Chapter 1

Physical Security in Quantum Key Distribution

Contents

1.1 Cryptography in the Age of Quantum Computers

For a decade or two now, Quantum Computing has been creating a buzz that nobody in Computer Science and adjacent fields could evade. Originating in the 1980ies as a highly academic fusion applying concepts from Computer Science in Quantum Physics, its concepts have long found their way into popular science articles. Quantum Computing encompasses a model of computation that is fundamentally different from the *classical*[1] digital circuits that underly all of modern computing. While at first this might seem like a step backwards into the era of early 1900s analog computing, the capabilites of a future quantum computer promise to far outpace those of contemporary classical computers. Key to this improved processing capability is a property called *Quantum Parallelism*. What this refers to is the fact that a quantum computer's internal state can simultaneously represent a multitude of states of a classical, digital computer, and the quantum computer can operate on all those states at once using a single quantum operation.

Applying Quantum Parallelism to practical problems is far more complicated than, e.g., translating a digital circuit solving some equation to a quantum circuit, but for certain problems we already know *quantum algorithms* that for large inputs solve these problems much faster than any classical computer ever could. Two of these algorithms, one by Shor and one by Grover are what caused most of the buzz around the field of quantum computing, because they spell trouble for a large part of modern cryptography.

Besides the computational speed-up promised by Quantum Parallelism, there is one more interesting aspect of Quantum Computing where it radically deviates from classical computing. The reason modern cryptography exists is that when we transmit (or store!) classical information through some channel (or storage!) that we do not control, there is nothing we can do to prevent an attacker from reading this information. Even with cryptography we cannot prevent this, but cryptography gives us tools to very effectively make whatever information the attacker is able to read useless to them.

A basic principle of Quantum Physics is the *No-Cloning Theorem*, which states that it is impossible to create an identical, independent copy of an arbitrary, unknown quantum state. An implication of this theorem is that when we encode classical information into quantum states in just the right way, we can make it so that an attacker atttempting to eavesdrop on our quantum information can only actually read this information by destroying it in the process. This property can be exploited to replace a number of classical asymmetric primitives in interactive settings, the most popular application of which is replacing an asymmetric Diffie-Hellman key exchange with a quantum process called Quantum Key Distribution that yields much of the same properties.

In the past decades, the field of cryptography has been fundamentally shaped by the development of Quantum Computing and Quantum Key Distri-

[1] In Quantum Computing, the term *classical* is used as the complement of *quantum*, and refers to the digital computers we know and (maybe) love. This terminology stems from the distinction between classical and quantum physics.

bution. However, the popular conception that all of today's cryptography will be broken and that we have to start from scratch is not accurate. Quantum Computing poses an unique threat to modern cryptography, and Quantum Key Distribution is a promising new tool, but the practical implications of both are much more subtle than how they may be portrayed. In the remainder of this chapter, we will look into the practical implications of these quantum technologies, and we will come to two major conclusions: First, that while the underlying cryptographic primitives will change, apart from some minor engineering issues cryptography as a whole will remain largely the same. Second, that while Quantum Key Distribution is hailed as a revolution for network security, its practical advantages will remain far short of how it is usually conceptualized, and hardware security will assume a pivotal role in the practical security of Quantum Key Distribution systems that is a stark departure from its relative irrelevance in today's applied cryptography.

Building on these conclusions, we will end this chapter with a study of a use case that illustrates a practical design for a secure network employing Quantum Key Distribution. Relying on both established classical and quantum primitives with known security properties we will elaborate how one can construct a large-scale network from those primitives that provides practical security to its users that goes beyond the (surprisingly limited) extents of quantum security proofs.

1.1.1 Computational Assumptions and Information-Theoretic Security

Shor's algorithm allows for the factorization of large numbers in polynomial time on a quantum computer, a problem whose hardness (or the hardness of variants of which) is the foundation for the vast majority of today's asymmetric cryptography.

While Shor's algorithm attacks the foundations of most modern asymmetric cryptography, Grover's algorithm can be applied to hash functionss and symmetric cryptography. Fundamentally, Grover's algorithm is a search algorithm that allows a quantum computer to find one target entry out of an *unstructured* list of N source entries in $\mathcal{O}\left(\sqrt{N}\right)$ time instead of the $\mathcal{O}(N)$ time that a classical computer would require for an exhaustive search. Applied to cryptography, we model the key space of a symmetric cipher as the unstructured list that is input to the algorithm, and set it to search for the key that results in the successful decryption of a given ciphtertext.

An important nuance applying these algorithms to cryptography is that while both provide significant speed-ups over classical computers, the speed-up of Shor's algorithm is exponential and effectively breaks most modern asymmetric cryptography as it erases the asymmetric nature of the underlying mathematical problem. That is, for an asymmetric cryptosystem susceptible to Shor's algorithm, there is no set of parameters that is large enough to be safe.

In contrast to this, while Grover's algorithm radically speeds up the breaking of a symmetric cryptosystem, this speed-up is only quadratic. In practice

this means that it halves the security level of a given symmetric cipher. While this is bad news for applications that parameterize these symmetric primitives to a security level at the lower end of what is considered secure today, the advantage provided by Grover's algorithm can easily be compensated by doubling key size. Longer key sizes require more storage or bandwidth for the additional bits and result in slightly slower operation of the cipher, but this additional cost is easily manageable even without any improvement in today's hardware.

1.2 Quantum Key Distribution

1.3 The Physics of Quantum Computing

1.4 Quantum Networking

1.5 Securing QKD Networks with Inertial HSMs

1.6 Outlook