

Symmetric Cryptography and Algebraic Curves

José Felipe Voloch

Abstract: We discuss some applications of the theory of algebraic curves to the study of S-boxes in symmetric cryptography.

0. Introduction

A symmetric block cipher usually consists of several iterations (rounds) of the following operations on the input message: An \mathbf{F}_2 -linear transformation (to “mix the bits”), a non-linear map (consisting of one or several S-boxes) and the \mathbf{F}_2 -addition of part of the key. For our purposes an S-box is simply a map $f : \mathbf{F}_{2^n} \rightarrow \mathbf{F}_{2^n}$. Two well-known attacks on such ciphers, differential and linear cryptanalysis, exploit situations in which an S-box is “close to \mathbf{F}_2 -linear”. There are two corresponding measures of nonlinearity for S-boxes, which we define below. These are closely related (see [CV]).

For a function $f : \mathbf{F}_{2^n} \rightarrow \mathbf{F}_{2^n}$ we define

$$\delta(f) = \max_{\alpha \neq 0, \beta} \#\{x \in \mathbf{F}_{2^n} \mid f(x + \alpha) - f(x) = \beta\}$$

For any f , $\delta(f)$ is a positive even integer and if f is a polynomial of degree m then $\delta(f) \leq m - 1$ unless f is an additive polynomial plus a constant. To defend against differential cryptanalysis one needs $\delta(f)$ to be small. A function f is said to be almost perfectly nonlinear (APN) if $\delta(f) = 2$. In this paper we will study the behaviour of $\delta(f)$ for polynomials f .

For a function $f : \mathbf{F}_{2^n} \rightarrow \mathbf{F}_{2^n}$ we define

$$\lambda(f) = \max_{\alpha \neq 0, \beta} |\#\{x \in \mathbf{F}_{2^n} \mid \text{Tr}(\alpha f(x) + \beta x) = 0\} - 2^{n-1}|$$

For any f , $\lambda(f) \geq 2^{(n-1)/2}$ and if f is a polynomial of degree m which is not an additive polynomial plus a constant then $\lambda(f) \leq (m-1)2^{(n-1)/2}$. To defend against linear cryptanalysis one needs $\lambda(f)$ to be small. The function f is said to be almost bent if $\lambda(f) = 2^{(n-1)/2}$. We will not discuss λ in this paper.

The S-box used by AES is $s : \mathbf{F}_{2^8} \rightarrow \mathbf{F}_{2^8}, s(x) = x^{-1}, x \neq 0, s(0) = 0$. We have that $\delta(s) = 4$. More generally, the same function on \mathbf{F}_{2^n} has $\delta(s) = 2$ for n odd and $\delta(s) = 4$ for n even. (see [N]).

Other examples of APN functions are the Gold functions, $f(x) = x^{2^j+1}, (n, j) = 1$, and the Kasami functions, $f(x) = x^{4^j-2^j+1}, (n, j) = 1$. These are the only examples known of polynomials which are APN in \mathbf{F}_{2^n} for infinitely many n and we conjecture that there are no others, up to a natural equivalence which we define in section 2.

Edel, Kyureghan and Pott [EKP] gave the following example of an APN function which is not equivalent in the natural sense alluded above to a monomial: $f(x) = x^3 + \omega x^{36}$ as a function on $\mathbf{F}_{2^{10}}$, where ω is a primitive cube root of unity. Byrne and McGuire [BM] showed that this function is APN for only finitely many fields \mathbf{F}_{2^n} . We will give a new proof of this result as a consequence of a more general fact, stated in Theorem 3 below.

For monomials, the following is known. For an integer $m > 0$, define l to be the largest integer such that 2^l divides $m - 1$. Also, let $m' = (m - 1)/2^{l-1} + 1$ and $d = (m - 1, 2^l - 1) = ((m' - 1)/2, 2^l - 1)$. Then Jedlicka [J] proved that if $d < (m - 1)/2^l, m > 5$ then $f(x) = x^m$ can only be APN for finitely many fields \mathbf{F}_{2^n} . He also showed that $f(x) = x^{-m}, x \neq 0, f(0) = 0$, for $m \equiv 1 \pmod{4}, m > 5$ can only be APN for finitely many fields \mathbf{F}_{2^n} .

It is not hard to show that if a polynomial f is APN, then the curves $F_\alpha(x, y) = 0$ have very few rational points, where

$$F_\alpha(x, y) = (f(x + \alpha) + f(x) + f(y + \alpha) + f(y))/((x + y)(x + y + \alpha)).$$

If one of these curves has an absolutely irreducible factor defined over \mathbf{F}_{2^n} and n is large enough, then Weil's theorem guarantees that the curve has enough points so that f is not APN. (See, e.g., [BM] Theorem 4 for a similar argument).

In the work of Jedlicka (which extends work of Janwa, McGuire and Wilson [JMW]) and the work of Byrne and McGuire mentioned above, they show the existence of this absolutely irreducible factor by using intersection theory and a study of the singularities of the curve.

To study the values of $\delta(f)$ other than $\delta(f) = 2$ we need to study other curves in addition to $F_\alpha(x, y) = 0$.

Our main results are the following:

Theorem 1. *For a given integer $m > 4, m \equiv 0, 3 \pmod{4}$ let $\delta_0 = m - 1$ or $m - 2$ according to whether m is odd or even. Then most polynomials f of degree m over \mathbf{F}_{2^n} satisfy $\delta(f) = \delta_0$. More precisely,*

$$\lim_{n \rightarrow \infty} \frac{\#\{f \in \mathbf{F}_{2^n}[x] \mid \deg f = m, \delta(f) = \delta_0\}}{\#\{f \in \mathbf{F}_{2^n}[x] \mid \deg f = m\}} = 1$$

Theorem 2. *Let m be an integer $m > 4$ and $f(x) = x^m + a_1x^{m-1} + a_2x^{m-2} + \dots$ be a polynomial over \mathbf{F}_{2^n} . Then $\delta(f)$ is strictly smaller than $m - 1$ or $m - 2$ according to whether m is odd or even, provided that one of the following holds:*

- (i) $a_1 = 0$ and $m \equiv 0 \pmod{4}$
- (ii) $a_2 = 0$, n is odd and $m \equiv 5 \pmod{8}$
- (iii) $a_1^2 + a_2 = 0$, n is odd and $m \equiv 3 \pmod{8}$

Theorem 3. *Let $f(x) = x^m + cx^r$, where $c \in \overline{\mathbf{F}}_2^*$, $3 \leq r < m$ are coprime integers, not both even, neither a power of two and such that $(m-1, r-1)$ is a power of two. Then F_α is irreducible in $\overline{\mathbf{F}}_2[x, y, \alpha]$. Consequently, if f is defined over \mathbf{F}_{2^n} , $\delta(f) > 2$ for n sufficiently large with respect to m .*

1. Proofs

Proof of Theorem 1: Fix for the moment $\alpha \in \mathbf{F}_{2^n}^*$ and $m > 3$ odd. Let f be a polynomial in $\mathbf{F}_{2^n}[x]$ of degree at most m , then there exists a polynomial g in $\mathbf{F}_{2^n}[x]$ of degree at most $d = (m - 1)/2$ such that $f(x + \alpha) + f(x) = g(x(x + \alpha))$. The function $L : f \mapsto g$ is linear and its kernel consists of the polynomials of the form $h(x(x + \alpha))$, $\deg h \leq d$. It follows that the kernel has dimension $d + 1$ and since f varies on a space of dimension $m + 1$, it follows that L is surjective. If m is even, then let $d = (m - 2)/2$, then again $f(x + \alpha) + f(x) = g(x(x + \alpha))$, $\deg g \leq d$. The kernel of L is now of dimension $m/2 + 1$ and again it follows that L is surjective. Note that either way, d is odd by hypothesis.

We now define a polynomial f to be generic if $\deg f = m$ and if $L(f)$ is a polynomial of degree d which when viewed as a morphism from \mathbf{P}^1 to itself is such that above each affine branch point there is only one ramification point and the ramification degree of such points is 2. The condition on $L(f)$ defines a Zariski open dense set of the coefficients of $L(f)$ and since L is surjective, we get an open dense condition on the coefficients of f as well.

The genericity condition ensures that the geometric Galois group of the Galois closure of the map $L(f)$ is the symmetric group S_d . (This follows from a classical argument, see e.g. [BW] Lemma 2.3 and the paragraph following that lemma.) We now compute the Galois group of the Galois closure of the map f . If t is a coordinate on \mathbf{P}^1 and u_0, \dots, u_{d-1} are the roots of $L(f)(u) = t$, then the roots of $f(x) = t$ are the solutions of $x_i^2 + \alpha x_i = u_i, i = 0, \dots, d-1$. For each place v of $F = \mathbf{F}_{2^n}(t, u_0, \dots, u_{d-1})$ above $t = \infty$ we have that u_0 a simple pole and that $u_j = \zeta^{\sigma(j)} u_0 + O(1)$, where ζ is a primitive d -th root of unity. The map $v \mapsto \sigma$ gives a bijection between the places of F above $t = \infty$ and S_d .

Let J be a set of indices such that $\sum_{j \in J} u_j$ has no poles (i.e. is constant), then $\sum_{j \in J} \zeta^{\sigma(j)} = 0, \forall \sigma \in S_d$. If J is neither empty nor the whole of $\{0, \dots, d-1\}$, consider the last equation with σ the identity and also $\sigma = (j_0 j_1)$ where $j_0 \in J, j_1 \notin J$. It follows that $\zeta^{j_0} = \sum_{j \in J, j \neq j_0} \zeta^j = \zeta^{j_1}$, contradiction. Now, we have that $\sum_j u_j = b_1/b_0$, where $L(f) = b_0 x^d + b_1 x^{d-1} + \dots$. It follows that the geometric Galois group of the Galois closure of the map f is an extension of S_d by $(\mathbf{Z}/2)^{d-1}$ and the arithmetic Galois group is either that or has an extra $\mathbf{Z}/2$ depending on whether $b_1/b_0 = y^2 + \alpha y, y \in \mathbf{F}_{2^n}$ or not. If the former is the case, then the curve corresponding to the Galois closure of the map f is defined over \mathbf{F}_{2^n} and an application of Chebotarev's density theorem gives the existence of d distinct pairs $x_i, x_i + \alpha$ with $f(x_i) + f(x_i + \alpha) = \beta$ for some β and thus $\delta(f) = 2d = \delta_0$, if n is large enough.

Now, if $f(x) = x^m + a_1x^{m-1} + a_2x^{m-2} + \dots$, then

$$b_1/b_0 = \begin{cases} (1 + \binom{d}{2})\alpha^2 + a_1\alpha + a_2, & m \equiv 3 \pmod{4} \\ (1 + \binom{d}{2})\alpha^2 + (\alpha^3 + a_2\alpha + a_3)/a_1 & m \equiv 0 \pmod{4} \end{cases} \quad (*)$$

It is not hard to check (see the proof of Theorem 2, item (iii)) that for n large enough it will exist α such that $b_1/b_0 = y^2 + \alpha y, y \in \mathbf{F}_{2^n}$, unless $m \equiv 3 \pmod{8}$, n is odd and $a_1^2 + a_2 = 0$. So, if we assume that f is generic and $a_1^2 + a_2 \neq 0$, we will be sure to find y for n sufficiently large. This completes the proof.

Proof of Theorem 2:

For item (i), note that $\deg L(f) < d$, when $a_1 = 0$.

For item (ii), with notation as in the proof of Theorem 1, we find that $b_1/b_0 = \binom{d}{2}\alpha^2 + a_2 = \alpha^2$ under the current hypothesis, and this cannot be of the form $y^2 + \alpha y, y \in \mathbf{F}_{2^n}$ for n odd.

For item (iii), using equation (*) from the proof of Theorem 1 (which is valid for all monic polynomials f), we get that if all u_i are in \mathbf{F}_{2^n} then there exists $y \in \mathbf{F}_{2^n}$ such that

$$(1 + \binom{d}{2})\alpha^2 + a_1\alpha + a_2 = y^2 + \alpha y.$$

Thus $\text{Tr}_{\mathbf{F}_{2^n}/\mathbf{F}_2}(((1 + \binom{d}{2})\alpha^2 + a_1\alpha + a_2)/\alpha^2) = 0$ but the trace is easily seen to be $\text{Tr}_{\mathbf{F}_{2^n}/\mathbf{F}_2}(1) = 1$ under the assumptions of item (iii).

Proof of Theorem 3: $F_\alpha(\alpha x, \alpha y) = \alpha^{r-2}(G\alpha^k + H)$, where $k = m - r$,

$$G = ((x+1)^m + x^m + (y+1)^m + y^m)/((x+y)(x+y+1))$$

and

$$H = c((x+1)^r + x^r + (y+1)^r + y^r)/((x+y)(x+y+1)).$$

We claim that it suffices to show that G and H are non-zero, have no common factor and that G/H is not an s -th power for any divisor $s > 1$ of k . Indeed, if these conditions hold, $G\alpha^k + H$ is irreducible as a polynomial in α so if it factors as a polynomial in α, x, y then one of the factors does not involve α and this contradicts the fact that G, H have no

common factor. Once we know the polynomial is irreducible as a polynomial in α, x, y , the Lang-Weil estimate implies that, for n large enough, there exists $\alpha, x, y \in \mathbf{F}_{2^n}, x \neq y, y + \alpha, F_\alpha(x, y) = 0$, hence $\delta(f) > 2$.

Assume first that both m and r are odd. Then, $G(x, x) = (x+1)^{m-1} + x^{m-1}, H(x, x) = c((x+1)^{r-1} + x^{r-1})$ are clearly non-zero. Furthermore, the map $x \mapsto (x+1)/x$ establishes a bijection between the roots of $G(x, x)$ and the $(m-1)$ -st roots of unity distinct from 1 and likewise for $H(x, x)$. It now follows that G and H have no common factor since $(m-1, r-1)$ is a power of 2 and thus G/H is not an s -th power for any divisor $s > 1$ of k , since $G(x, x)$ and $H(x, x)$ are of the form a polynomial with distinct roots raised to a power of two.

If either m or r is even, then since neither is a power of two, neither G nor H is identically zero. If say, $m = 2^u v$ is even but r, v are odd then $G = ((x+y)(x+y+1))^{2^u - 1} K^{2^u}$ for some polynomial K with $K(x, x)$ non-zero and a similar argument as in the case m, r odd applies with K in place of G . Finally the case m odd, r even is obtained by reversing the roles of G and H .

2. Low degrees

We conclude with some consequences of our methods in the case of low degrees. First of all, note that $\delta(f)$ is unchanged if f is replaced by $f+h$ where h is an additive polynomial or if f is replaced by $f(ax+b)/c$ where, $a, b, c \in \mathbf{F}_{2^n}, ac \neq 0$. It is elementary that $\delta(f) = 2$ if $\deg f \leq 4$ unless f is an additive polynomial plus a constant.

In the case of $\deg f = 5$, the above allows us to reduce the problem to the consideration of two cases $f = x^5, x^5 + x^3$. Theorem 2 gives that $\delta(x^5) = 2$ for n odd and one can check that $\delta(x^5) = 4$ for $n > 2$ even. Theorem 3 gives that $\delta(x^5 + x^3) = 4$ for n large and in fact $n > 2$ suffices.

The cases of $\deg f \geq 6$ cannot be fully analysed just by referring to the theorems but some cases can still be fully analysed by our methods as follows.

If $\deg f = 6$ and $L(f)$ is a separable polynomial, the extension $F/\mathbf{F}_{2^n}(t)$, from the proof of Theorem 1, has to have Galois group S_2 and the proof of Theorem 1 gives $\delta(f) = 4$

unless $a_1 = a_3 = 0$. In the case $a_1 = a_3 = 0$, f is equivalent to x^6 (and $L(f)$ is inseparable) and $\delta(f) = \delta(x^3) = 2$.

The case of $\deg f = 7$. As in the proof of Theorem 1, the extension $F/\mathbf{F}_{2^n}(t)$ has Galois group S_3 or A_3 and likewise for the geometric Galois group. Since there is a place above infinity such that $u_j = \zeta^j u_0 + O(1)$ and ζ is a primitive root of unity, it follows directly that $\sum_{j \in J} u_j$ is non-constant unless $J = \emptyset$ or $J = \{0, 1, 2\}$. A calculation shows that $b_1/b_0 = a_1\alpha + a_2$ and this will be of the form $y^2 + \alpha y$, $y \in \mathbf{F}_{2^n}$ for some α , assuming n is large enough. If we show that the arithmetic and geometric Galois groups coincide then the proof of Theorem 1 gives that $\delta(f) = 6$. The only way the two groups can differ is if the former is S_3 but the latter is A_3 . This can only happen if the quadratic polynomial $(L(f)(u) - L(f)(v))/(u - v)$ factors in a quadratic extension of \mathbf{F}_{2^n} for all α and a messy but straightforward calculation shows that this polynomial is irreducible. So $\delta(f) = 6$ for all f of degree 7 if n is large enough.

Polynomials of degree 8 are equivalent to polynomials of lower degree. For degree 9 and beyond we do not have complete results.

As mentioned in the introduction, we conjecture that the only polynomials that are APN for infinitely many n are those equivalent to the Gold and Kasami functions. We also make the following conjecture:

Conjecture. *For a given integer $m > 4$, there exists $\varepsilon_m > 0$ such that for all sufficiently large n , if f is a polynomial of degree m over \mathbf{F}_{2^n} for at least $\varepsilon_m 2^{2n}$ values of $\alpha \neq 0, \beta \in \mathbf{F}_{2^n}$, $\#\{x \in \mathbf{F}_{2^n} | f(x + \alpha) - f(x) = \beta\} = \delta(f)$.*

A corollary of this conjecture would be that picking $\alpha \neq 0, \beta \in \mathbf{F}_{2^n}$ at random gives a probabilistic polynomial time algorithm for computing $\delta(f)$. The analogue of the conjecture does not hold for rational functions and already fails for x^{-1} .

References.

[BM] E. Byrne and G. McGuire, *On the non-existence of quadratic APN and crooked functions on finite fields*, preprint, 2005. <http://www.maths.may.ie/staff/gmg/pubs.html>

[BW] A. O. Bender and O. Wittenberg, *A Potential Analogue of Schinzel's Hypothesis for Polynomials with Coefficients in $\mathbf{F}_q[t]$* , Int. Math. Res. Not. **36** (2005) 2237–2248.

[CV] F. Chabaud and S. Vaudenay, *Links between differential and linear cryptanalysis*, Advances in Cryptology-EUROCRYPT '94, A. De Santis, Ed., Lecture Notes in Computer Science, vol. 950, Springer-Verlag, New York, 1995, pp. 356–365.

[EKP] Y. Edel, G. Kyureghyan, and A. Pott, *A new APN function which is not equivalent to a power mapping* preprint, <http://arxiv.org/abs/math.CO/0506420>, 2005.

[JMW] H. Janwa, G. McGuire and R. M. Wilson, *Double-error-correcting cyclic codes and absolutely irreducible polynomials over $GF(2)$* , Journal of Algebra **178** (1995) 665–676.

[J] D. Jedlicka, *Classifying APN Monomials*, preprint 2005, <http://eprint.iacr.org/2005/096.pdf> ■

[N] K. Nyberg, *Differentially uniform mappings for cryptography*. Advances in Cryptology - EUROCRYPT '93, T. Helleseth, Ed., Lecture Notes in Computer Science, vol. 765, Springer-Verlag, New York, 1994, pp. 55-64.

Dept. of Mathematics, Univ. of Texas, Austin, TX 78712, USA

e-mail: voloch@math.utexas.edu