Quantum cryptography with pseudorandom bases and the problem of quantum state discrimination

P.A. Tregubov and A.S. Trushechkin

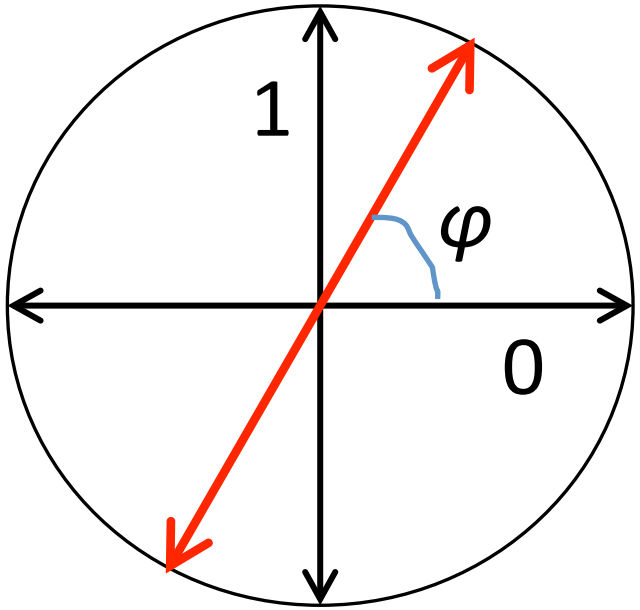
National Research Nuclear University “MEPhI”
Steklov Mathematical Institute
Russian Quantum Center

CTCrypt’16
Russia, Yaroslavl, June 6–8, 2016

Quantum cryptography

- Quantum cryptography and quantum computations are different things! Quantum cryptography does not need quantum computer
- In most cases, quantum cryptography is in fact quantum key distribution (QKD)
- I.e., if there is no eavesdropping and QKD is successful, Alice and Bob use the key to cipher messages using classical ciphers – GOST, AES, etc.
- If Alice and Bob detect eavesdropping, they abort the QKD protocol. The eavesdropper (Eve) does not obtain useful information, since there was no ciphering with insecure key.

Polarization of photon



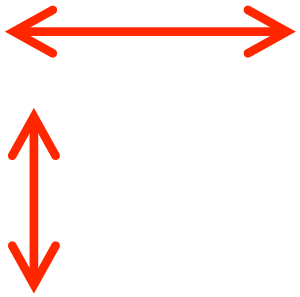
NB:
If you don't know φ,
the measurement
changes the state
(polarization)
of a photon

Probabilities of results:

$p_0 = \cos^2 \varphi$

$p_1 = \sin^2 \varphi$

New polarizations:



The role of quantumness

- If the light (signal) were classical, i.e., ininitely divisible, we could split a tiny part of it and measure this part – we get information with only negligible disturbance of the signal
- A photon is a minimal quantum (portion) of the light, indivisible, and the classical eavesdropping does not work

QKD protocol with pseudorandom bases

- Alice and Bob have an initial (short) secret key k
- They generate a pseudorandom sequence of angles $\varphi_1(k),\ldots, \varphi_N(k)$.
- Alice generates a random bit sequence $x_1,\ldots,x_N$
- Alice sends to Bob photons with polarizations $\varphi_1(k) + x_1\pi/2,\ldots, \varphi_N(k) + x_N\pi/2$
- Bob measures, whether the polarization is $\varphi_i(k)$ or $\varphi_i(k) + \pi/2$, obtains x_i
- Eve does not know $\varphi_i(k)$, hence, if she tries to measure photons, she introduces errors (some Alice's and Bob's values of x_i will differ)

QKD protocol with pseudorandom bases

- Alice and Bob randomly choose a test set T (subset of $\{1,\ldots, N\}$), public their values of x_i for i in T, and count the number of errors
- If the number of errors is too large, then Alice and Bob conclude that eavesdropping took place and abort the protocol
- If not, bits x_i not from T are used to establish a common secret key (error correction and privacy amplification)

Problem

- Rigorously prove the security of the QKD protocol (done for the BB84 protocol)
- In the most general case we assume that Eve obeys unlimited computing powet and quantum thechnologies (quantum memory, quantum computer).
  - She is limited only by the laws of nature
- *Unconditional (information-theoretic) security:* laws of nature + rigorous mathematical proof
- Device-independent proofs of security of QKD: Eve can even control the Alice's and Bob's QKD devices

Multiphoton pulses

- Problem: we cannot guarantee that every signal is strictly single-photon
- If there is more than one photon in the pulse, Eve can take one to her quantum memory
- Problem: how many photons Eve shoud have to calculate the initial key (seed) *k* and, hence, break the system?
- Analogous classical problem: how many terms of pseudorandom sequence are needed to calculate the secret seed?
- NB: we assume infinite computational power of Eve!

Mathematical formulation

- Let l be the length of the initial key (seed)
- Eve need to discriminate between 2^l quantum states, i.e., vectors of dimension 2^n:

$$\psi(k) = \begin{pmatrix} \cos\varphi_1(k) \\ \sin\varphi_1(k) \end{pmatrix} \otimes \ldots \otimes \begin{pmatrix} \cos\varphi_n(k) \\ \sin\varphi_n(k) \end{pmatrix}, \quad k \in \{0,1\}^l$$

  i.e., to find optimal measurement of them maximizing the guessing probability.

- Measurement: 2^l of positive-semidefinite $2^n \times 2^n$-matrices $\{M_k\}$:

$$\sum_{k\in\{0,1\}^l} M_k = Id, \quad p_{k'}(k) = \psi(k)^T M_{k'} \psi(k)$$

$$\frac{1}{2^l} \sum_{k\in\{0,1\}^l} p_k(k) = p_{succ}, \quad 1 - p_{succ} = p_{err}$$

Relation to classical mathematical statistics

- Discrimination of quantum states is a quantum analogue of discrimination between different probability distributions

Results

- $p_{err} \geq 1 - 2^{n-l}$ (rigorous result), hence, for $n \ll l$ Eve has practically no chance
- Under heuristic assumption that the pseudorandom sequence is "good" (indistinguishable from random):
- $p_{succ} \geq 1/(1 + 2^{l-n})$
- $p_{succ} \geq 1/2$ for n $\geq l$, hence, Eve breaks the system with non-negligible probability
- Relation to the Marchenko–Pastur law from probability theory

Results

- p_{succ} – probability of the successful guessing of the secret seed by Eve; $p_{err} = 1 - p_{succ}$
- $p_{err} \geq 1 - 2^{n-l}$ (rigorous result), hence, for $n \ll l$ Eve has practically no chance
- Under heuristic assumption that the pseudorandom sequence is "good" (indistinguishable from random):

  $p_{succ} \geq 1/(1 + 2^{l-n})$
- If $n = l - \Delta$, $\Delta \geq 0$, $n \to \infty$, then

  $p_{succ} \geq 2^{\Delta}\{1-2^{\Delta}[1 - 64/(9\pi^2)]\} \approx 2^{\Delta}(1 - 0{,}28\times 2^{\Delta})$
- $p_{succ} \geq 0{,}72$ for $n \geq l$, hence, Eve breaks the system with non-negligible probability

Conclusions

- New quantum key distribution protocol: use of the pseudorandom sequences
- Analysis of its security: quantum analogues of classical problems of breaking the cryptographic PRNGs, discrimination between probability distributions
- Hypothesis: the key generation rate of the new protocol will be greater than that of the BB84 protocol because of additional uncertainty for Eve