Cryptography in the World of Uncertainty

Islam Faisal

May 2018

Abstract

Quantum mechanics is a very complicated, yet influential field of physics. The recent rise of quantum computers has led to analogous algorithms in the quantum world doing what classical algorithms are doing right now. Cryptography is not special to this paradigm shift. In the future, quantum computers will be able to break some of the current established modern cryptosystems. This has led to directing the attention of cryptographers to building crypto algorithms that are resilient against quantum computers.

Some researchers overrate the threat of quantum computers. Quantum computers haven’t broken all of the known cryptosystems, and some are still resilient such as lattice-based cryptosystems, hash-based cryptosystems, and code-based cryptography. In this paper, we shed light on all of these aspects and give some parting thoughts on some of the challenging aspects in this field.

1 Introduction

Nobody knows exactly when quantum computing will become a reality, but when and if it does, it will signal the end of traditional cryptography.

Sergai Boukhonine

Cryptography is perhaps the foundational structure that keeps us safe online. It secures online transactions, e-commerce, web applications and many other types of services. Fortunately, most of the current cryptographic algorithms have proven strong for long time. However, unfortunately, this hardness is all based on assumptions. Determining if a cryptosystem is provably secure is a very hard task, so cryptography relies on reasonable assumptions about hardness of certain problems.

Moreover, these systems are not necessarily resilient against other paradigms of computing, of which is the quantum computer in which we are interested in this paper.
1.1 Quantum Computing

Quantum computing refers to the interdisciplinary branch of physics, mathematics, and computer science that is tasked with building basis, infrastructure, and algorithms for a paradigm of computing that utilizes concepts from quantum mechanics. Unlike electronic computers which depend on having data in either of two forms (1, 0), quantum computation uses quantum bits, which can be in superpositions of states $^1$.

Quantum computation has developed many algorithms for problems from classical computer science such as information theory including error correction, and detection, communication theory, and cryptography.

1.2 Motivation

Quantum computers have had its share of takes against the cryptography domain. Many quantum algorithms are now expected to be more efficient and secure. Also, some of the classical algorithms have been deemed weak against quantum computers. This necessitates the careful consideration of the intersection of the domains of crypto and quantum computing which is the topic of this paper.

Outline The rest of this paper is organized as follows: Section 2 describes the threat of quantum computers to cryptosystems. Section 3 introduces the solutions which include quantum and post-quantum algorithms. Section 4 continues with discussions on challenging aspects of this field, and finally section 5 concludes the paper.

2 What is the problem?

The problem with current cryptographic primitives is that many of them are not resilient against quantum computers. The Shor’s algorithm [1], introduced in 1994 provides a polynomial time algorithm for quantum computers to solve central problems in crypto such as the factorization of integers. Hardness of Factorization of integers is an underlying assumption in many cryptographic primitives. This algorithm is now public, and just awaits the introduction of large scale quantum computers to be executed.

Although quantum computers pose a great threat to cryptography, may researchers over-rate the impact of quantum computers on cryptography. So far, there are many crypto algorithms that are still resilient $^2$ against quantum computers such as: hash-based cryptography, code-based cryptography, lattice-based cryptography, or multivariate-quadratic-equations cryptography [2].

$^1$https://en.wikipedia.org/wiki/Quantum_computing
$^2$Because no attacks were found so far.
3 What are the solutions?

The solution to this threatening problem extends in two classes. One class of researchers are trying to introduce new algorithms that can be run on quantum computers. The other class introduces crypto algorithms that can be run on today’s computers but that depend on algebraic structures that are not broken via quantum computers so far such as lattices, or Ring Learning-With-Errors (RLWE).

3.1 Quantum Cryptography

One of the directions to overcome the weakness of some crypto primitives is building crypto algorithms for quantum computers. These rely on two principles from physics; the uncertainty principle and the no-cloning theorem. Of the famous quantum crypto algorithms is the Quantum key distribution (QKD) algorithm. Similar to the Diffie-Hellman key exchange protocol in classical crypto, QKD allows to parties to share a random secret key that they can both use later to encrypt and decrypt messages.3

3.2 Post-Quantum Cryptography

The algebraic structures used to build public-key cryptography when it first appeared were groups. Groups of integers, elliptic curves, and other types of groups have an underlying problem called the discrete logarithm problem (DLP). Cyclic groups have a special element called a generator, symbolized usually as $g$. A generator can be raised to different “powers”, each time obtaining a new element, up till the order of the group $n$, we have $g^n = e$ where $e$ is the identity element.

Given an element $x$ in a group $G$ with generator $g$, determine the discrete logarithm $h$ such that $g^h = x$. This problem is believed to be hard under the classical computing paradigm but fails in front of quantum algorithms.

One remedy is instead of using groups, we use another algebraic structure called lattices. The class of hard problems in the lattice world is related to optimization problems which are believed to be computationally infeasible, and no quantum algorithm so far can solve it efficiently.

3.2.1 Real-World Examples

In the real world, some organizations are experimenting with implementing post-quantum crypto algorithms in their products. Google has experimented with embedding an algorithm called A New Hope [2] on top of the classical encryption algorithm in one of its Google Chrome extensions [3]. This is a wise choice of wanting to experiment with new technologies, while relying on back-ups if this new technology is deemed to be a failure.

3https://en.wikipedia.org/wiki/Quantum_computing
4 Discussions

In this section, we give thought to some of the related aspects to quantum cryptography and the possibility of having efficient quantum computers in the future.

4.1 Scale of Quantum Computing

Research will still pour into quantum crypto and quantum computing, as the physics community is geared up to accept large amounts of government money, but there will be no full size quantum computers capable of factoring RSA keys. No-one will use quantum crypto.

---

Adi Shamir

Although quantum computers are improving, it is projected that it is still a while before a collaborative engineering work can lead to a masterpiece of a large-scale quantum computer. The recent advances point to 50-qubit quantum computers [4] which is still far from the bar that would result in the collapse of modern cryptosystems. However, this growth rate is not accurately predictable, and since the implementations are scalable, one can expect major leaps that can happen and lead to this quantum dream being possibility.

4.2 Hardness Assumption

Most of the researchers in cryptography are still focused on classical crypto. This makes the crypto algorithms rising in the quantum and post-quantum paradigms lack the horizon of scrutiny they receive in the classical world. Also, the algorithms are of short age. For example, New Hope that we just talked about has been published in 2016. The hardness assumptions associated with these algorithms are not as established as with classical public-key cryptography.

4.3 Retrospective Decryption

Some people mistakenly think that quantum power is a fear to be feared in the future only. However, the power of quantum computing threatens secrets communicated also nowadays. Military and top secrets are usually intended to be kept for large durations (sometimes hundreds of years). Imagine if a large-scale quantum computer is out 50 years from now. It can be used to decrypt messages from the past that were recorded but weren’t understood back then [5].
4.4 Blockchains and Financial Crypto

Indeed, cryptography will be affected by the emergence of large-scale quantum computers. However, cryptographic primitives are just the building blocks to large-scale security and privacy systems. This includes re-factoring protocols for auctions, bidding, and other protocols in the field of financial cryptography.

Being the one getting all attention of financial technologies right now, blockchains will probably be a critical target in the future. It is expected that they lead a revolution on the way financial systems are organized. Protecting blockchains and specially cryptocurrencies such as the bitcoin [6] will be a major task in quantum crypto. Some researchers have introduced early concepts for quantum-secured blockchains [7]. These ideas are expected to grow more in the future as the blockchain community is more oriented towards these concerns.

5 Conclusion

As we have seen, quantum computing is a very promising field with a lot of changing dynamics. It is going to affect a lot of domains in the field of computer science, including complexity theory, information theory, and cryptography. The Shor’s algorithm which, deems some of the classical cryptosystems a failure, requires the shift in the crypto community towards new paradigms and directions in resilient and efficient crypto.

The question of whether large-scale quantum computers is realizable in the near future is an open question. The answer will be determined in the next decades based on the performance and collaboration between physicists, mathematicians, computer scientists, and engineers.

References

[4] W. Knight, “Ibm raises the bar with a 50-qubit quantum computer,”