So far: Kerckhoff's Principle, need for deep math; Shannon's pessimistic theorem → Perfection: $|M| \leq |K|$, → Limited by bandwidth of secure (symm. key) channel (if it exists) (public key); Two necessary relaxations: PPTM adversary, negligible error probability; (Almost) sufficient → PRG ⟺ Security against eavesdropping

PRG not constructed from scratch, but provably secure since it relies on a hard problem.

One Way Function:

A function $f: \{0,1\}^* \to \{0,1\}^*$ is one-way if: family of

a) Easy to compute: $\exists$ PPTM M s.t. $\forall x$, $|x|=n$ $P[M(x)=f(x)] \geq 1 - negl(n)$

b) Hard to invert: $\forall$ PPTM A, $\forall x$ s.t. $|x|=n$, $P[A(f(x))=y \text{ s.t. } f(y)=f(x)] \leq negl(n)$

Discrete Logarithm Problem (DLP):

This course will use DLP as a running ex. for one way fns.

$(G, \cdot)$ is a group if

Closure: $\forall x, y \in G$, $x \cdot y \in G$

Associativity: $\forall x,y,z \in G$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$

Identity: $\exists e \in G$ s.t. $\forall x$, $e \cdot x = x \cdot e = x$

Inverse: $\forall x \in G$, $\exists y \in G$ s.t. $x \cdot y = y \cdot x = e$

Quantum Field Theory } is dependent on group theory
Error correction codes }

Input: A finite cyclic group $\langle G, \cdot \rangle$, $g, y \in G$.

Ex: Integer modulo prime under multiplication.

Output: $\log_g y$ i.e. x s.t. $g^x = y$

Ex: $Z_p^* : \langle \{1,2,3,\ldots p-1\}, * \pmod p \rangle$

Ex: $p=5$, $Z_5 = \{1,2,3,4\}$, $g=2$

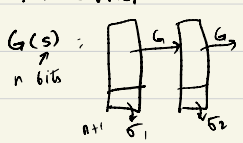
$\{2^1, 2^2, 2^3, 2^4\} \bmod 5 = \{2,4,3,1\}$

Solving DLP is $O(p)$, but here p is $O(2^n)$ where n is the number of bits to represent p.

Building a PRG from DLP:

A PRG that extends by 1 bit can be used to create a PRG that extends by any no. of bits $G: \{0,1\}^n \to \{0,1\}^{n+1}$

If G is a PRG:



$r_1\ r_2 \ldots r_{\ell(n)}$ Row 1

$\sigma_1\ r_2 \ldots r_{\ell(n)}$

$\sigma_1\ \sigma_2 \ldots \sigma_{\ell(n)}$ Row last

If an adversary can distinguish b/w first & last row then it can distinguish b/w 2 adjacent rows (use contradiction) & thus can distinguish b/w the expansion of 1 bit by G & truly random & G is thus not a PRG.

$f(x) = g^x \bmod p$

$G(x) = f(x) \| h(x)$ → what?

↳ pad

Given $f(x)$, $\forall$ PPTM A

$P(A(f(x)) = h(x)) \leq 1/2 + \text{negl}(|x|)$

$h(x)$: hardcore predicate of f : Given $f(x)$, bit whose preimage is hardest to get.

Ex: Given $g^x \bmod p$,

$$h(x) = \begin{cases} 0 & \text{if } x < \frac{p-1}{2} \\ 1 & \text{if } x \geq \frac{p-1}{2} \end{cases}$$