Aalto University
School of Science

Cryptographic Nonlinearity

Kaisa Nyberg

Department of Information and Computer Science
Aalto University

Reed Muller Workshop 2011

May 26, 2011

Linear Cryptanalysis

Highly Nonlinear Boolean Functions

Generalizations

Open Problem

Linear Cryptanalysis

Encryption System

$K \in \mathcal{K}$	the key
$x \in \mathcal{P}$	the plaintext
$y \in \mathcal{C}$	the ciphertext

Encryption system is a family $\{E_K\}$ of transformations

$$E_K : \mathcal{P} \rightarrow \mathcal{C}$$

parametrised using the key K such that, for each encryption transformation E_K, there is a decryption transformation

$$D_K : \mathcal{C} \rightarrow \mathcal{P}$$

such that

$$D_K(E_K(x))) = x, \text{ for all } x \in \mathcal{P}.$$

Block Cipher

$\mathcal{P} = \mathcal{C} = \mathbb{F}_2^n$
$\mathcal{K} = \mathbb{F}_2^\ell$

The data to be encrypted is split into blocks

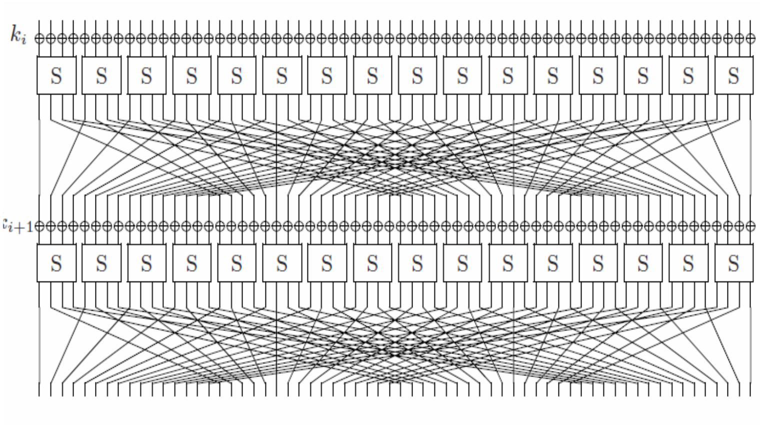
$$x_i, \ = 1, \ldots, N$$

of fixed length n.

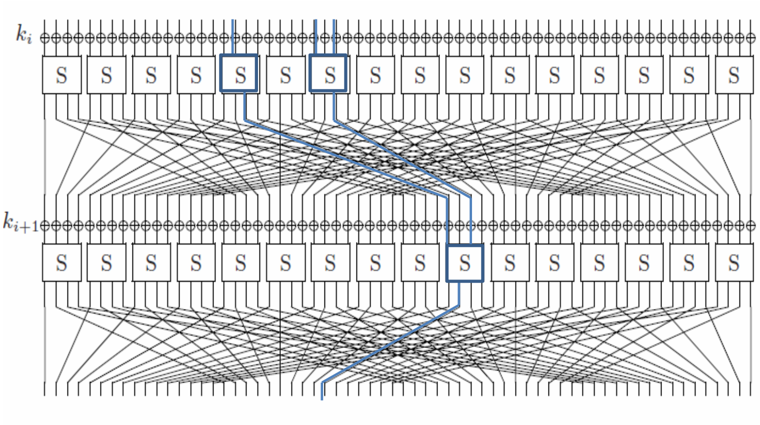
Typically $n = 128$ and $\ell = 128$

Still today designed as proposed by Claude Shannon 1949: alternating layers of diffusions and confusions.

Block Cipher Building Blocks



Linear Approximation of Block Cipher

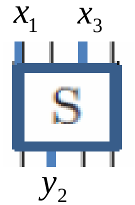


Trail Correlation

Piling-up lemma: The strength of a linear approximation trail is measured as the product of building block correlations.

Building block correlation is taken between $\oplus$ of all input bits and $\oplus$ of all output bits involved in the approximation.

Linear building block: correlation = 1
Nonlinear building block: | correlation | < 1
Linear trails are said to exist only if correlation $\neq$ 0
Also correlations = 0 can be meaningful



correlation between $x_1 \oplus x_3$ and y_2

Correlation over Block Cipher

- Correlation of linear approximation over block cipher is taken between

  $\oplus$ of all plaintext bits and $\oplus$ of all ciphertext bits

  involved in the approximation.
- Typically there exist many approximation trails involving the same plaintext bits and ciphertext bits.
- One trail correlation dominates: Correlation computed as trail correlation.
- Several trails with large correlations (Linear hull): Correlation (squared) is computed as the sum of all significant trail correlations (squared) [KN 1994]

Block Cipher PRESENT

- Recent design targeted for lightweight applications
- Abundant in single-bit strong linear approximation trails
- Best known attack (other than exhaustive key search) due to Joo Cho [2010]
  - breaks 26 out of 31 rounds
  - exploits linear hulls and multidimensional linear cryptanalysis developed by us
- The effect of linear hulls underestimated by the designers of PRESENT [Gregor Leander, Eurocrypt 2011]

Highly Nonlinear Boolean Functions

Binary Vector Space

- $\mathbb{F}_2^n$ the space of *n*-dimensional binary vectors
- $\oplus$ sum modulo 2
- Given two vectors

$$a = (a_1, \ldots, a_n),\ \ b = (b_1, \ldots, b_n) \in \mathbb{F}_2^n$$

the inner product (dot product) is defined as

$$a \cdot b = a_1 b_1 \oplus \cdots \oplus a_n b_n.$$

Boolean Function

- $f : \mathbb{F}_2^n \mapsto \mathbb{F}_2$ Boolean function.
- Linear Boolean function is of the form $f(x) = u \cdot x$, where $u \in \mathbb{F}_2^n$ is called a linear mask.
- $f : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ with $f = (f_1, \ldots, f_m)$, where f_i are Boolean functions, is called a vector Boolean function.

Correlation

- The correlation between Boolean functions $f : \mathbb{F}_2^n \to \mathbb{F}_2$ and $\mathbb{F}_2^n \to \mathbb{F}_2$, $x \mapsto u \cdot x$ is defined as

$$c(f, u) = \frac{1}{2^n} \left(\#\{x \in \mathbb{F}_2^n \mid f(x) = u \cdot x\} - \#\{x \in \mathbb{F}_2^n \mid f(x) \neq u \cdot x\}\right)$$

- Linear cryptanalysis makes use of large correlations between Boolean functions and linear approximations derived from cipher constructions.

Parseval's Theorem and Bent Functions

- *Parseval's Theorem*

$$\sum_{u \in \mathbb{F}_2^n} c(f,u)^2 = 1.$$

- A Boolean function is called *bent* if

$$|c(f,u)| = 2^{-\frac{n}{2}}, \text{ for all } u \in \mathbb{F}_2^n.$$

[Rothaus1976][Dillon1978]

- Theorem. If $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is bent then n is even.
- Meier and Staffelbach [1988] introduced the notion of perfect nonlinearity of Boolean functions as an important cryptographic criterion, and later observed that it is equivalent to bentness.

Vectorial Bent Functions

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a vector Boolean function. Then the following are equivalent [KN1991]

- f is *bent*, that is, $w \cdot f$ is bent, for all $w \neq 0$;
- f is *perfect nonlinear* (PN), that is,

$$f(x \oplus \alpha) \oplus f(x)$$

  is uniformly distributed as x varies, for all fixed $\alpha \in \mathbb{F}_2^n \setminus \{0\}$.

Theorem [KN1991]. If $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is bent then $n \geq 2m$.

APN S-Boxes

Let $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ be an S-box. Then f is said to be *almost perfect nonlinear* (APN) if $f(x \oplus \alpha) \oplus f(x)$ is as uniformly distributed as possible, as x varies, for all fixed $\alpha \in \mathbb{F}_2^n \setminus \{0\}$.

- The function
$$f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n,\ f(x) = x^{2^k+1},$$
with multiplication in $\mathbb{F}_{2^n}$ is APN.
- This function is bijective only for odd n [KN1993]

Highly Nonlinear S-Boxes

- $$f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n,\ f(x) = x^{-1},\ f(0) = 0$$
  with multiplication in $\mathbb{F}_{2^n}$ is bijective.
- For odd n, it is APN, and for even n,
  $$\#\{x \,|\, f(x \oplus \alpha) \oplus f(x) = \beta\} \leq 4,$$
  for all $\alpha \neq 0$ and β.
- In addition, all correlations $|c(w \cdot f(x) \oplus u \cdot x)|$ are upperbounded by $2^{-\frac{n}{2}+1}$ [KN1993].
- Was adapted as the core of the S-box for the Rijndael block cipher in 1998 to become the AES in 2001.

Discrete Logarithm

The n-bit *discrete logarithm* S-box $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ is defined as

$$f(x) = \begin{cases} \log_\alpha(x), & \text{for } x \neq 0 \\ (1, 1, \ldots, 1,) & \text{for } x = 0. \end{cases}$$

where α is a generator of $(\mathbb{F}_{2^n}, \times)$, x is considered as an element in $\mathbb{F}_{2^n}$, and n-bit integers $\log_\alpha(x)$ and $2^n - 1$ are considered as elements in $\mathbb{F}_2^n$.

For any single bit of f, its correlation with any linear function is upperbounded by

$$\mathcal{O}(n 2^{-n/2}).$$

For multiple-bit maskings no useful upperbound known.

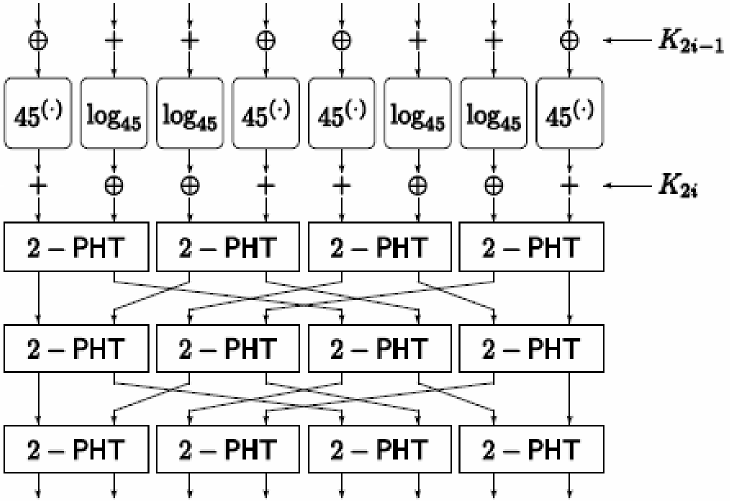
The best known bounds for the inverse of f

$$f^{-1}(y) = \begin{cases} \alpha^y, & \text{for } y \neq (1, 1, \ldots, 1) \\ 0, & \text{for } y = (1, 1, \ldots, 1). \end{cases}$$

is $\mathcal{O}(n^{1/4} 2^{-n/8})$ [Shparlinski and Winterhof, 2006]

Generalized Linearity

SAFER Block Cipher



Non-binary mod 256 Diffusion

$$[\text{2-PHT}](x, y) = (2x + y, x + y), \;\; x, y \in \mathbb{Z}_{256}$$

$$M = \begin{pmatrix} 8 & 4 & 4 & 2 & 4 & 2 & 2 & 1 \\ 4 & 2 & 2 & 1 & 4 & 2 & 2 & 1 \\ 4 & 4 & 2 & 2 & 2 & 2 & 1 & 1 \\ 2 & 2 & 1 & 1 & 2 & 2 & 1 & 1 \\ 4 & 2 & 4 & 2 & 2 & 1 & 2 & 1 \\ 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 \\ 2 & 2 & 2 & 2 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Generalized Bent Functions

Let $q \geq 2$ be integer and denote

$$e_q(x) = e^{\frac{2\pi x}{q} i}.$$

$f : \mathbb{F}_2^n \to \mathbb{F}_2$ is bent if and only if

$$|\sum_{x \in \mathbb{F}_2^n} e_2(f(x) \oplus u \cdot x)| = 2^{\frac{n}{2}}, \text{ for all } u \in \mathbb{F}_2^n.$$

Kumar-Scholtz-Welch [1985]:
$f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ is *generalized bent* if

$$|\sum_{x \in \mathbb{Z}_q^n} e_q(f(x) - ux)| = q^{\frac{n}{2}}, \text{ for all } u \in \mathbb{Z}_q^n.$$

Existence

- Theorem. For all odd primes p and all positive n, there exist generalized bent functions $f : \mathbb{Z}_p^n \to \mathbb{Z}_p$.
- Example. $f : \mathbb{Z}_p \to \mathbb{Z}_p$, $f(x) = x^2$.

$$\begin{aligned}
|\sum_{x \in \mathbb{Z}_p} e_p(x^2 - ux)|^2 &= (\sum_{x \in \mathbb{Z}_p} e_p(x^2 - ux))(\sum_{y \in \mathbb{Z}_p} \overline{e_p(y^2 - uy)}) \\
&= \sum_x e_p(x^2 - ux)) \sum_y \overline{e_p((x-y)^2 - u(x-y)))} \\
&= \sum_{x,y} e_p(x^2 - ux - (x-y)^2 + u(x-y)) \\
&= \sum_y e_p(-y^2 - uy) \sum_x e_p(2xy) \\
&= p
\end{aligned}$$

- This function is not bijective.

Generalized Correlation

- Baignéres, Vaudenay, Stern [2007]: Additive groups
- Drakakis, Requena, McGuire [2010]: $\mathbb{Z}_p$ and $\mathbb{Z}_{p-1}$
- Feng, Zhou, Wu, Feng [2011]: Subsets of $\mathbb{Z}_{2^n}$
- For any positive integers q and p and $f : A \to \mathbb{Z}_p$, where A is a subset of $\mathbb{Z}_q$, we define

$$c(wf(x), ux) = \frac{1}{|A|} \sum_{x \in A} e_p(wf(x)) \overline{e_q(ux)}$$

8×8-bit S-boxes of SAFER

$$f(x) = (45^x \bmod 257) - 1,\ x \in \mathbb{Z}_{256}$$

and its inverse

$$f^{-1}(y) = \log_{45}(y + 1),\ y \in \mathbb{Z}_{256}$$

Nonlinearity?

Welch-Costas Functions

p odd prime
g generator of the multiplicative group in $\mathbb{F}_p$

Exponential Welch-Costas function

$$f(x) = (g^x \bmod p) - 1,\ x \in \mathbb{Z}_{p-1}$$

and its inverse, namely, *logarithmic Welch-Costas function*

$$f^{-1}(y) = \log_g(y+1),\ y \in \mathbb{Z}_{p-1}$$

are bijections in $\mathbb{Z}_{p-1}$.

Drakakis, Requena, McGuire [2010] conjectured asymptotic upperbound for absolute values of correlations.
Hakala [2011] proved even a stronger upperbound $\mathcal{O}(p^{-\frac{1}{2}} \log p)$.

Almost Linear Embedding $\mathbb{Z}_p \setminus \{0\} \to \mathbb{Z}_{p-1}$

- Lemma [Hakala2011]. Let $\phi : \mathbb{Z}_p \setminus \{0\} \to \mathbb{Z}_{p-1}$ be defined as $\phi(y) = y - 1$. Then for all $v \in \mathbb{Z}_p$ and $w \in \mathbb{Z}_{p-1}$, $w \neq 0$, we have

$$\sum_{v \in \mathbb{Z}_p} |c(w\phi(y), vy)| \quad \leq \quad C \log p.$$

- Proof based on an idea of L. J. Mordell [1972].
- For any function $f : \mathbb{Z}_p \to \mathbb{Z}_p$

$$1 \leq \sum_{v \in \mathbb{Z}_p} |c(f(x), vx)| \leq p^{\frac{1}{2}},$$

  where the equality on the left hand side is obtained by linear functions of the form $f(x) = vx$, and on the right hand side by bent functions.
- The embedding $\phi : \mathbb{Z}_p \setminus \{0\} \to \mathbb{Z}_{p-1}$ is hence closer to the linear side. Is it the most linear in this sense?

Exponentiation $\mathbb{Z}_{p-1} \to \mathbb{Z}_p$ Perfect Nonlinear

- Exponentiation $\mathbb{Z}_{p-1} \to \mathbb{Z}_p \setminus \{0\}$ is perfect nonlinear, that is,
$$x \mapsto g^{x+\alpha} - g^x = g^x(g^\alpha - 1)$$
is bijective for all $\alpha \neq 0$.
- It follows:

Theorem [Drakakis-Requena-McGuire 2011].

$$|c(vg^x \bmod p, ux)| = \begin{cases} p^{-\frac{1}{2}}, & \text{for } u \neq 0 \\ p^{-1}, & \text{for } u = 0. \end{cases}$$

Bounds for Correlations of Exponential Costas-Welch

- Compute the correlation of the composition

$$\begin{array}{cccccc} f: & x & \mapsto & g^x & \mapsto & g^x - 1 \\ & \mathbb{Z}_{p-1} & \to & \mathbb{Z}_p & \to & \mathbb{Z}_{p-1} \end{array}$$

- Then

$$\begin{aligned} |c(wf(x), ux)| &\leq \sum_{v \in \mathbb{Z}_p} |c(w\phi(z), vz)||c(vg^x, ux)| \\ &\leq p^{-\frac{1}{2}} \sum_{v \in \mathbb{Z}_p} |c(w\phi(z), vz)| \\ &\leq Cp^{-\frac{1}{2}} \log p. \end{aligned}$$

Open Problems

Logarithm and Exponent Functions in $\mathbb{F}_2^n$

- $\phi : \mathbb{Z}_p \to \mathbb{Z}_{p-1}$ almost linear
- Problem: Can this approach be applied to the exponent function in $\mathbb{F}_2^n$ where exponentiation is taken in $\mathbb{F}_{2^n}$?

$$f(y) = \begin{cases} \alpha^y, & \text{for } y \neq (1, 1, \ldots, 1) \\ 0, & \text{for } y = (1, 1, \ldots, 1) \end{cases}$$

- Similar perfect nonlinearity as in $\bmod p$ case
- Natural embeddings

$$\mathbb{F}_2^n \setminus \{(1, 1, \ldots, 1)\} \to \mathbb{Z}_{2^n-1} \text{ or } \mathbb{F}_2^n \to \mathbb{Z}_{2^n}$$

not very linear, indeed, addition $\bmod 2^n$ and addition $\bmod 2^{n-1}$ are commonly used nonlinear components in cipher constructs.