Another view of the division property

Christina Boura and **Anne Canteaut**

CRYPTO 2016, Santa Barbara
August 17, 2016

Motivation

Let E_k be a block cipher with block size n. Choose an input set $X \subseteq \mathbf{F}_2^n$.

Goal: Find a distinguishing property for $\{E_k(x), x \in X\}$ valid for all k.

- At Eurocrypt 2015, Yosuke Todo introduced the division property.
- Generalization of integral and higher-order differential distinguishers.
- Construction of more powerful generic distinguishers for both SPN and Feistel constructions.
- Use of this new property for breaking full MISTY-1 (best paper award at CRYPTO 2015).

Monomials of n variables

For $x = (x_1, \ldots, x_n)$ and $u = (u_1, \ldots, u_n)$ in $\mathbf{F}_2^n$

$$x^u = \prod_{i=1}^{n} x_i^{u_i}$$

Example: $u = (1010)$

$$x^u = x_4^1 x_3^0 x_2^1 x_1^0 = x_4 x_2$$

If $x = (1100)$, then $1^1 1^0 0^1 0^0 = 0$.

Evaluation of a monomial:

$$x^u = 1 \text{ if and only if } u \preceq x,$$

where $u \preceq x \Leftrightarrow u_i \leq x_i$ for $i = 1, \ldots, n$.

Division property [Todo 2015]

Let X be a set of elements in $\mathbf{F}_2^n$.

For $0 \leq k \leq n$, we say that X has the division property $\mathcal{D}_k^n$ if

$$\bigoplus_{x \in X} x^u = 0,$$

for all $u \in \mathbf{F}_2^n$ such that $wt(u) < k$.

- If $k = 2$ then X has the balanced property ($\mathcal{B}$)
- If $k = n$ then X has the saturated property ($\mathcal{A}$)
- **Novelty:** Introduction and propagation of the intermediate properties $\mathcal{D}_k^n$ for $3 \leq k \leq n - 1$.

Overview

1. Parity set of a set
2. Propagation of a parity set through the block cipher
3. Application to PRESENT

Outline

Parity set of a set

Let X be a set of elements in $\mathbf{F}_2^n$. Then, the set

$$\mathcal{U}(X) = \{u \in \mathbf{F}_2^n : \bigoplus_{x \in X} x^u = 1\},$$

is called the parity set of X.

Correspondence between a set and its parity-set

Incidence vector of a set $X \subseteq \mathbf{F}_2^n$:

v_X: binary vector of length 2^n having a 1 at all positions $x \in X$

Example $(n = 3)$. Let $X = \{1, 4, 7\}$. Then,

$$v_X = (1, 0, 0, 1, 0, 0, 1, 0)$$

Let G be the $2^n \times 2^n$ binary matrix with coefficients

$$G_{u,a} = a^u, \; a, u \in \mathbf{F}_2^n$$

Equivalently, $G_{u,a} = 1$ if and only if $u \preceq a$.

Proposition:

$$v_{\mathcal{U}(X)} = G \cdot v_X$$

An example for $n = 3$

$$\overbrace{\begin{pmatrix} 0^0 & 1^0 & 2^0 & 3^0 & 4^0 & 5^0 & 6^0 & 7^0 \\ 0^1 & 1^1 & 2^1 & 3^1 & 4^1 & 5^1 & 6^1 & 7^1 \\ 0^2 & 1^2 & 2^2 & 3^2 & 4^2 & 5^2 & 6^2 & 7^2 \\ 0^3 & 1^3 & 2^3 & 3^3 & 4^3 & 5^3 & 6^3 & 7^3 \\ 0^4 & 1^4 & 2^4 & 3^4 & 4^4 & 5^4 & 6^4 & 7^4 \\ 0^5 & 1^5 & 2^5 & 3^5 & 4^5 & 5^5 & 6^5 & 7^5 \\ 0^6 & 1^6 & 2^6 & 3^6 & 4^6 & 5^6 & 6^6 & 7^6 \\ 0^7 & 1^7 & 2^7 & 3^7 & 4^7 & 5^7 & 6^7 & 7^7 \end{pmatrix}}^{G}$$

An example for $n = 3$

$$
\overbrace{\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}}^{G}
$$

An example for $n = 3$

$X = \{1, 3, 4\}$

$$\overbrace{\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}}^{G} \overbrace{\begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}}^{v_X}$$

An example for $n = 3$

$X = \{1, 3, 4\}$

$$\overbrace{\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}}^{G} \overbrace{\begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}}^{v_X} = \overbrace{\begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}}^{v_{\mathcal{U}(X)}}$$

$\mathcal{U}(X) = \{0, 2, 3, 4\}$.

Unicity of the parity set

Definition: The Reed-Muller code of length 2^n and order r, $RM(r,n)$, is the set of all $(f(x), x \in \mathbf{F}_2^n)$ with $\deg f \leq r$.

$\Rightarrow G$: generator matrix of $RM(n,n)$

Consequences : G has full rank and $G^{-1} = G$.

Theorem. For any $U \subseteq \mathbf{F}_2^n$, there exists a unique $X \subseteq \mathbf{F}_2^n$, such that

$$U = \mathcal{U}(X).$$

Link with the division property

Proposition. $X \subseteq \mathbf{F}_2^n$ fulfills the division property D_k^n, if

$$\mathcal{U}(X) \subseteq \{u \in \mathbf{F}_2^n : wt(u) \geq k\}.$$

$\Rightarrow \mathcal{D}_k^n$ is a lower bound on the weight of all elements in $\mathcal{U}(X)$.

The rows of G defined by the exponents u with $wt(u) < k$ form a generator matrix of the Reed-Muller code of order $(k-1)$.

Corollary. $X \subseteq \mathbf{F}_2^n$ fulfills the division property D_k^n if and only if its incidence vector belongs to $RM(k-1,n)^\perp = RM(n-k,n)$.

Some direct consequences

Corollary. [Sun et al. 15] If X fulfills $\mathcal{D}_k^n$, then $|X| \geq 2^k$.
Equality holds if and only if X is an affine subspace of dimension k.

Some specific cases:

- X fulfills $\mathcal{D}_1^n$: $|X|$ is even.
- X fulfills $\mathcal{D}_2^n$: $\bigoplus_{x \in X} x = 0$ [BALANCED]
- X fulfills $\mathcal{D}_n^n$: $\mathcal{U}(X) = \{1 \dots 1\} \Leftrightarrow X = \mathbf{F}_2^n$ [ALL]
- X fulfills $\mathcal{D}_{n-1}^n : v_X \in RM(1, n)$ or equivalently X is an (affine) hyperplane.

Outline

Propagation through key addition

Propagate the parity set after the XOR with an unknown key k.

$$(x \oplus k)^v = \bigoplus_{u \preceq v} x^u k^{v \oplus u}$$

Then,

$$\mathcal{U}(\mathsf{Add}_K(X)) \subseteq \bigcup_{u \in \mathcal{U}(X)} \{v \in \mathbf{F}_2^n : v \succeq u\}$$

Example: $n = 4$, $\mathcal{U}(X) = \{3, c\}$. Then,

$$\mathcal{U}(\mathsf{Add}_K(X)) \subseteq \{3, 7, b, c, d, e, f\}.$$

Propagating the parity set through an Sbox

By definition,

$$v \in \mathcal{U}(S(X)) \Leftrightarrow \bigoplus_{x \in X} S^v(x) = 1$$

$\Rightarrow$ the ANF of $S^v(x)$ contains some x^u with $u \in \mathcal{U}(X)$

Proposition. Let $V_S(u) = \{v \in \mathbf{F}_2^n : S^v(x) \text{ contains } x^u\}$
Then,

$$\mathcal{U}(S(X)) \subseteq \bigcup_{u \in \mathcal{U}(X)} V_S(u)$$

$V_S(u)$ for the PRESENT Sbox

	0	1	2	4	8	3	5	9	6	a	c	7	b	d	e	f
0	x			x	x						x					
1		x			x		x				x					
2			x		x				x		x					
4		x		x				x			x					
8		x	x	x	x	x					x					
3				x		x	x	x	x	x	x		x			
5							x	x			x					
9				x		x	x		x	x					x	
6		x			x			x	x	x	x					
a			x	x			x	x		x		x	x	x	x	x
c			x			x		x			x					
7			x		x	x		x	x				x	x		
b			x	x	x	x			x	x	x	x		x		x
d			x	x	x			x		x		x			x	
e							x					x	x	x	x	x
f																x

Link with the ANF

	0	1	2	4	8
0	x			x	
1		x			x
2			x		x
4		x		x	
8		x	x	x	x
3				x	
5					
9				x	
6		x			x
a			x	x	
c			x		
7			x		x
b			x	x	x
d			x	x	x
e					
f					

$$
\begin{aligned}
S_1 &= x_1 + x_3 + x_4 + x_2x_3 \\
S_2 &= x_2 + x_4 + x_2x_4 + x_3x_4 + x_1x_2x_3 \\
&+ x_1x_2x_4 + x_1x_3x_4 \\
S_3 &= 1 + x_3 + x_4 + x_1x_2 + x_1x_4 + x_2x_4 \\
&+ x_1x_2x_4 + x_1x_3x_4 \\
S_4 &= 1 + x_1 + x_2 + x_4 + x_2x_3 + x_1x_2x_3 \\
&+ x_1x_2x_4 + x_1x_3x_4 \ .
\end{aligned}
$$

Link with the inverse Sbox

Theorem. Let $S^* : x \mapsto \overline{S^{-1}(x)}$.
Then, $S(x)^v$ contains x^u if and only if $S^*(x)^{\overline{u}}$ contains x^v.

$$\Rightarrow V_S(u) = \{v : [S^*(x)]^{\overline{u}} \text{ contains } x^{\overline{v}}\}$$

Example: The 1st coordinate of S^* is:

$$1 + x_1 + x_2 + x_3 + x_4 + x_2x_4$$

$$\begin{aligned} \Rightarrow V_S(1110) &= \{0101, 0111, 1011, 1101, 1110, 1111\} \\ &= \{5, 7, \mathtt{b}, \mathtt{d}, \mathtt{e}, \mathtt{f}\}. \end{aligned}$$

	0	1	2	4	8	3	5	9	6	a	c	7	b	d	e	f
e							x					x	x	x	x	x

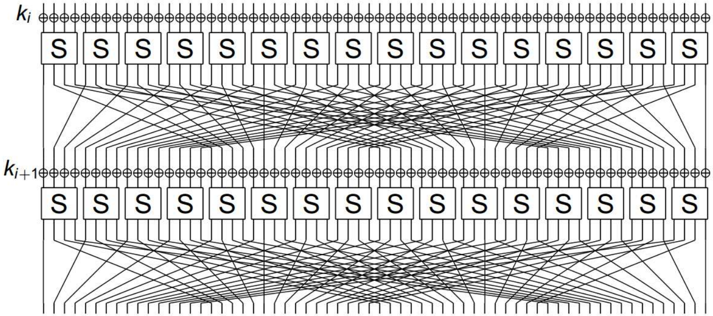
Outline

PRESENT

[Bogdanov – Knudsen – Le – Paar – Poschmann – Robshaw – Seurin – Vikkelsoe 2007]

64-bit block cipher with 80/128-bit key and 31 rounds.

- Confusion : Use of a 4-bit Sbox of degree 3.



4 rounds by exploiting the linear layer

$$X = \boxed{\mathcal{C}}\boxed{\mathcal{C}}\boxed{\mathcal{C}}\boxed{\mathcal{C}}\boxed{\mathcal{C}}\boxed{\mathcal{C}}\boxed{\mathcal{C}}\boxed{\mathcal{C}}\boxed{\mathcal{C}}\boxed{\mathcal{C}}\boxed{\mathcal{C}}\boxed{\mathcal{C}}\boxed{\mathcal{A}}\boxed{\mathcal{A}}\boxed{\mathcal{A}}\boxed{\mathcal{C}}$$

$$\mathcal{U}(X) \subseteq \{u : u \succeq \texttt{000000000000fff0}\}$$

- Invariant under the 1st Sbox layer.
- After the 1st linear layer:

$$\mathcal{U}(X) \subseteq \{u : u \succeq \texttt{000e000e000e000e}\} \rightarrow \text{ 4 active superboxes.}$$

- After the 3rd Sbox layer: $\mathcal{U} \subseteq \{u : wt(u) \geq 4\}$.
- After the 3rd linear layer:

$$\mathcal{U} \subseteq \{u \text{ with } \geq 2 \text{ active nibbles}\} \cup \{\texttt{0x00}\ldots\texttt{0f}, \ldots, \texttt{0xf0}\ldots\texttt{0}\}.$$

- Invariant under the 4th Sbox layer

$$\Rightarrow \mathcal{U}(E_K(X)) \subseteq \{v : wt(v) \geq 2\}$$

Does not work on 5 rounds for some Sboxes

A possible propagation

Input	–	–	–	–	–	–	–	–	–	–	–	–	f	f	f	–
1st S-layer	–	–	–	–	–	–	–	–	–	–	–	–	f	f	f	–
1st P-layer	–	–	–	e	–	–	–	e	–	–	–	e	–	–	–	e
2nd S-layer	–	–	–	2	–	–	–	1	–	–	–	1	–	–	–	1
2nd P-layer	–	–	–	–	–	–	–	–	1	–	–	–	–	1	1	1
3rd S-layer	–	–	–	–	–	–	–	–	1	–	–	–	–	1	1	1
3rd P-layer	–	–	–	–	–	–	–	–	–	–	–	–	–	–	8	7
4th S-layer	–	–	–	–	–	–	–	–	–	–	–	–	–	–	2	8
4th P-layer	–	–	–	3	–	–	–	–	–	–	–	–	–	–	–	–
5th S-layer	–	–	–	1	–	–	–	–	–	–	–	–	–	–	–	–

Does not work on 5 rounds for some Sboxes

A possible propagation

Input	–	–	–	–	–	–	–	–	–	–	–	–	f	f	f	–
1st S-layer	–	–	–	–	–	–	–	–	–	–	–	–	f	f	f	–
1st P-layer	–	–	–	e	–	–	–	e	–	–	–	e	–	–	–	e
2nd S-layer	–	–	–	2	–	–	–	1	–	–	–	1	–	–	–	1
2nd P-layer	–	–	–	–	–	–	–	–	1	–	–	–	–	1	1	1
3rd S-layer	–	–	–	–	–	–	–	–	1	–	–	–	–	1	1	1
3rd P-layer	–	–	–	–	–	–	–	–	–	–	–	–	–	–	8	7
4th S-layer	–	–	–	–	–	–	–	–	–	–	–	–	–	–	2	8
4th P-layer	–	–	–	3	–	–	–	–	–	–	–	–	–	–	–	–
5th S-layer	–	–	–	1	–	–	–	–	–	–	–	–	–	–	–	–

- Feasible if the Sbox makes the transitions e $\rightarrow$ 1 and e $\rightarrow$ 2 possible.

5-round distinguisher

	0	1	2	4	8	3	5	9	6	a	c	7	b	d	e	f
0	x			x	x						x					
1		x			x		x				x					
2			x		x				x		x					
4		x		x				x			x					
8		x	x	x	x	x					x					
3				x		x	x	x	x	x	x		x			
5							x	x			x					
9				x		x	x		x	x					x	
6		x			x			x	x	x	x					
a			x	x			x	x		x		x	x	x	x	x
c			x			x		x			x					
7			x		x	x		x	x				x	x		
b			x	x	x	x			x	x	x	x		x		x
d			x	x	x			x		x		x			x	
e							x					**x**	**x**	**x**	**x**	**x**
f																x

5-round distinguisher

	0	1	2	4	8	3	5	9	6	a	c	7	b	d	e	f
0	x			x	x						x					
1		x			x		x				x					
2			x		x				x		x					
4		x		x				x			x					
8		x	x	x	x	x					x					
3				x		x	x	x	x	x	x		x			
5							x	x			x					
9				x		x	x		x	x					x	
6		x			x			x	x	x	x					
a			x	x			x	x		x		x	x	x	x	x
c			x			x		x			x					
7			x		x	x		x	x				x	x		
b			x	x	x	x			x	x	x	x		x		x
d			x	x	x			x		x		x			x	
e							**x**					**x**	**x**	**x**	**x**	**x**
f																x

5-round distinguisher

	0	1	2	4	8	3	5	9	6	a	c	7	b	d	e	f
e							x					**x**	**x**	**x**	**x**	**x**

- $V_S(\mathrm{e})$ contains a few elements only.
- The transactions e $\rightarrow$ 1 and e $\rightarrow$ 2 are **not possible**.
- We've checked that no vector of Hamming weight 1 is in the output parity set after 5 rounds.

The output set has the balanced property after 5 rounds.

6-round distinguisher

	0	**1**	2	4	8	3	5	9	6	a	c	7	b	d	e	f
0	x			x	x						x					
1		**x**			x		x				x					
2			x		x				x		x					
4		**x**		x				x			x					
8		**x**	x	x	x	x					x					
3				x		x	x	x	x	x	x		x			
5							x	x			x					
9				x		x	x		x	x					x	
6		**x**			x			x	x	x	x					
a			x	x			x	x		x		x	x	x	x	x
c			x			x		x			x					
7			x		x	x		x	x				x	x		
b			x	x	x	x			x	x	x	x		x		x
d			x	x	x			x		x		x			x	
e							x					x	x	x	x	x
f																x

6-round distinguisher

	0	1
0	x	
1		x
2		
4		x
8		x
3		
5		
9		
6		x
a		
c		
7		
b		
d		
e		
f		

- After 6 rounds, the output parity set contains elements with Hamming weight 1.
- **But**, column corresponding to 1 is very sparse: most of the transitions $u \to 1$ are not possible.
- Only the nibble values 2, 4 and 8 are possible $\to 16$ values don't belong to the output parity set.
- Weaker distinguisher for 6 rounds

Conclusion and open problems

- The notion of parity set permits us to capture more information compared to the division property.
- Computing the propagation of the parity set is more expensive than computing the propagation of the division property. How to make the propagation more time and memory efficient?
- Use parity sets for identifying classes of weak keys.

Conclusion and open problems

- The notion of parity set permits us to capture more information compared to the division property.
- Computing the propagation of the parity set is more expensive than computing the propagation of the division property. How to make the propagation more time and memory efficient?
- Use parity sets for identifying classes of weak keys.

Thanks for your attention!