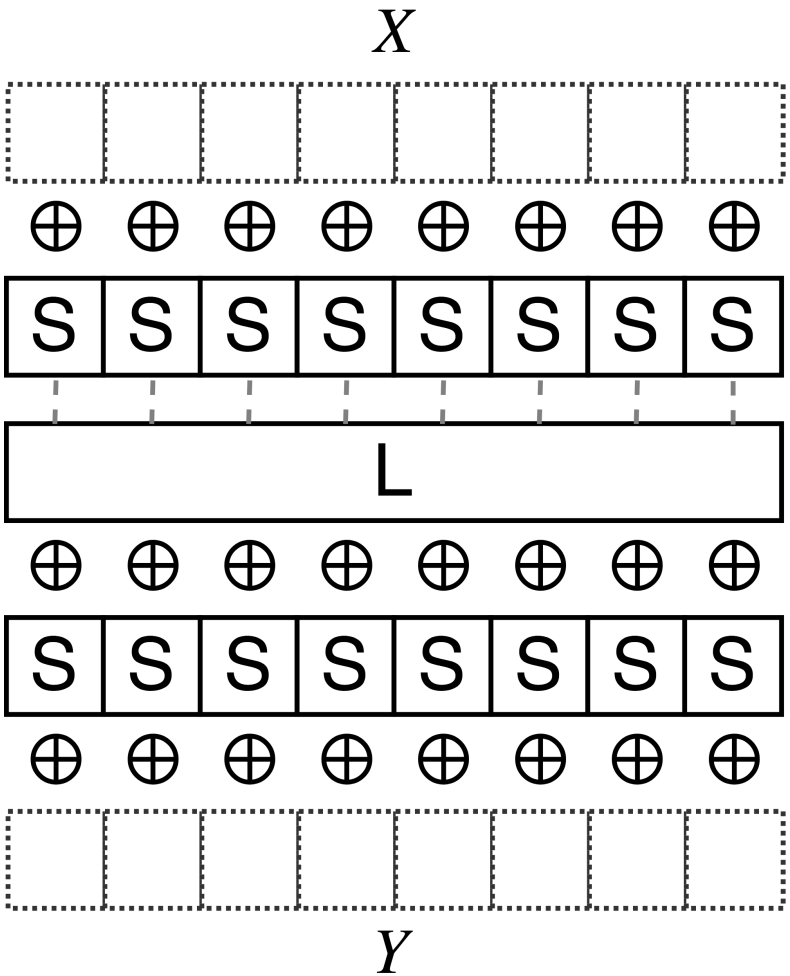
Exact MEDP/MELP for «heavy» 2R-SPN

Vitaly Kiryukhin, Anton Naumenko

JSC «InfoTeCS»

Fast Software Encryption – March 27, 2019

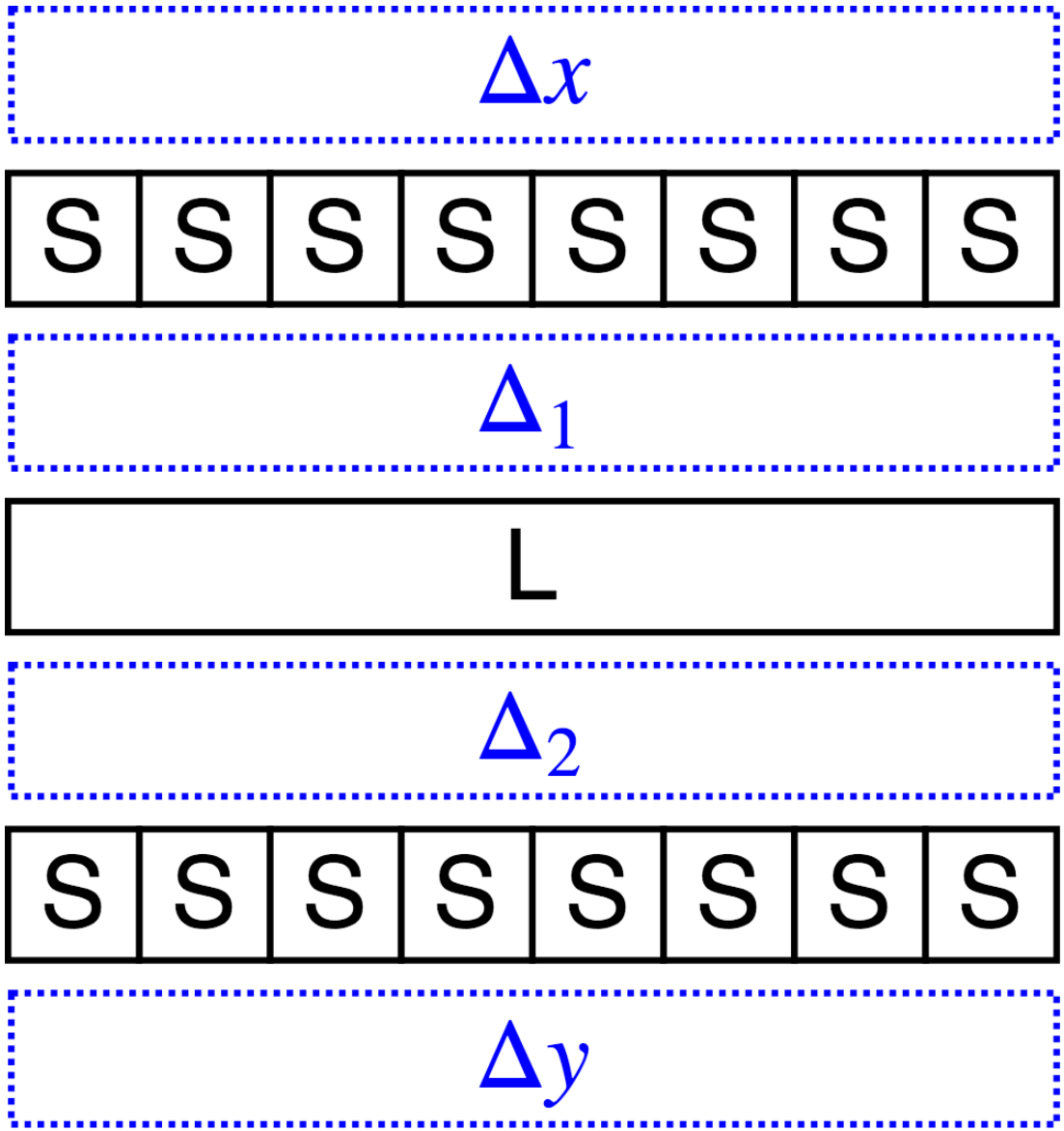
«Heavy» 2-round SPN



- m-bit bijective Sbox, $m \geq 8$
- Block size $n \cdot m \geq 64$ bits
- Branch number $\mathcal{B}_d = n + 1$

Typical example: **Khazad** and **Kuznyechik**

2-round trail and differential



2-round trail and differential

$\Omega = \Delta x \xrightarrow{S} \Delta_1 \xrightarrow{L} \Delta_2 \xrightarrow{S} \Delta y$ – 2-round differential trail

$EDCP(\Omega) = \prod_{i=1}^{n} DP(\Delta x[i] \to \Delta_1[i]) \cdot \prod_{i=1}^{n} DP(\Delta_2[i] \to \Delta y[i])$

$DIFF(\Delta x, \Delta y) = \{\Omega : \Omega = \Delta x \to \ldots \to \Delta y\}$

$$\mathrm{EDP}(\Delta x, \Delta y) = \sum_{\Omega \in DIFF(\Delta x, \Delta y)} \mathrm{EDCP}(\Omega)$$

$$\mathrm{MEDP} = \max_{DIFF(\Delta x, \Delta y)} \sum_{\Omega \in DIFF(\Delta x, \Delta y)} \mathrm{EDCP}(\Omega)$$

How to compute the exact MEDP?

- compute exact MEDP of minimum-weight ($\mathcal{B}_d = n + 1$) differentials
- compute the upper bound on non-minimum-weight differentials
- If the first is greater than the second then we have exact MEDP of 2R-SPN

Upper bound on non-minimum-weight differentials

We design dynamic programming algorithm for bounding non-minimum-weight differentials in 2R-SPN.

The algorithm uses only:

– difference distribution table of the Sbox

– $\mathcal{B}_d$ – the value of the branch number

Example: 2R-Khazad

FSE2003 Bound	Exact 2R-MEDP	Bound on non-min-weight differential
$2^{-43.36}$	$2^{-45} + 2^{-60}$	$2^{-45.02}$

Example of one of the best 2R-differentials

Δx	f0001208000f0000		$\log_2 \mathrm{EDCP}(\Omega_i)$
Ω_1	f0001248000f0000	b54800004800fbeb	-45
Ω_2	0a00c80700230000	1307000070053a6	-60
Δy		bf08000008001891	

Thank you for attention!

Questions?