Analysis of modulation parameters inequality in subcarrier wave quantum communication and its application to countering unambiguous state discrimination attack

A.A. Gaidash, A.V. Kozubov, V.I. Egorov, A.V. Gleim, G.P. Miroshnichenko

ITMO University, Department for Photonics and Optical Information Technology,
199034 Kadetskaya Line 3b, Saint Petersburg, Russia

Describing subcarrier wave quantum communication (SCWQC) system it is usually considered that legitimate quantum channel users (Alice and Bob) utilize identical electro-optical modulators (EOM) which process pulses in the same way. In our work we perform analysis of realistic modulation process and show how intrinsic EOM differences such as phase mismatch and unequal modulation indices (MI) affect secure key rates and prevent unambiguous state discrimination (USD) attack. The calculations were made for a practical SCWQC setup developed earlier [1].

Both EOM are synchronized providing the same phase of alternating electric field applied to them. However due to noises in electronics and non-perfect synchronization there might be some phase mismatch leading to increase of quantum bit error rate (QBER) and slight changes in raw key rates. Our developed mathematical model (based on [2]) takes into account this jittering of phase in the broadest sense, considering mean value of phase mismatch and its dispersion. The expressions for raw key rates and QBER are supposed to be integrated over additional phase distribution. Thus one can study its impact on resulting secret key rate.

Different MI of both EOM can also affect key distribution process. Their inequality can be considered as additional modulation with effective MI value equal to their difference. This effect leads to an increase of raw key rates due to higher mean photon number at SCWQC sidebands. At the same time, additional modulation produces photons at the sidebands even in case of otherwise destructive interference, leading to higher QBER values.

Using the developed EOM model, we consider unambiguous state discrimination (USD) attack [3] on SCWQC system. A standard technique used in SCWQC setup uses the carrier wave as a strong reference preventing adversary (Eve) to block unresolved pulses. If she leaves vacuum states at sidebands or chooses phases randomly, her actions can be detected due to increase of QBER. However, detecting the reference wave with high intensity requires spectrum filtration with very high extinction value, which can be an issue in practical implementations [1]. On the other hand, a weaker reference (quasi-classical carrier) might not give detection events for each pulse due to losses and quantum efficiency of the detector, leaving Eve a chance of unrevealed USD attack.

In our work we show how EOM parameter inequality can be used for detecting USD attacks on SCWQC. If Eve can block a fraction of pulses (sidebands and carrier together) with inconclusive results, she needs to increase their intensity in order to maintain raw key and carrier detection rates. However, the gain for sideband coherent states should be different to gain of the carrier, for instance due to nonlinear dependence of detection probability on intensity (saturation for quasi-classical carrier), resulting in different MI compared to Bob. Thus, this effect occurring in case of different MI prevents any possibility of unrevealed USD attack on SCWQC.

Presented results are valuable for precise parameter estimation of experimental SCWQC setups and analyzing its security aspects. SCWQC systems are prospective for network applications due to their unmatched spectral efficiency [1] and robustness against external conditions.

Acknowledgements
This work was financially supported by Government of Russian Federation, Grant 074-U01 and by the Ministry of Education and Science of Russian Federation (project № 14.578.21.0112, and contract № 02.G25.31.0229).

References

1. V. Gleim, V. I. Egorov, Yu. V. Nazarov, S. V. Smirnov, V. V. Chistyakov, O. I. Bannik, A. A. Anisimov, S. M. Kynev, A. E. Ivanova, R. J. Collins, S. A. Kozlov, and G. S. Buller. “Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using BB84 protocol with a strong reference”. Opt. Express, Vol. 24, No. 3, p.2619-2633, (2016).

2. G. P. Miroshnichenko, A. D. Kiselev, A. I. Trifanov, A. V. Gleim. "Algebraic approach to electro-optic modulation of light: Exactly solvable multimode quantum model". JOSA B, Vol. 34, No. 6, p.1177-1190, (2017).
3. M. Dušek, M. Jahma, N. Lütkenhaus. "Unambiguous state discrimination in quantum cryptography with weak coherent states". Physical Review A, Vol. 62, No. 2, 022306, (2000).