On Reducing Annihilation Degree inside Nonlinear Invariant Attacks on T-310 and DES

Nicolas T. Courtois, Matteo Abbondati and Aidan Patrick

Central European Conference on Cryptology 2020

Outline

- Construction of product invariant attacks from cycles (paper ICISC 2019)
- Normality and weak normality
- Direct sums with disjoint sets of variables
- Magic polynomials μ
- Spectral equation for annihilation of a direct sum

Ring of Invariants

A block cipher operating on states of N-bits is defined by a Group of key-dependent bijective transformations $\{\varphi_k\}_{k\in K}$

We have a Group action of $G = \{\varphi_k\}_{k\in K}$ on the Ring of Boolean polynomials in N variables

$$P^{\varphi_k}(x_1, \dots, x_N) := P(\varphi_k(x_1, \dots, x_n))$$

Definition

P is an invariant for the block cipher for a given subset of keys $\sum \subseteq K$

$$\updownarrow$$

$$P^{\varphi_k}(x_1, \dots, x_N) = P(x_1, \dots, x_N)\ \ \forall k \in \sum, \forall\ (x_1, \dots, x_N) \in {\mathbb{F}_2}^N$$

Trivial cases

The polynomials 0 and 1 are invariants for any key

Theorem

For any Block cipher and for any given subset of keys $\sum \subseteq K$, the set of invariants holding with probability 1.0 is a ring

Question: Is this ring always trivial? How to construct non trivial invariants?

Non trivial invariants are very hard to find in general, even for a single key.

Example

For $N = 3$, consider the transformation

$$\varphi_k : \mathbb{F}_2{}^3 \longrightarrow \mathbb{F}_2{}^3$$
$$(x_1, x_2, x_3) \mapsto (x_1x_2, kx_3, x_1{+}x_2x_3)$$

A Boolean polynomial P in 3 variables is then an invariant for this transformation φ_k i.f.f. for every input $(x_1, x_2, x_3) \in \mathbb{F}_2{}^3$ it satisfies:

$$P(x_1, x_2, x_3) = P^{\varphi}(x_1, x_2, x_3) = P(x_1x_2, kx_3, x_1{+}x_2x_3)$$

$$(P{=}x_1{+}x_2{+}x_3 \;\rightarrow\; P^{\varphi}{=}x_1x_2{+}\mathrm{k}x_3{+}x_1{+}x_2x_3)$$

It seems almost impossible even for this extremely simple case with just 3 variables and with only 1 parameter family of transformations not excessively complicated!!!

Much harder case

In block cipher cryptanalysis we consider many variables ($N \geq 36$) and transformations with key-dependent nonlinear Boolean polynomials on 6 variables

Impossible problem:

Finding P by brute force is impossible: 2^{2^N} Boolean polynomials in N variables to test

Not efficiently falsifiable:

A block cipher has no polynomial invariant P

From Diophantine equations' theory

- Pell-Fermat equation

$$x^2 - \mathrm{d}y^2 = 1$$

It "seems" efficiently falsifiable by testing non-solvability $(mod\ p)$ for different values of p

Brute force like "repeated game"

Self-similarity and Invariance for a simple case (d=2)

$P = x^2 - 2y^2$ is invariant with respect to the linear transformation

$$\varphi(x,y) = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

$P^{\varphi}(\mathrm{x},\mathrm{y})$=$P(3x+4y, 2x+3y)$=$(3x+4y)^2-2(2x+3y)^2$=
=$9x^2$+$24xy$+$16y^2$-$8x^2$-$24xy$-$18y^2$= $x^2 - 2y^2$

How to find non trivial invariants with respect to (more than just one) nonlinear transformations and with high number of variables??

From ICISC 2019…

- Nicolas Courtois, Matteo Abbondati, Hamy Ratoanina, and Marek Grajek **Systematic** Construction of Nonlinear Product Attacks on Block Ciphers, In ICISC, LNCS 11975, pp 20-51, Springer, 2020.

- General theorem applicable to any Block Cipher
- When P is a product of polynomials
- One or several closed cycles of linear transitions can define a non trivial product invariant

From ICISC 2019…

- Nicolas Courtois, Matteo Abbondati, Hamy Ratoanina, and Marek Grajek **Systematic** Construction of Nonlinear Product Attacks on Block Ciphers, In ICISC, LNCS 11975, pp 20-51, Springer, 2020.

- General theorem applicable to any Block Cipher
- When P is a product of polynomials
- One or several closed cycles of linear transitions can define a non trivial product invariant

Notation for transitions:

$P \leftarrow Q$ means that $P^{\varphi}(x_1, \dots, x_N) = \mathrm{Q}(x_1, \dots, x_N)$

From ICISC 2019…

Theorem:

Given a set of basic polynomials $\{Q_j\}$ in a closed loop of length n, s.t. (due to internal connections of the cipher) we have the transitions:

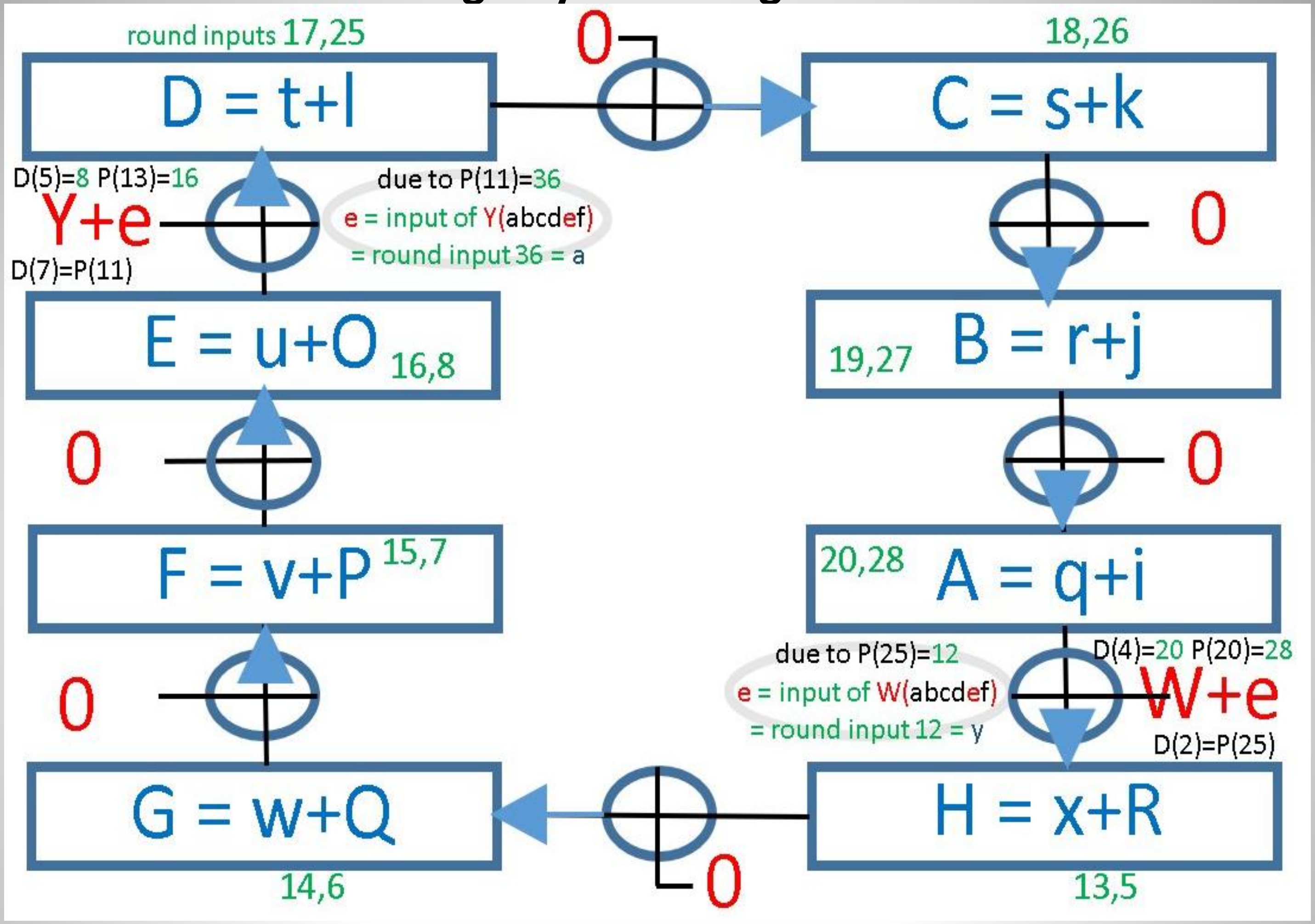
$$Q_{\pi(j)} \leftarrow Q_j + Z_j$$

Where $\pi = (1\ 2\ \ldots\ n) \in S_n$. And we assume that:

- $\exists j$ s.t. $Z_j = 0$ (corresponding Q_j is said to be transformable)
- $\forall j\ \prod_{k,\,transf.} Q_k Z_j = 0$

Then $P = \prod_j Q_j$ is an invariant for our cipher holding with probability 1, for any secret key, for any initial state on n bits and for any number of rounds.

An attack using a cycle of length 8 for T-310



Y+e and W+e are annihilated by the product of suitable transformable polynomials, which are B,C,D,F,G,H.

In particular:

- FG(W+e)= 0
- BC(Y+e)= 0

Strengths of our algebraic construction:

- High level of generality to any block cipher
- High freedom for the attacker in the construction of simple transitions defining complex product attacks
- Our ring is not empty, other invariants may exists

Strengths of our algebraic construction:

- High level of generality to any block cipher
- High freedom for the attacker in the construction of simple transitions defining complex product attacks
- Our ring is not empty, other invariants may exists

Weaknesses of our algebraic construction:

- It doesn't ensure that all product attacks follow this framework
- It doesn't take into account the additive structure of the ring of invariants
- Cycles generally tend to be too long, giving us few low degree invariants

Can this construction break DES?

Yes, but with weaker S-boxes and some keys.

Too few ways to make $W * f = 0$

Even harder when W is balanced and f is a product.

Trick to solve this problem: second order attack

We do not need to annihilate W!!!

We rather annihilate $W + Y$.

Trivial methods to do this:

1. $fW = 0, gY = 0 \Rightarrow (W + Y) * fg = 0$
2. $f\bar{W} = 0, g\bar{Y} = 0 \Rightarrow (W + Y) * fg = 0$

Three problems:

- Trivial
- Impossible
- High degree

Definition (k-normality)

A Boolean function $Z \in B_n$ is said to be k-normal if either of the following equivalent conditions holds:

i) There exists a (n-k)-dimensional flat U where Z is constant.

ii) Either Z or Z + 1 are annihilated by at least one product

$$\prod_{i=1}^{k} L_i$$

Of k linearly independent affine polynomials with either:

$$Z \prod_{i=1}^{k} L_i = 0 \qquad \text{or} \qquad (Z+1) \prod_{i=1}^{k} L_i = 0$$

Definition (k-weak-normality)

A Boolean function $Z \in B_n$ is said to be k-weak-normal if either of the following equivalent conditions holds:

i) There exists a (n-k)-dimensional flat U where Z is an affine function.

ii) There exists an affine shift $Z + L_0$ and a product

$$\prod_{i=1}^{k} L_i$$

Of k linearly independent affine polynomials such that:

$$(Z + L_0)\prod_{i=1}^{k} L_i = 0$$

We have examined the 150357 classes of Boolean functions on 6 variables

Frequencies of k-normal functions

K value →	0	1	2	3
150357	1	205	47466	150357
100 %	$2^{-17,2} \approx 10^{-4}$%	$2^{-9,52}$ ≈0,14%	$2^{-1,66}$ ≈32%	100%

Frequencies of k-weak-normal functions

K value →	0	1	2	3
150357	1	205	93760	150357
100 %	$2^{-17,2} \approx 10^{-4}$%	$2^{-9,52}$ ≈0,14%	$2^{-0,68} \approx$ 62%	100%

Normality of DES S-boxes

All 32 Boolean functions in DES are 3-normal,
all 32 are not 2-normal, and 26 out of 32 are 2-weakly-normal.

Theorem

Given $Z_1, Z_2 \in B_6$ then $Z_1 + Z_2 \in B_{12}$ is 6-normal

Is it possible to reduce the degree of this annihilation without Annihilating Z_1, Z_2 or their negations?

From Arxiv paper: Lack of unique factorization as a tool in Block Cipher Cryptoanalysis [Courtois,Patrick]

Example of attack on T-310 with annihilator of degree 5 for the sum. But it still annihilates Z_1+1, Z_2+1

Our general framework theorem allows Z_j to be an arbitrary sum of Boolean functions of the cipher, shifted by an arbitrary affine function L_0

New annihilation techniques for a direct sum of $m \geq 2$ Boolean functions with disjoint sets of variables

Theory of magic polynomials μ (Existence theorem)

Definition (magic polynomial μ)

Given a family of arbitrary $m \geq 2$ Boolean functions F=$\{Z_i\}_1{}^m \subseteq B_n$ with disjoint sets of variables. A magic polynomial for said family is a polynomial $\mu \in B_{mn}$ s.t.

$$\begin{cases} \mu * \left(\sum_{i=1}^{m} Z_i\right) = 0 \\ \mu * Z_i \neq 0 \qquad \forall i \\ \mu * (Z_i + 1) \neq 0 \ \ \forall i \end{cases}$$

This method gives rise to new annihilation events which can be exploited in our general framework theorem.

We have existence theorems for the cases $m = 2, m = 3$

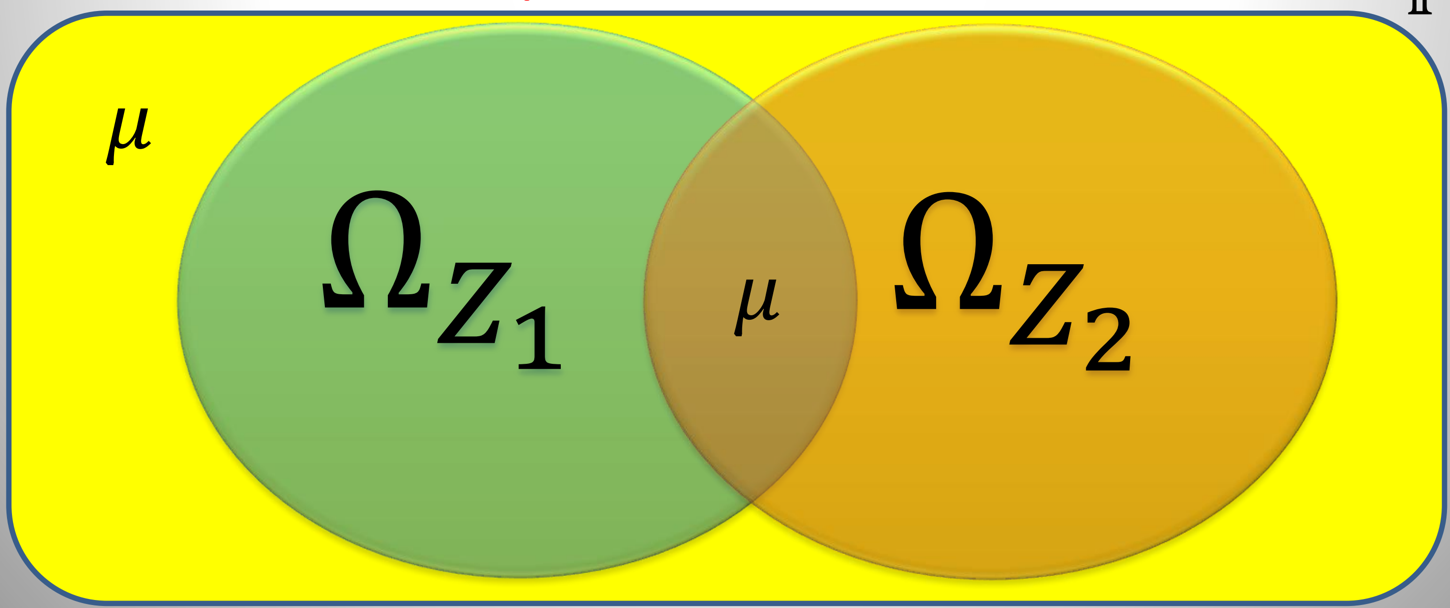
Existence theorem (m=2)

If $Z_1, Z_2 \in B_n$ are such that:

$$\begin{cases} Z_1 Z_2 \neq 0 \\ (Z_1 + 1)(Z_2 + 1) \neq 0 \end{cases}$$

Then it exists a magic polynomial $\mu \in B_{2n}$ for the family $\{Z_1, Z_2\}$.

Geometric idea of the proof:



Existence theorem (m=3)

If $Z_1, Z_2, Z_3 \in B_n$ are such that

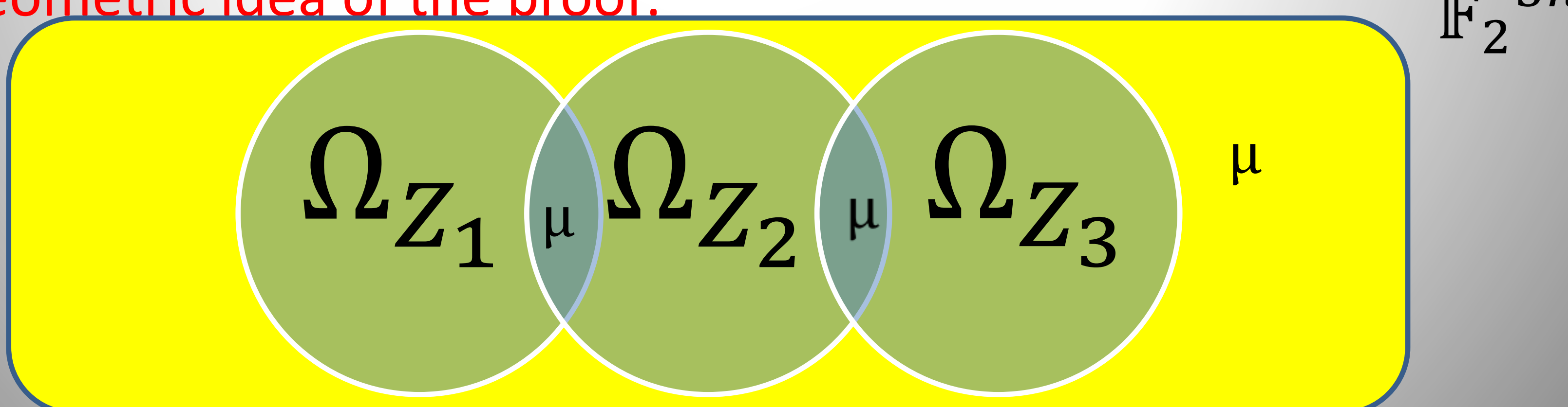
$$(Z_1 + 1)(Z_2 + 1)(Z_3 + 1) \neq 0$$

And at least two of the following conditions are true

$$\begin{cases} (Z_1+1)Z_2Z_3 \neq 0 \\ Z_1(Z_2 + 1)Z_3 \neq 0 \\ Z_1Z_2(Z_3 + 1) \neq 0 \end{cases}$$

Then it exists a magic polynomial $\mu \in B_{3n}$ for the family $\{Z_1, Z_2, Z_3\}$.

Geometric idea of the proof:



New proposed method with a Diophantine equation for finding new attacks or disprove their existence

Theorem (Spectral equation for annihilation of a direct sum)

Given a family of Boolean functions F=$\{Z_i\}_1{}^m \subseteq B_n$ with disjoint sets of variables, a set of k linearly independent vectors $S = \{\vec{a}_j = (\vec{a}_{j_1}|\ldots|\vec{a}_{j_m})\}_1{}^k \subseteq \mathbb{F}_2{}^{mn}$ $\forall i\ (\vec{a}_{j_i}) \in \mathbb{F}_2{}^n$, a vector $(\varepsilon_j)_1{}^k \in \mathbb{F}_2{}^k$. Then the polynomial

$$\mu = \prod_{j=1}^{k} (\varphi_{\vec{a}_j} + \varepsilon_j) \in B_{mn}$$

Is an annihilator for the sum $\sum_{i=1}^{m} Z_i \in B_{mn}$ i.f.f. the Walsh coefficients satisfy the following Diophantine equation of degree m in $m2^k$unknowns:

$$\sum_{\substack{(\vec{x}_{j_1}|\ldots|\vec{x}_{j_m}) \in \langle S \rangle_{\mathbb{F}_2} \\ \vec{x}_j = \sum_\nu \lambda_\nu \vec{a}_\nu}} (-1)^{\sum_\nu \lambda_\nu \varepsilon_\nu + \delta(\vec{x}) + 1} \prod_{i=1}^{m} W_{\hat{Z}_i}(\vec{x}_{j_i}) = 2^{mn}$$

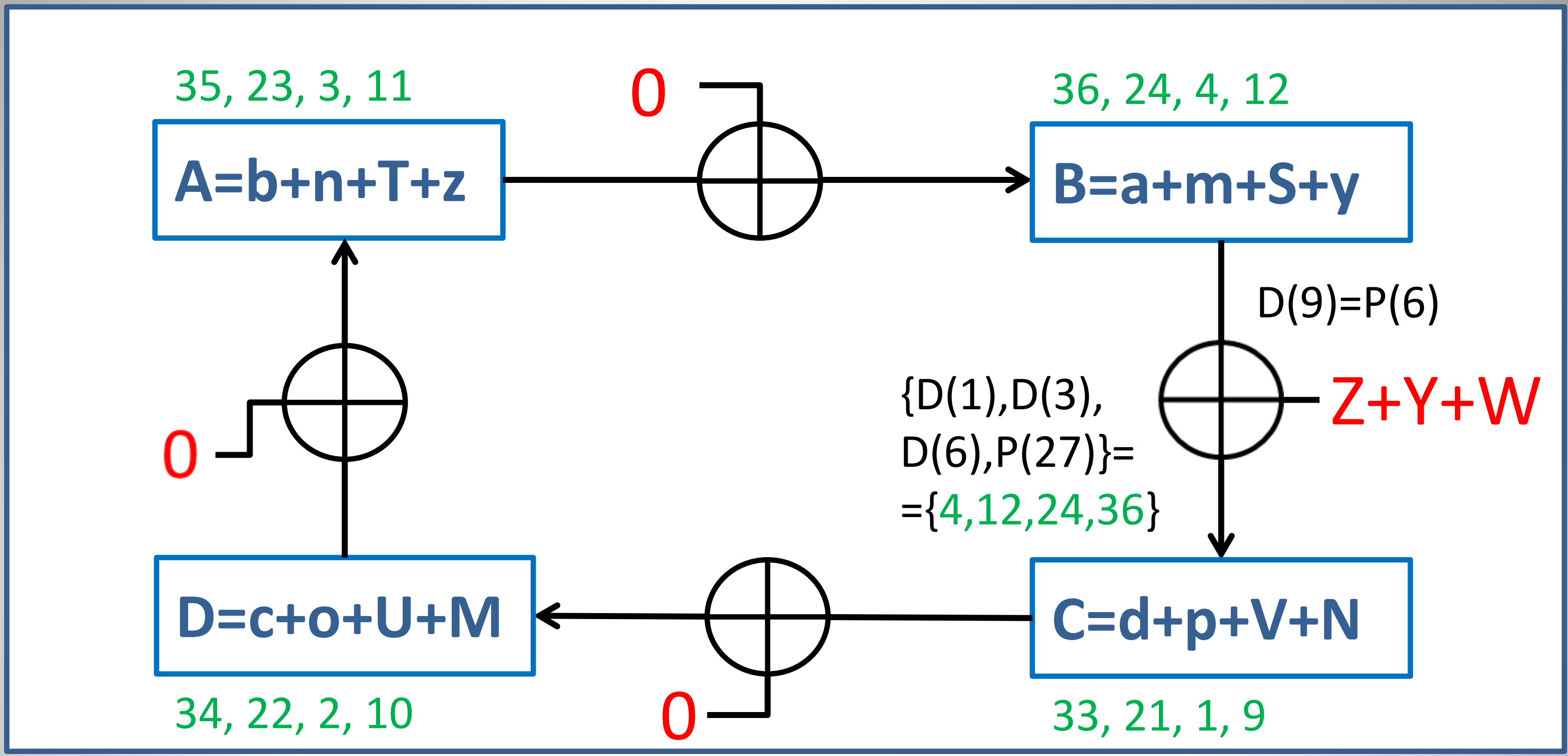
In the case of a family of balanced Boolean functions the equation reduces to:

$$\sum_{\substack{(\vec{x}_{j_1}|\ldots|\vec{x}_{j_m})\in\langle S\rangle_{\mathbb{F}_2} \\ \vec{x}_j=\sum_\nu \lambda_\nu \vec{a}_\nu \\ \vec{x}_{j_i}\neq 0\ \forall i}} (-1)^{\sum_\nu \lambda_\nu \varepsilon_\nu + 1} \prod_{i=1}^{m} W_{\hat{Z}_i}\left(\vec{x}_{j_i}\right) = 2^{mn}$$

Which, depending on the vectors inside the set S, has significantly less unknowns due to the condition $\vec{x}_{j_i} \neq 0\ \forall i$ and it could be used in two ways:

1. To determine magic polynomials for a given set of balanced Boolean functions
2. In our framework attack, given a cycle we could determine the existence of optimal solutions for the Boolean functions with certain desirable cryptographic properties of the Walsh spectrum

Example (For T-310 block cipher)



$P = ABCD$ is an invariant for 1 round of T-310 if the Boolean functions satisfy:

$(Z+Y+W)(b^{(Z)}+c^{(Z)}+d^{(W)}+e^{(W)})(b^{(Y)}+c^{(Y)}+d^{(Z)}+e^{(Z)})(b^{(W)}+c^{(W)}+d^{(Y)}+e^{(Y)}) = 0$

If we want the solutions to be balanced, then they must satisfy:

$W_{\hat{Z}}(\vec{a}_1+\vec{a}_2)W_{\hat{Y}}(\vec{a}_1)W_{\hat{W}}(\vec{a}_2) + W_{\hat{Z}}(\vec{a}_1)W_{\hat{Y}}(\vec{a}_2)W_{\hat{W}}(\vec{a}_1+\vec{a}_2) +$
$W_{\hat{Z}}(\vec{a}_2)W_{\hat{Y}}(\vec{a}_1+\vec{a}_2)W_{\hat{W}}(\vec{a}_1) + W_{\hat{Z}}(\vec{a}_1+\vec{a}_2)\, W_{\hat{Y}}(\vec{a}_1+\vec{a}_2)W_{\hat{W}}(\vec{a}_1+\vec{a}_2) = -2^{18}$

$\vec{a}_1=(0,1,1,0,0,0)$ $\vec{a}_2=(0,0,0,1,1,0) \in \mathbb{F}_2{}^6$

Thank you
for your attention