Quantum information theory for relativistic cryptography and quantum algorithms

Habilitation à Diriger les Rechercers présentée à

Inria de Paris

par

André Chailloux

soutenue le 20/01/2025 devant le jury composé de

Claude Crépeau	Rapporteur
Ronald de Wolf	Rapporteur
Jérémie Roland	Rapporteur
Eleni Diamanti	Examinatrice
Elham Kashefi	Examinatrice
Sophie Laplante	Examinatrice
Frédéric Magniez	Examinateur
Damian Markham	Examinateur
Nicolas Sendrier	Invité
Iordanis Kerenidis	Invité

Année 2025 EDITE

dla Ewy,
pour Caroline et Agnès.

Antoine.

Foreword

This manuscript for my *Habilitation à Diriger les Recherches* contains a selection of my work that I did after my thesis. I will now very briefly describe the different topics I have worked on since my thesis - many of which I won't talk about here - which also serves as a shout-out for all my coauthors.

After my thesis that dealt with the theoretical analysis of quantum cryptographic primitives, I worked on cryptographic primitives and multipartite entanglement verification schemes in real physical scenarios, which lead to their practical implementation. This was joint work with Eleni Diamanti, Iordanis Kerenidis, Anna Pappa, Damian Markham, Paul Jouguet, Tom Lawson, Matthieu Legré, Patrick Trinkler, Stephanie Wehner, Will McCutcheon, Bryn Bell, Alex McMillan, Mhlambululi Mafu, John Rarity, and Mark Tame [PCDK11, PCW$^+$12, PJL$^+$14]. I also worked on quantum oblivious transfer and relations with entangled games and random access codes. These were joint works with Jamie Sikora, Gus Gutoski, Iordanis Kerenidis and Srijita Kundu [CKKS14, SCK14, CGS16].

I discovered interesting research questions around the complexity class $\mathsf{QMA}(2)$ jointly with Or Sattath [CS12]. I also worked with Giannicola Scarpa on parallel repetition of entangled games [CS14a, CS14b], and with Iordanis Kerenidis and Mathieu Laurière on quantum communication complexity [CKL17]. I also worked on trying to understand the mysteries of Mochon's quantum weak coin flipping with Iordanis Kerenidis, Dorit Aharonov, Loïck Magnin and Maor Ganz [ACG$^+$16].

Later, I worked on cryptography that used relativistic principles for bit commitment and zero-knowledge protocols for NP, as well as for position verification. These were joint works with Anthony Leverrier, Kaushik Chakraborty, Rémi Bricout, Frédéric Grosshans, Andrea Olivo, Ulysse Chabaud and Yann Barsamian [CCL15, CCL16, CL17, BC17, OCCG20, CB21].

With colleagues from my Inria team, I worked on algorithms for quantum cryptanalysis for code-based and lattice-based cryptography as well as more general algorithms for the collision problem. This was joint work with Maria Naya-Plasencia, André Schrottenloher, Thomas Debris, Rémi Bricout and Matthieu Lequesne, Simona Etinski and Johanna Loyer [CNS17, BCDL19, Cha19, CL21, CDAE21, CL23]

I also worked on quantum security proofs for public key cryptography as well as symmetric key cryptography in joint works with Thomas, Maria, Simona, Gaëtan Leurent, André, Ritam Bhaumik, Xavier Bonnetain and Yannick Seurin [CD20, Cha19, BBC$^+$21, CE23].

I was lucky to participate in the second round of NIST's competition for post-quantum signature schemes. We submitted the code-based signature WAVE, jointly with Gustavo Banegas, Kévin Carrier, Alain Couveur, Thomas Debris-Alazard, Philippe Gaborit, Pierre Karmpan, Johanna Loyer, Ruben Niederhagen, Nicolas Sendier, Benjamin Smith and Jean-Pierre Tillich [BCC$^+$23].

Recently, I worked with Jean-Pierre on interesting developments of Regev's reduction for

codes [CT24] and I also discovered with Thomas the joys of packing bounds and association schemes [CD24].

In this manuscript, I present a personal view of a few of these research topics. However my research wouldn't have been one tenth as interesting without the great research collaborations and encounters that I have done throughout these years.

Here is also the good place for warmly thanking everyone that accepted being part of my jury. Claude, Ronald and Jérémie for accepting to review this habilitation and Eleni, Elham, Sophie, Frédéric, Damian, Nicolas and Iordanis for being in my jury. Every single one of you has had a positive and inspiring influence on the researcher I have become.

Introduction

This manuscript will have two parts. In the first part, I will present quantum information tools known as a quantum learning in sequence lemmata and show how they can be used to bound the value of some entangled games. I then show how this can be applied to relativistic cryptography, which corresponds to multi-prover cryptographic protocols where we ensure the non-signalling requirement between the provers by adding spacetime constraints. In the second part of the manuscript, I will present a few results revolving around the quantum collision problem as well as quantum algorithms for the Shortest Vector Problem used in lattice-based cryptography.

A habilitation thesis in France is often non-technical. Nevertheless, there will be some moments where I will provide some proofs or proof sketches. The goal is to present some of the key ideas around the work I present here, and it is sometimes necessary to give formal definitions. On the other hand, when formalizing everything damages the reading flow and the clarity, I omit some technical discussions and stay at a high level when conveying the main ideas. I now summarize the contributions presented in this thesis.

Chapter 1. Learning in Sequence lemmata and entangled games

If we encode some classical bits into a quantum state ρ, a particularly interesting feature of quantum information is that trying to learn one of the encoded bits via a measurement will modify ρ and hence can potentially destroy the information we have on other bits. The first part of this manuscript aims at understanding and bounding as tightly as possible this phenomenon in terms of learning in sequence lemmata. In its simplest form, a learning in sequence lemma states the following: suppose you are given a state ρ_{x_0,x_1} that depends on two bits x_0, x_1 and suppose you can recover x_0 and x_1 from ρ_{x_0,x_1} with some respective probabilities p_0 and p_1. What is the probability can you learn both bits (x_0, x_1)? While I used many variants of these statements as powerful technical tools in several of my papers, I haven't had the occasion to present them in a standalone fashion, which is the aim of this first chapter, where I will also show connections to entangled games.

Chapter 2. Relativistic zero-knowledge for NP

Relativistic cryptography is a way to bypass impossibility results for (quantum) bit commitment using a multi-prover setting, and using spacetime constraints to ensure that the provers cannot communicate. There is a known relativistic bit commitment protocol by Simard, and the goal of this chapter is to see how it can be used in a zero-knowledge protocol. Here, we choose the zero-knowledge protocol for Hamiltonian Cycle by Blum - which is an NP complete problem. The reason we chose this protocol over 3-colouring for instance is that in the relativistic setting, its security against entangled provers translates into bounds for the value of an entangled game

which is easily analysable using the tools of the previous chapter. This was the first proposal for a relativistic zero-knowledge protocol for NP which is secure against entangled provers.

Chapter 3. Practical aspects of relativistic zero-knowledge

The relativistic protocol studied in the previous chapter had a small challenge size, which helped in analysing its security but it is not very efficient. Indeed, Blum's protocol requires to commit to all the bits of the adjacency matrix of the underlying graph and this results in a large communication in the protocol. Since the relativistic protocol has some strict spacetime constraints, the communication between the parties has to be very fast and we have to use a more efficient protocol.

To do so, we consider more practical cryptographic constructions, namely signature schemes. Many signature schemes are built from zero-knowledge protocols using the Fiat-Shamir transform and the efficiency of the signature scheme is directly related to the efficiency of the zero-knowledge protocol. We choose Stern's signature scheme for the Syndrome Decoding problem, which is closely related to the problem of decoding a linear code. This problem is NP-complete and is also believed to be hard for random instances against quantum computers. Moreover, Stern's zero-knowledge protocol is quite efficient, which makes it a good candidate. We provide a full security analysis of the resulting relativistic zero-knowledge protocol for Syndrome Decoding, by extending the tools of the first chapter. The protocol was actually efficient enough so that we could perform a practical implementation of it without specific hardware, over ethernet cables or over standard internet connection.

We now move to the second part of this thesis on quantum algorithms.

Chapter 4. Quantum collision problem with small quantum memory

The collision finding problem - or Element Distinctness in the community of quantum query complexity - is a fundamental problem that has many applications, notably in cryptography. It is well known that for efficiently computable hash functions $f : \{0,1\}^n \to \{0,1\}^n$, finding a collision *i.e.* $x, y \neq x$ such that $f(x) = f(y)$ can be done in average time $O(2^{n/3})$ using a quantum algorithm and that this is optimal.

It seems that the question is totally solved and that there is nothing to do. The catch is that all of these algorithms use a lot of quantum resources: they use as much quantum memory as time and also require QRAM (Quantum Random Access Memory) operations which will not necessarily be possible even if quantum computers are built. In a joint work with María Naya-Plasencia and André Schrottenloher, we show how to find collisions in time $O(2^{2n/5})$ on random functions $f : \{0,1\}^n \to \{0,1\}^n$ using only $O(\mathsf{poly}(n))$ quantum memory and no QRAM.

Chapter 5. Quantum lower bounds for permutation symmetric functions

The problem of determining whether a collision in f exists is permutation symmetric, in the sense that if we permute the inputs of f this doesn't change whether a collision in f exists or not. We also know that we have at most a polynomial advantage in the quantum case for solving this problem. Aaronson and Ambanis showed that there is at most a polynomial quantum speed-up for problems which have strong symmetries. In this chapter, I show how to generalize this result to a weaker type of symmetries and also to improve their result from a query complexity perspective.

Chapter 6. Quantum algorithm for the Shortest Vector Problem

In this last chapter, I will present quantum algorithms for the Shortest Vector Problem where, given a Euclidean lattice, the goal is to find the shortest non-zero vector (or in some variants, just a short vector) of the lattice. This problem is of particular importance because some of the best attacks on lattice-based cryptography use the BKZ basis reduction algorithm, which uses as a subroutine an algorithm for solving SVP. For a d-dimensional lattice, we improve the best quantum algorithm for SVP from $2^{0.265d+o(d)}$ to $2^{0.257d+o(d)}$ which reduces by a few bits the quantum security of most lattice-based cryptography schemes. We extend previous work that used locality sensitive filtering by noticing that the problem boils down to a collision problem to which we add a geometrical constraint. We then use a quantum walk, extending the quantum walk on the Johnson graph for collision finding, to solve this problem.

Chapter 1

Learning in sequence Lemmata and bounding the value of entangled games

While I was still a PhD student, I was working on proving lower bounds for quantum coin flipping and bit commitment. Since we knew how to construct bit commitment from oblivious transfer, it was natural to extend the lower bounds we had to oblivious transfer. This seemed like a straightforward result and I was at first reluctant to look at this problem in detail, thinking it had very small scientific interest. I was extremely wrong on that one. It turned out that there are some interesting technical difficulties when extending the lower bound from bit commitment to oblivious transfer. In order to solve these issues, we had to introduce the notion of *quantum learning in sequence lemmata*, which are at the core of several of my later research results.

In this chapter, I will first present how we first encountered the need for a learning in sequence lemma as well as some generalizations. Then, I present how they can be used to prover lower bounds for the entangled value of some 2-player game.

1.1 Lower bounds for Quantum Oblivious Transfer from Bit Commitment

We consider here only one variant of oblivious transfer, Quantum Random 1-out-of-2 Oblivious Transfer, which we will simply denote QROT. In a QROT protocol, Bob has 2 random bits x_0, x_1 and Alice wants to learn a bit x_i for $i \in \{0, 1\}$. A QROT protocol should ensure that Alice learns x_i but not the other bit x_{1-i} and also that Bob doesn't learn i. We present here a formal definition of QROT[1].

Definition 1.1. *A QROT protocol is a quantum protocol between Alice and Bob such that:*

- *Bob outputs two bits (x_0, x_1) or 'Abort' and Alice outputs two bits (i, y) or 'Abort'.*
- *If Alice and Bob are honest, they never abort, $y = x_i$, Bob has no information about i and Alice has no information about x_{1-i}. Also, x_0, x_1 and i should be uniformly random bits.*
- *Alice and Bob's optimal cheating probabilities are respectively*

$$A^*_{QROT} = \sup\{\Pr[\textit{Alice guesses } (x_0, x_1) \textit{ and Bob does not Abort}]\},$$
$$B^*_{QROT} = \sup\{\Pr[\textit{Bob guesses } i \textit{ and Alice does not Abort}]\}$$

where the two suprema are taken over all cheating strategies for Alice and Bob respectively.

[1]There are several small variants of this definition. Here, we define QROT such that x_0, x_1 are part of Bob's output and not part of his input, which is simpler to use.

- *The cheating probability of the protocol is defined as* $P^*_{QROT} = \max\{A^*_{QROT}, B^*_{QROT}\}$

QROT has many cryptographic applications as it is universal for secure multi-party computation. There are many classical constructions of oblivious transfer that use computational assumptions, for example Rabin's Oblivious Transfer [Rab81]. We know also from the work of Mayers, as well as Lo and Chau, [May97, LC97] that QROT cannot be performed perfectly (*i.e.* with $P^*_{\text{QROT}} = \frac{1}{2}$) without computational assumptions. During my thesis as well as in later years, I worked on trying to prove unconditional lower bounds on P^*_{QROT} for any QROT.

In order to prove such lower bounds, we relate QROT to another important cryptographic primitive which is Quantum Bit Commitment (QBC). In a bit commitment scheme, Alice wants to commit to a bit b to Bob such that: (1) Bob has no information about b after the commit phase and (2) if Alice wants to reveal b then she cannot change her mind and reveal another value for b than the one she committed to. Commitment schemes have a lot of applications in cryptography, for example for constructing zero-knowledge protocols, which can then for example be used to construct signature schemes.

We now formally define QBC and show how to relate the cheating probabilities of these 2 primitives.

Definition 1.2. *A QBC scheme is a quantum interactive protocol between Alice and Bob with two phases, a Commit phase and a Reveal phase.*

- *In the* Commit *phase, Alice interacts with Bob in order to commit to a bit* b.
- *In the* Reveal *phase, Alice interacts with Bob in order to reveal* b. *Bob decides to accept or reject depending on the revealed value of* b *and his final state. We say that Alice successfully reveals* b *if Bob accepts the revealed value.*

We define the following security requirements for the commitment scheme.

- Completeness: *If Alice and Bob are both honest then Alice always successfully reveals the bit* b *she committed to.*
- Sum-binding property: *In order to determine the cheating probability of a cheating Alice* A^*, *we ask* A^* *to be able to reveal any of the values* $b = 0$ *and* $b = 1$ *for a fixed commit phase that depends on* A^*, *this is captured by the quantity below.*

$$P^*(A^*) = \frac{1}{2}\left(\Pr[\textit{Alice successfully reveals } b = 0] + \Pr[\textit{Alice successfully reveals } b = 1]\right)$$

where these success probabilities are taken for the same commit phase, but potentially for different strategies when revealing $b = 0$ *or* $b = 1$. *This means a cheating strategy for Alice is characterized by a cheating strategy for the commit phase and two different cheating strategies for the reveal phase, depending on whether she has to reveal* $b = 0$ *or* $b = 1$. *We then define*

$$A^*_{BC} = \sup_{A^*}\{P^*(A^*)\},$$

where the supremum is for all cheating strategies for Alice described above, which can be computationally unbounded.

- Hiding property: *For any cheating Bob and for honest Alice, we define Bob's cheating probability as*

$$B^*_{QBC} = \sup_{B^*}\{\Pr[\textit{Bob guesses } b \textit{ after the Commit phase}]\}.$$

where the supremum is taken over all cheating strategies for Bob, which can be computationally unbounded.

- *The cheating probability of the protocol is defined as* $P^*_{QBC} = \max\{A^*_{QBC}, B^*_{QBC}\}$

There are actually other interesting variants for the binding property, such as the CDMS-binding property [CDMS04] or the collapse-binding property[Unr16] which are more suited for a cryptographic setting. Since we are only interested in the stand-alone unconditional security without considering composability issues, we stick to the sum-binding definition.

In order to relate best cheating strategies for QBC and QROT, we use a standard construction that builds a QBC protocol from a QROT protocol.

QBC via QROT

1. *Commit phase*: Alice wants to commit to a bit b. Alice and Bob perform a QROT protocol so Alice has $(i, y = x_i)$ and Bob has (x_0, x_1). Alice sends $c = b \oplus i$ to Bob.
2. *Reveal phase*: Alice reveals b and $y = x_i = x_{b\oplus c}$ to Bob. Bob checks that $y = x_{b\oplus c}$. He accepts if the condition is satisfied, otherwise he aborts.

Let's compare the cheating probabilities of these 2 protocols. We first have:

$$\begin{aligned} B^*_{\text{QBC}} &= \Pr[\text{Bob guesses } b \text{ after the Commit phase}] \\ &= \Pr[\text{Bob guesses } i \text{ after the Commit phase}] = B^*_{\text{QROT}}. \end{aligned}$$

where the second equality uses the fact that $i = b \oplus c$ and that c is public after the Commit phase. Now, fix a cheating strategy A^* for Alice. For fixed commit phase, notice that Alice successfully reveals b iff. she correctly guessed $x_{b\oplus c}$ (where c is fixed from the commit phase). Therefore, we have

$$\begin{aligned} P^*(A^*) &= \frac{1}{2}\left(\Pr[\text{Alice successfully reveals } b = 0] + \Pr[\text{Alice successfully reveals } b = 1]\right), \\ &= \frac{1}{2}\left(\Pr[\text{Alice guesses } x_0] + \Pr[\text{Alice guesses } x_1]\right) \end{aligned}$$

which gives

$$A^*_{\text{QBC}} = \frac{1}{2}\left(\Pr[\text{Alice guesses } x_0] + \Pr[\text{Alice guesses } x_1]\right).$$

Moreover, we have

$$A^*_{\text{QROT}} = \Pr[\text{Alice guesses } (x_0, x_1)].$$

So we want to relate these 2 quantities, *i.e.* on the one hand the average probability for Alice of learning each bit x_i and on the other hand her probability of learning both bits. This is the first time such a question appeared in my work, a similar question appeared for example in [CSST11], already for bounding the entangled value of 2 player games. In the next section, I will present more formally this kind of statements, as well as generalizations that I made and which were used in several papers of my future work, both for cryptographic applications and for bounding the value of entangled 2 player games.

1.2 Quantum learning in sequence lemmata

Consider the following scenario: Alice has two strings $x_0, x_1 \in \{0,1\}^n$ and Bob has a state ρ_{x_0,x_1} that depends on these two strings. This means Alice and Bob share the state

$$\sum_{x_0,x_1\in\{0,1\}^n} P(x_0,x_1)|x_0,x_1\rangle\langle x_0,x_1| \otimes \rho_{x_0x_1},$$

for some probability function P. Suppose Bob can recover x_0 from his state ρ_{x_0,x_1} with probability p_0 and x_1 from ρ_{x_0,x_1} with probability p_1. What is the probability that he can learn both strings (x_0, x_1)? In order to answer this type of questions, we introduce learning in sequence lemmata. The first one is described below

Lemma 1 (Learning in sequence lemma)**.** *Let $a = \frac{1}{2}(p_0 + p_1)$. If $a \geq \frac{1}{2}$, we have in the above scenario:*

1. *Bob has a measurement that on input ρ_{x_0,x_1} outputs (x_0, x_1) with probability at least $a(2a-1)^2$.*
2. *if x_0, x_1 are bits, Bob has a measurement that on input ρ_{x_0,x_1} outputs $x_0 \oplus x_1$ with probability at least $(2a-1)^2$.*

Sketch. We will not go too deep in the proof of this statement but just present the main idea. Bob being able to guess each x_i with probability p_i means that there exist two quantum POVM measurements $\{M_a^i\}_{a\in\{0,1\}^n}$ for $i \in \{0,1\}$ such that

$$\sum_{x_0,x_1\in\{0,1\}^n} P(x_0,x_1)tr(M_{x_0}^0\rho_{x_0,x_1}) = p_0$$
$$\sum_{x_0,x_1\in\{0,1\}^n} P(x_0,x_1)tr(M_{x_1}^1\rho_{x_0,x_1}) = p_1$$

From these measurements, we construct a 4^n outcome measurement $\{N_{ij}\}_{i,j\in\{0,1\}^n}$ defined as

$$N_{ij} = \frac{1}{2}\left(M_j^1 M_i^0 + M_i^0 M_j^1\right).$$

One can check that this is indeed a valid quantum measurement, which corresponds to the following strategy:

- with probability $\frac{1}{2}$: run M^0 on ρ_{x_0,x_1} to get a guess for x_0 and then M^1 on the resulting state to get a guess for x_1 and output (x_0, x_1),
- with probability $\frac{1}{2}$: run M^1 on ρ_{x_0,x_1} to get a guess for x_1 and then M^0 on the resulting state to get a guess for x_0 and output (x_0, x_1).

In the case of bits, we proved in [CKS10] using geometric arguments that if the $\{M_a^i\}$ are projective measurements, then the probability to output the correct (x_0, x_1) with this strategy is at least $a(2a-1)^2$, where $a = \frac{1}{2}(p_0 + p_1)$. From this result, we then extend to any measurement using Naimark's dilation theorem. We generalize in [SCK14] in the case of strings.

In order to prove the second bullet, where x_0, x_1 are bits, we use the same strategy as above but output $x_0 \oplus x_1$ instead of (x_0, x_1). The advantage we gain in this case is that the guess of $x_0 \oplus x_1$ can be correct when both values of x_0, x_1 are wrong. The value $(2a-1)^2$ was proven in [SCK14]. □

The idea of the above proof is that if we have a projective measurement that guesses each x_i with high probability then performing one measurement after the other will give a fairly high probability of learning both strings. The difficulty is of course that the first measurement will modify the state and possibly destroy the information about the second string but if p_0, p_1 are high enough, this first measurement will only mildly modify the state.

As a first application, we have, using the notations of the previous section

$$A^*_{\text{QROT}} \geq f(A^*_{\text{QBC}}) \quad \text{with} \quad f(x) = x(2x-1)^2.$$

We used this bound in [CKS10] to relate bounds between quantum oblivious transfer and quantum bit commitment, and showed that $P^*_{\text{QROT}} \geq 0.5852$.[2] But the reason I introduce this topic is that it has many implications for some of my future work. What will be of particular interest in such learning in sequence lemmata is the contraposition of this statement. If Bob has a state ρ_{x_0,x_1} and if we have an upper bound on his probability of guessing (x_0, x_1) or $x_0 \oplus x_1$ (in our setting via non-signalling arguments), then we can upper bound Bob's maximal probability of learning x_0 and x_1 separately. As a first example, we show how to easily recover the entangled value of the CHSH game.

1.2.1 Using a learning sequence lemmata to prove the upper bound on the CHSH game

We start from the standard CHSH game. Alice and Bob receive respective random inputs $x, y \in \{0,1\}$ and win the game if they respectively output a, b such that $a \oplus b = x \cdot y$. Let $\omega^*(\mathsf{CHSH})$ be the entangled value of CHSH, *i.e.* the maximal winning probability over all quantum strategies of Alice and Bob that can share an entangled state.

We consider a quantum strategy $\mathcal{S}$ for CHSH consisting of a state $|\phi\rangle$ shared between Alice and Bob, a measurement for Alice and a measurement for Bob. Alice receives her input x, performs this measurement and gets an output a. In order to win the CHSH game, Bob, after obtaining his input y, has to output b such that $a \oplus b = x \cdot y$. In other terms:

- If $y = 0$, Bob must output $b = a$, so he must guess a.
- If $y = 1$, Bob must output $b = x \oplus a$ so he must guess $x \oplus a$.

This means that after Alice's measurement, and ignoring her residual quantum state, Alice and Bob share a state of the form

$$\sum_{x,a} P(x,a)|x,a\rangle\langle x,a| \otimes \rho_{x,a},$$

and

$$\Pr[\text{Alice and Bob win CHSH using } \mathcal{S}] = \frac{1}{2}\left(\Pr[\text{Bob guesses } a] + \Pr[\text{Bob guesses } x \oplus a]\right).$$

We know that Bob cannot guess $x = (a \oplus (x \oplus a))$ with probability greater than $\frac{1}{2}$ because of no-signalling. By using the contrapositive of Lemma 1, we have

$$(2\Pr[\text{Alice and Bob win CHSH using } \mathcal{S}] - 1)^2 \leq \frac{1}{2},$$

which implies $\Pr[\text{Alice and Bob win CHSH using } \mathcal{S}] \leq \cos^2(\pi/8)$. Since this is true for any strategy $\mathcal{S}$, this implies $\omega^*(\mathsf{CHSH}) \leq \cos^2(\pi/8)$ and we recover Cirel'son's bound [Cir80]. This shows as well that the second item of Lemma 1 is tight for some values since we recover the optimal entangled value of CHSH.

[2] This is actually quite far from the best known quantum protocol for oblivious transfer, which is $P^*(\text{QROT}) = \frac{3}{4}$ so the optimal value for QROT is still open.

1.2.2 The CHSH_Q game and a generalized learning in sequence in lemma

Let's pick a prime power Q and let's consider a generalization of CHSH on the finite field $\mathbb{F}_Q$, which is defined as follows

CHSH_Q game

- Alice and Bob respectively receive a uniformly random $X \in \mathbb{F}_Q$ and a random $Y \in \mathbb{F}_Q$. They output respectively $A \in \mathbb{F}_Q$ and $B \in \mathbb{F}_Q$.
- They win the game iff. $A + B = X * Y$, where $+, *$ are the addition and multiplication in the field $\mathbb{F}_Q$.

One can see that in the case $Q = 2$, we recover the original CHSH game. A natural question is whether it is possible to bound the entangled value of CHSH_Q using a learning in sequence lemma. First, let's fix an input/output pair (X, A) for Alice and notice that if Bob can give winning outputs for two different inputs Y, Y' then Bob can recover X. Indeed, on input Y, Bob must output $B = X * Y - A$ and on input Y', Bob must output $B' = X * Y' - A$. If these equalities are satisfied, we have

$$X = \frac{(B - B')}{(Y - Y')},$$

where the division is the division in $\mathbb{F}_Q$. Here, it is well defined since $Y \neq Y'$. So for a fixed input/output pair (X, A) for Alice, we can analyse the CHSH_Q game as follows:

- Alice has Q strings $\{B_y\}_{y \in \mathbb{F}_Q}$ where $B_y = X * y - A$.
- Bob has a random input $Y \in \mathbb{F}_Q$ and they win the game iff. he guesses B_Y.
- Bob's probability of guessing any pair $(B_Y, B_{Y'})$ for $Y \neq Y'$ (on average on the pair (X, A)) is at most $\frac{1}{Q}$ since this pair allows him to guess X, which happens with probability $\frac{1}{Q}$ from no-signalling.

This scenario is similar to the case of CHSH but Alice has more than 2 strings so we can't apply Lemma 1. In [CL17] we proved a more general learning in sequence lemma that deals with this setting

Lemma 2. *Assume Alice has any Q strings $B_1, \dots, B_Q$ and Bob has a state $\rho_{B_1,\dots,B_Q}$. Let*

$$V = \mathbb{E}_{i \in [Q]} \left[\textit{maximum probability that Bob can guess } B_i \textit{ from } \rho_{B_1,\dots,B_Q} \right]$$
$$E = \mathbb{E}_{i,j \neq i \in [Q]} \left[\textit{maximum probability that Bob can guess } (B_i, B_j) \textit{ from } \rho_{B_1,\dots,B_Q} \right]$$

We have $E \geq \frac{1}{64} \left(V - \frac{1}{Q} \right)^3$.

From this generalized lemma, one can get an upper bound on the entangled value CHSH_Q. Indeed, from the above discussion, and using a similar argument as the one for bounding the entangled value of CHSH, we have

$$\frac{1}{Q} \geq \frac{1}{64} \left(\omega^* \left(\mathsf{CHSH}_Q \right) - \frac{1}{Q} \right)^3,$$

which implies

$$\omega^*(\mathsf{CHSH}_Q) \leq \frac{1}{Q} + \frac{4}{Q^{1/3}}.$$

1.3 General bounds on entangled games using learning in sequence lemmata

We want to generalize the above approach to bound the value of some entangled games. In the above, the bound on the $\omega^*(\mathsf{CHSH}_Q)$ comes from a strong bound on winning the game when Bob gets simultaneously two different inputs and then using our learning in sequence lemma to bound $\omega^*(\mathsf{CHSH}_Q)$. In order to generalize this approach, we first formally present several definitions related to entangled games.

Definition 1.3. *A 2-player game $G = (I_A, I_B, O_A, O_B, V, p)$ is defined by finite input and output sets I_A, I_B and O_A, O_B as well as an accepting function $V : O_A \times O_B \times I_A \times I_B \to \{0, 1\}$ and a probability function $p : I_A \times I_B \to \mathbb{R}_+$.*

While our results can be slightly more general, we restrict our presentation here to 2-players games with inputs taken uniformly at random from their input set.

Definition 1.4. *A game $G = (I_A, I_B, O_A, O_B, V, p)$ is said to be on the uniform distribution iff. $p(x, y) = \frac{1}{|I_A||I_B|}$ for any $(x, y) \in I_A \times I_B$.*

In our argument for bounding $\omega^*(\mathsf{CHSH}_Q)$, we used the property that for any input/output pair (x, a) for Alice and for any input y for Bob, there was at most (here actually a unique) b such that $V(x, y, a, b) = 1$. A game with this property is called a projective game and is an important requirement for our argument.

Definition 1.5. *A game $G = (I_A, I_B, O, V, p)$ is a* projection game *if $\forall (x, y) \in I_A \times I_B$ and $\forall a \in O_A$, $|\{b : V(a, b, x, y) = 1\}| \leq 1$.*

We also propose a relaxation of the above definition

Definition 1.6. *A game $G = (I, O, V, p)$ is S-projective if $\forall (x, y) \in I_A \times I_B$ and $\forall a \in O_A$, $|\{b : V(a, b, x, y) = 1\}| \leq S$.*

In our bounds for CHSH and CHSH_Q, we crucially used the fact that it was hard for Bob to win when getting simultaneously 2 different inputs. This motivates the following definition of G_{coup}, which is the game G where Bob gets a couple of different inputs and must give a valid output separately for each one of them.

Definition 1.7. *For any game $G = (I_A, I_B, O_A, O_B, V, p)$ on the uniform distribution we define $G_{coup} = (I_A, (I_B \times I_B), O_A, (O_B \times O_B), V_{coup}, p_{coup})$ where:*

- *$p_{coup}(x, y, y') = \frac{1}{|I_A||I_B|(|I_B|-1)}$ for any $(x, y, y') \in I_A \times I_B \times I_B$ such that $y \neq y'$.*
- *$V_{coup}(a, b, b', x, y, y') = 1$ iff. $V(a, b, x, y) = 1 \wedge V(a, b', x, y') = 1$.*

We can now present our main statements, which were proven in [CL17] and which follow from Lemma 2

Proposition 1.1. *Let $G = (I_A, I_B, O_A, O_B, V, p)$ be a projective game on the uniform distribution.*

$$\omega^*(G_{coup}) \geq \frac{1}{64}\left(\omega^*(G) - \frac{1}{|I_B|}\right)^3,$$

which implies

$$\omega^*(G) \leq \frac{1}{|I_B|} + 4\left(\omega^*(G_{coup})\right)^{1/3}.$$

We also show how to extend this result to the case G is S-projective

Proposition 1.2. *Let $G = (I_A, I_B, O_A, O_B, V, p)$ be an S-projective game on the uniform distribution.*

$$\omega^*(G_{coup}) \geq \frac{1}{64S}\left(\omega^*(G) - \frac{1}{|I_B|}\right)^3,$$

which implies

$$\omega^*(G) \leq \frac{1}{|I_B|} + 4\left(S \cdot \omega^*(G_{coup})\right)^{1/3}.$$

These bounds will be very important to prove the security of relativistic protocols in cryptography, which is the topic we will cover in the next two chapters.

Chapter 2

Relativistic cryptography

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

The idea of using the NSS principle for cryptographic protocols originated in a work by Kent in 1999 [Ken99] as a way to physically enforce a no-communication constraint between the different agents of one party (the idea of splitting up a party into several agents dates back to [BOGKW88], but without any explicit implementation proposal). The original goal of Kent was to bypass the no-go theorems for quantum bit-commitment [May97, LC97].

The original idea of [BOGKW88] was revisited by Crépeau *et al.* in [CSST11] (see also [Sim07]) in order to construct a relativistic bit (and string) commitment. In this chapter, I will present this relativistic bit commitment scheme and show how to construct a relativistic zero-knowledge protocol for the Hamiltonian Cycle problem, which is NP-complete. In order to prove the security of these schemes against quantum adversaries, we will have to bound the entangled value of some two-player games, which we do using the tools of the previous chapter.

2.1 Relativistic string commitment

Recall the definitions of bit-commitment from Section 1.1. Alice wants to commit to a bit $d \in \{0, 1\}$ and Bob wants to make sure that Alice doesn't change her mind when she reveals this bit d. The idea here is that we split Alice (resp. Bob) into 2 agents $\mathcal{A}_1, \mathcal{A}_2$ (resp. $\mathcal{B}_1, \mathcal{B}_2$). The 2 agents for Alice cooperate as do the 2 agents for Bob. We will add some location/timing constraints such that $\mathcal{A}_1$ and $\mathcal{A}_2$ cannot communicate with each other during the protocol (and the same for $\mathcal{B}_1$ and $\mathcal{B}_2$). We detail these spacetime constraints after the description of the protocol.

Simard's Relativistic Bit Commitment Protocol

1. *Preparation phase*: $\mathcal{A}_1, \mathcal{A}_2$ share a random string $a \in \mathbb{F}_Q$. Here, Q is a prime power and $\mathbb{F}_Q$ refers to the Galois field of order Q. $\mathcal{A}_1, \mathcal{A}_2$ also know the bit d they want to commit to.
2. *Commit phase*: $\mathcal{B}_1$ sends a random $b \in \mathbb{F}_Q$ to $\mathcal{A}_1$, who returns $y = a + (d * b)$, where $+, *$ are the addition and multiplication in $\mathbb{F}_Q$.
3. *Reveal phase*: $\mathcal{A}_2$ reveals d and a to $\mathcal{B}_2$. $\mathcal{B}_1, \mathcal{B}_2$ share their information with each other and check that $a = y + (b * d)$.

This protocol is illustrated in the figure below.

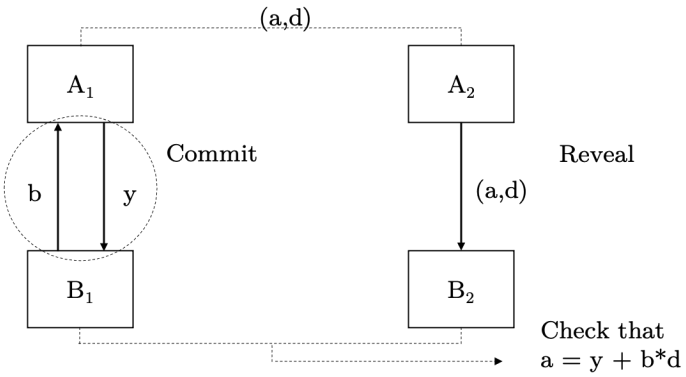

Figure 2.1: The relativistic $\mathbb{F}_Q$ bit commitment

After the commit phase, Bob (here $\mathcal{B}_1$) has the string $y = a + (b * d)$. Because a is random he has no information about d and the protocol is perfectly hiding. In order to prove the binding property of the protocol against cheating Alice, we need to add timing constraints:

Timing constraints for the protocol. The two pairs $(\mathcal{A}_1, \mathcal{B}_1)$ and $(\mathcal{A}_2, \mathcal{B}_2)$ are such that $\mathcal{B}_1$ and $\mathcal{B}_2$ are at a certain distance D. We want to add space-time constraints so that the message (a, d) $\mathcal{B}_2$ receives is independent of the string b sent by $\mathcal{B}_1$. Let t_1 be the time where $\mathcal{B}_1$ sends b and let t_2 the time where $\mathcal{B}_2$ receives (a, d). If

$$t_2 - t_1 < Dc, \text{ where } c \text{ is the speed of light in a vacuum}$$

then the no superluminal signalling ensures that (a, d) is independent of b. This statement will allow us to prove the unconditional security of this scheme against cheating Alice. Notice that the timing and distance constraint are only on the $\mathcal{B}_1, \mathcal{B}_2$ which are honest when analysing the binding property.

Binding property We now want to analyse Alice's cheating possibilities in this bit commitment scheme. As per Definition 1.2, we fix a commit phase and look at the probabilities for Alice to reveal $d = 0$ and $d = 1$. We fix therefore the strings (b, y). Now, if $\mathcal{A}_2$ wants to reveal $d = 0$, she has to send $a = y$ and if he wants to reveal $d = 1$, he has to reveal $a = y + b$. Notice that $\mathcal{A}_2$

knows both y and $y+b$, then she can recover b which happens with probability at most $\frac{1}{Q}$ from no-signalling - here enforced by the space-time constraints. We therefore have

Proposition 2.1. *Alice's cheating probability P_A^* for the binding property satisfies*

$$P_A^* \leq \frac{1}{2} + \frac{1}{\sqrt{2Q}}.$$

Proof.

$$\begin{aligned} P_A^* &= \frac{1}{2}\left(\Pr[\mathcal{A}_2 \text{ successfully reveals } d=0] + \Pr[\mathcal{A}_2 \text{ successfully reveals } d=1]\right) \\ &= \frac{1}{2}\left(\Pr\left[\mathcal{A}_2 \text{ guesses } y\right] + \Pr\left[\mathcal{A}_2 \text{ guesses } y+b\right]\right). \end{aligned}$$

We know from non-signalling that $\mathcal{A}_2$ can guess b with probability $\frac{1}{Q}$. Therefore, by using Lemma 1, we have

$$\frac{1}{Q} \geq P_A^*(2P_A^* - 1)^2,$$

which implies $P_A^* \leq \frac{1}{2} + \frac{1}{\sqrt{2Q}}$. □

Another way to look at this statement is that the above probability is exactly the probability for $\mathcal{A}_1$ and $\mathcal{A}_2$ to win the $\mathsf{CHSH}_{Q,2}$ game, defined below:

$\mathsf{CHSH}_{Q,2}$ game

- $\mathcal{A}_1$ receives a random string $b \in \mathbb{F}_{\mathsf{Q}}$, $\mathcal{A}_2$ has a random bit $d \in \{0,1\}$. They output respectively $y \in \mathbb{F}_Q$ and $a \in \mathbb{F}_Q$.
- They win the game iff $a = y + b * d$.

Here, Bob acts as a referee. One can notice that analysing Alice's cheating probability can be done by bounding the entangled value fo the above game. This means $P_A^* \leq \omega^*(\mathsf{CHSH}_{Q,2})$ and we have $\omega^*(\mathsf{CHSH}_{Q,2}) \leq \frac{1}{2} + \frac{1}{\sqrt{2Q}}$ using our first learning in sequence lemma. Notice also that this is quite efficient since the amount of communication between the players is $O(\log(Q))$.

One could ask here why is $d \in \{0,1\}$ chosen at random in the entangled game while it is chosen by Alice in the commitment scheme. The thing is that the entangled game is only here to analyse the case where Alice is cheating so according to the binding security definition, there isn't a bit d they want to commit to, rather the binding property asks to quantify the probability that Alice can reveal respectively $d=0$ and $d=1$ after a fixed commit phase, and this translates to choosing d uniformly at random in the entangled game.

2.2 Relativistic zero-knowledge for NP

The above results are promising for relativistic cryptography but have a limited scope. Indeed, bit commitment schemes are used as parts of larger cryptosystems. The only study of the composability of the $\mathbb{F}_{\mathsf{Q}}$ bit commitment scheme was done in [FF16], where they used many instances of this commitment scheme in order to increase the time between the commit phase and the reveal phase. There has not been any proposition to use this scheme for a more general purpose.

One natural application of bit commitment are zero-knowledge protocols. In such a protocol, a prover wishes to convince a verifier that a given statement is true without revealing any extra information. A zero-knowledge protocol is already a more advanced cryptographic primitive and has more direct applications such as identification schemes [GMR89].

2.2.1 Blum's protocol for Hamiltonian Cycle

In order to construct a zero-knowledge protocol, we first start from a promise problem $(L_{\text{Yes}}, L_{\text{No}})$ and for a given $x \in L_{\text{Yes}}$, a prover should be able to convince a verifier that $x \in L_{\text{Yes}}$ without conveying any additional information to the verifier. This is formalized by the existence of a polynomial-time simulator that can sample the distribution of transcripts generated during the zero-knowledge protocol. On the other hand, if $x \in L_{\text{No}}$ then even an all powerful prover shouldn't be able to convince the verifier that $x \in L_{\text{Yes}}$.

Here, we will consider the zero-knowledge construction for Hamiltonian Cycle, which is an NP complete problem.

Definition 2.1. *For a graph $G = (V, E)$, the adjacency matrix Adj_G of G is a binary symmetric matrix satisfying $(Adj_G)_{ij} = 1$ iff. $(i, j) \in E$.*

Definition 2.2. *A cycle of a vertex set V is a set $\mathcal{C} \subseteq V \times V$ such that $\mathcal{C} = \{(v_1, v_2), (v_2, v_3), \ldots, (v_{|V|}, v_1)\}$ where $\{v_1, \ldots, v_{|V|}\} = V$.*

Definition 2.3. *A Hamiltonian cycle of a graph $G = (V, E)$ is a cycle $\mathcal{C}$ of V such that $\mathcal{C} \subseteq E$.*

The prover will convince the verifier that a given graph $G = (V, E)$ has a Hamiltonian cycle, *i.e.* a cycle going through each vertex exactly once, without revealing any information, in particular no information about this cycle. Yes instances will correspond to the case where G has a Hamiltonian cycle and No instances to the case where such a Hamiltonian cycle does not exist. Since Hamiltonian Cycle is NP complete, a zero-knowledge protocol for this problem can be used to obtain a zero-knowledge protocol for arbitrary NP problems. There is a known zero-knowledge protocol for Hamiltonian Cycle using bit commitment first presented by Blum [Blu87]. In this protocol, the prover actually runs in polynomial time, and the only advantage he has is that he knows (in some auxiliary input) a Hamiltonian cycle of the graph when we are in a Yes instance.

Zero-knowledge protocol for Hamiltonian Cycle using bit commitment

Input: a graph $G = (V, E)$ containing a Hamiltonian cycle.
Auxiliary input: a Hamiltonian cycle $\mathcal{C}$ of G.

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

This protocol has perfect completeness, meaning that the protocol always succeeds when both parties are honest and we have a Yes instance. It has soundness error $\frac{1}{2}$ if we use a perfect commitment scheme meaning that if G doesn't have a Hamiltonian cycle, a (potentially all powerful) cheating prover can succeed the protocol with probability at most $\frac{1}{2}$. Finally, it is perfectly zero-knowledge (again if we use a perfect commitment scheme) and there exists a simulator that can sample from the transcript distribution of the protocol.

2.2.2 Constructing a relativistic zero-knowledge protocol from a zero-knowledge protocol with commitments.

It is natural to combine this zero-knowledge protocol with the $\mathbb{F}_{\mathsf{Q}}$ relativistic bit commitment protocol. The (single-round) $\mathbb{F}_{\mathsf{Q}}$ relativistic bit commitment protocol is secure against quantum adversaries but it doesn't directly imply that the zero-knowledge protocol remains secure. The generic strategy we use is depicted in the figure below.

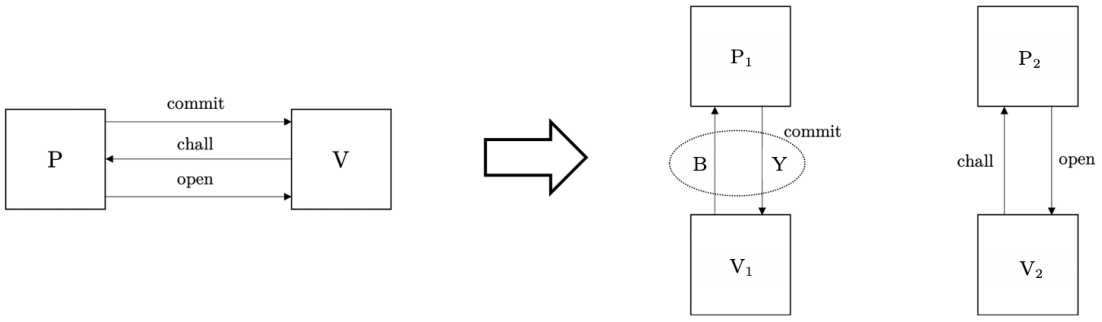

Figure 2.2: On the left: a 3 round zero-knowledge protocol using bit commitment. On the right: the resulting relativistic zero-knowledge using the relativistic $\mathbb{F}_Q$ commitment scheme. The prover splits into P_1, P_2 and the verifier splits into V_1, V_2. The messages B, Y correspond to the commit phase of the $\mathbb{F}_Q$ commitment scheme.

This can be directly applied to the zero-knowledge protocol for Hamiltonian Cycle using the relativistic $\mathbb{F}_Q$ commitment scheme. We obtain the following protocol.

Relativistic zero-knowledge protocol for Hamiltonian Cycle

Input — The provers P_1, P_2 and the verifiers V_1, V_2 are given a graph $G = (V, E)$.
Auxiliary Input — The provers P_1 and P_2 know a Hamiltonian cycle $\mathcal{C}$ of G.
Preprocessing — P_1 and P_2 agree beforehand on a random permutation $\Pi : V \to V$ and on an $n \times n$ matrix $A \in \mathcal{M}_n^{\mathbb{F}_Q}$ where each element of A is chosen uniformly at random in $\mathbb{F}_Q$.
Protocol —

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

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

The zero-knowledge property comes quite directly from the perfect zero-knowledge property of the original scheme for Hamiltonian cycle and the fact that the relativistic bit commitment is perfectly hiding, the interest reader can look at [CL17] for a full proof of the zero-knowledge property.

Soundness, especially against provers P_1, P_2 that can share entanglement, is definitely the most challenging part. We express the soundness as the value of an entangled game, and then bound this value by using the techniques we introduced in the previous chapter. A generic way of doing this of doing this is depicted in Figure 2.3.

In the case of our relativistic protocol for Hamiltonian cycle, the resulting game becomes the following:

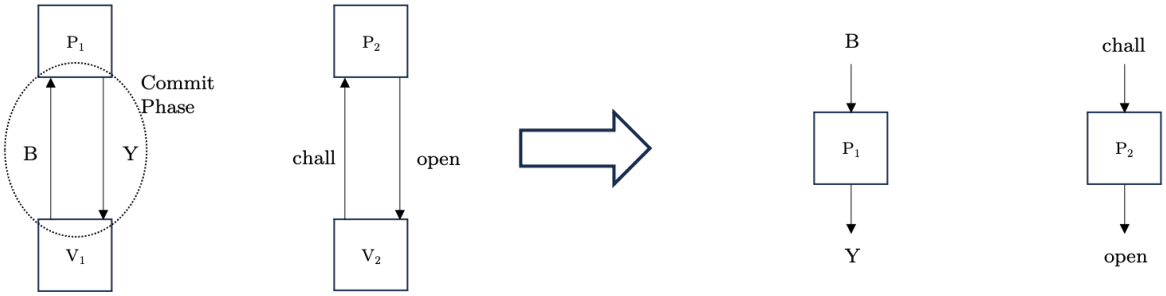

Figure 2.3: On the left: a relativistic zero-knowledge protocol using the $\mathbb{F}_Q$ commitment scheme. On the right: the associated entangled game used to analyse the soundness of the relativistic zero-knowledge protocol. P_1, P_2 are the two players of this entangled game and the verifiers play the role of the referee.

RZK-HAM(G) entangled game played between P_1 and P_2

Public parameter. a graph $G = (V, E)$ with $|V| = n$.
Input. P_1 receives a random $B \in \mathcal{M}_n^{\mathbb{F}_q}$ and P_2 receives a random $chall \in \{0, 1\}$.
Output. P_1 outputs $Y \in \mathcal{M}_n^{\mathbb{F}_q}$. Regarding P_2's output.

- If $chall = 0$, P_2 outputs (Π, A) where Π is a permutation on V and $A \in \mathcal{M}_n^{\mathbb{F}_q}$.
- If $chall = 1$, P_2 outputs a cycle $\mathcal{C}'$ of V and field elements $A_{ij} \in \mathbb{F}_q$ for $(i, j) \in \mathcal{C}'$.

Verification. The verification procedure for the game is the following

- If $chall = 0$, P_1 and P_2 win iff. $\forall i, j \in [n]$, $Y_{ij} = A_{ij} + (B_{ij} * (Adj_{\Pi(G)})_{ij})$.
- If $chall = 1$, P_1 and P_2 win iff. $\forall i, j \in \mathcal{C}'$, $Y_{ij} = A_{ij} + B_{ij}$.

If G contains a Hamiltonian cycle then this game can be won with probability 1 where P_1 and P_2 use the same strategy as in our relativistic zero-knowledge protocol for Hamiltonian Cycle in the honest setting.

If G does not contain a Hamiltonian cycle, then we have the following proposition

Proposition 2.2. *If G does not contain a Hamiltonian cycle, then $\omega^*(RZK\text{-}HAM(G)) \leq \frac{1}{2} + \left(\frac{64n!n^2}{Q}\right)^{1/3}$.*

Proof Sketch. Fix G that doesn't contain a Hamiltonian cycle. Fix any input/output pair (B, Y) for P_1. Notice that when $chall = 0$, for a fixed Π, there is a unique A such that (Π, A) is a winning output for P_2. Similarly, when $chall = 1$, for a fixed $\mathcal{C}$, there is a unique $\{A_{ij}\}_{ij\in\mathcal{C}}$ such that $(\mathcal{C}, \{A_{ij}\}_{ij\in\mathcal{C}})$ is a winning output for P_2. Since there are at most $n!$ possibilities for Π or for $\mathcal{C}$, we conclude that the game is $n!$-projective (where P_2 plays the role of Bob).

Now, we study the coupled game RZK-HAM$(G)_{coup}$. Here, Alice receives $B \in \mathcal{M}_n^{\mathbb{F}_q}$ and Bob receives the two challenges $chall = 0$ and $chall = 1$ (so there is no randomness in his input anymore). Alice outputs some matrix $Y \in \mathcal{M}_n^{\mathbb{F}_q}$ and Bob must give a valid output (Π, A^0) corresponding to challenge 0 and $(\mathcal{C}, A^1)$ corresponding to challenge 1. First notice that there exists $(u, v) \in \mathcal{C}$ such that $(Adj_{\Pi(G)})_{uv} = 0$ or else $\mathcal{C}$ would be a Hamiltonian cycle for $\Pi(G)$ which contradicts the fact that G (hence $\Pi(G)$) has no Hamiltonian cycle.

Now assume that Bob gives outputs that win the game. We have in particular

$$Y_{uv} = A^0_{uv}$$
$$Y_{uv} = A^1_{uv} + B_{uv}$$

which gives $B_{uv} = A^0_{uv} - A^1_{uv}$. This means Bob can guess B_{uv} for pair (u, v) unknown to him. Since the B_{ij} for $(i, j) \in V \times V$ are uniformly random elements of $\mathbb{F}_Q$ unknown to Bob so he can guess one of them with probability at most $\frac{|V|^2}{Q} = \frac{n^2}{Q}$. This means

$$\omega^*(\text{RZK-HAM}(G)_{coup}) \leq \frac{n^2}{Q}.$$

In order to conclude, we can use Proposition 1.2 where recall that RZK-HAM(G) is an $n!$ projective game with challenge size 2 on P_2's side. We therefore obtain

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

□

As a direct corollary, we have if we are in a No instance, cheating provers will be able to cheat with probability at most $\frac{1}{2} + \left(\frac{64n!n^2}{Q}\right)^{1/3}$ in the relativistic zero-knowledge protocol for Hamiltonian Cycle. First notice that the amount of communication is $O(\log(Q)$ so it is fine to take Q exponential in n in order to have the soundness close to $\frac{1}{2}$ and the protocol remains fairly efficient.

In order to decrease the soundness error, there are different possibilities. One could perform parallel repetition, in which case we have to study the game RZK-HAM$(G)^{\otimes k}$. One can show that the entangled value of this game goes to 0 as k increases for example using parallel repetition theorems such as [CS14a, CWY15] or directly using Proposition 1.2. In this case, it is actually enough to perform sequential repetition of this protocol for which bounds are tighter.

If we take $Q = \Theta(n!\mathsf{poly}(n))$, we can achieve soundness $\frac{1}{2} + \frac{1}{\mathsf{poly}(n)}$. We can then decrease this soundness error to $negl(n)$ for example by repeating this protocol n times sequentially. Because we commit to n^2 bits (each bit of a permuted adjacency matrix of G), the total amount of communication at each round is $O(n^2 \log(Q)) = \widetilde{O}(n^3)$. While this is polynomial, this will still be a bit too large in order to be practical, meaning that the communication per round is too large in order to satisfy the space-time constraints. In the next chapter, we present another protocol in order to overcome this issue.

Chapter 3

Relativistic zero-knowledge protocol over the internet

In this chapter, we will be interested in more practical aspects of relativistic zero-knowledge protocols for NP. How realistic are the space-time constraints and how close are we to constructing such a relativistic zero-knowledge protocol? The protocol we presented in the previous chapter manipulates adjacency matrices so we have to perform many $\mathbb{F}_Q$ commitments with a very large Q so the communication that has to be done is too high to ensure the space-time constraints. In [CMS+20], the authors construct a relativistic zero-knowledge protocol for the 3-colouring problem. This protocol is very efficient but because the challenge size is quite large (a random edge of the graph and not a single bit), the analysis against entangled provers is quite cumbersome and the number of repetitions becomes prohibitive if one requires security against entangled provers.

In order to circumvent these issues, we present another proposal for relativistic zero-knowledge for NP based on the Syndrome Decoding problem. This is a problem used in code-based cryptography, and we will use here Stern's zero-knowledge scheme [Ste93] which was used before for post-quantum signature schemes. We then combine it with the $\mathbb{F}_{\mathsf{Q}}$ relativistic string commitment. This protocol will have a moderate amount of communication, but also a small amount of rounds to decrease the soundness error. We also present an implementation of this scheme by looking more carefully into the timing constraints that have to be satisfied. We finally provide at the end of the chapter more details of the pros and cons of these different proposals (see Table 3.1).

3.1 Stern's zero-knowledge protocol for syndrome decoding

The syndrome decoding problem. The Hamming weight $|\mathbf{v}|_H$ of a binary vector $\mathbf{v}$ is the number of 1 coordinates of this vector.

Problem 1 (Syndrome Decoding - SD(n, k, w))**.**

- Instance: *a matrix* $\mathbf{H} \in \{0,1\}^{(n-k)\times n}$*, a column vector (called a syndrome)* $\mathbf{s} \in \{0,1\}^{n-k}$*,*
- Goal: *output a column vector* $\mathbf{e} \in \{0,1\}^n$ *such that* $\mathbf{He} = \mathbf{s}$ *and* $|\mathbf{e}|_H = w$*.*

The Syndrome Decoding problem is NP-complete and also believed to be hard for random instances even against quantum computers. It is the canonical hard problem for code-based cryptography. In order to construct a zero-knowledge protocol for this scheme, we first have to split the instances of our problem into Yes instances and No instances. For the SD(n, k, w) problem, Yes instances are the pairs $(\mathbf{H}, \mathbf{s})$ such that a solution (*i.e.* a vector $\mathbf{e} \in \{0,1\}^n$ such that $\mathbf{He} = \mathbf{s}$ and $|\mathbf{e}|_H = w$) exists. No instances are the pairs $(\mathbf{H}, \mathbf{s})$ where no such solution exists. We

now describe Stern's zero-knowledge protocol [Ste93] for the Syndrome Decoding problem which requires a string commitment scheme.

Again, the protocol is only described in the honest setting, *i.e.* when we have a Yes instance, and the prover has access to a solution $\mathbf{e}$ of the instance in some auxiliary input.

Stern's single round zero-knowledge protocol for SD.

Paramters: Integers n, k, w with $k, w \leq n$
Input: A matrix $\mathbf{H} \in \{0,1\}^{(n-k)\times n}$, a column vector $\mathbf{s} \in \{0,1\}^{n-k}$.
Auxiliary input: A column vector $\mathbf{e} \in \{0,1\}^n$ such that $|\mathbf{e}|_H = w$ and $\mathbf{He} = \mathbf{s}$.
Protocol:

1. The prover picks a random permutation σ acting on $[n]$ and a random column vector $\mathbf{t} \in \{0,1\}^n$. Let $\mathbf{s}' = \mathbf{Ht}$, $z_1 = (\sigma, \mathbf{s}')$, $z_2 = \sigma(\mathbf{t})$, $z_3 = \sigma(\mathbf{t} \oplus \mathbf{e})$, where permuting a vector means permuting its coordinates. He commits to z_1, z_2 and z_3 separately using a string commitment.
2. The verifier sends a uniformly random challenge $c \in \{1, 2, 3\}$.
3. The prover opens $z_{c'}$ for the two values c' different from c.
4. The verifier checks the validity of the 2 commitments and also performs the following checks:
   - if $c = 1$, accept iff. $|z_2 + z_3|_H = w$.
   - if $c = 2$, accept iff. $\mathbf{H} \cdot \sigma^{-1}(z_3) = \mathbf{s} \oplus \mathbf{s}'$.
   - if $c = 3$, accept iff. $\mathbf{H} \cdot \sigma^{-1}(z_2) = \mathbf{s}'$.

Without going into too much detail, let's see what information the verifier has at the end of protocol. If $c = 1$, he has $z_2 + z_3 = \sigma(\mathbf{e})$ so he has a permutation of the solution $\mathbf{e}$ but doesn't know σ. This allows him still to check that the weight of $\mathbf{e}$ is w. The other two challenges are here to ensure that $\mathbf{H}\sigma^{-1}(z_2 + z_3) = \mathbf{s}$ since we should have $\mathbf{H}\sigma^{-1}(z_2 + z_3) = \mathbf{He} = \mathbf{s}$ in the honest case.

Regarding the security against a cheating prover, one can show that the prover cannot answer simultaneously the 3 challenges of the verifier unless he knows a solution to the syndrome decoding problem or unless he can break the binding property of the commitment scheme. This means if we use a perfect commitment scheme, even an all powerful prover can convince a verifier wp. at most $\frac{2}{3}$ in the case the input doesn't have a valid solution $\mathbf{e}$.

3.1.1 Description of our 1-round relativistic zero-knowledge protocol for NP

We combine the $\mathbb{F}_{\mathsf{Q}}$ relativistic string commitment and Stern's single round zero-knowledge protocol in order to get our 1-round relativistic zero-knowledge protocol for SD. Again, $\mathcal{P}$ and $\mathcal{V}$ are split into 2 agents $\mathcal{P}_1, \mathcal{P}_2$ and $\mathcal{V}_1, \mathcal{V}_2$. In the honest case, we require $\mathcal{V}_1, \mathcal{V}_2$ to be at some distance D. We present this protocol in Figure 3.1.

We prove the security of this scheme. Completeness and the zero-knowledge property follow quite directly from the security of Stern's signature scheme and of the $\mathbb{F}_{\mathsf{Q}}$ commitment scheme. Regarding the binding property, we will again need to bound the value of an entangled game, which we call *RZK-SD*. The game is constructed in the same way as we did in the previous chapter (see Figure 2.3).

Input: Integers n, k, w, a matrix $\mathbf{H} \in \{0,1\}^{(n-k)\times n}$, a vector $\mathbf{s} \in \{0,1\}^{n-k}$. A parameter Q used for the commitment.
Auxiliary input (in the Yes case): A column vector $\mathbf{e} \in \{0,1\}^n$ such that $|\mathbf{e}|_H = w$ and $\mathbf{He} = \mathbf{s}$.
Pre-processing: $\mathcal{P}_1, \mathcal{P}_2$ agree beforehand on a random permutation σ acting on $[n]$, on a random column vector $\mathbf{t} \in \{0,1\}^n$ as well as on 3 strings $a_1, a_2, a_3 \in \mathbb{F}_\mathsf{Q}$. Let $s' = \mathbf{Ht}$. Let also $z_1 = (\sigma, \mathbf{s}'), z_2 = \sigma(\mathbf{t}), z_3 = \sigma(\mathbf{t} \oplus \mathbf{e})$, where permuting a vector means permuting its coordinates. Treat each z_i as an element of $\mathbb{F}_Q$ (we choose Q large enough so that we can embed the sets in which z_1, z_2, z_3 are into $\mathbb{F}_\mathsf{Q}$).
Protocol:

1. Phase 1: $\mathcal{V}_1$ sends 3 random strings $b_1, b_2, b_3 \in \mathbb{F}_\mathsf{Q}$ at time τ^1. $\mathcal{P}_1$ sends back $y_i = a_i + b_i * z_i$ for each $i \in \{1,2,3\}$. $\mathcal{V}_1$ receives these at time θ^1.
2. Phase 2: $\mathcal{V}_2$ sends a uniformly random challenge $c \in \{1,2,3\}$ to $\mathcal{P}_2$ at time τ^2. $\mathcal{P}_2$ sends $z_{c'}, a_{c'}$ for the two values c' different from c. $\mathcal{V}_2$ receives these at time θ^2.

Checking procedure: The verifier checks the 2 commitments *i.e.* that $y_{c'} = a_{c'} + b_{c'} * z_{c'}$ for $c' \neq c$, as well as the timing constraints

$$\theta^1 < \tau^2 + D/c \;\; ; \;\; \theta^2 < \tau^1 + D/c.$$

He also performs the following checks that come from Stern's zero-knowledge protocol:

- if $c = 1$, accept iff. $|z_2 + z_3|_H = w$.
- if $c = 2$, accept iff. $\mathbf{H} \cdot \sigma^{-1}(z_3) = \mathbf{s} \oplus \mathbf{s}'$.
- if $c = 3$, accept iff. $\mathbf{H} \cdot \sigma^{-1}(z_2) = \mathbf{s}'$.

Figure 3.1: 1-round Relativistic zero-knowledge protocol for SD using the $\mathbb{F}_\mathsf{Q}$ commitment scheme.

RZK-SD($\mathbf{H}, \mathbf{s}$) game played between P_1 and P_2

- P_1 receives $B = b_1, b_2, b_3 \in_R \mathbb{F}_\mathsf{Q}$. P_2 receives $c \in_R 1, 2, 3$.
- P_1 outputs $Y = y_1, y_2, y_3 \in \mathbb{F}_\mathsf{Q}$ and P_2 outputs $Z = \{(a_{c'}, z_{c'})\}_{c' \neq c}$ where each $a_i \in \mathbb{F}_\mathsf{Q}$. We have $z_1 \in S_1 = P_n \times \{0,1\}^n$, where P_n is the set of permutation on $[n]$ and $z_2, z_3 \in \{0,1\}^n$.
- We first check the constraint $y_{c'} = a_{c'} + z_{c'} * b_{c'}$ for $c' \neq c$. To do this, we embed both S_1 and $\{0,1\}^n$ into $\mathbb{F}_Q$ and we consider the $z_{c'}$ as elements of $\mathbb{F}_Q$. We take Q large enough so that this embedding is always possible. Then:
  1. if $c = 1$, we also require $|z_2 + z_3|_H = w$.
  2. if $c = 2$, we also require $\mathbf{H} \cdot \sigma^{-1}(z_3) = \mathbf{s} \oplus \mathbf{s}'$.
  3. if $c = 3$, we also require $\mathbf{H} \cdot \sigma^{-1}(z_2) = \mathbf{s}'$.

Without going into the full proof of the value of this entangled game, we can give the main ideas. In Stern's protocol the prover isn't able to correctly answer all 3 challenges without breaking the commitment scheme. This will translate into the fact that for a fixed input/output pair, P_2 can give good answers for the 3 challenges at the same with probability at most $\frac{1}{Q}$. In order to use similar arguments as before, we need a learning in sequence lemma that deals with learning triplets of strings and not pairs of strings. In [CB21], we prove the following

Lemma 3. *Assume Alice and Bob share the state*

$$\sum_{x_0,x_1,x_2\in\mathbb{F}_Q} P(x_0,x_1,x_1)|x_0x_1x_2\rangle\langle x_0x_1x_2|\otimes\rho_{x_0x_1x_2},$$

and there exist measurements $\{M_x^i\}$ *for* $i\in\{0,1,2\}$ *that on input* $\rho_{x_0x_1x_2}$*, outputs* x_i *with probability* p_i *and let* $a=\frac{1}{3}(p_0+p_1+p_2)$*. If* $a\geq\frac{2}{3}$ *then there exists a quantum measurement that on input* $\rho_{x_0x_1x_2}$ *outputs* (x_0,x_1,x_2) *with probability* P_T *satisfying*

$$P_T\geq\frac{9}{2}\left(a-\frac{2}{3}\right)^4. \tag{3.1}$$

The proof is actually similar to the case of two measurements (Lemma 1), we consider the measurement

$$N_{x_0,x_1,x_2}=\frac{1}{6}\sum_{\tau\in Perm_{\{0,1,2\}}} M_{x_0}^{\tau(0)}M_{x_1}^{\tau(1)}M_{x_2}^{\tau(2)},$$

where $Perm_{\{0,1,2\}}$ is the set of permutations in $\{0,1,2\}$. By a thorough calculation we can obtain Equation 3.1. Using this, we are able to show that

Proposition 3.1. *For parameters* n,k,w*, if* $(\mathbf{H},\mathbf{s})$ *is a No instance of the syndrome decoding problem, then*

$$\omega^*(RZK\text{-}SD(\mathbf{H},\mathbf{s}))\leq\frac{2}{3}+\left(\frac{2}{9}\cdot\frac{n!2^{4n}}{Q}\right)^{1/4}.$$

The key idea is to use Equation 3.1 combined with the fact that in a No instance, Bob can answer simultaneously to his 3 possible inputs (for a fixed input/output pair for Alice) wp. at most $\frac{1}{Q}$. The $n!2^{4n}$ term comes from the fact that the game is not projective. We refer to the full paper [CB21] for a detailed proof of these different steps. This proposition allows us to prove the following theorem

Theorem 3.1. *Our* 1*-round relativistic zero-knowledge protocol for* NP *based on Stern's protocol has perfect completeness, perfect zero-knowledge and has soundness* $\frac{2}{3}+\left(\frac{2}{9}\cdot\frac{n!2^{4n}}{Q}\right)^{1/4}$ *if the space-time constraints are satisfied.*

This means that for No instances, an all powerful cheating prover can convince the verifier with probability at most $\frac{2}{3}+\left(\frac{2}{9}\cdot\frac{n!2^{4n}}{Q}\right)^{1/4}$. By taking $Q=10^{12}n!2^{4n}$, the soundness becomes smaller than $\frac{2}{3}+0.001$. This seems like a very large Q but recall that sending an element of $\mathbb{F}_Q$ requires $\log_2(Q)$ and performing additions and multiplications in a field of this size is still very efficient.

3.2 Full protocol and implementation

Our full loss-tolerant relativistic zero-knowledge protocol for NP is described in Figure 3.2. We repeat our 1-round protocol R times sequentially and allow for a λ fraction of rounds where the space-time constraints are not satisfied, for eg. because of losses in the signal. We just present the general protocol and the timing constraints

Parameters: (n,k,w) for the SD problem. A parameter Q for the commitment used. A parameter D gives the distance between the 2 verifiers, and a time parameter Δ_T to delimit the time of a round, a time parameter T_{Shift} to determine the time shift between the 2 phases of the protocol. A number of rounds R and an allowed fraction of losses λ.

1. The 2 provers and verifiers agree together on an initial time T_1 on which they start the protocol.
2. For i from 1 to R: run the 1-round relativistic ZK protocol with the $\mathbb{F}_{\mathsf{Q}}$ commitment scheme. $\mathcal{V}_1$ sends his first message at time $\tau_i^1 \triangleq T_1 + (i-1) * \Delta_T$, and $\mathcal{V}_2$ sends his first message at time $\tau_i^2 \triangleq T_1 + (i-1) * \Delta_T + T_{\text{Shift}}$. Let θ_i^1 be the time at which $\mathcal{V}_1$ receives the message from $\mathcal{P}_1$ and θ_i^2 the time at which $\mathcal{V}_2$ receives the message from $\mathcal{P}_2$.
3. At the end of the protocol, the verifiers check the space-time constraints for each i from 1 to R, *i.e.* check that $\theta_i^1 < \tau_i^2 + D/c$ and $\theta_i^2 < \tau_i^1 + D/c$. Let F be the number of rounds where these space-time constraints are not satisfied.
4. The verifiers accept if they accept each iteration of the zero-knowledge protocol when the space-time constraints were satisfied and if $F \leq \lceil \lambda R \rceil$.

Figure 3.2: Full loss-tolerant relativistic zero-knowledge protocol for NP

Timing constraints. We added an extra parameter T_{shift} that will make the space-time constraints easier to satisfy. For round i, let $T_i^{\text{Phase1}} \triangleq \theta_i^1 - \tau_i^1$ and $T_i^{\text{Phase2}} \triangleq \theta_i^2 - \tau_i^2$. In phase 1, $\mathcal{V}_1$ sends 3 strings in $\mathbb{F}_{\mathsf{Q}}$, $\mathcal{P}_1$ does a computation and sends back 3 strings in $\mathbb{F}_{\mathsf{Q}}$. In phase 2, $\mathcal{V}_2$ sends a challenge in $\{1,2,3\}$ and gets back 2 messages in $\mathbb{F}_{\mathsf{Q}}$. This explains why phase 1 is longer than phase 2. The timing constraints become for each i:

$$\theta_i^1 < \tau_i^2 + D/c \quad \Rightarrow \quad T_i^{\text{Phase1}} - T_{\text{Shift}} < D/c \tag{3.2}$$

$$\theta_i^2 < \tau_i^1 + D/c \quad \Rightarrow \quad T_i^{\text{Phase2}} + T_{\text{Shift}} < D/c \tag{3.3}$$

Here, we see why we use T_{Shift}. Since the 2 phases take different times, the first constraint would be harder to achieve than the second one with $T_{\text{Shift}} = 0$. By taking T_{Shift} to be an estimate of $\frac{1}{2}\left(T_i^{\text{Phase1}} - T_i^{\text{Phase2}}\right)$ for an average i, we make the two constraints essentially equally hard to satisfy.

Our two scenarios. We perform a demonstration of this full scheme using only regular laptops as well as standard network links (ethernet or wifi). We run the experiment in 2 different scenarios.

1. $\mathcal{V}_1$ and $\mathcal{P}_1$ are in the same room and are connected through a direct ethernet cable. $\mathcal{V}_2$ and $\mathcal{P}_2$ are in a different location but also connected through an ethernet cable. The distance between $\mathcal{V}_1$ and $\mathcal{V}_2$ is about $400km$
2. $\mathcal{V}_1$ and $\mathcal{P}_1$ (resp. $\mathcal{V}_2, \mathcal{P}_2$) are in different cities and communicate through the usual internet. For each $i, \mathcal{V}_i, \mathcal{P}_i$ are about 400km away. We put $\mathcal{V}_1, \mathcal{V}_2$ at distance about $9000km$.

These scenarios are illustrated by the following, with examples of cities for which these constraints are satisfied, see Figure 3.3.

The authors of [ABC+21] considered the computational problems where the best quantum algorithms run in time 2^{100} so we consider the same setting, which means we have 100 bits of

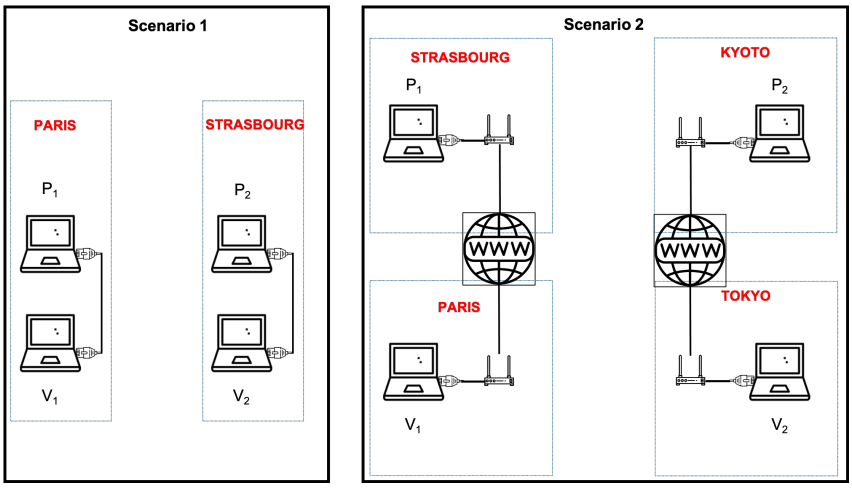

Figure 3.3: Scenarios that we consider for which we demonstrate the feasibility of our full relativistic zero-knowledge protocol for NP.

quantum security. This gives following parameters that appear in the two scenarios.

$$n = 1704,\ k = 769, w = 216$$
$$R = 340, F = 22,\ Q = 2^{23209} - 1$$

Let D be the distance between $\mathcal{V}_1$ and $\mathcal{V}_2$ and let D' be the distance between $\mathcal{V}_1, \mathcal{P}_1$ (and also between $\mathcal{V}_2, \mathcal{P}_2$). Depending on our scenario, we have the following parameters; where $c \approx 299.8km/sec$ in the speed of light in vacuum.

1. Scenario 1: $D = 400km$, $D' = 10m$, $D/c \approx 1.33ms$, $\Delta_T = 2ms$, $T_{shift} = 0.5ms$. With these parameters, the space-time constraints are satisfied for $T_i^{Phase1} < 1.83ms$ and $T_i^{Phase2} < 0.83ms$.

2. Scenario 2: $D = 9000km$, $D' = 400km$, $D/c \approx 30ms$, $\Delta_T = 40ms$, $T_{shift} = 2.5ms$. With these parameters, the space-time constraints are satisfied for $T_i^{Phase1} < 32.5ms$ and $T_i^{Phase2} < 27.5ms$.

We show in Figures 3.4 and 3.5 the real running times of the different phases. With these parameters, we finally manage to show the following:

Theorem 3.2. *In our experiments, the probability that the verifier rejects an honest run of the protocol is* 2^{-102} *(Completeness error), the soundness is* 2^{-103} *and it is perfect zero-knowledge.*

From a theoretical point of view, we present the different parameters of the different relativistic zero-knowledge protocols in Table 3.1, each with its upsides and downsides.

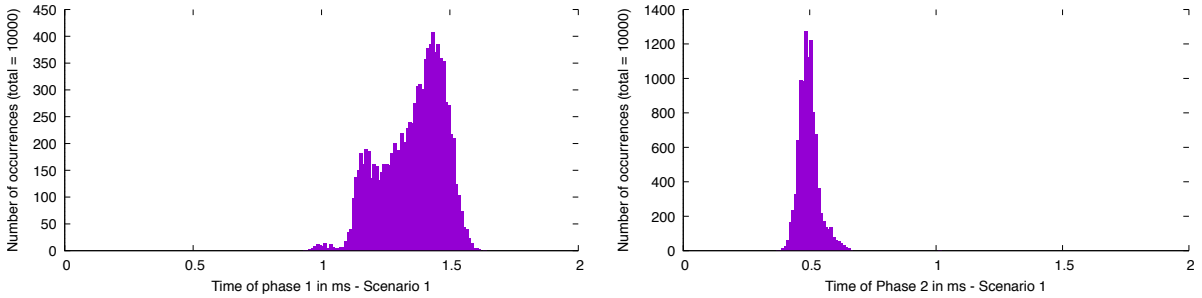

Figure 3.4: T^{Phase1} and T^{Phase2} for Scenario 1 with 10000 rounds, times are aggregated in intervals of size $0.01ms$.

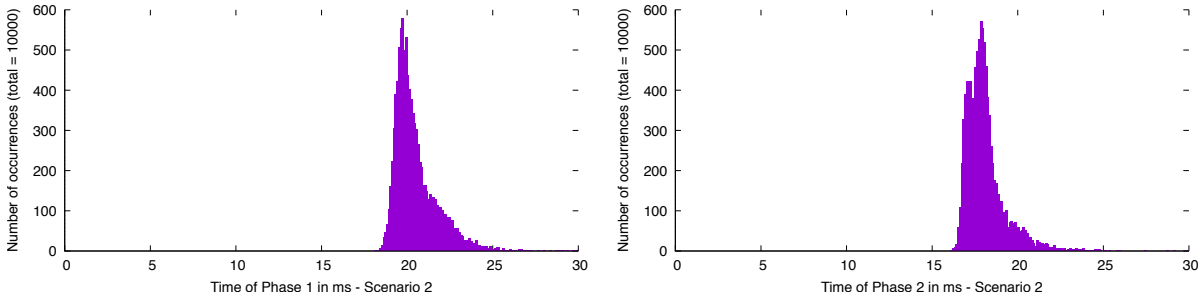

Figure 3.5: T^{Phase1} and T^{Phase2} for Scenario 2 with 10000 rounds, times are aggregated in intervals of size $0.1ms$.

	#Bytes/Round	#Repetitions	# Provers	Quantum Sec
[CL17]	1.89 MB	100	2	✓
[ABC$^+$21]	2 B	10^6	2	×
[ABC$^+$21]	2 B	10^{19}	3	✓
This work	17.03 KB	340	2	✓

Table 3.1: Parameters for different zero-knowledge proposals for 100 security bits.

Chapter 4

Quantum algorithms for the collision problem with small quantum memory

We now start the second part of this thesis, which focuses on quantum algorithms. In this chapter, we study the collision problem where, given a function f, the goal is to find $x \neq y$ such that $f(x) = f(y)$. There are several slight variants of this problem. Here, we consider the case where $f : \{0,1\}^n \to \{0,1\}^m$ is a random function to which we have (quantum) black box access.

The collision problem
Input: a random function $f : \{0,1\}^n \to \{0,1\}^m$ with black box access.
Goal: find $x, y \neq x$ such that $f(x) = f(y)$.

We will be interested both in the time complexity and the query complexity of this problem, and assume a query to the function f takes time 1. The classical and quantum complexity of this problem is very well understood.

Proposition 4.1 (for eg. [vOW99])**.** *There exists a classical algorithm that runs in time $\widetilde{O}(2^{m/2})$ and performs $\widetilde{O}(2^{m/2})$ calls to f that finds a collision in f with high probability.*

Moreover, one can show that we require at least $\Omega(2^{m/2})$ classical queries to f to find a collision so the above algorithm is close to optimal.

Proposition 4.2 ([AS04, Amb05, Zha15])**.** *There exists a quantum algorithm due to Ambanis that runs in time $\widetilde{O}(2^{m/3})$ and performs $O(2^{m/3})$ queries to O_f that finds a collision in f with high probability. Moreover, we require at least $\Omega(2^{m/3})$ queries to f to find a collision so this algorithm is close to optimal.*

This shows a quantum speed-up for the collision problem. However, Ambainis' algorithm requires $O(2^{m/3})$ quantum memory as well as efficient QRAM (Quantum Random Access Memory) operations on registers of size $O(2^{m/3})$. There is however still an ongoing discussion on the feasibility of such operations [JR23]. Notice that this is inherent to quantum algorithms, the classical algorithm of [vOW99] for collision finding only requires $\mathsf{poly}(m)$ memory. Therefore, a natural question arises

> Is it possible to have quantum speed-ups for the collision problem without using QRAM and with minimal quantum resources?

In a joint work with María Naya-Plasencia and André Schrottenloher [CNS17], we positively answer this question for the case $m = n$.

Theorem 4.1. *There exists a quantum algorithm for the collision problem with $m = n$ that runs in time $\widetilde{O}(2^{2m/5})$, performs $\widetilde{O}(2^{2m/5})$ queries to O_f and succeeds with high probability. This algorithm uses $O(m)$ qubits, no* QRAM *operations and $O(2^{m/5})$ classical memory.*

Our main idea is to adapt the quantum algorithm from Brassard, Hoyer and Tapp [BHT98] (hereafter called BHT algorithm) by adding the idea of distinguished points.

4.1 The BHT algorithm and the use of QRAM

We limit our presentation to the case $n = m$. The BHT quantum algorithm for collision finding can be described as follows:

The BHT algorithm

Input: a random function $f : \{0,1\}^n \to \{0,1\}^n$ with black box access to $O_f : |x\rangle|y\rangle \to |x\rangle|f(x) \oplus y\rangle$. The algorithm also has an extra parameter r.

1. Pick a random subset $I \subseteq \{0,1\}^n$ of size 2^r. Construct the list $L = \{f(i)\}_{i \in I}$ and sort it.
2. Let $g : \{0,1\}^n \to \{0,1\}$ satisfying $g(y) = 1 \Leftrightarrow (y \notin I \wedge \exists i \in I, f(y) = f(i))$.
3. Apply Grover's algorithm on g. Find y such that $g(y) = 1$.
4. Find $i \in I$ such that $f(i) = f(y)$. Output (i, y).

Complexity analysis. Constructing and sorting the list L takes time and queries $\widetilde{O}(2^r)$. We then apply Grover's algorithm on g. Grover's algorithm runs in time $O\left(\frac{1}{\sqrt{\varepsilon}}(T_I + T_g)\right)$ where ε is the fraction of solutions, T_I is the time to construct the uniform superposition of inputs (here $\{0,1\}^n$) and T_g is the running time to compute g. This means the total running time is

$$\widetilde{O}(2^r) + O\left(\frac{1}{\sqrt{\varepsilon}}(T_I + T_g)\right) \tag{4.1}$$

In our case, we have ε which is close to $\frac{2^r}{2^n}$ with high probability over the choice of the function f, $T_i = O(n)$ and $T_g = O(n)$ since L is sorted so one can check membership in L using dichotomic search. The total running time becomes

$$\widetilde{O}\left(2^r + \sqrt{\frac{2^n}{2^r}}\right),$$

which gives a running time of $\widetilde{O}(2^{\frac{n}{3}})$ for $r = \frac{n}{3}$.

The use of QRAM **in the BHT algorithm.** A crucial step for making the above time efficient is to be able to efficiently compute the function g. This is why we sort L so that we can perform dichotomic search on the list L and hence efficiently compute g. The efficiency of computing g therefore highly relies on efficient RAM operations of the form

$$RAM(L[0], \ldots, L[|L| - 1], i) \to L[i].$$

This is absolutely fine in the classical setting. However, when we perform Grover's algorithm on g, we have to construct the unitary $O_g : |x\rangle|y\rangle \to |x\rangle|y \oplus g(x)\rangle$. We have a procedure that

efficiently computes O_g given an efficient algorithm for g but if g uses RAM operations then O_g will necessarily use as many QRAM operations which are of the form

$$\text{QRAM} : |i, 0\rangle \to |i, L[i]\rangle \quad \text{with classical access to } L. \tag{4.2}$$

In our example, the size of L is exponential in n and performing this operation efficiently (typically in time $O(\log(|L|))$ seems much more tricky, you need to have somehow a reading head in quantum superposition and read all the list elements in superposition efficiently. While this is not forbidden by the laws of quantum mechanics, it is an additional quantum hardware challenge which might not be ultimately doable.

4.2 Quantum algorithm for collision finding with small quantum memory

We now present our quantum algorithm with little quantum resources. We assume we don't have access to QRAM so how can we compute g? We need, given a classical list L, to construct a quantum unitary $U : |x\rangle|0\rangle \to |x\rangle|\text{“}x \in L\text{”}\rangle$. This can be fairly easily done in time $O(|L|)$ using n qubits. Indeed, for each $i \in \{0, \ldots, |L|-1\}$, put $L[i]$ in a quantum register, test whether it is equal to x and then discard this register. This means that one can construct O_g in time $O(|L|)$ without QRAM but if we plug this in the analysis of the BHT algorithm, all the quantum speed-up is gone, and this for any choice of parameter r.

4.2.1 The idea of distinguished points

To circumvent this issue, our idea was not only to have smaller lists but also better lists *i.e.* lists from which we will find collisions more easily. Let

$$DP_u = \{x : \exists z \in \{0,1\}^{n-u},\ f(x) = \underbrace{0 \ldots 0}_{u \text{ times}} ||z\}$$

be the set of distinguished points with parameter u. The idea is to adapt the BHT algorithm and look for a collision only on inputs which are distinguished points and to construct the list L only using images of distinguished points. This will allow us to find collisions with greater probability while keeping the list L small. More precisely, our algorithm is the following

Algorithm using Distinguished Points

Input: a random function $f : \{0,1\}^n \to \{0,1\}^n$ with black box access to O_f.
Parameters: integers r, u.

1. Find a random subset $I \subseteq DP_u$ of size 2^r using Grover search. Construct the list $L = \{f(i)\}_{i \in I}$.
2. Let $g : DP_u \to \{0,1\}$ satisfying $g(y) = 1 \Leftrightarrow (y \notin I \wedge \exists i \in I, f(y) = f(i))$.
3. Apply Grover on g to find y such that $g(y) = 1$. Calls to g are done without QRAM.
4. Find $i \in I$ such that $f(i) = f(y)$. Output (i, y).

Proposition 4.3. *The above algorithm runs in time and queries*

$$\widetilde{O}\left(2^r 2^{\frac{u}{2}} + \sqrt{\frac{2^{n-u}}{2^r}}\left(2^{u/2} + 2^r\right)\right).$$

In particular, with $r = n/5$ and $u = 2n/5$, the above algorithm runs in time and queries $\widetilde{O}(2^{2n/5})$.

Proof Sketch. The first term corresponds to constructing the list L. Finding a random $x \in DP_u$ takes time and queries $\widetilde{O}(2^{u/2})$ using Grover's algorithm, so constructing the whole list L takes time and queries $\widetilde{O}(2^{r+\frac{u}{2}})$. As in Equation 4.1, the total running time is

$$\widetilde{O}(2^r 2^{\frac{u}{2}}) + O\left(\frac{1}{\sqrt{\varepsilon}}(T_I + T_g)\right).$$

Here, the fraction of solutions is $\varepsilon \approx \frac{2^r}{2^{n-u}}$ with high probability. Moreover, constructing the state $\frac{1}{\sqrt{|DP_u|}} \sum_{x \in DP_u} |x\rangle$ can be done by applying Grover's algorithm (without the final measurement) on the function $h(x) = 1$ iff. $x \in DP_u$. This gives $T_I = \widetilde{O}(2^{u/2})$. Finally $T_g = \widetilde{O}(|L|) = \widetilde{O}(2^r)$. This is the step where we significantly lose from not using QRAM. Putting everything together, we get our result. □

Notice that the above algorithm doesn't use QRAM and uses $O(n)$ qubits. Moreover, the classical memory is the size of the list which is $\widetilde{O}(2^{n/5})$. It is an interesting application of Grover's algorithm where the running T_I is non-trivial.

4.2.2 Variants of the result

The same idea of distinguished points can be used in related scenarios. For example, consider the following problem:

Problem 2 (Multi-target preimage search)**.** *Given access to a random function $f : \{0,1\}^n \to \{0,1\}^n$ and a list $L = \{y_1, \ldots, y_t\}$, where each y_i is a random element of $\{0,1\}^n$. Find $x \in \{0,1\}^n$ and $i \in [t]$ such that $f(x) = y_i$.*

Again, with a small amount of quantum memory and without QRAM, it seems unclear how to solve this problem in time better than $O(2^{n/2})$. Using the idea of distinguished points, we prove the following:

Proposition 4.4. *There exists a quantum algorithm that solves the multi-target preimage search problem on random functions in quantum time T_Q without* QRAM *using M_Q quantum memory and M_C classical memory where*

$$T_Q = \widetilde{O}(2^{n/2-t/6}) + \min(2^t, 2^{3n/7}) \quad ; \quad M_Q = \mathsf{poly}(n) \quad ; \quad M_C = \min\{2^{t/3}, 2^{n/7}\}.$$

We are not going to prove this statement here but once we have the idea of distinguished points, finding this algorithm is fairly easy. The running time T_Q is minimal for $t = \frac{3n}{7}$ and is equal to $2^{3n/7}$. Notice that the complexity here is worst than the one for collision finding. This is because the list L is given to us and we have to extract distinguished points from it, instead of directly constructing a list of distinguished points from the set $\{0,1\}^n$ using Grover's algorithm.

Proposition 4.5 (Searching many collisions.)**.** *Given a random function $f : \{0,1\}^n \to \{0,1\}^n$ on n bits, there exists a quantum algorithm using $O(n)$ qubits and outputting 2^c collisions:*

- *if $c \leq \frac{n}{3}$, in time $\widetilde{O}\left(2^{2n/5+4c/5}\right)$, using $2^{n/5+2c/5}$ classical memory;*
- *if $n \geq c > \frac{n}{3}$, in time $\widetilde{O}\left(2^{n/2+c/2}\right)$, using 2^c classical memory.*

This can be done again with distinguished points only by changing the parameters u and $|L|$. In [CNS17], we also present results on collision finding with multiple quantum processors, as well as applications in the cryptographic setting, which we won't detail here.

4.3 Discussion

Open Problem 1. *Can we solve the collision problem in time $O(2^{n/3})$ for random functions using $poly(n)$ quantum memory? Or on the opposite, can we show a $\Omega(2^{2n/5})$ lower bound for this problem? Or is the optimal algorithm somewhere in between?*

Proving lower bounds for quantum algorithms is already quite challenging, but it seems much harder to prove lower bounds when we limit the quantum resources we allow. I like this open problem because it actually reopens the study of quantum collision algorithms, which we thought was finished since we knew an optimal algorithm with a matching lower bound. Interestingly, there are some lower bounds if we bound both the classical and quantum memory [HM23].

Another interesting question is regarding the worst case scenario, meaning when f has potentially only 1 collision. This problem is more often referred as the element distinctness problem. In this case, BHT type quantum algorithms can solve the problem in time $O(2^{3n/4})$ [BDH$^+$01] while quantum random walks can solve it in time $O(2^{2n/3})$, which is optimal. We didn't manage to use distinguished points to still have quantum speed-ups in this setting with $poly(n)$ quantum memory. It was actually conjectured by Ambainis that this is not possible. This would mean the kind of speed-up we obtain for the collision problem only appears when there are many collisions, as in the case of random functions.

Chapter 5

Quantum lower bounds for permutation symmetric functions

5.1 Introduction

The previous chapter showed new quantum algorithms for the collision problem. In this next chapter, we show how (variants of) generic quantum lower bounds for the collision problem can be used for proving more general limitations for quantum algorithms in the black box model. Here, we will only be interested in query complexity.

More precisely, we will study permutation symmetric functions. There are several ways of defining such functions and we consider the following definitions for a function $f : S \to \{0,1\}$ with $S \subseteq [M]^n$, where $[M] = \{1 \dots, M\}$.

Definition 5.1.

- *f is permutation symmetric of the first type iff.* $\forall \pi \in S_n,\ f(x) = f(x \circ \pi)$.
- *f is permutation symmetric of the second type iff.* $\forall \pi \in S_n,\ \forall \sigma \in S_M,$ $f(x) = f(\sigma \circ x \circ \pi)$.

where S_n (resp. S_M) represents the set of permutations on $[n]$ (resp. $[M]$) and $\circ$ is the usual function composition.

Here, we consider strings $x \in [M]^n$ as functions from $[n] \to [M]$, so

$$x \circ \pi = x_{\pi(1)}, \dots, x_{\pi(n)} \quad ; \quad \sigma \circ x \circ \pi = \sigma(x_{\pi(1)}), \dots, \sigma(x_{\pi(n)}).$$

Notice that functions associated respectively to search, where $f(x) = 1$ iff. $\exists i, f(i) = 1$ and to element distinctness, where $f(x) = 1$ iff. $\exists i, j \neq i$ such that $x_i = x_j$ are permutation symmetric respectively of the first type and of the second type.

We want to relate the randomized query complexity $R(f)$, which corresponds to the minimal amount of classical queries to x required to compute $f(x)$ with probability at least $\frac{2}{3}$ and the quantum query complexity $Q(f)$, which corresponds to the minimal amount of quantum queries to x required to compute $f(x)$ with probability at least $\frac{2}{3}$. Aaronson and Ambainis showed that there is at most a polynomial quantum advantage for permutation symmetric functions of the second type.

Theorem 5.1 ([AA14])**.** *For any permutation symmetric function f of the second type, $R(f) \leq \widetilde{O}(Q^7(f))$.*

In a survey on quantum query complexity and quantum algorithms [Amb17], Ambainis writes: *"It has been conjectured since about* 2000 *that a similar result also holds for f with a symmetry of the first type."* In [Cha19], we answer Ambainis' conjecture and prove the following theorem

Theorem 5.2. *For any permutation symmetric function f of the first type, $R(f) \leq O(Q^3(f))$.*

This result not only proves Ambainis' conjecture, but also improves the exponent from 7 to 3. In the case where $M = 2$, this result was already known [AA14] with an exponent of 2, which is tight from Grover's algorithm. The proof technique is arguably simple, constructive and relies on the quantum hardness of distinguishing a random permutation from a random function with small range from Zhandry [Zha15]. We now present Zhandry's result and then show how to apply it for our lower bound.

5.2 Zhandry's lower bound for small range functions

We first introduce a few notations. For any function f, let $Im(f)$ be its range (or image).

Query algorithms. A query algorithm $\mathscr{A}^{\mathscr{O}}$ is described by an algorithm that calls another function $\mathscr{O}$ in a black box fashion. We will never be interested in the running time or the size of $\mathscr{A}$ but only in the number of calls, or queries, to $\mathscr{O}$. We will consider both cases where the algorithm $\mathscr{A}^{\mathscr{O}}$ is classical and quantum. In the latter $\mathscr{O}$ will be a quantum unitary. In both cases, we only consider algorithms that output a single bit.

Oracles. We use oracles to perform black box queries to a function. For any function g, $\mathscr{O}_g^{\text{Classical}}$ is a black box that on input i outputs $g(i)$ while $\mathscr{O}_g$ (without any superscript) is the quantum unitary satisfying

$$\mathscr{O}_g : |i\rangle|j\rangle \to |i\rangle|j + g(i)\rangle.$$

Our proof will use a quantum lower bound on distinguishing a random permutation from a random function with small range proven in [Zha15]. Following this paper, we define, for any $r \in [n]$, the distribution D_r on functions from $[n]$ to $[n]$ which can be sampled as follows.

- Draw a random function g from $[n] \to [r]$.
- Draw a random injective function h from $[r] \to [n]$.
- Output the composition $h \circ g$.

Notice that any function f drawn from D_r is of small range, it satisfies $|Im(f)| \leq r$. Let also D_{perm} be the uniform distribution on permutations on $[n]$. Zhandry's lower bound can be stated as follows:

Proposition 5.1 ([Zha15])**.** *There exists an absolute constant Λ such that for any $r \in [n]$ and any quantum query algorithm $\mathscr{B}^{\mathscr{O}}$ performing at most $\lceil \Lambda r^{1/3} \rceil$ queries to $\mathscr{O}$:*

$$\forall b \in \{0,1\},\ \left|\mathbb{E}_{\pi \leftarrow D_{perm}} \Pr[\mathscr{B}^{\mathscr{O}_\pi} \text{ outputs } b] - \mathbb{E}_{C \leftarrow D_r} \Pr[\mathscr{B}^{\mathscr{O}_C} \text{ outputs } b]\right| \leq \frac{2}{27}.$$

This is obtained immediately by combining Theorem 8 and Lemma 1 of [Zha15][1].

[1] Equivalently, this is obtained immediately by combining Lemma 3.2 and Lemma 3.4 from the arXiv version `quant-ph:1312.1027`.

5.3 Presentation of our result

We now present the proof of our main theorem.

Proof Theorem 5.2: We fix a permutation symmetric function f of the first type as well as an algorithm $\mathscr{A}_0$ that computes $f(x)$ with probability at least $\frac{2}{3}$ and making $Q(f)$ queries to O_x. Our goal is to construct a randomized algorithm that performs $O(Q^3(f))$ queries to $O_x^{Classical}$ and outputs $f(x)$ with probability at least $\frac{2}{3}$.

The main idea is the following, we want to replace calls to O_x with calls to $O_{x\circ C}$ for a randomly chosen $C \leftarrow D_r$ with $r = \Theta(Q(f)^3)$. We then show two things: (1) this algorithm will output $f(x)$ with sufficiently high probability and (2) its output can be emulated with a randomized classical algorithm performing r queries to x. More in detail, the argument is the following:

1. We first amplify the success probability of $\mathscr{A}_0^{O_x}$ to $\frac{20}{27}$ by repeating this algorithm 3 times and taking the majority vote. This means we have an algorithm $\mathscr{A}^{O_x}$ performing $3Q(f)$ queries to O_x such that

$$\Pr\left[\mathscr{A}^{O_x} \text{ outputs } f(x)\right] \geq \frac{20}{27} \tag{5.1}$$

2. Notice that f is permutation symmetric so $f(x) = f(x \circ \pi)$ for any permutation π. In particular, this gives us

$$\mathbb{E}_{\pi \leftarrow D_{\text{perm}}} \Pr\left[\mathscr{A}^{O_{x\circ\pi}} \text{ outputs } f(x)\right] \geq \frac{20}{27} \tag{5.2}$$

3. Notice that $\mathscr{A}^{\mathscr{O}_{x\circ\pi}}$ can be done with $6Q(f)$ calls to $\mathscr{O}_\pi$. Indeed, $\mathscr{A}^{\mathscr{O}_{x\circ\pi}}$ performs $3Q(f)$ to $\mathscr{O}_{x\circ\pi}$ and each such query can be done with 2 queries to $\mathscr{O}_\pi$ using the procedure below

$$|i\rangle|j\rangle|0\rangle \to |i\rangle|j\rangle|\pi(j)\rangle \to |i\rangle|j + (x\circ\pi)(j)\rangle|\pi(j)\rangle \to |i\rangle|j + (x\circ\pi)(j)\rangle|0\rangle,$$

   where we respectively apply $\mathscr{O}_\pi$ on register $(1,3)$, $\mathscr{O}_x$ on registers $(3,2)$ and $\mathscr{O}_\pi^\dagger$ on register $(1,3)$.

4. We replace the choice of a random function π with a random small range function C with parameter $r = \lceil 216Q^3(f)\Lambda^{-3}\rceil$ so that the number of queries $\mathscr{A}^{\mathscr{O}\circ\pi}$ does to $\mathscr{O}_\pi$ (which is $6Q(f)$) is less that $\lceil \Lambda r^{1/3}\rceil$. From Zhandry's lower bound, we have

$$\mathbb{E}_{C\leftarrow D_r} \Pr\left[\mathscr{A}^{O_{x\circ C}} \text{ outputs } f(x)\right] \geq \mathbb{E}_{\pi\leftarrow D_{\text{perm}}} \Pr\left[\mathscr{A}^{O_{x\circ\pi}} \text{ outputs } f(x)\right] - \frac{2}{27} \geq \frac{2}{3}. \tag{5.3}$$

5. Construct a randomized algorithm $\mathscr{B}$ that performs r classical queries to x and has the same output distribution as $\mathscr{A}^{O_{x\circ C}}$. This means, $\Pr[\mathscr{B}^{O_x^{Classical}} \text{ outputs } f(x)] \geq \frac{2}{3}$, which concludes the argument.

We now show how to perform the last step, which is the construction of the classical randomized algorithm for f.

Algorithm $\mathscr{B}^{O_x^{Classical}}$ with the same output distribution as $\mathscr{A}^{O_{x\circ C}}$

a We start from a random function C sampled according to distribution D_r, with $r = \lceil 216Q^3(f)\Lambda^{-3}\rceil$.

b Query $\mathscr{O}_x^{\text{Classical}}$ to get all values x_i for $i \in Im(C)$. This requires $|Im(C)| \leq r$ queries to $\mathscr{O}_x^{\text{Classical}}$. These queries fully characterize the function $x \circ C$, hence the quantum unitary $\mathscr{O}_{x\circ C}$.

c We consider $\mathscr{A}^{\mathscr{O}_{x\circ C}}$ as a quantum unitary circuit acting on t qubits. At each step of the algorithm, we store the 2^t amplitudes. When $\mathscr{O}_{x\circ C}$ is called, we use its representation from step 2 to calculate its action on the 2^t amplitudes. Other parts of $\mathscr{A}^{\mathscr{O}_{x\circ C}}$ are treated the same way. While this uses a lot of computing power, it does not require any queries to $\mathscr{O}_x^{\text{Classical}}$ or $\mathscr{O}_x$ other than those used at step 2.

The last step outputs the same output distribution than the quantum algorithm $\mathscr{A}^{\mathscr{O}_{x\circ C}}$, which means it outputs $f(x)$ with probability at least $\frac{2}{3}$ and performs r queries which implies

$$R(f) \leq r = \lceil 216Q^3(f)\Lambda^{-3}\rceil.$$

□

This concludes the proof of our theorem. Notice that after step 2, it is not possible to just compute $f(x\circ C)$, and try to show that it is equal to $f(x)$ since we don't even always have $x\circ C \in S$. This is yet another example in query complexity where we use the behavior of a query algorithm on inputs not necessarily in the domain of f.

5.4 Conclusion and Follow ups

This result extends the class of functions for which we can show a polynomial relationship between the quantum and the randomized query complexity and improves the polynomial in general for permutation symmetric functions. It was quite surprising to be able to directly prove this result only by using a quantum lower bound for a specific problem, namely distinguishing random small range functions with random permutations, which can be seen as a slight generalization of the collision lower bound.

The first obvious open question is to close the gap between the best known speed-up for permutation symmetric function - which is quadratic - and the cubic lower bound obtained here.

Open Question 1. *Can we show that for permutation symmetric functions,* $R(f) \leq O(Q^2(f))$?

More generally, it seemed that the technique used was very specific to this problem and wouldn't have many other applications. However, this method was used to prove quantum lower bounds for graph properties and more general symmetries [BCG+20].

Chapter 6

Quantum algorithms for lattice problems

6.1 Introduction

In this last chapter, we present quantum algorithms for the Shortest Vector Problem (SVP) for Euclidean lattices. There is an important focus on this problem. First from a complexity point of view, lattice problems have worst-case to average-case reductions [Ajt96] so there are theoretic arguments about the average-case hardness of this problem. Then, Regev presented strong links with the Learning With Errors (LWE) problem and showed how to build cryptosystems from LWE/SVP [Reg05]. These lattice-based cryptosystems are arguably the leading current proposal for post-quantum cryptography. A lattice is defined as follows

Definition 6.1. *Given a basis $B = (\mathbf{b}_1, \dots, \mathbf{b}_m)$ of linearly independent vectors in $\mathbb{R}^d$ the lattice generated by B is defined as $\mathcal{L}(B) = \{\sum_{i=1}^{m} z_i \mathbf{b}_i, z_i \in \mathbb{Z}\}$. For simplicity, we will consider only lattices of full rank i.e. $m = d$.*

The Shortest Vector Problem asks, given a basis B, to find the shortest non-zero vector of $\mathcal{L}(B)$ in Euclidean norm. Of course, if the basis B consisted of orthogonal vectors then the smallest vector of B would give the smallest non-zero vector of $\mathcal{L}(B)$. However, the basis B needn't be orthogonal and that makes the problem much harder.

SVP is a central problem in lattice-based cryptography, and its complexity directly impacts the security of most lattice-based cryptographic schemes. There are two main families of algorithms for SVP: those based on enumeration [FP85, Kan83, Poh81] and those based on sieving [NV08, MV10]. The latter have a much better asymptotic running time — especially with heuristics that improve the analysis of these algorithms — but require a very large amount of memory, sometimes as much as the running time. Despite these strong memory requirements, the current best algorithms for SVP in practice are based on sieving methods[1].

Theorem 6.1 (Best sieving algorithms for SVP,[BDGL16, Laa15])**.** *There exists a classical algorithm that solves SVP in time $2^{0.292d+o(d)}$ and there exists a quantum algorithm that solves SVP in time $2^{0.265d+o(d)}$.*

In a joint work with my student Johanna Loyer [CL21], we provide a new quantum algorithm for SVP with an improved asymptotic complexity.

[1] See https://www.latticechallenge.org/svp-challenge/

Theorem 6.2. *There exists a quantum algorithm that solves SVP in time* $2^{0.257d+o(d)}$.

We also show space-time trade-offs and quantum resource estimates for this algorithm. We first present sieving algorithm and then present our improvements.

6.2 Sieving algorithms.

We describe below a sieving algorithm introduced by Nguyen and Vidick [NV08].

NV-sieve algorithm for SVP

Input: a basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_d)$ that define a lattice $\mathcal{L}(B)$.

Parameter: a real number $\gamma < 1$.

1. We initialize the algorithm with a list L of N lattices points $\mathbf{x}_1, \ldots, \mathbf{x}_N \in \mathcal{L}(B)$ where for each i, $\|\mathbf{x}_i\| \leq R$ for a certain R exponential in d. This can be done for example using Klein's algorithm [Kle00].
2. For each $i, j \neq i$, we construct $\mathbf{y}_{ij} = \mathbf{x}_i - \mathbf{x}_j \in \mathcal{L}(B)$ and compute $\|\mathbf{y}_{ij}\|$.
3. Keep N points $\mathbf{y}_{ij}$ such that $\|\mathbf{y}_{ij}\| \leq \gamma R$ and start this procedure again by replacing R with γR.

We initialize with N large lattice points and perform the above in order to find N smaller points and then we repeat until we find a small lattice point. Such algorithms are extremely hard to analyse but this becomes much simpler using heuristic arguments. In particular, if we assume that the points $\mathbf{x}_1, \ldots, \mathbf{x}_N$ behave as random points on the sphere of radius R, it is much simpler to compute the probability that the points $\mathbf{y}_{ij}$ will be of norm γR. This heuristic argument is justified by numerical simulations and experiments on sieving algorithms [NV08].

Definition 6.2. *In the above algorithm, we say that a pair* $(\mathbf{x}_i, \mathbf{x}_j)$ *reduces or is reducible iff.* $\|\mathbf{x}_i - \mathbf{x}_j\| \leq \gamma R$.

One can show that as $\gamma \to 1$, the probability that a pair $(\mathbf{x}_i, \mathbf{x}_j)$ reduces is $p = \frac{1}{2^{\Gamma d+o(d)}}$ with $\Gamma \approx 0.2075$. If we start from N random points on the sphere, the number of reducible pairs will be on average $p\frac{N(N-1)}{2}$ which means we need to take at least $N = 2^{\Gamma d+o(d)}$ so that we can have at least N reducible pairs after step 3. Typically, we take $\gamma = 1 - \frac{1}{\mathsf{poly}(d)}$. Each sieving step takes time $O(N^2)$ and we have to repeat this $poly(d)$ times in order to get a short vector so the total running is $poly(d)2^{2\Gamma d+o(d)} \approx 2^{0.415d+o(d)}$.

6.3 Locality sensitive filtering

The main idea of sieving algorithms is to start from N lattices points $\mathbf{x}_1, \ldots, \mathbf{x}_N$ and to compute each sum $\mathbf{x}_i - \mathbf{x}_j$ in order to find smaller lattice points. This step takes time $O(N^2)$ and may seem very costly. A natural question to ask is whether it is possible to speed up this process?

Locality sensitive filtering can significantly improve lattice sieving algorithms. Take the sphere of radius R, hereafter denoted $S_d(R)$ and construct a partition $\{F_1, \ldots, F_C\}$ of $S_d(R)$. Each F_i will be called a filter and the idea is to check whether pairs $(\mathbf{x}_i, \mathbf{x}_j)$ reduce only for points in the same filter. We want these filters to satisfy the following two requirements: (1) two random points

in a filter should have a higher probability of reducing than 2 random points on the sphere and (2) determining in which filter a point is should be done efficiently.

A nice solution to this problem presented by[BCDL19] is to use error correcting codes on the sphere $S_d(R)$. They start from a random product code $\mathcal{C} = \{\mathbf{c}_1, \dots, \mathbf{c}_C\}$ on the sphere and the filters will be sets $F_j = \{\mathbf{y} \in S_d(R) : \langle \mathbf{y}, \mathbf{c}_j \rangle \geq \cos(\alpha)\}$ for some parameter α. $C = |\mathcal{C}|$ and α will be parameters that are chosen in particular so that these filters approximately partition the sphere. Random product codes behave similarly to random codes but can be easily decoded so requirement (2) will be satisfied. Moreover, 2 points close to a certain codeword have a higher probability of being close to each other hence (1) will also be satisfied. This construction is illustrated in Figure 6.1. A sieving step with this locality sensitive filtering works as follows

Sieving step with locality sensitive filtering

Input: a list $L = \{\mathbf{x}_1, \dots, \mathbf{x}_N\}$ of lattice points of norm at most R, a parameter $\gamma < 1$.
Goal: construct a list L' of N lattices points ot norm at most γR.

We initialize $L' = \emptyset$.

1. Construct C points $\mathbf{c}_1, \dots, \mathbf{c}_C$ taken from a random product code $\mathcal{C}$ on the sphere $S_d(R)$.
2. For each j, construct $U_j = F_j \cap L = \{\mathbf{x} \in L : \langle \mathbf{x}, \mathbf{c}_j \rangle \geq \cos(\alpha)\}$. To do this, we initialize each $U_j = \emptyset$. Then for each $\mathbf{x} \in L$, we put $\mathbf{x}$ in its corresponding filter(s) U_j. Because we use an efficiently decodable code $\mathcal{C}$, this can be done efficiently for each $\mathbf{x}$ and this whole step can be done in time $\mathsf{poly}(d)|L|$.
3. For each j, for each $\mathbf{x}_k, \mathbf{x}_l \in U_j, \mathbf{x}_l \neq \mathbf{x}_k$, compute $\mathbf{y}_{kl} = \mathbf{x}_k - \mathbf{x}_l$. If $\|\mathbf{y}_{kl}\| \leq \gamma R$, add $\mathbf{y}_{kl}$ to L'.
4. Repeat from step 1 until $|L'| \geq N$.

If we assume that each U_j contains approximately $\frac{N}{C}$ lattice points, we can see that step 3 takes time $O(C(\frac{N}{C})^2) = O(\frac{N^2}{C})$. The drawback of this filtering is that we miss many solutions and have to perform repetitions. Overall, this remains highly beneficial and by optimizing the parameters, we can take the classical running time from $2^{0.415d+o(d)}$ to $2^{0.292d+o(d)}$. In the quantum setting, step 3 is done using Grover's algorithm which improves the whole exponent to $2^{0.265d+o(d)}$.

6.4 The quantum setting

We now present our improved algorithm. We will only focus on step 3 of the above algorithm, which can be seen as solving the following problem:

Step 3 of the above algorithm for fixed j

- Input: lattice points $\mathbf{x}_1, \dots, \mathbf{x}_T \in U_j = F_j \cap \mathcal{L}$.
- Goal: Find all (or most) pairs $\mathbf{x}_u, \mathbf{x}_v \neq \mathbf{x}_u$ such that $\|\mathbf{x}_u - \mathbf{x}_v\| \leq \gamma R$.

As we said, this was done by Laarhoven by using Grover's algorithm. What we show is that performing a second layer of filtering combined with quantum walks can improve this step. We present this at a very high level, and refer to [CL21] for a full presentation of this algorithm.

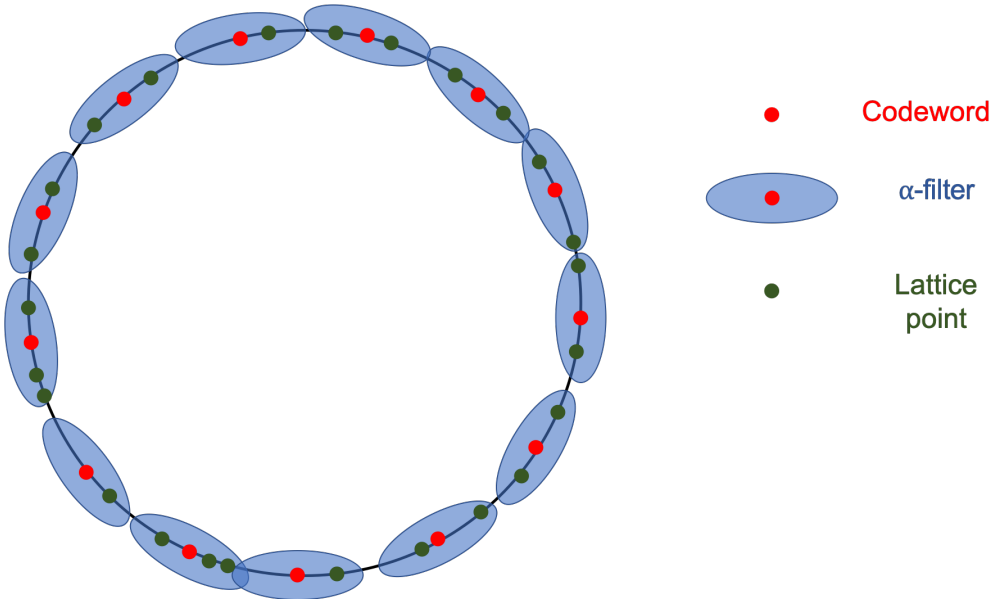

Figure 6.1: Decomposing the sphere S_d into filters

What we do is that we construct a second random product code $\mathcal{C}' = \mathbf{c}'_1, \ldots, \mathbf{c}'_{|\mathcal{C}'|}$ that lies in F_j. We then define new filters $F'_k = \{\mathbf{y} \in F_j : \langle \mathbf{y} | \mathbf{c}'_k \rangle \leq \cos(\beta)\}$ (we do not dive in how we construct the code $\mathcal{C}'$). We define the function $\phi : F_j \to [|\mathcal{C}'|]$ such that $\phi(\mathbf{y}) = k$ iff. $\mathbf{y} \in F'_k$. We assume for simplicity that this function is well defined, *i.e.* there is a unique k such that $\mathbf{y} \in F'_k$, and we choose parameters so that it is approximately the case. Again, we will only search for reducible pairs that are in the same filters, meaning that we search for pairs $\mathbf{x}_u, \mathbf{x}_v$ such that

$$(1) \quad \phi(\mathbf{x}_u) = \phi(\mathbf{x}_v) \quad \text{and} \quad (2) \quad \|\mathbf{x}_u - \mathbf{x}_v\| \leq \gamma R.$$

The first condition is a collision constraint while the second condition is geometrical. We can therefore perform a quantum walk for collision finding: we construct a Johnson graph where each node contains r-tuples $(\mathbf{x}_{u_1}, \ldots, \mathbf{x}_{u_r})$ as well as the values $\phi(\mathbf{x}_{u_1}), \ldots, \phi(\mathbf{x}_{u_r})$. A node will be marked if there is $\mathbf{x}_u, \mathbf{x}_v \neq \mathbf{x}_u$ such that $\phi(\mathbf{x}_u) = \phi(\mathbf{x}_v)$ and $(\mathbf{x}_u, \mathbf{x}_v)$ reduce so the geometrical condition will appear in the definition of marked elements. The update when walking in the Johnson graph is similar to the one for collision finding: when replacing an element $\mathbf{x}_u$ with some $\mathbf{x}_{u'}$, then we just have to compute $\phi(\mathbf{x}_{u'})$ (which can be done efficiently by our code construction) and then update the vertex information. There are a few technicalities here and we refer to the full paper for a detailed presentation of this quantum walk.

Plugging this quantum walk in the quantum sieving algorithm, and for well chosen parameters, we can show that there exists a quantum algorithm for SVP that runs in time $2^{0.257d+o(d)}$. A natural question is why we first perform a classical filtering (to construct the filters F_j) and only within these filters do we perform a quantum walk. Without this first classical filtering, we are in a regime where there is a very large amount of reducible pairs and finding many of them isn't sped up with quantum walks. In our case, the fraction of solutions is much smaller and even though we must repeat the quantum walk to find a constant fraction of marked vertices, we are in a regime where this is helpful.

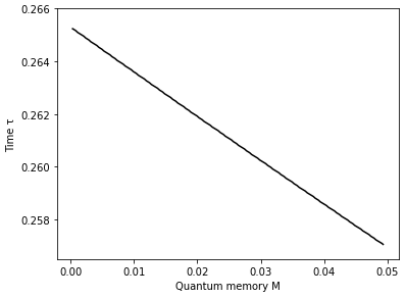

Figure 6.2: Quantum memory-time trade-off.

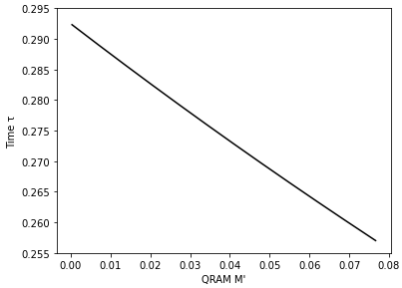

Figure 6.3: QRAM-time trade-off.

6.4.1 Quantum resource estimates and additional results

We now study what are the quantum resources required for our quantum algorithm. In Laarhoven's algorithm, we perform Grover's algorithm on a list of classical stored lattice points, this doesn't require a large amount of quantum memory but it does require QRAM operations on large registers (defined in Chapter 5, Equation 4.2). On the other hand, our algorithm uses quantum walks which require QRAM and quantum memory which could make it harder to implement in practice.

Our framework actually encompasses the best classical and previous quantum algorithms and we can perform full trade-offs between time and quantum memory or between time and QRAM size. These are illustrated by the figures above. We also give examples of values in the table below.

Time $\tau_{M'}$	**0.2925**	0.2827	0.2733	**0.2653**	0.2621	0.2598	**0.2570**
QRAM $\gamma_{M'}$	**0**	0.02	0.04	**0.0578**	0.065	0.070	**0.0767**
Q. memory $\mu_{M'}$	0	0	0	**0**	0.0190	0.0324	**0.0495**
Comment	[BDGL16] alg.			[Laa16] alg.			Thm 6.2

6.5 Discussion and follow-up work

Impact on lattice-based cryptography. Going from a running time of $2^{0.2653d+o(d)}$ to $2^{0.2570d+o(d)}$ slightly reduces the security claims based on the analysis of the SVP (usually via the BKZ algorithm). For example, if one claims 128 bits of security using the above exponent then one must reduce this claim to 124 bits of quantum security. This of course can usually be fixed with a slight increase of the parameters but cannot be ignored if one wants to have the same security claims as before.

Improvements. In our algorithm, we use a quantum walk on a Johnson graph to find reducible pairs. We are in the setting where there are many marked elements (say K) in the graph and we have to find a constant fraction of them. A natural question that arises is whether we have to repeat the whole quantum walk $O(K)$ times to find these marked and this is what we did in this paper. In a joint work with Xavier Bonnetain, André Schrottenloher and Yixin Shen [BCSS23], we showed it was possible to pay the Setup cost of the quantum walk only once in various scenarios including the one of this quantum walk. This slightly improved the quantum running time of this algorithm to $2^{0.2563d+o(d)}$.

Reducing the quantum resources. Another question is whether we can reduce the quantum resources of this algorithm. With Johanna Loyer, we also studied 3 and 4-sieve algorithms [CL23] where we consider triplets and quadruplets of lattice points instead of pairs. This increases the time but reduces the classical and quantum memory requirements.

Bibliography

[AA14] Scott Aaronson and Andris Ambainis. The need for structure in quantum speedups. *Theory of Computing*, 10(6):133–166, 2014.

[ABC+21] Pouriya Alikhani, Nicolas Brunner, Claude Crépeau, Sébastien Designolle, Raphaël Houlmann, Weixu Shi, Nan Yang, and Hugo Zbinden. Experimental relativistic zero-knowledge proofs. *Nature*, 599(7883):47–50, 2021.

[ACG+16] Dorit Aharonov, André Chailloux, Maor Ganz, Iordanis Kerenidis, and Loïck Magnin. A simpler proof of the existence of quantum weak coin flipping with arbitrarily small bias. *SIAM J. Comput.*, 45(3):633–679, 2016.

[Ajt96] Miklós Ajtai. Generating hard instances of lattice problems (extended abstract). In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '96, page 99–108, New York, NY, USA, 1996. Association for Computing Machinery.

[Amb05] Andris Ambainis. Polynomial degree and lower bounds in quantum complexity: Collision and element distinctness with small range. *Theory of Computing*, 1(3):37–46, 2005.

[Amb17] Andris. Ambainis. Understanding Quantum Algorithms via Query Complexity. *ArXiv e-prints*, December 2017. quant-ph: 1712.06349.

[AS04] Scott Aaronson and Yaoyun Shi. Quantum lower bounds for the collision and the element distinctness problems. *J. ACM*, 51(4):595–605, July 2004.

[BBC+21] Ritam Bhaumik, Xavier Bonnetain, André Chailloux, Gaëtan Leurent, María Naya-Plasencia, André Schrottenloher, and Yannick Seurin. QCB: Efficient quantum-secure authenticated encryption. In *Advances in Cryptology – ASIACRYPT 2021, Singapore, December 6–10, 2021*, page 668–698, Berlin, Heidelberg, 2021.

[BC17] Rémi Bricout and André Chailloux. Recursive cheating strategies for the relativistic F_Q bit commitment protocol. *Cryptogr.*, 1(2):14, 2017.

[BCC+23] Gustavo Banegas, Kévin Carrier, André Chailloux, Alain Couveur, Thomas Debris-Alazard, Philippe Gaborit, Pierre Karmpan, Johanna Loyer, Ruben Niederhagen, Nicolas Sendier, Benjamin Smith, and Jean-Pierre Tillich. Wave, 2023.

[BCDL19] Rémi Bricout, André Chailloux, Thomas Debris-Alazard, and Matthieu Lequesne. Ternary syndrome decoding with large weight. In *Selected Areas in Cryptography - SAC 2019 -*, volume 11959 of *Lecture Notes in Computer Science*, pages 437–466. Springer, 2019.

[BCG+20] Shalev Ben-David, Andrew M. Childs, András Gilyén, William Kretschmer, Supartha Podder, and Daochen Wang. Symmetries, graph properties, and quantum speedups. In *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, pages 649–660, 2020.

[BCSS23] Xavier Bonnetain, André Chailloux, André Schrottenloher, and Yixin Shen. Finding many collisions via reusable quantum walks: Application to lattice sieving. In *Advances in Cryptology – EUROCRYPT 2023, Lyon, France, April 23-27, 2023*, page 221–251, Berlin, Heidelberg, 2023.

[BDGL16] Anja Becker, Léo Ducas, Nicolas Gama, and Thijs Laarhoven. New directions in nearest neighbor searching with applications to lattice sieving. *Proc. of the 2016 Annual ACM-SIAM Symposium on Discrete Algorithms*, 2016.

[BDH+01] Harry Buhrman, Christoph Dürr, Peter Høyer, Frédéric Magniez, Miklos Santha, and Ronald de Wolf. Quantum algorithms for finding claws, collisions and triangles. In *Proc. of 16th IEEE Conf. on Computational Complexity*, pages 131–137, 2001.

[BHT98] Gilles Brassard, Peter Høyer, and Alain Tapp. Quantum cryptanalysis of hash and claw-free functions. In Cláudio L. Lucchesi and Arnaldo V. Moura, editors, *LATIN'98: Theoretical Informatics*, pages 163–169, Berlin, Heidelberg, 1998. Springer Berlin Heidelberg.

[Blu87] Manuel Blum. How to prove a theorem so no one else can claim it. In *In: Proceedings of the International Congress of Mathematicians*, pages 1444–1451, 1987.

[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.

[CB21] André Chailloux and Yann Barsamian. Relativistic zero-knowledge protocol for NP over the internet unconditionally secure against quantum adversaries, 2021. quant-ph 2112.01386.

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

[CCL16] Kaushik Chakraborty, André Chailloux, and Anthony Leverrier. Robust relativistic bit commitment. *Phys. Rev. A*, 94:062314, Dec 2016.

[CD20] André Chailloux and Thomas Debris-Alazard. Tight and optimal reductions for signatures based on average trapdoor preimage sampleable functions and applications to code-based signatures. In *Public-Key Cryptography - PKC 2020 - ,Edinburgh, UK, May 4-7, 2020*, volume 12111 of *Lecture Notes in Computer Science*, pages 453–479. Springer, 2020.

[CD24] André Chailloux and Thomas Debris-Alazard. New solutions to delsarte's dual linear programs. *IEEE Transactions on Information Theory*, pages 1–1, 2024.

[CDAE21] André Chailloux, Thomas Debris-Alazard, and Simona Etinski. Classical and quantum algorithms for generic syndrome decoding problems and applications to the lee metric. page 44–62, Berlin, Heidelberg, 2021. Springer-Verlag.

[CDMS04] Claude Crépeau, Paul Dumais, Dominic Mayers, and Louis Salvail. Computational collapse of quantum state with application to oblivious transfer. In Moni Naor, editor, *Theory of Cryptography*, pages 374–393, Berlin, Heidelberg, 2004. Springer Berlin Heidelberg.

[CE23] André Chailloux and Simona Etinski. On the (in)security of optimized stern-like signature schemes. *Des. Codes Cryptogr.*, 92:803–832, 2023.

[CGS16] André Chailloux, Gus Gutoski, and Jamie Sikora. Optimal bounds for semi-honest quantum oblivious transfer. *Chic. J. Theor. Comput. Sci.*, 2016.

[Cha19] André Chailloux. A note on the quantum query complexity of permutation symmetric functions. In Avrim Blum, editor, *10th Innovations in Theoretical Computer Science Conference, ITCS 2019, January 10-12, 2019, San Diego, California, USA*, volume 124 of *LIPIcs*, pages 19:1–19:7. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019.

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

[CKKS14] André Chailloux, Iordanis Kerenidis, Srijita Kundu, and Jamie Sikora. Optimal bounds for parity-oblivious random access codes with applications. In *9th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2014, May 21-23, 2014, Singapore*, volume 27, pages 76–87, 2014.

[CKL17] André Chailloux, Iordanis Kerenidis, and Mathieu Laurière. The information cost of quantum memoryless protocols. *AQIS, Asian Quantum Information Science Conference*, 2017.

[CKS10] André Chailloux, Iordanis Kerenidis, and Jamie Sikora. Lower bounds for Quantum Oblivious Transfer. In *Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2010)*, volume 8 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 157–168, Dagstuhl, Germany, 2010.

[CL17] André Chailloux and Anthony Leverrier. Relativistic (or 2-prover 1-round) zero-knowledge protocol for \mathsf NP secure against quantum adversaries. In *Advances in Cryptology EUROCRYPT 2017, Paris, France, April 30 - May 4, 2017*, volume 10212, pages 369–396, 2017.

[CL21] André Chailloux and Johanna Loyer. Lattice sieving via quantum random walks. In Mehdi Tibouchi and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2021*, pages 63–91, Cham, 2021. Springer International Publishing.

[CL23] André Chailloux and Johanna Loyer. Classical and quantum 3 and 4-sieves to solve SVP with low memory. In Thomas Johansson and Daniel Smith-Tone, editors, *Post-Quantum Cryptography, PQC*, pages 225–255, Cham, 2023. Springer Nature Switzerland.

[CMS+20] Claude Crépeau, Arnaud Y. Massenet, Louis Salvail, Lucas Shigeru Stinchcombe, and Nan Yang. Practical Relativistic Zero-Knowledge for NP. In *1st Conference on Information-Theoretic Cryptography (ITC 2020)*, volume 163 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 4:1–4:18, 2020.

[CNS17] André Chailloux, María Naya-Plasencia, and André Schrottenloher. An efficient quantum collision search algorithm and implications on symmetric cryptography. In *Advances in Cryptology ASIACRYPT 2017, Hong Kong, China, December 3-7, 2017*, volume 10625 of *Lecture Notes in Computer Science*, pages 211–240, 2017.

[CS12] Andre Chailloux and Or Sattath. The complexity of the separable hamiltonian problem. In *Proceedings of the 2012 IEEE Conference on Computational Complexity (CCC)*, CCC '12, page 32–41, USA, 2012. IEEE Computer Society.

[CS14a] André Chailloux and Giannicola Scarpa. Parallel repetition of entangled games with exponential decay via the superposed information cost. In Javier Esparza, Pierre Fraigniaud, Thore Husfeldt, and Elias Koutsoupias, editors, *Automata, Languages, and Programming - 41st International Colloquium, ICALP 2014, Copenhagen, Denmark, July 8-11, 2014, Proceedings, Part I*, volume 8572 of *Lecture Notes in Computer Science*, pages 296–307. Springer, 2014.

[CS14b] André Chailloux and Giannicola Scarpa. Parallel repetition of free entangled games: Simplification and improvements, 2014. quant-ph 1410.4397.

[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.

[CT24] André Chailloux and Jean-Pierre Tillich. The quantum decoding problem. In *TQC 2024, September 9-13, 2024, Okinawa, Japan*, volume 310 of *LIPIcs*, pages 6:1–6:14, 2024.

[CWY15] Kai-Min Chung, Xiaodi Wu, and Henry S. Yuen. Parallel repetition for entangled k-player games via fast quantum search. In David Zuckerman, editor, *30th Conference on Computational Complexity, CCC 2015, June 17-19, 2015, Portland, Oregon, USA*, volume 33 of *LIPIcs*, pages 512–536. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2015.

[FF16] Serge Fehr and Max Fillinger. On the composition of two-prover commitments, and applications to multi-round relativistic commitments. In *Proceedings, Part II, of the 35th Annual International Conference on Advances in Cryptology — EUROCRYPT 2016 - Volume 9666*, page 477–496, Berlin, Heidelberg, 2016. Springer-Verlag.

[FP85] Ulrich Fincke and Michael Pohst. Improved methods for calculating vectors of short length in a lattice. *Mathematics of Computation*, 44(170):463–471, 1985.

[GMR89] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM J. Comput.*, 18(1):186–208, 1989.

[HM23] Yassine Hamoudi and Frédéric Magniez. Quantum time–space tradeoff for finding multiple collision pairs. *ACM Trans. Comput. Theory*, 15(1–2), jun 2023.

[JR23] Samuel Jaques and Arthur G. Rattew. QRAM: A survey and critique, 2023. quant-ph 2305.10310.

[Kan83] R. Kannan. Improved algorithms for integer programming and related lattice problems. *Proceedings of the 15th Symposium on the Theory of Computing (STOC), ACM Press*, pages 99 – 108, 1983.

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

[Kle00] Philip Klein. Finding the closest lattice vector when it's unusually close. In *Proceedings of the Eleventh Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '00, page 937–941, USA, 2000. Society for Industrial and Applied Mathematics.

[Laa15] Thijs Laarhoven. Sieving for shortest vectors in lattices using angular locality-sensitive hashing. In Rosario Gennaro and Matthew Robshaw, editors, *Advances in Cryptology – CRYPTO 2015*, pages 3–22, Berlin, Heidelberg, 2015. Springer Berlin Heidelberg.

[Laa16] Thijs Laarhoven. *Search problems in cryptography, From fingerprinting to lattice sieving.* PhD thesis, Eindhoven University of Technology, 2016.

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

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

[MV10] Daniele Micciancio and Panagiotis Voulgaris. Faster exponential time algorithms for the shortest vector problem. *SODA*, page 1468 – 1480, 2010.

[NV08] P.Q. Nguyen and T. Vidick. Sieve algorithms for the shortest vector problem are practical. *J. Math. Crypt. 2*, pages 181 – 207, 2008.

[OCCG20] Andrea Olivo, Ulysse Chabaud, André Chailloux, and Frédéric Grosshans. Breaking simple quantum position verification protocols with little entanglement, 2020.

[PCDK11] Anna Pappa, Andre Chailloux, Eleni Diamanti, and Iordanis Kerenidis. Practical Quantum Coin Flipping. *Physical Review A*, 84(5):052305, November 2011.

[PCW+12] Anna Pappa, André Chailloux, Stephanie Wehner, Eleni Diamanti, and Iordanis Kerenidis. Multipartite entanglement verification resistant against dishonest parties. *Physical Review Letters*, 108(26):260502, June 2012. 5 pages, added appendix.

[PJL+14] Anna Pappa, Paul Jouguet, Thomas Lawson, André Chailloux, Matthieu Legré, Patrick Trinkler, Iordanis Kerenidis, and Eleni Diamanti. Experimental plug and play quantum coin flipping. *Nature Communications*, page 9, April 2014.

[Poh81] Michael E. Pohst. On the computation of lattice vectors of minimal length, successive minima and reduced bases with applications. *ACM SIGSAMBulletin*, 15(1):37–44, 1981.

[Rab81] Michael O. Rabin. How to exchange secrets with oblivious transfer. In David Zuckerman, editor, *Technical Report TR-81, Aiken Computation Lab, Harvard University*, 1981.

[Reg05] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing*, STOC '05, page 84–93, New York, NY, USA, 2005. Association for Computing Machinery.

[SCK14] Jamie Sikora, André Chailloux, and Iordanis Kerenidis. Strong connections between quantum encodings, nonlocality, and quantum cryptography. *Phys. Rev. A*, 89:022334, Feb 2014.

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

[Ste93] Jacques Stern. A new identification scheme based on syndrome decoding. In *Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '93, page 13–21, Berlin, Heidelberg, 1993. Springer-Verlag.

[Unr16] Dominique Unruh. Computationally binding quantum commitments. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology – EUROCRYPT 2016*, pages 497–527, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg.

[vOW99] Paul C. van Oorschot and Michael J. Wiener. Parallel collision search with cryptanalytic applications. *J. Cryptology*, 12:1–28, 1999.

[Zha15] Mark Zhandry. A note on the quantum collision and set equality problems. *Quantum Info. Comput.*, 15(7-8):557–567, May 2015.