CONJURA · OPEN PROBLEM

Randomness Extraction from Unpredictable Random-Oracle Sources

Two Leftover-Hash-Lemma Conjectures

Status. Statement: human-written, not yet formalized.

Category. Information-Theoretic Cryptography.

Setting. Fix nonempty finite sets $\mathcal{K}$ (seeds), $\mathcal{D}$ (inputs), $\mathcal{R}$ (outputs), and write $K := |\mathcal{K}|$, $D := |\mathcal{D}|$, $R := |\mathcal{R}|$. Let $\mathsf{Fun}(\mathcal{K} \times \mathcal{D}, \mathcal{R})$ be the set of all functions $\mathcal{K} \times \mathcal{D} \to \mathcal{R}$, let $\mathrm{SD}(\cdot,\cdot)$ denote statistical distance and $U_{\mathcal{R}}$ the uniform distribution on $\mathcal{R}$. The source S, the predictor P and the distinguisher D of Figure 1 are computationally unbounded and receive the *entire* function table of H as an explicit input. The two extraction games differ only in whether the seed *sd* is kept secret from D or given to it.

Definition 1. Set $\mathbf{Adv}^{\mathrm{pred}}_{\mathcal{K},\mathcal{D},\mathcal{R},S}(P) := \Pr[\mathrm{Pred}^{S}_{P} \Rightarrow 1]$ and

$$\mathbf{Adv}^{\mathrm{ext}}_{\mathcal{K},\mathcal{D},\mathcal{R}}(S,\mathsf{D}) := 2\Pr[\mathrm{Ext}^{S}_{\mathsf{D}} \Rightarrow 1] - 1,$$

$$\mathbf{Adv}^{\text{ext-pub}}_{\mathcal{K},\mathcal{D},\mathcal{R}}(S,\mathsf{D}) := 2\Pr[\text{Ext-pub}^{S}_{\mathsf{D}} \Rightarrow 1] - 1.$$

A source S is *ϵ-unpredictable* if $\mathbf{Adv}^{\mathrm{pred}}_{\mathcal{K},\mathcal{D},\mathcal{R},S}(P) \le \epsilon$ for every unbounded predictor P.

Conjecture 1 (Secret seed). *There is a universal constant $c > 0$, independent of $\mathcal{K}$, $\mathcal{D}$, $\mathcal{R}$ and ϵ, such that for all nonempty finite $\mathcal{K},\mathcal{D},\mathcal{R}$, all $\epsilon \in (0,1]$, every ϵ-unpredictable source S and every unbounded distinguisher D,*

$$\mathbf{Adv}^{\mathrm{ext}}_{\mathcal{K},\mathcal{D},\mathcal{R}}(S,\mathsf{D}) \;\le\; \delta(\epsilon,K,D,R) \;:=\; c \cdot \sqrt{\frac{\epsilon R + \log_2 D}{K}}\,.$$

Game Pred_P^S

$H \xleftarrow{\$} \mathsf{Fun}(\mathcal{K} \times \mathcal{D}, \mathcal{R})$; $(x,z) \xleftarrow{\$} S(H)$; $x' \xleftarrow{\$} P(H,z)$
return $(x = x')$

Game $\mathrm{Ext}_{\mathsf{D}}^S$ (secret seed)

$H \xleftarrow{\$} \mathsf{Fun}(\mathcal{K} \times \mathcal{D}, \mathcal{R})$; $(x,z) \xleftarrow{\$} S(H)$; $sd \xleftarrow{\$} \mathcal{K}$
$y_0 \leftarrow H(sd,x)$; $y_1 \xleftarrow{\$} \mathcal{R}$; $b \xleftarrow{\$} \{0,1\}$
$b' \xleftarrow{\$} \mathsf{D}(H, y_b, z)$; **return** $(b = b')$

Game $\text{Ext-pub}_{\mathsf{D}}^S$ (public seed)

$H \xleftarrow{\$} \mathsf{Fun}(\mathcal{K} \times \mathcal{D}, \mathcal{R})$; $(x,z) \xleftarrow{\$} S(H)$; $sd \xleftarrow{\$} \mathcal{K}$
$y_0 \leftarrow H(sd,x)$; $y_1 \xleftarrow{\$} \mathcal{R}$; $b \xleftarrow{\$} \{0,1\}$
$b' \xleftarrow{\$} \mathsf{D}(H, sd, y_b, z)$; **return** $(b = b')$

Figure 1: Prediction game (top) and the two extraction games: secret seed (middle) and public seed (bottom). The first argument of S, P and D is the *full function table* of H; the games Ext and Ext-pub differ only in whether D receives sd.

Conjecture 2 (Public seed). *There is a universal constant $c > 0$, independent of $\mathcal{K}$, $\mathcal{D}$, $\mathcal{R}$ and ϵ, such that for all nonempty finite $\mathcal{K}, \mathcal{D}, \mathcal{R}$, all $\epsilon \in (0,1]$, every ϵ-unpredictable source S and every unbounded distinguisher D,*

$$\mathbf{Adv}^{\text{ext-pub}}_{\mathcal{K},\mathcal{D},\mathcal{R}}(S,\mathsf{D}) \;\le\; \delta_{\text{pub}}(\epsilon,K,D,R) \;:=\; c \cdot \left(\sqrt{\epsilon R} + \sqrt{\frac{\log_2 D}{K}}\right).$$