An optimal universal construction of threshold implementation

Enrico Piccione

University of Bergen

Boolean Functions and their Applications (BFA)
September, 2023

Joint work between University of Bergen and KU Leuven.

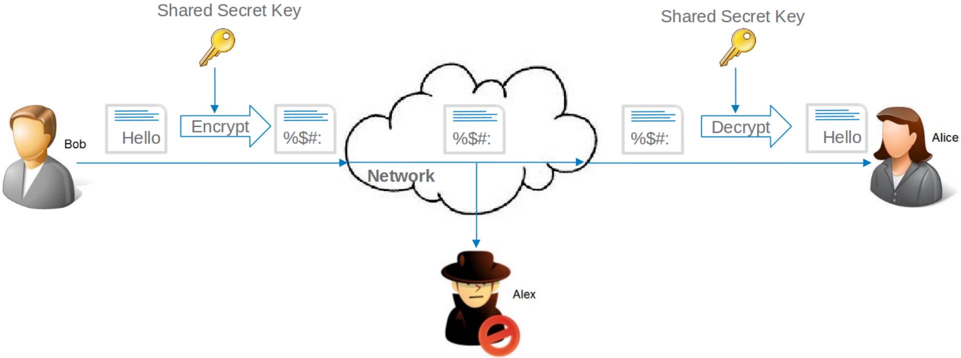
Enrico Piccione, Samuele Andreoli, Lilya Budaghyan, Claude Carlet, Siemen Dhooghe, Svetla Nikova, George Petrides, and Vincent Rijmen. "An Optimal Universal Construction for the Threshold Implementation of Bijective S-boxes". In: *IEEE Transactions on Information Theory* (2023)

Theorem

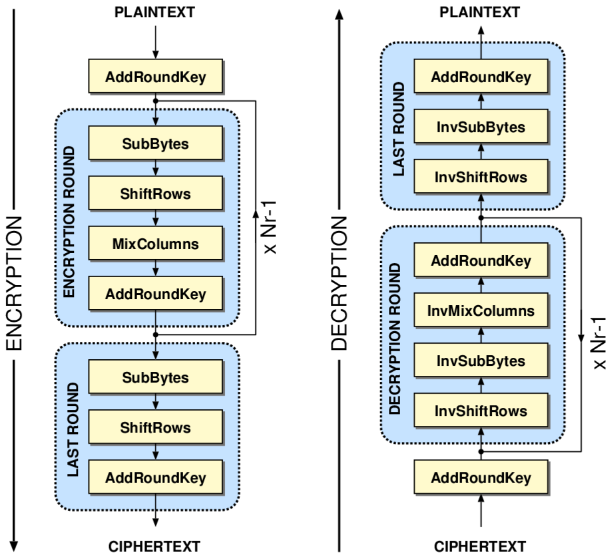
All bijective S-boxes admit a threshold implementation.

Introduction

Symmetric cryptography



Advanced Encryption Standard (AES)



Side-channel attacks

We consider passive attacks in hardware.

The attacker

- knows how the cryptographic algorithm is implemented
- has access to the physical device
- can measure the power consumption

So they can recover intermediate values during the encryption.

Boolean sharing: Take $(x_1, x_2)\ :\ x_1 + x_2 = x$.

Side-channel attacks

We consider passive attacks in hardware.

The attacker

- knows how the cryptographic algorithm is implemented
- has access to the physical device
- can measure the power consumption

So they can recover intermediate values during the encryption.

Boolean sharing: Take $(x_1, x_2)\ :\ x_1 + x_2 = x$.

Side-channel attacks

We consider passive attacks in hardware.

The attacker

- knows how the cryptographic algorithm is implemented
- has access to the physical device
- can measure the power consumption

So they can recover intermediate values during the encryption.

Boolean sharing: Take $(x_1, x_2) \, : \; x_1 + x_2 = x$.

Side-channel attacks

We consider passive attacks in hardware.

The attacker

- knows how the cryptographic algorithm is implemented
- has access to the physical device
- can measure the power consumption

So they can recover intermediate values during the encryption.

Boolean sharing: Take $(x_1, x_2) : x_1 + x_2 = x$.

Side-channel attacks

We consider passive attacks in hardware.

The attacker

- knows how the cryptographic algorithm is implemented
- has access to the physical device
- can measure the power consumption

So they can recover intermediate values during the encryption.

Boolean sharing: Take $(x_1, x_2) \; : \; x_1 + x_2 = x$.

Threshold Implementation

Svetla Nikova, Christian Rechberger, and Vincent Rijmen. “Threshold implementations against side-channel attacks and glitches”. In: *International conference on information and communications security*. Springer. 2006

Due to glitches, the attacker can read all the input values which flow to a wire until a register is reached.

A register stores the intermediate result until the active phase of the next clock cycle.

Computational search of threshold implementations

Begül Bilgin, Svetla Nikova, Ventzislav Nikov, Vincent Rijmen, and Georg Stütz. "Threshold implementations of all $3\times$ 3 and $4\times$ 4 S-boxes". In: *International workshop on cryptographic hardware and embedded systems*. Springer. 2012

Dušan Božilov, Begül Bilgin, and Hacı Ali Sahin. "A note on 5-bit quadratic permutations' classification". In: *IACR Transactions on Symmetric Cryptology* (2017)

Computational search of threshold implementations

Begül Bilgin, Svetla Nikova, Ventzislav Nikov, Vincent Rijmen, and Georg Stütz. "Threshold implementations of all 3× 3 and 4× 4 S-boxes". In: *International workshop on cryptographic hardware and embedded systems*. Springer. 2012

Dušan Božilov, Begül Bilgin, and Hacı Ali Sahin. "A note on 5-bit quadratic permutations' classification". In: *IACR Transactions on Symmetric Cryptology* (2017)

Decomposition of functions

Svetla Nikova, Ventzislav Nikov, and Vincent Rijmen. "Decomposition of permutations in a finite field". In: *Cryptography and Communications* (2019)

Instead of F, we implement $G_1, \ldots, G_\ell$ with

$$F = G_1 \circ \cdots \circ G_\ell.$$

- $G_1, \ldots, G_\ell$ with lower algebraic degree than F,
- ℓ is small.

Decomposition of functions

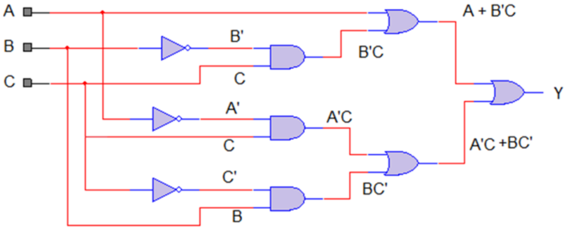
Svetla Nikova, Ventzislav Nikov, and Vincent Rijmen. "Decomposition of permutations in a finite field". In: *Cryptography and Communications* (2019)

Instead of F, we implement $G_1, \ldots, G_\ell$ with

$$F = G_1 \circ \cdots \circ G_\ell.$$

- $G_1, \ldots, G_\ell$ with lower algebraic degree than F,
- ℓ is small.

- **Area** the size of the physical circuit.
- **Latency** the number of cycles.
- **Randomness** the number of random generated bits.



First Uniform (by-design) implementation of the AES S-box

Table: Hardware cost of the masked AES S-box in the NANGATE 45nm library.

Design	Shares	Area [*kGE*]	Latency [*cc*]	Randomness [*bits*]
Piccione et al. 2023	9	166.37	1	0
Piccione et al. 2023	5	22.05	2	0
Wegener-Moradi 2018[1]	4	4.20	16	0
Sugawara 2019	3	3.50	4	0
Gross et al 2018	2	60.76	1	2 048
Gross et al. 2018	2	6.74	2	416

1. Wegener and Moradi wrote that without serialisation their design costs will be "more than 20 kGE".

Remark: $x^{254} = x^{26} \circ x^{49}$ over $\mathbb{F}_{2^8}$.

Preliminaries

Vectorial Boolean functions

$\mathbb{F}_{2^n}$ finite field of order 2^n.

$\mathbb{F}_2^n$ vector space over $\mathbb{F}_2$.

Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$

$$f(x_1, \dots, x_n) = \sum_{u \in \mathbb{F}_2^n} c(u) \prod_{i=1}^n x_i^{u_i}, \quad c(u) \in \mathbb{F}_2 \quad \text{(ANF)}$$

$d^\circ(f) = \deg(f)$ algebraic degree.

Vectorial Boolean function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$

$$F = (f_1, \dots, f_m)$$

$d^\circ(F) = \max_{i \in \{1,\dots,n\}} d^0(f_i)$ algebraic degree.

Vectorial Boolean functions

$\mathbb{F}_{2^n}$ finite field of order 2^n.

$\mathbb{F}_2^n$ vector space over $\mathbb{F}_2$.

Boolean function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$

$$f(x_1,\dots,x_n) = \sum_{u\in\mathbb{F}_2^n} c(u)\prod_{i=1}^n x_i^{u_i}, \quad c(u)\in\mathbb{F}_2 \quad \text{(ANF)}$$

$d^\circ(f) = \deg(f)$ algebraic degree.

Vectorial Boolean function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$

$$F = (f_1,\dots,f_m)$$

$d^\circ(F) = \max_{i\in\{1,\dots,n\}} d^0(f_i)$ algebraic degree.

Vectorial Boolean functions

$\mathbb{F}_{2^n}$ finite field of order 2^n.

$\mathbb{F}_2^n$ vector space over $\mathbb{F}_2$.

Boolean function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$

$$f(x_1, \ldots, x_n) = \sum_{u \in \mathbb{F}_2^n} c(u) \prod_{i=1}^n x_i^{u_i}, \quad c(u) \in \mathbb{F}_2 \quad \text{(ANF)}$$

$d^\circ(f) = \deg(f)$ algebraic degree.

Vectorial Boolean function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$

$$F = (f_1, \ldots, f_m)$$

$d^\circ(F) = \max_{i \in \{1,\ldots,n\}} d^0(f_i)$ algebraic degree.

Let $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$.

F is called balanced if $|F^{-1}(y)| = 2^{n-m}\ \forall y \in \mathbb{F}_2^m$.
A balanced function F with $m = n$ is also called a permutation over $\mathbb{F}_2^n$ (resp. $\mathbb{F}_{2^n}$).

If $m = n$, then F can be represented as

$$F(x) = \sum_{i=0}^{2^n-1} c_i x^i \in \mathbb{F}_{2^n}[x]$$

Then

$$d^\circ(F) = \max_{i\colon c_i \neq 0} \mathrm{w}_2(i)$$

Vectorial Boolean functions (part 2)

Let $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$.

F is called balanced if $|F^{-1}(y)| = 2^{n-m}\ \forall y \in \mathbb{F}_2^m$.
A balanced function F with $m = n$ is also called a permutation over $\mathbb{F}_2^n$ (resp. $\mathbb{F}_{2^n}$).

If $m = n$, then F can be represented as

$$F(x) = \sum_{i=0}^{2^n-1} c_i x^i \in \mathbb{F}_{2^n}[x]$$

Then

$$d^\circ(F) = \max_{i\colon c_i \neq 0} \mathrm{w}_2(i)$$

Multivariate functions

A vectorial Boolean function $\mathcal{F}\colon \mathbb{F}_2^{ns} \to \mathbb{F}_2^{ms'}$ can be represented as a function $(\mathbb{F}_2^n)^s \to (\mathbb{F}_2^m)^{s'}$

$$\mathcal{F}(x_1, \ldots, x_s) = (\mathcal{F}_1(x_1, \ldots, x_s), \ldots, \mathcal{F}_{s'}(x_1, \ldots, x_s)),$$

where $\mathcal{F}_1, \ldots, \mathcal{F}_{s'}\colon (\mathbb{F}_2^n)^s \to \mathbb{F}_2^m$.

If $n = m$, we can represent $\mathcal{F}_j$ as a function $\mathbb{F}_{2^n}^s \to \mathbb{F}_{2^n}$

$$\mathcal{F}_j(x_1, \ldots, x_s) = \sum_{u \in \{0,\ldots,2^n-1\}^s} c(u) \prod_{i=1}^{s} x_i^{u_i}, \ c(u) \in \mathbb{F}_{2^n}.$$

Multivariate functions

A vectorial Boolean function $\mathcal{F}\colon \mathbb{F}_2^{ns} \to \mathbb{F}_2^{ms'}$ can be represented as a function $(\mathbb{F}_2^n)^s \to (\mathbb{F}_2^m)^{s'}$

$$\mathcal{F}(x_1, \ldots, x_s) = (\mathcal{F}_1(x_1, \ldots, x_s), \ldots, \mathcal{F}_{s'}(x_1, \ldots, x_s)),$$

where $\mathcal{F}_1, \ldots, \mathcal{F}_{s'}\colon\ (\mathbb{F}_2^n)^s \to \mathbb{F}_2^m$.

If $n = m$, we can represent $\mathcal{F}_j$ as a function $\mathbb{F}_{2^n}^s \to \mathbb{F}_{2^n}$

$$\mathcal{F}_j(x_1, \ldots, x_s) = \sum_{u \in \{0,\ldots,2^n-1\}^s} c(u) \prod_{i=1}^{s} x_i^{u_i},\ \ c(u) \in \mathbb{F}_{2^n}.$$

Boolean sharing and secure hardware implementations

Boolean sharing is a well-established side-channel countermeasure.

Let $x \in \mathbb{F}_2^n$, then $\mathrm{Sh}_s(x)$ is the set of $\underline{x} = (x_1, \dots, x_s) \in (\mathbb{F}_2^n)^s \ : \ \sum_{i=1}^{s} x_i = x$.

$$x \mapsto F(x) = y$$

$$(x_1, \dots, x_s) = \underline{x} \mapsto \mathcal{F}(\underline{x}) = \underline{y} = (y_1, \dots, y_{s'})$$

$$\sum_{i=1}^{s} x_i = x, \quad \sum_{j=1}^{s} y_j = y$$

Let L be linear, $\mathcal{L}\colon (x_1, \dots, x_s) \mapsto (L(x_1), \dots, L(x_s))$ because $L\left(\sum_{i=1}^{s} x_i\right) = \sum_{i=1}^{s} L(x_i)$.

Boolean sharing and secure hardware implementations

Boolean sharing is a well-established side-channel countermeasure.

Let $x \in \mathbb{F}_2^n$, then $\mathrm{Sh}_s(x)$ is the set of $\underline{x} = (x_1, \ldots, x_s) \in (\mathbb{F}_2^n)^s \ : \ \sum_{i=1}^s x_i = x$.

$$x \mapsto F(x) = y$$

$$(x_1, \ldots, x_s) = \underline{x} \mapsto \mathcal{F}(\underline{x}) = \underline{y} = (y_1, \ldots, y_{s'})$$

$$\textstyle\sum_{i=1}^s x_i = x, \quad \sum_{j=1}^s y_j = y$$

Let L be linear, $\mathcal{L}\colon (x_1, \ldots, x_s) \mapsto (L(x_1), \ldots, L(x_s))$ because $L\left(\sum_{i=1}^s x_i\right) = \sum_{i=1}^s L(x_i)$.

Boolean sharing and secure hardware implementations

Boolean sharing is a well-established side-channel countermeasure.

Let $x \in \mathbb{F}_2^n$, then $\mathrm{Sh}_s(x)$ is the set of $\underline{x} = (x_1, \ldots, x_s) \in (\mathbb{F}_2^n)^s \; : \; \sum_{i=1}^s x_i = x$.

$$x \mapsto F(x) = y$$

$$(x_1, \ldots, x_s) = \underline{x} \mapsto \mathcal{F}(\underline{x}) = \underline{y} = (y_1, \ldots, y_{s'})$$

$$\textstyle\sum_{i=1}^s x_i = x, \quad \sum_{j=1}^s y_j = y$$

Let L be linear, $\mathcal{L}\colon (x_1, \ldots, x_s) \mapsto (L(x_1), \ldots, L(x_s))$ because $L\left(\sum_{i=1}^s x_i\right) = \sum_{i=1}^s L(x_i)$.

Threshold Implementation

Consequences of glitches

$x_1, x_2, x_3 \;:\; x_1 + x_2 + x_3 = x$

$$\begin{aligned} \mathcal{F}_1(x_1, x_2, x_3) &= y_1 \\ \mathcal{F}_2(x_1, x_2, x_3) &= y_2 \\ \mathcal{F}_3(x_1, x_2, x_3) &= y_3 \end{aligned}$$

(not secure)

$$\begin{aligned} \mathcal{F}_1(x_2, x_3) &= y_1 \\ \mathcal{F}_2(x_1, x_3) &= y_2 \\ \mathcal{F}_3(x_1, x_2) &= y_3 \end{aligned}$$

(secure)

Consequences of glitches

$x_1, x_2, x_3 \ : \ x_1 + x_2 + x_3 = x$

$$\begin{aligned} \color{red}{\mathcal{F}_1(x_1, x_2, x_3) = y_1} \\ \mathcal{F}_2(x_1, x_2, x_3) = y_2 \\ \mathcal{F}_3(x_1, x_2, x_3) = y_3 \end{aligned} \qquad \text{(not secure)}$$

$$\begin{aligned} \color{green}{\mathcal{F}_1(x_2, x_3) = y_1} \\ \mathcal{F}_2(x_1, x_3) = y_2 \\ \mathcal{F}_3(x_1, x_2) = y_3 \end{aligned} \qquad \text{(secure)}$$

A solution to glitches: the threshold implementation method

Definition

Let $\mathcal{F}\colon (\mathbb{F}_2^n)^s \to (\mathbb{F}_2^m)^{s'}$ and $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$.
We say that $\mathcal{F}$ is a Threshold Implementation (TI) of F if $\mathcal{F}$ is correct with respect to F, non-complete, and uniform.

In this talk, we concentrate on the case $m = n$ and $s' = s$.

$\mathcal{F}\colon (\mathbb{F}_2^n)^s \to (\mathbb{F}_2^n)^s$

$F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$

A solution to glitches: the threshold implementation method

Definition

Let $\mathcal{F}\colon (\mathbb{F}_2^n)^s \to (\mathbb{F}_2^m)^{s'}$ and $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$.
We say that $\mathcal{F}$ is a Threshold Implementation (TI) of F if $\mathcal{F}$ is correct with respect to F, non-complete, and uniform.

In this talk, we concentrate on the case $m = n$ and $s' = s$.

$\mathcal{F}\colon (\mathbb{F}_2^n)^s \to (\mathbb{F}_2^n)^s$

$F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$

Correctness

$$\mathrm{Sh}_s(x) := \left\{ (x_1, \ldots, x_s) \in (\mathbb{F}_2^n)^s \mid \sum_{i=1}^{s} x_i = x \right\}.$$

$\mathcal{F}$ is correct w.r.t. F if $\forall x \in \mathbb{F}_2^n$ and $\forall \underline{x} \in \mathrm{Sh}_s(x)$,

$$\mathcal{F}(\underline{x}) \in \mathrm{Sh}_s\left(F(x)\right).$$

Equivalently, if $\forall \underline{x} = (x_1, \ldots, x_s) \in (\mathbb{F}_2^n)^s$,

$$\sum_{j=1}^{s} \mathcal{F}_j(\underline{x}) = F\left(\sum_{i=1}^{s} x_i\right).$$

Correctness

$$\mathrm{Sh}_s(x) := \left\{ (x_1, \ldots, x_s) \in (\mathbb{F}_2^n)^s \mid \sum_{i=1}^{s} x_i = x \right\}.$$

$\mathcal{F}$ is correct w.r.t. F if $\forall x \in \mathbb{F}_2^n$ and $\forall \underline{x} \in \mathrm{Sh}_s(x)$,

$$\mathcal{F}(\underline{x}) \in \mathrm{Sh}_s\left(F(x)\right).$$

Equivalently, if $\forall \underline{x} = (x_1, \ldots, x_s) \in (\mathbb{F}_2^n)^s$,

$$\sum_{j=1}^{s} \mathcal{F}_j(\underline{x}) = F\left(\sum_{i=1}^{s} x_i\right).$$

Non-completeness

$\mathcal{F}$ is non-complete if $\forall j \in \{1, \ldots, s\}\ \exists i \in \{1, \ldots, s\} : \mathcal{F}_j$ is independent of its i-th input coordinate.

Equivalently, $\forall (x_1, \ldots, x_s) \in (\mathbb{F}_2^n)^s$ and $\forall a \in \mathbb{F}_2^n$,

$$\mathcal{F}_j(x_1, \ldots, x_s) = \mathcal{F}_j(x_1, \ldots, x_{i-1}, a, x_{i+1}, \ldots, x_s).$$

Proposition

Suppose that $\mathcal{F}$ is non-complete and correct w.r.t. F.
If F has algebraic degree t, then $s \geq t + 1$.

Non-completeness

$\mathcal{F}$ is non-complete if $\forall j \in \{1, \dots, s\}\ \exists i \in \{1, \dots, s\}\ :\ \mathcal{F}_j$ is independent of its i-th input coordinate.

Equivalently, $\forall (x_1, \dots, x_s) \in (\mathbb{F}_2^n)^s$ and $\forall a \in \mathbb{F}_2^n$,

$$\mathcal{F}_j(x_1, \dots, x_s) = \mathcal{F}_j(x_1, \dots, x_{i-1}, a, x_{i+1}, \dots, x_s).$$

Proposition

Suppose that $\mathcal{F}$ is non-complete and correct w.r.t. F.
If F has algebraic degree t, then $s \geq t + 1$.

Non-completeness

$\mathcal{F}$ is non-complete if $\forall j \in \{1, \dots, s\}\ \exists i \in \{1, \dots, s\} : \mathcal{F}_j$ is independent of its i-th input coordinate.

Equivalently, $\forall (x_1, \dots, x_s) \in (\mathbb{F}_2^n)^s$ and $\forall a \in \mathbb{F}_2^n$,

$$\mathcal{F}_j(x_1, \dots, x_s) = \mathcal{F}_j(x_1, \dots, x_{i-1}, a, x_{i+1}, \dots, x_s).$$

Proposition

Suppose that $\mathcal{F}$ is non-complete and correct w.r.t. F.
If F has algebraic degree t, then $s \geq t + 1$.

Uniformity

Let $\mathcal{F}$ be correct with respect to F.
$\mathcal{F}$ is uniform if $\forall x \in \mathbb{F}_2^n$ and $\forall \underline{y} \in \mathrm{Sh}_s(F(x))$ we have

$$\left|\{\underline{x} \in \mathrm{Sh}_s(x) \mid \mathcal{F}(\underline{x}) = \underline{y}\}\right| = 1.$$

Equivalently, if $\forall x \in \mathbb{F}_2^n$, the restriction $\mathcal{F}\colon \mathrm{Sh}_s(x) \to \mathrm{Sh}_s(F(x))$ is a balanced.

Proposition

Suppose that $\mathcal{F}$ is correct with respect to F.
Then $\mathcal{F}$ is a permutation if and only if $\mathcal{F}$ is uniform and F is a permutation.

Uniformity

Let $\mathcal{F}$ be correct with respect to F.
$\mathcal{F}$ is uniform if $\forall x \in \mathbb{F}_2^n$ and $\forall \underline{y} \in \mathrm{Sh}_s(F(x))$ we have

$$\left|\{\underline{x} \in \mathrm{Sh}_s(x) \mid \mathcal{F}(\underline{x}) = \underline{y}\}\right| = 1.$$

Equivalently, if $\forall x \in \mathbb{F}_2^n$, the restriction $\mathcal{F}\colon \mathrm{Sh}_s(x) \to \mathrm{Sh}_s(F(x))$ is a balanced.

Proposition

Suppose that $\mathcal{F}$ is correct with respect to F.
Then $\mathcal{F}$ is a permutation if and only if $\mathcal{F}$ is uniform and F is a permutation.

Let $\mathcal{F}$ be correct with respect to F.
$\mathcal{F}$ is uniform if $\forall x \in \mathbb{F}_2^n$ and $\forall \underline{y} \in \mathrm{Sh}_s(F(x))$ we have

$$\left|\{\underline{x} \in \mathrm{Sh}_s(x) \mid \mathcal{F}(\underline{x}) = \underline{y}\}\right| = 1.$$

Equivalently, if $\forall x \in \mathbb{F}_2^n$, the restriction $\mathcal{F}\colon \mathrm{Sh}_s(x) \to \mathrm{Sh}_s(F(x))$ is a balanced.

Proposition

Suppose that $\mathcal{F}$ is correct with respect to F.
Then $\mathcal{F}$ is a permutation if and only if $\mathcal{F}$ is uniform and F is a permutation.

Threshold Implementations of permutations

F is a permutation.

$\mathcal{F}$ is a threshold implementation of F with s shares.

- $s \geq t+1$ where t is the algebraic degree of F.
- **Correctness** $F(\sum_{i=1}^{s} x_i) = \sum_{j=1}^{s} \mathcal{F}_j(\underline{x})$
- **Non-completeness** $\forall i\ \exists j: \ \mathcal{F}_j(\underline{x})$ is independent of x_i
- **Uniformity** $\mathcal{F}$ is a permutation.

Threshold Implementations of permutations

F is a permutation.

$\mathcal{F}$ is a threshold implementation of F with s shares.

- $s \geq t + 1$ where t is the algebraic degree of F.
- **Correctness** $F(\sum_{i=1}^{s} x_i) = \sum_{j=1}^{s} \mathcal{F}_j(\underline{x})$
- **Non-completeness** $\forall i \; \exists j : \; \mathcal{F}_j(\underline{x})$ is independent of x_i
- **Uniformity** $\mathcal{F}$ is a permutation.

Threshold Implementations of permutations

F is a permutation.

$\mathcal{F}$ is a threshold implementation of F with s shares.

- $s \geq t + 1$ where t is the algebraic degree of F.
- **Correctness** $F(\sum_{i=1}^{s} x_i) = \sum_{j=1}^{s} \mathcal{F}_j(\underline{x})$
- **Non-completeness** $\forall i \ \exists j : \ \mathcal{F}_j(\underline{x})$ is independent of x_i
- **Uniformity** $\mathcal{F}$ is a permutation.

Threshold Implementations of permutations

F is a permutation.

$\mathcal{F}$ is a threshold implementation of F with s shares.

- $s \geq t + 1$ where t is the algebraic degree of F.
- **Correctness** $F(\sum_{i=1}^{s} x_i) = \sum_{j=1}^{s} \mathcal{F}_j(\underline{x})$
- **Non-completeness** $\forall i \; \exists j : \; \mathcal{F}_j(\underline{x})$ is independent of x_i
- **Uniformity** $\mathcal{F}$ is a permutation.

Computational investigation

Existence of threshold implementations up to affine equivalence

$$F' = A_1 \circ F \circ A_2$$

$$\mathcal{F}' = \mathcal{A}_1 \circ \mathcal{F} \circ \mathcal{A}_2$$

Let $L = A + A(0)$.

$$\mathcal{A}(x) = (L(x_1) + A(0), L(x_2), \ldots, L(x_s)).$$

Remark

The existence of a threshold implementation with s shares is an affine invariant.

Existence of threshold implementations up to affine equivalence

$$F' = A_1 \circ F \circ A_2$$

$$\mathcal{F}' = \mathcal{A}_1 \circ \mathcal{F} \circ \mathcal{A}_2$$

Let $L = A + A(0)$.

$$\mathcal{A}(x) = (L(x_1) + A(0), L(x_2), \ldots, L(x_s)).$$

Remark

The existence of a threshold implementation with s shares is an affine invariant.

The cube permutation

$F(x) = x^3$ over $\mathbb{F}_{2^n}$ with n odd.
F is a permutation since $\gcd(3, 2^n - 1) = 1$.
F has algebraic degree $t = 2$.

Theorem

$F(x) = x^3$ over $\mathbb{F}_{2^3}$ does not admit a threshold implementation with 3 shares.

So we investigated TIs with 4 shares.

Computational investigation on the cube permutation

Consider 4 shares $x_1, x_2, x_3, x_4 \in \mathbb{F}_{2^n}$.

$$(x_1 + x_2 + x_3 + x_4)^3 = \sum_{i,j \in \{1,2,3,4\}} x_i^2 x_j.$$

A simple algorithm:

1. Let $M = \{x_i^2 x_j : i, j \in \{1,2,3,4\}\}$. and let
$$\Phi = \left\{\phi \colon M \to \{1,2,3,4\} \mid \phi^{-1}(i) \text{ is non-complete } \forall i \in \{1,2,3,4\}\right\}.$$
2. Choose $\phi \in \Phi$ and $\Phi := \Phi \setminus \{\phi\}$.
3. Set $\mathcal{F} \colon (\mathbb{F}_{2^n})^4 \to (\mathbb{F}_{2^n})^4$ where $\mathcal{F}_i := 0$ for $i = 1,2,3,4$.
4. For each $m \in M$, $\mathcal{F}_i := \mathcal{F}_i + m$ where $i = \phi(m)$.
5. If $\mathcal{F}$ is a permutation, print $\mathcal{F}$.
6. If Φ is empty, then terminate. Otherwise, go back to 2.

Computational investigation on the cube permutation

Consider 4 shares $x_1, x_2, x_3, x_4 \in \mathbb{F}_{2^n}$.

$$(x_1 + x_2 + x_3 + x_4)^3 = \sum_{i,j \in \{1,2,3,4\}} x_i^2 x_j .$$

A simple algorithm:

1. Let $M = \{x_i^2 x_j : i,j \in \{1,2,3,4\}\}$. and let
$$\Phi = \left\{\phi \colon M \to \{1,2,3,4\} \mid \phi^{-1}(i) \text{ is non-complete } \forall i \in \{1,2,3,4\}\right\}.$$
2. Choose $\phi \in \Phi$ and $\Phi := \Phi \setminus \{\phi\}$.
3. Set $\mathcal{F} \colon (\mathbb{F}_{2^n})^4 \to (\mathbb{F}_{2^n})^4$ where $\mathcal{F}_i := 0$ for $i = 1,2,3,4$.
4. For each $m \in M$, $\mathcal{F}_i := \mathcal{F}_i + m$ where $i = \phi(m)$.
5. If $\mathcal{F}$ is a permutation, print $\mathcal{F}$.
6. If Φ is empty, then terminate. Otherwise, go back to 2.

Computational investigation on the cube permutation

Consider 4 shares $x_1, x_2, x_3, x_4 \in \mathbb{F}_{2^n}$.

$$(x_1 + x_2 + x_3 + x_4)^3 = \sum_{i,j \in \{1,2,3,4\}} x_i^2 x_j.$$

A simple algorithm:

1. Let $M = \{x_i^2 x_j : i, j \in \{1,2,3,4\}\}$. and let
$$\Phi = \left\{\phi \colon M \to \{1,2,3,4\} \mid \phi^{-1}(i) \text{ is non-complete } \forall i \in \{1,2,3,4\}\right\}.$$
2. Choose $\phi \in \Phi$ and $\Phi := \Phi \setminus \{\phi\}$.
3. Set $\mathcal{F} \colon (\mathbb{F}_{2^n})^4 \to (\mathbb{F}_{2^n})^4$ where $\mathcal{F}_i := 0$ for $i = 1, 2, 3, 4$.
4. For each $m \in M$, $\mathcal{F}_i := \mathcal{F}_i + m$ where $i = \phi(m)$.
5. If $\mathcal{F}$ is a permutation, print $\mathcal{F}$.
6. If Φ is empty, then terminate. Otherwise, go back to 2.

Computational investigation on the cube permutation

Consider 4 shares $x_1, x_2, x_3, x_4 \in \mathbb{F}_{2^n}$.

$$(x_1 + x_2 + x_3 + x_4)^3 = \sum_{i,j \in \{1,2,3,4\}} x_i^2 x_j.$$

A simple algorithm:

1. Let $M = \{x_i^2 x_j : i, j \in \{1,2,3,4\}\}$. and let
$$\Phi = \left\{\phi \colon M \to \{1,2,3,4\} \mid \phi^{-1}(i) \text{ is non-complete } \forall i \in \{1,2,3,4\}\right\}.$$
2. Choose $\phi \in \Phi$ and $\Phi := \Phi \setminus \{\phi\}$.
3. Set $\mathcal{F} \colon (\mathbb{F}_{2^n})^4 \to (\mathbb{F}_{2^n})^4$ where $\mathcal{F}_i := 0$ for $i = 1, 2, 3, 4$.
4. For each $m \in M$, $\mathcal{F}_i := \mathcal{F}_i + m$ where $i = \phi(m)$.
5. If $\mathcal{F}$ is a permutation, print $\mathcal{F}$.
6. If Φ is empty, then terminate. Otherwise, go back to 2.

Computational investigation on the cube permutation

Consider 4 shares $x_1, x_2, x_3, x_4 \in \mathbb{F}_{2^n}$.

$$(x_1 + x_2 + x_3 + x_4)^3 = \sum_{i,j \in \{1,2,3,4\}} x_i^2 x_j .$$

A simple algorithm:

1. Let $M = \{x_i^2 x_j : i, j \in \{1, 2, 3, 4\}\}$. and let
$$\Phi = \left\{\phi \colon M \to \{1, 2, 3, 4\} \mid \phi^{-1}(i) \text{ is non-complete } \forall i \in \{1, 2, 3, 4\}\right\} .$$
2. Choose $\phi \in \Phi$ and $\Phi := \Phi \setminus \{\phi\}$.
3. Set $\mathcal{F} \colon (\mathbb{F}_{2^n})^4 \to (\mathbb{F}_{2^n})^4$ where $\mathcal{F}_i := 0$ for $i = 1, 2, 3, 4$.
4. For each $m \in M$, $\mathcal{F}_i := \mathcal{F}_i + m$ where $i = \phi(m)$.
5. If $\mathcal{F}$ is a permutation, print $\mathcal{F}$.
6. If Φ is empty, then terminate. Otherwise, go back to 2.

$$\mathcal{F}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}^{\mathsf{T}} = \begin{pmatrix} x_1^3 \\ x_2^3 + x_2^2 x_3 + x_2^2 x_4 + x_2 x_3^2 + x_2 x_4^2 \\ x_4^3 + \sum_{i,j\in\{1,3,4\},\ i\neq j} x_i^2 x_j \\ x_3^3 + x_1^2 x_2 + x_1 x_2^2 \end{pmatrix}^{\mathsf{T}},$$

$$\mathcal{F}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}^{\mathsf{T}} = \begin{pmatrix} x_1^3 \\ (x_3 + x_4)^3 + (x_2 + x_3 + x_4)^3 \\ x_3^3 + x_1^3 + (x_1 + x_3 + x_4)^3 \\ x_3^3 + (x_1 + x_2)^3 + x_1^3 + x_2^3 \end{pmatrix}^{\mathsf{T}},$$

$$\mathcal{F}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}^{\mathsf{T}} = \begin{pmatrix} F(x_1) \\ F(x_3 + x_4) + F(x_2 + x_3 + x_4) \\ F(x_3) + F(x_1) + F(x_1 + x_3 + x_4) \\ F(x_3) + F(x_1 + x_2) + F(x_1) + F(x_2) \end{pmatrix}^{\mathsf{T}}.$$

Results and generalization

$$\mathcal{F}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}^{\mathsf{T}} = \begin{pmatrix} x_1^3 \\ x_2^3 + x_2^2 x_3 + x_2^2 x_4 + x_2 x_3^2 + x_2 x_4^2 \\ x_4^3 + \sum_{i,j \in \{1,3,4\},\, i \neq j} x_i^2 x_j \\ x_3^3 + x_1^2 x_2 + x_1 x_2^2 \end{pmatrix}^{\mathsf{T}},$$

$$\mathcal{F}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}^{\mathsf{T}} = \begin{pmatrix} x_1^3 \\ (x_3 + x_4)^3 + (x_2 + x_3 + x_4)^3 \\ x_3^3 + x_1^3 + (x_1 + x_3 + x_4)^3 \\ x_3^3 + (x_1 + x_2)^3 + x_1^3 + x_2^3 \end{pmatrix}^{\mathsf{T}},$$

$$\mathcal{F}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}^{\mathsf{T}} = \begin{pmatrix} F(x_1) \\ F(x_3 + x_4) + F(x_2 + x_3 + x_4) \\ F(x_3) + F(x_1) + F(x_1 + x_3 + x_4) \\ F(x_3) + F(x_1 + x_2) + F(x_1) + F(x_2) \end{pmatrix}^{\mathsf{T}}.$$

$$\mathcal{F}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}^{\mathsf{T}} = \begin{pmatrix} x_1^3 \\ x_2^3 + x_2^2 x_3 + x_2^2 x_4 + x_2 x_3^2 + x_2 x_4^2 \\ x_4^3 + \sum_{i,j\in\{1,3,4\},\, i\neq j} x_i^2 x_j \\ x_3^3 + x_1^2 x_2 + x_1 x_2^2 \end{pmatrix}^{\mathsf{T}},$$

$$\mathcal{F}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}^{\mathsf{T}} = \begin{pmatrix} x_1^3 \\ (x_3 + x_4)^3 + (x_2 + x_3 + x_4)^3 \\ x_3^3 + x_1^3 + (x_1 + x_3 + x_4)^3 \\ x_3^3 + (x_1 + x_2)^3 + x_1^3 + x_2^3 \end{pmatrix}^{\mathsf{T}},$$

$$\mathcal{F}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}^{\mathsf{T}} = \begin{pmatrix} F(x_1) \\ F(x_3 + x_4) + F(x_2 + x_3 + x_4) \\ F(x_3) + F(x_1) + F(x_1 + x_3 + x_4) \\ F(x_3) + F(x_1 + x_2) + F(x_1) + F(x_2) \end{pmatrix}^{\mathsf{T}}.$$

Observations for $t = 3$

We tried to replicate for $t = 3$.
We investigated $F(x) = x^7$ over $\mathbb{F}_{2^4}$.

There is no known TIs with $t + 1 = 4$ shares for F (but no non-existence result).
So we investigated 5 shares.

Problems:

- The domain of $\mathcal{F}$ is minimum $(\mathbb{F}_{2^4})^5$.
- The pattern for $t = 2$ is misleading.

Observations for $t = 3$

We tried to replicate for $t = 3$.
We investigated $F(x) = x^7$ over $\mathbb{F}_{2^4}$.

There is no known TIs with $t + 1 = 4$ shares for F (but no non-existence result).
So we investigated 5 shares.

Problems:

- The domain of $\mathcal{F}$ is minimum $(\mathbb{F}_{2^4})^5$.
- The pattern for $t = 2$ is misleading.

Observations for $t = 3$

We tried to replicate for $t = 3$.
We investigated $F(x) = x^7$ over $\mathbb{F}_{2^4}$.

There is no known TIs with $t + 1 = 4$ shares for F (but no non-existence result).
So we investigated 5 shares.

Problems:

- The domain of $\mathcal{F}$ is minimum $(\mathbb{F}_{2^4})^5$.
- The pattern for $t = 2$ is misleading.

Construction

Functions of algebraic degree t

F is affine $(t = 1)$

$$F(x_1 + x_2) + F(x_1) + F(x_2) + F(0) = 0$$

F is quadratic $(t = 2)$

$$F(x_1 + x_2 + x_3) + F(x_1 + x_2) + F(x_1 + x_3) + F(x_2 + x_3) + F(x_1) + F(x_2) + F(0) = 0$$

Lemma

$$F \text{ of algebraic degree } t \implies \sum_{I \subseteq \{1,\dots,t\}} F\left(\sum_{i \in I} x_i\right) = 0.$$

Functions of algebraic degree t

$$F \text{ is affine } (t = 1)$$
$$F(x_1 + x_2) + F(x_1) + F(x_2) + F(0) = 0$$

$$F \text{ is quadratic } (t = 2)$$
$$F(x_1 + x_2 + x_3) + F(x_1 + x_2) + F(x_1 + x_3) + F(x_2 + x_3) + F(x_1) + F(x_2) + F(0) = 0$$

Lemma

$$F \text{ of algebraic degree } t \implies \sum_{I \subseteq \{1,\dots,t\}} F\left(\sum_{i \in I} x_i\right) = 0.$$

Functions of algebraic degree t

$$F \text{ is affine } (t=1)$$
$$F(x_1+x_2)+F(x_1)+F(x_2)+F(0)=0$$

$$F \text{ is quadratic } (t=2)$$
$$F(x_1+x_2+x_3)+F(x_1+x_2)+F(x_1+x_3)+F(x_2+x_3)+F(x_1)+F(x_2)+F(0)=0$$

Lemma

$$F \textit{ of algebraic degree } t \implies \sum_{I\subseteq\{1,\dots,t\}} F\left(\sum_{i\in I} x_i\right)=0.$$

Algebraic decomposition (Carlet et al. 2015)

Lemma

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ *be of algebraic degree at most* $t \geq 1$ *and let* $s > t$*.*
Then for every $x_1, x_2, \ldots, x_s \in \mathbb{F}_2^n$ *we have that*

$$F\left(\sum_{i=1}^{s} x_i\right) = \sum_{j=0}^{t} \mu_{s,t}(j) \sum_{I \in \mathcal{P}_s,\, |I|=j} F\left(\sum_{i \in I} x_i\right)$$

where $\mu_{s,t}(j) = \binom{s-j-1}{t-j} \mod 2$ *for every* $j = 0, \ldots, t$ *(with the convention that* $\binom{0}{0} = 1$*).*

We recall that $\mathcal{F}$ is correct w.r.t. F if

$$F\left(\sum_{i=1}^{s} x_i\right) = \sum_{j=1}^{s} \mathcal{F}_j(\underline{x}).$$

Algebraic decomposition (Carlet et al. 2015)

Lemma

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ *be of algebraic degree at most* $t \geq 1$ *and let* $s > t$*.*
Then for every $x_1, x_2, \ldots, x_s \in \mathbb{F}_2^n$ *we have that*

$$F\left(\sum_{i=1}^{s} x_i\right) = \sum_{j=0}^{t} \mu_{s,t}(j) \sum_{I \in \mathcal{P}_s,\, |I|=j} F\left(\sum_{i \in I} x_i\right)$$

where $\mu_{s,t}(j) = \binom{s-j-1}{t-j} \mod 2$ *for every* $j = 0, \ldots, t$ *(with the convention that* $\binom{0}{0} = 1$*).*

We recall that $\mathcal{F}$ is correct w.r.t. F if

$$F\left(\sum_{i=1}^{s} x_i\right) = \sum_{j=1}^{s} \mathcal{F}_j(\underline{x}).$$

The universal optimal construction

Notation: $\mathcal{P}_k = \{I \mid I \subseteq \{1,\ldots,k\}\}$ and $\sum_{i\in\emptyset} x_i = 0$.
Let F be a permutation over $\mathbb{F}_2^n$ with algebraic degree $t \geq 2$.
Then $\mathcal{F}$ defined as

$$\mathcal{F}_1(\underline{x}) = x_1$$

$$\mathcal{F}_2(\underline{x}) = \sum_{i=3}^{t+2} x_i + F\left(\sum_{i=2}^{t+2} x_i\right)$$

$$\mathcal{F}_j(\underline{x}) = x_j + \sum_{I\in\mathcal{P}_{j-2}} F\left(\sum_{i\in I} x_i + \sum_{i=j}^{t+2} x_i\right), \quad j = 3,\ldots,t+1$$

$$\mathcal{F}_{t+2}(\underline{x}) = x_{t+2} + x_1 + \sum_{I\in\mathcal{P}_t} F\left(\sum_{i\in I} x_i\right)$$

is a threshold implementation of F.

Proving the correctness property

Let t be the algebraic degree of F.

Proposition

$$F\left(\sum_{i=1}^{t+2} x_i\right) = F\left(\sum_{i=2}^{t+2} x_i\right) + \sum_{j=3}^{t+1} \sum_{I\in\mathcal{P}_{j-2}} F\left(\sum_{i\in I} x_i + \sum_{i=j}^{t+2} x_i\right) + \sum_{I\in\mathcal{P}_t} F\left(\sum_{i\in I} x_i\right).$$

Proving the uniformity property

Let F be a permutation over $\mathbb{F}_2^n$ with algebraic degree $t \geq 2$.

Lemma

$\mathcal{F}$ is uniform if and only if $\mathcal{F}$ is a permutation.

The system defined by

$$\mathcal{F}(\underline{x}) = \underline{y}$$

can be solved like a triangular system by using the equation

$$\sum_{i=1}^{s} x_i = F^{-1}\left(\sum_{i=1}^{s} y_i\right).$$

Proving the uniformity property

Let F be a permutation over $\mathbb{F}_2^n$ with algebraic degree $t \geq 2$.

Lemma

$\mathcal{F}$ is uniform if and only if $\mathcal{F}$ is a permutation.

The system defined by

$$\mathcal{F}(\underline{x}) = \underline{y}$$

can be solved like a triangular system by using the equation

$$\sum_{i=1}^{s} x_i = F^{-1}\left(\sum_{i=1}^{s} y_i\right).$$

On the existence of threshold implementations with t+1 shares

Reaching $t + 1$ shares (Bilgin et al. 2012, Božilov et al. 2017)

size	degree	3 shares	4 shares	5 shares
3	2	2	1	
4	2	5	1	
	3	-	4	291
5	2	30	45	

Two known infinite constructions with $t+1$ shares

Feistel permutations[Boss et al. 2017] Let $F\colon \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^n \times \mathbb{F}_2^n$ be defined as

$$F(x, y) = (x, y + G(x)).$$

Let $\mathcal{G}\colon (\mathbb{F}_2^n)^{t+1} \to (\mathbb{F}_2^n)^{t+1}$ be non-complete and correct with respect to G.
Then

$$\mathcal{F}(\underline{x}, \underline{y}) = (\underline{x}, \underline{y} + \mathcal{G}(\underline{x})).$$

is a TI of F with $t+1$ shares.

Going upward in dimension[Varici et al. 2019]: They construct new $(n+1)$-bit and $(n+2)$-bit bijective S-boxes from F.
If F admits a TI with $t+1$ shares, then also those functions admit a TI with $t+1$ shares.

Two known infinite constructions with $t+1$ shares

Feistel permutations[Boss et al. 2017] Let $F\colon \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^n \times \mathbb{F}_2^n$ be defined as

$$F(x,y) = (x, y + G(x)).$$

Let $\mathcal{G}\colon (\mathbb{F}_2^n)^{t+1} \to (\mathbb{F}_2^n)^{t+1}$ be non-complete and correct with respect to G.
Then

$$\mathcal{F}(\underline{x},\underline{y}) = (\underline{x}, \underline{y} + \mathcal{G}(\underline{x})).$$

is a TI of F with $t+1$ shares.

Going upward in dimension[Varici et al. 2019]: They construct new $(n+1)$-bit and $(n+2)$-bit bijective S-boxes from F.
If F admits a TI with $t+1$ shares, then also those functions admit a TI with $t+1$ shares.

Conjectures on the existence of TIs with t+1 shares

Conjecture

No power permutation of algebraic degree $t \geq 2$ admits a threshold implementation with $t+1$ shares.

Conjecture

No APN permutation of algebraic degree t admits a threshold implementation with $t+1$ shares.

Conclusions

What we achieved:

- Low latency implementations with no additional randomness
- Every permutation has a $t + 2$ share TI

What we can do next:

- Which permutations do not admit a TI with $t + 1$ shares?
- Can we do $t + 1$ shares constructions for interesting classes of permutations?

Thanks for your attention!