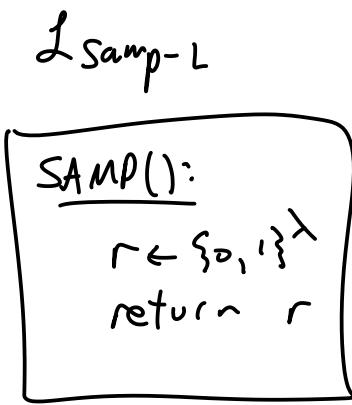


Indistinguishability / Birthday Bounds

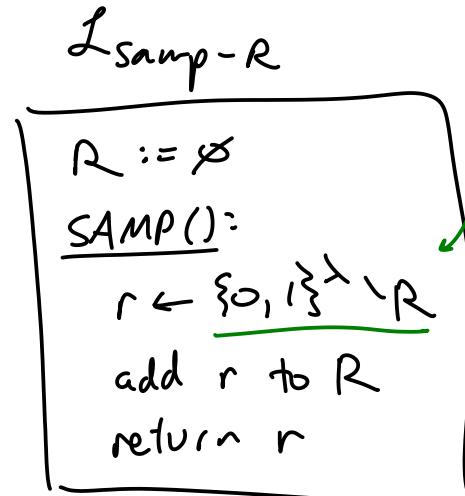
Big Picture:

Previously: Impossible in principle to distinguish libraries
 \Rightarrow information perfectly hidden

"Modern crypto" Just really hard to distinguish
 (comparable to probability of blindly
 guessing a long key)



\approx



all strings
except
ones
in R

"with replacement"

"without replacement"

Since 2 libs are \approx , I can design a crypto scheme that samples values uniformly from $\{0,1\}^\lambda$
 Adv can't tell whether I'm choosing w/ or w/o replacement

\Rightarrow can "just assume" I won't see a repeated value

"Obvious" Distinguisher

A:

```

call SAMP q times
if repeated value, return 1
else return 0
    
```

$$\Pr[A \circ L_{\text{Samp-R}} \Rightarrow 1] = 0$$

$$\Pr[A \circ L_{\text{Samp-L}} \Rightarrow 1] > 0$$

Def:

$\text{CollProb}(q, \lambda) = \text{probability of seeing a repeated output of SAMP in } A \leq \mathcal{L}_{\text{samp}} - L \quad (q \text{ calls to SAMP})$

= Advantage of "obvious distinguisher" A

Claim: No calling program that makes q calls to SAMP can distinguish with advantage better than $\text{CollProb}(q, \lambda)$ (book)

Q: What is $\text{CollProb}(q, \lambda)$?

say s_1, \dots, s_q are indep. samples from $\{0, 1\}^\lambda$

$$\begin{aligned} \Pr[s_1, \dots, s_q \text{ all distinct}] &= \Pr[s_2 \neq s_1] \\ &\times \Pr[s_3 \notin \{s_1, s_2\}] \\ &\times \Pr[s_4 \notin \{s_1, \dots, s_3\}] \\ &\times \dots \end{aligned}$$

$$= \left(1 - \frac{1}{2^\lambda}\right) \left(1 - \frac{2}{2^\lambda}\right) \left(1 - \frac{3}{2^\lambda}\right) \dots \left(1 - \frac{q-1}{2^\lambda}\right)$$

$$\text{CollProb}(q, \lambda) = 1 - \Pr[\text{distinct}]$$

$$= 1 - \prod_{i=1}^q \left(1 - \frac{i-1}{2^\lambda}\right)$$

Approximations

$$0.632 \frac{q(q-1)}{2^{x+1}} \leq \text{Coll Prob}(q, x) \leq \frac{q(q-1)}{2^{x+1}}$$

$$\left(\text{for } q \leq \sqrt{2^{x+1}} \right)$$

In Summary:

take q samples from $\{0, 1\}^x$
 \Rightarrow probability $\Theta\left(\frac{q^2}{2^x}\right)$ of repeat