Optimum Resource Allocation in Secure Quantum Networks: Survey

Savo Glisic, Senior Member IEEE, Worcester Polytechnic Institute, Massachusetts, sglisic@wpi.edu

Abstract - Our recent paper provides a detailed survey of the work on quantum and post quantum cryptography schemes and emphasizes their applicability in 7G networks. A comprehensive insight is provided into the solutions which could possibly replace RSA and ECC- *schemes.*

The paper argues that most probably post quantum schemes will dominate 6G networks and due to implementation complex quantum solutions will be fully employed in 7G.

In this paper we survey work on limits on quantum channel capacity and secret key rates and then design a framework for optimum allocation of these resources in quantum networks.

After introduction in Section I, discussing the motivation of the paper, we introduce the concept of quantum computing with continuous variable CV and notion of entanglement in Sections II and Section III respectively. Using CV instead of discreate variable (DV) computing is more feasible for practical implementation whereas entanglement is a basic ingredient of quantum cryptography. In Section IV we survey work on quantum channel capacity and secret key rates and Section V how much these results can be improved by quantum coding. Section VI surveys work on quantum key distribution across the quantum network. Section VII presents an original contribution on optimization frameworks for resource (capacity or secret key rate) allocation in quantum network.

The paper is designed to be used as a seed material for setting up a research group in this field, be a base for the initial research papers of the group and the first project proposals to NSF solicitations in this field.

Index Terms- *q- Cry, q- key distribution (QKD), q- memories (m^{em}), q- Networks (qN), satellite (s^{tell}) qN, QKD over sub-optical (o^{pti}) bands, Qubit (qb) physics, q- circuit (c^{irc}) libraries, $\mathcal{J}^{mpl}$ examples of continuous variable CV QKD hardware*

NOTE: At this point we would like to point out that 6/7G networks will be, as all previous generations, open standards enabling competition between different technical solutions and standardizing a minimum of the system parameters that will be required to secure the compatibility of these solutions. For these reasons here we do not propose specific solutions for different problems that 6/7G networks will face, but rather a variety of technology enablers for the designer to choose from when building his own specific solution.

In this paper we use specific notation where some characteristic terms (t^{rm}'s), often repeated in the text, are replaced with corresponding acronyms representing the original t^{rm} and its derivatives (conjugations). This approach (compressed language) enables more precise characterization of the system processes and operations and a specific t^{rm} sound more like a system parameter that can be used more efficiently throughout the text. While this opens new options for the system presentation the writing occasionally sounds like an AI synthesized text. We hope the readers will easily get used to this style. In anticipation of what is coming in the field of ML and AI, this approach of integration of classical language and language of acronyms, might be further studied to increase the efficiency of Human-AI communication, maybe in the long run resulting in H-AI language. Light acronymization used in this paper, only for illustration purposes, may be further intensified. The depth of acronymization would depend on specific application.