**Basic Research in Computer Science**

**BRICS RS-03-3 Crépeau et al.: On the Computational Collapse of Quantum Information**

# On the Computational Collapse of Quantum Information

**Claude Crépeau**
**Paul Dumais**
**Dominic Mayers**
**Louis Salvail**

**BRICS Report Series** **RS-03-3**

**ISSN 0909-0878** **January 2003**

**Copyright © 2003, Claude Crépeau & Paul Dumais & Dominic Mayers & Louis Salvail.**
**BRICS, Department of Computer Science**
**University of Aarhus. All rights reserved.**

**Reproduction of all or part of this work is permitted for educational or research use on condition that this copyright notice is included in any copy.**

**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/03/3/`

# On the Computational Collapse of Quantum Information

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] Department of Computer Science, Sherbrooke University, dmayers@dmi.usherb.ca
[3] BRICS*, Dept. of Computer Science, University of Århus, Ny Munkegade, building 540,DK-8000 salvail@brics.dk

**Abstract.** We analyze the situation where computationally binding string commitment schemes are used to force the receiver of a BB84 encoding of a classical bitstring to measure upon reception. Since measuring induces an irreversible collapse to the received quantum state, even given extra information after the measurement does not allow the receiver to evaluate reliably some predicates apply to the classical bits encoded in the state. This fundamental quantum primitive is called quantum measure commitment (QMC) and allows for secure two-party computation of classical functions. An adversary to QMC is one that can both provide valid proof of having measured the received states while still able to evaluate a predicate applied to the classical content of the encoding. We give the first quantum black-box reduction for the security of QMC to the binding property of the string commitment. We characterize a class of quantum adversaries against QMC that can be transformed into adversaries against a weak form for the binding property of the string commitment. Our result provides a construction for $1-2$-oblivious transfer that is computationally secure against the receiver and unconditionally secure against the sender from any string commitment scheme satisfying a weak binding property.
**keywords:** quantum bit commitment, oblivious transfer, quantum measurement, computational assumptions.

## 1 Introduction

As in the classical case, secure quantum 2-party cryptography must rely upon assumptions but the two models do not share the same capabilities and limits. In particular, given a classical black-box for bit commitment, there exists a quantum protocol, called the BBCS protocol [4], achieving $1-2$ oblivious transfer [7, 6, 22] (one-out-of-two oblivious transfer). This is in sharp contrast with the classical case where such a reduction is

* Basic Research in Computer Science (www.brics.dk), funded by the Danish National Research Foundation.

not only unknown but unlikely to exist [12]. The difference between the two models can intuitively be appreciated by observing that a classical black-box for bit commitment allows to transform the quantum channel into a noisy classical channel powerful enough to provide OT. To see this, consider the BB84 coding scheme [2, 4] 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* for $b$.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 $|1\rangle_{\hat{\theta}}$, providing the classical outcome $\hat{b} \in \{0, 1\}$. 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 $\hat{\theta} \neq \theta$. The error-rate of such a transmission is therefore $\frac{1}{4}$ when $\theta$ is not revealed to Alice. Dishonest Bob however, could send different states in order to temper with the error-rate of the channel so it becomes an *unfair noisy channel* (i.e. UNC) [9]. Bob could instead send $\cos\frac{\pi}{8}|b\rangle + (-1)^b \sin\frac{\pi}{8}|1-b\rangle$ for the encoding of $b$. In this case, the error-rate falls to $\sin^2\frac{\pi}{8}$. According to [9], the resulting $(\sin^2\frac{\pi}{8}, \frac{1}{4})$-UNC has no cryptographic capability since $2\sin^2\frac{\pi}{8}(1-\sin^2\frac{\pi}{8}) \leq \frac{1}{4}$. In order to prevent Bob from behaving in such way, a slightly different strategy is used. Bob is now asked to announce $\theta$ allowing Alice to determine whether $b$ has been received. The result is an oblivious transfer of bit $b$ from Bob to Alice only assuming Alice is honest. Dishonest Alice can easily learn $b$ all the time by waiting for $\theta$ before applying measurement $\mathbb{M}_{\hat{\theta}}$. Bob must make sure that Alice has measured before the announcement of $\theta$ so the initial state has collapsed irreversibly. An oblivious transfer is possible only given such a primitive. The natural way to build used commitments [4].

We call *Quantum Measure Commitment* (or QMC) the primitive that allows Alice to provide Bob with evidences that she measured the qubits received before the announcement of $\theta$. Implementing a QMC is simply done by sending a commitment containing $(\hat{\theta}, \hat{b})$ to Bob. A collapse occurred if given the transmission basis $\theta$, the bit $b$ cannot be determined perfectly. However, verifying the collapse of a single qubit cannot be done perfectly since Alice could always provide a commitment to random $(\hat{\theta}, \hat{b})$ while keeping $|b\rangle_\theta$ untouched until $\theta$ is announced. The probability of opening with success would then be $\frac{3}{4}$ while $b$ can always be received perfectly from $\theta$. To avoid a lucky Alice from learning too much about $b$, QMC

are made to $n$ random BB84 qubits $|b\rangle_\theta = |b_1\rangle_{\theta_1}, |b_2\rangle_{\theta_2}, \ldots, |b_n\rangle_{\theta_n}$ before Bob announces the transmission basis $\theta = \theta_1, \ldots, \theta_n$. The QMC is simply a string commitment containing the measurements $\hat{\theta} \in \{+, \times\}^n$ and the outcomes $\hat{b} \in \{0,1\}^n$. The classical transmission is encoded in some predicate $f(b_1, \ldots, b_n)$. Alice should be unable to evaluate $f(b_1, \ldots, b_n)$ even given the knowledge of $\theta$. The BBCS protocol can be seen as a reduction of oblivious transfer to such a QMC to $n$ random BB84 qubits with $f(b_1, \ldots, b_n) \equiv \oplus_{i=1}^n b_i$. A QMC is therefore an universal primitive for secure quantum 2-party computation of classical functions. A successful adversary to QMC is one that can unveil valid measurement outcomes with good probability while being able to get a bias on $f(b_1, \ldots, b_n)$ given $\theta \in \{+, \times\}^n$.

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 [10, 8], quantum bit commitment schemes satisfy different binding properties than classical ones. The difference becomes more obvious when string commitments are taken into account. We generalize the computational binding criteria of [10] to the case where commitments are made to strings of size $l(n) \in \Omega(n)$ for $n$ the security parameter. Intuitively, for a class of functions $F \subseteq \{f : \{0,1\}^{l(n)} \rightarrow \{0,1\}^{m(n)}\}$, we say that a string commitment scheme is $F$–binding if for all $f \in F$ and given $y \in_R \{0,1\}^{m(n)}$, the committer cannot open with success any $s \in \{0,1\}^{l(n)}$ such that $f(s) = y$. The smaller $m(n)$ is compared to $l(n)$, the weaker is the $F$–binding criteria. We relate the security of a QMC to a weak form of the $F$–binding property. Assume QMC's are made using some computationally binding string commitments 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 $|b\rangle_\theta$. At this point, Bob selects a challenge $c \in_R \{0,1\}$. If $c = 0$, Alice unveils all measurements and outcomes that Bob verifies. If $c = 1$, Bob announces the transmission basis $\theta \in_R \{+, \times\}^n$ and Alice tries to get a bias on the parity of $b$. Let $\tilde{p}_s$ be Alice's probability of success when $c = 0$ and let $\tilde{\epsilon}$ be Alice's expected bias when $c = 1$. Our main contribution describes how $\tilde{p}_s$ and $\tilde{\epsilon}$ relates to the $\mathcal{F}^n_{m(n)}$–binding criteria of the string commitment where $\mathcal{F}^n_{m(n)}$ is a class of functions with $m(n) \in O(polylog(n))$. We give a black-box reduction of any *good* quantum adversary against QMC into one against the $\mathcal{F}^n_{m(n)}$–binding property of the string commitment. 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 $\mathcal{F}^n_{m(n)}$–binding. Our reduction shows that using computationally binding commitments one can enforce a computational

collapse of quantum information. This is the first quantum black-box reduction linking the security of those two primitives. Previously, Yao [22] has shown that if the string commitment is modeled by a classical black-box then the BBCS protocol is secure. Our result can be used for proving the security of OT in the computational setting using a different approach. We describe a $1-2$ oblivious transfer unconditionally secure against the sender but computationally secure against the receiver that is very similar to the BBCS protocol. It is shown that any dishonest receiver able to get a non-negligible amount of information about each transmitted bit can break the $\mathcal{F}^n_{m(n)}$-binding property of the string commitment used in the construction. As for the Quantum Goldreich-Levin theorem of [1] and the computationally binding commitments of [10] and [8], our result clearly indicates that 2-party quantum cryptography in the computational setting can be based upon different assumptions (i.e. weaker to some extend) than its classical counterpart.

## 2 Preliminaries

**Notations and Tools.** In the following, $poly(n)$ stands for any polynomial in $n$. We write $A(n) < poly(n)$ for "$A(n)$ is smaller than any polynomial provided $n$ is sufficiently large" and $A(n) \leq poly(n)$ (resp. $A(n) \geq poly(n)$) 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, proved in Appendix A, provides a useful 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 for all $s, t \in \{0,1\}^n, s \neq t$,*

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

*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 Operators and Encoding.** In the following, we denote the $m$-dimensional Hilbert space by $\mathcal{H}_m$. 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 $|1\rangle_\times = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. The 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 $\otimes_{i=1}^n |x_i\rangle_{\theta_i}$. An orthogonal (or Von Neumann) measurement of a quantum state in $\mathcal{H}_m$ is described by a set of $m$ orthogonal projections $\mathbb{M} = \{\mathbb{P}_i\}_{i=1}^m$ acting in $\mathcal{H}_m$ thus satisfying $\sum_i \mathbb{P}_i = \mathbb{1}_m$ for $\mathbb{1}_m$ denoting the identity operator in $\mathcal{H}_m$. Each projection or equivalently each index $i \in \{1, \ldots, m\}$ is a possible classical outcome for $\mathbb{M}$. 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. The two possible measurements applied by the receiver of BB84 qubits are $\mathbb{M}_+ = \{\mathbb{P}_0, \mathbb{P}_1\}$ and $\mathbb{M}_\times = \{\mathbb{P}_{\times,0}, \mathbb{P}_{\times,1}\}$. 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 bitstring the obvious way. In order to indicate that $|\phi\rangle \in \mathcal{H}_{2^r}$ is the state of a quantum register $H_R \simeq \mathcal{H}_{2^r}$ we write $|\phi\rangle^R$. If $H_R \simeq \mathcal{H}_{2^r}$ and $H_S \simeq \mathcal{H}_{2^s}$ are two quantum registers and $|\phi\rangle = \sum_{x \in \{0,1\}^r} \sum_{y \in \{0,1\}^s} \gamma_{x,y} |x\rangle \otimes |y\rangle \in \mathcal{H}_{2^r} \otimes \mathcal{H}_{2^s}$ then we write $|\phi\rangle^{RS} = \sum_{x \in \{0,1\}^r} \sum_{y \in \{0,1\}^s} \gamma_{x,y} |x\rangle^R \otimes |y\rangle^S$ to denote the state of both registers $H_R$ and $H_S$. Given any transformation $U^R$ acting on a register $H_R$ and any state $|\phi\rangle \in H_R \otimes H_{Others}$, where $H_{Others}$ corresponds to the other registers, we define $U^R |\phi\rangle \stackrel{def}{=} (U^R \otimes \mathbb{1}_{Others}) |\phi\rangle$. We use the same notation when $U^R$ denotes a projection operator.

**Model of Computation and Protocols.** In this paper, we model protocols and algorithms by quantum circuits built out of the universal set of quantum gates $\mathcal{UG} = \{\texttt{CNot}, \texttt{H}, \texttt{P}, \texttt{T}\}$, where `CNot` denotes the controlled-NOT, `H` the one qubit Hadamard gate, `P` the phase gate, and `T` is a one

qubit gate sometimes refer to as the $\pi/8$ gate [19].In addition to the set of gates $\mathcal{UG}$, a quantum circuit is allowed to perform von Neumann measurements in the computational basis $\mathbb{M}_+$. A circuit $C$ executed in the reverse direction is denoted $C^\dagger$. The complexity of the circuit $C$ is simply the number $\|C\|_{\mathcal{UG}}$ of elementary gates in $\mathcal{UG}$ contained in $C$.

In the following, we use the two Pauli (unitary) transformations $\sigma_X$ (bit flip) and $\sigma_Z$ (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*) $|0^n\rangle^L \otimes |0^n\rangle^R$ after applying $n$ Hadamard `H` and `CNOT` gates. A 2-party quantum protocol taking place between $\mathcal{A}$ and $\mathcal{B}$ is a pair of interactive quantum circuits $(P^A, P^B)$ applied to some initial product state $|x_A\rangle^A \otimes |x_B\rangle^B$ representing $\mathcal{A}$'s and $\mathcal{B}$'s (maybe secret) inputs to the protocol neglecting to write explicitly the states of $\mathcal{A}$'s and $\mathcal{B}$'s registers that do not encode their respective input to the protocol (thus all in initial states $|0\rangle$). Since communication takes place between $\mathcal{A}$ and $\mathcal{B}$, the complete circuit representing one protocol execution may have quantum gates in $P^A$ and $P^B$ acting upon the same quantum registers. We write $P^A \odot P^B$ for the complete quantum circuit when $\mathcal{A}$ is interacting with $\mathcal{B}$. The final composite state $|\Psi_{final}\rangle$ obtained after the execution is then written as $|\Psi_{final}\rangle = (P^A \odot P^B) |x_A\rangle^A |x_B\rangle^B$. Protocols are to be understood, although not always explicitly stated, as specified by families of interactive quantum circuits, one for each possible value of the security parameter $n$. We denote by $\mathcal{P}^{AB} = \{(P_n^A, P_n^B)\}_{n>0}$ such a family of protocols.

## 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 $l(n)$-string commitment allows to commit upon strings of length $l(n)$ 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

$s \in \{0,1\}^{l(n)}$. 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 [10], the security criteria for computationally binding but otherwise concealing quantum bit commitment schemes were introduced. Here, we follow a similar 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 $|s\rangle^A$. Given the final state $|\tilde{\psi}_{final}\rangle = (\tilde{O}_n^A \odot O_n^B)\,|s\rangle^A\,|\tilde{\psi}\rangle$ we define $\tilde{p}_s(n)$ as the probability to open $s \in \{0,1\}^{l(n)}$ 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 fix the adversary's committed string $s$ after the committing phase of the protocol has been executed. Classically, this can be done by fixing the adversary's random tape so any $s' \neq s$ cannot be unveiled with non-negligible probability. In addition, techniques like rewinding have no quantum counterpart [20]. A committer (to a concealing commitment) can always commit upon any superposition of values for $s$ that will remain such until the opening phase. Even an honest committer does not necessarily know a single string that can be unveiled with non-negligible probability of success. Suppose a quantum $l(n)$–string commitment scheme has committing circuit $C_n^A \odot C_n^B$ such that $|\psi(s)\rangle^{AB} = (C_n^A \odot C_n^B)\,|s\rangle^A$. If the committer starts with superposition $\sum_s \sqrt{\tilde{p}_s(n)}\,|s\rangle$, for any probability distribution $\{(\tilde{p}_s(n), s)\}_{s\in\{0,1\}^{l(n)}}$, then the state obtained after the committing phase would be:

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

Equation (4) is a valid commitment to a superposition of strings that will always allow the sender to open $s$ with probability $\tilde{p}_s(n)$. The *honest* strategy described in (4) achieves $\sum_s \tilde{p}_s(n) = 1$. In [10], the binding condition is satisfied if no adversary can do significantly better than what is achievable by (4) in the special case where $l(n) = 1$. More precisely, a bit commitment scheme is binding if for all adversaries $\tilde{\mathcal{A}}$:

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

where $\tilde{p}_b(n)$ is the probability to open bit $b$ with success. Extending this definition to the case where $l(n) \in \Omega(n)$ must be done with care however. The obvious generalization of (5) to the requirement $\sum_{s\in\{0,1\}^{l(n)}} \tilde{p}_s(n) < 1+1/poly(n)$ is too strong whenever $l(n) \in \Omega(n)$. For example, if $l(n) = n$ and $\tilde{p}_s(n) = 2^{-n}(1 + \frac{1}{p(n)})$ for all strings $s \in \{0,1\}^n$ then the poly-time adversary $\tilde{\mathcal{A}}$ is indistinguishable from what is achievable with the *honest* state (4) resulting from distribution $\{(2^{-n}, s)\}_s$. Any attack that cannot be distinguished from the honest behaviour in polynomial time should hardly be considered successful. On the other hand, defining a successful adversary $\tilde{A}$ 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 $s \in \{0,1\}^{l(n)}$, an attacker could be interested in opening any $s \in \{0,1\}^{l(n)}$ such that $f(s) = y$ for some predetermined function $f : \{0,1\}^{l(n)} \to \{0,1\}^{m(n)}$ with $m(n) \leq l(n)$. 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 attack for a special class of functions. Such an adversary is characterized 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 $|\tilde{\psi}(y)\rangle = (\tilde{O}_n^A \odot O_n^B)\,|y\rangle^A\,|\tilde{\psi}\rangle^{AB}$ is the state (hopefully) allowing to open $s \in \{0,1\}^{l(n)}$ such that $f(s) = y$. The probability to succeed in opening such an $s$ is,

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

where $\mathbb{Q}_s^B$ is $\mathcal{B}$'s projector operator leading to accept the opening of $s \in \{0,1\}^{l(n)}$. The following security criteria takes into account a class of functions for which the binding condition is guaranteed:

**Definition 1.** *Let $F \subseteq \{f : \{0,1\}^{l(n)} \to \{0,1\}^{m(n)}\}$ be a set of functions. A $l(n)$-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 that*

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

Note that any standard attack can be expressed in terms of an appropriate class of functions $F$. In general, the smaller $m(n)$ is with respect to $l(n)$, the weaker is the $F$–binding requirement. 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 $\mathcal{I}^n_{m(n)}$ be the set of subsets of $\{1,\ldots,n\}$ having size exactly $m(n)$, we define the class of functions $\mathcal{F}^n_{m(n)}$ as,

$$\mathcal{F}^n_{m(n)} = \{f_I : \{0,1\}^{2n} \to \{0,1\}^{m(n)} | I \in \mathcal{I}^n_{m(n)}, f_I(x,y) = \blacklozenge_{h\in I} s_{j_h}(x_h, y_h), \text{ where } j_h \in \{1,2,3\} \text{ for } h \in I\}. \tag{8}$$

In other words, $\mathcal{F}^n_{m(n)}$ contains the set of functions $f : \{0,1\}^{2n} \to \{0,1\}^{m(n)}$ such that $f(x,y)$ is a set of $m(n)$ bits where each is either in $x$ or in $y$ or in $x \oplus y$.

### 3.2 Quantum Measure Commitment

Quantum Measure Commitment (QMC) is a primitive allowing the receiver of random qubits to show the sender that the qubits have been measured without disclosing any further information about the measurement and the outcome. 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 $\{\mathbb{M}_+, \mathbb{M}_\times\}$. For simplicity we model QMCs by the following game between players $\mathcal{A}$ and $\mathcal{B}$:

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. $\mathcal{A}$ measures the qubits with measurement $\mathbb{M}_{\hat{\theta}}$ for $\hat{\theta} \in_R \{+,\times\}^n$ thus and producing the classical outcome $\hat{b} \in \{0,1\}^n$,
3. $\mathcal{A}$ uses a $2n$-string commitment and commits to $(\hat{\theta}, \hat{b})$ toward $\mathcal{B}$,
4. $\mathcal{B}$ picks a random challenge $c \in_R \{0,1\}$,
   - If $c = 0$ then $\mathcal{B}$ asks $\mathcal{A}$ to open $(\hat{\theta}, \hat{b})$ and verifies that $\hat{b}_i = b_i$ for all $i$ such that $\hat{\theta}_i = \theta_i$ (if errors are found then $\mathcal{B}$ aborts),
   - If $c = 1$ then $\mathcal{B}$ announces $\theta$ and $\mathcal{A}$ tries to bias $[b]$.

$\mathcal{A}$ wants to maximize both her success probability when unveiling and the bias on $[b]$ whenever $\theta$ is announced. This is almost identical to the receiver's situation in the BBCS protocol[4]. Since we only consider unconditionally concealing string commitments, $\mathcal{B}$ gets information about $\mathcal{A}$'s measurements and results only if they are unveiled.

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 ($c$=0) phases. Circuit $\tilde{E}_n$ allows to extract the parity of $b$ upon the announcement of basis $\theta$. Circuit $\tilde{C}_n^A$ works upon $\tilde{\mathcal{A}}$'s internal registers $H_A$ together with the register $H_{channel}$ (the channel) carrying the BB84 qubits. We denote by

$$|\psi_{\theta,b}\rangle^{AB} = (\tilde{C}_n^A \odot C_n^B)\ |b\rangle_\theta^{channel}, \tag{9}$$

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 $\theta, b, x \in \{0,1\}^n$,

$$|\psi_{\theta,b}\rangle = 2^{-\frac{|x|}{2}} \sum_{y:y\preceq x} (-1)^{b\odot x \oplus b\odot y}\ |\psi_{\theta\oplus x, b\oplus y}\rangle. \tag{10}$$

The probability to open with success $\tilde{p}^{ok}_{(\theta,b)}(n)$, when $|b\rangle_\theta$ was sent, is

$$\tilde{p}^{ok}_{(\theta,b)}(n) = \sum_{(\hat{\theta},\hat{b})\in\Delta_\preceq(\theta,b)} \|\mathbb{Q}^B_{(\hat{\theta},\hat{b})}(\tilde{O}_n^A \odot O_n^B)\ |\psi_{\theta,b}\rangle\|^2 = \|\mathbb{Q}^*_{(\theta,b)}\ |\psi_{\theta,b}\rangle\|^2, \tag{11}$$

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 $\mathbb{Q}^*_{(\theta,b)} = \sum_{(\hat{\theta},\hat{b})\in\Delta_\preceq(\theta,b)} \mathbb{Q}^B_{(\hat{\theta},\hat{b})}$. The expected probability of success $\tilde{p}^{ok}(n)$ is,

$$\tilde{p}^{ok}(n) = \frac{1}{4^n} \sum_{b\in\{0,1\}^n} \sum_{\theta\in\{+,\times\}^n} \tilde{p}^{ok}_{(\theta,b)}(n). \tag{12}$$

When $c = 1$, $\tilde{\mathcal{A}}$ should be able, given the announcement of $\theta$, to extract information about the parity $[b]$.The extractor $\tilde{E}_n$ has access to an extra register $H_\Theta$ that contains 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

$$\tilde{\varepsilon}_{\theta,b}(n) = \|\mathbb{P}^\oplus_{[b]}(\tilde{E}_n \otimes \mathbb{1}_B)\ |\theta\rangle^\Theta\ |0\rangle^\oplus\ |\psi_{\theta,b}\rangle^{AB}\|^2, \tag{13}$$

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,

$$\tilde{\varepsilon}(n) = \frac{1}{4^n} \sum_{b\in\{0,1\}^n} \sum_{\theta\in\{+,\times\}^n} \tilde{\varepsilon}_{\theta,b}(n). \tag{14}$$

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

$$|\psi^*_{\theta,b}\rangle = \alpha(C_n^A \odot C_n^B)\,|b\rangle_\theta^{channel} + \beta(C_n^A \odot C_n^B)\,|0^n\rangle_{+^n}^{channel} \tag{15}$$

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 behaviour with probability $|\alpha|^2$ and the trivial attack consisting in not measuring the BB84 qubits received with probability $|\beta|^2$. The expected probability of success $p^*(n)$ is

$$p^*(n) = |\alpha|^2 + |\beta|^2(\frac{3}{4})^n \approx |\alpha|^2 \tag{16}$$

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

$$\varepsilon^*(n) = \frac{|\alpha|^2}{2}(\frac{1}{2})^n + \frac{|\beta|^2}{2} \approx \frac{|\beta|^2}{2} \tag{17}$$

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 allowing to extract $[b]$ perfectly. Such an attack does not enable the committer to break the binding property of the string commitment but 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 (15). The second flavor captures stronger adversaries for which our reduction will be shown to produce attacks against the $\mathcal{F}^n_{m(n)}$–binding property of the string commitment.

**Definition 2.** *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 (12) and (14) respectively.*

## 4 The Reduction

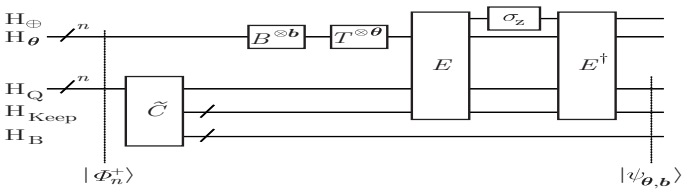
Using a *good* adversary $\tilde{\mathcal{A}}$ against QMC, we would like to build an adversary for the $F$-binding property of the string commitment scheme. In this section, we provide such a reduction provided $\tilde{\mathcal{A}}$'s parity extractor

is perfect. We construct a circuit built from $\tilde{\mathcal{A}}$ that allows to prepare a commitment from which any $|\psi_{\theta,b}\rangle$ can be generated efficiently during the opening phase. In Sect. 5, we shall use the resulting circuit, called the *switching circuit*, to provide an attack against the binding property of 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 qubit 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 $H_\Theta$ 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 $H_\Theta$ 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 $\sigma_Z$ is applied upon the extractor's output register $H_\oplus$. The transformation is completed by running the extractor in reverse. The following circuit is called the *switching circuit*:




Next, we see that whenever the parity extractor is perfect (i.e. $\tilde{E}_n \equiv E_n$), 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,

$$\begin{aligned} |\Phi_n^+\rangle \;&\equiv\; \sum_s \frac{1}{\sqrt{2^n}}\,|s\rangle\,|s\rangle \overset{\tilde{C}_n}{\longmapsto} \sum_s \frac{1}{\sqrt{2^n}}\,|s\rangle\,|\psi_{+^n,s}\rangle \\ &\overset{B^{\otimes b}}{\longmapsto} \sum_s \frac{(-1)^{b\odot s}}{\sqrt{2^n}}\,|b\oplus s\rangle\,|\psi_{+^n,s}\rangle \end{aligned} \tag{18}$$

$$\overset{T^{\otimes\theta}}{\longmapsto} \sum_{s,t\,:\,t\preceq\theta} \frac{(-1)^{b\odot s \,\oplus\, b\odot t \,\oplus\, s\odot t}}{\sqrt{2}^{n+|\theta|}} \,|b\oplus s\oplus t\rangle\,|\psi_{+^n,s}\rangle \tag{19}$$

$$= \sum_{\substack{s,t,v\,:\\ t\preceq\theta\\ v\preceq b\oplus s\oplus t}} \frac{(-1)^{b\odot t \,\oplus\, s\odot v \,\oplus\, s\odot s}}{\sqrt{2}^{n+|\theta|+|b\oplus s\oplus t|}} \,|b\oplus s\oplus t\rangle\,|\psi_{b\oplus s\oplus t,s\oplus v}\rangle. \tag{20}$$

The intermediary states up to (19) are obtained by definition of $|\Phi_n^+\rangle, \tilde{C}_n, B^{\otimes b}$, and $T^{\otimes\theta}$. Equation (20) follows after changing the basis from $+^n$ to $b\oplus s\oplus t$ using (10). From (20), we follow the evolution through $E_n^\dagger\sigma_Z E_n$,

$$|\Psi_{\theta,b}\rangle \quad\equiv\quad T^{\otimes\theta}B^{\otimes b}\mathcal{C}_n\,|\Phi_n^+\rangle \tag{21}$$

$$\overset{E_n^\dagger\sigma_z E_n}{\longmapsto} \sum_{\substack{s,t,v\,:\\ t\preceq\theta\\ v\preceq b\oplus s\oplus t}} \frac{(-1)^{b\odot t \,\oplus\, s\odot v \,\oplus\, v\odot v}}{\sqrt{2}^{n+|\theta|+|b\oplus s\oplus t|}} \,|b\oplus s\oplus t\rangle\,|\psi_{b\oplus s\oplus t,s\oplus v}\rangle \tag{22}$$

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

$$= \sum_{y\preceq x} \frac{(-1)^{b\odot\theta \,\oplus\, b\odot x \,\oplus\, b\odot y}}{\sqrt{2}^{n+|\theta|+|\theta\oplus x|-2|\theta\wedge\bar{x}|}} \,|\theta\oplus x\rangle\,|\psi_{\theta\oplus x,b\oplus y}\rangle$$

$$= \sum_{y\preceq x} \frac{(-1)^{b\odot\theta \,\oplus\, b\odot x \,\oplus\, b\odot y}}{\sqrt{2}^{n+|x|}} \,|\theta\oplus x\rangle\,|\psi_{\theta\oplus x,b\oplus y}\rangle \tag{23}$$

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

$$= \sum_{x} \frac{(-1)^{b\odot\theta}}{\sqrt{2}^{n}} \,|\theta\oplus x\rangle\,|\psi_{\theta,b}\rangle. \tag{24}$$

Equation (22) follows from the fact that the extractor is perfect. Equation (23) follows after using (1). We finally get (24) from (10).

In conclusion, a perfect extractor allows to produce a commitment inside which any $|\psi_{\theta,b}\rangle$ can be put *efficiently* during the opening 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 behaviour of the switching circuit by a table.In Sect. 5.3, we relate the table representation to attacks against the $\mathcal{F}^n_{m(n)}$–binding property of the string commitment.

### 5.1 Generalization to Imperfect Extractors

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

$$\tilde{E}_n \,|\theta\rangle^{\Theta} \,|\psi_{\theta,b}\rangle = \,|\theta\rangle^{\Theta} \otimes \left(\gamma_{\theta,b} \,|[b]\rangle^{\oplus} \,|\varphi_{\theta,b}\rangle + \hat{\gamma}_{\theta,b} \,|1 \oplus [b]\rangle^{\oplus} \,|\hat{\varphi}_{\theta,b}\rangle\right). \quad (25)$$

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 (14), the expected bias provided by $\tilde{E}_n$ is,

$$\tilde{\varepsilon}(n) \equiv 4^{-n} \sum_{\theta} \sum_{b} \tilde{\varepsilon}_{\theta,b}(n) = 4^{-n} \sum_{\theta} \sum_{b} \left| |\gamma_{\theta,b}|^2 - \frac{1}{2} \right|. \quad (26)$$

Compared to the case where the extractor is perfect, only the effect of transformation $\tilde{E}^{\dagger}_n \sigma_Z \tilde{E}_n$ needs to be recalculated. From (25), we obtain,

$$\begin{aligned} &\tilde{E}^{\dagger}_n \sigma_Z \tilde{E}_n \,|\theta\rangle \,|\psi_{\theta,b}\rangle = \\ &\qquad (-1)^{[b]} \,|\theta\rangle \,|\psi_{\theta,b}\rangle - 2(-1)^{[b]} \hat{\gamma}_{\theta,b} \tilde{E}^{\dagger}_n \left( \,|\theta\rangle \,|1 \oplus [b]\rangle^{\oplus} \,|\hat{\varphi}_{\theta,b}\rangle \right). \end{aligned} \quad (27)$$

We now define the vector $\boldsymbol{e}_{\theta,b}$ such that

$$|\theta\rangle \otimes \boldsymbol{e}_{\theta,b} \equiv -2\hat{\gamma}_{\theta,b} \tilde{E}^{\dagger}_n (\,|\theta\rangle \,|1 \oplus [b]\rangle \,|\hat{\varphi}_{\theta,b}\rangle)$$

so that (27) becomes

$$(\tilde{E}^{\dagger}_n \sigma_Z \tilde{E}_n) \,|\theta\rangle \,|\psi_{\theta,b}\rangle = (-1)^{[b]} \,|\theta\rangle \otimes (\,|\psi_{\theta,b}\rangle + \boldsymbol{e}_{\theta,b}). \quad (28)$$

The final state $|\tilde{\Psi}_{\theta,b}\rangle$ produced by the switching circuit can be obtained from (22) using (28). We get,

$$\begin{aligned} &\tilde{E}^{\dagger}_n \sigma_z \tilde{E}_n T^{\otimes\theta} B^{\otimes b} \mathcal{C}_n \,|\Phi^+_n\rangle = \\ &\qquad \sum_{y \preceq x} \frac{(-1)^{b \odot \theta \,\oplus\, b \odot x \,\oplus\, b \odot y}}{\sqrt{2}^{n+|x|}} \,|\theta \oplus x\rangle \otimes (\,|\psi_{\theta\oplus x, b\oplus y}\rangle + \boldsymbol{e}_{\theta\oplus x, b\oplus y}). \end{aligned} \quad (29)$$

Splitting the inner sum of (29) gives,

$$|\tilde{\Psi}_{\theta,b}\rangle = \,|\Psi_{\theta,b}\rangle - \boldsymbol{F}_{\theta,b} \quad (30)$$

where

$$|\Psi_{\theta,b}\rangle = \sum_{y\preceq x} \frac{(-1)^{b\odot\theta\oplus b\odot x\oplus b\odot y}}{\sqrt{2}^{n+|x|}}\ |\theta\oplus x\rangle\ |\psi_{\theta\oplus x,b\oplus y}\rangle, \text{ and}$$

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

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 (24)). The second part is the error term for which next lemma gives a precise characterization.

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

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

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

$$\begin{aligned} & 2^{-n}\textstyle\sum_{b\in\{0,1\}^n} \|\boldsymbol{F}_{\theta,b}\|^2 \qquad (31)\\ &= 2^{-n}\sum_b \|\sum_{y\preceq x} \frac{(-1)^{b\odot\theta\oplus b\odot x\oplus b\odot y}}{\sqrt{2}^{n+|x|}}\ |\theta\oplus x\rangle\otimes \boldsymbol{e}_{\theta\oplus x,b\oplus y}\|^2 \\ &= 2^{-n}\sum_b \|\sum_{x} \frac{(-1)^{b\odot\theta\oplus b\odot x}}{\sqrt{2}^{n+|x|}}\ |\theta\oplus x\rangle\otimes \sum_{y:y\preceq x}(-1)^{b\odot y}\boldsymbol{e}_{\theta\oplus x,b\oplus y}\|^2 \\ &= 2^{-2n-|x|}\sum_x\sum_b \|\sum_{y:y\preceq x}(-1)^{b\odot y}\boldsymbol{e}_{\theta\oplus x,b\oplus y}\|^2, \qquad (32)\end{aligned}$$

where (32) is obtained from the orthogonality of all terms $\boldsymbol{e}_{\theta\oplus x,b\oplus y}$ when $x$ varies, and from Phytagoras theorem. We now apply Lemma 1 to (32) with $A = \{y\in\{0,1\}^n | y\preceq x\}$, $w\equiv b$,$z\equiv y$, and $\boldsymbol{v}_{w,z}\equiv \boldsymbol{e}_{\theta\oplus x,b\oplus y}$. Let us 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 $x \in \{0,1\}^n$,

$$\sum_b \| \sum_{y:y\preceq x} (-1)^{b\odot y} \boldsymbol{e}_{\theta\oplus x, b\oplus y}\|^2 = \sum_{y:y\preceq x}\sum_b \|\boldsymbol{e}_{\theta\oplus x,b\oplus y}\|^2 \leq 2^{n+|x|}(2-4\tilde{\varepsilon}(n)). \tag{33}$$

The result follows after replacing (33) in (32). □

Using Lemma 2, we show how the the output of the switching circuit with imperfect extractors approaches the one with perfect extractors. The next lemma gives an upper bound on the expected overlap between the states produced in the two cases.

**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 (30), 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,

$$|\alpha_{\theta,b}| = \frac{\|\boldsymbol{F}_{\theta,b}\|^2}{2}. \tag{34}$$

Using (34) and Lemma 2 gives, $S_{\tilde{\mathcal{A}}} = \sum_{\theta,b} 4^{-n}|\langle\tilde{\Psi}_{\theta,b}|\Psi_{\theta,b}\rangle| \geq \sum_{\theta,b} 4^{-n}(1-|\alpha_{\theta,b}|) = 1 - \sum_{\theta,b} 4^{-n}\frac{\|\boldsymbol{F}_{\theta,b}\|^2}{2} \geq 2\tilde{\varepsilon}(n)$. □

Lemma 3 tells us that with a *good* extractor, one can generate states having *large* overlap with all QMCs to different BB84 qubits after the end of the committing stage.

### 5.2 Representing The Switching Circuit by a Table

In this section, we look at how to use the switching circuit in order to obtain an attack against the binding condition 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 (11). 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 $(\theta,b)$. The row $(\theta,b)$ contains values $T_{\theta,b}(\tau,\beta) = \|\mathbb{Q}^B_{(\theta\oplus\tau,b\oplus\beta)}\,|\psi_{\theta,b}\rangle\|^2$ for all $(\tau,\beta)$ such that $(\theta\oplus\tau, b\oplus\beta) \in \Delta_{\preceq}(\theta,b)$. This condition is equivalent to $(\tau,\beta)$ such that $\beta \preceq \tau$. The table values for the case $n=1$ are shown in Fig. 1. The sum of each row is added to the right. The construction

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

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

is easily generalized for arbitrary $n$. Each 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,

$$T_{\theta,b}(\tau,\beta) = \|\mathbb{Q}^B_{(\theta\oplus\tau,b\oplus\beta)}\,|\tilde{\Psi}_{\theta,b}\rangle\|^2. \tag{35}$$

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 $\tilde{\mathcal{A}}$ adds up to $4^n poly(\delta(n))$. The proof is a consequence of 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*

$$\sum_{\theta,b,\tau}\sum_{\beta\preceq\tau} T_{\theta,b}(\tau,\beta) \geq \frac{4^n\delta(n)^3}{32}. \tag{36}$$

Theorem 1 establishes the existence of one column in table $T_{\tilde{\mathcal{A}}}$ providing a *weak* attack against the binding property since any table with $3^n$

columns all summing up to more than $\frac{4^n\delta(n)^3}{32}$ has one column exceeding $(\frac{2}{3})^n\frac{\delta(n)^2}{32} \geq 1 + 1/poly(n)$. Let $(\tau, \beta)$ be such a column and consider the class of functions $\mathbb{1}_{2n}$ containing only the identity. 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 $\sum_{(y,y')}\tilde{p}^f_{(y,y')}(n) = \sum_{(y,y')}T_{y\oplus\tau,y'\oplus\beta}(\tau, \beta) > 1 + 1/poly(n)$ which provides an attack against the $\mathbb{1}_{2n}$–binding property of string commitment according (7). As we have seen in Sect. 3.1 however, this attack might not even be statistically distinguishable from the trivial adversary. 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 $\mathcal{F}^n_{m(n)}$–binding property of the $2n$–string commitment with $m(n) \in O(polylog(n))$ whenever $\delta(n) \geq 1/poly(n)$. We show this using a counting argument. We cover uniformly the table $T_{\tilde{\mathcal{A}}}$ with all attacks in $\mathcal{F}^n_{m(n)}$. Theorem 1 is then invoked in order to conclude that for some $f \in \mathcal{F}^n_{m(n)}$, condition (7) does not hold.

Attacking the binding condition according to a function $f \in \mathcal{F}^n_{m(n)}$ 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 $2^{m(n)}$ while the number of columns can be shown to be $2^{m(n)}3^{n-m(n)}$ (see Appendix C and Lemma 4). This means that any attack in $\mathcal{F}^n_{m(n)}$ covers $t = 3^{n-m(n)}4^{m(n)}$ 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 $t_{\tilde{\mathcal{A}}} = 3^n4^n$ 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 the attacks in $\mathcal{F}^n_{m(n)}$ covers $T_{\tilde{\mathcal{A}}}$ uniformly:

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

Let $s^*$ be the maximum of (7) for all attacks $f \in \mathcal{F}^n_{m(n)}$. 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 $f \in \mathcal{F}^n_{m(n)}$ is uniform and $a \cdot t/t_{\tilde{\mathcal{A}}}$ is the number of times $T_{\tilde{\mathcal{A}}}$ is generated by attacks in $\mathcal{F}^n_{m(n)}$. In

other words,

$$a \cdot s^* \geq \frac{a \cdot t \cdot s_{\tilde{\mathcal{A}}}}{t_{\tilde{\mathcal{A}}}} = \frac{a \cdot t \cdot s_{\tilde{\mathcal{A}}}}{3^n 4^n} \Rightarrow s^* \geq \frac{t \cdot s_{\tilde{\mathcal{A}}}}{3^n 4^n} = \frac{4^{m(n)} \cdot s_{\tilde{\mathcal{A}}}}{3^{m(n)} 4^n}. \quad (37)$$

Assuming that $\tilde{\mathcal{A}}$ is $\delta(n)$–good, Theorem 1 tells us that $s_{\tilde{\mathcal{A}}} \geq \frac{4^n \delta(n)^3}{32}$. Replacing in (37) finally leads to,

$$s^* \geq \frac{\delta(n)^3 4^{m(n)}}{32 \cdot 3^{m(n)}} \geq 1 + \delta(n), \quad (38)$$

for any $m(n) \geq \lceil \log_{\frac{4}{3}} \left( \frac{32}{\delta(n)^3} \right) \rceil$. Equation (38) guarantees that for at least one $f \in \mathcal{F}^n_{m(n)}$, condition (7) is not satisfied thereby providing an attack against the $\mathcal{F}^n_{m(n)}$–binding property of the string commitment. Moreover, for $\delta(n) \geq 1/poly(n)$ it is sufficient that $m(n) \in O(polylog(n))$.

## 6 The Main Result and Its Application to Oblivious Transfer

Putting together Theorem 1 and (38) leads to our main result:

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

Theorem 2 has an immediate application to the security of $1-2$-OT in the computational setting. We can easily observe that a QMC implements a *weak* $1-2$ *oblivious transfer* (i.e. WOT) where 1)the sender has no information about the receiver's selection bit and 2)the receiver, according Theorem 2, can only extract a limited amount of information about both bits (provided the string commitments are $\mathcal{F}^n_{m(n)}$-binding). The following primitive, called $\mathcal{W}_n$, accepts $\mathcal{B}$'s input bits $(\beta_0, \beta_1)$ and $\mathcal{A}$'s selection bit $s$ and builds a WOT from a QMC:

`Protocol` $\mathcal{W}_n$

1. $\mathcal{B}$ and $\mathcal{A}$ run the committing phase of a QMC (i.e. built upon any $\mathcal{F}^n_{m(n)}$-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 OK then $\mathcal{A}$ and $\mathcal{B}$ return to 1 otherwise $\mathcal{B}$ ABORTS,

– if $c = 1$ then $\mathcal{B}$ announces $\theta$, $\mathcal{A}$ announces a partition $I_0, I_1 \subseteq \{1, \ldots, n\}$, 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 $1-2$ OT since an honest receiver $\mathcal{A}$ can always get bit $\beta_s = b_s \oplus a_s$ by announcing $I_s$ such that for all $i \in I_s$ the measurements were made in basis $\hat{\theta}_i = \theta_i$. The adversary $\tilde{\mathcal{A}}$'s information about the other bit can be further reduced using the following simple protocol accepting $\mathcal{B}$'s input bits $(\beta_0, \beta_1)$ and the selection bit $s$ for the honest receiver:

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

1. $\mathcal{W}$ is executed $t$ times, with inputs $(\beta_{0i}, \beta_{1i}), i = 1..t$ for the sender and input $s$ for the receiver where $\beta_{01} \oplus \ldots \oplus \beta_{0t} = \beta_0$ 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 R-Reduce$(t, \mathcal{W}_n)$ is *promising* if it runs in polytime 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* R-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 $t$.*

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 $(\beta_{0i}, \beta_{1i})$ cannot be guessed with bias better than $\varepsilon_{max}(\delta) < 1$. In this case, the guessing probability for the parity of the $t$ random bits can be shown to approach $\frac{1}{2}$ exponentially fast in $t$ as one would expect in the classical case.

Clearly, the sender $\mathcal{B}$ in R-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 R-Reduce$(t, \mathcal{W}_n)$ lead to:

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

In other words, basing the security of $1-2$-OT upon Theorem 2 allows for a simple proof of security in the computational setting. Note that for simplicity, we assumed an error-free quantum channel.

## 7 Conclusion and Open Questions

Our first open question is 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 optimal. It is also of interest to find attacks against weaker binding properties. In particular, is it possible to transform an adversary against QMC into one against the $F$–binding property where $F$ is class of functions with range of size in $o(\log 1/\delta(n))$? Our transformation of an adversary against QMC to one against the binding condition is non-uniform since we did not provide an efficient way to find an $f$–attack against the binding property. Our result would be stronger if a uniform reduction was found. It is also an interesting problem to show that the computationally binding bit commitments of [10] and [8] can be turned the obvious way into $\mathcal{F}^n_{m(n)}$–binding string commitments. This would show that QMCs and therefore OT can be based upon any one-way permutation from [10] and upon any one-way function from [8]. Recent work of Mayers [18] seems to indicate that it is indeed the case for [10].

Finally, it would be of great interest to formally proof the security of the BBCS 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 original proof [22]. It is also an interesting problem to proof Corollary 1 in the case where the quantum channel is not error-free.

## 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)*,to appear, 2002.
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*, pages 175–179. IEEE, 1984.

3. Barenco, A., C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin and H. Weinfurter, "Elementary Gates for Quantum Computation", *Physical Review A*, vol. 52, no. 5, November 1995, pp. 3457–3467.
4. Bennett, C. H., G. Brassard, C. Crépeau and M.-H. Skubiszewska, "Practical Quantum Oblivious Transfer", *Advances in Cryptology : CRYPTO '91 : Proceedings*, Lecture Notes in Computer Science, vol. 576, Springer-Verlag, august 1992, pp. 362–371.
5. Brassard, G., D. Chaum and C. Crépeau, "Minimum Disclosure Proofs of Knowledge", *Journal of Computing and System Science*, vol. 37 , 1988, pp. 156–189.
6. Crépeau, C., "Quantum Oblivious Transfer", *Journal of Modern Optics*, vol. 41, no 12, December 1994, pp. 2445–2454.
7. Crépeau, C. and J. Kilian, "Achieving oblivious transfer using weakened security assumptions", *Proceedings of 29th IEEE Symposium on the Foundations of Computer Science*, October 1988, pp. 42–52.
8. Crépeau, C., F. Légaré, and L. Salvail, "How to Convert the Flavor of a Quantum Bit Commitment", *Advances in Cryptology : EUROCRYPT '01 : Proceedings*, Lecture Notes in Computer Science, vol. 2045 , Springer-Verlag, 2001, pp. 60–77.
9. Damgård, I., J. Kilian, and L. Salvail, "On the (Im)possibility of Basing Oblivious Transfer and Bit Commitment on Weakened Security Assumptions", *Advances in Cryptology : EUROCRYPT '99 : Proceedings*, Lecture Notes in Computer Science, vol. 1592, Springer-Verlag, 1999, pp. 56–73.
10. Dumais, P., D. Mayers, and L. Salvail, "Perfectly Concealing Quantum Bit Commitment From Any Quantum One-Way Permutation", *Advances in Cryptology : EUROCRYPT '00 : Proceedings*, Lecture Notes in Computer Science, vol. 1807, Springer-Verlag, 2000, pp. 300–315.
11. Goldreich, O., and L. Levin,"A Hard-Core Predicate for Any One-Way Function", *Proceedings of the 21st ACM Symposium on Theory of Computing*, 1989, pp. 25–32.
12. Impagliazzo, R. and S. Rudich, "Limits on Provable Consequences of One-Way Permutations", *Advances in Cryptology : CRYPTO '88 : Proceedings*, Lecture Notes in Computer Science, vol. 403, Springer-Verlag, 1989, pp. 2–7.
13. Kilian, J., "Founding cryptography on oblivious transfer", *Proceedings of the 20th ACM Symposium on Theory of Computing*, 1988, pp. 20–31.
14. Lo, H.–K.,and H. F. Chau, "Is quantum Bit Commitment Really Possible?", *Physical Review Letters*, vol. 78, no 17, April 1997, pp. 3410–3413.
15. Levin, L., "One-way Functions and Pseudorandom Generators ", *Proceedings of the 17th ACM Symposium on Theory of Computing*, 1985, pp. 363–365.
16. Mayers, D., "The Trouble With Quantum Bit Commitment", available at `http://xxx.lanl.gov/abs/quant-ph/9603015`.
17. Mayers, D., "Unconditionally Secure Quantum Bit Commitment is Impossible", *Physical Review Letters*, vol. 78, no 17, April 1997, pp. 3414–3417.
18. Mayers, D., in preparation, 2002.
19. Nielsen, M.A,and I.L. Chuang, "Quantum Computation and Quantum Information", *Cambridge University Press*, 2000.
20. van de Graaf, J., *Torwards a Formal Definition of Security for Quantum Protocols*, Ph.D. thesis, Computer Science and Operational Research Department, Université de Montréal, 1997.

21. Yao, A. C., "Theory and Applications of Trapdoor Functions", *Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science*, 1982, pp. 80–91.
22. 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 1

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,

$$\begin{aligned}&(\forall s,t \in\{0,1\}^n, s \neq t)\\ &\qquad [\sum_{w} \sum_{z_1:w\oplus z_1=s} \sum_{z_2:w\oplus z_2=t} (-1)^{w\odot(z_1\oplus z_2)} \langle \boldsymbol{u}_{w,z_1}, \boldsymbol{u}_{w,z_2}\rangle = 0]\end{aligned} \tag{39}$$

Then,

$$\sum_{w} \| \sum_{z} (-1)^{w\odot z} \boldsymbol{u}_{w,z}\|^2 = \sum_{w,z\in\{0,1\}^n} \|\boldsymbol{u}_{w,z}\|^2. \tag{40}$$

*Proof.* We carry out the calculation for (40):

$$\begin{aligned}\sum_{w} \| \sum_{z} (-1)^{w\odot z}\ \boldsymbol{u}_{w,z}\ \|^2 &= \sum_{w} \langle \sum_{z_1} (-1)^{w\odot z_1} \boldsymbol{u}_{w,z_1}, \sum_{z_2} (-1)^{w\odot z_2} \boldsymbol{u}_{w,z_2}\rangle\\ &= \sum_{w,z_1,z_2} (-1)^{w\odot(z_1\oplus z_2)} \langle \boldsymbol{u}_{w,z_1}, \boldsymbol{u}_{w,z_2}\rangle\\ &= \sum_{w,z} \|\boldsymbol{u}_{w,z}\|^2 + \sum_{w,z_1,z_2:z_1\neq z_2} (-1)^{w\odot(z_1\oplus z_2)} \langle \boldsymbol{u}_{w,z_1}, \boldsymbol{u}_{w,z_2}\rangle. \end{aligned} \tag{41}$$

We now re-arrange the terms in the right-hand part of (41):

$$\begin{aligned}&\sum_{w,z_1,z_2:z_1\neq z_2} (-1)^{w\odot(z_1\oplus z_2)} \langle \boldsymbol{u}_{w,z_1}, \boldsymbol{u}_{w,z_2}\rangle\\ &\qquad = \sum_{w,z_1} \sum_{s:w\oplus z_1=s} \sum_{z_2:z_2\neq z_1} \sum_{t:w\oplus z_2=t} \langle \boldsymbol{u}_{w,z_1}, \boldsymbol{u}_{w,z_2}\rangle\\ &\qquad = \sum_{s,t:s\neq t} \sum_{w} \sum_{z_1:w\neq z_1} \sum_{z_2:w\oplus z_2=t} \langle \boldsymbol{u}_{w,z_1}, \boldsymbol{u}_{w,z_2}\rangle\\ &\qquad = 0,\end{aligned} \tag{42}$$

where the final equality follows from condition (39). Replacing (42) in (41) concludes the proof. □

*Proof (Lemma 1).* The proof of 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 (39). Our result then follows from (40). □

## 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,

$$\tilde{p}^{ok}(n) + \sum_{\theta,b} 4^{-n} |\langle \Psi_{\theta,b} | \tilde{\Psi}_{\theta,b} \rangle|^2 = 4^{-n} \sum_{\theta,b} \left( \tilde{p}^{ok}_{(\theta,b)}(n) + |\langle \Psi_{\theta,b} | \tilde{\Psi}_{\theta,b} \rangle|^2 \right) \geq 1 + \delta(n). \tag{43}$$

The sum of any row $(\theta, b) \in T_{\tilde{\mathcal{A}}}$ is given by,

$$\begin{aligned} &\| \mathbb{Q}^*_{(\theta,b)} \, |\tilde{\Psi}_{\theta,b}\rangle \|^2 \geq \\ &\qquad \| \mathbb{Q}^*_{(\theta,b)} \left( |\langle \Psi_{\theta,b} | \tilde{\Psi}_{\theta,b} \rangle| \, |\Psi_{\theta,b}\rangle - \sqrt{1 - |\langle \Psi_{\theta,b} | \tilde{\Psi}_{\theta,b} \rangle|^2} \, |\Psi^{\perp}_{\theta,b}\rangle \right) \|^2, \end{aligned} \tag{44}$$

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 $|\alpha_{\theta,b}| \leq \sqrt{1 - \tilde{p}^{ok}_{(\theta,b)}(n)}$. Using the above observations [4], we rewrite (44) as,

$$\begin{aligned} \| \mathbb{Q}^*_{(\theta,b)} \, |\tilde{\Psi}_{\theta,b}\rangle \|^2 \geq & \frac{1}{4} ( \| \langle \Psi_{\theta,b} | \tilde{\Psi}_{\theta,b} \rangle \mathbb{Q}^*_{(\theta,b)} \, |\Psi_{\theta,b}\rangle \|^2 \\ & \qquad - \| \sqrt{1 - |\langle \Psi_{\theta,b} | \tilde{\Psi}_{\theta,b} \rangle|^2} \mathbb{Q}^*_{(\theta,b)} \, |\Psi^{\perp}_{\theta,b}\rangle \|^2 )^2 \\ \geq & \frac{1}{4} ( |\langle \Psi_{\theta,b} | \tilde{\Psi}_{\theta,b} \rangle \sqrt{\tilde{p}^{ok}_{(\theta,b)}(n)}|^2 \\ & \qquad - |\sqrt{1 - |\langle \Psi_{\theta,b} | \tilde{\Psi}_{\theta,b} \rangle|^2} |\alpha_{\theta,b}| |^2 )^2 \\ \geq & \frac{1}{4} ( |\langle \Psi_{\theta,b} | \tilde{\Psi}_{\theta,b} \rangle|^2 \tilde{p}^{ok}_{(\theta,b)}(n) - \\ & \quad (1 - |\langle \Psi_{\theta,b} | \tilde{\Psi}_{\theta,b} \rangle|^2)(1 - \tilde{p}^{ok}_{(\theta,b)}(n)) )^2 \end{aligned}$$

[4] and the fact that $(\sqrt{a} - \sqrt{a-b})^2 \geq 1/4b^2$ for any $0 \leq b \leq a \leq 1$.

$$\geq \frac{1}{4}\left(\tilde{p}^{ok}_{(\theta,b)}(n) + |\langle \Psi_{\theta,b}|\tilde{\Psi}_{\theta,b}\rangle|^2 - 1\right)^2. \quad (45)$$

Since $\tilde{\mathcal{A}}$ is $\delta(n)$–good, we use (43) to conclude that the set $G = \{(\theta,b)|\tilde{p}^{ok}_{(\theta,b)}(n) + |\langle \Psi_{\theta,b}|\tilde{\Psi}_{\theta,b}\rangle|^2 \geq 1 + \frac{\delta(n)}{2}\}$ must satisfy $\#G \geq 4^n\delta(n)/2$. Any $(\theta,b) \in G$ is such that (45) 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 $f \in \mathcal{F}^n_{m(n)}$. We call such an attack an $f$-attack since its purpose is to try to open $s \in f^{-1}(y)$ for any $y \in \{0,1\}^{m(n)}$. To make the description easier, let us consider the case $n = 1$ resulting in table $T_{\tilde{\mathcal{A}}}$ shown at Fig. 2 (this is almost identical to Fig.1). We have seen how

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

**Fig. 2.** Table $T_{\tilde{\mathcal{A}}}$ for the case $n = 1$.

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 as length 2) according to function $f_1 \in \mathcal{F}^n_1$ 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

$$\tilde{p}^f_0(n) = \|(\mathbb{Q}^B_{(+,0)} + \mathbb{Q}^B_{(\times,0)})\,|\tilde{\Psi}_{+,0}\rangle\|^2 \text{ and } \tilde{p}^f_1(n) = \|(\mathbb{Q}^B_{(+,1)} + \mathbb{Q}^B_{(\times,1)})\,|\tilde{\Psi}_{+,1}\rangle\|^2.$$

The quality of this $f_1$–attack is given by (2). That is, the attack succeed if $\tilde{p}^f_0(n) + \tilde{p}^f_1(n) > 1 + \delta$ for some large enough $\delta$. Looking at Fig. 2, this particular $f_1$–attack is formed by the $2\times 2$ upper left sub-array of $T_{\tilde{\mathcal{A}}}$. The quality of the attack $\tilde{p}^f_0(n) + \tilde{p}^f_1(n)$ 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 $2 \times 2$ 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 ($f \in \mathcal{F}^n_{m(n)}$) is $2^{m(n)}$ and the number of columns is $2^{m(n)}3^{n-m(n)}$. That is, the number of elements in $T_{\tilde{\mathcal{A}}}$ involved in such an $f$–attack is $4^{m(n)}3^{n-m(n)}$. 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:

$$r_1,\ r_2,\ \ldots,\ r_n \in \{0,1,2,3\}, \tag{46}$$

$$u_1,\ u_2,\ \ldots,\ u_n \in \{\mathtt{0},\mathtt{1}\}, \tag{47}$$

$$v_1,\ v_2,\ \ldots,\ v_n \in \{\mathtt{0},\mathtt{1}\} \tag{48}$$

subject to the condition

$$\#\{j\ :\ r_j \neq 0\} = m. \tag{49}$$

Accordingly, there will be $C(m,n)3^m4^n$ 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 (49). We now describe the sub-array defined by that choice. The column $(\tau, \beta)$ is part of the sub-array if and only if:

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

$$r_j = 1 \Longrightarrow (\tau_j, \beta_j) \in \{(1,0),(1,1)\} \qquad \text{i.e.: } \tau_j = 1, \tag{51}$$

$$r_j = 2 \Longrightarrow (\tau_j, \beta_j) \in \{(0,0),(1,0)\} \qquad \text{i.e.: } \beta_j = 0, \tag{52}$$

$$r_j = 3 \Longrightarrow (\tau_j, \beta_j) \in \{(0,0),(1,1)\} \qquad \text{i.e.: } \beta_j = \tau_j. \tag{53}$$

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

$$r_j = 0 \Longrightarrow (\theta_j, b_j) \in \{(u_j, v_j)\}, \tag{54}$$

$$r_j = 1 \Longrightarrow (\theta_j, b_j) \in \{(0, u_j),(1, v_j)\}, \tag{55}$$

$$r_j = 2 \Longrightarrow (\theta_j, b_j) \in \{(u_j, 0),(v_j, 1)\}, \tag{56}$$

$$r_j = 3 \Longrightarrow (\theta_j, b_j) \in \{(u_j, u_j),(v_j, 1-v_j)\}. \tag{57}$$

One can easily verify that the lines (50) to (57) 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 (46) to (48) will lead to different sub-arrays.

We can now state and prove the combinatorial lemma:

**Lemma 5.** *Every cell $(\theta, b, \tau, \beta)$ of $T$ belongs to exactly $C(m,n)4^m$ sub-arrays.*

| 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. 3.** Eligible triplets $(r_j, u_j, v_j)$ given $(\theta_j, b_j, \tau_j, \beta_j)$

*Proof.* Let us fix $j \in \{1, \ldots, n\}$. Figure 3 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 $(\theta_j, b_j, \tau_j, \beta_j)$ 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. □

## 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:

$$\tilde{p}^{ok}(n) + (2\tilde{\varepsilon}(n))^2 \leq 1 + 1/poly(n) \tag{58}$$

for some polynomial $poly(n)$ 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,

$$\begin{aligned} \tilde{p}_{abort,\mathcal{W}_n} &= \sum_{j=1}^{\infty} 2^{-j} (\tilde{p}^{ok}(n))^{j-1} (1 - \tilde{p}^{ok}(n)) \\ &> \frac{1 - \tilde{p}^{ok}(n)}{2} \Rightarrow \tilde{p}^{ok}(n) > 1 - 2\tilde{p}_{abort,\mathcal{W}_n}. \end{aligned} \tag{59}$$

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 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 $\mathtt{out}\{G_n \cdot (C_n |b\rangle_\theta) \otimes |\theta\rangle\}$ 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, $\Pr(h_I(b,s) \neq \mathtt{out}\{G_n \cdot (C_n |b\rangle_\theta) \otimes |\theta\rangle\}) \geq \frac{1}{2} - \epsilon$, 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 (59), we get that $\tilde{\mathcal{A}}$ also defines an adversary against QMC with $\tilde{p}^{ok}(n) \geq 1 - 2\delta$. From (58), we conclude that

$$\tilde{\varepsilon}(n) \leq \frac{\sqrt{2\delta + \frac{1}{poly(n)}}}{2} \tag{60}$$

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:

**Lemma 6.**

$$(\forall\{C_n\}_{n>0}\in\mathcal{C}_\delta)(\forall I\in\mathcal{I}_n)(\exists s\in\{0,1\})(\forall\{G_n\}_{n>0}\in QPoly(n))(\forall n>n_0)$$
$$\left[\Pr\left(h_I(b,s)\neq \mathtt{out}\left\{G_n\cdot(C_n\,|b\rangle_\theta)\otimes\,|\theta\rangle\right\}\right)\geq\frac{1-2\tilde{\varepsilon}(n)}{10}\right], \tag{61}$$

*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* $\delta$ *and* $n$ *defined in (60).*

The proof of Lemma 6 is easy and omitted due to space limitations. It 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 $\sqrt{2\delta+1/poly(n)}/2$ contradicting (58).

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

$$\tilde{p}_{abort}(1)=\tilde{p}_{abort,\mathcal{W}_n}\text{ and} \tag{62}$$
$$\tilde{p}_{abort}(\ell+1)=\tilde{p}_{abort}(\ell)+(1-\tilde{p}_{abort}(\ell))\tilde{p}_{stop}(\ell+1). \tag{63}$$

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 $\tilde{\mathcal{A}}=\{(C_{n,t},G_{n,t}^0,G_{n,t}^1)\}_{n,t>0}$ where $C_n$ runs the committing phase and circuits $G_n^0$ and $G_n^1$ 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* $\tilde{\mathcal{A}}=\{(C_{n,t},G_{n,t}^0,G_{n,t}^1)\}_{n,t>0}$ *against* R-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 (61) to any adversary $\tilde{\mathcal{A}}$ against R-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 R-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 R-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* R-Reduce$(t, \mathcal{W}_n)$ *are polynomially related. Then,*

$$\begin{aligned}
&(\forall \delta > 0)(\forall \gamma > 0)(\forall \text{ promising } \tilde{\mathcal{A}} = \{(C_{n,t}, \cdot)\}_{n,t>0}) \\
&(\exists L \subseteq \{1, \ldots, t\} : \#L \geq (1-\gamma)t)(\forall \ell \in L)(\forall I \in \mathcal{I}_n) \\
&(\exists s \in \{0,1\})(\forall \{G_{n,t}\}_{n,t>0} \in \mathrm{QPoly}(n,t)) \\
&\left[\Pr\left( h_I(b^{(\ell)}, s) \neq \mathtt{out}\{G_{n,t}(C_{n,t}\,|b\rangle_\theta) \otimes |\theta\rangle\} | \{(b^{(j)}, \theta^{(j)})\}_{j \neq \ell} \right) \right. \\
&\qquad\qquad \left. \geq \frac{1 - \sqrt{2\delta + \frac{1}{poly(n)}}}{10} \right],
\end{aligned} \tag{64}$$

*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 $i \in \{1, \ldots, t\}$.*

The proof can easily be obtained using Lemma 6.From Lemma 7, we would like to conclude that given any announcement $\boldsymbol{I} = (I^{(0)}, I^{(1)}, \ldots, I^{(t)})$ during R-Reduce$(t, \mathcal{W}_n)$, the *amplification function*

$$g_{\boldsymbol{I}}(b^{(1)}, \ldots, b^{(t)}, s) \equiv \bigoplus_{i=1}^{t} h_{I^{(i)}}(b^{(i)}, s) \in \{0,1\} \tag{65}$$

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.** *Let $n$ and $t$ be polynomially related security parameters in* R-Reduce$(t, \mathcal{W}_n)$. *Then,*

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

*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 $i \in \{1, \ldots, t\}$.*

# Recent BRICS Report Series Publications

**RS-03-3** Claude Crépeau, Paul Dumais, Dominic Mayers, and Louis Salvail. *On the Computational Collapse of Quantum Information*. January 2003. 31 pp.

**RS-03-2** Olivier Danvy and Pablo E. Martínez López. *Tagging, Encoding, and Jones Optimality*. January 2003. To appear in Degano, editor, *Programming Languages and Systems: Twelfth European Symposium on Programming*, ESOP '03 Proceedings, LNCS, 2003.

**RS-03-1** Vladimiro Sassone and Pawel Sobocinski. *Deriving Bisimulation Congruences: 2-Categories vs. Precategories*. January 2003. To appear in Gordon, editor, *Foundations of Software Science and Computation Structures*, FoSSaCS '03 Proceedings, LNCS, 2003.

**RS-02-52** Olivier Danvy. *A New One-Pass Transformation into Monadic Normal Form*. December 2002. 16 pp. To appear in Hedin, editor, *Compiler Construction, 12th International Conference*, CC '03 Proceedings, LNCS, 2003.

**RS-02-51** Gerth Stølting Brodal, Rolf Fagerberg, Anna Östlin, Christian N. S. Pedersen, and S. Srinivasa Rao. *Computing Refined Buneman Trees in Cubic Time*. December 2002. 14 pp.

**RS-02-50** Kristoffer Arnsfelt Hansen, Peter Bro Miltersen, and V. Vinay. *Circuits on Cylinders*. December 2002. 16 pp.

**RS-02-49** Mikkel Nygaard and Glynn Winskel. *HOPLA—A Higher-Order Process Language*. December 2002. 18 pp. Appears in Brim, Jančar, Křetínský and Antonín, editors, *Concurrency Theory: 13th International Conference*, CONCUR '02 Proceedings, LNCS 2421, 2002, pages 434–448.

**RS-02-48** Mikkel Nygaard and Glynn Winskel. *Linearity in Process Languages*. December 2002. 27 pp. Appears in Plotkin, editor, *Seventeenth Annual IEEE Symposium on Logic in Computer Science*, LICS '02 Proceedings, 2002, pages 433–446.