Symmetric-Key Encryption: constructions

Lecture 4

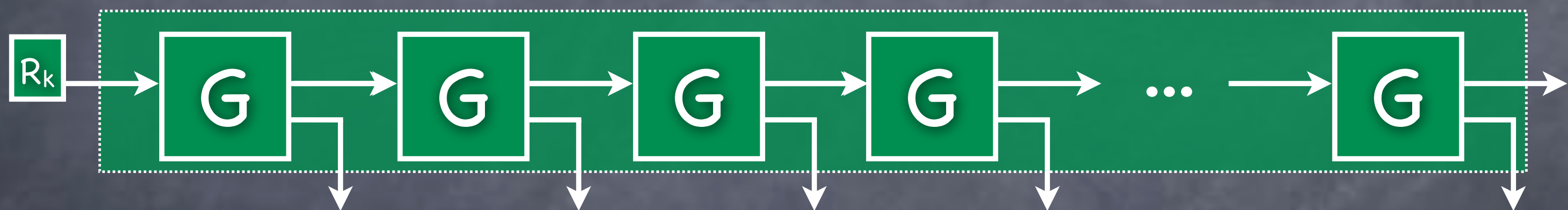
PRF, Block Cipher

RECALL

PRG from One-Way Permutations

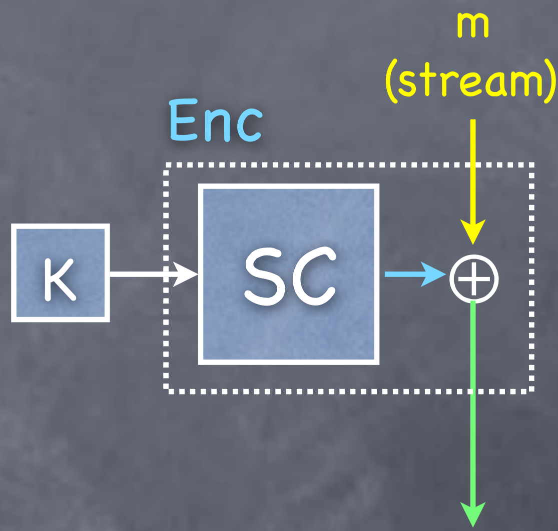
- One-bit stretch PRG, G_k: $\{0,1\}^k \rightarrow \{0,1\}^{k+1}$

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



  - If the intermediate seeds are never output, can keep stretching on demand (for any "polynomial length")
  - A stream cipher

One-time CPA-secure SKE with a Stream-Cipher



- One-time Encryption with a stream-cipher:
  - Generate a one-time pad from a short seed
  - Can share just the seed as the key
  - Mask message with the pseudorandom pad
- Security: indistinguishability from using a real random pad
- If SC can spit out bits on demand, the message can arrive bit by bit, and the length of the message doesn't have to be a priori fixed

Beyond One-Time?

- Need to make sure same part of the one-time pad is never reused
  - Sender and receiver will need to maintain state
    - Or Sender can send the index, but then receiver will need to run the stream-cipher to get to that index
    - A PRG with direct access to any part of the output stream?
- Pseudo Random Function (PRF)

Pseudorandom Function (PRF)

Pseudorandom Function (PRF)

- A compact representation of an exponentially long (pseudorandom) string

Pseudorandom Function (PRF)

- A compact representation of an exponentially long (pseudorandom) string
  - Allows "random-access" (instead of just sequential access)

Pseudorandom Function (PRF)

- A compact representation of an exponentially long (pseudorandom) string
  - Allows "random-access" (instead of just sequential access)
    - A function F(s;i) outputs the i^{th} block of the pseudorandom string corresponding to seed s

Pseudorandom Function (PRF)

- A compact representation of an exponentially long (pseudorandom) string
  - Allows "random-access" (instead of just sequential access)
    - A function F(s;i) outputs the i^{th} block of the pseudorandom string corresponding to seed s
    - Exponentially many blocks (i.e., large domain for i)

Pseudorandom Function (PRF)

- A compact representation of an exponentially long (pseudorandom) string
  - Allows "random-access" (instead of just sequential access)
    - A function F(s;i) outputs the i^{th} block of the pseudorandom string corresponding to seed s
    - Exponentially many blocks (i.e., large domain for i)
- Pseudorandom Function

Pseudorandom Function (PRF)

- A compact representation of an exponentially long (pseudorandom) string
  - Allows "random-access" (instead of just sequential access)
    - A function F(s;i) outputs the i^{th} block of the pseudorandom string corresponding to seed s
    - Exponentially many blocks (i.e., large domain for i)
- Pseudorandom Function
  - Need to define pseudorandomness for a function (not a string)

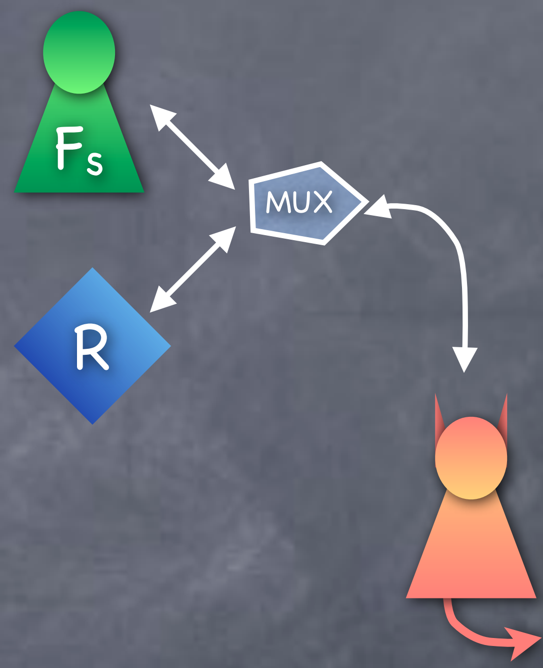
Pseudorandom Function (PRF)

Pseudorandom Function (PRF)

- F: $\{0,1\}^k \times \{0,1\}^{m(k)} \rightarrow \{0,1\}^{n(k)}$ is a PRF if all PPT adversaries have negligible advantage in the PRF experiment

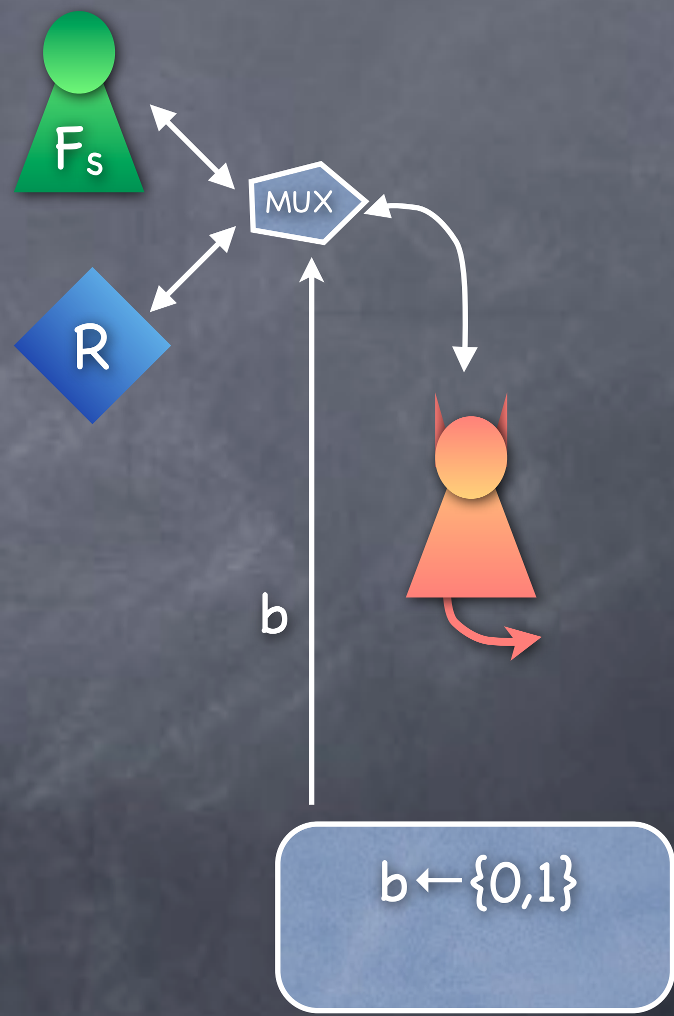
Pseudorandom Function (PRF)

- F: $\{0,1\}^k \times \{0,1\}^{m(k)} \rightarrow \{0,1\}^{n(k)}$ 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. Needs to guess which.



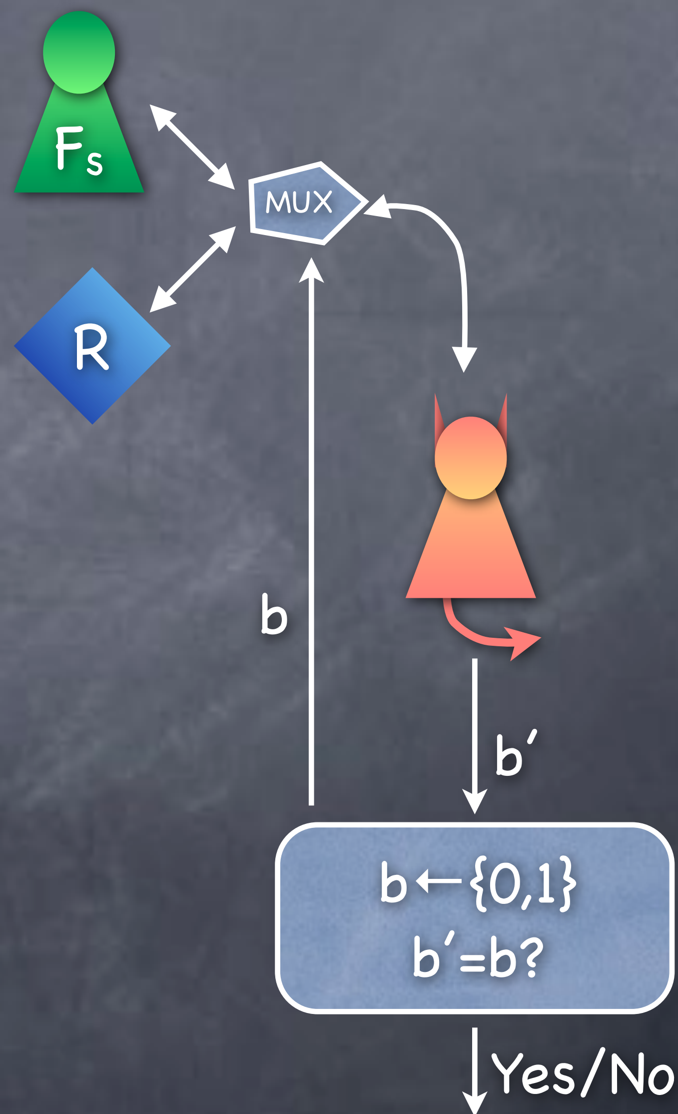
Pseudorandom Function (PRF)

- F: $\{0,1\}^k \times \{0,1\}^{m(k)} \rightarrow \{0,1\}^{n(k)}$ 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. Needs to guess which.



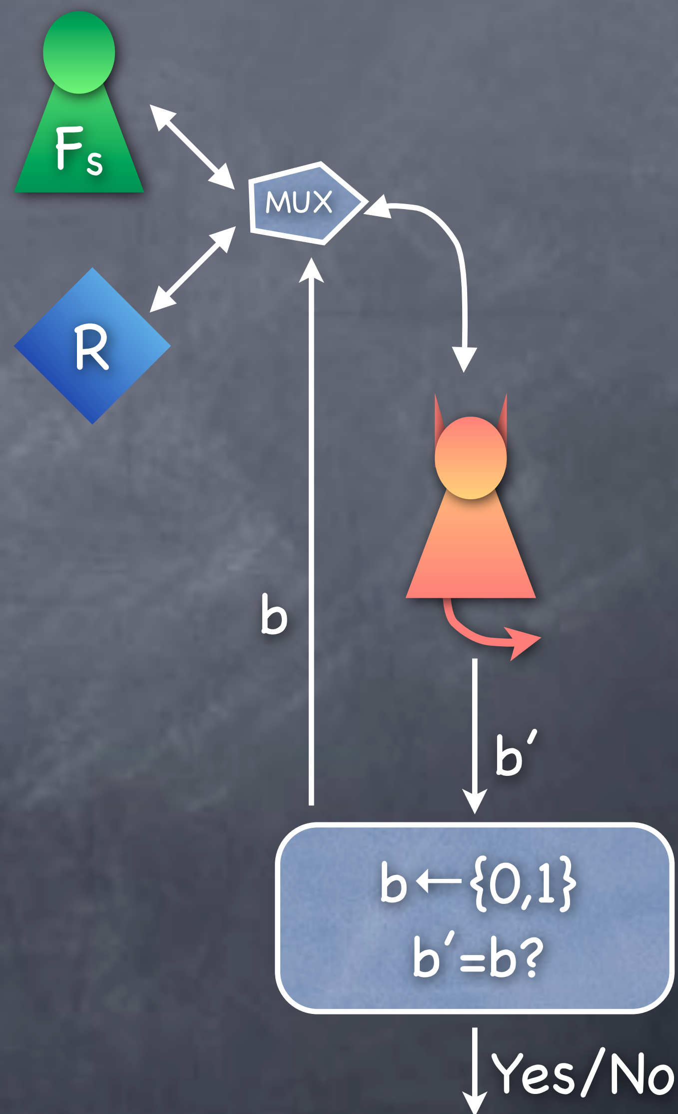
Pseudorandom Function (PRF)

- F: $\{0,1\}^k \times \{0,1\}^{m(k)} \rightarrow \{0,1\}^{n(k)}$ 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. Needs to guess which.



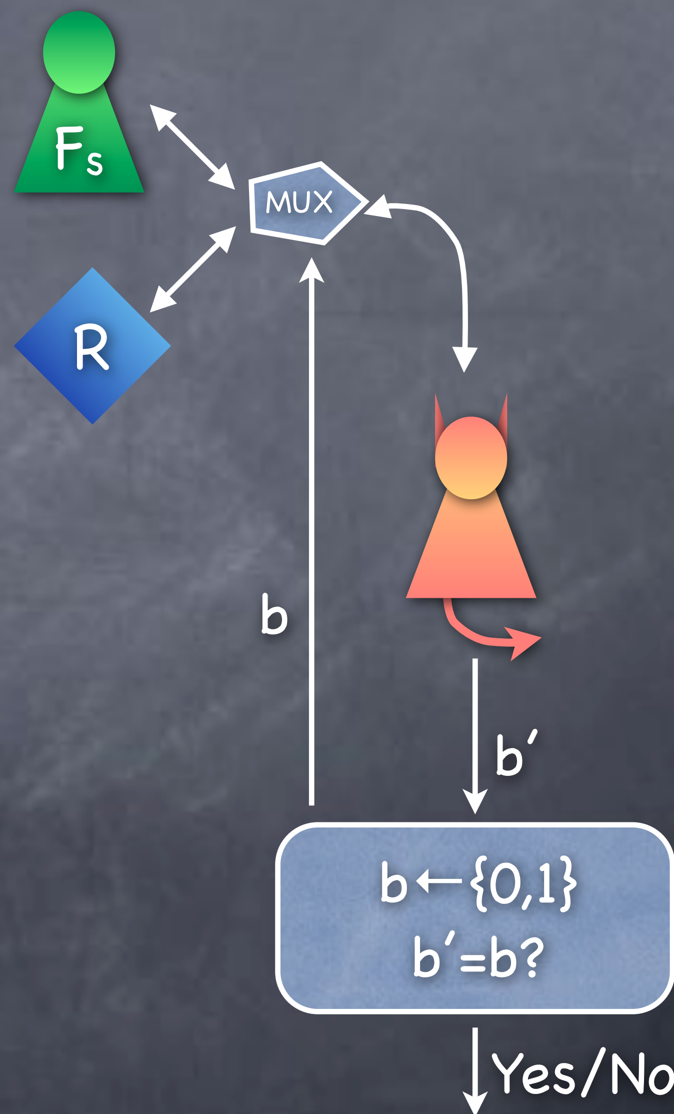
Pseudorandom Function (PRF)

- F: $\{0,1\}^k \times \{0,1\}^{m(k)} \rightarrow \{0,1\}^{n(k)}$ 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. Needs to guess which.
  - Note: Only 2^k seeds for F



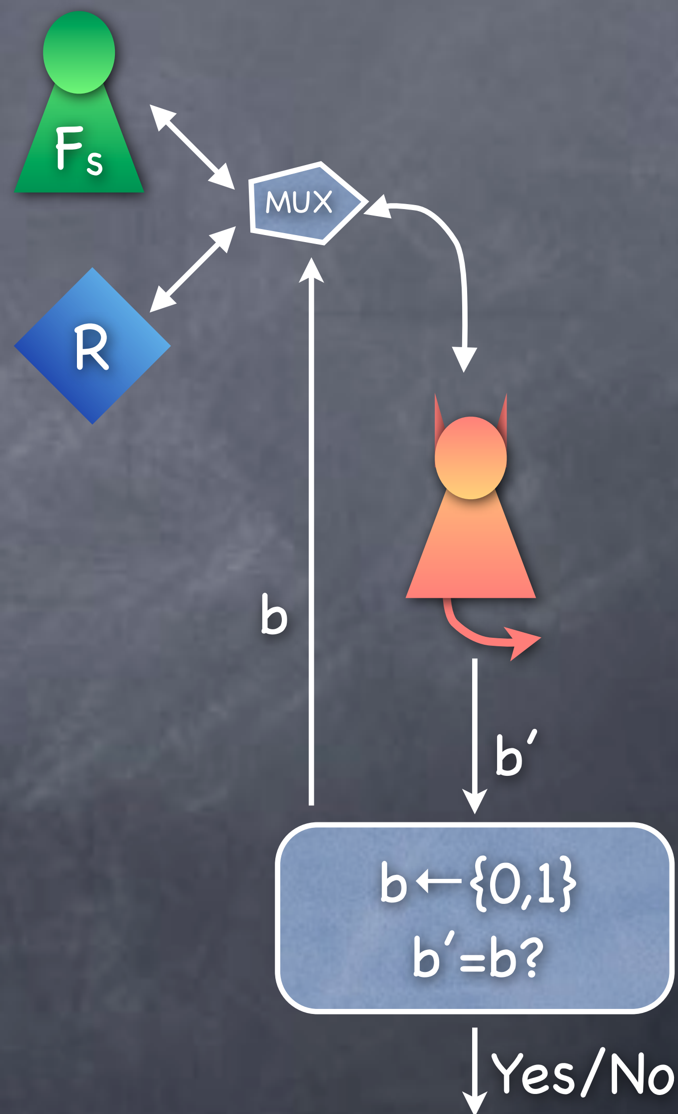
Pseudorandom Function (PRF)

- F: $\{0,1\}^k \times \{0,1\}^{m(k)} \rightarrow \{0,1\}^{n(k)}$ 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. Needs to guess which.
  - Note: Only 2^k seeds for F
    - But $2\hat{}(n2^m)$ functions R



Pseudorandom Function (PRF)

- F: $\{0,1\}^k \times \{0,1\}^{m(k)} \rightarrow \{0,1\}^{n(k)}$ 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. Needs to guess which.
  - Note: Only 2^k seeds for F
    - But $2^{\wedge}(n2^m)$ functions R
  - PRF stretches k bits to $n2^m$ bits



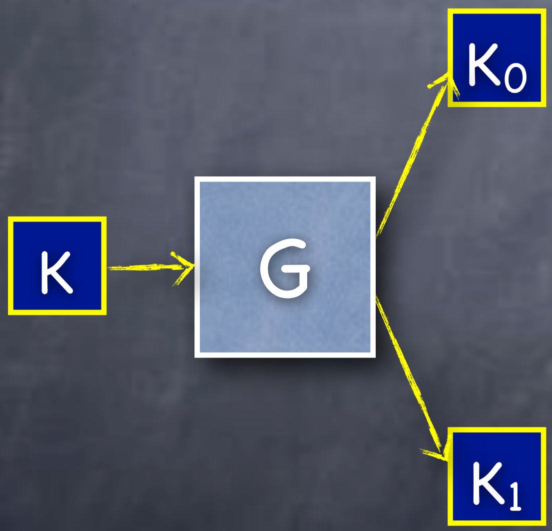
Pseudorandom Function (PRF)

Pseudorandom Function (PRF)

- A PRF can be constructed from any PRG

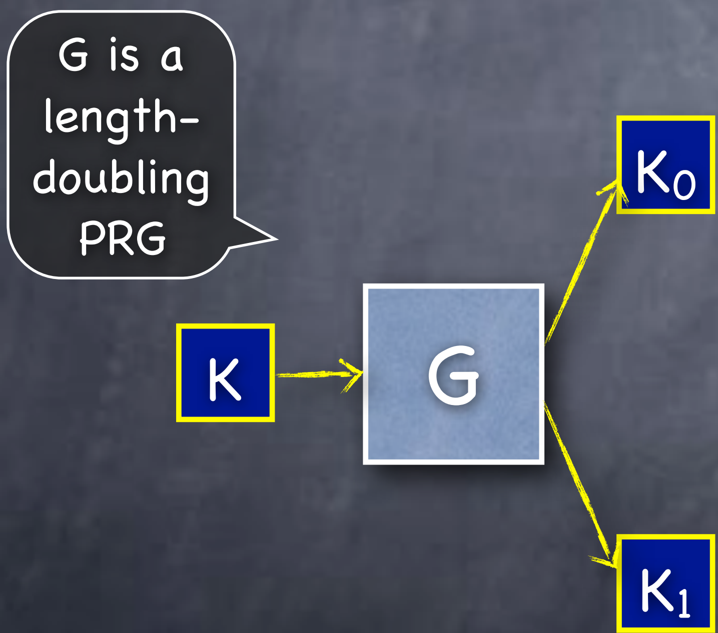
Pseudorandom Function (PRF)

- A PRF can be constructed from any PRG



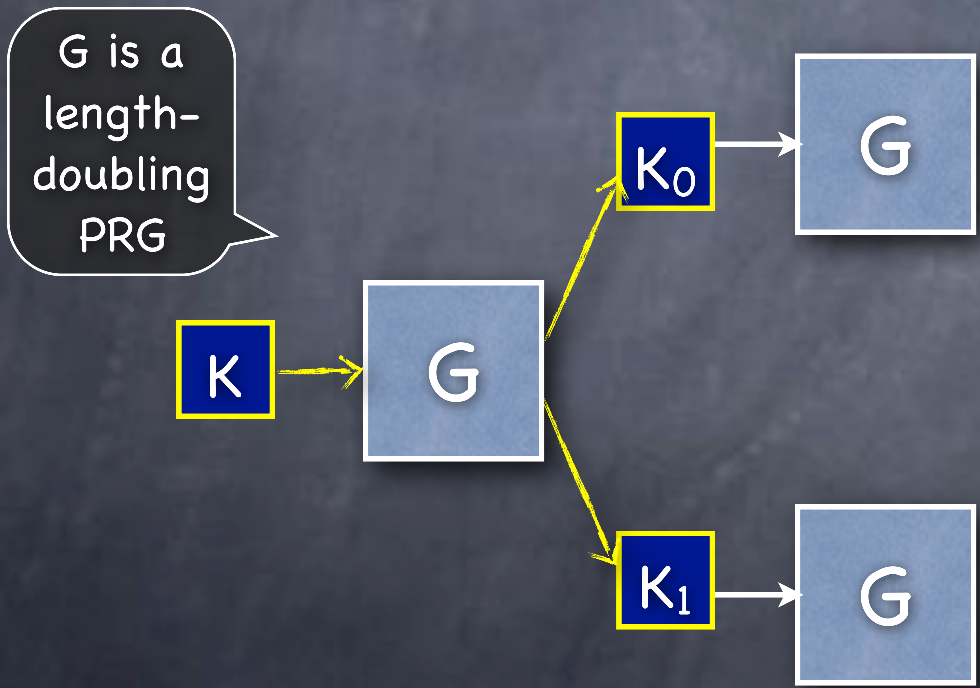
Pseudorandom Function (PRF)

- A PRF can be constructed from any PRG



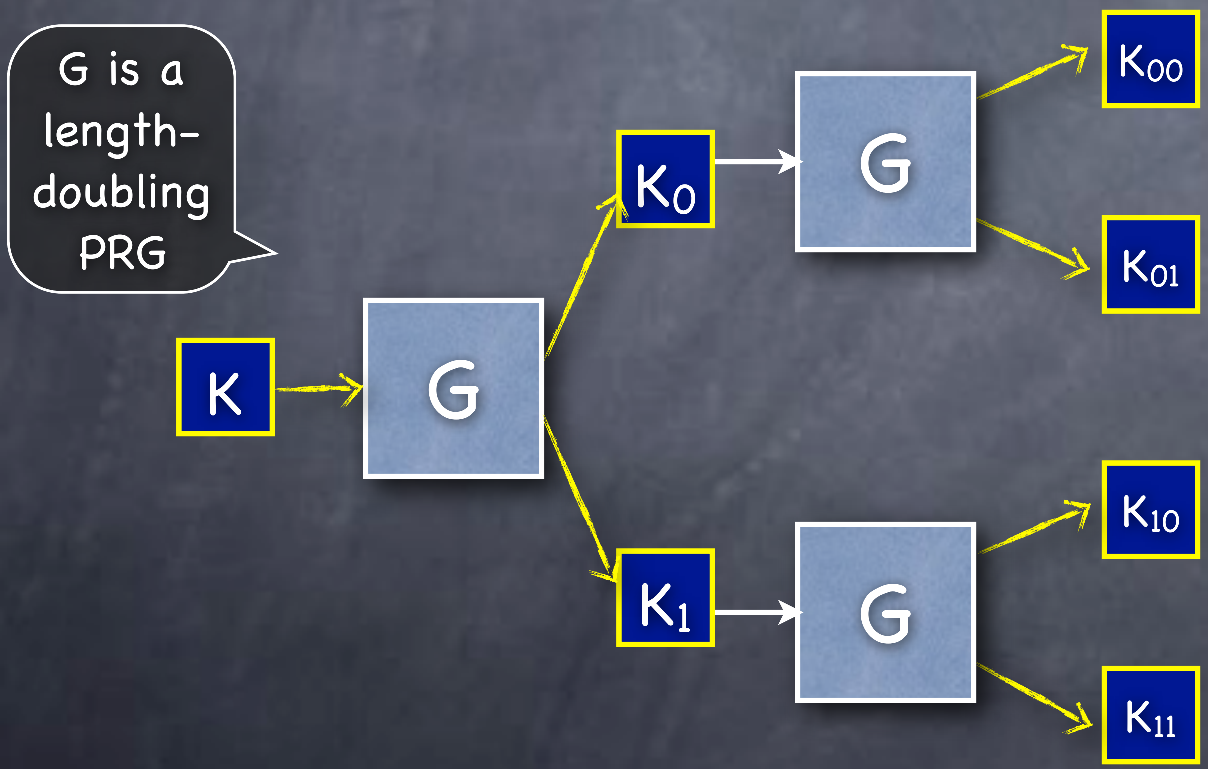
Pseudorandom Function (PRF)

- A PRF can be constructed from any PRG



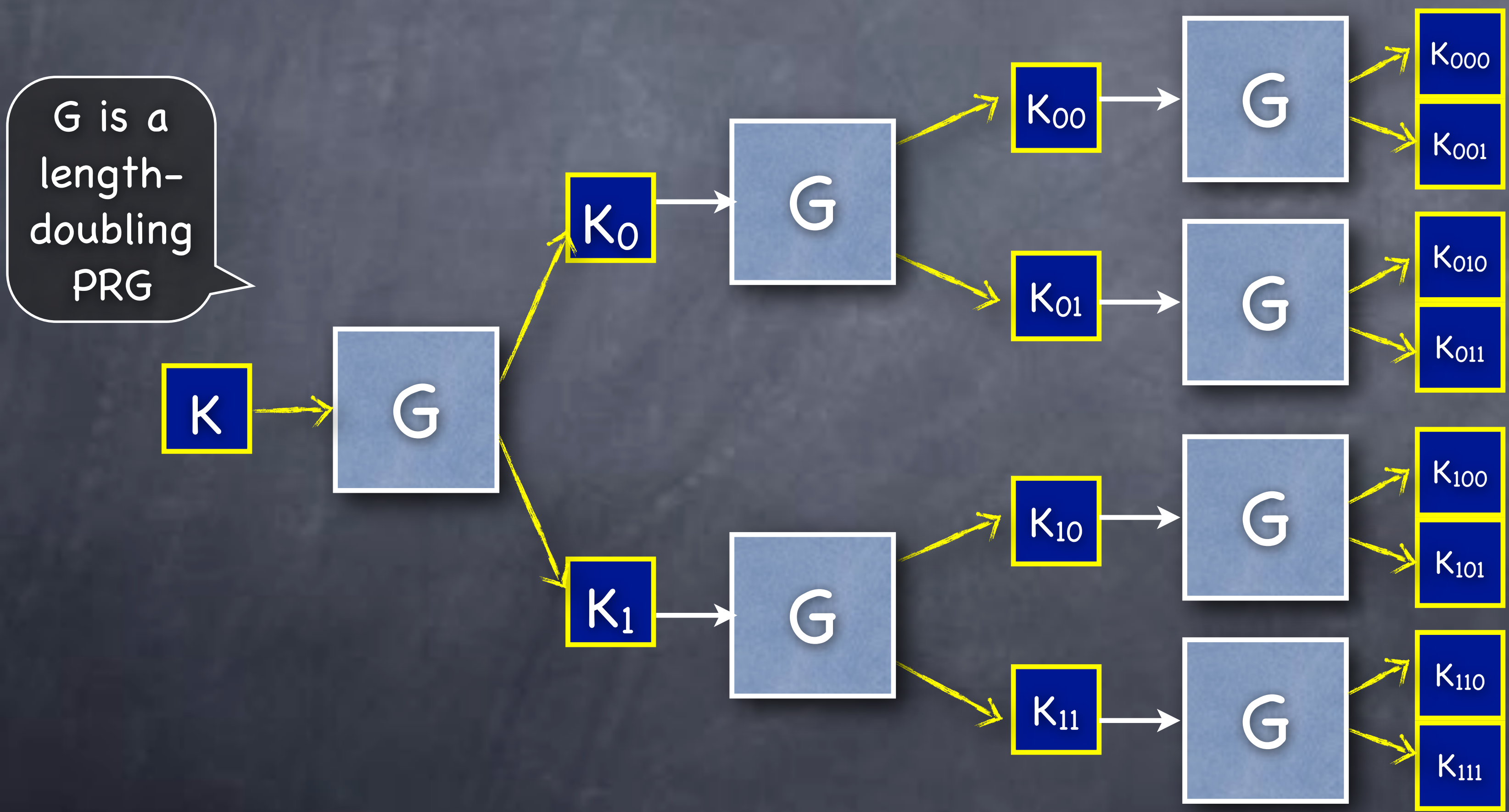
Pseudorandom Function (PRF)

- A PRF can be constructed from any PRG



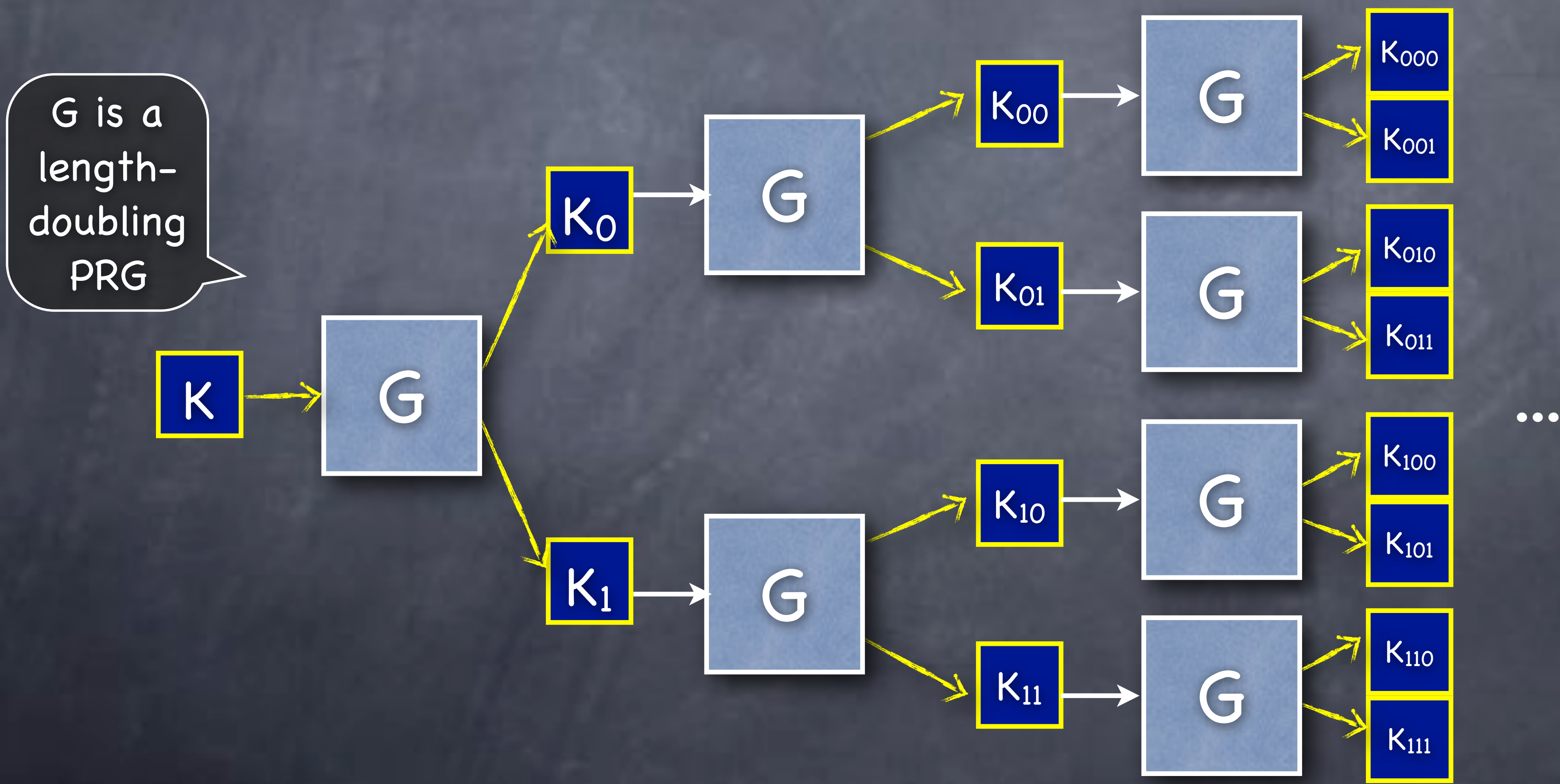
Pseudorandom Function (PRF)

- A PRF can be constructed from any PRG



Pseudorandom Function (PRF)

- A PRF can be constructed from any PRG



Pseudorandom Function (PRF)

- A PRF can be constructed from any PRG

Pseudorandom Function (PRF)

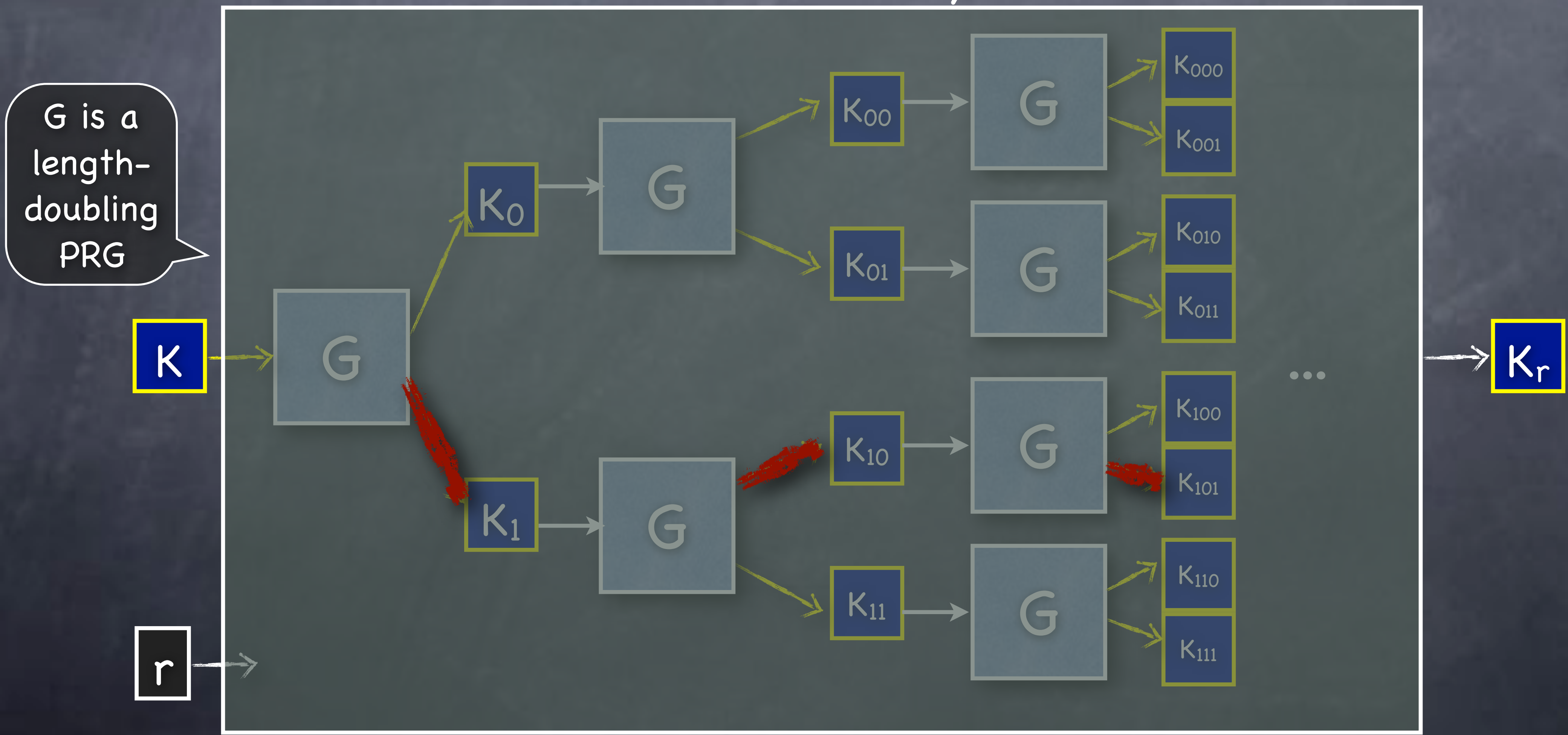
- A PRF can be constructed from any PRG

Pseudorandom Function (PRF)

- A PRF can be constructed from any PRG

Pseudorandom Function (PRF)

- A PRF can be constructed from any PRG



Pseudorandom Function (PRF)

- A PRF can be constructed from any PRG

Pseudorandom Function (PRF)

- A PRF can be constructed from any PRG
  - Not blazing fast

Pseudorandom Function (PRF)

- A PRF can be constructed from any PRG
  - Not blazing fast
  - Faster constructions based on specific number-theoretic computational complexity assumptions

Pseudorandom Function (PRF)

- A PRF can be constructed from any PRG
  - Not blazing fast
  - Faster constructions based on specific number-theoretic computational complexity assumptions
  - Fast heuristic constructions

Pseudorandom Function (PRF)

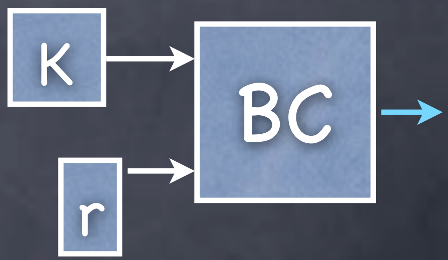
- A PRF can be constructed from any PRG
  - Not blazing fast
  - Faster constructions based on specific number-theoretic computational complexity assumptions
  - Fast heuristic constructions
- In practice: Block Cipher

Pseudorandom Function (PRF)

- A PRF can be constructed from any PRG
  - Not blazing fast
  - Faster constructions based on specific number-theoretic computational complexity assumptions
  - Fast heuristic constructions
- In practice: Block Cipher
  - (Best modeled as) A "strong" pseudorandom permutation, with an inversion trapdoor

Pseudorandom Function (PRF)

- A PRF can be constructed from any PRG
  - Not blazing fast
  - Faster constructions based on specific number-theoretic computational complexity assumptions
  - Fast heuristic constructions
- In practice: Block Cipher
  - (Best modeled as) A "strong" pseudorandom permutation, with an inversion trapdoor



CPA-secure SKE with a Block Cipher

CPA-secure SKE with a Block Cipher

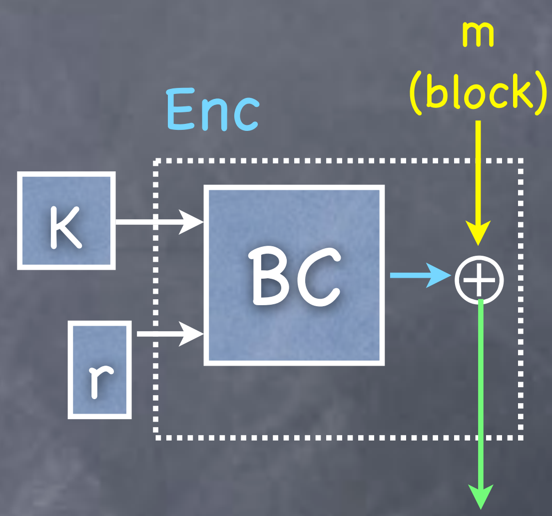
- Suppose Alice and Bob have shared a key (seed) for a block-cipher (PRF) BC

CPA-secure SKE with a Block Cipher

- Suppose Alice and Bob have shared a key (seed) for a block-cipher (PRF) BC
- For each encryption, Alice will pick a fresh pseudorandom pad, by picking a fresh value r and setting pad=$BC_K(r)$

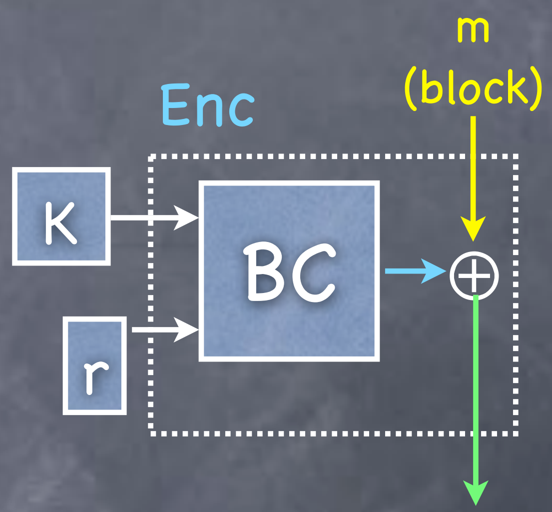
CPA-secure SKE with a Block Cipher

- Suppose Alice and Bob have shared a key (seed) for a block-cipher (PRF) BC
- For each encryption, Alice will pick a fresh pseudorandom pad, by picking a fresh value r and setting pad=$BC_K(r)$



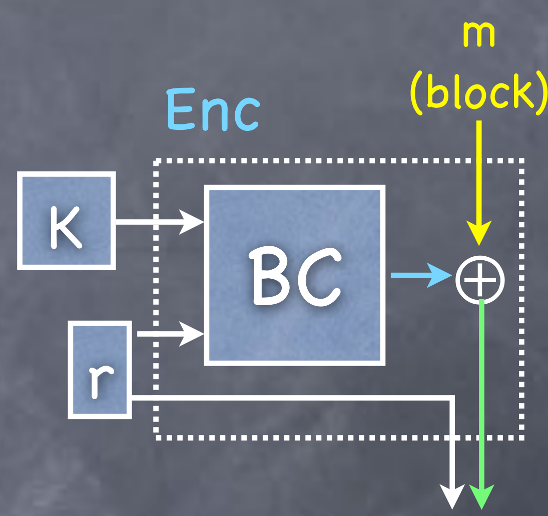
CPA-secure SKE with a Block Cipher

- Suppose Alice and Bob have shared a key (seed) for a block-cipher (PRF) BC
- For each encryption, Alice will pick a fresh pseudorandom pad, by picking a fresh value r and setting pad=$BC_K(r)$
- Bob needs to be able to generate the same pad, so Alice sends r (in the clear, as part of the ciphertext) to Bob



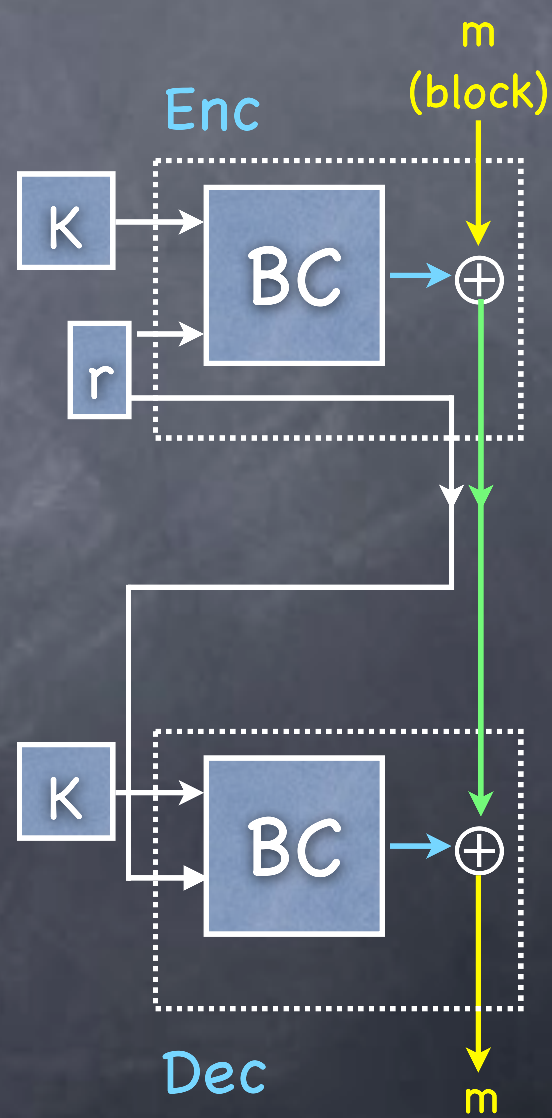
CPA-secure SKE with a Block Cipher

- Suppose Alice and Bob have shared a key (seed) for a block-cipher (PRF) BC
- For each encryption, Alice will pick a fresh pseudorandom pad, by picking a fresh value r and setting pad=$BC_K(r)$
- Bob needs to be able to generate the same pad, so Alice sends r (in the clear, as part of the ciphertext) to Bob



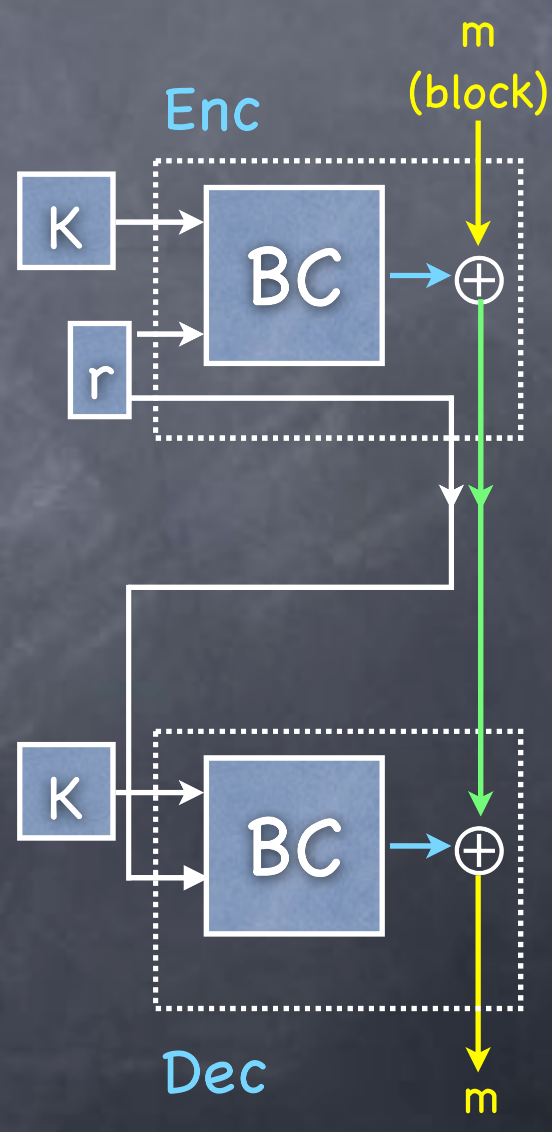
CPA-secure SKE with a Block Cipher

- Suppose Alice and Bob have shared a key (seed) for a block-cipher (PRF) BC
- For each encryption, Alice will pick a fresh pseudorandom pad, by picking a fresh value r and setting pad=$BC_K(r)$
- Bob needs to be able to generate the same pad, so Alice sends r (in the clear, as part of the ciphertext) to Bob



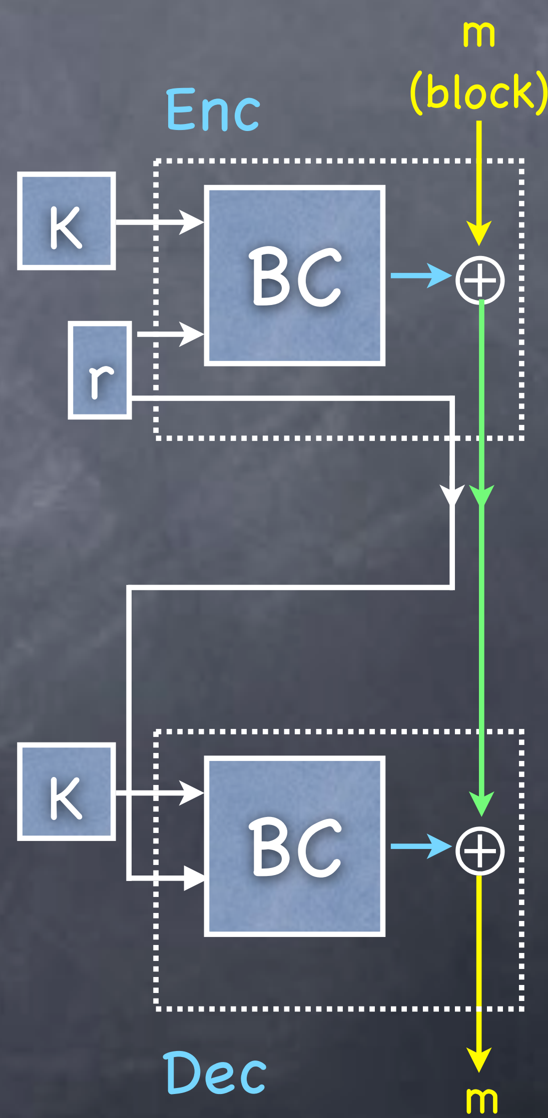
CPA-secure SKE with a Block Cipher

- Suppose Alice and Bob have shared a key (seed) for a block-cipher (PRF) BC
- For each encryption, Alice will pick a fresh pseudorandom pad, by picking a fresh value r and setting pad= $BC_K(r)$
- Bob needs to be able to generate the same pad, so Alice sends r (in the clear, as part of the ciphertext) to Bob
- Even if Eve sees r, PRF security guarantees that $BC_K(r)$ is pseudorandom. (In fact, Eve could have picked r, as long as we ensure no r is reused.)



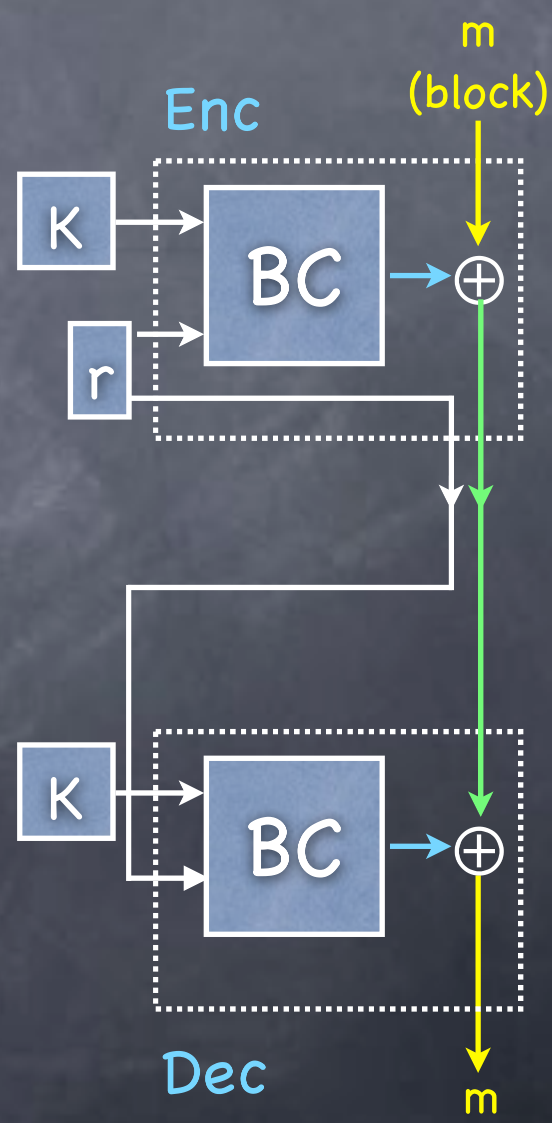
CPA-secure SKE with a Block Cipher

- Suppose Alice and Bob have shared a key (seed) for a block-cipher (PRF) BC
- For each encryption, Alice will pick a fresh pseudorandom pad, by picking a fresh value r and setting pad=$BC_K(r)$
- Bob needs to be able to generate the same pad, so Alice sends r (in the clear, as part of the ciphertext) to Bob
- Even if Eve sees r, PRF security guarantees that $BC_K(r)$ is pseudorandom. (In fact, Eve could have picked r, as long as we ensure no r is reused.)
- How to pick a fresh r?



CPA-secure SKE with a Block Cipher

- Suppose Alice and Bob have shared a key (seed) for a block-cipher (PRF) BC
- For each encryption, Alice will pick a fresh pseudorandom pad, by picking a fresh value r and setting pad=$BC_K(r)$
- Bob needs to be able to generate the same pad, so Alice sends r (in the clear, as part of the ciphertext) to Bob
- Even if Eve sees r, PRF security guarantees that $BC_K(r)$ is pseudorandom. (In fact, Eve could have picked r, as long as we ensure no r is reused.)
- How to pick a fresh r?
  - Pick at random!



CPA-secure SKE with a Block Cipher

CPA-secure SKE with a Block Cipher

- How to encrypt a long message (multiple blocks)?

CPA-secure SKE with a Block Cipher

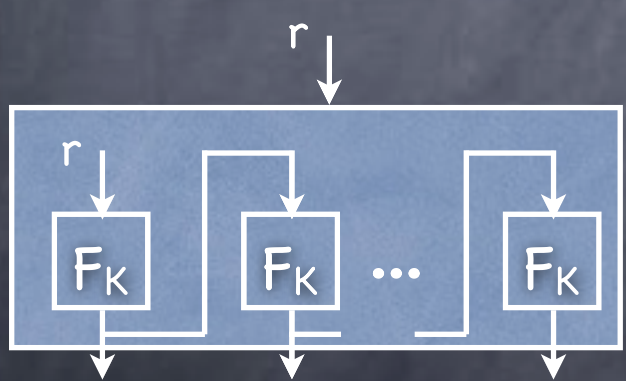
- How to encrypt a long message (multiple blocks)?
  - Can chop the message into blocks and independently encrypt each block as before. Works, but ciphertext size is double that of the plaintext (if $|r|$ is one-block long)

CPA-secure SKE with a Block Cipher

- How to encrypt a long message (multiple blocks)?
  - Can 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 PRF (w/o increasing input length)

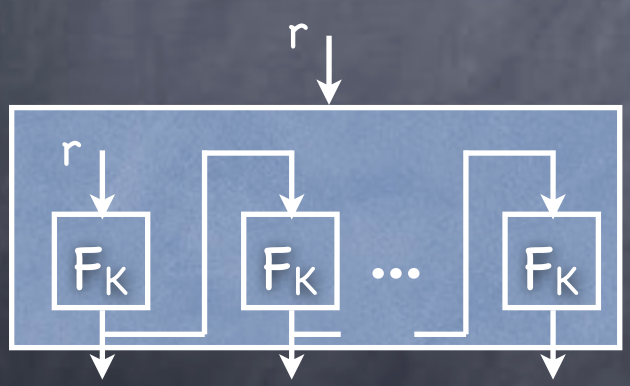
CPA-secure SKE with a Block Cipher

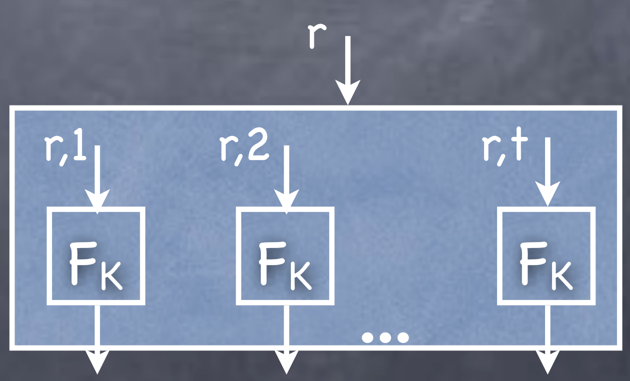
- How to encrypt a long message (multiple blocks)?
  - Can chop the message into blocks and independently encrypt each block as before. Works, but ciphertext size is double that of the plaintext (if |r| is one-block long)
- Extend output length of PRF (w/o increasing input length)



CPA-secure SKE with a Block Cipher

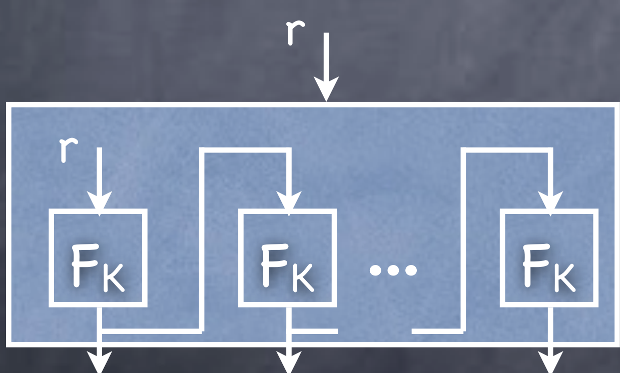
- How to encrypt a long message (multiple blocks)?
  - Can chop the message into blocks and independently encrypt each block as before. Works, but ciphertext size is double that of the plaintext (if |r| is one-block long)
- Extend <u>output length</u> of PRF (w/o increasing input length)

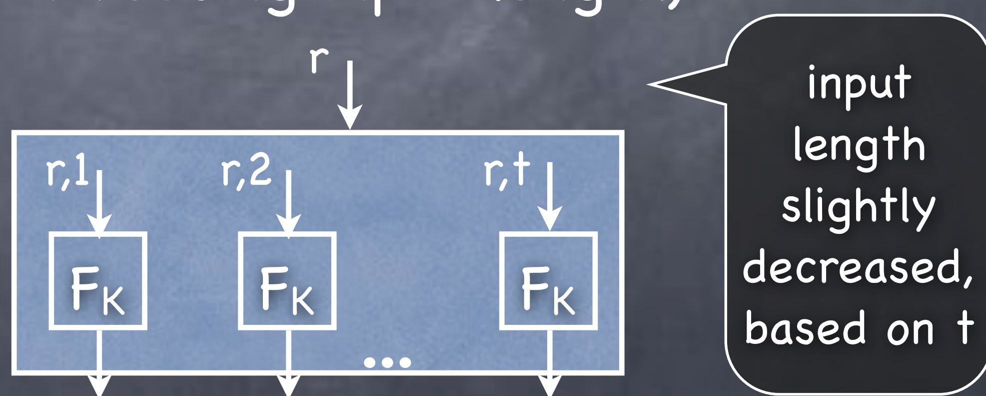




CPA-secure SKE with a Block Cipher

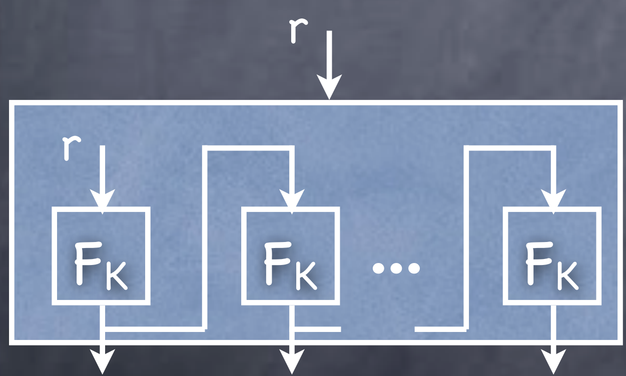
- How to encrypt a long message (multiple blocks)?
  - Can chop the message into blocks and independently encrypt each block as before. Works, but ciphertext size is double that of the plaintext (if |r| is one-block long)
- Extend <u>output length</u> of PRF (w/o increasing input length)

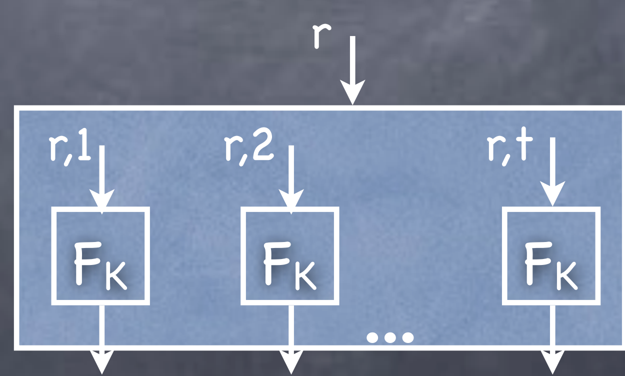




CPA-secure SKE with a Block Cipher

- How to encrypt a long message (multiple blocks)?
  - Can 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 <u>output length</u> of PRF (w/o increasing input length)





input length slightly decreased, based on t

- Output is indistinguishable from t random blocks (even if input to F_K known/chosen)

CPA-secure SKE with a Block Cipher

CPA-secure SKE with a Block Cipher

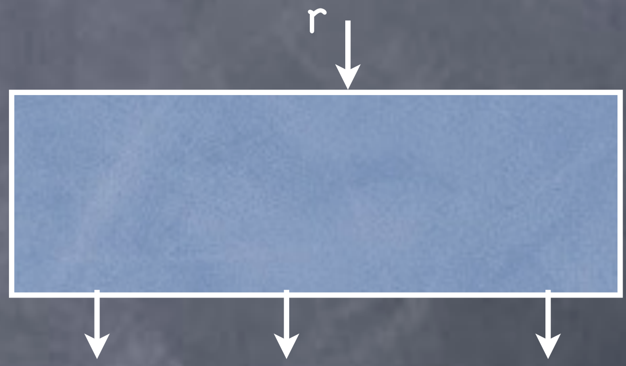
- Various "modes" of operation of a Block-cipher (i.e., encryption schemes using a block-cipher). All with one block overhead.

CPA-secure SKE with a Block Cipher

- Various "modes" of operation of a Block-cipher (i.e., encryption schemes using a block-cipher). All with one block overhead.
  - **Output Feedback (OFB) mode:** Extend the pseudorandom output using the first construction in the previous slide

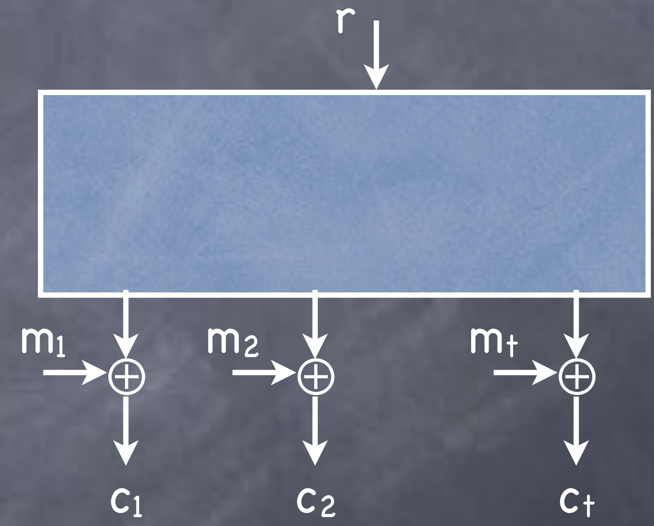
CPA-secure SKE with a Block Cipher

- Various "modes" of operation of a Block-cipher (i.e., encryption schemes using a block-cipher). All with one block overhead.
  - **Output Feedback (OFB) mode:** Extend the pseudorandom output using the first construction in the previous slide



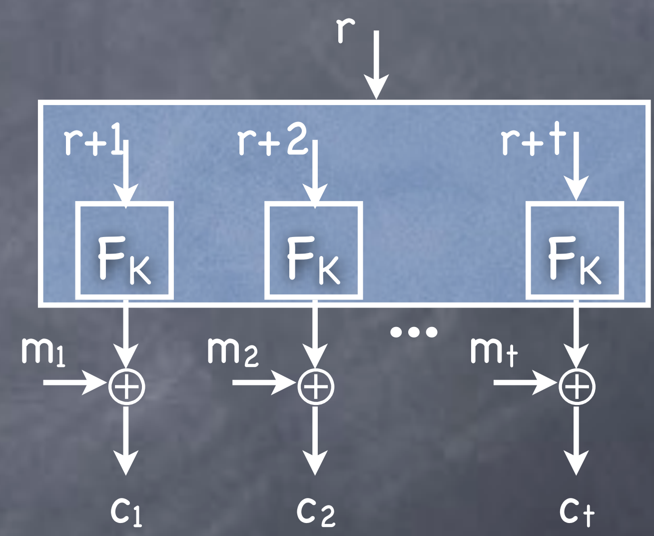
CPA-secure SKE with a Block Cipher

- Various "modes" of operation of a Block-cipher (i.e., encryption schemes using a block-cipher). All with one block overhead.
  - **Output Feedback (OFB) mode:** Extend the pseudorandom output using the first construction in the previous slide



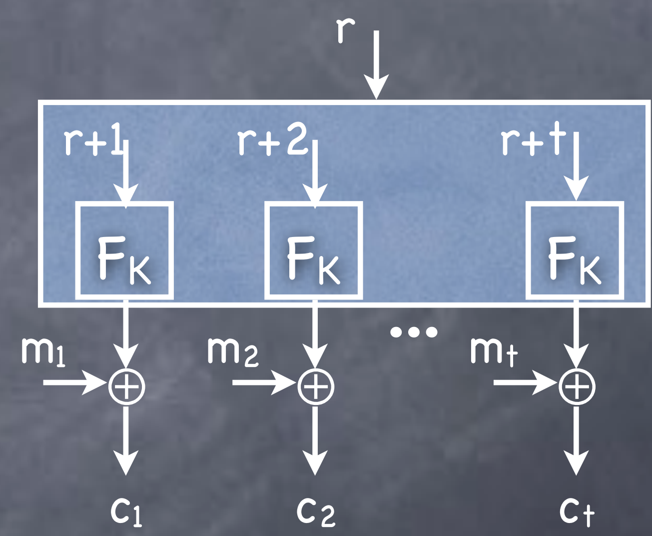
CPA-secure SKE with a Block Cipher

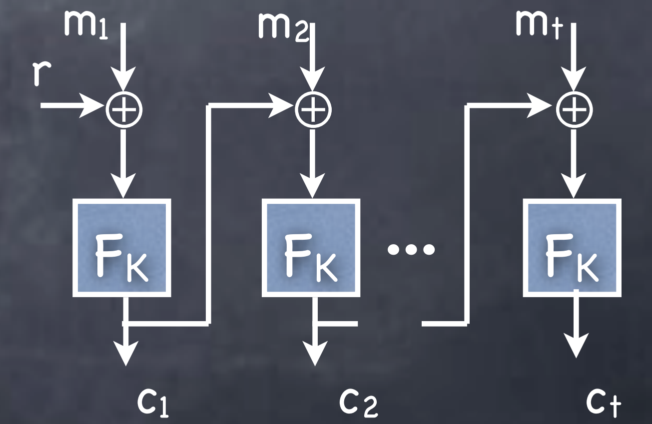
- Various "modes" of operation of a Block-cipher (i.e., encryption schemes using a block-cipher). All with one block overhead.
  - **Output Feedback (OFB) mode:** Extend the pseudorandom output using the first construction in the previous slide
  - **Counter (CTR) Mode:** Similar idea as in the second construction, but not a PRF extension (Why?). No a priori limit on number of blocks in a message. Security from low likelihood of (r+1,...,r+t) running into (r'+1,...,r'+t')



CPA-secure SKE with a Block Cipher

- Various "modes" of operation of a Block-cipher (i.e., encryption schemes using a block-cipher). All with one block overhead.
  - **Output Feedback (OFB) mode:** Extend the pseudorandom output using the first construction in the previous slide
  - **Counter (CTR) Mode:** Similar idea as in the second construction, but not a PRF extension (Why?). No a priori limit on number of blocks in a message. Security from low likelihood of (r+1,...,r+t) running into (r'+1,...,r'+t')
  - **Cipher Block Chaining (CBC) mode:** Sequential encryption. Decryption uses F_K^{-1}. Ciphertext an integral number of blocks.





Active Adversary

Active Adversary

- An active adversary can inject messages into the channel

Active Adversary

- An active adversary can inject messages into the channel
  - Eve can send ciphertexts to Bob and get them decrypted

Active Adversary

- An active adversary can inject messages into the channel
  - Eve can send ciphertexts to Bob and get them decrypted
    - Chosen Ciphertext Attack (CCA)

Active Adversary

- An active adversary can inject messages into the channel
  - Eve can send ciphertexts to Bob and get them decrypted
    - Chosen Ciphertext Attack (CCA)
  - If Bob decrypts all ciphertexts for Eve, no security possible

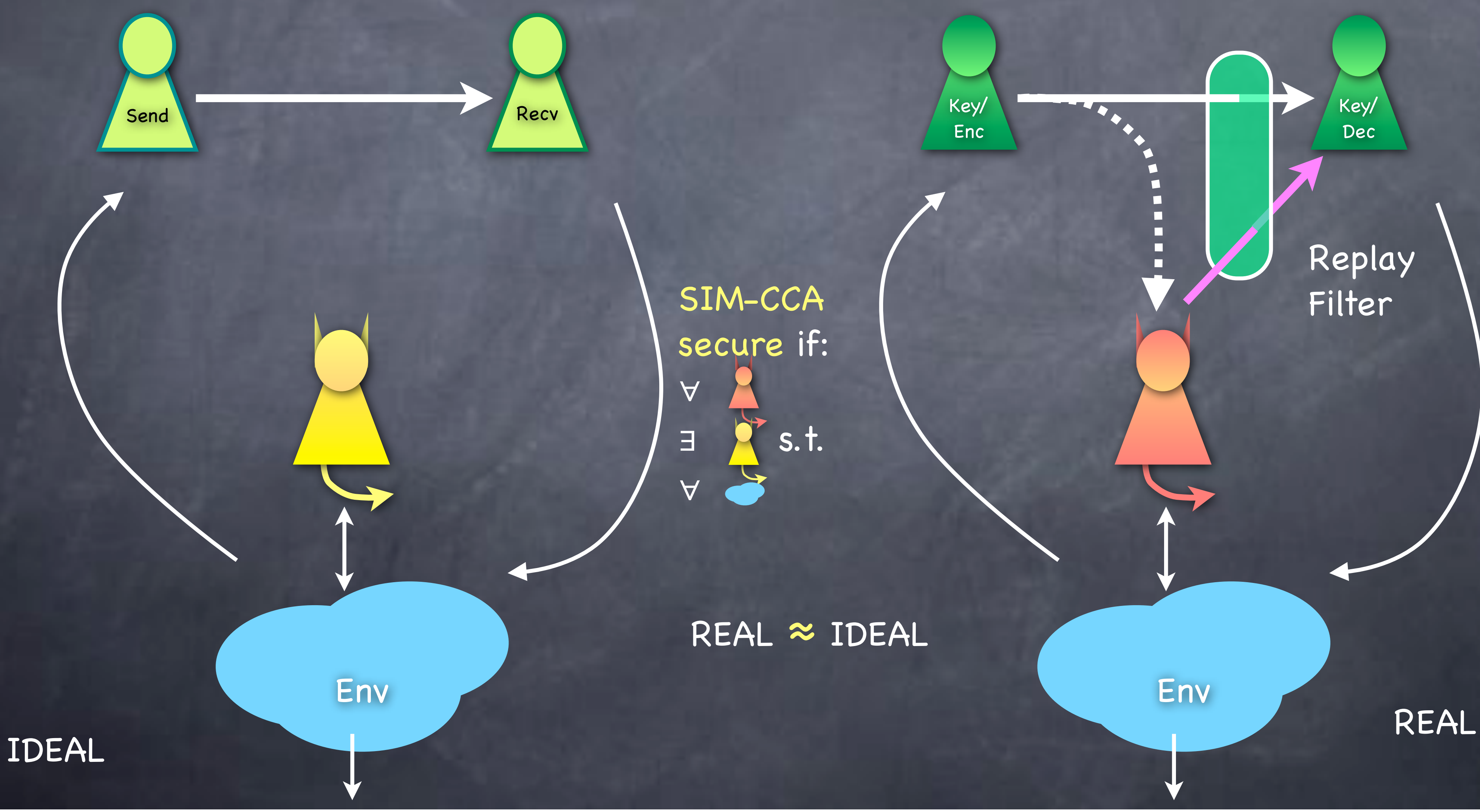
Active Adversary

- An active adversary can inject messages into the channel
  - Eve can send ciphertexts to Bob and get them decrypted
    - Chosen Ciphertext Attack (CCA)
  - If Bob decrypts all ciphertexts for Eve, no security possible
    - What can Bob do?

RECALL

Symmetric-Key Encryption

SIM-CCA Security



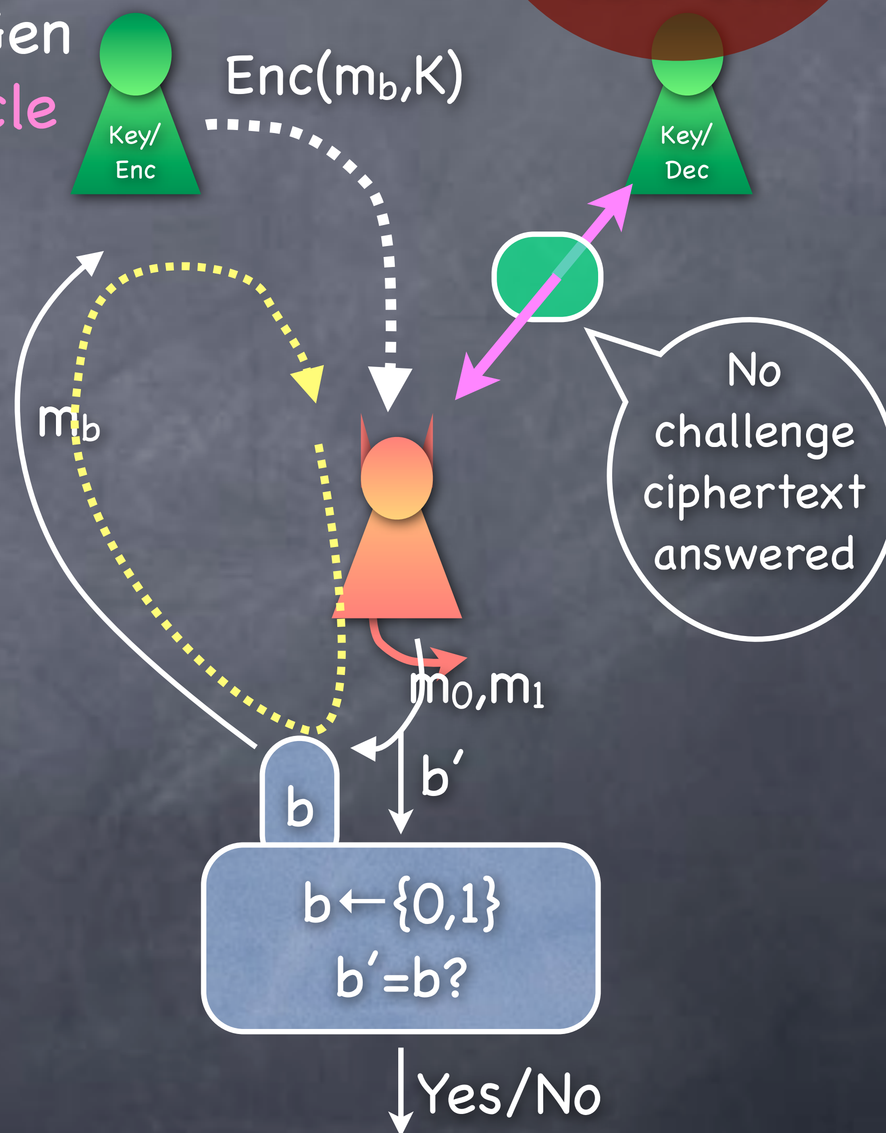
RECALL

Symmetric-Key Encryption

IND-CCA Security

IND-CCA + ~correctness equivalent to SIM-CCA

- Experiment picks b←{0,1} and K←KeyGen
  Adv gets (guarded) access to Dec_K oracle
  - For as long as Adversary wants
    - Adv sends two messages m_0, m_1 to the experiment
    - Expt returns $Enc(m_b,K)$ to the adversary
- Adversary returns a guess b′
- Experiments outputs 1 iff b′=b
- IND-CCA secure if for all feasible adversaries $Pr[b'=b] \approx 1/2$



CCA Security

CCA Security

- How to obtain CCA security?

CCA Security

- How to obtain CCA security?
- Use a CPA-secure encryption scheme, but make sure Bob "accepts" and decrypts only ciphertexts produced by Alice

CCA Security

- How to obtain CCA security?
- Use a CPA-secure encryption scheme, but make sure Bob "accepts" and decrypts only ciphertexts produced by Alice
  - i.e., Eve can't create new ciphertexts that will be accepted by Bob

CCA Security

- How to obtain CCA security?
- Use a CPA-secure encryption scheme, but make sure Bob "accepts" and decrypts only ciphertexts produced by Alice
  - i.e., Eve can't create new ciphertexts that will be accepted by Bob
- CCA secure SKE reduces to the problem of CPA secure SKE and (shared key) message authentication

CCA Security

- How to obtain CCA security?
- Use a CPA-secure encryption scheme, but make sure Bob "accepts" and decrypts only ciphertexts produced by Alice
  - i.e., Eve can't create new ciphertexts that will be accepted by Bob
- CCA secure SKE reduces to the problem of CPA secure SKE and (shared key) message authentication
  - MAC: Message Authentication Code

Message Authentication Codes

Message Authentication Codes

- A single short key shared by Alice and Bob

Message Authentication Codes

- A single short key shared by Alice and Bob
  - Can sign any (polynomial) number of messages

Message Authentication Codes

- A single short key shared by Alice and Bob
  - Can sign any (polynomial) number of messages
- A triple (KeyGen, MAC, Verify)

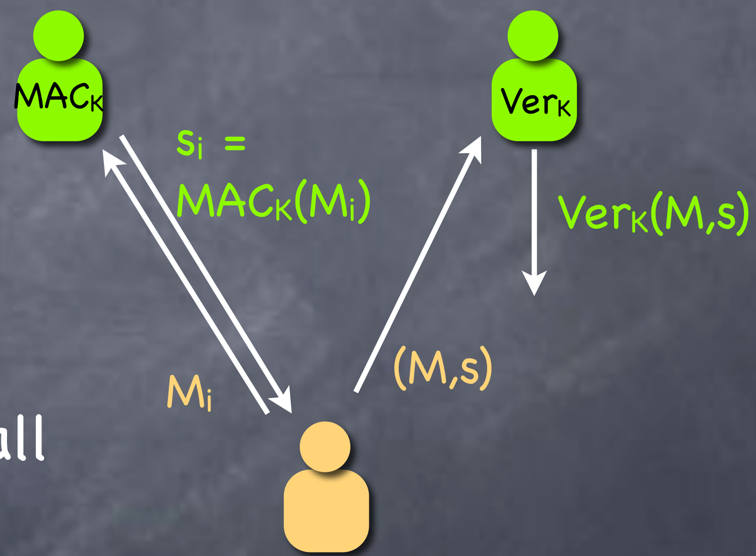
Message Authentication Codes

- A single short key shared by Alice and Bob
  - Can sign any (polynomial) number of messages

- A triple (KeyGen, MAC, Verify)
- Correctness: For all K from KeyGen, and all messages M, $Verify_K(M,MAC_K(M))=1$

Message Authentication Codes

- A single short key shared by Alice and Bob
  - Can sign any (polynomial) number of messages
- A triple (KeyGen, MAC, Verify)
- Correctness: For all K from KeyGen, and all messages M, $\text{Verify}_K(M,\text{MAC}_K(M))=1$
- Security: probability that an adversary can produce (M,s) s.t. $\text{Verify}_K(M,s)=1$ is negligible unless Alice produced an output $s=\text{MAC}_K(M)$



Advantage
$= \Pr[\ \text{Ver}_K(M,s)=1 \text{ and } (M,s) \notin \{(M_i,s_i)\}\ ]$

CCA Secure SKE

CCA Secure SKE

- $\text{CCA-Enc}_{K1,K2}(m) = (\ c := \text{CPA-Enc}_{K1}(m),\ t := \text{MAC}_{K2}(c)\ )$

CCA Secure SKE

- $\text{CCA-Enc}_{K1,K2}(m) = (\ c := \text{CPA-Enc}_{K1}(m),\ t := \text{MAC}_{K2}(c)\ )$
  - CPA secure encryption: Block-cipher/CTR mode construction

CCA Secure SKE

- $\text{CCA-Enc}_{K1,K2}(m) = (\ c := \text{CPA-Enc}_{K1}(m),\ t := \text{MAC}_{K2}(c)\ )$
  - CPA secure encryption: Block-cipher/CTR mode construction
  - MAC: from a PRF or Block-Cipher (next time)

CCA Secure SKE

- CCA-Enc$_{K1,K2}$(m) = (c:= CPA-Enc$_{K1}$(m), t:= MAC$_{K2}$(c))
  - CPA secure encryption: Block-cipher/CTR mode construction
  - MAC: from a PRF or Block-Cipher (next time)
- SKE in practice uses Block-Cipher standards (next time)

CCA Secure SKE

- CCA-Enc$_{K1,K2}$(m) = (c:= CPA-Enc$_{K1}$(m), t:= MAC$_{K2}$(c))
  - CPA secure encryption: Block-cipher/CTR mode construction
  - MAC: from a PRF or Block-Cipher (next time)
- SKE in practice uses Block-Cipher standards (next time)
- In principle, constructions (less efficient) based on any One-Way Permutation or even One-Way Function (hence more secure)