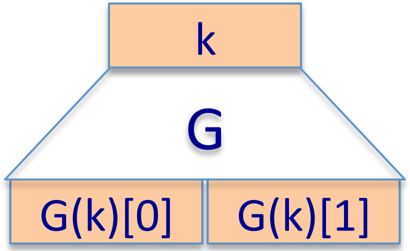
Block ciphers

Block ciphers from PRGs

Can we build a PRF from a PRG?

Let G: K ⟶ K^2 be a secure PRG



Define 1-bit PRF F: K × {0,1} ⟶ K as

$$F(k, x \in \{0,1\}) = G(k)[x]$$

Thm: If G is a secure PRG then F is a secure PRF

Can we build a PRF with a larger domain?

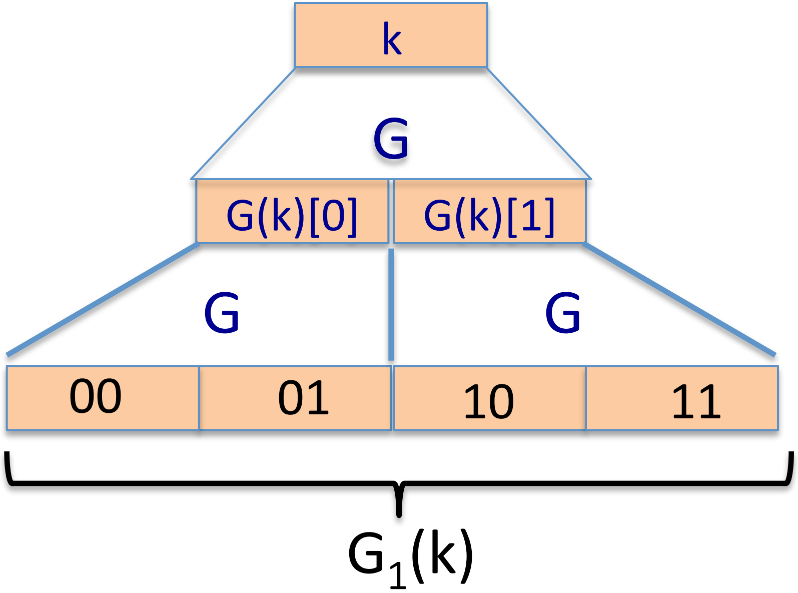
Extending a PRG

Let $G: K \longrightarrow K^2$.

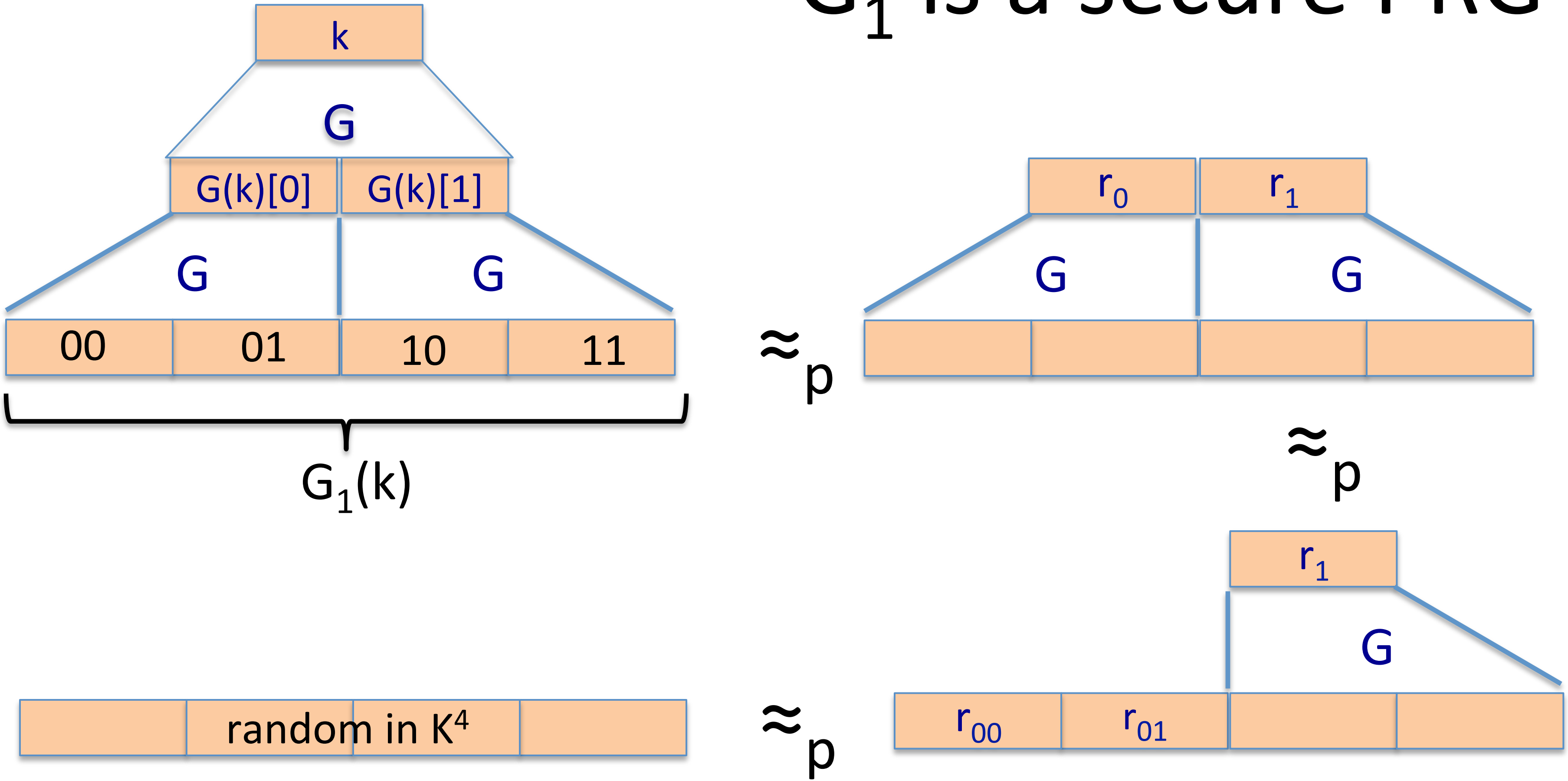
define $G_1: K \longrightarrow K^4$ as $G_1(k) = G\big(G(k)[0]\big) \parallel G\big(G(k)[1]\big)$

We get a 2-bit PRF:

$F(k, x \in \{0,1\}^2) = G_1(k)[x]$



G_1 is a secure PRG

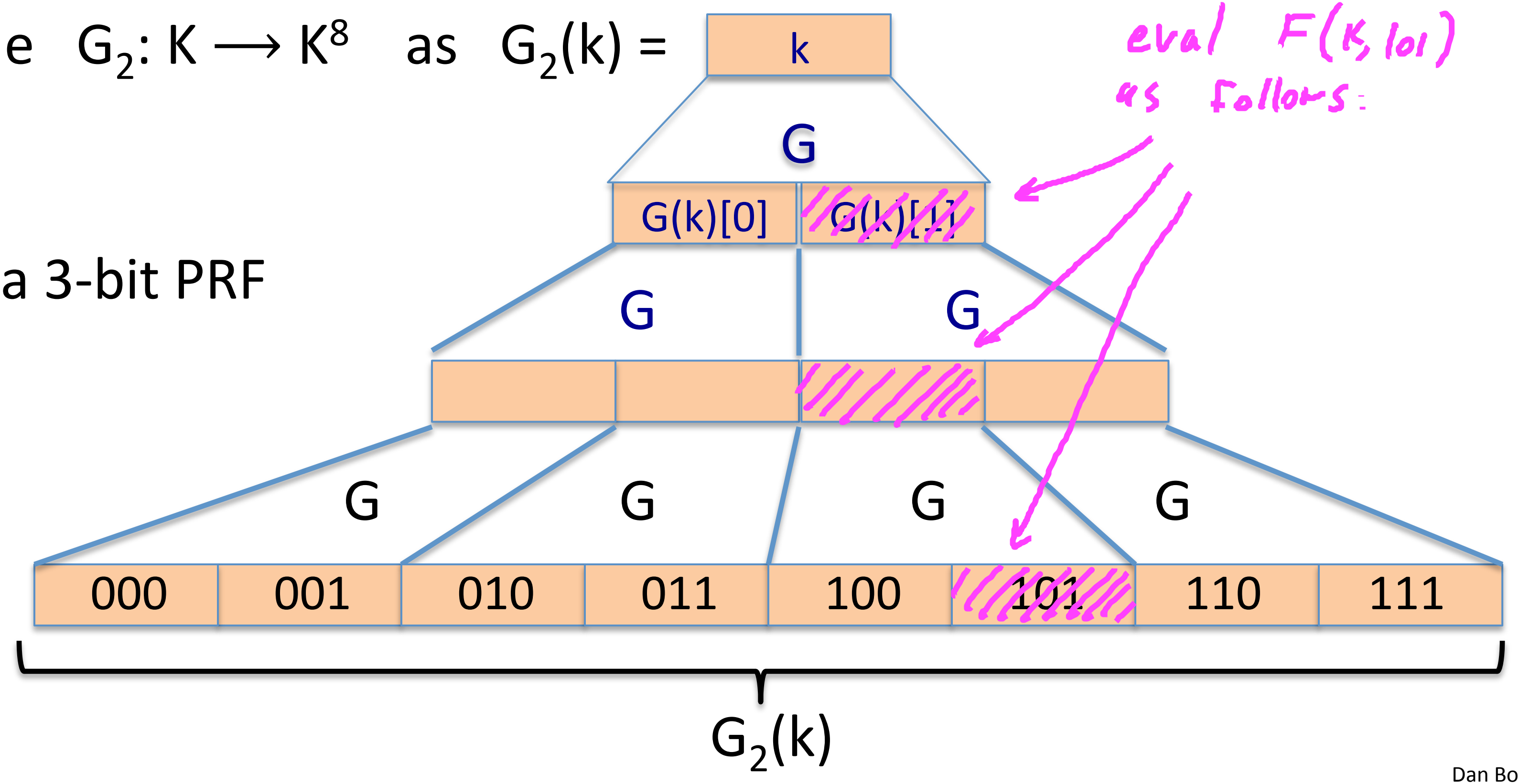


Extending more

Let $G: K \longrightarrow K^2$.

define $G_2: K \longrightarrow K^8$ as $G_2(k) =$

We get a 3-bit PRF



Extending even more: the GGM PRF

Let $G: K \longrightarrow K^2$. define PRF $F: K \times \{0,1\}^n \longrightarrow K$ as

For input $x = x_0\, x_1 \ldots x_{n-1} \in \{0,1\}^n$ do:

$$\begin{tikzcd}
k \arrow[r, "G(k)\lbrack x_0\rbrack"] & k_1 \arrow[r, "G(k_1)\lbrack x_1\rbrack"] & k_2 \arrow[r, "G(k_2)\lbrack x_2\rbrack"] & k_3 & \cdots \arrow[r, "G(k_{n-1})\lbrack x_{n-1}\rbrack"] & k_n
\end{tikzcd}$$

Security: G a secure PRG $\Rightarrow$ F is a secure PRF on $\{0,1\}^n$.

Not used in practice due to slow performance.

Secure block cipher from a PRG?

Can we build a secure PRP from a secure PRG?

○ No, it cannot be done

[✓ ○ Yes, just plug the GGM PRF into the Luby-Rackoff theorem]

○ It depends on the underlying PRG

○

End of Segment