西安電子科技大學
XIDIAN UNIVERSITY

Block cipher

The AES block cipher

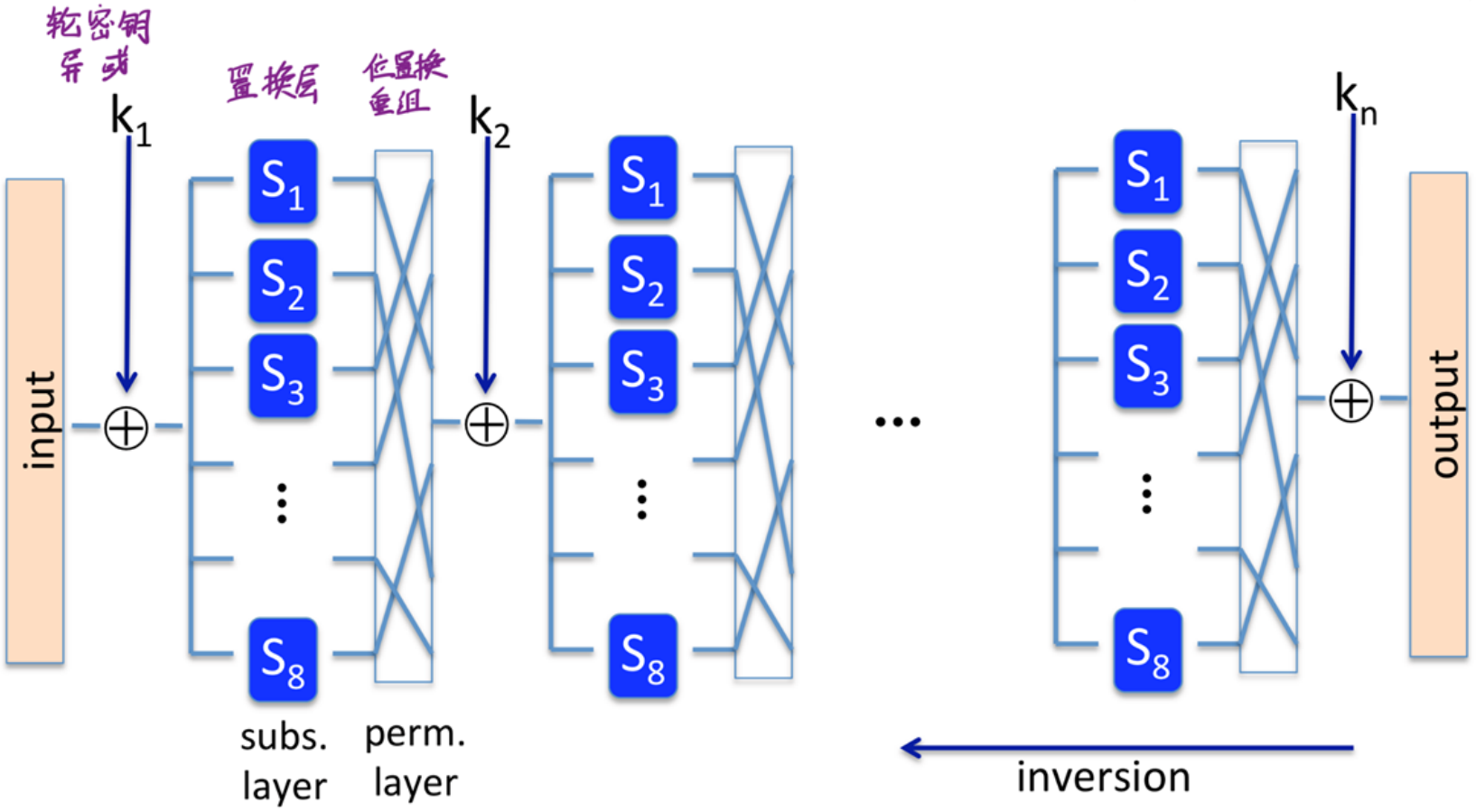
人们逐渐认识到DES和三重DES并不适合加密现代硬件，速度慢，达不到要求

AES

- 块大小—128bit
- 三种秘钥：128bit，192bit，256bit
- 秘钥越大，密码安全性越高，速度越慢

- 使用SPN代换置换网络，而非Faist网络

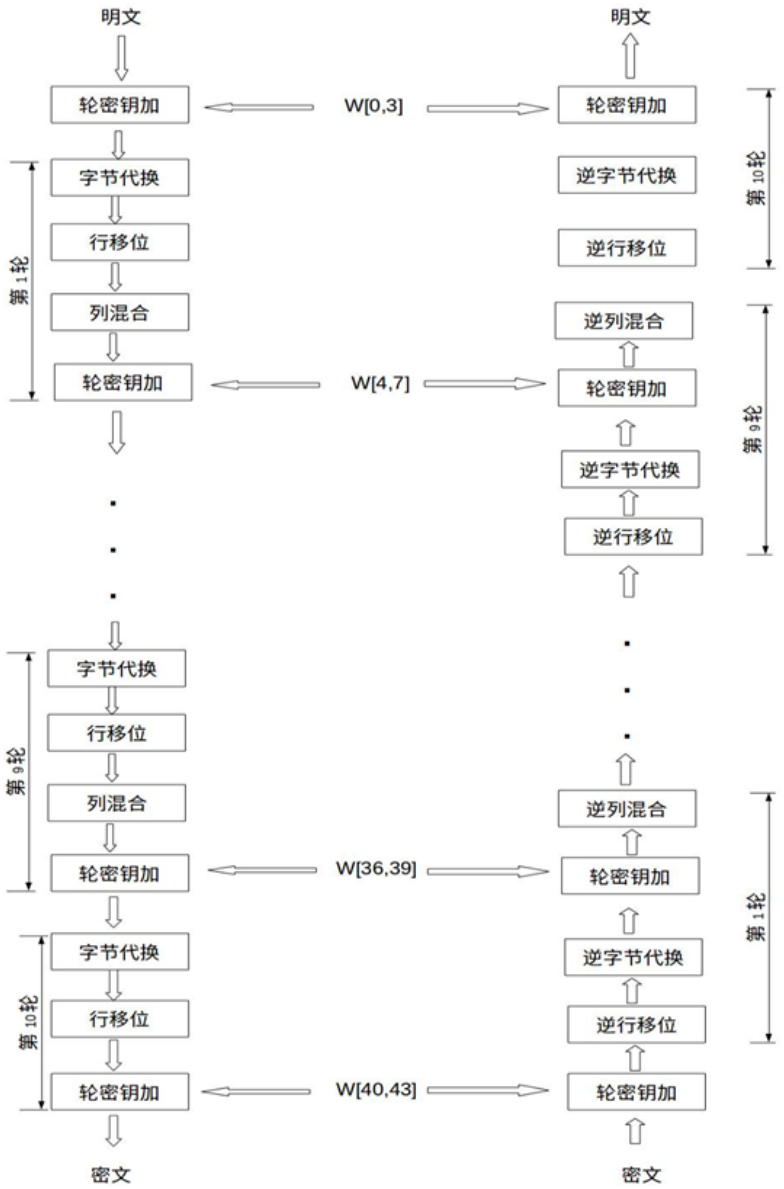
AES is a Subs-Perm network (not Feistel)

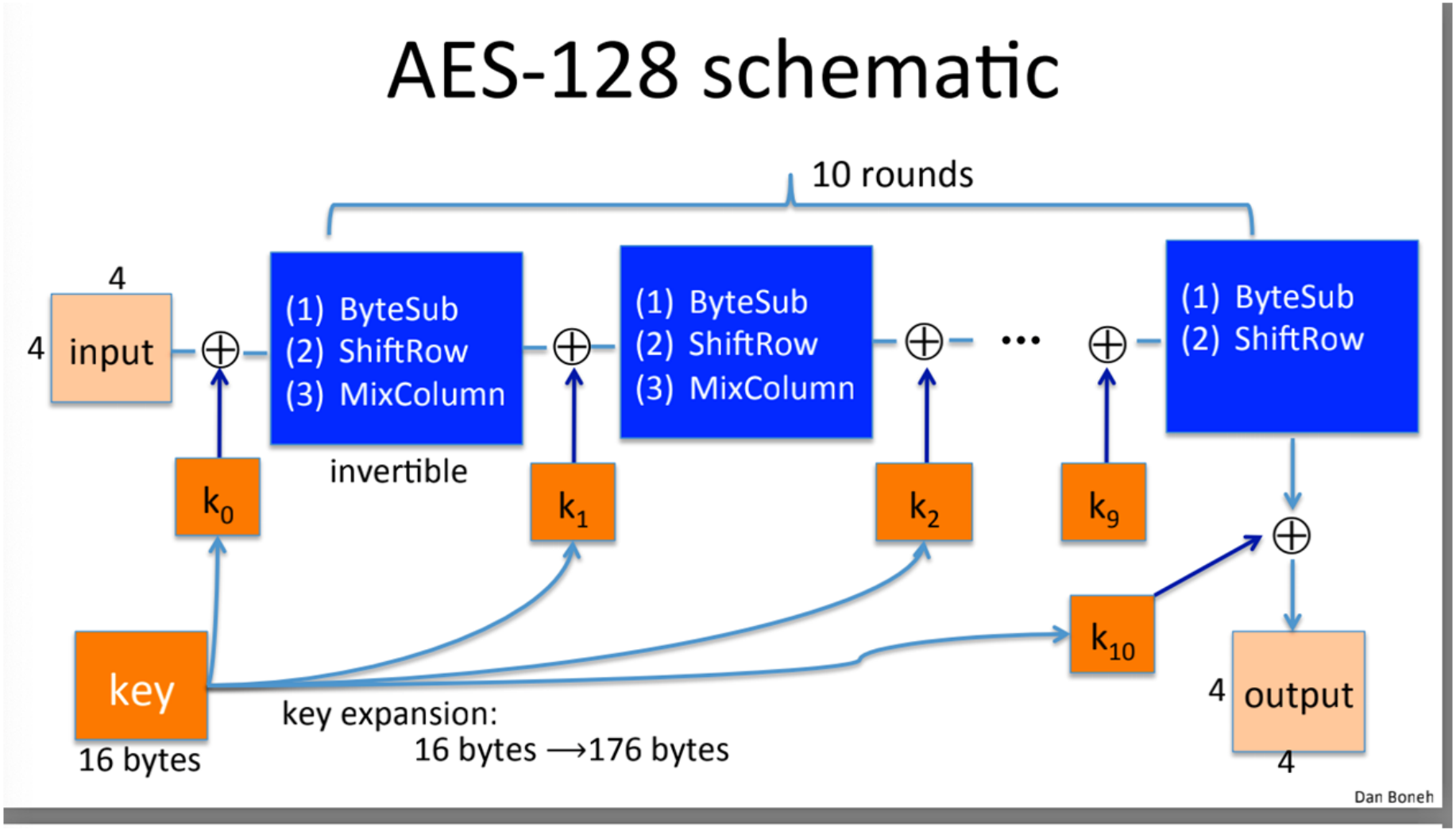


Dan Bone

AES加密

- 轮密钥加密
- 字节代换
- 行移位
- 列混合




AES-128 schematic
10 rounds
4
4
input
(1) ByteSub
(2) ShiftRow
(3) MixColumn
invertible
(1) ByteSub
(2) ShiftRow
(3) MixColumn
(1) ByteSub
(2) ShiftRow
k0
k1
k2
k9
k10
key
16 bytes
key expansion:
16 bytes ⟶176 bytes
4
output
4
Dan Boneh

- AES加密：轮密钥加是将128位轮密钥Ki同状态矩阵中的数据进行逐位异或操作

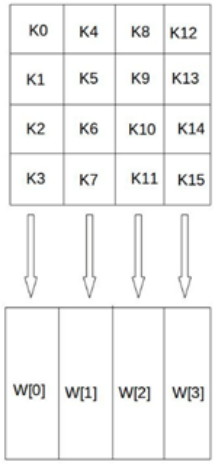
- 秘钥扩展：
- 递归产生新矩阵

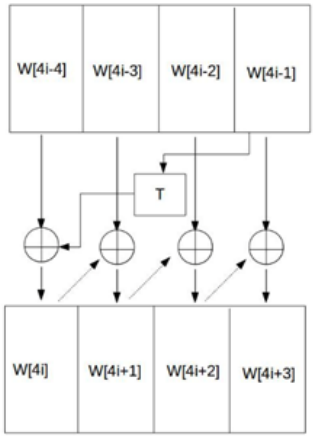
-a.字循环：将1个字中的4个字节循环左移1个字节。即将输入字[b0, b1, b2, b3]变换成[b1,b2,b3,b0]

-b.字节代换：对字循环的结果使用S盒进行字节代换

-c.轮常量异或：将前两步的结果同轮常量Rcon[j]进行异或

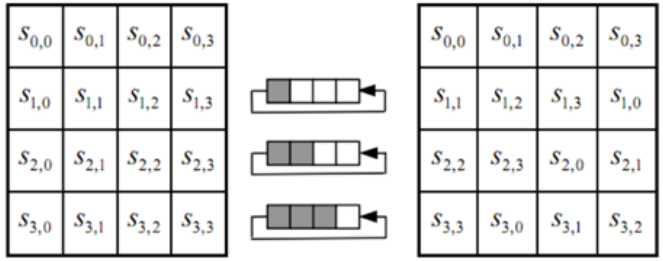
j	1	2	3	4	5
Rcon[j]	01 00 00 00	02 00 00 00	04 00 00 00	08 00 00 00	10 00 00 00
j	6	7	8	9	10
Rcon[j]	20 00 00 00	40 00 00 00	80 00 00 00	1B 00 00 00	36 00 00 00



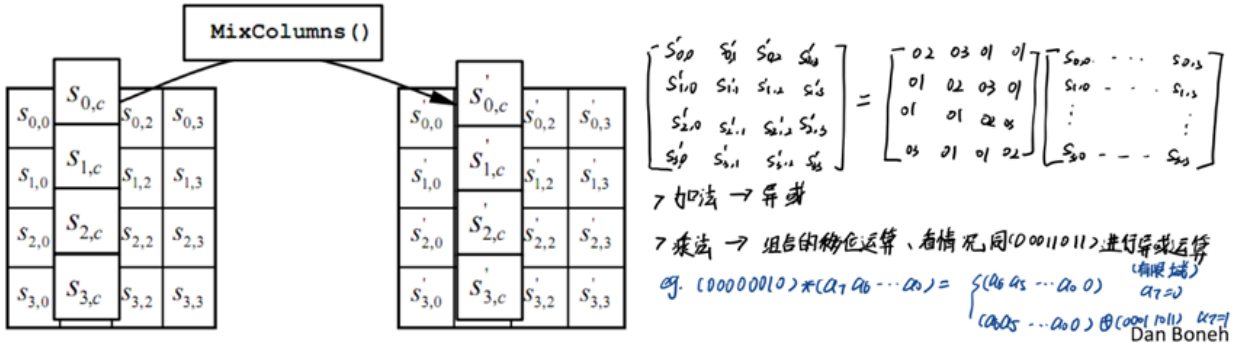


The round function

- **ByteSub**: a 1 byte S-box. 256 byte table (easily computable)
- **ShiftRows**:



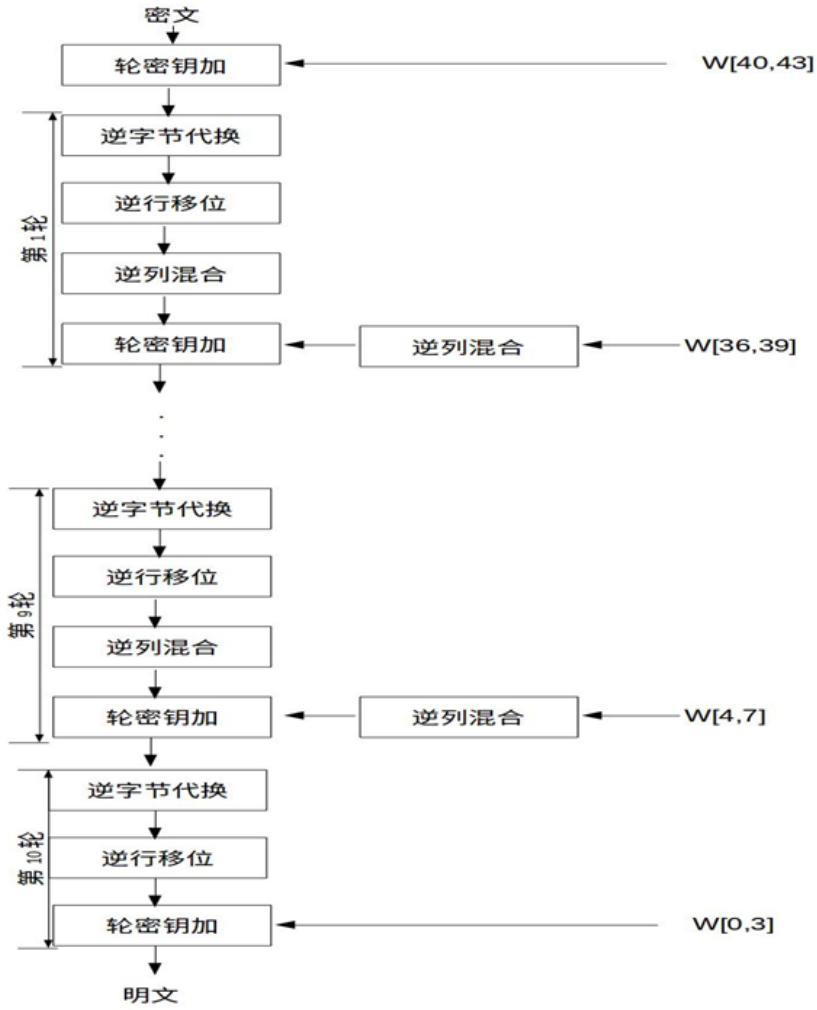
- **MixColumns**:



逆变换矩阵同正变换矩阵的乘积恰好为单位矩阵。

AES解密

- 逆过程


密文
轮密钥加
W[40,43]
逆字节代换
逆行移位
逆列混合
第1轮
轮密钥加
逆列混合
W[36,39]
逆字节代换
逆行移位
逆列混合
第9轮
轮密钥加
逆列混合
W[4,7]
逆字节代换
逆行移位
第10轮
轮密钥加
W[0,3]
明文

Code size/performance tradeoff

	Code size	Performance
Pre-compute round functions (24KB or 4KB)	largest	fastest: table lookups and xors
Pre-compute S-box only (256 bytes)	smaller	slower
No pre-computation	smallest	slowest

Dan Boneh

AES in hardware

aesenc : ByteSub、ShiftRow、MixColumn
aesenclast : Bytesub、shiftRow

AES instructions in Intel Westmere:

- **aesenc, aesenclast**: do one round of AES 9x aesenc + 1x aesenclast

  128-bit registers: xmm1=state, xmm2=round key

  aesenc xmm1, xmm2 ; puts result in xmm1

- **aeskeygenassist**: performs AES key expansion
- Claim 14 x speed-up over OpenSSL on same hardware

Similar instructions on AMD Bulldozer

Attacks

Best key recovery attack:

four times better than ex. search [BKR'11]

Related key attack on AES-256: [BK'09]

Given 2^{99} inp/out pairs from **four related keys** in AES-256

can recover keys in time $\approx 2^{99}$

Dan Boneh

•相关秘钥攻击(秘钥间汉明距离小)对AES加密造成的实用局限性影响不大
•因为相关秘钥攻击，key要相关，因此随机选取秘钥，保证系统秘钥不会相互关联

西安电子科技大学
XIDIAN UNIVERSITY

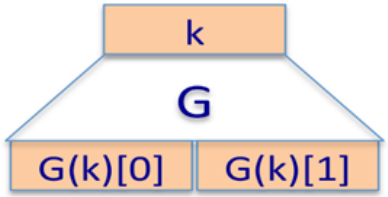
Block cipher

Block ciphers from PRGs

Can we build a PRF from a PRG?

Let G: K ⟶ K^2 be a secure PRG

means: 输出与K^2密钥空间一个真正随机元素无法区别



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?

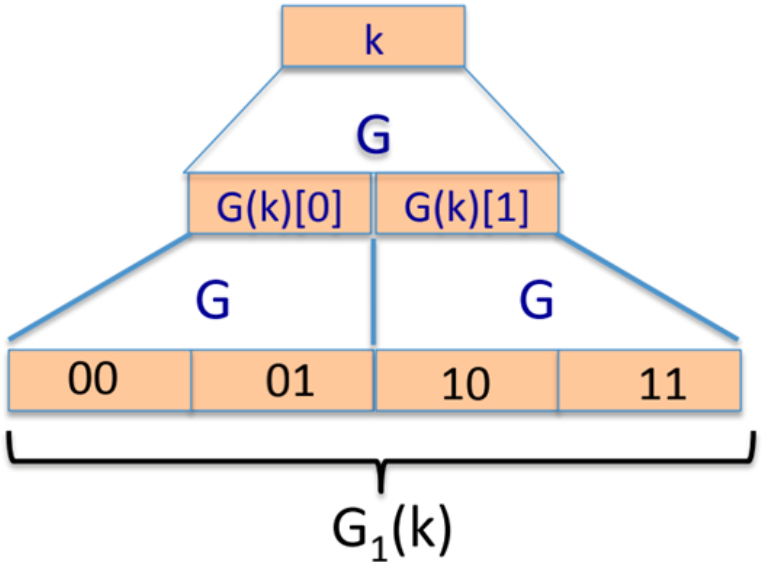
Extending a PRG

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

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

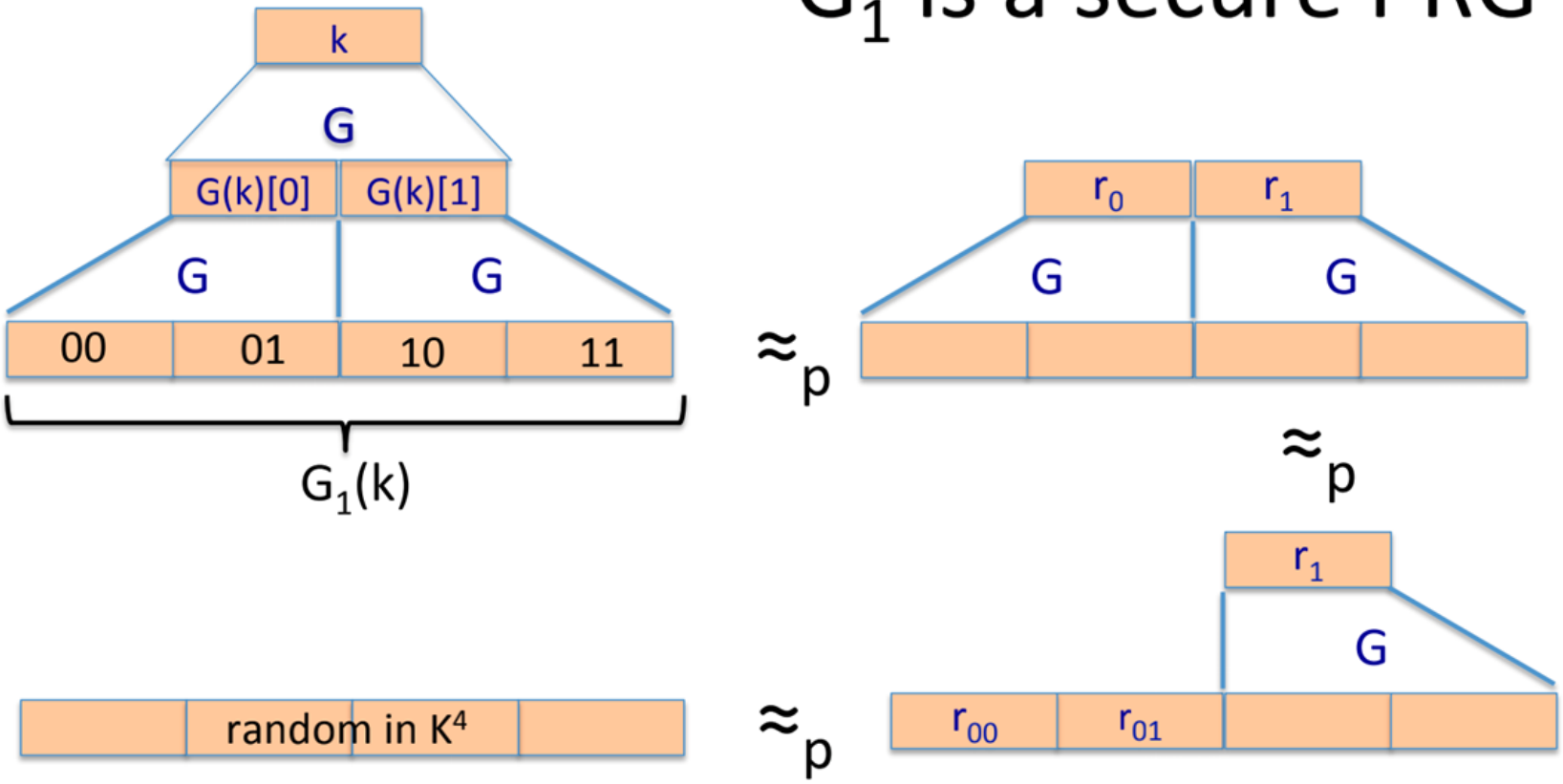
We get a 2-bit PRF:

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



Dan Boneh

G_1 is a secure PRG



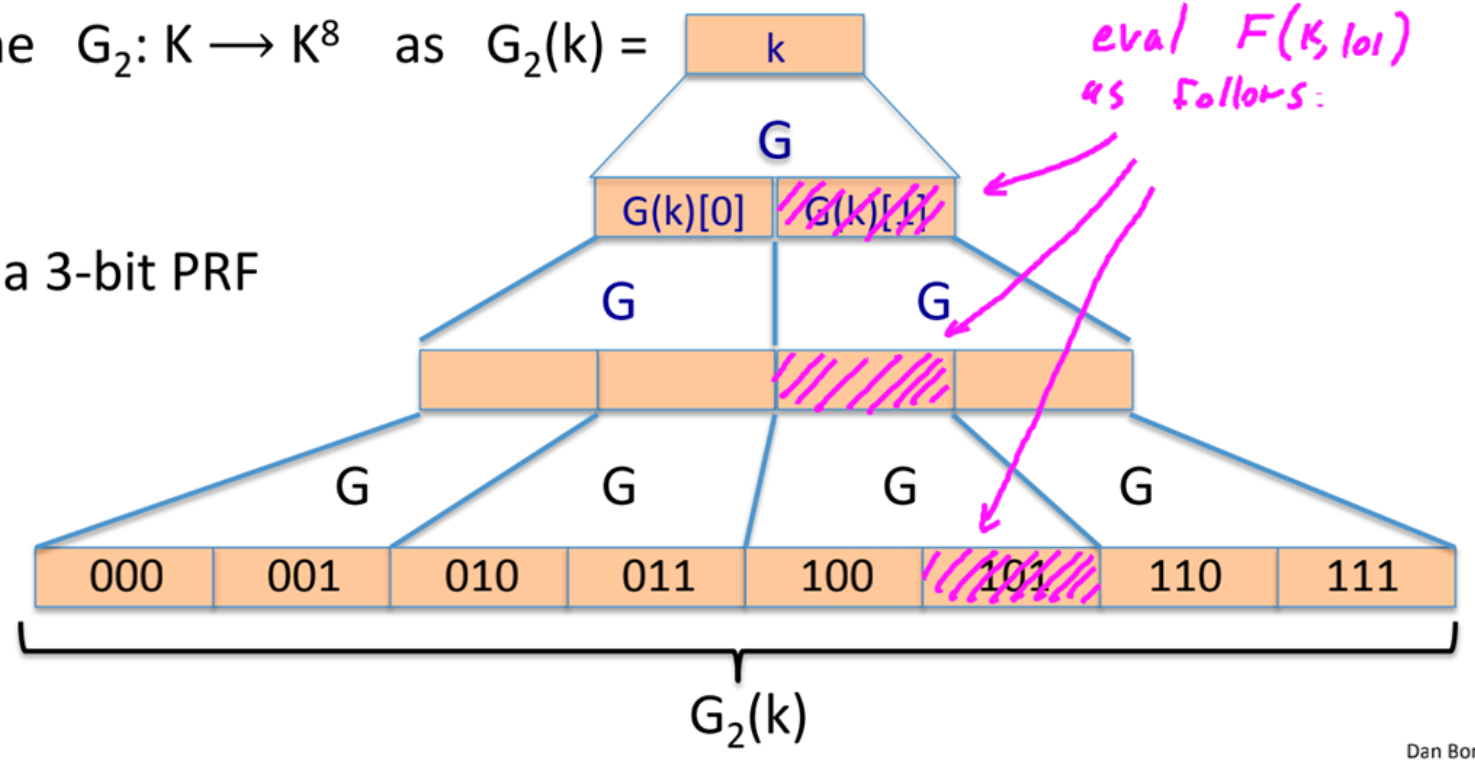
Dan Boneh

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

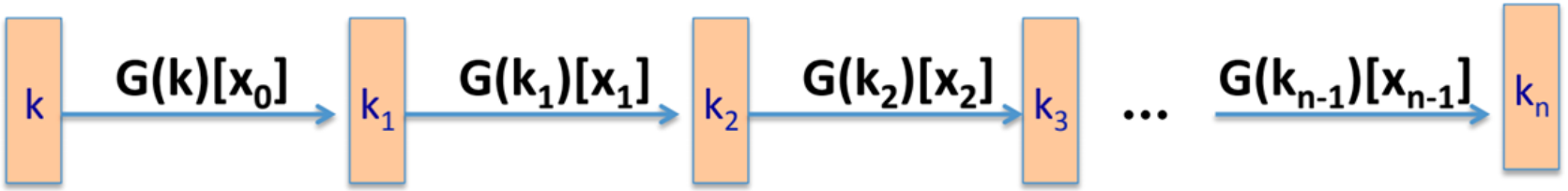


Dan Boneh

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:



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

Not used in practice due to slow performance.

Dan Boneh

- 工作速度慢，实际中不应用

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
- ○

西安電子科技大學
XIDIAN UNIVERSITY

Thanks for listening