So for in this course, we have shown that PRF => CPA-secure encryption => authenticated => secure MAC From HW1, we saw how to construct a PRF from a (length-doubling) PRG

[can be built from any PRG with 1-bit stretch

Question: Can we distill this further? Can we have symmetric cryptography on an even simpler primitive? - Cryptography is about exploiting some kind of asymmetry: we want an operation that is "easy" for honest users, but hard for adversaries - Suggests a notion of "hard to invert": (cannot recover seed from PRG, cannot decrypt without) (knowledge of secret, etc.

Definition. A function $f: X \rightarrow Y$ is one-way if I. f is efficiently computable 2. for all efficient adversaries A: $Pr[X \ll X, y \leftarrow A(f(x)): f(x) = f(y)] = negl(x)$ Function is hard to invert on average

<u>Theorem</u> (Håstad-Impagliazzo-Levin-Luby). OWF => PRG ('implies OWF is sufficient (and necessary) for symmetric cryptography

We will consider a weaker statement: one-way permutation => PRG

<u>Definition</u>. A function $f: X \rightarrow X$ is a one-way permutation if h f is one-way 2. f is a permutation

Definition. Let $f: X \rightarrow Y$ be a one-way function. Then $h: X \rightarrow R$ is a hand-core predicate for f if no efficient adversary can distinguish the following distributions: $D_0: \{x \not\in X : (f(x), h(x)) \\ D_1: \{x \not\in X, r \not\in R : (f(x), r)\}$

If a OWP has a hard-core predicate, that immediately implies a PRG: Typically, we will consider hard-core bits PRG(s):= f(s) || h(s) (i.e., R = {0,13})

<u>Lemma</u>. Let $f: X \rightarrow Y$ be a one-way function. Suppose $h: X \rightarrow \{0, 1\}$ is unpredictable in the following sense: for all efficient adversaries A: $\left| \Pr\left[x \in X : A(f(x)) = h(x) \right] - \frac{1}{2} \right| = negl(\lambda)$

If h is unpredictable, then it is a hard-core bit. [Note: Converse of this is immediate]

Theorem (Gold reich-Levin). Let $f: \{0, 1\}^n \rightarrow \{0, 1\}^n$ be a one-way function. For a string $\tau \in \{0, 1\}^n$, define the function $h_r: \{0, 1\}^n \rightarrow \{0, 1\}$ where $h_r(x) = \sum r_i x_i \pmod{2}$. Then the function g(x, r) := (f(x), r)is one-way and hr is a hard-core predicate for g.

Observe that if f is a OWP, then so is g

Proof Idea. One-wayness of g immediately follows from one-wayness of f. Suffices to show that he is hard-core. Suppose that her is not a hard-core predicate for g. This means that there is an adversary A. that can predict h_r given (f(x), r) with probability $\frac{1}{2} + \varepsilon$. We will use g to construct an adversary B that can invert f (and thus g).

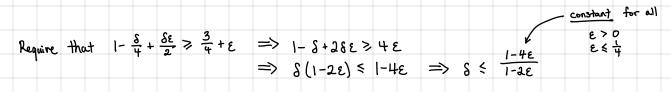
Suppose now that A succeeds with probability $3/4 + \varepsilon$ for constant $\varepsilon > 0$: Evaluating at $e_1, ..., e_n$ not guaranteed to work since A could be wrong on all of these inputs

Analysis proceeds in two steps:

$$\sum_{k \in \mathbb{N}} \sup_{x \in \mathbb{N}} \sum_{k \in \mathbb{N}} \sup_{x \in \mathbb{N}} \sum_{k \in \mathbb{$$

If A succeeds on $(\frac{3}{4} + \epsilon)$ - fraction of x's, cannot have too many bad x's. (Averaging argument). Suppose S fraction of x's are bad. Then, probability of A succeeding over choice of $x, r \in \{0, 1\}^n$ is at most

$$S\left(\frac{3}{4} + \frac{\varepsilon}{2}\right) + (1 - \delta)$$
$$= 1 - \frac{\delta}{4} + \frac{\delta\varepsilon}{2}$$



Conclusion: At most constant fraction is "bad" so inversion will succeed on constant fraction of inputs,

HW3: Show how to go from $\frac{3}{4} + \varepsilon$ to $\frac{1}{2} + \varepsilon$ for constant $\varepsilon > 0$