Recursive cheating strategies for the relativistic F_Q bit commitment protocol

Rémi Bricout, André Chailloux

Recursive cheating strategies for the relativistic $\mathbb{F}_Q$ bit commitment protocol

Rémi Bricout and André Chailloux
Inria, Paris.

Abstract

In this paper, we study relativistic bit commitment, which uses timing and location constraints to achieve information theoretic security. We consider the $\mathbb{F}_Q$ multi-round bit commitment scheme introduced by Lunghi *et al.* [LKB+15]. This protocol was shown secure against classical adversaries as long as the number of rounds m is small compared to $\sqrt{Q}$ where Q is the size of the used field in the protocol [CCL15, FF16].

In this work, we study classical attacks on this scheme. We use classical strategies for the CHSH_Q game described in [BS15] to derive cheating strategies for this protocol. In particular, our cheating strategy shows that if Q is an even power of any prime, then the protocol is not secure when the number of rounds m is of the order of $\sqrt{Q}$. For those values of Q, this means that the upper bound of [CCL15, FF16] is essentially optimal.

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 at a speed greater than the speed of light. Note that NSS 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 infinite computing power. This is in contrast with used schemes, which most often rely on computational assumptions such as the hardness of factoring [RSA78].

The idea of using physical assumptions laws to ensure information theoretic security for cryptographic schemes is not a new one. The most striking example in recent years is Quantum Key Distribution (QKD) which allows two distant parties to distill a secret key with information-theoretic security [BB84]. The main idea of QKD is to exchange quantum states on an insecure quantum channel and check a posteriori whether they have been disturbed. If not, it means that no eavesdropper was tampering with the quantum channel and the quantum states can be safely used to distill a secret. In fact, this works provided that the quantum states are not too noisy. QKD is quite practical and has indeed been widely deployed, but at the same time, it requires dedicated hardware and can only work today provided the 2 parties are not too far away from each other, at most a few hundred kilometers (see for instance [KLH+15] for the current record).

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 non 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 an explicit implementation proposal). The original goal of Kent was to bypass the no-go theorems for quantum bit-commitment [May97, LC97]. Interestingly, this original protocol was classical and allowed for several rounds which increased the lifespan of the protocol. However, the protocol required to exchange

messages whose length scaled exponentially in the number of rounds (i.e. the commitment time) and a feasible implementation was not possible for a large number of rounds. A subsequent work [Ken05] improved this scaling, but to our knowledge, no precise time/security tradeoff is available for this protocol.

More recently, quantum relativistic bit commitment protocols were developed where the parties exchange quantum systems, with the hope that combining the no superluminal signaling principle with quantum theory will lead to more secure (but less practical) protocols [Ken11, Ken12, KTHW13]. In particular, the protocol [Ken12] was implemented in Ref. [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.* [CSST11] (see also [Sim07]). Based on this work, Lunghi *et al.* devised a multi-round bit commitment protocol involving only four agents, two for Alice and two for Bob [LKB$^+$15]. They managed to prove that this protocol, which we call the "$\mathbb{F}_Q$ protocol" from now on, remains secure for several rounds, against classical attacks. Unfortunately, this proof was rather inefficient since the complexity of the protocol (the size of the messages the agents need to exchange at each round) scaled exponentially with the number of rounds. Recently, two papers improved the security proof and showed that the complexity of the protocol in fact only scales logarithmically with the number of rounds [CCL15, FF16], implying that the commitment time is essentially unlimited:

Theorem 1 ([CCL15, FF16])**.** *The $\mathbb{F}_Q$ relativistic m-round bit commitment protocol is ε-binding with $\varepsilon = \mathcal{O}(\frac{m}{\sqrt{Q}})$ against classical adversaries, meaning that Alice's cheating probability is at most $\frac{1}{2} + \mathcal{O}(\frac{m}{\sqrt{Q}})$.*

While the two proofs of this fact are very different, they rely to some extent on the analysis of CHSH_Q, a non-signaling game that generalizes the well-known CHSH game to the case where inputs and outputs are not restricted to being bits, but rather belong to $\mathbb{F}_Q$ the Galois Field of order Q.

Notice that in the way the cheating probability is defined, a perfectly secure protocol will have cheating probability of $\frac{1}{2}$ for both Alice and Bob. So an ε-secure (here ε-binding) protocol will have a cheating probability of $\frac{1}{2} + \varepsilon$. The protocol has (stand-alone) security when ε is small.

The above result shows that the protocol is secure as long as $m \ll \sqrt{Q}$ but it was not known for larger values of Q, in particular when m approaches, or even exceeds $\Omega(\sqrt{Q})$. Very recently, this protocol has been implemented by keeping the agents 7 km apart and demonstrated a sustain period of 24 hours [VMH$^+$16]. Also, it is important to know that the number of bits sent at each round is $\log(Q)$ and therefore Q can be efficiently made exponentially big in the security parameter.

Until now, no cheating strategy has been proposed for this scheme.

1.2 Contributions

Our main contribution is to present the first attack on the $\mathbb{F}_Q$ protocol. We show the following

Theorem 2. *There exists an attack on the m-round $\mathbb{F}_Q$ protocol in which Alice's cheating probability is*

$$1 - \frac{1}{2}\left(\left(1 - \frac{1}{Q}\right)\left(1 - \omega(\mathsf{CHSH}_Q)\right)\right)^{\lfloor \frac{m-1}{3} \rfloor}$$

where $\omega(\mathsf{CHSH}_Q)$ is the classical value of the CHSH_Q game and $m \geq 3$.

In [BS15], it was shown for any prime p and integer n that

$$\omega(\mathsf{CHSH}_Q) = \begin{cases} \Omega(\sqrt{\frac{1}{Q}}) & \text{if } Q = p^{2n} \\ \mathcal{O}(Q^{-\frac{1}{2}-\varepsilon_0}) & \text{if } Q = p^{2n+1} \end{cases}$$

where ε_0 is a constant proven to be positive.

In particular, Theorem 2, combined with the above bound, shows that the upper bound of [CCL15, FF16] (Theorem 1) is essentially optimal when considering an even prime power :

Corollary 1. *For any integer n, prime number p and $Q = p^{2n}$ there is a cheating strategy for Alice that achieves success probability*

$$1 - \frac{1}{2}\left(1 - \Omega(\frac{1}{\sqrt{Q}})\right)^{\lfloor \frac{m-1}{3} \rfloor}.$$

- *If $m \ll \sqrt{Q}$ then the above cheating probability is equal to $\frac{1}{2} + \Omega(\frac{m}{\sqrt{Q}}) - o(\frac{m}{\sqrt{Q}})$.*
- *If $m = t\sqrt{Q}$ then the above cheating probability is lower bounded by $1 - \frac{1}{2}e^{-\frac{t}{3}}$, which quickly approaches 1 as t increases.*

From the above bounds, we can conclude that up to constant factors, our attack is optimal when Q is an even power of a prime.

We note also that there is an upper bound on the value of CHSH_Q when Q is an odd power of a prime. In this case, we have $\omega(\mathsf{CHSH}_Q) = \Omega(Q^{-2/3})$ [BS15, PP16]. From there, we have

Corollary 2. *For any integer n, prime number p and $Q = p^{2n+1}$ there is a cheating strategy for Alice that achieves success probability*

$$1 - \frac{1}{2}\left(1 - \Omega(Q^{-2/3})\right)^{\lfloor \frac{m-1}{3} \rfloor}.$$

and if $m = tQ^{\frac{2}{3}}$ then Alice can cheat with probability $1 - \frac{1}{2}e^{-\frac{t}{3}}$ which quickly converges to 1 as t increases.

This result also shows that even an improved bound on $\omega(\mathsf{CHSH}_\mathsf{Q})$ variants presented in [PPP16] cannot be used to improve - except in the constants - the security of the $\mathbb{F}_Q$ protocol, at least for even prime powers of Q.

Our second contribution is an extension of this attack to more realistic scenarios from the attacker's point of view. In the relativistic model, we assume that cheating Alice can perform communications between $\mathcal{A}_1$ and $\mathcal{A}_2$ such that both agents of Alice know exactly the whole transcript of the protocol, except the last round message sent to the other Alice. Proving security in this setting allows us to minimize the spacetime requirements in order to achieve security.

However, our attack also assumes this power for cheating Alice and this could be very challenging in practice. Therefore, we introduce the notion of propagation time which corresponds to the number of rounds ρ that can pass until the Alices are able to send some information to one another. In the original model, this propagation time is 2 rounds. We perform extend Theorem 2 to the following setting

- The propagation time ρ can be larger than 2.
- The two Alices know the bit they want to reveal only after $k_0 \geq 1$ rounds. We call k_0 the decision time.

Showing that the attack works in this setting ensures that simple countermeasures consisting of increasing the distance between the two pairs will not significantly reduce the efficiency of the attack. We show the following:

Theorem 3. *For any propagation time $\rho \geq 2$, and any decision time k_0, there exists an attack on the m-round $\mathbb{F}_Q$ protocol where Alice's cheating probability is*

$$1 - \frac{1}{2}\left((1 - \frac{1}{Q})\,(1 - \omega(\mathsf{CHSH}_\mathsf{Q}))\right)^{\lfloor \frac{m-k_0-1}{\rho+1} \rfloor}.$$

for $m \geq k_0 + 2$.

Organisation — In Section 2, we present the $\mathbb{F}_Q$ protocol as well as the CHSH_Q game. In Section 3, we present our main result, namely the attack on the $\mathbb{F}_Q$ protocol. Finally, in Section 4, we present the extension of this attack to more realistic scenarios.

2 Preliminaries

2.1 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 random 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 knows no information about d. 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.

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 has no information about the key 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 most usual models.

We now give a formal definition of the bit commitment scheme.

Definition 1. *A bit 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 "Accept" or "Reject".*

We also define the following security requirements for the commitment scheme.

Definition 2. *A bit commitment protocol is said to be correct if when both players are honest, Bob never outputs "Reject".*

A cheating strategy S for Alice can be therefore decomposed into a cheating strategy S_{commit} for the commit phase and S_{reveal} for the reveal phase and we will usually write $S = (S_{commit}, S_{reveal})$. The goal of a cheating Alice is to choose the value she wants to reveal only after the commit phase. The reveal strategy S_{reveal} will depend on the value d she wants to reveal. We denote by $S_{reveal}(d)$ Alice's cheating strategy in the reveal phase for a fixed d.

Definition 3. *For a fixed cheating strategy $S = (S_{Commit}, S_{reveal})$ for Alice, we define Alice's cheating probability $P_A^*(S)$ as*

$$P_A^*(S) := \frac{1}{2}\Pr[\textit{ Alice successfully reveals } d = 0 | (S_{Commit}, S_{reveal}(0))] + \frac{1}{2}\Pr[\textit{ Alice successfully reveals } d = 1 | (S_{Commit}, S_{reveal}(1))].$$

Definition 4. *We define Alice's optimal cheating probability P_A^* as*

$$P_A^* := \max_{S=(S_{Commit}, S_{reveal})} P_A^*(S).$$

We say that a bit commitment is ε sum-binding if $P_A^* \leq \frac{1}{2} + \varepsilon$.

Here, we used one of several possible definitions for the binding property. This definition is weak, since it doesn't necessarily behave well under composition. In order to prove security, even for relativistic bit

commitment protocols, some stronger definitions of security are used (see for example [FF16]). While using a stronger security definitions strengthens upper bounds on the cheating probability, it is by using the weakest security definition that we have the strongest lower bounds on those cheating probabilities. Since in this paper, we present cheating strategies, *i.e.* lower bounds, we use the weak notion of sum-binding.

Another security condition we want to ensure is the hiding property. At the end of the commit phase, we don't want Bob to have a lot of information about the committed bit d. This means that to ensure the hiding property, we will only be interested in a cheating Bob's strategy during the commit phase, and a cheating strategy S^B for Bob will be a strategy that he will use to try to learn d after the commit phase.

Definition 5. *For a fixed cheating strategy S^B for Bob, we define his cheating probability $P_B^*(S^B)$ as*

$$P_B^*(S^B) := \Pr[\textit{Bob guesses } d \textit{ after the Commit phase}|S^B].$$

Definition 6. *We define Bob's optimal cheating probability P_B^* as*

$$P_B^* := \max_{S^B} P_B^*(S^B).$$

We say that a bit commitment is ε-hiding is $P_B^* \leq \frac{1}{2} + \varepsilon$.

2.2 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 $i \in \{1, 2\}$, Alice$_i$ interacts only with Bob$_i$. 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 create some non-signaling type scenarios. Here, we will only use the property that the two honest Bobs 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 in the above Section. We will now describe the $\mathbb{F}_Q$ relativistic bit commitment scheme. This description 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 know at the beginning of the sustain phase the bit d they want to reveal. In Section 4, we will relax this requirement.

The single-round $\mathbb{F}_Q$ protocol. — The single-round version corresponds 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 x to $\mathcal{A}_1$, who returns $y = a + d \cdot x$ where $d \in \{0, 1\}$ is the committed bit.
3. *Sustain phase*: $\mathcal{A}_1$ and $\mathcal{A}_2$ wait for some time $\tau < D/c$.
4. *Reveal phase*: $\mathcal{A}_2$ reveals the values of d and a to $\mathcal{B}_2$ who checks that $y = a + d \cdot x$.

The multi-round protocol.— The protocol above was recently extended to a multi-round commitment scheme [LKB$^+$15]. The main idea to increase the commitment time is to delay the reveal phase and have $\mathcal{A}_2$ commit to the string a instead of revealing it. In fact, the new sustain phase will now consist of many

rounds where the active players (i.e. the player to commits in that given round and the corresponding player for Bob) alternate between locations 1 and 2, separated by a distance D. The m-round bit commitment protocol goes as follows

1. *Preparation phase*: $\mathcal{A}_1, \mathcal{A}_2$ (resp. $\mathcal{B}_1, \mathcal{B}_2$) share m random numbers $a_1, \ldots, a_m$ (resp. $x_1, \ldots, x_m$) $\in \mathbb{F}_Q$.
2. *Commit phase*: $\mathcal{B}_1$ sends x_1 to $\mathcal{A}_1$, who returns $y_1 = d \cdot x_1 + a_1$, where $d \in \{0, 1\}$ is the committed bit.
3. *Sustain phase*: for each round k, with $2 \leq k < m$, $\mathcal{B}_{k \bmod 2}$ sends x_k to $\mathcal{A}_{k \bmod 2}$, who returns $y_k = x_k \cdot a_{k-1} + a_k$.
4. *Reveal phase*: $\mathcal{A}_1$ reveals d and $y_m = a_{m-1}$ to $\mathcal{B}_1$. Bob checks that $y_m = \alpha_{m-1}$, where we recursively define $\alpha_0 := d$, $\alpha_i := y_i - b_i * \alpha_{i-1}$. α_i corresponds to what a_i "should be".

The main idea of the multi-round protocol is to delay the reveal phase in order to increase the commitment time. This delay is obtained by making the passive Alice commit to the value of the string she was supposed to reveal in the previous round. Since each round increases the total commitment time by D/c, modulo the time needed for the various algebraic manipulations in $\mathbb{F}_Q$, one sees that the required number of rounds scales linearly with the commitment time one wishes to achieve.

We require that round j finishes before any information about x_{j-1} reaches the other Alice. For any j, we therefore have the following : active Alice has no information about x_{j-1}. This means that y_j is independent of x_{j-1}. This will be crucial in order to show security of the protocol. One important thing to notice is that d, the bit Alice wants to reveal can be decided just after the commit phase. Therefore, y_1 is independent of d but all the other messages $y_2, \ldots, y_m$ can depend on d.

Both those protocol are perfectly hiding. Moreover, from Theorem 1, the multi-round protocol is ε sum-binding, with $\varepsilon = O(\frac{m}{\sqrt{Q}})$.

2.3 The CHSH_Q game

A crucial tool for our attack (and for the previous security analysis), is the CHSH_Q two-player game introduced by Buhrman and Massar [BM05]. This game is a natural generalization of the CHSH game to the field $\mathbb{F}_Q$, where two cooperating but non-communicating parties, Alice and Bob, are respectively given an input x and y chosen uniformly at random from $\mathbb{F}_Q$, and must output two numbers $a, b \in \mathbb{F}_Q$. They win the game whenever the condition $a + b = x \cdot y$ is satisfied. The value of a game G, denoted $\omega(G)$, corresponds to the maximum probability of winning the game. A recent result by Bravarian and Shor [BS15] establishes bounds on $\omega(\mathrm{CHSH}_Q)$. They show the following

Proposition 1. *for any prime p and integer n, we have*

$$\omega(\mathsf{CHSH}_Q) = \begin{cases} \Omega(\sqrt{\frac{1}{Q}}) & \text{if } Q = p^{2n} \\ \mathcal{O}(Q^{-\frac{1}{2}-\varepsilon_0}) & \text{if } Q = p^{2n+1} \end{cases}$$

for some absolute constant $\varepsilon_0 > 0$.

We define a variant of the CHSH_Q game, that we call CHSH_Q^γ, which will be well defined for any $\gamma \in [0, 1]$. We will use this variant in Section 4, when we will have longer propagation and decision times.

Definition 7. *In $CHSH_Q^\gamma$, Alice receives $x = 0$ with probability γ and a random element $x \in \mathbb{F}_Q^*$, each with probability $\frac{1-\gamma}{Q-1}$. Bob receives an input y according to the same probability distribution. They output respectively a and b in $\mathbb{F}_Q$ and they win the game iff. $a + b = x \cdot y$.*

In short, CHSH_Q^γ is the same game as CHSH_Q, but the input distribution of each player is slightly biased towards 0. We have by definition $\mathsf{CHSH}_Q^{\frac{1}{Q}} = \mathsf{CHSH}_Q$. When playing CHSH_Q^γ, we have:

- The probability that Alice and Bob get $(0, 0)$ is γ^2.

- The probability that they get an element $(0,i)$ or $(i,0)$ with $i \in \mathbb{F}_Q^*$ is equal to $\frac{\gamma(1-\gamma)}{Q-1}$ for each such element.
- The probability that they get an element (i,j) with $i,j \in \mathbb{F}_Q^*$ is equal to $\frac{(1-\gamma)^2}{(Q-1)^2}$ for each such element.

Inspired by shift techniques used in [BS15], we can show:

Lemma 1. *For any $\gamma \in [0,1]$, $\omega(CHSH_Q^\gamma) \geq \omega(\mathsf{CHSH}_Q)$.*

Proof. As randomized strategies are nothing more than linear combinations of deterministic strategies, of which winning probability is given by the same linear combination, we can assume that all used optimal strategies are deterministic without loss of generality.

We consider an optimal strategy $S = (s_1, s_2)$ for the CHSH game i.e. function $s_1, s_2 : \mathbb{F}_Q \to \mathbb{F}_Q$ such that $\Pr_{x,y}[s_1(x) + s_2(y) = xy] = \omega(\mathsf{CHSH_Q})$, where the probability is over uniform x and y. We define $p_{x,y} := 1$ if $s_1(x) + s_2(y) = xy$ and 0 otherwise, which implies $\mathbb{E}_{xy} p_{xy} = \omega(\mathsf{CHSH}_Q)$. Let

$$Z_{u,v} := \gamma^2 p_{u,v} + \frac{\gamma(1-\gamma)}{Q-1}\left(\sum_{x\in\mathbb{F}_Q-\{u\}} p_{xv} + \sum_{y\in\mathbb{F}_Q-\{v\}} p_{uy}\right) + \frac{(1-\gamma)^2}{(Q-1)^2}\sum_{\substack{x\in\mathbb{F}_Q-\{u\}\\ y\in\mathbb{F}_Q-\{v\}}} p_{xy}.$$

$Z_{u,v}$ corresponds to the probability of winning the game $\mathsf{CHSH_Q}$ on a changed probability distribution. In particular, $Z_{0,0}$ corresponds to the probability of winning CHSH_Q^γ when using strategy S. One can check that $\mathbb{E}_{u,v}[Z_{u,v}] = \omega(\mathsf{CHSH_Q})$, so we can fix a pair (u,v) such that $Z_{u,v} \geq \omega(\mathsf{CHSH_Q})$.

We now consider the strategy $S' = (s_1', s_2')$ where $s_1'(x) = s_1(x+u) - xw$ and $s_2'(y) = s_2(y+v) - yu - uv$. S' wins for (x,y) precisely when S wins for $(x+u, y+v)$. Indeed :

$$\begin{array}{rcl} s_1'(x) + s_2'(y) = xy & \Leftrightarrow & s_1(x+u) - xv + s_2(y+u) - yu - uv = xy \\ & \Leftrightarrow & s_1(x+u) + s_2(y+v) = (x+u)(y+v) \end{array}$$

Similarly, as before, we define $p'_{xy} = 1$ if $s_1'(x) + s_2'(y) = x \cdot y$ and 0 otherwise. From the above equivalence, we have $p'_{x,y} = p_{(x+u),(y+v)}$. We also define

$$Z'_{u,v} := \gamma^2 p'_{u,v} + \frac{\gamma(1-\gamma)}{Q-1}\left(\sum_{x\in\mathbb{F}_Q-\{u\}} p'_{xv} + \sum_{y\in\mathbb{F}_Q-\{v\}} p'_{uy}\right) + \frac{(1-\gamma)^2}{(Q-1)^2}\sum_{\substack{x\in\mathbb{F}_Q-\{u\}\\ y\in\mathbb{F}_Q-\{v\}}} p'_{xy}.$$

Notice that $Z'_{0,0}$ corresponds to the probability of winning CHSH_Q^γ when using strategy S'. Moreover, for any (x,y), we have $Z'_{x,y} = Z_{x+u,y+v}$. From there, we conclude

$$\omega(\mathsf{CHSH}_Q^\gamma) \geq Z'_{0,0} = Z_{u,v} \geq \omega(\mathsf{CHSH}_Q),$$

which proves the desired result. ∎

3 Attack with perfect conditions

In this Section, we present our construction of a cheating strategy which will be essentially optimal for some values of Q. The protocol is perfectly hiding. Therefore, we are only interested in the binding property, *i.e.* in cheating Alice.

The idea of the attack is the following. Every three rounds (or more in Section 4), Alice's agents have an occasion to play a CHSH_Q game. If they win this game, which happens with probability $\omega(\mathsf{CHSH}_Q)$, they can easily fool Bob (with the provided strategy, sending only zeros until *reveal phase* is fine). If they do not manage to win the CHSH_Q game, they just try again three rounds later. More precisely, for each step of three rounds, the last two rounds are used to play the CHSH_Q game. The first one allows $\mathcal{A}_1$ and $\mathcal{A}_2$ to

determine if they won during the previous step, or calculate a corrective factor η if they did not. Thus, for a m-round long protocol, Alice's agent can play roughly $\frac{m}{3}$ such CHSH_Q games. As it is sufficient for them to win one of these games, we see that cheating probability grows exponentially with the number of rounds. Moreover, at each of these sets of three rounds, an additional factor $(1 - \frac{1}{Q})$ appears. Indeed, if at the third round of the set Bob sends a 0, Alice is also in a situation in which she can cheat, because this 0 makes Alice's error collapse to zero. However, the contribution of this additional factor can be neglected (it is only $\mathcal{O}(\frac{1}{Q})$, compared to the $\mathcal{O}(\frac{1}{\sqrt{Q}})$ given by CHSH_Q).

We assume for now that the propagation time of the information is 2 rounds. This means that when $\text{Alice}_{(i \bmod 2)}$ receives x_i, the other Alice will know the value of x_i at round $i+2$. Therefore, a cheating strategy for Alice is described by a m-tuple of functions $S = (s_1, \ldots, s_m)$, where each s_i corresponds to Alice's output function at round i. s_1 is a function of x_1 and s_i is a function of $(x_0, \ldots, x_{i-2}, x_i)$ for $i \geq 1$ where we use the convention $x_0 = d$. For each $i \geq 1, x_i \in \mathbb{F}_Q$ and the output space of each s_i is $\mathbb{F}_Q$.

Consider any fixed cheating strategy S for Alice. At the end of the protocol, Bob checks that $y_m = \alpha_{m-1}$. When we expand α_{m-1} as a function of $(d, x_1, \ldots, x_{m-1})$, the checking condition, that we call $\mathcal{C}_m$ becomes

$$y_m = y_{m-1} - x_{m-1}\Big(y_{m-2} - x_{m-2}\Big(\ldots\ \ldots - x_2(y_1 - d \cdot x_1)\ldots\Big)\Big).$$

If this equality is not verified, Alice is caught cheating. On the other hand, if $\mathcal{C}_m$ is verified then Bob cannot distinguish an honest Alice from a dishonest one, and he does not abort.

Let $\mathcal{C}_m(S, d, x_1, \ldots, x_{m-1})$ the event which corresponds to the above equality being verified. Alice's cheating probability using S, that we note $g_m(S)$ is therefore

$$g_m(S) := \Pr_{d, x_1, \ldots, x_{m-1}}[\mathcal{C}_m(S, d, x_1, \ldots, x_{m-1})]$$

where d is a uniformly random bit and $x_1, \ldots, x_{m-1}$ are uniformly random elements of $\mathbb{F}_Q$. We also define $g_m := \max_S g_m(S)$ which is Alice's maximal cheating probability in $\mathcal{P}_m$. In this section, we present a cheating strategy S for Alice such that

$$g_m(S) = \frac{1}{2} + \frac{1}{2}\left(1 - (1 - \omega(\mathsf{CHSH}_Q))^{\lfloor \frac{m-1}{3} \rfloor}\right).$$

which will prove Theorem 2. In order to do so, we first modify protocol $\mathcal{P}_m$ to make it more symmetric (Section 3.1). Then, we describe our attack (Section 3.2) and we prove its cheating probability (Section 3.3).

3.1 Symmetrization of the protocol

We want to describe a recursive strategy for protocol $\mathcal{P}_m$. Unfortunately, this protocol induces a difference between Alice's strategy at round $1 \leq k < m$ and her strategy at round m. Because of that, it is difficult to study the protocol recursively.

We therefore consider a modified protocol $\mathcal{P}'_m$, which, as we will show, is a bit easier than $\mathcal{P}_m$ to win, but harder than $\mathcal{P}_{m+1}$. In this modified version, at round m, $\text{Bob}_{m \bmod 2}$ sends an additional random string $x_m \in \mathbb{F}_Q$, and $\text{Alice}_{m \bmod 2}$ returns $y_m = x_m \cdot a_{m-1}$ instead of $y_m = a_{m-1}$. All other rounds are unchanged. Similarly, as for $\mathcal{P}_m$, a cheating strategy for Alice S' can be described as a m-tuple of functions $(s'_1, \ldots, s'_m)$ that give Alice's outputs y_i depending on her accessible information at round i.

Bob checks now that $y_m = x_m \cdot \alpha_{m-1}$ and therefore, the condition Alice must satisfied to win is modified into $\mathcal{C}'_m(S', d, x_1, \ldots, x_m)$, where

$$\mathcal{C}'_m(S', d, x_1, \ldots, x_m) \Leftrightarrow y_m = x_m\left(y_{m-1} - x_{m-1}\left(y_{m-2} - x_{m-2}\Big(\ldots\ \ldots - x_2(y_1 - d \cdot x_1)\ldots\Big)\right)\right)$$

By expanding ${\mathcal{C}'}_m(S', d, x_1, \ldots, x_m)$, it can be written down as :

$$\begin{array}{rcl} y_m & = & x_m \cdot y_{m-1} \\ & - & x_m \cdot x_{m-1} \cdot y_{m-2} \\ & + & x_m \cdot x_{m-1} \cdot x_{m-2} \cdot y_{m-3} \\ & \vdots & \vdots \\ & - & (-1)^m x_m \cdot x_{m-1} \cdot x_{m-2} \cdot \ldots \cdot x_1 \cdot d \end{array}$$

or, using a compact form:

$${\mathcal{C}'}_m(S', d, x_1, \ldots, x_m) \Leftrightarrow y_m = \sum_{i=1}^{m-1} \left((-1)^{m-i} y_i \cdot \prod_{j=i+1}^{m} x_i \right) - (-1)^m d \cdot \prod_{j=1}^{m} x_j$$

For a cheating strategy S', Alice's winning probability $g'_m(S')$ for this modified protocol is therefore defined as

$$g'_m(S') := \Pr_{d, x_1, \ldots, x_m}[{\mathcal{C}'}_m(S', d, x_1, \ldots, x_m)] \quad \text{and} \quad g'_m := \max_{S'} g'_m(S')$$

We show the following

Lemma 2. *$\forall m \geq 2$, we have $g_m \leq g'_m \leq g_{m+1}$.*

Proof.

- For the first inequality, let us consider the optimal strategy $S = (s_1, ..., s_m)$ for $\mathcal{P}_m$, where s_k is Alice's strategy at round k (i.e. a function that outputs y_k when given Alice's knowledge at round k). Alice's cheating probability for $\mathcal{P}_m$ is $g_m(S)$. Consider the following strategy $S' := (s_1, ..., s_{m-1}, s'_m)$ for $\mathcal{P}'_m$, where $s'_m(d, x_1, \ldots, x_{m-2}, x_m) := x_m \cdot s_m(d, x_1, \ldots, x_{m-2})$. S' allows to win on ${\mathcal{P}'}_m$ at least as efficiently as S on $\mathcal{P}_m$, because S' wins whenever S does. Indeed, suppose that S is a winning strategy for a given $(d, x_1, ..., x_{m-1})$. This means that $\mathcal{C}_m(S, d, x_1, \ldots, x_{m-1})$ is satisfied or equivalently:

  $$s_m(d, x_1, \ldots, x_{m-2}) = y_{m-1} - x_{m-1}\Big(y_{m-2} - \ldots \ldots - x_2(y_1 - d \cdot x_1)...\Big)$$

  Then, since $s'_m(d, x_1, \ldots, x_{m-2}, x_m) = x_m \cdot s_m(d, x_1, \ldots, x_{m-2})$, we get

  $$s'_m(d, x_1, \ldots, x_{m-2}, x_m) = x_m \left(y_{m-1} - x_{m-1}\Big(y_{m-2} - \ldots \ldots - x_2(y_1 - d \cdot x_1)...\Big) \right)$$

  which implies $\mathcal{C}'_m(S', d, x_1, \ldots, x_m)$, for any x_m. From there, we immediately get

  $$g_m = g_m(S) \leq g'_m(S') \leq g'_m.$$

- For the other inequality, we fix an optimal strategy $S' = (s_1, ..., s_m)$ for ${\mathcal{P}'}_m$. We consider the following strategy $S := (s_1, ..., s_m, \overline{0})$ for $\mathcal{P}_{m+1}$, where $\overline{0}$ is the function that always outputs 0, no matter the inputs. This means that when performing S, we always have $y_{m+1} = 0$. S is at least as good to win $\mathcal{P}_{m+1}$ as S' is to win ${\mathcal{P}'}_m$. Indeed, if for a tuple $(d, x_1, ..., x_m)$, S' wins on ${\mathcal{P}'}_m$, then $\mathcal{C}'(S', d, x_1, \ldots, x_m)$ holds or equivalently

  $$y_m = x_m \left(y_{m-1} - x_{m-1}\left(y_{m-2} - x_{m-2}\Big(\ldots \ldots - x_2(y_1 - d \cdot x_1)...\Big) \right) \right)$$

  From there, we immediately have

  $$y_{m+1} = 0 = y_m - x_m \left(y_{m-1} - x_{m-1}\left(y_{m-2} - x_{m-2}\Big(\ldots \ldots - x_2(y_1 - d \cdot x_1)...\Big) \right) \right)$$

  which implies $\mathcal{C}_{m+1}(S, d, x_1, \ldots, x_m)$. From there, we immediately get

  $$g'_m = g'_m(S') \leq g_{m+1}(S) \leq g_{m+1}.$$

■

The above lemma shows in particular how to transform a strategy for $\mathcal{P}'_m$ into a strategy for $\mathcal{P}_{m+1}$ with at least as good cheating probability. This means that we can study $\mathcal{P}'_m$ instead of $\mathcal{P}_{m+1}$. The first inequality shows that we do not lose much doing so.

We also make another change. In order to simplify calculations, we ask Alice to answer at each round i $\tilde{y}_i := (-1)^{i+1} y_i$ instead of y_i. For the protocol, it is totally equivalent to use $\tilde{y}_i$ or y_i but it allows to avoid all (-1) factors. With this notation, Alice's victory condition $\mathcal{C}'_m(S', d, x_1, \ldots, x_m)$ for the protocol becomes:

$$\sum_{i=1}^{m} \left(\tilde{y}_i \prod_{j=i+1}^{m} x_j \right) = d \prod_{j=1}^{m} x_j$$

In the next section, we present a cheating strategy for protocol $\mathcal{P}'_m$.

3.2 Description of the attack

In the previous section, we transformed protocol $\mathcal{P}$ into a slightly modified protocol $\mathcal{P}'$, which has extra symmetries and for which it will be simpler to construct a recursive cheating strategy. In this section, we describe this strategy for $\mathcal{P}'$.

More precisely, we define recursively a strategy with a step of three rounds. To initialize, we consider the following strategy for $\mathcal{P}'_3$:

- $\mathcal{A}_1$ always outputs $\tilde{y}_1 = 0$.
- $\mathcal{A}_1$ and $\mathcal{A}_2$ perform the optimal strategy for the CHSH_Q game with inputs x_1 and x_2. Let a and b be their respective outputs.
- $\mathcal{A}_2$ outputs $\tilde{y}_2 = d \cdot a$ for round 2 and $\mathcal{A}_1$ outputs $\tilde{y}_3 = x_3 \cdot d \cdot b$ for round 3.

With this strategy, $\mathcal{C}'_3$ becomes $x_3 \cdot d \cdot (a + b - x_1 \cdot x_2) = 0$. Alice wins if $x_3 = 0$, if $d = 0$, or if $a + b = x_1 \cdot x_2$. These events are independent, which gives $g'_3 \geq 1 - \frac{1}{2}(1 - \frac{1}{Q})(1 - \omega(\mathsf{CHSH}_Q))$.

We now describe a strategy for $k+3$ rounds using a strategy for k rounds. We fix a cheating strategy S'_k for Alice for $\mathcal{P}'_k$ and we present a cheating strategy S'_{k+3} for $\mathcal{P}'_{k+3}$.

Recursive Description of a cheating strategy S'_{k+3} given S'_k

- Rounds 1 to k: Alice performs the strategy S'_k to get outputs $\tilde{y}_1, \ldots, \tilde{y}_k$.
- Round $k+1$: Alice always outputs $\tilde{y}_{k+1} = 0$.
- Rounds $k+2$ and $k+3$: From round $k+2$, $\mathcal{A}_1$ and $\mathcal{A}_2$ both know $d, x_1, \ldots, x_k$. Let

$$\eta := d \prod_{j=1}^{k} x_j - \sum_{i=1}^{k} (\tilde{y}_i \prod_{j=i+1}^{k} x_j).$$

  $\mathcal{A}_{(k+2) \bmod 2}$ and $\mathcal{A}_{(k+3) \bmod 2}$ perform the optimal strategy for CHSH_Q on respective inputs x_{k+2} and x_{k+1} to get respective outputs a and b. Their outputs of the protocol are respectively $\tilde{y}_{k+2} = \eta \cdot a$ and $\tilde{y}_{k+3} = \eta \cdot b \cdot x_{k+3}$. Notice that if $\eta = 0$, which will correspond to the strategy S'_k succeeding to achieve $\mathcal{C}'_k$, Alice outputs $\tilde{y}_{k+2}, \tilde{y}_{k+3} = 0$ independently of a and b.

In the next section, we will prove the cheating probability achieved by this strategy, which will imply our main theorem.

3.3 Analysis

Lemma 3. *$\forall k \geq 2$, g'_k satisfies :*

$$1 - g'_{k+3}(S'_{k+3}) \leq (1 - \frac{1}{Q})\,(1 - \omega(\mathsf{CHSH_Q}))\,(1 - g'_k(S'_k)).$$

Proof. We consider ${\mathcal{P}'}_{k+3}$. Alice's winning condition ${\mathcal{C}'}_{k+3}$ is:

$$\sum_{i=1}^{k+3} \left(\tilde{y_i} \prod_{j=i+1}^{k+3} x_j \right) = d \prod_{j=1}^{k+3} x_j$$

or, by taking apart the last 3 terms :

$$\begin{array}{lll} & \tilde{y}_{k+3} & \\ + & x_{k+3} \cdot \tilde{y}_{k+2} & \\ + & x_{k+3} \cdot x_{k+2} \cdot \tilde{y}_{k+1} & \\ + & x_{k+3} \cdot x_{k+2} \cdot x_{k+1} \cdot \sum_{i=1}^{k} \left(\tilde{y_i} \prod_{j=i+1}^{k} x_j \right) & \\ = & x_{k+3} \cdot x_{k+2} \cdot x_{k+1} \cdot d \prod_{j=1}^{k} x_j & \end{array}$$

Recall that $\eta := d \prod_{j=1}^{k} x_j - \sum_{i=1}^{k} (\tilde{y_i} \prod_{j=i+1}^{k} x_j) \in \mathbb{F}_q$. Using η, we get :

$${\mathcal{C}'}_{k+3} \Leftrightarrow \tilde{y}_{k+3} + x_{k+3} \cdot \tilde{y}_{k+2} + x_{k+3} \cdot x_{k+2} \cdot \tilde{y}_{k+1} = x_{k+3} \cdot x_{k+2} \cdot x_{k+1} \cdot \eta$$

Recall from our protocol description that $\tilde{y}_{k+2} = \eta \cdot a$ and $\tilde{y}_{k+3} = \eta \cdot b \cdot x_{k+3}$, where a and b are the Alice's outputs of the CHSH_Q game. From there, we have

$$\begin{array}{lll} {\mathcal{C}'}_{k+3} & \Leftrightarrow & \tilde{y}_{k+3} + x_{k+3} \cdot \tilde{y}_{k+2} + x_{k+3} \cdot x_{k+2} \cdot \tilde{y}_{k+1} = x_{k+3} \cdot x_{k+2} \cdot x_{k+1} \cdot \eta \\ & \Leftrightarrow & x_{k+3} \cdot b \cdot \eta + x_{k+3} \cdot a \cdot \eta + 0 = x_{k+3} \cdot x_{k+2} \cdot x_{k+1} \cdot \eta \\ & \Leftrightarrow & \eta \cdot x_{k+3} \cdot (a + b - x_{k+1} \cdot x_{k+2}) = 0 \\ & \Leftrightarrow & (x_{k+3} = 0) \vee (\eta = 0) \vee (a + b = x_{k+1} \cdot x_{k+2}) \end{array}$$

These 3 events are independent as :

- $(x_{k+3} = 0)$ only depends on x_{k+3}, and happens with probability $\frac{1}{Q}$.
- $(\eta = 0)$ only depends on $d, x_1, ..., x_k$, and happens with probability $g'_k(S'_k)$.
- $(a + b = x_{k+1} \cdot x_{k+2})$ only depends on x_{k+1} and x_{k+2} ($\mathcal{A}_1$ and $\mathcal{A}_2$ optimally play the CHSH_Q game on inputs x_{k+1}, x_{k+2}, ignoring any unnecessary information). This happens therefore with probability $\omega(\mathsf{CHSH}_Q)$.

Thus, this particular strategy gives

$$g'_{k+3}(S'_{k+3}) = \Pr[{\mathcal{C}'}_{k+3}] = 1 - (1 - g'_k(S'_k))(1 - \frac{1}{Q})(1 - \omega(\mathsf{CHSH_Q}))$$

or equivalently

$$1 - g'_{k+3}(S'_{k+3}) \leq (1 - \frac{1}{Q})\,(1 - \omega(\mathsf{CHSH_Q}))\,(1 - g'_k(S'_k)).$$

■

We can now prove our main theorem

Theorem 2. *$\forall m \geq 3$, we have :*

$$g_m \geq 1 - \frac{1}{2}\left(\left(1 - \frac{1}{Q}\right)(1 - \omega(\mathsf{CHSH_Q}))\right)^{\lfloor \frac{m-1}{3} \rfloor}$$

Proof. By iterating the above lemma, we obtain

$$1 - g'_{3k}(S'_{3k}) \leq \left(\left(1 - \frac{1}{Q}\right)(1 - \omega(\mathsf{CHSH_Q}))\right)^{k-1}(1 - g'_3(S'_3))$$

Combining this with the initialization step $g'_3(S_3) \geq 1 - \frac{1}{2}(1 - \frac{1}{Q})(1 - \omega(\mathsf{CHSH}_Q))$ gives

$$g'_{3k} \geq g'_{3k}(S_{3k}) \geq 1 - \frac{1}{2}\left(\left(1 - \frac{1}{Q}\right)(1 - \omega(\mathsf{CHSH_Q}))\right)^{k}.$$

Using the symmetrization lemma (Lemma 2), we immediately get

$$g_{3k+1} \geq g'_{3k} \geq 1 - \frac{1}{2}\left(\left(1 - \frac{1}{Q}\right)(1 - \omega(\mathsf{CHSH_Q}))\right)^{k}.$$

If m can be written $m = 3k + 1$ for some k, we have

$$g_m \geq 1 - \frac{1}{2}\left(\left(1 - \frac{1}{Q}\right)(1 - \omega(\mathsf{CHSH_Q}))\right)^{\frac{m-1}{3}}$$

Since g_m is an increasing function, we have for all $m \geq 3$:

$$g_m \geq 1 - \frac{1}{2}\left(\left(1 - \frac{1}{Q}\right)(1 - \omega(\mathsf{CHSH_Q}))\right)^{\lfloor \frac{m-1}{3} \rfloor}$$

■

4 Generalization

In the previous part, we assumed that $\mathcal{A}_1$ and $\mathcal{A}_2$ can communicate efficiently, very efficiently, meaning that the propagation time ρ is 2 rounds. With such a propagation time, relativistic constraints ensure that at a given round k, Alice cannot use any information concerning the round $k-1$. However, we supposed that she knows everything about the rounds $k-2$ and before. Note that she obviously has access to the information of round $k-2$, because it occurs at the same place than round k.

What happens if $\mathcal{A}_1$ and $\mathcal{A}_2$ cannot reliably share their knowledge so fast? In this case, the propagation time ρ will be larger, and at any round k, Alice knows everything about rounds $1, 2, ..., k - \rho$ with . We use an even propagation time without loss of generality since computations rotate between two places, and Alice always knows what happened at rounds $k-2$, $k-4$, etc. In this situation, we will show that $\mathcal{A}_1$ and $\mathcal{A}_2$ cannot just play the CHSH_Q game. They will have to play the CHSH_Q^γ game, for some γ that will be specified later.

Another restriction that we do on the cheating players is that $\mathcal{A}_1$ and $\mathcal{A}_2$ may need some time to determine the bit d they want to decommit to. We call k_0 the round starting from which both $\mathcal{A}_1$ and $\mathcal{A}_2$ know if they try to reveal $d = 0$ or $d = 1$.

In this more practical setting, we propose the following recursive variant of our attack, for $k > k_0$, for any propagation time $\rho \geq 2$.

Recursive Description of a cheating strategy $S_{k+\rho+1}$ given S_k

- Rounds 1 to k: Alice performs the strategy S_k to get outputs $\tilde{y}_1, \ldots, \tilde{y}_k$.
- Rounds $k+1$ to $k+\rho-1$: Alice outputs $\tilde{y}_{k+1}, \ldots, \tilde{y}_{k+\rho-1} = 0$.
- Rounds $k+\rho$ and $k+\rho+1$: From round $k+\rho$, $\mathcal{A}_1$ and $\mathcal{A}_2$ both know $d, x_1, \ldots, x_k$. Let

$$\eta := d \prod_{j=1}^{k} x_j - \sum_{i=1}^{k} (\tilde{y}_i \prod_{j=i+1}^{k} x_j).$$

$\mathcal{A}_1$ also knows $X = \prod_{j \text{ odd} \,:\, k+1 \leq j \leq k+\rho} x_j$ and $\mathcal{A}_2$ knows $Y = \prod_{j \text{ even} \,:\, k+1 \leq j \leq k+\rho} x_j$. $\mathcal{A}_{(k+\rho) \bmod 2}$ and $\mathcal{A}_{(k+\rho+1) \bmod 2}$ perform the optimal strategy for CHSH_Q^γ with $\gamma := 1 - (1 - \frac{1}{Q})^{\frac{\rho}{2}}$ on respective inputs X and Y to get respective outputs a and b. Their outputs of the protocol are respectively $\tilde{y}_{k+\rho} = \eta \cdot a$ and $\tilde{y}_{k+\rho+1} = \eta \cdot b \cdot x_{k+\rho+1}$.

Lemma 4. *$\forall k \geq k_0$, we have*

$$g'_{k+\rho+1} \geq \left(1 - \frac{1}{Q}\right)(1 - \omega(\mathsf{CHSH_Q}))\, g'_k + 1 - \left(1 - \frac{1}{Q}\right)(1 - \omega(\mathsf{CHSH_Q}))$$

Proof. This demonstration will be similar to Lemma 3. We consider the cheating strategy described above. Alice's winning condition $\mathcal{C}'_{k+\rho+1}$ is:

$$\sum_{i=1}^{k+\rho+1} \left(\tilde{y}_i \prod_{j=i+1}^{k+\rho+1} x_j \right) = d \prod_{j=1}^{k+\rho+1} x_j$$

or, by separating the last $\rho+1$ terms :

$$\begin{array}{rl} & \tilde{y}_{k+\rho+1} \\ + & x_{k+\rho+1} \cdot \tilde{y}_{k+\rho} \\ + & 0 \\ \vdots & \\ + & 0 \\ + & \left(\prod_{j=k+1}^{k+\rho+1} x_j \right) \sum_{i=1}^{k} \left(\tilde{y}_i \prod_{j=i+1}^{k} x_j \right) \\ = & \left(\prod_{j=k+1}^{k+\rho+1} x_j \right) d \prod_{j=1}^{k} x_j \end{array}$$

Recall that $\eta := d \prod_{j=1}^{k} x_j - \sum_{i=1}^{k} (\tilde{y}_i \prod_{j=i+1}^{k} x_j)$, which allows to simplify $\mathcal{C}'_{k+\rho+1}$ as follows

$$\begin{aligned} \mathcal{C}'_{k+\rho+1} &\Leftrightarrow \tilde{y}_{k+\rho+1} + x_{k+\rho+1} \cdot \tilde{y}_{k+\rho} = \left(\prod_{j=k+1}^{k+\rho+1} x_j \right) \cdot \eta \\ &\Leftrightarrow \tilde{y}_{k+\rho+1} + x_{k+\rho+1} \cdot \tilde{y}_{k+\rho} = X \cdot Y \cdot \eta. \end{aligned}$$

In her cheating strategy, Alice answers $\tilde{y}_{k+\rho} = a \cdot \eta$ and $\tilde{y}_{k+\rho+1} = x_{k+\rho+1} \cdot b \cdot \eta$, where a and b are the Alices' answers when playing the CHSH_Q^γ game, on inputs X and Y. Thus

$$\mathcal{C}'_{k+\rho+1} \Leftrightarrow (x_{k+\rho+1} = 0) \vee (\eta = 0) \vee (a + b = XY)$$

These three events are independent. The first one occurs with probability $\frac{1}{Q}$, the second one with probability g'_k. For the third one, notice that X is a product of $\frac{\rho}{2}$ uniformly random number in $\mathbb{F}_Q$. Therefore, we have $\Pr[X = 0] = 1-(1-\frac{1}{Q})^{\frac{\rho}{2}} = \gamma$ and for any $z \in \mathbb{F}_Q^*$, $\Pr[X = z] = \frac{1-\gamma}{Q-1}$. Y satisfies the same probability distribution. Therefore, $\Pr[a + b = XY]$ is exactly the probability of winning the CHSH_Q^γ game using its optimal strategy.

This gives :

$$g'_{k+\rho+1} \geq 1 - \left(1 - \frac{1}{Q}\right)(1 - g'_k)\left(1 - \omega(\mathsf{CHSH}_Q^\gamma)\right)$$

Then using Lemma 1 :

$$g'_{k+\rho+1} \geq 1 - \left(1 - \frac{1}{Q}\right)(1 - g'_k)(1 - \omega(\mathsf{CHSH}_Q))$$

i.e.

$$g'_{k+\rho+1} \geq \left(1 - \frac{1}{Q}\right)(1 - \omega(\mathsf{CHSH}_Q))\, g'_k + 1 - \left(1 - \frac{1}{Q}\right)(1 - \omega(\mathsf{CHSH}_Q))$$

■

Theorem 3. *For any $k_0 \geq 1$ and $\rho \geq 2$, for any $m \geq k_0 + \rho + 1$, we have*

$$g_m \geq 1 - \frac{1}{2}\left((1 - \frac{1}{Q})(1 - \omega(\mathsf{CHSH}_\mathsf{Q}))\right)^{\frac{m-k_0-1}{\rho+1}}$$

Proof. We use the recursive inequality from Lemma 4, and the trivial initialization $g'_{k_0} \geq \frac{1}{2}$. This gives us $\forall k \geq k_0$, we have

$$g'_{k_0+k(\rho+1)} \geq 1 - \frac{1}{2}\left((1 - \frac{1}{Q})(1 - \omega(\mathsf{CHSH}_\mathsf{Q}))\right)^k,$$

and by using Lemma 2

$$g_{k_0+k(\rho+1)+1} \geq 1 - \frac{1}{2}\left((1 - \frac{1}{Q})(1 - \omega(\mathsf{CHSH}_\mathsf{Q}))\right)^k.$$

If m can be written $m = k_0 + k(\rho + 1) + 1$, we have $k = \frac{m-k_0-1}{\rho+1}$ and

$$g_m \geq 1 - \frac{1}{2}\left((1 - \frac{1}{Q})(1 - \omega(\mathsf{CHSH}_\mathsf{Q}))\right)^{\frac{m-k_0-1}{\rho+1}}.$$

In order, to conclude, notice that g_m is an increasing function in m. We can therefore conclude that

$$g_m \geq 1 - \frac{1}{2}\left((1 - \frac{1}{Q})(1 - \omega(\mathsf{CHSH}_\mathsf{Q}))\right)^{\lfloor\frac{m-k_0-1}{\rho+1}\rfloor}.$$

■

References

[BB84] Bennett and Brassard. Quantum cryptography: Public key distribution and coin tossing. in Proc. Of IEEE Inter. Conf. on Computer Systems and Signal Processing, Bangalore, Kartarna, (Institute of Electrical and Electronics Engineers, New York, 1984.

[BCF+14] Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, and Christian Schaffner. Position-based quantum cryptography: Impossibility and constructions. *SIAM Journal on Computing*, 43(1):150–178, 2014.

[BM05] Harry Buhrman and Serge Massar. Causality and tsirelson's bounds. *Physical Review A*, 72(5):052103, 2005.

[BOGKW88] Michael Ben-Or, Shafi Goldwasser, Joe Kilian, and Avi Wigderson. Multi-prover interactive proofs: How to remove intractability assumptions. In *Proceedings of the twentieth annual ACM symposium on Theory of computing*, pages 113–131. ACM, 1988.

[BS15] Mohammad Bavarian and Peter W. Shor. Information causality, szemerédi-trotter and algebraic variants of CHSH. In *Proceedings of the 2015 Conference on Innovations in Theoretical Computer Science, ITCS 2015, Rehovot, Israel, January 11-13, 2015*, pages 123–132, 2015.

[CCL15] Kaushik Chakraborty, André Chailloux, and Anthony Leverrier. Arbitrarily long relativistic bit commitment. *Phys. Rev. Lett.*, 115:250501, Dec 2015.

[CGMO09] Nishanth Chandran, Vipul Goyal, Ryan Moriarty, and Rafail Ostrovsky. Position based cryptography. In *Advances in Cryptology-CRYPTO 2009*, pages 391–407. Springer, 2009.

[CSST11] Claude Crépeau, Louis Salvail, Jean-Raymond Simard, and Alain Tapp. Two provers in isolation. In *Advances in Cryptology–ASIACRYPT 2011*, pages 407–430. Springer, 2011.

[FF16] Serge Fehr and Max Fillinger. On the composition of two-prover commitments, and applications to multi-round relativistic commitments. In *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part II*, pages 477–496, 2016.

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

[Ken05] Adrian Kent. Secure classical bit commitment using fixed capacity communication channels. *Journal of Cryptology*, 18(4):313–335, 2005.

[Ken11] Adrian Kent. Unconditionally secure bit commitment with flying qudits. *New Journal of Physics*, 13(11):113015, 2011.

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

[KLH+15] Boris Korzh, Charles Ci Wen Lim, Raphael Houlmann, Nicolas Gisin, Ming Jun Li, Daniel Nolan, Bruno Sanguinetti, Rob Thew, and Hugo Zbinden. Provably secure and practical quantum key distribution over 307 km of optical fibre. *Nature Photonics*, 2015.

[KMS11] Adrian Kent, William J. Munro, and Timothy P. Spiller. Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints. *Phys. Rev. A*, 84:012326, Jul 2011.

[KTHW13] Jed Kaniewski, Marco Tomamichel, Esther Hanggi, and Stephanie Wehner. Secure bit commitment from relativistic constraints. *Information Theory, IEEE Transactions on*, 59(7):4687–4699, 2013.

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

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

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

[LL11] Hoi-Kwan Lau and Hoi-Kwong Lo. Insecurity of position-based quantum-cryptography protocols against entanglement attacks. *Physical Review A*, 83(1):012322, 2011.

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

[PP16] Matej Pivoluska and Martin Plesch. An explicit classical strategy for winning a CHSH_q game. *New Journal of Physics*, 18(2):025013, 2016.

[PPP16] Matej Pivoluska, Marcin Pawlowski, and Martin Plesch. Experimentally secure relativistic bit commitment. *arXiv preprint quant-ph:1601.08095*, 2016.

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, February 1978.

[Sim07] Jean-Raymond Simard. Classical and quantum strategies for bit commitment schemes in the two-prover model. Master's thesis, McGill University, 2007.

[Unr14] Dominique Unruh. Quantum position verification in the random oracle model. In *Advances in Cryptology–CRYPTO 2014*, pages 1–18. Springer Berlin Heidelberg, 2014.

[VMH+16] E. Verbanis, A. Martin, R. Houlmann, G. Boso, F. Bussières, and H. Zbinden. 24-hour relativistic bit commitment. *arXiv preprint arXiv:1605.07442*, 2016.