Southern Federal University

Review of Synchronization Algorithms in Quantum Key Distribution Systems

Anton Pljonkin, Gennady Veselov, Sandeep Joshi and Pradeep Kumar Singh

SpacSec 2026

Introduction

Quantum Cryptography

Banknotes and notebooks

The history of quantum cryptography began back in the late 1960s, when Columbia University student Steven Wiesner told Charles Bennett the idea of quantum banknotes. They cannot be faked in principle, because it is excluded by the laws of nature. The essence of the idea was to place several quantum objects on each banknote. These can be, for example, traps with photons, each of which is polarized at a certain angle in one of two bases. Either at an angles of 0 and 90, or 45 and 135 degrees. The serial number is printed on a banknote, but the combination of polarizations and bases (filters, by means of which the photon polarization is measured or set) corresponding to the number is known only to the bank. To counterfeit such a banknote, the counterfeiter must measure the polarization of each photon. However, he does not know in which basis each of them is polarized. If he makes a mistake with the basis, the polarization of the photon will change and the counterfeit banknote will be incorrectly polarized.

Introduction

Shannon rules

The most valuable information is encryption keys. There are three rules for absolutely secret ciphers (Shannon rules):

- **If the key has a length equal to the message itself or even longer**
- **If the key is equiprobable**
- **If the key is used once**

then it is impossible to decipher the message in principle.

Quantum Key Distribution Systems

Transceiver station



Coding station



Quantum key distribution technology based on the laws of quantum physics to create sequences of random bits, which is used as a cryptographic key, for two remote users. It is believed that the QKD systems can meet the requirements of absolute secrecy when encrypting messages. A symmetric cryptosystem generates a shared secret key and distributes it among legitimate users for both encryption and decryption of messages. An attacker attempting to investigate transmitted data cannot measure photons without distorting the original message. Legal users on an open channel compare and discuss signals transmitted on a quantum channel, thereby verifying them for the possibility of interception. If they do not find any errors, then the transmitted information can be considered randomly distributed and secret, despite all the technical possibilities that a cryptanalyst can use.

Fiber optic only





Quantum Key Distribution Systems



SEQURENET
A QUANTUM KEY TO NETWORK SECURITY

SOUTHERN FEDERAL UNIVERSITY
SFedU
ROSTOV-ON-DON · TAGANROG

MITSUBISHI ELECTRIC

TOSHIBA

GENERAL DYNAMICS

THALES

BBN TECHNOLOGIES

MagiQ

QinetiQ

Telcordia

NEC

НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЯДЕРНЫЙ УНИВЕРСИТЕТ МИФИ

NASA

IBM

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени М.В.ЛОМОНОСОВА

id Quantique

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

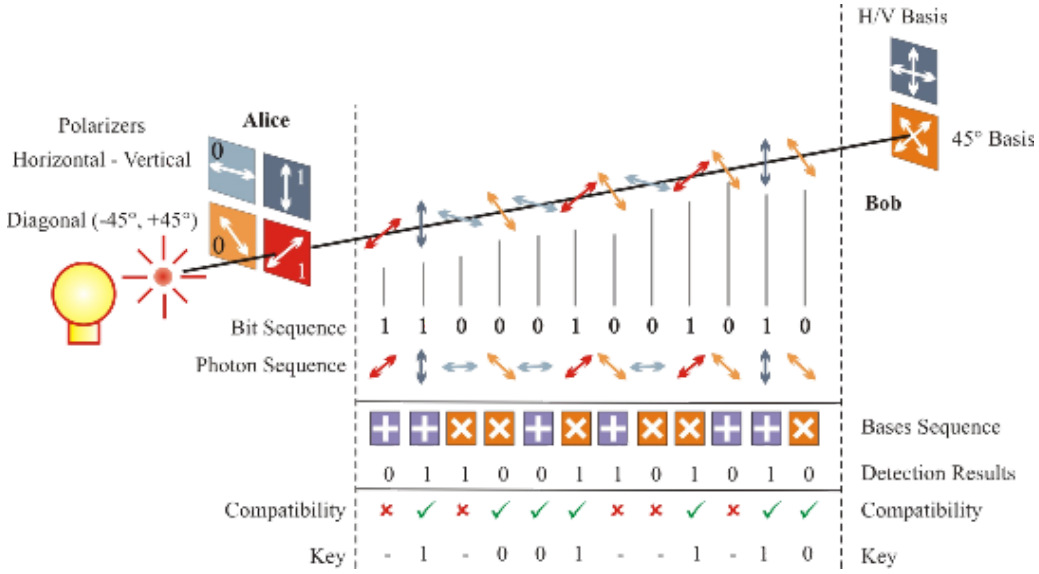
RQC
Russian Quantum Center

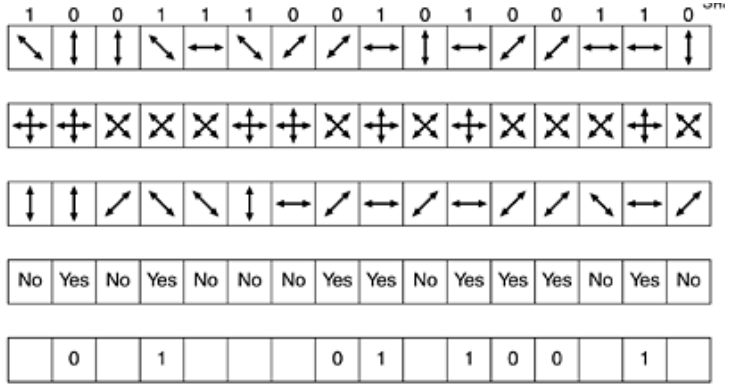
First Quantum Protocol

BB84

QKD systems operate under the control of quantum protocols. There are several protocols of quantum cryptography based on the transmission of information by coding the states of single photons, for example: BB84 (Bennett-Brassard-84), B92 (Bennett-92), BB84 (4+2), Koashi-Imoto, SARG04 and their modifications. Note that under the signal in QKD systems is meant the transmitted quantum state of the photon. The first protocol that was implemented in QKD systems is called BB84. Note that this protocol has more effective modifications. And in the last system of quantum key distribution (2016 produced by idQuantique) one-way protocol COW is applied.

The figure shows the known scheme of the protocol BB84, which shows: the sender's sequence (a*), the recipient's random basis (b*), the measurement result (c*), the coincidence result (d*), the one-time notepad key (e*), Yes - the match, No - the result does not match.





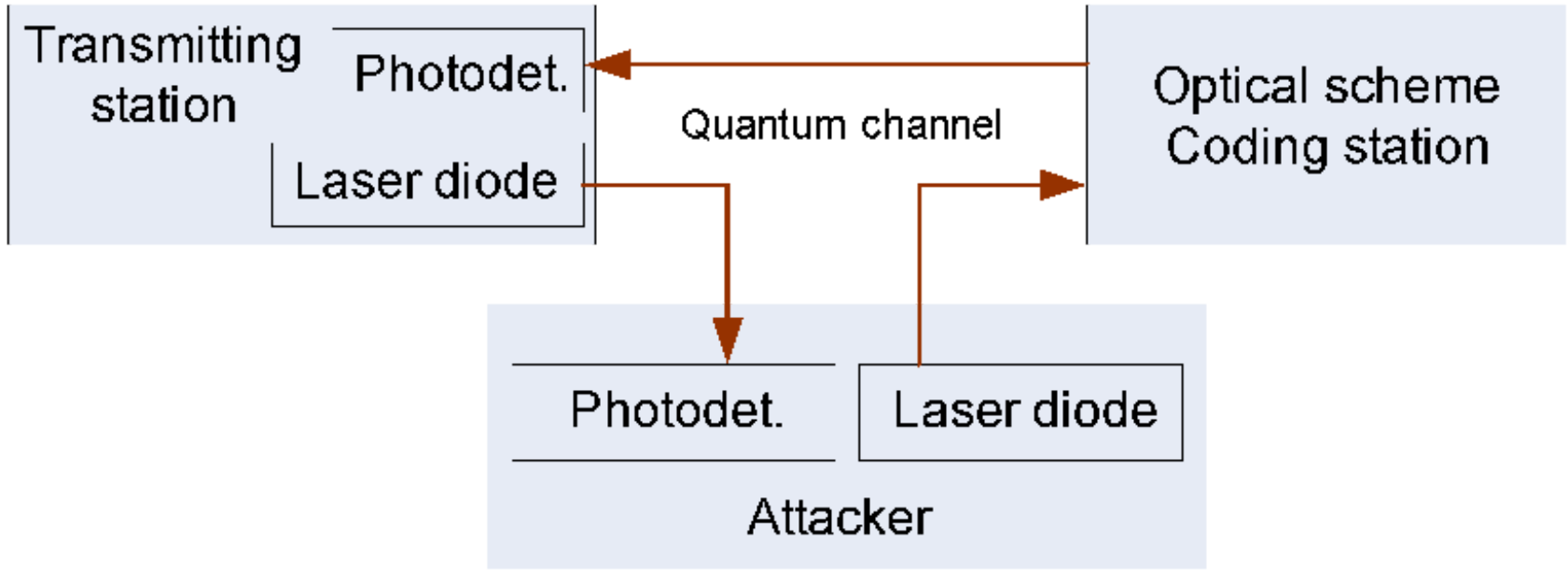
Synchronization

Attacks on the quantum communication channel

Analysis of the literature and experimental studies of a two-pass auto-compensation QKDS with phase coding of photon states show that the pre-synchronization process is realized in a multiphoton mode.

Theoretically, attacker is able to generate copies of optical pulses intercepted from the transceiver station and send them to the coding station. It is established that under this attack scheme, the percentage of quantum errors in the formation of a key with the presence of an attacker does not exceed the specified threshold. Thus, legitimate users Bob and Alice are not able to recognize the presence of an attacker in the quantum channel of fiber optic transmission line.

Dual fiber optic scheme

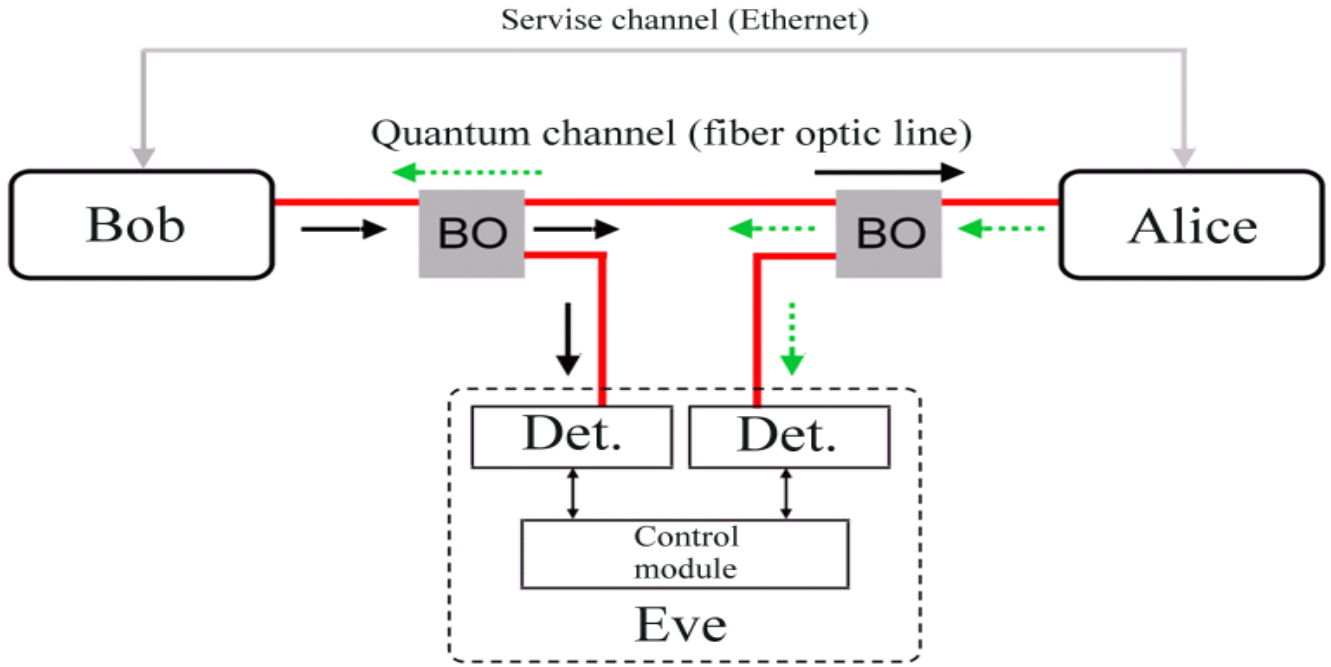


Synchronization

Attacks on the quantum communication channel

Such an implementation considerably complicates the attacker's task of unauthorized access to the quantum communication channel. As in the scheme described above, an attacker simulates the operation of a transceiver and a coding station. He intercepts signals from the receiving and transmitting station and directs the swing signals to the coding station. There pulses are coded, reflected and follow the same fiber optic path to the attacker. The moment of arrival (interception) of an optical pulse during a direct passage does not give complete information to an attacker about the operation of a QKD system (as in the case of using a two-wire circuit). The decisive moment is the appearance of an optical pulse in the backward propagation of a reflected signal in a quantum channel.

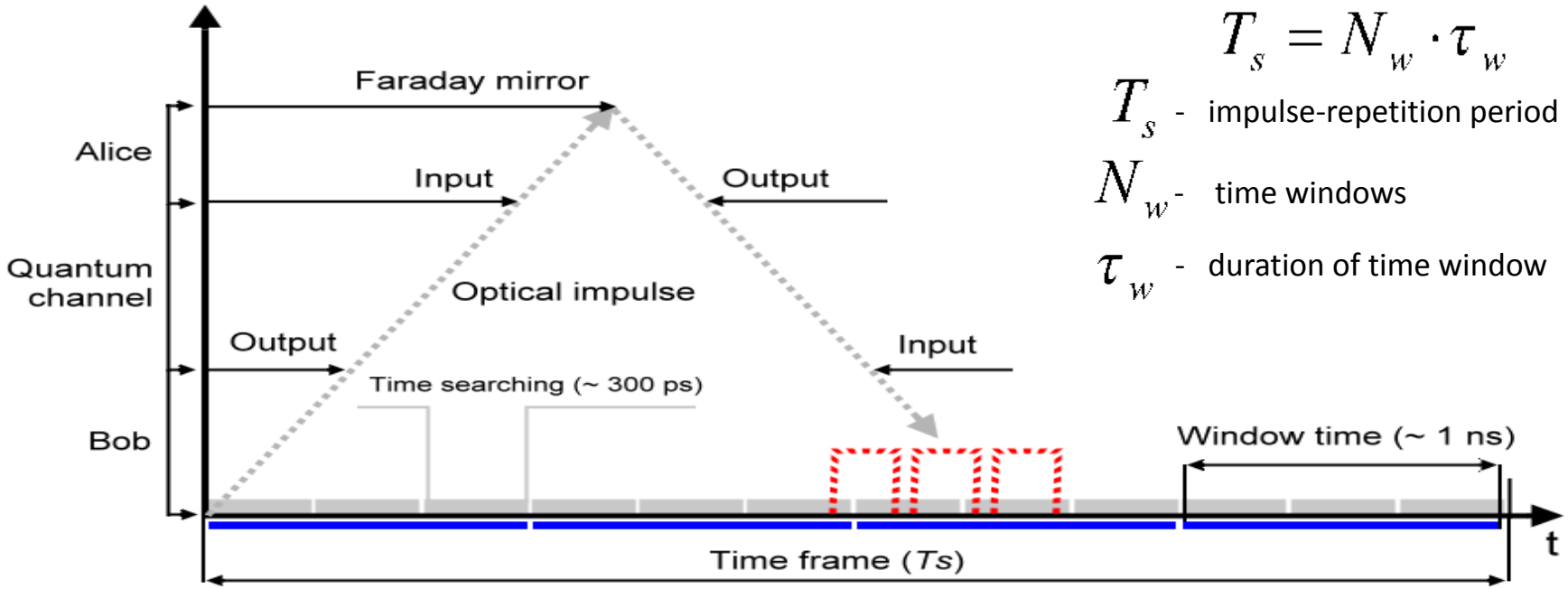
Scheme with single fiber optic channel



Synchronization

Recall that synchronization means the determination of the propagation path length of the optical pulse. The path length is not only the quantum communication channel itself, but also the lengths of all the fiber-optic components inside the stations. The optical path includes direct and reverse propagation of the signal.

Search for an optical synchronization signal scheme



$$T_s = N_w \cdot \tau_w$$

T_s - impulse-repetition period

N_w - time windows

τ_w - duration of time window

What's inside and what's next?

The slide shows a simple scheme of a quantum-cryptographic network. This is a valid stand that uses 512-bit keys.

