 1994). Shor's algorithm can extract the discrete logarithms classical cryptography algorithms vulnerable. However, DES algorithm still has shown that it cannot be efficiently breakable by quantum computers.

## QKD Protocols

Quantum key distribution (QKD) is a method for secure communication using quantum mechanics. QKD uses quantum properties of photons, that represent data, to be transmitted to another user. Another property is that if someone tries to measure the state, it will disturb it and leave a detectable trace behind (Alleaume, 2014). This feature makes it secure as both parties could use it to test if someone is eavesdropping on their communications. It can be detected by analysing their measurements they took and if there are many errors it means that someone is intercepting their photons.

To generate the key both parties need to be connected through two channels, quantum channel and classical channel that could potentially be insecure. One of the users will generate a random sequence of bits, 1s and 0s. For each bit the user will select the basis, like horizontal and vertical polarization or diagonal polarization (Alleaume, 2014). After basis was set for each bit, the photons will be sent over the quantum channel to other user.

Second user will select the basis for each photon user receives, the measurements will be recorded as 0s and 1s, and the basis the user used (Alleaume, 2014). Once it done both of the parties communicate the bases they used for each photon over classical channel.

To detect if someone eavesdropping over the channel, both parties can compare the random subset of their remaining bits and if its below the certain threshold. If its below certain threshold that means their communication has been compromised and they can discard the key and start the process again.

The security feature QKD protocol provides will be beneficial to large financial institutions, such as international bank, because they will be able to detect if someone is trying to eavesdrop the communication channel. Also, it's very easy and quick to drop the keys and create new ones between both parties, therefore it provides less hustle and doesn't require to perform any complicated calculations.

## Example

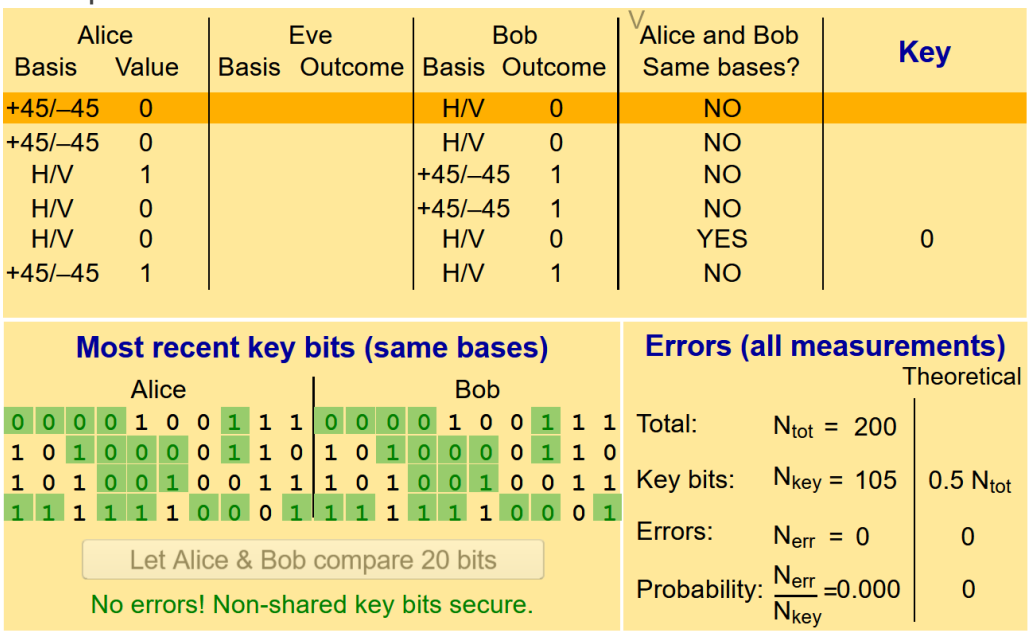


FIGURE 1

In figure 1 above it shows results after 100 photons have been sent from Alice to Bob. Both can now compare the 20 bits they sent over the channel. During the initial stage when they both share the bases that they got right between each other, they will keep the values secret and use those values as a key. So when Alice and Bob checks the communication, they compare the bases that represented the key, if no errors are detected, Alice and Bob will assume no one is eavesdropping their communication.

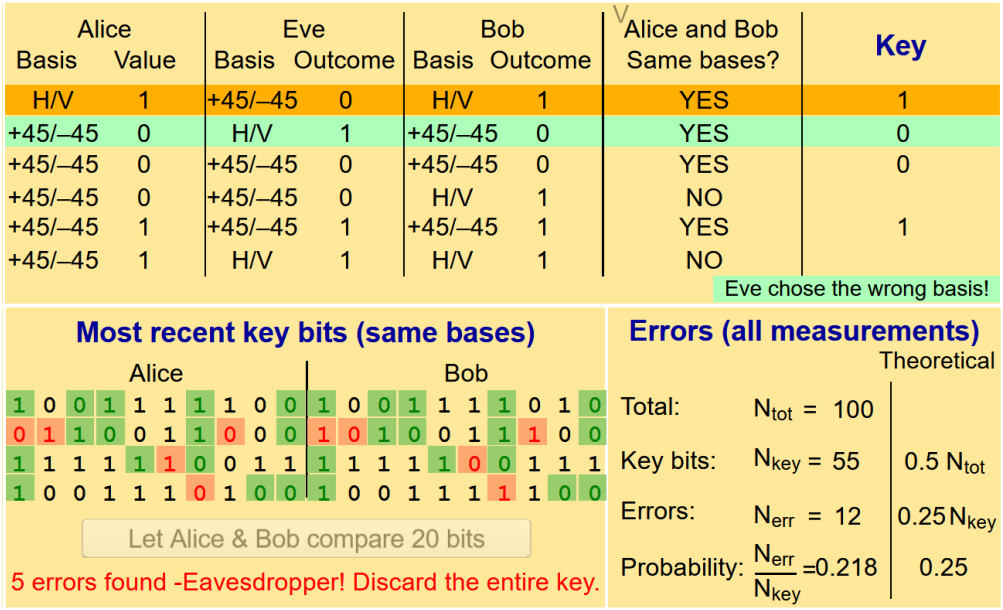


FIGURE 2

However, in figure 2 above it shows what happens if someone started to eavesdrop their communication. The bits that represented the key had errors because the eavesdropper used wrong basis when intercepting the photons which changed the value of the photons. In this case there was 5 errors meaning that it exceeded the threshold in this communication and keys needs to be discarded.

## QKD Practical Implementation

The implementation of the QKD is not very difficult. For the practical implementation there are several components that need to be included in the setup. The first component is fibre optic (Gordon, Fernandez, Townsend, and Buller, 2004) or optics (such as lasers) because both options produce light. However, both have their own disadvantages, for example fibre optics cannot be used for long distances without requiring repeaters that boost the signal (Gordon, Fernandez, Townsend, and Buller, 2004). On other hand optics have a greater distance but are affected by atmospheric conditions such as poor weather, fog or snow (Razaq and Saad, 2023) Whereas fibre optics can be used underground. Both of the following options will be used as a communication channel.

The second component is QKD devices such as a photon source what can generate photons or weak laser pulses. Moreover, it should be able to precisely control the properties of photons (e.g. horizontal and vertical, or diagonal polarizations). Another device needs to be able capture those photons or weak laser pulses.

The third component is a classical communication channel, and it must have an authentication to prevent a man-in-the-middle attack. This channel will be used to share and discuss the bases that has been used by both parties and agree upon the key that they going to use.

The last component is a system that integrates everything together and enables the communication between two parties. This system also needs to have a way to store the keys securely and have a key management function.

However, it may sound simple to implement but the disadvantages of it is cost because it going to be very high. For example, to use fibre optics it probably needs to be rented from third party companies. Furthermore, creating a system that integrates everything together will require an additional cost for building such a system and making it work.

## Recommendations and Conclusions

In conclusion, QKD protocol can be used by large financial institutions such as international banks, to make their communications and transactions secure and protected from interception. Due to the nature of the quantum mechanics is that if its being monitored it may disturb the photons which could produce incorrect results at the receiving end, meaning that interceptor has been noticed, and the keys get be discarded. Another advantage is that it requires expensive technology to capture photons and be able to have polarization. All factors reduce the chance of information being intercepted. However, this level of security comes at the cost as it will be very expensive, but large financial institutions should not have a problem with this as they will be able to fund it for better security which may reduce their costs in the future and increase the trust of their clients.

## References


Yassein, MBY., Aljawarneh, SA., Qawasmeh, EQ., Mardini, WM., and Khamayseh, YK. (2017) 'Comprehensive study of symmetric key and asymmetric key encryption algorithms', *2017 International Conference on Engineering and Technology (ICET)*, pp 1-7. Available at: https://doi.org/10.1109/ICEngTechnol.2017.8308215

Vignesh, RSV., Sudharssun, SS., Kumar, KJJK. (2009) 'Limitations of Quantum & the Versatility of Classical Cryptography: A comprehensive Study', *Second International Conference on Environmental and Computer Science*, pp 333-337. Available at: https://doi.org/10.1109/ICECS.2009.21

Hayward, MH. (2005) *Quantum Computing and Shor's Algorithm*. Available at: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=c4c3ad4aef68f3970d187fec0f13755471579018 (Accessed: 2 February 2025).

Brassard, GB. (1994) *Cryptology Column – Quantum Computing: The End of Classical Cryptography?*. Available at: https://dl.acm.org/doi/pdf/10.1145/190616.190617 (Accessed: 3 February 2025).

Alleaume, R., Branciard, C., Bouda, J., Debuisschert, T., Dianati, M., Gisin, N., Godfrey, M., Grangier, P., Langer, T., Lutkenhaus, N., Monyk, C., Painchault., Peev, M., Poppe, A., Pornin, T., Rarity, J., Renner, R., Ribordy, G., Riguidel, M., Salvail, L., Shields, A., Weinfurter, H., and Zeilinger, A. (2014) 'Using quantum key distribution for cryptographic purposes: A survey', *theoretical Computer Science*, Volume 560, part 1, pp 62-81. Available at: https://www.sciencedirect.com/science/article/pii/S0304397514006963

Gordon, K.J., Fernandez, V., Townsend, P.D., and Buller, G.S (2004) 'A short wavelength GigaHertz clocked fiber-optic quantum key distribution system', *IEEE Journal of Quantum Electronics*, vol.40, pp 900-908. Available at: https://doi.org/10.1109/JQE.2004.830182

Razaq, H.M. and Saad, W.K. (2023) 'Review of Free Space Optical Communication: Advantages and Disadvantages', *10th International Conference on Wireless Networks and Mobile Communications (WINCOM)*, pp 1-5. Available at: https://doi.org/10.1109/WINCOM59760.2023.10322932