Links between Differential and Linear Cryptanalysis

Florent CHABAUD
Serge VAUDENAY

Laboratoire d'Informatique, URA 1327 du CNRS
Département de Mathématiques et d'Informatique
Ecole Normale Supérieure

LIENS - 94 - 3

March 1994

Links between differential and linear cryptanalysis

Florent Chabaud Serge Vaudenay

Groupe de Recherche En Complexité et Cryptographie

March 9, 1994

Links between differential and linear cryptanalysis

Florent Chabaud[1]
Florent.Chabaud@ens.fr

Serge Vaudenay
Serge.Vaudenay@ens.fr

Groupe de Recherche En Complexité et Cryptographie
Laboratoire d'Informatique de l'ENS
45, rue d'Ulm
75230 Paris Cedex 05

March 9, 1994

Résumé

La cryptanalyse linéaire a été introduite l'an dernier par Matsui au congrès Eurocrypt '93. Elle ouvre des perspectives pour de nouvelles méthodes d'attaques plus performantes que la cryptanalyse différentielle.

Dans ce rapport, nous étudions plusieurs classes de fonctions qui sont parmi les plus difficiles à cryptanalyser par les méthodes différentielle d'une part, linéaire de l'autre, et nous obtenons des relations entre ces classes.

Les fonctions différentiellement résistantes correspondent à des propriétés de non-linéarité liées aux fonctions courbes. Nous montrons que les fonctions linéairement résistantes sont aussi liées aux fonctions courbes, et qu'en un certain sens, une fonction linéairement résistante est aussi différentiellement résistante.

Abstract

Linear cryptanalysis, introduced last year by Matsui, will most certainly open-up the way to new attack methods which may be made more efficient when compared or combined with differential cryptanalysis.

This report exhibits new relations between linear and differential cryptanalysis and presents new classes of functions which are optimally resistant to these attacks. In particular, we prove that linear-resistant functions, which generally present Bent properties, are differential-resistant as well and thus, present Perfect Nonlinear properties.

[1]On leave from *Délégation Générale de l'Armement*

— I

Introduction

Matsui has introduced last year a new cryptanalysis method for DES-like cryptosystems [Mat94]. The idea of the method is to approximate the non-linear S-boxes with linear forms. Beside, the performances of linear cryptanalysis seems next to differential cryptanalysis ones, though a little better. These similitudes seem to mean that the two methods are based on common fundamental principles.

Each type of cryptanalysis measures the resistance of functions. In this report, we investigate functions $F : K^p \to K^q$, where K is the Galois field with two elements, and p and q are two integers. Using well known results on Bent functions we will show that linear resistant functions are also differential resistant.

I-1° Notations

- We call "characteristic function of F" and denote θ_F the boolean function

$$\begin{aligned} \theta_F : K^p \times K^q &\to K \\ \theta_F(x,y) &\mapsto \begin{cases} 1 & \text{if } y = F(x), \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

- Let $f : K^p \to \mathbb{R}$ be a function, we denote by $\hat{f}$ the Hadamard-Walsh transform (discrete Fourier transform):

$$\forall w \in K^p \quad \hat{f}(w) = \sum_{x \in K^p} f(x)(-1)^{x.w},$$

  where $x.w$ is the dot-product over K and where the sum is evaluated over the reals.

- Let f and g be two functions over K^p, we denote $f \otimes g$ the convolutional product

$$\forall a \in K^p \quad (f \otimes g)(a) = \sum_{x \in K^p} f(x) g(a \oplus x),$$

  where $\oplus$ is the sum over K^p (bit-wise Xor).

- Let $f : K^p \to K$ be a boolean function, we denote by $\chi_f(x) = (-1)^{f(x)}$ the ± 1-representation of f.

I-2° Cryptanalysis objects

Let $F : K^p \to K^q$ be the function we want to cryptanalyse. If we use the differential cryptanalysis method, we will need non empty sets

$$D_F(a,b) = \{z \in K^p \ / \ F(z \oplus a) \oplus F(z) = b\},$$

where $a \in K^p - \{0\}$ and $b \in K^q$. The efficiency of differential cryptanalysis based upon a set $D_F(a,b)$ is measured by its cardinality

$$\delta_F(a,b) = \# D_F(a,b).$$

Similarly, if we use the linear cryptanalysis method, we will take advantage of sets

$$L_F(a,b) = \{z \in K^p \ / \ a.z \oplus b.F(z) = 0\},$$

where $a \in K^p$ and $b \in K^q - \{0\}$, such that $\# L_F(a,b) \neq \frac{|K^p|}{2}$. The efficiency of linear cryptanalysis that uses the set $L_F(a,b)$ is measured by the discrepency between the cardinality of $L_F(a,b)$ and the average cardinality

$$\lambda_F(a,b) = \# L_F(a,b) - \frac{|K^p|}{2}.$$

Hence the resistance of the function F can be measured by:

$$\begin{aligned} \Delta_F &= \sup_{a \neq 0, b} \delta_F(a,b) \text{ for the differential cryptanalysis.} \\ \Lambda_F &= \sup_{b \neq 0, a} |\lambda_F(a,b)| \text{ for the linear cryptanalysis.} \end{aligned}$$

The lower these values are, the more resistant the function F will be against the corresponding cryptanalysis method.

Note 1 *If $\Delta_F = \delta$, then F is said differentially δ-uniform [Nyb94].*

Definition 1 *For a given set $\mathcal{F}$ of functions, we will say a function $F \in \mathcal{F}$ is differential resistant in $\mathcal{F}$ if Δ_F is minimal. As the same, we will say F is linear resistant in $\mathcal{F}$ if Λ_F is minimal.*

I-3° Bent functions

We just recall here the definitions of Bent functions.

Definition 2 *Let p be an even integer. A boolean function f over K^p is called Bent if and only if*

$$\forall s \in K^p \widehat{\chi_f}(s) = \pm 2^{p/2}.$$

In fact, $2^{p/2}$ is an absolute lower bound for $\sup_{s \in K^p} |\widehat{\chi_f}(s)|$. Hence, the Bent functions are exactly those which reach this bound. This definition has been extended by Nyberg [Nyb91]:

Definition 3 *A function $F : K^p \to K^q$ is Bent if and only if, for all $c \in K^q$ the boolean function $x \mapsto c.F(x)$ is Bent.*

This is equivalent to

$$\forall c \neq 0 \forall s \quad \hat{\theta}_F(s,c) = \pm 2^{p/2},$$

as $\widehat{\chi_{c.F}}(s) = \hat{\theta}_F(s,c)$. Thus, $2^{p/2}$ is a lower bound for $\sup_{s \in K^p, c \neq 0} |\hat{\theta}_F(s,c)|$. Hence, the vectorial Bent functions are exactly those which reach this bound.

— II

Resistance to cryptanalysis

In the following, we still consider the set $\mathcal{F}$ of the functions $F : K^p \to K^q$ with p and q fixed integers.

II-1° Differential resistant functions in $\mathcal{F}$

Resistance to differential cryptanalysis have already been studied. We just recall here a few results.

Lemma 1 *For all (a, b) in $K^p \times K^q$, we have $\delta_F(a, b) = (\theta_F \otimes \theta_F)(a, b)$.*

Proof: We have:

$$\begin{aligned}(\theta_F \otimes \theta_F)(a,b) &= \sum_{x \in K^p, y \in K^q} \theta_F(x,y)\theta_F(a \oplus x, b \oplus y) \\ &= \sum_{x \in K^p} \theta_F(a \oplus x, b \oplus f(x)) \\ &= \#\{x \in K^p \ / \ b \oplus f(x) = f(a \oplus x)\} \\ &= \delta_F(a,b).\end{aligned}$$

Theorem 1 *For any mapping F, we have $\Delta_F \geq 2^{p-q}$.*

Proof: It is easy to see that for all fixed $a \in K^p$, we have $\sum_{b \in K^q} \delta_F(a, b) = 2^p$, which ensures the result.

Note that this bound cannot be reached if $p < q$ as this is not an integer. We still define:

Definition 4 *A function F is called Perfect Nonlinear if and only if $\Delta_F = 2^{p-q}$.*

II-2° Linear resistant functions in $\mathcal{F}$

Lemma 2 *For all (a, b) in $K^p \times K^q$, we have $\lambda_F(a, b) = \frac{1}{2}\hat{\theta}_F(a, b)$.*

Proof: We have:

$$\begin{aligned}\hat{\theta}_F(a,b) &= \sum_{x\in K^p, y\in K^q} \theta(x,y)(-1)^{a.x\oplus b.y} \\ &= \sum_{x\in K^p} (-1)^{a.x\oplus b.F(y)} \\ &= |L_F(a,b)| - (2^p - |L_F(a,b)|) \\ &= 2\lambda_F(a,b).\end{aligned}$$

The theory of Bent functions shows that $2^{p/2}$ is an absolute lower bound for $\sup|\theta_F(a,b)|$ (see section I-3°). The functions which reach this bound are precisely vectorial Bent functions. Hence, when p and q are such that this bound can be reached, the linear resistant functions are the vectorial Bent functions.

II-3° Links between the absolute bounds

Theorem 2 ([Nyb91, MS90]) *A function is Perfect Nonlinear if and only if it is Bent.*

Proof: Let $F : K^p \to K^q$ be a Perfect Nonlinear function. Then $\Delta_F = 2^{p-q}$, and so for all $a \neq 0$, $\delta_F(a,b) = (\theta_F \otimes \theta_F)(a,b) = 2^{p-q}$. Besides, $\delta_F(0,0) = 2^p$, and for all $a \neq 0$ $\delta_F(a,0) = 0$. Hence, we get

$$\begin{aligned}(\hat{\theta}_F)^2(a,b) &= (\widehat{\theta_F \otimes \theta_F})(a,b), \\ &= \sum_{x,y} (\theta_F \otimes \theta_F)(x,y)(-1)^{a.x\oplus b.y}, \\ &= 2^p + 2^{p-q} \sum_{x\neq 0,y} (-1)^{a.x\oplus b.y}, \\ &= \begin{cases} 2^p & \text{if } b \neq 0, \\ 0 & \text{if } b = 0 \text{ and } a \neq 0, \\ 2^{2p} & \text{if } a = b = 0.\end{cases}\end{aligned}$$

So F is Bent as $\hat{\theta}_F(a,b) = \pm 2^{p/2}$ for all $(a,b), b \neq 0$. The converse can be proved similarly using the classical Walsh transform formulas:

$$(\theta_F \otimes \theta_F)(a,b) = \frac{1}{2^{p+q}} (\widehat{\widehat{\theta_F \otimes \theta_F}})(a,b) = \frac{1}{2^{p+q}} (\widehat{\hat{\theta}_F})^2.$$

Theorem 3 ([Nyb91]) *Bent functions exist only for $p \geq 2q$ and p even.*

Proof: If F is Bent, then for all $b \neq 0$, $\hat{\theta}_F(a,b) = \pm 2^{\frac{p}{2}}$. Hence, p is even. We denote S the sum

$$S = 2^{-\frac{p}{2}} \sum_{b\neq 0} \hat{\theta}_F(0,b).$$

If r_0 is the cardinality of the set $\{b \neq 0 \,/\, \hat{\theta}_F(a,b) = +2^{p/2}\}$, then

$$\begin{aligned} S &= r_0 - (2^q - 1 - r_0), \\ &= 2r_0 - 2^q + 1.\end{aligned}$$

Hence, S is an odd integer. Besides, we have

$$\begin{aligned}\sum_{b\neq 0}\hat{\theta}_F(0,b) &= \sum_{b}\hat{\theta}_F(0,b)-\hat{\theta}_F(0,0),\\ &= \sum_{b}\sum_{x}(-1)^{b.F(x)}-2^p\\ &= \sum_{x}\sum_{b}(-1)^{b.F(x)}-2^p\\ &= 2^q a_0-2^p\end{aligned}$$

where a_0 is the cardinality of the set $\{x \;/\; F(x)=0\}$. Hence, as $S=2^{-\frac{p}{2}}(2^q a_0-2^p)$, we have

$$a_0 = 2^{\frac{p}{2}-q}(S+2^{\frac{p}{2}}).$$

As a_0 is an integer and S is an odd integer, $2^{\frac{p}{2}-q}$ must be an integer. Hence $p \geq 2q$.

So, differential-resistance is equivalent to linear-resistance when p is even and greater than $2q$. With these dimensions, such functions are well studied. We can build an instance with construction similar to those of boolean Bent functions.

Example 1 *Similarly to the construction of Maiorana-McFarland's class of boolean Bent functions, for all permutation* $\pi : K^p \to K^p$, *and all function* $f : K^p \to K^p$, *the mapping* $F : K^p \times K^p \to K^p$ *defined as*

$$F(x,y) = x \times \pi(y) + f(y)$$

where $\times$ *is the multiplication over* $GF(2^p)$, *is Bent.*

For $p < 2q$, we have to look for other bounds.

— III

Almost Perfect Functions

III-1° Almost Perfect Nonlinear functions

Definition 5 ([NK93]) *We have $\Delta_F \geq 2$. The functions such that $\Delta_F = 2$ are called Almost Perfect Nonlinear (APN).*

As $\Delta_F \geq 2^{p-q}$, the APN functions can exist only when $q \geq p$ (the case $(p, q) = (2, 1)$ is trivial). In this case, the differential resistant functions are the APN functions.

III-2° Almost Bent functions

Similarly, we can get a lower bound for Λ_F.

Lemma 3 *For all mapping F, we have*

$$\sum_{b \neq 0, a} \hat{\theta}_F^4(a, b) \geq 2^{2p}(3 \times 2^{p+q} - 2^{q+1} - 2^{2p}),$$

with equality if and only if F is Almost Perfect Nonlinear.

Proof: For all function f over K^n, let us recall these classical properties of Walsh transform:

$$\begin{aligned} (\hat{f})^2 &= \widehat{f \otimes f}, \\ \widehat{(\hat{f})} &= 2^n f, \\ \text{and } \sum_a f(a) &= \hat{f}(0). \end{aligned}$$

From the definition of λ_F we have

$$\lambda_F(a, 0) = \begin{cases} 2^{p-1} & \text{if } a = 0, \\ 0 & \text{otherwise,} \end{cases}$$

and from the definition of δ_F, we have also $\delta_F(0, 0) = 2^p$. Hence, we have for any mapping F:

$$\sum_{b \neq 0, a} \hat{\theta}_F^4(a, b) = \sum_{b \neq 0, a} (\widehat{\theta_F \otimes \theta_F})^2(a, b),$$

$$
\begin{aligned}
&= \sum_{a,b} (\theta_F \widehat{\otimes} \theta_F)^2(a,b) - \sum_a (\theta_F \widehat{\otimes} \theta_F)^2(a,0),\\
&= [\widehat{(\hat{\delta}_F)^2}](0,0) - \sum_a (\hat{\delta}_F)^2(a,0),\\
&= 2^{p+q}[\delta_F \otimes \delta_F](0,0) - 2^4 \sum_a (\lambda_F)^4(a,0).
\end{aligned}
$$

From the definition of convolutional product we have

$$
\begin{aligned}
[\delta_F \otimes \delta_F](0,0) &= \sum_{a,b} \delta_F(a,b)\delta_F(a,b),\\
&= \sum_{a\neq 0,b} \delta_F^2(a,b) + \delta_F^2(0,0).
\end{aligned}
$$

Collecting these results, we have

$$
\sum_{b\neq 0,a} \hat{\theta}_F^4(a,b) = 2^{p+q} \sum_{a\neq 0,b} \delta_F^2(a,b) + 2^{3p+q} - 2^{4p}.
$$

For all even number $n \geq 0$, we have $n^2 \geq 2n$, and $n^2 = 2n$ if and only if $n = 2$ or $n = 0$. Hence, for all $a \neq 0$ and all b, we have $\delta_F^2(a,b) \geq 2\delta_F(a,b)$, and we have the equality if and only if F is Almost Perfect Nonlinear. Beside, we have

$$
\begin{aligned}
\sum_{a\neq 0,b} \delta_F(a,b) &= \sum_{a\neq 0}\sum_b \delta_F(a,b),\\
&= \sum_{a\neq 0} 2^p,\\
&= 2^p \times (2^p - 1).
\end{aligned}
$$

Hence, we have

$$
\begin{aligned}
\sum_{b\neq 0,a} \hat{\theta}_F^4(a,b) &\geq 2^{p+q} \times 2 \times 2^p \times (2^p - 1) + 2^{3p+q} - 2^{4p},\\
&\geq 2^{2p}(3 \times 2^{p+q} - 2^{q+1} - 2^{2p}).
\end{aligned}
$$

with equality if and only if F is Almost Perfect Nonlinear.

We can now prove the following bound on Λ_F:

Theorem 4 *For all mapping F, we have*

$$
\Lambda_F \geq \frac{1}{2}\left(3 \times 2^p - 2 - 2\frac{(2^p-1)(2^{p-1}-1)}{2^q - 1}\right)^{1/2}.
$$

When the bound is reached, we will say the function Almost Bent. Moreover, an Almost Bent function F is Almost Perfect Nonlinear as well.

Proof: First, we notice that

$$
\begin{aligned}
\Lambda_F^2 &= \sup_{a,b\neq 0} \lambda_F^2(a,b),\\
&= \sup_{a,b\neq 0} \frac{1}{4}(\hat{\theta}_F)^2(a,b),
\end{aligned}
$$

and that for all mapping $N(a,b)$ over $\mathbb{Z}$,

$$M = \sup_{a,b\neq 0} N^2(a,b) \geq \frac{\sum_{a,b\neq 0} N^4(a,b)}{\sum_{a,b\neq 0} N^2(a,b)}.$$

with equality if and only if

$$\forall a,b \neq 0 \begin{cases} N(a,b)=0, \\ \text{or } N(a,b) = -\sqrt{M}, \\ \text{or } N(a,b) = +\sqrt{M}. \end{cases}$$

We will now evaluate the sum $\sum_{b\neq 0,a} \hat{\theta}_F^2(a,b)$. For all mapping F, we have

$$\begin{aligned} \sum_{b\neq 0,a} \hat{\theta}_F^2(a,b) &= \sum_{b\neq 0,a} (\theta_F \widehat{\otimes} \theta_F)(a,b), \\ &= \sum_{b\neq 0,a} \hat{\delta}_F(a,b), \\ &= \sum_{a,b} \hat{\delta}_F(a,b) - \sum_a \hat{\delta}_F(a,0), \\ &= \widehat{[\hat{\delta}_F]}(0,0) - 4\sum_a \lambda_F^2(a,0), \\ &= 2^{p+q}\delta_F(0,0) - 4\lambda_F^2(0,0), \\ &= 2^{2p}(2^q-1). \end{aligned}$$

Hence, using lemma 3 we have

$$4\Lambda_F^2 = \sup_{a,b\neq 0} (\hat{\theta}_F)^2(a,b) \geq \frac{2^{2p}(3\times 2^{p+q} - 2^{q+1} - 2^{2p})}{2^{2p}(2^q-1)}, \tag{III.1}$$

$$\geq \frac{3\times 2^{p+q} - 2^{q+1} - 2^{2p}}{2^q-1}, \tag{III.2}$$

$$\geq 3\times 2^p - 2 - 2\frac{(2^p-1)(2^{p-1}-1)}{2^q-1}, \tag{III.3}$$

with equality if and only if F is Almost Perfect Nonlinear, and

$$\forall a,b \neq 0 \begin{cases} \lambda_F(a,b)=0, \\ \text{or } \lambda_F(a,b) = -\Lambda_F, \\ \text{or } \lambda_F(a,b) = +\Lambda_F. \end{cases}$$

Note 2 *For Almost Bent Functions, the function $\lambda_F(a,b)$ for $b\neq 0$ takes at most three different values that is to say 0, $-\Lambda_F$ or Λ_F. This looks like Bent functions for which $\lambda_F(a,b)$ for $b\neq 0$ takes at most two different values $-\Lambda_F$ or Λ_F.*

Lemma 4 *If $F: K^p \to K^q$ is Almost Bent and not Bent, then $p \leq q$.*

Proof: We already have the absolute bound of the Bent functions

$$\Lambda_F \geq \frac{1}{2}2^{\frac{p}{2}}.$$

Hence, if F is Almost Bent and not Bent, then using expression III.2 we have

$$\begin{aligned}
\frac{1}{2}\sqrt{\frac{3\times 2^{p+q}-2^{q+1}-2^{2p}}{2^q-1}} &> \frac{1}{2}\sqrt{2^p},\\
\frac{3\times 2^{p+q}-2^{q+1}-2^{2p}}{2^q-1} &> 2^p,\\
3\times 2^{p+q}-2^{q+1}-2^{2p} &> 2^{p+q}-2^p,\\
2^{p+q+1}-2^{q+1}-2^{2p}+2^p &> 0,\\
2^{q+1}(2^p-1)-2^p(2^p-1) &> 0,\\
q+1 &> p.
\end{aligned}$$

Lemma 5 ([Cas94]) *For all $q > p$, the amount*

$$\frac{(2^p-1)(2^{p-1}-1)}{2^q-1} \tag{III.4}$$

is not an integer.

Proof: We have

$$\begin{aligned}
(2^p-1)(2^{p-1}-1) &= (2^q-1)2^{2p-1-q}-(3\times 2^{p-1}-2^{2p-1-q}-1),\\
&= A\times(2^q-1)-B.
\end{aligned}$$

As $q > p$, we have $-2^{2p-1-q} > -2^{p-1}$, hence $3\times 2^{p-1}-2^{2p-1-q} > 2^p > 1$ and the remainder B is strictly positive. Besides, we have

$$\begin{aligned}
B < 2^q-1 &\iff 3\times 2^{p-1}-2^{2p-1-q}-1 < 2^q-1,\\
&\iff 2^{p-1}(3-2^{p-q}) < 2^q.
\end{aligned}$$

As $q \geq p+1$, $2 < 3-2^{p-q} < 3$, hence $2^{p-1}(3-2^{p-q}) < 3\times 2^{p-1}$, and besides $2^q > 2^{p+\lg 2(\frac{3}{2})}$. Consequently, we have

$$(2^p-1)(2^{p-1}-1) = A\times(2^q-1)-B,$$

with $0 < B < 2^q-1$, and the amount III.4 cannot be an integer if $q > p$.

Theorem 5 *If $F : K^p \to K^q$ is Almost Bent and not Bent, then $p = q$, p is odd. The above bound then turns in*

$$\Lambda_F = \frac{1}{2}2^{\frac{p+1}{2}}. \tag{III.5}$$

Proof: The bound III.3 cannot be reached if the fraction III.4 is not an integer. Hence, using lemmas 4 and 5 we get $p = q$. The bound III.3 then gives III.5, and so p must be odd.

Example 2 *Let $F(x) = x^{2^k+1}$ be a power polynomial in $GF(2^n)$. If n is odd, $1 < k < n$ and $gcd(n,k) = 1$, then F is an Almost Bent permutation [Nyb94, proposition 3].*

Example 3 *(C. Carlet) Let $F(x) = x^{-1}$ be the inversion mapping in $GF(2^n)$ completed in 0 by $F(0) = 0$. If n is odd, then F is an Almost Perfect Nonlinear Permutation [Nyb94, proposition 6]. Yet, it is not an Almost Bent function (consequence of [LW90, theorem 3.4]).*

— IV

Conclusion

To sum up the results, we have :

- When $p \geq 2q$ and p even, differential-resistant is equivalent to linear-resistant and to vectorial Bentness. We have in this case $\Lambda_F = \frac{1}{2}2^{p/2}$ and $\Delta_F = 2^{p-q}$.
- For $p = q$ and p odd, differential-resistance is equivalent to Almost Perfect Nonlinearity (where $\Delta_F = 2$), linear-resistant is equivalent to Almost Bentness (where $\Lambda_F = \frac{1}{2}2^{(p+1)/2}$) and linear-resistance implies differential-resistance.
- For $q \geq p$, 2 is a lower bound for Δ_F, and we have :

$$\Lambda_F \geq \frac{1}{2}\left(3 \times 2^p - 2 - 2\frac{(2^p-1)(2^{p-1}-1)}{2^q-1}\right)^{1/2}$$

Results in the other cases are still open. Particularly, if $p = q$ and p even, there is no simple characterization of linear-resistant functions. Similarly, for $q < p < 2q$, ther exists functions such that $\Lambda_F = \frac{1}{2}2^{\frac{p+1}{2}}$, but we ignore whether ther exists functions such that $\frac{1}{2}2^{\frac{p}{2}} < \Lambda_F < \frac{1}{2}2^{\frac{p+1}{2}}$ in this case.

Acknowledgement

We wish to thank Claude Carlet for very helpful discussions. We also wish to thank Jacques Stern who suggested this work and Julien Cassaigne for his useful lemma.

References

[Cas94] J. Cassaigne, 1994. personal communication.

[LW90] G. Lachaud and J. Wolfmann. The weights of the orthogonals of the extended quadratic binary Goppa codes. *IEEE Trans. Inform. Th.*, 36:686–692, May 1990.

[Mat94] M. Matsui. Linear cryptanalysis method for DES cipher. In *Lecture Notes in Computer Science, Advances in Cryptology – EUROCRYPT '93*, volume 765, pages 386–397. Springer-Verlag, 1994.

[MS90] W. Meier and O. Staffelbach. Nonlinearity criteria for cryptographic functions. In *Lecture Notes in Computer Science, Advances in Cryptology – EUROCRYPT '89*, pages 549–562. Springer-Verlag, 1990.

[NK93] K. Nyberg and L. Ramkilde Knudsen. Provable security against differential cryptanalysis. In *Lecture Notes in Computer Science, Advances in Cryptology – CRYPTO '92*, volume 740, pages 566–574. Springer-Verlag, 1993.

[Nyb91] K. Nyberg. Perfect nonlinear S-boxes. In *Lecture Notes in Computer Science, Advances in Cryptology – EUROCRYPT '91*, volume 547, pages 378–385. Springer-Verlag, 1991.

[Nyb94] K. Nyberg. Differentially uniform mappings for cryptography. In *Lecture Notes in Computer Science, Advances in Cryptology – EUROCRYPT '93*, volume 765, pages 55–64. Springer-Verlag, 1994.