$$- \Pr[Y = z]\Big| \leq \varepsilon$$

Equivalent: An UNBOUNDED ADV can't distinguish a sample $z \leftarrow X$ from $z \leftarrow Y$ w.p. better than ε.

THM. Let $\mathcal{H} = \{ h_s : \{0,1\}^n \to \{0,1\}^\ell \}$ where $s \in \{0,1\}^d$ be a family of PAIRWISE INDEP. hash functions. Then,

$$\mathrm{Ext}(s, x) = h_s(x) = h(s, x)$$

is a (k, ε)-extractor for

$$k \geq \ell + 2\log(1/\varepsilon) - 2$$

Made with Goodnotes

LEMMA. Let Y be a RV over $\mathcal{Y}$ s.t.

$$\mathrm{Col}(Y) = \Pr[Y = Y']$$

$$= \sum_{y \in \mathcal{Y}} \Pr[Y = y]^2$$

$$\leq \frac{1}{|\mathcal{Y}|} \cdot (1 + 4\varepsilon^2)$$

Then, $SD(Y; U) \leq \varepsilon$.

$\hookrightarrow$ UNIFORM over $\mathcal{Y}$.

Example: $\mathrm{Col}(U_n) = \sum_{u \in \{0,1\}^n} \Pr[U_n = u]^2$

$$= 2^n \cdot 2^{-2n} = 2^{-n}$$

First: We use the lemma to prove Theorem.

PROOF (of THM). Set $Y = (S, h(S,X))$

$U \equiv U_{d+l} \equiv (S, U_l)$, $\mathcal{Y} = \{0,1\}^{d+l}$

$Col(Y) = \Pr[Y = Y']$

$= \Pr[S = S' \wedge h(S,X) = h(S',X')]$

$= \Pr[S = S' \wedge h(S,X) = h(S,X')]$

$= \Pr[S = S'] \cdot \Pr[h(S,X) = h(S,X')]$

$= 2^{-d} \cdot \Pr[h(S,X) = h(S,x')]$

$= 2^{-d} \cdot (\Pr[X = X'] \cdot \Pr[h(S,X) = h(S,X')$

$\mid X = X'] + \Pr[X \neq X'] \cdot$

$\Pr[h(S,x) = h(S,x') \mid x \neq x'])$

(This because

$$\Pr[A] = \Pr[A \wedge B] + \Pr[A \wedge \bar{B}]$$

$$= \Pr[B] \cdot \Pr[A \mid B] + \Pr[\bar{B}] \cdot \Pr[A \mid \bar{B}])$$

$$= 2^{-d} \left(\mathrm{Col}(X) + \Pr[h(S,X) = h(S,X') \wedge X \neq X'] \right)$$

$$\leq 2^{-d}\left(2^{-k} + 2^{-\ell}\right)$$

$$= \frac{1}{2^{d+\ell}}\left(2^{\ell-k} + 1\right)$$

$$\left(\ell - k \leq 2 - 2\log(1/\varepsilon)\right)$$

$$\leq \frac{1}{|\mathcal{Y}|} \cdot \left(2^{2-2\log(1/\varepsilon)} + 1\right)$$

$$= \frac{1}{|\mathcal{Y}|} \cdot \left(1 + 4\varepsilon^2\right) \quad \blacksquare$$

If $H_\infty(X) \geq k$; $Col(X) \leq 2^{-k}$

Proof (of Lemma). By definition:

$$SD(Y; U) = \frac{1}{2} \sum_{y \in \mathcal{Y}} \left| \Pr[Y = y] - \frac{1}{|\mathcal{Y}|} \right|$$

$$= \frac{1}{2} \sum_{y \in \mathcal{Y}} q_y \cdot s_y$$

$$q_y = \left(\Pr[Y = y] - \frac{1}{|\mathcal{Y}|} \right)$$

$$s_y = \begin{cases} 1 & \text{if } q_y > 0 \\ -1 & \text{otw} \end{cases}$$

$$= \frac{1}{2} \langle \vec{q}, \vec{s} \rangle$$

by CAUCHY SHWARTZ

$$\leq \frac{1}{2} \sqrt{\langle \vec{q}, \vec{q} \rangle \cdot \langle \vec{s}, \vec{s} \rangle}$$

$$= \frac{1}{2} \sqrt{\sum_{y \in \mathcal{Y}} q_y^2 \cdot |\mathcal{Y}|}$$

$$\vec{s} = (s_y)_{y \in \mathcal{Y}}$$

$$\langle \vec{s}, \vec{s} \rangle = \sum_y s_y^2 = |\mathcal{Y}|$$

Now, let's expand $\sum_{y \in \mathcal{Y}} q_y^2$

$$\sum_{y \in \mathcal{Y}} q_y^2 = \sum_{y \in \mathcal{Y}} \left(\Pr[Y = y] - \frac{1}{|\mathcal{Y}|} \right)^2$$

$$= \sum_{y \in \mathcal{Y}} \left(\Pr[Y = y]^2 + \frac{1}{|\mathcal{Y}|^2} - 2 \frac{\Pr[Y = y]}{|\mathcal{Y}|} \right)$$

$$= \mathrm{Col}(Y) + \sum_{y \in \mathcal{Y}} \frac{1}{|\mathcal{Y}|^2} + \sum_{y \in \mathcal{Y}} - 2 \frac{\Pr[Y = y]}{|\mathcal{Y}|}$$

$$= \mathrm{Col}(Y) + \frac{1}{|Y|} - \frac{2}{|Y|}$$

$$\leq \frac{1}{|Y|}\left(1 + 4\varepsilon^2\right) - \frac{1}{|Y|}$$

$$= \frac{4\varepsilon^2}{|Y|}$$

$$SD(Y; U) \leq \frac{1}{2}\sqrt{\frac{4\varepsilon^2}{\cancel{|Y|}} \cdot \cancel{|Y|}} = \varepsilon$$

COMPUTATIONAL SECURITY

Move away from INFORMATION THEORY.

GOAL: Overcome all the limitations we have encountered.

TRADE-OFF: Weaker security.

- Adv is resource-bounded

PROBABILISTIC POLYNOMIAL-TIME TURING MACHINE.

It can use coins (randomness)?

Intuitively: For every input x, every random tape r

$$A(x; r)$$

terminates in some polynomial number of steps in $|x|, |r| = \lambda$

POLYNOMIAL: $p(\lambda) = poly(\lambda)$

$$p(\lambda) = O(\lambda^c) \text{ for some constant } c \in \mathbb{N}$$

- Small probability of not being secure (small as a function of sec. par. λ).

$\hookrightarrow$ for us <u>negligible</u>: $\varepsilon(\lambda) = O(1/p(\lambda))$

for every polynomial $p(\lambda)$.

Examples: $2^{-\lambda}$, $2^{-\lambda/\log\lambda}$

Exercise: If $\varepsilon, \varepsilon' = negl(\lambda)$ then so is:

1) $\varepsilon(\lambda) + \varepsilon'(\lambda)$

2) $p(\lambda) \cdot \varepsilon(\lambda)$ for every $poly(\lambda) = p(\lambda)$

- Introduce computationally hard problems and prove security is equivalent to breaking those problems.