Lightweight Cryptography –

When Cryptography Meets Mathematics

Anne Canteaut

Inria, Paris, France

University of Bergen - October 17, 2019

Inria

New implementation constraints

HOME SECTIONS SEARCH NEW YORK POST

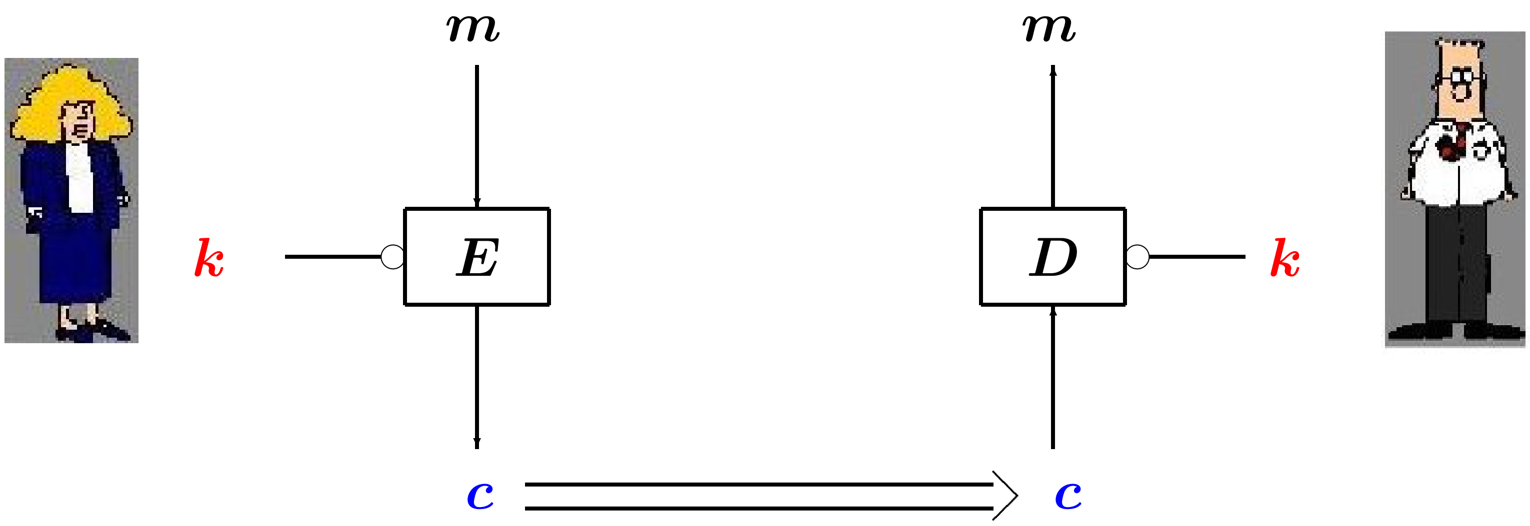
NEWS

Cheney feared terrorists would 'hack' pacemaker

By Bob Fredericks October 19, 2013 | 4:11am

Block ciphers

k is the secret key.



Problem 1: design a family of permutations E_k of $\{0,1\}^n$ which "behave as random permutations".

Problem 2: design a mode of operation describing how E_k can used for encrypting messages of any length.

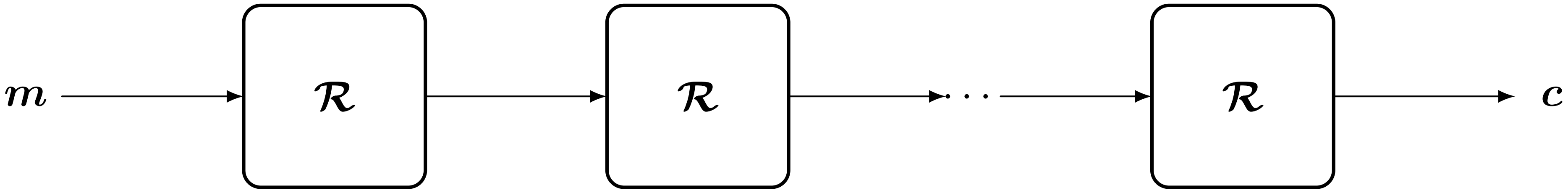
What is a block cipher?

$$E_k : \{0,1\}^n \longrightarrow \{0,1\}^n, \quad n \in \{64, 128\}$$

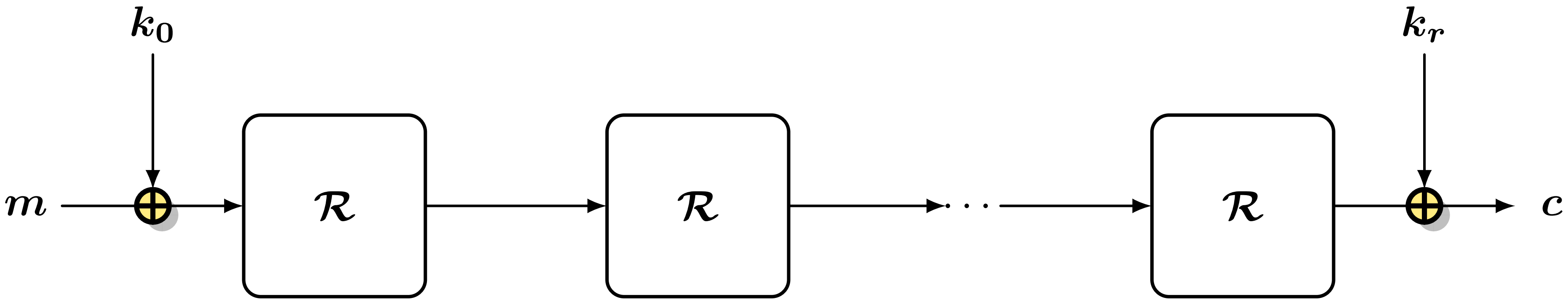
- indistinguishable from a set of randomly chosen permutations of $\{0,1\}^n$
- implementable

$\rightarrow$ Contradiction!

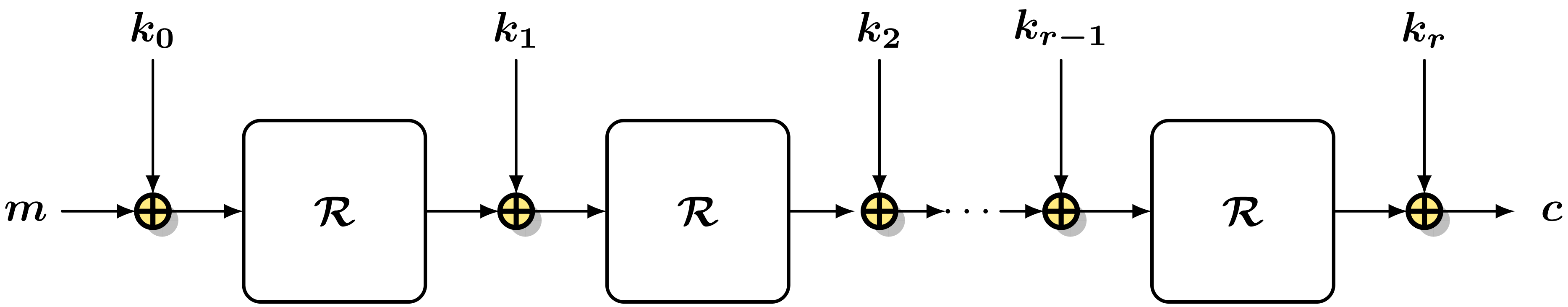
Iterated block ciphers



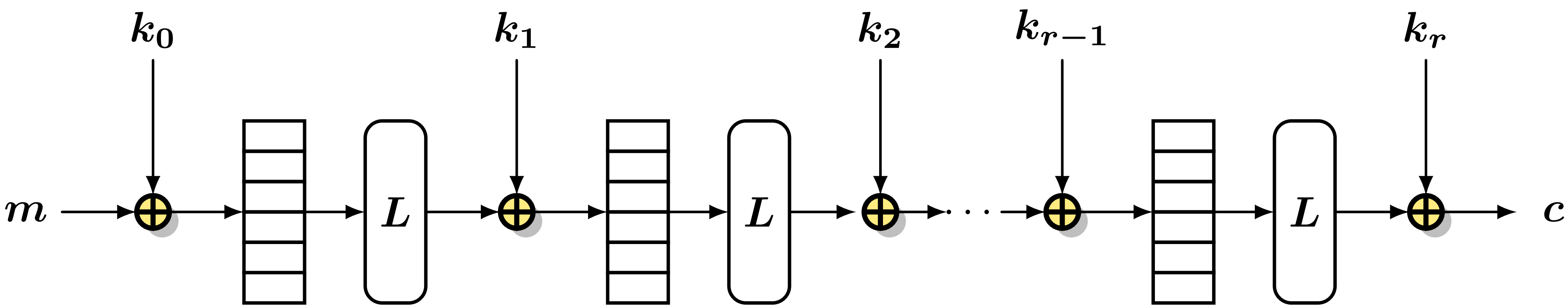
Iterated block ciphers



Iterated block ciphers



Iterated block ciphers



AES [Daemen-Rijmen 98][FIPS PUB 197]

- blocksize: $\mathbf{128}$ bits
- $\mathbf{10}$ rounds for the $\mathbf{128}$-bit key version
- Sbox operates on $\mathbf{8}$ bits
- diffusion layer is linear over $\mathbf{F}_{\mathbf{2}^8}$

How to make it lightweight?

Lightweight block ciphers

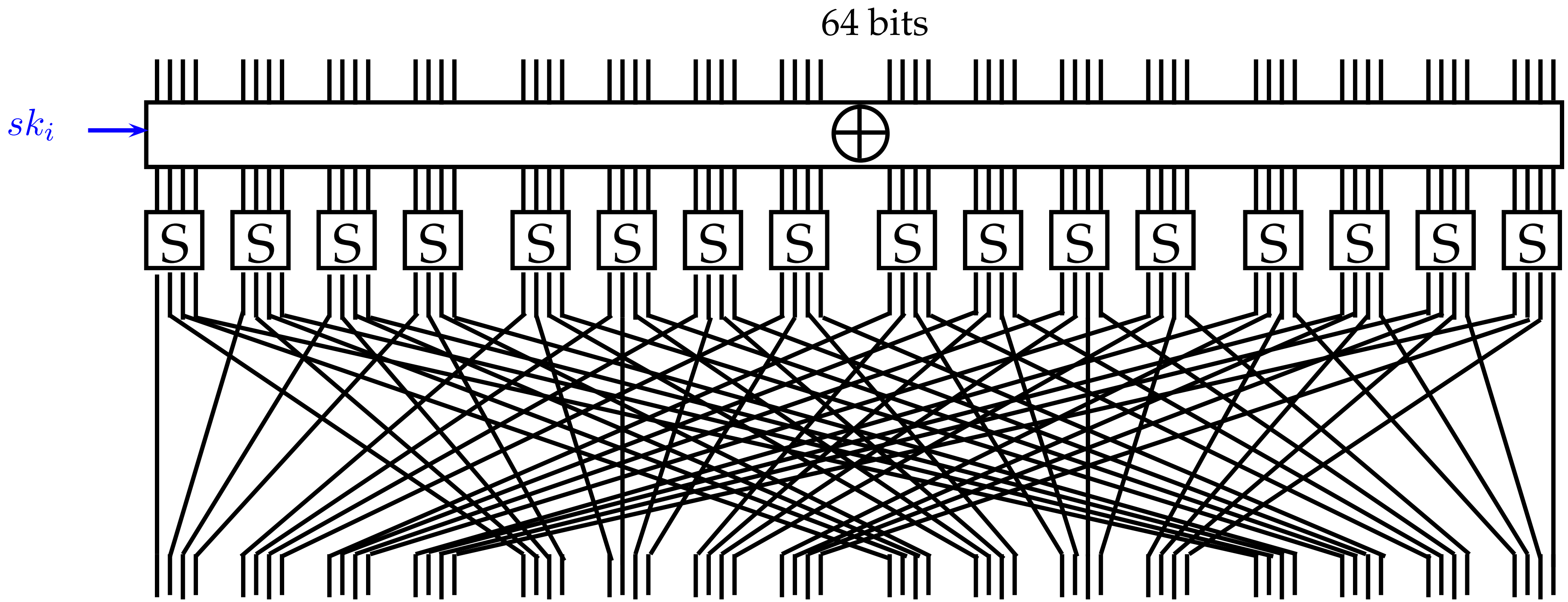
AES [Daemen-Rijmen 98][FIPS PUB 197]

- blocksize: $\mathbf{128}$ bits
- Sbox operates on $\mathbf{8}$ bits
- diffusion layer is linear over $\mathbf{F}_{\mathbf{2}^8}$

To make it smaller in hardware:

- blocksize: $\mathbf{64}$ bits
- smaller Sbox, on $\mathbf{3}$ or $\mathbf{4}$ bits
- linear diffusion layer over a smaller alphabet
- simplified key-schedule

The usual design strategy: PRESENT [Bogdanov et al. 07]



31 rounds (+ a key addition)

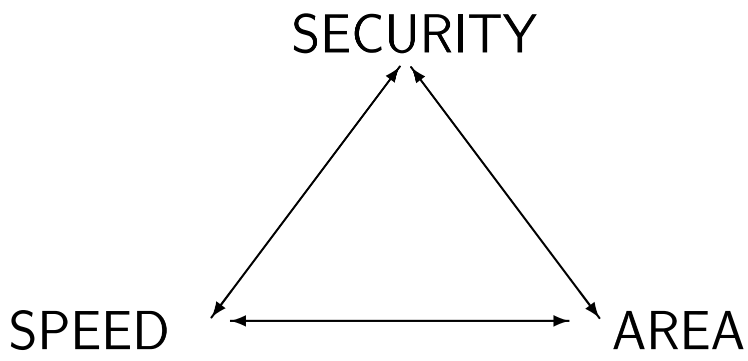
Lightweight but secure...

Increase the number of rounds!

- PRESENT [Bogdanov et al. 07]. 31 rounds
- LED [Guo et al. 11]:
  LED-64: 32 rounds, LED-128: 48 rounds
- SPECK [Beaulieu et al. 13]:
  SPECK64/128: 27 rounds, SPECK128/256: 34 rounds
- SIMON [Beaulieu et al. 13]:
  SIMON64/128: 44 rounds, SIMON128/256: 72 rounds

Does lightweight mean "light + wait"? [Knežević et al. 12]

Does lightweight mean "light + wait"? [Knežević et al. 12]



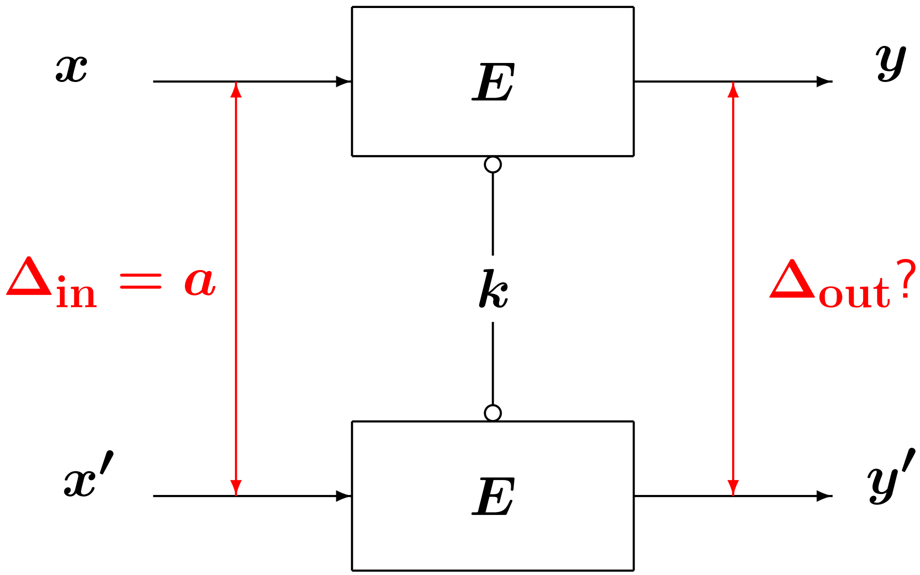
Low-latency encryption.

- Memory encryption
- VANET (Vehicular ad-hoc network)
- encryption for high-speed networking...

$\rightarrow$ small unrolled implementation

Find better building-blocks

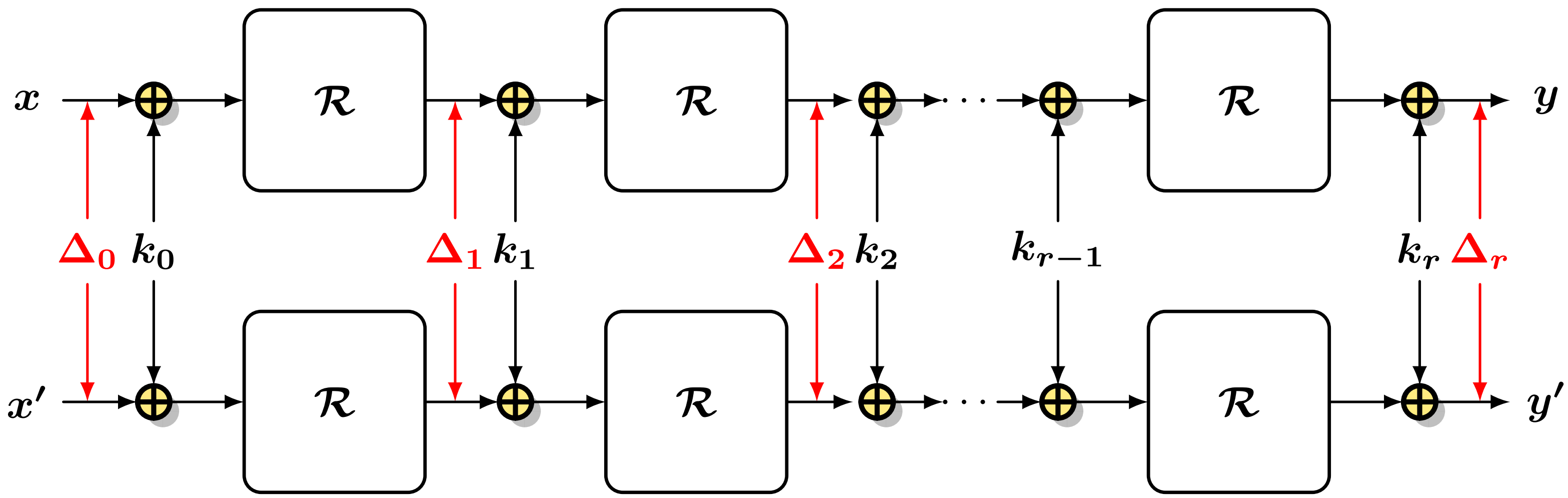
Differential cryptanalysis [Biham-Shamir 90]



Security criterion.

$$\max_{a \neq 0, b \neq 0} \Pr_{x,k}[E_k(x \oplus a) \oplus E_k(x) = b] \text{ should be small.}$$

Minimize the probability of all differential characteristics



$$\Pr_x\left[\mathcal{R}^i(x \oplus \Delta_0) \oplus \mathcal{R}^i(m) = \Delta_i, \forall i\right] = \prod_{i=0}^{r-1} \Pr_x\left[\mathcal{R}(x \oplus \Delta_i) \oplus \mathcal{R}(x) = \Delta_{i+1}\right]$$

Differential uniformity of $S : \mathbf{F}_2^m \to \mathbf{F}_2^m$

$$\delta(a, b) = \#\{x \in \mathbf{F}_2^m, \;\; S(x \oplus a) \oplus S(x) = b\}$$

Differential uniformity of S.

$$\delta(S) = \max_{a \neq 0, b} \delta(a, b)$$

$$\Rightarrow \max_{\Omega} \mathrm{Pr}(\Omega) \leq \left(\frac{\delta(S)}{2^m}\right)^{d_{\min}}$$

Theorem. [Nyberg-Knudsen 92] For any $S : \mathbf{F}_2^m \to \mathbf{F}_2^m$

$$\delta(S) \geq 2 \; .$$

Difference distribution table

$a \setminus b$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	2	0	4	2	0	2	2	0	0	0	2	0	0	0	2
2	2	2	0	2	4	0	2	0	4	0	0	0	0	0	0
3	2	0	4	0	2	0	0	0	0	6	0	0	0	2	0
4	2	0	2	4	0	0	0	2	2	0	0	2	0	0	2
5	0	4	2	0	0	0	2	2	0	0	4	2	0	0	0
6	4	0	0	0	0	4	0	4	0	0	0	0	4	0	0
7	0	2	0	0	2	2	2	0	2	2	2	0	0	2	0
8	0	4	0	0	0	4	0	0	0	0	0	0	4	0	4
9	2	2	0	2	2	0	0	0	4	0	0	2	0	2	0
10	0	0	2	2	0	2	2	2	0	2	2	0	0	0	2
11	0	0	2	0	4	0	2	2	0	0	0	6	0	0	0
12	0	2	0	0	0	2	0	0	2	2	2	2	0	4	0
13	2	0	0	0	2	0	0	0	0	2	0	0	8	2	0
14	0	0	0	0	0	0	4	0	0	0	4	0	0	4	4
15	0	0	0	4	0	0	0	4	2	2	0	2	0	0	2

$$\delta(a, b) = \#\{x \in \mathbf{F}_2^m, \quad S(x \oplus a) \oplus S(x) = b\}$$

Good permutations of $\mathbf{F}_2^m$, m even

Permutations with $\delta(S) = 2$.

The only known permutation S with an even number of variables and $\delta(S) = 2$ is for $m = 6$ [Dillon 09].

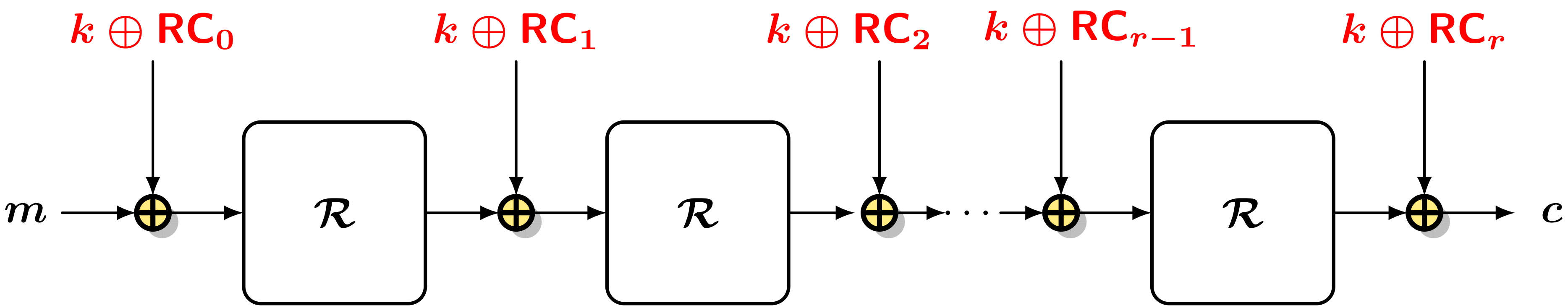
$\longrightarrow$ Usually, we search for permutations S with $\delta(S) = 4$.

Monomials permutations $S(x) = x^s$ over $\mathbf{F}_{2^m}$.

$2^i + 1$, $\gcd(i, m) = 2$	$m \equiv 2 \bmod 4$	[Gold 68]
$2^{2i} - 2^i + 1$, $\gcd(i, m) = 2$	$m \equiv 2 \bmod 4$	[Kasami 71]
$2^{\frac{m}{2}} + 2^{\frac{m}{4}} + 1$	$m \equiv 4 \bmod 8$	[Bracken-Leander 10]
$2^m - 2$		[Lachaud-Wolfmann 90]

Use a simpler key-schedule

Lightweight key schedules

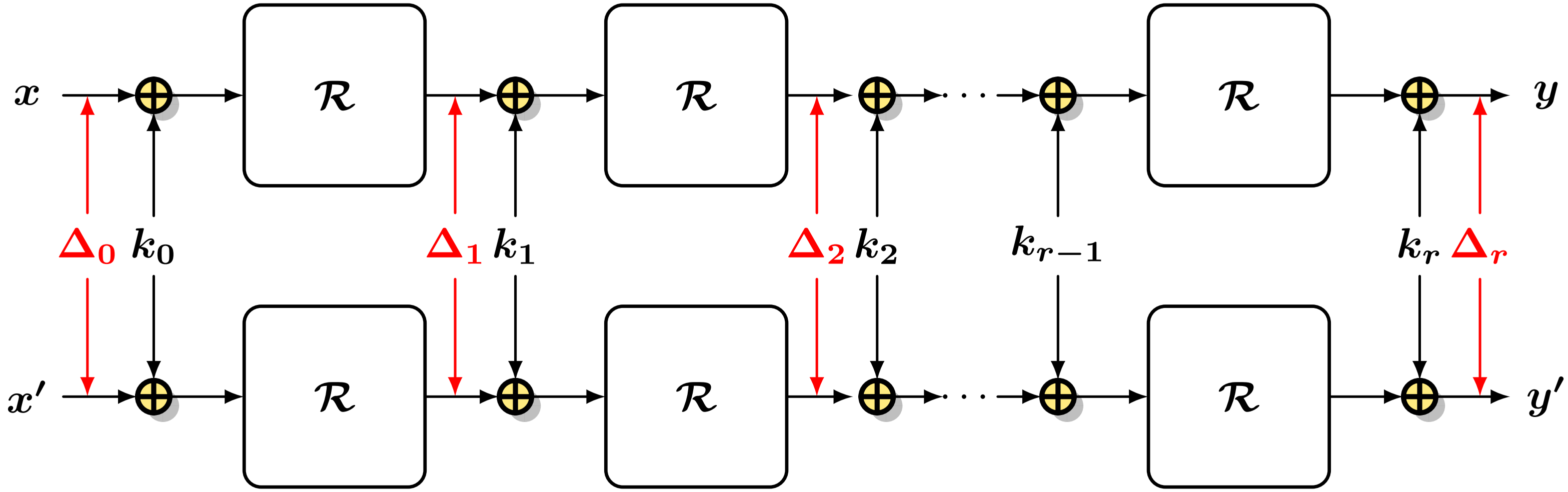


where $\mathbf{RC}_0, \mathbf{RC}_1, \ldots, \mathbf{RC}_r$ are fixed round-constants.

Examples:

- PrintCipher [Knudsen et al. 10]
- LED [Guo et al. 11]
- Prince [Borghoff et al. 12]
- Scream and iScream [Grosso et al. 14]
- Midori [Banik et al. 15]
- Skinny and Mantis [Beierle et al. 16]...

$k_0, k_1, \ldots, k_r$ should behave as iid random variables!!



We expect:

$$\Pr_x\left[\mathcal{R}^i(x \oplus \Delta_0) \oplus \mathcal{R}^i(m) = \Delta_i, \forall i\right] = \prod_{i=0}^{r-1} \Pr_x\left[\mathcal{R}(x \oplus \Delta_i) \oplus \mathcal{R}(x) = \Delta_{i+1}\right]$$

Invariant attacks [Todo-Leander-Sasaki 16]

Principle:

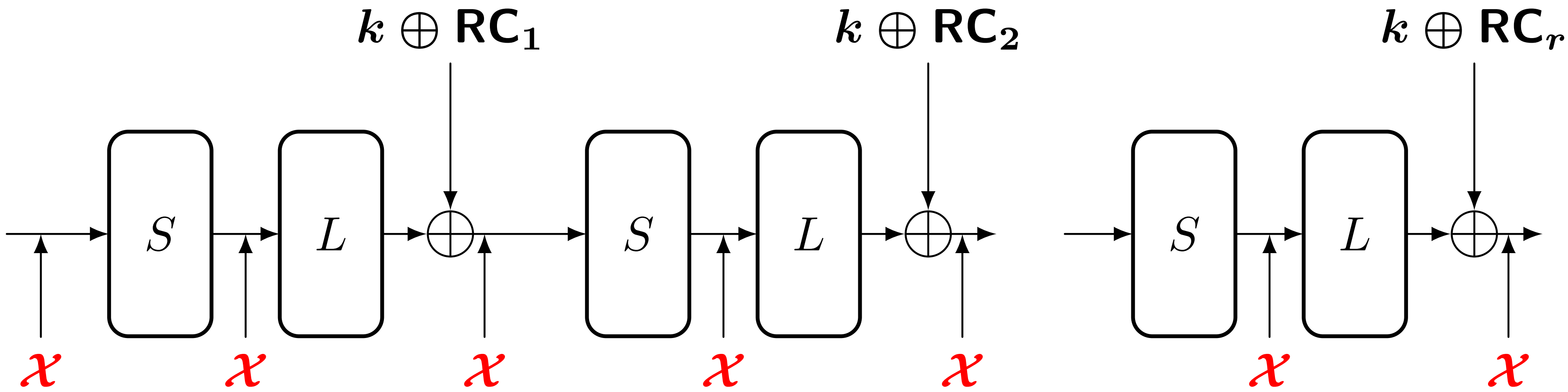
Exhibit a set $\mathcal{X}$ of inputs invariant under E_k for many weak keys.

Ex: Invariant subspace for Midori64 [Guo et al. 16]

For any 128-bit key $k \in \{0,1\}^{32}$, $\mathcal{X} = \{8,9\}^{16}$ is invariant under E_k.

For $k = (1100110011001100, 0011001100110011)$,
$m = 9999999999999999$ leads to the ciphertext $c = 8999999988988989$

Using the same invariant for all layers in an iterated cipher



Condition on the existence of invariant sets

$$D := \{(\mathsf{RC}_i \oplus \mathsf{RC}_j),\ \ 0 \leq i < j \leq r\}$$

$W_L(D) :=$ smallest subspace invariant under L which contains D .

Problem.

Is there a set $\mathcal{X} \subset \{0,1\}^n$ such that $S(\mathcal{X}) = \mathcal{X}$ and
$\mathcal{X}$ is invariant under addition of any element in $W_L(D)$?

Condition on the existence of invariant sets

$$D := \{(\mathsf{RC}_i \oplus \mathsf{RC}_j),\ \ 0 \leq i < j \leq r\}$$

$W_L(D) :=$ smallest subspace invariant under L which contains D .

Problem.

Is there a set $\mathcal{X} \subset \{0,1\}^n$ such that $S(\mathcal{X}) = \mathcal{X}$ and $\mathcal{X}$ is invariant under addition of any element in $W_L(D)$?

No if $W_L(D) = \{0,1\}^n$

Some lightweight ciphers with $n = 64$

Skinny-64-64.

$$D = \{\mathsf{RC}_1 \oplus \mathsf{RC}_{17},\ \mathsf{RC}_2 \oplus \mathsf{RC}_{18},\ \mathsf{RC}_3 \oplus \mathsf{RC}_{19},\ \mathsf{RC}_4 \oplus \mathsf{RC}_{20},\ \mathsf{RC}_5 \oplus \mathsf{RC}_{21}\}$$

$$\dim W_L(D) = 64$$

The round-constants and L guarantee that the attack does not apply.

Prince.

$$D = \{\mathsf{RC}_1 \oplus \mathsf{RC}_2,\ \mathsf{RC}_1 \oplus \mathsf{RC}_3,\ \mathsf{RC}_1 \oplus \mathsf{RC}_4,\ \mathsf{RC}_1 \oplus \mathsf{RC}_5,\ \alpha\}.$$

$$\dim W_L(D) = 56$$

Midori-64.

$$W_L(D) = \{0000, 0001\}^{16}, \quad \dim W_L(D) = 16$$

Maximizing the dimension of $W_L(d)$

$$W_L(d) = \langle L^t(d), t \in \mathbb{N} \rangle \ .$$

Theorem. There exists d such that $\dim W_L(d) = k$ if and only if k is the degree of a divisor of the minimal polynomial of L.

$$\Rightarrow \max_{d \in \mathbb{F}_2^n} \dim W_L(d) = \deg \textsf{Min}_L$$

For some lightweight ciphers

LED.

$$\mathrm{Min}_L(X) = (X^8 + X^7 + X^5 + X^3 + 1)^4 (X^8 + X^7 + X^6 + X^5 + X^2 + X + 1)^4$$

There exist some d such that $\dim W_L(d) = 64$

Skinny-64.

$$\mathrm{Min}_L(X) = X^{16} + 1 = (X + 1)^{16}$$

There exist some d such that $\dim W_L(d) = k$ for any $1 \leq k \leq 16$.

Prince.

$$\mathrm{Min}_L(X) \;=\; X^{20} + X^{18} + X^{16} + X^{14} + X^{12} + X^8 + X^6 + X^4 + X^2 + 1$$

$$\max_d \dim W_L(d) = 20$$

Midori.

$$\mathrm{Min}_L(X) = (X + 1)^6 \Rightarrow \max_d \dim W_L(d) = 6$$

Rational canonical form

When $\deg(\mathbf{Min}_L) = n$, there is a basis for which the matrix of L is

$$C(\mathbf{Min}_L) = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & & & \\ 0 & 0 & 0 & \dots & 1 \\ p_0 & p_1 & p_2 & \cdots & p_{n-1} \end{pmatrix}$$

More generally, there is a basis for which the matrix of L is

$$\begin{pmatrix} C(Q_1) & & & \\ & C(Q_2) & & \\ & & \ddots & \\ & & & C(Q_\ell) \end{pmatrix}$$

for ℓ polynomials $Q_\ell \mid Q_{\ell-1} \mid \cdots \mid Q_1 = \mathbf{Min}_L$ called the invariant factors of L.

Example

For Prince.

$$\begin{aligned}\mathsf{Min}_L(X) &= X^{20}+X^{18}+X^{16}+X^{14}+X^{12}+X^{8}+X^{6}+X^{4}+X^{2}+1\\ &= (X^4+X^3+X^2+X+1)^2(X^2+X+1)^4(X+1)^4\end{aligned}$$

8 invariant factors:

$$\begin{aligned}Q_1(X) &= Q_2(X)\\ &= X^{20}+X^{18}+X^{16}+X^{14}+X^{12}+X^{8}+X^{6}+X^{4}+X^{2}+1\\ Q_3(X) &= Q_4(X) = X^8+X^6+X^2+1 = (X+1)^4(X^2+X+1)^2\\ Q_5(X) &= Q_6(X) = Q_7(X) = Q_8(X) = (X+1)^2\end{aligned}$$

Maximizing the dimension of $W_L(d_1, \ldots, d_t)$

Theorem. Let $Q_1, Q_2, \ldots, Q_\ell$ be the ℓ invariant factors of L.

For any $t \leq \ell$,

$$\max_{d_1,\ldots,d_t} \dim W_L(d_1, \ldots, d_t) = \sum_{i=1}^{t} \deg Q_i.$$

We need ℓ elements to get $W_L(D) = \{0,1\}^n$.

For Prince.

For $t = 5, \ \max \dim W_L(d_1, \ldots, d_5) = 20 + 20 + 8 + 8 + 2 = 58$

We need 8 elements to get the full space.

Conclusions

- risky
- standardization process launched by NIST

Use mathematics to clarify the design criteria!