Quantum computing

Sean Hallgren[1] and Ulrich Vollmer[2]

[1] The Pennsylvania State University.
[2] Berlin, Germany.

In this chapter we will explain how quantum algorithms work and how they can be used to attack crypto systems. We will outline the current state of the art of quantum algorithmic techniques that are, or might become relevant for cryptanalysis. And give an outlook onto possible future developments.

1 Classical cryptography and quantum computing

Quantum computation challenges the dividing line for tractable versus intractable problems for computation. The most significant examples for this are efficient quantum algorithms for breaking cryptosystems which are believed to be secure for classical computers. In 1994 Shor found quantum algorithms for factoring and discrete log, and these can be used to break the widely used RSA cryptosystem and Diffie-Hellman key-exchange using a quantum computer. The most obvious question this raises is what cryptosystems to use after quantum computers are built. Once a good replacement system is found there will still issues with the logistics of changing every cryptosystem in use, and it will take time to do so. Furthermore, the most sensitive of today's encrypted information should stay secure even after quantum computers are built. This data must therefore already be encrypted with quantum resistant cryptosystems.

Classical cryptography [12, 13] consists of problems and tools including encryption, key distribution, digital signatures, pseudo-random number generation, zero-knowledge proofs, and one-way functions. There are many applications such as signing contracts, electronic voting, and secure encryption. It turns out that these systems can only exist if there is some kind of computational difficulty which can be used to build these systems. For example, RSA is secure only if factoring is computationally hard for classical computers to solve. However, complexity theory does not provide the tools to prove that an efficient algorithm does not exist for a problem. Instead, decisions about which problems are difficult to solve are based entirely on empirical evidence. Namely, if researchers have tried over a long period of time and the problem still seems difficult, then at least it appears difficult to find an algorithm. In order to understand which problems are difficult for quantum computers, we must conduct a long-term extensive study of the problems by many researchers.

Designing cryptographic schemes is a difficult task. The goal is to have schemes which meet security requirements no matter which way an adversary may use the system. Modern cryptography has focused on building a sound foundation to achieve this goal. In particular, the only assumption made about an adversary is its computational ability. Typically one assumes the adversary has a classical computer, and is restricted to randomized polynomial time. But if one now assumes that the adversary has a quantum computer, then which classical cryptosystems are secure, and which are not? Quantum computation uses rules which are new and unintuitive. Some subroutines, such as computing the quantum Fourier transform, can be performed exponentially faster than by classical computers. However, this is not for free. The methods to input and output the data from the Fourier transform are very restricted. Hence, finding quantum algorithms relies on walking a fine line between using extra power while being limited in some important ways. How do we design new classical cryptosystems that will remain secure even in the presence of quantum computers? Such systems would be of great importance since they could be implemented now, but will remain secure when quantum computers are built. Table 1 shows the current status of several cryptosystems.

Cryptosystem	**Broken by Quantum Algorithms?**
RSA public key encryption	Broken
Diffie-Hellman key-exchange	Broken
Elliptic curve cryptography	Broken
Buchmann-Williams key-exchange	Broken
Algebraically Homomorphic	Broken
McEliece public key encryption	Not broken yet
NTRU public key encryption	Not broken yet
Lattice-based public key encryption	Not broken yet

Table 1. Current status of security of classical cryptosystems in relation to quantum computers.

Given that the cryptosystems currently in use can be broken by quantum computers, what would it take for people to switch to new cryptosystems safe in a quantum world, and why hasn't it happened yet? First of all, the replacement systems must be efficient. There are alternative cryptosystems such as lattice-based systems or the McEliece system, but they are currently