# META-ANALYSIS OF THE CURRENT STATE OF THE QUANTUM CRYPTOGRAPHY IDENTIFYING AREAS OF DEVELOPMENT AND IMPLEMENTATION

¿Which are the areas that the Quantum Cryptography has been implemented?

Alexander Hernández Niño
Catholic University of Colombia
Bogotá, Colombia
ahernandez63@ucatolica.edu.co

Alexander Reyes Quintero
Catholic University of Colombia
Bogotá, Colombia
areyes22@ucatolica.edu.co

***Abstract*—The meta-analysis answers the question ¿Which are the areas that the Quantum Cryptography is implemented? from this question we applied the methodology and we found a group of countries carrying out research, development and application in different fields such as secure communication for transmitting messages (votes) in the parliamentary elections in Switzerland in 2007, until the transmission quantum key distribution in the satellite communications from NASA. The meta-analysis showed that the most commonly used protocols are BB84 and B92 for its ease of coding and polarize the qubits, using the principles of quantum mechanics with the ability to identify spies in transmission.**

***Keywords***

***Quantum cryptography, BB84 Protocol, Qubit, meta-analysis, photon polarization, Catholic University of Colombia***

## I. INTRODUCTION

Today, secure cryptography requires keys that encrypts and decrypts messages cannot be discovered by other. Public key cryptography is a form of secrets keys provides encryption so that only made by Alice can be decrypted by Bob and anyone else; and that, although part of the relevant information is in the public domain.

The safety of the procedure depends on certain mathematical problems hampered as factoring a number, calculate the product of two numbers is more difficult if these numbers are prime. It is based on the RSA encryption algorithm, widely used in public key cryptography. The confidential message is transmitted between Alice and Bob previously converted by a standard procedure in a number, is encrypted by a mathematical operation which involves a number 408.508.091 and another may be related to the prime number factors, in this case 18,313 and 22.307 .

Breaking public key encryption is very difficult, the secret key can be held for a dozen years.

## II. STEP OF QUANTUM CRYPTOGRAPHY

Alice (sender) and Bob (receiver) are trying to keep secret key quantum cryptography. They transmit polarized photons, procedure devised in the BB84 protocol. To create a key, Alice sends a photon through the slit 0 or 1 of a straight or diagonal polarizing filters; different orientations lie scores.

**Bases polarization**

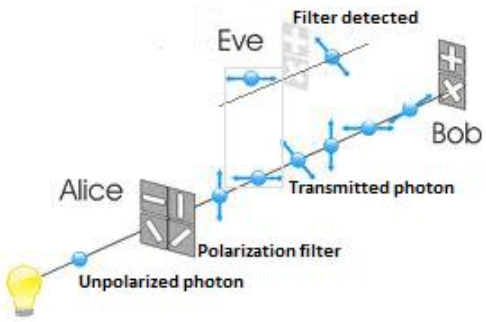
Straight polarization mode 

Diagonal polarization mode 

For each bit that arrives, Bob randomly chooses which filter used for detection and scores both polarization as the bit value. Eva (eavesdropper) she wants to spy train photons, but quantum mechanics forbids her to see both use filters to detect the orientation of each of the photons. If you choose the wrong folder, it will modify its polarization and make mistakes.

Once all the photons have reached Bob, he tells Alice for a public channel, email or phone, the sequence of measurement modes used for incoming photons, but not the bit value of the photons.

**Polarization process**




| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Alice bit sequence | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 |
| Alice filters | ↗ | ↑ | ↘ | ↓ | ↘ | ↙ | ↖ | ↖ | ← |
| Detection modes Bob | + | + | + | + | x | + | + | x | + |
| Bob measurements bits | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 |
| Conserved sequence of bits (key) | - | 0 | - | 0 | 1 | - | - | 1 | 1 |

Alice tells Bob, during the same conversation, in which cases correctly chose the key Alice and Bob will use it to encrypt messages.

The development and implementation of quantum cryptography has created new paradigms from their completely different characteristics from ordinary classical information. Quantum cryptography does not belong to the domain of science fiction, as currently performed in many laboratories. Transmission has been achieved by this method encrypted between points over twenty kilometers connected by fiber optics and several hundred meters in the case of airborne messages. The necessary technology based on quantum optics, progresses very quickly and it seems quite likely that the "commercial" application of quantum cryptography, with all its vast implications in a globally connected world via the Internet, is a matter of a decade. With quantum computing, according to studies and theories developed, you can exponentially increase the processing of data on supercomputers today.

This large computing power may be used for example in the areas of computer graphics to significantly reduce the time it takes place in the completion and production (render) modeled in databases, improving search objects in databases million data records, scientific computing, increased accuracy in model calculations for the prediction of physical, chemical and biological phenomena with a time cost much less. In information security, particularly in cryptography, changes will be seen upon both the ability to provide greater integrity to the current (to the data sent in a communication) and in the ability to make cryptanalysis on algorithms existing encryption, the impact that this would entail in fields such as economics, finance and military security, which is why the importance of the study of Quantum Cryptography.

## III. OBJECTIVE

### A. *Principal objective*

Develop a qualitative meta-analysis of the current state of quantum cryptography identifying areas of development, technologies and applications.

### B. *Specific objectives*

• Identify areas associated with development, technologies and applications in quantum cryptography according to the stage of locating research studies concerning informal setting, primary and secondary sources.

• Characterize the meta-analysis in the areas of development, and applications of quantum cryptography technologies, according to the references identified in the previous objective.

• Present the results of qualitative meta-analyzes derived from applying the methodology previously defined areas of development, technologies and applications where the greatest advances in quantum cryptography according to established characterization were located.

## IV. METHODOLOGY

This research was based on qualitative meta-analysis methodology for the research process.

The meta-analysis is defined as a set of techniques for reviewing and combining results of various studies to answer the same scientific question. Meta-analysis methodology has become increasingly important in the research fields for its successful methodology, which requires the following to their development[1]:

A. Establishment of the problem and the hypothesis to be appraised: Presenting the clear scientific problem, formulate the objectives and define all the specifications on the collection of information and data.

B. Quantification of effects: the measures to be used to describe and represent the research will be established.

C. Locating the information: Each of the research should have the study characteristics (type of sample, monitor and other for evaluating the degree of homogeneity, heterogeneity of the studies to be combined).

D. Location of research studies: For the literature search can be assumed informal sources, primary sources and secondary sources.

E. Criteria for inclusion / exclusion of studies: inclusion and exclusion criteria to be established so as to ensure its reliability and accuracy.

F. Quality assessment of included studies: score values and/or group of studies to weigh the information collected is allocated.

G. Analysis of heterogeneity: Using statistical methods, results from different studies to be summarized in a single measure is valued.

H. Combination of results: By combining statistical methods and present the results.

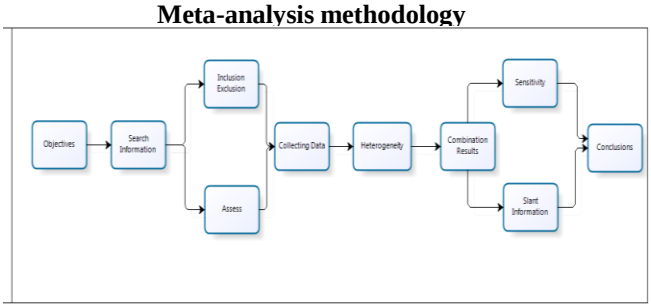
I. Identification of publication bias: All Meta-analysis should assess the possibility of the existence of publication bias that could compromise its results and conclusions.

J. Sensitivity analysis: Sensitivity analysis aims to study the influence of individual studies on the overall estimate of effect and, therefore, the robustness and stability of the final measurement obtained.

K. Publication: Delivering Results.

H. Combination of results: Using statistical methods

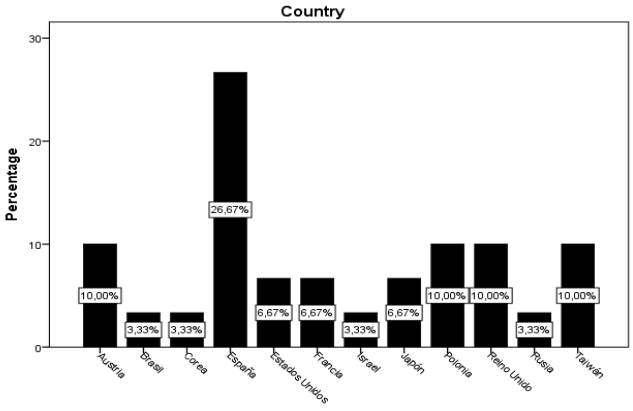
**Meta-analysis methodology**



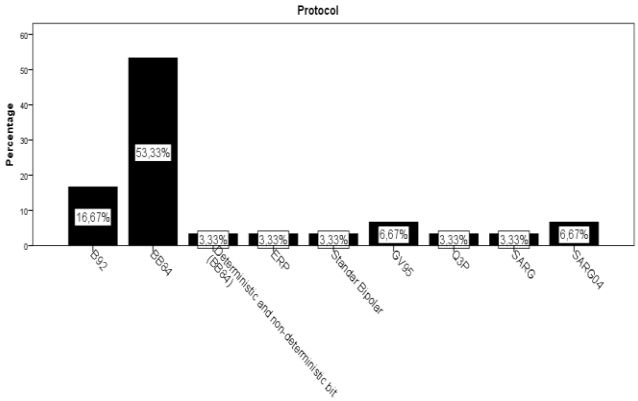

[1]SEQC Metaanálisis [en línea] http://dxsp.sergas.es/ApliEdatos/Epidat/Ayuda/11-Ayuda%20Meta-an%E1lisis.pdf [citado 04 Marzo de 2014]

## V. RESULTS

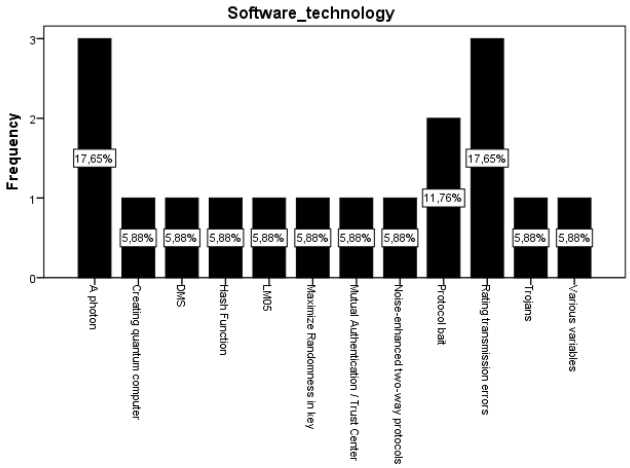
It is observed in the frequency data of the data on country of origin of quantum cryptography research on the country more research on Q.C. is Spain who led the research with a percentage of 26.7%, followed by Austria, Poland, United Kingdom and Taiwan with a percentage of 10% for each additional United States, France and Japan have 6.7% each. At the end is Brazil, Israel, Korea and Russia at a rate of 3.3% each. Allowing you to identify the size of the sample (30 items) one of the countries that has generated more research topic has been Spain.



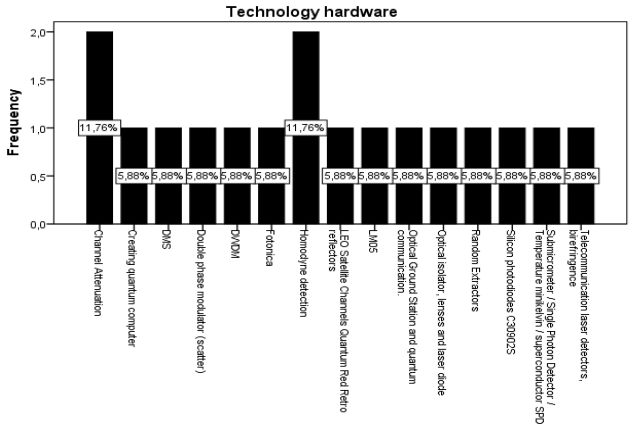

In the second protocol frequency analysis we can identify the most commonly used protocol is the BB84 with a percentage of 53.3%, followed by the B92 with a percentage of 16.7% subsequently found to GV95 and SARG04 protocols with a percentage 6.7% each and finally the deterministic protocols are not deterministic bit (BB84), ERP, bipolar standard Q3P and SARG each with a value of 3.3%, indicating that the greatest advances and implementations on quantum cryptography studies have been performed on the BB82 protocol, the oldest and most widely used protocol in trials and deployments.



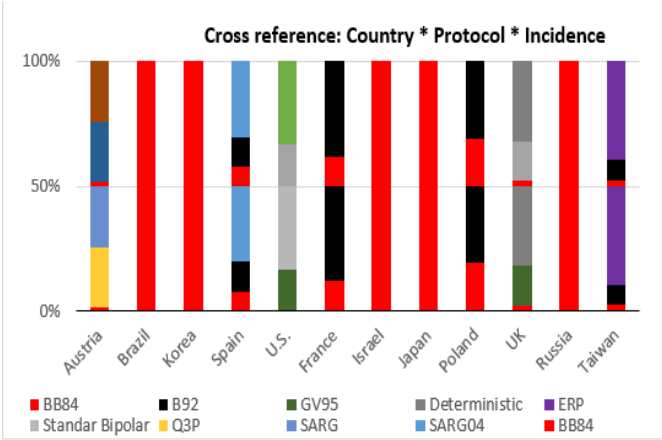

• According to the frequency analysis software technology, one can show that in the sample obtained different proposals focused on new software technologies, where proposals for assessment of transmission errors and a photon with stand will present a 17.65% followed by the decoy protocol with a 11.76%.




• In the frequency analysis technology hardware, quite isolated proposals on the sample are presented and worked only lead to proposals for a channel attenuation and homodyne detection with 11.76%.




• Finally the methodology of meta-analysis allowed us to demonstrate the cross-subgroups selected information, to get a better view of the research process of quantum cryptography on leading research countries versus the implemented protocols.



## VI.CONCLUSIONS

The proposed technology of quantum cryptography allows us to envision a future of greater security in data transmission and all investigative processes tending to that end, will contribute to faster and more accessible worldwide implementation. Meta- degree work of the current state of quantum cryptography identifying areas of development and implementation, discloses the community an overview on research on quantum cryptography. Identified through the process of meta-analysis in this research leaders countries valued at more protocols such investigations, as well as software and hardware technologies proposed and implemented in quantum cryptography. So that this work would not only know the current state of quantum cryptography if you wake up in the academic community the firm intention to delve into more research for the benefit of methods and / or technologies that enable data transmission safely in no distant future if not a technological mind that acclaims immediately.

## ACKNOWLEDGMENT

We would like to give thanks to the Universidad Católica de Colombia. We would like to take this opportunity to express our gratitude to Eng. Angelica Veloza our Project Manager Grade who provided us with her experience. Furthermore, a special thanks to Eng. Holman Bolivar for discussions and explanations of Information and methodology of meta-analysis.

## REFERENCES

[1] CNN-CERT. Glosario [En línea]. Febrero 02 de 2009- [citada en Febrero 10 de 2014]. Disponible en internet:<https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-Glosario_y_abreviaturas/ glosario/index.html?n=314.html >

[2] GISIN Nelson, RIBORDY Gabriel. Quantum Communications and Cryptography. New York: Taylor & Francis Group, 2006. p. 145-150.ISBN 0-8493-8.

[3] IBM, SPSS. SPSS Statistics [CD-ROM]: MAC Versión 21. c. 2013. ISBN-10: 1446249182

[4] ICONTEC. Norma técnica colombiana NTC 1486. 6 ed. Bogotá D.C.: Contacto grafico Ltda., 2008. ISBN 978-958-9383-81-0.

[5] ICONTEC. Norma técnica colombiana NTC 4490. Bogotá D.C.: Contacto grafico Ltda., 1998. ISBN 978-958-9383-81-0.

[6] ICONTEC. Norma técnica colombiana NTC 5613. Bogotá D.C.: Contacto grafico Ltda., 2008.

[7] LETÓN MOLINA, Emilio. Introducción al análisis de datos en Metaanálisis. Ediciones Díaz de Santos, 2006. p. 5 ISBN 84-7978-489.

[8] Making quantum encryption practical [En línea]. MIT News, Mayo 20 de 2013- [citada en Febrero 01 de 2014]. Disponible en internet: <http://web.mit.edu/newsoffice/2013/making-quantum-encryption-practical-0520.htmll>

[9] Quantum computing with light [En línea]. MIT News, Septiembre 09 de 2011- [Citada en Febrero 01 de 2014]. Disponible en internet: <http://web.mit.edu/newsoffice/2011/quantum-light-0909.html>

[10] RIVEST Ronald, Cryptography and the Limits of Secrecy [En línea] http://web.mit.edu/ssp/seminars/wed_archives99fall/rivest.pdf [Citada Enero 31 de 2014]

[11] SEQC. Metaanálisis. SEQC [En línea], ] Mayo 10 de 2008 [citada en Marzo 11 de 2014]. Disponible en internet:< http://dxsp.sergas.es/ApliEdatos/Epidat/Ayuda/11-Ayuda%20Meta-an%E1lisis.pdf>

[12] Tendencias científicas [en línea]. Marzo 24 de 2003. [Citada Enero 31 de 2014]. Disponible en internet < http://www.tendencias21.net/La-realidad-cuantica-revoluciona-el-mundo-de-la-informacion_a133.html> ISSN 2174-6850.

[13] Textos Científicos. Criptografía cuántica - Conceptos de criptografía [en línea]. Junio 24 de 2005. Disponible en internet <http://www.textoscientificos.com/criptografia/quantica> [Citada en Febrero 01 de 2014]