**Improving cyber security using quantum computing**

***Abstract –*** The aim of this paper is to describe a new possible encryption algorithm which proposes to combine the facilities provided by quantum computing with the implementation of hash functions, symmetric and asymmetric-key algorithms as a result of quantum super positioning, as well as introduce readers to key aspects of quantum computing and elucidate its implications in present cryptography. In particular the reader can delve into the following subjects: present cryptographic schemes (symmetric and asymmetric), differences between quantum and classical computing, challenges in quantum computing, quantum algorithms (Shor’s and Grover’s), public key encryption schemes affected, symmetric schemes affected, the impact on hash functions, and post quantum cryptography. The experiments taken on the available data show a possible improvement compared to other related work due to a lower value of the Quantum Bit Error Rate, which is a metric for measuring how efficient and reliable a quantum algorithm is.

***ACM and AMS classifications:***

**AMS:**

81-XX Quantum theory

81Pxx Foundations, quantum information and its processing, quantum axioms, and philosophy

81P40 Quantum coherence, entanglement, quantum correlations

68-XX Computer science {For papers containing software, source code, etc. in a specific mathematical area, see the classification number -04 in that area}

68Mxx Computer system organization

68M25 Computer security

97-XX Mathematics education

97Pxx Computer science (educational aspects)

97P20 Theoretical computer science (educational aspects)

**ACM**:

* [D.](http://www.acm.org/about/class/ccs98-html#D.): Software
  + [D.4](http://www.acm.org/about/class/ccs98-html#D.4): OPERATING SYSTEMS
    - [D.4.6](http://www.acm.org/about/class/ccs98-html#D.4.6): Security and Protection
* [E.](http://www.acm.org/about/class/ccs98-html#E.): Data
  + [E.3](http://www.acm.org/about/class/ccs98-html#E.3): DATA ENCRYPTION
* [F.](http://www.acm.org/about/class/ccs98-html#F.): Theory of Computation
  + [F.m](http://www.acm.org/about/class/ccs98-html#F.m): MISCELLANEOUS

* [I.](http://www.acm.org/about/class/ccs98-html#I.): Computing Methodologies
  + [I.m](http://www.acm.org/about/class/ccs98-html#I.m): MISCELLANEOUS

**Table of contents**

1. Introduction
   1. Quantum cyber security in a nutshell
   2. Nowadays cyber security vs. quantum cyber security
2. Quantum era
   1. Security threats
   2. Possible solutions
   3. A new approach on improving security
3. Existing Work
4. Research Methodology
5. Results
6. Discussion
7. Conclusion