Computational Security of Quantum Encryption

(extended abstract of arXiv:1602.01441 for QCRYPT 2016)

Gorjan Alagic[1], Anne Broadbent[2], Bill Fefferman[3], Tommaso Gagliardoni[4], Christian Schaffner[5], and Michael St. Jules[2]

[1] Department of Mathematical Sciences, University of Copenhagen
[2] Department of Mathematics and Statistics, University of Ottawa
[3] QuICS, University of Maryland
[4] TU Darmstadt, Germany
[5] QuSoft, University of Amsterdam and CWI, The Netherlands

1 Introduction

Outline. Quantum-mechanical devices have the potential to transform cryptography. Past research in this area has typically focused either on the information-theoretic advantages of quantum protocols, or on the security of classical schemes against quantum attacks. In this work, we consider a new topic: the encryption of quantum data against computationally-bounded adversaries. In this direction, we establish quantum versions of several fundamental classical results. First, we develop natural definitions for private-key and public-key encryption schemes for quantum data. We then define and motivate notions of semantic security and indistinguishability, and, in analogy with the classical work of Goldwasser and Micali, show that these notions are equivalent. Finally, we construct secure quantum encryption schemes from basic primitives. In particular, we show that quantum-secure one-way functions imply IND-CCA1-secure symmetric-key quantum encryption, and that quantum-secure trapdoor permutations imply semantically-secure public-key quantum encryption.

Motivation. Quantum information processing carries significant consequences for cryptography. Most public-key cryptographic primitives in use today are easily defeated by quantum adversaries [Sho94]. Moreover, quantum mechanics itself predicts physical phenomena that can be exploited in order to achieve new levels of security, e.g., in quantum key distribution (QKD) [BB84].

In fact, the cryptographic possibilities of quantum information go well beyond QKD. Quantum copy-protection [Aar09], quantum money [Wie83,AC12,MS10] and revocable time-release encryption [Unr14] are just some examples where properties unique to quantum data enable new cryptographic constructions. Thanks in part to these tremendous cryptographic opportunities, we envisage an increasing need for an information infrastructure that enables quantum information. Such an infrastructure will enable honest parties to efficiently store, exchange, and compute on quantum data, all in a manner which is secure against quantum adversaries. If this infrastructure is to ever approach the scale and efficiency of the current, classical Internet, it would be utopistic to always demand

information-theoretic security. This motivates the need for a study of quantum security against computationally-bounded adversaries.

The current state-of-the-art is lacking even the most basic cryptographic concepts in this context. In particular, the study of encryption of quantum data (arguably the most fundamental building block) has so far been almost exclusively limited to the quantum one-time pad [AMTdW00] and other aspects of the information-theoretic setting [Des09,DD10] (one notable exception being [BJ15]). This situation leaves many open questions about what can be achieved in the "fully quantum world." Our work aims to lay the foundation for this area of research.

Quantum encryption. In our setting, all parties are modeled by polynomial-time quantum algorithms (QPTs) whose inputs and outputs are described by density operators. The starting point is a notion of quantum encryption scheme.

Definition 1. [BJ15] *A quantum encryption scheme is a triple of QPTs:*
1. KeyGen*: accepts a security parameter* n *and outputs a key* $k \in \{0,1\}^n$*;*
2. Enc*: given a key* k*, maps states* ρ *(plaintext) to* $\mathsf{Enc}_k(\rho)$ *(ciphertext);*
3. Dec*: given a key* k*, maps states* σ *to* $\mathsf{Dec}_k(\sigma)$*;*

such that $\mathsf{Dec}_k \circ \mathsf{Enc}_k = \mathbb{1}$ *for all* k *output by* KeyGen.

A public-key variant (where the encryption and decryption keys differ) is straightforward. These schemes admit an appropriate definition of indistinguishability security, following the classical approach [BJ15]: the quantum adversary outputs a challenge template ρ; given either $\mathsf{Enc}_k(\rho)$ or $\mathsf{Enc}_k(|0\rangle\langle 0|)$ (each with probability $1/2$), the adversary must decide which was the case.

2 Summary of Contributions

In this work, we establish quantum versions of several fundamental classical results about encryption. A summary is as follows.

Quantum semantic security. Semantic security formalizes an intuitive notion: possession of the ciphertext should not help any adversary in computing anything about the plaintext, regardless of their prior knowledge. We give several natural formulations of semantic security for quantum schemes, and show them to be equivalent. The main formulation posits that two settings are computationally indistinguishable:

1. an adversary $\mathcal{A}$ generates a state ρ_{ME} consisting of a message, possibly entangled with some side information; the message is encrypted and returned to $\mathcal{A}$, who then produces some output state;
2. a simulator $\mathcal{S}$ generates ρ_{ME}, discards the message register, and then produces some output state.

We then show the following for both private-key and public-key schemes.

Theorem 2. *A quantum encryption scheme is semantically secure if and only if it has indistinguishable encryptions.*

The theorem holds in two additional settings: (i.) when $\mathcal{A}$ has access to an encryption oracle (CPA), and (ii.) when $\mathcal{A}$ has access to an encryption oracle as well as a decryption oracle (prior to the challenge) (CCA1).

Private-key quantum encryption. Next, we construct a private-key encryption scheme for quantum states, using only a classical primitive: a quantum-secure one-way function (qOWF). The existence of a qOWF implies the existence of a quantum-secure pseudorandom function (qPRF) [Zha12]. In what follows, we choose a bijection between $2n$-bit strings and the n-qubit Pauli group, and denote it by $s \mapsto P_s$.

Scheme 1 *Let $f : \{0,1\}^n \times \{0,1\}^{2n} \to \{0,1\}^{2n}$ be a qPRF. Define:*

1. *(key generation)* $\mathsf{KeyGen}(1^n)$*: output* $k \xleftarrow{\$} \{0,1\}^n$*;*
2. *(encryption)* $\mathsf{Enc}_k(\rho)$*: choose* $r \xleftarrow{\$} \{0,1\}^{2n}$ *and output* $|r\rangle\langle r| \otimes P_{f_k(r)}\rho P_{f_k(r)}$*.*
3. *(decryption)* $\mathsf{Dec}_k(\sigma)$ *: measure first* $2n$ *qubits to get* r'*; apply* $P_{f_k(r')}$ *to rest.*

We show that the above scheme satisfies the strongest form of both semantic security and indistinguishability. This implies the following:

Theorem 3. *If quantum-secure one-way functions exist, then so do* IND-CCA1*-secure private-key quantum encryption schemes.*

Public-key quantum encryption. Finally, we show that one can also construct public-key encryption schemes for quantum states, using only a classical primitive. In this case, the primitive is a *quantum-secure one-way permutation with trapdoors*[6] (qTOWP). This is a qOWF with an additional property: each function f_i in the family is a permutation whose efficient inversion is possible only if one possesses a secret string t (the trapdoor). It's not hard to show that qTOWPs exhibit "hard core bits" (denoted b) and provide a quantum-secure pseudorandom generator (qPRG). A sketch of our scheme is as follows:

Scheme 2 *Let f be a qTOWP with qPRG $G : \{0,1\}^n \to \{0,1\}^{2n}$. Define:*

1. *(key-pair generation)* $\mathsf{KeyGen}(1^n)$*: output* $(i,t) \in \{0,1\}^n \times \{0,1\}^n$*;*
2. *(encryption)* $\mathsf{Enc}_i(\rho)$*: sample* d*; output* $|f_i^{2n}(d)\rangle\langle f_i^{2n}(d)| \otimes P_{G(d)}\rho P_{G(d)}$*;*
3. *(decryption)* $\mathsf{Dec}_t(|s\rangle\langle s| \otimes \sigma)$ *:*
   - *iteratively use* t *to invert* $|s\rangle\langle s|$ *and compute hard core bits;*
   - *concatenate hard core bits to get* $u \in \{0,1\}^{2n}$*; output* $P_u \sigma P_u$*.*

We show that this scheme satisfies IND-CPA security. By Theorem 2, we have the following result.

Theorem 4. *If quantum-secure trapdoor permutations exist, then so do chosen-plaintext semantically secure public-key quantum encryption schemes.*

[6] This notion is also of significant relevance in the security of classical quantum-secure cryptosystems; promising candidates are known [PW08,GPV08].

References

Aar09. Scott Aaronson. Quantum copy-protection and quantum money. In *Computational Complexity, 2009. CCC'09. 24th Annual IEEE Conference on*, pages 229–242. IEEE, 2009.

AC12. Scott Aaronson and Paul Christiano. Quantum money from hidden subspaces. In *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*, pages 41–60. ACM, 2012.

AMTdW00. Andris Ambainis, Michele Mosca, Alain Tapp, and Ronald de Wolf. Private quantum channels. In *Foundations of Computer Science, 2000. Proceedings. 41st Annual Symposium on*, pages 547–553, 2000.

BB84. Charles Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the International Conference on Computers, Systems, and Signal Processing*, pages 175–179, 1984.

BJ15. Anne Broadbent and Stacey Jeffery. Quantum homomorphic encryption for circuits of low T-gate complexity. In *Crypto 2015*, pages 609–629, 2015.

DD10. Simon Pierre Desrosiers and Frédéric Dupuis. Quantum entropic security and approximate quantum encryption. *IEEE Transactions on Information Theory*, 56(7):3455–3464, 2010.

Des09. Simon Pierre Desrosiers. Entropic security in quantum cryptography. *Quantum Information Processing*, 8(4):331–345, August 2009.

GPV08. Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*, STOC '08, pages 197–206, New York, NY, USA, 2008. ACM.

MS10. Michele Mosca and Douglas Stebila. Quantum coins. *Error-Correcting Codes, Finite Geometries and Cryptography*, 523:35–47, 2010.

PW08. Chris Peikert and Brent Waters. Lossy trapdoor functions and their applications. In *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*, STOC '08, pages 187–196, New York, NY, USA, 2008. ACM.

Sho94. Peter W. Shor. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In *FOCS 1994*, pages 124–134. IEEE Computer Society Press, 1994.

Unr14. Dominique Unruh. Revocable quantum timed-release encryption. In *Advances in Cryptology–EUROCRYPT 2014*, pages 129–146. Springer, 2014.

Wie83. Stephen Wiesner. Conjugate coding. *ACM Sigact News*, 15(1):78–88, 1983.

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