Symmetric-Key Encryption: constructions

Lecture 5

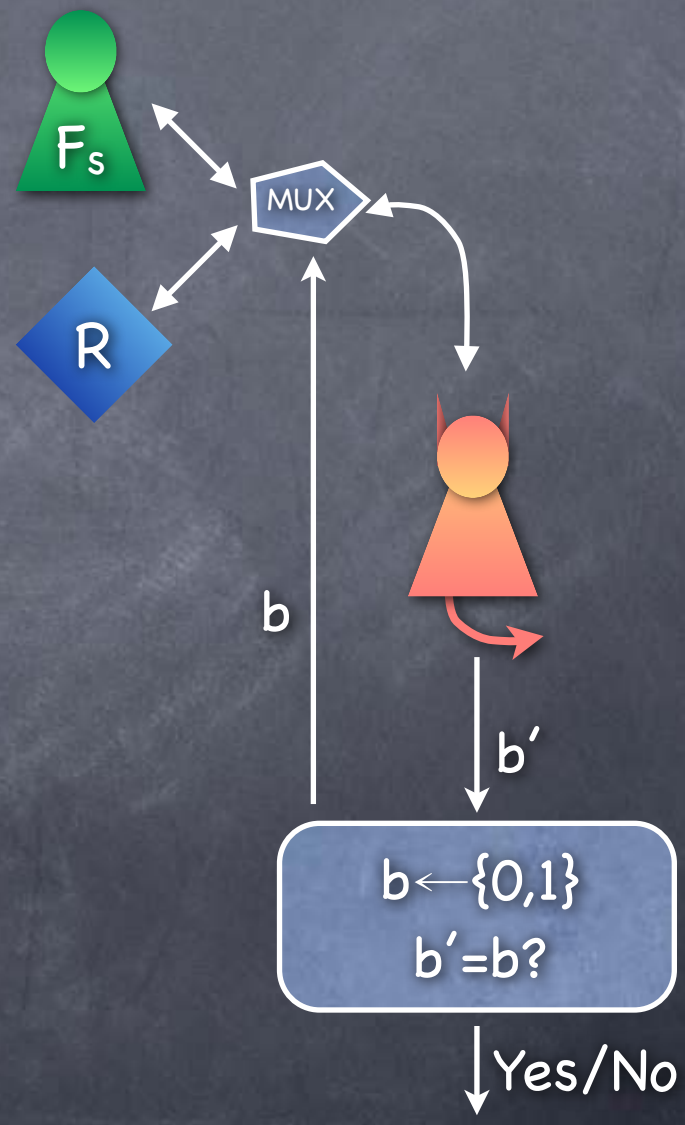
Block Cipher Modes

Theoretical Constructions of PRFs

RECALL

Pseudorandom Function (PRF)

- F: $\{0,1\}^k \times \{0,1\}^m \rightarrow \{0,1\}^n$ is a PRF if all PPT adversaries have negligible advantage in the PRF experiment
  - Adversary given oracle access to either F with a random seed, or a random function R: $\{0,1\}^m \rightarrow \{0,1\}^n$. Needs to guess which.
  - Note: Only 2^k seeds for F
    - But 2^(n2^m) functions R
  - PRF stretches k bits to n2^m bits



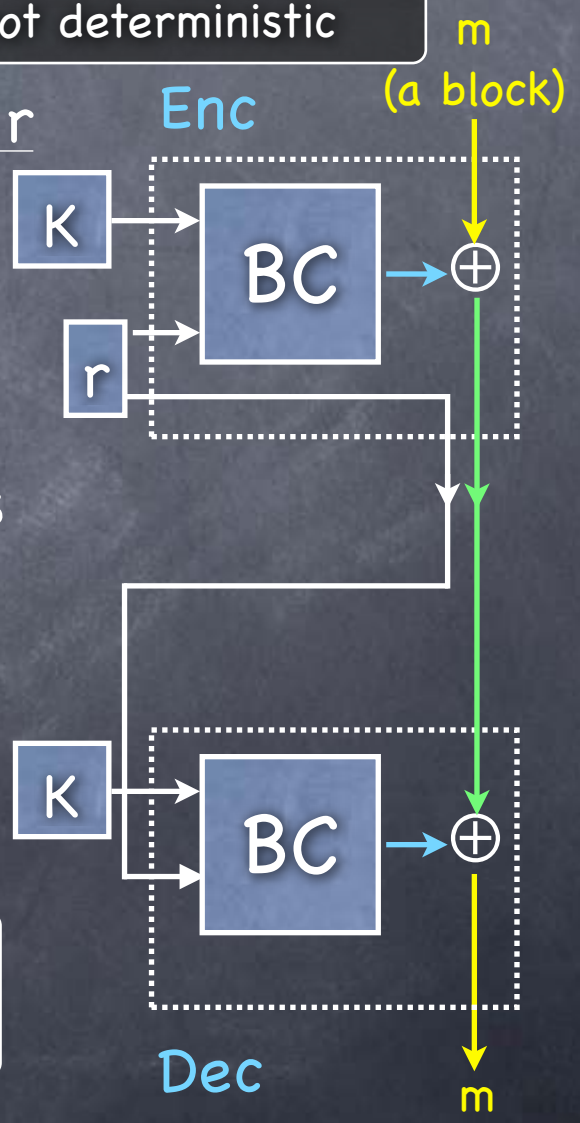
RECALL

CPA-secure SKE with a PRF (or Block Cipher)

- Key = Seed for a block-cipher (or PRF) BC
- To encrypt a block message: pick a random value r and set ciphertext = $(r, BC_K(r) \oplus m)$
- Idea for CPA security:
  - If we modify the CPA security experiment to use random z_i instead of $BC_K(r_i)$, adversary has zero advantage
  - When K is randomly chosen (hidden from the adversary), for random $r_1, r_2, \ldots$, $(r_i, BC_K(r_i)) \approx (r_i, z_i)$ where z_i are random, provided BC is a PRF

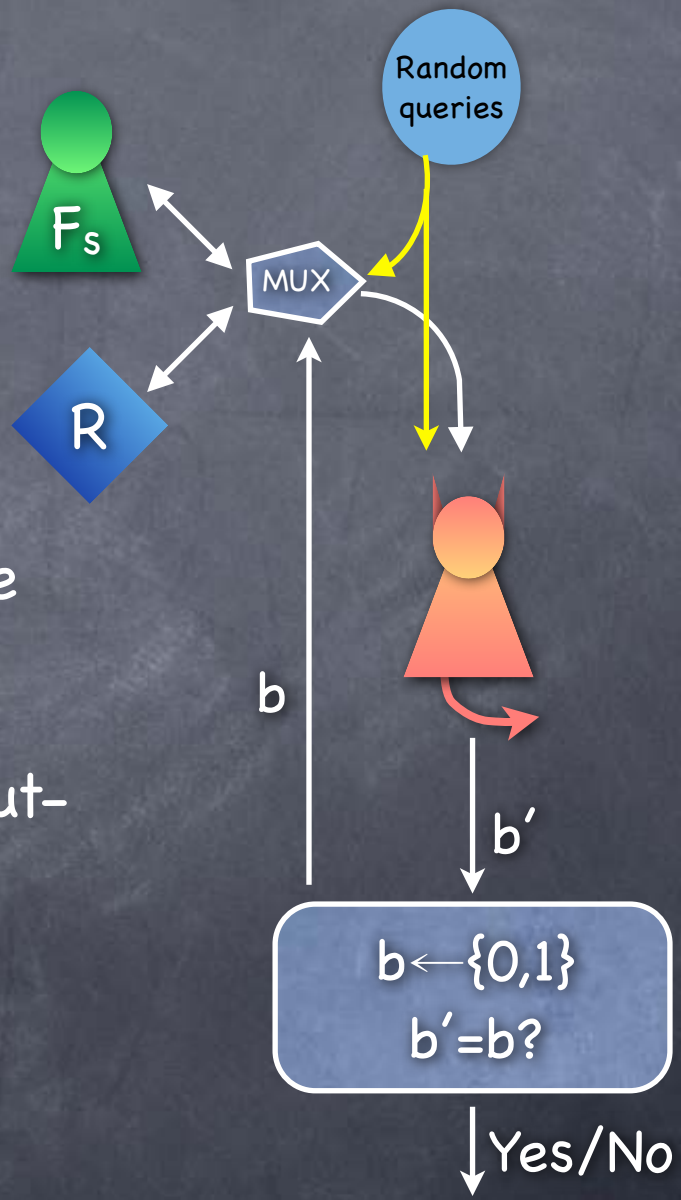
For CPA security, essential that encryption is not deterministic

PRF would work even if r_i are simply distinct



Weak PRF

- Weak PRF: Similar to PRF, but the inputs to the oracle are chosen randomly
  - The adversary does not get to choose the inputs
  - As in the case of a PRF, adversary can see both the input and the output
  - As before, adversary can see as many input-output pairs as it wants
- In a Weak PRF, there can be discernible correlations between say, $F_S(r)$ and $F_S(r+1)$
- Weak PRF suffices for CPA-secure SKE

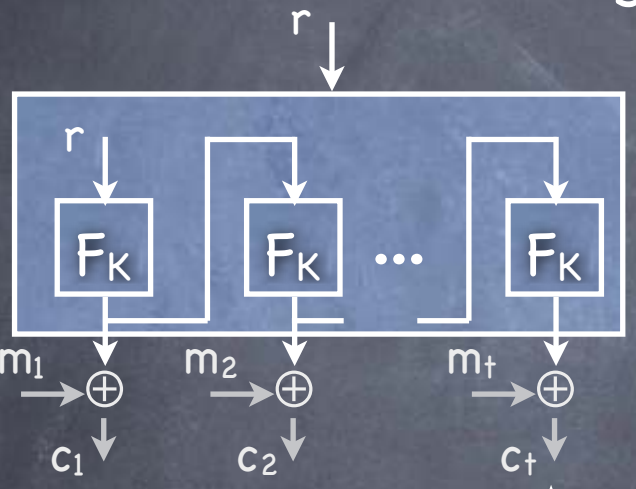


CPA-secure SKE with a Block Cipher

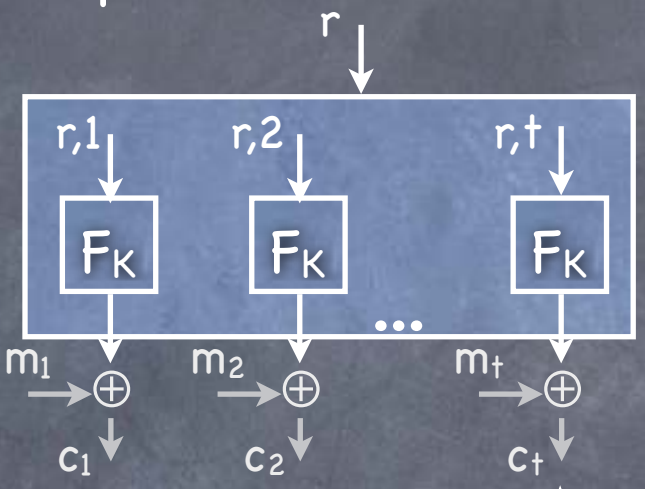
- How to encrypt a long message (multiple blocks)?
  - Chop the message into blocks and independently encrypt each block as before?
  - Works, but ciphertext size is double that of the plaintext (if r is one-block long)
- Extend output length of a PRF (w/o increasing input length)
  - Enough to obtain a weak PRF, starting from a PRF
  - Several ways (coming up)
  - Results in different encryption schemes using a block-cipher, all with one block overhead

CPA-secure SKE with a Block Cipher

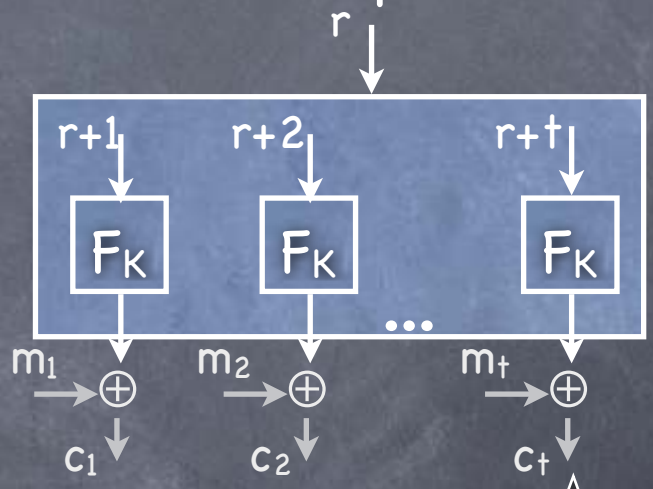
- A weak PRF with a long output from a PRF with a block output



Output Feedback (OFB) mode
Sequential. Weak PRF.

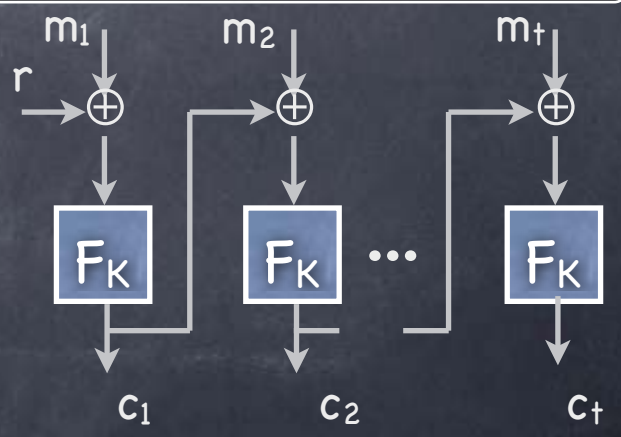


PRF. Shorter input. A priori bound on output length.



Counter (CTR) mode
Weak PRF. Supports variable length output

- Not all modes follow the template of pseudorandom one-time pad.
- **Cipher Block Chaining (CBC) mode:**
  - Invented in 1976. Encryption is sequential. Decryption uses F_K^{-1}. Ciphertext needs to be an integral number of blocks.



A Word of Caution

- In describing block-ciphers, the terminology commonly used is misleading
  - Applying the PRF is called "encryption"
  - The PRF is required to be efficiently invertible using the key, and inverting it is called "decryption"
  - Input to the PRF is called "plaintext" and its output is called the "ciphertext"

Electronic Codebook (ECB) mode

Ciphers in Practice

Stream Ciphers

- A key should be used for only a single stream
- RC4, eSTREAM portfolio, ...
- In practice, stream ciphers take a key and an "IV" (initialization vector) as inputs
  - Heuristic goal: behave somewhat like a PRF (instead of a PRG) so that it can be used for multi-message encryption
  - But often breaks if used this way
- NIST Standard: For multi-message encryption, use a block-cipher in CTR mode

Also used to denote the random nonce chosen for encryption using a block-cipher

Block Ciphers

- DES, 3DES, Blowfish, AES, ...
  - Heuristic constructions
  - Permutations that can be inverted with the key
    - PRFs that are permutations are called PRPs
  - Speed (hardware/software) is of the essence
  - But should withstand known attacks
    - As a PRP (or at least, against key recovery)

Block Ciphers

- Data Encryption Standard (DES)
  NIST Standard. 1976
- DES has short key/block lengths (56 bits and 64 bits), and has been broken since late 90's
  - By 2006, brute-force key recovery using $10K hardware, running for under a week. By now, in under a day; 1-2 days in general purpose GPUs.
  - Remedies: DES-X uses extra keys to pad input and output. Triple DES uses 3 successive applications of DES (or DES^{-1}) with 3 keys
- Advanced Encryption Standard (AES)
  NIST Standard. 2001
  - AES-128, AES-192, AES-256 (3 key sizes; block size = 128 bits)
  - Very efficient in software implementations (unlike DES)
  - Some implementations may lead to side-channel attacks (e.g. cache-timing attacks). Countered by using AES instruction set (available in x86, ARM, RISC-V, ...)
  - Widely considered secure, but no "simple" hardness assumption known to imply any sort of security for AES

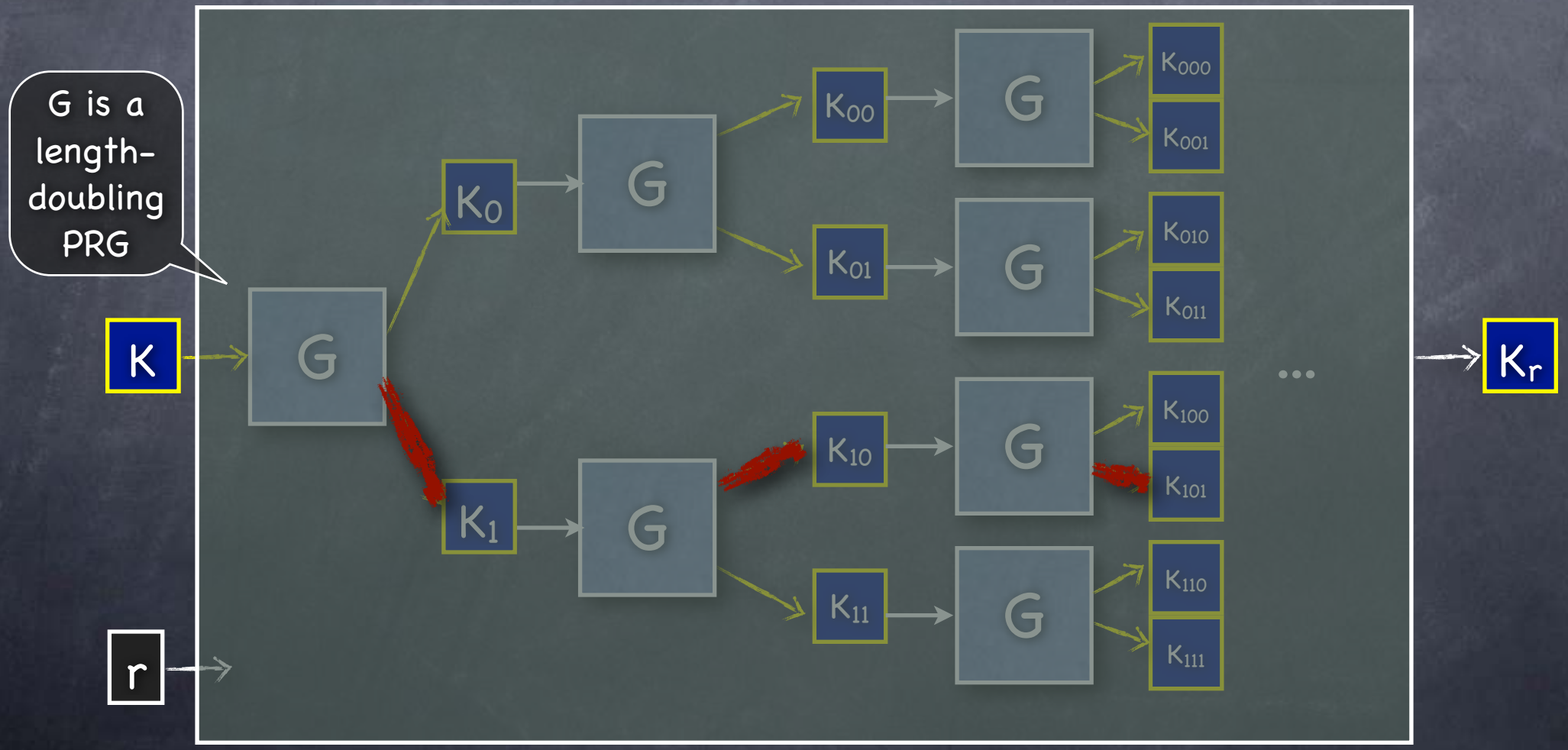
Cryptanalysis

- Attacking stream ciphers and block ciphers
  - Typically for key recovery
- Brute force cryptanalysis, using specialized hardware
  - e.g. Attack on DES in 1998
- Several other analytical techniques to speed up attacks
  - Sometimes "theoretical": on weakened ("reduced round") constructions, showing improvement over brute-force attack
  - Meet-in-the-middle, linear cryptanalysis, differential cryptanalysis, impossible differential cryptanalysis, boomerang attack, integral cryptanalysis, cube attack, ...
- Side-channel attacks on implementations

Theoretically Secure Constructions of PRG & PRF

PRF from PRG

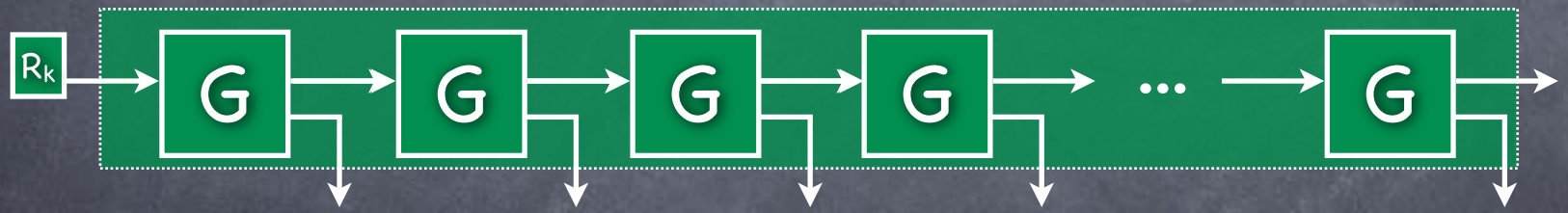
- A PRF can be constructed from any PRG



PRG from 1-Bit Stretch PRG

- Suppose given a t-bit stretch PRG, G_k: $\{0,1\}^k \rightarrow \{0,1\}^{k+t}$ $(t \geq 1)$

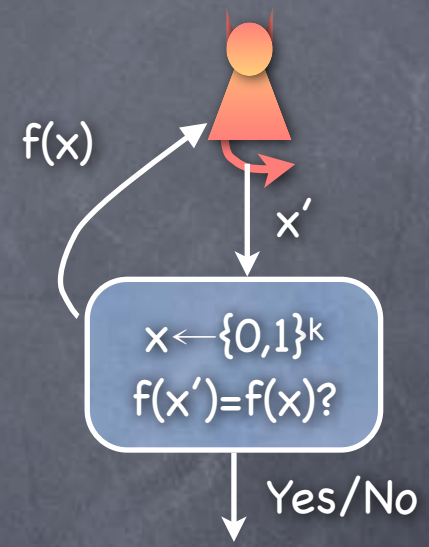
- Increasing the stretch
  - Can use part of the PRG output as a new seed



- How to build a 1-bit stretch PRG?
  - "HILL theorem" (1989): Can be constructed from any One-Way Function (OWF)
  - Coming up: Construction from One-Way Permutation

One-Way Function

- $f: \{0,1\}^k \to \{0,1\}^n$ is a one-way function (OWF) if
  - f is efficiently computable
  - For all (non-uniform) PPT adversary, probability of success in the "OWF experiment" is negligible
  - Note: x may not be completely hidden by f(x)



- Several candidates:
  - Multiplication of two prime numbers $f_{mult}(x,y) = x \cdot y$
  - Subset sum $f_{subsum}(x_1 \ldots x_k, S) = (x_1 \ldots x_k, \sum_{i \in S} x_i)$
  - Exponentiation in certain multiplicative groups $f_{exp}(g,x) = (g, g^x)$
  - RSA function, Rabin function, Goldreich's function, ...
- A one-way permutation is a one-way function that is also a bijection

1-Bit Stretch PRG from OWP

- One-bit stretch PRG, G: $\{0,1\}^{2d} \rightarrow \{0,1\}^{2d+1}$
  - G(x,r) = (f(x), r, <x,r>)
  - Where f: $\{0,1\}^d \rightarrow \{0,1\}^d$ is a one-way permutation, and <x,r> denotes the inner product (mod 2)

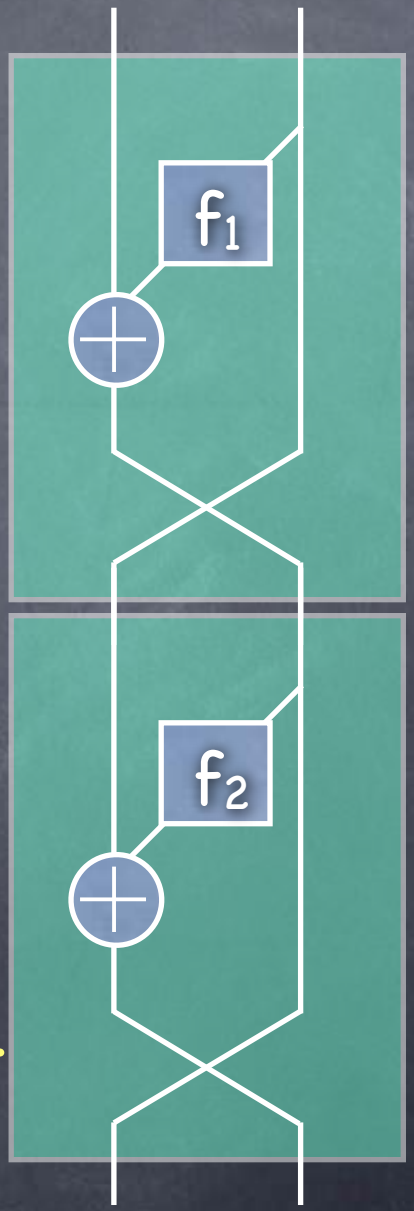
- Claim: G is a PRG
  - Goldreich-Levin Theorem: If f is a one-way function, then if (x,r) is sampled uniformly at random, <x,r> is unpredictable given (f(x), r)
  - Now, for uniformly random x, f(x) is also uniform (since f is a permutation), and hence all of (f(x), r) is next-bit unpredictable. Finally, <x,r> is unpredictable given (f(x), r)

Theoretical Constructions: Summary

- Starting from a OWP (or even OWF) one can construct a PRF
  - OWP → 1-bit stretch PRG → Length doubling PRG → PRF
- Weak PRF is enough for SKE, but block cipher provides more structure: permutations that are invertible given the key
  - Further, assumed to be indistinguishable from a random permutation, even if the adversary has access to the inversion oracle as well: called a Strong PRP
  - A "Feistel network" can be used to transform a PRF into a (strong) PRP

Feistel Network

- Building a permutation from a (block) function
  - Let $f: \{0,1\}^m \rightarrow \{0,1\}^m$ be an arbitrary function
  - $F_f: \{0,1\}^{2m} \rightarrow \{0,1\}^{2m}$ defined as $F_f(x,y) = (y, x \oplus f(y))$
    - F_f is a permutation (Why?)
      - Can invert (How?)
        - As efficient as computing f
  - Given functions $f_1,\ldots,f_t$ can build a t-layer Feistel network $F_{f1\ldots ft}$
    - Still a permutation from $\{0,1\}^{2m}$ to $\{0,1\}^{2m}$
- **Luby-Rackoff**: A 3-layer Feistel network with PRFs (with independent seeds) as round functions is a PRP. A 4-layer Feistel of PRFs gives a strong PRP.
  - Fewer layers do not suffice!



Theoretical Constructions: Summary

- Starting from a OWP (or even OWF) one can construct a PRF
  - OWP → 1-bit stretch PRG → Length doubling PRG → PRF
- Weak PRF is enough for SKE, but block cipher provides more structure: permutations that are invertible given the key
  - Further, assumed to be indistinguishable from a random permutation, even if the adversary has access to the inversion oracle as well: called a Strong PRP
  - A "Feistel network" can be used to transform a PRF into a (strong) PRP