An All-But-One Entropic Uncertainty Relation, and Application to Password-Based Identification

Niek J. Bouman[1], Serge Fehr[1],
Carlos González-Guillén[2,3], and Christian Schaffner[4,1]

[1] Centrum Wiskunde & Informatica (CWI), Amsterdam, The Netherlands
[2] Depto. de Matemática Aplicada, Technical University of Madrid, Spain
[3] IMI, Universidad Complutense de Madrid, Spain
[4] University of Amsterdam (UvA), The Netherlands

Abstract. Entropic uncertainty relations are quantitative characterizations of Heisenberg's uncertainty principle, which make use of an entropy measure to quantify uncertainty. We propose a new entropic uncertainty relation. It is the first such uncertainty relation that lower bounds the uncertainty in the measurement outcome for *all but one* choice for the measurement from an arbitrary (and in particular an arbitrarily *large*) set of possible measurements, and, at the same time, uses the *min-entropy* as entropy measure, rather than the Shannon entropy. This makes it especially suited for quantum cryptography.

As application, we propose a new *quantum identification scheme* in the bounded-quantum-storage model. It makes use of our new uncertainty relation at the core of its security proof. In contrast to the original quantum identification scheme proposed by Damgård *et al.* [4], our new scheme also offers some security in case the bounded-quantum-storage assumption fails to hold. Specifically, our scheme remains secure against an adversary that has unbounded storage capabilities but is restricted to (non-adaptive) single-qubit operations. The scheme by Damgård *et al.*, on the other hand, completely breaks down under such an attack.

1 Introduction

In this work[1], we propose and prove a new general entropic uncertainty relation. Entropic uncertainty relations are quantitative characterizations of Heisenberg's uncertainty principle, which make use of an entropy measure (usually Shannon entropy) to quantify uncertainty. Our new entropic uncertainty relation distinguishes itself from previously known uncertainty relations by the following collection of features:

1. It uses the *min-entropy* as entropy measure, which is a *stronger* type of uncertainty than Shannon entropy. Since min-entropy allows for privacy amplification, such entropic uncertainty relations are useful tools in quantum cryptography.

[1] The full version of this paper can be found online [2].

K. Iwama, Y. Kawano, and M. Murao (Eds.): TQC 2012, LNCS 7582, pp. 29–44, 2013.

2. It lower bounds the uncertainty in the measurement outcome for *all but one* choice for the measurement from an *arbitrary*, and in particular arbitrarily large, family of possible measurements. This is clearly *stronger* than typical entropic uncertainty relations that lower bound the uncertainty on *average* (over the choice of the measurement).
3. The measurements can be chosen to be qubit-wise measurements, in the computational or Hadamard basis, and thus the uncertainty relation is applicable to settings that can be implemented using current technology.

To the best of our knowledge, no previous entropic uncertainty relation satisfies (1) and (2) simultaneously, let alone in combination with (3). Indeed, as pointed out in the recent overview article by Wehner and Winter [13], little is known about entropic uncertainty relations for more than two measurement outcomes, let alone when considering min-entropy.

In the remainder of this introduction, we explain the statement of our new uncertainty relation and we discuss an application: we propose a new password-based quantum identification scheme, whose security (in the bounded-quantum-storage model) relies on the new uncertainty relation.

Our Result Explained. To better understand our new uncertainty relation, we find it helpful to first discuss a simpler variant, which does not satisfy (1), and which follows trivially from known results. Fix an arbitrary family $\{\mathcal{B}_1, \ldots, \mathcal{B}_m\}$ of bases for a given quantum system (i.e., Hilbert space). The *maximum overlap* of such a family is defined as $c := \max\{|\langle\phi|\psi\rangle| : |\phi\rangle \in \mathcal{B}_j, |\psi\rangle \in \mathcal{B}_k, 1 \leq j < k \leq m\}$, and we write $d := -\log(c^2)$. Let ρ be an arbitrary quantum state of that system, and let X denote the measurement outcome when ρ is measured in one of the bases. We model the choice of the basis by a random variable J, so that $H(X|J=j)$ denotes the Shannon entropy of the measurement outcome when ρ is measured in basis $\mathcal{B}_j$. It follows immediately from Maassen and Uffink's uncertainty relation [8] that $H(X|J=j) + H(X|J=k) \geq -\log(c^2) = d$ for any $j \neq k$. As a direct consequence, there exists a choice j' for the measurement so that $H(X|J=j) \geq \frac{d}{2}$ for all $j \in \{1, \ldots, m\}$ with $j \neq j'$. In other words, for any state ρ there exists j' so that unless the choice for the measurement coincides with j', which happens with probability at most $\max_j P_J(j)$, there is at least $d/2$ bits of entropy in the outcome X.

Our new high-order entropic uncertainty relation shows that this very statement essentially still holds when we replace Shannon by min-entropy, except that j' becomes randomized: for any ρ, there exists a *random variable* J', independent of J, such that[2]

$$H_{\min}(X|J=j, J'=j') \gtrsim \frac{d}{2} \quad \forall\, j \neq j' \in \{1, \ldots, m\}$$

no matter what the distribution of J is. Thus, unless the measurement J coincides with J', there is roughly $d/2$ bits of min-entropy in the outcome X.

[2] The approximate inequality $\gtrsim$ will be made rigorous in the main body.

Furthermore, since J' is *independent* of J, the probability that J coincides with J' is at most $\max_j P_J(j)$, as is the case for a fixed J'.

Note that we have no control over (the distribution of) J'. We can merely guarantee that it exists and is independent of J. It may be insightful to interpret J' as a *virtual guess* for J, guessed by the party that prepares ρ, and whose goal is to have little uncertainty in the measurement outcome X. The reader may think of the following specific way of preparing ρ: sample j' according to some arbitrary distribution J', and then prepare the state as the, say, first basis vector of $\mathcal{B}_{j'}$. If the resulting mixture ρ is then measured in some basis $\mathcal{B}_j$, sampled according to an arbitrary (independent) distribution J, then unless $j = j'$ (i.e., our guess for j was correct), there is obviously lower bounded uncertainty in the measurement outcome X (assuming a non-trivial maximum overlap). Our uncertainty relation can be understood as saying that for *any* state ρ, no matter how it is prepared, there exists such a (virtual) guess J', which exhibits this very behavior: if it differs from the actual choice for the measurement then there is lower bounded uncertainty in the measurement outcome X. As an immediate consequence, we can for instance say that X has min-entropy at least $d/2$, except with a probability that is given by the probability of guessing J, e.g., except with probability $1/m$ if the measurement is chosen uniformly at random from the family. This is clearly the best we can hope for.

We stress that because the min-entropy is more conservative than the Shannon entropy, our high-order entropic uncertainty relation does not follow from its simpler Shannon-entropy version. Neither can it be deduced in an analogue way; the main reason being that for fixed pairs $j \neq k$, there is no strong lower bound on $H_{\min}(X|J=j) + H_{\min}(X|J=k)$, in contrast to the case of Shannon entropy. More precisely and more generally, the *average* uncertainty $\frac{1}{|J|}\sum_j H_{\min}(X|J=j)$ does not allow a lower bound higher than $\log|J|$. To see this, consider the following example for $|J| = 2$ (the example can easily be extended to arbitrary $|J|$). Suppose that ρ is the uniform mixture of two pure states, one giving no uncertainty when measured in basis j, and the other giving no uncertainty when measured in basis k. Then, $H_{\min}(X|J=j) = H_{\min}(X|J=k) = 1$ and so is their average. For a similar reason, we cannot hope to get a good bound for all but a *fixed* choice of j'; the probabilistic nature of J' is necessary (in general). Hence, compared to bounding the average uncertainty, the all-but-one form of our uncertainty relation not only makes our uncertainty relation stronger in that uncertainty for all-but-one implies uncertainty on average (yet not vice versa), but it also allows for *more* uncertainty.

Note that by using asymptotically good error correcting codes, one can construct families $\{\mathcal{B}_1, \ldots, \mathcal{B}_m\}$ of bases that have a large value of d, and thus for which our uncertainty relation guarantees a large amount of min-entropy. These families consist of qubit-wise measurements in the computational or the Hadamard basis, and thus are implementable with current technology.

The proof of our new uncertainty relation is rather involved. First, we extend a technique used in (the journal version of) [3], which is based on a norm inequality for the sum of orthogonal projectors, and then we combine this with some

involved probability reasoning to prove the existence of the random variable J' as required.

Application. As an application of our entropic uncertainty relation, we propose a new *quantum identification scheme*. Informally, the goal of (password-based) identification is to prove knowledge of a possibly low-entropy password w, without giving away any information on w (beyond what is unavoidable).

It is known (see [4]) that any quantum identification scheme can be broken by a dishonest participant having unbounded quantum storage *and* unbounded quantum-computation capabilities. Damgård *et al.* [4] showed the existence of such an identification scheme[3] in the *bounded-quantum-storage model* (BQSM), where an upper bound is assumed on the number of qubits that the dishonest server can store. If, however, this assumption fails to hold, then the security of the scheme of Damgård *et al.* breaks down completely. Hence, it would actually be desirable to have an identification scheme for which unbounded quantum storage *and* unbounded quantum-computation capabilities are *necessary* to break it. Our new scheme can be appreciated as a first step towards achieving this, in that large quantum storage and *non-trivial* quantum computation capabilities are necessary for a successful attack. A disadvantage of our scheme is that it only offers security in case of a perfect quantum source, which emits precisely one qubit when triggered (i.e., there is no multi-photon emission or the like). Since current technology only admits (close to) perfect quantum sources under "lab conditions," our scheme is currently mainly of theoretical interest.

Our uncertainty relation gives us the right tool to prove security of the new quantum identification scheme in the BQSM. Additionally, we prove security of our new scheme in the so-called *single-qubit-operations model* (SQOM), i.e., against a dishonest server that has unbounded quantum-storage capabilities and can reliably store all the qubits communicated during the course of the scheme, but is restricted to single-qubit operations and measurements (i.e., cannot operate on several qubits coherently). Proving security of our scheme in the SQOM is non-trivial.

2 Preliminaries

We write $\mathcal{D}(\mathcal{H})$ for the set of all density matrices on Hilbert space $\mathcal{H}$.

Definition 1 (Min-Entropy [10,7]). *For any density matrix $\rho_{XE} \in \mathcal{D}(\mathcal{H}_{XE})$ with classical X, the min-entropy of X when given $\mathcal{H}_E$ is defined as*

$$H_{\min}(X|E) := -\log p_{\text{guess}}(X|E)$$

where the guessing probability $p_{\text{guess}}(X|E) := \max_{\{M_x\}} \sum_x P_X(x) \operatorname{tr}(M_x \rho_E^x)$ is the maximal success probability of guessing X by a positive operator-valued measurement $\{M_x\}$ of E.

[3] Actually, [4] proposed *two* such schemes: QID and QID$^+$. QID offers security against *impersonation attacks*, and QID$^+$ additionally offers security against *man-in-the-middle attacks* but is not truly password-based. In this work, we focus on impersonation attacks only (with truly password-based security).

For classical random variables X and Y, the conditional min-entropy $H_{\min}(X|Y)$ simplifies to $H(X|Y) = -\log \sum_y P_Y(y) \max_x P_{X|Y}(x|y) = -\log \sum_y \max_x P_{XY}(x,y)$.

For a matrix ρ, the trace norm is defined as $\|\rho\|_1 := \mathrm{tr}\sqrt{\rho\rho^*}$, where ρ^* denotes the Hermitian transpose of ρ.

Definition 2 (Trace Distance [9]). *The* trace distance *between two density matrices $\rho, \sigma \in \mathcal{D}(\mathcal{H})$ is defined as $\delta(\rho,\sigma) := \frac{1}{2}\|\rho - \sigma\|_1$.*

If two states ρ and σ are ε-close in trace distance, i.e. $\frac{1}{2}\|\rho - \sigma\|_1 \leq \varepsilon$, we use $\rho \approx_\varepsilon \sigma$ as shorthand.

Definition 3 (Distance to Uniform). *For a density matrix $\rho_{XE} \in \mathcal{D}(\mathcal{H}_X \otimes \mathcal{H}_E)$ with classical X, the* distance to uniform *of X given E is defined as*

$$d_{\mathrm{unif}}(X|E) := \tfrac{1}{2}\|\rho_{XE} - \rho_U \otimes \rho_E\|_1,$$

where $\rho_U := \frac{1}{\dim(\mathcal{H}_X)}\mathbb{I}_X$.

Definition 4 (Conditional Independence [4]). *For a density matrix on $\mathcal{D}(\mathcal{H}_X \otimes \mathcal{H}_Y \otimes \mathcal{H}_E)$ with classical X and Y for which the random variable X is independent of the quantum subsystem E* when given the random variable Y, *we write $\rho_{X\leftrightarrow Y\leftrightarrow E}$, i.e.,*

$$\rho_{X\leftrightarrow Y\leftrightarrow E} := \sum_{x,y} P_{XY}(x,y)|x\rangle\langle x| \otimes |y\rangle\langle y| \otimes \rho_E^y.$$

3 Formal Statement and Proof of the Main Result

To obtain our entropic uncertainty relation that lower bounds the min-entropy of the measurement outcome for all but one measurement, we first state an uncertainty relation that expresses uncertainty by means of the probability measure of given sets.

As above, $\{\mathcal{B}_1, \ldots, \mathcal{B}_m\}$ is an arbitrary but fixed family of bases for the state space $\mathcal{H}$ of a quantum system, and c denotes the maximum overlap. For simplicity, we restrict our attention to an n-qubit system, such that $\mathcal{H} = (\mathbb{C}^2)^{\otimes n}$ for $n \in \mathbb{N}$, but our results immediately generalize to arbitrary quantum systems.

Theorem 5 (Theorem 4.18 in [12]). *Let ρ be an arbitrary state of n qubits. For $j \in [m]$, let $Q^j(\cdot)$ be the distribution of the outcome when ρ is measured in the $\mathcal{B}_j$-basis. Then, for any family $\{\mathcal{L}^j\}_{j\in[m]}$ of subsets $\mathcal{L}^j \subset \{0,1\}^n$, it holds that*

$$\sum_{j\in[m]} Q^j(\mathcal{L}^j) \leq 1 + c\,(m-1) \cdot \max_{j\neq k\in[m]} \sqrt{|\mathcal{L}^j||\mathcal{L}^k|}.$$

A special case of Theorem 5, obtained by restricting the family of bases to $\{\mathcal{B}_+, \mathcal{B}_\times\}$ with $\mathcal{B}_+ = \{|x\rangle\}_{x\in\{0,1\}^n}$ and $\mathcal{B}_\times = \{H^{\otimes n}|x\rangle\}_{x\in\{0,1\}^n}$ (i.e., either the computational or Hadamard basis for all qubits), is an uncertainty relation that

was proven and used in the original paper about the BQSM [3]. The proof of Theorem 5 (Appendix A.2) goes along similar lines as the proof in the journal version of [3] for the special case outlined above. It is based on the norm inequality (see Appendix A.1)

$$\big\|A_1 + \ldots + A_m\big\| \leq 1 + (m-1) \cdot \max_{j \neq k \in [m]} \big\|A_j A_k\big\|$$

for arbitrary orthogonal projectors $A_1, \ldots, A_m$, where $\|\cdot\|$ denotes the operator norm.

We can reformulate Theorem 5 in terms of a "good event" $\mathcal{E}$ with lower bounded probability, and if it occurs, then the measurement outcome has high min-entropy. The statement is obtained by choosing the sets $\mathcal{L}^j$ in Theorem 5 appropriately (see Appendix A.3).

Because we now switch to entropy notation, it will be convenient to work with a measure of overlap between bases that is logarithmic in nature and expressed *relative* to the number n of qubits. Hence, we define $\delta := -\frac{1}{n}\log(c^2)$.

Corollary 6. *Let ρ be an arbitrary n-qubit state, let J be a random variable over $[m]$, and let X be the outcome when measuring ρ in basis $\mathcal{B}_J$.*[4] *Then, for any $0 < \epsilon < \delta/4$, there exists an event $\mathcal{E}$ such that*

$$\sum_{j \in [m]} \Pr[\mathcal{E}|J{=}j] \geq (m-1) - (2m-1) \cdot 2^{-\epsilon n}$$

$$\text{and} \qquad H_{\min}(X|J{=}j, \mathcal{E}) \geq \Big(\frac{\delta}{2} - 2\epsilon\Big)n$$

for $j \in [m]$ with $P_{J|\mathcal{E}}(j) > 0$.

We will now state and prove our main result.

Theorem 7 (Our New Uncertainty Relation). *Let ρ be an arbitrary n-qubit state, let J be a random variable over $[m]$, and let X be the outcome when measuring ρ in basis $\mathcal{B}_J$. Then, for any $0 < \epsilon < \delta/4$, there exists a random variable J' such that (1) J and J' are independent and (2) there exists an event Ω with $\Pr[\Omega] \geq 1 - 2 \cdot 2^{-\epsilon n}$ such that*[5]

$$H_{\min}(X|J = j, J' = j', \Omega) \geq \Big(\frac{\delta}{2} - 2\epsilon\Big)n - 1$$

for all $j, j' \in [m]$ with $j \neq j'$ and $P_{JJ'|\Omega}(j, j') > 0$.

Proof (of Theorem 7). From Corollary 6 we know that for any $0 < \epsilon < \delta/4$, there exists an event $\mathcal{E}$ such that $\sum_{j \in [m]} \Pr[\mathcal{E}|J = j] = m - 1 - \alpha$, and thus $\sum_{j \in [m]} \Pr[\bar{\mathcal{E}}|J = j] = 1 + \alpha$, for $-1 \leq \alpha \leq (2m-1)2^{-\epsilon n}$. We make the case distinction between $\alpha = 0$, $\alpha > 0$ and $\alpha < 0$. We will only proof the case $\alpha = 0$

[4] I.e., $P_{X|J}(x|j) = Q^j(x)$, using the notation from Theorem 5.

[5] Instead of introducing such an event Ω, we could also express the min-entropy bound by means of the *smooth* min-entropy of X given $J = j$ and $J' = j'$.

here; the other two cases are proved in Appendix A.4, by reducing them to the case $\alpha = 0$ by "inflating" and "deflating" the event $\mathcal{E}$ appropriately. The approach for the case $\alpha = 0$ is to define J' in such way that $\mathcal{E} \iff J \neq J'$, i.e., the event $J \neq J'$ coincides with the event $\mathcal{E}$. The min-entropy bound from Corollary 6 then immediately translates to $H_{\min}(X|J = j, J' \neq J) \geq (\delta/2 - 2\epsilon)n$, and to $H_{\min}(X|J = j, J' = j') \geq (\delta/2 - 2\epsilon)n$ for $j' \neq j$ with $P_{JJ'}(j, j') > 0$, as we will show. What is not obvious about the approach is how to define J' when it is supposed to be different from J, i.e., when the event $\mathcal{E}$ occurs, so that in the end J and J' are independent.

Formally, we define J' by means of the following conditional probability distributions:

$$P_{J'|JX\bar{\mathcal{E}}}(j'|j,x) := \begin{cases} 1 \text{ if } j = j' \\ 0 \text{ if } j \neq j' \end{cases}$$

$$P_{J'|JX\mathcal{E}}(j'|j,x) := \begin{cases} 0 & \text{if } j = j' \\ \frac{\Pr[\bar{\mathcal{E}}|J=j']}{\Pr[\mathcal{E}|J=j]} & \text{if } j \neq j' \end{cases}$$

We assume for the moment that the denominator in the latter expression does not vanish for any j; we take care of the case where it does later. Trivially, $P_{J'|JX\bar{\mathcal{E}}}$ is a proper distribution, with non-negative probabilities that add up to 1, and the same holds for $P_{J'|JX\mathcal{E}}$:

$$\sum_{j' \in [m]} P_{J'|JX\bar{\mathcal{E}}}(j'|j,x) = \sum_{j' \in [m] \setminus \{j\}} P_{J'|JX\bar{\mathcal{E}}}(j'|j,x) = \sum_{j' \in [m] \setminus \{j\}} \frac{\Pr[\bar{\mathcal{E}}|J = j']}{\Pr[\mathcal{E}|J = j]} = 1,$$

where we used that $\sum_{j \in [m]} \Pr[\bar{\mathcal{E}}|J = j] = 1$ (because $\alpha = 0$) in the last equality. Furthermore, it follows immediately from the definition of J' that $\bar{\mathcal{E}} \implies J = J'$ and $\mathcal{E} \implies J \neq J'$. Hence, $\mathcal{E} \iff J \neq J'$, and thus the bound from Corollary 6 translates to $H_{\min}(X|J = j, J' \neq J) \geq (\delta/2 - 2\epsilon)n$. It remains to argue that J' is independent of J, and that the bound also holds for $H_{\min}(X|J = j, J' = j')$ whenever $j \neq j'$.

The latter follows immediately from the fact that conditioned on $J \neq J'$ (which is equivalent to $\mathcal{E}$), X, J and J' form a Markov chain $X \leftrightarrow J \leftrightarrow J'$, and thus, given $J = j$, additionally conditioning on $J' = j'$ does not change the distribution of X. For the independence of J and J', consider the joint probability distribution of J and J', given by

$$\begin{aligned} P_{JJ'}(j,j') &= P_{J'J\mathcal{E}}(j',j) + P_{J'J\bar{\mathcal{E}}}(j',j) \\ &= P_J(j)\Pr[\mathcal{E}|J=j]P_{J'|J\mathcal{E}}(j'|j) + P_J(j)\Pr[\bar{\mathcal{E}}|J=j]P_{J'|J\bar{\mathcal{E}}}(j'|j) \\ &= P_J(j)\Pr[\bar{\mathcal{E}}|J=j'], \end{aligned}$$

where the last equality follows by separately analyzing the cases $j = j'$ and $j \neq j'$. It follows immediately that the marginal distribution of J' is $P_{J'}(j') = \sum_j P_{JJ'}(j,j') = \Pr[\bar{\mathcal{E}}|J = j']$, and thus $P_{JJ'} = P_J \cdot P_{J'}$.

What is left to do for the case $\alpha = 0$ is to deal with the case where there exists j^* with $\Pr[\mathcal{E}|J = j^*] = 0$. Since $\sum_{j \in [m]} \Pr[\bar{\mathcal{E}}|J = j] = 1$, it holds that

$\Pr[\bar{\mathcal{E}}|J = j] = 0$ for $j \neq j^*$. This motivates to define J' as $J' := j^*$ with probability 1. Note that this definition directly implies that J' is independent from J. Furthermore, by the above observations: $\mathcal{E} \iff J \neq J'$. This concludes the case $\alpha = 0$; the rest of the proof is found in Appendix A.4.

4 A New Quantum Identification Scheme

The goal of (password-based) identification is to "prove" knowledge of a password w (or PIN) without giving w away. More formally, given a *user* U and a *server* S that hold a pre-agreed password w, the user wants to convince the server that he indeed knows w, but in such a way that he gives away as little information on w as possible in case he is actually interacting with a dishonest server. We use the security definitions of [4].

Definition 8 (Correctness). *An identification protocol is said to be* ε-correct *if, after an execution by honest* U *and honest* S, S *accepts with probability* $1 - \varepsilon$.

Definition 9 (Server Security). *An identification protocol for two parties* U, S *is* ε*-secure for the server* S *against (dishonest) user* U^* *if the following holds: whenever the initial state of* U^* *is independent of* W*, then there exists a random variable* W' *(possibly* $\perp$*) that is independent of* W *such that if* $W \neq W'$ *then* S *accepts with probability at most* ε*. Furthermore, the common state* ρ_{WE} *after execution of the protocol (including* S*'s announcement to accept or reject) satisfies*

$$\rho_{WW'E|W\neq W'} \approx_\varepsilon \rho_{W\leftrightarrow W'\leftrightarrow E|W\neq W'}.$$

Definition 10 (User Security). *An identification protocol for two parties* U, S *is* ε*-secure for the user* U *against (dishonest) server* S^* *if the following holds: If the initial state of* S^* *is independent of* W*, then its state* E *after execution of the protocol is such that there exists a random variable* W' *that is independent of* W *and such that*

$$\rho_{WW'E|W\neq W'} \approx_\varepsilon \rho_{W\leftrightarrow W'\leftrightarrow E|W\neq W'}.$$

Our new identification scheme, `Q-ID`, is shown below, where $\mathcal{F}$ is a universal class of functions[6] from $\{0,1\}^n$ to $\{0,1\}^\ell$ and $\mathcal{G}$ is a strongly universal class of functions from $[m]$ to $\{0,1\}^\ell$. We use the following simple construction for the family $\{\mathcal{B}_1, \ldots, \mathcal{B}_m\}$ of bases. For a suitable binary code $\mathcal{C} \subset \{0,1\}^n$ of size m, minimum distance d and encoding function $\mathfrak{c} : [m] \to \mathcal{C}$, the basis $\mathcal{B}_j$ measures qubit-wise in the computational or the Hadamard basis, depending on the corresponding coordinate of $\mathfrak{c}(j)$. The maximum overlap of the family obtained this way is directly related to the minimum distance d of $\mathcal{C}$, namely $\delta = -\frac{1}{n}\log(c^2) = d/n$.

[6] A class of functions $\mathcal{F}$ is called *universal*, if for any distinct $x, y \in \mathcal{X}$, it holds that $\Pr[f(x) = f(y)] \leq 2^{-\ell}$ when picking f uniformly from $\mathcal{F}$. The class is called *strongly universal*, if the random variables $F(x)$ and $F(y)$ are independent and uniform if F is uniform in $\mathcal{F}$.

Protocol Q-ID

(1) U picks $x \in \{0,1\}^n$ at random and sends $H^{\mathfrak{c}(w)}|x\rangle$ to S.
(2) S measures in basis $\mathfrak{c}(w)$. Let x' be the outcome.
(3) U picks $f \in \mathcal{F}$ randomly and independently and sends it to S
(4) S picks $g \in \mathcal{G}$ randomly and independently and sends it to U
(5) U computes and sends $z := f(x) \oplus g(w)$ to S
(6) S accepts if and only if $z = z'$ where $z' := f(x') \oplus g(w)$

It is easy to see that Q-ID perfectly satisfies correctness. It is unconditionally secure against an arbitrary dishonest user U^*.

Theorem 11. Q-ID *is ε-secure for the server with $\varepsilon = \binom{m}{2} 2^{-\ell}$.*

The proof of this claim can be found in the full version [2]. In the BQSM, we achieve the following security for the user.

Theorem 12. *Let S^* be a dishonest server whose quantum memory is at most q qubits at Step (3) of* Q-ID*. Then, for any $0 < \kappa < \delta/4$,* Q-ID *is ε-secure for the user with*

$$\varepsilon = 2^{-\frac{1}{2}((\delta/2-2\kappa)n-1-q-\ell)} + 4 \cdot 2^{-\kappa n}.$$

The proof follows quite easily from our new uncertainty relation and vitally relies on its all-but-one feature. We show the first (and most important) part of the proof below, the rest of the proof can be found in Appendix A.5. To prove Theorem 12 we will use the following lemma.

Lemma 13. *For any density matrix ρ on $\mathcal{H}_{XYE}$ with classical X and Y and E consisting of q qubits, it holds that*

$$H_{\min}(X|YE) \geq H_{\min}(X|Y) - q.$$

The proof of this lemma can be found in the full version [2].

Proof (of Theorem 12). We consider and analyze a purified version of Q-ID where in step (1) instead of sending $|X\rangle_c$ to S^* for a uniformly distributed X, U prepares a fully entangled state $2^{-n/2} \sum_x |x\rangle|x\rangle$ and sends the second register to S^* while keeping the first. Then, in step (3) when the memory bound has applied, U measures his register in the basis $\mathfrak{c}(W)$ in order to obtain X. Note that this procedure produces exactly the same common state as in the original (non-purified) version of Q-ID. Thus, we may just as well analyze this purified version.

The state of S^* consists of his initial state and his part of the EPR pairs, and may include an additional ancilla register. Before the memory bound applies, S^* may perform any unitary transformation on his composite system. When the memory bound is applied (just before step (3) is executed in Q-ID), S^* has to measure all but q qubits of his system. Let the classical outcome of this measurement be denoted by y, and let E' be the remaining quantum state of at most q qubits. The common state has collapsed to a $(n+q)$-qubit state and

depends on y; the analysis below holds for any y. Next, U measures his n-qubit part of the common state in basis $\mathfrak{c}(W)$; let X denote the classical outcome of this measurement. By our new uncertainty relation (Theorem 7) and subsequently applying the min-entropy chain rule that is given in Lemma 13 (to take the q stored qubits into account) it follows that there exists W', independent of W, and an event Ω that occurs at least with probability $1 - 2 \cdot 2^{-\kappa n}$, such that

$$H_{\min}(X|E', W = w, W' = w', \Omega) \geq (\delta/2 - 2\kappa)n - 1 - q.$$

for any w, w' such that $w \neq w'$.

It remains to show via privacy amplification that this bound implies the claim, this is done in Appendix A.5.

Before stating our user-security result in the single-qubit-operations model (SQOM), we briefly introduce this model; the motivations behind the model and its full description are given in [2]. A dishonest server S^* in the SQOM may reliably store the n-qubit state $|x\rangle_{\mathfrak{c}(w)} = |x_1\rangle_{\mathfrak{c}(w)_1} \otimes \cdots \otimes |x_n\rangle_{\mathfrak{c}(w)_n}$ received in Step (1) of `Q-ID`. At the end of the scheme, in Step (5), it may choose an arbitrary sequence $\theta = (\theta_1, \ldots, \theta_n)$, where each θ_i describes an arbitrary orthonormal basis of $\mathbb{C}^2$, and measure each qubit $|x_i\rangle_{\mathfrak{c}(w)_i}$ in basis θ_i to observe $y_i \in \{0, 1\}$. The choice of θ may depend on all the classical information gathered during the execution of the scheme, but we assume here a *non-adaptive* setting where θ_i does not depend on y_j for $i \neq j$, i.e., S^* has to choose all of θ before performing any measurement. Under these restrictions, we achieve the following security result.

Theorem 14. *Let S^* be a dishonest server with unbounded quantum storage that is restricted to single-qubit operations, as specified above. Then, for any $0 < \beta < \frac{1}{4}$, `Q-ID` is ε-secure for the user with*

$$\varepsilon \leq \tfrac{1}{2} 2^{\frac{1}{2}\ell - \frac{1}{4}(\frac{1}{4} - \beta)d} + \tbinom{m}{2} 2^{2\ell} \exp(-2d\beta^2)$$

The proof is quite involved. Since the dishonest server can store all the qubits and then decide in the end how to measure them, depending on all the information obtained during the scheme, standard tools like privacy amplification are not applicable. The proof, which relies on a certain minimum-distance property of random binary matrices and makes use of Diaconis and Shahshahani's XOR inequality [5], can be found in the full version [2].

Acknowledgments. NJB is supported by an NWO Open Competition grant. CGG is supported by Spanish Grants I-MATH, MTM2008-01366, QUITEMAD and QUEVADIS. CS is supported by an NWO VENI grant.

References

1. Bhatia, R.: Matrix Analysis. Springer, New York (1997)
2. Bouman, N.J., Fehr, S., González-Guillén, C., Schaffner, C.: An all-but-one entropic uncertainty relation, and application to password-based identification (2011), full version `http://arxiv.org/abs/1105.6212`

3. Damgård, I., Fehr, S., Salvail, L., Schaffner, C.: Cryptography in the bounded quantum-storage model. In: 46th Ann. IEEE FOCS, pp. 449–458 (2005); also in SIAM Journal on Computing 37(6),1865–1890 (2008)
4. Damgård, I.B., Fehr, S., Salvail, L., Schaffner, C.: Secure Identification and QKD in the Bounded-Quantum-Storage Model. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 342–359. Springer, Heidelberg (2007)
5. Diaconis, P.: Group Representations in Probability and Statistics. Lecture Notes — Monograph series, vol. 11. Inst. of Math. Stat., Hayward (1988)
6. Kittaneh, F.: Norm inequalities for certain operator sums. Journal of Functional Analysis 143(2), 337–348 (1997)
7. König, R., Renner, R., Schaffner, C.: The operational meaning of min-and max-entropy. IEEE Tran. Inf. Th. 55(9), 4337–4347 (2009)
8. Maassen, H., Uffink, J.B.M.: Generalized entropic uncertainty relations. Phys. Rev. Lett. 60(12), 3 (1988)
9. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information, 1st edn. Cambridge University Press (2000)
10. Renner, R.: Security of Quantum Key Distribution. PhD thesis, ETH Zürich (Switzerland) (September 2005), `http://arxiv.org/abs/quant-ph/0512258`
11. Renner, R., König, R.: Universally Composable Privacy Amplification Against Quantum Adversaries. In: Kilian, J. (ed.) TCC 2005. LNCS, vol. 3378, pp. 407–425. Springer, Heidelberg (2005)
12. Schaffner, C.: Cryptography in the Bounded-Quantum-Storage Model. PhD thesis, University of Aarhus (Denmark) (September 2007)
13. Wehner, S., Winter, A.: Entropic uncertainty relations—a survey. New J. of Phys. 12(2) (2010)

A Proofs

A.1 A Useful Norm Inequality (Proposition 16)

Before stating the inequality, we recall some basic properties of the operator norm $\|A\| := \sup \|A|\psi\rangle\|$, where the supremum is over all norm-1 vectors $|\psi\rangle \in \mathcal{H}$. First of all, it is easy to see that

$$\left\| \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \right\| = \max\{\|A\|, \|B\|\}.$$

Also, from the fact that $\|A\| = \sup |\langle\psi|A|\varphi\rangle|$, where the supremum is over all norm-1 $|\psi\rangle, |\varphi\rangle \in \mathcal{H}$, it follows that $\|A^*\| = \|A\|$, where A^* is the Hermitian transpose of A, and thus that for Hermitian matrices A and B:

$$\|AB\| = \|(AB)^*\| = \|B^*A^*\| = \|BA\|.$$

Furthermore, if A is Hermitian then $\|A\| = \lambda_{\max}(A) := \max\{|\lambda_j| : \lambda_j \text{ an eigenvalue of } A\}$. Finally, the operator norm is *unitarily invariant*, i.e., $\|A\| = \|UAV\|$ for all A and for all unitary U, V.

Lemma 15. *Any two $n \times n$ matrices X and Y for which the products XY and YX are Hermitian satisfy*

$$\|XY\| = \|YX\|$$

Proof. For any two $n \times n$ matrices X and Y, XY and YX have the same eigenvalues, see e.g. [1, Exercise I.3.7]. Therefore, $\|XY\| = \lambda_{\max}(XY) = \lambda_{\max}(YX) = \|YX\|$.

We are now ready to state and prove the norm inequality. We recall that an orthogonal projector P satisfies $P^2 = P$ and $P^* = P$.

Proposition 16. *For orthogonal projectors $A_1, A_2, \ldots, A_m$, it holds that*

$$\big\|A_1 + \ldots + A_m\big\| \leq 1 + (m-1) \cdot \max_{1 \leq j < k \leq m} \big\|A_j A_k\big\|.$$

The case $m = 2$ was proven in [3], adapting a technique by Kittaneh [6]. We extend the proof to an arbitrary m.

Proof. Defining

$$X := \begin{pmatrix} A_1 & A_2 & \cdots & A_m \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \quad \text{and} \quad Y := \begin{pmatrix} A_1 & 0 & \cdots & 0 \\ A_2 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ A_m & 0 & \cdots & 0 \end{pmatrix}$$

yields

$$XY = \begin{pmatrix} S & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, \quad \text{and} \quad YX = \begin{pmatrix} A_1 & A_1A_2 & \cdots & A_1A_m \\ A_2A_1 & A_2 & \cdots & A_2A_m \\ \vdots & \vdots & \ddots & \vdots \\ A_mA_1 & A_mA_2 & \cdots & A_m \end{pmatrix}$$

where $S := A_1 + A_2 + \ldots + A_m$. The matrix YX can be additively decomposed into m matrices according to the following pattern

$$YX = \begin{pmatrix} * & & & \\ & * & & \\ & & \ddots & \\ & & & * \\ & & & * \end{pmatrix} + \begin{pmatrix} 0 & * & & \\ & 0 & & \\ & & \ddots & \ddots \\ & & & 0 & * \\ * & & & & 0 \end{pmatrix} + \ \ldots \ + \begin{pmatrix} 0 & & & * \\ * & 0 & & \\ & \ddots & \ddots & \\ & & & 0 \\ & & & * & 0 \end{pmatrix}$$

where the $*$ stand for entries of YX and for $i = 1, \ldots, m$ the ith star-pattern after the diagonal pattern is obtained by i cyclic shifts of the columns of the diagonal pattern.

XY and YX are Hermitian and thus we can apply Lemma 15. Then, by applying the triangle inequality, the unitary invariance of the operator norm and the facts that for all $j \neq k : \|A_j\| = 1$, $\|A_jA_k\| = \|A_kA_j\|$, we obtain the desired statement.

A.2 Proof of Theorem 5

For $j \in [m]$, we define the orthogonal projectors $A^j := \sum_{x \in \mathcal{L}^j} |x\rangle_j\langle x|_j$. Using the spectral decomposition of $\rho = \sum_w \lambda_w |\varphi_w\rangle\langle\varphi_w|$ and the linearity of the trace, we have

$$\begin{aligned}\sum_{j\in[m]} Q^j(\mathcal{L}^j) &= \sum_{j\in[m]} \mathrm{tr}(A^j\rho) = \sum_{j\in[m]}\sum_w \lambda_w \mathrm{tr}(A^j|\varphi_w\rangle\langle\varphi_w|) \\ &= \sum_w \lambda_w \Big(\sum_{j\in[m]} \langle\varphi_w|A^j|\varphi_w\rangle\Big) = \sum_w \lambda_w \langle\varphi_w|\Big(\sum_{j\in[m]} A^j\Big)|\varphi_w\rangle \\ &\leq \Big\|\sum_{j\in[m]} A^j\Big\| \leq 1 + (m-1)\cdot \max_{j\neq k\in[m]} \big\|A^jA^k\big\|,\end{aligned}$$

where the last inequality is the norm inequality (Proposition 16 in Appendix A.1). To conclude, we show that $\|A^jA^k\| \leq c\sqrt{|\mathcal{L}^j||\mathcal{L}^k|}$. Let us fix $j \neq k \in [m]$. Note that by the restriction on the overlap of the family of bases $\{\mathcal{B}_j\}_{j\in[m]}$, we have that $|\langle x|_j|y\rangle_k| \leq c$ holds for all $x, y \in \{0,1\}^n$. Then, with the sums over x and y understood as over $x \in \mathcal{L}^j$ and $y \in \mathcal{L}^k$, respectively,

$$\begin{aligned}\Big\|A^jA^k|\psi\rangle\Big\|^2 &= \Big\|\sum_x |x\rangle_j\langle x|_j \sum_y |y\rangle_k\langle y|_k|\psi\rangle\Big\|^2 \\ &= \Big\|\sum_x |x\rangle_j \sum_y \langle x|_j|y\rangle_k \langle y|_k|\psi\rangle\Big\|^2 = \sum_x \Big|\sum_y \langle x|_j|y\rangle_k \langle y|_k|\psi\rangle\Big|^2 \\ &\leq \sum_x \Big(\sum_y \big|\langle x|_j|y\rangle_k \langle y|_k|\psi\rangle\big|\Big)^2 \leq c^2 \sum_x \Big(\sum_y \big|\langle y|_k|\psi\rangle\big|\Big)^2 \leq c^2\big|\mathcal{L}^j\big|\big|\mathcal{L}^k\big|.\end{aligned}$$

The third equality follows from Pythagoras, the first inequality holds by triangle inequality, the second inequality by the bound on $|\langle x|_j|y\rangle_k|$, and the last follows from Cauchy-Schwarz. This implies $\|A^jA^k\| \leq c\sqrt{|\mathcal{L}^j||\mathcal{L}^k|}$ and finishes the proof. □

A.3 Proof of Corollary 6

For $j \in [m]$ define

$$\mathcal{S}^j := \big\{x \in \{0,1\}^n : Q^j(x) \leq 2^{-(\delta/2-\epsilon)n}\big\}$$

to be the sets of strings with small probabilities and denote by $\mathcal{L}^j := \overline{\mathcal{S}}^j$ their complements[7]. Note that for all $x \in \mathcal{L}^j$, we have that $Q^j(x) > 2^{-(\delta/2-\epsilon)n}$ and therefore $|\mathcal{L}^j| < 2^{(\delta/2-\epsilon)n}$. It follows from Theorem 5 that

$$\begin{aligned}\sum_{j\in[m]} Q^j(\mathcal{S}^j) &= \sum_{j\in[m]} (1 - Q^j(\mathcal{L}^j)) \geq m - (1 + (m-1)\cdot 2^{-\epsilon n}) \\ &= (m-1) - (m-1)2^{-\epsilon n}.\end{aligned}$$

[7] Here's the mnemonic: $\mathcal{S}$ for the strings with *S*mall probabilities, $\mathcal{L}$ for *L*arge.

We define $\mathcal{E} := \{X \in \mathcal{S}^J \wedge Q^J(\mathcal{S}^J) \geq 2^{-\epsilon n}\}$ to be the event that $X \in \mathcal{S}^J$ and at the same time the probability that this happens is not too small. Then $\Pr[\mathcal{E}|J=j] = \Pr[X \in \mathcal{S}^j \wedge Q^j(\mathcal{S}^j) \geq 2^{-\epsilon n}|J=j]$ either vanishes (if $Q^j(\mathcal{S}^j) < 2^{-\epsilon n}$) or else equals $Q^j(\mathcal{S}^j)$. In either case, $\Pr[\mathcal{E}|J=j] \geq Q^j(\mathcal{S}^j) - 2^{-\epsilon n}$ holds and thus the first claim follows by summing over $j \in [m]$ and using the derivation above. Furthermore, let $p = \max_j P_J(j)$, then

$$\begin{aligned}\Pr[\bar{\mathcal{E}}] &= \sum_{j\in[m]} P_J(j)\Pr[\bar{\mathcal{E}}|J=j] \leq p \sum_{j\in[m]} \Pr[\bar{\mathcal{E}}|J=j] \\ &\leq p(m - (\sum_{j\in[m]} Q^j(\mathcal{S}^j) - 2^{-\epsilon n})) \leq p(1 + (2m-1)\cdot 2^{-\epsilon n}),\end{aligned}$$

and $\Pr[\mathcal{E}] \geq (1-p) - p(2m-1)\cdot 2^{-\epsilon n}$

Regarding the second claim, in case $J = j$, we have

$$\begin{aligned}H_{\min}(X|J=j,\mathcal{E}) &= -\log\left(\max_{x\in\mathcal{S}^j} \frac{Q^j(x)}{Q^j(\mathcal{S}^j)}\right) \geq -\log\left(\frac{2^{-(\delta/2-\epsilon)n}}{Q^j(\mathcal{S}^j)}\right) \\ &= (\delta/2-\epsilon)n + \log(Q^j(\mathcal{S}^j)).\end{aligned}$$

As $Q^j(\mathcal{S}^j) \geq 2^{-\epsilon n}$ by definition of $\mathcal{E}$, we have

$$H_{\min}(X|J=j,\mathcal{E}) \geq (\delta/2 - 2\epsilon)n.$$

□

A.4 Remainder of the Proof of Theorem 7

What remains to prove are the cases where $\alpha \neq 0$. We start with the case $\alpha > 0$. The idea is to "inflate" the event $\mathcal{E}$ so that α becomes 0, i.e., to define an event $\mathcal{E}'$ that contains $\mathcal{E}$ (meaning that $\mathcal{E} \implies \mathcal{E}'$) so that $\sum_{j\in[m]} \Pr[\mathcal{E}'|J=j] = m-1$, and to define J' as in the case $\alpha = 0$ (but now using $\mathcal{E}'$). Formally, we define $\mathcal{E}'$ as the disjoint union $\mathcal{E}' = \mathcal{E} \vee \mathcal{E}_\circ$ of $\mathcal{E}$ and an event $\mathcal{E}_\circ$. The event $\mathcal{E}_\circ$ is defined by means of $\Pr[\mathcal{E}_\circ|\mathcal{E}, J=j, X=x] = 0$, so that $\mathcal{E}$ and $\mathcal{E}_\circ$ are indeed disjoint, and $\Pr[\mathcal{E}_\circ|J=j, X=x] = \alpha/m$, so that indeed

$$\begin{aligned}\sum_{j\in[m]} \Pr[\mathcal{E}'|J=j] &= \sum_{j\in[m]} (\Pr[\mathcal{E}|J=j] + \Pr[\mathcal{E}_\circ|J=j]) \\ &= (m-1-\alpha) + \alpha = m-1\,.\end{aligned}$$

We can now apply the analysis of the case $\alpha = 0$ to conclude the existence of J', independent of J, such that $J \neq J' \iff \mathcal{E}'$ and thus $(J \neq J') \wedge \bar{\mathcal{E}}_\circ \iff \mathcal{E}' \wedge \bar{\mathcal{E}}_\circ \iff \mathcal{E}$. Setting $\Omega := \bar{\mathcal{E}}_\circ$, it follows that

$$H_{\min}(X|J=j, J\neq J', \Omega) = H_{\min}(X|J=j,\mathcal{E}) \geq (\delta/2 - 2\epsilon)n\,,$$

where $\Pr[\Omega] = 1 - \Pr[\mathcal{E}_\circ] = 1 - \alpha/m \geq 1 - (2m-1)2^{-\epsilon n}/m \geq 1 - 2\cdot 2^{-\epsilon n}$. Finally, using similar reasoning as in the case $\alpha = 0$, it follows that the same

bound holds for $H_{\min}(X|J=j,J'=j',\Omega)$ whenever $j \neq j'$. This concludes the case $\alpha > 0$.

Finally, we consider the case $\alpha < 0$. The approach is the same as above, but now $\mathcal{E}'$ is obtained by "deflating" $\mathcal{E}$. Specifically, we define $\mathcal{E}'$ by means of $\Pr[\mathcal{E}'|\bar{\mathcal{E}}, J=j, X=x] = \Pr[\mathcal{E}'|\bar{\mathcal{E}}] = 0$, so that $\mathcal{E}'$ is contained in $\mathcal{E}$, and $\Pr[\mathcal{E}'|\mathcal{E}, J=j, X=x] = \Pr[\mathcal{E}'|\mathcal{E}] = \frac{m-1}{m-1-\alpha}$, so that

$$\sum_{j\in[m]} \Pr[\mathcal{E}'|J=j] = \sum_{j\in[m]} \Pr[\mathcal{E}'|\mathcal{E}] \cdot \Pr[\mathcal{E}|J=j] = m-1\,.$$

Again, from the $\alpha = 0$ case we obtain J', independent of J, such that the event $J \neq J'$ is equivalent to the event $\mathcal{E}'$.

It follows that

$$\begin{aligned} H_{\min}(X|J=j, J\neq J') &= H_{\min}(X|J=j,\mathcal{E}') = H_{\min}(X|J=j,\mathcal{E}',\mathcal{E}) \\ &\geq H_{\min}(X|J=j,\mathcal{E}) - \log(P[\mathcal{E}'|\mathcal{E},J=j]) \geq (\delta/2-2\epsilon)n-1\,, \end{aligned}$$

where the second equality holds because $\mathcal{E}' \implies \mathcal{E}$, the first inequality holds because additionally conditioning on $\mathcal{E}'$ increases the probabilities of X conditioned on $J=j$ and $\mathcal{E}$ by at most a factor $1/P[\mathcal{E}'|\mathcal{E},J=j])$, and the last inequality holds by Corollary 6) and because $P[\mathcal{E}'|\mathcal{E},J=j]) = \frac{m-1}{m-1-\alpha} \geq \frac{1}{2}$, where the latter holds since $\alpha \geq -1$. Finally, using similar reasoning as in the previous cases, it follows that the same bound holds for $H_{\min}(X|J=j,J'=j')$ whenever $j \neq j'$. This concludes the proof. □

A.5 Remainder of the Proof of Theorem 12

We will use the following theorem.

Theorem 17 (Privacy amplification, [10,11]). *Let ρ_{XE} be a hybrid state with classical X. Let $g : \mathcal{R}\times\mathcal{X} \to \{0,1\}^\ell$ be a universal hash function, and let R be uniformly distributed over $\mathcal{R}$, independent of X and E. Then $K = g(R,X)$ satisfies*

$$d_{\text{unif}}(K|RE) \leq \frac{1}{2}\cdot 2^{-\frac{1}{2}(H_{\min}(X|E)-\ell)}\,.$$

Because U chooses F independently at random from a 2-universal family, privacy amplification guarantees that

$$\begin{aligned} &d_{\text{unif}}(F(X)|E'F,W=w,W'=w') \\ &\qquad\leq \varepsilon' := \frac{1}{2}\cdot 2^{-\frac{1}{2}((\delta/2-2\kappa)n-1-q-\ell)} + 2\cdot 2^{-\kappa n}, \end{aligned}$$

for any w, w' such that $w \neq w'$. Recall that $Z = F(X)\oplus G(W)$. By security of the one-time pad it follows that

$$d_{\text{unif}}(Z|E'FG,W=w,W'=w') \leq \varepsilon', \tag{1}$$

for any w, w' such that $w \neq w'$. To prove the claim, we need to bound,

$$\begin{aligned}
&\delta(\rho_{WW'E|W\neq W'}, \rho_{W\leftrightarrow W'\leftrightarrow E|W\neq W'}) \\
&\quad = \tfrac{1}{2}\|\rho_{WW'E'FGZ|W\neq W'} - \rho_{W\leftrightarrow W'\leftrightarrow E'FGZ|W\neq W'}\|_1 \\
&\quad \leq \tfrac{1}{2}\|\rho_{WW'E'FGZ|W\neq W'} - \rho_{WW'E'FG|W\neq W'} \otimes 2^{-\ell}\mathbb{I}\|_1 \\
&\qquad + \tfrac{1}{2}\|\rho_{WW'E'FG|W\neq W'} \otimes 2^{-\ell}\mathbb{I} - \rho_{W\leftrightarrow W'\leftrightarrow E'FGZ|W\neq W'}\|_1 \qquad (2)
\end{aligned}$$

where the equality follows by definition of trace distance (Definition 2) and the fact that the output state E is obtained by applying a unitary transformation to the set of registers (E', F, G, W', Z). The inequality is the triangle inequality; in the remainder of the proof, we will show that both terms in (2) are upper bounded by ε'.

$$\begin{aligned}
&\tfrac{1}{2}\|\rho_{WW'E'FGZ|W\neq W'} - \rho_{WW'E'FG|W\neq W'} \otimes 2^{-\ell}\mathbb{I}\|_1 \\
&\quad = \sum_{w\neq w'} P_{WW'|W\neq W'}(w,w')\, d_{\mathrm{unif}}(Z|E'FG, W=w, W'=w') \leq \varepsilon',
\end{aligned}$$

where the latter inequality follows from (1). For the other term, we reason as follows:

$$\begin{aligned}
&\tfrac{1}{2}\|\rho_{WW'E'FG|W\neq W'} \otimes 2^{-\ell}\mathbb{I} - \rho_{W\leftrightarrow W'\leftrightarrow E'FGZ|W\neq W'}\|_1 \\
&\quad = \tfrac{1}{2}\sum_{w\neq w'} P_{WW'|W\neq W'}(w,w')\, \|\rho^{w,w'}_{E'FG|W\neq W'} \otimes 2^{-\ell}\mathbb{I} - \rho^{w'}_{E'FGZ|W\neq W'}\|_1 \\
&\quad = \tfrac{1}{2}\sum_{w\neq w'} P_{WW'|W\neq W'}(w,w')\, \|\rho^{w,w'}_{E'FG|W\neq W'} \otimes 2^{-\ell}\mathbb{I} \\
&\qquad - \sum_{\substack{w'' \\ \text{s.t. } w''\neq w'}} P_{W|W',W\neq W'}(w''|w')\rho^{w'',w'}_{E'FGZ|W\neq W'}\|_1 \\
&\quad = \tfrac{1}{2}\sum_{w'} P_{W'|W\neq W'}(w')\, \|\sum_{\substack{w \\ \text{s.t. } w\neq w'}} P_{W|W',W\neq W'}(w|w')\rho^{w,w'}_{E'FG|W\neq W'} \otimes 2^{-\ell}\mathbb{I} \\
&\qquad - \sum_{\substack{w'' \\ \text{s.t. } w''\neq w'}} P_{W|W',W\neq W'}(w''|w')\rho^{w'',w'}_{E'FGZ|W\neq W'} \sum_{\substack{w \\ \text{s.t. } w\neq w'}} P_{W|W',W\neq W'}(w|w')\|_1 \\
&\quad = \tfrac{1}{2}\sum_{w\neq w'} P_{WW'|W\neq W'}(w,w')\, \|\rho^{w,w'}_{E'FG|W\neq W'} \otimes 2^{-\ell}\mathbb{I} - \rho^{w,w'}_{E'FGZ|W\neq W'}\|_1 \\
&\quad = \sum_{w\neq w'} P_{WW'|W\neq W'}(w,w')\, d_{\mathrm{unif}}(Z|E'FG, W=w, W'=w') \leq \varepsilon',
\end{aligned}$$

where the first equality follows by definition of conditional independence and by a basic property of the trace distance; the third and fourth equality follow by linearity of the trace distance. The inequality on the last line follows from (1). This proves the claim.