On the Cryptographic Structure Required for Verifying Qubits

James Bartusek* Itay Shalit†

June 9, 2026

Abstract

Classically testing for the presence of anti-commuting operators on a quantum device is a critical tool underpinning recent progress in classical verification of quantum computation. While we can base such tests on certain cryptographic assumptions, known results require highly structured assumptions, e.g. trapdoor claw-free functions.

In this work, we seek to explain this state of affairs by *constructing* strong cryptography from (certain forms of) classical tests of anti-commutation. In particular, we formulate the notion of a "test of non-commutation" (ToNC), which is an interactive protocol between a quantum prover and classical verifier where, in the final round, the prover applies one of two binary observables P_0, P_1 depending on the verifier's challenge bit c. An (ϵ, δ)-ToNC is any such protocol where there exists a quantum strategy that attains ϵ advantage in making the verifier accept, but any quantum strategy with *commuting* P_0, P_1 can attain at most δ advantage. We then show the following results.

- (ϵ, δ)-ToNC implies (classical-communication) key agreement (KA) for any $\delta < \frac{5\epsilon-1}{4}$.
- (ϵ, δ)-ToNC plus one-way functions implies (classical-communication) oblivious transfer (OT) for any $\delta < \frac{\epsilon^2+\epsilon}{2}$.

Along the way, we develop tools for and provide the first known results on hardness amplification for *post-quantum* KA and OT, where the communication is classical but the adversary may be quantum. In particular, we prove the following results of independent interest.

- Post-quantum hard-core measure theorem: For any efficiently sampleable, high min-entropy distribution D over classical (x, b) such that quantum circuits have advantage at most δ in predicting b given x, there exists a sub-distribution $M \preceq D$ of density $1 - \delta$ such that b is (nearly) optimally quantum-hard to predict on $(x, b) \leftarrow M$.
- Post-quantum interactive XOR lemma: Given any classically-interactive protocol such that quantum adversaries have advantage at most δ in guessing a private challenger bit b, repeating sequentially yields a protocol where quantum adversaries have advantage at most $\delta^2 + \mathrm{negl}(\lambda)$ in guessing the XOR of the two challenger bits $b_1 \oplus b_2$.

*Columbia University. Email: bartusek.james@gmail.com.

†Stanford University. Email: ishalit@stanford.edu. Supported by a Shoucheng Zhang Graduate Fellowship.

Contents

1 Introduction **3**
- 1.1 Results . . . 4
- 1.2 Related work . . . 9
- 1.3 Open problems . . . 11

2 Technical overview **11**
- 2.1 Weak BA from ToNC . . . 12
- 2.2 Weak OT from ToNC . . . 12
- 2.3 BA amplification . . . 14
- 2.4 OT amplification . . . 17

3 Preliminaries **19**
- 3.1 Cryptographic primitives . . . 20
- 3.2 Alternating projectors . . . 23

4 Tests of non-commutation **24**
- 4.1 Definitions . . . 24
- 4.2 Normal form compiler . . . 25

5 Weak cryptography from tests of non-commutation **30**
- 5.1 Weak bit agreement . . . 30
- 5.2 Weak (committed-bit) oblivious transfer . . . 32

6 Hardness amplification **37**
- 6.1 Post-quantum hard-core measure theorem . . . 37
- 6.2 Key agreement amplification . . . 54
- 6.3 Post-quantum interactive XOR lemma . . . 63
- 6.4 Oblivious transfer amplification . . . 67

1 Introduction

The qubit, being the basic unit of quantum information, lies at the foundation of quantum computation and the theory of quantum mechanics itself. While one can define a qubit as a unit vector in $\mathbb{C}^2$, it can alternatively be understood as any pair of anti-commuting binary observables [Vid20]. This idea traces its origins back to the Heisenberg view of quantum mechanics, and is justified by the fact that any pair of anti-commuting binary observables is, up to an isometry, equivalent to the Pauli observables σ_X and σ_Z operating on $\mathbb{C}^2$. It turns out that this definition has particularly nice operational properties, as discussed at length in [Vid20].

Verifying qubits. A natural question of importance to the theory of quantum mechanics, and especially so in the early days of quantum information-processing, is whether it is possible to *classically* test for the presence of a qubit on a purported quantum device. That is, can we validate the existence of anti-commuting operators just by sending classical signals and receiving classical responses? This motivates the following definition of a "qubit test".

> ***Qubit test (informal).*** A qubit test is a classical interactive protocol between a classical (polynomial-time) verifier and a quantum (polynomial-time) prover, whose description includes two binary observables P_0, P_1. In the final round, the verifier sends a challenge $c \in \{0,1\}$, and the prover returns the bit obtained by applying P_c to its current state. For any prover that makes the verifier accept with probability greater than some threshold α, it must be the case that $P_0 P_1 \approx -P_1 P_0$.

While qubit tests are of inherent interest as a bridge between the classical and quantum worlds, in recent years they have also played a key role in the construction of several more advanced classical verification protocols. For example, methods developed to test for the presence of qubits underpin certifiable randomness protocols [BCM+21], classical verification of general BQP computation [Mah22, NZ23], verifiable remote state preparation (and applications) [GV19, Zha25, Zha23], and computational self-testing (and applications) [MV21, MDCAF21], to name a few.

Cryptographic instantiations. By now, the community has developed several constructions of qubit tests. The first result was due to [BCM+21], who instantiated them[1] from the assumption of learning with errors (LWE), or more generally from trapdoor claw-free functions that satisfy an "adaptive hard-core bit" property. Followup work has diversified and broadened the set of assumptions known to imply qubit tests, yielding constructions from "plain" trapdoor claw-free functions [KMCVY22, BGKM+23], quantum fully-homomorphic encryption [KLVY23], cryptographic group actions [AMR22], oblivious state preparation [BK25], and the lattice isomorphism problem (LIP) [BMM25].

However, a common pattern can be identified behind these results. In particular, all instantiations rely on mathematically "structured" assumptions (LWE, group actions, LIP) that imply strong forms of asymmetric cryptography such as (classical-communication) oblivious transfer. In fact, it remains open to construct qubit tests even given some basic forms of asymmetric structure, such as a (plain) trapdoor function.

[1] Strictly speaking, this construction does not conform to the qubit test defined above, as the final prover answers are strings instead of single bits.

Comparison with proofs of quantumness. This situation can be contrasted with what is known about the relaxed goal of (classically) verifiable *proofs of quantumness*. Here, the goal is to devise a protocol where quantum provers have a strictly greater advantage than classical provers, but do not guarantee anything beyond the fact that the prover is non-classical. It is known that efficiently-verifiable proofs of quantumness exist in the random oracle model (that is, from a heuristic use of unstructured cryptography) [YZ24] and *inefficiently*-verifiable proofs of quantumness exist if (and only if) one-way puzzles exist [MSY25], which are believed to be weaker even than one-way functions [KT24, Kre21, MY22].

While proofs of quantumness have relevance to the goal of establishing quantum advantage, they do not appear to serve as a bedrock for obtaining more advanced forms of classical verification. This state of affairs brings into focus a potential dividing line between proofs of quantumness and qubit tests, both in terms of functionality (the methods behind qubit tests appear to have much more powerful applications) and feasibility (proofs of quantumness can be instantiated with hash functions, while qubit tests are only known from structured assumptions). The goal of this work is to gain a more principled understanding of why this line exists.

Tests of non-commutation. In fact, we consider a weaker primitive which merely certifies that the prover's observables do not *fully* commute, rather than that they approximately anti-commute. We refer to this primitive as a test of non-commutation (ToNC). It differs from a qubit test only in the soundness guarantee: For any quantum polynomial-time prover that succeeds with probability greater than α, we require that $P_0P_1 \neq P_1P_0$ in place of the stronger conclusion that $P_0P_1 \approx -P_1P_0$. We proceed to show that ToNCs imply certain strong forms of cryptography, which establishes the same for full-fledged qubit tests.

1.1 Results

We give constructions of fully-secure oblivious transfer and key agreement protocols with purely classical communication, starting from (even weakly-secure) tests of non-commutation (ToNC). Along the way, we obtain the first *post-quantum* hardness amplification results for bit agreement (BA) and oblivious transfer (OT), which are of independent interest. Our main novel techniques go into building weakly-secure OT, and amplifying both weakly-secure BA and OT to their fully-secure variants. In order to present these results precisely, we first fix definitions of ToNC, weak bit agreement, and OT.

Definitions. We begin by formalizing our notion of ToNC. As discussed above, we consider interactive protocols where the prover's strategy consists of three parts: a quantum polynomial-time (QPT) interactive machine P_{Prep} that interacts with a PPT verifier V, and two (potentially non-commuting) binary observables P_0, P_1. The interactive phase is denoted as

$$|\psi\rangle, c, a^* \leftarrow \langle P_{\mathsf{Prep}}(1^\lambda), V(1^\lambda)\rangle,$$

where $|\psi\rangle$ is the prover's final state, $c \in \{0,1\}$ is a challenge bit sent to the prover, and a^* is the "correct" answer bit kept private by the verifier. We then define a (ϵ, δ)-ToNC as satisfying the following properties.[2]

[2]The reader may notice that the verification procedure implicit in this definition is not fully general. Indeed, rather than apply an arbitrary predicate on its state and the prover's response a, the verifier simply checks whether $a = a^*$. In fact, in the body we define a ToNC more generally, and then show that any ToNC can be compiled into the form written here (which we call a "normal form" ToNC) while preserving the completeness-soundness gap.

- **ToNC Completeness**: It holds that

$$\Pr\left[a = a^* : \begin{array}{r} |\psi\rangle, c, a^* \leftarrow \langle P_{\mathsf{Prep}}(1^\lambda), V(1^\lambda)\rangle \\ a \leftarrow P_c(|\psi\rangle) \end{array}\right] \geq \frac{1}{2} + \frac{\epsilon}{2}.$$

- **ToNC Soundness**: For any QPT strategy $\widetilde{P}_{\mathsf{Prep}}, \widetilde{P}_0, \widetilde{P}_1$ such that $\widetilde{P}_0\widetilde{P}_1 = \widetilde{P}_1\widetilde{P}_0$,

$$\Pr\left[a = a^* : \begin{array}{r} |\psi\rangle, c, a^* \leftarrow \langle \widetilde{P}_{\mathsf{Prep}}(1^\lambda), V(1^\lambda)\rangle \\ a \leftarrow \widetilde{P}_c(|\psi\rangle) \end{array}\right] \leq \frac{1}{2} + \frac{\delta}{2} + \mathrm{negl}(\lambda).$$

It may be useful to keep a running example of a ToNC in mind. Consider the "compiled" CHSH game [KMCVY22, KLVY23]. Here, the (honest) state $|\psi\rangle$ is a single qubit either in the standard or the Hadamard basis, and the challenge c tells the (honest) prover whether to measure it in the $X+Z$ or $X-Z$ basis. In the compiled CHSH game, we have $\epsilon = 2\cos^2(\pi/8) - 1 \approx 0.7$, while there are several instantiations under various cryptographic assumptions attaining the soundness bound $\delta = 0.5$.

Next, we consider standard game-based definitions for (weak) bit agreement and (weak) OT. Bit agreement is an interactive protocol that takes place between two parties A and B, denoted as

$$k_A, k_B, \tau \leftarrow \langle A(1^\lambda), B(1^\lambda)\rangle,$$

where $k_A \in \{0,1\}$ is A's output, $k_B \in \{0,1\}$ is B's output, and τ denotes the (classical) transcript of interaction that occurs between A and B. We then define a (ϵ, δ)-BA as satisfying the following properties.

- **Lack of bias:**

$$\left|\Pr_{(k_A,k_B,\tau)\leftarrow\langle A(1^\lambda),B(1^\lambda)\rangle}[k_A = 0] - \frac{1}{2}\right| = \mathrm{negl}(\lambda), \quad \left|\Pr_{(k_A,k_B,\tau)\leftarrow\langle A(1^\lambda),B(1^\lambda)\rangle}[k_B = 0] - \frac{1}{2}\right| = \mathrm{negl}(\lambda),$$

- **BA Correctness**:

$$\Pr_{(k_A,k_B,\tau)\leftarrow\langle A(1^\lambda),B(1^\lambda)\rangle}[k_A = k_B] \geq \frac{1}{2} + \frac{\epsilon}{2} - \mathrm{negl}(\lambda).$$

- **BA Security**: For any QPT adversary $\widetilde{E}$,

$$\Pr_{(k_A,k_B,\tau)\leftarrow\langle A(1^\lambda),B(1^\lambda)\rangle}\left[\widetilde{E}(\tau) = k_A \mid k_A = k_B\right] \leq \frac{1}{2} + \frac{\delta}{2} + \mathrm{negl}(\lambda).$$

Note that $(1,0)$-BA is the fully-secure notion, which we will just call bit agreement, or sometimes key agreement.

Finally, (weak) OT is an interactive protocol that takes place between a sender S and receiver R, denoted as

$$(b, r), (r_0, r_1) \leftarrow \langle R(1^\lambda), S(1^\lambda)\rangle,$$

where $(b, r) \in \{0,1\}^2$ is the output of R and $(r_0, r_1) \in \{0,1\}^2$ is the output of S. We then define a $(\epsilon, \delta, \gamma)$-OT as satisfying the following properties.

- **OT Correctness**: It holds that

$$\Pr\Big[r = r_b : \ \ (b,r),(r_0,r_1) \leftarrow \langle R(1^\lambda), S(1^\lambda)\rangle \ \Big] \geq \frac{1}{2} + \frac{\epsilon}{2} - \mathrm{negl}(\lambda).$$

- **OT Receiver security**: For any QPT adversarial sender $\widetilde{S}$,

$$\Pr\Big[\widetilde{b} = b : (b,r), \widetilde{b} \leftarrow \langle R(1^\lambda), \widetilde{S}\rangle\Big] \leq \frac{1}{2} + \frac{\gamma}{2} + \mathrm{negl}(\lambda).$$

- **OT Sender security**: For any QPT adversarial receiver $\widetilde{R}$,

$$\Pr\Big[\widetilde{r} = r_0 \oplus r_1 : \ \ \widetilde{r}, (r_0,r_1) \leftarrow \langle \widetilde{R}, S(1^\lambda)\rangle \ \Big] \leq \frac{1}{2} + \frac{\delta}{2} + \mathrm{negl}(\lambda).$$

Note that $(1,0,0)$-OT is the fully-secure notion, which we just refer to as OT.

Main results: BA and OT from ToNC. We are now in a position to state our main results, establishing that strong forms of cryptography are inherent to tests of non-commutation. In this section, whenever we say ToNC, we always mean *normal-form* ToNC as defined above, where there is always exactly one correct answer bit (as discussed above).

Before stating the theorems, we note that (ϵ,δ)-ToNC is impossible whenever $\delta < \epsilon/2$. This is because, given any (potentially non-commuting) strategy that attains advantage ϵ, one can derive a commuting strategy with advantage $\epsilon/2$, by sampling a random bit c', running the ϵ-good strategy when $c = c'$, and outputting a uniformly random bit when $c = 1 - c'$.

We first consider an implication to (classical-communication) key agreement, which holds unconditionally.

Theorem 1.1. *(ϵ,δ)-ToNC implies classical-communication key agreement for any constants ϵ,δ such that*

$$\delta < \frac{5\epsilon - 1}{4}.$$

Moreover, (ϵ,δ)-ToNC with robust completeness[3] *implies classical-communication key agreement for* any *non-trivial parameters, i.e., whenever $\delta < \epsilon$.*

Due to the nature of our techniques, we establish the above in the presence of adversaries with non-uniform *classical* advice, but not necessarily non-uniform quantum advice.

Next, we build (classical-communication) OT. Here, we make use of (post-quantum) one-way functions in addition to the ToNC.

Theorem 1.2. *(ϵ,δ)-ToNC plus one-way functions implies classical-communication oblivious transfer for any constants ϵ,δ such that*

$$\delta < \frac{\epsilon^2 + \epsilon}{2}.$$

Here, we actually establish the above in the presence of adversaries with non-uniform *quantum* advice, but not necessarily non-uniform classical advice.[4]

[3] Robust completeness (Definition 4.4) demands that the honest strategy succeeds with the same probability for any sampling of the preamble, which is a natural property that is satisfied by schemes such as the compiled CHSH and magic square games.

[4] Note that the classical advice case does not necessarily follow as a special case of the quantum advice case, and indeed our particular reduction requires the use of quantum advice.

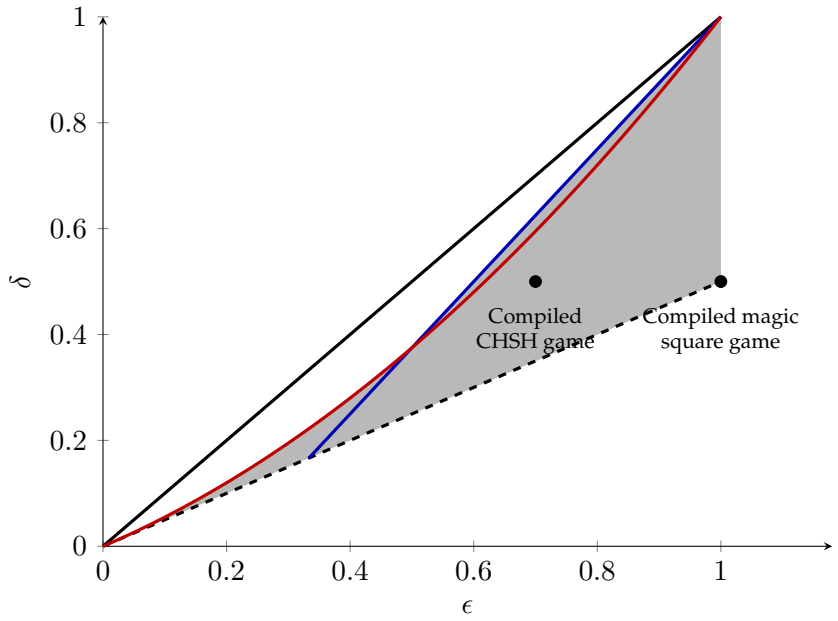

Figure 1: Visualization of the parameter regimes captured by Theorem 1.1 and Theorem 1.2. The solid black line is $\delta = \epsilon$, and the dashed black line is $\delta = \epsilon/2$, so the region between is the region of parameters where (normal form) ToNC plausibly exists. The dark gray shade denotes the sub-region where we show that ToNC implies KA or OT (additionally assuming one-way functions for the latter). The blue curve is the key agreement threshold $\delta = (5\epsilon - 1)/4$, and the red curve is the oblivious transfer threshold $\delta = (\epsilon^2 + \epsilon)/2$. It remains open to show that ToNC in the white region below the solid black line implies KA or OT. However, we note that ToNC with *robust completeness* and any $\epsilon/2 \leq \delta < \epsilon$ implies KA, which is not reflected in the figure above.

Checking parameters for our running example of the compiled CHSH game where $\epsilon \approx 0.7$ and $\delta = 0.5$, we see that

$$0.5 < \frac{5(0.7) - 1}{4} \approx 0.63, \quad \text{and} \quad 0.5 < \frac{0.7^2 + 0.7}{2} \approx 0.6.$$

As another example, one can consider the compiled *magic square* game [CMM+26], which fits our definition of (ϵ, δ)-ToNC with $\epsilon = 1$ and $\delta = 0.5$. These are strictly better parameters than the compiled CHSH game and thus also fall in the range supported by our theorem statements.

Post-quantum hardness amplification. Our main results are obtained in two steps: (1) construct weak forms of BA and OT from ToNC, and (2) amplify the hardness of the BA or OT.

Even though our protocols utilize only classical communication, the honest parties may be quantum, and the adversaries of course may be quantum as well. Thus, we need *post-quantum* hardness amplification for BA and OT. While BA and OT amplification enjoys a long history of study in the purely classical setting, to the best of our knowledge there is no prior work that considers post-quantum hardness amplification for BA or OT.

We first consider post-quantum BA amplification. Here, the adversarial Eve receives a classical input (the transcript of the protocol) and applies a quantum circuit in an attempt to guess the shared bit. In the purely classical setting, Holenstein [Hol05] gave a tight amplification result,

establishing that (ϵ, δ)-BA implies fully-secure key agreement whenever $\delta < \frac{2\epsilon}{1+\epsilon}$. This is tight since (ϵ, δ)-BA exists unconditionally whenever $\delta \geq \frac{2\epsilon}{1+\epsilon}$ [Hol05].

This result was derived from a tight hard-core set theorem, improving on that of [Imp95], and stated roughly as follows. Consider any function f and predicate P such that for any polynomial-size classical circuit, $\Pr_{x\leftarrow\{0,1\}^n}[C(f(x)) = P(x)] \leq 1 - \frac{\delta}{2}$. Then there exists a set $S \subset \{0,1\}^n$ of density roughly δ such that C has very close to $1/2$ advantage on $x \leftarrow S$.

We give a post-quantum analogue of this tight hard-core set theorem. The fact that the predictor is now a quantum predictor requires modifying the proof of the original theorem, as well as slightly modifying the statement. We discuss these changes further in Section 2.3.

Theorem 1.3. *(Informal: Post-quantum hard-core measure) Let $\{D_\lambda\}_{\lambda\in\mathbb{N}}$ be any family of distributions over (x, b) that can be sampled in quantum polynomial time, such that $\max_{(x,b)}\{D_\lambda(x, b)\} = \mathrm{negl}(\lambda)$. If for any polynomial-size quantum circuit Q,*

$$\Pr_{(x,b)\leftarrow D_\lambda}[Q(x) = b] \leq \frac{1}{2} + \frac{\delta}{2},$$

then there exists a measure $M_\lambda \preceq D_\lambda$ of density roughly $1 - \delta$ such that

$$\Pr_{(x,b)\leftarrow M_\lambda}[Q(x) = b] \approx \frac{1}{2}.$$

By combining our post-quantum hard-core measure theorem with the techniques of [Hol05], we derive tight post-quantum key agreement amplification (the fact that this bound is tight is shown in [Hol05]).

Theorem 1.4. *For constants ϵ, δ, post-quantum (ϵ, δ)-BA secure against adversaries with non-uniform classical advice, implies post-quantum $(1, 0)$-BA if and only if*

$$\delta < \frac{2\epsilon}{1 + \epsilon}.$$

Next, we consider post-quantum OT amplification. Here, additional complications arise in the post-quantum setting due to the fact that the adversary is *interactive*, which we discuss in depth in Section 2.4.

Our main technique here is a sequential repetition theorem from which our OT amplification results can be derived, which can be seen as a post-quantum analogue of the "interactive XOR lemma" from [HR08, Lemma 3.1]. Informally, the theorem can be stated as follows.

Theorem 1.5. *(Informal: Post-quantum sequential XOR lemma) Consider any interactive protocol between a (potentially quantum) adversary and a classical challenger who obtains a private bit b at the end of interaction. Suppose that any QPT adversary has advantage at most δ in guessing b. Then, if we repeat the protocol ℓ times sequentially, no QPT adversary has advantage better than $\delta^\ell + \mathrm{negl}(\lambda)$ in guessing $\bigoplus_{i\in[\ell]} b_i$, where b_i is the challenger's (private) bit obtained in the i'th repetition.*

Even given the recent progress on parallel repetition in the (post-)quantum setting [BQSY24, HK25], the above theorem does not follow directly from prior work (see more discussion in Section 1.2). To prove it, we use Marriott-Watrous [MW04] style rewinding arguments to establish a post-quantum analogue of Levin's isolation lemma [Lev85, GNW11].

Finally, we use our sequential XOR lemma to amplify weak OT to fully-secure OT. For technical reasons, the first half of this amplification process only applies to a specialized form of OT we

define called "committed-bit OT" (Definition 3.8), which we build from ToNC. This technique amplifies $(\epsilon, \delta, 0)$ committed-bit OT to $(1, 1/2, 0)$ committed-bit OT for any $\delta < \epsilon^2$. The next part follows essentially directly from the sequential XOR lemma, and applies to any OT satisfying the standard game-based definition. That is, we prove the following theorem.

Theorem 1.6. *For any $\delta < 1$, post-quantum $(1, \delta, 0)$-OT implies post-quantum $(1, 0, 0)$-OT.*

Discussion. Our work is motivated by the apparent gap between the type of cryptography known to be sufficient for qubit tests (and related forms of classical verification) and the type of cryptography sufficient for weaker primitives such as tests of quantumness.

Starting with the work of [IR89], cryptographers have studied an often elucidating characterization of cryptographic primitives into two groups: (1) those that exist unconditionally in the random oracle model (sometimes called "minicrypt" primitives), and (2) those that *provably do not* exist unconditionally in the random oracle model (sometimes called "cryptomania" primitives). While the group (1) primitives can be heuristically instantiated with unstructured cryptography such as hash functions, group (2) primitives seem to require highly structured, e.g. algebraic, forms of cryptographic hardness.

While tests of quantumness are known to exist unconditionally in the (quantum) random oracle model [YZ24], and thus exist in group (1), we so far do not know such a result for qubit tests. Our work shows that (at least, in the parameter ranges covered by our theorem statements above) establishing qubit tests as a group (1) or "minicrypt" primitive would *also* establish classical-communication key agreement and oblivious transfer as minicrypt primitives. This would be a highly surprising result, for the following reasons. First of all, even though the study of (classical-communication) key agreement goes back to the earliest days of modern cryptography [DH76], there have been no candidates proposed from unstructured cryptography. This is partially explained by the result of [IR89], who showed that there is no black-box construction from one-way functions assuming that the honest parties and adversaries make only *classical* queries to the one-way function. Extending this result to the setting of quantum queries remains an open question, though there has been recent progress towards this goal [ACC+22, LLLL25].

In fact, current results suggest that qubit tests may require *more* structure than even classical-communication key agreement. For example, consider that injective trapdoor functions, which are known to imply key agreement, are not known to imply qubit tests. Instead, current constructions of qubit tests utilize *two-to-one* trapdoor functions, at the very least.

This situation can be partially explained by our result establishing that tests of non-commutation plus one-way functions imply oblivious transfer. Indeed, while injective trapdoor functions imply key agreement, they are black-box separated from oblivious transfer [GKM+00].[5] Thus, if one could build qubit tests from injective trapdoor functions (which trivially also imply one-way functions), this would yield classical-communication OT from injective trapdoor functions, which would be considered a very surprising result.

1.2 Related work

Proofs of quantum memory [HMOY25]. Recently, [HMOY25] introduced the notion of a proof of quantum memory (PoQM), which is a classical-communication protocol that occurs in two stages. After the first stage, there is a one-message challenge from the verifier that is answered by the prover. It has completeness α if there exists a prover that can cause the verifier to accept with

[5] Again, note that this result only considers honest parties and adversaries that make classical queries to the primitives, and the quantum-query case remains open

probability α, and it has soundness β if any prover that maintains only *classical* memory between stages can cause the verifier to accept with probability at most β.[6]

PoQM is, in general, a less structured primitive than ToNC. For example, it is not hard to see that (normal form) (ϵ, δ)-ToNC implies PoQM with completeness $\frac{1}{2}+\frac{\epsilon}{2}$ and soundness $\frac{1}{2}+\frac{\delta}{2}$, as well as "extraction probability" $\frac{1}{2}+\frac{\epsilon}{2}$, which refers to the probability that the verifier can predict the prover's final message. Moreover, [HMOY25] establish that PoQM with (1) extraction probability $1-1/\mathrm{poly}$ and, (2) a $1/\mathrm{poly}$ gap between completeness and soundness, implies (fully-secure) classical-communication key agreement. Thus, our result that $(1, \delta)$-ToNC implies KA for any $\delta < 1$ can also be achieved by an alternate route that goes through PoQM.

However, the majority of our results do not follow from [HMOY25]. This includes our constructions of KA from (ϵ, δ)-ToNC for any setting of $\epsilon < 1$ (covering important examples such as the compiled CHSH game), as well as all of our constructions of OT from ToNC (plus one-way functions), explaining the lack of approaches to building ToNC from weaker forms of asymmetric cryptography such as plain trapdoor functions.

Oblivious state preparation [BK25]. Recently, [BK25] introduced the notion of oblivious state preparation (OSP), which is a classical-communication protocol that allows a client to prepare a BB84 quantum state in the server's memory in such a manner that the server has negligible advantage in determining whether it is in the standard or Hadamard basis. They show that OSP implies both (classical-communication) key agreement and OT.[7]

OSP is a stronger primitive than ToNC: While OSP is known to imply $(2\cos^2(\pi/8)-1, 0.5)$-ToNC [BK25] by compiling the CHSH game, the reverse direction is not known. Whether we can obtain (some form of) OSP from ToNC is an interesting question, though appears somewhat difficult.

Foundations of interactive quantum advantage [TZ25]. In another recent work, [TZ25] study the cryptographic implications of verifiable quantum advantage. Their result most relevant to this work establishes that there is no construction of constant-round interactive quantum advantage from the black-box use of indistinguishability obfuscation and one-way permutations. Since constant-round (ϵ, δ)-ToNC immediately implies constant-round quantum advantage for any $\delta < \epsilon$, this establishes the same for any non-trivial constant-round ToNC. Our results differ from theirs in the following ways:

- Our cryptographic implications of ToNC apply to ToNC with any number of rounds, and are not limited to black-box constructions of ToNC.
- Our results give evidence that ToNC cannot be constructed from random oracles, while [TZ25]'s results do not rule out the possibility that ToNC can be constructed from collision-resistant hashing (which exists in the random oracle model).

(Post-)quantum parallel repetition [BQSY24, HK25]. A couple of recent works have ushered in the study of hardness amplification in the post-quantum and quantum settings, in particular when protocols are *parallel* repeated. However, as we discuss further in Section 2, these results do not have implications to post-quantum key agreement and oblivious transfer amplification, for the following reasons. [HK25] focus primarily on *public-coin arguments*, where the job of the adversary

[6] They also consider a more general variant, where there is a number of qubits of memory that suffice for completeness, and a fewer number of qubits for which the soundness bound holds.

[7] In fact, they require one-way functions as well to obtain the notion of OT that we consider in this paper.

is to *convince the verifier to accept*, as opposed to guess a hidden bit known to a private-coin challenger. While they do have a private-coin result, it is limited to three-message protocols. [BQSY24] focus on *three-message, quantum-communication* protocols (they also have a round-compression theorem for quantum-communication arguments, but this does not apply to classical-communication protocols). While they do derive a quantum analogue of Yao's XOR lemma, it does not apply to the classically-interactive private-coin setting that we require for OT amplification.

1.3 Open problems

Our work motivates several directions for future research, which we outline here.

1. Can we tighten our implications from ToNC to key agreement and OT? For example, there exists a region of $\delta < \epsilon$ for which we don't know how to derive OT from (ϵ, δ)-ToNC. Moreover, can we hope to remove the reliance on one-way functions and establish OT from ToNC unconditionally?

2. As mentioned earlier, our BA amplification techniques only apply to adversaries with non-uniform classical advice, while our OT amplification techniques only apply to adversaries with non-uniform quantum advice. Can we give post-quantum BA and OT amplification for *both* types of advice? Can we give post-quantum BA and OT amplification in the *uniform* setting?

3. Can we continue to improve our understanding of the relationships between PoQM, ToNC, OSP, and OT? For example, does some variant of ToNC imply OSP? Does OT imply ToNC, or is there a separation? One current gap between what is known about OT vs. ToNC is the fact that trapdoor permutations are known to imply OT, but not known to imply ToNC.

4. In this work, we consider ToNC where the prover's final-round strategy consists of *binary-outcome observables*. While this is a natural setting, one could consider a more general type of protocol where the prover's final-round strategy outputs a string of bits as opposed to a single bit. In fact, this is the setting considered by the original qubit test protocol of [BCM+21]. Can we show cryptographic implications from such multi-bit answer ToNCs?

5. As we are the first to study post-quantum hardness amplification for key agreement and OT, several questions remain. For example, can we derive more general amplification results for OT? Such results would presumably extend the parameter regime in which our construction of OT from ToNC remains valid. Additionally, are there other applications of our post-quantum hard-core measure theorem or post-quantum interactive XOR lemma?

2 Technical overview

In this overview, we will first cover our constructions of weak bit agreement (BA) and weak oblivious transfer (OT) from tests of non-commutation (ToNC), and proceed to discuss our post-quantum hardness amplification techniques.

Normal-form ToNC. Recall from the previous section that we work with a notion that we call "normal-form" ToNC. In such a ToNC, the interaction between quantum prover and classical verifier always reaches a final stage where the prover receives a challenge bit c and the verifier obtains a (private) answer bit a^*. The prover then applies one of two binary observables P_0 or P_1 to its state

$|\psi\rangle$, depending on the choice of c, to obtain an answer a. We say that the prover has ϵ advantage if $\Pr[a = a^*] = \frac{1}{2} + \frac{\epsilon}{2}$.

In Section 4.2, we show that a more-general variant of ToNC (where the verifier may sometimes accept both or neither possible answers) can be compiled into normal-form ToNC with the same completeness-soundness gap. Hence, in the remainder of this section, we will focus on building cryptography from normal-form ToNC.

2.1 Weak BA from ToNC

It turns out that (normal-form) ToNC can essentially already be seen as a weak bit agreement between prover and verifier. Indeed, suppose that the prover computes a but keeps it private. Then we have that the prover and verifier agree on a bit $a = a^*$ with advantage ϵ.

Now consider an eavesdropper E who may observe the (classical) transcript τ of interaction between the prover and verifier, and suppose that they are able to guess the value of a^* with advantage γ (meaning probability $\frac{1}{2} + \frac{\gamma}{2}$). Since the transcript τ is disjoint from the prover's state $|\psi\rangle$, such an E can be used to derive a *commuting* strategy with advantage $\frac{\epsilon+\gamma}{2}$. In particular, consider a prover that, prior to seeing the final challenge bit c, flips a random coin $b \leftarrow \{0, 1\}$. If $b = c$, it runs the honest prover strategy on its final state $|\psi\rangle$ while if $b = 1 - c$, it runs E on the classical transcript of the protocol. Such a prover is commuting by inspection and has advantage exactly $\frac{\epsilon+\gamma}{2}$.

Now, suppose we start with a (ϵ, δ)-ToNC according to the definition provided in the previous section (and formally in Definition 4.1 and Definition 4.2). Then we obtain a bit agreement protocol with correctness advantage ϵ, and where any E has advantage at most $2\delta - \epsilon$ in guessing the verifier's bit (call her Alice). Due to technical reasons in the ensuing bit agreement amplification, we care in particular about E's advantage *conditioned* on Alice and Bob outputting the same bit. Thus, the best *conditional* advantage bound we can derive comes out to

$$\delta' = \frac{1 + 4\delta - 3\epsilon}{1 + \epsilon},$$

yielding a (ϵ, δ')-BA protocol for such δ' according to the definition given in the previous section (and formally in Definition 3.5). The formal protocol and analysis are given in Section 5.1.

2.2 Weak OT from ToNC

Next, we discuss our construction of weak OT from ToNC. Building OT presents several complications that did not arise in the construction of BA. For instance, the adversary *actively* participates (potentially maliciously) in the protocol. Moreover, to prepare for our OT amplification step, we will actually build a stronger notion of OT than what was presented in the previous section, which we call committed-bit OT.

Skeleton protocol. In this overview, we give a sense of the core of our idea by presenting a bare-bones OT protocol that works only if several conditions are satisfied. In the body, we utilize techniques such as cryptographic commitments (which introduces an additional assumption of one-way functions), cut-and-choose, and random-termination to "compile" the skeleton protocol into a full-fledged committed-bit OT. However, the main intuition can be appreciated with the following skeleton, which uses a (normal-form) (ϵ, δ)-ToNC.

- Let the OT sender be the verifier and the OT receiver be the prover in two runs of the ToNC. That is, run

$$|\psi_0\rangle, c_0, a_0^* \leftarrow \langle P_{\mathsf{Prep}}(1^\lambda), V_{\mathsf{Prep}}(1^\lambda)\rangle, \quad |\psi_1\rangle, c_1, a_1^* \leftarrow \langle P_{\mathsf{Prep}}(1^\lambda), V_{\mathsf{Prep}}(1^\lambda)\rangle.$$

  However, the sender (verifier) does not send (c_0, c_1) to the receiver (prover) yet.

- The receiver samples $c_{R,0}, c_{R,1} \leftarrow \{0,1\}$ and computes answers

$$a_{R,0} \leftarrow P_{c_{R,0}}(|\psi_0\rangle), \quad a_{R,1} \leftarrow P_{c_{R,1}}(|\psi_1\rangle).$$

- The receiver sends $c_{R,0} \oplus c_{R,1}$ and the protocol only continues if $c_{R,0} \oplus c_{R,1} \neq c_0 \oplus c_1$. In this case, the sender sends c_0, c_1 to the receiver and outputs $r_0 = a_0^*$ and $r_1 = a_1^*$ as its OT bits.

- The receiver sets b to be the unique bit such that $c_{R,b} = c_b$, and sets $r = a_{R,b}$.

First, note that if the receiver uses the honest prover strategy, then $r = r_b$ with advantage ϵ, as in this case the challenge $c_{R,b}$ it used to produce $a_{R,b}$ was the same as the verifier's challenge c_b.

Next, note that receiver security is optimal: The sender learns nothing about the receiver's bit b since it learns $c_{R,0} \oplus c_{R,1}$ but neither bit individually.

Finally, it remains to prove a bound on the advantage that the (potentially adversarial) receiver has in guessing r_{1-b}.

Enforcing good behavior. We say that an adversarial receiver is "well-behaved" if (1) its advantage in guessing $a_{R,b} = a_b^*$ is indeed (roughly) ϵ, (2) $c_{R,0}, c_{R,1}$ are chosen uniformly at random, and (3) it honestly reports the value of $c_{R,0} \oplus c_{R,1}$. In the full protocol, we enforce that the receiver is well-behaved by using a coin-flipping protocol to sample $c_{R,0}, c_{R,1}$, having the receiver commit to its challenges $c_{R,0}, c_{R,1}, c_{R,0} \oplus c_{R,1}$ and answers $a_{R,0}, a_{R,1}$, and running a cut-and-choose plus random-termination strategy that repeats the protocol and requires them to open all but one of these sets of commitments.

Reduction to ToNC. Now, we argue that any well-behaved receiver with advantage γ in guessing r_{1-b} implies a *commuting* prover strategy in the ToNC with advantage roughly $\frac{\epsilon+\gamma}{2}$. To see this, consider a prover $\widetilde{P}$ that utilizes the well-behaved receiver as follows. $\widetilde{P}$ simulates the receiver's interaction with the sender in two ToNC executions except that it performs the verifier itself in one of them, and forwards messages to its own verifier in the other. Which one is forwarded to the "real" verifier will be chosen uniformly at random, but for the sake of discussion let's say protocol 0 is forwarded and protocol 1 is simulated in $\widetilde{P}$'s head.

Condition on $c_{R,0} \oplus c_{R,1} \neq c_0 \oplus c_1$ and let b be such that $c_{R,b} = c_b$. If $b = 0$, then we know the receiver's answer $a_{R,b}$ will yield advantage ϵ in predicting the verifier's bit a^*, so $\widetilde{P}$ will return $a_{R,b}$ to its verifier. Otherwise, if $b = 1$, then we know that the receiver's guess for $r_{b-1} = r_0$ has advantage γ in predicting the verifier's bit a^*, so $\widetilde{P}$ will return its guess for r_{b-1} instead. Since $c_{R,0}, c_{R,1}$ are random, and we randomize the choice of which of the two protocols are forwarded to the verifier, both cases happen with probability exactly $1/2$, yielding an overall advantage of $\frac{\epsilon+\gamma}{2}$. By soundness of the ToNC, we have that $\frac{\epsilon+\gamma}{2} < \delta$, and thus $\gamma < 2\delta - \epsilon$.

Using non-uniformity. This is the main idea that underlies our result that (ϵ, δ)-ToNC implies $(\epsilon, 2\delta - \epsilon, 0)$ (committed-bit) OT. However, before moving on, we point out one complication that arises in the above strategy. On the one hand, $\widetilde{P}$ actually has to *learn* the values $c_{R,0}, c_{R,1}, a_{R,0}, a_{R,1}$ used by the adversarial receiver in the OT protocol, but on the other hand, these cannot be revealed in the transcript as they may leak the receiver's choice bit. To remedy this, we have the receiver *commit* to these values and then have $\widetilde{P}$ *extract* them in the reduction. As we use only one-way functions for the commitment, this extraction procedure is not efficient. However, it turns out that we can push all of the inefficiency required to *before* the beginning of the ToNC protocol, and have $\widetilde{P}$ make use of non-uniformity to perform an inefficient operation before the beginning of the protocol. Thus, our final result is actually that (ϵ, δ)-ToNC secure against adversaries with non-uniform (potentially quantum) advice implies $(\epsilon, 2\delta - \epsilon, 0)$ (committed-bit) OT. The formal protocol and analysis are given in Section 5.2.

2.3 BA amplification

In the remainder of the paper, we prove amplification theorems for BA and OT in the post-quantum setting. That is, we address the setting where adversaries and the communicating parties are quantum (rather than classical) polynomial-time machines. Due to structural differences between BA and OT, we were compelled to take different amplification routes for each. We begin by describing at a high level how we amplify weak BA into full-fledged key agreement, presented in Section 6.1 and Section 6.2.

The classical setting. Our starting point is Holenstein's tight classical amplification theorem [Hol05], which characterizes exactly when weakly-secure BA can be amplified to fully-secure key agreement. We briefly recall the classical approach and then explain the modifications needed in our (post-quantum) setting.

Secure random variables. Following Holenstein, we consider the notion of an *information-theoretically* secure weak BA, where a single execution produces correlated bits (X, Y) for Alice and Bob, together with side information Z held by Eve – namely, the transcript. One says that (X, Y, Z) is an (ϵ, δ)-*secure random variable* if (i) X and Y are unbiased, (ii) $\Pr[X = Y] \geq \frac{1}{2} + \frac{\epsilon}{2}$, and (iii) there exists an event E that implies $X = Y$ such that $\Pr[E \mid X = Y] \geq \delta$ and $I(X; Z \mid E) = 0$. That is, conditioned on E, Eve's view gives *no information* about the shared bit. Definition 6.10 formalizes this notion.

An information-theoretic amplification protocol. Given ℓ independent (ϵ, δ)-secure random variables, Holenstein gives an efficient protocol that compiles them into a perfect (up to negligible factors) secure random variable – and hence fully-secure key agreement, assuming the following condition on (ϵ, δ) holds:

$$\delta > \frac{1 - \epsilon}{1 + \epsilon}.$$

It is now left to show that applying such a compilation protocol to multiple independent *computationally-secure* weak BA instances results in a fully-secure BA instance. To do so, Holenstein proves a variant of Impagliazzo's hard-core set lemma against non-uniform classical circuits, with improved parameters [Hol05, Lemma 2.1]. Let us state it in terms of bit agreement for the sake of discussion.

Hard-core set lemma. Fix some arbitrarily small constant $\gamma > 0$, and suppose that any adversarial circuit of size s given the communication transcript can succeed in guessing the output bit (conditioned on the parties agreeing on the same bit) with probability at most $1 - \delta/2$. Then, there exists a set S of transcripts whose total mass depends on δ, s, such that when sampling a weak BA instance from S, all circuits of size somewhat smaller than s succeed in guessing the agreed bit (conditioned on agreement) with probability at most $\frac{1+\gamma}{2}$.

Amplification in the (classical) computational security setting. The amplified protocol works exactly as in the information-theoretic case.

1. The parties perform $\ell(\lambda) = \mathrm{poly}(\lambda)$ independent instances of the weak computationally-secure BA protocol, producing pairs of bits $(x_i, y_i)_{i=1,\ldots,\ell}$.
2. They run the compilation protocol on $(x_i, y_i)_{i=1,\ldots,\ell}$, producing final output bits k_A, k_B.

Using the hard-core set lemma, one proves that any potential adversary attempting to break the amplified protocol over weak computationally-secure BA instances, cannot do significantly better than it would on a series of information theoretic (ϵ, δ)-secure random variables.

Indeed, given a hard-core set S, define the event E to be "the transcript corresponds to $x \in S$ and the parties output the same bit". Conditioned on E, the weak BA transcript z carries essentially no efficiently-computable information about the shared bit $x = y$, so for the computationally-bounded adversary, the triplet (x, y, z) is indistinguishable from an information-theoretically secure $(\epsilon, \delta_{\mathrm{sec}})$-secure random variable, with $\delta_{\mathrm{sec}} \approx \Pr[E \mid X = Y]$. The proof is completed using an appropriate hybrid argument.

Moving to the quantum setting. It turns out that given an appropriate post-quantum analogue of the hard-core set lemma, the BA amplification works using an argument similar to that described above. So we will focus on the hard-core set lemma itself. In particular, our goal is to re-prove it in the setting where the adversary can apply a quantum circuit rather than a classical circuit.

The approach laid out by [Hol05, HS11] for proving the hard-core set lemma in the classical setting, consists of two main steps.

- **A hard set for each predictor.** Assume that no efficient adversary can guess the output bit of the protocol from the communication transcript with probability better than $1 - \delta/2$, conditioned on agreement. Then for any fixed predictor Q and any slack $\gamma \in (0, \delta)$, there is a set of transcripts of mass at least $\delta - \gamma$ on which Q has essentially no advantage, i.e. its success is at most $1/2 + \gamma/2$.
- **Per-set predictors $\Rightarrow$ one universal predictor.** Now suppose that for every large set there exists *some* adversary of size s that computes the output bit with noticeable advantage γ on that measure. Then one can "fix" the predictor: There exists a *single* predictor (with a moderate size blowup) that achieves advantage better than $\gamma/2$ *simultaneously on all* sets of mass at least δ. This contradicts the previous item.

Together, these two components imply the existence of a hard-core set on which *all* predictors of size s have advantage close to $1/2$. The key component in the proof of the second step is von Neumann's minimax theorem, which translates to the setting of quantum circuits without requiring significant adaptations. In what follows, we describe how we adapt the proof of the first step in some more detail.

A hard *measure* for any quantum predictor. Fix a deterministic predicate $P : \{0,1\}^n \to \{0,1\}$ and any randomized classical circuit $C(x, b)$ that is intended to output 1 when $b = P(x)$ and 0 otherwise. Theorem 3 in [HS11] (which is similar in spirit to Lemma 2.4 from [Hol05]) shows that one can *decompose* the input space relative to this particular C into a large "hard" subset of the domain $S \subseteq \{0,1\}^n$ of probability mass δ and its complement. That is, on S, C's acceptance probability is essentially *insensitive* to whether $b = P(x)$ or $b = 1 - P(x)$, meaning that flipping P on S is nearly indistinguishable to C. Moreover, one can convert C into an explicit predictor Q that recovers $P(x)$ with an overall success at least $1 - \delta/2$ on the entire domain.

In the classical hard-core set proof, the first component is a statement of the form: *given a fixed predictor A, there exists a large region on which A has only tiny advantage.* The above decomposition can be used as an alternative route to such a statement, as follows. Define a distinguisher $C_A(x, b)$ that outputs 1 iff $A(x) = b$. Applying the decomposition to C_A yields a set S where C_A cannot reliably distinguish $b = P(x)$ from $b = 1 - P(x)$, which exactly means that on $x \leftarrow S$, the predictor A has success close to $1/2$. Moreover, under the *assumed global hardness* parameter δ (namely, no predictor can achieve success $\geq 1 - \delta/2$ overall), the theorem's predictor Q forces the extracted set S to have density at least about δ – otherwise Q would contradict hardness.

Our Theorem 6.1 is a generalization of Theorem 3 in [HS11], which differs in several respects:

- **Quantum circuits.** We allow the distinguisher C to be a *quantum* circuit, and thus the resulting predictor Q is quantum.
- **Arbitrary input distributions.** Rather than working only with the uniform distribution over $\{0,1\}^n$, we formulate the statement with respect to an arbitrary distribution $\mathcal{D}$ over inputs. This enables applying the theorem to the case of bit agreement protocols, where the distribution over communication transcripts is typically not uniform. We note that in the classical case, one can often utilize the uniform distribution over the participant's random coins, thus avoiding the necessity of generalizing the distribution. However, this is not possible if the participants are quantum.
- **A hard measure rather than a hard set.** As a consequence of allowing a quantum distinguisher C, we construct a quantum predictor which maps a pair $(x, P(x))$ *probabilistically* to a bit. Since the predictor is non-deterministic, it does not immediately give rise to a hard subset. Instead, its prediction statistics constitute a *sub-distribution measure* of $\mathcal{D}$ that designates the portion of the domain on which C is insensitive to flipping P. The measure is explicitly constructed in Corollary 6.3.

The measure vs. set discrepancy comes from the fact that the proof in [HS11] relies on derandomizing the distinguisher C through fixing a set R of random seeds. Evaluations of $C(x, r)$ on any $r \in R$ are used to compute a criterion which determines whether $x \in S$—thus S becomes a deterministic set. This perspective breaks down in the quantum setting, where the distinguisher's behavior is inherently probabilistic and cannot be derandomized in the same manner. Instead, the hard region is represented by a weight function $w(x) \in [0, 1]$ derived from the prediction statistics of the quantum distinguisher, yielding a sub-distribution $M \preceq D$. Consequently, the remainder of the amplification argument is reformulated so that Holenstein's hard-core-set reasoning continues to hold when the hard object is a weighted measure rather than a deterministic subset.[8]

A further subtlety is that the weak-BA distribution is not necessarily a deterministic predicate. After conditioning on the two parties agreeing on the same bit, we obtain a distribution over

[8] As mentioned before, [Hol05]'s proof also relied on a randomness fixing argument, though we found [HS11]'s approach easier to adapt to the quantum setting while maintaining optimal parameters.

transcript/bit pairs (Z, X). To apply a predicate-style hard-core theorem, we lift the domain to (Z, b_0), where b_0 is the agreed-upon bit, and define the deterministic predicate $P(Z, b_0) = b_0$. Given a transcript predictor $C(Z)$, we form a distinguisher $C((Z, b_0), b)$ that ignores b_0 and checks whether $C(Z) = b$. The obliviousness of the predictor returned by our decomposition theorem is essential for using weak BA security to prove a hard-core measure: if the hard-core measure has too little mass, the resulting predictor on the lifted domain collapses back to a predictor of X from Z, contradicting weak-BA security.

Lemma 6.6 establishes the minimax fixing step needed for the hard-core measure theorem, which appears as Theorem 6.7. Theorem 6.13 establishes the generic amplification statement with a hybrid argument, and Theorem 6.9 states that the amplifiable parameter range in the quantum setting is identical to Holenstein's tight result in the classical setting.

2.4 OT amplification

Finally, we discuss our approach to post-quantum OT amplification, which requires a new set of techniques, presented in Section 6.3 and Section 6.4.

New challenges. The fundamental differences with BA amplification stem from the fact that the adversary participates in the protocol itself. That is, one must consider the "input" of the weakly hard distinguishing problem to be the *quantum state* produced at the end of the protocol, as opposed to just the classical transcript. Moreover, as we allow the adversary to be malicious,[9] it may influence the generation of this (transcript, state) pair.

While hard-core set theorems have been applied successfully to obtain (semi-honest)[10] OT amplification in the purely classical setting [Wul07], the fact that we must consider *quantum* inputs now prevents us from applying the techniques from last section.[11] Instead, we prove a novel post-quantum XOR lemma that applies to classical-communication interactive protocols, and put it to work to obtain our OT amplification results.

Interactive XOR lemma. The interactive XOR lemma can be motivated by considering the following desired form of OT amplification. Suppose we have a $(1, \delta, 0)$-OT protocol (according to the definition given in Section 1.1 and formally in Definition 3.6) for some constant $\delta < 1$, and our goal is to obtain fully-secure OT, i.e. (1,0,0)-OT. A natural idea is to repeat the protocol λ times sequentially, instructing the sender to XOR together their bits across runs. That is, letting $\{r_{i,0}, r_{i,1}\}_{i\in[\lambda]}$ be the set of sender bits obtained from the λ repetitions, we know that any adversarial receiver has δ advantage in guessing each $r_{i,0} \oplus r_{i,1}$, and it is natural to conjecture that any adversarial receiver thus has $\delta^\lambda = \mathrm{negl}(\lambda)$ advantage in guessing $\bigoplus_{i\in[\lambda]} r_{i,0} \oplus r_{i,1}$. Crucially, note that we are not asking that the receiver make a guess for each $r_{i,0} \oplus r_{i,1}$ directly after the i'th repetition of the protocol (in which case it would be trivial to show that all guesses are correct

[9] One might wonder about the possibility of post-quantum *semi-honest* OT amplification, where both the honest and adversarial participants are quantum but the communication is classical. This appears to be a bit tricky to reason about; in particular, the accepted model of quantum semi-honest adversaries allow them to *purify* their actions in the protocol [DNS10], resulting in an interaction that now involves quantum communication. We believe that several of the non-trivialities involved in the setting of malicious post-quantum amplification would also arise in any reasonable semi-honest quantum model, and thus we focus on the malicious case.

[10] In the classical setting, semi-honest amplification is sufficient, since maliciously-secure OT follows generically from semi-honest OT [GMW87, Kil88]. No such semi-honest to malicious compiler is known in the quantum setting.

[11] One might wonder about the possibility of obtaining some analogue of a hard-core measure for distributions over quantum states, but we leave this possibility to future work (and indeed, are not convinced that reasonable formulations of this statement are possible).

with probability at most δ^λ), but are rather asking that they guess a single bit at the end of all λ repetitions.

A useful abstraction of this setting can be phrased as follows. Suppose we have a protocol Γ that takes place between a (potentially quantum) adversary A and a classical verifier V, who obtains an output $b \in \{0,1\}$ at the end of the protocol. Let δ be the maximum advantage that any A can obtain in guessing the verifier's output b. Then, if we sequentially repeat the protocol twice, letting b_1 and b_2 denote the two verifier outputs, the maximum advantage that any A can obtain in guessing $b_1 \oplus b_2$ is $\delta^2 + \mathrm{negl}(\lambda)$. Note that in the full statement (Theorem 6.16), we allow for different protocols Γ_1, Γ_2 with different advantage bounds δ_1, δ_2.

In fact, this is precisely the post-quantum analogue of a classical claim due to Halevi and Rabin [HR08, Lemma 3.1], which itself is an interactive analogue of Levin's Isolation Lemma [Lev85], as stated in [GNW11]. Unfortunately, the classical proof makes heavy use of rewinding, which is non-trivial and sometimes impossible in the quantum setting. However, the core rewinding idea *has* been adapted to the quantum setting in a recent work of [BQSY24], though we note that their theorems do not directly apply to our setting as they are stated for three-message parallel-repeated quantum-communication protocols. We proceed to give an overview of our proof technique, which is somewhat related to [BQSY24], but ultimately different and self-contained.

Proof technique. For convenience, let's move to the $\{+1,-1\}$ basis for classical bits, and suppose that the adversary's output is $b_A \in \{+1,-1\}$, while the two verifier outputs are $b_1, b_2 \in \{+1,-1\}$. Then, for contradiction, we assume the existence of an adversary A such that

$$\mathbb{E}[b_A \cdot b_1 \cdot b_2] > \delta^2.$$

Rearranging, we have that

$$\mathbb{E}[b_1 \cdot \mathbb{E}[b_A \cdot b_2 \mid |\psi\rangle]] > \delta^2 \quad \Rightarrow \quad \mathbb{E}\left[b_1 \cdot \mathbb{E}\left[\frac{b_A \cdot b_2}{\delta} \;\middle|\; |\psi\rangle\right]\right] > \delta,$$

where $|\psi\rangle$ is the intermediate state that A has between the executions of Γ_1 and Γ_2. By security of Γ_2 we know that for any such $|\psi\rangle$, it holds that

$$-\delta \leq \mathbb{E}[b_A \cdot b_2 \mid |\psi\rangle] \leq \delta.$$

This suggests the following strategy for breaking security of the *first* protocol:

1. Run the first stage of A until it finishes interacting with Γ_1 and produces state $|\psi\rangle$.
2. Use $|\psi\rangle$ to obtain a real number $\alpha \in [-\delta, \delta]$ whose expectation is distributed identically to $\mathbb{E}[b_A \cdot b_2]$.
3. Output $b_A \in \{1,-1\}$ sampled as a Bernoulli random variable which takes the value 1 with probability $\frac{1}{2}(\frac{\alpha}{\delta} + 1)$.

The only step that is potentially problematic in the quantum setting is (2). Indeed, in the classical setting, this is accomplished by repeatedly simulating executions with Γ_2 and estimating the probability of success. Note that it does *not* suffice to run a single execution, as this would output a value in $\{+1,-1\}$ which has the correct expectation but is not within the range $[-\delta, \delta]$ required to get step (3) to work.

Fortunately, Marriott-Watrous [MW04] style rewinding applied to $|\psi\rangle$ allows us to implement step (2). Indeed, alternating the projector Π_0 corresponding to initializing the verifier for Γ_2 and

the projector Π_1 corresponding to running the interaction and checking whether $b_A = b_2$ allows us to (approximately) sample from a distribution with the correct expectation *and* the correct support. However, to prove that the distribution is supported on $[-\delta, \delta]$, we must actually assume that Γ_2 is secure against adversaries with non-uniform *quantum* advice. In particular, this guarantees that the eigenvalues of $\Pi_0\Pi_1\Pi_0$ all fall in the range $[-\delta, \delta]$. Indeed, Marriott-Watrous (approximately) samples from a distribution supported only on eigenvalues, and thus the output α will be in $[-\delta, \delta]$ (with high probability).

Completing OT amplification. Recursively applying the interactive XOR lemma allows us to prove our motivating example, that $(1, \delta, 0)$-OT implies $(1, 0, 0)$-OT for any $\delta < 1$.[12] While this result is already of inherent interest, it does not suffice to complete our desired implications from ToNC. In particular, if the ToNC does not have completeness 1 (e.g. the compiled CHSH game), then we obtain some $(\epsilon, \delta, 0)$ for both $\epsilon < 1$ and $\delta < 1$.

To boost correctness of $(\epsilon, \delta, 0)$-OT, we adapt an approach of [Wul07] establishing that for any $\delta < \epsilon^2$, *classical semi-honest* $(\epsilon, \delta, 0)$-OT implies *classical semi-honest* $(1, \delta', 0)$-OT for some $\delta' < 1$. The approach involves two steps:

1. Boost security by applying a sequential XOR lemma (which also brings correctness down with it). We already have the tool for analyzing this.
2. Boost correctness by repeating the protocol several times with the *same* input bits from each party.

In step (2), it is imperative for security that the receiver indeed uses the same choice bit b in each execution. While this holds by definition in the classical semi-honest model, we have to somehow enforce that our quantum malicious receiver exhibits this behavior. To do so, we rely on another layer of cut-and-choose, utilizing the fact that our weak OT protocol is in fact a "committed-bit" OT. This means that after the protocol has completed, the receiver can *open* the interaction to its choice bit b, convincing the sender that it indeed used this b during the interaction. This allows us to implement step (2) securely, and we thus establish that $(\epsilon, \delta, 0)$ committed-bit OT implies $(1, 1/2, 0)$-OT for any $\delta < \epsilon^2$.

3 Preliminaries

Let λ be the security parameter. By default, we consider non-uniform families of quantum adversaries, but the *type* of non-uniformity will vary. In particular, we will sometimes consider adversaries with non-uniform *classical* advice, given by $\{Q_\lambda\}_{\lambda\in\mathbb{N}}$, and sometimes consider adversaries with non-uniform *quantum* advice, given by $\{\rho_\lambda, Q_\lambda\}_{\lambda\in\mathbb{N}}$. In both cases, we will often suppress the parameterization over λ and write just Q or ρ, Q.

Definition 3.1 (Sub-distribution measure)**.** *Let Ω be a finite set. A* sub-distribution *(equivalently, a* sub-probability measure*) on Ω is a function $M : \Omega \to [0, 1]$ such that its* total mass

$$\mu(M) \ := \sum_{\omega\in\Omega} M(\omega)$$

satisfies $\mu(M) \leq 1$. If $\mu(M) > 0$, we write $\omega \leftarrow M$ to denote sampling from the normalized distribution $M/\mu(M)$, i.e.,

$$\Pr[\omega = \omega_0] \ = \ \frac{M(\omega_0)}{\mu(M)} \qquad (\omega_0 \in \Omega).$$

[12] In fact this also establishes that $(1, 0, \delta)$-OT implies $(1, 0, 0)$-OT by first applying a standard OT reversal.

Given a distribution D on Ω, we write $M \preceq D$ if $M(\omega) \leq D(\omega)$ for all $\omega \in \Omega$.

Theorem 3.2 (von Neumann's minimax theorem [vN28])**.** *Let $\mathcal{A}$ be a finite set, let $Y \subseteq \mathbb{R}^d$ be a nonempty compact convex set, and let $u : \mathcal{A} \times Y \to \mathbb{R}$ be such that $u(a, \cdot)$ is affine on Y for every $a \in \mathcal{A}$. Write $\Delta(\mathcal{A})$ for the simplex of distributions over $\mathcal{A}$, and define $\bar{u}(p, y) := \mathbb{E}_{a\sim p}[u(a, y)]$. Then*

$$\min_{y\in Y} \max_{a\in\mathcal{A}} u(a, y) \;=\; \max_{p\in\Delta(\mathcal{A})} \min_{y\in Y} \bar{u}(p, y).$$

In particular, there exists $p^\star \in \Delta(\mathcal{A})$ such that for all $y \in Y$, $\bar{u}(p^\star, y) \;\geq\; \min_{y'\in Y} \max_{a\in\mathcal{A}} u(a, y')$.

3.1 Cryptographic primitives

Definition 3.3 (Inefficiently-extractable commitment)**.** *An inefficiently-extractable commitment between a classical committer and classical receiver consists of an interaction*

$$\mathsf{st}_{\mathsf{Com}}, \tau \leftarrow \langle \mathsf{Com}(1^\lambda, b), \mathsf{Rec}(1^\lambda)\rangle,$$

where $\mathsf{st}_{\mathsf{Com}}$ is the private state of the committer, and τ is the public transcript of interaction produced by the protocol, along with a PPT algorithm

$$\mathsf{Ver}(\mathsf{st}_{\mathsf{Com}}, \tau, b) \to \{\top, \bot\}.$$

It should satisfy the following properties.

- ***Correctness**: for any $b \in \{0, 1\}$,*

$$\Pr\left[\mathsf{Ver}(\mathsf{st}_{\mathsf{Com}}, \tau, b) = \top : \;\; \mathsf{st}_{\mathsf{Com}}, \tau \leftarrow \langle \mathsf{Com}(1^\lambda, b), \mathsf{Rec}(1^\lambda)\rangle \;\right] = 1 - \mathrm{negl}(\lambda).$$

- ***Hiding**: For any QPT adversarial receiver ρ, $\widetilde{\mathsf{Rec}}$ outputting a bit $\widetilde{b}$,*

$$\left|\Pr\left[\widetilde{b} = 0 : \widetilde{b} \leftarrow \langle \mathsf{Com}(1^\lambda, 0), \widetilde{\mathsf{Rec}}(\rho)\rangle\right] - \Pr\left[\widetilde{b} = 0 : \widetilde{b} \leftarrow \langle \mathsf{Com}(1^\lambda, 1), \widetilde{\mathsf{Rec}}(\rho)\rangle\right]\right| = \mathrm{negl}(\lambda).$$

- ***Binding:** There exists a (potentially inefficient) function Ext such that for any unbounded adversarial committer $\widetilde{\mathsf{Com}}$,*

$$\Pr\left[\mathsf{Ver}(\widetilde{\mathsf{st}}_{\mathsf{Com}}, \tau, 1 - b) = \top : \begin{array}{r} \widetilde{\mathsf{st}}_{\mathsf{Com}}, \tau \leftarrow \langle \widetilde{\mathsf{Com}}, \mathsf{Rec}(1^\lambda)\rangle \\ b := \mathsf{Ext}(\tau) \end{array}\right] = \mathrm{negl}(\lambda).$$

Remark 3.4. *We remark that Naor's commitment [Nao89] based on any (post-quantum) pseudo-random generator satisfies the above definition.*

Definition 3.5 (Bit Agreement)**.** *An (ϵ, δ)-weak bit agreement (BA) protocol with classical communication consists of an interaction between polynomial-time (potentially quantum) parties A and B, denoted by*

$$(k_A, k_B, \tau) \leftarrow \langle A(1^\lambda), B(1^\lambda)\rangle,$$

where $k_A \in \{0, 1\}$ is A's output, $k_B \in \{0, 1\}$ is B's output, and τ denotes the (classical) transcript of interaction that occurs between A and B. The protocol satisfies the following properties.

- ***Lack of bias.***

$$\left|\Pr_{(k_A,k_B,\tau)\leftarrow\langle A(1^\lambda),B(1^\lambda)\rangle}[k_A=0]-\frac{1}{2}\right|=\mathrm{negl}(\lambda),\quad \left|\Pr_{(k_A,k_B,\tau)\leftarrow\langle A(1^\lambda),B(1^\lambda)\rangle}[k_B=0]-\frac{1}{2}\right|=\mathrm{negl}(\lambda),$$

- ***Correctness.***

$$\Pr_{(k_A,k_B,\tau)\leftarrow\langle A(1^\lambda),B(1^\lambda)\rangle}[k_A=k_B]\geq\frac{1}{2}+\frac{\epsilon}{2}-\mathrm{negl}(\lambda).$$

- ***Security.*** *For any QPT adversary $\rho,\widetilde{E}$,*

$$\Pr_{(k_A,k_B,\tau)\leftarrow\langle A(1^\lambda),B(1^\lambda)\rangle}\left[\widetilde{E}(\rho,\tau)=k_A\mid k_A=k_B\right]\leq\frac{1}{2}+\frac{\delta}{2}+\mathrm{negl}(\lambda).$$

We introduce two definitions of oblivious transfer (OT). First, we give a standard game-based definition, specified as follows.

Definition 3.6 (Oblivious transfer)**.** *An (ϵ,δ,γ)-weak oblivious transfer (OT) with classical communication is a protocol that takes place between a polynomial-time (potentially quantum) sender S and a polynomial-time (potentially quantum) receiver R, denoted by*

$$(b,r),(r_0,r_1),\tau\leftarrow\langle R(1^\lambda),S(1^\lambda)\rangle,$$

where (b,r) is the output of R, (r_0,r_1) is the output of S, and τ is the (classical) transcript of interaction produced by the protocol. It should satisfy the following properties.

- ***Correctness****: It holds that*

$$\Pr\Big[r=r_b:\ \ (b,r),(r_0,r_1),\tau\leftarrow\langle R(1^\lambda),S(1^\lambda)\rangle\ \Big]\geq\frac{1}{2}+\frac{\epsilon}{2}-\mathrm{negl}(\lambda).$$

- ***Receiver security****: For any QPT adversarial sender $\rho,\widetilde{S}$,*

$$\Pr\Big[\widetilde{b}=b:(b,r),\widetilde{b}\leftarrow\langle R(1^\lambda),\widetilde{S}(\rho)\rangle\Big]\leq\frac{1}{2}+\frac{\gamma}{2}+\mathrm{negl}(\lambda).$$

- ***Sender security****: For any QPT adversarial receiver $\rho,\widetilde{R}$,*

$$\Pr\Big[\widetilde{r}=r_0\oplus r_1:\ \ \widetilde{r},(r_0,r_1)\leftarrow\langle\widetilde{R}(\rho),S(1^\lambda)\rangle\ \Big]\leq\frac{1}{2}+\frac{\delta}{2}+\mathrm{negl}(\lambda).$$

Remark 3.7. *We refer to $(1,0,0)$-weak OT as "standard OT", or just "OT", as it satisfies the standard notions of correctness and security.*

Next, we give a specialized variant of OT that we call *committed-bit* OT.

Definition 3.8 (Committed-bit OT)**.** *An (ϵ,δ,γ)-weak committed-bit OT with classical communication is a protocol that takes place between a polynomial-time (potentially quantum) sender S and a polynomial-time (potentially quantum) receiver R. The protocol begins with a setup phase, denoted by*

$$\mathsf{init}_R,\tau_{\mathsf{Setup}}\leftarrow\mathsf{Setup}\langle R(1^\lambda),S(1^\lambda)\rangle,$$

where init_R *is* R*'s private state and* τ_{Setup} *is the public (classical) transcript of interaction. Next, for any* $b \in \{0,1\}$*, the parties run*

$$(r, \mathsf{st}_R), (r_0, r_1, \mathsf{st}_S), \tau \leftarrow \mathsf{OT}\langle R(b, \mathsf{init}_R), S(\tau_{\mathsf{Setup}})\rangle.$$

In addition, there exists a (potentially inefficient) function $\mathsf{TrapGen}$*, a polynomial-time function* Ext*, and a verification protocol*

$$\{\top, \bot\} \leftarrow \mathsf{Ver}\langle R(\mathsf{st}_R), S(b, \mathsf{st}_S)\rangle,$$

such that the following properties hold.

- ***Correctness****: For any* $b \in \{0,1\}$*,*

$$\Pr\left[r = r_b : \begin{array}{r} \mathsf{init}_R, \tau_{\mathsf{Setup}} \leftarrow \mathsf{Setup}\langle R(1^\lambda), S(1^\lambda)\rangle \\ (r, \mathsf{st}_R), (r_0, r_1, \mathsf{st}_S), \tau \leftarrow \mathsf{OT}\langle R(b, \mathsf{init}_R), S(\tau_{\mathsf{Setup}})\rangle \end{array}\right] \geq \frac{1}{2} + \frac{\epsilon}{2} - \mathrm{negl}(\lambda).$$

- ***Completeness****: For any* $b \in \{0,1\}$*,*

$$\Pr\left[\mathsf{Ver}\langle R(\mathsf{st}_R), S(b, \mathsf{st}_S)\rangle = \top : \begin{array}{r} \mathsf{init}_R, \tau_{\mathsf{Setup}} \leftarrow \mathsf{Setup}\langle R(1^\lambda), S(1^\lambda)\rangle \\ (r, \mathsf{st}_R), (r_0, r_1, \mathsf{st}_S), \tau \leftarrow \mathsf{OT}\langle R(b, \mathsf{init}_R), S(\tau_{\mathsf{Setup}})\rangle \end{array}\right] = 1 - \mathrm{negl}(\lambda).$$

- ***Receiver security****: For any QPT adversarial sender* $\rho, \widetilde{S}$*,*

$$\left|\Pr\left[\widetilde{b} = 0 : \begin{array}{r} \mathsf{init}_R, \mathsf{init}_S, \tau_{\mathsf{Setup}} \leftarrow \mathsf{Setup}\langle R(1^\lambda), \widetilde{S}(\rho)\rangle \\ (r, \mathsf{st}_R), (\widetilde{b}, \mathsf{st}_S), \tau \leftarrow \mathsf{OT}\langle R(0, \mathsf{init}_R), \widetilde{S}(\mathsf{init}_S)\rangle \end{array}\right]\right.$$
$$\left. - \Pr\left[\widetilde{b} = 0 : \begin{array}{r} \mathsf{init}_R, \mathsf{init}_S, \tau_{\mathsf{Setup}} \leftarrow \mathsf{Setup}\langle R(1^\lambda), \widetilde{S}(\rho)\rangle \\ (r, \mathsf{st}_R), (\widetilde{b}, \mathsf{st}_S), \tau \leftarrow \mathsf{OT}\langle R(1, \mathsf{init}_R), \widetilde{S}(\mathsf{init}_S)\rangle \end{array}\right]\right| \leq \gamma + \mathrm{negl}(\lambda).$$

- ***Sender security****: For any unbounded algorithm* $\widetilde{R}_{\mathsf{init}}$*, with probability* $1 - \mathrm{negl}(\lambda)$ *over*

$$\mathsf{init}_R, \tau_{\mathsf{Setup}} \leftarrow \mathsf{Setup}\langle \widetilde{R}_{\mathsf{init}}, S(1^\lambda)\rangle, \quad \mathsf{td} \coloneqq \mathsf{TrapGen}(\tau_{\mathsf{Setup}}),$$

it holds that for any QPT adversarial receiver $\widetilde{R}$*,*

$$\Pr\left[\widetilde{R}(\mathsf{st}_R, r_b) = r_{1-b} : \begin{array}{r} \mathsf{st}_R, (r_0, r_1, \mathsf{st}_S), \tau \leftarrow \mathsf{OT}\langle \widetilde{R}(\mathsf{init}_R), S(\tau_{\mathsf{Setup}})\rangle \\ b \coloneqq \mathsf{Ext}(\mathsf{td}, \tau) \end{array}\right] \leq \frac{1}{2} + \frac{\delta}{2} + \mathrm{negl}(\lambda),$$

and,

$$\Pr\left[\mathsf{Ver}\langle \widetilde{R}(\mathsf{st}_R), S(1-b, \mathsf{st}_S)\rangle = \top : \begin{array}{r} \mathsf{st}_R, (r_0, r_1, \mathsf{st}_S), \tau \leftarrow \mathsf{OT}\langle \widetilde{R}(\mathsf{init}_R), S(\tau_{\mathsf{Setup}})\rangle \\ b \coloneqq \mathsf{Ext}(\mathsf{td}, \tau) \end{array}\right] = \mathrm{negl}(\lambda).$$

Remark 3.9. *We note that any* $(\epsilon, \delta, \gamma)$*-weak committed-bit OT implies* $(\epsilon, \delta, \gamma)$*-weak OT secure against adversaries with non-uniform quantum advice. Correctness and receiver security are immediate, while sender security follows due to the fact that if* $\widetilde{R}$ *can compute* $r_0 \oplus r_1$ *with some advantage, then, given* r_b*, it can output* r_{1-b} *with (at least) the same advantage.*

3.2 Alternating projectors

Marriott and Watrous introduce algorithms based on alternating projectors, which they used for witness-preserving QMA amplification [MW04]. Chiesa et al. present tools for analyzing these algorithms [CMSZ22]; we now review these tools, which will later be used for proving Theorem 6.16.

Jordan decomposition. By Jordan's lemma applied to (Π_A, Π_B), $\mathcal{H}$ decomposes orthogonally as

$$\mathcal{H} \;=\; \bigoplus_j S_j,$$

where each S_j has dimension at most 2, and is preserved by both projections. For a 2-dimensional block S_j choose orthonormal pairs $\{\left|v^A_{j,1}\right\rangle, \left|v^A_{j,0}\right\rangle\}$ and $\{\left|v^B_{j,1}\right\rangle, \left|v^B_{j,0}\right\rangle\}$ such that $\left|v^A_{j,1}\right\rangle \in \mathrm{im}(\Pi_A)$, $\left|v^A_{j,0}\right\rangle \in \ker(\Pi_A)$ and similarly for B. Define the overlap parameter

$$p_j := |\left\langle v^A_{j,1} \middle| v^B_{j,1}\right\rangle|^2 \in [0,1].$$

By convention, phases may be fixed so that within S_j, the bases are related by a planar rotation:

$$\left|v^A_{j,1}\right\rangle = \sqrt{p_j}\,\left|v^B_{j,1}\right\rangle + \sqrt{1-p_j}\,\left|v^B_{j,0}\right\rangle, \qquad \left|v^B_{j,1}\right\rangle = \sqrt{p_j}\,\left|v^A_{j,1}\right\rangle + \sqrt{1-p_j}\,\left|v^A_{j,0}\right\rangle.$$

Corollary 3.10. *In the Jordan decomposition notation above, fix a 2-dimensional block S_j and let $p_j := |\langle v^A_{j,1} \mid v^B_{j,1}\rangle|^2$, where the bases are chosen so that*

$$|v^A_{j,1}\rangle \;=\; \sqrt{p_j}\,|v^B_{j,1}\rangle + \sqrt{1-p_j}\,|v^B_{j,0}\rangle. \tag{1}$$

Then

$$(\Pi_A\Pi_B\Pi_A)\,|v^A_{j,1}\rangle \;=\; p_j\,|v^A_{j,1}\rangle.$$

In particular, each Jordan parameter p_j is an eigenvalue of the restriction $\Pi_A\Pi_B\Pi_A|_{\mathrm{im}(\Pi_A)}$. Consequently, if

$$\mathrm{spec}\Big(\Pi_A\Pi_B\Pi_A|_{\mathrm{im}(\Pi_A)}\Big) \subseteq [a,b],$$

then every Jordan parameter p_j lies in $[a,b]$.

Proof. Fix j and abbreviate $|v^A\rangle := |v^A_{j,1}\rangle$ and $|v^B\rangle := |v^B_{j,1}\rangle$. Since $|v^A\rangle \in \mathrm{im}(\Pi_A)$ we have $\Pi_A|v^A\rangle = |v^A\rangle$. Using the rotation relation (1) and that $\Pi_B|v^B_{j,1}\rangle = |v^B_{j,1}\rangle$ and $\Pi_B|v^B_{j,0}\rangle = 0$, we get

$$\Pi_B|v^A\rangle \;=\; \sqrt{p_j}\,|v^B\rangle.$$

Applying Π_A again and using the second rotation relation $|v^B\rangle = \sqrt{p_j}\,|v^A\rangle + \sqrt{1-p_j}\,|v^A_{j,0}\rangle$ together with $\Pi_A|v^A_{j,0}\rangle = 0$, we obtain

$$\Pi_A|v^B\rangle \;=\; \sqrt{p_j}\,|v^A\rangle.$$

Combining,

$$\Pi_A\Pi_B\Pi_A|v^A\rangle \;=\; \Pi_A\Pi_B|v^A\rangle \;=\; \sqrt{p_j}\,\Pi_A|v^B\rangle \;=\; p_j\,|v^A\rangle,$$

as claimed. The final implication follows since p_j is an eigenvalue of $\Pi_A\Pi_B\Pi_A|_{\mathrm{im}(\Pi_A)}$. □

The following analysis is concerned with algorithms that alternately apply two binary projective measurements $A = (\Pi_A, I - \Pi_A)$ and $B = (\Pi_B, I - \Pi_B)$ on a Hilbert space $\mathcal{H}$, stopping after a prescribed number of steps or upon observing a desired outcome.

A classical distribution for alternating outcomes. Fix $T \in \mathbb{N}$ and $p \in [0,1]$. Define a distribution $\mathrm{MWDist}(T,p)$ on bit strings $(b_1,\ldots,b_T)$ by:

1. Sample independent $a_1,\ldots,a_T \in \{0,1\}$ with $\Pr[a_i = 1] = p$.
2. Set $b_0 := 1$ and update $b_i := b_{i-1} \oplus a_i$ for $i = 1,\ldots,T$.
3. Output $(b_1,\ldots,b_T)$.

Lemma 3.11 (Lemma 4.4 in [CMSZ22]). *If the initial post-measurement state is $\left|v^B_{j,1}\right\rangle$ and we apply T measurements alternating $A, B, A, B, \ldots$, then the resulting outcome bits $(b_1,\ldots,b_T)$ are distributed as $\mathrm{MWDist}(T,p_j)$.*

Lemma 3.12 (Lemma 4.5 in [CMSZ22]). *If the initial state lies in $\mathrm{im}(\Pi_B)$, it must take the form $|\psi\rangle = \sum_j \alpha_j \left|v^B_{j,1}\right\rangle$. Then the outcome distribution equals: sample an index j with probability $|\alpha_j|^2$, then sample from $\mathrm{MWDist}(T,p_j)$.*

Let $\tilde{b} = (b_0, b_1, \ldots, b_n) \in \{0,1\}^{n+1}$. Define the normalized count of consecutive repeats

$$\mathrm{NReps}(\tilde{b}) \;:=\; \frac{1}{n}\big|\{\, j \in \{1,\ldots,n\} : b_j = b_{j-1} \,\}\big|.$$

Proposition 3.13 (Proposition 4.7 in [CMSZ22]). *If $(b_1,\ldots,b_T) \sim \mathrm{MWDist}(T,p)$, then $\mathrm{NReps}(1,b_1,\ldots,b_T)$ has the same distribution as $\mathrm{Bin}(T,p)/T$. In particular, $\mathbb{E}[\mathsf{NReps}(1,b_1,\ldots,b_T)] = p$.*

Hence, applying T alternating measurements and outputting the repeat fraction provides an estimator whose expectation (in block j) is p_j.

Proposition 3.14 (Additive Chernoff bound, Proposition 3.1 in [CMSZ22]). *Let $X \sim \mathrm{Bin}(n,p)$. For $\varepsilon, \eta > 0$, if*

$$n \;\geq\; \frac{\ln(1/2\eta)}{2\varepsilon^2},$$

then

$$\Pr\Big[\; |X/n - p| \leq \varepsilon \;\Big] \;\geq\; 1 - \eta.$$

Using Chernoff's bound, we have $\Pr[|\mathrm{NReps}(\mathrm{MWDist}(T,p_j)) - p_j| \leq \varepsilon] \;\geq\; 1-\eta$ whenever $T \geq \ln(1/2\eta)/(2\varepsilon^2)$.

4 Tests of non-commutation

4.1 Definitions

Definition 4.1 (Test of Non-Commutation). *An (α,β) classical test of non-commutation (ToNC) is a two-stage interactive protocol between a QPT (uniform) prover P and a PPT (uniform) verifier V. The first stage is defined by interactive strategies P_{Prep} and V_{Prep}, which we denote by*

$$(|\psi\rangle, (c, \mathsf{st})) \leftarrow \langle P_{\mathsf{Prep}}(1^\lambda), V_{\mathsf{Prep}}(1^\lambda)\rangle,$$

where $|\psi\rangle$ is P's output, (c,st) is V's output, and $c \in \{0,1\}, \mathsf{st} \in \{0,1\}^*$. The second stage is defined by two binary-outcome observables P_0, P_1, where P_c is applied in the case that the first stage outputs c, and a verification predicate $V_{\mathsf{Ver}}(\mathsf{st}, a) \to \{0,1\}$. It should satisfy the following properties.

- ***Completeness**: It holds that*[13]

$$\Pr\left[V_{\mathsf{Ver}}(\mathsf{st}, a) = 1 : \begin{array}{r} |\psi\rangle, (c, \mathsf{st}) \leftarrow \langle P_{\mathsf{Prep}}(1^\lambda), V_{\mathsf{Prep}}(1^\lambda)\rangle \\ a \leftarrow P_c(|\psi\rangle) \end{array}\right] \geq \beta.$$

- ***Soundness**: For any non-uniform QPT strategy $\rho, \widetilde{P}_{\mathsf{Prep}}, \widetilde{P}_0, \widetilde{P}_1$ such that $\widetilde{P}_0\widetilde{P}_1 = \widetilde{P}_1\widetilde{P}_0$,*

$$\Pr\left[V_{\mathsf{Ver}}(\mathsf{st}, a) = 1 : \begin{array}{r} |\psi\rangle, (c, \mathsf{st}) \leftarrow \langle \widetilde{P}_{\mathsf{Prep}}(1^\lambda, \rho), V_{\mathsf{Prep}}(1^\lambda)\rangle \\ a \leftarrow \widetilde{P}_c(|\psi\rangle) \end{array}\right] \leq \alpha + \mathrm{negl}(\lambda).$$

Definition 4.2 (Normal form test of non-commutation)**.** *We say that the test of non-commutation (Definition 4.1) is in* normal form *if:*

- $\mathsf{st} = a^* \in \{0, 1\}$*, and*
- $V_{\mathsf{Ver}}(a^*, a) = 1$ *iff* $a = a^*$*.*

That is, there is always exactly one answer bit that the verifier accepts.

Remark 4.3. *In any normal-form ToNC, both $\beta, \alpha \geq 1/2$ since there always exists a trivial strategy which outputs a uniformly random bit. Thus, it is often convenient to write the parameters of a normal-form ToNC using the* advantage *of the prover as opposed to the raw probability of success. That is, we will often refer to a normal form (α, β)-ToNC where $\alpha, \beta \in [1/2, 1]$ as an (ϵ, δ)-ToNC, where $\epsilon := 2\beta - 1, \delta := 2\alpha - 1 \in [0, 1]$. We will also assume without loss of generality that $\delta \geq \epsilon/2$, as justified in our discussion in Section 1.1.*

Next, we specify a stronger completeness guarantee stating that for *all* preambles, the (honest) prover's advantage is at least ϵ. Note that this is satisfied by the compiled CHSH game (with $\epsilon = 2\cos^2(\pi/8) - 1$) and the compiled magic square game (with $\epsilon = 1$).

Definition 4.4 (Test of non-commutation with robust completeness)**.** *We say that a (normal form) (ϵ, δ)-ToNC has* robust completeness *if with probability 1 over $|\psi\rangle, (c, \mathsf{st}) \leftarrow \langle P_{\mathsf{Prep}}(1^\lambda), V_{\mathsf{Prep}}(1^\lambda)\rangle$,*

$$\Pr\left[V_{\mathsf{Ver}}(\mathsf{st}, a) = 1 : a \leftarrow P_c(|\psi\rangle)\right] = \frac{1}{2} + \frac{\epsilon}{2}.$$

4.2 Normal form compiler

In this subsection, we present a procedure that transforms a less structured form of ToNC into a normal-form ToNC as in Definition 4.2. This transformation incurs an inverse-polynomial parameter loss. Whereas in the final round of a normal-form ToNC the verifier accepts exactly one of the two possible prover answers, in the less structured form, the verifier may alternatively accept both or neither. Since our constructions of oblivious transfer and key agreement use normal-form ToNCs, the compilation procedure below shows that the same implications hold for a broader class of ToNC protocols. Moreover, this compilation procedure suggests that normal-form ToNC is not merely a convenient technical restriction, but a natural abstraction: it captures, up to bounded parameter loss, a broad class of ToNC protocols.

[13] In an abuse of notation, we write $P(|\psi\rangle)$ to denote the distribution induced by measuring state $|\psi\rangle$ with projective measurement $\{P, I - P\}$.

Theorem 4.5 (Normal form compiler)**.** *Let I be two-stage protocol satisfying Definition 4.1, except that the second-stage predicate $V_{\mathsf{Ver}}(\mathsf{st}, \cdot)$ may (for some values of st) accept both $a \in \{0,1\}$ or accept neither. Then for any inverse-polynomial function $\varepsilon(\lambda)$, there exists a* normal-form *test I^{nf} with parameters (α', β') such that*

$$\beta' - \alpha' \;\geq\; \beta - \alpha - O(\varepsilon).$$

Remark 4.6. *As we explain in the proof below, the verifier in the constructed normal-form test I^{nf} may include a* quantum *polynomial-time preprocessing phase that takes as input the security parameter and outputs some classical information. After this, its interaction with the prover is entirely classical. While this does not exactly fit the syntax of Definition 4.1, we remark that all the implications of (normal-form) ToNC that we show (i.e. to classical-communication KA and OT) follow in exactly the same manner if we start with a ToNC with quantum verifier preprocessing.*

Proof. By the completeness of I, there exists a uniform QPT strategy $S = (P_{\mathsf{Prep}}, P_0, P_1)$ that succeeds with probability at least β for any value of the security parameter λ. Let (c, st) be the verifier output in the preparation stage when interacting with P_{Prep}. For any such output, define the acceptance set

$$A(c, \mathsf{st}) := \{a \in \{0,1\} : V_{\mathsf{Ver}}(c, \mathsf{st}, a) = 1\},$$

so that $|A(c, \mathsf{st})| \in \{0, 1, 2\}$. Define

$$\ell(\lambda) := \Pr[|A(c, \mathsf{st})| = 2], \qquad \mu(\lambda) := \Pr[|A(c, \mathsf{st})| = 0], \qquad \gamma(\lambda) := \Pr[|A(c, \mathsf{st})| = 1],$$

where the probabilities are taken over random interactions between $S(\lambda)$ and the verifier $V(\lambda)$.

Given the security parameter λ, the verifier in our normal-form test I^{nf} must determine the numbers $\ell(\lambda), \mu(\lambda), \gamma(\lambda)$. For all non-commutation tests we are aware of, these numbers are in fact constants independent of the security parameter, and thus they can be hard-coded into the verifier. However, in general, this may not be the case, so the verifier will *estimate* these values by running a quantum pre-processing step in I^{ns} (Step 1 in the protocol described below).

Now, let a be the answer obtained by applying P_c to the prover state, and define the conditional success on *unique-accepting* transcripts

$$\xi(\lambda) := \Pr[a = a^\star(c, \mathsf{st}) \mid |A(c, \mathsf{st})| = 1],$$

where if $|A(c, \mathsf{st})| = 1$, $a^\star(c, \mathsf{st})$ is the unique accepted answer. Then the overall success of S decomposes as

$$\Pr[I \text{ accepts with } S] \;=\; \ell + \gamma\,\xi \;\geq\; \beta. \tag{2}$$

Consider the following strategy in I. It executes S in the first stage of the protocol, and in the second stage it sends the verifier a uniformly random bit. This strategy succeeds in the protocol with probability $\ell + \frac{\gamma}{2}$, and applies perfectly commuting observables in the second stage. Therefore, the soundness of I implies that $\ell + \frac{\gamma}{2} \leq \alpha$. On the other hand, $\ell + \gamma\xi \geq \beta$. Thus,

$$\beta - \alpha \leq (\xi - \frac{1}{2})\gamma \to \gamma \geq \frac{\beta - \alpha}{\xi - \frac{1}{2}} \qquad \text{(and indeed } \xi > \frac{1}{2} \text{ because } \beta > \alpha).$$

We deduce that $\gamma > 0$. Moreover, since $\alpha < \beta$ are constants, we get $\gamma(\lambda) \geq \frac{1}{\mathrm{poly}(\lambda)}$.

The normal-form protocol I^{nf}. Fix functions $\varepsilon(\lambda) = \frac{1}{\mathrm{poly}(\lambda)}$ such that $\varepsilon < \frac{\gamma}{4}$, and $\eta > 0$, where $\eta(\lambda) = \mathrm{negl}(\lambda)$, and let r, v be two polynomials. The verifier operates as follows:

1. Obtain estimates of $\ell := \ell(\lambda), \mu := \mu(\lambda), \gamma := \gamma(\lambda)$, either as hard-coded values or by simulating interaction with the prover strategy S several times and taking the averages. By running enough times, the verifier can obtain estimates that, with overwhelming probability, are arbitrarily inverse-polynomial close to the real values. We suppress mention of this approximation for the rest of the proof, and assume that the verifier obtains the exact values $\ell := \ell(\lambda), \mu := \mu(\lambda), \gamma := \gamma(\lambda)$.

2. Sets a variable $\mathsf{FLAG} := 0$, draws $w \in [v(\lambda)]$ uniformly at random. For $i = 1, \ldots, w$:

   (a) Runs r copies of I sequentially with the prover, using fresh verifier randomness at each copy. The verifier completes only the first step of the protocol at each copy, producing outputs (c_i, st_i).

   (b) Computes $|A(c_i, \mathsf{st}_i)|$ by executing $V_{\mathsf{Ver}}(\mathsf{st}_i, 0)$ and $V_{\mathsf{Ver}}(\mathsf{st}_i, 1)$, and sets

   $$\widehat{\ell} := \frac{1}{r}|\{i : |A(c_i, \mathsf{st}_i)| = 2\}|, \quad \widehat{\mu} := \frac{1}{r}|\{i : |A(c_i, \mathsf{st}_i)| = 0\}|, \quad \widehat{\gamma} := \frac{1}{r}|\{i : |A(c_i, \mathsf{st}_i)| = 1\}|.$$

   (c) If $\widehat{\gamma} = 0$, or if any of $|\widehat{\ell} - \ell|, |\widehat{\mu} - \mu|, |\widehat{\gamma} - \gamma|$ exceeds ε, the verifier sets $\mathsf{FLAG} := 1$ and exits the loop.

3. The verifier then runs the following steps.

   (a) Runs step 2 (a) once, and thus produces outputs (c_i, st_i).

   (b) Samples $i \leftarrow [r]$ uniformly at random, sets $c := c_i$ and sends i to the prover. If $|A(c_i, \mathsf{st}_i)| \neq 1$, sets $\mathsf{FLAG} = 1$.

   (c) If $\mathsf{FLAG} = 1$, the verifier draws a uniformly random bit $\mathsf{st} \leftarrow \{0, 1\}$, sends c to the prover and receives an answer bit a, and then accepts if and only if $\mathsf{st} = a$.

   (d) Otherwise, the verifier sets $\mathsf{st} := a^\star(c_i, \mathsf{st}_i)$, where $a^\star(c_i, \mathsf{st}_i)$ is the unique answer accepted by the verifier in the i-th instance. The prover sends an answer bit a, and the verifier accepts if and only if $\mathsf{st} = a$.

Completeness. We consider the prover strategy $\widetilde{S}$ for I^{nf}, which executes S independently in each copy of I. By standard concentration bounds and a union bound over the three empirical frequencies, for large enough polynomials r, v we obtain that the probability that $\mathsf{FLAG} = 1$ at the end of stage 2 of the protocol is at most $\eta(\lambda)$.

Conditioned on the event that $\mathsf{FLAG} = 0$ at the end of step 2, with probability γ, the verifier does not set $\mathsf{FLAG} = 1$ in stage 3(b), and in that case the acceptance probability is $\xi = \frac{\beta - \ell}{\gamma}$. ξ is the acceptance probability of a prover running the strategy S in the original protocol I, conditioned on $|A(c, \mathsf{st})| = 1$. If the verifier does set $\mathsf{FLAG} = 1$ in stage 3(b), the acceptance probability is $\frac{1}{2}$.

Overall,

$$\Pr\left[I^{\mathsf{nf}} \text{ accepts with } \widetilde{S}\right] \;\geq\; \xi\gamma + \frac{1}{2}(1 - \gamma) - \eta, \text{ where } \xi = \frac{\beta - \ell}{\gamma}. \tag{3}$$

Soundness. Let

$$\widetilde{S} = (\widetilde{P}_{\mathsf{Prep}}, \widetilde{P}_0, \widetilde{P}_1)$$

be an arbitrary QPT strategy for I^{nf} whose final observables commute:

$$\widetilde{P}_0 \widetilde{P}_1 = \widetilde{P}_1 \widetilde{P}_0.$$

Let s denote the success probability of $\widetilde{S}$ in I^{nf}.

Recall that a block consists of r first-stage executions of I. We call a block *good* if its empirical frequencies satisfy

$$|\widehat{\ell} - \ell| \le \varepsilon, \qquad |\widehat{\mu} - \mu| \le \varepsilon, \qquad |\widehat{\gamma} - \gamma| \le \varepsilon.$$

Since we chose $\varepsilon < \gamma/4$, every good block also satisfies $\widehat{\gamma} > 0$. Let F be the event that $\mathsf{FLAG} = 0$ at the end of stage 2, and write

$$u := \Pr[F].$$

Thus, F is the event that every one of the w cut-and-choose blocks in stage 2 is good.

We first record the following random-stopping fact. This is the point where we use the fact that $w \leftarrow [v]$ is hidden from the prover.

Claim 4.7. *For every strategy $\widetilde{S}$,*

$$\Pr[F \wedge \textit{the stage-3 block is bad}] \le \frac{1}{v}.$$

Consequently, if $u > 0$, then

$$\Pr[\textit{the stage-3 block is bad} \mid F] \le \frac{1}{uv}.$$

Proof. Consider the coupled execution in which the verifier keeps generating blocks of r first-stage executions using the same interface that the prover sees before the index i is sent. Let T be the index of the first bad block in this coupled execution, with $T = \infty$ if no bad block ever occurs.

The stopping time $w \leftarrow [v]$ is sampled independently of the prover's behavior and is not revealed before the stage-3 block has already been generated. Then, consider the event

$$F \wedge \text{the stage-3 block is bad.}$$

This is exactly the events that $T = w + 1$. Since w is uniform in $[v]$, this event has probability at most $1/v$. The conditional bound follows by dividing by $\Pr[F] = u$. □

We now split into two cases.

Case 1: $u \le \varepsilon$. Conditioned on $\neg F$, the verifier has already set $\mathsf{FLAG} = 1$, and therefore the final target bit st is uniform and independent of the prover's final answer. Thus the prover succeeds with probability exactly $1/2$ conditioned on $\neg F$. Conditioned on F, its success probability is at most 1. Therefore

$$s \le \frac{1-u}{2} + u = \frac{1}{2} + \frac{u}{2} \le \frac{1}{2} + \frac{\varepsilon}{2}.$$

On the other hand, the strategy for I that runs the honest first-stage strategy S and then answers with a uniformly random bit has commuting final observables and succeeds with probability $\ell + \gamma/2$. By the soundness of I,

$$\ell + \frac{\gamma}{2} \le \alpha + \mathrm{negl}(\lambda).$$

Hence, in this case,

$$s \le \frac{1}{2} + \frac{\varepsilon}{2} \le \frac{1}{2} + \alpha - \ell - \frac{\gamma}{2} + O(\varepsilon) + \mathrm{negl}(\lambda).$$

Case 2: $u > \varepsilon$. Choose v large enough so that $v \ge 1/\varepsilon^2$. By Claim 4.7,

$$\Pr[\text{the stage-3 block is bad} \mid F] \le \frac{1}{uv} \le \varepsilon.$$

Let $q \leftarrow [r]$ be the uniformly random coordinate selected by the verifier in stage 3. Conditioned on F, define

$$\overline{\ell} := \Pr[|A(c_q, \mathsf{st}_q)| = 2 \mid F], \qquad \overline{\gamma} := \Pr[|A(c_q, \mathsf{st}_q)| = 1 \mid F].$$

Since, conditioned on F, the stage-3 block is good except with probability at most ε, and since q is uniform in the stage-3 block, we have

$$|\overline{\ell} - \ell| \leq 2\varepsilon, \qquad |\overline{\gamma} - \gamma| \leq 2\varepsilon. \tag{4}$$

Next define

$$\overline{\chi} := \Pr[a = a^\star(c_q, \mathsf{st}_q) \mid F \wedge |A(c_q, \mathsf{st}_q)| = 1],$$

where a is the answer output by $\widetilde{S}$ after receiving the selected index q and the challenge c_q. If the conditioning event has probability 0, set $\overline{\chi} = 1/2$.

We now construct a commuting strategy K for the original protocol I. The strategy K internally runs $\widetilde{S}$ and simulates the verifier of I^{nf}. It first simulates stages 1–2 of I^{nf}. If $\mathsf{FLAG} = 1$ at the end of stage 2, it restarts this simulation with a fresh copy of $\widetilde{S}$. Since $u > \varepsilon$, after

$$z = \mathrm{poly}(1/\varepsilon, \lambda)$$

repetitions, K obtains an execution satisfying F, except with negligible probability. If all repetitions fail, K answers randomly.

Once an execution satisfying F has been obtained, K generates the stage-3 block. It samples $q \leftarrow [r]$ uniformly at random and embeds its external interaction with the verifier of I in the q-th coordinate of this block, while simulating all other coordinates honestly. After the r first-stage executions have been completed, K sends the index q to $\widetilde{S}$. When the external verifier of I sends its challenge bit c, the strategy K forwards this challenge to $\widetilde{S}$, obtains an answer a, and returns a to the external verifier.

The final observables of K are precisely the final observables induced by $\widetilde{S}$ after the simulated transcript and the classical index q have been fixed. Therefore they commute, because $\widetilde{S}$'s final observables commute.

By construction, up to the negligible probability that K fails to obtain an execution satisfying F, the external instance of I is distributed as the selected coordinate of the stage-3 block conditioned on F. Therefore the success probability of K in I is

$$\overline{\ell} + \overline{\gamma}\,\overline{\chi} - \mathrm{negl}(\lambda).$$

Indeed, if $|A(c_q, \mathsf{st}_q)| = 2$, every answer is accepted; if $|A(c_q, \mathsf{st}_q)| = 0$, no answer is accepted; and if $|A(c_q, \mathsf{st}_q)| = 1$, the success probability is exactly $\overline{\chi}$. By the soundness of the original protocol I, we obtain

$$\overline{\ell} + \overline{\gamma}\,\overline{\chi} \leq \alpha + \mathrm{negl}(\lambda). \tag{5}$$

We now relate this to the success probability s of $\widetilde{S}$ in I^{nf}. Conditioned on $\neg F$, the verifier uses a uniformly random target bit, so the success probability is $1/2$. Conditioned on F, the verifier uses the real unique accepting bit only if the selected coordinate is unique-accepting; otherwise it sets $\mathsf{FLAG} = 1$ and uses a uniformly random target bit. Hence

$$s = \frac{1-u}{2} + u\left(\overline{\gamma}\,\overline{\chi} + \frac{1-\overline{\gamma}}{2}\right) = \frac{1}{2} + u\,\overline{\gamma}\left(\overline{\chi} - \frac{1}{2}\right).$$

If $\overline{\chi} \leq 1/2$, then $s \leq 1/2$, and using $\ell + \gamma/2 \leq \alpha + \mathrm{negl}(\lambda)$, we again get

$$s \leq \frac{1}{2} + \alpha - \ell - \frac{\gamma}{2} + \mathrm{negl}(\lambda).$$

Otherwise, $\overline{\chi} > 1/2$. Since $u \leq 1$,

$$s \leq \frac{1}{2} + \overline{\gamma}\left(\overline{\chi} - \frac{1}{2}\right) = \frac{1}{2} + \overline{\gamma}\,\overline{\chi} - \frac{\overline{\gamma}}{2}.$$

Using (5), this gives

$$s \leq \frac{1}{2} + \alpha - \overline{\ell} - \frac{\overline{\gamma}}{2} + \mathrm{negl}(\lambda).$$

Finally, by (4),

$$s \leq \frac{1}{2} + \alpha - \ell - \frac{\gamma}{2} + O(\varepsilon) + \mathrm{negl}(\lambda).$$

Since $\widetilde{S}$ was arbitrary, the soundness parameter α' of I^{nf} satisfies

$$\alpha' \leq \frac{1}{2} + \alpha - \ell - \frac{\gamma}{2} + O(\varepsilon) + \mathrm{negl}(\lambda). \tag{6}$$

Gap analysis. From the completeness analysis, we have

$$\beta' \geq \frac{1}{2} + \gamma\xi - \frac{\gamma}{2} - \eta.$$

Using the decomposition

$$\ell + \gamma\xi \geq \beta,$$

we get

$$\beta' \geq \frac{1}{2} + \beta - \ell - \frac{\gamma}{2} - \eta. \tag{7}$$

Combining (6) and (7),

$$\beta' - \alpha' \geq \beta - \alpha - O(\varepsilon) - \eta - \mathrm{negl}(\lambda).$$

Choosing the completeness parameters so that $\eta \leq O(\varepsilon)$, and absorbing the negligible term into the $O(\varepsilon)$ loss, we conclude that

$$\beta' - \alpha' \geq \beta - \alpha - O(\varepsilon),$$

as required.

Recall that I^{nf} is constructed with a choice of ε, and it remains efficient for any $\varepsilon(\lambda) = \frac{1}{\mathrm{poly}(\lambda)}$. Thus, the above gap is attainable for any such ε. This completes the proof. □

5 Weak cryptography from tests of non-commutation

5.1 Weak bit agreement

Weak bit agreement is a protocol run between two potentially quantum parties A and B that communicate classically. The protocol is parameterized by ϵ, which determines the probability that A and B agree on a bit, and δ, which determines how much information an eavesdropper can obtain about the shared bit.

Theorem 5.1. *Given any normal-form (ϵ, δ) test of non-commutation secure against adversaries with non-uniform classical (resp. quantum) advice (Definition 4.1, Remark 4.3), there exists a (ϵ, δ')-BA secure against adversaries with non-uniform classical (resp. quantum) advice (Definition 3.5) for any*

$$\delta' \geq \frac{1 + 4\delta - 3\epsilon}{1 + \epsilon}.$$

Moreover, given any normal-form (ϵ, δ) test of non-commutation secure against adversaries with non-uniform classical (resp. quantum) advice with robust *completeness (Definition 4.4), there exists a (ϵ, δ')-BA secure against adversaries with non-uniform classical (resp. quantum) advice for any*

$$\delta' \geq 2\delta - \epsilon.$$

Proof. The protocol is given in Protocol 5.1. The theorem follows by combining Lemma 5.2 and Lemma 5.3. □

Protocol: Weak bit agreement

Parties. Alice A and Bob B (classical communication; parties may be quantum).
Ingredient. Normal-form (ϵ, δ) test of non-commutation $P_{\mathsf{Prep}}, V_{\mathsf{Prep}}, P_0, P_1, V_{\mathsf{Ver}}$ (Definition 4.1).

Step 1: Non-commutation test. The parties run

$$|\psi\rangle, (c, a^*) \leftarrow \langle P_{\mathsf{Prep}}(1^\lambda), V_{\mathsf{Prep}}(1^\lambda)\rangle,$$

with A playing the role of verifier and B playing the role of prover. At its conclusion, A obtains the "correct" answer bit a^* and sends the challenge bit c to B.

Step 2: Random mask. A samples $r \leftarrow \{0, 1\}$ uniformly at random and sends it to B.

Step 3: Outputs. A outputs the bit $k_A := a^* \oplus r$. Upon receiving (c, r), B applies $a \leftarrow P_c(|\psi\rangle)$ and outputs $k_B := a \oplus r$.

Lemma 5.2 (Correctness). *Protocol 5.1 satisfies Lack of bias and Correctness according to Definition 3.5 with the same ϵ from the ToNC parameters.*

Proof. The event $k_A = k_B$ is exactly the event that $a = a^*$, and hence occurs with advantage ϵ due to the completeness of the ToNC. Moreover, due to the random masking,

$$\Pr[k_A = 0] = \Pr[k_B = 0] = \tfrac{1}{2}.$$

□

Lemma 5.3 (Security). *Protocol 5.1 satisfies Security according to Definition 3.5 with $\delta' = \frac{1+4\delta-3\epsilon}{1+\epsilon}$. In the case that the ToNC has robust completeness, it satisfies Security with $\delta' = 2\delta - \epsilon$.*

Proof. Fix a QPT adversary $\widetilde{E}$ and let γ be such that $\Pr\left[\widetilde{E}(\tau) = k_A\right] = \frac{1}{2} + \frac{\gamma}{2}$ in an execution with honest A, B, where τ is the transcript produced by the interaction. By completeness of the ToNC, fix a QPT prover strategy $P_{\mathsf{Prep}}, P_0, P_1$ that accepts with probability at least $\frac{1}{2} + \frac{\epsilon}{2}$. E may or may not have non-uniform quantum advice ρ, which determines whether our new prover strategy does. We suppress mention of ρ in what follows.

We build a new prover strategy $\widetilde{P}_{\mathsf{Prep}}, \widetilde{P}_0, \widetilde{P}_1$ with commuting final-round observables, as follows. $\widetilde{P}_{\mathsf{Prep}}$ interacts with the verifier through the preparation stage by executing P_{Prep}. After receiving the final-round challenge $c \in \{0,1\}$, it samples a fresh uniform bit $b \leftarrow \{0,1\}$ and proceeds as follows:

- If $c = b$, it answers using P_c.
- If $c \neq b$, it answers using $\widetilde{E}$ applied to the (classical) transcript τ.

Equivalently, $\widetilde{P}_{\mathsf{Prep}}$ can execute a *joint* measurement producing both candidate answers $(\hat{a}_0, \hat{a}_1)$: sample b; measure using P_c to obtain $\hat{a}_b$; compute $\hat{a}_{1-b} \leftarrow \widetilde{E}(\tau_{1-b})$ (where τ_t denotes the transcript with final challenge set to t). Then, on challenge c, output $\hat{a}_c$. Since this procedure produces both answers in one joint measurement, it is clear that the induced final-round observables commute.

Conditioned on $b = c$ (probability $1/2$), $\widetilde{P}$ behaves like P on the final round, and thus has advantage at least ϵ. Conditioned on $b \neq c$ (probability $1/2$), $\widetilde{P}$ has advantage γ, by definition. Hence, the advantage of $\widetilde{P}$ is at least $\frac{\epsilon+\gamma}{2}$.

By soundness of the ToNC against commuting strategies,

$$\frac{\epsilon+\gamma}{2} \leq \delta \quad \Rightarrow \quad \gamma \leq 2\delta - \epsilon.$$

Since $\Pr[k_A = k_B] \geq \frac{1}{2} + \frac{\epsilon}{2}$, we have

$$\begin{aligned} 2\Pr\left[\widetilde{E}(\tau) = k_A \mid k_A = k_B\right] - 1 &\leq 2\left(\frac{\Pr\left[\widetilde{E}(\tau) = k_A\right]}{\Pr[k_A = k_B]}\right) - 1 \\ &\leq 2\left(\frac{\frac{1}{2} + \delta - \frac{\epsilon}{2}}{\frac{1}{2} + \frac{\epsilon}{2}}\right) - 1 \\ &= \frac{2 + 4\delta - 2\epsilon}{1+\epsilon} - 1 \\ &= \frac{1 + 4\delta - 3\epsilon}{1+\epsilon}, \end{aligned}$$

which completes the proof.

Now, in the case that the ToNC satisfies robust completeness, we have that the event $\widetilde{E}(\tau) = k_A$ is *independent* of the event $k_A = k_B$, and thus

$$2\Pr\left[\widetilde{E}(\tau) = k_A \mid k_A = k_B\right] - 1 = 2\Pr\left[\widetilde{E}(\tau) = k_A\right] - 1 = \gamma \leq 2\delta - \epsilon.$$

□

5.2 Weak (committed-bit) oblivious transfer

Theorem 5.4. *Assume the existence of an inefficiently-extractable commitment (Definition 3.3) and a normal form (ϵ, δ) test of non-commutation secure against adversaries with non-uniform quantum advice (Definition 4.1, Remark 4.3). Then for any $\delta' > 2\delta - \epsilon$, there exists an $(\epsilon, \delta', 0)$-weak committed-bit OT (Definition 3.8).*

Proof. The protocol is given in Protocol 5.2. The theorem follows by combining Lemma 5.5, Lemma 5.6, Lemma 5.7, and Lemma 5.8. □

Protocol: Weak committed-bit OT

Parties. Sender S and receiver R (classical communication; parties may be quantum).
Ingredients. Inefficiently-extractable commitment $(\mathsf{Com}, \mathsf{Rec}, \mathsf{Ver}_{\mathsf{Com}}, \mathsf{Ext}_{\mathsf{Com}})$ (Definition 3.3) and normal-form (ϵ, δ) test of non-commutation $(P_{\mathsf{Prep}}, V_{\mathsf{Prep}}, P_0, P_1, V_{\mathsf{Ver}})$ (Definition 4.1).

$\mathsf{Setup}\langle R(1^\lambda), S(1^\lambda)\rangle$:

- **Challenge commitments.** For each $k \in [\lambda]$, $i \in [2\lambda]$, R samples $x_i^k \leftarrow \{0,1\}$ and the parties run
$$\mathsf{st}^k_{\mathsf{Com},i}, \tau_i^k \leftarrow \left\langle \mathsf{Com}\left(1^\lambda, x_i^k\right), \mathsf{Rec}\left(1^\lambda\right)\right\rangle,$$
with R playing the role of Com and S playing the role of Rec.
- R sets $\mathsf{init}_R := \left\{\mathsf{st}^k_{\mathsf{Com},i}\right\}_{k\in[\lambda], i\in[2\lambda]}$.

$\mathsf{OT}\langle R(b, \mathsf{init}_R), S(\mathsf{init}_S)\rangle$:

- **Answer commitments.** For each $k \in [\lambda]$, $i \in [2\lambda]$, R samples $y_i^k \leftarrow \{0,1\}$ and the parties run
$$\mathsf{st}'^k_{\mathsf{Com},i}, \tau'^k_i \leftarrow \left\langle \mathsf{Com}\left(1^\lambda, y_i^k\right), \mathsf{Rec}\left(1^\lambda\right)\right\rangle,$$
with R playing the role of Com and S playing the role of Rec.
- **Pair commitments.** For each $k \in [\lambda]$ and unordered pair $\{i,j\} \subseteq [2\lambda]$, R sets $x^k_{i,j} := x_i^k \oplus x_j^k$, and the parties run
$$\mathsf{st}^k_{\mathsf{Com},\{i,j\}}, \tau^k_{\{i,j\}} \leftarrow \left\langle \mathsf{Com}\left(1^\lambda, x^k_{i,j}\right), \mathsf{Rec}\left(1^\lambda\right)\right\rangle,$$
with R playing the role of Com and S playing the role of Rec.
- **Main loop.** S samples $k^* \leftarrow [\lambda]$. For $k = 1$ to k^*:
  - **Non-commutation tests.** For each $i \in [2\lambda]$, the parties run
  $$|\psi_i^k\rangle, \left(c_i^k, a_i^k\right) \leftarrow \langle P_{\mathsf{Prep}}(1^\lambda), V_{\mathsf{Prep}}(1^\lambda)\rangle,$$
  with R playing the role of the prover and S playing the role of the verifier. For each $i \in [2\lambda]$, S samples $z_i^k \leftarrow \{0,1\}$ and sends z_i^k to R. For each $i \in [2\lambda]$, R sets $c^k_{R,i} := x_i^k \oplus z_i^k$, computes
  $$a^k_{R,i} \leftarrow P_{c^k_{R,i}}\left(|\psi_i^k\rangle\right)$$
  and sends $\widehat{a}_i^k := a^k_{R,i} \oplus y_i^k$ to S.
  - **Pairing and checks.** S partitions $[2\lambda]$ uniformly at random into a disjoint set of λ pairs $\mathcal{P}$, and sends $\mathcal{P}$ to R. For each $\{i,j\} \in \mathcal{P}$, R sends $\left(x^k_{i,j}, \mathsf{st}^k_{\mathsf{Com},\{i,j\}}\right)$ to S, who aborts if
  $$\mathsf{Ver}_{\mathsf{Com}}\left(\mathsf{st}^k_{\mathsf{Com},\{i,j\}}, \tau^k_{\{i,j\}}, x^k_{i,j}\right) = \bot.$$
  S chooses a pair $P^* = \{i^*, j^*\} \in \mathcal{P}$ uniformly at random conditioned on $x^k_{i^*,j^*} \oplus z^k_{i^*} \oplus z^k_{j^*} \neq c^k_{i^*} \oplus c^k_{j^*}$ (or aborts if no such pair exists), and sends P^* to R. For each $\{i,j\} \in \mathcal{P} \setminus \{P^*\}$:

* R sends $x_i^k, \mathsf{st}_{\mathsf{Com},i}^k, x_j^k, \mathsf{st}_{\mathsf{Com},j}^k, y_i^k, \mathsf{st}'^k_{\mathsf{Com},i}, y_j^k, \mathsf{st}'^k_{\mathsf{Com},j}$ to S, who aborts if any of the respective $\mathsf{Ver}_{\mathsf{Com}}$ checks fail.
* S aborts if $x_{i,j}^k \neq x_i^k \oplus x_j^k$. Otherwise, S sets

$$c_{R,i}^k = x_i^k \oplus z_i^k, c_{R,j}^k = x_j^k \oplus z_j^k, a_{R,i}^k = \widehat{a}_i^k \oplus y_i^k, a_{R,j}^k = \widehat{a}_j^k \oplus y_j^k.$$

S aborts if:

* For less than $1/4$ fraction of $i \in [2\lambda] \setminus P^*$, $c_{R,i}^k = c_i^k$.
* For less than $\frac{1}{2} + \frac{\epsilon}{2} - \lambda^{1/3}$ fraction of $i \in [2\lambda] \setminus P^*$ such that $c_{R,i}^k = c_i^k$, $a_{R,i}^k = a_i^k$.

- **Final transfer.** Re-define

$$\begin{aligned}
&c_0 = c_{i^*}^{k^*}, c_1 = c_{j^*}^{k^*}, \quad c_{R,0} = c_{R,i^*}^{k^*}, c_{R,1} = c_{R,j^*}^{k^*} \\
&a_0 = a_{i^*}^{k^*}, a_1 = a_{j^*}^{k^*}, \quad a_{R,0} = a_{R,i^*}^{k^*}, a_{R,1} = a_{R,j^*}^{k^*} \\
&x_0 = x_{i^*}^{k^*}, x_1 = x_{j*}^{k^*}, \quad z_0 = z_{i^*}^{k^*}, z_1 = z_{j^*}^{k^*} \\
&\mathsf{st}_{\mathsf{Com},0} = \mathsf{st}_{\mathsf{Com},i^*}^{k^*}, \mathsf{st}_{\mathsf{Com},1} = \mathsf{st}_{\mathsf{Com},j^*}^{k^*}, \quad \tau_0 = \tau_{i^*}^{k^*}, \tau_1 = \tau_{j^*}^{k^*}.
\end{aligned}$$

  - S sends $\{c_0, c_1\}$ to R.
  - Let $\widehat{b} \in \{0,1\}$ be the unique bit such that $c_{R,\widehat{b}} = c_{\widehat{b}}$. R sends $b' = b \oplus \widehat{b}$ to S.
  - S outputs $(r_0 \coloneqq a_{b'}, r_1 \coloneqq a_{1-b'})$ and $\mathsf{st}_S = (b', \tau_0, \tau_1, c_0, c_1, z_0, z_1)$.
  - R outputs $r \coloneqq a_{R,\widehat{b}}$ and $\mathsf{st}_R = (x_0, x_1, \mathsf{st}_{\mathsf{Com},0}, \mathsf{st}_{\mathsf{Com},1})$.

$\mathsf{Ver}\langle R(\mathsf{st}_R), S(b, \mathsf{st}_S)\rangle$:

- If $\mathsf{Ver}_{\mathsf{Com}}(\mathsf{st}_{S,0}, \mathsf{st}_{R,0}, x_0) = \bot$ or $\mathsf{Ver}_{\mathsf{Com}}(\mathsf{st}_{S,1}, \mathsf{st}_{R,1}, x_1) = \bot$, output $\bot$.
- Let $c_{R,0} = x_0 \oplus z_0$, $c_{R,1} = x_1 \oplus z_1$. If $c_0 \oplus c_1 = c_{R,0} \oplus c_{R,1}$, output $\bot$.
- Let $\widehat{b}$ be the unique bit such that $c_{R,\widehat{b}} = c_{\widehat{b}}$. Output $\top$ iff $b = \widehat{b} \oplus b'$.

$\mathsf{TrapGen}(\tau_{\mathsf{Setup}})$:

- For each $k \in [\lambda], i \in [2\lambda]$, run $x_i^k \coloneqq \mathsf{Ext}_{\mathsf{Com}}\left(\tau_i^k\right)$. Set $\mathsf{td} \coloneqq \left\{x_i^k\right\}_{i \in [2\lambda]}$.

$\mathsf{Ext}(\mathsf{td}, \tau)$:

- τ includes z_0, z_1, c_0, c_1, b' and td includes $x_0 = x_{i^*}$ and $x_1 = x_{j^*}$.
- Let $c_{R,0} = x_0 \oplus z_0$, $c_{R,1} = x_1 \oplus z_1$. If $c_0 \oplus c_1 = c_{R,0} \oplus c_{R,1}$, output 0.
- Let $\widehat{b}$ be the unique bit such that $c_{R,\widehat{b}} = c_{\widehat{b}}$. Output $\widehat{b} \oplus b'$.

Lemma 5.5 (Correctness). *Protocol 5.2 satisfies Correctness according to Definition 3.8 with* $\epsilon = 2\beta - 1$.

Proof. By inspection, and the completeness of the ToNC (Definition 4.1), we have that $r = r_b$ with probability $\beta = \frac{1}{2} + \frac{\epsilon}{2}$, *conditioned on* S not aborting during one of the iterations of the main loop. So, it remains to show that S aborts with $\mathrm{negl}(\lambda)$ probability. We will show that S aborts in an iteration for any $k \in [\lambda]$ with $\mathrm{negl}(\lambda)$ probability, which establishes the above by a union bound.

First, consider the check that for $1/4$ fraction of $i \in [2\lambda] \setminus P^*$, $c^k_{R,i} = c^k_i$. Since the bits $c^k_{R,i}$ are masked by the z^k_i, which are sampled uniform and independent of the rest of the protocol, this check fails with probability bounded by the following Hoeffding inequality:

$$\Pr\left[\frac{\#\{i : c^k_{R,i} \neq c^k_i\}_{i\in[2\lambda]\setminus P^*}}{2\lambda - 2} < \frac{1}{4}\right] \leq \exp\left(-2\frac{2\lambda-2}{16}\right) = \mathrm{negl}(\lambda).$$

Next, consider the check that for less than $\frac{1}{2}+\frac{\epsilon}{2}-\lambda^{1/3}$ fraction of $i \in [2\lambda]\setminus P^*$ such that $c^k_{R,i} = c^k_i$, $a^k_{R,i} = a^k_i$. Conditioned on the above, we have that the number of such i is at least $(2\lambda-2)/4$. Due to the completeness of ToNC, each event $a^k_{R,i} = a^k_i$ is an independent Bernoulli random variable with success $\frac{1}{2}+\frac{\epsilon}{2}$. Thus, this check fails with probability bounded by the following Hoeffding inequality:

$$\Pr\left[\frac{\#\{i : c^k_{R,i} = c^k_i \wedge a^k_{R,i} = a^k_i\}}{\#\{i : c^k_{R,i} = c^k_i\}} < \frac{1}{2} + \frac{\epsilon}{2} - \lambda^{1/3}\right] \leq \exp\left(-2\frac{2\lambda-2}{4\lambda^{2/3}}\right) = \mathrm{negl}(\lambda).$$

It is easy to check that all other abort conditions happen with $\mathrm{negl}(\lambda)$ probability, so we can conclude that $r = r_b$ with probability at least $\frac{1}{2}+\frac{\epsilon}{2} - \mathrm{negl}(\lambda)$. □

Lemma 5.6 (Completeness). *Protocol 5.2 satisfies Completeness according to Definition 3.8.*

Proof. This follows directly from the correctness of the commitment scheme (Definition 3.3). □

Lemma 5.7 (Receiver security). *Protocol 5.2 satisfies Receiver security according to Definition 3.8 with* $\gamma = 0$.

Proof. This follows from the hiding of the commitment scheme (Definition 3.3). Indeed, the only information that S receives about b is masked by $\widehat{b}$, which is determined by x_{i^*}, x_{j^*} as well as public information in the transcript. S receives $x_{i^*} \oplus x_{j^*}$, which fixes x_{i^*}, x_{j^*} to either $\{00, 11\}$ or $\{01, 10\}$. In either case, $\widehat{b}$ (along with other public information) is determined by which of the two strings was committed to. By a standard hybrid argument, commitments to 00 and 11 can only be distinguished with $\mathrm{negl}(\lambda)$ advantage and likewise for commitments to 01 and 10. This completes the proof. □

Lemma 5.8 (Sender security). *Protocol 5.2 satisfies Sender security according to Definition 3.8 for any constant* $\delta' > 2\delta - \epsilon$.

Proof. Sender security for committed-bit OT has two requirements. The second follows directly from the binding of the commitment scheme (Definition 3.3), so it remains to establish the first.

We exhibit a reduction that takes any $(\widetilde{R}_{\mathsf{init}}, \widetilde{R})$ that has δ' advantage in the first part of sender security and produces a non-uniform commuting prover that has $\frac{1}{2}(\epsilon+\delta') - o(1)$ advantage in the soundness game of the ToNC. When $\delta' = 2\delta - \epsilon + \Omega(1)$, this yields an adversary with advantage $\delta + \Omega(1)$, a contradiction.

Our non-uniform ToNC prover $(P_{\mathsf{init}}, P_{\mathsf{Prep}}, P_0, P_1)$ is specified as follows, where P_{init} is a potentially-inefficient operation that runs prior to the beginning of the interaction with the verifier, and outputs a quantum state. Note that this model of non-uniform adversary with quantum advice is identical to the model where we allow P_{Prep} to be initialized with a (potentially inefficiently-computable) mixed state ρ.

$\underline{P_{\mathsf{init}}}$:

- Run the following loop until it succeeds:
  - Run $\mathsf{init}_R, \tau_{\mathsf{Setup}} \leftarrow \mathsf{Setup}\langle \widetilde{R}_{\mathsf{init}}, S(1^\lambda)\rangle$ and $\mathsf{td} := \mathsf{TrapGen}(\tau_{\mathsf{Setup}})$. Parse td as $\left\{x_i^k\right\}_{k\in[\lambda],i\in[2\lambda]}$.
  - Interact with $\widetilde{R}$ during the "answer commitment" phase of OT.
  - For each $k \in [\lambda], i \in [2\lambda]$, run $y_i^k := \mathsf{Ext}_{\mathsf{Com}}(\tau_i')$.
  - Interact with $\widetilde{R}$ during the "pair commitment", and "main loop" phases of OT up until the beginning of the k^*'th loop.
  - If there has not been an abort yet, then declare success and move on, otherwise try the loop again.

$\underline{P_{\mathsf{Prep}}}$:

- Sample $i^* \leftarrow [\lambda]$. For each $i \in [2\lambda]$, interact with $\widetilde{R}$ as V_{Prep} in the protocol

$$|\psi_i\rangle, \left(c_i^{k^*}, a_i^{k^*}\right) \leftarrow \langle \widetilde{R}, V_{\mathsf{Prep}}(1^\lambda)\rangle,$$

  except that for the i^*'th instance, P forwards the message to its own external challenger. Note that P knows $\left\{c_i^{k^*}, a_i^{k^*}\right\}_{i\neq i^*}$ but not $c_{i^*}^{k^*}, a_{i^*}^{k^*}$.

- Sample $z^{k^*} \leftarrow \{0,1\}^{2\lambda}$, send z^{k^*} to $\widetilde{R}$, and receive $\left\{\widehat{a}_i^{k^*}\right\}_{i\in[2\lambda]}$. Set $c_{R,i^*}^{k^*} := x_{i^*}^{k^*} \oplus z_{i^*}^{k^*}$ and $a_{R,i^*}^{k^*} := \widehat{a}_{i^*}^{k^*} \oplus y_{i^*}^{k^*}$.

$\underline{P_{c_{R,i^*}}}$

- In this case, the external challenge $c = c_{R,i^*}^{k^*}$.
- Output $a' := a_{R,i^*}^{k^*}$.

$\underline{P_{1-c_{R,i^*}}}$

- In this case, the external challenge $c = 1 - c_{R,i^*}^{k^*}$.
- In what follows, if there is an abort, then output a uniformly random bit.
- Set $c_{i^*}^{k^*} := c$ and for $i \in [2\lambda]$, set $c_{R,i}^{k^*} := x_i^{k^*} \oplus z_i^{k^*}$. Sample j^* uniformly at random such that $c_{R,i^*}^{k^*} \oplus c_{R,j^*}^{k^*} \neq c_{i^*}^{k^*} \oplus c_{j^*}^{k^*}$, meaning $c_{R,j^*}^{k^*} = c_{j^*}^{k^*}$, and set $P^* := \{i^*, j^*\}$. Partition the rest of $[2\lambda] \setminus P^*$ uniformly at random to form $\mathcal{P}$.
- Send $\mathcal{P}$ to $\widetilde{R}$, receive $\left\{x_{i,j}^{k^*}\right\}_{\{i,j\}\in\mathcal{P}}$, and abort if

$$\mathsf{Ver}_{\mathsf{Com}}\left(\mathsf{st}_{\mathsf{Com},\{i,j\}}^{k^*}, \tau_{\{i,j\}}^{k^*}, x_{i,j}\right) = \bot$$

  for any $\{i,j\} \in \mathcal{P}$. Send P^* to $\widetilde{R}$ and receive

$$x_i^{k^*}, \mathsf{st}_{\mathsf{Com},i}^{k^*}, x_j^{k^*}, \mathsf{st}_{\mathsf{Com},j}^{k^*}, y_i^{k^*}, \mathsf{st}'^{k^*}_{\mathsf{Com},i}, y_j^{k^*}, \mathsf{st}'^{k^*}_{\mathsf{Com},j}$$

  for each $\{i,j\} \in \mathcal{P} \setminus P^*$. Perform the remainder of the abort checks implemented by S.

- Send $\left\{c_{i^*}^{k^*}, c_{j^*}^{k^*}\right\}$ and $r_b := a_{j^*}^{k^*}$ to $\widetilde{R}$, and let r_{1-b} be $\widetilde{R}'s$ final output. Output $a' := r_{1-b}$.

Note that the operations P_0 and P_1 are commuting by definition, since one of them directly outputs a classical bit stored in memory. The fact that this adversary has advantage $\frac{1}{2}(\epsilon+\delta)-o(1)$ in guessing the external verifier's bit a^* follows from the following sequence of observations.

- $\widetilde{R}$'s view given by the reduction is the same as its view in its real interaction with S except that:
  - It is conditioned on not aborting (that is, causing S to abort) during the first k^*-1 runs of the main loop.
  - It potentially differs in the event that $x_{i^*,j^*}^{k^*} \neq x_{i^*}^{k^*} \oplus x_{j^*}^{k^*}$ but S does not abort in the k^*'th loop.

  Note that the probability that the above event occurs is $1/\lambda + \mathrm{negl}(\lambda) = o(1)$ due to the cut-and-choose on pair commitments and the binding of the commitment scheme.

- Note that, conditioned on S aborting, any adversary's advantage in the first part of sender security is exactly 0. Thus, since $\widetilde{R}$ has non-zero constant advantage, it has a non-zero constant probability of not aborting, and thus P_{init}'s loop will terminate in finite time. Moreover, since k^* is sampled uniformly at random, $\widetilde{R}$'s probability of aborting in the k^*'th loop *conditioned on not aborting in the first* k^*-1 *loops* is bounded by $1/\lambda = o(1)$. Finally, this also implies that $\widetilde{R}$'s advantage *conditioned on not aborting* must be at least δ.

- Since $z_{i^*}^{k^*}$ is uniformly random, $c^{k^*} = c_{R,i^*}^{k^*}$ with probability exactly $1/2$, and thus the prover runs $P_{c_{R,i^*}^{k^*}}$ and $P_{1-c_{R,i^*}^{k^*}}$ each with probability $1/2$.

- First condition on $c = c_{R,i^*}^{k^*}$. Due to the fact that S does not abort except with probability $o(1)$, the binding of the commitment scheme, and the fact that i^* is uniformly random conditioned on $c_{R,i^*}^{k^*} = c_{i^*}^{k^*}$, we have that $a' = a^*$ with advantage $\epsilon - o(1)$.

- Next condition on $c = 1 - c_{R,i^*}^{k^*}$. By the fact that $\widetilde{R}$'s advantage conditioned on not aborting is at least δ and the fact that $\widetilde{R}$'s view is consistent with its real view conditioned on not aborting except with probability $o(1)$, we have that conditioned on $c = 1 - c_{R,i^*}^{k^*}$, $a' = a^*$ with advantage $\delta - o(1)$.

□

6 Hardness amplification

6.1 Post-quantum hard-core measure theorem

Fix a deterministic predicate $P : \{0,1\}^n \to \{0,1\}$ and any randomized classical circuit $C(x,b)$ that is intended to output 1 when $b = P(x)$ and 0 otherwise. Theorem 3 in [HS11] (which is similar in spirit to Lemma 2.4 from [Hol05]) shows that one can *decompose* the input space relative to this particular C into a large "hard" subset of the domain $S \subseteq \{0,1\}^n$ of probability mass δ and its complement. That is, on S, C's acceptance probability is essentially *insensitive* to whether $b = P(x)$ or $b = 1 - P(x)$, meaning that flipping P on S is nearly indistinguishable to C. Moreover, one can convert C into an explicit predictor Q that recovers $P(x)$ with an overall success at least $1 - \delta/2$ on the entire domain.

We prove a variation of [HS11, Theorem 3] which differs in the following respects.

- **Post-quantum setting.** We allow the distinguisher C to be a *quantum* circuit, and thus the resulting predictor Q is quantum.
- **Arbitrary input distributions.** Rather than working only with the uniform distribution over $\{0,1\}^n$, we formulate the statement with respect to an arbitrary distribution $\mathcal{D}$ over inputs.
- **A measure rather than a hard set.** As a consequence of allowing a quantum distinguisher C, we construct a quantum predictor which maps a pair $(x, P(x))$ *probabilistically* to a bit. Since the predictor is non-deterministic, it does not immediately give rise to a hard subset. Instead, its prediction statistics constitute a *sub-distribution measure* of $\mathcal{D}$ (as in Definition 3.1) that designates the portion of the domain on which C is insensitive to flipping P. The measure is explicitly constructed in Corollary 6.3.

The measure vs. set discrepancy comes from the fact that the proof in [HS11] relies on derandomizing the distinguisher C through fixing a set R of random seeds. Evaluations of $C(x, r)$ on any $r \in R$ are used to compute a criterion which determines whether $x \in S$—thus S becomes a deterministic set. Such derandomization is impossible in our setting, where C is no longer classical. However, shifting to working with a measure enables recovering analogous results in this setting as well.

Next, we define a function that will be used in the Theorem's statement.

Definition. For parameters $\tau \in \mathbb{R}$ and $\xi > 0$, define

$$\mathrm{Soft}_{\tau,\xi}(t) := \begin{cases} 1, & t \le \tau - \xi, \\ \frac{\tau - t}{\xi}, & \tau - \xi < t < \tau, \\ 0, & t \ge \tau. \end{cases}$$

$\mathrm{Soft}_{\tau,\xi}(t) \in [0,1]$ and it is $1/\xi$-Lipschitz in t and also $1/\xi$-Lipschitz in τ (for each fixed t).

$\mathrm{Soft}_{\tau,\xi}(t)$ can be thought of as a "soft indicator" of being in the hard region: it is 1 when t is clearly below τ, it is 0 when t is above τ, and it interpolates linearly in a narrow boundary band.

Theorem 6.1 (A generalization of Theorem 3 in [HS11])**.** *Let there be:*

- *A function $n : \mathbb{N} \to \mathbb{N}$, such that $n(\lambda) = \mathrm{poly}(\lambda)$.*
- *A family of predicates $\{P_\lambda\}_{\lambda \in \mathbb{N}}$, where $P_\lambda : \{0,1\}^{n(\lambda)} \to \{0,1\}$.*
- *A family of distributions $\{\mathcal{D}_\lambda\}_{\lambda \in \mathbb{N}}$, where $\mathcal{D}_\lambda$ is over $\{0,1\}^{n(\lambda)}$, such that the following min-entropy condition holds: for $m(\lambda) := \max\{D_\lambda(z) \mid z \in \{0,1\}^{n(\lambda)}\}$, it holds that $m(\lambda) \le \mathrm{negl}(\lambda)$.*
- *A family of samplers $\{\mathsf{Samp}_\lambda\}_{\lambda \in \mathbb{N}}$ such that Samp_λ outputs $(x, P_\lambda(x))$ where x is sampled from D_λ. Samp runs in time $\mathrm{poly}(\lambda)$.*

Consider any function $\varepsilon : \mathbb{N} \to (0,1)$ satisfying $\varepsilon(\lambda) = 1/\mathrm{poly}(\lambda)$. Then there exists a uniform quantum polynomial-time oracle algorithm Gen *such that for every security parameter value λ and every quantum circuit*

$$\mathcal{C} : \{0,1\}^{n(\lambda)+1} \to \{0,1\},$$

on input $(\varepsilon(\lambda), 1^\lambda)$ and with oracle access to $\mathcal{C}$, Gen outputs:

- *A parameter $\xi > 0$ and a threshold $\tau \in [0, 1+\xi]$.*

- *Quantum circuits S, Q with oracle access to $\mathcal{C}$,*
- *a parameter $\delta \in [0,1]$,*

such that except with probability $\mathrm{negl}(\lambda)$ over measurements of $\mathsf{Gen}^{\mathcal{C}}$, the following properties hold[14]*. For $x \in \{0,1\}^{n(\lambda)}$ and $b \in \{0,1\}$ define the* pointwise gaps

$$p_x(b) \;:=\; \Pr[\mathcal{C}(x,b)=1], \qquad \Delta_x \;:=\; p_x(P(x)) - p_x(1-P(x)),$$

and define the global gap

$$\Delta \;:=\; \Pr_{x\leftarrow\mathcal{D}}[\mathcal{C}(x,P(x))=1] \;-\; \Pr_{x\leftarrow\mathcal{D}}[\mathcal{C}(x,1-P(x))=1] \;=\; \mathop{\mathbb{E}}_{x\leftarrow\mathcal{D}}[\Delta_x].$$

Additionally, denote

$$w_\tau(x) \;:=\; \mathrm{Soft}_{\tau,\xi}(\Delta_x) \in [0,1], \qquad \delta_\tau \;:=\; \mathop{\mathbb{E}}_{x\leftarrow\mathcal{D}}[w_\tau(x)].$$

1. ***(Correct mass).*** *For every fixed x,*

$$\Pr[S(x,P(x))=1] \;=\; w_\tau(x) \;\pm\; (\varepsilon/200 + \mathrm{negl}(\lambda)).$$

   Moreover, Gen*'s output δ satisfies $\delta_\tau - \epsilon/200 \le \delta \;\le\; \delta_\tau$.*

2. ***(Indistinguishability).*** *Let $P'(x)$ be the randomized predicate $P'(x) := P(x) \oplus S(x,P(x))$, then*

$$\left| \Pr_{x\leftarrow\mathcal{D}}[\mathcal{C}(x,P(x))=1] - \Pr_{x\leftarrow\mathcal{D}}[\mathcal{C}(x,P'(x))=1] \right| \;\le\; \varepsilon.$$

3. ***(Predictability).*** *The circuit Q satisfies*

$$\Pr_{x\leftarrow\mathcal{D}}[Q(x)=P(x)] \;\ge\; 1 - \frac{\delta}{2} - \mathrm{negl}(\lambda).$$

4. ***(Obliviousness).***

   The circuit $Q(x)$ can be written as $Q^{C(x,\cdot),C(\cdot,\cdot)}$. That is, the underlying oracle circuit Q is fixed and independent of x, and it utilizes x only within a fixed, x-independent procedure of oracle queries to $C(x,\cdot)$. In this sense, Q is oblivious to x.

There exist fixed polynomials $q(\cdot,\cdot)$ and $r(\cdot,\cdot)$ such that the oracle circuits S, Q:

- *make at most $q(\lambda, 1/\varepsilon)$ oracle calls to $\mathcal{C}$, and*
- *the remaining circuit has size at most $r(\lambda, 1/\varepsilon)$.*

Consequently, after hardwiring $\mathcal{C}$ and replacing each oracle gate by a copy of $\mathcal{C}$, the compiled circuit $\widehat{Q}$ satisfies

$$|\widehat{Q}| \;\le\; q(\lambda,1/\varepsilon)\cdot|\mathcal{C}| \;+\; r(\lambda,1/\varepsilon),$$

and similarly for $\widehat{S}$.

Proof. Fix λ. All probabilities over $\mathcal{C}, S, Q$ are over their internal measurements. Fix $\nu \le \mathrm{negl}(\lambda)$.

Given (x,b) and accuracy $\alpha > 0$, using Chernoff's bound, one can estimate $p_x(b)$ to within $\pm\alpha$ with failure probability at most ν by running $\mathcal{C}(x,b)$ independently

$$T = \Theta(\log(1/\nu)/\alpha^2)$$

times and taking the empirical mean. The same holds for the gap

$$\Delta_x^{(b)} := p_x(b) - p_x(1-b),$$

up to constant factors.

[14] Fix λ and suppress the subscript λ.

Normalizing the global gap. Using $\mathrm{poly}(\lambda, 1/\varepsilon)$ samples $(x, P(x)) \leftarrow \mathsf{Samp}$ and a constant number of calls to $\mathcal{C}$ per sample, estimate Δ to within $\pm\varepsilon/20$ except with probability $\mathrm{negl}(\lambda)$. If the estimate $\widehat{\Delta}$ satisfies $|\widehat{\Delta}| \le \varepsilon/10$, output $\delta := 1$, $\xi := \varepsilon^2/1000$, $\tau := 1 + \xi$, let S always output 1, and let Q output a uniform bit. All four conclusions are immediate. Otherwise, if $\widehat{\Delta} < -\varepsilon/10$, replace $\mathcal{C}$ by $1 - \mathcal{C}$. Henceforth assume

$$\Delta \ge \varepsilon/20.$$

Defining a function F. Fix

$$\xi := \varepsilon^2/1000.$$

For $\tau \in \mathbb{R}$, recall

$$w_\tau(x) := \mathrm{Soft}_{\tau,\xi}(\Delta_x)$$

and define the associated function

$$F(\tau) := \mathbb{E}_{x \leftarrow \mathcal{D}}\big[\Delta_x \cdot w_\tau(x)\big].$$

We will apply the intermediate value theorem on the interval $[0, 1 + \xi]$. First,

$$F(0) \le 0,$$

since for any x such that $w_0(x) \neq 0$, necessarily $\Delta_x < 0$. Second, for all $\Delta_x \in [-1, 1]$ we have $\mathrm{Soft}_{1+\xi,\xi}(\Delta_x) = 1$, hence

$$F(1 + \xi) = \mathbb{E}_{x \leftarrow \mathcal{D}}[\Delta_x] = \Delta.$$

The map $\tau \mapsto F(\tau)$ is continuous, and by Step 0 we have $\Delta \ge \varepsilon/20$. Therefore there exists $\tau^\star \in [0, 1 + \xi]$ such that

$$F(\tau^\star) = \frac{\varepsilon}{25}. \tag{8}$$

A mean-correct estimator for $F(\tau)$. Fix

$$\alpha := \xi\varepsilon/800.$$

For each sampled $(x, P(x))$, compute two *independent* estimates of Δ_x:

$$\widehat{\Delta}_x^{(A)} \quad \text{and} \quad \widehat{\Delta}_x^{(B)},$$

each satisfying $|\widehat{\Delta}_x^{(\cdot)} - \Delta_x| \le \alpha$, except with probability at most ν. Define

$$Y_\tau(x) := \widehat{\Delta}_x^{(B)} \cdot \mathrm{Soft}_{\tau,\xi}(\widehat{\Delta}_x^{(A)}) \in [-1, 1].$$

Let $X \sim \mathcal{D}$ and define $\mu_\tau := \mathbb{E}[Y_\tau(X)]$.

Lemma 6.2 (Mean correctness)**.** *For every $\tau \in \mathbb{R}$,*

$$|\mu_\tau - F(\tau)| \le \alpha/\xi + \nu.$$

Proof. Condition on $X = x$. Because $\widehat{\Delta}_x^{(B)}$ is an unbiased estimator of Δ_x conditioned on x and is independent of $\widehat{\Delta}_x^{(A)}$, we have

$$\mathbb{E}[Y_\tau(X) \mid X = x] = \Delta_x \cdot \mathbb{E}\Big[\mathrm{Soft}_{\tau,\xi}(\widehat{\Delta}_x^{(A)}) \,\Big|\, X = x\Big].$$

The function $t \mapsto \mathrm{Soft}_{\tau,\xi}(t)$ is $1/\xi$-Lipschitz, hence on the event $|\widehat{\Delta}_x^{(A)} - \Delta_x| \le \alpha$ we have

$$\left|\mathrm{Soft}_{\tau,\xi}(\widehat{\Delta}_x^{(A)}) - \mathrm{Soft}_{\tau,\xi}(\Delta_x)\right| \le \alpha/\xi.$$

This event fails with probability at most ν, and $\mathrm{Soft}_{\tau,\xi}(\cdot) \in [0,1]$. Therefore

$$\left|\mathbb{E}\Big[\mathrm{Soft}_{\tau,\xi}(\widehat{\Delta}_x^{(A)}) \mid X = x\Big] - \mathrm{Soft}_{\tau,\xi}(\Delta_x)\right| \le \alpha/\xi + \nu.$$

Multiplying by $|\Delta_x| \le 1$ and averaging over $x \sim \mathcal{D}$ yields the claim. □

Choosing τ. Choose a grid step

$$\rho := \xi\varepsilon/800$$

and define a grid

$$\mathcal{T} := \{j\rho : j = 0, 1, \ldots, N\} \cup \{1+\xi\}, \qquad N := \left\lfloor \frac{1+\xi}{\rho} \right\rfloor,$$

so that $\mathcal{T} \subseteq [0, 1+\xi]$. For each $\tau \in \mathcal{T}$, estimate μ_τ by sampling $m = \mathrm{poly}(\lambda, 1/\varepsilon)$ independent points from Samp, computing $Y_\tau(\cdot)$ for each point independently, and averaging:

$$\widehat{F}(\tau) := \frac{1}{m}\sum_{i=1}^{m} Y_\tau(x_i).$$

Output the smallest $\tau \in \mathcal{T}$ such that

$$\widehat{F}(\tau) \in \Big[\frac{\varepsilon}{100}, \frac{\varepsilon}{20}\Big]. \tag{9}$$

Hoeffding's bound (since each $Y_\tau \in [-1,1]$) implies that there exists $m = \mathrm{poly}(\lambda, 1/\varepsilon)$ such that $|\widehat{F}(\tau) - \mu_\tau| \le \varepsilon/800$ except with probability ν. Union bounding over $\tau \in \mathcal{T}$, and using Lemma 6.2, we obtain that except with probability $\mathrm{negl}(\lambda)$,

$$|\widehat{F}(\tau) - F(\tau)| \le |\widehat{F}(\tau) - \mu_\tau| + |\mu_\tau - F(\tau)| \le \varepsilon/400 + \nu \quad \text{for all } \tau \in \mathcal{T}. \tag{10}$$

Denote this *good* event by $\mathcal{G}$. We next argue that (9) has at least one solution. By (8) there exists $\tau^\star$ with $F(\tau^\star) = \varepsilon/25$. Since for each fixed t the map $\tau \mapsto \mathrm{Soft}_{\tau,\xi}(t)$ is $1/\xi$-Lipschitz, we have

$$|F(\tau) - F(\tau')| \le |\tau - \tau'|/\xi \quad \text{for all } \tau, \tau'.$$

Hence there exists $\widetilde{\tau} \in \mathcal{T}$ with

$$|F(\widetilde{\tau}) - F(\tau^\star)| \le \rho/\xi = \varepsilon/800.$$

Together with (10), this implies

$$\widehat{F}(\widetilde{\tau}) \in [\varepsilon/100, \varepsilon/20].$$

For any $\tau \in \mathcal{T}$ satisfying (9), on $\mathcal{G}$,

$$F(\tau) \ge \widehat{F}(\tau) - \varepsilon/400 - \nu \ge \varepsilon/100 - \varepsilon/400 - \nu = \frac{3\varepsilon}{400} - \nu \ge \frac{\varepsilon}{150} - \nu,$$

$$F(\tau) \le \widehat{F}(\tau) + \varepsilon/400 + \nu \le \varepsilon/20 + \varepsilon/400 + \nu \le \frac{\varepsilon}{10} + \nu.$$

Therefore, except with probability $\mathrm{negl}(\lambda)$, the τ output by $\mathsf{Gen}^{\mathcal{C}}$ satisfies (11):

$$\frac{\varepsilon}{150} - \nu \;\le\; F(\tau) \;\le\; \frac{\varepsilon}{10} + \nu \qquad \text{and} \qquad \tau \;\ge\; \frac{\varepsilon}{150} - \nu. \tag{11}$$

The lower bound on τ follows since on the support of w_τ we have $\Delta_x \le \tau$, hence

$$F(\tau) = \mathbb{E}[\Delta_x w_\tau(x)] \le \tau \cdot \mathbb{E}[w_\tau(X)] \le \tau.$$

Defining S and outputting δ. We define the circuit S:

A quantum circuit S

The circuit takes an input $(x, b) \in \{0,1\}^{n(\lambda)+1}$.

1. estimates $\Delta_x^{(b)} := p_x(b) - p_x(1-b)$ within $\pm\alpha$ except with probability $\mathrm{negl}(\lambda)$, obtaining $\widehat{\Delta}_x^{(b)}$;
2. outputs 1 with probability $\mathrm{Soft}_{\tau,\xi}(\widehat{\Delta}_x^{(b)})$.

Let

$$w(x) := \mathrm{Soft}_{\tau,\xi}(\Delta_x) \quad \text{and} \quad \delta_\tau := \mathbb{E}[w_\tau(X)].$$

Because $\mathrm{Soft}_{\tau,\xi}$ is $1/\xi$-Lipschitz, for every fixed x:

$$\Pr[S(x, P(x)) = 1 \mid x] = \mathrm{Soft}_{\tau,\xi}(\Delta_x) \pm (\alpha/\xi + \mathrm{negl}(\lambda)) = w_\tau(x) \pm (\varepsilon/800 + \mathrm{negl}(\lambda)). \tag{12}$$

Independently sample $m_\delta = \mathrm{poly}(n, 1/\varepsilon)$ points $x_1, \ldots, x_{m_\delta} \sim \mathcal{D}$ via Samp. For each x_i, estimate Δ_{x_i} within $\pm\alpha$ (except with probability $\mathrm{negl}(\lambda)$), obtaining $\widehat{\Delta}_{x_i}$, and form

$$Z_i := \mathrm{Soft}_{\tau,\xi}(\widehat{\Delta}_{x_i}) \in [0,1].$$

Let

$$\widehat{\delta} := \frac{1}{m_\delta} \sum_{i=1}^{m_\delta} Z_i.$$

Recall $\delta_\tau = \mathbb{E}_{X\sim\mathcal{D}}[w_\tau(X)]$. Conditioning on $x_i = x$, on the good event $|\widehat{\Delta}_x - \Delta_x| \le \alpha$ the $1/\xi$-Lipschitz property gives $\left|\mathrm{Soft}_{\tau,\xi}(\widehat{\Delta}_x) - \mathrm{Soft}_{\tau,\xi}(\Delta_x)\right| \le \alpha/\xi$, whereas on the bad event we have $\mathrm{Soft}_{\tau,\xi}(\cdot) \in [0,1]$. Hence

$$|\mathbb{E}[Z_i \mid x_i = x] - w(x)| = \left|\mathbb{E}[\mathrm{Soft}_{\tau,\xi}(\widehat{\Delta}_x) \mid x_i = x] - \mathrm{Soft}_{\tau,\xi}(\Delta_x)\right| \le \alpha/\xi + \nu,$$

and averaging over $x \sim \mathcal{D}$ yields

$$\left|\mathbb{E}[Z_i] - \delta_\tau\right| \le \alpha/\xi + \nu.$$

Moreover, since $Z_i \in [0,1]$ are i.i.d., Hoeffding's inequality implies that there exists $m_\delta = \mathrm{poly}(n, 1/\varepsilon)$ such that, except with probability ν,

$$\left|\widehat{\delta} - \mathbb{E}[Z_i]\right| \le \varepsilon/800.$$

Thus, by the triangle inequality, except with probability $\mathrm{negl}(\lambda)$,

$$|\widehat{\delta} - \delta_\tau| \le |\widehat{\delta} - \mathbb{E}[Z_i]| + |\,\mathbb{E}[Z_i] - \delta_\tau| \le \varepsilon/800 + \alpha/\xi + \nu \le \varepsilon/400 + \nu,$$

where we used $\alpha/\xi = \varepsilon/800$. Define

$$\delta := \max\{0,\ \widehat{\delta} - \varepsilon/400\}.$$

Then (except with probability $\mathrm{negl}(\lambda)$) we have $\delta \le \delta_\tau$ and

$$0 \le \delta_\tau - \delta \le \varepsilon/200,$$

hence also $|\delta - \delta_\tau| \le \varepsilon/200$.

Indistinguishability. Define

$$P'(x) := P(x) \oplus S(x, P(x))$$

By definition of P', for a fixed x,

$$\Pr[\mathcal{C}(x, P(x)) = 1] - \Pr[\mathcal{C}(x, P'(x)) = 1] = \Pr[S(x, P(x)) = 1 \mid x] \cdot \Delta_x.$$

Averaging over $x \sim \mathcal{D}$ gives

$$\Pr_{x\sim\mathcal{D}}[\mathcal{C}(x, P(x)) = 1] - \Pr_{x\sim\mathcal{D}}[\mathcal{C}(x, P'(x)) = 1] = \mathbb{E}_{x\sim\mathcal{D}}[\Delta_x \cdot \Pr[S(x, P(x)) = 1 \mid x]].$$

Due to (12), replacing $\Pr[S(x, P(x)) = 1 \mid x]$ by $w(x) = \mathrm{Soft}_{\tau,\xi}(\Delta_x)$ incurs an error smaller than $\varepsilon/200 + \mathrm{negl}(\lambda)$, hence the right-hand side equals $F(\tau) \pm (\varepsilon/200 + \mathrm{negl}(\lambda))$. Using (11), its absolute value is at most

$$\varepsilon/10 + \varepsilon/200 + \mathrm{negl}(\lambda) \le \varepsilon.$$

Predictability. Define

$$g_x := p_x(1) - p_x(0).$$

Then for every x,

$$g_x = (2P(x) - 1)\Delta_x, \qquad \text{equivalently} \qquad (2P(x) - 1)\, g_x = \Delta_x, \qquad |g_x| = |\Delta_x|.$$

A quantum circuit Q

The circuit takes an input $x \in \{0,1\}^{n(\lambda)}$.

1. Estimates g_x to within $\pm\alpha$ with failure probability at most $\nu \le \mathrm{negl}(\lambda)$, obtaining a random estimate $\widehat{g}_x$ satisfying
$$\Pr[\, |\widehat{g}_x - g_x| \le \alpha \;\mid\; x] \;\ge\; 1 - \nu. \tag{13}$$
2. Outputs a bit according to the following randomized rule (depending only on $\widehat{g}_x$):
$$Q(x) := \begin{cases} 1, & \widehat{g}_x \ge \tau, \\ 0, & \widehat{g}_x \le -\tau, \\ 1 \text{ with prob. } \frac{1}{2}\Big(1 + \frac{\widehat{g}_x}{\tau}\Big), & \text{otherwise.} \end{cases}$$

A Lipschitz bound. Fix x and $b \in \{0,1\}$. Define

$$\phi_b(t) \;:=\; \Pr[Q(x) = b \;\mid\; \widehat{g}_x = t].$$

By inspection, ϕ_b is piecewise linear with slope in $[-\frac{1}{2\tau}, \frac{1}{2\tau}]$; hence it is $1/(2\tau)$-Lipschitz :

$$|\phi_b(t) - \phi_b(t')| \;\le\; \frac{|t - t'|}{2\tau} \qquad \forall\, t, t' \in \mathbb{R}. \tag{14}$$

Let $\mathcal{E}_x := \{|\widehat{g}_x - g_x| \le \alpha\}$. On the event $\mathcal{E}_x$,

$$\phi_{P(x)}(\widehat{g}_x) \;\ge\; \phi_{P(x)}(g_x) - \frac{\alpha}{2\tau},$$

using (14). Taking expectation conditioned on x and $\mathcal{E}_x$ gives

$$\Pr[Q(x) = P(x) \mid x, \mathcal{E}_x] = \mathbb{E}[\phi_{P(x)}(\widehat{g}_x) \mid x, \mathcal{E}_x] \;\ge\; \phi_{P(x)}(g_x) - \frac{\alpha}{2\tau}.$$

Removing the conditioning on $\mathcal{E}_x$ incurs a loss of at most ν:

$$\Pr[Q(x) = P(x) \mid x] \;\ge\; \phi_{P(x)}(g_x) - \frac{\alpha}{2\tau} - \nu. \tag{15}$$

Exact success when $\widehat{g}_x = g_x$. Define the function $s_\tau : \mathbb{R} \to [0,1]$ by

$$s_\tau(u) \;:=\; \begin{cases} 1, & u \geq \tau, \\ \frac{1}{2}\left(1 + \frac{u}{\tau}\right), & |u| < \tau, \\ 0, & u \leq -\tau. \end{cases}$$

Observe that

$$\phi_{P(x)}(g_x) \;=\; s\big((2P(x)-1)g_x\big) \;=\; s_\tau(\Delta_x), \tag{16}$$

using $(2P(x)-1)g_x = \Delta_x$. Combining (15) and (16) yields, for every x,

$$\Pr[Q(x) = P(x) \mid x] \;\geq\; s_\tau(\Delta_x) - \frac{\alpha}{2\tau} - \nu. \tag{17}$$

A pointwise comparison using the soft weight. Assume, as ensured by our parameter choices in Step 3, that $\tau \geq \xi$. We claim that for every $\Delta_x \in [-1,1]$,

$$s_\tau(\Delta_x) \;\geq\; 1 - \frac{\mathrm{Soft}_{\tau,\xi}(\Delta_x)}{2} + \frac{\Delta_x \,\mathrm{Soft}_{\tau,\xi}(\Delta_x)}{2\tau} - \frac{\xi}{8\tau}. \tag{18}$$

Proof of (18). We consider three cases.

Case 1: $\Delta_x \geq \tau$. Then $\mathrm{Soft}_{\tau,\xi}(\Delta_x) = 0$ and the right-hand side equals $1 - \xi/(8\tau) \leq 1 = s_\tau(\Delta_x)$.

Case 2: $\Delta_x \leq \tau - \xi$. Then $\mathrm{Soft}_{\tau,\xi}(\Delta_x) = 1$ and the right-hand side is

$$\frac{1}{2}\left(1 + \frac{\Delta_x}{\tau}\right) - \frac{\xi}{8\tau}.$$

If $\Delta_x \leq -\tau$ then $s_\tau(\Delta_x) = 0$ and the inequality holds since the displayed quantity is ≤ 0. If $-\tau < \Delta_x \leq \tau - \xi$ then $s_\tau(\Delta_x) = \frac{1}{2}(1 + \Delta_x/\tau)$ and the inequality holds with slack $\xi/(8\tau)$.

Case 3: $\Delta_x \in (\tau - \xi, \tau)$. Write $u := \tau - \Delta_x \in (0, \xi)$. Then $\mathrm{Soft}_{\tau,\xi}(\Delta_x) = u/\xi$ and the right-hand side of (18) (without the $-\xi/(8\tau)$ term) equals

$$1 - \frac{u}{2\xi} + \frac{\Delta_x}{2\tau} \cdot \frac{u}{\xi} = 1 - \frac{u}{2\xi} + \frac{\tau - u}{2\tau} \cdot \frac{u}{\xi} = 1 - \frac{u^2}{2\tau\xi}.$$

Since $\tau \geq \xi$ and $u \in (0, \xi)$, we have $\Delta_x = \tau - u > 0$, hence $\Delta_x \in (-\tau, \tau)$ and therefore

$$s_\tau(\Delta_x) = \frac{1}{2}\left(1 + \frac{\Delta_x}{\tau}\right) = 1 - \frac{u}{2\tau}.$$

Thus,

$$s_\tau(\Delta_x) - \left(1 - \frac{u^2}{2\tau\xi}\right) = \frac{u}{2\tau}\left(\frac{u}{\xi} - 1\right) \geq -\frac{\xi}{8\tau},$$

because the minimum over $u \in [0, \xi]$ occurs at $u = \xi/2$ and equals $-\xi/(8\tau)$. This proves (18) in all cases. □

Combining (17) and (18) gives, for every x,

$$\Pr[Q(x) = P(x) \mid x] \geq 1 - \frac{w_\tau(x)}{2} + \frac{\Delta_x w_\tau(x)}{2\tau} - \frac{\xi}{8\tau} - \frac{\alpha}{2\tau} - \nu. \tag{19}$$

Averaging and concluding. Taking expectation of (19) over $x \leftarrow \mathcal{D}$ yields

$$\Pr_{x\sim\mathcal{D}}[Q(x) = P(x)] \geq 1 - \frac{\delta_\tau}{2} + \frac{F(\tau)}{2\tau} - \frac{\xi}{8\tau} - \frac{\alpha}{2\tau} - \nu,$$

since $\delta_\tau = \mathbb{E}[w(X)]$ and $F(\tau) = \mathbb{E}[\Delta_X w(X)]$.

Using the concrete choice $\alpha = \xi\varepsilon/800$ and $\varepsilon \leq 1$ without loss of generality, we have $\alpha \leq \xi/800$, and hence

$$\frac{\xi}{8\tau} + \frac{\alpha}{2\tau} \;\leq\; \frac{\xi}{8\tau} + \frac{\xi}{1600\tau} \;<\; \frac{\xi}{2\tau}. \tag{20}$$

Therefore,

$$\Pr_{x\sim\mathcal{D}}[Q(x) = P(x)] \geq 1 - \frac{\delta_\tau}{2} + \frac{F(\tau) - \xi}{2\tau} - \nu.$$

Finally, by Step 4 we have $0 \leq \delta_\tau - \delta \leq \varepsilon/200$ except with probability $\mathrm{negl}(\lambda)$, and by Step 3 we have $F(\tau) \geq \varepsilon/150$ and $\tau \leq 1 + \xi$. Since $\xi = \varepsilon^2/1000$, for all sufficiently large λ,

$$\frac{F(\tau) - \xi}{2\tau} \;\geq\; \frac{\varepsilon/150 - \varepsilon^2/1000}{2(1+\xi)} \;\geq\; \frac{\varepsilon}{400} \;\geq\; \frac{\delta_\tau - \delta}{2}.$$

Plugging this in gives

$$\Pr_{x\sim\mathcal{D}}[Q(x) = P(x)] \geq 1 - \frac{\delta_\tau}{2} + \frac{\delta_\tau - \delta}{2} - \nu = 1 - \frac{\delta}{2} - \nu,$$

which completes the predictability claim.

Obliviousness. The obliviousness property stems directly from the definition of Q.

Efficiency. All estimation steps use $\mathrm{poly}(\lambda, 1/\varepsilon)$ oracle calls to $\mathcal{C}$, and the grid has $\mathrm{poly}(\lambda, 1/\varepsilon)$ points. Thus Gen runs in $\mathrm{poly}(\lambda, 1/\varepsilon)$ time. By inspection, S and Q are obtained by composing a $\mathrm{poly}(\lambda, 1/\varepsilon)$-number of invocations of $\mathcal{C}$ arising only from the estimation subroutines, with $\mathrm{poly}(\lambda, 1/\varepsilon)$ additional non-oracle computation. Hence there exist fixed polynomials $q(\cdot,\cdot)$ and $r(\cdot,\cdot)$ such that S and Q make at most $q(\lambda, 1/\varepsilon)$ oracle calls to $\mathcal{C}$ and have non-oracle size at most $r(\lambda, 1/\varepsilon)$. Therefore, the compiled circuits satisfy $|\widehat{Q}| \leq q(\lambda, 1/\varepsilon) \cdot |\mathcal{C}| + r(\lambda, 1/\varepsilon)$, and similarly for $\widehat{S}$.

□

Next, we state and prove a corollary of Theorem 6.1.

Corollary 6.3. *Let $\lambda \in \mathbb{N}$ and let $n = n(\lambda) = \mathrm{poly}(\lambda)$. Let D_λ be a distribution over $\mathcal{X}_\lambda \times \{0,1\}$ where $\mathcal{X}_\lambda := \{0,1\}^n$, and assume D_λ is samplable in $\mathrm{poly}(\lambda)$ time. Write $(X, B) \leftarrow D_\lambda$. Assume the following min-entropy condition:*

$$m(\lambda) \;:=\; \max_{x\in\mathcal{X}_\lambda} \Pr_{D_\lambda}[X = x] \;=\; \mathrm{negl}(\lambda).$$

Let $\delta = \delta(\lambda) \in (0,1)$ and let $s(\lambda)$ be a circuit size bound. Suppose that for every uniform (resp. non-uniform) quantum circuit $Q : \mathcal{X}_\lambda \to \{0,1\}$ of size at most $s(\lambda)$,

$$\Pr_{(X,B)\leftarrow D_\lambda}[Q(X) = B] \;\leq\; 1 - \frac{\delta}{2}.$$

Fix any $\epsilon = \epsilon(\lambda) = 1/\mathrm{poly}(\lambda)$ with $\epsilon \le \delta/2$. Let $\varepsilon := \delta\epsilon$, and let $C : \mathcal{X}_\lambda \to \{0,1\}$ be a uniform (resp. non-uniform) quantum circuit such that

$$q\Big(\lambda, \tfrac{1}{\varepsilon}\Big) \cdot (|C| + n) \;+\; r\Big(\lambda, \tfrac{1}{\varepsilon}\Big) \;\le\; s(\lambda), \tag{21}$$

where $r(\cdot,\cdot), q(\cdot,\cdot)$ are the polynomials defined in the statement of Theorem 6.1. Then, there exists a measure $M_\lambda \preceq D_\lambda$ with total mass $\mu(M_\lambda) \ge \delta - \epsilon$ such that

$$\Pr_{(X,B)\leftarrow M_\lambda}\big[C(X) = B\big] \;\le\; \frac{1}{2} + 2\epsilon,$$

where $(X, B) \leftarrow M_\lambda$ denotes sampling from the normalized distribution $M_\lambda/\mu(M_\lambda)$.

Proof. Fix λ and suppress the subscript λ.

Define a deterministic predicate. Define the lifted domain $\mathcal{X}' := \mathcal{X} \times \{0,1\}$ and define the deterministic predicate $P : \mathcal{X}' \to \{0,1\}$ by

$$P(x, b_0) \;:=\; b_0.$$

A sampler for $(X', P(X'))$ is immediate: sample $(x, b_0) \leftarrow D$ and output $\big((x, b_0), b_0\big)$.

Build an oracle circuit for Theorem 6.1. Given the predictor $C : \mathcal{X} \to \{0,1\}$, define a quantum circuit

$$\mathcal{C} : \mathcal{X}' \times \{0,1\} \to \{0,1\}$$

that on input $\big((x, b_0), b\big)$ outputs 1 iff $C(x) = b$. Crucially, $\mathcal{C}$ ignores b_0.

Invoke $\mathsf{Gen}^{\mathcal{C}}(\varepsilon, 1^\lambda)$ from Theorem 6.1 on the distribution D with the accuracy parameter set to $\varepsilon := \delta\epsilon$, obtaining ξ, τ, circuits S, Q with oracle access to $\mathcal{C}$, and an output parameter δ_{out}. Importantly, D meets the min-entropy condition in the statement of Theorem 6.1. With probability $1 - \mathrm{negl}(\lambda)$, the properties correct mass, indistinguishability, predictability, and obliviousness all hold.

As in Theorem 6.1, let the pointwise gaps be

$$p_{x'}(b) := \Pr[\mathcal{C}(x', b) = 1], \qquad \Delta_{x'} := p_{x'}(P(x')) - p_{x'}(1 - P(x')).$$

For $x' = (x, b_0)$ we have

$$p_{(x,b_0)}(b) = \Pr[C(x) = b], \qquad \Delta_{(x,b_0)} = \Pr[C(x) = b_0] - \Pr[C(x) = 1 - b_0] = 2\Pr[C(x) = b_0] - 1.$$

Define the soft weight and its mean:

$$w_\tau(x') := \mathrm{Soft}_{\tau,\xi}(\Delta_{x'}) \in [0,1], \qquad \delta_\tau := \mathop{\mathbb{E}}_{X'\sim\mathcal{D}}\big[w_\tau(X')\big].$$

Define a measure M. Note that for any x', $0 \le w_\tau(x') \le 1$. Define the measure $M \preceq D$ by

$$M(x, b) \;:=\; D(x, b) \cdot w_\tau(x, b). \tag{22}$$

Then, the total mass of M is as follows

$$\mu(M) = \sum_{x,b} M(x, b) = \mathop{\mathbb{E}}_{X'\sim\mathcal{D}}[w_\tau(X')] = \delta_\tau. \tag{23}$$

Lower bound the total mass $\mu(M)$. We claim $\delta_\tau \geq \delta - \epsilon$. By the *correct mass* property from Theorem 6.1, except with negligible probability,

$$\delta_{\mathsf{out}} \leq \delta_\tau \qquad \text{and} \qquad |\delta_{\mathsf{out}} - \delta_\tau| \leq \varepsilon/200.$$

Hence it suffices to show $\delta_{\mathsf{out}} \geq \delta - \epsilon$.

Assume toward contradiction that $\delta_{\mathsf{out}} < \delta - \epsilon$ and that the Theorem 6.1 guarantees hold. By the *predictability* property from Theorem 6.1,

$$\Pr_{X' \sim \mathcal{D}}[Q(X') = P(X')] \geq 1 - \frac{\delta_{\mathsf{out}}}{2} - \mathrm{negl}(\lambda) > 1 - \frac{\delta}{2} + \frac{\epsilon}{2} - \mathrm{negl}(\lambda).$$

Define $\widetilde{Q} : \mathcal{X} \to \{0,1\}$ by $\widetilde{Q}(x) := Q((x,0))$. We claim that for every $(x, b_0) \in \mathcal{X}'$,

$$\Pr[Q((x,b_0)) = b_0] = \Pr[Q((x,0)) = b_0]. \tag{24}$$

Indeed, by *obliviousness* of Q (Theorem 6.1), on any input $x' = (x, b_0)$ the circuit Q utilizes x only within a fixed, x-independent procedure of oracle queries to $C(x, \cdot)$.

Since $\mathcal{C}((x,b_0),\cdot)$ ignores b_0, the joint distribution of oracle answers returned to Q is identical for inputs $(x,0)$ and $(x,1)$. Therefore the output distribution of $Q((x,b_0))$ is the same as that of $Q((x,0))$, establishing (24). Averaging (24) over $(X,B) \sim D$ yields

$$\Pr_{(X,B)\sim D}[Q((X,B)) = B] = \Pr_{(X,B)\sim D}[Q((X,0)) = B] = \Pr_{(X,B)\sim D}[\widetilde{Q}(X) = B].$$

Consequently,

$$\Pr_{(X,B)\sim D}[\widetilde{Q}(X) = B] = \Pr_{X'\sim\mathcal{D}}[Q(X') = P(X')] > 1 - \frac{\delta}{2} + \frac{\epsilon}{2} - \mathrm{negl}(\lambda).$$

Size of the compiled predictor. We now argue that $\widetilde{Q}$ can be realized by a (non-oracle) quantum circuit of size at most $s(\lambda)$. Recall that Q is produced by invoking Theorem 6.1 on the oracle circuit $\mathcal{C}$ with accuracy parameter $\varepsilon = \delta\epsilon$.

By Theorem 6.1, the circuit Q makes at most $q(\lambda, 1/\varepsilon)$ oracle calls to $\mathcal{C}$ on any input and has non-oracle size at most $r(\lambda, 1/\varepsilon)$. By hardwiring $\mathcal{C}$ and replacing each oracle gate by a copy of $\mathcal{C}$, we obtain an explicit (non-oracle) circuit $\widehat{Q}$ of size at most

$$|\widehat{Q}| \leq q(\lambda, 1/\varepsilon) \cdot |\mathcal{C}| + r(\lambda, 1/\varepsilon).$$

In our construction, $\mathcal{C}$ on input $((x,b_0),b)$ evaluates $C(x)$ and compares it to b while ignoring b_0, and hence

$$|\mathcal{C}| \leq |C| + n.$$

Therefore, the size condition (21) implies $|\widehat{Q}| \leq s(\lambda)$. This contradicts the assumed hardness of D against size-$s(\lambda)$ circuits. Therefore $\delta_{\mathsf{out}} \geq \delta - \epsilon$, and since $\delta_{\mathsf{out}} \leq \delta_\tau$ we get

$$\mu(M) = \delta_\tau \geq \delta - \epsilon. \tag{25}$$

An upper bound on the success of C on M. We analyze C under the normalized distribution $M/\mu(M)$. Using $\Delta_{(x,b)} = 2\Pr[C(x) = b] - 1$, we have

$$\Pr_{(X,B)\leftarrow M}[C(X) = B] = \frac{1}{2} + \frac{1}{2} \cdot \mathop{\mathbb{E}}_{(X,B)\leftarrow M}[\Delta_{(X,B)}] = \frac{1}{2} + \frac{1}{2\delta_\tau} \cdot \mathop{\mathbb{E}}_{(X,B)\sim D}[\Delta_{(X,B)}\, w_\tau(X,B)]. \tag{26}$$

where the last equality stems from (22) and (23). Let $F(\tau) := \mathbb{E}_{X'\sim\mathcal{D}}[\Delta_{X'}\, w_\tau(X')]$, as in the proof of Theorem 6.1. Let $P'(x') := P(x') \oplus S(x', P(x'))$. Fixing x', we get

$$\begin{aligned}\Pr[\mathcal{C}(x', P(x')) = 1 \mid x'] - \Pr[\mathcal{C}(x', P'(x')) = 1 \mid x'] = \\ \Pr[P'(x') = 1 - P(x')] \cdot (\Pr[\mathcal{C}(x', P(x')) = 1 \mid x'] - \Pr[\mathcal{C}(x', 1 - P(x')) = 1 \mid x']) = \\ \Pr[S(x', P(x')) = 1 \mid x'] \cdot \Delta_{x'}.\end{aligned}$$

Averaging over $X' \sim \mathcal{D}$ and using the *indistinguishability* property from Theorem 6.1 gives

$$A := \left| \mathop{\mathbb{E}}_{X'\sim\mathcal{D}}\Big[\Delta_{X'} \cdot \Pr[S(X', P(X')) = 1 \mid X']\Big] \right| \;\le\; \varepsilon. \tag{27}$$

By the *correct mass* property from Theorem 6.1, for each fixed x' we have

$$\Pr[S(x', P(x')) = 1 \mid x'] = w_\tau(x') \pm (\varepsilon/200 + \mathrm{negl}(\lambda)).$$

Combining with (27) and observing that $|\Delta_{x'}| \le 1$,

$$|F(\tau)| \;=\; |\mathop{\mathbb{E}}_{X'\sim\mathcal{D}}[\Delta_{X'}\, w_\tau(X')]| \;\le\; A + \varepsilon/200 + \mathrm{negl}(\lambda) \;\le\; \varepsilon + \varepsilon/200 + \mathrm{negl}(\lambda) \;\le\; 2\varepsilon$$

for all sufficiently large λ. From (26) we have the identity

$$\Pr_{(X,B)\leftarrow M}[C(X) = B] = \frac{1}{2} + \frac{1}{2\delta_\tau} \cdot F(\tau),$$

Because $\delta_\tau > 0$ this results in the first inequality below:

$$\Pr_{(X,B)\leftarrow M}[C(X) = B] \;\le\; \frac{1}{2} + \frac{|F(\tau)|}{2\delta_\tau} \;\le\; \frac{1}{2} + \frac{2\varepsilon}{2(\delta - \epsilon)} \;=\; \frac{1}{2} + \frac{\delta\epsilon}{\delta - \epsilon} \;\le\; \frac{1}{2} + 2\epsilon.$$

Here, the second inequality relies on (25), and the last inequality uses $\epsilon \le \delta/2$, so $\delta/(\delta - \epsilon) \le 2$. This completes the proof. □

In the next proof, we make use of the following lemma.

Lemma 6.4 ([BSW03])**.** *Let D be a distribution on $\{0,1\}^n$, F be a set of functions $f : \{0,1\}^n \to [-1,1]$, and $\overline{f}$ be a convex combination of functions from F. Then for any $\epsilon \in (0,1)$ and for some $k \le n/2\epsilon^2$, there exist functions $f_1, \ldots, f_k$ such that*

$$\max_{x\in\{0,1\}^n} \left| \overline{f}(x) - \left(\frac{1}{k} \sum_{i=1}^{k} f_i(x) \right) \right| \le \epsilon.$$

Remark 6.5. *We note that Lemma 6.4 does not guarantee that the functions $f_1, \ldots, f_k$ can be computed efficiently given $\overline{f}$. Therefore, the following theorems we prove in this section, which all rely on Lemma 6.4, are stated in the non-uniform security model.*

Lemma 6.6 (Minimax fixing lemma)**.** *Let $\{D_\lambda\}_{\lambda\in\mathbb{N}}$ be a family of distributions over $\{0,1\}^{n(\lambda)}\times\{0,1\}$. Fix functions $\alpha(\lambda)\in(0,1]$ and $\gamma(\lambda)\in(0,1)$, and a size bound $t(\lambda)$.*

Assume that for all sufficiently large λ, for every measure $M_\lambda \preceq D_\lambda$ with $\mu(M_\lambda)\geq\alpha(\lambda)$, there exists a quantum circuit Q'_λ of size at most $t(\lambda)$ such that

$$\Pr_{(X,B)\leftarrow M_\lambda}\big[\,Q'(X)=B\,\big] \;>\; \frac{1}{2}+\gamma(\lambda).$$

Define

$$t''(\lambda) \;:=\; \Big(\frac{n(\lambda)}{\gamma(\lambda)^2}+1\Big)\cdot t(\lambda) \;+\; \log\Big(\frac{n(\lambda)+1}{\gamma(\lambda)^2}\Big).$$

Then for all sufficiently large λ, there exists a quantum circuit Q''_λ of size at most $t''(\lambda)$ such that for every measure $M_\lambda \preceq D_\lambda$ with $\mu(M_\lambda)\geq\alpha(\lambda)$,

$$\Pr_{(X,B)\leftarrow M_\lambda}\big[\,Q''_\lambda(X)=B\,\big] \;>\; \frac{1}{2}+\frac{\gamma(\lambda)}{2}.$$

Proof. Fix $\lambda\in\mathbb{N}$ and suppress it from the notation.

Mass-normalization. Throughout this proof, the notation $(X,B)\leftarrow M$ denotes sampling from the *normalized* distribution $M/\mu(M)$, so $\mathbb{E}_{(x,b)\leftarrow M}[\cdot]$ is not linear in M. To apply minimax, we may w.l.o.g. restrict Bob to measures of *exact* mass α. Indeed, for any measure $M\preceq D$ with $\mu(M)\geq\alpha$, define the scaled measure

$$\widetilde{M} \;:=\; \frac{\alpha}{\mu(M)}\cdot M.$$

Then $\widetilde{M}\preceq D$, $\mu(\widetilde{M})=\alpha$, and the normalized distributions coincide:

$$\frac{\widetilde{M}}{\mu(\widetilde{M})} \;=\; \frac{M}{\mu(M)}.$$

Hence, for every circuit Q,

$$\Pr_{(X,B)\leftarrow M}[Q(X)=B] \;=\; \Pr_{(X,B)\leftarrow \widetilde{M}}[Q(X)=B]. \tag{28}$$

Therefore, the lemma's assumption and desired conclusion are unchanged if we quantify Bob only over

$$R_\alpha \;:=\; \{\, M\preceq D \mid \mu(M)=\alpha\,\}.$$

Note that R_α is nonempty (since $\alpha D\in R_\alpha$), convex, and compact when identified with a subset of $\mathbb{R}^{\{0,1\}^n\times\{0,1\}}$.

The game. For any circuit Q', define the function $g_{Q'}:\{0,1\}^n\times\{0,1\}\to[-1,1]$ by

$$g_{Q'}(x,b) \;:=\; 2\Pr[Q'(x)=b]-1 \;=\; \Pr[Q'(x)=b]-\Pr[Q'(x)=1-b].$$

Then for any measure M,

$$\mathop{\mathbb{E}}_{(x,b)\leftarrow M}[g_{Q'}(x,b)] \;=\; 2\Pr_{(x,b)\leftarrow M}[Q'(x)=b]-1.$$

Consider the following zero-sum game between Alice and Bob. Alice chooses a circuit Q' of size at most t; Bob chooses a measure $M \in R_\alpha$; and Alice's payoff is

$$\Pi(Q', M) \;:=\; \frac{1}{\alpha} \sum_{x,b} M(x,b) \cdot g_{Q'}(x,b) \qquad \text{for } M \in R_\alpha.$$

For $M \in R_\alpha$ we have $\Pi(Q', M) = \mathbb{E}_{(x,b)\leftarrow M}[g_{Q'}(x,b)]$, and $\Pi(Q', \cdot)$ is linear in M on R_α. By the lemma assumption, for every $M \in R_\alpha$ there exists a circuit Q' of size at most t such that

$$\Pr_{(X,B)\leftarrow M}[Q'(X) = B] \;>\; \frac{1}{2} + \gamma,$$

and hence

$$\Pi(Q', M) \;=\; 2 \Pr_{(X,B)\leftarrow M}[Q'(X) = B] - 1 \;>\; 2\gamma.$$

Equivalently,

$$\min_{M \in R_\alpha} \; \max_{Q' :\, |Q'| \le t} \Pi(Q', M) \;>\; 2\gamma.$$

Minimax. Apply von Neumann's minimax theorem with Alice's finite action set being the set of size-t circuits (with a finite universal gate set), Bob's action set $Y = R_\alpha$ (compact convex), and payoff $u(Q', M) = \Pi(Q', M)$ (affine in M). We obtain a mixed strategy for Alice, i.e. a distribution over size-t circuits which we denote $\overline{Q}$, such that for all $M \in R_\alpha$,

$$\mathbb{E}_{Q' \sim \overline{Q}}\big[\Pi(Q', M)\big] \;>\; 2\gamma.$$

Define the (pointwise) averaged payoff function

$$g_{\overline{Q}}(x,b) \;:=\; \mathbb{E}_{Q' \sim \overline{Q}}\big[g_{Q'}(x,b)\big].$$

By linearity,

$$\mathbb{E}_{Q' \sim \overline{Q}}\big[\Pi(Q', M)\big] \;=\; \frac{1}{\alpha} \sum_{x,b} M(x,b)\, g_{\overline{Q}}(x,b) \;=\; \mathbb{E}_{(x,b)\leftarrow M}\big[g_{\overline{Q}}(x,b)\big],$$

so we have for every $M \in R_\alpha$,

$$\mathbb{E}_{(x,b)\leftarrow M}\big[g_{\overline{Q}}(x,b)\big] \;>\; 2\gamma. \tag{29}$$

Sparsifying the mixed strategy. Note that $g_{Q'}(x,1) = -g_{Q'}(x,0)$ for every x, since $\Pr[Q'(x) = 0] + \Pr[Q'(x) = 1] = 1$. Define the one-argument function $h_{Q'} : \{0,1\}^n \to [-1,1]$ by

$$h_{Q'}(x) \;:=\; g_{Q'}(x,0),$$

so that for all (x,b),

$$g_{Q'}(x,b) \;=\; (1-2b)\, h_{Q'}(x).$$

Define $h_{\overline{Q}}(x) := \mathbb{E}_{Q' \sim \overline{Q}}[h_{Q'}(x)]$; then $g_{\overline{Q}}(x,b) = (1-2b)\, h_{\overline{Q}}(x)$.

Now apply Lemma 6.4 to the convex combination $h_{\overline{Q}}$ over the domain $\{0,1\}^n$: there exist circuits $Q'_1, \ldots, Q'_k$ of size at most t with

$$k \;\le\; \left\lceil \frac{n}{\gamma^2} \right\rceil$$

such that

$$\max_{x\in\{0,1\}^n}\left|h_{\overline{Q}}(x) \;-\; \frac{1}{k}\sum_{i=1}^{k} h_{Q'_i}(x)\right| \;\le\; \gamma.$$

Multiplying by $(1-2b)\in\{\pm 1\}$ shows that, for all (x,b),

$$\left|g_{\overline{Q}}(x,b) \;-\; \frac{1}{k}\sum_{i=1}^{k} g_{Q'_i}(x,b)\right| \;\le\; \gamma.$$

Define Q'' as follows: on input x, sample $i\leftarrow[k]$ uniformly and output $Q'_i(x)$. Then for every (x,b) we have

$$g_{Q''}(x,b) \;=\; \frac{1}{k}\sum_{i=1}^{k} g_{Q'_i}(x,b),$$

and hence for every $M\in R_\alpha$,

$$\mathop{\mathbb{E}}_{(x,b)\leftarrow M}[g_{Q''}(x,b)] \;\ge\; \mathop{\mathbb{E}}_{(x,b)\leftarrow M}[g_{\overline{Q}}(x,b)] \;-\; \gamma \;>\; 2\gamma-\gamma \;=\; \gamma,$$

where the strict inequality uses (29).

Extending back to all $\mu(M)\ge\alpha$. Let

$$R \;:=\; \{\, M \preceq D \mid \mu(M)\ge\alpha \,\}.$$

For any $M\in R$, let $\widetilde{M}=\frac{\alpha}{\mu(M)}M\in R_\alpha$. By (28), sampling from M or $\widetilde{M}$ yields the same normalized distribution, so the same success probability for Q''. Therefore, for every $M\in R$,

$$\Pr_{(x,b)\leftarrow M}[Q''(x)=b] \;=\; \frac{1}{2}+\frac{1}{2}\mathop{\mathbb{E}}_{(x,b)\leftarrow M}[g_{Q''}(x,b)] \;>\; \frac{1}{2}+\frac{\gamma}{2}.$$

Size bound. By construction, Q'' can be implemented by wiring in the k circuits $Q'_1,\dots,Q'_k$ and using $\log k$ bits to sample i; thus

$$|Q''| \;\le\; k\cdot t \;+\; \log k.$$

With $k\le\lceil n/\gamma^2\rceil$, we have $k\le n/\gamma^2+1$, and since $\gamma\in(0,1)$,

$$\log k \;\le\; \log\Big(\frac{n}{\gamma^2}+1\Big) \;\le\; \log\Big(\frac{n+1}{\gamma^2}\Big).$$

Hence

$$|Q''| \;\le\; \Big(\frac{n}{\gamma^2}+1\Big)\cdot t \;+\; \log\Big(\frac{n+1}{\gamma^2}\Big) \;=\; t'',$$

as required. □

Theorem 6.7 (Post-quantum hard-core measure). *Let $\{D_\lambda\}_{\lambda\in\mathbb{N}}$ be a family of distributions over $\{0,1\}^{n(\lambda)}\times\{0,1\}$ that are sampleable in time $\mathrm{poly}(\lambda)$, and assume the min-entropy condition*

$$\max_{(x,b)\in\{0,1\}^{n(\lambda)}\times\{0,1\}} D_\lambda(x,b) \;\le\; \mathrm{negl}(\lambda).$$

Fix a function $\delta(\lambda) \in (0,1)$ and a size bound $s(\lambda)$. Let $q(\cdot,\cdot)$ and $r(\cdot,\cdot)$ be the polynomials from Theorem 6.1. Assume that for all sufficiently large λ, for every quantum circuit $Q : \{0,1\}^{n(\lambda)} \to \{0,1\}$ of size at most $s(\lambda)$,

$$\Pr_{(X,B)\leftarrow D_\lambda}\big[\,Q(X) = B\,\big] \;\le\; 1 - \frac{\delta(\lambda)}{2}.$$

Let $\gamma(\lambda)$ be any function such that $\gamma(\lambda) \in [1/\mathrm{poly}(\lambda), \delta(\lambda)]$, and define

$$\epsilon(\lambda) \;:=\; \frac{\gamma(\lambda)}{4}, \qquad \varepsilon(\lambda) \;:=\; \delta(\lambda)\cdot\epsilon(\lambda) \;=\; \frac{\delta(\lambda)\gamma(\lambda)}{4},$$

and

$$s''(\lambda) \;:=\; \left\lfloor \frac{s(\lambda) - r(\lambda, 1/\varepsilon(\lambda))}{q(\lambda, 1/\varepsilon(\lambda))} \right\rfloor - n(\lambda), \qquad s'(\lambda) \;:=\; \left\lfloor \frac{\gamma(\lambda)^2}{4\,n(\lambda)} \cdot s''(\lambda) \right\rfloor.$$

Then for all sufficiently large λ, there exists a measure $M_\lambda \preceq D_\lambda$ such that

$$\mu(M_\lambda) \;\ge\; \delta(\lambda) - \epsilon(\lambda) \;=\; \delta(\lambda) - \frac{\gamma(\lambda)}{4},$$

and for every quantum circuit $Q' : \{0,1\}^{n(\lambda)} \to \{0,1\}$ of size at most $s'(\lambda)$,

$$\Pr_{(X,B)\leftarrow M_\lambda}\big[\,Q'(X) = B\,\big] \;\le\; \frac{1}{2} + \gamma(\lambda).$$

Proof. Fix a sufficiently large security parameter λ and suppress it from the notation. Write $n := n(\lambda)$, $\delta := \delta(\lambda)$, $\gamma := \gamma(\lambda)$, $\epsilon := \gamma/4$, and $\varepsilon := \delta\epsilon = \delta\gamma/4$. Note that $0 < \gamma < \delta < 1$ and also $n \ge 1$: indeed, if $n = 0$ then the domain has size 2 and hence $\max_{x,b} D(x,b) \ge 1/2$, contradicting $\max_{x,b} D(x,b) \le \mathrm{negl}(\lambda)$. We first dispose of the degenerate case $s' \le 0$.

Case 1: $s' < 0$. Then there is no circuit of size at most s', so the prediction condition is vacuous. Take $M := (\delta - \epsilon)\cdot D$. Then $M \preceq D$ and $\mu(M) = \delta - \epsilon$, as required.

Case 2: $s' = 0$. Let $p_b := \Pr_{(X,B)\leftarrow D}[B = b]$ for $b \in \{0,1\}$. By the hypothesis of the theorem (applied to the constant circuits of size 0),

$$p_b = \Pr_{(X,B)\leftarrow D}[Q_b(X) = B] \;\le\; 1 - \frac{\delta}{2} \qquad \text{for} \qquad Q_b(x) \equiv b.$$

Hence $p_{1-b} = 1 - p_b \ge \delta/2$, so in fact $p_0, p_1 \ge \delta/2$. Define a measure $M \preceq D$ by reweighting labels:

$$M(x,b) \;:=\; \frac{\delta - \epsilon}{2p_b}\, D(x,b) \qquad b \in \{0,1\}.$$

Since $p_b \ge \delta/2 \ge (\delta-\epsilon)/2$, we have $(\delta-\epsilon)/(2p_b) \le 1$, and therefore $M \preceq D$. Moreover,

$$\mu(M) = \sum_{b\in\{0,1\}} \sum_x M(x,b) = \sum_{b\in\{0,1\}} \frac{\delta-\epsilon}{2p_b} \sum_x D(x,b) = \sum_{b\in\{0,1\}} \frac{\delta-\epsilon}{2p_b}\, p_b = \delta - \epsilon.$$

Finally, under M the label is perfectly balanced:

$$\Pr_{(X,B)\leftarrow M}[B = b] = \frac{\sum_x M(x,b)}{\mu(M)} = \frac{(\delta-\epsilon)/2}{\delta-\epsilon} = \frac{1}{2}.$$

Thus any size-0 circuit is constant and succeeds with probability exactly $1/2$, which is at most $1/2 + \gamma$. This establishes the theorem when $s' = 0$.

Case 3: $s' \geq 1$**.** Assume towards contradiction that for every measure $M \preceq D$ with $\mu(M) \geq \delta - \epsilon$ there exists a quantum circuit Q' of size at most s' such that

$$\Pr_{(X,B)\leftarrow M}[Q'(X) = B] \;>\; \frac{1}{2} + \gamma. \tag{30}$$

Apply Lemma 6.6 with parameters $\alpha := \delta - \epsilon$, $t := s'$, and γ (as above). We obtain a single quantum circuit Q'' such that for all measures $M \preceq D$ with $\mu(M) \geq \delta - \epsilon$,

$$\Pr_{(X,B)\leftarrow M}[Q''(X) = B] \;>\; \frac{1}{2} + \frac{\gamma}{2}, \tag{31}$$

and whose size satisfies

$$|Q''| \;\leq\; \left(\frac{n}{\gamma^2} + 1\right) s' \;+\; \log\!\left(\frac{n+1}{\gamma^2}\right) \leq 2\left(\frac{n}{\gamma^2} + 1\right) s'. \tag{32}$$

Recall the definition $s' = \left\lfloor \frac{\gamma^2}{4n} s'' \right\rfloor$ and note that $s' \geq 1$ implies $s'' > 0$, so multiplying by s'' below preserves inequalities. Thus, we get

$$|Q''| \;\leq\; 2\left(\frac{n}{\gamma^2} + 1\right) \cdot \frac{\gamma^2}{4n}\, s'' = \frac{1}{2}\left(1 + \frac{\gamma^2}{n}\right) s''.$$

Finally, since $0 < \gamma < 1$ and $n \geq 1$, we have $\gamma^2/n \leq 1$, hence $\frac{1}{2}(1 + \gamma^2/n) \leq 1$, and therefore

$$|Q''| \;\leq\; s''. \tag{33}$$

Applying Corollary 6.3. We verify that the min-entropy premise of Corollary 6.3 holds. Indeed, for every $x \in \{0,1\}^n$,

$$\Pr[X = x] = \sum_{b\in\{0,1\}} D(x,b) \;\leq\; 2 \cdot \max_{(x,b)} D(x,b) = \mathrm{negl}(\lambda).$$

Apply Corollary 6.3 to the circuit $C := Q''$ with parameter $\epsilon := \gamma/4$. We verify the corollary's size condition (21). By (33) and the definition $s'' = \left\lfloor \frac{s - r(\lambda, 1/\varepsilon)}{q(\lambda, 1/\varepsilon)} \right\rfloor - n$, we have

$$|C| + n \;\leq\; s'' + n \;\leq\; \left\lfloor \frac{s - r(\lambda, 1/\varepsilon)}{q(\lambda, 1/\varepsilon)} \right\rfloor.$$

Let $q_\lambda := q(\lambda, 1/\varepsilon)$ and $r_\lambda := r(\lambda, 1/\varepsilon)$. Since $q_\lambda \geq 1$ (interpreting q_λ as the integer oracle-call bound from Theorem 6.1), multiplying by q_λ and adding r_λ yields

$$q_\lambda \cdot (|C| + n) + r_\lambda \;\leq\; q_\lambda \cdot \left\lfloor \frac{s - r_\lambda}{q_\lambda} \right\rfloor + r_\lambda \leq s.$$

which is exactly the needed size condition. Therefore the corollary yields a measure $M^\star \preceq D$ with $\mu(M^\star) \geq \delta - \epsilon$ such that

$$\Pr_{(X,B)\leftarrow M^\star}[Q''(X) = B] \;\leq\; \frac{1}{2} + 2\epsilon \;=\; \frac{1}{2} + \frac{\gamma}{2}.$$

This contradicts (31) applied to $M^\star$, and hence the assumption (30) was false. Thus there exists a measure $M \preceq D$ with $\mu(M) \geq \delta - \epsilon$ such that every size-s' circuit predicts B from X under M with probability at most $1/2 + \gamma$, completing the proof. □

To conclude this subsection, we state a corollary that follows immediately from 6.7 by taking the contrapositive.

Corollary 6.8 (Contrapositive of Theorem 6.7)**.** *Let $\{D_\lambda\}_{\lambda\in\mathbb{N}}$ be a family of distributions over $\{0,1\}^{n(\lambda)}\times\{0,1\}$ that are sampleable in time $\mathrm{poly}(\lambda)$, and assume*

$$\max_{(x,b)\in\{0,1\}^{n(\lambda)}\times\{0,1\}} D_\lambda(x,b) \;\leq\; \mathrm{negl}(\lambda).$$

Fix functions $\delta(\lambda)\in(0,1)$ and $s(\lambda)\in\mathbb{N}$, and let $q(\cdot,\cdot)$ and $r(\cdot,\cdot)$ be the polynomials from Theorem 6.1. Let $\gamma(\lambda)$ be any function such that $\gamma(\lambda)\in[1/\mathrm{poly}(\lambda),\delta(\lambda)]$ and define

$$\epsilon(\lambda) \;:=\; \frac{\gamma(\lambda)}{4}, \qquad \varepsilon(\lambda) \;:=\; \delta(\lambda)\cdot\epsilon(\lambda) \;=\; \frac{\delta(\lambda)\gamma(\lambda)}{4},$$

and

$$s''(\lambda) \;:=\; \left\lfloor \frac{s(\lambda)-r(\lambda,1/\varepsilon(\lambda))}{q(\lambda,1/\varepsilon(\lambda))} \right\rfloor - n(\lambda), \qquad s'(\lambda) \;:=\; \left\lfloor \frac{\gamma(\lambda)^2}{4\,n(\lambda)}\cdot s''(\lambda) \right\rfloor.$$

Suppose that for infinitely many λ, for every *measure $M_\lambda \preceq D_\lambda$ satisfying*

$$\mu(M_\lambda) \;\geq\; \delta(\lambda)-\epsilon(\lambda) \;=\; \delta(\lambda)-\frac{\gamma(\lambda)}{4},$$

there exists a quantum circuit $Q'_\lambda:\{0,1\}^{n(\lambda)}\to\{0,1\}$ of size at most $s'(\lambda)$ such that

$$\Pr_{(X,B)\leftarrow M_\lambda}\left[\,Q'_\lambda(X)=B\,\right] \;>\; \frac{1}{2}+\gamma(\lambda).$$

Then for infinitely many λ, there exists a quantum circuit $Q_\lambda:\{0,1\}^{n(\lambda)}\to\{0,1\}$ of size at most $s(\lambda)$ such that

$$\Pr_{(X,B)\leftarrow D_\lambda}\left[\,Q_\lambda(X)=B\,\right] \;>\; 1-\frac{\delta(\lambda)}{2}.$$

6.2 Key agreement amplification

In this section, we prove a theorem which enables generically amplifying a weak bit agreement protocol to a full-fledged key agreement protocol, in a manner that preserves post-quantum security.

Theorem 6.9. *Assuming there exists a post-quantum (ϵ,δ)-BA protocol secure against adversaries with non-uniform classical advice for constants $\epsilon,\delta\in[0,1]$ such that*

$$\delta < \frac{2\epsilon}{1+\epsilon},$$

there exists a $(1,0)$-BA protocol secure against adversaries with non-uniform classical advice.

A proof of this theorem is presented at the end of this section, after developing the necessary tools. We begin by defining the notion of a (ϵ,δ)-secure random variable, and of an information theoretic key-agreement amplification for a set of such independent variables.

Definition 6.10 ((ϵ,δ)-secure random variable [Hol05])**.** *A triple $X\times Y\times Z$ of random variables over $\{0,1\}\times\{0,1\}\times\{0,1\}^*$ is (ϵ,δ)-secure for $\epsilon=\epsilon(\lambda)$ and $\delta=\delta(\lambda)$ if*

- $\Pr[X = 0] = \Pr[X = 1] = \Pr[Y = 0] = \Pr[Y = 1] = 1/2$.
- $\Pr[X = Y] \geq 1/2 + \epsilon/2$.
- *There exists an event E which implies $X = Y$ such that $\Pr[E \mid X = Y] \geq \delta$ and $I(X; Z \mid E) = 0$. That is, conditioned on E, Z gives no information about X.*

Definition 6.11 (Information-theoretic key agreement protocol for (ϵ, δ)-secure random variables [Hol05])**.** *Let $\epsilon = \epsilon(\lambda), \delta = \delta(\lambda), n = n(\lambda)$, and $\{(X_i, Y_i, Z_i)\}_{i\in[\ell]}$ be ℓ independent (ϵ, δ)-secure random variables. Let $X = \{X_i\}_{i\in[\ell]}$, $Y = \{Y_i\}_{i\in[\ell]}$, $Z = \{Z_i\}_{i\in[\ell]}$. An information-theoretic key agreement protocol for (ϵ, δ)-secure random variables is a protocol where A has input $(1^\lambda, X)$, B has input $(1^\lambda, Y)$, and they communicate (classically) to produce a transcript T, an output k_A for A, and an output k_B for B. The guarantee is that $(k_A, k_B, (T, Z))$ is an $(1 - 2^{-\lambda}, 1 - 2^{-\lambda})$-secure random variable, and the protocol is called* efficient *if the running time for both A and B is* $\mathsf{poly}(\lambda)$.

We will rely on the following claim:

Claim 6.12 ([Hol05])**.** *For any constants ϵ, δ such that $\delta > \frac{1-\epsilon}{1+\epsilon}$, there exists an efficient information-theoretic key agreement protocol for (ϵ, δ)-secure random variables.*

Next, we state and prove an amplification theorem of weak bit-agreement to key agreement.

Theorem 6.13 (Adaptation of Theorem 2.17 from [Hol05])**.** *Let $\epsilon(\lambda), \delta(\lambda) : \mathbb{N} \to (0, 1)$. If there exists a post-quantum $(\epsilon(\lambda), \delta(\lambda))$-BA protocol secure against adversaries with non-uniform classical advice, and an efficient information-theoretic key agreement protocol for $(\epsilon(\lambda), 1 - \delta(\lambda) - \frac{1}{\mathrm{poly}(\lambda)})$-secure random variables, then there exists a $(1, 0)$-WBA, and thus a standard (computationally-secure) key agreement protocol.*

Proof. Let $\ell = \ell(\lambda)$ be the number of invocations of the WBA protocol required by the information-theoretic key agreement protocol, and let $n = n(\lambda)$ be the number of bits in the transcript of each WBA protocol. Let $D = \{D_\lambda\}_{\lambda\in\mathbb{N}}$ be the distribution over transcripts and output bits $(Z, X) \in \{0, 1\}^n \times \{0, 1\}$ in the WBA protocol, conditioned on A and B obtaining the same output bit X. Let

$$\delta_{\mathsf{hc}}(\lambda) \ := \ 1 - \delta(\lambda).$$

By the theorem's assumption, there exists an inverse-polynomial function $\kappa(\lambda) = 1/\mathrm{poly}(\lambda)$ such that the information-theoretic key agreement protocol works for

$$(\epsilon(\lambda), \delta_{\mathsf{hc}}(\lambda) - \kappa(\lambda))$$

-secure random variables. By decreasing κ if necessary, we assume that $\kappa(\lambda) \leq \delta_{\mathsf{hc}}(\lambda)/2$ for all sufficiently large λ.

Now consider the following key agreement protocol. A and B first use the WBA protocol ℓ times to obtain outputs

$$X_1, \ldots, X_\ell \qquad \text{and} \qquad Y_1, \ldots, Y_\ell$$

along with transcripts $Z_1, \ldots, Z_\ell$. Then, for every $i \in [\ell]$, party A publicly samples and sends a uniformly random bit $G_i \leftarrow \{0, 1\}$, and the parties define

$$\overline{X}_i := X_i \oplus G_i, \qquad \overline{Y}_i := Y_i \oplus G_i, \qquad \overline{Z}_i := (Z_i, G_i).$$

They use $\overline{X}_1, \ldots, \overline{X}_\ell$ and $\overline{Y}_1, \ldots, \overline{Y}_\ell$ as inputs to the information-theoretic key agreement protocol and run it, producing a transcript T. Their outputs k_A and k_B are the outputs of the information-theoretic key agreement protocol.

The public masks preserve correctness, since $\overline{X}_i = \overline{Y}_i$ if and only if $X_i = Y_i$. They also preserve the WBA security of each coordinate: any predictor for $\overline{X}_i = X_i \oplus G_i$ given (Z_i, G_i) can be converted into a predictor for X_i given Z_i by XORing the predictor's output with G_i. Suppose for contradiction that there exists a QPT adversary $\{\mathsf{Adv}_\lambda\}_{\lambda\in\mathbb{N}}$ such that

$$\Pr\left[\mathsf{Adv}_\lambda(\overline{Z}_1, \ldots, \overline{Z}_\ell, T) = k_A \mid k_A = k_B\right] \geq \frac{1}{2} + \mathsf{non\text{-}negl}(\lambda).$$

Define its conditional key-guessing advantage by

$$\beta(\lambda) := \Pr\left[\mathsf{Adv}_\lambda(\overline{Z}_1, \ldots, \overline{Z}_\ell, T) = k_A \mid k_A = k_B\right] - \frac{1}{2}.$$

By assumption, $\beta(\lambda) = \mathsf{non\text{-}negl}(\lambda)$. Our goal is to obtain a QPT adversary $\{\mathsf{Adv}'_\lambda\}_{\lambda\in\mathbb{N}}$ such that, for infinitely many λ,

$$\Pr_{(Z,X)\leftarrow D_\lambda}\left[\mathsf{Adv}'_\lambda(Z) = X\right] \geq \frac{1}{2} + \frac{\delta(\lambda)}{2} + \mathsf{non\text{-}negl}(\lambda). \tag{34}$$

Min-entropy alignment. We denote

$$\eta(\lambda) := \max\{\Pr_{(Z,X)\leftarrow D_\lambda}[Z = z] \mid z \in \{0,1\}^{n(\lambda)}\}.$$

If it is not the case that $\eta(\lambda) \leq \mathrm{negl}(\lambda)$, we modify Π_{WBA} so that, at the end of the protocol, one of the parties sends a uniformly random bitstring $U \leftarrow \{0,1\}^\lambda$, which is then ignored. We include U as part of the WBA transcript. Since U is independent of the parties' outputs, this leaves correctness and security unchanged and ensures that

$$\max_{(z,x)} D_\lambda(z,x) \leq \mathrm{negl}(\lambda).$$

Henceforth, we assume without loss of generality that this min-entropy condition holds.

Parameter translation. The WBA security guarantee can be rewritten as

$$\Pr[\widetilde{E}(\tau) = k_A \mid k_A = k_B] \leq \frac{1}{2} + \frac{\delta(\lambda)}{2} + \mathrm{negl}(\lambda) = 1 - \frac{\delta_{\mathsf{hc}}(\lambda)}{2} + \mathrm{negl}(\lambda).$$

Define

$$\delta_*(\lambda) := \delta_{\mathsf{hc}}(\lambda) - \frac{\kappa(\lambda)}{2}.$$

Earlier, we defined $\kappa(\lambda) \leq \delta_{\mathsf{hc}}(\lambda)/2$ for all sufficiently large λ. Hence $\delta_*(\lambda) \in (0,1)$ for all sufficiently large λ.

Fixing the hard-core parameter. Since $\beta(\lambda) = \mathsf{non\text{-}negl}(\lambda)$, there exists a polynomial $p(\cdot)$ and infinitely many security parameters λ such that

$$\beta(\lambda) \geq \frac{1}{p(\lambda)}.$$

In the remainder of the proof, we restrict attention to this infinite set of security parameters. Define

$$\gamma(\lambda) := \min\left\{\frac{\delta_*(\lambda)}{8}, \frac{\kappa(\lambda)}{4}, \frac{1}{8\ell(\lambda)p(\lambda)}\right\}. \tag{35}$$

Then $\gamma(\lambda) = \Omega(1/\mathrm{poly}(\lambda))$ on this infinite set, and for all sufficiently large λ we have

$$0 < \gamma(\lambda) \leq \delta_*(\lambda),$$

as required in Corollary 6.8.

Invoking the hard-core contrapositive. We will apply Corollary 6.8 to the distribution D_λ over (Z, X) with density parameter $\delta_*(\lambda)$ and hard-core parameter $\gamma(\lambda)$. It suffices to show that for every measure $M_\lambda \preceq D_\lambda$ satisfying

$$\mu(M_\lambda) \geq \delta_*(\lambda) - \frac{\gamma(\lambda)}{4}, \tag{36}$$

there exists a non-uniform QPT predictor Adv''_λ such that

$$\Pr_{(Z,X)\leftarrow M_\lambda}\left[\mathsf{Adv}''_\lambda(Z) = X\right] > \frac{1}{2} + \gamma(\lambda), \tag{37}$$

where $(Z, X) \leftarrow M_\lambda$ denotes sampling from the normalized distribution $M_\lambda/\mu(M_\lambda)$. Indeed, once this is shown, Corollary 6.8 yields a non-uniform QPT predictor Adv'_λ such that, for infinitely many λ,

$$\Pr_{(Z,X)\leftarrow D_\lambda}\left[\mathsf{Adv}'_\lambda(Z) = X\right] > 1 - \frac{\delta_*(\lambda)}{2} = \frac{1}{2} + \frac{\delta(\lambda)}{2} + \frac{\kappa(\lambda)}{4}.$$

contradicting WBA security.

A hybrid argument. Fix any such measure $M := M_\lambda \preceq D := D_\lambda$, and define

$$\rho(z, x) := \begin{cases} \frac{M(z,x)}{D(z,x)}, & D(z, x) > 0, \\ 0, & D(z, x) = 0. \end{cases}$$

Since $M \preceq D$, we have $\rho(z, x) \in [0, 1]$ for every (z, x). For $i \in \{0, \ldots, \ell\}$, define the hybrid $\mathcal{H}_i$ as follows. First, run the WBA protocol ℓ times to produce

$$X_1, \ldots, X_\ell, \qquad Y_1, \ldots, Y_\ell, \qquad Z_1, \ldots, Z_\ell.$$

Set initially

$$(\widehat{X}_j, \widehat{Y}_j) := (X_j, Y_j) \qquad \text{for every } j \in [\ell].$$

For every $j \in [\ell]$, if $X_j = Y_j$, sample a flag bit B_j according to

$$\Pr[B_j = 1 \mid X_j, Y_j, Z_j] = \rho(Z_j, X_j).$$

If $X_j \neq Y_j$, set $B_j := 0$. For every $j \leq i$ such that $B_j = 1$, replace $(\widehat{X}_j, \widehat{Y}_j)$ by (R_j, R_j), where $R_j \leftarrow \{0, 1\}$ is freshly sampled and uniform. After this replacement step, sample independent public bits

$$G_1, \ldots, G_\ell \leftarrow \{0, 1\},$$

and define

$$\overline{X}_j := \widehat{X}_j \oplus G_j, \qquad \overline{Y}_j := \widehat{Y}_j \oplus G_j, \qquad \overline{Z}_j := (Z_j, G_j).$$

Run the information-theoretic key agreement protocol on

$$\overline{X}_1, \ldots, \overline{X}_\ell \qquad \text{and} \qquad \overline{Y}_1, \ldots, \overline{Y}_\ell$$

to obtain transcript T and output bits (k_A, k_B). Run

$$\mathsf{Adv}_\lambda(\overline{Z}_1, \ldots, \overline{Z}_\ell, T)$$

to obtain c. The hybrid outputs 1 if and only if

$$c = k_A \qquad \text{and} \qquad k_A = k_B.$$

We first note that the joint distribution of the input bits

$$(\overline{X}_1, \overline{Y}_1), \ldots, (\overline{X}_\ell, \overline{Y}_\ell)$$

to the information-theoretic key agreement protocol is identical in all hybrids. Indeed, the only replacement occurs when $X_j = Y_j$, and after the public mask G_j is applied, both

$$(X_j \oplus G_j, Y_j \oplus G_j) \qquad \text{and} \qquad (R_j \oplus G_j, R_j \oplus G_j)$$

are distributed as a uniformly random equal pair. Therefore, if

$$p_{\mathsf{agr}} := \Pr[k_A = k_B],$$

then p_{agr} is the same in all hybrids. The hybrid $\mathcal{H}_0$ is exactly the real attack experiment for the amplified protocol. Hence, by the contradiction assumption,

$$\Pr[\mathcal{H}_0 = 1] = p_{\mathsf{agr}} \cdot \left(\frac{1}{2} + \beta(\lambda)\right). \tag{38}$$

We next argue that in $\mathcal{H}_\ell$, the variables

$$(\overline{X}_j, \overline{Y}_j, \overline{Z}_j)_{j \in [\ell]}$$

are independent $(\epsilon(\lambda), \delta_{\mathsf{hc}}(\lambda) - \kappa(\lambda))$-secure random variables.

Fix any $j \in [\ell]$. Since G_j is uniform and independent, we have

$$\Pr\left[\overline{X}_j = 0\right] = \Pr\left[\overline{X}_j = 1\right] = \Pr\left[\overline{Y}_j = 0\right] = \Pr\left[\overline{Y}_j = 1\right] = \frac{1}{2}.$$

Moreover, equality is preserved by the mask, and the replacement step only occurs when $X_j = Y_j$. Therefore

$$\Pr\left[\overline{X}_j = \overline{Y}_j\right] = \Pr[X_j = Y_j] \geq \frac{1}{2} + \frac{\epsilon(\lambda)}{2} - \mathrm{negl}(\lambda).$$

Define the event

$$F_j := \{X_j = Y_j \ \wedge \ B_j = 1\}.$$

Then F_j implies $\overline{X}_j = \overline{Y}_j$. Furthermore, because $\overline{X}_j = \overline{Y}_j$ if and only if $X_j = Y_j$, and conditioned on $X_j = Y_j$ the pair (Z_j, X_j) is distributed according to D, we have

$$\Pr\left[F_j \mid \overline{X}_j = \overline{Y}_j\right] = \mathop{\mathbb{E}}_{(Z,X) \leftarrow D}[\rho(Z, X)] = \mu(M).$$

By (36) and the definitions of δ_* and γ, we have

$$\mu(M) \geq \delta_*(\lambda) - \frac{\gamma(\lambda)}{4} = \delta_{\mathsf{hc}}(\lambda) - \frac{\kappa(\lambda)}{2} - \frac{\gamma(\lambda)}{4}.$$

Since $\gamma(\lambda) \leq \kappa(\lambda)/4$, this implies

$$\mu(M) \geq \delta_{\mathsf{hc}}(\lambda) - \frac{\kappa(\lambda)}{2} - \frac{\kappa(\lambda)}{16} \geq \delta_{\mathsf{hc}}(\lambda) - \kappa(\lambda).$$

Thus the event F_j has sufficiently large conditional probability to witness that the variables in $\mathcal{H}_\ell$ are $(\epsilon(\lambda), \delta_{\mathsf{hc}}(\lambda) - \kappa(\lambda))$ -secure random variables. Finally,

$$I(\overline{X}_j; \overline{Z}_j \mid F_j) = 0.$$

Indeed, conditioned on F_j, in $\mathcal{H}_\ell$ we have

$$\overline{X}_j = R_j \oplus G_j,$$

where R_j is uniform and independent of (Z_j, G_j).

Thus the variables in $\mathcal{H}_\ell$ satisfy the input condition for the information-theoretic key agreement protocol. Hence the output triple

$$(k_A, k_B, (T, \overline{Z}_1, \ldots, \overline{Z}_\ell))$$

is an $(1 - 2^{-\lambda}, 1 - 2^{-\lambda})$-secure random variable. In particular,

$$p_{\mathsf{agr}} = \Pr[k_A = k_B] \geq 1 - \mathrm{negl}(\lambda),$$

and any predictor of k_A from $(T, \overline{Z}_1, \ldots, \overline{Z}_\ell)$ has success probability at most $1/2 + \mathrm{negl}(\lambda)$ conditioned on $k_A = k_B$. Therefore

$$\Pr[\mathcal{H}_\ell = 1] = p_{\mathsf{agr}} \cdot \left(\frac{1}{2} + \mathrm{negl}(\lambda)\right). \tag{39}$$

Combining (38) and (39), we obtain

$$\tau(\lambda) := \Pr[\mathcal{H}_0 = 1] - \Pr[\mathcal{H}_\ell = 1] = p_{\mathsf{agr}} \cdot (\beta(\lambda) - \mathrm{negl}(\lambda)).$$

Since $p_{\mathsf{agr}} \geq 1 - \mathrm{negl}(\lambda)$, for all sufficiently large λ in the infinite set under consideration,

$$\tau(\lambda) \geq \frac{\beta(\lambda)}{2}. \tag{40}$$

Therefore, there exists an index $i = i(\lambda) \in [\ell]$ such that

$$\Pr[\mathcal{H}_{i-1} = 1] - \Pr[\mathcal{H}_i = 1] \geq \alpha(\lambda), \qquad \text{where } \alpha(\lambda) := \frac{\beta(\lambda)}{2\ell(\lambda)}. \tag{41}$$

Let W denote the tuple of post-randomization values in all coordinates except i:

$$W := \left((\overline{X}_j, \overline{Y}_j, \overline{Z}_j)\right)_{j \neq i}.$$

The distribution of W is the same in $\mathcal{H}_{i-1}$ and $\mathcal{H}_i$. By averaging, there exists a value $w = w(\lambda)$ in the support of W such that

$$\Pr[\mathcal{H}_{i-1} = 1 \mid W = w] - \Pr[\mathcal{H}_i = 1 \mid W = w] \geq \alpha(\lambda). \tag{42}$$

Defining Adv''_λ. Hard-code $i = i(\lambda)$ and $w = w(\lambda)$ into Adv''_λ. Given input a WBA transcript z, the predictor Adv''_λ operates as follows.

1. Sample independent uniform bits $R_i, G_i \leftarrow \{0,1\}$, and set

$$\overline{x}_i = \overline{y}_i := R_i \oplus G_i, \qquad \overline{z}_i := (z, G_i).$$

   Combine this coordinate with the hard-coded values w in all coordinates $j \neq i$, and run the information-theoretic key agreement protocol to obtain transcript T and outputs (k_A, k_B).

2. Query

$$\mathsf{Adv}_\lambda(\overline{z}_1, \ldots, \overline{z}_\ell, T)$$

   to obtain c.

3. If $c = k_A$ and $k_A = k_B$, output R_i. Otherwise, output $1 \oplus R_i$.

Let $s_{\mathsf{Adv}}(\lambda)$ be an upper bound on the circuit size of Adv_λ, and let $s_{\mathsf{KA}}(\lambda)$ upper bound the circuit size needed to execute the efficient information-theoretic key-agreement protocol once on $\ell(\lambda)$ input bits, producing (T, k_A, k_B). Both s_{Adv} and s_{KA} are polynomial in λ. Hard-coding w, i contributes

$$O(\ell(\lambda) \cdot (n(\lambda) + 3))$$

bits of advice and hence $O(\ell(\lambda) \cdot n(\lambda))$ circuit-size overhead. Therefore the constructed non-uniform predictor Adv''_λ can be implemented by a quantum circuit of size at most

$$t(\lambda) := s_{\mathsf{Adv}}(\lambda) + s_{\mathsf{KA}}(\lambda) + O(\ell(\lambda) \cdot n(\lambda)) + \mathrm{poly}(\lambda) = \mathrm{poly}(\lambda). \tag{43}$$

Recall

$$F_i = \{X_i = Y_i \ \wedge \ B_i = 1\}.$$

By construction, conditioned on $W = w$, the hybrids $\mathcal{H}_{i-1}$ and $\mathcal{H}_i$ are identical conditioned on $\neg F_i$. Conditioned on F_i, they differ only in the value fed to the information-theoretic protocol in coordinate i: in $\mathcal{H}_{i-1}$ it is $X_i \oplus G_i$, while in $\mathcal{H}_i$ it is $R_i \oplus G_i$ for an independent uniform R_i. Therefore

$$\begin{aligned}&\Pr[\mathcal{H}_{i-1} = 1 \mid W = w] - \Pr[\mathcal{H}_i = 1 \mid W = w] \\ &\quad = \Pr[F_i \mid W = w] \cdot \Big(\Pr[\mathcal{H}_{i-1} = 1 \mid W = w, F_i] - \Pr[\mathcal{H}_i = 1 \mid W = w, F_i]\Big).\end{aligned}$$

Combining this identity with (42), and using $\Pr[F_i \mid W = w] \leq 1$, yields

$$\Pr[\mathcal{H}_{i-1} = 1 \mid W = w, F_i] - \Pr[\mathcal{H}_i = 1 \mid W = w, F_i] \geq \alpha(\lambda). \tag{44}$$

Let G_{out} denote the event that the hybrid outputs 1, namely

$$G_{\mathsf{out}} := \{c = k_A \ \wedge \ k_A = k_B\}.$$

Then (44) says

$$\Pr\Big[G_{\mathsf{out}} \mid W = w, F_i, \overline{X}_i = X_i \oplus G_i\Big] - \Pr\Big[G_{\mathsf{out}} \mid W = w, F_i, \overline{X}_i \leftarrow R_i \oplus G_i\Big] \geq \alpha(\lambda).$$

Since R_i is uniform and independent of X_i, the second term is the average of the two cases

$$\overline{X}_i = X_i \oplus G_i \qquad \text{and} \qquad \overline{X}_i = (1 - X_i) \oplus G_i.$$

Hence

$$\begin{aligned}\Delta_G := \Pr\Big[G_{\mathsf{out}} \mid W = w, F_i, \overline{X}_i = X_i \oplus G_i\Big] \\ - \Pr\Big[G_{\mathsf{out}} \mid W = w, F_i, \overline{X}_i = (1 - X_i) \oplus G_i\Big] \geq 2\alpha(\lambda).\end{aligned} \tag{45}$$

Conditioned on F_i, the pair (Z_i, X_i) is distributed according to the normalized measure M. Indeed, for every (z, x) in the support of D,

$$\begin{aligned}\Pr[(Z_i, X_i) = (z, x) \mid F_i] &= \frac{D(z,x)\rho(z,x)}{\mathbb{E}_{(Z,X)\leftarrow D}[\rho(Z,X)]} \\ &= \frac{M(z,x)}{\mu(M)}.\end{aligned}$$

Therefore, by construction of Adv''_λ,

$$\begin{aligned}\Pr_{(Z_i,X_i)\leftarrow M}\left[\mathsf{Adv}''_\lambda(Z_i) = X_i\right] &= \Pr[G_{\mathsf{out}} \wedge R_i = X_i \mid W = w, F_i] \\ &\quad + \Pr[\neg G_{\mathsf{out}} \wedge R_i = 1 - X_i \mid W = w, F_i] \\ &= \frac{1}{2}\Big(\Pr[G_{\mathsf{out}} \mid W = w, F_i, R_i = X_i] \\ &\qquad + \Pr[\neg G_{\mathsf{out}} \mid W = w, F_i, R_i = 1 - X_i]\Big) \\ &= \frac{1}{2}(1 + \Delta_G) \\ &\geq \frac{1}{2} + \alpha(\lambda).\end{aligned}$$

On the infinite set under consideration, $\beta(\lambda) \geq 1/p(\lambda)$, and hence

$$\alpha(\lambda) = \frac{\beta(\lambda)}{2\ell(\lambda)} \geq \frac{1}{2\ell(\lambda)p(\lambda)} > \gamma(\lambda),$$

by (35). Thus

$$\Pr_{(Z_i,X_i)\leftarrow M_\lambda}\left[\mathsf{Adv}''_\lambda(Z_i) = X_i\right] > \frac{1}{2} + \gamma(\lambda),$$

which establishes (37).

Finally, choose the size bound $s(\lambda)$ in Corollary 6.8 so that for all sufficiently large λ,

$$s(\lambda) \geq q(\lambda, 1/\varepsilon(\lambda)) \cdot \Big(n(\lambda) + \Big\lceil \frac{4n(\lambda)}{\gamma(\lambda)^2}\,(t(\lambda) + 1)\Big\rceil\Big) + r(\lambda, 1/\varepsilon(\lambda)),$$

where

$$\varepsilon(\lambda) = \frac{\delta_*(\lambda)\gamma(\lambda)}{4}.$$

Then the resulting parameter $s'(\lambda)$ from Corollary 6.8 satisfies $s'(\lambda) \geq t(\lambda)$, so Adv''_λ is a valid witness circuit in the premise of the corollary. Therefore Corollary 6.8, invoked with density parameter $\delta_*(\lambda)$ and hard-core parameter $\gamma(\lambda)$, gives a predictor Adv'_λ such that, for infinitely many λ,

$$\Pr_{(Z,X)\leftarrow D_\lambda}\left[\mathsf{Adv}'_\lambda(Z) = X\right] > 1 - \frac{\delta_*(\lambda)}{2}.$$

By definition of $\delta_*(\lambda)$,

$$1 - \frac{\delta_*(\lambda)}{2} = 1 - \frac{\delta_{\mathsf{hc}}(\lambda)}{2} + \frac{\kappa(\lambda)}{4} = \frac{1}{2} + \frac{\delta(\lambda)}{2} + \frac{\kappa(\lambda)}{4}.$$

Since $\kappa(\lambda) = 1/\mathrm{poly}(\lambda)$, this exceeds the WBA security threshold

$$\frac{1}{2} + \frac{\delta(\lambda)}{2} + \mathrm{negl}(\lambda)$$

by an inverse-polynomial amount for all sufficiently large λ in the infinite set under consideration. This contradicts WBA security.

This contradiction proves that the amplified protocol is computationally secure. Its correctness and lack of bias follow from the guarantee of the information-theoretic key agreement protocol, and hence the protocol is a fully secure bit-agreement protocol. This completes the proof.

□

We conclude this section by relating our key-agreement amplification result to non-commutation tests, and prove that non-commutation tests in a certain parameter regime imply key agreement. We also conclude that *any* non-commutation test with robust completeness implies key agreement.

Corollary 6.14. *Given any normal-form (ϵ, δ)-ToNC such that*

$$\epsilon \;>\; \frac{1 + 4\delta}{5} \;+\; \frac{1}{\mathrm{poly}(\lambda)},$$

there exists classical-communication key agreement.

Proof. By Theorem 5.1, a normal-form (ϵ, δ)-ToNC implies (ϵ, γ)-WBA with

$$\gamma = \frac{1 + 4\delta - 3\epsilon}{1 + \epsilon} = \frac{4(1 + \delta)}{1 + \epsilon} - 3.$$

Next, by Theorem 6.13, it suffices that for some slack $\zeta(\lambda) = 1/\mathrm{poly}(\lambda)$, there exists an efficient information-theoretic key-agreement protocol for $(\epsilon, 1 - \gamma - \zeta(\lambda))$-secure random variables. By Claim 6.12, such a protocol exists whenever

$$1 - \gamma - \zeta(\lambda) \;>\; \frac{1 - \epsilon}{1 + \epsilon}.$$

Substituting $\gamma = \frac{4(1+\delta)}{1+\epsilon} - 3$ yields

$$4 - \frac{4(1 + \delta)}{1 + \epsilon} - \zeta(\lambda) \;>\; \frac{1 - \epsilon}{1 + \epsilon}.$$

Multiplying by $1 + \epsilon$ and rearranging gives

$$(5 - \zeta(\lambda))\,\epsilon \;>\; 1 + 4\delta + \zeta(\lambda),$$

equivalently

$$\epsilon \;>\; \frac{1 + 4\delta + \zeta(\lambda)}{5 - \zeta(\lambda)}.$$

Since $\zeta(\lambda) = 1/\mathrm{poly}(\lambda)$, this is implied by

$$\epsilon \;>\; \frac{1 + 4\delta}{5} \;+\; \frac{1}{\mathrm{poly}(\lambda)}.$$

Under this condition we obtain key agreement, completing the proof. □

Corollary 6.15. *Given any normal-form (ϵ, δ)-ToNC with robust completeness and $\epsilon > \delta + 1/\mathrm{poly}(\lambda)$, there exists classical-communication key agreement.*

Proof. By Theorem 5.1, a normal-form (ϵ, δ)-ToNC with robust completeness implies (ϵ, γ)-WBA with $\gamma = 2\delta - \epsilon$. Therefore, if $\epsilon > \delta + 1/\mathrm{poly}(\lambda)$, there exists a (ϵ, γ)-WBA with $\gamma < \epsilon - 1/\mathrm{poly}(\lambda)$. Then by Claim 6.12 and Theorem 6.13, there exists a standard key agreement protocol.

□

6.3 Post-quantum interactive XOR lemma

The multiplicative Isolation Lemma—introduced and proved by Levin—is used in his work to prove Yao's XOR lemma [Lev85]. Halevi and Rabin [HR08, Lemma 3.1] extend Levin's proof of Yao's XOR lemma, which relies on the Isolation Lemma, to the setting of classical interactive protocols. In particular, they show that if every computationally bounded adversary can predict the protocol's single secret bit with correlation advantage at most ε, then the t-fold sequential XOR-composition amplifies secrecy so that every efficient adversary's advantage drops to roughly ε^t (up to negligible terms).

We extend their result to the post-quantum setting, by proving an analogous theorem which enables amplifying security against computationally-bounded *quantum* adversaries. The main challenge in proving such a theorem, is the reliance of the classical proof on rewinding the adversary, which is non-trivial and at times potentially impossible when the adversary is quantum, due to the no-cloning principle. In order to overcome it, we utilize an approach for quantum rewinding developed by Marriott and Watrous [MW04] and further analyzed by [CMSZ22] (see our Preliminaries section for an introduction to this approach).

Theorem 6.16. *Let Γ_1, Γ_2 be two protocols such that for any $i \in \{1, 2\}$, for any QPT adversary A and state $|\psi\rangle$,*

$$\mathop{\mathbb{E}}_{\substack{r \leftarrow \{0,1\}^*, \\ b_A,\, \xi \leftarrow \Gamma_i\langle A(|\psi\rangle), V_i(r)\rangle}} [b_A \cdot P_i(r, \xi)] \leq \delta_i,$$

where V_i is the verifier in Γ_i, r_i are its random bits, ξ is the interaction transcript, $P_i(r, \xi) \in \{-1, +1\}$ is a $\mathrm{poly}(\lambda)$-time computable predicate, and $b_A \in \{-1, +1\}$ is the adversary's output.

Then for any QPT adversary A and state $|\psi\rangle$,

$$\mathop{\mathbb{E}}_{\substack{r_1, r_2 \leftarrow \{0,1\}^*, \\ |\psi'\rangle,\, \xi_1 \leftarrow \Gamma_1\langle A_1(|\psi\rangle), V_1(r_1)\rangle, \\ b_A,\, \xi_2 \leftarrow \Gamma_2\langle A_2(|\psi'\rangle), V_2(r_2)\rangle}} [b_A \cdot P_1(r_1, \xi_1) \cdot P_2(r_2, \xi_2)] \leq \delta_1 \cdot \delta_2 + \mathrm{negl}(\lambda),$$

where we view A as a sequential adversary $A = (A_1, A_2)$: first A_1 interacts with $V_1(r_1)$ on input $|\psi\rangle$, producing a transcript ξ_1 and leaving a residual state $|\psi'\rangle$; then A_2, initialized with $|\psi'\rangle$, interacts with $V_2(r_2)$ producing a transcript ξ_2 and output bit b_A.

Proof. Suppose for contradiction that there exist a QPT adversary A and a quantum state $|\psi\rangle$ such that

$$\mathop{\mathbb{E}}_{\substack{r_1, r_2 \leftarrow \{0,1\}^*, \\ |\psi'\rangle,\, \xi_1 \leftarrow \Gamma_1\langle A_1(|\psi\rangle), V_1(r_1)\rangle, \\ b_A,\, \xi_2 \leftarrow \Gamma_2\langle A_2(|\psi'\rangle), V_2(r_2)\rangle}} [b_A \cdot P_1(r_1, \xi_1) \cdot P_2(r_2, \xi_2)] > \delta_1 \cdot \delta_2 + \kappa(\lambda).$$

for a function $\kappa = \Omega(1/\mathrm{poly}(\lambda))$. We can write this as

$$\mathop{\mathbb{E}}_{\substack{r_1\leftarrow\{0,1\}^*\\ |\psi'\rangle,\,\xi_1\leftarrow\Gamma_1\langle A_1(|\psi\rangle),V_1(r_1)\rangle}}\left[P_1(r_1,\xi_1)\cdot \mathop{\mathbb{E}}_{\substack{r_2\leftarrow\{0,1\}^*\\ b_A,\,\xi_2\leftarrow\Gamma_2\langle A_2(|\psi'\rangle),V_2(r_2)\rangle}}[b_A\cdot P_2(r_2,\xi_2)]\right] > \delta_1\cdot\delta_2+\kappa(\lambda), \quad (46)$$

Now, for any $|\psi'\rangle$, let

$$T(|\psi'\rangle) := \mathop{\mathbb{E}}_{\substack{r_2\leftarrow\{0,1\}^*\\ b_A,\,\xi_2\leftarrow\Gamma_2\langle A_2(|\psi'\rangle),V_2(r_2)\rangle}}[b_A\cdot P_2(r_2,\xi_2)]\,.$$

Due to the security guarantee of Γ_2, for any state $|\psi'\rangle$

$$|T(|\psi'\rangle)| \le \delta_2. \quad (47)$$

Note that if $T(|\psi'\rangle) < -\delta_2$ using an adversary A_2, we obtain an adversary which breaks the security by flipping the sign of the predictions of A_2. This justifies the bound on the *absolute value* of $T(|\psi'\rangle)$.

Due to (46), we have that

$$\mathop{\mathbb{E}}_{\substack{r_1\leftarrow\{0,1\}^*\\ |\psi'\rangle,\,\xi\leftarrow\Gamma_1\langle A_1(|\psi\rangle),V_1(r_1)\rangle}}\left[P_1(r_1,\xi_1)\cdot\frac{T(|\psi'\rangle)}{\delta_2}\right] > \delta_1+\frac{\kappa(\lambda)}{\delta_2}. \quad (48)$$

To complete the proof, it suffices to give a procedure B that, given $|\psi'\rangle$, outputs a real number $\alpha\in[-\delta_2,\delta_2]$ so that for any $|\psi'\rangle$,

$$\tau(\lambda) := |\mathbb{E}[B(|\psi'\rangle)] - T(|\psi'\rangle)|$$

such that

$$\frac{\kappa-\tau}{\delta_2} = \Omega(\frac{1}{\mathrm{poly}(\lambda)}). \quad (49)$$

Indeed, given such a B, an adversary A could perform the following steps:

1. Run A_1 in the interaction with v_1 and keep the intermediate state $|\psi'\rangle$.
2. Run $B(|\psi'\rangle)$ and obtain α.
3. Output $b_A\in\{1,-1\}$ sampled as a Bernoulli random variable which takes the value 1 with probability $\frac{\alpha/\delta_2+1}{2}$.

In that case, we would have

$$
\begin{aligned}
&\mathop{\mathbb{E}}_{\substack{r\leftarrow\{0,1\}^*,\\ b_A,\ \xi\leftarrow\Gamma_1\langle A,V_1(r)\rangle}} [b_A\cdot P(r,\xi)]\\
&= \mathop{\mathbb{E}}_{\substack{r\leftarrow\{0,1\}^*,\\ |\psi'\rangle,\ \xi\leftarrow\Gamma_1\langle A_1,V_1(r)\rangle}} \left[\mathop{\mathbb{E}}_{\substack{\alpha\leftarrow B(|\psi'\rangle),\\ b_A\leftarrow\mathsf{Ber}(\frac{\alpha/\delta_2+1}{2})}} [b_A]\cdot P_1(r,\xi)\right]\\
&= \mathop{\mathbb{E}}_{\substack{r_1\leftarrow\{0,1\}^*\\ |\psi'\rangle,\ \xi_1\leftarrow\Gamma_1\langle A_1,V_1(r_1)\rangle}} \left[\frac{\mathbb{E}[B(|\psi'\rangle)]}{\delta_2}\cdot P_1(r_1,\xi_1)\right]\\
&= \mathop{\mathbb{E}}_{\substack{r_1\leftarrow\{0,1\}^*\\ |\psi'\rangle,\ \xi_1\leftarrow\Gamma_1\langle A_1,V_1(r_1)\rangle}} \left[\left(\frac{T(|\psi'\rangle)}{\delta_2}+\frac{\mathbb{E}[B(|\psi'\rangle)]-T(|\psi'\rangle)}{\delta_2}\right)\cdot P_1(r_1,\xi_1)\right]\\
&\geq \mathop{\mathbb{E}}_{\substack{r_1\leftarrow\{0,1\}^*\\ |\psi'\rangle,\ \xi_1\leftarrow\Gamma_1\langle A_1,V_1(r_1)\rangle}} \left[\frac{T(|\psi'\rangle)}{\delta_2}\cdot P_1(r_1,\xi_1)\right] - \frac{1}{\delta_2}\mathop{\mathbb{E}}_{\substack{r_1\leftarrow\{0,1\}^*\\ |\psi'\rangle,\ \xi_1\leftarrow\Gamma_1\langle A_1,V_1(r_1)\rangle}} [|\mathbb{E}[B(|\psi'\rangle)]-T(|\psi'\rangle)|]\\
&\geq \mathop{\mathbb{E}}_{\substack{r_1\leftarrow\{0,1\}^*\\ |\psi'\rangle,\ \xi_1\leftarrow\Gamma_1\langle A_1,V_1(r_1)\rangle}} \left[\frac{T(|\psi'\rangle)}{\delta_2}\cdot P_1(r_1,\xi_1)\right] - \frac{\tau(\lambda)}{\delta_2}.
\end{aligned}
\tag{50}
$$

a contradiction with the hardness of Γ_1. In the second equality, we rely on the following identity

$$
\mathop{\mathbb{E}}_{\substack{\alpha\leftarrow B(|\psi'\rangle),\\ b_A\leftarrow\mathsf{Ber}(\frac{\alpha/\delta_2+1}{2})}} [b_A] = \mathop{\mathbb{E}}_{\alpha\leftarrow B(|\psi'\rangle)} \left[2\,\mathbb{E}[\mathsf{Ber}(\frac{\alpha/\delta_2+1}{2})]-1\right] = \mathop{\mathbb{E}}_{\alpha\leftarrow B(|\psi'\rangle)} [\alpha/\delta_2] = \frac{\mathbb{E}[B(|\psi'\rangle)]}{\delta_2}
$$

Combined with (48), we get:

$$
\mathbb{E}\,[b_A\cdot P_1(r_1,\xi_1)] \;=\; \mathbb{E}\left[\frac{\mathbb{E}[B(|\psi'\rangle)]}{\delta_2}\cdot P_1(r_1,\xi_1)\right] \;>\; \delta_1+\frac{\kappa(\lambda)}{\delta_2}-\frac{\tau(\lambda)}{\delta_2} = \delta_1+\Omega(\frac{1}{\mathrm{poly}(\lambda)}), \tag{51}
$$

contradicting the security of Γ_1. The last equality is due to (49).

We next define B. Let X be the adversary register holding the intermediate state $|\psi'\rangle$ at the start of the *second* execution. Let Y be an auxiliary register that contains the ancilla qubits to be used by both parties for computations and communication. It includes one designated qubit Z that indicates whether the final outputs match. By purification and deferred measurement, there exists a unitary

$$U : X\otimes Y \to X\otimes Y$$

that coherently implements the full second execution of Γ_2 between A_2 and V_2.

Define the match projector by

$$\Pi_{\mathsf{match}} \;:=\; I_{X,Y\setminus Z}\otimes|0\rangle\langle 0|_Z,$$

and define

$$\Pi_1 \;:=\; U^\dagger\Pi_{\mathsf{match}}U.$$

Also define the projector onto the clean start state of Y:

$$\Pi_0 \;:=\; I_X\otimes|0\rangle\langle 0|_Y.$$

Fix $\varepsilon, \eta > 0$ and let

$$n \;:=\; \left\lceil \frac{\ln(1/2\eta)}{2\varepsilon^2} \right\rceil$$

.

On input $|\psi'\rangle_X$, algorithm B:

1. Prepares Y in $|0\rangle_Y$, so the joint state is $|\Psi_0\rangle = |\psi'\rangle_X|0\rangle_Y \in \mathrm{im}(\Pi_0)$.
2. Performs n alternating binary projective measurements, starting with Π_1:

   $$(\Pi_1, I-\Pi_1),\ (\Pi_0, I-\Pi_0),\ (\Pi_1, I-\Pi_1),\ (\Pi_0, I-\Pi_0), \ldots$$

   Let $b_i \in \{0,1\}$ be the outcome bit of the i-th measurement.
3. Sets

   $$\widetilde{p} := \mathsf{NReps}(1, b_1, \ldots, b_n), \qquad \widetilde{\alpha} := 2\widetilde{p} - 1.$$

4. Outputs the clipped value

   $$\alpha \;:=\; \max\{-\delta_2,\ \min\{\delta_2,\ \widetilde{\alpha}\}\} \in [-\delta_2, \delta_2].$$

Let $q(\psi') := \Pr[b_A = P(r_2, \xi_2) \;:\; \Gamma_2\langle A_2(|\psi'\rangle), V(r_2)\rangle]$ be the probability in the second execution, so that

$$T(|\psi'\rangle) \;=\; \mathbb{E}[b_A \cdot P_2(r_2, \xi_2)] \;=\; 2q(\psi') - 1.$$

By Proposition 3.13 applied with $B = (\Pi_0, \mathbb{I} - \Pi_0)$ and $A = (\Pi_1, \mathbb{I} - \Pi_1)$, the estimator $\widetilde{p}$ satisfies $\mathbb{E}[\widetilde{p}] = q(\psi')$, hence

$$\mathbb{E}[\widetilde{\alpha}] \;=\; 2\mathbb{E}[\widetilde{p}] - 1 \;=\; 2q(\psi') - 1 \;=\; T(|\psi'\rangle).$$

Furthermore, the hardness of Γ_2 implies that all eigenvalues of $\Pi_0\Pi_1\Pi_0$ restricted to $\mathrm{im}(\Pi_0)$ lie in $[\,\frac{1}{2} - \frac{\delta_2}{2}, \frac{1}{2} + \frac{\delta_2}{2}\,]$. Let us show this. Fix any unit vector $|\phi\rangle \in \mathrm{im}(\Pi_0)$. Since $\Pi_0 = I_X \otimes |0\rangle\langle 0|_Y$, every such vector is of the form $|\phi\rangle = |\psi'\rangle_X|0\rangle_Y$ for some unit $|\psi'\rangle_X$, and hence

$$\langle\phi|\Pi_0\Pi_1\Pi_0|\phi\rangle \;=\; \langle\phi|\Pi_1|\phi\rangle.$$

By construction of $\Pi_1 := U^\dagger \Pi_{\mathsf{match}} U$, the quantity $q(\psi')$ is equal to $\langle\psi' 0|\Pi_1|\psi' 0\rangle$. Moreover, due to (47), $|T(|\psi'\rangle)| \le \delta_2$, and recall that $T(|\psi'\rangle) = 2q(\psi') - 1$. Hence, $q(\psi') \in [\frac{1}{2} - \frac{\delta_2}{2}, \frac{1}{2} + \frac{\delta_2}{2}]$. Therefore, for every unit $|\phi\rangle \in \mathrm{im}(\Pi_0)$,

$$\tfrac{1}{2} - \tfrac{\delta_2}{2} \;\le\; \langle\phi|\Pi_0\Pi_1\Pi_0|\phi\rangle \;\le\; \tfrac{1}{2} + \tfrac{\delta_2}{2},$$

which implies the stated restriction of the eigenvalues.

Therefore, Corollary 3.10 implies that every Jordan parameter p_j lies in this interval, so $2p_j - 1 \in [-\delta_2, \delta_2]$. By Chernoff's bound, $\Pr[|\widetilde{p} - p_j| \le \varepsilon] \ge 1 - \eta$ in each Jordan block, hence $|\widetilde{\alpha} - (2p_j - 1)| \le 2\varepsilon$ except with probability η. Therefore, the clipping step changes $\widetilde{\alpha}$ by at most 2ε on the good event and by at most 2 always, yielding the expectation bound

$$\left|\mathbb{E}[\alpha] - \mathbb{E}[\widetilde{\alpha}]\right| \;\le\; 2\varepsilon + 2\eta.$$

Combining the last two displays,

$$\tau(\lambda) := \left|\mathbb{E}[B(|\psi'\rangle)] - T(|\psi'\rangle)\right| \;=\; \left|\mathbb{E}[\alpha] - T(|\psi'\rangle)\right| \;\le\; 2\varepsilon + 2\eta.$$

Choosing, for example, $\varepsilon(\lambda), \eta(\lambda) := \frac{\kappa(\lambda)}{8}$, implies $\frac{\kappa - \tau}{\delta_2} = \Omega(\frac{1}{\mathrm{poly}(\lambda)})$ as required. □

Remark 6.17. *We stress that our Theorem holds in the non-uniform computational model, where the security of the protocol holds against any QPT adversary with non-uniform* quantum *advice. Levin's Isolation Lemma is also proven in the non-uniform model, and Goldreich et al. extend it to the uniform model under an assumption on sampling [GNW11]. We leave the question of extending our result to the uniform model for future work.*

By applying Theorem 6.16 repeatedly, we immediately obtain the following corollary.

Corollary 6.18. *Let $\{\Gamma_i\}_{i\in[\ell]}$ be $\ell = \mathrm{poly}(\lambda)$ many protocols such that for each $i \in [\ell]$, any QPT adversary A, and any state $|\psi\rangle$,*

$$\mathop{\mathbb{E}}_{\substack{r\leftarrow\{0,1\}^*,\\ b_A,\, \xi\leftarrow\Gamma_i\langle A(|\psi\rangle),V_i(r)\rangle}} [b_A \cdot P_i(r,\xi)] \le \delta_i,$$

where V_i is the verifier in Γ_i, r are its random bits, ξ is the interaction transcript, $P_i(r,\xi) \in \{-1,+1\}$ is a $\mathrm{poly}(\lambda)$-time computable predicate, and $b_A \in \{-1,+1\}$ is the adversary's output.

Then for any QPT adversary A and state $|\psi\rangle$,

$$\mathop{\mathbb{E}}_{\substack{\{r_i\leftarrow\{0,1\}^*\}_{i\in[\ell]},\\ |\psi'\rangle,\, \xi_1\leftarrow\Gamma_1\langle A_1(|\psi\rangle),V_1(r_1)\rangle,\\ \vdots\\ b_A,\, \xi_\ell\leftarrow\Gamma_\ell\langle A_\ell(|\psi'\rangle),V_\ell(r_\ell)\rangle}} [b_A \cdot P_1(r_1,\xi_1)\cdot\cdots\cdot P_\ell(r_\ell,\xi_\ell)] \le \prod_{i\in[\ell]} \delta_i + \mathrm{negl}(\lambda),$$

where we view A as a sequential adversary $A = (A_1,\ldots,A_\ell)$: first A_1 interacts with $V_1(r_1)$ on input $|\psi\rangle$, producing transcript ξ_1 and leaving a residual state $|\psi'\rangle$; this repeats ℓ times sequentially until A_ℓ, initialized with $|\psi'\rangle$, interacts with $V_\ell(r_\ell)$ producing transcript ξ_ℓ and final output bit b_A.

6.4 Oblivious transfer amplification

First, we give an OT amplification theorem that follows fairly immediately from Corollary 6.18.

Theorem 6.19. *Given any $(1,\delta,0)$-OT or $(1,0,\delta)$-OT secure against adversaries with non-uniform quantum advice (Definition 3.6) for $\delta \le 1 - 1/\mathrm{poly}(\lambda)$, there exists standard OT secure against adversaries with non-uniform quantum advice.*

Proof. Note that $(1,0,\delta)$-weak OT implies $(1,\delta,0)$-weak OT by standard OT reversal. So let S', R' be an $(1,\delta,0)$-weak OT. We perform standard sequential repetition to achieve the standard OT:

$\underline{(1,0,0)\ \mathsf{OT}}$

- Let $\ell = \lambda/(1-\delta)$. For $i \in [\ell]$, the parties run
$$(b_i, r_i), (r_{0,i}, r_{1,i}) \leftarrow \langle R'(1^\lambda), S'(1^\lambda)\rangle.$$
- R samples $b \leftarrow \{0,1\}$, sends $\{b \oplus b_i\}_{i\in[\ell]}$ to S, and outputs $r_b := \bigoplus_{i\in[\ell]} r_i$.
- S receives $\{b'_i\}_{i\in[\ell]}$ and outputs
$$r_0 := \bigoplus_{i\in[\ell]} r_{i,b'_i}, \quad r_1 := \bigoplus_{i\in[\ell]} r_{i,1-b'_i}.$$

Correctness follows by inspection, and receiver security follows from a standard hybrid argument. Sender security follows from Corollary 6.18. Indeed, we fix each of $\Pi_1, \ldots, \Pi_\ell$ to be the interactive protocol between honest sender S' and adversarial receiver, where the predicate P outputs the XOR of the sender outputs $r_{0,i} \oplus r_{1,i}$. Then note that $\delta^\ell + \mathrm{negl}(\lambda) \leq e^{-\lambda} = \mathrm{negl}(\lambda)$. □

Next, we amplify our committed-bit OT to the point where we can apply the above theorem. As discussed in Section 2.4, our strategy is inspired by a strategy from [Wul07] in the classical semi-honest case.

Lemma 6.20. *Given any $(\epsilon, \delta, 0)$ committed-bit OT (Definition 3.8) for constants ϵ, δ such that $\delta < \epsilon^2$, there exists a $(1, 1/2, 0)$ committed-bit OT.*

Proof. Let $\mathsf{Setup}', \mathsf{OT}', \mathsf{Ver}', \mathsf{TrapGen}', \mathsf{Ext}'$ be the committed-bit OT. Set $\ell = \log_{\epsilon^2/\delta}(2\lambda)$, and $t = \frac{1}{2\delta^\ell}$. Note that $\ell = O(\lambda)$ and $t = \mathrm{poly}(\lambda)$. Our protocol between receiver R and sender S is defined as follows.

$(1, 1/2, 0)$ committed-bit OT

- $\mathsf{Setup}\langle R(1^\lambda), S(1^\lambda)\rangle$:
  - For $i \in [\lambda], j \in [t], k \in [\ell]$, the parties run $\mathsf{init}_{R,i,j,k}, \tau_{\mathsf{Setup},i,j,k} \leftarrow \mathsf{Setup}'\langle R'(1^\lambda), S'(1^\lambda)\rangle$.
  - Set $\mathsf{init}_R \coloneqq \{\mathsf{init}_{R,i,j,k}\}_{i,j,k}$.
- $\mathsf{OT}\langle R(b, \mathsf{init}_R), S(\mathsf{init}_S)\rangle$:
  - For $i \in [\lambda]$:
    - R samples $b_i \leftarrow \{0,1\}$.
    - For $j \in [t], k \in [\ell]$, the parties run

      $$(r_{i,j,k}, \mathsf{st}_{R,i,j,k}), (r_{i,j,k,0}, r_{i,j,k,1}, \mathsf{st}_{S,i,j,k}), \tau_{i,j,k} \leftarrow \mathsf{OT}'\langle R'(b_i, \mathsf{init}_{R,i,j,k}), S'(\tau_{\mathsf{Setup},i,j,k})\rangle.$$
  - S samples $i^* \leftarrow [\lambda]$. For $i \in [\lambda] \setminus \{i^*\}$:
    - R sends b_i.
    - For $j \in [t], k \in [\ell]$, the parties run

      $$\mathsf{Ver}'\langle R'(\mathsf{st}_{R,i,j,k}), S'(b_i, \mathsf{st}_{S,i,j,k})\rangle,$$

      and S aborts if any of the results are $\perp$.
  - R sends $b' \coloneqq b \oplus b_i$.
  - S samples $r_0, r_1 \leftarrow \{0,1\}$, sends

    $$\left\{ r'_{j,b'} \coloneqq r_0 \oplus \bigoplus_{k\in[\ell]} r_{i^*,j,k,b'}, \quad r'_{j,1\oplus b'} \coloneqq r_1 \oplus \bigoplus_{k\in[\ell]} r_{i^*,j,k,1\oplus b'} \right\}_{j\in[t]}$$

    to R and outputs r_0, r_1 and $\mathsf{st}_S \coloneqq b', i^*, \{\mathsf{st}_{S_{i^*,j,k}}\}_{j,k}$.

– R outputs

$$r \coloneqq \mathsf{maj}\left\{r'_{j,b_{i^*}} \oplus \bigoplus_{k\in[\ell]} r_{i^*,j,k}\right\}_{j\in[t]}$$

and $\mathsf{st}_R \coloneqq \{\mathsf{st}_{R_{i^*,j,k}}\}_{j,k}$.

- $\mathsf{Ver}\langle R(\mathsf{st}_R), S(b,\mathsf{st}_S)\rangle$:
  - For $j\in[t], k\in[\ell]$, the parties run

$$\mathsf{Ver}'\langle R'(\mathsf{st}_{R,i^*,j,k}), S'(b\oplus b', \mathsf{st}_{S,i^*,j,k})\rangle,$$

    and output $\top$ only if all are $\top$.
- $\mathsf{TrapGen}(\tau_{\mathsf{Setup}})$: For $i\in[\lambda], j\in[t], k\in[\ell]$, run $\mathsf{td}_{i,j,k} \coloneqq \mathsf{TrapGen}'(\tau_{\mathsf{Setup},i,j,k})$ and output $\mathsf{td} \coloneqq \{\mathsf{td}_{i,j,k}\}_{i,j,k}$.
- $\mathsf{Ext}(\mathsf{td},\tau)$: For $j\in[t], k\in[\ell]$, run $b_{j,k} \coloneqq \mathsf{Ext}'(\mathsf{td}_{i^*,j,k}, \tau_{i^*,j,k})$. If there exists b^* such that $b_{j,k}=b^*$ for all j,k, then output $b^*\oplus b'$, and otherwise output 0.

First, we argue correctness. By correctness of OT', we have that for any fixed i^*, j, k,

$$\Pr[\forall k\in[\ell]\ r_{i^*,j,k} = r_{i^*,j,k,b_i}] \geq \epsilon^\ell - \mathrm{negl}(\lambda).$$

Thus, by a Hoeffding inequality, we have that

$$\Pr\left[\mathsf{maj}\left\{\bigoplus_{k\in[\ell]} r_{i^*,j,k} \oplus \bigoplus_{k\in[\ell]} r_{i^*,j,k,b_i}\right\} = 0\right] \geq 1-e^{-2(\epsilon^\ell-\mathrm{negl}(\lambda))^2 t} \geq 1-e^{-(\epsilon^2/\delta)^\ell} - \mathrm{negl}(\lambda) = 1-\mathrm{negl}(\lambda).$$

By construction, this event implies that $r=r_b$, which completes the proof.

Next, completeness follows from the completeness of OT', and receiver security follows from the receiver security of OT' and a standard hybrid argument. Thus, it remains to argue sender security.

We define Hyb_ι for each $\iota = 0,\ldots,t$, as follows. Here, $(\widetilde{R}_{\mathsf{init}}, R)$ is the adversarial receiver, and we describe their interaction with a challenger running a variant of the honest sender algorithms. To avoid notational clutter, we don't explicitly notate the adversary's state as it evolves throughout this process.

$\underline{\mathsf{Hyb}_\iota}$

- For $i\in[\lambda], j\in[t], k\in[\ell]$, run $\tau_{\mathsf{Setup},i,j,k} \leftarrow \mathsf{Setup}'\langle \widetilde{R}_{\mathsf{init}}, S'(1^\lambda)\rangle$ and $\mathsf{td}_{i,j,k} \coloneqq \mathsf{TrapGen}'(\tau_{\mathsf{Setup},i,j,k})$.
- For $i\in[\lambda], j\in[t], k\in[\ell]$, run $(r_{i,j,k,0}, r_{i,j,k,1}, \mathsf{st}_{S,i,j,k}), \tau_{i,j,k} \leftarrow \mathsf{OT}'\langle \widetilde{R}, S'(\tau_{\mathsf{Setup},i,j,k})\rangle$ and $b_{i,j,k} \coloneqq \mathsf{Ext}(\mathsf{td}_{i,j,k}, \tau_{i,j,k})$.
- Sample $i^*\leftarrow[\lambda]$. For $i\in[\lambda]\setminus\{i^*\}$:
  - Receive b_i from $\widetilde{R}$.
  - For $j\in[t], k\in[\ell]$, run $\mathsf{Ver}'\langle \widetilde{R}, S'(b_i, \mathsf{st}_{S,i,j,k})\rangle$, and abort if any of the results are $\bot$.
- Receive b' from $\widetilde{R}$.

- For each $j \in [t], k \in [\ell]$, run $b_{j,k} \coloneqq \mathsf{Ext}'(\mathsf{td}_{i^*,j,k}, \tau_{i^*,j,k})$. If there does not exist b^* such that $b_{j,k} = b^*$ for all j, k, then abort (and the adversary wins with probability exactly $1/2$, i.e. 0 advantage). Otherwise, set $b = b' \oplus b^*$.
- Sample $r_b \leftarrow \{0,1\}$, set $r_{b,j} \coloneqq r_b$ for all $j \in [t]$, set $r_{1\oplus b,j} \coloneqq 1$ for all $j \le \iota$, and set $r_{1\oplus b,j} \coloneqq 0$ for all $j > \iota$.
- Send
$$\left\{ r'_{j,b'} \coloneqq r_{b',j} \oplus \bigoplus_{k\in[\ell]} r_{i^*,j,k,b'}, \quad r'_{j,1\oplus b'} \coloneqq r_{1\oplus b',j} \oplus \bigoplus_{k\in[\ell]} r_{i^*,j,k,1\oplus b'} \right\}_{j\in[t]}$$
and r_b to R.

Now, note that Hyb_0 is the same as the sender security game for $(\widetilde{R}_{\mathsf{init}}, \widetilde{R})$ conditioned on:

- $r_b = 0$, and
- there exists b^* such that $b_{j,k} = b^*$ for all j, k (and the sender did not abort earlier).

Moreover, Hyb_t is the same as the sender security game for $(\widetilde{R}_{\mathsf{init}}, \widetilde{R})$ conditioned on:

- $r_b = 1$, and
- there exists b^* such that $b_{j,k} = b^*$ for all j, k (and the sender did not abort earlier).

Note that the event that there does *not* exist b^* such that $b_{j,k} = b^*$ for all j, k, but the sender did not abort earlier occurs with probability at most $1/\lambda$ due to the sender security (in particular the second part) of OT'. Thus, letting p_i be the probability that $(\widetilde{R}_{\mathsf{init}}, \widetilde{R})$ outputs 0 in Hyb_i, we have that the receiver's advantage in the sender security game is bounded by $|p_0 - p_t| + o(1)$.

To complete the proof, we argue that for any $\iota \in [t]$, $|p_{\iota-1} - p_\iota| \le \delta^\ell + \mathrm{negl}(\lambda)$, as this implies that $|p_0 - p_t| \le t \cdot \delta^\ell + \mathrm{negl}(\lambda) \le 1/2 + \mathrm{negl}(\lambda)$. This follows by a reduction to Corollary 6.18. Indeed, we note that the only difference between $\mathsf{Hyb}_{\iota-1}$ and Hyb_ι is the bit $r_{1\oplus b,\iota}$, which is masked by $\bigoplus_{k\in[\ell]} r_{i^*,\iota,k,1\oplus b}$. Thus, it suffices to argue that an appropriate ℓ-wise sequential repetition of the sender security game of OT' yields advantage $\delta^\ell + \mathrm{negl}(\lambda)$. In particular, it suffices to show that adversary has $\delta^\ell + \mathrm{negl}(\lambda)$ advantage in the following game.

- For $k \in [\ell]$, run $\tau_{\mathsf{Setup},k} \leftarrow \mathsf{Setup}'\langle \widetilde{R}_{\mathsf{init}}, S'(1^\lambda)\rangle$ and $\mathsf{td}_k \leftarrow \mathsf{TrapGen}'(\tau_{\mathsf{Setup},k})$.
- For $k \in [\ell]$, run $(r_{k,0}, r_{k,1}), \tau_k \leftarrow \mathsf{OT}'\langle \widetilde{R}, S'(\tau_{\mathsf{Setup},k})\rangle$, $b_k \coloneqq \mathsf{Ext}(\mathsf{td}_k, \tau_k)$, and send r_{b_k} to $\widetilde{R}$.
- $\widetilde{R}$ outputs a bit r^* and wins if $r^* = \bigoplus_{k\in[\ell]} r_{1\oplus b_k}$.

By the sender security of OT', we know that with $1 - \mathrm{negl}(\lambda)$ probability over
$$\left\{ \tau_{\mathsf{Setup},k} \leftarrow \mathsf{Setup}'\langle \widetilde{R}_{\mathsf{init}}, S'(1^\lambda)\rangle, \quad \mathsf{td}_k \coloneqq \mathsf{TrapGen}'(\tau_{\mathsf{Setup},k}) \right\}_{k\in[\ell]},$$
$\widetilde{R}$ has advantage at most $\delta + \mathrm{negl}(\lambda)$ in guessing $r_{1\oplus b_k}$ for any fixed $k \in [\ell]$, even given arbitrary inefficiently-computable advice about $\tau_{\mathsf{Setup},1}, \ldots, \tau_{\mathsf{Setup},\ell}$. Thus, it suffices to show that for any such $\tau_{\mathsf{Setup},1}, \ldots, \tau_{\mathsf{Setup},\ell}$, $\widetilde{R}$ has advantage at most $\delta^\ell + \mathrm{negl}(\lambda)$ in guessing $\bigoplus_{k\in[\ell]} r_{1\oplus b_k}$. This follows directly from Corollary 6.18, by setting each Γ_k to run $(r_{k,0}, r_{k,1}), \tau_k \leftarrow \mathsf{OT}'\langle \widetilde{R}, S'(\tau_{\mathsf{Setup},k})\rangle$ and the predicate P to compute $b_k \coloneqq \mathsf{Ext}(\mathsf{td}_k, \tau_k)$ and output $r_{1\oplus b_k}$.

□

References

[ACC+22] Per Austrin, Hao Chung, Kai-Min Chung, Shiuan Fu, Yao-Ting Lin, and Mohammad Mahmoody. On the impossibility of key agreements from quantum random oracles. In *Advances in Cryptology – CRYPTO 2022: 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15–18, 2022, Proceedings, Part II*, page 165–194, Berlin, Heidelberg, 2022. Springer-Verlag.

[AMR22] Navid Alamati, Giulio Malavolta, and Ahmadreza Rahimi. Candidate trapdoor claw-free functions from group actions with applications to quantum protocols. In Eike Kiltz and Vinod Vaikuntanathan, editors, *Theory of Cryptography*, pages 266–293, Cham, 2022. Springer Nature Switzerland.

[BCM+21] Zvika Brakerski, Paul Christiano, Urmila Mahadev, Umesh Vazirani, and Thomas Vidick. A cryptographic test of quantumness and certifiable randomness from a single quantum device. *J. ACM*, 68(5), August 2021.

[BGKM+23] Zvika Brakerski, Alexandru Gheorghiu, Gregory D. Kahanamoku-Meyer, Eitan Porat, and Thomas Vidick. Simple tests of quantumness also certify qubits. In Helena Handschuh and Anna Lysyanskaya, editors, *Advances in Cryptology – CRYPTO 2023*, pages 162–191, Cham, 2023. Springer Nature Switzerland.

[BK25] James Bartusek and Dakshita Khurana. On the power of oblivious state preparation. In *Advances in Cryptology – CRYPTO 2025: 45th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17–21, 2025, Proceedings, Part II*, page 575–607, Berlin, Heidelberg, 2025. Springer-Verlag.

[BMM25] Pedro Branco, Giulio Malavolta, and Zayd Maradni. Fully-homomorphic encryption from lattice isomorphism. In *Theory of Cryptography: 23rd International Conference, TCC 2025, Aarhus, Denmark, December 1–5, 2025, Proceedings, Part I*, page 220–252, Berlin, Heidelberg, 2025. Springer-Verlag.

[BQSY24] John Bostanci, Luowen Qian, Nicholas Spooner, and Henry Yuen. An efficient quantum parallel repetition theorem and applications. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*, STOC 2024, page 1478–1487, New York, NY, USA, 2024. Association for Computing Machinery.

[BSW03] Boaz Barak, Ronen Shaltiel, and Avi Wigderson. Computational analogues of entropy. In Sanjeev Arora, Klaus Jansen, José D. P. Rolim, and Amit Sahai, editors, *Approximation, Randomization, and Combinatorial Optimization.. Algorithms and Techniques*, pages 200–215, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg.

[CMM+26] David Cui, Giulio Malavolta, Arthur Mehta, Anand Natarajan, Connor Paddock, Simon Schmidt, Michael Walter, and Tina Zhang. A Computational Tsirelson's Theorem for the Value of Compiled XOR Games. *Quantum*, 10:1987, January 2026.

[CMSZ22] Alessandro Chiesa, Fermi Ma, Nicholas Spooner, and Mark Zhandry. Post-quantum succinct arguments: Breaking the quantum rewinding barrier. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 49–58, 2022.

[DH76] Whitfield Diffie and Martin E Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

[DNS10] Frédéric Dupuis, Jesper Buus Nielsen, and Louis Salvail. Secure two-party quantum evaluation of unitaries against specious adversaries. In Tal Rabin, editor, *Advances in Cryptology – CRYPTO 2010*, pages 685–706, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[GKM+00] Y. Gertner, S. Kannan, T. Malkin, O. Reingold, and M. Viswanathan. The relationship between public key encryption and oblivious transfer. In *Proceedings of the 41st Annual Symposium on Foundations of Computer Science*, FOCS '00, page 325, USA, 2000. IEEE Computer Society.

[GMW87] O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game. In *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing*, STOC '87, page 218–229, New York, NY, USA, 1987. Association for Computing Machinery.

[GNW11] Oded Goldreich, Noam Nisan, and Avi Wigderson. *On Yao's XOR-Lemma*, pages 273–301. Springer Berlin Heidelberg, Berlin, Heidelberg, 2011.

[GV19] Alexandru Gheorghiu and Thomas Vidick. Computationally-secure and composable remote state preparation. *2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1024–1033, 2019.

[HK25] Andrew Huang and Yael Tauman Kalai. Parallel repetition for post-quantum arguments. Cryptology ePrint Archive, Paper 2025/1027, 2025.

[HMOY25] Minki Hhan, Tomoyuki Morimae, Yasuaki Okinaka, and Takashi Yamakawa. Proofs of quantum memory, 2025.

[Hol05] Thomas Holenstein. Key agreement from weak bit agreement. In *Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing*, STOC '05, page 664–673, New York, NY, USA, 2005. Association for Computing Machinery.

[HR08] Shai Halevi and Tal Rabin. Degradation and amplification of computational hardness. In *Proceedings of the 5th Conference on Theory of Cryptography*, TCC'08, page 626–643, Berlin, Heidelberg, 2008. Springer-Verlag.

[HS11] Thomas Holenstein and Grant Schoenebeck. General hardness amplification of predicates and puzzles. In *Proceedings of the 8th Conference on Theory of Cryptography*, TCC'11, page 19–36, Berlin, Heidelberg, 2011. Springer-Verlag.

[Imp95] R. Impagliazzo. Hard-core distributions for somewhat hard problems. In *Proceedings of the 36th Annual Symposium on Foundations of Computer Science*, FOCS '95, page 538, USA, 1995. IEEE Computer Society.

[IR89] R. Impagliazzo and S. Rudich. Limits on the provable consequences of one-way permutations. In *Proceedings of the Twenty-First Annual ACM Symposium on Theory of Computing*, STOC '89, page 44–61, New York, NY, USA, 1989. Association for Computing Machinery.

[Kil88] Joe Kilian. Founding cryptography on oblivious transfer. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, STOC '88, page 20–31, New York, NY, USA, 1988. Association for Computing Machinery.

[KLVY23] Yael Kalai, Alex Lombardi, Vinod Vaikuntanathan, and Lisa Yang. Quantum advantage from any non-local game. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, STOC 2023, page 1617–1628, New York, NY, USA, 2023. Association for Computing Machinery.

[KMCVY22] Gregory D. Kahanamoku-Meyer, Soonwon Choi, Umesh V. Vazirani, and Norman Y. Yao. Classically verifiable quantum advantage from a computational Bell test. *Nature Physics*, 18(8), 08 2022.

[Kre21] William Kretschmer. Quantum pseudorandomness and classical complexity. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021.

[KT24] Dakshita Khurana and Kabir Tomer. Commitments from quantum one-wayness. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*, STOC 2024, page 968–978, New York, NY, USA, 2024. Association for Computing Machinery.

[Lev85] L A Levin. One-way functions and pseudorandom generators. In *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing*, STOC '85, page 363–365, New York, NY, USA, 1985. Association for Computing Machinery.

[LLLL25] Longcheng Li, Qian Li, Xingjian Li, and Qipeng Liu. Cryptomania v.s. Minicrypt in a Quantum World. Cryptology ePrint Archive, Paper 2025/639, 2025.

[Mah22] Urmila Mahadev. Classical verification of quantum computations. *SIAM Journal on Computing*, 51(4):1172–1229, 2022.

[MDCAF21] Tony Metger, Yfke Dulek, Andrea Coladangelo, and Rotem Arnon-Friedman. Device-independent quantum key distribution from computational assumptions. *New J. Phys.*, 23(12):123021, 2021.

[MSY25] Tomoyuki Morimae, Yuki Shirakawa, and Takashi Yamakawa. Cryptographic characterization of quantum advantage. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, STOC '25, page 1863–1874, New York, NY, USA, 2025. Association for Computing Machinery.

[MV21] Tony Metger and Thomas Vidick. Self-Testing of a Single Quantum Device Under Computational Assumptions. In James R. Lee, editor, *12th Innovations in Theoretical Computer Science Conference (ITCS 2021)*, volume 185 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 19:1–19:12, Dagstuhl, Germany, 2021. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[MW04] Chris Marriott and John Watrous. Quantum Arthur-Merlin games. In *Proceedings of the 19th IEEE Annual Conference on Computational Complexity*, CCC '04, page 275–285, USA, 2004. IEEE Computer Society.

[MY22] Tomoyuki Morimae and Takashi Yamakawa. *Quantum Commitments and Signatures Without One-Way Functions*, page 269–295. Springer Nature Switzerland, 2022.

[Nao89] Moni Naor. Bit commitment using pseudo-randomness. In *Proceedings of the 9th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '89, page 128–136, Berlin, Heidelberg, 1989. Springer-Verlag.

[NZ23] Anand Natarajan and Tina Zhang. Bounding the quantum value of compiled nonlocal games: from CHSH to BQP verification, 2023.

[TZ25] Kabir Tomer and Mark Zhandry. On the cryptographic foundations of interactive quantum advantage, 2025.

[Vid20] Thomas Vidick. Course FSMP, Fall'20: Interactions with quantum devices, 2020.

[vN28] John von Neumann. Zur theorie der gesellschaftsspiele. *Mathematische Annalen*, 100(1):295–320, 1928.

[Wul07] Jürg Wullschleger. Oblivious-transfer amplification. In *Proceedings of the 26th Annual International Conference on Advances in Cryptology*, EUROCRYPT '07, page 555–572, Berlin, Heidelberg, 2007. Springer-Verlag.

[YZ24] Takashi Yamakawa and Mark Zhandry. Verifiable quantum advantage without structure. *J. ACM*, 71(3), June 2024.

[Zha23] Jiayu Zhang. A quantum approach for reducing communications in classical secure computations with long outputs. Cryptology ePrint Archive, Paper 2023/1492, 2023.

[Zha25] Jiayu Zhang. Formulations and Constructions of Remote State Preparation with Verifiability, with Applications. In Raghu Meka, editor, *16th Innovations in Theoretical Computer Science Conference (ITCS 2025)*, volume 325 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 96:1–96:19, Dagstuhl, Germany, 2025. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.