Computational Security & Birthday Bounds

HW1 due

Big idea: Breaking security (distinguishing 2 libs)
might be possible in principle, just very hard
(clarify: how hard?)

Last time:

Left
haystack (x \(\xi\):

return false

Iright

Needle $\leftarrow \{0,1\}^{\lambda}$ haystack $(x \in \{0,1\}^{\lambda})$:

return $x \stackrel{?}{=} needle$

Def: Advantage of adversary A is:

Ex: (haystack) If A makes 1 query, then advantage is \leq 1/2x

If A makes 20 queries, then advantage is $\leq \frac{20}{2}$

Q: how big of advantage should we care about??

Def: A function f is negligible if for every polynomial p(x), $\lim_{x\to\infty} p(x) \cdot f(x) \to 0$

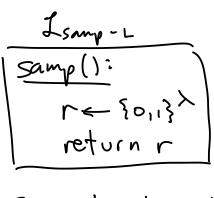
Idea: Suppose A (poly-e) with some advantage f

If I repeat attack p times, resulting attack
is still poly-time (if p is poly) and maybe

has advantage p.f., which should be negligible gresto- $\frac{E\times 2}{2}$ is negligible $\frac{\lambda^{c}}{2^{\lambda}} = \frac{2^{c \log \lambda}}{2^{\lambda}} = 2^{c \log \lambda - \lambda}$ 1/2 is not negligible (x2 / 0) Def: $I_1 \approx I_2$ (libs are indistinguishable) if for all polynomial-time A, the advantage of A is negligible (s) a function of x Ex: the two "haystack" libraries are indistinguishable. If A is poly-time, then # of queries it makes is polynomial in $x \Rightarrow Advantage \leq \frac{p(x)}{2^x} = negl.$ Def: Write $f \approx g$ if |f(x) - g(x)| is negligible

(libraries are indist. if $\forall A: \Pr[A \circ J_1 \Rightarrow 1] \approx \Pr[A \circ J_z \Rightarrow 1]$)

Birthday Bounds



Samp w/ replacement

Samp W/o replacement

Claim: $L_{samp-R} \approx L_{samp-R}$, more precisely, Advantage of A is g(g-1) = 7 if A m

g(g-1) if A makes 2×+1
g queries

(If g is polynomial func of >, advantage is negl.)

<u>Notes</u>: advantage of A ≤ Pr[Lsamp-L repeats an output]

$$\leq \frac{g(q-1)}{2^{\lambda + 1}}$$

Pr[repeated output] = 1 - Pr[all outputs unique]

(call outputs of SAMP: r1, r2, ..., rg)

 $P_r[all outputs unique] = P_r[r_2 \neq r_1] \cdot P_r[r_3 \notin \{r_1, r_2\} \mid r_1 \neq r_2]$ · Pr[ry & {r,... rg} | {r,...rg} distinct)

 $= \left(1 - \frac{1}{2^{2}}\right)\left(1 - \frac{2}{2^{2}}\right)\left(1 - \frac{3}{2^{2}}\right) - \cdots \left(1 - \frac{3^{-1}}{2^{2}}\right)$