# Quantum XOR and Rabin Oblivious Transfer 

Lara Stroh

Submitted for the Degree of Doctor of Philosophy


Heriot-Watt University<br>Institute of Photonics and Quantum Sciences<br>School of Engineering and Physical Sciences

May 2023

The copyright in this thesis is owned by the author. Any quotation from the thesis or use of any of the information contained in it must acknowledge this thesis as the source of the quotation or information.


#### Abstract

Oblivious transfer is a cryptographic primitive involving two non-trusting communicating parties. Since it is a basic building block for any two-party computation, it is a quite powerful and important cryptographic functionality and thus topic of various research investigations in the classical as well as in the quantum setting. It was unfortunately shown that oblivious transfer can in neither setting be done with information-theoretic security. However, in the quantum case, it is possible to limit the cheating probabilities of unrestricted dishonest parties.

The most well-known variant is 1 -out-of- 2 oblivious transfer, where the sender sends two bits and the receiver receives one of them without the sender learning which one was received. While this has been the primary focus of investigations, there exist other variants of the protocol which have been less studied. This thesis focuses on two such variants, XOR oblivious transfer and Rabin oblivious transfer.

Different quantum protocols for these two variants are presented and analysed for their security against cheating parties. Calculating the cheating probabilities in general for non-interactive XOR oblivious transfer with symmetric states, the optimality of the presented XOR oblivious transfer protocol is shown. Non-interactive means that there is only one state transmission from the sender to the receiver who applies a measurement, and no further communication between the parties. We further extend the concept of XOR oblivious transfer to the sender not sending two but $n$ bits and analyse the effect of an increasing $n$ on the participants' cheating probabilities.

The reversal of oblivious transfer is also looked at; that is, implementing oblivious transfer in both directions even if only one of the two communicating parties can send a quantum state and the other one can only measure. We determine the reversed protocol versions of a 1-out-of-2 and an XOR oblivious transfer protocol and show that the protocols' cheating probabilities remain unchanged.

For Rabin oblivious transfer, both protocols using pure states and protocols using mixed states are investigated. Comparing them to each other, we determine under which circumstances the protocol with the pure states outperforms the protocol with the mixed states and vice versa.


## Acknowledgements

I wish to thank the following people without whom this PhD thesis would not have been possible:

First of all, I would like to thank my supervisor Professor Erika Andersson for her support and advice during the past three and a half years. Thank you for all the helpful discussions and diverse exchanges which gave me a deeper understanding of quantum physics. I always found those discussions and exchanges constructive, enriching, encouraging, and motivating. This was also especially so during the aggravating times of lockdowns and remote working, where the flexible and immediate change to virtual meetings made it possible for me to keep my motivation, to stay on track with my studies, and to now be able to submit this thesis on time.

I also thank Dr Ittoop Puthoor for his scientific support and help during my PhD.
I wish to thank my collaborators at Palacký University Olomouc, Professor Miloslav Dušek, Dr Robert Stárek, Nikola Horová, and Dr Michal Mičuda, for the great and fruitful collaboration on the realisation of quantum communication protocols.

Furthermore, I would like to thank Dr Moritz Cygorek. It was great to have you as my desk neighbour in the office. Our conversations and exchanges about research, work, and university life were enriching

My thanks also goes to my second supervisor Professor Erik Gauger and his group for "adopting" me and including me in their socials. They were, particularly during the lockdowns, relieving and joyful for me.

I certainly wish to thank my friends and family. In particular, I would like to thank my grandfather, Reinhard Novak, who supported and motivated me to take this scientific course of education.

My thanks also goes to Dr Timothy Anderson for his assistance and support during my university years.

Then, of course, a special thank you to my parents, Michaela and Robert Stroh, my brother, Valentin, and my sister, Emily, my grandparents, Rosi and Peter Baller as well as Christl and Roger Stroh, and my great-aunt and great-uncle, Sybille and Toni Heinz, for your continuous support and encouragement. You made this thesis possible.

## Inclusion of Published Works Form

Please note you are only required to complete this form if your thesis contains published works. If this is the case, please include this form within your thesis before submission.

## Declaration

This thesis contains one or more multi-author published works. I hereby declare that the contributions of each author to these publications is as follows:

| Citation details | L. Stroh, N. Horová, R. Stárek, I. V. Puthoor, M. Mičuda, M. Dušek, <br> E. Andersson, Non-interactive XOR quantum oblivious transfer: optimal <br> protocols and their experimental implementations, arXiv:2209.11300 (2022) <br> Accepted/In press in PRX Quantum |
| :--- | :--- |
| Author 1,4,7 | Examined general non-interactive XOT protocols with pure symmetric states, <br> analysed optimal non-interactive XOT protocol, investigated reversal of <br> oblivious transfer and illustrated process on protocols. |
| Author $1,2,3,4,5,6,7$ | Contributed to writing the manuscript. |
| Author $2,3,5,6$ | Designed and performed the experiment. |
| Author 7 | Conceived the research and supervised the project. |


| Citation details | E. Andersson, L. Stroh, I. V. Puthoor, D. Reichmuth, N. Horová, R. Stárek, <br> M. Mičuda, M. Dušek, P. Wallden, Quantum cryptography beyond quantum <br> key distribution: variants of quantum oblivious transfer, in PR Hemmer \& AL <br> Migdall (eds), Quantum Computing, Communication, and Simulation III. vol. <br> 12446, SPIE, SPIE Photonics West 2023, San Francisco, USA (2023) |
| :--- | :--- |
| Author 1, 2, 3 | Examined and analysed the non-interactive XOT protocol, the reversal of <br> oblivious transfer, and the presented reversed protocols. |
| Author 1, 3, 4, 9 | Compared quantum oblivious transfer and random access codes. |
| Author 1 | Contributed to writing the manuscript, conceived the research, and <br> supervised the project. |
| Author 5, 6,7,8 | Designed and performed the experiment. |

## Contents

1 Introduction ..... 1
1.1 Motivation ..... 1
1.2 Thesis Outline ..... 2
2 Background ..... 4
2.1 Oblivious Transfer ..... 4
2.1.1 Different Variants of Oblivious Transfer ..... 5
2.1.2 Impossibility of Unconditional Security ..... 5
2.1.3 Limitations and Restrictions for Improving Security ..... 6
2.1.4 Lower Bounds for Cheating Probabilities ..... 9
2.2 Other Cryptographic Primitives ..... 10
2.2.1 Private Information Retrieval ..... 11
2.2.2 Coin Flipping ..... 12
2.3 Quantum State Elimination ..... 12
3 Non-interactive Quantum XOR Oblivious Transfer ..... 14
3.1 Introduction ..... 14
3.2 Optimal XOT Protocol Using Symmetric Pure States ..... 15
3.2.1 The Protocol ..... 15
3.2.2 Equivalence between Semi-random XOT and Standard XOT ..... 17
3.2.3 Dishonest Bob ..... 21
3.2.4 Dishonest Alice ..... 22
3.2.5 Comparison to a Classical XOT Protocol ..... 26
3.3 Quantum XOT with Symmetric States ..... 27
3.3.1 Bob's Cheating Probability ..... 30
3.3.2 Alice's Cheating Probability without Testing by Bob ..... 31
3.3.3 Alice's Cheating Probability with Testing by Bob ..... 36
3.3.4 Optimal Sets of States ..... 42
3.4 Experimental Implementation ..... 45
3.5 Conclusion ..... 46
4 Reversed Quantum Oblivious Transfer ..... 48
4.1 Introduction ..... 48
4.2 Reversing a 1-out-of-2 OT Protocol ..... 50
4.2.1 Dishonest Receiver ..... 52
4.2.2 Dishonest Sender ..... 52
4.3 Reversing an XOT Protocol ..... 57
4.3.1 Dishonest Receiver ..... 58
4.3.2 Dishonest Sender ..... 59
4.3.3 Experimental Implementation ..... 62
4.4 Classical Post-Processing for Reversed Protocols ..... 63
4.5 Conclusion ..... 65
5 Generalising Quantum XOR Oblivious Transfer ..... 67
5.1 Introduction ..... 67
5.2 1-out-of- $n$ XOR Oblivious Transfer ..... 67
5.3 Non-interactive 1-out-of- $n$ XOT Protocol ..... 70
5.3.1 Dishonest Bob ..... 74
5.3.2 Dishonest Alice ..... 75
5.3.3 Change of Cheating Probabilities with Increasing $n$ ..... 76
5.3.4 Comparison to Classical XOT Protocols ..... 78
5.4 Similarities to Quantum Retrieval Games ..... 80
5.5 Conclusion ..... 82
6 Quantum Rabin Oblivious Transfer ..... 84
6.1 Introduction ..... 84
6.2 Rabin OT Using Pure States ..... 85
6.2.1 The Protocol ..... 85
6.2.2 Dishonest Bob ..... 86
6.2.3 Dishonest Alice ..... 88
6.2.4 Comparison to Classical Rabin OT ..... 100
6.3 Rabin OT Using Mixed States ..... 105
6.3.1 The Protocol ..... 105
6.3.2 Dishonest Bob ..... 107
6.3.3 Dishonest Alice ..... 108
6.3.4 Comparison to Classical Rabin OT ..... 111
6.4 Comparison between Mixed States and Pure States Protocols ..... 112
6.5 Further Generalisation of Rabin OT Protocol Based on Mixed States ..... 114
6.5.1 Security against Alice and Bob ..... 114
6.5.2 Protocol Performance when $P$ (no bit) $=P($ bit $)$ ..... 116
6.6 Conclusion ..... 117
7 Conclusion ..... 119
Bibliography ..... 121

## Chapter 1

## Introduction

### 1.1 Motivation

Secret communication and cryptography have always played a part in people's affairs. There are plenty of examples in recent as well as in ancient history where either successful or failed secret communication played a decisive factor in the development of events [1]. Cryptography is and always has been an ever-evolving field that, due to the many and rapid technological developments in the past century, has not only seen a tremendous change and evolution, but has also become increasingly important and essential for a wider range of users and applications. With the advances of existing and the development of new technologies, new opportunities as well as new threats and security risks arise.

The use of quantum mechanics and its special properties for the development of new technologies has been a major field of study in recent decades [2]. An important area of research is quantum computing which promises, for some tasks, to surpass the performance of classical computing. For example, the quantum computing algorithm called Shor's factoring algorithm can be used to factor an integer into its prime factors [3]. Integer factorisation on classical computers is a very complicated and time-consuming task, which is why this task is called the factorisation problem. The best classical factorisation algorithm currently known takes exponential time, in particular, it takes $O\left(\exp \left((64 / 9)^{1 / 3}(\log n)^{1 / 3}(\log \log n)^{2 / 3}\right)\right)$ to factorise an integer $n$ [4]. Shor's algorithm on a quantum computer, however, only takes polylogarithmic time, in particular, $O\left((\log n)^{2}(\log \log n)(\log \log \log n)\right)[3]$. Therefore, it could resolve the factorisation problem. Since many classical communication and cryptographic protocols base their security on the factorisation problem, quantum computing is a significant threat to such protocols.

To be prepared for the time when quantum computing is an acute risk to these classical protocols, another important area of research, quantum communication/quantum cryptography, has developed. Its aim is to use quantum mechanics
to create communication protocols and develop quantum cryptosystems that provide information-theoretic security, that is, security which cannot be broken by adversaries with unlimited computing power. The most famous quantum communication protocol is quantum key distribution (QKD) [5] which has been the focus of much research. Quantum key distribution is a protocol in which two parties exchange a jointly shared secret key whereby the exchange process is secure against third-party adversaries and can be done with information-theoretic security. QKD is therefore important for any type of symmetric-key cryptography.

In general, the sending of secret messages using encryption and decryption methods is the main notion that comes to mind when thinking of the field of cryptography. This field, however, has developed rapidly and greatly over the last few decades and nowadays includes many topics and concepts other than basic encryption and decryption techniques. With the growth of research in quantum communication, these new concepts are also investigated when including quantum mechanics and its properties.

One of the new topics is the cryptographic primitive called oblivious transfer, a powerful protocol that can be used as basic component to build any two-party computation [6]. Generally, oblivious transfer protocols are for transmitting secrets between two untrusting parties. In particular, the aim is for sender Alice to hold $n \geq 1$ secrets and for receiver Bob to obtain $0 \leq k \leq n$ of them ( $n, k \in \mathbb{N}$ ) without Alice being able to learn which of the secrets Bob has received. There are different variants of oblivious transfer which are specified by $n, k$, and the nature of the secrets, that is, are they for example single bits or XORs of several bits or strings of bits.

In this work, we look at different variants of quantum oblivious transfer and investigate more general as well as specific protocols for these variants. Analysing their performance and security, we can identify optimal protocols and compare the quantum protocols to their classical counterparts.

### 1.2 Thesis Outline

In the next chapter, Chapter 2, we provide the background for the work. We outline the research in oblivious transfer and explain the concept of quantum state elimination, a measurement that will be repeatedly used in the quantum oblivious transfer protocols in the following chapters. Furthermore, we briefly mention and describe a few examples of cryptographic primitives other than oblivious transfer.

Chapter 3 covers non-interactive XOR oblivious transfer protocols. We first
present and analyse a specific such protocol that uses symmetric pure states. Continuing on to considering quantum XOR oblivious transfer protocols with symmetric states in general and deriving the communicating parties' cheating probabilities, we can show that the former protocol is actually optimal within the considered framework.

Chapter 4 deals with the reversal of oblivious transfer protocols. Introducing the concept at first, we then illustrate it by reversing two example protocols. These protocols are the 1-out-of-2 oblivious transfer protocol presented by Amiri et al. [7] and the optimal XOR oblivious transfer protocol investigated in Chapter 3.

In Chapter 5, we generalise the XOR oblivious transfer definition to 1 -out-of$n$ XOR oblivious transfer. Presenting an outline for a non-interactive 1-out-of- $n$ XOR oblivious transfer protocol, we analyse it for its security against dishonest communicating parties and for the effect of increasing $n$. We briefly discuss observed similarities between 1-out-of- $n$ XOR oblivious transfer and the notion of quantum retrieval games.

Chapter 6 focuses on another variant of oblivious transfer called Rabin oblivious transfer. At first, we consider and analyse protocols which use pure states, followed by looking at a protocol using mixed states. We directly compare these two Rabin oblivious transfer protocols, investigating if one of them has a security advantage over the other one.

## Chapter 2

## Background

### 2.1 Oblivious Transfer

Oblivious Transfer (OT) is an important cryptographic primitive. The first time such a general process was described was by Wiesner in [8] who, at the same time, also initiated quantum cryptography with this paper. Assuming we have two communicating parties, Wiesner described a method whereby one party can send two different messages using varying polarizations to another party who can receive only one of these depending on the way the analysers are set up. While he had already written about this method, that he called "quantum multiplexing", around 1970, the paper was not published until 1983 [9]. By that time, the oblivious transfer process had already been discussed independently by Rabin [10]. His specific type of oblivious transfer is now known as Rabin OT and describes a particular protocol situation. In this situation, Alice sends some information to Bob and Bob then either learns the information or he does not learn anything while Alice will not know which of the two cases has occurred. A few years later, Even et al. [11] presented another type of OT, the 1-out-of-2 oblivious transfer (1-2 OT). In such a protocol, Alice sends two bits of information to Bob. While Bob learns one and only one of these, Alice stays ignorant of which one he has obtained. It is apparent that this type resembles the general description of Wiesner's "quantum multiplexing".

The oblivious transfer primitive is often integrated as a subprotocol in other, more extensive protocols. Rabin [10], for example, used OT in one step of the exchange of secrets protocol he introduced and Even et al. [11] implemented it in order to perform a contract signing protocol. Consequently, the importance of oblivious transfer for multi-party computations became apparent. It was Kilian [6] who proved that any two-party computation can actually be implemented with oblivious transfer as a basic building block, i.e. OT is universal.

### 2.1.1 Different Variants of Oblivious Transfer

Further development of the primitive of oblivious transfer has led to various specifications and generalisations of oblivious transfer. Hence, there exist several different variants in addition to the previously mentioned 1-out-of-2 OT and Rabin OT, which, due to the fact that here the receiver either receives something or nothing, is also called all-or-nothing OT. To mention but a few, there are variations such as 1-out-of-n OT where one of $n$ potential secret information is transmitted to Bob while keeping Alice ignorant of which one it is [12], or 1-out-of-2 string OT where Alice's secret information are not single bits but strings of several bits length (discussed, for instance, in Ref. [13]). There is also Generalised OT in which Alice's two secret bits are used as inputs for a one-bit function and Bob decides which of the potential one-bit functions (Boolean functions) he wants to learn the value of while he stays ignorant of the input bits themselves and Alice does not learn which function he chose [13]. Another variation of OT that has been defined and played a role in the literature, is XOR oblivious transfer (XOT). XOT extends the regular 1-out-of-2 OT by also including the exclusive-or (XOR) of the transmitted bits as a potential value the receiver Bob can obtain [13].

Classically, the variants are equivalent despite their differences. In Ref. [14], it has been proven that classical Rabin OT and classical 1-out-of-2 OT are equivalent and several other papers have dealt with the equivalence of other OT variations to 1 -out-of-2 OT in the classical setting [15, 16]. Relations and reductions between cryptographic tasks in the classical setting do not, however, necessarily hold in the quantum setting [17]. If or to what extent these equivalencies then hold is unclear. So, for instance, He and Wang [18] claim to have proven that the equivalence between Rabin OT and 1-out-of-2 OT does not hold in the quantum setting.

### 2.1.2 Impossibility of Unconditional Security

Over the years, considerable research in oblivious transfer protocols has been conducted both in the classical as well as in the quantum setting. In the classical setting, it has been shown that it is possible to have information-theoretic secure multi-party protocols if less than a third of the communication parties is dishonest [19, 20]. That is, if for $n$ participants less than $n / 3$ try to cheat by actively deviating from the protocol, these dishonest parties will neither succeed in gaining additional information nor in influencing the output of the remaining parties in any way. Oblivious transfer, however, is a protocol between only two parties, so, when one of them is dishonest, the requirement is not satisfied. Thus, it is not possible
to classically achieve oblivious transfer with information-theoretic security and the hope was put in quantum oblivious transfer.

Mayers [21] and Lo [22], however, presented impossibility results regarding infor-mation-theoretic quantum OT. In Ref. [21], Mayers proved that quantum bit commitment ( BC ) is not implementable with information-theoretic security without introducing any restrictions. A BC protocol consists of two phases, a commit phase where the sender Alice commits to one certain bit and a reveal phase where the receiver Bob learns that bit. The essential part is that Bob cannot learn the committed bit before the reveal phase and Alice cannot change the bit anymore after she has committed to it. That Mayers' impossibility result also holds for quantum OT can be concluded since, on one hand, OT can be used to implement BC due to its universality and, on the other hand, quantum BC can be used to obtain quantum OT protocols [23, 24]. In both of these cases, the insecurity of quantum OT is entailed. Lo [22] has proven a more general impossibility result, namely that no one-sided quantum two-party computation is information-theoretically secure. In general, a one-sided two-party computation has the characteristic that only one of the two communication partners obtains the final result while the other one learns nothing about it. Thus, this applies exactly to the primitive of oblivious transfer and Lo's impossibility result holds for it. Furthermore, he also briefly looked at twosided two-party computations where both parties learn the final output but nothing about the input from the respective other person except for what they can deduce from the final output. Also for this concept, he has shown the insecurity for some particular such functions. This result has been extended by a proof showing that, for any two-sided quantum two-party computation, when the protocol is perfectly secure against one cheating party, the other party can cheat perfectly and vice versa [25].

He and Wang [26] present a Rabin OT protocol based on quantum entanglement that they claim is unconditionally secure since it does not satisfy certain assumptions made in the impossibility results by Mayers [21] and Lo [22]. This claim, however, is not correct and valid and successful cheating strategies for both dishonest Alice and dishonest Bob can be developed [27].

### 2.1.3 Limitations and Restrictions for Improving Security

Since the impossibility of unconditional secure quantum OT has been determined [21, 22], possible restrictions and assumptions for OT protocols which can make them information-theoretically secure, have been considered and different approaches have
been examined.
It has been shown that information-theoretically secure BC is possible in a relativistic setting where the protocol is constrained by the theory of special relativity [28], thus, disproving Mayers' presumption that his obtained impossibility result holds for any quantum BC, no matter if in the nonrelativistic or relativistic scenario [21]. An exception to this information-theoretic feasibility of relativistic quantum BC is the so-called bit commitment with a certificate of classicality (BCCC) [29]. In other quantum BC protocols, a mixture $\alpha|0\rangle+\beta|1\rangle$ can be sent by the committing party Alice, that is, she basically can commit to a probability distribution. The significant characteristic of a BCCC protocol is that Alice can only choose whether to commit to $|0\rangle$ or $|1\rangle$, i.e. setting $\alpha=1$ and $\beta=0$ or $\alpha=0$ and $\beta=1$. Here, even a relativistic setting cannot achieve quantum BCCC with information-theoretic security.

Since BC can be used to create OT, the possibility of using secure relativistic BC to also achieve the desired security level for quantum OT has been investigated. In Ref. [30], the security of the BC based OT construction presented in Ref. [24] was examined when using a relativistic quantum BC. It was concluded that this method does not help to achieve information-theoretically secure quantum OT, though. Indeed, it was generally shown that oblivious transfer cannot be achieved with information-theoretic security even when including restrictions imposed by special relativity [31, 32].

A special case is the relativistic 1-out-of-2 OT in Minkowski spacetime called space-time constrained oblivious transfer (SCOT) [33]. This is a quantum variation of OT that has been proven to be information-theoretically secure since the impossibility results do not apply here due to Minkowski causality. In particular, the reason why this special case does not fall under the impossibility results is that the definition of OT is slightly modified. That is, while the receiver should never be able to learn the bit(s) he did not receive in normal OT, the receiver can and is allowed to learn these bit(s) outside the relevant space-time region in SCOT. Even though the experimental realisation of the quantum SCOT protocol in Minkowski spacetime in Ref. [33] is not feasible with current technology, there has been a development of another SCOT protocol which is implementable with existing technological developments [34]. The results of these papers have been further extended to 1 -out-of- $m$ space-time constrained OT in Ref. [35].

Another possibility to limit OT protocols is to impose restrictions on the quantum storage. Explicitly, there exist two different models, the bounded-quantumstorage model [36] and the noisy-quantum-storage model [37]. In the first model,
the quantum storage is bounded by the number of qubits that can be stored in quantum memory. Its effectiveness has been shown with three protocols implementing Rabin OT in the bounded-quantum-storage model and the model was proven to be secure as an honest party does not need any quantum memory but a dishonest one would need to store at least half of the transmitted qubits to cheat successfully [36]. The size of the available storage can even be expanded further as demonstrated in Ref. [38], where an oblivious transfer protocol was presented that is secure even when a dishonest party can store all but a small fraction of the transmitted states. The second model arose out of the first and can be seen as a generalisation of it. Instead of limiting the number of qubits that can be stored, it is assumed that there is some noise present in the quantum storage. Hence, every qubit stored there will be subject to noise, resulting in some decoherence. As an example, a (sender-) randomized Rabin OT where the sender does not select the two input bits but is given them by the protocol, is proposed in Ref. [37] and its security is analysed in the noisy-quantum-storage model. The security proof included only individual attacks on the individual qubits obtained in the protocol, so, in Ref. [39], the proof was generalised to cover security against arbitrary attacks.

The security proofs of the protocols in the aforementioned models assume that the quantum devices used are transparent in the sense that their actions are perfectly known, i.e. the exact measurements and state preparations are known [40]. This, however, cannot always be guaranteed leading to the introduction of the concept of device-independence [41]. Device-independence (DI) refers to regarding the quantum devices as black boxes where the actual inner working of these is unknown and tested as part of the protocol. This assumption can be used to achieve secure OT with methods given in Ref. [41]. Full DI protocols yield many difficulties when trying to implement them, thus, a weaker concept, the measurement-device independence (MDI), has been developed [40]. In this concept, only the measurement devices are regarded as black boxes which is much more practical. Ribeiro and Wehner [40] considered quantum OT protocols with the restriction of MDI and have found that some of them are secure while others are not, depending primarily on the photon sources used (whether the honest parties use perfect or imperfect single photon sources) but also on some general assumptions underlying the protocols. Measurement-device independent protocols (for quantum key distribution and other types of protocols) have been experimentally implemented [42, 43]. Only recently, progress has also been made on the experimental realisation of the more challenging concept of device-independence and proof-of-principle demonstrations for DI quantum key distribution have been presented [44, 45].

### 2.1.4 Lower Bounds for Cheating Probabilities

In addition to the research on which limitations could be imposed to obtain informationtheoretically secure quantum OT, the best lower bounds for the cheating probabilities that can be achieved by imperfect quantum OT with unrestricted parties/adversaries, have been investigated. Imperfect thereby means that either one or both parties are able to cheat better than with just a random guess, but their cheating probabilities are limited.

Chailloux et al. [46] proved that there is a constant lower bound on the optimal cheating probability for any quantum OT protocol. In particular, at least one of the communicating parties has a cheating strategy with which he/she can succeed with a probability of at least 0.5852 . For this, they defined cheating Alice as wanting to learn which information the receiver Bob has learnt and cheating Bob as wanting to learn all the transmitted bits. This bound has also been considered for 1-out-of-2 quantum OT especially, for which the concept of semi-honest OT was introduced [47]. A semi-honest receiver should learn as much as he would when he acts honestly, i.e. the requirement is for him to get to know one of the bits with certainty and then to try to learn the other bit as well. The lower bound was increased and it was shown that $\max (P($ Alice cheating $), P($ Bob cheating $)) \geq 2 / 3$, that is, the optimal cheating probability for any semi-honest quantum OT is at least $2 / 3$. This bound has been rederived independently and differently in Ref. [7], which considers any cheating strategy and not just necessarily semi-honest ones. For the special case where, in an honest implementation of a protocol, the states in the final step are pure and symmetric, the lower bound increases to 0.749 [7]. This paper also presents the cheating-probability-wise best known quantum 1-out-of-2 OT, where $P($ Alice cheating $)=3 / 4$ and $P($ Bob cheating $)=0.729$. With this result, the heretofore best known 1-out-of-2 OT protocol in Ref. [46] has been surpassed since there $P($ Alice cheating $)=3 / 4$ and $P($ Bob cheating $)=3 / 4$. No known quantum 1-out-of-2 OT protocol, however, has come close to the $2 / 3$ boundary. Nonetheless, these results have shown that quantum OT, even though not perfect, is still better than classical OT since classically one of the parties can always cheat perfectly [47]. It is possible though to decrease the average cheating probabilities of the parties in classical 1-out-of-2 OT when considering a probabilistic combination of a protocol where Alice can cheat perfectly and Bob only with a random guess and a protocol where Bob can cheat perfectly and Alice only with a random guess. In such a combined protocol, neither party cheats perfectly and the lowest average cheating probability achievable for both is $3 / 4$.

XOR oblivious transfer has also generated interest in the past few years years. The quantum OT protocol in Ref. [46] is presented for a 1-out-of-2 OT version, but briefly mentioned also is how it can be used for XOT. In Ref. [48], this protocol has been looked at in the specific XOT setting and its cheating probabilities have been shown to be equal to $P$ (Alice cheating $)=1 / 2$ and $P($ Bob cheating $)=$ $3 / 4$. Apart from this, [48] also investigated the concept of device-independence for XOT protocols and presents a specific DI XOT protocol with cheating probabilities $P($ Alice cheating $)=0.96440$ and $P($ Bob cheating $)=0.99204$.

Osborn and Sikora [49], by further investigating the impossibility results concerning quantum protocols for secure function evaluation in Refs. [22, 25], present a general lower bound on the cheating probabilities of any such protocol. They apply it to different specific protocols, thereby also to different oblivious transfer variants such as 1-out-of- $n$ oblivious transfer or XOR oblivious transfer. It is, however, not known if these bounds are attainable, that is, if there actually exist protocols that are tight with them.

Another line of research is to consider incomplete oblivious transfer protocols. Usually regarded are protocols where, if both parties are honest, the receiver Bob always gets a correct outcome, thus they are called complete protocols. A failure probability is included in incomplete protocols, that is, Bob sometimes gets an incorrect outcome, even when he and Alice are both honest. Since it is possible to lower the cheating probabilities for a non-zero failure probability, it is of interest to explore these incomplete protocols. In Ref. [50], incomplete 1-out-of-2 oblivious transfer protocols, where Alice cannot cheat at all, were considered and analysed with respect to lowering Bob's cheating probability and the failure probability.

### 2.2 Other Cryptographic Primitives

There are many other cryptographic primitives for multi-party (two-party) computations besides oblivious transfer and many of them are also studied in quantum settings. One of these primitives is bit commitment which has already been mentioned and described in the previous subsection. Others are for example private information retrieval, which in a sense is closely related to oblivious transfer, and coin flipping, a cryptographic primitive that is often used as part of larger protocols. These two primitives are introduced in more detail in the following subsections.

### 2.2.1 Private Information Retrieval

The notion of private information retrieval (PIR) was first introduced by Chor et al. [51] and addresses the matter of how a user querying a database can privately retrieve the information he/she is seeking. That is, how can a user retrieve a bit $x_{i}$ stored in an $n$-bit database $x=x_{1}, \ldots, x_{n}$ without revealing any information about the chosen $i \in\{1, \ldots, n\}$ to the server that holds the database. The most obvious solution is for the server to send the whole database to the user. This solution, however, requires $n$ bits to be sent. Thus, Chor et al. [51] investigated more efficient solutions involving $k \geq 2$ servers that cannot communicate with each other and where all $k$ servers have a copy of the database. In the considered schemes, it is required that none of the $k$ individual servers gets any information about $i$ when the user sends a query to all of the servers and computes the bit of interest $x_{i}$ from their replies.

Gertner et al. [52] extended private information retrieval to symmetrically private information retrieval (SPIR) where not only the user's privacy but also the server's privacy matters. Hence, when the user queries the database, the only information about the content of the database he/she should obtain is one single bit. As already noted in Ref. [52], this SPIR concept is highly related to the oblivious transfer variant 1-out-of- $n$ OT [12]; the user is supposed to learn one and only one bit of $n$ potential bits while the server is kept ignorant of which bit the user has learnt. It was later proven that actually any PIR protocol with one server (i.e. $k=1$ ) can be reduced to a 1-out-of-n OT protocol [53].

Aside from the investigation of these concepts in the classical setting, research has also been conducted on PIR and SPIR in the quantum setting and protocols for quantum private information retrieval (QPIR) [54, 55] and quantum symmetrically private information retrieval (QSPIR) [56] were developed. A different version of QSPIR, called the quantum private query (QPQ), was introduced by Giovannetti et al. [57]. The definition of such schemes differs to the original SPIR definition in that, rather than guaranteeing the user's privacy as incorporated part of the protocol, the user adds a test to his/her query with which it can be determined if the server has tried to learn anything about the user's query. Hence, in QPQ, the user queries a database and the server's reply consists of the answer to the query and a quantum certificate certifying that the server has not acquired any information about the user's query.

### 2.2.2 Coin Flipping

Coin flipping is another cryptographic primitive involving non-trusting parties. The concept of protocols for coin flipping between parties at different locations was first presented by Blum [58]. The idea of these protocols is for two or more communicating parties to output an agreed uniformly random bit while being at different locations and not trusting each other. There are two different types: strong coin flipping and weak coin flipping. In strong coin flipping, no party should be able to bias the coin toward any outcome. In weak coin flipping, however, the preferred outcome for each party is known and it should only be prevented that any party can bias the coin toward their preferred outcome.

It is impossible to have unconditional secure coin flipping protocols in the classical setting [59] as well as in the quantum setting [22]. However, while in classical protocols the cheating probability is never less than 1 , there are lower bounds for the cheating probabilities in quantum coin flipping protocols. Kitaev [60] has proven that the lower bound for cheating probabilities for quantum strong coin flipping protocols is $1 / \sqrt{2}$ and a protocol that gets arbitrarily close to this bound was presented in Ref. [61]. On the other hand, Mochon [62] has shown that there exist quantum weak coin flipping protocols with cheating probabilities of $1 / 2+\epsilon$, where $\epsilon>0$ can be arbitrarily small; so quantum weak coin flipping protocols can get very close to achieving information-theoretic security.

Progress in coin flipping has also been made on the experimental side. For example, the quantum coin flipping protocol proposed in Ref. [63] was experimentally realised [64] and was shown to be better than classical coin flipping protocols at communication distances suitable for metropolitan area communication networks.

### 2.3 Quantum State Elimination

Quantum state elimination is a measurement that eliminates rather than identifies a quantum state [65]. It is less known than the more common quantum state discrimination [66] where the focus is on identifying what state a quantum system has. In quantum state elimination, the aim is to exclude states, that is, to learn which state the quantum system has not been prepared in.

Minimum-error state elimination on a given set of states is equivalent to minimumerror state discrimination on a related set of states which consist of mixtures of the original states [67], but such an equivalence does not exist for unambiguous state elimination and unambiguous state discrimination. In unambiguous quantum state
elimination, one wants to learn with certainty in which state the quantum system has not been prepared in by unambiguously excluding states. Such a measurement is always possible when allowing for the possibility that sometimes there is also an inconclusive result. In Ref. [68], unambiguous quantum state elimination was considered for qubit sequences, also covering elimination of one or two states out of four two-qubit states. The measurements presented in this paper were later experimentally realised [69].

Unambiguous quantum state elimination measurements can be used for applications in quantum communication. For instance, it was applied in a protocol for quantum digital signatures [70] and it has also been used for oblivious transfer. That is, the 1-out-of-2 oblivious transfer protocol in Ref. [7] is based on an honest Bob implementing an unambiguous quantum state elimination measurement to obtain one of the two possible bits.

## Chapter 3

## Non-interactive Quantum XOR Oblivious Transfer

### 3.1 Introduction

As mentioned in the previous chapter, one variant of oblivious transfer is XOR oblivious transfer (XOT) [13]. In XOT, the sender Alice has two bits $x_{0}$ and $x_{1}$ and the receiver Bob will obtain one bit $x_{b}$, where $b \in\{0,1,2\}$ and $x_{2}=x_{0} \oplus x_{1}$; see Figure 3.1. Alice is not supposed to learn which bit Bob has learnt, and Bob is not supposed to be able to learn more than this one bit.


Figure 3.1: XOR oblivious transfer from Alice to Bob.
In this chapter, we look at non-interactive quantum XOR oblivious transfer with symmetric pure states. Non-interactive means that there is only one state transmission from the sender to the receiver who applies a measurement to get his/her output. In the usual definition of XOR oblivious transfer, Bob chooses if he wants to receive the first bit, the second bit, or their XOR, i.e. he picks the value of $b$ uniformly at random. Due to the non-interactivity of these protocols, this active choice is not a direct part of the quantum protocol but added by classical post-processing. We describe the classical post-processing here and show that it does not increase cheating probabilities.

The security of the protocols in this chapter is analysed by calculating the cheating probabilities for Alice and Bob. A dishonest Alice and a dishonest Bob are
therefore defined in the following way.

## Dishonest Alice:

A cheating Alice wants to learn which of the three bits Bob has learnt, i.e. has he received $x_{0}, x_{1}$, or $x_{2}$. In other words, she wants to learn $b$.

## Dishonest Bob:

A cheating Bob wants to not only learn one bit but all three of them.
Note that, in the XOT case, it is sufficient for a dishonest Bob to learn two of the bits, as he will be able to deduce the third bit from the other two. That is, when he learns for example $x_{0}$ and $x_{1}$, he will also know $x_{0} \oplus x_{1}$ and similarly for the other bit combinations.

The work in this chapter, including the protocol presented, its analysis, and the general investigation of non-interactive quantum XOT protocols using symmetric pure states, was presented and published in Ref. [71]. The specific XOT protocol was further also described in Ref. [72]. Here, we add details about how the results were derived and computed.

### 3.2 Optimal XOT Protocol Using Symmetric Pure States

In this section, we look at a specific non-interactive quantum XOR oblivious transfer protocol based on symmetric pure states. As a matter of fact, the protocol presented here is optimal among non-interactive protocols using symmetric pure states as shown in Section 3.3.

Furthermore, this protocol is also experimentally realisable [71], having been realised in the case when the communicating parties are both honest as well as in the cases where one of them is dishonest. Both Alice's and Bob's optimal cheating strategies, which we identify and analyse in this section, have been implemented. The feasibility of the protocol has hence been shown and the experimental results are in very good agreement with the theoretical results. More details about the experiment can be found in Section 3.4.

### 3.2.1 The Protocol

In the protocol, sender Alice encodes her two bit values $\left(x_{0}, x_{1}\right) \in\{0,1\}$ in a respective qutrit state $\left|\phi_{x_{0} x_{1}}\right\rangle$ and receiver Bob applies a quantum state elimination measurement.

In order to be able to learn either $x_{0}, x_{1}$, or $x_{0} \oplus x_{1}$ with certainty, the states $\left|\phi_{x_{0} x_{1}}\right\rangle$ need to be chosen in a way that it is possible to unambiguously exclude two of them. At the same time, it should not be possible to unambiguously determine which single state was received, so that it is impossible to perfectly learn both $x_{0}$ and $x_{1}$. This means that the four states $\left|\phi_{x_{0} x_{1}}\right\rangle$ need to be non-orthogonal to each other. One set of states that satisfies these criteria is

$$
\begin{array}{ll}
\left|\phi_{00}\right\rangle=\frac{1}{\sqrt{3}}(|0\rangle+|1\rangle+|2\rangle), & \left|\phi_{01}\right\rangle=\frac{1}{\sqrt{3}}(|0\rangle-|1\rangle+|2\rangle), \\
\left|\phi_{11}\right\rangle=\frac{1}{\sqrt{3}}(|0\rangle-|1\rangle-|2\rangle), & \left|\phi_{10}\right\rangle=\frac{1}{\sqrt{3}}(|0\rangle+|1\rangle-|2\rangle) . \tag{3.1}
\end{array}
$$

These non-orthogonal pure states are symmetric, in the sense that $\left|\phi_{01}\right\rangle=U\left|\phi_{00}\right\rangle$, $\left|\phi_{11}\right\rangle=U^{2}\left|\phi_{00}\right\rangle$, and $\left|\phi_{10}\right\rangle=U^{3}\left|\phi_{00}\right\rangle$ for the unitary

$$
U=\left(\begin{array}{ccc}
1 & 0 & 0  \tag{3.2}\\
0 & 0 & -1 \\
0 & 1 & 0
\end{array}\right)
$$

for which it holds that $U^{4}=\mathbb{1}$.
After Alice has sent to Bob the state corresponding to her bits chosen uniformly at random $\left(x_{0}, x_{1}\right) \in\{0,1\}$, Bob makes an unambiguous quantum state elimination measurement to exclude two out of the four possible states. There are six different pairs of states he can exclude, whereby each excluded pair corresponds to learning either $x_{0}, x_{1}$, or $x_{0} \oplus x_{1}$, with either the value 0 or 1 . Constructing Bob's measurement operators requires the six states that are each orthogonal to a pair of states in Eq. (3.1). The measurement operators are then proportional to projectors onto these six states, normalised so that their sum is equal to the identity matrix. For instance, Bob will get outcome bit $x_{0}=0$ when the excluded states are $\left|\phi_{11}\right\rangle$ and $\left|\phi_{10}\right\rangle$ and the corresponding measurement operator for this is $\Pi_{A}=\frac{1}{4}(|0\rangle+|2\rangle)(\langle 0|+\langle 2|)$; similarly for the other outcomes. Table 3.1 shows the measurement operators with their respective excluded pair of states and deduced output bit for Bob.

Having determined both an honest Alice's states as given in Eq. (3.1) and an honest Bob's measurement operators (Table 3.1), we can summarise and outline the XOR oblivious transfer protocol's procedure as follows.

1. Alice uniformly at random chooses the bits $\left(x_{0}, x_{1}\right) \in\{0,1\}$ and sends the corresponding state $\left|\phi_{x_{0} x_{1}}\right\rangle$ to the receiver Bob.
2. Bob performs an unambiguous quantum state elimination measurement, excluding two of the possible states with certainty, from which he can deduce either $x_{0}, x_{1}$, or $x_{2}=x_{0} \oplus x_{1}$.

| Outcome bit | Eliminated states | Measurement operator |
| :---: | :---: | :---: |
| $x_{0}=0$ | $\left\|\phi_{11}\right\rangle$ and $\left\|\phi_{10}\right\rangle$ | $\Pi_{A}=\frac{1}{4}(\|0\rangle+\|2\rangle)(\langle 0\|+\langle 2\|)$ |
| $x_{0}=1$ | $\left\|\phi_{00}\right\rangle$ and $\left\|\phi_{01}\right\rangle$ | $\Pi_{B}=\frac{1}{4}(\|0\rangle-\|2\rangle)(\langle 0\|-\langle 2\|)$ |
| $x_{1}=0$ | $\left\|\phi_{11}\right\rangle$ and $\left\|\phi_{01}\right\rangle$ | $\Pi_{C}=\frac{1}{4}(\|0\rangle+\|1\rangle)(\langle 0\|+\langle 1\|)$ |
| $x_{1}=1$ | $\left\|\phi_{00}\right\rangle$ and $\left\|\phi_{10}\right\rangle$ | $\Pi_{D}=\frac{1}{4}(\|0\rangle-\|1\rangle)(\langle 0\|-\langle 1\|)$ |
| $x_{2}=0$ | $\left\|\phi_{01}\right\rangle$ and $\left\|\phi_{10}\right\rangle$ | $\Pi_{E}=\frac{1}{4}(\|1\rangle+\|2\rangle)(\langle 1\|+\langle 2\|)$ |
| $x_{2}=1$ | $\left\|\phi_{00}\right\rangle$ and $\left\|\phi_{11}\right\rangle$ | $\Pi_{F}=\frac{1}{4}(\|1\rangle-\|2\rangle)(\langle 1\|-\langle 2\|)$ |

Table 3.1: Bob's measurement operators, the respective eliminated states, and thereof deduced outcome bits.

### 3.2.2 Equivalence between Semi-random XOT and Standard XOT

In oblivious transfer, the sender and receiver are usually presumed to choose their inputs uniformly at random, i.e. the values for the bits $\left(x_{0}, x_{1}\right)$ for Alice and the value for $b$ for Bob. The price for the non-interactivity, however, is that, in the execution of the quantum protocol, Bob cannot actively choose if he wants to receive the first bit, the second bit, or their XOR. That is, here, Bob does not have an input but he will obtain one of the three outcomes at random, that is, he obtains either $x_{0}, x_{1}$, or $x_{0} \oplus x_{1}$ with a probability of $1 / 3$ each.

This notion of a party randomly obtaining outputs that, in standard oblivious transfer protocols, are their respective inputs, has already been explored for 1-2 OT. Chailloux et al. [46] defined random 1-out-of-2 oblivious transfer, where Alice and Bob get the random outputs $\left(x_{0}, x_{1}\right)$ or $b$, respectively, and showed that it is equivalent to standard 1-out-of-2 oblivious transfer, where these outputs are their respective inputs. Amiri et al. [7] defined semi-random 1-out-of-2 oblivious transfer, where Bob gets the random output $b$, and showed that it is equivalent to not only
standard 1-out-of-2 oblivious transfer, where this output is his input, but also to random 1-out-of-2 oblivious transfer as described in Ref. [46].

In accordance with this and using the terminology in Ref. [7], the XOT protocol in the previous subsection can be de facto classified as a semi-random XOT protocol. A semi-random XOR oblivious transfer protocol is generally defined as follows.

Definition 3.1 (Semi-random XOR oblivious transfer). Semi-random XOT is a two-party protocol where

1. Alice chooses her input bits $\left(x_{0}, x_{1}\right) \in\{0,1\}$ uniformly at random, thereby specifying also their XOR $x_{2}=x_{0} \oplus x_{1}$, or she chooses Abort.
2. Bob outputs the value $b \in\{0,1,2\}$ and a bit $y$, or Abort.
3. If both parties are honest, then they never abort, $y=x_{b}$, Alice has no information about $b$, and Bob has no information about $x_{(b+1) \bmod 3}$ or about $x_{(b+2) \bmod 3}$.

Using similar arguments as in Refs. [7] and [46], it is possible to prove that semi-random and standard XOR oblivious transfer are equivalent up to classical post-processing. That is, implementing semi-random XOT with cheating probabilities $A_{O T}$ and $B_{O T}$ allows realisation of standard XOT with the same cheating probabilities and vice versa; similarly as for 1-2 OT. So, adding classical post-processing enables Bob to nevertheless actively (but randomly from Alice's point of view) choose whether he wants to learn $x_{0}, x_{1}$, or $x_{2}=x_{0} \oplus x_{1}$ without affecting either party's cheating probability.

Proposition 3.1. Having a semi-random XOT protocol with cheating probabilities $A_{O T}$ and $B_{O T}$ is equivalent to having a standard XOT protocol with the same cheating probabilities.

Proof. We examine both directions, i.e. constructing a semi-random XOT protocol from a standard XOT protocol, and constructing a standard XOT protocol from a semi-random XOT protocol. That is, the situation where the parties possess means to implement standard XOT, but both of them instead wish to implement semirandom XOT, or vice versa.
Case 1: Let $P$ be a standard XOT protocol with cheating probabilities $A_{O T}(P)$ and $B_{O T}(P)$. A semi-random XOT protocol $Q$ with the same cheating probabilities can be constructed in the following way:

1. Alice picks $\left(x_{0}, x_{1}\right) \in\{0,1\}$ uniformly at random. Bob generates $b \in\{0,1,2\}$ uniformly at random (in a way so that he no longer actively chooses $b$ ).
2. Alice and Bob perform the XOT protocol $P$ where Alice inputs $x_{0}, x_{1}$, and $x_{2}=x_{0} \oplus x_{1}$ and Bob inputs $b$. Let $y$ be Bob's output.
3. Alice and Bob abort in $Q$ if and only if they abort in $P$. Otherwise, the outputs of protocol $Q$ are $(b, y)$ for Bob.

Evidently, $Q$ implements semi-random XOT if both parties follow the protocol. Furthermore, because of the way $Q$ is constructed, Alice can cheat in $Q$ if and only if she can cheat in $P$, and the same for Bob cheating. Cheating probabilities for Alice and Bob are therefore equal in $P$ and $Q, A_{O T}(Q)=A_{O T}(P)$ and $B_{O T}(Q)=B_{O T}(P)$.

Case 2: Let $P$ be a semi-random XOT protocol with cheating probabilities $A_{O T}(P)$ and $B_{O T}(P)$. A standard XOT protocol $Q$ with the same cheating probabilities can be constructed in the following way:

1. Alice has inputs $X_{0}, X_{1}$, with $X_{2}=X_{0} \oplus X_{1}$, and Bob has input $B \in\{0,1,2\}$.
2. Alice and Bob perform the semi-random XOT protocol $P$ where Alice inputs $x_{0}, x_{1}$, with $x_{2}=x_{0} \oplus x_{1}$, whereby she chooses $\left(x_{0}, x_{1}\right) \in\{0,1\}$ uniformly at random. Let $(b, y)$ be Bob's outputs.
3. Bob sends $r=(b+B+B) \bmod 3$ to Alice. Let $x_{c}^{\prime}=x_{(c+r) \bmod 3}$ for $c \in\{0,1,2\}$.
4. Alice sends $\left(s_{0}, s_{1}\right)$ to Bob, whereby $s_{c}=x_{c}^{\prime} \oplus X_{c}$ for $c \in\{0,1\}$ and $s_{2}=s_{0} \oplus s_{1}$. Let $y^{\prime}=y \oplus s_{B}$.
5. Alice and Bob abort in $Q$ if and only if they abort in $P$. Otherwise, the output of protocol $Q$ is $y^{\prime}$ for Bob.

If Alice and Bob are both honest, then $y=x_{b}$ holds true. Note that $x_{B}^{\prime}=x_{(B+r) \bmod 3}$ $=x_{(B+b+B+B) \bmod 3}=x_{b}$. Hence,

$$
\begin{equation*}
y^{\prime}=y \oplus s_{B}=x_{b} \oplus s_{B}=x_{B}^{\prime} \oplus x_{B}^{\prime} \oplus X_{B}=X_{B}, \tag{3.3}
\end{equation*}
$$

i.e. $y^{\prime}$ is indeed equal to $X_{B}$. This also holds for $B=2$ since

$$
\begin{equation*}
s_{2}=s_{0} \oplus s_{1}=x_{0}^{\prime} \oplus X_{0} \oplus x_{1}^{\prime} \oplus X_{1}=x_{0} \oplus x_{1} \oplus X_{0} \oplus X_{1}=x_{2} \oplus X_{2}=x_{2}^{\prime} \oplus X_{2} . \tag{3.4}
\end{equation*}
$$

The following is true with respect to the classical post-processing described in steps 3 and 4 and security against Alice and Bob:

- If Alice is honest, she knows $r$ but has no information about $b$. From $r=$ $(b+B+B) \bmod 3$ she can deduce that $2 B=(r-b) \bmod 3$ but she cannot obtain any information about $B$ from this. Hence, the classical post-processing does not give an honest Alice any more information about which bit Bob has obtained.
- If Alice is dishonest, she can correctly guess $b$ with probability $A_{O T}(P)$. She knows $r$. Since $2 B=(r-b) \bmod 3$, guessing $2 B$, equivalently guessing $B$, is equivalent to guessing $b$. Therefore, $A_{O T}(Q)=A_{O T}(P)$.
- If Bob is honest, he knows $s_{0}, s_{1}, s_{2}=s_{0} \oplus s_{1}$, and $r$ but has no information about $x_{(b+1) \bmod 3}$ and $x_{(b+2) \bmod 3}$. He cannot learn anything about the other two of Alice's bits, $X_{(B+1) \bmod 3}$ and $X_{(B+2) \bmod 3}$, since

$$
\begin{align*}
X_{(B+1) \bmod 3} & =x_{(B+1) \bmod 3}^{\prime} \oplus s_{(B+1) \bmod 3}=x_{(B+1+r) \bmod 3} \oplus s_{(B+1) \bmod 3} \\
& =x_{(b+1) \bmod 3} \oplus s_{(B+1) \bmod 3}, \\
X_{(B+2) \bmod 3} & =x_{(B+2) \bmod 3}^{\prime} \oplus s_{(B+2) \bmod 3}=x_{(B+2+r) \bmod 3} \oplus s_{(B+2) \bmod 3} \\
& =x_{(b+2) \bmod 3} \oplus s_{(B+2) \bmod 3} . \tag{3.5}
\end{align*}
$$

Hence, the classical post-processing does not give an honest Bob any more information about the other two bits Alice has sent.

- If Bob is dishonest, he can guess $x_{(b+1) \bmod 3}$ and $x_{(b+2) \bmod 3}$ with probability $B_{O T}(P)$. He knows $s_{0}, s_{1}, s_{2}=s_{0} \oplus s_{1}$, and $r$. Since $s_{c}=x_{c}^{\prime} \oplus X_{c}=$ $x_{(c+r) \bmod 3} \oplus X_{c}$ for $c \in\{0,1,2\}, X_{c}=x_{(c+r) \bmod 3} \oplus s_{c}$ and, for Bob, guessing $\left(X_{0}, X_{1}, X_{2}\right)$ is equivalent to guessing $\left(x_{0}, x_{1}, x_{2}\right)$. Therefore, $B_{\text {ОT }}(Q)=$ $B_{\text {OT }}(P)$.

Step 3 and Step 4 in the second case of the proof describe the classical postprocessing that needs to be added to a semi-random XOT protocol to realise a standard XOT protocol. The process can be illustrated more clearly. Alice's actual input bits are $\left(X_{0}, X_{1}\right)$ with $X_{2}=X_{0} \oplus X_{1}$, while the uniformly at random chosen bits ( $x_{0}, x_{1}$ ) with $x_{2}=x_{0} \oplus x_{1}$ are only "dummy" values. The semi-random XOT protocol is implemented using these "dummy" values $\left(x_{0}, x_{1}\right)$. In the first part of the classical post-processing, Step 3, Bob defines a variable $r$ whose value will tell

Alice how to permute the order of the bits $x_{i}$ for $i \in\{0,1,2\}$, and the bits in new order are called $x_{c}^{\prime}$ for $c \in\{0,1,2\}$. She will then compute and send the bits $\left(s_{0}, s_{1}\right)$ to Bob, from which he can learn the bit $X_{B}$ that he wants to learn. That is, when $r=0$, then $b=B$ and the order of the bits is right, i.e. $\left(x_{0}^{\prime}, x_{1}^{\prime}, x_{2}^{\prime}\right)=\left(x_{0}, x_{1}, x_{2}\right)$. So Alice does not need to change anything before computing and sending ( $s_{0}, s_{1}$ ). When $r=1$, however, $b \neq B$ and the order of the bits needs to be shifted once to the left, i.e. $\left(x_{0}^{\prime}, x_{1}^{\prime}, x_{2}^{\prime}\right)=\left(x_{1}, x_{2}, x_{0}\right)$, before Alice can compute and send $\left(s_{0}, s_{1}\right)$. Also when $r=2, b \neq B$ and the order of the bits needs to be shifted once to the right, i.e. $\left(x_{0}^{\prime}, x_{1}^{\prime}, x_{2}^{\prime}\right)=\left(x_{2}, x_{0}, x_{1}\right)$, before Alice can compute and send $\left(s_{0}, s_{1}\right)$. Bob has output $(b, y)$ from the semi-random XOT protocol and wants to learn the bit $X_{B}$. He receives $\left(s_{0}, s_{1}\right)$, where $s_{2}=s_{0} \oplus s_{1}$ holds for all $r \in\{0,1,2\}$. The value of $s_{B}$ will tell him what he needs to do with $y$ in order to learn his chosen bit. That is, when $s_{B}=0$, then the value of $y$ matches the value of $X_{B}$ and he does not do anything. However, when $s_{B}=1$, then he needs to flip the bit $y$ to get the correct value for $X_{B}$.

### 3.2.3 Dishonest Bob

Let us suppose that Bob is dishonest and wants to cheat. Bob cheating is defined as him wanting to know all three bits, i.e. the first bit, the second bit, and their XOR. Since knowledge of the values of any two of these bits implies knowledge of the value of the third one, Bob aims, without loss of generality, to correctly guess both $x_{0}$ and $x_{1}$ which in turn implies knowledge of $x_{2}=x_{0} \oplus x_{1}$.

Note that by following the protocol honestly and then randomly guessing the value of the bit(s) that he did not obtain, a dishonest Bob can always cheat with a probability of at least $1 / 2$. Bob's best cheating strategy though is to distinguish between honest Alice's states in Eq. (3.1) with minimum error. The optimal minimum-error measurement in this case is the square-root measurement (SRM), also called pretty good measurement [73, 74], since he wants to distinguish between equiprobable and symmetric states.

Thus, the measurement operator corresponding to a state $\left|\phi_{x_{0} x_{1}}\right\rangle$ is

$$
\begin{equation*}
\Pi_{x_{0} x_{1}}=\rho_{\text {average }}^{-1 / 2}\left|\phi_{x_{0} x_{1}}\right\rangle\left\langle\phi_{x_{0} x_{1}}\right| \rho_{\text {average }}^{-1 / 2}, \tag{3.6}
\end{equation*}
$$

where the average density matrix sent from Alice to Bob is

$$
\begin{equation*}
\rho_{\text {average }}=\sum_{x_{0}, x_{1}=0,1} p_{x_{0} x_{1}}\left|\phi_{x_{0} x_{1}}\right\rangle\left\langle\phi_{x_{0} x_{1}}\right|=\frac{1}{3} \mathbb{1} \tag{3.7}
\end{equation*}
$$

since Alice sends each one of the four possible states with equal probability and so $p_{x_{0} x_{1}}=1 / 4 \forall x_{0}, x_{1} \in\{0,1\}$. Specifically, dishonest Bob's measurement operators are then given by $\Pi_{x_{0} x_{1}}=\frac{1}{4}\left|\phi_{x_{0} x_{1}}\right\rangle\left\langle\phi_{x_{0} x_{1}}\right|$ for each state $\left|\phi_{x_{0} x_{1}}\right\rangle$, respectively, and his cheating probability $B_{O T}^{q}$ is

$$
\begin{equation*}
B_{O T}^{q}=\frac{1}{4} \sum_{x_{0}, x_{1}=0,1} \operatorname{Tr}\left(\Pi_{x_{0} x_{1}}\left|\phi_{x_{0} x_{1}}\right\rangle\left\langle\phi_{x_{0} x_{1}}\right|\right)=\frac{3}{4} \tag{3.8}
\end{equation*}
$$

### 3.2.4 Dishonest Alice

Let us suppose that Alice is dishonest and wants to cheat. Alice cheating is defined as her wanting to know which of the three bits Bob has obtained, i.e. whether he has learnt the first bit, the second bit, or their XOR.

Note that, by following the protocol honestly and then randomly guessing whether Bob has obtained $x_{0}, x_{1}$, or $x_{2}=x_{0} \oplus x_{1}$, a dishonest Alice can always cheat with a probability of at least $1 / 3$. Otherwise, there are two different types of protocols that can be considered. In one of them, Bob tests the states Alice sends to him and, in the other one, Bob does not apply any testing. If Bob does not test, a dishonest Alice can send him any state that suits her best. However, if Bob tests, this can restrict Alice's available cheating strategies. The particular testing process considered here is similar to the testing process in the 1-out-of-2 oblivious transfer protocol investigated by Amiri et al. [7]. For this process, Alice has to send Bob a sequence of states and Bob then picks a fraction of them for which he asks Alice to declare what they are. He makes an appropriate measurement on these states and checks if his measurement results match with Alice's declarations. When Bob is testing, Alice's average cheating probability is obtained as opposed to her cheating probability for each individual state transmission. In general, when Bob is not testing, dishonest Alice can cheat at least as well as when Bob is applying some testing.

## No testing by Bob

We first consider the case where Bob does no testing. A dishonest Alice can then choose to send any state for which the probability of Bob obtaining either $x_{0}, x_{1}$, or $x_{2}$ is maximised. In general, Bob's probability to receive the outcome associated with his measurement operator $\Pi_{B}^{k}$ is $\operatorname{Tr}\left(\Pi_{B}^{k} \rho^{j}\right)$, when $\rho^{j}$ was sent. To maximise this probability, it is best for Alice to send him the eigenstate of $\Pi_{B}^{k}$ corresponding to its largest eigenvalue. The largest eigenvalue of Bob's relevant measurement operators will yield Alice's cheating probability.

Looking at Bob's measurement operators, we note that $\Pi_{A}$ and $\Pi_{B}$ correspond to Bob obtaining the first bit, $\Pi_{C}$ and $\Pi_{D}$ to Bob obtaining the second bit, and $\Pi_{E}$ and $\Pi_{F}$ to Bob obtaining their XOR. Hence, these pairwise combinations need to be considered, i.e. $\Pi_{A}+\Pi_{B}=(|0\rangle\langle 0|+|2\rangle\langle 2|) / 2, \Pi_{C}+\Pi_{D}=(|0\rangle\langle 0|+|1\rangle\langle 1|) / 2$, and $\Pi_{E}+\Pi_{F}=(|1\rangle\langle 1|+|2\rangle\langle 2|) / 2$. All three pairwise added measurement operators have eigenvalues $(1 / 2,1 / 2,0)$. Bob's probability to obtain the first bit is then maximal and equal to $1 / 2$, when Alice sends Bob any superposition of $|0\rangle$ and $|2\rangle$. Similarly, Bob's probability to obtain the second bit is maximal and equal to $1 / 2$, when Alice sends Bob any superposition of $|0\rangle$ and $|1\rangle$, and Bob's probability to obtain the XOR is maximal and equal to $1 / 2$, when Alice sends Bob any superposition of $|1\rangle$ and $|2\rangle$ We can conclude that, with no testing by Bob, Alice can cheat with probability of at most $A_{O T}^{q}=1 / 2$.

## Bob testing

Next, we consider the case where Bob tests Alice's states, whereby Alice wants to make sure that her cheating stays undetected. Since this places restrictions on dishonest Alice's choice of states to send, this generally might lower Alice's cheating probability. For this particular protocol, though, we will see that the cheating probability for Alice actually remains the same.

For Bob to carry out the testing, it is necessary to implement not only one instance of the XOT protocol but multiple instances. Following the method in [7], Alice transmits not only one but $N$ states. Bob randomly chooses a small fraction $F$ of the states, where $0<F \ll 1$. He asks Alice to declare what these selected states are and measures them in the basis where one of the basis states is the state Alice declared. Bob then checks if his results confirm Alice's declaration. If he finds any mismatches, Bob aborts the protocol. Otherwise, he discards the tested states and proceeds with the protocol for the remaining $N(1-F)$ states.

In order to always pass Bob's tests, a dishonest Alice has to send a superposition of the states she is supposed to send, entangled with some system she keeps. Generally, such a state is

$$
\begin{equation*}
\left|\Phi_{\text {cheat }}\right\rangle=a|0\rangle_{\text {Alice }} \otimes\left|\phi_{00}\right\rangle+b|1\rangle_{\text {Alice }} \otimes\left|\phi_{01}\right\rangle+c|2\rangle_{\text {Alice }} \otimes\left|\phi_{11}\right\rangle+d|3\rangle_{\text {Alice }} \otimes\left|\phi_{10}\right\rangle, \tag{3.9}
\end{equation*}
$$

where $\left\{|0\rangle_{\text {Alice }},|1\rangle_{\text {Alice }},|2\rangle_{\text {Alice }},|3\rangle_{\text {Alice }}\right\}$ is an orthonormal basis for the system Alice keeps and $|a|^{2}+|b|^{2}+|c|^{2}+|d|^{2}=1$. Alice can then ensure that, whenever she is tested, she can prepare one of the states she is supposed to send by measuring her system in this basis; i.e. she will always be able to declare a state matching Bob's
information if she is asked to do so.
Whenever she is not tested, Alice, however, measures her system in the way that maximises her probability to correctly guess which bit Bob has obtained. After Bob has made his unambiguous quantum state elimination measurement, Alice's system is prepared in one of three states, depending on whether Bob has obtained $x_{0}, x_{1}$, or $x_{2}=x_{0} \oplus x_{1}$. That is,

$$
\begin{equation*}
\rho_{0}=\frac{1}{p_{A}+p_{B}} \operatorname{Tr}_{\text {Bob }}\left[\left(\Pi_{A}+\Pi_{B}\right)^{1 / 2}\left|\Phi_{\text {cheat }}\right\rangle\left\langle\Phi_{\text {cheat }}\right|\left(\Pi_{A}+\Pi_{B}\right)^{1 / 2}\right], \tag{3.10}
\end{equation*}
$$

where $p_{A}+p_{B}=\operatorname{Tr}\left[\left|\Phi_{\text {cheat }}\right\rangle\left\langle\Phi_{\text {cheat }}\right|\left(\Pi_{A}+\Pi_{B}\right)\right]=1 / 3$, and analogously for $\rho_{1}$ and $\rho_{2}$. The states she needs to distinguish between are therefore

$$
\begin{align*}
& \rho_{0}=\left(\begin{array}{cccc}
|a|^{2} & a b^{*} & 0 & 0 \\
a^{*} b & |b|^{2} & 0 & 0 \\
0 & 0 & |c|^{2} & c d^{*} \\
0 & 0 & c^{*} d & |d|^{2}
\end{array}\right), \\
& \rho_{1}=\left(\begin{array}{cccc}
|a|^{2} & 0 & 0 & a d^{*} \\
0 & |b|^{2} & b c^{*} & 0 \\
0 & b^{*} c & |c|^{2} & 0 \\
a^{*} d & 0 & 0 & |d|^{2}
\end{array}\right), \\
& \rho_{2}=\left(\begin{array}{cccc}
|a|^{2} & 0 & -a c^{*} & 0 \\
0 & |b|^{2} & 0 & -b d^{*} \\
-a^{*} c & 0 & |c|^{2} & 0 \\
0 & -b^{*} d & 0 & |d|^{2}
\end{array}\right), \tag{3.11}
\end{align*}
$$

corresponding to Bob obtaining $x_{0}, x_{1}$, or $x_{2}=x_{0} \oplus x_{1}$, and all three states occur with equal probability $1 / 3$.

Alice's optimal measurement is a minimum-error measurement. Thus, she will want to make the states as distinguishable as possible when choosing the values for $a, b, c$, and $d$. Since the probabilities of all three state are independent of the constants $a, b, c$, and $d$, it is optimal for Alice to choose their values in a way to minimise the pairwise fidelities between the states, making them as distinct and hence as distinguishable as possible. Because any complex phase factors can be absorbed into the kets $|0\rangle_{\text {Alice }},|1\rangle_{\text {Alice }},|2\rangle_{\text {Alice }},|3\rangle_{\text {Alice }}$, the constants $a, b, c$, and $d$ can be assumed to be real numbers without loss of generality. It can be shown that for real $a, b, c$, and $d$, the pairwise fidelities between the $\rho_{i}$, for $i \in\{0,1,2\}$, are
minimised when the variables are all equal, i.e. when $a=b=c=d=1 / 2$.
Alice's basis states can be realised as two-qubit states, in particular, $|0\rangle_{\text {Alice }} \equiv$ $|00\rangle,|1\rangle_{\text {Alice }} \equiv|01\rangle,|2\rangle_{\text {Alice }} \equiv|10\rangle$, and $|3\rangle_{\text {Alice }} \equiv|11\rangle$. For $a=b=c=d=1 / 2$, the states in Eq. (3.11) can be rewritten as
where $| \pm\rangle=(|0\rangle \pm|1\rangle) / \sqrt{2}$ and the Bell states $\left|\Psi^{+}\right\rangle=(|01\rangle+|10\rangle) / \sqrt{2}$ and $\left|\Phi^{+}\right\rangle=$ $(|00\rangle+|11\rangle) / \sqrt{2}$.

Looking at the states in Eq. (3.12), we note that they are all diagonal in the
 Alice's measurement operators in the three-dimensional subspace spanned by the states she has, can for instance be picked as

$$
\begin{align*}
\Pi_{0} & =\frac{1}{2}|++\rangle\langle++|+\frac{1}{2}|-+\rangle\langle-+|, \\
\Pi_{1} & =\frac{1}{2}|++\rangle\langle++|+\frac{1}{2}|--\rangle\langle--|, \\
\Pi_{2} & =\frac{1}{2}|--\rangle\langle--|+\frac{1}{2}|-+\rangle\langle-+| . \tag{3.13}
\end{align*}
$$

Summing up these measurement operators together with the "unused" projector
 state could be a different basis state when $a, b, c$, and $d$ get multiplied with suitable phase factors or when the basis states are permuted.

An optimal minimum-error measurement needs to satisfy the Helstrom conditions [66]

$$
\begin{equation*}
\Pi_{j}\left(p_{j} \rho_{j}-p_{k} \rho_{k}\right) \Pi_{k}=0 \quad \forall j, k, \quad \text { and } \quad \sum_{j} p_{j} \rho_{j} \Pi_{j}-p_{k} \rho_{k} \geq 0 \quad \forall k . \tag{3.14}
\end{equation*}
$$

It can be shown that the states in Eq. (3.12) and the measurement operators in Eq. (3.13) satisfy these conditions. Therefore, we can conclude that this is an optimal measurement and Alice's maximal cheating probability $A_{O T}^{q}$ is given by

$$
\begin{equation*}
A_{O T}^{q}=\frac{1}{3}\left[\operatorname{Tr}\left(\rho_{0} \Pi_{0}\right)+\operatorname{Tr}\left(\rho_{1} \Pi_{1}\right)+\operatorname{Tr}\left(\rho_{2} \Pi_{2}\right)\right]=\frac{1}{2} . \tag{3.15}
\end{equation*}
$$

This is the same success probability as in the case where Bob is not testing. It further confirms that choosing $a=b=c=d=1 / 2$ is optimal, since Alice cannot cheat more often when Bob is testing the states she sends, than she can when he is not testing her states. Testing by Bob therefore does not lower Alice's cheating probability in this protocol and can be omitted. Alice's cheating probability $A_{O T}^{q}=1 / 2$ is then not just valid as her average cheating probability over multiple instances of OT, but it is valid for each individual instance of OT.

### 3.2.5 Comparison to a Classical XOT Protocol

In this subsection, we compare the quantum XOT protocol to a classical protocol. For this purpose, we define a classical protocol which is a combination of two trivial classical protocols. In one of the trivial protocols, Alice can cheat perfectly, and, in the other one, Bob can cheat perfectly. These two trivial protocols are defined similar to the two "bad" classical XOT protocols presented in Ref. [48].

Protocol 1: Alice has the two bits $\left(x_{0}, x_{1}\right)$, and chooses to send Bob either one of the individual bits $x_{0}$ or $x_{1}$ or their XOR $x_{2}=x_{0} \oplus x_{1}$. Afterwards she "forgets" what she has sent.

Here, Alice can obviously cheat perfectly with probability 1. Bob, on the other hand, can only cheat with probability $1 / 2$ by guessing one of the bits that he did not receive, and getting the third by means of taking the XOR of the two bits he now holds.

Protocol 2: Alice sends all of $\left(x_{0}, x_{1}, x_{2}=x_{0} \oplus x_{1}\right)$ to Bob, who chooses one of these bits to read and discards the others without looking at them.

Here, Bob can obviously cheat perfectly with probability 1 by reading out both the bits $x_{0}$ and $x_{1}$. Alice, however, can only cheat with probability $1 / 3$ by guessing which bit Bob has chosen to read out.

To generate the classical XOT protocol to which we will compare the quantum protocol, we will combine these trivial protocols using a method described in Ref. [47]. In this method, Alice and Bob conduct an unbalanced weak coin flipping protocol whose outcome will specify which protocol gets implemented. This ultimately results in:

Protocol 3: Protocol 1 is implemented with probability $s$ and Protocol 2 is implemented with probability $(1-s)$.

Alice's and Bob's cheating probabilities in Protocol 3 are

$$
\begin{align*}
& A_{O T}^{c}=s(1)+(1-s) \frac{1}{3}=\frac{1}{3}+\frac{2}{3} s \\
& B_{O T}^{c}=s \frac{1}{2}+(1-s)(1)=1-\frac{1}{2} s . \tag{3.16}
\end{align*}
$$

This yields a trade-off relation $f^{t}\left(A_{O T}^{c}, B_{O T}^{c}\right)=c_{1} A_{O T}^{c}+c_{2} B_{O T}^{c}$ when choosing the values for the constants $c_{1}$ and $c_{2}$ such that $s$ gets eliminated. That is,

$$
\begin{equation*}
f^{t}\left(A_{O T}^{c}, B_{O T}^{c}\right)=3 A_{O T}^{c}+4 B_{O T}^{c}=3\left(\frac{1}{3}+\frac{2}{3} s\right)+4\left(1-\frac{1}{2} s\right)=5 . \tag{3.17}
\end{equation*}
$$

If a quantum protocol beats that bound, $f^{t}\left(A_{O T}^{q}, B_{O T}^{q}\right)<f^{t}\left(A_{O T}^{c}, B_{O T}^{c}\right)=5$, then it achieves a quantum advantage over the considered protocol. For the quantum protocol in this section, Alice's cheating probability is $A_{O T}^{q}=1 / 2$ and Bob's cheating probability is $B_{O T}^{q}=3 / 4$. So the trade-off relation is

$$
\begin{equation*}
f^{t}\left(A_{O T}^{q}, B_{O T}^{q}\right)=3 A_{O T}^{q}+4 B_{O T}^{q}=4.5 . \tag{3.18}
\end{equation*}
$$

Obviously $4.5<5$, therefore, the quantum protocol does indeed have a quantum advantage over the considered classical protocol.

### 3.3 Quantum XOT with Symmetric States

As mentioned earlier, the protocol considered in Section 3.2 can be said to be optimal among non-interactive protocols using symmetric pure states. This is shown here by considering quantum XOR oblivious transfer with symmetric pure states in general and analysing the cheating probabilities for Alice and Bob in these protocols.

The quantum XOT protocols we consider satisfy the following properties.

1. They are non-interactive protocols, in which Alice encodes her bit values $x_{0}$ and $x_{1}$ into a quantum state $\left|\psi_{x_{0} x_{1}}\right\rangle$ and sends it to Bob, who measures it.
2. Alice's states $\left|\psi_{x_{0} x_{1}}\right\rangle$ are pure and symmetric. That is, for some unitary $U$, where $U^{4}=\mathbb{1}$, it holds that $\left|\psi_{01}\right\rangle=U\left|\psi_{00}\right\rangle,\left|\psi_{11}\right\rangle=U\left|\psi_{01}\right\rangle$, and $\left|\psi_{10}\right\rangle=$ $U\left|\psi_{11}\right\rangle$.
3. Each one of Alice's four bit combinations is chosen with an equal probability of $1 / 4$.
4. Bob obtains either $x_{0}, x_{1}$, or $x_{2}=x_{0} \oplus x_{1}$ with an equal probability of $1 / 3$, when measuring each state $\left|\psi_{x_{0} x_{1}}\right\rangle$.

Regarding conditions one and two, if we have interactive protocols, where Bob needs to distinguish between symmetric states in the final step of the protocol, then the results are also valid lower bounds on the cheating probabilities for these protocols. With regards to conditions three and four, assuming equiprobability for the inputs and outputs is more sensible than considering biased inputs and/or outputs, because any bias can be exploited by cheating parties. Hence, biased protocols, even though generally of course also possible, are usually not considered.

The states $\left|\psi_{x_{0} x_{1}}\right\rangle$ sent by an honest Alice, need to be picked in a way that it is always possible for Bob to correctly obtain one output, i.e. either $x_{0}$ or $x_{1}$ or $x_{2}=x_{0} \oplus x_{1}$. Furthermore, we specified that they are pure and symmetric states and, for a set of such states, the pairwise overlaps satisfy

$$
\begin{align*}
& \left\langle\psi_{01} \mid \psi_{00}\right\rangle=\left\langle\psi_{11} \mid \psi_{01}\right\rangle=\left\langle\psi_{10} \mid \psi_{11}\right\rangle=\left\langle\psi_{00} \mid \psi_{10}\right\rangle=F, \\
& \left\langle\psi_{00} \mid \psi_{11}\right\rangle=\left\langle\psi_{01} \mid \psi_{10}\right\rangle=G . \tag{3.19}
\end{align*}
$$

The eigenvalues of the unitary $U$ are the $4^{\text {th }}$ roots of unity and, thus, $U^{2}$ has eigenvalues $\pm 1$ only. Since $\left|\psi_{11}\right\rangle=U^{2}\left|\psi_{00}\right\rangle, G$ is always real, whereas $F$ is in general complex.

Honest Bob's measurement consists of six measurement operators denoted by $\Pi_{0 *}, \Pi_{1 *}, \Pi_{* 0}, \Pi_{* 1}, \Pi_{\mathrm{XOR}=0}$, and $\Pi_{\mathrm{XOR}=1}$ for Bob getting outcome $x_{0}=0, x_{0}=1$, $x_{1}=0, x_{1}=1, x_{2}=0$, and $x_{2}=1$, respectively. The probability of obtaining outcome $m$ is given by $\left\langle\psi_{i j}\right| \Pi_{m}\left|\psi_{i j}\right\rangle$ for $m \in\{0 *, 1 *, * 0, * 1, \mathrm{XOR}=0, \mathrm{XOR}=1\}$ and $i, j \in\{0,1\}$. When an outcome is possible, this probability should be equal to $1 / 3$ and, when it is not possible, equal to 0 .

In order for honest Bob to be able to correctly learn either $x_{0}, x_{1}$, or $x_{2}=$ $x_{0} \oplus x_{1}$ with probability $1 / 3$ each, the states need to be distinguishable enough, which requires $|F| \leq 1 / 3$ and $|G| \leq 1 / 3$ to hold.

Proposition 3.2. For Bob to correctly learn either the first bit, the second bit, or their XOR, whereby each of these outcomes occurs with a probability of $1 / 3$, it is necessary to hold that

$$
\begin{equation*}
|F| \leq \frac{1}{3} \quad \text { and } \quad|G| \leq \frac{1}{3} \tag{3.20}
\end{equation*}
$$

Proof. The measurement operators $\Pi_{m}$ can be expressed in terms of their eigenvalues and eigenvectors. For instance, $\Pi_{0 *}=\sum_{k} \lambda_{k}\left|\lambda_{k}\right\rangle\left\langle\lambda_{k}\right|$ and similar for the other operators. Looking at the state $\left|\psi_{10}\right\rangle$, it holds that

$$
\begin{equation*}
0=\left\langle\psi_{10}\right| \Pi_{0 *}\left|\psi_{10}\right\rangle=\sum_{k} \lambda_{k}\left|\left\langle\psi_{10} \mid \lambda_{k}\right\rangle\right|^{2}, \tag{3.21}
\end{equation*}
$$

thus, we have $\left\langle\psi_{10} \mid \lambda_{k}\right\rangle=0 \forall k$. For other states and measurement operators, we can derive analogous conditions and we can use these conditions to re-express the overlaps in Eq. (3.19). That is, we, for example, have

$$
\begin{equation*}
F=\left\langle\psi_{01} \mid \psi_{00}\right\rangle=\left\langle\psi_{01}\right| \sum_{m} \Pi_{m}\left|\psi_{00}\right\rangle=\left\langle\psi_{01}\right| \Pi_{0 *}\left|\psi_{00}\right\rangle . \tag{3.22}
\end{equation*}
$$

Proceeding analogously for the other states' overlaps, all the relations in Eq. (3.19) can be rewritten as

$$
\begin{align*}
& \left\langle\psi_{01}\right| \Pi_{0 *}\left|\psi_{00}\right\rangle=\left\langle\psi_{11}\right| \Pi_{* 1}\left|\psi_{01}\right\rangle=\left\langle\psi_{10}\right| \Pi_{1 *}\left|\psi_{11}\right\rangle=\left\langle\psi_{00}\right| \Pi_{* 0}\left|\psi_{10}\right\rangle=F, \\
& \left\langle\psi_{00}\right| \Pi_{\mathrm{XOR}=0}\left|\psi_{11}\right\rangle=\left\langle\psi_{01}\right| \Pi_{\mathrm{XOR}=1}\left|\psi_{10}\right\rangle=G . \tag{3.23}
\end{align*}
$$

Defining the vectors $\mathbf{X}$ and $\mathbf{Y}$ with elements $x_{k}=\sqrt{\lambda_{k}}\left\langle\psi_{01} \mid \lambda_{k}\right\rangle$ and $y_{k}=\sqrt{\lambda_{k}}\left\langle\psi_{00} \mid \lambda_{k}\right\rangle$, respectively, then

$$
\begin{equation*}
|\mathbf{X}|^{2}=\sum_{k} \lambda_{k}\left|\left\langle\psi_{01} \mid \lambda_{k}\right\rangle\right|^{2}=\frac{1}{3} \quad \text { and } \quad|\mathbf{Y}|^{2}=\sum_{k} \lambda_{k}\left|\left\langle\psi_{00} \mid \lambda_{k}\right\rangle\right|^{2}=\frac{1}{3} . \tag{3.24}
\end{equation*}
$$

So it has to hold that

$$
\begin{equation*}
|F|^{2}=\left|\sum_{k} \lambda_{k}\left\langle\psi_{01} \mid \lambda_{k}\right\rangle\left\langle\lambda_{k} \mid \psi_{00}\right\rangle\right|^{2}=\left|\sum_{k} x_{k} y_{k}^{*}\right|^{2} \leq|\mathbf{X}|^{2}|\mathbf{Y}|^{2}=\frac{1}{9} . \tag{3.25}
\end{equation*}
$$

Therefore, $|F| \leq 1 / 3$ and it can be analogously proven that also the condition $|G| \leq 1 / 3$ has to hold.

With these conditions and relations in mind, we look at the cheating probabilities for Alice and Bob in the next subsections. Generally speaking, we will notice that, when the states sent by an honest Alice become more distinguishable, Bob's cheating probability will increase while Alice's cheating probability will decrease. Vice versa is true when honest Alice's states become less distinguishable. Thus, there is a trade-off between Alice's and Bob's cheating probabilities in XOT, as is also the case for 1-2 OT [7, 46, 47].

### 3.3.1 Bob's Cheating Probability

A dishonest Bob wants to learn all three bits, so his aim is to guess both bits $x_{0}$ and $x_{1}$ which implies knowledge of the bit $x_{0} \oplus x_{1}$ as well, as explained in Subsection 3.2.3. Just as for the specific XOT protocol in the previous section, Bob can always cheat with a probability of at least $1 / 2$ by following the protocol honestly and then guessing at random the value(s) of the bit(s) he did not receive. Bob's optimal cheating strategy, however, is the one that minimises the probability of wrongly distinguishing between honest Alice's states, i.e. a minimum-error measurement. As before, since the states are equiprobable and symmetric, his best minimum-error measurement is the square-root measurement (SRM) [73, 74] with measurement operators

$$
\begin{equation*}
\Pi_{x_{0} x_{1}}=\rho_{\text {average }}^{-1 / 2}\left|\psi_{x_{0} x_{1}}\right\rangle\left\langle\psi_{x_{0} x_{1}}\right| \rho_{\text {average }}^{-1 / 2}, \tag{3.26}
\end{equation*}
$$

where $\rho_{\text {average }}=(1 / 4) \sum_{x_{0}, x_{1}=0,1}\left|\psi_{x_{0} x_{1}}\right\rangle\left\langle\psi_{x_{0} x_{1}}\right|$ is the average density matrix sent from Alice to Bob.

Using an approach from [75, 76], the success probability of the SRM for $n$ equiprobable symmetric states can be calculated by

$$
\begin{equation*}
P_{\text {success }}=\frac{1}{n^{2}}\left(\sum_{k=1}^{n} \sqrt{\lambda_{k}}\right)^{2}, \tag{3.27}
\end{equation*}
$$

where $\lambda_{k}$ are the eigenvalues of the Gram matrix for the set of states. The elements of the Gram matrix $\Gamma$ are given by $\Gamma_{i j}=\left\langle\psi_{i} \mid \psi_{j}\right\rangle$, that is, the overlaps between the states. Thus, for Alice's four states, the Gram matrix is

$$
\Gamma=\left(\begin{array}{cccc}
1 & F & G & F^{*}  \tag{3.28}\\
F^{*} & 1 & F & G \\
G & F^{*} & 1 & F \\
F & G & F^{*} & 1
\end{array}\right)
$$

and its eigenvalues are $\lambda_{0}=1-F+G-F^{*}, \lambda_{1}=1-G+i F-i F^{*}, \lambda_{2}=1+F+G+F^{*}$, and $\lambda_{3}=1-G-i F+i F^{*}$. Substituting these eigenvalues into Eq. (3.26), Bob's cheating probability $B_{O T}$ is

$$
\begin{align*}
B_{O T}= & \frac{1}{16}(\sqrt{1+G-2 \operatorname{Re} F}+\sqrt{1-G-2 \operatorname{Im} F} \\
& +\sqrt{1+G+2 \operatorname{Re} F}+\sqrt{1-G+2 \operatorname{Im} F})^{2} \tag{3.29}
\end{align*}
$$

We can make the following observations about the consequences of certain values
for $F$ and $G$ on Bob's cheating probability.

- $B_{O T}$ stays unchanged when $F \rightarrow-F$, while $G$ is kept the same.
- Fixing the absolute values $|F|$ and $|G|, B_{O T}$ is minimised for real $F$ (i.e. $\operatorname{Im} F=0$ ) if $G \leq 0$ and for purely imaginary $F$ (i.e. $\operatorname{Re} F=0$ ) if $G \geq 0$.
- When $|F|$ and $|G|$ decrease, $B_{O T}$ increases, because the states become more distinguishable for smaller $|F|$ and $|G|$. In particular, if $F=G=0$, then $B_{O T}=1$ and the states are perfectly distinguishable.
- On the other hand, if $|F|$ and $|G|$ are equal to their maximum of $1 / 3$ (see Eq. $(3.20)), B_{O T}=3 / 4$, the lowest value it can attain here.


### 3.3.2 Alice's Cheating Probability without Testing by Bob

A dishonest Alice wants to know if Bob has learnt $x_{0}, x_{1}$, or $x_{2}=x_{0} \oplus x_{1}$. As in the specific XOT protocol in the previous section, Alice can always cheat with a probability of at least $1 / 3$ by following the protocol honestly and then randomly guessing which output Bob has received.

When Bob is not doing any testing, Alice wants to maximise Bob's probability to obtain a certain outcome. Her best cheating strategy is to send Bob the pure state within the subspace spanned by the states she sends when she is honest, for which Bob's probability to obtain either the first bit $(b=0)$, the second bit $(b=1)$, or their XOR $(b=2)$ is maximised. Such a state can be written as

$$
\begin{equation*}
\left|\Psi_{\text {cheat }}\right\rangle=\alpha\left|\psi_{00}\right\rangle+\beta\left|\psi_{01}\right\rangle+\gamma\left|\psi_{11}\right\rangle+\delta\left|\psi_{10}\right\rangle, \tag{3.30}
\end{equation*}
$$

where the coefficients $\alpha, \beta, \gamma, \delta \in \mathbb{C}$ are chosen so that the state is normalised. Using the conditions in Eq. (3.23), Bob's probabilities to obtain outcome $b=i$ when measuring $\left|\Psi_{\text {cheat }}\right\rangle, P(b=i)$ for $i \in\{0,1,2\}$, can be expressed as

$$
\begin{align*}
P(b=0) & =\left\langle\Psi_{\text {cheat }}\right| \Pi_{0 *}+\Pi_{1 *}\left|\Psi_{\text {cheat }}\right\rangle \\
& =\frac{1}{3}\left(|\alpha|^{2}+|\beta|^{2}+|\gamma|^{2}+|\delta|^{2}\right)+\left(\alpha \beta^{*}+\gamma \delta^{*}\right) F+\left(\alpha^{*} \beta+\gamma^{*} \delta\right) F^{*}, \\
P(b=1) & =\left\langle\Psi_{\text {cheat }}\right| \Pi_{* 0}+\Pi_{* 1}\left|\Psi_{\text {cheat }}\right\rangle \\
& =\frac{1}{3}\left(|\alpha|^{2}+|\beta|^{2}+|\gamma|^{2}+|\delta|^{2}\right)+\left(\alpha^{*} \delta+\beta \gamma^{*}\right) F+\left(\alpha \delta^{*}+\beta^{*} \gamma\right) F^{*}, \\
P(b=2) & =\left\langle\Psi_{\text {cheat }}\right| \Pi_{\mathrm{XOR}=0}+\Pi_{\mathrm{XOR}=1}\left|\Psi_{\text {cheat }}\right\rangle \\
& =\frac{1}{3}\left(|\alpha|^{2}+|\beta|^{2}+|\gamma|^{2}+|\delta|^{2}\right)+\left(\alpha^{*} \gamma+\beta^{*} \delta+\alpha \gamma^{*}+\beta \delta^{*}\right) G . \tag{3.31}
\end{align*}
$$

Since dishonest Alice's aim is to maximise one of these probabilities, she needs to pick the values for $\alpha, \beta, \gamma$, and $\delta$ in a way to achieve this, while at the same time satisfying the normalisation condition which is $P(b=0)+P(b=1)+P(b=2)=1$.

The expressions for Bob's probabilities $P(b=i)$ with $i \in\{0,1,2\}$ in Eq. (3.31) can be written in terms of vectors and a matrix. In particular,

$$
\begin{equation*}
P(b=i)=\left(\alpha^{*}, \beta^{*}, \gamma^{*}, \delta^{*}\right) M_{i}(\alpha, \beta, \gamma, \delta)^{T}, \tag{3.32}
\end{equation*}
$$

where $i \in\{0,1,2\}$ and the respective matrices are

$$
\begin{align*}
& M_{0}=\left(\begin{array}{cccc}
1 / 3 & F^{*} & 0 & 0 \\
F & 1 / 3 & 0 & 0 \\
0 & 0 & 1 / 3 & F^{*} \\
0 & 0 & F & 1 / 3
\end{array}\right), \\
& M_{1}
\end{align*}=\left(\begin{array}{cccc}
1 / 3 & 0 & 0 & F \\
0 & 1 / 3 & F^{*} & 0  \tag{3.33}\\
0 & F & 1 / 3 & 0 \\
F^{*} & 0 & 0 & 1 / 3
\end{array}\right), ~ 又\left(\begin{array}{cccc}
1 / 3 & 0 & G & 0 \\
0 & 1 / 3 & 0 & G \\
G & 0 & 1 / 3 & 0 \\
0 & G & 0 & 1 / 3
\end{array}\right) .
$$

Using these expressions for the probabilities, the normalisation condition can be written as

$$
\begin{equation*}
\left(\alpha^{*}, \beta^{*}, \gamma^{*}, \delta^{*}\right)\left(M_{0}+M_{1}+M_{2}\right)(\alpha, \beta, \gamma, \delta)^{T}=1 . \tag{3.34}
\end{equation*}
$$

This equation describes an ellipsoid in a four-dimensional complex space and, similarly, when defining constants $C_{0}, C_{1}, C_{2} \in \mathbb{R}$ and setting $P(b=0)=C_{0}, P(b=$ 1) $=C_{1}$, and $P(b=2)=C_{2}$, these probabilities are ellipsoids in a four-dimensional complex space. Using this geometrical interpretation, we derive Alice's cheating probability, when Bob is not testing, as a function of $F$ and $G$. To find the maximum value that $P(b=i)$ can attain while satisfying the normalisation constraint, we need to look for the value of $C_{i}$ for which the two ellipsoids are tangent to each other, when expressed in the same basis. This value for $C_{i}$ is the largest value for it for which the normalisation ellipsoid in Eq. (3.34) and the ellipsoid for $P(b=i)$ still have common points.

The first step is to rescale the principal axes of the normalisation ellipsoid so that they all have the same length and, thereby, transform the ellipsoid into a sphere in four-dimensional complex space. In particular, the sphere should have a radius of one, i.e. all its semi-axes should have length one. Later, we will also rescale the other ellipsoids in the same way so that they are transformed into the same basis as the normalisation ellipsoid.

Expressing an ellipsoid in terms of the eigenvalues and eigenvectors of its corresponding matrix, gives information about the principal axes. That is, in the eigenbasis of the corresponding matrix, the ellipsoid can be expressed as $\sum_{i} \lambda_{i}\left|x_{i}\right|^{2}=C$. The $\lambda_{i}$ are thereby the eigenvalues of the matrix and the reciprocals of the squares of the semi-axes, the $x_{i}$ are the eigenvectors of the matrix and the coordinates of the principal axes expressed in the eigenbasis, and $C$ is a constant. For such an ellipsoid, the lengths of the semi-axes are specified by $\sqrt{C / \lambda_{i}}$. To rescale the principal axes of the normalisation ellipsoid, we need the eigenvalues and eigenvectors of the matrix $\left(M_{0}+M_{1}+M_{2}\right)$. This matrix is circulant and has normalised eigenvectors

$$
\begin{array}{rlrl}
\left|\lambda_{0}\right\rangle & =\frac{1}{2}(1,1,1,1)^{T}, & \left|\lambda_{1}\right\rangle & =\frac{1}{2}(1, i,-1,-i)^{T}, \\
\left|\lambda_{2}\right\rangle & =\frac{1}{2}(1,-1,1,-1)^{T}, & \left|\lambda_{3}\right\rangle=\frac{1}{2}(1,-i,-1,1)^{T}
\end{array}
$$

with their respective eigenvalues

$$
\begin{array}{ll}
\lambda_{0}=1+G+2 \operatorname{Re} F, & \lambda_{1}=1-G+2 \operatorname{Im} F, \\
\lambda_{2}=1+G-2 \operatorname{Re} F, & \lambda_{3}=1-G-2 \operatorname{Im} F . \tag{3.36}
\end{array}
$$

We transform the normalisation ellipsoid, i.e. scale its coordinates so that it coincides with a sphere, by first diagonalising its corresponding matrix. The resulting diagonal matrix has the eigenvalues as its elements. Dividing them by the respective eigenvalues, that is, by themselves, yields the ellipsoid which is a sphere of radius one in four-dimensional complex space. Defining a matrix $V$ whose columns are the eigenvectors given in Eq. (3.35), and a diagonal matrix with elements equal to the square-roots of the eigenvalues in Eq. (3.36), i.e. $D_{s q}=\operatorname{diag}\left(\sqrt{\lambda_{0}}, \sqrt{\lambda_{1}}, \sqrt{\lambda_{2}}, \sqrt{\lambda_{3}}\right)$, allows expressing this whole process as

$$
\begin{equation*}
D_{s q}^{-1} V^{\dagger}\left(M_{0}+M_{1}+M_{2}\right) V D_{s q}^{-1}=\operatorname{diag}(1,1,1,1) . \tag{3.37}
\end{equation*}
$$

In order to obtain the largest value possible for $C_{i}$ while satisfying the condition that the normalisation ellipsoid and the ellipsoid of $M_{i}$ still share some points, we
need to transform the matrix $M_{i}$ into the same basis as $\left(M_{0}+M_{1}+M_{2}\right)$. This "squashes" the ellipsoid corresponding to the matrix $M_{i}$. The largest value for $C_{i}$ is then attained when the shortest principal axis of the transformed ellipsoid for $M_{i}$ also has length one. This results in the normalisation ellipsoid (now a sphere) being contained within this transformed ellipsoid. Since generally the lengths of the semi-axes are given by $\sqrt{C / \lambda_{i}}$, it is necessary to consider the largest eigenvalue $\lambda_{\max }$ for the shortest semi-axis. Because the length of this shortest semi-axis needs to be equal to one, it must hold that $\lambda_{\max }=C$. Thus, we first transform the matrices $M_{0}$, $M_{1}$, and $M_{2}$ accordingly and then calculate their eigenvalues. After transformation $D_{s q}^{-1} V^{\dagger} M_{i} V D_{s q}^{-1}$ for $i \in\{0,1,2\}$, the matrices become

$$
\begin{align*}
& \widetilde{M}_{0}=\left(\begin{array}{cccc}
\frac{(1 / 3)+\operatorname{Re} F}{1+G+2 \operatorname{Re} F} & 0 & \frac{i \operatorname{Im} F}{\sqrt{(1+G)^{2}-4(\operatorname{Re} F)^{2}}} & 0 \\
0 & \frac{(1 / 3)+\operatorname{Im} F}{1-G+2 \operatorname{Im} F} & 0 & \frac{-i \operatorname{Re} F}{\sqrt{(1-G)^{2}-4(\operatorname{Im} F)^{2}}} \\
\frac{-i \operatorname{Im} F}{\sqrt{(1+G)^{2}-4(\operatorname{Re} F)^{2}}} & 0 & \frac{(1 / 3)-\operatorname{Re} F}{1+G-2 \operatorname{Re} F} & 0 \\
0 & \frac{i \operatorname{Re} F}{\sqrt{(1-G)^{2}-4(\operatorname{Im} F)^{2}}} & 0 & \frac{(1 / 3)-\operatorname{Im} F}{1-G-2 \operatorname{Im} F}
\end{array}\right), \\
& \widetilde{M}_{1}=\left(\begin{array}{cc}
\frac{(1 / 3)+\operatorname{Re} F}{1+G+2 \operatorname{Re} F} & 0 \\
0 & \frac{(1 / 3)+\operatorname{Im} F}{1-G+2 \operatorname{Im} F} \\
\frac{i \operatorname{Im} F}{\sqrt{(1+G)^{2}-4(\operatorname{Re} F)^{2}}} & 0 \\
0 & \frac{-i \operatorname{Re} F}{\sqrt{(1-G)^{2}-4(\operatorname{Im} F)^{2}}}
\end{array}\right. \\
& \frac{-i \operatorname{Im} F}{\sqrt{(1+G)^{2}-4(\operatorname{Re} F)^{2}}} \\
& \widetilde{M}_{2}=\left(\begin{array}{cccc}
\frac{(1 / 3)+G}{1+3 G+2 \operatorname{Re} F} & 0 & 0 & 0 \\
0 & \frac{(1 / 3)-G}{1-G+2 \operatorname{m} F} & 0 & 0 \\
0 & 0 & \frac{(1 / 3)+G}{1+G-2 \operatorname{Re} F} & 0 \\
0 & 0 & 0 & \frac{(1 / 3)-G}{1-G-2 \operatorname{Im} F}
\end{array}\right) . \tag{3.38}
\end{align*}
$$

The matrices $\widetilde{M}_{0}$ and $\widetilde{M}_{1}$ share the same eigenvalues, that is,

$$
\begin{aligned}
\tilde{\lambda}_{00 / 02}=\widetilde{\lambda}_{10 / 12}= & \frac{1}{(1+G)^{2}-4(\operatorname{Re} F)^{2}}\left[\frac{1}{3}(1+G)-2(\operatorname{Re} F)^{2}\right. \\
& \left. \pm \sqrt{\left(\frac{1}{3}+G\right)^{2}(\operatorname{Re} F)^{2}+\left[(1+G)^{2}-4(\operatorname{Re} F)^{2}\right](\operatorname{Im} F)^{2}}\right]
\end{aligned}
$$

$$
\begin{align*}
\tilde{\lambda}_{01 / 03}=\tilde{\lambda}_{11 / 13}= & \frac{1}{(1-G)^{2}-4(\operatorname{Im} F)^{2}}\left[\frac{1}{3}(1-G)-2(\operatorname{Im} F)^{2}\right. \\
& \left. \pm \sqrt{\left(\frac{1}{3}-G\right)^{2}(\operatorname{Im} F)^{2}+\left[(1-G)^{2}-4(\operatorname{Im} F)^{2}\right](\operatorname{Re} F)^{2}}\right] \tag{3.39}
\end{align*}
$$

where the + sign is used for $\widetilde{\lambda}_{00}, \widetilde{\lambda}_{10}, \widetilde{\lambda}_{01}$, and $\widetilde{\lambda}_{11}$ and the - sign is used for $\widetilde{\lambda}_{02}$, $\widetilde{\lambda}_{12}, \widetilde{\lambda}_{03}$, and $\widetilde{\lambda}_{13}$. Since the eigenvalues for $b=0$ and $b=1$ are identical, we will, for simplicity, from now on only refer to the ones for $b=0$, which then yield the valid probability for both cases.

Obviously, the eigenvalues with the + sign are larger. Depending on which of $\widetilde{\lambda}_{00}$ or $\widetilde{\lambda}_{01}$ is the larger eigenvalue, the value in question gives the largest possible probability for $P(b=0)$ and $P(b=1)$, i.e.

$$
\begin{equation*}
P(b=0)_{\max }=P(b=1)_{\max }=\max \left(\widetilde{\lambda}_{00}, \widetilde{\lambda}_{01}\right) . \tag{3.40}
\end{equation*}
$$

The transformed matrix $\widetilde{M}_{2}$ is diagonal, hence the eigenvalues can be read off from the elements along the main diagonal, yielding

$$
\begin{array}{ll}
\tilde{\lambda}_{20}=\frac{(1 / 3)+G}{1+G+2 \operatorname{Re} F}, & \widetilde{\lambda}_{21}=\frac{(1 / 3)-G}{1-G+2 \operatorname{Im} F}, \\
\tilde{\lambda}_{22}=\frac{(1 / 3)+G}{1+G-2 \operatorname{Re} F}, & \widetilde{\lambda}_{23}=\frac{(1 / 3)-G}{1-G-2 \operatorname{Im} F} . \tag{3.41}
\end{array}
$$

When $\operatorname{Re} F$ is smaller than zero, then $\widetilde{\lambda}_{20}>\widetilde{\lambda}_{22}$ and vice versa otherwise. Similarly, when $\operatorname{Im} F$ is smaller than zero, then $\widetilde{\lambda}_{21}>\widetilde{\lambda}_{23}$ and vice versa otherwise. Since only the larger eigenvalues are of interest, we can combine them, changing their denominators, as $[(1 / 3)+G] /[1+G-2|\operatorname{Re} F|]$ and $[(1 / 3)-G] /[1-G-2|\operatorname{Im} F|]$. Furthermore, we can calculate in terms of $\operatorname{Re} F$ and $\operatorname{Im} F$ the values of $G$ for which these expressions intersect, and, by plotting them, we can confirm which expression is larger for $G$ values greater or smaller than the $G$ values at the intersection. That is, the largest possible probability for $P(b=2)$ is

$$
P(b=2)_{\max }= \begin{cases}\frac{(1 / 3)+G}{1+G-2|\operatorname{Re} F|} & \text { if } G \geq \frac{|\operatorname{Im} F|-|\operatorname{Re} F|}{2-3|\operatorname{Re} F|-3|\operatorname{Im} F|}  \tag{3.42}\\ \frac{(1 / 3)-G}{1-G-2|\operatorname{Im} F|} & \text { if } G<\frac{|\operatorname{Im} F|-|\operatorname{Re} F|}{2-3|\operatorname{Re} F|-3|\operatorname{Im} F|}\end{cases}
$$

All in all, Alice's cheating probability when Bob is not testing is then given by
the maximum of Eqns. (3.40) and (3.42), that is,

$$
\begin{equation*}
\left.A_{O T}=\max (P(b=0))=P(b=1), P(b=2)\right) . \tag{3.43}
\end{equation*}
$$

In order to be able to get a better understanding about the expressions describing Alice's cheating probability, we plot $A_{O T}$ in terms of $\operatorname{Re} F$ and $\operatorname{Im} F$, when fixing $G=-1 / 3, G=-1 / 6$, and $G=0$, in Figure 3.2.

We can make the following observations about the consequences of certain values for $\operatorname{Re} F, \operatorname{Im} F$, and $G$ on Alice's cheating probability.

- The sign of $\operatorname{Re} F$ and $\operatorname{Im} F$ does not have influence on $A_{O T}$ as either their absolute values are used or they are squared.
- When interchanging $\operatorname{Re} F$ and $\operatorname{Im} F$ and simultaneously changing $G$ to $-G$, then $A_{O T}$ remains unchanged.
- When $|F|$ and $|G|$ increase, $A_{O T}$ increases.

We look in more detail at what the best choices for $F$ and $G$ are in Subsection 3.3.4. In the analysis, we will consider Alice's cheating probability with and without testing by Bob as well as Bob's cheating probability.

### 3.3.3 Alice's Cheating Probability with Testing by Bob

Next, we will look at Alice's cheating probability when Bob is implementing some testing procedure. The testing method is the same as in Subsection 3.2.4 for the specific XOT protocol. That is, Bob tests a fraction of the states Alice sends him, and checks if they are what she claims they are.

Since Alice does not want Bob to detect that she is cheating, she needs to always pass Bob's tests, which she can do when she sends an equal superposition of the states she is supposed to send, entangled with a system she keeps on her side. Such a state is of the form

$$
\begin{equation*}
\left|\Psi_{\text {cheat }}\right\rangle=a|0\rangle_{A} \otimes\left|\psi_{00}\right\rangle+b|1\rangle_{A} \otimes\left|\psi_{01}\right\rangle+c|2\rangle_{A} \otimes\left|\psi_{11}\right\rangle+d|3\rangle_{A} \otimes\left|\psi_{10}\right\rangle, \tag{3.44}
\end{equation*}
$$

where $\left\{|0\rangle_{A},|1\rangle_{A},|2\rangle_{A},|3\rangle_{A}\right\}$ is an orthonormal basis for the system Alice keeps and $|a|^{2}+|b|^{2}+|c|^{2}+|d|^{2}=1$. When Alice measures her system in this basis, she prepares one of the states she is supposed to send to Bob, thus, she can always pass his tests.

(b)


(d)
(e)


$\square \frac{1 / 3+G}{1+G-2|\operatorname{Re} F|}$

$$
\square \frac{1 / 3-G}{1-G-2|\operatorname{Im} F|}
$$

Figure 3.2: Alice's cheating probability as given by the maximum expressions in Eqns. (3.40) and (3.42) fixing certain values of $G$. That is, in (a) and (d), we have $G=-1 / 3$, in (b) and (e), we have $G=-1 / 6$, and, in (c) and (f), we have $G=0$. The plots in the first column, i.e. (a), (b), and (c), show the top view of their 3D counterparts in the second column, i.e. (d), (e), and (f), respectively.

We suspect that it is optimal for Alice to have $a=b=c=d=1 / 2$, so all four constants are set equal to $1 / 2$ in further calculations. Even if these values are not optimal, this will nevertheless give a lower bound on Alice's cheating probability. After honest Bob has done his measurement, described by the measurement operators $\Pi_{0 *}, \Pi_{1 *}, \Pi_{* 0}, \Pi_{* 1}, \Pi_{\mathrm{XOR}=0}$, and $\Pi_{\mathrm{XOR}=1}$, on the system he received, Alice's $A$ system is prepared in one of three states, depending on whether Bob has obtained
$x_{0}, x_{1}$, or $x_{2}=x_{0} \oplus x_{1}$. That is,

$$
\begin{equation*}
\mu_{A}^{b=0}=\frac{1}{p_{0 *}+p_{1 *}} \operatorname{Tr}_{\text {Bob }}\left[\left(\Pi_{0 *}+\Pi_{1 *}\right)^{1 / 2}\left|\Psi_{\text {cheat }}\right\rangle\left\langle\Psi_{\text {cheat }}\right|\left(\Pi_{0 *}+\Pi_{1 *}\right)^{1 / 2}\right], \tag{3.45}
\end{equation*}
$$

where $p_{0 *}+p_{1 *}=\operatorname{Tr}\left[\left|\Psi_{\text {cheat }}\right\rangle\left\langle\Psi_{\text {cheat }}\right|\left(\Pi_{0 *}+\Pi_{1 *}\right)\right]=1 / 3$, and analogously for $\mu_{A}^{b=1}$ and $\mu_{A}^{b=2}$. Using the conditions given in Eq. (3.23), the states Alice needs to distinguish between can be expressed as

$$
\begin{align*}
& \mu_{A}^{b=0}=\frac{1}{4}\left(\begin{array}{cccc}
1 & 3 F & 0 & 0 \\
3 F^{*} & 1 & 0 & 0 \\
0 & 0 & 1 & 3 F \\
0 & 0 & 3 F^{*} & 1
\end{array}\right), \\
& \mu_{A}^{b=1}=\frac{1}{4}\left(\begin{array}{cccc}
1 & 0 & 0 & 3 F^{*} \\
0 & 1 & 3 F & 0 \\
0 & 3 F^{*} & 1 & 0 \\
3 F & 0 & 0 & 1
\end{array}\right), \\
& \mu_{A}^{b=2}=\frac{1}{4}\left(\begin{array}{cccc}
1 & 0 & 3 G & 0 \\
0 & 1 & 0 & 3 G \\
3 G & 0 & 1 & 0 \\
0 & 3 G & 0 & 1
\end{array}\right), \tag{3.46}
\end{align*}
$$

corresponding to Bob obtaining $x_{0}, x_{1}$, or $x_{2}=x_{0} \oplus x_{1}$, and all three states occur with equal probability $1 / 3$.

The states in Eq. (3.46) are mirror-symmetric; the unitary transformation that takes $|0\rangle \rightarrow|3\rangle,|3\rangle \rightarrow|2\rangle,|2\rangle \rightarrow|1\rangle$, and $|1\rangle \rightarrow|0\rangle$, interchanges $\mu_{A}^{b=0}$ and $\mu_{A}^{b=1}$ with each other while keeping $\mu_{A}^{b=2}$ unchanged. For some sets of mirror-symmetric states, the optimal minimum-error measurement is known [77, 78] but this set of states is not one of them.

We can, however, obtain Alice's optimal minimum-error measurement by making use of a basis transform that block-diagonalises all three $\mu_{A}^{b=i}$ with $i \in\{0,1,2\}$. First of all, note that Alice's basis states can be realised as two-qubit states $|0\rangle_{A} \equiv$ $|00\rangle,|1\rangle_{A} \equiv|01\rangle,|2\rangle_{A} \equiv|10\rangle$, and $|3\rangle_{A} \equiv|11\rangle$ and this is the same as using the
 we will use as the "primary" basis for the rest of the calculations.

Now, applying the unitary transformation $U$ that is proportional to a $4 \times 4$

Hadamard-Walsh matrix,

$$
U=\frac{1}{2}\left(\begin{array}{cccc}
1 & 1 & 1 & 1  \tag{3.47}\\
1 & -1 & 1 & -1 \\
1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1
\end{array}\right)
$$

to the states in Eq. (3.46), i.e. $U \mu_{A}^{b=i} U^{\dagger}$ for $i \in\{0,1,2\}$, changes the density matrices to

$$
\begin{align*}
& \mu_{A}^{b=0}=\frac{1}{4}\left(\begin{array}{cccc}
1+3 \operatorname{Re} F & -3 i \operatorname{Im} F & 0 & 0 \\
3 i \operatorname{Im} F & 1-3 \operatorname{Re} F & 0 & 0 \\
0 & 0 & 1+3 \operatorname{Re} F & -3 i \operatorname{Im} F \\
0 & 0 & 3 i \operatorname{Im} F & 1-3 \operatorname{Re} F
\end{array}\right), \\
& \mu_{A}^{b=1}=\frac{1}{4}\left(\begin{array}{cccc}
1+3 \operatorname{Re} F & 3 i \operatorname{Im} F & 0 & 0 \\
-3 i \operatorname{Im} F & 1-3 \operatorname{Re} F & 0 & 0 \\
0 & 0 & 1-3 \operatorname{Re} F & -3 i \operatorname{Im} F \\
0 & 0 & 3 i \operatorname{Im} F & 1+3 \operatorname{Re} F
\end{array}\right), \\
& \mu_{A}^{b=2}=\frac{1}{4}\left(\begin{array}{cccc}
1+3 G & 0 & 0 & 0 \\
0 & 1+3 G & 0 & 0 \\
0 & 0 & 1-3 G & 0 \\
0 & 0 & 0 & 1-3 G
\end{array}\right) . \tag{3.48}
\end{align*}
$$

As indicated, the basis transform made all three density matrices block-diagonal and we can deduce the optimal minimum-error measurement. In particular, Alice first needs to perform a projective measurement on the subspaces corresponding to each block and then, depending on the outcome, she needs to distinguish between the three density matrices in the relevant subspace. Considering that the density matrices are written in the $\{|++\rangle,|+-\rangle,|-+\rangle,|--\rangle\}$ basis, the two subspaces are the one where the first qubit is $|+\rangle$, and the one where the first qubit is $|-\rangle$. Thus, Alice needs to measure the first qubit in the $\{|+\rangle,|-\rangle\}$ basis, in order to determine the relevant subspace.

In the next step, Alice wants to distinguish between the three density matrices in the relevant subspace. Thus, we examine them in order to find the optimal measurement within each subspace. Since $\mu_{A}^{b=2}$ is proportional to an identity matrix in both subspaces, no further additional measurement will provide any more information about the likelihood that this was the state Alice held. Therefore, we
focus on how best to distinguish the other two density matrices in the subspaces. In the subspace belonging to the outcome $|+\rangle$ for the first qubit, the elements that disagree for $\mu_{A}^{b=0}$ and $\mu_{A}^{b=1}$, are the ones on the off-diagonals. So, projecting onto $|R\rangle=(|+\rangle+i|-\rangle) / \sqrt{2}$ and $|L\rangle=(|+\rangle-i|-\rangle) / \sqrt{2}$ allows distinguishing between them. On the other hand, in the subspace belonging to the outcome $|-\rangle$ for the first qubit, the elements that disagree for $\mu_{A}^{b=0}$ and $\mu_{A}^{b=1}$, are the ones on the diagonal and they can be distinguished by measuring the second qubit in the $\{|+\rangle,|-\rangle\}$ basis as well.

Still in the basis $\{|++\rangle,|+-\rangle,|-+\rangle,|--\rangle\}$, Alice's optimal measurement operators for the minimum-error measurement are therefore

$$
\begin{align*}
& \Pi_{+R}=|+R\rangle\langle+R|=\frac{1}{2}\left(\begin{array}{cccc}
1 & -i & 0 & 0 \\
i & 1 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{array}\right), \quad \Pi_{-+}=|-+\rangle\langle-+|=\left(\begin{array}{llll}
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0
\end{array}\right), \\
& \Pi_{+L}=|+L\rangle\langle+L|=\frac{1}{2}\left(\begin{array}{cccc}
1 & i & 0 & 0 \\
-i & 1 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{array}\right), \quad \Pi_{--}=|--\rangle\langle--|=\left(\begin{array}{llll}
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1
\end{array}\right) . \tag{3.49}
\end{align*}
$$

The probability of a certain outcome $x$ when Alice holds $\mu_{A}^{b=i}$, with $i \in\{0,1,2\}$ and $x \in\{+R,+L,-+,--\}$, is $P\left(x \mid \mu_{A}^{b=i}\right)=\operatorname{Tr}\left(\Pi_{x} \mu_{A}^{b=i}\right)$. Thus,

$$
\begin{align*}
& P\left(+R \mid \mu_{A}^{b=0}\right)=P\left(+L \mid \mu_{A}^{b=1}\right)=\frac{1}{4}(1+3 \operatorname{Im} F), \\
& P\left(+L \mid \mu_{A}^{b=0}\right)=P\left(+R \mid \mu_{A}^{b=1}\right)=\frac{1}{4}(1-3 \operatorname{Im} F), \\
& P\left(+L \mid \mu_{A}^{b=2}\right)=P\left(+R \mid \mu_{A}^{b=2}\right)=\frac{1}{4}(1+3 G), \\
& P\left(-+\mid \mu_{A}^{b=0}\right)=P\left(--\mid \mu_{A}^{b=1}\right)=\frac{1}{4}(1+3 \operatorname{Re} F), \\
& P\left(--\mid \mu_{A}^{b=0}\right)=P\left(-+\mid \mu_{A}^{b=1}\right)=\frac{1}{4}(1-3 \operatorname{Re} F), \\
& P\left(-+\mid \mu_{A}^{b=2}\right)=P\left(--\mid \mu_{A}^{b=2}\right)=\frac{1}{4}(1-3 G) . \tag{3.50}
\end{align*}
$$

Depending on the outcome Alice obtained, she will always choose the most likely value for $b$. Which $b$ is the most likely can, however, vary since the probabilities depend on the values of $\operatorname{Re} F, \operatorname{Im} F$, and $G$. First note that, for $\mu_{A}^{b=0}$ and $\mu_{A}^{b=1}$,
opposite outcomes, i.e. $+R$ and $+L$ or -+ and -- , have the same probability. The same outcome for $\mu_{A}^{b=0}$ and $\mu_{A}^{b=1}$ has different probabilities though and which probability is larger depends on if $\operatorname{Im} F$ or $\operatorname{Re} F$ is greater or smaller than zero. For instance, for outcome $+R, \mu_{A}^{b=0}$ is more likely when $\operatorname{Im} F>0$, but $\mu_{A}^{b=1}$ is more likely when $\operatorname{Im} F<0$. Thus, we combine the probabilities for certain outcomes when either $\mu_{A}^{b=0}$ or $\mu_{A}^{b=1}$ was held by Alice, into $(1+3|\operatorname{Im} F|) / 4$ and $(1+3|\operatorname{Re} F|) / 4$. These are used in the following analysis determining which expressions from Eq. (3.50) are larger for certain values of $\operatorname{Re} F, \operatorname{Im} F$, and $G$.

|  | $G>0$ | $G \leq 0$ |
| :---: | :---: | :---: |
| $\|G\|<\|\operatorname{Im} F\|$ | $1+3 G<1+3\|\operatorname{Im} F\|$ | $1+3 G<1+3\|\operatorname{Im} F\|$ |
| $\|G\|>\|\operatorname{Im} F\|$ | $1+3 G>1+3\|\operatorname{Im} F\|$ | $1+3 G<1+3\|\operatorname{Im} F\|$ |
| $\|G\|<\|\operatorname{Re} F\|$ | $1-3 G<1+3\|\operatorname{Re} F\|$ | $1-3 G<1+3\|\operatorname{Re} F\|$ |
| $\|G\|>\|\operatorname{Re} F\|$ | $1-3 G<1+3\|\operatorname{Re} F\|$ | $1-3 G>1+3\|\operatorname{Re} F\|$ |

Summarising and combining the results from Eq. (3.50) and the consequences of certain values for $F$ and $G$ presented in the table above allows bounding Alice's cheating probability $A_{O T}$ by

$$
A_{O T} \geq \begin{cases}\frac{1}{3}+\frac{1}{2}|\operatorname{Im} F|+\frac{1}{2} \max (|\operatorname{Re} F|,|G|) & \text { for } G \leq 0  \tag{3.51}\\ \frac{1}{3}+\frac{1}{2}|\operatorname{Re} F|+\frac{1}{2} \max (|\operatorname{Im} F|,|G|) & \text { for } G>0\end{cases}
$$

We can make the following observations about the consequences of certain values for $F$ and $G$ on Alice's cheating probability.

- $A_{O T}$ stays unchanged when $F \rightarrow-F$, while $G$ is kept the same.
- Fixing the absolute values $|F|$ and $|G|, A_{O T}$ is minimised for real $F$ (i.e. $\operatorname{Im} F=0$ ) if $G \leq 0$ and for purely imaginary $F$ (i.e. $\operatorname{Re} F=0$ ) if $G \geq 0$.
- The bound, if $G=0$, is the same for a real $F$ and a purely imaginary $F$, as long as they have the same $|F|$.
- When $|F|$ and $|G|$ increase, $A_{O T}$ increases.

This demonstrates the trade-off between Alice's and Bob's cheating probabilities since $A_{O T}$ increases when $|F|$ and $|G|$ increase, while $B_{O T}$ decreases when $|F|$ and
$|G|$ increase. The trade-off was the same for a dishonest Alice with no testing by Bob. For fixed absolute values $|F|$ and $|G|$, however, the same options that will minimise $A_{O T}$ here, also minimise $B_{O T}$ as shown in Subsection 3.3.1.

### 3.3.4 Optimal Sets of States

Since the condition in Eq. (3.20), that $|F|,|G| \leq 1 / 3$, needs to hold for Bob to correctly obtain one of the three possible outcomes, this restricts the range for the overlaps. The question remains as to what conclusions are possible about the best values for the overlaps and, hence, the optimal sets of states to use in the considered kind of XOT protocols.

As already mentioned in Subsection 3.3.1, Bob's cheating probability reaches its minimum $B_{\text {OT }}=3 / 4$ when both $|F|$ and $|G|$ are equal to their maximum value of $1 / 3$. Since $G$ is real, this means that we have either $G=-1 / 3$ or $G=1 / 3 . \quad F$, however, can be a complex number, so, in order to obtain the best values for $F$, we need to include its phase in the consideration. That is, we set

$$
\begin{equation*}
F=\frac{1}{3} e^{i \theta_{F}}=\frac{1}{3}\left(\cos \theta_{F}+i \sin \theta_{F}\right), \tag{3.52}
\end{equation*}
$$

which means that $\operatorname{Re} F=\frac{1}{3} \cos \theta_{F}$ and $\operatorname{Im} F=\frac{1}{3} \sin \theta_{F}$. Substituting these into the expression for Bob's cheating probability in Eq. (3.29), gives
$B_{O T}= \begin{cases}\frac{1}{24}\left(\sqrt{2-\cos \theta_{F}}+\sqrt{2+\cos \theta_{F}}+\sqrt{1-\sin \theta_{F}}+\sqrt{1+\sin \theta_{F}}\right)^{2} & \text { if } G=+\frac{1}{3} \\ \frac{1}{24}\left(\sqrt{1-\cos \theta_{F}}+\sqrt{1+\cos \theta_{F}}+\sqrt{2-\sin \theta_{F}}+\sqrt{2+\sin \theta_{F}}\right)^{2} & \text { if } G=-\frac{1}{3} .\end{cases}$
$B_{O T}=3 / 4$, when $\theta_{F}=(2 n+1) \pi / 2$, where $n \in\{0,1\}$, in the first case and when $\theta_{F}=(n+1) \pi$, where $n \in\{0,1\}$, in the second case. Thus, the best overlap combinations to restrict a dishonest Bob are either $G=1 / 3$ and $F= \pm i / 3$ or $G=-1 / 3$ and $F= \pm 1 / 3$.

Because of the trade-off between Alice's and Bob's cheating probabilities, we know that having $|F|$ and $|G|$ as large as possible is generally the worst choice against a dishonest Alice. However, decreasing $|F|$ and $|G|$ will increase $B_{O T}$ which is already rather high at $3 / 4$. Thus, we will fix $|F|=|G|=1 / 3$ and check which phase for $F$ is then the best to choose, depending on if $G$ is greater or smaller than zero.

In the case where Bob is not testing if Alice cheats, Bob's probabilities to obtain
$b=0, b=1$, or $b=2$ in Eq. (3.31) can be rewritten. Substituting in $F=|F| e^{i \theta_{F}}$, the equation for $P(b=0)$ becomes

$$
\begin{align*}
P(b=0) & =\frac{1}{3}\left(|\alpha|^{2}+|\beta|^{2}+|\gamma|^{2}+|\delta|^{2}\right)+|F|\left(\alpha \beta^{*} e^{i \theta_{F}}+\gamma \delta^{*} e^{i \theta_{F}}+\alpha^{*} \beta e^{-i \theta_{F}}+\gamma^{*} \delta e^{-i \theta_{F}}\right) \\
& =\left(\frac{1}{3}-|F|\right)\left(|\alpha|^{2}+|\beta|^{2}+|\gamma|^{2}+|\delta|^{2}\right)+|F|\left(\left|\alpha e^{i \theta_{F}}+\beta\right|^{2}+\left|\gamma e^{i \theta_{F}}+\delta\right|^{2}\right) \tag{3.54}
\end{align*}
$$

and, similarly, $P(b=1)$ and $P(b=2)$ can be rewritten as

$$
\begin{align*}
& P(b=1)=\left(\frac{1}{3}-|F|\right)\left(|\alpha|^{2}+|\beta|^{2}+|\gamma|^{2}+|\delta|^{2}\right)+|F|\left(\left|\alpha e^{-i \theta_{F}}+\delta\right|^{2}+\left|\beta+\gamma e^{-i \theta_{F}}\right|^{2}\right), \\
& P(b=2)=\left(\frac{1}{3}-|G|\right)\left(|\alpha|^{2}+|\beta|^{2}+|\gamma|^{2}+|\delta|^{2}\right)+|G|\left(|\alpha \pm \gamma|^{2}+|\beta \pm \delta|^{2}\right) \tag{3.55}
\end{align*}
$$

where, in the equation for $P(b=2)$, the $+\operatorname{sign}$ is used when $G>0$ and the - sign is used when $G<0$.

A cheating Alice wants to minimise two of these equations, while maximising the third one. For $|F|=|G|=1 / 3$, Alice can actually set $P(b=2)$ and either $P(b=0)$ or $P(b=1)$ equal to zero while simultaneously having a probability of 1 for the remaining $b$. The only exceptions are when $G=1 / 3$ and $F= \pm i / 3$ or $G=-1 / 3$ and $F= \pm 1 / 3$. Thus, unless one of these four combinations for the overlaps are picked, Alice can cheat perfectly when $|F|=|G|=1 / 3$.

For instance, when $G=1 / 3$, dishonest Alice can pick $\alpha=-\delta e^{i \theta_{F}}=\beta e^{i \theta_{F}}=-\gamma$ which will result in $P(b=1)=P(b=2)=0$. At the same time, $P(b=0)=1$ due to the normalisation condition. However, when $e^{2 i \theta_{F}}=-1$, then $P(b=0)$ cannot equal 1 , so the normalisation condition cannot be satisfied and the chosen relationship between $\alpha, \beta, \gamma$, and $\delta$ is not a valid choice for Alice. When $\theta_{F}=(2 n+1) \pi / 2$ with $n \in\{0,1\}, e^{2 i \theta_{F}}=-1$ holds and in this case $F= \pm i / 3$.

Similarly, it can be shown that it is necessary to have $\theta_{F}=(n+1) \pi$ with $n \in$ $\{0,1\}$, i.e. $F= \pm 1 / 3$, in order to avoid perfect cheating by Alice when $G=-1 / 3$. In these cases, Alice's cheating probability with no testing by Bob equals $A_{O T}=1 / 2$.

Furthermore, also for a dishonest Alice with testing by Bob, these same choices for $\theta_{F}$ are optimal. We can conclude this from the observation made at the end of Subsection 3.3.3 that, for fixed $|F|$ and $|G|$, it is best to choose $\operatorname{Im} F=0$ if $G \leq 0$ and $\operatorname{Re} F=0$ if $G \geq 0$; i.e. have a real $F$ when $G=-1 / 3$ and a purely imaginary $F$ when $G=1 / 3$. These choices yield Alice's cheating probability $A_{O T}=1 / 2$, when

Bob is testing.
Therefore, we can say that states which satisfy these overlap combinations are optimal among non-interactive XOT protocols with symmetric pure states. We present sets of such states below. Note that the set of states for $F=1 / 3$ and $G=-1 / 3$ is the same as in the protocol in Section 3.2, thus, confirming that this protocol is indeed optimal as was already indicated in that section.
$\underline{G=-1 / 3, F=1 / 3}$

$$
\begin{array}{ll}
\left|\phi_{00}\right\rangle=\frac{1}{\sqrt{3}}(|0\rangle+|1\rangle+|2\rangle), & \left|\phi_{01}\right\rangle=\frac{1}{\sqrt{3}}(|0\rangle-|1\rangle+|2\rangle), \\
\left|\phi_{11}\right\rangle=\frac{1}{\sqrt{3}}(|0\rangle-|1\rangle-|2\rangle), & \left|\phi_{10}\right\rangle=\frac{1}{\sqrt{3}}(|0\rangle+|1\rangle-|2\rangle) \tag{3.56}
\end{array}
$$

$\underline{G=-1 / 3, F=-1 / 3}$

$$
\begin{array}{ll}
\left|\phi_{00}\right\rangle=\frac{1}{\sqrt{3}}(|0\rangle+|1\rangle+|2\rangle), & \left|\phi_{01}\right\rangle=\frac{1}{\sqrt{3}}(-|0\rangle-|1\rangle+|2\rangle), \\
\left|\phi_{11}\right\rangle=\frac{1}{\sqrt{3}}(|0\rangle-|1\rangle-|2\rangle), & \left|\phi_{10}\right\rangle=\frac{1}{\sqrt{3}}(-|0\rangle+|1\rangle-|2\rangle) . \tag{3.57}
\end{array}
$$

$\underline{G=+1 / 3, F=i / 3}$

$$
\begin{array}{ll}
\left|\phi_{00}\right\rangle=\frac{1}{\sqrt{3}}(|0\rangle+|1\rangle+|2\rangle), & \left|\phi_{01}\right\rangle=\frac{1}{\sqrt{3}} i(|0\rangle-|1\rangle-|2\rangle), \\
\left|\phi_{11}\right\rangle=\frac{1}{\sqrt{3}}(|0\rangle+|1\rangle-|2\rangle), & \left|\phi_{10}\right\rangle=\frac{1}{\sqrt{3}} i(|0\rangle-|1\rangle+|2\rangle) . \tag{3.58}
\end{array}
$$

$\underline{G=+1 / 3, F=-i / 3}$

$$
\begin{array}{ll}
\left|\phi_{00}\right\rangle=\frac{1}{\sqrt{3}}(|0\rangle+|1\rangle+|2\rangle), & \left|\phi_{01}\right\rangle=\frac{1}{\sqrt{3}} i(|0\rangle-|1\rangle+|2\rangle), \\
\left|\phi_{11}\right\rangle=\frac{1}{\sqrt{3}}(|0\rangle+|1\rangle-|2\rangle), & \left|\phi_{10}\right\rangle=\frac{1}{\sqrt{3}} i(|0\rangle-|1\rangle-|2\rangle) . \tag{3.59}
\end{array}
$$

With closer inspection of the states in these sets, we realise that they actually all come down to the same four density matrices which are only assigned to different bit value encodings for the different cases of the overlaps. That is, for instance, $\left|\phi_{01}\right\rangle\left\langle\phi_{01}\right|$ for $G=-1 / 3$ and $F=1 / 3$ is equal to $\left|\phi_{10}\right\rangle\left\langle\phi_{10}\right|$ for $G=-1 / 3$ and
$F=-1 / 3$ and similar for other states and overlap combinations. Thus, these sets of states are fundamentally the same, only differing in the global phases of some of the states in the sets. Starting from the set of states in Eq. (3.56) and correctly tweaking the overall phase of some of the states, allows determining other sets of states that satisfy the other optimal overlap combinations of $F$ and $G$.

### 3.4 Experimental Implementation

As mentioned at the beginning of this chapter, the XOT protocol in Section 3.2 has been optically implemented in a proof-of-principle experiment, including not only the realisation of the protocol when both parties are honest, but also of the optimal cheating strategies of dishonest parties [71].

In the experimental setup, a heralded single-photon source was used on the sender Alice's side. Time-correlated photon pairs were generated. One photon was used as the heralding photon and the other one was used as the "message" photon to encode Alice's quantum states using half-wave plates and calcite beam displacers. The encoding is based on the spatial and polarisation degrees of freedom of the "message" photon. That is, there are two output ports with one horizontally and one vertically polarised mode each and the basis states $|0\rangle,|1\rangle$, and $|2\rangle$ are represented by three of the four possible output port/mode-combinations. In order to prevent a dishonest Alice from making use of the fourth output port/mode-combination, a linear polariser needs to be placed in the input port corresponding to the output port with the unused mode. In the proof-of-principle experiment realised in Ref. [71], this was, however, deliberately left out to simplify the setup.

On the receiver Bob's side, a generalised quantum measurement needed to be implemented. This was accomplished by extending the Hilbert space with auxiliary basis states that were represented by additional modes added on Bob's side using half-wave plates, beam displacers, and polarising beam-splitters. The single-photon detection was carried out as coincidence measurement where the heralding photon was used as trigger signal and the coincidence window was set as 2.5 ns .

A detailed scheme of the experimental setup is shown in Figure 3.3, taken from Ref. [71]. The cut between the sender's and the receiver's side passes between the half-wave plates 1 and 2, which are still on the sender's side, and the half-wave plate 3, which is the first element on the receiver's side. The angles of the wave-plates need to be set to certain values to realise the protocol with honest parties. When one of the parties cheats, then the associated cheating strategy is implemented by modifying the angles of the wave-plates of this dishonest party as necessary.


Figure 3.3: Schematic of the experimental setup for the XOT protocol (taken from Ref. [71]). The half-wave plates are depicted by the narrow green rectangles labeled with the black numbers, the larger semi-transparent cyan rectangles are the beam displacers, and the square on the right-hand side is a polarising beam-splitter. The small orange rectangles represent glass plates used for phase compensation, the gray half-circles are the detectors, and the insets display the arrangement of the respective half-wave plates.

On the theoretical side, we assumed that the protocol works faultless and is complete, i.e., when both parties are honest, Bob always gets the correct output. In the experimental realisation, however, there were naturally some sources of experimental error that had to be dealt with. For instance, one of these sources is connected to the detectors. On rare occasion, at most once in 2000 measurements, more than one detector clicked with the trigger signal. In these cases, one of the measurement results was chosen at random and only that one was counted. Other sources of experimental error were the unequal fiber-coupling efficiencies and the unequal efficiencies of the single-photon detectors used. In compensation for both these inequalities, detection electronics were utilised. Another example for a source of experimental error was that the optical losses in different optical paths differed slightly. There was nothing done to directly compensate for this irregularity, though.

All in all, this optical implementation demonstrates the feasibility of the XOT protocol. The optimal cheating strategies of dishonest parties were also shown to be experimentally realisable and the cheating probabilities obtained by the experimental measurements agreed very well with the predicted theoretical values in all cases.

### 3.5 Conclusion

In Section 3.3, we looked at quantum XOR oblivious transfer protocols with symmetric states in general. To analyse how well a dishonest Alice or a dishonest Bob can do in these protocols, we looked at their optimal cheating strategies and derived
equations for their cheating probabilities, depending on the overlaps of the states Alice is supposed to send when following the protocol honestly. This analysis led to finding four combinations of values for the overlaps which are optimal in the sense that they achieve the lowest possible cheating probability for Bob, which is $3 / 4$, and, when given that Bob's cheating probability is $3 / 4$, also the lowest possible cheating probability for Alice, which is then $1 / 2$. A further advantage of the protocols using these particular overlaps for honest Alice's states, is that Alice's cheating probability is the same no matter if Bob tests or not, making any added testing pointless. The protocols with these overlaps can hence be said to be optimal among non-interactive XOT protocols using symmetric pure states.

One of these protocols is the protocol that was investigated in Section 3.2 and the results for Alice's and Bob's cheating probabilities confirm the results in the subsequent section. Comparing this protocol to a classical XOT protocol showed that there is a quantum advantage. We presented the classical post-processing that needs to be added to this non-interactive XOT protocol in order to enable Bob to actively choose which of the three bits he wants to learn. Even though the non-interactivity makes addition of this extra step necessary in order to realise a standard XOT protocol, the advantage of the non-interactivity is that no entanglement is needed. Entanglement is a resource frequently used in quantum protocols, such as in an interactive XOT protocol presented by Kundu et al. [48]. As a matter of fact, the protocol by Kundu et al. and the one presented in Section 3.2 are related; in Ref. [71], it is shown how one can be derived from the other. Entanglement, however, complicates experimental implementation. Not making use of entanglement in the non-interactive protocol hence simplifies its implementation and it was indeed demonstrated in Ref. [71] that this non-interactive protocol is experimentally feasible.

## Chapter 4

## Reversed Quantum Oblivious Transfer

### 4.1 Introduction

Reversing a protocol describes the concept of implementing a protocol between two parties in both directions without changing their physical role, i.e. their actions. Imagine a protocol where party A encodes some information and sends the encoding to party B; A is both the functional sender (sending the information) and physical sender (physically sending the encoding). Party B receives the encoding and can decode it to retrieve the information; B is both the functional receiver (receiving the information) and the physical receiver (physically receiving the encoding). When reversing such a protocol, party A sends party B some encoding which will tell A some information; $A$ is the functional receiver (receiving the information) while remaining the physical sender (physically sending the encoding). Party B receives the encoding that encoded some of B's information which was shared with A; B is the functional sender (sending the information) while remaining the physical receiver (physically receiving the encoding).

We further illustrate this concept by describing the reversal process specifically with regard to non-interactive quantum oblivious transfer protocols. For this, we differentiate more explicitly between the functional and physical roles. Following convention, the functional sender (sending $x_{0} x_{1}$ ) will be referred to as Alice and the functional receiver (receiving $x_{b}$ ) as Bob. The physical sender (sending the quantum state) will be referred to as Sender and the physical receiver (making a measurement on the received state) as Receiver.

In Figure 4.1, oblivious transfer is implemented as usual in the upper part of the graphic, while it is reversed in the lower part of the graphic. Thereby, the physical Sender is always on the left and the physical Receiver is always on the right. The concept of OT is to send some of the information of a bit string $x_{0} x_{1}$ to someone


Figure 4.1: Oblivious transfer between Alice and Bob in the unreversed (top) and reversed (bottom) versions.
who will only receive the partial information $x_{b}$; the party with all of the information $x_{0} x_{1}$ is the functional sender in OT and the party with the partial information $x_{b}$ is the functional receiver in OT. We note that Alice is always the one with $x_{0} x_{1}$, i.e. the functional sender, and Bob is always the one obtaining $x_{b}$, i.e. the functional receiver. While the Receiver of the quantum state in the unreversed version is Bob who obtains $x_{b}$, the Receiver of the quantum state in the reversed version is Alice who gets $x_{0} x_{1}$. Alice as the Sender of the quantum state in the unreversed version sends a quantum state encoding $x_{0} x_{1}$, but Bob as the Sender of the quantum state in the reversed version sends a quantum state encoding $x_{b}$. Thus, the physical roles of Alice and Bob swap when reversing oblivious transfer, while their functional roles remain unchanged.

The reversal process is particularly helpful when the two communicating parties do not have the same computational or technological power. For instance, only one of the two might have the ability to prepare and send quantum states and/or the other one might be the only one who can detect quantum states. In this situation, by reversing the protocol, it would still be possible to implement the protocol in both directions. The concept of reversing the protocol in the case of classical oblivious transfer was studied in Ref. [79].

In the next sections, we present two reversed protocols, one of them a 1-out-of-2 oblivious transfer protocol described in Ref. [7] and the other one the XOR oblivious transfer protocol described in Section 3.2 of the previous chapter. Thereby, we observe that the reversal process has a common effect on the cheating probabilities of the functional and physical roles.

The above differentiation between the functional and physical roles will be used in the remainder of this chapter, especially when examining the cheating probabilities. The functional sender referred to as Alice has cheating probability $A_{\mathrm{OT}}$ and the
functional receiver referred to as Bob has cheating probability $B_{\text {OT }}$. For the physical roles, we denote the Sender's cheating probability as $P_{\mathrm{OT}}$ (Sender) and the Receiver's cheating probability as $P_{\mathrm{OT}}$ (Receiver).

Parts of this chapter were presented and published in Ref. [71]. In particular, the work about the reversal of the XOT protocol was presented, but also the reversal of the 1-out-of-2 OT protocol in Ref. [7] was briefly described and its cheating probabilities were stated. The two reversed protocols were further also outlined in Ref. [72]. Here, we add details about how the results were derived and computed.

### 4.2 Reversing a 1-out-of-2 OT Protocol

The protocol considered and reversed here, was presented by Amiri et al. [7]. It is a semi-random 1-2 OT protocol using a quantum state elimination measurement and can be changed into a standard 1-2 OT protocol, where Bob can actively choose if he wants to learn $x_{0}$ or $x_{1}$, by adding classical post-processing as described in Ref. [46]. This protocol is defined as follows.

1. The Sender Alice uniformly at random chooses the bits $\left(x_{0}, x_{1}\right) \in\{0,1\}$ and encodes them according to the mapping $00 \rightarrow|00\rangle, 01 \rightarrow|++\rangle, 11 \rightarrow|11\rangle$, and $10 \rightarrow|--\rangle$, where $| \pm\rangle=(|0\rangle \pm|1\rangle) / \sqrt{2}$. She sends the applicable quantum state to Bob.
2. The Receiver Bob measures the first qubit in the $Z$ basis and the second qubit in the $X$ basis. He can then with certainty rule out two of the possible states and can thus deduce either $x_{0}$ or $x_{1}$.

In order to restrict Alice's cheating probability, a testing scheme is added to this protocol [7]. Otherwise, a dishonest Alice would be able to cheat perfectly. The testing scheme is the same as in Chapter 3, where the protocol needs to be implemented multiple rounds, some testing and some regular XOT rounds, and where, in the testing rounds, the receiver Bob checks if the quantum states Alice sends agree with their declared identity. This results in Alice's cheating probability being an average cheating probability and, in particular, dishonest Alice can cheat on average with probability $A_{1-2}^{\text {unreversed }}=P_{1-2}^{\text {unreversed }}($ Sender $)=0.75$. A dishonest Bob can cheat with probability $B_{1-2}^{\text {unreversed }}=P_{1-2}^{\text {unreversed }}($ Receiver $) \approx 0.729$ with a minimum-error measurement on each individual bit, where in this case the square-root measurement is optimal since honest Alice's state are equiprobable and symmetric.

When reversing the protocol, Bob becomes the Sender of the quantum state and Alice the Receiver of the quantum state who measures, while still implementing 1-out-of-2 OT from Alice to Bob. The protocol then proceeds as follows.

1. Bob uniformly at random chooses the bit $b \in\{0,1\}$ and a random bit $y \in$ $\{0,1\}$, thereby determining $x_{b}=y$. He encodes this information according to the mapping $x_{0}=0 \rightarrow|00\rangle, x_{0}=1 \rightarrow|11\rangle, x_{1}=0 \rightarrow|++\rangle$, and $x_{1}=1 \rightarrow|--\rangle$, where $| \pm\rangle=(|0\rangle \pm|1\rangle) / \sqrt{2}$, and sends the applicable quantum state to Alice.
2. Alice measures one qubit in the $Z$ basis and the other one in the $X$ basis, whereby the order of the two measurements is randomised; that is, Alice will measure $Z \otimes X$ with a probability of $1 / 2$ and, otherwise, she will measure $X \otimes Z$. The outcomes of her measurements determine the values of her classical bits, her $Z$ measurement result determining $x_{0}$ and her $X$ measurement result determining $x_{1}$, and her results are derived according to the mapping $|0+\rangle \rightarrow$ $00,|0-\rangle \rightarrow 01,|1-\rangle \rightarrow 11$, and $|1+\rangle \rightarrow 10$.

In Step 1 of the reversed protocol, when picking the value for $b$, an honest Bob randomly chooses if he wants to know the result of Alice's $Z$ measurement ( $b=0$ ) or of her $X$ measurement $(b=1)$. He will be able to predict the outcome for the chosen measurement with certainty, but will have no information about the other outcome. The randomisation of the order of Alice's measurements in Step 2 is important to restrict a dishonest Bob's cheating. If Alice were to use a fixed order of her measurements, Bob could cheat perfectly by sending a state that "fits" the measurement; for instance, if he knows Alice will measure $Z \otimes X$, he can send $|0+\rangle$ and will then perfectly know both of Alice's bit values. Later, by selecting her $Z$ measurement to refer to $x_{0}$ and her $X$ measurement to $x_{1}$, Alice ensures that the values of her bits $x_{0} x_{1}$ match with the measurement outcomes Bob expects, that is, the correct measurement is done for $x_{b}$.

This is different to the unreversed version of the protocol where, without testing, Alice as the Sender of the quantum state can cheat perfectly no matter if Bob as the Receiver of the quantum state randomises the order of his measurements or not [7]. That is, randomisation does not restrict a dishonest Alice's cheating in the unreversed protocol and testing by the Receiver of the quantum state (Bob) is needed to limit her available cheating strategies.

Since the functional roles remain unchanged in the reversed version of the protocol, also the aims of the dishonest parties remain unchanged; that is, a dishonest

Alice still wants to learn Bob's $b$ and a dishonest Bob still wants to learn all of Alice's bits and not only $x_{b}$. In the following subsections, we examine how well Alice and Bob can cheat in the reversed 1-2 OT protocol described.

### 4.2.1 Dishonest Receiver

If Alice is dishonest, she wants to learn Bob's $b$. To do so she will have to distinguish between the sets of states $\{|00\rangle,|11\rangle\}$ and $\{|++\rangle,|--\rangle\}$ since the first bit $x_{0}$, thus $b=0$, is associated with the $Z$ measurement and the second bit $x_{1}$, thus $b=1$, is associated with the $X$ measurement. Bob sends each of the four possible states with equal probability, so Alice needs to distinguish between the two equiprobable states $\rho_{0}=\frac{1}{2}(|00\rangle\langle 00|+|11\rangle\langle 11|)$ and $\rho_{1}=\frac{1}{2}(|++\rangle\langle++|+|--\rangle\langle--|)$. The optimal measurement to do so is a minimum-error measurement, in particular the Helstrom measurement [80], and the success probability of this measurement yields Alice's cheating probability

$$
\begin{equation*}
A_{1-2 \mathrm{OT}}^{\text {reversed }}=P_{1-2 \mathrm{OT}}^{\text {reversed }}(\text { Receiver })=1-\frac{1}{2}\left[1-\frac{1}{2} \operatorname{Tr}\left(\left|\rho_{1}-\rho_{0}\right|\right)\right]=\frac{3}{4}, \tag{4.1}
\end{equation*}
$$

where $|\sigma|=\sqrt{\sigma^{\dagger} \sigma}$.
Looking at the functional role, Alice's cheating probability is the same in the reversed and in the unreversed protocol versions, that is, $A_{1-2}^{\text {reversed }}=A_{1-2}^{\text {unreversed }}=3 / 4$. The security against the physical Receiver, i.e. the party who physically obtains the quantum state and applies a measurement on it, however, is slightly worse in the reversed protocol than in the unreversed one, where the Receiver of the quantum state (Bob) can cheat with probability $B_{1-2 ~ O T}^{\text {unreved }}=P_{1-2 \text { OT }}^{\text {unreversed }}($ Receiver $) \approx 0.729$ [7]. That is, because, in the unreversed 1-2 OT protocol, the Receiver of the quantum state wants to distinguish between all four states $\{|00\rangle,|++\rangle,|11\rangle,|--\rangle\}$ to learn both $x_{0}$ and $x_{1}$ and not only between the two sets $\{|00\rangle,|11\rangle\}$ and $\{|++\rangle,|--\rangle\}$. The former is a little harder to do and Bob succeeds with a slightly smaller cheating probability.

### 4.2.2 Dishonest Sender

If Bob is dishonest, he wants to learn all of Alice's bits. As the physical Sender, he can cheat by sending a quantum state different to one of the four he is supposed to send. We look at two situations, one with a testing Receiver and one without any testing by the Receiver. When Alice (here the Receiver of the quantum state) applies no testing, Bob can cheat by sending whatever state suits him best, but,
when Alice applies some testing, Bob needs to implement a cheating strategy with which he can pass Alice's test since he does not want his cheating to be detected.

## No testing by the Receiver

If the Receiver Alice applies no testing, Sender Bob's choice of quantum state has no restrictions entailed from the need to pass some testing scheme and he can choose to send the state that will maximise his cheating probability. Bob knows that Alice will measure $Z \oplus X$ half of the time and $X \oplus Z$ the other half of the time and thus he knows her measurement operators that can be expressed as

$$
\begin{array}{ll}
\Pi_{00}^{A}=\frac{1}{2}|0+\rangle\langle 0+|+\frac{1}{2}|+0\rangle\langle+0|, & \Pi_{01}^{A}=\frac{1}{2}|0-\rangle\langle 0-|+\frac{1}{2}|-0\rangle\langle-0|, \\
\Pi_{11}^{A}=\frac{1}{2}|1-\rangle\langle 1-|+\frac{1}{2}|-1\rangle\langle-1|, & \Pi_{10}^{A}=\frac{1}{2}|1+\rangle\langle 1+|+\frac{1}{2}|+1\rangle\langle+1| . \tag{4.2}
\end{array}
$$

For some state $\sigma$, Alice will obtain outcome $x_{0} x_{1}$ with probability $\operatorname{Tr}\left(\Pi_{x_{0} x_{1}}^{A} \sigma\right)$ and, given that he sent $\sigma$, Bob can cheat with a probability at most equal to the probability of Alice's most likely result. This probability is maximised by sending the eigenstate corresponding to the largest eigenvalue of Alice's measurement operator $\Pi_{x_{0} x_{1}}^{A}$, whereby the eigenvalue will then yield Bob's cheating probability.

The four operators $\Pi_{00}^{A}, \Pi_{01}^{A}, \Pi_{11}^{A}$, and $\Pi_{10}^{A}$ all have eigenvalues ( $3 / 4,1 / 4,0,0$ ) and therefore $B_{1-2}^{\text {reversed }}=P_{1-2}^{\text {reversed }}($ Sender $)=3 / 4$. Bob can achieve this probability for the outcomes $00,01,11$, and 10 by sending one of the following states

$$
\begin{array}{ll}
\left|\Phi_{00}\right\rangle=\sqrt{\frac{2}{3}}|00\rangle+\sqrt{\frac{1}{6}}(|01\rangle+|10\rangle), & \left|\Phi_{01}\right\rangle=\sqrt{\frac{2}{3}}|00\rangle-\sqrt{\frac{1}{6}}(|01\rangle+|10\rangle), \\
\left|\Phi_{11}\right\rangle=\sqrt{\frac{2}{3}}|11\rangle-\sqrt{\frac{1}{6}}(|01\rangle+|10\rangle), \quad\left|\Phi_{10}\right\rangle=\sqrt{\frac{2}{3}}|11\rangle+\sqrt{\frac{1}{6}}(|01\rangle+|10\rangle), \tag{4.3}
\end{array}
$$

which are the eigenstates of the largest eigenvalue of $\Pi_{00}^{A}, \Pi_{01}^{A}, \Pi_{11}^{A}$, and $\Pi_{10}^{A}$, respectively.

Thus, the cheating probability of the physical Sender is the same as in the unreversed 1-2 OT protocol, $A_{1-2}^{\text {unreversed }}=P_{1-2}^{\text {unreversed }}$ (Sender) $=3 / 4[7]$. While the unreversed protocol needs testing to achieve this cheating probability, the reversed protocol does not need any testing. This means that $3 / 4$ is the cheating probability of the Sender of the quantum state for every single round in the reversed protocol, while it is only the average cheating probability in the unreversed protocol.

## Testing by the Receiver

If the Receiver Alice applies some testing, Sender Bob's cheating strategies are restricted to the ones which will guarantee that he passes the test. Hence, we examine if this can lower the physical Sender's cheating probability in the reversed protocol. Receiver Alice's applied testing method is the same as the one that was considered previously and that was also used for the unreversed version of the protocol [7]. That is, Bob sends $N$ states to Alice who chooses a small fraction $F$ of them to test, where $0<F \ll 1$. For these selected states, Bob needs to declare their identity and Alice then makes a measurement in a basis where one basis state is the one Bob declared. If Alice's results all agree with Bob's declarations, she discards the states used for testing and continues with the OT protocol for the remaining $N(1-F)$ states. Otherwise, if there are any mismatches, Alice aborts the protocol.

In order to always pass Alice's test, Bob will have to send a superposition of the states he is supposed to send entangled with a system that he keeps on his side. This will enable him to always declare a state that will match Alice's testing measurement, when asked to do so. A state of such a form is

$$
\begin{equation*}
\left|\Psi_{\text {cheat }}\right\rangle=a|0\rangle_{B} \otimes|00\rangle+b|1\rangle_{B} \otimes|++\rangle+c|2\rangle_{B} \otimes|11\rangle+|3\rangle_{B} \otimes|--\rangle, \tag{4.4}
\end{equation*}
$$

where $\left\{|0\rangle_{B},|1\rangle_{B},|2\rangle_{B},|3\rangle_{B}\right\}$ is an orthonormal basis for the system Bob keeps and $|a|^{2}+|b|^{2}+|c|^{2}+|d|^{2}=1$. If it is not a testing round, Alice will make the measurement described by her measurement operators in Eq. (4.2) and this will prepare Bob's system on his side in one of four states, depending on if Alice has obtained outcome $00,01,11$, or 10 . When Alice's outcome is 00 , for instance, the unnormalised state conditionally prepared on Bob's side will be

$$
\begin{equation*}
\frac{1}{2}\left(\left\langle 0+\mid \Psi_{\text {cheat }}\right\rangle+\left\langle+0 \mid \Psi_{\text {cheat }}\right\rangle\right)=\frac{1}{\sqrt{2}}\left(a|0\rangle_{B}+b|1\rangle_{B}\right) \tag{4.5}
\end{equation*}
$$

and similarly for the other three states. Thus, Bob will have to distinguish between the pure states

$$
\begin{align*}
& \left|\theta_{00}\right\rangle=\frac{1}{\sqrt{|a|^{2}+|b|^{2}}}\left(a|0\rangle_{B}+b|1\rangle_{B}\right), \quad\left|\theta_{01}\right\rangle=\frac{1}{\sqrt{|a|^{2}+|d|^{2}}}\left(a|0\rangle_{B}+d|3\rangle_{B}\right), \\
& \left|\theta_{11}\right\rangle=\frac{1}{\sqrt{|c|^{2}+|d|^{2}}}\left(c|2\rangle_{B}+d|3\rangle_{B}\right), \quad\left|\theta_{10}\right\rangle=\frac{1}{\sqrt{|b|^{2}+|c|^{2}}}\left(b|1\rangle_{B}+c|2\rangle_{B}\right), \tag{4.6}
\end{align*}
$$

corresponding to Alice obtaining $00,01,11$, or 10 . These states occur with probabilities $\left(|a|^{2}+|b|^{2}\right) / 2,\left(|a|^{2}+|d|^{2}\right) / 2,\left(|c|^{2}+|d|^{2}\right) / 2$, and $\left(|b|^{2}+|c|^{2}\right) / 2$, respectively.

To distinguish between multiple states, it generally intuitively holds that the less equiprobable the states are, the better, since one can be more certain to guess correctly when one of the states occurs more often than the others. However, by choosing the constants $a, b, c$, and $d$ in a way such that the prior probabilities of the states in Eq. (4.6) are less equal, some of their pairwise overlaps become rather large, that is, the states will be closer together. This results in increasing difficulty to distinguish between them. Hence, it appears to be best for a dishonest Bob to choose the constants in such a way that the prior probabilities of the states are all the same, that is, having them equiprobable with a probability of $1 / 4$ each. While this condition holds true for values such as $a=c=1 / \sqrt{2}, b=d=0$ and similar, such a choice will result in always two of the states being equal to each other; for example $\left|\theta_{00}\right\rangle=\left|\theta_{01}\right\rangle$ and $\left|\theta_{11}\right\rangle=\left|\theta_{10}\right\rangle$ with the above mentioned choice. Hence, an additional condition is to pick $a, b, c$, and $d$ so, that the four states in Eq. (4.6) are distinct to some extent, i.e. no pairwise overlaps of 1 .

A choice that Bob can make to fulfil these conditions is to pick $a=b=c=d=$ $1 / 2$. The equiprobable states he needs to distinguish between are then given by

$$
\begin{array}{ll}
\left|\theta_{00}\right\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle_{B}+|1\rangle_{B}\right), & \left|\theta_{01}\right\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle_{B}+|3\rangle_{B}\right), \\
\left|\theta_{11}\right\rangle=\frac{1}{\sqrt{2}}\left(|2\rangle_{B}+|3\rangle_{B}\right), & \left|\theta_{10}\right\rangle=\frac{1}{\sqrt{2}}\left(|1\rangle_{B}+|2\rangle_{B}\right) . \tag{4.7}
\end{array}
$$

These states are symmetric. That is, for the unitary

$$
U=\left(\begin{array}{llll}
0 & 1 & 0 & 0  \tag{4.8}\\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0
\end{array}\right)
$$

for which it holds that $U^{4}=\mathbb{1}$, we have $\left|\theta_{01}\right\rangle=U\left|\theta_{00}\right\rangle,\left|\theta_{11}\right\rangle=U^{2}\left|\theta_{00}\right\rangle$, and $\left|\theta_{10}\right\rangle=U^{3}\left|\theta_{00}\right\rangle$.

To distinguish between multiple states with the lowest probability to be wrong, the optimal measurement is a minimum-error measurement. Since the states in Eq. (4.7) are equiprobable, pure, and symmetric, the square-root measurement is Bob's optimal minimum-error measurement. The measurement operators of the squareroot measurement can be calculated by $\Pi_{i}=p_{i} \rho_{\text {total }}^{-1 / 2} \rho_{i} \rho_{\text {total }}^{-1 / 2} \forall i$, whereby $p_{i}$ is the prior probability of a certain state $\rho_{i}$ and $\rho_{\text {total }}=\sum_{i} p_{i} \rho_{i}[66]$.

The measurement operators here are

$$
\begin{array}{ll}
\Pi_{00}=\frac{1}{16}\left(\begin{array}{cccc}
\alpha & \alpha & -1 & -1 \\
\alpha & \alpha & -1 & -1 \\
-1 & -1 & \beta & \beta \\
-1 & -1 & \beta & \beta
\end{array}\right), & \Pi_{01}=\frac{1}{16}\left(\begin{array}{cccc}
\alpha & -1 & -1 & \alpha \\
-1 & \beta & \beta & -1 \\
-1 & \beta & \beta & -1 \\
\alpha & -1 & -1 & \alpha
\end{array}\right), \\
\Pi_{11}=\frac{1}{16}\left(\begin{array}{cccc}
\beta & \beta & -1 & -1 \\
\beta & \beta & -1 & -1 \\
-1 & -1 & \alpha & \alpha \\
-1 & -1 & \alpha & \alpha
\end{array}\right), & \Pi_{10}=\frac{1}{16}\left(\begin{array}{cccc}
\beta & -1 & -1 & \beta \\
-1 & \alpha & \alpha & -1 \\
-1 & \alpha & \alpha & -1 \\
\beta & -1 & -1 & \beta
\end{array}\right), \tag{4.9}
\end{array}
$$

where $\alpha=3+2 \sqrt{2}$ and $\beta=3-2 \sqrt{2}$ and $\Pi_{i j}$ is the respective measurement operator for $\left|\theta_{i j}\right\rangle, \forall i, j \in\{0,1\}$. The Sender Bob's cheating probability for a testing Alice is then

$$
\begin{equation*}
B_{1-2}^{\text {reversed }}=P_{1-2 \text { OT }}^{\text {reversed }}(\text { Sender })=\sum_{i=0}^{4} p_{i} \operatorname{Tr}\left(\Pi_{i} \rho_{i}\right)=4 \times \frac{1}{32}(3+2 \sqrt{2}) \approx 0.729 \tag{4.10}
\end{equation*}
$$

This is a lower probability than in the case of a dishonest Bob with no testing by Alice and we can conclude that testing can indeed lower the physical Sender's cheating probability in the reversed protocol. Just as in the unreversed protocol with testing, this is an average cheating probability for the Sender of the quantum state.

With respect to the functional role, the added testing means that the cheating probability of Bob in the reversed protocol stays the same as in the unreversed protocol, that is, $B_{1-2}^{\text {reversed }}=B_{1-2 \mathrm{OT}}^{\text {unreved }} \approx 0.729$. The security against the physical Sender, i.e. the party who physically sends the quantum state, with testing by the physical Receiver is slightly better in the reversed protocol than in the unreversed one. In the unreversed protocol, the testing scheme lowers the cheating probability of the Sender of the quantum state to $A_{1-2}^{\text {unreversed }}=P_{1-2}^{\text {unreversed }}($ Sender $)=3 / 4[7]$. This makes intuitive sense. After the physical Receiver has made a measurement on $\left|\Psi_{\text {cheat }}\right\rangle$ (Eq. (4.4)), the number of states that are prepared on the physical Sender's side and that the Sender of the quantum state needs to distinguish between, is smaller in the unreversed case than in the reversed one. For the unreversed protocol, the physical Sender, who in this case wants to learn $b \in\{0,1\}$, needs to only distinguish between two states, while, in the reversed case, the physical Sender, who wants to learn $\left(x_{0}, x_{1}\right) \in\{0,1\}$, needs to distinguish between four states.

### 4.3 Reversing an XOT Protocol

Here, the XOR oblivious transfer protocol that was presented in Chapter 3, is reversed. The unreversed version of this protocol is defined in Section 3.2 and its cheating probabilities are $A_{\mathrm{XOT}}^{\text {unreversed }}=P_{\mathrm{XOT}}^{\text {unreversed }}($ Sender $)=1 / 2$ for Sender Alice and $B_{\mathrm{XOT}}^{\text {unreversed }}=P_{\mathrm{XOT}}^{\text {unreversed }}($ Receiver $)=3 / 4$ for Receiver Bob. For this protocol, the testing scheme was not needed as a dishonest Sender Alice can cheat as well when there is no testing by the Receiver Bob, as when there is testing.

When reversing the XOT protocol, Bob becomes the Sender of the quantum state and Alice the Receiver who applies a measurement on the received state, while still implementing XOT from Alice to Bob. The reversed XOT protocol is then carried out as follows.

1. Bob uniformly at random chooses $b \in\{0,1,2\}$ and a random bit $y \in\{0,1\}$, thereby determining $x_{b}=y$. He sends to Alice the appropriate one of the six quantum states

$$
\begin{array}{ll}
\left|\phi_{x_{0}=0}\right\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|2\rangle), \quad\left|\phi_{x_{1}=0}\right\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle), \quad\left|\phi_{x_{2}=0}\right\rangle=\frac{1}{\sqrt{2}}(|1\rangle+|2\rangle), \\
\left|\phi_{x_{0}=1}\right\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|2\rangle), \quad\left|\phi_{x_{1}=1}\right\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle), \quad\left|\phi_{x_{2}=1}\right\rangle=\frac{1}{\sqrt{2}}(|1\rangle-|2\rangle) . \tag{4.11}
\end{array}
$$

2. Alice performs a measurement on the state she has received from Bob, learning the bit values $\left(x_{0}, x_{1}\right)$. Her measurement operators $\prod_{x_{0} x_{1}}^{A}$ are

$$
\begin{align*}
& \Pi_{00}^{A}=\frac{1}{4}(|0\rangle+|1\rangle+|2\rangle)(\langle 0|+\langle 1|+\langle 2|), \\
& \Pi_{01}^{A}=\frac{1}{4}(|0\rangle-|1\rangle+|2\rangle)(\langle 0|-\langle 1|+\langle 2|), \\
& \Pi_{11}^{A}=\frac{1}{4}(|0\rangle-|1\rangle-|2\rangle)(\langle 0|-\langle 1|-\langle 2|), \\
& \Pi_{10}^{A}=\frac{1}{4}(|0\rangle+|1\rangle-|2\rangle)(\langle 0|+\langle 1|-\langle 2|) . \tag{4.12}
\end{align*}
$$

As in the unreversed XOT protocol, when both parties act honestly, Alice will have two bits, but will not know whether Bob knows her first bit, her second bit, or their XOR. Bob will have one of $x_{0}, x_{1}$, or $x_{2}=x_{0} \oplus x_{1}$, but will not know anything else, since he can only deduce one bit of information with certainty based on the state he has sent (if he is honest).

Just as when reversing the 1-2 OT protocol, the aims of the dishonest parties stay the same when reversing the XOT protocol, since the functional roles remain unchanged. Hence, a dishonest Alice wants to learn Bob's $b$ and a dishonest Bob wants to learn all of Alice's bits and not only $x_{b}$. In the following subsections, we examine how well Alice and Bob can cheat in the described reversed XOT protocol.

### 4.3.1 Dishonest Receiver

If Alice is dishonest, she wants to learn Bob's $b$, i.e. did he learn the value of the first bit, the second bit, or their XOR. In this case, this means that she will have to distinguish between the sum of the two states for $x_{0}$, the sum of the two states for $x_{1}$, and the sum of the two states for $x_{2}$. Thus, Alice needs to distinguish between the three states

$$
\begin{align*}
& \rho_{x_{0}}=\frac{1}{2}\left|\phi_{x_{0}=0}\right\rangle\left\langle\phi_{x_{0}=0}\right|+\frac{1}{2}\left|\phi_{x_{0}=1}\right\rangle\left\langle\phi_{x_{0}=1}\right|=\frac{1}{2}|0\rangle\langle 0|+\frac{1}{2}|2\rangle\langle 2|, \\
& \rho_{x_{1}}=\frac{1}{2}\left|\phi_{x_{1}=0}\right\rangle\left\langle\phi_{x_{1}=0}\right|+\frac{1}{2}\left|\phi_{x_{1}=1}\right\rangle\left\langle\phi_{x_{1}=1}\right|=\frac{1}{2}|0\rangle\langle 0|+\frac{1}{2}|1\rangle\langle 1|, \\
& \rho_{x_{2}}=\frac{1}{2}\left|\phi_{x_{2}=0}\right\rangle\left\langle\phi_{x_{2}=0}\right|+\frac{1}{2}\left|\phi_{x_{2}=1}\right\rangle\left\langle\phi_{x_{2}=1}\right|=\frac{1}{2}|1\rangle\langle 1|+\frac{1}{2}|2\rangle\langle 2| . \tag{4.13}
\end{align*}
$$

The honest Sender Bob sends each of the six states in Eq. (4.11) with equal probability of $1 / 6$, so the three mixed states above all have prior probability $1 / 3$. They are all diagonal in the $\{|0\rangle,|1\rangle,|2\rangle\}$ basis, so a measurement in this basis is likely optimal. One choice of measurement operators for a minimum-error measurement by Alice is

$$
\begin{align*}
\Pi_{x_{0}} & =\frac{1}{2}(|0\rangle\langle 0|+|2\rangle\langle 2|) \\
\Pi_{x_{1}} & =\frac{1}{2}(|0\rangle\langle 0|+|1\rangle\langle 1|) \\
\Pi_{x_{2}} & =\frac{1}{2}(|1\rangle\langle 1|+|2\rangle\langle 2|) \tag{4.14}
\end{align*}
$$

This is indeed an optimal measurement since the conditions an optimal minimumerror measurement needs to satisfy [66], hold for these measurement operators; i.e.

$$
\begin{align*}
& \Pi_{j}\left(p_{j} \rho_{j}-p_{k} \rho_{k}\right) \Pi_{k}=0 \quad \forall j, k, \\
& \sum_{j} p_{j} \rho_{j} \Pi_{j}-p_{k} \rho_{k} \geq 0 \quad \forall k \tag{4.15}
\end{align*}
$$

hold true for the measurement operators in Eq. (4.14). So, the Receiver Alice's
cheating probability is

$$
\begin{equation*}
A_{\mathrm{XOT}}^{\mathrm{reversed}}=P_{\mathrm{XOT}}^{\mathrm{reversed}}(\text { Receiver })=\sum_{i=0}^{2} p_{i} \operatorname{Tr}\left(\Pi_{x_{i}} \rho_{x_{i}}\right)=3 \times \frac{1}{3}\left(\frac{1}{2}\right)=\frac{1}{2} . \tag{4.16}
\end{equation*}
$$

When considering the functional role, the cheating probability in the reversed version of the protocol is the same as in the unreversed version, that is, $A_{\text {XOT }}^{\text {reversed }}=$ $A_{\mathrm{XOT}}^{\mathrm{unreversed}}=1 / 2$. The physical Receiver in the unreversed protocol can cheat with a higher probability, $B_{\mathrm{XOT}}^{\text {unreversed }}=P_{\mathrm{XOT}}^{\text {unreversed }}($ Receiver $)=3 / 4$, than in the reversed version though. Intuitively this makes sense as the Receiver of the quantum state in the unreversed version (Bob) wants to know all of the Sender Alice's bits and hence has to distinguish between the four states in Eq. (3.1) in Section 3.2, whereas the Receiver of the quantum state in the reversed version (Alice) only needs to distinguish between the three states in Eq. (4.13).

### 4.3.2 Dishonest Sender

If Bob is dishonest, he wants to learn all of Alice's bits, i.e. the first bit, the second bit, and their XOR. Since knowledge of any two of the bits $x_{0}, x_{1}$, or $x_{2}=x_{0} \oplus x_{1}$ implies knowledge about the third bit, Bob's aim is to learn the values of two of the bits. Without loss of generality, it is possible to pick $x_{0}$ and $x_{1}$, thus Bob wants to learn which of the four two-bit combinations Alice has obtained. As previously in the case of a dishonest physical Sender, we consider two situations: one, where the physical Receiver of the state (here Alice) tests the state, and one, where the physical Receiver of the state does not test.

## No testing by the Receiver

If the Receiver Alice applies no testing, Sender Bob's optimal cheating strategy is similar to previous cases with a cheating Sender of the quantum state with no testing by the Receiver of the quantum state. That is, Bob will maximise his cheating probability by sending the eigenstate corresponding to the largest eigenvalue of Alice's measurement operators.

Alice's measurement operators $\Pi_{x_{0} x_{1}}^{A}$ for $\left(x_{0}, x_{1}\right) \in\{0,1\}$ given in Eq. (4.12) all have eigenvalues $(3 / 4,0,0)$. The corresponding eigenvectors are the pure-state projectors which the measurement operators are proportional to. Hence, Bob needs
to send one of the states

$$
\begin{array}{ll}
\left|\Phi_{00}\right\rangle=\frac{1}{\sqrt{3}}(|0\rangle+|1\rangle+|2\rangle), & \left|\Phi_{01}\right\rangle=\frac{1}{\sqrt{3}}(|0\rangle-|1\rangle+|2\rangle), \\
\left|\Phi_{11}\right\rangle=\frac{1}{\sqrt{3}}(|0\rangle-|1\rangle-|2\rangle), & \left|\Phi_{10}\right\rangle=\frac{1}{\sqrt{3}}(|0\rangle+|1\rangle-|2\rangle) \tag{4.17}
\end{array}
$$

to achieve a cheating probability of $B_{\mathrm{XOT}}^{\text {reversed }}=P_{\mathrm{XOT}}^{\mathrm{reversed}}($ Sender $)=3 / 4$.
Comparing to the unreversed version of the XOT protocol, the cheating probability of the functional role remains unchanged, $B_{\mathrm{XOT}}^{\text {reversed }}=B_{\mathrm{XOT}}^{\text {unreversed }}=3 / 4$. The cheating probability of the physical role, however, changes. In particular, it increases $P_{\mathrm{XOT}}^{\mathrm{reversed}}($ Sender $)=3 / 4>P_{\mathrm{XOT}}^{\text {unreversed }}($ Sender $)=1 / 2$. The increase in the cheating probability of the physical Sender makes intuitive sense since the Sender of the quantum state in the unreversed version, who wants to learn $b \in\{0,1,2\}$, needs to distinguish between three states, while the Sender of the quantum state in the reversed version wants to learn $\left(x_{0}, x_{1}\right) \in\{0,1\}$ and so needs to distinguish between four states.

## Testing by the Receiver

If the Receiver Alice is testing, Sender Bob needs to send a state with which he passes Alice's test. The testing scheme is analogous to the one applied by Bob in the unreversed XOT protocol and in the discussed 1-2 OT protocol. Alice tests a fraction of the states she receives to see if her measurement results match Bob's declarations for this fraction of states. She aborts the protocol if there are any mismatches, and otherwise continues with the XOT protocol for the remaining states.

As before, this will restrict Bob's cheating strategies and his optimal one will be to send a superposition of the states in Eq. (4.11) entangled with a system he keeps on his side. This is a state of the form

$$
\begin{align*}
\left|\Phi_{\text {cheat }}\right\rangle & =a|0\rangle_{B} \otimes\left|\phi_{x_{0}=0}\right\rangle+b|1\rangle_{B} \otimes\left|\phi_{x_{0}=1}\right\rangle+c|2\rangle_{B} \otimes\left|\phi_{x_{1}=0}\right\rangle \\
& +d|3\rangle_{B} \otimes\left|\phi_{x_{1}=1}\right\rangle+e|4\rangle_{B} \otimes\left|\phi_{x_{2}=0}\right\rangle+f|5\rangle_{B} \otimes\left|\phi_{x_{2}=1}\right\rangle, \tag{4.18}
\end{align*}
$$

where $\left\{|0\rangle_{B},|1\rangle_{B},|2\rangle_{B},|3\rangle_{B},|4\rangle_{B},|5\rangle_{B}\right\}$ is an orthonormal basis for the system Bob keeps and $|a|^{2}+|b|^{2}+|c|^{2}+|d|^{2}+|e|^{2}+|f|^{2}=1$. If it is not a testing round, Alice will apply her measurement described by the measurement operators in Eq. (4.12). By this, Bob's system on his side is prepared in one of four states, depending on whether Alice has obtained $00,01,11$, or 10 . The states he needs to distinguish
between are the pure states

$$
\begin{align*}
& \left|\theta_{00}\right\rangle=\frac{1}{\sqrt{|a|^{2}+|c|^{2}+|e|^{2}}}\left(a|0\rangle_{B}+c|2\rangle_{B}+e|4\rangle_{B}\right), \\
& \left|\theta_{01}\right\rangle=\frac{1}{\sqrt{|a|^{2}+|d|^{2}+|f|^{2}}}\left(a|0\rangle_{B}+d|3\rangle_{B}-f|5\rangle_{B}\right), \\
& \left|\theta_{11}\right\rangle=\frac{1}{\sqrt{|b|^{2}+|d|^{2}+|e|^{2}}}\left(b|1\rangle_{B}+d|3\rangle_{B}-e|4\rangle_{B}\right), \\
& \left|\theta_{10}\right\rangle=\frac{1}{\sqrt{|b|^{2}+|c|^{2}+|f|^{2}}}\left(b|1\rangle_{B}+c|2\rangle_{B}+f|5\rangle_{B}\right), \tag{4.19}
\end{align*}
$$

corresponding to Alice obtaining $00,01,11$, or 10 . The states occur with probabilities $\left(|a|^{2}+|c|^{2}+|e|^{2}\right) / 2,\left(|a|^{2}+|d|^{2}+|f|^{2}\right) / 2,\left(|b|^{2}+|d|^{2}+|e|^{2}\right) / 2$, and $\left(|b|^{2}+|c|^{2}+|f|^{2}\right) / 2$ for $\left|\theta_{00}\right\rangle,\left|\theta_{01}\right\rangle,\left|\theta_{11}\right\rangle$, and $\left|\theta_{10}\right\rangle$, respectively.

When considering which choice of values for the constants $a, b, c$, and $d$ is best, the same issue as for a dishonest Sender of the quantum state with testing Receiver of the quantum state in Subsection 4.2.2 arises. That is, even though generally it seems sensible to have unequal prior probabilities for the states we need to distinguish between, making one of the states here occur more often than the others will lead to some of the states in Eq. (4.19) being very close to each other with some of the pairwise overlaps rather large. Hence, we expect that it is best for dishonest Bob to choose the constants such that the states are all equiprobable with a probability of $1 / 4$, for example, $a=b=c=d=e=f=1 / \sqrt{6}$. We prove below that this is indeed an optimal choice for the values of these constants.

Substituting $a=b=c=d=e=f=1 / \sqrt{6}$ into Eq. (4.19), the states' pairwise overlaps match the pairwise overlaps of the states an honest Sender sends in the unreversed version of the XOT protocol (see Section 3.2). Thus, $\left|\theta_{00}\right\rangle,\left|\theta_{01}\right\rangle$, $\left|\theta_{11}\right\rangle$, and $\left|\theta_{10}\right\rangle$ are equivalent to these states and dishonest Bob needs to distinguish between

$$
\begin{array}{ll}
\left|\phi_{00}\right\rangle=\frac{1}{\sqrt{3}}(|0\rangle+|1\rangle+|2\rangle), & \left|\phi_{01}\right\rangle=\frac{1}{\sqrt{3}}(|0\rangle-|1\rangle+|2\rangle), \\
\left|\phi_{11}\right\rangle=\frac{1}{\sqrt{3}}(|0\rangle-|1\rangle-|2\rangle), & \left|\phi_{10}\right\rangle=\frac{1}{\sqrt{3}}(|0\rangle+|1\rangle-|2\rangle), \tag{4.20}
\end{array}
$$

corresponding to Alice obtaining $00,01,11$, or 10 , and where each state occurs with a probability of $1 / 4$.

Bob's best measurement is once again a minimum-error measurement. The square-root measurement is optimal, as the states are equiprobable and symmet-
ric and the measurement operators can be calculated $[73,74]$ to be
$\Pi_{00}=\frac{3}{4}\left|\phi_{00}\right\rangle\left\langle\phi_{00}\right|, \quad \Pi_{01}=\frac{3}{4}\left|\phi_{01}\right\rangle\left\langle\phi_{01}\right|, \quad \Pi_{11}=\frac{3}{4}\left|\phi_{11}\right\rangle\left\langle\phi_{11}\right|, \quad \Pi_{10}=\frac{3}{4}\left|\phi_{10}\right\rangle\left\langle\phi_{10}\right|$.

With this measurement, Sender Bob's cheating probability, when Receiver Alice is testing the states he has sent to her, is

$$
\begin{equation*}
B_{\mathrm{XOT}}^{\text {reversed }}=P_{\mathrm{XOT}}^{\mathrm{reversed}}(\text { Sender })=\frac{1}{4} \sum_{i, j=0}^{1} \operatorname{Tr}\left(\Pi_{i j} \rho_{i j}\right)=\frac{3}{4} . \tag{4.22}
\end{equation*}
$$

We can conclude that the choice for $a, b, c, d, e$, and $f$ is an optimal choice, since Bob can never cheat with a higher probability when Alice tests a fraction of the states Bob sends her, than he can do when Alice does not test any of his states. Since $B_{\mathrm{XOT}}^{\text {reversed }}=P_{\mathrm{XOT}}^{\text {reversed }}($ Sender $)=3 / 4$ also for the case with no tests by the Receiver, there is no better way for Bob to choose the constants $a, b, c, d, e$, and $f$. Though, there might be other choices that do just as well.

Thus, as in the unreversed case, any testing by the Receiver of the quantum state does not help to lower the Sender's cheating probability and can be omitted. $B_{\text {XOT }}^{\text {reversed }}=P_{\text {XOT }}^{\text {reversed }}($ Sender $)=3 / 4$ is therefore valid for every individual round of reversed XOT and is not only an average bound as was the case for the better cheating probability in 1-2 OT. Also valid here are the conclusions and comparisons in the previous Subsection 4.3.2 where no testing was applied by the Receiver of the quantum state, that is, the cheating probability of the physical role changes while the cheating probability of the functional role remains unchanged when reversing.

### 4.3.3 Experimental Implementation

As aforementioned, this reversed XOT protocol was presented in Ref. [71]. Apart from the analysis of the protocol and its cheating probabilities, this includes an experimental implementation of the protocol with honest communicating parties and of the cheating strategies of dishonest parties.

The experimental setup for the realisation of the reversed XOT protocol is the same as the one for the unreversed XOT protocol and was described in more detail in Section 3.4. As Alice is the receiver now and Bob the sender, their roles, however, interchange. That is, Bob has the single-photon source and encodes the state and Alice implements the generalised measurement and carries out the photon detection. Once again, it is the angles of the wave-plates and their set values which are modified
and differ depending on if the reversed protocol is implemented with two honest parties or with a dishonest party.

Generally, the experiment demonstrates the feasibility of the reversed XOT protocol and of the relevant cheating strategies of dishonest parties. Also in this case, the experimental results obtained for the cheating probabilities agreed very well with the predicted theoretical values for the cheating probabilities.

### 4.4 Classical Post-Processing for Reversed Protocols

Since the reversed versions of the oblivious transfer protocols are non-interactive, same as the unreversed versions, the Receiver (here Alice) cannot choose the values of the bits $x_{0}, x_{1}$, and thus also not $x_{2}=x_{0} \oplus x_{1}$ in the case of XOR oblivious transfer. However, similar to the post-processing for the unreversed protocols (see Chapter 3 for the XOT protocol and [7] for the 1-2 OT protocol), post-processing can also be added to the reversed versions in order to enable the Receiver of the quantum state to have an active choice of the values of his/her inputs.

The post-processing is straightforward and involves only classical communication from Alice to Bob. Suppose Alice has obtained the two bits ( $x_{0}, x_{1}$ ) from the reversed protocol, but her desired bits are $\left(X_{0}, X_{1}\right)$. If either $x_{0}$ or $x_{1}$ is not the bit value she wants, she needs to ask Bob to flip the corresponding bit value, if he holds it. This obviously gives Bob no more information about Alice's bit values ( $X_{0}, X_{1}$ ). Alice's steps in the classical post-processing are thereby analogous to Alice's steps in the construction of semi-random 1-2 OT from random 1-2 OT as shown by Amiri et al. [7].

A reversed oblivious transfer protocol including classical post-processing as described above can be defined more formally.

1. Alice has input bits $\left(X_{0}, X_{1}\right)$ (with $X_{2}=X_{0} \oplus X_{1}$ for XOT).
2. Sender Bob uniformly at random chooses $b \in\{0,1\}$ (or $b \in\{0,1,2\}$ for XOT) and a random bit $y \in\{0,1\}$, thereby determining $x_{b}=y$. He encodes this information according to the protocol's mapping and sends the applicable quantum state to Alice.
3. Receiver Alice makes the measurement of the executed oblivious transfer protocol and obtains output $\left(x_{0}, x_{1}\right)$.
4. Alice calculates $t_{c}=x_{c} \oplus X_{c}$ for $c \in\{0,1\}$ (it also holds for $t_{2}=t_{0} \oplus t_{1}=$ $x_{0} \oplus X_{0} \oplus x_{1} \oplus X_{1}=x_{2} \oplus X_{2}$ for XOT) and sends ( $\left.t_{0}, t_{1}\right)$ to Bob.
5. Bob has his chosen value for $b$ and the random value $y$. He calculates his final output $y^{\prime}=y \oplus t_{b}$ (for XOT, if $b=2$, then $y^{\prime}=y \oplus t_{2}=y \oplus t_{0} \oplus t_{1}$ ).

The bits $\left(t_{0}, t_{1}\right)$ and by extension also $t_{2}$, can be seen as bits that let Bob know if he has to flip the bit he holds or not; i.e., if $t_{b}=0$, Bob does not have to flip the bit, but, if $t_{b}=1$, then he has to flip it to match the value of Alice's $X_{b}$.

The examined classical post-processing works both for non-interactive reversed 1-2 OT and non-interactive reversed XOT. We now formally prove that it can be done without affecting the cheating probabilities of dishonest parties. The proof uses arguments similar to those in Refs. [7, 46].

Proposition 4.1. There exists classical post-processing for non-interactive reversed 1-out-of-2 and XOR oblivious transfer protocols which enables the Receiver of the quantum state to actively choose the values of his/her inputs, but does not change the cheating probabilities of dishonest parties.

Proof. Assume that a non-interactive reversed oblivious transfer protocol $P$ is executed, with cheating probabilities $A_{O T}(P)$ for a dishonest Alice and $B_{O T}(P)$ for a dishonest Bob. By implementing $P$, the Receiver Alice gets outputs $\left(x_{0}, x_{1}\right)$. Her chosen bits, however, are $\left(X_{0}, X_{1}\right)$, so she defines $t_{c}=x_{c} \oplus X_{c}$ for $c \in\{0,1\}$ and sends $\left(t_{0}, t_{1}\right)$ to Sender Bob. For XOT, $X_{2}=X_{0} \oplus X_{1}, x_{2}=x_{0} \oplus x_{1}$, and hence it holds that $t_{2}=t_{0} \oplus t_{1}=x_{0} \oplus X_{0} \oplus x_{1} \oplus X_{1}=x_{2} \oplus X_{2}$. By implementing $P$, Bob has his chosen input $b$ and a random bit $y$ used to determine $x_{b}=y$, which specified which quantum state he sends to Alice in $P$. After receiving $\left(t_{0}, t_{1}\right)$ from Alice, Bob calculates his final output $y^{\prime}=y \oplus t_{b}$. For XOT, when Bob's $b=2$, his output is $y^{\prime}=y \oplus t_{2}=y \oplus t_{0} \oplus t_{1}$.

If both, Alice and Bob, are honest, then $y^{\prime}=X_{b}$. This is because, using definitions $x_{b}=y$ and $t_{b}=x_{b} \oplus X_{b}$, then

$$
\begin{equation*}
y^{\prime}=y \oplus t_{b}=x_{b} \oplus x_{b} \oplus X_{b}=X_{b} \tag{4.23}
\end{equation*}
$$

and, in the case of $b=2$ in XOT,

$$
\begin{equation*}
y^{\prime}=y \oplus t_{2}=x_{2} \oplus t_{0} \oplus t_{1}=x_{2} \oplus x_{0} \oplus X_{0} \oplus x_{1} \oplus X_{1}=x_{2} \oplus x_{2} \oplus X_{2}=X_{2} \tag{4.24}
\end{equation*}
$$

The following is true with respect to the classical post-processing and security against Alice and Bob:

- By implementing $P$, an honest Alice will learn $\left(x_{0}, x_{1}\right)$, but nothing about $b$. Since Alice receives no communication from Bob during the classical postprocessing, it provides her with no new information about what bit Bob has obtained.
- If Alice is dishonest, she can correctly learn $b$ with probability $A_{O T}(P)$. Since there is no communication from Bob to Alice during the classical post-processing, it does not increase her cheating probability and it stays equal to $A_{O T}(P)$.
- By implementing $P$, an honest Bob will know $b$ and the bit $x_{b}$. In the classical post-processing, he gets $\left(t_{0}, t_{1}\right)$ and calculates his final bit $X_{b}=x_{b} \oplus t_{b}$. This will not give him more information about $X_{\bar{b}}$ since $X_{\bar{b}}=x_{\bar{b}} \oplus t_{\bar{b}}$ and he does not know $x_{\bar{b}}$. Thus, the classical post-processing does not give an honest Bob any more information about Alice's other bit(s).
- If Bob is dishonest, he can correctly guess Alice's other bit(s) $x_{\bar{b}}$ with probability $B_{\text {ОT }}(P)$. He knows $\left(t_{0}, t_{1}\right)$ and that $X_{b}=x_{b} \oplus t_{b}$. Since he does not know anything about $x_{\bar{b}}$ and it holds that $X_{\bar{b}}=x_{\bar{b}} \oplus t_{\bar{b}}$, he cannot learn anything about $X_{\bar{b}}$. He can only correctly guess $X_{\bar{b}}$ with the same probability as $x_{\bar{b}}$. Hence, the classical post-processing does not increase Bob's cheating probability and it stays equal to $B_{O T}(P)$.


### 4.5 Conclusion

In this chapter, we have presented the concept of reversing a protocol, illustrating it by means of oblivious transfer. We applied the concept to two particular protocols, a 1-2 OT protocol [7] and the XOT protocol described in Chapter 3, and analysed the reversed protocol versions for their cheating probabilities. Thereby, we made the following discovery: when reversing a protocol, the cheating probabilities of the functional roles remain unchanged while the cheating probabilities of the physical roles swap.

When summarising the cheating probabilities for the different roles in the 1-2 OT protocol and XOT protocol in tables, this becomes obvious. The subtables in Table 4.1 show that, in both the protocols (left table for 1-2 OT and right table for XOT), the cheating probabilities of the functional roles, Alice and Bob, stay the same, while the cheating probabilities of the physical roles, Sender and Receiver of the quantum state, swap. This presumably stems from the fact that, when reversing
a protocol, the functional roles stay the same and, therefore, also the aims of the cheating parties.

| 1-2 OT | $A_{1-2 \text { OT }}$ | $B_{1-2 \text { OT }}$ |
| :---: | :---: | :---: |
| $P_{1-2 ~ \text { OT }}($ Sender $)$ | $3 / 4$ | 0.729 |
| $P_{1-2 \text { OT }}($ Receiver $)$ | $3 / 4$ | 0.729 |


| XOT | $A_{\text {XOT }}$ | $B_{\text {XOT }}$ |
| :---: | :---: | :---: |
| $P_{\text {XOT }}($ Sender $)$ | $1 / 2$ | $3 / 4$ |
| $P_{\text {XOT }}($ Receiver $)$ | $1 / 2$ | $3 / 4$ |

Table 4.1: Tables summarising the cheating probabilities for the physical and functional roles. The left table is for the 1-2 OT protocol and the right table for the XOT protocol, whereby within these tables always the diagonal cells are a pair; i.e. the upper left and lower right cells correspond to the cheating probabilities in the unreversed versions and the lower left and upper right cells to the cheating probabilities in the reversed versions.

We also showed a classical post-processing that can be added to the non-interactive reversed protocol versions to enable the physical Receiver (here Alice) to actively choose her values for $x_{0}$ and $x_{1}$. It is valid for both 1-2 OT and XOT and we proved that the classical post-processing can be carried out without affecting the cheating probabilities of dishonest parties.

Further work on the topics in this chapter can include applying the reversal process to other protocols than oblivious transfer and examining which conditions generally have to hold for a protocol to be reversable. Moreover, it might be interesting to examine the exact reason why the cheating probabilities of the functional roles remain unchanged when reversing a protocol, that is, what happens on the "mathematical level" to cause this effect.

## Chapter 5

## Generalising Quantum XOR Oblivious Transfer

### 5.1 Introduction

The XOR oblivious transfer protocols considered so far in the previous chapters followed the concept of 1-out-of-2 oblivious transfer in the sense that Alice has a string of two classical bits. 1-2 OT can be generalised to 1-out-of- $n$ oblivious transfer [12], where Alice has a string consisting of $n$ classical bits and Bob can learn the value of one of the $n$ bits. With this in mind, we generalise XOR oblivious transfer in this chapter. Instead of having Bob learn one of two bits or their XOR, the assumption is that Alice has a classical string of length $n$ and Bob can learn either the value of one of the $n$ bits or the pairwise XOR of any two of the bits.

We at first formally define such a generalised XOR oblivious transfer protocol and then present a protocol outline for 1-out-of- $n$ XOT based on unambiguous quantum state elimination. Determining equations for the cheating probabilities for a dishonest Alice and a dishonest Bob in a protocol following this outline, allows investigation of how these probabilities change with increasing $n$. Lastly, we discuss the similarities of 1-out-of- $n$ XOR oblivious transfer to the concept of quantum retrieval games [81].

### 5.2 1-out-of- $n$ XOR Oblivious Transfer

In 1-out-of- $n$ XOR oblivious transfer (1- $n$ XOT), Alice has a string of $n$ input bits $x_{i} \in\{0,1\}$, where $i \in\{1, \ldots, n\}, n \in \mathbb{N}$, and $n \geq 2$, and Bob chooses to learn either the value of one of the $n$ bits or of one of the $\binom{n}{2}=\frac{1}{2} n(n-1)$ pairwise XORs. Ideally, Alice does not know which information Bob has learnt, and Bob does not learn anything more about the other bits. A dishonest Alice aims to learn what information, that is, which bit $x_{i}$ or pairwise XOR $x_{i} \oplus x_{j}$ for $i, j \in\{1, \ldots, n\}$ and
$i \neq j$, Bob has received. A dishonest Bob, on the other hand, aims to learn all of the $n$ bits, which will then also imply knowledge about all the pairwise XORs.

We can assume that Bob is equally likely to choose to learn any of the $n$ bits or any of the $\binom{n}{2}=\frac{1}{2} n(n-1)$ pairwise XORs and Alice is equally likely to have any of the $2^{n}$ possible bit strings as input. These assumptions are valid and sensible since biased protocols, where some of Bob's choices or Alice's inputs are more likely than others, have an additional weak point for cheating parties who can exploit any occurring bias.

## Guessing Bob

If Bob wants to learn about all $n$ bits in Alice's string, which will then also tell him about all of the XORs, he can always use a guessing strategy to do so, just as in 1-2 XOT. Following the protocol honestly, he will then guess the values of the remaining bits that he did not choose to learn the value of. Note that, when Bob chooses to learn the value of a pairwise XOR, he will still need the same number of guesses to learn the whole bit string. That is, he will have to guess the value of one of the two bits composing the XOR value he knows, which will then also give him the value of the other bit in the XOR, plus additionally he will have to guess the values of the remaining $n-2$ bits. Thus, all in all, Bob will have to guess the values of $n-1$ bits and his guessing probability $B_{O T}^{g}$, where the superscript $g$ indicates it being a guessing probability, is

$$
\begin{equation*}
B_{O T}^{g}=\frac{1}{2^{n-1}} . \tag{5.1}
\end{equation*}
$$

## Guessing Alice

If Alice wants to learn which information Bob has chosen to learn, she can also always do so by using a guessing strategy. That is, she follows the protocol honestly and then guesses the most-likely outcome for Bob afterwards. In 1-n XOT, Bob has $n$ bits and $\binom{n}{2}=\frac{1}{2} n(n-1)$ pairwise XORs to choose from, so in total he has $n+\frac{1}{2} n(n-1)=\frac{1}{2} n(n+1)$ possible outcomes. Since we assume that all of these outcomes are equally likely to occur, we know that Alice's guessing probability $A_{O T}^{g}$ is given by

$$
\begin{equation*}
A_{O T}^{g}=\frac{2}{n(n+1)} \tag{5.2}
\end{equation*}
$$

This type of protocol is formalised by defining 1-out-of-n XOR oblivious transfer as follows.

Definition 5.1 (1-out-of- $n$ XOR oblivious transfer). A 1-out-of- $n$ XOR oblivious transfer protocol is a two-party protocol between a sender Alice and a receiver Bob, where

- Alice's input is a string consisting of $n$ bits $x_{i} \in\{0,1\}$, where $i \in\{1, \ldots, n\}$, $n \in \mathbb{N}$, and $n \geq 2$, and Bob has an input $b \in\left\{1, \ldots, n, n+1, \ldots, n+\frac{1}{2} n(n-1)\right\}$. At the start of the protocol, Alice has no information about $b$ and Bob has no information about any of the $x_{i}$ in Alice's string.
- The protocol ends, when either Bob outputs $y$ or he or Alice Abort.
- If both parties are honest, then they never Abort and $y=x_{b}$, where, if $b \in$ $\left\{n+1, \ldots, n+\frac{1}{2} n(n-1)\right\}$, Bob learns about a pairwise overlap, that is

$$
\begin{array}{llll}
x_{n+1}=x_{1} \oplus x_{2}, & x_{n+2}=x_{1} \oplus x_{3}, & \ldots, & x_{n+n-1}=x_{1} \oplus x_{n} \\
x_{n+n}=x_{2} \oplus x_{3}, & x_{2 n+1}=x_{2} \oplus x_{4}, & \ldots, & x_{n+\frac{1}{2} n(n-1)}=x_{n-1} \oplus x_{n}
\end{array}
$$

Furthermore, Alice has no information about $b$ and Bob has no information about any of the other $x_{\bar{b}}$.

- Alice's cheating probability, where $0 \leq \epsilon_{A} \leq 1-A_{O T}^{g}$, is

$$
\begin{align*}
A_{O T} & :=\sup \{P(\text { Alice correctly guesses } b) \wedge \text { Bob does not Abort }\} \\
& =\frac{2}{n(n+1)}+\epsilon_{A} . \tag{5.3}
\end{align*}
$$

- Bob's cheating probability, where $0 \leq \epsilon_{B} \leq 1-B_{O T}^{g}$, is

$$
\begin{align*}
B_{O T} & :=\sup \left\{P\left(\text { Bob correctly guesses all } n \text { bits } x_{i} \wedge \text { Alice does not Abort }\right\}\right. \\
& =\frac{1}{2^{n-1}}+\epsilon_{B} \tag{5.4}
\end{align*}
$$

When a cheating strategy other than the simple guessing strategy is applied, the cheating probability for a dishonest party usually increases. The probability of successfully cheating that can be achieved on top of the probability of just guessing correctly, is represented by $\epsilon_{A}$ and $\epsilon_{B}$ for a dishonest Alice and a dishonest Bob, respectively. For Alice's and Bob's cheating probabilities, all cheating strategies available to them are considered and the suprema are taken over all of them, in order to get the least upper bound. The relevant cheating strategies in both cases are ultimately the ones yielding the largest $\epsilon_{A}$ for Alice or the largest $\epsilon_{B}$ for Bob.

### 5.3 Non-interactive 1-out-of- $n$ XOT Protocol

In this section, we give an outline for a non-interactive 1-out-of- $n$ quantum XOT protocol based on honest Alice sending pure states and honest Bob performing an unambiguous quantum state elimination measurement. Since the protocol is based on quantum state elimination, Bob does not get the choice of which information $x_{b}$ he wants to learn, but he gets an output at random. Hence, using the terminology in Ref. [7], this is a semi-random 1-out-of- $n$ XOR oblivious transfer protocol. Analogous to the specific Definition 3.1 about semi-random 1-2 XOT, the general case is defined as follows.

Definition 5.2 (Semi-random 1-out-of- $n$ XOR oblivious transfer). A semi-random 1-out-of- $n$ XOR oblivious transfer protocol is a two-party protocol between a sender Alice and a receiver Bob, where

1. Alice chooses her input string consisting of $n$ bits $x_{i} \in\{0,1\}$, for $i \in\{1, \ldots, n\}$, $n \in \mathbb{N}$, and $n \geq 2$, uniformly at random, or she chooses Abort.
2. Bob outputs the value $b \in\left\{1, \ldots, n, n+1, \ldots, n+\frac{1}{2} n(n-1)\right\}$ and a bit $y$, or Abort.
3. If both parties are honest, then they never abort and $y=x_{b}$, where, if $b \in$ $\left\{n+1, \ldots, n+\frac{1}{2} n(n-1)\right\}$, Bob learns about a pairwise overlap, that is

$$
\begin{array}{llll}
x_{n+1}=x_{1} \oplus x_{2}, & x_{n+2}=x_{1} \oplus x_{3}, & \ldots, & x_{n+n-1}=x_{1} \oplus x_{n} \\
x_{n+n}=x_{2} \oplus x_{3}, & x_{2 n+1}=x_{2} \oplus x_{4}, & \ldots, & x_{n+\frac{1}{2} n(n-1)}=x_{n-1} \oplus x_{n}
\end{array}
$$

Furthermore, Alice has no information about $b$ and Bob has no information about any of the other $x_{\bar{b}}$.

By adding classical post-processing, we can realise standard 1-out-of-n XOT, where Bob can make an active (but random from Alice's point of view) choice about which $x_{b}$ he receives. This will not change the cheating probabilities of either party. Generalising Proposition 3.1 and its proof (using similar arguments as in Refs. [7] and [46]), we can show that general semi-random 1-n XOT is equivalent to standard $1-n$ XOT up to classical post-processing and this is valid for any $n \geq 2$.

Proposition 5.1. Having a semi-random 1-out-of-n XOT protocol with cheating probabilities $A_{O T}$ and $B_{O T}$ is equivalent to having a standard 1-out-of- $n$ XOT protocol with the same cheating probabilities.

Proof. We examine both directions, i.e. constructing a semi-random 1-n XOT protocol from a standard 1-n XOT protocol and constructing a standard 1-n XOT protocol from a semi-random 1-n XOT protocol. That is, the situation where the parties possess means to implement standard 1-out-of-n XOT, but both of them instead wish to implement semi-random 1-out-of- $n$ XOT, or vice versa.
Case 1: Let $P$ be a standard 1- $n$ XOT protocol with cheating probabilities $A_{O T}(P)$ and $B_{O T}(P)$. We can construct a semi-random 1-n XOT protocol $Q$ with the same cheating probabilities in the following way:

1. Alice picks $x_{1}, x_{2}, \ldots, x_{n} \in\{0,1\}$ uniformly at random. Bob generates $b \in$ $\left\{1,2, \ldots, n, n+1, \ldots, n+\frac{1}{2} n(n-1)\right\}$ uniformly at random (in a way so that he no longer actively chooses $b$ ).
2. Alice and Bob perform the 1- $n$ XOT protocol $P$ where Alice inputs $x_{1}, x_{2}, \ldots, x_{n}$, and all pairwise XORs $x_{i} \oplus x_{j}$, where $i, j \in\{1,2, \ldots, n\}$ and $i \neq j$, and Bob inputs $b$. Let $y$ be Bob's output.
3. Alice and Bob abort in $Q$ if and only if they abort in $P$. Otherwise, the outputs of protocol $Q$ are $(b, y)$ for Bob.

Evidently, $Q$ implements semi-random 1-n XOT if both parties follow the protocol. Furthermore, because of the way $Q$ is constructed, Alice can cheat in $Q$ if and only if she can cheat in $P$, and the same for a cheating Bob. Cheating probabilities for Alice and Bob are therefore equal in $P$ and $Q, A_{O T}(Q)=A_{O T}(P)$ and $B_{O T}(Q)=B_{O T}(P)$.

Case 2: Let $P$ be a semi-random 1-n XOT protocol with cheating probabilities $A_{O T}(P)$ and $B_{O T}(P)$. We can construct a standard 1-n XOT protocol $Q$ with the same cheating probabilities in the following way:

1. Alice has inputs $X_{1}, X_{2}, \ldots, X_{n}$, with $X_{n+1}=X_{1} \oplus X_{2}, X_{n+2}=X_{1} \oplus X_{3}, \ldots$, $X_{n+\frac{1}{2} n(n-1)}=X_{n-1} \oplus X_{n}$ and Bob has input $B \in\{1,2, \ldots, n, n+1, \ldots, n+$ $\left.\frac{1}{2} n(n-1)\right\}$.
2. Alice and Bob perform the semi-random 1-n XOT protocol $P$ where Alice inputs $x_{1}, x_{2}, \ldots, x_{n}$, with $x_{n+1}=x_{1} \oplus x_{2}, x_{n+2}=x_{1} \oplus x_{3}, \ldots, x_{n+\frac{1}{2} n(n-1)}=$ $x_{n-1} \oplus x_{n}$, whereby she chooses $x_{1}, x_{2}, \ldots, x_{n} \in\{0,1\}$ uniformly at random. Let $(b, y)$ be Bob's outputs.
3. Bob sends $r=\left(b+\left[n-1+\frac{1}{2} n(n-1)\right] \times B\right) \bmod \left[n+\frac{1}{2} n(n-1)\right]$ to Alice. Let $x_{c}^{\prime}=x_{(c+r) \bmod \left[n+\frac{1}{2} n(n-1)\right]}$ for $c \in\left\{1,2, \ldots, n, n+1, \ldots, n+\frac{1}{2} n(n-1)\right\}$.
4. Alice sends $\left(s_{1}, s_{2}, \ldots, s_{n}\right)$ to Bob, whereby $s_{c}=x_{c}^{\prime} \oplus X_{c}$ for $c \in\{1,2, \ldots, n\}$ and the pairwise XORs $s_{n+1}=s_{1} \oplus s_{2}, s_{n+2}=s_{1} \oplus s_{3}, \ldots, s_{n+\frac{1}{2} n(n-1)}=s_{n-1} \oplus s_{n}$. Let $y^{\prime}=y \oplus s_{B}$.
5. Alice and Bob abort in $Q$ if and only if they abort in $P$. Otherwise, the output of protocol $Q$ is $y^{\prime}$ for Bob.

If Alice and Bob are honest, then $y=x_{b}$. Note that $x_{B}^{\prime}=x_{(B+r) \bmod \left[n+\frac{1}{2} n(n-1)\right]}=$ $x_{\left(B+b+\left[n-1+\frac{1}{2} n(n-1)\right] \times B\right) \bmod \left[n+\frac{1}{2} n(n-1)\right]}=x_{b}$. Hence,

$$
\begin{equation*}
y^{\prime}=y \oplus s_{B}=x_{b} \oplus s_{B}=x_{B}^{\prime} \oplus x_{B}^{\prime} \oplus X_{B}=X_{B}, \tag{5.5}
\end{equation*}
$$

i.e. $y^{\prime}$ is indeed equal to $X_{B}$. This also holds for the pairwise XORs, that is, when $B \in\left\{n+1, n+2, \ldots, n+\frac{1}{2} n(n-1)\right\}$, since for

$$
\begin{equation*}
s_{l}=s_{i} \oplus s_{j}=x_{i}^{\prime} \oplus X_{i} \oplus x_{j}^{\prime} \oplus X_{j}=x_{i} \oplus x_{j} \oplus X_{i} \oplus X_{j}=x_{l} \oplus X_{l}=x_{l}^{\prime} \oplus X_{l} \tag{5.6}
\end{equation*}
$$

when $x_{l}=x_{i} \oplus x_{j}$ holds for $l \in\left\{n+1, n+2, \ldots, n+\frac{1}{2} n(n-1)\right\}, i, j \in\{1,2, \ldots, n\}$, and $i \neq j$.
The following is true with respect to the classical post-processing described in steps 3 and 4 and security against Alice and Bob:

- If Alice is honest, she knows $r$ but has no information about $b$. From $r=$ $\left(b+\left[n-1+\frac{1}{2} n(n-1)\right] \times B\right) \bmod \left[n+\frac{1}{2} n(n-1)\right]$ she can deduce that $[n-$ $\left.1+\frac{1}{2} n(n-1)\right] B=(r-b) \bmod \left[n+\frac{1}{2} n(n-1)\right]$ but she cannot obtain any information about $B$ from this. Hence, the classical post-processing does not give an honest Alice any more information about which bit Bob has obtained.
- If Alice is dishonest, she can correctly guess $b$ with probability $A_{O T}(P)$. She knows $r$. Since $\left[n-1+\frac{1}{2} n(n-1)\right] B=(r-b) \bmod \left[n+\frac{1}{2} n(n-1)\right]$, guessing $\left[n-1+\frac{1}{2} n(n-1)\right] B$, equivalently guessing $B$, is equivalent to guessing $b$. Therefore, $A_{\text {ОT }}(Q)=A_{\text {OT }}(P)$.
- If Bob is honest, he knows $r,\left(s_{1}, s_{2}, \ldots, s_{n}\right)$, and the pairwise XORs $s_{n+1}=$ $s_{1} \oplus s_{2}, s_{n+2}=s_{1} \oplus s_{3}, \ldots, s_{n+\frac{1}{2} n(n-1)}=s_{n-1} \oplus s_{n}$. But he has no information about the bits $x_{\bar{b} \bmod \left[n+\frac{1}{2} n(n-1)\right]}$. He cannot learn anything about the other
$\left[n+\frac{1}{2} n(n-1)-1\right]$ of Alice's bits, $X_{\bar{B} \bmod \left[n+\frac{1}{2} n(n-1)\right]}$, since

$$
\begin{align*}
X_{\bar{B} \bmod \left[n+\frac{1}{2} n(n-1)\right]} & =x_{\bar{B} \bmod \left[n+\frac{1}{2} n(n-1)\right]}^{\prime} \oplus s_{\bar{B} \bmod \left[n+\frac{1}{2} n(n-1)\right]} \\
& =x_{(\bar{B}+r) \bmod \left[n+\frac{1}{2} n(n-1)\right]} \oplus s_{\bar{B} \bmod \left[n+\frac{1}{2} n(n-1)\right]} \\
& =x_{\bar{b} \bmod \left[n+\frac{1}{2} n(n-1)\right]} \oplus s_{\bar{B} \bmod \left[n+\frac{1}{2} n(n-1)\right]} \tag{5.7}
\end{align*}
$$

Hence, the classical post-processing does not give an honest Bob any more information about the other two bits Alice has sent.

- If Bob is dishonest, he can guess the bits $x_{\bar{b} \bmod \left[n+\frac{1}{2} n(n-1)\right]}$ with probability $B_{\text {OT }}(P)$. He knows $r$, $\left(s_{1}, s_{2}, \ldots, s_{n}\right)$, and the pairwise XORs $s_{n+1}=$ $s_{1} \oplus s_{2}, s_{n+2}=s_{1} \oplus s_{3}, \ldots, s_{n+\frac{1}{2} n(n-1)}=s_{n-1} \oplus s_{n}$. We have $s_{c}=x_{c}^{\prime} \oplus$ $X_{c}=x_{(c+r) \bmod \left[n+\frac{1}{2} n(n-1)\right]} \oplus X_{c}$ for $c \in\{1,2, \ldots, n\}$ and, when $x_{l}=x_{i} \oplus x_{j}$ holds, $s_{l}=s_{i} \oplus s_{j}=x_{l}^{\prime} \oplus X_{l}=x_{(l+r) \bmod \left[n+\frac{1}{2} n(n-1)\right]} \oplus X_{l}$ for $l \in\{n+$ $\left.1, n+2, \ldots, n+\frac{1}{2} n(n-1)\right\}, i, j \in\{1,2, \ldots, n\}$, and $i \neq j$. Thus, $X_{c}=$ $x_{(c+r) \bmod \left[n+\frac{1}{2} n(n-1)\right]} \oplus s_{c}$ as well as $X_{l}=x_{(l+r) \bmod \left[n+\frac{1}{2} n(n-1)\right]} \oplus s_{l}$, and, for Bob, guessing $\left(X_{1}, X_{2}, \ldots, X_{n}, X_{n+1}, \ldots, X_{n+\frac{1}{2} n(n-1)}\right)$ is equivalent to guessing $\left(x_{1}, x_{2}, \ldots, x_{n}, x_{n+1}, \ldots, x_{n+\frac{1}{2} n(n-1)}\right)$. Therefore, $B_{\text {OT }}(Q)=B_{\text {OT }}(P)$.

The protocol that we consider and analyse in the following subsections is a natural extension from the optimal protocol analysed in Section 3.2, which covers the specific case where $n=2$, i.e. 1 -out-of-2 XOT. This extended version of the non-interactive 1-out-of- $n$ XOT protocol proceeds as follows.

1. Let $s=x_{1} x_{2} \ldots x_{n}$, where $n \geq 2$ and $n \in \mathbb{N}$, be Alice's string of $n$ classical bits $x_{i} \in\{0,1\}$, for $i \in\{1, \ldots, n\}$, and she encodes $s$ into the $(n+1)$-dimensional pure quantum state

$$
\begin{equation*}
\left|\phi_{s}\right\rangle=\frac{1}{\sqrt{n+1}}\left(|0\rangle+\sum_{i=1}^{n}(-1)^{x_{i}}|i\rangle\right) . \tag{5.8}
\end{equation*}
$$

Alice picks each of the possible $2^{n}$ bit strings with an equal probability of $1 / 2^{n}$. She sends the state $\left|\phi_{s}\right\rangle$ to Bob.
2. Bob applies an unambiguous quantum state elimination measurement on the received state, excluding $2^{n-1}$ states with certainty, from which he can deduce either one of the bits or one pairwise XOR. The measurement consists of
$2\left[n+\binom{n}{2}\right]=n(n+1)$ operators,

$$
\begin{array}{ll}
\Pi_{x_{i}=0}=\frac{1}{2 n}(|0\rangle+|i\rangle)(\langle 0|+\langle i|), & \Pi_{x_{i} \oplus x_{j}=0}=\frac{1}{2 n}(|i\rangle+|j\rangle)(\langle i|+\langle j|), \\
\Pi_{x_{i}=1}=\frac{1}{2 n}(|0\rangle-|i\rangle)(\langle 0|-\langle i|), & \Pi_{x_{i} \oplus x_{j}=1}=\frac{1}{2 n}(|i\rangle-|j\rangle)(\langle i|-\langle j|), \tag{5.9}
\end{array}
$$

where $i, j \in\{1, \ldots, n\}$ and $i \neq j$. That is, there are $2 n$ operators for the individual bits and $2\binom{n}{2}=n(n-1)$ operators for the pairwise XORs. Bob obtains his output at random and each one of the different results occurs with an equal probability of $2 /[n(n+1)]$.

### 5.3.1 Dishonest Bob

We consider a dishonest Bob who wants to learn all $n$ bits and, in this way, will also learn all pairwise XORs. Eq. (5.1) gives the probability for how well Bob can do so using the guessing strategy, where he follows the protocol honestly and then guesses the most likely outcome. This is obviously not his best cheating strategy, but he can maximise the probability to correctly learn all $n$ bits by applying a minimum-error measurement.

The states in Eq. (5.8) are multiply symmetric, whereby the symmetry unitary operators are those that either apply a phase shift to a basis $|i\rangle$ or not. Since the states are symmetric and equiprobable, the square-root measurement (SRM) is the optimal minimum-error measurement [82] and it is possible to calculate this optimal measurement and associated minimum error probability [73, 74]. The measurement operators of the SRM are

$$
\begin{equation*}
\Pi_{i}=p_{i} \rho_{\text {total }}^{-1 / 2} \cdot \rho_{i} \cdot \rho_{\text {total }}^{-1 / 2}=\frac{n+1}{2^{n}} \rho_{i} \tag{5.10}
\end{equation*}
$$

where $p_{i}=1 / 2^{n}$ and $\rho_{\text {total }}=\mathbb{1} /(n+1)$. Each individual measurement operator, when the corresponding state was sent, has success probability

$$
\begin{equation*}
\operatorname{Tr}\left(\Pi_{i} \rho_{i}\right)=\operatorname{Tr}\left(\frac{n+1}{2^{n}} \rho_{i}^{2}\right)=\frac{n+1}{2^{n}} \operatorname{Tr}\left(\rho_{i}\right)=\frac{n+1}{2^{n}} . \tag{5.11}
\end{equation*}
$$

Here we make use of the fact that we have pure states and hence $\rho_{i}^{2}=\rho_{i}$. Bob's cheating probability $B_{O T}^{q}$ therefore is

$$
\begin{equation*}
B_{O T}^{q}=2^{n} p_{i} \operatorname{Tr}\left(\Pi_{i} \rho_{i}\right)=\frac{n+1}{2^{n}} \tag{5.12}
\end{equation*}
$$

### 5.3.2 Dishonest Alice

We consider a dishonest Alice who wants to learn which bit or pairwise XOR Bob has learnt. Eq. (5.2) gives the probability for how well Alice can do so using the guessing strategy, where she follows the protocol honestly and then guesses the most likely outcome. While a valid strategy, it is obviously not her best cheating strategy. When we assume that Bob is not doing any testing, then Alice can send Bob any state and she will want to send him the pure state within the subspace spanned by the states she is supposed to send, which maximises Bob's probability to obtain a certain outcome. Thus, she needs to consider the pairwise combinations of Bob's elimination measurement operators in Eq. (5.9) that refer to the same output; one for the output with value 0 and the other one for the output with value 1 . By sending the eigenstate that corresponds to the highest eigenvalue of the combined measurement operators, Alice can maximise Bob's probability of obtaining the associated outcome. The eigenvalue will thereby yield Bob's outcome probability as well as Alice's cheating probability.

For the individual bits $x_{i}$, where $i \in\{1, \ldots, n\}$,

$$
\begin{equation*}
\Pi_{x_{i}=0}+\Pi_{x_{i}=1}=\frac{1}{n}(|0\rangle\langle 0|+|i\rangle\langle i|) \tag{5.13}
\end{equation*}
$$

and we have the $n+1$ eigenvalues $(1 / n, 1 / n, 0, \ldots, 0)$ with the eigenvectors associated to the highest (here the non-zero) eigenvalues being $|0\rangle$ and $|i\rangle$. For the XORs $x_{i} \oplus x_{j}$, where $i, j \in\{1, \ldots, n\}$ and $i \neq j$,

$$
\begin{equation*}
\Pi_{x_{i} \oplus x_{j}=0}+\Pi_{x_{i} \oplus x_{j}=1}=\frac{1}{n}(|i\rangle\langle i|+|j\rangle\langle j|) \tag{5.14}
\end{equation*}
$$

and we have the $n+1$ eigenvalues $(1 / n, 1 / n, 0, \ldots, 0)$ with the eigenvectors associated to the highest (here the non-zero) eigenvalues being $|i\rangle$ and $|j\rangle$. Thus, Alice's cheating probability $A_{O T}^{q}$ is

$$
\begin{equation*}
A_{O T}^{q}=\frac{1}{n} . \tag{5.15}
\end{equation*}
$$

This cheating probability might be reduced when testing is added. Since this is not the case for the 1-2 XOT protocol that follows the same protocol outline and was presented in Section 3.2, it might also be that testing would not reduce Alice's cheating probability in the more general case. Nevertheless, Eq. (5.15) gives a valid upper bound for Alice's cheating probability.

### 5.3.3 Change of Cheating Probabilities with Increasing $n$

Alice's and Bob's cheating probabilities change with increasing $n$, i.e. with increasing length of Alice's bit string. Here, we not only look at and compare the cheating probabilities in Eqns. (5.12) and (5.15), but also the differences between these and the respective guessing strategies in Eqns. (5.1) and (5.2).


Figure 5.1: The cheating (filled symbols) and guessing (unfilled symbols) probabilities for Alice and Bob. Alice's probabilities are plotted by the triangles and Bob's probabilities by the circles.

In Figure 5.1, both Alice's and Bob's cheating and guessing probabilities are plotted. For both Alice and Bob, these probabilities decrease and converge towards 0 for an increasing $n$. Bob's probabilities (plotted in circles), however, have a steeper decrease than Alice's (plotted in triangles). The graphs for $A_{O T}^{q}$ and $B_{O T}^{q}$ as well as the graphs for $A_{O T}^{g}$ and $B_{O T}^{g}$ intersect at around $n \approx 4.798$. Hence, Bob's cheating and guessing probabilities are higher than Alice's for $n \in\{2,3,4\}$ and the other way round for $n \geq 5$. This can be explained by looking at the number of potential answers for dishonest Alice and dishonest Bob and noticing that $2^{n-1}>\frac{1}{2} n(n+1)$ for $n \geq 5$, that is, the number for potential answers for a cheating Bob becomes larger than for a cheating Alice when $n \geq 5$, while it is the other way round for $n \in\{2,3,4\}$.

Figure 5.2 shows the absolute difference between the guessing and cheating probabilities for Alice (triangles) and Bob (circles). Both graphs reach their maximum when $n=2$ or $n=3$, that is, the absolute difference between the guessing and cheating probabilities is maximal at these values for $n$. For Alice, the difference between her guessing and cheating probabilities reaches its maximum of $1 / 6$ there, i.e. $A_{O T}^{q}-A_{O T}^{g}=1 / 6$ when $n=2$ or $n=3$. For Bob, the difference between his guessing
and cheating probabilities reaches its maximum of $1 / 4$ there, i.e. $B_{O T}^{q}-B_{O T}^{g}=1 / 4$ when $n=2$ or $n=3$. Beyond those points (for $n \geq 4$ ), both graphs tend towards zero. We can conclude that, while the cheating probability will always be larger than the guessing probability for both parties, the absolute differences become smaller for increasing $n$.


Figure 5.2: Absolute differences of the guessing and cheating probabilities. The plot with the triangles shows $A_{O T}^{q}-A_{O T}^{g}$ and the one with the circles shows $B_{O T}^{q}-B_{O T}^{g}$.

This is not the case when considering the relative difference which increases with increasing $n$. We note that, even though the absolute differences between cheating and guessing probabilities differ for Alice and Bob, the relative difference is the same for both. That is,

$$
\begin{equation*}
\frac{A_{O T}^{q}-A_{O T}^{g}}{A_{O T}^{g}}=\frac{B_{O T}^{q}-B_{O T}^{g}}{B_{O T}^{g}}=\frac{n-1}{2} \tag{5.16}
\end{equation*}
$$

and this linear function is plotted by the stars in Figure 5.3. For comparison, we also consider and plot the relative differences between the guessing probabilities and perfect cheating with probability 1. These turn out to differ for Alice and Bob, in particular,

$$
\begin{align*}
& \frac{1-A_{O T}^{g}}{A_{O T}^{g}}=\frac{1}{2}\left(k^{2}+k-2\right), \\
& \frac{1-B_{O T}^{g}}{B_{O T}^{g}}=2^{k-1}-1 \tag{5.17}
\end{align*}
$$

Both are exponential functions, with the one for Alice having a steeper increase than the one for Bob. In the ideal case, the relative difference equals zero since the ideal possible cheating probability is equal to the guessing probability. Figure 5.3 shows that with increasing $n$ the relative difference of the protocol's cheating and guessing
probabilities stays comparatively close to the relative difference of the ideal case, while it moves further and further away from the relative differences corresponding to perfect cheating.


Figure 5.3: Relative differences of the guessing and cheating probabilities. The stars plot the relative difference for $\left(A_{O T}^{q}-A_{O T}^{g}\right) / A_{O T}^{g}$ and $\left(B_{O T}^{q}-B_{O T}^{g}\right) / B_{O T}^{g}$. As comparison, the plots for the relative differences between perfect cheating and guessing probabilities are included, $\left(1-A_{O T}^{g}\right) / A_{O T}^{g}$ shown by the triangles and ( $1-$ $\left.B_{O T}^{g}\right) / B_{O T}^{g}$ by the circles.

### 5.3.4 Comparison to Classical XOT Protocols

Just as for 1-2 XOT, we want to evaluate the performance of the generalised quantum $1-n$ XOT protocols when compared to classical 1-n XOT protocols. As before, we define two trivial classical 1-n XOT protocols.

Protocol 1: Alice has the $n$ bits $\left(x_{1}, x_{2}, \ldots, x_{n}\right)$, and chooses to send Bob either one of the individual bits $x_{i}$ or a pairwise XOR $x_{i} \oplus x_{j}$, for $i, j \in\{1,2, \ldots, n\}$ and $i \neq j$. Afterwards she "forgets" what she has sent.

Here, Alice can obviously cheat perfectly with probability 1 , while Bob can only cheat with probability $1 / 2^{n-1}$ by guessing the remaining $n-1$ bits that he is missing to complete the whole bit string $\left(x_{1}, x_{2}, \ldots, x_{n}\right)$ which also implies knowledge of all the XORs.

Protocol 2: Alice sends all of $\left(x_{1}, x_{2}, \ldots, x_{n}, x_{1} \oplus x_{2}, \ldots, x_{n-1} \oplus x_{n}\right)$ to Bob, who chooses one of these bits to read and discards the others without looking at them.

Here, Bob can obviously now cheat perfectly with probability 1 by reading out at least the bits $x_{1}, x_{2}, \ldots x_{n}$. Alice on the other hand can only cheat with probability $2 /[n(n+1)]$ by guessing which bit Bob has chosen to read out.

We combine these protocols using a method described in Ref. [47]: The outcome of an unbalanced weak coin flipping protocol conducted by Alice and Bob will specify which protocol gets implemented. This ultimately results in:

Protocol 3: Protocol 1 is implemented with probability $s$ and Protocol 2 is implemented with probability $(1-s)$.

The cheating probabilities for Alice and Bob in Protocol 3 are

$$
\begin{align*}
& A_{O T}^{c}=s(1)+(1-s) \frac{2}{n(n+1)}=\frac{2}{n(n+1)}+s\left(1-\frac{2}{n(n+1)}\right) \\
& B_{O T}^{c}=s \frac{1}{2^{n-1}}+(1-s)(1)=1-s\left(1-\frac{1}{2^{n-1}}\right) \tag{5.18}
\end{align*}
$$

The trade-off relation $f^{t}\left(A_{O T}^{c}, B_{O T}^{c}\right)=c_{1} A_{O T}^{c}+c_{2} B_{O T}^{c}$, where the constants $c_{1}$ and $c_{2}$ are chosen so that $s$ gets eliminated, is

$$
\begin{align*}
f^{t}\left(A_{O T}^{c}, B_{O T}^{c}\right) & =\left(2^{n-1}-1\right) n(n+1) A_{O T}^{c}+2^{n-1}[n(n+1)-2] B_{O T}^{c} \\
& =2^{n-1} n(n+1)-2 . \tag{5.19}
\end{align*}
$$

For the quantum protocol, Eq. (5.15) gives Alice's cheating probability and Eq. (5.12) gives Bob's cheating probability, thus we obtain the trade-off relation

$$
\begin{align*}
f^{t}\left(A_{O T}^{q}, B_{O T}^{q}\right) & =\left(2^{n-1}-1\right) n(n+1) A_{O T}^{q}+2^{n-1}[n(n+1)-2] B_{O T}^{q} \\
& =0.5(n+1)\left[2^{n}-4+n(n+1)\right] . \tag{5.20}
\end{align*}
$$

To compare the trade-off relations in the quantum and classical case for the different $n$, it is sensible to subtract the expression of the trade-off relation of the guessing probabilities from both $f^{t}\left(A_{O T}^{c}, B_{O T}^{c}\right)$ and $f^{t}\left(A_{O T}^{q}, B_{O T}^{q}\right)$. The guessing probabilities are a baseline, showing what is desirable for an ideal protocol, and they are the same in the quantum and classical case. The difference between the cheating and the guessing probabilities indicates how successful a cheating strategy is in comparison to the guessing strategy. So it is of interest how this difference develops with respect to $n$ and if the quantum or the classical cheating strategies have a bigger advantage over the guessing strategy.

The trade-off relation for the guessing probabilities given in Eqns. (5.2) and (5.1) is

$$
\begin{align*}
f^{t}\left(A_{O T}^{g}, B_{O T}^{g}\right) & =\left(2^{n-1}-1\right) n(n+1) A_{O T}^{g}+2^{n-1}[n(n+1)-2] B_{O T}^{g} \\
& =n^{2}+n+2^{n}-4 . \tag{5.21}
\end{align*}
$$

Figure 5.4 shows the differences $f^{t}\left(A_{O T}^{c}, B_{O T}^{c}\right)-f^{t}\left(A_{O T}^{g}, B_{O T}^{g}\right)$ and $f^{t}\left(A_{O T}^{q}, B_{O T}^{q}\right)-$ $f^{t}\left(A_{O T}^{g}, B_{O T}^{g}\right)$ with respect to $n$. The graph for the function of the difference in the classical case is always above the one of the difference in the quantum case, that is, $f^{t}\left(A_{O T}^{c}, B_{O T}^{c}\right)-f^{t}\left(A_{O T}^{g}, B_{O T}^{g}\right)>f^{t}\left(A_{O T}^{q}, B_{O T}^{q}\right)-f^{t}\left(A_{O T}^{g}, B_{O T}^{g}\right)$ for $n \geq 2$. Hence, there is a quantum advantage over the considered classical protocol since the quantum cheating strategies offer a smaller advantage over the guessing strategies than the classical cheating strategies. Furthermore, the quantum advantage increases with increasing $n$ as the gap between the two graphs widens.


Figure 5.4: Trade-off relations with respect to $n$ of the classical protocol (squares) and the quantum protocol (diamond) after subtraction of the relation for the guessing probabilities.

### 5.4 Similarities to Quantum Retrieval Games

There are some cryptographic concepts which exhibit similarities to oblivious transfer. One example was mentioned in Chapter 2. In particular, the cryptographic primitive of symmetrically private information retrieval [52] is related to the OT variant 1-out-of- $n$ oblivious transfer. Another concept that has similarities to specifically the variant 1-out-of-n XOT are quantum retrieval games (QRG) [81]. The
notion of QRGs can be used as building block for quantum protocols and has been applied as part of quantum money schemes [81, 83, 84].

In a quantum retrieval game, a sender Alice sends to a receiver Bob a quantum state $\rho_{x}$ that encodes some randomly selected bit string $x$ of some length $n$. The string $x$ is thereby chosen at random according to a probability distribution $p(x)$. Bob then measures $\rho_{x}$ in order to be able to answer a question about the string, whereby the goal is for the answer to be correct with the highest possible probability or in some applications even with certainty [84, 85]. Mathematically, a question is described as a relation $\sigma$. That is, for a set of inputs $X$ and a set of answers $A$, a relation $\sigma$ is a subset of $X \times A$ such that $(x, a) \in \sigma$ means that $a$ is a valid answer to the question described by the relation $\sigma$ when $x$ is given. More formally, in Ref. [85], QRGs are defined as follows.

Definition 5.3 (Quantum retrieval game [85]). Let $X \subseteq N$ and $A \subseteq N$ be the set of inputs and answers, respectively. Let also $\sigma \subseteq X \times A$ be a relation and $\left\{p(x), \rho_{x}\right\}$ be an ensemble of states and their a priori probabilities. Then the tuple $G=\left(X, A, \sigma,\left\{p(x), \rho_{x}\right\}\right)$ is called a quantum retrieval game (QRG). For a given $x \in X$, an answer $a \in A$ is correct if $(x, a) \in \sigma$.

A specific class of quantum retrieval games is based on the hidden matching problem (HM) first introduced in Ref. [86].

Definition 5.4 (Hidden matching). Alice has a bit string of length $n$ as input and Bob has a matching $M \in \mathcal{M}_{n}$, where $\mathcal{M}_{n}$ is the set of all perfect (no free nodes, all paired up) matchings on $n$ nodes. The output should be the tuple $\langle i, j, a\rangle$, where $a=x_{i} \oplus x_{j}$ for the matching $M$ connecting the nodes $x_{i}$ and $x_{j}$.

In the class of hidden matching QRGs, the relations $\sigma$ are described by the matchings and their answers are the parities of two bits of Alice's string which are connected by the respective matching. Alice encodes her bit string $x=x_{1} x_{2} \ldots x_{n}$, where $n$ is even, into the $n$-dimensional pure state [ $81,84,85$ ]

$$
\begin{equation*}
\left|\phi_{x}\right\rangle=\frac{1}{\sqrt{n}} \sum_{i=1}^{n}(-1)^{x_{i}}|i\rangle . \tag{5.22}
\end{equation*}
$$

This makes the similarity to 1-out-of- $n$ XOT rather obvious. The state used for $1-n \mathrm{XOT}$ as given in Eq. (5.8) differs from the state in Eq. (5.22) only in that it has the basis state $|0\rangle$ added to it and has an adjusted normalisation factor, i.e. a string of length $n$ gets encoded into an $(n+1)$-dimensional state instead. When an XOR of two bits is the result for the oblivious transfer protocol, then this matches the parity
between these two bits which is the result in a coinciding hidden matching QRG. On the other hand, when an individual bit is the result for the oblivious transfer protocol, then this can still be seen as the XOR or parity between that bit and a bit $x_{0}$ describing the power that is applied to a factor of $(-1)$ in front of $|0\rangle$. This means, we can imagine a factor $(-1)^{x_{0}}$ in front of $|0\rangle$ and set $x_{0}=0$ always. The XOR $x_{0} \oplus x_{i}(i \in\{1, \ldots, n\})$ then gives the value of the bit $x_{i}$ which is also the same as the parity, i.e. 0 if $x_{i}=x_{0}$ or 1 if $x_{i} \neq x_{0}$.

A difference is that we can have a string of an odd length $n$ in oblivious transfer, while $n$ needs to be even in hidden matching quantum retrieval games in order to satisfy the requirement that a matching on $n$ nodes is perfect. Furthermore, in hidden matching QRGs, only a dishonest sender (Alice) is considered, that is, Alice wanting to know which parity the receiver (Bob) has learnt. A dishonest receiver is not of interest in this concept. Arrazola et al. [85] investigated 1-out-of- $k$ hidden matching quantum retrieval games where $k$ is the number of different matchings. They bound the cheating probability of a dishonest Alice, deriving the same equation as the one for Alice's cheating probability in 1-out-of- $n$ XOT (Eq. (5.15)) but in terms of the number of relations $k$ instead of in terms of the length of the bit string $n$.

### 5.5 Conclusion

In this chapter, we generalised XOR oblivious transfer to 1-out-of-n XOT, where Alice encodes a classical string consisting of $n$ bits. Introducing a specific protocol which is a natural extension of the non-interactive 1-2 XOT protocol considered in Section 3.2, we calculated Alice's and Bob's cheating probabilities as functions of $n$. Unsurprisingly, their cheating probabilities decrease with increasing $n$. This is, because the increase in length of Alice's bit string and thus the increase in number of possible outcomes for Bob, results in larger sets of potential outcomes that the dishonest party needs to guess correctly from. Comparing this quantum 1-n XOT protocol to a classical 1-n XOT protocol shows that the quantum advantage over the considered classical protocol increases with an increasing $n$. This generalised XOR oblivious transfer, 1-out-of- $n$ XOT, shows similarities to the notion of hidden matching quantum retrieval games as was indicated and briefly discussed in the last subsection.

It is possible to expand on the work in this chapter. The situation of a dishonest Alice when Bob is testing in the considered 1-n XOT protocol remains unexamined. This examination can answer the open question if testing can decrease Alice's
cheating probability or if her cheating probability is independent of any testing and remains unchanged as in the specific 1-2 XOT case. Also the comparison between 1-out-of- $n$ XOT and hidden matching QRGs can be investigated further to examine if there is a possible reduction from XOT to hidden matching QRGs.

## Chapter 6

## Quantum Rabin Oblivious Transfer

### 6.1 Introduction

As mentioned in Chapter 2, Rabin oblivious transfer was one of the first oblivious transfer protocols specified [10] and is also called all-or-nothing oblivious transfer. In Rabin OT, the sender Alice has a bit $x$ with value 0 or 1 and sends it to the receiver Bob. Bob will either receive nothing with probability $p_{\text {? }}$ or he will receive the bit with probability $1-p_{?}$; see Figure 6.1. Alice is not supposed to learn whether Bob has obtained the bit or not, and Bob is not supposed to be able to learn a bit value he did not receive. In the traditional definition of Rabin OT the probability $p_{\text {? }}=1 / 2$, i.e. Bob is equally likely to obtain the bit or to obtain nothing.


Figure 6.1: Rabin oblivious transfer from Alice to Bob.

In this chapter, we first look at Rabin oblivious transfer using pure states and then at a Rabin OT protocol with mixed states. Focus remains on the category of non-interactive protocols, that is, protocols where there is only one state transmission from sender to receiver followed by the receiver's measurement.

However, analysing the sender's cheating probability, we discover that, for the protocols considered in this chapter, testing by the receiver needs to be introduced to restrict the sender's cheating probability. Depending on the method of testing, we might lose the non-interactivity to some extent. That is, if the testing scheme used is the same as applied in previous chapters, where the receiver checks some states to make sure they are what the receiver declares them to be, then classical
communication is added in the testing rounds and leaves us with some interaction between sender and receiver. We, however, also consider another testing method not based on interaction between sender and receiver, thus maintaining the noninteractivity of the protocols.

The security of the protocols in this chapter is analysed by calculating the cheating probabilities for Alice and Bob. In respect thereof, a dishonest Alice and a dishonest Bob are defined as:

## Dishonest Alice:

A cheating Alice wants to learn if Bob has received the bit or not.

## Dishonest Bob:

A cheating Bob wants to always know the value of the bit Alice has sent, even when he did not receive anything.

### 6.2 Rabin OT Using Pure States

The simplest way to construct a non-interactive quantum Rabin OT protocol with pure states is by picking two non-orthogonal pure states in which Alice encodes her bit value and having Bob make an unambiguous discrimination measurement so that he can either learn the bit value unambiguously or learn nothing at all. Such a protocol was considered by Cheong et al. [87]. In this section, we extend the security analysis to different cheating strategies and look at it from a slightly different angle. That is, we examine Alice's cheating probability, whereas Cheong et al. looked instead at how much a dishonest Alice can decrease or increase the probability of Bob receiving a bit value. We also include testing by Bob and a direct comparison with a classical Rabin OT protocol, both of which were not considered in Ref. [87].

### 6.2.1 The Protocol

Alice encodes her bit value $v \in\{0,1\}$ in a respective pure state $\left|\psi_{v}\right\rangle$. Without loss of generality, we can choose the two pure states

$$
\begin{align*}
& \left|\psi_{0}\right\rangle=\cos \theta|0\rangle+\sin \theta|1\rangle, \\
& \left|\psi_{1}\right\rangle=\cos \theta|0\rangle-\sin \theta|1\rangle, \tag{6.1}
\end{align*}
$$

whose overlap is $\left\langle\psi_{0} \mid \psi_{1}\right\rangle=\cos (2 \theta)$, where $0^{\circ} \leq \theta \leq 45^{\circ}$, and is real. The Rabin OT protocol is then carried out as follows.

1. Alice randomly chooses the state $\left|\psi_{0}\right\rangle$ or $\left|\psi_{1}\right\rangle$, with a probability of $1 / 2$ each, and sends it to Bob.
2. Bob performs an unambiguous discrimination measurement on the received state [88, 89, 90]. His measurement operators are

$$
\begin{align*}
& \Pi_{0}=\frac{1}{2 \cos ^{2} \theta}\left|\overline{\psi_{1}}\right\rangle\left\langle\overline{\psi_{1}}\right|, \\
& \Pi_{1}=\frac{1}{2 \cos ^{2} \theta}\left|\overline{\psi_{0}}\right\rangle\left\langle\overline{\psi_{0}}\right|, \\
& \Pi_{?}=\left(1-\tan ^{2} \theta\right)|0\rangle\langle 0|, \tag{6.2}
\end{align*}
$$

with $\left|\overline{\psi_{0}}\right\rangle=\sin \theta|0\rangle-\cos \theta|1\rangle$ and $\left|\overline{\psi_{1}}\right\rangle=\sin \theta|0\rangle+\cos \theta|1\rangle$ being the orthogonal states to Alice's states in Eq. (6.1). $\Pi_{0}$ corresponds to a bit value of $0, \Pi_{1}$ to a bit value of 1 , and $\Pi_{\text {? }}$ to obtaining no bit.

Bob will then obtain an inconclusive result with probability $p_{\text {? }}=\cos (2 \theta)[88,89$, 90] and will learn the bit value with probability $1-p_{\text {? }}=2 \sin ^{2} \theta$. When looking at Rabin OT in the traditional definition, where, in an honest implementation of the protocol, Bob receives no bit with probability $1 / 2$ and receives the bit with probability $1 / 2$, we need $\theta=30^{\circ}$. Other values for $\theta$, and hence for Bob's probabilities to receive the bit or not, are also possible. Analysis of the protocol generally for $0^{\circ} \leq \theta \leq 45^{\circ}$ shows for which values of $\theta$ Alice's and Bob's cheating probabilities might be better or worse.

### 6.2.2 Dishonest Bob

First, we look at a cheating Bob who always wants to know which bit Alice has sent. A cheating strategy that Bob can always apply in any Rabin oblivious transfer protocol, whether quantum or classical, and that does not require him to deviate from the protocol, is to follow the protocol honestly and then randomly guess the bit value whenever he obtains an inconclusive result. We call this the guessing strategy and use it as a baseline for comparison with Bob's cheating probability. In an ideal case, he would not be able to cheat any better than this.

Bob learns the bit value with probability $1-p_{?}=2 \sin ^{2} \theta$ and, when he does not obtain the bit, he can guess the value correctly with probability $1 / 2$ since Alice sends the two states, i.e. chooses the two bit values, with equal probabilities. Thus, Bob's guessing probability $B_{\text {pure }}^{g}$ OT is

$$
\begin{equation*}
B_{\text {pure } O T}^{g}=1-\frac{1}{2} p_{?}=1-\frac{1}{2} \cos (2 \theta) . \tag{6.3}
\end{equation*}
$$

Bob can cheat more successfully in the quantum protocol if he does not follow its steps honestly. His optimal cheating strategy involves him applying a minimum-error measurement on the received state. This will enable him to distinguish between $\left|\psi_{0}\right\rangle$ and $\left|\psi_{1}\right\rangle$ with a minimum probability of being wrong. Bob's cheating probability $B_{\text {pure } O T}^{q}$ can be calculated with the Helstrom bound [80]

$$
\begin{equation*}
B_{\text {pure } O T}^{q}=\frac{1}{2}\left(1+\sqrt{1-p_{?}^{2}}\right)=\frac{1}{2}[1+\sin (2 \theta)] . \tag{6.4}
\end{equation*}
$$

The measurement with which he can achieve this probability is the projective measurement in the eigenbasis of $\left(\frac{1}{2}\left|\psi_{0}\right\rangle\left\langle\psi_{0}\right|-\frac{1}{2}\left|\psi_{1}\right\rangle\left\langle\psi_{1}\right|\right)$. Thus, the measurement operators are

$$
\begin{equation*}
\Pi_{\left|\psi_{0}\right\rangle}=\frac{1}{2}(|0\rangle+|1\rangle)(\langle 0|+\langle 1|) \quad \text { and } \quad \Pi_{\left|\psi_{1}\right\rangle}=\frac{1}{2}(|0\rangle-|1\rangle)(\langle 0|-\langle 1|) . \tag{6.5}
\end{equation*}
$$

In Figure 6.2, we plot Bob's guessing and cheating probabilities, once in terms of $\theta$ and once in terms of $p_{\text {? }}$. Except for $\theta=0^{\circ}$ and $\theta=45^{\circ}$, where these probabilities coincide, Bob's cheating strategy is always better than simply guessing. When $\theta=0^{\circ}$, then $p_{?}=1$ and $\left|\psi_{0}\right\rangle=\left|\psi_{1}\right\rangle$, and Bob cannot cheat better than with a random guess, $B_{\text {pure } O T}^{q}=1 / 2=B_{\text {pure } O T}^{g}$. For $\theta=45^{\circ},\left|\psi_{0}\right\rangle$ and $\left|\psi_{1}\right\rangle$ are orthogonal. Thus, Bob can perfectly distinguish between the two states, $B_{\text {pure } O T}^{q}=1$. However, in this case $p_{\text {? }}=0$ so, if he is honest, he would also always receive the bit value, $B_{\text {pure } O T}^{g}=1$. In the case where $\theta=30^{\circ}$, giving $p_{\text {? }}=1 / 2$, Bob's cheating probability is relatively high at $B_{\text {pure } O T}^{q}=(2+\sqrt{3}) / 4 \approx 0.933$, whereas his guessing probability $B_{\text {pure } O T}^{g}=3 / 4$.


Figure 6.2: Bob's guessing and cheating probabilities as functions of the angle $\theta$ (subfigure (a)) and as functions of $p_{\text {? }}$ (subfigure (b)). His guessing probability $B_{\text {pure OT }}^{g}$ is plotted as the solid line and his cheating probability $B_{\text {pure } O T}^{q}$ as the dashed line.

### 6.2.3 Dishonest Alice

For a cheating Alice who wants to know if Bob has received the bit or not, there are several different cheating strategies that we can consider. Depending on whether Bob does some testing to check if Alice is cheating, and on how he tests, her optimal cheating strategy varies. In this subsection, we present different scenarios and the respective optimal cheating strategies.

First of all, there also exists a guessing strategy for Alice which can be used as baseline to compare to her cheating probabilities. Alice will not deviate from the protocol, but follows it honestly and then randomly guesses if Bob has received the bit or not. In an ideal case, Alice would not be able to cheat any better than this. Alice knows that Bob receives no bit with probability $p_{\text {? }}=\cos (2 \theta)$ and receives the bit with probability $1-p_{\text {? }}$. Thus, she will always guess the more likely of the two outcomes which will depend on $\theta$. Specifically, for $0^{\circ} \leq \theta \leq 30^{\circ}, p_{\text {? }} \geq 1 / 2$, so Alice will guess that Bob did not receive the bit, and, for $30^{\circ} \leq \theta \leq 45^{\circ}, p_{?} \leq 1 / 2$, so she will guess that he received the bit. Note that, in this case, she also knows which bit value he obtained since she knows which of the states she has sent. Thus, Alice's guessing probability $A_{\text {pure } O T}^{g}$ is

$$
A_{\text {pure } O T}^{g}=\max \left(1-p_{?}, p_{?}\right)= \begin{cases}\cos (2 \theta) & \text { for } 0^{\circ} \leq \theta \leq 30^{\circ}  \tag{6.6}\\ 2 \sin ^{2} \theta & \text { for } 30^{\circ} \leq \theta \leq 45^{\circ}\end{cases}
$$

Alice can perfectly guess Bob's outcome, that is $A_{\text {pure } O T}^{g}=1$, when $\theta=0^{\circ}$ since Bob will never get the bit, or when $\theta=45^{\circ}$ since Bob will always receive the bit. Her guessing probability is at its minimum $A_{\text {pure } O T}^{g}=1 / 2$ when $p_{?}=1 / 2$, corresponding to $\theta=30^{\circ}$, since Bob is then equally likely to receive the bit or not.

After discussion of Alice's other cheating scenarios, we will compare the different cheating probabilities and guessing probability in Figure 6.4.

## No testing by Bob

If there is no testing by Bob, Alice is free to send whatever state suits her best. Looking at honest Bob's measurement operators in Eq. (6.2), we find that his inconclusive measurement operator $\Pi_{\text {? }}$ is orthogonal to the state $|1\rangle$. Thus, Alice's best choice is to always send the state $|1\rangle$ and then she will know that Bob will always receive a bit value. Therefore, without any testing by Bob, Alice can cheat perfectly, $A_{\text {pure } O T}^{q}=1$. In this case, however, Alice is maximally uncertain about which of the two bit values Bob has obtained.

## Bob testing - Monitoring the occurrence probabilities

A testing strategy for Bob is to keep track of the probabilities of obtaining a bit or obtaining no bit and to check if they are what he expects them to be. He makes no further checks, asks Alice for no more information, nor discards any states. Thus, this testing method does not affect the protocol's non-interactivity. In order to not get detected, a cheating Alice needs to choose what she sends Bob in such a way that the occurrence probabilities for bit with value 0 , bit with value 1 , and no bit match Bob's expectations. Note that, for this test to work, multiple rounds of the protocol are necessary in order for Bob to be able to obtain the statistics. This results in the cheating probability calculated here for Alice becoming an average cheating probability.

Since Alice can be sure that Bob has received a bit, when she sends $|1\rangle$, we suspect that Alice's best choice of states to distinguish between Bob received a bit and Bob received no bit are $|0\rangle$ and $|1\rangle$. We prove that sending a statistical mixture of theses states is indeed Alice's optimal cheating strategy here.

Proposition 6.1. Alice's optimal cheating strategy, when Bob is monitoring the probabilities, is to send an appropriate statistical mixture of the states $|0\rangle$ and $|1\rangle$.

Proof. Bob's measurement operators for the cases bit and no bit are

$$
\begin{align*}
\Pi_{\mathrm{bit}} & =\Pi_{0}+\Pi_{1}=\tan ^{2} \theta|0\rangle\langle 0|+|1\rangle\langle 1|=\left(\begin{array}{cc}
\tan ^{2} \theta & 0 \\
0 & 1
\end{array}\right), \\
\Pi_{?} & =\left(1-\tan ^{2} \theta\right)|0\rangle\langle 0|=\left(\begin{array}{cc}
1-\tan ^{2} \theta & 0 \\
0 & 0
\end{array}\right) . \tag{6.7}
\end{align*}
$$

Let us define the states

$$
\rho_{\mathrm{bit}}=\left(\begin{array}{cc}
b_{1} & b_{2}  \tag{6.8}\\
b_{2}^{*} & 1-b_{1}
\end{array}\right), \quad \rho_{\mathrm{no} \text { bit }}=\left(\begin{array}{cc}
n_{1} & n_{2} \\
n_{2}^{*} & 1-n_{1}
\end{array}\right)
$$

and assume that Alice sends a mixture of them $(0 \leq x \leq 1)$

$$
\rho_{\text {cheat }}=x \rho_{\text {no bit }}+(1-x) \rho_{\mathrm{bit}}=\left(\begin{array}{cc}
x n_{1}+(1-x) b_{1} & x n_{2}+(1-x) b_{2}  \tag{6.9}\\
x n_{2}^{*}+(1-x) b_{2}^{*} & x\left(1-n_{1}\right)+(1-x)\left(1-b_{1}\right)
\end{array}\right) .
$$

Bob's measurement probabilities are then given by

$$
\begin{align*}
\operatorname{Tr}\left(\Pi_{\text {bit }} \rho_{\text {cheat }}\right) & =1+\left(\tan ^{2} \theta-1\right)\left[x n_{1}+(1-x) b_{1}\right] \\
\operatorname{Tr}\left(\Pi_{?} \rho_{\text {cheat }}\right) & =\left(1-\tan ^{2} \theta\right)\left[x n_{1}+(1-x) b_{1}\right] \tag{6.10}
\end{align*}
$$

and we know that he expects $\operatorname{Tr}\left(\Pi_{\text {bit }} \rho_{\text {cheat }}\right)=2 \sin ^{2} \theta$ and $\operatorname{Tr}\left(\Pi_{?} \rho_{\text {cheat }}\right)=\cos (2 \theta)$. This yields the constraint

$$
\begin{equation*}
\left(1-\tan ^{2} \theta\right)\left[x n_{1}+(1-x) b_{1}\right]=\cos (2 \theta) \tag{6.11}
\end{equation*}
$$

Furthermore, we know Alice's conditional probabilities of sending a state and then guessing the outcome correctly. In particular,

$$
\begin{align*}
\operatorname{Tr}\left(\Pi_{\mathrm{bit}} \rho_{\mathrm{bit}}\right) & =1+b_{1}\left(\tan ^{2} \theta-1\right) \\
\operatorname{Tr}\left(\Pi_{?} \rho_{\mathrm{no}} \text { bit }\right) & =n_{1}\left(1-\tan ^{2} \theta\right) \tag{6.12}
\end{align*}
$$

However, we need to note that

$$
\begin{equation*}
\operatorname{Tr}\left(\Pi_{\text {bit }} \rho_{\text {no bit }}\right)=1-n_{1}\left(1-\tan ^{2} \theta\right) \geq \operatorname{Tr}\left(\Pi_{?} \rho_{\text {no bit }}\right) \tag{6.13}
\end{equation*}
$$

for $\theta \geq \arcsin (1 / \sqrt{3})$. Alice's cheating probability when sending $\rho_{\text {cheat }}$ is, therefore, given by one of two equations depending on the angle. For $\theta \leq \arcsin (1 / \sqrt{3}) \approx$ $35.264^{\circ}$

$$
\begin{equation*}
A_{\text {pure } O T}^{q}=x n_{1}\left(1-\tan ^{2} \theta\right)+(1-x)\left[1+b_{1}\left(\tan ^{2} \theta-1\right)\right] \tag{6.14}
\end{equation*}
$$

and for $\theta \geq \arcsin (1 / \sqrt{3}) \approx 35.264^{\circ}$

$$
\begin{equation*}
A_{\text {pure } O T}^{q}=x\left[1-n_{1}\left(1-\tan ^{2} \theta\right)\right]+(1-x)\left[1+b_{1}\left(\tan ^{2} \theta-1\right)\right] . \tag{6.15}
\end{equation*}
$$

Using the constraint in Eq. (6.11), Eq. (6.14) can be rewritten as

$$
\begin{equation*}
A_{\text {pure } O T}^{q}=1-\cos (2 \theta)+x\left[2 n_{1}\left(1-\tan ^{2} \theta\right)-1\right] . \tag{6.16}
\end{equation*}
$$

To maximise this equation, $x 2 n_{1}\left(1-\tan ^{2} \theta\right)$ needs to be as large as possible and, thus, $x$ and $n_{1}$ need to be chosen as large as possible while satisfying the constraint $x n_{1}+(1-x) b_{1}=\cos ^{2} \theta$ deduced from Eq. (6.11). The constraint indicates that $x n_{1} \leq \cos ^{2} \theta$ and equality holds when $b_{1}=0$. The largest possible value for $n_{1}$ is 1 and then it follows that $x=\cos ^{2} \theta$. The maximised value for Alice's cheating
probability given by Eq. (6.14) is then

$$
\begin{equation*}
A_{\mathrm{pure} O T}^{q}=\cos ^{2} \theta . \tag{6.17}
\end{equation*}
$$

Similarly, using the constraint in Eq. (6.11) to rewrite Eq. (6.15), gives

$$
\begin{equation*}
A_{\mathrm{pure} \text { OT }}^{q}=1-\cos (2 \theta)=2 \sin ^{2} \theta . \tag{6.18}
\end{equation*}
$$

We can can see that the values for $n_{1}, b_{1}$, and $x$ do not matter whenever $\theta \geq$ $\arcsin (1 / \sqrt{3})$. Alice will always guess that Bob obtained a bit and her guess will be correct with the expected occurrence probability. Thus, $n_{1}=1, b_{1}=0$, and $x=\cos ^{2} \theta$ are optimal and, considering the properties of a density matrix, it follows that $n_{2}=0$ and $b_{2}=0$. The cheating state is then

$$
\begin{equation*}
\rho_{\text {cheat }}=\cos ^{2} \theta|0\rangle\langle 0|+\left(1-\cos ^{2} \theta\right)|1\rangle\langle 1| . \tag{6.19}
\end{equation*}
$$

We can further show that this combination also satisfies the requirement that Bob obtains the first and the second state with equal probabilities since the probabilities for Bob, when he measures $|0\rangle$ or $|1\rangle$, are $\operatorname{Tr}\left(\Pi_{0}|1\rangle\langle 1|\right)=\operatorname{Tr}\left(\Pi_{1}|1\rangle\langle 1|\right)=1 / 2$ and $\operatorname{Tr}\left(\Pi_{0}|0\rangle\langle 0|\right)=\operatorname{Tr}\left(\Pi_{1}|0\rangle\langle 0|\right)=\frac{1}{2} \tan ^{2} \theta$, i.e. equiprobable for these two outcomes.

Thus, we have proven that the states $|0\rangle$ and $|1\rangle$ are the optimal states for Alice to use in her cheating strategy when Bob is monitoring the probabilities. She should send $|0\rangle$ with probability $x=\cos ^{2} \theta$ and $|1\rangle$ with probability $1-x=\sin ^{2} \theta$. Her cheating probability $A_{\text {pure } O T}^{q}$ is then

$$
A_{\text {pure } O T}^{q}=\max \left(1-p_{?}, \frac{1}{2}\left[1+p_{?}\right]\right)= \begin{cases}\cos ^{2} \theta & \text { for } \theta \leq \arcsin (1 / \sqrt{3})  \tag{6.20}\\ 2 \sin ^{2} \theta & \text { for } \theta \geq \arcsin (1 / \sqrt{3})\end{cases}
$$

Up to the intersection of the two cases in Eq. (6.20) at $\theta=\arcsin (1 / \sqrt{3}) \approx$ $35.264^{\circ}$, corresponding to $p_{\text {? }}=1 / 3$, Alice follows the strategy where she guesses that Bob has received no bit when $|0\rangle$ is sent, and after the intersection she follows the strategy where she guesses that he has received a bit when $|0\rangle$ is sent. At the intersection, she can, obviously, use both strategies and achieve the same cheating probability. When $|1\rangle$ is sent, Alice always guesses that Bob has received a bit.

For $\theta \geq \arcsin (1 / \sqrt{3})$, Alice's cheating probability is equal to her guessing probability. Using the cheating strategy does, however, give her the advantage that,
when she sends $|1\rangle$, she knows for sure that Bob has received a bit, even though she will not know which value it was. Alice can cheat perfectly when $\theta=0^{\circ}$ or $\theta=45^{\circ}$. These are the same values for $\theta$ as when she can guess perfectly. As explained earlier, the traditional definition of Rabin OT, where $p_{\text {? }}=1 / 2$ and Bob receives each of the bit values with equal probability, requires $\theta=30^{\circ}$. For this angle, $A_{\text {pure } O T}^{q}=3 / 4$, whereby Alice will need to send $|0\rangle 3 / 4$ of the time, guessing no bit, and $|1\rangle$ the rest of the time, guessing that Bob has received a bit.

## Bob testing - Checking the states

As seen above, the testing strategy of just monitoring the occurrence probabilities of the outcomes can restrict Alice's cheating probability when compared to Bob not doing any testing. We now check if it can be restricted further by adding another test. Apart from monitoring the occurrence probabilities, Bob can additionally also check the states that Alice sends him. This also requires the protocol to be implemented multiple rounds, consequently yielding an average cheating probability for Alice. In particular, Alice needs to transmit $N$ states to Bob, so that he can randomly choose a small fraction $F$, where $0<F \ll 1$, of the states to test and can proceed with the protocol using the remaining $N(1-F)$ states. Such a testing strategy was suggested by Amiri et al. [7] and we will refer to it plus the keeping track of the occurrence probabilities as the full testing scheme. For the fraction of states Bob chose to test, he will ask Alice to declare their identity and will then check this declaration by measuring the qubit in the appropriate basis. If any of his measurement outcomes do not agree with Alice's declaration, Bob will abort. Otherwise, Bob will continue the protocol with the remaining $N(1-F)$ states, discarding the ones he had used for testing. As was mentioned at the start of the chapter, this testing method requires classical communication between Alice and Bob and, therefore, forfeits the non-interactivity of the whole protocol to some extent.

Alice obviously wants her cheating to stay undetected, thus, she needs to send a state with which she can always pass Bob's test. Such a state is the superposition of the two states she would send when honest, entangled with a system she keeps on her side. Hence, Alice will send a state of the form

$$
\begin{equation*}
\left|\Psi_{\text {cheat }}\right\rangle=a|0\rangle_{A}\left|\psi_{0}\right\rangle+b|1\rangle_{A}\left|\psi_{1}\right\rangle, \tag{6.21}
\end{equation*}
$$

where $\left\{|0\rangle_{A},|1\rangle_{A}\right\}$ is an orthonormal basis for the system she keeps, $|a|^{2}+|b|^{2}=1$, and $a, b \in \mathbb{R}$. Without loss of generality, the parameters $a$ and $b$ can be chosen as real and positive since any phase factor can always be absorbed into the kets $|0\rangle_{A}$
and $|1\rangle_{A}$. When Alice measures her part of the system of $\left|\Psi_{\text {cheat }}\right\rangle$ in the $\left\{|0\rangle_{A},|1\rangle_{A}\right\}$ basis, she will always be able to declare a correct state when Bob tests.

Since Bob also monitors the occurrence probabilities and he expects to receive the bit values 0 and 1 with the same probability, it would seem to imply that we need $a=b$ in Eq. (6.21). It is, however, possible for Alice to alternate between sending two entangled states that are mirror images of each other, that is, two states where $a$ and $b$ are swapped. In this way, she can achieve equiprobability for the two bit values on average. Hence, it is sensible to look at a state of the more general form given in Eq. (6.21).

Alice guessing only whether Bob received a bit or not Bob's measurement on his part of $\left|\Psi_{\text {cheat }}\right\rangle$ will change Alice's system into one of two possible states, depending on whether he has received a bit or not. She will want to distinguish between these two states which are

$$
\rho_{\text {no bit }}=\left(\begin{array}{cc}
|a|^{2} & a b^{*}  \tag{6.22}\\
a^{*} b & |b|^{2}
\end{array}\right) \quad \text { and } \quad \rho_{\text {bit }}=\left(\begin{array}{cc}
|a|^{2} & 0 \\
0 & |b|^{2}
\end{array}\right)
$$

corresponding to Bob obtaining no bit and to Bob obtaining a bit, respectively. The first case occurs with probability $p_{\text {no bit }}=\cos (2 \theta)$ and the second with probability $p_{\text {bit }}=2 \sin ^{2} \theta$. For her optimal cheating strategy, Alice needs to distinguish between $\rho_{\text {no bit }}$ and $\rho_{\text {bit }}$ with a minimum-error discrimination measurement. Following an approach in Ref. [91], we calculate Alice's general cheating probability for this case.

The weighted difference $\left[\cos (2 \theta) \rho_{\text {no bit }}-2 \sin ^{2} \theta \rho_{\text {bit }}\right]$, using the fact that $|a|^{2}+$ $|b|^{2}=1$, has eigenvalues

$$
\begin{equation*}
\lambda_{ \pm}=\frac{1}{2}\left[\left(1-4 \sin ^{2} \theta\right) \pm \sqrt{\left(1-4 \sin ^{2} \theta\right)^{2}+16 \sin ^{2} \theta\left(1-3 \sin ^{2} \theta\right)|a b|^{2}}\right] \tag{6.23}
\end{equation*}
$$

Alice's cheating probability $A_{\text {pure } O T}^{q}$ is given by

$$
\begin{align*}
A_{\text {pure } O T}^{q} & =1-\frac{1}{2}\left(1-\sum_{k}\left|\lambda_{k}\right|\right) \\
= & \frac{1}{4}\left[2+\left|\left(1-4 \sin ^{2} \theta\right)+\sqrt{\left(1-4 \sin ^{2} \theta\right)^{2}+16 \sin ^{2} \theta\left(1-3 \sin ^{2} \theta\right)|a b|^{2}}\right|\right. \\
& \left.+\left|\left(1-4 \sin ^{2} \theta\right)-\sqrt{\left(1-4 \sin ^{2} \theta\right)^{2}+16 \sin ^{2} \theta\left(1-3 \sin ^{2} \theta\right)|a b|^{2}}\right|\right] \tag{6.24}
\end{align*}
$$

This can be further simplified by considering how the terms of the eigenvalues change for different values of $\theta$. Firstly, note that $1-4 \sin ^{2} \theta \geq 0$ when $\sin \theta \leq 1 / 2$, thus for $\theta \leq 30^{\circ}$. Similarly, $1-3 \sin ^{2} \theta \geq 0$ when $\sin \theta \leq 1 / \sqrt{3}$, thus for $\theta \leq$ $\arcsin (1 / \sqrt{3}) \approx 35.264^{\circ}$. Hence, we need to consider the three ranges $0^{\circ} \leq \theta \leq 30^{\circ}$, $30^{\circ} \leq \theta \leq \arcsin (1 / \sqrt{3})$, and $\arcsin (1 / \sqrt{3}) \leq \theta \leq 45^{\circ}$.

|  | $1-4 \sin ^{2} \theta$ | $\sqrt{\left(1-4 \sin ^{2} \theta\right)^{2}+16 \sin ^{2} \theta\left(1-3 \sin ^{2} \theta\right)\|a b\|^{2}}$ |
| :---: | :---: | :---: |
| $0^{\circ} \leq \theta \leq 30^{\circ}$ | $\geq 0$ | $\geq 0$ and $\geq\left\|1-4 \sin ^{2} \theta\right\|$ |
| $30^{\circ} \leq \theta \leq \arcsin (1 / \sqrt{3})$ | $\leq 0$ | $\geq 0$ and $\geq\left\|1-4 \sin ^{2} \theta\right\|$ |
| $\arcsin (1 / \sqrt{3}) \leq \theta \leq 45^{\circ}$ | $\leq 0$ | $\geq 0$ and $\leq\left\|1-4 \sin ^{2} \theta\right\|$ |

Assume $x, y \in \mathbb{R}$, whereby $y$ is always greater than zero while $x$ can also be negative. Wanting to simplify $|x+y|+|x-y|$, we will generally consider the three different combinations occurring in the table above.
(1) $x \geq 0, y \geq 0$, and $|x| \leq|y|: \quad|x+y|+|x-y|=x+y-(x-y)=2 y$
(2) $x \leq 0, y \geq 0$, and $|x| \leq|y|: \quad|x+y|+|x-y|=x+y-(x-y)=2 y$
(3) $x \leq 0, y \geq 0$, and $|x| \geq|y|: \quad|x+y|+|x-y|=-(x+y)-(x-y)=-2 x=2|x|$

Applying these simplifications, allows cancelling terms in Eq. (6.24). We notice that, for $\arcsin (1 / \sqrt{3}) \leq \theta \leq 45^{\circ}$, the values of $a$ and $b$ do not affect Alice's cheating probability. In particular, we obtain $A_{\text {pure } O T}^{q}=\frac{1}{2}\left(1+\left|1-4 \sin ^{2} \theta\right|\right)$ and, since $1-4 \sin ^{2} \theta \leq 0$ for this range, it simplifies further to $A_{\text {pure } O T}^{q}=\frac{1}{2}\left(1-1+4 \sin ^{2} \theta\right)=$ $2 \sin ^{2} \theta$. This is the same as Alice's guessing probability for this range of $\theta$. Therefore, Alice's cheating probability is

$$
\begin{align*}
& A_{\text {pure } O T}^{q}=\max \left(\frac{1}{2}\left[1+\sqrt{\left(1-2 p_{?}\right)^{2}-4 a^{2} b^{2}\left(1-p_{?}\right)\left(1-3 p_{?}\right)}\right], 1-p_{?}\right) \\
& = \begin{cases}\frac{1}{2}\left(1+\sqrt{\left(1-4 \sin ^{2} \theta\right)^{2}+16 \sin ^{2} \theta\left(1-3 \sin ^{2} \theta\right)|a b|^{2}}\right) & \text { for } \theta \leq \arcsin (1 / \sqrt{3}) \\
2 \sin ^{2} \theta & \text { for } \theta \geq \arcsin (1 / \sqrt{3}) .\end{cases} \tag{6.25}
\end{align*}
$$

Next, we want to determine the optimal choice for $a$ and $b$. As mentioned, the second case of Alice's cheating probability does not depend on $a$ or $b$, so it is possible to solely focus on the first case of Eq. (6.25). Alice wants to maximise her cheating probability, so she will want to maximise the term beneath the square root. All the terms beneath the square root are positive for $\theta \leq \arcsin (1 / \sqrt{3})$ and, considering $\theta$ as a fixed value, we need to maximise the product $16 \sin ^{2} \theta\left(1-3 \sin ^{2} \theta\right)|a b|^{2}$. It
reaches its maximum when $a^{2} b^{2}=a^{2}\left(1-a^{2}\right)$ is the largest, which happens for $a=1 / \sqrt{2}$. Hence, dishonest Alice's best choice is to pick $a=b=1 / \sqrt{2}$.

In this optimum case, Alice wants to distinguish between the pure state and the uniformly mixed state

$$
\rho_{\mathrm{no} \text { bit }}=\left(\begin{array}{ll}
1 / 2 & 1 / 2  \tag{6.26}\\
1 / 2 & 1 / 2
\end{array}\right)=|+\rangle\langle+| \quad \text { and } \quad \rho_{\mathrm{bit}}=\left(\begin{array}{cc}
1 / 2 & 0 \\
0 & 1 / 2
\end{array}\right)=\frac{1}{2} \mathbb{1} .
$$

Substituting $a=b=1 / \sqrt{2}$ into Eq. (6.25) gives Alice's optimal cheating probability when Bob is doing the full testing scheme.

$$
A_{\text {pure } O T}^{q}=\max \left(1-p_{?}, \frac{1}{2}\left[1+p_{?}\right]\right)= \begin{cases}\cos ^{2} \theta & \text { for } \theta \leq \arcsin (1 / \sqrt{3})  \tag{6.27}\\ 2 \sin ^{2} \theta & \text { for } \theta \geq \arcsin (1 / \sqrt{3})\end{cases}
$$

Once again Alice can cheat perfectly when $\theta=0^{\circ}$ or $\theta=45^{\circ}$. For these two values of $\theta$, either $p_{\text {no bit }}$ or $p_{\text {bit }}$ is equal to 0 and the other one equal to 1 . So, it is not surprising that Alice can cheat with probability 1 . When $\theta=30^{\circ}$, that is, $p_{\text {? }}=1 / 2$, we have $A_{O T}^{q}=3 / 4$. Alice's cheating probability is at its minimum with $A_{O T}^{q}=2 / 3$ when $\theta=\arcsin (1 / \sqrt{3})$ or $p_{?}=1 / 3$. Whenever $\theta \geq \arcsin (1 / \sqrt{3})$, Alice's cheating strategy has the same success as her guessing strategy. That is, Alice's cheating probability is equal to her guessing probability.

In general, comparing Eq. (6.20) to Eq. (6.27), we can conclude that Alice's cheating probability when Bob is monitoring the occurrence probabilities is exactly the same as when Bob is doing the full testing scheme (with the optimal values $a=b=1 / \sqrt{2})$.

This might at first seem surprising, but it can be explained by taking a closer look at Alice's cheating state $\left|\Psi_{\text {cheat }}\right\rangle$ and her cheating measurement, when Bob is doing the full testing. If it is not a testing round, Alice cheats by measuring her system of $\left|\Psi_{\text {cheat }}\right\rangle$ in the $\left\{|+\rangle_{A},|-\rangle_{A}\right\}$ basis. And indeed, when $a=b=1 / \sqrt{2}$, the states on Bob's side become $|0\rangle$ or $|1\rangle$, the same states dishonest Alice sends in her optimal cheating strategy when Bob is monitoring the occurrence probabilities. Thus, it does not help Bob to do the full testing and he can just monitor the probabilities which simplifies his testing process. Also Alice does not benefit from sending the (more complicated) entangled state, but can just choose the cheating strategy of sending the appropriate statistical mixture of the states $|0\rangle$ and $|1\rangle$.

We observed that, when dishonest Alice sends $|1\rangle$, she can be sure that Bob will receive a bit while being maximally uncertain about its value. On the other
hand, in the guessing strategy, Alice will always know for certain which value Bob's possible bit has, but cannot be sure if he has received the bit or not. There is no way for Alice to unambiguously know both, whether Bob has received the bit or not, and the bit's value. In her cheating strategy when Bob is doing the full testing, Alice can unambiguously learn the bit value when she measures her system in the $\left\{|0\rangle_{A},|1\rangle_{A}\right\}$ basis, hence collapsing her cheating state into one of the two states she would send when she is honest. Then again, when she measures her system in the
 above. If dishonest Alice wants to additionally also learn the bit value that Bob has received, she can also get these information with some probability but she needs to adjust her cheating strategy for this.

Alice guessing also Bob's bit values In this part, the slightly changed definition of a dishonest Alice is considered where we assume that dishonest Alice wants to not only learn if Bob has received the bit or not, but also wants to know what Bob's received bit value is. This situation will change her cheating strategy and cheating probability.

Going back to Alice sending the cheating state in Eq. (6.21), Bob's measurement on his part of $\left|\Psi_{\text {cheat }}\right\rangle$ will, in this case, change Alice's system into one of three possible states, depending on whether he has received the bit with value 0 , the bit with value 1 , or no bit. Alice will have to distinguish between

$$
\rho_{\text {no bit }}=\left(\begin{array}{cc}
|a|^{2} & a b^{*}  \tag{6.28}\\
a^{*} b & |b|^{2}
\end{array}\right), \quad \rho_{\text {bit } 0}=\left(\begin{array}{cc}
1 & 0 \\
0 & 0
\end{array}\right), \quad \rho_{\text {bit } 1}=\left(\begin{array}{ll}
0 & 0 \\
0 & 1
\end{array}\right)
$$

corresponding to Bob obtaining no bit, Bob obtaining the bit with value 0 , or the bit with value 1 , respectively. The corresponding probabilities are $\cos (2 \theta)$ for $\rho_{\text {no bit }}$, $2|a|^{2} \sin ^{2}(\theta)$ for $\rho_{\text {bit } 0}$, and $2|b|^{2} \sin ^{2}(\theta)$ for $\rho_{\text {bit } 1}$.

Finding the optimum minimum-error measurement to distinguish between the three general states in Eq. (6.28) is not straightforward. We can, however, bound Alice's cheating probability by assuming she performs a square-root measurement (SRM) [73]. This is not necessarily the optimum strategy for her. In fact, it turns out that for some values of $\theta$ and $a$ she can cheat successfully with a higher probability when using her guessing strategy. Nevertheless, the SRM is a valid strategy, not detectable by Bob, and will provide a lower bound. The lower bound on Alice's
cheating probability given by the SRM can be calculated as

$$
\begin{align*}
A_{\text {pure OT }}^{q} & \geq \frac{\left(1-p_{?}+2 p_{?}^{2}\right)\left(1+2 a b \sqrt{\frac{1-p_{?}}{1+p_{?}}}\right)+p_{?}\left(6 p_{?} a^{2} b^{2} \frac{1-p_{?}}{1+p_{?}}-1\right)}{1+2 a b \sqrt{1-p_{?}^{2}}} \\
& =\frac{\left[1-\cos (2 \theta)+2 \cos ^{2}(2 \theta)\right][1+2 a b \tan \theta]+\cos (2 \theta)\left[6 a^{2} b^{2} \tan ^{2} \theta \cos (2 \theta)-1\right]}{1+2 a b \sin (2 \theta)} . \tag{6.29}
\end{align*}
$$

To decide which choice for $a$ and $b$ is best for Alice, we will look at the partial derivative of the bound for $A_{\text {pure }}^{q}$ ОT. Substituting in $b^{2}=1-a^{2}$ and taking the partial derivative with respect to $a$, we obtain

$$
\begin{equation*}
\frac{\delta A_{\text {pure } O T}^{q}}{\delta a}=\frac{\left(1-2 a^{2}\right)\left[3 a \sqrt{1-a^{2}}+\left(1+3 a^{2}-3 a^{4}\right) \sin (2 \theta)\right][\tan \theta-\sec \theta \sin (3 \theta)]^{2}}{\sqrt{1-a^{2}}\left[1+2 a \sqrt{1-a^{2}} \sin (2 \theta)\right]^{2}} . \tag{6.30}
\end{equation*}
$$

When $a=1 / \sqrt{2},\left(1-2 a^{2}\right)=0$ for all $\theta$ and thus $\delta A_{\text {pure } \text { OT }^{q} / \delta a=0 \text {. It follows that }}$ the plot for the bound of $A_{\text {pure }}^{q}$ OT has an extremum at $a=1 / \sqrt{2}$. We can determine the nature of the extemum by looking at the plot in Figure 6.3 which illustrates the gradient for $A_{\text {pure } O T}^{q}$, i.e. $\delta A_{\text {pure } O T}^{q} / \delta a$. The extremum at $a=1 / \sqrt{2}$ is a maximum since $\delta A_{\text {pure } О T}^{q} / \delta a \geq 0$ for $a<1 / \sqrt{2}$ and $\delta A_{\text {pure } \text { OT }}^{q} / \delta a \leq 0$ for $a>1 / \sqrt{2}$. Hence, Alice's optimal choice for $a$ and $b$ is $a=b=1 / \sqrt{2}$.


Figure 6.3: The partial derivative of Alice's cheating probability with respect to $a$. The orange line at $a=1 / \sqrt{2}$ emphasizes the change of signs for the function $\delta A_{\text {pure } O T}^{q} / \delta a$ for the values of $a$ bigger or smaller than $1 / \sqrt{2}$.

For this optimal case, the three states in Eq. (6.28) become

$$
\begin{align*}
\rho_{\mathrm{no} \text { bit }} & =\left(\begin{array}{ll}
1 / 2 & 1 / 2 \\
1 / 2 & 1 / 2
\end{array}\right)=|+\rangle\langle+|, \\
\rho_{\mathrm{bit} 0} & =\left(\begin{array}{ll}
1 & 0 \\
0 & 0
\end{array}\right)=|0\rangle\langle 0|, \\
\rho_{\text {bit } 1} & =\left(\begin{array}{ll}
0 & 0 \\
0 & 1
\end{array}\right)=|1\rangle\langle 1|, \tag{6.31}
\end{align*}
$$

occurring with probabilities $\cos (2 \theta), \sin ^{2} \theta$, and $\sin ^{2} \theta$, respectively. We notice that the unitary operation $U$ for which $U|0\rangle=|1\rangle$ and $U|1\rangle=|0\rangle$, interchanges $\rho_{\text {bit } 0}$ and $\rho_{\text {bit } 1}$ while keeping $\rho_{\text {no bit }}$ unchanged. That is, the states in Eq. (6.31) are mirror-symmetric and we can obtain the optimal minimum-error measurement for them.

The states are those covered in the paper by Andersson et al. [77] rotated by the angle $\Theta=45^{\circ}$. Thus, the formulas derived there can be used to calculate Alice's cheating probability. We need to consider two different cases, depending on if $p$, defined as the the prior probability of the two mirror image states, is greater or smaller than

$$
\begin{equation*}
\frac{1}{2+\cos \Theta(\cos \Theta+\sin \Theta)}=\frac{1}{3} . \tag{6.32}
\end{equation*}
$$

For the states in Eq. (6.31), the prior probability of the two mirror image states $\rho_{\text {bit } 0}$ and $\rho_{\text {bit } 1}$ is $\sin ^{2} \theta$, thus $p=\sin ^{2} \theta$. This means that the two cases to consider will depend on the angle $\theta$. If $\sin ^{2} \theta=1 / 3$, then $\theta=\arcsin (1 / \sqrt{3}) \approx 35.264^{\circ}$ and Alice's cheating probability is

$$
A_{\text {pure } O T}^{q}=\max \left(1-p_{?}, \frac{4 p_{?}^{2}}{5 p_{?}-1}\right)= \begin{cases}\frac{4 \cos ^{2}(2 \theta)}{5 \cos (2 \theta)-1} & \text { for } \theta \leq \arcsin (1 / \sqrt{3})  \tag{6.33}\\ 2 \sin ^{2} \theta & \text { for } \theta \geq \arcsin (1 / \sqrt{3})\end{cases}
$$

As before, Alice can cheat perfectly when $\theta=0^{\circ}$ or $\theta=45^{\circ}$. When $p_{\text {? }}=2 / 5$, corresponding to $\theta=\frac{1}{2} \arccos (2 / 5) \approx 33.211^{\circ}$, Alice's cheating probability is at its minimum with $A_{\text {pure } O T}^{q}=16 / 25=0.64$. We get $A_{\text {pure } O T}^{q}=2 / 3$ when $\theta=30^{\circ}$ or $\theta=$ $\arcsin (1 / \sqrt{3})$. Alice's cheating probability coincides with her guessing probability whenever $\theta \geq 35.264^{\circ}$ or $p_{\text {? }} \leq 1 / 3$. From this angle onwards, it also coincides with her cheating probability in the standard cheating scenario.

For the special case, where $a=1$ and $b=0$, the states become $\rho_{\text {no bit }}=|0\rangle\langle 0|$,
$\rho_{\text {bit } 0}=|0\rangle\langle 0|$, and $\rho_{\text {bit } 1}=|1\rangle\langle 1|$ with prior probabilities $\cos (2 \theta), 2 \sin ^{2} \theta$, and 0 . I.e. Alice can know that Bob never gets the second bit and has to choose between no bit and the first bit depending on $\theta$ since the two states are the same and she cannot directly distinguish between them. Similarly, for the special case, where $a=0$ and $b=1$, the states become $\rho_{\text {no bit }}=|1\rangle\langle 1|, \rho_{\text {bit } 0}=|0\rangle\langle 0|$, and $\rho_{\text {bit } 1}=|1\rangle\langle 1|$ with prior probabilities $\cos (2 \theta), 0$, and $2 \sin ^{2} \theta$. I.e. Alice can know that Bob never gets the first bit and has to choose between no bit and the second bit depending on $\theta$ since the two states are the same and she cannot directly distinguish between them.

These two special cases, where $a$ and $b$ are equal to 0 and 1 and vice versa are the same for when Alice only wants to distinguish between Bob getting a bit and him not getting a bit; she will know the bit value for sure if Bob receives it. In other words, these cases are equivalent to the guessing scenario.


Figure 6.4: Alice's guessing and cheating probabilities as functions of the angle $\theta$ (subfigure (a)) and as functions of $p_{\text {? }}$ (subfigure (b)). Her guessing probability $A_{\text {pure } O T}^{g}$ is plotted as the solid line. The dashed line shows her cheating probability when Bob monitors the probabilities or when Bob does the full testing scheme (for the optimal case where $a=b=1 / \sqrt{2}$ ). When Bob does not do any testing, Alice's cheating probability is shown by the dotted-dashed line. Alice's cheating probability in the special case, where Bob does the full testing and Alice wants to not only distinguish between bit and no bit but also the bit's values, is plotted by the dotted line (for the optimal case where $a=b=1 / \sqrt{2}$ ).

Alice's guessing probability and her different cheating strategies discussed in this section are plotted in Figure 6.4 as functions of the angle $\theta$ and as functions of $p_{\text {? }}$. For any kind of testing from Bob and an angle of $\theta \geq \arcsin (1 / \sqrt{3}) \approx 35.264^{\circ}$, Alice's cheating probabilities are the same as her guessing probability. In the cheating strategies, however, Alice might have some additional knowledge; e.g. when Bob is monitoring the occurrence probabilities and Alice sends $|1\rangle$, she can be sure that Bob has received a bit value. Comparing the graph where Bob does the full testing and dishonest Alice cheats with the standard cheating definition to the graph where Bob does the full testing and dishonest Alice also wants to know which bit value

Bob obtained when he has received a bit, shows, as expected, that it is harder for Alice to cheat in the latter case; at least up to $\theta=\arcsin (1 / \sqrt{3})$, i.e. $p_{\text {? }}=1 / 3$.

Alice's cheating probability for the special case where she also wants to know the bit value is based on the optimal values for $a$ and $b$ derived from the lower bound given by the SRM. Hence, even though we have the optimum minimumerror measurement for the states when $a=b=1 / \sqrt{2}$, we cannot say for sure if these values are the best among all possible values of $a$ and $b$ when looking at all the optimum minimum-error measurements to distinguish between the states in Eq. (6.28). Thus, the cheating probability and corresponding graph for this special case can only be considered as a lower bound.

### 6.2.4 Comparison to Classical Rabin OT

To evaluate the performance of the quantum Rabin OT protocol, we compare it to a classical Rabin OT protocol obtained by probabilistically choosing between two simple classical protocols. The probabilistic distribution of the two protocols is established by a weak coin flip as in a procedure in Ref. [47], that is, the outcome of the coin flip determines which of the two simple classical protocols is implemented. These two protocols are defined as follows.

Protocol 1: Alice holds a bit which is equally likely to have value 0 or 1 . She sends the bit to Bob with probability $1-p_{\text {? }}$ and otherwise does not send anything. Afterwards she "forgets" what she has done and does not keep a record to track her action.

Protocol 2: Alice holds a bit which is equally likely to have value 0 or 1 . She sends the bit to Bob who chooses to read it with probability $1-p_{\text {? }}$ and discards it unread the rest of the time.

Obviously, in these protocols, one of the two parties can always cheat perfectly without being detected, while the other one can cheat no better than with a random guess. In particular, in Protocol 1, a dishonest Alice can cheat with probability 1, whereas a dishonest Bob can only cheat with the guessing probability $B_{O T}^{g}=1-p_{?} / 2$ and, in Protocol 2, a dishonest Bob can cheat with probability 1, whereas a dishonest Alice can only cheat with the guessing probability $A_{O T}^{g}=\max \left(p_{?}, 1-p_{?}\right)$.

We define a third protocol, which is a probabilistic mixture of the other two protocols specified by a weak coin flip as described earlier.

Protocol 3: Protocol 1 is executed with probability $y$, and Protocol 2 is executed with probability $(1-y)$.

The probability for Bob to receive the bit in Protocol 3 is then also equal to $1-p_{\text {? }}$. Protocol 3 is a combination of Protocol 1 and Protocol 2, hence, its cheating probabilities can be calculated by combining the cheating probabilities of Protocol 1 and Protocol 2. In particular, Alice's and Bob's cheating probabilities for Protocol 3 are

$$
\begin{align*}
& A_{O T}^{c}= \begin{cases}1-p_{?}+y p_{?} & \text { for } p_{?} \leq 1 / 2 \\
p_{?}+y\left(1-p_{?}\right) & \text { for } p_{?}>1 / 2,\end{cases}  \tag{6.34}\\
& B_{O T}^{c}=1-\frac{y p_{?}}{2} . \tag{6.35}
\end{align*}
$$

There is a trade-off relationship between Alice's and Bob's cheating probabilities and the specific relation can be specified by considering $s A_{O T}+t B_{O T}$, where the constants $s$ and $t$ are chosen such that $y$ is eliminated from the equation. The trade-off relations are

$$
\begin{array}{ll}
f_{1}\left(A_{O T}^{c}, B_{O T}^{c}\right)=A_{O T}^{c}+2 B_{O T}^{c}=3-p_{?} & \text { for } p_{?} \leq 1 / 2 \\
f_{2}\left(A_{O T}^{c}, B_{O T}^{c}\right)=p_{?} A_{O T}^{c}+2\left(1-p_{?}\right) B_{O T}^{c}=\left(1-p_{?}\right)^{2}+1 & \text { for } p_{?}>1 / 2 \tag{6.36}
\end{array}
$$

To compare with a quantum protocol, we need to calculate the relation $s A_{O T}+$ $t B_{O T}$ in terms of $p_{\text {? }}$ using the quantum cheating probabilities and the same values for $s$ and $t$. Whenever the resulting expression in terms of $p_{\text {? }}$ is smaller for the quantum than for the classical case, we can conclude that the quantum protocol is better; vice versa is true if the expression is smaller for the classical than for the quantum case. Using Alice's cheating probability for the traditional situation where she only wants to know if Bob has obtained a bit or not, the trade-off relations for the quantum Rabin OT protocol based on pure states are

$$
\begin{align*}
& f_{1}\left(A_{\text {pure } O T}^{q}, B_{\text {pure } O T}^{q}\right)= \begin{cases}2-p_{?}+\sqrt{1-p_{?}^{2}} & \text { for } p_{?} \leq 1 / 3 \\
\frac{1}{2}\left(3+p_{?}\right)+\sqrt{1-p_{?}^{2}} & \text { for } 1 / 3<p_{?} \leq 1 / 2,\end{cases} \\
& f_{2}\left(A_{\text {pure OT }}^{q}, B_{\text {pure OT }}^{q}\right)=1-\left(1-p_{?}\right)\left(\frac{1}{2} p_{?}-\sqrt{1-p_{?}^{2}}\right) \quad \text { for } p_{?}>1 / 2 \tag{6.37}
\end{align*}
$$

We can now compare the trade-off relations of the quantum and classical case to see which one is lower. However, in order to better judge the difference between the classical and quantum expressions, it is sensible to subtract from them the expressions for the trade-off relations of the guessing probabilities. Alice's and Bob's guessing probabilities are baselines and the same for both the classical and quantum protocol. Hence, it is essentially the difference between the cheating and guessing probabilities that will differentiate whether the classical or quantum protocol is more secure. This advantage, i.e. the additional probability of success, of the cheating strategies over the guessing strategies can be investigated by looking at the difference between the trade-off relations for the classical/quantum cheating probabilities and the trade-off relation for the guessing probabilities. Calculating $f_{1}\left(A_{O T}^{g}, B_{O T}^{g}\right)$ and $f_{2}\left(A_{O T}^{g}, B_{O T}^{g}\right)$ for the guessing probabilities, we obtain

$$
\begin{array}{ll}
f_{1}\left(A_{O T}^{g}, B_{O T}^{g}\right)=3-2 p_{?} & \text { for } p_{?} \leq 1 / 2 \\
f_{2}\left(A_{O T}^{g}, B_{O T}^{g}\right)=2+2 p_{?}^{2}-3 p_{?} & \text { for } p_{?}>1 / 2 \tag{6.38}
\end{array}
$$

In Figure 6.5, the difference $f_{i}\left(A_{O T}^{c}, B_{O T}^{c}\right)-f_{i}\left(A_{O T}^{g}, B_{O T}^{g}\right)$ is plotted as the dotted line and the difference $f_{i}\left(A_{\text {pure } O T}^{q}, B_{\text {pure } O T}^{c}\right)-f_{i}\left(A_{O T}^{g}, B_{O T}^{g}\right)$ as the solid line; for $i \in$ $\{1,2\}$ and with respect to $p_{\text {? }}$. In order to display continuous graphs, we multiplied the trade-off relations $f_{2}$ by a factor of 2 . Since this same operation was done for all, the classical, quantum, and guessing expressions of $f_{2}$, it does not affect the ratio between them.

The two graphs intersect at four points over the range of $0 \leq p_{\text {? }} \leq 1$. For $0<$ $p_{?}<5 / 13 \approx 0.385$ and $4 / 5<p_{\text {? }}<1$, the curve for the quantum protocol lies below the curve for the classical protocol, thus, the quantum protocol outperforms the classical protocol in these regions. That is, the advantage of the cheating strategies over the guessing strategies is smaller for the quantum protocol making it more secure than the classical protocol. In the area in between these regions, the curve for the classical protocol lies below the curve for the quantum protocol, so the classical protocol is better than the quantum protocol for $5 / 13<p_{?}<4 / 5$. That is, the advantage of the cheating strategies over the guessing strategies is larger for the quantum protocol making it less secure than the classical protocol.


Figure 6.5: Trade-off relations with respect to $p_{\text {? }}$ of the classical protocol (dotted) and the quantum protocol based on pure states (solid) after subtraction of the relations for the guessing probabilities.

To further investigate the relation between the classical and quantum cheating probabilities, we can examine how the values for $y$, the probability of executing Protocol 1, affect Alice's and Bob's cheating probabilities. Plotting the expressions for the classical and quantum cheating probabilities in the 3D plane with $\theta$ and $y$ on the $x$-axis and $y$-axis, results in the planes intersecting each other in a line. This line describes where the classical and quantum cheating probabilities are equal to each other. Deriving an expression for this line in terms of $\theta$ will yield the $y$ values for which the cheating probabilities are the same.

At first, we consider a dishonest Alice, looking at the traditional definition of a cheating Alice, i.e. when she only wants to know if Bob has received the bit or not, and when Bob is testing. The equality $A_{\mathrm{pure} ~}^{q} O T^{q}=A_{O T}^{c}$, where $A_{\mathrm{pure} ~}^{\text {OT }} \boldsymbol{q}$ is given in Eq. (6.20) and $A_{O T}^{c}$ is given in Eq. (6.34) with $p_{\text {? }}=\cos (2 \theta)$ substituted in, is rearranged to give the following values for $y$ depending on $\theta$.

$$
y= \begin{cases}1 / 2 & \text { for } 0^{\circ} \leq \theta \leq 30^{\circ}  \tag{6.39}\\ {[3-\sec (2 \theta)] / 2} & \text { for } 30^{\circ}<\theta \leq \arcsin (1 / \sqrt{3}) \\ 0 & \text { for } \arcsin (1 / \sqrt{3})<\theta \leq 45^{\circ}\end{cases}
$$

When, for a given $\theta, y$ is larger than the value given by Eq. (6.39), then Alice's classical cheating probability increases above the quantum one. This is obvious because, when $y$ becomes larger, Protocol 1, where Alice can cheat perfectly, is implemented more often, which entails that Alice's classical cheating probability
given in Eq. (6.34) increases. In such a case, the quantum protocol is then better than the classical protocol with regards to a dishonest Alice.

Looking at a dishonest Bob, the equality $B_{\mathrm{pure} O T}^{q}=B_{O T}^{c}$, where $B_{\mathrm{pure} O T}^{q}$ is given in Eq. (6.4) and $B_{O T}^{c}$ is given in Eq. (6.35) with $p_{\text {? }}=\cos (2 \theta)$ substituted in, is rearranged to give the function $y=\sec (2 \theta)-\tan (2 \theta)$. When, for a given $\theta, y$ is smaller than the value given by this function for $y$ in terms of $\theta$, then Bob's classical cheating probability increases above the quantum one. This is obvious because, when $y$ becomes smaller, Protocol 2, where Bob can cheat perfectly, is implemented more often, which entails that Bob's classical cheating probability given in Eq. (6.35) increases. In such a case, the quantum protocol is then better than the classical protocol with regards to a dishonest Bob.


Figure 6.6: Values for $y$ depending on $\theta$ for which Alice's (solid line) and Bob's (dashed line) cheating probabilities coincide in the classical and quantum protocols. The areas for comparison between the classical and quantum protocols are coloured differently and are described in the legend on the right hand side.

Plotting the graphs for the values of $y$ as functions of $\theta$ in Figure 6.6, gives areas where either just one or both or neither of the parties have lower, i.e. better, cheating probabilities in the quantum protocol than in the classical protocol. In particular, Bob's function for $y$ is plotted by the dashed line and, for each $\theta$, any value of $y$ below this dashed line results in Bob's quantum cheating probability being lower than his classical cheating probability. Alice's function for $y$ is plotted by the solid line and, for each $\theta$, any value of $y$ above this solid line results in Alice's quantum cheating probability being lower than her classical cheating probability. The green areas show which values for $y$ yield a better quantum cheating probability for both Alice and Bob for a given $\theta$. On the other hand, the combinations of $y$ and $\theta$ values that lie within the red area, are the value combinations for which neither Alice's nor Bob's quantum cheating probability is lower than their respective classical one. This area
lies in the range of $\arctan (1 / 3) \approx 18.425^{\circ} \leq \theta \leq \arctan (2 / 3) \approx 33.690^{\circ}$, in terms of $p_{\text {? }}$ that is $5 / 13 \approx 0.385 \leq p_{\text {? }} \leq 4 / 5$. The range for $p_{\text {? }}$ matches the one in Figure 6.5 , where the classical protocol is better than the quantum protocol. For the other values of $\theta$, where, depending on the value of $y$, at least one if not even both parties have a lower quantum than classical cheating probability, these match the ranges in Figure 6.5, where the quantum protocol outperforms the classical protocol.

### 6.3 Rabin OT Using Mixed States

In the previous section, we have seen that quantum Rabin oblivious transfer protocols using pure states are not necessarily better than classical Rabin oblivious transfer protocols. Hence, the question arises if mixed states can help improve the performance of the quantum protocols. In this section, we look at a quantum Rabin oblivious transfer protocol that makes use of mixed quantum states.

Even though the below protocol is defined as a quantum protocol with quantum states, it can theoretically be implemented using only classical means. As we will see, the used mixed states and operators only have diagonal elements, so they essentially represent classical mixtures of states. Nevertheless, it is a valid quantum Rabin OT protocol using mixed states that can be used to compare to the protocol using pure states.

Furthermore, it will provide us with another benchmark for the performance of classical Rabin OT protocols. So far, the classical Rabin OT protocols considered are based on coin flips which entails that, when the coin flip "chooses" Protocol 2 to be implemented, both parties know that Alice definitely has to send something. Hence, this does not include protocols where Bob is always uncertain if Alice has sent something. By the introduction of the statistical distribution in the parties' actions, we can consider classical Rabin OT protocols where Alice sends the bit with some probability and Bob reads it with some probability.

### 6.3.1 The Protocol

Honest Alice encodes her bit value $v \in\{0,1\}$ in a respective mixed state $\rho_{v}$. The two mixed states share a part of their ensemble and are orthogonal in the other part of their ensemble, so that honest Bob's measurement sometimes results in an inconclusive outcome, i.e. him not learning the bit value, and sometimes results in an unambiguous outcome, i.e. him learning the bit value with certainty. The Rabin OT protocol is then carried out as follows.

1. Alice randomly chooses one of the two mixed states $(0 \leq r \leq 1)$

$$
\begin{equation*}
\rho_{0}=(1-r)|0\rangle\langle 0|+r|1\rangle\langle 1|, \quad \rho_{1}=(1-r)|0\rangle\langle 0|+r|2\rangle\langle 2|, \tag{6.40}
\end{equation*}
$$

with a probability of $1 / 2$ each, and sends it to Bob.
2. Bob performs an unambiguous discrimination measurement on the received state. His measurement operators are $(0 \leq r \leq 1)$

$$
\begin{align*}
& \Pi_{?}=|0\rangle\langle 0|+(1-r)|1\rangle\langle 1|+(1-r)|2\rangle\langle 2|, \\
& \Pi_{0}=r|1\rangle\langle 1|, \\
& \Pi_{1}=r|2\rangle\langle 2| . \tag{6.41}
\end{align*}
$$

The constant $r$ is included for randomisation. In Alice's states in Eq. (6.40), r specifies the probabilistic mixture of the pure states in the mixed states' ensembles and influences if Bob is more likely to obtain the bit ( $r>1 / 2$ ) or not ( $r<1 / 2$ ). Including $r$ in the measurement operators in Eq. (6.41), further randomises Bob's outcome from Alice's perspective, since the probabilities for Bob obtaining the bit or not depend on $r$. In particular, these probabilities can be calculated to be

$$
\begin{align*}
P(\text { no bit }) & =\frac{1}{2}\left[\operatorname{Tr}\left(\Pi_{?} \rho_{0}\right)+\operatorname{Tr}\left(\Pi_{?} \rho_{1}\right)\right]=1-r^{2} \\
P(\text { bit }) & =\frac{1}{2}\left[\operatorname{Tr}\left(\Pi_{0} \rho_{0}\right)+\operatorname{Tr}\left(\Pi_{1} \rho_{1}\right)\right]=r^{2} \tag{6.42}
\end{align*}
$$

As before, the probability of Bob not obtaining the bit, i.e. him getting an inconclusive result, is $p_{\text {? }}$ and here $p_{\text {? }}=P($ no bit $)=1-r^{2}$.

The random factors in the states and in the measurement operators do not necessarily have to be the same factor $r$, but they could be represented by two distinct ones. To better compare the protocol here to the Rabin OT protocol with pure states in Section 6.2, only one free variable is considered. Whereas the free variable here is the constant $r$, the free variable in the pure state protocol is the angle $\theta$. Both these variables have an impact on $p_{\text {? }}$ which will be the common variable with respect to which we will compare the protocols. Another option would have been to only add randomness to either the states or the measurement operators. However, choosing, for example $r=1 / 2$, for either the states or the measurement operators, would narrow the range of $p_{\text {? }}$. In particular, when $r=1 / 2$ in either Eq. (6.40) or Eq. (6.41), then $p_{\text {? }}=P($ no bit $)=1-\frac{1}{2} r$ and, since $0 \leq r \leq 1$ holds, $1 / 2 \leq p_{\text {? }} \leq 1$. For other values of $r$ this would be similar, but wanting to consider
the whole range of $p_{\text {? }}$ for the comparison we decided to add randomness to both the states and measurement operators.

### 6.3.2 Dishonest Bob

A dishonest Bob always wants to know which bit Alice has sent. As per definition, it is equally likely that honest Alice sends the bit with value 0 and the bit with value 1. This is also the best thing to do as it maximises Bob's uncertainty about which value the bit has and, hence, minimises his probability of correctly guessing the value in the case where he does not receive the bit.

As in Section 6.2, we first look at Bob's guessing strategy, that is, the cheating strategy where Bob follows the protocol honestly and then randomly guesses the bit value whenever he obtains an inconclusive result. Bob learns the bit value with probability $P$ (bit) and, when he does not obtain the bit, he can guess its value correctly with a probability of $1 / 2$. Thus, Bob's guessing probability $B_{\text {mixed } O T}^{g}$ is

$$
\begin{equation*}
B_{\text {mixed } O T}^{g}=P(\mathrm{bit}) \times 1+P(\text { no bit }) \times \frac{1}{2}=1-\frac{1}{2} p_{?}=\frac{1}{2}+\frac{1}{2} r^{2} . \tag{6.43}
\end{equation*}
$$

When dishonest Bob does not follow the protocol honestly, but applies a different measurement than he is supposed to, he can increase his cheating probability. His aim is to minimise the error of distinguishing between $\rho_{0}$ and $\rho_{1}$, thus his optimal cheating strategy is to apply a minimum-error measurement on the states. The eigenvalues $\lambda_{k}$ of $\frac{1}{2}\left(\rho_{1}-\rho_{0}\right)$ are $(0,-r / 2, r / 2)$, thus, Bob's cheating probability $B_{\text {mixed } O T}^{q}$ is [80]

$$
\begin{equation*}
B_{\text {mixed } O T}^{q}=1-\left[\frac{1}{2}\left(1-\sum_{k}\left|\lambda_{k}\right|\right)\right]=\frac{1}{2}\left(1+\sqrt{1-p_{?}}\right)=\frac{1}{2}+\frac{r}{2} . \tag{6.44}
\end{equation*}
$$

In Figure 6.7, we plot Bob's cheating and guessing probability, once in terms of $r$ and once in terms of $p_{?}$. His guessing and cheating probabilities intersect at $r=0$ and $r=1$. Everywhere else, his cheating strategy is always more successful. When $r=0$, then $p_{\text {? }}=1$ and $\rho_{0}=\rho_{1}$ meaning that Bob never gets the bit and he can only cheat with a random guess, $B_{\text {mixed } O T}^{q}=1 / 2=B_{\text {mixed } O T}^{g}$. For $r=1$, that is $p_{\text {? }}=0$, Bob can cheat perfectly $B_{\text {mixed } O T}^{q}=1=B_{\text {mixed } O T}^{g}$ because the states in Eq. (6.40) are orthogonal and, even when he follows the protocol honestly, he will always receive the bit value. In the traditional Rabin OT task where $p_{\text {? }}=1 / 2$, we have $B_{\text {mixed } O T}^{q}=\frac{1}{2}(1+1 / \sqrt{2}) \approx 0.855$ while $B_{\text {mixed } O T}^{g}=3 / 4$.


Figure 6.7: Bob's guessing and cheating probability as functions of $r$ (subfigure (a)) and as functions of $p_{\text {? }}$ (subfigure (b)). His guessing probability $B_{\text {mixed } O T}^{g}$ is plotted as the solid line and his cheating probability $B_{\text {mixed } O T}^{q}$ as the dashed line.

### 6.3.3 Dishonest Alice

A dishonest Alice wants to know if Bob has received the bit or not. Similarly as for Bob, Alice can apply a guessing strategy in which she will follow the protocol honestly and then guess the more likely outcome on Bob's side, that is, will he receive the bit or will he receive nothing with a higher probability. Hence, her guessing probability $A_{\text {mixed } O T}^{g}$ is given by the bigger of the probabilities in Eq. (6.42), in particular,

$$
A_{\text {mixed } O T}^{g}=\max \left(1-p_{?}, p_{?}\right)= \begin{cases}1-r^{2} & \text { for } r \leq 1 / \sqrt{2}  \tag{6.45}\\ r^{2} & \text { for } r>1 / \sqrt{2}\end{cases}
$$

In the case where Alice guesses that Bob has received the bit, she knows what value it has since she followed the protocol and knows what state she has sent. The guessing strategy can usually be outperformed by cheating strategies where Alice does not follow the protocol honestly. As in previous protocols where we considered a dishonest sender, we look at two of different situations: one with testing by Bob and one without testing by Bob. We compare the resulting cheating probabilities with each other and also with Alice's guessing probability which is the baseline. All of these probabilities are plotted in Figure 6.8.

## No testing by Bob

When Bob does not test, dishonest Alice can cheat perfectly in this protocol. That is, because both of Bob's measurement operators for the bit, i.e. $\Pi_{0}$ for the bit of value 0 and $\Pi_{1}$ for the bit of value 1 , are orthogonal to $|0\rangle$. So, by sending $|0\rangle$, she will always know that Bob has not received a bit. Thus, in the case of no testing by

Bob, Alice can cheat with probability $1, A_{\text {mixed } O T}^{q}=1$.
Furthermore, if $r$ equals 0 or 1, Alice has even more states that she could send to Bob to learn his outcome perfectly. If $r=0$, Bob will always receive no bit since $p_{\text {? }}=1$. This value for $r$ means that Alice's states are equal, $\rho_{0}=\rho_{1}$, and Bob's measurement operators $\Pi_{0}=0$ and $\Pi_{1}=0$. On the other hand, if $r=1$, Bob will always receive the bit since $p_{\text {? }}=0$. Alice's states are then orthogonal and so are Bob's measurement operators. Hence, by sending any of the states $|0\rangle,|1\rangle$, or $|2\rangle$ when $r=0$ or $r=1$, Alice knows Bob's outcome perfectly to the point of also being able to tell what value the bit has whenever he obtains the bit $(r=1)$. These values for $r$ are thus not sensible to pick for this Rabin OT protocol.

## Bob testing - Monitoring the occurrence probabilities

A testing strategy that Bob can apply is to monitor the occurrence probabilities and check if the probabilities of receiving the bit with value 0 , the bit with value 1 , or no bit are what he expects them to be. Bob will not discard any states nor will he need any more information from Alice, so this testing procedure will not affect the non-interactivity of the overall protocol. However, in order to implement this testing scheme, the protocol needs to be repeated many times and the cheating probability obtained is an average cheating probability.

For dishonest Alice to maximise the probability of Bob getting a particular outcome, it is best for her to send him the pure state which is the eigenstate corresponding to the highest eigenvalue of Bob's measurement operator for this particular outcome. His measurement operator $\Pi_{\text {? }}$ has eigenvalues $(1,1-r, 1-r)$ with corresponding eigenvectors $(|0\rangle,|1\rangle,|2\rangle)$, respectively, and his measurement operator $\Pi_{\mathrm{bit}}=\Pi_{0}+\Pi_{1}$ has eigenvalues $(r, r, 0)$ with corresponding eigenvectors $(|1\rangle,|2\rangle,|0\rangle)$, respectively. Therefore, Alice needs to send an appropriate statistical mixture, which meets Bob's expected outcome probabilities, of the states $|0\rangle,|1\rangle$, and $|2\rangle$.

Alice knows that Bob expects $P($ no bit $)=1-r^{2}=p_{\text {? }}$ and $P($ bit $)=r^{2}=1-p_{\text {? }}$. She will need to send $|1\rangle$ and $|2\rangle$ with equal probability to ensure Bob gets the bit with value 0 and the bit with value 1 equally often. Thus, she sends $|0\rangle$ with probability $x$ and $|1\rangle$ and $|2\rangle$ with probability $\frac{1}{2}(1-x)$ each. Bob's measurement outcome probabilities are

$$
\begin{equation*}
x \operatorname{Tr}\left(\Pi_{?}|0\rangle\langle 0|\right)+\frac{1}{2}(1-x)\left(\operatorname{Tr}\left(\Pi_{?}|1\rangle\langle 1|\right)+\operatorname{Tr}\left(\Pi_{?}|2\rangle\langle 2|\right)\right)=x+(1-x)(1-r) \tag{6.46}
\end{equation*}
$$

for receiving no bit and

$$
\begin{equation*}
x \operatorname{Tr}\left(\Pi_{\mathrm{bit}}|0\rangle\langle 0|\right)+\frac{1}{2}(1-x)\left(\operatorname{Tr}\left(\Pi_{\mathrm{bit}}|1\rangle\langle 1|\right)+\operatorname{Tr}\left(\Pi_{\mathrm{bit}}|2\rangle\langle 2|\right)\right)=(1-x) r \tag{6.47}
\end{equation*}
$$

for receiving the bit. In order to meet Bob's expected probabilities, $(1-x) r=r^{2}$ has to hold. Thus, we need $x=1-r$. Noting that $\operatorname{Tr}\left(\Pi_{?}|1\rangle\langle 1|\right) \geq \operatorname{Tr}\left(\Pi_{\mathrm{bit}}|1\rangle\langle 1|\right)$ and $\operatorname{Tr}\left(\Pi_{?}|2\rangle\langle 2|\right) \geq \operatorname{Tr}\left(\Pi_{\text {bit }}|2\rangle\langle 2|\right)$ for $r \leq 1 / 2$, Alice will, for $0 \leq r \leq 1 / 2$, guess that Bob did not receive the bit even when sending state $|1\rangle$ or $|2\rangle$. Her cheating probability $A_{\text {mixed } O T}^{q}$, given by the probability of correctly guessing if Bob did receive the bit or not, is

$$
A_{\text {mixed OT }}^{q}=\max \left(2-\sqrt{1-p_{?}}-p_{?}, p_{?}\right)= \begin{cases}1-r^{2} & \text { for } r \leq 1 / 2  \tag{6.48}\\ 1-r+r^{2} & \text { for } r>1 / 2\end{cases}
$$

Figure 6.8 shows the plots for Alice's guessing probability and for her cheating probability with and without testing by Bob. Alice's cheating probability when Bob is testing, is equal to her guessing probability for $p_{\text {? }} \geq 3 / 4$ and $r \leq 1 / 2$. In the cheating strategy, she might have some additional knowledge since, when she sends $|0\rangle$, she knows for sure that Bob did not receive the bit while in the guessing strategy it is just the more likely guess. At these points where $p_{\text {? }}=3 / 4$ or $r=1 / 2$, Alice's cheating probability also reaches its minimum for both the expressions in terms of $r$ and of $p_{\text {? }}$, in particular, $A_{\text {mixed } O T}^{q}=3 / 4$ there. For the traditional value $p_{\text {? }}=1 / 2$, $A_{\text {mixed } O T}^{q}=\frac{1}{2}(3-\sqrt{2}) \approx 0.793$ whereas $A_{\text {mixed } \text { OT }}^{g}=1 / 2$.


Figure 6.8: Alice's guessing and cheating probabilities as functions of $r$ (subfigure (a)) and as functions of $p_{\text {? }}$ (subfigure (b)). Her guessing probability $A_{\text {mixed } O T^{g} \text { is }}$ plotted as the solid line. The dashed line shows her cheating probability when Bob monitors the probabilities. When Bob does not do any testing, Alice's cheating probability is shown by the dotted-dashed line.

### 6.3.4 Comparison to Classical Rabin OT

We want to compare this quantum Rabin OT protocol based on mixed states with the classical protocol considered in Subsection 6.2.4. The classical protocol which is a statistical mixture of two trivial classical protocols and has cheating probabilities $A_{O T}^{c}$ and $B_{O T}^{c}$ given in Eqns. (6.34) and (6.35), respectively, has trade-off relations $f_{1}\left(A_{O T}^{c}, B_{O T}^{c}\right)=A_{O T}^{c}+2 B_{O T}^{c}$ and $f_{2}\left(A_{O T}^{c}, B_{O T}^{c}\right)=p_{?} A_{O T}^{c}+2\left(1-p_{?}\right) B_{O T}^{c}$ as was presented in Eq. (6.36). For the mixed states protocol, $f_{1}\left(A_{\text {mixed } O T}^{q}, B_{\text {mixed } O T}^{q}\right)$ and $f_{2}\left(A_{\text {mixed } O T}^{q}, B_{\text {mixed OT }}^{q}\right)$ can be calculated to be
$f_{1}\left(A_{\text {mixed } O T}^{q}, B_{\text {mixed } O T}^{q}\right)=3-p_{\text {? }} \quad$ for $p_{\text {? }} \leq 1 / 2$,
$f_{2}\left(A_{\text {mixed } O T}^{q}, B_{\text {mixed } O T}^{q}\right)= \begin{cases}1+p_{?}\left(1-p_{?}\right)+\left(1-2 p_{?}\right) \sqrt{1-p_{?}} & \text { for } 1 / 2<p_{?} \leq 3 / 4 \\ p_{?}^{2}+\left(1-p_{?}\right)\left(1+\sqrt{1-p_{?}}\right) & \text { for } p_{?}>3 / 4 .\end{cases}$

As in Subsection 6.2.4, we will consider the difference between the trade-off relations for the classical/quantum cheating probabilities and the trade-off relations for the guessing probabilities. Since the guessing probabilities in terms of $p_{\text {? }}$ are the same for the mixed states quantum Rabin OT protocol as they were for the classical and pure states quantum protocols, we use the expressions presented in Eq. (6.38).


Figure 6.9: Trade-off relations with respect to $p_{\text {? }}$ of the classical protocol (dotted) and the quantum protocol based on mixed states (solid) after subtraction of the relations for the guessing probabilities.

In Figure 6.9, the difference $f_{i}\left(A_{O T}^{c}, B_{O T}^{c}\right)-f_{i}\left(A_{O T}^{g}, B_{O T}^{g}\right)$ is plotted as the dotted line and the difference $f_{i}\left(A_{\text {mixed } O T}^{q}, B_{\text {mixed } O T}^{c}\right)-f_{i}\left(A_{O T}^{g}, B_{O T}^{g}\right)$ as the solid line; for $i \in\{1,2\}$ and with respect to $p_{\text {? }}$. As previously, the trade-off relations $f_{2}$ are multiplied by a factor of 2 in order to display continuous graphs.

The two graphs coincide for the range $0 \leq p_{\text {? }} \leq 1 / 2$, which includes the value $p_{\text {? }}=1 / 2$ that is used for the traditional definition of Rabin OT. But, for $p_{\text {? }}>1 / 2$, the curve for the quantum protocol lies below the curve for the classical protocol. Hence, we can conclude that the quantum protocol with mixed states does equally as well as the classical protocol for the first half of the range of $p$ ? and then it outperforms the classical protocol. In terms of the advantage of the cheating strategies over the guessing strategies, we can say that the advantage when $p_{?}>1 / 2$ is smaller for the quantum protocol making it more secure than the classical protocol.

In other respects, when bringing to mind that this quantum protocol can also be viewed as a classical Rabin OT protocol, then the category of classical Rabin OT protocols it represents seems to provide a better benchmark for the performance of classical Rabin OT protocols than the considered protocols using coin flips.

### 6.4 Comparison between Mixed States and Pure States Protocols

Comparisons of the quantum protocols with the classical protocol have shown that the mixed states protocol is never worse than the classical protocol, while this is sometimes the case for the pure states protocol. To get a more thorough picture about whether mixed states can help to improve quantum Rabin OT protocols, we will directly compare the mixed states and pure states protocols using the same trade-off relations specified in Subsections 6.2.4 and 6.3.4.

In particular, we will compare the differences $f_{i}\left(A_{\text {pure } O T}^{q}, B_{\text {pure } O T}^{c}\right)-f_{i}\left(A_{O T}^{g}, B_{O T}^{g}\right)$ and $f_{i}\left(A_{\text {mixed } O T}^{q}, B_{\text {mixed } O T}^{c}\right)-f_{i}\left(A_{O T}^{g}, B_{O T}^{g}\right)$ for $i \in\{1,2\}$. Since the guessing probability is the same for both the protocol based on pure states and the one based on mixed states, it is sensible to consider these differences for the same reason as mentioned in Subsection 6.2.4. We plot the trade-off relation referring to the pure states protocol as the dashed line and the trade-off relation referring to the mixed states protocol as the dotted-dashed line in Figure 6.10. Both of them are with respect to $p_{\text {? }}$ and the expressions for $f_{2}$ are multiplied by 2 to obtain continuous graphs.


Figure 6.10: Trade-off relations with respect to $p_{\text {? }}$ of the quantum Rabin OT protocol based on pure states (dashed line) and the quantum Rabin OT protocol based on mixed states (dotted-dashed line) after subtraction of the relations for the guessing probabilities.

In Figure 6.10, the two graphs intersect at three points, $p_{\text {? }}=0, p_{?}=5 / 13 \approx$ 0.385 , and $p_{\text {? }}=1$. The curve for the pure states protocol is lower in the region $0<p_{\text {? }}<5 / 13$, while the curve for the mixed states protocol is lower in the region $5 / 13<p_{\text {? }}<1$. We can deduce that the mixed states protocol is lower than the pure states protocol for a larger region $(8 / 13>5 / 13)$. Thus, the advantage of the cheating strategies over the guessing strategies is, for a larger range of $p_{\text {? }}$, smaller for the protocol based on mixed states and hence it is more often securer than the protocol based on pure states.

It is likely that mixed states can indeed help to improve quantum Rabin OT protocols. This is indicated by the direct comparison between the protocol based on pure states and the protocol based on mixed states and the additional fact that the mixed states protocol is never worse than the classical protocol (only equally as well or better) while the pure states protocol is at times outperformed by the classical protocol.

Once again viewing the protocol with mixed states as a classical protocol, we can compare the quantum Rabin OT protocol using pure states to an improved benchmark. In this case, we conclude that the pure state protocol performs worse than previously identified as it does no longer surpass performance of the classical Rabin OT protocol in the region $4 / 5<p_{\text {? }}<1$ (see Subsection 6.2.4).

### 6.5 Further Generalisation of Rabin OT Protocol Based on Mixed States

As noted earlier, the Rabin oblivious transfer protocol based on mixed states investigated in Section 6.3 was somewhat constrained. That is, introducing the same randomisation factor $r$ for both the states sent by an honest Alice and the measurement operators describing the measurement of an honest Bob limited the protocol's modifiability to one free variable. In this section, we expand the protocol by considering two free variables, one randomisation factor $q$ for honest Alice's states and another randomisation factor $r$ for honest Bob's measurement operators. The protocol can then be described as follows.

1. Alice randomly chooses one of the two mixed states $(0 \leq q \leq 1)$

$$
\begin{equation*}
\rho_{0}=(1-q)|0\rangle\langle 0|+q|1\rangle\langle 1|, \quad \rho_{1}=(1-q)|0\rangle\langle 0|+q|2\rangle\langle 2|, \tag{6.50}
\end{equation*}
$$

with a probability of $1 / 2$ each, and sends it to Bob.
2. Bob performs an unambiguous discrimination measurement on the received state. His measurement operators are $(0 \leq r \leq 1)$

$$
\begin{align*}
& \Pi_{?}=|0\rangle\langle 0|+(1-r)|1\rangle\langle 1|+(1-r)|2\rangle\langle 2|, \\
& \Pi_{0}=r|1\rangle\langle 1| \\
& \Pi_{1}=r|2\rangle\langle 2| \tag{6.51}
\end{align*}
$$

This means that the probabilities for honest Bob obtaining the bit or not are expressed as $P($ bit $)=q r$ and $P($ no bit $)=p_{?}=1-q r$.

Also this more general form of the Rabin OT protocol using mixed states can be implemented using only classical means. The only difference is that the probability distributions of Alice's and Bob's actions are no longer necessary the same, that is, Alice's probability of sending a state and Bob's probability of reading the state can be chosen independently from each other.

### 6.5.1 Security against Alice and Bob

When looking at security against a dishonest Alice or a dishonest Bob, we can note that their cheating strategies stay the same as their cheating strategies in the protocol with the common randomisation factor $r$, but the expressions for their
cheating probabilities change slightly and will be functions in terms of $q$ and $r$ instead.

A dishonest Bob who always wants to know which value Alice's bit has, will apply a minimum-error measurement to distinguish between $\rho_{0}$ and $\rho_{1}[80]$ and will be successful with probability

$$
\begin{equation*}
B_{\text {general mixed } O T}^{q}=\frac{1}{2}+\frac{1}{2} q . \tag{6.52}
\end{equation*}
$$

For a dishonest Alice, in one situation Bob does no testing and, in another, Bob monitors the probabilities of obtaining the bit or not to verify that they are equal to the probabilities he expects. In the first case, Alice will, as before, be able to cheat perfectly by sending $|0\rangle$, the orthogonal state to $\Pi_{0}$ and $\Pi_{1}$, which will result in Bob never getting the bit. When Bob follows the monitoring procedure, Alice will need to send a correct statistical mixture of $|0\rangle,|1\rangle$, and $|2\rangle$. Following the same reasoning as in Subsection 6.3.3, we know that $(1-x) r=r q$ needs to hold for the probability of Bob obtaining the bit and, thus, $x=1-q$. A cheating Alice will send $|0\rangle$ with probability $x$ and $|1\rangle$ or $|2\rangle$ with probability $\frac{1}{2}(1-x)$ each, achieving her average cheating probability

$$
A_{\text {general mixed } O T}^{q}= \begin{cases}1-q r & \text { for } r \leq 1 / 2  \tag{6.53}\\ 1-q+q r & \text { for } r>1 / 2\end{cases}
$$

We plot Alice's and Bob's cheating probabilities in terms of $q$ and $r$ in Figure 6.11. It shows that $r=1 / 2$ is the best value to minimise Alice's cheating probability for any $q$ and, since Bob's cheating probability is independent of the former variable, $1 / 2$ can be straightforwardly picked as the optimum value for $r$. It is not quite as easy with the value for $q$ since this affects both $A_{\text {general mixed } O T}^{q}$ and $B_{\text {general mixed } O T}^{q}$. When $q \rightarrow 0$, Bob's cheating probability tends to $1 / 2$ while Alice's tends to 1 for any value of $r$. On the other hand, when $q \rightarrow 1$, Bob's cheating probability tends to 1 while Alice's goes to the minimums attainable with respect to a chosen $r$. The seemingly best value appears to be $q=1 / 2$ as this is the middle ground. Also, the plane created by the two cheating probabilities when taking into account the larger of the two probabilities for the respective values of $r$ and $q$, has a dip where $r=q=1 / 2$. Hence, it seems reasonable to have used $r=q=1 / 2$ in the analysis of the quantum Rabin OT protocol based on mixed states in Section 6.3 and in the comparison with the quantum Rabin OT protocol based on pure states in Section 6.4.


Figure 6.11: Alice's and Bob's cheating probabilities with respect to $q$ and $r$. The plot in (b) is the top view of the 3-dimensional plot in (a).

### 6.5.2 Protocol Performance when $P$ (no bit) $=P($ bit $)$

The dip when $r=q=1 / 2$ mentioned in the previous subsection, coincides with $P($ no bit $)=3 / 4$. However, in the traditional definition of Rabin oblivious transfer, we want $P($ no bit $)=P($ bit $)=1 / 2$, that is, Bob receiving the bit or not happens with equal probability. We investigate here how well the considered protocol does in this case.

Without loss of generality, the analysis is carried out in terms of $r$. Since $P($ bit $)=$ $r q=1 / 2$, we can set $q=1 / 2 r$. However, since it needs to hold that $q \leq 1$, we have $1 / 2 r \leq 1$ and so the range is restricted to $1 / 2 \leq r \leq 1$. This results in $1 / 2 \leq q \leq 1$ as well and we can conclude that the combinations of $r$ and $q$ that can yield $P($ no bit $)=P($ bit $)=1 / 2$, are restricted to a part of the range of their possible values. The cheating probabilities in Eqns. (6.52) and (6.53) can then be reformulated to

$$
\begin{equation*}
B_{\text {general mixed } O T}^{q}=\frac{1}{2}+\frac{1}{4 r} \quad \text { and } \quad A_{\text {general mixed } O T}^{q}=\frac{3}{2}-\frac{1}{2 r} \tag{6.54}
\end{equation*}
$$

for Bob and Alice, respectively.
Figure 6.12 shows the graphs of these cheating probabilities in terms of $r$. For $r=0$, Bob (solid line) can cheat perfectly while Alice (dashed line) cannot cheat any better than with a random guess and vice versa when $r=1$. The two cheating probabilities intersect at $r=3 / 4$ where $A_{\text {general mixed } O T}^{q}=B_{\text {general mixed } O T}^{q}=5 / 6 \approx$ 0.833 .


Figure 6.12: Cheating probabilities for Alice (dashed line) and Bob (solid line) as functions of $r$.

### 6.6 Conclusion

In this chapter, we looked at two quantum Rabin oblivious transfer protocols and compared them both to a classical Rabin OT protocol as well as to each other.

The protocol considered in Section 6.2 is based on pure states. We analysed its cheating probabilities and concluded that, in order to restrict a dishonest Alice, Bob needs to monitor the probabilities of his obtaining a bit and his obtaining no bit and check if they agree with what he expects. This will result in an average cheating probability for Alice and the need to implement multiple rounds of the protocol, where in a single round she could cheat perfectly.

The protocol in Section 6.3 is based on mixed states. Also here, we analysed the cheating probabilities and concluded that Bob needs to monitor the occurrence probabilities in order to prevent Alice from cheating perfectly, which results in an average cheating probability for Alice. The assumption of a common randomisation factor for honest Alice's states and honest Bob's measurement operators was adhered to in this part. But in Section 6.5, we loosened it and examined the protocol more generally with a differing randomisation factor for Alice's states and Bob's measurement operators. These protocols based on mixed states can be implemented using only classical means and therefore provide another benchmark for the performance of classical Rabin OT protocols.

The comparison of the two protocols in Section 6.2 and 6.3 with the classical protocol, showed that, while the pure states protocol is sometimes worse than the classical protocol, the mixed states protocol always performs at least as well as the
classical protocol. The direct comparison of the two protocols in Section 6.4 showed that there is a range when $p_{\text {? }}<5 / 13$, where the pure states protocol is better than the mixed states protocol. The mixed states protocol outperforms the pure states one for any value $p_{\text {? }}>5 / 13$ though and, thus, is the better protocol for the larger range of $p_{\text {? }}$. This strengthens the assumption that mixed states can help to improve the security of quantum Rabin OT protocols.

For further investigation of this assumption, it would be interesting to examine other quantum Rabin OT protocols based on mixed states in further work and compare them to the quantum Rabin OT protocol based on pure states as well as to the benchmark of the performance of classical Rabin OT protocols provided by the considered quantum Rabin OT protocol based on mixed states.

## Chapter 7

## Conclusion

The fields of cryptography and communication were extended in recent decades to include new areas of research: quantum cryptography and quantum communication. That is, the question about how quantum mechanics and its inherent properties can benefit and help to create secure communication protocols has become a big area of investigation. It includes not only the study of protocols in which the threat is an outside adversary who wants to eavesdrop on secret communications, but also the study of protocols in which the two communicating parties do not trust each other and one of them might be an adversary who wants to get more information from the protocol than he/she is supposed to.

A protocol fitting into the second category is oblivious transfer. Oblivious transfer is a powerful cryptographic primitive since it can be used as basic building block to realise any two-party computation. Research in the classical setting has shown that OT cannot be done classically with information-theoretic security. Unfortunately, also in the quantum setting it is not possible to have information-theoretically secure quantum OT without any restrictions. Nevertheless, also without any restrictions it is possible to bound the sender's and receiver's cheating probabilities in quantum oblivious transfer.

In this thesis, we focused on different variants of oblivious transfer, investigating their security when no restrictions are placed on the dishonest party. We especially focused on the less investigated variant of XOR oblivious transfer. In Chapter 3 and Chapter 5, we examined non-interactive XOT protocols. Deriving general bounds for such protocols based on the use of symmetric pure states, we presented a specific protocol that was provably optimal among non-interactive XOT protocols using symmetric pure states. We then further generalised the concept and this specific protocol to consider XOR oblivious transfer where the sender encodes not only a string of two classical bits but a string of $n$ classical bits.

Considering the situation when the two communicating parties do not have the same computational or technological power, but want to implement oblivious trans-
fer in both directions, we focused on the concept of reversing a protocol in Chapter 4. We reversed a 1-2 OT protocol [7] and the optimal XOT protocol presented in this thesis and observed that the cheating probabilities are linked to the parties' role in the protocol as opposed to their physical action, i.e. being the one sending the quantum state or the one measuring the quantum state.

In the last part, Chapter 6, we focused on another variant of oblivious transfer, namely Rabin oblivious transfer. Examining Rabin OT using pure states and then Rabin OT using mixed states, we at first analysed the protocols separately for their security and then compared them to each other. We concluded that, for a part of the probability distribution, that is, the distribution of the probability of the receiver obtaining the bit or not, the pure states protocol outperforms the mixed states protocol. For the larger part of the probability distribution, however, the mixed states protocol outperforms the pure states protocol.

All in all, it can be seen that oblivious transfer remains an area for future research and many questions remain open. In particular, variants other than the most wellknown and fairly well investigated 1-out-of-2 oblivious transfer variant offer many avenues for further work. With regards to the variants investigated in this thesis, future work can built upon and extend the question about a potential connection between 1-out-of- $n$ oblivious transfer and hidden matching quantum retrieval games or also the question if quantum Rabin oblivious transfer protocols based on mixed states perform better than quantum Rabin oblivious transfer protocols based on pure states. Another topic that can be expanded and provides many still to be investigated questions is the concept of reversal. It is not only interesting to study the reversal of protocols other than oblivious transfer, but also to examine the fundamentals of this concept, such as which characteristics make a protocol reversible or if the cheating probabilities of the functional roles always stay the same for any reversed protocol.

## Bibliography

[1] S. Singh. The Code Book - The secret history of codes and codebreaking. Fourth Estate, London, 2002.
[2] J. P. Dowling and G. J. Milburn. Quantum technology: the second quantum revolution. Phil. Trans. R. Soc. A, 361(1809):1655-1674, 2003.
[3] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput., 26(5):1484-1509, 1997.
[4] J. P. Buhler, H. W. Lenstra, Jr., and C. Pomerance. Factoring integers with the number field sieve. In The development of the number field sieve. Lecture Notes in Mathematics, volume 1554, pages 50-94. Springer Berlin Heidelberg, 1993.
[5] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems 83 Signal Processing, pages 175-179, Bangalore, India, 1984.
[6] J. Kilian. Founding crytpography on oblivious transfer. In Proceedings of the twentieth annual ACM symposium on Theory of computing, STOC '88, pages 20-31. ACM, 1988.
[7] R. Amiri, R. Stárek, D. Reichmuth, I. V. Puthoor, M. Mičuda, L. Mišta, Jr., M. Dušek, P. Wallden, and E. Andersson. Imperfect 1-out-of-2 quantum oblivious transfer: Bounds, a protocol, and its experimental implementation. $P R X$ Quantum, 2(1):010335, 2021.
[8] S. Wiesner. Conjugate coding. SIGACT News, 15(1):78-88, 1983. Originally written around 1970.
[9] G. Brassard. Brief history of quantum cryptography: a personal perspective. In IEEE Information Theory Workshop on Theory and Practice in InformationTheoretic Security, 2005., pages 19-23. IEEE, 2005.
[10] M. O. Rabin. How to exchange secrets with oblivious transfer. IACR Cryptol. ePrint Arch., 2005:187, 2005.
[11] S. Even, O. Goldreich, and A. Lempel. A randomized protocol for signing contracts. Commun. ACM, 28(6):637-647, 1985.
[12] G. Brassard, C. Crépeau, and J.-M. Robert. All-or-nothing disclosure of secrets. In Advances in Cryptology - CRYPTO '86, pages 234-238. Springer Berlin Heidelberg, 1986.
[13] G. Brassard and C. Crépeau. Oblivious transfers and privacy amplification. In Advances in Cryptology - EUROCRYPT '97, pages 334-347. Springer Berlin Heidelberg, 1997.
[14] C. Crépeau. Equivalence between two flavours of oblivious transfers. In $A d-$ vances in Cryptology - CRYPTO '87, pages 350-354. Springer Berlin Heidelberg, 1987.
[15] G. Brassard, C. Crépeau, and J.-M. Robert. Information theoretic reductions among disclosure problems. In 27th Annual Symposium on Foundations of Computer Science (sfcs 1986), pages 168-173. IEEE, 1986.
[16] G. Brassard, Crépeau C., and S. Wolf. Oblivious transfers and privacy amplification. J. Cryptol., 16(4):219-237, 2003.
[17] A. Kent. Quantum bit string commitment. Phys. Rev. Lett., 90(23):237901, 2003.
[18] G. P. He and Z. D. Wang. Nonequivalence of two flavors of oblivious transfer at the quantum level. Phys. Rev. A, 73(4):044304, 2006.
[19] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for noncryptographic fault-tolerant distributed computation. In Symposium on the Theory of Computing, pages 351-371, 1988.
[20] D. Chaum, C. Crépeau, and I. B. Damgård. Multiparty unconditionally secure protocols. In Proceedings of the 20th Annual ACM Symposium on Theory of Computing, STOC '88, pages 11-19. Association for Computing Machinery, 1988.
[21] D. Mayers. Unconditionally secure quantum bit commitment is impossible. Phys. Rev. Lett., 78(17):3414, 1997.
[22] H.-K. Lo. Insecurity of quantum secure computations. Phys. Rev. A, 56(2):1154, 1997.
[23] C. H. Bennett, G. Brassard, C. Crépeau, and M.-H. Skubiszewska. Practical quantum oblivious transfer. In Advances in Cryptology - CRYPTO '91, pages 351-366. Springer Berlin Heidelberg, 1992.
[24] A. C.-C. Yao. Security of quantum protocols against coherent measurements. In Proceedings of the Twenty-Seventh Annual ACM Symposium on Theory of Computing, STOC '95, pages 67-75. ACM, 1995.
[25] H. Buhrman, M. Christandl, and C. Schaffner. Complete insecurity of quantum protocols for classical two-party computation. Phys. Rev. Lett., 109(16):160501, 2012.
[26] G. P. He and Z. D. Wang. Oblivious transfer using quantum entanglement. Phys. Rev. A, 73(1):012331, 2006.
[27] J. Peat and E. Andersson. Breaking an OT protocol. Unpublished Work, 2022.
[28] A. Kent. Unconditionally secure bit commitment. Phys. Rev. Lett., 83(7):1447, 1999.
[29] A. Kent. Impossibility of unconditionally secure commitment of a certified classical bit. Phys. Rev. A, 61(4):042301, 2000.
[30] G. P. He. Can relativistic bit commitment lead to secure quantum oblivious transfer? Eur. Phys. J. D, 69(4), 2015.
[31] R. Colbeck and A. Kent. Variable-bias coin tossing. Phys. Rev. A, 73(3):032320, 2006.
[32] R. Colbeck. Impossibility of secure two-party classical computation. Phys. Rev. A, 76(6):062308, 2007.
[33] D. Pitalúa-García. Spacetime-constrained oblivious transfer. Phys. Rev. A, 93(6):062346, 2016.
[34] D. Pitalúa-García and I. Kerenidis. Practical and unconditionally secure spacetime-constrained oblivious transfer. Phys. Rev. A, 98(3):032327, 2018.
[35] D. Pitalúa-García. One-out-of- $m$ spacetime-constrained oblivious transfer. Phys. Rev. A, 100(1):012302, 2019.
[36] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner. Cryptography in the bounded quantum-storage model. In 46 th Annual IEEE Symposium on Foundations of Computer Science, FOCS'05, pages 449-458. IEEE, 2005.
[37] S. Wehner, C. Schaffner, and B. M. Terhal. Cryptography from noisy storage. Phys. Rev. Lett., 100(22):220502, 2008.
[38] P. Mandayam and S. Wehner. Achieving the physical limits of the boundedstorage model. Phys. Rev. A, 83(2):022329, 2011.
[39] R. König, S. Wehner, and J. Wullschleger. Unconditional security from noisy quantum storage. IEEE Trans. Inf. Theory, 58(3):1962-1984, 2012.
[40] J. Ribeiro and S. Wehner. On bit commitment and oblivious transfer in measurement-device independent settings, 2020. arXiv:2004.10515.
[41] J. Kaniewski and S. Wehner. Device-independent two-party cryptography secure against sequential attacks. New J. Phys., 18(5):055004, 2016.
[42] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, C.-Z. Peng, Q. Zhang, and J.-W. Pan. Experimental measurement-device-independent quantum key distribution. Phys. Rev. Lett., 111(13):130502, 2013.
[43] C. Wang, W. Y. Kon, H. J. Ng, and C. C. W. Lim. Experimental symmetric private information retrieval with measurement-device-independent quantum network. Light Sci Appl, 11(1):268, 2022.
$[44]$ D. P. Nadlinger, P. Drmota, B. C. Nichol, G. Araneda, D. Main, R. Srinivas, D. M. Lucas, C. J. Ballance, K. Ivanov, E. Y.-Z. Tan, P. Sekatski, R. L. Urbanke, R. Renner, N. Sangouard, and J. D. Bancal. Experimental quantum key distribution certified by Bell's theorem. Nature, 607(7920):682, 2022.
[45] W. Zhang, T. van Leent, K. Redeker, R. Garthoff, R. Schwonnek, F. Fertig, S. Eppelt, W. Rosenfeld, V. Scarani, C. C. W. Lim, and H. Weinfurter. A device-independent quantum key distribution system for distant users. Nature, 607(7920):687, 2022.
[46] A. Chailloux, I. Kerenidis, and J. Sikora. Lower bounds for quantum oblivious transfer. Quant. Inf. Comput., 13(1-2):158-177, 2013.
[47] A. Chailloux, G. Gutoski, and J. Sikora. Optimal bounds for semi-honest quantum oblivious transfer. Chicago J. Theor. Comput. Sci., 2016.
[48] S. Kundu, J. Sikora, and E. Y.-Z. Tan. A device-independent protocol for XOR oblivious transfer. Quantum, 6:725, 2022.
[49] S. Osborn and J. Sikora. A constant lower bound for any quantum protocol for secure function evaluation, 2022. arXiv:2203.08268.
[50] D. Reichmuth, I. V. Puthoor, P. Wallden, and E. Andersson. One-sided information-theoretic security in quantum oblivious transfer. Unpublished Work, 2021.
[51] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan. Private information retrieval. J. ACM, 45(6):965-981, 1998.
[52] Y. Gertner, Y. Ishai, E. Kushilevitz, and T. Malkin. Protecting data privacy in private information retrieval schemes. In Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing, STOC '98, pages 151—160, New York, NY, USA, 1998. Association for Computing Machinery.
[53] G. Di Crescenzo, T. Malkin, and R. Ostrovsky. Single database private information retrieval implies oblivious transfer. In Advances in Cryptology EUROCRYPT 2000, pages 122-138. Springer Berlin Heidelberg, 2000.
[54] I. Kerenidis and R. de Wolf. Exponential lower bound for 2-query locally decodable codes via a quantum argument. J. Comput. Syst. Sci., 69(3):395-420, 2004.
[55] L. Olejnik. Secure quantum private information retrieval using phase-encoded queries. Phys. Rev. A, 84(2):022313, 2011.
[56] I. Kerenidis and R. de Wolf. Quantum symmetrically-private information retrieval. Inf. Process. Lett., 90(3):109-114, 2004.
[57] V. Giovannetti, S. Lloyd, and L. Maccone. Quantum private queries. Phys. Rev. Lett., 100(23):230502, 2008.
[58] Blum Manuel. Coin flipping by telephone a protocol for solving impossible problems, volume 15. Association for Computing Machinery, 1983.
[59] C. Döscher and M. Keyl. An introduction to quantum coin-tossing. Fluct. Noise Lett., 02(04), 2002.
[60] A. Kitaev. Quantum coin-flipping. In Talk at the Quantum Information Processing Conference, QUIP 2003, MSRI, Berkeley, CA, 2003.
[61] A. Chailloux and I. Kerenidis. Optimal quantum strong coin flipping. In 2009 50th Annual IEEE Symposium on Foundations of Computer Science, pages 527-533, 2009.
[62] Carlos Mochon. Quantum weak coin flipping with arbitrarily small bias, 2007. arXiv:0711.4114.
[63] A. Pappa, A. Chailloux, E. Diamanti, and I. Kerenidis. Practical quantum coin flipping. Phys. Rev. A, 84(5):052305, 2011.
[64] A. Pappa, P. Jouguet, T. Lawson, A. Chailloux, M. Legré, P. Trinkler, I. Kerenidis, and E. Diamanti. Experimental plug and play quantum coin flipping. Nat. Commun., 5:3717, 2014.
[65] S. M. Barnett. Quantum Information. Oxford University Press, Oxford, 2009.
[66] S. M. Barnett and S. Croke. Quantum state discrimination. Adv. Opt. Photon., 1(2):238-278, 2009.
[67] S. Bandyopadhyay, R. Jain, J. Oppenheim, and C. Perry. Conclusive exclusion of quantum states. Phys. Rev. A, 89(2):022336, 2014.
[68] J. Crickmore, I. V. Puthoor, B. Ricketti, S. Croke, M. Hillery, and E. Andersson. Unambiguous quantum state elimination for qubit sequences. Phys. Rev. Res., 2(1):013256, 2020.
[69] J. W. Webb, I. V. Puthoor, J. Ho, J. Crickmore, E. Blakely, A. Fedrizzi, and E. Andersson. Experimental demonstration of optimal unambiguous two-out-of-four quantum state elimination, 2022. arXiv:2207.00019.
[70] R. J. Collins, R. J. Donaldson, V. Dunjko, P. Wallden, P. J. Clarke, E. Andersson, J. Jeffers, and G. S. Buller. Realization of quantum digital signatures without the requirement of quantum memory. Phys. Rev. Lett., 113(4):040502, 2014.
[71] L. Stroh, N. Horová, R. Stárek, I. V. Puthoor, M. Mičuda, M. Dušek, and E. Andersson. Non-interactive XOR quantum oblivious transfer: optimal protocols and their experimental implementations, 2022. arXiv:2209.11300. Accepted/In Press in PRX Quantum.
[72] E. Andersson, L. Stroh, I. V. Puthoor, D. Reichmuth, N. Horová, R. Stárek, M. Mičuda, M. Dušek, and P. Wallden. Quantum cryptography beyond quantum key distribution: variants of quantum oblivious transfer. In Quantum Computing, Communication, and Simulation III, SPIE Photonics West 2023, page 124460C, San Francisco, California, USA, 2023. SPIE.
[73] P. Hausladen and W. K. Wootters. A 'pretty good' measurement for distinguishing quantum states. J. Mod. Opt., 41(12):2385-2390, 1994.
[74] M. Ban, K. Kurokawa, R. Momose, and O. Hirota. Optimum measurements for discrimination among symmetric quantum states and parameter estimation. Int. J. Theor. Phys., 36(6):1269-1288, 1997.
[75] P. Wallden, V. Dunjko, and E. Andersson. Minimum-cost quantum measurements for quantum information. J. Phys. A: Math. Theor., 47(12):125303, 2014.
[76] N. Dalla Pozza and G. Pierobon. Optimality of square-root measurements in quantum state discrimination. Phys. Rev. A, 91(4):042334, 2015.
[77] E. Andersson, S. M. Barnett, C. R. Gilson, and K. Hunter. Minimum-error discrimination between three mirror-symmetric states. Phys. Rev. A, 65(5):052308, 2002.
[78] C. L. Chou. Minimum-error discrimination among mirror-symmetric mixed quantum states. Phys. Rev. A, 70(6):062316, 2004.
[79] C. Crépeau and M. Sántha. On the reversibility of oblivious transfer. In Advances in Cryptology - EUROCRYPT '91, pages 106-113. Springer Berlin Heidelberg, 1991.
[80] C. W. Helstrom. Quantum Detection and Estimation Theory. Academic Press, 1976.
[81] D. Gavinsky. Quantum money with classical verification. In 2012 IEEE 27 th Conference on Computational Complexity, pages 42-52, 2012.
[82] S. M. Barnett. Minimum-error discrimination between multiply symmetric states. Phys. Rev. A, 64(3):030303, 2001.
[83] M. Georgiou and I. Kerenidis. New constructions for quantum money. In 10th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2015), volume 44 of Leibniz International Proceedings in

Informatics (LIPIcs), pages 92-110. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2015.
[84] R. Amiri and J. M. Arrazola. Quantum money with nearly optimal error tolerance. Phys. Rev. A, 95(6):062334, 2017.
[85] J. M. Arrazola, M. Karasamanis, and N. Lütkenhaus. Practical quantum retrieval games. Phys. Rev. A, 93(6):062311, 2016.
[86] Z. Bar-Yossef, T. S. Jayram, and I. Kerenidis. Exponential separation of quantum and classical one-way communication complexity. In Proceedings of the Thirty-Sixth Annual ACM Symposium on Theory of Computing, STOC '04, pages 128-137. Association for Computing Machinery, 2004.
[87] K. Y. Cheong, M.-H. Hsieh, and T. Koshiba. A weak quantum oblivious transfer, 2018. arXiv:1010.0702.
[88] I. D. Ivanovic. How to differentiate between non-orthogonal states. Phys. Lett. A, 123(6):257-259, 1987.
[89] D. Dieks. Overlap and distinguishability of quantum states. Phys. Lett. A, 126(5-6):303-306, 1988.
[90] A. Peres. How to differentiate between non-orthogonal states. Phys. Lett. A, 128(1-2):19, 1988.
[91] U. Herzog. Minimum-error discrimination between a pure and a mixed twoqubit state. J. Opt. B: Quantum Semiclass. Opt., 6(3):S24-S28, 2004.

