Semantic Security and Indistinguishability in the Quantum World

(extended abstract of arXiv:1504.05255 for QCRYPT 2015)

Tommaso Gagliardoni[*], Andreas Hülsing[†], and Christian Schaffner[‡]

Abstract

At CRYPTO 2013, Boneh and Zhandry initiated the study of quantum-secure encryption. They proposed first indistinguishability definitions for the quantum world where the actual indistinguishability only holds for classical messages, and they provide arguments why it might be hard to achieve a stronger notion. In this work, we show that stronger notions are achievable, where the indistinguishability holds for quantum superpositions of messages. We investigate exhaustively the possibilities and subtle differences in defining such a quantum indistinguishability notion. We justify our stronger definition by showing their equivalence to novel quantum semantic-security notions that we introduce. Furthermore, we give a generic transformation to turn a big class of encryption schemes into quantum indistinguishable and hence quantum semantically secure ones.

The field of *post-quantum cryptography* [BBD09] studies classical cryptography resistant against quantum adversaries. Quantum adversaries might be able to use *quantum superpositions* of messages $\sum_x \alpha_x |x\rangle$ instead of classical messages when communicating, even though the cryptographic primitive is still classical. This kind of scenario is considered, e.g., in [BZ13, DFNS13, Unr12, Wat06, Zha12]. Such a setting might for example occur in a situation where one party using a quantum computer encrypts messages for another party that uses a classical computer and an adversary is able to observe the outcome of the quantum computation before measurement. Other examples are an attacker which is able to trick a classical device into showing quantum behavior, or a classical scheme which is used as subprotocol in a larger quantum protocol. Notions covering such settings are often called *quantum-security* notions. In this work we propose new quantum-security notions for encryptions.

For classical encryption schemes, the notion of *semantic security* [GM84, Gol04] has been traditionally used. This notion models in abstract terms the fact that, without the corresponding decryption key, it is impossible not only to correctly decrypt a ciphertext, but even to recover any non-trivial information about the underlying plaintext. The exact definition of semantic security is cumbersome to work with in security proofs as it is simulation-based. Therefore, the simpler notion of *ciphertext indistinguishability* has been introduced. This notion is given in terms of an interactive game where an adversary has to distinguish the encryptions of two messages of his choice. The advantage of this definition is that it is easier to work with than (but equivalent to) semantic security.

[*] CASED,Technische Universität Darmstadt, Germany, `tommaso@gagliardoni.net`

[†] TU Eindhoven, The Netherlands, `andreas.huelsing@googlemail.com`

[‡] University of Amsterdam, CWI Amsterdam, The Netherlands, `c.schaffner@uva.nl`

To the best of our knowledge, no quantum semantic-security notions have been proposed so far. For indistinguishability, Boneh and Zhandry recently introduced indistinguishability notions for quantum-secure encryption under chosen-plaintext attacks [BZ13]. They consider a model (IND-qCPA) where a quantum adversary can query the encrypting device in superposition during a learning phase, but is limited to classical communication during the actual challenge phase. However, this approach has the following shortcoming: If we assume that an adversary can get quantum access in a learning phase, it seems unreasonable to assume that he cannot get such access when the actual message of interest is encrypted. Boneh and Zhandry showed that a seemingly natural notion of quantum indistinguishability (fqIND-qCPA) is unachievable. In order to restore a meaningful definition, they resorted to the compromise of IND-qCPA.

Our contributions. In this paper we achieve two main results. On the one hand, we initiate the study of semantic security in the quantum world, providing new definitions and a thorough discussion about the motivations and difficulties of modeling these notions correctly. This study (in [GHS15, Section 4]) is concluded by a suitable Definition 4.4 of *quantum semantic security under chosen-plaintext attacks (qSEM-qCPA).*

On the other hand, we extend the fundamental work initiated in [BZ13] by defining notions of indistinguishability in the quantum world. We show that the compromise that had to be reached there in order to define an achievable notion instead of a more natural one (i.e., IND-qCPA vs. fqIND-qCPA) can be overcome – although not trivially. We show how various other possible notions of quantum indistinguishability can be defined. All these security notions span a tree of possibilities which we analyze exhaustively (in Section 3) in order to find the most suitable definition of *quantum indistinguishability under chosen-plaintext attacks (qIND-qCPA).*

In Section 5, we prove this notion to be strictly stronger than IND-qCPA, and equivalent to our new notion of semantic security qSEM-qCPA defined above. Thereby, we complete an elegant framework of security notions in the quantum world, see Figure 1 for an overview.

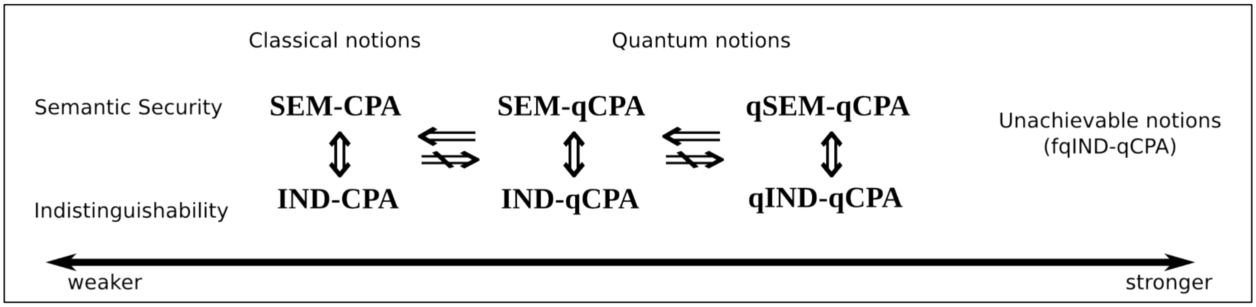

Figure 1: The relations between notions of indistinguishability and semantic security in the quantum world, see [GHS15] for formal definitions and proofs.

In Section 6, we show the impossibility of achieving our new security notion qIND-qCPA for encryption schemes which essentially do not increase the plaintext size, such as stream ciphers and many block ciphers including AES. On the positive side, we prove in Theorem 6.5 the qIND-qCPA security of Construction 6.4 which turns a quantum-secure pseudorandom permutation into a secure encryption scheme. Thereby, we prove that our new notions are achievable. The main technique used in this construction is to introduce message-expansion during the encryption in a careful way.

Interestingly, message-expansion happens in most public-key post-quantum encryption schemes, like for example LWE based schemes [LP11] or the McEliece scheme [McE78].

Related work. The idea of considering scenarios where a quantum adversary can force other parties into quantum behaviour has been considered in [DFNS13] where the authors study superposition attacks for multi-party computation, secret sharing, and zero-knowledge. The quantum security of zero-knowledge and zero-knowledge proofs of knowledge has been investigated in [Wat06] and [Unr12]. In [BZ13] the authors also consider the security of signature schemes where the adversary can have quantum access to a signing oracle. Quantum superposition queries have also been investigated relatively to the random oracle model [BDF+11]. A quantum indistinguishability notion has been suggested (but not further analyzed) by Velema in [Vel13, Def. 5.3].

Relevance and Further Directions We believe that many of the current security notions used in different areas of cryptography are unsatisfying in case quantum computers become reality. In this respect, our work contributes to a better understanding of which properties are important for the long-term security of modern cryptographic primitives. Our work opens various interesting follow-up questions.

There are many other directions to investigate, once the basic framework of 'indistinguishability versus semantic security' presented in this work is completed. A natural direction is to look at quantum CCA security in this framework. This topic was also initiated in [BZ13] relative to the IND-qCPA model; it is intriguing to extend the definition of CCA security to stronger notions obtained by starting from our qIND-qCPA model. With respect to qIND-qCPA, we have left as an open problem a detailed study of other possible notions. We have not yet taken into account models which lead to the study of *quantum fault attacks*. Moreover, we have not considered superpositions of keys or randomness: these lead to a quantum study of *weak-key* and *bad-randomness* models. The authors of this paper are not aware of any results in these directions. With respect to semantic security, it is also possible to weaken qSEM-qCPA by restricting the messages to be quantum, but the advice function to be classical. All the semantic security notions can be also studied in the *uniform model*.

Our secure construction shows how to turn block ciphers into qIND-qCPA secure schemes. An interesting research question is whether there exists a general patch transforming an IND-CPA secure scheme into a qIND-qCPA secure one. It is important to study how our transformation can be applied to general modes of operation. Finally, although much different in scope, it would also be possible to study *fully quantum encryption*, i.e., encryption schemes for protecting quantum information, meant to be run on quantum computers, where all the data and parties involved behave fully quantum, and the encryption and decryption operations are arbitrary unitaries.

References

[BBD09] Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen. *Post-Quantum Cryptography*. Springer, 2009.

[BDF+11] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random Oracles in a Quantum World. In *Asiacrypt 2011*, number 7073 in LNCS, pages 41–69. Springer, 2011.

[BZ13] Dan Boneh and Mark Zhandry. Secure Signatures and Chosen Ciphertext Security in a Post-Quantum World. Cryptology ePrint Archive, Report 2013/088, 2013. An extended abstract appeared in Ran Canetti and Juan A. Garay, editors, *Crypto 2013*, volume 8043 of *LNCS*, pages 361379. Springer, 2013.

[DFNS13] Ivan Damgård, Jakob Funder, Jesper Buus Nielsen, and Louis Salvail. Superposition Attacks on Cryptographic Protocols. In Carles Padró, editor, *ICITS 2013*, volume 8317 of *LNCS*, pages 142–161. Springer, 2013.

[GHS15] Tommaso Gagliardoni, Andreas Hülsing, and Christian Schaffner. Semantic security and indistinguishability in the quantum world. http://arxiv.org/abs/1504.05255, 2015.

[GM84] Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *Journal of computer and system sciences*, 28(2):270–299, 1984.

[Gol04] Oded Goldreich. *Foundations of Cryptography: Volume 2, Basic Applications*. Cambridge University Press, Cambridge, UK, 2004.

[LP11] Richard Lindner and Chris Peikert. Better Key Sizes (and Attacks) for LWE-Based Encryption. In Aggelos Kiayias, editor, *CT-RSA 2011*, volume 6558 of *LNCS*, pages 319–339. Springer, 2011.

[McE78] Robert J. McEliece. A public-key cryptosystem based on algebraic coding theory. *DSN progress report*, 42(44):114–116, 1978.

[Unr12] Dominique Unruh. Quantum proofs of knowledge. In David Pointcheval and Thomas Johansson, editors, *Eurocrypt 2012*, volume 7237 of *LNCS*, pages 135–152. Springer, 2012.

[Vel13] Maria Velema. Classical encryption and authentication under quantum attacks. Master's thesis, Master of Logic, University of Amsterdam, 2013. http://arxiv.org/abs/1307.3753.

[Wat06] John Watrous. Zero-knowledge Against Quantum Attacks. In *STOC '06*, pages 296–305. ACM, 2006.

[Zha12] Mark Zhandry. How to Construct Quantum Random Functions. In *FOCS 2012*, pages 679–687. IEEE, 2012.