A Simple Construction of Quantum Public-Key Encryption from Quantum-Secure One-Way Functions

Khashayar Barooti[1], Giulio Malavolta[2], and Michael Walter[3]

[1]EPFL, Lausanne, Switzerland
[2]Max-Planck Institute in Security and Privacy, Bochum, Germany
[3]Ruhr-Universität Bochum, Bochum, Germany

Abstract

Quantum public-key encryption [Gottesman; Kawachi et al., Eurocrypt'05] generalizes public-key encryption (PKE) by allowing the public keys to be quantum states. Prior work indicated that quantum PKE can be constructed from assumptions that are potentially weaker than those needed to realize its classical counterpart. In this work, we show that quantum PKE can be constructed from any quantum-secure one-way function. In contrast, classical PKE is believed to require more structured assumptions. Our construction is simple, uses only classical ciphertexts, and satisfies the strong notion of *CCA security*.

1 Introduction

Quantum public-key encryption was proposed by Gottesman [11] and Kawachi et al. [14] as a generalization of the standard notion of public-key encryption, allowing public keys to be quantum states. More specifically, this primitive allows Alice to locally generate (many copies of) a state $|\mathsf{pk}\rangle$ and upload it to some certificate authority. Later on, Bob can query the certificate authority to retrieve a copy of $|\mathsf{pk}\rangle$ and use it to send a private message to Alice. Similarly to the classical setting, quantum PKE assumes that the certificate authority provides Bob with the correct information (in this case the state $|\mathsf{pk}\rangle$), but does not otherwise make any assumption on the behavior of the certificate authority, who could try to learn the secret key of Alice in some arbitrary way. However, contrary to the classical case, since quantum states cannot in general be copied, one has to assume that Alice uploads many copies of $|\mathsf{pk}\rangle$, if she wants to establish a secure channel with multiple parties. In spite of this limitation, quantum PKE is still an interesting object to study: (i) Because of the use of quantum information, quantum PKE may be realizable from weaker computational assumptions than standard (classical) PKE, or perhaps even unconditionally. (ii) In contrast to quantum key-distribution (QKD) protocols [2], which require more interaction, quantum PKE preserves the interaction pattern of classical PKE, and thus enables *round-optimal* secure communication. Yet, the current state of affairs of quantum PKE leaves open many questions regarding the minimal assumptions needed to construct this primitive. Existing proposals [14] rely on ad-hoc assumptions that are seemingly insufficient for classical PKE, but do not give a clear complexity-theoretic characterization of this primitive. There are even proposals of unconditionally secure quantum PKE [11], although without security proofs. We note that conjecturing unconditional security for quantum PKE is at the very least plausible – after all, QKD does achieve information-theoretic security (assuming authenticated channels).

1.1 Our results

In this work, we show that quantum-secure one-way functions are sufficient to build quantum public-key encryption schemes.While elementary, our construction satisfies the strong notion of *CCA security*, and the ciphertexts are classical. Our results should be contrasted with the case of classical PKE, where one-way functions are widely believed to be insufficient for realizing this primitive, and in fact black-box separations are known [12]. Thus, our result also implies a black-box separation between classical and quantum PKE.

Theorem 1.1 (Informal)**.** If quantum-secure one-way functions exist, then there exists a (CCA-secure) quantum PKE scheme with classical ciphertexts.

1.2 Open problems

Our results demonstrate that in fact quantum PKE can be realized only assuming the existence of one-way functions. However, in contrast to classical cryptography, in quantum cryptography one-way functions are not considered to be a minimal assumption. The work of Kretschmer [15] shows that there exists an oracle relative to which one-way functions do not exist, but pseudorandom states [13] do. Thus a question left open by our work is whether quantum PKE can be constructed from presumably weaker assumptions than quantum-secure one-way functions.

1.3 Quantum PKE in context

Although the notion of quantum PKE is not an original contribution of our work, we feel compelled to discuss its relation to related primitives in classical and quantum cryptography. While quantum PKE mimics the interaction pattern of traditional (classical) PKE, the presence of quantum information in the public keys introduces some important conceptual differences. As alluded at earlier, an important difference is that public keys can no longer be copied. This means that Alice (the receiver) must upload many copies of the quantum state $|\mathsf{pk}\rangle$ to the certificate authority, and each copy gets "consumed" once Bob uses it to encrypt a message for Alice. One possible way to mitigate this limitation is to let Alice and Bob use their first message to exchange a secret key, and then continue the remainder of the interaction using standard symmetric encryption. In this way, only one state is used up in this interaction.

Another important point of having a quantum state for a public key is that it becomes less obvious how to check whether the certificate authority sent us the "correct" public key. This is not a problem unique to the quantum setting, since also in the classical case the certificate authority must be trusted to supply the public keys correctly. One standard approach to address this problem is to have multiple authorities storing the same keys, so that one can check their honesty by just comparing the public keys that we receive. With quantum information, the same idea can be implemented by using the SWAP test, which allows comparing two unknown quantum states [5]. This problem and its solution based on the SWAP test were already observed by Gottesman [11].

Quantum PKE can also be compared with quantum key distribution (QKD). On the one hand, quantum PKE has a single round of interaction (from Alice to Bob and back), thus satisfying a *stronger* notion of efficiency. On the other hand, quantum PKE requires Alice to keep a long-term secret key that she would use for all subsequent communications, whereas in QKD there is no requirement to keep a state across different executions. More significantly, in quantum PKE the certificate authority is guaranteed to correctly deliver the public key $|\mathsf{pk}\rangle$ from Alice to Bob, whereas in QKD the eavesdropper can behave arbitrarily during all rounds of the protocol. Thus, quantum PKE satisfies a *weaker* security notion, although the difference is slightly more nuanced than what appears superficially – while the certificate authority is required to deliver the correct state to Bob, it can do arbitrary computations locally to try to recover the secret key. In fact, the security definition provides it with many copies of $|\mathsf{pk}\rangle$ that it could potentially use to learn the secret key. A more thorough discussion on this aspect, along with the modelling choices for the attacker, is given in Section 2.2.

Given the above discussion it is natural to ask whether one can generalize the notion of quantum PKE to allow for quantum secret keys. If one allows the public key and the secret key to form a (possibly entangled) quantum state, then quantum PKE can be realized unconditionally via quantum teleportation [3].

2 Preliminaries

In this section, we provide some preliminary background on quantum mechanics and quantum information. The state space of a quantum system can be characterized by a Hilbert space $\mathcal{H}$. For a more in-depth introduction to quantum information, we refer the reader to [18]. The state of a machine can be represented as a *density matrix*, a positive semi-definite operator of trace one, on $\mathcal{H}$. We call a state *pure* if this operator is a rank one projector, i.e., equal to $|\psi\rangle\langle\psi|$, where $|\psi\rangle \in \mathcal{H}$ is a unit vector. This allows us to represent pure states as unit vectors of $\mathcal{H}$ instead of density operators.

When $\mathcal{H} = (\mathbb{C}^2)^{\otimes n}$, the quantum system consists of n *quantum bits* or *qubits*. The standard product basis $|x\rangle = |x_1\rangle \otimes \ldots \otimes |x_n\rangle$ of $\mathcal{H}$ is labeled by bit strings $x \in \{0,1\}^n$ and is known as the *computational basis*. For sake of convenience, we often leave out $\otimes$ and we also write $|0\rangle$ instead of $|0\rangle \otimes \cdots \otimes |0\rangle$. Every pure state can be represented as $|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle$, where the α_x are called amplitudes and satisfy $\sum_x |\alpha_x|^2 = 1$. When measuring the qubits of a quantum system in this state, the probability of the measurement outcome being x is given by $|\alpha_x|^2$. When the amplitudes are all equal, i.e., the state is at a uniform superposition, we drop the normalization $2^{-n/2}$ and simply write $\sum_{x\in\{0,1\}^n} |x\rangle$. Next, we state a well-known fact about the quantum evaluation of classical circuits.

Fact 2.1. Let $f\colon \{0,1\}^n \to \{0,1\}^m$ be a function which is efficiently computable by a classical circuit. Then there exists a unitary U_f on $(\mathbb{C}^2)^{\otimes n+m}$ which is efficiently computable by a quantum circuit (possibly using ancillas) such that, for all $x \in \{0,1\}^n$ and $y \in \{0,1\}^m$,

$$U_f\colon\ |x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle\,.$$

Next, we recall the one-way to hiding lemma [1].

Lemma 2.2 (One-way to hiding)**.** Let $G, H : X \to Y$ be random functions and $S \subset X$ an arbitrary set with the condition that $\forall x \notin S, G(x) = H(x)$, and let z be a random bitstring. Further, let $\mathbf{A}^H(z)$ be a quantum oracle algorithm that queries H with depth at most d. Define $\mathbf{B}^H(z)$ to be an algorithm that picks $i \in [d]$ uniformly, runs $\mathbf{A}^H(z)$ until just before its i^{th} round of queries to H and measures all query input registers in the computational basis and collects them in a set T. Let

$$P_{\text{left}} = \Pr[1 \leftarrow \mathbf{A}^H(z)], \quad P_{\text{right}} = \Pr[1 \leftarrow \mathbf{A}^G(z)], \quad P_{\text{guess}} = \Pr[S \cap T \neq \emptyset | T \leftarrow \mathbf{B}^H(z)].$$

Then we have that

$$|P_{\text{left}} - P_{\text{right}}| \leq 2d\sqrt{P_{\text{guess}}} \quad \text{and} \quad |\sqrt{P_{\text{left}}} - \sqrt{P_{\text{right}}}| \leq 2d\sqrt{P_{\text{guess}}} \tag{1}$$

2.1 Quantum-secure pseudorandom functions

Our construction relies on a *pseudorandom function* (PRF) [10]. This is a keyed function, denoted PRF, that can be evaluated in polynomial time satisfying a certain security property. In this work we require PRF to be *quantum-secure*, which, loosely speaking, says that an adversary with oracle access to PRF cannot distinguish it from a truly random function, even given superposition queries. It is known that quantum-secure PRFs can be constructed from any quantum-secure one-way function [19].

Definition 2.3 (Quantum-secure PRF)**.** We say that a keyed function PRF is a *quantum-secure pseudorandom function (PRF)* if, for any quantum polynomial time (QPT) adversary $\mathbf{A}$, we have

$$\big|\Pr\big[1 \leftarrow \mathbf{A}(1^\lambda)^{\mathsf{PRF}_k}\big] - \Pr\big[1 \leftarrow \mathbf{A}(1^\lambda)^f\big]\big| \leq \mu(\lambda),$$

where $k \overset{\$}{\leftarrow} \{0,1\}^\lambda$, f is a truly random function, and the oracles can be accessed in superposition, that is, they implement the following unitaries

$$|x\rangle|z\rangle \xmapsto{U_{\mathsf{PRF}_k}} |x\rangle|z \oplus \mathsf{PRF}_k(x)\rangle \quad \text{and} \quad |x\rangle|z\rangle \xmapsto{U_f} |x\rangle|z \oplus f(x)\rangle\,,$$

respectively.

2.2 Quantum public-key encryption

We start by formalizing the notion of a quantum public-key encryption (PKE) scheme [14]. For convenience, we consider a PKE with binary message space $\{0,1\}$, however the scheme can be generically upgraded to encrypt messages of arbitrary length, via the standard hybrid encryption paradigm. This transformation is known to preserve CPA security, by a standard hybrid argument. Classically, it is known that bit-encryption is also complete for CCA security [17], however we leave the proof of such a statement in the quantum settings as ground for future work.

Definition 2.4 (Quantum PKE)**.** A *quantum public key encryption (PKE)* scheme is defined as a tuple $\Gamma = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ such that:

- $(|\mathsf{pk}\rangle, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda)$ is a QPT algorithm which outputs a *pure* quantum state $|\mathsf{pk}\rangle$ and a bit string sk;
- $\mathsf{ct} \leftarrow \mathsf{Enc}(|\mathsf{pk}\rangle, \mathsf{pt})$ is a QPT algorithm which, given a bit $\mathsf{pt} \in \{0,1\}$, outputs a quantum state ct (that needs not be pure);
- $\mathsf{pt} \leftarrow \mathsf{Dec}(\mathsf{sk}, \mathsf{ct})$ is a QPT algorithm which outputs a bit $\mathsf{pt} \in \{0,1\}$.

If the ciphertext is classical then we call Γ a *quantum PKE scheme with classical ciphertexts.* In general, we say that Γ has *correctness error* ε (which can be a function of λ) if for all $\mathsf{pt} \in \{0,1\}$ we have

$$\Pr\big[\mathsf{Dec}(\mathsf{sk}, \mathsf{Enc}(|\mathsf{pk}\rangle, \mathsf{pt})) = \mathsf{pt} \ : \ (|\mathsf{pk}\rangle, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda)\big] \geq 1 - \varepsilon.$$

Finally, we say Γ is *correct* if it has negligible correctness error.

Next we define the notion of CCA security [7]. The version that is going to be relevant for us is the definition of CCA security for quantum PKE with classical ciphertext, which we present below. We also explicitly mention here that CCA security is not easy to define when ciphertexts are quantum states, and it is currently an open question to find the correct analogue of CCA security in the quantum settings [4, 9, 6]. However, in this work, we will only consider CCA security for schemes with *classical* ciphertexts, and therefore the decryption oracle is queried only classically.

Definition 2.5 (CCA Security)**.** We say $\Gamma = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is *CCA-secure*, if for any polynomial $n = n(\lambda)$, and any QPT adversary $\mathbf{A} = (\mathbf{A}_0, \mathbf{A}_1)$ we have

$$\Pr\left[b \leftarrow \mathbf{A}_1^{\mathsf{Dec}^*(\mathsf{sk},\cdot)}(\mathsf{ct}, |\mathsf{st}\rangle) : \begin{array}{l} (|\mathsf{pk}\rangle, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda) \\ |\mathsf{st}\rangle \leftarrow \mathbf{A}_0^{\mathsf{Dec}(\mathsf{sk},\cdot)}(|\mathsf{pk}\rangle^{\otimes n}) \\ b \xleftarrow{\$} \{0,1\} \\ \mathsf{ct} \leftarrow \mathsf{Enc}(|\mathsf{pk}\rangle, b) \end{array} \right] \leq 1/2 + \varepsilon(\lambda)$$

where ε is a negligible function, and the oracle Dec^* is defined as Dec, except that it returns $\perp$ on input the challenge ciphertext ct.

A few remarks about the above definitions are in order. First of all, we would like to stress that Definition 2.4 *crucially* imposes that the public key pk must be a pure state. If the public key was allowed to be the classical mixture, there there is a trivial scheme that satisfies this notion. Namely, the public key consists of a pair

$$\mathsf{SK.Enc}(0; r) \text{ and } \mathsf{SK.Enc}(1; r)$$

where r is uniformly sampled and $\mathsf{SK.Enc}$ is a secret-key encryption scheme. Formally, the public key is modelled as a classical mixture over the randomness r. The encryption algorithm would the just select one out of these two ciphertexts, depending on the input message. Note that this scheme is fully classical. This is the approach suggested by [16] and, as the authors also point out, it can hardly be considered a public key encryption scheme, since it does not even protect against a *passive* certificate authority, who can break the scheme by simply looking at the public key. While we do no formalize the notion of security against passive (possibly quantum) adversaries here, we believe that our definition, by forcing the state to be pure, models the intuition behind a semi-honest certificate authority who is trusted to deliver the correct state, but can otherwise do arbitrary computations on the public key.

An alternative definition that also captures this intuition is the notion of *specious adversaries* [8], where the adversary is actually allowed to maul the public keys arbitrarily, conditioned on the fact that the state that it returns must be indistinguishable from the original one. Arguably, this is the "right" formalization of semi-honest adversaries in the quantum settings and in fact it is not satisfied by the trivial construction outlined above. This definition is slightly more general than Definition 2.5, which on the other hand has the advantage to be simpler to state.

3 CCA-secure quantum PKE from one-way functions

In the following section, we describe our quantum PKE scheme and show that it satisfies the strong notion of CCA security. The construction relies on a quantum-secure pseudorandom function

$$\mathsf{PRF}\colon \{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^{3\lambda}$$

which, as mentioned earlier in Section 2.1, can be constructed from any quantum-secure one-way function. Then our quantum PKE scheme $\Gamma = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is defined as follows:

- The key generation algorithm $\mathsf{Gen}(1^\lambda)$ samples two keys $k_0 \overset{\$}{\leftarrow} \{0,1\}^\lambda$ and $k_1 \overset{\$}{\leftarrow} \{0,1\}^\lambda$, then it prepares the states
$$|\mathsf{pk}_0\rangle = \sum_{x \in \{0,1\}^\lambda} |x, \mathsf{PRF}_{k_0}(x)\rangle \quad \text{and} \quad |\mathsf{pk}_1\rangle = \sum_{x \in \{0,1\}^\lambda} |x, \mathsf{PRF}_{k_1}(x)\rangle\,.$$
Note that both states are efficiently computable since the PRF can be efficiently evaluated in superposition in view of Fact 2.1. The quantum public key is then given by the pure state $|\mathsf{pk}\rangle = |\mathsf{pk}_0\rangle \otimes |\mathsf{pk}_1\rangle$, whereas the classical secret key consists of the pair $\mathsf{sk} = (k_0, k_1)$.
- Given a message $\mathsf{pt} \in \{0,1\}$, the encryption algorithm $\mathsf{Enc}(|\mathsf{pk}\rangle, \mathsf{pt})$ simply measures $|\mathsf{pk}_{\mathsf{pt}}\rangle$ in the computational basis, and outputs the measurement outcome as the *classical* ciphertext $\mathsf{ct} = (x, y)$.
- Given the ciphertext $\mathsf{ct} = (x, y)$, the decryption algorithm $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct})$ first checks whether $\mathsf{PRF}_{k_0}(x) = y$ and returns 0 if this is the case. Next, it checks whether $\mathsf{PRF}_{k_1}(x) = y$ and returns 1 in this case. Finally, if neither is the case, the decryption algorithm returns $\perp$.

Next, we establish correctness of this scheme.

Theorem 3.1. If PRF is a quantum-secure one-way function, then the quantum PKE scheme Γ is correct.

Proof. Observe that the scheme is perfectly correct if the ranges of PRF_{k_0} and PRF_{k_1} are disjoint. By a standard argument, we can instead analyze the case of two truly random functions f_0 and f_1, and the same will hold for PRF_{k_0} and PRF_{k_1}, except on a negligible fraction of the inputs. Fix the range of f_0, which is of size at most 2^λ. Then the probability that any given element of f_1 falls into the same set is at most $2^{-2\lambda}$, and the desired statement follows by a union bound. □

Finally, we show that the scheme is CCA-secure.

Theorem 3.2. If PRF is a quantum-secure one-way function, then the quantum PKE scheme Γ is CCA-secure.

Proof. It suffices to show that the CCA experiment with the bit b fixed to 0 is indistinguishable from the same experiment but with b fixed to 1. To this end we consider a series of hybrids, starting with the former and ending with the latter:

- **Hybrid 0:** This is the original CCA experiment except that the bit b fixed to 0.

- **Hybrid 1:** In this (inefficient) hybrid, we modify hybrid 0 to instead compute $|\mathsf{pk}_0\rangle$ as
$$|\mathsf{pk}_0\rangle = \sum_{x\in\{0,1\}^\lambda} |x, f(x)\rangle\,,$$
where f is a truly uniformly random function.

The indistinguishability between these two hybrids follows by a standard reduction against the quantum security of PRF: To simulate the desired n copies of $|\mathsf{pk}_0\rangle$, and to answer decryption queries (except the one that contains the challenge ciphertext), the reduction simply queries the oracle provided by the PRF security experiment (possibly in superposition). Note that whenever the oracle implements PRF, then the view of the distinguisher is identical to hybrid 0, whereas if the oracle implements a truly random function, then the view of the distinguisher is identical to hybrid 1.

- **Hybrid 2:** In this (inefficient) hybrid, we modify hybrid 1 such that the challenge ciphertext is sampled as
$$x \xleftarrow{\$} \{0,1\}^\lambda \quad \text{and} \quad y \xleftarrow{\$} \{0,1\}^{3\lambda}.$$

The indistinguishability of hybrids 1 and 2 follows from the one-way to hiding lemma (Lemma 2.2). Let H be such that $H(x) = y$ and for all $x' \neq x$ we set $H(x') = f(x')$, and let $S = \{x\}$. Let $\mathbf{A}$ be the adversary playing the security experiment. We claim that $\mathbf{A}^f$ is the adversary playing in hybrid 1 whereas $\mathbf{A}^H$ corresponds to the adversary playing hybrid 2: Observe that the public keys can be simulated with oracle access to f (H, respectively) by simply querying on a uniform superposition of the input domain, whereas the decryption queries can be simulated by query basis states. Importantly, for all queries after the challenge phase, the adversary is not allowed to query x to Dec^*. Hence the set T, collected by $\mathbf{B}$ is a set of at most n uniform elements from the domain of f, along with Q basis states, where Q denotes the number of queries made by the adversary to the decryption oracle *before* the challenge ciphertext is issued. By a union bound
$$P_{\text{guess}} = \Pr[T \cap \{x\} \neq \emptyset] \leq \frac{(n+Q)}{2^\lambda} = \mathsf{negl}(\lambda)$$
since x is uniformly sampled. Applying Lemma 2.2, we deduce that $|P_{\text{left}} - P_{\text{right}}|$ is also negligible, i.e., which bounds the distance between the two hybrids.

- **Hybrid 3:** In this (efficient) hybrid, we modify hybrid 2 to compute $|\mathsf{pk}_0\rangle$ by using the pseudorandom function PRF_{k_0} instead of the truly random function f. That is, we revert the change done in hybrid 1.

Indistinguishability follows from the same argument as above.

- **Hybrid 4:** In this (inefficient) hybrid, we modify hybrid 3 to compute $|\mathsf{pk}_1\rangle$ as
$$|\mathsf{pk}_1\rangle = \sum_{x\in\{0,1\}^\lambda} |x, f(x)\rangle$$
where f is a truly uniformly random function.

Indistinguishability follows from the same argument as above.

- **Hybrid 5:** In this (inefficient) hybrid, we modify hybrid 4 by fixing the bit b to 1 and computing the challenge ciphertext honestly, i.e., as
$$x \xleftarrow{\$} \{0,1\}^\lambda \quad \text{and} \quad y = f(x).$$

Indistinguishability follows from the same argument as above.

- **Hybrid 6:** In this (efficient) hybrid, we modify hybrid 5 to compute $|\mathsf{pk}_1\rangle$ by using the pseudorandom function PRF_{k_1} instead of the truly random function f. That is, we revert the change done in hybrid 4.

Indistinguishability follows from the same argument as above. The proof is concluded by observing that the last hybrid is identical to the CCA experiment with the bit b fixed to 1. □

References

[1] Ambainis, A., Hamburg, M., Unruh, D.: Quantum security proofs using semi-classical oracles. In: Boldyreva, A., Micciancio, D. (eds.) Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II. Lecture Notes in Computer Science, vol. 11693, pp. 269–295. Springer (2019). https://doi.org/10.1007/978-3-030-26951-7_10, https://doi.org/10.1007/978-3-030-26951-7_10

[2] Bennett, C.H., Brassard, G.: Quantum public key distribution reinvented. SIGACT News **18**(4), 51–53 (1987). https://doi.org/10.1145/36068.36070, https://doi.org/10.1145/36068.36070

[3] Bennett, C.H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., Wootters, W.K.: Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. Physical review letters **70**(13), 1895 (1993)

[4] Boneh, D., Zhandry, M.: Secure signatures and chosen ciphertext security in a quantum computing world. In: Annual cryptology conference. pp. 361–379. Springer (2013)

[5] Buhrman, H., Cleve, R., Watrous, J., De Wolf, R.: Quantum fingerprinting. Physical Review Letters **87**(16), 167902 (2001)

[6] Carstens, T.V., Ebrahimi, E., Tabia, G.N., Unruh, D.: Relationships between quantum ind-cpa notions. In: Theory of Cryptography Conference. pp. 240–272. Springer (2021)

[7] Dolev, D., Dwork, C., Naor, M.: Non-malleable cryptography. In: Proceedings of the twenty-third annual ACM symposium on Theory of computing. pp. 542–552 (1991)

[8] Dupuis, F., Nielsen, J.B., Salvail, L.: Secure two-party quantum evaluation of unitaries against specious adversaries. In: Rabin, T. (ed.) Advances in Cryptology - CRYPTO 2010, 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings. Lecture Notes in Computer Science, vol. 6223, pp. 685–706. Springer (2010). https://doi.org/10.1007/978-3-642-14623-7_37, https://doi.org/10.1007/978-3-642-14623-7_37

[9] Gagliardoni, T., Hülsing, A., Schaffner, C.: Semantic security and indistinguishability in the quantum world. In: Annual international cryptology conference. pp. 60–89. Springer (2016)

[10] Goldreich, O., Goldwasser, S., Micali, S.: How to construct random functions. J. ACM **33**(4), 792–807 (1986). https://doi.org/10.1145/6490.6503, https://doi.org/10.1145/6490.6503

[11] Gottesmann, D.: Quantum public-key cryptography with information-theoretic security. https://www2.perimeterinstitute.ca/personal/dgottesman/Public-key.ppt

[12] Impagliazzo, R., Rudich, S.: Limits on the provable consequences of one-way permutations. In: Johnson, D.S. (ed.) Proceedings of the 21st Annual ACM Symposium on Theory of Computing, May 14-17, 1989, Seattle, Washington, USA. pp. 44–61. ACM (1989). https://doi.org/10.1145/73007.73012, https://doi.org/10.1145/73007.73012

[13] Ji, Z., Liu, Y., Song, F.: Pseudorandom quantum states. In: Shacham, H., Boldyreva, A. (eds.) Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part III. Lecture Notes in Computer Science, vol. 10993, pp. 126–152. Springer (2018). https://doi.org/10.1007/978-3-319-96878-0_5, https://doi.org/10.1007/978-3-319-96878-0_5

[14] Kawachi, A., Koshiba, T., Nishimura, H., Yamakami, T.: Computational indistinguishability between quantum states and its cryptographic application. In: Cramer, R. (ed.) Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications

of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings. Lecture Notes in Computer Science, vol. 3494, pp. 268–284. Springer (2005). https://doi.org/10.1007/11426639_16, https://doi.org/10.1007/11426639_16

[15] Kretschmer, W.: Quantum pseudorandomness and classical complexity. In: Hsieh, M. (ed.) 16th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2021, July 5-8, 2021, Virtual Conference. LIPIcs, vol. 197, pp. 2:1–2:20. Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2021). https://doi.org/10.4230/LIPIcs.TQC.2021.2, https://doi.org/10.4230/LIPIcs.TQC.2021.2

[16] Morimae, T., Yamakawa, T.: One-wayness in quantum cryptography. Cryptology ePrint Archive, Paper 2022/1336 (2022), https://eprint.iacr.org/2022/1336, https://eprint.iacr.org/2022/1336

[17] Myers, S.A., Shelat, A.: Bit encryption is complete. In: 50th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2009, October 25-27, 2009, Atlanta, Georgia, USA. pp. 607–616. IEEE Computer Society (2009). https://doi.org/10.1109/FOCS.2009.65, https://doi.org/10.1109/FOCS.2009.65

[18] Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information (10th Anniversary edition). Cambridge University Press (2016), https://www.cambridge.org/de/academic/subjects/physics/quantum-physics-quantum-information-and-quantum-computation/quantum-computation-and-quantum-information-10th-anniversary-edition?format=HB

[19] Zhandry, M.: How to construct quantum random functions. J. ACM **68**(5), 33:1–33:43 (2021). https://doi.org/10.1145/3450745, https://doi.org/10.1145/3450745