Quantum vs Post-Quantum Security for Future Networks: Survey

second revision

Savo Glisic, Senior Member IEEE, WPI, Massachusetts, sglisic@wpi.edu

Abstract: Classical cryptography (c^{rypt}) schemes (s^{che}) have been compromised by the practical results on quantum (q) computers in recent years. Nowadays these s^{che} 's can be compromised by using the Shor's methodology. This paper provides a detailed survey of the work on so called post- q c^{rypt} (PQC) s^{che} 's, which are based on different principles, minimizing the threats coming from advances of q- computers. Even so, post- q- s^{che} 's do not completely solve the problem (p^{rblm}) but rather represent (r^{prs}) a temporary solution. On the other hand, q- c^{rypt} (QC) and q- key distribution (d^{istr}) (QKD), discussed in this paper, offer the ultimate solution: by relying on entanglement ($\mathcal{E}^{gle}$) between q- states ($\mathcal{S}^{tat}$'s). At least in the beginning, a competition is anticipated between the two approaches to security (S) s^{che} 's, so the paper provides comprehensive survey of both QC and PQC algorithms ($\mathcal{A}^{lgrt}$'s), enabling full understanding of pros and cons when choosing implementation ($\mathcal{J}^{mpl}$) options in future networks (n^{et}'s).

To further encourage the n^{et} designers to consider q- solutions for future n^{et} 's, the paper presents original, fundamental research work on LEO satellite n^{et} optimization ($\mathcal{O}^{ptmz}$) $\mathcal{A}^{lgrt}$'s for global QKD. The solutions using exclusively LEO orbits instead the combinations of LEO and GEO orbits, considered so far, enable up to two orders of magnitude power savings which is of importance when it comes to $\mathcal{J}^{mpl}$ of the n^{et} using power constrained terminals. The $\mathcal{A}^{lgrt}$'s are designed for using q- Search $\mathcal{A}^{lgrt}$'s (QSA), like Grover $\mathcal{A}^{lgrt}$, and q- Approximate (a^{prx}) $\mathcal{O}^{ptmz}$ -$\mathcal{A}^{lgrt}$'s (QAOA), especially powerful for solving combinatorial $\mathcal{O}^{ptmz}$ -p^{rblm} 's. *Index Terms: PQC, QC, QKD.*

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.