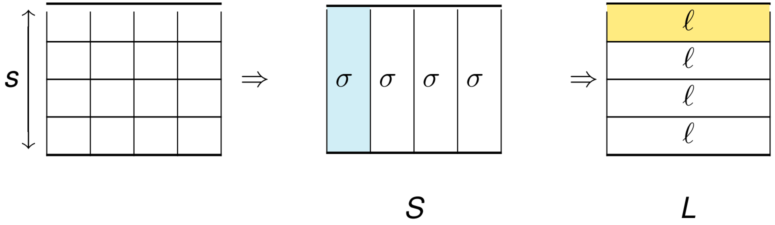
LS-design Exploration

Sébastien Duval

July 3, 2019

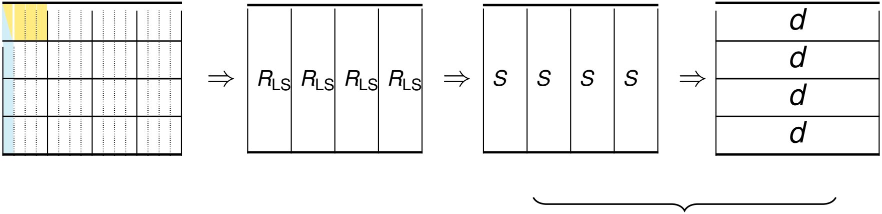
LS-Designs



$$R_{\mathrm{LS}} = L \circ S$$

$$\mathrm{LS}(\sigma, \ell, r) = (L \circ S)^r = (R_{\mathrm{LS}})^r$$

mLS-Designs



R_{intra}

R_{inter}

$$R_{mLS} = R_{inter} \circ R_{intra}$$

$$\text{mLS}(\sigma, \ell, d, r) = (R_{mLS})^r$$

L-boxes

L-boxes

- (16-bit L-box: branch numbers 8) ;
- 32-bit L-box: branch numbers 12 ;
- 2 × 32-bit L-box: branch numbers 16 ;

D-boxes

- 4-word D-box: branch numbers 4 ;
- (4-word D-box: branch numbers 5) ;
- 3-word D-box: branch numbers 4 ;

S-boxes Functional Criteria

Main functional criteria

- Algebraic degree
- Differential uniformity
- Linearity

Additional criteria

- Branch numbers
- …

S-boxes Implementation Criteria

Unmasked

SW

- Nb instructions

HW

- Nb gates
- Depth

Masked

SW

- Nb ANDs

HW

- Nb ANDs
- AND depth

S-boxes Results

1. Explored existing S-boxes from 3 to 16 bits.
2. Explored Feistel, Misty, Lai-Massey-like structures.
3. For each size, selected one S-box.
    - $n = 3$: x^6
    - $n = 4$: Skinny-like
    - $n = 5$: x^3
    - $n = 6$: Quadratic / 3-round Misty

Exploration: mLS-designs

1. Restricted to $n =$3- to 6-bit S-boxes for simplicity.
2. Selected the 2×32 L-box with $BN = 16$.
3. Considered MDS D for 3×3, 4×4, $5{\times}5$, 6×6, plus almost-MDS for 4×4.
4. Considered all mLS-designs, with $1 \leq m \leq n$.
5. Computed the number of rounds to be secure against differential / linear attacks (wide-trail) and algebraic attacks.
6. 2 objectives: 128-bit security and full-state security.
7. Computed the total number of AND gates / AND depth / gates / depth for each mLS(σ, L, D, r).
8. Compared the total costs to get 128-bit security and to get full-state security (note: throughput depends on state size, and state size has a cost in regsiters).

Shadow and Clyde

State size

1. Selected state size of roughly 128 bits for Clyde.
2. Selected state size of either roughly 384 or 512 bits for Shadow.
3. Selected best S-box for each case (trade-offs between speed and area / implem. size).

LS-design choice: Clyde

Robin → Skinny-like

mLS-design choice: Shadow

Robin → Skinny-like
D almost-MDS for cost reduction.

Remarks

- Choice of σ and D is not clear (lots of trade-offs).
- Choice of state size is not clear (throughput / S-box size / cost of registers / NIST specs).
- 128-bit- vs full codebook-security is not clear and has a huge impact on the number of rounds.
- Integrity proofs require better understanding of truncated differentials, which we could consider in the design.
- L has an import impact on the speed of Shadow.