Patarin's 'HFE' Public Key Signature

Mukesh Tiwari
Anisha Lamsal
Samrajya Raj Acharya

Supervisor : Dr. Gokul K.C.

Kathmandu University

Cryptographic Signature Schemes

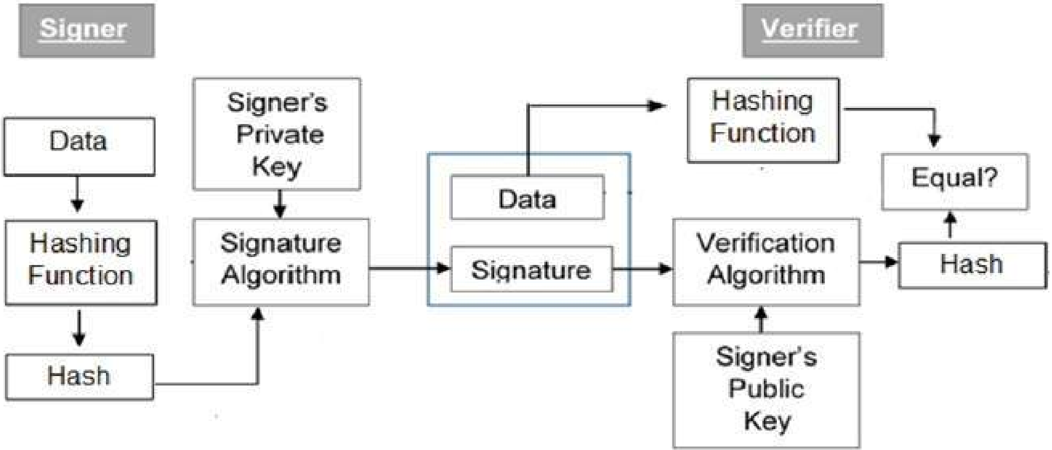


Figure 1: Digital Signature Schemes

Multivariate Polynomial System

use Multivariate Quadratic Polynomial system

Given a quadratic polynomial map $P : F_q^n \to F_q^m$ over a finite field F_q, find $x \in F_q^n$ that satisfies $P(x) = 0$.

Public key : quadratic polynomial map P

Private key : knowledge about inverting the map

let $m \in F_q^m$ be our message. then the signature s is simply $s \in F_q^n$ such that

$$P(s) = m$$

C-star

$$
\begin{tikzcd}
& Y \in \mathbb{E} \arrow[r, "\mathcal{F}"] & X \in \mathbb{E} \arrow[d, "\phi^{-1}"] & \\
\mathbf{z} \in \mathbb{F}^n \arrow[r, "\mathcal{T}"] \arrow[rrr, bend right, "\boxed{\mathcal{P}}"'] & \mathbf{y} \in \mathbb{F}^n \arrow[u, "\phi"] \arrow[r, "\bar{\mathcal{F}}"] & \mathbf{x} \in \mathbb{F}^n \arrow[r, "\mathcal{S}"] & \mathbf{w} \in \mathbb{F}^n
\end{tikzcd}
$$

Pros and Cons

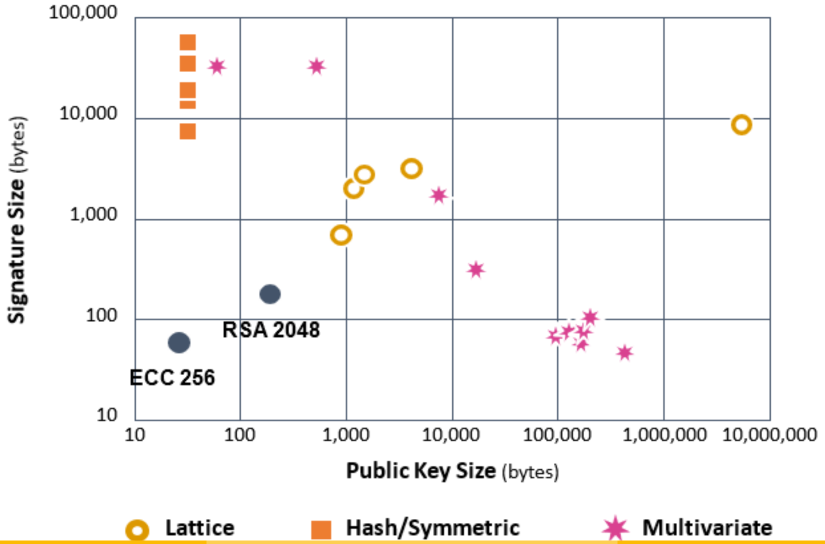
Advantages

- Small Signature Size
- Classical and Quantum Resilient
- Operations of finite field are easier

Disadvantages

- Large Public Key Size
- Difficulty in key generation

Key vs Signature Sizes



Computer Implementation

```
: q = 4
  F.<a> = GF(2^2)
  F
```

```
: Finite Field in a of size 2^2
```

```
: R.<x> = F[]
  R
```

```
: Univariate Polynomial Ring in x over Finite Field in a of size 2^2
```

```
R.<x1,x2,x3> = PolynomialRing(F)
R
```

```
Multivariate Polynomial Ring in x1, x2, x3 over Finite Field in a of size 2^2
```

```
z = vector([0,a,a+1])
S(vector(central_map(phi(T(z))).list()))
```

```
(a, a, 0)
```

github Repo : https://github.com/mukeshdroid/multivariate_signature_schemes