


Chapter 5

A Review on Quantum Computing and Security

K. Muthumanickam

 <https://orcid.org/0000-0003-2491-3253>

*Department of Information Technology, Kongunadu College of Engineering and Technology
(Autonomous), India*

P. C. Senthil Mahesh

Department of Computer Science and Engineering, Excel Engineering College, India

Mahmoud Ragab

Faculty of Computing and Information Technology, King Abdulaziz University, Saudi Arabia

ABSTRACT

Modern encryption methods are built upon the fundamentally “uncomfortable” process of computing huge integers to their primes. However, current cryptography is vulnerable to both increases in processing power and the emergence of quickly reversing huge integer factorization in mathematics. Therefore, incorporating quantum physics into encryption is the solution, which leads to an assessment of quantum cryptography. The field of cryptography and security is undergoing significant change as a result of the potential of scalable quantum computing. In this theoretical paper, the authors examine the development of quantum computing. The authors continue by listing the current threats to cryptographic primitives. Readers can deduce knowledge of a variety of topics from this review article, including risks posed by quantum technologies to traditional cryptography, modern cryptography – private key cryptography, post-quantum cryptography, quantum key distribution, and effects on hash functions and post-quantum cryptography.

INTRODUCTION

Quantum annealers and universal gate reliant quantum computers can be used to categorizes quantum computers in general (Johnson, 2011). Such computers or processors can be thought of as the quantum equivalent of a general-purpose microprocessor, and companies like IBM (IBM, 2001) and others are

DOI: 10.4018/978-1-6684-6697-1.ch005

A Review on Quantum Computing and Security

working feverishly to develop faster and more powerful universal gate-based quantum computers. The quantum annealers, on the other hand, are comparable to application explicit IC, which is capable of being used to resolve a particular set of combinatorial optimization issues over discrete search space. Although the development of universal quantum computers, which are not polynomial comparable to quantum annealer, is an important problem in the security field. However, the security risks posed by large-scale quantum computers are not the only thing driving their development.

Quantum computers have the potential to significantly improve performance in a number of areas, including machine learning, supply-chain optimization, molecular chemistry, and financial derivative pricing, to name a few. Additionally, there is a determined effort to show the supposed quantum gain even with noisy, small quantum computers (Arute, 2019). There are increasingly potent quantum computers that are made available by the manufacturers and system designers using cloud reliant services to test these algorithmic advancements. Software development kits are also made available by vendors like IBM, Google, Xanadu, Microsoft, and Rigetti to support design efforts. The ability of a quantum computer to achieve entanglement over a larger number of qubits and the capacity to carry out a huge number of quantum gate reliant operations specifically in a noise robust way are key indicators of its development. A number of physical qubits are required to operate a single qubit since accompanying error correcting codes are required. It may take up to 1000 physical qubits to actualize 1 logical qubit, depending on the error correcting codes used in the primary quantum reliant technology (Fowler, 2012). These factors must be taken into consideration when estimating the complexity of a quantum attack because, for all currently used cryptosystems, the quantum computing power currently available is insufficient to mount a successful attack.

Cryptology

Cryptology is nothing more than the phenomenon of message deception. To ensure that the intended recipient is the only one who can decipher the message, the sender initially sends it as cypher text. In the case that any unauthorized access was made, this inhibits its misuse. The opposite procedure, known as decryption, converts the cypher text back into the plain text so that the recipient can read the communication. In addition to ensuring data security, cryptology also aims to protect information's confidentiality, integrity, and authentication.

Quantum Computing

Our understanding of quantum computing is advancing as we make rapid strides in computer power. It has a greater potential for disruption than smartphones, the Internet, and cloud computing taken together. Due to the superposition property of a qubit, which can compare and handle all the values in between dual states, quantum computers are able to perform complex calculations a hundred million times quicker than conventional computers. This may alter the way mathematical operations are carried out, allowing for the simultaneous consideration of all potential calculations in an endless number of combinations (Haner, 2020).

17 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/a-review-on-quantum-computing-and-security/319863

Related Content

A Quantum Secure Entity Authentication Protocol Design for Network Security

Surjit Paul, Sanjay Kumar and Rajiv Ranjan Suman (2021). *Research Anthology on Advancements in Quantum Technology* (pp. 289-301).

www.irma-international.org/chapter/a-quantum-secure-entity-authentication-protocol-design-for-network-security/277779

Optimal Circuit Decomposition of Reversible Quantum Gates on IBM Quantum Computers

Hilal Ahmad Bhat, Farooq Ahmad Khanday and Khurshed Ahmad Shah (2023). *Handbook of Research on Quantum Computing for Smart Environments* (pp. 149-164).

www.irma-international.org/chapter/optimal-circuit-decomposition-of-reversible-quantum-gates-on-ibm-quantum-computers/319866

Quantum Internet and E-Governance: A Futuristic Perspective

Manan Dhaneshbhai Thakkar and Rakesh D. Vanzara (2021). *Research Anthology on Advancements in Quantum Technology* (pp. 247-266).

www.irma-international.org/chapter/quantum-internet-and-e-governance/277777

Tunable Attenuator Based on Hybrid Metal-Graphene Structure on Spoof Surface Plasmon Polaritons Waveguide

Aymen Hlali and Hassen Zairi (2022). *Technology Road Mapping for Quantum Computing and Engineering* (pp. 154-164).

www.irma-international.org/chapter/tunable-attenuator-based-on-hybrid-metal-graphene-structure-on-spoof-surface-plasmon-polaritons-waveguide/300522

Cyber Security: New Realities for Industry 4.0 and Society 5.0

Atharva Deshmukh, Disha Sunil Patil, Gulshan Soni and Amit Kumar Tyagi (2023). *Handbook of Research on Quantum Computing for Smart Environments* (pp. 299-325).

www.irma-international.org/chapter/cyber-security/319875