Impossibility of Efficient Information-Theoretic Fuzzy Extraction

Luke Demarest
University of Connecticut
luke.h.demarest@gmail.com

Benjamin Fuller
University of Connecticut
benjamin.fuller@uconn.edu

Alexander Russell
University of Connecticut
acr@uconn.edu

March 3, 2023

Abstract

Fuzzy extractors convert noisy signals from the physical world into reliable cryptographic keys. Fuzzy min-entropy is an important measure the ability of a fuzzy extractor to distill keys from a distribution: in particular, it bounds the length of the key that can be derived (Fuller, Reyzin, and Smith, IEEE Transactions on Information Theory 2020). In general, fuzzy min-entropy that is superlogarithmic in the security parameter is required for a noisy distribution to be suitable for key derivation.

There is a wide gap between what is possible with respect to computational and information-theoretic adversaries. Under the assumption of general-purpose obfuscation, keys can be securely derived from all distributions with superlogarithmic entropy. Against information-theoretic adversaries, however, it is impossible to build a single fuzzy extractor that works for all distributions (Fuller, Reyzin, and Smith, IEEE Transactions on Information Theory 2020).

A weaker information-theoretic goal is to build a fuzzy extractor for each particular probability distribution. This is the approach taken by Woodage et al. (Crypto 2017). Prior approaches use the full description of the probability mass function and are inefficient. We show this is inherent: **for a quarter of distributions with fuzzy min-entropy and 2^k points there is no secure fuzzy extractor that uses less $2^{\Theta(k)}$ bits of information about the distribution.** This result rules out the possibility of efficient, information-theoretic fuzzy extractors for many distributions with fuzzy min-entropy.

We show an analogous result with stronger parameters for information-theoretic secure sketches. Secure sketches are frequently used to construct fuzzy extractors.

1 Introduction

Information reconciliation and privacy amplification are the two fundamental tasks for key derivation from noisy sources. Roughly speaking, information reconciliation takes two correlated distributions w and w' and maps them to the same value while minimizing what is leaked about that value. Privacy amplification converts the uncertainty in this mapped value to a uniform value suitable for cryptography. Applications areas include quantum key agreement, biometrics, and physically uncloneable functions [BBR88, DORS08].

We focus on non-interactive versions of these problems [DORS08] as defined by secure sketches, which perform information-reconciliation, and fuzzy extractors, which perform both information-reconciliation and privacy amplification. A Secure Sketch consists of a pair of algorithms *sketch* or SS where:

1. $\mathsf{SS}(w) = ss$ should reveal as little information as possible about w; and
2. $\mathsf{SS}(w) = ss$ should allow one to reconstruct w from a nearby w'. That is, it should be the case that for all nearby $w', \mathsf{Rec}(w', ss) = w$. In the above, "nearby" is w' such that $\mathsf{dis}(w, w') \leq t$ for distance metric dis and distance t.

These two properties are in tension because allowing recovery of w requires information about w. The most natural (inefficient) construction is for ss to be a pairwise independent [CW77] hash h of w [ST09, FRS16, WCD+17, FRS20]. The hash h should be long enough so that $\{w|h(w) = y \wedge \mathsf{dis}(w, w') \leq t\} = 1$ and short enough so $\{w|h(w) = y\}$ is large. Constructions are also known based on error-correcting codes. In fact, upper bounds on the unpredictability of $w|ss$ are related to the size of the best error-correcting codes [DORS08, FMR20].

Given a good information reconciliation, one can achieve privacy amplification using an average-case randomness extractor [NZ93] to convert w into a uniform value. Fuzzy extractors perform both tasks simultaneously. They consist of a pair $(\mathsf{Gen}, \mathsf{Rep})$ where $(r, p) \leftarrow \mathsf{Gen}(w)$ is indistinguishable from (u, p) and $\mathsf{Rep}(w', p) = r$. Both SS and Gen are allowed to have private internal randomness.

Since noisy sources come from the physical world, an important goal is to be able to support as many distributions W as possible. This goal is the focus of this work. Throughout the Introduction, we use the notation of fuzzy extractors and note when there are material differences for secure sketches. Fuller, Reyzin, and Smith [FRS16, FRS20] identified the notion of fuzzy min-entropy $\mathrm{H}^{\mathtt{fuzz}}_{t,\infty}(W)$ which measures the adversary's success when given oracle access to $\mathsf{Rep}(\cdot, p)$ but is unable to learn anything from the value p. Mathematically, fuzzy min-entropy quantifies the weight of the heaviest ball in the probability mass function of W. That is,

$$\mathrm{H}^{\mathtt{fuzz}}_{t,\infty}(W) := -\mathsf{log}\left(\max_{w'} \sum_{w|\mathsf{dis}(w,w')\leq t} \Pr[W = w]\right).$$

A primary goal of fuzzy extractor research is to build a single fuzzy extractor that works for the family of all distributions $\mathcal{W}^{\mathtt{all}}_{\mathtt{fuzz}} = \{W|\mathrm{H}^{\mathtt{fuzz}}_{t,\infty}(W) = \omega(\mathsf{log}(\lambda))\}$ for some security parameter λ. We call such a fuzzy extractor *universal* as it simultaneously works for any secureable distribution W. If one desires computational security, a universal fuzzy extractor is achievable using general obfuscation [BBC+14, BCKP14, BCKP17] or under specific number-theoretic assumptions [GZ19].

The situation for information-theoretic security is more complicated.[1] Fuller, Reyzin, and Smith [FRS20] showed that it is impossible to build a universal fuzzy extractor with information-theoretic security. More precisely, they constructed a family of distributions $\mathcal{W}' = \{W_z\}$ and showed that any fuzzy extractor $(\mathsf{Gen}, \mathsf{Rep})$ must be insecure for an average member of $\mathcal{W}'$. We let Z describe a uniformly chosen index for the family $\mathcal{W}'$, and use the notation W_Z to indicate the distribution arising from this

[1] Fuzzy extractors were first designed as an information-theoretic primitive because of strong connections to randomness extraction and coding theory. Many computational constructions use an information-theoretic secure sketch [WL18, WLG19]. (Exceptions exist such as the universal constructions listed above and constructions for distributions with additional properties [ACEK17, ABC+18, FMR20, CFP+21].)

choice of Z. Importantly, in the impossibility result the adversary knows the entire description of the chosen distribution (that is, W_Z) but not the individual point w that was input to Gen.

On the positive side, multiple works [HTW14, HTW16, FRS16, WCD+17, TW17, TVW18, LA18, FP19, FRS20] presented a construction that works for each $W_Z \in \mathcal{W}^{\mathtt{all}}_{\mathtt{fuzz}}$. This is called the *distribution-sensitive* setting as Gen also knows the entire probability mass function Z of the chosen W_Z, denoted as $\mathsf{Gen}_{W_Z}, \mathsf{Rec}_{W_Z}$. All constructions in this line are computationally inefficient; for an input point w they look up the probability that $\Pr[W_Z = w]$ and the probability of points w' where $\mathsf{dis}(w, w') \leq t$.

We show this inefficiency is unavoidable:

> **Any distribution-sensitive information-theoretic fuzzy extractor requires an exponential amount of information about the distribution W.**

Our results are for the Hamming metric over $\{0,1\}^n$. Below we present the two informal theorems for fuzzy extractors (see Theorem 6) and secure sketches (see Theorem 14) respectively. For a value $p \in [0,1]$ let h_2 be the binary entropy of p.

Theorem 1 (Informal Theorem 6)**.** *Consider $\{0,1\}^n$ and $t < n/2$ be a distance parameter. Let $\mathcal{W}_\gamma = \{W | \mathrm{H}^{\mathtt{fuzz}}_{t,\infty}(W) = \gamma\}$. Let $c > 0$ be a constant and suppose that*

$$\gamma \leq n \cdot \min\left\{(1 - h_2(t/n)) + o(1), \frac{1 - \Theta(c) - h_2(1/2 - t/n)}{3}\right\}.$$

For a quarter of $W \in \mathcal{W}_\gamma$ there is no fuzzy extractor that simultaneously has 1) no error 2) is of size at most $2^{\gamma + cn}$ 3) extracts keys of length $\omega(\log(n))$ that are within statistical distance $1/3 - \mathtt{ngl}(n)$ to a uniform key.

Theorem 2 (Informal Theorem 14)**.** *Consider $\{0,1\}^n$ and $t < n/2$ be a distance parameter. Let $\mathcal{W}_\gamma = \{W | \mathrm{H}^{\mathtt{fuzz}}_{t,\infty}(W) = \gamma\}$. Let $\delta < 1/4$ be the error of the secure sketch, let $c > 0$ be a constant and suppose that*

$$\gamma \leq n \cdot \min\left\{(1 - h_2(t/n)) + o(1), \frac{c_\delta}{3} h_2(t/n) - \Theta(c) - \Theta(1/n)\right\}.$$

where $1/3 < c_\delta < 2/3$ and depends on $h_2(\delta)$. For 2^{-4} fraction of $W \in \mathcal{W}_\gamma$ there is no secure sketch of size of at most $2^{\gamma + cn}$ that retains unpredictability of $w|ss$ of at least 4.

The relevant parameter regimes of impossibility are shown in Figure 1. The two most important parameters are the noise rate t/n and the fuzzy entropy rate γ/n. The area under the curves represents parameters where the construction is impossible for the fraction of distributions in the informal theorems unless one has algorithms of $2^{\Theta(n)}$ size. In spirit, our result rules out constructions that do not have a full description of the probability mass function written in their description. Our results are actually stronger, restricting only the amount of information about W not the running time or size.

There are (at least) two natural interpretations of the above result: 1) that fuzzy min-entropy does not measure the suitability of distributions for key derivation or 2) that efficient fuzzy extractors are an inherently computational object.

The notion of fuzzy min-entropy One of the principal components of a fuzzy extractor is privacy amplification where smooth conditional min-entropy [RW05] is a necessary and sufficient condition. This rather precisely characterizes the regime of feasibility for efficient privacy amplification as an information-theoretic task. However, the gap between necessary and sufficient conditions for *efficient* primitives that perform information reconciliation appears much wider. The only known efficient constructions for information reconciliation fall into one of two categories:

High entropy If the source W has high entropy $\mathrm{H}_\infty(W) \geq \omega(\log(n)) + \log(|B_t|)\,|$ (where $|B_t|$ is the size of a Hamming ball of radius t) then one can build a good secure sketch by writing down the syndrome of an error correcting code which corrects t errors. This syndrome construction leaks

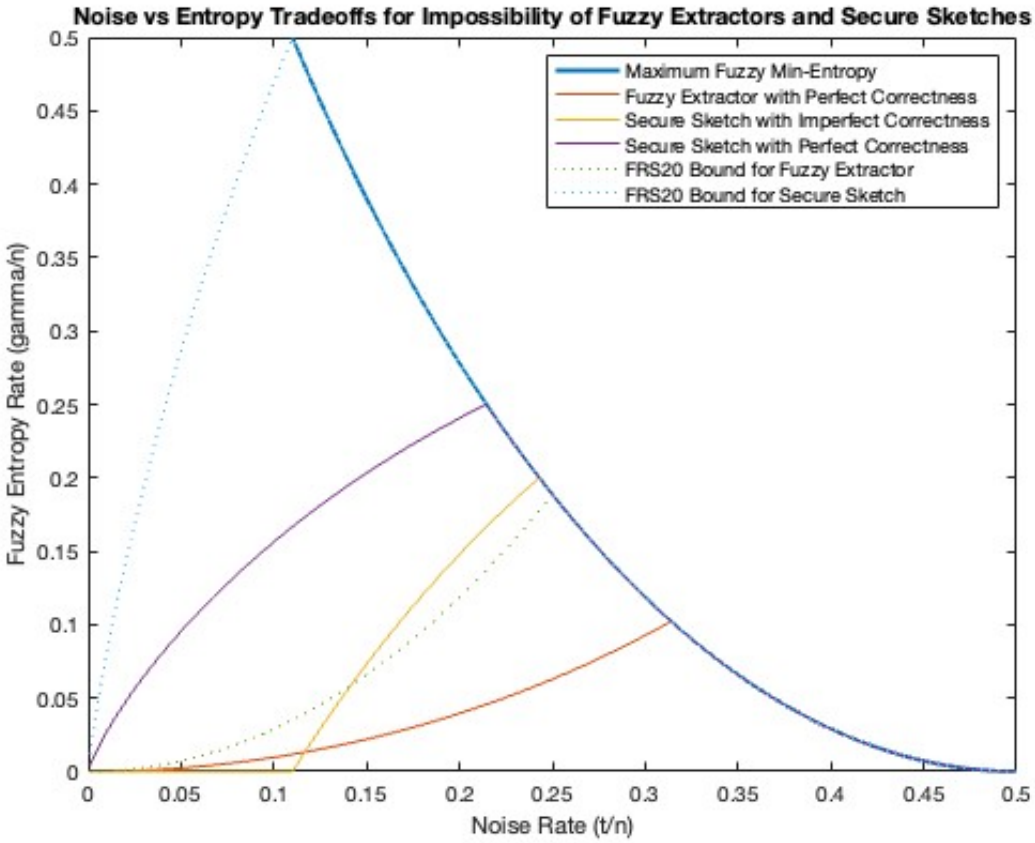

Figure 1: The region of error rate t/n (x-axis) and fuzzy entropy rate γ/n (y-axis) pairs for which the two negative results apply. The six curves are maximum fuzzy min-entropy $\gamma/n = (1 - h_2(t/n))$, Theorem 6, Theorem 14 with $\delta = .25$, Theorem 14 with $\delta = 0$, [FRS20, Theorem 5.1] and [FRS20, Theorem 7.2]. The parameter δ is how frequently the secure sketch is allowed to be incorrect. We consider fuzzy extractors with perfect correctness where $\delta = 0$.

at least $\mathsf{log}(|B_t|)$ bits of information about W.[2] Unfortunately, this construction provides no guarantee when $\mathrm{H}_\infty(W) < \mathsf{log}(|B_t|)$ which is the case for biometrics, see [CFP+21, Proposition 1] and [SSF19, Introduction].

Highly structured Sources where each bit is i.i.d. can be analyzed using Shannon entropy. In this setting, key rate asymptotically approaches $\mathrm{H}^{\mathbf{fuzz}}_{t,\infty}(W)$ if one assumes the second reading w' will be uniformly distributed in the ball around the first reading [TG04, Theorem 2]. Unfortunately, coordinates of real-physical sources are rarely i.i.d. [Dau04].

Unfortunately, there isn't an obvious sufficient condition to adopt rather than fuzzy min-entropy. Various weaker structured conditions have been used in the computational regime but with little evidence that physical sources have these properties [DFR21, Figure 1] and [SSF19]. Thus, a desirable research goal is to identify statistical properties possessed by physical sources that bypass our negative results.

[2] A construction that leaks only $\mathsf{log}(|B_t|)$ bits about W requires a perfect code which are rarely achievable.

Fuzzy extractors are computational objects The other natural explanation of the result is that non-interactive information reconciliation should be considered a computational object. This is our preferred interpretation since one can build universal (and efficient) fuzzy extractors if computational security suffices. We note that the only known constructions assume either general obfuscation [BBC+14, BCKP14, BCKP17] or specific number-theoretic assumptions that are not well studied [GZ19]. Thus, an important direction of research is to understand the required assumptions to build efficient, universal fuzzy extractors with computational security.

1.1 Proof Techniques

Our results are information-theoretic. As discussed above, we shall consider a family of distributions $\mathcal{W} = \{W_z\}$, let Z denote a uniformly random index for $\mathcal{W}$, and let W_Z denote the distribution determined by this choice of Z. Lastly, we use $w \leftarrow W_Z$ to denote sampling a point from the distribution. We show the impossibility of two types of fuzzy extractors:

Def. 8 (Universal) Fuzzy extractors with distributional advice. This is triple of algorithms $(\mathsf{advice}, \mathsf{Gen}, \mathsf{Rep})$ designed to work for all $W_Z \in \mathcal{W}$ where $\mathcal{W}$ consists of all distributions with a certain amount of fuzzy min-entropy for a fixed error tolerance t. However, the fuzzy extractor is given information about Z. Namely, there is a deterministic algorithm $\mathsf{advice} = \mathsf{advice}(Z)$. Then both Gen and Rep are given advice. Define $w \leftarrow W_Z$ and $(r, p) \leftarrow \mathsf{Gen}(w, \mathsf{advice})$, it should be true that

$$(r, p, Z) \approx (U, p, Z).$$

Note that all information about Z given to Gen is contained in advice and the point w.

Def. 6 Fuzzy extractors for a specific distribution W that are required to have a bounded size description of $(\mathsf{Gen}, \mathsf{Rep})$.

We show impossibility of building a fuzzy extractor with distributional advice of length ℓ for $\mathcal{W}$ implies impossibility of building a space bounded fuzzy extractor for length ℓ (Lemma 4). The core of our negative results is to show the impossibility of building fuzzy extractors with distributional advice. Before introducing our proof techniques we perform a brief overview of Fuller, Reyzin, and Smith's [FRS20] impossibility result.

Review of Fuller, Reyzin, and Smith [FRS20] The correctness constraint of a fuzzy extractor says that for $(r, p) \leftarrow \mathsf{Gen}(w)$ for all w' close to w the correct key is reproduced, i.e., $\mathsf{Rep}(w', p) = r$. As such, one can partition the input space $\{0,1\}^n$ by what value of r the point $v \in \{0,1\}^n$ produces. Values v that could have produced r will be at least distance t from the boundary of this partition, we call the set of such v, $\mathtt{Viable}_{r,p}$. $\mathtt{Viable}_{r,p}$ can be bounded geometrically using the isoperimetric inequality [Har66]. This bound applies for any distribution over the inputs w.

Consider the following simple distinguisher for a triple r, p, z. One computes the key partition described above and the set $\mathtt{Viable}_{r,p}$. If $\mathtt{Viable}_{r,p} \cap W_z = \emptyset$ output the key is random, otherwise output key is real. The core of Fuller, Reyzin, and Smith's impossibility was to build a family $\mathcal{W}^{FRS}$ with three properties:

1. The distribution was 2-universal [CW77], so the remainder of the distribution was unknown conditioned on the input w.
2. Distributions $W_Z \in \mathcal{W}^{FRS}$ shared few points, and
3. Each distribution $\mathcal{W}^{FRS}$ had fuzzy min-entropy.

Together these three properties meant that for any partition most distributions W_Z would have few nonempty interiors and the real key could be distinguished from a uniform key. The family is as follows: let $\mathbf{C}$ be a linear error-correcting code with distance t, let $\mathbf{H}$ be its syndrome, let c be a coset. Then each $Z = (\mathbf{H}, c)$ is the set of all points $\{w \mid \mathbf{H}w = c\}$.

Moving to the distributional advice setting To set notation for the distributional advice game, we consider the following game for a tuple of algorithms $(\mathsf{advice}, \mathsf{Gen}, \mathsf{Rep})$:

1. A uniform sample from $W_Z \leftarrow \mathcal{W}$ where Z describes the distribution.
2. A bounded length $\mathsf{advice} = \mathsf{advice}(Z)$ is computed.
3. One computes $w \leftarrow W_Z$.
4. The algorithm computes $(r, p) \leftarrow \mathsf{Gen}(w, \mathsf{advice})$.
5. The adversary is given either (r, p, Z) or (u, p, Z) for a uniform u.

In [FRS20], the only information that Gen had about Z was the input point w. In our setting, Gen gets advice. Fuller, Reyzin, and Smith's family had a short description so advice could completely write Z, allowing Gen to align the interior of the parts with points in W_Z. Thus, it is clear that the distributional advice setting requires a distribution with no short description. It also requires showing that aligning the interior of the parts is difficult given an arbitrary bounded length advice. Both problems can be approached by removing the structure from the family and considering the set of all distributions $W_Z \in \mathcal{W}$ with fuzzy min-entropy at least γ.

We show there are few distributions with 2^k points chosen uniformly without replacement that do not have fuzzy min-entropy γ where $k = \gamma + cn$ for some $c > 0$. We call this set of distributions $U_{n,k}$ and use this set of distributions throughout most of our proofs. Let $w_1, ..., w_{2^k}$ be the points with nonzero probability. The key to the proof is showing that as long as $|\mathsf{advice}|$ is shorter than 2^k, most points $w_i|\mathsf{advice}$ are unpredictable. This argument must account for the fact that advice can choose to completely determine some points or provide equal information about all points.

The techniques for the secure sketch setting are similar, however, there are stronger geometric bounds on the number of viable points because secure sketches imply Shannon error correcting codes [DORS08, FMR20]. Our result considers a secure sketch that retains smooth min-entropy instead of min-entropy. This is so we can use $U_{n,k}$ throughout the proof and show this implies the hardness of building a secure sketch for all distributions with sufficient fuzzy min-entropy. Our final result also applies to secure sketches that retain non-smooth conditional min-entropy.

Importantly, both results operate generically in the size of the maximum number of viable points for the relevant primitive. Such bounds have been well established in the literature due to their connections with coding theory. This means if one can provide a new bound on fuzzy extractor or secure sketch quality this can be directly used in our results.

Comparing with Fuller, Reyzin, and Smith [FMR20] Our fuzzy extractor result requires the $|r| = \omega(\mathsf{log}(n))$. This is in contrast to Fuller, Reyzin, and Smith [FMR20] who showed an impossibility for a key length of 3.[3] This change comes because advice can supply a lot of information about a small number of points in W_Z, allowing Gen to ensure that some $\mathtt{Viable}_{r,p}$ are nonempty. Furthermore, all bounds are weaker than those of Fuller, Reyzin, and Smith. The core of the difference is that since $\mathcal{W}^{FRS}$ the adversary received entirely new information by the leftover hash lemma [HILL93, BDK+11]. In our setting, we argue about the expected number of points in W_Z that are included in the $\mathtt{Viable}$ region.

Our secure sketch result also considers an object that retains smooth conditional min-entropy [RW05]. Smooth conditional min-entropy means that one is statistically close to a distribution with min-entropy. Setting the closeness parameter to 0 gives traditional conditional min-entropy. This is so we can conduct the argument using $U_{n,k}$ and "smooth" to the family where all distributions have fuzzy min-entropy. Smooth conditional min-entropy is the necessary and sufficient condition for privacy amplification using a randomness extractor.

Organization The rest of this work is organized as follows, Section 2 covers preliminaries including the relevant definitions of fuzzy extractors and secure sketches. Section 3 presents the negative result

[3]Our result for secure sketches requires them to retain at least 4 bits of min-entropy about the input in comparison with [FMR20] which required the sketch to maintain 3 bits of entropy.

for fuzzy extractors including a proof outline, and Section 4 presents the negative result for secure sketches.

2 Preliminaries

For distributions X, Y over the same discrete domain,

$$\Delta(X,Y) \stackrel{def}{=} \frac{1}{2}\sum_{x\in X} \left|\Pr[X=x] - \Pr[Y=y]\right|.$$

For a metric space $(\mathcal{M}, \mathsf{dis})$ let $B_t(x) = \{y | \mathsf{dis}(x,y) \leq t\}$. If the size of $B_t(x)$ is the same for all points x we use $|B_t|$ to denote this quantity and say that the *size of balls is center independent*. All logarithms are base 2.

This work considers the possibility of constructing fuzzy extractors from a finite family of distributions that we will call $\mathcal{W}$. Throughout, we will need the ability to describe a particular value in this family. We let Z be an index for the distributions in the family and we denote a distribution as W_Z. The distribution W_Z can then be sampled, and we denote a sample of $w \leftarrow W_Z$ where $w \in \{0,1\}^n$.

2.1 Notions of Entropy

Entropy, denoted $\mathrm{H}(X)$, for some discrete random variable X is $\mathrm{H}(X) := \mathbb{E}_x\left[-\mathsf{log}(\Pr[X=x])\right]$. For a random variable X whose outcomes are in $\{0,1\}$, let $\Pr[X=1] = p$. The **binary entropy** of X is $h_2(X) := H(X) = -p\cdot\mathsf{log}(p) - (1-p)\cdot\mathsf{log}(1-p)$. For a discrete random variable X, **min-entropy** is $\mathrm{H}_\infty(X) := -\mathsf{log}(\max_{x_i}\Pr(X=x_i))$.

Definition 1 (Average Min Entropy)**.** *Let X be a discrete random variable and let Y be a random variable. The* average min-entropy *of $X|Y$ is*

$$\tilde{\mathrm{H}}_\infty(X|Y) := -\mathsf{log}\left(\mathop{\mathbb{E}}_{y\leftarrow Y}\left[\max_x \Pr[X=x \mid Y=y]\right]\right).$$

Definition 2 (Smooth Conditional Min Entropy [RW05])**.** Smooth Conditional Min Entropy*, denoted $\tilde{\mathrm{H}}^\epsilon_\infty(X|Y)$ for two random variables X and Y is*

$$\tilde{\mathrm{H}}^\epsilon_\infty(X|Y) := \max_{(X',Y')|\Delta((X',Y'),(X,Y))\leq\epsilon} \tilde{\mathrm{H}}_\infty(X'|Y').$$

The above definition combines definitions from Renner and Wolf [RW05] and Dodis et al. [DORS08]. Renner and Wolf's definition considers the worst case Y. We focus on the average case Y because the above definition suffices for randomness extraction.

2.2 Fuzzy Min-Entropy and Hamming Balls

Definition 3 (Fuzzy min-entropy [FRS20])**.** *For a distribution W and a distance parameter t, the fuzzy min-entropy of W, denoted $\mathrm{H}^{\mathtt{fuzz}}_{t,\infty}(W)$ is*

$$\mathrm{H}^{\mathtt{fuzz}}_{t,\infty}(W) := -\mathsf{log}\left(\max_{w^*}\left(\sum_{w,\mathsf{dis}(w,w^*)\leq t}\Pr[W=w]\right)\right).$$

Proposition 3. *For all distributions W over a metric space $(\mathcal{M},\mathsf{dis})$,*

$$\mathrm{H}^{\mathtt{fuzz}}_{t,\infty}(W) \leq \mathsf{log}(|\mathcal{M}|) - \mathsf{log}(|B_t|).$$

For $\mathcal{M} = \{0,1\}^n$ and the binary Hamming metric, Using Ash [Ash12, Lemma 4.7.2, Equation 4.7.5, p. 115] one has

$$nh_2(t/n) - 1/2\mathsf{log}(n) - 1/2 \leq \mathsf{log}(|B_t|) \leq nh_2(t/n). \tag{1}$$

and thus,

$$\mathrm{H}^{\mathtt{fuzz}}_{t,\infty}(W) \leq \mathsf{log}(|\mathcal{M}|) - \mathsf{log}(|B_t|) \leq n\left(1 - h_2\left(\frac{t}{n}\right)\right) + \frac{\mathsf{log}(n)}{2} + 1/2.$$

We now introduce the notion of β-density which measures the size of a Hamming ball in comparison to the whole metric space.

Definition 4. *Let $(\mathcal{M}, \mathsf{dis})$ be a metric space where the size of balls is center independent. The β density is*

$$\beta := \mathsf{log}\left(\frac{|\mathcal{M}| - |B_t|}{|B_t|}\right)$$

Claim 1. *For the binary Hamming metric over $\{0,1\}^n$ for $t < n/2$*

$$n\left(1 - h_2\left(\frac{t}{n}\right)\right) - 1 \leq \beta \leq n\left(1 - h_2\left(\frac{t}{n}\right)\right) + \frac{\mathsf{log}(n)}{2} + \frac{1}{2}.$$

Proof. By Equation 1 one has:

$$\beta = \mathsf{log}\left(\frac{2^n}{|B_t|} - 1\right) \leq \mathsf{log}\left(2^{n\left(1-h_2\left(\frac{t}{n}\right)\right)+1/2\mathsf{log}(n)+1/2} - 1\right) \leq n\left(1 - h_2\left(\frac{t}{n}\right)\right) + \frac{1}{2}\mathsf{log}(n) + \frac{1}{2}$$
$$\beta \geq \mathsf{log}\left(2^{n\left(1-h_2\left(\frac{t}{n}\right)\right)} - 1\right) \geq \mathsf{log}\left(2^{n\left(1-h_2\left(\frac{t}{n}\right)\right)-1}\right) \geq n(1 - h_2(t/n)) - 1.$$

□

2.3 Fuzzy Extractors and Secure Sketches

Definition 5 (Secure Sketch [DORS08])**.** *For metric space $(\mathcal{M}, \mathsf{dis})$ and distribution W with probability mass function z, a $(\mathcal{M}, \tilde{m}, t, \epsilon, \delta, \ell)$-*secure sketch *is a pair of algorithms $(\mathsf{SS}_z, \mathsf{Rec}_z)$ with the following properties*

1. ***Correctness*** *For all w, w' such that $\mathsf{dis}(w, w')$, then $\Pr_{ss \leftarrow \mathsf{SS}(w)}[\mathsf{Rec}_z(w', ss) = w] \geq 1 - \delta$.*
2. ***Security*** $\tilde{\mathrm{H}}^{\epsilon}_{\infty}(W|\mathsf{SS}_z(W)) \geq \tilde{m}$.
3. ***Space Bounded*** *The circuits SS_z and Rec_z require at most ℓ bits to describe. That is, $|\mathsf{SS}_z| + |\mathsf{Rec}_z| \leq \ell$.*

The use of smooth min-entropy In the above, the secure sketch is required to retain smooth conditional min-entropy of W conditioned on the sketch. Many definitions consider $\epsilon = 0$ or average min-entropy. However, smooth min-entropy is the necessary and sufficient condition for privacy amplification through the use of an average-case randomness extractor [RW05].

Definition 6 (Fuzzy Extractor [DORS08])**.** *For metric space $(\mathcal{M}, \mathsf{dis})$ and probability distribution W with probability mass function z, a $(\mathcal{M}, \kappa, t, \epsilon)$-*fuzzy extractor *is a pair of algorithms $(\mathsf{Gen}_z, \mathsf{Rep}_z)$ with the following properties*

1. ***Correctness*** *For all w, w' such that $\mathsf{dis}(w, w')$, then $\Pr_{r,p \leftarrow \mathsf{Gen}(w)}[\mathsf{Rep}(w', p) = r] = 1$.*
2. ***Security*** *Let $R, P \leftarrow \mathsf{Gen}_z(W)$ and U_κ be a uniformly distributed random variable over $\{0,1\}^\kappa$, $\Delta((R, P), (U_\kappa, P)) \leq \epsilon$.*
3. ***Space Bounded*** *The circuits Gen_z and Rep_z require ℓ bits to describe. That is, $|\mathsf{Gen}| + |\mathsf{Rec}| \leq \ell$.*

We now define fuzzy extractors and secure sketches with advice. This is an intermediate definition that will be used in proofs throughout. As we show in Lemmas 4 and 5, the impossibility of building a fuzzy extractor (resp. secure sketch) with advice for a family $\mathcal{W}$ implies the impossibility of building a fuzzy extractor (resp. secure sketch) for many $W_Z \in \mathcal{W}$.

Definition 7 (Secure Sketch with distributional advice)**.** *Let $\mathcal{W}$ be a family of distributions indexed by z. That is, denote each distribution in $\mathcal{W}$ as W_Z with Z describing the probability mass function of W. For metric space $(\{0,1\}^n, \mathsf{dis})$, a $(\{0,1\}^n, \mathcal{W}, \tilde{m}, t, \epsilon, \delta, \ell)$*-secure sketch with distributional advice *is a triple of algorithms $(\mathsf{Gen}, \mathsf{Rep}, \mathsf{Advice})$ with the following properties:*

1. ***Correctness*** *For all w, w' such that $\mathsf{dis}(w, w')$, let $\Pr_{ss \leftarrow \mathsf{SS}(w)}[\mathsf{Rec}(w', ss) = w] \geq 1 - \delta$.*
2. ***Security*** *Let Advice be a deterministic function with output in $\{0,1\}^\ell$. For all distributions $W_Z \in \mathcal{W}$, define $\mathsf{advice}_Z := \mathsf{Advice}(Z)$ and let $ss \leftarrow \mathsf{SS}(W_Z, \mathsf{advice}_Z)$. Then, $\mathbb{E}_Z[\tilde{\mathrm{H}}^{\epsilon}_{\infty}(W_Z|ss)] \geq \tilde{m}$.*

Definition 8 (Fuzzy Extractor with distributional advice)**.** *Let $\mathcal{W}$ be a family of distributions indexed by z. That is, denote each distribution in $\mathcal{W}$ as W_Z with Z describing the probability mass function of W. For metric space $(\{0,1\}^n, \mathsf{dis})$, a $(\{0,1\}^n, \mathcal{W}, \kappa, t, \epsilon, \ell)$*-fuzzy extractor with distributional advice *is a triple of algorithms $(\mathsf{Gen}, \mathsf{Rep}, \mathsf{Advice})$ with the following properties:*

1. ***Correctness*** *For all w, w' such that $\mathsf{dis}(w, w')$, let $\Pr_{(r,p) \leftarrow \mathsf{Gen}(w)}[\mathsf{Rep}(w', p) = r] = 1$.*
2. ***Security*** *Let Advice be a deterministic function with output in $\{0,1\}^\ell$. For a distribution $W_Z \in \mathcal{W}$, define $\mathsf{advice}_Z := \mathsf{Advice}(Z)$, let $(R, P) \leftarrow \mathsf{Gen}(W, \mathsf{advice}_Z)$ and U_κ be a uniformly distributed random variable over $\{0,1\}^\kappa$ it holds that $\Delta((R, P, Z), (U_\kappa, P, Z)) \leq \epsilon$.*

Lemma 4. *Let $\mathcal{W}$ be a distribution family indexed by the set Z and suppose that no $(\mathcal{M}, \mathcal{W}, \kappa, t, \epsilon, \ell)$-fuzzy extractor with distributional advice exists. For all families $\mathcal{W}' \subseteq \mathcal{W}$ indexed by $Z' \subseteq Z$ where*

$$\frac{|Z' \cap Z|}{|Z|} = \frac{|Z'|}{|Z|} \leq 1 - \zeta$$

there is some Z' there is no $(\{0,1\}^n, \kappa, t, (\epsilon - \zeta)/(1 - \zeta), \ell)$ fuzzy extractor $(\mathsf{Gen}_Z, \mathsf{Rep}_Z)$.

Proof of Lemma 4. We proceed by contrapositive. Let $\mathcal{W}'$ be some subset of $\mathcal{W}$ with relative size at least $1 - \zeta$ where for every $W_Z \in \mathcal{W}'$ there exists an $(\{0,1\}^n, \kappa, t, (\epsilon - \zeta)/(1 - \zeta), \ell)$-fuzzy extractor. We denote these algorithms by $(\mathsf{Gen}_Z, \mathsf{Rep}_Z)$ respectively. We now describe how to build the fuzzy extractor $(\mathsf{Gen}, \mathsf{Rep}, \mathsf{advice})$ with distributional advice. Let

$$\mathsf{advice}(Z) = \begin{cases} (\mathsf{Gen}_Z, \mathsf{Rep}_Z) & Z \in Z' \\ \perp & \text{otherwise.} \end{cases}$$

In both cases, $\mathsf{advice}(Z)$ has length at most ℓ. Then define $\mathsf{Gen}(x, C)$ as follows: if $C = \perp$ sample a random key r output (r, r), otherwise interpret C as two circuits $\mathsf{Gen}', \mathsf{Rep}'$ and output $\mathsf{Gen}'(x)$. Define $\mathsf{Rep}(x, p, C)$ interpret C if $C = \perp$ output p, otherwise parse C as two circuits $\mathsf{Gen}', \mathsf{Rep}'$ and output $\mathsf{Rep}'(x', p)$. Then

$$\begin{aligned} \Delta((R, P, Z), (U_\kappa, P, Z)) &= \Delta((R, P, Z), (U_\kappa, P, Z)|Z \in Z') + \Delta((R, P, Z), (U_\kappa, P, Z)|Z \notin Z') \\ &\leq \frac{\epsilon - \zeta}{1 - \zeta} * (1 - \zeta) + 1 * \zeta = \epsilon. \end{aligned}$$

It is clear that $(\mathsf{Gen}, \mathsf{Rep}, \mathsf{advice})$ is a $(\mathcal{M}, \mathcal{W}, \kappa, t, \epsilon, \ell)$ fuzzy extractor with distributional advise. □

Interpretation In the setting when $\epsilon = \Theta(1)$ then setting $\zeta = \epsilon/2$ implies that for all subsets $\mathcal{W}' \subseteq \mathcal{W}$ where $\Pr[Z \in Z'] \geq 1 - \epsilon/2 = 1 - \Theta(1)$ there is no $(\{0,1\}^n, \kappa, t, \epsilon/(2 - \epsilon), \ell)$-fuzzy extractor for some element of $\mathcal{W}'$. This shows that at least $\epsilon/2 = \Theta(1)$ fraction of elements in $\mathcal{W}$ do not have $(\{0,1\}^n, \kappa, t, \epsilon/(2 - \epsilon), \ell)$-fuzzy extractors. This is the setting considered in Section 3.

Lemma 5. *Let $\mathcal{W}$ be a distribution family indexed by Z and suppose that no $(\{0,1\}^n, \mathcal{W}, \tilde{m}, t, \epsilon, \delta, \ell)$-secure sketch with distributional advice exists. For all families $\mathcal{W}' \subseteq \mathcal{W}$ indexed by $Z' \subseteq Z$ where*

$$\frac{|Z \cap Z'|}{|Z|} = \frac{|Z'|}{|Z|} \geq 1 - 2^{-\zeta}$$

there is some Z' for which no $(\{0,1\}^n, \min\{\tilde{m}, \zeta\}, t, \epsilon, \delta, \ell)$ fuzzy extractor $(\mathsf{SS}_{Z'}, \mathsf{Rec}_{Z'})$ exists.

Proof. The proof of Lemma 5 follows the structure of the proof of Lemma 4. With $ss = w$ and with the following equation for computing the remaining smooth conditional min-entropy.

$$\begin{aligned}
\mathop{\mathbb{E}}_{Z}[\tilde{\mathrm{H}}^{\epsilon}_{\infty}(W_Z|\mathsf{SS}(W_Z), Z)] &= -\mathsf{log}\Big(\Pr[Z \in Z'] \mathop{\mathbb{E}}_{Z} 2^{-\tilde{\mathrm{H}}^{\epsilon}_{\infty}(W_Z|ss, Z \in Z')} + \Pr[Z \notin Z'] \mathop{\mathbb{E}}_{Z} 2^{-\tilde{\mathrm{H}}^{\epsilon}_{\infty}(W_Z|ss, Z \notin Z')}\Big) \\
&\geq -\mathsf{log}\big(1 \cdot 2^{-\tilde{m}} + 2^{-\zeta} \cdot 1\big) \\
&\geq -\mathsf{log}\big(2^{-\tilde{m}} + 2^{-\zeta}\big) \geq \min\{\tilde{m}, \zeta\}.
\end{aligned}$$

□

Interpretation The natural parameter setting of the above is setting $\zeta = \max\{\tilde{m}, 1\}$ which shows that at least $2^{-\tilde{m}}$ of the distributions have no secure sketch. Later in this work, we consider $\tilde{m} = \Theta(1)$ which suffices to that show that a constant fraction of distributions have no secure sketch.

3 Efficient Information-Theoretic Fuzzy Extractors do not exist for most distributions with fuzzy min-entropy

Our main theorem considers the following distribution of distributions:

$\mathtt{PCode}_{n,k,t,\gamma}$ The uniform distribution over all sets $X = \{x_i\}$ of size 2^k with the additional condition that $\mathrm{H}^{\mathtt{fuzz}}_{t,\infty}(X) \geq \gamma$. Some points are allowed to lie within distance t as long as fewer than $2^{k-\gamma}$ lie within a single ball of radius t.

Theorem 6. *Let $\gamma \in \mathbb{R}^+, n, \kappa, t, \ell, \gamma \in \mathbb{Z}^+$ be parameters.*

1. *The β-density is at least 1 which is satisfied as long as $t < n/2$ (see Definition 4),*
2. *Let $\nu \in \mathbb{Z}^+$ be a free parameter, and*
3. *Let $\mu = n \cdot h_2\big(\frac{1}{2} - \frac{t}{n}\big)$.*

For a $(1/4 - (\epsilon_1 + \epsilon_2 + \epsilon_3)/2)$-fraction of the distributions $W \in \mathtt{PCode}_{n,k,t,\gamma}$ there is no $(\{0,1\}^n, W, \kappa, t, \epsilon, \ell)$-fuzzy extractor for

$$\epsilon < \frac{1}{3} - \frac{2(\epsilon_1 + \epsilon_2 + \epsilon_3)}{3}.$$

For

$$\begin{aligned}
\mathsf{log}(\epsilon_1) &:= -\left(\kappa + \frac{\alpha - \ell}{2^k} - \mu - 2k + \mathsf{log}(\nu)\right), \\
\epsilon_2 &:= \frac{\nu + 1}{2^{\kappa+1}} \\
\epsilon_3 &:= \left(e 2^{\gamma - \beta}\right)^{2^{k-\gamma}} 2^n.
\end{aligned}$$

Recall that Lemma 4 states that to show the hardness of building a fuzzy extractor with distributional advise for $\mathtt{PCode}_{n,k,t,\gamma}$ it suffices to show the hardness of building an auxiliary input fuzzy extractor for the family $\mathtt{PCode}_{n,k,t,\gamma}$.

Our proof uses the following structure:

1. The family $\mathtt{PCode}_{n,k,t,\gamma}$ is complicated to work with. Thus, as a first step we show it is statistically close to the family that picks k points without replacement, which we denote as $U_{n,k}$.[4] Lemma 7 shows that the distribution $\mathtt{PCode}_{n,k,t,\gamma}$ is statistically close to the distribution $U_{n,k}$. For the remainder of the proof we consider $U_{n,k}$.
2. Lemma 8 which bounds the number of "viable" points for most public values p. Note that this Lemma bounds the total number of points and holds even if $\mathsf{Gen}, \mathsf{Rep}$ have access to an arbitrary advice string.
3. Lemma 9 for the distribution, $U_{n,k}$ the advice string can only reduce the entropy of almost all viable points by a small amount. We call such points **Average Points**. There are some points that the adversary has a large amount of information on that we call **Free Points**.
4. Corollary 10 puts together the above two Lemmas to show that the adversary includes a small number of points from the distribution in the viable set.
5. Lemma 11 shows that since the construction cannot align the viable points with the distribution there exists a distinguisher that can distinguish a uniform triple from a key triple.

The rest of this section is organized as follows:

Section 3.1 We present the formal versions of the above statements,

Section 3.2 We present the proof of Theorem 6,

Section 3.3 We present our preferred setting of parameters, and

Section 3.4 We prove the above statements.

3.1 Proof Overview

Lemma 7 shows that $\mathtt{PCode}_{n,k,t,\gamma}$ is statistically close to $U_{n,k}$.

Lemma 7. *Let n, k, t, γ be parameters such that the β density is at least 0 (which is satisfied as long as $t < n/2$). Then one has that*

$$\Delta(U_{n,k}, \mathtt{PCode}_{n,k,t,\gamma}) \leq \left(e2^{\gamma-\beta}\right)^{2^{k-\gamma}} 2^n.$$

Fuller, Reyzin, and Smith [FRS16, FRS20] bound the number of points that could have produced the output of a fuzzy extractor. Such points are called viable. We present a stronger version of their lemma that is contained in their proof. The difference is we bound the union of viable points across different values of key while they only bound the size of a single key corresponding to the true point. Their argument is purely geometric, so it also applies to fuzzy extractors with distributional advice. We restate the stronger version of [FRS20, Lemma 5.2].

Lemma 8. *Suppose $\mathcal{M}$ is $\{0,1\}^n$ with the Hamming Metric, $\kappa \geq 2$, $0 \leq t \leq n/2$, $\epsilon > 0, \ell \in \mathbb{Z}^+$. Suppose $(\mathsf{Gen}, \mathsf{Rep})$ is a $(\mathcal{M}, \mathcal{W}, \kappa, t, \ell, \epsilon)$-fuzzy extractor with distributional advice for some distribution family $\mathcal{W}$ over $\mathcal{M}$. For any fixed p, for any value $\mathsf{advice} \in \{0,1\}^\ell$, there is a set $\mathsf{GoodKey}_p \subseteq \{0,1\}^\kappa$ of size at least $2^{\kappa-1}$ such that for every $\mathsf{key} \in \mathsf{GoodKey}_p$,*

$$\mu := \sum_{\mathsf{key} \in \mathsf{GoodKey}_p} \left(\log(|\{v \in \mathcal{M} | (\mathsf{key}, p) \in \mathsf{supp}(\mathsf{Gen}(v, \mathsf{advice}))\}|)\right) \leq n \cdot h_2\left(\frac{1}{2} - \frac{t}{n}\right).$$

We consider the following family Z which chooses 2^k points without replacement from the space $\{0,1\}^n$. That is, if one samples Z uniformly then one obtains the distribution $U_{n,k}$. For convenience we use $W_{z,1}, ..., W_{z,2^k}$ to describe the 2^k points with nonzero probability in W_z for some value z. We assume no ordering over these points.

[4] For $U_{n,k}$, there are $\binom{2^n}{2^k}$ outcomes each occurring with probability $1/\binom{2^n}{2^k}$.

Lemma 9 bounds how much information advice contains about the points in the distribution. Let Z describe a uniform sample of $U_{n,k}$. Let $(\mathsf{Gen}, \mathsf{Rep}, \mathsf{Advice})$ be an auxiliary input fuzzy extractor. Let $\mathsf{advice} = \mathsf{Advice}(Z)$ be of length ℓ. For a tuple $(v, p, r, \mathsf{advice})$ define

$$\texttt{Viable}(v, p, r, \mathsf{advice}) = \begin{cases} 1 & \Pr[\mathsf{Gen}(v, \mathsf{advice}) = (r, p)] > 0 \\ 0 & \text{otherwise} \end{cases}.$$

Fix some p and let $\texttt{GoodKey}_p$ be defined as in Lemma 8.

Lemma 9. *Let Z describe a uniform sample of $U_{n,k}$. Let $\mathsf{advice} = \mathsf{Advice}(Z)$ be of length ℓ. For a particular $Z = z$ let $w_{z,1}, ..., w_{z,2^k}$ denote the points in W_Z. Let $\alpha := \log\left(\binom{2^n}{2^k}\right)$. Let μ be defined as in Lemma 8. For each value advice there is some set $\mathcal{I}_{\mathsf{advice}}$ of size at most $\nu + 1$, it is true for each $i \notin \mathcal{I}_{\mathsf{advice}}$ that*

$$\log(\Pr[\texttt{Viable}(w_{z,i}, p, \mathsf{key}, \mathsf{advice}) = 1]) \leq -\frac{\alpha - |\mathsf{advice}|}{2^k} + 1 + \mu + k - \log(\nu).$$

Corollary 10. *Suppose that*

$$\sum_{\mathsf{key} \in \texttt{GoodKey}_p} (\log(|\{v \in \mathcal{M} | (\mathsf{key}, p) \in \mathsf{supp}(\mathsf{Gen}(v))\}|)) \leq 2^\mu$$

For a particular $Z = z$ let $w_{z,1}, ..., w_{z,2^k}$ denote the points in W_Z. Let $\alpha := \log\left(\binom{2^n}{2^k}\right)$. Then for each value advice there is some set $\mathcal{I}_{\mathsf{advice}}$ of size at most $\nu + 1$, then it is true for each $i \notin \mathcal{I}_{\mathsf{advice}}$ that

$$\Pr\left[\left(\sum_{\mathsf{key} \in \texttt{Goodkey}_p} \texttt{Viable}(w_{z,i}, p, \mathsf{key}, \mathsf{advice}, z)\right) = 1 \middle| \begin{array}{r} z \leftarrow Z \\ \mathsf{advice} = \mathsf{Advice}(z) \\ w \leftarrow W_Z \\ (r, p) \leftarrow \mathsf{Gen}(w, \mathsf{advice}) \end{array}\right] < 2^{-\frac{\alpha - |\mathsf{advice}|}{2^k} + 1 + \mu + k - \log(\nu)}.$$

And thus, for on average across Z, the expected number of points outside of $\mathcal{I}_{\mathsf{advice}}$ that are included in $\texttt{Viable}$ *is at most*

$$\mathop{\mathbb{E}}_{Z}\left[\sum_{\mathsf{key} \in \texttt{Goodkey}_p} \sum_{i | w_{z,i} \notin \mathcal{I}_{\mathsf{advice}}} \texttt{Viable}(w_{z,i}, p, \mathsf{key}, \mathsf{advice}) \middle| \begin{array}{r} z \leftarrow Z \\ \mathsf{advice} \leftarrow \mathsf{Advice}(z) \\ w \leftarrow W_Z \\ (r, p) \leftarrow \mathsf{Gen}(w, \mathsf{advice}) \end{array}\right] < 2^{-\frac{\alpha - |\mathsf{advice}|}{2^k} + 1 + \mu + 2k - \log(\nu)}.$$

And finally,

$$\mathop{\mathbb{E}}_{Z}\left[\sum_{\mathsf{key} \in \texttt{Goodkey}_p} \sum_{i} \texttt{Viable}(w_{z,i}, p, \mathsf{key}, \mathsf{advice}) \middle| \begin{array}{r} z \leftarrow Z \\ \mathsf{advice} \leftarrow \mathsf{Advice}(z) \\ w \leftarrow W_Z \\ (r, p) \leftarrow \mathsf{Gen}(w, \mathsf{advice}) \end{array}\right] < 2^{-\frac{\alpha - |\mathsf{advice}|}{2^k} + 1 + \mu + 2k - \log(\nu)} + \nu + 1.$$

Lemma 11. *Let all parameters be as in Corollary 10 with $\nu \in \mathbb{Z}^+$. Then there is no $(\{0,1\}^n, \mathcal{W}, \kappa, t, \epsilon, \ell)$-fuzzy extractor with distributional advise (see Definition 8) if*

$$\epsilon < 1/2 - (\epsilon_1 + \epsilon_2)$$

where

$$\epsilon_1 = 2^{-\kappa - \frac{\alpha - |\mathsf{advice}|}{2^k} + 1 + \mu + 2k - \log(\nu)},$$
$$\epsilon_2 = \frac{\nu + 1}{2^\kappa}.$$

Furthermore, there exists an algorithm $\mathcal{D}$ that always outputs 1 when given samples of the form r, p, z that are correctly generated by the fuzzy extractor.

3.2 Proof of Theorem 6

Proof of Theorem 6. Restating Lemma 11 one has that for $(R_{U_{n,k}}, P_{U_{n,k}}) \leftarrow \mathsf{Gen}(U_{n,k}, \mathsf{advice}(Z_{U_{n,k}}))$

$$\Delta((R_{U_{n,k}}, P_{U_{n,k}}, Z_{U_{n,k}}), (U_n, P_{U_{n,k}}, Z_{U_{n,k}})) \geq 1/2 - (\epsilon_1 + \epsilon_2).$$

Let $\mathcal{D}$ be one distinguisher that always outputs 1 on any value key, p, z for any distribution z, then

$$\Pr[\mathcal{D}((R_{U_{n,k}}, P_{U_{n,k}}, Z_{U_{n,k}})) = 1] = 1$$
$$\Pr[\mathcal{D}(U_n, P_{U_{n,k}}, Z_{U_{n,k}}) = 1] \leq 1/2 + (\epsilon_1 + \epsilon_2).$$

Recall that $\Delta(U_{n,k}, \mathtt{PCode}^*_{n,k,t,\alpha}) \leq \epsilon_3$ by Lemma 7 . Define

$$(R_{\mathtt{PCode}^*_{n,k,t,\alpha}}, P_{\mathtt{PCode}^*_{n,k,t,\alpha}}) \leftarrow \mathsf{Gen}(\mathtt{PCode}^*_{n,k,t,\alpha}, \mathsf{advice}(Z_{\mathtt{PCode}^*_{n,k,t,\alpha}})).$$

it is thus true that

$$\Pr[\mathcal{D}(R_{\mathtt{PCode}^*_{n,k,t,\alpha}}, P_{\mathtt{PCode}^*_{n,k,t,\alpha}}, Z_{\mathtt{PCode}^*_{n,k,t,\alpha}}) = 1] = 1,$$
$$\Pr[\mathcal{D}(U_n, P_{\mathtt{PCode}^*_{n,k,t,\alpha}}, Z_{\mathtt{PCode}^*_{n,k,t,\alpha}}) = 1] \leq 1/2 + (\epsilon_1 + \epsilon_2 + \epsilon_3).$$

Where the second and thus that

$$\Delta((R_{\mathtt{PCode}^*_{n,k,t,\alpha}}, P_{\mathtt{PCode}^*_{n,k,t,\alpha}}, Z_{\mathtt{PCode}^*_{n,k,t,\alpha}}), (U_n, P_{\mathtt{PCode}^*_{n,k,t,\alpha}}, Z_{\mathtt{PCode}^*_{n,k,t,\alpha}})) \geq 1/2 - (\epsilon_1 + \epsilon_2 + \epsilon_3).$$

Finally, the theorem follows by application of Lemma 4 with the setting of $\zeta = 1/4$. □

3.3 Analysis of parameters

We separately consider ϵ_1, ϵ_2 and ϵ_3. We refer to these three terms as average points, free points, and distributional closeness respectively. This is because ϵ_1 describes how much information the advice has about average points in W_Z, ϵ_2 considers a small number of points that are more thoroughly described by advice, and ϵ_3 controls the statistical distance between $U_{n,k}$ and $\mathtt{PCode}_{n,k,t,\alpha}$. We consider parameters in order of simplicity (rather than index ordering).

3.3.1 Free Points - ϵ_2

For ϵ_2 to be negligible it suffices that $\nu/2^\kappa$ is negligible. Note that for the fuzzy extractor to have meaningful security requires $\kappa = \omega(\log(n))$. We set

Condition 1 $\nu = 2^{c_\kappa \kappa}$ for some constant $0 < c_\kappa < 1$.

This yields

$$\epsilon_2 = \frac{\nu + 1}{2^\kappa} = 2^{(c_\kappa - 1)\kappa} + 2^{-\kappa} = \mathtt{ngl}(n).$$

3.3.2 Distributional Closeness - ϵ_3

Recall that $\epsilon_3 := \left(e2^{\gamma-\beta}\right)^{2^{k-\gamma}} 2^n$. Consider the following settings:

Condition 2 That $\gamma \leq \beta - \mathsf{log}(2e)$, which implies $2^{\gamma-\beta} \leq \frac{1}{2e}$, and

Condition 3 For some constant $0 < c_{|k|} < 1$, we set $k = \gamma + c_{|k|}n$ which implies $2^{k-\gamma} \geq n + \omega(\mathsf{log}(n))$.

Together, these settings imply that

$$\begin{aligned}\epsilon_3 &= \left(e2^{\gamma-\beta}\right)^{2^{k-\gamma}} 2^n \\ &\leq \left(\frac{1}{2}\right)^{n+\omega(\mathsf{log}(n))} 2^n = 2^{-\omega(\mathsf{log}(n))} = \mathtt{ngl}(n).\end{aligned}$$

Discussion By Lemma 3 for any W in $\{0,1\}^n$ it is true that

$$\mathrm{H}^{\mathtt{fuzz}}_{t,\infty}(W) \leq n\left(1 - h_2\left(\frac{t}{n}\right)\right) + \frac{\mathsf{log}(n)}{2} + 1/2.$$

Thus, the additional constraint that

$$\mathrm{H}^{\mathtt{fuzz}}_{t,\infty}(W) := \gamma \leq \beta - \mathsf{log}(2e) \leq n\left(1 - h_2\left(\frac{t}{n}\right)\right) + \frac{\mathsf{log}(n)}{2} + \frac{1}{2} - \mathsf{log}(2e)\,.$$

imposes an additive $\mathsf{log}(2e)$ impact on the maximal fuzzy min-entropy that can be supported.

3.3.3 Average Points - ϵ_1

We now turn to our analysis of ϵ_1. Recall that $\mathsf{log}(\epsilon_1) := -\left(\kappa + \frac{\alpha-\ell}{2^k} - \mu - 2k + \mathsf{log}(\nu)\right)$. Recall that

$$\begin{aligned}(n/k)^k \leq \binom{n}{k} &< ((ne)/k)^k \\ \mu &\leq nh_2(1/2 - t/n), \\ \alpha = \mathsf{log}\left(\binom{2^n}{2^k}\right) &\geq \mathsf{log}\left(2^{n2^k}/2^{k2^k}\right) = (n-k)2^k,\end{aligned}$$

Recall that $\nu = 2^{c_\kappa \kappa}$. This implies that

$$\begin{aligned}-\mathsf{log}(\epsilon_1) &= \kappa + \frac{\alpha-\ell}{2^k} - \mu - 2k + \mathsf{log}(\nu) \\ &\geq \kappa + \frac{\alpha-\ell}{2^k} - nh_2(1/2 - t/n) - 2k + \mathsf{log}(\nu)\,, \\ &\geq \kappa + \frac{(n-k)2^k - \ell}{2^k} - nh_2(1/2 - t/n) - 2k + c_\kappa\kappa, \\ &\geq (1+c_\kappa)\kappa + \frac{(n-k)2^k - 2k2^k - \ell}{2^k} - nh_2(1/2 - t/n) \\ &> (1+c_\kappa)\kappa + \frac{(n-3k)2^k - \ell}{2^k} - nh_2(1/2 - t/n).\end{aligned}$$

We now focus on showing a parameter setting when $\psi := \frac{(n-3k)2^k-\ell}{2^k} - nh_2(1/2 - t/n) \geq 0$.

Condition 4 Let $0 < c_\ell < 1$ be a parameter such that $\ell \leq 3c_\ell n 2^k$,

Condition 5 and

$$\gamma \leq \frac{n(1-3c_{|k|}-c_\ell-h_2(1/2-t/n))}{3}.$$

Then it holds that

$$\begin{aligned}\psi :&= \frac{(n-3k)2^k-\ell}{2^k} - nh_2(1/2-t/n)\\ &\geq \frac{(n-3k)2^k-c_\ell n2^k}{2^k} - nh_2(1/2-t/n)\\ &\geq \frac{(1-3(\gamma/n+c_{|k|})-c_\ell n2^k}{2^k} - nh_2(1/2-t/n)\\ &\geq n(1-3c_{|k|}-c_\ell) - 3\gamma - nh_2(1/2-t/n) \geq 0\end{aligned}$$

which suffices to ensure that

$$\mathsf{log}(\epsilon_1) \leq -\left((1+c_\kappa)\kappa+\psi\right) \leq -(1+c_\kappa)\kappa = -\omega(\mathsf{log}(n)).$$

3.3.4 Overall Parameters

Combining Conditions 2 and 5 one obtains a negligible statistical distance as long as for constants $c_\kappa, c_{|k|}, c_\ell \in (0,1)$ one has:

$$\begin{aligned}&\nu = 2^{c_\kappa \kappa},\\ &k = \gamma + c_{|k|}n,\\ &\ell \leq 3c_\ell n 2^k,\\ 0 \leq \frac{\gamma}{n} \leq \min&\left\{(1-h_2(t/n)) + \frac{\mathsf{log}(n)+1-2\mathsf{log}(2e)}{2n}, \frac{1-3c_{|k|}-c_\ell-h_2(1/2-t/n)}{3}\right\}.\end{aligned}$$

3.4 Proof of Technical Lemmas

3.4.1 Proof of Lemma 7

Proof of Lemma 7. We begin by showing the fraction of items in the support of $U_{n,k}$ that are not in the support of $\mathtt{PCode}_{n,k,t,\gamma}$ is at most $\left(e2^{\gamma-\beta}\right)^{2^{k-\gamma}} 2^n$. That is,

$$\Pr\left[U_{n,k} \notin \mathtt{PCode}_{n,k,t,\alpha}\right] \leq \left(e2^{\gamma-\beta}\right)^{2^{k-\gamma}} 2^n$$

A distribution is not in $\mathtt{PCode}_{n,k,t,\gamma}$ if there exists some center y such that there are at least $2^{-\gamma}2^k = 2^{k-\gamma}$ points within distance t of y. Fix some arbitrary y^*. The point y^* defines a set A_{y^*} of all points within distance t and note that $|A_{y^*}| = |B_t|$. We now show that the probability that values in $U_{n,k}$ has a large intersection with A_{y^*} is small.

Lemma 12. *Let n, k, a be positive integers for which $\mathsf{log}(a) < k$. Let $a^* = a/(1-a2^{-k})$. Let K be a random variable uniform among all subsets of $\{0,1\}^n$ of size 2^k. Let A be a fixed subset of size $a \cdot 2^{n-k}$. Then $\mathbb{E}[|K \cap A|] = a$ and any $\zeta > 0$,*

$$\Pr[|K \cap A| \geq a^*(1+\zeta)] \leq \left[\frac{e^\zeta}{(1+\zeta)^{1+\zeta}}\right]^{a^*}.$$

Proof. For the purposes of bookkeeping, arrange the elements of A in an arbitrary order and note that $|A| = a2^{n-k} < 2^k 2^{n-k} = 2^n$ so $A \subset \{0,1\}^n$, and let

$$X_1, \ldots, X_{a2^{n-k}}$$

be indicator random variables so that $X_i = 1$ if and only if the ith element of A lies in K. Note that for any individual i, $\Pr[X_i = 1] = a2^{n-k}/2^n = a2^{-k}$ and thus $\mathbb{E}[|K \cap A|] = \sum_i \mathbb{E}[X_i] = 2^k \mathbb{E}[X_i] = 2^k(a2^{-k}) = a$ by linearity of expectation. Observe that under any conditioning on the variables $X_1, \ldots, X_t$,

$$\Pr[X_{t+1} = 1] \leq \frac{2^k}{2^n - a2^{n-k}} = \frac{2^k}{2^n(1 - a2^{-k})}\,.$$

Let Y_i be a sequence of i.i.d. random variables (with the same index set) for which

$$\Pr[Y_i = 1] = \frac{2^k}{2^n(1 - a2^{-k})}\,.$$

It follows that the random variable $\sum_i X_i$ is stochastically dominated by the random variable $\sum_i Y_i$. Observe that $\mathbb{E}[\sum Y_i] = a^*$. Applying a standard Chernoff upper tail bound to the Y_i then yields the result. This completes the proof of Lemma 12. □

We now continue using the notation of Lemma 12, let

$$a^* = \frac{2^k|B_t|}{2^n - |B_t|} = 2^{k-\beta}.$$

Fix the value of ζ such that

$$1 + \zeta = \frac{2^{-\gamma}(2^n - |B_t|)}{|B_t|} \geq 2^{\beta-\gamma}.$$

then the probability that an entry in $U_{n,k}$ intersects with A_{y^*} in at least $2^{k-\gamma}$ places is at most

$$\begin{aligned}\Pr[|U_{n,k} \cap A_{y^*}| \geq a^*(1+\zeta)] \leq \\ \Pr[|U_{n,k} \cap A_{y^*}| \geq 2^{k-\gamma}] &\leq \left(\left(e2^{\gamma-\beta}\right)^{2^{\beta-\gamma}}\right)^{2^{k-\beta}} \\ &= \left(e2^{\gamma-\beta}\right)^{2^{k-\gamma}}\end{aligned}$$

Now we consider a union bound across all y^* which is equivalent to asking the probability that $U_{n,k}$ has fuzzy min-entropy γ. That is

$$\Pr_{U \leftarrow U_{n,k}}[\mathrm{H}^{\mathtt{fuzz}}_{t,\infty}(U) \geq \gamma] = \left(e2^{\gamma-\beta}\right)^{2^{k-\gamma}} 2^n.$$

The difference between $U_{n,k}$ and $\mathtt{PCode}_{n,k,t,\gamma}$ is exactly the above probability mass which is removed from the entries of $U_{n,k}$ that are not in $\mathtt{PCode}_{n,k,t,\gamma}$ and uniformly distributed to the entries in $\mathtt{PCode}_{n,k,t,\gamma}$. This means that

$$\Delta(U_{n,k}, \mathtt{PCode}^*_{n,k,t,\gamma}) \leq \left(e2^{\gamma-\beta}\right)^{2^{k-\gamma}} 2^n,$$

completing the proof of Lemma 7. □

3.4.2 Proof of Lemma 9

Proof of Lemma 9. Let Z and advice be defined as above. We begin by noting that

$$\mathrm{H}_\infty(W_{z,1},...,W_{z,2^k}) = \alpha.$$

It is thus, the case that

$$\tilde{\mathrm{H}}_\infty(W_{z,1},...,W_{z,2^k}|\mathsf{advice}) \geq \alpha - |\mathsf{advice}|.$$

For all values x, y,

$$\Pr[W_{z,i} = x | W_{z,j} = y] = \begin{cases} \frac{1}{2^n - 1} & x \neq y \\ 0 & x = y. \end{cases}$$

Claim 2. *One has that*

$$\mathop{\mathbb{E}}_{i=1}^{2^k}\left[\tilde{\mathrm{H}}_\infty(W_{z,i}|\mathsf{advice})\right] \geq \frac{\alpha - |\mathsf{advice}|}{2^k}.$$

Proof. It is true that $\forall w_{z,1},...,w_{z,i-1}$ that

$$\tilde{\mathrm{H}}_\infty(W_{z,i}|\mathsf{advice}, W_{z,1} = w_{z,1},...,W_{z,i-1} = w_{z,i-1}) \leq \tilde{\mathrm{H}}_\infty(W_{z,i}|\mathsf{advice}).$$

This is because conditioned on $W_{z,j} = w_{z,j}$ only removes the outcome $w_{z,j}$ from the support of $W_{z,i}$ increasing all other outcomes proportionally. We now proceed to the proof of the claim.

Suppose not, then there exists the following predictor $\mathcal{P}$ for the joint distribution $W_{z,1},...,W_{z,k}|\mathsf{advice}$:

1. For $i = 1$ to k predict $w_{z,i} \leftarrow W_{z,i}|\mathsf{advice}, W_{z,1} = w_{z,1},...,W_{z,i-1} = w_{z,i-1}$
2. Output the joint prediction $w_{z,1},...,w_{z,k}$.

Let α_i denote the values $\tilde{\mathrm{H}}_\infty(W_{z,i}|\mathsf{advice}) = \alpha_i$ for $i = 1$ to k. The probability that $\mathcal{P}$ issues a correct prediction is

$$\prod_{i=1}^{2^k} 2^{-\tilde{\mathrm{H}}_\infty(W_i|\mathsf{advice}, W_{z,1}=w_{z,1},...,W_{z,i-1}=w_{z,i-1})} \geq \prod_{i=1}^{2^k} 2^{-\tilde{\mathrm{H}}_\infty(W_i|\mathsf{advice})} = \prod_{i=1}^{2^k} 2^{-\alpha_i} = 2^{-\sum_{i=1}^{2^k}\alpha_i}.$$

Suppose that $\sum_{i=1}^{2^k}\alpha_i < \alpha - \mathsf{advice}$ then $\mathcal{P}$ correctly predicts with probability greater than $2^{-(\alpha-\mathsf{advice})}$, a contradiction. Thus, $\mathbb{E}_{1\leq i\leq k}\,\alpha_i \geq (\alpha - \mathsf{advice})/2^k$. This completes the proof of Claim 2. □

Before proceeding to the proof of Lemma 9 we need an elementary lemma:

Lemma 13. *Let $\vec{X} = (X_1, X_2, \ldots, X_{2^k})$ be random variables and let Y be a random variable arbitrarily correlated with $\vec{X}$. Suppose that $\mathbb{E}_i[\mathrm{H}_\infty(X_i|Y)] \geq \Delta$. Then*

$$\left|\left\{X_i|\tilde{\mathrm{H}}_\infty(X_i|Y) < \Delta - (k - \mathsf{log}(\nu))\right\}\right| \leq \nu.$$

Proof of Lemma 13. Let $\mathbb{E}_i[\tilde{\mathrm{H}}_\infty(X_i|Y)] = \Delta$. Then by Markov's inequality

$$\Pr_i\left[\mathop{\mathbb{E}}_y\left(\max_x \Pr[X_i = x \,|\, Y = y]\right) \geq \alpha \cdot 2^{-\Delta}\right] \leq \frac{1}{\alpha}$$

Which implies that

$$\Pr_i\left[-\mathsf{log}\left(\mathop{\mathbb{E}}_y\left(\max_x \Pr[X_i = x \,|\, Y = y]\right)\right) \leq \Delta - \mathsf{log}(\alpha)\right] \leq \frac{1}{\alpha}$$

and finally

$$\Pr_i\left[\tilde{\mathrm{H}}_\infty(X_i \,|\, Y) < \Delta - \mathsf{log}(\alpha)\right] \leq \frac{1}{\alpha}$$

The statement of the lemma follows by setting $\alpha = 2^k/\nu$. □

By Lemma 13 it is true that there exists a set $\mathcal{I} \subseteq \{1, ..., 2^k\}$ of size ν where such that for all $i \notin \{1, ..., 2^k\} \setminus \mathcal{I}$ is true that

$$\eta := \tilde{\mathrm{H}}_\infty(W_{z,i}|\mathsf{advice}) \geq \frac{\alpha - |\mathsf{advice}|}{2^k} - (k - \mathsf{log}(\nu)) .$$

Let i^* denote the index of the point that will be given to Gen that is $p \leftarrow (w_{z,i^*}, \mathsf{advice})$. We define the set $\mathcal{I}_{\mathsf{advice}} = \mathcal{I} \cup \{w_{z,i^*}\}$ where w is the point given to $\mathsf{Gen}(w, \mathsf{advice})$. Then for $i \notin \mathcal{I}_{\mathsf{advice}}$ it is true that

$$\begin{aligned} &\tilde{\mathrm{H}}_\infty(W_{z,i}|\mathsf{key} \in \mathtt{GoodKey}, p) \geq \\ &\tilde{\mathrm{H}}_\infty(W_{z,i}|\mathsf{advice}, W_{z,i^*} = w_{z,i^*}) \geq -\mathsf{log}\left(\frac{1}{2^\eta - 1}\right) \geq \eta - 1. \end{aligned}$$

We now proceed to bounding $\mathtt{Viable}(w_i, p, \mathsf{key})$. By assumption, By Lemma 8 we know that there are at most 2^μ points in $\mathtt{Viable}(w_i, p, \mathsf{key})$. Thus, for all $i \notin \mathcal{I}_{\mathsf{advice}}$

$$\begin{aligned} \mathsf{log}(\Pr[\mathtt{Viable}(w_{z,i}, p, \mathsf{key}, \mathsf{advice}) = 1]) &\leq -(\eta - 1 - \mu) \\ &= -\left(\frac{\alpha - |\mathsf{advice}|}{2^k} - 1 - \mu - (k - \mathsf{log}(\nu))\right). \end{aligned}$$

This completes the proof of Lemma 9. □

3.4.3 Proof of Lemma 11

Proof of Lemma 11. . We prove the result for an average member of Z. Consider the following distinguisher $\mathcal{D}$ for triples of the form r, p, z:

1. If $r \notin \mathsf{GoodKey}_p$ output 1,
2. If $\sum_i \mathtt{Viable}(w_{z,i}, r, p, \mathsf{advice}(z)) = 0$ output 0,
3. Else output 1.

First note that by perfect correctness it is always the case that when given key, p that $\mathcal{D}$ outputs 1. We proceed to bound the probability that $\mathcal{D}$ outputs 1 when given U_κ, p. Note that the probability that $\Pr[U_\kappa \in \mathtt{GoodKey}_p] \geq 1/2$ by the definition of $\mathtt{GoodKey}_p$.

We bound the number of parts with at least one point in viable. We begin by assuming that all points in viable are in different values r so the bound on the size of

$$\left\{ w_{z,i} \middle| \sum_{\mathsf{key} \in \mathtt{Goodkey}_p} \mathtt{Viable}(w_{z,i}, p, \mathsf{key}, \mathsf{advice}) > 0 \right\}_{i=1}^{k}$$

gives a bound on the number of nonempty parts. By Corollary 10

$$\mathop{\mathbb{E}}_{Z}\left[\sum_{\mathsf{key} \in \mathtt{Goodkey}_p} \sum_i \mathtt{Viable}(w_{z,i}, p, \mathsf{key}, \mathsf{advice}) \middle| \begin{array}{r} z \leftarrow Z \\ \mathsf{advice} \leftarrow \mathsf{Advice}(z) \\ w \leftarrow W_Z \\ (r, p) \leftarrow \mathsf{Gen}(w, \mathsf{advice}) \end{array} \right] < 2^{-\frac{\alpha - |\mathsf{advice}|}{2^k} + 1 + \mu + 2k - \mathsf{log}(\nu)} + \nu + 1.$$

Thus the fraction of non-empty parts in $\mathsf{Goodkey}_p$ on average is at most

$$2^{-\kappa - \frac{\alpha - |\mathsf{advice}|}{2^k} + 1 + \mu + 2k - \mathsf{log}(\nu)} + \frac{\nu + 1}{2^\kappa}.$$

Thus, the probability that $\mathcal{D}$ outputs 0 when given U_κ, p, z is at least $1/2 - (\epsilon_1 + \epsilon_2)$ where

$$\epsilon_1 := 2^{-\kappa - \frac{\alpha - |\mathsf{advice}|}{2^k} + 1 + \mu + 2k - \mathsf{log}(\nu)},$$
$$\epsilon_2 := \frac{\nu + 1}{2^\kappa}.$$

This completes the Proof of Lemma 11. □

4 Secure Sketches

This section creates an upper bound on the quality of efficient secure sketches. This bound considers has stronger parameters than Theorem 6 due largely to the difference between Lemmas 8 and 15.

Theorem 14. *Let $\gamma \in \mathbb{R}^+, n, \kappa, t, \ell, \gamma \in \mathbb{Z}^+$ be parameters.*

1. *The β-density is at least 1 which is satisfied as long as $t < n/2$ (see Definition 4),*
2. *Let $\nu \in \mathbb{Z}^+$ be a free parameter, and*
3. *Let $\mu = (n(1 - h_2(t/n)) + h_2(2\delta))/(1 - 2\delta)$.*

For $2^{-\tilde{m}}$ of the distributions $W \in \mathtt{PCode}^*_{n,k,t,\gamma}$ there is no $(\{0,1\}^n, W, \tilde{m}, t, \epsilon, \delta, \ell)$-secure sketch for

$$\tilde{m} \geq -\mathsf{log}(1 - \epsilon') + 1 + 2\max\left\{-\frac{\alpha - \ell}{2^k} + 1 + \mu + 2k - \mathsf{log}(\nu), \mathsf{log}(\nu + 1)\right\}.$$

where $\epsilon' = \epsilon + \left(e2^{\gamma - \beta}\right)^{2^{k-\gamma}} 2^n$.

Proof of Theorem 14. Fuller, Reyzin, and Smith [FRS20, Lemma 7.3] showed that good secure sketches are bounded in size as they imply good Shannon error correcting codes. This result holds true if one considers a secure sketch that retains smooth min-entropy with no loss in parameters because it only relies on the correctness of the secure sketch (not the security property).

Lemma 15. *Suppose $\mathcal{M}$ is $\{0,1\}^n$ with the Hamming Metric. Suppose $(\mathsf{SS}, \mathsf{Rec})$ is a $(\{0,1\}^n, \mathcal{W}, \tilde{m}, t, \epsilon_{\mathsf{SS}}, \delta)$-secure sketch, for some family $\mathcal{W}$.*

For every $v \in \mathcal{M}$ there exists a set $\mathsf{GoodSketch}_v$ where $\Pr[\mathsf{SS}(v) \in \mathsf{GoodSketch}_v] \geq 1/2$ and for any fixed SS,

$$\mu := \mathsf{log}(|\{v \in \mathcal{M} | \mathsf{SS} \in \mathsf{GoodSketch}_v\}|) \leq \frac{n - \mathsf{log}(|B_t|) + h_2(2\delta)}{1 - 2\delta} \leq \frac{n(1 - h_2(t/n)) + h_2(2\delta)}{1 - 2\delta}.$$

We present an analog of Lemma 9 adapted to the secure sketch setting. Let $\mathsf{GoodSketch}_v$ be defined as in Lemma 15. For a triple (v, ss, z) define $\mathtt{Viable}(v, ss, z) = 1$ if

1. $\Pr[\mathsf{Gen}(v, \mathsf{advice}(z)) = ss] > 0$,
2. $ss \in \mathsf{GoodSketch}_v$, and
3. $\Pr[W_z = v] > 0$.

and set $\mathtt{Viable}(v, ss, z) = 0$ otherwise.

Lemma 16. *Let Z describe a uniform sample of $U_{n,k}$. Let $\mathsf{advice} = \mathsf{Advice}(Z)$ be of length ℓ. For a particular $Z = z$ let $w_{z,1}, ..., w_{z,2^k}$ denote the points in W_Z. Let $\alpha := \mathsf{log}\left(\binom{2^n}{2^k}\right)$. Let μ be defined as in Lemma 15. For each value advice there is some set $\mathcal{I}_{\mathsf{advice}}$ of size at most $\nu + 1$, it is true for each $i \notin \mathcal{I}_{\mathsf{advice}}$ that*

$$\mathsf{log}(\Pr[\mathtt{Viable}(w_{z,i}, ss, \mathsf{advice}) = 1]) \leq -\frac{\alpha - |\mathsf{advice}|}{2^k} + 1 + \mu + k - \mathsf{log}(\nu).$$

The proof of Lemma 16 is identical to the proof of Lemma 9 and is omitted. Lemma 16 suffices to bound how many points are "viable" from the output of the secure sketch.

Corollary 17. *Let Z describe a uniform sample of $U_{n,k}$. Let $(\mathsf{Gen}, \mathsf{Rep}, \mathsf{Advice})$ be an auxiliary input fuzzy extractor. Let $\mathsf{advice} = \mathsf{Advice}(Z)$ be of length ℓ. For every $v \in \mathcal{M}$ there exists a set $\mathsf{GoodSketch}_v$ where $\Pr[\mathsf{SS}(v) \in \mathsf{GoodSketch}_v] \geq 1/2$ and for any fixed SS,*

$$\mu := \mathsf{log}(|\{v \in \mathcal{M} | \mathsf{SS} \in \mathsf{GoodSketch}_v\}|) \leq \frac{n - \mathsf{log}(|B_t|) + h_2(2\delta)}{1 - 2\delta} \leq \frac{n(1 - h_2(t/n)) + h_2(2\delta)}{1 - 2\delta}.$$

For a triple (v, ss, z) define $\mathtt{Viable}(v, ss, z) = 1$ if

1. $\Pr[\mathsf{Gen}(v, \mathsf{advice}(z)) = ss] > 0$,
2. $ss \in \mathsf{GoodSketch}_v$, *and*
3. $\Pr[W_z = v] > 0$.

and set $\mathtt{Viable}(v, ss, z) = 0$ otherwise. For a particular $Z = z$ let $w_{z,1}, ..., w_{z,2^k}$ denote the points in W_Z. Let $\alpha := \mathsf{log}\left(\binom{2^n}{2^k}\right)$. Then for each value advice there is some set $\mathcal{I}_{\mathsf{advice}}$ of size at most $\nu + 1$, then it is true for each $\forall i \notin \mathcal{I}_{\mathsf{advice}}, \forall ss$

$$\Pr_{z \leftarrow Z}[\mathtt{Viable}(w_{z,i}, ss, z) = 1] < 2^{-\frac{\alpha - |\mathsf{advice}|}{2^k} + 1 + \mu + k - \mathsf{log}(\nu)}.$$

And thus, for on average across Z, for all ss the expected number of points outside of $\mathcal{I}_{\mathsf{advice}}$ that are included in $\mathtt{Viable}$ is at most

$$\mathop{\mathbb{E}}_{z \leftarrow Z}\left[\sum_{i | w_{z,i} \notin \mathcal{I}_{\mathsf{advice}}} \mathtt{Viable}(w_{z,i}, ss, z)\right] < 2^{-\frac{\alpha - |\mathsf{advice}|}{2^k} + 1 + \mu + 2k - \mathsf{log}(\nu)}.$$

And finally, for all ss

$$\mathop{\mathbb{E}}_{z \leftarrow Z}\left[\sum_{i} \mathtt{Viable}(w_{z,i}, ss, \mathsf{advice})\right] < 2^{-\frac{\alpha - |\mathsf{advice}|}{2^k} + 1 + \mu + 2k - \mathsf{log}(\nu)} + \nu + 1.$$

The above corollary follows by combination of Lemma 15 and 16. □

Lemma 18. *Let all parameters be as in Corollary 17 with $\nu \in \mathbb{Z}^+$. Then there is no $(\{0,1\}^n, \mathcal{W}, \kappa, t, \epsilon_{\mathsf{SS}}, \delta, \ell)$-secure sketch with distributional advise (see Definition 7) if*

$$\tilde{m} > -\mathsf{log}(1 - \epsilon_{\mathsf{SS}}) + 1 + 2\max\left\{-\frac{\alpha - |\mathsf{advice}|}{2^k} + 1 + \mu + 2k - \mathsf{log}(\nu), \mathsf{log}(\nu + 1)\right\}.$$

Furthermore, there exists an algorithm $\mathcal{D}$ that always outputs 1 when given samples of the form w, ss, z that are correctly generated by the secure sketch.

We defer the proof of Lemma 18 to Section 4.1 and proceed with the proof of Theorem 14.

The main proof We now proceed to the proof of Theorem 14. Let

$$\chi := -\mathsf{log}(1 - \epsilon_{\mathsf{SS}}) + 1 + 2\max\left\{-\frac{\alpha + -|\mathsf{advice}|}{2^k} + 1 + \mu + 2k - \mathsf{log}(\nu), \mathsf{log}(\nu + 1)\right\}.$$

Restating Lemma 18 one has that

$$\tilde{\mathrm{H}}_\infty^{\epsilon_{\mathsf{SS}}}(U_{n,k} | \mathsf{SS}(U_{n,k}), Z_{U_{n,k}})) \leq \chi.$$

That is, for all A, B, C such that $\Delta((A,B,C),(U_{n,k},\mathsf{SS}(U_{n,k}),Z_{U_{n,k}})) \leq \epsilon_{\mathsf{SS}}$ it is true that $\tilde{\mathrm{H}}_\infty(A|B,C) \leq \tilde{m}$. Define

$$P_{\mathtt{PCode}^*_{n,k,t,\alpha}} \leftarrow \mathsf{SS}(\mathtt{PCode}^*_{n,k,t,\alpha}, \mathsf{advice}(Z_{\mathtt{PCode}^*_{n,k,t,\alpha}})).$$

Recall that $\Delta(U_{n,k}, \mathtt{PCode}^*_{n,k,t,\alpha}) \leq \epsilon_{\mathtt{PCode}}$ by Lemma 7 . It is thus true that

$$\tilde{\mathrm{H}}^{\epsilon_{\mathsf{SS}}-\epsilon_{\mathtt{PCode}}}_\infty(\mathtt{PCode}^*_{n,k,t,\alpha}|\mathsf{SS}(\mathtt{PCode}^*_{n,k,t,\alpha}), Z_{\mathtt{PCode}^*_{n,k,t,\alpha}}) \leq \tilde{m}.$$

Suppose not, then there exists some A, B, C where

$$\Delta((A,B,C),(\mathtt{PCode}^*_{n,k,t,\alpha},\mathsf{SS}(\mathtt{PCode}^*_{n,k,t,\alpha}),Z_{\mathtt{PCode}^*_{n,k,t,\alpha}})) \leq \epsilon_{\mathsf{SS}} - \epsilon_{\mathtt{PCode}}.$$

and $\tilde{\mathrm{H}}_\infty(A|B,C) > \chi$. Thus,

$$\begin{aligned}
&\Delta((A,B,C),(U_{n,k},\mathsf{SS}(U_{n,k}),Z_{U_{n,k}})) \\
&\quad\leq \Delta((A,B,C),((\mathtt{PCode}^*_{n,k,t,\alpha},\mathsf{SS}(\mathtt{PCode}^*_{n,k,t,\alpha}),Z_{\mathtt{PCode}^*_{n,k,t,\alpha}})) + \Delta(U_{n,k},\mathtt{PCode}^*_{n,k,t,\alpha}) \\
&\quad\leq \epsilon_{\mathsf{SS}} - \epsilon_{\mathtt{PCode}} + \epsilon_{\mathtt{PCode}} = \epsilon_{\mathsf{SS}}.
\end{aligned}$$

This contradicts the fact that $\tilde{\mathrm{H}}^{\epsilon_{\mathsf{SS}}}_\infty(U_{n,k}|\mathsf{SS}(U_{n,k}),Z_{U_{n,k}})) \leq \chi$. Finally, Theorem 14 follows by application of Lemma 5 with setting $\zeta = \chi$ and noting that $\chi \geq 1$.

4.1 Proof of Lemma 18

Proof of Lemma 18. We prove the result for an average member of Z. First note that for every $v \in \mathcal{M}$ there exists a set $\mathsf{GoodSketch}_v$ where $\Pr[\mathsf{SS}(v) \in \mathsf{GoodSketch}_v] \geq 1/2$. We first need an elementary lemma:

Lemma 19. *Let (X,Y) be a pair of random variables and, $S(X,Y)$ be a set, let f be a randomized function taking inputs on the domain of (X,Y). Then*

$$\tilde{\mathrm{H}}^{\epsilon}_\infty(X|Y, f(X,Y) \in S(X,Y)) \geq \tilde{\mathrm{H}}^{\epsilon}_\infty(X|Y) + \mathsf{log}(\Pr[f(X,Y) \in S(X,Y)])\,.$$

Proof of Lemma 19. Let X', Y' be a distribution such that $\Delta((X,Y),(X',Y')) \leq \epsilon$. By [FRS20, Lemma 7.8] for any event η

$$\tilde{\mathrm{H}}_\infty(X'|Y',\eta) \geq \tilde{\mathrm{H}}_\infty(X'|Y') + \mathsf{log}(\Pr[\eta])\,.$$

Let η denote the event that $f(X,Y) \in S(X,Y)$. The proof completes by noting that $\Delta((X,Y),(X',Y')) \leq \epsilon$ implies that

$$\Delta((X,Y,f(X,Y) \in S(X,Y)),(X',Y',f(X',Y') \in S(X',Y'))) \leq \epsilon$$

by the information processing lemma. This is turn implies that

$$\tilde{\mathrm{H}}^{\epsilon}_\infty(X|Y, f(X,Y) \in S(X,Y)) \geq \tilde{\mathrm{H}}^{\epsilon}_\infty(X|Y) + \Pr[f(X,Y) \in S(X,Y)].$$

This completes the proof of Lemma 19. □

By Lemma 19

$$\tilde{\mathrm{H}}^{\epsilon}_\infty(W|\mathsf{SS}(W)) \leq \tilde{\mathrm{H}}^{\epsilon}_\infty(W|\mathsf{SS}(W), \mathsf{SS}(W) \in \mathsf{GoodSketch}_W) + 1.$$

We now restrict our attention to the case when $\mathsf{SS}(w) \in \mathsf{GoodSketch}_w$. Let X', Y' be distributions be an event where $\Delta((W,\mathsf{SS}(W)),(X',Y')) \leq \epsilon$. Note that

$$\Pr[\mathtt{Viable}(W,\mathsf{SS}(W),Z) = 1 | \mathsf{SS}_W \in \mathsf{GoodSketch}_W] = 1.$$

Thus, it must be the case that

$$\Pr[\texttt{Viable}(X', Y', Z) = 1] \geq 1 - \epsilon.$$

By the definition of `Viable`, the support of X' must be drawn from points in W_Z. For any fixed value of $y \in Y$ by Corollary 17, it is true that

$$\mathop{\mathbb{E}}_{z \leftarrow Z}\left[\sum_i \texttt{Viable}(w_{z,i}, y', \mathsf{advice})\right] < 2^{-\frac{\alpha - |\mathsf{advice}|}{2^k} + 1 + \mu + 2k - \mathsf{log}(\nu)} + \nu + 1.$$

One has,

$$\begin{aligned} 2^{-\tilde{\mathrm{H}}_\infty(X'|Y')} &\geq \Pr[X' \in W_Z] 2^{-\tilde{\mathrm{H}}_\infty(X'|Y', X' \in W_Z)} + \Pr[X' \notin W_Z] 2^{-\tilde{\mathrm{H}}_\infty(X'|Y', X' \notin W_Z)} \\ &\geq (1 - \epsilon) 2^{-\tilde{\mathrm{H}}_\infty(X'|Y', X' \in W_Z)} \end{aligned}$$

And thus,

$$\tilde{\mathrm{H}}_\infty(X'|Y') \leq -\mathsf{log}(1 - \epsilon_{\mathsf{SS}}) + \tilde{\mathrm{H}}_\infty(X'|Y', X' \in W_Z).$$

The min-entropy of $X'|Y'$ is maximized by considering the uniform distribution over such points.

$$\begin{aligned} \tilde{\mathrm{H}}_\infty(X'|Y', X' \in W_Z) &\leq \mathsf{log}\Big(2^{-\frac{\alpha - |\mathsf{advice}|}{2^k} + 1 + \mu + 2k - \mathsf{log}(\nu)} + \nu + 1\Big) \\ &\leq 2 \max\left\{-\frac{\alpha - |\mathsf{advice}|}{2^k} + 1 + \mu + 2k - \mathsf{log}(\nu), \mathsf{log}(\nu + 1)\right\}. \end{aligned}$$

This implies that

$$\tilde{\mathrm{H}}^\epsilon_\infty(W|\mathsf{SS}(W)) \leq -\mathsf{log}(1 - \epsilon_{\mathsf{SS}}) + 1 + 2 \max\left\{-\frac{\alpha - |\mathsf{advice}|}{2^k} + 1 + \mu + 2k - \mathsf{log}(\nu), \mathsf{log}(\nu + 1)\right\}.$$

This completes the Proof of Lemma 18. □

4.2 Analysis of parameters

We assume that $\epsilon \leq 1/4$ and $\delta < 1/4$. As before for $\left(e 2^{\gamma - \beta}\right)^{2^{k-\gamma}} 2^n$ to be negligible it suffices that

Condition 1 That $\gamma \leq \beta - \mathsf{log}(2e)$.[5]

Condition 2 Let $0 < c_k < 1$ be some arbitrary constant and suppose that $k = \gamma + c_k n$ which implies that $k \geq \gamma + \mathsf{log}(n + \omega(\mathsf{log}(n)))$.

These two conditions imply that $\epsilon' \leq 1/2$ and $-\mathsf{log}(1 - \epsilon') \leq 1$.

Condition 3 That $\nu = 1$.

Define

$$\chi := -\frac{\alpha - \ell}{2^k} + 1 + \mu + 2k - \mathsf{log}(\nu) = -\frac{\alpha - |\mathsf{advice}|}{2^k} + 1 + \mu + 2k$$

We now turn to our analysis of χ. Recall that $(n/k)^k \leq \binom{n}{k} < ((ne)/k)^k$. Recalling parameters:

$$\begin{aligned} \mu &\leq \frac{(n(1 - h_2(t/n)) + h_2(2\delta))}{(2\delta)}, \\ \alpha &= \mathsf{log}\left(\binom{2^n}{2^k}\right) \geq \mathsf{log}\left(2^{n 2^k} / 2^{k 2^k}\right) = (n - k) 2^k, \end{aligned}$$

[5] As in Section 3.3 the additional constraint that $\gamma \leq \beta - \mathsf{log}(2e)$ imposes an additive $\mathsf{log}(2e)$ impact on the maximal fuzzy min-entropy that can be supported.

This implies that

$$\begin{aligned}\chi &= -\frac{\alpha-\ell-k}{2^k}+\mu+2k+1\\ &\le -\frac{\alpha+\mathsf{log}(\nu)-\ell-k}{2^k}+\frac{n(1-h_2(t/n))+h_2(2\delta)}{1-2\delta}+2k+1,\\ &\le -\frac{(n-k)2^k+\mathsf{log}(\nu)-\ell-k}{2^k}+\frac{n(1-h_2(t/n))+h_2(2\delta)}{1-2\delta}+2k+1,\\ &\le -\frac{(n-3k)2^k-\ell-k}{2^k}+\frac{n(1-h_2(t/n))+h_2(2\delta)}{1-2\delta}+1.\end{aligned}$$

We consider two settings for δ one when $\delta < 1/4$ and another when $\delta = 0$.

Constant error, $\delta < 1/4$ As long as for constants c_k, c_ℓ one has

$$\begin{aligned}&\ell \le 3c_\ell n 2^k,\\ &\delta < 1/4,\\ 0 \le \frac{\gamma}{n} &\le \min\left\{(1-h_2(t/n))+\frac{\mathsf{log}(n)+1-2\mathsf{log}(2e)}{2n}, \frac{2}{3}h_2(t/n)-\frac{1}{3}-\frac{4c_k+c_\ell}{3}-\frac{2}{3n}\right\}.\end{aligned}$$

then

$$\begin{aligned}\chi &\le -\frac{(n-3k)2^k-\ell-k}{2^k}+\frac{n(1-h_2(t/n))+h_2(2\delta)}{1-2\delta}+1\\ &\le -\frac{(n-3k)2^k-\ell-k}{2^k}+\frac{n(1-h_2(t/n))+h_2(2\delta)}{1-2\delta}+1\\ &\le -\frac{(n-3k)2^k-\ell-k}{2^k}+2n(1-h_2(t/n))+2\\ &\le -(n-(4c_k+c_\ell)n-3\gamma)+2n(1-h_2(t/n))+2\\ &\le -n+(4c_k+c_\ell)n+3\gamma+2n(1-h_2(t/n))+2\\ &\le n+(4c_k+c_\ell)n+3\gamma-2nh_2(t/n))+2 \le 0\end{aligned}$$

then $\tilde{m} \le 2+2\max\{\chi, \mathsf{log}(2)\} \le 4$ which implies that $1/16$ of the distributions have no secure sketch.

No error, $\delta = 0$ When $\delta = 0$ one has

$$\begin{aligned}&\ell \le 3c_\ell n 2^k,\\ &\delta < 1/4,\\ 0 \le \frac{\gamma}{n} &\le \min\left\{(1-h_2(t/n))+\frac{\mathsf{log}(n)+1-2\mathsf{log}(2e)}{2n}, \frac{1}{3}h_2(t/n)-\frac{4c_k+c_\ell}{3}-\frac{2}{3n}\right\}.\end{aligned}$$

yielding $\tilde{m} \le 4$ which implies that $1/16$ of the distributions have no secure sketch.

Acknowledgements

L.D. is supported by the Giolas Harriott Fellowship. A.R. is supported by a research grant from IOG and NSF grant #1801487; B.F. is supported by NSF Grants #2232813 and #2141033 and the Office of Naval Research.

References

[ABC+18] Quentin Alamélou, Paul-Edmond Berthier, Chloé Cachet, Stéphane Cauchie, Benjamin Fuller, Philippe Gaborit, and Sailesh Simhadri. Pseudoentropic isometries: A new framework for fuzzy extractor reusability. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, pages 673–684, 2018.

[ACEK17] Daniel Apon, Chongwon Cho, Karim Eldefrawy, and Jonathan Katz. Efficient, reusable fuzzy extractors from lwe. In *International Conference on Cyber Security Cryptography and Machine Learning*, pages 1–18. Springer, 2017.

[Ash12] Robert B Ash. *Information theory*. Courier Corporation, 2012.

[BBC+14] Boaz Barak, Nir Bitansky, Ran Canetti, Yael Tauman Kalai, Omer Paneth, and Amit Sahai. Obfuscation for evasive functions. In *Theory of Cryptography Conference*, pages 26–51. Springer, 2014.

[BBR88] Charles H Bennett, Gilles Brassard, and Jean-Marc Robert. Privacy amplification by public discussion. *SIAM journal on Computing*, 17(2):210–229, 1988.

[BCKP14] Nir Bitansky, Ran Canetti, Yael Tauman Kalai, and Omer Paneth. On virtual grey box obfuscation for general circuits. In *Advances in Cryptology - CRYPTO 2014*, 2014.

[BCKP17] Nir Bitansky, Ran Canetti, Yael Tauman Kalai, and Omer Paneth. On virtual grey box obfuscation for general circuits. *Algorithmica*, 79(4):1014–1051, 2017.

[BDK+11] Boaz Barak, Yevgeniy Dodis, Hugo Krawczyk, Olivier Pereira, Krzysztof Pietrzak, François-Xavier Standaert, and Yu Yu. Leftover hash lemma, revisited. In *Annual Cryptology Conference*, pages 1–20. Springer, 2011.

[CFP+21] Ran Canetti, Benjamin Fuller, Omer Paneth, Leonid Reyzin, and Adam Smith. Reusable fuzzy extractors for low-entropy distributions. *Journal of Cryptology*, 34(1):1–33, 2021.

[CW77] J Lawrence Carter and Mark N Wegman. Universal classes of hash functions. In *Proceedings of the ninth annual ACM symposium on Theory of computing*, pages 106–112, 1977.

[Dau04] John Daugman. How iris recognition works. *Circuits and Systems for Video Technology, IEEE Transactions on*, 14(1):21 – 30, January 2004.

[DFR21] Luke Demarest, Benjamin Fuller, and Alexander Russell. Code offset in the exponent. In *2nd Conference on Information-Theoretic Cryptography*, 2021.

[DORS08] Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin, and Adam Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM journal on computing*, 38(1):97–139, 2008.

[FMR20] Benjamin Fuller, Xianrui Meng, and Leonid Reyzin. Computational fuzzy extractors. *Information and Computation*, 275:104602, 2020.

[FP19] Benjamin Fuller and Lowen Peng. Continuous-source fuzzy extractors: source uncertainty and insecurity. In *2019 IEEE International Symposium on Information Theory (ISIT)*, pages 2952–2956. IEEE, 2019.

[FRS16] Benjamin Fuller, Leonid Reyzin, and Adam Smith. When are fuzzy extractors possible? In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 277–306. Springer, 2016.

[FRS20] Benjamin Fuller, Leonid Reyzin, and Adam Smith. When are fuzzy extractors possible? *IEEE Transactions on Information Theory*, 66(8):5282–5298, 2020.

[GZ19] Steven D Galbraith and Lukas Zobernig. Obfuscated fuzzy hamming distance and conjunctions from subset product problems. In *Theory of Cryptography Conference*, pages 81–110. Springer, 2019.

[Har66] Lawrence H Harper. Optimal numberings and isoperimetric problems on graphs. *Journal of Combinatorial Theory*, 1(3):385–393, 1966.

[HILL93] Johan Håstad, Russell Impagliazzo, Leonid A Levin, and Michael Luby. Construction of a pseudo-random generator from any one-way function. In *SIAM Journal on Computing*. Citeseer, 1993.

[HTW14] Masahito Hayashi, Himanshu Tyagi, and Shun Watanabe. Secret key agreement: General capacity and second-order asymptotics. In *2014 IEEE International Symposium on Information Theory*, pages 1136–1140. IEEE, 2014.

[HTW16] Masahito Hayashi, Himanshu Tyagi, and Shun Watanabe. Secret key agreement: General capacity and second-order asymptotics. *IEEE Transactions on Information Theory*, 62(7):3796–3810, 2016.

[LA18] Cheuk Ting Li and Venkat Anantharam. One-shot variable-length secret key agreement approaching mutual information. *CoRR*, abs/1809.01793, 2018.

[NZ93] Noam Nisan and David Zuckerman. Randomness is linear in space. *Journal of Computer and System Sciences*, pages 43–52, 1993.

[RW05] Renato Renner and Stefan Wolf. Simple and tight bounds for information reconciliation and privacy amplification. In *International conference on the theory and application of cryptology and information security*, pages 199–216. Springer, 2005.

[SSF19] Sailesh Simhadri, James Steel, and Benjamin Fuller. Cryptographic authentication from the iris. In *International Conference on Information Security*, pages 465–485. Springer, 2019.

[ST09] Boris Skoric and Pim Tuyls. An efficient fuzzy extractor for limited noise. *Cryptology ePrint Archive*, 2009.

[TG04] Pim Tuyls and Jasper Goseling. Capacity and examples of template-protecting biometric authentication systems. In *International Workshop on Biometric Authentication*, pages 158–170. Springer, 2004.

[TVW18] Himanshu Tyagi, Pramod Viswanath, and Shun Watanabe. Interactive communication for data exchange. *IEEE Trans. Information Theory*, 64(1):26–37, 2018.

[TW17] Himanshu Tyagi and Shun Watanabe. Universal multiparty data exchange and secret key agreement. *IEEE Transactions on Information Theory*, 63(7):4057–4074, 2017.

[WCD+17] Joanne Woodage, Rahul Chatterjee, Yevgeniy Dodis, Ari Juels, and Thomas Ristenpart. A new distribution-sensitive secure sketch and popularity-proportional hashing. In *Advances in Cryptology – CRYPTO*, pages 682–710. Springer, 2017.

[WL18] Yunhua Wen and Shengli Liu. Robustly reusable fuzzy extractor from standard assumptions. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 459–489. Springer, 2018.

[WLG19] Yunhua Wen, Shengli Liu, and Dawu Gu. Generic constructions of robustly reusable fuzzy extractor. In *IACR International Workshop on Public Key Cryptography*, pages 349–378. Springer, 2019.