Non-local Games with a Promise

Nicolas Courtemanche, School of Computer Science

McGill University, Montreal

April, 2024

A thesis submitted to McGill University in partial fulfillment of the requirements of the degree of

Master of Computer Science

Abstract

Nonlocal games are a type of protocol commonly used for the study of nonlocality. Many protocols devised to be resistant against quantum adversaries use this model. The study of nonlocality has also uncovered a theoretical but powerful resource, supra-quantum no-signaling channels, which can also be used in nonlocal games. As attempts are made to create secure protocols against these theoretical no-signalling channels, a framework in which they can be defined mathematically has also been established. In this work, we explore a new way of defining the distribution of inputs of nonlocal games which uses multi-prover interactive proofs as their underlying structure. We introduce the notion of promises, meaning that we change the probability of occurrence of certain inputs and observe the changes in potential real-world security of our protocol following those changes. We will show how the importance of this notion has appeared to us as we studied nonlocal games involving no-signalling channels. We use as our main example a 3-prover bit commitment protocol from a paper by S. Fehr and M.J. Fillinger to illustrate the impact that the application of a promise on the protocol's inputs would have on its security, reducing it from no-signalling-resistant to quantum-resistant. We conclude our work by presenting a reworked security model of nonlocal games which allows for promises on games and channels, and show the impact it may have on the security of these games.

Abrégé

Les jeux non locaux sont un type de protocole couramment utilisé pour l'étude de la non-localité. De nombreux protocoles conçus pour résister aux adversaires quantiques utilisent ce modèle. L'étude de la non-localité a également mis au jour une ressource théorique mais puissante, les canaux supra-quantiques non-signalants, qui peuvent également être utilisés dans les jeux non locaux. Alors que des tentatives sont faites pour créer des protocoles sécurisés contre ces canaux théoriques non-signalants, un cadre dans lequel ils peuvent être définis mathématiquement a également été établi. Dans ce travail, nous explorons une nouvelle façon de définir la distribution des entrées de jeux non-locaux qui utilisent des preuves interactives multi-prouveurs comme structure sous-jacente. Nous introduisons la notion de promesses, ce qui signifie que nous modifions la probabilité d'occurrence de certaines entrées et observons les changements dans la sécurité potentielle réelle de notre protocole suite à ces changements. Nous montrerons comment l'importance de cette notion nous est apparue dans l'étude des jeux non-locaux impliquant des canaux non-signalants. Nous utilisons comme exemple principal un protocole de mise en gage de bits à 3 prouveurs issu d'un article de S. Fehr et M.J. Fillinger pour illustrer l'impact qu'aurait l'application d'une promesse sur les entrées du protocole sur sa sécurité le réduisant d'une résistance au non-signalant à une résistant au quantique. Nous concluons notre travail en présentant un modèle de sécurité retravaillé des jeux non-locaux qui permet des promesses sur les jeux et les canaux, et montrons l'impact qu'il peut avoir sur la sécurité de ces jeux.

Acknowledgements

Je voudrais remercier mon superviseur, Claude Crépeau, pour son support indéfectible et son conseil tout au long de mon parcours dans le domaine de la cryptographie et dans ma maîtrise. Un homme passionné et d'une grande humanité.

Je voudrais aussi remercier ma famille et mes amis pour leur soutien moral durant mes études, grâce à qui la balance de ma vie durant cette période est restée en équilibre.

The author would like to acknowledge the cooperation of Serge Fehr in the aid given in analyzing his and his student M.J. Fillinger's bit-commitment protocol and conversations on the inclusion of promises in no-signalling definitions.

Table of Contents

List of Figures

Chapter 1

Introduction

Nonlocal games are an important type of protocol in the field of cryptography, on which are based many modern security systems. Often used for the study of nonlocality, they are a type of multi-player game containing a referee, as well as players which will try and bolster the level of correlation of their answers using an information-theoretic tool commonly known as *nonlocal channels*. Such channels can feature quantum entangled systems of particles, for example, to make quantum channels. The relevance of the study of such games is accrued by recent developments in quantum computers, for one, as it is known that certain quantum-enabled protocols such as the well known Shor's algorithm [Sho97] can break parts of our modern cryptographic ecosystem. Nonlocal games can lead to, among other things, quantum-resistant cryptographic protocols.

The study of nonlocality has also uncovered another theoretical but powerful resource: supra-quantum no-signalling channels. These channels, which can also be used in nonlocal games, could be even more powerful than quantum channels if successfully implemented in the real world. This gives us a clear motivation to study these channels and, similarly to quantum channels, attempt to ward our cryptographic protocols against them.

With quantum channels only being slowly implemented and no-signalling channels not being implemented yet tough, the mathematical and general framework in which these chan-

nels operate in different contexts such as nonlocal games is not fully fleshed-out. Many concepts related to them are still rigid and lack generality.

Bit commitment schemes are a particular cryptographic primitive which allows the committing to a particular binary (bit) value during a protocol, which is to later be revealed but must also be unchanged during this period of time. Many modern bit commitment protocols are wrought using a particular protocol basis called *Multi-Prover Interactive Proof*, or MIP for short. This type of proof functions similarly to the prisoner's dilemma, where two or more prisoners are interrogated while being kept apart to check the consistency of their alibis. An MIP can be elevated to a nonlocal game by giving the provers (the prisoners in the example) nonlocal channels.

This is one way of creating bit-commitment schemes secure against quantum channels-equipped players. No-signalling-resistant bit-commitment schemes however have not yet been successfully designed.

In [FF15] in 2015 was initially introduced and in [FF19] in 2019 was presented the final version of a 3-prover MIP bit commitment scheme which was in these works claimed to be resistant to no-signalling by their authors, Max Fillinger and Serge Fehr. Examining this protocol, we found what we thought to be an issue. The bit commitment could only happen when the inputs of two of the players were the same. In the protocol's context, it meant that they were revealing the same bit, so naturally it should be the case that they are the same value. The scheme, though, needed the fact that technically the bits don't have to be the same in order to preserve its security against no-signalling opponents.

This led us to propose a new notion for nonlocal games: **promises.** Our analysis revealed that when enacting the aforementioned promise on the inputs of the protocol, its security actually dropped from no-signalling resistant to quantum-resistant.

In this work, we will demonstrate the impact the promises not only on the inputs of games but also on the inputs of channel can have on the overall security considerations of nonlocal games. We will present a new security model for nonlocal games and argue that the

traditional model is too rigid, and forbids looking at scenarios that may accurately represent the behavior of no-signalling channels as well as channels in general.

Chapter 2

Cryptographic background

We split the literature review in two chapter. In each chapters we will progressively build up the knowledge required to tackle our main work and findings.

In this first chapter, we will start with the cryptography-related concepts related to our work.

2.1 Multi-Prover Interactive Proofs (MIP)

At the core of the scenarios we present later is the fact that these protocols are to be implemented using Multi-Prover Interactive Proofs (MIP). Such a proof is an interaction between a polynomial time-bounded verifier, to whom the proof is presented, and two or more computationally unbounded provers, which attempt to convince the verifier that they have a valid proof of a statement. This model draws its origins from [BOGKW88]. This system functions in a way similar to the commonly known "Prisoners' Dilemma", in which two prisoners are separated by their interrogators in an attempt to check their alibis for consistency flaws.

The verifier, which can be a single entity or multiple ones, each interrogating their own set of provers, will ask questions to the provers in an attempt to either accept their proof or

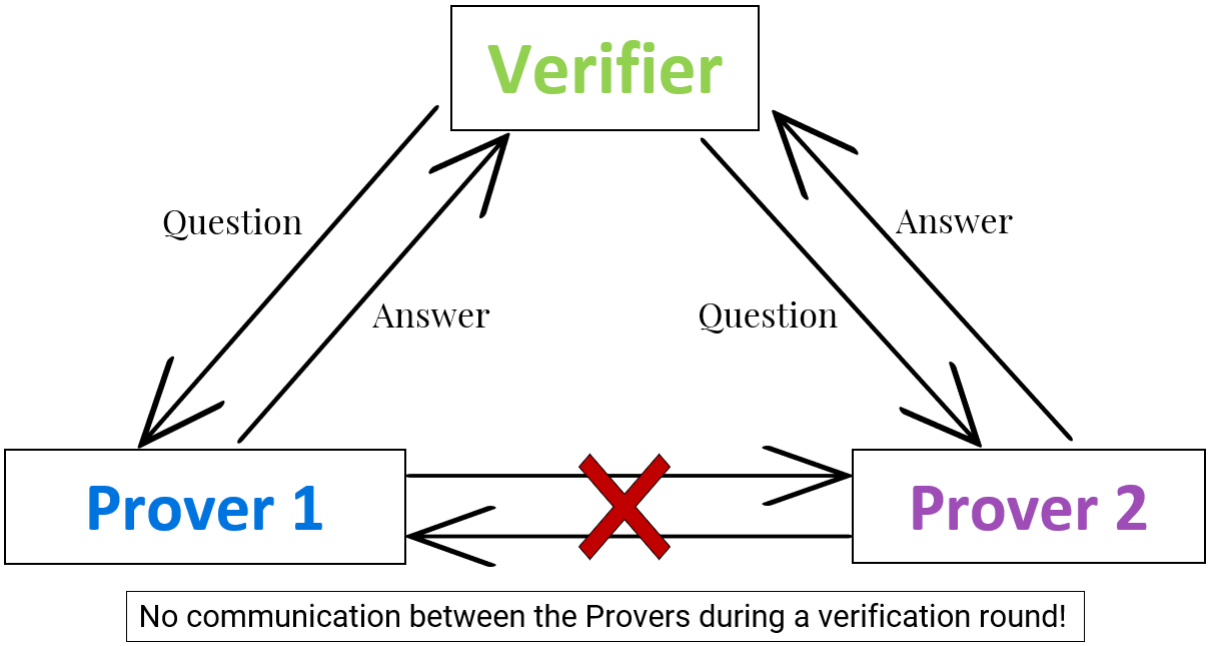

Figure 2.1: A simplified representation of an MIP with two provers and a verifier.

find a flaw in it and reject it. These questions can be the same for all provers or different ones, depending on the protocol.

Formally,

Definition 2.1.1 (Multi-Prover Interactive Proof)**.** *Let L be a language and x be an element of this language. Let V be the verifier and $P_1, ..., P_n$ the provers of an n-prover MIP. Through their interaction with the verifier, the provers will attempt to demonstrate that $x \in L$. This is done by the verifier asking provers questions to which they must answer according to rules agreed upon by all participants. The verification can be done over multiple rounds, in between which there is no formal requirement for the behavior of the provers or the verifier. The verifier V should output Accept if it is convinced that $x \in L$ and Reject otherwise.*

Of course, this kind of protocol relies on the fact that the provers are separated in a way that they cannot communicate any information. We will formalize this notion later, and name the act of communicating any amount of information "signalling".

2.1.1 The proof: soundness and completeness

The proof given by the provers of the MIP may not always be correct, but they will try and pass it as a valid proof regardless. In the MIP, there are two notions which are crucial to the understanding of the security of the protocol. The first notion is **completeness**. This is the probability that the verifier will reject a valid solution.

Definition 2.1.2 (completeness)**.** *Let L be the language and x an element of this language. Then we say the language is complete if*

$$P(V \ \textit{Accepts} \ | x \in L) = 1 \tag{2.1.1}$$

where V is the verifier. In practice though, we would rather define the notion of ϵ-completeness, where we want V to accept if $x \in L$ except with some small probability ϵ which can be made arbitrarily small, thus

$$\forall \epsilon > 0, \ P(V \ \textit{Accepts} \ | x \in L) \geq 1 - \epsilon. \tag{2.1.2}$$

Twin to this notion is that of **soundness**. This is the probability that the verifier will accept a solution when it is false. In the context of nonlocal games, which we will explore further on, the players can increase the level of correlation of their answers, potentially decreasing the soundness of the game. Therefore, we define the soundness of a game in relationship to its level of nonlocality.

Definition 2.1.3 (soundness)**.** *Let L the language and x not an element of this language. The soundness is then defined, if S_P is the set of all possible provers within a nonlocality level and the MIP is an n-prover protocol, as*

$$\max_{p_i \in S_P} P(V \ \textit{Accepts} \ | V \ \textit{interacted with} \ p_i \ \textit{and} \ x \notin L). \tag{2.1.3}$$

Similarly as for completeness, we define ϵ-soundness where we want the V to accept if $x \notin L$ only with some small probability ϵ which can be made arbitrarily small, thus

$$\forall \epsilon > 0, \ \max_{p_i \in S_P} P(V \ \textit{Accepts} \ | V \ \textit{interacted with} \ p_i \ \textit{and} \ x \notin L) < \epsilon. \tag{2.1.4}$$

2.2 Relativistic protocols

Different ways can be used to prevent signalling between provers, but the most common ones are simply to either separate them far enough in space or reduce the amount of time they have to answer the questions. This means that they must answer before information from another prover can get to them during a round of verification, assuming information will travel no faster than the speed of light. We call such protocols "relativistic". A protocol can have a single or multiple rounds. Multiple rounds are usually favored as it allows a relaxation of security in exchange for repeating the protocol multiple times, over which the chance of successfully cheating every time is low, which could reduce, for example, the amount of data that needs to be sent overall. But that is not the only advantage. The more information that needs to be sent within a round between the prover and the verifier, the bigger the spatial separation needs to be between the provers. This is because while the prover and the verifier are having a "conversation", the prover can send information to another prover. Spatial separation can only be so great in practical settings, so at some point, the round must end.

2.3 Gaining security through repetition

In the previous section we mentioned that we could repeat verification rounds sequentially instead of creating extremely tight security conditions within a single round. One motivation of this is the fact that to create very tight security conditions, there must always be a trade-off. Most often this will be resulting in a very big quantity of communication. As we saw in the previous section, this is not desirable for relativistic protocols because it means that

the spatial separation will be greater. We will show that we can nevertheless achieve a high protocol security by repeating rounds, we will use the notion of **soundness** defined previously.

Theorem 2.3.1. *The soundness of a multi-round protocol can be made arbitrarily low unless it is 1.*

Proof. Recall from definition 2.1.3 that soundness is the probability that the protocol will accept a solution when it is false. Let S be an upper bound on the soundness of the protocol, a value between 0 and 1, then after n rounds of repetition it will have an overall soundness bounded by $(S)^n$, representing the provers' chances of winning after n rounds. Unless the soundness is 1, it can be decreased to an arbitrarily low value. □

The security of the protocol can therefore be ensured by balancing the amount of information sent and the number of rounds played.

Chapter 3

Information-Theoretic Background

In this second part of our literature review, we examine concepts from information theory which, when combined with the cryptography knowledge from earlier, will give us all the requirements to delve into nonlocal games.

3.1 Channels

Given the previously established cryptographic background, we can now name the tool that will be of greatest importance in the context of nonlocal games: channels. In our context, we will mostly observe **bidirectional channels**.

Definition 3.1.1 (Channel)**.** *A channel is the link that maps an input to an output. These channels:*

- *Have a* ***distribution*** *of outputs given their inputs. In a bidirectional channel with the inputs being x, y and the outputs being a, b, we can write the distribution as $P(a, b|x, y)$.*
- *The level of* ***correlation*** *of the outputs determines the level of correlation of the channel itself.*

- *In the context of nonlocal games, we will refer to the level of correlation as the level of '**nonlocality**'. Later we will define this concept, as well as a scale on which nonlocality can be measured.*

3.1.1 Channels in the context of nonlocal games and MIPs

In the context of an MIP, these characteristics take greater meanings. When the MIP is the format used for a nonlocal game, a game where nonlocal resources are used, the provers are never allowed to communicate, but that does not rule out the possibility of them having access to a channel that does not permit signalling (communicating).

In these channels the players can input the input they received from the verifier and will give the output of the channel to the verifier. When there are operations to be done on the channel's output before transmitting it to the verifier, we simply "add" these operations to the channel. The channel will therefore represent the entirety of the provers' operations on the inputs they are given by the verifier before giving the result to the verifier.

At this end, we refer to the questions asked by the verifier as the **inputs** to the channel and the answers from the provers as the **outputs**. The **distribution** in this case will be the conditional joint distribution of the outputs given the inputs.

We can now come back to the level of correlation of channels. Referring back to the example of the Prisoners' Dilemma, it is intuitive enough to see that the classical prisoners, when separated, will have no way of correlating their answers else than some predefined strategy, to which they both agree upon, as well as some shared randomness. The players can increase their level of correlation by using certain resources as black boxes. Those resources, in a general sense, are what we refer to when using the term **channel**. This means that we will consider the resource as taking in inputs and returning the provers some outputs according to a certain distribution, while not considering the mechanisms inside the box. We will define concrete examples of such resources later on.

3.2 Bell's Inequalities

We will take a brief tangent to explain a tool that is crucial in the understanding of nonlocality. The Bell inequalities are a tool devised by John Bell in 1964 [Bel64] to test the theory of locality. In essence, they are inequalities composed of the average results of measurements of an experiment of classical random states or quantum states. On average, the value on one side of the equality must be smaller or equal to different threshold values to determine its nonlocality level. Given that quantum experiments violate the first threshold, the one determining whether or not the experiment is local, Bell deducted that quantum theory is incompatible with the local theory, and therefore such a theory must be incomplete in a general sense, or else it would be respected in all contexts.

In our context, these inequalities are applied to measure more than the simple first threshold violation of locality. Indeed, theoretically, there is a maximal violation of the inequalities by quantum experiment (this is obtained from maximally entangled states). However, this threshold is smaller than the global maximal theoretical violation of Bell's inequalities. From this, we deduct that there are multiple classes of nonlocality and that it is not a binary classification.

Let us give some concrete examples. The most commonly used inequality from Bell's Theorem is the CHSH inequality. While its derivation is out of the scope of this document, the reader can find it in [CH74]. This inequality is written in the form

$$|\langle A_0 B_0\rangle + \langle A_0 B_1\rangle + \langle A_1 B_0\rangle - \langle A_1 B_1\rangle| \leq 2 \tag{3.2.1}$$

representing the joint expectation values of the measurements of each observable A_n and B_m. When the values are classical and therefore have no quantum properties, these are simply the joint expected values, and therefore can be each rewritten as

$$\langle A_n B_m\rangle = \sum_{a,b=\pm 1} a \cdot b \cdot P(a,b|A_n,B_m) \tag{3.2.2}$$

with a, b being the potential results of those measurements written in the ± 1 binary form. Let us demonstrate the inequality for every nonlocality level. We will again use the binary values -1 or 1, converting 0-valued bits to -1 for the purpose of this calculation when necessary. To start with the local level, let us consider the CHSH game [CH74]. In this game, Alice and Bob are given a bit x and y. They must answer with their own bits a and b such that $a \oplus b = x \wedge y$. The optimal classical strategy for this game [BCP$^+$14] is simply for both of them to answer with the same bits, $a = b$, all the time. They will have 75% chance of winning regardless of their choice of bit. If the chosen output bits are always $a = b = 0$, for example, every part of the inequality will therefore be equal to

$$\sum_{a,b=\pm 1} -1 \cdot -1 \cdot P(0,0|A_n, B_m) = (-1 \cdot -1) \cdot 1 = 1$$

and the inequality becomes

$$|1 + 1 + 1 - 1| \leq 2 \iff 2 \leq 2.$$

As we can see, the local bound of 2 is respected.

For an example for a quantum state and its maximal violation of the inequality, we refer the reader to [BCP$^+$14] as well as [Cir80], as the derivation involve calculations that are beyond the scope of this work. We can observe that the quantum maximal violation is of $2\sqrt{2}$.

Finally, we have the supra-quantum no-signalling case, the name given to nonlocal correlation which violate the quantum bound can nevertheless still not be used to signal information. The complete 2-player no-signalling channel is called the PR-box [PR94]. This channel allows players to win the CHSH game. We will therefore simply look at the violation from having the perfect answer to the CHSH game, as defined before. The following table 3.1 contains the pairs of input value, their multiplication modulo 2 (equivalent to AND) and therefore which pairs of output could have an equivalent XOR, and finally their translation to CHSH binary notation (+1,-1).

Input values (x, y)	Multiplication mod 2	Possible outputs (a, b)	Outputs in $(+1, -1)$ notation
(0,0)	$0 \cdot 0 = 0$	(0,0), (1,1)	$(-1,-1), (1,1)$
(0,1)	$0 \cdot 1 = 0$	(0,0), (1,1)	$(-1,-1), (1,1)$
(1,0)	$1 \cdot 0 = 0$	(0,0), (1,1)	$(-1,-1), (1,1)$
(1,1)	$1 \cdot 1 = 1$	(1,0), (0,1)	$(1,-1), (-1,1)$

Figure 3.1: The possible outputs for the PR-box as inputs for the CHSH inequality.

Plugging each of these values in equation 3.2.2 and in turn in equation 3.2.1 we get the following violated inequality:

$$|\frac{(-1 \cdot -1) + (1 \cdot 1)}{2} + \frac{(-1 \cdot -1) + (1 \cdot 1)}{2} + \frac{(-1 \cdot -1) + (1 \cdot 1)}{2} - \frac{(1 \cdot -1) + (-1 \cdot 1)}{2}| \leq 2$$

On the left hand side we obtain the maximum algebraic value of the CHSH inequality, 4, achievable by a no-signalling channel.

3.3 Nonlocality

Nonlocality describes how correlated a certain joint distribution is, using the reference point of a classically correlated channel's joint distribution. We refer to a distribution that can be achieved through classical operations and local strategies as "local". More precisely, a channel that is local has no interaction between the parties' inputs. It can be achieved by both parties by simply applying a function as well as shared randomness to their respective inputs.

Definition 3.3.1 (Local Channel)**.** *For a two-party channel with the parties' inputs being x, y and their outputs being a, b, as well as shared randomness r, the channel's action on the inputs is fully defined by the simple functions $a = f(x, r)$ and $b = f'(y, r)$.*

In the following nonlocality hierarchy from figure 3.2, this is the **LHV** level, referring to the complete name **local hidden variable**. It is also sometimes simply referred to as **LOC**.

We define the nonlocality of a strategy, and sometimes the provers themselves, by the nonlocality of the channels they can use. The figure 3.2 shows the current state of the non-local hierarchy.

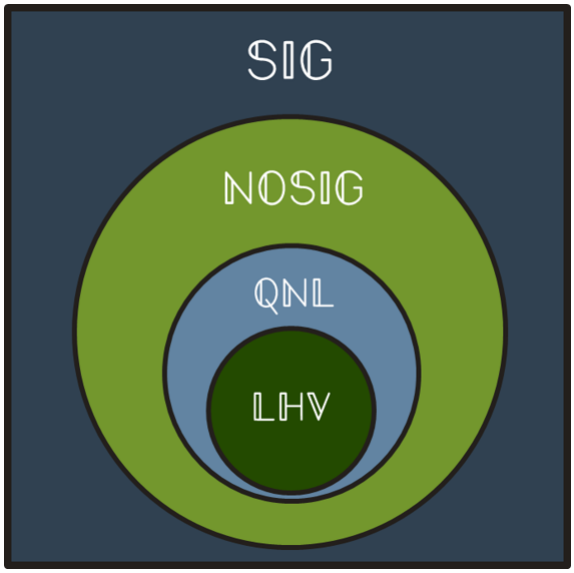

Figure 3.2: The current state of the nonlocal hierarchy.

Using, for example, a pair of entangled particles, we can achieve a level of correlation between the provers that cannot be achieved through local means.

Definition 3.3.2 (Quantum Channel)**.** *A quantum channel is created by having an entangled system of particles shared between parties. The parties can use POVMs on their side of the entangled system and the result of such a measurement is considered to be the party's output of the channel.*

In the nonlocality hierarchy from figure 3.2, this is the **QNL** level, meaning quantum nonlocality. Every channel that can be made through local means can also be made using quantum means [BCP$^+$14].

In certain cases, such as the magic square game [BBT05], this can drastically improve the winning probability to certain games.

Pushing further, we also examine correlations which are signalling (**SIG**), and opposed to this, those which are no-signalling (**NOSIG** or **NS**). Given that the maximal theoretical violation of Bell's inequalities is only found in theory and has no implementation in practice, we cannot give concrete examples of no-signalling channels. There exist, though, theoretical NS channels, such as the PR-box, which we have seen in the previous section. Signalling channels, in turn, are simply channels through which information can be communicated. We will define this rigorously in the following section.

3.4 Signalling and No-Signalling

As we can see in the previous nonlocality hierarchy diagram, we have nonlocality levels which go higher than quantum. One of these, the topmost level, is "Signalling".

3.4.1 What does it mean to signal?

To signal through a channel, there must be an effect to the joint distribution when changing one of the inputs. Intuitively, this simply means that by sending different inputs, the receiving party will be able to distinguish different outputs. Let us formalise this using definitions from [CC21].

Definition 3.4.1 (Signalling Channel)**.** *In a two-party channel with values that are not restricted to binary, with inputs* $\{x_0, x_1\}$ *and outputs* $\{a_0, a_1\}$ *where the indices 0 and 1 are used to differentiate the input/output pairs, i.e. to differentiate the players, this means*

$$\exists i \in \{0,1\}, a_i, x_i, x_{\bar{\imath},0}, x_{\bar{\imath},1}, \quad \Pr(a_i|x_i, x_{\bar{\imath},0}) \neq \Pr(a_i|x_i, x_{\bar{\imath},1}). \tag{3.4.1}$$

If player $\bar{\imath}$ wants to communicate bit b, they may input $x_{\bar{\imath},b}$ while the other player inputs x_i. Repeating this operation will clearly define which output distribution is being received by player i. What does it mean not to signal then?

Definition 3.4.2 (No-Signalling)**.** *In a two-party distribution again with values unrestricted to binary, inputs* $\{x_0, x_1\}$ *and outputs* $\{a_0, a_1\}$ *where the indices 0 and 1 are used to differentiate the input/output pairs, i.e. to differentiate the players, this is described as*

$$\forall i \in \{0,1\}, a_i, x_i, x_{\bar{\imath},0}, x_{\bar{\imath},1}, \quad \Pr(a_i|x_i, x_{\bar{\imath},0}) = \Pr(a_i|x_i, x_{\bar{\imath},1}). \tag{3.4.2}$$

It is also important to note that the definition of signalling above is that of **one-way signalling**, specifically from player $\bar{\imath}$ to player i. We say a channel is signalling when it signals in at least one direction, but it can also signal in both directions.

Simply put, a correlation is of nonlocality "No-Signalling" when varying a player's input has no effect upon the distribution of the other player's outputs, for each of the former player's inputs. This means that that no information can be transmitted through this channel. Breaking this definition, the provers using a channel like this could transmit information and therefore signal, or communicate.

3.4.2 n-Player Signalling

We will now define what it means to signal in a setting where there is more than two players. Previously we had restricted ourselves to two players. This definition will still useful.

Definition 3.4.3 (n-Player Signalling)**.** *We say that a n-player channel is* ***signalling*** *if we can apply the 2-player definition of signalling between two different subsets of the n players.*

Definition 3.4.4 (n-Player No-Signalling)**.** *We say that a n-player channel is* ***no-signalling*** *definition 3.4.3 is not satisfied.*

Chapter 4

Games and Promises

4.1 Defining games

Now that we have defined the various tools required from the cryptographic and information-theoretic background, we can group them together in the context that will be used throughout the following sections: games. These will follow the intuition of a game while being much more rigorous in their definition. Informally, a game will have inputs *given to* the players, output *from* the players, and a predicate which takes the inputs and outputs and deterministically decides if the players have won or lost. Finally, the game will also have a probability distribution for its inputs. The game can have two or more players, but always at least two, because they are games of *correlation*, and we will refer to them most often as **nonlocal games**.

4.2 Promises on the inputs

There are instances in which a channel may not have all its inputs be used in the context of a game. We call it a "promise" as we promise not to use certain inputs in the context of a game or some other context. As we will show in the examples following this section, under promises the nonlocality of a channel can decrease. The same idea can be applied to games

and the inputs of a game, and since games can be played using certain channels available to the players, a promise on a game will also affect the inputs of the channels used to play the game.

This is well known intuitively: if two players decide to play a game of chess with only half the pieces, they will only look at what they are able to achieve with the remaining pieces, and not tarry about the excluded pieces. In the world of information-theoretic games, though, this is not as well defined. In fact, there is no formal definition of a promise, and in some instances its existence is implied by the authors, and in others, its existence is ignored. In this work, we set out to show how crucial this can be, how to define it in a way that follows the intuition and basic premises of games, as well show examples of its use.

When we apply a promise to our general game, we will restrict the input set to a smaller input set by removing certain inputs. When we say remove, we mean reducing their probability to zero.

4.3 Formal definition of games and promises

Definition 4.3.1 (n-party game $\boldsymbol{G}$)**.** Formally, we define a general n-party game $\boldsymbol{G}$ as

$$G = \{U \subseteq X = (X_1 \times ... \times X_n), A = (A_1 \times ... \times A_n), P(x_1, ..., x_n), V(x_1, ..., x_n, a_1, ..., a_n)\}$$

- $(x_1, ..., x_n) \in U$ **are the elements of the input set**, as the inputs are tuples of two or more values. But we also note that $U \subseteq X = (X_1 \times ... \times X_n)$ where X is the complete set of inputs and the X_i are finite sets. We do this to allow promises on the original input set X, as we want the game to be as general as possible. If there are no promises on X, then $U = X$. This corresponds to the standard definition of nonlocal games.

- $(a_1, ..., a_n) \in A$ **are the elements of the output set** of the game. The A_i are finite sets.

- $V(x_1, ..., x_n, a_1, ..., a_n)$ **is the predicate** determining the outcome of the game and is defined as a function $V : U \times A \to \{0, 1\}$.

- $P(x_1, ..., x_n)$ **is the probability function** that defines the probability for all tuples of inputs, itself defined as $P : U \to [0, 1]$ and has the property that $\sum_{(x_1,...,x_n)\in U} P(x_1, ..., x_n) = 1$.

Definition 4.3.2 (local, quantum, no-signalling or signalling game)**.** We say that a game is **local**, **quantum**, **no-signalling** or **signalling** if it can be won with probability 1 using channels no stronger than *local*, *quantum*, *no-signalling* or *signalling*, respectively, with strength referring to the channel's position on the nonlocal hierarchy (see section 3.2).

We denote $w(G)$, the maximal probability of winning a game G. We will sometimes use additional markers when denoting the probability of winning a game under certain condition. An example is the commonly used $w^*(G)$ used to denote the maximal probability of winning a game using quantum channels. We may sometimes talk about the nonlocality of the game when referring to the channel required to win it interchangeably.

We now introduce a formal notation for a game $\boldsymbol{G}$ under a promise.

Definition 4.3.3 (n-party game $\boldsymbol{G}$ under a promise)**.** Let F be the set of inputs we want to remove from U. Then, we define $G' = G \setminus F$ to be the game G minus the inputs F. Formally, this means

$$G' = \{U \setminus F, A, P'(x_1, ..., x_n), V'(x_1, ..., x_n, a_1, ..., a_n)\}$$

with the new P' being defined as

$$P'(x_1, ..., x_n) = \begin{cases} \dfrac{P(x_1, ..., x_n)}{\sum_{(x'_1,...,x'_n)\in U} P(x'_1, ..., x'_n) - \sum_{(x'_1,...,x'_n)\in F} P(x'_1, ..., x'_n)}, & \text{if } (x_1, ..., x_n) \notin F \\ 0 \quad , & \text{if } (x_1, ..., x_n) \in F \end{cases}$$

and the new V' being defined as $V'(x'_1, ..., x'_n, a_1, ...a_n) = V(x'_1, ..., x'_n, a_1, ...a_n)$ where $(x'_1, ..., x'_n) \in U \setminus F$ and $V' : U \setminus F \times A \to \{0, 1\}$.

4.4 The CHSH Game

A simple example for this is the CHSH game. In this 2-player game, each of the players has an input, x and y, and they must output bits a and b such that $a \oplus b = x \wedge y$. Formally, this is

$$G = \{(X \times Y), (A \times B), P(x, y), V(x, y, a, b)\}$$

In binary, $X = Y = A = B = \{0, 1\}$ the inputs and outputs are the pairs $(0, 0),\ (0, 1),\ (1, 0),\ (1, 1)$. The standard probability of inputs is 25% chance for each, and V simply verifies that $a \oplus b = x \cdot y$.

This game is only known to be solvable on all inputs with supra-quantum no-signalling strength, the channel used to solve it being called the PR-box [PR94]. Nevertheless, it is interesting to note that classical players can solve it 75% of the time. Indeed, laying out all the possibilities, we find out that for any possible output, if the players answer it every time, they will have only one out of the four possible answers for which it fails. For example, answering $(0, 0)$ will work all the time except when the input is $(1, 1)$. If we were therefore to exclude a single input, $(1, 1)$, this case would be solvable classically. This can be done for every output choice by the players, hence by excluding a single input, the players can choose which output will lead to them winning the game 100% of the time. Under this promise, we can write

$$G' = G \setminus (1, 1) = \{(X \times Y) \setminus (1, 1), (A \times B), P'(x, y), V'(x, y, a, b)\}$$

with

$$P'(x, y) = \begin{cases} \frac{1}{3}\ , & \text{if } (x, y) \neq (1, 1) \\ 0\ , & \text{if } (x, y) = (1, 1) \end{cases}$$

4.5 A More Complex Example: The Magic-CHSH Game

We here draw a more complex example where the nonlocality requirement to win a game changes when altering the promise on the inputs, which we shall name Magic-CHSH. Let us define a two player game such that depending on an input which is given to the players by the verifier, the game will be either the magic square game as examined in [BBT05] or the CHSH game. Formally, this is

$$G = \{(X \times Y), (A \times B), P(x, y), V(x, y, a, b)\}$$

where each of the players has an input in the form of a pair consisting of a trit and a bit, x and y, and they must each output a pair of bits a and b. We name the variation bit included in the input pair of each player z. When Magic-CHSH$|z = 0$, the players must win the magic square game, as found in [BBT05]. When Magic-CHSH$|z = 1$, the players must win the CHSH game. Figure 4.1 depicts the unified channel required to win this game.

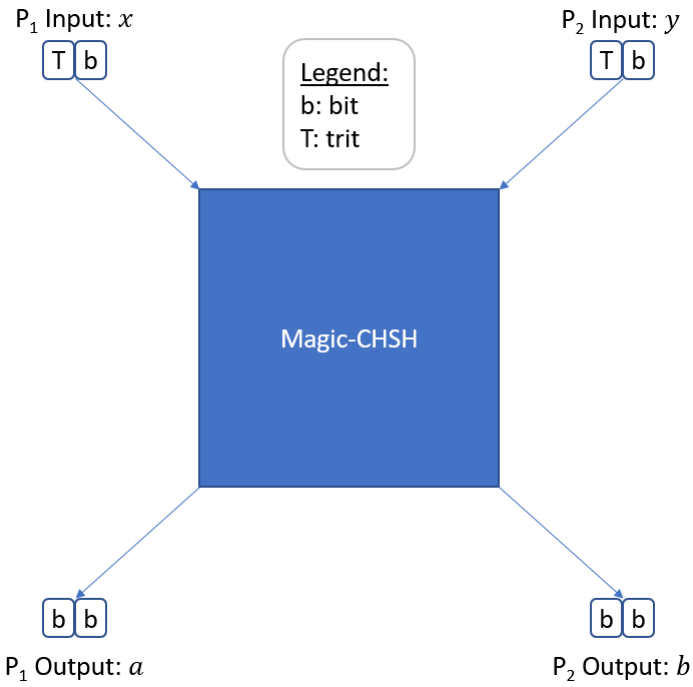

Figure 4.1: The Magic-CHSH channel represented as a black box.

When playing the magic square game, the players will receive a trit indicating their row or column, as well as the $z = 0$ bit. Out of the channel they will receive the two bits needed to complete their parity calculation. When playing the CHSH game, they will receive a trit that can be converted by their channel to a bit by using the modulo 2 operation, and they they will get an output that is two bits: one bit b, their answer to the CHSH game, to be transmitted to the verifier, and the other bit, b', will simply be a random bit output by the channel.

It is known that the magic square game can be solved perfectly by two quantum players [BBT05], and that the CHSH game can be solved by two no-signalling players using a channel equivalent to the PR-box [BCP$^+$14]. When there is no promise on the variation bit, both games need to be solvable by the players to win. Recalling the nonlocal hierarchy from figure 3.2, the channel required to win Magic-CHSH game is therefore a no-signalling one.

When not putting any promise on the inputs, there is no requirement that the two game-deciding bits agree with each other. Given that this is a fictive example, we will play nice and set that when they do not agree, the players win whatever they answer, meaning

$$\forall\ T_1, T_2, z, a, b, V((T_1, z), (T_2, \neg z), a, b) = \text{ True.}$$

This means that the players will act in the same way whether or not they are playing the same game.

When we place a promise on the inputs, the nonlocality requirements can change. If we guarantee that the only game that will be played is the CHSH game, therefore we set $G' = G \setminus \{z = 0\}$, the players will still need no-signalling strength to win the game. On the other hand, if we have that $G' = G \setminus \{z = 1\}$, the only game being played is now the magic square game, and the players can win 100% of the time with only a quantum channel. By enacting a promise on the inputs, specifically on the variation bit, we change the level of nonlocality required of the players to win the game. We can go even further and restrict other inputs. For example, when $G' = G \setminus \{z = 0\}$, we can restrict the input trits so that

one of the four possible values for the CHSH game is not possible. As we have seen in the when examining the CHSH game, this version only needs local power to win.

4.6 Channels under promises

One significant thing to note from this is that, by enacting a sufficient amount of promises, this channel, as well as any channel, will become local. As more promises are added, the channel will descend in the nonlocality hierarchy, be it by going down one class at a time (NS→quantum→local), or possibly many at once (SIG→local). We reiterate that the idea of adding a promise signifies forbidding one possibility of input or more from all the possible inputs.

4.6.1 A curious phenomenon about underlying channels

We end this recapitulation section with a curious phenomenon about promises.
Let $G = \{(X \times Y), (A \times B), P(x, y), V(x, y, a, b)\}$ be the game G, with X, Y the sets of inputs of players Alice and Bob and A, B the sets of outputs of those same players. $P(x, y) \in [0, 1]$ is the probability distribution of the input pairs and $V(x, y, a, b)$ is the predicate which determines if the game is won or lost. Let us then define a new game,
$G \setminus F = \{(X \times Y) \setminus F, (A \times B), P'(x, y), V'(x, y, a, b)\}$ with $F \subset (X \times Y)$.

Having defined these terms, we can now observe, keeping in mind that as we talk about games in the following statements, we are actually talking about the channels required to beat them, that

Theorem 4.6.1 (Existence of an overlying absolute channel)**.**

- if $G \setminus F$ is local, then there exists a local G' s.t. $G' \setminus F = G \setminus F$.
- if $G \setminus F$ is quantum, then there exists a quantum G' s.t. $G' \setminus F = G \setminus F$.
- This is not necessarily true for no-signalling. Indeed, there exists $G \setminus F$ which is no-signalling such that there is no no-signalling G' s.t. $G' \setminus F = G \setminus F$.

In the following section we will prove this last statement and formalize their definition, but first let us examine the previous two statements.

Proof. The first two statements are born of the idea that the local and quantum strategies are a deterministic recipe to be executed. Indeed, the method we use to prove the statements is the same for both: from the game $G \setminus F$, we create the game G' by adding F, but changing the game such that the players win no matter their answer on F. It is trivial to see that local players which win on $G \setminus F$ will win on G'. Quantum players use a joint state for which there exist measurements such that their outputs will win on any input from $G \setminus F$. The same measurements are perfectly capable of giving an answer on inputs from F, even if they do not win the game G, in G' they are given an automatic win.

To formalize this, notice that in both the local and the quantum cases, the strategy used is deterministic and therefore well-defined for any inputs. Given that they are binary, extending the strategy to further inputs is therefore not a problem. □

So why does this not work in the no-signalling case? In the following sections, will we come to know a specific example which breaks this rule, and we will see that adding the fact that the players win all the time in the no-signalling case will alter the channel in a way that allows them to signal. This is due to the fact that the tool used to create this channel is the PR-box, which itself has no strategy, but rather a correlation that is the precedent for that same channel.

4.7 A note about strategies

The players, when trying to solve the games, will put in place strategies and use resources to apply those strategies. In the local setting this strategy may only use shared randomness and a predetermined way to answer the questions, and in the nonlocal setting they may use further resources. It is important to note that players are not bound to use the same strategy unilaterally on all inputs. In the Magic-CHSH game for example, the players can apply a

quantum strategy when playing the magic square game, and a no-signalling strategy when playing the CHSH game.

Chapter 5

Complete Example with Promises in Games

5.1 FF15

We now will lay out a 3-player game inspired from [FF15] [FF19], and we shall reuse it all along our main example on promises. The authors claim that this protocol is resistant to no-signalling adversaries. In the following sections we will lay out the protocol as well as its main issues. We will show that while it, or an adapted version of it, does indeed require a signalling channel to beat, in an applied setting it might be defeated by no-signalling adversaries.

5.1.1 Honest Players' Strategy

For this game, in its most basic version, a verifier will give each of the players a binary value as input, a, b and c. The outputs from the players must then be $x := r + a \cdot b$, $y := r$ and $z = r$, with r being an uniformly random value chosen by the players as their shared randomness. **The players win if** $y = z$ **and** $x - y = a \cdot b$. This strategy will be used by honest players which have no further resources than local channels.

Given that the two last provers using this channel are going to want to answer the same value, we can deduce that $y = x - a \cdot b$ and $z = x - a \cdot c$. Now it is easy to see that the satisfaction of these conditions alongside the one for which $y = z = r$ and the possibility that $b \neq c$ is not going to be possible all the time, notably when $a = 1$. In short, this game is not winnable 100% of the time.

5.1.2 Dishonest Players' Strategy

At this moment, FF15 still depends on factors that make its analysis cumbersome. Let us trim it it down to something equivalent but more easily manageable by only keeping what is necessary for no-signalling players attempting to win by using nonlocal resources such as no-signalling channels. Firstly, the reliance on an independent r for randomness is not actually needed. We can simply make the outputs of the players as x, $y = a \cdot b - x$ and $z = a \cdot c - x$. This scheme is equivalent to the previous one, and from those answers **we can still get the winning conditions** $y = z$ **and** $(y + x) = a \cdot b$. We represent the channel required to win the game in this manner in the figure 5.1.

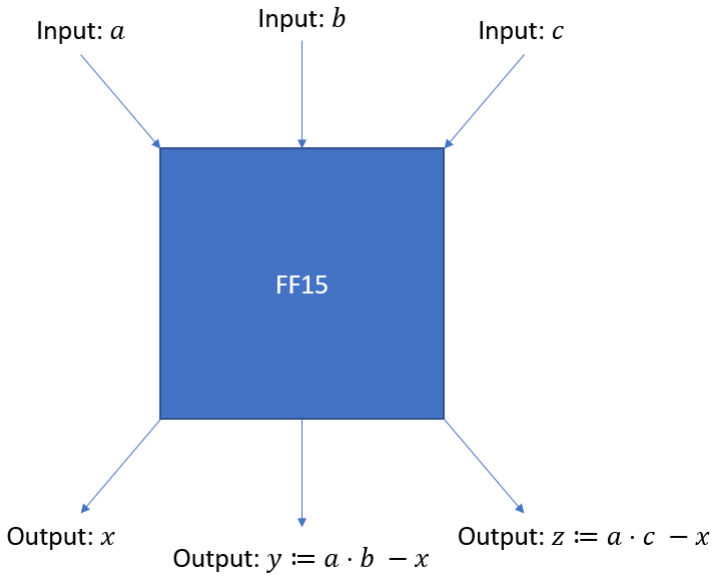

Figure 5.1: The FF15 channel.

5.2 Finalizing FF15 and Proving its Security

Having simplified the game as well as the channel required to play it, we are now left with our final problem: the game is not solvable all the time. To resolve this issue, we will give a new version of the game, **G'**, which is at least as easy as the original game **G**, so that if it is necessary to have a signalling channel to obtain $w(G') = 1$, it will also be necessary have one to obtain the highest $w(G)$ possible (given that $w(G) = 1$ is impossible).

Consider then the generalised version,

$$G' = G \text{ except } \forall a, b, x, y, z, V_{G'}(a, b, \neg b, x, y, z) = \text{ True.}$$

a	b	c	x	y	z	Pr
0	0	0	0	0	0	½
0	0	0	1	1	1	½
0	0	1	0/1	0/1	0/1	?
0	1	0	0/1	0/1	0/1	?
0	1	1	0	0	0	½
0	1	1	1	1	1	½
1	0	0	0	0	0	½
1	0	0	1	1	1	½
1	0	1	0/1	0/1	0/1	?
1	1	0	0/1	0/1	0/1	?
1	1	1	0	1	1	½
1	1	1	1	0	0	½

Figure 5.2: A representation as a table of the G' game. The coloured rows indicate each combination of a and $b = c$. In each case, there are two combination of resulting x, y, z which are possible with equal probability. The greyed out rows indicate the combinations of a and $b \neq c$. In these cases there is no probability on the results because they do no matter on the outcome.

This game is represented as a table in figure 5.2. This version is obviously easier than (or equal in difficulty to) the original game, which means that if the provers need a signalling channel to win G', they will need a signalling channel to maximize their chances of winning G.

Claim 5.2.1. *If there is a promise on the inputs, namely when we establish the game as $G' \setminus \{b \neq c\}$, we see that the game actually becomes no-signalling.*

Proof. This is because when $b = c$, we can see that the condition boils down to the first prover making a PR-box with each of the second and third provers. Recall definition 3.4.4 of n-player no-signalling. There are three ways of subdividing the players. When we put P_2 and P_3 together, they gather no new information as $b = c$ and therefore we still have the equivalent of the PR-box. When P_2 is put with P_1 in the subdivision, no new information can be signalled to P_1 and P_2 because they will already have learned of P_3's input bit as $b = c$. No new information can be signalled to P_3 either because its correlation with P_1 is equivalent to the PR-box (which is NS) and because it already knows P_2 input and output. As similar reasoning can be used when P_3 and P_1 are put together in the subdivision. Since there is no way of signalling between two subsets of the 3 players, the $G' \setminus \{b \neq c\}$ channel is no-signalling. □

Claim 5.2.2. *The game **G** will require a signalling channel to be won under no promise.*

Proof. Recall definition 3.4.3. We will show that for every one of the three possible subdivisions of players in two separate groups, there will be information which is signalled from one group to another.

If there is a configuration a, $b \neq c$ such that $a \cdot b - x \neq y$ then the game is signalling from the third to the two first players, as they are able to observe that $a \cdot b - x \neq y$ and hence conclude that $b \neq c$.

If there is a configuration a, $b \neq c$ such that $a \cdot c - x \neq z$ then the game is signalling from the second to the first and third players, as they are able to observe that $a \cdot c - x \neq z$ and hence conclude that $c \neq b$.

If we always have $a \cdot b - x = y$ and $a \cdot c - x = z$ then when $b \neq c$ we obtain $\pm a = y - z$ which is signalling from the first player to the second and third.

To always win the game then, including when the $b = c$ condition is not enforced, the players need to have signalling power. □

5.3 The original context: Bit Commitment Schemes

Originally, FF15's context is one of a bit commitment protocol. Such protocols are a way for a party of committing to some information while only revealing it later. This has uses in many different applications, including those of authentication protocols, for example. The security of those protocols rely on two main properties. The first is the **binding** property, indicating that a commitment cannot be changed after it is made.

Definition 5.3.1 (ϵ-Binding)**.** *We say that a BC is ϵ-binding when its commitment cannot be changed after it is made except with a small chance ϵ.*

The second is the **hiding** property, indicating that the commitment cannot be deciphered without the key by another party.

Definition 5.3.2 (ϵ-Hiding)**.** *We say that a BC is ϵ-hiding when its encryption cannot be broken except with a small probability ϵ.*

An intuitive example of bit commitment is that of a safe. If Alice gives Bob a safe with an object inside, she then cannot change the object inside it, and Bob cannot open the safe until he is given the key at a later moment.

A concrete example of a bit commitment protocol is the FF15 protocol. In its most simple version, a random value a is given to the first prover, who then outputs the value $x = a \cdot b - r$, with b being the committed value and r being the key. At a later point, the second prover (and a third one as well in this case) will reveal the key, which solves the equation and also reveals the value the provers were committed to. We can see now that in the complete protocol, the first prover is tasked to commit, and the two last provers are

tasked to open the commitment. Given this, it is obvious to see why the $b = c$ condition is important: they must open the same bit.

Understanding this, we can see that our updated definition of NS could mean a difference in expected security for a real-life implementation of the protocol. Indeed, since in its application there would always be the $b = c$ condition, then it could actually never be resistant to no-signalling opponents. We cannot lay out a blanket statement beyond this, for we have no implementation of Supra-Quantum-NS resources yet. This debate remains as asking whether or not unicorns have wings, for now...

5.4 Relativistic issue

Another important aspect of the protocol to consider is the fact that provers, given the context, may have to synchronize themselves in their opening of the bit commitment. Specifically, this is due to the fact that this protocol is a "bare bones" implementation, and could later inspire a slightly modified version of itself which would be used to attempt NS-resistant bit commitment schemes (BCS), such as a protocol that uses 3-coloring as the game to be solved. In many such protocols, there can be a commitment to multiple values at once, meaning that there may be more than one instance of the protocol being run in parallel. The provers must therefore not be played for fools by the verifier to get both of the opening provers to open a different commitment, which could have heavy consequences for the security of the provers' tactics. One solution proposed by the authors of [FF19] for such a verification is that of sending an authenticated message from the first prover to the verifier, which would then relay it to the second and third provers. In this message, P_1 would dictate whether or not to open a certain commitment. The message itself would be too small to allow the inclusion of an element of text allowing the players to cheat on their commitment. Instead, it is the authentication tag, a technique commonly used to verify the authenticity of the message's provenance, which must be restricted in length in accordance to the protocol's security parameters in order to prevent its misuse as a cheating device.

The problem that arises, thought, is that during the time that this authenticated message is relayed, the provers inevitably have time to signal to each other. Given that the separation between the provers is enforced through relativistic means, it will inevitably fail and the provers will be able to communicate, nullifying the security of the bit commitment.

5.4.1 Extending The Commitment

To solve this problem, we propose using a technique to extend the duration of commitments from [LKB+15]. As mentioned in the paper, this technique uses a repeated relativistic commitment by the provers to their secret, for which the provers would continuously renew their commitment for the duration of the authenticated message's transit. Once the provers have agreed to open a certain bit, they can open the multiple commitments they would have made in accordance to [LKB+15]'s protocol with one final message to the verifier.

Let us show what this might look like. Note that we will forgo some details, such as the delay the provers would have between each renewal of their commitment or the security parameters for the lengths of the random strings, as we are merely outlining a general scenario. Let us recall our improved FF15 scheme. We start out by renaming the provers P, P', P'' for legibility and adding that the they will share uniformly random strings p, p', p'' of length $l = n \times m$, where m is a substring length related to the protocol's security parameters, and n is the number of substrings required by the security parameters of the protocol sustain the commitment long enough. The verifier will also have similarly uniformly random strings v, v', v'' of length l. We name each substring of those strings p_k, p'_k, p''_k and v_k, v'_k, v''_k, with $k \in \{0, ..., n\}$. Note that in each round γ, the p_k's added in that round will have indices $k \in \{2^{\gamma-1}, ..., 2^{\gamma}-1\}$, except for the 0^{th} round which will only use index 0. We will now slightly modify the protocol to fit with this extended commitment scheme, whilst still maintaining a seeming equivalence. The verifier will start out by sending v_0 to P. This is more or less equivalent to the a from FF15. P will directly commit to bit b by replying with $x_0 = v_0 \cdot b \oplus p_0$. This is clearly represented in table 5.1.

Provers	P	P'	P''
Query by Verifier	v_0	-	-
Answer to Verifier	$x_0 = v_0 \cdot b \oplus p_0$	-	-

Table 5.1: Table representation of the 0^{th} round of our 3-prover adaptation of the [LKB+15] protocol.

Provers	P	P'	P''
Query by Verifier	-	v'_1	v''_1
Answer to Verifier	-	$y_1 = v'_1 \cdot p_0 \oplus p'_1$	$z_1 = v''_1 \cdot p_0 \oplus p''_1$

Table 5.2: Table representation of the first round of our 3-prover adaptation of the [LKB+15] protocol.

At preset intervals, determined such that the provers do not have enough time to signal, the verifier will ask the provers for another round of commitment. For the security to hold, the provers must commit to each of the p_k's used by the other provers in the previous round. We represent the exchange between provers and verifier in the first complete round in table 5.2.

The commitment should be set up so that the transit of the authenticated message should take no more rounds than there is available length of the p and v strings. When the provers have agreed on the bit they want to open, they simply send strings p, p', p'', revealing all the p_k's used and opening all the commitments. After a single round of recommitment, they could simply send p_0, p'_1, p''_1 for simplicity. We show this scheme clearly for a single round of recommitment in figure 5.3.

This technique can, on paper, be used to extend the commitments as long as it may be required, but the amount of resources required to enact it, namely shared randomness and communication bandwidth, will also increase exponentially with this length of time.

We can demonstrate this explosion of commitment by showing one more round. We represent the commitments in this round in table 5.3.

As we can see, the first prover P must now commit to two different values, as both P' and P'' made a commitment in the previous round. As the rounds increase, the number of

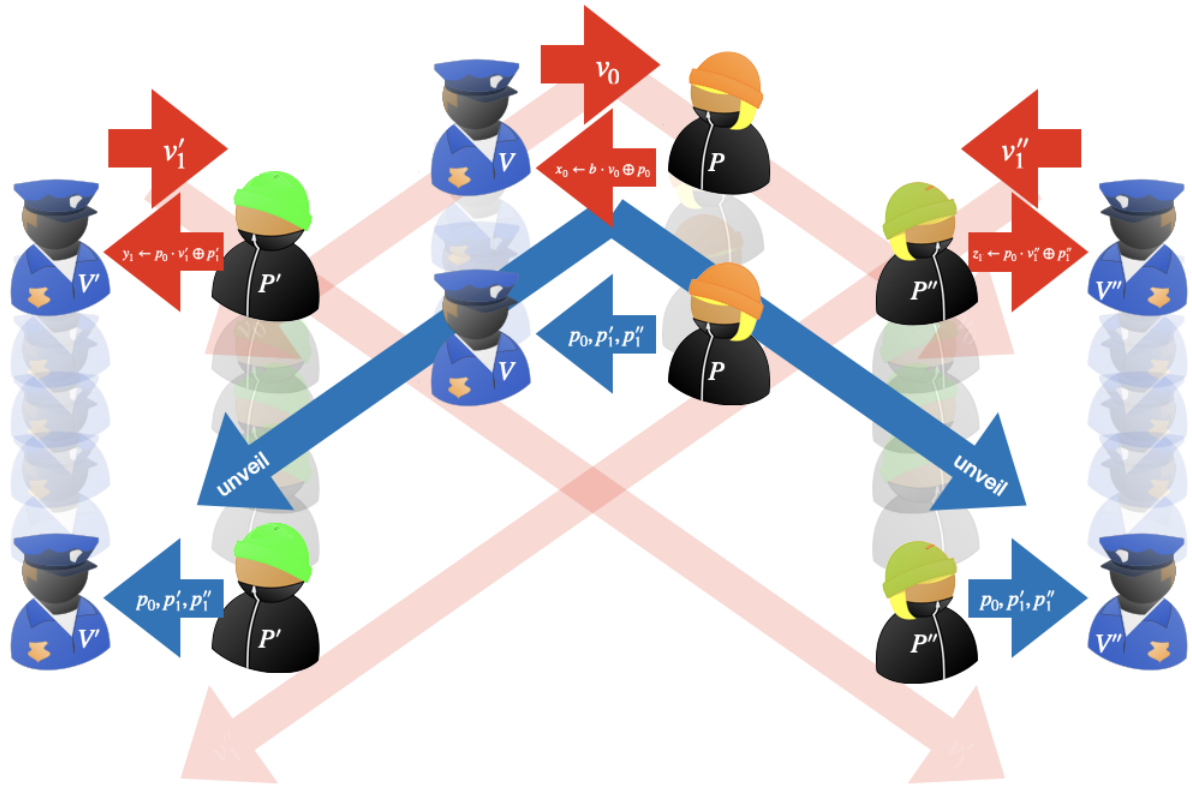

Figure 5.3: Representation of the the 0^{th} and first round of the recommitment scheme, and the unveiling of the commitments afterwards.

commitments made by the provers will increase exponentially. It is in the best interest of everyone involved in the protocol to keep the number of recommitments as low as possible so that the amount of resources expended is minimized.

Provers	P	P'	P''
Query	v_2, v_3	v_2'	v_2''
Answer	$x_2 = v_2 \cdot p_1' \oplus p_2$ $x_3 = v_3 \cdot p_1'' \oplus p_3$	$y_2 = v_2' \cdot p_1'' \oplus p_2'$	$z_2 = v_2'' \cdot p_1' \oplus p_2''$

Table 5.3: Table representation of the 2^{nd} rounds of our 3-prover adaptation of the [LKB+15] protocol.

It is of note that when using this technique to extend the duration of the commitments, the initial solution by the authors of [FF19] to send an authenticated message through the verifier becomes obsolete, and we can simply let the provers signal while making recommitments and decide between themselves when they are ready to unveil.

Chapter 6

A New Model of Security

In this final chapter we now put everything together. We combine the knowledge we have extracted from analyzing FF15 as well as our other toy examples with the definitions we have established for promises.

6.1 Absolute and Restricted Channels

Recall section 4.6.1. In this section, we observed the idea of *absolute* and *restricted* channels, the latter being a channel with promises on the inputs and the former simply being the same channel without the promises. We can now define these channels formally. Let it be said that while we sometimes use the name of the game to talk about the channel required to play or win it, we will now distinguish them for clarity.

6.1.1 Defining Restricted Channels

We see no downside in simply extending the notation we have created in section 4.3.

Definition 6.1.1 (Restricted Channel)**.** *Let C be an absolute channel, with no promise on its inputs. We can say that*

$$C = \{X = (X_1 \times ... \times X_n), A = (A_1 \times ... \times A_n), P(a_1, ..., a_n | x_1, ..., x_n)\}$$

for some $P : X \times A \to [0,1]$.

Define a restricted channel $C' := C \setminus E$ *with* E *some subset of the inputs of channel* C. *Formally,*

$$C' = C \setminus E = \{X \setminus E, A, P'(a_1, ..., a_n | x_1, ..., x_n)\}$$

Where $P' : (X \setminus E) \times A \to [0,1]$ *and*

$$P' = \begin{cases} \dfrac{P(a_1, ... | x_1, ..., x_n)}{\sum_{(x'_1,...,x'_n) \in X} P(a_1, ... | x'_1, ..., x'_n) - \sum_{(x'_1,...,x'_n) \in E} P(a_1, ... | x'_1, ..., x'_n)}, & \text{if } (x_1, ..., x_n) \notin E \\ 0 \quad , & \text{if } (x_1, ..., x_n) \in E \end{cases}$$

6.1.2 Nonlocality of restricted channels

The definitions of nonlocality used in section 3.3 and 3.4 are still applicable to restricted channels. Instead of using the full sets of inputs, we will simply now use the restricted sets of inputs. The nonlocality of the channel will depend on the nonlocality definitions it satisfies with those restricted sets of inputs.

6.1.3 Existence of overlying absolute channels

Let $G' = G \setminus F$ for some game G. The case which will be of particular interest to us is the one in which the inputs of G' and C' are the same. In this case, C' can be used to play the game G'.

We also observed that, for local and quantum channels, this difference is trivial. Let C be a channel and C' a restricted version of the channel.

Theorem 6.1.1 (Existence of an overlying absolute local channel)**.**

$$\forall C' := C \setminus E \in \boldsymbol{LOC},\ \exists C'' \in \boldsymbol{LOC}\ s.t.\ C'' \setminus E = C', \tag{6.1.1}$$

with C'' *being an absolute channel.*

Proof. From the game $G \setminus F$, we create the game G'' by adding F, but changing the game such that the players win no matter their answer on F. Local players which win on $G \setminus F$ will win on G'' because their strategy is deterministic and well-defined for any input, using only simple functions and shared randomness, and adding the special F will not change this strategy. The channel C'' is therefore local. □

Theorem 6.1.2 (Existence of an overlying absolute quantum channel)**.**

$$\forall C' := C \setminus E \in \boldsymbol{QNL},\ \exists C'' \in \boldsymbol{QNL}\ s.t.\ C'' \setminus E = C', \tag{6.1.2}$$

with C'' being an absolute channel.

Proof. From the game $G \setminus F$, we create the game G'' by adding F, but changing the game such that the players win no matter their answer on F. Quantum players which win on $G \setminus F$ will win on G'' because their strategy is deterministic and well-defined for any input, using only simple functions, shared randomness and POVMs on their side of an entangled particle system, and adding the special F will not change this strategy. The channel C'' is therefore quantum. □

For no-signalling channels, as we have seen through the example of FF15, this is not always the case.

Theorem 6.1.3 (Lack of existence of an overlying absolute no-signalling channel)**.**

$$\exists C' := C \setminus E \in \boldsymbol{NOSIG}\ s.t\ \nexists C'' \in \boldsymbol{NOSIG}\ s.t.\ C'' \setminus E = C', \tag{6.1.3}$$

with C'' being an absolute channel.

Proof. Let G be the original FF15 game from section 5.1.2, and G' the new game represented in table 5.2. We prove this statement with the proof 5.2, as in that case every channel which can win the game G' is signalling, whereas the channel $FF15 \setminus \{b \neq c\}$ is no-signalling. These are all the possible C'' channels in the definition above and the $FF15 \setminus \{b \neq c\}$ is the C' channel. □

6.1.4 Relevance of the Inclusion of Restricted Channels

When studying the security of FF15 against no-signalling, we have seen that it relies on the fact that there is no promise on its inputs. When we forced $b = c$, we were able to downgrade its security such that the channel required to win FF15$\backslash\{b \neq c\}$ is no-signalling. This is where the point made in section 4.6.1 shines: there is no absolute no-signalling channel that can win FF15$\backslash\{b \neq c\}$. The proof of this being in the fact that the unrestricted channel, which can win FF15 under no promise, was proven to be signalling.

Recall earlier when we mentioned that the interesting case is when the inputs of the restricted channel matches the ones of the restricted game. Here, we can see that if we want FF15$\backslash\{b \neq c\}$ *game* to be won with a no-signalling channel, we need to allow the provers to use a signalling channel with a promise on its inputs, in this case being the FF15$\backslash\{b \neq c\}$ *channel*.

6.1.5 Absolute versus Restricted Channel Nonlocality

This brings us to revisiting what we consider to be the level of nonlocality of a channel, which have also often referred to in this work as its *strength* or *power*. Traditionally, channels are judged by their nonlocality when considering them on all possible inputs. This is an incorrect interpretation, because in practice a channel cannot harness its full power unless it is played without restriction. An FF15 *channel* for example, which wins the game with probability 1, is signalling, but there exist an FF15$\backslash\{b \neq c\}$ *channel* which is only no-signalling. Similarly then to earlier when we made a case for determining the nonlocality of a channel required to win a game with probability 1 depending on which inputs will actually be used, we can see the relevance of determining the nonlocality of a channel based on which inputs it will have access to.

6.2 Culmination of our Rework of Nonlocal Games

We can now state our suggestions for reworking the model of security of nonlocal games. Its main points are twofold:

1. **Allow promises on the inputs of nonlocal games**, which essentially change the probability distribution of inputs by reducing the probability of some inputs to zero.

2. **Evaluate the nonlocality of channels based on the promises on their inputs**, and give players access to channels which are more powerful than required, as long as the channels are of the correct nonlocality level when limited to the game's inputs.

While the second statement is made in a general form, it will have the greatest impact on no-signalling channels, as seen in section 4.6.1. As the search for no-signalling-resistant bit commitment protocols carries on, for example, this will allow the examination of protocols which feature restricted channels and promise games, which might lead to discoveries we would not have made while restricting our horizons otherwise.

While this will allow the greatest level of generality for nonlocal games, it will also pose no greater threat to security compared to what is offered by the traditional model. If the provers can be trusted to solely use the channels allowed of them in a game, then they can obviously be trusted to only use these tools on the allowed inputs as well.

Chapter 7

Conclusion

In conclusion, we suggest a new model of security for nonlocal games in which we allow promises on the inputs of the games and we evaluate the level of nonlocality of a channel based on the inputs it will use rather than on its absolute form. This more general form allows the consideration of games and channels which we would not have allowed in the traditional security model. Given that no-signalling channels do not yet have a physical implementation, this additional generality allows us to consider cases where the traditional model might have been disconnected from a potential real-world implementation of protocols.

To get to this, we examined *nonlocal games*, a type of multi-player game in which the level of correlation of the answers of the players can affect their chances of winning. These games are traditionally defined such that players must expect all possible inputs from the field on which the game's inputs are defined on. The players will then use different types of *communication channels* with various levels of nonlocality to bolster the correlation of their answers. Similarly to the games, it is traditionally defined that, since a channel will be used as a tool by the players, its strength will be defined by what it can do on all possible inputs for the field its inputs are defined on.

As we examined a 3-prover bit commitment scheme from [FF15] which was claiming to be resistant to no-signalling adversaries, we realised the importance that promises on inputs could have and their potential impact on real-world security. We then showed that the FF15

protocol is actually not necessarily resistant to no-signalling under this new model of security which encompasses promises.

The most interesting aspect we draw from this work is the future analysis of promise games with restricted channels. While it may be that some bit-commitment schemes are resistant against no-signalling channels, it will be of great interest to figure out if there are bit commitment schemes resistant against restricted no-signalling channels, and why. While FF15 is resistant to no-signalling, it is not "realistic" in the sense that in a real world application we will always have $b = c$. Given FF15$\backslash\{b \neq c\}$'s vulnerability to restricted no-signalling channels, the search for a truly NS-resistant bit commitment scheme is not over.

Our foray into the implementation possibilities of the full commitment scheme itself also shows promise for future research. The commitment scheme derived from [LKB$^+$15] in section 5.4.1 could be setup with a full set of security parameters and it could be evaluated to determine its resistance against no-signalling opponents. It is significant as there is little data on no-signalling resistance for multi-round protocols, much less when adding the possibility of a promise on the inputs.

Bibliography

[BBT05] Gilles Brassard, Anne Broadbent, and Alain Tapp. Quantum pseudo-telepathy. *Foundations of Physics*, 35(11):1877–1907, November 2005.

[BCP+14] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Reviews of Modern Physics*, 86(2):419–478, April 2014.

[Bel64] J. S. Bell. On the Einstein Podolsky Rosen paradox. *Physics Physique Fizika*, 1:195–200, Nov 1964.

[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*, STOC '88, page 113–131, New York, NY, USA, 1988. Association for Computing Machinery.

[CC21] Nicolas Courtemanche and Claude Crépeau. A sufficient clarification of "super-quantum correlations: A necessary clarification" by Pierre Uzan. *Journal of Quantum Information Science*, 11(02):65–70, 2021.

[CH74] John F. Clauser and Michael A. Horne. Experimental consequences of objective local theories. *Phys. Rev. D*, 10:526–535, Jul 1974.

[Cir80] B.S. Cirel'son. Quantum generalizations of Bell's inequality. *Letters in Mathematical Physics*, 4:93–100, 1980.

[FF15] Serge Fehr and Max Fillinger. Multi-prover commitments against non-signaling attacks. In Rosario Gennaro and Matthew Robshaw, editors, *Advances in Cryptology – CRYPTO 2015*, pages 403–421, Berlin, Heidelberg, 2015. Springer Berlin Heidelberg.

[FF19] M.J Fillinger and S. Fehr. Two-prover bit-commitments: Classical, quantum and non-signaling. *Leiden University Scholarly Publications*, Mar 2019.

[LKB+15] T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, S. Wehner, and H. Zbinden. Practical relativistic bit commitment. *Physical Review Letters*, 115(3), July 2015.

[PR94] Sandu Popescu and Daniel Rohrlich. Quantum nonlocality as an axiom. *Foundations of Physics*, 24(3):379–385, March 1994.

[Sho97] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, October 1997.