Enabling Technologies for Quantum Security in 7G: Survey

Quantum Networks

Savo Glisic, Senior Member IEEE, WPI Massachusetts, sglisic@wpi.edu, savo.glisic@ieee.org

Abstract - Our recent paper provides a detailed survey of the work on post-quantum (q-) and q-cryptography (*Cry*) algorithms (a^{lg}*'s*) with focus on their applicability in 7G networks (n^{et}*'s*). A comprehensive insight is provided into the candidate a^{lg}*'s* to replace RSA and ECC schemes.

The paper argues that most probably post- q schemes will dominate 6G n^{et}*'s* and due to implementation complexity q-solutions will be fully employed in 7G.

Since the paper focuses on the cryptography a^{lg}*'s* as a follow up, in this paper, we cover the most important segments of q-n^{et}*'s* design to support these algorithms.

For the applications in 7G networks, existing work on q-key distribution over sub-optical bands, surveyed in Section II is essential. As a next step, results on dynamic q- n^{et}'s topology design are reviewed in Section III and it's optimization in Section IV including the work on q- n^{et}'s stability surveyed ibn Section V. Special space (Section VI) is devoted to survey of the work on q- n^{et}*'s* designed over satellite constellations since these networks are bases for global systems.

As a special contribution of this paper Section VII presents new optimization frameworks for energy efficiency optimization in q- satellite networks, cost efficient q-network topology design and optimum resource (capacity and secrete key rates) allocations in these networks.

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- Quantum Cryptography (q-Cry), q-n^{et}'s (N), Satellite qN, Quantum Key Distribution (QKD) over sub- optical bands,

NOTE: At this point we would like to point out that 6/7G n^{et}'s 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 n^{et}'s will face, but rather a performance/complexity comparison of a variety of technology enablers to choose from when building up a specific solution.

In this paper we use specific notation where some characteristic terms, often repeated in the text, are replaced with corresponding acronyms representing the original term and its derivatives (conjugations). This approach (compressed language) enables more precise characterization of the system (s^{yst}) processes and operations (o^{per}'s) and a specific term sounds more like a s^{yst} parameter that can be used more efficiently throughout the text. While this opens new options for the s^{yst} 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.