BRICS RS-03-37 Crépeau et al.: Computational Collapse of Quantum State with Application to Oblivious Transfer

BRICS

Basic Research in Computer Science

Computational Collapse of Quantum State with Application to Oblivious Transfer

Claude Crépeau
Paul Dumais
Dominic Mayers
Louis Salvail

BRICS Report Series **RS-03-37**

ISSN 0909-0878 **November 2003**

See back inner page for a list of recent BRICS Report Series publications.
Copies may be obtained by contacting:

BRICS
Department of Computer Science
University of Aarhus
Ny Munkegade, building 540
DK–8000 Aarhus C
Denmark
Telephone: +45 8942 3360
Telefax: +45 8942 3255
Internet: BRICS@brics.dk

BRICS publications are in general accessible through the World Wide Web and anonymous FTP through these URLs:

http://www.brics.dk
ftp://ftp.brics.dk
This document in subdirectory RS/03/37/

Computational Collapse of Quantum State with Application to Oblivious Transfer

Claude Crépeau[1⋆], Paul Dumais[1⋆⋆], Dominic Mayers[2⋆⋆⋆], and Louis Salvail[3†]

[1] School of Computer Science, McGill University, {crepeau|dumais}@cs.mcgill.ca
[2] IQI, California Institute of Technology, dmayers@cs.caltech.edu
[3] BRICS[‡], FICS[§], Dept. of Computer Science, University of Århus, salvail@brics.dk

Abstract. Quantum 2-party cryptography differs from its classical counterpart in at least one important way: Given blak-box access to a perfect commitment scheme there exists a secure $1-2$ *quantum* oblivious transfer. This reduction proposed by Crépeau and Kilian was proved secure against any receiver by Yao, in the case where perfect commitments are used. However, quantum commitments would normally be based on computational assumptions. A natural question therefore arises: What happens to the security of the above reduction when computationally secure commitments are used instead of perfect ones?

In this paper, we address the security of $1-2$ QOT when computationally binding string commitments are available. In particular, we analyse the security of a primitive called *Quantum Measurement Commitment* when it is constructed from unconditionally concealing but computationally binding commitments. As measuring a quantum state induces an irreversible collapse, we describe a QMC as an instance of "computational collapse of a quantum state". In a QMC a state appears to be collapsed to a polynomial time observer who cannot extract full information about the state without breaking a computational assumption.

We reduce the security of QMC to a *weak* binding criteria for the string commitment. We also show that *secure* QMCs implies QOT using a straightforward variant of the reduction above.

1 Introduction

Quantum 2-party cryptography differs from its classical counterpart in at least one important way: Given blak-box access to a perfect commitment scheme there

⋆ Part of this research was done while visiting University of Århus and was funded by Québec's FQRNT and MDER, and Canada's NSERC and MITACS.
⋆⋆ Part of this research was funded by NSERC
⋆⋆⋆ This work has been supported in part by the National Science Foundation under Grant No. EIA-0086038.
† Part of this research was funded by European projects QAIP and PROSECCO.
‡ Funded by the Danish National Research Foundation.
§ FICS, Foundations in Cryptography and Security, funded by the Danish Natural Sciences Research Council.

exists a secure $1-2$ *quantum* oblivious transfer (i.e. 1-2 QOT) scheme[5, 3, 4]. Classically, it is known that such a reduction is unlikely to exist [9]. By *1-2 QOT* we mean a standard oblivious transfer of two classical messages using quantum communication. In [5], Crépeau and Kilian have shown how 1-2 QOT can be obtained from perfect commitments (i.e. the CK protocol). The security analysis of the CK protocol was provided by Crépeau in [4] with respect to receivers restricted to perform only immediate and complete measurements. The assumption was relaxed in [14] by showing that privacy for the sender is garanteed against any individual measurements applied by the receiver. The security against any receiver was obtained by Yao in [19]. This important paper provides a full proof of security for 1-2 QOT when constructed from perfect commitments under the assumption that the quantum channel is error-free. Yao's result was then generalized by Mayers[12] for the case of noisy quantum channel [3] and where strings are transmitted instead of bits. Mayers then reduced the security of quantum key distribution to the security of such a generalized 1-2 QOT. If 2-party cryptography in the quantum world seems to rely upon weaker assumptions than its classical counterpart, it also shares some of its limits. As it was shown in [11, 13, 10], no statistically binding and concealing quantum bit commitment can exist. On the other hand, quantum commitments can be based upon physical[16] and computational[7, 6] assumptions. A natural question arises: What happens to the security of the CK protocol when computationally secure commitments are used instead of perfect ones? It should be stressed that Yao's proof does not apply in this case since it relies heavily upon the fact that the commitment scheme is modelled by a classical black-box (i.e. one with classical inputs and outputs). The proof is information theoretic provided the sender and the receiver have black-box access to perfect commitments. For Yao's proof to apply, the committing phase should be modelled by the transmission of a *classical bit* to a third party who conceals it to the receiver until the opening phase. Although any unconditionally binding commitment scheme defines such a classical bit, unconditionally concealing commitments do not (i.e. both committed values can be explained by the information provided to the receiver). In this paper, we address the security of 1-2 QOT when computationally binding string commitments are available. In particular, we analyse the security of a primitive called *Quantum Measurement Commitment* (i.e. QMC) when it is constructed from unconditionally concealing but computationally binding commitments. We reduce the security of QMC to a *weak* binding criteria for the string commitment. We also show that *secure* QMCs implies 1-2 QOT using a straightforward variant of the CK protocol. It follows that unlike Yao's proof (and the proof in [14]), our security proof applies when computionally binding commitments are used.

The CK protocol can be seen as a quantum reduction of 1-2 OT to bit commitment. To see how it works, consider the BB84 coding scheme[2, 5] for classical bit b into a random state in $\{\,|b\rangle_+,\ |b\rangle_\times\}$.The random $\theta \in \{+, \times\}$ used to encode b into the quantum state $|b\rangle_\theta$, is called the *transmission basis*.Since only orthogonal quantum states can be distinguished with certainty, the transmitted bit b is not received perfectly by the receiver, Alice, who does not know the transmission basis. The coding scheme also specifies what an honest Alice should be doing with the received state $|b\rangle_\theta$. She picks $\hat{\theta} \in_R \{+, \times\}$ and measures $|b\rangle_\theta$ with measurement $\mathbb{M}_{\hat{\theta}}$ that distinguishes perfectly orthogonal states $|0\rangle_{\hat{\theta}}$ and $|1\rangle_{\hat{\theta}}$.If Bob and Alice follow honestly the BB84 coding scheme then b is received with probability 1 when $\hat{\theta} = \theta$ whereas a random bit is received when $\hat{\theta} \neq \theta$. In other words, If Bob announces the transmission basis a the end of the transmission then the BB84 coding scheme implements a Rabin's oblivious transfer [15] from Bob to Alice provided she is honest. Otherwise, Alice can easily cheat the protocol by postponing the measurement until the basis is announced. In this case she gets the transmitted bit all the time. In order to make the BB84 transmission resistant to active adversaries, the CK protocol uses n BB84 transmissions where for each of them, Alice is asked to commit upon the measurements and outcomes prior the announcement of the transmission bases by Bob.

We call *Quantum Measurement Commitment* (or QMC) the primitive that allows Alice to provide Bob with evidences of measurements she claims having performed on n BB84 qubits before the announcement of $\theta \in \{+, \times\}^n$. Implementing a QMC is simply done by sending a string commitment containing $(\hat{\theta}, \hat{b})$ to Bob where $\hat{\theta} \in \{+, \times\}^n$ is the measurements Alice claims having performed and $\hat{b} \in \{0,1\}^n$ are the outcomes. The classical bit encoded in the transmission is defined as the value of some predicate $f(b_1, \ldots, b_n)$. Once the QMC has been performed, Alice should be unable to evaluate $f(b_1, \ldots, b_n)$ even given the knowledge of the transmission bases θ. A *computational collapse* occurred if, given the transmission basis θ, $f(b_1, \ldots, b_n)$ cannot be determined efficiently. The CK protocol constructs a 1-2 QOT from a QMC with $f(b_1, \ldots, b_n) \equiv \oplus_{i=1}^n b_i$. A QMC is therefore a universal primitive for secure 2-party computation (of classical functions).

Our contribution. In this paper, we address the question of determining how the binding property of the string commitment scheme used for implementing a QMC enforces its security. As already pointed out in [7, 6], quantum bit commitment schemes satisfy different binding properties than classical ones. The difference becomes more obvious when string commitments are taken into account. In Sect. 3.1, we generalize the computational binding criteria of [7] to the case where commitments are made to strings of size $\ell \in \Theta(n)$ for n the security parameter, and ℓ some value depending on n. Intuitively, for a class of functions $F \subseteq \{f : \{0,1\}^\ell \rightarrow \{0,1\}^m\}$, with $m < \ell$ both depending on n, we say that a string commitment scheme is F–binding if for all $f \in F$, for all commitment prepared by the sender, and for a random $y \in_R \{0,1\}^m$, the commitment cannot be opened efficiently to any $s \in \{0,1\}^\ell$ such that $f(s) = y$ with success probability significantly better than $1/2^m$. The smaller m is compared to ℓ, the weaker is the F–binding criteria. We relate the security of QMC to a weak form of the F–binding property. We assume that a QMC is made using a computationally binding and unconditionally concealing string commitment containing the bases $\hat{\theta} \in \{+, \times\}^n$ and the results $\hat{b} \in \{0,1\}^n$ obtained by Alice after Bob's transmission of $|b\rangle_\theta$. We then define the security of a QMC by the following game between Alice and Bob. Bob selects a challenge $c \in_R \{0,1\}$. If $c=0$, Alice unveils all measurements and outcomes which Bob verifies (by testing that $\hat{\theta}_i = \theta_i \Rightarrow \hat{b}_i = b_i$). If $c=1$, Bob announces the transmission basis $\theta \in_R \{+,\times\}^n$ and Alice tries to maximize her bias on b's parity. Let $\tilde{p}_s$ be Alice's probability of success when $c=0$ and let $\tilde{\epsilon}$ be Alice's expected bias when $c=1$. First, notice that if $\tilde{p}_s + 2\tilde{\epsilon} = 2$ then the QMC is not accomplishing anything since Alice can always unveil perfectly ($\tilde{p}_s = 1$) and bias the parity of b as she likes ($\tilde{\epsilon} = 1/2$). In this case it is impossible to build a secure OT from that QMC. However, as we will see in Section 3.2, an honest Alice can always achieve $\tilde{p}_s + 2\tilde{\epsilon} = 1$ and thus all adversaries such that $\tilde{p}_s + 2\tilde{\epsilon} \leq 1$ are considered trivial. Our main contribution describes how $\tilde{p}_s$ and $\tilde{\epsilon}$ relate to the $\mathcal{F}_m^n$–binding criteria of the string commitment for $\mathcal{F}_m^n$ a class of functions with *small range* $m \in O(\text{polylog}(n))$. In Sect. 5, we give a black-box reduction of any *good* quantum adversary against QMC into one against the string commitent $\mathcal{F}_m^n$–binding criteria. We show that if $\tilde{p}_s + 4\tilde{\epsilon}^2 \geq 1 + \delta(n)$ for non-negligible $\delta(n)$, then the string commitment is not $\mathcal{F}_m^n$–binding. In Sect. 6, we show that the converse condition $\tilde{\epsilon} \leq \sqrt{1+\delta(n)-\tilde{p}_s}/2$ (for negligible $\delta(n)$) is sufficient to build a secure 1-2 QOT. We construct a 1-2 QOT along the same lines than the CK protocol by invoking $O(n)$ times a QMC built from a $\mathcal{F}_m^n$-binding string commitment scheme. After making sure that $\tilde{p}_s$ is sufficiently close to 1 for a large fraction of all QMC executions, we show how to obtain a correct and private (according the definition of [4] adapted the obvious way to deal with computational security against the receiver) 1-2 QOT.

Our reduction shows that using computationally binding commitments one can enforce a *computational or apparent collapse of quantum information.* Using such a QMC allows to construct a 1-2 QOT that is unconditionally secure against Bob (i.e. the sender) and computationally secure against Alice (i.e. the receiver) provided the string commitment scheme used to construct the QMC is $\mathcal{F}_m^n$-binding. As for the quantum version of the Goldreich-Levin theorem[1] and the computationally binding commitments of [7] and [6], our result clearly indicates that 2-party quantum cryptography in the computational setting can be based upon different if not weaker assumptions than its classical counterpart.

2 Preliminaries

Notations and Tools. In the following, poly(n) stands for any polynomial in n. We write $A(n) < \text{poly}(n)$ for "$A(n)$ is smaller than any polynomial provided n is sufficiently large" and $A(n) \leq \text{poly}(n)$ (resp. $A(n) \geq \text{poly}(n)$) means that $A(n)$ is upper bounded by some polynomial (resp. lower bounded by some polynomial). For $w \in \{0,1\}^n$, $x \preceq w$ means that $x_i = 0$ for all $1 \leq i \leq n$ such that $w_i = 0$ (x belongs to the support of w). We denote by "$\blacklozenge$" the string concatenation operator. For $w \in \{0,1\}^n$, we write $[w] \equiv \oplus_{i=1}^n w_i$. For $w, z \in \{0,1\}^n$, we write $|w|$ for the Hamming weight of w, $\Delta(w,z) = |w \oplus z|$ for the Hamming distance, and $w \odot z \equiv \oplus_{i=1}^n w_i \cdot z_i$ is the boolean inner product. Notation $\|\boldsymbol{u}\|$ denotes the Euclidean norm of $\boldsymbol{u}$ and $\boldsymbol{u}^\dagger$ denotes its complex conjugate transposed. The following well-known identity will be useful,

$$(\forall y \in \{0,1\}^n)[y \neq 0^n \Rightarrow \sum_{x\in\{0,1\}^n} (-1)^{x\odot y} = 0]. \tag{1}$$

Next lemma, proven in Appendix A, provides a generalization of the parallelogram identity:

Lemma 1. *Let $A \subseteq \{0,1\}^n$ be a set of bitstrings. Let $\{\boldsymbol{v}_{w,z}\}_{w,z}$ be any family of vectors indexed by $w \in \{0,1\}^n$ and $z \in A$ that satisfies,*

$$(\forall s,t \in \{0,1\}^n, s \neq t)[\sum_w \sum_{\substack{z_1\in A: w\oplus z_1 = s\\ z_2 \in A: w\oplus z_2 = t}} (-1)^{w\odot(z_1\oplus z_2)} \langle \boldsymbol{v}_{w,z_1}, \boldsymbol{v}_{w,z_2}\rangle = 0] \tag{2}$$

Then,

$$\sum_w \| \sum_{z\in A} (-1)^{w\odot z} \boldsymbol{v}_{w,z}\|^2 = \sum_{w\in\{0,1\}^n} \sum_{z\in A} \|\boldsymbol{v}_{w,z}\|^2. \tag{3}$$

Finally, for $\theta, b \in \{0,1\}^n$, we define $\Delta_{\preceq}(\theta,b) = \{(\hat{\theta},\hat{b}) \in \{0,1\}^n \times \{0,1\}^n | (\forall i, 1 \leq i \leq n)[\hat{\theta}_i = \theta_i \Rightarrow \hat{b}_i = b_i]\}$. It is easy to verify that $\#\Delta_{\preceq}(\theta,b) = 3^n$ and that $(\theta\oplus\tau, b\oplus\beta) \in \Delta_{\preceq}(\theta,b)$ iff $\beta \preceq \tau$.

Quantum Stuff. The basis $\{\,|0\rangle, |1\rangle\}$ denotes the computational or rectilinear or "+" basis for $\mathcal{H}_2$. When the context requires, we write $|b\rangle_+$ to denote the bit b in the rectilinear basis. The diagonal basis, denoted "×", is defined as $\{\,|0\rangle_\times, |1\rangle_\times\}$ where $|0\rangle_\times = \frac{1}{\sqrt{2}}(\,|0\rangle + |1\rangle)$ and $|1\rangle_\times = \frac{1}{\sqrt{2}}(\,|0\rangle - |1\rangle)$. States $|0\rangle$, $|1\rangle$, $|0\rangle_\times$ and $|1\rangle_\times$ are the four BB84 states. For any $x \in \{0,1\}^n$ and $\theta \in \{+,\times\}^n$, the state $|x\rangle_\theta$ is defined as $\otimes_{i=1}^n |x_i\rangle_{\theta_i}$. In the following, we write $\mathbb{P}_{+,0} \equiv \mathbb{P}_0 = |0\rangle\langle 0|$, $\mathbb{P}_{+,1} \equiv \mathbb{P}_1 = |1\rangle\langle 1|$, $\mathbb{P}_{\times,0} = |0\rangle_\times\langle 0|$ and $\mathbb{P}_{\times,1} = |1\rangle_\times\langle 1|$ for the projections along the four BB84 states. We define measurements $\mathbb{M}_+ \equiv \{\mathbb{P}_0, \mathbb{P}_1\}$ and $\mathbb{M}_\times \equiv \{\mathbb{P}_{\times,0}, \mathbb{P}_{\times,1}\}$ allowing to distinguish the BB84 encoded bit in the computational and diagonal basis respectively. For $\theta \in \{+,\times\}^n$, measurement $\mathbb{M}_\theta$ is the composition of measurements $\mathbb{M}_{\theta_i}$ for $1 \leq i \leq n$. In order to simplify the notation, we sometimes associate the rectilinear basis "+" with bit 0 and the diagonal basis with bit 1. We map sequences of rectilinear and diagonal bases into bitstrings the obvious way.

We refer to [7, 6] for a more complete description of how quantum protocols are modeled by quantum circuits. We denote by $\mathcal{UG}$ an universal set of quantum gates. The complexity of a quantum circuit C is simply the number $\|C\|_{\mathcal{UG}}$ of elementary gates in C. In the following, we use the two Pauli (unitary) transformations σ_X (bit flip) and σ_Z (conditional phase shift) defined for $b \in \{0,1\}$ as, $\sigma_X : |b\rangle \mapsto |1-b\rangle$ and $\sigma_Z : |b\rangle \mapsto (-1)^b |b\rangle$. Assuming U is a one qubit operation and $s \in \{0,1\}^n$, we write $U^{\otimes s} = \otimes_{i=1}^n U_i$ where $U_i = \mathbb{1}_2$ if $s_i = 0$ and $U_i = U$ if $s_i = 1$. $U^{\otimes s}$ is therefore a conditional application of U on each of n registers depending upon the value of s. The maximally entangled state $|\Phi_n^+\rangle = 2^{-n/2}\sum_{x\in\{0,1\}^n} |x\rangle \otimes |x\rangle$ will be useful in our reduction. This state can easily be constructed from scratch by a circuit of $O(n)$ elementary gates.

3 Definitions

3.1 Computationally Binding Quantum String Commitment

In the following we shall always refer to $\mathcal{A}$ as the sender and $\mathcal{B}$ as the receiver of some commitment. Such a scheme can be specified by two families of protocols $\mathcal{C}^{AB} = \{(C_n^A, C_n^B)\}_{n>0}$, and $\mathcal{O}^{AB} = \{(O_n^A, O_n^B)\}_{n>0}$ where each pair defined $\mathcal{A}$'s and $\mathcal{B}$'s circuits for the committing and the opening phase respectively. A ℓ-string commitment allows to commit upon strings of length ℓ for n a security parameter. The committing stage generates the state $|\psi_s\rangle = (C_n^A \odot C_n^B)\, |s\rangle^A\, |0\rangle^B$ when $\mathcal{A}$ commits to $s \in \{0,1\}^\ell$. The opening stage is executed from the shared state $|\psi_s\rangle$ and produces $|\psi_{final}\rangle = (O_n^A \odot O_n^B)\, |\psi_s\rangle$. In [7], a natural security criteria for computationally binding but otherwise concealing quantum bit commitment schemes was introduced. In the following, we generalize this approach for string commitment schemes.

An adversary $\tilde{\mathcal{A}} = \{(\tilde{C}_n^A, \tilde{O}_n^A)\}_{n>0}$ for the binding condition is such that $|\tilde{\psi}\rangle = (\tilde{C}_n^A \odot C_n^B)\, |0\rangle^A\, |0\rangle^B$ is generated during the committing stage. The dishonest opening circuit $\tilde{O}_n^A$ tries to open $s \in \{0,1\}^l$ given as an extra input in state $|s\rangle^X$. Given the final state $|\tilde{\psi}_{final}\rangle = (\tilde{O}_n^A \odot O_n^B)\, |s\rangle^X\, |\tilde{\psi}\rangle^{AB}$ we define $\tilde{p}_s(n)$ as the probability to open $s \in \{0,1\}^\ell$ with success. More precisely, $\tilde{p}_s(n) = \|\mathbb{Q}_s^B\, |\tilde{\psi}_{final}\rangle\|^2$ where $\mathbb{Q}_s^B$ is $\mathcal{B}$'s projection operator on the subspace leading to accept the opening of s. The main difference between quantum and classical commitments is the impossibility in the quantum case to determine the committed string s after the committing phase of the protocol. Classically, this can be done by fixing the parties' random tapes so s becomes uniquely determined. In other words, a quantum adversary able to open any string s with probability $p(s)$ is not necessarily able to compute simultaneously the openings of all or even a subset of all strings s. In particular, classical security proof techniques like rewinding have no quantum analogue[8, 17]. A committer (to a concealing commitment) can always commit upon any superposition of values for s that will remain such until the opening phase. A honest committer does not necessarily know a single string that can be unveiled with non-negligible probability of success. Suppose a quantum ℓ–string commitment scheme has committing circuit $C_n^A \odot C_n^B$ and let $|\psi(s)\rangle^{AB} = (C_n^A \odot C_n^B)\, |s\rangle^A\, |0\rangle^B$. If the committer starts with superposition $\sum_s \sqrt{\tilde{p}_s(n)}\, |s\rangle$, for any probability distribution $\{(\tilde{p}_s(n), s)\}_{s\in\{0,1\}^\ell}$, then the state obtained after the committing phase would be:

$$\sum_{s\in\{0,1\}^\ell} \sqrt{\tilde{p}_s(n)}\, |\psi(s)\rangle^{AB} = C_n^A \odot C_n^B \left(\Big(\sum_{s\in\{0,1\}^\ell} \sqrt{\tilde{p}_s(n)}\, |s\rangle^A \Big) \otimes\, |0\rangle^B \right). \quad (4)$$

Equation (4) is a valid commitment to a superposition of strings that will always allow the sender to unveil s with probability $\tilde{p}_s(n)$. The *honest* strategy described in (4) achieves $\sum_s \tilde{p}_s(n) = 1$. In [7], the binding condition is satisfied if no adversary can do significantly better than what is achievable by (4) in the special case $\ell = 1$. More precisely, a bit commitment scheme is computationally binding if for all poly-time adversaries $\tilde{\mathcal{A}}$:

$$\tilde{p}_0(n) + \tilde{p}_1(n) < 1 + 1/\text{poly}(n) \tag{5}$$

where $\tilde{p}_b(n)$ is the probability for $\tilde{\mathcal{A}}$ to open bit b with success. Extending this definition to the case where $\ell \in \Theta(n)$ must be done with care however. The obvious generalization of (5) to the requirement $\sum_{s\in\{0,1\}^\ell} \tilde{p}_s(n) < 1+1/\text{poly}(n)$ is too strong whenever $\ell \in \Theta(n)$. For example, if $\ell = n$ and $\tilde{p}_s(n) = 2^{-n}(1 + \frac{1}{p(n)})$ for all strings $s \in \{0,1\}^n$ then $\tilde{\mathcal{A}}$'s behavior is indistinguishable in polynomial time from what is achievable with the *honest* state (4) resulting from distribution $\{(2^{-n}, s)\}_s$. Any such attack that cannot be distinguished from the honest behavior should hardly be considered successful. On the other hand, defining a successful adversary $\tilde{\mathcal{A}}$ as one who can open s and s' ($s \neq s'$) such that $\tilde{p}_s(n) + \tilde{p}_{s'}(n) \geq 1 + 1/p(n)$ is in general too weak when one tries to reduce the security of a protocol to the security of the string commitment used by that protocol (as we shall see for QMCs). Breaking a protocol could be reduced to breaking the string commitment scheme in a more subtle way. In general, the possibility to commit upon several strings in superposition can be used by the adversary to make his attack against the binding condition even more peculiar. Instead of trying to open a particular string $s \in \{0,1\}^\ell$, an attacker could be interested in opening any $s \in \{0,1\}^\ell$ such that $f(s) = y$ for some function $f : \{0,1\}^\ell \rightarrow \{0,1\}^m$ with $m \leq \ell$. Henceforth, we call such an attack an **f-attack**. We shall see in the following that the *security* of QMC is guaranteed provided the string commitment does not allow the committer to mount such an f-attack for any $f \in F$ where F is a special class of functions. Such an adversary is defined by a family of interactive quantum circuits $\tilde{\mathcal{A}}^f = \{(\tilde{C}_n^A, \tilde{O}_n^A)\}_{n>0}$ such that $|\tilde{\psi}\rangle = (\tilde{C}_n^A \odot C_n^B)\,|0\rangle^A\,|0\rangle^B$ is the state generated during the committing phase of the protocol and $|\tilde{\psi}(y)\rangle = (\tilde{O}_n^A \odot O_n^B)\,|y\rangle^X\,|\tilde{\psi}\rangle^{AB}$ is the state (hopefully) allowing to open $s \in \{0,1\}^\ell$ such that $f(s) = y$. The probability to succeed during the opening stage is,

$$\tilde{p}_y^f(n) = \| \sum_{s\in\{0,1\}^\ell : f(s)=y} \mathbb{Q}_s^B\,|\tilde{\psi}(y)\rangle\|^2, \tag{6}$$

where $\mathbb{Q}_s^B$ is $\mathcal{B}$'s projector operator leading to accept the opening of $s \in \{0,1\}^\ell$. The following binding criteria takes into account such attacks:

Definition 1. *Let $F \subseteq \{f : \{0,1\}^\ell \rightarrow \{0,1\}^m\}$ be a set of functions where $m \leq \ell$. A ℓ-string commitment scheme is* computationally F-binding *if for any $f \in F$ and any adversary $\tilde{\mathcal{A}}^f$ such that $\|\tilde{\mathcal{A}}^f\|_{\mathcal{UG}} \leq poly(n)$, we have*

$$\sum_{y\in\{0,1\}^m} \tilde{p}_y^f(n) < 1 + 1/poly(n) \text{ where } \tilde{p}_y^f(n) \text{ is defined as in (6).} \tag{7}$$

Notice that all natural attacks can be expressed by an appropriate class of functions F. In general, the smaller m is with respect to ℓ, the weaker is the

F–binding criteria. A class of functions of particular interest is built out of $s_1(x,y) = x, s_2(x,y) = y$, and $s_3(x,y) = x \oplus y$ for all $x, y \in \{0,1\}$. Let $\mathcal{I}_m^n$ be the set of subsets of $\{1,\ldots,n\}$ having size m. For $I \in \mathcal{I}_m^n$, let $S_I^n = \{s : \{0,1\}^{2n} \rightarrow \{0,1\}^m | (\exists j \in \{1,2,3\}^m)(\forall x, y \in \{0,1\}^n)[s(x,y) = \blacklozenge_{h\in I} s_{j_h}(x_h, y_h)]\}$, we define:

$$\mathcal{F}_m^n = \left\{f : \{0,1\}^{2n} \rightarrow \{0,1\}^m | (\exists I \in \mathcal{I}_m^n)[f \in S_I^n]\right\} .$$

In other words, $\mathcal{F}_m^n$ contains the set of functions f such that each of the m output bit of $f(x,y)$ is a bit of either x or y or $x \oplus y$. Notice that no quantum string commitment has been formally shown F-binding for a non-trivial F. We believe however that the commitment of [6] can be turned into a $\mathcal{F}_m^n$-binding string commitment for *small* m but this analysis is beyond the scope of this paper.

3.2 Commitment to Quantum Measurement

Quantum Measurement Commitment (QMC) is a primitive allowing the receiver of random qubits to show the sender that they have been measured without disclosing any further information (i.e. unconditionally) about the measurement and the outcome. As discussed in the Sect. 1, this primitive is the main ingredient in order to provide security in 1-2 QOT against the receiver $\mathcal{A}$. In this paper we restrict our attention to quantum transmission of random BB84 qubits. The measurements performed by the receiver are, for each transmission, independently chosen in $\{\mathbb{M}_+, \mathbb{M}_\times\}$. We model QMCs by the following game between the sender $\mathcal{B}$ and the receiver $\mathcal{A}$:

1. $\mathcal{B}$ sends n random BB84 qubits in state $|b\rangle_\theta$ for $b \in_R \{0,1\}^n$ and $\theta \in_R \{+,\times\}^n$,
2. $\mathcal{A}$ applies measurement $\mathbb{M}_{\hat{\theta}}$ for $\hat{\theta} \in_R \{+,\times\}^n$ producing classical outcome $\hat{b} \in \{0,1\}^n$,
3. $\mathcal{A}$ uses a $2n$-string commitment in order to commit to $(\hat{\theta}, \hat{b})$ toward $\mathcal{B}$,
4. $\mathcal{B}$ picks and announces a random challenge $c \in_R \{0,1\}$,
   - If $c = 0$ then $\mathcal{A}$ opens $(\hat{\theta}, \hat{b})$ and $\mathcal{B}$ verifies that $\hat{b}_i = b_i$ for all i such that $\hat{\theta}_i = \theta_i$, otherwise $\mathcal{B}$ ABORTS,
   - If $c = 1$ then $\mathcal{B}$ announces θ and $\mathcal{A}$ tries to bias $[b]$.

$\mathcal{A}$ wants to maximize both her success probability when unveiling and the bias on $[b]$ whenever θ is announced. This is almost identical to the receiver's situation in the CK protocol[5]. Since we only consider unconditionally concealing string commitments, $\mathcal{B}$ gets information about $\mathcal{A}$'s measurements and results only if they are unveiled. As we shall see next, this flavor of commitments allows $\mathcal{A}$ to postpone her measurement until the unveiling stage. The commitment stage should nevertheless ensure $\mathcal{B}$ that $\mathcal{A}$ cannot use this ability for improving her situation compared to the case where she measures completely before committing. In other words, although this flavor of commitment cannot force $\mathcal{A}$ to measure upon the committing stage, it should do as such through the actions of a computationally bounded $\mathcal{A}$.

We model the adversary $\tilde{\mathcal{A}}$ by a family of interactive quantum circuits $\tilde{\mathcal{A}} = \{(\tilde{C}_n^A, \tilde{O}_n^A, \tilde{E}_n)\}_{n>0}$ where $\tilde{C}_n^A$ and $\tilde{O}_n^A$ are $\tilde{\mathcal{A}}$'s circuits for the committing and the opening phases. Circuit $\tilde{E}_n$ allows to extract the parity of b upon the announcement of basis θ. Circuit $\tilde{C}_n^A$ works upon $\tilde{\mathcal{A}}$'s internal registers H_A together with the register $H_{channel}$ storing the BB84 qubits. We denote by

$$|\psi_{\theta,b}\rangle^{AB} = (\tilde{C}_n^A \odot C_n^B)\, |b\rangle_\theta^{channel}, \tag{8}$$

the resulting state after the committing phase (step 3). This state should allow $\tilde{\mathcal{A}}$ to succeed both challenges with *good* probability. By linearity, we have that for all $\theta, b, x \in \{0,1\}^n$,

$$|\psi_{\theta,b}\rangle = 2^{-\frac{|x|}{2}} \sum_{y: y \preceq x} (-1)^{b\odot x \oplus b \odot y}\, |\psi_{\theta\oplus x, b\oplus y}\rangle, \tag{9}$$

where $\theta \oplus x$ defines a new basis in which $|\psi_{\theta,b}\rangle$ is represented. The probability to open with success $\tilde{p}^{ok}_{(\theta,b)}(n)$, when $|b\rangle_\theta$ was sent, is

$$\tilde{p}^{ok}_{(\theta,b)}(n) = \sum_{(\hat{\theta},\hat{b})\in \Delta_{\preceq}(\theta,b)} \|\mathbb{Q}^B_{(\hat{\theta},\hat{b})}(\tilde{O}_n^A \odot O_n^B)\, |\psi_{\theta,b}\rangle\|^2 = \|\mathbb{Q}^*_{(\theta,b)}\, |\psi_{\theta,b}\rangle\|^2, \tag{10}$$

for $\mathbb{Q}^B_{(\hat{\theta},\hat{b})}$ the projection operator applied upon $\mathcal{B}$'s registers and leading to a valid opening of $(\hat{\theta},\hat{b}) \in \{0,1\}^{2n}$. The opening of $(\hat{\theta},\hat{b})$ is accepted by $\mathcal{B}$ iff $(\hat{\theta},\hat{b}) \in \Delta_{\preceq}(\theta,b)$. For simplicity, circuits $\tilde{O}_n^A \odot O_n^B$ can be included in the description of $\mathbb{Q}^B_{(\hat{\theta},\hat{b})}$ so the opening process can be seen as a single projection $\mathbb{Q}^*_{(\theta,b)} = \sum_{(\hat{\theta},\hat{b})\in\Delta_{\preceq}(\theta,b)} \mathbb{Q}^B_{(\hat{\theta},\hat{b})}$. Therefore, the expected probability of success $\tilde{p}^{ok}(n)$ is,

$$\tilde{p}^{ok}(n) = \frac{1}{4^n} \sum_{b\in\{0,1\}^n} \sum_{\theta\in\{+,\times\}^n} \tilde{p}^{ok}_{(\theta,b)}(n). \tag{11}$$

When $c = 1$, $\tilde{\mathcal{A}}$ should be able, given the announcement of θ, to extract information about the parity $[b]$.The extractor $\tilde{E}_n$ has access to an extra register H_Θ storing the basis $\theta \in \{+,\times\}^n$. The extractor stores the guess for $[b]$ in register $H_\oplus$. The bias $\tilde{\varepsilon}_{\theta,b}(n)$ provided by the extractor when the qubits were initially in state $|b\rangle_\theta$ is

$$\frac{1}{2} + \tilde{\varepsilon}_{\theta,b}(n) = \|\mathbb{P}^\oplus_{[b]}(\tilde{E}_n \otimes \mathbb{1}_B)\, |\theta\rangle^\Theta\, |0\rangle^\oplus\, |\psi_{\theta,b}\rangle^{AB}\|^2, \tag{12}$$

where $\mathbb{P}^\oplus_{[b]}$ is applied upon the output register $H_\oplus$. The expected value $\tilde{\varepsilon}(n)$ for the bias provided by $\tilde{E}_n$ is simply,

$$\tilde{\varepsilon}(n) = \frac{1}{4^n} \sum_{b\in\{0,1\}^n} \sum_{\theta\in\{+,\times\}^n} \tilde{\varepsilon}_{\theta,b}(n). \tag{13}$$

We characterize $\tilde{\mathcal{A}}$'s behavior against QMC by both $\tilde{p}^{ok}(n)$ and $\tilde{\varepsilon}(n)$. Independently of the string commitment scheme used, there always exists $\tilde{\mathcal{A}}^*$ preparing a superposition of attacks that 1) succeeds with probability 1 during the opening and 2) provides $[b]$ with certainty. Such an attack can be implemented as follows:

$$|\psi^*_{\theta,b}\rangle = \alpha(C_n^A \odot C_n^B)\,|b\rangle_\theta^{channel} + \beta(C_n^A \odot C_n^B)\,|0^n\rangle_{+^n}^{channel} \tag{14}$$

where $|\alpha|^2+|\beta|^2 = 1$ and C_n^A and C_n^B are the honest circuits for committing. The state $|\psi^*_{\theta,b}\rangle$ is a superposition of the honest behavior with probability $|\alpha|^2$ and the trivial attack consisting in not measuring the qubits received with probability $|\beta|^2$. The expected probability of success $p^*(n)$ is

$$p^*(n) = |\alpha|^2 + |\beta|^2(\frac{3}{4})^n \approx |\alpha|^2 \tag{15}$$

since with probability $|\alpha|^2$ an honest QMC was executed and with probability $|\beta|^2$ a QMC to the fixed state $|0^n\rangle_\theta$ was made. In the later case, the probability to pass $\mathcal{B}$'s test is $(3/4)^n$. The expected bias satisfies

$$\varepsilon^*(n) = \frac{|\alpha|^2}{2}(\frac{1}{2})^n + \frac{|\beta|^2}{2} \approx \frac{|\beta|^2}{2} \tag{16}$$

since with probability $|\alpha|^2$ a QMC to $|b\rangle_\theta$ is recovered (in which case a nonzero bias on $[b]$ occurs only when $\hat{\theta} = \theta$) and with probability $|\beta|^2$ a QMC to a dummy value is made thus allowing to extract $[b]$ perfectly. Such an attack does not enable the committer to break the binding property of the string commitment but nevertheless achieves: $p^*(n)+2\varepsilon^*(n) > 1$. We define two flavors of adversaries against QMC. The first flavor captures any adversary that achieves anything better than the trivial adversary $\tilde{\mathcal{A}}^*$ defined in (14). The second flavor captures stronger adversaries for which our reduction will be shown to produce attacks against the $\mathcal{F}_m^n$–binding property of the string commitment.

Definition 2. *An adversary* $\tilde{\mathcal{A}} = \{(\tilde{C}_n^A, \tilde{O}_n^A, \tilde{E}_n)\}_{n>0}$ *against QMC is* $\delta(n)$–non-trivial *if* $\tilde{p}^{ok}(n) + 2\tilde{\varepsilon}(n) \geq 1 + \delta(n)$, *and* $\delta(n)$–good *if* $\tilde{p}^{ok}(n) + 4\tilde{\varepsilon}(n)^2 \geq 1 + \delta(n)$ *for* $\tilde{p}^{ok}(n)$ *and* $\tilde{\varepsilon}(n)$ *defined as in (11) and (13) respectively.*

Notice that if $\tilde{\mathcal{A}}$ is not $\delta(n)$-good (or $\delta(n)$-non-trivial) then an upper bound on the expected bias $\tilde{\varepsilon}(n)$ can be obtained from a lower bound on $\tilde{p}^{ok}(n)$. This is how we use QMCs for implementing oblivious transfer in Sect. 6.

4 The Reduction

Using a *good* adversary $\tilde{\mathcal{A}}$ against QMC, we would like to build an adversary against the $\mathcal{F}_m^n$-binding property of the underlying string commitment. In this section, we provide the first step of the reduction given that $\tilde{\mathcal{A}}$'s parity extractor is perfect (i.e. it always returns the parity of the committed string). We construct a circuit built from $\tilde{\mathcal{A}}$ allowing to prepare a commitment into which any $|\psi_{\theta,b}\rangle$ can be inserted efficiently at the opening stage. In Sect. 5, we show how to use this circuit for attacking the binding property of the string commitment.

4.1 The Switching Circuit

Let $\tilde{\mathcal{A}} = \{(\tilde{C}_n^A, \tilde{O}_n^A, \tilde{E}_n)\}_{n>0}$ be an adversary in QMC. We call H_{Keep} the register kept by $\tilde{A}$ after the committing phase. We denote by H_B the register containing what is sent by $\mathcal{A}$ and kept by $\mathcal{B}$ after the committing phase. $H_Q \simeq \mathcal{H}_{2^n}$ denotes the register containing the BB84 qubits before the commitment, $H_\Theta \simeq \mathcal{H}_{2^n}$ denotes the register for the basis given as input to the extractor, and $H_\oplus \simeq \mathcal{H}_2$ denotes the register in which the guess on $[b]$ is stored by the extractor.

Instead of running $\tilde{C}_n \equiv (\tilde{C}_n^A \odot C_n^B)$ upon some BB84 qubits, we run it with the maximally entangled state $|\Phi_n^+\rangle$ where the first half is stored in H_Θ and the second half stored in H_Q. Therefore, the basis given as input to the extractor is not a classical state but is rather entangled with register H_Q containing the qubits $\tilde{A}$ is committed upon. After the execution of $\tilde{C}_n\, |\Phi_n^+\rangle^{\Theta,Q}$, transformations $B^{\otimes b}$ and $T^{\otimes \theta}$ are applied to register H_Θ in order to prepare the input for the extractor where, $B = \sigma_X\, \sigma_Z$ and $T = \mathtt{H}\, \sigma_Z$. $\tilde{E}_n$ is then run before σ_Z is applied upon the extractor's output register $H_\oplus$. The transformation is completed by running the extractor in reverse. The resulting circuit, shown in Fig. 1, is called the *switching circuit*. Next, we see that whenever the parity extractor is perfect,

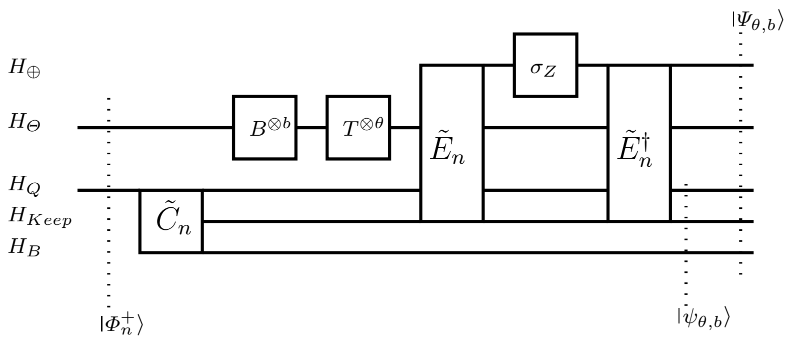

Fig. 1. The Switching Circuit

the instance of the switching circuit using transformations $B^{\otimes b}$ and $T^{\otimes \theta}$ generates $|\psi_{\theta,b}\rangle$. To see this, we follow its evolution from the initial state $|\Phi_n^+\rangle$. We first look at the state generated before the extractor is applied,

$$|\Phi_n^+\rangle \equiv \sum_s \frac{1}{\sqrt{2}^n}\,|s\rangle\,|s\rangle \overset{\tilde{C}_n}{\longmapsto} \sum_s \frac{1}{\sqrt{2}^n}\,|s\rangle\,|\psi_{+^n,s}\rangle \overset{B^{\otimes b}}{\longmapsto} \sum_s \frac{(-1)^{b\odot s}}{\sqrt{2}^n}\,|b\oplus s\rangle\,|\psi_{+^n,s}\rangle$$

$$\overset{T^{\otimes\theta}}{\longmapsto} \sum_{s,t\,:\,t\preceq\theta} \frac{(-1)^{b\odot s\,\oplus\, b\odot t\,\oplus\, s\odot t}}{\sqrt{2}^{n+|\theta|}}\,|b\oplus s\oplus t\rangle\,|\psi_{+^n,s}\rangle \tag{17}$$

$$= \sum_{\substack{s,t,v\,:\, t\preceq\theta \\ v\preceq b\oplus s\oplus t}} \frac{(-1)^{b\odot t\,\oplus\, s\odot v\,\oplus\, s\odot s}}{\sqrt{2}^{n+|\theta|+|b\oplus s\oplus t|}}\,|b\oplus s\oplus t\rangle\,|\psi_{b\oplus s\oplus t,s\oplus v}\rangle. \tag{18}$$

The states up to (17) are obtained by definition of $|\Phi_n^+\rangle, \tilde{C}_n, B^{\otimes b}$, and $T^{\otimes\theta}$. Equation (18) follows after changing the basis from $+^n$ to $b \oplus s \oplus t$ using (9). From (18), we follow the evolution through $\tilde{E}_n^\dagger \sigma_Z \tilde{E}_n$,

$$
\begin{aligned}
T^{\otimes\theta} B^{\otimes b} \mathcal{C}_n \,|\Phi_n^+\rangle \overset{\tilde{E}_n^\dagger \sigma_z \tilde{E}_n}{\longmapsto} & \sum_{\substack{s,t,v\,:\, t\preceq\theta \\ v\preceq b\oplus s\oplus t}} \frac{(-1)^{b\odot t\,\oplus\, s\odot v\,\oplus\, v\odot v}}{\sqrt{2}^{n+|\theta|+|b\oplus s\oplus t|}} \,|b\oplus s\oplus t\rangle^{\Theta}\, |\psi_{b\oplus s\oplus t, s\oplus v}\rangle & (19)\\
= & \sum_{\substack{x,y,v\,:\, v\oplus x\oplus y\preceq\theta \\ v\preceq\theta\oplus x}} \frac{(-1)^{b\odot\theta\,\oplus\, b\odot x\,\oplus\, b\odot y\,\oplus\, v\odot y}}{\sqrt{2}^{n+|\theta|+|\theta\oplus x|}} \,|\theta\oplus x\rangle^{\Theta}\, |\psi_{\theta\oplus x, b\oplus y}\rangle & (20)\\
= & \sum_{y\preceq x} \frac{(-1)^{b\odot\theta\,\oplus\, b\odot x\,\oplus\, b\odot y}}{\sqrt{2}^{n+|\theta|+|\theta\oplus x|-2|\theta\wedge\bar{x}|}} \,|\theta\oplus x\rangle^{\Theta}\, |\psi_{\theta\oplus x, b\oplus y}\rangle & \\
= & \sum_{y\preceq x} \frac{(-1)^{b\odot\theta\,\oplus\, b\odot x\,\oplus\, b\odot y}}{\sqrt{2}^{n+|x|}} \,|\theta\oplus x\rangle^{\Theta}\, |\psi_{\theta\oplus x, b\oplus y}\rangle & (21)\\
= & \sum_{x} \frac{(-1)^{b\odot\theta}}{\sqrt{2}^{n}} \,|\theta\oplus x\rangle^{\Theta} \otimes \sum_{y\,:\,y\preceq x} \frac{(-1)^{b\odot x\,\oplus\, b\odot y}}{\sqrt{2}^{|x|}} \,|\psi_{\theta\oplus x, b\oplus y}\rangle & \\
= & \sum_{x} \frac{(-1)^{b\odot\theta}}{\sqrt{2}^{n}} \,|\theta\oplus x\rangle^{\Theta}\, |\psi_{\theta,b}\rangle \equiv |\Psi_{\theta,b}\rangle. & (22)
\end{aligned}
$$

Notice that in addition to H_Θ, $\tilde{E}_n$ acts upon another extra register $H_\oplus$ ignored in the above derivation. W.l.g one may assume it is included in the Hilbert space where $|\psi_{\theta,b}\rangle$ belongs. Equation (19) follows from the fact that the extractor is perfect. Equation (20) follows after a reorganizing the terms of the sum. Equation (21) follows after using (1). We finally get (22) using (9).

In conclusion, a perfect extractor allows to produce a commitment inside which any $|\psi_{\theta,b}\rangle$ can be put *efficiently* even when θ and b are chosen after the end of the committing phase.

5 Analysis

We analyze the switching circuit when it is run with imperfect parity extractors. We first show how states $\{|\tilde{\Psi}_{\theta,b}\rangle\}_{\theta,b}$, produced in this case, overlap with states $\{|\Psi_{\theta,b}\rangle\}_{\theta,b}$ generated when perfect extractors are available. In Sect. 5.2, we represent the behavior of the switching circuit by a table. In Sect. 5.3, we relate this table to attacks against the $\mathcal{F}_m^n$–binding property of the string commitment.

5.1 Generalization to Imperfect Extractors

Assume the adversary $\tilde{\mathcal{A}} = \{(\tilde{C}_n^A, \tilde{O}_n^A, \tilde{E}_n)\}_{n>0}$ has access to an imperfect extractor. In this case, $\tilde{E}_n$ is modeled as follows:

$$
\tilde{E}_n\,|\theta\rangle^{\Theta}\,|\psi_{\theta,b}\rangle = |\theta\rangle^{\Theta} \otimes \left(\gamma_{\theta,b}\,|[b]\rangle^{\oplus}\,|\varphi_{\theta,b}\rangle + \hat{\gamma}_{\theta,b}\,|1\oplus[b]\rangle^{\oplus}\,|\hat{\varphi}_{\theta,b}\rangle\right). \qquad (23)
$$

Without loss of generality, we may assume that both $\gamma_{\theta,b}$ and $\hat{\gamma}_{\theta,b}$ are real positive numbers such that $|\gamma_{\theta,b}|^2 \geq \frac{1}{2}$ (i.e. arbitrary phases can be added to $|\varphi_{\theta,b}\rangle$ and $|\hat{\varphi}_{\theta,b}\rangle$). According (13), the expected bias provided by $\tilde{E}_n$ is,

$$\tilde{\varepsilon}(n) \equiv 4^{-n} \sum_{\theta} \sum_{b} \tilde{\varepsilon}_{\theta,b}(n) = 4^{-n} \sum_{\theta} \sum_{b} \left| |\gamma_{\theta,b}|^2 - \frac{1}{2} \right|. \tag{24}$$

Compared to the case where the extractor is perfect, only the effect of transformation $\tilde{E}_n^{\dagger} \sigma_Z \tilde{E}_n$ needs to be recomputed. From (23), we obtain,

$$(\tilde{E}_n^{\dagger} \sigma_Z \tilde{E}_n) |\theta\rangle |\psi_{\theta,b}\rangle = (-1)^{[b]} |\theta\rangle \otimes (|\psi_{\theta,b}\rangle + \boldsymbol{e}_{\theta,b}), \tag{25}$$

where the *error vector* $\boldsymbol{e}_{\theta,b}$ satisfies $|\theta\rangle \otimes \boldsymbol{e}_{\theta,b} \equiv -2\hat{\gamma}_{\theta,b}\tilde{E}_n^{\dagger}(|\theta\rangle |1 \oplus [b]\rangle^{\oplus} |\hat{\varphi}_{\theta,b}\rangle)$. The final state $|\tilde{\Psi}_{\theta,b}\rangle$, produced by the switching circuit, can be obtained easily from (19) using (25). We get that $|\tilde{\Psi}_{\theta,b}\rangle = \tilde{E}_n^{\dagger} \sigma_z \tilde{E}_n T^{\otimes\theta} B^{\otimes b} \mathcal{C}_n |\Phi_n^+\rangle$ satisfies:

$$|\tilde{\Psi}_{\theta,b}\rangle = \sum_{y \preceq x} \frac{(-1)^{b\odot\theta \,\oplus\, b\odot x \,\oplus\, b\odot y}}{\sqrt{2}^{n+|x|}} |\theta \oplus x\rangle \otimes (|\psi_{\theta\oplus x, b\oplus y}\rangle + \boldsymbol{e}_{\theta\oplus x, b\oplus y}). \tag{26}$$

Splitting the inner sum of (26) after distributing the tensor product gives,

$$|\tilde{\Psi}_{\theta,b}\rangle = |\Psi_{\theta,b}\rangle + \boldsymbol{F}_{\theta,b}. \tag{27}$$

The first part $|\Psi_{\theta,b}\rangle = (2^{-n/2} \sum_x (-1)^{b\odot\theta} |\theta\rangle) \otimes |\psi_{\theta,b}\rangle$ is exactly what one gets when the switching circuit is run with a perfect extractor (see (22)). The second part is the error term for which next lemma gives a characterization.

Lemma 2. *Consider the switching circuit built from adversary* $\tilde{\mathcal{A}} = \{(\tilde{C}_n^A, \tilde{O}_n^A, \tilde{E}_n)\}_{n>0}$. *Then,*

$$4^{-n} \sum_{\theta} \sum_{b} \|\boldsymbol{F}_{\theta,b}\|^2 \leq 2 - 4\tilde{\varepsilon}(n).$$

Proof. Let θ be fixed. Using the definition of $\boldsymbol{F}_{\theta,b}$, we get

$$\begin{aligned} 2^{-n} \sum_{b\in\{0,1\}^n} \|\boldsymbol{F}_{\theta,b}\|^2 &= 2^{-n} \sum_{b} \Big\| \sum_{y\preceq x} \frac{(-1)^{b\odot\theta\oplus b\odot x\oplus b\odot y}}{\sqrt{2}^{n+|x|}} |\theta\oplus x\rangle \otimes \boldsymbol{e}_{\theta\oplus x, b\oplus y} \Big\|^2 \\ &= 2^{-n} \sum_{b} \Big\| \sum_{x} \frac{(-1)^{b\odot\theta\oplus b\odot x}}{\sqrt{2}^{n+|x|}} |\theta\oplus x\rangle \sum_{y: y\preceq x} (-1)^{b\odot y} \boldsymbol{e}_{\theta\oplus x, b\oplus y} \Big\|^2 \\ &= 2^{-2n-|x|} \sum_{x} \sum_{b} \Big\| \sum_{y:y\preceq x} (-1)^{b\odot y} \boldsymbol{e}_{\theta\oplus x, b\oplus y} \Big\|^2, \end{aligned} \tag{28}$$

where (28) is obtained from the orthogonality of all $\boldsymbol{e}_{\theta\oplus x, b\oplus y}$ when x varies, and from Pythagoras theorem. We now apply Lemma 1 to (28) with $A = \{y \in \{0,1\}^n | y \preceq x\}$, $w \equiv b, z \equiv y$, and $\boldsymbol{v}_{w,z} \equiv \boldsymbol{e}_{\theta\oplus x, b\oplus y}$. We first verify that the condition expressed in (2) is satisfied:

$$\sum_b \sum_{y_1 \in A: b\oplus y_1 = s} \sum_{y_2 \in A: b \oplus y_2 = t} (-1)^{b\odot(y_1 \oplus y_2)} \langle \boldsymbol{e}_{\theta\oplus x, b\oplus y_1}, \boldsymbol{e}_{\theta \oplus x, b\oplus y_2}\rangle =$$
$$\langle \boldsymbol{e}_{\theta\oplus x, s}, \boldsymbol{e}_{\theta\oplus x, t}\rangle \sum_{\substack{b: \\ b\oplus s \preceq x, b\oplus t \preceq x}} (-1)^{b\odot(s\oplus t)} = 0,$$

from an identity equivalent to (1) since b runs aver all substrings in the support of $s \oplus t \preceq x$. We therefore apply the conclusion of Lemma 1 to get that for all $x \in \{0,1\}^n$,

$$\sum_b \| \sum_{y: y\preceq x} (-1)^{b\odot y} \boldsymbol{e}_{\theta\oplus x, b\oplus y}\|^2 = \sum_{y:y\preceq x} \sum_b \|\boldsymbol{e}_{\theta\oplus x, b\oplus y}\|^2 \leq 2^{n+|x|}(2-4\tilde{\varepsilon}(n)). \quad (29)$$

The result follows after replacing (29) in (28). □

Using Lemma 2, we show how the the output of the switching circuit with imperfect extractors approaches the one with perfect extractors. Next lemma gives an upper bound on the expected overlap between the states produced using perfect and imperfect extractors.

Lemma 3. *Let $\tilde{\mathcal{A}} = \{(\tilde{C}_n^A, \tilde{O}_n^A, \tilde{E}_n)\}_{n>0}$ be the circuits for the adversary such that the extractor $\tilde{E}_n$ has expected bias $\tilde{\varepsilon}(n)$. Then, the set of states $\{ |\tilde{\Psi}_{\theta,b}\rangle\}_{b,\theta}$ produced by the switching circuit satisfies,*

$$S_{\tilde{\mathcal{A}}} = 4^{-n} \sum_{b,\theta} |\langle \tilde{\Psi}_{\theta,b} | \Psi_{\theta,b}\rangle| \geq 2\tilde{\varepsilon}(n).$$

Proof. According (27), we can write $|\tilde{\Psi}_{\theta,b}\rangle = |\Psi_{\theta,b}\rangle + \boldsymbol{F}_{\theta,b} = (1-\alpha_{\theta,b})|\Psi_{\theta,b}\rangle + \beta_{\theta,b}|\Psi_{\theta,b}^{\perp}\rangle$, where $1 = \| |\tilde{\Psi}_{\theta,b}\rangle\|^2 = |(1-\alpha_{\theta,b})|^2 + |\beta_{\theta,b}|^2$ and $\langle \Psi_{\theta,b}|\Psi_{\theta,b}^{\perp}\rangle = 0$. Isolating $|\alpha_{\theta,b}|$ and using the fact that $|\alpha_{\theta,b}|^2 + |\beta_{\theta,b}|^2 = \|\boldsymbol{F}_{\theta,b}\|^2$ gives $|\alpha_{\theta,b}| = \frac{\|\boldsymbol{F}_{\theta,b}\|^2}{2}$ which, after invoking Lemma 2, leads to $S_{\tilde{\mathcal{A}}} = \sum_{\theta,b} 4^{-n} |\langle \tilde{\Psi}_{\theta,b}|\Psi_{\theta,b}\rangle| \geq \sum_{\theta,b} 4^{-n}(1-|\alpha_{\theta,b}|) = 1 - \sum_{\theta,b} 4^{-n}\frac{\|\boldsymbol{F}_{\theta,b}\|^2}{2} \geq 2\tilde{\varepsilon}(n)$. □

Lemma 3 tells us that with *good* extractors, one can generate states having *large* overlap (in the expected sense) with all QMCs to different BB84 qubits which states are chosen at the beginning of the opening stage (i.e. after the end of the committing phase). It remains to show how to use this ability to break the binding property. This second and last step of our reduction is addressed in next section.

5.2 Representing The Switching Circuit by a Table

In this section, we look at how to invoke the switching circuit in order to attack the binding property of the string commitment. Remember first that $|\psi_{\theta,b}\rangle$ has probability $\tilde{p}^{ok}_{(\theta,b)}(n) = \|\mathbb{Q}^*_{(\theta,b)} |\psi_{\theta,b}\rangle\|^2$ to open a valid QMC to $|b\rangle_\theta$ where $\mathbb{Q}^*_{(\theta,b)}$ is defined as in (10). Remember that a valid opening of $|b\rangle_\theta$ consists in the opening of any $2n$–bit string $(\hat{\theta}, \hat{b}) \in \Delta_{\preceq}(\theta, b)$. We take advantage of the structure of $\Delta_{\preceq}(\theta, b)$ in order to exhibit attacks against the binding condition.

Suppose first that adversary $\tilde{\mathcal{A}}$ has access to a perfect parity extractor E_n. From Sect. 4.1, such an adversary can generate $|\psi_{\theta,b}\rangle$ for any choice of $\theta \in \{+, \times\}^n$ and $b \in \{0,1\}^n$. Each of 4^n sets of valid announcements $\Delta_{\preceq}(\theta, b)$ is of size $\#\Delta_{\preceq}(\theta, b) = 3^n$. We define a table of positive real numbers having 4^n rows and 3^n columns where each row is labeled by a pair (θ, b). The row (θ, b) contains values $T_{\theta,b}(\tau, \beta) = \|\mathbb{Q}^B_{(\theta\oplus\tau, b\oplus\beta)} |\psi_{\theta,b}\rangle\|^2$ for all (τ, β) such that $(\theta \oplus \tau, b \oplus \beta) \in \Delta_{\preceq}(\theta, b)$. This condition is equivalent to (τ, β) such that $\beta \preceq \tau$. The table values for the case $n = 1$ are shown in Fig. 2. The sum of each row is added to the right. The construction is easily generalized for arbitrary n in which case, each

$$
\begin{array}{ccc|c}
\|\mathbb{Q}^B_{(+,0)} |\psi_{+,0}\rangle\|^2 & \|\mathbb{Q}^B_{(\times,0)} |\psi_{+,0}\rangle\|^2 & \|\mathbb{Q}^B_{(\times,1)} |\psi_{+,0}\rangle\|^2 & \tilde{p}^{ok}_{(+,0)}(n) = \|\mathbb{Q}^*_{(+,0)} |\psi_{+,0}\rangle\|^2 \\
\|\mathbb{Q}^B_{(+,1)} |\psi_{+,1}\rangle\|^2 & \|\mathbb{Q}^B_{(\times,1)} |\psi_{+,1}\rangle\|^2 & \|\mathbb{Q}^B_{(\times,0)} |\psi_{+,1}\rangle\|^2 & \tilde{p}^{ok}_{(+,1)}(n) = \|\mathbb{Q}^*_{(+,1)} |\psi_{+,1}\rangle\|^2 \\
\|\mathbb{Q}^B_{(\times,0)} |\psi_{\times,0}\rangle\|^2 & \|\mathbb{Q}^B_{(+,0)} |\psi_{\times,0}\rangle\|^2 & \|\mathbb{Q}^B_{(+,1)} |\psi_{\times,0}\rangle\|^2 & \tilde{p}^{ok}_{(\times,0)}(n) = \|\mathbb{Q}^*_{(\times,0)} |\psi_{\times,0}\rangle\|^2 \\
\|\mathbb{Q}^B_{(\times,1)} |\psi_{\times,1}\rangle\|^2 & \|\mathbb{Q}^B_{(+,1)} |\psi_{\times,1}\rangle\|^2 & \|\mathbb{Q}^B_{(+,0)} |\psi_{\times,1}\rangle\|^2 & \tilde{p}^{ok}_{(\times,1)}(n) = \|\mathbb{Q}^*_{(\times,1)} |\psi_{\times,1}\rangle\|^2
\end{array}
$$

Fig. 2. The table for the case $n = 1$ and perfect extractor.

column contains 4^n orthogonal projectors applied to the 4^n states $\{|\psi_{\theta,b}\rangle\}_{\theta,b}$. The sum of all values in the table is simply $4^n \tilde{p}^{ok}(n) = \sum_{\theta,b} \tilde{p}^{ok}_{(\theta,b)}(n)$.

The table is defined similarly for imperfect parity extractors. In this case, table $T_{\tilde{\mathcal{A}}} = \{T_{\theta,b}(\tau, \beta)\}_{\theta,b,\tau,\beta\preceq\tau}$ associated with adversary $\tilde{\mathcal{A}}$ contains elements,

$$T_{\theta,b}(\tau, \beta) = \|\mathbb{Q}^B_{(\theta\oplus\tau, b\oplus\beta)} |\tilde{\Psi}_{\theta,b}\rangle\|^2. \tag{30}$$

While for perfect extractors the sum over all elements in the table is at least $4^n \tilde{p}^{ok}(n)$, next theorem shows that any table $T_{\tilde{\mathcal{A}}}$ built from a $\delta(n)$–good adversary adds up to $4^n \text{poly}(\delta(n))$. The proof follows easily from Lemma 3 and can be found in Appendix B.

Theorem 1. *If $\tilde{\mathcal{A}} = \{(\tilde{C}^A_n, \tilde{O}^A_n, \tilde{E}_n)\}_{n>0}$ is a $\delta(n)$–good adversary against QMC and $T_{\tilde{\mathcal{A}}} = \{T_{\theta,b}(\tau, \beta)\}_{\theta,b,\tau,\beta\preceq\tau}$ is its associated table, then*

$$\sum_{\theta,b,\tau} \sum_{\beta\preceq\tau} T_{\theta,b}(\tau, \beta) \geq \frac{4^n \delta(n)^3}{32}. \tag{31}$$

Theorem 1 establishes the existence of one column in $T_{\tilde{\mathcal{A}}}$ providing a *weak* attack since any table with 3^n columns all summing up to more than $\frac{4^n \delta(n)^3}{32}$ has one column exceeding $(\frac{4}{3})^n \frac{\delta(n)^2}{32} \gg 1 + 1/\text{poly}(n)$. Let (τ, β) be such a column and consider the class of functions containing only the identity $\mathbb{1}_{2n}$. For $(y, y') \in \{0,1\}^{2n}$, the state $|\tilde{\Psi}_{y\oplus\tau, y'\oplus\beta}\rangle$ can be generated using the switching circuit. The probability to unveil (y, y') is $T_{y\oplus\tau, y'\oplus\beta}(\tau, \beta) = \|\mathbb{Q}^B_{(y,y')} |\tilde{\Psi}_{y\oplus\tau, y'\oplus\beta}\rangle\|^2$. By construction, we have $\sum_{(y,y')} \tilde{p}^f_{(y,y')}(n) = \sum_{(y,y')} T_{y\oplus\tau,y'\oplus\beta}(\tau,\beta) > 1+1/\text{poly}(n)$ which provides an attack against the string commitment's $\mathbb{1}_{2n}$–binding property in accordance with (7). As we pointed out in Sect. 3.1 however, this attack might not even be statistically distinguishable from the trivial adversary. This implies that proving a string commitment computationally $\mathbb{1}_{2n}$-binding would be impossible. In the next section, we find stronger attacks allowing to relax the binding property required for secure QMC.

5.3 Strong Attacks Against the String Commitment

We now show that the table $T_{\tilde{\mathcal{A}}}$, built out of any $\delta(n)$–good adversary $\tilde{\mathcal{A}}$, contains an attack against the $\mathcal{F}^n_m$–binding property of the $2n$–string commitment with $m \in O(\text{polylog}(n))$ whenever $\delta(n) \geq 1/\text{poly}(n)$. We show this using a counting argument. We cover uniformly the table $T_{\tilde{\mathcal{A}}}$ with all attacks in $\mathcal{F}^n_m$. Theorem 1 is then invoked in order to conclude that for some $f \in \mathcal{F}^n_m$, condition (7) does not hold.

Attacking the binding condition according to a function $f \in \mathcal{F}^n_m$ is done by grouping columns in $T_{\tilde{\mathcal{A}}}$ as described in (6) and discussed in more details in Appendix C. The number of lines involved in such an attack is clearly 2^m while the number of columns can be shown to be $2^m 3^{n-m}$ (for information see Appendix C and Lemma 4 below). This means that any attack in $\mathcal{F}^n_m$ covers $t = 3^{n-m}4^m$ elements in $T_{\tilde{\mathcal{A}}}$. The quality of such an attack is characterized by the sum of all elements in the sub-array defined by the attack since this sum corresponds to the value of (7). Let $t_{\tilde{\mathcal{A}}} = 3^n 4^n$ be the total number of elements in $T_{\tilde{\mathcal{A}}}$ and let $s_{\tilde{\mathcal{A}}}$ be its sum. The following lemma, proved in Appendix D, shows that all attacks in $\mathcal{F}^n_m$ cover $T_{\tilde{\mathcal{A}}}$ uniformly:

Lemma 4. *All f-attacks with $f \in \mathcal{F}^n_m$ cover $T_{\tilde{\mathcal{A}}}$ uniformly, that is, each element in $T_{\tilde{\mathcal{A}}}$ belongs to exactly $a = C(m,n)4^m$ attacks each of size $t = 3^{n-m}4^m$.*

Let s^* be the maximum of (7) for all f-attacks with $f \in \mathcal{F}^n_m$. Clearly, $a \cdot s^* \geq \frac{a \cdot t \cdot s_{\tilde{\mathcal{A}}}}{t_{\tilde{\mathcal{A}}}}$ since by Lemma 4, the covering of $T_{\tilde{\mathcal{A}}}$ by $f \in \mathcal{F}^n_m$ is uniform and $a \cdot t/t_{\tilde{\mathcal{A}}}$ is the number of times $T_{\tilde{\mathcal{A}}}$ is generated by attacks in $\mathcal{F}^n_m$. In other words,

$$a \cdot s^* \geq \frac{a \cdot t \cdot s_{\tilde{\mathcal{A}}}}{t_{\tilde{\mathcal{A}}}} = \frac{a \cdot t \cdot s_{\tilde{\mathcal{A}}}}{3^n 4^n} \Rightarrow s^* \geq \frac{t \cdot s_{\tilde{\mathcal{A}}}}{3^n 4^n} = \frac{4^m \cdot s_{\tilde{\mathcal{A}}}}{3^m 4^n}. \tag{32}$$

Assuming that $\tilde{\mathcal{A}}$ is $\delta(n)$–good, Theorem 1 tells us that $s_{\tilde{\mathcal{A}}} \geq \frac{4^n \delta(n)^3}{32}$ so (32) implies that,

$$s^* \geq \frac{\delta(n)^3 4^m}{32 \cdot 3^m} \geq 1 + 1/\text{poly}(n), \tag{33}$$

for any $m \geq \lceil \log_{\frac{4}{3}} \left(\frac{32}{\delta(n)^3} \right) \rceil$. Equation (33) guarantees that for at least one $f \in \mathcal{F}^n_m$, condition (7) is not satisfied thereby providing an attack against the $\mathcal{F}^n_m$–binding criteria. Moreover, since $\delta(n) \geq 1/\text{poly}(n)$ it is sufficient that $m \in O(\text{polylog}(n))$. It follows that at least one f-attack in $\mathcal{F}^n_m$ is statistically distinguishable from any trivial one.

6 The Main Result and Its Application

Putting together Theorem 1 and (33) leads to our main result:

Theorem 2 (Main). *Any $\delta(n)$–good adversary $\tilde{\mathcal{A}}$ against QMC can break the $\mathcal{F}_m^n$–binding property of the string commitment it is built upon for $m \in O(\log \frac{1}{\delta(n)})$ using a circuit of size $O(\|\tilde{\mathcal{A}}\|_{\mathcal{UG}})$.*

Theorem 2 can be applied for the construction of 1-2 QOT in the computational setting. We can use QMCs for building a weak 1-2 QOT such that:

– the sender has no information about the receiver's selection bit and,
– the receiver, according Theorem 2, can only extract a limited amount of information about both bits.

This *weak flavor* of 1-2 QOT is easily obtained by the following primitive, called $\mathcal{W}_n$, accepting $\mathcal{B}$'s input bits (β_0, β_1) and $\mathcal{A}$'s selection bit s (i.e this construction is very similar to the CK protocol[5]):

`Protocol` $\mathcal{W}_n$

1. $\mathcal{B}$ and $\mathcal{A}$ run the committing phase of a QMC (i.e. built from a $\mathcal{F}_m^n$-binding string commitment scheme) upon $|b\rangle_\theta$ for $b \in_R \{0,1\}^n, \theta \in_R \{+,\times\}^n$ picked by $\mathcal{B}$,
2. $\mathcal{B}$ chooses $c \in_R \{0,1\}$ and announces it to $\mathcal{A}$,
   – if $c = 0$ then $\mathcal{A}$ unveils the QMC, if UNVEIL SUCCEEDS then $\mathcal{A}$ and $\mathcal{B}$ return to 1 otherwise $\mathcal{B}$ ABORTS,
   – if $c = 1$ then $\mathcal{B}$ announces θ, $\mathcal{A}$ announces a partition $I_0, I_1 \subseteq \{1,\ldots,n\}$ such that for all $i \in I_s$ the measurements were made in basis $\hat{\theta}_i = \theta_i$, then $\mathcal{B}$ announces $a_0, a_1 \in \{0,1\}$ s.t. $\beta_0 = a_0 \oplus_{i \in I_0} b_i$ and $\beta_1 = \oplus_{i \in I_1} b_i$:
      • $\mathcal{A}$ does her best to guess $(\hat{b}_0, \hat{b}_1) \approx (\bigoplus_{i \in I_0} b_i, \bigoplus_{i \in I_1} b_i)$.

Clearly, $\mathcal{W}_n$ is a correct 1-2 QOT since an honest receiver $\mathcal{A}$ can always get bit $\beta_s = b_s \oplus a_s$. $\tilde{\mathcal{A}}$'s information about the other bit can be further reduced using the following simple protocol accepting $\mathcal{B}$'s input bits (β_0, β_1) and the selection bit s for the honest receiver:

`Protocol` $\mathsf{R\text{-}Reduce}(t, \mathcal{W}_n)$

1. $\mathcal{W}$ is executed t times, with random inputs $(\beta_{0i}, \beta_{1i}), i = 1..t$ for the sender and input s for the receiver such that $\beta_{01} \oplus \ldots \oplus \beta_{0t} = \beta_0$ and $\beta_{11} \oplus \ldots \oplus \beta_{1t} = \beta_1$.
2. The receiver computes the XOR of all bits received, that is $\beta_s = \oplus_{i=1}^t \beta_{si}$.

Classically, it is straightforward to see that the receiver's information about one-out-of-two bit decreases exponentially in t. We say that a quantum adversary $\tilde{\mathcal{A}}$ against $\mathsf{R\text{-}Reduce}(t, \mathcal{W}_n)$ is *promising* if it runs in poly-time and the probability to complete the execution is non-negligible. Using Theorem 2, it is not difficult to show that $\tilde{\mathcal{A}}$'s information about one of the transmitted bits also decreases exponentially in t whenever $\tilde{\mathcal{A}}$ is promising:

Theorem 3. *For any promising receiver $\tilde{\mathcal{A}}$ in $\mathsf{R\text{-}Reduce}(t, \mathcal{W}_n)$ and for all executions, there exists $\tilde{s} \in \{0,1\}$ such that $\tilde{\mathcal{A}}$'s expected bias on $\beta_{\tilde{s}}$ is negligible in t (even given β_s).*

A sketch of proof can be found in Appendix E. It relies upon the fact that any promising adversary must run almost all $\mathcal{W}_n$ with $\tilde{p}^{ok}(n) > 1 - \delta$ for any $\delta > 0$. Using Theorem 2, this means that independently for each of those executions $1 \leq i \leq t$, one bit $\beta_{\tilde{s}i}$ out of (β_{0i}, β_{1i}) cannot be guessed with bias better than $\varepsilon_{max}(\delta) << \frac{1}{2}$. In this case, the bias on $\beta_{\tilde{s}}$ can be shown to be negligible in t.

Clearly, the sender $\mathcal{B}$ in $\mathsf{R\text{-}Reduce}(t, \mathcal{W}_n)$ cannot get any non-negligible amount of information about $\mathcal{A}$'s selection bit when the commitments are statistically concealing. This remark together with Theorem 3 and the correctness of $\mathsf{R\text{-}Reduce}(t, \mathcal{W}_n)$ lead to:

Corollary 1. *A correct and private 1-2 QOT can be based upon any $\mathcal{F}_m^n$-binding and statistically concealing quantum string commitment scheme. The resulting 1-2 QOT statistically hides the selection bit and computationally hides one out of two transmitted bits.*

In other words, building 1-2 QOT upon Theorem 2 allows for an easy security proof in the computational setting. Our analysis assumes for simplicity that $\mathcal{A}$ and $\mathcal{B}$ have access to a perfect quantum channel. Nevertheless, noise may be tolerated if we construct 1-2 QOT along the lines of BBCS [3] instead of CK [5].

7 Open Questions

An obvious open problem is how to build $\mathcal{F}_m^n$-string commitments from computationally binding bit commitment schemes. In particular, how one can transform the computationally binding bit commitments of [7] and [6] into $\mathcal{F}_m^n$–binding string commitments? This would show that QMCs and therefore 1-2 QOT can be based upon any one-way permutation[7] and/or any one-way function[6]. It is an open question whether or not Theorem 2 holds for $\delta(n)$–non-trivial adversaries against QMC. Such an extension would show that our reduction from an adversary to QMC into one against the binding condition is to some extent optimal. It is also of interest to find attacks against weaker binding properties.

Finally, it would be very interesting to formally prove the security of the CK protocol using Theorem 2. This would result in a proof of security that, in addition to apply in the computational setting, would be based upon a completely different approach than Yao's proof [19]. Moreover, the CK protocol is more practical than our construction since it only requires a constant number of rounds with fewer qubits transmitted (i.e. $\Theta(n)$ vs. $\Theta(tn)$). It would also be useful to prove Corollary 1 in the case where the quantum channel is noisy.

References

1. Adcock, M.,and R. Cleve, "A Quantum Goldreich-Levin Theorem with Cryptographic Applications", In *proceedings of 19th International Symposium on Theoretical Aspects of Computer Science (STACS 2002)*,LNCS, vol. 2285,Springer-Verlag, 2002, pp. 323–334.

2. Bennett, C. H., and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, 1984, pp. 175–179.
3. Bennett, C. H., G. Brassard, C. Crépeau and M.-H. Skubiszewska, "Practical Quantum Oblivious Transfer", In *Advances in Cryptology –CRYPTO'91 : Proceedings*, LNCS, vol. 576, Springer-Verlag, 1992, pp. 362–371.
4. Crépeau, C., "Quantum Oblivious Transfer", *Journal of Modern Optics*, vol. 41, no 12, 1994, pp. 2445–2454.
5. Crépeau, C. and J. Kilian, "Achieving oblivious transfer using weakened security assumptions", *Proceedings of 29th IEEE Symposium on the Foundations of Computer Science*, 1988, pp. 42–52.
6. Crépeau, C., F. Légaré, and L. Salvail, "How to Convert the Flavor of a Quantum Bit Commitment", In *Advances in Cryptology –EUROCRYPT'01 : Proceedings*, LNCS, vol. 2045, Springer-Verlag, 2001, pp. 60–77.
7. Dumais, P., D. Mayers, and L. Salvail, "Perfectly Concealing Quantum Bit Commitment From Any Quantum One-Way Permutation", In *Advances in Cryptology –EUROCRYPT'00 : Proceedings*, LNCS, vol. 1807, Springer-Verlag, 2000, pp. 300–315.
8. van de Graaf, J., *Towards a Formal Definition of Security for Quantum Protocols*, Ph.D. thesis, Computer Science and Operational Research Department, Université de Montréal, 1997.
9. Impagliazzo, R. and S. Rudich, "Limits on Provable Consequences of One-Way Permutations", In *Advances in Cryptology –CRYPTO'88 : Proceedings*, LNCS, vol. 403, Springer-Verlag, 1989, pp. 2–7.
10. Lo, H.–K.,and H. F. Chau, "Is quantum Bit Commitment Really Possible?", *Physical Review Letters*, vol. 78, no 17, 1997, pp. 3410–3413.
11. Mayers, D., "The Trouble With Quantum Bit Commitment", available at `http://xxx.lanl.gov/abs/quant-ph/9603015`, 1996.
12. Mayers, D., "Quantum Key Distribution and String Oblivious Transfer in Noisy Channels", In *Advances in Cryptology –CRYPTO'96 : Proceedings*, LNCS, vol. 1109 , Springer-Verlag, 1996, pp. 343–357.
13. Mayers, D., "Unconditionally Secure Quantum Bit Commitment is Impossible", *Physical Review Letters*, vol. 78, no 17, 1997, pp. 3414–3417.
14. Mayers, D., and L. Salvail,"Quantum Oblivious Transfer is Secure Against All Individual Measurements", In *Proceedings of the Workshop on Physics and Computationm, PhysComp'94*, Dallas, 1994, pp. 69–77.
15. Rabin, M. O., "How to exchange secrets by oblivious transfer", *Technical Memo TR–81*, Aiken Computation Laboratory, Harvard University, 1981.
16. Salvail, L., "Quantum Bit Commitment From a Physical Assumption", In *Advances in Cryptology –CRYPTO'98 : Proceedings*, LNCS, vol. 1462 , Springer-Verlag, 1998, pp. 338–354.
17. Watrous, J, "Limits on the Power of Quantum Statistical Zero-Knowledge", *Proceedings of the 43rd Annual Symposium on Foundations of Computer Science*, 2002, pp. 495–504.
18. Yao, A. C., "Theory and Applications of Trapdoor Functions", *Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science*, 1982, pp. 80–91.
19. Yao, A. C., "Security of Quantum Protocols Against Coherent Measurements", *Proceedings of the 27th ACM Symposium on Theory of Computing*, 1995, pp. 67–75.

A Proof of Lemma 2

First, we prove the following related claim:

Claim. Let $\{\boldsymbol{u}_{w,z}\}_{w,z}$ be any family of vectors, indexed by $w, z \in \{0,1\}^n$, that satisfies,

$$(\forall s, t \in \{0,1\}^n, s \neq t)[\sum_w \sum_{\substack{z_1 : w \oplus z_1 = s \\ z_2 : w \oplus z_2 = t}} (-1)^{w \odot (z_1 \oplus z_2)} \langle \boldsymbol{u}_{w,z_1}, \boldsymbol{u}_{w,z_2} \rangle = 0] \tag{34}$$

Then,

$$\sum_w \| \sum_z (-1)^{w \odot z} \boldsymbol{u}_{w,z} \|^2 = \sum_{w,z \in \{0,1\}^n} \| \boldsymbol{u}_{w,z} \|^2. \tag{35}$$

Proof. We carry out the calculation for (35):

$$\begin{aligned} \sum_w \| \sum_z (-1)^{w \odot z} \boldsymbol{u}_{w,z} \|^2 &= \sum_w \langle \sum_{z_1} (-1)^{w \odot z_1} \boldsymbol{u}_{w,z_1}, \sum_{z_2} (-1)^{w \odot z_2} \boldsymbol{u}_{w,z_2} \rangle \\ &= \sum_{w,z_1,z_2} (-1)^{w \odot (z_1 \oplus z_2)} \langle \boldsymbol{u}_{w,z_1}, \boldsymbol{u}_{w,z_2} \rangle \\ &= \sum_{w,z} \| \boldsymbol{u}_{w,z} \|^2 + \sum_{w,z_1,z_2 : z_1 \neq z_2} (-1)^{w \odot (z_1 \oplus z_2)} \langle \boldsymbol{u}_{w,z_1}, \boldsymbol{u}_{w,z_2} \rangle . \end{aligned} \tag{36}$$

We now re-arrange the terms in the right-hand part of (36):

$$\begin{aligned} \sum_{w,z_1,z_2 : z_1 \neq z_2} (-1)^{w \odot (z_1 \oplus z_2)} \langle \boldsymbol{u}_{w,z_1}, \boldsymbol{u}_{w,z_2} \rangle &= \sum_{w,z_1} \sum_{z_2 : z_2 \neq z_1} (-1)^{w (z_1 \oplus z_2)} \sum_{\substack{s : w \oplus z_1 = s \\ t : w \oplus z_2 = t}} \langle \boldsymbol{u}_{w,z_1}, \boldsymbol{u}_{w,z_2} \rangle \\ &= \sum_{\substack{s,t : s \neq t \\ w}} \sum_{\substack{z_1 : w \oplus z_1 = s \\ z_2 : w \oplus z_2 = t}} (-1)^{w (z_1 \oplus z_2)} \langle \boldsymbol{u}_{w,z_1}, \boldsymbol{u}_{w,z_2} \rangle \\ &= 0, \end{aligned} \tag{37}$$

where (37) follows from condition (34). Replacing (37) in (36) concludes the proof. □

Proof (Lemma 1). Follows from the Claim after setting $\boldsymbol{u}_{w,z} = \boldsymbol{v}_{w,z}$ if $z \notin A$ and $\boldsymbol{u}_{w,z} = 0$ if $z \in A$. It is easy to verify that if condition (2) is satisfied by $\{\boldsymbol{v}_{w,z}\}_{w,z}$ then $\{\boldsymbol{u}_{w,z}\}_{w,z}$ satisfies (34). Our result then follows from (35). □

B Proof of Theorem 1

Proof. We use Lemma 3 together with the fact that $\tilde{\mathcal{A}}$ is $\delta(n)$–good. From Lemma 3, any $\delta(n)$–good adversary is such that,

$$\tilde{p}^{ok}(n) + \sum_{\theta,b} 4^{-n} | \langle \Psi_{\theta,b} | \tilde{\Psi}_{\theta,b} \rangle |^2 =$$

$$4^{-n}\sum_{\theta,b}\left(\tilde{p}^{ok}_{(\theta,b)}(n)+|\langle\Psi_{\theta,b}|\tilde{\Psi}_{\theta,b}\rangle|^2\right)\geq 1+\delta(n). \tag{38}$$

Let $\delta_{\theta,b}=\tilde{p}^{ok}_{(\theta,b)}(n)+|\langle\Psi_{\theta,b}|\tilde{\Psi}_{\theta,b}\rangle|^2-1$ be such that $\delta=4^{-n}\sum_{\theta,b}\delta_{\theta,b}$. The sum of any row $(\theta,b)\in T_{\tilde{\mathcal{A}}}$ is given by,

$$\|\mathbb{Q}^*_{(\theta,b)}\,|\tilde{\Psi}_{\theta,b}\rangle\|^2\geq$$
$$\|\mathbb{Q}^*_{(\theta,b)}\left(|\langle\Psi_{\theta,b}|\tilde{\Psi}_{\theta,b}\rangle|\,|\Psi_{\theta,b}\rangle-\sqrt{1-|\langle\Psi_{\theta,b}|\tilde{\Psi}_{\theta,b}\rangle|^2}\,|\Psi^{\perp}_{\theta,b}\rangle\right)\|^2, \tag{39}$$

where $|\Psi^{\perp}_{\theta,b}\rangle$ is any state orthogonal to $|\Psi_{\theta,b}\rangle$. Now, notice that we can always write $|\Psi_{\theta,b}\rangle=\sqrt{\tilde{p}^{ok}_{(\theta,b)}(n)}\,|\xi_{\theta,b}\rangle+\sqrt{1-\tilde{p}^{ok}_{(\theta,b)}(n)}\,|\xi^{\perp}_{\theta,b}\rangle$ for $|\xi_{\theta,b}\rangle=\mathbb{Q}^*_{(\theta,b)}\,|\Psi_{\theta,b}\rangle/\sqrt{\tilde{p}^{ok}_{(\theta,b)}(n)}$ and $|\xi^{\perp}_{\theta,b}\rangle=(\mathbb{1}-\mathbb{Q}^*_{(\theta,b)})\,|\Psi_{\theta,b}\rangle/\sqrt{1-\tilde{p}^{ok}_{(\theta,b)}(n)}$. We can also write $|\Psi^{\perp}_{\theta,b}\rangle=\alpha_{\theta,b}\,|\xi_{\theta,b}\rangle+\beta_{\theta,b}\,|\xi^{\perp}_{\theta,b}\rangle+\zeta_{\theta,b}\,|\Lambda_{\theta,b}\rangle$ where $|\Lambda_{\theta,b}\rangle$ is orthogonal to both $|\xi_{\theta,b}\rangle$ and $|\xi^{\perp}_{\theta,b}\rangle$ and where $|\alpha_{\theta,b}|^2+|\beta_{\theta,b}|^2+|\zeta_{\theta,b}|^2=1$. Since by construction $\langle\Psi_{\theta,b}|\Psi^{\perp}_{\theta,b}\rangle=0$, it is easy to verify that $|\alpha_{\theta,b}|\leq\sqrt{1-\tilde{p}^{ok}_{(\theta,b)}(n)}$. In order to simplify the notation, we let $c_{\theta,b}=\langle\Psi_{\theta,b}|\tilde{\Psi}_{\theta,b}\rangle$. Using the above observations, we re-write (39) as,

$$\|\mathbb{Q}^*_{(\theta,b)}\,|\tilde{\Psi}_{\theta,b}\rangle\|^2\geq\|(c_{\theta,b}\sqrt{\tilde{p}^{ok}_{(\theta,b)}(n)}-\sqrt{(1-|c_{\theta,b}|^2)(1-\tilde{p}^{ok}_{(\theta,b)}(n))})\,|\xi_{\theta,b}\rangle\|^2 \tag{40}$$
$$=\left(\sqrt{|c_{\theta,b}|^2\tilde{p}^{ok}_{(\theta,b)}(n)}-\sqrt{(1-|c_{\theta,b}|^2)(1-\tilde{p}^{ok}_{(\theta,b)}(n))}\right)^2$$
$$=\left(\sqrt{|c_{\theta,b}|^2\tilde{p}^{ok}_{(\theta,b)}(n)}-\sqrt{|c_{\theta,b}|^2\tilde{p}^{ok}_{(\theta,b)}(n)-\delta_{\theta,b}}\right)^2 \tag{41}$$
$$\geq\frac{\delta^2_{\theta,b}}{4}, \tag{42}$$

where (40) comes from definitions of $|\Psi_{\theta,b}\rangle$ and $|\tilde{\Psi}_{\theta,b}\rangle$ in terms of $|\xi_{\theta,b}\rangle$, (41) comes from the definition of $\delta_{\theta,b}$, and (42) follows from the fact that $(\sqrt{a}-\sqrt{a-b})^2\geq b^2/4$ for any $0\leq b\leq a\leq 1$. Since $\tilde{\mathcal{A}}$ is $\delta(n)$–good, we use (38) to conclude that the set $G=\{(\theta,b)|\delta_{\theta,b}\geq\delta(n)/2\}$ must satisfy $\#G\geq 4^n\delta(n)/2$. Any $(\theta,b)\in G$ is such that (42) is at least $\frac{\delta(n)^2}{4}$. The result follows easily from $\sum_{\theta,b}\|\mathbb{Q}^*_{(\theta,b)}\,|\tilde{\Psi}_{\theta,b}\rangle\|^2\geq\sum_{(\theta,b)\in G}\|\mathbb{Q}^*_{(\theta,b)}\,|\tilde{\Psi}_{\theta,b}\rangle\|^2\geq\frac{4^n\delta(n)^3}{32}$. □

C Implementing an f-attack From the Switching Circuit

In this appendix, we briefly describe how one can use the switching circuit in order to attack the binding property of the string commitment relative to some function $f\in\mathcal{F}^n_m$. We call such an attack an f-attack since its purpose is to try to open $s\in f^{-1}(y)$ for any $y\in\{0,1\}^m$. To make the description easier, let us consider the case $n=1$ resulting in table $T_{\tilde{\mathcal{A}}}$ shown at Fig. 3 (this is

$$
\begin{array}{ccc}
\|\mathbb{Q}^B_{(+,0)}\ |\tilde{\Psi}_{+,0}\rangle\|^2 & \|\mathbb{Q}^B_{(\times,0)}\ |\tilde{\Psi}_{+,0}\rangle\|^2 & \|\mathbb{Q}^B_{(\times,1)}\ |\tilde{\Psi}_{+,0}\rangle\|^2 \\
\|\mathbb{Q}^B_{(+,1)}\ |\tilde{\Psi}_{+,1}\rangle\|^2 & \|\mathbb{Q}^B_{(\times,1)}\ |\tilde{\Psi}_{+,1}\rangle\|^2 & \|\mathbb{Q}^B_{(\times,0)}\ |\tilde{\Psi}_{+,1}\rangle\|^2 \\
\|\mathbb{Q}^B_{(\times,0)}\ |\tilde{\Psi}_{\times,0}\rangle\|^2 & \|\mathbb{Q}^B_{(+,0)}\ |\tilde{\Psi}_{\times,0}\rangle\|^2 & \|\mathbb{Q}^B_{(+,1)}\ |\tilde{\Psi}_{\times,0}\rangle\|^2 \\
\|\mathbb{Q}^B_{(\times,1)}\ |\tilde{\Psi}_{\times,1}\rangle\|^2 & \|\mathbb{Q}^B_{(+,1)}\ |\tilde{\Psi}_{\times,1}\rangle\|^2 & \|\mathbb{Q}^B_{(+,0)}\ |\tilde{\Psi}_{\times,1}\rangle\|^2
\end{array}
$$

Fig. 3. Table $T_{\tilde{\mathcal{A}}}$ for the case $n = 1$.

almost identical to Fig.2). We have seen how the switching circuit allows for generating any state $|\tilde{\Psi}_{\theta,b}\rangle$. Suppose now that the attacker wants to open a string commitment (in this case the string has length 2) according to function $f_1 \in \mathcal{F}_1^n$ defines as $f_1(\theta, b) = b$ for $\theta, b \in \{0, 1\}$. One way consists in generating (using the switching circuit) $|\tilde{\Psi}_{+,0}\rangle$ in order to open $f_1(\theta, b) = 0$ and $|\tilde{\Psi}_{+,1}\rangle$ in order to open $f_1(\theta, b) = 1$. According to (6), the probability to succeed in unveiling s s.t. $f_1(s) = 0$ and $f_1(s) = 1$ satisfies

$$\tilde{p}_0^f(n) = \|(\mathbb{Q}^B_{(+,0)} + \mathbb{Q}^B_{(\times,0)})\ |\tilde{\Psi}_{+,0}\rangle\|^2 \text{ and } \tilde{p}_1^f(n) = \|(\mathbb{Q}^B_{(+,1)} + \mathbb{Q}^B_{(\times,1)})\ |\tilde{\Psi}_{+,1}\rangle\|^2.$$

The quality of this f_1–attack is given by (2). That is, the attack succeed if $\tilde{p}_0^f(n) + \tilde{p}_1^f(n) > 1 + \delta$ for some large enough δ. Looking at Fig. 3, this particular f_1–attack is formed by the 2×2 upper left sub-array of $T_{\tilde{\mathcal{A}}}$. The quality of the attack $\tilde{p}_0^f(n) + \tilde{p}_1^f(n)$ is simply the sum of all elements in the sub-array. The same function f_1 can be attacked using the elements in the lower left 2×2 sub-array of $T_{\tilde{\mathcal{A}}}$. This means that the attacker prepare $|\tilde{\Psi}_{\times,0}\rangle$ and $|\tilde{\Psi}_{\times,1}\rangle$ in order to open $s \in f_1^{-1}(0)$ and $s \in f_1^{-1}(1)$ respectively. In this case, one gets $\tilde{p}_0^f(n) = \|(\mathbb{Q}^B_{(\times,0)} + \mathbb{Q}^B_{(+,0)})\ |\tilde{\Psi}_{\times,0}\rangle\|^2$ and $\tilde{p}_1^f(n) = \|(\mathbb{Q}^B_{(\times,1)} + \mathbb{Q}^B_{(+,1)})\ |\tilde{\Psi}_{\times,1}\rangle\|^2$. There are two other ways to implement an f_1–attack by mixing the first two. The attacker could generate $|\tilde{\Psi}_{+,0}\rangle$ to unveil $s \in f_1^{-1}(0)$ and $|\tilde{\Psi}_{\times,1}\rangle$ to unveil $s \in f_1^{-1}(1)$. Similarly, $|\tilde{\Psi}_{+,1}\rangle$ to unveil $s \in f_1^{-1}(1)$ and $|\tilde{\Psi}_{\times,0}\rangle$ to unveil $s \in f_1^{-1}(0)$ can be used. This adds up to 4 possible implementations of the f_1–attack using the first two columns of $T_{\tilde{\mathcal{A}}}$.

Now consider function $f_2 \in \mathcal{F}_1^n$ defines as $f_2(\theta, b) = \theta$. As for f_1–attacks, there are four f_2–attacks located in the two last columns of $T_{\tilde{\mathcal{A}}}$. In the first case, states $|\tilde{\Psi}_{+,0}\rangle$ and $|\tilde{\Psi}_{\times,0}\rangle$ are generated (by the switching circuit) in order to open $s \in f_2^{-1}(1)$ and $s \in f_2^{-1}(0)$ respectively (using $'+' = 0$ and $'\times' = 1$). We get $\tilde{p}_1^f(n) = \|(\mathbb{Q}^B_{(\times,0)} + \mathbb{Q}^B_{(\times,1)})\ |\tilde{\Psi}_{+,0}\rangle\|^2$ and $\tilde{p}_0^f(n) = \|(\mathbb{Q}^B_{(+,0)} + \mathbb{Q}^B_{(+,1)})\ |\tilde{\Psi}_{\times,0}\rangle\|^2$. The second way of attacking f_2 is by generating states $|\tilde{\Psi}_{+,1}\rangle$ and $|\tilde{\Psi}_{\times,1}\rangle$ in order to open $s \in f_2^{-1}(1)$ and $s \in f_2^{-1}(0)$ respectively. The other two are obtained similarly.

There is only one function left in $\mathcal{F}_1^n$, that is $f_3(\theta, b) = \theta \oplus b$. This one can be attacked in four different ways using the first and third columns in $T_{\tilde{\mathcal{A}}}$. In the first case, states $|\tilde{\Psi}_{+,0}\rangle$ and $|\tilde{\Psi}_{+,1}\rangle$ are generated in order to open $s \in f_3^{-1}(0)$ and $s \in f_3^{-1}(1)$. We get $\tilde{p}_0^f(n) = \|(\mathbb{Q}^B_{(+,0)} + \mathbb{Q}^B_{(\times,1)})\ |\tilde{\Psi}_{+,0}\rangle\|^2$ and $\tilde{p}_1^f(n) = \|(\mathbb{Q}^B_{(+,1)} + \mathbb{Q}^B_{(\times,0)})\ |\tilde{\Psi}_{+,1}\rangle\|^2$. The two others can be found similarly.

Remark that any element in $T_{\tilde{\mathcal{A}}}$ belongs to exactly 4 attacks and that any attack uses exactly 4 elements in $T_{\tilde{\mathcal{A}}}$. This is what we mean when we say that all attacks in $\mathcal{F}_1^n$ covers $T_{\tilde{\mathcal{A}}}$ uniformly. The construction can easily be generalized for arbitrary n. The number of rows of $T_{\tilde{\mathcal{A}}}$ uses in any f–attack ($f \in \mathcal{F}_m^n$) is 2^m and the number of columns is $2^m 3^{n-m}$. That is, the number of elements in $T_{\tilde{\mathcal{A}}}$ involved in such an f–attack is $4^m 3^{n-m}$. As we shall see in Lemma 4, the covering remains uniform for all values of n.

D Proof of Lemma 4

Lemma 4 follows from the combinatorial lemma 5 below. To make the statement of this combinatorial lemma more succinct we first set the stage for it.

Let T be a 4^n lines by 3^n columns array. The lines are indexed by the 4^n strings $(\theta, b) \in \{0,1\}^n \times \{0,1\}^n$. The columns are indexed by the 3^n strings $(\tau, \beta) \in \{0,1\}^n \times \{0,1\}^n$ such that $\beta \preceq \tau$.

We now consider sub-arrays of T. Each sub-array will be composed of cells lying at the intersections of 2^m lines of T and $3^{n-m}2^m$ columns of T. Any choice of the following $3n$ parameters will define a unique sub-array and different choices of parameters will define different sub-arrays:

$$r_1,\ r_2,\ \ldots,\ r_n \in \{0,1,2,3\}, \tag{43}$$

$$u_1,\ u_2,\ \ldots,\ u_n \in \{\mathtt{0},\mathtt{1}\}, \tag{44}$$

$$v_1,\ v_2,\ \ldots,\ v_n \in \{\mathtt{0},\mathtt{1}\} \tag{45}$$

subject to the condition

$$\#\{j\ :\ r_j \neq 0\} = m. \tag{46}$$

Accordingly, there will be $C(m,n)3^m 4^n$ different sub-arrays.

Let us fix a choice for $r_j \in \{0,1,2,3\}$, $u_j, v_j \in \{0,1\}$ for all $j \in \{1,\ldots,n\}$ satisfying (46). We now describe the sub-array defined by that choice. The column (τ, β) is part of the sub-array if and only if:

$$r_j = 0 \Longrightarrow (\tau_j, \beta_j) \in \{(0,0),(1,0),(1,1)\} \qquad \text{i.e.: } \beta_j \preceq \tau_j, \tag{47}$$

$$r_j = 1 \Longrightarrow (\tau_j, \beta_j) \in \{(1,0),(1,1)\} \qquad \text{i.e.: } \tau_j = 1, \tag{48}$$

$$r_j = 2 \Longrightarrow (\tau_j, \beta_j) \in \{(0,0),(1,0)\} \qquad \text{i.e.: } \beta_j = 0, \tag{49}$$

$$r_j = 3 \Longrightarrow (\tau_j, \beta_j) \in \{(0,0),(1,1)\} \qquad \text{i.e.: } \beta_j = \tau_j. \tag{50}$$

The line (θ, b) is part of the sub-array if and only if:

$$r_j = 0 \Longrightarrow (\theta_j, b_j) \in \{(u_j, v_j)\}, \tag{51}$$

$$r_j = 1 \Longrightarrow (\theta_j, b_j) \in \{(0, u_j),(1, v_j)\}, \tag{52}$$

$$r_j = 2 \Longrightarrow (\theta_j, b_j) \in \{(u_j, 0),(v_j, 1)\}, \tag{53}$$

$$r_j = 3 \Longrightarrow (\theta_j, b_j) \in \{(u_j, u_j),(v_j, 1-v_j)\}. \tag{54}$$

One can easily verify that the lines (47) to (54) define a $2^m \times 3^{n-m}2^m$ sub-array, thus containing $3^{n-m}4^m$ cells, and that different choices of the parameters (43) to (45) will lead to different sub-arrays.

We can now state and prove the combinatorial lemma:

Lemma 5. *Every cell (θ, b, τ, β) of T belongs to exactly $C(m,n)4^m$ sub-arrays.*

Proof. Let us fix $j \in \{1, \ldots, n\}$. Figure 4 shows the possible values for (r_j, u_j, v_j) given the value of $(\theta_j, b_j, \tau_j, \beta_j)$. One can verify that, for all j, any 4-tuple

0000	0010	0011	0100	0110	0111	1000	1010	1011	1100	1110	1111
(0, 0, 0)	(0, 0, 0)	(0, 0, 0)									
			(0, 0, 1)	(0, 0, 1)	(0, 0, 1)						
						(0, 1, 0)	(0, 1, 0)	(0, 1, 0)			
									(0, 1, 1)	(0, 1, 1)	(0, 1, 1)
	(1, 0, 0)	(1, 0, 0)					(1, 0, 0)	(1, 0, 0)			
	(1, 0, 1)	(1, 0, 1)								(1, 0, 1)	(1, 0, 1)
				(1, 1, 0)	(1, 1, 0)		(1, 1, 0)	(1, 1, 0)			
				(1, 1, 1)	(1, 1, 1)					(1, 1, 1)	(1, 1, 1)
(2, 0, 0)	(2, 0, 0)		(2, 0, 0)	(2, 0, 0)							
(2, 0, 1)	(2, 0, 1)								(2, 0, 1)	(2, 0, 1)	
			(2, 1, 0)	(2, 1, 0)		(2, 1, 0)	(2, 1, 0)				
						(2, 1, 1)	(2, 1, 1)		(2, 1, 1)	(2, 1, 1)	
(3, 0, 0)		(3, 0, 0)	(3, 0, 0)		(3, 0, 0)						
(3, 0, 1)		(3, 0, 1)				(3, 0, 1)		(3, 0, 1)			
			(3, 1, 0)		(3, 1, 0)				(3, 1, 0)		(3, 1, 0)
						(3, 1, 1)		(3, 1, 1)	(3, 1, 1)		(3, 1, 1)

Fig. 4. Eligible triplets (r_j, u_j, v_j) given $(\theta_j, b_j, \tau_j, \beta_j)$

$(\theta_j, b_j, \tau_j, \beta_j)$ allows exactly 1 triplet (r_j, u_j, v_j) if $r_j = 0$, and exactly 4 if $r_j \neq 0$. From that follows the statement of this combinatorial lemma. $\square$

E Sketch of Proof for Theorem 3

Protocol $\mathcal{W}_n$, which is almost identical to a QMC, is also a weak form of 1−2-OT. Theorem 2 tells us that any efficient adversary $\tilde{\mathcal{A}}$ against $\mathcal{W}_n$ must satisfy:

$$\tilde{p}^{ok}(n) + (2\tilde{\varepsilon}(n))^2 \leq 1 + 1/\mathrm{poly}(n), \tag{55}$$

where $\tilde{p}^{ok}(n)$ is the probability to succeed in challenge $c = 0$ and $\tilde{\varepsilon}(n)$ is the maximum bias on $[b] = b_0 \oplus b_1$ that $\tilde{\mathcal{A}}$ can extract in challenge $c = 1$.

The only difference between $\mathcal{W}_n$ and a QMC (as far as $\tilde{p}^{ok}(n)$ and $\tilde{\varepsilon}(n)$ are concerned) is that in $\mathcal{W}_n$, QMCs are made until challenge $c = 1$ has been reached. Let $\tilde{p}_{abort,\mathcal{W}_n}$ be the probability for $\mathcal{B}$ to abort the execution of $\mathcal{W}_n$. Notice that there is no reason for $\tilde{\mathcal{A}}$ to change $\tilde{p}^{ok}(n)$ during the same execution of $\mathcal{W}_n$ since the challenges are independent and random. We have,

$$\tilde{p}_{abort,\mathcal{W}_n} = \sum_{j=1}^{\infty} 2^{-j} (\tilde{p}^{ok}(n))^{j-1} (1 - \tilde{p}^{ok}(n))$$

$$> \frac{1-\tilde{p}^{ok}(n)}{2} \Rightarrow \tilde{p}^{ok}(n) > 1 - 2\tilde{p}_{abort,\mathcal{W}_n}. \tag{56}$$

Let $\mathcal{I}_n = \{(I_0, I_1) | I_0 \cup I_1 = \{1, \ldots, n\}, I_0 \cap I_1 = \emptyset\}$ be the set of possible announcements for $\tilde{\mathcal{A}}$ in $\mathcal{W}_n$. Let $I = (I_0, I_1) \in \mathcal{I}_n$ be the set of positions announced by $\tilde{\mathcal{A}}$'s during an execution of $\mathcal{W}_n$. We define $f_I(b)$ as the 2-bit output function:

$$f_I(b) \equiv (\bigoplus_{i \in I_0} b_i, \bigoplus_{i \in I_1} b_i).$$

For $s \in \{0,1\}$ and $b \in \{0,1\}^n$, let $h_I(b,s) \equiv f_I(b)_{[s]}$ where $f_I(b)_{[s]}$ denotes the s-th output bit of $f_I(b)$. Let QPoly(n) and QPoly(n,t) be the classes of families of polynomial-size quantum circuits in one and two variables respectively having one-bit output. Let $\mathcal{C}_\delta$ be the non-uniform class of all families of polynomial size quantum circuits allowing to run $\mathcal{W}_n$ with success probability at least $1-\delta$. That is, any family $\{C_n\}_{n>0} \in \mathcal{C}_\delta$ can be used to define the committing phase of an adversary $\tilde{\mathcal{A}} = \{(C_n, \cdot)\}_{n>0}$ against $\mathcal{W}_n$ where C_n allows for $\tilde{p}_{abort,\mathcal{W}_n} \leq \delta$ given n is large enough. For simplicity, we abuse the notation by writing the output state of the committing phase on $|b\rangle_\theta$ as $C_n |b\rangle_\theta$ although formally, C_n is the circuit obtained by combining $\tilde{\mathcal{A}}$'s and $\mathcal{B}$'s interactive circuits. Let G_n be a quantum circuit with a one-bit output register so $G_n \cdot (C_n |b\rangle_\theta)$ defines a probability distribution over the possible outcomes for the measurement in the computational basis of G_n's output register. When we write $\texttt{out}\{G_n \cdot (C_n |b\rangle_\theta) \otimes |\theta\rangle\}$ we are not only designating the value of G_n's output register but any classical mapping from the output into $\{0,1\}$. Using this convention, $\Pr(h_I(b,s) \neq \texttt{out}\{G_n \cdot (C_n |b\rangle_\theta) \otimes |\theta\rangle\}) \geq \frac{1}{2} - \epsilon$, means that any *classical* mapping from the value of the output register to $\{0,1\}$ has expected probability of error at least $\frac{1}{2} - \epsilon$ in guessing the value of $h_I(b,s)$.

Using (56), we get that $\tilde{\mathcal{A}}$ also defines an adversary against QMC with $\tilde{p}^{ok}(n) \geq 1 - 2\delta$. From (55), we conclude that

$$\tilde{\varepsilon}(n) \leq \frac{\sqrt{2\delta + \frac{1}{\text{poly}(n)}}}{2} \tag{57}$$

given the output of any family of poly-size quantum circuits $\{G_n\}_{n>0} \in$ QPoly(n). Remember that $\tilde{\varepsilon}(n)$ is the maximum expected bias on $h_I(b,0) \oplus h_I(b,1)$ for any announcement $I \in \mathcal{I}_n$. The following lemma follows easily from Theorem 2, it tells us that for each execution of $\mathcal{W}_n$, there exists $s \in \{0,1\}$ such that $h_I(b,s)$ cannot be guessed with arbitrary precision. The proof proceeds by contradiction showing that if both bits $h_I(b,0)$ and $h_I(b,1)$ can be guessed respectively by G_n^0 and G_n^1 with probability larger than $\frac{1-2\tilde{\varepsilon}(n)}{10}$ then $\tilde{\mathcal{A}}$ could attack a QMC with success probability $\tilde{p}^{ok}(n) \geq 1 - 2\delta$ and expected bias larger than $\sqrt{2\delta + 1/\text{poly}(n)}/2$ contradicting (55).

Lemma 6.

$$(\forall \{C_n\}_{n>0} \in \mathcal{C}_\delta)(\forall I \in \mathcal{I}_n)(\exists s \in \{0,1\})(\forall \{G_n\}_{n>0} \in \mathit{QPoly(n)})(\forall n > n_0)$$
$$\left[\Pr(h_I(b,s) \neq \texttt{out}\{G_n \cdot (C_n |b\rangle_\theta) \otimes |\theta\rangle\}) \geq \frac{1-2\tilde{\varepsilon}(n)}{10}\right], \tag{58}$$

where the probability is taken over $\theta \in_R \{+,\times\}^n$ and $b \in_R \{0,1\}^n$ and where $\tilde{\varepsilon}(n)$ is the function of δ and n defined in (57).

Proof. Assume any committing circuit $C_n \in \mathcal{C}_\delta$ for an arbitrary value of δ. We now verify that (58) follows from (55). Suppose predicate $f(b) = h_I(b,0) \oplus h_I(b,1)$ cannot be guessed by any circuit in poly(n) (i.e. given as input the state $(C_n\,|b\rangle_\theta) \otimes |\theta\rangle)$ with expected bias larger than $\varepsilon^{\mathcal{A}}$. Assume for a contradiction that there exists $G_n^0, G_n^1 \in \text{poly}(n)$ such that

A1: $\Pr\left(h_I(b,0) = \texttt{out}\left\{G_n^0 \cdot (C_n\,|b\rangle_\theta) \otimes |\theta\rangle\right\}\right) \geq \frac{1}{2} + \epsilon^0$, and
A2: $\Pr\left(h_I(b,1) = \texttt{out}\left\{G_n^1 \cdot (C_n\,|b\rangle_\theta) \otimes |\theta\rangle\right\}\right) \geq \frac{1}{2} + \epsilon^1$,

where as usual the probabilities are taken over $b, \theta \in_R \{0,1\}^n$. We denote by $\epsilon^0_{\theta,b}$ and $\epsilon^1_{\theta,b}$ the bias of G_n^0 and G_n^1 on $h_I(b,0)$ and $h_I(b,1)$ respectively for a fixed input state $|b\rangle_\theta$. That is,

$$\epsilon^0 = 4^{-n}\sum_{\theta,b}\epsilon^0_{\theta,b} \text{ and } \epsilon^1 = 4^{-n}\sum_{\theta,b}\epsilon^1_{\theta,b}.$$

Given G_n^0 and G_n^1 we can easily construct a circuit for guessing $f(b)$. The guess for $f(b)$ will be $x \oplus y$ with probability $\|P_y G_n^1 (G_n^0)^\dagger P_x G_n^0 (C_n\,|b\rangle_\theta) \otimes |\theta\rangle\|^2$. In other words, the guessing circuit for $f(b)$ simply runs G_n^0, stores its classical output $x \in \{0,1\}$, undoes G_n^0 before running G_n^1 providing classical output $y \in \{0,1\}$. Let $p_{err}(b,\theta)$ be the error probability of such a procedure when the initial input state is $|b\rangle_\theta$. We have,

$$\begin{aligned}
p_{err}(b,\theta) &= \|\mathbb{P}^{out}_{h_I(b,1)} G_n^1 (G_n^0)^\dagger (\mathbb{1} - \mathbb{P}^{out}_{h_I(b,0)}) G_n^0 (C_n\,|b\rangle_\theta) \otimes |\theta\rangle + \\
&\qquad (\mathbb{1} - \mathbb{P}^{out}_{h_I(b,1)}) G_n^1 (G_n^0)^\dagger \mathbb{P}^{out}_{h_I(b,0)} G_n^0 (C_n\,|b\rangle_\theta) \otimes |\theta\rangle\|^2 \\
&= \|\mathbb{P}^{out}_{h_I(b,1)} G_n^1 (G_n^0)^\dagger (\mathbb{1} - \mathbb{P}^{out}_{h_I(b,0)}) G_n^0 (C_n\,|b\rangle_\theta) \otimes |\theta\rangle\|^2 + \\
&\qquad \|(\mathbb{1} - \mathbb{P}^{out}_{h_I(b,1)}) G_n^1 (G_n^0)^\dagger \mathbb{P}^{out}_{h_I(b,0)} G_n^0 (C_n\,|b\rangle_\theta) \otimes |\theta\rangle\|^2 \qquad (59) \\
&\equiv \|A\|^2 + \|B\|^2.
\end{aligned}$$

By definition, we have that $G_n^0(C_n\,|b\rangle_\theta)\,|\theta\rangle = \sqrt{\frac{1}{2}+\epsilon^0_{\theta,b}}\,|h_I(b,0)\rangle\,|\phi^0_{\theta,b}\rangle + \sqrt{\frac{1}{2}-\epsilon^0_{\theta,b}}\,|\overline{h_I(b,0)}\rangle\,|\overline{\phi}^0_{\theta,b}\rangle$ and $G_n^1(C_n\,|b\rangle_\theta)\,|\theta\rangle = \sqrt{\frac{1}{2}+\epsilon^1_{\theta,b}}\,|h_I(b,1)\rangle\,|\phi^1_{\theta,b}\rangle + \sqrt{\frac{1}{2}-\epsilon^1_{\theta,b}}\,|\overline{h_I(b,1)}\rangle\,|\overline{\phi}^1_{\theta,b}\rangle$. We now apply these specifications for G_n^0 and G_n^1 to each part, $\|A\|^2$ and $\|B\|^2$, appearing in (59). The first part can be rewritten as,

$$\begin{aligned}
\|A\|^2 &= \|\mathbb{P}^{out}_{h_I(b,1)} G_n^1 (C_n\,|b\rangle_\theta) \otimes |\theta\rangle - \mathbb{P}^{out}_{h_I(b,1)} G_n^1 (G_n^0)^\dagger \sqrt{\frac{1}{2}+\epsilon^0_{\theta,b}}\,|h_I(b,0)\rangle\,|\phi^0_{\theta,b}\rangle\|^2 \\
&= \|\mathbb{P}^{out}_{h_I(b,1)} G_n^1 (C_n\,|b\rangle_\theta) \otimes |\theta\rangle - \\
&\qquad \mathbb{P}^{out}_{h_I(b,1)} G_n^1 \left((C_n\,|b\rangle_\theta)\,|\theta\rangle - \sqrt{\frac{1}{2}-\epsilon^0_{\theta,b}}(G_n^0)^\dagger\,|\overline{h_I(b,0)}\rangle\,|\overline{\phi}^0_{\theta,b}\rangle\right)\|^2
\end{aligned}$$

$$\leq \| \sqrt{\frac{1}{2} - \epsilon^0_{\theta,b}} \mathbb{P}^{out}_{h_I(b,1)} G^1_n (G^0_n)^\dagger \, |\overline{h_I(b,0)}\rangle \, |\overline{\phi}^0_{\theta,b}\rangle \|^2 \leq \frac{1}{2} - \epsilon^0_{\theta,b}.$$

Similarly, one can show that $\|B\|^2 \leq 2(1 - \epsilon^0_{\theta,b} - \epsilon^1_{\theta,b})$ which leads to,

$$p_{err}(b,\theta) \leq 2(\frac{5}{4} - \frac{3\epsilon^0_{\theta,b}}{2} - \epsilon^1_{\theta,b}).$$

The probability of success $p_{suc}(b,\theta) = 1 - p_{err}(b,\theta)$ in guessing $f(b)$ from $|b\rangle_\theta$ therefore satisfies, $p_{suc}(b,\theta) \geq 3\epsilon^0_{\theta,b} + 2\epsilon^1_{\theta,b} - \frac{3}{2}$. Using assumptions A1 and A2 with $\epsilon^0, \epsilon^1 \geq \overline{\epsilon}$, we get that the expected probability of success p_{suc}, over all choices of $b,\theta \in_R \{0,1\}^n$, satisfies:

$$p_{suc} = 4^{-n} \sum_{b,\theta} p_{suc}(b,\theta) \geq 5\overline{\epsilon} - \frac{3}{2}.$$

It follows that the expected bias $\varepsilon(G^0_n, G^1_n)$ on $f(b)$ provided by such circuit built from G^0_n and G^1_n is,

$$\varepsilon(G^0_n, G^1_n) = p_{suc} - \frac{1}{2} \geq 5\overline{\epsilon} - 2.$$

Since our circuit is in poly(n), it follows that $\varepsilon(G^0_n, G^1_n) \leq \varepsilon^{\mathcal{A}}$ otherwise, there would be an efficient extractor with expected bias better than $\varepsilon^{\mathcal{A}}$ from state $(C_n \, |b\rangle_\theta) \, |\theta\rangle$ with $C_n \in \mathcal{C}_\delta$ in contradiction with the definition of $\varepsilon^{\mathcal{A}}$. In other words, $\overline{\epsilon} \leq \frac{\varepsilon^{\mathcal{A}}+2}{5}$, which means that for at least one $s \in \{0,1\}$, for all $G_n \in$ poly(n),

$$\Pr\left(h_I(b,s) \neq \mathtt{out}\left\{G_n \cdot (C_n \, |b\rangle_\theta) \otimes \, |\theta\rangle\right\}\right) \geq \frac{1}{2} - \overline{\epsilon} \geq \frac{1 - 2\varepsilon^{\mathcal{A}}}{10}.$$

Equation (58) follows. □

Let $\tilde{p}_{abort}(\ell)$ be the probability that $\mathcal{B}$ aborts the execution no later than during the ℓ–th call to $\mathcal{W}_n$ in R-Reduce. Let $\tilde{p}_{stop}(\ell+1)$ be the probability that given the first ℓ calls to $\mathcal{W}_n$ were successful, $\mathcal{B}$ aborts during the ℓ+1-th execution of $\mathcal{W}_n$. We have,

$$\tilde{p}_{abort}(1) = \tilde{p}_{abort,\mathcal{W}_n} \text{ and} \tag{60}$$

$$\tilde{p}_{abort}(\ell+1) = \tilde{p}_{abort}(\ell) + (1 - \tilde{p}_{abort}(\ell))\tilde{p}_{stop}(\ell+1). \tag{61}$$

In order for $\tilde{\mathcal{A}}$'s success probability $1 - \tilde{p}_{abort}(t)$ to be non-negligible in t, $\tilde{p}_{stop}(\ell)$ must be *small* for most executions $\ell \in [1 \ldots t]$. Let $\delta > 0$ and $\alpha > 0$ be two arbitrary constants. Assuming $\tilde{p}_{stop}(\ell) > \delta$ for all $\ell \in L$ with $\#L \geq \alpha t$ then $\tilde{p}_{abort}(t) \geq 1 - (1-\delta)^{\alpha t}$. In other words, if $\tilde{p}_{stop}(\ell) > \delta$ for a constant fraction of the t executions then $1 - \tilde{p}_{abort}(t)$ is negligible in t. In general, an adversary $\tilde{\mathcal{A}}$ against R-Reduce$(t, \mathcal{W}_n)$ is modeled by a family of quantum circuits $\tilde{\mathcal{A}} = \{(C_{n,t}, G^0_{n,t}, G^1_{n,t})\}_{n,t>0}$ where C_n runs the committing phase and circuits G^0_n and G^1_n extract information about b_0 and b_1 respectively. Promising adversaries in R-Reduce$(t, \mathcal{W}_n)$ are defined as follows:

Definition 3. *A polynomial size adversary* $\tilde{\mathcal{A}} = \{(C_{n,t}, G^0_{n,t}, G^1_{n,t})\}_{n,t>0}$ *against* $\mathsf{R\text{-}Reduce}(t, \mathcal{W}_n)$ *is* promising *if* $\tilde{p}_{abort}(t) \leq 1 - \frac{1}{p(t)}$ *for some* $p(t) \in poly(t)$.

We now consider the limitations implied by (58) to any adversary $\tilde{\mathcal{A}}$ against $\mathsf{R\text{-}Reduce}(t, \mathcal{W}_n)$. Let $|b\rangle_\theta = \otimes_{i=1}^t |b^{(i)}\rangle_{\theta^{(i)}}$ be the random $n \cdot t$ BB84 qubits picked and sent by $\mathcal{B}$. The following lemma links promising adversaries against $\mathsf{R\text{-}Reduce}(t, \mathcal{W}_n)$ to Lemma 6. It tells us that if $\tilde{\mathcal{A}}$ is promising then there exists a *large* subset L of all executions of $\mathcal{W}_n$ in $\mathsf{R\text{-}Reduce}(t, \mathcal{W}_n)$ for which independently of each other, predicates $h_I(b^\ell, s)$, $\ell \in L$ cannot be guessed with arbitrary precision given the output of any polynomial size circuit.

Lemma 7. *Assume the security parameters* n *and* t *in* $\mathsf{R\text{-}Reduce}(t, \mathcal{W}_n)$ *are polynomially related. Then,*

$$\begin{aligned}(\forall \delta > 0)(\forall \gamma > 0)(\forall \textit{ promising } \tilde{\mathcal{A}} = \{(C_{n,t}, \cdot)\}_{n,t>0})\\ (\exists L \subseteq \{1, \ldots, t\} : \#L > (1-\gamma)t)(\forall \ell \in L)\\ (\forall I \in \mathcal{I}_n)(\exists s \in \{0,1\})(\forall \{G_{n,t}\}_{n,t>0} \in \mathrm{QPoly}(n,t))\end{aligned}$$
$$\left[\Pr\left(h_I(b^{(\ell)}, s) \neq \mathsf{out}\left\{G_{n,t}\left(C_{n,t}\,|b\rangle_\theta\right) \otimes |\theta\rangle\right\} \middle| \{(b^{(j)}, \theta^{(j)})\}_{j \neq \ell}\right) \geq \frac{1 - \sqrt{2\delta + \frac{1}{poly(n)}}}{10}\right] \tag{62}$$

where the probability is computed over $b = b^{(1)}, \ldots, b^{(t)}$, *and* $\theta = \theta^{(1)}, \ldots, \theta^{(t)}$ *for* $b^{(i)} \in_R \{0,1\}^n$ *and* $\theta^{(i)} \in_R \{0,1\}^n$ *for all* $i \in \{1, \ldots, t\}$.

Proof. Let $\delta \in [0, \frac{1}{2}[$ be a constant. Let $\overline{L} \subseteq \{1, \ldots, t\}$ be the subset of all executions $\ell \in \{1, \ldots, t\}$ of $\mathcal{W}_n$ in $\mathsf{R\text{-}Reduce}(t, \mathcal{W}_n)$ such that $p^{\mathcal{A}}_{stop}(\ell) > \delta$. Since $\mathcal{A} = \{(C_{n,t}, \cdot)\}_{n,t>0}$ is a good adversary, we have

$$1 - \frac{1}{p(t)} \geq \tilde{p}_{abort}(t) \geq 1 - (1-\delta)^{\#\overline{L}}, \tag{63}$$

which implies that,

$$\forall \gamma \in]0,1[, \#\overline{L} \leq \gamma t, \tag{64}$$

provided t is large enough. Let $L = \{1, \ldots, t\} \setminus \overline{L}$ be the set of all executions $\ell \in \{1, \ldots, t\}$ of $\mathcal{W}_n$ such that $p^{\mathcal{A}}_{stop}(\ell) \leq \delta$. By construction, we have that

$$\forall \gamma > 0, \#L > (1-\gamma)t, \tag{65}$$

provided t is large enough. We now pick any $\ell \in L$ for which execution we apply Lemma 6. This is possible since using $C_{n,t}$, one can build $C'_{n,t}$ implementing $\mathcal{A}$'s algorithm against $\mathcal{W}_n$ with $\tilde{p}_{abort,\mathcal{W}_n} < 1 - \delta$. $\mathcal{A}$'s behavior in $\mathcal{W}_n$ is defined by circuit $C'_{n,t}$ running $C_{n,t}$ upon any known $\otimes_{i=1}^{\ell-1} |b^{(i)}\rangle_{\theta^{(i)}}$ until the $\ell - 1$ first executions of $\mathcal{W}_n$ were successful (none of them aborted). Then, $\mathcal{B}$'s state $|b^{(\ell)}\rangle_{\theta^{(\ell)}}$ transmitted in $\mathcal{W}_n$ is given as input to $C_{n,t}$ which by definition satisfies

$\tilde{p}_{abort,\mathcal{W}_n} < 1 - \delta$. Clearly, the size of $C'_{n,t}$ is polynomial in the size of $C_{n,t}$. Therefore, $\{C'_{n,t}\}_{n,t>0} \in \mathcal{C}_\delta$ allowing us to invoke Lemma 6 whenever n and t are polynomially related. Since the same is true independently for all $\ell \in L$, we conclude (62) after replacing $\varepsilon^{\mathcal{A}}$ in (58) using (57). □

>From Lemma 7, we would like to conclude that given any announcement $\boldsymbol{I} = (I^{(0)}, I^{(1)}, \ldots, I^{(t)})$ during $\textsf{R-Reduce}(t, \mathcal{W}_n)$, the *amplification function*

$$g_{\boldsymbol{I}}(b^{(1)}, \ldots, b^{(t)}, s) \equiv \bigoplus_{i=1}^{t} h_{I^{(i)}}(b^{(i)}, s) \in \{0,1\} \tag{66}$$

is such that for $\tilde{s} \in \{0,1\}$, the value $g_{\boldsymbol{I}}(b^{(1)}, \ldots, b^{(t)}, \tilde{s})$ cannot be guessed with bias non-negligible in t. Next theorem follows from Lemma 7 and is equivalent to Theorem 3:

Theorem 4 (Security Against the Receiver). *Let n and t be polynomially related security parameters in* $\textsf{R-Reduce}(t, \mathcal{W}_n)$. *Then,*

$$\begin{gathered}(\forall \delta > 0)(\forall \gamma > 0)(\forall \textit{ promising } \tilde{\mathcal{A}} = \{(C_{n,t}, \cdot)\}_{n,t>0})(\forall \boldsymbol{I} \in \mathcal{I}_n^t)(\exists s \in \{0,1\}) \\ (\forall \{G_{n,t}\}_{n,t>0} \in \text{QPoly}(n,t)) \\ \left[\Pr\left(g_{\boldsymbol{I}}(b^{(1)}, \ldots, b^{(t)}, s) \neq \texttt{out}\{G_{n,t}(C_{n,t}|b\rangle_\theta) \otimes |\theta\rangle\}\right) \geq \frac{1}{2} - 2^{-\alpha t}\right],\end{gathered} \tag{67}$$

for $\alpha = \frac{(1-\gamma)}{2} \log \frac{5}{4+\sqrt{\delta}}$ and where the probability is computed over $b = b^{(1)}, \ldots, b^{(t)}$, and $\theta = \theta^{(1)}, \ldots, \theta^{(t)}$ for $b^{(i)} \in_R \{0,1\}^n$ and $\theta^{(i)} \in_R \{0,1\}^n$ for all $i \in \{1, \ldots, t\}$.

Proof. For $s \in \{0,1\}$,$\beta \in \{0,1\}$, and $\boldsymbol{I} \subseteq \{1, \ldots, n\}^t$, let

$$\mathcal{Z}_\beta(\boldsymbol{I}, s) = \{(b^{(1)}, \ldots, b^{(t)}) | g_{\boldsymbol{I}}(b^{(1)}, \ldots, b^{(t)}, s) = \beta, b^{(\ell)} \in \{0,1\}^n \text{ for } \ell \in 1..t\}$$

be the set of strings $b^{(1)}, \ldots, b^{(t)}$ that would lead to the transfer of $\beta \in \{0,1\}$ when $\mathcal{A}$'s selection bit is s. Since n and t are polynomially related, we now show that Lemma 7 implies,

$$\begin{gathered}(\forall \delta > 0)(\forall \gamma > 0)(\forall \text{ good } \mathcal{A} = \{(C_{n,t}, \cdot)\}_{n,t>0})(\forall I \subseteq \{1, \ldots, n\}) \\ (\forall \{G_{n,t}\}_{n,t>0} \in \text{QPoly}(n,t))(\exists s \in \{0,1\}) \\ \left[\Pr\left((b^{(1)}, \ldots, b^{(t)}) \notin \mathcal{Z}_\beta(\boldsymbol{I}, s) \wedge \texttt{out}\{G_{n,t}(C_{n,t}|b\rangle_\theta) \otimes |\theta\rangle\} = \beta\right) \geq \frac{1 - (\frac{4+\sqrt{\tilde{\delta}}}{5})^{(1-\gamma)t/2}}{2}\right],\end{gathered} \tag{68}$$

provided n and t are large enough and where $\tilde{\delta} \equiv 2\delta + \frac{1}{poly(n)}$. Since guessing $g_{\boldsymbol{I}}(b^{(1)}, \ldots, b^{(t)}, s)$ given the output of $G_{n,t}$ is equivalent to determining whether

$(b^{(1)}, \ldots, b^{(t)}) \in \mathcal{Z}_\beta(\boldsymbol{I}, s)$ then (67) follows from (68). We now establish (68). From Lemma 7, there exists a subset of positions L, $\#L > (1-\gamma)t$ such that independently for each $\ell \in L$, any family of polynomial size quantum circuits has error probability $p_e \geq \frac{1-\sqrt{2\delta + \frac{1}{poly(n)}}}{10}$ when guessing $h_{I^{(\ell)}}(b^{(\ell)}, s_\ell)$ for at least one $s_\ell \in \{0,1\}$. This holds for any announcement $I^{(\ell)}$ made by $\mathcal{A}$ for the ℓ-th execution of $\mathcal{W}_n$ in $\mathsf{R\text{-}Reduce}(t, \mathcal{W}_n)$. Given any announcement $\boldsymbol{I} = (I^{(1)}, \ldots, I^{(t)})$, and for all $\{G_{n,t}\}_{n,t>0} \in \text{QPoly}(n,t)$, the output of circuit $G_{n,t}$ guesses $h_{I^{(\ell)}}(b^{(\ell)}, s_\ell)$ with error probability p_e independently for each $\ell \in L$. Let s be defined such that $m = \#\{\ell \in L | s_\ell = s\}$ is maximized. Clearly, $m \geq (1-\gamma)t/2$ for any $\gamma > 0$. It is a well-known fact that the parity of m independently distributed boolean variables, each occurring with probability $p_e < 1/2$, is 1 with probability $q(m, p_e) = (1-(1-2p_e)^m)/2$. That is, given the output of any $G_{n,t}$, the probability that $(b^{(1)}, \ldots, b^{(t)}) \notin \mathcal{Z}_\beta(\boldsymbol{I}, s)$ is at least $q(m, p_e)$. Equation (68) is simply $q(\frac{(1-\gamma)t}{2}, \frac{1-\sqrt{2\delta + \frac{1}{poly(n)}}}{10})$ and (67) follows. □

Theorem 4 establishes that any good adversary $\mathcal{A}$'s can only guess $g_{\boldsymbol{I}}(b^{(1)}, \ldots, b^{(t)}, s)$ with negligible bias using polynomial size families of quantum circuits. We conclude the security of $\mathsf{R\text{-}Reduce}(t, \mathcal{W}_n)$ against any poly-time dishonest receiver as stated in Theorem 3.

Recent BRICS Report Series Publications

RS-03-37 **Claude Crépeau, Paul Dumais, Dominic Mayers, and Louis Salvail.** ***Computational Collapse of Quantum State with Application to Oblivious Transfer*****. November 2003. 30 pp.**

RS-03-36 **Ivan B. Damgård, Serge Fehr, Kirill Morozov, and Louis Salvail.** ***Unfair Noisy Channels and Oblivious Transfer*****. November 2003.**

RS-03-35 **Mads Sig Ager, Olivier Danvy, and Jan Midtgaard.** ***A Functional Correspondence between Monadic Evaluators and Abstract Machines for Languages with Computational Effects*****. November 2003. 31 pp.**

RS-03-34 **Luca Aceto, Willem Jan Fokkink, Anna Ingólfsdóttir, and Bas Luttik.** ***CCS with Hennessy's Merge has no Finite Equational Axiomatization*****. November 2003. 37 pp.**

RS-03-33 **Olivier Danvy.** ***A Rational Deconstruction of Landin's SECD Machine*****. October 2003. 32 pp. This report supersedes the earlier BRICS report RS-02-53.**

RS-03-32 **Philipp Gerhardy and Ulrich Kohlenbach.** ***Extracting Herbrand Disjunctions by Functional Interpretation*****. October 2003. 17 pp.**

RS-03-31 **Stephen Lack and Paweł Sobociński.** ***Adhesive Categories*****. October 2003. 25 pp.**

RS-03-30 **Jesper Makholm Byskov, Bolette Ammitzbøll Madsen, and Bjarke Skjernaa.** ***New Algorithms for Exact Satisfiability*****. October 2003. 31 pp.**

RS-03-29 **Aske Simon Christensen, Christian Kirkegaard, and Anders Møller.** ***A Runtime System for XML Transformations in Java*****. October 2003. 15 pp.**

RS-03-28 **Zoltán Ésik and Kim G. Larsen.** ***Regular Languages Definable by Lindström Quantifiers*****. August 2003. 82 pp. This report supersedes the earlier BRICS report RS-02-20.**

RS-03-27 **Luca Aceto, Willem Jan Fokkink, Rob J. van Glabbeek, and Anna Ingólfsdóttir.** ***Nested Semantics over Finite Trees are Equationally Hard*****. August 2003. 31 pp.**