Constructions of S-boxes with Uniform Sharing

Kerem Varici[1], Svetla Nikova[1], Ventzislav Nikov[2], and Vincent Rijmen[1]

[1] KU Leuven, imec-COSIC, Belgium, {name.surname}@esat.kuleuven.be
[2] NXP Semiconductors, Belgium, venci.nikov@gmail.com

Two S-boxes $S_1(x)$ and $S_2(x)$ are *affine equivalent* if there exists a pair of invertible affine permutations $A(x)$ and $B(x)$, such that $S_1 = A \circ S_2 \circ B$. The set of invertible 3×3 S-boxes contains 4 equivalence classes: 3 classes containing quadratic functions, and one class containing the affine functions. There is a transformation [2] which expands the 3-bit classes Q_1^3, Q_2^3, and Q_3^3 into 4-bit classes Q_4^4, Q_{12}^4 and Q_{300}^4. Recently a classification of all quadratic 5×5 S-boxes was presented [1]. The 5-bit classes $Q_1^5, Q_3^5, Q_4^5, Q_7^5, Q_{13}^5$ and Q_{30}^5 are extensions of the 4-bit quadratic classes Q_4^4, Q_{294}^4, Q_{12}^4, Q_{299}^4, Q_{293}^4 and Q_{300}^4. Thus the method used in the above publications can be summarized as follows: define $S_1(\bar{x}) = (t_1, t_2, \ldots, t_n)$, $S(\bar{x}, x_{n+1}) = (y_1, y_2, \ldots, y_{n+1})$, where $\bar{x} = (x_1, x_2, \ldots x_n)$ and

$$\begin{aligned} y_i(\bar{x}, x_{n+1}) &= t_i(\bar{x}), \quad \text{for } i = 1, \ldots, n \\ y_{n+1}(\bar{x}, x_{n+1}) &= x_{n+1} \end{aligned} \tag{1}$$

Another well known construction is the so-called *Shannon expansion*: any function F can be presented as follows

$$F(\bar{x}) = x_i F_{x_i=1}(\bar{x}) + (x_i + 1) F_{x_i=0}(\bar{x}) \tag{2}$$

where $F_{x_i=1}(\bar{x}) = F(x_1, ..., x_i = 1, ..., x_n)$ and $F_{x_i=0}(\bar{x}) = F(x_1, ..., x_i = 0, ..., x_n)$.

Threshold implementation is a method to provide side-channel resistance based on the use of *uniform sharings* [2]. For efficiency reasons, one wants to find uniform sharings with a minimal number of shares. Recall that uniform sharing with 3 shares exists for all 3×3 S-boxes except for class Q_3^3; and a uniform sharing with $4, 5$ and more shares exists for all 3 classes. When $n = 4$ a uniform sharing with 3 shares exists for all 5 quadratic classes except for Q_{300}^4; and a uniform sharing with $4, 5$ and more shares exists for all 6 of them. When $n = 5$ a 3-share uniform sharing exists for 30 of the quadratic permutation classes. Moreover, all 5-bit quadratic permutation classes have uniform sharing with 4 and more shares.

Given two $n \times n$ bijective S-boxes $S_1(\bar{x}) = (t_1, t_2, \ldots, t_n)$ and $S_2(\bar{x}) = (u_1, u_2, \ldots, u_n)$ then using (2) we get an $(n+1) \times (n+1)$ S-box $S(\bar{x}, x_{n+1}) = (y_1, y_2, \ldots, y_{n+1})$:

$$\begin{aligned} y_i(\bar{x}, x_{n+1}) &= x_{n+1} t_i(\bar{x}) + (1 + x_{n+1}) u_i(\bar{x}), \text{ for } i = 1, \ldots, n \\ y_{n+1}(\bar{x}, x_{n+1}) &= x_{n+1} F(\bar{x}) + (1 + x_{n+1}) G(\bar{x}) \end{aligned} \tag{3}$$

Theorem 1. *Given S_1 and S_2 are bijections then S is a bijection if and only if*

$$G(\bar{x}) = F(S_1^{-1}(S_2(\bar{x}))) + 1 \quad \textit{or equivalently} \quad G = S_2 \circ S_1^{-1} \circ F + 1 \quad \textit{holds.}$$

When $S_1 = S_2$ this simplifies to:

$$\begin{aligned} y_i(\bar{x}, x_{n+1}) &= t_i(\bar{x}), \qquad \text{for } i = 1, \ldots, n \\ y_{n+1}(\bar{x}, x_{n+1}) &= x_{n+1} + F(\bar{x}) \end{aligned} \tag{4}$$

Note that compared to the constructions (1) used in [2] to get from 3×3 an 4×4 S-box and similarly in [1] from 4×4 an 5×5 S-box, the construction (4) extends it to allow F to be any Boolean function of n variables. We can prove that uniform sharing with s shares exist for S in (4) if and only if S_1 and F have uniform sharing with s shares.

References

1. D. Bozilov, B. Bilgin, H. Sahin. "A Note on 5-bit Quadratic Permutations Classification", FSE 2017.
2. B. Bilgin, S. Nikova, V. Rijmen, V. Nikov, G. Stutz. "Threshold Implementations of all 3×3 and 4×4 S-boxes", CHES 2012, LNCS 7428, 76-91.