Security of practical quantum cryptography with heralded single photon sources

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

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

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

1. Abstract

Although in theory quantum cryptography protocols can be proven to be totally safe, in practice their maximal distance of security and key generation rate (K) are limited due to several imperfections of a realistic setup [1]. While using a heralded single photon source (HSPS) (*e.g.* SPDC process) with additional binary on/off detector as the source of single photons for quantum key distribution (QKD) can increase the maximal distance of security in comparison with the case of using a laser emitting weak coherent pulses (WCP), over short distances it is still better to use WCP which gives higher K. Here we show that over intermediate distances between Alice and Bob, the best option is to use HSPS with multiplexing detection system, which gives higher key rate than HSPS with binary on/off detector and longer distance of QKD security than WCP.

2. Key generation rate

General formula for key generation rate:

$$K = p_{sift} p_{exp} \left[I_{AB} - y I_{AE}^{(1)} \left(\frac{Q}{y} \right) - (1-y) I_{AE}^{(2)} \right]$$

p_{sift} - probability of accepting a bit in the process of sifting
p_{exp} - total expected probability of a detection event
I_{AB} - mutual information between Alice and Bob
$I_{AE}^{(n)}$ - Eve's information on Alice's key from single photon ($n=1$) and multiphoton ($n=2$) events
y - fraction of single photon events among all the events registered by Bob
Q - QBER in Bob's version of the key

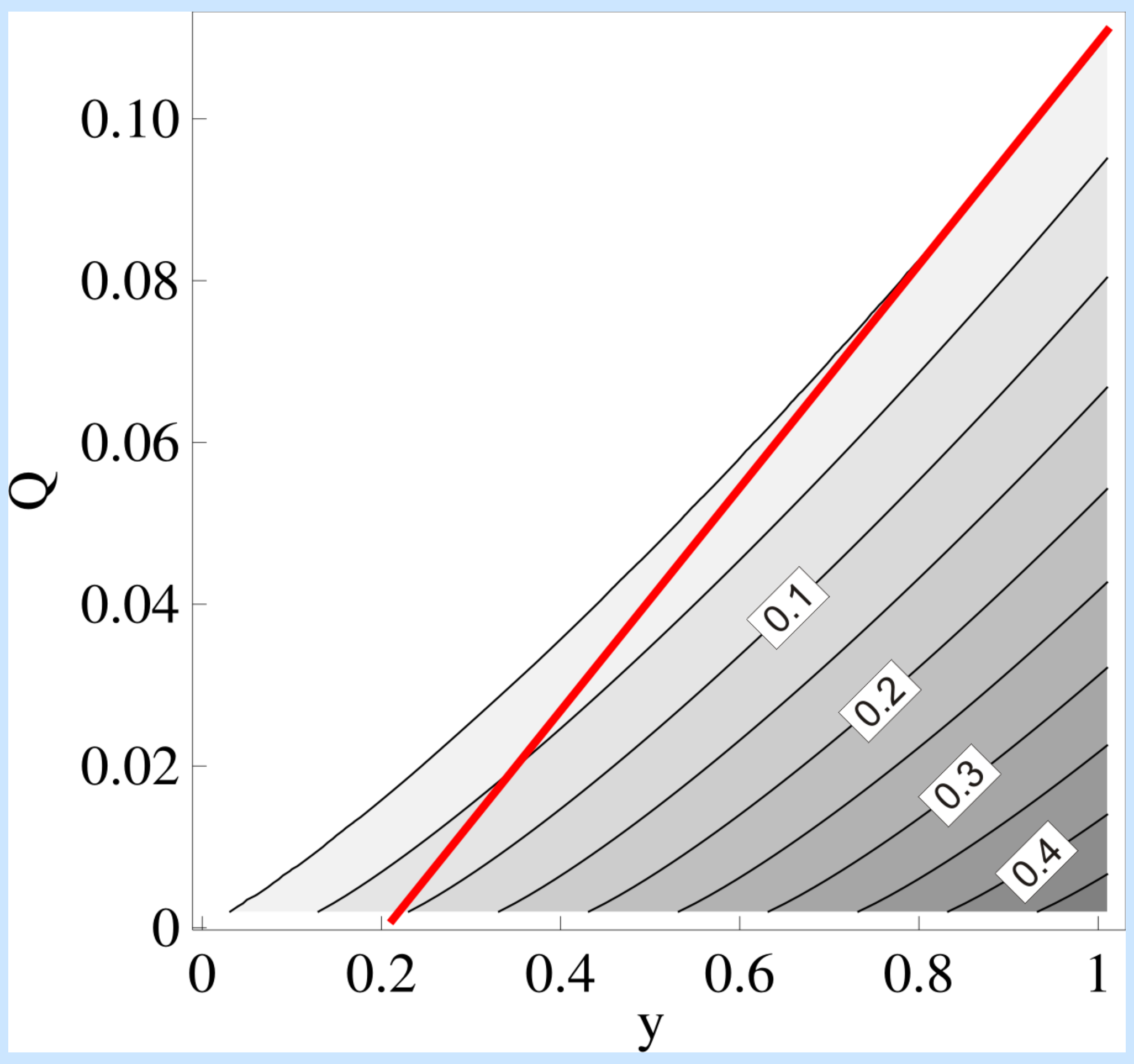

Figure 1: *$K(Q, y)/p_{exp}$ plotted for BB84 [2] protocol. The red line depicts the right hand side of the inequality (1) for $Q^{th} = 0.11$ and $\xi = 1.25$.*

Approximate condition for the positivity of K:

$$Q < Q^{th} \left[1 - \xi (1-y) \right] \qquad (1)$$

Q^{th} - threshold QBER for an ideal single photon source
ξ - factor describing the influence of source's imperfection (it can be calculated numerically)

3. Low and high transmission limits

Minimal transmission of the channel required for QKD security:

$$T_{min}^{HSPS} = d_B \frac{1-2Q^{th}}{Q^{th}} + \left(2 d_B \xi \frac{1-2Q^{th}}{Q^{th}} \frac{q_0 q_2}{q_1^2} \right)^{1/2} = \\ = T_{min}^{SGL} + \left(\frac{q_0 q_2}{q_1^2} \right)^{1/2} T_{min}^{WCP}$$

T_{min}^{SGL} - minimal transmission required for QKD security in the case of ideal single photon source
q_i - probability for one click in Alice's detection system when there were created i pairs of photons in SPDC process

Key generation rate in high transmission limit:

$$K^{HSPS} = \frac{q_1^2}{q_2} K^{WCP}$$

Relation between minimal transmission of the channel and the maximal distance of security:

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

η_B - detection efficiency of Bob's detectors
α, β - constants describing losses of light inside a fiber (in dB/km and dB respectively)

4. Multiplexing detection system

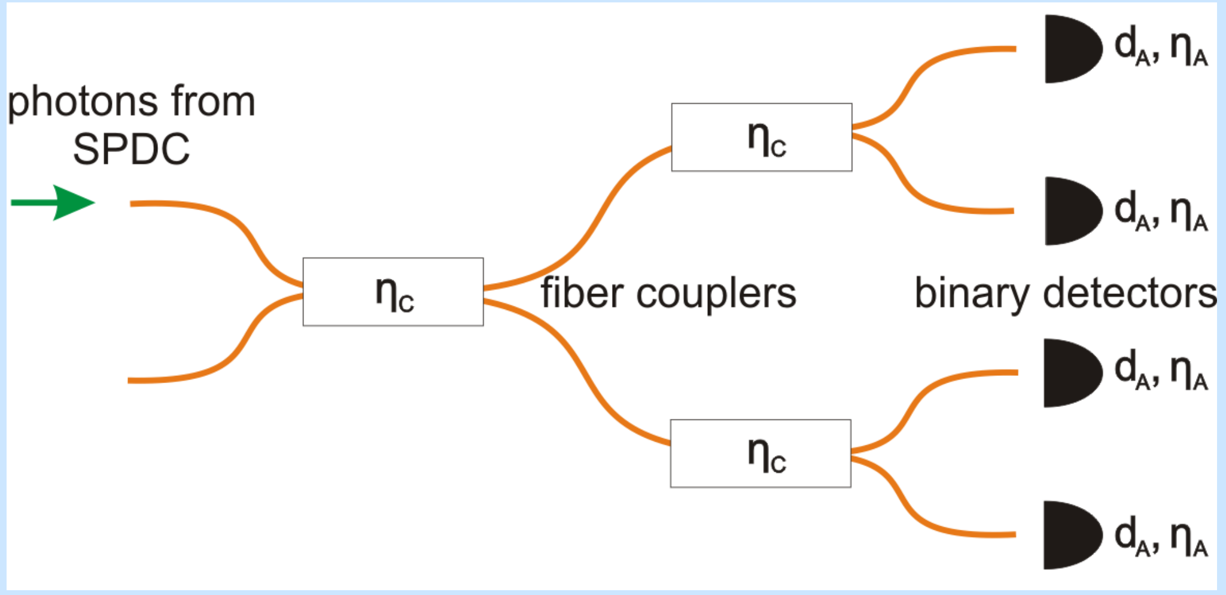

Figure 2: *An example of multiplexing arrangement for detection of photons.*

d_A - probability of a dark count in a detector
η_A - detection efficiency of a detector
η_C - transmission through an individual coupler

In general case of 2^N detectors and $2^N - 1$ couplers:

$$\boxed{\lim_{d_A \to 0} \frac{q_0 q_2}{q_1^2} = d_A \left(1 + 2^{N+1} \frac{1-\eta_A \eta_C^N}{\eta_A \eta_C^N} \right)}$$

Conclusions:
- $(q_0 q_2)/q_1^2$ is typically much lower than 1. Thus T_{min} is much lower for HSPS than for WCP QKD.
- $(q_0 q_2)/q_1^2$ is the lowest for $N = 0$. Thus multiplexing detection scheme cannot help in terms of maximal distance of security.

$$\boxed{\lim_{d_A \to 0} \frac{q_1^2}{q_2} = \left(\frac{2}{\eta_A \eta_C^N} + \frac{1}{2^N} - 2 \right)^{-1}}$$

Conclusions:
- For $N = 0$: **always** $K^{HSPS} < K^{WCP}$.
- For $N > 0$: it **can be** $K^{HSPS} > K^{WCP}$ for sufficiently good setup ($\eta_A \eta_C^N > \frac{2}{3}$) for $N \to \infty$).

5. Numerical results

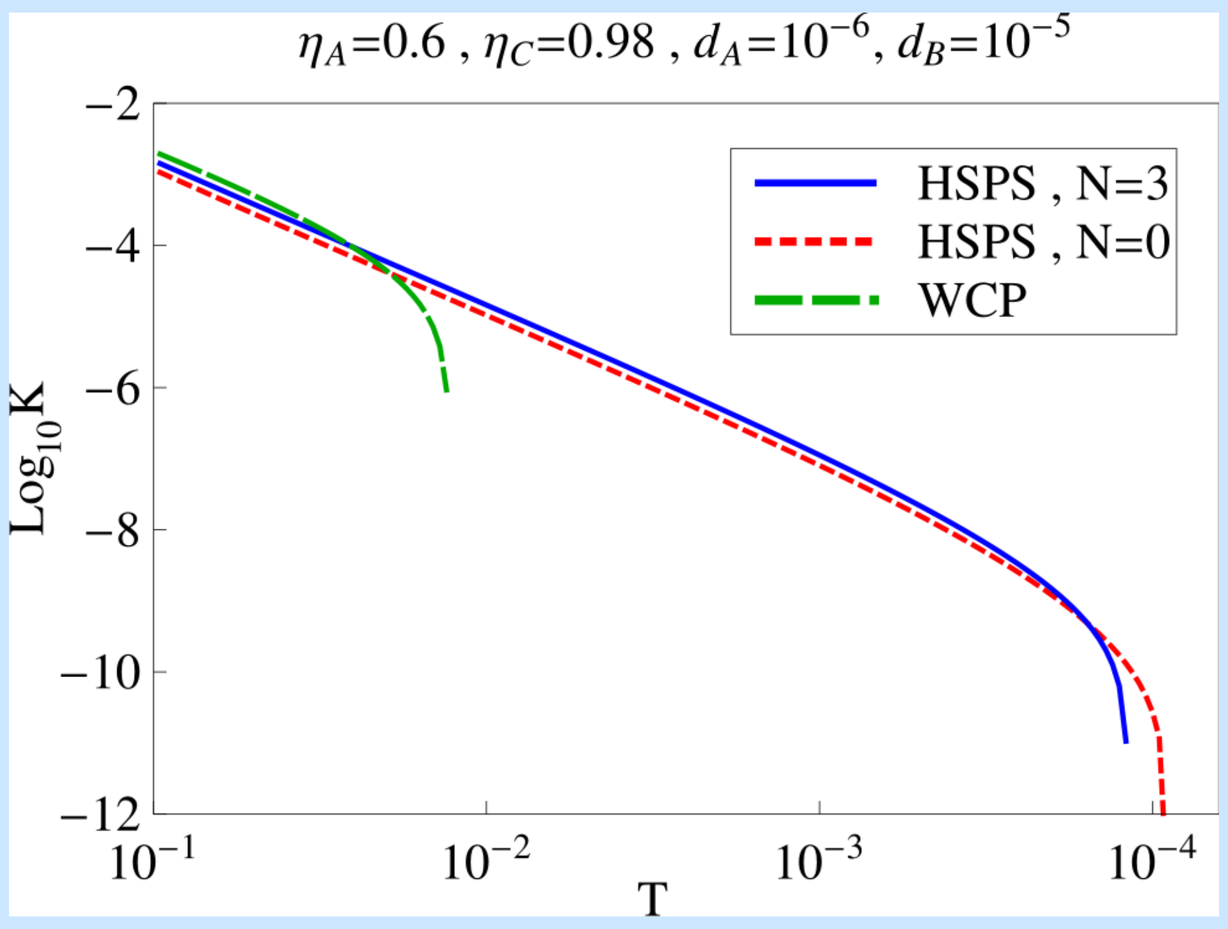

Figure 3: *Dependency of key generation rate on the transmission of the channel connecting Alice and Bob calculated numerically for some realistic values of important parameters of the setup (written above the figure) for BB84 protocol WCP and HSPS QKD with single binary on/off detector and multiplexing detection system with 8 detectors (for the chosen values of η_A and η_C maximal value of K on intermediate distances can be obtained for $N = 3$ – nearly 40% larger than for $N = 0$).*

Main conclusion:
For intermediate distance QKD it is best to use HSPS scheme with multiplexing.

References

[1] Phys. Rev. Lett. **85,** 1330–1333 (2000)

[2] 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.

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)

SEVENTH FRAMEWORK PROGRAMME

INNOVATIVE ECONOMY
NATIONAL COHESION STRATEGY

FNP
Foundation for Polish Science

EUROPEAN UNION
EUROPEAN REGIONAL
DEVELOPMENT FUND