Security of quantum cryptography with heralded single photons

M. Lasota[1], K. Banaszek[2], R. Demkowicz-Dobrzanski[2]

[1]Faculty of Physics, Astronomy and Applied Informatics, Nicolaus Copernicus University, ul. Grudziadzka 5, 87-100 Torun, Poland

[2]Faculty of Physics, University of Warsaw, ul. Hoza 69, 00-681, Warsaw, Poland

1. Abstract

Although in theory quantum cryptography protocols can be proven to be totally safe, security of their implementations is limited due to some imperfections of our setup. Here we show a generalization of the simplified analysis [1] on this topic to the case of using any quantum cryptography protocol and heralded single photon source (HSPS) with any additional detection system. We also present a more detailed analysis of quantum key distribution (QKD) security (based on [2]) and numerically find the maximum attainable key generation rate as a function of distance for BB84 ([3]) and SARG04 ([4]) protocols.

2. QKD in practice

Problems:
- loses of photons inside a fiber connecting Alice and Bob
- limited detection efficiency and dark counts in Bob's detectors
- multiphoton pulses emitted by Alice's single photon source

Effect: The security of quantum cryptography protocols is strongly limited in practice and QKD can be safely performed only on short distances between the legitimate participants.

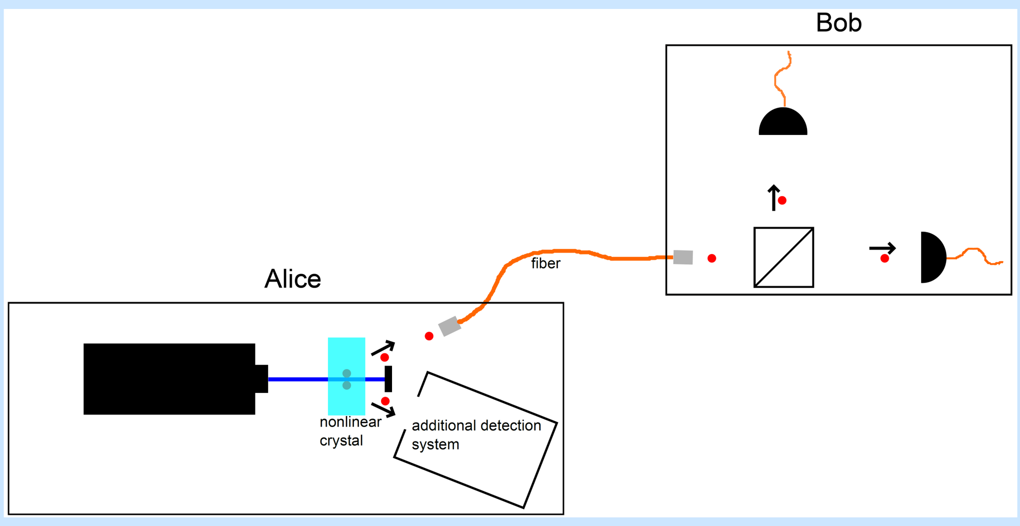

Figure 1: *A scheme for QKD with SPDC as a source of single photons.*

Some ways of improving the security:
- Alice can use HSPS and add an auxiliary detection system to her part of the QKD setup, strongly limiting the ratio of dark counts contributing to Bob's key.
- Alice and Bob can use a protocol, which limits the information Eve can get from multiphoton pulses emitted by Alice's source (*e.g.* SARG04 protocol)

3. Maximal distance of QKD security

Our goal: To find an approximate expression for the maximal distance of QKD security in the most general case *i.e.* without making any assumptions about the protocol or Alice's detection system.

Our result: Minimal required value of the complete transmission of a cryptography scheme for a given QKD process to be safe:

$$T_{\min} = 2\sqrt{y\frac{1-2Q_{th}}{Q_{th}}d_B\frac{q_0q_2}{q_1^2}} + \frac{1-2Q_{th}}{Q_{th}}d_B$$

y - fraction of multiphoton pulses which are useful for Eve in a given protocol
Q_{th} - quantum bit error rate (QBER) threshold (*i.e.* the maximum ratio of errors in Bob's key for a given QKD process to be safe in theory) for a particular case
d_B - ratio of dark counts in one of Bob's detectors
q_i - probability for one click in Alice's detection system when there were created i pairs in HSPS

Relation between minimal complete transmission of a QKD scheme and the maximal distance of security:

$$T_{\min} = \xi_B \times 10^{\frac{-(\alpha L_{\max}+\beta)}{10}}$$

ξ_B - detection efficiency of Bob's detectors
α, β - constants describing losses of light inside a particular fiber connecting Alice and Bob

4. Tree-like detection system

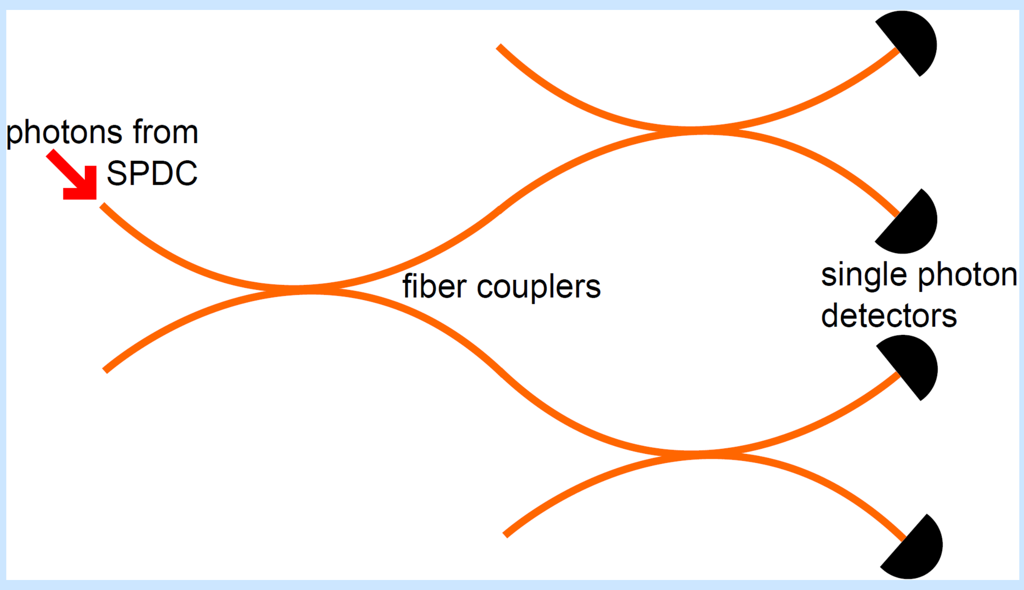

Figure 2: *An example of "tree"-like arrangement for detection of photons on Alice's side with four single photon detectors.*

Our goal: To find if tree-like detector could give us longer maximal distance of security than a simple single photon detector without photon number resolution.

In general case of 2^n detectors joined by $2^n - 1$ couplers:

$$\begin{cases} q_0 = (1-d_A)^{2^n-1} \times 2^n d_A \\ q_1 = (1-d_A)^{2^n-1} \times \left[2^n d_A(1-\xi_A\eta^n) + \xi_A\eta^n\right] \\ q_2 = (1-d_A)^{2^n-1} \times \Big[2^n d_A(1-\xi_A\eta^n)^2 + \\ \quad + 2\xi_A\eta^n(1-\xi_A\eta^n) + \frac{1}{2^n}(\xi_A\eta^n)^2\Big] \end{cases}$$

d_A - probability of a dark counts in one of the detectors
ξ_A - detection efficiency of the detectors
$1-\eta$ - loss of light in a single fiber coupler

Our result: $\lim_{d_A\to 0}\frac{q_0q_2}{q_1^2} = d_A\left(1 + 2^{n+1}\frac{1-\xi_A\eta^n}{\xi_A\eta^n}\right)$

Conclusion: Calculated ratio of $\frac{q_0q_2}{q_1^2}$ is the lowest for $n=0$. This implies that our proposed tree-like detector scheme can't increase maximal security distance for quantum cryptography.

5. Key generation rate

Dependency of key generation rate on the distance between Alice and Bob for different values of nonlinearity coefficient χ of the crystal used for production of photon pairs:

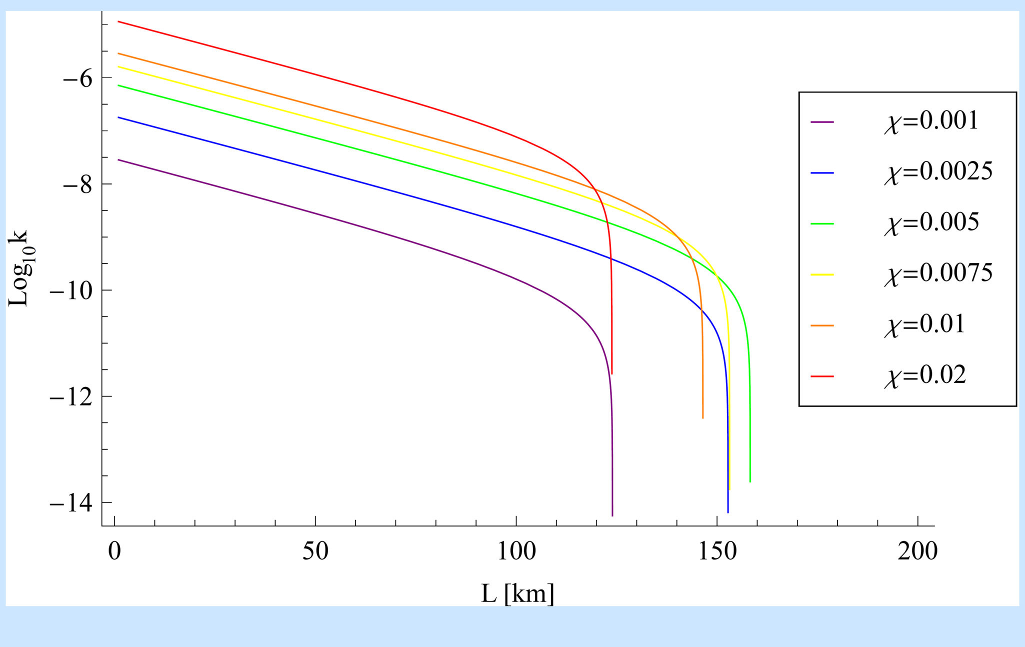

Figure 3: *Plot of* $\log_{10} k$ *(for BB84 protocol) as a function of* L *for six different values of* χ *and for the following values of the other parameters:* $\alpha = 0.2$, $\beta = 0$, $\xi_A = 0.6$, $\xi_B = 0.1$, $\xi_E = 1$ *and* $d_A = d_B = 5\times 10^{-6}$

Our goal: To find numerically the function of maximal key generation rate depending on distance between Alice and Bob for BB84 and SARG04 protocols.
Our result:

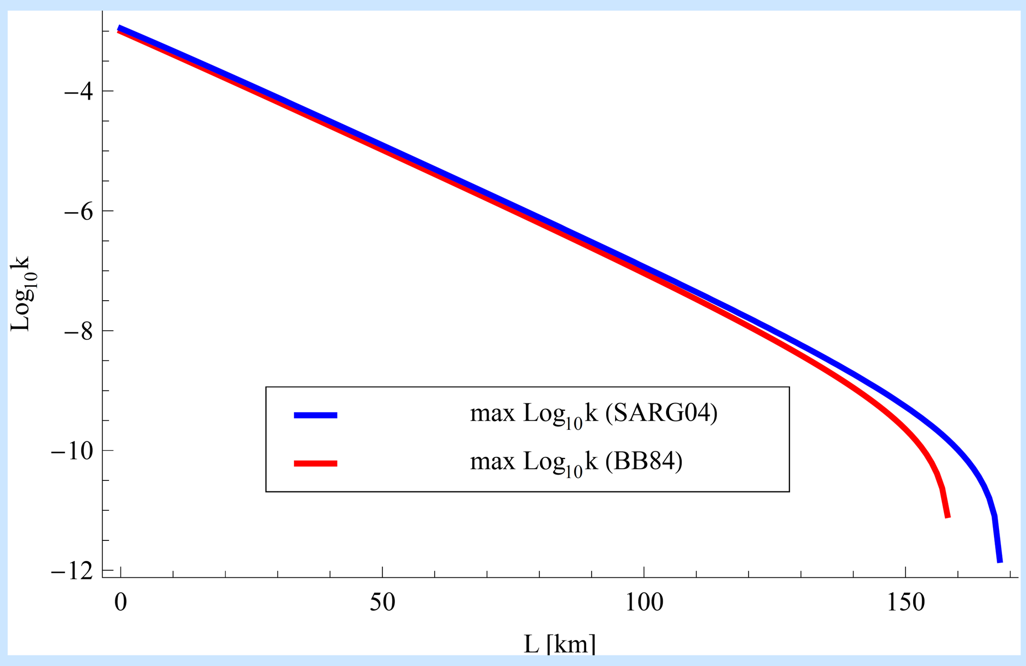

Figure 4: *Maximal key generation rate (comparison between BB84 and SARG04 protocols)*

Dependency of the maximal key generation rate on n for a tree-like additional detection scheme for distances far shorter than the maximal security distance:

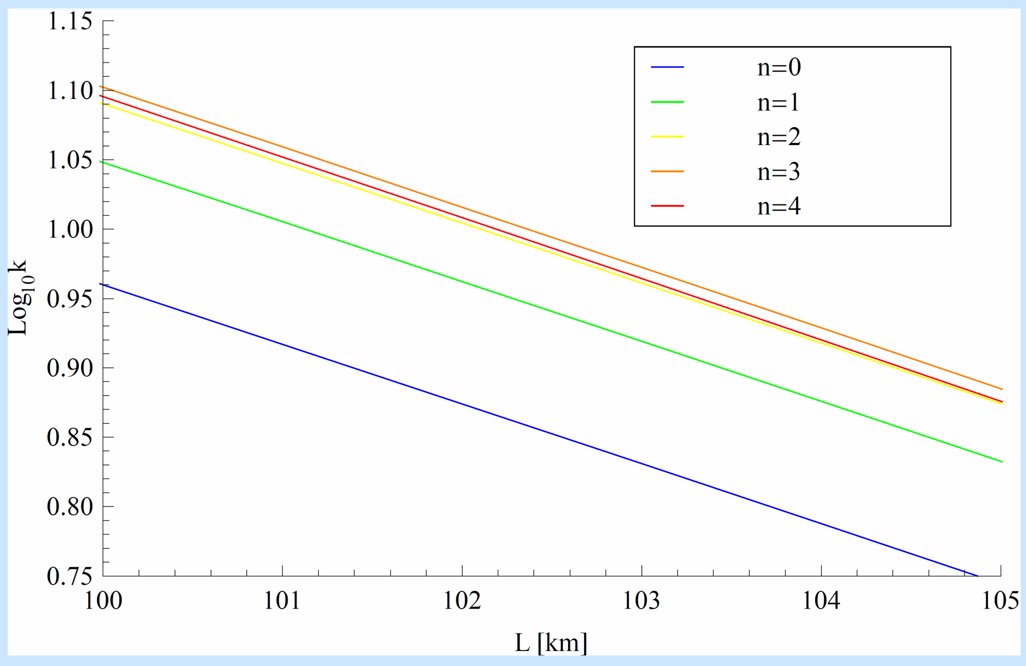

Figure 5: *A fragment of the plot of* $\log_{10} k$ *(for BB84 protocol) for* $100\,\text{km} < L < 105\,\text{km}$ *for different values of* n.

Conclusion: Using tree-like detection system, Alice can increase the ratio of key generation rate on distances much shorter than the maximal security distance.

References

[1] Phys. Rev. Lett. **85,** 1330–1333 (2000)
[2] Quantum Inf. Comput. **4,** 325–360 (2004)
[3] Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, December 1984 (Institute of Electrical and Electronics Engineers, New York, 1988), pp. 175–179.
[4] Phys. Rev. Lett. **92,** 057901 (2004)

The project "Photonic implementations of quantum-enhanced technologies" is realized within the TEAM programme of Foundation for Polish Science, cofinanced from European Union, Regional Development Fund (Programme Innovative Economy 2007-2013)

INNOVATIVE ECONOMY NATIONAL COHESION STRATEGY

FNP Foundation for Polish Science

EUROPEAN UNION EUROPEAN REGIONAL DEVELOPMENT FUND