Spook: L-Box Errata

The Spook team

No institute given.

The L-box used in Spook is an interleaved L-box that applies jointly to pairs of 32-bit words. Denoting the two words on which it is applied as x and y it can be written as:

$$(a, b) = \mathsf{L}(x, y) = \begin{pmatrix} \mathsf{circ}(\texttt{0xec045008}) \cdot x^{\mathsf{T}} \oplus \mathsf{circ}(\texttt{0x36000f60}) \cdot y^{\mathsf{T}} \\ \mathsf{circ}(\texttt{0x1b0007b0}) \cdot x^{\mathsf{T}} \oplus \mathsf{circ}(\texttt{0xec045008}) \cdot y^{\mathsf{T}} \end{pmatrix},$$

where circ denotes the circulant matrix whose first line is given in hexadecimal notation, so that the number $b = \sum_{i=0}^{31} 2^i b_i$ corresponds to the row vector $(b_0, \ldots, b_{31})$. Concretely, this L-box can be efficiently implemented (in the direct and inverse directions) thanks to six word-level rotations and six 32-bit XORs per word as shown by Algorithms 1 and 2. Unfortunately, the picture describing the L-box in the Spook specification contains a mistake and does not describe the correct operations.

Branch number. In the specification, we claim that the L-box has branch number 16 over pairs of input bits for x and y. However, we made a mistake when building the L-box: it is based on a linear code with distance 16 over two-bit words, but the L-box input/output are not correctly mapped to the linear code. As specified, the L-box has branch number 15 (it has branch number 16 if we consider pairs of bits (x_{i+1}, y_i), but this is not the correct notion).

Tweak. We can fix the branch number by slightly tweaking the L-box, adding a rotation at the output:

$$(a, b) = \mathsf{L}'(x, y) = \begin{pmatrix} \mathsf{circ}(\texttt{0x36000f60}) \cdot x^{\mathsf{T}} \oplus \mathsf{circ}(\texttt{0xd808a011}) \cdot y^{\mathsf{T}} \\ \mathsf{circ}(\texttt{0xec045008}) \cdot x^{\mathsf{T}} \oplus \mathsf{circ}(\texttt{0x36000f60}) \cdot y^{\mathsf{T}} \end{pmatrix},$$

The modified L-box can be implemented efficiently as shown by Algorithms 3 and 4 has the correct branch number 16, restoring the bounds on linear and differential trails given in the specification.

Acknowledgment

We would like to thank Gwezheneg Robert for pointing out the mistake.

Algorithm 1 Spook L-box

Input: (x, y)
Word size: 32
$a \leftarrow x \oplus \mathsf{rot}(x, 12)$
$b \leftarrow y \oplus \mathsf{rot}(y, 12)$
$a \leftarrow a \oplus \mathsf{rot}(a, 3)$
$b \leftarrow b \oplus \mathsf{rot}(b, 3)$
$a \leftarrow a \oplus \mathsf{rot}(x, 17)$
$b \leftarrow b \oplus \mathsf{rot}(y, 17)$
$c \leftarrow a \oplus \mathsf{rot}(a, 31)$
$d \leftarrow b \oplus \mathsf{rot}(b, 31)$
$a \leftarrow a \oplus \mathsf{rot}(d, 26)$
$b \leftarrow b \oplus \mathsf{rot}(c, 25)$
$a \leftarrow a \oplus \mathsf{rot}(c, 15)$
$b \leftarrow b \oplus \mathsf{rot}(d, 15)$
return (a, b)

Algorithm 2 Spook L-box inverse

Input: (x, y)
Word size: 32
$a \leftarrow x \oplus \mathsf{rot}(x, 25)$
$b \leftarrow y \oplus \mathsf{rot}(y, 25)$
$c \leftarrow x \oplus \mathsf{rot}(a, 31)$
$d \leftarrow y \oplus \mathsf{rot}(b, 31)$
$c \leftarrow c \oplus \mathsf{rot}(a, 20)$
$d \leftarrow d \oplus \mathsf{rot}(b, 20)$
$a \leftarrow c \oplus \mathsf{rot}(c, 31)$
$b \leftarrow d \oplus \mathsf{rot}(d, 31)$
$c \leftarrow c \oplus \mathsf{rot}(b, 26)$
$d \leftarrow d \oplus \mathsf{rot}(a, 25)$
$a \leftarrow a \oplus \mathsf{rot}(c, 17)$
$b \leftarrow b \oplus \mathsf{rot}(d, 17)$
$a \leftarrow \mathsf{rot}(a, 16)$
$b \leftarrow \mathsf{rot}(b, 16)$
return (a, b)

Algorithm 3 Tweaked L-box

Input: (x, y)
Word size: 32
$a \leftarrow x \oplus \mathsf{rot}(x, 12)$
$b \leftarrow y \oplus \mathsf{rot}(y, 12)$
$a \leftarrow a \oplus \mathsf{rot}(a, 3)$
$b \leftarrow b \oplus \mathsf{rot}(b, 3)$
$a \leftarrow a \oplus \mathsf{rot}(x, 17)$
$b \leftarrow b \oplus \mathsf{rot}(y, 17)$
$c \leftarrow a \oplus \mathsf{rot}(a, 31)$
$d \leftarrow b \oplus \mathsf{rot}(b, 31)$
$a \leftarrow a \oplus \mathsf{rot}(d, 26)$
$b \leftarrow b \oplus \mathsf{rot}(c, 25)$
$a \leftarrow a \oplus \mathsf{rot}(c, 15)$
$b \leftarrow b \oplus \mathsf{rot}(d, 15)$
$b \leftarrow \mathsf{rot}(b, 1)$
return (b, a)

Algorithm 4 Tweaked L-box inverse

Input: (x, y)
Word size: 32
$a \leftarrow x \oplus \mathsf{rot}(x, 25)$
$b \leftarrow y \oplus \mathsf{rot}(y, 25)$
$c \leftarrow x \oplus \mathsf{rot}(a, 31)$
$d \leftarrow y \oplus \mathsf{rot}(b, 31)$
$c \leftarrow c \oplus \mathsf{rot}(a, 20)$
$d \leftarrow d \oplus \mathsf{rot}(b, 20)$
$a \leftarrow c \oplus \mathsf{rot}(c, 31)$
$b \leftarrow d \oplus \mathsf{rot}(d, 31)$
$c \leftarrow c \oplus \mathsf{rot}(b, 26)$
$d \leftarrow d \oplus \mathsf{rot}(a, 25)$
$a \leftarrow a \oplus \mathsf{rot}(c, 17)$
$b \leftarrow b \oplus \mathsf{rot}(d, 17)$
$a \leftarrow \mathsf{rot}(a, 15)$
$b \leftarrow \mathsf{rot}(b, 16)$
return (b, a)