# CSE 539: Applied Cryptography
# Lec 6: Block Cipher

Ni Trieu (ASU)

Reading: https://joyofcryptography.com/pdf/chap6.pdf

# Recap: Pseudorandom Generator (PRG)

- A PRG is a function $\mathbf{G}: \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{\lambda}} \to \{\mathbf{0},\mathbf{1}\}^{\boldsymbol{\lambda}+\boldsymbol{\ell}}$
- Security:

*Let* $G : \{0,1\}^{\lambda} \to \{0,1\}^{\lambda+\ell}$ *be a deterministic function with* $\ell > 0$. *We say that* $G$ *is a* ***secure pseudorandom generator (PRG)*** *if* $\mathcal{L}^{G}_{\text{prg-real}} \approx \mathcal{L}^{G}_{\text{prg-rand}}$, *where:*

$\mathcal{L}^{G}_{\text{prg-real}}$

QUERY():
$s \leftarrow \{0,1\}^{\lambda}$
return $G(s)$

$\mathcal{L}^{G}_{\text{prg-rand}}$

QUERY():
$r \leftarrow \{0,1\}^{\lambda+\ell}$
return $r$

# Recap: Pseudorandom Function

- A PRF is a function F: $\{0,1\}^{\lambda} \times \{0,1\}^{in} \rightarrow \{0,1\}^{out}$
- Security:

Definition 6.1 (PRF security) *Let $F : \{0,1\}^{\lambda} \times \{0,1\}^{in} \rightarrow \{0,1\}^{out}$ be a deterministic function. We say that $F$ is a secure* ***pseudorandom function (PRF)*** *if $\mathcal{L}^{F}_{\text{prf-real}} \approx \mathcal{L}^{F}_{\text{prf-rand}}$, where:*

$\mathcal{L}^{F}_{\text{prf-real}}$

$k \leftarrow \{0,1\}^{\lambda}$

LOOKUP($x \in \{0,1\}^{in}$):

return $F(k, x)$

$\mathcal{L}^{F}_{\text{prf-rand}}$

$T :=$ empty assoc. array

LOOKUP($x \in \{0,1\}^{in}$):

if $T[x]$ undefined:

$T[x] \leftarrow \{0,1\}^{out}$

return $T[x]$

# Pseudorandom Generator

- Quiz Sample: Is the below function a secure PRG?
  - $G(s) = f(s)||f(f(s))$ where $f$ is the secure PRG

# Pseudorandom Generator

- How to build a PRG?
  - From block cipher or PRF

Construction 6.2 (Counter PRG)

$G(s)$:
$x := F(s, 0\cdots00)$
$y := F(s, 0\cdots01)$
return $x \| y$

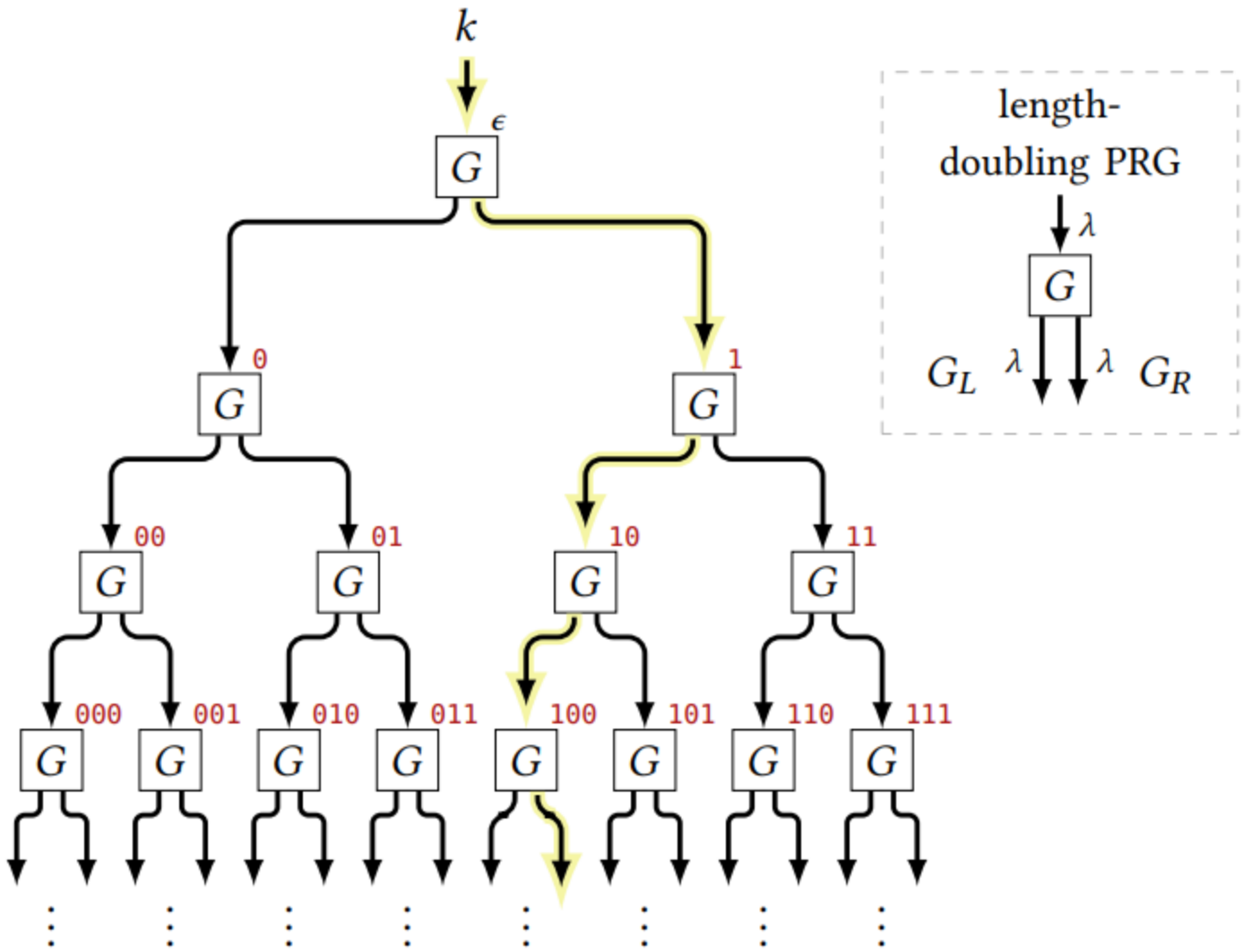
# Pseudorandom Function

- How to build a PRF?
  - From PRG

Construction 6.4
(GGM PRF)

$in = arbitrary$
$out = \lambda$

$F(k, x \in \{0,1\}^{in})$:
$v := k$
for $i = 1$ to $in$:
  if $x_i = 0$ then $v := G_L(v)$
  if $x_i = 1$ then $v := G_R(v)$
return $v$


k
ϵ
G
0
1
00
01
10
11
000
001
010
011
100
101
110
111
length-
doubling PRG
λ
$G_L$
$G_R$

# Pseudorandom Function

- How to build a PRF?
  - From PRG
- Why is it secure?
  - HW: https://joyofcryptography.com/pdf/chap6.pdf (Section 6.2)

Construction 6.4 (GGM PRF)

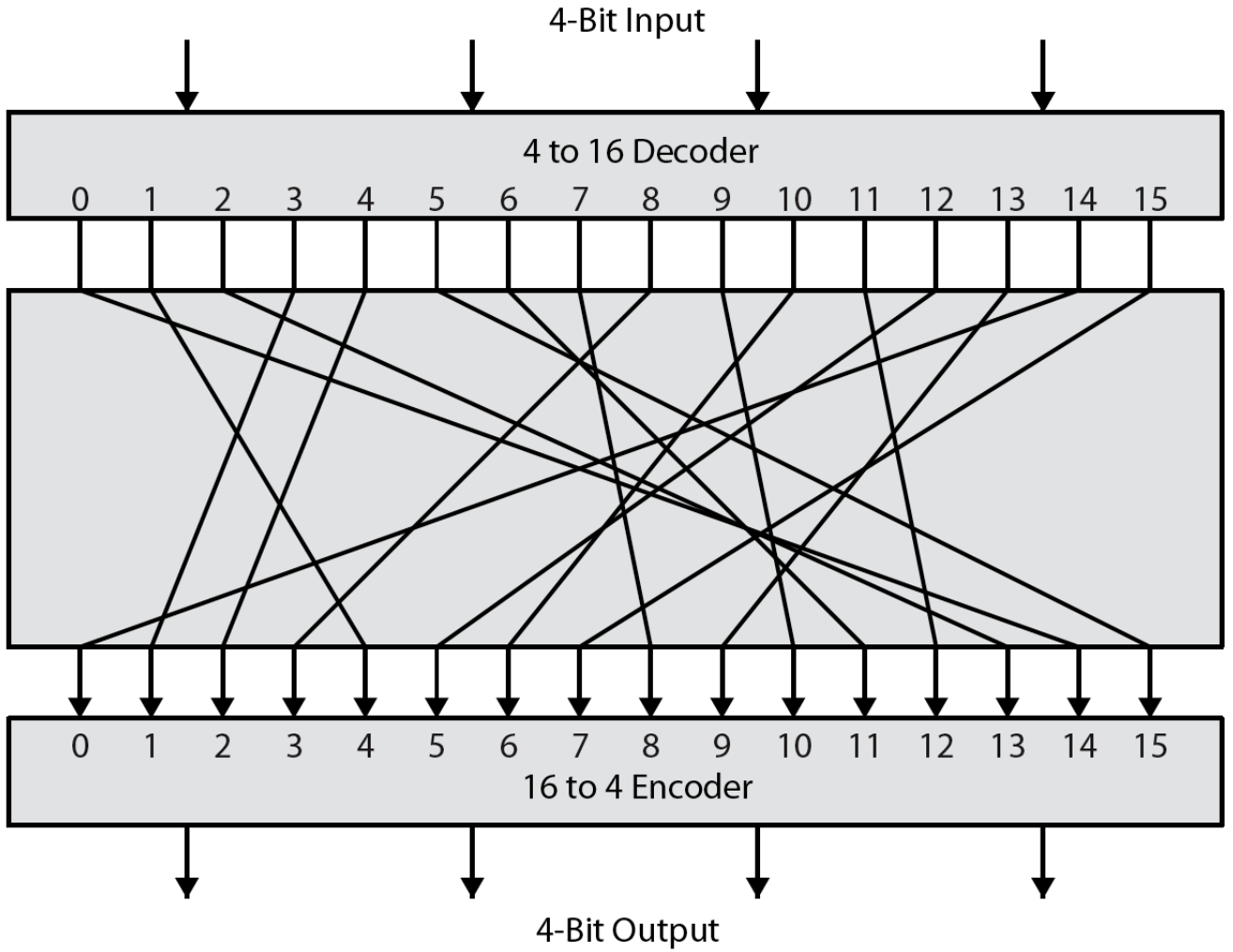
$in = arbitrary$
$out = \lambda$

$F(k, x \in \{0,1\}^{in})$:
$v := k$
for $i = 1$ to $in$:
  if $x_i = 0$ then $v := G_L(v)$
  if $x_i = 1$ then $v := G_R(v)$
return $v$

# Block Cipher (Pseudorandom Permutation)

- A pseudorandom permutation (PRP) — also called a block cipher — is essentially a PRF that is guaranteed to be invertible for every choice of seed
- A PRP is a function F: $\{0,1\}^{\lambda} \times \{0,1\}^{blen} \rightarrow \{0,1\}^{blen}$

# Block Cipher (Pseudorandom Permutation)



# Block Cipher (Pseudorandom Permutation)

Definition 6.6 (PRP syntax)

*Let* $F : \{0,1\}^\lambda \times \{0,1\}^{blen} \to \{0,1\}^{blen}$ *be a deterministic function. We refer to blen as the* ***blocklength*** *of F and any element of* $\{0,1\}^{blen}$ *as a* ***block****.*

*We call F a* ***secure pseudorandom permutation (PRP)*** *(****block cipher****) if the following two conditions hold:*

1. *(Invertible given k) There is a function* $F^{-1} : \{0,1\}^\lambda \times \{0,1\}^{blen} \to \{0,1\}^{blen}$ *satisfying*

$$F^{-1}(k, F(k,x)) = x,$$

*for all* $k \in \{0,1\}^\lambda$ *and all* $x \in \{0,1\}^{blen}$*.*

2. *(Security)* $\mathcal{L}^F_{\text{prp-real}} \approx \mathcal{L}^F_{\text{prp-rand}}$*, where:*

$\mathcal{L}^F_{\text{prp-real}}$

$k \leftarrow \{0,1\}^\lambda$

LOOKUP($x \in \{0,1\}^{blen}$):

return $F(k,x)$

$\mathcal{L}^F_{\text{prp-rand}}$

$T :=$ empty assoc. array

LOOKUP($x \in \{0,1\}^{blen}$):

if $T[x]$ undefined:

$T[x] \leftarrow \{0,1\}^{blen}$ \ $T$.values

return $T[x]$

# Constructing a PRP from a PRF

- The Feistel Construction

**Construction 6.11 (Feistel cipher)**

$\mathbb{F}_r((k_1, \ldots, k_r), v_0 \| v_1)$:

for $i = 1$ to $r$:

$v_{i+1} := F(k_i, v_i) \oplus v_{i-1}$

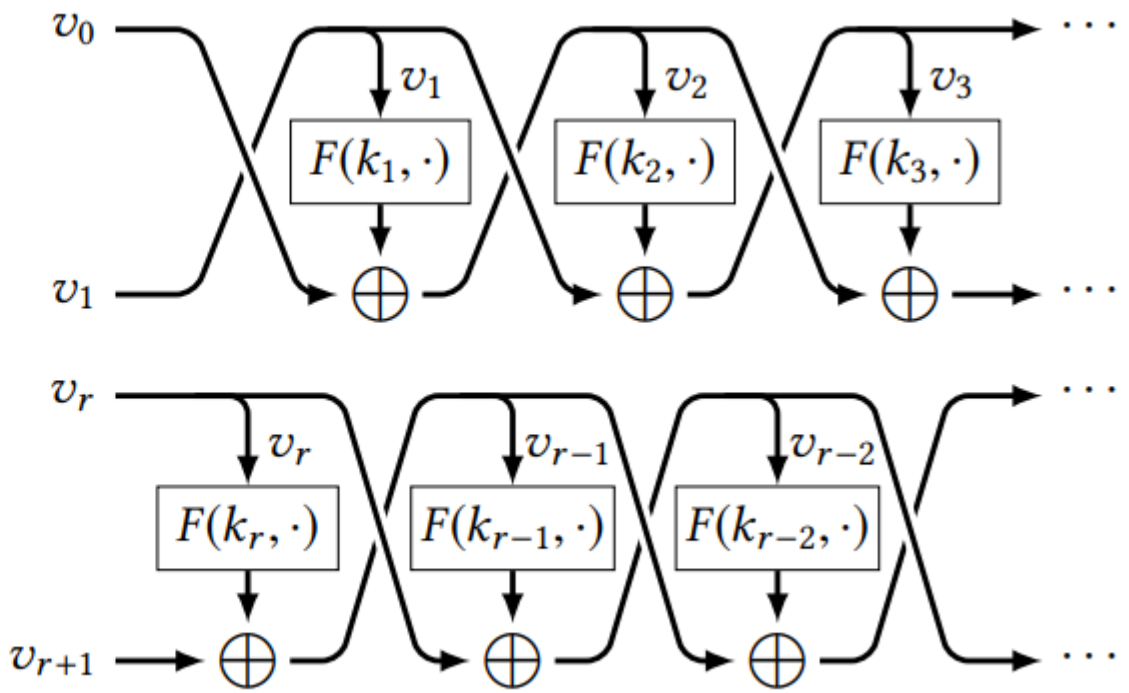
return $v_r \| v_{r+1}$

$\mathbb{F}_r^{-1}((k_1, \ldots, k_r), v_r \| v_{r+1})$:

for $i = r$ downto 1:

$v_{i-1} := F(k_i, v_i) \oplus v_{i+1}$

return $v_0 \| v_1$



# In practice

We use block ciphers that are designed “from scratch,” and then use these block ciphers to construct simpler PRGs and PRFs when we need them:

- The AES block cipher has a block length of 128 bits, and offers 3 different variants with 128-bit, 192-bit, and 256-bit keys.
  - https://www.nist.gov/publications/advanced-encryption-standard-aes
- Secure PRF from AES
  - If F be a secure PRP, then F is also a secure PRF.
    - HW: see Corollary 6.8 (https://joyofcryptography.com/pdf/chap6.pdf)
- A simple PRG from PRF