Similarities between encryption and decryption: how far can we go?

Anne Canteaut

Inria, France and DTU, Denmark
Anne.Canteaut@inria.fr
http://www-rocq.inria.fr/secret/Anne.Canteaut/

SAC 2013

based on a joint work with Lars Knudsen and Gregor Leander
Outline

• Low-latency and lightweight ciphers

• Minimizing the overhead of decryption: involutional ciphers and involutional building-blocks

• Minimizing the overhead of decryption: reflection ciphers

• PRINCE
Iterated block ciphers

\[ K \text{ master key} \]

key schedule

\[ k_1 \quad k_2 \quad k_r \]

plaintext \( x \) \( F(1) \quad F(2) \quad \ldots \quad F(r) \) ciphertext \( y \)

where each \( F^{(i)} \) is a keyed permutation of \( F_2^n \).
Lightweight block ciphers

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

- blocksize: **128** bits
- Sbox operates on 8 bits
- linear diffusion layer is a linear permutation of $\mathbb{F}_{2^8}^4$

To make it smaller in hardware:

- blocksize: **64** bits
- smaller Sbox, on 3 or 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...
How can we design a fast and lightweight cipher?

Unrolled implementation.

- small number of rounds;

- each round of encryption and decryption should have a low implementation cost;

- the rounds do not need to be similar.

Related open problem.
Is it possible to provide security arguments for a cipher iterating very different rounds?
Minimizing the overhead of decryption:

involutional building-blocks
When lightweight encryption was really an issue...

http://www.nsa.gov/museum/enigma.html
Scherbius’ solution: add a reflector

\[ E_K = F_K^{-1} \circ M \circ F_K \] where \( M = M^{-1} \)
**Can \( E_K \) be an involution?**

**Fixed points.** [Youssef-Tavares-Heys 96]

- A random permutation of \( \mathbb{F}_2^n \) has 1 fixed point on average;
- A random involution of \( \mathbb{F}_2^n \) has \( 2^n + O(1) \) fixed points.

In particular, for \( E_K = F_K^{-1} \circ M \circ F_K \)

\( E_K \) has the same cycle structure (and the same number of fixed points) as \( M \).

- Enigma: the reflector has no fixed points;
- DES with a weak key: \( M \) is the swapping of the 2 halves → It has \( 2^{32} \) fixed points [Coppersmith 85].
Add some whitening keys [Rivest 84]

**FX construction**

Slide attack with complexity $2^{\frac{n+1}{2}}$

[Youssef-Tavares-Heys 96][Dunkelman et al. 12]

If $(m, c)$ and $(m', c')$ satisfy $m \oplus c = m' \oplus c'$, then check whether $k_0 \oplus k_2 = m' \oplus c$. 

Using involutional building-blocks

Examples:

- Feistel ciphers
- Involutional SPNs [Youssef-Tavares-Heys 96]
- Khazad [Barreto-Rijmen 00]
- ANUBIS [Barreto-Rijmen 00]
- NOEKEON [Daemen et al. 00]
- ICEBERG [Standaert et al. 04]...
$S$ is a permutation over $\mathbb{F}_2^m$

The diffusion layer is linear over $\mathbb{F}_{2^m}$ and has maximal branch number.
Involutional Sboxes with an SPN

Maximal expected probability for a two-round differential:

\[ \text{MEDP}_2 = \max_{a \neq 0, b} \Pr_{x, K}[\Delta E_K(x) = b | \Delta x = a] \]

For the AES Sbox \( S(x) = \ell(x^{254}) \):
\[ \text{MEDP}_2 = 53 \times 2^{-34} \quad \text{[Keliher-Sui 07]} \]

For the naive Sbox \( S(x) = x^{254} \):
\[ \text{MEDP}_2 = 79 \times 2^{-34} \quad \text{[Daemen-Rijmen 06]} \]
\( \rightarrow \) Highest possible value for a function having similar values in its difference table \([Park et al. 03]\)
A new bound (particular case) [C.-Roué 13]

Consider an SPN with a nonlinear layer composed of $t$ parallel applications of a function $S$ over $\mathbb{F}_{2^m}$ and with an MDS linear diffusion layer over $\mathbb{F}_{2^m}$, if $S(x) = \ell(x^s)$ or $S(x) = (\ell(x))^s$ where $\ell$ is an affine permutation of $\mathbb{F}_{2^m}$, we have

$$\text{MEDP}_2 \leq 2^{-m(t+1)} \max_{1 \leq u \leq t} \max_{\alpha, \beta \neq 0} \sum_{\gamma \in \mathbb{F}_{2^m}^*} \delta(\alpha, \gamma)^u \delta(\gamma, \beta)^{t+1-u}$$

where $\delta(a, b) = \#\{x \in \mathbb{F}_{2^m}^2, S(x + a) + S(x) = b\}$.

Moreover, the bound is tight for all MDS linear layers if one of the following conditions holds:

- $S(x) = x^s$;
- $S(x) = \ell(x^s)$ and the maximum is attained for $u = 1$. 
<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>ζ</th>
<th>ζ²</th>
<th>ζ³</th>
<th>ζ⁴</th>
<th>ζ⁵</th>
<th>ζ⁶</th>
<th>ζ⁷</th>
<th>ζ⁸</th>
<th>ζ⁹</th>
<th>ζ¹⁰</th>
<th>ζ¹¹</th>
<th>ζ¹²</th>
<th>ζ¹³</th>
<th>ζ¹⁴</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>ζ</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>ζ²</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>ζ³</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ζ⁴</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ζ⁵</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>ζ⁶</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>ζ⁷</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>ζ⁸</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>ζ⁹</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>ζ¹⁰</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ζ¹¹</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>ζ¹²</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>ζ¹³</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>ζ¹⁴</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
</tbody>
</table>

Difference table of the inverse function over $\mathbb{F}_{16}$
MEDP$_2$ for AES and variants

\[ 2^{-m(t+1)} \max_{1 \leq u \leq t} \max_{\alpha, \beta \neq 0} \sum_{\gamma \in F_{2m}^*} \delta(\alpha, \gamma)^u \delta(\gamma, \beta)^{t+1-u} \]

**AES Sbox** $S(x) = \ell(x^{254})$.

\[ \rightarrow \text{MEDP}_2 = 53 \times 2^{-34} \]

**Naive Sbox** $S(x) = x^{254}$.

\[ \delta(a, b) = \delta(b, a) \]

\[ \max_{\alpha, \beta \neq 0} \sum_{\gamma \in F_{2m}^*} \delta(\alpha, \gamma)^u \delta(\gamma, \beta)^{t+1-u} = \max_{\alpha, \beta \neq 0} \sum_{\gamma \in F_{2m}^*} \delta(\alpha, \gamma)^u \delta(\beta, \gamma)^{t+1-u} \]

\[ = \max_{\alpha \neq 0} \sum_{\gamma \in F_{2m}^*} \delta(\alpha, \gamma)^{t+1} \]

\[ \rightarrow \text{MEDP}_2 = 79 \times 2^{-34} \]
Minimizing the overhead of decryption:

reflection ciphers
Reflection ciphers

**Definition.** A block cipher $E$ is a reflection cipher if there exists a permutation $P$ of the key space such that, for all $K$,

$$(E_K)^{-1} = E_{P(K)}$$

**Examples.**

- Feistel cipher with independent round keys:
  $$P(k_1, \ldots, k_r) = (k_r, \ldots, k_1)$$

- RSA:
  $$P = \text{inversion modulo } (p - 1)(q - 1).$$
Properties of the coupling permutation

\[(E_K)^{-1} = E_P(K)\]

implies

\[E_K = E_{P^2}(K)\]

Choice of \(P\).

\(P\) should be an involution.

Example:

\[P(K) = K \oplus \alpha\]
Iterated reflection cipher with $P(K) = K \oplus \alpha$

Encryption:

$m \rightarrow F_1 \rightarrow F_2 \rightarrow K \rightarrow F_r \rightarrow M \rightarrow F_r^{-1} \rightarrow K \oplus \alpha \rightarrow F_2^{-1} \rightarrow F_1^{-1} \rightarrow c$

Decryption:

$c \rightarrow F_1 \rightarrow F_2 \rightarrow K \oplus \alpha \rightarrow F_r \rightarrow M \rightarrow F_r^{-1} \rightarrow K \rightarrow F_2^{-1} \rightarrow F_1^{-1} \rightarrow m$

where $M$ is an involution.
Example of a reflection cipher with $P(k_1, k_2) = (k_2 \oplus \alpha, k_1 \oplus \alpha)$

For all keys with $k_2 = k_1 \oplus \alpha$, the cipher is an involution, and it has the same number of fixed points as $M$.

$\rightarrow$ Large class of weak keys.
Fixed points of the coupling permutation

Fixed points of $P$.
The keys for which the encryption function is an involution can be detected with $\mathcal{O}(2^{n/2})$ plaintext-ciphertext pairs.

Choice of $P$.
$P$ should be an involution without fixed points.

Example:

$$P(K) = K \oplus \alpha$$
On related-key distinguishers for reflection ciphers

**Trivial related-key distinguishers:**
are not considered.
(they may be important in some scenarios, e.g., [Iwata-Kurosawa 03])

**Related-key distinguishers:**
may have an impact in a single-key model.

A related-key distinguisher for $E_K$ involving two keys $K$ and $K'$ related by $K' = P(K)$ is a distinguisher in the single-key model.

→ Related-key distinguishers may be relevant!
On differential related-key distinguishers

Distinguishers involving $K$ and $K' = P(K)$ should be avoided.

Two strategies:

- Choose $P$ such that the existence of such distinguishers is very unlikely, e.g., such that $K \oplus P(K)$ has always a high weight;

- Choose $P$ such that such related-key distinguishers can be exploited for a few $K$ only.

Trade-off between

$$\min_{K} \text{wt}(K \oplus P(K)) \text{ and } \max_{\delta} \# \{K : K \oplus P(K) = \delta\}$$

For $P(K) = K \oplus \alpha$ where $\text{wt}(\alpha)$ is high, we maximize the first quantity.
PRINCE
Reflection cipher with $P(K) = K \oplus \alpha$
Increasing the key length

**FX construction** [Rivest 84]

\[ k = (k_0 || k_1) \]

\[ k_1 \]

\[ \pi(k_0) \]

\[ \oplus \]

\[ \oplus \]

\[ m \rightarrow c \]

with \( \pi(x) = (x \gg 1) \oplus (x \gg 63) \)

\( \rightarrow (k_0 \oplus k_1, \pi(k_0) \oplus k_1) \) takes all possible values when \((k_0, k_1)\) varies.
Security of the $FX$ construction [Kilian–Rogaway 96]

$$FX_{k_0,k_1,k_2}(m) = F_{k_1}(m \oplus k_0) \oplus k_2$$

The advantage of any adversary who makes $D$ queries to $E = FX$ and $T$ queries to $(F, F^{-1})$ is at most

$$DT2^{-(\kappa_1+n-1)}$$
Impact of the reflection property on the $FX$ construction

**Ideal reflection cipher with coupling permutation $P$.**

If $P$ is an involution without fixed points, the key space can be decomposed as

$$F_2^{\kappa_1} = H \cup P(H)$$

where $H$ contains half of the keys.

Let $F$ be an ideal block cipher with key space $H$.

We extend it by

$$\tilde{F}_k(x) = \begin{cases} F_k(x) & \text{if } k \in H \\ F_{P(k)}^{-1}(x) & \text{if } k \in P(H) \end{cases}$$

**Security of the $\tilde{FX}$ construction.**

The advantage of any adversary who makes $D$ queries to $E = \tilde{F}X$ and $T$ queries to $(F, F^{-1})$ is at most

$$DT2^{-(\kappa_1+n-2)}.$$
Parameters

- Block size: 64 bits
- Key size: 128 bits
- Nb of Sbox layers: 12

Security claim in the single-key model:

126-bit security

There is no attack with time and data complexities are such that

$$DT \ll 2^{126}$$

Best attack.

MitM attack on 8 rounds with $$DT = 2^{124}$$

[C. Naya-Plasencia Vayssière 13].
Conclusions and open issues

- **Involutional building-blocks** may introduce some weaknesses in some cases. How can we use them in secure way?

- Reflection ciphers considerably reduce the overhead on decryption on top of encryption for unrolled implementations.

- Find some **other key schedules** (work in progress).