Recovering or Testing Extended-Affine Equivalence

Anne Canteaut, Alain Couvreur, Léo Perrin

Inria, France

Carleton Finite Fields eSeminar - April 2021, 14

Extended-Affine Equivalence

F and G: $\mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$

Affine equivalence:

$$G = A \circ F \circ B$$

for some affine permutations A and B.

Extended-affine equivalence (EA-equivalence):

$$G = A \circ F \circ B + C$$

for some affine permutations A and B, and some affine function C.

Two different problems

EA-recovery:

Given F and G, find, if they exist, three affine mappings A, B and C such that $G = A \circ F \circ B + C$.

EA-testing:

Given $\{F_i\}_{0 \leq i < \ell}$, partition this set in such a way that two functions in distinct subsets are not EA-equivalent.

$\longrightarrow$ testing EA-equivalence between a set of 20,000+ 8-bit quadratic APN functions [Yu-Wang-Li 14][Beierle-Leander 20]

Outline

1. A new algorithm for EA-recovery for quadratic functions
   - Jacobian matrices for Boolean functions
   - A new algorithm
   - Complexity analysis and differential spectrum

2. A new algorithm for EA-testing for quadratic APN functions

EA-recovery

Known Algorithms for EA-recovery

Affine equivalence ($C = 0$):

- Guess-and-determine [Biryukov et al 2003]
  only when F and G are bijective.

$$\mathcal{O}\left(n^3 2^{2n}\right)$$

- Rank table [Dinur 2018]
  only when $\deg F \geq n - 1$

$$\mathcal{O}\left(n^3 2^{n}\right)$$

Extended-affine equivalence (any C):

partial results when $A(x) = x + a$, $B(x) = x + b$ [Budaghyan-Kazymyrov 2012]

Here: solve EA-recovery when $\deg F = 2$

$$\mathcal{O}\left(n^{2\omega} 2^{2n}\right) \text{ for APN functions (worst case)}$$

Differential uniformity and APN functions

$F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ coordinates $= (F_1, \ldots, F_m)$.

Derivative of F:

$$\Delta_a F : x \longmapsto F(x+a) + F(x)$$

Differential properties of F [Nyberg 93]

$$\delta_F(a,b) = \#\{x \in \mathbb{F}_2^n : \Delta_a F(x) = b\}$$

- Differential spectrum: $\{\delta_F(a,b), a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^m\}$
- Differential uniformity:

$$\delta(F) = \max_{a \neq 0, b} \delta_F(a,b)$$

- Functions with optimal differential uniformity:

$\delta(F) \geq 2^{n-m}$, with equality for Perfect-Nonlinear (PN) functions.

When $m \geq n$,

$\delta(F) \geq 2$, with equality for Almost Perfect-Nonlinear (APN) functions.

Jacobian matrix

$F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ with coordinates $(F_1, \ldots, F_m)$ $\quad (e_1, \ldots, e_n) =$ canonical basis of $\mathbb{F}_2^n$.

Jacobian matrix of F:

$$\mathrm{Jac}\, F(x) := \begin{pmatrix} \Delta_{e_1} F_1(x) & \cdots & \Delta_{e_n} F_1(x) \\ \vdots & & \vdots \\ \Delta_{e_1} F_m(x) & \cdots & \Delta_{e_n} F_m(x) \end{pmatrix}$$

When the coordinates of F are in ANF, it is similar to

$$\begin{pmatrix} \frac{\partial F_1}{\partial x_1} & \cdots & \frac{\partial F_1}{\partial x_n} \\ \vdots & & \vdots \\ \frac{\partial F_m}{\partial x_1} & \cdots & \frac{\partial F_m}{\partial x_n} \end{pmatrix}$$

Linear part of the Jacobian matrix when $\deg F = 2$:

$$\mathrm{Jac}_{\mathrm{lin}}\, F(x) := \mathrm{Jac}\, F(x) + \mathrm{Jac}\, F(0)$$

Jacobian matrices of EA-equivalent quadratic functions

Proposition. Let F and G be two EA-equivalent quadratic functions:

$$G = A \circ F \circ B + C$$

Then, for all $x \in \mathbb{F}_2^n$,

$$\mathrm{Jac}_{\mathrm{lin}} G(x) = A_0 \cdot \mathrm{Jac}_{\mathrm{lin}} F(B(x)) \cdot B_0$$

where A_0 and B_0 are the matrices corresponding to the linear parts of A and B.

EA-recovery for quadratic functions

We can assume wlog that $\boldsymbol{B}$ and $\boldsymbol{C}$ are linear.

$$\boldsymbol{A \circ F \circ B(x) + C(x) = A_0 \cdot F(B_0 x + b) + a + C_0 x + c}$$

- The constant part of $\boldsymbol{B}$ can be included in $\boldsymbol{C}$ since

$$\boldsymbol{F(B_0 x + b) = F(B_0 x) + \underbrace{\Delta_b F(B_0 x)}_{\text{affine}}}$$

- The constant parts of $\boldsymbol{C}$ and of $\boldsymbol{\Delta_b F(B_0 x)}$ can be included in $\boldsymbol{a}$.

Algorithm for EA-recovery: basic steps

$$\forall x \in \mathbb{F}_2^n, \quad A_0^{-1} \cdot \mathrm{Jac}_{\mathrm{lin}} G(x) = \mathrm{Jac}_{\mathrm{lin}} F(B_0 x) \cdot B_0$$

Search for pairs (v_i, w_i) such that $B_0 v_i = w_i$.

Choose v_i and w_i such that $\mathrm{Jac}_{\mathrm{lin}} G(v_i)$ and $\mathrm{Jac}_{\mathrm{lin}} F(w_i)$ have the same rank.

Solve the linear system

$$\begin{cases} X \cdot \mathrm{Jac}_{\mathrm{lin}} G(v_i) - \mathrm{Jac}_{\mathrm{lin}} F(w_i) \cdot Y & = & 0 \\ Y \cdot v_i & = & w_i \end{cases} \qquad \forall i \in \{1, \ldots, s\}$$

For each solution $A_0 = X^{-1}$ and $B_0 = Y$, compute

$$\begin{aligned} a &= G(0) + A_0 F(0) \\ C_0 x &= G(x) + A_0 F(B_0 x) + a \end{aligned}$$

Algorithm for EA-recovery: basic steps

$$\forall x \in \mathbb{F}_2^n, \quad A_0^{-1} \cdot \mathrm{Jac}_{\mathrm{lin}} G(x) = \mathrm{Jac}_{\mathrm{lin}} F(B_0 x) \cdot B_0$$

Search for pairs (v_i, w_i) such that $B_0 v_i = w_i$.

Choose v_i and w_i such that $\mathrm{Jac}_{\mathrm{lin}} G(v_i)$ and $\mathrm{Jac}_{\mathrm{lin}} F(w_i)$ have the same rank.

What is the rank distribution of all $\mathrm{Jac}_{\mathrm{lin}} F(x)$?

Solve the linear system

$$\begin{cases} X \cdot \mathrm{Jac}_{\mathrm{lin}} G(v_i) - \mathrm{Jac}_{\mathrm{lin}} F(w_i) \cdot Y & = 0 \\ Y \cdot v_i & = w_i \end{cases} \qquad \forall i \in \{1, \dots, s\}$$

How many pairs (v_i, w_i) do we need?

For each solution $A_0 = X^{-1}$ and $B_0 = Y$, compute

$$\begin{aligned} a &= G(0) + A_0 F(0) \\ C_0 x &= G(x) + A_0 F(B_0 x) + a \end{aligned}$$

Rank distribution of a quadratic function

$$\mathcal{R}(F)[r] := \{u \in \mathbb{F}_2^n \mid \textsf{rank}(\mathrm{Jac}_{\mathrm{lin}} F(u)) = r\}$$

Proposition. For any r, $0 \leq r \leq \min(m, n)$,

$$\#\mathcal{R}(F)[r] = 2^{-r}\#\{(a, b) : \delta_F(a, b) = 2^{n-r}\}$$

Sketch of proof. For any given $u \in \mathbb{F}_2^n$,

$$\mathrm{Jac}_{\mathrm{lin}} F(u) \cdot x = \mathrm{Jac}_{\mathrm{lin}} F(x) \cdot u = \Delta_u F(x) + \Delta_u F(0)$$

Corollary.
F is APN iff $\mathrm{Jac}_{\mathrm{lin}} F(x)$ has rank $(n-1)$ for all $x \neq 0$.

How many pairs $w_i = B_0 v_i$ are needed?

Rank of

$$\begin{cases} X \cdot \mathrm{Jac_{lin}}\, G(v) - \mathrm{Jac_{lin}}\, F(w) \cdot Y &= 0 \\ Y \cdot v &= w \end{cases}$$

$(m^2 + n^2)$ unknowns, $(m+1)n$ equations

$$\textbf{rank} \leq r(m+n-r) + (n-r)$$

where $r = \textbf{rank}\mathrm{Jac_{lin}}\, F(w)$.

$\longrightarrow$ In practice, the rank corresponds to this bound.

For s pairs (v_i, w_i)

$$\textbf{rank} \leq \sum_{i=1}^{s} r_i(m+n-r_i) + (n-r_i)$$

$\longrightarrow$ In practice, the rank is slightly lower.

Experimental results

m	n	$m^2 + n^2$	s	Ranks of $\mathbf{Jac}_{\mathbf{lin}} F(w_i)$	Expected rank	Observed rank
6	6	72	1	3	30	30
6	6	72	1	4	34	34
6	6	72	2	(3,3)	60	50...54
6	6	72	2	(3,4)	64	56...57
6	6	72	2	(4,4)	68	60...61
6	6	72	3	(3,4,4)	72	69...72
6	6	72	3	(4,4,4)	72	66...72

In most cases, $s = 3$ pairs (v_i, w_i) are enough.

Complexity

$$R := \min_{0<r<\min(m,n)} \#\{u \in \mathbb{F}_2^n \mid \textbf{rank}(\mathrm{Jac}_{\mathrm{lin}} F(u)) = r\}$$

In many cases, the number of candidates for $(v_1, w_1), \ldots, (v_s, w_s)$ is roughly R^s.

$$\mathcal{O}\left(\underbrace{\max(n,m)^{\omega} 2^n}_{\text{computation of the rank tables}} + \underbrace{R^s}_{\text{nb of guesses}} (m^2 + n^2)^{\omega} \right)$$

- For random quadratic functions,
  R is small and $s = 3$.

- For quadratic APN functions,
  $R = 2^n - 1$ and $s = 2$,

$$\mathcal{O}\left(2^{2n} n^{2\omega}\right)$$

Examples of running times

Implementation with SageMath

`https://github.com/alaincouvreur/EA_equivalence_for_quadratic_functions`

m	n	Rank distribution	Number of guesses	Time (seconds)
6	6	$[1, 0, 0, 2, 18, 43, 0]$	21	0.68
6	6	$[1, 0, 0, 1, 24, 38, 0]$	386	5.36
6	6	$[1, 0, 0, 0, 27, 36, 0]$	4605	61.1
6	8	$[1, 0, 0, 0, 9, 96, 150]$	127	15.5
6	8	$[1, 0, 1, 12, 98, 144]$	24	13.8
8	6	$[1, 0, 0, 0, 0, 63, 0]$	11067	195.1
8	6	$[1, 0, 0, 0, 3, 60, 0]$	318	53.4
8	8	$[1, 0, 0, 0, 0, 6, 93, 156, 0]$	95	20.3
8	8	$[1, 0, 0, 0, 1, 13, 104, 137, 0]$	36	15.3

EA-testing

EA-testing

Problem:

Given $\{F_i\}_{0\leq i<\ell}$, partition this set in such a way that two functions in distinct subsets are not EA-equivalent.

$\longrightarrow$ testing EA-equivalence between a set of 20,000+ 8-bit quadratic APN functions [Yu-Wang-Li 14][Beierle-Leander 20]

Using EA-invariants:

- Compute EA-invariant(s) and use it for each F_i as a bucket label
- Solve the EA-recovery problem for each pair (F_i, F_j) in the same bucket.

Examples of EA-invariants

Invariant	Condition	
Extended Walsh spectrum		
Differential spectrum		
Γ-rank	$m = n$	[Browning et al. 09]
Δ-rank	$m = n$	[Browning et al. 09]
# Subspaces with dim n in the Walsh zeroes		[Canteaut-Perrin19]
Algebraic degree		
Thickness spectrum		[Canteaut-Perrin19]
Σ^k-spectrum, k even		[Kaleyski 20]
# of subspaces in non-bent components	$\deg(F) = 2$	[Budaghyan et al. 20]

Orthoderivatives of quadratic functions

Definition. Let $F : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$ with $\deg F = 2$.

A function $\pi : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$ is an orthoderivative for F if

$$\forall x, a \in \mathbb{F}_2^n : \ \pi(a) \cdot (\Delta_a F(x) + \Delta_a F(0)) = 0$$

Orthoderivative of quadratic APN functions.

F is APN if and only if it has a unique orthoderivative π such that $\pi(0) = 0$ and $\pi(x) \neq 0$ for all $x \neq 0$.

Orthoderivatives of EA-equivalent quadratic APN functions

Proposition. Let F and G be two EA-equivalent quadratic APN functions:

$$G = A \circ F \circ B + C$$

Then,

$$\pi_G = (A_0^T)^{-1} \circ \pi_F \circ B_0$$

where A_0 and B_0 are the linear parts of A and B.

Any invariant under affine equivalence applied to π_F is an EA-invariant for F.

Invariants of quadratic APN functions based on orthoderivatives

Any invariant under affine equivalence applied to π_F is an EA-invariant for F.

Such invariants have by far the finest grained.

13 classes of 6-bit quadratic APN functions (Banff list).

The differential spectra of the 13 orthoderivatives are all different.

i	Linearity	rank Γ	rank Δ	Differential Spectrum of π_F
1	16	1102	94	$\{0:2205, 2:1764, 8:63\}$
2	16	1146	94	$\{0:2583, 2:1008, 4:378, 8:63\}$
3	16	1158	96	$\{0:2454, 2:1176, 4:370, 6:30, 10:2\}$
4	16	1166	94	$\{0:2338, 2:1428, 4:210, 6:56\}$
5	16	1166	96	$\{0:2373, 2:1428, 4:168, 8:63\}$
6	16	1168	96	$\{0:2442, 2:1229, 4:303, 6:51, 8:7\}$
7	**32**	1170	96	$\{0:2401, 2:1371, 4:195, 6:50, 14:15\}$
8	16	1170	96	$\{0:2426, 2:1255, 4:297, 6:49, 8:5\}$
9	16	1170	96	$\{0:2439, 2:1235, 4:297, 6:57, 8:4\}$
10	16	1170	96	$\{0:2422, 2:1271, 4:279, 6:53, 8:7\}$
11	16	1172	96	$\{0:2385, 2:1339, 4:258, 6:45, 8:2, 12:3\}$
12	16	1172	96	$\{0:2404, 2:1307, 4:261, 6:53, 8:7\}$
13	16	1174	96	$\{0:2414, 2:1271, 4:303, 6:37, 8:7\}$

Invariants of quadratic APN functions based on orthoderivatives

8-bit quadratic APN functions.

21,102 distinct quadratic APN functions from [Yu-Wang-Li 14][Beierle-Leander 20]

The differential and the extended Walsh spectra of their orthoderivatives are different
$\longrightarrow$ All of them belong to different EA-classes (running time: a few minutes)

Conclusions

New algorithms for solving EA-recovery and EA-testing for quadratic functions.

Open problem.

Find general algorithms that could be applied to functions of any degree.