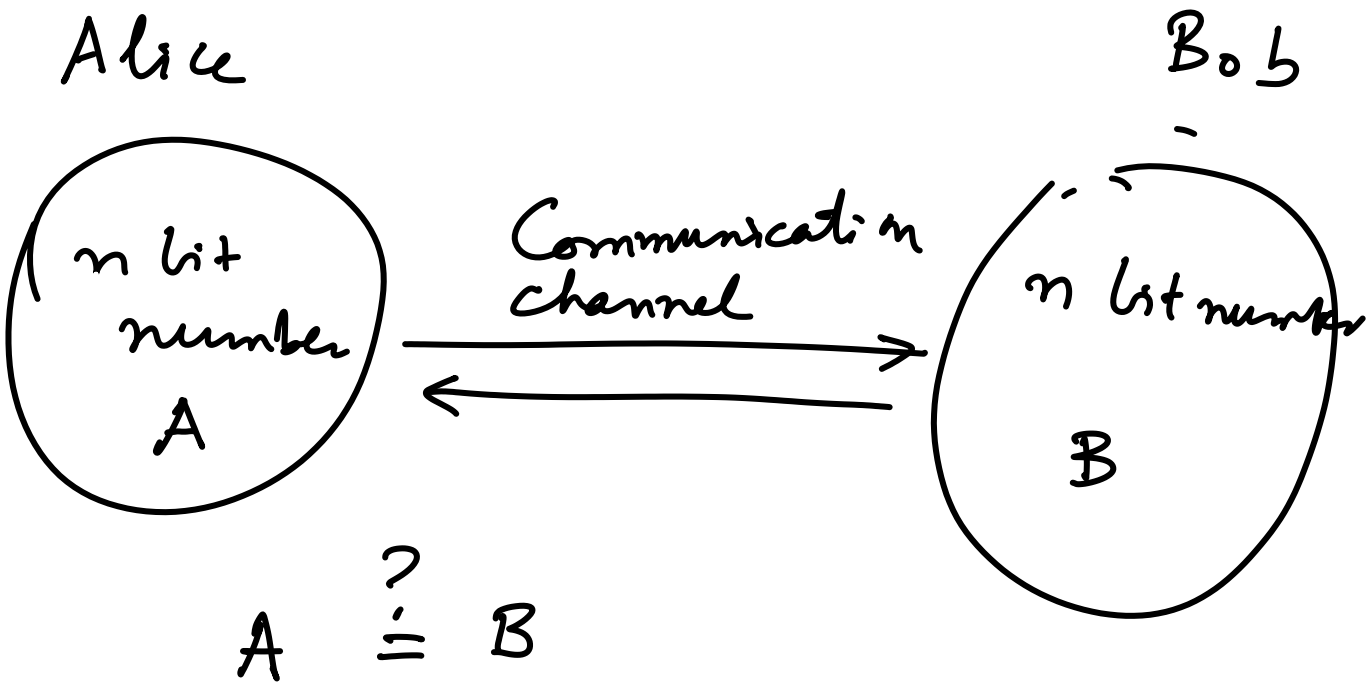
CSL 356 Lecture 34 Oct 29



without exchanging all the n bits

$f : N \to N$

$f(A)$ and $f(B)$ are much smaller than A/B

$A = B$ iff $f(A) = f(B)$

(fingerprints)

If $f(A) \neq f(B)$ then $A \neq B$

If $f(A) = f(B)$ then $\boxed{A = B}$ * with prob. $\frac{1}{2}$

We look at a function f of the form $f(n) = n \bmod p$ where p is prime.

We choose p to be "sufficiently" large but $\ll n$

Clearly $f(A) = f(B)$ if $|A - B| \equiv_p 0$

Observation: An n bit number has at most n prime factors.

Let us choose p as a random prime among $p_1, p_2, p_3, \ldots, p_{2n}$ where p_i is the i^{th} prime

What is the probability that $|A - B|$ is a multiple of p?

$\leq \frac{1}{2}$

What is the size of the $f(A)$?

$\leq \|p\|$ i.e. no. of bits in p

From prime no density theorem, there must be $2n$ primes among the first $2n \ln n$ integers

$\Rightarrow$ the integers have no more than $\log(2n \ln n)$

$\leq 2 \log n$ bits

Rabin-Karp pattern Match

$f(i) = \max_{j<i} X(j)$ (in a suffix of $X(i)$) $\sqsubset$

↑ function of