# Adaptive Versus Non-Adaptive Strategies in the Quantum Setting with Applications

Frédéric Dupuis[2], Serge Fehr[1], Philippe Lamontagne[3(✉)], and Louis Salvail[3]

[1] CWI, Amsterdam, The Netherlands
[2] Faculty of Informatics, Masaryk University, Brno, Czech Republic
[3] Université de Montréal (DIRO), Montréal, Canada
lamontph@iro.umontreal.ca

**Abstract.** We prove a general relation between *adaptive* and *non-adaptive* strategies in the quantum setting, i.e., between strategies where the adversary can or cannot adaptively base its action on some auxiliary quantum side information. Our relation holds in a very general setting, and is applicable as long as we can control the bit-size of the side information, or, more generally, its "information content". Since adaptivity is notoriously difficult to handle in the analysis of (quantum) cryptographic protocols, this gives us a very powerful tool: as long as we have enough control over the side information, it is sufficient to restrict ourselves to non-adaptive attacks.

We demonstrate the usefulness of this methodology with two examples. The first is a quantum bit commitment scheme based on *1-bit cut-and-choose*. Since bit commitment implies oblivious transfer (in the quantum setting), and oblivious transfer is universal for two-party computation, this implies the universality of 1-bit cut-and-choose, and thus solves the main open problem of [9]. The second example is a quantum bit commitment scheme proposed in 1993 by Brassard *et al.* It was originally suggested as an unconditionally secure scheme, back when this was thought to be possible. We partly restore the scheme by proving it secure in (a variant of) the bounded quantum storage model.

In both examples, the fact that the adversary holds quantum side information obstructs a direct analysis of the scheme, and we circumvent it by analyzing a non-adaptive version, which can be done by means of known techniques, and applying our main result.

## 1 Introduction

**Adaptive Versus Non-Adaptive Attacks.** We consider attacks on cryptographic schemes, and we compare adaptive versus non-adaptive strategies for the adversary. In our context, a strategy is *adaptive* if the adversary's action can depend on some auxiliary side information, and it is *non-adaptive* if the adversary has no access to any such side information. Non-adaptive strategies are typically much easier to analyze than adaptive ones.

Adaptive strategies are clearly more powerful than non-adaptive ones, but this advantage is limited by the amount and quality of the side-information available to the attacker. In the classical case, this can be made precise by the following

© International Association for Cryptologic Research 2016
M. Robshaw and J. Katz (Eds.): CRYPTO 2016, Part III, LNCS 9816, pp. 33–59, 2016.
DOI: 10.1007/978-3-662-53015-3_2

simple argument. If the side information consists of a classical $n$-bit string, then adaptivity increases the adversary's success probability in breaking the scheme by at most a factor of $2^n$. Indeed, a particular non-adaptive strategy is to try to guess the $n$-bit side information and then apply the best adaptive strategy. Since the guess will be correct with probability at least $2^{-n}$, it follows that $P_{\text{succ}}^{\text{NA}} \geq 2^{-n} P_{\text{succ}}^{\text{A}}$, and thus $P_{\text{succ}}^{\text{A}} \leq 2^n P_{\text{succ}}^{\text{NA}}$, where $P_{\text{succ}}^{\text{A}}$ and $P_{\text{succ}}^{\text{NA}}$ respectively denote the optimal adaptive and non-adaptive success probabilities for the adversary to break the scheme. Even though there is an exponential loss, this is a very powerful relation between adaptive and non-adaptive strategies as it applies very generally, and it provides a non-trivial bound as long as we can control the size of the side information, and the non-adaptive success probability is small enough.

**Our Technical Result.** In this work, we consider the case where the side information (and the cryptographic scheme as a whole) may be *quantum*. A natural question is whether the same (or a similar) relation holds between adaptive and non-adaptive quantum strategies. The quantum equivalent to guessing the side information would be to emulate the $n$-qubit quantum side information by the completely mixed state $\frac{\mathbb{I}_A}{2^n}$. Since it always holds that $\rho_{AB} \leq 2^{2n} \frac{\mathbb{I}_A}{2^n} \otimes \rho_B$, we immediately obtain a similar relation $P_{\text{succ}}^{\text{A}} \leq 2^{2n} P_{\text{succ}}^{\text{NA}}$, but with an additional factor of 2 in the exponent. The bound is tight for certain choices of $\rho_{AB}$, and thus this additional loss is unavoidable in general; this seems to mostly answer the above question.

In this work, we show that this is actually not yet the end of the story. Our main technical result consists of a more refined treatment — and analysis — of the relation between adaptive and non-adaptive quantum strategies. We show that in a well-defined and rather general context, we can actually bound $P_{\text{succ}}^{\text{A}}$ as

$$P_{\text{succ}}^{\text{A}} \leq 2^{I_{\max}^{\text{acc}}(B;A)} P_{\text{succ}}^{\text{NA}},$$

where $I_{\max}^{\text{acc}}(B;A)$ is a new (quantum) information measure that is upper bounded by the number of qubits of $A$. As such, we not only recover the classical relation $P_{\text{succ}}^{\text{A}} \leq 2^n P_{\text{succ}}^{\text{NA}}$ in the considered context, but we actually improve on it.

In more detail, we consider an abstract "game", specified by an arbitrary bipartite quantum state $\rho_{AB}$, of which the adversary Alice and a challenger Bob hold the respective registers $A$ and $B$, and by an arbitrary family $\{E^j\}_{j \in \mathcal{J}}$ of binary-outcome POVMs acting on register $B$. The game is played as follows: Alice chooses an index $j$, communicates it to Bob, and Bob measures his state $B$ using the POVM $E^j = \{E_0^j, E_1^j\}$ specified by Alice. Alice wins the game if Bob's measurement outcome is 1. In the adaptive version of the game, Alice can choose the index $j$ by performing a measurement on $A$; in the non-adaptive version, she has to decide upon $j$ without resorting to $A$. As we will see, this game covers a large class of quantum cryptographic schemes, where Bob's binary measurement outcome specifies whether Alice succeeded in breaking the scheme.

Our main result shows that in any such game it holds that $P_{\text{succ}}^{\text{A}} \leq 2^n P_{\text{succ}}^{\text{NA}}$ where $n = \text{H}_0(A)$, i.e., the number of qubits of $A$. Actually, as already mentioned, we show a more general and stronger bound $P_{\text{succ}}^{\text{A}} \leq 2^{I_{\max}^{\text{acc}}(B;A)} P_{\text{succ}}^{\text{NA}}$ that also

applies if we have no bound on the number of qubits of $A$, but we have some control over its "information content" $I_{\max}^{\mathrm{acc}}(B;A)$, which is a new information measure that we introduce and show to be upper bounded by $\mathrm{H}_0(A)$.

To give a first indication of the usefulness of our result, we observe that it easily provides a lower-bound on the quantity, *or quality*, of entanglement (as measured by $I_{\max}^{\mathrm{acc}}(B;A)$) that a dishonest committer needs in order to carry out the standard attack [18] on a quantum bit commitment scheme. Let Alice be the committer and Bob the receiver in a bit commitment scheme in which the opening phase consists of Alice announcing a classical string $j$ and Bob applying a verification described by POVM $\{E_{\mathrm{accept}}^j, E_{\mathrm{reject}}^j\}$. In the standard attack, Alice always commits to 0 while purifying her actions and applies an operation on her register if she wants to change her commitment to 1. If we let $\rho_{AB}$ be the state of Bob's register $B$ that corresponds to a commitment to 0, then the probability that a memoryless Alice successfully changes her commitment to 1 is $P_{\mathrm{succ}}^{\mathrm{NA}} = \max_j \mathrm{tr}(E_{\mathrm{accept}}^j \rho_{AB})$ where the maximum is over all $j$ that open 1. If Alice holds a register $A$ entangled with $B$, our main result implies that $I_{\max}^{\mathrm{acc}}(B;A)$ must be proportional to $-\log P_{\mathrm{succ}}^{\mathrm{NA}}$ for Alice to have a constant probability of changing her commitment.

But the real potential lies in the observation that adaptivity is notoriously difficult to handle in the analysis of cryptographic protocols, and as such our result provides a very powerful tool: as long as we have enough control over the side information, it is sufficient to restrict ourselves to non-adaptive attacks.

**Applications.** We demonstrate the usefulness of this methodology by proving the security of two commitment schemes. In both examples, the fact that the adversary holds quantum side information obstructs a direct analysis of the scheme, and we circumvent it by analyzing a non-adaptive version and applying our general result.

*One-Bit Cut-and-Choose is Universal for Two-Party Computation.* As a first example, we propose and prove secure a quantum bit commitment scheme that uses an ideal *1-bit cut-and-choose* primitive $\mathsf{1CC}$ (see Fig. 1 in Sect. 4) as a black box. Since bit commitment ($\mathsf{BC}$) implies oblivious transfer ($\mathsf{OT}$) in the quantum setting [2,7,20], and oblivious transfer is universal for two-party computation, this implies the universality of $\mathsf{1CC}$ and thus completes the zero/xor/one law proposed in [9]. Indeed, it was shown in [9] that in the information-theoretic quantum setting, every primitive is either trivial (zero), universal (one), or can be used to implement an XOR — *except* that there was one missing piece in their characterization: it excluded $\mathsf{1CC}$ (and any primitive that implies $\mathsf{1CC}$ but not $\mathsf{2CC}$). How $\mathsf{1CC}$ fits into the landscape was left as an open problem in [9]; we resolve it here.

*The BCJL Bit Commitment Scheme in (A Variant of) The Bounded Quantum Storage Model.* As a second application, we consider a general class of non-interactive commitment schemes and we show that for any such scheme, security

against an adversary with no quantum memory *at all* implies security in a slightly strengthened version of the standard bounded quantum storage model[1], with a corresponding loss in the error parameter.[2]

As a concrete example scheme, we consider the classic BCJL scheme that was proposed in 1993 by Brassard *et al.* [6] as a candidate for an unconditionally-secure scheme — back when this was thought to be possible — but until now has resisted any rigorous *positive* security analysis. Our methodology of relating adaptive to non-adaptive security allows us to prove it secure in (a variant of) the bounded quantum storage model.

## 2 Preliminaries

### 2.1 Basic Notation

For any string $x = (x_1, \ldots, x_n) \in \{0,1\}^n$ and any subset $t = \{t_1, \ldots t_k\} \subseteq [n]$, we write $x_t$ for the substring $x_t = (x_{t_1}, \ldots, x_{t_k}) \in \{0,1\}^{|t|}$. The $n$-bit all-zero string is denoted as $0^n$. The Hamming distance between two strings $x, y \in \{0,1\}^n$ is defined as $d(x,y) = \sum_{i=1}^{n} x_i \oplus y_i$. For $\delta > 0$ and $x \in \{0,1\}^n$, $B^\delta(x)$ denotes the set of all $n$ bit strings at Hamming distance at most $\delta n$ from $x$. We denote by $\lg(\cdot)$ the logarithm with respect to base 2. It is well known that the set $B^\delta(x)$ contains at most $2^{nh(\delta)}$ strings where $h(\delta) = -\delta \lg(\delta) - (1-\delta)\lg(1-\delta)$ is the binary entropy function.

Ideal cryptographic *functionalities* (or *primitives*) are referenced by their name written in sans-serif font. They are fully described by their input/output behaviour (see, e.g., functionality $\mathsf{1CC}$ described in Fig. 1 in Sect. 4). Cryptographic *protocols* have their names written in small capitals with a primitive name in superscript if the protocol has black-box access to this primitive (e.g. protocol $\textsc{bc}^{\mathsf{1CC}}$ in Sect. 4).

### 2.2 Quantum States and More

We assume familiarity with the basic concepts of quantum information; we merely fix notation and terminology here. We label quantum registers by capital letters $A, B$ etc. and their corresponding Hilbert spaces are respectively denoted by $\mathcal{H}_A, \mathcal{H}_B$ etc. We say that a quantum register $A$ is "empty" if $\dim(\mathcal{H}_A) = 1$. The state of a quantum register is specified by a density operator $\rho$, a positive semidefinite trace-1 operator. We typically write $\rho_A$ for the state of $A$, etc. The set of density operators for register $A$ is denoted $\mathcal{D}(\mathcal{H}_A)$. We write $X \geq 0$ to express that the operator $X$ is positive semidefinite, and $Y \geq X$ to express that $Y - X$ is positive semidefinite.

[1] Beyond bounding the adversary's quantum memory, we also restrict its measurements to be projective; this can be justified by the fact that to actually implejections onto thement a non-projective measurement, additional quantum memory is needed.

[2] We have already shown above how to argue for the standard attack [18] against quantum bit commitment schemes; taking care of *arbitrary* attacks is more involved.

We measure the distance between two states $\rho$ and $\sigma$ in terms of their *trace distance* $D(\rho,\sigma) := \frac{1}{2}\|\rho-\sigma\|_1$, where $\|X\|_1 := \mathrm{tr}(\sqrt{X^\dagger X})$ is the *trace norm*. We say that $\rho$ and $\sigma$ are $\epsilon$-close if $D(\rho,\sigma) \leq \epsilon$, and we call them *indistinguishable* if their trace distance is negligible (in the security parameter).

The *computational* (or rectilinear) basis for a single qubit quantum register is denoted by $\{|0\rangle_+, |1\rangle_+\}$, and the *diagonal* basis by $\{|0\rangle_\times, |1\rangle_\times\}$. Recall that $|0\rangle_\times = \frac{1}{\sqrt{2}}(|0\rangle_+ + |1\rangle_+)$ and $|1\rangle_\times = \frac{1}{\sqrt{2}}(|0\rangle_+ - |1\rangle_+)$. For any $x \in \{0,1\}^n$ and $\theta \in \{+,\times\}^n$, we set $|x\rangle_\theta := \bigotimes_{i=1}^n |x_i\rangle_{\theta_i}$. In the following, we will view and represent any sequence of diagonal and computational bases by a bit string $\theta \in \{0,1\}^n$, where $\theta_i = 0$ represents the computational basis and $\theta_i = 1$ the diagonal basis. In other words, for $b \in \{0,1\}$, $|b\rangle_0 := |b\rangle_+$ and $|b\rangle_1 := |b\rangle_\times$. And for $\theta, x \in \{0,1\}^n$, we define $|x\rangle_\theta := \bigotimes_{i=1}^n |x_i\rangle_{\theta_i}$.

Operations on quantum registers are modeled as completely-positive trace-preserving (CPTP) maps. To indicate that a CPTP map $\mathcal{E}$ takes inputs in $A$ and outputs to $B$, we use subscript $A \to B$. If $\mathcal{E}_{A\to B}$ is a CPTP map acting on register $A$, we slightly abuse notation and write $\mathcal{E}(\rho_{AC})$ instead of $\mathcal{E} \otimes \mathbb{I}_C(\rho_{AC})$ where $\mathbb{I}_C$ is the CPTP map that leaves register $C$ unchanged. A *measurement* on a quantum register $A$, producing a measurement outcome $X$, is a CPTP map $\mathcal{E}_{A\to X}$ of the form

$$\mathcal{E}(\rho_A) = \sum_{x\in\mathcal{X}} \mathrm{tr}(E_x\rho_A)|x\rangle\langle x|_X,$$

where $\{|x\rangle\}$ a basis of $\mathcal{H}_X$ and $E = \{E_x\}_{x\in\mathcal{X}}$ is a POVM, i.e., a collection of positive semidefinite operators satisfying $\sum_{x\in\mathcal{X}} E_x = \mathbb{I}$.

The *spectral norm* of an operator $X$ is defined as $\|X\| := \max_{|u\rangle} \|X|u\rangle\|$, where the maximum is over all normalized vectors $|u\rangle$, and an operator is called an *orthogonal projector* if $X^\dagger = X$ and $X^2 = X$. The following was shown in [8].

**Lemma 1.** *For any two orthogonal projectors $X$ and $Y$: $\|X+Y\| \leq 1 + \|XY\|$.*

### 2.3 Entropy and Privacy Amplification

In the following, the two notions of entropy that we will be dealing with are the min-entropy and the zero-entropy of a quantum register. They are defined as follows:

**Definition 1.** *The* min-entropy *of a bipartite quantum state $\rho_{AB}$ relative to register $B$ is the largest number $\mathrm{H}_\infty(A|B)_\rho$ such that there exists a $\sigma_B \in \mathcal{D}(\mathcal{H}_B)$,*

$$2^{-\mathrm{H}_\infty(A|B)_\rho} \cdot \mathbb{I}_A \otimes \sigma_B \geq \rho_{AB}.$$

*The* zero-entropy *of a state $\rho_A$ is defined as*

$$\mathrm{H}_0(A)_\rho = \lg(\mathrm{rank}(\rho_A)).$$

*We write $\mathrm{H}_\infty(A|B)$ and $\mathrm{H}_0(A)$ when the state of the registers is clear from the context.*

The min-entropy has the following operational interpretation [13]. Let $\rho_{XB}$ be a so-called cq-state, i.e., of the from $\rho_{XB} = \sum_x P_X(x)|x\rangle\langle x|_X \otimes \rho_B^x$. Then $P_{\text{guess}}(X|B) = 2^{-\mathrm{H}_\infty(X|B)_\rho}$ where $P_{\text{guess}}(X|B)$ is the probability of guessing the value of the classical random variable $X$, maximized over all POVMs on $B$.

Let $\mathcal{G}_n$ be a family of hash functions $g : \{0,1\}^n \to \{0,1\}$ with a binary output. The family $\mathcal{G}_n$ is said to be *two-universal* if for any $x, y \in \{0,1\}^n$ with $x \neq y$ and $G \in_R \mathcal{G}_n$,

$$\Pr\left(G(x) = G(y)\right) \leq \frac{1}{2}.$$

Privacy amplification against quantum side information, in case of hash functions with a binary-output, can be stated as follows:

**Theorem 1 (Privacy Amplification [19]).** *Let $\mathcal{G}_n$ be a two-universal family of hash functions $g : \{0,1\}^n \to \{0,1\}$ with a binary output. Furthermore, let $\rho_{XE} = \sum_{x\in\{0,1\}^n} P_X(x)|x\rangle\langle x|_X \otimes \rho_E^x$ be an arbitrary cq-state, and let*

$$\rho_{YGXE} := \frac{1}{|\mathcal{G}_n|} \sum_{g\in\mathcal{G}_n} \sum_{x\in\{0,1\}^n} P_X(x)|g(x)\rangle\langle g(x)|_Y \otimes |g\rangle\langle g|_G \otimes |x\rangle\langle x|_X \otimes \rho_E^x$$

*be the state obtained by choosing a random $g$ in $\mathcal{G}_n$, applying $g$ to the value stored in $X$, and storing the result in register $Y$. Then,*

$$D\left(\rho_{YGE}, \frac{\mathbb{I}_Y}{2} \otimes \rho_{GE}\right) \leq \frac{1}{2} \cdot 2^{-\frac{1}{2}(\mathrm{H}_\infty(X|E)-1)}.$$

## 3 Main Result

We consider an abstract game between two parties Alice and Bob. The game is specified by a joint state $\rho_{AB}$, shared between Alice and Bob who hold respective registers $A$ and $B$, and by a non-empty finite family $\mathbf{E} = \{E^j\}_{j\in\mathcal{J}}$ of binary-outcome POVMs $E^j = \{E_0^j, E_1^j\}$ acting on $B$. An execution of the game works as follows: Alice announces an index $j \in \mathcal{J}$ to Bob, and Bob measures register $B$ of the state $\rho_{AB}$ using the POVM $E^j$ specified by Alice's choice of $j$. Alice *wins* the game if the measurement outcome is 1. We distinguish between an *adaptive* and a *non-adaptive* Alice. An *adaptive* Alice can obtain $j$ by performing a measurement on her register $A$ of $\rho_{AB}$; on the other hand, an *non-adaptive* Alice has to produce $j$ from scratch, i.e., without accessing $A$. This motivates the following formal definitions.

**Definition 2.** *Let $\rho_{AB}$ be a bipartite quantum state, and let $\mathbf{E} = \{E^j\}_{j\in\mathcal{J}}$ be a non-empty finite family of binary-outcome POVMs $E^j = \{E_0^j, E_1^j\}$ acting on $B$. Then, we define*

$$P_{\text{succ}}(\rho_{AB}, \mathbf{E}) := \max_{\{F_j\}_j} \sum_{j\in\mathcal{J}} \mathrm{tr}\Big(\big(F_j \otimes E_1^j\big)\rho_{AB}\Big),$$

*where the maximum is over all POVMs* $\{F_j\}_{j\in\mathcal{J}}$ *acting on* $A$*. We call* $P_{\mathrm{succ}}(\rho_{AB},\mathbf{E})$ *the* adaptive success probability*, and we call* $P_{\mathrm{succ}}(\rho_B,\mathbf{E})$ *the* non-adaptive success probability*, where the latter is naturally understood by considering an "empty"* $A$*, and it equals*

$$P_{\mathrm{succ}}(\rho_B,\mathbf{E}) = \max_{j\in\mathcal{J}} \mathrm{tr}\big(E_1^j\rho_B\big).$$

*If* $\rho_{AB}$ *and* $\mathbf{E}$ *are clear from the context, we write* $P_{\mathrm{succ}}^{\mathrm{A}}$ *and* $P_{\mathrm{succ}}^{\mathrm{NA}}$ *instead of* $P_{\mathrm{succ}}(\rho_{AB},\mathbf{E})$ *and* $P_{\mathrm{succ}}(\rho_B,\mathbf{E})$*.*

As a matter of fact, for the sake of generality, we consider a setting with an additional quantum register $A'$ to which both the adaptive and the non-adaptive Alice have access to, but, as above only the adaptive Alice has access to $A$. In that sense, we will compare an adaptive with a *semi-adaptive* Alice. Formally, we will consider a tripartite state $\rho_{AA'B}$ and relate $P_{\mathrm{succ}}(\rho_{AA'B},\mathbf{E})$ to $P_{\mathrm{succ}}(\rho_{A'B},\mathbf{E})$. Obviously, the special case of an "empty" $A'$ will then provide a relation between $P_{\mathrm{succ}}^{\mathrm{A}}$ and $P_{\mathrm{succ}}^{\mathrm{NA}}$.

We now introduce a new measure of (quantum) information $I_{\max}^{\mathrm{acc}}(B;A|A')_\rho$, which will relate the adaptive to the non- or semi-adaptive success probability in our main theorem. In its unconditional form $I_{\max}^{\mathrm{acc}}(B;A)_\rho$, it is the accessible version of the max-information $I_{\max}(B;A)_\rho$ introduced in [3]; this means that it is the amount of max-information that can be accessed via measurements on Alice's share.

**Definition 3.** *Let* $\rho_{AA'B}$ *be a tripartite quantum state. Then, we define* $I_{\max}^{\mathrm{acc}}(B;A|A')_\rho$ *as the smallest real number such that, for every measurement* $\mathcal{M}_{AA'\to X}$ *there exists a measurement* $\mathcal{N}_{A'\to X}$ *such that*

$$\mathcal{M}(\rho_{AA'B}) \le 2^{I_{\max}^{\mathrm{acc}}(B;A|A')_\rho}\mathcal{N}(\rho_{A'B}).$$

*The unconditional version* $I_{\max}^{\mathrm{acc}}(B;A)_\rho$ *is naturally defined by considering* $A'$ *to be "empty"; the above condition then coincides with*

$$\mathcal{M}(\rho_{AB}) \le 2^{I_{\max}^{\mathrm{acc}}(B;A)_\rho}\sigma_X\otimes\rho_B,$$

*for some normalized density matrix* $\sigma_X\in\mathcal{D}(\mathcal{H}_X)$*, which can be interpreted as the outcome of a measurement* $\mathcal{N}_{\mathbb{C}\to X}$ *on an "empty" register.*

We are now ready to state and prove our main result.

**Theorem 2.** *Let* $\rho_{AA'B}$ *be a tripartite quantum state, and let* $\mathbf{E}=\{E^j\}_{j\in\mathcal{J}}$ *be a non-empty finite family of binary-outcome POVMs* $E^j$ *acting on* $B$*. Then, we have that*

$$P_{\mathrm{succ}}(\rho_{AA'B},\mathbf{E}) \le 2^{I_{\max}^{\mathrm{acc}}(B;A|A')_\rho}P_{\mathrm{succ}}(\rho_{A'B},\mathbf{E}).$$

By considering an "empty" $A'$, we immediately obtain the following.

**Corollary 1.** *Let* $\rho_{AB}$ *be a bipartite quantum state, and let* $\mathbf{E}=\{E^j\}_{j\in\mathcal{J}}$ *be as above. Then,*

$$P_{\mathrm{succ}}^{\mathrm{A}} \le 2^{I_{\max}^{\mathrm{acc}}(B;A)_\rho}P_{\mathrm{succ}}^{\mathrm{NA}}.$$

*Proof (of* Theorem 2*).* Let $\{F_j\}_{j\in\mathcal{J}}$ be an arbitrary POVM acting on $AA'$, and let $\mathcal{M}_{AA'\to J}$ be the corresponding measurement $\mathcal{M}(\sigma_{AA'}) = \sum_j \mathrm{tr}(F_j\sigma)|j\rangle\langle j|$. We define the map

$$\mathcal{E}_{JB\to\mathbb{C}}(\sigma_{JB}) := \sum_j \mathrm{tr}((|j\rangle\langle j| \otimes E_1^j)\sigma_{JB}),$$

which is completely positive (but not trace-preserving in general). From the definition of $I_{\max}^{\mathrm{acc}}$, we know that there exists a measurement $\mathcal{N}_{A'\to J}$, i.e., a CPTP map of the form $\mathcal{N}(\sigma_{A'}) = \sum_j \mathrm{tr}(F'_j\sigma)|j\rangle\langle j|$ for a POVM $\{F'_j\}_{j\in\mathcal{J}}$ acting on $A'$, such that

$$\mathcal{M}(\rho_{AA'B}) \leq 2^{I_{\max}^{\mathrm{acc}}(B;A|A')_\rho}\mathcal{N}(\rho_{A'B}).$$

Applying $\mathcal{E}$ on both sides gives

$$(\mathcal{E}\circ\mathcal{M})(\rho_{AA'B}) \leq 2^{I_{\max}^{\mathrm{acc}}(B;A|A')_\rho}(\mathcal{E}\circ\mathcal{N})(\rho_{A'B}),$$

and expanding both sides using the definitions of $\mathcal{E}$, $\mathcal{M}$ and $\mathcal{N}$ gives

$$\begin{aligned}\sum_j \mathrm{tr}((F_j\otimes E_1^j)\rho_{AA'B}) &\leq 2^{I_{\max}^{\mathrm{acc}}(B;A|A')_\rho}\sum_j \mathrm{tr}((F'_j\otimes E_1^j)\rho_{A'B})\\ &\leq 2^{I_{\max}^{\mathrm{acc}}(B;A|A')_\rho}P_{\mathrm{succ}}(\rho_{A'B},\mathbf{E}).\end{aligned}$$

This yields the theorem statement, since the left-hand side equals to $P_{\mathrm{succ}}(\rho_{AA'B},\mathbf{E})$ when maximized over the choice of the POVM $\{F_j\}_{j\in\mathcal{J}}$. □

By the following proposition, we see that Corollary 1 implies a direct generalization of the classical bound, which ensures that giving access to $n$ bits increases the success probability by at most $2^n$, to qubits.

**Proposition 1.** *For any $\rho_{AB}$, we have that $I_{\max}^{\mathrm{acc}}(B;A)_\rho \leq H_0(A)_\rho$.*

*Proof.* Let $|\psi\rangle_{ABR}$ be a purification of $\rho_{AB}$ and let $\mathcal{M}_{A\to X}$ be a measurement on $A$. Since $|\psi\rangle$ is also a purification of $\rho_A$, there exists a linear operator $V_{\bar{A}\to BR}$ from a register $\bar{A}$ of the same dimension as $A$ into $BR$ such that $|\psi\rangle_{ABR} = (\mathbb{I}_A\otimes V)|\Phi\rangle_{A\bar{A}}$, with $|\Phi\rangle = \sum_i |i\rangle_A\otimes|i\rangle_{\bar{A}}$. Now, first note that

$$2^{-H_0(A)}(\mathcal{M}\otimes\mathbb{I})(\Phi_{A\bar{A}}) = \sum_x \lambda_x|x\rangle\langle x|_X\otimes\omega_{\bar{A}}^x \leq \sum_x \lambda_x|x\rangle\langle x|_X\otimes\mathbb{I}_{\bar{A}},$$

where $\{\lambda_x\}$ is a probability distribution, and each $\omega_{\bar{A}}^x$ is normalized because $\mathrm{tr}(\Phi) = 2^{\mathrm{H}_0(A)}$. Multiplying both sides of the inequality by $2^{H_0(A)}$ and conjugating by $V$, we get

$$(\mathcal{M}\otimes\mathbb{I})(|\psi\rangle\langle\psi|) \leq 2^{H_0(A)}\sum_x \lambda_x|x\rangle\langle x|\otimes VV^\dagger.$$

Using the fact that $VV^\dagger = \psi_{BR} := \mathrm{tr}_A(|\psi\rangle\langle\psi|)$, this yields

$$(\mathcal{M}\otimes\mathbb{I})(|\psi\rangle\langle\psi|) \leq 2^{H_0(A)}\sum_x \lambda_x|x\rangle\langle x|\otimes\psi_{BR}.$$

Tracing out $R$ on both sides and defining $\sigma_X = \sum_x \lambda_x |x\rangle\langle x|$ then yields

$$(\mathcal{M} \otimes \mathbb{I})(\rho_{AB}) \leq 2^{H_0(A)} \sigma_X \otimes \rho_B,$$

which proves the claim. □

One might naively expect that also the conditional version $I^{\text{acc}}_{\max}(B; A|A')_\rho$ is upper bounded by $H_0(A)_\rho$, implying a corresponding statement for a *semi-adaptive* Alice: giving access to $n$ *additional* qubits increases the success probability by at most $2^n$. However, this is not true, as the following example illustrates. Let register $B$ contain two random classical bits, and let $A$ and $A'$ be two qubit registers, containing one of the four Bell states, and which one it is, is determined by the two classical bits. Alice's goal is to guess the two bits. Clearly, $A'$ alone is useless, and thus a semi-adaptive Alice having access to $A'$ has a guessing probability of at most $\frac{1}{4}$. On the other hand, adaptive Alice can guess them with certainty by doing a Bell measurement on $AA'$.

However, Proposition 1 does generalize to the conditional version in case of a *classical* $A'$.

**Proposition 2.** *For any state $\rho_{ZAB}$ with classical $Z$:*

$$I^{\text{acc}}_{\max}(B; A|Z)_\rho \leq \max_z I^{\text{acc}}_{\max}(B; A)_{\rho^z} \leq H_0(A)_\rho.$$

An additional property of $I^{\text{acc}}_{\max}$ is that quantum operations that are in tensor product form on registers $A$ and $B$ cannot increase the max-accessible-information.

**Proposition 3.** *Let $\mathcal{E}_{AB\to A'B'}$ be a CPTP map of the form $\mathcal{E} = \mathcal{E}^A \otimes \mathcal{E}^B$. Then*

$$I^{\text{acc}}_{\max}(B'; A')_{\mathcal{E}(\rho)} \leq I^{\text{acc}}_{\max}(B; A)_\rho.$$

The proofs the two previous results can be found in Appendix A.

## 4 Application 1: 1CC Is Universal

### 4.1 Background

It is a well-known fact that information-theoretically secure two-party computation is impossible without assumptions. As a result, one of the natural questions that arises is: what are the minimal assumptions required to achieve it? One way to attack this question is to try to identify the simplest cryptographic primitives which, when made available in a black-box way to the two parties, allow them to perform arbitrary two-party computations. We then say that such a primitive is "universal". Perhaps the best known such primitive is one-out-of-two oblivious transfer (OT), which has been shown to be universal by Kilian [10]. Since then, the power of various primitives for two-party computation has been studied in much more detail [11,12,14–17]. Recently, it has been shown in [16] that every non-trivial two-party primitive (i.e. any primitive that cannot be done

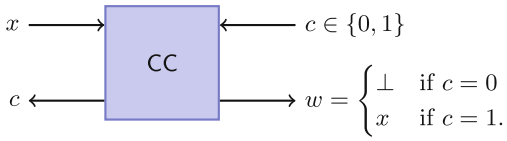


**Fig. 1.** The cut-and-choose functionality. The one-bit and two-bit versions of the functionality refer to the length of $x$. One player chooses $x$, and the other player chooses whether he wants to see $x$ or not. The first player then learns the choice that was made.

from scratch without assumptions) can be used as a black-box to implement one of four basic primitives: oblivious transfer (OT), bit commitment (BC), an XOR between Alice's and Bob's inputs, or a primitive called *cut-and-choose* (CC) as depicted in Fig. 1.

Interestingly, this picture becomes considerably simpler when we consider quantum protocols. First, BC can be used to implement OT [2,7,20] and is therefore universal. Furthermore, as was shown in [9], even a 2-bit cut-and-choose (2CC) is universal in the quantum setting, giving rise to what they call a zero/xor/one law: every primitive is either trivial (zero), universal (one), or can be used to implement an XOR. However, there was one missing piece in this characterization: it applies to all functionalities except those that are sufficient to implement 1-bit cut-and-choose (1CC), but not 2CC. In this section, we resolve this issue by showing that 1CC is universal. We do this by presenting a quantum protocol for bit commitment that uses 1CC as a black box, and we prove its security using our adaptive to non-adaptive reduction.

### 4.2 The Protocol

The protocol is given in Fig. 2, where Alice is the committer and Bob the receiver. The protocol is parameterized by $N \in \mathbb{N}$, which acts as security parameter, and by constants $q, \tau$ and $r$, where $q, \tau > 0$ are small and $r < 1$ is close to 1. Intuitively, our bit commitment protocol uses the 1CC primitive to ensure that the state Alice sends to Bob is close to what it is supposed to be: $|0^N\rangle_\theta$ for some randomly chosen but fixed basis $\theta$. Indeed, the 1CC primitive allows Bob to sample a small random subset of the qubits and check for correctness on that subset; if the state looks correct on this subset, we expect that it cannot be too far off on the unchecked part.

Note that our protocol uses the B92 [1] encoding $(\{|0\rangle_+, |0\rangle_\times\})$, rather than the more common BB84 encoding. This allows us to get away with a *one*-bit cut-and-choose functionality; with the BB84 encoding, Alice would have to "commit" to *two* bits: the basis and the measurement outcome.

We use the quantum sampling framework of Bouman and Fehr [4] to analyze the checking procedure of the protocol. Actually, we use the *adaptive* version of [9], which deals with an Alice that can decide on the next basis adaptively depending on what Bob has asked to see so far. On the other hand, to deal with Bob choosing his sample subset adaptively depending on what he has seen so

$\text{COMMIT}^{\mathsf{1CC}}_{N,q,\tau,r}(b)$:

1. Alice chooses random $\theta \in \{0,1\}^N$ and sends the $N$ qubit state $|0^N\rangle_\theta$ to Bob.
2. For $i = 1 \ldots N$, do
   (a) Alice and Bob invoke an instance of $\mathsf{1CC}$: Alice inputs the bit $\theta_i$, and Bob inputs bit 1 with probability $q$ and bit 0 with probability $1-q$.
   (b) If Bob's input was 1, he measures the $i$th qubit of the state he received in basis $\theta_i$ and checks that the result is 0. If it is not, he aborts.
   Let $t \subset [N]$ the set of positions that Bob checked, $\bar{t} = [N] \setminus t$, and $n = |\bar{t}|$.
3. Alice aborts the protocol if Bob checked more than $2qN$ positions.
4. Bob chooses a generator matrix $G$ of a $[n,k,d]$-code with rate $k/n \geq r$ and $d/n \geq \tau$, and he sends $G$ to Alice, who checks that indeed $k/n \geq r$.
5. Alice picks a random member $g \in \mathcal{G}_n$ from a family $\mathcal{G}_n$ of two-universal hash functions, and she computes the syndrome $s$ of $\theta_{\bar{t}}$ for the linear code. Then, she sends $g$, $s$ and $w = g(\theta_{\bar{t}}) \oplus b$ to Bob.

$\text{REVEAL}^{\mathsf{1CC}}$:

1. Alice sends $\theta_{\bar{t}}$ and $b$ to Bob.
2. Bob checks that he obtains 0 by measuring the $i$th qubit in basis $\theta_i$ for all $i \in \bar{t}$. He checks that $\theta_{\bar{t}}$ has syndrome $s$, and that $g(\theta_{\bar{t}}) \oplus w = b$. If one of the above checks failed, he aborts.
3. If Bob is honest, this eventuality only occurs with probability less than $2\exp(-2q^2N)$ according to Hoeffding's inequality.

**Fig. 2.** Bit commitment protocol $\text{BC}^{\mathsf{1CC}}$ based on the 1-bit cut-and-choose primitive.

far, we require the sample subset to be rather small, so that we can then apply union bound over all possible choices.

### 4.3 Security Proofs

We use the standard notion of hiding for a (quantum) bit commitment scheme.

**Definition 4 (Hiding).** *A bit-commitment scheme is* $\epsilon$-hiding *if, for any dishonest receiver Bob, his state* $\rho_0$ *corresponding to a commitment to* $b = 0$ *and his state* $\rho_1$ *corresponding to a commitment to* $b = 1$ *satisfy* $D(\rho_0, \rho_1) \leq \epsilon$.

Since the proof that our protocol is hiding uses a standard approach, we only briefly sketch it.

**Theorem 3.** *Protocol* $\text{COMMIT}^{\mathsf{1CC}}_{N,q,\tau,r}$ *is* $2^{-\frac{1}{2}N(\lg(1/\gamma)-2q-(1-r))}$*-hiding, where* $\gamma = \cos^2(\pi/8) \approx 0.85$ *(and hence* $\lg(1/\gamma) \approx 0.23$*).*

*Proof (sketch).* We need to argue that there is sufficient min-entropy in $\theta_{\bar{t}}$ for Bob; then, privacy amplification does the job. This means that we have to show that Bob has small success probability in guessing $\theta_{\bar{t}}$. What makes the argument

slightly non-trivial is that Bob can choose $t$ depending on the qubits $|0^N\rangle_\theta$. Note that since Alice aborts in case $|t| > 2qN$, we may assume that $|t| \leq 2qN$.

It is a straightforward calculation to show that Bob's success probability in guessing $\theta$ right after step 1 of the protocol, i.e., when given the qubits $|0^N\rangle_\theta$, is $\gamma^N$, where $\gamma = \cos^2(\pi/8) \approx 0.85$. From this it then follows that right after step 2, Bob's success probability in guessing $\theta_{\bar{t}}$ is at most $\gamma^N \cdot 2^{2qN}$: if it was larger, then he could guess $\theta$ right after step 1 with probability larger than $\gamma^N$ by simulating the sampling and guessing the $|t| \leq 2qN$ bits $\theta_i$ that Alice provides. It follows that right after step 2, Bob's min-entropy in $\theta_{\bar{t}}$ is $N(\lg(1/\gamma) - 2q)$. Finally, by the chain rule for min-entropy, Bob's min-entropy in $\theta_{\bar{t}}$ when additionally given the syndrome $s$ is $N\big(\lg(1/\gamma) - 2q\big) - (n-k) = N\big(\lg(1/\gamma) - 2q\big) - n(1-k/n) \geq N\big(\lg(1/\gamma) - 2q - (1-r)\big)$. The statement then directly follows from privacy amplification (Theorem 1) and the triangle inequality. □

As for the binding property of our commitment scheme, as we will show, we achieve a strong notion of security that not only guarantees the existence of a bit to which Alice is bound in that she cannot reveal the other bit, but this bit is actually *universally extractable* from the classical information held by Bob together with the inputs to the 1CC:

**Definition 5 (Universally Extractable).** *A bit-commitment scheme (in the* 1CC*-hybrid model) is* $\epsilon$-universally extractable *if there exists a function* $c$ *that acts on the classical information* $view_{Bob,1\mathsf{CC}}$ *held by Bob and* 1CC *after the commit phase, so that for any pure commit and open strategy for dishonest Alice, she has probability at most* $\epsilon$ *of successfully unveiling the bit* $1 - c(view_{Bob,1\mathsf{CC}})$.

Our strategy for proving the binding property for our protocol is as follows. First, we show that due to the checking part, the (joint) state after the commit phase is of a restricted form. Then, we show that, based on this restriction on the (joint) state, a *non-adaptive* Alice who has no access to her quantum state, cannot open to the "wrong" bit. And finally, we apply our main result to conclude security against a general (adaptive) Alice.

The following lemma follows immediately from (the adaptive version of) Bouman and Fehr's quantum sampling framework [4,9]. Informally, it states that if Bob did not abort during sampling, then the post-sampling state of Bob's register is close to the correct state, up to a few errors. In other words, after the commit phase, Bob's state is a superposition of strings close to $0^n$ in the basis specified by $\theta_{\bar{t}}$.

**Lemma 2.** *Consider an arbitrary pure strategy for Alice in protocol* $\text{COMMIT}^{1\mathsf{CC}}_{N,q,\tau,r}$. *Let* $\rho_{AB}$ *be the joint quantum state at the end of the commit phase, conditioned (and thus dependent) on* $t, \theta, g, w$ *and* $s$. *Then, for any* $\delta > 0$, *on average over the choices of* $t, \theta, g, w$ *and* $s$, *the state* $\rho_{AB}$ *is* $\epsilon$*-close to an "ideal state"* $\tilde{\rho}_{AB}$ *(which is also dependent on* $t, \theta$ *etc.) with the property that the conditional state of* $\tilde{\rho}_{AB}$ *conditioned on Bob not aborting is pure and of the form*

$$|\phi_{AB}\rangle = \sum_{y \in B^{\delta}(0^n)} \alpha_y |\xi^y\rangle_A |y\rangle_{\theta_{\bar{t}}} \tag{1}$$

*where* $|\xi^y\rangle$ *are arbitrary states on Alice's register and* $\epsilon \leq \sqrt{4\exp(-q^2\delta^2 N/8)}$.

The following lemma implies that after the commit phase, if Alice and Bob share a state of the form of (1), then a non-adaptive Alice is bound to a fixed bit which is defined by some string $\theta'$.

**Lemma 3.** *For any* $t, \theta$ *and* $s$ *there exists* $\theta'$ *with syndrome* $s$ *such that for every* $\theta'' \neq \theta'$ *with syndrome* $s$*, and for every state* $|\phi_{AB}\rangle$ *of the form of* (1)*,*

$$\mathrm{tr}\big((\mathbb{I} \otimes |0\rangle\langle 0|_{\theta''})\phi_{AB}\big) \leq 2^{-\frac{d}{2}+nh(\delta)}.$$

*Proof.* Let $\theta' \in \{0,1\}^n$ be the string with syndrome $s$ closest to $\theta_{\bar{t}}$ (in Hamming distance). Then, since the set of strings with a fixed syndrome form an error correcting code of distance $d$, every other $\theta'' \in \{0,1\}^n$ of syndrome $s$ is at distance at least $d/2$ from $\theta_{\bar{t}}$. Bob's reduced density operator of state (1) is $\phi_B = \sum_{y,y' \in B^{\delta}(0^n)} \alpha_y \alpha^*_{y'} \langle \xi_{y'} | \xi_y \rangle |y\rangle\langle y'|_{\theta_{\bar{t}}}$. Using the fact that $d(\theta_{\bar{t}}, \theta'') \geq d/2$ for every $\theta'' \neq \theta'$ (and hence $|\,\mathrm{tr}(|0\rangle\langle 0|_{\theta''} |y\rangle\langle y'|_{\theta_{\bar{t}}})| \leq 2^{-\frac{d}{2}}$) and the triangle inequality, we get:

$$\begin{aligned}
\mathrm{tr}(|0\rangle\langle 0|_{\theta''}\phi_B) &\leq 2^{-\frac{d}{2}} \sum_{y,y' \in B^{\delta}(0^n)} \left|\alpha_y \alpha^*_{y'} \langle \xi_{y'} | \xi_y \rangle\right| \\
&\leq 2^{-\frac{d}{2}} \sum_{y,y' \in B^{\delta}(0^n)} |\alpha_y||\alpha^*_{y'}| \\
&= 2^{-\frac{d}{2}} \left( \sum_y |\alpha_y| \right)^2 \\
&\leq 2^{-\frac{d}{2}+nh(\delta)},
\end{aligned}$$

where the last inequality is argued by viewing $\sum_y |\alpha_y|$ as inner product of the vectors $\sum_y |\alpha_y||y\rangle$ and $\sum_y |y\rangle$, and applying the Cauchy-Schwarz inequality. □

We are now ready to prove that the scheme is universally extractable:

**Theorem 4.** *For any* $\delta > 0$, $\textsc{commit}^{\mathsf{1CC}}_{N,q,\tau,r}$ *is* $\epsilon$*-universally extractable with*

$$\epsilon \leq 2^{-N(1-2q)(\tau/2-2h(\delta))} + \sqrt{4\exp(-q^2\delta^2 N/8)}.$$

*Proof.* We need to show the existence of a binary-valued function $c(\theta, t, g, w, s)$ as required by Definition 5, i.e., such that for any commit strategy, there is no opening strategy that allows Alice to unveil $\bar{c}$, except with small probability. We define this function as $c(t, \theta, g, s, w) := g(\theta') \oplus w$ where $\theta'$ is as in Lemma 3, depending on $t, \theta$ and $s$ only.

Now, consider an arbitrary pure strategy for Alice in protocol $\textsc{commit}^{\mathsf{1CC}}$. Let $\theta, g, w$ and $s$ be the values chosen by Alice during the commit phase and let

$\rho_{AB}$ be the joint state of Alice and Bob after the commit phase. Fix $\delta > 0$ and consider the states $\tilde{\rho}_{AB}$ and $|\phi_{AB}\rangle$ as promised by Lemma 2. Recall that $\rho_{AB}$ is $\epsilon$-close to $\tilde{\rho}_{AB}$ (on average over $\theta, g, w$ and $s$, and for $\epsilon \leq \sqrt{4\exp(-q^2\delta^2 N/8)}$), and $\tilde{\rho}_{AB}$ is a mixture of Bob aborting in the commit phase and of $|\phi_{AB}\rangle$; therefore, we may assume that Alice and Bob share the pure state $\phi_{AB} = |\phi_{AB}\rangle\langle\phi_{AB}|$ instead of $\rho_{AB}$ by taking into account the probability at most $\epsilon$ that the two states behave differently.

Let $\mathcal{B}$ be the set of strings $\theta''$ with syndrome $s$ such that $g(\theta'') \oplus w = \bar{c}$ and let $\mathbf{E} = \{\{E_0^{\theta''}, E_1^{\theta''}\}\}_{\theta'' \in \mathcal{B}}$ be the family of POVMs that correspond to Bob's verification measurement when Alice announces $\theta''$, i.e. where $E_1^{\theta''} = |0\rangle\langle 0|_{\theta''}$ and $E_0^{\theta''} = \mathbb{I} - |0\rangle\langle 0|_{\theta''}$. Then, Alice's probability of successfully unveiling bit $\bar{c}$ equals $P_{\text{succ}}(\phi_{AB}, \mathbf{E})$ as defined in Sect. 3. In order to apply Corollary 1, we must first control the size of the side-information that Alice holds. By looking at the definition of $|\phi_{AB}\rangle$ in (1), we notice that it is a superposition of at most $|B^\delta(0^n)| \leq 2^{nh(\delta)}$ terms. Therefore, the rank of $\phi_A$ is at most $2^{nh(\delta)}$ and $\mathrm{H}_0(A) \leq nh(\delta)$. We can now bound Alice's probability of opening $\bar{c}$:

$$P_{\text{succ}}(\phi_{AB}, \mathbf{E}) \leq 2^{\mathrm{H}_0(A)} P_{\text{succ}}(\phi_B, \mathbf{E}) \leq 2^{-\frac{d}{2}+2nh(\delta)} \leq 2^{-n(\tau/2-2h(\delta))}$$

where the first inequality follows from Corollary 1 and Proposition 1, and the second from the bound on $\mathrm{H}_0(A)$ and from Lemma 3. □

Regarding the choice of parameters $q, \tau$ and $r$, and the choice of the code, we note that the Gilbert-Varshamov bound guarantees that the code defined by a random binary $n \times (n - rn)$ generator matrix $G$ has minimal distance $d \geq \tau n$, except with negligible probability, as long as $r < 1 - h(\tau)$. On the other hand, for the hiding property, we need that $r > 1 - 0.23 + 2q$. As such, as long as $h(\tau) < 0.23 - 2q$, there exists a suitable rate $r$ and a suitable generator matrix $G$, so that our scheme offers statistical security against both parties.

### 4.4 Universality of 1CC

By using our 1CC-based bit commitment scheme $\text{BC}^{\mathsf{1CC}}$ in the standard construction for obtaining OT from BC in the quantum setting [2,7], we can conclude that 1CC implies OT in the quantum setting, and since OT is universal we thus immediately obtain the universality of 1CC. However, strictly speaking, this does not solve the open problem of [9] yet. The caveat is that [9] asks about the universality of 1CC in the *UC security model* [20], in other words, whether 1CC is "universally-composable universal". So, to truly solve the open problem of [9] we still need to argue *UC security* of the resulting OT scheme, for instance by arguing that our scheme $\text{BC}^{\mathsf{1CC}}$ is UC secure.

UC-security of $\text{BC}^{\mathsf{1CC}}$ against malicious Alice follows immediately from our binding criterion (Definition 5); after the commit phase, Alice is bound to a bit that can be extracted in a black-box way from the classical information held by Bob and the 1CC functionality. Thus, a simulator can extract that bit from

malicious Alice and input it into the ideal commitment functionality, and since Alice is bound to this bit, this ideal-world attack is indistinguishable from the real-world attack.

However, it is not clear if $\text{BC}^{\mathsf{1CC}}$ is UC-secure against malicious Bob. The problem is that it is unclear whether it is *universally equivocable*, which is a stronger notion than the standard hiding property (Definition 4).

Nevertheless, we *can* still obtain a UC-secure $\mathsf{OT}$ scheme in the $\mathsf{1CC}$-hybrid model, and so solve the open problem of [9]. For that, we slightly modify the standard $\mathsf{BC}$-based $\mathsf{OT}$ scheme [2,7] with $\mathsf{BC}$ instantiated by $\text{BC}^{\mathsf{1CC}}$ as follows: for every BB84 qubit that the receiver is meant to measure, he commits to the basis using $\text{BC}^{\mathsf{1CC}}$, but he uses the $\mathsf{1CC}$-functionality *directly* to "commit" to the measurement outcome, i.e., he inputs the measurement outcome into $\mathsf{1CC}$ — and if the sender asks $\mathsf{1CC}$ to reveal it, the receiver also unveils the accompanying basis by opening the corresponding commitment.

Definition 5 ensures universal extractability of the committed bases and thus of the receiver's input. This implies UC-security against dishonest receiver. In order to argue UC-security against dishonest sender, we consider a simulator that acts like the honest receiver, i.e., chooses random bases and commits to them, but only measures those positions that the sender wants to see — because the simulator controls the $\mathsf{1CC}$-functionality he can do that. Then, once he has learned the sender's choices for the bases, he can measure all (remaining) qubits in the correct basis, and thus reconstruct *both* messages and send them to the ideal $\mathsf{OT}$ functionality. The full details of the proof are in Appendix B.

## 5 Application 2: On the Security of BCJL Commitment Scheme

In this section, we show that for a wide class of bit-commitment schemes, the binding property of the scheme in (a slightly strengthened version of) the *bounded-quantum-storage model* reduces to its binding property against a dishonest committer that has *no quantum memory at all*. We then demonstrate the usefulness of this on the example of the BCJL commitment scheme [6].

### 5.1 Setting up the Stage

The class of schemes to which our reduction applies consists of the schemes that are non-interactive: all communication goes from Alice, the committer, to Bob, the verifier. Furthermore, we require that Bob's verification be "projective" in the following sense.

**Definition 6.** *We say that a bit-commitment scheme is* non-interactive and with projective verification*, if it is of the following form.*

Commit: *Alice sends a classical message $x$ and a quantum register $B$ to Bob.*
Opening to $b$: *Alice sends a classical opening $y_b$ to Bob, and Bob applies a binary-outcome projective measurement $\{\mathbb{V}_{x,y_b}, \mathbb{I} - \mathbb{V}_{x,y_b}\}$ to register $B$.*

Since $x$ is fixed after the commit phase, we tend to leave the dependency of $\mathbb{V}_{x,y_b}$ from $x$ implicit and write $\mathbb{V}_{y_b}$ instead. Also, to keep language simple, we will just speak of a *non-interactive* bit-commitment scheme and drop the *projective verification* part in the terminology.

We consider the security — more precisely: the binding property — of such bit-commitment schemes in a slightly strengthened version of the bounded-quantum-storage model [8], where we bound the quantum memory of Alice, but we also restrict her measurement (for producing $y_b$ in the opening phase) to be *projective*. This restriction on Alice's measurement is well justified since a general non-projective measurement requires additional quantum storage in the form of an ancilla to be performed coherently. From a technical perspective, this restriction (as well as the restriction on Bob's verification) is a byproduct of our proof technique, which requires the measurement operator describing the (joint) opening procedure to be repeatable; avoiding it is an open question.[3]

Formally, we capture the binding property as follows in this variation of the bounded-quantum-storage model.

**Definition 7 (Binding).** *A non-interactive bit commitment scheme is called* $\epsilon$-binding against $q$-quantum-memory-bounded *(or* $q$-QMB *for short)* projective adversaries *if, for all states* $\rho_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ *with* $\dim(\mathcal{H}_A) \leq 2^q$ *and for all classical messages* $x$*,*

$$P_0^A(\rho_{AB}) + P_1^A(\rho_{AB}) \leq 1 + \epsilon$$

*where*

$$P_b^A(\rho_{AB}) := \max_{\{\mathbb{F}_{y_b}\}_{y_b}} \sum_{y_b} \mathrm{tr}((\mathbb{F}_{y_b} \otimes \mathbb{V}_{x,y_b})\rho_{AB})$$

*is the probability of successfully opening bit* $b$*, maximized over all* projective *measurements* $\{\mathbb{F}_{y_b}\}_{y_b}$*.*

In case $q = 0$, where the above requirement reduces to

$$P_0^{NA}(\rho_{AB}) + P_1^{NA}(\rho_{AB}) \leq 1 + \epsilon \quad \text{with} \quad P_b^{NA}(\rho_{AB}) := \max_{y_b} \mathrm{tr}(\mathbb{V}_{x,y_b}\rho_B)$$

and $\rho_B = \mathrm{tr}_A(\rho_{AB})$, we also speak of $\epsilon$-binding against *non-adaptive* adversaries.

**On the Binding Criterion for Non-interactive Commitment Schemes.** Binding criteria analogous to the one specified in Definition 7 have traditionally been weak notions of security against dishonest committers for quantum commitment schemes, as opposed to criteria that are more in the spirit of a bit that cannot be opened by the adversary. While more convenient for proving security of commitment schemes, a notable flaw of the $p_0 + p_1 \leq 1 + \epsilon$ definition is that it does not rule out the following situation. An adversary might, by some complex measurement, either completely ruin its capacity to open the commitment, or be

[3] The standard technique (using Naimark's dilation theorem) does not work here.

able to open the bit of its choice. Then the total probability of opening 0 and 1 sum to 1, but, conditioned on the second outcome of this measurement, they sum to 2. This is obviously an undesirable property of a quantum bit-commitment scheme.

Non-interactive schemes that are secure according to Definition 7 are binding in a stronger sense. For instance, the above problem of the $p_0 + p_1 \leq 1 + \epsilon$ definition does not hold for non-interactive schemes. If a scheme is $\epsilon$-binding, then any state $\rho$ obtained by conditioning on some measurement outcome must satisfy $P_0^A(\rho) + P_1^A(\rho) \leq 1 + \epsilon$. If the total probability of opening 0 and 1 was any higher, then the adversary could have prepared the state $\rho$ in the first place, contradicting the fact that the protocol is $\epsilon$-binding. It remains an open question how to accurately describe the security of non-interactive commitment schemes that satisfy Definition 7.

### 5.2 The General Reduction

We want to reduce security against a $q$-QMB projective adversary to the security against a non-adaptive adversary (which should be much easier to show) by means of applying our general adaptive-to-non-adaptive reduction. However, Corollary 1 does not apply directly; we need some additional gadget, which is in the form of the following lemma. It establishes that if there is a commit strategy for Alice so that the cumulative probability of opening 0 and 1 exceeds 1 by a non-negligible amount, then there is also a commit strategy for her so that she can open 0 *with certainty* and 1 with still a non-negligible probability.

**Lemma 4.** *Let $\rho \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and $\epsilon > 0$ be such that $P_0^A(\rho) + P_1^A(\rho) \geq 1 + \epsilon$. Then, there exists $\rho^0 \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ such that $P_0^A(\rho^0) = 1$ and $P_1^A(\rho^0) \geq \epsilon^2$.*

*Proof.* Let $\{\mathbb{F}_{y_0}\}_{y_0}$ and $\{\mathbb{G}_{y_1}\}_{y_1}$ be the projective measurements maximizing $P_0^A(\rho)$ and $P_1^A(\rho)$, respectively. Define the projections onto the 0/1-accepting subspaces as

$$\mathbb{P}_0 := \sum_{y_0} \mathbb{F}_{y_0} \otimes \mathbb{V}_{y_0} \text{ and } \mathbb{P}_1 := \sum_{y_1} \mathbb{G}_{y_1} \otimes \mathbb{V}_{y_1}.$$

Since $\mathrm{tr}((\mathbb{P}_0 + \mathbb{P}_1)\rho) = P_0^A(\rho) + P_1^A(\rho) \geq 1 + \epsilon$, it follows that $\|\mathbb{P}_0 + \mathbb{P}_1\| \geq 1 + \epsilon$. From Lemma 1, we have that

$$1 + \|\mathbb{P}_1\mathbb{P}_0\| \geq \|\mathbb{P}_0 + \mathbb{P}_1\| \geq 1 + \epsilon.$$

Therefore there exists $|\phi\rangle$ such that $\|\mathbb{P}_1\mathbb{P}_0|\phi\rangle\| \geq \epsilon$. Define $|\phi_0\rangle := \mathbb{P}_0|\phi\rangle / \|\mathbb{P}_0|\phi\rangle\|$, which we claim has the required properties. The probability to open 0 from $|\phi_0\rangle$ is $\|\mathbb{P}_0|\phi_0\rangle\|^2 = 1$, and the probability to open 1 from $|\phi_0\rangle$ is $\|\mathbb{P}_1\mathbb{P}_0|\phi_0\rangle\|^2 = \|\mathbb{P}_1\mathbb{P}_0|\phi\rangle\|^2 / \|\mathbb{P}_0|\phi\rangle\|^2 \geq \epsilon^2$. □

Now, we are ready to state and prove the general reduction.

**Theorem 5.** *If a non-interactive bit-commitment scheme is $\epsilon$-binding against non-adaptive adversaries, then it is $(2^{\frac{1}{2}q}\sqrt{\epsilon})$-binding against $q$-QMB projective adversaries.*

*Proof.* Let $\rho_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ be the joint state of Alice and Bob where $\dim(\mathcal{H}_A) \leq 2^q$ and let $\alpha > 0$ be such that the opening probabilities satisfy $P_0^A(\rho) + P_1^A(\rho) = 1 + \alpha$. From Lemma 4, we know that there exists $\rho_{AB}^0 \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ constructed from $\rho$ such that

$$P_0^A(\rho^0) = 1 \text{ and } P_1^A(\rho^0) \geq \alpha^2.$$

We use Corollary 1 and the assumption that the protocol is $\epsilon$-binding against non-adaptive adversaries to show that $\alpha$ cannot be too large. Let $\{\mathbb{F}_{y_0}\}_{y_0}$ be the measurement that maximizes $P_0^A(\rho^0)$. Let us consider Bob's reduced density operator of $\rho^0$:

$$\rho_B^0 = \mathrm{tr}_A(\rho_{AB}^0) = \sum_{y_0} \mathrm{tr}_A((\mathbb{F}_{y_0} \otimes \mathbb{I})\rho_{AB}^0) = \sum_{y_0} \lambda_{y_0}\sigma_{y_0}$$

where for each $y_0$, it holds that $\mathrm{tr}(\mathbb{V}_{y_0}\sigma_{y_0}) = 1$. This implies $\mathrm{tr}(\mathbb{V}_{y_1}\sigma_{y_0}) \leq \epsilon$ for every $y_1$ that opens 1 from our assumption of the non-adaptive security of the commitment scheme. Then

$$P_1^{NA}(\rho_{AB}^0) = \max_{y_1} \mathrm{tr}(\mathbb{V}_{y_1}\rho_B^0) = \max_{y_1} \sum_{y_0} \lambda_{y_0}\, \mathrm{tr}(\mathbb{V}_{y_1}\sigma_{y_0}) \leq \epsilon.$$

Applying Corollary 1 completes the proof:

$$\alpha^2 \leq P_1^A(\rho^0) \leq 2^{I_{\max}^{\mathrm{acc}}(B;A)_{\rho_0}} P_1^{NA}(\rho^0) \leq 2^{\mathrm{H}_0(A)_{\rho_0}}\epsilon \leq 2^q\epsilon.$$

□

### 5.3 Special Case: The BCJL Bit-Commitment Scheme

In this subsection, we use the results of the previous section to prove the security of the BCJL scheme in the bounded storage model against projective measurement attacks.

The BCJL bit-commitment scheme was proposed in 1993 by Brassard et al. [6]. They proposed to hide the committed bit using a two-universal family of hash functions applied on the codeword of an error correcting code and then send this codeword through BB84 qubits. The idea behind this protocol is that privacy amplification hides the committed bit while the error correcting code makes it hard to change the value of this bit without being detected. While their intuition was correct, their proof ultimately was not, as shown by Mayers' impossibility result for bit commitment [18].

The following scheme (Fig. 3) differs only slightly from the original [6], this allows us to recycle some of the analysis from Sect. 4.

COMMIT$(b)$:

1. Let $\mathcal{C}$ be a linear $[n, k, d]$-error correcting code with $k > 0.78n$.
2. Alice chooses a random string $x \in_R \{0,1\}^n$ and a random basis $\theta \in_R \{+, \times\}^n$. She sends $|x\rangle_\theta$ to Bob.
3. Upon reception of the qubits, Bob chooses a random basis $\hat{\theta}$ and measures the qubits in basis $\hat{\theta}$. Let $\hat{x}$ denote his measurement result.
4. Let $\mathcal{G}_n$ be a family of two-universal hash functions. Alice chooses $g \in_R \mathcal{G}_n$ and computes the syndrome $s$ of $x$ for the linear code $\mathcal{C}$. She sends $w = g(x) \oplus b$, $g$ and $s$ to Bob.

REVEAL:

1. Alice sends $x$, $\theta$ and $b$ to Bob.
2. Bob checks that $x$ has syndrome $s$. He then checks that $\hat{x}_i = x_i$ for every $i$ such that $\hat{\theta}_i = \theta_i$. He accepts if $g(x) \oplus w = b$ and none of the above tests failed.

**Fig. 3.** The BCJL bit-commitment scheme

**Theorem 6.** BCJL *is statistically hiding as long as* $0.22 - (1 - k/n) \in \Omega(1)$.

The proof of Theorem 6 is straightforward. It follows the same approach as that of Theorem 3 by noticing that Bob has the same uncertainty about each $x_i$ as he had about $\theta_i$ in protocol COMMIT$^{1\mathsf{CC}}$.

Instead of proving that BCJL is binding, we prove that an equivalent scheme BCJL$_\delta$ (see Fig. 4) is binding. The BCJL$_\delta$ scheme is a modified version of BCJL in which Bob has unlimited quantum memory and stores the qubits sent by Alice during the commit phase instead of measuring them. The opening phase of BCJL$_\delta$ is characterized by a parameter $\delta$ which determines how close it is to the opening phase of BCJL. The following lemma shows that the two protocols are equivalent from Alice's point of view; if Alice can cheat an honest Bob then she can cheat a Bob with unbounded quantum computing capabilities.

**Lemma 5.** *Let* $\delta > 0$. *If* BCJL$_\delta$ *is* $\epsilon$*-binding then* BCJL *is* $(\epsilon + 2 \cdot 2^{-\delta n})$*-binding.*

*Proof.* Let $(x, \theta)$ be an opening to 0. First notice that Bob's actions in BCJL are equivalent to holding onto his state until the opening procedure, measuring in basis $\theta$ and verifying $x_T = \hat{x}_T$ for a randomly chosen sample $T \subseteq [n]$. From this point of view, Bob's measurement result is identically distributed in both protocols and we can speak of $\hat{x}$ without ambiguity. If $d(x, \hat{x}) > \delta n$, then the probability that $x_i = \hat{x}_i$ for all $i \in T$ is at most $2^{-\delta n}$. Therefore, if Bob rejects in REVEAL$_\delta$ with measurement outcome $\hat{x}$, then the probability that he rejects in REVEAL with the same outcome is at least $1 - 2^{-\delta n}$. If we let $p_0$ denote Bob's accepting probability in the original protocol and $p_0^\delta$ in the modified protocol, we have $p_0 \leq p_0^\delta + 2^{-\delta n}$. Since the same holds for openings to 1, we have

COMMIT$_\delta(b)$:

1. Let $\mathcal{C}$ be a linear $[n, k, d]$-error correcting code with $k > 0.78n$.
2. Alice chooses a random string $x \in_R \{0,1\}^n$ and a random basis $\theta \in_R \{+, \times\}^n$. She sends $|x\rangle_\theta$ to Bob.
3. Bob stores all the qubits he received to measure them later.
4. Let $\mathcal{G}_n$ be a family of two-universal hash functions. Alice chooses $g \in_R \mathcal{G}_n$ and computes the syndrome $s$ of $x$ for the linear code $\mathcal{C}$. She sends $w = g(x) \oplus b$, $g$ and $s$ to Bob.

REVEAL$_\delta$:

1. Alice sends $x$, $\theta$ and $b$ to Bob.
2. Bob checks that $x$ has syndrome $s$. He then measures his stored qubits in basis $\theta$ to obtain $\hat{x}$. He accepts if $d(x, \hat{x}) \leq \delta n$ and $g(x) \oplus w = b$ and none of the above tests failed.

**Fig. 4.** The BCJL$_\delta$ bit-commitment scheme.

$$p_0 + p_1 \leq p_0^\delta + p_1^\delta + 2 \cdot 2^{-\delta n} \leq 1 + \epsilon + 2 \cdot 2^{-\delta n}.$$

□

The following proposition establishes the security of BCJL$_\delta$ in the non-adaptive setting. Its proof is straightforward and can be found in Appendix A.

**Proposition 4.** BCJL$_\delta$ *is* $2^{-d/2+\delta n+h(\delta)n}$*-binding against non-adaptive adversaries.*

Since the bit-commitment scheme BCJL$_\delta$ is non-interactive, it directly follows from Theorem 5 and Proposition 4 that BCJL$_\delta$ is $2^{\frac{1}{2}(q-d/2+\delta n+h(\delta)n)}$-binding against $q$-QMB projective adversaries. Combining the above with Lemma 5, we have the following statement for the BCJL scheme.

**Theorem 7.** *The* BCJL *bit-commitment scheme is* $(2^{\frac{1}{2}(q-d/2+\delta n+h(\delta)n)} + 2 \cdot 2^{-\delta n})$*-binding against q-QMB projective adversaries.*

**Acknowledgments.** FD acknowledges the support of the Czech Science Foundation (GAČR) project no. GA16-22211S and of the EU FP7 under grant agreement no. 323970 (RAQUEL). LS is supported by Canada's NSERC discovery grant.

## A Additional proofs

**Proposition 2.** *For any state* $\rho_{ZAB}$ *with classical* $Z$*:*

$$I_{\max}^{\mathrm{acc}}(B; A|Z)_\rho \leq \max_z I_{\max}^{\mathrm{acc}}(B; A)_{\rho^z} \leq H_0(A)_\rho.$$

*Proof.* By assumption, $\rho_{ZAB}$ is of the form $\rho_{ZAB} = \sum_z P_Z(z)|z\rangle\langle z| \otimes \rho^z_{AB}$. Let $\mathcal{M}_{ZA\to X}$ be a measurement on $Z$ and $A$. By linearity, and by definition of $I^{\mathrm{acc}}_{\max}$, we have that

$$\begin{aligned}\mathcal{M}(\rho_{ZAB}) &= \sum_z P_Z(z)\mathcal{M}\big(|z\rangle\langle z| \otimes \rho^z_{AB}\big)\\ &\leq \sum_z P_Z(z)\cdot 2^{I^{\mathrm{acc}}_{\max}(B;A|Z)_{|z\rangle\langle z|\otimes\rho^z}}\mathcal{N}^z\big(|z\rangle\langle z| \otimes \rho^z_B\big)\end{aligned}$$

for suitably chosen measurements $\mathcal{N}^z_{Z\to X}$. Now, noting that $I^{\mathrm{acc}}_{\max}(B;A|Z)_{|z\rangle\langle z|\otimes\rho^z} = I^{\mathrm{acc}}_{\max}(B;A)_{\rho^z}$, and that there exists a fixed measurement $\mathcal{N}_{Z\to X}$ so that $\mathcal{N}^z(|z\rangle\langle z|) = \mathcal{N}(|z\rangle\langle z|)$ for all $z$, it follows that

$$\mathcal{M}(\rho_{ZAB}) \leq 2^{\max_z I^{\mathrm{acc}}_{\max}(B;A)_{\rho^z}}\mathcal{N}(\rho_{ZB}),$$

which implies the first claimed inequality. The second inequality follows immediately by observing that $I^{\mathrm{acc}}_{\max}(B;A)_{\rho^z} \leq H_0(A)_{\rho^z} \leq H_0(A)_\rho$. □

**Proposition 3.** *Let $\mathcal{E}_{AB\to A'B'}$ be a CPTP map of the form $\mathcal{E} = \mathcal{E}^A \otimes \mathcal{E}^B$. Then*

$$I^{\mathrm{acc}}_{\max}(B';A')_{\mathcal{E}(\rho)} \leq I^{\mathrm{acc}}_{\max}(B;A)_\rho.$$

*Proof.* Since the CPTP map $\mathcal{E}^B$ commutes with any measurement applied on Alice's register, it cannot increase the maximal accessible information.

To show that the CPTP map $\mathcal{E}^A$ cannot increase $I^{\mathrm{acc}}_{\max}$, it suffices to show that for every measurement $\mathcal{M}$ on register $A$, the CPTP map $\mathcal{M}\circ\mathcal{E}^A$ is also a measurement. Let $\{E_k\}_k$ be the Kraus operators associated with $\mathcal{E}^A$ and let $\{F_x\}_x$ be the POVM operators describing the measurement $\mathcal{M}$. Then, the positive operators $F'_x := \sum_k E_k^\dagger F_x E_k$ describe a POVM $\mathcal{M}'$, and

$$\mathcal{M}\circ\mathcal{E}^A(\rho) = \mathcal{M}'(\rho) \leq 2^{I^{\mathrm{acc}}_{\max}(B;A)_\rho}\sigma_X \otimes \rho_B$$

by the definition of $I^{\mathrm{acc}}_{\max}(B;A)_\rho$ for some normalized $\sigma_X$. □

**Proposition 4.** *Protocol* BCJL$_\delta$ *is $2^{-d/2+\delta n+h(\delta)n}$-binding against non-adaptive adversaries.*

*Proof.* Let $\rho_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ be the joint state of Alice and Bob and let $\mathbb{V}^\delta_{x,\theta} := \sum_{z\in B^\delta(x)}|z\rangle\langle z|_\theta$ be the projective measurement corresponding to Bob's verification procedure in protocol BCJL$_\delta$ if Alice announced $(x,\theta)$. Using Lemma 1, we have that for any two distinct openings $(x,\theta)$ and $(x',\theta')$,

$$\begin{aligned}\mathrm{tr}(\mathbb{V}^\delta_{x,\theta}\rho_B) + \mathrm{tr}(\mathbb{V}^\delta_{x',\theta'}\rho_B) &= \mathrm{tr}((\mathbb{V}^\delta_{x,\theta} + \mathbb{V}^\delta_{x',\theta'})\rho_B)\\ &\leq ||\mathbb{V}^\delta_{x,\theta} + \mathbb{V}^\delta_{x',\theta'}||\\ &\leq 1 + ||\mathbb{V}^\delta_{x,\theta}\mathbb{V}^\delta_{x',\theta'}||.\end{aligned}$$

Using techniques from [5], we can show that

$$||\mathbb{V}^\delta_{x,\theta}\mathbb{V}^\delta_{x',\theta'}|| \leq \max_{\substack{z\in B^\delta(x)\\ z'\in B^\delta(x')}} |\langle z|_\theta|z'\rangle_{\theta'}|\sqrt{|B^\delta(x)||B^\delta(x')|}.$$

Using the fact that $d(z, z') \geq d - 2\delta n$ for $z \in B^\delta(x)$ and $z' \in B^\delta(x')$ for any two strings $x$ and $x'$ with the same syndrome, and the fact that $|B^\delta(x)| \leq 2^{h(\delta)n}$, it follows that when maximizing over openings to 0 and 1, we obtain

$$P_0^{NA}(\rho_{AB}) + P_1^{NA}(\rho_{AB}) \leq 1 + 2^{-d/2+\delta n+h(\delta)n}.$$

□

# B UC-Completeness of 1CC

## B.1 The UC Model

In order to show that a scheme securely implements a given functionality F in the universally composable (UC) model, one has to show that for any *adversary* that attacks the scheme by corrupting participants, there exists a *simulator* $\mathcal{S}$ that instead attacks the functionality, but is indistinguishable from the adversary from an outside observer's perspective. More precisely, one considers an *environment* $\mathcal{Z}$ that interacts with the adversary in the *real* model where the scheme is executed, or with $\mathcal{S}$ in the *ideal* model where the functionality F is executed, and it provides input to and obtains output from the uncorrupt players (see Fig. 5). The scheme is said to *statistically quantum-UC-emulate* the functionality if the environment cannot distinguish the real from the ideal model with non-negligible probability. For a more detailed description of the quantum UC framework, we refer to [9,20].

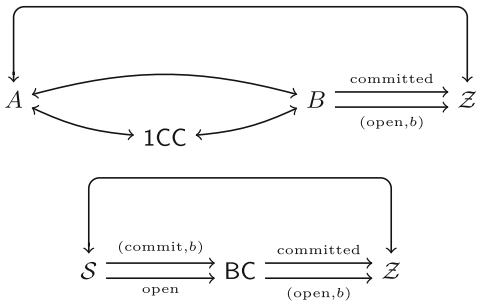


**Fig. 5.** The real model (top) and the ideal model (bottom) for protocol $\text{BC}^{\text{1CC}}$ and functionality BC, respectively, with a dishonest Alice. $\text{BC}^{\text{1CC}}$ statistically quantum-UC-emulates BC (against dishonest Alice) if the two models are indistinguishable for $\mathcal{Z}$.

Most UC security proofs follow a similar mold. $\mathcal{S}$ internally runs a copy of the adversary, and it simulates the actions and interactions of the honest party, and of functionalities that are possibly used as subroutines in the scheme. $\mathcal{S}$ must look like the real model adversary to the environment $\mathcal{Z}$, so it forwards any message it receives from $\mathcal{Z}$ to (its internal execution of) the adversary and vice versa. Furthermore, from the interaction with the adversary, it extracts the input(s) it has to provide to F (see Fig. 6).

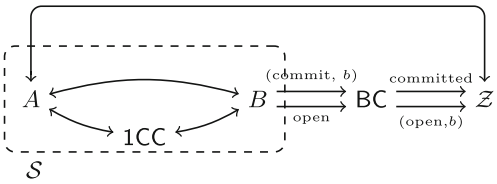


**Fig. 6.** The standard way for constructing $\mathcal{S}$: run dishonest Alice internally and simulate honest Bob and the calls to the functionality 1CC, and extract the input to BC.

In all our proofs below, the honest party is simulated by $\mathcal{S}$ by running it *honestly*, up to possible small modifications that are unnoticeable to the adversary, and that do not affect the (simulated) honest party's output. As such, in our proofs below, for showing indistinguishability of the real and the ideal model, it is sufficient to argue that, in the ideal model, the output of the simulated honest party equals what F outputs to $\mathcal{Z}$ upon the input that is provided by $\mathcal{S}$.

### B.2 UC Security of OT from 1CC

As explained in Sect. 4.4, our protocol $\text{BC}^{\text{1CC}}$ does not seem to satisfy the UC security definition in case of a corrupted verifier Bob. As such, we cannot conclude UC security of the standard BC-based OT scheme [2,7] with BC instantiated by $\text{BC}^{\text{1CC}}$. Instead, we show UC security of OT from 1CC by means of the following strategy.

First, we show UC security of $\text{BC}^{\text{1CC}}$ against a corrupted committer Alice (Proposition 5). Then, we show that BC and 1CC together imply 2CC (actually, a variation of 2CC that gives Alice the option to abort) by means of a straightforward protocol (Proposition 6), and we recall that 2CC implies OT by means of the protocol $\text{OT}^{\text{2CC}}$ from [9]. Instantiating the underlying functionality BC by $\text{BC}^{\text{1CC}}$ then gives us a protocol $\text{OT}^{\text{1CC}}$ (Fig. 8) with UC security against a corrupted receiver (Lemma 6). Finally, it is rather straightforward to prove UC security of $\text{OT}^{\text{1CC}}$ against a corrupted sender directly (Lemma 7).

**Proposition 5.** *Protocol* $\text{BC}^{\text{1CC}}$ *statistically quantum-UC-emulates* BC *against corrupted committer Alice.*

*Proof.* The construction of $\mathcal{S}$ follows the paradigm outlined above. $\mathcal{S}$ runs dishonest Alice internally, and it simulates honest Bob and 1CC by running them honestly. Note that $\mathcal{S}$ gets to see Alice's inputs to 1CC. Once Alice announces $g, w$ and $s$ at the end of the commit phase, $\mathcal{S}$ computes $b = g(\theta') \oplus w$, where $\theta'$ is the string of syndrome $s$ closest to the stored $\theta_{\bar{t}}$, and inputs "(commit, $b$)" into the BC functionality. Finally, when corrupted Alice opens her commitment, $\mathcal{S}$ inputs "open" into BC if Bob accepted the opening, and inputs "abort" if Bob aborted.

It now follows immediately from Lemma 3 that the bit $b'$ output by the simulated Bob equals the bit $b$ computed by $\mathcal{S}$ and input to BC, except with negligible probability. As such, real and ideal model are statistically indistinguishable. □

**Parties**: The sender Alice and the receiver Bob.
**Inputs**: Alice receives $s_0, s_1 \in \{0,1\}$ and Bob receives $c \in \{0,1\}$.

1. Alice inputs "(commit, $s_0$)" in $\mathsf{BC}$, Bob receives "committed".
2. Alice and Bob invoke $\mathsf{1CC}$ with respective inputs $s_1$ and $c$.
3. If Alice receives $c = 1$ from $\mathsf{1CC}$, she sends "open" to $\mathsf{BC}$. Bob receives $s_0$ from $\mathsf{1CC}$ and $s_1$ from $\mathsf{BC}$.
4. Alice outputs $c$, Bob outputs $(s_0, s_1)$ if $c = 1$ and $\perp$ if $c = 0$. Bob outputs "abort" if $c = 1$ but Alice refuses to open her commitment.

**Fig. 7.** Protocol $2\text{CC}^{\mathsf{BC},\mathsf{1CC}}$.

Consider the candidate 2-bit cut-and-choose protocol $2\text{CC}^{\mathsf{BC},\mathsf{1CC}}$ from Fig. 7. This protocol does not implement the full-fledged $\mathsf{2CC}$ functionality, but a variation $\mathsf{2CC}'$ that gives the sender the option to abort after it sees the receiver's input $c$. This is because in the protocol the sender can refuse to open its commitments (or try to cheat when opening them so that the receiver will reject). In that case, the receiver will only learn one of the receiver's two inputs. This will not influence the security of the resulting $\mathsf{OT}$ scheme since aborting in any instance of $\mathsf{2CC}'$ will stop the protocol.

Formally, $\mathsf{2CC}'$ is described as follows: it first waits for inputs $(s_0, s_1)$ from Alice and $c$ from Bob. Upon reception of both inputs, it sends $c$ to Alice. If $c = 0$, it sends $\perp$ to Bob. If $c = 1$, it waits for response "abort" or "continue" from Alice. On input "continue", $\mathsf{2CC}'$ outputs $(s_0, s_1)$ to Bob and on input "abort", it outputs "abort".

**Proposition 6.** *Protocol* $2\text{CC}^{\mathsf{BC},\mathsf{1CC}}$ *statistically quantum-UC-emulates* $\mathsf{2CC}'$.

*Proof.* We first consider a corrupted sender Alice. $\mathcal{S}$ simulates Bob, $\mathsf{BC}$ and $\mathsf{1CC}$ by running them honestly. After step 2, when $\mathcal{S}$ has learned Alice's respective inputs $s_0$ and $s_1$ to $\mathsf{BC}$ and $\mathsf{1CC}$, it inputs $(s_0, s_1)$ into the functionality $\mathsf{2CC}'$. After receiving $c$ from the $\mathsf{2CC}'$, $\mathcal{S}$ makes Bob input $c$ into the $\mathsf{1CC}$. If $c = 0$ then the simulated Bob and $\mathsf{2CC}'$ both output $\perp$. If $c = 1$ then Alice is supposed to open her commitment. If she refuses then $\mathcal{S}$ inputs "abort" into $\mathsf{2CC}'$, and the simulated Bob and $\mathsf{2CC}'$ both output "abort". Otherwise, i.e., if Alice opens the commitment (to $s_0$), $\mathcal{S}$ inputs "continue", and the simulated Bob and $\mathsf{2CC}'$ both output $(s_0, s_1)$. This proves the claim for a corrupted sender Alice. Security against a corrupted receiver Bob is similarly straightforward. □

**Corollary 2.** *Protocol* $2\text{CC}^{\mathsf{1CC}}$*, obtained by replacing each instance of* $\mathsf{BC}$ *by* $\text{BC}^{\mathsf{1CC}}$*, statistically quantum-UC-emulates* $\mathsf{2CC}'$ *against corrupted sender.*

*Proof.* Since $\text{BC}^{\mathsf{1CC}}$ statistically quantum UC-emulates $\mathsf{BC}$ against malicious committer, and since the sender in $2\text{CC}^{\mathsf{BC},\mathsf{1CC}}$ is the committer of $\mathsf{BC}$, we can replace $\mathsf{BC}$ with $\text{BC}^{\mathsf{1CC}}$ in protocol $2\text{CC}^{\mathsf{BC},\mathsf{1CC}}$ and still maintain UC-security against corrupted sender. □

**Parameters**: A family $\mathcal{F} = \{\{0,1\}^n \to \{0,1\}^\ell\}$ of universal hash functions.
**Parties**: The sender Alice and the receiver Bob.
**Inputs**: Alice receives $s_0, s_1 \in \{0,1\}^\ell$ and Bob receives $c \in \{0,1\}$.

1. Alice chooses $x^A \in_R \{0,1\}^n$ and $\theta^A \in_R \{+,\times\}^n$ and sends the state $|x^A\rangle_{\theta^A}$ to Bob.
2. Upon reception, Bob chooses $\theta^B \in_R \{+,\times\}^n$ and measures the received state in basis $\theta^B$. Lets $x^B$ denote the measurement outcome.
3. For $i = 1 \ldots n$, do
   (a) Alice and Bob perform protocol $\text{COMMIT}^{\mathsf{1CC}}$ with Bob as the sender and input $\theta_i^B$.
   (b) Alice chooses a selection bit $t_i \in_R \{0,1\}$ and they invoke an instance of $\mathsf{1CC}$ with Bob as the sender and inputs $t_i$ and $x_i^B$.
   (c) Whenever $t_i = 1$, Bob opens the $i$th commitment using protocol $\text{REVEAL}^{\mathsf{1CC}}$.
4. If for some $i$ s.t. $t_i = 1$, $\theta_i^A = \theta_i^B$, but $x_i^B \neq x_i^A$, Alice aborts. Bob aborts if $t_i = 1$ for more than $3n/5$ positions. Let $\hat{x}^A$ (resp. $\hat{\theta}^A, \hat{x}^B, \hat{\theta}^B$) be the restriction of $x^A$ (resp. $\theta^A, x^B, \theta^B$) to the indices $i$ for which $t_i = 0$.
5. Alice sends $\hat{\theta}^A$ to Bob. Bob constructs sets $I_c = \{i \mid \hat{\theta}_i^A = \hat{\theta}_i^B\}$ and $I_{1-c} = \{i \mid \hat{\theta}_i^A \neq \hat{\theta}_i^B\}$ then sends $(I_0, I_1)$ to Alice.
6. Alice chooses $f \in_R \mathcal{F}$, computes $m_i = s_i \oplus f(\hat{x}_{I_i}^A)$ for $i = 0, 1$ and sends $(f, m_0, m_1)$ to Bob.
7. Bob outputs $s = m_c \oplus f(\hat{x}_{I_c}^B)$.

**Fig. 8.** Protocol $\text{OT}^{\mathsf{1CC}}$.

**Lemma 6.** *Protocol* $\text{OT}^{\mathsf{1CC}}$ *statistically quantum UC-emulates* $\mathsf{OT}$ *for corrupted receiver.*

*Proof.* Note that steps 3a through 3c of protocol $\text{OT}^{\mathsf{1CC}}$ are identical to protocol $\text{2CC}^{\mathsf{1CC}}$ defined above with Bob as the sender and Alice as the receiver. Since $\text{2CC}^{\mathsf{1CC}}$ statistically quantum-UC-emulates $\mathsf{2CC}'$ against corrupted sender, we may replace steps 3a–3c by a single call to $\mathsf{2CC}'$ with Bob as the sender and Alice as the receiver, and analyze the security of this protocol instead. The only difference between this protocol and the $\mathsf{2CC}$-based oblivious-transfer protocol from [9] is that the former uses $\mathsf{2CC}'$ instead. However, this change does not affect UC-security since any adversary that aborts during one of the $\text{2CC}^{\mathsf{1CC}}$ subroutines is indistinguishable from an adversary that aborts right after the same subroutine. It directly follows from the analysis of [9], that protocol $\text{OT}^{\mathsf{1CC}}$ statistically quantum-UC-emulates $\mathsf{OT}$ against corrupted receiver. □

**Lemma 7.** *Protocol* $\text{OT}^{\mathsf{1CC}}$ *statistically quantum UC-emulates* $\mathsf{OT}$ *for corrupted sender.*

*Proof.* Let Alice be the corrupted sender and Bob the honest receiver. $\mathcal{S}$ simulates Bob and $\mathsf{1CC}$ by running them honestly, *except* that Bob does *not* measure

the received state in step 2 but stores it, and in step 3b, whenever Alice inputs $t_i = 1$ into $\mathsf{1CC}$, $\mathcal{S}$ "rushes" and measures the $i$th qubit in basis $\theta_i^B$ and inputs the outcome $x_i^B$ in the $\mathsf{1CC}$. Furthermore, in step 5, $\mathcal{S}$ replies to Alice with a random partition $(I_0, I_1)$. At the end of the protocol, $\mathcal{S}$ measures the remaining qubits in Alice's basis $\hat{\theta}^A$ to obtain $\hat{x}^B$, computes $s_i = m_i \oplus f(\hat{x}^B_{I_i})$ for $i = 0, 1$, and sends $(s_0, s_1)$ to the ideal $\mathsf{OT}$ functionality.

The output of $\mathsf{OT}$, i.e., $s_c$, coincides with the string that a fully honest Bob would have output; hence, we have indistinguishability between the real and the ideal model. □

**Theorem 8.** $\mathsf{1CC}$ *is statistically quantum UC-complete.*

*Proof.* We have shown that $\text{OT}^{\mathsf{1CC}}$ statistically quantum-UC-emulates $\mathsf{OT}$. Since $\mathsf{OT}$ is quantum-UC-complete, we conclude that $\mathsf{1CC}$ is also quantum-UC-complete. □

## References


1. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68**, 3121–3124 (1992)
2. Bennett, C.H., Brassard, G., Crépeau, C., Skubiszewska, M.-H.: Practical quantum oblivious transfer. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 351–366. Springer, Heidelberg (1992)
3. Berta, M., Christandl, M., Renner, R.: The quantum reverse Shannon theorem based on one-shot information theory. Commun. Math. Phys. **306**(3), 579–615 (2011)
4. Bouman, N.J., Fehr, S.: Sampling in a quantum population, and applications. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 724–741. Springer, Heidelberg (2010)
5. Bouman, N.J., Fehr, S., González-Guillén, C., Schaffner, C.: An all-but-one entropic uncertainty relation, and application to password-based identification. In: Kawano, Y. (ed.) TQC 2012. LNCS, vol. 7582, pp. 29–44. Springer, Heidelberg (2012)
6. Brassard, G., Crépeau, C., Jozsa, R., Langlois, D.: A quantum bit commitment scheme provably unbreakable by both parties. In: Proceedings of the 34th Annual IEEE Symposium on the Foundation of Computer Science, pp. 362–371 (1993)
7. Crépeau, C.: Quantum oblivious transfer. J. Mod. Opt. **41**(12), 2445–2454 (1994)
8. Damgård, I., Fehr, S., Salvail, L., Schaffner, C.: Cryptography in the bounded-quantum-storage model. SIAM J. Comput. **37**(6), 1865–1890 (2008)
9. Fehr, S., Katz, J., Song, F., Zhou, H.-S., Zikas, V.: Feasibility and completeness of cryptographic tasks in the quantum world. In: Sahai, A. (ed.) TCC 2013. LNCS, vol. 7785, pp. 281–296. Springer, Heidelberg (2013)
10. Kilian, J.: Founding cryptography on oblivious transfer. In: Proceedings of the ACM Symposium on Theory of Computing, STOC 1988, pp. 20–31. ACM, New York (1988)
11. Kilian, J.: A general completeness theorem for two party games. In: Proceedings of the Twenty-Third Annual ACM Symposium on Theory of Computing, STOC 1991, pp. 553–560 (1991)

12. Kilian, J.: More general completeness theorems for secure two-party computation. In: Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, STOC 2000, pp. 316–324 (2000)
13. König, R., Renner, R., Schaffner, C.: The operational meaning of min- and max-entropy. IEEE Trans. Inf. Theor. **55**(9), 4337–4347 (2009)
14. Kraschewski, F.: Complete primitives for information-theoretically secure two-party computation. Ph.D. thesis, Karlsruhe Institute of Technology (2013)
15. Kraschewski, D., Müller-Quade, J.: Completeness theorems with constructive proofs for finite deterministic 2-party functions. In: Ishai, Y. (ed.) TCC 2011. LNCS, vol. 6597, pp. 364–381. Springer, Heidelberg (2011)
16. Maji, H.K., Prabhakaran, M., Rosulek, M.: A zero-one law for cryptographic complexity with respect to computational UC security. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 595–612. Springer, Heidelberg (2010)
17. Maji, H.K., Prabhakaran, M., Rosulek, M.: A unified characterization of completeness and triviality for secure function evaluation. In: Galbraith, S., Nandi, M. (eds.) INDOCRYPT 2012. LNCS, vol. 7668, pp. 40–59. Springer, Heidelberg (2012)
18. Mayers, D.: Unconditionally secure quantum bit commitment is impossible. Phys. Rev. Lett. **78**, 3414–3417 (1997)
19. Renner, R.S., König, R.: Universally composable privacy amplification against quantum adversaries. In: Kilian, J. (ed.) TCC 2005. LNCS, vol. 3378, pp. 407–425. Springer, Heidelberg (2005)
20. Unruh, D.: Universally composable quantum multi-party computation. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 486–505. Springer, Heidelberg (2010)

http://www.springer.com/978-3-662-53014-6

Advances in Cryptology – CRYPTO 2016
36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part III
Robshaw, M.; Katz, J. (Eds.)
2016, XIII, 651 p. 77 illus., Softcover
ISBN: 978-3-662-53014-6