Pseudorandomness Against Mean and Variance Bounded Attackers

Maciej Skorski
Austria
maciej.skorski@gmail.com

Abstract

The recent progress in key derivation (Barak at al. CRYPTO'11, Dodis Yu TCC'2013) introduced the concept of constrained profiles for attackers advantage, recognizing that security bounds can be significantly improved (alternatively: lots of randomness can be saved) when the advantage, as the function of the key, is bounded in mean or variance. This paper studies *minimal requirements for keys* to achieve security under such restricted attackers.

We frame the problem as characterizing *pseudorandomness against constrained distinguishers* and show that minimal assumptions are respectively (a) high smooth min-entropy and (b) high smooth collision entropy. This matches the (folklore extension of) assumptions of previous works.

Besides providing lower bounds, we offer more insights into this key derivation problem and elegant proof techniques of geometric flavor.

2012 ACM Subject Classification Security and privacy→Cryptography→Information-theoretic techniques

Keywords and phrases key derivation, cryptography with weak keys, pseudorandomness

1 Introduction

1.1 Security games under weak keys

Security of many cryptographic objects is defined by *security games* where an attacker A (limited by some resources) interacts with the challenger C (defined depending on the application) and this interaction eventually determines if A has won the game or not; here both A and C are probabilistic. Additional randomness $r \in \{0,1\}^n$ is usually required by $\mathsf{C} = \mathsf{C}(r)$ to build the challenge task and fit its hardness to security needs; this randomness is referred to as the *key*[1]. Now it makes sense to speak about the *winning probability* $\Pr[\mathsf{A} \text{ wins with } \mathsf{C}(r)]$ and the *advantage* conditioned on the key being r

$$\mathsf{Adv}^{\mathsf{A}}(r) = \Pr[\mathsf{A} \text{ wins with } \mathsf{C}(r)] - c \tag{1}$$

where c corresponds to the "trivial" winning probability and equals $c = \frac{1}{2}$ for bit-guessing games (e.g. encryption schemes) and $c = 0$ for so called unpredictability (search) games where the challenge is to come up with a long bit string (e.g. one-way functions or message-authentication codes). For good security the advantage should be small when averaged over the key distribution R

$$\mathbb{E}_{r\sim R}\mathsf{Adv}^{\mathsf{A}}(r) \leqslant \epsilon, \tag{2}$$

this however depends on the quality of randomness R. In the ideal setup R is the uniform distribution over n-bit strings U, for appropriate n. However, uniform randomness is rarely

[1] For example, for a one-way function r sampled from $\{0,1\}^n$ and the challenge is to find the preimage of $f(r)$. For ind-cpa secure encryption r is the secret key for encryption, retained by the challenger (which makes encryption calls randomized).

available in practice and needs to be extracted from *imperfect but somewhat random sources*. Extraction of nearly uniform bit strings is possible but wastes lots of randomness, which is a major drawback for entropy-limited settings like biometrics. Interestingly, in past years, research on key derivation originated by Barak at al. [1] and finalized by Dodis at al. [3, 2] has shown that several crypto applications tolerate "weak" keys, that is distributions R with *sufficiently small entropy deficiency* (e.g. $n = 128$ and entropy bigger than $k = 120$). The technical argument, quite simple and elegant, establishes first the inequalities

$$\mathbb{E}_{r\sim R}\mathsf{D}(r) \leqslant \mathbb{E}_{r\sim U}\left[\mathsf{D}(r)\right]\cdot 2^{n-\mathbf{H}_\infty(R)}, \quad \text{when } \mathsf{D}(\cdot)\geqslant 0 \tag{3}$$

$$\mathbb{E}_{r\sim R}\mathsf{D}(r) \leqslant \sqrt{\mathbb{Var}_{r\sim U}\left[\mathsf{D}(r))\right]}\cdot\sqrt{2^{n-\mathbf{H}_2(R)}} \tag{4}$$

where $\mathsf{D}(r) = \mathsf{Adv}^{\mathsf{A}}(r)$ is the advantage profile, $\mathbf{H}_\infty(R) = \min_r \log\frac{1}{\Pr[R=r]}$ is the min-entropy (basic notion for cryptography) and $\mathbf{H}_2(R) = -\log\sum_r \Pr[R=r]^2$ is the Renyi entropy [5] of order 2 (less restrictive). The advantage profile is usually *not known explicitly* (complicated dependency on r). Nevertheless, we can constrain and control it effectively[1, 3]:

(a) for unpredictability applications, the *first advantage moment* $\mathbb{E}_{r\sim U}\left[\mathsf{D}(r)\right]$ is small. Then Equation (3) applies.

(b) for many indistinguishability applications, so called "square-friendly" (for example weak PRFs, CPA and CCA-secure encryption) *the advantage variance* $\mathbb{Var}_{r\sim U}\left[\mathsf{D}(r)\right]$ is small. Then Equation (4) applies.

the first observation follows directly from security assumptions; the second one applies to security games which, roughly speaking, allow a legitimate adversary to play "double-run" (see [3] for a discussion).

1.2 Problem Statement

We are interested in further relaxing the notion of the *weak key*, which can be stated as

> **Problem**: what are *minimal* requirements for the key R so that we have security almost as for the ideal key
>
> $$\mathbb{E}_{r\sim R}\mathsf{D}(r) \approx \mathbb{E}_{r\sim U}\mathsf{D}(r)$$
>
> against mean-bounded or variance-bounded advantage profiles D?

As discussed, previous works obtained good security assuming high entropy (Equations (3) and (4)). We discuss complementary optimal (up to constant factors) characterizations of weak keys.

1.3 Preliminaries

Unless said otherwise, all distinguishers and measures are defined on the key space $\{0,1\}^n$; the uniform distribution is denoted by U.

It will be convenient to frame our problem using the notion of indistinguishability. We say that X and Y are $(\mathcal{D},\epsilon)$-close (indistinguishable) denoted by $X \approx^{\mathcal{D},\epsilon} Y$ when $|\mathbb{E}_{r\sim X}\mathsf{D}(r) - \mathbb{E}_{r\sim Y}\mathsf{D}(r)| \leqslant \epsilon$ for all $\mathsf{D}\in\mathcal{D}$. When $X \approx^{\mathcal{D},\epsilon} U$ we say that X is $(\mathcal{D},\epsilon)$-pseudorandom.

The ℓ_p-distance, $1 \leqslant p < \infty$ of two measures Z_1, Z_2 is defined by $d_p(Z_1,Z_2) = \left(\sum_r |Z_1(r) - Z_2(r)|^p\right)^{1/p}$ and $d_\infty(Z_1,Z_2) = \max_r |Z_1(r) - Z_2(r)|$. When $d_i \leqslant \epsilon$ for $i \in \{1,2,\infty\}$ we say that Z_1 and Z_2 are ϵ-close in d_i. Similarly, when $d_i \geqslant \epsilon$ for $i\in\{1,2,\infty\}$ we say that Z_1 and Z_2 are ϵ-far in d_i.

The ϵ-smooth min-entropy [4] of (probabilistic measure) X is said to be at least k if $\mathbf{H}_\infty(X') \geqslant k$ for some X' which is 2ϵ-close[2] in d_1 to X. The ϵ-smooth collision entropy of X is said to be at least k if $\mathbf{H}_2(X') \geqslant k$ for some X' which is 2ϵ-close in d_1 to X.

When r is sampled from the uniform distribution we denote for shortness $\mathbb{E}\mathsf{D} = \mathbb{E}_r\mathsf{D}(r)$ and $\mathbb{V}\mathrm{ar}\mathsf{D} = \mathbb{V}\mathrm{ar}_r\mathsf{D}(r)$. We use $\mathsf{clip}_{[a,b]}(x) = \max(\min(x,b),a)$ to denote the clipping operation.

2 Our Contribution

2.1 Man Result: Pseudorandom Keys

We start with the answer to the posted question.

▶ Corollary 1 (Optimal keys for unpredictability applications). Let $2^{-n} < \sigma < \frac{1}{2}$ and

$$\mathcal{D} = \{\mathsf{D} : \mathsf{D}(r) \in [0,1] \text{ for all } r \text{ and } \mathbb{E}\mathsf{D} \leqslant \sigma\}$$

Then

$$X \approx^{\mathcal{D},\epsilon} U$$

if and only if

$$\mathbf{H}_\infty^{\epsilon'}(X) \geqslant n - \log(1 + O(\epsilon/\sigma)), \quad \epsilon' = O(\epsilon). \tag{5}$$

The proof is given in Appendix A.3.

▶ Corollary 2 (Optimal keys for indistingishability applications). Let $2^{-n} < \sigma < \frac{1}{2}$ and

$$\mathcal{D} = \{\mathsf{D} : \mathsf{D}(r) \in [-0.5, 0.5] \text{ for all } r \text{ and } \mathbb{V}\mathrm{ar}\mathsf{D} \leqslant \sigma\}$$

Then

$$X \approx^{\mathcal{D},\epsilon} U$$

if and only if

$$\mathbf{H}_2^{\epsilon'}(X) \geqslant n - \log(1 + O(\epsilon^2/\sigma)), \quad \epsilon' = O(\epsilon). \tag{6}$$

We give the proof in Appendix A.5. In Table 1 we compare our results with previous works. Since Equations (3) and (4) give multiplicative errors w.r.t. the uniform key, for additive error we need to adapt arguments from [1, 3] bounds (see "sufficient" parts of the proofs.

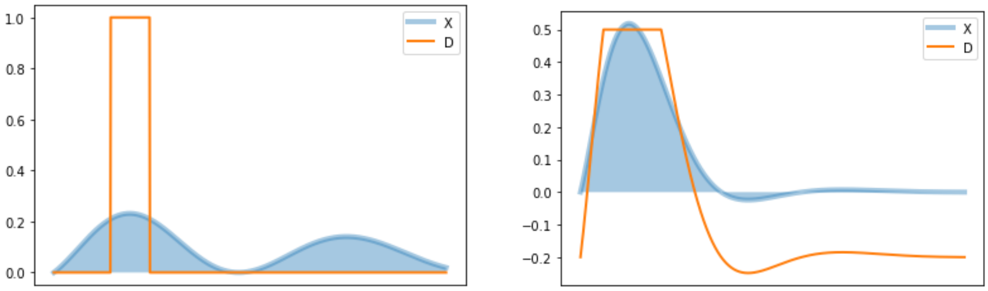
application	sufficient condition (adapted [1, 3])	optimal condition (**this paper**)
unpredictability	$\mathbf{H}_\infty(X) \geqslant n - \log(1 + O(\epsilon/\sigma))$	$\mathbf{H}_\infty^{O(\epsilon)}(X) \geqslant n - \log(1 + O(\epsilon/\sigma))$
indistinguishability	$\mathbf{H}_2(X) \geqslant n - \log(1 + O(\epsilon^2/\sigma))$	$\mathbf{H}_2^{O(\epsilon)}(X) \geqslant n - \log(1 + O(\epsilon^2/\sigma))$

Table 1 Our results vs previous works. Conditions for the key X to achieve a gap of at most ϵ in the advantage, with respect to the uniform key. Distinguishers D are constrained by $\mathbb{E}\mathsf{D} \leqslant \sigma$, $\mathsf{D} \in [0,1]$ for unpredictability and $\mathbb{V}\mathrm{ar}\mathsf{D} \leqslant \sigma$, $\mathsf{D} \in [-0.5, 0.5]$ for indistinguishability.

[2] In cryptography d_1 is usually normalized by $\frac{1}{2}$, so called statistical distance, hence the term 2ϵ.

2.2 Best Advantage Profiles for Attackers

An important part of our analysis (which we state as the fact of independent interest) is a characterization of *theoretically optimal advantage profiles* under a given key (measure) X, for mean and variance-bounded attackers (corresponding to Equation (3) and Equation (4)). Their shapes are related to the shape of the key distribution as illustrated in Figure 1 below. The importance and usefulness is the elegant *geometrical relation between shapes* of optimal attackers and keys: the constraints on (optimal) attackers imply constraints on keys. Based on this, we will later obtain claimed characterizations (minimal requirements) for keys. Detailed statements are given in the lemmas below.



(a) Mean-bounded attackers. The optimal profile is the indicator of top heaviest weights Lemma 1).

(b) Variance-bounded attackers. The optimal profile is a clipped linear transformation of the pmf (see Lemma 2).

Figure 1 Optimal advantage profiles.

▶ Lemma 1 (Explicit best mean-bounded distinguisher). For any *non-negative* measure X the maximum advantage

$$\max_{\mathsf{D}} \sum_r X(r)\mathsf{D}(r)$$

over $[0,1]$-valued distinguishers D with bounded mean $\mathbb{E}\mathsf{D} \leqslant \sigma$ is achieved for D such that $\mathsf{D}(r) = 1$ when $X(r)$ is within top $\lfloor 2^n\sigma \rfloor$ values of $X(\cdot)$, and $\mathsf{D}(r) = 2^n\sigma - \lfloor 2^n\sigma \rfloor$ if $X(r)$ is the $\lfloor 2^n\sigma \rfloor + 1$-th biggest value of $X(\cdot)$ and $\mathsf{D}(r) = 0$ otherwise.

Although this claim is intuitive, we give the formal proof in Appendix A.1.

▶ Lemma 2 (Explicit best variance-bounded distinguisher). For any *real* measure X, and any[3] interval $[q_0, q_1]$, the maximum advantage

$$\max_{\mathsf{D}} \sum_r X(r)\mathsf{D}(r)$$

over $[q_0, q_1]$-valued distinguishers D with bounded variance $\mathbb{V}\mathrm{ar}\mathsf{D} \leqslant \sigma$ is achieved for

$$\mathsf{D}(r) = \mathsf{clip}_{[q_1,q_2]}(X(r)/b + a)$$

with some constant a, b. Moreover, if $\sum_r X(r) = 0$ then

- we can assume that $\sum_r \mathsf{D}(r) = 0$ and $b > 0$.

[3] We require $q_0 < q_1$.

- the optimal solution satisfies $\mathbb{V}\mathrm{ar}\,\mathsf{D} = \sigma$, or it is of the simpler form $\mathsf{D}(r) = q_0$ when $X(r) < 0$ and $\mathsf{D}(r) = q_1$ when $X(r) > 0$ and then $\sum_r X(r)\mathsf{D}(r) = \frac{q_1 - q_0}{2}\sum_r |X(r)|$.

The proof follows by standard convex optimization tools and is given in Appendix A.2. We will apply this result for indistinguishability games with $[q_0, q_1] = [-0.5, 0.5]$.

2.3 Comparable Security ⇔ Similar Key Shapes

One requires a good key to offer "almost same" security as the ideal (uniform) key. In this work we solve a slightly more general problem:

> If two keys guarantee similar security, how much are they similar?

The important conclusion is that for similar level of security (under mean or variance-bounded attackers) the keys must have "similar" shapes. The results are derived from characterizations of optimal advantage profiles (discussed previously) in the following manner: (a) from all (constrained) profiles we choose the "extreme" attacker who achieves the biggest gap in security (b) by our characterizations its shape is explicitly related to the key distribution, (c) this eventually implies constraints on the key distribution itself. The precise meaning of this "similarity" is explained by the theorems below.

▶ **Theorem 1** (Secure keys for mean-bounded distiguishers). *Suppose that two key distributions X and Y give "comparable security", namely for the class $\mathcal{D}$ of all $[0,1]$-valued distinguishers D with bounded mean $\mathbb{E}\mathsf{D} \leqslant \sigma$ it holds that*

$$X \approx^{\mathcal{D},\epsilon} Y \tag{7}$$

Then for any subset $\mathcal{S}$ of at most $2^n\sigma$ elements, X and Y on $\mathcal{S}$ are $\epsilon' \leqslant 2\epsilon$ close in ℓ_1-norm. Conversely, if for any subset $\mathcal{S}$ of at most $2^n\sigma$ elements, $\sigma > 2^{-n}$, we have that X and Y on $\mathcal{S}$ are ϵ'-close in ℓ_1-norm then Equation (7) holds true with $\epsilon \leqslant 2\epsilon'$.

Note that the statement can be simplified slightly, if we take $\mathcal{S}$ to be the set of keys r corresponding to the $2^n\sigma$-top values of $|X(r) - Y(r)|$. The claim is then illustrated in Figure 2. This theorem implies

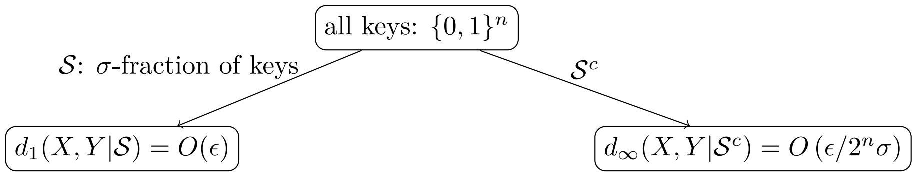

all keys: $\{0,1\}^n$
$\mathcal{S}$: σ-fraction of keys
$\mathcal{S}^c$
$d_1(X,Y|\mathcal{S}) = O(\epsilon)$
$d_\infty(X,Y|\mathcal{S}^c) = O\left(\epsilon/2^n\sigma\right)$

Figure 2 Illustration for Theorem 1.

▶ **Theorem 2** (Optimal characterization of keys secure under variance-bounded distinguishers). *Suppose that two distributions X and Y give "comparable security", namely*

$$X \approx^{\mathcal{D},\epsilon} Y \tag{8}$$

where $\mathcal{D}$ contains all $[-0.5, 0.5]$-valued distinguishers D with bounded variance $\max_{\mathsf{D}} \mathrm{Var}(\mathsf{D}) = \sigma$. Then there exists a subset of keys $\mathcal{S} \subset \mathcal{W}$ such that

- *X and Y on $\mathcal{S}$ are $\epsilon' = O(\epsilon)$-close in the ℓ_1-norm*
- *X and Y on $\mathcal{S}^c$ are $\epsilon'' = O(\epsilon/\sqrt{2^n\sigma})$-close in the ℓ_2-norm*

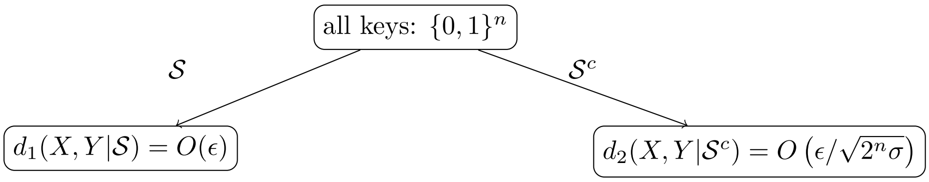

all keys: $\{0,1\}^n$
$\mathcal{S}$
$\mathcal{S}^c$
$d_1(X,Y|\mathcal{S}) = O(\epsilon)$
$d_2(X,Y|\mathcal{S}^c) = O\left(\epsilon/\sqrt{2^n\sigma}\right)$

Figure 3 Illustration for Theorem 2.

Conversely, if on some subset $\mathcal{S}$ the ℓ_1-distance is ϵ' and on the complement $\mathcal{S}^c$ the ℓ_2-distance equals ϵ'' then Equation (8) holds with

$$\epsilon = \epsilon' + \sqrt{2^n\sigma\epsilon''}$$

for every distinguisher with variance at most σ. In particular if X and Y satisfy the two conditions above then the bound in Equation (8) becomes $O(\epsilon)$.

This proof, among our results, is most challenging and is included in Section 3; what makes it complicated is the clipping transform. The theorem is illustrated in Figure 3. The result implies .

▶ Corollary 3 (Optimal keys for indistingishability applications). Suppose that $2^{-n} < \sigma < \frac{1}{2}$. The sufficient and necessary condition for a key distribution X to satisfy

$$|\mathbb{E}_{r\sim X}\mathsf{D}(r) - \mathbb{E}_{r\sim U_n}\mathsf{D}(r)| \leqslant \epsilon$$

for all D such that $\mathsf{D} \in [-0.5, 0.5]$ and $\mathbb{V}\mathrm{ar}\mathsf{D} \leqslant \sigma$, is

$$\mathbf{H}_2^{\epsilon'}(X) \geqslant n - \log(1 + O(\epsilon^2/\sigma)), \quad \epsilon' = O(\epsilon). \tag{9}$$

3 Proof of Theorem 2

Here we consider the necessary part, as the sufficient part follows easily by the Cauchy-Schwarz inequality (we skip the proof).

If X and Y are $O(\epsilon)$-close in ℓ_1 then we can just take $\mathcal{S} = \{0,1\}^n$. From now on, we therefore assume this is not the case. Define $\mathcal{W} = \{0,1\}^n$ as we will be working on several subsets of $\{0,1\}^n$. Also suppose that the range is $[-1,1]$ for the sake of cleaner calculations (the true range is $[-0.5, 0.5]$ and the results can be transformed by scalling). Consider

$$\text{maximize} \quad \sum_r \mathsf{D}(r)(X(r) - Y(r)) \tag{10}$$
$$\text{s.t.} \quad \begin{cases} \mathbb{V}\mathrm{ar}\mathsf{D} \leqslant \sigma^2 \\ \mathsf{D} \in [-1,1] \end{cases}$$

By Lemma 2 applied to $X(r) := X(r) - Y(r)$ (note that $\sum_r (X(r) - Y(r)) = 0$ as X, Y are probabilities) this is equivalent to

$$\text{maximize} \quad \mathsf{D} \cdot (X - Y) \tag{11}$$
$$\begin{cases} \dfrac{1}{|\mathcal{W}|}\displaystyle\sum_r \mathsf{D}(r)^2 \leqslant \sigma \\ \displaystyle\sum_r \mathsf{D}(r) = 0 \\ \mathsf{D} \in [-1,1] \end{cases}$$

with the optimal solution given by

$$\mathsf{D}^*(r) = \mathsf{clip}\left(\frac{X(r)-Y(r)}{b} + a\right). \tag{12}$$

We can also assume that

$$\mathbb{Var}\,\mathsf{D} = \sigma \tag{13}$$

as otherwise Lemma 2 implies that X and Y are $O(\epsilon)$-close.

3.1 Bounding the clipped set

Consider now the optimal solution D^*. Let $\mathcal{W}^+ = \{w : \mathsf{D}^*(r) = 1\}$. We have $\sum_r(\mathsf{D}^*(r))^2 \leqslant |\mathcal{W}|\sigma$ by Equation (11), therefore in particular

$$|\mathcal{W}^+| = \sum_{r\in\mathcal{W}^+}(\mathsf{D}^*(r))^2 \leqslant \sum_{r\in\mathcal{W}}(\mathsf{D}^*(r))^2 \leqslant |\mathcal{W}|\sigma. \tag{14}$$

In the same way, defining $\mathcal{W}^- = \{w : \mathsf{D}^*(r) = -1\}$ we obtain

$$|\mathcal{W}^-| = \sum_{r\in\mathcal{W}^-}(\mathsf{D}^*(r))^2 \leqslant \sum_{r\in\mathcal{W}}(\mathsf{D}^*(r))^2 \leqslant |\mathcal{W}|\sigma. \tag{15}$$

This justifies the claim that we clip only at a small fraction of the domain.

3.2 Divergence on the clipped set

Consider the following distinguisher

$$\mathsf{D}(r) = \mathbf{1}_{\mathcal{W}^+}(r) - \frac{|\mathcal{W}^+|}{|\mathcal{W}|} \tag{16}$$

By definition we have $\sum_r \mathsf{D}(r) = 0$, also $\sum_r \mathsf{D}(r)^2 \leqslant |\mathcal{W}^+|$. To justify this inequality, instead direct calculations, we can think of a random variable $Z = \mathbf{1}_{\mathcal{W}^+}(r)$ under uniformly distributed w; then we have $Z - \mathbf{E}Z = D$ and our inequality follows from the probabilistic inequality $\mathrm{Var}(Z) \leqslant \mathbf{E}Z^2$). This discussion shows that D is feasible to Equation (11) and therefore we have

$$\sum_r \mathsf{D}(r)\cdot(X(r)-Y(r)) \leqslant \sum_r \mathsf{D}^*(r)\cdot(X(r)-Y(r)) \leqslant \epsilon.$$

However, X and Y are probabilistic measures therefore $\sum_r X(r) = \sum_r Y(r) = 1$. Now using the explict form of D we obtain

$$\begin{aligned}
&\sum_r \mathsf{D}(r)\cdot(X(r)-Y(r)) = \\
&\sum_r \mathbf{1}_{\mathcal{W}^+}(r)\cdot(X(r)-Y(r)) + \frac{|\mathcal{W}^+|}{|\mathcal{W}|}\sum_r(X(r)-Y(r)) \\
&\qquad\qquad = \sum_{r\in\mathcal{W}^+}(X(r)-Y(r)) + 0
\end{aligned}$$

This together with the previous inequality shows that $\sum_{r\in\mathcal{W}^+}(X(r)-Y(r)) \leqslant \epsilon$. Repeating the same reasoning with respect to $-D$ in place of D ($-D$ is also feasible), we obtain also $\sum_{r\in\mathcal{W}^+}(X(r)-Y(r)) \geqslant -\epsilon$ which leads to the conclusion

$$\left|\sum_{r\in\mathcal{W}^+}(X(r)-Y(r))\right| \leqslant \epsilon. \tag{17}$$

The same discussion for $\mathsf{D}(r) = \mathbf{1}_{\mathcal{W}^-}(r) - \frac{|\mathcal{W}^-|}{|\mathcal{W}|}$ shows

$$\left|\sum_{r\in\mathcal{W}^-}(X(r)-Y(r))\right| \leqslant \epsilon. \tag{18}$$

These are desired bounds for the probability mass at the clipped values.

3.3 Bounding the linear transform

Let $\mathcal{W}^0 = \{w : -1 < \mathsf{D}^*(r) < 1\}$ be the set of arguments corresponding to not-clipped values. By Equation (12) for some constants a and $b > 0$ we have

$$\forall w \in \mathcal{W}^0 : \quad \mathsf{D}^*(r) = \frac{X(r)-Y(r)}{b} + a. \tag{19}$$

We start by observing that the difference $\delta(r) = X(r) - Y(r)$ on $\mathcal{W}^0$ takes both *positive and negative* values. Indeed, say that $\delta(r) > 0$ for all $w \in \mathcal{W}^0$. Since δ and D^* are co-monotone by Equation (12), all the negative values of $\delta(\cdot)$ are achieved on $\mathcal{W}^-$. In particular $\left|\sum_{r:\delta(r)<0}\delta(r)\right| \leqslant |\sum_{r:\in\mathcal{W}^-}\delta(r)| \leqslant \epsilon$ by Equation (18). Since $\sum_{r:\delta(r)<0}\delta(r) = -\sum_{r:\delta(r)\geqslant 0}\delta(r)$, this implies $d_1(X,Y) \leqslant 2\epsilon$ (which we already excluded). The same holds true when $\delta(r) < 0$ for all $w \in \mathcal{W}^0$. Therefore, if $d_{\mathrm{TV}}(X,Y) > \epsilon$ the function δ on $\mathcal{W}^0$ takes values of both signs. Recall that

$$\forall w \in \mathcal{W}^0 \quad a = \mathsf{D}^*(r) - \frac{X(r)-Y(r)}{b} = \mathsf{D}^*(r) - \frac{\delta(r)}{b}$$

Since $b > 0$ and D^* is bounded between 1 and -1, by substituting w_1, w_2 such that $\delta(w_1) < 0 < \delta(w_2)$ in place of w, we conclude that

$$-1 < a < 1 \tag{20}$$

We will now bound b. Recall that $\mathsf{D}^*(r) = \frac{X(r)-Y(r)}{b} + a \geqslant 1$ for $w \in \mathcal{W}^+$ by the definition of $\mathcal{W}^+$ and Equation (12). This implies $X(r) - Y(r) \geqslant b(1-a)$ for $w \in \mathcal{W}^+$. By Equation (17) we obtain

$$\epsilon \geqslant \sum_{r\in\mathcal{W}^+}(X(r)-Y(r)) \geqslant b(1-a)|\mathcal{W}^+| \tag{21}$$

Similarly, we have $\mathsf{D}^*(r) = \frac{X(r)-Y(r)}{b} + a \leqslant -1$ for $w \in \mathcal{W}^-$. Then $X(r) - Y(r) \leqslant -b(1+a)$ for $w \in \mathcal{W}^-$. By Equation (18)

$$-b(1+a)|\mathcal{W}^-| \geqslant \sum_{r\in\mathcal{W}^-}(X(r)-Y(r)) \geqslant -\epsilon \tag{22}$$

Combining the last two inequalites (and using Equation (20) to justify dividing inequalities by positive numbers $1+a$ and $1-a$), we obtain the following bound

$$b \leqslant \min\left(\frac{\epsilon}{(1-a)|\mathcal{W}^{+}|}, \frac{\epsilon}{(1+a)|\mathcal{W}^{-}|}\right). \tag{23}$$

Define now

$$\epsilon^{0} = \sum_{r\in\mathcal{W}^{0}} \mathsf{D}^{*}(r)(X(r)-Y(r))$$

Note that $\sum_{r\in\mathcal{W}^{0}}\mathsf{D}^{*}(r) = -\sum_{r\in\mathcal{W}^{+}\cup\mathcal{W}^{-}}\mathsf{D}^{*}(r) = -|\mathcal{W}^{+}|+|\mathcal{W}^{-}|$ (by feasibility and the definitions of $\mathcal{W}^{+},\mathcal{W}^{-}$). Also, $\sum_{r\in\mathcal{W}^{0}}(\mathsf{D}^{*}(r))^{2} = |\mathcal{W}|\sigma - |\mathcal{W}^{+}| - |\mathcal{W}^{-}|$. Therefore, using Equation (19), we obtain

$$\frac{\epsilon^{0}}{b} = |\mathcal{W}|\sigma - (1-a)|\mathcal{W}^{+}| - (1+a)|\mathcal{W}^{-}| \tag{24}$$

Note that by Equation (23) we have $(1-a)|\mathcal{W}^{+}| \leqslant \frac{\epsilon}{b}$ and $(1+a)|\mathcal{W}^{-}| \leqslant \frac{\epsilon}{b}$. Using this in Equation (24) we get

$$\frac{\epsilon^{0}+2\epsilon}{b} \geqslant |\mathcal{W}|\sigma = \frac{\epsilon^{0}}{b} + (1-a)|\mathcal{W}^{+}| + (1+a)|\mathcal{W}^{-}|. \tag{25}$$

It remains to bound ϵ^{0}. We have

$$\begin{aligned}\epsilon^{0} &= \sum_{r\in\mathcal{W}} \mathsf{D}^{*}(r)(X(r)-Y(r)) - \sum_{r\in\mathcal{W}^{-}\cup\mathcal{W}^{+}} \mathsf{D}^{*}(r)(X(r)-Y(r)) \\ &=^{(a)} \epsilon - \sum_{r\in\mathcal{W}^{-}\cup\mathcal{W}^{+}} \mathsf{D}^{*}(r)(X(r)-Y(r)) \\ &=^{(b)} \epsilon - \sum_{r\in\mathcal{W}^{+}} (X(r)-Y(r)) + \sum_{r\in\mathcal{W}^{-}} (X(r)-Y(r)) \\ &\leqslant^{(c)} \epsilon \end{aligned} \tag{26}$$

where (a) follows by the security assumption, (b) follows by definitions of $\mathcal{W}^{+},\mathcal{W}^{-}$, and (c) follows by Equation (21) and Equation (22) (note that a weaker bound of $\epsilon+2\epsilon$ can be obtained from Equation (17) and Equation (18)). Combining Equation (26) with Equation (24) we finally obtain $\frac{3\epsilon}{b} \geqslant |\mathcal{W}|\sigma$ or equivalently

$$b \leqslant \frac{3\epsilon}{|\mathcal{W}|\sigma} \tag{27}$$

which completes the proof of the promised bound on b.

3.4 Divergence on the unclipped set

From Equation (19) it follows that

$$\sum_{r\in\mathcal{W}^{0}} (X(r)-Y(r))^{2} = \\ b\sum_{r\in\mathcal{W}^{0}} \mathsf{D}^{*}(r)(X(r)-Y(r)) - ab\sum_{r\in\mathcal{W}^{0}} (X(r)-Y(r))$$

Since X and Y are probabilistic measures we have $\sum_{r\in\mathcal{W}}(X(r)-Y(r))=0$ and therefore we can rewrite the above equation as

$$\sum_{r\in\mathcal{W}^0}(X(r)-Y(r))^2 = \\ b\sum_{r\in\mathcal{W}^0}\mathsf{D}^*(r)(X(r)-Y(r)) + ab\sum_{r\in\mathcal{W}^-\cup\mathcal{W}^+}(X(r)-Y(r))$$

Note that the first sum equals ϵ^0 (defined previously) and the second sum is at most 2ϵ by Equations (17) and (18); in fact it is at most ϵ because contributions from $\mathcal{W}^-$ are negative as follows from Equation (22). Furthermore, ϵ_0 is at most ϵ as shown in Equation (26). Thus

$$\sum_{r\in\mathcal{W}^0}(X(r)-Y(r))^2 \leqslant b\epsilon + ab\epsilon.$$

Using bounds on a and b developed in Equation (20) and Equation (27) we finally obtain

$$\sum_{r\in\mathcal{W}^0}(X(r)-Y(r))^2 \leqslant 2b\epsilon \leqslant \frac{6\epsilon^2}{|\mathcal{W}|\sigma}. \tag{28}$$

4 Conclusion

By techniques of geometric flavor, we have shown optimal security bounds for games with mean and variance-bounded attackers. The obtained results are complementary to [3, 1] and show that the notion of weak keys as defined there cannot be much relaxed.

References

[1] Boaz Barak et al. “Leftover Hash Lemma, Revisited”. In: *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*. 2011, pp. 1–20. DOI: doi:10.1007/978-3-642-22792-9_1. URL: http://dx.doi.org/10.1007/978-3-642-22792-9_1.

[2] Yevgeniy Dodis, Krzysztof Pietrzak and Daniel Wichs. “Key Derivation without Entropy Waste”. In: *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*. 2014, pp. 93–110. DOI: doi:10.1007/978-3-642-55220-5_6. URL: http://dx.doi.org/10.1007/978-3-642-55220-5_6.

[3] Yevgeniy Dodis and Yu Yu. “Overcoming Weak Expectations”. In: *Theory of Cryptography - 10th Theory of Cryptography Conference, TCC 2013, Tokyo, Japan, March 3-6, 2013. Proceedings*. 2013, pp. 1–22. DOI: doi:10.1007/978-3-642-36594-2_1. URL: http://dx.doi.org/10.1007/978-3-642-36594-2_1.

[4] Renato Renner and Stefan Wolf. “Simple and Tight Bounds for Information Reconciliation and Privacy Amplification”. In: *Advances in Cryptology - ASIACRYPT 2005, 11th International Conference on the Theory and Application of Cryptology and Information Security, Chennai, India, December 4-8, 2005, Proceedings*. 2005, pp. 199–216. DOI: 10.1007/11593447_11. URL: https://doi.org/10.1007/11593447_11.

[5] Alfréd Rényi. “On Measures of Entropy and Information”. In: *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Contributions to the Theory of Statistics*. Berkeley, Calif.: University of California Press, 1961, pp. 547–561. URL: https://projecteuclid.org/euclid.bsmsp/1200512181.

A Proofs

A.1 Proof of Lemma 1

Since X is non-negative we can assume $\mathbb{E}\mathsf{D} = \sigma$, because increasing $\mathsf{D}(r)$ for any r can only increase the objective $\sum_r X(r)\mathsf{D}(r)$. Next, we can assume that X and D are co-monotone, in other words $X(r_1) \geqslant X(r_2)$ implies $\mathsf{D}(r_1) \geqslant \mathsf{D}(r_2)$ (otherwise swapping values of $\mathsf{D}(r_1)$ and $\mathsf{D}(r_2)$ doesn't decrease the objective). Finally, when $X(r_1) \geqslant X(r_2)$ then either $\mathsf{D}(r_1) = 1$ or $\mathsf{D}(r_2) = 0$; otherwise we have $1 > \mathsf{D}(r_1) \geqslant \mathsf{D}(r_2) > 0$ and we can modify $\mathsf{D}(r_1) \leftarrow \mathsf{D}(r_1) + \delta$, $\mathsf{D}(r_2) = \mathsf{D}(r_2) - \delta$ for small δ, so that $\mathsf{D}(r_1), \mathsf{D}(r_2) \in [0, 1]$ and the objective changes by $X(r_1)\delta - X(r_2)\delta \geqslant 0$. The last observation implies that $\mathsf{D}(r)$ takes values 0 or 1 for all but possibly one r. Since $\mathbb{E}\mathsf{D} = \sigma$ we conclude that $\mathsf{D}(r) = 1$ for $\lfloor 2^n\sigma \rfloor$ values of r and $\mathsf{D}(r) = 2^n\sigma - \lfloor 2^n\sigma \rfloor$ for some r. Since D and X are co-monotone, these r correspond respectively to $\lfloor 2^n\sigma \rfloor$ top values of $X(r)$ and the $(\lfloor 2^n\sigma \rfloor + 1)$-th top value of $X(r)$.

A.2 Proof of Lemma 2

Consider the problem of maximizing $\sum_r X(r)\mathsf{D}(r)$ subjected to the constraints $q_0 \leqslant \mathsf{D}(r) \leqslant q_1$ for all r and $\mathbb{V}\mathrm{ar}(\mathsf{D}) = 2^{-n}\sum_r \mathsf{D}(r)^2 - \left(2^{-n}\sum_r \mathsf{D}(r)\right)^2 \leqslant \sigma$. We form the lagrangian

$$L(\lambda, \lambda_3(\cdot), \lambda_4(\cdot)) = \sum_r X(r)\mathsf{D}(r) - \lambda \cdot \left(2^{-n}\sum_r \mathsf{D}(r)^2 - \left(2^{-n}\sum_r \mathsf{D}(r)\right)^2 - \sigma\right) \\ - \lambda_3(r)\cdot(q_0 - \mathsf{D}(r)) - \lambda_4(r)\cdot(\mathsf{D}(r) - q_1)$$

with non-negative $\lambda, \lambda_3(\cdot), \lambda_4(\cdot)$ satisfying the complementary conditions

$$-\lambda_3(r)\cdot(q_0 - \mathsf{D}(r)) = 0, \quad \lambda_4(r)\cdot(\mathsf{D}(r) - q_1) = 0.$$

We note that the Slater constraint qualification holds with $\mathsf{D}(r) = (q_0 + q_1)/2$, as then inequality constraints are strict: $q_0 < \mathsf{D}(r) < q_1$ and $\mathbb{V}\mathrm{ar}\mathsf{D} = 0 < \sigma$, and the program is convex. By the first order KKT conditions $\frac{\partial L}{\partial \mathsf{D}(r)} = 0$. Since

$$\frac{\partial L}{\partial \mathsf{D}(r)} = X(r) - c_1 \cdot \mathsf{D}(r) + \lambda_3(r) - \lambda_4(r) \tag{29}$$

for $c_1 = 2\lambda \cdot 2^{-n} \geqslant 0$, the first order conditions imply the claim if we can show that $c_1 \neq 0$ (the clipping part comes from λ_3 and λ_4 which are active only when $\mathsf{D}(r) = q_0$ and $\mathsf{D}(r) = q_1$ respectively). Note that when $\sum_r X(r) = 0$ we can shift $\mathsf{D}(r) := \mathsf{D}(r) - 2^{-n}\sum_{r'} \mathsf{D}(r')$ not changing the objective neither violating constraints (the variance doesn't change). In particular we can assume $\sum_r \mathsf{D}(r) = 0$. The lagrangian then gets an extra term $-\lambda' \sum_r \mathsf{D}(r)$ so that

$$\frac{\partial L}{\partial \mathsf{D}(r)} = X(r) - c_1 \cdot \mathsf{D}(r) - c_2 + \lambda_3(r) - \lambda_4(r) \tag{30}$$

Since $\lambda \geqslant 0$ we have $c_1 \geqslant 0$ and $b \geqslant 0$.

It remains to consider $c_1 = 0$. Consider only Equation (30) as Equation (29) is a special case of it. For every r we either have $X(r) = c_2$ or one of the multipliers $\lambda_3(r)$,$\lambda_4(r)$ is not zero and then $\mathsf{D}(r) = q_0$ when $X(r) = c_2 - \lambda_3(r)$ and $\mathsf{D}(r) = q_1$ when $X(r) = c_2 + \lambda_4(r)$. On the set $\{r : X(r) = c_2\}$ we can replace all the values of $\mathsf{D}(r)$ by their average, not changing the objective; also the variance can only decrease. Thus we have $\mathsf{D}(r) = c_3$ when $X(r) = c_2$ for some constant c_3. But then we can write

$$\mathsf{D}(r) = \mathsf{clip}_{[q_0,q_1]}\left(c_3 + (X(r) - c_2)/b\right)$$

for some sufficently small $b > 0$ which gives us again the desired formula.

Finally, let's consider whether the constraint $\mathbb{Var}\mathsf{D} \leqslant \sigma$ is binding or not. If $\mathbb{Var}\mathsf{D} < \sigma$ then $\lambda = 0$ and $c_1 = 0$ in Equation (29). Then for every r we have $X(r) = -\lambda_3(r)$ or $X(r) = \lambda_4(r)$. In particular, when $X(r) < 0$ then $\mathsf{D}(r) = q_0$ and when $X(r) > 0$ then $\mathsf{D}(r) = q_1$. If $\sum_r X(r) = 0$ we obtain

$$\sum_r X(r)\mathsf{D}(r) = q_1 \sum_{r:X(r)>0} X(r) - q_0 \sum_{r:X(r)<0} X(r) \qquad = (q_1 - q_0) \cdot \frac{1}{2} \sum_r |X(r)|.$$

A.3 Proof of Theorem 1

To see how Section 2.3 follows from Theorem 1 consider the set $\mathcal{S}$ of keys r corresponding to the $\lfloor 2^n\sigma \rfloor$ heaviest values $X(r)$ and r_0 be such that $X(r_0)$ is the top $\lfloor 2^n\sigma \rfloor + 1$ value. We have

$$\begin{aligned} X(r_0) &\leqslant |\mathcal{S}|^{-1} \sum_{r\in\mathcal{S}} X(r) \\ &\leqslant 2^{-n} + \frac{2}{2^n\sigma} \sum_{r\in\mathcal{S}} \left(X(r) - 2^{-n}\right) \\ &\leqslant 2^{-n} + 2^{-n+2}\epsilon/\sigma \end{aligned}$$

where in the first inequality we used the definition of r_0 and $\mathcal{S}$, the second is because we know the size of $\mathcal{S}$ and the last inequality follows from Theorem 1. Consider shifting the probability mass from $\mathcal{S}$ as follows $X'(r) = \min(X(r), 2^{-n}) + 2^{-n}\delta$ for $r \in \mathcal{S}$ and $X'(r) = X(r) + 2^{-n}\delta$ for $r \in \mathcal{S}^c$ where $\delta = \sum_{r\in\mathcal{S}}(X(r) - \min(X(r), 2^{-n}))$ and $\delta = O(\epsilon)$ by Theorem 1. Then X' and X are $\epsilon' = \delta$ far in ℓ_1. Moreover for every r we have

$$X(r) \leqslant \max(2^{-n} + 2^{-n}\delta, 2^{-n} + 2^{-n+2}\epsilon/\sigma + 2^{-n}\delta)$$

which is $2^{-n}(1 + O(\epsilon/\delta))$. Thus X' has min-entropy of $\mathbf{H}_\infty(X') = n - \log(1 + O(\epsilon/\sigma)$.

Conversely, if X is $O(\epsilon)$-close in ℓ_1 to a distribution with min-entropy k we have

$$|\mathbb{E}_{r\sim X}\mathsf{D}(r) - \mathbb{E}_{r\sim U_n}\mathsf{D}(r)| \leqslant O(\epsilon) + (2^{n-k} - 1)\sigma$$

because $|X(r) - 2^{-n}| \leqslant 2^{-k} - 2^{-n}$ and $\sum_r \mathsf{D}(r) \leqslant 2^n\sigma$. If $k \geqslant n - \log(1 + O(\epsilon/\sigma)$ then we can bound it by $O(\epsilon)$.

A.4 Proof of Theorem 1

Proof. Consider two non-negative measures $Z^+(r) = \max(X(r) - Y(r), 0)$ and $Z^-(r) = -\min(X(r) - Y(r), 0)$. We have

$$\mathbb{E}_{r\sim X}\mathsf{D}(r) - \mathbb{E}_{r\sim Y}\mathsf{D}(r) = \sum_r Z^+(r)\mathsf{D}(r) - \sum_r Z^-(r)\mathsf{D}(r) \tag{31}$$

Let D be the distiguisher obtained from Lemma 1 applied to the measure Z^+ (and same σ). It follows that for any at most $\lfloor 2^n\sigma \rfloor$-element subset $\mathcal{S}$

$$\sum_{r\in\mathcal{S}} Z^+(r) \leqslant \sum_r \mathsf{D}(r)Z^+(r)$$

Lemma 1 ensures $\mathbb{E}\mathsf{D} = \sigma$, but we can put $\mathsf{D}(r) \leftarrow 0$ whenever $Z^{+}(r) = 0$ so that the above inequality still holds true (then $\mathbb{E}\mathsf{D} \leqslant \sigma$). Then we have $\sum_{z} Z^{-}(r)\mathsf{D}(r) = 0$ because $Z^{-}(r) > 0$ implies $Z^{+}(r) = 0$. Thus

$$\sum_{r\in\mathcal{S}} Z^{+}(r) = \sum_{r} \mathsf{D}(r)Z^{+}(r) - \sum_{r} Z^{-}(r)\mathsf{D}(r) \leqslant \epsilon$$

where the second inequality follows by the assumption (D is feasible: $\mathbb{E}\mathsf{D} \leqslant \sigma$ and $\mathsf{D}(r) \in [0,1]$ by construction). Thus we have shown that for any at most $2^{n}\sigma$-element subset $\mathcal{S}$

$$\sum_{r\in\mathcal{S}} \max(X(r) - Y(r), 0) \leqslant \epsilon$$

and by swapping the roles of X and Y (which doesn't change the assumptions!)

$$\sum_{r\in\mathcal{S}} \max(Y(r) - X(r), 0) \leqslant \epsilon.$$

The last two inequalities imply that

$$\sum_{r\in\mathcal{S}} |X(r) - Y(r)| \leqslant 2\epsilon \tag{32}$$

which finishes the proof of the first part. For the converse part we reconsider Equation (31). By Lemma 1 applied to the measure Z^{+} and our assumptions

$$\sum_{r} Z^{+}(r)\mathsf{D}(r) \leqslant \sum_{r\in\mathcal{S}\cup\{r'\}} Z^{+}(r)$$

where $\mathcal{S}$ is the set of r corresponding to the top $\lfloor 2^{n}\sigma \rfloor$ values of $Z^{+}(r)$ and r' corresponds to the top $\lfloor 2^{n}\sigma \rfloor + 1$-th value of $Z^{+}(r)$. By the defimition of r' and our assumption with respect ot $\mathcal{S}$ we finally obtain

$$\sum_{r} Z^{+}(r)\mathsf{D}(r) \leqslant \sum_{r\in\mathcal{S}} Z^{+}(r) + \frac{1}{\lfloor 2^{n}\sigma \rfloor} \sum_{r\in\mathcal{S}} Z^{+}(r) \leqslant \epsilon \cdot' (1 + 1/\lfloor 2^{n}\sigma \rfloor) \tag{33}$$

which is at most $2\epsilon'$. We have bounded the non-negative part in Equation (31) and thus

$$\mathbb{E}_{r\sim X}\mathsf{D}(r) - \mathbb{E}_{r\sim Y}\mathsf{D}(r) \leqslant 2\epsilon' \tag{34}$$

for all feasible D'. Swapping the roles of X and Y we obtain also the lower bound $-2\epsilon'$, which completes the proof of the converse part. ◀

A.5 Proof of Corollary 3

Proof. Consider first the "necessary" part. Let Y be uniform and let $\mathcal{S}$ be as in Theorem 2. Let $X'(r) = X(r)$ for $r \in \mathcal{S}^{c}$ and $X'(r) = Y(r)$ where $r \in \mathcal{S}$. Define $X''(r) = X'(r) + 2^{-n}\delta$ where $\delta = \sum_{r\in\mathcal{S}}(X(r) - Y(r))$ (the probability mass where $X(r)$ differs from $X'(r)$). Then X'' is probabilistic and

$$\sum_{r} X''(r)^{2} = \sum_{r} X'(r)^{2} + 2\cdot 2^{-n}\delta \sum_{r} X'(r) + 2^{-n}\delta^{2}$$

We also have

$$\sum_r X'(r)^2 = \sum_r (X'(r) - Y(r))^2 + 2 \cdot 2^{-n} \sum_r X'(r) - 2^{-n}$$

and thus

$$\sum_r X''(r)^2 = \sum_r (X'(r) - Y(r))^2 + 2 \cdot 2^{-n}(1+\delta) \sum_r X'(r) - 2^{-n}(1-\delta^2)$$

Note that $\delta = \sum_{r \in \mathcal{S}} (X(r) - Y(r)) = \sum_r (X(r) - X'(r))$ and therefore $\sum_r X'(r) = 1 - \delta$. We obtain

$$\sum_r X''(r)^2 = \sum_r (X'(r) - Y(r))^2 + 2^{-n}(1-\delta^2).$$

By Theorem 2 we have $\delta = O(\epsilon)$ and $\sum_{r \in \mathcal{S}^c} (X'(r) - Y(r))^2 = O(2^{-n}\epsilon^2\sigma^{-1})$ and therefore

$$\sum_r X''(r)^2 = 2^{-n} \cdot (1 + O(\epsilon^2\sigma^{-1})).$$

To prove the opposite part, observe that

$$\mathbb{E}_{r \sim X} \mathsf{D}(r) - \mathbb{E}_{r \sim U_n} \mathsf{D}(r) = O(\epsilon') + \mathbb{E}_{r \sim X'} \mathsf{D}(r) - \mathbb{E}_{r \sim U_n} \mathsf{D}(r)$$

and by the Cauchy-Schwarz inequality

$$|\mathbb{E}_{r \sim X'} \mathsf{D}(r) - \mathbb{E}_{r \sim U_n} \mathsf{D}(r)| \leqslant \left(\sum_r |X'(r) - 2^{-n}|^2 \right)^{1/2} \cdot \left(2^n \mathbb{Var} \mathsf{D}\right)^{1/2}.$$

note that $\sum_r |X'(r) - 2^{-n}|^2 = \sum_r (X'(r) - 2^{-n})^2 = \sum_r X'(r)^2 - 2^{-n}$ which, by the assumption on entropy, equals $O\left(2^{-n}\epsilon^2/\sigma\right)$. Since $\mathbb{Var}\mathsf{D} \leqslant \sigma$ we obtain the bound $O(\epsilon)$. ◀