Construction of Lightweight S-Boxes using Feistel and MISTY structures

Anne Canteaut Sébastien Duval Gaëtan Leurent

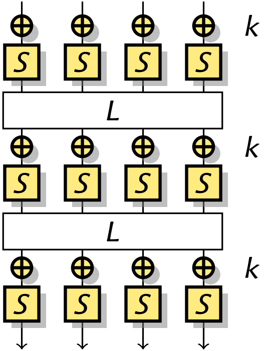
Inria, France

SAC 2015

Block cipher design

Shannon's criteria (1949)

- Diffusion
  - Every bit of plaintext and key should affect every bit of output
  - Usually linear mixing layers
- Confusion
  - Relation between plaintext and ciphertext must be intractable
  - Confusion requires non-linear operations
  - Often implemented with tables: S-Box



SPN cipher

- S-Boxes are critical components of modern ciphers.

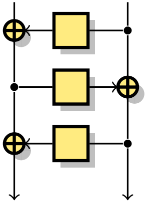
Lightweight cryptography

- 8-bit S-Boxes are expensive
  - Maybe too large for RFID...

- Smaller S-Boxes require less resources
  - table-based software: smaller table
  - hardware: lower gate count
  - bit-sliced implementation: lower instruction count
  - vectorized implementation: 4-bit S-Box using vector permutation
  - FPGA: small S-Boxes with LUT
- But require more rounds
  - Differential probability: 2^{-6} for an 8-bit S-Box, 2^{-2} for a 4-bit S-Box
- And a more complex linear layer

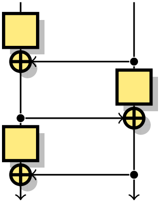
- Can we find some trade-off?

Constructing S-Boxes from smaller ones



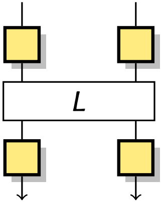
Feistel

- Crypton v0.5
- ≈ Zorro
- Robin



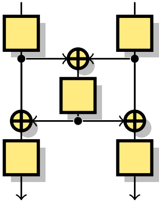
Misty

- Fantomas



SPN

- Crypton v1.0
- Iceberg
- Khazad



Lai-Massey

- Whirlpool

Objective of this talk

- Study the construction of S-Boxes with Feistel and Misty structures
  - In particular, construction of 8-bit S-Boxes from 4-bit ones
  - Tradeoff between implementation cost and security parameters

- Focus on differential uniformity
  - Linearity results in the paper

Our results

1. Determine best properties achievable with these structures
   - Application to 8-bit S-Boxes

2. Construct concrete lightweight S-Boxes

S-Box security parameters

Definition (Differential uniformity [Nyberg93])

Let F be a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$. The differential table of F is:

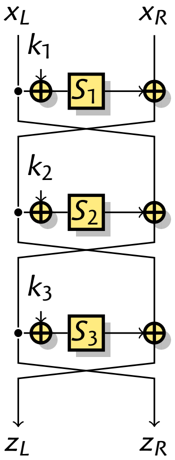
$$\delta_F(a \to b) = \#\{x \in \mathbb{F}_2^n \mid F(x \oplus a) = \oplus F(x) \oplus b\} .$$

Moreover, the *differential uniformity* of F is

$$\delta(F) = \max_{a \neq 0, b} \delta_F(a, b) .$$

- $\delta_F(a \to b)$ is always even
- $\delta(F) = 2$ for APN functions (almost perfect nonlinear)
  - *e.g.* $x \to x^3$ is APN

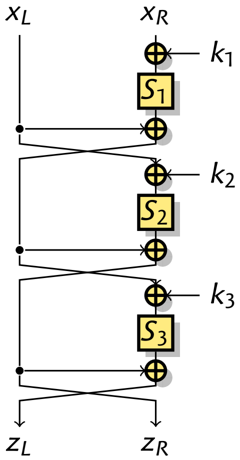
Feistel and Misty constructions



3-round Feistel network

- Introduced by Feistel in 1973 for Lucifer, DES
- Builds a $2n$-bit permutation out of n-bit functions
- In this talk: balanced
- Notations:
  - Small functions S_1, S_2, S_3
  - Full construction F
  - Fixed key, $k = 0$

Feistel and Misty constructions



3-round MISTY network

- Introduced by Matsui in 1996 for MISTY1
- Builds a $2n$-bit function out of n-bit functions
- In this talk: balanced
- Notations:
  - Small functions S_1, S_2, S_3
  - Full construction F
  - Fixed key, $k = 0$

Feistel and Misty constructions

- Come from block cipher design: keyed permutation
- Widely studied, lots of security results known

$$\mathrm{MEDP}(F_K) = \max_{a\neq 0,b} \frac{1}{2^k} \sum_{K\in\mathbb{F}_2^k} \frac{\delta_{F_K}(a,b)}{2^n}$$

$$\mathrm{MELP}(F_K) = \max_{a,b\neq 0} \frac{1}{2^k} \sum_{K\in\mathbb{F}_2^k} \left(\frac{\lambda_{F_K}(a,b)}{2^n}\right)^2$$

$$\mathrm{MEDP}(S_i) \leq p \Rightarrow \mathrm{MEDP}(F) \leq p^2$$ [NK95, M96]

$$\mathrm{MELP}(S_i) \leq q \Rightarrow \mathrm{MELP}(F) \leq q^2$$ [N94, AO97]

- But not applicable in the fixed key setting!

MEDP *and* EMDP

Example

- 3-round Misty structure
- $S_i = [\mathtt{A}, \mathtt{7}, \mathtt{9}, \mathtt{6}, \mathtt{0}, \mathtt{1}, \mathtt{5}, \mathtt{B}, \mathtt{3}, \mathtt{E}, \mathtt{8}, \mathtt{2}, \mathtt{C}, \mathtt{D}, \mathtt{4}, \mathtt{F}]$.
- $\delta(S_i) = 4$, $\mathrm{MEDP}(S_i) = 2^{-2}$
- $\mathrm{MEDP}(F) \leq 2^{-4}$
- For every key, there is a differential with probability 2^{-3}

- MEDP bound means:
  1. Choose input/output differences
  2. For a random key, the differential probability is low
- No bound when the difference is chosen after the key!

Feistel: Previous results

Theorem ([Li & Wang, CHES'14])

- $\delta(F) \geq 2\delta(S_2)$
- $\delta(F) \geq 2^{n+1}$ *if* S_2 *is not a permutation*

In particular, for $n = 4$

- $\delta(F) \geq 8$, *tight*

Feistel: New results

Theorem

- $\delta(F) \geq \delta(S_2) \max(\delta_{\min}(S_1), \delta_{\min}(S_3))$
- $\delta(F) \geq 2^{n+1}$ *if* S_2 *is not a permutation*
- $\delta(F) \geq \max_{i\neq 2, j\neq i,2}\left(\delta(S_i)\delta_{\min}(S_j),\ \delta(S_i)\delta_{\min}(S_2^{-1})\right)$ *if* S_2 *is a permutation*

In particular, for $n = 4$

- $\delta(F) \geq 8$, *tight*

- $\delta_{\min}(S) = \min_{a\neq 0} \max_b \delta_S(a, b)$
- Bounds involving all three S-boxes

MISTY: New results

Theorem

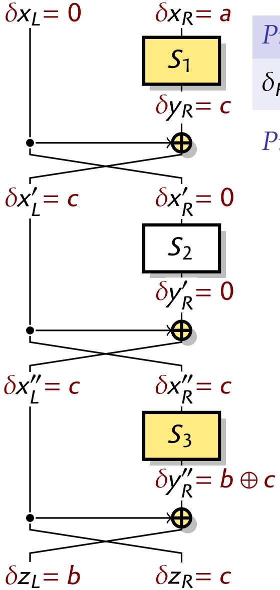
- $\delta(F) \geq \delta(S_1) \max(\delta_{\min}(S_2), \delta_{\min}(S_3))$
- $\delta(F) \geq 2^{n+1}$ *if* S_1 *is not a permutation*
- $\delta(F) \geq \max_{i \neq 1, j \neq 1, i} \left(\delta(S_i)\delta_{\min}(S_j),\ \delta(S_i)\delta_{\min}(S_1^{-1})\right)$ *if* S_1 *is a permutation*

In particular, for $n = 4$

- $\delta(F) \geq 8$, *tight*

- $\delta_{\min}(S) = \min_{a \neq 0} \max_b \delta_S(a, b)$
- No previous results on fixed-key Misty structure

Proof



Proposition

$$\delta_F(0 \,\|\, a, b \,\|\, c) = \delta_{S_1}(a,c) \times \delta_{S_3}(c, b \oplus c)$$

Proof

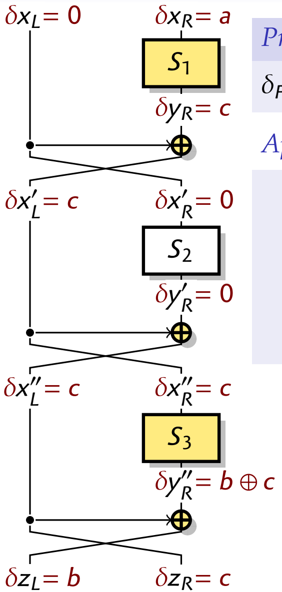
$$F(x_L \,\|\, x_R) \oplus F(x_L \,\|\, (x_R \oplus a)) = b \,\|\, c$$

$$\Leftrightarrow \begin{cases} S_3(S_1(x_R) \oplus x_L) \oplus S_3(S_1(x_R \oplus a) \oplus x_L) = b \oplus c, \\ S_2(x_L) \oplus S_1(x_R) \oplus x_L \oplus S_2(x_L) \oplus S_1(x_R \oplus a) \oplus x_L = c \end{cases}$$

$$\Leftrightarrow \begin{cases} S_3(S_1(x_R) \oplus x_L) \oplus S_3(S_1(x_R \oplus a) \oplus x_L) = b \oplus c, \\ S_1(x_R) \oplus S_1(x_R \oplus a) = c \end{cases}$$

$$\Leftrightarrow \begin{cases} x_R \in D_{S_1}(a \to c) \\ x_L \in S_1(x_R) \oplus D_{S_3}(c \to b \oplus c) \end{cases}$$

Proof



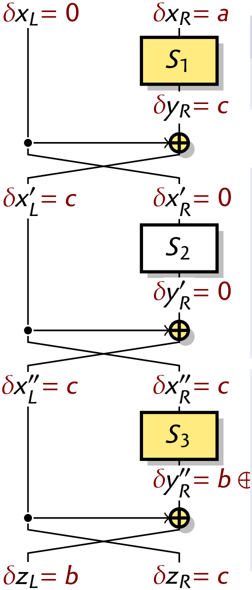
Proposition

$$\delta_F(0 \,\|\, a, b \,\|\, c) = \delta_{S_1}(a, c) \times \delta_{S_3}(c, b \oplus c)$$

Application: if S_1 is not invertible

- Set $b = c = 0$, $\delta_{S_3}(0, 0) = 2^n$
- Select a, so that $\delta_{S_1}(a, 0) \geq 2$
- $\delta(F) \geq \delta_F(0 \,\|\, a, 0 \,\|\, 0) \geq 2^{n+1}$

Proof



Proposition

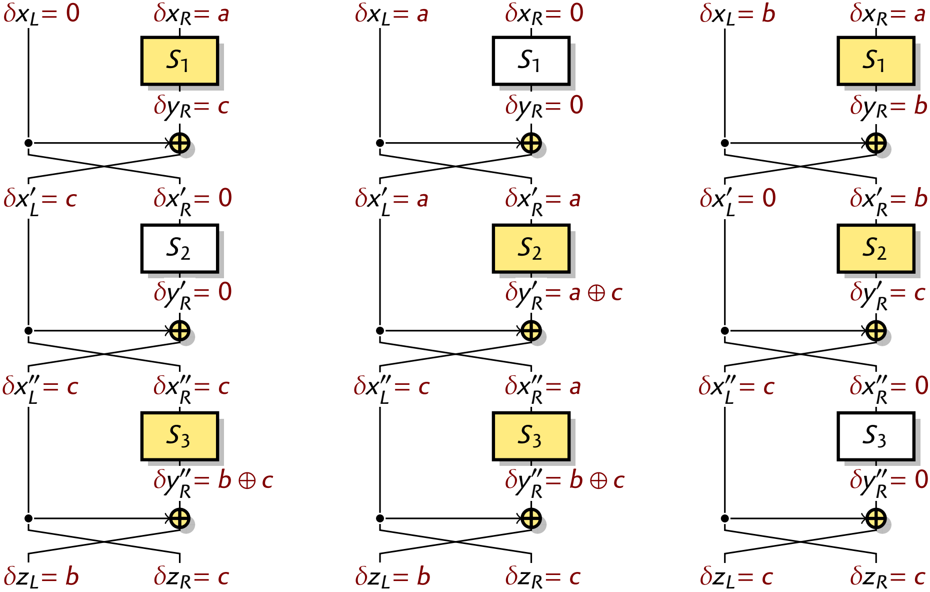
$$\delta_F(0 \,\|\, a, b \,\|\, c) = \delta_{S_1}(a,c) \times \delta_{S_3}(c, b \oplus c)$$

Application: if S_1 is invertible

- Select a, c so that $\delta_{S_1}(a,c) = \delta(S_1)$
- Select b with $\delta_{S_3}(c, b \oplus c) \geq \delta_{\min}(S_3)$
- $\delta(F) \geq \delta_F(0 \,\|\, a, b \,\|\, c) \geq \delta(S_1) \times \delta_{\min}(S_3)$

- Select b, c so that $\delta_{S_3}(c, b \oplus c) = \delta(S_3)$
- Select a with $\delta_{S_1}(a,c) \geq \delta_{\min}(S_1^{-1})$
- $\delta(F) \geq \delta_F(0 \,\|\, a, b \,\|\, c) \geq \delta(S_3) \times \delta_{\min}(S_1^{-1})$

Proof


δx_L = 0
δx_R = a
S_1
δy_R = c
δx'_L = c
δx'_R = 0
S_2
δy'_R = 0
δx''_L = c
δx''_R = c
S_3
δy''_R = b ⊕ c
δz_L = b
δz_R = c
δx_L = a
δx_R = 0
S_1
δy_R = 0
δx'_L = a
δx'_R = a
S_2
δy'_R = a ⊕ c
δx''_L = c
δx''_R = a
S_3
δy''_R = b ⊕ c
δz_L = b
δz_R = c
δx_L = b
δx_R = a
S_1
δy_R = b
δx'_L = 0
δx'_R = b
S_2
δy'_R = c
δx''_L = c
δx''_R = 0
S_3
δy''_R = 0
δz_L = c
δz_R = c

Application to $n = 4$

Properties of 4-bit S-Boxes

- Full classification of 4-bit permutations
  - 302 affine eq. classes [de Cannière; Leander & Poschmann '07]
- Full classification of 4-bit APN functions
  - 2 extended affine eq. classes [Brinkmann & Leander '08]
- There exist 4-bit APN functions
  - $\delta(S_i) = 2$, $\delta_{\min}(S_i) = 2$
- There are no 4-bit APN permutations
  - If S_i is a permutation, $\delta(S_i) \geq 4$, $\delta_{\min}(S_i) \geq 2$

8-bit MISTY S-Box

Theorem

- $\delta(F) \geq \delta(S_1) \max(\delta_{\min}(S_2), \delta_{\min}(S_3))$
- $\delta(F) \geq 2^{n+1}$ *if* S_1 *is not a permutation*
- $\delta(F) \geq \max_{i\neq 1, j\neq 1, i} \left(\delta(S_i)\delta_{\min}(S_j),\ \delta(S_i)\delta_{\min}(S_1^{-1})\right)$ *if* S_1 *is a permutation*

- If S_1 is a permutation, $\delta(S_1) \geq 4$, then $\delta(F) \geq 8$
- If S_1 is not a permutation, then $\delta(F) \geq 32$

- Can we reach $\delta(F) = 8$?

8-bit MISTY S-Box with $\delta(F) = 8$

Necessary conditions for $\delta(F) = 8$

- S_1 a permutation, with $\delta(S_1) = 4$
- S_2, S_3 APN

Proof.

- Let's assume $\delta(S_3) \geq 4$
  - There exist a, b with $\delta_{S_3}(a, b) \geq 4$
  - There are two pairs $(x, x \oplus a)$, $(y, y \oplus a)$ in $D_{S_3}(a \to b)$
  - Also two pairs (x, y), $(x \oplus a, y \oplus a)$ in $D_{S_3}(a' \to d')$ with $a' = x \oplus y$, $d' = S_3(x) \oplus S_3(y)$
  - Also two pairs $(x, y \oplus a)$, $(x \oplus a, y)$ in $D_{S_3}(a \oplus a' \to b \oplus b')$
  - There exist three columns $a, a', a \oplus a'$, with values ≥ 4

8-bit MISTY S-Box with $\delta(F) = 8$

Necessary conditions for $\delta(F) = 8$

- S_1 a permutation, with $\delta(S_1) = 4$
- S_2, S_3 APN

Proof.

- Let's assume $\delta(S_3) \geq 4$
  - There exist three columns $a, a', a \oplus a'$, with values ≥ 4
- We have $\delta_F(0 \parallel a, b \parallel c) = \delta_{S_1}(a, c) \times \delta_{S_3}(c, b \oplus c)$
  - Lines of δ_{S_1} and columns of δ_{S_3}
- We need S_1 with three lines $a, a', a \oplus a'$ with value ≤ 2
  - Property invariant by affine equivalence
  - Test equivalence class: no solution □

8-bit Feistel S-Box

Theorem

- $\delta(F) \geq \delta(S_2) \max(\delta_{\min}(S_1), \delta_{\min}(S_3))$
- $\delta(F) \geq 2^{n+1}$ *if S_2 is not a permutation*
- $\delta(F) \geq \max_{i \neq 2, j \neq i,2} \left(\delta(S_i)\delta_{\min}(S_j),\ \delta(S_i)\delta_{\min}(S_2^{-1})\right)$ *if S_2 is a permutation*

- If S_2 is a permutation, $\delta(S_2) \geq 4$, then $\delta(F) \geq 8$
- If S_2 is not a permutation, then $\delta(F) \geq 32$

Necessary conditions for $\delta(F) = 8$

- S_2 a permutation, with $\delta(S_2) = 4$
- S_1, S_3 APN

8-bit Feistel & MISTY S-Box

Feistel

- $\delta(F) \geq 8$, tight
  - Requires S_1, S_3 APN, S_2 permutation with $\delta(S_2) = 4$
- $\mathcal{L}(F) \geq 48$
  - $\mathcal{L}(F) \geq 64$ if $\delta(F) < 32$

MISTY

- $\delta(F) \geq 8$, tight
  - Requires S_2, S_3 APN, S_1 permutation with $\delta(S_1) = 4$
  - F is not a permutation!
- $\mathcal{L}(F) \geq 48$
  - $\mathcal{L}(F) \geq 64$ if $\delta(F) < 32$
- Permutation:
  $\delta(F) = 16$, tight

Building a good S-Box for lightweight designs

- According to previous results, Feistel structure is better
- We need S_1, S_3 APN, S_2 permutation with $\delta(S_2) = 4$
  - Can we choose them with a small implementation?
    Small hardware, bitslice software

- Exhaustive search over small implementations
  until good property are reached [Üllrich & *al.* '11]
  - Search sequences of instructions for bit-sliced implementation
  - Use equivalences class to cut branches
  - Minimize non-linear operations

Concrete example

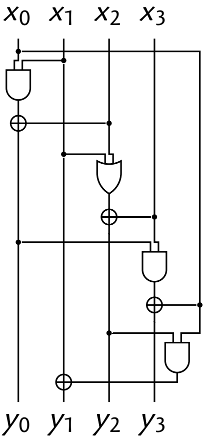
Permutation with $\delta = 4$

- Easy search
  - Re-use results from Üllrich *et al.*
- 9-instruction solutions
  - 4 non-linear
  - 4 XOR
  - 1 copy
- 4 NL gates is optimal

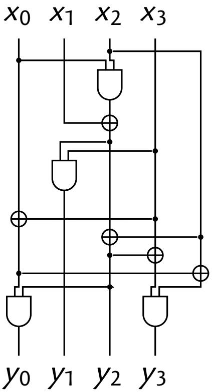
APN function

- Expensive search
  - No permutation filtering
  - 6k core-hours
- 10-instruction solutions
  - But 6 non-linear
- 11-instruction solutions
  - 4 non-linear
  - 5 XOR
  - 2 copy
- 4 NL gates is optimal

Concrete example



Permutation with $\delta = 4$



APN function

Results

		Implem.		Properties		
S-Box	Construction	$\wedge, \vee$	$\oplus$	$\mathcal{L}$	δ	cost
AES	Inversion	32	83	32	4	1
Whirlpool	Lai-Massey	36	58	64	8	1.35
CRYPTON	3-r. Feistel	49	12	64	8	1.83
Robin	3-r. Feistel	12	24	64	16	0.56
Fantomas	3-r. MISTY (3/5 bits)	11	25	64	16	0.51
LS (unnamed)	Whirlpool-like	16	41	64	10	0.64
New	3-r. Feistel	12	26	64	8	0.45

Conclusion

1. Bounds on the security of fixed-key Feistel & MISTY networks

2. Application to 8-bit S-Boxes
   - Necessary conditions
   - Refined bounds for permutations
   - Feistel structure is better for 8-bit invertible S-Box

3. Construction of a concrete lightweight S-Box
   - 8-bit S-Box with 3-round Feistel
   - Improvement over previously used S-Boxes

Thanks

Questions?