Accumulating Entropy with Adversarial Sources

Let

1. D be a 2-monotone distribution with min-entroppy k.
2. $n \in \mathbb{N}$ be the length of sources x_i for $0 \leq i < N$ for some N.
3. $\pi : [n] \to [n]$ be a cyclic permutation ($\pi^m = id$ iff $n|m$). Then $f_\pi : [2]^n \to [2]^n$ where $(x_0, \ldots, x_{n-1}) \mapsto (x_{\pi(0)}, \ldots, x_{\pi(n-1)}$. Clearly, $f_\pi^m = f_{\pi^m}$.
4. $\mathcal{A}$ denote the adversary.
5. for any $0 \leq p \leq 1$, let D_p be the distribution where 1 occurs with probability p and 0 with probability $1-p$.
6. p be the probability that $\mathcal{A}$ can replace a source with one of its choosing.

1 Version 1 (Sept 24, 2021)

Hybrid H_0:

1. Let $R_0 = 0^n$.
2. For $0 \leq i < N$,
   (a) Sample $x_i \leftarrow D$.
   (b) $\mathcal{A}$ samples $b_i \leftarrow D_p$. If $b_i = 1$, $\mathcal{A}$ chooses $y_i \in [2]^n$ and sets $x_i = y_i$. Otherwise, x_i is unaffected.
   (c) $R_{i+1} = R_i \oplus f_\pi^i(x_i)$
3. $\mathcal{A}$ chooses and outputs $R_\mathcal{A} \in [2]^n$.
4. If $R_\mathcal{A} = R_N$, output 1. Otherwise, output 0. modify for $R_\mathcal{A} \approx R_N$

Hybrid H_1: Same as H_0 except $\mathcal{A}$ chooses $R_\mathcal{A}$ before the experiment begins and always replaces x_{N-1} with its choice y_{N-1}.

Lemma 1.1.

$$P(H_0 = 1) \leq P(H_1 = 1)$$

I think $P(H_1 = 1) = P(H_0 = 1)/(p + (1-p)P(\mathcal{A}\text{ correctly guesses }x_{N-1})) \geq P(H_0 = 1)$.

Proof. Suppose $H_0 = 1$. Then $\mathcal{A}$ predicted the value of R_N. Let $R_\mathcal{A}$ be the string $\mathcal{A}$ choose before the experiment started. Then choose $y_{N-1} = x_{N-1} \oplus R_N \oplus R_\mathcal{A}$. Then

$$R'_N := R_{N-1} \oplus y_{N-1} = R_{N-1} \oplus x_{N-1} \oplus R_N \oplus R_\mathcal{A} = R_N \oplus R_N \oplus R_\mathcal{A} = R_\mathcal{A}$$

where R'_N is the value of the register at the end of H_1.

Suppose $H_1 = 1$. If $\mathcal{A}$ in H_0 successfully replaces x_{N-1} (which happens with probability p), then $H_0 = 1$ by an analogous argument to the one above. If not, $\mathcal{A}$ must correctly guess x_{N-1}. Since $(H_0 = 1) \implies (H_1 = 1)$, $(H_1 = 0) \implies (H_0 = 0)$, so $P(H_0 = 1) = (p + (1-p)P(\mathcal{A} \text{ correctly guesses } x_{N-1}))P(H_1 = 1) \leq P(H_1 = 1)$. ☐

Hybrid H_2: Same as H_1 except $\mathcal{A}$ always chooses $R_{\mathcal{A}} = 0^n$.

Lemma 1.2.

$$P(H_1 = 1) = P(H_2 = 1)$$

Proof. Suppose $H_1 = 1$. Then $R_{\mathcal{A}} = R_N$. If $\mathcal{A}$ replaced x_{N-1} with $y_{N-1} \oplus R_{\mathcal{A}}$ instead of y_{N-1}, then $H_2 = 1$. Thus $P(H_1 = 1) \leq P(H_2 = 1)$. The same argument proves $P(H_1 = 1) \geq P(H_2 = 1)$. ☐

it is very easy (actually "easier") in the proof of the first lemma to jump to H_2. Is it worth having H_1?

Hybrid H_3: Same as H_2 except $\mathcal{A}$ computes $T_0 = 0^n$ and $T_{i+1} = T_i \oplus f_\pi^i(y_i)$ if $b_i = 1$ and $T_{i+1} = T_i$ otherwise.

$\mathcal{A}$ only does computations on information it already knows, so it is equivalent to H_2.

Hybrid H_4: Same as H_3 except if $b_i = 1$, the choice of y_i must satisfy $f_\pi^i(y_i) \& T_i = 0^n$.

Alternate Hybrid H'_3: Same as H_2 except if $i < N-1$ and $b_i = 1$, $\mathcal{A}$ always chooses $y_i = 0$. $\mathcal{A}$ can choose any string for y_{N-1}.

I think this has the same effect as tagging, but is more streamlined. This is Hybrid E? I am not convinced this is trivially secure from No Time to Hash. This behaves like having a sequence of permutations π^{ℓ_i} where ℓ_i are "increasing" mod n instead of a constant permutation (which corresponds to the sequence π^i. No Time to Hash does not give a description in that case. We should be ok if for each $0 \leq \ell < n$, $\exists 0 \leq i < N$ such that $\ell_i = \ell$. Seems stronger than we need, but would definitely work. If N is a multiple of n, "increasing" corresponds to increasing as integers except at $N/n - 1$ many i.

2 Version 2 (Sept 28, 2021)

Hybrid H_0:

1. Let $R_0 = 0^n$.
2. For $0 \leq i < N$,
   (a) Sample $x_i \leftarrow D$.
   (b) $\mathcal{A}$ samples $b_i \leftarrow D_p$. If $b_i = 1$, $\mathcal{A}$ chooses $y_i \in \{0,1\}^n$ and sets $x_i = y_i$. Otherwise, x_i is unaffected.
   (c) $R_{i+1} = R_i \oplus f_\pi^i(x_i)$
3. $\mathcal{A}$ chooses and outputs $R_\mathcal{A} \in \{0,1\}^n$.
4. If $R_\mathcal{A} = R_N$, output 1. Otherwise, output 0. modify for $R_\mathcal{A} \approx R_N$

Hybrid H_1:

0. $\mathcal{A}$ chooses $R_\mathcal{A}$.
1. Let $R_0 = 0^n$.
2. For $0 \leq i < N$,
   (a) Sample $x_i \leftarrow D$.
   (b) $\mathcal{A}$ samples $b_i \leftarrow D_p$. If $b_i = 1$, $\mathcal{A}$ chooses $y_i \in \{0,1\}^n$ and sets $x_i = y_i$. Otherwise, x_i is unaffected.
   (c) $R_{i+1} = R_i \oplus f_\pi^i(x_i)$
3. $\mathcal{A}$ chooses $y_N \in \{0,1\}^n$ and outputs $R_\mathcal{A}$. Compute $R_{N+1} = R_N \oplus y_N$.
4. If $R_\mathcal{A} = R_{N+1}$, output 1. Otherwise, output 0.

Lemma 2.1.

$$P(H_0 = 1) = P(H_1 = 1)$$

Proof. Suppose $H_0 = 1$. Then $\mathcal{A}$ predicted the value of R_N. Let $R_\mathcal{A}$ be the string $\mathcal{A}$ choose before the experiment started. Then choose $y_N = \oplus R_N \oplus R_\mathcal{A}$. Then $R_{N+1} := R_N \oplus y_N = R_\mathcal{A}$.

Suppose $H_1 = 1$. Then $R_\mathcal{A} = R_N \oplus y_N$. The adversary in H_0 would know $R_\mathcal{A}$ and y_N, so they can $R_\mathcal{A} \oplus y_N$ at step 3. Then $H_0 = 1$. □

Hybrid H_2:

0. ~~$\mathcal{A}$ chooses $R_\mathcal{A}$.~~
1. Let $R_0 = 0^n$.

2. For $0 \leq i < N$,

   (a) Sample $x_i \leftarrow D$.

   (b) $\mathcal{A}$ samples $b_i \leftarrow D_p$. If $b_i = 1$, $\mathcal{A}$ chooses $y_i \in \{0,1\}^n$ and sets $x_i = y_i$. Otherwise, x_i is unaffected.

   (c) $R_{i+1} = R_i \oplus f_\pi^i(x_i)$

3. $\mathcal{A}$ chooses $y_N \in \{0,1\}^n$ ~~and outputs $R_\mathcal{A}$~~. Compute $R_{N+1} = R_N \oplus y_N$.

4. If $R_{N+1} = 0$, output 1. Otherwise, output 0.

Lemma 2.2.

$$P(H_1 = 1) = P(H_2 = 1)$$

Proof. Suppose $H_1 = 1$. Then $R_\mathcal{A} = R_{N+1}$, so $\mathcal{A}$ knows R_{N+1} and thus $R_N = R_{N+1} \oplus y_N$. To succeed in H_2, $\mathcal{A}$ chooses $y_N = R_N$ instead.

Now suppose $H_2 = 1$. Then $R_{N+1} = R_N \oplus y_N = 0$, so $\mathcal{A}$ was able to guess $y_N = R_N$. Let $y_N = R_N \oplus R_\mathcal{A}$ instead. Then $R_{N+1} = R_\mathcal{A}$. □

Hybrid H_3:

1. Let $R_0 = 0^n$ and $E = 0$.

2. For $0 \leq i < N$,

   (a) Sample $x_i \leftarrow D$.

   (b) $\mathcal{A}$ samples $b_i \leftarrow D_p$. If $b_i = 1$, $\mathcal{A}$ chooses $y_i \in \{0,1\}^n$ and sets $x_i = y_i$. If $y_i \neq 0$, set $E = 1$. Otherwise, x_i is unaffected.

   (c) $R_{i+1} = R_i \oplus f_\pi^i(x_i)$

3. $\mathcal{A}$ chooses $y_N \in \{0,1\}^n$. Compute $R_{N+1} = R_N \oplus y_N$.

4. If $R_{N+1} = 0$ and $E = 0$, output 1. Otherwise, output 0.

Lemma 2.3.

$$P(H_2 = 1) = P(H_3 = 1)$$

Proof. Suppose $H_2 = 1$. Since the x_i are independent, they do not depend on R_j for $j < 1$. Thus if an x_i is replaced with y_i, it does not influence the other x_j. Suppose $\mathcal{A}$ in H_3 chooses the same y_i as $\mathcal{A}$ in H_2, but they set $x_i = 0$ if $b_i = 1$. Then choose $y'_N = y_N \bigoplus_{b_i=1} f_\pi^i(y_i)$. Then $R'_{N+1} = R'_N \oplus y'_N = R_N \oplus y_N = 0$, so $H_3 = 1$.

Suppose $H_3 = 1$. Then $R_{N+1} = 0$, so $H_2 = 1$. □