**Simulation and adaptation of DPS and DQPS QKD protocols for practical implementation and coexistence within PON architecture**

Nemanja Miljković, Petar Matavulj

*School of Electrical Engineering, University of Belgrade, Serbia*

e-mail: mnemanja92.etf@gmail.com

Technology of quantum computing and quantum computers is no longer topic of the future but the topic which represents one of the main focuses of nowadays research with fast traction and concrete practical results in last years. Taking this into account it became clear that all modern encryption algorithms will face serious challenges in incoming years especially if secure key exchange can’t be guaranteed. One of considered approach to overcome this problem is technology of Quantum Key Distribution (QKD) that guarantees key exchange security by the laws of fundamental physics. Previous decades of research led to various practical implementations of QKD with constant pressure for further improvement of performances while lowering down costs of the placement of this new technology within existing optical network infrastructure. Result of this urge are new protocols and new methodologies with one goal to simplify and expand possibilities of integration within modern optical networks including Passive Optical Network (PON).

Due to the fact that implementing QKD within PON has some specific requirements, like simple and low-cost integration and multi-user scalability, there was a need for pairing it with newly developed protocols like Differential Phase Shift QKD (DPS QKD) and Differential Quadrature Phase Shift QKD (DQPS QKD) [1]. Results of recent studies, covering practical network implementation [2], also showed that these protocols are probably the best fit for first generation of Quantum Access Network (QAN).

In our previous work we were focused on most mature and most widely implemented QKD protocols BB84 and B92 where we proposed generalized QKD authentication architecture to enhance security of authentication mechanism [3]. We performed simulation and system characterization for this architecture with main focus on comparing performances of three proposed schemes.

In this paper our focus is on simulation, characterization and adaptation of DPS-QKD and DQPS-QKD aimed for integration and coexistence within PON architecture, with special focus on state-of-the-art versions of GPON and NG-PON2 [4]. Following principles from our previous research we are investigating which adaptations of mentioned protocols and their combination can result in most secure and yet most easy to implement solution for QKD integration within PON. General authentication architecture is proposed for this set of protocols and different variations of the setup are simulated and compared.

ACKNOWLEDGEMENT: This work was financially supported by the Ministry of Science, Technological Development and Innovation of the Republic of Serbia under contract number: 451-03-137/2025-03/200103.

REFERENCES:

1. H. Takesue et al., 2008 First ITU-T Kaleid. Academ. Conf. 229-236 (2008).
2. N. Vokić et al., IEEE J. Sel. Top. Quant. Electron. 26, 3, 1-9 (2020).
3. N. Miljkovic et al., Opt. Quant. Electron. 50, 319 (2018).
4. <https://www.itu.int/rec/T-REC-G.989.2>