Non-Interactive Quantum Key Distribution

Giulio Malavolta[1] and Michael Walter[2]

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

Abstract

Quantum key distribution (QKD) allows Alice and Bob to agree on a shared secret key, while communicating over a public (untrusted) quantum channel. Compared to classical key exchange, it has two main advantages: (i) The key is *unconditionally* hidden to the eyes of any attacker, and (ii) its security assumes only the existence of authenticated classical channels which, in practice, can be realized using Minicrypt assumptions, such as the existence of digital signatures. On the flip side, QKD protocols typically require multiple rounds of interactions, whereas classical key exchange can be realized with the minimal amount of two messages. A long-standing open question is whether QKD requires more rounds of interaction than classical key exchange.

In this work, we propose a two-message QKD protocol that satisfies *everlasting* security, assuming only the existence of quantum-secure one-way functions. That is, the shared key is unconditionally hidden, provided computational assumptions hold during the protocol execution. Our result follows from a new quantum cryptographic primitive that we introduce in this work: the *quantum-public-key one-time pad*, a public-key analogue of the well-known one-time pad.

1 Introduction

Quantum key distribution (QKD) [2] enables Alice and Bob to exchange a secret key over a public (untrusted) quantum channel. Compared to classical key exchange, it offers two main advantages: (i) It hides the key *unconditionally* or *information-theoretically* to the eyes of any (possibly unbounded and quantum) attacker, and (ii) it relies only on the existence of authenticated classical channels, which in practice can be instantiated using Minicrypt [9] computational assumptions. The former is plainly impossible to achieve without quantum information, and we also have strong evidence [10] that classical key exchange requires more structured (Cryptomania) computational assumptions.

Over the past decades, QKD has inspired a staggering amount of research, ranging from profound theoretical works [16, 14, 15, 19] all the way to large-scale experiments [12, 13, 22]. As such, QKD is one of the most studied topics in the theory quantum information. Despite the vast literature on the topic, QKD protocols still do not outperform classical key exchange in all aspects: whereas classical key exchange can be realized using two messages [4], which is optimal, to the best of our knowledge all known QKD protocols require more than two rounds of interaction.

This raises the question of whether more rounds of interaction are really necessary for QKD. Apart from its theoretical importance, there are also practical reasons for addressing this question. Indeed, two-message protocols are particularly desirable for practical scenarios where parties may drop offline during the protocol execution, or may want to send their message at a later point in time. Arguably, this minimal interaction pattern is the property makes traditional cryptographic primitives, such as public-key encryption, so useful. However, despite this strong motivation and almost fifty years of intense research, the optimal round complexity of QKD is still an open problem.

1.1 Our Results

In this work we show that two messages are sufficient to build a QKD protocol with everlasting security. Specifically, we prove the following statement:

If quantum-secure one-way functions exist, then there exists two-message QKD.

Since two messages are clearly necessary for QKD, our protocol achieves the optimal round complexity. Henceforth, following traditional naming conventions in cryptography [11], we refer to such a protocol as *non-interactive* QKD. Furthermore, only the first message (from Alice to Bob) is quantum, whereas Bob's response is entirely classical. The protocol satisfies the strong notion of *everlasting security*: As long as the attacker runs in quantum polynomial time during the execution of the protocol, the shared key is hidden in an *information-theoretic* sense.

We view our approach as a big departure from the traditional design of QKD protocols [2, 5]. Both our protocol and its analysis are entirely elementary and they are simple enough to be fully described in an undergraduate class. For comparison, it took more than ten years for researchers to establish a formal proof of the first QKD protocol [2].

Our main technical ingredient is a new cryptographic primitive, that we refer to as *quantum-public-key one-time pad* (QPK-OTP): QPK-OTP allows Alice to sample a public key consisting of a quantum state ρ and a classical string pk. Bob can then use these to encrypt a message m that remains *information-theoretically* hidden, even if the distinguisher is given pk, and it is allowed to tamper arbitrarily with the quantum state ρ. In this sense, we view this notion as the natural public-key analogue of the well-known one-time pad.

Everlasting Security. We point out a subtle difference between the attacker model that we consider in this work, compared to the standard attacker model for QKD. The latter, considered for instance in [20, 21], models the attacker as a computationally unbounded quantum channel, that is however not allowed to tamper with the information sent over the *classical channels*. That is, it only assumes the existence of authenticated classical channels, but otherwise does not impose any restriction on the runtime of the distinguisher. On the other hand, in this work we consider – in addition to the existence of authenticated classical channels – an attacker that runs in *quantum polynomial time* during the protocol execution, but it is allowed to be unbounded once the protocol terminates. That is, we prove *everlasting security* in the sense of [17].

While technically different, we argue that for most practical scenarios the two models are in fact equivalent. The assumption of an authenticated classical channel is most often justified by having each party sign their own messages with a digital signature, which would require computational assumptions to hold (at the very least) during the execution of the protocol. In this sense, the mere existence of authenticated classical channels already restricts the attacker to run in quantum polynomial time during the protocol execution (as otherwise it could just break the security of the digital signature).

1.2 Open Problems

Our work leaves open a series of questions, that we hope will inspire further research in this area. For starters, our protocols are described in the presence of perfect (noiseless) quantum channels. Any practical protocol would need to withstand the presence of noise. While theoretically one could simply encode all states using a quantum error correcting code, this may lead to poor concrete efficiency. We leave open the question of investigating variants our non-interactive QKD protocol that are efficient in the presence of noise.

A compelling aspect of standard QKD protocols such as [2] is that all quantum states consists of tensor products of single qubits, whereas our protocols require coherent superpositions of many-qubit states. The former property is desirable, since it allows the experimental realization of the protocol on present-day quantum hardware. We view the problem of constructing a non-interactive QKD protocol in this qubit-by-qubit model as fascinating research direction, and believe that it might require substantially different techniques from the present approach.

1.3 Organization of this Paper

In Section 2, we discuss preliminaries in quantum information and cryptography. In Section 3, we define our new primitive, the quantum-public-key one-time pad (QPK-OTP), and explain how it can be constructed from quantum-secure one-way functions. In Section 4 we discuss applications of this primitive, including our non-interactive quantum key distribution protocol with everlasting security.

2 Preliminaries

Throughout this work, we denote the security parameter by λ. We denote by 1^λ the all-ones string of length λ. We say that a function negl is *negligible* in the security parameter λ if $\mathsf{negl} = o(\lambda^{-c})$ for all $c \in \mathbb{N}$. For a finite set S, we write $x \leftarrow S$ to denote that x is sampled uniformly at random from S. We write Tr for the trace of a matrix or operator.

2.1 Quantum Information

In this section, we provide some preliminary background on quantum information. For a more in-depth introduction, we refer the reader to [18]. A *register* x consisting of n qubits is given by a Hilbert space $(\mathbb{C}^2)^{\otimes n}$ with name or label x. Given two registers x and y, we write $\mathsf{x} \otimes \mathsf{y}$ for the composite register, with Hilbert space the tensor product of the individual registers' Hilbert spaces. A *pure quantum state* on register x is a unit vector $|\Psi\rangle_{\mathsf{x}} \in (\mathbb{C}^2)^{\otimes n}$. A *mixed quantum state* on register x is represented by a density operator ρ_{x} on $(\mathbb{C}^2)^{\otimes n}$, which is a positive semi-definite Hermitian matrix with trace 1. Any pure state $|\Psi\rangle_{\mathsf{x}}$ can also be regarded as a mixed state $\rho_{\mathsf{x}} = |\Psi\rangle_{\mathsf{x}} \langle\Psi|_{\mathsf{x}}$, but there are mixed states that are not pure. In the above, we use subscripts to denote registers, but we often omit these when clear from context. We adopt the convention that

$$\{|0\rangle, |1\rangle\} \text{ and } \left\{\frac{|0\rangle + |1\rangle}{\sqrt{2}}, \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right\}$$

denote the *computational* and the *Hadamard basis* states, respectively.

A *quantum channel* F is a completely-positive trace-preserving (CPTP) map from a register x to a register y. That is, on input any density matrix ρ_{x}, the operation F produces $F(\rho_{\mathsf{x}}) = \tau_{\mathsf{y}}$, another state on register y, and the same is true when we apply F to the x register of a quantum state ρ_{xz}. For any unitary operator U, meaning $U^\dagger U = UU^\dagger = \mathsf{Id}$, one obtains a quantum channel that maps input states ρ to output states $\tau := U\rho U^\dagger$. The Pauli operators $\mathsf{X}, \mathsf{Y}, \mathsf{Z}$ are 2×2 matrices that are unitary and Hermitian. More specifically:

$$\mathsf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \mathsf{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \mathsf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

A *projector* Π is a Hermitian operator such that $\Pi^2 = \Pi$. A *projective measurement* is given by a collection of projectors $\{\Pi_j\}_j$ such that $\sum_j \Pi_j = \mathsf{Id}$. Given a state ρ, the measurement yields outcome j with probability $p_j = \mathsf{Tr}(\Pi_j \rho)$, upon which the state changes to $\Pi_j \rho \Pi_j / p_j$ (this can be modeled by a quantum channel, but we will not need this). For any two registers x and y, the partial trace Tr_{y} is the unique channel from $\mathsf{x} \otimes \mathsf{y}$ to x such that $\mathsf{Tr}_{\mathsf{y}}(\rho_{\mathsf{x}} \otimes \tau_{\mathsf{y}}) = \mathsf{Tr}_{\mathsf{y}}(\tau_{\mathsf{y}})\rho_{\mathsf{x}}$ for all ρ_{x} and τ_{y}.

The *trace distance* between two states ρ and τ, denoted by $\mathsf{Td}(\rho, \tau)$ is defined as

$$\mathsf{Td}(\rho, \tau) = \frac{1}{2}\|\rho - \tau\|_1 = \frac{1}{2}\mathsf{Tr}\left(\sqrt{(\rho - \tau)^\dagger(\rho - \tau)}\right).$$

The operational meaning of the trace distance is that $\frac{1}{2}(1 + \mathsf{Td}(\rho, \tau))$ is the maximal probability that two states ρ and τ can be distinguishdd by any (possibly unbounded) quantum channel or algorithm. If $\tau = |\Phi\rangle\langle\Phi|$ is a pure state, we have the following version of the Fuchs-van de Graaf inequalities:

$$1 - \langle\Phi|\rho|\Phi\rangle \le \mathsf{Td}(\rho, \tau) \le \sqrt{1 - \langle\Phi|\rho|\Phi\rangle}. \tag{2.1}$$

Quantum Algorithms. A non-uniform *quantum polynomial-time (QPT) machine* $\{\mathcal{A}_\lambda\}_{\lambda \in \mathbb{N}}$ is a family of polynomial-size quantum machines $\mathcal{A}_\lambda$, where each is initialized with a polynomial-size advice state $|\alpha_\lambda\rangle$. Each $\mathcal{A}_\lambda$ can be described by a CPTP map. A quantum interactive machine is simply a sequence of quantum channels, with designated input, output, and work registers. We say that two probability distributions $\mathcal{X}$ and $\mathcal{Y}$ are *computationally indistinguishable* if there exists a negligible function negl such that for all QPT algorithms $\mathcal{A}_\lambda$ it holds that

$$\left|\Pr\left[1 \leftarrow \mathcal{A}_\lambda(x) : x \leftarrow \mathcal{X}\right] - \Pr\left[1 \leftarrow \mathcal{A}_\lambda(y) : y \leftarrow \mathcal{Y}\right]\right| = \mathsf{negl}(\lambda).$$

We say that they are *statistically indistinguishable* if the same holds for all (possibly unbounded) algorithms.

2.2 One-Time Signatures

We recall the notion of a one-time signature scheme [6].

Definition 2.1 (One-Time Signature)**.** A *one-time signature (OTS)* scheme is defined as a tuple of algorithms $(\mathsf{SGen}, \mathsf{Sign}, \mathsf{Ver})$ such that:

- $(\mathsf{vk}, \mathsf{sk}) \leftarrow \mathsf{SGen}(1^\lambda)$: A polynomial-time algorithm which, on input the security parameter 1^λ, outputs two bit strings vk and sk.
- $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}, m)$: A polynomial-time algorithm which, on input the signing key sk and a message m, outputs signature σ.

- $\{0,1\} \leftarrow \mathsf{Ver}(\mathsf{vk}, m, \sigma)$: A polynomial-time algorithm which, on input the verification key vk, a message m, and a signature σ, returns a bit denoting accept or reject.

The OTS scheme is *correct* if for all $\lambda \in \mathbb{N}$ and all messages m it holds that

$$\Pr\left[1 = \mathsf{Ver}(\mathsf{vk}, m, \mathsf{Sign}(\mathsf{sk}, m)) : (\mathsf{vk}, \mathsf{sk}) \leftarrow \mathsf{SGen}(1^\lambda)\right] = 1.$$

Next we define the notion of strong existential unforgeability for OTS, which states that one should not be able to produce a different signature (even if on the same message) than the one provided by the signing oracle. It is well-known that strongly unforgeable signatures can be constructed from any one-way function (OWF) [6]. For convenience we define a slightly weaker notion, where the message to be signed is fixed in advance – this notion is clearly implied by the standard one, where the attacker can query the signing oracle adaptively.

Definition 2.2 (Strong Existential Unforgeability)**.** We say that an OTS scheme $(\mathsf{SGen}, \mathsf{Sign}, \mathsf{Ver})$ satisfies *(quantum-secure) strong existential unforgeability* if there exists a negligible function negl such that for all QPT $\{\mathcal{A}_\lambda\}$, for all $\lambda \in \mathbb{N}$, and for all messages m, it holds that

$$\Pr\left[1 = \mathsf{Ver}(\mathsf{vk}, m^*, \sigma^*) \text{ and } (m^*, \sigma^*) \neq (m, \sigma) : \begin{array}{l} (\mathsf{vk}, \mathsf{sk}) \leftarrow \mathsf{SGen}(1^\lambda); \\ \sigma \leftarrow \mathsf{Sign}(\mathsf{sk}, m); \\ (m^*, \sigma^*) \leftarrow \mathcal{A}_\lambda(\mathsf{vk}, m, \sigma) \end{array}\right] = \mathsf{negl}(\lambda).$$

3 Quantum Public-Key One-Time Pad

In the following we define the central cryptographic primitive of this work, which we refer to as *quantum-public-key one-time pad (QPK-OTP)*. For notational convenience, we define the primitive for encrypting one-bit messages, but it is easy to generalize the notion and the corresponding construction to multiple bits, via the standard bit-by-bit encryption. Security of the multi-bit construction follows by a standard hybrid argument.

Definition 3.1 (QPK-OTP)**.** A *quantum-public-key one-time pad (QPK-OTP)* protocol is defined as a tuple of algorithms $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ such that:

- $(\rho, \mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda)$: A QPT algorithm which, on input the security parameter 1^λ, outputs a (possibly mixed) quantum state ρ and two bit strings pk and sk.
- $\mathsf{ct} \leftarrow \mathsf{Enc}(\rho, \mathsf{pk}, m)$: A QPT algorithm which, on input the public key (ρ, pk) and a message $m \in \{0,1\}$, outputs a classical ciphertext ct.
- $m \leftarrow \mathsf{Dec}(\mathsf{sk}, \mathsf{ct})$: A QPT algorithm which, on input the secret key sk and the ciphertext ct, outputs a message $m \in \{0,1\}$.

The QPK-OTP scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is *correct* if for all $\lambda \in \mathbb{N}$ and all $m \in \{0,1\}$ it holds that:

$$\Pr\left[m = \mathsf{Dec}(\mathsf{sk}, \mathsf{ct}) : (\rho, \mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda); \mathsf{ct} \leftarrow \mathsf{Enc}(\rho, \mathsf{pk}, m)\right] = 1.$$

Next, we define the notion of *everlasting security* for QPK-OTP. Informally, we require that the message is unconditionally hidden from the eyes of an attacker, even if a QPT attacker is allowed to tamper with the public key arbitrarily.

Definition 3.2 (Everlasting Security)**.** For a family of QPT algorithms $\{\mathcal{A}_\lambda\}_{\lambda\in\mathbb{N}}$, we define the experiment $\mathsf{Exp}^{\mathcal{A}_\lambda}(1^\lambda, m)$ as follows:

1. Sample $(\rho, \mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda)$ and send the corresponding public key (ρ, pk) to $\mathcal{A}_\lambda$.
2. $\mathcal{A}_\lambda$ returns two quantum registers. The first register is parsed as the modified public-key register, whereas the second register is arbitrary and will be referred to as the adversary's internal register.
3. Compute ct by applying the map defined by $\mathsf{Enc}(\cdot, \mathsf{pk}, m)$ to the public-key register returned by the adversary in the previous round.
4. The output of the experiment is defined to be the joint state of ct and the internal register of the adversary.

Then we say that a QPK-OTP scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ satisfies *everlasting security* if there exists a negligible function negl such that for all $\lambda \in \mathbb{N}$ and all QPT $\mathcal{A}_\lambda$ it holds that

$$\mathsf{Td}\left(\mathsf{Exp}^{\mathcal{A}_\lambda}(1^\lambda, 0), \mathsf{Exp}^{\mathcal{A}_\lambda}(1^\lambda, 1)\right) = \mathsf{negl}(\lambda).$$

Let us comment on the definition as stated above. First, we remark that the definition can be easily extended to the case of multi-bit messages, provided that the syntax of the encryption scheme is extended accordingly. As a second point, we stress the fact that, while the attacker is allowed to modify the quantum states arbitrarily, it cannot tamper with the classical information (such as pk or ct). This models the presence of *authenticated classical channels*, which are assumed to deliver the classical information faithfully. Note that the same assumption is also present (although somewhat more implicitly) for the standard notion of *classical* PKE, where the encryption algorithm in the CPA/CCA-security experiment is always provided as input the correct public key sampled by the challenger. This restriction is of course necessary, since if the attacker is allowed to choose the public key arbitrarily, then the definition would be impossible to achieve.

Finally, we also mention that an alternative definition might also allow the adversary to do some arbitrary post-processing on the output of the experiment. However, our definition is equivalent (and arguably simpler) by the monotonicity of the trace distance.

3.1 QPK-OTP from One-Way Functions

We describe our scheme below. As the only computational ingredient, we assume the existence of a quantum-secure strongly existentially unforgeable one-time signature scheme $(\mathsf{SGen}, \mathsf{Sign}, \mathsf{Ver})$, see Section 2.2. As discussed, this can be constructed from any quantum-secure one-way function.

- $\mathsf{Gen}(1^\lambda)$:
  - Sample two key pairs $(\mathsf{sk}_0, \mathsf{vk}_0) \leftarrow \mathsf{SGen}(1^\lambda)$ and $(\mathsf{sk}_1, \mathsf{vk}_1) \leftarrow \mathsf{SGen}(1^\lambda)$.
  - Compute $\sigma_0 \leftarrow \mathsf{Sign}(\mathsf{sk}_0, 0)$ and $\sigma_1 \leftarrow \mathsf{Sign}(\mathsf{sk}_1, 1)$.
  - Define the state
  $$|\Psi\rangle = \frac{|0, 0, \sigma_0\rangle + |1, 1, \sigma_1\rangle}{\sqrt{2}}.$$
  This state is efficiently computable by preparing an EPR pair and CNOT-ing the bits of the signatures into an auxiliary register, controlled on the value of the first qubit.

- Measure the first qubit in the Hadamard basis to obtain a bit $d_0 \in \{0,1\}$.
- Set the quantum part of the public key ρ to be the state the unmeasured registers, set the classical part of the public key and the classical secret key to

$$\mathsf{pk} = (\mathsf{vk}_0, \mathsf{vk}_1) \qquad \text{and} \qquad \mathsf{sk} = (\sigma_0, \sigma_1, d_0),$$

respectively, and return $(\rho, \mathsf{pk}, \mathsf{sk})$.

- $\mathsf{Enc}(\rho, \mathsf{pk}, m)$:
  - Project ρ onto the subspace of valid signatures of 0 and 1, under vk_0 and vk_1, respectively. More precisely, denote by Σ_0 and Σ_1 the set of accepting signatures on 0 and 1, under vk_0 and vk_1, respectively, and consider the projector

$$\Pi = \sum_{\sigma \in \Sigma_0} |0, \sigma\rangle\langle 0, \sigma| + \sum_{\sigma \in \Sigma_1} |1, \sigma\rangle\langle 1, \sigma| \,.$$

Apply the projective measurement $\{\Pi, \mathsf{Id} - \Pi\}$, and abort the execution (return $\perp$) if the measurement returns the second outcome. Note that this measurement can be implemented efficiently by running the verification algorithm coherently, CNOT-ing the output bit on a separate register and measuring it.
  - Measure the residual state in the Hadamard basis, to obtain a bit string (d_1, d_2), where we denote by $d_1 \in \{0,1\}$ the first bit of the measurement outcome and by d_2 the rest.
  - Return the following as the classical ciphertext:

$$\mathsf{ct} = (m \oplus d_1, d_2). \tag{3.1}$$

- $\mathsf{Dec}(\mathsf{sk}, \mathsf{ct})$:
  - Parse $\mathsf{ct} = (\mathsf{ct}_1, \mathsf{ct}_2)$, where $\mathsf{ct}_1 \in \{0,1\}$ is one bit, and return

$$m = d_0 \oplus \mathsf{ct}_1 \oplus \mathsf{ct}_2 \cdot (\sigma_0 \oplus \sigma_1). \tag{3.2}$$

Analysis. We first analyze the correctness of the scheme. To show that decryption algorithm returns the correct bit with certainty, we analyze the correctness of a slightly different algorithm, where the measurement in the key generation (returning outcome d_0) is deferred until the end of the encryption algorithm. Since the encryption algorithm measures on a different register, by the principle of delayed measurements, this does not change the output distributions of the algorithms.

Now, observe that the reduced state ρ taken as input by the encryption algorithm is the classical mixed state

$$\rho = \frac{|0, \sigma_0\rangle\langle 0, \sigma_0| + |1, \sigma_1\rangle\langle 1, \sigma_1|}{2}$$

and in particular is in the image of the projector Π as defined above. Consequently, applying the projective measurement $\{\Pi, \mathsf{Id} - \Pi\}$ returns the outcome associated with Π with certainty and does not change the state. Next, since we delayed the measurement of the first qubit, we now measure all qubits of $|\Psi\rangle$ in the Hadamard basis, to obtain (d_0, d_1, d_2). Note that applying Hadamard gates to all qubit gives

$$\mathsf{H} |\Psi\rangle = \sum_d (-1)^{d \cdot (0,0,\sigma_0)} |d\rangle + (-1)^{d \cdot (1,1,\sigma_1)} |d\rangle = \sum_{d \,:\, d \cdot (1,1,\sigma_0 \oplus \sigma_1) = 0} |d\rangle \,,$$

omitting overall normalization factors. Therefore, a measurement returns a uniformly random bit string $d = (d_0, d_1, d_2)$ satisfying $(d_0, d_1, d_2) \cdot (1, 1, \sigma_0 \oplus \sigma_1) = 0$, that is,

$$d_1 \oplus d_2 \cdot (\sigma_0 \oplus \sigma_1) = d_0.$$

Substituting Eq. (3.1) in Eq. (3.2) and using this relation, we obtain

$$d_0 \oplus \mathsf{ct}_1 \oplus \mathsf{ct}_2 \cdot (\sigma_0 \oplus \sigma_1) = d_0 \oplus (m \oplus d_1) \oplus d_2 \cdot (\sigma_0 \oplus \sigma_1) = m,$$

as desired. Next, we show that the scheme satisfies everlasting security.

Theorem 3.3 (Everlasting security)**.** If quantum-secure one-way functions exist, then the QPK-OTP $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ satisfies everlasting security.

Proof. We proceed by defining a series of hybrid experiments that we show to be indistinguishable from the eyes of any (possibly unbounded) algorithm. For convenience, we define

$$\mathsf{Adv}(i) = \mathsf{Td}\left(\mathsf{Hyb}_i^{\mathcal{A}_\lambda}(1^\lambda, 0), \mathsf{Hyb}_i^{\mathcal{A}_\lambda}(1^\lambda, 1)\right).$$

- $\mathsf{Hyb}_0^{\mathcal{A}_\lambda}(1^\lambda, b)$: This is the original experiment $\mathsf{Exp}^{\mathcal{A}_\lambda}(1^\lambda, b)$, as defined in Definition 3.2.
- $\mathsf{Hyb}_1^{\mathcal{A}_\lambda}(1^\lambda, b)$: In this experiment, we modify the Gen algorithm to measure the first qubit of the state $|\Psi\rangle$ in the computational basis, instead of the Hadamard basis.

Since the result sk of the Gen algorithm is not used, we only need to argue that the reduced states of (pk, ρ) are unchanged by this modification. This is indeed the case, since in either experiment we measure the first qubit, ignore the outcome, and return the state of the unmeasured qubits – which is indistinguishable from simply tracing over the first qubit. Thus the two experiments are identical from the perspective of the adversary and therefore $\mathsf{Adv}(0) = \mathsf{Adv}(1)$.

- $\mathsf{Hyb}_2^{\mathcal{A}_\lambda}(1^\lambda, b)$: In this experiment, we further modify the Gen algorithm to sample the state ρ as follows. Flip a random coin $c \leftarrow \{0, 1\}$. If $c = 0$ then return $|0, \sigma_0\rangle\langle 0, \sigma_0|$, and otherwise return $|1, \sigma_1\rangle\langle 1, \sigma_1|$.

Observe that the state ρ returned by the modified Gen algorithm is the classical mixture

$$\rho = \frac{|0, \sigma_0\rangle\langle 0, \sigma_0| + |1, \sigma_1\rangle\langle 1, \sigma_1|}{2}$$

which is identical to the state returned in the previous hybrid. Therefore $\mathsf{Adv}(1) = \mathsf{Adv}(2)$.

Next, let us denote by ρ^* the reduced density matrix of the modified public-key register returned by the adversary in step 2 of the experiment. We will assume that the state ρ^* returned by the adversary is such that the encryption algorithm accepts (i.e., does not abort) with non-negligible probability (for otherwise $\mathsf{Adv}(2) = \mathsf{negl}(\lambda)$ and we are done). We can then establish that the state ρ^*, once projected onto the image of Π, must be negligibly close in trace distance from the state produced by the Gen algorithm.

Claim 3.4. There exists a negligible function negl such that, for $c \in \{0, 1\}$ the result of the coin toss in the Gen algorithm,

$$\mathsf{Td}\left(\frac{\Pi\rho^*\Pi}{\mathsf{Tr}\left(\Pi\rho^*\right)}, |c, \sigma_c\rangle\langle c, \sigma_c|\right) = \mathsf{negl}(\lambda).$$

Proof of Claim 3.4. The proof follows by a reduction to the unforgeability of the OTS. Indeed, assume for sake of contradiction that the post-measurement state is non-negligibly far from $|c, \sigma_c\rangle$ in trace distance. By Eq. (2.1), the latter is equivalent to saying that if we measure in the computational basis then the probability of obtaining outcome (c, σ_c) is non-negligibly smaller than 1. Since the post-measurement state is supported on range of Π, it follows that if we measure in the computational basis then we must with non-negligible probability obtain an outcome (z, σ) such that

$$(z, \sigma) \neq (c, \sigma_c) \quad \text{and} \quad \mathsf{Ver}(\mathsf{vk}_z, z, \sigma) = 1,$$

that is, $(z, \sigma) \neq (c, \sigma_c)$ is a valid message-signature pair. As the adversary along with the projective measurement $\{\Pi, I - \Pi\}$ and the standard basis measurement run in quantum polynomial time, and the projective measurement returns Π with non-negligible probability, this contradicts the strong existential unforgeability of the OTS scheme. $\square$

We conclude by establishing that the message m is statistically hidden in the last experiment.

Claim 3.5. There exists a negligible function negl such that $\mathsf{Adv}(2) = \mathsf{negl}(\lambda)$.

Proof of Claim 3.5. By Claim 3.4, the post-measurement state is negligibly close to the state $|c, \sigma_c\rangle$. As the latter is a pure state and extensions of pure states are always in tensor product, by Uhlmann's theorem it follows that the post-measurement register is negligibly close to being in tensor product with the internal register of the adversary. Thus it suffices to show that the output distribution of the Enc algorithm does not depend on the message m when given as input $|c, \sigma_c\rangle$. To see this, observe that the rotated state in the Hadamard basis is up to overall normalization given by

$$\mathsf{H} |c, \sigma_c\rangle = \sum_{d'} (-1)^{d' \cdot (c, \sigma_c)} |d'\rangle ,$$

and therefore a measurement returns a uniformly random bit string $d' = (d_1, d_2)$. In particular, $\mathsf{ct} = (m \oplus d_1, d_2)$ has the same distribution for $m \in \{0, 1\}$. As explained above, it is also negligibly close to being independent from the internal register of the adversary, and thus the claim follows. $\square$

By Claim 3.5 we have that

$$\mathsf{Adv}(0) = \mathsf{Adv}(1) = \mathsf{Adv}(2) = \mathsf{negl}(\lambda),$$

and this concludes the proof of Theorem 3.3. $\square$

4 Applications and Extensions

We discuss how QPK-OTP leads to new protocols for QKD and quantum teleportation, as immediate corollaries. We also present a modified construction where the secret key of Alice can be reused, at the cost of settling for computational security. For brevity we omit formal definitions and we only present a high-level overview of the protocols.

4.1 Non-Interactive Quantum Key Distribution

In the following we outline how to use a QPK-OTP scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ to construct a QKD protocol with a minimal number of two rounds of interaction, as announced in the introduction. For notational convenience, we assume that the encryption and decryption algorithms allow one to exchange multi-bit messages, which can be achieved using bit-by-bit encryption. We also assume the existence of an authenticated classical channel, along with an OTS scheme $(\mathsf{SGen}, \mathsf{Sign}, \mathsf{Ver})$.

- *(1st Message) Alice:* Sample a QPK-OTP key pair $(\rho, \mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda)$ and send pk via an authenticated classical channel and ρ via a quantum channel to Bob.
- *(2nd Message) Bob:* Upon receiving the messages from the previous round, sample an OTS key pair $(\mathsf{vk}, \mathsf{zk}) \leftarrow \mathsf{SGen}(1^\lambda)$ and a key $k \leftarrow \{0,1\}^\lambda$. Compute

  $$\sigma \leftarrow \mathsf{Sign}(\mathsf{zk}, k) \text{ and } \mathsf{ct} \leftarrow \mathsf{Enc}(\rho, \mathsf{pk}, (k, \sigma)).$$

  Send vk, ct via an authenticated classical channel to Alice. Return k as the shared secret key.
- *(Post-Processing) Alice:* Decrypt the incoming ciphertext ct and verify that the plaintext consists of a valid message-signature pair (k, σ), against the vk received in the previous round. If this check fails, output $\perp$, otherwise return k as the shared key.

It is easy to show that no efficient attacker can convince Alice and Bob to agree on a different key, with a simple reduction against the unforgeability of the OTS. On the other hand, the key k is unconditionally hidden via an invocation of the everlasting security of the QPK-OTP scheme.

4.2 Authenticated Quantum Teleportation

We show how QPK-OTP (with everlasting security) leads to a simple variant of quantum teleportation, where an eavesdropper is allowed to tamper with the quantum state arbitrarily. I.e., we consider the scenario where Bob wants to send to Alice an arbitrary state $|\Psi\rangle$, and Bob is guaranteed that only Alice can learn the teleported state in an information-theoretic sense, without assuming that Alice and Bob pre-share any entangled state. Note that the celebrated protocol from [3] is insecure in this attacker model, since an attacker could simply swap the EPR pairs of Alice with some locally sampled EPR pair. The following protocol also assumes the existence of authenticated classical channels. For notational convenience, we present the protocol for teleporting a single-qubit state $|\Psi\rangle$, but it can straightforwardly be generalized to multiple qubits.

- *(1st Message) Alice:* Sample a QPK-OTP key pair $(\rho, \mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda)$ and an EPR pair

  $$\left|\Phi^+\right\rangle_{\mathsf{a},\mathsf{b}} = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

  Send pk via an authenticated classical channel, and send ρ together with the content of the b register via a quantum channel to Bob.
- *(2nd Message) Bob:* Upon receiving the messages from the previous round, apply a teleportation measurement to the register containing $|\Psi\rangle$ and b and let (x, z) be the output bits. Compute

  $$\mathsf{ct} \leftarrow \mathsf{Enc}(\rho, \mathsf{pk}, (x, z)).$$

  Then send ct via an authenticated classical channel to Alice.

- *(Post-Processing) Alice:* Decrypt the incoming ciphertext ct to recover x and z and apply the operator $\mathsf{X}^x\mathsf{Z}^z$ to the residual state in the register a.

To see why the protocol protects Bob against a malicious eavesdropper, it suffices to observe that, by the strong everlasting security of the QPK-OTP, no matter what quantum state Bob receives, the bits (x, z) are information theoretically hidden. It follows that, regardless of the state that Bob received in the register b, the view of the attacker is statistically close to a view that is formally independent of the state $|\Psi\rangle$.

4.3 Reusable Secret Key

In the construction presented in Section 3.1, the secret key sk cannot be reused. For practical purposes, it is desirable to have a construction where the secret key can be stored for long-term use and does not have to be sampled for every ciphertext. In the following we present a construction with reusable secret key, albeit sacrificing everlasting security and settling for *computational indistinguishability*. Compared with the standard notion of public-key encryption, our scheme has the advantage of being realizable assuming only quantum-secure one-way functions. On the flip side, it requires quantum communication (and authenticated *classical* channels). In this alternative scheme, the public key consists of single state

$$\frac{|0,\sigma_0\rangle + |1,\sigma_1\rangle}{\sqrt{2}}, (\mathsf{vk}_0, \mathsf{vk}_1), r$$

where σ_0 and σ_1 are valid signatures on 0 and 1 under vk_0 and vk_1, respectively, and $r \in \{0,1\}^\lambda$ is a random bit string. The secret key consists of the key k of a pseudorandom function, which can also be built from one-way functions [7], that, on input r, is used to fix the random coins of the SGen and Sign algorithms. This allows the decrypter to recompute this information, while only keeping k in memory. To encrypt a message $m \in \{0,1\}$, one simply applies a controlled Z gate to compute

$$\frac{|0,\sigma_0\rangle + (-1)^m |1,\sigma_1\rangle}{\sqrt{2}}$$

and the decrypter can recover m by measuring the state in the

$$\left\{\frac{|0,\sigma_0\rangle + |1,\sigma_1\rangle}{\sqrt{2}}, \frac{|0,\sigma_0\rangle - |1,\sigma_1\rangle}{\sqrt{2}}\right\}$$

basis. To see why this scheme is secure, it suffices to observe that, by the "distinguishing implies swapping" principle [1] the state in the public key is computationally indistinguishable from the classical mixture

$$\frac{|0,\sigma_0\rangle + |1,\sigma_1\rangle}{\sqrt{2}} \otimes \frac{\langle 0,\sigma_0| + \langle 1,\sigma_1|}{\sqrt{2}} \approx \frac{|0,\sigma_0\rangle\langle 0,\sigma_0| + |1,\sigma_1\rangle\langle 1,\sigma_1|}{2} \tag{4.1}$$

and applying a phase flip to a basis state only adds a global phase. For completness, we provide a formal proof of this fact in Appendix A.

Acknowledgments

The authors would like to thank Khashayar Barooti for many discussion on quantum public key encryption. G.M. was partially funded by the German Federal Ministry of Education and Research (BMBF) in the course of the 6GEM research hub under grant number 16KISK038 and by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA – 390781972. M.W. acknowledges support by the the European Union (ERC, SYMOPTIC, 101040907), by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA - 390781972, by the BMBF through project QuBRA, and by the Dutch Research Council (NWO grant OCENW.KLEIN.267). Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Council Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

References

[1] Aaronson, S., Atia, Y., Susskind, L.: On the hardness of detecting macroscopic superpositions. Electron. Colloquium Comput. Complex. **TR20-146** (2020), `https://eccc.weizmann.ac.il/report/2020/146`

[2] Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing. p. 175. India (1984)

[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] Diffie, W., Hellman, M.E.: New directions in cryptography. IEEE Trans. Inf. Theory **22**(6), 644–654 (1976). https://doi.org/10.1109/TIT.1976.1055638

[5] Ekert, A.K.: Quantum cryptography based on Bell's theorem. Physical review letters **67**(6), 661 (1991)

[6] Goldreich, O.: The Foundations of Cryptography - Volume 2: Basic Applications. Cambridge University Press (2004). https://doi.org/10.1017/CBO9780511721656

[7] Goldreich, O., Goldwasser, S., Micali, S.: How to construct random functions. Journal of the ACM (JACM) **33**(4), 792–807 (1986)

[8] Hhan, M., Morimae, T., Yamakawa, T.: From the hardness of detecting superpositions to cryptography: Quantum public key encryption and commitments. IACR Cryptol. ePrint Arch. p. 1375 (2022), `https://eprint.iacr.org/2022/1375`

[9] Impagliazzo, R.: A personal view of average-case complexity. In: Proceedings of Structure in Complexity Theory. Tenth Annual IEEE Conference. pp. 134–147. IEEE (1995)

[10] 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`

[11] Ishai, Y., Kushilevitz, E., Ostrovsky, R., Prabhakaran, M., Sahai, A.: Efficient non-interactive secure computation. In: Paterson, K.G. (ed.) Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings. Lecture Notes in Computer Science, vol. 6632, pp. 406–425. Springer (2011). https://doi.org/10.1007/978-3-642-20465-4_23, `https://doi.org/10.1007/978-3-642-20465-4_23`

[12] Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangier, P., Diamanti, E.: Experimental demonstration of long-distance continuous-variable quantum key distribution. Nature Photonics **7**(5), 378–381 (2013)

[13] Korzh, B., Lim, C.C.W., Houlmann, R., Gisin, N., Li, M.J., Nolan, D., Sanguinetti, B., Thew, R., Zbinden, H.: Provably secure and practical quantum key distribution over 307 km of optical fibre. Nature Photonics **9**(3), 163–168 (2015)

[14] Lo, H.K., Chau, H.F.: Unconditional security of quantum key distribution over arbitrarily long distances. Science **283**(5410), 2050–2056 (1999)

[15] Mayers, D.: Unconditional security in quantum cryptography. Journal of the ACM (JACM) **48**(3), 351–406 (2001)

[16] Mayers, D., Yao, A.C.: Quantum cryptography with imperfect apparatus. In: 39th Annual Symposium on Foundations of Computer Science, FOCS '98, November 8-11, 1998, Palo Alto, California, USA. pp. 503–509. IEEE Computer Society (1998). https://doi.org/10.1109/SFCS.1998.743501

[17] Müller-Quade, J., Unruh, D.: Long-term security and universal composability. J. Cryptol. **23**(4), 594–671 (2010). https://doi.org/10.1007/s00145-010-9068-8

[18] Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information (10th Anniversary edition). Cambridge University Press (2016)

[19] Renner, R.: Security of quantum key distribution. International Journal of Quantum Information **6**(01), 1–127 (2008)

[20] Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Physical review letters **85**(2), 441 (2000)

[21] Tomamichel, M., Leverrier, A.: A largely self-contained and complete security proof for quantum key distribution. Quantum **1**, 14 (2017)

[22] Yin, J., Cao, Y., Li, Y.H., Liao, S.K., Zhang, L., Ren, J.G., Cai, W.Q., Liu, W.Y., Li, B., Dai, H., et al.: Satellite-based entanglement distribution over 1200 kilometers. Science **356**(6343), 1140–1144 (2017)

A Indistinguishability of Signature States

We show a formal proof for Equation (4.1), since it is a statement that could be of independent interest. First, we recall the formal statement of the equivalence between distinguishing states and swapping on the conjugate basis. This was proven in [1] and below we show a rephrased version borrowed from [8]. We actually only state one direction of the implication (the converse is also shown to be true in [1]), since it is the one needed for our purposes.

Theorem A.1 (Distinguishing Implies Swapping [1])**.** Let $|\Psi\rangle$ and $|\Phi\rangle$ be orthogonal n-qubit states, and suppose that a QPT distinguisher $\mathcal{A}_\lambda$ distinguishes $|\Psi\rangle$ and $|\Phi\rangle$ with advantage δ without using any ancilla qubits. Then, there exists a polynomial-time computable unitary U over n-qubit states such that

$$\frac{|\langle y| U |x\rangle + \langle x| U |y\rangle|}{2} = \delta \text{ where } |x\rangle = \frac{|\Psi\rangle + |\Phi\rangle}{\sqrt{2}} \text{ and } |y\rangle = \frac{|\Psi\rangle - |\Phi\rangle}{\sqrt{2}}.$$

Moreover, if $\mathcal{A}_\lambda$ does not act on some qubits, then U also does not act on those qubits.

Next, we provide a formal statement and a proof of the indistinguishability of our hidden-basis states and the corresponding classical mixture. This proof is inspired by, and closely follows, the work of [8].

Lemma A.2. Let $(\mathsf{SGen}, \mathsf{Sign}, \mathsf{Ver})$ be an OTS scheme that satisfies strong existential unforgeability. Then the following distribution ensambles are computationally indistinguishable

$$\left\{ \frac{|0,\sigma_0\rangle + |1,\sigma_1\rangle}{\sqrt{2}} \otimes \frac{\langle 0,\sigma_0| + \langle 1,\sigma_1|}{\sqrt{2}}, (\mathsf{vk}_0, \mathsf{vk}_1) \right\} \approx \left\{ \frac{|0,\sigma_0\rangle\langle 0,\sigma_0| + |1,\sigma_1\rangle\langle 1,\sigma_1|}{2}, (\mathsf{vk}_0, \mathsf{vk}_1) \right\}$$

where $(\mathsf{vk}_b, \mathsf{sk}_b) \leftarrow \mathsf{SGen}(1^\lambda)$ and $\sigma_b \leftarrow \mathsf{Sign}(\mathsf{sk}_b, b)$, for $b \in \{0, 1\}$.

Proof. By convexity, it suffices to show that no QPT adversary acting on registers v and x can distinguish between the states $|\Psi_0\rangle$ and $|\Psi_1\rangle$ with non-negligible probability, where

$$|\Psi_b\rangle = \sum_{(\mathsf{vk},\mathsf{sk})} \sqrt{D(\mathsf{vk}, \mathsf{sk})}\, |\mathsf{vk}, \mathsf{sk}\rangle_{\mathsf{s}} |\mathsf{vk}\rangle_{\mathsf{v}} \otimes \frac{|0,\sigma_0\rangle_{\mathsf{x}} + (-1)^b |1,\sigma_1\rangle_{\mathsf{x}}}{\sqrt{2}}$$

and we adopt the following convention for the notation:

$$\mathsf{sk} = \{\mathsf{sk}_0, \mathsf{sk}_1\} \ ; \ \mathsf{vk} = \{\mathsf{vk}_0, \mathsf{vk}_1\} \ ; \ \sigma_b = \mathsf{Sign}(\mathsf{sk}_b, b) \text{ and } D(\mathsf{vk}, \mathsf{sk}) = \Pr[(\mathsf{vk}, \mathsf{sk}) = \mathsf{SGen}(1^\lambda)].$$

Assume towards contradiction that there exists a QPT distinguisher acting on registers v, x, as well as an auxiliary register $|\alpha_\lambda\rangle_{\mathsf{a}}$ that succeeds with probability δ. Then, by Theorem A.1 there exists a polynomial-time computable unitary U such that

$$\frac{1}{2} \left| \begin{array}{l} \langle \Psi'_1|_{\mathsf{s,v,x}} \langle \alpha_\lambda|_{\mathsf{a}} (U_{\mathsf{v,x,a}} \otimes \mathsf{Id}_{\mathsf{s}}) |\Psi'_0\rangle_{\mathsf{s,v,x}} |\alpha_\lambda\rangle_{\mathsf{a}} \\ + \langle \Psi'_0|_{\mathsf{s,v,x}} \langle \alpha_\lambda|_{\mathsf{a}} (U_{\mathsf{v,x,a}} \otimes \mathsf{Id}_{\mathsf{s}}) |\Psi'_1\rangle_{\mathsf{s,v,x}} |\alpha_\lambda\rangle_{\mathsf{a}} \end{array} \right| = \delta$$

where

$$|\Psi'_b\rangle = \frac{|\Psi_0\rangle + (-1)^b |\Psi_1\rangle}{\sqrt{2}} = \sum_{(\mathsf{vk},\mathsf{sk})} \sqrt{D(\mathsf{vk}, \mathsf{sk})}\, |\mathsf{vk}, \mathsf{sk}\rangle_{\mathsf{s}} |\mathsf{vk}\rangle_{\mathsf{v}} \otimes |b, \sigma_b\rangle_{\mathsf{x}}.$$

Consequently, it must be the case that either

- $\langle \Psi_1' |_{\mathsf{s,v,x}} \langle \alpha_\lambda |_{\mathsf{a}} (U_{\mathsf{v,x,a}} \otimes \mathsf{Id}_{\mathsf{s}}) | \Psi_0' \rangle_{\mathsf{s,v,x}} | \alpha_\lambda \rangle_{\mathsf{a}} \geq \delta$, or
- $\langle \Psi_0' |_{\mathsf{s,v,x}} \langle \alpha_\lambda |_{\mathsf{a}} (U_{\mathsf{v,x,a}} \otimes \mathsf{Id}_{\mathsf{s}}) | \Psi_1' \rangle_{\mathsf{s,v,x}} | \alpha_\lambda \rangle_{\mathsf{a}} \geq \delta$.

Without loss of generality we assume that the former holds, but the argument works symmetrically also for the latter case. We will show that this leads to a contradiction with a reduction against the one-time unforgeability of OTS. In fact we will consider an even weaker definition where the adversary receives *no signature*.

On input a verification key vk_1 and an advice $|\alpha_\lambda\rangle_{\mathsf{a}}$ the reduction samples a uniform $(\mathsf{vk}_0, \mathsf{sk}_0) \leftarrow \mathsf{SGen}(1^\lambda)$, and sets $\mathsf{vk} = \{\mathsf{vk}_0, \mathsf{vk}_1\}$. Then it computes $\sigma_0 \leftarrow \mathsf{Sign}(\mathsf{sk}_0, 0)$ and

$$U_{\mathsf{v,x,a}} |\mathsf{vk}\rangle_{\mathsf{v}} |0, \sigma_0\rangle_{\mathsf{x}} |\alpha_\lambda\rangle_{\mathsf{a}}$$

and returns the result of a measurement of the x register in the computational basis.

We now analyze the success probability of the reduction in producing a valid signature, for a fixed key pair $(\mathsf{vk}_1, \mathsf{sk}_1)$. Let us denote by Σ_1 the set of all valid signatures on 1 under vk_1, and by $\sigma_1 = \mathsf{Sign}(\mathsf{sk}_1, 1)$. Then we have that the success probability of the reduction equals

$$\begin{aligned}
&\sum_{\sigma_1' \in \Sigma_1} |\Sigma_1| \cdot \left\| \langle 1, \sigma_1' |_{\mathsf{x}} U_{\mathsf{v,x,a}} |\mathsf{vk}\rangle_{\mathsf{v}} |0, \sigma_0\rangle_{\mathsf{x}} |\alpha_\lambda\rangle_{\mathsf{a}} \right\|^2 \\
&\qquad \geq \| \langle 1, \sigma_1 |_{\mathsf{x}} U_{\mathsf{v,x,a}} |\mathsf{vk}\rangle_{\mathsf{v}} |0, \sigma_0\rangle_{\mathsf{x}} |\alpha_\lambda\rangle_{\mathsf{a}} \|^2 \\
&\qquad \geq | \langle \mathsf{vk} |_{\mathsf{v}} \langle 1, \sigma_1 |_{\mathsf{x}} \langle \alpha_\lambda |_{\mathsf{a}} U_{\mathsf{v,x,a}} |\mathsf{vk}\rangle_{\mathsf{v}} |0, \sigma_0\rangle_{\mathsf{x}} |\alpha_\lambda\rangle_{\mathsf{a}} |^2 \\
&\qquad = | \langle \mathsf{vk}, \mathsf{sk} |_{\mathsf{s}} \langle \mathsf{vk} |_{\mathsf{v}} \langle 1, \sigma_1 |_{\mathsf{x}} \langle \alpha_\lambda |_{\mathsf{a}} (U_{\mathsf{v,x,a}} |\mathsf{vk}\rangle_{\mathsf{v}} \otimes \mathsf{Id}_{\mathsf{s}}) |\mathsf{vk}, \mathsf{sk}\rangle_{\mathsf{s}} |0, \sigma_0\rangle_{\mathsf{x}} |\alpha_\lambda\rangle_{\mathsf{a}} |^2
\end{aligned}$$

where the second inequality follows from the fact that inserting $\langle \mathsf{vk}|_{\mathsf{v}}$ and $\langle \alpha_\lambda|_{\mathsf{a}}$ can only decrease the norm. Now, over the random choice of $(\mathsf{vk}, \mathsf{sk})$ the success probability of the reduction can be lower bounded by

$$\begin{aligned}
&\mathbb{E}_{(\mathsf{vk},\mathsf{sk})} \left[| \langle \mathsf{vk}, \mathsf{sk} |_{\mathsf{s}} \langle \mathsf{vk} |_{\mathsf{v}} \langle 1, \sigma_1 |_{\mathsf{x}} \langle \alpha_\lambda |_{\mathsf{a}} (U_{\mathsf{v,x,a}} |\mathsf{vk}\rangle_{\mathsf{v}} \otimes \mathsf{Id}_{\mathsf{s}}) |\mathsf{vk}, \mathsf{sk}\rangle_{\mathsf{s}} |0, \sigma_0\rangle_{\mathsf{x}} |\alpha_\lambda\rangle_{\mathsf{a}} |^2 \right] \\
&\geq \left| \mathbb{E}_{(\mathsf{vk},\mathsf{sk})} \left[\langle \mathsf{vk}, \mathsf{sk} |_{\mathsf{s}} \langle \mathsf{vk} |_{\mathsf{v}} \langle 1, \sigma_1 |_{\mathsf{x}} \langle \alpha_\lambda |_{\mathsf{a}} (U_{\mathsf{v,x,a}} |\mathsf{vk}\rangle_{\mathsf{v}} \otimes \mathsf{Id}_{\mathsf{s}}) |\mathsf{vk}, \mathsf{sk}\rangle_{\mathsf{s}} |0, \sigma_0\rangle_{\mathsf{x}} |\alpha_\lambda\rangle_{\mathsf{a}} \right] \right|^2 \\
&\geq \delta
\end{aligned}$$

where the first inequality follows from Jensen's inequality. This contradicts the unforgeability of OTS and concludes our proof. □