UC, Berkeley, CS294-90, Cryptanalysis, Spring, 2013, Homework 4

John Manferdelli

For this homework, you need to remember (or learn) a little bit about polynomials over finite fields like the fact that polynomials with coefficients from an (arbitrary, including finite, field) form a unique factorization domain. Also recall that if f(x) and g(x) are polynomials over a field F, that the greatest common divisor of f(x) and g(x), denoted by gcd(f(x), g(x)) or simply (f(x), g(x))can be written as

$$(f(x), g(x)) = a(x)f(x)+b(x)g(x)$$

for some polynomials, a(x), b(x).

1. Rijndael uses the fact that $m(x)= x^8+x^4+x^3+x+1$ is an irreducible polynomial over GF(2). Prove it!

2. Suppose we consider the finite field $GF(2)^8$ generated by the irreducible polynomial m(x) above. What is the best linear approximation (over GF(2)) to $f_1(z)$ where is the low order bit (the constant term in the polynomial representation) of the function $f(z)= z^{-1}$, if $z\neq0$ and $f(0)=0$, where $z\in GF(2)^8$.

3. What is the best linear approximation to the function $f(x_1, x_2, x_3, x_4, x_5, x_6)= x_1+x_2+x_4x_5$?

4. Calculate the bias of the differential 0x80800000→0x20000000 in FEAL.