LDACS1310: Introduction to Applied Cryptography

Lecture 3: block ciphers

T. Peters, ***F.-X. Standaert***

UCLouvain Crypto Group, fstandae@uclouvain.be

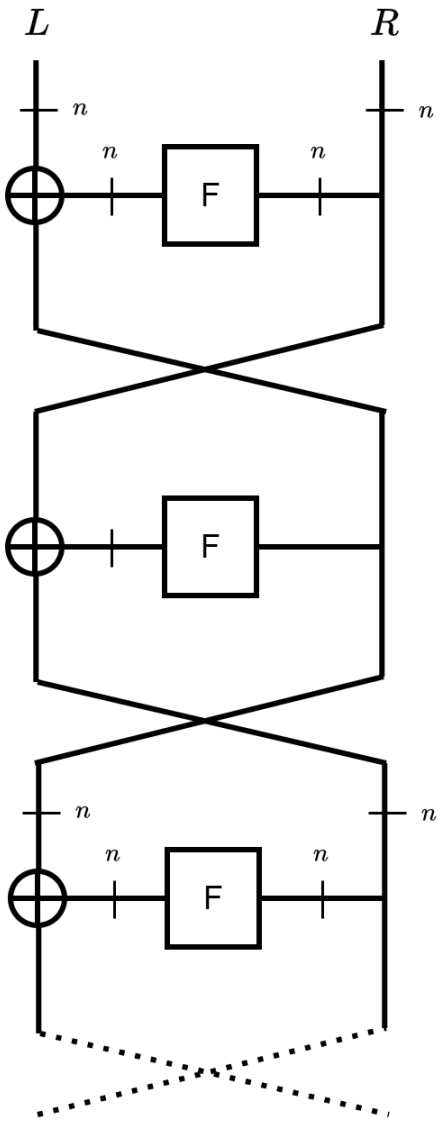
Reminder



https://perso.uclouvain.be/fstandae/LDACS1310/

And questions from last lecture?

Assumptions dilemma: P from F



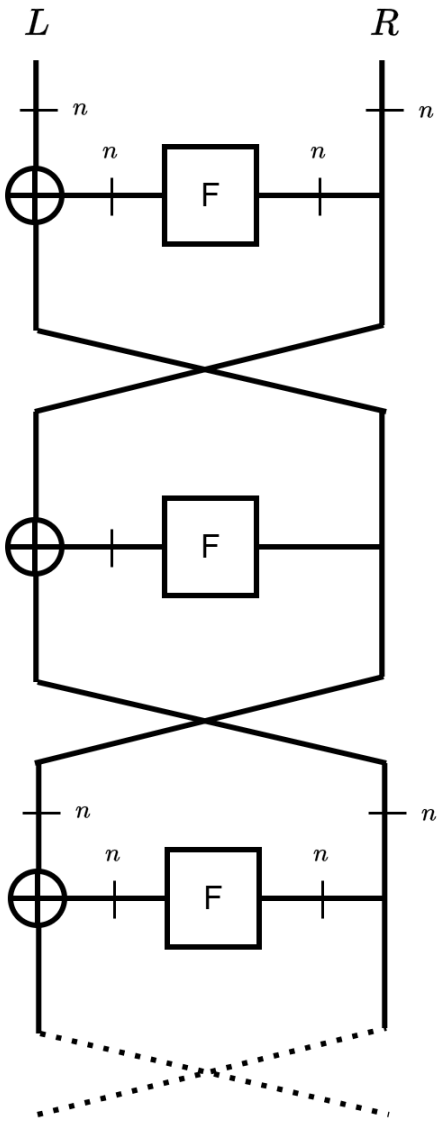
- $\mathrm{F} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$
  $\Rightarrow \mathrm{P} : \{0,1\}^n \times \{0,1\}^{2n} \to \{0,1\}^{2n}$

3 rounds: $\epsilon_{\mathrm{P}} \approx \frac{q^2}{2^n} + 3 \cdot \epsilon_{\mathrm{F}}$

How to invert? Is it tight? {…}

[*Luby, Rackoff, SIAM 1988*]

Assumptions dilemma: P from F



- $\mathrm{F} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$
  $\Rightarrow \mathrm{P} : \{0,1\}^n \times \{0,1\}^{2n} \to \{0,1\}^{2n}$

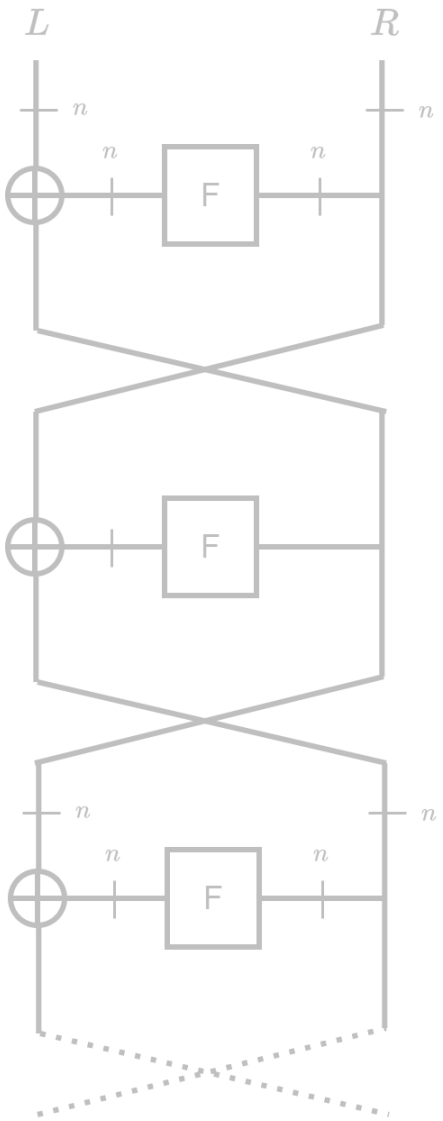
3 rounds: $\epsilon_{\mathrm{P}} \approx \frac{q^2}{2^n} + 3 \cdot \epsilon_{\mathrm{F}}$

How to invert? Is it tight? {…}

7+ rounds: $\epsilon_{\mathrm{P}} \approx 2^{\mathrm{n} \cdot (1-\alpha)} + 3 \cdot \epsilon_{\mathrm{F}}$

[*Luby, Rackoff, SIAM 1988*]

Assumptions dilemma: P from F



- $\mathrm{F} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$
  $\Rightarrow \mathrm{P} : \{0,1\}^n \times \{0,1\}^{2n} \to \{0,1\}^{2n}$

3 rounds: $\epsilon_{\mathrm{P}} \approx \frac{q^2}{2^n} + 3 \cdot \epsilon_{\mathrm{F}}$

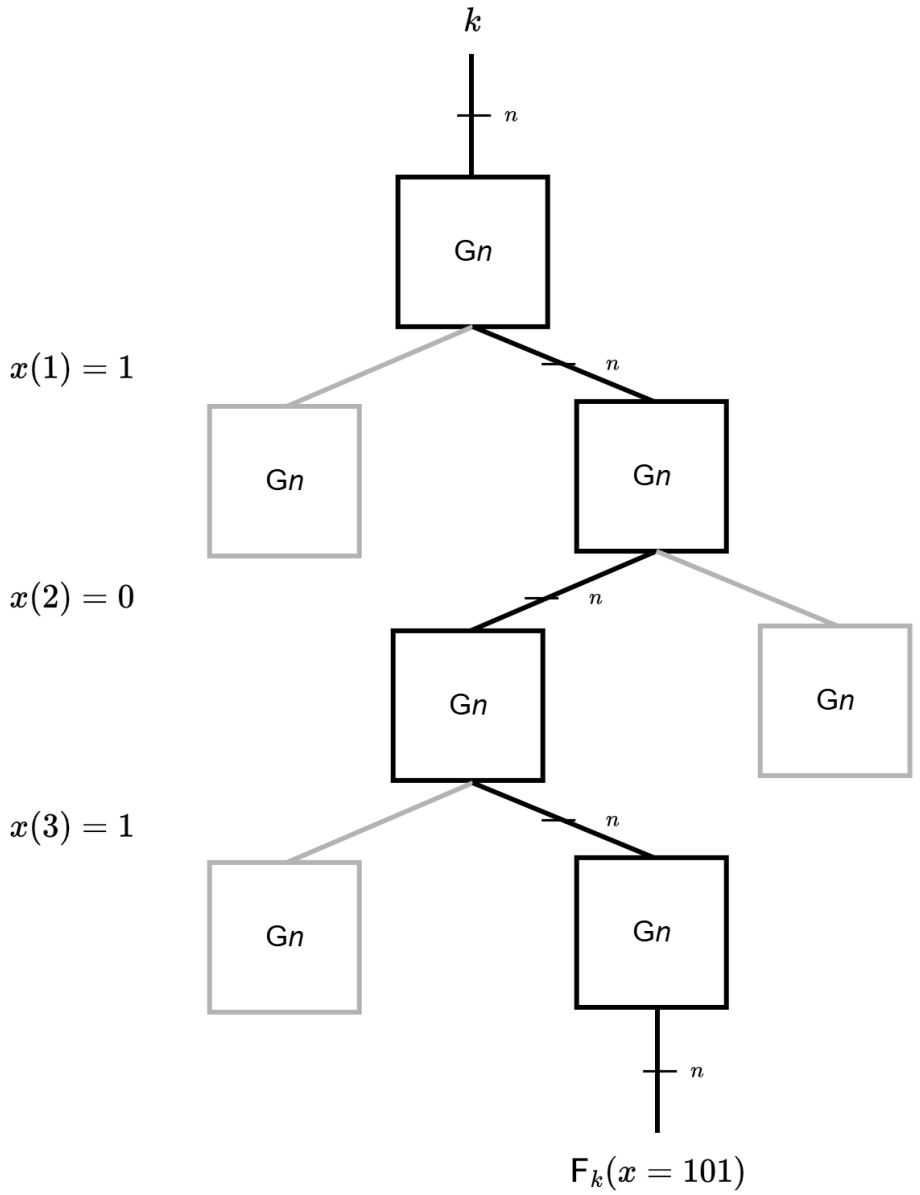
How to invert? Is it tight? {…}

7+ rounds: $\epsilon_{\mathrm{P}} \approx 2^{n \cdot (1-\alpha)} + 3 \cdot \epsilon_{\mathrm{F}}$

- Reverse direction is trivial (use the PRP as PRF) but $\epsilon_{\mathrm{F}} \approx \frac{q^2}{2^{2n}} + \epsilon_{\mathrm{P}}$

[*Luby, Rackoff, SIAM 1988*]

Assumptions dilemma: F from G*n*



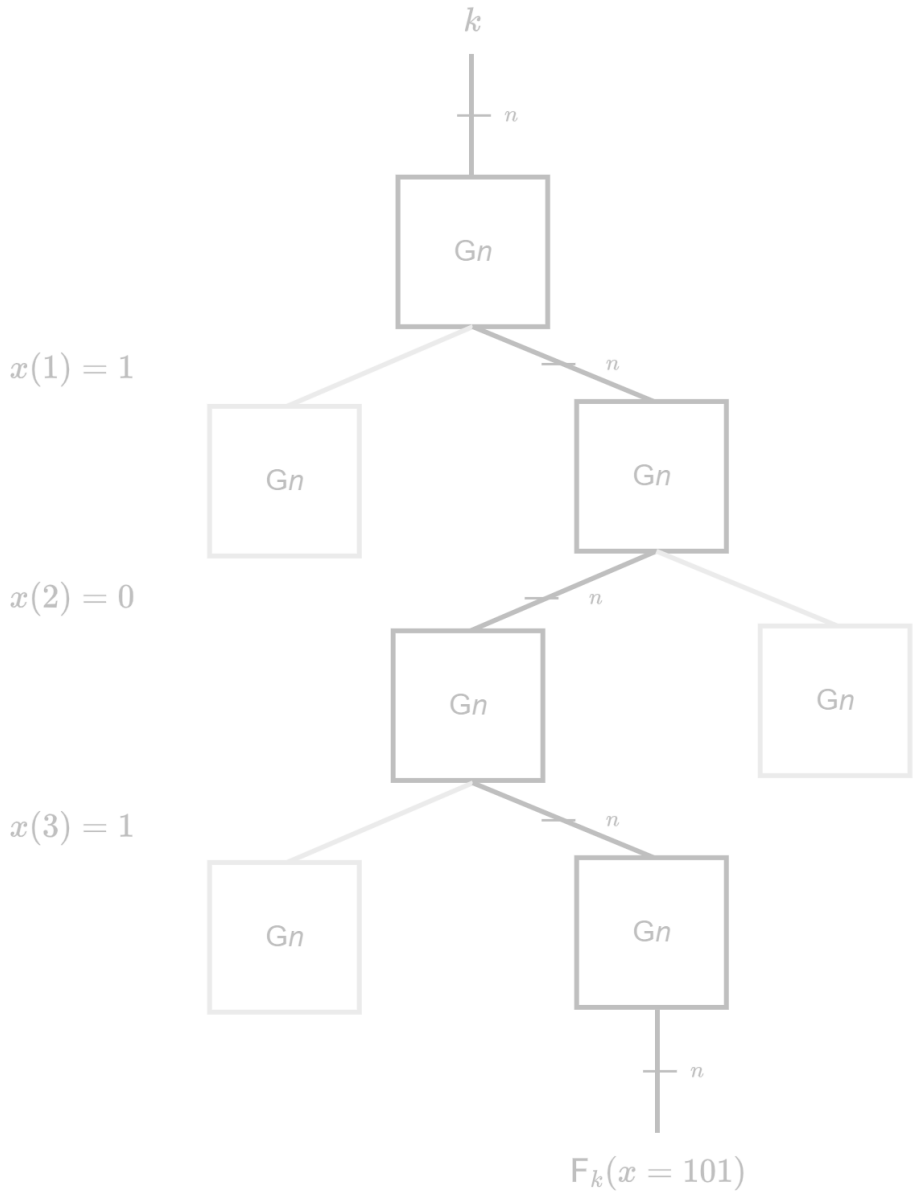
- $\mathsf{G}n: \{0,1\}^n \to \{0,1\}^{2n}$
  $\Rightarrow \mathsf{F} : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}^n$

$$\epsilon_{\mathrm{F}} \approx q \cdot m \cdot \epsilon_{\mathrm{G}n}$$

Is it tight? {…}

[*Goldreich, Goldwasser, Micali, FOCS 1984*]

Assumptions dilemma: F from G*n*



- $\mathrm{G}n: \{0,1\}^n \to \{0,1\}^{2n}$
  $\Rightarrow \mathrm{F} : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}^n$

$$\epsilon_{\mathrm{F}} \approx q \cdot m \cdot \epsilon_{\mathrm{G}n}$$

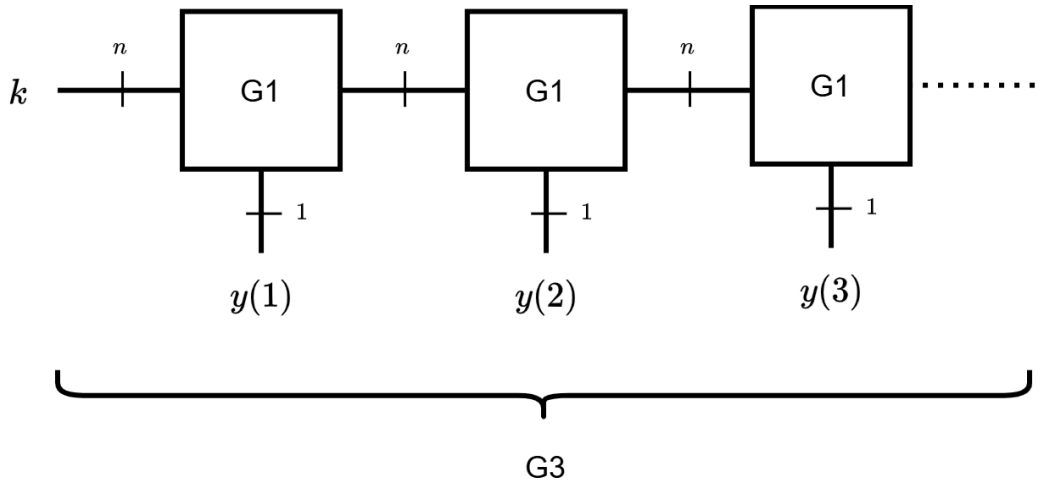
Is it tight? {…}

- Reverse direction is trivial (just use a counter as PRF input)

[*Goldreich, Goldwasser, Micali, FOCS 1984*]

Assumptions dilemma: G*n* from G1

- $\mathrm{G1}: \{0,1\}^n \to \{0,1\}^l \Rightarrow \mathrm{G}n: \{0,1\}^n \to \{0,1\}^{2n}$



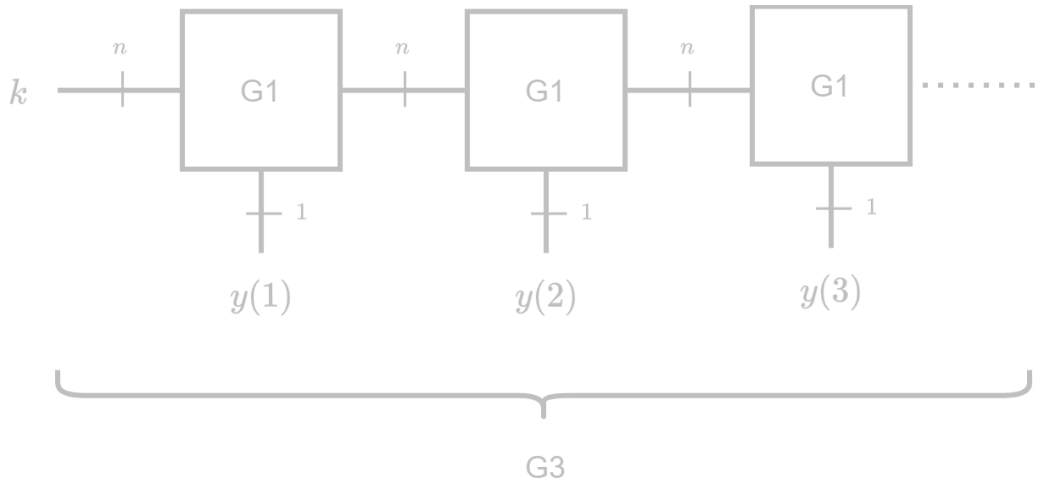
$\epsilon_{\mathrm{G}n} \approx n \cdot \epsilon_{\mathrm{G1}}$

Is it tight? {…}

[*Yao, FOCS 1982*]

Assumptions dilemma: G*n* from G1

- $\mathrm{G1}: \{0,1\}^n \to \{0,1\}^l \Rightarrow \mathrm{G}n: \{0,1\}^n \to \{0,1\}^{2n}$



$\epsilon_{\mathrm{G}n} \approx n \cdot \epsilon_{\mathrm{G1}}$

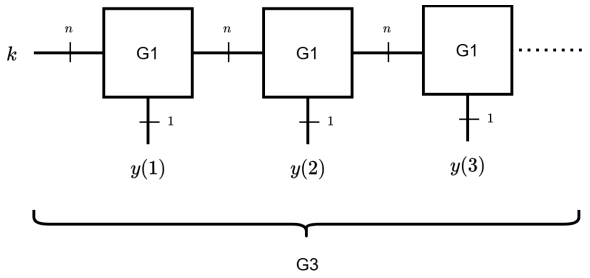
Is it tight? {…}

- Reverse direction is trivial (just take one bit out of n)

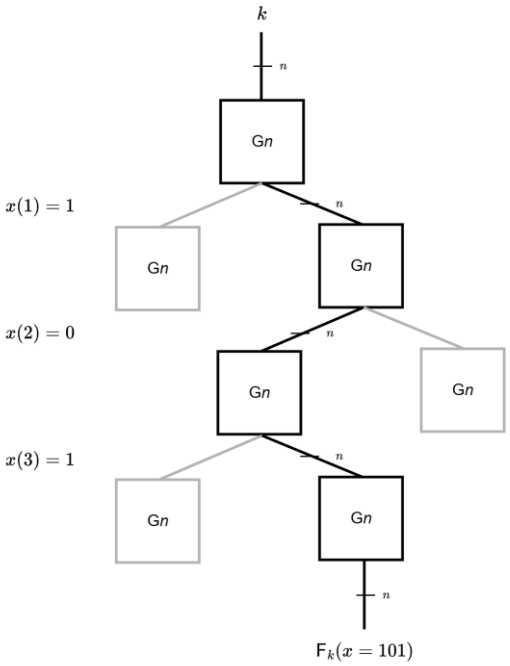
[*Yao, FOCS 1982*]

Efficiency challenge

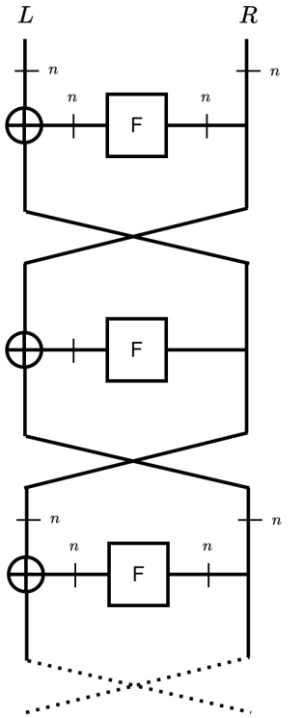
- Question: say $n = 128$, G1 takes 1ms, how long for 16 PRP rounds?



+



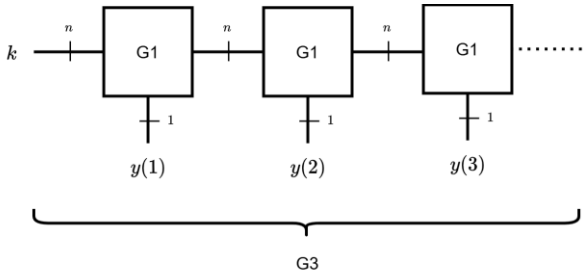
+



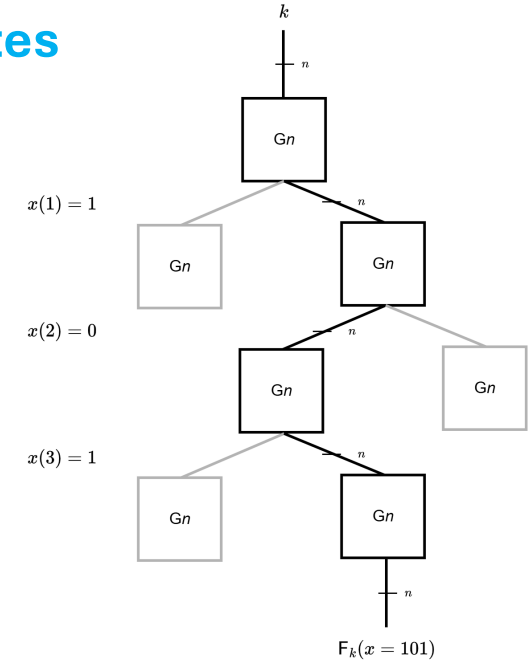
Efficiency challenge

- Question: say $n = 128$, G1 takes 1ms, how long for 16 PRP rounds?

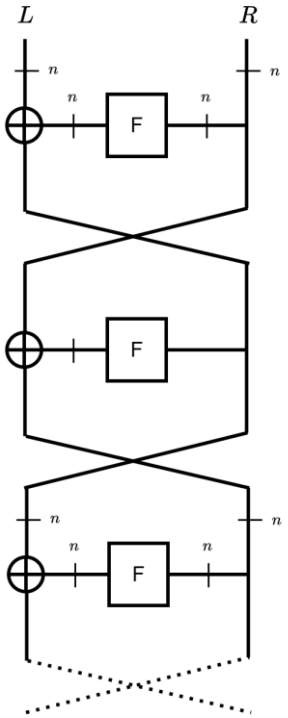
$16 \times 128 \times 128 = 2^{18}$ ms $\approx$ **4 minutes**



+



+



⇒ Strong motivation for direct PRP design (≈ heuristic shortcut)

Efficiency challenge, revisited

- Question: to design a 128-bit PRP, why not picking it at random and storing it as a table?

Efficiency challenge, revisited

- Question: to design a 128-bit PRP, why not picking it at random and storing it as a table? Table would have size $(2^{128} \times 128)$

- Question: could a n-bit PRP be linear, e.g., $y = A \cdot (x \oplus k)$ with A defined as a $n \times n$ invertible (bit) matrix in $\mathbb{F}_2$?
  - How many such linear functions are there?

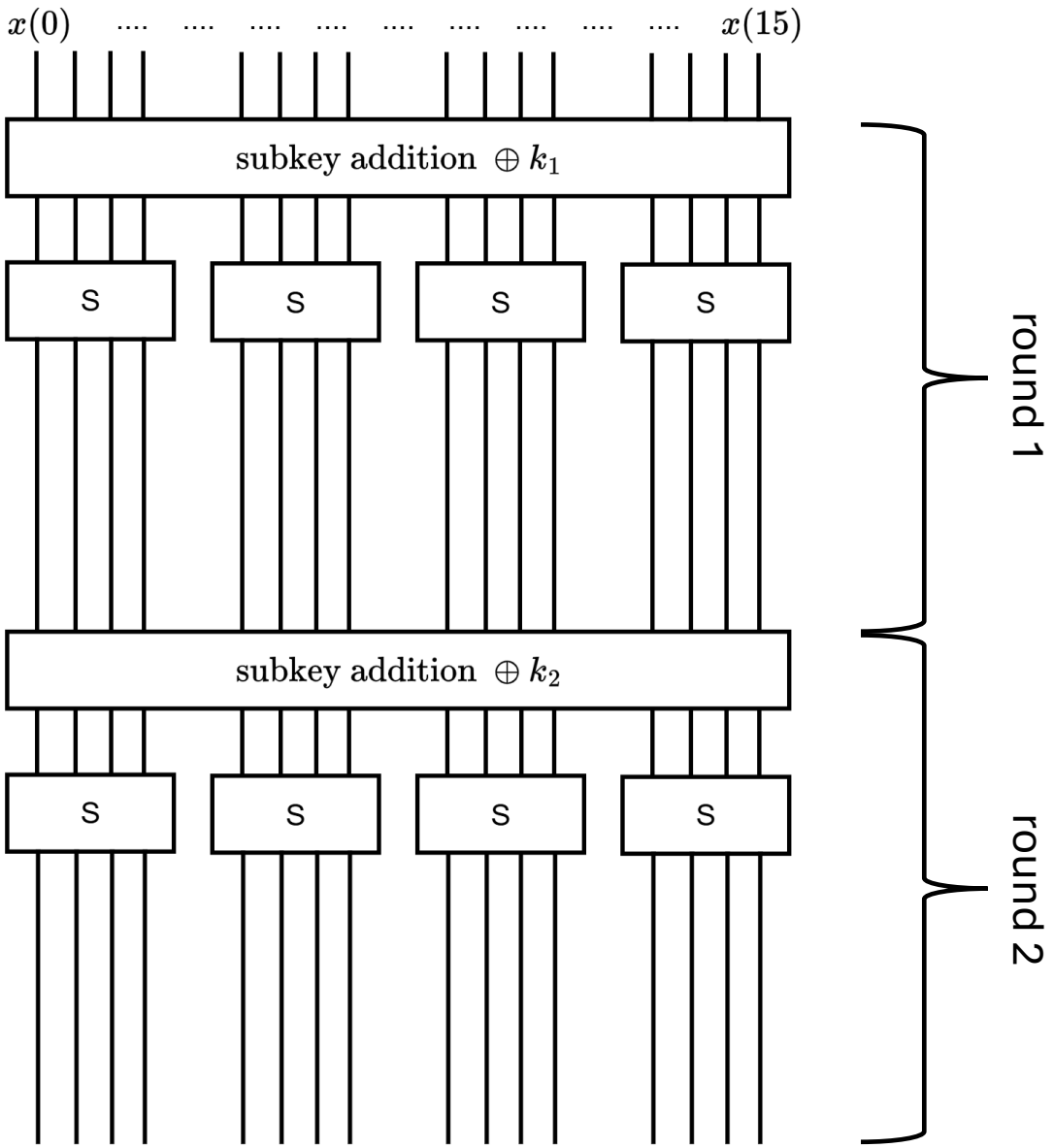
Efficiency challenge, revisited

- Question: to design a 128-bit PRP, why not picking it at random and storing it as a table? Table would have size $(2^{128} \times 128)$

- Question: could a n-bit PRP be linear, e.g., $y = A \cdot (x \oplus k)$ with A defined as a $n \times n$ invertible (bit) matrix in $\mathbb{F}_2$?
  - How many such linear functions are there? $n \cdot 2^n$
  - Complexity of solving a system of n linear equations in n variables? $\mathcal{O}(n^\omega)$ with $\omega = 3$ (Gaussian elimination) or $\omega = 2.3$ (fast algebra)

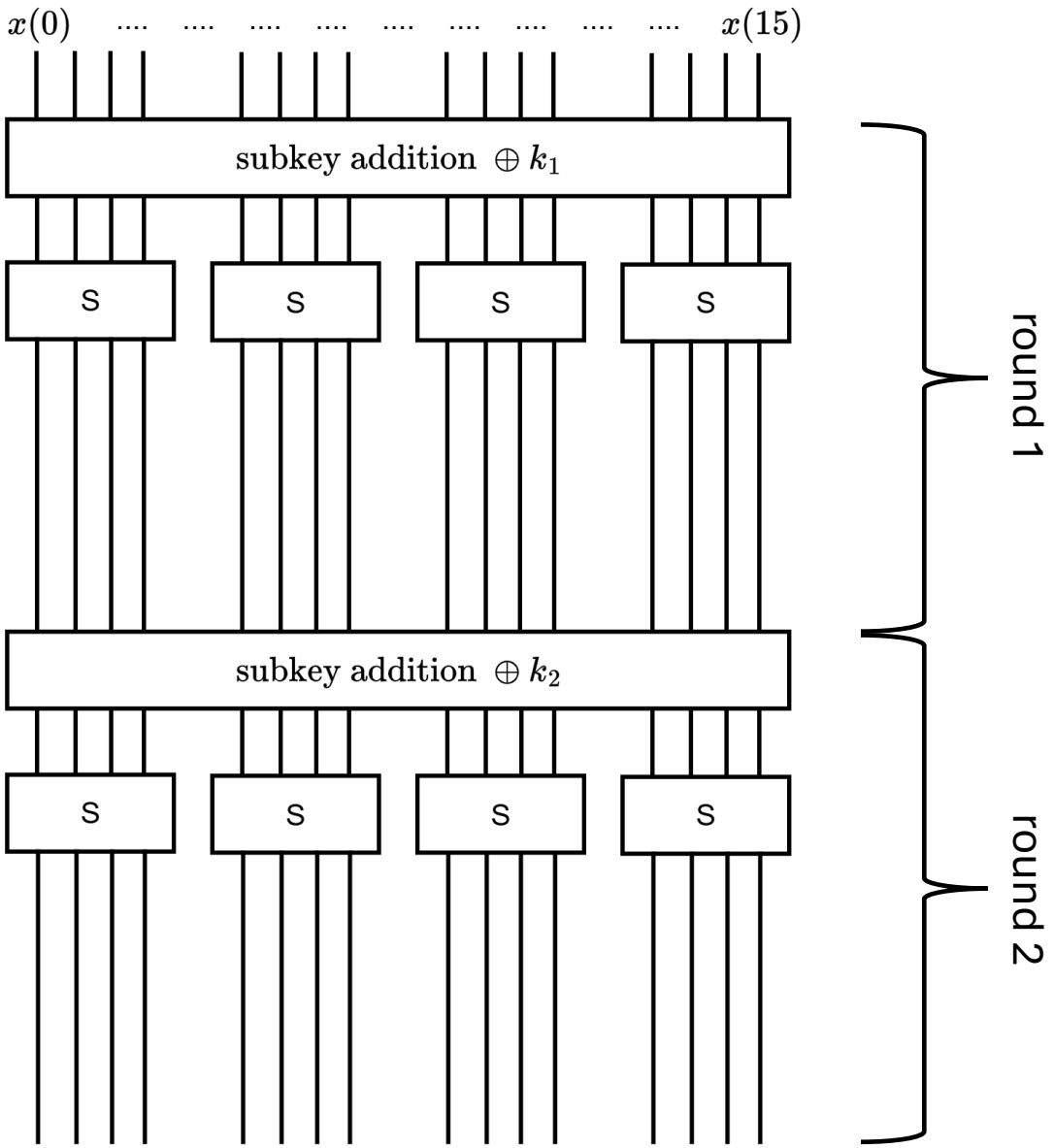
⇒ Block ciphers (≈ efficient PRP) must be non-linear (bring *confusion*)

Key alternating cipher



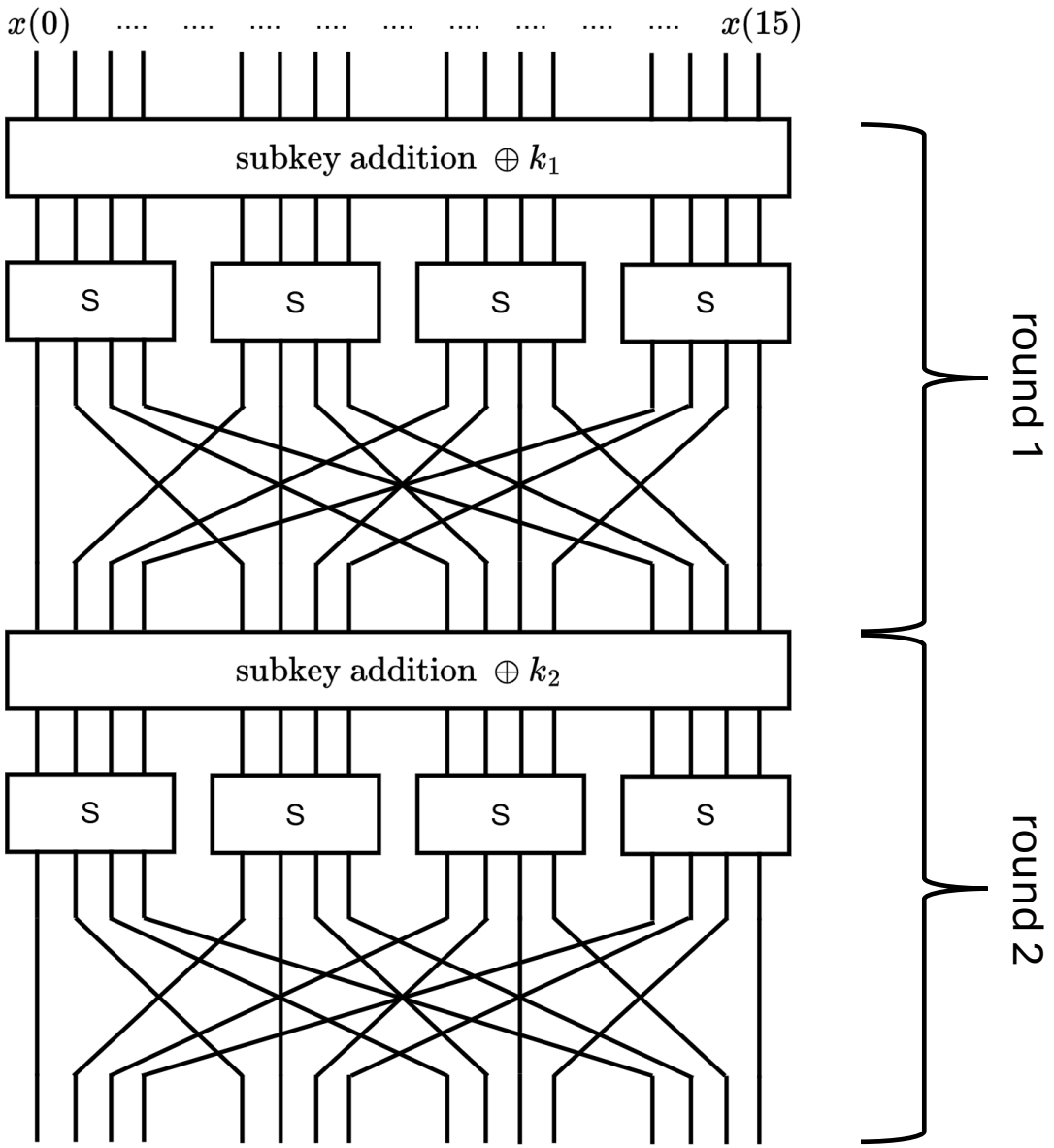
- Question: say S is a (small) random permutation (called S-box), what is the complexity of an exhaustive key search against the toy block cipher of the figure?
  - Expected:
  - Observed:

Key alternating cipher



- Question: say S is a (small) random permutation (called S-box), what is the complexity of an exhaustive key search against the toy block cipher of the figure?
  - Expected: 2^{16} $(2^{4 \cdot 4})$
  - Observed: $4 \cdot 2^4$

Key alternating cipher



- Question: say S is a (small) random permutation (called S-box), what is the complexity of an exhaustive key search against the toy block cipher of the figure?
  - Expected: 2^{16} $(2^{4\cdot 4})$
  - Observed: $4 \cdot 2^4$

⇒ Block ciphers also need *diffusion*

Algebraic cryptanalysis

- Even simpler toy example x and k are 2-bit wide and

$$y(0) = x(0) \oplus k(0) \qquad y(1) = x(1) \oplus k(1)$$
$$z(0) = y(0) \cdot y(1) \qquad z(1) = y(1) \oplus y(1)$$

2-bit key addition and S-box

- Leading to $z(0) = x(0) \cdot x(1) \oplus x(0) \cdot k(1) \oplus x(1) \cdot k(0) \oplus k(0) \cdot k(1)$

$$z(1) = x(0) \oplus x(1) \oplus k(0) \oplus k(1)$$

Algebraic cryptanalysis

- Even simpler toy example x and k are 2-bit wide and

$$y(0) = x(0) \oplus k(0) \qquad y(1) = x(1) \oplus k(1)$$
$$z(0) = y(0) \cdot y(1) \qquad z(1) = y(1) \oplus y(1)$$

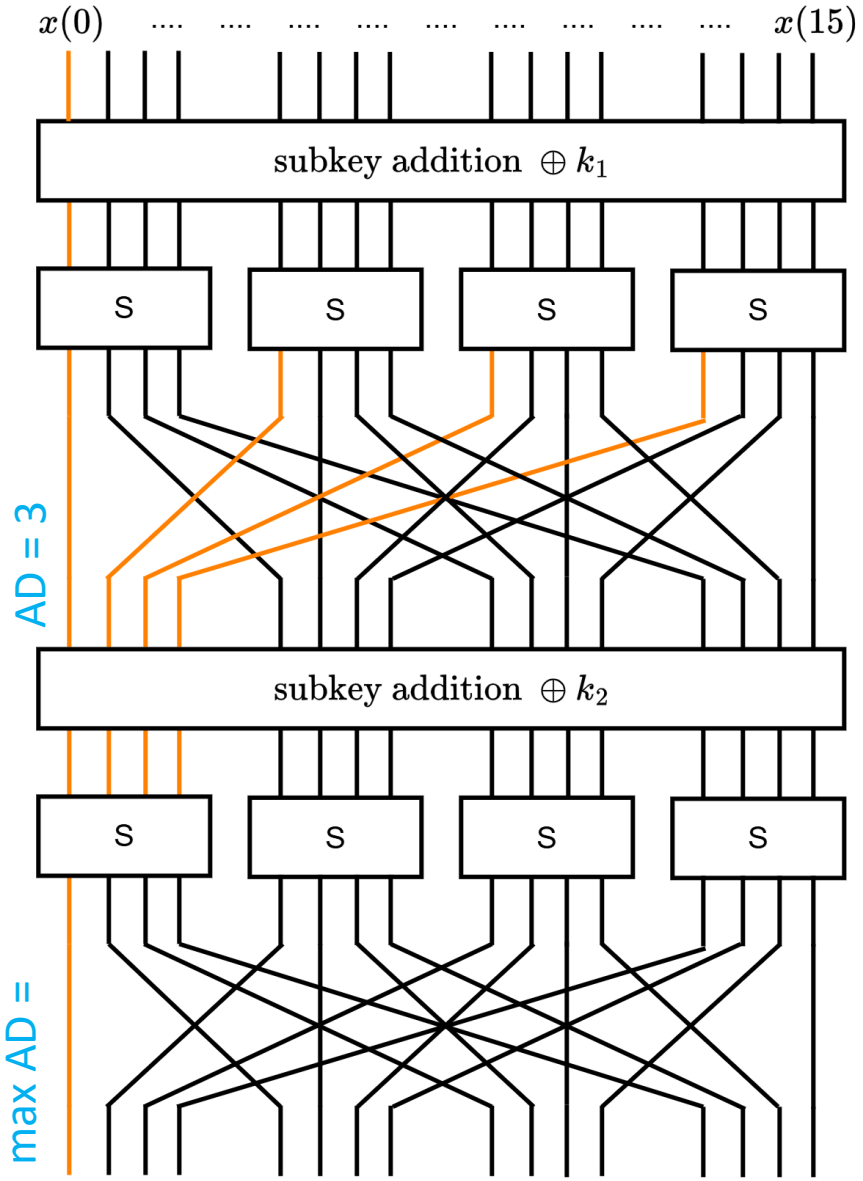
} 2-bit key addition and S-box

- Leading to $z(0) = x(0) \cdot x(1) \oplus x(0) \cdot k(1) \oplus x(1) \cdot k(0) \oplus k(0) \cdot k(1)$

$$z(1) = x(0) \oplus x(1) \oplus k(0) \oplus k(1)$$

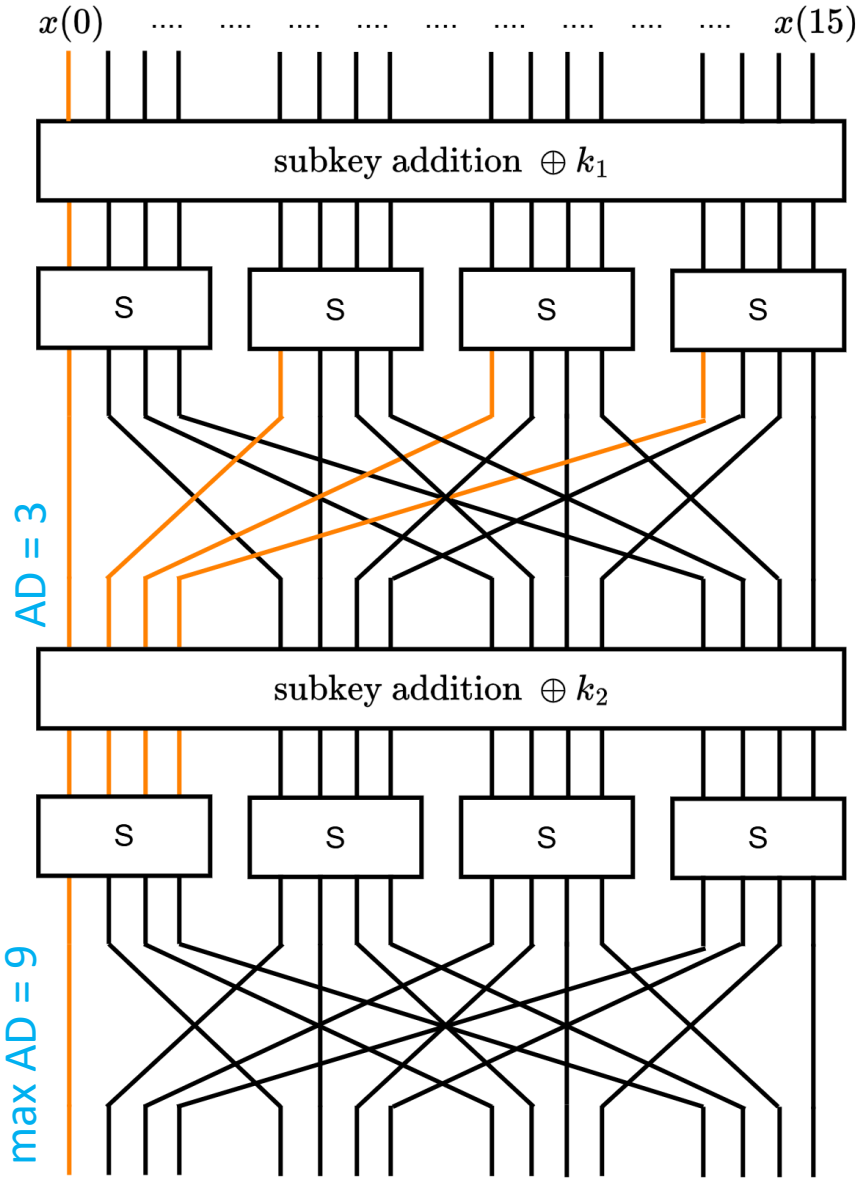
- Quadratic term (algebraic degree 2), can be solved via linearization: replace non-linear terms by extra variables, e.g., $\mathrm{v} = k(0) \cdot k(1)$
- Security impact: one more variable & one more linear equation

Security argument



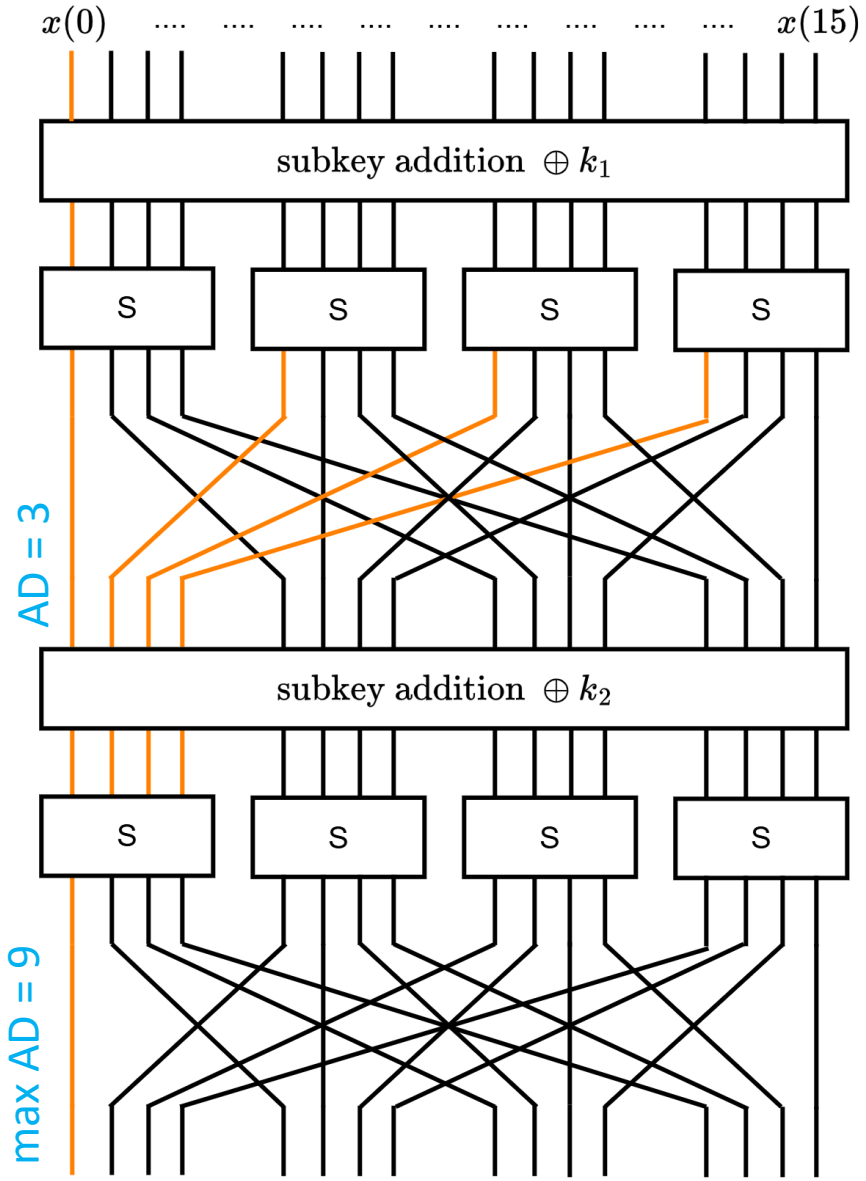
- Question: say S has optimal algebraic degree (i.e., $d = b - 1$ for a b-bit S-box), meaning $d = 3$ in our example, what is the maximum algebraic degree that can be reached at round 2?

Security argument



- Question: say S has optimal algebraic degree (i.e., $d = b - 1$ for a b-bit S-box), meaning $d = 3$ in our example, what is the maximum algebraic degree that can be reached at round 2? 3^2 (In general, one can hope for d^r at best)
- Question total/average # of monomials of degree d for a random Boolean function:

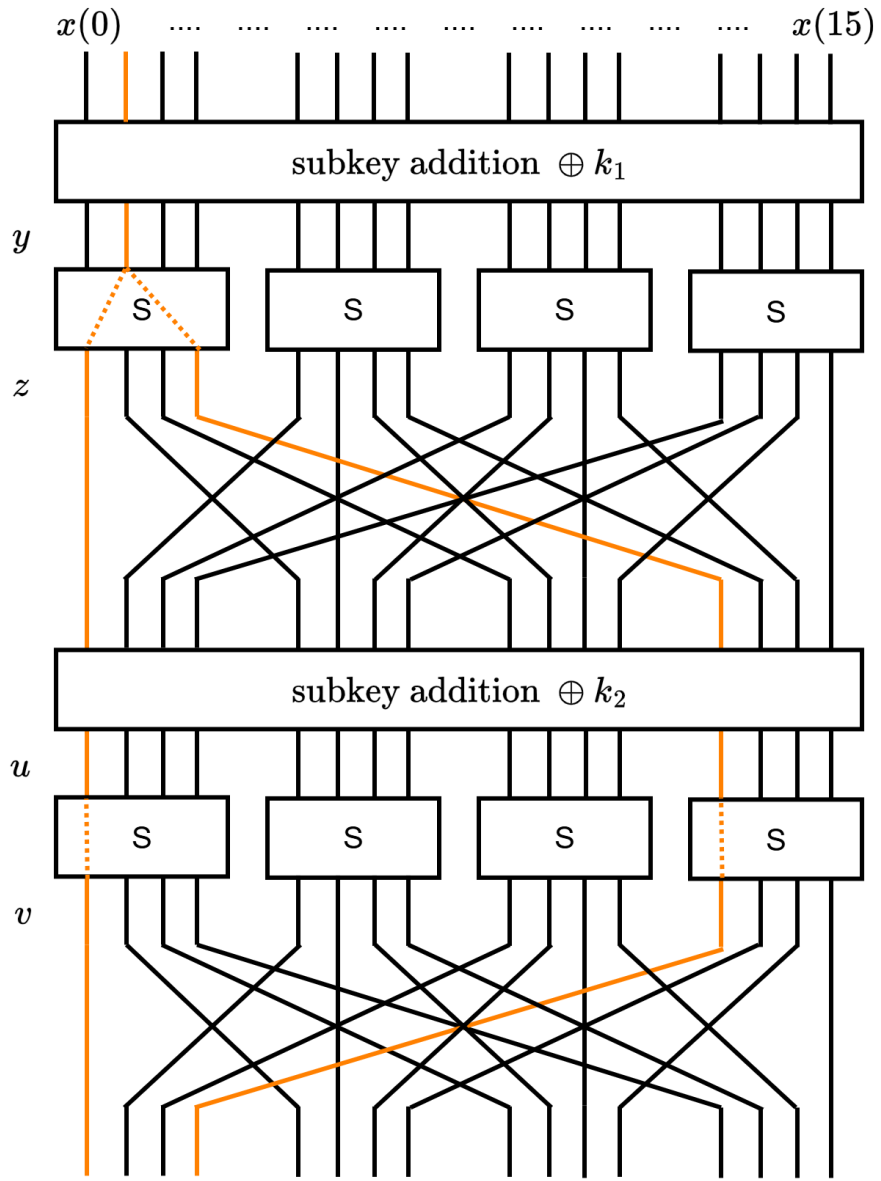
Security argument



- Question: say S has optimal algebraic degree (i.e., $d = b - 1$ for a b-bit S-box), meaning $d = 3$ in our example, what is the maximum algebraic degree that can be reached at round 2? 3^2 (In general, one can hope for d^r at best)
- Question total/average # of monomials of degree d for a random Boolean function: $\binom{n}{d}$, $\binom{n}{d}/2$, with $\binom{n}{n/2} \approx \frac{2^n}{\sqrt{\pi n/2}}$

- Linearized system rapidly hard to solve
  - Beware: algebraic degree is only a proxy

Statistical (linear) cryptanalysis (I)



- Say S-box has optimal algebraic degree but
  - $y(1) = z(0) \oplus z(3)$ with proba p_1
  - $u(0) = v(0)$ with proba p_2
  - $u(12) = v(12)$ with proba p_3

- Define the bias $\epsilon_i = p_i - 1/2$. Then

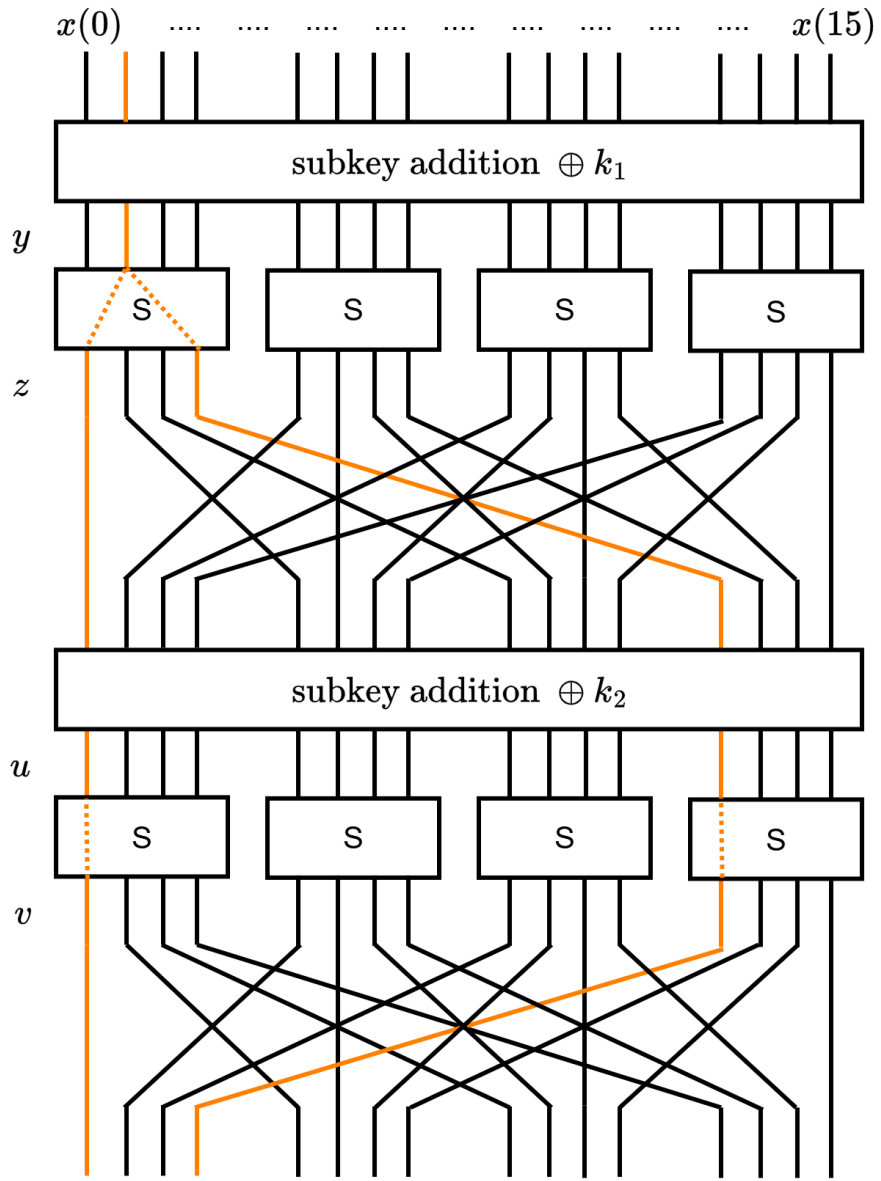
  $x(1) \oplus k_1(1) = v(0) \oplus k_2(0) \oplus v(12) \oplus k_2(12)$

  holds with bias $\epsilon = 2^{3-1} \cdot \prod_{i=1}^{3} \epsilon_i$

❑ Say all $\epsilon_i = 2^{-2}$, then $\epsilon =$

(*cf. reading on the course website*)

Statistical (linear) cryptanalysis (I)



- Say S-box has optimal algebraic degree but
  - $y(1) = z(0) \oplus z(3)$ with proba p_1
  - $u(0) = v(0)$ with proba p_2
  - $u(12) = v(12)$ with proba p_3

- Define the bias $\epsilon_i = p_i - 1/2$. Then

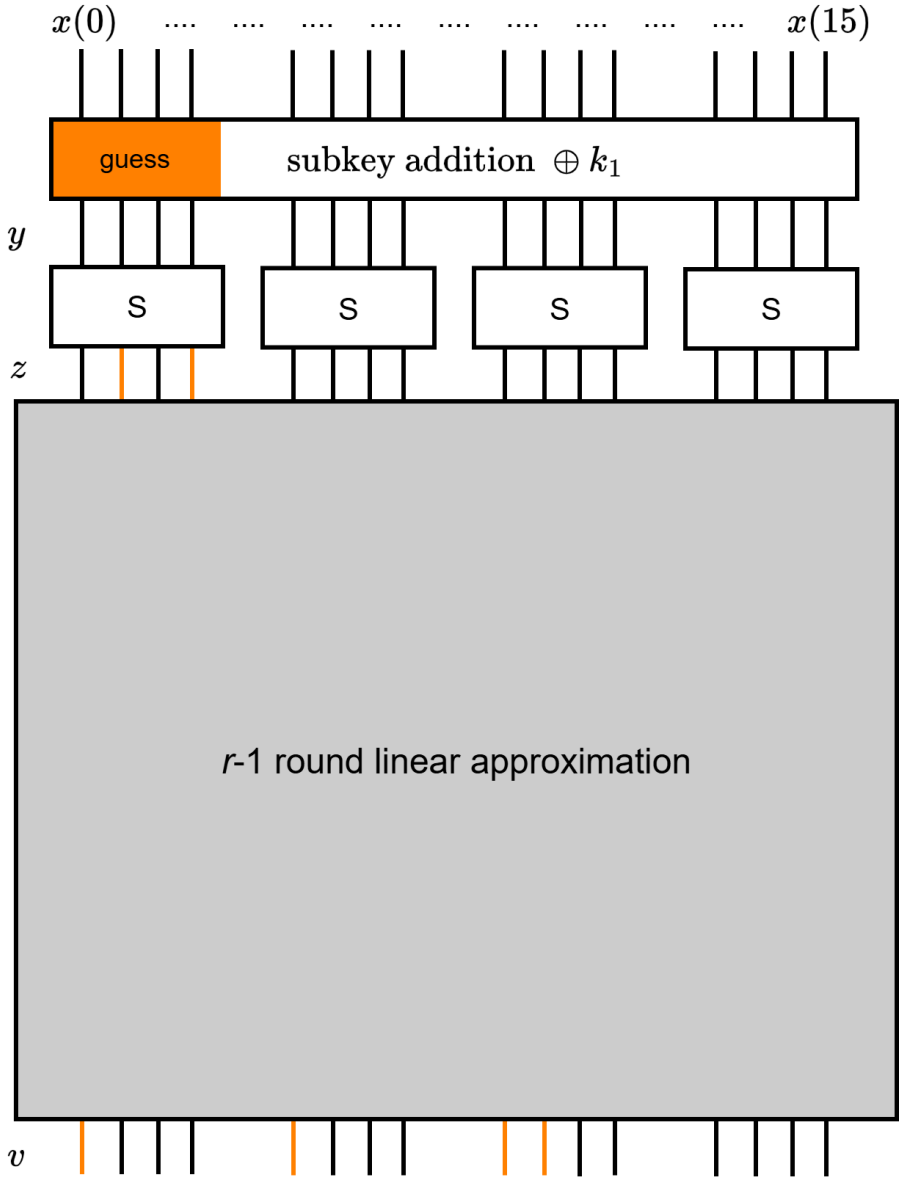
$$x(1) \oplus k_1(1) = v(0) \oplus k_2(0) \oplus v(12) \oplus k_2(12)$$

holds with bias $\epsilon = 2^{3-1} \cdot \prod_{i=1}^{3} \epsilon_i$

❑ Say all $\epsilon_i = 2^{-2}$, then $\epsilon = 2^{-4}$
How does that enable key recovery? {…}

(*cf. reading on the course website*)

Statistical (linear) cryptanalysis (II)



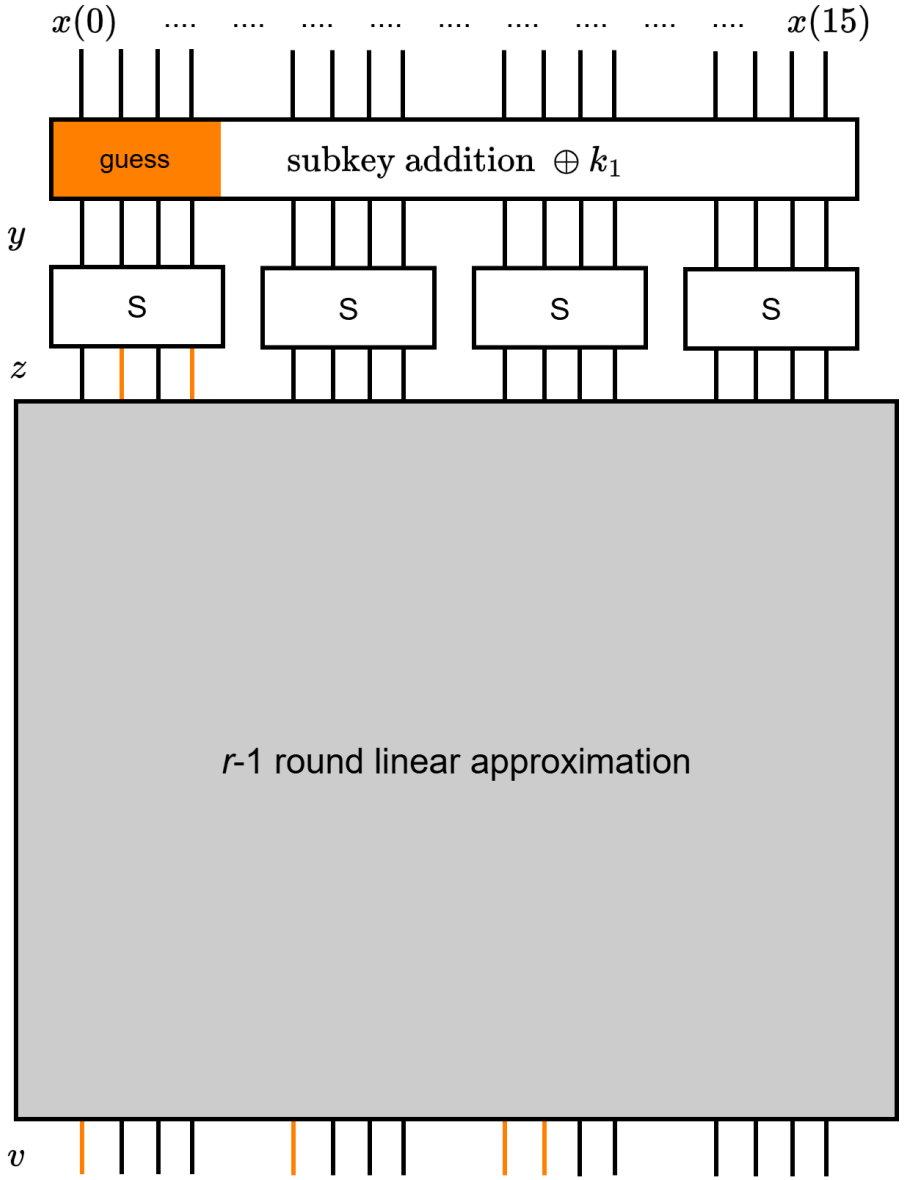
- Use a r-1 linear approximation with bias ϵ
- Collect q input / output block cipher pairs
- For all possible $(k_1(0), k_1(1), k_1(2), k_1(3))$, estimate the empirical bias ϵ_{k^*}, that is

$$\widehat{\Pr}(z^*(1) \oplus z^*(3) = v(0) \oplus v(4) v(8) \oplus v(9)) - 1/2$$

- The bias of the correct key candidate ϵ_{k^*} should be max for $k^* = k$ after $q \approx$

(*cf. reading on the course website*)

Statistical (linear) cryptanalysis (II)



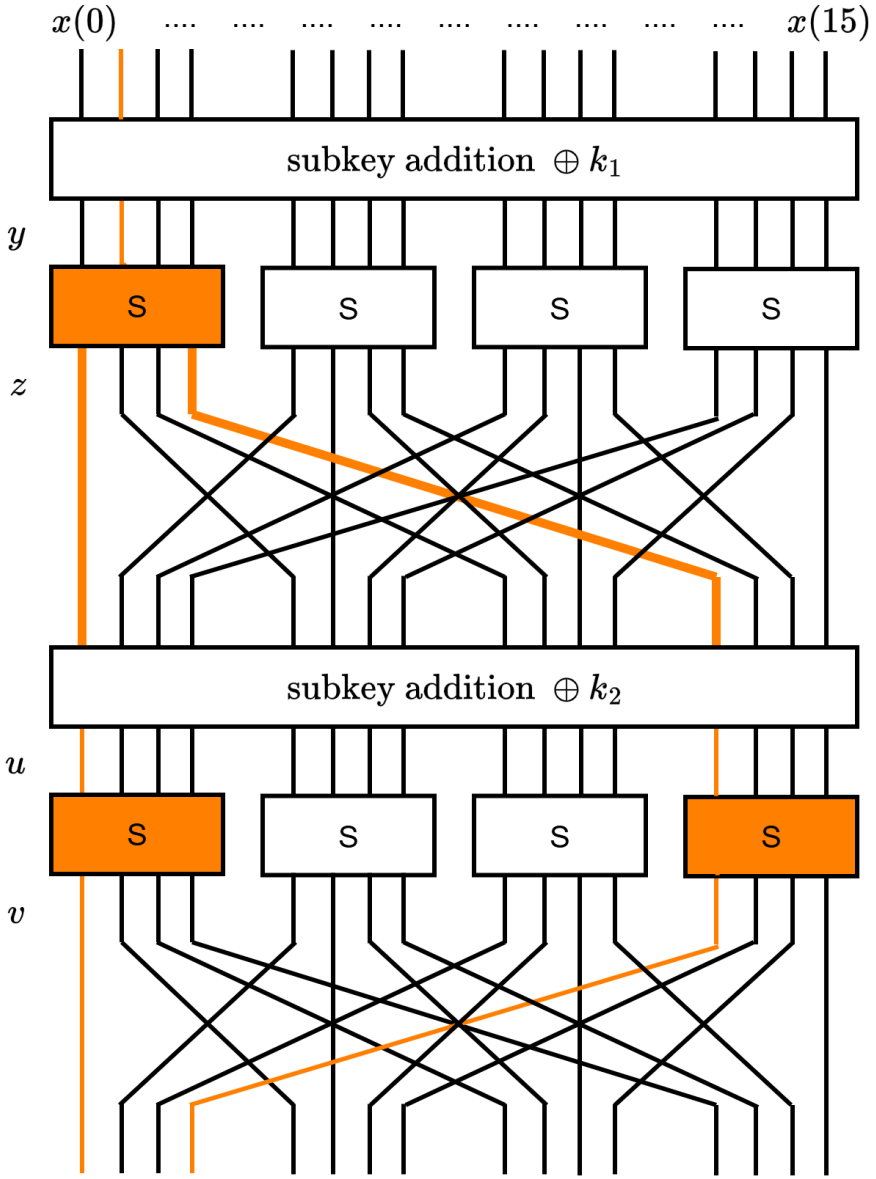
- Use a r-1 linear approximation with bias ϵ
- Collect q input / output block cipher pairs
- For all possible $(k_1(0), k_1(1), k_1(2), k_1(3))$, estimate the empirical bias ϵ_{k^*}, that is

$$\widehat{\Pr}(z^*(1) \oplus z^*(3) = v(0) \oplus v(4) v(8) \oplus v(9)) - 1/2$$

- The bias of the correct key candidate ϵ_{k^*} should be max for $k^* = k$ after $q \approx 1/\epsilon^2$
- Repeat for other bits of k_1 *(other approx.)*

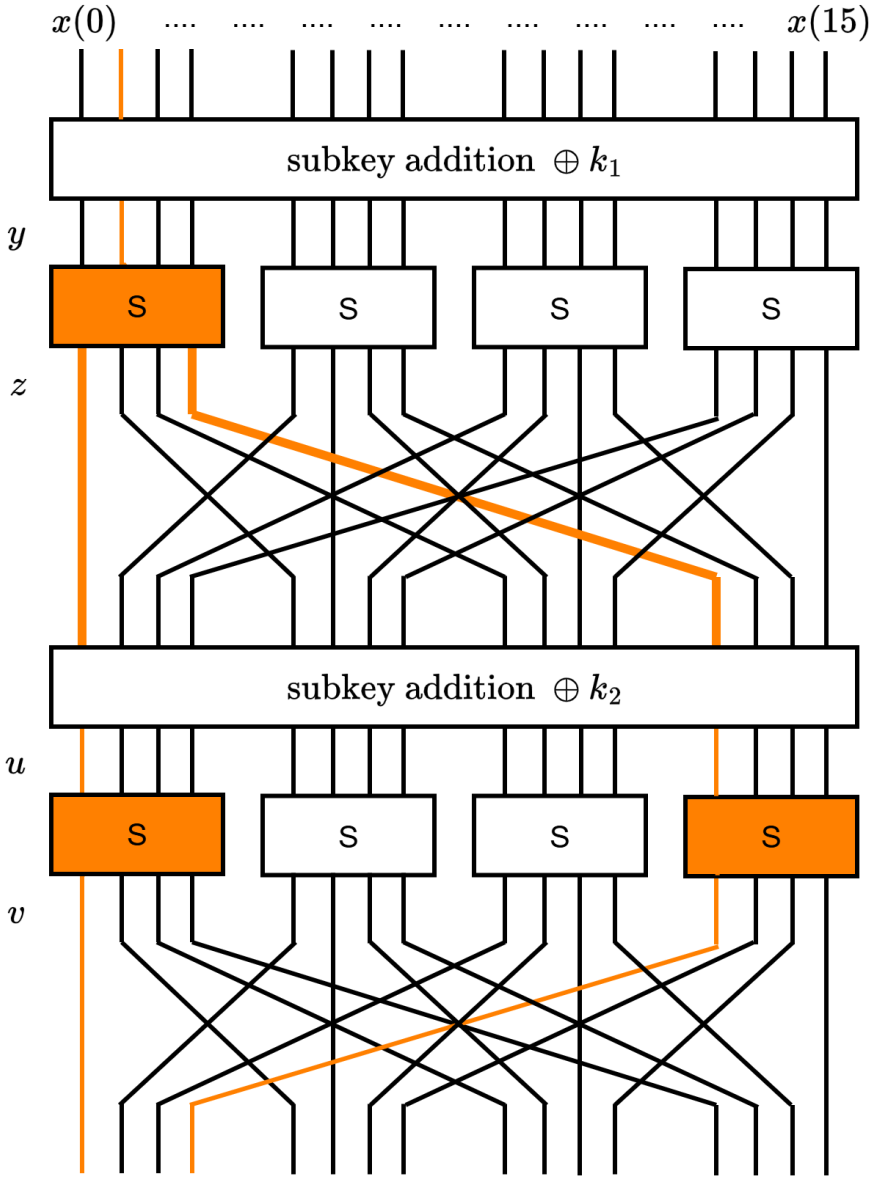
(*cf. reading on the course website*)

Security argument



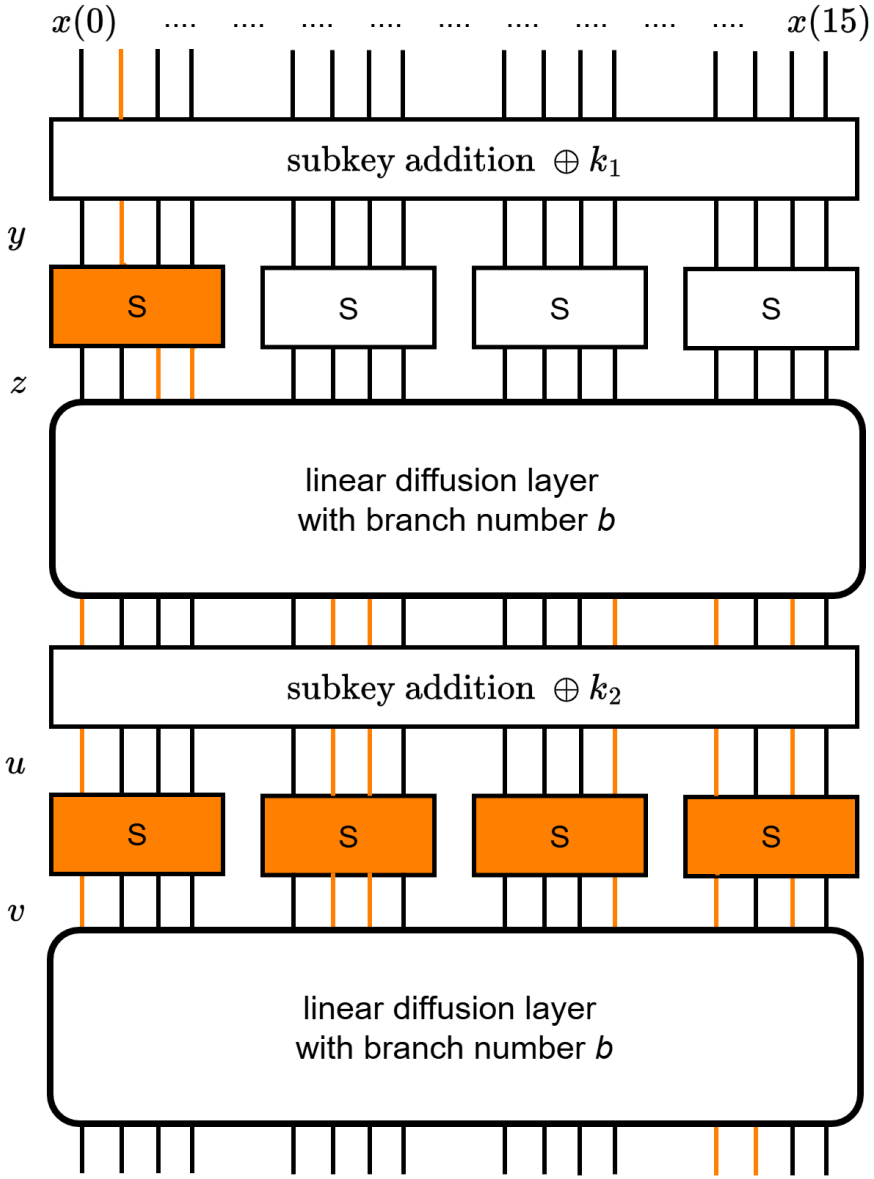
- What makes linear cryptanalysis hard?
  -
  -
  -

Security argument



- What makes linear cryptanalysis hard?
  - Increasing the number of rounds
  - Having S-boxes with small bias
  - Having many “active” S-boxes

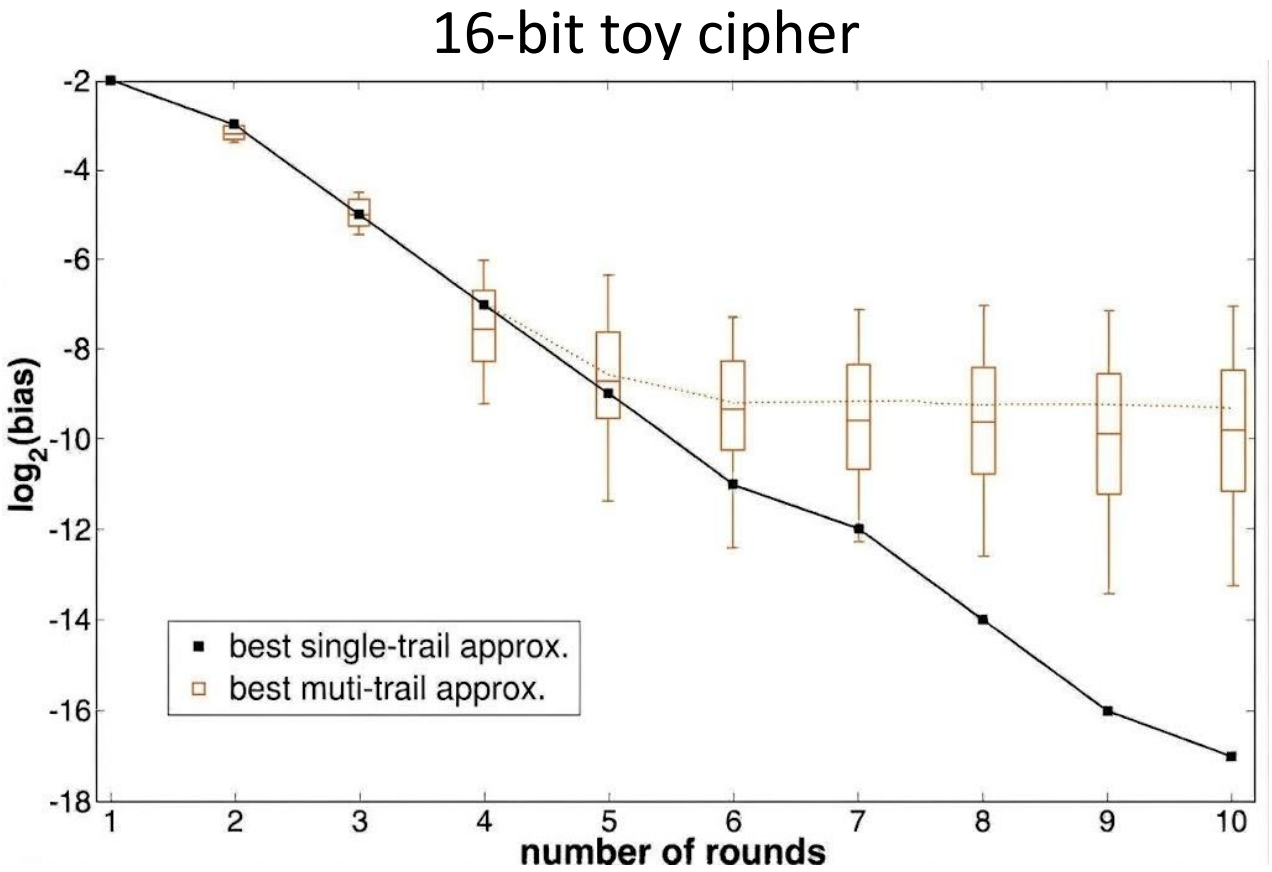
Security argument



- What makes linear cryptanalysis hard?
  - Increasing the number of rounds
  - Having S-boxes with small bias
  - Having many "active" S-boxes

- Advanced Encryption Standard (AES) ensures that with "separation of duties"
  - S-boxes with max bias $\epsilon = 2^{-4}$
  - Linear layer with good branch number (the sum of the # of active S-boxes at the layer's inputs and outputs equals *b*)
  - "Square amplification" with ShifRows {…}

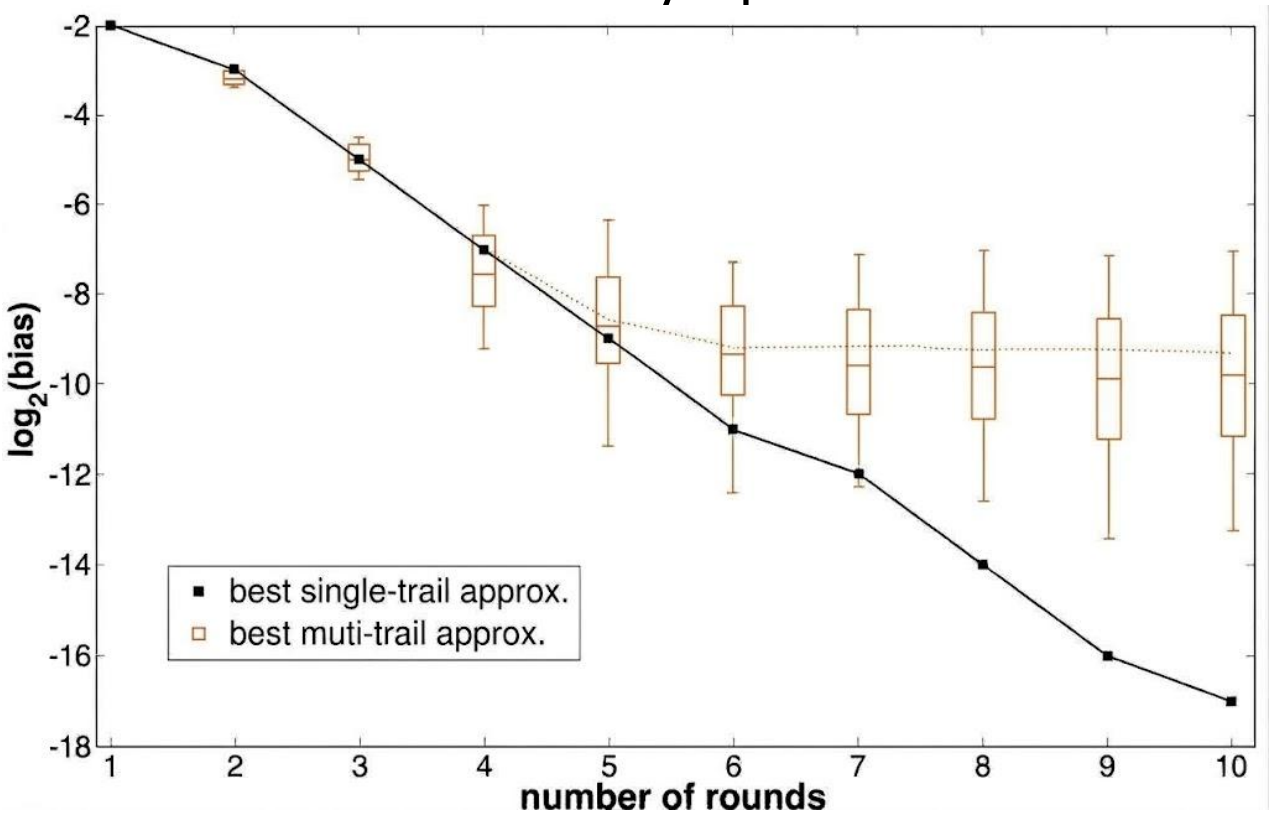
Discussion



- For low # of rounds, a single linear trail dominates
- For larger # of rounds, many linear trails interfere
- Concretely, it means
  - $\lim_{r\to\infty}(\varepsilon_{\text{single-trail}})$
  - $\lim_{r\to\infty}(\varepsilon_{\text{multi-trail}})$

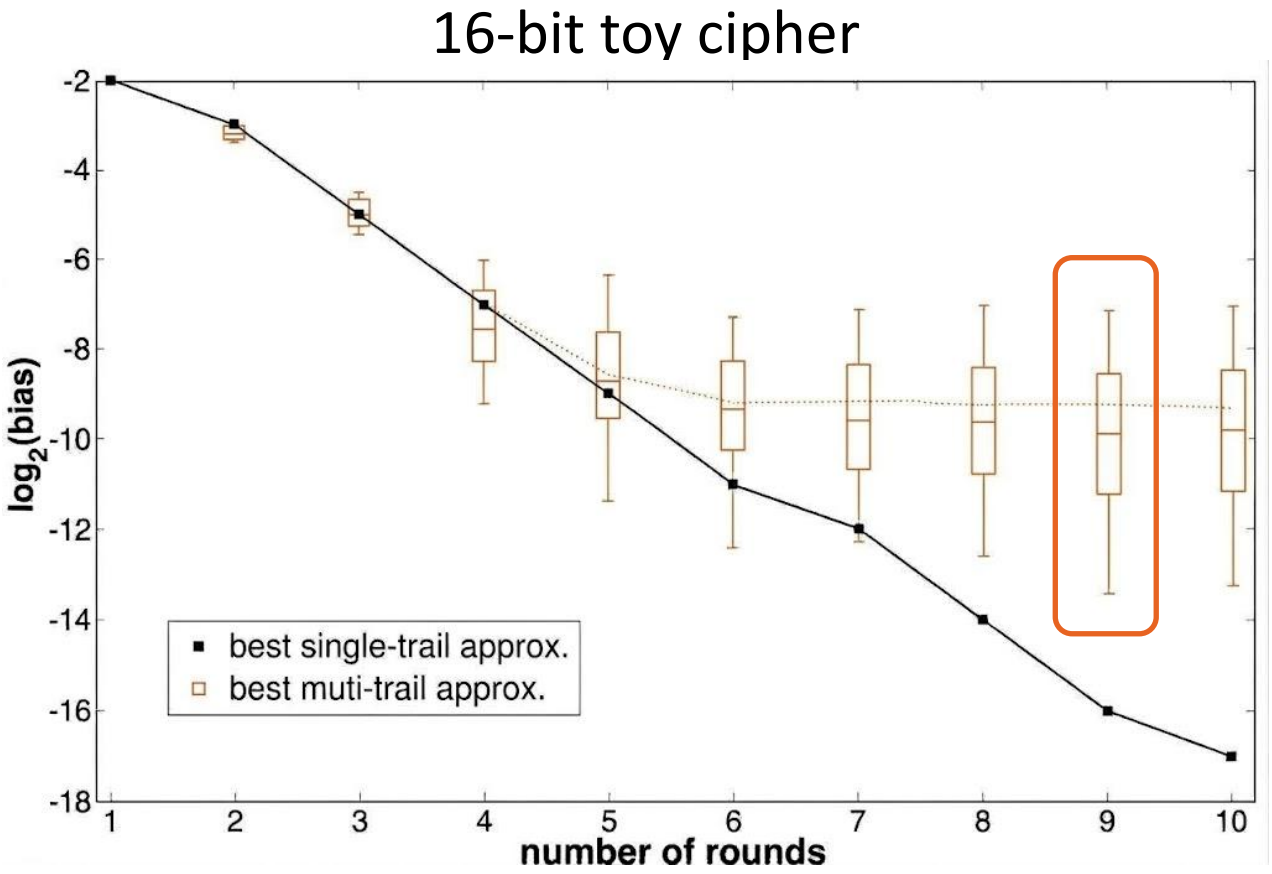
Discussion

16-bit toy cipher



- For low # of rounds, a single linear trail dominates
- For larger # of rounds, many linear trails interfere
- Concretely, it means
  - $\lim_{r\to\infty}(\varepsilon_{\text{single-trail}}) = 0$
  - $\lim_{r\to\infty}(\varepsilon_{\text{multi-trail}}) \neq 0$

Discussion

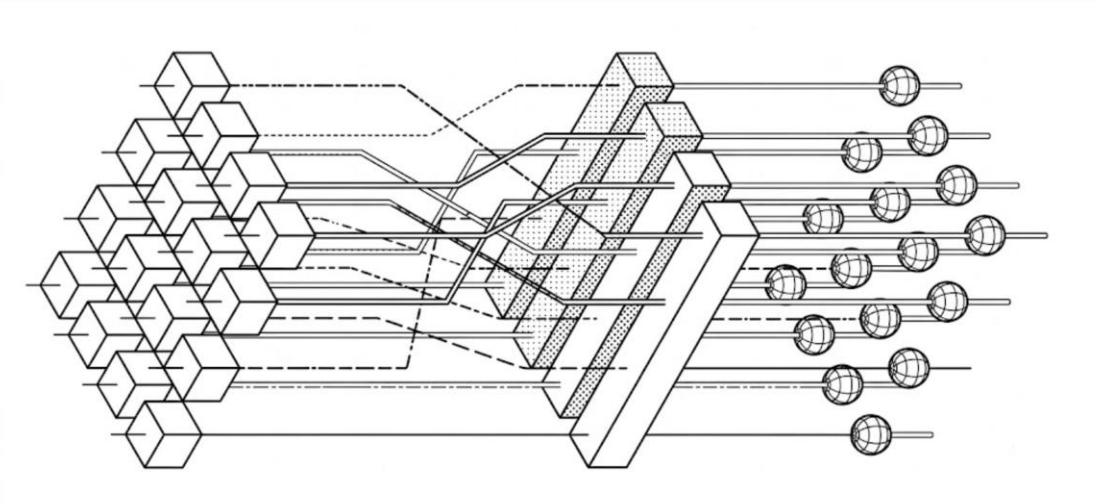


- For low # of rounds, a single linear trail dominates
- For larger # of rounds, many linear trails interfere
- Concretely, it means
  - $\lim_{r\to\infty}(\varepsilon_{\text{single-trail}}) = 0$
  - $\lim_{r\to\infty}(\varepsilon_{\text{multi-trail}}) \neq 0$

- But multi-trail approx. are hard to exploit (key-dependent) so having the squared bias of the best linear approximation $\ll 2^{-n}$ is a good proxy

Summarizing

- AES is standardized as Federal Inf. Process. Std. (NIST FIPS) 197
- It is widely believed to resist cryptanalysis (20+ years effort)
  - This includes algebraic & linear but also many others



- AES operations are carried in binary fields (for efficiency)
  - It offers excellent performances in software and hardware

Towards composition challenges

- Quantum threat: Grover's algorithm theoretically allows quadratic speedup for exhaustive key search ($\approx$ the need of 2^{128}classical operations is reduced to a need of 2^{64} quantum operations)
  - One needs to double the key size to cover this risk

Towards composition challenges

- Quantum threat: Grover's algorithm theoretically allows quadratic speedup for exhaustive key search ($\approx$ the need of 2^{128}classical operations is reduced to a need of 2^{64} quantum operations)
  - One needs to double the key size to cover this risk

❑ Question, can we use $\mathrm{AES_k}(\mathrm{AES_k},(\mathrm{x}))$ for this purpose?

- Expected (classical) complexity:
- Observed complexity:

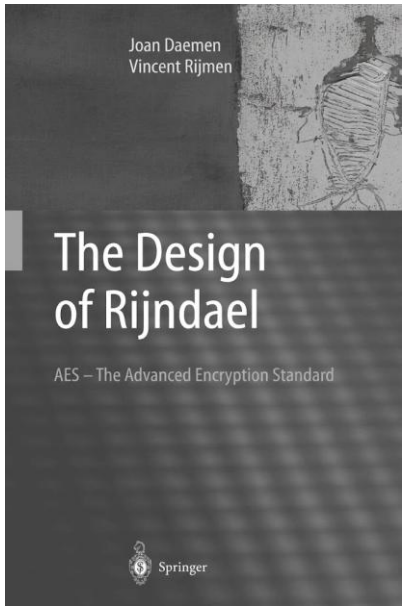
Towards composition challenges

- Quantum threat: Grover's algorithm theoretically allows quadratic speedup for exhaustive key search (≈ the need of 2^{128}classical operations is reduced to a need of 2^{64} quantum operations)
  - One needs to double the key size to cover this risk

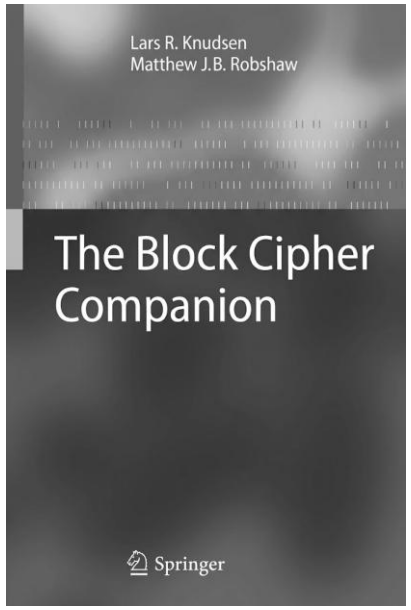
❑ Question, can we use $\mathrm{AES}_k(\mathrm{AES}_{k'}(x))$ for this purpose?
- Expected (classical) complexity: 2^{256} (⇒ quantum: 2^{128})
- Observed complexity: meet-in-the-middle attack {…}

⇒ Extending a cipher's domain is not trivial (remember P from F) and motivates ad hoc designs (e.g., AES-256 is a good PRP)

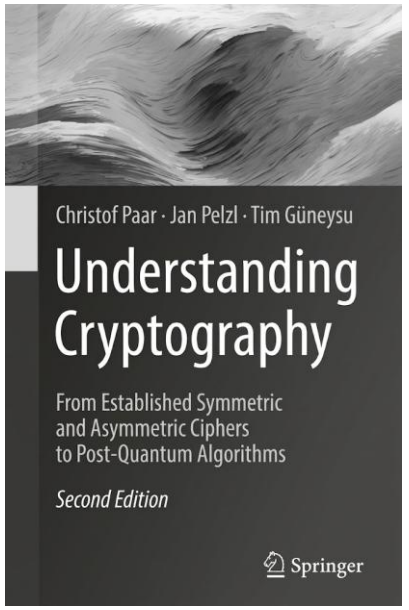
References



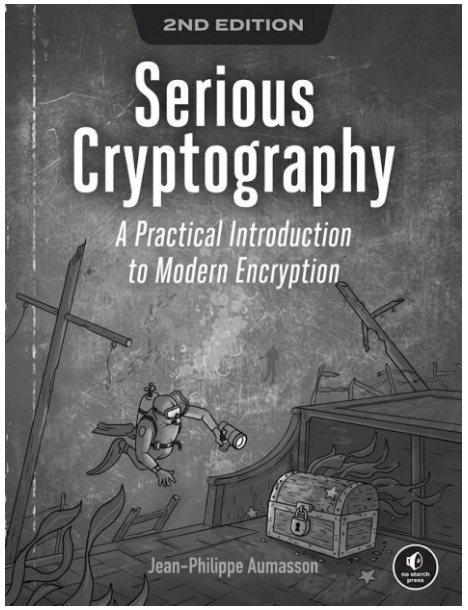
(a)



(b)



(c)



(d)

This lecture builds on the content of References (a), (b) and (c), which provide a detailed and complementary view of the design principles of modern block ciphers. Reference (a) additionally provides a gentle introduction to finite fields, which is useful to understand the internal operations of the AES, on which it focuses. Reference (d) provides discusses these topics in a less technical manner and provides a simple explanation and discussion of padding oracle attacks.

Questions?