1 Introduction

Multivariate cryptography (MC) is the generic term for asymmetric cryptographic primitives based on multivariate polynomials over a finite field $\mathbb{F}$. The simplest examples of finite fields are the fields of prime order: $\mathbb{F}_p$ may be constructed as the integers modulo p.

This means MC is a system of nonlinear polynomial equations with coefficients over a finite field: $\mathbb{F} = \mathbb{F}_q$ with q elements:

$$\begin{aligned}
p^{(1)}(x_1, \ldots, x_n) &= \sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij}^{(1)} \cdot x_i x_j + \sum_{i=1}^{n} p_i^{(1)} \cdot x_i + p_0^{(1)} \\
p^{(2)}(x_1, \ldots, x_n) &= \sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij}^{(2)} \cdot x_i x_j + \sum_{i=1}^{n} p_i^{(2)} \cdot x_i + p_0^{(2)} \\
&\vdots \\
p^{(m)}(x_1, \ldots, x_n) &= \sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij}^{(m)} \cdot x_i x_j + \sum_{i=1}^{n} p_i^{(m)} \cdot x_i + p_0^{(m)}
\end{aligned}$$

If the polynomials have a degree of two, they are called multivariate quadratics (MQ). MC is very fast and only requires moderate computational resources, which makes it attractive for applications in low-cost devices.

2 Keys, Encryption and Decryption

In multivariate cryptography, the process to and fro a ciphertext $w \in \mathbb{F}^m$ and a message $z \in \mathbb{F}^n$ can be summarized in the image below.

$$\begin{array}{ccc}
z \in \mathbb{F}^n & \xrightarrow{\mathcal{P}} & w \in \mathbb{F}^m \\
\mathcal{T}\downarrow & & \uparrow\mathcal{S} \\
y \in \mathbb{F}^n & \xrightarrow{\mathcal{F}} & x \in \mathbb{F}^m
\end{array}$$

2.1 Keys

The public key of MC is the system of MC polynomials. To build this system based on the MQ problem, it needs an easily invertible quadratic map $\mathcal{F} : \mathbb{F}^n \to \mathbb{F}^m$, the so-called central map. Because it is easily invertible, it needs

to be hidden in the public key by invertible affine maps: $\mathcal{S} : \mathbb{F}^m \to \mathbb{F}^m$ and $\mathcal{T} : \mathbb{F}^n \to \mathbb{F}^n$ The public key of this system is a composed map:

$$\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T} : \mathbb{F}^n \to \mathbb{F}^m$$

and the private key consists of three maps $\mathcal{S}, \mathcal{F}$ and $\mathcal{T}$, also known as a trapdoor.
The public key should be hard to invert without the knowledge of the trapdoor.

2.2 Encryption

To get a ciphertext w, a message $z \in \mathbb{F}^n$ can be easily encrypted by evaluation of the public key $\mathcal{P}$:

$$w = \mathcal{P}(z) \in \mathbb{F}^m$$

2.3 Decryption

For the decryption of the ciphertext, it needs to be evaluated by the private key in three steps:

$$x = \mathcal{S}^{-1}(w) \in \mathbb{F}^m, y = \mathcal{F}^{-1}(x) \in \mathbb{F}^n, z = \mathcal{T}^{-1}(y) \in \mathbb{F}^n$$

There is a required condition $m \geq n$, this way the public key $\mathcal{P}$ will be injective and the decryption will output a unique plaintext.

3 Signature

Signatures are generated using the private key and are verified using the public key as follows. The message is hashed to a vector in $y \in \mathcal{F}^n$ via a known hash function. The signature is

$$x = \mathcal{P}^{-1}(y) = \mathcal{T}^{-1}\left(\mathcal{P}'^{-1}\left(\mathcal{S}^{-1}(y)\right)\right)$$

The receiver of the signed document must have the public key $\mathcal{P}$ in possession. He computes the hash y and checks that the signature x fulfils $\mathcal{P}(x) = y$.