Constructions of S-boxes with uniform sharing

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

[1]imec-COSIC, KU Leuven, Belgium

[2]NXP Semiconductors, Belgium

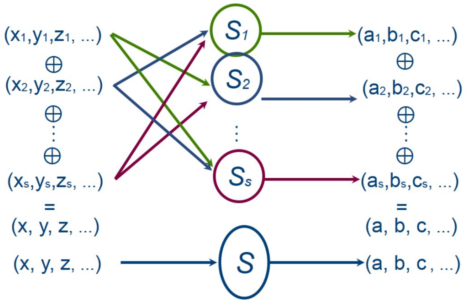
September, 2017

Threshold Implementations

Threshold Implementation (TI) [Nikova, Rechberger, Rijmen, 2006] is a provably secure Masking Scheme based on Secret Sharing and Multiparty Computation.

- TI protects implementations against any order DPA.
- TI is secure in a circuit with glitches
- Efficient in HW
- Independent of the HW technology

Threshold Implementations



Properties: Correctness, Non-completeness, [optional] Uniformity

Uniformity implies that if unshared function is a permutation, the shared function should also be a permutation.

Threshold Implementations

Two S-boxes S_1 and S_2 are *affine equivalent* if there exists a pair of affine permutations A and B, such that $S_1 = A \circ S_2 \circ B$.

remark	unshared	3 shares				4 shares			5 shares
		1	2	3	4	1	2	3	1
affine	1	1				1			1
quadratic	6	5	1			6			6
cubic in A_{16}	30		28	2			30		30
cubic in A_{16}	114			113	1			114	114
cubic in $S_{16} \setminus A_{16}$	151					4	22	125	151

4 affine equivalent classes of 3x3 S-boxes
302 affine equivalent classes of 4x4 S-boxes, [CHES2012]
$\mathcal{A}$ - Affine, $\mathcal{Q}$ - Quadratic, $\mathcal{C}$ - Cubic

back-to-3 back-to-4

Our approach

- Most papers so far have studied TI sharings for given S-boxes
- Here we go the opposite way:
  we start from $n \times n$ S-boxes with known sharings and then construct new $(n+1) \times (n+1)$ S-boxes from them, with desired sharings.

Shannon's Expansion

Let F be a Boolean vectorial function of n variables $\bar{x} = x_1, ..., x_n$:

$$F : \{0,1\}^n \rightarrow \{0,1\}^m$$

Let define $\bar{x_i} = x_1, ..., x_{i-1}, x_{i+1}, ..., x_n$ and two new Boolean vectorial functions of $n-1$ variables as follows:

$$\begin{aligned} F_{x_i=1}(\bar{x_i}) &= F(x_1, ..., x_{i-1}, x_i = 1, x_{i+1}, ..., x_n) \text{ and} \\ F_{x_i=0}(\bar{x_i}) &= F(x_1, ..., x_{i-1}, x_i = 0, x_{i+1}, ..., x_n) \text{ then} \end{aligned}$$

F can be written as:

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

Application of Shannon's Expansion to S-boxes

Given two $n \times n$ S-boxes (permutations):

$$\begin{aligned} S_1(\bar{x}) &= (t_1, t_2, \ldots, t_n) \text{ and} \\ S_2(\bar{x}) &= (u_1, u_2, \ldots, u_n) \end{aligned}$$

then using Shannon's expansion one gets an $(n+1) \times (n+1)$ S-box $S(x_1, \ldots, x_n, x_{n+1}) = (y_1, \ldots, y_n, y_{n+1})$:

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

where F and G are Boolean functions of n inputs.

Theorem 1

Let S be the S-box generated by using Shannon's expansion using two permutations S_1 and S_2. Then, S is a permutation if and only if

$$\begin{aligned} G(\bar{x}) &= F(S_1^{-1}(S_2(\bar{x}))) + 1 \text{ or equivalently} \\ G &= S_2 \circ S_1^{-1} \circ F + 1 \end{aligned}$$

holds.

First fix S_1 to a class representative and go (class per class) then we will explore two approaches:

- $S_2 = S_1$ implies $S = (S_1, x_{n+1} + F)$, next we vary F over all possible Boolean functions
- $S_2 \neq S_1$ the general case, next we vary S_2 over all possible S-boxes and F over all possible Boolean functions

Results of Theorem 1 first approach

Table: Extension of 3-bit S-box classes into 4-bit S-box classes

3-bit Class	4-bit Class		
$\mathcal{A}_0^3$	$\mathcal{A}_0^4$,	$\mathcal{C}_1^4$,	$\mathcal{Q}_4^4$
$\mathcal{Q}_1^3$	$\mathcal{C}_3^4$,	$\mathcal{Q}_4^4$,	$\mathcal{Q}_{294}^4$
$\mathcal{Q}_2^3$	$\mathcal{C}_{13}^4$,	$\mathcal{Q}_{12}^4$,	$\mathcal{Q}_{293}^4$
$\mathcal{Q}_3^3$	$\mathcal{C}_{301}^4$,	$\mathcal{Q}_{300}^4$	

▸ Table

$\mathcal{A}$ - Affine, $\mathcal{Q}$ - Quadratic, $\mathcal{C}$ - Cubic

- $\mathcal{Q}_{299}^4$ can't be obtained
- The extensions in blue were already known from [CHES2012]
- The obtained 4 cubic classes are the only 4 which have uniform sharing with 4 shares [CHES2012]

Results of Theorem 1 first approach

Table: Extension of non-cubic 4-bit S-box classes into 5-bit S-box classes

4-bit Class	5-bit Class
$\mathcal{A}_0^4$	$\mathcal{Q}_0^5, \mathcal{Q}_1^5, \mathcal{Q}_{14}^5$
$\mathcal{Q}_4^4$	$\mathcal{Q}_1^5, \mathcal{Q}_2^5, \mathcal{Q}_3^5, \mathcal{Q}_{15}^5, \mathcal{Q}_{18}^5$
$\mathcal{Q}_{12}^4$	$\mathcal{Q}_4^5, \mathcal{Q}_6^5, \mathcal{Q}_{13}^5, \mathcal{Q}_{17}^5, \mathcal{Q}_{20}^5, \mathcal{Q}_{21}^5$
$\mathcal{Q}_{293}^4$	$\mathcal{Q}_{13}^5, \mathcal{Q}_{24}^5, \mathcal{Q}_{31}^5$
$\mathcal{Q}_{294}^4$	$\mathcal{Q}_3^5, \mathcal{Q}_5^5, \mathcal{Q}_{12}^5, \mathcal{Q}_{16}^5, \mathcal{Q}_{19}^5, \mathcal{Q}_{23}^5$
$\mathcal{Q}_{299}^4$	$\mathcal{Q}_7^5, \mathcal{Q}_{22}^5$
$\mathcal{Q}_{300}^4$	$\mathcal{Q}_{30}^5, \mathcal{Q}_{32}^5$

▸ Table

- Constructed 23 out of 75 quadratic classes [FSE2017]
- $\mathcal{Q}_{30}^5, \mathcal{Q}_{32}^5$ no uniform sharing is known [FSE2017]
- Now we can obtain uniform sharing with 4 shares for them

Theorem 2

Given any $n \times n$ S-box S_1 which has a **uniform sharing** *with m shares and any Boolean function F with n variables which also has a* **uniform sharing** *with m shares.*
If S_2 is chosen in one of the $n+1$ forms:

$$S_1(\bar{x}), S_1(\bar{x} + \bar{1}_i) \text{ for } i = 1, ..., n$$

then the generated $(n+1) \times (n+1)$-bit S-box S by using Shannon's expansion with S_1, S_2 and F has also a **uniform sharing** *with m shares.*

Results of Theorem 1 second approach

This approach generates all S-boxes which can be obtained with this construction.

From 3-bit S-box classes we generated all the 4-bit classes except:

193	196	197	231	270	272	273	278	282	283	295
	G_7		G_{13}	G_4	G_6		G_5	G_3	G_{12}	G_{11}

Notice that 8 out of the 11 belong to Optimal Golden S-boxes. Recall there are exactly 8 classes of best 4-bit S-boxes. i.e., $\{Diff(S) = 4, Lin(S) = 8, deg = 3\}$ (Leander, Poschmann 2007)

Still work in progress!

Double application of Shannon's Expansion to S-boxes

Given four $n \times n$ S-boxes (permutations):

$$S_1(\bar{x}) = (t_1, t_2, \ldots, t_n), S_2(\bar{x}) = (u_1, u_2, \ldots, u_n),$$
$$S_3(\bar{x}) = (v_1, v_2, \ldots, v_n) \text{ and } S_4(\bar{x}) = (w_1, w_2, \ldots, w_n)$$

using Shannon's expansion one can get an $(n+2) \times (n+2)$ S-box $S(x_1, \ldots, x_n, x_{n+1}, x_{n+2}) = (y_1, \ldots, y_n, y_{n+1}, y_{n+2})$:

$$\begin{array}{lclcl} y_i & = & x_{n+2}[x_{n+1}t_i + (1+x_{n+1})u_i] & + & (1+x_{n+2})[x_{n+1}v_i + (1+x_{n+1})w_i] \\ y_{n+1} & = & x_{n+2}[x_{n+1}F_1(\bar{x}) + (1+x_{n+1})G_1(\bar{x})] & + & (1+x_{n+2})[x_{n+1}F_2(\bar{x}) + (1+x_{n+1})G_2(\bar{x})] \\ y_{n+2} & = & x_{n+2}[x_{n+1}F_3(\bar{x}) + (1+x_{n+1})G_3(\bar{x})] & + & (1+x_{n+2})[x_{n+1}F_4(\bar{x}) + (1+x_{n+1})G_4(\bar{x})] \end{array}$$

for $i = 1, \ldots, n$ and where F_j and G_j, $j = 1, 2, 3, 4$ are Boolean functions of n inputs.

Theorem 3

Let S be the S-box generated with the Shannon's expansion using four permutations S_1, S_2, S_3 and S_4. Then, S is a permutation if and only if both

$$
\begin{aligned}
F_1(S_1^{-1}(\bar{x})) &= G_2(S_4^{-1}(\bar{x})) + 1 = F_2(S_3^{-1}(\bar{x})) = G_1(S_2^{-1}(\bar{x})) + 1 \\
&\textit{and} \\
F_3(S_1^{-1}(\bar{x})) &= G_4(S_4^{-1}(\bar{x})) + 1 = F_4(S_3^{-1}(\bar{x})) + 1 = G_3(S_2^{-1}(\bar{x}))
\end{aligned}
$$

hold.

Conclusion

We have shown that Shannon's expansion can be used to construct uniform sharing for certain affine equivalent classes of S-boxes.

Our goal is to generate all 4-bit S-box classes from the 3-bit S-box classes. There are still some classes we cannot ...