

# Information Security in a Quantum World

Renato Renner

Institute for Theoretical Physics, ETH Zurich, Switzerland

**Abstract.** It is well known that classical computationally-secure cryptosystems may be susceptible to quantum attacks, i.e., attacks by adversaries able to process quantum information. A prominent example is the RSA public key cryptosystem, whose security is based on the hardness of factoring; it can be broken using a quantum computer running Shor’s efficient factoring algorithm. In this extended abstract, we review an argument which shows that a similar problem can arise even if a cryptosystem provides information-theoretic security. As long as its security analysis is carried out within classical information theory, attacks by quantum adversaries cannot in general be excluded.

## 1 Introduction

It is generally impossible to efficiently represent the state of a quantum system using classical information carriers. In fact, the number of *classical bits* required to approximate  $n$  *quantum bits (qubits)* grows exponentially in  $n$ . It is therefore reasonable to assume (and widely conjectured) that quantum computers cannot in general be efficiently simulated by classical computers. In complexity-theoretic terms, this means that quantum computing is not accurately characterized by the classical model of computation.<sup>1</sup> Therefore, even if a given computational problem was known to be *hard* according to the classical theory, this would not exclude the existence of a quantum algorithm that solves it efficiently. As a consequence, cryptosystems that are based on classical hardness assumptions are not necessarily secure against adversaries equipped with quantum computers. The most prominent example is the RSA public key cryptosystem [RSA78], whose security relies on the hardness of factoring—a problem that a quantum computer can solve efficiently [Sho94].

One may now be tempted to think that this problem is restricted to computational cryptography, where security is based on computational problems whose hardness is anyway only conjectured. This is however not the case. As we shall see, there exist cryptographic systems that

---

<sup>1</sup> This is equivalent to say that the *Strong Church-Turing Thesis* does not hold in a world where quantum information can be processed (see, e.g., [KLM07]).

are provably secure within the framework of classical information theory, whereas their security can be compromised by adversaries able to process quantum information. Remarkably, these cryptosystems may be purely classical, i.e., the legitimate parties only need to process and exchange classical data.

We start the discussion in Section 2 with the observation that information stored in a quantum memory cannot in general be accurately characterized within classical probability and information theory. In Section 3, we consider, as an example, a (classical) key expansion protocol which is secure in the bounded storage model, i.e., under the assumption that an adversary has only limited storage space. We then argue that this scheme, although provably secure within classical information theory, is vulnerable to quantum attacks.

## 2 Limitations of classical information theory

Consider a coin that randomly takes one of two values, labelled by 0 and 1, respectively. The coin may be biased, i.e, there may be a value  $b \in [-\frac{1}{2}, \frac{1}{2}]$  by which the probability of outcome 1 deviates from  $\frac{1}{2}$ . We may model the coin as well as the bias by random variables,  $C$  and  $B$ , respectively. Then, by assumption, we have

$$P_{C|B=b}(1) = \frac{1}{2} + b ,$$

where  $P_{C|B=b}(c)$  denotes the probability that  $C$  equals 1 conditioned on the event  $B = b$  that the bias takes a specific value  $b$ .

Assume now that we know the value of the bias,  $B$ , but are ignorant about the outcome of the coin toss,  $C$ . The knowledge we have about  $C$  is then completely determined by the conditional probability distribution  $P_{C|B=b}$ . In particular, given  $P_{C|B=b}$ , we can compute operational quantities such as the probability by which the outcome  $C$  can be correctly predicted, or the average number of uniform bits that can be extracted from independent copies of  $C$ .

Let us now move to a slightly modified scenario, where the bias  $B$  is not available as a classical value, but instead encoded into the state of a qubit,  $Q$ . More precisely, we assume that the state of  $Q$  is given by a vector of the form

$$|\phi_b\rangle = \cos \frac{\pi b}{2} |e_0\rangle + \sin \frac{\pi b}{2} |e_1\rangle , \tag{1}$$

where  $\{|e_0\rangle, |e_1\rangle\}$  is an orthonormal basis of the state space. Similarly to the previous example, assume that we do not know the outcome of the coin toss  $C$ , but now have access to  $Q$  (instead of  $B$ ). We may then ask whether there is a compact mathematical description of the knowledge we have about  $C$ , analogously to the conditional distribution  $P_{C|B=b}$  of the previous example. Crucially, however, because of the quantum nature of  $Q$  (which now takes the role of  $B$ ), there is no longer a classical event on which we could condition the probability distribution of the (still classical) value  $C$  on.

To be a bit more specific, let us assume that  $B$  is uniformly distributed over the interval  $[-\frac{1}{2}, \frac{1}{2}]$ . Then, using the fact that the classical values of  $C$  can without loss of generality be represented by two orthogonal quantum states, denoted  $|0\rangle_C$  and  $|1\rangle_C$ , respectively, the joint state of  $C$  and  $Q$  is given by<sup>2</sup>

$$\rho_{CQ} = \int_{-\frac{1}{2}}^{\frac{1}{2}} [P_{C|B=b}(0)|0\rangle\langle 0|_C \otimes |\phi_b\rangle\langle \phi_b| + P_{C|B=b}(1)|1\rangle\langle 1|_C \otimes |\phi_b\rangle\langle \phi_b|] db .$$

A simple calculation shows that this state can be rewritten as

$$\rho_{CQ} = \frac{1}{2}|0\rangle\langle 0|_C \otimes \rho_Q^0 + \frac{1}{2}|1\rangle\langle 1|_C \otimes \rho_Q^1$$

where the density operators  $\rho_Q^0$  and  $\rho_Q^1$  are given by

$$\rho_Q^0 = \begin{pmatrix} \frac{1}{2} + \frac{1}{\pi} & -\frac{2}{\pi^2} \\ -\frac{2}{\pi^2} & \frac{1}{2} - \frac{1}{\pi} \end{pmatrix} \quad \text{and} \quad \rho_Q^1 = \begin{pmatrix} \frac{1}{2} + \frac{1}{\pi} & \frac{2}{\pi^2} \\ \frac{2}{\pi^2} & \frac{1}{2} - \frac{1}{\pi} \end{pmatrix} ,$$

respectively. Note that  $\rho_Q^0$  and  $\rho_Q^1$  are not simultaneously diagonalizable. The state of the qubit  $Q$  can therefore not be identified with a classical value.

One may now ask whether it is possible to nevertheless define a classical value  $B'$  which is equally useful as having access to  $Q$ . One possibility could be to set  $B'$  equal to the actual bias,  $B$ . However, the  $B'$  would then be strictly more informative (about  $C$ ) than  $Q$ . To see this, consider for example the case where  $B$  and, hence,  $B'$  are (almost) equal to  $\frac{1}{2}$ . Knowing  $B'$  then immediately allows us to infer the value of  $C$  (which will be 1 with almost certainty). In contrast, since both density operators  $\rho_Q^0$  and

---

<sup>2</sup> Note that  $\rho_{CQ}$  describes the joint state of a classical and a quantum system, assuming that the values of the classical system are represented by the elements of an orthonormal basis. Such states are sometimes termed *classical-quantum states* or *cq states*.

$\rho_Q^1$  have full rank, there is no event (e.g., defined via a measurement of  $Q$ ) conditioned on which the value of  $C$  is fully known.<sup>3</sup> The classical value  $B'$  would therefore be strictly more informative than  $Q$ .

More generally, it can be shown that it is impossible to define a classical random variable  $B'$  which is equivalent to  $Q$ , in the sense that any information about  $C$  that is extractable from  $Q$  can also be obtained from  $B'$ , and vice versa. Roughly, the argument is that, if  $B'$  can be obtained from  $Q$ , there must exist a measurement of  $Q$  whose result is  $B'$ . However, from the measurement outcome  $B'$  it is generally impossible to reconstruct the state that  $Q$  had before the measurement.<sup>4</sup> Hence, the information  $Q$  can no longer be obtained from  $B'$ , which means that  $B'$  is strictly less informative than  $Q$ . We conclude from this that, in a situation where we have access to quantum information  $Q$ , our knowledge about  $C$  cannot be equivalently described by a classical value  $B'$ . In particular, it is not possible to define a conditional probability distribution of  $C$  which fully characterizes all information we have about  $C$ .

The remarkable feature of this example is that  $C$  is classical. This illustrates that, even when we are talking about a classical object such as the outcome of a coin toss, the knowledge we may have about it cannot necessarily be accurately characterized within the classical framework of probability theory. In the next section, we will show that this leads to problems in cryptography, where—even if the data that the legitimate parties are processing and communicating is purely classical—it may be advantageous for an adversary to process her information quantum-mechanically.

### 3 An example: the bounded storage model

The bounded storage model, introduced by Maurer [Mau92] (see also [Lu04,Vad04,DM04]) can be seen as an alternative to the standard computational model used in cryptography. Instead of imposing any limitations on the adversary’s computing power, one assumes that her storage capacity is limited. This facilitates security proofs that are information

---

<sup>3</sup> If the states  $\rho_Q^0$  and  $\rho_Q^1$  have full rank then, for any outcome of a measurement on  $Q$  that has strictly positive probability conditioned on  $C = 0$ , the same outcome also has positive probability when conditioned on  $C = 1$ , and vice versa. This implies that the measurement outcome does not uniquely determine the value of  $C$ .

<sup>4</sup> This is because the *accessible information* between  $B$  and  $Q$  (which is defined by a maximization of the mutual information over all measurements on  $Q$ ) can be strictly smaller than the mutual information between  $B$  and  $Q$ ; see [KRBM07] for an example.

theoretic. One of the most prominent examples is a *key expansion protocol* proposed in [Mau92]. It allows two legitimate parties, connected only over an insecure communication channel, to expand an initially short key to an arbitrary long one. The protocol requires in addition that the legitimate parties have access to a large source of randomness (such as cosmic background radiation). The source is assumed to be public (and hence also accessible to an adversary), but the amount of randomness emitted by the source exceeds the adversary's storage capacity.

The idea of the protocol is, roughly, that the legitimate parties use their initial key to decide on positions from which they read the randomness of the large public source in order to form a *raw key*. Since the adversary cannot know these positions, and is furthermore unable to store all randomness of the source, he has large uncertainty about the raw key. Hence, using *privacy amplification* techniques [BBCM95], the legitimate parties can turn their raw keys into highly secure (final) keys.

In the early security proofs for this protocol, the adversary's memory is (implicitly) assumed to be purely classical [Lu04, Vad04, DM04]. Following the discussion in Section 2, we know however that this assumption strictly does not include situations where the adversary can store (parts of her) information in a quantum memory. Consequently, even if the adversary has only *one single* quantum bit available to store data (which, given the recent progress in experimental quantum information science is certainly realistic) the classical security proofs are no longer directly applicable.

So far, we have argued that security proofs referring to a purely classical model of information do not *imply* security of protocols in a quantum world, where adversaries can make use of quantum information processing. This however, does not necessarily imply that cryptographic protocols *are* insecure in the presence of quantum adversaries. One may therefore wonder whether classical security proofs can generally be extended to proofs that include quantum adversaries.

This is however generally not the case. An explicit example can be obtained using a result of Gavinsky, Kempe, Kerenidis, Raz, and de Wolf [GKK<sup>+</sup>07] on the one-way communication complexity of certain functions. Based on this, it is possible to construct *randomness extractors*, i.e., functions that turn weak randomness into uniform randomness, which have the following property. Whenever the extractor is applied to a uniform classical value  $C$  which is correlated to another classical value  $B$  consisting of  $t$  bits (for some appropriately chosen  $t \in \mathbb{N}$ ), then the extractor output is virtually uniform and uncorrelated to  $B$ . However, when the same extractor is applied to a classical value  $C$  correlated to

a register  $Q$  consisting of  $t$  quantum bits, then the output may still be strongly correlated to  $Q$ . If such an extractor is used for privacy amplification in the key expansion protocol sketched above (so that  $C$  takes the role of the weakly secure raw key), the scheme will be secure against classical adversaries (holding information  $B$ ), while a quantum adversary (holding  $Q$ ) can break it.

## 4 Conclusions

The proof that a cryptographic system is secure against any classical adversary does not in general imply that it is also secure in the presence of quantum adversaries. While this is not very surprising for cryptosystems that use quantum communication (such as Quantum Key Distribution schemes), the example shown in Section 3 illustrates that even purely classical cryptosystems may become insecure in the presence of quantum adversaries.

Nevertheless, in various cases the full (quantum) security of a cryptographic scheme may follow generically from its security against classical adversaries (see [Unr10]). Furthermore, in the particular case of key expansion protocols in the bounded storage model, security can be obtained via the use of *quantum-proof* extractors, as shown in [KR11] (see also [DPVR09]). However, it is an open question whether general cryptographic concepts such as privacy amplification schemes based on extractors—for which there is a classical security proof—can in a generic way be shown secure against quantum adversaries.

## Acknowledgements

This work was supported by the Swiss National Science Foundation (grant 200020-135048 and through the National Centre of Competence in Research *Quantum Science and Technology*) and the European Research Council (grant 258932).

## References

- [BBCM95] C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer. Generalized privacy amplification. *IEEE Transaction on Information Theory*, 41(6):1915–1923, 1995.
- [DM04] S. Dziembowski and U. Maurer. Optimal randomizer efficiency in the bounded-storage model. *Journal of Cryptology*, 17(1):5–26, 2004.

- [DPVR09] A. De, C. Portmann, T. Vidick, and R. Renner. Trevisan’s extractor in the presence of quantum side information. arXiv:0912.5514, 2009.
- [GKK<sup>+</sup>07] D. Gavinsky, J. Kempe, I. Kerenidis, R. Raz, and R. de Wolf. Exponential separations for one-way quantum communication complexity, with applications to cryptography. In *Proceeding of the 39th Symposium on Theory of Computing (STOC)*, 2007.
- [KLM07] P. Kaye, R. Laflamme, and M. Mosca. *An introduction to quantum computing*. Oxford University Press, 2007.
- [KR11] R. König and R. Renner. Sampling of min-entropy relative to quantum knowledge. *IEEE Transactions on Information Theory*, 57:4760–4787, 2011.
- [KRBM07] R. König, R. Renner, A. Bariska, and U. Maurer. Small accessible quantum information does not imply security. *Phys. Rev. Lett.*, 98:140502, 2007.
- [Lu04] C.-J. Lu. Encryption against storage-bounded adversaries from on-line strong extractors. *Journal of Cryptology*, 17(1):27–42, 2004.
- [Mau92] U. Maurer. Conditionally-perfect secrecy and a provably-secure randomized cipher. *Journal of Cryptology*, 5(1):53–66, 1992.
- [RSA78] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.
- [Sho94] P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pages 124–134. IEEE Computer Society Press, 1994.
- [Unr10] D. Unruh. Universally composable quantum multi-party computation. In *Advances in Cryptology—Eurocrypt 2010*, volume 6110, pages 486–505, 2010.
- [Vad04] S. P. Vadhan. Constructing locally computable extractors and cryptosystems in the bounded-storage model. *Journal of Cryptology*, 17(1):43–77, 2004.