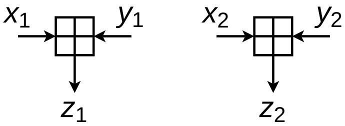
Maximum Probability Output Differences for ARX

Nicky Mouha

COSIC, KU Leuven, Belgium

FSE 2012 Rump Session

xdp^{+}: The XOR Differential Probability of Addition



- Given $\alpha = x_1 \oplus x_2$ and $\beta = y_1 \oplus y_2$,
  - probability that $z_1 \oplus z_2 = \gamma$ for a certain γ?
- XOR-differential probability of addition
  - $\mathrm{xdp}^{+}(\alpha, \beta \to \gamma)$

xdp^+: Motivating Example

$$\mathrm{xdp}^+(\mathtt{11100}, \mathtt{00110} \rightarrow \mathtt{10110})$$

$$= LA_{101}A_{100}A_{111}A_{011}A_{000}C = \frac{1}{4}$$

where

$$A_{000} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad A_{001} = A_{010} = A_{100} = \frac{1}{2}\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix},$$

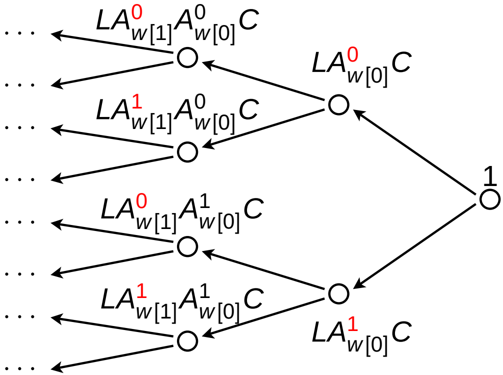
$$A_{011} = A_{101} = A_{110} = \frac{1}{2}\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \quad A_{111} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix},$$

$$L = [\ 1 \quad 1\ ], \quad C = [\ 1 \quad 0\ ]^T .$$

xdp^+ (FSE’01), $\mathrm{adp}^\oplus$ (FSE’04), general constructions (SAC’10)

Maximum Probability Output Difference

For $\mathrm{xdp}^{+}_{\max}$: see FSE’01. For general constructions?



$LA^{0}_{w[1]}A^{0}_{w[0]}C$
$LA^{0}_{w[0]}C$
$LA^{1}_{w[1]}A^{0}_{w[0]}C$
1
$LA^{0}_{w[1]}A^{1}_{w[0]}C$
$LA^{1}_{w[1]}A^{1}_{w[0]}C$
$LA^{1}_{w[0]}C$
$\cdots$

$$P = LA_{w[n-1]} \cdots A_{w[1]} A_{w[0]} C$$

$$L = [\ 1 \quad 1 \quad \cdots \quad 1\ ], \qquad C = [\ 1 \quad 0 \quad \cdots \quad 0\ ]^T$$

A* Search Algorithm

- Our approach: A* search algorithm
  - Fast admissible heuristic
  - Always finds best output difference
  - Can find second-best,... output differences as well

A* Search Algorithm

- Our approach: A* search algorithm
  - Fast admissible heuristic
  - Always finds best output difference
  - Can find second-best,... output differences as well

- Algorithm introduced in UNAF-paper
  - Presented this afternoon by Vesselin Velichkov

- Source code included in S-functions toolkit
  - `http://www.ecrypt.eu.org/tools/`