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

## (QCRYPT 2011 Abstract)

Niek Bouman*, Serge Fehr*, Carlos González-Guillén[‡§], and Christian Schaffner*[†]
*Centrum Wiskunde & Informatica (CWI), Amsterdam, The Netherlands
[‡]Depto. de Matemática Aplicada, E.T.S. Ingenieros Industriales, Universidad Politécnica de Madrid, Spain
[§]IMI, Universidad Complutense de Madrid, Spain [†]University of Amsterdam (UvA), The Netherlands

### What the Paper is About

*Entropic uncertainty relations* are quantitative characterizations of Heisenberg's uncertainty principle, which make use of an entropy measure to quantify uncertainty. In quantum cryptography, they are often used as vital tools in security proofs.

We propose and prove a new entropic uncertainty relation. It is the first entropic uncertainty relation that lower bounds the *min-entropy* of the measurement outcome with respect to *all but one* measurements, out of a given class of measurements.

To demonstrate its applicability, we propose a new *quantum identification scheme* in the bounded quantum storage model (BQSM). The new uncertainty relation forms the core of the scheme's security proof.

The technical (full) version of this work can be found at `arxiv.org/abs/1105.6212`.

### Novelty

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, rather than the Shannon entropy. Since the min-entropy is a more conservative measure (i.e., never larger than the Shannon entropy), it guarantees a *stronger* type of uncertainty. Furthermore, since min-entropy allows for privacy amplification, such entropic uncertainty relations are useful tools in quantum cryptography.

2. It lower bounds the uncertainty of *all but one* measurement outcome with respect to *arbitrarily large* (but specifically chosen) sets 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 are qubit-wise measurements (in the computational or Hadamard basis), and thus the uncertainty relation applies to a setting 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, in the recent overview article [1], Wehner and Winter declare it an interesting open question whether strong entropic uncertainty relations exist for a small constant number of measurement settings and more than two measurement outcomes. We feel that our new uncertainty relation answers this question in the affirmative by all means.

### Our New Uncertainty Relation 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. We consider the following setting, which is the same for the simpler variant as well as for the actual new uncertainty relation. We let $n$ be an arbitrary positive integer, and we fix an arbitrary set of $n$-bit strings $\mathcal{C} \subset \{0,1\}^n$; any such set shall give us an uncertainty relation. We view $\mathcal{C}$ as a code and consider its *minimal distance* $d$. Any code word $c = (c_1, \ldots, c_n) \in \mathcal{C}$ naturally specifies a measurement on an $n$-qubit state: for any $i \in \{1, \ldots, n\}$, measure the $i$-th qubit in the computational basis if $c_i = 0$ and in the Hadamard basis if $c_i = 1$. Let now $\rho$ be an arbitrary $n$-qubit state, and let $X$ be the measurement outcome when measuring $\rho$ in basis $C$ (as specified above), where $C$ is arbitrarily distributed over $\mathcal{C}$ (but independent of $\rho$). It follows immediately from Maassen and Uffink's uncertainty relation [2] that $H(X|C=c) + H(X|C=\tilde{c}) \geq d$ for any distinct pair $c, \tilde{c} \in \mathcal{C}$, where $H(\cdot|\cdot)$ represents the conditional Shannon entropy. As a direct consequence, there exists a code word/measurement $c' \in \mathcal{C}$ so that $H(X|C=c) \geq \frac{d}{2}$ for all $c \in \mathcal{C}$ with $c \neq c'$. In other words, for any state $\rho$ there exists $c' \in \mathcal{C}$ so that unless the choice for the measurement coincides with $c'$, there is at least $d/2$ bits of entropy in the outcome $X$.

Our new entropic uncertainty relation shows that this very statement essentially still holds when we replace the Shannon entropy by min-entropy, except that $c'$ becomes randomized: for any $\rho$, there exists a *random variable* $C'$, independent of $C$, such that

$$H_{\min}(X|C=c, C'=c') \gtrsim \frac{d}{2} \quad \forall\, c \neq c' \in \mathcal{C}$$

asymptotically for large $n$, no matter what the distribution of $C$ is.[1] Thus, unless the measurement $C$ coincides with $C'$, there is roughly $d/2$ bits of min-entropy in the outcome $X$.

Note that we have no control over (the distribution of) $C'$. We can merely guarantee that it exists and is independent of $C$. It may be insightful to interpret $C'$ as a *virtual guess* for $C$, guessed by the party that contributes $\rho$, and whose goal is to have little uncertainty in the measurement outcome $X$. Then, our uncertainty relation guarantees that there is lots of uncertainty in $X$ (if $d$ is large), unless the guess was correct. This is the best we can hope for (at least qualitatively), because $\rho$ can indeed be prepared based on an actual guess for $C$, where the guess may be arbitrarily distributed (but is independent of $C$), such that there is no uncertainty in $X$ in case the guess was correct. However, it is important to realize, that *no matter* how $\rho$ is prepared — based on an actual guess for $C$ or not — our uncertainty relation holds and there exists such a virtual guess $C'$.

We stress that because the min-entropy is more conservative than the Shannon entropy, our 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 $c, \tilde{c} \in \mathcal{C}$ of distinct code words, there is no strong lower bound on $H_{\min}(X|C=c) + H_{\min}(X|C=\tilde{c})$, in contrast to the case of Shannon entropy. Indeed, $\rho$ might be the uniform mixture of two pure states, one giving no uncertainty when measured in basis $c$, and the other giving no uncertainty when measured in basis $\tilde{c}$, so that $H_{\min}(X|C=c) = H_{\min}(X|C=\tilde{c}) \leq 1$. Because of a similar reason, we cannot hope to get a good bound for all but a *fixed* choice of $c'$; the probabilistic nature of $C'$ is necessary (in general).

Finally, we would like to point out that our uncertainty relation generalizes to an *arbitrary* set of $m$ measurements, not necessarily characterized by a code $\mathcal{C}$, as long as the overlap between any two bases is at most $2^{-d/2}$, i.e., $|\langle\varepsilon|\gamma\rangle| \leq 2^{-d/2}$ for all basis vector pairs $|\varepsilon\rangle, |\gamma\rangle$ coming from different bases.

### Formal Statement and Proof Idea

In order 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.

Throughout this section, $n$ is an arbitrary but fixed positive integer, and $\mathcal{C} \subseteq \{0,1\}^n$ is an arbitrary but fixed (not necessary linear) code with minimal distance $d = \delta n$. For any codeword $c \in \mathcal{C}$, a 0-entry indicates the computational basis and a 1-entry the Hadamard basis, and we write $|x\rangle_c$ for the $n$-qubit state $H^{c_1}|x_1\rangle \otimes \ldots \otimes H^{c_n}|x_n\rangle$, where $H$ denotes the Hadamard matrix.

**Theorem 1.** *Let $\rho$ be an arbitrary state of $n$ qubits. For $c \in \mathcal{C}$, let $Q^c(\cdot)$ be the distribution of the outcome when $\rho$ is measured in the $c$-basis, i.e., $Q^c(x) = \langle x|_c \rho |x\rangle_c$. Then, for any family $\{\mathcal{L}^c\}_{c\in\mathcal{C}}$ of subsets $\mathcal{L}^c \subset \{0,1\}^n$:*

$$\sum_{c\in\mathcal{C}} Q^c(\mathcal{L}^c) \leq 1 + (m-1)\cdot 2^{-\delta n/2} \max_{c\neq c'\in\mathcal{C}} \sqrt{|\mathcal{L}^c||\mathcal{L}^{c'}|}.$$

The proof is along similar lines as the proof in the journal version of [3], which is for the special case of Theorem 1 where $\mathcal{C} = \{0\cdots 0, 1\cdots 1\} \subset \{0,1\}^n$. It is based on the operator norm inequality

$$\left\|A_1 + \ldots + A_m\right\| \leq 1 + (m-1)\cdot \max_{i<j} \left\|A_i A_j\right\|,$$

for arbitrary orthogonal projectors $A_1, \ldots, A_m$.

We can reformulate above uncertainty relation 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 $\mathcal{L}^c$ in Theorem 1 appropriately.

**Corollary 1.** *Let $\rho$ be an arbitrary $n$-qubit state, let $C$ be an arbitrarily distributed random variable over $\mathcal{C}$, and let $X$ be the outcome when measuring $\rho$ in basis $C$.[2] Then, for any $0 < \epsilon < \delta/4$, there exists an event $\mathcal{E}$ such that*

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

*and*

$$H_{\min}(X|C{=}c,\mathcal{E}) \geq \Big(\frac{\delta}{2} - 2\epsilon\Big)n$$

*for $c \in \mathcal{C}$ with $P_{C|\mathcal{E}}(c) > 0$.*

We are now ready to state our new all-but-one entropic uncertainty relation.

**Theorem 2.** *Let $\rho$ be an arbitrary $n$-qubit state, let $C$ be an arbitrarily distributed random variable over $\mathcal{C}$, and let $X$ be the outcome when measuring $\rho$ in basis $C$. Then, for any $0 < \epsilon < \delta/4$, there exists a random variable $C'$ such that (1) $C$ and $C'$ are independent and (2) there exists an event $\Omega$ with $\Pr[\Omega] \geq 1 - 2\cdot 2^{-\epsilon n}$ such that*[3]

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

*for any $c, c' \in \mathcal{C}$ such that $c \neq c'$ and $P_{CC'|\Omega}(c,c') > 0$. Furthermore, the distribution of $C'$ is determined by $\rho$ alone.*

---

[1] A formal version of this statement can be found in Theorem 2.

[2] I.e., $P_{X|C}(x|c) = Q^c(x)$, using the notation from Theorem 1.

[3] Instead of introducing such an event $\Omega$, we could also express the min-entropy bound by means of the *smooth* min-entropy of $X$ given $C = c$ and $C' = c'$.

The idea of the proof of Theorem 2 is to (try to) define the random variable $C'$ in such a way that the event $C \neq C'$ coincides with the "good event" $\mathcal{E}$ from Corollary 1. It then follows immediately from Corollary 1 that $H_{\min}(X|C=c, C' \neq C) \geq (\delta/2 - 2\epsilon)n$, which is already close to the actual min-entropy bound we need to prove. This approach dictates that if the event $\mathcal{E}$ does not occur, then $C'$ needs to *coincide* with $C$. Vice versa, if $\mathcal{E}$ does occur, then $C'$ needs to be *different* to $C$. However, it is a priori unclear *how* to choose $C'$ different to $C$ in case $\mathcal{E}$ occurs. There are many ways to set $C'$ to be different to $C$ (unless $m = 2$). It needs to be done in such a way that without conditioning on $\mathcal{E}$ or its complement, $C$ and $C'$ are independent.

Somewhat surprisingly, it turns out that the following does the job. To simplify this informal discussion, we assume that the sum of the $m$ probabilities $\Pr[\mathcal{E}|C=c]$ from Corollary 1 equals $m-1$ exactly. It then follows that the corresponding complementary probabilities, $\Pr[\bar{\mathcal{E}}|C=c]$ for the $m$ different choices of $c \in \mathcal{C}$, add up to 1 and thus form a probability distribution. $C'$ is now chosen, in the above spirit depending on the event $\mathcal{E}$, so that its marginal distribution $P_{C'}$ coincides with this probability distribution: $P_{C'}(c') = \Pr[\bar{\mathcal{E}}|C=c']$ for all $c' \in \mathcal{C}$. The technical details, and how to massage the argument in case the sum of the $\Pr[\mathcal{E}|C=c]$'s is not exactly $m-1$, are worked out in the full version of the paper.

### A New Quantum Identification Scheme

As an application of our entropic uncertainty relation, we propose 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* $\mathsf{U}$ and a *server* $\mathsf{S}$ that hold a pre-agreed password $w$, the user wants to convince the server that he indeeds 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.

Our new identification scheme, `Q-ID`, is as follows

**Protocol `Q-ID`**

- $\mathsf{U}$ picks $x \in_R \{0,1\}^n$ and sends $|x\rangle_{c(w)}$ to $\mathsf{S}$.
- $\mathsf{S}$ measures in basis $c(w)$. Let $x'$ be the outcome.
- $\mathsf{U}$ picks random $f \in \mathcal{F}$ and sends it to $\mathsf{S}$
- $\mathsf{S}$ picks random $g \in \mathcal{G}$ and sends it to $\mathsf{U}$
- $\mathsf{U}$ computes and sends $z := f(x) \oplus g(w)$ to $\mathsf{S}$
- $\mathsf{S}$ accepts if and only if $z = z'$ where $z' := f(x') \oplus g(w)$

where $\mathcal{F}$ and $\mathcal{G}$ are suitable classes of hash functions, and $c(\cdot)$ is encoding function of a suitable code $\mathcal{C} \subset \{0,1\}^n$.

Our uncertainty relation gives us the right tool to prove security of the new quantum identification scheme `Q-ID` against a dishonest server, in the bounded quantum storage model (BQSM). The latter assumes that the dishonest server has limited quantum storage capabilities. Security against a dishonest user holds unconditionally, i.e., without any restrictions.

The distinguishing feature of our new scheme is that it also offers some security in case the assumption underlying the BQSM fails to hold. Indeed, we additionally prove security of `Q-ID` against a dishonest server that is equipped with the following capabilities. He has unbounded quantum storage and can reliably store all the qubits communicated during the course of the scheme, and he has unbounded classical computation power, but he is restricted to single-qubit operations and measurements (i.e., cannot operate on several qubits coherently). This additional security guarantee is in sharp contrast to the scheme of Damgård *et al.* [4], which completely breaks down against a dishonest server that can store all the communicated qubits untouched and later measure them qubit-wise in one or the other basis. On the downside, `Q-ID` only offers security in case of a perfect quantum source, which emits precisely one qubit when triggered (i.e., there are no multi-photon emissions), hence our scheme is currently mainly of theoretical interest.

It is known (see [4]) that any quantum identification scheme can be broken by a dishonest participant that has both: unbounded quantum storage *and* unbounded quantum computation capabilities. It is thus a desirable goal to have a 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 this goal, in that large quantum storage and *non-trivial* quantum computation capabilities are necessary for a successful attack.

The security proof of our scheme against a quantum-memory-bounded dishonest server follows quite easily by means of our new uncertainty relation. Proving security against a dishonest server that is restricted to single-qubit operations is more 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. Our proof involves certain properties of random linear codes and makes use of Diaconis and Shahshahani's XOR Lemma.


[1] S. Wehner and A. Winter, New J. of Phys. **12** (2010).

[2] H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60** (1988).

[3] I. Damgård, S. Fehr, L. Salvail, and C. Schaffner, in *46th Ann. IEEE FOCS* (2005), pp. 449–458, also in *SIAM Journal on Computing*, 37(6):1865-1890, 2008.

[4] I. Damgård, S. Fehr, L. Salvail, and C. Schaffner, in *CRYPTO '07* (Springer, 2007), vol. 4622 of *LNCS*, pp. 342–359.