Public-key cryptography based on bounded quantum reference frames

L. M. Ioannou\textsuperscript{1} and M. Mosca\textsuperscript{1,2,†}

\textsuperscript{1}Institute for Quantum Computing, University of Waterloo, 200 University Avenue, Waterloo, Ontario, N2L 3G1, Canada
\textsuperscript{2}Perimeter Institute for Theoretical Physics 31 Caroline Street North, Waterloo, Ontario, N2L 2Y5, Canada

We demonstrate that the framework of bounded quantum reference frames has application to building quantum-public-key cryptographic protocols and proving their security. Thus, the framework we introduce can be seen as a public-key analogue of the framework of Bartlett et al. \cite{Bartlett2007}, where a private shared reference frame is shown to have cryptographic application. The protocol we present in this paper is an identification scheme, which, like a digital signature scheme, is a type of authentication scheme. We prove that our protocol is both reusable and secure under the honest-verifier assumption. Thus, we also demonstrate that secure reusable quantum-public-key authentication is possible to some extent.

1 Introduction

Since its inception, the focus of quantum cryptography has been on symmetric-key protocols, where Alice and Bob attempt to generate or are assumed to hold private shared correlations. Such correlations can usually be defined or encoded by a string of bits — the secret key — but Bartlett et al. \cite{Bartlett2007} showed that they may also take the form of a private shared reference frame. Symmetric-key quantum protocols are usually unconditionally secure, meaning that the sole assumption is that (some part of) quantum theory is correct; however, Damgaard et al. \cite{Damgaard2002, Damgaard2004} have investigated information-theoretically secure protocols in the bounded storage model, where an extra assumption is that the size of the adversary’s quantum memory is limited.

Going beyond the symmetric-key model, but retaining unconditional security, Gottesman and Chuang \cite{Gottesman2001} introduced quantum-public-key cryptography — where the public keys are quantum systems, each of whose state encodes the (same) classical private key — by giving a secure one-time (digital) signature scheme for signing classical messages. The public-key framework eliminates the need for Alice and Bob to establish private shared correlations, which has practical advantages in large networks of users (where there may be many “Alices” or “Bobs”).

\textsuperscript{\dagger}lmi@iqc.ca
\textsuperscript{†}mmosca@iqc.ca
One aspect of quantum-public-key cryptography that sets it apart from classical public-key cryptography is that the necessary limit on the number of copies of the public key implies that not everyone can use the protocol; however, in practice, the maximum number of users (or uses) of any particular protocol can be estimated, and thus the parameters of the protocol can be adjusted so that the limit allows for this maximum. Increasing this limit would presumably result in a less efficient instance of the protocol, and this is one kind of tradeoff between efficiency and usability in the quantum-public-key setting. Another kind concerns reusability. For instance, the abovementioned 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 signature schemes, where either the same 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.

Our work appears to be of a dramatically different character when compared to other explorations of quantum-public-key protocols [5, 6, 7, 8, 9]: we demonstrate that the framework of bounded quantum reference frames [10] has application to building such protocols and proving their security. Thus, the framework we introduce can be seen as a public-key analogue of the framework of Bartlett et al. [1].

The protocol we present in this paper is an identification scheme, which, like a signature scheme, is a type of authentication scheme. We prove that our protocol is both reusable and secure under the honest-verifier assumption (defined in the next section). Thus, we also demonstrate that secure reusable quantum-public-key authentication is possible to some extent.

We now proceed with a description of our protocol (Section 2) and the honest-verifier security proof (Section 3).

2 An identification scheme

Suppose Alice generates a private key and authentically distributes copies of the corresponding public key to any potential users of the scheme, including Bob. The following is an intuitive description (adapted from Section 4.7.5.1 in Goldreich’s book [11]) of how a secure identification scheme works. If 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 (assuming Bob possesses public keys from many different people). The ensuing protocol (whatever it is) 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. An honest-verifier identification protocol is only intended to be secure under the extra assumption that, whenever Eve engages the prover Alice in the protocol, Eve follows the verification protocol as if she were honest. Note that no identification protocol is secure against a person-in-the-middle attack, where Eve concurrently acts as a verifier with Alice and as a prover with Bob. 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.

A summary of our protocol is as follows. Alice chooses a private phase reference and distributes a limited number of samples of her reference frame as quantum public keys. The samples are used by Bob to verify that the prover is actually Alice. Because Alice has a perfect phase reference, she can carry out the identification protocol with no error (assuming perfect quantum channels). But, because Eve only has a bounded quantum reference frame (in the form of a limited number of copies of the public key), she inevitably incurs an error that Bob can detect with sufficiently high probability.

2.1 Protocol specification

A typical identification protocol is a challenge-response interactive proof, consisting of a kernel that is repeated several times; each iteration uses different random local parameter-values chosen by Alice or Bob (in describing protocol parameters, we use “local” to describe parameters whose values change in each kernel-iteration, and “global” to describe parameters whose values are constant over the entire protocol instance). The number $s$ of times that the kernel is repeated is a global security parameter. Thus, in our case, when the other global parameters of the scheme are fixed, the probability that Eve can break the protocol (in an honest-verifier setting) is exponentially small in $s$.

The private key in our protocol will be an $s$-tuple

$$(x_1, x_2, \ldots, x_s),$$

(1)

where $x_j$ is used only in the $j$th kernel-iteration. Alice chooses each $x_j$ independently and randomly, from some discrete uniform distribution. We note that, throughout the paper, the variable "$j$" will be reserved for the kernel-iteration index.

Corresponding to each $x_j$ is a quantum state $|\psi_j\rangle := |\psi(x_j)\rangle$, via a fixed map $x \mapsto |\psi(x)\rangle$; we will sometimes write "$|\psi_x\rangle$" for "$|\psi(x)\rangle$". The state of (one copy of) the public key in our protocol is denoted

$$\otimes_{j=1}^{s} |\psi_j\rangle.$$ 

(2)
Bob will use the $j$th subsystem of the public key (which is in the state $|\psi_j\rangle$) only in the $j$th kernel-iteration.

Now that we understand the global structure of the keys, we shall give the details of how every $x_j$ and $|\psi_j\rangle$ are chosen, usually dropping the subscript $j$ (since the procedure is the same for all $j$). For the integer-valued, global parameter $r > 0$, Alice chooses the value $x$ uniformly from \{1, 2, ..., $r + 1$\} and authentically distributes (e.g. via trusted courier) at most $r$ copies of (a system in the state) $(|0\rangle + e^{2\pi ix/(r+1)}|1\rangle)$. This implicitly defines the fixed map above, that is, $|\psi(x)\rangle := |0\rangle + e^{2\pi ix/(r+1)}|1\rangle$ (we often omit normalization factors). Thus, by the above notation,

$$|\psi_j\rangle = |0\rangle + e^{2\pi ix_j/(r+1)}|1\rangle. \quad (3)$$

The parameter $r$ is the reusability parameter, dictating the maximum number of secure uses of the scheme for a fixed public key. This completes the definition of the private and public keys.

The kernel of our interactive protocol is the following three steps. For convenience, let

$$\phi_x := 2\pi x/(r + 1). \quad (4)$$

We assume that all quantum channels are perfect.

1. Bob creates $|0\rangle|1\rangle + |1\rangle|0\rangle$, and sends one register of this system to Alice.

2. Alice measures the received register in the basis \{|0\rangle\pm e^{i\phi_x}|1\rangle\}. If the state of the register immediately after the measurement is $|0\rangle + e^{i\phi_x}|1\rangle$, then Alice sends “0” to Bob; otherwise, Alice sends “1”.

3. If Bob receives “1”, then he applies the Pauli-$Z$ gate

$$Z := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad (5)$$

to the register that he kept in Step 1. Finally, Bob swap-tests\footnote{The swap-test of two registers (labelled 2 and 3) in the states $|\xi\rangle_2$ and $|\chi\rangle_3$ is a measurement (with respect to the computational basis \{|0\rangle_1, |1\rangle_1\}) of the control register (labelled 1) of the state $$(H_1 \otimes I_2 \otimes I_3)(c - \text{SWAP}_{2,3})(|0\rangle_1 + |1\rangle_1)|\xi\rangle_2|\chi\rangle_3)/\sqrt{2}, \quad (6)$$

where $H_1$ is the usual Hadamard gate (applied to register 1) and $c - \text{SWAP}_{2,3}$ is the controlled-swap gate. The probability that the state is $|0\rangle_1$ immediately after the measurement — which corresponds to a pass — is $(1 + |\langle\xi|\chi\rangle|^2)/2$. When the registers 2 and 3 are in the mixed states $\rho$ and $\rho'$, this probability is $(1 + \text{tr}(\rho\rho'))/2.$} this register with his authentic copy of $|\psi_x\rangle$. 

3 The swap-test of two registers (labelled 2 and 3) in the states $|\xi\rangle_2$ and $|\chi\rangle_3$ is a measurement (with respect to the computational basis \{|0\rangle_1, |1\rangle_1\}) of the control register (labelled 1) of the state

$$(H_1 \otimes I_2 \otimes I_3)(c - \text{SWAP}_{2,3})(|0\rangle_1 + |1\rangle_1)|\xi\rangle_2|\chi\rangle_3)/\sqrt{2}, \quad (6)$$

where $H_1$ is the usual Hadamard gate (applied to register 1) and $c - \text{SWAP}_{2,3}$ is the controlled-swap gate. The probability that the state is $|0\rangle_1$ immediately after the measurement — which corresponds to a pass — is $(1 + |\langle\xi|\chi\rangle|^2)/2$. When the registers 2 and 3 are in the mixed states $\rho$ and $\rho'$, this probability is $(1 + \text{tr}(\rho\rho'))/2.$
After the kernel is repeated $s$ times, Bob “accepts” if all the swap-tests passed; otherwise, Bob “rejects”. It is clear that, when Alice and Bob are honest, the protocol is correct, that is, Bob always “accepts”. To see this, note that, up to global phase, the state $|01⟩ + |10⟩$ equals

$$\left(|0⟩ + e^{iφ_1}|1⟩\right)(|0⟩ + e^{iφ_2}|1⟩) - \left(|0⟩ - e^{iφ_2}|1⟩\right)(|0⟩ - e^{iφ_1}|1⟩).$$  \hfill (7)

As a final specification for the protocol, we also stipulate that Alice not engage in the protocol more than $r$ times (when there are $r$ copies of the public key in circulation) for a particular value of the private key.

3 Honest-verifier security

We now present the proof of security of the above protocol under the simplifying assumptions that (1) Eve, the adversary, never passively monitors any protocol instances between Alice and Bob, and (2) Eve never participates in the protocol as a verifier (Alice and Bob are always honest). We will show at the end of the paper (in Section 3.5) how to modify the protocol so that it is secure under the proper honest-verifier assumption (where Eve is allowed to passively monitor as well as follow the verifier protocol honestly with Alice).

Note that if Eve has $t$ copies of the public key, then she has at most $(r - t)$ chances to fool Bob, i.e., cause Bob to “accept”. Most of the argument, beginning in Section 3.1, is devoted to showing that

$$\Pr[\text{Eve fools Bob on first attempt, using } t \text{ copies}] \leq (1 - 1/8(t + 1))^s.$$ \hfill (8)

$$\Pr[\text{Eve fools Bob on } l\text{th attempt, using } t \text{ copies}] \leq \Pr[\text{Eve fools Bob on first attempt, using } (t + l - 1) \text{ copies}].$$ \hfill (9)

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 the public key per kernel-iteration, we have, for $l = 2, 3, \ldots, (r - t),$

$$\Pr[\text{Eve fools Bob on } l\text{th attempt, using } t \text{ copies}] \leq \Pr[\text{Eve fools Bob on first attempt, using } (t + l - 1) \text{ copies}].$$
Given this, we use the union bound:

\[
\Pr[\text{Eve fools Bob at least once, using } t \text{ copies}] \\
\leq \sum_{l=1}^{r-t} \Pr[\text{Eve fools Bob on } l\text{th attempt, using } t \text{ copies}] \\
\leq \sum_{l=1}^{r-t} \Pr[\text{Eve fools Bob on first attempt, using } (t + l - 1) \text{ copies}] \\
\leq \sum_{l=1}^{r-t} (1 - 1/8(t + l))^s \\
\leq (r - t)(1 - 1/8r)^s.
\]

It follows that the probability that Eve can fool Bob at least once, that is, break the protocol, is

\[
P_{\text{break}} \leq r(1 - 1/8r)^s, \quad (10)
\]

which, for fixed \( r \), is exponentially small in \( s \).

We note that, for a secure protocol, one can use \( s \in \Omega(r \log(r)) \); this shows how the efficiency of the protocol scales with its reusability.

The remainder of the proof establishes the bound in Lines (8) and (9).

### 3.1 Preliminary analysis

Since each \( x_j \) is independently and randomly selected from the set \( \{1, 2, \ldots, r + 1\} \), then any information about the values of \( x_k \) for \( k \neq j \) will be of no help to Eve in (kernel-)iteration \( j \). In other words, her probability of passing the SWAP-test in Step 3 with public key \(|\psi(x_j)\rangle\) is no higher given any information about the values of \( x_k \) for \( k \neq j \). In particular, the probability of passing the SWAP-test in iteration \( j \) conditioned on passing the SWAP-test in any other iteration can be no higher than the optimal probability of passing the SWAP-test in iteration \( j \). In this section, we show that the probability of passing the SWAP-test for any particular iteration is at most \( 1 - 1/8(t + 1) \), and thus the probability of passing all \( s \) SWAP-tests is at most \( (1 - 1/8(t + 1))^s \).

Now, we show that, from Bob’s and Eve’s points of view, Alice’s choosing the private phase angle \( \phi_x \) from the discrete set \( \{2\pi x/(r + 1) : x = 1, 2, \ldots, r + 1\} \) is equivalent to her choosing the phase angle from the continuous interval \([0, 2\pi)\). The only information that Eve (who is never allowed to act as verifier) and Bob have about \( \phi_x \) comes from the \( r \) copies of \(|\psi_x\rangle\). They
describe the state of these \( r \) systems by the density operator
\[
\frac{1}{r+1} \sum_{x=1}^{r+1} (|0\rangle + e^{2\pi ix/(r+1)} |1\rangle)(|0\rangle + e^{-2\pi ix/(r+1)} \langle 1|) \otimes_r.
\] (11)

Had \( \phi_x \) been chosen uniformly from \( \{2\pi x/(r+1) : x \in [0, r+1]\} = [0, 2\pi) \), they would describe the state by
\[
\frac{1}{2\pi} \int_0^{2\pi} (|0\rangle + e^{i\phi} |1\rangle)(|0\rangle + e^{-i\phi} \langle 1|) \otimes_r d\phi.
\] (12)

It is straightforward to show that the above two density operators are both equal to
\[
\frac{1}{2^r} \sum_{w=0}^r \binom{r}{w} |S^r_w \rangle \langle S^r_w|,
\] (13)

where \( |S^r_w \rangle \) is the normalized symmetric sum of all \( \binom{r}{w} \) states in \( \{|0\rangle, |1\rangle\} \otimes_r \) whose binary labels have Hamming weight \( w \). Thus, without loss, we may drop the subscript “\( x \)” on “\( \phi_x \)”, write “\( \phi \)” for Alice’s private phase angle, and assume she did (somehow) choose \( \phi \) uniformly randomly from \( [0, 2\pi) \).4

### 3.2 Equivalence of assuming no shared reference frame

Thus far, we have implicitly assumed that Alice, Bob, and Eve share a perfect phase reference (frame), in that all three are assumed able to implement the same (Hadamard) gate
\[
\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},
\] (16)

4This requires the following two facts: (1) for any integer \( a \),
\[
\frac{1}{2\pi} \int_0^{2\pi} e^{ia\theta} d\theta = \begin{cases} 0 & \text{if } a \neq 0, \\ 1 & \text{otherwise}; \end{cases}
\] (14)

and (2) for any integer \( p \geq 2 \) and integer \( a \):
\[
\frac{1}{p} \sum_{k=1}^p e^{2\pi iak/p} = \begin{cases} 0 & \text{if } a \text{ is not a multiple of } p, \\ 1 & \text{otherwise}, \end{cases}
\] (15)

where the second fact is applied at \( p = r+1 \).

5One way to interpret this result is that even if Alice encodes infinitely many bits into \( \phi \), it is no better than if she encoded \( \lceil \log_2(r+1) \rceil \) bits. Note that if Eve performs an optimal phase estimation \( [12] \) in order to learn \( \phi \) and then cheat Bob, she can only learn at most \( \lceil \log_2(r-1) \rceil \) bits of \( \phi \) (here, we assume Eve has \( r-1 \) copies of the public key, having left Bob one copy), whereas Alice actually encoded \( \lceil \log_2(r+1) \rceil \) bits into \( \phi \).
defined with respect to the common basis \{|0\rangle, |1\rangle\}. Now, we show that our protocol (where Alice chooses a private random \(\phi\)) under this assumption is equivalent to a protocol (where Alice need not choose any random phase parameter) under a new assumption that Alice, Bob, and Eve have maximal ignorance about one another’s phase reference. This is easily done in three steps: (1) first, we rewrite our protocol under the new assumption of no shared phase reference; (2) then, we note that the honest version of our protocol under the new assumption still works the same way as under the original assumption, but that Alice’s private phase angle \(\phi\) becomes redundant; (3) finally, we consider Eve’s perspective, noting that her task of cheating looks the same as it did under the original assumption, and that, as far as she is concerned, \(\phi\) is redundant.

Each player can now be assumed to have his or her own perfect phase reference. Consider first Alice. Having her own perfect phase reference will mean for us that she has the system \(|0\rangle + e^{i\phi_A} |1\rangle\otimes N_A\) for arbitrarily large \(N_A\) and some \(\phi_A \in [0,2\pi]\). We assume Alice has maximal ignorance of the value of \(\phi_A\); we have written the state of her phase reference from the perspective of a fictitious omniscient. With this setup, Alice’s public-key-element is thus \(r\) copies of \(|0\rangle + e^{i(\phi+\phi_A)} |1\rangle\).

Bob has his own independent, perfect phase reference, defined analogously by \(\phi_B\). He can still create \(|0\rangle |1\rangle + |1\rangle |0\rangle\) (up to global phase \(e^{i\phi_B}\)) in Step 1 of the kernel. In Step 2, Alice measures with respect to the basis \{\(|0\rangle \pm e^{i(\phi+\phi_A)} |1\rangle\}\) and sends Bob “0” if she gets the outcome corresponding to “+” and sends “1” otherwise. Step 3 looks the same. It is easy to see that, when Alice and Bob are honest, our protocol under the new assumption works the same way as it did originally. Furthermore, \(\phi\) is redundant, since it may be absorbed into \(\phi_A\).

Let us now consider Eve, whose independent and perfect phase reference is defined by \(\phi_E\). We assume Eve gets a hold of \(t\) copies of the system \(|0\rangle + e^{i\phi'} |1\rangle\). Let \(|1'\rangle := e^{i\phi_E} |1\rangle\) and let \(\phi' := \phi + \phi_A - \phi_E\). Thus, to summarize: Eve has \(t\) copies of \(|0\rangle + e^{i\phi'} |1\rangle\), for uniformly random (and unknown) \(\phi' \in [0,2\pi]\), and she has a perfect phase reference with respect to the basis \{\(|0\rangle, |1'\rangle\}\}, and Alice performs a measurement in the basis \{\(|0\rangle \pm e^{i\phi'} |1'\rangle\}\}. Therefore, the situation for Eve is equivalent to that in our original protocol, and once again \(\phi\) is redundant as it can be absorbed into \(\phi_A\).

For the remainder of the proof, we adopt the new assumption and protocol (where \(\phi\) has been absorbed into \(\phi_A\)). To simplify the presentation, we take \(\phi_A = 0\) without loss of generality. Thus, the public-key-element (for any particular kernel-iteration \(j\) that we are considering) now looks like \(r\) copies of \(|0\rangle + |1\rangle\).

---

6 In practice, no phase reference is perfect. But we can assume that it is arbitrarily good, which we call “perfect”.

7 There are many different types of states that can serve as phase reference frames, the most popular type being an optical coherent state; see e.g. [10].
3.3 Sufficiency of maximizing successful guessing probability

The security of our protocol follows from a result of Bartlett et al. [10], which concerns a slightly different problem for Eve than the problem of her trying to fool Bob. This different problem is for Eve to guess whether she has been given the system $|0\rangle + |1\rangle$ or $|0\rangle - |1\rangle$, where each case occurs with equal probability. The purpose of this section is to show that any good cheating strategy gives a good guessing strategy; we will show that an upper bound on the average successful guessing probability gives an upper bound on the cheating probability, so that, in order to prove security, it suffices to show that the maximum successful guessing probability is sufficiently small (which we will do in the next section).

Any cheating strategy of Eve can be modeled as follows. Let

$$|\pm\rangle := |0\rangle \pm |1\rangle.$$ (17)

Recall that Bob creates a system in the state $|0\rangle |1\rangle + |1\rangle |0\rangle$ and that

$$|0\rangle |1\rangle + |1\rangle |0\rangle = |+\rangle |+\rangle - |-\rangle |-\rangle.$$ (18)

Eve’s system before Bob sends one of his registers can be represented by $|\Xi\rangle$, which consists of the $t$ copies of $|0\rangle + |1\rangle$ as well as any ancillary registers (which we can assume are in the pure state $|0\rangle$). Eve’s (optimal) POVM can thus be modeled by a unitary operation $U_E$ acting on her system (which now includes the register Bob sends), which transforms the state of the total system as follows:

$$\frac{1}{\sqrt{2}}(|+\rangle_B |+\rangle_E - |−\rangle_B |−\rangle_E)|\Xi\rangle_E \xrightarrow{U_E}$$ (19)

$$\frac{1}{\sqrt{2}} \left(|+\rangle_B (\alpha |0\rangle_E |\psi_0^+\rangle_E + \beta |1\rangle_E |\psi_1^+\rangle_E) - |−\rangle_B (\gamma |0\rangle_E |\psi_0^-\rangle_E + \delta |1\rangle_E |\psi_1^-\rangle_E) \right),$$ (20)

so that the leftmost register of Eve’s system encodes the measurement outcome. Bob’s application of the $Z$ gate conditioned on the value of the measurement outcome can be modeled by a controlled-$Z$ gate, which will take the state of the total system to

$$\frac{1}{\sqrt{2}} \left(|+\rangle_B (\alpha |0\rangle_E |\psi_0^+\rangle_E - \delta |1\rangle_E |\psi_1^-\rangle_E) + |−\rangle_B (\beta |1\rangle_E |\psi_1^+\rangle_E - \gamma |0\rangle_E |\psi_0^-\rangle_E) \right).$$ (22)

Let $\tau$ represent the density operator for this state after Eve’s system has been traced out. The
probability that Bob’s swap-test passes is easily calculated to be

\[ P_{\text{pass}} = \frac{1 + \langle + | \tau | + \rangle}{2} \]
\[ = \frac{1 + (|\alpha|^2 + |\delta|^2)/2}{2}. \]

Now, suppose Eve is faced with the different problem of guessing whether Bob gave her \(|+\rangle\) or \(|-\rangle\), where each case occurs with probability 1/2. Since, as can be seen from the mapping in Line (19), \(U_E\) maps

\[ |+\rangle_E |\Xi\rangle_E \mapsto \alpha |0\rangle_E |\psi_0^+\rangle_E + \beta |1\rangle_E |\psi_1^+\rangle_E \]
\[ |-\rangle_E |\Xi\rangle_E \mapsto \gamma |0\rangle_E |\psi_0^-\rangle_E + \delta |1\rangle_E |\psi_1^-\rangle_E, \]

Eve can use the same procedure she used for her attack in order to guess which state Bob prepared: upon measuring her leftmost register, she guesses “\(|+\rangle\)” if she gets outcome “0”, and otherwise she guesses “\(|-\rangle\)” . The probability that she guesses successfully on average using this strategy is clearly

\[ P_{\text{succ}} = \frac{1}{2} \times \Pr(\text{outcome = “0”} | \text{Bob prepared } |+\rangle) + \]
\[ \frac{1}{2} \times \Pr(\text{outcome = “1”} | \text{Bob prepared } |-\rangle) \]
\[ = \frac{(|\alpha|^2 + |\delta|^2)}{2}. \]

Thus, any upper bound on \(P_{\text{succ}}\) gives an upper bound on \(P_{\text{pass}}\).

### 3.4 Bounding the successful guessing probability

Bartlett et al. [10] give an expression for the average successful guessing probability in terms of the state \(\rho\) of a general single-mode bounded phase reference frame. A single mode is mathematically modeled by \(\mathbb{C}^N\), and a basis for this space is \(\{|n\rangle : n = 0, 1, \ldots, N\}\) (do not think of \(n\) as shorthand for the binary representation of \(n\): \(n \neq |n_1\rangle |n_2\rangle \cdots |n_m\rangle\) for \(n_1 n_2 \cdots n_m\) the binary representation of integer \(n\)). Note that \(N\) can equal \(\infty\), but, for us, it will suffice to take \(N = t\). We have implicitly assumed that Eve’s bounded reference frame, consisting of \(t\) copies of \(|0\rangle + |1\rangle\), is a \(t\)-mode system, modeled by \((\mathbb{C}^2)^\otimes t\), but where we only ever used a two-dimensional subspace \(\text{sp}\{|0\rangle, |1\rangle\}\) of each mode. So that we may apply Bartlett et al.’s analysis, it suffices for us to show that Eve’s multi-mode reference frame is unitarily equivalent
to a single-mode reference frame and that the unitary operation that relates the two is perfectly implementable by Eve.

Recalling the definition following Line (13), Eve’s reference frame is in the state

$$(|0⟩ + |1⟩)^\otimes t = \sum_{w=0}^{t} \sqrt{\frac{t}{w}} |S_w⟩,$$  

where $|S_w⟩$ is a $t$-mode state. Now we note that the transformation

$$|S_w⟩ \mapsto |0⟩\otimes (t-1)|w⟩, \text{ for all } w = 0, 1, \ldots, t,$$  

where $|w⟩$ is a single-mode state, can be completed on the vector space $(C^t)^\otimes t$ so that it is unitary and phase invariant. Thus, Eve can carry out this transformation with no error. Therefore, we may assume that Eve’s phase reference frame is in the state (described from the omniscient’s perspective)

$$\rho := \sum_{w=0}^{t} \sum_{w'=0}^{t} \sqrt{\frac{t}{w}} \frac{t}{w'} |w⟩⟨w'|. $$

We are now ready to apply the result of Bartlett et al. [10]. Using Equation (21) of their paper gives

$$P_{\text{succ}} = \frac{1}{2} + \frac{1}{2} \sum_{m=0}^{\infty} \Re((m+1|\rho|m))$$  

$$= \frac{1}{2} + \frac{1}{2} \sum_{m=0}^{t-1} \sqrt{\frac{t}{m}} \frac{t}{m+1},$$

which we can show to be in $1 - \Omega(1/t)$ (up to logarithmic factors) using some simple approximations. Cheung [14] has improved our asymptotic bound on this quantity by showing

---

8Define the unitary re-phasing map $U(\theta)$ on $(C^t)^\otimes t$ as the mapping

$$|w_1⟩|w_2⟩\cdots|w_t⟩ \mapsto e^{i\theta(w_1+w_2+\cdots+w_t)}|w_1⟩|w_2⟩\cdots|w_t⟩$$

for any $\theta$ and all $w_l = 0, 1, \ldots, t$, for $l = 1, 2, \ldots, t$. A unitary operation $V$ on $(C^t)^\otimes t$ is said to be phase invariant if $U(\theta)VU(\theta)^\dagger = V$ for all $\theta$. This, if $V$ is phase invariant, Eve does not need any particular phase reference to perform $V$ — she can use her own phase reference (defined by $\phi_E$; see Section 3.2), and the result will be the same as if Alice performed $V$ using her own phase reference (defined by $\phi_A$). See Section II.B of Bartlett et al. [13] for more details.
that

$$\frac{1}{2^t} \sum_{m=0}^{t-1} \sqrt{\binom{t}{m} \binom{t}{m+1}} \leq 1 - \frac{1}{2(t+1)} - \frac{1}{2^{t+1}}, \tag{38}$$

which implies

$$P_{\text{succ}} \leq 1 - \frac{1}{4(t+1)}. \tag{39}$$

It follows that

$$P_{\text{pass}} \leq 1 - \frac{1}{8(t+1)}, \tag{40}$$

which we recall is an upper bound on the probability that Bob’s swap-test passes in any particular kernel-iteration, when Eve is acting as a dishonest prover and using \( t \) copies of the public key. Thus, as we showed at the beginning of Section 3.1, the total probability that Eve causes all \( s \) of Bob’s swap-tests to pass is

$$\Pr[\text{Eve fools Bob on first attempt, using } t \text{ copies}] \leq (1 - \frac{1}{8(t+1)})^s,$$

as claimed in Lines (8) and (9). This completes the proof of security of the protocol under the two simplifying assumptions mentioned at the beginning of Section 3. Next, we show how to remove these assumptions.

### 3.5 Removing the simplifying assumptions

Recall the two simplifying assumptions: (1) Eve never passively monitors any protocol instances between Alice and Bob, and (2) Eve never participates in the protocol as a verifier. With regard to the first assumption, note that Eve only sees uniformly random bits when passively monitoring any protocol instance between Alice and Bob, and thus does not gain any useful information in doing so. For the second assumption, note that Eve can at best extract one extra copy of the public key from Alice when Eve follows the verifier protocol honestly, for a maximum of \( r \) extra copies (recall Alice only participates in the protocol \( r \) times before refreshing her keys). Thus, it follows that, in order to modify the protocol so that it is (fully) honest-verifier secure, we just need to have Alice choose the private key \( x \) uniformly from the larger set \([1, 2, \ldots, 2r + 1]\) with corresponding public-key-element \( |0\rangle + e^{2\pi i x/(2r+1)} |1\rangle\); this ensures that Alice’s private phase-angle looks to Bob and Eve like it was chosen uniformly from \([0, 2\pi)\) (recall Section 3.1). For the corresponding modified analysis, we just need to assume
that Eve has $r$ additional copies of the public key; ultimately, this only changes the constant in Line 11 from 8 to 16. Thus, the security of the modified protocol under the honest-verifier assumption is asymptotically equivalent (in terms of the relationship between $r$ and $s$) to that of the original protocol under the two simplifying assumptions.

Acknowledgements

We acknowledge useful discussions with Daniel Gottesman and Rob Spekkens. L. M. Ioannou was partially supported by EPSRC and SCALA. M. Mosca was partially supported by NSERC, DTO-ARO, CFI, CIFAR, Ontario-MRI, CRC, OCE, QuantumWorks and MITACS.

References

[1] Stephen D. Bartlett, Terry Rudolph, and Robert W. Spekkens. Decoherence-full subsystems and the cryptographic power of a private shared reference frame. Phys. Rev. A, 70:032307, 2004.

[2] Ivan Damgaard, Serge Fehr, Louis Salvail, and Christian Schaffner. Cryptography in the bounded quantum-storage model. In IEEE Press, editor, Proceedings of the 46th IEEE Symposium on Foundations of Computer Science - FOCS 2005, pages 449–458, 2005.

[3] Ivan Damgaard, Serge Fehr, Louis Salvail, and Christian Schaffner. Secure identification and QKD in the bounded-quantum-storage model. CRYPTO 2007, Lecture Notes in Computer Science, 4622:342–359, 2007.

[4] Daniel Gottesman and Isaac L. Chuang. Quantum digital signatures, 2001. quant-ph/0105032.

[5] Daniel Gottesman. 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

[6] Akinori Kawachi, Takeshi Koshiba, Harumichi Nishimura, and Tomoyuki Yamakami. Computational indistinguishability between quantum states and its cryptographic application. In Advances in Cryptology EUROCRYPT 2005, volume 3494 of Lecture Notes in Computer Science, pages 268–284. Springer, 2005. full version at http://arxiv.org/abs/quant-ph/0403069
[7] Masahito Hayashi, Akinori Kawachi, and Hirotada Kobayashi. Quantum measurements for hidden subgroup problems with optimal sample complexity. *Quantum Information and Computation*, 8:0345–0358, 2008.

[8] Subhash Kak. A three-stage quantum cryptography protocol. *Foundations of Physics Letters*, 19:293–296, 2006.

[9] Georgios M. Nikolopoulos. Applications of single-qubit rotations in quantum public-key cryptography. *Phys. Rev. A*, 77:032348, 2008. see also Phys. Rev. A. 78, 019903.

[10] Stephen D. Bartlett, Terry Rudolph, Robert W. Spekkens, and Peter S. Turner. Degradation of a quantum reference frame. *New J. Phys.*, 8:58, 2006.

[11] O. Goldreich. *Foundations of cryptography (Volume I): Basic tools*. Cambridge University Press, Cambridge, 2001.

[12] Wim van Dam, G. Mauro D’Ariano, Artur Ekert, Chiara Macchiavello, and Michele Mosca. Optimal phase estimation in quantum networks. *Journal of Physics A: Mathematical and Theoretical*, 40:7971–7984, 2007.

[13] Stephen D. Bartlett, Terry Rudolph, and Robert W. Spekkens. Reference frames, superselection rules, and quantum information. *Rev. Mod. Phys.*, 79(555), 2007.

[14] Donny Cheung. Unpublished notes, 2009.