Math 259 - Spring 2019
Homework 6

This homework is due on Monday, April 22.

1. Consider the multivariate quadratic map

$$\begin{aligned} F\colon \mathbb{F}_2^4 &\to \mathbb{F}_2^3 \\ x &\mapsto (f_1(x), f_2(x), f_3(x)) \end{aligned}$$

   given by the quadratic polynomials

$$\begin{aligned} f_1(x_1,x_2,x_3,x_4) &= x_1x_2 + x_2x_3 + x_1 + x_4, \\ f_2(x_1,x_2,x_3,x_4) &= x_2x_4 + x_3x_4 + x_1 + x_2 + x_3, \\ f_3(x_1,x_2,x_3,x_4) &= x_1x_3 + x_2x_3 + x_3x_4 + 1. \end{aligned}$$

   By brute force or whatever other technique you want, for each of the following $y$, give $x$ such that $F(x) = y$.

   (a) $y = (0, 1, 0)$
   (b) $y = (1, 1, 0)$

2. Let

$$\begin{aligned} F\colon \mathbb{F}_2^4 &\to \mathbb{F}_2^3 \\ x &\mapsto (f_1(x), f_2(x), f_3(x)) \end{aligned}$$

   be a public key given by the quadratic polynomials

$$\begin{aligned} f_1(x_1,x_2,x_3,x_4) &= x_1x_2 + x_2x_3 + x_1 + x_4, \\ f_2(x_1,x_2,x_3,x_4) &= x_2x_4 + x_3x_4 + x_1 + x_2 + x_3, \\ f_3(x_1,x_2,x_3,x_4) &= x_1x_3 + x_2x_3 + x_3x_4 + 1. \end{aligned}$$

   (This is the same $F$ as in Problem 1.) For each of the following message digests $y$ below, determine if the value $x$ given is a valid signature for the digest or not.

   (a) $y = (1, 1, 1)$, $x = (1, 1, 0, 1)$
   (b) $y = (0, 0, 1)$, $x = (0, 1, 0, 1)$

3. In the following multivariate quadratic polynomial, the variables $x_1, x_2, x_3$ are "oil" variables, and $x_4$ and $x_5$ are "vinegar" variables:

$$\begin{aligned} P\colon \mathbb{F}_2^5 &\to \mathbb{F}_2^3 \\ x &\mapsto (p_1(x), p_2(x), p_3(x)), \end{aligned}$$

where

$$p_1(x_1,x_2,x_3,x_4,x_5) = x_1x_4 + x_2x_4 + x_2x_5 + x_4x_5 + x_2 + x_5,$$
$$p_2(x_1,x_2,x_3,x_4,x_5) = x_1x_5 + x_2x_5 + x_3x_4 + x_3 + x_5 + 1,$$
$$p_3(x_1,x_2,x_3,x_4,x_5) = x_3x_4 + x_3x_5 + x_2 + x_4.$$

Use this knowledge to solve the systems of multivariate quadratic equations below:

(a) $P(x) = (0,0,0)$

(b) $P(x) = (1,1,0)$

4. (a) There is a unique *monic irreducible* polynomial $f \in \mathbb{F}_2[x]$ of degree 2. What is $f$?

   (b) Let $\beta$ be a root of $f$, where $f$ is as in part (a). Then $\mathbb{F}_4 = \mathbb{F}_2[\beta]$. Write a multiplication table for $\mathbb{F}_2[\beta]$.

5. We will now work over $\mathbb{F}_3$, the field with three elements. There are three monic irreducible polynomials of degree 2 over $\mathbb{F}_3$:

$$f_1(x) = x^2 + 1, \quad f_2(x) = x^2 + x + 2, \quad f_3(x) = x^2 + 2x + 2.$$

   (a) Let $\beta$ be a root of $f_1$. Then $\mathbb{F}_9 = \mathbb{F}_3[\beta]$. Compute the following quantities in $\mathbb{F}_3[\beta]$. To obtain credit, your answer must be in the form $a_0 + a_1\beta$, with $a_0, a_1 \in \mathbb{F}_3$.

      i. $\beta(2\beta + 1)$

      ii. $\beta^{-1}$ (the multiplicative inverse of $\beta$, which is the unique $a_0 + a_1\beta$ such that $\beta(a_0 + a_1\beta) = 1$)

      iii. $(\beta + 2)^{-1}$

   (b) Now let $\gamma$ be a root of $f_2$. Then $\mathbb{F}_9 = \mathbb{F}_3[\gamma]$, so it must be the case that somehow $\mathbb{F}_3[\beta] = \mathbb{F}_3[\gamma]$! What this means is that there is a map $\phi\colon \mathbb{F}_3[\beta] \to \mathbb{F}_3[\gamma]$ that is a *field isomorphism* (a bijection respecting addition and multiplication). It is a fact that to specify $\phi$, it suffices to say what $\phi(\beta)$ is (then $\phi(a_0 + a_1\beta) = a_0 + a_1\phi(\beta)$, which tells you the image of everything in $\mathbb{F}_3[\beta]$). It is another fact that $\phi(\beta)$ must be some element $a_0 + a_1\gamma$ such that

$$(a_0 + a_1\gamma)^2 + 1 = 0.$$

   (In other words, $\phi(\beta)$ must be a root of $f_1$!) Find $a_0 + a_1\gamma$ such that $(a_0 + a_1\gamma)^2 + 1 = 0$.

   (c) Let $\delta$ be a root of $f_3$. Find $a_0 + a_1\delta$ such that $(a_0 + a_1\delta)^2 + 1 = 0$.

6. For each of the HFE polynomials $G \in \mathbb{F}_{p^r}[X]$ below, give the associated multivariate quadratic polynomial $G\colon (\mathbb{F}_p)^r \to (\mathbb{F}_p)^r$. In each case, use the field structure given.

   (a) $G(X) \in \mathbb{F}_9[X]$, $G(X) = X^{10} + 2X^3 + 1$, $\mathbb{F}_9 = \mathbb{F}_3[\beta]$, $\beta$ a root of $f(x) = x^2 + 1$

(b) $G(X) \in \mathbb{F}_4[X]$, $G(X) = X^9+X^5+X^4+1$, $\mathbb{F}_4 = \mathbb{F}_2[\beta]$, $\beta$ a root of $f(x) = x^2+x+1$

(c) $G(X) \in \mathbb{F}_8[X]$, $G(X) = X^9+X^5+X^4+1$, $\mathbb{F}_8 = \mathbb{F}_2[\beta]$, $\beta$ a root of $f(x) = x^3+x+1$

Extra problem for graduate credit:

1. We haven't talked about how to find the roots of a polynomial $G(X) \in \mathbb{F}_q[X]$. One way to do it is the so-called Berlekamp algorithm, which relies on the computation of $\gcd(G(X), X^q - X)$. Explain why the roots of $\gcd(G(X), X^q - X)$ are exactly the roots of $G$ that are in $\mathbb{F}_q$.