# Quantum cryptography

**Ilija Barukčić**
Horandstrasse, Jever, Germany.
Email: Barukcic@t-online.de

**How to cite this paper:** Ilija Barukčić (2016) Qunatum cryptography? http://vixra.org/

**Received:** 27.11.2016
**Accepted:** **27.11.2016**
**Published:** **27.11.2016**



## Abstract

The culmination of quantum entanglement, which can be measured, transformed, and purified, a lively and speculative domain of research, may serve as the foundation of the information-processing capabilities of quantum systems and provide one pillar of quantum information theory. A quantum information channel can be used to perform computational and cryptographic tasks. What is extraordinary about this phenomenon is that a possible alteration of the properties of a distant system (receiver, instantaneously or the probabilities of these properties) by acting on a local system (sender) should be impossible.

## Keywords

Quantum theory, Special relativity, Unified field theory, Causality

## 1. Introduction

In priniciple, one of the known examples of quantum cryptography is the so caled quantum key distribution. At quantum level, observation or measurements of quanta can changes its behavior. This can help to detect quickly non-desired observations by a third party and provides a method for secure communication. In this paper we will show how to transmit quantum mechanical observables by encrypting the same. The encrypted quantum mechanical observable may be received and decoded under some circumstances. In particular, (quantum) encryption is of use for secure communication (via networks, mobile telephones, wireless microphones, wireless intercom systems, Bluetooth devices and bank automatic teller machines et cetera) , to protect information stored on computers and storage devices and so on. Especially Bell's theorem is advocated for these puposes but the same is not necessary at all.

## 2. Material and Methods

### 2.1. Definitions

**Definition. Quantum Sender A**

Suppose A (Alice) and B (Bob) are spatialy separated and want to communicate a secret message, without revealing any information to C (Chris), an eavesdropper. Let $E({}_{A}X_{t})$ denote the original 'plain-text', the information which is to be communicated as a secret message such that only an authorized receiver B (Bob) can read it..

**Definition. Encryption and decryption key**

Let $f_{1}({}_{A}X_{t})$, $f_{2}({}_{A}X_{t})$, …, $f_{n}({}_{A}X_{t})$ denote some different encryption and decryption algorithm (cryptographic keys) used by the sender A (Alice) and the receiver B (Bob) to encrypt and decrypt the desired massage. Somebody who is not authorized to access data is excluded because the required decryption key is missed, without which it is impossible to read the encrypted information

**Definition. Quantum receiver B**

Suppose A (Alice) and B (Bob) are spatialy separated and want to communicate a secret message, without revealing any information to C (Chris), an eavesdropper. Let $E({}_{B}X_{t})$ denote the information as received by the observer B (Bob). The same information can be encrypted by the sender A.

### 2.2. Axioms

This theory is based on the following axiom.

Axiom I.

$$+1 = +1.$$

## 3. Results

### 3.1. The foundation of encryption and decrytption

**Claim.**
In general, it is

$$E({}_AX_t) = E({}_BX_t) / ( f_1({}_AX_t) + f_2({}_AX_t) +\ldots+ f_n({}_AX_t) )$$

**Proof.**
It is

$$+1 = +1 \qquad (1)$$

Multiplying by the information $E({}_AX_t)$ which has to be encrypted, we obtain

$$E({}_AX_t) = E({}_AX_t) \qquad (2)$$

The sender is encrypting his information by the key $(f_1({}_AX_t) + f_2({}_AX_t) +\ldots+ f_n({}_AX_t))$. It is

$$E({}_AX_t)\times(f_1({}_AX_t) + f_2({}_AX_t) +\ldots+ f_n({}_AX_t)\ ) = E({}_AX_t)\times(f_1({}_AX_t) + f_2({}_AX_t) +\ldots+ f_n({}_AX_t)) \qquad (3)$$

The receiver B receives an enrypted information $E({}_BX_t)$ as

$$E({}_BX_t) = E({}_AX_t)\times(f_1({}_AX_t) + f_2({}_AX_t) +\ldots+ f_n({}_AX_t)) \qquad (4)$$

To obtain the original information, the receiver B must decrypt the received information using a decrpytion key. We obtain

$$E({}_AX_t) = E({}_BX_t) / ( f_1({}_AX_t) + f_2({}_AX_t) +\ldots+ f_n({}_AX_t) ) \qquad (6)$$

**Q. e. d.**

*Scholium.*
In other words, it is

$$E({}_AX_t) = E({}_AX_t)\times( 1/1 ) \qquad (7)$$

or

$$E({}_AX_t) = E({}_AX_t)\times( (f_1({}_AX_t) +\ldots+ f_n({}_AX_t)) / (f_1({}_AX_t) +\ldots+ f_n({}_AX_t)) ) \qquad (8)$$

## 4. Discussion

Quantum encryption is of use to protect the confidentiality of private messages and to ensure that only who is authorized to access information. An authorized recipient should be able to easily decrypt a message with the key provided by the originator to recipients, but not to unauthorized interceptors. Still, in principle it is possible to decrypt a message without possessing the key, but, for a well-designed encryption key, very large computational resources and skill are required. Bell's theorem is not necessary for this puposes.

## 5. Conclusion

The use simple encryption algorithm can help to ensure secure private communication.

## Acknowledgements

None.

## References

[1] Wiesner, S. (1983) Conjugate Coding. SIGACT News, **15**, 78–88.

[2] Ekert. A. K. (1991) Quantum cryptography based on Bell's theorem. *Physical Review Letters*, **67**, 661-663.