Attack strategies for position-based quantum cryptography based on the Clifford Hierarchy

Kaushik Chakraborty and Anthony Leverrier
*Inria, EPI SECRET, B.P. 105, 78153 Le Chesnay Cedex, France**

The goal of position-based cryptography is for an honest party to use her spatio-temporal position as her only credential in a cryptographic protocol. In particular, Position-Verification aims at verifying that a certain party, called the prover, holds a given position in space-time. Such a protocol typically goes as follows: a set of verifiers will coordinate and send some challenge to the prover, and it is expected that only someone sitting in the supposed position of the prover can successfully pass the challenge.

Two papers established that information theoretic security is not possible for Position-Based Quantum Cryptography (PBQC) protocols: neither in the classical [1], nor in the quantum [2] regime. More precisely, it is always possible for a *coalition* of adversaries to convince the verifiers, even if none of the adversary sits in the spatio-temporal region where the prover is supposed to be. At the same time, the best known attack strategies require the adversaries to share very entangled states: the attacks described in [2] are based on Vaidman's protocol for nonlocal computation [3] and consist in the cheaters teleporting some quantum state back and forth, with a total cost in terms of required EPR pairs that scales double exponentially in n, the number of qubits involved in the PBQC protocol. Later, new generic attacks based on port-based teleportation[4] were proposed and require only exponential entanglement to succeed [5]. Finally, it is also know that a linear amount of entanglement is not sufficient to break the PBQC protocol [5], [6].

A major open question in the field is to bridge the gap between lower and upper bounds: does there exist a protocol that requires exponentially many EPR pairs to break, or are all PBQC protocols insecure against a coalition of adversaries that shares polynomially many EPR pairs? While we do not settle this question in the present paper, we make some progress towards it by exhibiting new attack strategies with polynomial complexity against a large family of practical protocols. These attacks rely on teleportation gates and their precise complexity can be quantified with the notion of *Clifford hierarchy* [7] of a quantum gate. We then introduce a new family of protocols, that generalizes a construction by Lau and Lo [8], which appears to be immune against these polynomial-complexity attacks.

Another main challenge is to determine whether there exist some PBQC protocol resistant to channel imperfections, either losses or noise, between the verifiers and the prover. Some approach was recently developed in [9]. Here, we argue that our new protocols provide an alternative route towards loss tolerance because the quantum part of the challenge can be distributed to the prover in advance compared to the classical part of the challenge. Therefore, the protocol becomes loss-tolerant provided that the honest parties have access to reasonably good quantum memories.

* kaushik.chakraborty@inria.fr,anthony.leverrier@inria.fr

I. PBQC PROTOCOLS

For simplicity, we mainly focus on one-dimensional protocols where two verifiers V_0 and V_1 aim at verifying the position of a prover P located between them. Moreover, without loss of generality, we can always assume that the position P is exactly at the middle of V_0 and V_1 and that it takes one unit of time for light to travel from V_0 (or V_1) to P.

In this one-dimensional case, a coalition of cheaters consists of two players, Alice and Bob, whose goal is to win a distributed game G where their respective input is the challenge part given by V_0 or V_1, and their output should match that of a honest prover.

A. Protocol Family 1

Our first family of protocols corresponds to games denoted by $G_1(n,\mathcal{U},\eta)$ where n refers to the number of qubits involved in the protocol, $\mathcal{U}$ is a set of n-qubit unitaries, and η is the tolerance threshold.

1. The verifier V_0 chooses an n-qubit unitary operator $U \in_R \mathcal{U}$ and an n-bit string $x = (x_1, \ldots, x_n) \in_R \{0,1\}^n$. V_0 prepares $|\psi\rangle = U|x\rangle$, where $|x\rangle = \bigotimes_{i=1}^n |x_i\rangle$, and $|0\rangle$, $|1\rangle$ correspond to the computational basis. V_0 sends x and U to V_1 through some secure authenticated classical channel.

2. V_0 sends the n qubit quantum state $|\psi\rangle$ to prover P at time 0. V_1 sends the unitary U to P at time $t = 0$

3. The prover P receives both $|\psi\rangle$ and U at time $t = 1$. After receiving $|\psi\rangle$ and U, prover P computes $U^\dagger|\psi\rangle = |x\rangle$, where $x \in \{0,1\}^n$ and measures it in computational basis, obtaining some outcome string y. P then sends back y to both V_0 and V_1.

4. The prover P wins the game if V_0 and V_1 receive the same string y at time $t = 2$, and if the Hamming distance between x and y is less than ηn: $d_H(x,y) \leq \eta n$.

B. Protocol Family 2

Our second family of protocols, denoted by $G_2(n,t,\eta)$, is based on interleaved group product. Here, we assume single-qubit gates and t refers to the size of the product of such unitaries that the prover will need to implement. More formally, we have:

1. V_0 chooses a random bit string $x \in_R \{0,1\}^n$ and $2t$ single-qubit unitaries: $u_1, \ldots u_t, v_1, \ldots, v_t$ and informs V_1 of these choices thanks to a secure authenticated classical channel. V_0 prepares the n-qubit state $|\psi\rangle = \bigotimes_{i=1}^n U|x_i\rangle$ where $U = \prod_{i=1}^t u_i v_i$.
2. At time $t = 0$, V_0 sends the state $|\psi\rangle$ as well as the classical description of $(u_1, \ldots, u_t)$ to the prover, and V_1 sends the classical description of $(v_1, \ldots, v_t)$ to P.
3. At time $t = 1$, the prover receives $|\psi\rangle$, computes $U = \prod_{i=1}^t u_i v_i$, applies $(U^\dagger)^{\otimes n}$ to $|\psi\rangle$ and measures the resulting state in the computational basis, obtaining some outcome $y \in \{0,1\}^n$, which is sent to both V_0 and V_1.
4. The prover P wins the game if V_0 and V_1 both receive an identical string y at time $t = 2$, and if $d_H(x,y) \leq \eta n$.

Interestingly for this protocol, the honest prover is only required to measure a qubit in a given basis, which is quite practical. We note that a similar family of protocols was considered in [8], but more verifiers were considered, which made the protocol less practical. Here we make the choice that the same unitary U is applied to all the qubits. A variant of the protocol would be to send n successive challenges to the prover, with n different choices for the unitary.

In order to fully define this protocol, we need to choose a measure on the set of single-qubit unitaries, corresponding to the random choice of $u_1, \ldots, u_t, v_1, \ldots v_t$ and u. We choose the Haar measure on the unitary group $U(2)$ in the following sense:

- U is chosen from the Haar measure on $U(2)$.
- $u_1, \ldots, u_t, v_1, \ldots, v_{t-1}$ are chosen independently from the Haar measure on $U(2)$.
- v_t is computed as $v_t = u_t v_{t-1} u_{t-1} \cdots v_1 u_1 U$.

In fact, for a practical implementation, each of the unitary should be described with a given (finite) level of accuracy, meaning that describing a unitary is done with say m bits. We ignore this subtlety in the present paper.

II. ATTACKS BASED ON THE CLIFFORD HIERARCHY FOR THE FIRST FAMILY

The *Clifford Hierarchy* introduced in [7] is an infinite hierarchy of sets $C_1(n) \subset C_2(n) \subset \cdots \subset C_k(n) \cdots$ of n-qubit unitaries where $C_1(n) = \mathcal{P}_n$ corresponds to the Pauli group (on n qubits), and the higher levels are defined recursively by:

$$U \in C_{k+1}(n) \text{ iff } U\sigma U^\dagger \in C_k(n) \text{ for all } \sigma \in C_1(n).$$

When n is clear from context, we simply write C_k instead of $C_k(n)$ for the k^{th} level of the Clifford hierarchy for n-qubit gates. It should be noted that the first two levels of the hierarchy are groups, namely the Pauli and the Clifford groups, whereas none of the higher levels are groups.

We define the *Clifford complexity* of the set $\mathcal{U}$ denoted by $\text{CliffCompl}(\mathcal{U})$ to be the minimum number of EPR pairs that Alice and Bob must share to perfectly win the game $G_1(n,\mathcal{U},1)$.

It is easy to see that if the unitary U is a Pauli matrix, then Alice and Bob can win the game $G(n,1,1)$ without sharing any entanglement because $|\psi\rangle$ is also a basis state $|y\rangle$. The two strings x and y coincide on the qubits for which U is the identity or a Z Pauli matrix, and differ for the other qubits. Therefore, Alice simply needs to measure $|\psi\rangle$ in the computational basis and to forward her results to Bob, who can recover the correct string x using his knowledge of U. This shows that

$$\text{CliffCompl}(C_1(n)) = 0.$$

If the unitary U belongs to the Clifford group C_2, then Alice and Bob can again win the game perfectly if they share n EPR pairs. The idea is for Alice to teleport the state $|\psi\rangle$ to Bob using the n EPR pairs. Bob obtains the state $\sigma|\psi\rangle$ where $\sigma \in C_1$ is a Pauli correction. Applying the unitary $U^\dagger$ to his state, Bob obtains

$$U^\dagger \sigma U U^\dagger |\psi\rangle = U^\dagger \sigma U |x\rangle,$$

where $U^\dagger \sigma U \in C_2$. This means that Bob simply needs to measure his state in the computational basis, and forward his result to Alice. Once they know both the value of σ and the result of the measurement, both Alice and Bob are able to recover the correct value of the string x and they win the game. This proves that

$$\text{CliffCompl}(C_2(n)) \leq n.$$

If the unitary U to be implemented belongs to the k^{th} level of the Clifford hierarchy, then Alice and Bob can apply an iterative procedure that still allows them to win the game perfectly. We show that

Theorem 1.

$$\text{CliffCompl}(C_k(n)) \leq 4n\, 4^{n(k-2)}. \tag{1}$$

The attack is general and works for any n-qubit gate in some given level of the Clifford hierarchy. In the context of PBQC protocols, however, the interesting set of gates $\mathcal{U}$ from which the unitary to be implemented is chosen, is often more restricted. Indeed, if the protocol is

to be practical, then a honest prover should be able to implement the unitaries reasonably efficiently. For this reason, it is interesting to consider unitaries described by quantum circuits.

In a practical scenario, where the quantum states given to Alice are photonic qubits, it makes sense to consider photonic implementations for the quantum circuit, and therefore to consider unitaries with a fixed layout for the quantum circuit, and adjustable single and two-qubit gates. This is typically the case for experimental implementations based on integrated photonics [10].

For this reason, the set $\mathcal{U}$ of unitaries considered in the first family of protocols could be described by a fixed layout, and a specific unitary $U \in \mathcal{U}$ is then described by giving the value of each single or two-qubit gate in the layout. For a quantum circuit based on linear optics, the layout $\mathcal{L}$ corresponds to the position of the phase-shifters and beamsplitters, and the unitary is given by the specific values of the phase-shifts and transmission of the beamsplitters.

We are interested in the complexity of attacks for such schemes as a function of the depth and width of such quantum circuits and prove:

Theorem 2. *Let $\mathcal{L}$ be the layout of a quantum circuit acting on n-qubit state of depth d and consisting of at most r-qubit gates in C_k. Then* $\mathrm{CliffCompl}(\mathcal{U}_{\mathcal{L}}) \leq 4^{rd(k-2)} \times (4rn)^d$.

III. SECOND FAMILY OF PROTOCOLS

By construction, the second family of protocols seems to be immune against the previous attacks: each gate is chosen from the Haar measure (i.e. not from some low level of the Clifford hierarchy) and the circuit has large depth. We study two attack strategies for these protocols, using either port-based teleportation, or the previous attacks together with the Solovay-Kitaev theorem to approximate any gate by a product of gates in C_2 or C_3. Both attacks have exponential complexity.

Theorem 3. *Port-based teleportation provides an attack strategy against $G_2(n, t, 1 - \epsilon)$ that requires $\exp(O(t \log(t/\epsilon)))$ EPR pairs.*

Theorem 4. *The Clifford hierarchy together with the Solovay-Kitaev approximation provide an attack against $G_2(n, t, 1-\epsilon)$ that requires $2^{4t \log^c(\frac{2t}{\epsilon})} n$ EPR pairs, where $c < 3$ and $\eta = \epsilon$.*

In addition to their inherent security against all known attacks strategies, the protocol from the second family can be straightforwardly modified to be made loss-tolerant. The crucial point to note here is that these protocols appear to remain secure even if the quantum state is distributed in advance compared to the classical information required to decide in which basis to measure the state. From this observation, we propose the following modification of these protocols:

In addition to the verifiers, there is a central "bank" of quantum states available to the prover. This bank (whose role can be played by the verifiers) distributes quantum states, along with some identification number, to interested parties. The value of the states is not revealed to the client but the verifiers have access to a complete listing of pairs: (state ID/ state value). When a prover wants to play a PBQC game, she should therefore obtain a quantum state from the bank, put it in a quantum memory, and then inform the verifiers of the state ID. Then, the verifiers can apply the usual protocol, with the exception that the state $|\psi\rangle$ does not need to be distributed since the game is played with the state the prover obtained from the bank.

It seems to us that these modified protocols are as secure as the original ones. More precisely, we could not think of any attack working against the modified version that would not also work against the original version.

The advantage of this modified version is that the quantum channel between the verifiers and the prover is replaced by the quantum memory of the prover. This can be quite advantageous in a scenario where the physical distance between the verifiers and the prover is large, meaning that fiber optics communication would lead to high losses, provided that the prover has access to a good quantum memory.

[1] N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky, in *Advances in Cryptology-CRYPTO 2009* (Springer, 2009) pp. 391–407.

[2] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner, in *Advances in Cryptology–CRYPTO 2011* (Springer, 2011) pp. 429–446.

[3] L. Vaidman, Phys. Rev. Lett. **90**, 010402 (2003).

[4] S. Ishizaka and T. Hiroshima, Physical review letters **101**, 240501 (2008).

[5] S. Beigi and R. König, New Journal of Physics **13**, 093036 (2011).

[6] M. Tomamichel, S. Fehr, J. Kaniewski, and S. Wehner, in *Advances in Cryptology–EUROCRYPT 2013* (Springer, 2013) pp. 609–625.

[7] D. Gottesman and I. L. Chuang, Nature **402**, 390 (1999).

[8] H.-K. Lau and H.-K. Lo, Physical Review A **83**, 012322 (2011).

[9] B. Qi and G. Siopsis, arXiv preprint arXiv:1502.02020 (2015).

[10] J. L. O'Brien, A. Furusawa, and J. Vučković, Nature Photonics **3**, 687 (2009).

Attack strategies for position-based quantum cryptography based on the Clifford Hierarchy (Full version)

Kaushik Chakraborty[*], Anthony Leverrier[†]

1 Introduction

The goal of position-based cryptography is for an honest party to use her spatio-temporal position as her only credential in a cryptographic protocol. In particular, Position-Verification aims at verifying that a certain party, called the prover, holds a given position in space-time. Such a protocol typically goes as follows: a set of verifiers will coordinate and send some challenge to the prover, and it is expected that only someone sitting in the supposed position of the prover can successfully pass the challenge.

Such protocols have been studied in the classical setting where the challenges are described by classical information, and it was shown by [1] that information-theoretic security could never be obtained in the standard (Vanilla) model. More precisely, it is always possible for a *coalition* of adversaries to convince the verifiers, even if none of the adversary sits in the spatio-temporal region where the prover is supposed to be. Note, however, that the same paper gives secure constructions in the Bounded-Retrieval Model, which is a variant of the Bounded-Storage Model.

A possible way-out of this no-go theorem would be to consider a quantum setting. Indeed, several classical tasks which are known to be impossible in the classical domain can be achieved in the quantum domain: this is the case for instance of secret key expansion [2], randomness amplification [3] or randomness expansion [4].

Position-based cryptography in the quantum setting was first investigated under the name of *quantum tagging* by Kent around 2002, but only appeared in the literature much later in [5] where attacks against possible quantum constructions are described. Malaney independently introduced a quantum position verification scheme in [6]. An example of a quantum protocol for position verification is one with two verifiers: one sending a qubit $|\phi\rangle = U|x\rangle$ with $x \in \{0, 1\}$ and U some unitary, and the second verifier sending a classical description of the unitary U. The task for the prover is then to measure the qubit in the basis $\{U|0\rangle, U|1\rangle\}$ and to return the classical value of x to both provers. There are many variations around this protocol, and the intuition for the possible security of such protocols is that only someone sitting in P can obtain both U and $|\phi\rangle$, perform the required measurement, and return the correct value x on time.

In [7] Lau and Lo extended the attack from [5] to show that the above intuition is only correct if the unitary U is not a *Clifford* gate. Otherwise, a couple of cheaters, Alice lying between V_0 and P, and Bob lying between V_1 and P, can always fool the verifiers provided that they share a small number of EPR pairs. This result was later extended by Buhrman *et al.* [8] who showed that

[*]Inria, EPI SECRET, B.P. 105, 78153 Le Chesnay Cedex, France. Email: kaushik.chakraborty@inria.fr.
[†]Inria, EPI SECRET, B.P. 105, 78153 Le Chesnay Cedex, France. Email: anthony.leverrier@inria.fr.

such an attack always exists for any Position-Based quantum protocol, provided that the coalition of cheaters share sufficiently many EPR pairs: no quantum position-based quantum cryptographic protocol can display information-theoretic security.

Two general families of attacks have been considered in the literature so far, both based on quantum teleportation. The first attack is inspired by Vaidman's protocol for nonlocal computation [9] and consists of the cheaters teleporting some quantum state back and forth, with the number of exchanges depending on the success probability of the attack. If the position-based protocol involves n qubits, the resource (number of EPR pairs) required for this type of attacks to succeed typically scales double-exponentially with n. Another class of attacks uses *port-based* teleportation [10] and requires only exponential entanglement to succeed [11]. If one could prove that such an attack was indeed optimal, one would obtain a secure position-based protocol for all practical purposes.

A different class of position-based verification protocols based on the nonlocal computation of Boolean functions was introduced by Buhrman *et al.* in [12], for which they suggested a new type of attacks based on the *Garden-hose complexity* of the Boolean function. They showed in particular that finding an explicit Boolean function with polynomial circuit complexity (so that the honest prover can compute it) but exponential attack complexity in the garden-hose model is at least as difficult as separating the classes of languages P and L, corresponding respectively to decision problems decidable in polynomial time or logarithmic space. This result was recently extended by Klauck and Podder who showed that explicit Boolean functions on k variables with Garden-hose complexity $\Omega(k^{2+\epsilon})$ will be hard to obtain [13].

Concerning lower-bounds, it has been established that a constant or even linear amount of entanglement shared by the cheaters is not sufficient to break the security of the protocol [11], [14]. Moreover, Unruh has shown that security could be established in the quantum random oracle model [15]. In other words, security can be obtained provided one has access to one-way functions.

Recently, Qi and Siopsis initiated the study of imperfections in quantum position-based schemes, in particular in the presence of losses in the quantum channel between the verifiers and the prover [16].

In this paper, we investigate the family of protocols described above, where the state $|\phi\rangle$ and the unitary U are a general n-qubit states and unitary. We present some new attacks against such protocols that will be efficient as soon as the protocol is practical for the honest prover. We also introduce a second family of protocols that seems to be immune against such attacks.

2 PBQC Protocols

For simplicity, we mainly focus on one-dimensional protocols where two verifiers V_0 and V_1 aim at verifying the position of a prover P located between them. Moreover, without loss of generality, we can always assume that the position P is exactly at the middle of V_0 and V_1 and that it takes one unit of time for light to travel from V_0 (or V_1) to P.

Roughly speaking, a general PCQB protocol consists of three distinct phases:

- *the preparation phase*, where V_0 and V_1 prepare a challenge for the prover. The challenge typically involves a quantum state (usually an n-qubit state in the protocols considered in the present paper) as well as some classical information. The challenge is always given to the prover in a distributed fashion, one part coming from V_0, the other part coming from V_1.

- *the execution phase*, during which V_0 and V_1 send their respective share of the challenge towards the prover P, who executes the task she is given, and returns her answer to the

verifiers.

- *the verification phase*, during which the verifiers check that (i) the answer is correct, and that (ii) they received it not more than two time units after the beginning of the protocol. This assumes the idealized scenario where all communications are performed at the speed of light, and local computation take negligible time. Even in that idealized scenario, it makes sense to allow the honest prover to err a small fraction of the time. For this reason, the provers accept the answer if it meets some tolerance threshold η.

We note that some protocols investigated in the literature, for instance in **??**, allow the prover to sometimes reply that she did not received the quantum state (because of losses). In that case, one adds a second tolerance threshold corresponding to the minimum fraction of challenges answered by the prover. In the present paper, for simplicity, we require the prover to always give an answer to each challenge.

We will consider two families of PBQC protocols:

1. in the first family, V_0 sends a n-qubit state and V_1 sends the classical description of a measurement basis, and the prover is required to measure the state in the correct measurement basis and to communicate the outcome to both verifiers;

2. the second family of protocols is based on *interleaved group product*: V_0 sends an n-qubit state as well as a sequence of unitaries $u_1, \ldots, u_t$, V_1 sends a sequence of unitaries $v_1, \ldots, v_t$ and the prover is supposed to measure the state in the basis corresponding to $\prod u_i v_i$.

We note that the first family of protocols has been widely discussed in the literature (for instance in [17] or [7], but that the second family appears to be reasonably new (even if similar protocols, with more verifiers, were considered in [7]). Let us also point out that the interleaved group product has been considered in the communication complexity literature, for instance in a recent paper by Gowers and Viola [18].

Before defining these protocols more formally, let us comment on some assumptions we make here. In this paper, our main goal is to present some natural PBQC protocols and to study general classes of attacks that can be carried out by coalitions of cheaters. While we try to be as general as possible, we think it is sensible to make some specific choices in order to simplify the analysis. For instance, we restrict our protocols to using qubit states, and more importantly, we consider one-dimensional protocols with only 2 verifiers. Most of our analysis would carry through to arbitrary qudit protocols involving many verifiers. We also decided to leave aside all the problems related to timing in order to focus on the genuinely quantum part of the procedure. This means that we consider that all communication (classical or quantum) is performed at the speed of light, and that all computation is instantaneous. These are obviously unrealistic assumptions, but dealing with more realistic ones can be done independently as the analysis we provide here (see for instances the work of Kent [19]). The main source of imperfection in a PBQC protocol is the quantum channel between the verifiers and the prover, which can never be assumed to be perfect. In general, the channel is both lossy and noisy, which is why even an ideal prover cannot possibly pass the test perfectly. On the other hand, it makes sense to assume that the classical channels are essentially perfect (lossless and noiseless).

Following the literature, we will find it useful to describe the various protocols in terms of distributed collaborative games, where two players, named Alice and Bob (corresponding to the coalition of cheaters), independently receive some query from some referee, are allowed a single round of (bipartite) communication and need to output some answer. The games considered here all share the property that if Alice and Bob can communicate arbitrarily, then they have a trivial

winning strategy. The main result of [8] is that it implies that one round of communication is in fact sufficient, provided that Alice and Bob are sufficiently entangled.

Let us now formally define the two families of protocols that will be considered in this paper.

2.1 Protocol Family 1

Our first family of protocols corresponds to games denoted by $G_1(n,\mathcal{U},\eta)$ where n refers to the number of qubits involved in the protocol, $\mathcal{U}$ is a set of n-qubit unitaries, and η is the tolerance threshold. We will also write $G_1(n,k,\eta)$ when the set $\mathcal{U}$ is a subset of C_k, the k^{th} level of the Clifford hierarchy (see Section 3 for a definition).

Preparation Phase:

1. The verifier V_0 chooses an n-qubit unitary operator $U \in_R \mathcal{U}$ and an n-bit string $x = (x_1,\ldots,x_n) \in_R \{0,1\}^n$. V_0 prepares $|\psi\rangle = U|x\rangle$, where $|x\rangle = \bigotimes_{i=1}^n |x_i\rangle$, and $|0\rangle$, $|1\rangle$ correspond to the computational basis.
2. V_0 sends x and U to V_1 through some secure authenticated classical channel.

Execution Phase:

1. V_0 sends the n qubit quantum state $|\psi\rangle$ to prover P at time 0. V_1 sends the unitary U to P at time $t = 0$
2. The prover P receives both $|\psi\rangle$ and U at time $t = 1$.
3. After receiving $|\psi\rangle$ and U, the honest prover P computes $U^\dagger|\psi\rangle$ and measures it in computational basis, obtaining some outcome string y. P then sends back y to both V_0 and V_1.

Verification Phase:

1. The prover P wins the game if V_0 and V_1 receive the same string y at time $t = 2$, and if the Hamming distance between x and y is less than ηn: $d_H(x,y) \leq \eta n$.

In the literature, this first family is often considered in the single qubit case. Then it makes sense to repeat the protocol n times in order to build some statistics. In our case, we aim at giving a more general picture of the possible attacks working against this scheme and consider n-qubit gates. Unfortunately, given the present experimental state-of-the-art for quantum computation, this first family is rather unrealistic in the honest prover case for n larger than 2. This practicality issue leads us to consider our second family of protocols, with the hope that they are much easier to implement experimentally.

2.2 Protocol Family 2

Our second family of protocols corresponds to games $G_2(n,t,\eta)$ and is based on interleaved group product. Here, we assume single-qubit gates and t refers to the size of the product of such unitaries that the prover will need to implement. More formally, we have:

Preparation Phase:

1. V_0 chooses a random bit string $x \in_R \{0,1\}^n$ and $2t$ single-qubit unitaries: $u_1, \ldots u_t, v_1, \ldots, v_t$ and informs V_1 of these choices thanks to a secure authenticated classical channel.

2. V_0 prepares the n-qubit state $|\psi\rangle = \bigotimes_{i=1}^n U|x_i\rangle$ where $U = \prod_{i=1}^t u_i v_i$.

Execution Phase:

1. At time $t = 0$, V_0 sends the state $|\psi\rangle$ as well as the classical description of $(u_1, \ldots, u_t)$ to the prover, and V_1 sends the classical description of $(v_1, \ldots, v_t)$ to P.

2. At time $t = 1$, the prover receives $|\psi\rangle$, computes $U = \prod_{i=1}^t u_i v_i$, applies $(U^\dagger)^{\otimes n}$ to $|\psi\rangle$ and measures the resulting state in the computational basis, obtaining some outcome $y \in \{0,1\}^n$, which is sent to both V_0 and V_1.

Verification Phase:

1. The prover P wins the game if V_0 and V_1 both receive an identical string y at time $t = 2$, and if $d_H(x, y) \leq \eta n$.

Interestingly for this protocol, the honest prover is only required to measure a qubit in a given basis, which is quite practical. We note that a similar family of protocols was considered in [7], but more verifiers were considered, which made the protocol less practical. Here we make the choice that the same unitary U is applied to all the qubits. A variant of the protocol would be to send n successive challenges to the prover, with n different choices for the unitary.

In order to fully define these protocols, we need to choose a measure on the set of single-qubit unitaries, corresponding to the random choice of $u_1, \ldots, u_t, v_1, \ldots v_t$ and u. We choose the Haar measure on the unitary group $U(2)$ in the following sense:

- U is chosen from the Haar measure on $U(2)$.
- $u_1, \ldots, u_t, v_1, \ldots, v_{t-1}$ are chosen independently from the Haar measure on $U(2)$.
- v_t is computed as $v_t = u_t v_{t-1} u_{t-1} \cdots v_1 u_1 U$.

In fact, for a practical implementation, each of the unitary should be described with a given (finite) level of accuracy, meaning that describing a unitary is done with say m bits. We ignore this subtlety in the present paper.

3 Preliminaries

In this section, we fix the notation and review some technical notions needed for the rest of the paper.

A recurring theme of this paper concerns techniques allowing distant parties to implement some given unitary operation described in a distributed setting. We will mainly use two concepts: standard teleportation and its link to the Clifford hierarchy, as well as port-based teleportation.

3.1 The Clifford Hierarchy

The *Clifford Hierarchy* introduced in [20] is an infinite hierarchy of sets $C_1(n) \subset C_2(n) \subset \cdots \subset C_k(n) \cdots$ of n-qubit unitaries where $C_1(n) = \mathcal{P}_n$ corresponds to the Pauli group (on n qubits), and the higher levels are defined recursively by:

$$U \in C_{k+1}(n) \text{ if and only if } U\sigma U^\dagger \in C_k(n) \text{ for all } \sigma \in C_1(n).$$

When n is clear from context, we simply write C_k instead of $C_k(n)$ for the k^{th} level of the Clifford hierarchy for n-qubit gates. It should be noted that the first two levels of the hierarchy are groups, namely the Pauli and the Clifford groups, whereas none of the higher levels are groups.

The gates from C_1 and C_2 can be "easily" implemented fault tolerantly [21]. However, it is well known that they do not form a universal set for quantum computation. One therefore requires at least one gate from C_3 to obtain a universal set of gates. Not surprisingly, gates from C_3 or higher levels are usually much harder to implement fault-tolerantly.

3.2 Teleportation Gates

Teleportation gates are a tool introduced by Gottesman and Chuang [20] to implement a unitary operator U on any state provided that one can apply it to a special state. In particular, teleportation and the ability to perform single qubit operators are sufficient to obtain (fault-tolerant) universal quantum computation.

The main idea relies on the fact that if one uses the state $(I \otimes U)|\Phi^+\rangle$ instead of $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ to teleport a quantum state $|\psi\rangle$ then the teleported state will be of the form $U|\psi\rangle$ (up to some Pauli correction). To implement an n-qubit quantum gate $U \in C_3$, one first prepares the state $|\Psi_U^n\rangle = (I \otimes U)|\Phi^+\rangle^{\otimes n}$. Let $|\psi\rangle$ be an unknown state on which U has to be applied. Then taking $|\psi\rangle$ and performing a Bell basis measurement on $|\psi\rangle$ and on the first register of $|\Psi_U^n\rangle$ leaves n qubits in the state $|\psi_{\text{out}}\rangle = UR|\psi\rangle = R^1U|\psi\rangle$, where the correction $R \in C_1$ is a Pauli operator and $R^1 = URU^\dagger \in C_2$. Since $R^1 \in C_2$, its inverse can easily be implemented, thus giving the state $U|\psi\rangle$. Hence, using only n EPR pairs, one can implement any n-qubit quantum gate from C_3 provided that the state $|\Psi_U^n\rangle$ can be prepared efficiently.

If U belongs to some higher level C_k with $k > 3$ of the Clifford hierarchy, then one can apply the technique outlined above iteratively for $k-2$ steps. Indeed, in that case, the correction R^1 belongs to C_{k-1}. It should be clear that higher levels of the hierarchy require more teleportation steps and Bell measurements.

3.3 Semi-Clifford Gates

Semi-Clifford gates are another special type of gates with different structural properties than the gates in Clifford hierarchy. The concept of semi-Clifford gates was first introduced for the single-qubit case by D. Gross and M. Van den Nest in [22], and generalized to n-qubit states by Zeng *et al* in [23].

Definition 1. *An n-qubit unitary operation is called* semi-Clifford *if it sends by conjugation at least one maximal abelian subgroup of $\mathcal{P}_n$ to another maximal abelian subgroup of $\mathcal{P}_n$.*

In particular, if U is an n-qubit semi-Clifford operation, then there must exist at least one maximal abelian subgroup G of $\mathcal{P}_n$, such that $UGU^\dagger$ is another maximal abelian subgroup of $\mathcal{P}_n$. While the general structure of the semi-Clifford gates is not yet completely understood for arbitrary n, we have a characterization for $n = 1, 2$ and a partial characterization for $n = 3$.

Theorem 2 (from [23]). *The gates in $C_k(1), C_k(2)$ are semi-Clifford for all k. For $n = 3$, all the gates in $C_3(3)$ are semi-Clifford.*

In our work, semi-Clifford gates will be of interest as they allow the cheaters to perform more efficient attack strategies for the second family of protocols.

3.4 Port-based teleportation

Port-based teleportation is a specific teleportation scheme introduced in [10], that allows *Alice* to teleport an arbitrary quantum state to Bob, using many EPR pairs, called *ports*. After Alice's measurement on her state and her half of the EPR pairs, the state is teleported (approximately) to one of Bob's port, known to Alice. Alice simply sends this classical information to Bob, who only needs to trace out the other ports to recover Alice's state. The main feature of this teleportation scheme is that apart from tracing out some registers, Bob needs not apply any correction to the state. The fidelity $F_p(|\Psi^{\text{in}}\rangle, |\Psi^{\text{out}}\rangle)$ between Alice's initial state and Bob's final state using port-based teleportation depends on both the number N of EPR pairs consumed in the scheme and the dimension d of Alice's state. The following lower-bound was established in [24].

Lemma 3 (from [24]).

$$F_p(|\Psi^{\text{in}}\rangle, |\Psi^{\text{out}}\rangle) \geq 1 - \frac{d^2}{N}. \tag{1}$$

3.5 Quantum cloning

While it is well-known that cloning an unknown quantum state exactly is forbidden by the unitary of quantum theory, approximate quantum cloning is not ruled out (see [25] and [26] for reviews on quantum cloning). In particular, $N \to M$ quantum cloning is the task where one receives N copies of an unknown state and should prepare $M > N$ copies of this state, as close as possible to the input state.

Werner [27] and Keyl and Werner [28] established that the fidelity of optimal $N \to M$ universal cloning machines for d-dimensional states is given by:

$$F_{N\to M}(d) = \frac{M(N+1) + (d-1)N}{M(N+d)}. \tag{2}$$

For our purpose, we will be interested in the case where $d = 2$, $N = 1$ and $M \to \infty$ which gives

$$F_{1\to\infty}(2) = \frac{2}{3}. \tag{3}$$

4 General attacks strategies against PBQC protocols

As was proved in [8], there always exists a working attack strategy against any PBQC protocol that allows a coalition of adversaries to perfectly impersonate the honest prover. In the case of the one-dimensional protocols considered in this paper, such a coalition consists without loss of generality of 2 players, Alice (A) and Bob (B), with Alice lying on the line between V_0 and P, and Bob lying between V_1 and P.

The attack strategies we will consider have the following structure:

1. Alice and Bob initially share a (possibly entangled) initial bipartite state ρ_{AB} of dimension to be specified later.

2. Alice intercepts the communication from V_0, namely a quantum register ρ_C (where C stands for challenge), as well as some classical information.

3. Bob intercepts the classical communication from V_1.

4. Depending on the classical information they received, Alice and Bob perform respectively a quantum measurement on their respective registers, AC and B.

5. They forward all the classical information as well as the outcomes of the measurement to their partner.

6. Finally, upon receiving this information, they prepare and send their response to the verifiers.

The main question of interest is to decide how the dimension of ρ_{AB}, and more particularly the entanglement of this state, scales with the parameters of the PBQC protocol.

This scenario allows us to see the cheating procedure as a distributed task, or game, where Alice and Bob are asked questions (possibly consisting of a quantum state), are allowed a single round of communication and are required to output some specific answer. They win the game if they fool the verifiers.

Let us interpret our two families of PBQC protocols in these terms.

Family 1

- **Input:** $|\psi\rangle = U|x\rangle$ for Alice, $U \in \mathcal{U}$ for Bob
- **Output:** $a \in \{0,1\}^n$ for Alice, $b \in \{0,1\}^n$ for Bob
- **Winning condition:** $a = b$ and $d_H(a,x) \leq \eta n$

Family 2

- **Input:** $|\psi\rangle = \bigotimes_{i=1}^n \left(\prod_{j=1}^t u_j v_j |x_i\rangle \right)$ and $(u_1, \ldots, u_t)$ for Alice, $(v_1, \ldots, v_t)$ for Bob
- **Output:** $a \in \{0,1\}^n$ for Alice, $b \in \{0,1\}^n$ for Bob
- **Winning condition:** $a = b$ and $d_H(a,x) \leq \eta n$

We now list a few questions of interest. In the perfect setting ($\eta = 1$), how many EPR pairs do Alice and Bob need to share to carry out a successful attack with high probability? One of the main open questions of the field is to find an explicit protocol that requires an exponential number of EPR pairs to break. At the other hand of the spectrum, what is the maximum value of η for which non entangled cheaters can win the game with high probability? A typical attack for non entangled cheaters will typically consist in Alice measuring the state in a random basis and forwarding her measurement outcome to Bob. It would also be interesting to understand the level of security when the cheaters share polynomially many EPR pairs.

5 Attacks for $\eta = 1$ based on the Clifford hierarchy

In this section, we first study attack techniques based on the Clifford hierarchy that can be applied by cheaters against the first family of protocols $G_1(n, \mathcal{U}, 1)$ in the case where the value of the tolerance threshold η is set to 1.

In particular, we will give explicit attacks which are efficient in the following relevant cases:

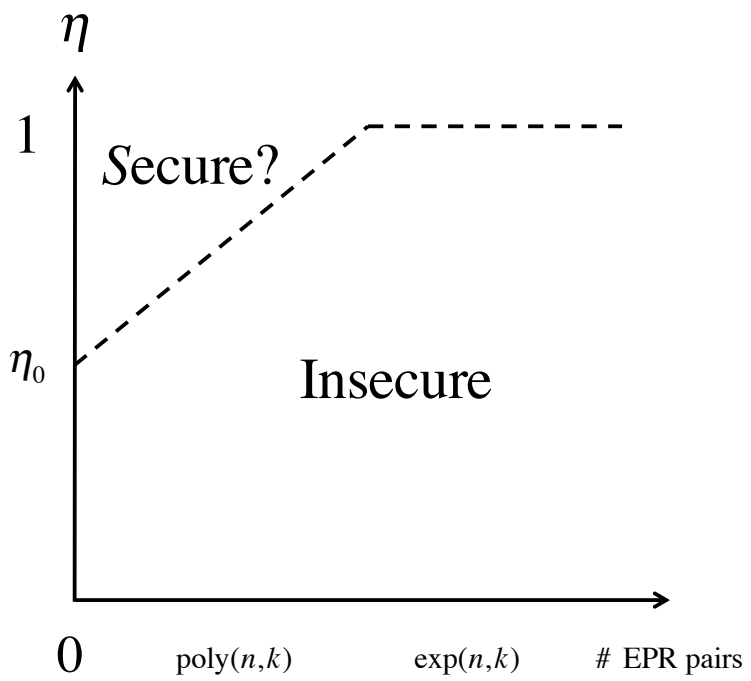

Figure 1: General picture for the security of a PBQC protocol: there exists some value η_0 such that even non-entangled cheaters can win a game for $\eta \leq \eta_0$. On the other hand, if η is set to 1, then an exponential number of EPR pairs makes the protocol insecure. The security in the regime where the cheaters share polynomially many EPR pairs is usually much less understood.

- if $\mathcal{U} \subseteq C_k(n)$, that is if the unitaries all belong to some low level of the Clifford hierarchy,
- if the unitaries in $\mathcal{U}$ can all be implemented with a quantum circuit with a fixed layout.

We note that these two cases correspond to protocols that appear to be practical for a honest prover. Indeed, gates in a low level of the Clifford Hierarchy are much easier to implement than arbitrary gates. Moreover, if the quantum states are photonic states, and the honest prover uses integrated photonics to implement the unitaries in $\mathcal{U}$, a fairly reasonable choice in practice, then it makes sense to fix some layout, that is an optical circuit consisting of single or 2-qubit gates for instance, and to obtain the family $\mathcal{U}$ by changing the value of the single and 2-qubit gates.

In both cases, our results show that there exists an efficient attack strategy for the coalition of cheaters.

5.1 A general attack for $\mathcal{U} = C_k$

Let us first define the *Clifford complexity* of a family $\mathcal{U}$ of unitaries.

Definition 4. *Let $\mathcal{U}$ be a set of n-qubit unitaries. We define the Clifford complexity of the set $\mathcal{U}$ denoted by* $\mathrm{CliffCompl}(\mathcal{U})$ *to be the minimum number of EPR pairs that Alice and Bob must share to perfectly win the game $G_1(n,\mathcal{U},1)$.*

It is easy to see that if the unitary U is a Pauli matrix, then Alice and Bob can win the game $G(n,1,1)$ without sharing any entanglement because $|\psi\rangle$ is also a basis state $|y\rangle$. The two strings x and y coincide on the qubits for which U is the identity or a Z Pauli matrix, and differ for the other

qubits. Therefore, Alice simply needs to measure $|\psi\rangle$ in the computational basis and to forward her results to Bob, who can recover the correct string x using his knowledge of U. This shows that

$$\text{CliffCompl}(C_1(n)) = 0.$$

If the unitary U belongs to the Clifford group C_2, then Alice and Bob can again win the game perfectly if they share n EPR pairs. The idea is for Alice to teleport the state $|\psi\rangle$ to Bob using the n EPR pairs. Bob obtains the state $\sigma|\psi\rangle$ where $\sigma \in C_1$ is a Pauli correction. Applying the unitary $U^\dagger$ to his state, Bob obtains

$$U^\dagger \sigma U U^\dagger |\psi\rangle = U^\dagger \sigma U |x\rangle,$$

where $U^\dagger \sigma U \in C_2$. This means that Bob simply needs to measure his state in the computational basis, and forward his result to Alice. Once they know both the value of σ and the result of the measurement, both Alice and Bob are able to recover the correct value of the string x and they win the game. This proves that

$$\text{CliffCompl}(C_2(n)) \leq n.$$

If the unitary U to be implemented belongs to the k^{th} level of the Clifford hierarchy, then Alice and Bob can apply an iterative procedure which is described in Algorithm 1.

Lemma 5. *If Alice and Bob apply Algorithm 1, then they win the game.*

Proof. To prove the correctness of the algorithm, we need to show that $U_j \in C_{k-j}$ and that Bob can perform $U_j^\dagger$ since he knows the value of U_j. The first point is shown by recurrence: $U_0 = U \in C_k$ and if $U_j \in C_{k-j}$, then $U_{j+1} = \sigma_{B_{j+1}} U_j^\dagger A_{j+1} U_j \in C_{k-j-1}$. Moreover, the value of U_j is a function of U_{j-1}, σ_{A_j} and B_j. For the quantum channel labeled by σ_{A_j}, Bob is therefore able to apply $U_j^\dagger$. □

The existence of the attack strategy described in Algorithm 1 allows us to obtain the following upper bound for the Clifford complexity of the set $C_k(n)$.

Theorem 6.

$$\text{CliffCompl}(C_k(n)) \leq 4n\, 4^{n(k-2)}. \tag{4}$$

Proof. The loop at Step 3 in Algorithm 1 can be viewed as a branching tree with depth $k-2$. This tree is regular with each internal node having 4^n children (corresponding to the 4^n possible values for Alice's Bell measurement result). Each layer of the tree corresponds to a round trip between Alice and Bob, that is $2n$ EPR pairs. Computing the complexity of the attack therefore amounts at counting the number of branches in the tree. For a tree of depth $k-2$, the number of branches is $\sum_{j=0}^{k-3} 4^{jn}$. Moreover, the last step of the protocol consists in a quantum teleportation of $n \times 4^{n(k-2)}$ qubits from Alice to Bob. In total, the number of EPR pairs used in the protocols is therefore

$$2n \sum_{j=0}^{k-2} 4^{jn} + n4^{n(k-2)} \leq 4n4^{n(k-2)}.$$

□

Input: n, k known to everyone, $|\psi\rangle = U|x\rangle$ received by Alice, $U = U_0 \in C_k$ received by Bob

Output: $x \in \{0,1\}^n$

1 Alice teleports the state $|\psi\rangle$ to B using n EPR pairs and obtains a string describing $\sigma_{A_1} \in \mathcal{P}_n$. Bob obtains the state $\sigma_{A_1}|\psi\rangle = \sigma_{A_1}U|x\rangle$.

2 Bob applies $U^\dagger$ to his state and teleports the outcome $U^\dagger\sigma_{A_1}U|x\rangle$ to Alice, obtaining some classical description of $\sigma_{B_1} \in \mathcal{P}_n$. Alice obtains the state $U_1|x\rangle$ where $U_1 = \sigma_{B_1}U^\dagger\sigma_{A_1}U \in C_{k-1}$.

for $j = 1$ *to* $k-3$ **do**

3 Alice knows the value of $\sigma_{A_1}, \ldots, \sigma_{A_j}$ (among the 4^{jn} possibilities). Alice and Bob share $4^n \times (n4^{(j-1)n})$ EPR pairs devoted to round j, corresponding to 4^n sets of $n \times 4^{(j-1)n}$ EPR pairs, one set for each possible value of σ_{A_j}. Alice teleports back each of the $4^{(j-1)n}$ n-qubit states (of the form $U_j|x\rangle$ for some given U_j) she received from Bob using the "teleportation channel" indexed by σ_{A_j}. In that teleportation channel, Bob obtains the state $\sigma_{A_{j+1}}U_j|x\rangle$, applies $U_j^\dagger$ to that state, before teleporting it back to Alice in the corresponding teleportation channel. Alice receives $U_{j+1}|x\rangle$ with $U_{j+1} = \sigma_{B_{j+1}}U_j^\dagger A_{j+1}U_j \in C_{k-j-1}$.

end

4 Alice uses a final round of teleportation for the $4^{(k-2)n}$ n-qubit states, and obtains a classical description of $\sigma_{A_{k-1}}$.

5 Alice sends the classical value of $\sigma_{A_1}, \ldots, \sigma_{A_{k-1}}$ to Bob.

6 Bob applies $U_{k-1}^\dagger$ to each n-qubit state, measures in the computational basis, and forwards the classical output, as well as the value of $\sigma_{B_1}, \ldots, \sigma_{A_{k-2}}$ to Alice.

7 Both Alice and Bob compute the value of x.

Algorithm 1: Cheating strategy based on the Clifford hierarchy

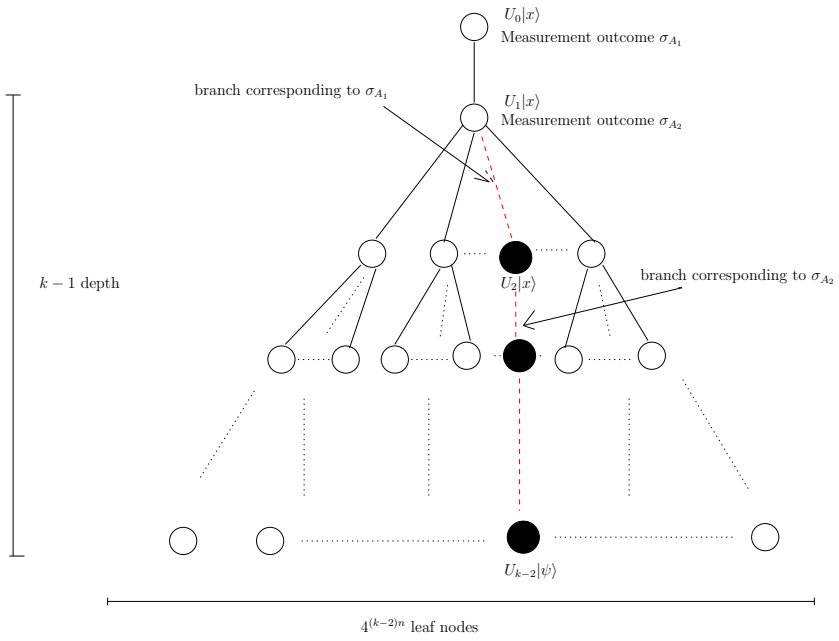

Figure 2: Pictorial view of Step 3 of Algorithm 1: Each level of the tree indicates one round of the loop. The root node contains the state $U_0|x\rangle = U|x\rangle$ and one of the nodes on the j^{th} layer contains the state $U_j|x\rangle$ (indicated in black on the figure). The path in dashed line is the correct one, and each branch of this path corresponds to the $2n$ EPR pairs labeled by measurement outcomes $\sigma_{A_1}, \ldots, \sigma_{A_{k-3}}$.

5.2 Attacks when $\mathcal{U}$ correspond to quantum circuits with a fixed layout

The attack corresponding to Algorithm 1 is general and works for any n-qubit gate in some given level of the Clifford hierarchy. In the context of PBQC protocols, however, the interesting set of gates $\mathcal{U}$ from which the unitary to be implemented is chosen, is often more restricted. Indeed, if the protocol is to be practical, then a honest prover should be able to implement the unitaries reasonably efficiently. For this reason, it is interesting to consider unitaries described by quantum circuits.

In a practical scenario, where the quantum states given to Alice are photonic qubits, it makes sense to consider photonic implementations for the quantum circuit, and therefore to consider unitaries with a fixed layout for the quantum circuit, and adjustable single and two-qubit gates. This is typically the case for experimental implementations based on integrated photonics [29].

For this reason, the set $\mathcal{U}$ of unitaries considered in the first family of protocols could be described by a fixed layout, and a specific unitary $U \in \mathcal{U}$ is then described by giving the value of each single or two-qubit gate in the layout. For a quantum circuit based on linear optics, the layout $\mathcal{L}$ corresponds to the position of the phase-shifters and beamsplitters, and the unitary is given by the specific values of the phase-shifts and transmission of the beamsplitters.

We will be interested in the complexity of attacks for such schemes as a function of the depth and width of such quantum circuits.

Definition 7. *Let $\mathcal{L}$ be the layout for an n-qubit quantum circuit, consisting of adjustable elementary gates. The set $\mathcal{U}_{\mathcal{L}}$ of n-qubit unitaries corresponds to the set of unitaries which can be implemented with a quantum circuit with layout $\mathcal{L}$.*

Lemma 8 (Parallel circuits)**.** *Let $\mathcal{L}_1, \mathcal{L}_2$ be two layouts for quantum circuits. Then*

$$\text{CliffCompl}(\mathcal{U}_{\mathcal{L}_1}||\mathcal{U}_{\mathcal{L}_2}) \leq \text{CliffCompl}(\mathcal{U}_{\mathcal{L}_1}) + \text{CliffCompl}(\mathcal{U}_{\mathcal{L}_2}), \tag{5}$$

where $\mathcal{L}_1||\mathcal{L}_2$ is the layout corresponding to putting $\mathcal{L}_1$ and $\mathcal{L}_2$ in parallel.

We note that for the quantum unitary corresponding to two circuits in parallel is simply the tensor product of the unitaries: $U_{\mathcal{L}_1||\mathcal{L}_2} = U_{\mathcal{L}_1} \otimes U_{\mathcal{L}_2}$ and therefore

$$\mathcal{U}_{\mathcal{L}_1||\mathcal{L}_2} \subset \mathcal{U}_{\mathcal{L}_1} \otimes \mathcal{U}_{\mathcal{L}_2}.$$

Proof. Consider any gate $U_1 \otimes U_2 \in \mathcal{U}_{\mathcal{L}_1||\mathcal{L}_2}$. Since both Alice and Bob know the decomposition $U_1 \otimes U_2$, they can implement the optimal attack for U_1 and for U_2 independently, since these unitaries act on distinct sets of qubits. The complexity of the overall attack is simply the sum of the complexities of implementing U_1 and U_2, which is upper bounded by $\text{CliffCompl}(\mathcal{U}_{\mathcal{L}_1}) + \text{CliffCompl}(\mathcal{U}_{\mathcal{L}_2})$. □

Lemma 9 (Concatenated circuits)**.** *Let $\mathcal{L}_1, \mathcal{L}_2$ be two layouts for quantum circuits. Then*

$$\text{CliffCompl}(\mathcal{U}_{\mathcal{L}_1\mathcal{L}_2}) \leq \text{CliffCompl}(\mathcal{U}_{\mathcal{L}_1})\text{CliffCompl}(\mathcal{U}_{\mathcal{L}_2}), \tag{6}$$

where $\mathcal{L}_1\mathcal{L}_2$ is the layout corresponding to concatenating the layouts $\mathcal{L}_1$ and $\mathcal{L}_2$.

Proof. The strategy consists in first applying the unitary $U_1 \in \mathcal{U}_{\mathcal{L}_1}$. Then, at the last round, instead of measuring the state, Bob continues the teleportation protocol in order to implement $U_2 \in \mathcal{U}_{\mathcal{L}_2}$. There are at most $\text{CliffCompl}(\mathcal{U}_{\mathcal{L}_1})$ leaves in the tree corresponding to the implementation of U_1, and it is sufficient to apply the protocol to each of these leaves in order to implement to concatenation of U_1 and U_2. Therefore, $\text{CliffCompl}(\mathcal{U}_{\mathcal{L}_1})\text{CliffCompl}(\mathcal{U}_{\mathcal{L}_2})$ EPR pairs are sufficient to implement the total unitary. □

From Lemma 8 and 9, it is possible to compute an upper bound for the Clifford complexity of any layout, as a function of its depth and size.

Theorem 10. *Let $\mathcal{L}$ be the layout of a quantum circuit acting on n-qubit state of depth d and consisting of at most r-qubit gates in C_k. Then*

$$\text{CliffAtt}(\mathcal{U}_{\mathcal{L}}) \leq 4^{rd(k-2)} \times (4rn)^d. \tag{7}$$

Proof. The layout $\mathcal{L}$ can be decomposed into d layers: $\mathcal{L} = \mathcal{L}_1\mathcal{L}_2 \cdots \mathcal{L}_d$, each layer consisting itself of at most n parallel gates of size at most r. Lemma 8 together with the result of Theorem 6 applied to gates acting on r_i qubits gives $\text{CliffCompl}(\mathcal{U}_{\mathcal{L}_i}) \leq \sum_j 4r_j 4^{r_j(k-2)}$ with $\sum_j r_j = n$. Using that $r_j \leq r$ gives $\text{CliffCompl}(\mathcal{U}_{\mathcal{L}_i}) \leq 4rn4^{r(k-2)}$. Combining this with the result of Lemma 9 finally gives

$$\text{CliffCompl}(\mathcal{U}_{\mathcal{L}}) \leq \prod_{i=1}^{d} \text{CliffCompl}(\mathcal{U}_{\mathcal{L}_i}) \leq 4^{rd(k-2)} \times (4rn)^d.$$

□

This result shows that the complexity for winning the game $G_1(n, \mathcal{U}, 1)$ is only polynomial in n if the layout of the quantum circuit has constant depth, and if individual gates act on a finite number of qubits while being in some low level of the Clifford hierarchy.

This establishes an inherent limitation of the first family of protocols for PBQC: if the protocol can be implemented realistically by a honest prover (i.e. either the unitary lies in a low level of the Clifford hierarchy, or the quantum circuit to implement it has low depth), then there exists an efficient attack strategy.

6 General attacks against the second family of PBQC protocols

Our second family of protocols is by construction immune to the attacks mentioned above. In particular, all the individual gates are chosen from the Haar measure and therefore do not belong to some low level of the Clifford hierarchy. Moreover, the product structure enforces a large depth (of order t which can be taken very large in practice) for the quantum circuit. Note that in the proposal of [7], neither of these conditions was enforced because t corresponded to the number of verifiers (which should remain quite small for practical protocols) and all the gates belong to some low level of the Clifford hierarchy.

There exist, however, some attacks working in the regime $\eta < 1$, which we investigate now. The first strategy uses port-based teleportation over $2t$ rounds. The second strategy we will consider relies on the Solovay-Kitaev theorem for approximating arbitrary gates with gates in a low level of the Clifford hierarchy, for which the attack of Algorithm 1 can be applied. Both attacks lead to the same complexity: they require $2^{O(t\log(t/\epsilon))}$ EPR pairs to achieve $\eta = 1 - \epsilon$.

We end this section with a discussion of possible attacks for non-entangled cheaters, which works if $\eta \leq \eta_0$, with $\eta_0 = 2/3$.

6.1 Port-based teleportation

The attack proceeds as follows:

- Alice applies the unitary $u_1^\dagger$ to her qubits and uses m_1 EPR pairs to teleport each qubit to Bob. This consumes a total of $M_1 = m_1 n$ EPR pairs.
- Bob applies the unitary $v_1^\dagger$ to all of his qubits, and uses m_2 EPR pairs to teleport each one back to Alice. This consumes a total of $M_2 = m2M_1$ EPR pairs.
- This process is repeated for $2t$ rounds, after which the unitary $U^\dagger$ has been applied to all the qubits. At each step, Alice or Bob uses m_i EPR pairs to perform the port-based teleportation of a single qubit.
- At the last step, Bob measures each qubit in the computational basis, and both he and Alice exchange their measurement results.

There are two quantities of interest to analyze the attacks: the total number of EPR pairs used by Alice and Bob, and the fidelity of the final state. Recall indeed that port-based teleportation is not perfect, and that the teleported state is only an approximation of the input state.

The number M of EPR pairs is given by:

$$M = M_1 + M_2 + \cdots + M_{2t-1} \tag{8}$$

$$= n\left[m_1 + m_1 m_2 + \cdots + \prod_{i=1}^{2t-1} m_i\right]. \tag{9}$$

The fidelity F between the qubit after the $2t-1$ rounds of teleportation and the initial qubit is:

$$F \geq \prod_{i=1}^{2t-1}\left(1 - \frac{4}{m_i}\right). \tag{10}$$

Choosing the slightly suboptimal strategy $m_i = m$ gives: $M = nm\frac{m^{2t-1}-1}{m-1} \approx nm^{2t-1}$ and $F = (1-4/m)^{2t-1}$, that is:

$$M \approx n\left(\frac{8t}{\epsilon}\right)^{2t-1}, \tag{11}$$

where $\epsilon = 1 - F$.

This establishes the following result.

Theorem 11. *Port-based teleportation provides an attack strategy against $G_2(n,t,\eta)$ that requires $\exp(O(t\log(t/\epsilon)))$ EPR pairs, where $\eta = 1-\epsilon$.*

6.2 Attack based on the Solovay-Kitaev approximation

We now consider a different attack strategy based on the Solovay-Kitaev approximation, which guarantees that any single-qubit unitary can be approximated with accuracy ϵ by a sequence of unitaries taken from some fixed universal set of gates.

Theorem 12 (Solovay-Kitaev [30])**.** *If $\mathcal{G} \subseteq SU(d)$ is a universal family of gates (where $SU(d)$ is the group of unitary operators in a d-dimensional Hilbert space), $\mathcal{G}$ is closed under inverse and $\mathcal{G}$ generates a dense subset of $SU(d)$, then for any $U \in SU(d)$, $\epsilon > 0$, there exist $g_1, g_2, \ldots, g_l \in \mathcal{G}$ such that $\|U - U_{g_1}U_{g_2}\ldots U_{g_l}\| \leq \epsilon$ and $l = O(\log^c\left(\frac{1}{\epsilon}\right))$, where $c < 3$ is a positive constant.*

Let us fix $\mathcal{G} = \{H, T\}$ where H is the Hadamard operator and T is the $\frac{\pi}{8}$ qubit gate, and note that this set lies in the third level C_3 of the Clifford hierarchy. The Solovay-Kitaev theorem guarantees that for each unitary U_i used in the game $G_2(n,t,\eta)$, there exists another unitary U_i', obtained as a product of exactly l gates from $\{H, T, \mathbb{1}_2\}$ (where the identity is chosen so that the size l can be chosen to be independent the unitary U_i). By decomposing their respective gates U_i and V_i into products of gates in C_3, Alice and Bob are able to implement the attack strategy of Algorithm 1.

Theorem 13. *There exists an attack strategy for $G_2(n,t,1-\epsilon)$ requiring $2^{8t\log^c\left(\frac{2t}{\epsilon}\right)}n$ EPR pairs, where $c < 3$.*

Proof. According to Solovay-Kitaev theorem 12, one can approximate each unitary U_i used in protocol family 2 by another unitary U_i' such that $\|U_i - U_i'\| \leq \frac{\epsilon}{2t}$, using a sequence of $l = O(\log^c(2t/\epsilon))$ gates. Overall, the approximation quality is given by

$$\left\|\prod_{i=1}^{t} U_iV_i - \prod_{i=1}^{t} U_i'V_i'\right\| \leq \epsilon.$$

The circuit to implement the gate $\prod_{i=1}^{t} U_i'V_i'$ has depth $2tl$ and uses only gates from C_2 or C_3. According to Theorem 10, the number M of EPR pairs needed to perform the attack is

$$M = 2^{8tl} = 2^{8t\log^c\left(\frac{2t}{\epsilon}\right)}. \tag{12}$$

Performing this attack for each of the n qubits proves the theorem.

□

This attack can in fact be improved by noting that the gates in $\mathcal{G} = \{H, T\}$ are semi-Clifford. Recall that for a semi-Clifford unitary U, there are 2^n operators $\sigma \in \mathcal{P}_n$ such that $U\sigma U^\dagger \in \mathcal{P}_n$. This implies that for such gates, the tree described in Algorithm 1 can be take to have degree $4^n - 2^n$. For $n = 1$, as is the case with the second family of protocols, this means that the complexity of approximating $\prod_{i=1}^{t} U_iV_i$ can be reduced to 2^{4lt} instead of 2^{8lt}, leading to an overall quadratic improvement in the complexity of the attack.

6.3 Attacks for a non-entangled coalition of cheaters: value of η_0

An important remark, which was already made in [16], is that non-entangled cheaters can always win a game $G_1(n, \mathcal{U}, \eta)$ or $G_2(n, t, \eta)$ provided that the value of η is low enough. Let us denote by η_0 the maximum value of η for a game that non-entangled cheaters can win with high probability. Clearly $\eta = 1/2$ is always achievable by a simple random guessing strategy.

In the case of the second family of protocols, the cheaters can do slightly better if Alice measures each incoming qubit in a random basis. More precisely, Alice will measure each qubit $|\psi_i\rangle$ of the incoming state in a random basis, obtain some measurement result corresponding to a qubit state $|\tilde{\psi}_i\rangle$ and communicate the classical description of $\tilde{\psi}_i$ to Bob. When Alice and Bob learn the value of the unitary U, they can simply consider the state $U^\dagger|\tilde{\psi}_i\rangle$ and output 0 or 1, depending on whether $U^\dagger|\tilde{\psi}_i\rangle$ is closer to $|0\rangle$ or to $|1\rangle$. This strategy gives them the correct bit with probability 2/3. This can be seen for instance by noticing that the random basis measurement corresponds to symmetric $1 \to \infty$ cloning, a process that works with fidelity 2/3 according to Eq. 2. Overall, this strategy leads to an expected fraction of correct bits equal to 2/3, which means that $\eta_0 = 2/3$ for the second family of protocols.

7 Loss-tolerant protocols

In general, the trivial cloning strategies allow the cheaters to win a constant fraction of the n "rounds" of a game. This is problematic because it seems that a honest prover cannot do much better as soon as the quantum channel from the verifiers is imperfect, either lossy or noisy. As a consequence, it would appear that PBQC is not robust against losses or noise (see [16] for possible trade-offs between loss and noise). Fortunately, this conclusion is a little bit too pessimistic.

The protocols of the second family can indeed be straightforwardly modified to be made loss-tolerant. The crucial point to note here is that these protocols appear to remain secure even if the quantum state is distributed in advance compared to the classical information required to decide in which basis to measure the state. From this observation, we propose the following modification of these protocols:

In addition to the verifiers, there is a central "bank" of quantum states available to the prover. This bank (whose role can be played by the verifiers) distributes quantum states, along with some identification number, to interested parties. The value of the states is not revealed to the client but the verifiers have access to a complete listing of pairs: (state ID/ state value). When a prover wants to play a PBQC game, she should therefore obtain a quantum state from the bank, put it in a quantum memory, and then inform the verifiers of the state ID. Then, the verifiers can apply the usual protocol, with the exception that the state $|\psi\rangle$ does not need to be distributed since the game is played with the state the prover obtained from the bank.

It seems to us that these modified protocols are as secure as the original ones. More precisely, we could not think of any attack working against the modified version that would not also work against the original version.

The advantage of this modified version is that the quantum channel between the verifiers and the prover is replaced by the quantum memory of the prover. This can be quite advantageous in a scenario where the physical distance between the verifiers and the prover is large, meaning that fiber optics communication would lead to high losses, provided that the prover has access to a good quantum memory.

8 Discussion & Conclusion

In this paper we have studied two families of position based quantum cryptography protocols and considered possible attack strategies. In particular, we have established a connection between several well studied quantum information processing tasks and position based quantum cryptography. It was previously known that there exist some efficient attack when the verifiers choose the challenge unitary from Clifford group. Here, we showed that this remains true if the unitaries lie in a low level of the Clifford hierarchy. This actually connects notions relevant in fault tolerant quantum computing with attack complexity of position based quantum cryptography.

We have further proved that for the first family of protocols, practicality in the honest case leads to some security weaknesses in terms of the existence of efficient attack strategies.

Finally, we have introduced a new family of position-based quantum verification protocols that appear to be immune to these attacks, and that display the further advantage of being loss-tolerant in a scenario where the quantum state is distributed independently from the classical challenge.

References

[1] Nishanth Chandran, Vipul Goyal, Ryan Moriarty, and Rafail Ostrovsky. Position based cryptography. In *Advances in Cryptology-CRYPTO 2009*, pages 391–407. Springer, 2009.

[2] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of modern physics*, 81(3):1301, 2009.

[3] Roger Colbeck and Renato Renner. Free randomness can be amplified. *Nature Physics*, 8(6):450–453, 2012.

[4] Umesh Vazirani and Thomas Vidick. Certifiable quantum dice: or, true random number generation secure against quantum adversaries. In *Proceedings of the 44th symposium on Theory of Computing*, pages 61–76. ACM, 2012.

[5] Adrian Kent, William J. Munro, and Timothy P. Spiller. Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints. *Phys. Rev. A*, 84:012326, Jul 2011.

[6] Robert A Malaney. Quantum location verification in noisy channels. *arXiv preprint arXiv:1004.4689*, 2010.

[7] Hoi-Kwan Lau and Hoi-Kwong Lo. Insecurity of position-based quantum-cryptography protocols against entanglement attacks. *Physical Review A*, 83(1):012322, 2011.

[8] Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, and Christian Schaffner. Position-based quantum cryptography: Impossibility and constructions. In *Advances in Cryptology–CRYPTO 2011*, pages 429–446. Springer, 2011.

[9] Lev Vaidman. Instantaneous measurement of nonlocal variables. *Phys. Rev. Lett.*, 90:010402, Jan 2003.

[10] Satoshi Ishizaka and Tohya Hiroshima. Asymptotic teleportation scheme as a universal programmable quantum processor. *Physical review letters*, 101(24):240501, 2008.

[11] Salman Beigi and Robert König. Simplified instantaneous non-local quantum computation with applications to position-based cryptography. *New Journal of Physics*, 13(9):093036, 2011.

[12] Harry Buhrman, Serge Fehr, Christian Schaffner, and Florian Speelman. The garden-hose model. In *Proceedings of the 4th conference on Innovations in Theoretical Computer Science*, pages 145–158. ACM, 2013.

[13] Hartmut Klauck and Supartha Podder. New bounds for the garden-hose model. In *34th International Conference on Foundation of Software Technology and Theoretical Computer Science, FSTTCS 2014, December 15-17, 2014, New Delhi, India*, pages 481–492, 2014.

[14] Marco Tomamichel, Serge Fehr, Jedrzej Kaniewski, and Stephanie Wehner. One-sided device-independent qkd and position-based cryptography from monogamy games. In *Advances in Cryptology–EUROCRYPT 2013*, pages 609–625. Springer, 2013.

[15] Dominique Unruh. Quantum position verification in the random oracle model. In *Advances in Cryptology–CRYPTO 2014*, pages 1–18. Springer Berlin Heidelberg, 2014.

[16] Bing Qi and George Siopsis. Loss-tolerant position-based quantum cryptography. *arXiv preprint arXiv:1502.02020*, 2015.

[17] Adrian Kent, William J Munro, and Timothy P Spiller. Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints. *Physical Review A*, 84(1):012326, 2011.

[18] WT Gowers and Emanuele Viola. The communication complexity of interleaved group products. 2015.

[19] Adrian Kent. Quantum tasks in minkowski space. *Classical and Quantum Gravity*, 29(22):224013, 2012.

[20] Daniel Gottesman and Isaac L Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, 402(6760):390–393, 1999.

[21] Daniel Gottesman. Stabilizer codes and quantum error correction. *PhD Thesis, California Institute of Technology, arXiv:quant-ph/9705052*, 1997.

[22] David Gross and M Van den Nest. The lu-lc conjecture, diagonal local operations and quadratic forms over gf (2). *Quant. Inf. Comp.*, 8:263, 2008.

[23] Bei Zeng, Xie Chen, and Isaac L Chuang. Semi-Clifford operations, structure of C_k hierarchy, and gate complexity for fault-tolerant quantum computation. *Physical Review A*, 77(4):042313, 2008.

[24] Satoshi Ishizaka and Tohya Hiroshima. Quantum teleportation scheme by selecting one of multiple output ports. *Physical Review A*, 79(4):042306, 2009.

[25] Valerio Scarani, Sofyan Iblisdir, Nicolas Gisin, and Antonio Acin. Quantum cloning. *Reviews of Modern Physics*, 77(4):1225, 2005.

[26] Nicolas J Cerf and Jaromír Fiurášek. Optical quantum cloning. *Progress in Optics*, 49:455–545, 2006.

[27] Reinhard F Werner. Optimal cloning of pure states. *Physical Review A*, 58(3):1827, 1998.

[28] Michael Keyl and Reinhard F Werner. Optimal cloning of pure states, testing single clones. *Journal of Mathematical Physics*, 40(7):3283–3299, 1999.

[29] Jeremy L O'Brien, Akira Furusawa, and Jelena Vučković. Photonic quantum technologies. *Nature Photonics*, 3(12):687–695, 2009.

[30] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.