Aalto University
School of Science

Computing Averages over Fixed Inputs and Links between Linear and Differential Attacks

Kaisa Nyberg

Department of Information and Computer Science
Aalto University School of Science

ESC 2013

January 16, 2013

Introduction

Introduction

Leander 2011 proved that

Statistical Saturation Attack [Collard-Standaert 2009]

$\Leftrightarrow$

Multidimensional Linear Cryptanalysis [Hermelin-Nyberg 2009]

in the following sense:
If $F(x, z) = y$ then the average non-uniformity of the distributions of the values

$$y \text{ , as } z \text{ takes on all values}$$

computed over all fixed values x is equal to the non-uniformity of the distribution of the values

$$(x, y) \text{ , as } x \text{ and } z \text{ take on all values}$$

Overview

This talk presents:

- remarks on the equivalence proof,
- implications on actual attacks,
- further links,

and is based on joint work and discussions with C. Blondeau, A. Bogdanov, and G. Leander.

The Fundamental Theorem

Notation

$f : \mathbb{F}_2^n \to \mathbb{F}_2$ Boolean function

$$\hat{f}(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle u,x \rangle + f(x)}$$

$$\mathbf{Pr}(\langle u, x \rangle + f(x) = 0) = \frac{c+1}{2}$$

$$c = \mathbf{cor}(\langle u, x \rangle + f(x)) = \mathbf{cor}_f(u) = \frac{\hat{f}(u)}{2^n}$$

The Fundamental Theorem

$$f : \mathbb{F}_2^r \times \mathbb{F}_2^s \to \mathbb{F}_2 \quad \hat{f}(u,v) = \sum_{x \in \mathbb{F}_2^r,\, z \in \mathbb{F}_2^s} (-1)^{\langle u,x\rangle + \langle v,z\rangle + f(x,z)}$$

$$f_x(z) = f(x,z),\ f_x : \mathbb{F}_2^s \to \mathbb{F}_2,\ x \in \mathbb{F}_2^r$$

Theorem *For all* $v \in \mathbb{F}_2^s$

$$2^r \sum_{x \in \mathbb{F}_2^r} \widehat{f_x}(v)^2 = \sum_{u \in \mathbb{F}_2^r} \hat{f}(u,v)^2, \quad \textit{or equivalently,}$$

$$2^{-r} \sum_{x \in \mathbb{F}_2^r} \mathbf{cor}_{f_x}(v)^2 = \sum_{u \in \mathbb{F}_2^r} \mathbf{cor}_f(u,v)^2.$$

A. Canteaut, C. Carlet, P. Charpin, C. Fontaine. On cryptographic properties of the cosets of r(1, m). IEEE Trans. IT 47(4), 14941513 (2001)

N. Linial, Y. Mansour and N. Nisan. Constant depth circuits, Fourier transform, and learnability. Journal of the ACM 40 (3), 607-620 (1993).

The Fundamental Theorem

Theorem *Let X, Z and Y be random variables in $\mathbb{F}_2^m$, $\mathbb{F}_2^\ell$, and $\mathbb{F}_2^n$, resp. where $Y = F(X, Z)$ and X and Z are independent. If Z is uniformly distributed, then for all $a \in \mathbb{F}_2^m$ and $b \in \mathbb{F}_2^n$,*

$$\mathrm{Exp}_Z \mathbf{cor}(\langle a, X\rangle + \langle b, Y\rangle)^2 = \sum_{c \in \mathbb{F}_2^\ell} \mathbf{cor}(\langle a, X\rangle + \langle b, Y\rangle + \langle c, Z\rangle)^2.$$

Application to $F(X, Z) = E_Z(X)$ gives the Linear Hull Theorem.

Usage: From average behaviour over all keys deduce information about the behaviour in the case of the fixed unknown key.

K. Nyberg: Linear approximation of block ciphers. In: Advances in Cryptology - EUROCRYPT'94, LNCS 950, 439-444 (1995)

Partially Fixed Plaintext

Statistical Saturation Link

[Leander 2011]

$$F : \mathbb{F}_2^r \times \mathbb{F}_2^s \to \mathbb{F}_2^k$$

$$2^{-r} \sum_{x \in \mathbb{F}_2^r} \sum_{w \in \mathbb{F}_2^k} \mathbf{cor}(\langle w, F(x,z) \rangle)^2 = \sum_{u \in \mathbb{F}_2^r} \sum_{w \in \mathbb{F}_2^k} \mathbf{cor}(\langle u, x \rangle + \langle w, F(x,z) \rangle)^2$$

The expression on the right is the capacity of the multidimensional linear approximation

$$\langle u, x \rangle + \langle w, F(x,z) \rangle, u \in \mathbb{F}_2^r,\ w \in \mathbb{F}_2^k.$$

Running the known plaintext multidimensional linear attack takes 2^{r+k} memory.

Sampling for evaluation of the expression on the left can be done with 2^k memory using chosen plaintext.

Question: How much the behaviour for a fixed x differs from the average behaviour?

Integral Link

[Bogdanov et al. 2012]

The SSA link gives

$$2^{-r} \sum_{x \in \mathbb{F}_2^r} \sum_{w \in \mathbb{F}_2^k \setminus \{0\}} \mathbf{cor}(\langle w, F(x,z) \rangle)^2$$

$$= \sum_{u \in \mathbb{F}_2^r} \sum_{w \in \mathbb{F}_2^k \setminus \{0\}} \mathbf{cor}(\langle u, x \rangle + \langle w, F(x,z) \rangle)^2$$

$\mathbf{cor}(\langle w, F(x,z) \rangle) = 0$, for all $x \in \mathbb{F}_2^r$ and $w \in \mathbb{F}_2^k \setminus \{0\}$ means that we have an integral distinguisher. By the SSA link, it means that

$$\mathbf{cor}(\langle u, x \rangle + \langle w, F(x,z) \rangle) = 0, \ u \in \mathbb{F}_2^r, \ w \in \mathbb{F}_2^k, \ (u,w) \neq (0,0),$$

that is, we have a zero-correlation distinguisher.

New Link

Truncated Differential Link

[Blondeau-Nyberg 2013]
The link between differential and linear cryptanalysis [Chabaud-Vaudenay 1994] we obtain

$$\sum_{u\in\mathbb{F}_2^r,\, w\in\mathbb{F}_2^k} \mathbf{cor}(\langle u,x\rangle + \langle w,F(x,z)\rangle)^2 = 2^{s-k} \sum_{\delta\in\mathbb{F}_2^s} \mathbf{Pr}(F(x,z+\delta)+F(x,z)=0)$$

For $s = k$, we obtain

$$\sum_{(u,w)\in\mathbb{F}_2^r\times\mathbb{F}_2^s\setminus\{(0,0)\}} \mathbf{cor}(\langle u,x\rangle + \langle w,F(x,z)\rangle)^2 = \sum_{\delta\in\mathbb{F}_2^s\setminus\{0\}} \mathbf{Pr}(F(x,z+\delta)+F(x,z)=0)$$

- Non-uniformity of the distribution of $(x, F(x,z))$ is equal to the sum of probabilities of all nontrivial differentials $(0,\delta) \to 0$.
- Zero-correlation distinguisher is equivalent to impossible differential distinguisher.

Conclusions

- The Fundamental Theorem and its different appearances discussed
- Old and new mathematical links between attacks presented
- Implications of the links to attack complexities remains to be studied

Thanks for your attention!