# A survey on quantum-secure cryptographic systems

Tomoka Kan

May 24, 2018

## 1 Abstract

Post-quantum cryptography refers to the search for classical cryptosystems which remain secure in the presence of a quantum adversary. Most post-quantum cryptographic systems only consider adversaries which have access to a quantum machine but interact classically with honest parties and oracles. However, it is important to consider security against adversaries which may make quantum queries to honest parties and oracles, since these types of cryptographic attacks may become a reality when quantum machines are widely available in the future. This paper aims to survey recent work on constructing classical cryptographic primitives which are secure in the presence of these stronger quantum adversaries.

## 2 Introduction

Although quantum computers are still not a reality, Shor [Shor97] has shown that once fully realized, they will be able to break most public key cryptosystems, namely those based on classically hard problems such as the difficulty of factoring large numbers and the discrete log problem. This threat has generated interest in post-quantum cryptography, the search for classical cryptosystems which remain secure in the presence of a quantum adversaries.

Most of these post-quantum cryptographic systems only consider adversaries which can perform quantum computations between queries but can only make classical queries to honest parties or oracles. However in the future, it is highly likely that these cyrptographic systems will be implemented on quantum machines. In this case, there is no reason to assume that adversaries will not be able to make quantum queries. Therefore, in keeping with the conservative approach to cryptosystem design, it is important to consider this stronger notion of security where adversaries are able to make quantum queries. Thus in this paper, when we mention quantum security, we will be referring to this stronger notion of security described here.

Allowing an adversary to make quantum queries means that it can query quantum superpositions of inputs and receive a superpostion of the corresponding outputs in return. This ability means that many classical proofs and techniques fail to hold under this new notion of security. For example, many classical proofs in the random oracle model which rely on the fact that any adversary will only get see a polynomial number of points, fail to hold because quantum adversaries can query exponentially many points in superposition. Therefore, recent work in this area has been aiming to either tweak these proofs or construct new proofs, in order to construct classical cryptographic systems which are quantum-secure.

This paper is intended to be a brief introduction into classical cryptographic primitives which are quantum-secure, which have been constructed so far. We start with a basic introduction to quantum concepts in section 3. Section 4 describes separation results, which confirm the expectation that quantum security is a stronger notion than classical security. Section 5 describes the quantum-secure cryptographic primitives themselves and the techniques used to construct them. Finally, section 6 concludes with open questions in this area.

# 3 Quantum preliminaries

We give a short introduction to the quantum concepts that are used in the constructions described in the main text of this paper. More detailed discussions on quantum computation can be found in [Mermin07].

## 3.1 States and superposition

In classical computation, the bit (also called the Cbit) is the fundamental unit of information. The corresponding fundamental unit in quantum computation is called the Qbit, and is represented mathematically by a vector of unit length in a two-dimensional complex vector space. Vectors representing quantum states are written using Dirac notation: if the value represented by the quantum state of a Qbit is $\psi$, then the state of that Qbit is denoted as $|\psi\rangle$. The two states $|0\rangle$ and $|1\rangle$ form the two orthonormal basis vectors for the underlying two-dimensional vector space. Therefore, the state of any single Qbit is of the form $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $|\alpha|^2+|\beta|^2= 1$. If $\alpha \neq \beta \neq 0$, this state is referred to as a superposition (linear combination) of the states $|0\rangle$ and $|1\rangle$. $|\alpha\rangle$ and $|\beta\rangle$ are referred to as amplitudes.

The quantum state of two or more Qbits is described by a tensor product. For example, the four basis states for two Qbits are $|0\rangle \otimes |0\rangle$, $|0\rangle \otimes |1\rangle$, $|1\rangle \otimes |0\rangle$ and $|1\rangle \otimes |1\rangle$, which are usually abbreviated as $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$ respectively. Extending this to $n$ Qbits, we can see that the $2^n$ orthonormal basis states for $n$ Qbits are $|00\cdots0\rangle$, $|00\cdots1\rangle$, $\dots$, $|11\cdots1\rangle$. Note that these basis states are exactly the $2^n$ possible Cbits of length $n$. It follows that a general $n$ Qbit state is of the form

$$\alpha_0|00\cdots0\rangle + \alpha_1|00\cdots1\rangle + \cdots + \alpha_{2^n-1}|11\cdots1\rangle,$$

where $\sum_{i=0}^{2^n-1}|\alpha_i|^2= 1$. This sum is a superposition of the $n$-Qbit basis vectors.

## 3.2 Measurement

The process of measuring (or observing) a Qbit $|\psi\rangle$ always outputs a classical bit $|x\rangle$. If $|\psi\rangle = \sum_{i=1}^{n} \alpha_i|x_i\rangle$, where the $|x_i\rangle$ are basis states, then the measurement process outputs $|x_i\rangle$ with probability $|\alpha_i|^2$. Thus the measurement process induces a probability distribution over classical states, where the probabilities are given by the amplitudes squared. In addition to outputting classical bits, the measurement process also collapses the Qbit into the output it produces. Therefore measuring a quantum state collapses it into a classical one, and any further measurements will be deterministic.

Although we have described the measurement process with respect to the standard basis above, measurements can be made with respect to any arbitrary basis. In this case, the probabilities of the outcomes are calculated by first applying a change of basis, and then applying a standard basis measurement.

# 4 Separation results

We first present constructions which are secure in the classical case but not in the quantum case. These separation results confirm the expectation that allowing an adversary to make quantum queries gives it additional power:

- Zhandry [Zha12b] proves that classical pseudorandom functions may not be as secure as quantum pseudorandom functions by proving the existence of classically secure pseudorandom functions which are not quantum-secure.

- Boneh, Dagdelen, Fischlin, Lehmann, Schaffner, and Zhandry [BDF11] separate classical and quantum-accessible random oracle models. They do this by presenting a two-party protocol which is secure in the classical random oracle model but not in the quantum-accessible random oracle model.

- Boneh and Zhandry [BZ13b] show that quantum chosen message queries give an adversary more power than classical chosen message queries by presenting a signature scheme that is secure under classical queries but insecure once an adversary can make quantum queries.
- Boneh and Zhandry [BZ13] prove that a pair-wise independent hash family is insufficient for constructing a quantum-secure one-time Message Authentication Code (MAC), although this is sufficient in the classical case. This proves that quantum security is stronger than classical security for MACs. They prove that a four-wise independent family is sufficient in the quantum case, however.

# 5 Quantum-secure constructions

The separation results in the previous section show that many classical systems are not quantum-secure. However, this does not mean that there do not exist classical systems which are quantum-secure. The following six subsections provide an overview of the types of quantum-secure classical cryptographic systems which have been constructed so far, and the techniques used to construct them.

## 5.1 Quantum random oracles

In the classical random oracle model, adversaries are given oracle access to a random hash function $O : \{0,1\}^* \to \{0,1\}^*$, and learn a value $O(x)$ by querying the value $x$. This random oracle is replaced with a hash function $H$, whenever the scheme is instantiated. A quantum adversary may evaluate this function $H$ on a superposition of inputs. Thus to model this ability, in the quantum random oracle model, adversaries are also allowed to query superpositions of states, $|\varphi\rangle = \sum \alpha_x |x\rangle$, and receive the corresponding superposition of outputs, $\sum \alpha_x |O(x)\rangle$, in return.

One of the many challenges of proving security in the quantum random oracle model is efficiently simulating the quantum random oracle. In the classical case, random oracles are simulated using a 'lazy' approach, only generating randomness when required. However, this approach does not work in the quantum case, since the adversary is able to query the oracle on an exponential superposition of inputs. Therefore, it seems as though the quantum adversary making even one query would require having exponential randomness. Thus, simulating a quantum random oracle would require defining the entire function before making any queries. Additionally, many classical random oracle techniques, such as Bellare's and Rogaway's [BR93] proof of the security of the Full Domain Hash signature scheme, fail to hold under if the adversary has quantum access to the oracle.

The first quantum random oracle model was constructed by Boneh, Dagdelen, Fischlin, Lehmann, Schaffner, and Zhandry [BDF11] in 2011. They did this by specifying conditions under which a classical random oracle proof implied security for a quantum random oracle. Specifically, they proved that that security was implied when the classical proof was a history-free reduction (which at a high level means that the reduction answers oracle queries independent of previous queries).

Zhandry [Zha12a] improved upon these results, demonstrating how to simulate a quantum random oracle without any additional assumptions at all. His approach involved finding new techniques to argue that quantum algorithms cannot distinguish between two distributions of oracles. He applied this argument to show that a new type of distribution of oracles, called semi-constant oracles, could not be distinguished from random oracles.

## 5.2 Quantum pseudorandom functions

Quantum pseudorandom functions (QPRFs) are defined in a similar way to quantum random oracles: For any QPRF $P$, adversaries may query superpositions of states, $|\varphi\rangle = \sum \alpha_x |x\rangle$, and receive the corresponding superposition of outputs, $\sum \alpha_x |P(x)\rangle$ in return.

In the classical world, pseudorandom functions (PRFs) are generally built from pseudorandom generators (PRGs). One such construction is from length-doubling PRGs, which is known as the GGM construction [GGM86]. These PRGs are in turn built from one-way functions, as shown by Håstad et al [HILL99]. Håstad et al's security proof does not make any assumptions about the computational model of the adversary, meaning that it immediately carries over to the quantum case, as long as the underlying one-way function is quantum-secure. However, the classical proof of security of the GGM construction does not hold in the presence of a quantum adversary.

In order to understand why this the GGM construction does not hold in the quantum case, we give a brief high level overview of the classical security proof of the construction. The GGM construction involves considering a binary tree with depth $n$. Each leaf of this tree corresponds to an input / output pair of the PRF. To evaluate the PRF, we start at the root and travel down a path to the leaf corresponding to the input. The proof of the security of this construction relies on two hybrid arguments. The first hybrid argument is across the levels of the tree, and therefore has only polynomially many hybrids, since the depth of the tree is polynomial. The second hybrid argument is across the nodes in a particular level. Since a classical adversary only queries the PRF polynomially many times, the paths used to evaluate the PRF only visit polynomially many nodes on each level. Thus there are also only polynomially many hybrids for the second argument. These hybrid arguments allow us to conclude that any adversary which breaks the security of the PRF with probability $\varepsilon$ can be reduced to an adversary that breaks the security of the underlying PRG with probability only polynomially smaller than $\varepsilon$.

The problem with this argument in the quantum case is that an adversary may query the PRF on a superposition of exponentially many inputs. Then, every level of the tree would have exponentially many nodes, so the second hybrid argument would require exponentially many hybrids. This would reduce the probability of the adversary breaking the security of the underlying PRG to only an exponentially small probability. A similar problem occurs for other classical constructions of PRFs from PRGs.

Zhandry [Zha12b] gives the first construction of quantum-secure PRFs. Although we have seen that classical constructions of PRFs do not work in the quantum world, Zhandry found that many classically secure PRFs can also be shown to be quantum-secure using new techniques. In particular, Zhandry showed that the GGM construction of PRFs described above is in fact quantum-secure, as is a construction based on pseudorandom synthesizers, and a construction based on the Learning With Errors problem. The general idea of Zhandry's new technique was to first define a seemingly stronger definition of security for the underlying cryptographic primitive. He then showed that any adversary breaking the security of the PRF could be reduced to an adversary breaking the security of the underlying cryptographic primitive. He then showed the equivalence of this stronger definition with the standard definition of security in the quantum world.

## 5.3 Quantum message authentication codes

Building on from the quantum-secure PRFs discussed in the previous subsection, quantum-secure message authentication codes (MACs) have also been constructed.

Quantum MACs are defined to be secure if they are existentially unforgeable against quantum chosen message attacks. Such quantum chosen message attacks refer to attacks where the adversary is able to query superpositions of messages, $\sum_m \psi_m |m\rangle$, and receive a superposition of MAC tags on those messages, $\sum_m \psi_m |m, S(k,m)\rangle$, where $S(k,m)$ is the MAC tag on the message $m$ with secret key $k$. If the adversary has made $q$ queries by the end of its interaction with the MAC signing oracle, we define the MAC to be quantum-secure if the adversary cannot produce $q+1$ valid message-tag pairs. This definition is due to the fact that the adversary can produce $q$ message-tag pairs just by trivially sampling the $q$ superpositions it received from the MAC signing oracle but cannot produce a $q + 1$th pair without forgery.

In the classical setting, MACs are built out of PRFs. Since quantum PRFs exist, as described in the section above, an obvious question is whether secure quantum PRFs give rise to secure quantum MACs. Since a quantum-secure PRF is indistinguishable from a random function to an adversary by definition, proving that the quantum MAC is secure is equivalent to proving that if an adversary has made $q$ quantum queries to a random oracle $H : \mathcal{X} \rightarrow \mathcal{Y}$, the probability that it can produce $q + 1$ input-output pairs of $H$ must be negligible. This is trivial in the classical case, since in this case the adversary only learns the value of $H$ at $q$ distinct points, which gives it no information about the value of $H$ at any other points. However, this argument fails in the quantum case, since the adversary could query a superposition of all possible inputs, which would give it information about the all of $H$.

Using a new proof technique, Boneh and Zhandry [BZ13] show that it is in fact the case that secure quantum PRFs give rise to secure quantum MACs, thus constructing the first quantum-secure MACs. Their argument provides tight bounds to the question presented in the paragraph above by: first lower bounding the probability that an adversary will produce $q + 1$ output pairs if $q < |\mathcal{X}|$ by using a technique called the rank method, which bounds the success probability of algorithms that succeed with only a small probability. They then show that this lower bound is tight by extending a related algorithm presented by van Dam [vD98] for oracles outputting one bit, to multi-bit oracles. Additionally, Boneh and Zhandry [BZ13] also show the quantum security of a variant of Carter-Wegman MACs.

## 5.4 Quantum signatures

Quantum-secure signatures are defined in a similar manner to quantum-secure MACs: a signature is quantum-secure if it is existentially unforgeable under a quantum chosen message attack, where a quantum chosen message attack is defined as in 5.3.

Boneh and Zhandry [BZ13b] give the first construction of such quantum-secure signatures, by building compilers which convert a classically secure signature scheme into a quantum-secure one. Their constructions are as follows:

- Using a chameleon hash [KR00], they show how to transform any signature scheme that is existentially unforgeable in the classical world into a signature scheme which is existentially unforgeable in the quantum world. They then apply this transformation to several existing signature schemes, including signature schemes which rely on the quantum hardness of lattice problems.
- They also prove that signature schemes which are universally unforgeable in the classical world can be made existentially unforgeable under a quantum chosen message attack in the random oracle model. They apply this conversion to a randomized variant of GPV signatures [GPV08].
- Finally, they also show how to build quantum-secure signatures from collision resistant hash functions. They do this through proving that classical constructions such as Lamport one-time signatures and Merkle signatures are existentially unforgeable under a quantum chosen message attack.

## 5.5 Quantum encryption

Boneh and Zhandry [BZ13b] also build the first public-key and symmetric-key encryption schemes which are secure against quantum chosen ciphertext attacks. They define the chosen ciphertext security game in the quantum case as follows:

In the classical chosen ciphertext security game, the adversary is given classical access to both the encryption and decryption oracles. In the quantum case, the quantum adversary is given quantum access to the decryption oracle. Thus it is able to query a superposition of ciphertexts and get back a superposition of the corresponding decryptions:

$$\sum_m \varphi_c |c\rangle \to \sum_c \varphi_c |c, D(sk, c)\rangle,$$

where $D(sk, c)$ is the decryption of $c$ using secret key $sk$. It would also be natural to wonder whether we can give the adversary quantum access to encryption oracle. However, Boneh and Zhandry [BZ13b] showed that this stronger definition would be insatisfiable.

Boneh's and Zhandry's encryption schemes work as follows:

- They construct a quantum-secure symmetric-key system from a quantum-secure PRF using the encrypt-then-MAC paradigm. Although the classical proof that the encrypt-then-MAC paradigm is secure does not extend to the quantum case, they give a different proof of security for their specific construction.
- They show that they can use any identity-based encryption scheme that is selectively secure under a quantum chosen identity attack to construct a quantum-secure public-key system. They also show that such an identity-based encryption scheme can be built from lattice assumptions.

## 5.6 Quantum pseudorandom permutations

Finally, also building off of the quantum-secure PRFs discussed in section 5.2, quantum-secure pseudorandom permutations (PRPs) have also been constructed.

Quantum-secure PRPs are defined in a similar way to quantum-secure PRFs: they must be secure against an adversary who is able to make quantum superposition queries to the permutation.

In classical cryptography, PRPs can be constructed from one-way functions. This construction is as follows:

1. First, one-way functions can be used to build PRGs, as shown by Håstad et al [HILL99].
2. Next, PRGs can be used to build PRFs, using the GGM construction [GGM98].
3. Finally, Luby and Rackoff [LR88] showed that a PRP can be obtained by plugging PRFs into a 4-round Feistel Network.

In section 5.2, we discussed how 1) immediately carries over to the quantum case for quantum immune one-way functions, and how 2) holds because there exists a different proof which shows the security of the GGM PRF against quantum adversaries.

The classical proof of 3) involves first replacing the PRF in the Feistel network with a random function. In the quantum case, we will need the PRF to be quantum-secure, but translating this step to the quantum case is otherwise relatively simple. However, this is not true of the next step. The next step involves showing that once we have made this replacement, the Feistel network becomes indistinguishable from a random function. Since the classical proof of this step relies on the fact that the adversary will only get to see a polynomial number of points, it breaks down in the quantum case where adversaries can query exponentially many points.

Zhandry [Zha17] uses a completely different technique to obtain quantum-secure PRPs from quantum-secure PRFs, thus completing the construction of quantum PRPs from quantum immune one-way functions. The main crux of Zhandry's technique involves using an object called a Function-to-Permutation Converter (FPC). At a high level, this is an algorithm $P$ which makes oracle queries to a function $O$, and whose inputs and outputs belong to a domain $\mathcal{X}$. For any function $O$, $P^O$ is a permutation of $\mathcal{X}$, and if $O$ is a random function, $P^O$ is indistinguishable from a random permutation. Clearly, full-domain classical FPCs, where

$P^O$ remains indistinguishable from random even if the adversary can query $P^O$ on its entire domain, are also quantum FPCs secure against up to $|X|$ queries via a simple reduction. Thus given a quantum FPC adversary, Zhandry proposes to construct a classical FPC adversary that queries the entire domain so that it knows the entire function, and then answers the quantum FPC adversary's queries using this knowledge. Plugging in a quantum PRF as $O$ into this quantum FPC results in a quantum-secure PRP. Such full-domain classical FPCs can be found in the context of format preserving encryption [BRRS09].

# 6 Conclusions

The study of classical cryptosystems which are secure against adversaries which can make quantum queries is still an emerging research area, with most major results coming from within the last 10 years. Thus although we have presented numerous quantum-secure cryptographic primitives in the previous section, there are still many major open questions. One of the most general open questions is how to design primitives that remain secure in the presence of such adversaries, for any cryptographic primitive modeled as an interactive game. For example, is it possible to design quantum-secure threshold signatures and group signatures? Is it possible to build a quantum-secure PRF for a large domain out of a quantum-secure PRF for a small domain?

# 7 References

[BDF11]: Boneh D., Dagdelen O., Fischlin M., Lehmann A., Schaffner C., Zhandry M.: Random oracles in a quantum world (2011).

[BR93]: Bellare M., Rogaway P.: Random oracles are practical: A paradigm for designing efficient protocols (1993).

[BRRS09]: Bellare M., Ristenpart T., Rogaway P., Stegers T.: Format-preserving encryption (2009).

[BZ13]: Boneh D., Zhandry M.: Quantum-secure message authentication Codes (2013).

[BZ13b]: Boneh D., Zhandry M.: Secure signatures and chosen ciphertext security in a quantum computing world (2013).

[GGM86]: Goldreich O., Goldwasser S., Micali S.: How to construct random functions (1986).

[GPV08]: Gentry C., Peikert C., Vaikuntanathan V.: Trapdoors for hard lattices and new cryptographic constructions (2008).

[HILL99]: Håstad J., Impagliazzo R., Levin L., Luby M.: A pseudorandom generator from any one-way function (1999).

[KR00]: Krawczyk H., Rabin T.: Chameleon hashing and signatures (2000).

[LR88]: Luby M., Rackoff C.: How to construct pseudorandom permutations from pseudorandom functions (1988).

[Mermin07]: Mermin N.: Quantum computer science: an introduction (2007).

[Shor97]: Shor P.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer (1997).

[vD98]: van Dam W.: Quantum oracle interrogation: Getting all information for almost half the price (1998).

[Zha12a]: Zhandry M.: Secure identity-based encryption in the quantum random oracle model (2012).

[Zha12b]: Zhandry M.: How to construct quantum random functions (2012).

[Zha17]: Zhandry M.: A Note on quantum-secure PRPs (2017).