On the Generalized Linear Equivalence of Functions over Finite Fields

L. Breveglieri, A. Cherubini, M. Macchetti

Politecnico di Milano

Outline

- Introduction
- A geometric representation
- Generalized linear equivalence
- Cryptographic robustness
- APN functions
- Conclusions

Introduction (1)

- This paper proposes an extension of the classical concept of “linear equivalence” between functions.
- The concept is applicable to any set of functions f: $F_p^m \Rightarrow F_p^n$, although probably the most interesting case is that of bijective functions (S-boxes) on Fields with even characteristic.
- Early work has been done by Lorens, Harrison, Berlekamp, Denev et al. for vectorial Boolean functions.

Introduction (2)

- The most general instance of classical linear equivalence between two functions
  $f, g : F_p^m \Rightarrow F_p^n$ is:

$$g(x) = Bf(Ax) + Cx$$

- The two functions have essentially the same non-linear behavior, provided that A and B are non-singular matrices over F_p.

Introduction (3)

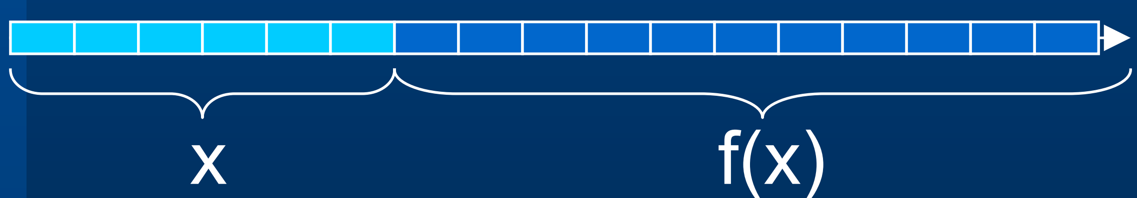
- The DDTs and LATs of two linearly equivalent functions are characterized by the same distributions of values.
- If they are invertible, then this is also true for the inverse functions f^{-1}, g^{-1} that are sometimes quoted to be "cryptographically equivalent".
- But, f^{-1}, g^{-1} are clearly not linearly equivalent to f, g! No formal consistency.
- Do we need a more general definition?

A Geometric Representation (1)

- We can build a geometric representation of function *f* by computing the non-ordered set of vectors:

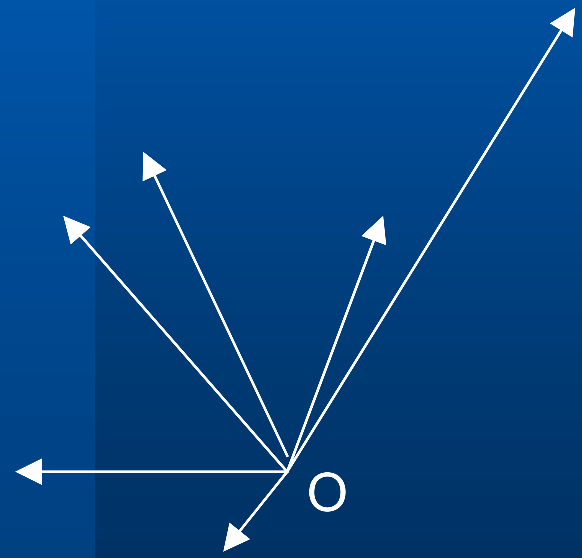
$$\mathbf{F} = \{(x|f(x)),\ x \in F_p^m,\ f(x) \in F_p^n\}$$

- Each vector of the set represents one complete row of the truth table of *f*.



A Geometric Representation (2)

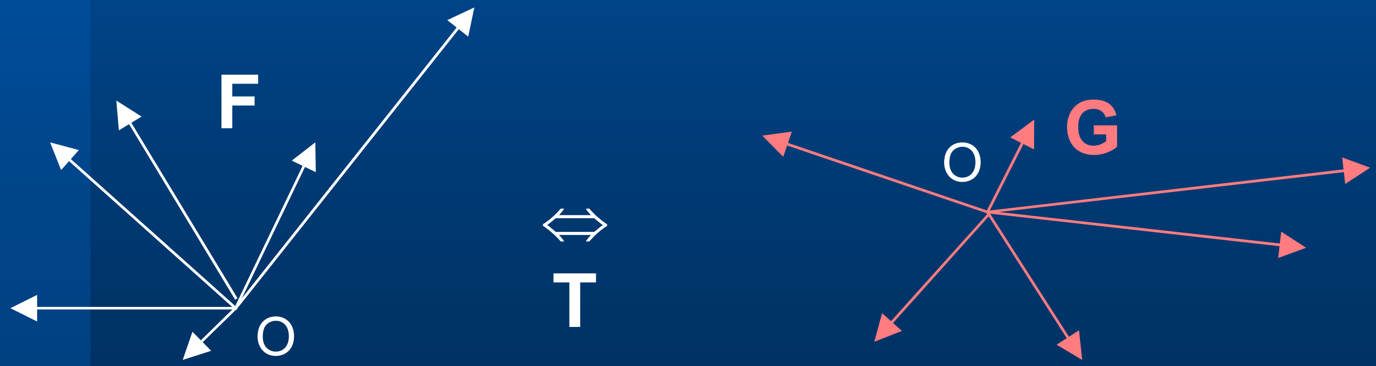
- Every completely specified function is thus associated with a unique *implicit embedding* ***F*** in the linear space F_p^{m+n}.



Not all possible sets of vectors represent functions! For instance, the first *m* components of all vectors must span the whole subspace F_p^m.

Generalized Linear Equivalence (1)

- If we apply an invertible linear transformation of coordinates **T** to the space F_p^{m+n}, the information contained in the set of vectors is not changed; we only change the way we are geometrically looking at this object, **G=T(F)**.



Generalized Linear Equivalence (2)

- Two functions *f,g* are generally linearly equivalent if **G**=**T**(**F**), where T is governed by a non-singular (m+n) × (m+n) matrix over F_p.

$$\begin{array}{c} m \\ n \end{array} \begin{pmatrix} y \\ g(y) \end{pmatrix} = \begin{array}{c} \left(\begin{array}{c:c} \mathbf{A} & \mathbf{D} \\ \hdashline \mathbf{C} & \mathbf{B} \end{array}\right) \\ \begin{array}{cc} m & \quad n \end{array} \end{array} \begin{pmatrix} x \\ f(x) \end{pmatrix}$$

Generalized Linear Equivalence (3)

- G.L.E. is an *extension* of the classical equivalence criterion.
- If *f,g* are classically linearly equivalent, they are also generally linearly equivalent, i.e.

$$g(x) = Bf(A^{-1}x) + CA^{-1}x \;\Leftrightarrow\; \mathbf{G} = \begin{pmatrix} A & 0 \\ C & B \end{pmatrix} \mathbf{F}$$

- Moreover, if *f* is invertible, then f^{-1} is generally linearly equivalent to *f*.

$$\mathbf{F}^{-1} = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} \mathbf{F}$$

Generalized Linear Equivalence (4)

- The most general relation between two G.L.E. functions is:

$$\mathbf{G} = \begin{pmatrix} A & D \\ C & B \end{pmatrix} \mathbf{F}$$

- In this case, the truth-table of *g* is given by the following non-trivial relation, provided that Ax + Df(x) is a permutation function of x.

$$g : Ax + Df(x) \Rightarrow Cx + Bf(x)$$

Cryptographic Robustness (1)

- The cryptographic robustness of a function versus linear and differential analyses is invariant under classical linear equivalence transformations.
- Also, it is invariant under the operation of inversion.
- Can we extend this invariance to generally equivalent functions?

Cryptographic Robustness (2)

- **Theorem**: the distributions of DDT and LAT values for two G.L.E. functions are identical.
- The proof is easy; in the DDT of *f*, every cell contains the number of couples (a,b) such that $b-a=\delta_1$ and $f(b)-f(a)=\delta_2$.
- If we join the two differentials $(\delta_1|\delta_2)=\Delta$, then the cell contains the number of couples (A,B) of vectors of the implicit embedding for which:

$$B-A=\Delta \qquad A=(a|f(a)),\ B=(b|f(b))$$

Cryptographic Robustness (3)

- If *g* is G.L.E. to *f*, then the linear invertible transformation **T** is applied to all the vectors of **F**, i.e.:

$$A' = \mathbf{T}A,\ B' = \mathbf{T}B \quad \Rightarrow \quad B' - A' = \Delta' = \mathbf{T}\Delta$$

- Thus, the number contained in the DDT cell of *f* associated with Δ will be contained in the DDT cell of *g* associated with $\mathbf{T}\Delta$.
- The LAT proof is similar.

Cryptographic Robustness (4)

- The main difference is that while a classical linear transformation rearranges the rows and the columns of the DDTs and LATs, the G.L.E. transformations induce linear rearrangements of the cells in the tables.
- The one-one correspondence between the cells of *f* and *g* is guaranteed by the non-singularity of matrix **T**.
- If the operation is inversion, the tables are merely transposed.

Cryptographic Robustness (5)

- The fact that the distribution of values inside the DDTs and LATs of two G.L.E. functions are equal can be used as a necessary condition by algorithms that check for linear equivalence.
- If the distribution differ, it can be immediately concluded that the functions are not G.L.E. and they are not linearly equivalent as well.
- However, to give a positive answer, optimized algorithms are needed (further research).

APN functions (1)

- Perfect nonlinear functions are characterized by the highest robustness versus differential cryptanalysis.
- In even characteristic, only Almost-Perfect-Nonlinear (APN) functions exist, since the smallest possible global maximum inside the DDT is 2.
- The only known APN functions are power monomials of certain kind (see Dobbertin).

APN functions (2)

- The G.L.E. can be used to find APN functions that are not classically equivalent to power monomials.
- Unfortunately, there is a mistake in the paper: the method used in example 2 is correct, but the function presented is not. We apologize!
- The “addendum” paper contains the correct example that follows; it will be soon made available on the Cryptology e-print archive.

APN functions (3)

- The power monomial x^3 is always APN over $GF(2^n)$ [Gold case]. Moreover, if n is odd, the following is always a permutation polynomial:

$$P(x) = x^3 + x^2 + x$$

- This fact can be used to construct a function which is generally, but not classically, equivalent to x^3. The squaring operation is linear on $GF(2^n)$, thus governed by matrix **S**.
- Let us consider the finite field $GF(2^5)$.

APN functions (4)

$$\begin{pmatrix} y \\ g(y) \end{pmatrix} = \left(\begin{array}{c:c} \mathbf{I+S} & \mathbf{I} \\ \hdashline \mathbf{I} & \mathbf{0} \end{array}\right) \begin{pmatrix} x \\ x^3 \end{pmatrix}$$

- Function g is G.L.E. to x^3 and thus is APN.
- Its truth table is described by the relation:

$$g: x^3 + x^2 + x \Rightarrow x$$

- Lagrange interpolation leads to the explicit form:

$$g(x) = x^{21} + x^{20} + x^{17} + x^{16} + x^5 + x^4 + x$$

APN functions (5)

g(x) cannot be obtained classically from x^3, since only x^{17} can be linearly obtained as $(x^3)^{16}$. All other terms belong to different cosets.

Cyclotomic classification of power monomials over $GF(2^5)$

$C_0=\{0\}$
$C_1=\{1, 2, 4, 8, 16\}$
$C_3=\{3, 6, 12, 24, 17\}$
$C_5=\{5, 10, 20, 9, 18\}$
$C_7=\{7, 14, 28, 25, 19\}$
$C_{11}=\{11, 22, 13, 26, 21\}$
$C_{15}=\{15, 30, 29, 27, 23\}$

APN functions (6)

g(x) defined over $GF(2^3)$ gives:

$g(x) = x^5 + x^4 + x$

which is classically linearly equivalent to x^3. Error in ex.2! See "addendum" paper.

Cyclotomic classification of power monomials over $GF(2^3)$

$C_0 = \{ 0 \}$
$C_1 = \{ 1, 2, 4 \}$
$C_3 = \{ 3, 6, 5 \}$

APN functions (7)

- Function g defined over $GF(2^7)$ is:

$$g(x) = x^{85} + x^{84} + x^{81} + x^{80} + x^{69} + x^{68} + x^{65} + x^{64} + x^{21} + x^{20} + x^{17} + x^{16} + x^5 + x^4 + x$$

- The method provides actually a family of previously unknown APN permutations.
- Other families may be obtainable using different permutation polynomials.
- Further research needed.

Conclusions

- We have introduced an extension of the concept of functional linear equivalence.
- Known cases become special instances of G.L.E.
- The cryptographic robustness is invariant under the analyzed transformations.
- We have discovered a family of unknown APN permutations over $GF(2^n)$, n odd.
- www.macchetti.name
- Thank you for the attention!