Squeezing a vectorial nonlinear binary transformation between the generator and parity check matrices of a linear code

The 4^{th} International Workshop
on **B**oolean **F**unctions and their **A**pplications
BFA 2019

Joint work with Daniel Panario

Parameter notations

1. n : word size,
2. N : number of words,
3. N_i : number of input words for non-linear part, $N_i < N$,
4. N_o : number of input words for non-linear part, $N_o < N$,
5. $\frac{N}{N_i} \in \mathbb{Q}$: the compression/contraction factor,
6. $\frac{N}{N_o} \in \mathbb{Q}$: the decompression/expansion factor.

Permutation definition

For $V = \mathbb{F}_2^n$, consider $F : V^N \to V^N$ defined by :

$$F_k(x) = T\big(x + B\big(f_k\big(A(x)\big)\big)\big), \tag{1}$$

where

1. $k \in K$, and K is the keyspace with $\dim_{\mathbb{F}_2} K \geq Nn$,
2. $f_k : V^{N_i} \mapsto V^{N_o}$ is a nonlinear function,
3. T, an invertible matrix of size $N \times N$ over V,
4. A, a full rank matrix of size $N_i \times N$ over V,
5. B, a full rand matrix of size $N_o \times N$ over V,

such that

$$AB^t = 0 \quad (\textit{perpendicularity}).$$

Overview of results

1. F is invertible even if f is not invertible.
2. Differential and linear cryptanalysis of F reduces to those of f.
3. $\max\left\{\frac{N}{N_o}, \frac{N}{N_i}\right\}$ is the minimal number of rounds to prevent both differential and linear attacks up to a certain threshold (to be specified later), and assuming independent keys across rounds.

LEMMA (L1)

The perpendicularity criterion is equivalent to the invertibility of F even though f may not be invertible.

Proof overview of Lemma L1: Let $y = F(x)$ so that $T^{-1}y = x + B^{\mathrm{t}} f(Ax)$. $AB^{\mathrm{t}} = 0$ implies $AT^{-1}y = Ax$. Thus

$$\begin{aligned} x &= T^{-1}y + B^{\mathrm{t}} f(Ax) \\ &= T^{-1}y + B^{\mathrm{t}} f(AT^{-1}y). \end{aligned}$$

The inverse of F is

$$G(y) = T^{-1}y + B^{\mathrm{t}} f(AT^{-1}y),$$

Since the characteristic of the underlying field is two, $(G \circ F)(x) = (F \circ G)(x) = x$.

DEFINITION (DIFFERENCE TABLE–DT)

Given a vectorial boolean function $g : \mathbb{F}_2^d \to \mathbb{F}_2^d$ for some d, and a pair $(u, v) \in \mathbb{F}_2^d \times \mathbb{F}_2^d$, we denote the entries of the difference table (hereafter DT) of g by $\delta_g(u, v)$ where

$$\delta_g(u, v) = \frac{1}{2^d} \sum_{x \in \mathbb{F}_2^d} \mathbb{1}\{g(x + u) + g(x) = v\},$$

where $\mathbb{1}$ denotes the indicator function.

DEFINITION (LINEAR APPROXIMATION TABLE–LAT)

Given a vectorial boolean function $g : \mathbb{F}_2^d \to \mathbb{F}_2^d$ for some d, and a pair $(u, v) \in \mathbb{F}_2^d \times \mathbb{F}_2^d$, we denote the entries of the linear approximation table (hereafter LAT) of g by $\lambda_g(u, v)$ where

$$\lambda_g(u, v) = \frac{1}{2^d} \sum_{x \in \mathbb{F}_2^d} (-1)^{(v \cdot g(x) + u \cdot x)},$$

Theorem (T1)

Knowledge of the DT/LAT of f implies complete knowledge of the DT/LAT of F. We have that

$$\delta_F(\alpha,\beta) = \begin{cases} \delta_f(A\alpha, R_B^t(\alpha + T^{-1}\beta)) & \text{if } \alpha + T^{-1}\beta \in rowsp(B), \\ 0 & \text{otherwise,} \end{cases}$$

where R_B is the right inverse of B, i.e., BR_B is the identity matrix of size $N_o \times N_o$ over V, and R_B is of size $N \times N_o$ over V. Similarly we have that

$$\lambda_F(\alpha,\beta) = \begin{cases} \lambda_f\big(R_A\big(\alpha + T^t\beta\big), B^tT^t\beta\big) & \text{if } \alpha + T^t\beta \in rowsp(A), \\ 0 & \text{otherwise,} \end{cases}$$

where R_A is the right inverse of A, i.e., AR_A is the identity matrix of size $N_i \times N_i$ over V, and R_A is of size $N \times N_i$ over V.

By definition,

$$\delta_F(\alpha, \beta) = \frac{1}{2^{nN}} \sum_{x \in V^N} \mathbb{1}\{F(x+\alpha) + F(x) = \beta\}.$$

Suppose $F(x+\alpha) + F(x) = \beta$, then

$$\begin{aligned} \beta &= F(x+\alpha) + F(x) \\ &= T\alpha + TB^{\mathrm{t}}\big(f(Ax + A\alpha) + f(Ax)\big), \\ &\Updownarrow \\ \alpha + T^{-1}\beta &= B^{\mathrm{t}}\big(f(Ax + A\alpha) + f(Ax)\big). \end{aligned}$$

Using the right inverse R_B,

$$\begin{aligned} \delta_F(\alpha, \beta) &= \frac{1}{2^{nN}} \sum_{x \in V^N} \mathbb{1}\{F(x+\alpha) + F(x) = \beta\} \\ &= \frac{1}{2^{nN_i}} \sum_{u \in V^{N_i}} \mathbb{1}\{f(u+a) + f(u) = b\}, \end{aligned}$$

Some additional notation

1. ℓ is the number of iterations or rounds
2. $x \in V^N$ is an arbitrary input
3. $k = (k_0, \ldots, k_{\ell-1}) \in K^\ell$ is an independent and identically distributed sequence of keys from the uniform distribution.

Note that the values of x and k defined the sequence

$$x \to F_{k_0}(x) \to \left(F_{k_1} \circ F_{k_0}\right)(x) \to \cdots \to \left(F_{k_{\ell-1}} \circ \cdots \circ F_{k_0}\right)(x).$$

Non-trivial step definition

For arbitrarily chosen α and, possibly arbitrarily chosen β, consider the random sequence $(\alpha_i)_{i=0}^{\ell}$ with $\alpha_0 = \alpha$, $\alpha_\ell = \beta$ and that satisfies for $0 \leq i < \ell$ either

$$\alpha_{i+1} = F_{k_i} \circ \cdots \circ F_{k_1}(x + \alpha_i) + F_{k_i} \circ \cdots \circ F_{k_1}(x)$$

or

$$0 = \alpha_{i+1} \cdot F_{k_i} \circ \cdots \circ F_{k_1}(x) + \alpha_i \cdot x.$$

Definition (Non-trivial step)

A step (α_i, α_{i+1}) is non-trivial if $\delta_{F_k}(\alpha_i, \alpha_{i+1}) = 0$ and $\delta_{f_k}(\alpha_i, \alpha_{i+1}) \neq 0$.

Definition (Non-trivial walk)

A walk $\alpha = \alpha_0 \to \cdots \to \alpha_i \to \alpha_n = \beta$ is non-trivial if it contains a non-trivial step.

Sequences for which $\prod_{i=0}^{\ell-1} \delta_{F_{k_i}}(\alpha_i, \alpha_{i+1})$ or $|\prod_{i=0}^{\ell-1} \lambda_{F_{k_i}}(\alpha_i, \alpha_{i+1})|$ are high are of interest for an attacker.

If $\alpha_i + T^{-1}\alpha_{i+1} \notin \mathrm{rowsp}(B)$ or $\alpha_i + T^t\alpha_{i+1} \notin \mathrm{rowsp}(A)$, then a walk on the space of differentials has probability 0, or a walk in the space of correlations has probability 0, respectively.

With

$$\delta = \max_{(k,\alpha,\beta)} \delta_{f_k}(\alpha,\beta),$$

$$\lambda = \max_{(k,\alpha,\beta)} \lambda_{f_k}(\alpha,\beta).$$

THEOREM (T2)

Let $\ell^\star = \max\left\{\frac{N}{N_i}, \frac{N}{N_o}\right\} \in \mathbb{Q}$. If the number $\ell > 0$ of iterations is such that $\ell \geq \ell^\star$, then

$$\prod_{i=0}^{\ell-1} \delta_F(\alpha_i, \alpha_{i+1}) \leq \delta^{\ell^\star} \quad \textit{and} \quad \left|\prod_{i=0}^{\ell-1} \lambda_{F_{k_i}}(\alpha_i, \alpha_{i+1})\right| \leq \lambda^{\ell^\star}.$$

Briefly it goes like this:

The matrix B is full rank so $\dim \ker(B) = nN - nN_o$, and $\operatorname{codim} \ker(B) = nN_o$.

The subadditivity of codim for subspaces of a vector space implies that

$$nN = \operatorname{codim}\{0\} = \operatorname{codim}\left(\bigcap_{j=0}^{\ell_w - 1} \left(T^{-j}\right)^{\mathrm{t}} \ker B\right)$$
$$\leq \sum_{j=0}^{\ell_w - 1} \operatorname{codim}\left(\left(T^{-j}\right)^{\mathrm{t}} \ker B\right) = \sum_{j=0}^{\ell_w - 1} nN_o = (nN_o)\ell_w.$$

An example–A Generalized Feistel

Referring to Hoang and Rogaway (2018), for one round of Type-1 Feistel:

1. $V = \mathbb{F}_2^n$, $\mathbf{I}$ and $\mathbf{0}$ are respectively the $n \times n$ identity and zero matrices,
2. the 4-tuple input (x_1, x_2, x_3, x_4) with $x_i \in V$, and non-linear part f such that $f : V \to V$.

The template matrices :

$$A = \begin{pmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{pmatrix},$$
$$B = \begin{pmatrix} \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} \end{pmatrix},$$
$$T = \begin{pmatrix} \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{pmatrix}.$$