

Birthday bound $\approx \frac{q^2}{N}$

The probability that q random values from a domain size N has at least one respected pair.

$\Pr[\text{choice 1 matches a prior choice}] = 0$

" " 2 " " " " "] = $\frac{1}{N}$

" " 3 " " " " "] $\leq \frac{2}{N}$

" " 4 " " " " "] $\leq \frac{3}{N}$

" " q " " " " "] $\leq \frac{q-1}{N}$

Summation

$\Pr[\text{any of the first } q \text{ choices match}] \leq \sum = \frac{q(q-1)}{2N}$

Birthday Bound is an upper bound

$< \frac{q^2}{N}$

Distinguishing: Block cipher vs. random permutation

Security bounds: range of possible attack advantages.

- lower bounds: an attacker can achieve at least this much. Show via an attack
- upper bounds: no attacker can do better than this.

Lower bound on Block cipher vs. random permutation

Let $E: \{0,1\}^k \rightarrow (\{0,1\}^b \rightarrow \{0,1\}^b)$ be a block cipher

World 1

$k = \text{random } k \text{ bits}$

$$f = E_k$$

World 2

$f = \{0,1\}^b \rightarrow \{0,1\}^b$ random perm

Distinguish (f):

$$x_0 = f(\langle 0 \rangle)$$

$$x_1 = f(\langle 1 \rangle)$$

for $i = 1$ to t

if $(x_0 = E_{z_i}(\langle 0 \rangle) \text{ and } x_1 = E_{z_i}(\langle 1 \rangle))$

output "block cipher"

output "random perm"

Advantage = $\Pr[\text{output block cipher} \mid f \text{ is block cipher}]$

- $\Pr[\text{output block cipher} \mid f \text{ is random perm}]$

percentage
of keys
tried over
 t time

$$= \frac{t}{2^k} - \left(\frac{1}{2^b} \times \frac{1}{2^b} \right) t$$

$$= \frac{t}{2^k} - \frac{t}{2^{2b}}$$

$$= t \left(\frac{1}{2^k} - \frac{1}{2^{2b}} \right)$$

$\text{Advantage} \approx \frac{t}{2^k}$

Much smaller
than $\frac{1}{2^k}$

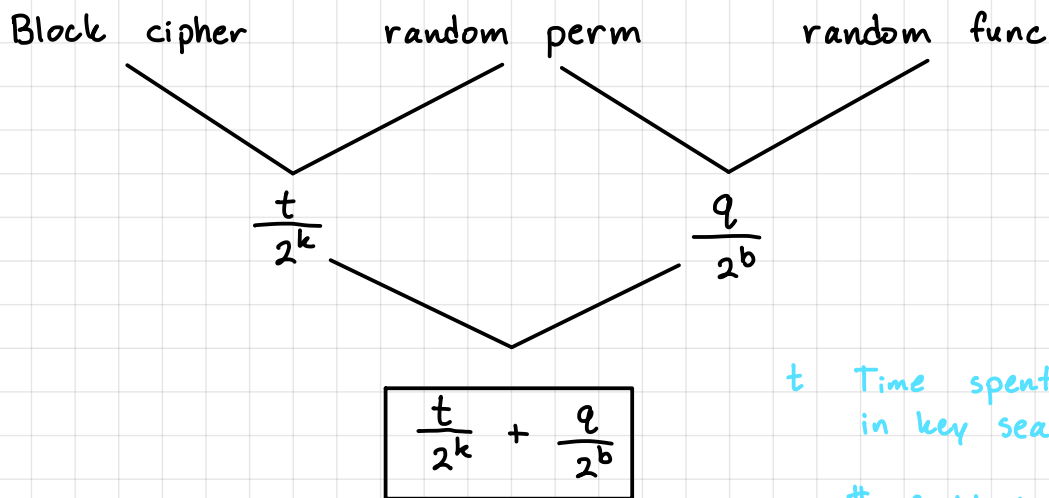
lower bound on Block Cipher Security: $\frac{t}{2^k}$

upper bound on Block Cipher Security: ??? ϵ

// Unknown placeholder for unknown upper bound.

Assume to be
 $\approx \frac{t}{2^k}$ for a
good block cipher

Distinguishing: Block cipher vs. random function



t Time spent offline in key search

q # of black box invocations

Upper bound on CTR encryption: no adversary can do better

* Proven via "reduction"

Let f be either a block cipher with random key or a random function

BCDistinguisher (f)

let g = CTR encryption using f

if Real or Random Distinguisher (g) = "real"

output "block cipher"

else

output "random function"

A Reduction

If RRDist exist, then BCDist exists

Note: if f is a block cipher, then g is exactly CTR mode

if f is a random function, then g output uniform random bits

These are the two worlds a real or random distinguisher looks as.

if $\text{BCDistinguisher adv} < x$, then $\text{RRDistinguisher adv} < x$

$$\text{BCDistinguish advantage} < \frac{t}{2^k} + \frac{q}{2^b}$$

$$\text{so RRDistinguisher adv} < \frac{t}{2^k} + \frac{q}{2^b}$$

* Reductions will not be studied in this class