Bitwise Quantum Min-Entropy Sampling and New Lower Bounds for Random Access Codes

Jürg Wullschleger(✉)

DIRO, Université de Montréal, Canada McGill University, Montréal, Canada
juerg@wulli.com

Abstract. *Min-entropy sampling* gives a bound on the min-entropy of a randomly chosen subset of a string, given a bound on the min-entropy of the whole string. König and Renner showed a min-entropy sampling theorem that holds relative to quantum knowledge. Their result achieves the optimal rate, but it can only be applied if the bits are sampled in blocks, and only gives weak bounds for the non-smooth min-entropy.
We give two new quantum min-entropy sampling theorems that do not have the above weaknesses. The first theorem shows that the result by König and Renner also applies to bitwise sampling, and the second theorem gives a strong bound for the non-smooth min-entropy. Our results imply a new lower bound for k-out-of-n random access codes: while previous results by Ben-Aroya, Regev, and de Wolf showed that the decoding probability is exponentially small in k if the storage rate is smaller than 0.7, our results imply that this holds for any storage rate strictly smaller than 1, which is optimal.

1 Introduction

Let two players share a long string $x \in \{0,1\}^n$, on which an adversary has only partial knowledge. They would like to get a shared key, over which the adversary has almost no knowledge. Since x is long, using a 2-universal hash function or, more generally, a strong extractor would be inefficient and hence impractical. Vadhan showed in [Vad04] that the two players can instead first randomly sample a relatively small substring $x' \in \{0,1\}^k$ of x, and then apply an extractor to x'. The main part of his proof is a sampling lemma, which shows that with high probability, the string x' will have almost $\frac{t}{n} \cdot k$ bits of min-entropy, if the min-entropy of x is at least t. König and Renner showed in [KR07] that this lemma can be generalized[1] to the setting where the adversary has quantum information about x. Again, with high probability the string x' will have almost $\frac{t}{n} \cdot k$ bits of quantum min-entropy.

Related to these results are lower bounds for *random access codes*. A random access code is an encoding of a message of n classical bits into $m < n$ qubits, such that from these m qubits, k uniformly chosen bits of the message can be guessed with probability at least p. The first lower bound was given for the case

[1] It is however important to note that the results in [KR07] do not converge as fast as in [Vad04]. See also discussion in Sect. 3.

D. Bacon et al. (Eds.): TQC 2011, LNCS 6745, pp. 164–173, 2014.
DOI: 10.1007/978-3-642-54429-3_11, © Springer-Verlag Berlin Heidelberg 2014

where $k = 1$ by Ambainis, Nayak, Ta-Shma and Vazirani in [ANTSV99]. It was later improved by Nayak in [Nay99] to $m \geq (1 - H(p))n$, where $H(\cdot)$ is the binary entropy function. For the general case where $k \geq 1$, a lower bound was presented by Ben-Aroya, Regev, and de Wolf in [BARdW08]. They showed that for any $\eta > 2 \ln 2$ there exists a constant C_η such that

$$p \leq C_\eta \left(\frac{1}{2} + \frac{1}{2} \sqrt{\frac{\eta m}{n}} \right)^k .$$

This implies that if $m \leq 0.7n$, then $p \leq 2^{-\Omega(k)}$. In the same work they also showed lower bounds for a variant of random access codes called *XOR random access codes*, where the decoder has to guess the XOR of a uniform subset of size k. De and Vidick presented in [DV10] lower bounds for *functional access codes.* They are generalizations of XOR random access codes where the decoder has to guess the output of a function with binary output, where the function is chosen uniformly from a given set.

The result in [Vad04] implies a classical lower bound for k-out-of-n random access codes. In principle, this would also be possible in the quantum setting, as the min-entropy is defined as minus the logarithm of the guessing probability. Unfortunately, the results by König and Renner are not general enough to do that, because they require the sampling to be done in blocks.

1.1 Contributions

In this work we give two new results for quantum min-entropy sampling.

First, we show in Theorems 4 and 5 in Sect. 3 that the bounds given in Corollary 6.19 and Lemma 7.2 in [KR07] also apply to the case where the sample is chosen bitwise, instead of (recursively) in blocks. This result simplifies some protocols[2] as it eliminates an artificial extra step in which the bits have to be grouped in blocks.

Second, building on previous results given in [BARdW08] and [DV10], in Sect. 4 we proof the following quantum sampling theorem.

Theorem 1. *Let ρ_{XQ} be a state that is classical on $X \in \{0,1\}^n$. Let T be a uniformly chosen subset of $[n]$ of size k. Then*[3]

$$H_{\min}(X_T \mid TQ)_\rho \geq H^{-1} \left(\frac{H_{\min}(X \mid Q)_\rho}{2n} \right) \frac{k}{6} - 5 .$$

Compared with the results in [KR07] and Theorems 4 and 5, Theorem 1 gives stronger bounds for non-smooth min-entropy, but does not achieve the optimal rate[4]. Also note that Theorem 1 only applies to the case where the sample is chosen uniformly, which requires a lot of randomness.

[2] For example in [KWW09].

[3] $H_{\min}$ is defined in Sect. 2.

[4] Therefore, if we are interested in extracting a key, Theorem 1 only gives better bounds if the sample size is small enough.

Theorem 1 immediately implies the following bound for random access codes.

Corollary 1. *Let $0 < \varepsilon < \frac{1}{2}$. For any k-out-of-n random access code where the code length is bounded by $m \leq (1 - 2H(\varepsilon))n$, the success probability of decoding is at most $2^{-\varepsilon k/6+5}$.*

As the results in [BARdW08], Corollary 1 generalizes the bound given by Nayak to the case where $k \geq 1$. But while the results in [BARdW08] require that $m < 0.7n$, our results imply that the success probability decreases exponentially in k even if m is close to n.

Note that together with Lemma 8 in [BARdW08], Corollary 1 implies a strong lower bound for the one-way communication complexity of k independent instances of the disjointness problem.

2 Preliminaries

The *binary entropy function* is defined as $H(x) := -x \log x - (1-x) \log(1-x)$ for $x \in [0,1]$, where we use the convention $0 \log 0 = 0$. For $y \in [0,1]$, let $H^{-1}(y)$ be the value $x \in [0, \frac{1}{2}]$ such that $H(x) = y$. The *Hamming distance* $d_H(\cdot,\cdot)$ between two strings is defined as the number of bits where the two strings disagree. We use the notion $[n] := \{1, \ldots, n\}$. The substring of $x \in \{0,1\}^n$ defined by the set $s \subset [n]$ is denoted by x_s. We call a state ρ_{XQ} a *cq-state* if it is classical on X, which means that it has the form $\rho_{XQ} = \sum_x p_x |x\rangle\langle x| \otimes \rho_Q^x$.

The *conditional min-entropy* of a cq-state ρ_{XQ} is defined as

$$H_{\min}(X \mid Q)_\rho := -\log P_{\text{guess}}(X \mid Q)_\rho \ ,$$

where

$$P_{\text{guess}}(X \mid Q)_\rho := \max_{\mathcal{E}} \sum_{x \in \mathcal{X}} P_X(x) \operatorname{tr}(E_x \rho_Q^x) \ .$$

The maximum is taken over all POVMs $\mathcal{E} = \{E_x\}_{x \in \mathcal{X}}$ on $\mathcal{Q}$. Therefore, $P_{\text{guess}}(X \mid Q)_\rho$ is the maximal probability to correctly guess X by measuring system Q. The equivalence of this definition of $H_{\min}$ with the definition used in [KR07] has been shown in [KRS09] in Theorem 1.

The *statistical distance* $D(\rho, \phi)$ between two states ρ and ϕ is defined as[5]

$$D(\rho, \phi) := \max_{\mathcal{E}} \ |\operatorname{tr}(E_1 \rho) - \operatorname{tr}(E_1 \phi)| \ ,$$

where we maximize over all POVMs $\mathcal{E} = \{E_x\}_{x \in \{0,1\}}$. $D(\rho, \phi)$ is therefore the maximal probability to distinguish ρ and ϕ by a measurement. The following lemma shows the connection between the statistical distance and the guessing probability.

Lemma 1. *Let ρ_{XQ} be a cq-state where $X \in \{0,1\}$ and let τ_X be the fully mixed state. Then $D(\rho_{XQ}, \tau_X \otimes \rho_Q) \leq \varepsilon$ implies that $P_{\text{guess}}(X \mid Q)_\rho \leq \frac{1}{2} + \varepsilon$.*

[5] This definition is equivalent to $D(\rho, \phi) := \frac{1}{2}\|\rho - \phi\|_1 = \frac{1}{2} \operatorname{tr}[\sqrt{(\rho - \phi)^\dagger (\rho - \phi)}]$.

Proof. Let us assume that there exists a POVM $\mathcal{E}$ on $\mathcal{Q}$ which can guess X with a probability bigger than $\frac{1}{2}+\varepsilon$. We define a POVM $\mathcal{E}'$ on $\mathcal{X}\otimes\mathcal{Q}$ in the following way: we measure Q using $\mathcal{E}$ and XOR the output with X. We get $\mathrm{tr}(E'_1\rho_{XE}) < \frac{1}{2}-\varepsilon$ and $\mathrm{tr}(E'_1(\tau_X\otimes\rho_Q)) = \frac{1}{2}$. It follows that $D(\rho_{XQ},\tau_X\otimes\rho_Q) > \varepsilon$, which contradicts the assumption. □

Lemma 2. (Chernoff/Hoeffding). *Let $P_{X_0\ldots X_n} = P_X^n$ be a product distribution with $X_i \in [0,1]$. Let $X := \frac{1}{n}\sum_{i=0}^{n-1} X_i$, and $\mu = E[X]$. Then, for any $\varepsilon > 0$, $\Pr\left[X \leq \mu - \varepsilon\right] \leq e^{-2n\varepsilon^2}$.*

3 Bitwise Sampling from Blockwise Sampling

In this section we show that the min-entropy sampling results from [KR07], which require blockwise sampling, also imply the same bounds for uniform bitwise sampling.

The following theorem is the statement of Corollary 6.19 in [KR07] for uniform blockwise sampling. Here $H_{\min}^{\varepsilon}$ is the *smooth min-entropy*, and H_0 the *Rényi 0-entropy*. The definitions of these entropies and their properties can be found in Sect. 5 in [KR07] or Chap. 3 in [Ren05].

Theorem 2 ([KR07]). *Let ρ_{XQ} be a cq-state where $X = (X_1,\ldots,X_n) \in \mathcal{X}^n$. Let $S \subset [n]$ be chosen uniformly at random among all subsets of size r. Assume that $\kappa = \frac{n}{r\log|\mathcal{X}|} \leq 0.15$. Then for any $\xi \in [0,1]$,*

$$\frac{H_{\min}^{\varepsilon}(X_S \mid SQ)}{H_0(X_{\mathcal{S}})} \geq \frac{H_{\min}(X \mid Q)}{H_0(X)} - 3\xi - 2\kappa\log 1/\kappa\ ,$$

where $\varepsilon = 2\cdot 2^{-\xi n\log|\mathcal{X}|} + 3e^{-r\xi^2/8}$.

The statement says that with high probability, the min-entropy rate of a random subset is almost as big as the min-entropy rate of the whole string.

If X is a bit-string, the required condition $n \leq 0.15\cdot r\log|\mathcal{X}|$ can be achieved by first grouping the bits into blocks. But as pointed out in [BARdW08], even then we need the length of the sampled bit-string to be at least $\Omega(\sqrt{n})$. To overcome this problem, [KR07] proposed a *recursive* application of Theorem 2. The following theorem is Lemma 7.2 in [KR07]. See Section 7 in [KR07] for the definition of the sampling algorithm $\mathrm{ReSamp}(X,f,r,S)$.

Theorem 3 ([KR07]). *Let ρ_{XQ} be a cq-state where $X \in \{0,1\}^n$. Let n, f and r be such that $n^{(3/4)^f} \geq r^4$. Let S be a string of uniform random bits, and let $Z = \mathrm{ReSamp}(X,f,r,S)$. Then Z is a $n^{(3/4)^f}$-bit substring of X, with*

$$\frac{H_{\min}^{\varepsilon}(Z \mid SQ)}{H_0(Z)} \geq \frac{H_{\min}(X \mid Q)}{H_0(X)} - 5f\frac{\log r}{r^{1/4}}\ ,$$

where $\varepsilon = 5f\cdot 2^{-\sqrt{r}/8}$.

Our results from this section, Theorems 4 and 5, will follow directly from the following lemma.

Lemma 3. *The bounds of Theorems 2 and 3 also apply if the sample is chosen bitwise uniformly.*

Proof. Let $k, n \in \mathbb{N}$, were $k < n$. Let ρ_{XQ} be a cq-state where $X \in \{0,1\}^n$. Let $S \subset [n]$ be chosen uniformly at random from all subset of size k and let $T \subset [n]$ be a random subset of size k chosen according to a given distribution P_T. Let $\mathit{\Pi}$ a permutation chosen uniformly at random, but such that it maps all elements in S into T. Strong subadditivity (Theorem 3.2.12 in [Ren05]) implies

$$\begin{aligned} H^{\varepsilon}_{\min}(X_S \mid SQ) &\geq H^{\varepsilon}_{\min}(X_S \mid S\mathit{\Pi}Q) \\ &= H^{\varepsilon}_{\min}(\mathit{\Pi}(X)_T \mid T\mathit{\Pi}Q) \ . \end{aligned}$$

Note that from $(S, \mathit{\Pi})$ it is possible to calculate $(T, \mathit{\Pi})$, and vice-versa. Furthermore, since $\mathit{\Pi}$ is chosen independent of ρ_{XQ}, we have

$$H^{\varepsilon}_{\min}(\mathit{\Pi}(X) \mid \mathit{\Pi}Q) = H^{\varepsilon}_{\min}(X \mid \mathit{\Pi}Q) = H^{\varepsilon}_{\min}(X \mid Q) \ .$$

Since S was chosen uniformly and independent of T and ρ_{XQ}, $\mathit{\Pi}$ is independent of T and ρ_{XQ}. For $Q' := (Q, \mathit{\Pi})$, we can apply Theorem 2 or 3 to the state $\rho_{\mathit{\Pi}(X)Q'}$. We now choose P_T as the particular sampling required by the theorem and get a bound on $H^{\varepsilon}_{\min}(\mathit{\Pi}(X)_T \mid T\mathit{\Pi}Q)$, which then directly implies the same bound for $H^{\varepsilon}_{\min}(X_S \mid SQ)$. □

Theorem 4. *Let $b, r \in \mathbb{N}$. Let ρ_{XQ} be a cq-state where $X \in \{0,1\}^n$. Let $S \subset [n]$ be chosen uniformly among all subsets of size $k = rb$. Assume that $\kappa = \frac{n}{kb} \leq 0.15$. Then for any constant $\xi \in [0,1]$,*

$$\frac{H^{\varepsilon}_{\min}(X_S \mid SQ)}{H_0(X_S)} \geq \frac{H_{\min}(X \mid Q)}{H_0(X)} - 3\xi - 2\kappa \log 1/\kappa \ ,$$

where $\varepsilon = 2 \cdot 2^{-\xi n} + 3e^{-k\xi^2/(8b)}$.

Note that even though we sample bitwise in Theorem 4, the block-size parameter b is still present. It can be chosen depending on the required result: a bigger value b gives a better rate, but results in a slower convergence of the error ε. The best convergence of ε is achieved by choosing $b = \frac{n}{0.15k}$, where we get

$$\varepsilon = 2 \cdot 2^{-\xi n} + 3e^{-k\xi^2/(8b)} = 2 \cdot 2^{-\xi n} + 3e^{-0.15k^2\xi^2/(8n)} \ .$$

Hence, as mentioned before, we need $k = \Omega(\sqrt{n})$.

Theorem 5. *Let n, f and $r \in \mathbb{N}$ be such that $n^{(3/4)^f} \geq r^4$. Let ρ_{XQ} be a cq-state where $X \in \{0,1\}^n$. Let $S \subset [n]$ be chosen uniformly among all subsets of size $k = n^{(3/4)^f}$. Then*

$$\frac{H^{\varepsilon}_{\min}(X_S \mid SQ)}{H_0(X_S)} \geq \frac{H_{\min}(X \mid Q)}{H_0(X)} - 5f\frac{\log r}{r^{1/4}} \ ,$$

where $\varepsilon = 5f \cdot 2^{-\sqrt{r}/8}$.

Theorem 5 can be applied even if $k = o(\sqrt{n})$, but the error converges rather slow: since $k \geq r^4$, we have

$$\varepsilon = 5f \cdot 2^{-\sqrt{r}/8} \geq 5f \cdot 2^{-\sqrt[8]{k}/8} .$$

4 A Sampling Theorem from Quantum Bit Extractors

In this section we give a new min-entropy sampling theorem (Theorem 1) using a completely different approach than [KR07]. Our proof has two steps. First, we show a bound on the guessing probability of the XOR of a randomly chosen substring of X using the same approach as [DV10], which is based on a result by König and Terhal [KT08] on strong bit-extractors against quantum adversaries. Second, we will show that this implies a bound on the guessing probability of a randomly chosen substring of X. To show this we use a result from [BARdW08].

A function $\text{ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ is a (ℓ, ε)-*strong extractor against quantum adversaries*, if for all cq-states ρ_{XQ} with $H_{\min}(X \mid Q)_\rho \geq \ell$ and for a uniform seed R, we have $D(\rho_{\text{ext}(X,R)RQ}, \tau_U \otimes \rho_R \otimes \rho_Q) \leq \varepsilon$, where τ_U is the fully mixed state. A strong *classical* extractor is the same, but with a trivial system Q. If $m = 1$, we call it a *bit-extractor*. König and Terhal showed in [KT08] that any classical bit-extractor is also a quantum bit-extractor.

Theorem 6 (Theorem III.1 in [KT08]). *Any* (ℓ, ε)*-strong bit-extractor is a* $(\ell + \log 1/\varepsilon, 3\sqrt{\varepsilon})$*-strong bit-extractor against quantum adversaries.*

One way to construct a strong bit-extractor is to use a *(*$\varepsilon, \delta,$ *L)-approximately list-decodable code*. This is a code $C : \{0,1\}^n \to \{0,1\}^m$ where for every $c \in \{0,1\}^m$ there exist L strings $x_1, \ldots, x_L \in \{0,1\}^n$, such that for any string $x \in \{0,1\}^n$ satisfying $d_H(c, C(x)) < (\frac{1}{2} - \varepsilon)m$, there exists an $i \in \{1, \ldots, L\}$ such that $d_H(x_i, x) \leq \delta m$. From a code $C : \{0,1\}^n \to \{0,1\}^{2^t}$, we can build a bit-extractor $\text{ext} : \{0,1\}^n \times \{0,1\}^t \to \{0,1\}$ as $\text{ext}(x, y) := C(x)_y$, where $C(x)_y$ is the yth position of the codeword $C(x)$.

Lemma 4 (Claim 3.7 in [DV10]). *Let* $\delta \in [0, \frac{1}{2}]$*. An extractor build from a* (ε, δ, L)*-approximately list-decodable code* $C : \{0,1\}^n \to \{0,1\}^{2^t}$ *is a* (ℓ, ε)*-strong classical bit-extractor for* $\ell > H(\delta)n + \log L + \log 2/\varepsilon$.

The (n, k)-XOR-code over strings of length n is the code where the string x gets encoded into a string of size $\binom{n}{k}$ where each bit is the XOR of a subset of x of size k.

Lemma 5 (Lemma 42 in [IJK06], adapted to Lemma 3.11 in [DV10]). *For* $\varepsilon > 2k^2/2^n$*, the* (n, k)*-XOR-code is a* $(\varepsilon, \frac{1}{k} \ln \frac{2}{\varepsilon}, 4/\varepsilon^2)$*-approximately list-decodable code.*

Combining Lemmas 4 and 5 with Theorem 6, we get the following lemma.

Lemma 6. *Let $\varepsilon > 2k^2/2^n$ and $k \geq 2 \ln \frac{2}{\varepsilon}$. The extractor build from the (n,k)-XOR-code implies a $(\ell, 3\sqrt{\varepsilon})$-strong bit-extractor against quantum adversaries for*

$$\ell > H\Big(\frac{1}{k} \ln \frac{2}{\varepsilon}\Big) n + 4 \log \frac{1}{\varepsilon} + 3 \ .$$

Proof. Using Lemmas 4 and 5, the (n,k)-XOR-code implies a (ℓ, ε)-strong classical bit-extractor for

$$\ell > H\Big(\frac{1}{k} \ln \frac{2}{\varepsilon}\Big) n + \log \frac{4}{\varepsilon^2} + \log \frac{2}{\varepsilon} = H\Big(\frac{1}{k} \ln \frac{2}{\varepsilon}\Big) n + 3 \log \frac{1}{\varepsilon} + 3 \ .$$

The statement follows from Theorem 6. □

From Lemmas 1 and 6 follows that if a string X can only be guessed from Q with probability at most $2^{-\ell}$, i.e., $H_{\min}(X \mid Q) \geq \ell$, then the XOR of a random subset of size k can be guessed with probability at most $1/2 + 3\sqrt{\varepsilon}$. The following lemma gives a bound on the probability to guess a whole substring, given bounds on the probability to guess the XOR of substrings. It has been proven as a part of Theorem 2 in [BARdW08].

Lemma 7 (part of Theorem 2 in [BARdW08]). *Let ρ_{XQ} be a cq-state where $X \in \{0,1\}^n$ and let $p_j > 0$ for $j \in \{0, \ldots, k\}$ be upper bounds on the probability to guess the XOR of a random subset of X of size j given Q and the subset. Then the probability to guess a random subset of X of size k from Q and the subset is at most*

$$\frac{1}{2^k} \sum_{j=0}^{k} \binom{k}{j} (2p_j - 1) \ .$$

We can now use Lemmas 6 and 7 to proof the following sampling lemma.

Lemma 8. *Let a cq-state ρ_{XQ} be given, where $X \in \{0,1\}^n$. Let T be a uniformly chosen subset of $[n]$ of size k. If $\log \frac{1}{p} \leq k/12 - 5$ and*

$$H_{\min}(X \mid Q)_\rho \geq H\left(\frac{6}{k} \log \frac{17}{p}\right) n + 8 \log \frac{12}{p} + 3 \ ,$$

then $H_{\min}(X_T \mid TQ)_\rho \geq \log \frac{1}{p}$.

Proof. From $\log \frac{1}{p} \leq k/12 - 5$ follows that

$$k \geq 12 \log \frac{17}{p} \geq 17 \ln \frac{17}{p} \ . \tag{1}$$

Since $k \leq n$ and $5k/12 + 5 \geq \log(17k)$, it follows also that

$$\log \frac{1}{p} \leq \frac{k}{12} - 5 = \frac{k}{2} - \frac{5k}{12} - 5 \leq \frac{k}{2} - \log(17k) \leq \frac{n}{2} - \log(17k)$$

and hence $p^2 \geq 288 \cdot k^2/2^n$. For $j \in \{0, \dots, k\}$, let p_j be the guessing probability of the XOR for random subsets of size j. From Lemma 7 follows that

$$\begin{aligned} P_{\text{guess}}(X_T \mid TQ)_\rho &\leq \frac{1}{2^k} \sum_{j=0}^{k} \binom{k}{j} (2p_j - 1) \\ &\leq \frac{1}{2^k} \sum_{j=0}^{k/4} \binom{k}{j} + \max_{j' \in [k/4+1, k]} (2p_{j'} - 1) \cdot \frac{1}{2^k} \sum_{j=k/4+1}^{k} \binom{k}{j} \\ &\leq \frac{1}{2^k} \sum_{j=0}^{k/4} \binom{k}{j} + \max_{j' \in [k/4+1, k]} (2p_{j'} - 1)\ . \end{aligned}$$

We have

$$\sum_{j=0}^{k/4} \frac{1}{2^k} \binom{k}{j} = \Pr\left[J \leq k/4\right] ,$$

where $J = \sum_{i \in [k]} J_i$ and the random variables J_i are independent and uniform on $\{0, 1\}$. From Lemma 2 follows that

$$\Pr[J \leq k/4] \leq \exp(-k/8) \leq p/2\ ,$$

since $k \geq 17 \ln \frac{17}{p} > 8 \ln \frac{2}{p}$. Let $\varepsilon := p^2/144$. From Eq. (1) follows that

$$\frac{1}{2} \geq \frac{6}{k} \log \frac{17}{p} \geq \frac{17}{2k} \ln \frac{17}{p} \geq \frac{4}{k} \ln \frac{288}{p^2} = \frac{4}{k} \ln \frac{2}{\varepsilon} \geq \frac{1}{j'} \ln \frac{2}{\varepsilon}\ ,$$

for any $j' \in [k/4 + 1, k]$. Since $8 \log(12/p) = 4 \log(1/\varepsilon)$, we have

$$H_{\min}(X \mid Q)_\rho \geq H\Big(\frac{1}{j'} \ln \frac{2}{\varepsilon}\Big) n + 4 \log \frac{1}{\varepsilon} + 3\ .$$

From $p^2 \geq 288 \cdot k^2/2^n$ follows that $\varepsilon \geq 2k^2/2^n \geq 2{j'}^2/2^n$. Lemmas 1 and 6 imply that $p_{j'} \leq 1/2 + 3\sqrt{\varepsilon}$, and hence

$$\max_{j' \in [k/4+1, k]} (2p_{j'} - 1) \leq 6\sqrt{\varepsilon} = p/2\ .$$

So $P_{\text{guess}}(X_T \mid TQ)_\rho \leq p$. The statement follows from the definition of $H_{\min}$. □

Proof. (Theorem 1). Let $m := H_{\min}(X \mid Q)_\rho$ and $p := 2^{-H^{-1}(m/2n)k/6+5}$. We have

$$\log \frac{1}{p} = \frac{H^{-1}(m/2n)}{6} k - 5\ ,$$

which implies

$$\frac{m}{2} = H\left(\frac{6}{k} \log \frac{32}{p}\right) n \geq H\left(\frac{6}{k} \log \frac{17}{p}\right) n \tag{2}$$

and, since $H^{-1}(m/2n) \leq \frac{1}{2}$,

$$\log \frac{1}{p} = \frac{H^{-1}(m/2n)}{6} k - 5 \leq \frac{k}{12} - 5 \; . \qquad (3)$$

From $n \geq k$ and $\frac{1}{2} \geq x/2 \geq H^{-1}(x)$ for any $x \in [0,1]$ follows

$$\log \frac{1}{p} = \frac{H^{-1}(m/2n)}{6} k - 5 \leq H^{-1}\left(\frac{m}{2n}\right) \cdot \frac{n}{6} - 5 \leq \frac{m}{4n} \cdot \frac{n}{6} - 5 = \frac{m}{24} - 5 \; ,$$

which implies

$$8 \log \frac{12}{p} + 3 = 8 \log \frac{1}{p} + 8 \log(12) + 3 \leq \frac{m}{3} - 40 + 32 + 3 \leq \frac{m}{2} \; .$$

Together with Eq. (2), we get

$$m \geq H\left(\frac{6}{k} \log \frac{17}{p}\right) n + 8 \log \frac{12}{p} + 3 \; . \qquad (4)$$

The statement follows from Lemma 8 and Eqs. (3) and (4). □

5 Lower Bounds for Random Access Codes

Corollary 1 directly implies a lower bound for k-out-of-n random access codes: if we choose the string $X \in \{0,1\}^n$ uniformly at random and the quantum system Q has at most $m \leq (1 - 2H(\varepsilon))n$ qubits, then by Proposition 2' in [KT08], we have $H_{\min}(X \mid Q) \geq 2H(\varepsilon)n$. Corollary 1 follows.

Note that in the same way Theorems 4 or 5 could be used to give a bound for random access codes, since $H_{\min}^{\varepsilon}(X \mid Q) \geq \ell$ implies $P_{\text{guess}}(X \mid Q) \geq 2^{-\ell} + \varepsilon$. But since the error ε converges slowly, we would only get a weak bound on the guessing probability.

6 Open Problems

Our sampling results only apply to the case where the sample is chosen uniformly. It would be interesting to know if they can be generalized to other sampling strategies.

Acknowledgements. I thank Robert König, Thomas Vidick and Stephanie Wehner for helpful discussions and the anonymous reviewers for useful comments. This work was funded by the U.K. EPSRC grant EP/E04297X/1 and the Canada-France NSERC-ANR project FREQUENCY. Most of this work was done while I was at the University of Bristol.

References

ANTSV99. Ambainis, A., Nayak, A., Ta-Shma, A., Vazirani, U.: Dense quantum coding and a lower bound for 1-way quantum automata. In: Proceedings of the Thirty-first Annual ACM Symposium on Theory of Computing (STOC '99). ACM (1999)

BARdW08. Ben-Aroya, A., Regev, O., de Wolf, R.: A hypercontractive inequality for matrix-valued functions with applications to quantum computing and LDCs. In: Proceedings of the 40th Annual IEEE Symposium on Foundations of Computer Science (FOCS '08) (2008)

DV10. De, A., Vidick, T.: Near-optimal extractors against quantum storage. In: Proceedings of the Fourty-Second Annual ACM Symposium on Theory of Computing (STOC '10). ACM (2010)

IJK06. Impagliazzo, I., Jaiswal, R., Kabanets, V.: Approximately list-decoding direct product codes and uniform hardness amplification. In: Proceedings of the 42th Annual IEEE Symposium on Foundations of Computer Science (FOCS '06), pp. 187–196 (2006)

KR07. König, R., Renner, R.: Sampling of min-entropy relative to quantum knowledge. arXiv:0712.4291 (2007)

KRS09. König, R., Renner, R., Schaffner, C.: The operational meaning of min- and max-entropy. IEEE Trans. Inf. Theory **55**(9), 4337–4347 (2009)

KT08. König, R., Terhal, B.M.: The bounded storage model in the presence of a quantum adversary. IEEE Trans. Inf. Theory **54**(2), 749–762 (2008)

KWW09. König, R., Wehner, S., Wullschleger, J.: Unconditional security from noisy quantum storage. arXiv:0906.1030 (2009)

Nay99. Nayak, A.: Optimal lower bounds for quantum automata and random access codes. In: Proceedings of the 40th Annual IEEE Symposium on Foundations of Computer Science (FOCS '99), pp. 369–376 (1999)

Ren05. Renner, R.: Security of quantum key distribution. Ph.D thesis, ETH Zürich, Switzerland. arXiv:quant-ph/0512258 (2005)

Vad04. Vadhan, S.: Constructing locally computable extractors and cryptosystems in the bounded-storage model. J. Cryptol. **17**, 2004 (2004)