Rainbow and Mastumoto-Imai as Signature Schemes

Reporte de Estancia de Investigación

Pérez Ibarra Miguel Esteban **20th October 2020**

Indice

MPKC

- Multivariate Cryptography is the study of PKC's where the public key is given by a set of quadratic polynomials.

MPKC

- Multivariate Cryptography is the study of PKC's where the public key is given by a set of quadratic polynomials.

$$P = (p_1(w_1, \ldots, w_n), \ldots, p_m(w_1, \ldots, w_n))$$

MPKC

- Multivariate Cryptography is the study of PKC's where the public key is given by a set of quadratic polynomials.

$$P = (p_1(w_1, \ldots, w_n), \ldots, p_m(w_1, \ldots, w_n))$$

- These polynomials are defined on a finite field $\mathbb{K} = \mathbb{F}_q$.

Signature Scheme

Private Key for Rainbow

The maps

$$L_1 : K^{n-v} \mapsto K^{n-v},$$
$$L_2 : K^n \mapsto K^n, \text{ and}$$
$$F : K^n \mapsto K^{n-v}.$$

Signature Scheme

Public Key for Rainbow

The $n - v$ polynomial components of F and the algebraic structure of K

Signing a Document

To sign a document an entity A must consider the next steps:

- let m be a document, we first apply a hash function $h : M \mapsto K^{n-v}$ and get

$$\bar{m} = h(m)$$

Signing a Document

To sign a document an entity A must consider the next steps:

- let m be a document, we first apply a hash function $h : M \mapsto K^{n-v}$ and get
$$\bar{m} = h(m)$$
- apply the signing transformation S_A to $\bar{m}$ to get a digital signature
$$s^* = S_A(\bar{m}) = L_1^{-1} \circ F^{-1} \circ L_2^{-1}(\bar{m})$$

Signing a Document

To sign a document an entity A must consider the next steps:

- let m be a document, we first apply a hash function $h : M \mapsto K^{n-v}$ and get
$$\bar{m} = h(m)$$
- apply the signing transformation S_A to $\bar{m}$ to get a digital signature
$$s^* = S_A(\bar{m}) = L_1^{-1} \circ F^{-1} \circ L_2^{-1}(\bar{m})$$
- define the verification transformation $V_A : M_h S \mapsto \{true, false\}$
$$V_{A,h}(\bar{m}, s^*) = \begin{cases} true & \text{if } L_1 \circ F \circ L_2(s^*) := h(m) \\ false & \text{otherwise,} \end{cases} .$$

Verifying the signature

Once entity A hands over the document m, s^*, and $V_{A,h}$

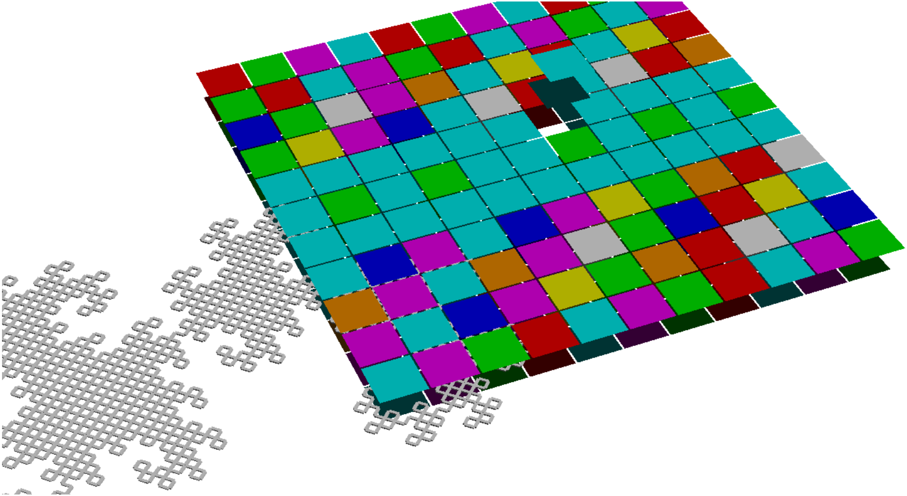
- Entity B must evaluate $\bar{m} = h(m)$

Verifying the signature

Once entity A hands over the document m, s^*, and $V_{A,h}$

- Entity B must evaluate $\bar{m} = h(m)$
- given $\bar{m}$ and s^*, compute $u = V_{A,h}(\bar{m}, s^*)$

Matsumoto-Imai Signature Scheme



Private Key

Properties

- $F(X) = X^{1+q^i}, \forall X \in K^n$

Private Key

Properties

- $F(X) = X^{1+q^i}, \forall X \in K^n$
- $\tilde{F}(X) := \varphi \circ F \circ \varphi^{-1}(X)$

Private Key

Properties

- $F(X) = X^{1+q^i}, \forall X \in K^n$
- $\tilde{F}(X) := \varphi \circ F \circ \varphi^{-1}(X)$
- entity A must choose $r < n$ linear maps $z_1, \ldots, z_r$

Private Key

Properties

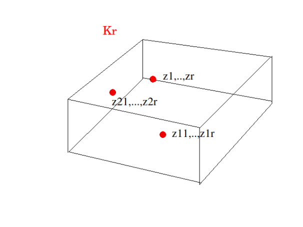
- $F(X) = X^{1+q^i}, \forall X \in K^n$
- $\tilde{F}(X) := \varphi \circ F \circ \varphi^{-1}(X)$
- entity A must choose $r < n$ linear maps $z_1, \ldots, z_r$
- 

Figure: The set of z's available for entity A

Private Key

Properties

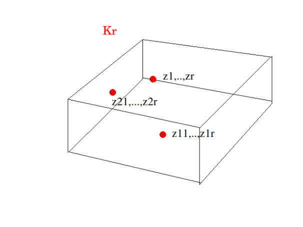
- $F(X) = X^{1+q^i}, \forall X \in K^n$
- $\tilde{F}(X) := \varphi \circ F \circ \varphi^{-1}(X)$
- entity A must choose $r < n$ linear maps $z_1, \ldots, z_r$
- 

Figure: The set of z's available for entity A

- $z_i(x_1, \ldots, x_n) := \sum_{j=1}^{n} \alpha_{ji} x_j + \beta_i$

Private Key

Properties

- Entity A must also define a random map $f : K^r \mapsto K^n$ given by
$$f(z_1, \ldots, z_r) := (f_1(z_1, \ldots, z_r), \ldots, f_n(z_1, \ldots, z_r))$$

Private Key

Properties

- Entity A must also define a random map $f : K^r \mapsto K^n$ given by

$$f(z_1, \ldots, z_r) := (f_1(z_1, \ldots, z_r), \ldots, f_n(z_1, \ldots, z_r))$$

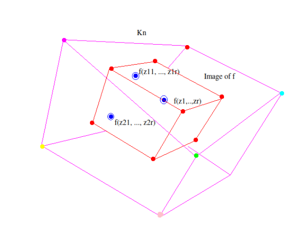
- 

Figure: Image of all the z's in K^r

Private Key

Properties

- Entity A defines the set P of all the pairs (λ, μ) such that

Private Key

Properties

- Entity A defines the set P of all the pairs (λ, μ) such that
  - $\lambda := (z_1(x, \ldots, x_n), \ldots, z_r(x, \ldots, x_n))$

Private Key

Properties

- Entity A defines the set P of all the pairs (λ, μ) such that
  - $\lambda := (z_1(x, \ldots, x_n), \ldots, z_r(x, \ldots, x_n))$
  - $\mu := f(\lambda)$

Private Key

Properties

- Entity A defines the set P of all the pairs (λ, μ) such that
  - $\lambda := (z_1(x, \ldots, x_n), \ldots, z_r(x, \ldots, x_n))$
  - $\mu := f(\lambda)$

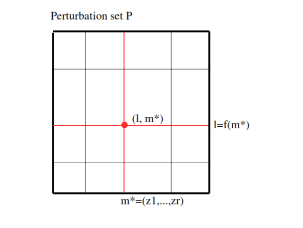


Figure: Perturbation points

Private Key

Properties

The final property is are the linear maps:

$$L_1, L_2 : K^n \mapsto K^n$$

Public key

Properties

- The n multivariate polynomial components of F

Public key

Properties

- The n multivariate polynomial components of F
- the algebraic structure of K

Signature generation

Signing process

Generating a signature s^* for an entity A goes as follows:

- given a message $m \in M$ apply the hash function $h : M \mapsto K^n$

$$\tilde{m} := h(m)$$

Signature generation

Signing process

Generating a signature s^* for an entity A goes as follows:

- given a message $m \in M$ apply the hash function $h : M \mapsto K^n$

$$\tilde{m} := h(m)$$

- define the map $\bar{\bar{F}} := \tilde{F} + f(\lambda)$

Signature generation

Signing process

Generating a signature s^* for an entity A goes as follows:

- given a message $m \in M$ apply the hash function $h : M \mapsto K^n$

$$\tilde{m} := h(m)$$

- define the map $\bar{\bar{F}} := \tilde{F} + f(\lambda)$
- finally we encapsulate $\hat{F} := L_1 \circ \bar{\bar{F}} \circ L_2$

Signature generation

Signing process

Generating a signature s^* for an entity A goes as follows:

- given a message $m \in M$ apply the hash function $h : M \mapsto K^n$

$$\tilde{m} := h(m)$$

- define the map $\bar{\bar{F}} := \tilde{F} + f(\lambda)$
- finally we encapsulate $\hat{F} := L_1 \circ \bar{\bar{F}} \circ L_2$
- our **digital signature** is then

$$s^* := \hat{F}(\bar{m})$$

Verification Process

Verification

Given m, and s^*, entity B must follow the steps:

- Compute $\bar{y} := L_1^{-1}(s^*)$

Verification Process

Verification

Given m, and s^*, entity B must follow the steps:

- Compute $\bar{y} := L_1^{-1}(s^*)$
- For any $(\lambda_0, \mu_0) \in P$ we compute

$$y_{\lambda_0} := \varphi^{-1} \circ F^{-1}(\bar{y} + \lambda_0)$$

Verification Process

Verification

Given m, and s^*, entity B must follow the steps:

- Compute $\bar{y} := L_1^{-1}(s^*)$
- For any $(\lambda_0, \mu_0) \in P$ we compute

$$y_{\lambda_0} := \varphi^{-1} \circ F^{-1}(\bar{y} + \lambda_0)$$

- If $Z(y_{\lambda_0}) := \mu_0$ go to the next step

Verification Process

Verification

Given m, and s^*, entity B must follow the steps:

- Compute $\bar{y} := L_1^{-1}(s^*)$
- For any $(\lambda_0, \mu_0) \in P$ we compute

$$y_{\lambda_0} := \varphi^{-1} \circ F^{-1}(\bar{y} + \lambda_0)$$

- If $Z(y_{\lambda_0}) := \mu_0$ go to the next step
- Finally if $\bar{m}_0 := L_2^{-1}(y_\lambda)$ is such that $\bar{m}_0 = h(m)$, we are done.

References I

W. Gilbert.
Modern Algebra With Applications.
Wiley-Interscience, 2004.

D. Bernstein.
Post-Quantum Cryptography.
Springer, 2009.

J. Ding.
A New Variant of the Matsumoto-Imai Cryptosystem through Perturbation.
PKC 2004, LNC 2947, pp.305-318 2004

Pérez Ibarra Miguel Esteban

Rainbow and Mastumoto-Imai as Signature Schemes

Reporte de Estancia de Investigación