Take away one-way functions

1. Practically almost “useless” security definition
    - Can leak half of its input
    - Cannot hide short inputs
    - Does not capture confidenfiality to any reasoneable degree

2. Conceptual essence of hardness I
    - OWFs imply PRGs, PRFs, MACs, ENC…

3. Conceptual essence of hardness II
    - Most crypto primitives imply OWFs

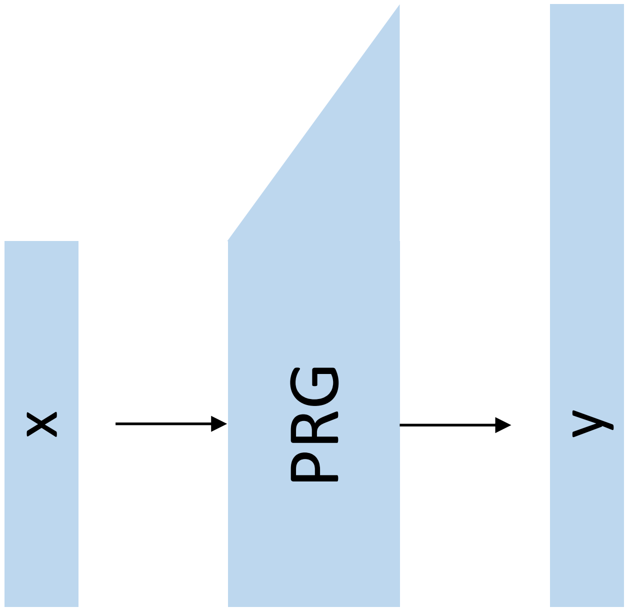
Take away pseudorandom generators (PRG)

1. Generate pseudorandom bits in systems
    - Systems don’t provide *uniform* randomness
    - Need to extract from whatever is provided by the environment
    - PRGs allow to obtain as much randomness as we like

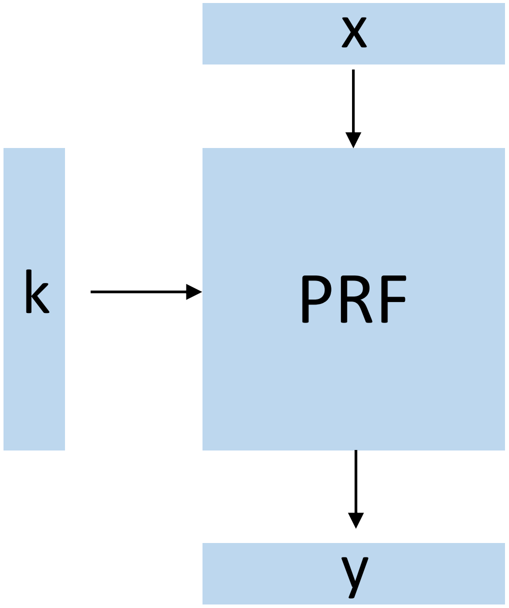
2. PRGs are deterministic
    - (since they mitigate the “insufficient randomness” problem)

3. PRGs are length-expanding
    - (since we want to get *more* randomness than we have, not less)

PRG vs. PRF



single-use



multi-use

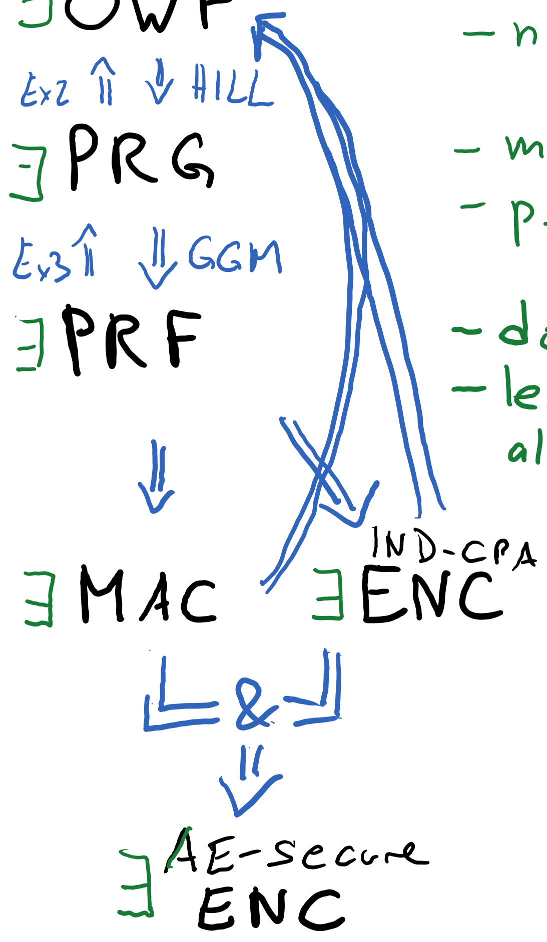
Take away pseudorandom functions (PRFs)

1. Cipher = length-preserving PRF
   - PRF: only forward-direction, also called stream cipher
   - PRP: can be efficiently evaluated in both direction, also called block cipher
   - Main state-of-the-art block cipher: AES
2. Length-expansion is not trivial
   - Need to be careful with length-extension attacks
   - HMAC turns a cipher into an arbitrary input-length PRF
3. Used in most symmetric-key applications
   - Message authentication codes (MACs)
   - Symmetric encryption
   - Often, even PRGs are implemented using ciphers
   - Hash-functions usually rely on ciphers as smaller building blocks.
   - ...

Take away message authentication codes (MACs)

1. Protect integrity and authenticity
2. Used in authenticated channels.
3. Usually implemented by a PRF
    - An unknown pseudorandom value is hard to guess

Cryptographic Primitives



- might reveal input
- not pseudorando

- might reveal input
- pseudorandom

- do not leak input
- leak repetitions/ allow to check value

Constructions

- $f(x_{1...|x|/2}) \| x_{|x|/2...|x|}$
- $f(x) \| 0...0$
- $g(x_{1...|x|/2}) \| x_{|x|/2...|x|}$
- $\underbrace{\overset{?}{f}(x)}_{\text{bijective length-pres. OWF}} \| r \| \underbrace{hb_{GL}(x,r)}_{\bigoplus_{i=1}^{|x|} x_i \wedge r_i}$
- f_{GGM}: binary tree + length-doubling PRG
- m.mac$(k,x) :=$ prf(k,x)
  m.ver$(k,x,t) :=$ (prf$(k,x) \overset{?}{=} t$)

• Techniques

- defining properties (search / decision)
- generic counterexamples
- reductions
- games & packages
- game hopping

Notation:

∃A ⇒∃ : The existence of **A** implies the existence of **B**.

∃A ⇐∃ : The existence of **B** implies the existence of **A**.

∃A ⇔∃ : **A** exists if and only if **B** exists.