On the division property

Jan Schoone

Radboud University

1 March, 2019

Overview

This talk is about Symmetric Cryptography, some permutation-based.

We discuss some properties of polynomials that arise in this context and the vulnerabilities they show.

Content

Higher Order Derivatives

Higher Order Derivatives – general

Definition. Let $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a function and $v \in \mathbb{F}_2^n$. The *derivative of F with respect to v* is the function $D_v F$ defined by:

$$D_v F(x) = F(x \oplus v) \oplus F(x).$$

Let $V = \langle\!\langle\, v_1, \ldots, v_k \,\rangle\!\rangle$, then the *$k$-th order derivative of F with respect to V* is the function $D_V F$ defined by:

$$D_V F(x) = D_{v_1} D_{v_2} \cdots D_{v_k} F(x) = \bigoplus_{v \in V} F(x + v).$$

Higher Order Derivatives – general II

Theorem. Let $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ and $v \in \mathbb{F}_2^n$ be arbitary. Then

$$\deg D_v F \leq \deg F - 1.$$

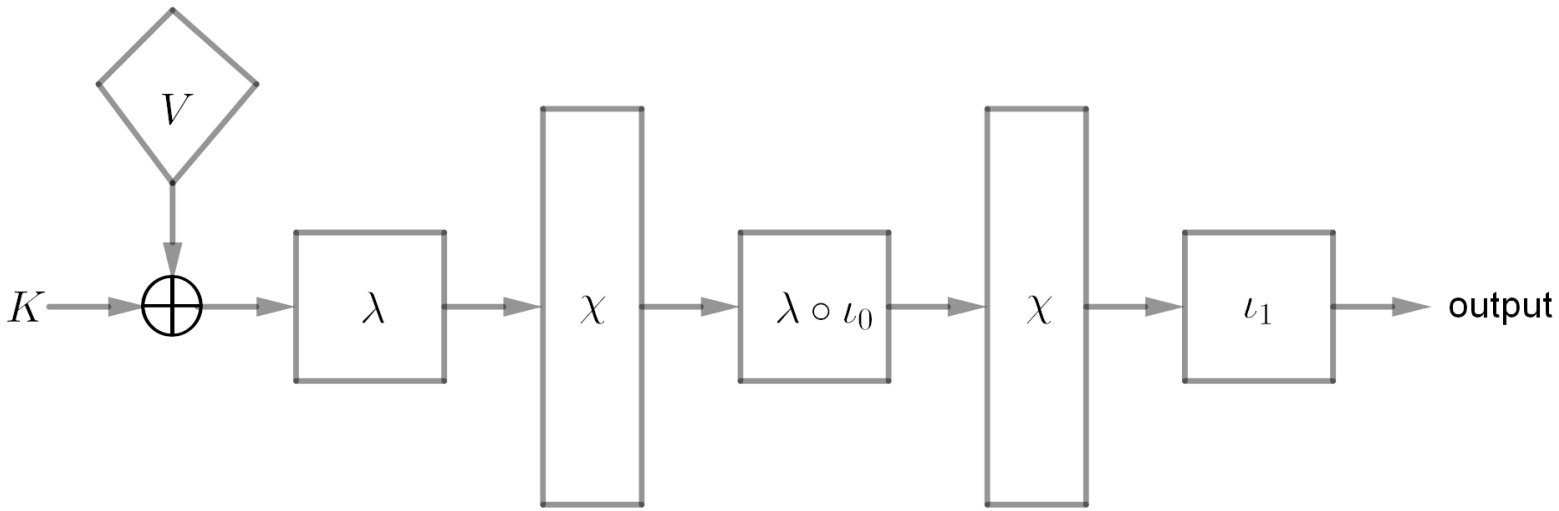
So if we have a function F of degree n, then after $n-1$ derivations, we are left with an at most linear function.

Thus for an $(n-1)$-dimensional vector space V, we find that

$$D_{v_1} D_{v_2} \cdots D_{v_{n-1}} F(x) = \bigoplus_{v \in V} F(x+v)$$

is at most linear.

Higher Order Derivatives – example



Higher Order Derivatives – example II

One finds that by applying the vector space

$$V_0 = \left\langle\!\!\left\langle \begin{pmatrix}0\\1\\0\\1\\0\end{pmatrix}, \begin{pmatrix}1\\0\\0\\0\\0\end{pmatrix} \right\rangle\!\!\right\rangle$$

we get

$$\bigoplus_{v \in V_0} F(K+v) = \begin{pmatrix} Q \\ k_1 + k_3 + 1 \\ 0 \\ k_4 \\ k_2 + k_4 \end{pmatrix}$$

Higher Order Derivatives – example III

Now applying the vector space

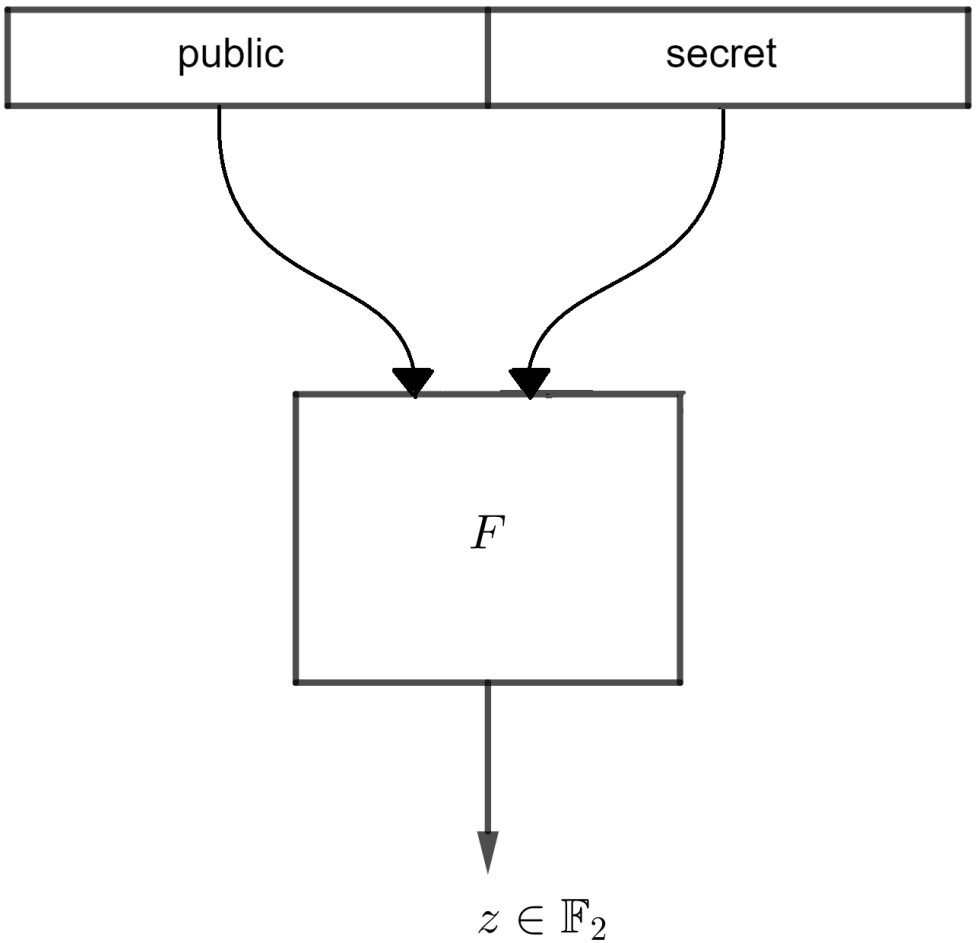
$$V_1 = \left[\!\!\left[\begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \right]\!\!\right]$$

we get

$$\bigoplus_{v \in V_1} F(K+v) = \begin{pmatrix} k_1 + k_4 + 1 \\ k_3 + 1 \\ Q \\ k_3 + 1 \\ 1 \end{pmatrix}$$

Cube attacks

Cube attacks – general



The polynomial from the example

$$F_1(x_1, x_2, x_3, x_4, x_5, y_1, y_2, y_3, y_4, y_5) = x_1x_2x_3x_4 + x_1x_2x_3y_4 + x_1x_2x_4x_5 +$$
$$x_1x_2x_4y_3 + x_1x_2x_4y_5 + x_1x_2x_4 + x_1x_2x_5y_4 + x_1x_2x_5 + x_1x_2y_3y_4 + x_1x_2y_4y_5 + x_1x_2y_4 +$$
$$x_1x_2y_5 + x_1x_3x_4y_2 + x_1x_3x_4 + x_1x_3y_2y_4 + x_1x_3y_4 + x_1x_4x_5y_2 + x_1x_4x_5 + x_1x_4y_2y_3 + x_1x_4y_2y_5 +$$
$$x_1x_4y_2 + x_1x_4y_3 + x_1x_4y_5 + x_1x_5y_2y_4 + x_1x_5y_2 + x_1x_5y_4 + x_1x_5 + x_1y_2y_3y_4 + x_1y_2y_4y_5 + x_1y_2y_4 +$$
$$x_1y_2y_5 + x_1y_3y_4 + x_1y_4y_5 + x_1y_5 + x_2x_3x_4x_5 + x_2x_3x_4y_1 + x_2x_3x_4y_5 + x_2x_3x_4 + x_2x_3x_5y_4 + x_2x_3x_5 +$$
$$x_2x_3y_1y_4 + x_2x_3y_4y_5 + x_2x_3y_4 + x_2x_3y_5 + x_2x_4x_5y_1 + x_2x_4x_5y_3 + x_2x_4x_5 + x_2x_4y_1y_3 + x_2x_4y_1y_5 +$$
$$x_2x_4y_1 + x_2x_4y_3y_5 + x_2x_4y_3 + x_2x_4y_5 + x_2x_5y_1y_4 + x_2x_5y_1 + x_2x_5y_3y_4 + x_2x_5y_3 + x_2x_5y_4 +$$
$$x_2y_1y_3y_4 + x_2y_1y_4y_5 + x_2y_1y_4 + x_2y_1y_5 + x_2y_3y_4y_5 + x_2y_3y_4 + x_2y_3y_5 + x_2y_4y_5 + x_2 + x_3x_4x_5y_2 +$$
$$x_3x_4x_5 + x_3x_4y_1y_2 + x_3x_4y_1 + x_3x_4y_2y_5 + x_3x_4y_2 + x_3x_4y_5 + x_3x_4 + x_3x_5y_2y_4 + x_3x_5y_2 + x_3x_5y_4 +$$
$$x_3y_1y_2y_4 + x_3y_1y_4 + x_3y_2y_4y_5 + x_3y_2y_4 + x_3y_2y_5 + x_3y_4y_5 + x_3y_4 + x_4x_5y_1y_2 + x_4x_5y_1 + x_4x_5y_2y_3 +$$
$$x_4x_5y_2 + x_4x_5y_3 + x_4y_1y_2y_3 + x_4y_1y_2y_5 + x_4y_1y_2 + x_4y_1y_3 + x_4y_1y_5 + x_4y_2y_3y_5 + x_4y_2y_3 + x_4y_2y_5 +$$
$$x_4y_3y_5 + x_4y_3 + x_5y_1y_2y_4 + x_5y_1y_2 + x_5y_1y_4 + x_5y_1 + x_5y_2y_3y_4 + x_5y_2y_3 + x_5y_2y_4 + x_5y_3y_4 + x_5 +$$
$$y_1y_2y_3y_4 + y_1y_2y_4y_5 + y_1y_2y_4 + y_1y_2y_5 + y_1y_3y_4 + y_1y_4y_5 + y_1y_5 + y_2y_3y_4y_5 + y_2y_3y_4 + y_2y_3y_5 +$$
$$y_2y_4y_5 + y_2 + y_3y_4y_5 + y_3y_4 + y_5 + 1$$

Cube attacks – example

We can write

$$F_1 = x_1x_2x_3P + q$$

where P and q do not contain any multiple of $x_1x_2x_3$.

P is called the *superpoly* belonging to $x_1x_2x_3$.

But...

we need to know the algebraic normal form of F_1!

Cube attacks – example II

We will now determine the superpoly of F_1 for the monomial $x_1x_2x_3$.

We construct the 'cube':

$$C := \{00000, 10000, 00100, 10100, 01000, 11000, 01100, 11100\}$$

What we will do next is compute

$$\bigoplus_{x \in C} F_1(x, K).$$

Cube attacks – example III

Constant term:

$$x_2 + 1 + \sum_{i=1}^{3} x_i c_i + \sum_{i<j} x_i x_j c_{ij} + x_1 x_2 x_3 c_{123}$$

Then the constant term is y_4.

Coefficient for x_4:

$$x_1 x_2 x_3 + x_1 x_2 + x_1 x_3 + x_2 x_3 + x_2 + x_3 + 1 +$$
$$\sum_{i=1}^{3} x_i c_i + \sum_{i<j} x_i x_j c_{ij}$$

The coefficient for x_4 is then 1.

The superpoly for $x_1 x_2 x_3$ is $x_4 + y_4$.

Cube attacks – general II

So with these cube attacks we can find linear equations in the key bits.

But...

- Cube of n bits requires 2^n initializations;
- Only one linear equation, we need 128 for 128 key bits;
- With diversifier of 96 bits how big will the cube get?

Division property

Division property – general

Given $u \in \mathbb{F}_2^n$ and $x = (x_1, \ldots, x_n)$ we write $x^u := \prod_{i=1}^n x_i^{u_i}$.

Example: $x^{1011} = x_1 x_3 x_4$ or $x^{0011} = x_3 x_4$.

If $x = 0111$ then we get $0111^{1011} = 0$ and $0111^{0011} = 1$.

Definition. Let $X \subset \mathbb{F}_2^n$ be given. Then X has the *division property of order* $1 \leq k \leq n$ if for all $u \in \mathbb{F}_2^n$ with $\mathrm{wt}(u) < k$ we have:

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

We will say that X has $\mathcal{D}_k^n$ as shorthand for the division property of order k.

Division property – example

The subset $X := \{1100, 1011, 1110, 0101, 0110, 1010\}$ of $\mathbb{F}_2^4$ has $\mathcal{D}_2^4$.

For $u = 0000$ we have $\bigoplus_{x \in X} x^u = 0$. (Since X has even cardinality.)

For $u = 0100$ we have

$$\begin{aligned} \bigoplus_{x \in X} x^u &= 1100^{0100} + 1011^{0100} + 1110^{0100} + \\ &\quad 0101^{0100} + 0110^{0100} + 1010^{0100} \\ &= 1 + 0 + 1 + 1 + 1 + 0 = 0 \end{aligned}$$

For $u = 1000, 0010$ and $u = 0001$ we can follow the same procedure.

Parity sets

Intermezzo: Partial Order

On $u, v \in \mathbb{F}_2^n$ we can bestow a partial order in the following way:

$u \preccurlyeq v$ if and only if $u_i \leq v_i$ for all i.

Example: $0001 \preccurlyeq 0111$

$0001 \not\preccurlyeq 1110$

Remark: We have $x^u = 1$ if and only if $u \preccurlyeq x$.

Parity sets – general

X has the division property of order k if for all $u \in \mathbb{F}_2^n$ with $\mathrm{wt}(u) < k$ we have:

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

Definition. Let $X \subset \mathbb{F}_2^n$ be given. Then

$$\mathcal{U}(X) := \left\{ u \in \mathbb{F}_2^n \,\middle|\, \bigoplus_{x \in X} x^u = 1 \right\}$$

is called the *parity set of* X.

Examples: $\mathcal{U}(\emptyset) = \emptyset$

$\mathcal{U}(\{x\}) := \{u \in \mathbb{F}_2^n \mid x^u = 1\} = \{u \in \mathbb{F}_2^n \mid u \preccurlyeq x\}.$

Parity sets – general II

Theorem. The correspondence between X and $\mathcal{U}(X)$ is an involutory correspondence!

Hence we find that

$$\mathcal{U}(\{u \in \mathbb{F}_2^n \mid u \preccurlyeq x\}) = \{x\},$$

and hence that $\mathcal{U}(\mathbb{F}_2^n) = \{\underline{1}\}$.

Parity sets – example

We find the parity set of
$X = \{1100, 1011, 1110, 0101, 0110, 1010\} \subset \mathbb{F}_2^4$.

That is find all $u \in \mathbb{F}_2^n$ with
$1100^u + 1011^u + 1110^u + 0101^u + 0110^u + 1010^u = 1$.

For each $x \in X$ we know the parity set:
$\mathcal{U}(\{1100\}) = \{u \in \mathbb{F}_2^n \mid u \preccurlyeq 1100\} = \{0000, 1000, 0100, 1100\}$.

Parity sets – example II

Then we determine the multiset-union of these six parity sets:

$$\{0000, 1000, 0100, 1100, 0000, 0100, 0001, 0101,$$

$$0000, 0100, 0010, 0110, 0000, 1000, 0010, 1010,$$

$$0000, 1000, 0010, 0001, 1010, 1001, 0011, 1011,$$

$$0000, 1000, 0010, 0100, 1100, 1010, 0110, 1110\}.$$

Hence

$$\mathcal{U}(X) = \{1001, 0101, 1010, 1110, 0011, 1011\}.$$

Parity sets and division property

Proposition. A set $X \subset \mathbb{F}_2^n$ satisfies the division property of order $1 \leq k \leq n$ iff $\mathcal{U}(X) \subset \{u \in \mathbb{F}_2^n \mid \mathrm{wt}(u) \geq k\}$.

PROOF: Note that the following statements are equivalent:

$$X \text{ satisfies the division property of order } k$$

$$\bigoplus_{x \in X} x^u = 0 \text{ when } \mathrm{wt}(u) < k$$

$$\bigoplus_{x \in X} x^u = 1 \text{ only when } \mathrm{wt}(u) \geq k$$

$$\left\{ u \in \mathbb{F}_2^n \,\middle|\, \bigoplus_{x \in X} x^u = 1 \right\} \subset \{u \in \mathbb{F}_2^n \mid \mathrm{wt}(u) \geq k\}$$

$$\mathcal{U}(X) \subset \{u \in \mathbb{F}_2^n \mid \mathrm{wt}(u) \geq k\}$$

□

Parity sets and division property II

Proposition. Let $X \subset \mathbb{F}_2^n$ satisfy $\mathcal{D}_k^n$. Then $|X| \geq 2^k$.

Furthermore, $X \subset \mathbb{F}_2^n$ with $|X| = 2^k$ satisfies $\mathcal{D}_k^n$ iff X is an affine subspace of dimension k.

Distinguishers

Todo et al's Distinguishers

General setting:

- E_K some (keyed) permutation;
- X such that $E_K(X)$ satisfies some property for all K;
- minimize complexity, so $|X|$ small;

Todo et al suggested to find an affine space $v + V$ such that $E_K(v + V)$ satisfies $\mathcal{D}_2^n$.

Todo et al's Distinguishers II

If $P\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is a permutation, we write for any $x, u \in \mathbb{F}_2^n$

$$P(x)^u = \prod_{i=1}^{n} P_i(x)^{u_i}.$$

$$\begin{aligned} & u \in \mathcal{U}(P(v+V)) \\ & \bigoplus_{x \in P(v+V)} x^u = 1 \\ & \bigoplus_{y \in v+V} P(y)^u = 1 \\ & D_V P(v)^u = 1 \end{aligned}$$

Proposition. We have $u \in \mathcal{U}(P(v+V))$ iff $D_V P(v)^u = 1$.

Todo et al's Distinguishers III

Corollary. Let $V \subset \mathbb{F}_2^n$ and $v \in \mathbb{F}_2^n$. Let $P\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a permutation. Then $P(v+V)$ satisfies the division property of order k iff for all u with $\mathrm{wt}(u) < k$ we have $D_V P(v)^u \neq 1$.

With $V = \{w \in \mathbb{F}_2^n \mid w \preccurlyeq a\}$ for some $a \in \mathbb{F}_2^n$, the following are equivalent:

i. For all $v \in \mathbb{F}_2^n$, we have $u \notin \mathcal{U}(P(v+V))$;
ii. The superpoly of a in P^u vanishes;
iii. The algebraic normal form of P^u contains no monomial that is a multiple of x^a.

Todo et al's Distinguishers IV

So to summarize, using the division property of order 2, we can easily see if the superpoly of a in P^u vanishes.

A vanishing superpoly is a distinguisher for the cipher, a so-called zero-sum distinguisher.

Conclusion

Conclusions

- Cube attacks are very similar to higher order derivatives;
- Division property can be investigated on sets and their parity sets;
- Parity sets correspond to higher order derivatives;
- Parity set of a singleton yields a cube;
- ...

Future Research

Many open areas for these algebraic attacks, cube attacks are a very special example.

Also, a very new paper:

Linearly equivalent S-boxes and the division property
by Derbez, Fouque & Lambin

When no distinguisher for E_K there might be one for $L' \circ E_K \circ L$, which is still relevant.

Discussion

Thank you all for your attention, are there questions to start the discussion?