Quiz 9/24

① Suppose a blockcipher E is a PRF. Does PRF security necessarily hold if the key to E is set such that the first half of the bits are zero's? NO

② CTR-\$ generates a "pseudo one-time pad" YES

③ If F is a PRF, then for random K, and random x, from $F_K(x)$ it is hard to guess the first bit of x. yes

④ A mode of operation specifies how to use a blockcipher to encrypt large amounts of data. YES

⑤ If F is a PRF, then necessarily given $F_K(K)$ for random K it is hard to recover K. NO

KDM

G^{*} is a counter example

assume

$$E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$$

define

$$E' : \{0,1\}^{2k} \times \{0,1\}^n \to \{0,1\}^n$$

$$E'_{k_1 \| k_2}(x) = E_{k_1}(x)$$

$k_1 = 00\ldots00$

Let A be the first-bit-guesser. (guesses better than $1/2$)

Define PRF adversary

$B^{Fn(\cdot)}$

$x \xleftarrow{\$} \{0,1\}^n$

$y \leftarrow Fn(x)$

$b \leftarrow A(y)$

If $b = x[1]$ ret 1

Else ret 0

Let $G : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a PRF. Define $G : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$

$$\boxed{G'_K(x)} = \begin{cases} G_K(x) & \text{if } x \neq K \\ K & \text{o.w.} \end{cases}$$

Suppose A is a PRF adversary against G'. Then define B against G:

Adversary $B^{Fn(\cdot)}$

Run A

When A makes query x do:

→ If x is the key half & ret 1

Else ret $Fn(x)$

Until A outputs b

Ret b

(Randomness)

Extractors

Let X, Y be R.V.'s (same domain D)

$X : D \to [0,1]$

$$\sum_{d \in D} \boxed{Pr_X[d]} = 1$$

$X \approx_s Y$

$X \approx_c Y$

For an adversary A define:

$$\boxed{\underline{Adv(A)} = Pr[A(X) \Rightarrow 1] - Pr[A(Y) \Rightarrow 1]}$$

$\underline{\forall A}$ A's advantage is small

$\hookrightarrow$ unbounded $A \to$ statistical

bounded $A \to$ computational

$X \approx_{t, \varepsilon(t)} Y$

Min-entropy

$$-\log \max_{d} \Pr[X=d]$$

Randomness Extractor:

Can we find a function

$$H: \underline{\{0,1\}^n} \to \{0,1\}^m$$

such that

$m << n$ $\qquad \underline{H(X) \approx_s U_m}$ $\qquad$ uniform R.V. on m-bit strings

$\forall$ "high min-entropy" X.

(X takes values from $\{0,1\}^n$)

$S := \{x \in \{0,1\}^n \mid H(x) = 0\}$

Consider X uniform on S

efficient?

$g \cdot h$ $\quad$ $G_{op}(g,h)$

Two ways to get around it:

* Restrict to "efficiently sampleable" sources and computational indistinguishability

Def. H as above is a computational randomness extractor if

$$H(X) \approx_c U_m$$

for all "efficient" high-entropy X.

$$x \xleftarrow{\$} X$$

reasonable assumption:

SHA256 is a computational randomness extractor

* Second way:

Use seeded extractors

$G : \{0,1\}^s \times \{0,1\}^n \to \{0,1\}^m$

$\forall$ high min-entropy X

$$G(\boxed{U_s}, \underline{X}) \approx_s U_m$$

"weak extractor"

$$(t, G(s, X)) \approx (t, U_m)$$

$$t \xleftarrow{\$} \{0,1\}^s$$

"strong extractor"

Leftover Hash Lemma

Pairwise independent hash function family is a strong seeded extractor.

Pairwise Independence:

$H : \{0,1\}^k \times \{0,1\}^d \to \{0,1\}^r$

is pairwise independent if **1**

$\forall x_1, x_2 \in \{0,1\}^d$ $\big(H_k(x_1), H_k(x_2) \big)$

$$\approx$$

$$(U_1 \quad , \quad U_2)$$

where $K \xleftarrow{\$} \{0,1\}^k$

U_1, U_2 are independent on $\{0,1\}^r$

2

$$\Pr_K \big[H_K(x_1) = y_1 \wedge H_K(x_2) = y_2 \big] = \frac{1}{2^{2r}} = \left(\frac{1}{2^r}\right)^2$$

$\forall x_1, x_2 \in \{0,1\}^d$

$\forall y_1, y_2 \in \{0,1\}^r$

Lemma. Let $H : \{0,1\}^k \times \{0,1\}^d \to \{0,1\}^r$ be pairwise independent. Then for all X st $H_\infty(X) \geq 2 \cdot \log(\frac{1}{\varepsilon}) + 1 + r$

$$(K, H_K(X)) \approx_\varepsilon (K, U)$$

min-entropy