Chapter 5
Quantum Algorithms: Application Perspective

Renata Wong
https://orcid.org/0000-0001-5468-0716
Nanjing University, China

Amandeep Singh Bhatia
Chitkara University Institute of Engineering and Technology, Chitkara University, Patiala, India

ABSTRACT

In the last two decades, the interest in quantum computation has increased significantly among research communities. Quantum computing is the field that investigates the computational power and other properties of computers on the basis of the underlying quantum-mechanical principles. The main purpose is to find quantum algorithms that are significantly faster than any existing classical algorithms solving the same problem. While the quantum computers currently freely available to wider public count no more than two dozens of qubits, and most recently developed quantum devices offer some 50-60 qubits, quantum computer hardware is expected to grow in terms of qubit counts, fault tolerance, and resistance to decoherence. The main objective of this chapter is to present an introduction to the core quantum computing algorithms developed thus far for the field of cryptography.

INTRODUCTION

In recent years, quantum computing has become an area of high interest for both the academia and the industry. Although some companies such as IBM and Microsoft have made available quantum devices of up to 16 qubits and with varying qubit layouts, the era of quantum computing that would involve a number of qubits that facilitates useful and scalable quantum applications lies still well ahead. Once quantum computers become physically possible and economically viable, though, it is believed that they will be able to outperform classical devices, both in terms of the required space as well as time, by utilizing such quantum mechanical phenomena as superposition, entanglement and, equally importantly, destructive and constructive interference. It is clear however that quantum computers will not solve computationally

DOI: 10.4018/978-1-7998-6677-0.ch005

Copyright © 2021, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

unsolvable problems such as the halting problem. They might though be useful for certain problems for which classical algorithms are currently unable to provide efficient solutions.

The potential for quantum computing to become an important discipline was realized in 1994 with the emergence of Shor's algorithms for integer factorization and discrete logarithms (Shor, 1994). Shor's were the first quantum algorithms that offered a promise of a direct commercial usage especially in the field of cryptography. In 1996 quantum search algorithm (Grover) was proposed, which thanks to its simplicity proved to be applicable as a subroutine in many other quantum algorithms, such as quantum counting (Brassard, Høyer and Tapp, 1998) or protein structure prediction (Wong and Chang, 2020). While Shor's algorithms have applications in asymmetric cryptography, Grover's algorithm can be used to tackle symmetric keys.

The possibility of a practical development of quantum computers was given a boost with the publication by Arute et al. (2019) of their results of boson-sampling (Aaronson and Arkhipov, 2013) experiments on a noisy 53-qubit quantum device. These experiments are widely held as the first successful attempt at demonstrating that quantum mechanical computing methods might indeed be faster than classical ones for certain problems, despite the fact that no practical problem was solved by these experiments.

Quantum computing is intended to improve the computational performance of hard problems. As cryptographic algorithms are designed around assumptions of computational hardness of such problems as large prime number factorization, lattice problems such as lwe (learning with errors) (Regev, 2009), or that, more generally, $\boldsymbol{P^1NP}$. Quantum algorithms other than Shor's and Grover's might as well prove useful in handling information security issues.

The discorvery of the three quantum algorithms mentioned above has led to the development of the field of post-quantum cryptography (Bhatia and Zheng, 2020). It seeks to counteract against the potential threat of currently unbreakable classical codes being eventually broken by the quantum technology. Within the post-quantum cryptographic research, it is believed that certain lattice-based cryptographic optimization schemes will be insurmountable by quantum-mechanical methods (Peikert, 2016), (Bhatia and Kumar, 2019).

Table 1. Unexhaustive list of some of the most significant quantum algorithms developed thus far for cryptography

Quantum Algorithm	Proposed by
Integer factorization	(Shor, 1994)
Discrete logarithms	(Shor, 1994)
Unstructured search	(Grover, 1996)
Pell's equation & principal ideal	(Hallgren, 2002)
Shortest lattice vector	(Kuperberg, 2005)
Linear systems of equations	(Harrow, Hassidim and Lloyd, 2009)

In this chapter, the authors present the quantum algorithms that are currently the most relevant to quantum cryptography, as well as some of those that constitute advances in quantum computing and might thus one day be found to the applicable in cryptographic schemes due to the hardness of problems they optimize. The list of described algorithms is given in Table 1. For a broader selection of quantum algorithms, not only for cryptography, the reader is referred to the Quantum Algorithm Zoo (Jordan). A

18 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/quantum-algorithms/272366

Related Content

Adaptive LSB Substitution and Combination of LSB Substitution, PVD, and EMD
(2019). *Advanced Digital Image Steganography Using LSB, PVD, and EMD: Emerging Research and Opportunities (pp. 136-156).*
www.irma-international.org/chapter/adaptive-lsb-substitution-and-combination-of-lsb-substitution-pvd-and-emd/230060

Cryptographic Techniques Based on Bio-Inspired Systems
Petre Anghelescu (2020). *Cryptography: Breakthroughs in Research and Practice (pp. 99-119).*
www.irma-international.org/chapter/cryptographic-techniques-based-on-bio-inspired-systems/244908

A Brief Analysis of Blockchain Algorithms and Its Challenges
Rajalakshmi Krishnamurthiand Tuhina Shree (2019). *Architectures and Frameworks for Developing and Applying Blockchain Technology (pp. 69-85).*
www.irma-international.org/chapter/a-brief-analysis-of-blockchain-algorithms-and-its-challenges/230191

Reversible Watermarking in Medical Image Using RDWT and Sub-Sample
Lin Gao, Tiegang Gaoand Jie Zhao (2020). *Cryptography: Breakthroughs in Research and Practice (pp. 480-497).*
www.irma-international.org/chapter/reversible-watermarking-in-medical-image-using-rdwt-and-sub-sample/244934

Authentication of Smart Grid: The Case for Using Merkle Trees
Melesio Calderón Muñozand Melody Moh (2020). *Cryptography: Breakthroughs in Research and Practice (pp. 257-276).*
www.irma-international.org/chapter/authentication-of-smart-grid/244918