Relativistic (or 2-Prover 1-Round) Zero-Knowledge Protocol for NP Secure Against Quantum Adversaries

André Chailloux(✉) and Anthony Leverrier

Inria, Paris, France
{andre.chailloux,anthony.leverrier}@inria.fr

Abstract. In this paper, we show that the zero-knowledge construction for Hamiltonian Cycle remains secure against quantum adversaries in the relativistic setting. Our main technical contribution is a tool for studying the action of consecutive measurements on a quantum state which in turn gives upper bounds on the value of some entangled games. This allows us to prove the security of our protocol against quantum adversaries. We also prove security bounds for the (single-round) relativistic string commitment and bit commitment in parallel against quantum adversaries. As an additional consequence of our result, we answer an open question from [Unr12] and show tight bounds on the quantum knowledge error of some Σ-protocols.

Keywords: Relativistic cryptography · Zero-knowledge protocols · Quantum security

1 Introduction

1.1 Context

The goal of relativistic cryptography is to exploit the no superluminal signaling (NSS) principle in order to perform various cryptographic tasks. NSS states that no information carrier can travel faster than the speed of light. Note that this principle is closely related to the non-signaling principle that says that a local action performed in a laboratory cannot have an *immediate* influence outside of the lab. NSS is more precise since it gives an upper bound on the speed at which such an influence can propagate. Apart from this physical principle, we want to ensure information-theoretic security meaning that the schemes proposed cannot be attacked by any classical (or quantum) computers, even with unlimited computing power.

The idea of using the NSS principle for cryptographic protocols originated in a pioneering work by Kent in 1999 [Ken99] as a way to physically enforce a no-communication constraint between the different agents of one party (the idea of splitting up a party into several agents dates back to [BOGKW88], but without any explicit implementation proposal). The original goal of Kent

J.-S. Coron and J.B. Nielsen (Eds.): EUROCRYPT 2017, Part III, LNCS 10212, pp. 369–396, 2017.
DOI: 10.1007/978-3-319-56617-7_13

was to bypass the no-go theorems for quantum bit-commitment [May97,LC97]. More recently, quantum relativistic bit commitment protocols were developed where the parties exchange quantum systems, with the hope that combining the NSS principle together with quantum theory would lead to more secure (but less practical) protocols [Ken11,Ken12,KTHW13]. In particular, the protocol [Ken12] was implemented in [LKB+13]. We note that the scope of relativistic cryptography is not limited to bit commitment. For instance, there was recently some interest (sparked again by Kent) for position-verification protocols [KMS11,LL11,Unr14] but contrary to the case of bit commitment, it was shown that secure position-verification is impossible both in the classical and the quantum settings [CGMO09,BCF+14].

The original idea of [BOGKW88] was recently revisited by Crépeau *et al.* in [CSST11] (see also [Sim07]). Based on this work, Lunghi *et al.* devised a bit commitment protocol involving only four agents, two for Alice and two for Bob [LKB+15]. Their protocol is secure against quantum adversaries and a multi-round variant, with longer duration time, was shown to be secure against classical adversaries [LKB+15,CCL15,FF15]. While those protocols only seemed of theoretical interest at first, recent implementations have convincingly demonstrated that the required timing and location constraints can be efficiently enforced. In [VMH+16], the authors performed a 24-hour-long bit commitment with the pairs of agents standing 8 km apart.

The security analysis against quantum adversaries of [LKB+15] and against classical adversaries of [CCL15] relies on the study of variants of **CHSH** games where the inputs and outputs belong to the field $\mathbb{F}_Q$ for some large prime power Q, instead of $\{0,1\}$ for the usual **CHSH** game. In many cases, the (quantum) security of a relativistic protocol can be derived from the value of an (entangled) 2-player game. Because the relativistic constraint essentially boils down to 2 non-communicating provers, a relativistic protocol can also be seen as a 2-prover interactive protocol.

—

The above results are promising for relativistic cryptography but very limited in scope. Indeed, bit commitment schemes are used as parts of larger cryptosystems. The only study of the composability of the $\mathbb{F}_Q$ bit commitment scheme was done in [FF15] but mainly with itself, in order to increase the commit time. There has not been any proposition to use this scheme for a more general purpose.

One natural application of bit commitment are zero-knowledge protocols. With such a protocol, a prover wishes to convince a verifier that a given statement is true without revealing any extra information. A zero-knowledge protocol is already a more advanced cryptographic primitive and has more direct applications such as identification schemes [GMR89] for instance. Here, we will consider the zero-knowledge construction for Hamiltonian Cycle, which is an NP complete problem. The prover will convince the verifier that a given graph $G = (V, E)$ has a Hamiltonian cycle, *i.e.* a cycle going through each vertex exactly once, without revealing any information, in particular no information about this cycle. Since Hamiltonian Cycleis NP complete, a zero-knowledge

protocol for this problem can be used to obtain a zero-knowledge protocol for arbitrary NP problems.

There is a known zero-knowledge protocol for Hamiltonian Cycle using bit commitment first presented by Blum [Blu86] which we recall now.

Zero-knowledge protocol for Hamiltonian Cycle using bit commitment

1. The prover picks a random permutation $\Pi : V \to V$. He commits to each of the bits of the adjacency matrix $M_{\Pi(G)}$ of $\Pi(G)$.
2. The verifier sends a random bit (called the challenge) $chall \in \{0, 1\}$ to the prover.
3. – If $chall = 0$, the prover decommits to all the elements of $M_{\Pi(G)}$, and reveals Π.
   – If $chall = 1$, he reveals only the bits (of value 1) of the adjacency matrix that correspond to a Hamiltonian cycle $\mathcal{C}'$ of $\Pi(G)$.
4. The verifier checks that these decommitments are valid and correspond, for $chall = 0$ to $M_{\Pi(G)}$ and, for $chall = 1$, to a Hamiltonian cycle.

It is natural to combine this zero-knowledge protocol with the $\mathbb{F}_{\mathsf{Q}}$ relativistic bit commitment protocol mentioned above. The (single-round) $\mathbb{F}_{\mathsf{Q}}$ relativistic bit commitment protocol is secure against quantum adversaries but it doesn't directly imply that the zero-knowledge protocol remains secure. Indeed, the security definition considered for the bit commitment is fairly weak and composes poorly with other protocols. The soundness of the protocol against entangled provers will be reduced to a 2-player entangled game. Proving zero-knowledge against a quantum verifier can sometimes be complicated because of the presence of a quantum auxiliary input. In this case, however, due to properties of the relativistic $\mathbb{F}_{\mathsf{Q}}$ bit commitment, we will not need any rewinding from our simulator and the simulation will actually be rather simple.

—

The goal of this paper is to show that it is indeed possible to plug in the $\mathbb{F}_{\mathsf{Q}}$ relativistic bit commitment protocol into Blum's zero-knowledge protocol for Hamiltonian Cycle. This widens the possible applications for relativistic cryptography and will encourage further implementations.

The main contribution of this paper is a technical analysis involving successive measurements on a quantum system. Indeed, to prove that the above scheme is secure against quantum adversaries, we use the fact that an adversary who can answer both challenges at the same time can guess the value of a string on which he has no information, due to non-signaling. This naturally involves consecutive measurements on a quantum system, and leads us to analyze how the first measurement disturbs the system before the second measurement.

1.2 Relativistic Zero-Knowledge Protocol for Hamiltonian Cycle

Here, we show how the final protocol will look like and where exactly we rely on the physical NSS principle. The final protocol is the following:

Relativistic zero knowledge protocol for Hamiltonian Cycle

Input — The provers and the verifiers are given a graph $G = (V, E)$.
Auxiliary Input — The provers P_1 and P_2 know a Hamiltonian cycle $\mathcal{C}$ of G.
Preprocessing — P_1 and P_2 agree beforehand on a random permutation $\Pi : V \to V$ and on an $n \times n$ matrix $A \in \mathcal{M}_n^{\mathbb{F}_Q}$ where each element of A is chosen uniformly at random in $\mathbb{F}_Q$.
Protocol —

1. Commitment to each bit of $M_{\Pi(G)}$: V_1 sends a matrix $B \in \mathcal{M}_n^{\mathbb{F}_Q}$ where each element of B is chosen uniformly at random in $\mathbb{F}_Q$. P_1 outputs the matrix $Y \in \mathcal{M}_n^{\mathbb{F}_Q}$ such that $\forall i, j \in [n],\ Y_{i,j} = A_{i,j} + (B_{i,j} * (M_{\Pi(G)})_{i,j})$.
2. The verifier sends a random bit (called the challenge) $chall \in \{0, 1\}$ to the prover.
3. – If $chall = 0$, P_2 decommits to all the elements of $M_{\Pi(G)}$, *i.e.* he sends all the elements of A to V_2 and reveals Π.
   – If $chall = 1$, P_2 reveals only the bits (of value 1) of the adjacency matrix that correspond to a Hamiltonian cycle $\mathcal{C}'$ of $\Pi(G)$, *i.e.* for all edges (u, v) of $\mathcal{C}'$, he sends $A_{u,v}$ as well as $\mathcal{C}'$.
4. The verifier checks that those decommitments are valid and correspond to what the provers have declared. He also checks that the timing constraint of the bit commitment is satisfied. This means that
   – if $chall = 0$, the prover's opening A must satisfy $\forall i, j \in [n],\ Y_{i,j} = A_{i,j} + (B_{i,j} * (M_{\Pi(G)})_{i,j})$.
   – if $chall = 1$, the prover's opening A must satisfy $\forall (u, v) \in \mathcal{C}',\ Y_{u,v} = A_{u,v} + B_{u,v}$.

The above protocol is obtained by plugging in the $\mathbb{F}_Q$ relativistic bit commitment protocol into Blum's zero-knowledge protocol for Hamiltonian Cycle. We discuss more the setting in Sects. 4 and 5. We just want here to briefly present in which way we use the no superluminal signaling condition in this protocol.

In order for the protocol to be secure, we require the following:

1. Both the prover and the verifier are split into 2 agents, respectively P_1, P_2 and V_1, V_2.
2. V_1 and V_2 are far apart (we discuss this later).
3. The opening phase (steps 2 and 3) must be performed as soon as the commit phase (step 1) is completed.

Constraints (2) and (3) are here to enforce that during step 3 of the protocol, *the message P_2 sends to V_2 does not depend on the matrix B sent by V_1.*

Because information travels at most at light speed, by synchronizing the steps well enough, the verifiers can enforce this condition. For instance, it is sufficient to check that V_2 receives the message from P_2 before the information on B sent by V_1 had time to reach V_2. If this is the case, then it guarantees that P_2's answer to the challenge cannot depend on the value of the matrix B, since otherwise it would violate the NSS. An important consequence is that we do not require the verifiers to know anything about the spatial locations of the provers: it is sufficient for the verifiers to know their own relative position.

As said before, there were already several experiments made that showed how to achieve the above constraints. The most notable one [VMH+16] succeeded in performing the above bit commitment protocol by having V_1 and V_2 being 8 km apart, which shows it can be achievable in real life conditions.

In summary, the main contribution of the paper is to prove the security of the above protocol for Hamiltonian Cycle against quantum adversaries. The main challenge is to prove the soundness property, *i.e.* security against a cheating prover on an input which *does not* contain a Hamiltonian cycle. Here, we have two dishonest provers P_1 and P_2 that want to pass the protocol even though the input graph does not contain a Hamiltonian cycle. A cheating prover that would be able to answer simultaneously to both challenges could break the underlying string commitment scheme, which is a consequence of the special soundness property of the scheme.

To prove the security of the above protocol against quantum adversaries, we will, from a cheating strategy, construct a strategy that will successfully answer both challenges by consecutively applying the cheating strategy for each challenge, which is expressed by our consecutive measurement theorem (see Theorem 1 below). We can also view this cheating scenario as a 2-player entangled game and we will show how in general our theorem regarding quantum consecutive measurements can be translated into a bound on the entangled value of 2-player games.

1.3 Consecutive Measurements

Our main technical contribution is expressed by the following theorem

Theorem 1. *Consider n projectors $P_1, \dots, P_n$ such that for each i, we can write $P_i := \sum_{s=1}^{S} P_i^s$ where the $\{P_i^s\}_s$ are orthogonal projectors for each i, i.e. for each i and s, s', we have $P_i^s P_i^{s'} = \delta_{s,s'} P_i^s$. Let σ be any quantum state, let $V := \frac{1}{n}\sum_{i=1}^{n} tr(P_i\sigma)$, and let $E := \frac{1}{n(n-1)}\sum_{i,j\neq i}\sum_{s,s'=1}^{S} tr(P_j^{s'} P_i^s \sigma P_i^s P_j^{s'})$. Then it holds that $E \geq \frac{1}{64S}\left(V - \frac{1}{n}\right)^3$.*

Such a statement can be fairly easily transposed to the context of games: see Proposition 1 below. This theorem can be seen as a generalization of the *gentle measurement* lemma [Win99], which is similar to the above with $n = 2$ and $S = 1$. The case of $n = 2$ can be seen as a worst-case consecutive measurement theorem: how much can the first measurement disturb the measured state before the second measurement? However, for larger values of n, this shows that when

we pick 2 measurements out of n, the disturbance is much smaller, as shown by the dependence of the lower bound in n. Our theorem also improves on known results since it deals with larger values of S.

Interestingly, this kind of statement has already appeared previously in a paper by Unruh [Unr12], who studied quantum sigma protocols and in particular quantum proofs of knowledge. He showed the following

Theorem 2 [Unr12]**.** *Consider n projectors $P_1, \ldots, P_n$ and an arbitrary quantum state σ. Let $V := \frac{1}{n}\sum_{i=1}^{n} tr(P_i\sigma)$, and let $E := \frac{1}{n(n-1)}\sum_{i,j\neq i} tr(P_jP_i\sigma P_iP_j)$. If $V \geq \frac{1}{\sqrt{n}}$ then $E \geq V(V^2 - \frac{1}{n})$.*

Let us now compare our main theorem to Unruh's one, for the case of $S = 1$ where they are comparable. If $V \gg \frac{1}{\sqrt{n}}$ then both bounds give essentially the same bound $E \geq \Omega(V^3)$ which will translate into the relation $\omega^*(G_{coup}) \geq \Omega(\omega^*(G)^3)$ for the entangled values of a game G and its coupled version G_{coup} (see below). However, Theorem 2 is only valid when $V \geq \frac{1}{\sqrt{n}}$ while Theorem 1 works for any $V \geq \frac{1}{n}$. Moreover, Theorem 1 is tight in its extremal point in the sense that there exist a quantum state and n projectors such that $V = \frac{1}{n}$ and $E = 0$, as can be seen by considering for example $\sigma = |\phi\rangle\langle\phi|$ with $|\phi\rangle := \frac{1}{\sqrt{n}}\sum_i |i\rangle$ and $P_i = |i\rangle\langle i|$.

—

A natural application of our consecutive measurement theorem is to bound the value of some entangled games. The phrasing in terms of nonlocal games is sometimes more comfortable to use. In this paper, our security proofs will usually reduce to bounding the entangled value of such game, that is the maximum winning probability for a pair of players allowed to share arbitrary entangled states as a resource. For any game G on the uniform distribution (meaning that the inputs of the game are drawn independently from the uniform distribution), we define the game G_{coup} (consisting of a certain *couple* of instances of G) as follows:

- In G, Alice and Bob respectively receive x and y taken from the uniform distribution on the sets I_A and I_B, respectively, and output a and b such that $V(a, b|x, y) = 1$ for some valuation function V specified by G.
- In G_{coup}, Alice receives a random x as in G and Bob receives a pair of distinct random inputs (y, y'). Alice outputs a and Bob outputs a pair (b, b'). They win the game if $V(a, b|x, y) = 1$ and $V(a, b'|x, y') = 1$, that is, if they win both instances of the game G, but for the same input/output pair of Alice.

In many cases, upper bounding the value of G_{coup} will follow directly from a non-signaling argument of the form: "If the players are able to win G_{coup} with probability p then Bob can learn some (or all) bits of x with probability p and no-signaling implies that $p \leq 1/|I_A|$". What is left to do is to relate the entangled values of both games, $\omega^*(G)$ and $\omega^*(G_{coup})$. To do this, we construct the following strategy for G_{coup}: Alice follows the same strategy as for G; on

inputs (y, y'), Bob performs the same strategy (measurement) as for G on input y to get output b and then on input y' to get b'. Note here that the non trivial part is that Bob's second measurement is applied on the post-measurement state resulting from his first measurement. Because we are in the quantum setting, this first measurement will generally perturb the state shared by Alice and Bob, which makes it non trivial to relate the success probability of this strategy for G_{coup} with the entangled value $\omega^*(G)$ of the original game G.

A similar construction of *squared games* was introduced in [DS14,DSV15] to study projective classical and entangled games. There, the input x is not revealed to the players but they receive respectively y and y' and output b and b'. They win if there exists a such that $V(a, b|x, y) = V(a, b'|x, y') = 1$. It would be interesting to see the similarities and differences between those two approaches.

We show the following.

Proposition 1. *For any game G on the uniform distribution which is S-projective, we have $\omega^*(G_{coup}) \geq \frac{1}{S \cdot 64} \cdot (\omega^*(G) - \frac{1}{n})^3$ where n is dimension of Bob's input.*

A game G is said to be S-projective if for all x, y, a, there are at most S possible outputs for Bob that allow them to win the game, *i.e.* $\max_{x,y,a} |\{b : V(a, b|x, y) = 1\}| \leq S$.

In order to prove this statement, we need to analyze the strategy that we presented above. As already mentioned, the main difficulty is that the first measurement from Bob will modify the common shared state and therefore we cannot directly bound the probabilities related to the second measurement. One way of analyzing these consecutive measurements would be to use a kind of gentle measurement lemma but unfortunately, this would only work when the winning probability $\omega^*(G)$ is close to 1, which isn't the case for the games we consider.

Fortunately, Theorem 1 is tailored for this kind of applications and can be used directly to prove the above proposition. We can notice the exact transposition of the parameters of Theorem 1 to Proposition 1.

1.4 Applications of the Bound

1. First, we prove that the extensions of the $\mathbb{F}_{\mathsf{Q}}$ bit commitment to string commitment and its parallel repetition remain secure against quantum adversaries with using the sum-binding definition. This is a direct consequence on upper bounds on the entangled value of **CHSH** variants, like the $\mathbf{CHSH}_{\mathbf{Q}}(P)$ game introduced in [CCL15].
2. We show that the presented relativistic zero-knowledge protocol for Hamiltonian Cycle is secure against quantum adversaries. This also implies a 2-prover 1-round zero-knowledge protocol for Hamiltonian Cycle also secure against quantum adversaries.
3. Finally, as a direct corollary of our consecutive measurement claim, we answer an open question from Unruh regarding quantum proofs of knowledge [Unr12]. We show tight bounds on the quantum knowledge error of a Σ-protocol with

strict and special soundness as function of the challenge size, matching the classical bound. We will not discuss in detail this result as it just requires to plug our bound in the proof of [Unr12] and is a bit beyond the scope of this paper. However, this shows that our results are useful beyond just the study of relativistic protocols or entangled games.

The last point shows that our bound could find even more applications when considering security against quantum adversaries. Indeed, when studying cryptographic protocols, for instance Σ-protocols, a notion that often appears is *special soundness* which roughly states that an attacker shouldn't be able to simultaneously answer successfully to 2 verifier's challenges. The relativistic zero-knowledge protocol we study is one example of this and Unruh's quantum proofs of knowledge setting is another one but there are more where our theorem could be useful.

Organisation of the Paper. In Sect. 2, we prove our main consecutive measurement theorem. In Sect. 3, we show how to use this bound for proving upper bounds on the entangled value of nonlocal games. In Sect. 4, we present in more detail the relativistic model and the $\mathbb{F}_{\mathsf{Q}}$ relativistic bit commitment protocol. Finally, in Sect. 5, we describe the protocol obtained by plugging this bit commitment into Blum's zero-knowledge protocol for Hamiltonian Cycle and we prove that it remains secure, even against quantum adversaries.

2 Consecutive Measurement Theorems

We first present some useful lemmata in the preliminaries. Then, we dive in directly in the proof of our consecutive measurements theorems.

2.1 Preliminaries

Lemma 1. *Let $|\phi\rangle$ a quantum pure state, $P \leq \mathbb{I}$ a projector acting on $|\phi\rangle$ and $|\psi\rangle := \frac{P(|\phi\rangle)}{||P(|\phi\rangle)||}$. We have $|\langle\phi|\psi\rangle|^2 = ||P(|\phi\rangle)||^2 = tr(P|\phi\rangle\langle\phi|)$.*

Proof. We write $|\phi\rangle = P(|\phi\rangle) + (\mathbb{I} - P)(|\phi\rangle) = ||P(|\phi\rangle)||\ |\psi\rangle + (\mathbb{I} - P)(|\phi\rangle)$. By noticing that $\langle\psi|\mathbb{I} - P|\phi\rangle = 0$, we get $|\langle\phi|\psi\rangle|^2 = ||P(|\phi\rangle)||^2 = tr(P|\phi\rangle\langle\phi|)$.

Lemma 2. *Let $|\phi\rangle$ a quantum pure state, $P \leq \mathbb{I}$ a projector acting on $|\phi\rangle$ and $|\psi\rangle$ such that $P|\psi\rangle = |\psi\rangle$. We have $|\langle\phi|\psi\rangle|^2 \leq tr(P|\phi\rangle\langle\phi|)$.*

Proof. We decompose $|\phi\rangle$ in order to make $|\psi\rangle$ appear. We write $|\phi\rangle = \alpha|\psi\rangle + \beta|\psi^\perp\rangle$ with $|\alpha|^2 + |\beta|^2 = 1$ and $\langle\psi|\psi^\perp\rangle = 0$. This gives us $P|\phi\rangle = \alpha|\psi\rangle + \beta P|\psi^\perp\rangle$. Notice that we also have $\langle\psi|P|\psi^\perp\rangle = 0$. From there, we conclude

$$tr(P|\phi\rangle\langle\phi|) = ||P|\phi\rangle||^2 = |\alpha|^2 + |\beta|^2||P|\psi^\perp\rangle||^2 \geq |\alpha|^2 = |\langle\phi|\psi\rangle|^2.$$

2.2 Single Outcome Case : S = 1

We first prove the theorem for the case where $S = 1$.

Theorem 3. *Consider n projectors $P_1, \ldots, P_n$ and a quantum mixed state σ in some Hilbert space $\mathcal{B}$. Let $V := \frac{1}{n}\sum_{i=1}^{n} tr(P_i\sigma)$, and let*

$$E := \frac{1}{n(n-1)} \sum_{i,j\neq i} tr(P_j P_i \sigma P_i P_j).$$

Then it holds that $E \geq \frac{1}{64}\left(V - \frac{1}{n}\right)^3$.

Proof. We fix a quantum mixed state σ in some Hilbert space $\mathcal{B}$ and n projectors $P_1, \ldots, P_n$ acting on $\mathcal{B}$. We first move to the realm of pure states which will be easier to analyze by adding an extra Hilbert space $\mathcal{E}$. We consider a purification $|\phi\rangle$ of σ in some space $\mathcal{BE} = \mathcal{B} \otimes \mathcal{E}$. We define

$$|\phi_i\rangle := \frac{(P_i \otimes \mathbb{1}_{\mathcal{E}})|\phi\rangle}{||(P_i \otimes \mathbb{1}_{\mathcal{E}})|\phi\rangle||}.$$

The state $|\phi_i\rangle$ corresponds to the normalized projection of $|\phi\rangle$ using P_i. We first express E and V as inner products of the quantum pure states we defined:

Lemma 3. $E \geq \frac{1}{n(n-1)} \sum_{i,j\neq i} |\langle\phi|\phi_i\rangle|^2 |\langle\phi_i|\phi_j\rangle|^2$ *and* $V = \frac{1}{n}\sum_{i=1}^{n} |\langle\phi|\phi_i\rangle|^2$.

Proof. We write

$$\begin{aligned} E &= \frac{1}{n(n-1)} \sum_{i,j\neq i} tr(P_j P_i \sigma P_i P_j) \\ &= \frac{1}{n(n-1)} \sum_{i,j\neq i} tr\left((P_j \otimes \mathbb{1}_{\mathcal{E}})(P_i \otimes \mathbb{1}_{\mathcal{E}})|\phi\rangle\langle\phi|(P_i \otimes \mathbb{1}_{\mathcal{E}})(P_j \otimes \mathbb{1}_{\mathcal{E}})\right) \end{aligned}$$

Here, by using Lemma 1, notice that

$$(P_i \otimes \mathbb{1}_{\mathcal{E}})|\phi\rangle\langle\phi|(P_i \otimes \mathbb{1}_{\mathcal{E}}) = ||(P_i \otimes \mathbb{1}_{\mathcal{E}})|\phi\rangle||^2 |\phi_i\rangle\langle\phi_i| = |\langle\phi|\phi_i\rangle|^2 |\phi_i\rangle\langle\phi_i|.$$

From there, we can continue have

$$\begin{aligned} E &= \frac{1}{n(n-1)} \sum_{i,j\neq i} |\langle\phi|\phi_i\rangle|^2 tr\left((P_j \otimes \mathbb{1}_{\mathcal{E}})|\phi_i\rangle\langle\phi_i|\right) \\ &\geq \frac{1}{n(n-1)} \sum_{i,j\neq i} |\langle\phi|\phi_i\rangle|^2 |\langle\phi_i|\phi_j\rangle|^2 \end{aligned}$$

where the last inequality comes from Lemma 2. Notice also that we immediately have $V = \frac{1}{n}\sum_{i=1}^{n} tr(P_i\sigma) = \sum_i |\langle\phi|\phi_i\rangle|^2$.

Our goal is to relate E and V. We will deal with the terms $|\langle\phi_i|\phi_j\rangle|^2$ using the following proposition on almost orthogonal states.

Proposition 2. *Consider n quantum pure states $|\phi_1\rangle, \ldots, |\phi_n\rangle$. Let*

$$S := \max_{|\Omega\rangle} \sum_{i=1}^{n} |\langle \Omega | \phi_i \rangle|^2 \quad \textit{and} \quad C := \sum_{i,j \neq i}^{n} |\langle \phi_i | \phi_j \rangle|^2.$$

We have $S \leq 1 + \sqrt{\frac{(n-1)C}{n}} \leq 1 + \sqrt{C}$.

Proof. Let $M = \sum_{i=1}^{n} |\phi_i\rangle\langle\phi_i|$. M is a positive semi-definite matrix of dimension at most n. Let $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$ the n eigenvalues of M in decreasing order. We have $\sum_i \lambda_i = tr(M) = \sum_j tr(|\phi_j\rangle\langle\phi_j|) = n$. Moreover, notice that $S = \max_{|\Omega\rangle} \sum_i |\langle \Omega | \phi_i \rangle|^2 = \lambda_1$.

We write $M^2 = \sum_{i,j} \langle \phi_i | \phi_j \rangle |\phi_i\rangle\langle\phi_j|$ and $tr(M^2) = \sum_{i,j} |\langle \phi_i | \phi_j \rangle|^2 = n + C$. Moreover, we have $tr(M^2) = \sum_i \lambda_i^2$. This gives us

$$\begin{aligned} n + C = tr(M^2) &= \sum_{i=1}^{n} \lambda_i^2 = \lambda_1^2 + \sum_{i=2}^{n} \lambda_i^2 \geq \lambda_1^2 + (n-1)\left(\frac{n-\lambda_1}{n-1}\right)^2 \\ &= \lambda_1^2 + \frac{(n-\lambda_1)^2}{n-1} = S^2 + \frac{(n-S)^2}{n-1} \end{aligned}$$

where the inequality comes from the convexity of the square function. From there, we have

$$(n-1)S^2 + (n-S)^2 - n(n-1) \leq (n-1)C$$

Using $(n-1)S^2 + (n-S)^2 - n(n-1) = n(S-1)^2$, we conclude that $n(S-1)^2 \leq (n-1)C$ or equivalently $S \leq 1 + \sqrt{\frac{(n-1)C}{n}}$.

In particular, the above proposition implies that

$$V \leq \frac{1}{n} + \frac{n-1}{n} \sqrt{\frac{1}{n(n-1)} \sum_{i,j \neq i} |\langle \phi_i | \phi_j \rangle|^2}.$$

The term in the squared root is very similar to E. Unfortunately, the expression for E contains an extra factor $|\langle \phi | \phi_i \rangle|^2$ in the sum under the square-root. If the quantity $|\langle \phi | \phi_i \rangle|^2$ was independent of i, it would be equal to V and we would be able to conclude. However, this is not always the case and this adds a difficulty in the proof. In order to overcome it, we will use Proposition 2 only with the states for which $|\langle \phi | \phi_i \rangle|^2$ is not too small. We will choose a threshold κ (that will be fixed later) and consider only the indices i for which $|\langle \phi | \phi_i \rangle|^2 \geq V/\kappa$. This is the goal of the next proposition.

Proposition 3. $\forall \kappa > 1,\ V \leq \left(1 + \frac{1}{\kappa - 1}\right)\left(\frac{1}{n} + \sqrt{\frac{\kappa E}{V}}\right)$.

Proof. For all i, let $p_i := |\langle\phi|\phi_i\rangle|^2$. We have by definition $V = \sum_i p_i$. We fix $\kappa > 1$ and define the set $Z := \{i \in [n] : p_i \geq \frac{V}{\kappa}\}$. We have

$$\frac{1}{n}\sum_{i\notin Z} p_i \leq \frac{1}{n}\sum_{i\notin Z}\frac{V}{\kappa} \leq \frac{V}{\kappa},$$

which implies

$$\frac{1}{n}\sum_{i\in Z} p_i \geq (1-\frac{1}{\kappa})V. \tag{1}$$

We write

$$E \geq \frac{1}{n(n-1)}\sum_{i,j\neq i} p_i|\langle\phi_i|\phi_j\rangle|^2 \geq \frac{1}{n(n-1)}\sum_{\substack{i,j\in Z\\ i\neq j}} p_i|\langle\phi_i|\phi_j\rangle|^2 \tag{2}$$

$$\geq \frac{V}{\kappa}\cdot\frac{1}{n(n-1)}\sum_{\substack{i,j\in Z\\ i\neq j}}|\langle\phi_i|\phi_j\rangle|^2. \tag{3}$$

Now, starting from Eq. 1, we have

$$V \leq \frac{1}{1-\frac{1}{\kappa}}\frac{1}{n}\sum_{i\in Z} p_i = \frac{1}{1-\frac{1}{\kappa}}\frac{1}{n}\sum_{i\in Z}|\langle\phi|\phi_i\rangle|^2 \leq \left(1+\frac{1}{\kappa-1}\right)\max_{|\Omega\rangle}\frac{1}{n}\sum_{i\in Z}|\langle\Omega|\phi_i\rangle|^2$$

$$\leq \left(1+\frac{1}{\kappa-1}\right)\left(\frac{1}{n}+\sqrt{\frac{1}{n(n-1)}\sum_{\substack{i,j\in Z\\ i\neq j}}|\langle\phi_i|\phi_j\rangle|^2}\right) \tag{4}$$

$$\leq \left(1+\frac{1}{\kappa-1}\right)\left(\frac{1}{n}+\sqrt{\frac{\kappa E}{V}}\right) \tag{5}$$

where we used Lemma 2 in Eqs. 4 and 2 for the last inequality. This proves the proposition.

We can now use Proposition 3 to prove our theorem. We distinguish two cases:

1. If $(\frac{V}{n^2E})^{1/3} > 2$. We take $\kappa = (\frac{V}{n^2E})^{1/3} > 2$ which implies $\kappa(\frac{n^2E}{V})^{1/3} = 1$ and $(\kappa\frac{n^2E}{V})^{\frac{1}{2}} = \frac{1}{\kappa}$. We get

$$V \leq \frac{1}{n}\Big(1+\frac{1}{\kappa-1}\Big)\left(1+\left[\kappa\frac{n^2E}{V}\right]^{1/2}\right) = \frac{1}{n}\Big(1+\frac{1}{\kappa-1}\Big)\Big(1+\frac{1}{\kappa}\Big)$$
$$\leq \frac{1}{n}(1+\frac{4}{\kappa}) = \frac{1}{n}+4\left(\frac{E}{nV}\right)^{1/3}.$$

This gives $E \geq \frac{nV}{64}(V - \frac{1}{n})^3$ which implies $E \geq \frac{1}{64}(V - \frac{1}{n})^3$. To see this last implication, consider the following two cases: if $V \geq \frac{1}{n}$ then the equality comes immediately from the previous inequality. If $V \leq \frac{1}{n}$, we immediately have $E \geq 0 \geq \frac{1}{64}(V - \frac{1}{n})^3$.

2. If $(\frac{V}{n^2 E})^{1/3} \leq 2$. This implies $\left(\frac{V}{E}\right)^{1/2} \leq n \cdot 2^{3/2}$. We take $\kappa = 2$ and obtain

$$V \leq \left(1 + \frac{1}{\kappa - 1}\right)\left(\frac{1}{n} + \sqrt{\frac{\kappa E}{V}}\right) = 2(\frac{1}{n} + \sqrt{\frac{2E}{V}})$$
$$\leq 2(2^{2/3}\sqrt{\frac{E}{V}} + \sqrt{\frac{2E}{V}}) \leq 6\sqrt{\frac{E}{V}}$$

which implies $E \geq \frac{V^3}{36} \geq \frac{1}{64}(V - \frac{1}{n})^3$.

2.3 General Case

We can now show our theorem for any S. The general case will be a direct corollary of the following.

Proposition 4. *Let a projector $P := \sum_{i=1}^m P_i$ where $\{P_i\}_{i \in [m]}$ are orthogonal projectors. For any pure state $|\psi\rangle$, we have*

$$\sum_{i=1}^m P_i |\psi\rangle\langle\psi| P_i \geq \frac{1}{m} P|\psi\rangle\langle\psi|P.$$

We note that this result can be obtained as an application of the pinching inequality [Hay02,SBT16], but we provide a proof here for completeness.

Proof. We define the following *unnormalized states* $|\psi^P\rangle = P(|\psi\rangle)$ and $|\psi_i^P\rangle = P_i(|\psi\rangle)$. Because $P = \sum_i P_i$, we have $|\psi^P\rangle = \sum_i |\psi_i^P\rangle$. This gives

$$\sum_{i=1}^m P_i|\psi\rangle\langle\psi|P_i = \sum_{i=1}^m |\psi_i^P\rangle\langle\psi_i^P|$$
$$P|\psi\rangle\langle\psi|P^\dagger = |\psi^P\rangle\langle\psi^P|$$

Consider now any state $|\phi\rangle = \sum_i \alpha_i |\psi_i^P\rangle + |\xi\rangle$ where $|\xi\rangle$ is orthogonal to all the $|\psi_i^P\rangle$. We have

$$\langle\phi|\sum_{i=1}^m P_i|\psi\rangle\langle\psi|P_i|\phi\rangle = \sum_i |\langle\psi_i^P|\phi\rangle|^2 = |\alpha_i|^2 \left|\langle\psi_i^P|\psi_i^P\rangle\right|^2$$

and

$$\langle\phi|P|\psi\rangle\langle\psi|P|\phi\rangle = |\langle\psi^P|\phi\rangle|^2 = \left|\sum_i \alpha_i \langle\psi_i^P|\psi_i^P\rangle\right|^2$$

From there, we can conclude. We have:

$$\begin{aligned}\langle\phi|\sum_{i=1}^{m} P_i|\psi\rangle\langle\psi|P_i|\phi\rangle &= \sum_i |\alpha_i|^2 |\langle\psi_i^P|\psi_i^P\rangle|^2 \\ &\geq \frac{1}{m}\left|\sum_i |\alpha_i||\langle\psi_i^P|\psi_i^P\rangle|\right|^2 \qquad \text{(from Cauchy-Schwarz)} \\ &\geq \frac{1}{m}\langle\phi|P|\psi\rangle\langle\psi|P|\phi\rangle\end{aligned}$$

Since this holds for any state $|\phi\rangle$, we can conclude that

$$\sum_{i=1}^{m} P_i|\psi\rangle\langle\psi|P_i \geq \frac{1}{m}P|\psi\rangle\langle\psi|P^\dagger.$$

From there, and using the previous theorem, we can show our main technical result.

Theorem 1. *Consider n projectors $P_1, \ldots, P_n$ such that for each i, we can write $P_i := \sum_{s=1}^{S} P_i^s$ where the $\{P_i^s\}_s$ are orthogonal projectors for each i, i.e. for each i and s, s', we have $P_i^s P_i^{s'} = \delta_{s,s'} P_i^s$. Let σ be any quantum state, let $V := \frac{1}{n}\sum_{i=1}^{n} tr(P_i\sigma)$, and let $E := \frac{1}{n(n-1)}\sum_{i,j\neq i}\sum_{s,s'=1}^{S} tr(P_j^{s'} P_i^s \sigma P_i^s P_j^{s'})$. Then it holds that $E \geq \frac{1}{64S}\left(V - \frac{1}{n}\right)^3$.*

Proof. We fix n projectors $P_1, \ldots, P_n$ such that for each i, we can write $P_i := \sum_{s=1}^{S} P_i^s$ where the $\{P_i^s\}_s$ are orthogonal projectors for each i. We fix a quantum state σ. We have

$$\begin{aligned}E &= \frac{1}{n(n-1)}\sum_{i,j\neq i}\sum_{s,s'=1}^{S} tr(P_j^{s'} P_i^s \sigma(P_i^{s'})(P_j^s)) \\ &= \frac{1}{n(n-1)}\sum_{i,j\neq i}\sum_{s=1}^{S} tr(P_j P_i^s \sigma(P_i^{s'})P_j) \\ &\geq \frac{1}{Sn(n-1)}\sum_{i,j\neq i} tr(P_j P_i \sigma(P_i)P_j) \qquad \text{(from Proposition 4)} \\ &\geq \frac{1}{64S}\left(V - \frac{1}{n}\right)^3 \qquad \text{(from Theorem 3)}\end{aligned}$$

3 Entangled Games

The goal of this section is to use the consecutive measurement theorems of the previous section to establish upper bounds on the value of entangled games. For a game G on the uniform distribution, we will define a game G_{coup} which corresponds to a couple of instances of G where Alice plays twice with the same

input and Bob receives two distinct inputs and they need to win both instances in order to win the game G_{coup}. In the cases we consider, upper bounding G_{coup} will be easily done from non-signaling. Our learning lemmata will allow us to relate the winning probabilities of G and G_{coup}. These two steps together will give us bounds on the value of G.

3.1 First Definitions

Definition 1. *A game $G = (I_A, I_B, O_A, O_B, V, p)$ is defined by*

- *2 input sets I_A, I_B which are respectively Alice's and Bob's input sets.*
- *2 output sets sets O_A, O_B which are respectively Alice's and Bob's output sets.*
- *A valuation function $V : I_A \times I_B \times O_A \times O_B \to \{0, 1\}$ which indicates whether the game is won for some fixed input and outputs. The game is won if the value of V is 1.*
- *A probability function $p : I_A \times I_B \to [0, 1]$ which corresponds to the input distribution. We have $\sum_{(x,y)\in I_A\times I_B} p_{xy} = 1$.*

Definition 2. *A game $G = (I_A, I_B, O_A, O_B, V, p)$ is said to be* on the uniform distribution *if $\forall (x, y) \in I_A \times I_B,\ p_{xy} = \frac{1}{|I_A||I_B|}$.*

Definition 3. *A game $G = (I_A, I_B, O_A, O_B, V, p)$ is* projective *if*

$$\forall (x, y) \in I_A \times I_B \text{ st. } p_{xy} \neq 0,\ \forall a \in O_A,\ \exists!\ b \in O_B,\ \text{st. } V(x, y, a, b) = 1.$$

*A game G is S-*projective *if*

$$\forall (x, y) \in I_A \times I_B \text{ st. } p_{xy} \neq 0, \forall a \in O_A, |\{b \in O_B : V(x, y, a, b) = 1\}| \leq S.$$

In particular, a projective game is 1-projective.

In the case where Alice and Bob are classical and want to win a game G, it is known that their optimal strategy to win is to perform a deterministic strategy. Notice that a projective game is asymmetric in Alice and Bob.

Definition 4. *For a game $G = (I_A, I_B, O_A, O_B, V, p)$, we denote by $\omega^*(G)$ its entangled value, i.e. the maximum winning probability for the game when Alice and Bob are quantum and share an entangled state.*

In order to study this maximal winning probability, it is enough to consider the case where Alice and Bob perform projective measurements.

In order to prove upper bounds on $\omega^*(G)$ for a game G on the uniform distribution, we introduce the notion of coupled game G_{coup}.

Definition 5. *For any game $G = (I_A, I_B, O_A, O_B, V, p)$ on the uniform distribution we define G_{coup} as follows:*

- *Alice receives a random $x \in_R I_A$. Bob receives a random pair of* different *inputs (y, y') from I_B.*
- *Alice outputs $a \in O_A$. Bob outputs $b, b' \in O_B$.*
- *They win the game if $V(x, y, a, b) = V(x, y', a, b') = 1$.*

3.2 Relating G and G_{coup}

In this section, we use our results from the previous section to relate the values of G and G_{coup}.

Proposition 1. *For any game G on the uniform distribution which is S- projective, we have $\omega^*(G_{coup}) \geq \frac{1}{S \cdot 64}(\omega^*(G) - \frac{1}{n})^3$ where $n = |I_B|$.*

Proof. Consider an optimal strategy for Alice and Bob for the game G. In particular, for each y, let $Q^y = \{Q_b^y\}$ the projective measurement that corresponds to his strategy for input y. Fix an input/output pair (x, a) for Alice and let σ^{xa} be the state held by Bob, conditioned on this pair. For each y, let $W_y = \{b : V(a, b|x, y) = 1\}$ be the set of winning outputs for Bob. Since G is S-projective, we have $|W_y| \leq S$. We define $Q_W^y = \sum_{b \in W_y} Q_b^y$.

We denote by V^{xa} the probability that Alice and Bob win the game for a fixed x, a. Notice that $\omega^*(G) = \mathbb{E}_{xa}[V^{xa}]$. We have

$$V^{xa} = \frac{1}{n} \sum_y tr(Q_W^y \sigma^{xa}(Q_W^y)),$$

since y is uniformly distributed over the set I_B of size n.

We now consider the following quantum strategy for G_{coup}: Alice and Bob share the same initial state as in the optimal strategy for G; Alice performs the same measurement strategy as for G; on inputs y, y, Bob applies the first measurement Q^y and obtains outcome b, then applies the measurement $P^{y'}$ on his resulting state and gets outcome b'. Bob outputs (b, b'). Let E^{xa} be the probability that Alice and Bob win G_{coup} using this strategy for a fixed x, a. Notice that $\omega^*(G_{coup}) \geq \mathbb{E}_{xa}[E^{xa}]$ since the value $\mathbb{E}_{xa}[E^{xa}]$ is achievable. We have

$$\begin{aligned} E^{xa} &= \frac{1}{n(n-1)} \sum_{y, y' \neq y} \sum_{\substack{b : V(ab|xy)=1 \\ b' : V(ab'|xy')=1}} tr(Q_{b'}^{y'} Q_b^y \sigma^{xa} Q_b^y Q_{b'}^{y'}) \\ &\geq Pos(\frac{1}{64S}(V^{xa} - \frac{1}{n})^3) \qquad \text{from Theorem 1} \end{aligned}$$

where $Pos(x) := \max(x, 0)$ is the positive part of x. By taking the expectation on each side, we obtain

$$\begin{aligned} \omega^*(G_{coup}) = \mathbb{E}_{xa}[E^{xa}] &\geq \mathbb{E}_{xa}[Pos(\frac{1}{64S}(V^{xa} - \frac{1}{n})^3)] \geq Pos(\frac{1}{64S}(\omega^*(G) - \frac{1}{n})^3) \\ &\geq \frac{1}{64S}(\omega^*(G) - \frac{1}{n})^3 \end{aligned}$$

where we used the convexity of the function $x \mapsto Pos(x^3)$.

3.3 Retrieving the Value of Certain Entangled Games

We now use the technique developed above in order to obtain upper bounds on games based on the $\mathbb{F}_{\mathsf{Q}}$ variant of $CHSH$.

$\mathbf{CHSH}^{\mathbf{Q}}(\mathbf{P})$ — We consider the nonlocal game called $CHSH^Q(P)$ with $P \leq Q$. Here, Alice and Bob receive inputs x and y, where x is a uniformly random element in $\mathbb{F}_Q$ and y is an element of $\mathbb{F}_Q$ taken uniformly at random from $\{0, \ldots, P-1\}$. They output values $a, b \in \mathbb{F}_{\mathsf{Q}}$ and win if $a + b = x * y$, where the addition and multiplication are with respect to $\mathbb{F}_{\mathsf{Q}}$. Notice that $CHSH^Q(P)$ is a projective game on the uniform distribution.

Let's analyze $CHSH^Q(P)_{coup}$. Fix an input/output pair (x, a) and a pair (y, y') of inputs for Bob with $y \neq y'$. Let b, b' Bob's output. If Alice and Bob win the game then we have $a + b = x * y$ and $a + b' = x * y'$ which implies that $(b - b') * (y - y')^{-1} = x$. This means that Bob can use any strategy for $CHSH^Q(P)_{coup}$ as a strategy to guess x with the same winning probability. Because of non-signaling, this happens with probability at most $\frac{1}{Q}$. We therefore have $\omega^*(CHSH^Q(P)_{coup}) \leq \frac{1}{Q}$. Using Proposition 1 (we have $S = 1$ in this setting), we obtain $\omega^*(CHSH^Q(P)) \leq \frac{1}{P} + \frac{4}{Q^{1/3}}$.

$\mathbf{CHSH}^{\mathbf{Q}}(\mathbf{2})^{\otimes n}$ — This is the parallel repetition of $\mathbf{CHSH}^Q$ where Alice and Bob receive n uniform strings $x_1, \cdots, x_n$ and $y_1, \cdots, y_n \in \{0, 1\}$ and output strings $a_1, \cdots, a_n$ and $b_1, \cdots, b_n$, respectively. They win the $\mathbf{CHSH}^Q(2)^{\otimes n}$ game if they win all n instances of the $\mathbf{CHSH}^Q$ games, *i.e.* if $a_i + b_i = x_i * y_i$ for all $i \in \{1, \cdots, n\}$. Consider now the coupled version of this game. For any two inputs $y = y_1, \ldots, y_n, y' = y'_1, \ldots, y'_n$ given to Bob, if Alice and Bob win the game then similarly as in $\mathbf{CHSH}$, Bob can recover Alice's input bits x_i for each i where $y_i \neq y'_i$. From non signaling, this happens with probability at most $Q^{-|y-y'|_H}$, where $|y - y'|_H$ is the Hamming distance between strings y and y', counting in how many indices both strings differ. Therefore, we have $\omega^*(CHSH^Q(2)^{\otimes n}_{coup}) = \mathbb{E}_{y,y' \neq y}[Q^{-|y-y'|_H}] = \frac{1}{2^n}\left((1 + \frac{1}{Q})^n - 1\right)$. If $Q > n$, we have

$$\omega^*(CHSH^Q(2)^{\otimes n}_{coup}) \leq \frac{2n}{Q2^n} \quad \text{which gives} \quad \omega(CHSH^Q(2)^{\otimes n}) \leq \frac{1}{2^n} + 4\left(\frac{2n}{Q2^n}\right)^{1/3}.$$

In particular, if we take $Q = \frac{64 \cdot 2^{2n}}{2n\varepsilon^3}$, we obtain $\omega(CHSH^Q(2)^{\otimes n}) \leq \frac{1}{2^n}(1 + \varepsilon)$.

4 Relativistic Bit and String Commitment

In this section, we will review the relativistic $\mathbb{F}_Q$ bit commitment scheme and its natural extension to string commitment. We will show how the sum-binding property (with worst parameters) is preserved when considering string commitment or the parallel repetition of bit commitment. This is showed by Propositions 5 and 6.

4.1 Bit Commitment

Bit commitment is a cryptographic primitive between two distrustful parties Alice and Bob which consists of 2 phases: a *Commit phase* and a *Reveal phase*. Alice has a bit d at the beginning of the protocol. In the commit phase, Alice will commit to this value d by performing some communication protocol such that at end of the commit phase, Bob has no information about d (hiding property). In the second phase, the reveal phase, Alice and Bob also perform some communication which results in Alice revealing d. A desired property here is that Alice is unable to reveal a bit different from the one chosen during the commit phase (binding property).

In some sense, a bit commitment protocol simulates a digital safe. In the commit phase, Alice writes her input d on a piece of paper, puts that paper into the safe and sends the safe to Bob. If Bob doesn't hold the key of the safe then he cannot open it and therefore has no information about d. In the reveal phase, Alice would send to Bob the key to open the safe. But she cannot change the value of the bit in the safe because Bob has control of the safe. This primitive has been widely studied. However, bit commitment can only be performed with computational security in the most usual models.

We now define more formally a bit commitment scheme.

Definition 6. *A quantum commitment scheme is an interactive protocol between Alice and Bob with two phases, a Commit phase and a Reveal phase.*

- Commit phase. *Alice chooses a uniformly random input d that she wants to commit to. To do so, Alice and Bob perform a communication protocol that corresponds to this commit phase.*
- Reveal phase. *Alice interacts with Bob in order to reveal d. To do so, they perform a second communication protocol where at the end, Bob should know the value revealed by Alice. Bob, depending on this revealed value and the interaction with Alice, outputs either "Accept" or "Reject".*

A commitment scheme $\Pi = (COMM, OPEN)$ is the description of the protocol followed by the honest parties during both the commit and the open phases. All protocols that we will consider will be perfectly hiding and we will only be interested in the binding property. Therefore, we only consider the case of a cheating Alice, which will be described through her cheating strategy $Str^* = (Comm^*, Open^*)$ in both phases of the protocol. The binding property we consider is the standard sum-property, that was also used in previous work regarding relativistic bit commitment [LKB+15, FF15, CCL15].

Definition 7 (Sum-binding). *We say that a bit commitment protocol Π is* ε-sum-binding *if*

$$\forall\ \mathrm{Comm}^*, \sum_{d=0}^{1} \max_{\mathrm{Open}^*} \left(\Pr[\textit{Alice successfully reveals } d \mid (\mathrm{Comm}^*, \mathrm{Open}^*)]\right) \leq 1+\varepsilon.$$

In the case of string commitment, meaning Alice wants to commit/reveal to a string of dimension P (*i.e.* $\lceil \log(P) \rceil bits$), we can extend the sum-binding property as follows.

Definition 8 (String sum-binding). *We say that a P-string commitment protocol Π is* ε-sum-binding *if*

$$\forall\, \mathrm{Comm}^*, \sum_{d=0}^{P-1} \max_{\mathrm{Open}^*} (\Pr[\textit{Alice successfully reveals } d \,|\, (\mathrm{Comm}^*, \mathrm{Open}^*)]) \leq 1+\varepsilon.$$

The sum-binding property for bit commitment is a relatively weak one. Indeed, it is very hard to use this definition when combining it with other primitives. For example, when committing to n bits in parallel, it is not always the case that this overall commitment, seen as a 2^n-string commitment, satisfies a good string sum-binding property. On the other hand, the string sum-binding for strings seems more exploitable.

4.2 Relativistic Bit Commitment

A relativistic bit commitment scheme is a commitment scheme where we use physical property that no information carrier can travel faster than the speed of light. In order to take advantage of this principle, we split Alice (resp. Bob) into 2 agents $\mathcal{A}_1$ and $\mathcal{A}_2$ (respectively $\mathcal{B}_1$ and $\mathcal{B}_2$). For each $i \in \{1, 2\}$, $\mathcal{A}_i$ interacts only with $\mathcal{B}_i$. If we put the two pairs $(\mathcal{A}_1, \mathcal{B}_1)$ and $(\mathcal{A}_2, \mathcal{B}_2)$ far apart, and use some timing constraints, we can enforce some non-signaling type scenarios. Here, we will only use the property that the two honest Bob's know their respective location. In particular, there is no trust needed regarding the location of the cheating parties.

The security definitions for relativistic bit commitment are the ones we presented above: Definitions 7 and 8. We will now describe the $\mathbb{F}_Q$ relativistic bit commitment scheme. This scheme will consist of 4 phases, the preparation phase, the commit phase, the sustain phase and the reveal phase. The preparation phase is some preprocessing phase that can be done anytime before the protocol. The sustain phase can be seen as a part of the reveal phase, and corresponds to the time where the committed bit is safe. We assume here that the two Alices learn at the beginning of the sustain phase the bit d they should try to reveal (which doesn't necessarily correspond to the bit, if any, they committed to).

The Single-Round $\mathbb{F}_Q$ Protocol. The single-round version corresponds $\mathbf{CHSH_Q}$ to the protocol introduced by Crépeau *et al.* [CSST11] (see also [Sim07]). Both players, Alice and Bob, have agents $\mathcal{A}_1, \mathcal{A}_2$ and $\mathcal{B}_1, \mathcal{B}_2$ present at two spatial locations, 1 and 2, separated by a distance D. We consider the case where Alice makes the commitment. The protocol (followed by honest players) consists of 4 phases: preparation, commit, sustain and reveal. The sustain phase in the single-round protocol is trivial and simply consists in waiting for a time less than D/c, which is the time needed for light to travel between the two locations. The bit commitment protocol goes as follows.

1. *Preparation phase*: $\mathcal{A}_1, \mathcal{A}_2$ (resp. $\mathcal{B}_1, \mathcal{B}_2$) share a random number $a \in \mathbb{F}_Q$ (resp. $x \in \mathbb{F}_Q$).
2. *Commit phase*: $\mathcal{B}_1$ sends b to $\mathcal{A}_1$, who immediately returns $y = a + d * x$ where $d \in \{0, 1\}$ is the committed bit.
3. *Sustain phase*: $\mathcal{A}_1$ and $\mathcal{A}_2$ wait for some time $\tau < D/c$, where c is the speed of light. Crucially, for any time less than D/c, the NSS principle guarantees that $\mathcal{A}_2$ has no information about the value of b.
4. *Reveal phase*: $\mathcal{A}_2$ reveals the values of d and a to $\mathcal{B}_2$ who checks that $y = a + d * tx$.

This relativistic bit commitment protocol is known to be $O(\frac{1}{\sqrt{Q}})$-sum-binding [LKB+15]. It can be easily extended to a P-string commitment where d is an element of $\mathbb{F}_P$ instead of an element of $\{0, 1\}$. The above construction is well defined as long as $Q \geq P$ (all the operations are still the modular operations in $\mathbb{F}_Q$).

Proposition 5. *The above relativistic P-string commitment protocol is ε-sum-binding with $\varepsilon = \frac{4P}{Q^{1/3}}$.*

Proof. Consider a P-string commitment Π and a cheating strategy $Str^* = (Comm^*, Open^*)$. In this strategy, $\mathcal{A}_1$ and $\mathcal{A}_2$ share an entangled state $|\psi\rangle$. After receiving b, $\mathcal{A}_1$ performs a measurement on her part of the state to produce an output y which she sends to $\mathcal{B}_1$. For a random d that $\mathcal{A}_2$ wants to reveal, she performs a measurement on her part of the state to produce an output a. We have

$$\frac{1}{P}\sum_{d=0}^{P-1}(\Pr[\text{Alice successfully reveals } d \mid (Comm^*, Open^*)]) = \Pr[a + y = b * d].$$

One can directly use the above strategy to construct a strategy for a $\mathbf{CHSH}_{\mathbf{Q}}(P)$ game (defined in Sect. 3), with respective inputs $b \in F_Q$, $d \in F_P$ and with respective outputs y and a. We have immediately

$$\Pr[a + y = b * d] \leq \omega^*(\mathbf{CHSH}_{\mathbf{Q}}(P)) \leq \frac{1}{P} + \frac{4}{Q^{1/3}},$$

where the bound on the entangled is the one from Sect. 3. This gives us

$$\sum_{d=0}^{P-1}\max_{Open^*}(\Pr[\text{Alice successfully reveals } d \mid (Comm^*, Open^*)]) \leq 1 + \frac{4P}{Q^{1/3}}$$

which proves the desired proposition.

If we want to perform an ε-sum-binding P-string commitment protocol then we need to send $\log(Q) = \log(\frac{64P^3}{\varepsilon^3}) = 3(\log(P) + |\log(\varepsilon)|) + 8$ bits for each round of the protocol.

4.3 Parallel Repetiton of *RBC*

The problem with string commitment is that it is not possible to reveal only some bits of the string: by construction, one has to reveal the whole string. In order to circumvent this issue, we need to consider performing a bit commitment n times in parallel. This then allows one to reveal only a fraction of the bits. The scheme will still feature sum-binding property but the scaling in parameters – although still polynomial – will not be as good as for string commitment.

1. *Preparation phase*: $\mathcal{A}_1, \mathcal{A}_2$ (resp. $\mathcal{B}_1, \mathcal{B}_2$) share n random bits $a_1, \ldots, a_n \in \mathbb{F}_{\mathsf{Q}}$ (resp. $b_1, \ldots, b_n \in \mathbb{F}_{\mathsf{Q}}$).
2. *Commit phase*: $\mathcal{B}_1$ sends each b_i to $\mathcal{A}_1$, who returns for each i $y_i = a_i + d_i * b_i$ where $d_1, \ldots, d_n \in \{0,1\}$ is the sequence of committed bits.
3. *Sustain phase*: $\mathcal{A}_1$ and $\mathcal{A}_2$ wait for some time $\tau \leq D/c$.
4. *Reveal phase*: Let S be the subset of indices Alice wants to reveal. $\mathcal{A}_2$ indicates S to $\mathcal{B}_2$ and reveals the values $\{a_i\}_{i\in S}$ and $\{d_i\}_{i\in S}$ to $\mathcal{B}_2$ who checks that for each $i \in S$, the relation $y_i = a_i + d_i * b_i$ holds.

Proposition 6. *Fix a subset S of indices Alice will reveal to. Relative to S, the above protocol is ε-sum binding with $\varepsilon = 4(\frac{2|S|2^{2|S|}}{Q})^{1/3} \leq 4(\frac{2n2^{2n}}{Q})^{1/3}$.*

Proof. Fix a subset S. As before, we can use a strategy for the relativistic bit commitment to solve an instance of $\mathbf{CHSH}_{\mathbf{Q}}(2)^{\otimes|S|}$ which implies

$$\sum_{d\in\{0,1\}^{|S|}} \max_{Open^*} (\Pr[\text{Alice successfully reveals } d \mid (Comm^*, Open^*)]) \leq 2^{|S|}\omega^*(\mathbf{CHSH}_{\mathbf{Q}}(2)^{\otimes|S|}).$$

Since we know that $\omega^*(\mathbf{CHSH}_{\mathbf{Q}}(2)^{\otimes|S|}) \leq \frac{1}{2^{|S|}} + 4(\frac{2|S|}{Q2^{|S|}})^{1/3}$, we can immediately conclude that

$$\sum_{d\in\{0,1\}^{|S|}} \max_{Open^*} (\Pr[\text{Alice successfully reveals } d \mid (Comm^*, Open^*)]) \leq 2^{|S|} \leq 1 + 4(\frac{2|S|2^{2|S|}}{Q})^{1/3}.$$

If we want the above protocol to be ε-sum-binding, we need to send $n\log(Q) = O(n^2\log(n) + n|\log(\varepsilon)|)$ bits at each round.

5 Relativistic Zero-Knowledge

In this section, we present our relativistic zero-knowledge protocol for NP. Our protocol will be based on the well known protocol for the NP-complete problem Hamiltonian Cycle, which uses bit commitment.

5.1 The Zero-Knowledge Hamiltonian Cycle Protocol

Here, we present the zero-knowledge Hamiltonian cycle protocol and its adaptation to the relativistic setting. Let S_n the set of permutation on $\{1, \ldots, n\}$.

Definition 9. *A cycle of* $\{1, \ldots, n\}$ *is a set of couples*

$$\{(\Pi(1), \Pi(2)), (\Pi(2), \Pi(3)), \ldots, (\Pi(n-1), \Pi(n)), (\Pi(n), \Pi(1))\}$$

for a permutation $\Pi \in S_n$. *We denote by* Γ_n *the set of cycles of* $\{1, \ldots, n\}$. *We have* $|\Gamma_n| = (n-1)!$. *For a cycle* $\mathcal{C} = \{(u, v)\}$ *and a permutation* Π, *we also define* $\Pi(\mathcal{C}) := \{(\Pi(u), \Pi(v)\}$.

Definition 10. *A Hamiltonian cycle of a graph* $G = (V, E)$ *is a cycle* $\mathcal{C}$ *of* $\{1, \ldots, |V|\}$ *such that* $\mathcal{C} \in E$ *i.e.* $\forall (i, j) \in \mathcal{C},\ (i, j) \in E$.

Determining whether a graph G has a Hamiltonian cycle or not is an NP-complete problem. The corresponding decision problem is Hamiltonian Cycle and $G \in$ Hamiltonian Cycle means that the graph contains a Hamiltonian cycle.

5.2 The Protocol

We recall the zero-knowledge protocol for Hamiltonian Cycle first presented by Blum [Blu86].

Zero knowledge protocol for Hamiltonian Cycle

Input — The prover and the verifier are given a graph $G = (V, E)$.
Auxiliary Input — The prover knows a Hamiltonian cycle $\mathcal{C}$ of G.
Protocol —

1. The prover picks a random permutation $\Pi : V \to V$. He commits to each of bit of the adjacency matrix $M_{\Pi(G)}$ of $\Pi(G)$.
2. The verifier sends a random bit (called the challenge) $chall \in \{0, 1\}$ to the prover.
3. – If $chall = 0$, the prover decommits to all the elements of $M_{\Pi(G)}$, and reveals Π.
   – If $chall = 1$, he reveals only the bits (of value 1) of the adjacency matrix that correspond to a Hamiltonian cycle $\mathcal{C}' = \Pi(\mathcal{C})$ of $\Pi(G)$.
4. The verifier checks that these decommitments are valid and correspond, for $chall = 0$ to $M_{\Pi(G)}$ and, for $chall = 1$, to a Hamiltonian cycle.

We now present the relativistic zero-knowledge protocol, that uses the $\mathbb{F}_Q$ bit commitment.

Relativistic zero knowledge protocol for Hamiltonian Cycle

Input — The provers and the verifiers are given a graph $G = (V, E)$.
Auxiliary Input — The provers P_1 and P_2 know a Hamiltonian cycle $\mathcal{C}$ of G.
Preprocessing — P_1 and P_2 agree beforehand on a random permutation $\Pi : V \to V$ and on an $n \times n$ matrix $A \in \mathcal{M}_n^{\mathbb{F}_Q}$ where each element of A is chosen uniformly at random in $\mathbb{F}_Q$.
Protocol —

1. Commitment to each bit of $M_{\Pi(G)}$: V_1 sends a matrix $B \in \mathcal{M}_n^{\mathbb{F}_Q}$ where each element of B is chosen uniformly at random in $\mathbb{F}_Q$. P_1 outputs the matrix $Y \in \mathcal{M}_n^{\mathbb{F}_Q}$ such that $\forall i, j \in [n],\ Y_{i,j} = A_{i,j} + (B_{i,j} * (M_{\Pi(G)})_{i,j})$.
2. The verifier V_2 sends a random bit (called the challenge) $chall \in \{0, 1\}$ to the prover P_2.
3. – If $chall = 0$, P_2 decommits to all the elements of $M_{\Pi(G)}$, *i.e.* he sends all the elements of A to V_2 and reveals Π.
   – If $chall = 1$, P_2 reveals only the bits (of value 1) of the adjacency matrix that correspond to a Hamiltonian cycle $\mathcal{C}'$ of $\Pi(G)$, *i.e.* for all edges (u, v) of $\mathcal{C}'$, he sends $A_{u,v}$ as well as $\mathcal{C}'$.
4. The verifier checks that those decommitments are valid and correspond to what the provers have declared. He also checks that the timing constraint of the bit commitment is satisfied. This means that
   – if $chall = 0$, the prover's opening A must satisfy $\forall i, j \in [n],\ Y_{i,j} = A_{i,j} + (B_{i,j} * (M_{\Pi(G)})_{i,j})$.
   – if $chall = 1$, the prover's opening A must satisfy $\forall (u, v) \in \mathcal{C}',\ Y_{u,v} = A_{u,v} + B_{u,v}$.

5.3 Proof of Security

Our goal is to show that the above protocol is a relativistic zero-knowledge protocol for Hamiltonian Cycle. In order to do this, we show the following

– Completeness: If the prover and the verifier are honest then for any graph G that has a Hamiltonian cycle, the verifier accepts with certainty.
– Soundness: If we take $Q = 64n!2^{3k}$, we have that for any cheating prover, $\forall G \notin$ Hamiltonian Cycle, the verifier accepts with probability at most $\frac{1}{2} + 2^{-k}$. With this parameter Q, the amount of bits sent during the protocol is $\log(Q)$ for each committed bit and is therefore $n^2 \log(Q) = O(kn^3 \log(n))$ at each round.
– Perfect zero-knowledge: for any cheating verifier V^*, there exists a quantum poly-time simulator Σ that can reproduce the cheating verifier's view of the protocol for any input $G \in$ Hamiltonian Cycle and any auxiliary input ρ. More details about this zero-knowledge property can be found in the corresponding subsection.

Completeness. If both players are honest and G contains a Hamiltonian cycle then the protocol always succeeds. Indeed, the original protocol from Blum has perfect completeness. Moreover, the $\mathbb{F}_{\mathsf{Q}}$ bit commitment always succeeds when done honestly.

Soundness. The soundness can be reduced to the following 2-player game $G^{RZK-HAM}$.

- P_1 receives a matrix $B \in \mathcal{M}_n^{\mathbb{F}_Q}$ where each element of B is chosen uniformly at random in $\mathbb{F}_Q$. P_2 receives a random input bit *chall*.
- P_1 outputs a matrix $Y \in \mathcal{M}_n^{\mathbb{F}_Q}$. If $chall = 0$ then P_2 outputs a permutation Π and a matrix $A \in \mathcal{M}_n^{\mathbb{F}_Q}$. If $chall = 1$ then P_2 outputs a cycle $\mathcal{C}'$ and n strings $\{A'_{(u,v)}\}_{(u,v)\in\mathcal{C}'}$ in $\mathbb{F}_{\mathsf{Q}}$.
- If $chall = 0$, the two players win if $\forall i, j \in [n],\ Y_{i,j} = A_{i,j} + (B_{i,j} * (M_{\Pi(G)})_{i,j})$. If $chall = 1$, the two players win if for all edges (u, v) of $\mathcal{C}'$, $Y_{u,v} = A_{u,v} + B_{u,v}$, which corresponds to revealing 1 for each edge of the cycle $\mathcal{C}'$.

This game is $n!$-projective: once the permutation (or the cycle) is chosen, the winning output is fixed. In order to study this game, we study the game $G^{RZK-HAM}_{coup}$. We fix an input/output pair (B, Y) for P_1 and we consider winning outputs for P_2 for both inputs. For $chall = 0$, we have a permutation Π and a matrix $A \in \mathcal{M}_n^{\mathbb{F}_Q}$ which is a valid opening of $M_{\Pi(G)}$ meaning that

$$\forall (i, j),\ A_{i,j} = Y_{i,j} - B_{i,j} * (M_{\Pi(G)})_{i,j}. \tag{6}$$

For $chall = 1$, we have a cycle $\mathcal{C}'$ of $\{1, \ldots, |V|\}$ as well as openings $A'_{u,v}$ for each $(u, v) \in \mathcal{C}'$. Because it is a winning output, the openings must satisfy

$$\forall (u, v) \in \mathcal{C}',\ A'_{u,v} = Y_{u,v} - B_{u,v}. \tag{7}$$

If the graph G (hence also $\Pi(G)$) does not contain a Hamiltonian cycle then there has to be an edge (u, v) of $\mathcal{C}'$ such that $\left(M_{\Pi(G)}\right)_{u,v} = 0$. For this specific (u, v), we combine Eqs. 6 and 7 and get:

$$A_{u,v} = Y_{u,v}; \quad A'_{u,v} = Y_{u,v} - B_{u,v}.$$

This implies that $A_{u,v} - A'_{u,v} = B_{u,v}$ which happens with probability at most $\frac{1}{Q}$ from non-signaling. We therefore conclude that $\omega^*(G^{RZK-HAM}_{coup}) \leq \frac{1}{Q}$. From there, we can apply Proposition 1 and obtain

$$\omega^*(G^{RZK-HAM}) \leq \frac{1}{2} + \left(\frac{64n!}{Q}\right)^{1/3}.$$

If we take $Q = 64n!2^{3k}$ then the protocol has soundness $\frac{1}{2} + 2^{-k}$. The amount of bits sent during the protocol is $\log(Q)$ for each committed bit and is therefore $n^2 \log(Q) = O(kn^3 \log(n))$, which shows that the protocol is efficient.

5.4 Zero-Knowledge Property

In this section, we show that the above protocol is zero-knowledge. One of the main difficulties in proving zero-knowledge in the quantum setting arises when requiring the simulator to perform rewinding while preserving an auxiliary state. Here, there is no need for rewinding and the simulation can be done perfectly and quite simply. The simulator will simply simulate each round of the protocol from the first one to the last one. The reason of this simplicity is that in our bit commitment scheme, the verifier and the simulator are able, for any commitment, to reveal an arbitrary value of their choice. This is a rare feature because the prover shouldn't be able to do this to preserve the binding property. In our case, this asymmetry comes from the relativistic constraints imposed on the provers.

Zero-Knowledge in the Relativistic Setting. From the provers' point of view, each of them receives a message and replies. We assume that a cheating verifier can totally bypass the timing constraints. We therefore consider one cheating verifier that interacts with both provers. Moreover, we allow the verifier to send a query to the second prover after receiving the answer from the first prover or vice-versa. All of this is meant to have a cheating verifier as strong as possible. Proving the zero-knowledge property in this setting will therefore be stronger in this model. Also, this will show the zero-knowledge property both for relativistic zero-knowledge and for the (very related) 2-prover 1-round multi-prover interactive proof model.

A cheating verifier V^* is modeled by a polynomial-time uniform family of pairs of circuits $\{(V_1^*(n), V_2^*(n)\}$ where each $V_i^*(n)$ represents the verifier action towards prover P_i on input size n. The verifier sends a query to each prover in respective classical registers Q_1 and Q_2 and gets responses in respective classical registers R_1 and R_2. The verifier also has access to private quantum register $\mathcal{V}$, which initially contains a quantum auxiliary state ρ.

Fix a cheating verifier V^*. For any message $B \in \mathcal{M}_n^{\mathbb{F}_Q}$ sent from the verifier to P_1, the message from P_1 is a uniformly random matrix $Y = \mathcal{M}_n^{\mathbb{F}_Q}$ while the message from P_2 consists of:

- if $chall = 0$, a random permutation Π and a matrix A satisfying $Y = A + B * M_{\Pi(G)}$ where the multiplication is the entry-wise matrix multiplication.
- if $chall = 1$, a random cycle $\mathcal{C}'$ and a family of strings $\{A'_{u,v}\}_{(u,v)\in\mathcal{C}'}$ satisfying

$$\forall (u,v) \in \mathcal{C}',\ Y_{u,v} = A'_{u,v} + B_{u,v}.$$

The verifier receives as a first message a random matrix Y and as second message a random permutation (for chall = 0) or a cycle (for chall = 1) with a uniquely determined message A or A' that he can perfectly infer from the information available to him. Notice that in the soundness analysis, the prover doesn't know what message he has to send because of relativistic constraints which do not apply for the verifier (as we said, this only increases our claim on zero-knowledge).

All of the above remains true for any strategy for the cheating verifier and with any auxiliary input, and even if the verifier queries a prover depending on

the answer of the other prover. Moreover, simulating the interaction between V^* and the provers can be done step by step following V^*'s actions, without any need for rewinding. This therefore shows the perfect zero-knowledge property of our scheme. In order to illustrate this, we present below a step by step simulation of the verifier's view in a more formal way than what we did above.

Step by Step Simulation of the Verifier's View of the Protocol. For a cheating verifier V^*, we construct a quantum poly-time simulator such that on any input $G \in$ Hamiltonian Cycle and auxiliary input ρ, the simulator can recreate the verifier's view of the protocol perfectly. The simulator will use V^* as a black box and will mimic the verifier's view of the protocol after each round. When considering the interaction between the verifier and the provers, we will always distinguish 2 cases

1. The action of V_2^* depends on the interaction with P_1.
2. The action of V_1^* depends on the interaction with P_2.

Note that both of these events cannot happen simultaneously. In the analysis below, we will consider case 1 but the other one can be treated in the exact same way.

We first describe the different view for a cheating verifier V^* and then show how to perform the simulation. Let σ_i be the verifier's view at step i of the protocol.

- At the beginning of the protocol, the verifier's view consists of $\sigma_0 := \rho_{\mathcal{V}}$.
- After the verifier's first message to P_1, the verifier's view is

$$\sigma_1 := V_1^*(\rho) = \sum_{B \in \mathcal{M}_n^{\mathbb{F}Q}} p_B |B\rangle\langle B|_{Q_1} \otimes \rho(B)_{\mathcal{V}}.$$

- After the first prover's answer, the shared state between the provers and the verifier is

$$\sigma_2 := \frac{1}{n!}\frac{1}{Q^{n^2}} \sum_{\Pi \in S_n} \sum_{A \in \mathcal{M}_n^{\mathbb{F}Q}} \sum_{B \in \mathcal{M}_n^{\mathbb{F}Q}} p_B \, |Y(\Pi, A)\rangle\langle Y(\Pi, A)|_{R_1} \otimes |B\rangle\langle B|_{Q_1} \otimes \rho(B)_{\mathcal{V}}.$$

  where $Y(\Pi, A) := A + B * \Pi(G)$ with $*$ being the entry wise matrix multiplication.
- Now, the verifier sends his challenge bit, which can depend on everything that happened before. His view becomes

$$\sigma_3 := \frac{1}{n!}\frac{1}{Q^{n^2}} \sum_{\Pi \in S_n} \sum_{A \in \mathcal{M}_n^{\mathbb{F}Q}} \sum_{B \in \mathcal{M}_n^{\mathbb{F}Q}} \sum_{c \in \{0,1\}} p_{B,c} |Y(\Pi, A)\rangle\langle Y(\Pi, A)|_{R_1} \otimes |c\rangle\langle c|_{Q_2}$$
$$\otimes |B\rangle\langle B|_{Q_1} \otimes \rho(B, c, Y(\Pi, A))_{\mathcal{V}}.$$

– After the final message from the prover, the verifier's view becomes

$$\sigma_4 := \frac{1}{n!}\frac{1}{Q^{n^2}} \sum_{\Pi\in S_n} \sum_{A\in\mathcal{M}_n^{\mathbb{F}_Q}} \sum_{B\in\mathcal{M}_n^{\mathbb{F}_Q}} |Y(\Pi,A)\rangle\langle Y(\Pi,A)|_{R_1} \otimes |B\rangle\langle B|_{Q_1} \otimes \Big(p_{B,0}|0\rangle\langle 0|_{Q_2} \otimes |\Pi,A\rangle\langle\Pi,A|_{R_2} \otimes \rho(B,0,Y(\Pi,A)) + p_{B,1}|1\rangle\langle 1|_{Q_2} \otimes |\Pi(\mathcal{C}),A_{\Pi(\mathcal{C})}\rangle\langle\Pi(\mathcal{C}),A_{\Pi(\mathcal{C})}|_{R_2} \otimes \rho(B,1,Y(\Pi,A))\Big).$$

Notice that we are interested here in the verifier's view on a 'Yes' instance, meaning that on challenge $'1'$ in register Q_2, the answer $|\Pi(\mathcal{C}),A_{\Pi(\mathcal{C})}\rangle\langle\Pi(\mathcal{C}),A_{\Pi(\mathcal{C})}|$ satisfies

$$\forall (i,j)\in\Pi(\mathcal{C}),\ Y_{i,j} = A_{i,j} + B_{i,j}.$$

meaning that the prover revealed the output bit '1' for entry $\Pi(G)_{i,j}$. Notice also that for a fixed cycle $\mathcal{C}$, the mapping $\Pi \to \Pi(\mathcal{C})$ is a bijection between the set of permutation and the set of cycles.

We show now how to simulate the view of the verifier. The simulator can easily simulate σ_0 and σ_1 since he has a copy of ρ and knows V_1^*. Notice that in σ_2, the message from the prover is a uniform random matrix because of the randomness A. Therefore, we have

$$\sigma_2 = \frac{1}{Q^{n^2}} \sum_{Y\in\mathcal{M}_n^{\mathbb{F}_Q}} \sum_{B\in\mathcal{M}_n^{\mathbb{F}_Q}} p_B\ |Y\rangle\langle Y|_{R_1} \otimes |B\rangle\langle B|_{Q_1} \otimes \rho(B)_{\mathcal{V}}.$$

This can be easily created by the simulator by just tensoring the totally mixed state in register R_1 to σ_1. In order to construct σ_3, the simulator just applies V_2^* to transform σ_2 into σ_3 as the cheating verifier would and gets exactly

$$\sigma_3 = \frac{1}{Q^{n^2}} \sum_{Y\in\mathcal{M}_n^{\mathbb{F}_Q}} \sum_{B\in\mathcal{M}_n^{\mathbb{F}_Q}} \sum_{c\in\{0,1\}} p_{B,c}\ |Y\rangle\langle Y|_{R_1} \otimes |c\rangle\langle c|_{Q_2} \otimes |B\rangle\langle B|_{Q_1} \otimes \rho(B,c,Y)_{\mathcal{V}}.$$

Finally, in order to construct σ_4, the simulator does the following

– conditioned on $c = 0$ in register Q_2, the simulator picks a random permutation Π and puts $|\Pi, A(\Pi,B,Y)\rangle\langle\Pi, A(\Pi,B,Y)|$ in register R_2 where $A(\Pi,B,Y) := Y - B * \Pi(G)$, with $*$ being the entry wise matrix multiplication.
– conditioned on $c = 1$ in register Q_2, the simulator picks a random cycle $\mathcal{C}'$ and outputs $|\mathcal{C}', A'(\mathcal{C}',B,Y)\rangle\langle\mathcal{C}', A'(\mathcal{C}',B,Y)|$ such that for all $(i,j)\in\mathcal{C}'$, it holds that $A'(\mathcal{C}',B,Y)_{i,j} := Y_{i,j} - B_{i,j}$.

The state constructed by the simulator is therefore

$$\frac{1}{Q^{n^2}} \sum_{A\in\mathcal{M}_n^{\mathbb{F}_Q}} \sum_{B\in\mathcal{M}_n^{\mathbb{F}_Q}} |Y\rangle\langle Y|_{R_1} \otimes |B\rangle\langle B|_{Q_1} \otimes \Big(p_{B,0}|0\rangle\langle 0|_{Q_2} \otimes \frac{1}{n!} \sum_{\Pi\in S_n} |\Pi, A(\Pi,B,Y)\rangle\langle\Pi, A(\Pi,B,Y)|_{R_2} \otimes \rho_{B,0,Y} + p_{b,1}|1\rangle\langle 1|_{Q_2} \otimes \frac{1}{(n-1)!} \sum_{\mathcal{C}'\in\Gamma_n} |\mathcal{C}', A'(\mathcal{C}',B,Y)\rangle\langle\mathcal{C}', A'(\mathcal{C}',B,Y)|_{R_2} \otimes \rho_{B,1,Y}\Big).$$

By simple changes of variables, we can see that the above state is actually exactly equal to σ_4. Therefore, we succeeded in the simulation and we can conclude that our protocol is perfectly zero-knowledge against quantum adversaries.

Acknowledgements. The authors were partially supported by ANR DEREC <ANR-16-CE39-0001-01>.

References

[BCF+14] Buhrman, H., Chandran, N., Fehr, S., Gelles, R., Goyal, V., Ostrovsky, R., Schaffner, C.: Position-based quantum cryptography: impossibility and constructions. SIAM J. Comput. **43**(1), 150–178 (2014)

[Blu86] Blum, M.: How to prove a theorem so no one else can claim it. In: Proceedings of the International Congress of Mathematicians, vol. 1, p. 2. Citeseer (1986)

[BOGKW88] Ben-Or, M., Goldwasser, S., Kilian, J., Wigderson, A.: Multi-prover interactive proofs: how to remove intractability assumptions. In: Proceedings of the twentieth annual ACM symposium on Theory of computing, pp. 113–131. ACM (1988)

[CCL15] Chakraborty, K., Chailloux, A., Leverrier, A.: Arbitrarily long relativistic bit commitment. arXiv preprint arXiv:1507.00239 (2015)

[CGMO09] Chandran, N., Goyal, V., Moriarty, R., Ostrovsky, R.: Position based cryptography. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 391–407. Springer, Heidelberg (2009). doi:10.1007/978-3-642-03356-8_23

[CSST11] Crépeau, C., Salvail, L., Simard, J.-R., Tapp, A.: Two provers in isolation. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 407–430. Springer, Heidelberg (2011). doi:10.1007/978-3-642-25385-0_22

[DS14] Dinur, I., Steurer, D.: Analytical approach to parallel repetition. In: Proceedings of the 46th Annual ACM Symposium on Theory of Computing, STOC 2014, New York, NY, USA, pp. 624–633. ACM (2014)

[DSV15] Dinur, I., Steurer, D., Vidick, T.: A parallel repetition theorem for entangled projection games. Comput. Complex. **24**(2), 201–254 (2015)

[FF15] Fehr, S., Fillinger, M. On the composition of two-prover commitments, applications to multi-round relativistic commitments. arXiv preprint arXiv:1507.00240v1 (2015)

[GMR89] Goldwasser, S., Micali, S., Rackoff, C.: The knowledge complexity of interactive proof systems. SIAM J. Comput. **18**, 186–208 (1989)

[Hay02] Hayashi, M.: Optimal sequence of quantum measurements in the sense of Stein's lemma in quantum hypothesis testing. J. Phys. A: Math. Gen. **35**(50), 10759 (2002)

[Ken99] Kent, A.: Unconditionally secure bit commitment. Phys. Rev. Lett. **83**, 1447–1450 (1999)

[Ken11] Kent, A.: Unconditionally secure bit commitment with flying qudits. New J. Phys. **13**(11), 113015 (2011)

[Ken12] Kent, A.: Unconditionally secure bit commitment by transmitting measurement outcomes. Phys. Rev. Lett. **109**, 130501 (2012)

[KMS11] Kent, A., Munro, W.J., Spiller, T.P.: Quantum tagging: authenticating location via quantum information and relativistic signaling constraints. Phys. Rev. A **84**, 012326 (2011)

[KTHW13] Kaniewski, J., Tomamichel, M., Hanggi, E., Wehner, S.: Secure bit commitment from relativistic constraints. IEEE Trans. Inf. Theory **59**(7), 4687–4699 (2013)

[LC97] Lo, H.-K., Chau, H.F.: Is quantum bit commitment really possible? Phys. Rev. Lett. **78**(17), 3410–3413 (1997)

[LKB+13] Lunghi, T., Kaniewski, J., Bussières, F., Houlmann, R., Tomamichel, M., Kent, A., Gisin, N., Wehner, S., Zbinden, H.: Experimental bit commitment based on quantum communication and special relativity. Phys. Rev. Lett. **111**, 180504 (2013)

[LKB+15] Lunghi, T., Kaniewski, J., Bussières, F., Houlmann, R., Tomamichel, M., Wehner, S., Zbinden, H.: Practical relativistic bit commitment. Phys. Rev. Lett. **115**, 030502 (2015)

[LL11] Lau, H.-K., Lo, H.-K.: Insecurity of position-based quantum-cryptography protocols against entanglement attacks. Phys. Rev. A **83**(1), 012322 (2011)

[May97] Mayers, D.: Unconditionally secure quantum bit commitment is impossible. Phys. Rev. Lett. **78**(17), 3414–3417 (1997)

[SBT16] Sutter, D., Berta, M., Tomamichel, M.: Multivariate trace inequalities. arXiv preprint arXiv:1604.03023 (2016)

[Sim07] Simard, J.R.: Classical and quantum strategies for bit commitment schemes in the two-prover model. Master's thesis, McGill University (2007)

[Unr12] Unruh, D.: Quantum proofs of knowledge. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 135–152. Springer, Heidelberg (2012). doi:10.1007/978-3-642-29011-4_10

[Unr14] Unruh, D.: Quantum position verification in the random oracle model. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014. LNCS, vol. 8617, pp. 1–18. Springer, Heidelberg (2014). doi:10.1007/978-3-662-44381-1_1

[VMH+16] Verbanis, E., Martin, A., Houlmann, R., Boso, G., Bussières, F., Zbinden, H.: 24-hour relativistic bit commitment. Phys. Rev. Lett. arXiv:1605.07442 (2016, to appear)

[Win99] Winter, A.: Coding theorem and strong converse for quantum channels. IEEE Trans. Inf. Theory **45**(7), 2481–2485 (1999)