On No-signaling secure bit commitment

M2 Intership, supervised by Alex Bredariol Grilo

Jérôme Guyot*

* ENS Paris-Saclay, Université Paris-Saclay, France

Introduction

General context

Bit commitment is a fundamental primitive introduced by [2] and used to create many more complex cryptographic primitives. In particular, bit commitment is ubiquitous in multiparty computation. Informally it is a two phase process between two parties, where one places a secret inside a locked box and gives it to the other party. The receiver cannot open the box and learn the secret, it is said to be hiding. In a later stage, the first party sends the key of the lock to the receiver who can now open the box and learn the secret. Furthermore, while giving the key, the sender cannot use this opportunity to somehow change the secret, that is the binding property.

Bit commitment is also primordial in zero-knowledge proofs, for example [1] uses a special kind of bit commitment to build an oblivious transfer protocol, which applied to the result of [8] generates an oblivious circuit evaluation. Finally, using bit commitment, [1] shows that any multi-prover interactive proof can be made zero-knowledge, thus showing the potential of bit commitment.

However, one cannot hope for unconditional hiding and unconditional binding in a bit commitment, this can be proven easily in the classical setting and has been proven in the quantum setting independently by [9,10]. It thus brings the question of under which assumption can there be bit commitment. One way to escape the impossibility result is to reduce the power of the parties, either the committer or the receiver. In this work, and similarly to [1,5] we consider systems where the committer is split into two sub-parties that cannot communicate. This makes it fall into the world of multiparty interactive systems, and used in [1] to achieve zero-knowledge for multi-prover interactive proofs.

Now let us focus on the setting where the committer is actually composed of two provers, one might wonder what is the minimal assumption such that bit commitment exists. By this we mean, what amount of correlation is allowed between the two provers ? In [1] the commitment scheme is classical and is binding against classical adversaries. Furthermore, [4] proves that a variation of this commitment scheme is not binding against quantum adversaries, while this exact bit commitment is binding against quantum adversaries but not against no-signaling adversaries.

The notion of no-signaling appeared in the context of quantum mechanics [12,7] and more precisely Bell inequalities. Intuitively adversaries are no-signaling if they do not communicate with each other. In this sense, since we restricted to schemes where the committer is made of two sub-parties, showing security against no-signaling adversaries would result in the maximal level of security.

While this would not be unconditionally secure, assuming that nothing can signal faster than light, one could put the two sub-parties of the committer sufficiently far to ensure they cannot signal during the execution of the protocol. Under such no-signaling security, this practical implementation of bit commitment would be secure, under the standard assumption that nothing can travel faster than light.

Research problem

The research for no-signaling secure bit commitment also has many more applications. It is mainly linked with the work of [6] which creates a bridge between delegation schemes and multi-prover interactive proof

* Email : jerome.guyot@ens-paris-saclay.fr

that are no-signaling secure. In their work, they show that the security of their delegation scheme, can be reduced to the no-signaling security of some multi-prover interactive proof system. Thus, the existence of a no-signaling secure bit commitment would allow the creation of more complex no-signaling secure cryptographic primitives, which could lead to a zero-knowledge version of their delegation scheme.

The work of [5] presents the first bit commitment which is binding against no-signaling adversaries. However this protocol does not offer selective opening. More precisely, if one commits more than one bit, using their protocol it is impossible to guarantee that a malicious receiver opens only one bit. Selective opening is a crucial property when using bit commitment to construct other schemes, which makes it impossible to use their bit commitment in this case. Thus, in this work, we aim at creating a bit commitment protocol which would be selective opening, with the guarantee that the receiver can open only one commit of its choosing, hiding and binding against no-signaling adversaries.

Contribution

In this work, we introduced a new object called interpretation games, which appears naturally when considering variants of the protocol from [5]. We explained how one could build a bit commitment protocol whose binding relies on the no-signaling value of the underlying interpretation game. Finally, we linked the desired properties of the commitment with properties on the interpretation and study to what extent such an object existed. Unfortunately, we proved that one cannot hope for an interpretation which would provide a bit commitment with perfect hiding and statistical binding against no-signaling adversaries. More generally, we prove that there is no bit commitment with these properties when restricting to 3 provers, thus generalizing the impossibility result of [5].

We want to highlight that while interpretation games are not useful for this type of bit commitment protocol, interpretation game may be of use in other context, and thus are interesting on their own.

We also explore alternative protocols for a bit commitment protocol, and using linear programming we test those ideas experimentally and observe that none of them are binding. This, combined with the new impossibility result (Theorem 2), raise the question of the existence of selective opening bit commitment which are perfectly hiding and statistically binding against no-signaling adversaries.

Arguments supporting its validity

As explained, the first approach, using interpretation games, was not successful. However, the idea introduced : the interpretation game is interesting on its own. While we cannot provide any concrete argument for the existence or the impossibility of such a bit commitment, we provide an extensive study in the case of interpretation games which gives some intuition about why having both hiding and binding is difficult. We also experimentally test other implementations using linear programming and could not obtain both hiding and binding simultaneously. Finally, the impossibility result of such a bit commitment with 3 provers generalizes previous impossibility results and raises the question of the existence of such bit commitments.

Summary and future work

In future work, one might want to study the existence of such a bit commitment and try to prove its impossibility. It would be very interesting if such a bit commitment exists, as it would open the way for an interesting development which would be to work on a no-signaling version of [1]. On the other hand, if it is indeed impossible, it would be very interesting to understand the exact threshold of correlation after which bit commitment with selective opening is impossible.

1 Preliminaries

1.1 Probability distributions

Definition 1. *Let $\mathcal{X}$ be a finite non-empty set, a function $p : \mathcal{X} \mapsto \mathbb{R}$ is a probability distribution if $\sum_{x\in\mathcal{X}} p(x) = 1$ and for all $x \in \mathcal{X}, p(x) \geq 0$.*

In this work we will only consider discrete probability distributions. Furthermore, for any subset $E \subseteq \mathcal{X}, p(E) = \sum_{x \in E} p(x)$. A probability distribution p is said to be bipartite if it is of the form $\mathcal{X} \times \mathcal{Y} \mapsto \mathbb{R}$. In this case, we write $p((x,y))$ as $p(x,y)$ and as usually, we write $p(x=y)$ instead of $p(\{(x,y) \in \mathcal{X} \times \mathcal{Y} | x = y\})$. In the case of bipartite distributions, taking w to be an element of $\mathcal{X}$ (and not a random variable), the marginals are given by $p(x=w) = \sum_{y \in \mathcal{Y}} p(w,y)$ and $p(y=w) = \sum_{x \in \mathcal{X}} p(x,w)$. Furthermore, this naturally extends to multipartite distributions. A conditional probability distribution is a function $p : \mathcal{X} \times \mathcal{A} \mapsto \mathbb{R}$ such that for any $a_0 \in \mathcal{A}$ the function $p(x|a=a_0)$ is a probability distribution. This also extends to multipartite distributions : from $p(x,y|a,b)$ we can naturally define $p(x|a,b)$. However $p(x|a)$ is not well defined unless $p(x|a,b)$ is independent of b or $p(b|a)$ is defined. In this sense, we will often write $p(x|a) = p(x|a,b)$ to express that $p(x|a,b)$ is independent of b.

1.2 Bit commitment

The idea behind the bit commitment protocol is that some party A commits to a value, one can see this as "putting a secret in a box" such that another party B cannot guess the value : "cannot open/see through the box", and A cannot modify it anymore. Once it is time to open, A sends a key to B, who opens the box, and learns the secret. This is in particular very useful in multiparty computation or to make protocol zero-knowledge.

Definition 2. *(Bit commitment)*
A bit commitment scheme is defined by three algorithms :

- *Setup*(1^λ) *which given the security parameter* λ *returns the parameter of the scheme.*
- *Commit*(b,r) *which given a bit* b *and a randomness* r *outputs a commit* c *of* b *and an opening value* t*.*
- *Verify*(c,t,b) *open the commit using* t *and checks that it is consistent with* b*.*

It is required to satisfy two properties :

Hiding *: Calling* $D_b(c)$ *the distribution of* c*, the scheme is perfectly (resp statistically) hiding if* $D_0(c) = D_1(c)$ *(resp* $|D_0(c) = D_1(c)|$ *is negligible).*

Binding *: Calling* $\text{Prob}(Cheat)$ *the probability that the verifier accepts when* c,t *open to both* b *and* $1-b$*. We say that the scheme is perfectly (resp statistically) binding if* $\text{Prob}(Cheat) = 0$ *(resp* $\text{Prob}(Cheat)$ *is negligible).*

Remark 1. There is also a notion of soundness to a commitment scheme [5]. A commitment scheme is said to be α-sound if the honest opening of a committed value succeeds with probability at least α[1]. A perfectly sound scheme would thus have $\alpha = 1$.

Alternatively, one could represent a one round bit commitment as a two rounds interactive system Fig. 1. As such, a commitment scheme can be represented using the different probability distributions involved in the interactive system[5].

Definition 3. *(Bit commitment as a bipartite protocol)*
A one round commitment scheme consists of a probability distribution $p(s)$*, two conditional distributions* $p_0(c,t|s)$ *and* $p_1(c,t|s)$ *and an acceptation predicate* $\mathsf{Acc}(c,t|s,b)$*.*

In this framework, $p(s)$ represents the question of A which allows to commit on b, this commitment is represented by c and t is the opening. Here $p_0(c,t|s)$ and $p_1(c,t|s)$ represent the behavior of the honest committer. The probability that honest committer opens to b when committed on b is given by

$$\text{Prob}(\mathsf{Acc}|b) = \sum_s \sum_c \sum_t p_b(c,t|s)\mathsf{Acc}(c,t|s,b) \quad .$$

[1] In a way, the "soundness" of a commitment scheme is very similar to the completeness of an interactive proof. While the binding would be closer to the soundness of the interactive proof.

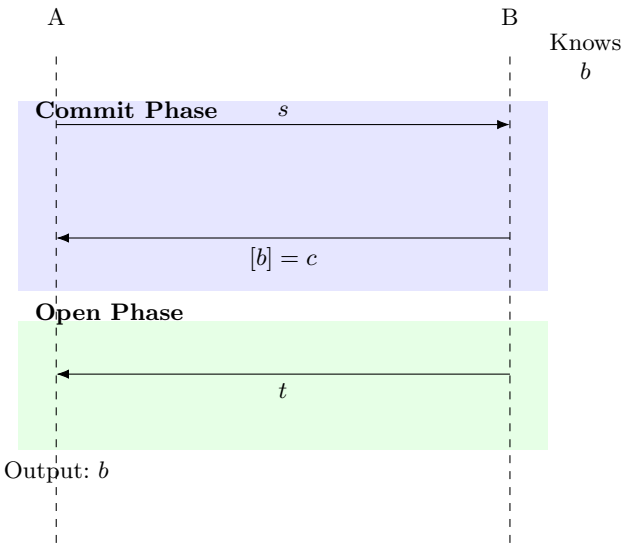

Fig. 1: Diagram of bit commitment

Remark 2. In this work, the committer (B) will be composed of 2 or more sub-parties that cannot signal to each other during the protocol. In this setting, the commitment scheme will be said to be classical/quantum/no-signaling if the honest committer behavior is classical/quantum/no-signaling.

From now on, we will only consider one round commitment scheme as bipartite systems and use this probability distributions framework. We note that here we see s, c, t as strings but if each party is made of different sub-parties, then those would be tuples. In particular, in [5] B was composed of 2 or 3 provers. Later in this work, we will consider B to be composed of 3 and 4 non-communicating provers.

Using this framework we can define the notion of soundness, hiding and binding in a more precise way.

Definition 4. *A commitment scheme is said to be α-sound if* $\text{Prob}_b(\mathsf{Acc}|b) \geq \alpha$, *and perfectly sound if* $\alpha = 1$.

Definition 5. *A commitment scheme is said to be ϵ-hiding if for all s we have* $\frac{1}{2}\sum_{c,t} |p_0(c|s) - p_1(c|s)| \leq \epsilon$. *It is perfectly hiding if* $\epsilon = 0$.

Definition 6. *A commitment scheme is ϵ-binding if for any strategy, the value on the following binding game is less than* $\frac{1+\epsilon}{2}$ *:*

1. *A sends s*
2. *B commits by sending c*
3. *A sends a bit b*
4. *B sends opening t*
5. *V accepts if t opens c to b*

Example 1. Consider the following two provers commitment scheme were $P1, P2$ cannot communicate :

1. On security parameter λ, Setup returns $n = \lambda$.
2. V chose uniformly at random $s \in \{0,1\}^n$, and $P1, P2$ agree on some value t.
3. To commit, V sends s to $P1$, and $P1$ returns $c = t \oplus b \cdot s$.
4. To open, $P2$ sends t to V and V verifies that $c \oplus t$ is equal to 0 or s and deduce the value of b.

This is perfectly hiding as $p_0(c|s) = p_1(c|s) = Unif(\{0,1\}^n)$.

For the binding, for fixed s, c and after receiving b from the verifier $P2$ needs to open c as b. However, to open the value to b, P_2 needs to send $t \oplus b \cdot s$. Classically and quantumly, one can show that the best strategy is guessing this value. Thus, the scheme is 2^{-n} binding against classical (and quantum) adversaries.

However, this commitment scheme is not binding when we allow more powerful strategies called no-signaling, which we will now explain.

1.3 No-signaling

In the context of non-local games, two parties play together by agreeing on a strategy. In the case of two player, they receive respectively inputs x, y and need to output a, b satisfying some acceptation condition $\mathsf{Acc}(a, b|x, y)$.

For a given game, one can classify the different strategies using the type of correlation between the answers of all parties. For example, in a two player game, if both parties are restricted to be classical and deterministic, then the set of possible strategies is of the form $\{p(a, b|x, y) = \delta_{a'}(a) \cdot \delta_{b'}(b)|a' \in \mathcal{A}, b \in \mathcal{B}\}$ where δ_a is the probability distribution where $\delta_a(a) = 1$ and $\delta_a(a') = 0$ if $a' \neq a$. If however we allow the players not to be deterministic then we have access to all strategies of the form $\{p(a, b|x, y) = \sum_r p(r)\delta_{a'}(x|a, r)\cdot\delta_{b'}(y|b, r)|a' \in \mathcal{A}, b' \in \mathcal{B}\}$. Similarly we can define other class of strategies, their mutual inclusions are represented in Fig. 2. In this work we are interested in strategies which are no-signaling. A strategy is said to be no-signaling if it can be implemented using players which do not communicate during the game.

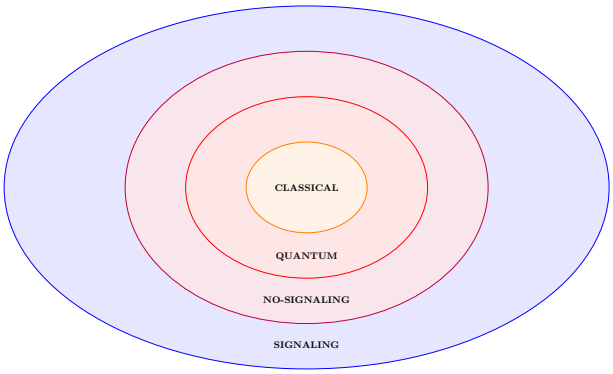

Fig. 2: Hierarchy of correlations

The differences between theses classes of strategy is highlighted by the CHSH game. In this game, two player receive two bits x, y and they need to output a, b such that $a \oplus b = x \cdot y$. One can show that classically, the best strategy gives a winning probability of $\frac{3}{4}$. When allowed to share an entangled quantum state, the provers can use more powerful strategies and can win with probability $\cos^2(\frac{\pi}{8}) \simeq 0.85$. Finally, when we consider no-signaling strategies one can win with probability 1.

In order to explain how such a strategy can exist, we will explain the formal way to define no-signaling.

Definition 7. *(No-signaling strategy)*
A strategy θ in a one-round non-local game is said to be no-signaling if

$$\theta(a|x, y) = \theta(a|x) \quad \text{and} \quad \theta(b|x, y) = \theta(b|y)$$

Remark 3. It is very important to note that this does not mean that the answer b cannot depend on x. It means that b can depend on x as a function but not as a random variable, ie the marginal distribution of b cannot depend on x. This can be subtle but this is what makes no-signaling strategies powerful.

Let us now explain how we can win with probability one in the CHSH game. Consider the following strategy

$$\theta(a, b|x, y) = \begin{cases} \frac{1}{2} & \text{if } a \oplus b = x \cdot y \\ 0 & \text{otherwise} \end{cases} .$$

First, let us show that this corresponds to a valid probability distribution.

$$\sum_{a,b} \theta(a, b|x, y) = \sum_{a,b=(x\cdot y)\oplus a} \theta(a, b|x, y) = \sum_a \frac{1}{2} = 1 \quad .$$

Let us now consider the value of this strategy on the CHSH game :

$$\begin{aligned} w(\theta) &= \sum_{x,y} \mathrm{Prob}(x,y) \sum_{a,b} \theta(a,b|x,y) \mathsf{Acc}(a,b|x,y) \\ &= \sum_{x,y} \frac{1}{4} \sum_{a,b=(x\cdot y)\oplus a} \theta(a,b|x,y) \\ &= \sum_{x,y} \frac{1}{4} \sum_{a} \frac{1}{2} \\ &= 1 \quad . \end{aligned}$$

We now need to show that the strategy is no-signaling.

$$\begin{aligned} \theta(a|x,y) &= \sum_{b} \theta(a,b|x,y) \\ &= \sum_{b=(x\cdot y)\oplus a} \theta(a,b|x,y) \quad \text{as for the rest the probability is 0} \\ &= \frac{1}{2} \\ &= \theta(a|x) \end{aligned}$$

and similarly for $\theta(b|x,y)$ as this is symmetric in a,b and x,y. Thus, this is indeed a valid no-signaling strategy and it has value 1.

2 The bit commitment of [5]

In [5], the authors prove that any 2 prover bit commitment which is one-round, perfectly hiding, perfectly sound cannot be binding against no-signaling adversaries. They actually show a way to break the binding with probability 1 on those commitment scheme. Furthermore, they provide a three provers commitment scheme which is perfectly hiding, perfectly sound and statistically binding against no-signaling adversaries. This scheme is basically the same as the commitment from Example 1 but with one more prover, which is asked to imitate the opener. We present their scheme in Figs. 3 and 4.

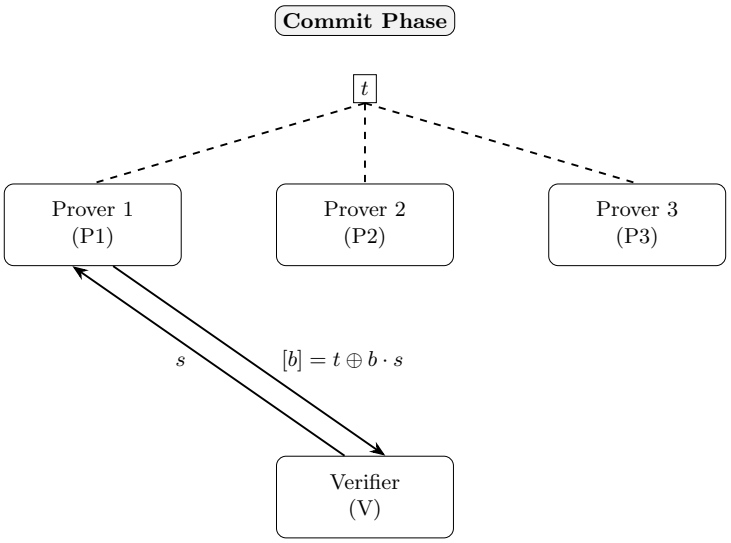

Fig. 3: Commit phase diagram

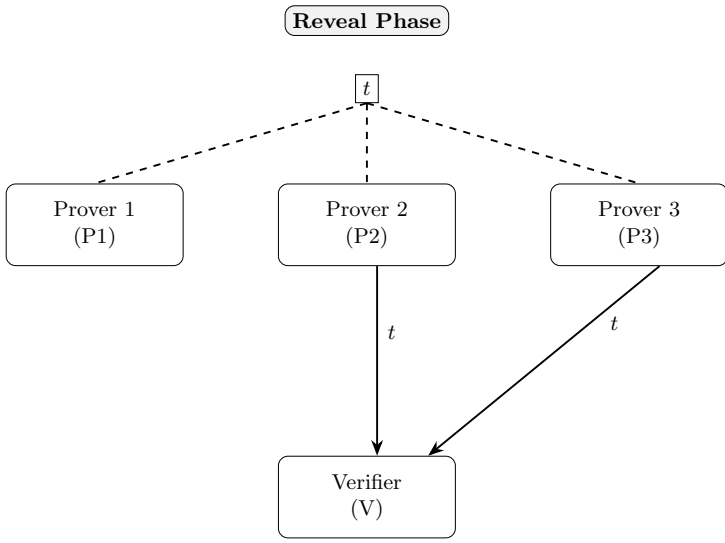

Fig. 4: Reveal phase diagram

Let us prove that this commitment is indeed perfectly hiding, perfectly sound and statistically binding to get used with the different notions.

For the hiding, to commit to 0, $P1$ sends t, thus $p_0(c|s) = Unif(\{0,1\}^n)$ as t is taken uniformly at random in $\{0,1\}^n$. To commit to 1, $P1$ sends $t \oplus b \cdot s$ meaning that $p_1(c|s) = Unif(\{0,1\}^n)$. Thus $p_0(c|s) = p_1(c|s)$ and the scheme is perfect hiding.

Now, let us show that this is perfectly sound

$$\begin{aligned}
\text{Prob}[\mathsf{Acc}|b] &= \sum_{s,c,t,t'} \text{Prob}(s) p_b(c,t,t'|s) \mathsf{Acc}(c,t,'t|s,b) \\
&= \sum_{s,c,t,t'} \text{Prob}(s) p_b(c,t,t'|s) 1[c \oplus t = b \cdot s, c \oplus t' = b \cdot s] \\
&= \sum_s \sum_t \text{Prob}(s) p_b(t \oplus b \cdot s, t, t|s) \quad \text{Since in the honest case } c = t \oplus b \cdot s \text{ and honest openers send } t \\
&= \sum_s \sum_t 2^{-2n} \\
&= 1 \quad .
\end{aligned}$$

Finally, we need to show that this scheme is binding against no-signaling adversaries. For this let us consider the binding game : the first prover commits on a value c after receiving s. The two other prover receive a bit b and need to return a_2, a_3 such that it opens c to b. Let θ a no-signaling strategy, and let us call b, d the bits received by $P2, P3$.

$$\begin{aligned}
\text{Prob}_\theta(\mathsf{Acc}|0) + \text{Prob}_\theta(\mathsf{Acc}|1) &= \theta(a_2 = c \oplus b \cdot s, a_3 = c \oplus d \cdot s | b = 0, d = 0) + \theta(a_2 = c \oplus b \cdot s, a_3 = c \oplus d \cdot s | b = 1, d = 1) \\
&\leq \theta(a_2 = c \oplus b \cdot s | b = 0, d = 0) + \theta(a_3 = c \oplus d \cdot s | b = 1, d = 1) \\
&= \theta(a_2 = c \oplus b \cdot s | b = 0, d = 1) + \theta(a_3 = c \oplus d \cdot s | b = 0, d = 1) \quad \text{Using no-signaling} \\
&\leq 1 + \theta(a_2 = c \oplus b \cdot s, a_3 = c \oplus d \cdot s | b = 0, d = 1) \\
&\leq 1 + \theta(a_2 \oplus a_3 = s | b = 0, d = 1) \\
&\leq 1 + 2^{-n} \quad \text{Using no-signaling, as } a_2, a_3 \text{ are independent of } s.
\end{aligned}$$

However, this commitment scheme has a very important flaw. Bit commitment is a very useful primitive to build zero-knowledge, but in order to do so, we often have to commit to several bits and open only few of them. In this case, we must guarantee the hiding property of the remaining ones. For example, if one wants to convince they know a coloring of a graph without revealing it, they need to commit to the whole coloring and only reveal the colors of an edge. However, using this bit commitment, one cannot obtain this selective opening. In particular, if one commits several bits using this method, $P2$,$P3$ when asked respectively i, i' will answer $t_i, t_{i'}$. But in this case, one can learn four different colors, which breaks the hiding needed for zero-knowledge.

Thus, this work aims at creating a one round bit commitment which would be perfectly hiding, perfectly sound, statistically binding against no-signaling adversaries and which would guarantee that any verifier can only learn one bit, and can chose which bit they open.

3 Interpretation Games

Definition 8. *(Interpretation)*
An interpretation I is a family of 4^n bijections of $\{0,1\}^n$. Thus we can write $I = (I_{x,b})_{x,b \in \{0,1\}^n}$.

Definition 9. *(Interpretation game)*
Let $(I_{x,b})_{x,b}$ an interpretation, consider two parties A, B such that A receives x and B receives y. To win the interpretation game, A and B must respectively answer a, b such that $I_{x,b}(a) = y$ without communicating.

Interpretation games represent a strict subset of a more general family called projection games [11]. A game is said to be a projection if for any pair of input, and any answer from player 2, then there is exactly one answer player 1 can output which end up in a win. More formally, given x, y, b the winning condition of a projection game can be written as $a = \pi_{x,y}(b)$ where $\pi_{x,y}$ is the function linking the answer of player 2 to the only good answer of player 1.

In our case, we can define π as $\pi_{x,y}(b) = I_{x,b}^{-1}(y)$. Thus, interpretation games are projection games. However, they represent a strict subset as $CHSH$ is a projection game but cannot be written as an interpretation game. More generally, given $\pi_{x,y}$ the function $J_{x,b} : y \mapsto \pi_{x,y}(b)$ might not be invertible which does not allow to write the winning condition as $I_{x,b}(a) = y$.

Projection games can be seen as a function $\Pi : (x, y) \mapsto \pi_{x,y}$ where $\pi_{x,y}$ is a function. In particular, interpretation games are the projection games where $\Pi(x, \cdot)(b) : y \mapsto \Pi(x, y)(b)$ is bijective for all $x, b \in \{0; 1\}^n$.

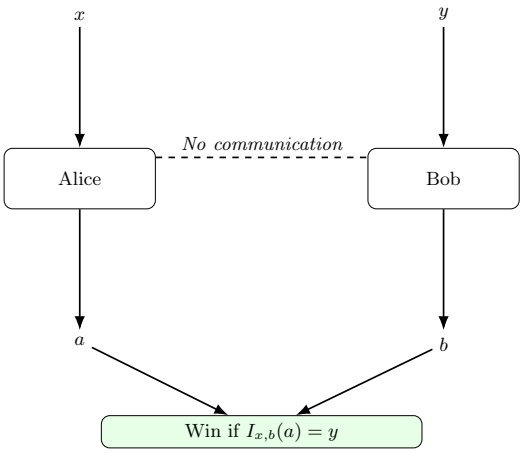

Fig. 5: Schematic of the interpretation game: A receives x, B receives y, and must output a and b such that $I_{x,b}(a) = y$.

Example 2. Take $I_{x,b}(a) = x \oplus a \oplus b$. This is a valid interpretation, and the associated interpretation game has classical value 1, using strategy $a = x, b = y$,for example.

Proposition 1. *There exists interpretation games for which the non-signaling value is strictly smaller than* 1.

Proof. Let us consider the case where $n = 2$, and take two functions Id and π where π is a permutation sending 00 to 01, 01 to 00 and acts as identity on the rest. We define $I_{x,b}$ as Id if $b = 00$ else π.

Let us consider a strategy on this interpretation game with winning probability 1.

Let us study the dependency of a on y :

$$\begin{aligned}\text{Prob}(a = 00|x, y = 00) = \text{Prob}(I_{x,b}^{-1}(00) = 00|x, y = 00) = \text{Prob}(I_{x,b} = Id) = \text{Prob}(b = 00)\\ \text{Prob}(a = 00|x, y = 01) = \text{Prob}(I_{x,b}^{-1}(01) = 00|x, y = 01) = \text{Prob}(I_{x,b} = \pi) = \text{Prob}(b \neq 00)\\ \text{Prob}(a = 00|x, y = 10) = \text{Prob}(I_{x,b}^{-1}(10) = 00|x, y = 10) = 0 \quad .\end{aligned}$$

Thus, either $\text{Prob}(a = 00|x, y = 00) \neq \text{Prob}(a = 00|x, y = 10)$ or $\text{Prob}(a = 00|x, y = 01) \neq \text{Prob}(a = 00|x, y = 10)$ since $\text{Prob}(b = 00) + \text{Prob}(b \neq 00) = 1$. Hence, it violates the non-signaling condition, and there cannot be a non-signaling strategy with winning probability 1 on this game. □

The above interpretation game explains the intuition behind the link between some imbalance in the preimages and the decrease in no-signaling value. The idea is that if there are some pairs (a, y) such that no

b can send a to y then they should not be output a otherwise they will lose. However, if we show that the probability of such a cannot be 0, since the y is uniformly random, then we can bound the winning probability.

Let us now design some harder interpretation games, which also satisfies another property: having many different bijections for a fixed x. This will be very important during the application step as we will see that few bijections leave space to a brute search attack on the hiding.

Lemma 1. *Let us assume x and y are distributed uniformly at random in $\{0,1\}^n$. There exists an efficiently computable interpretation I, such that for a given x, there are exponentially many different $I_{x,b}$ and $w_{NS}(I) \leq \frac{1}{4}$.*

Proof. Consider $\{0,1\}^n$ and partition it depending on the last two bits of the strings : $\{0,1\}^n = F_{00} \sqcup F_{01} \sqcup F_{10} \sqcup F_{11}$. We thus get a partition into 4 subsets of size 2^{n-2}. Now, let us fix some $F_{\alpha\beta}$ and see it as the space of integers from 0 to $2^{n-2}-1$. Consider the cyclic shifts on this group : $(x \mapsto x+k \mod 2^{n-2})_{0\leq k\leq 2^{n-2}-1}$. Those are efficiently computable permutations and there are 2^{n-2} different ones. We can do this for all the subsets $F_{\alpha\beta}$. Finally, we consider the sets of permutations on $\{0,1\}^n$ of the form $p = p_{00} \circ p_{01} \circ p_{10} \circ p_{11}$ where $p_{\alpha\beta}$ is a permutation on $F_{\alpha\beta}$ extended to $\{0,1\}^n$ by acting as identity on the rest of the space. Since we have 2^{n-2} permutation of $F_{\alpha\beta}$ for all α, β then we get a set of $2^{4(n-2)}$ different permutations of $\{0,1\}^n$ that are efficiently computable. We can thus index all those permutations using strings of size $4n-8$. Finally, we define the interpretation I to be the one such that $I_{x,b}$ is the permutation indexed by $x|b|0^{2n-8}$ where $s|s'$ represents the concatenation of strings s, s'. This gives us an interpretation I which contains 4^n different permutations and which is efficiently computable.

Now, let us call I some fixed interpretation constructed as presented above, and θ some strategy on the interpretation game.

$$
\begin{aligned}
w(\theta, I) &= \sum_a \text{Prob}(win|a)\theta(a) \\
&= \sum_a \text{Prob}(win|a) \sum_x \frac{1}{2^n}\theta(a|x) \\
&= \sum_a \sum_{x,y} \frac{1}{4^n}\theta(a, S_{x,y,a}|x, y) \quad \text{, where } S_{x,y,a} \text{ denotes the set } \{y : I_{x,b}(a) = y\} \\
&= \sum_a \sum_{x,y\in F(a)} \frac{1}{4^n}\theta(a, S_{x,y,a}|x, y) \quad \text{, where } F(a) \text{ denotes the coset of } \{0,1\}^n \ a \text{ belongs to} \\
&\leq \sum_a \sum_{x,y\in F(a)} \frac{1}{4^n}\theta(a|x) \quad \text{, as } \theta(a, S_{x,y,a}|x, y) \leq \theta(a|x) \\
&= \frac{2^n \cdot |F(a)|}{4^n} \quad \text{, with } |F(a)| = 2^n/4 \\
&= \frac{1}{4} \quad .
\end{aligned}
$$

Thus, as claimed $w_{NS}(I) \leq \frac{1}{4}$. □

This interpretation game is exactly what we aim to use as a basis for our cryptographic primitive. Let us now explain how we can construct a selective opening bit-commitment using interpretation games.

4 Commitment using interpretation games

Let us now use interpretation games as the underlying security for a commitment scheme. The idea is to guarantee the binding of the commitment using the no-signaling value of the interpretation game. However for this we need to explain how we can use interpretation in a commitment scheme, and we then need

to show how an attack on the commitment can be adapted into a winning strategy on the associated interpretation game. The first subsection describes the construction of the commitment scheme, while the two other subsection respectfully identify interpretations that could be useful and study the security of the scheme.

4.1 From interpretation games to bit commitment

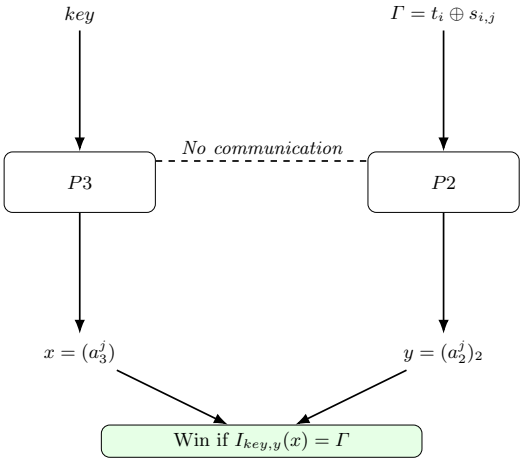

Fig. 6: Interpretation game associated to an attack on the binding.

Let us now design a bit commitment scheme based on an interpretation game. The idea is the following : the verifier sends one-time-pads $s_{i,j}$ for $1 \leq i \leq k, 1 \leq j \leq m$ to the prover $P1$. $P1$ then encodes each of its k bits in m different ways using m one-time-pads for each bit.

To open the j^{th} commitment of b_i, V can ask $P2$ for t_i by sending them i, and similarly to $P3$ by sending i and key. $P3$ then invert the bijection I_{key,k_i} and sends $I^{-1}_{key,k_i}(t_i)$ which V can then interpret by computing I_{key,k_i}. V considers an opening valid if the answer of $P2$ coincides with the interpretation of the answer of $P3$. As the notation in the commitment and in the interpretation game are different, Fig. 6 illustrates the interpretation game played with the commitment notations.

To open b_i, V will open all $[b_i]^j$ for $1 \leq j \leq m$: all the commitment of b_i. Then for each j, V deduces some value $\tilde{b}_i^j$, and do a majority vote to get its value $\tilde{b}_i$. Now, if $P2, P3$ want to break the binding and get $\tilde{b}_i \neq b_i$, they need to win at least $m/2$ instances of the underlying interpretation game.

Let us consider an attack on some $[b_i]^j$, meaning a string Γ such that $\Gamma \oplus [b_i]^j = (1 - b_i) \cdot s_{i,j}$. This gives $\Gamma = s_{i,j} \oplus t_i$. Thus, if all $s_{i,j}$ are taken independently at random, it is the same for the attacks on the $[b_i]^j$. Hence, breaking the binding of this new protocol, would imply winning in $\frac{m}{2}$ independent interpretation games, as key and Γ are independent between each game.

Let us now make the link between interpretation games and attacks on the commitment scheme more explicit. Furthermore, as the notation used in each context is not exactly the same, let us make it more understandable.

First, let us abstract the protocol : we will denote by q_1, q_2, q_3 respectively the question from the verifier to prover $P1, P2, P3$, similarly for the answers a_1, a_2, a_3. Furthermore, for a message that would have multiple parts we denote m^i as the i^{th} part of the message : $m = m^1, m^2$. We refer to Fig. 7 for the abstract representation of the protocol.

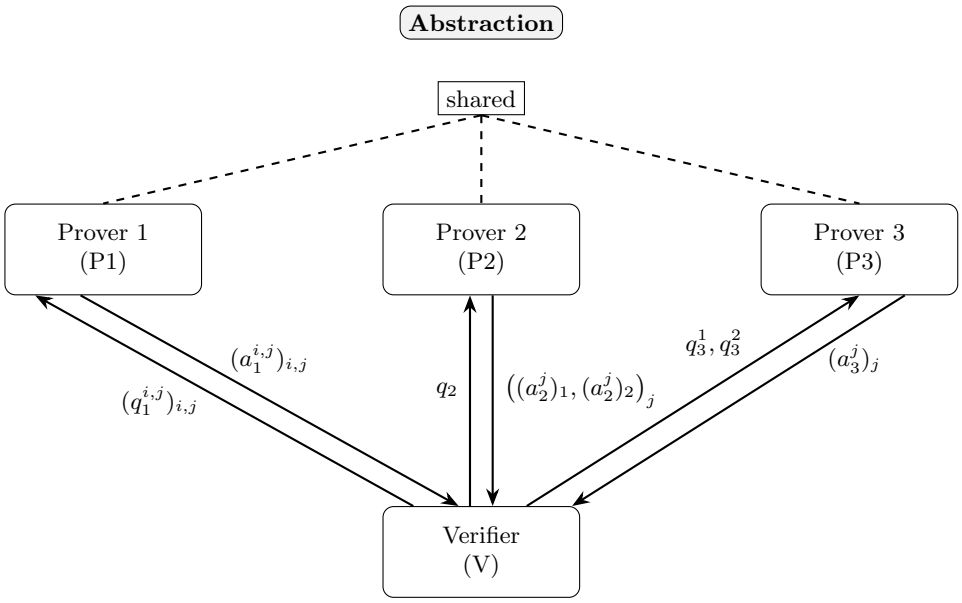

Fig. 7: Abstraction of the protocol

For example in the honest protocol we would have :

- $q_1 = (s_{i,j})_{i,j}$ and $q_1^{i,j} = s_{i,j}$
- $q_2 = i$
- $q_3 = (i', key)$ and $q_3^1 = i'$, $q_3^2 = key$
- $a_1 = ([b_i]^j)_{i,j}$ and $a_1^{i,j} = [b_i]^j$
- $a_2 = (t_i, k_i)_{1 \leq j \leq m}$ and $a_2^j = (t_i, k_i)$ and $(a_2^j)_1 = t_i$
- $a_3 = (I^{-1}_{key,k_{i'}}(t_{i'}))_{1 \leq j \leq m}$

Let us consider an attack on the binding of the commitment scheme. This means that the provers $P2, P3$ managed to respond with consistent answers that open the opposite bit as the one committed. Let us call Γ the answer that they return (after interpretation for the one of $P3$) we have that $(a_2^j)_1 = \Gamma$, and $I_{key,(a_2^j)_2}(a_3^j) = \Gamma$. Since the answers of $P2, P3$ cannot depend as random variable on Γ due to no-signaling conditions, we have that from any attack on the commitment scheme we can extract a strategy on the interpretation game whose value depend on the success probability of the attack. Since the answer of $P2$ is independent of $P3$, we can just consider the case where $P2$ is the one receiving Γ in the interpretation game and tries to make the interpretation of a_3^j equal to Γ. This is exactly the setting of interpretation games with : $\Gamma = t_i \oplus s_{i,j}, key = key, x = a_3^j$ and $y = (a_2^j)_2$. We represent this link in Fig. 6.

4.2 Finding good interpretation games

The framework of interpretation games can be directly implemented in the bit commitment protocol, as shown in the diagram of the protocol (Fig. 9) when considering $P3$ as Alice and $P2$ as Bob. The idea is that the verifier is going to interpret the answer of $P3$ according to some interpretation. To be able to use the proof of [5] we need to prove that the probability of acceptation is the same when $P2, P3$ agree on the value they want to open and when they disagree. Since the interpretation of the answer of $P3$ depends on $P2$ it is not obvious how to achieve it.

The interpretation should have for each key an exponential amount of different functions $I_{key,y}$, else the verifier could try them all. Furthermore, for a wrong function, the interpretation of the message of $P3$ will be uniformly random while for the valid one it will give either 0 or s_i when adding $[b_i]$. Since a brute search is possible, we need to ensure an exponential number of possible functions.

Furthermore, to preserve the proof, we would require an interpretation with negligible no-signaling value. As this might be hard to find, we for now focus on looking for interpretation with constant (or $1 - \frac{1}{Poly}$) no-signaling value, with exponential number of different $I_{key,y}$ for each *key*. This would be further improved with parallel repetition.

Lemma 2. *Let I be an interpretation constructed in Lemma 1, and assume key, Γ are distributed uniformly in $\{0,1\}^n$, call G the associated interpretation game. There exists $\mu > 0$ which depends on G such that for any $n \in \mathbb{N}$, $w_{NS}(G^{\frac{m}{2}/m}) < 8e^{\frac{-\mu n}{256}}$, where $G^{\frac{m}{2}/m}$ denote the $m/2$-out-of-m parallel repetition of G where one wins if they win in at least half of the instances of the game.*

Proof. Using Lemma 1 we know that $w_{NS}(G) \leq \frac{1}{4} < \frac{1}{2}$. Furthermore, any pair *key*, Γ appear with probability $\frac{1}{4^n} > 0$. Thus, we can use the ($m/2$-out-of-m) parallel repetition for complete support games of [3], their theorem 15 gives the result with $\delta = \frac{1}{4}$. □

We finally need to argue that the hypothesis made above make sense in the context of this cryptographic protocol. We can enforce the honest verifier to chose the *key* uniformly at random. However, for the Γ, we need to prove that attacks must be also uniformly randomly distributed.

Proposition 2. *Let Γ be a string such that given Γ as answer, $\tilde{b}_i^j = 1 - b_i$, then Γ is distributed uniformly at random in $\{0,1\}^n$.*

Proof. Using the verifier's program we know that

$$\begin{cases} \tilde{b}_i^j = 0 \text{ if } \Gamma \oplus [b_i]^j = 0 \\ \tilde{b}_i^j = 1 \text{ if } \Gamma \oplus [b_i]^j = s_{i,j} \end{cases}$$

Thus, if Γ induces $\tilde{b}_i^j = 1 - b_i$ we get that $\Gamma \oplus [b_i]^j = (1 - b_i)s_{i,j}$, and hence $\Gamma = t_i \oplus s_{i,j}$.
Now, as $s_{i,j}$ is distributed uniformly at random in $\{0,1\}^n$, we get that it is the same for Γ. □

4.3 Security of the bit commitment

Let us now use the abstract notation of the commitment introduced in Section 4.1.

In order for the j^{th} answer of $P2$ to be a valid opening of $[b_i]^j$ on value c we need

$$(a_2^j)_1 = a_1^{i,j} \oplus c \cdot q_1^{i,j}$$

Similarly, for the answer of $P3$ to be a valid opening of $[b_i]^j$ on value d we need

$$a_3^j = I^{-1}_{q_3^2,(a_2^j)_2}(a_1^{i,j} \oplus d \cdot q_1^{i,j})$$

Let us show that using the interpretation games framework, we can ensure that the probability that $P3$ successfully outputs an opening of b_i on value d is independent of the value c chosen by $P2$. More formally, let us prove that

$$\left|\theta\left(Maj(a_3) = I^{-1}_{q_3^2,a_2^2}(a_1^{q_2} \oplus d \cdot q_1^{q_2}) | q_1, q_2, q_3, c = 0, d\right) - \theta\left(Maj(a_3) = I^{-1}_{q_3^2,a_2^2}(a_1^{q_2} \oplus d \cdot q_1^{q_2}) | q_1, q_2, q_3, c = 1, d\right)\right| \leq \epsilon \quad (1)$$

where ϵ is negligible and $Maj(a_3)$ returns the valid answer with the most occurrences, with the definition that a_3^j is valid if the verifier can deduce a value $\tilde{b}_i^j$ from it and if its interpretation coincides with $(a_2^j)_1$. Furthermore, we add the requirement that all the openings for a given b_i must be valid for V not to abort in the protocol.

In order to prove this inequality, let us show that any strategy θ violating it would imply the existence of a winning strategy on the repeated interpretation game with probability greater than ϵ. Then using the parallel repetition theorem, we can show that the no-signaling value of the repeated interpretation game can be made smaller than ϵ, thus showing that θ cannot exist.

Lemma 3. *Let I be an interpretation as constructed in Lemma 1 and consider the bit commitment protocol as defined above. Then for any no-signaling cheating strategy θ Eq. (1) holds.*

Proof. As stated above, let us show that a violation of the inequality implies a winning strategy on a repeated interpretation game.

Assume the existence of θ such that

$$\left|\theta\left(Maj(a_3) = I^{-1}_{q_3^2,a_2^2}(a_1^{q_2} \oplus d \cdot q_1^{q_2})|q_1,q_2,q_3,c=0,d\right) - \theta\left(Maj(a_3) = I^{-1}_{q_3^2,a_2^2}(a_1^{q_2} \oplus d \cdot q_1^{q_2})|q_1,q_2,q_3,c=1,d\right)\right| > \epsilon$$

Given i,j, let us call c_j, d_j the value $P2, P3$ chose to open for the j^{th} version of the commit of b_i.

In the case where $c_j \neq d_j$, if both the answers of $P2$ and $P3$ are valid opening to their chosen values, then

$$I_{q_3^2,(a_2^j)_2}(a_3^j) \oplus (a_2^j)_1 = c_j \cdot q_1^{i,j} \oplus d_j \cdot q_1^{i,j} = q_1^{i,j}$$

However due to no-signaling condition, the answers of $P2, P3$ cannot depend on the question to $P1$ as random variables. Thus the probability happening is smaller than 2^{-n}.

Let us now consider the case where $c_j = d_j \neq b_i$: the provers are trying to break the binding property. Since $(a_2^j)_1$ and $I_{q_3^2,(a_2^j)_2}(a_3^j)$ need to coincide, we can see this as an interpretation game where $q_3^2 = key, (a_2^j)_2 = y, a_3^j = x$ and $(a_2^j)_1 = \Gamma = t_i \oplus s_{i,j}$ as they want to cheat on the opening.

More precisely, consider θ' to be the strategy on interpretation game I, where on input $t_i \oplus s_{i,j}$ and key to $P2, P3$ acts as :

$$\begin{aligned}\theta'(x,y|\Gamma,key) &= \sum_{q_2} \theta(a_2 = (I_{key_j,y_j}(x_j),y_j)_j, a_3 = (x_j)_j|q_1,q_2,q_3)\text{Prob}(q_2) \\ &= \theta(a_2 = (I_{key_j,y_j}(x_j),y_j)_j, a_3 = (x_j)_j|q_1^i,q_2 = i,q_3) \quad ,\end{aligned}$$

where we can fix $i = q_2$ as the strategy θ is symmetric on q_2 : which bit is being opened does not change anything. Let us now study the winning probability of θ' on the $m/2$ out of m parallel repetition of the interpretation game.

$$\begin{aligned}w(\theta',I) &= \sum_{\Gamma=(\Gamma_j)_j} \sum_{key=(key_j)_j} \text{Prob}(\Gamma,key) \sum_{x,y} \theta'(x,y|\Gamma,key) \mathbb{1}_{[|\{j:I_{key_j,y_j}(x_j)=\Gamma_j\}|\geq m/2]} \\ &= \sum_{\Gamma=(\Gamma_j)_j} \sum_{key=(key_j)_j} \text{Prob}(\Gamma,key) \sum_{x,y} \theta(a_2 = (I_{key_j,y_j}(x_j),y_j)_j, a_3 = x|q_1^i,q_2=i,q_3) \mathbb{1}_{[|\{j:I_{key_j,y_j}(x_j)=\Gamma_j\}|\geq m/2]} \\ &\quad \text{where } q_1^i = \Gamma_j \oplus t_i \text{ and } q_3 = i,(key_j)_j \\ &= \sum_{q_1^i=(q_1^{i,j})_j} \sum_{q_3=i,(q_3^j)_j} \text{Prob}(q_1^i,q_3) \sum_{x,y} \theta(a_2 = (I_{key_j,y_j}(x_j),y_j)_j, a_3 = x|q_1^i,q_2=i,q_3) \mathbb{1}_{[|\{j:I_{key_j,y_j}(x_j)=\Gamma_j\}|\geq m/2]} \\ &= \text{Prob}(\theta \text{ breaks binding } |q_2 = i) \\ &= \text{Prob}(\theta \text{ breaks binding })\end{aligned}$$

Thus if

$$\left|\theta\left(Maj(a_3) = I^{-1}_{q_3^2,a_2^2}(a_1^{q_2} \oplus d \cdot q_1^{q_2})|q_1,q_2,q_3,c=0,d\right) - \theta\left(Maj(a_3) = I^{-1}_{q_3^2,a_2^2}(a_1^{q_2} \oplus d \cdot q_1^{q_2})|q_1,q_2,q_3,c=1,d\right)\right| > \epsilon$$

Then it means that with probability at least $2^{-n} + \epsilon$ θ breaks the binding of the commitment scheme, which implies that θ' wins the $\frac{m}{2}$ out of m parallel repetition of the interpretation game. However, as proved in Lemma 2 the no-signaling value of this game can be made arbitrarily negligible. Thus θ cannot exist.

Hence, for any cheating no-signaling strategy θ, we have that Eq. (1) holds. □

Remark

It is important to note that breaking the binding is even stronger than winning in the interpretation game in the sense that the strategy allowed to break the binding are more restrictive than the one allowed in the interpretation game. To see this, one can realize that in the commitment, the answer of $P2$ and $P3$ cannot depend on q_1 as a random variable, and we use this to derive the binding property. However in the interpretation game, the answer of B which corresponds to $P2$ is allowed to depend on Γ which depends on q_1.

However what is important to see here is that if a strategy θ is no-signaling and breaking the binding on the commit, then in particular the associated strategy θ' on the interpretation game is no-signaling on the interpretation game and wins the $m/2$ out of m parallel repetition of this game.

Let us now prove using Lemma 3 that the bit-commitment is secure against no-signaling adversaries.

Theorem 1. *The bit commitment protocol describe above is $2^{-(n-1)}$ binding against no-signaling adversaries.*

Proof. Let θ be a no-signaling strategy on the commitment scheme described above. Let us assume that some bits have been committed, and we are now trying to open on of them : b_i. We want to show that the sum of acceptance for both openings will be smaller than $1 + 2^{-(n-1)}$, which would make the commit statistically binding. Let us write $\theta(q, a|c, d) = \text{Prob}(q)\theta(a|q, c, d)$ where $q = (q_1, q_2, q_3)$ and $a = (a_1, a_2, a_3)$, and c, d are the values $P2, P3$ want to open b_i on.

$$
\begin{aligned}
&\text{Prob}^*_\theta[\mathsf{Acc}|0] + \text{Prob}^*_\theta[\mathsf{Acc}|1] \\
&= \theta\left(Maj((a_2^j)_1) = a_1^{q_2} \oplus c \cdot q_1^{q_2}, Maj(a_3) = I^{-1}_{q_3^2,a_2^2}(a_1^{q_2} \oplus d \cdot q_1^{q_2})|c = 0, d = 0\right) \\
&\quad + \theta\left(Maj((a_2^j)_1) = a_1^{q_2} \oplus c \cdot q_1^{q_2}, Maj(a_3) = I^{-1}_{q_3^2,a_2^2}(a_1^{q_2} \oplus d \cdot q_1^{q_2})|c = 1, d = 1\right) \\
&\leq \theta\left(Maj((a_2^j)_1) = a_1^{q_2} \oplus c \cdot q_1^{q_2}|c = 0, d = 0\right) + \theta\left(Maj(a_3) = I^{-1}_{q_3^2,a_2^2}(a_1^{q_2} \oplus d \cdot q_1^{q_2})|c = 1, d = 1\right) \\
&\leq \theta\left(Maj((a_2^j)_1) = a_1^{q_2} \oplus c \cdot q_1^{q_2}|c = 0, d = 1\right) \\
&\quad + \theta\left(Maj(a_3) = I^{-1}_{q_3^2,a_2^2}(a_1^{q_2} \oplus d \cdot q_1^{q_2})|c = 0, d = 1\right) + 2^{-n} \qquad \text{Using Eq. (1) with } \epsilon = 2^{-n}, m = \mathcal{O}(n) \\
&\leq 1 + \theta\left(Maj((a_2^j)_1) = a_1^{q_2} \oplus c \cdot q_1^{q_2}, Maj(a_3) = I^{-1}_{q_3^2,a_2^2}(a_1^{q_2} \oplus d \cdot q_1^{q_2})|c = 0, d = 1\right) + 2^{-n} \\
&\leq 1 + 2^{-n} + \theta\left(Maj((a_2^j)_1) \oplus I_{q_3^2,a_2^2}(Maj(a_3)) = q_1^{q_2}|c = 0, d = 1\right) \\
&\leq 1 + 2^{-(n-1)} \qquad \text{as } a_2, a_3 \text{ are independent of } q_1 \text{ as random variables.}
\end{aligned}
$$

Thus, with $m = Poly(n)$, and I constructed as in Lemma 1, the commitment scheme designed in Section 4.1 is $2^{(n-1)}$ binding. □

Lemma 4. *The protocol of Theorem 1 is perfectly sound, but does not guarantee selective opening.*

Proof. Consider the commitment scheme designed in Section 4.1 with the interpretation of Lemma 1. We already proved the $2^{-(n-1)}$ binding against no-signaling adversaries in Theorem 1.

For the perfect soundness, in the honest case, $P2$ can output t_i when asked i, and $P3$ can output $I^{-1}_{key,k_i}(t_i)$ as it is a bijection, so $P3$ can compute the good preimage to the honest bijection. Thus, with probability 1, the provers can honestly open the commit. I can be noted that this honest strategy is classical.

The perfect hiding of the scheme comes from the perfect hiding of the scheme in [5] as the commit part of the scheme is the same (though we ask for $\mathcal{O}(n)$ versions of the commits).

However, we also need to show that introducing the interpretations does not allow V to learn more than one committed bit and this is where the problem is. As honest $P2$ returns t_i when asked i, V can learn the

value of the bit b_i. However, given $([b_{i'}]^j)_j$ and $I_{key,k_{i'}^{-1}(t_{i'})}$ the verifier can also guess the value of $b_{i'}$ with $i' \neq i$.

Recall the structure of the interpretation I. We partitioned the set $\{0,1\}^n$ in 4 subspaces and each $I_{key,y}$ preserves each subspace. Thus, given x the answer of $P3$ we know which subset $t_{i'}$ is in. We can also compute which subset $t \oplus s$ is in. And then we can compare it to the subset of $[b]$. Furthermore, for the interpretation of Lemma 1, the only case where the subsets are the same is when s finishes by 00. Thus the malicious verifier can make sure no s finishes in 00 and can always guess $b_{i'}$.

Remark

What is very important to take from this lemma is that the attack is linked to the fact that we partitioned the set of words. If there was no such partition then we would have a secure bit commitment.

Definition 10. *(Good interpretation)*
An interpretation I is said to be good if it satisfies the following properties :

- $w_{NS}(I) \leq 1 - \frac{1}{Poly}$
- *For any key,* $|\{I_{key,y}\}_y| = 2^n$
- *For all key, y* $I_{key,y}$ *is efficiently computable (in PPT)*
- *For all key, x* $T_{key,x} = \{\Gamma : \exists y, I_{key,y}(x) = \Gamma\} = \{0,1\}^n$

Remark

Asking that for any *key*, $|\{I_{key,y}\}_y| = 2^n$ is necessary to ensure that learning $I_{key,y}(t_{i'})$ does not reveal any information about $t_{i'}$, and thus get perfect hiding.

Corollary 1. *Assuming the existence of a good interpretation I, for every positive integers n, k, there exists a classical one round three provers selective opening commitment scheme that is perfectly sound, perfectly hiding and $2^{-(n-1)}$ binding against no-signaling adversaries, where with probability $1-2^{-n}$ the verifier learns the value of only one bit. The verifier communicates $k \times \mathcal{O}(n^2)$ bits to the first prover, receives $k \times \mathcal{O}(n^2)$ bits from the first prover and $\mathcal{O}(n^2)$ bits from the others, where k is the number of bits committed.*

Proof. Consider the commitment scheme designed in Section 4.1 with the good interpretation. We already proved the $2^{-(n-1)}$ binding against no-signaling adversaries in Theorem 1, and the hiding and soundness can be derived from Lemma 4.

Let us explain in more detail why in this case V cannot learn two committed bits. Since we have that for all key, x we get $T_{key,x} = \{0,1\}^n$ we get that knowing $I^{-1}_{key,k_{i'}}(t_{i'})$ does not give any information about $t_{i'}$, since V does not have any information about $k_{i'}$ and that for any fixed *key* the set $\{I_{key,y}\}_y$ has size 2^n. Thus, with probability $1 - 2^{-n}$ V learns only one bit. □

What we essentially did here is reducing the existence of a no-signaling secure, selective opening bit commitment scheme to the existence of a particular object that we call good interpretations. In Appendix B, we study interpretations and their associated games in more depth and analyze the existence of such objects. It is proven in Theorem 3 that in fact no good interpretations exists, and as such any commitment scheme designed as above, based on interpretation games, would not be no-signaling statistically binding and perfectly hiding with selective opening.

5 Taking a step back

Before trying to design a new bit commitment using another tool, let us take a step back and try to understand what went wrong with the previous design. Since we wanted that the verifier could not open more than one bit, we asked that given the commit and the answer of $P3$, V could not guess the committed bit. In a way, $P3$ was actually part of the commit and not really part of the opening. Thus, one can take a step back and wonder about the existence of a bit commitment scheme using 2 committers and one opener which would be perfectly hiding, perfectly sound and binding against no-signaling adversaries. In this case, we can

use the impossibility result of [5] for the 2 prover commitment scheme, and adapt it to 2 committers and one opener schemes.

Lemma 5. *For all $k \in \mathbb{N}$, there is no commitment scheme with k committers, 1 opener which is perfectly sound, perfectly hiding and has binding against no-signaling adversaries.*

Proof. (Informal)
First recall that on the binding game, the k first provers commit, then the verifier sends b to the opener which need to open the commit on value b. Let us call s all the messages sent to the first k provers and c their answer, and t the answer of the opener.

Let us consider the following strategy on the binding game :

$$\theta(c, t|s, b) = \text{Prob}_b(c, t|s)$$

Meaning that θ behaves as the honest provers trying to commit and then open b.

First of all, as the scheme is perfectly sound, this strategy has winning strategy 1. However we need to show that this is no-signaling.

First we have $\theta(c|s, b) = \theta(c|s, 1 - b)$ since the commitment is perfectly hiding. Now for the other condition, $\theta(t|s, b) = \sum_c \text{Prob}_b(c, t|s)$, and $\sum_c \text{Prob}_b(c, t|s)$ do not depend on s as the honest provers do not communicate and thus are no-signaling. □

Remark 4. A more formal proof can be found in Appendix C

This gives the intuition that the commitment scheme we are trying to design cannot exist when using only 3 provers. However, we need to prove this more formally. In this sense, Theorem 2 formally proves the impossibility by identifying a binding breaking no-signaling strategy for any simple one round perfectly hiding and perfectly sound commitment scheme where the verifier can open at most one bit. One can think of the commitment scheme as committing m bits, and the verifier asks indices i, j to $P2, P3$. The idea is that not learning more than one bit, means that either $commit, t_2$ or $commit, t_3$ is hiding.

Definition 11. *A one round commitment scheme is said to be simple if each prover involved in the scheme appears in either the commitment phase or in the reveal phase but not in both.*
Furthermore, a commitment is said to be fixed set hiding if there exists a set $S \neq \emptyset$ such $(c, (t_i)_{i\in S})$ is hiding.

Remark 5. In the attempt to build a commitment scheme using interpretation games, we defined a commitment which was fixed set hiding as c, t_3 was hiding, where t_3 is the answer of $P3$.

Now we need to state formally what "learning only one bit" means. When asking i to $P2$ and j to $P3$, V can only learn one bit b_i or b_j. This means that for all s, i, j at least t_2 or t_3 is hiding. Since the honest provers being no-signaling we have that $p_b(t_2|s, i, j) = p_b(t_2|i)$ and $p_b(t_3|s, i, j) = p_b(t_3|j)$. Let us denote by I (resp J) the set of indices i such that $p_0(c_i, t_2|i) \neq p_1(c_i, t_2|i)$ (resp $p_0(c_j, t_3|j) \neq p_1(c_j, t_3|j)$). Meaning that $i \in I$ if $P1, P2$ are not hiding on query i. Let us assume that both I, J are non-empty. There exists $i_0 \in I, j_0 \in J$, if $i_0 \neq j_0$ then on query i_0, j_0 V obtain information on two bits. Thus this is not perfectly hiding. Thus, either $I = J = \{i_0\}$ or $I = \emptyset$ or $J = \emptyset$. If one of the set is empty, we get that the scheme is fixed set hiding. Thus, not learning more than one bit implies either fixed set hiding or that the leakage of information is restricted to only one committed bit.

Theorem 2. *There is no simple one-round commitment scheme with 3 provers which is perfectly hiding, perfectly sound, statistically binding against no-signaling provers, where the prover can open only one bit.*

Proof. Let us consider a simple one round 3 provers commitment scheme Com which is perfectly hiding, perfectly sound, where the prover can open only one bit. As proved above, if there are two committers and one opener, the scheme is not binding. In the case of one committer and two openers, we have that the

commitment scheme is either fixed set hiding or has restricted leakage.

Let us first consider the fixed set hiding case, and suppose without loss of generality that the commit and the answer of $P2$ are perfectly hiding. Com is defined by the distributions $p(s_1), p_0(c_1,t_2,t_3|s_1,i,j), p_1(c_1,t_2,t_3|s_1,i,j)$ and the predicate $Acc(c_1,t_2,t_3|s_1,b,i)$.

Let us consider the strategy on the associated binding game defined as

$$q(c_1,t_2,t_3|s_1,b_2,i,b_3,j) = p_{b_3}(c_1,t_2,t_3|s_1,j)$$

Let us prove that this indeed breaks the binding :

$$\begin{aligned}\text{Prob}(Acc|b) &= \sum_{s_1,i}\sum_{c_1,t_2,t_3} p(s_1)q(c_1,t_2,t_3|s_1,b,b,i,i)\mathsf{Acc}(c_1,t_2,t_3|s,i)\\ &= \sum_{s_1,i}\sum_{c_1,t_2,t_3} p(s_1)p_b(c_1,t_2,t_3|s_1,i)\mathsf{Acc}(c_1,t_2,t_3|s_1,b,i)\\ &= 1 \quad \text{, as } Com \text{ is perfectly sound.}\end{aligned}$$

Let us now prove that this strategy is indeed no-signaling. For this we need to compute all the marginals for each subset of provers and show that they are independent of the queries to the other provers.

$$q(c_1|s_1,b_2,i,b_3,j) = p_{b_3}(c_1|s_1) = p_{1-b_3}(c_1|s_1) = q(c_1|s_1) \quad \text{, as } Com \text{ is perfectly hiding}$$

$$\begin{aligned}q(c_1,t_2|s_1,b_2,i,b_3,j) &= \sum_{t_3} q(c_1,t_2,t_3|s_1,b_2,i,b_3,j)\\ &= \sum_{t_3} p_{b_3}(c_1,t_2,t_3|s_1,i,j)\\ &= p_{b_3}(c_1,t_2|s_1,i) \quad \text{, as honest provers are no-signaling}\\ &= p_{1-b_3}(c_1,t_2|s_1,i) \quad \text{, as } c_1,t_2 \text{ are perfectly hiding for all } i\\ &= q(c_1,t_2|s_1,i)\end{aligned}$$

$$q(c_1,t_3|s_1,b_2,i,b_3,j) = p_{b_3}(c_1,t_3|s_1,j) = q(c_1,t_3|s_1,b_3,j)$$

$$q(t_2|s_1,b_2,i,b_3,j) = \sum_{c_1,t_3} q(c_1,t_2,t_3|s_1,b_2,i,b_3,j) = p_{b_3}(t_2|s_1,i) = p_{b_3}(t_2|i) = p_{1-b_3}(t_2|i) = q(t_2|b_2,i)$$

$$q(t_3|s_1,b_2,i,b_3,j) = \sum_{c_1,t_2} q(c_1,t_2,t_3|s_1,b_2,i,b_3,j) = p_{b_3}(t_3|j) = q(t_3|b_3,j)$$

$$\begin{aligned}q(t_2,t_3|s_1,b_2,i,b_3,j) &= \sum_{c_1} q(c_1,t_2,t_3|s_1,b_2,i,b_3,j)\\ &= \sum_{c_1} p_{b_3}(c_1,t_2,t_3|s_1,b_2,i,b_3,j)\\ &= p_{b_3}(t_2,t_3|s_1,b_2,i,b_3,j)\\ &= p_{b_3}(t_2,t_3|b_2,i,b_3,j), \text{ as honest provers are no-signaling}\\ &= q(t_2,t_3|b_2,i,b_3,j)\end{aligned}$$

Thus, this strategy is indeed no-signaling, and it has value 1.

Let us now consider the restricted leakage case. Meaning that there exists exactly one index i_0 such that $p_0(c_{i_0}, t_2|i_0) \neq p_(c_{i_0}, t_2|i_0)$. In this case, there is no probability 1 attack on the binding as the attack restricted to the case $i = j = i_0$ would be an attack on the scheme from [5]. However, consider an attack inspired by the previous case defined as

$$q(c_1, t_2, t_3|s_1, b_2, i, b_3, j) = \begin{cases} p_{b_3}(c_1, t_2, t_3|s_1, i, j) & \text{if } = i \neq i_0 \text{ and } j \neq i_0 \\ 2^{-n} p_{b_2}(c_1, t_2|s_1, i) & \text{if } i \neq i_0 \text{ and } j = i_0 \text{ where} \\ 2^{-n} p_{b_3}(c_1, t_3|s_1, j) & \text{if } i = i_0 \text{ and } j \neq i_0 \\ 4^{-n} & \text{if } i = i_0 \text{ and } j = i_0 \end{cases}$$

One can check that this strategy is indeed no-signaling and has value $1 - \frac{1}{m}$ on the binding game, where $m = Poly(n)$ is the number of committed bits. Thus, even in this case, the commitment scheme does not have statistical binding. Furthermore, parallel repetition would not work as it would create the opportunity to learn more than one bit.

Thus, any three prover commitment scheme where the verifier cannot learn more than one bit cannot be perfectly hiding, perfectly sound and statistically binding against no-signaling adversaries.

□

This theorem only captures the case where we have 3 provers. In the general case, it seems hard to define a binding breaking strategy that is no-signaling : the first intuition would be to commit honestly on the bit that has majority among the b_i, but this might induce difference of behavior between P_i is part or the majority or not, and thus some signaling.

Another important observation, is that Theorem 2 only consider the case of perfectly hiding commitment schemes. In fact, just as it is done in [5], if the scheme was ϵ-hiding, we could derive a $\alpha - \epsilon$ binding breaking strategy on the commitment from the attack of Theorem 2 where $\alpha = 1$ if the scheme is fixed set hiding and $1 - \frac{1}{m}$ in the other case. [5] also extends their results to non-simple commitment schemes which we did not do in this work, but would be an interesting follow-up.

6 On the possibility of bit commitment with 4 provers

This step back was very useful as we now know that we need at least 4 provers involved in the scheme to get the desired properties. We now want to find such commitment schemes. However, to study them, we will use another technique : linear programming.

The space of no-signaling strategies is a convex polytope, due to the linearity of the constraints it is subject to. Thus, one can use convex optimization to study the no-signaling binding property of a commitment scheme. For this we can use linear programming, with exponentially many constraints. The fact that we can study the set of no-signaling strategy using linear programming with exponentially many constraints is the reason why $\mathbf{MIP^{NS}} \subseteq \mathbf{EXP}$.

As such, we implemented the commitment schemes from [5] : the two prover scheme and the three prover alternative to check their result experimentally. Thus, for $n \leq 3$ we retrieve their result. Furthermore, the bound 2^{-n} on the binding parameter of the three prover scheme is tight. We then implemented other commitment schemes to gain intuition on their binding.

6.1 1 committer, 2 openers and an imitator

The idea behind this scheme is to keep the exact same commit as before : $[b] = t \oplus b \cdot s$. Then $P2, P3$ need to output a_2, a_3 such that $a_2 \oplus a_3 = t$. Finally, to ensure binding, the idea was to add $P4$ such that on input 2 $P4$ must output a_2 else on input 3 $P4$ outputs a_3. The intuition comes from the 3 prover commitment of [5] where $P3$ imitates $P2$. However, linear programming revealed that this scheme is not binding. We detail the algorithm used for this analysis in Algorithm 1.

6.2 Using secret sharing for bit commitment

One solution for this is to consider a scheme where there are 4 provers, $P1$ commits just as before, and $P2, P3, P4$ are doing a $2,3$ secret sharing on the $(t_i)_i$ (see Figs. 10 and 11). Meaning that $P2$ has $(t_i^2)_i$ similarly for $P3, P4$ and for any i having any pair of $t_i^j, t_i^{j'}$ with $j \neq j'$ reveals t_i. However, if one posses only on t_i^j they do not learn anything about t_i.

Using $2,3$ secret sharing we directly get that the new scheme is perfectly hiding and V can only learn one bit, it is also perfectly sound. We now need to study the binding against no-signaling adversaries. Linear programming reveals that for $n = 2$ there is a non-signaling strategy breaking the binding with probability 1. After analyzing this attack, we can then extend it to arbitrary n, and show that the bit commitment using secret sharing is not binding.

Let us denote by $\text{check}_{i,j}$ the fact that the condition $\frac{a_i - a_j}{c_i - c_j} = a_1 + b_i \cdot s$ is satisfied. To break the binding, one can consider the following strategy :

$$\theta(a_1, a_2, a_3, a_4 | s, c_2, c_3, c_4, b_2, b_3, b_4) = \begin{cases} \frac{1}{q^2} & \text{if } b_2 = b_3 = b_4 \text{ and } \text{check}_{2,3}, \text{check}_{2,4}, \text{check}_{3,4} \\ \frac{1}{q^3} & \text{if } b_2 = b_3 \neq b_4 \text{ and } \text{check}_{2,3} \\ \frac{1}{q^3} & \text{if } b_2 = b_4 \neq b_3 \text{ and } \text{check}_{2,4} \\ \frac{1}{q^3} & \text{if } b_3 = b_4 \neq b_2 \text{ and } \text{check}_{3,4} \\ 0 & \text{otherwise} \end{cases}$$

It is proved in Proposition 5 that this is indeed a no-signaling strategy with value 1 on the binding game.

7 Conclusion

In this work, we explored the design of selective opening bit commitment schemes secure against no-signaling adversaries. We introduced the interpretation game framework, analyzed its cryptographic potential, and established strong limitations, including impossibility results in certain settings and negative outcomes from linear programming experiments. These findings, together with the inherent constraints highlighted in our analysis, lead us to think that such commitment schemes might be impossible. We leave as future work to try to prove a general impossibility result.

Acknowledgments

I would like to thank Alex Bredariol Grilo for his guidance and support during those 5 months, as well as the QI team of Sorbonne Université. I am also grateful to Tom Gur, Philip Verduyn Lunel, and Claude Crépeau for the many insightful and enriching discussions we shared.

References

1. 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. p. 113–131. STOC '88, Association for Computing Machinery, New York, NY, USA (1988). https://doi.org/10.1145/62212.62223, https://doi.org/10.1145/62212.62223
2. Blum, M.: Coin flipping by telephone a protocol for solving impossible problems. SIGACT News **15**(1), 23–27 (Jan 1983). https://doi.org/10.1145/1008908.1008911, https://doi.org/10.1145/1008908.1008911
3. Buhrman, H., Fehr, S., Schaffner, C.: On the parallel repetition of multi-player games: The no-signaling case. Schloss Dagstuhl – Leibniz-Zentrum für Informatik (2014). https://doi.org/10.4230/LIPICS.TQC.2014.24, https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.TQC.2014.24
4. Crépeau, C., Salvail, L., Simard, J.R., Tapp, A.: Two provers in isolation. In: Lee, D.H., Wang, X. (eds.) Advances in Cryptology – ASIACRYPT 2011. pp. 407–430. Springer Berlin Heidelberg, Berlin, Heidelberg (2011)

5. Fehr, S., Fillinger, M.: Multi-prover commitments against non-signaling attacks. Cryptology ePrint Archive, Paper 2015/501 (2015), https://eprint.iacr.org/2015/501
6. Kalai, Y.T., Raz, R., Rothblum, R.D.: How to delegate computations: The power of no-signaling proofs. Cryptology ePrint Archive, Paper 2013/862 (2013), https://eprint.iacr.org/2013/862
7. Khalfin, L.A., Tsirelson, B.S.: Quantum/classical correspondence in the light of bell's inequalities. Foundations of Physics **22**(7), 879–948 (Jul 1992). https://doi.org/10.1007/BF01889686, https://doi.org/10.1007/BF01889686
8. Kilian, J.: Founding crytpography on oblivious transfer. In: Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing. p. 20–31. STOC '88, Association for Computing Machinery, New York, NY, USA (1988). https://doi.org/10.1145/62212.62215, https://doi.org/10.1145/62212.62215
9. Lo, H.K., Chau, H.: Why quantum bit commitment and ideal quantum coin tossing are impossible. Physica D: Nonlinear Phenomena **120**(1), 177–187 (1998). https://doi.org/https://doi.org/10.1016/S0167-2789(98)00053-0, https://www.sciencedirect.com/science/article/pii/S0167278998000530, proceedings of the Fourth Workshop on Physics and Consumption
10. Mayers, D.: Unconditionally secure quantum bit commitment is impossible. Phys. Rev. Lett. **78**, 3414–3417 (Apr 1997). https://doi.org/10.1103/PhysRevLett.78.3414, https://link.aps.org/doi/10.1103/PhysRevLett.78.3414
11. Rao, A.: Parallel repetition in projection games and a concentration bound. In: Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing. p. 1–10. STOC '08, Association for Computing Machinery, New York, NY, USA (2008). https://doi.org/10.1145/1374376.1374378, https://doi.org/10.1145/1374376.1374378
12. Rastall, P.: Locality, bell's theorem, and quantum mechanics. Foundations of Physics **15**(9), 963–972 (Sep 1985). https://doi.org/10.1007/BF00739036, https://doi.org/10.1007/BF00739036

A Commitment protocol diagrams

A.1 Commitment using interpretation games

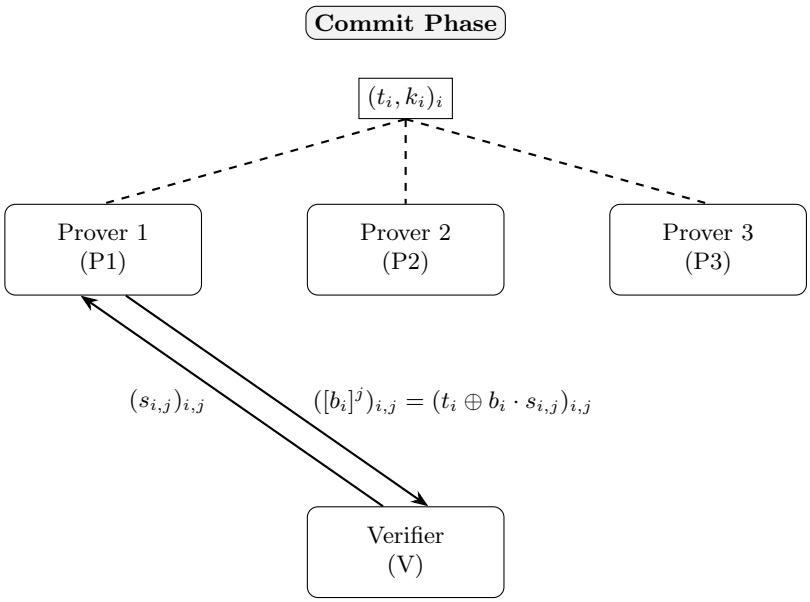

Fig. 8: Commit phase diagram

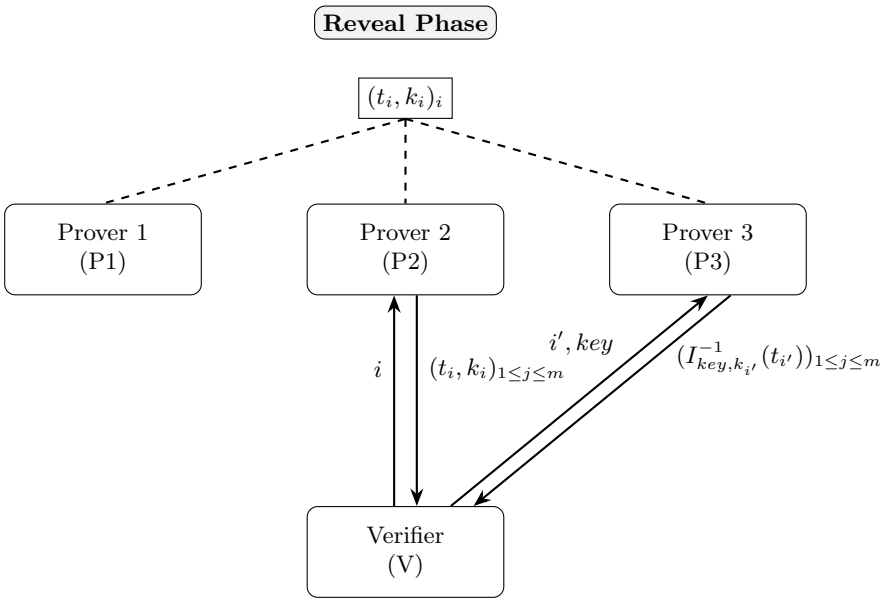

Fig. 9: Reveal phase diagram

A.2 Commitment using secret sharing

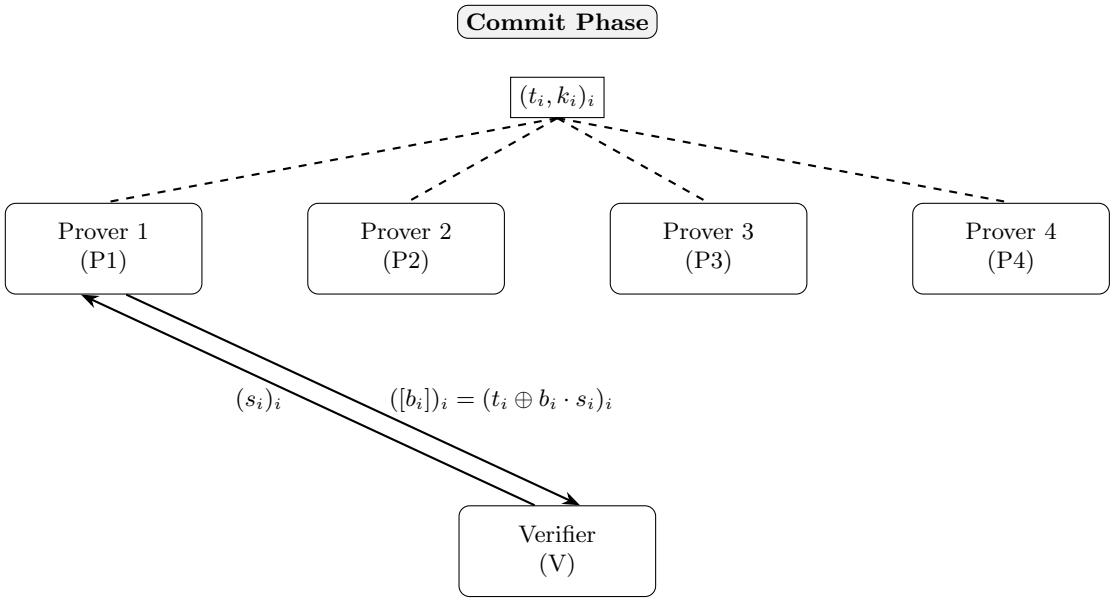

Fig. 10: Commit phase diagram using secret sharing

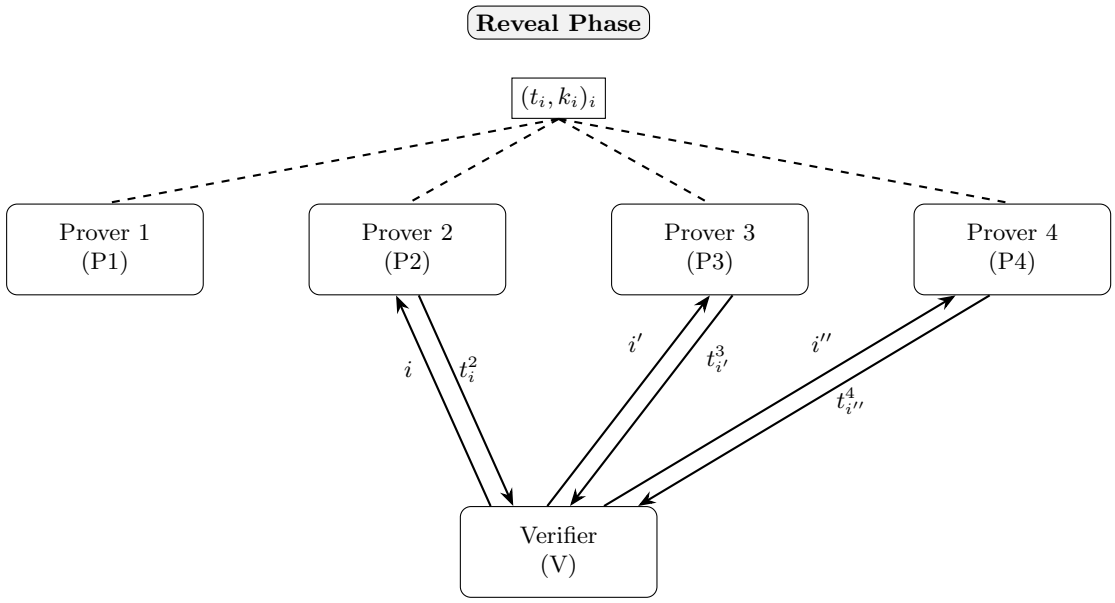

Fig. 11: Reveal phase diagram using secret sharing

B More on interpretation games

Let us explore a bit more the properties of interpretation games, partly as we want to know if we can build good interpretation games but also as this is an interesting object.

The first idea would be to check if some well known non-local games can be written in the way of interpretation games. In this way we can check that the CHSH game cannot be written this way, we explain this in the following proposition.

Proposition 3. *The CHSH game is not an interpretation game.*

Proof. The CHSH game consists of the following : two players Alice and Bob receive respectively inputs x, y and need to output a, b such that $a \oplus b = x \cdot y$. Thus, given x, y and the answer of Bob b, there is only one good answer defined as $a = b \oplus (x \cdot y) = \pi_{x,y}(b)$. Hence, the CHSH game is a projection game.

Let us study the function $\Pi : (x, y) \mapsto \pi_{x,y}$.

- $\pi_{0,0}(0) = 0, \quad \pi_{0,0}(1) = 1$
- $\pi_{1,0}(0) = 0, \quad \pi_{0,0}(1) = 1$
- $\pi_{0,1}(0) = 0, \quad \pi_{0,0}(1) = 1$
- $\pi_{1,1}(0) = 1, \quad \pi_{0,0}(1) = 0$

We recall that for a projection game to be an interpretation game we need that for all fixed x, b, $\Pi(x, \cdot)(b) : y \mapsto \Pi(x, y)(b)$ is bijective.

Here, for $x = 0, b = 0$ we have that $\Pi(0, 0)(0) = 0 = \Pi(0, 1)(0)$. Thus the CHSH game is not an interpretation game. □

Let us now show that we can easily find the no-signaling value for some interpretation games that we call constant size interpretation games.

Definition 12. *Constant size Interpretation*
An interpretation is said to be constant size if there exists constants S, T, F such that for any x, y and any a we have that

– $|S_{x,y,a}|$ *is either* 0 *or* S *where* $S_{x,y,a} = \{b | I_{x,b}(a) = y\}$
– $|T_{x,a}| = T$ *where* $T_{x,a} = \{y | S_{x,y,a} \neq \emptyset\}$.
– $|F_{x,y}|$ *is either* 0 *or* F *where* $F_{x,y} = \{a | S_{x,y,a} \neq \emptyset\}$.

Example 3. Take $n = 3$ and let us order the 8 binary words of length 3. Let $b_1b_2b_3b_4$ represent a function on those words which sends 1 to 2 if $b_1 = 1$ else 1 to 1 and 2 to 2, similarly for b_2 with 3 and 4, etc... Consider the 2^6 words made of the concatenation of 2 words of length 3, we can attach to each function 4 such words. To do this, let us say that given (x, b) the two 3 bits word of the index, $x_1x_2b_1b_2$ represents the function and x_3b_3 are useless.

Finally, we have that in this case, for all x, y, a $|S_{x,y,a} = 2^2|$: knowing x, a, y half of the b send a to y as long as a, y are in the same block. We also have $|T_{x,a}| = 2$ for all x, a, and $|F_{x,y}| = 2$ if it is not empty. Hence, this is a constant size interpretation.

Remark 6. If I is a constant size interpretation we get that $F = T$. To see prove this, observe that if $a \in F_{x,y}$ then $y \in Tx, a$. Thus, a is in exactly T sets $F_{x,y}$. This is similar for all a, thus $\sum_y |F_x, y| = 2^n F = 2^n T$. Hence $F = T$.

It is important to note that $|T_{x,a}| = T$ for all x, a does not imply $|F_{x,y}| = F$ for all x, y, we do need the condition on F in the definition of constant size, and similarly for T.

Proposition 4. *For any interpretation* I *we have* $w_{NS}(I) \leq 2^{-n}T$ *where* $T = \max_{x,a} |T_{x,a}|$.

Proof. Let θ be a no-signaling strategy on the interpretation game associated to I.

$$
\begin{aligned}
w(\theta, I) &= \sum_a \text{Prob}(win|a)\theta(a) \\
&= \sum_a \text{Prob}(win|a) \sum_x \frac{1}{2^n}\theta(a|x) \\
&= \sum_a \sum_{x,y \in T_{x,a}} \frac{1}{4^n}\theta(a, S_{x,y,a}|x, y) \\
&= \sum_a \sum_{x,y \in T_{x,a}} \frac{1}{4^n}\theta(a, S_{x,y,a}|x, y) \\
&\leq \sum_a \sum_{x,y \in Tx,a} \frac{1}{4^n}\theta(a, y) \quad \text{as } \theta(a, S_{x,y,a}|x, y) \leq \theta(a|y) \\
&= \sum_a \sum_x 4^{-n}|T_{x,a}|\theta(a|y) \quad \text{As } \theta(a|y) \text{ only depends on } a \\
&\leq \sum_a \sum_x 4^{-n}T\theta(a|y) \quad \text{As } T = \max_{x,a} |T_{x,a}| \\
&= 2^{-n}T
\end{aligned}
$$

□

Thus, considering the interpretation we built in Example 3 we get that its no-signaling value cannot exceed $\frac{1}{4}$. Furthermore, applying Proposition 4 to the interpretation of Lemma 1 directly gives that the no-signaling value is less than $\frac{1}{4}$.

Lemma 6. *For any constant size interpretation* I *with* $T = 2^n$ *we have* $w_{NS}(I) = 1$.

Proof. Consider the following strategy :

$$
\theta(a, b|x, y) = \begin{cases} \frac{1}{2^n S} & \text{if } I_{x,b}(a) = y \\ 0 & \text{otherwise} \end{cases}
$$

First of all, it is easy to show that this strategy has value 1.

$$\begin{aligned}
w(\theta, I) &= \sum_{x,y} 4^{-n} \sum_{a,b} \theta(a,b|x,y) 1[I_{x,b}(a) = y] \\
&= \sum_{x,y} 4^{-n} \sum_{a} \sum_{b \in S_{x,y,a}} \theta(a,b|x,y) \\
&= \sum_{x,y} 4^{-n} \sum_{a} \sum_{b \in S_{x,y,a}} \frac{1}{2^n S} \\
&= \sum_{x,y} 4^{-n} \quad \text{Here we use } T = 2^n \text{ and } I \text{ is constant size, as we implicitly said } |S_{x,y,a}| = S \text{ for all } x, y, a. \\
&= 1
\end{aligned}$$

Let us now prove that the strategy is indeed a no-signaling strategy. Let us for now fix some x, y and show that θ defines a valid probability distribution on the outputs.

$$\sum_{a,b} \theta(a,b|x,y) = \sum_{a} \sum_{b \in S_{x,y,a}} \theta(a,b|x,y) = \sum_{a} \sum_{b \in S_{x,y,a}} \frac{1}{2^n S} = 1$$

Now let us study the no-signaling conditions :

$$\begin{aligned}
\text{Prob}(a|x,y) &= \sum_{b} \theta(a,b|x,y) \\
&= \sum_{b \in S_{x,y,a}} \theta(a,b|x,y) \\
&= \sum_{b \in S_{x,y,a}} \frac{1}{2^n S} \\
&= 2^{-n} \quad \text{and this in independent of } y
\end{aligned}$$

$$\begin{aligned}
\text{Prob}(b|x,y) &= \sum_{a} \theta(a,b|x,y) \\
&= \sum_{a = I_{x,b}^{-1}(y)} \theta(a,b|x,y) \\
&= \theta(I_{x,b}^{-1}(y), b|x,y) \\
&= \frac{1}{2^n S} \quad \text{and this in independent of } x
\end{aligned}$$

Hence, the strategy is indeed no-signaling.

□

Remark 7. We do not need any assumption on the $F_{x,y}$ for this result.

This result is important as in the context of commitment using interpretation games, we would need sets $T_{x,a}$ of constant size with $T = 2^n$ to get perfect hiding. And such interpretation has to be non-constant size, else the no-signaling value would be 1 using Lemma 6.

However if $T_{x,a} = \{0,1\}^n$ for all x, a. We get that for all y there is exactly one b in $S_{x,y,a}$. Thus, $T = 2^n$ implies $S = 1$.

Theorem 3. *There is no good interpretation.*

Proof. Since Lemma 6 does not use any assumption on $F_{x,y}$, and since $T_{x,a} = \{0,1\}^n$ for all x, a implies $|S_{x,y,a}| = 1$ for all x, y, a. We have that any interpretation with $T_{x,a} = \{0,1\}^n$ for all x, a has a no-signaling value of 1. Thus, there is no good interpretation. □

As interpretation games are of interest on their own, let us now try to extend the previous result to arbitrary constant size interpretations.

Theorem 4. *For any constant size interpretation I we have $w_{NS}(I) = 2^{-n}T$.*

Proof. Consider the following strategy :

$$\theta(a,b|x,y) = \begin{cases} \frac{1}{2^n S} & \text{if } I_{x,b}(a) = y \\ 0 & \text{if } y \in T_{x,a}, I_{x,b}(a) \neq y \\ \frac{1}{4^n} & \text{otherwise} \end{cases}$$

Let us first prove that this defines a valid probability distribution over the outputs for any inputs x, y.

$$\begin{aligned}
\sum_{a,b} \theta(a,b|x,y) &= \sum_{a \in F_{x,y}} \left[\sum_{b \in S_{x,y,a}} \theta(a,b|x,y) + \sum_{b \notin S_{x,y,a}} \theta(a,b|x,y) \right] + \sum_{a \notin F_{x,y}} \sum_{b} \theta(a,b|x,y) \\
&= \sum_{a \in F_{x,y}} \left[\sum_{b \in S_{x,y,a}} \frac{1}{2^n S} + \sum_{b \notin S_{x,y,a}} 0 \right] + \sum_{a \notin F_{x,y}} \sum_{b} \frac{1}{4^n} \\
&= 2^{-n} F + 0 + 2^n (2^n - F) 4^{-n} \\
&= 1
\end{aligned}$$

Thus, this indeed defines a valid probability distribution. Now, let us study the value of this strategy and check if it is no-signaling.

$$\begin{aligned}
w(\theta, I) &= \sum_{x,y} 4^{-n} \sum_{a,b} \theta(a,b|x,y) 1[I_{x,b}(a) = y] \\
&= \sum_{x,y} 4^{-n} \sum_{a \in F_{x,y}} \sum_{b \in S_{x,y,a}} \theta(a,b|x,y) \\
&= \sum_{x,y} 4^{-n} \sum_{a \in F_{x,y}} \sum_{b \in S_{x,y,a}} \frac{1}{2^n S} \\
&= 2^{-n} F \\
&= 2^{-n} T \quad \text{as } T = F \text{ for constant size interpretations}
\end{aligned}$$

$$\begin{aligned}
\theta(a|x,y) &= \sum_{b} \theta(a,b|x,y) \\
&= \delta_{a \in F_{x,y}} \left[\sum_{b \in S_{x,y,a}} \theta(a,b|x,y) + \sum_{b \notin S_{x,y,a}} \theta(a,b|x,y) \right] + (1 - \delta_{a \in F_{x,y}}) 2^n \frac{1}{4^n} \\
&= \delta_{a \in F_{x,y}} 2^{-n} + (1 - \delta_{a \in F_{x,y}}) \frac{1}{2^n} \\
&= \theta(a|x)
\end{aligned}$$

$$\begin{aligned}\theta(b|x,y) &= \sum_a \theta(a,b|x,y)\\ &= \sum_{a\in F_{x,y}} \theta(a,b|x,y) + \sum_{a\notin F_{x,y}} \theta(a,b|x,y)\\ &= \sum_{a=I_{x,b}^{-1}(y)} \theta(a,b|x,y) + (2^n - F)4^{-n}\\ &= \frac{1}{2^n S} + \frac{2^n - F}{4^n}\\ &= \theta(b|y)\end{aligned}$$

This proves that the strategy indeed satisfy the no-signaling conditions. Finally, we get that for all constant size interpretation game, there is a strategy winning with probability $2^{-n}T$, which gives $w_{NS}(I) \geq 2^{-n}T$. And using Proposition 4 we already have that $w_{NS}(I) \leq 2^{-n}T$. Thus $w_{NS}(I) = 2^{-n}T$ for all constant size interpretations I. □

C More on the impossibility results

Lemma 7. *For all $k \in \mathbb{N}$, there is no commitment scheme with k committers, 1 opener which is perfectly sound, perfectly hiding and has binding against no-signaling adversaries.*

Proof. Let us consider a simple one round $k+1$ provers commitment scheme Com which is perfectly hiding, perfectly sound, with k committers and 1 opener. Com is defined by the distributions $p(s_1,\dots,s_k)$, $p_0(c_1,\dots,c_k,t|s_1,\dots,s_k), p_1(c_1,\dots,c_k,t|s_1,\dots,s_k)$ and the predicate $Acc(c_1,\dots,c_k,t|s_1,\dots,s_k,b)$.

Let us consider the strategy on the associated binding game defined as

$$q(c_1,\cdots,c_k,t|s_1,\dots,s_k,b) = p_b(c_1,\cdots,c_k,t|s_1,\dots,s_k) \quad .$$

Let us prove that this strategy is indeed no-signaling : Let $I \subseteq [\![k]\!]$ a subset of the committers,

$$\begin{aligned}q(c_I,t|s_1,\dots,s_k,b) &= \sum_{c_i:i\notin I} p_b(c_1,\dots c_k,t|s_1,\dots,s_k)\\ &= p_b(c_I,t|s_I) \quad \text{, as honest provers are no-signaling}\\ &= q(c_I,t|s_I,b) \quad .\end{aligned}$$

$$\begin{aligned}q(c_I|s_1,\dots,s_k,b) &= \sum_t \sum_{c_i,i\notin I} p_b(c_1,\dots c_k,t|s_1,\dots,s_k)\\ &= p_b(c_I|s_I) \quad \text{, as honest provers are no-signaling}\\ &= p_{1-b}(c_I|s_I) \quad \text{, as Com is perfect hiding}\\ &= q(c_I|s_I) \quad .\end{aligned}$$

Thus, the strategy is indeed no-signaling. Let us now prove that it breaks the binding property with probability 1.

$$\begin{aligned}\text{Prob}(\mathsf{Acc}|b) &= \sum_{s_1,\dots,s_k} p(s_1,\dots,s_k) \sum_{c_1,\dots,c_k} \sum_t q(c_1,\dots,c_k,t|s_1,\dots,s_k,b)\mathsf{Acc}(c_1,\dots,c_k,t|s_1,\dots,s_k,b)\\ &= \sum_{s_1,\dots,s_k} p(s_1,\dots,s_k) \sum_{c_1,\dots,c_k} \sum_t p_b(c_1,\dots,c_k,t|s_1,\dots,s_k)\mathsf{Acc}(c_1,\dots,c_k,t|s_1,\dots,s_k,b)\\ &= 1 \quad \text{, as Com is perfectly sound.}\end{aligned}$$

This strategy also defines a valid probability distribution. Thus, there is no one round simple commitment scheme with one opener which is perfectly hiding, perfectly sound and statistically binding against no-signaling adversaries. □

D More on 4 prover bit commitments

D.1 Linear programming algorithm

Algorithm 1 Check Binding of Commitment Using LP

Input: Security parameter n
Generate all bitstrings $\mathcal{S} = \{0,1\}^n$
Define decision variable $P(a_1, a_2, a_3, a_4, s, b_2, b_3, b_4, c_4) \geq 0$
Initialize constraint list $\mathcal{C} \leftarrow \emptyset$
▷ Normalization
for all $s \in \mathcal{S}$ and $b_2, b_3, b_4, c_4 \in \{0,1\}$ **do**
    Add constraint: $\sum_{a_1,a_2,a_3,a_4} P(\cdot|s, b_2, b_3, b_4, c_4) = 1$ to $\mathcal{C}$
end for
▷ No-signaling constraints across marginal views
for all appropriate marginals (e.g., a_1, a_2, a_3, a_1a_2,$a1a3$, etc...) **do**
    Add equality of marginals to $\mathcal{C}$
end for
▷ Define objective function
Initialize `objective` $\leftarrow 0$
for all $s \in \mathcal{S}, b \in \{0,1\}$ **do**
    for all $a_1 \in \mathcal{S}$ **do**
        $t = \texttt{XOR}(a_1, s \cdot b)$
        for all $a_2 \in \mathcal{S}$ **do**
            $a_3 \leftarrow t \oplus a_2$
            Add $P(a_1, a_2, a_3, a2, s, b, b, b, 0)$ to objective
            Add $P(a_1, a_2, a_3, a3, s, b, b, b, 1)$ to objective
        end for
    end for
end for
Solve the LP: max `objective` subject to constraints $\mathcal{C}$
Output: Optimal value of LP and whether binding is broken

D.2 Attack on commitment using secret sharing

Let us denote by $\text{check}_{i,j}$ the fact that the condition $\frac{a_i - a_j}{c_i - c_j} = a_1 + b_i \cdot s$ is satisfied. To break the binding, one can consider the following strategy :

$$\theta(a_1, a_2, a_3, a_4|s, c_2, c_3, c_4, b_2, b_3, b_4) = \begin{cases} \frac{1}{q^2} & \text{if } b_2 = b_3 = b_4 \text{ and } \text{check}_{2,3}, \text{check}_{2,4}, \text{check}_{3,4} \\ \frac{1}{q^3} & \text{if } b_2 = b_3 \neq b_4 \text{ and } \text{check}_{2,3} \\ \frac{1}{q^3} & \text{if } b_2 = b_4 \neq b_3 \text{ and } \text{check}_{2,4} \\ \frac{1}{q^3} & \text{if } b_3 = b_4 \neq b_2 \text{ and } \text{check}_{3,4} \\ 0 & \text{otherwise} \end{cases}$$

Proposition 5. *The strategy has value* 1 *and is no-signaling.*

Proof. Let us start by the value of this strategy on the binding game :

$$\begin{aligned}
w(\theta) &= \sum_s \sum_{c=(c_2,c_3,c_4)} \sum_{b_2,b_3,b_4} \text{Prob}(s,c,b_2,b_3,b_4) \sum_{a_1,a_2,a_3,a_4} \theta(a_1,a_2,a_3,a_4|s,c,b_2,b_3,b_4)\mathsf{Acc}(\theta(a_1,a_2,a_3,a_4|s,c,b_2,b_3,b_4)) \\
&= \sum_s \sum_{|\{c_2,c_3,c_4\}|=3} \sum_b \text{Prob}(s,c_2,c_3,c_4,b_2,b_3,b_4) \sum_{a_1,a_2,a_3,a_4 \text{ st } \text{check}_{2,3},\ \text{check}_{2,4},\ \text{check}_{3,4}} \frac{1}{q^2} \\
&= \sum_s \sum_{|\{c_2,c_3,c_4\}|=3} \sum_b \text{Prob}(s,c_2,c_3,c_4,b_2,b_3,b_4) \sum_{a_1,a_2} \frac{1}{q^2} \text{ As fixing } a_1,a_2 \text{ and asking the checks fixes } a_3,a_4 \\
&= \sum_s \sum_{|\{c_2,c_3,c_4\}|=3} \sum_b \text{Prob}(s,c_2,c_3,c_4,b_2,b_3,b_4) \\
&= 1 \text{ As those are the only queries the honest verifier makes}
\end{aligned}$$

Let us now prove that this strategy is indeed no-signaling. Since this strategy is symmetric in a_2,a_3,a_4 we will only show the marginals involving a_1 and a_2.

$$\begin{aligned}
\theta(a_1|s,c_2,c_3,c_4,b_2,b_3,b_4) &= \sum_{a_2,a_3,a_4} \theta(a_1,a_2,a_3,a_4|s,c,b_2,b_3,b_4) \\
&= \begin{cases} \sum_{a_2,a_3,a_4 \text{ st } \text{check}_{2,3},\ \text{check}_{2,4},\ \text{check}_{3,4}} \frac{1}{q^2} & \text{if } b_2=b_3=b_4 \\ \sum_{a_2,a_3,a_4 \text{ st } \text{check}_{2,3}} \frac{1}{q^3} & \text{if } b_2=b_3\neq b_4 \\ \sum_{a_2,a_3,a_4 \text{ st } \text{check}_{2,4}} \frac{1}{q^3} & \text{if } b_2=b_4\neq b_3 \\ \sum_{a_2,a_3,a_4 \text{ st } \text{check}_{3,4}} \frac{1}{q^3} & \text{if } b_3=b_4\neq b_2 \end{cases} \\
&= \begin{cases} q\frac{1}{q^2} & \text{if } b_2=b_3=b_4 \\ q^2\frac{1}{q^3} & \text{if } b_2=b_3\neq b_4 \\ q^2\frac{1}{q^3} & \text{if } b_2=b_4\neq b_3 \\ q^2\frac{1}{q^3} & \text{if } b_3=b_4\neq b_2 \end{cases} \\
&= \frac{1}{q} \\
&= \theta(a_1|s)
\end{aligned}$$

$$\begin{aligned}
\theta(a_1,a_2|s,c_2,c_3,c_4,b_2,b_3,b_4) &= \sum_{a_3,a_4} \theta(a_1,a_2,a_3,a_4|s,c,b_2,b_3,b_4) \\
&= \begin{cases} \sum_{a_3,a_4 \text{ st } \text{check}_{2,3},\ \text{check}_{2,4},\ \text{check}_{3,4}} \frac{1}{q^2} & \text{if } b_2=b_3=b_4 \\ \sum_{a_3,a_4 \text{ st } \text{check}_{2,3}} \frac{1}{q^3} & \text{if } b_2=b_3\neq b_4 \\ \sum_{a_3,a_4 \text{ st } \text{check}_{2,4}} \frac{1}{q^3} & \text{if } b_2=b_4\neq b_3 \\ \sum_{a_3,a_4 \text{ st } \text{check}_{3,4}} \frac{1}{q^3} & \text{if } b_3=b_4\neq b_2 \end{cases} \\
&= \begin{cases} \frac{1}{q^2} & \text{if } b_2=b_3=b_4 \text{ as there is only once possible choice of } a_3,a_4 \\ q\frac{1}{q^3} & \text{if } b_2=b_3\neq b_4 \text{ as there is only once possible choice of } a_3 \text{ and } q \text{ for } a_4 \\ q\frac{1}{q^3} & \text{if } b_2=b_4\neq b_3 \text{ as there is only once possible choice of } a_4 \text{ and } q \text{ for } a_3 \\ q\frac{1}{q^3} & \text{if } b_3=b_4\neq b_2 \text{ as there are } q \text{ possible choice of } a_3 \text{ and then it fixes } a_4 \end{cases} \\
&= \frac{1}{q^2} \\
&= \theta(a_1,a_2|s,c_2,b_2)
\end{aligned}$$

We could very similarly study the marginal of a_2, a_1,a_2,a_3, a_2,a_3, a_2,a_4, etc... and we would obtain that this strategy is no-signaling.

□