An Old Hack of Multivariate Cryptography (The Matsumoto-Imai Scheme)

Carl Miller

References:

J. Ding, J. Gower, D. Schimdt, *Multivariate Public Key Cryptosystems*, Advances in Information Security, vol. 25 (2006).

M. Sala et al., eds., *Grobner bases, coding, and cryptography*, Springer, 2009.

The Matsumoto-Imai Scheme

The Matsumoto-Imai Scheme

1.2 Finite fields

For any n, there is a unique field of 2^n elements $\mathbb{F}_{2^n}$.

The Matsumoto-Imai Scheme

1.3 Building a one-way function

Consider the function

$$f_\theta(x) \quad = \quad (x)(x^{2^\theta}) = x^{1+2^\theta}.$$

(with $1 < \theta < n$).

The Matsumoto-Imai Scheme

1.4 The Matsuomoto-Imai Scheme

Obscure the inverse of $x \mapsto x^{1+2^\theta}$?

)

The Matsumoto-Imai Scheme

$$F(x) = M^{-1}(L(x)^{1+2^{\theta}})$$

The Larger Picture

A multivariate public key crypto scheme is a function on $\mathbb{F}_\ell^m$ of the form

$$G(x) \quad = \quad A \circ B \circ C(x)$$

where

The Larger Picture

Encryption: $c := G(x)$.

The Larger Picture

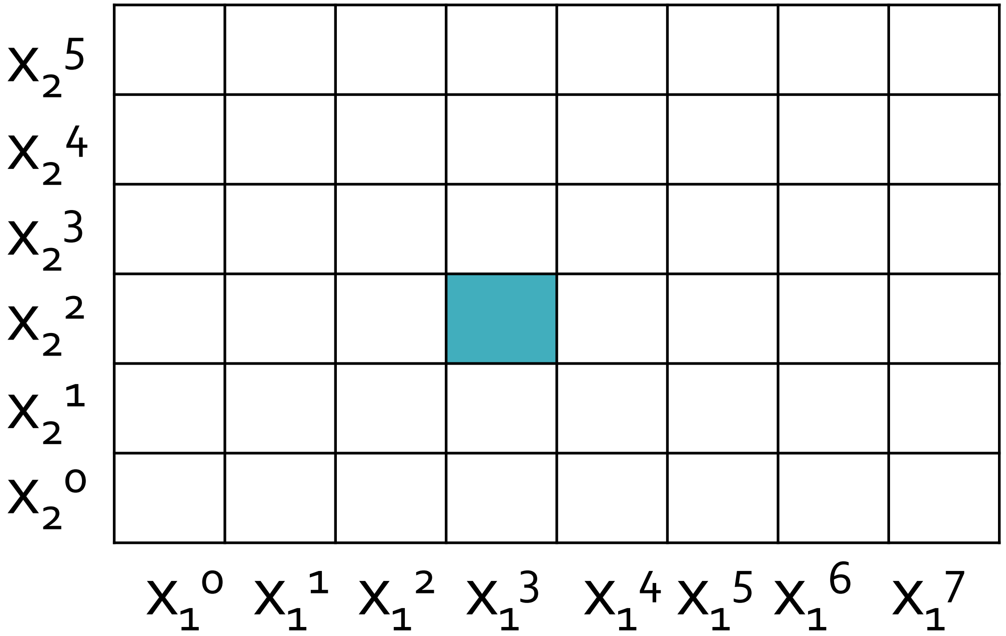
2.2 Groebner bases - a general attack

The Larger Picture

In the multivariate case, this is harder: **leading terms may be incomparable.**

The Larger Picture

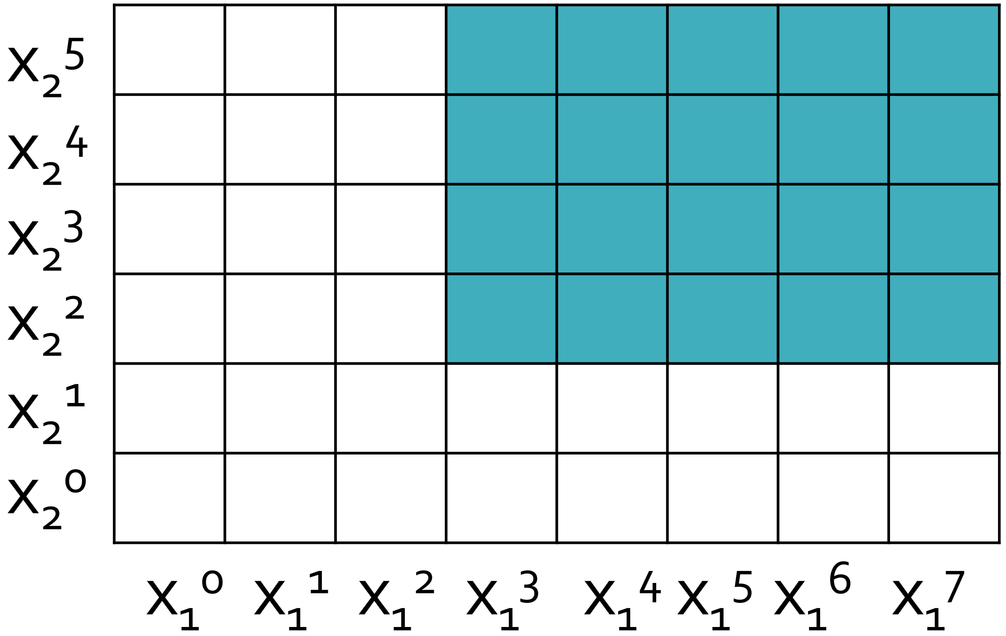
Look at the ideal generated by the **leading terms** of $f_1, \ldots, f_n$ (under some appropriate monomial ordering).



The Larger Picture

Look at the ideal generated by the **leading terms** of $f_1, \ldots, f_n$ (under some appropriate monomial ordering).

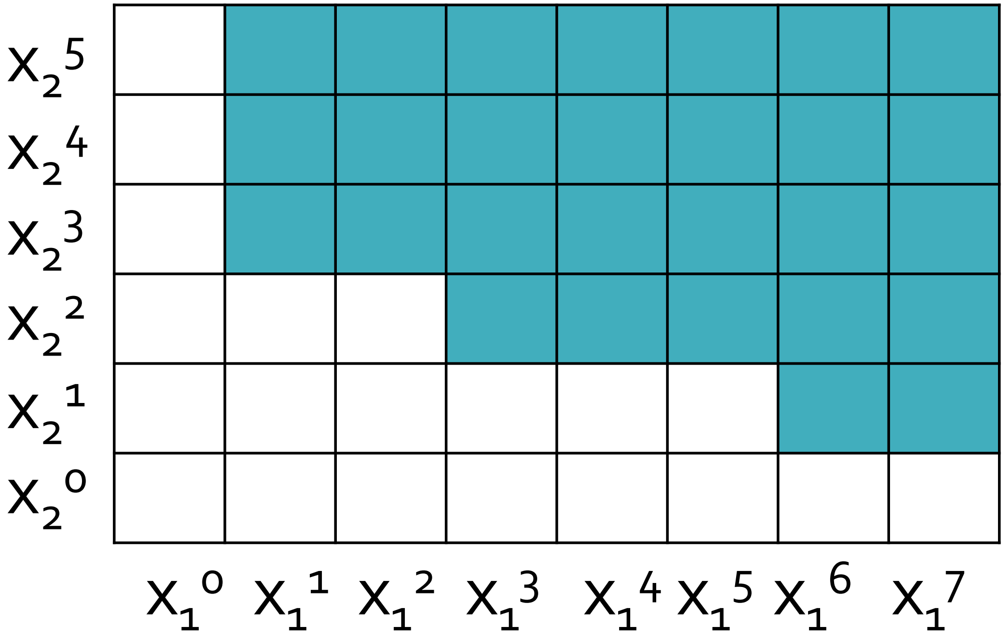
$$f_1 = \underline{x_1^3 x_2^2} + x_1^2 + x_1 x_2 + 4.$$



The Larger Picture

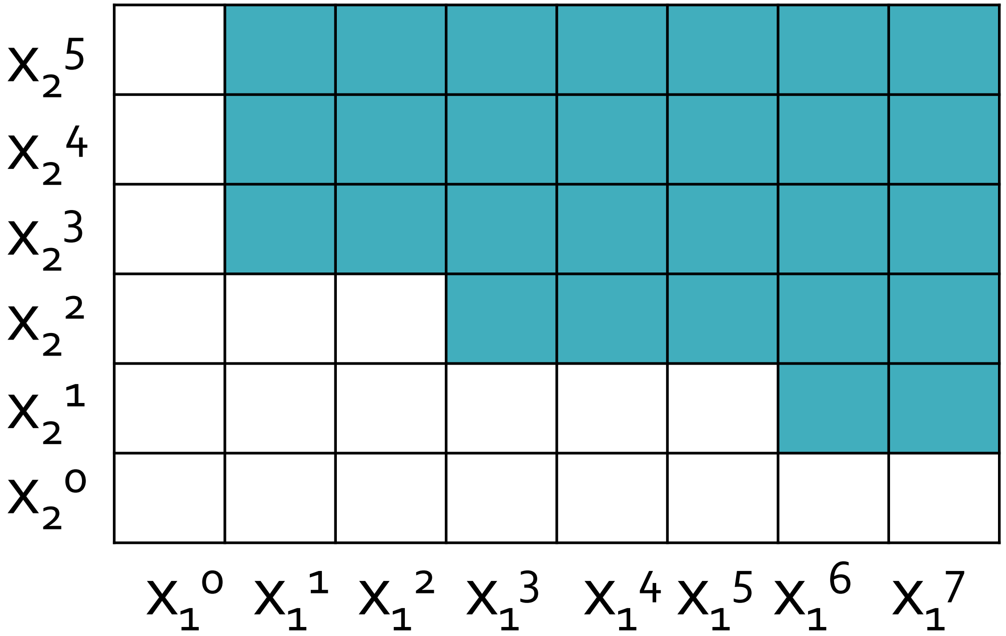
Look at the ideal generated by the **leading terms** of $f_1, \ldots, f_n$ (under some appropriate monomial ordering).

$$f_1 \quad = \quad \underline{x_1^3 x_2^2} + x_1^2 + x_1 x_2 + 4.$$



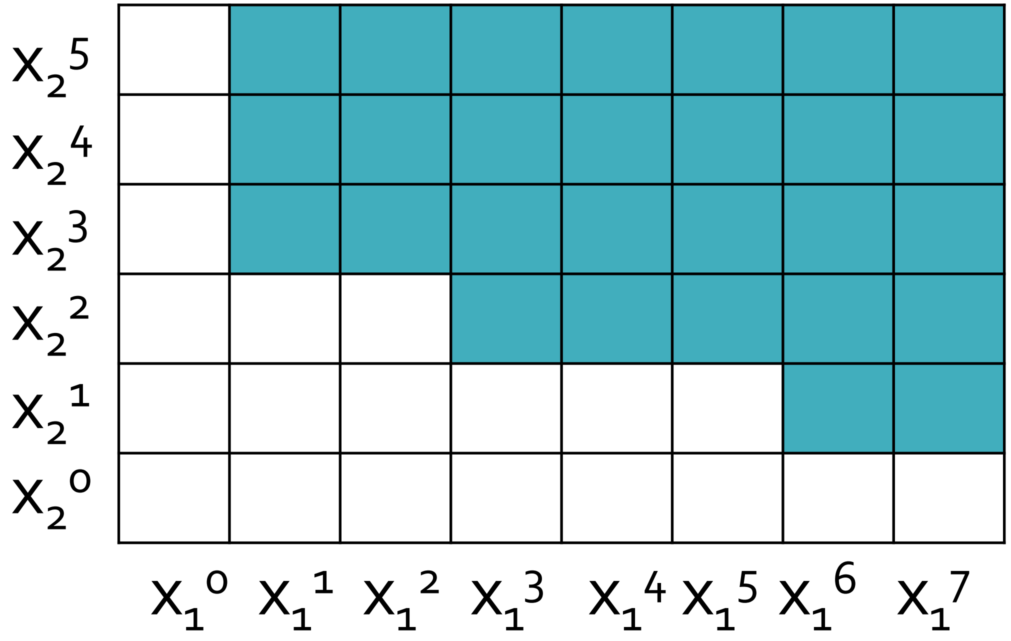
The Larger Picture

If we can find n elements in the ideal $(f_1, \ldots, f_n)$ whose leading terms are $x_1, \ldots, x_n$, respectively, we are done.



The Larger Picture

Buchberger's algorithm: Apply a process (like in single-variable case) to iteratively enlarge the ideal of leading coefficients until it is maximal. (I.e., compute a Groebner basis.)



The M-I Scheme: A Specific Attack

3.1 Linearizing

The M-I Scheme: A Specific Attack

$$y = x^{2^\theta + 1}$$

The M-I Scheme: A Specific Attack

Why this is bad news: The adversary knows (in some cases) that there exists a bilinear function B such that

$$B(x, F(x)) = 0$$

for all x and $B(\cdot, y) = 0$ always has a unique solution.

The M-I Scheme: A Specific Attack

Moral: When there's too much structure in the intermediate function, we leave the door open for an attack.

An Old Hack of Multivariate Cryptography (The Matsumoto-Imai Scheme)

Carl Miller

References:

J. Ding, J. Gower, D. Schimdt, *Multivariate Public Key Cryptosystems*, Advances in Information Security, vol. 25 (2006).

M. Sala et al., eds., *Grobner bases, coding, and cryptography*, Springer, 2009.