Unconditionally-Secure and Reusable Public-Key Authentication

Lawrence M. Ioannou[1,2](✉) and Michele Mosca[1,2,3]

[1] Institute for Quantum Computing, University of Waterloo, 200 University Avenue,
Waterloo, ON N2L 3G1, Canada

[2] Department of Combinatorics and Optimization, University of Waterloo, 200
University Avenue, Waterloo, ON N2L 3G1, Canada
lmioannou@gmail.com

[3] Perimeter Institute for Theoretical Physics, 31 Caroline Street North,
Waterloo, ON N2L 2Y5, Canada

Abstract. We present a quantum-public-key identification protocol and show that it is secure against a computationally-unbounded adversary. This demonstrates for the first time that unconditionally-secure and reusable public-key authentication is possible in principle with (pure-state) public keys.

1 Introduction

Public-key cryptography has proved to be an indispensable tool in the modern information security infrastructure. Most notably, digital signature schemes form the backbone of Internet commerce, allowing trust to be propagated across the network in an efficient fashion. In turn, public-key encryption allows the private communication of messages (or, more usually, the establishment of symmetric secret keys) among users who are authenticated via digital signatures. The security of these classical public-key cryptosystems relies on assumptions on the difficulty of certain mathematical problems [1]. Gottesman and Chuang [2] initiated the study of quantum-public-key cryptography, where the public keys are quantum systems, with the goal of obtaining the functionality and efficiency of public-key cryptosystems but with information-theoretic security. They presented a secure one-time digital signature scheme for signing classical messages, based on Lamport's classical scheme [3].

In a public-key framework, Alice chooses a random private key, creates copies of the corresponding public key via some publicly-known algorithm, and distributes the copies in an authenticated fashion to all potential "Bobs". In principle, this asymmetric setup allows, e.g., any Bob to send encrypted messages to Alice or to verify any signature for a message that Alice digitally signed. By eliminating the need for each Alice-Bob pair to establish a secret key (in large networks where there may be many "Alices" and "Bobs"), the framework vastly simplifies key distribution, which is often the most costly part of any cryptosystem, compared to a framework that uses only symmetric keys.

D. Bacon et al. (Eds.): TQC 2011, LNCS 6745, pp. 121–142, 2014.
DOI: 10.1007/978-3-642-54429-3_8,

Some remarks about the quantum-public-key framework are in order. First, we address the issue of *purity* of the quantum public keys. In principle, the quantum public key can be either in a pure or mixed state from Alice's point of view (a mixed state is a fixed probabilistic distribution of pure states). Gottesman and Chuang [2] assumed pure-state public keys. For digital signature schemes, this purity is crucial; for, otherwise, Alice could cheat by sending different public keys to different "Bobs". Purity prevents Alice's cheating in this case because different "Bobs" can compare their copies of the public key via a "distributed SWAP-test" [2] to check they are the same (with high probability), much like can be done in the case of classical public keys. But any scheme can benefit from an equality test, since an adversary who tries to substitute bad keys for legitimate ones could thus be caught. There is no known equality test guaranteed to recognize when two mixed states are equal. Thus, having mixed-state public keys seems to be at odds with what it means to be "public", i.e., publicly verifiable.[1] Even though the scheme we present in this paper does not make explicit use of the "distributed SWAP-test" (because we assume the public keys have been securely distributed), it can do so in principle. We view this as analogous to how modern public-key protocols do not specify use of an equality test among unsure "Bobs", but how such a test is supported by the framework to help thwart attempts to distribute fake keys.

Second, we address the issue of *usability* of quantum-public-key systems. The states of two quantum public keys corresponding to two different private keys always have overlap less than $(1-\delta)$, for some positive and publicly known δ. Thus, a striking aspect of the quantum-public-key framework is that the number of copies of the public key in circulation must be limited (if we want information-theoretic security). If this were not the case, then an adversary could collect an arbitrarily large number of copies, measure them all, and determine the private key. By adjusting protocol parameters, this limit on the number of copies of the quantum public key can be increased in order to accommodate more users (or uses; see next paragraph for a discussion on "reusability"). Thus, in practice, there is no restriction on the usability of a quantum-public-key system as long as an accurate estimate can be made of the maximum number of users/uses.

Presumably, adjusting the protocol parameters (as discussed above) in order to increase the maximum number of copies of the quantum public key in circulation would result in a less efficient protocol instance, and this is one kind of tradeoff between efficiency and usability in the quantum-public-key setting. Another kind concerns *reusability.* The abovementioned digital signature scheme is "one-time" because only one message may be signed under a particular key-value (even though many different users can verify that one signature). If a second message needs to be signed, the signer must choose a new private key and then distribute corresponding new public keys. One open problem is thus whether there exist reusable digital signature schemes, where either the same

[1] Other authors have defined the framework to include mixed public keys, and Ref. [4] proposes an encryption scheme with mixed public keys that is reusable and unconditionally secure [5].

copy of the public key can be used to verify many different message-signature pairs securely, or where just the same key-values can be used to verify many different message-signature pairs securely (but a fresh copy of the public key is needed for each verification). The latter notion of "reusability" is what we adopt here.

In this paper, we consider an identification scheme, which, like a digital signature scheme, is a type of authentication scheme. Authentication schemes seek to ensure the *integrity* of information, rather than its privacy. While digital signature schemes ensure the integrity of origin of messages, identification schemes ensure the integrity of origin of communication *in real time* [1]. Identification protocols are said to ensure "aliveness"—that the entity proving its identity is active at the time the protocol is executed; we describe them in more detail in the next section.

We prove that an identification scheme based on the one in Ref. [6] is secure against a computationally-unbounded adversary (only restricted by finite cheating strategies), demonstrating for the first time that unconditionally-secure and reusable public-key authentication is possible in principle. We regard our result more as a proof of concept than a (potentially) practical scheme. Still, we are confident that an extension of the techniques used here may lead to more efficient protocols.

We now proceed with a description of the protocol (Sect. 2) and the security proof (Sect. 3).

2 Identification Protocol

In the following, Alice and Bob are always assumed to be honest players and Eve is always assumed to be the adversary. Suppose Alice generates a private key and authentically distributes copies of the corresponding public key to any potential users of the scheme, including Bob.

Here is a description (adapted from Sect. 4.7.5.1 in Ref. [7]) of how a secure public-key identification scheme works. When Alice wants to identify herself to Bob (i.e. prove that it is she with whom he is communicating), she invokes the identification protocol by first telling Bob that she is Alice, so that Bob knows he should use the public key corresponding to Alice. The ensuing protocol has the property that the *prover* Alice can convince the *verifier* Bob (except, possibly, with negligible probability) that she is indeed Alice, but an adversary Eve cannot fool Bob (except with negligible probability) into thinking that she is Alice, even after having listened in on the protocol between Alice and Bob or having participated as a (devious) verifier in the protocol with Alice several times. Public-key identification schemes are used in smart-card systems (e.g., inside an automated teller machine (ATM) for access to a bank account, or beside a doorway for access to a building); the smart card "proves" its identity to the card reader.[2]

[2] Note that it is not a user's personal identification number (PIN) that functions as the prover's private key; the PIN only serves to authenticate the user to the smart card (not the smart card to the card reader).

Note that no identification protocol is secure against an attack where Eve concurrently acts as a verifier with Alice and as a prover with Bob (but note also that, in such a case, the "aliveness" property is still guaranteed). Note also that, by our definition of "reusable," an identification scheme is considered reusable if Alice can prove her identity many times using the same key-values but the verifier needs a fresh copy of the public key for each instance of the protocol.

Note also that public-key identification can be trivially achieved via a digital signature scheme (Alice signs a random message presented by Bob), but we do not know of an unconditionally-secure and reusable digital signature scheme.[3] Similarly, public-key identification can be achieved with a public-key encryption scheme (Bob sends an encrypted random challenge to Alice, who returns it decrypted), but we do not know of an unconditionally-secure and reusable public-key encryption scheme (that uses pure-state public keys; though, see Ref. [9] for a promising candidate).

2.1 Protocol Specification

The identification protocol takes the form of a typical "challenge-response" interactive proof system, consisting of a kernel (or subprotocol) that is repeated several times in order to amplify the security, i.e., reduce the probability that Eve can break the protocol. The following protocol is a simplification of the original protocol from Ref. [6] (but our security proof applies to both protocols, with only minor adjustments). We assume all quantum channels are perfect.

Parameters

- The *security* parameter $s \in \mathbf{Z}^+$
  - $\diamond$ equals the number of kernel iterations.
  - $\diamond$ The probability that Eve can break the protocol is exponentially small in s.
- The *reusability* parameter $r \in \mathbf{Z}^+$
  - $\diamond$ equals the maximum number of copies of the quantum public key in circulation and
  - $\diamond$ equals the maximum number of times the protocol may be executed by Alice, before she needs to pick a new private key.

Keys

- The *private key* is

$$(x_1, x_2, \ldots, x_s), \tag{1}$$

  where Alice chooses each x_j, $j = 1, 2, \ldots, s$, independently and uniformly randomly from $\{1, 2, \ldots, 2r+1\}$.
  - $\diamond$ The value x_j is used only in the jth kernel-iteration.

[3] Pseudo-signature schemes, such as the one in Ref. [8], are information-theoretically secure but assume broadcast channels.

- One copy of the *public key* is an s-partite system in the state

$$\otimes_{j=1}^{s} |\psi_{x_j}\rangle, \tag{2}$$

where (omitting normalization factors)

$$|\psi_{x_j}\rangle := |0\rangle + e^{2\pi i x_j/(2r+1)}|1\rangle. \tag{3}$$

  - $\diamond$ Alice authentically distributes (e.g. via trusted courier) at most r copies of the public key.
  - $\diamond$ The jth subsystem of the public key (which is in the state $|\psi_{x_j}\rangle$) is only used in the jth kernel-iteration.

Actions

- The *kernel* $\mathcal{K}(x)$ of the protocol is the following three steps, where we use the shorthand

$$\phi_x := 2\pi x/(r+1), \tag{4}$$

and where we have dropped the subscript "j" from "x_j":
  - (1) Bob secretly chooses a uniformly random bit b and transforms the state of his authentic copy of $|\psi_x\rangle$ into $|0\rangle + (-1)^b e^{i\phi_x}|1\rangle$. Bob sends this qubit to Alice.
  - (2) Alice performs the phase shift $|1\rangle \mapsto e^{-i\phi_x}|1\rangle$ on the received qubit and then measures the qubit in the basis $\{|0\rangle \pm |1\rangle\}$ (in order to determine Bob's secret b above). If Alice gets the outcome corresponding to "+", she sends 0 to Bob; otherwise, Alice sends 1.
  - (3) Bob receives Alice's bit as b' and tests whether b' equals b.
- When Alice wants to identify herself to Bob, they take the following actions:
  - (i) Alice checks that she has not yet engaged in the protocol r times before with the current value of the private key; if she has, she aborts (and refreshes the private and public keys).
  - (ii) Alice sends Bob her purported identity ("Alice"), so that Bob may retrieve the public keys corresponding to Alice.
  - (iii) The kernel $\mathcal{K}(x)$ is repeated s times, for $x = x_1, x_2, \ldots, x_s$. Bob "accepts" if he found that b' equaled b in all the kernel iterations; otherwise, Bob "rejects".

2.2 Completeness of the Protocol

It is clear that the protocol is correct for honest players: Bob always "accepts" when Alice is the prover. In the Appendix ("Sect. 3"), we prove that the protocol is also secure against any adversary (only restricted by finite cheating strategies): given r and $\epsilon > 0$, there exists a value of $s = s(r, \epsilon)$ such that Bob "accepts" with probability at most ϵ when Eve is the prover.

3 Security

Let us clearly define what Eve is allowed to do in our attack model. Eve can

- passively monitor Alice's and Bob's interactions (which means that Eve can read the classical bits sent by Alice, and read the bit that indicates whether Bob "accepts" or "rejects"), and
- participate as the verifier in one or more complete instances of the protocol, and
- participate as the prover, impersonating Alice, in one or more complete instances of the protocol.

Eve is assumed not to be able to actively interfere with Alice's and Bob's communications during the protocol, as this would allow Eve to concurrently act as verifier with Alice and as prover with Bob (thus trivially breaking any such scheme[4]).

Evidently, Eve's passive monitoring only gives her independent and random bits (and the bit corresponding to "accept"), thus giving her no useful information (in that she may as well generate random bits herself). So, we can ignore the effects of her passive monitoring.

With regard to Eve acting as verifier, we will give Eve potentially more power by assuming that Alice, instead of performing both the phase shift and the measurement in Step 2 of the kernel $\mathcal{K}(x)$, only performs the phase shift (Eve could perform Alice's measurement herself, if she desired). Furthermore, we will assume that the phase shift Alice performs is

$$u_{\phi_x} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi_x} \end{bmatrix} . \tag{5}$$

Even though Alice actually performs the inverse phase shift $u_{-\phi_x}$, note that the two phase shifts are equivalent in the sense that $Zu_{\phi_x}Z$ equals $u_{-\phi_x}$ up to global phase, where

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} . \tag{6}$$

Thus the protocol is unchanged had we assumed that Alice, instead of performing $u_{-\phi_x}$ in Step 2 of the kernel $\mathcal{K}(x)$, performs $Zu_{\phi_x}Z$. Since Eve can perform

[4] For password-based identification in a symmetric-key model, as in Ref. [10], where both Alice and Bob know something that Eve does not (i.e. the password), one can define a nontrivial "man-in-the-middle" attack, where Eve's goal is to learn the password in order to impersonate Alice in a later instance of the protocol. However, in public-key identification, Eve's goal of learning the private key may, without loss of generality, be accomplished by participating as a dishonest verifier and by obtaining copies of the public key, since Bob does not perform any action that Eve cannot perform herself given a copy of the public key.

Z gates on her qubit immediately before and after she gives it to Alice, our assumption indeed gives Eve at least as much power to cheat. Thus, Eve can effectively extract up to r black boxes for u_{ϕ_x} from Alice (recall Alice only participates in the protocol r times before refreshing her keys).

We will also give Eve potentially more power by giving her a black box for u_{ϕ_x} in place of every copy of $|\psi_x\rangle$ that she obtained legitimately. For each $x \in \{x_1, x_2 \ldots, x_s\}$, let t be the total number of black boxes for u_{ϕ_x} that Eve has in her possession; that is, for simplicity, and without loss of generality, we assume she has the same number of black boxes u_{ϕ_x} for each value of x. Note that $t \leq (2r-1)$, since we always assume that at least one copy of the public key is left for Bob, so that Eve can carry out the protocol with him.

Therefore, to prove security in our setting, it suffices to consider attacks where Eve first uses her st black boxes to create a reference system in some $(\phi_{x_1}, \phi_{x_2}, \ldots, \phi_{x_s})$-dependent state, denoted $|\Psi_R(\phi_{x_1}, \phi_{x_2}, \ldots, \phi_{x_s})\rangle$, and then she uses this system while she participates as a prover, impersonating Alice, in one or many instances of the protocol in order to try to cause Bob to "accept". We use the following definition of "security":

Definition 1 (Security). *An identification protocol (for honest prover Alice and honest verifier Bob) is* secure with error ϵ *if the probability that Bob "accepts" when any adversary Eve participates in the protocol as a prover is less than ϵ.*

The only assumption we make on Eve is that her cheating strategy is finite in the sense that her quantum computations are restricted to a finite-dimensional complex vector space; the dimension itself, though, is unbounded.

We will assume that Eve has always extracted the r black boxes for u_{ϕ_x} from Alice (for all $x = x_1, x_2, \ldots, x_s$), and we define t' to be the number black boxes that Eve obtained legitimately (via copies of the public key):

$$t = r + t'. \tag{7}$$

Note that Eve can make at most $(r - t')$ attempts at fooling Bob, i.e., causing Bob to "accept". Let $E(a, b)$ denote the event that Eve fools Bob on her ath attempt using b black boxes for u_{ϕ_x} for all $x = x_1, x_2, \ldots, x_s$. Most of the argument, beginning in Sect. 3.1, is devoted to showing that

$$\Pr[E(1, t)] \leq (1 - c/(t+2)^2)^s, \tag{8}$$

for some positive constant c defined at the end of Sect. 3. In general, Eve learns something from one attempt to the next; however, because Eve can simulate her interaction with Bob at the cost of using one copy of $|\psi_x\rangle$ per simulated iteration of $\mathcal{K}(x)$, we have, for $\ell = 2, 3, \ldots, (r - t')$,

$$\Pr[E(\ell, t)] \leq \Pr[E(1, t + \ell - 1)]. \tag{9}$$

Given this, we use the union bound:

$$
\begin{aligned}
&\Pr[\text{Eve fools Bob at least once, using } t \text{ black boxes for } u_{\phi_x}, \forall x] && (10)\\
&\leq \sum_{\ell=1}^{r-t'} \Pr[E(\ell,t)] && (11)\\
&\leq \sum_{\ell=1}^{r-t'} \Pr[E(1,t+\ell-1] && (12)\\
&\leq \sum_{\ell=1}^{r-t'} (1-c/(t+\ell+1)^2)^s && (13)\\
&\leq (r-t')(1-c/(2r+1)^2)^s, && (14)
\end{aligned}
$$

since $t+\ell \leq 2r$. It follows that the probability that Eve can fool Bob at least once, that is, break the protocol, is

$$P_{\text{break}} \leq r(1-c/(2r+1)^2)^s, \tag{15}$$

which, for fixed r, is exponentially small in s. Note that this bound is likely not tight, since it ultimately assumes that all of Eve's attempts are equally as powerful. In particular, this bound assumes that Eve's state $|\Psi_R(\phi_{x_1}, \phi_{x_2}, \ldots, \phi_{x_s})\rangle$ does not degrade with use. A more detailed analysis using results about degradation of quantum reference frames [11] may be possible.

From Eq. (15) follows our main theorem (see Appendix A.3 for the proof):

Theorem 1 (Security of the protocol). *For any $\epsilon > 0$ and any $r \in \mathbf{Z}^+$, the identification protocol specified in Sect. 2.1 is secure with error ϵ according to Definition 1 if*

$$s > (2r+1)^2 \log(r/\epsilon)/c, \tag{16}$$

for some positive constant c.

The theorem shows how the efficiency of the protocol scales with its reusability: it suffices to have

$$s \in O(r^2 \log(r/\epsilon)). \tag{17}$$

The remainder of the paper establishes the bound in Line (8).

3.1 Sufficiency of Individual Attacks

At each iteration, we may assume Eve performs some measurement, in order to get an answer to send back to Bob. Generally, Eve can mount a coherent attack, whereby her actions during iteration j may involve systems that she used or will use in previous or future iterations as well as systems created using black boxes for $u_{\phi_{x_k}}$ for any k—not just for $k = j$. Since each x_j is *independently* selected from the set $\{1, 2, \ldots, 2r + 1\}$, intuition suggests that Eve's measurement at iteration j may be assumed to be independent of her measurement at any other iteration and in particular does not need to involve any black boxes other than ones for $u_{\phi_{x_j}}$. In other words, it seems plausible that the optimal strategy for Eve can consist of the "product" of identical optimal strategies for each iteration individually. This intuition can indeed be shown to be correct by combining a technique from Ref. [12], for expressing the maximum output probability in a multiple-round quantum interactive protocol as a semidefinite program, with a result in Ref. [13], which implies that the semidefinite program satisfies the product rule that we need; see Appendix A.1 for a proof.

The remainder of Sect. 3 establishes the following proposition:

Proposition 2. *The probability that Eve guesses correctly in any particular iteration j, using t black boxes for $u_{\phi_{x_j}}$, is at most $(1 - c/(t+2)^2)$ for some positive constant c.*

Assuming Proposition 2, the result proved in Appendix A.1 implies that the probability of Eve's guessing correctly in all s iterations, using t black boxes for u_{ϕ_x}, for $x = x_1, x_2, \ldots, x_s$, is at most $(1 - c/(t + 2)^2)^s$, establishing the bound in Line (8).

3.2 Equivalence of Discrete and Continuous Private Phases

To help us prove Proposition 2, we now show that, from Bob's and Eve's points of view, Alice's choosing the private phase angle ϕ_x from the discrete set $\{2\pi x/(2r+1) : x = 1, 2, \ldots, 2r + 1\}$ is equivalent to her choosing the phase angle from the continuous interval $[0, 2\pi)$. We have argued that the only information that Eve or Bob—or anyone but Alice—has about ϕ_x may be assumed to come from a number of black boxes for u_{ϕ_x} that can be no greater than $2r$ (there are r legitimate copies of the public key, and one can extract r more black boxes from Alice); let this number be d, where $1 \leq d \leq 2r$.

In order to access the information from the black boxes, they must, in general, be used in a quantum circuit in order to create some state. Using the d black boxes, the most general (purified) state that can be made is without loss of generality of the form

$$|\psi(\phi_x)\rangle = \sum_{k=0}^{N-1} \left(\sum_{j=0}^{d} \beta_{j,k} e^{ij\phi_x} \right) |a_k\rangle, \tag{18}$$

where $\{|a_k\rangle : k = 0, 1, ..., N - 1\}$ is an orthonormal basis of arbitrary but finite size (the assumption of finite N comes from our restricting Eve to using only finite cheating strategies). In general, the numbers N and $\beta_{j,k}$ may depend on d. Here we have followed Ref. [14] by noting that each amplitude is a polynomial in $e^{i\phi_x}$ of degree at most d; this fact follows from an inductive proof just as in Ref. [15], where the polynomial method is applied to an oracle revealing one of many Boolean variables.

Averaging over Alice's random choices of x, one would describe the previous state by the density operator

$$\frac{1}{2r+1}\sum_{x=1}^{2r+1}|\psi(\phi_x)\rangle\langle\psi(\phi_x)|, \tag{19}$$

since x is chosen uniformly randomly from $\{1,2,\ldots,2r+1\}$. Had ϕ_x been chosen uniformly from $\{2\pi x/(2r+1) : x\in[0,2r+1)\}=[0,2\pi)$, one would describe the state by

$$\int_0^{2\pi}\frac{d\phi}{2\pi}|\psi(\phi)\rangle\langle\psi(\phi)|. \tag{20}$$

It is straightforward to show[5] that the above two density operators are both equal to

$$\sum_{k,k'=0}^{N-1}\sum_{j=0}^{d}\beta_{j,k}\beta^*_{j,k'}|a_k\rangle\langle a_{k'}|. \tag{23}$$

Thus, without loss of generality, we may drop the subscript "x" on "ϕ_x", write "ϕ" for Alice's private phase angle, and assume she did (somehow) choose ϕ uniformly randomly from $[0,2\pi)$.[6] We are now ready to prove Proposition 2.

3.3 Bound on Relative Phase Shift Estimation

Eve's task of cheating in one iteration of the kernel may be phrased as follows. Eve is to decide the difference between the relative phases encoded in two subsystems R and S, where S is a given one-qubit system and R is under her control. The given subsystem S is in the state

$$|\psi_S(\phi,\theta)\rangle=|0\rangle+e^{i(\phi+\theta)}|1\rangle, \tag{24}$$

[5] This requires the following two facts: (1) for any integer a,

$$\frac{1}{2\pi}\int_0^{2\pi}e^{ia\theta}d\theta=\begin{cases}0 & \text{if } a\neq 0\ ,\\ 1 & \text{otherwise}\ ;\end{cases} \tag{21}$$

and (2) for any integer $p\geq 2$ and integer a:

$$\frac{1}{p}\sum_{k=1}^{p}e^{2\pi iak/p}=\begin{cases}0 & \text{if } a \text{ is not a multiple of } p,\\ 1 & \text{otherwise}\ ,\end{cases} \tag{22}$$

where the second fact is applied at $p=2r+1$.

[6] One way to interpret this result is that even if Alice encodes infinitely many bits into ϕ, it is no better than if she encoded $\lceil\log_2(2r+1)\rceil$ bits. Note that if Eve performs an optimal phase estimation [16] in order to learn ϕ and then cheat Bob, she can only learn at most $\lfloor\log_2(2r-1)\rfloor$ bits of ϕ (here, we assume Eve has $2r-1$ copies of the public key, having left Bob one copy), whereas Alice actually encoded $\lceil\log_2(2r+1)\rceil$ bits into ϕ.

where θ is unknown and uniformly random in $\{0, \pi\}$, and ϕ is unknown and uniformly random in $[0, 2\pi]$. Eve can make the state $|\psi_R(\phi)\rangle$ of subsystem R by using arbitrary operations interleaved with at most t black boxes for the one-qubit gate u_ϕ. Note that the problem is nontrivial because ϕ is unknown and uniformly random and the qubit S is given to Eve *after* she has used all her black boxes. We seek the optimal success probability for Eve to guess θ correctly.

Eve's estimation problem can be treated within the framework of quantum estimation of group transformations [17]. As such, we regard her problem as finding the optimal measurement (probability) to correctly distinguish the states in the two-element orbit

$$\{V_\theta \rho V_\theta^\dagger : \theta \in \{0, \pi\}\}, \tag{25}$$

where $V_\theta = I_R \otimes (|0\rangle\langle 0| + e^{i\theta}|1\rangle\langle 1|)$ and

$$\rho = \int \frac{d\phi}{2\pi} |\psi_R(\phi)\rangle\langle\psi_R(\phi)| \otimes |\psi_S(\phi, 0)\rangle\langle\psi_S(\phi, 0)|. \tag{26}$$

The probabilities of her estimation procedure can be assumed to be generated by a POVM $\{E_0, E_\pi\}$. In general, it is known how to solve for the POVM that performs optimally on average when the unitarily-generated orbit consists of pure states, but not when the orbit is generated from a mixed state (ρ, in our case). Thus, we now effectively reduce the problem to several instances of an estimation problem where the orbit is pure.

Indeed, suppose that $|\psi_R(\phi)\rangle$ were a state on q qubits that satisfied the property

$$|\psi_R(\phi)\rangle\langle\psi_R(\phi)| = (u_\phi)^{\otimes q} |\psi_R(0)\rangle\langle\psi_R(0)| (u_\phi^\dagger)^{\otimes q} \tag{27}$$

for all $\phi \in [0, 2\pi]$. Then, letting $U_\phi \equiv (u_\phi)^{\otimes(q+1)}$ and $|\psi_{RS}(\phi, \theta)\rangle \equiv |\psi_R(\phi)\rangle|\psi_S(\phi, \theta)\rangle$, we would have that

$$\rho = \int \frac{d\phi}{2\pi} U_\phi |\psi_{RS}(0,0)\rangle\langle\psi_{RS}(0,0)| U_\phi^\dagger \tag{28}$$

$$= \sum_w P_w |\psi_{RS}(0,0)\rangle\langle\psi_{RS}(0,0)| P_w \tag{29}$$

$$= \sum_w P_w \rho P_w, \tag{30}$$

where P_w is the projection onto the subspace of Hamming weight $w = 0, 1, \ldots, q+1$, and we used the formulas $U_\phi = \sum_w P_w e^{iw\phi}$ and $\delta_{w,0} = \int (d\phi/2\pi) e^{iw\phi}$. In other words, the state ρ would be block diagonal with respect to the direct-sum decomposition of the total state space of R into subspaces of constant Hamming weight w. Then we would have that the probability that Eve guesses $\theta = \theta'$ given that $\theta = \theta''$ is

$$\Pr[\text{Eve guesses } \theta = \theta' | \theta = \theta''] = \mathrm{Tr}\left[E_{\theta'}\left(V_{\theta''}\rho V_{\theta''}^{\dagger}\right)\right] \quad (31)$$

$$= \mathrm{Tr}\left[E_{\theta'}V_{\theta''}\sum_{w} P_w \rho P_w V_{\theta''}^{\dagger}\right] \quad (32)$$

$$= \mathrm{Tr}\left[\left(\bigoplus_{w} E_{w,\theta'}\right)\left(V_{\theta''}\rho V_{\theta''}^{\dagger}\right)\right], \quad (33)$$

where $E_{w,\theta'} \equiv P_w E_{\theta'} P_w$, and we used cyclicity of trace and the fact that V_θ and P_w commute. Thus, the elements of Eve's POVM $\{E_0, E_\pi\}$ would without loss of generality have the same block diagonal structure as ρ. In principle, this would allow Eve to measure first (just) the Hamming weight of ρ in order to find w, and then deal with the group transformation estimation problem with respect to the pure orbit

$$\mathcal{O}_w \equiv \{V_\theta|\Psi_w\rangle : \theta \in \{0, \pi\}\}, \quad (34)$$

where $|\Psi_w\rangle$ is the state such that $|\Psi_w\rangle \propto P_w|\psi_{RS}(0,0)\rangle$; we note that $|\Psi_w\rangle$ is independent of ϕ (and θ). The following lemma shows that, without loss of generality, we may assume that the situation just described is indeed the case:

Lemma 1. *Without loss of generality, Eve's state $|\psi_R(\phi)\rangle$, which she prepares with at most t black boxes for u_ϕ, may be assumed to be on $q = (2t+1)$ qubits and satisfy*

$$|\psi_R(\phi)\rangle\langle\psi_R(\phi)| = (u_\phi)^{\otimes q}|\psi_R(0)\rangle\langle\psi_R(0)|(u_\phi^{\dagger})^{\otimes q} \quad (35)$$

for all $\phi \in [0, 2\pi]$.

Proof. As noted in the previous section, using the t black boxes, the most general (purified) state of R that Eve can make is without loss of generality

$$\sum_{k=0}^{N-1}\left(\sum_{j=0}^{t}\beta_{j,k}e^{ij\phi}\right)|a_k\rangle_R, \quad (36)$$

where, again, N is a priori unknown but finite (we use subscripts on the kets in this proof to indicate the physical systems). Note that we can rewrite the state in Eq. (36) by changing the order of the summations as

$$\sum_{j=0}^{t}\beta_j e^{ij\phi}|\tilde{g}_j\rangle_R, \quad (37)$$

where we have defined the numbers β_j and the not-necessarily-orthogonal set of unit vectors $\{|\tilde{g}_j\rangle : j = 0, 1, ..., t\}$ such that

$$\beta_j|\tilde{g}_j\rangle_R = \sum_{k=0}^{N-1}\beta_{j,k}|a_k\rangle_R. \quad (38)$$

Using the Gram-Schmidt orthonormalization procedure on $\{|\tilde{g}_j\rangle\}_j$ to get the orthonormal set $\{|g_j\rangle\}_j$, we can write

$$|\tilde{g}_j\rangle_R = \sum_{h=0}^{t} \gamma_{j,h} |g_h\rangle_R. \tag{39}$$

Introduce a new system R' consisting entirely of qubits and define U to be any unitary map acting on $R \otimes R'$ that takes $|0\rangle_R |c_h\rangle_{R'} \mapsto |g_h\rangle_R |0\rangle_{R'}$, where $\{|c_h\rangle_{R'}\}_{h=0,1,\ldots,t}$ is an orthonormal set of size $t+1$ with elements that are computational basis states whose labels have constant Hamming weight; note that R' needs only $O(\log(t+1))$ qubits whereas R is of unknown (but finite) size (however, following this proof, we will construct R' using $t+1$ qubits, as this makes things simpler). We first claim that, without loss of generality,

$$|\psi_R(\phi)\rangle = \sum_{j,h} \beta_j \gamma_{j,h} e^{ij\phi} |S_j^t\rangle_A |c_h\rangle_{R'}, \tag{40}$$

where A is a t-qubit ancilla, and $|S_j^t\rangle_A$ is the symmetric state of weight j. To see this, note that Eve's optimal measurement can include the following preprocessing operations (in sequence), so that she recovers the most general state in Eq. (36) (and Eq. (37)) on R but for a different random value of ϕ:

– add an ancillary register R in state $|0\rangle_R$ in between the two registers A and R' and perform U on $R \otimes R'$ to get (after throwing out system R')

$$\sum_j \beta_j \sum_h \gamma_{j,h} e^{ij\phi} |S_j^t\rangle_A |g_h\rangle_R = \sum_j \beta_j e^{ij\phi} |S_j^t\rangle_A |\tilde{g}_j\rangle_R \tag{41}$$

– on A, do the $(t+1)$-dimensional inverse quantum Fourier transform in the symmetric basis on A, i.e. mapping

$$|S_j^t\rangle_A \mapsto \frac{1}{\sqrt{t+1}} \sum_y e^{-i2\pi yj/(t+1)} |S_y^t\rangle_A, \tag{42}$$

to get

$$\sum_j \sum_y \beta_j e^{ij(\phi - 2\pi y/(t+1))} |S_y^t\rangle_A |\tilde{g}_j\rangle_R \tag{43}$$

and measure the Hamming weight of A to get result y_0, which leaves the state (after throwing out system A)

$$\sum_j \beta_j e^{ij(\phi - 2\pi y_0/(t+1))} |\tilde{g}_j\rangle_R \tag{44}$$

– correct the relative phase on qubit S by $2\pi y_0/(t+1)$.

Doing these operations does not change the estimation problem, since ϕ is uniformly random anyway; these operations just change the unknown ϕ to $\phi' = \phi - 2\pi y_0/(t+1)$.

Finally, note that Eq. (40) implies that $|\psi_R(\phi)\rangle$ can be made from $|\psi_R(0)\rangle$ with at most t black boxes for u_ϕ, by applying $(u_\phi)^{\otimes t}$ on the t qubits of system A, and note that $|\psi_R(\phi)\rangle$ satisfies Eq. (27), since the states $|c_h\rangle$ are of constant Hamming weight.

Remark 1. (Quantum Fourier transform as analytical tool) Note that Eve's optimal strategy is not necessarily to measure R to get an estimate ϕ' of ϕ first, then apply $u_{-\phi'}$ on S, and then measure S to estimate θ. However, the operation that is optimal for estimating ϕ (see Ref. [14]), i.e. the inverse quantum Fourier transform applied above, is still useful as an analytical tool in order to derive (a convenient form of) an optimal state for her estimation of θ.

Thus, by Lemma 1, we assume Eq. (40) holds, which allows us to derive the following proposition. For convenience, we define

$$\alpha_{j,h} \equiv \beta_j \gamma_{j,h}. \tag{45}$$

Proposition 3. *The elements of the POVM* $\{E_0, E_\pi\}$ *are without loss of generality defined as*

$$E_0 = |\Xi_0\rangle|0\rangle\langle\Xi_0|\langle 0| + \sum_{w=2}^{t+1} |w,+\rangle\langle w,+| \tag{46}$$

$$E_\pi = \sum_{w=2}^{t+1} |w,-\rangle\langle w,-| + |\Xi_t\rangle|1\rangle\langle\Xi_t|\langle 1|, \tag{47}$$

where

$$|w,\pm\rangle \equiv \frac{1}{\sqrt{2}}(|\Xi_{w-1}\rangle|0\rangle \pm |\Xi_{w-2}\rangle|1\rangle), \tag{48}$$

and $|\Xi_{w-1}\rangle$ *and* $|\Xi_{w-2}\rangle$ *are states such that, for* $j = 0, 1, \ldots, t$,

$$|\Xi_j\rangle \propto \sum_h \frac{\alpha_{j,h}}{\sqrt{2}} |S_j^t\rangle|c_h\rangle. \tag{49}$$

The proof of Proposition 3 is similar to the argument given in Ref. [11] and is given in Appendix A.2 . The total success probability of Eve's strategy can now be computed as

$$\sum_{\theta'\in\{0,\pi\}} \Pr[\text{Eve guesses } \theta = \theta' | \theta = \theta'] \Pr[\theta = \theta'] \tag{50}$$

$$= \frac{1}{2} \sum_{\theta'\in\{0,\pi\}} \mathrm{Tr}(E_{\theta'} V_{\theta'} \rho V_{\theta'}^\dagger) \tag{51}$$

$$= \frac{1}{2} \sum_{\theta'\in\{0,\pi\}} \mathrm{Tr}(E_{\theta'} V_{\theta'} |\psi_{RS}(0,0)\rangle\langle\psi_{RS}(0,0)| V_{\theta'}^\dagger) \tag{52}$$

$$= \frac{1}{2} + \frac{1}{4}\langle\psi_R(0)|M_t|\psi_R(0)\rangle, \tag{53}$$

where

$$M_t \equiv \sum_{j=0}^{t-1} |\Xi_{j+1}\rangle\langle\Xi_j| + |\Xi_j\rangle\langle\Xi_{j+1}|. \tag{54}$$

As a last task, we now seek the value of $|\psi_R(0)\rangle$—i.e. the values of $\alpha_{j,h}$—such that $\langle\psi_R(0)|M_t|\psi_R(0)\rangle$ is maximal. The proof of the following proposition is in Appendix A.4:

Proposition 4. *The state* $|\psi_R(0)\rangle \propto \sum_{j=0}^{t} \sin\left[\frac{(j+1)\pi}{t+2}\right] |\Xi_j\rangle$ *achieves the maximum value in Eq. (53).*

Thus (as in Ref. [11]—see Appendix A.4), we get a maximal success probability of

$$\frac{1}{2} + \frac{1}{2}\cos(\pi/(t+2)) \tag{55}$$

$$\leq \frac{1}{2} + \frac{1}{2}\left(1 - \frac{(\pi/(t+2))^2}{2!} + \frac{(\pi/(t+2))^4}{4!}\right) \tag{56}$$

$$= 1 - \frac{\pi^2}{4}\frac{1}{(t+2)^2} + \frac{\pi^4}{48}\frac{1}{(t+2)^4} \tag{57}$$

$$\leq 1 - \left(\frac{\pi^2}{4} - \frac{\pi^4}{48}\right)\frac{1}{(t+2)^2} \tag{58}$$

$$= 1 - c/(t+2)^2, \tag{59}$$

for the constant $c = (\pi^2/4 - \pi^4/48) \doteq 0.438$ and all $t \geq 1$. This completes the proof of Proposition 2 and thus the proof of Theorem 1.

A Appendices

A.1 Proof of Sufficiency of Individual Attacks

Consider the following non-cryptographic, $(t+1)$-round interactive protocol (or game) between Evelyn and Bobby (neither of whom is considered adversarial, hence we distinguish these two players from Eve and Bob), denoted $\mathcal{L} = \mathcal{L}(\Phi)$, where

$$\Phi = (\Phi_1, \Phi_2, \ldots, \Phi_{t+1}) \tag{60}$$

and the Φ_i are quantum operations (super-operators) that specify Evelyn's actions in the game (the quantities r and t are as defined previously):

- (1′) Bobby chooses a uniformly random $x \in \{1, 2, \ldots, 2r+1\}$ and sends a qubit in the state $|0\rangle$ to Evelyn (who can ignore this qubit—it carries no significant information).
- (2′) For $i = 1, 2, \ldots, t$ {
    - ◇ Evelyn performs the quantum operation Φ_i on her system, and then sends one qubit to Bobby.

$\diamond$ Bobby performs the unitary gate u_{ϕ_x} on the qubit received from Evelyn and sends it back to Evelyn.}

- (3′) Bobby chooses a uniformly random $b \in \{0,1\}$ and sends a qubit in the state $|0\rangle + (-1)^b e^{i\phi_x}|1\rangle$ to Evelyn.
- (4′) Evelyn performs the quantum operation Φ_{t+1} on her system, and then sends one qubit to Bobby.
- (5′) Bobby measures the received qubit in the computational basis $\{|0\rangle, |1\rangle\}$, getting outcome 0 or 1 (corresponding to $|0\rangle$ and $|1\rangle$ respectively); he tests whether this outcome equals b.

The following proposition is straightforward to prove:

Proposition 5. *The probability that Eve, using t black boxes $u_{\phi_{x_j}}$, causes Bob's equality test to pass in a particular iteration j of the protocol in Sect. 2.1 is at most*

$$\alpha := \max_{\Phi} \Pr[\text{Bobby's equality test passes in } \mathcal{L}(\Phi)], \tag{61}$$

where Φ ranges over all $(t+1)$-tuples of admissible quantum operations that Evelyn can apply in the game $\mathcal{L}$.

Now consider the parallel s-fold repetition of $\mathcal{L}$, which we denote $\mathcal{L}^{\|s} = \mathcal{L}^{\|s}(\Phi')$, where now Φ' denotes Evelyn's quantum operation in $\mathcal{L}^{\|s}$. The following proposition is also straightforward to prove:

Proposition 6. *The probability that Eve fools Bob on the first attempt using t black boxes per x-value in the protocol in Sect. 2.1 is at most*

$$\alpha' := \max_{\Phi'} \Pr[\text{all of Bobby's equality tests pass in } \mathcal{L}^{\|s}(\Phi')], \tag{62}$$

where Φ' ranges over all $(t+1)$-tuples of admissible quantum operations that Evelyn can apply in the game $\mathcal{L}^{\|s}$.

Therefore, in order to prove that it is sufficient to consider individual (as opposed to coherent) attacks by Eve, it suffices to show that $\alpha' = \alpha^s$.

In Ref. [12], the above game is viewed as an interaction between a $(t+1)$-round *(non-measuring) strategy* and a *(compatible) measuring co-strategy*; Evelyn's operations Φ form the non-measuring strategy and Bobby's actions form the measuring co-strategy (technically, Steps (1′), (3′), and (4′) would have to be slightly modified in order to fit the co-strategy formalism: in Steps (1′) and (3′), Bobby should make his random choices in superposition and use the quantum registers storing these choices as a control register whenever requiring these random values subsequently; in Step (4′), Bobby should only make one final measurement whose outcome indicates whether the equality test passes; we assume that these modifications have been made).

For all i, let $\mathcal{X}_i$ and $\mathcal{Y}_i$ be the input and output spaces, respectively, of Evelyn's quantum operation Φ_i in $\mathcal{L}$, i.e. $\Phi_i : \mathrm{L}(\mathcal{X}_i) \to \mathrm{L}(\mathcal{Y}_i)$, where $\mathrm{L}(\mathcal{X}_i)$ is the space of all linear operators from the complex Euclidean space $\mathcal{X}_i$ to itself (and likewise for $\mathrm{L}(\mathcal{Y}_i)$). Let $\mathrm{Pos}(\mathcal{Y} \otimes \mathcal{X})$ denote the set of all positive semidefinite operators in $\mathrm{L}(\mathcal{Y} \otimes \mathcal{X})$, where $\mathcal{Y} = \mathcal{Y}_1 \otimes \mathcal{Y}_2 \otimes \cdots \otimes \mathcal{Y}_{t+1}$ (and similarly for $\mathcal{X}$). For any Euclidean space $\mathcal{Z}$, let $\mathbb{I}_{\mathcal{Z}}$ denote the identity operator $\mathcal{Z}$.

Reference [12] shows that Evelyn's strategy can be equivalently expressed by a single positive semidefinite operator in $\mathrm{Pos}(\mathcal{Y} \otimes \mathcal{X})$ while Bobby's measuring co-strategy can be expressed by the collection $\{B_0, B_1\}$ of two positive semidefinite operators in $\mathrm{Pos}(\mathcal{Y} \otimes \mathcal{X})$, where, without loss of generality, we assume that B_0 corresponds to the measurement outcome indicating that Bobby's test for equality in Step ($5'$) passes. We briefly note that these positive semidefinite operators are the Choi-Jamiołkowski representations of quantum operations corresponding to the players' actions. A more general version of the following theorem is proved in Ref. [12]:

Theorem 7 (Interaction output probabilities [12]). *For any non-measuring strategy $X \in \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{X})$ of Evelyn, the probability that Bobby's equality test passes is $Tr(B_0^\dagger X)$.*

Using Theorem 7, it is shown, in the proof of Theorem 3.3 of Ref. [12], that the maximal probability with which Bobby's measuring co-strategy can be forced to output the outcome corresponding to B_0 by some (compatible) strategy of Evelyn's can be expressed as a semidefinite (optimization) program (see Ref. [18] for a relevant review of semidefinite programming). Thus α and α' can be expressed, respectively, as solutions to the following semidefinite programs π_α and $\pi_{\alpha'}$:

$$\begin{array}{rl} & \underline{\pi_\alpha} \\ \text{maximize:} & \mathrm{Tr}(B_0^\dagger X) \\ \text{subject to:} & \mathrm{Tr}_{\mathcal{Y}}(X) = \mathbb{I}_{\mathcal{X}}, \\ & X \in \mathrm{Pos}(\mathcal{Y} \otimes \mathcal{X}) \end{array} \qquad \begin{array}{rl} & \underline{\pi_{\alpha'}} \\ \text{maximize:} & \mathrm{Tr}((B_0^{\otimes s})^\dagger X) \\ \text{subject to:} & \mathrm{Tr}_{\mathcal{Y}'}(X) = \mathbb{I}_{\mathcal{X}'}, \\ & X \in \mathrm{Pos}(\mathcal{Y}' \otimes \mathcal{X}'), \end{array}$$

where, for all i, $\mathcal{X}_i' = \mathcal{X}_i^{\otimes s}$ and $\mathcal{X}' = \mathcal{X}_1' \otimes \mathcal{X}_2' \otimes \cdots \otimes \mathcal{X}_{t+1}'$ (and similarly for $\mathcal{Y}_i'$ and $\mathcal{Y}'$). We note that the first constraint in each semidefinite program above codifies the property of trace-preservation for the quantum operation corresponding to X, while the second constraint codifies the property of complete positivity (see Ref. [18] for details). Furthermore, it is shown in Ref. [12] that such semidefinite programs (arising from interactions between strategies and compatible co-strategies) satisfy the condition of strong duality, which means that the solution to each semidefinite program above coincides with that of its dual.

In Ref. [13], the following theorem is proven:

Theorem 8 (Condition for product rule for semidefinite programs [13]). *Suppose that the following two semidefinite programs π_1 and π_2 satisfy strong duality:*

$$\begin{array}{rl} & \underline{\pi_1} \\ \textit{maximize:} & \mathrm{Tr}(J_1^\dagger W) \\ \textit{subject to:} & \Psi_1(W) = C_1, \\ & W \in \mathrm{Pos}(\mathcal{W}_1) \end{array} \qquad \begin{array}{rl} & \underline{\pi_2} \\ \textit{maximize:} & \mathrm{Tr}(J_2^\dagger W) \\ \textit{subject to:} & \Psi_2(W) = C_2, \\ & W \in \mathrm{Pos}(\mathcal{W}_2), \end{array}$$

where $\Psi_1 : \mathrm{L}(\mathcal{W}_1) \to \mathrm{L}(\mathcal{Z}_1)$ *and* $\Psi_2 : \mathrm{L}(\mathcal{W}_2) \to \mathrm{L}(\mathcal{Z}_2)$*, for complex Euclidean spaces* $\mathcal{W}_1, \mathcal{Z}_1, \mathcal{W}_2, \mathcal{Z}_2$*, and* $J_1 \in \mathrm{L}(\mathcal{W}_1)$ *and* $J_2 \in \mathrm{L}(\mathcal{W}_2)$ *are Hermitian. Let* $\alpha(\pi_1)$ *and* $\alpha(\pi_2)$ *denote the semidefinite programs' solutions. If* J_1 *and* J_2 *are positive semidefinite, then the solution to the following semidefinite program, denoted* $\pi_1 \otimes \pi_2$*, is* $\alpha(\pi_1 \otimes \pi_2) = \alpha(\pi_1)\alpha(\pi_2)$*:*

$$\begin{array}{rl} & \underline{\pi_1 \otimes \pi_2} \\ \textit{maximize:} & \mathrm{Tr}((J_1 \otimes J_2)^\dagger W) \\ \textit{subject to:} & \Psi_1 \otimes \Psi_2(W) = C_1 \otimes C_2, \\ & W \in \mathrm{Pos}(\mathcal{W}_1 \otimes \mathcal{W}_2). \end{array}$$

Since B_0 is positive semidefinite and $\pi_{\alpha'} = \pi_\alpha^{\otimes s}$ (using the associativity of $\otimes$), Theorem 8 can be applied $(s-1)$ times in order to prove that $\alpha' = \alpha^s$ as required. See Ref. [12] for a similar approach, based on ideas in Ref. [19]. The idea of expressing the acceptance probability of a quantum interactive proof system as a semidefinite program first appeared in Ref. [20].

Note that this argument, combined with the arguments in the main body of the paper, shows that both the serial and parallel versions of our identification protocol are secure.

A.2 Proof of Proposition 3

Two facts hold without loss of generality:

- the POVMs $\{E_{w,0}, E_{w,\pi}\}$, for all w, may be assumed to be covariant, i.e. $E_{w,\pi} = V_\pi E_{w,0} V_\pi^\dagger$ (to see this, note that any not-necessarily-covariant POVM $\{F_{w,0}, F_{w,\pi}\}$ gives the same average probability of successfully guessing θ, given w, as the covariant POVM $\{E_{w,0}, E_{w,\pi}\}$ defined by $E_{w,0} = (F_{w,0} + V_\pi^\dagger F_{w,\pi} V_\pi)/2$);
- each $E_{w,0}$ has support only on $\mathrm{sp}(\mathcal{O}_w)$ and thus $E_{w,0} + E_{w,\pi} = I_{\mathrm{sp}(\mathcal{O}_w)}$, where $I_{\mathrm{sp}(\mathcal{O}_w)}$ is the identity operator on $\mathrm{sp}(\mathcal{O}_w)$.

To compute a basis of $\mathrm{sp}(\mathcal{O}_w)$, we now further define the system R' in the proof of Lemma 1 to consist of exactly $t+1$ qubits and the states $|c_h\rangle$, $h = 0, 1, \ldots, t$, to be all those computational basis states whose labels have Hamming weight 1 (thus $q = 2t+1$, which is larger than necessary, but simplifies the structure of the POVMs). The total subspace

$$S \equiv \mathrm{sp}\left(\{|S_j^t\rangle\}_{j=0,\ldots,t} \otimes \{|c_h\rangle\}_{h=0,1,\ldots,t} \otimes \{|0\rangle, |1\rangle\}\right) \tag{63}$$

supporting $|\psi_{RS}(\phi,\theta)\rangle$ breaks up into mutually orthogonal subspaces S_w of weight w, i.e., spanned by computational basis states whose labels have Hamming weight w:

$$S_1 = \mathrm{sp}\left(|S_0^t\rangle \otimes \{|c_h\rangle\}_h \otimes |0\rangle\right) \tag{64}$$

$$S_k = \mathrm{sp}\left(|S_{k-1}^t\rangle \otimes \{|c_h\rangle\}_h \otimes |0\rangle, |S_{k-2}^t\rangle \otimes \{|c_h\rangle\}_h \otimes |1\rangle\right), \tag{65}$$

$$S_{t+2} = \mathrm{sp}\left(|S_t^t\rangle \otimes \{|c_h\rangle\}_h \otimes |1\rangle\right), \tag{66}$$

for $k = 2, 3, \ldots, t+1$. Thus, for each w, we will do the following:

- write P_w in the basis in which S_w is expressed in Eqs. (64), (65), (66),
- derive an expression for $P_w|\psi_{RS}(0,0)\rangle$ (which is proportional to $|\Psi_w\rangle$) in order to find a basis for $\mathrm{sp}(\mathcal{O}_w) = \mathrm{sp}\{|\Psi_w\rangle, V_\pi|\Psi_w\rangle\}$ (which fully supports $E_{w,0}$), and
- derive the form of $E_{w,0}$ and thus, by covariance, the form of the POVM $\{E_{w,0}, E_{w,\pi}\}$ in each subspace S_w.

Recalling Eq. (40), it will be convenient to let $\alpha_{j,h} \equiv b_j g_{j,h}$ and so

$$|\psi_R(0)\rangle = \sum_{j,h} \alpha_{j,h}|S_j^t\rangle|c_h\rangle. \tag{67}$$

<u>*w=1:*</u>

Writing

$$P_1|\psi_{RS}(0,0)\rangle \tag{68}$$

$$= \left(\sum_h |S_0^t\rangle\langle S_0^t| \otimes |c_h\rangle\langle c_h| \otimes |0\rangle\langle 0|\right)|\psi_R(0)\rangle(|0\rangle + |1\rangle)/\sqrt{2} \tag{69}$$

$$= |S_0^t\rangle\left(\sum_h [(\langle S_0^t|\langle c_h||\psi_R(0)\rangle)/\sqrt{2}]|c_h\rangle\right)|0\rangle \tag{70}$$

$$= |S_0^t\rangle\left(\sum_h [\alpha_{0,h}/\sqrt{2}]|c_h\rangle\right)|0\rangle, \tag{71}$$

we see that $V_\pi|\Psi_1\rangle = |\Psi_1\rangle$ so that $E_{1,0} = E_{1,\pi} = |\Xi_0\rangle|0\rangle\langle\Xi_0|\langle 0|$, where $|\Xi_0\rangle$ is a state such that

$$|\Xi_0\rangle \propto |S_0^t\rangle \sum_h [\alpha_{0,h}/\sqrt{2}]|c_h\rangle. \tag{72}$$

We note that getting the outcome corresponding to this POVM element does not give any information about θ; we arbitrarily assign a guess of "$\theta = 0$" to this outcome, without affecting optimality (since θ is a priori uniformly distributed).

<u>$w \in \{2, 3, \ldots, t+1\}$:</u>

Similarly, we can write

$$P_w|\psi_{RS}(0,0)\rangle \tag{73}$$

$$= |S_{w-1}^t\rangle\left(\sum_h [\alpha_{w-1,h}/\sqrt{2}]|c_h\rangle\right)|0\rangle + \tag{74}$$

$$|S_{w-2}^t\rangle\left(\sum_h [\alpha_{w-2,h}/\sqrt{2}]|c_h\rangle\right)|1\rangle. \tag{75}$$

Chiribella et al. [17] show that $E_{w,0}$ may be assumed to have rank 1 without loss of generality. Thus $E_{w,0}$ may be written $|\eta_w\rangle\langle\eta_w|$, where

$$|\eta_w\rangle = a|\Xi_{w-1}\rangle|0\rangle + b|\Xi_{w-2}\rangle|1\rangle, \tag{76}$$

for some complex coefficients a and b, such that $|a|^2 + |b|^2 = 1$, where $|\Xi_{w-1}\rangle$ and $|\Xi_{w-2}\rangle$ are states such that, for $j = 0, 1, \ldots, t$,

$$|\Xi_j\rangle \propto \sum_h \frac{\alpha_{j,h}}{\sqrt{2}} |S_j^t\rangle |c_h\rangle. \tag{77}$$

We have (using covariance to get $E_{w,\pi}$)

$$E_{w,0} + E_{w,\pi} \tag{78}$$

$$= 2(|a|^2 |\Xi_{w-1}\rangle|0\rangle\langle\Xi_{w-1}|\langle 0| + |b|^2 |\Xi_{w-2}\rangle|1\rangle\langle\Xi_{w-2}|\langle 1|). \tag{79}$$

But

$$E_{w,0} + E_{w,\pi} \tag{80}$$

$$= \qquad I_{\mathrm{sp}(\mathcal{O}_w)} \tag{81}$$

$$= |\Xi_{w-1}\rangle|0\rangle\langle\Xi_{w-1}|\langle 0| + |\Xi_{w-2}\rangle|1\rangle\langle\Xi_{w-2}|\langle 1|. \tag{82}$$

Equating the two expressions implies that

$$|\eta_w\rangle = \frac{1}{\sqrt{2}}(|\Xi_{w-1}\rangle|0\rangle + e^{i\varphi_w}|\Xi_{w-2}\rangle|1\rangle), \tag{83}$$

for some phase φ_w. But we must have $\varphi_w = 0$ since $E_{w,0}$ corresponds to the guess "$\theta = 0$".

$\underline{w = t + 2:}$

Similar to the case $w = 1$ and using the definition from Eq. (77), we have $E_{t+2,0} = E_{t+2,\pi} = |\Xi_t\rangle|1\rangle\langle\Xi_t|\langle 1|$. We assign the guess "$\theta = \pi$" to getting the outcome corresponding to this POVM element.

To summarize, the elements of the overall POVM $\{E_0, E_\pi\}$ describing the measuring-and-guessing strategy may be expressed

$$E_0 = |\Xi_0\rangle|0\rangle\langle\Xi_0|\langle 0| + \sum_{w=2}^{t+1} |w,+\rangle\langle w,+| \tag{84}$$

$$E_\pi = \sum_{w=2}^{t+1} |w,-\rangle\langle w,-| + |\Xi_t\rangle|1\rangle\langle\Xi_t|\langle 1|, \tag{85}$$

where

$$|w,\pm\rangle \equiv \frac{1}{\sqrt{2}}(|\Xi_{w-1}\rangle|0\rangle \pm |\Xi_{w-2}\rangle|1\rangle). \tag{86}$$

A.3 Proof of Theorem 1, Assuming Eq. (15)

For security with error ϵ, we require

$$r(1 - c/(2r+1)^2)^s < \epsilon, \tag{87}$$

which, by taking the logarithm of both sides, is equivalent to

$$s > \log(\epsilon/r)/\log(1 - c/(2r+1)^2). \tag{88}$$

Using the series expansion $\log(1-x) = -(x + x^2/2 + x^3/3 + \cdots)$, the right-hand side of Eq. (88) is upper-bounded by

$$(2r+1)^2 \log(r/\epsilon)/c, \tag{89}$$

from which the theorem follows.

A.4 Proof of Proposition 4

This maximization problem is very similar to that in Ref. [11], where it was required to maximize $\langle\zeta|M'_t|\zeta\rangle$ over all states $|\zeta\rangle \in \mathrm{sp}\{|j\rangle : j = 0, 1, \ldots, t\}$ for

$$M'_t = \sum_{j=0}^{t-1} |j+1\rangle\langle j| + |j\rangle\langle j+1|. \tag{90}$$

In fact, in light of Eq. (40), the phase estimation problem in Ref. [11] may be viewed as the same as the one we consider, but where Eve does not have access to the register R'. (Indeed, our optimal success probability cannot be less than that in Ref. [11], since at the very least Eve can forgo the use of the ancillary register R'.) Finally, below, we show that our optimal success probability is exactly equal to that obtained in Ref. [11].

Let $\alpha^\star_{j,h}$ denote the optimal values for our maximization problem, and let $M^\star_t$, $|\psi_R(0)^\star\rangle$, and $|\varXi^\star_j\rangle$ denote the values of M_t, $|\psi_R(0)\rangle$, and $|\varXi_j\rangle$ at those optimal values. Note that $\{|\varXi_j\rangle : j = 0, 1, \ldots, t\}$ is orthonormal for all values of $\alpha_{j,h}$, thus $\{|\varXi^\star_j\rangle : j = 0, 1, \ldots, t\}$ is orthonormal. Consider now optimizing $\langle\psi|M^\star_t|\psi\rangle$ over all unit vectors $|\psi\rangle \in \mathrm{sp}\{|\varXi^\star_j\rangle : j = 0, 1, \ldots, t\}$ for fixed $M^\star_t$; denote the optimal $|\psi\rangle$ as $|\psi^\star\rangle$. It must be that

$$\langle\psi^\star|M^\star_t|\psi^\star\rangle \geq \langle\psi_R(0)^\star|M^\star_t|\psi_R(0)^\star\rangle, \tag{91}$$

since $|\psi_R(0)^\star\rangle \in \mathrm{sp}\{|\varXi^\star_j\rangle : j = 0, 1, \ldots, t\}$ by inspecting Eqs. (67) and (77). Now note that the coefficients of $|\psi^\star\rangle$ with respect to the basis $\{|\varXi^\star_j\rangle : j = 0, 1, \ldots, t\}$ must be precisely those coefficients of the optimal $|\zeta\rangle$ with respect to the standard orthonormal basis $\{|j\rangle : j = 0, 1, \ldots, t\}$ found in Ref. [11]; otherwise, substituting the coefficients of $|\psi^\star\rangle$ would give a higher maximum than that in Ref. [11]. (The argument works because, in both cases, the orthonormal basis is fixed for the optimization.) Therefore, we have, as in Ref. [11],

$$|\psi^\star\rangle \propto \sum_{j=0}^{t} \sin\left[\frac{(j+1)\pi}{t+2}\right] |\varXi_j\rangle. \tag{92}$$

References

1. Menezes, A.J., van Oorschot, P., Vanstone, S.: Handbook of Applied Cryptography. CRC Press LLC, Boca Raton (1996)

2. Gottesman, D., Chuang, I.L.: Quantum Digital Signatures (2001). quant-ph/0105032
3. Lamport, L.: Constructing digital signatures from a one-way function. CSL 98, SRI International (1979)
4. Kawachi, A., Koshiba, T., Nishimura, H., Yamakami, T.: Computational indistinguishability between quantum states and its cryptographic application. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 268–284. Springer, Heidelberg (2005). http://arxiv.org/abs/quants-ph/0403069
5. Hayashi, M., Kawachi, A., Kobayashi, H.: Quantum measurements for hidden subgroup problems with optimal sample complexity. Quantum Inf. Comput. **8**, 0345–0358 (2008)
6. Ioannou, L.M., Mosca, M.: Public-key cryptography based on bounded quantum reference frames. http://arxiv.org/abs/0903.5156
7. Goldreich, O.: Foundations of Cryptography (Volume I): Basic Tools. Cambridge University Press, Cambridge (2001)
8. Chaum, D., Roijakkers, S.: Unconditionally secure digital signatures. In: Menezes, A., Vanstone, S.A. (eds.) CRYPTO 1990. LNCS, vol. 537, pp. 206–214. Springer, Heidelberg (1991)
9. Gottesman, D.: Quantum public key cryptography with information-theoretic security. Workshop on classical and quantum information security, Caltech, 15–18 December 2005. http://www.cpi.caltech.edu/quantum-security/program.html; see also http://www.perimeterinstitute.ca/personal/dgottesman
10. Damgaard, I., Fehr, S., Salvail, L., Schaffner, C.: Secure identification and QKD in the bounded-quantum-storage model. CRYPTO 2007 **4622**, 342–359 (2007)
11. Bartlett, S.D., Rudolph, T., Spekkens, R.W., Turner, P.S.: Degradation of a quantum reference frame. New J. Phys. **8**, 58 (2006)
12. Gutoski, G.: Quantum strategies and local operations. Ph.D. thesis, University of Waterloo (2009)
13. Mittal, R., Szegedy, M.: Product rules in semidefinite programming. In: Csuhaj-Varjú, E., Ésik, Z. (eds.) FCT 2007. LNCS, vol. 4639, pp. 435–445. Springer, Heidelberg (2007)
14. van Dam, W., Mauro D'Ariano, G., Ekert, A., Macchiavello, C., Mosca, M.: Optimal quantum circuits for general phase estimation. Phys. Rev. Lett. **98**(9), 090501 (2007)
15. Beals, R., Buhrman, H., Cleve, R., Mosca, M., de Wolf, R.: Quantum lower bounds by polynomials. In FOCS '98: Proceedings of the 39th Annual Symposium on Foundations of Computer Science (1998)
16. van Dam, W., Mauro D'Ariano, G., Ekert, A., Macchiavello, C., Mosca, M.: Optimal phase estimation in quantum networks. J. Phys. A: Math. Theor. **40**, 7971–7984 (2007)
17. Chiribella, G., D'Ariano, G.M., Sacchi, M.F.: Optimal estimation of group transformations using entanglement. Phys. Rev. A **72**(4), 042338 (2005)
18. Watrous, J.: Theory of quantum information. Lecture notes for course CS 789, University of Waterloo, http://www.cs.uwaterloo.ca/~watrous/ (2008)
19. Cleve, R., Slofstra, W., Unger, F., Upadhyay, S.: Strong parallel repetition theorem for quantum XOR proof systems (2006). arXiv:quant-ph/0608146v1
20. Kitaev, A., Watrous, J.: Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In STOC '00: Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing (2000)