UNIVERSITY OF AMSTERDAM

UvA-DARE (Digital Academic Repository)

A Quantum Cloning Game with Applications to Quantum Position Verification

Palais, Léo Colisson; Escolà-Farràs, Llorenç; Speelman, Florian

DOI
10.4230/LIPIcs.TQC.2025.2

Publication date
2025

Document Version
Final published version

Published in
20th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2025

License
CC BY

Link to publication

Citation for published version (APA):
Palais, L. C., Escolà-Farràs, L., & Speelman, F. (2025). A Quantum Cloning Game with Applications to Quantum Position Verification. In B. Fefferman (Ed.), *20th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2025* Article 2 (Leibniz International Proceedings in Informatics; Vol. 350). Schloss Dagstuhl - Leibniz-Zentrum für Informatik. https://doi.org/10.4230/LIPIcs.TQC.2025.2

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: https://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, P.O. Box 19185, 1000 GD Amsterdam, The Netherlands. You will be contacted as soon as possible.

UvA-DARE is a service provided by the library of the University of Amsterdam (https://dare.uva.nl)

Download date:05 Sep 2026

A Quantum Cloning Game with Applications to Quantum Position Verification

Léo Colisson Palais
Laboratoire Jean Kuntzmann, Université Grenoble Alpes, France

Llorenç Escolà-Farràs
TU Eindhoven, The Netherlands

Florian Speelman
QuSoft & Informatics Institute, University of Amsterdam, The Netherlands

Abstract

We introduce a quantum cloning game in which k separate collaborative parties receive a classical input, determining which of them has to share a maximally entangled state with an additional party (referee). We provide the optimal winning probability of such a game for every number of parties k, and show that it decays exponentially when the game is played n times in parallel. These results have applications to quantum cryptography, in particular in the topic of quantum position verification, where we show security of the routing protocol (played in parallel), and a variant of it, in the random oracle model.

2012 ACM Subject Classification Security and privacy → Cryptography

Keywords and phrases Quantum position verification, cloning game, random oracle, parallel repetition

Digital Object Identifier 10.4230/LIPIcs.TQC.2025.2

Related Version *Previous Version*: https://arxiv.org/abs/2410.22157

Funding *Léo Colisson Palais*: European Union (ERC, ASC-Q, 101040624) and the Dutch Ministry of Economic Affairs and Climate Policy (EZK), as part of the Quantum Delta NL programme.
Llorenç Escolà-Farràs: Dutch Ministry of Economic Affairs and Climate Policy (EZK), as part of the Quantum Delta NL programme.
Florian Speelman: Dutch Ministry of Economic Affairs and Climate Policy (EZK), as part of the Quantum Delta NL programme.

1 Introduction

Non-local correlations have extensively been studied in the field of quantum information theory, see e.g. [12]. Bell [9] originally showed that distant parties sharing quantum resources can reproduce correlations that could never be attained by any classical theory. Often, non-local correlations are studied as *non-local games*, which provide an operational framework for understanding them. These games are interesting per se from a fundamental point of view, since they give rise to understanding the underlying essence of nature, but they additionally lead to applications such as secure key distribution [1], certified randomness [33], reduced communication complexity [14], self-testing [32, 37], and computation [5].

A vast literature in non-local games covers the scenario where a classical referee sends questions to non-communicating collaborative parties, and their task is to produce answers according to a certain publicly-known predicate, where the questions and answers are all *classical*. The best-known non-local game is the CHSH game [18]. Non-locality has also been investigated in terms of supersets of non-local games, called *monogamy-of-entanglement (MoE) games* [38], where a quantum referee sends the same classical question to the players and the parties have to guess the (classical) outcome of a referee's quantum measurement

© Léo Colisson Palais, Llorenç Escolà-Farràs, and Florian Speelman;
licensed under Creative Commons License CC-BY 4.0

(depending on the question). MoE games have been used to provide security proofs for the quantum cryptographic primitives device-independent quantum key distribution [10] and quantum position verification [28]. Such games were later generalized under the name of *extended non-local games* [27].

Here, we introduce the concept of the *quantum cloning game*, played by k distant parties and a quantum referee. The referee publically announces a party, i.e., sends the same classical question to all the players, and the chosen party has to end up with the maximally entangled (EPR) state with the referee. At the beginning of the game, the players are allowed to share any quantum state with the referee. In this work, we show that the optimal winning probability for players using any quantum resources is given by $\frac{1}{2} + \frac{1}{2k}$, converging to $\frac{1}{2}$ for a large number of players. We analyze the game when it is played n times in parallel, showing an exponential decay in n of the optimal winning probability. Additionally, the quantum cloning game can be generalized to any arbitrary quantum state instead of an EPR state, and we provide its optimal winning probability.

We show that these results have applications in quantum position verification (QPV), which is a cryptographic primitive consisting of verifying the location of an untrusted party. Securely implementing this primitive is unachievable using only classical information, because a general attack exists even when using computational assumptions [17]. Due to the no-cloning theorem [41] the general classical attack does not apply if quantum information is used instead [28, 31], however, a general quantum attack exists which requires exponential entanglement [13, 8]. This means that hope for protocols secure against reasonable amounts of entanglement is alive, and indeed there has been much analysis on attacks on specific protocols [2, 28, 29, 34, 16, 36, 21, 22, 25, 20], and security analysis under extra assumptions [30, 24], such as the random oracle model [39]. A generic 1-dimensional (the main ideas generalize to higher dimensions) QPV protocol is described in the following way: two verifiers V_0 and V_1, placed on the left and right of an untrusted prover P, supposedly at the position *pos*, send quantum and classical messages to P at the speed of light, and he has to pass a challenge and reply correctly to them at the speed of light as well, if so, the verifiers *accept*, and if any of them receives a wrong answer or the timing does not correspond with the time it would have taken for light to travel back from the honest prover, the verifiers *reject*. The time consumed by the prover to perform the challenge is assumed to be negligible, and the verifiers are assumed to have perfectly-synchronized clocks.

In this work, we consider the *routing* QPV protocol [28], which has an appealing simple form: the prover has to return a received qubit to one of the verifiers, where the choice of verifier is a function of the classical information sent by the verifiers [28]. Besides the theoretical interest of this protocol, it is also an appealing candidate for free-space quantum position verification, when the quantum messages can travel with the vacuum speed of light, since the hardware of the prover could hypothetically be as simple as a mirror or an optical switch. Despite theoretical work on this protocol [15, 20, 11, 3, 6], there were gaps left in our understanding relative to measurement-based QPV protocol variants: namely the security of parallel repetition of this protocol against unentangled attackers and attackers who pre-share a linear (in the security parameter) amount of entangled qubits, and its security in the random-oracle model against arbitrary adversaries. As an application of the quantum cloning game, we show the security of the routing protocol in these scenarios.

2 Preliminaries

For $k \in \mathbb{N}$, we will denote $[k] := \{0, \dots, k-1\}$. Let $\mathcal{H}$, $\mathcal{H}'$ be finite-dimensional Hilbert spaces, we denote by $\mathcal{B}(\mathcal{H}, \mathcal{H}')$ the set of bounded operators from $\mathcal{H}$ to $\mathcal{H}'$ and $\mathcal{B}(\mathcal{H}) = \mathcal{B}(\mathcal{H}, \mathcal{H})$. Denote by $\mathcal{S}(\mathcal{H})$ the set of quantum states on $\mathcal{H}$, i.e. $\mathcal{S}(\mathcal{H}) = \{\rho \in \mathcal{B}(\mathcal{H}) \mid \rho \geq 0, \mathrm{Tr}[\rho] = 1)\}$. A pure state will be denoted by a ket $|\psi\rangle \in \mathcal{H}$. The maximally entangled state or EPR pair is $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. We denote the identity matrix by $\mathbb{I}$. For $M \in \mathcal{B}(\mathcal{H})$, we denote its Schatten ∞-norm by $\|M\|$. We will use the notation $1, \dots, \not{i}, \dots, k-1$ to denote $1, \dots, i-1, i+1, \dots, k-1$.

▶ **Definition 1.** *Let $N \in \mathbb{N}$. Two permutations $\pi, \pi' : [N] \to [N]$ are said to be* orthogonal *if $\pi(i) \neq \pi'(i)$ for all $i \in [N]$.*

▶ **Lemma 2** (Lemma 2 in [38])**.** *Let $\Pi^1, \dots, \Pi^N$ be projectors acting on a Hilbert space $\mathcal{H}$. Let $\{\pi_k\}_{k\in[n]}$ be a set of mutually orthogonal permutations. Then,*

$$\left\| \sum_{i\in[N]} \Pi^i \right\| \leq \sum_{k\in[N]} \max_{i\in[N]} \left\| \Pi^i \Pi^{\pi_k(i)} \right\|. \tag{1}$$

▶ Remark 3. There always exist a set of N permutations of $[N]$ that are mutually orthogonal, an example is the N cyclic shifts.

▶ **Lemma 4** (Lemma 1 in [38])**.** *Let $A, B, L \in \mathcal{B}(\mathcal{H})$ such that $AA^\dagger \succeq B^\dagger B$. Then it holds that $\|AL\| \geq \|BL\|$.*

3 k-party quantum cloning game

In the following definition, we introduce the quantum cloning game.

▶ **Definition 5.** *The k-party* quantum cloning game*, shortly denoted by QCG_k, consists of a referee R with associated Hilbert space $\mathcal{H}_R = \mathbb{C}^2$ and k collaborative distant parties (players) $P_0, \dots, P_{k-1}$. Before the game starts, the parties prepare a joint quantum state of arbitrary dimension between themselves and the referee. During the game, the referee sends $x \in [k]$, drawn uniformly at random, to all the collaborative parties. The players win the game if and only if the party P_x (holding a qubit register P_x) ends up sharing the maximally entangled state with the referee, i.e. if a projection onto $|\Phi^+\rangle_{RP_x}$ yields the correct outcome.*

See Figure 1 for a schematic representation of the QCG_k. Intuitively, in such a game, the referee publically announces which party has to create an entangled state with herself.

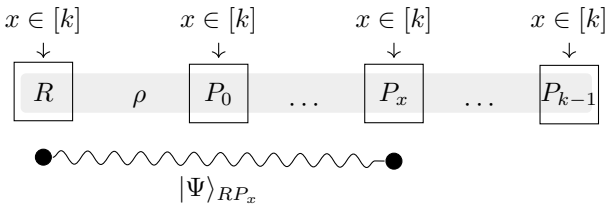

Figure 1 Schematic representation of the k-party quantum cloning game, where $|\Psi\rangle_{RP_x} = |\Phi^+\rangle_{RP_x}$, where the gray-shaded region represents the shared state ρ. If $|\Psi\rangle_{RP_x}$ is arbitrary, this represents a Ψ-QCG_k.

A strategy S for the QCG_k is described by a quantum state $\rho \in \mathcal{S}(\mathcal{H}_R \otimes \mathcal{H}_{P_0E_0} \otimes \cdots \otimes \mathcal{H}_{P_{k-1}E_{k-1}})$, where, for $i \in [k]$, registers P_i are of the same dimension as $\mathcal{H}_R$ and E_i are auxiliary systems of arbitrary dimension that each party possess, and completely positive trace-preserving (CPTP) maps $\{\mathcal{E}^x_{P_iE_i\to P_i}\}_x$, where the subscript $P_iE_i \to P_i$ indicates that the map has input and output registers P_iE_i and P_i, respectively, i.e. $\mathcal{E}^x_{P_iE_i\to P_i} : \mathcal{B}(\mathcal{H}_{P_iE_i}) \to \mathcal{B}(\mathcal{H}_{P_i})$. The winning probability of such a game, given the strategy S, is provided by

$$\omega(\mathrm{QCG}_k, S) = \frac{1}{k}\sum_{x\in[k]} \mathrm{Tr}\left[|\Phi^+\rangle\langle\Phi^+|_{RP_x} \mathrm{Tr}_{P_0\ldots\not{P}_x\ldots P_{k-1}}\left[\mathbb{I}_R \bigotimes_{i\in[k]} \mathcal{E}^x_{P_iE_i\to P_i}(\rho)\right]\right]. \tag{2}$$

The optimal winning probability of such games is given by

$$\omega^*(\mathrm{QCG}_k) = \sup_S \omega(\mathrm{QCG}_k, S), \tag{3}$$

where the supremum is taken over all the possible strategies over all possible Hilbert spaces. The following theorem gives the optimal winning probability of this game for every number of parties k.

▶ **Theorem 6.** *For every $k \in \mathbb{N}$, the optimal winning probability of the QCG_k is given by*

$$\omega^*(\mathrm{QCG}_k) = \frac{1}{2} + \frac{1}{2k}. \tag{4}$$

Intuitively, this game cannot be perfectly won since, otherwise, it would be possible to have maximal entanglement between the referee and each of the parties, and this is not possible since entanglement is *monogamous* [19]. In the proof, see below, the key part is to show that the optimal winning probability is attainable by the actions of the players being *independent* of x, intuitively, each party acts as if they were chosen to reproduce the maximally entangled state with the referee. In addition, in the proof, we show that the optimal value can be attained by preparing an initial state ρ where, locally, each of the parties holds a qubit and no further actions taken by the players, i.e. their local actions are described by the identity channel ($\mathbb{I}_{P_i}$). We then specify a strategy by providing a quantum state, since any local actions are independent of x, they can be absorbed in the quantum state. More precisely, the optimal winning probability for the QCG_k can be attained by the strategy given by the (pure) quantum state

$$|\varphi\rangle = \sqrt{\frac{2}{k(k+1)}} \sum_{x\in[k]} |\Phi^+\rangle_{RP_x}|0\rangle_{P_0\ldots\not{P}_x\ldots P_{k-1}}. \tag{5}$$

Note that other natural multi-party entangled states that have been widely studied in the literature, such as the GHZ state ([26]) $|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ and the W state ([23]) $|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$, and their respective generalizations to arbitrary dimensions, as well as the strategy of "guessing" which party has to reproduce the quantum state, e.g. guessing $x = 0$, given by preparing the state $|\Phi^+\rangle_{VP_0}|0\rangle_{P_1}\ldots|0\rangle_{k-1}$, provide significantly suboptimal winning probabilities. For 2-players, $\omega^*(\mathrm{QCG}_2) = \frac{3}{4}$, and

$$\omega^*(\mathrm{QCG}_k) \xrightarrow{k\to\infty} \frac{1}{2}, \tag{6}$$

which converges to the value attained by the strategy given by preparing the state $|0\rangle_R|0\rangle_{P_0}\ldots|0\rangle_{P_{k-1}}$, showing that when k increases even unentangled states allow for a near-optimal winning probability.

Proof. A strategy S for the QCG_k is described by a quantum state $\rho \in \mathcal{S}(\mathcal{H}_R \otimes \mathcal{H}_{P_0E_0} \otimes \ldots \otimes \mathcal{H}_{P_{k-1}E_{k-1}})$, where, for $i \in [k]$, registers P_i are of the same dimension as $\mathcal{H}_R$ and E_i are auxiliary systems of arbitrary dimension that each party possesses, and unitary transformations $U = \{U^x_{P_iE_i}\}_x$, acting on the registers in the subscripts (due to the Stinespring dilation of the quantum channels, we restrict our attention to unitary transformations $U^x_{P_iE_i}$ instead of quantum channels $\mathcal{E}^x_{P_iE_i \to P_i}$). Let d be the dimension of the above (total) Hilbert space, which we denote by $\mathcal{H}_d$. Then, the winning probability of the QCG_k, given the strategy S on a d-dimensional Hilbert space, is provided by

$$
\begin{aligned}
&\omega(\mathrm{QCG}_k, S, d)\\
&= \frac{1}{k}\sum_{x\in[k]} \mathrm{Tr}\left[\left(|\Phi^+\rangle\langle\Phi^+|_{RP_x}\otimes\mathbb{I}_{E_x}\bigotimes_{i\neq x\in[k]}\mathbb{I}_{P_iE_i}\right)\left(\left(\mathbb{I}_R\otimes U^x_{P_iE_i}\otimes\ldots\otimes U^x_{P_iE_i}\right)\rho(\mathbb{I}_R\otimes U^x_{P_iE_i}\otimes\ldots\otimes U^x_{P_iE_i})^\dagger\right)\right]\\
&= \frac{1}{k}\sum_{x\in[k]} \mathrm{Tr}\left[\left(\mathbb{I}_R\otimes U^{x\dagger}_{P_iE_i}\otimes\ldots\otimes U^{x\dagger}_{P_iE_i}\right)\left(|\Phi^+\rangle\langle\Phi^+|_{RP_x}\otimes\mathbb{I}_{E_x}\bigotimes_{i\neq x\in[k]}\mathbb{I}_{P_iE_i}\right)(\mathbb{I}_R\otimes U^x_{P_iE_i}\otimes\ldots\otimes U^x_{P_iE_i})\rho\right],
\end{aligned}
$$

where in the last equation we used cyclicity of the trace. For a specific choice of unitary transformations $U = \{U^x_{P_iE_i}\}_x$, the optimal winning probability is given by

$$
\begin{aligned}
&\omega^*(\mathrm{QCG}_k, U, d)\\
&= \sup_{\rho\in\mathcal{S}(\mathcal{H}_d)} \frac{1}{k}\sum_{x\in[k]} \mathrm{Tr}\left[\left(\mathbb{I}_R\otimes U^{x\dagger}_{P_iE_i}\otimes\ldots\otimes U^{x\dagger}_{P_iE_i}\right)\left(|\Phi^+\rangle\langle\Phi^+|_{RP_x}\otimes\mathbb{I}_{E_x}\bigotimes_{i\neq x\in[k]}\mathbb{I}_{P_iE_i}\right)(\mathbb{I}_R\otimes U^x_{P_iE_i}\otimes\ldots\otimes U^x_{P_iE_i})\rho\right]\\
&= \frac{1}{k}\Big\|\sum_{x\in[k]}\left(\mathbb{I}_R\otimes U^{x\dagger}_{P_iE_i}\otimes\ldots\otimes U^{x\dagger}_{P_iE_i}\right)\left(|\Phi^+\rangle\langle\Phi^+|_{RP_x}\otimes\mathbb{I}_{E_x}\bigotimes_{i\neq x\in[k]}\mathbb{I}_{P_iE_i}\right)(\mathbb{I}_R\otimes U^x_{P_iE_i}\otimes\ldots\otimes U^x_{P_iE_i})\Big\|\\
&= \frac{1}{k}\Big\|\sum_{x\in[k]}\left(\left(\mathbb{I}_R\otimes U^{x\dagger}_{P_xE_x}\right)\left(|\Phi^+\rangle\langle\Phi^+|_{RP_x}\otimes\mathbb{I}_{E_x}\right)\left(\mathbb{I}_R\otimes U^x_{P_xE_x}\right)\right)\bigotimes_{i\neq x\in[k]}U^{x\dagger}_{P_iE_i}\bigotimes_{i\neq x\in[k]}\mathbb{I}_{P_iE_i}\bigotimes_{i\neq x\in[k]}U^x_{P_iE_i}\Big\|\\
&= \frac{1}{k}\Big\|\sum_{x\in[k]}\left(\left(\mathbb{I}_R\otimes U^{x\dagger}_{P_xE_x}\right)\left(|\Phi^+\rangle\langle\Phi^+|_{RP_x}\otimes\mathbb{I}_{E_x}\right)\left(\mathbb{I}_R\otimes U^x_{P_xE_x}\right)\right)\bigotimes_{i\neq x\in[k]}U^{x\dagger}_{P_iE_i}U^x_{P_iE_i}\Big\|,
\end{aligned}
$$

Notice that, since $\{U^x_{P_iE_i}\}_x$ are unitary matrices, $U^{x\dagger}_{P_iE_i}U^x_{P_iE_i} = \mathbb{I}_{P_iE_i}$, moreover, $\mathbb{I}_{P_iE_i} = U^{i\dagger}_{P_iE_i}U^i_{P_iE_i}$, then we can use $U^{x\dagger}_{P_iE_i}U^x_{P_iE_i} = U^{i\dagger}_{P_iE_i}U^i_{P_iE_i}$, and therefore

$$
\begin{aligned}
&\omega^*(\mathrm{QCG}_k, U, d)\\
&= \frac{1}{k}\Big\|\sum_{x\in[k]}\left(\left(\mathbb{I}_R\otimes U^{x\dagger}_{P_xE_x}\right)\left(|\Phi^+\rangle\langle\Phi^+|_{RP_x}\otimes\mathbb{I}_{E_x}\right)\left(\mathbb{I}_R\otimes U^{x\dagger}_{P_xE_x}\right)\right)\bigotimes_{i\neq x\in[k]}U^{i\dagger}_{P_iE_i}U^i_{P_iE_i}\Big\|\\
&= \frac{1}{k}\Big\|\sum_{x\in[k]}\left(\mathbb{I}_R\bigotimes_{i\neq\in[k]}U^{i\dagger}_{P_iE_i}\right)\left(|\Phi^+\rangle\langle\Phi^+|_{RP_x}\otimes\mathbb{I}_{E_x}\bigotimes_{i\neq x\in[k]}\mathbb{I}_{P_iE_i}\right)\left(\mathbb{I}_R\bigotimes_{i\in[k]}U^i_{P_iE_i}\right)\Big\|\\
&= \frac{1}{k}\Big\|\left(\mathbb{I}_R\bigotimes_{i\neq\in[k]}U^{i\dagger}_{P_iE_i}\right)\left(\sum_{x\in[k]}|\Phi^+\rangle\langle\Phi^+|_{RP_x}\otimes\mathbb{I}_{E_x}\bigotimes_{i\neq x\in[k]}\mathbb{I}_{P_iE_i}\right)\left(\mathbb{I}_R\bigotimes_{i\in[k]}U^i_{P_iE_i}\right)\Big\|\\
&= \frac{1}{k}\Big\|\sum_{x\in[k]}|\Phi^+\rangle\langle\Phi^+|_{RP_x}\otimes\mathbb{I}_{E_x}\bigotimes_{i\neq x\in[k]}\mathbb{I}_{P_iE_i}\Big\|\\
&= \sup_{\rho\in\mathcal{S}(\mathcal{H}_d)}\frac{1}{k}\sum_{x\in[k]}\mathrm{Tr}\left[\left(|\Phi^+\rangle\langle\Phi^+|_{RP_x}\otimes\mathbb{I}_{E_x}\bigotimes_{i\neq x\in[k]}\mathbb{I}_{P_iE_i}\right)\rho\right] = \omega^*(\mathrm{QCG}_k, d)
\end{aligned}
\tag{7}
$$

where in the fourth equality we used that the Schatten ∞-norm is unitarily invariant, i.e. $\|V * W\| = \| * \|$ for unitary matrices V and W, and $\omega^*(\mathrm{QCG}_k, d)$ denotes the optimal

winning probability if the dimension of the total initial Hilbert space is d. Equation (7) shows that, given a Hilbert space $\mathcal{H}_R \otimes \mathcal{H}_{P_0E_0} \otimes \ldots \otimes \mathcal{H}_{P_{k-1}E_{k-1}}$, the optimal winning probability can be attained by an optimal quantum state independently of the actions of the players after knowing x, i.e. the optimal winning probability is independent of $\{U^x_{P_iE_i}\}_x$ and they can apply $\{\mathbb{I}^x_{P_iE_i}\}_x$. We are going to see that, actually, the optimal winning probability can be attained by each of the parties possessing a qubit (2-dimensional Hilbert space), i.e. by the total Hilbert space being $\mathcal{H}_{2^k} = \bigotimes_{i\in[k]} \mathbb{C}^2$. From (7),

$$\begin{aligned}
\omega^*(\mathrm{QCG}_k) &= \sup_{d\in\mathbb{N}} \omega^*(\mathrm{QCG}_k, d) = \sup_{d\in\mathbb{N}} \frac{1}{k} \Big\| \left(\sum_{x\in[k]} |\Phi^+\rangle\langle\Phi^+|_{RP_x} \otimes \mathbb{I}_{P_0\ldots \not{P}_x \ldots P_{k-1}} \right) \bigotimes_{i\in[k]} \mathbb{I}_{E_i} \Big\| \\
&= \sup_{d\in\mathbb{N}} \frac{1}{k} \Big\| \sum_{x\in[k]} |\Phi^+\rangle\langle\Phi^+|_{RP_x} \otimes \mathbb{I}_{P_0\ldots \not{P}_x \ldots P_{k-1}} \Big\| \Big\| \bigotimes_{i\in[k]} \mathbb{I}_{E_i} \Big\| \\
&= \sup_{d\in\mathbb{N}} \frac{1}{k} \Big\| \sum_{x\in[k]} |\Phi^+\rangle\langle\Phi^+|_{RP_x} \otimes \mathbb{I}_{P_0\ldots \not{P}_x \ldots P_{k-1}} \Big\| \\
&= \sup_{\rho\in\mathcal{S}(\mathcal{H}_{2^k})} \frac{1}{k} \sum_{x\in[k]} \mathrm{Tr}\Big[\Big(|\Phi^+\rangle\langle\Phi^+|_{RP_x} \otimes \mathbb{I}_{P_0\ldots \not{P}_x \ldots P_{k-1}} \Big) \rho \Big], \qquad (8)
\end{aligned}$$

where, in the arguments of the supremums, the dependence on d is implicit in the auxiliary spaces, which, together with the registers P_i and V, fully describe the total Hilbert space, and thus its dimension.

In order to provide the explicit value for the optimal winning probability, we have that, from (8),

$$\omega^*(\mathrm{QCG}_k) = \frac{1}{k} \Big\| \sum_{x\in[k]} |\Phi^+\rangle\langle\Phi^+|_{RP_x} \otimes \mathbb{I}_{P_0\ldots \not{P}_x \ldots P_{k-1}} \Big\| = \frac{1}{2} + \frac{1}{2k}, \qquad (9)$$

where the last equation is obtained by direct computation. ◀

3.1 Quantum cloning game with any target state

The concept of QCG_k can be generalized to the case where, instead of the parties having to reproduce EPR pairs with the referee, the state that has to be reproduced is an arbitrary-fixed state, i.e. the referee's Hilbert space $\mathcal{H}_R$ is now of arbitrary dimension, and on input x the party P_x has to generate a given state $|\Psi\rangle_{RP_x}$. Here, the dimension of the registers P_i is the same for all $i \in [k]$. We will refer to such a game as a k-party *quantum cloning game with target state* $|\Psi\rangle$, in short denoted by Ψ-QCG_k, see Figure 1. Notice that this game becomes trivial if the target state $|\Psi\rangle_{RP}$ is a tensor product state. In the following theorem, we provide the optimal winning probability for any Ψ-QCG_k for every number of parties k and for any target state $|\Psi\rangle$.

▶ **Theorem 7.** *The optimal winning probability for every* Ψ-QCG_k is given by

$$\omega^*(\Psi\text{-}\mathrm{QCG}_k) = \frac{1}{k} \Big\| \sum_{x\in[k]} |\Psi\rangle\langle\Psi|_{RP_x} \otimes \mathbb{I}_{P_0\ldots \not{P}_x \ldots P_{k-1}} \Big\|. \qquad (10)$$

Along the lines of the proof of Theorem 6, the key idea relies on showing that the optimal winning probability can be attained by the actions of the players being independent on x.

Proof. The result follows from the proof of Theorem 6 by repeating the same steps, replacing $|\Phi^+\rangle_{VP_x}$ by $|\Psi\rangle_{VP_x}$, and from (8), we obtain (10). ◀

4 Parallel repetition of QCG_k

A case of particular interest is given when QCG_k is played n times in parallel, denoted by $\mathrm{QCG}_k^{\times n}$. Specifically, we will analyze QCG_2 where now the two collaborative parties, who we rename as Alice and Bob, will receive $x = x_0 \dots x_{n-1} \in \{0,1\}^n$. We denote by $R_0 \dots R_{n-1}$, $A_0 \dots A_{n-1}$ and $B_0 \dots B_{n-1}$ the final (qubit) registers of the referee, Alice and Bob, respectively. The players win if at the end of the game Alice is able to create the maximally entangled state with the referee in all her registers such that $x_i = 0$, and analogously for Bob in all his registers such that $x_i = 1$. See Figure 2 for a schematic representation.

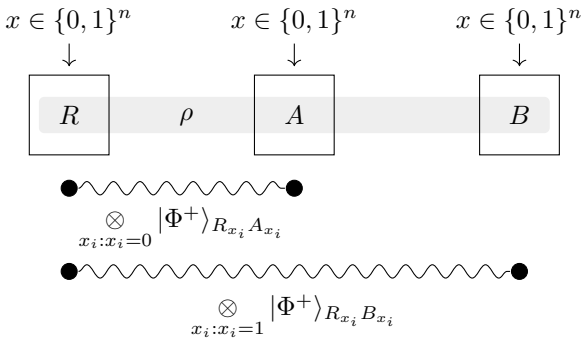

Figure 2 Schematic representation of the n-fold parallel repetition of the 2-party quantum cloning game. The gray-shaded region represents the tripartie state ρ that Alice and Bob prepare.

Similarly as before, at the beginning of the game the three parties are allowed to share any arbitrary quantum state and, upon receiving the classical information, Alice and Bob can apply CPTP maps $\{\mathcal{E}^x_{A_0\dots A_{n-1}E_A \to A_0\dots A_{n-1}}\}_x$ and $\{\mathcal{E}^x_{B_0\dots B_{n-1}E_B \to B_0\dots B_{n-1}}\}_x$, where E_A and E_B are arbitrary auxiliary systems that Alice and Bob possess, respectively.

In the following theorem, we state that the optimal winning probability decays exponentially with the number of parallel repetitions n.

▶ **Theorem 8.** *The optimal winning probability for n parallel repetitions of the QCG_2 is such that*

$$\left(\frac{3}{4}\right)^n \leq \omega^*(\mathrm{QCG}_2^{\times n}) \leq \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^n. \tag{11}$$

The key idea of the proof relies on combining ideas used in the proof of Theorem 7 together with Proposition 4.3 in [35], which was also used in [38] to prove parallel repetition for monogamy-of-entanglement games.

Proof. A strategy S_n for the n-parallel repetition of QCG_2 is described by a quantum state $\rho \in \mathcal{S}(\mathcal{H}_R \otimes \mathcal{H}_{A_0\dots A_{n-1}E_A} \otimes \mathcal{H}_{B_0\dots B_{n-1}E_B})$, where, for $i \in [n]$, registers A_i and B_i are of the same dimension as $\mathcal{H}_R$ and E_A and E_B are auxiliary systems of arbitrary dimension that each party possess, and unitary transformations $\{U^x_{A_0\dots A_{n-1}E_A}\}_x$ and $\{V^x_{B_0\dots B_{n-1}E_B}\}_x$, acting on the registers in the subscripts (due to the Stinespring dilation of the quantum channels, we restrict our attention to unitary transformations). For $x = x_0 \dots x_{n-1} \in \{0,1\}^n$, let $Q_{x_i} = A_i$ if $x_i = 0$ and $Q_{x_i} = B_i$ if $x_i = 1$, and we use the shorthand notation $R = R_0 \dots R_{n-1}$, $A = A_0 \dots A_{n-1}$ and $B = B_0 \dots B_{n-1}$. Then, the winning probability of this game, given the strategy S_n, is provided by

$$
\begin{aligned}
&\omega(\mathrm{QCG}_2^{\times n}, S_n)\\
&=\frac{1}{2^n}\sum_{x\in\{0,1\}^n}\mathrm{Tr}\left[\left(\left(\bigotimes_{i\in[n]}|\Phi^+\rangle\langle\Phi^+|_{R_iQ_{x_i}}\otimes\mathbb{I}_{Q_{1-x_i}}\right)\otimes\mathbb{I}_{E_AE_B}\right)(\mathbb{I}_R\otimes U^x_{AE_A}\otimes V^x_{BE_B})\rho(\mathbb{I}_R\otimes U^x_{AE_A}\otimes V^x_{BE_B})^\dagger\right]\\
&=\frac{1}{2^n}\sum_{x\in\{0,1\}^n}\mathrm{Tr}\left[(\mathbb{I}_R\otimes U^{x\dagger}_{AE_A}\otimes V^{x\dagger}_{BE_B})\left(\left(\bigotimes_{i\in[n]}|\Phi^+\rangle\langle\Phi^+|_{R_iQ_{x_i}}\otimes\mathbb{I}_{Q_{1-x_i}}\right)\otimes\mathbb{I}_{E_AE_B}\right)(\mathbb{I}_R\otimes U^x_{AE_A}\otimes V^x_{BE_B})\rho\right]\\
&\leq\frac{1}{2^n}\|\sum_{x\in\{0,1\}^n}(\mathbb{I}_R\otimes U^{x\dagger}_{AE_A}\otimes V^{x\dagger}_{BE_B})\left(\left(\bigotimes_{i\in[n]}|\Phi^+\rangle\langle\Phi^+|_{R_iQ_{x_i}}\otimes\mathbb{I}_{Q_{1-x_i}}\right)\otimes\mathbb{I}_{E_AE_B}\right)(\mathbb{I}_R\otimes U^x_{AE_A}\otimes V^x_{BE_B})\|.
\end{aligned}
$$

Denote

$$
M^x:=(\mathbb{I}_R\otimes U^{x\dagger}_{AE_A}\otimes V^{x\dagger}_{BE_B})\left(\left(\bigotimes_{i\in[n]}|\Phi^+\rangle\langle\Phi^+|_{R_iQ_{x_i}}\otimes\mathbb{I}_{Q_{1-x_i}}\right)\otimes\mathbb{I}_{E_AE_B}\right)(\mathbb{I}_R\otimes U^x_{AE_A}\otimes V^x_{BE_B}),\tag{12}
$$

then,

$$
\omega(\mathrm{QCG}_2^{\times n}, S_n)\leq\frac{1}{2^n}\|\sum_{x\in\{0,1\}^n}M^x\|\leq\frac{1}{2^n}\sum_{k\in[2^n]}\max_{x,x'}\|M^xM^{x'}\|,\tag{13}
$$

where we used Lemma 2, and $x'=\pi_k(x)$, for $\{\pi_k\}_k$ being a set of mutually orthogonal permutations. Fix x and x', and let $\mathcal{T}$ be the set of indices where x and x' differ, i.e. $\mathcal{T}=\{i\mid x_i\neq x'_i\}$, and let $t=|\mathcal{T}|$. Let $\mathcal{T}_A=\{i\in\mathcal{T}\mid x_i=0\}$, and $t_A:=|\mathcal{T}_A|$, then we have that

$$
\begin{aligned}
&M^x\preceq M^x_A\\
&:=(\mathbb{I}_R\otimes U^{x\dagger}_{AE_A}\otimes V^{x\dagger}_{BE_B})\\
&\quad\left(\left(\bigotimes_{i\in\mathcal{T}_A}|\Phi^+\rangle\langle\Phi^+|_{R_iQ_{x_i}}\otimes\mathbb{I}_{Q_{1-x_i}}\right)\otimes\left(\bigotimes_{i\in[n]\setminus\mathcal{T}_A}\mathbb{I}_{R_iQ_{x_i}Q_{1-x_i}}\right)\otimes\mathbb{I}_{E_AE_B}\right)(\mathbb{I}_R\otimes U^x_{AE_A}\otimes V^x_{BE_B})\\
&=(\mathbb{I}_R\otimes U^{x\dagger}_{AE_A}\otimes V^{x\dagger}_{BE_B})\left(\left(\bigotimes_{i\in\mathcal{T}_A}|\Phi^+\rangle\langle\Phi^+|_{R_iA_i}\bigotimes_{i\in[n]\setminus\mathcal{T}_A}\mathbb{I}_{R_iA_iE_A}\right)\otimes\mathbb{I}_{BE_B}\right)(\mathbb{I}_R\otimes U^x_{AE_A}\otimes V^x_{BE_B})\\
&=(\mathbb{I}_R\otimes U^{x\dagger}_{AE_A}\otimes V^{x'\dagger}_{BE_B})\left(\left(\bigotimes_{i\in\mathcal{T}_A}|\Phi^+\rangle\langle\Phi^+|_{R_iA_i}\bigotimes_{i\in[n]\setminus\mathcal{T}_A}\mathbb{I}_{R_iA_iE_A}\right)\otimes\mathbb{I}_{BE_B}\right)(\mathbb{I}_R\otimes U^x_{AE_A}\otimes V^{x'}_{BE_B}),
\end{aligned}
$$

where in the last equality we used that $V^{x\dagger}_{BE_B}V^{x\dagger}_{BE_B}=\mathbb{I}_{BE_B}=V^{x'\dagger}_{BE_B}V^{x'}_{BE_B}$. Similarly,

$$
\begin{aligned}
&M^{x'}\preceq M^{x'}_B\\
&:=(\mathbb{I}_R\otimes U^{x'\dagger}_{AE_A}\otimes V^{x'\dagger}_{BE_B})\\
&\quad\left(\left(\bigotimes_{i\in\mathcal{T}_A}|\Phi^+\rangle\langle\Phi^+|_{R_iQ_{x'_i}}\otimes\mathbb{I}_{Q_{1-x'_i}}\right)\otimes\left(\bigotimes_{i\in[n]\setminus\mathcal{T}_A}\mathbb{I}_{R_iQ_{x'_i}Q_{1-x'_i}}\right)\otimes\mathbb{I}_{E_AE_B}\right)(\mathbb{I}_R\otimes U^{x'}_{AE_A}\otimes V^{x'}_{BE_B})\\
&=(\mathbb{I}_R\otimes U^{x\dagger}_{AE_A}\otimes V^{x'\dagger}_{BE_B})\left(\left(\bigotimes_{i\in\mathcal{T}_A}|\Phi^+\rangle\langle\Phi^+|_{R_iB_i}\bigotimes_{i\in[n]\setminus\mathcal{T}_A}\mathbb{I}_{R_iB_iE_B}\right)\otimes\mathbb{I}_{AE_A}\right)(\mathbb{I}_R\otimes U^x_{AE_A}\otimes V^{x'}_{BE_B}),
\end{aligned}\tag{14}
$$

By Lemma 4,

$$
\|M^xM^{x'}\|\leq\|M^x_AM^{x'}_B\|,\tag{15}
$$

then

$$
\begin{aligned}
&M_A^x M_B^{x'} \\
&= (\mathbb{I}_R \otimes U_{AE_A}^{x\dagger} \otimes V_{BE_B}^{x'\dagger}) \left(\left(\bigotimes_{i\in\mathcal{T}_A} |\Phi^+\rangle\langle\Phi^+|_{R_iA_i} \bigotimes_{i\in[n]\setminus\mathcal{T}_A} \mathbb{I}_{R_iA_iE_A} \right) \otimes \mathbb{I}_{BE_B} \right) (\mathbb{I}_R \otimes U_{AE_A}^{x} \otimes V_{BE_B}^{x'}) \\
&\cdot (\mathbb{I}_R \otimes U_{AE_A}^{x\dagger} \otimes V_{BE_B}^{x'\dagger}) \left(\left(\bigotimes_{i\in\mathcal{T}_A} |\Phi^+\rangle\langle\Phi^+|_{R_iB_i} \bigotimes_{i\in[n]\setminus\mathcal{T}_A} \mathbb{I}_{R_iB_iE_B} \right) \otimes \mathbb{I}_{AE_A} \right) (\mathbb{I}_R \otimes U_{AE_A}^{x} \otimes V_{BE_B}^{x'}).
\end{aligned}
$$

We have that $(\mathbb{I}_R \otimes U_{AE_A}^{x} \otimes V_{BE_B}^{x'})(\mathbb{I}_R \otimes U_{AE_A}^{x\dagger} \otimes V_{BE_B}^{x'\dagger}) = \mathbb{I}_{RAEABE_B}$, and, since the Schatten ∞-norm is unitarily invariant,

$$
\begin{aligned}
&\|M_A^x M_B^{x'}\| \\
&= \| \left(\bigotimes_{i\in\mathcal{T}_A} |\Phi^+\rangle\langle\Phi^+|_{R_iA_i} \bigotimes_{i\in[n]\setminus\mathcal{T}_A} \mathbb{I}_{R_iA_iE_A} \otimes \mathbb{I}_{BE_B} \right) \left(\bigotimes_{i\in\mathcal{T}_A} |\Phi^+\rangle\langle\Phi^+|_{R_iB_i} \bigotimes_{i\in[n]\setminus\mathcal{T}_A} \mathbb{I}_{R_iB_iE_B} \otimes \mathbb{I}_{AE_A} \right) \| \\
&= \| \left(\bigotimes_{i\in\mathcal{T}_A} \left(|\Phi^+\rangle\langle\Phi^+|_{R_iA_i} \otimes \mathbb{I}_{B_i} \right) \left(|\Phi^+\rangle\langle\Phi^+|_{R_iB_i} \otimes \mathbb{I}_{A_i} \right) \right) \bigotimes_{i\in[n]\setminus\mathcal{T}_A} \mathbb{I}_{R_iA_iB_i} \otimes \mathbb{I}_{E_AE_B} \| \\
&= \| \bigotimes_{i\in\mathcal{T}_A} \left(|\Phi^+\rangle\langle\Phi^+|_{R_iA_i} \otimes \mathbb{I}_{B_i} \right) \left(|\Phi^+\rangle\langle\Phi^+|_{R_iB_i} \otimes \mathbb{I}_{A_i} \right) \| \| \bigotimes_{i\in[n]\setminus\mathcal{T}_A} \mathbb{I}_{R_iA_iB_i} \otimes \mathbb{I}_{E_AE_B} \| \\
&= \prod_{i\in\mathcal{T}_A} \| \left(|\Phi^+\rangle\langle\Phi^+|_{R_iA_i} \otimes \mathbb{I}_{B_i} \right) \left(|\Phi^+\rangle\langle\Phi^+|_{R_iB_i} \otimes \mathbb{I}_{A_i} \right) \| \\
&= 2^{-t_A},
\end{aligned}
\tag{16}
$$

where we used that, for every i,

$$
\| \left(|\Phi^+\rangle\langle\Phi^+|_{R_iA_i} \otimes \mathbb{I}_{B_i} \right) \left(|\Phi^+\rangle\langle\Phi^+|_{R_iB_i} \otimes \mathbb{I}_{A_i} \right) \| = 2^{-1}. \tag{17}
$$

Without loss of generality, assume $t_A \geq t/2$, then, combining (15) and (16), we have that

$$
\|M^x M^{x'}\| \leq \|M_A^x M_B^{x'}\| \leq 2^{-\frac{t}{2}}. \tag{18}
$$

In order to apply the bound in Lemma 4, consider the set of permutations given by $\pi_k(x) = x \oplus k$, where $x, k \in \{0,1\}^n$ (they are such that they have the same Hamming distance). There are $\binom{n}{i}$ permutations with Hamming distance i. Then, we have

$$
\omega(\mathrm{QCG}_2^{\times n}, S_n) \leq \frac{1}{2^n} \sum_{k\in[2^n]} \max_{x,x'} \|M^x M^{x'}\| \leq \frac{1}{2^n} \sum_{t=0}^{n} \binom{n}{t} 2^{-\frac{t}{2}} = \left(\frac{1}{2} + \frac{1}{2\sqrt{2}} \right)^n. \tag{19}
$$

◀

5 Application to QPV in the No-PE and BE(m) models

In this section, we analyze the security of the *routing* QPV protocol, originally introduced in [28]. A round of this protocol, see Figure 3 for a schematic representation, is described as follows:

1. The verifier V_0 selects a qubit $|\phi\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, and the verifier V_1 selects $x \in \{0,1\}$, both picked uniformly at random. They send $|\phi\rangle$ and x (at time $t = 0$) so that they arrive at the same time ($t = 1$) at *pos*.
2. Upon receiving the information sent by V_0 and V_1, the prover sends the qubit $|\phi\rangle$ to the verifier V_x.

3. If $|\phi\rangle$ arrives at the time consistent with *pos* ($t = 2$), and a projective measurement performed by V_x on the state sent by V_0 leads to the correct outcome, the verifiers accept. Otherwise, they reject.

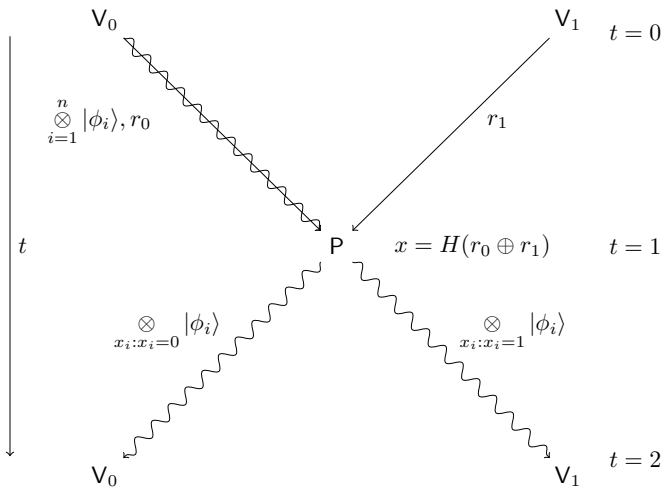

Figure 3 Schematic representation of the (H, n)-routing QPV protocol. If r_0 is an empty bit string, and $x = r_1$, this figure represents the n-parallel repetition of the routing QPV protocol. The time arrow is represented by t.

The most general attack to the routing protocol, pictured in Figure 4, consists of having two attackers Alice (A) and Bob (B), located between V_0 and P, and between P and V_0, respectively. Before $t = 0$, the attackers agree on a strategy and might prepare an entangled state. After $t = 0$, Alice (A_0) and Bob (B_0) intercept the information sent from their closest verifier, respectively. Due to timing constraints, they are allowed to perform one round of simultaneous communication. After communicating (after $t = 1$), Alice (A_1) and Bob (B_1) answer to their closest verifier, respectively.

Here, we analyze security within three attack models: (i) the *No Pre-shared Entanglement* (No-PE) model [13], where adversaries do not (pre-)share any entanglement before the protocol's execution; (ii) the *Bounded-Entanglement* BE(m) model, where adversaries pre-share at most m entangled qubits; and (iii) the *Random Oracle Model* (ROM), where attackers (pre-)share any amount of entanglement before the protocol's execution. We formalize the concept of security, given an attack model $\mathcal{M}$, as follows:

▶ **Definition 9.** *The routing protocol is said to be* α-sound *in the* $\mathcal{M}$ *model if, for any attackers acting according to such an attack model, the verifiers* accept *with probability at most* α.

The security of a variation of this protocol, the f-routing QPV protocol, where the classical information x is split into two bit strings, each sent from each verifier, and the qubit has to be routed according to the outcome of a boolean function f on those bit strings has been studied in the BE(m) model [11, 6, 7]. The authors of these works showed that the f-routing QPV protocol remains secure as long as m is at most linear in the size of the bit strings. However, unlike other protocols [13, 38, 4] the security of the routing QPV protocol in the No-PE model was never analyzed. The No-PE assumption is necessary to obtain non-trivial bounds, since there is a perfect attack if the attackers pre-share entanglement [28].

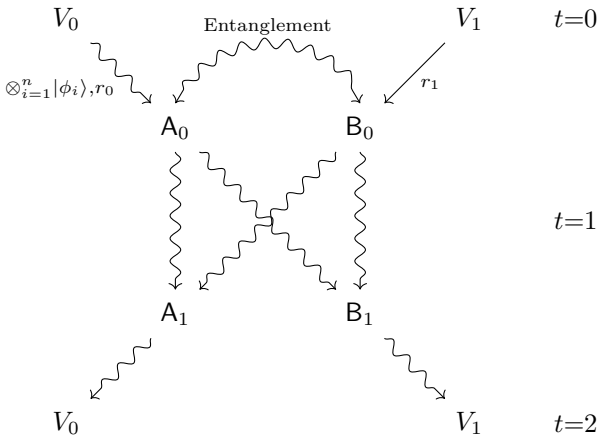

Figure 4 Schematic representation of a generic attack to the (H, n)-routing protocol (and in particular, to the routing protocol).

We show security in the No-PE model, providing the tight result, summarized in the following proposition:

▶ **Proposition 10.** *In the No-PE model, the routing QPV protocol is $\frac{3}{4}$-sound. Moreover, this is optimal.*

The intuition behind Proposition 10 relies on the fact that the most general attack can be reduced to a QCG_2. Consider the purified version of the routing protocol, which is equivalent to the original version, and where the only difference relies on V_0, instead of sending the qubit $|\phi\rangle$, prepares the state $|\Phi^+\rangle$ and keeps a register for herself and sends the other register to the prover. Then, as seen in Figure 4, the most general attack to the routing QPV protocol is to place an adversary between V_0 and the prover, Alice, and another adversary between the prover and V_1, Bob. In the No-PE model, we can simplify it further, as Alice intercepts the qubit sent by V_0, applies an arbitrary quantum operation to it, and possibly some ancillary systems she possesses. She keeps a part of it and sends the other to Bob. On the other side, Bob intercepts x, copies it and sends the copy to Alice. Since they share no entanglement, any quantum operation that Bob could perform as a function of x can be included in Alice's operation. After one-round of simultaneous communication, Alice and Bob share a tripartite state with V_0, and their task is that the party designated by x has to end up with a maximally entangled state with the V_0. By Theorem 7, even if Alice and Bob can share any state with the referee (in this case V_0), they can succeed with at most probability $\frac{3}{4}$.

On the other hand, to show optimality, consider the attack where (i) at the beginning of the protocol Alice prepares the 3-qubit state $\frac{1}{\sqrt{3}}(|\Phi^+\rangle_{A_0A}|0\rangle_B + |\Phi^+\rangle_{A_0B}|0\rangle_A)$, (ii) intercepts $|\phi\rangle$ and performs a Bell measurement on the intercepted state and her register A_0, immediately she applies the teleportation corrections to both of her registers A and B, (iii) she keeps register A and sends register B to Bob, (iv) in the meantime, Bob intercepts and broadcasts x, after receiving the information from their fellow attacker, if $x = 0$, Alice sends her register (A) to V_0, whereas if $x = 1$, Bob sends his register (B) to V_1. This attack has a winning probability of $\frac{3}{4}$.

An analogous reduction applies when the routing QPV protocol is executed n times in parallel, and therefore, its security can be reduced to the n-parallel repetition of QCG_2:

▶ **Proposition 11.** *In the No-PE model, the routing QPV protocol executed n times in parallel is $(\frac{1}{2}+\frac{1}{2\sqrt{2}})^n$-sound.*

A direct consequence of Lemma 5.3 in [8] implies, similarly as in [38], security for the routing protocol executed in parallel for attackers who pre-share a linear amount of qubits:

▶ **Corollary 12.** *In the $BE(m)$ model, the routing QPV protocol executed n times in parallel is $\left(2^m(\frac{1}{2}+\frac{1}{2\sqrt{2}})^n\right)$-sound.*

In particular, the above soundness is exponentially small in n if $m < n\log\left((\frac{1}{2}+\frac{1}{2\sqrt{2}})^{-1}\right) \simeq 0.228n$.

6 Application to QPV in the random oracle model

Consider the n-parallel repetition of the routing QPV protocol but instead of V_1 sending $x \in \{0,1\}^n$, V_0 and V_1 send $r_0, r_1 \in \{0,1\}^\ell$, for $\ell \in \mathbb{N}$, to the prover, respectively. Then, the x used in the rest of the protocol is computed via $x = H(r_0 \oplus r_1)$, for a given hash function $H : \{0,1\}^\ell \to \{0,1\}^n$. We will denote this variation as (H,n)-routing QPV protocol, see Figure 3 for a schematic representation.

To provide security in the quantum random oracle model against adversaries sharing an arbitrary amount of entanglement, we use some techniques introduced in [40]. A quantum random oracle is defined as a fixed function $H\colon \{0,1\}^\ell \to \{0,1\}^n$ that is sampled uniformly at random from the set of functions from ℓ bits to n bits[1]. The parties are not given the full description of H directly, but they are given oracle access to H, in the sense that they have access to a special gate implementing the unitary $U_H\colon |r\rangle|b\rangle \to |r\rangle|b \oplus H(r)\rangle$. We denote the number of queries made by the adversary by q. As a proof technique, an oracle can also be reprogrammed, where security of the protocol is shown by first studying a variant where the gate applied by the oracle may change over time. A typical setting is where we change a single entry of the oracle: we denote by $H[r \mapsto x]$ the new oracle that behaves like H except that $H(r) = x$. The chances of distinguishing whether H has been reprogrammed or not can be bounded using [40], which informally states that if we can distinguish whether the oracle has been reprogrammed or no, then we have queried it on r before it has been reprogrammed (for completeness, see Lemma 14). In the following theorem, we show security of the (H,n)-routing protocol in the ROM.

▶ **Theorem 13.** *If the (possibly entangled) attackers Alice and Bob perform at most q queries to the (quantum) random oracle H, the (H,n)-routing QPV protocol is ϵ-sound, with*

$$\epsilon = 2q2^{-\frac{\ell}{2}} + \left(\frac{1}{2}+\frac{1}{2\sqrt{2}}\right)^n. \tag{20}$$

In particular, ϵ is negligible if q and ℓ scale polynomially with n.

The starting idea of the proof follows [40], where we send Bell pairs instead of single qubits in order to make the input state independent of x, the output of the oracle. Then we reprogram this oracle *after* adversaries share their state to ensure x is truly random and independent of

[1] This can be done by simply sampling a large table T of size 2^ℓ, and outputting $T[r]$ when queried on input r. Note that this sampling procedure is not efficient: while having an efficient oracle [42] is sometimes required, for instance when working with composable security and computationally bounded distinguishers, or when reducing to problems that are hard only for bounded adversaries, in our case we do not need this additional property since we do a reduction to a problem that is hard even for unbounded adversaries.

the state shared by malicious parties at time $t = 1$. Finally, we realize that we can rewrite this into an instance of Theorem 8. In the proof of Theorem 13, we will rely on this lemma by Unruh:

▶ **Lemma 14** ([40, Lemma 3]). *Let $(\mathcal{A}_1, \mathcal{A}_2)$ be oracle algorithms sharing state between invocations that perform at most q queries to H. Let C be an oracle algorithm that on input (j, r) does the following: Run $\mathcal{A}_1^H(r)$ until the j-th query to H, then measure the argument of that query in the computational basis, and output the measurement outcome (or $\perp$ if no j-th query occurs). Let:*

$$P_{\mathcal{A}}^1 := \Pr_{\substack{H \xleftarrow{\$} (\{0,1\}^\ell \to \{0,1\}^n) \\ r \xleftarrow{\$} \{0,1\}^l, \mathcal{A}_1^H(r) \\ b' \to \mathcal{A}_2^H(r, H(r))}} [b' = \mathsf{Accept}], \tag{21}$$

$$P_{\mathcal{A}}^2 := \Pr_{\substack{H \xleftarrow{\$} (\{0,1\}^\ell \to \{0,1\}^n) \\ r \xleftarrow{\$} \{0,1\}^l, x \xleftarrow{\$} \{0,1\}^n \\ H' := H[r \mapsto x], \mathcal{A}_1^H(r) \\ b' \to \mathcal{A}_2^{H'}(r, x)}} [b' = \mathsf{Accept}], \tag{22}$$

$$P_C := \Pr_{\substack{H \xleftarrow{\$} (\{0,1\}^\ell \to \{0,1\}^n) \\ r \xleftarrow{\$} \{0,1\}^l, j \xleftarrow{\$} \{1,\dots,q\} \\ x' \to C^H(j, x)}} [x = x']. \tag{23}$$

Then, $|P_{\mathcal{A}}^1 - P_{\mathcal{A}}^2| \leq 2q\sqrt{P_C}$.

Proof (of Theorem 13). To prove this theorem, we must show that the probability that the verifiers accept in a malicious run of the protocol is lower bounded by ϵ, i.e., if we denote by $\mathsf{V}_0 \leftrightsquigarrow \mathsf{A} \leftrightsquigarrow \mathsf{B} \leftrightsquigarrow \mathsf{V}_1$ the output of the verifiers (Accept or Reject) at the end of a protocol involving a malicious Alice A and a malicious Bob B, we want to show that

$$\Pr[\mathsf{V}_0 \leftrightsquigarrow \mathsf{A} \leftrightsquigarrow \mathsf{B} \leftrightsquigarrow \mathsf{V}_1 = \mathsf{Accept}] \leq \epsilon. \tag{24}$$

We prove this by defining a series of games, where the probability of accepting each game is close to the probability of accepting the next game. By ensuring that the first game corresponds to the real protocol, and that the probability of the last game can easily be computed, we can bound ϵ by transitivity.

Game_1. This game is defined as the real protocol, i.e. $\mathsf{Game}_1 := \mathsf{V}_0 \leftrightsquigarrow \mathsf{A} \leftrightsquigarrow \mathsf{B} \leftrightsquigarrow \mathsf{V}_1$. Therefore, we trivially have:

$$\Pr[\mathsf{V}_0 \leftrightsquigarrow \mathsf{A} \leftrightsquigarrow \mathsf{B} \leftrightsquigarrow \mathsf{V}_1 = \mathsf{Accept}] = \Pr[\mathsf{Game}_1 = \mathsf{Accept}]. \tag{25}$$

Game_2. Is like Game_1, except that each $|\phi_i\rangle$ is replaced with one half of a Bell pair. Similarly, instead of projecting on $|\phi_i\rangle$, the verifier will do a Bell measurement between the state sent by the prover and its corresponding half of Bell pair, accepting only if the outcome is $(0, 0)$. This trick is often used in literature, hence we skip the computations. Hence

$$\Pr[\mathsf{Game}_1 = \mathsf{Accept}] = \Pr[\mathsf{Game}_2 = \mathsf{Accept}]. \tag{26}$$

Game_3. Is like Game_2, except that at time $t = 1$, one samples the random bit string $x \xleftarrow{\$} \{0,1\}^n$, and reprogram the oracle to implement $H' := H[r_0 \oplus r_1 \mapsto x]$ (i.e., A_1 and B_1 will have oracle access to H' instead of H). Note that the simulators will use this value of

$x = H'(r_0 \oplus r_1)$ instead of $H(r_0 \oplus r_1)$ to perform the verification at the end. Intuitively, the only way to distinguish this game from the previous game is if the adversary managed to query $H(r_0 \oplus r_1)$ before $t = 0$ and after, but this is highly unlikely since neither A_0 nor B_0 know both r_0 and r_1 (and remember that they cannot query the oracle more than q times, so they cannot just evaluate the oracle on all inputs). This intuition is formalized thanks to Lemma 14: if we define $\mathcal{A}_1(r)$ as the execution of the protocol in Game_2 until $t = 1$ (which is the same as in Game_3), except that r_2 is chosen as $r_2 \coloneqq r_1 \oplus r$, and $\mathcal{A}_2(r, x)$ as the execution of the protocol after time $t = 1$, we can remark that (using notations from Lemma 14):

$$P^1_{\mathcal{A}} = \Pr[\mathsf{Game}_2 = \mathsf{Accept}]. \tag{27}$$

since sampling (r_1, r_2) uniformly at random is strictly equivalent to sampling (r_1, r) randomly and then defining $r_2 \coloneqq r \oplus r_1$. Similarly, we also have:

$$P^2_{\mathcal{A}} = \Pr[\mathsf{Game}_3 = \mathsf{Accept}]. \tag{28}$$

The remaining part is to bound P_C. To compute P_C, we need to bound the probability of querying $H(r)$ during the first part of the protocol on j-th query. But when A_0 does this query, we know that it must be independent of r since all inputs of A_0 are independent of r (if not, we could break non-signaling). Similarly, queries made by B_0 are independent of r: the exact same argument does not hold since $r_2 = r_1 \oplus r$ does depend on $r\ldots$ but this is only a very superficial dependency, since we could have exactly the same probability distributions of r_1 and r_2 by sampling instead r_2 randomly and $r_1 = r_2 \oplus r$, making r_2 independent of r now. Hence, the j-th query is independent of r, so the best probability of it being equal to r is lower bounded by $P_C \leq \frac{1}{2^\ell}$. Hence, using Lemma 14, we have:

$$|\Pr[\,\mathsf{Game}_2 = \mathsf{Accept}\,] - \Pr[\,\mathsf{Game}_3 = \mathsf{Accept}\,]| \tag{29}$$

$$\overset{(28)}{=} |P^1_{\mathcal{A}} - P^2_{\mathcal{A}}| \overset{(14)}{\leq} 2q\sqrt{P_C} \leq 2q2^{-\ell/2}. \tag{30}$$

Game_4. Now, we can realize that all operations in Game_3 until $t = 1$ is independent of x. So let us call $|\psi\rangle_{RP_AP_B}$ the (purification) of the state owned by the verifier (consisting in a list of qubits part of a shared Bell pair), Alice and Bob (we also include in P_B the message sent by A_0 to B_1, and similarly in P_A the message sent by B_0 to A_1). Additionally, we also include in $|\psi\rangle$ the (exponentially large) definition of H, r_0 and r_1 in both registers P_A and P_B, one copy for each party. Then, we define the referee operation R as the identity, P_A as the map that runs A_1, simulating the query to H' using the table H, r_0 and r_1 that are part of $|\psi\rangle$, and x that is given as an input to P_A, and we define similarly P_B simulating B_1. We define then Game_4 as the game $\mathrm{QCG}_2^{\times n}$, i.e. the parallel repetition of the 2-party quantum cloning game (Definition 5), involving the shared state $|\psi\rangle$, the referee R, and the two parties P_A and P_B. This game is exactly like Game_3 as we simulate exactly the same process, just grouping differently the various circuits involved. Hence, $\Pr[\,\mathsf{Game}_4 = \mathsf{Accept}\,] = \Pr[\,\mathsf{Game}_3 = \mathsf{Accept}\,]$. But using Theorem 8, we have:

$$\Pr[\,\mathsf{Game}_4\,] = \omega^*(\mathrm{QCG}_2^{\times n}) \overset{(8)}{\leq} \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^n. \tag{31}$$

Hence, we can combine all the above equations to obtain:

$$\Pr[\,\mathsf{V}_0 \rightsquigarrow \mathsf{A} \rightsquigarrow \mathsf{B} \rightsquigarrow \mathsf{V}_1 = \mathsf{Accept}\,] = \Pr[\,\mathsf{Game}_1 = \mathsf{Accept}\,] \leq \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^n + 2q2^{-\ell/2}, \tag{32}$$

concluding the proof. ◀

7 Discussion

We have introduced the concept of the k-party quantum cloning game and provided the optimal winning probability for any number of parties. The parallel repetition for the two-party version was studied, showing an exponential decay of the optimal winning probability. We applied the above results to show security of the routing QPV protocol in the *No Pre-shared Entanglement* and *Bounded-Entanglement* models, as well as in the *Random Oracle Model*. The tightness of Theorem 8 remains an open question, either by showing a strategy attaining the value (11), or if strong parallel repetition holds and actually the optimal value is $\left(\frac{3}{4}\right)^n$ (or neither of them). Closing this gap would imply knowing what is the optimal security for the routing protocol in the No-PE model, and would further tighten its security in the BE(m) and random-oracle models.

References

1 Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-Independent Security of Quantum Cryptography against Collective Attacks. *Physical Review Letters*, 98(23):230501, June 2007. doi:10.1103/PhysRevLett.98.230501.

2 Tomothy Spiller Adrian Kent, William Munro and Raymond Beausoleil. Tagging systems. us patent nr 2006/0022832, 2006.

3 Rene Allerstorfer, Harry Buhrman, Alex May, Florian Speelman, and Philip Verduyn Lunel. Relating non-local quantum computation to information theoretic cryptography. *Quantum*, 8:1387, June 2024. doi:10.22331/q-2024-06-27-1387.

4 Rene Allerstorfer, Harry Buhrman, Florian Speelman, and Philip Verduyn Lunel. On the role of quantum communication and loss in attacks on quantum position verification, 2022. arXiv:2208.04341.

5 Janet Anders and Dan E. Browne. Computational Power of Correlations. *Physical Review Letters*, 102(5):050502, February 2009. doi:10.1103/PhysRevLett.102.050502.

6 Vahid Asadi, Richard Cleve, Eric Culf, and Alex May. Linear gate bounds against natural functions for position-verification, 2024. doi:10.22331/q-2025-01-21-1604.

7 Vahid Asadi, Eric Culf, and Alex May. Rank lower bounds on non-local quantum computation. In *16th Innovations in Theoretical Computer Science Conference (ITCS 2025)*, Leibniz International Proceedings in Informatics (LIPIcs), pages 11:1–11:18, 2025. doi:10.4230/LIPIcs.ITCS.2025.11.

8 Salman Beigi and Robert König. Simplified instantaneous non-local quantum computation with applications to position-based cryptography. *New Journal of Physics*, 13(9):093036, September 2011. doi:10.1088/1367-2630/13/9/093036.

9 J. S. Bell. On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1:195–200, November 1964. doi:10.1103/PhysicsPhysiqueFizika.1.195.

10 Charles H. Bennett and Gilles Brassard. Quantum cryptography: public key distribution and coin tossing. *Proc. IEEE Int. Conf. on Computers, Systems, and Signal Process (Bangalore) (Piscataway, NJ: IEEE)*, 1984.

11 Andreas Bluhm, Matthias Christandl, and Florian Speelman. A single-qubit position verification protocol that is secure against multi-qubit attacks. *Nature Physics*, pages 1–4, 2022.

12 Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Rev. Mod. Phys.*, 86:419–478, April 2014. doi:10.1103/RevModPhys.86.419.

13 Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, and Christian Schaffner. Position-based quantum cryptography: Impossibility and constructions. *SIAM Journal on Computing*, 43(1):150–178, January 2014. doi:10.1137/130913687.

14 Harry Buhrman, Richard Cleve, Serge Massar, and Ronald de Wolf. Nonlocality and communication complexity. *Reviews of Modern Physics*, 82(1):665–698, March 2010. doi:10.1103/RevModPhys.82.665.

15 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 - ITCS '13*. ACM Press, 2013. doi:10.1145/2422436.2422455.

16 Kaushik Chakraborty and Anthony Leverrier. Practical position-based quantum cryptography. *Physical Review A*, 92(5), November 2015. doi:10.1103/physreva.92.052304.

17 Nishanth Chandran, Vipul Goyal, Ryan Moriarty, and Rafail Ostrovsky. Position based cryptography. In *Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference*, volume 5677 of *Lecture Notes in Computer Science*, pages 391–407. Springer, 2009. doi:10.1007/978-3-642-03356-8_23.

18 John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett. 23*, 1969.

19 Valerie Coffman, Joydip Kundu, and William K. Wootters. Distributed entanglement. *Physical Review A*, 61(5), April 2000. doi:10.1103/physreva.61.052306.

20 Sam Cree and Alex May. Code-routing: a new attack on position-verification. *Quantum*, 7, 1079, 2022. doi:10.22331/q-2023-08-09-1079.

21 Kfir Dolev. Constraining the doability of relativistic quantum tasks. *arXiv preprint*, 2019. arXiv:1909.05403.

22 Kfir Dolev and Sam Cree. Non-local computation of quantum circuits with small light cones. *arXiv preprint*, 2022. arXiv:2203.10106.

23 W. Dür, G. Vidal, and J. I. Cirac. Three qubits can be entangled in two inequivalent ways. *Phys. Rev. A*, 62:062314, November 2000. doi:10.1103/PhysRevA.62.062314.

24 Fei Gao, Bin Liu, and QiaoYan Wen. Quantum position verification in bounded-attack-frequency model. *SCIENCE CHINA Physics, Mechanics & Astronomy*, 59(11):1–11, 2016.

25 Alvin Gonzales and Eric Chitambar. Bounds on instantaneous nonlocal quantum computation. *IEEE Transactions on Information Theory*, 66(5):2951–2963, 2019.

26 Daniel M. Greenberger, Michael A. Horne, and Anton Zeilinger. Going beyond bell's theorem. In Menas Kafatos, editor, *Bell's Theorem, Quantum Theory and Conceptions of the Universe*, pages 69–72. Springer Netherlands, Dordrecht, 1989. doi:10.1007/978-94-017-0849-4_10.

27 Nathaniel Johnston, Rajat Mittal, Vincent Russo, and John Watrous. Extended non-local games and monogamy-of-entanglement games. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 472(2189):20160003, May 2016. doi:10.1098/rspa.2016.0003.

28 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), July 2011. doi:10.1103/physreva.84.012326.

29 Hoi-Kwan Lau and Hoi-Kwong Lo. Insecurity of position-based quantum-cryptography protocols against entanglement attacks. *Physical Review A*, 83(1), January 2011. doi:10.1103/physreva.83.012322.

30 Jiahui Liu, Qipeng Liu, and Luowen Qian. Beating Classical Impossibility of Position Verification. In Mark Braverman, editor, *13th Innovations in Theoretical Computer Science Conference (ITCS 2022)*, volume 215 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 100:1–100:11, Dagstuhl, Germany, 2022. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.ITCS.2022.100.

31 Robert A. Malaney. Location-dependent communications using quantum entanglement. *Phys. Rev. A*, 81:042319, April 2010. doi:10.1103/PhysRevA.81.042319.

32 Dominic Mayers and Andrew Yao. Self Testing Quantum Apparatus. *Quantum Info. Comput.*, 4(4):273–286, July 2004. URL: http://dl.acm.org/citation.cfm?id=2011827.2011830.

33 S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe. Random numbers certified by Bell's theorem. *Nature*, 464(7291):1021–1024, April 2010. doi:10.1038/nature09008.

34 Jérémy Ribeiro and Frédéric Grosshans. A tight lower bound for the bb84-states quantum-position-verification protocol, 2015. doi:10.48550/arXiv.1504.07171.

35 Christian Schaffner. Cryptography in the bounded-quantum-storage model, 2007. arXiv:0709.0289.

36 Florian Speelman. Instantaneous non-local computation of low T-depth quantum circuits. In *11th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2016)*. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2016.

37 Ivan Šupić and Joseph Bowles. Self-testing of quantum systems: a review. *arXiv:1904.10042 [quant-ph]*, April 2019. arXiv: 1904.10042. arXiv:1904.10042.

38 Marco Tomamichel, Serge Fehr, Jedrzej Kaniewski, and Stephanie Wehner. A monogamy-of-entanglement game with applications to device-independent quantum cryptography. *New Journal of Physics*, 15(10):103002, October 2013. doi:10.1088/1367-2630/15/10/103002.

39 Dominique Unruh. Quantum position verification in the random oracle model. In Juan A. Garay and Rosario Gennaro, editors, *Advances in Cryptology – CRYPTO 2014*, pages 1–18, Berlin, Heidelberg, 2014. Springer Berlin Heidelberg.

40 Dominique Unruh. Quantum Position Verification in the Random Oracle Model. In Juan A. Garay and Rosario Gennaro, editors, *Advances in Cryptology – CRYPTO 2014*, Lecture Notes in Computer Science, pages 1–18, Berlin, Heidelberg, 2014. Springer. doi:10.1007/978-3-662-44381-1_1.

41 William K. Wootters and Wojciech Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

42 Mark Zhandry. How to Record Quantum Queries, and Applications to Quantum Indifferentiability. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology – CRYPTO 2019*, Lecture Notes in Computer Science, pages 239–268. Springer International Publishing, 2019. doi:10.1007/978-3-030-26951-7_9.