Introduction to Multivariate Public Key Cryptography

Geovandro Carlos C. F. Pereira

PhD advisor: Prof. Dr. Paulo S. L. M. Barreto

LARC - Computer Architecture and Networking Lab
Department of Computer Engineering and Digital Systems
Escola Politécnica
University of Sao Paulo

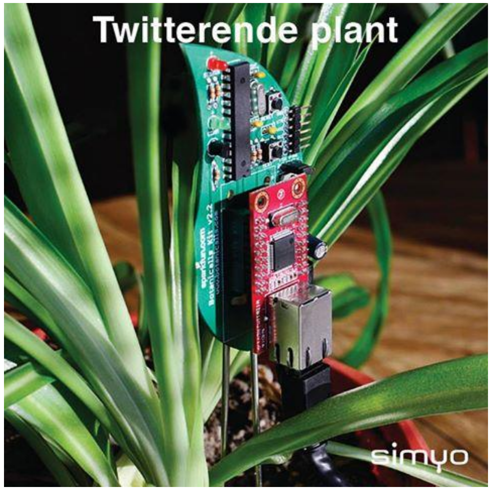
Agenda

- Motivation to Post-Quantum Crypto
- Introduction to MPKC
  - Matsumoto-Imai Encryption
  - UOV Signature
- Technique for Key Size Reduction
- Security Analysis

Motivation

Internet of Things (IoT)

Any object connected to the internet

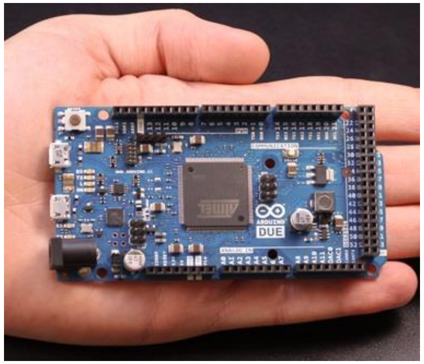


Motivation

- **Typical Platforms**

Smartcard (Java Card)

Sensor node



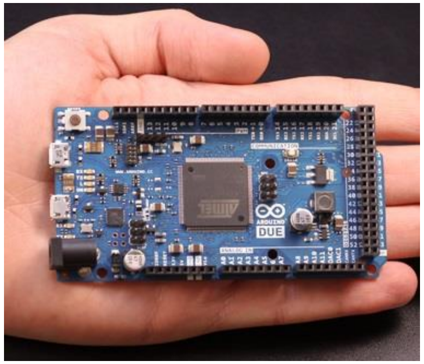
Arduino

Motivation

- **Typical Platforms**

Smartcard (Java Card)

Sensor node



Arduino

- **Resources**
  - **Instruction set of 8, 16 or 32 bits**
  - **Small amount of RAM(2-8 KiB) and ROM (32-128 KiB)**
  - **Low clock: 5-40 MHz**
  - **Energy is expensive**

Motivation

- Symmetric Crypto: ok

Motivation

- Symmetric Crypto: ok
- Conventional Asymmetric Criptography: bottleneck

Security relies on a few computational problems.

Motivation

- Symmetric Crypto: ok
- Conventional Asymmetric Criptography: bottleneck

Security relies on a few computational problems.

"Complex" operations (e.g. multiple-precision arithmetic).

Motivation

- Symmetric Crypto: ok
- Conventional Asymmetric Criptography: bottleneck

  Security relies on a few computational problems.

  “Complex” operations (e.g. multiple-precision arithmetic).

  Threats in medium and long-terms:

  - Shor [1997]

    Quantum algorithm for DLP e IFP

Motivation

- Symmetric Crypto: ok
- Conventional Asymmetric Criptography: bottleneck

  Security relies on a few computational problems.

  "Complex" operations (e.g. multiple-precision arithmetic).

  Threats in medium and long-terms:

  - Shor [1997]

    Quantum algorithm for DLP e IFP
  - Barbulescu, Joux,...[2013]

    Conventional algorithms for DLP over binary fields in quase-polynomial time

    End of pairings over binary fields (it was the most suitable for WSNs)

Motivation

- Symmetric Crypto: ok
- Conventional Asymmetric Criptography: bottleneck

  Security relies on a few computational problems.

  “Complex” operations (e.g. multiple-precision arithmetic).

  Threats in medium and long-terms:

  - Shor [1997]

    Quantum algorithm for DLP e IFP

  - Barbulescu, Joux,...[2013]

    Conventional algorithms for DLP over binary fields in quase-polynomial time

    End of pairings over binary fields (it was the most suitable for WSNs)

- **Need for alternatives!**

Motivation

- Post-Quantum Cryptography

  Cryptosystems that resist to quantum algorithms.

Motivation

- Post-Quantum Cryptography

  Cryptosystems that resist to quantum algorithms.

  Main lines of research:

  - Hash-based
    - Very efficient, large signatures.

Motivation

- Post-Quantum Cryptography

  Cryptosystems that resist to quantum algorithms.

  Main lines of research:

  - Hash-based
    - Very efficient, large signatures.
  - Code-based
    - Public Key Encryption schemes
    - Singatures (one-time, large keys)

Motivation

- Post-Quantum Cryptography

  Cryptosystems that resist to quantum algorithms.

  Main lines of research:

  - Hash-based
    - Very efficient, large signatures.
  - Code-based
    - Public Key Encryption schemes
    - Singatures (one-time, large keys)
  - Lattice-based
    - Encryption, Digital signatures, FHE

Motivation

- Post-Quantum Cryptography

  Cryptosystems that resist to quantum algorithms.

  Main lines of research:

  - Hash-based
    - Very efficient, large signatures.
  - Code-based
    - Public Key Encryption schemes
    - Singatures (one-time, large keys)
  - Lattice-based
    - Encryption, Digital signatures, FHE
  - **Multivariate Quadratic (MQ)**
    - **Some digital signature schemes are robust (original UOV, 14 years)**
    - **Most of the encryption constructions were broken (Jintai has a new perspective about it)**

Departamento de Engenharia de Computação e Sistemas Digitais

Motivation

- Conventional Public Key Cryptography
  - Need coprocessors in smartcards.
    - Low flexibility for use or optimizations.

Motivation

- Conventional Public Key Cryptography
  - Need coprocessors in smartcards.
    - Low flexibility for use or optimizations.
- Advantages of MPKC
  - Simplicity of Operations (matrices and vectors).
  - Small fields avoid multiple-precision arithmetic.
  - Long term security. (prevention against spying)
  - Efficiency

    Signature generation in 804 cycles by Ding [ASAP 2008].

Motivation

- Conventional Public Key Cryptography
  - Need coprocessors in smartcards.
    - Low flexibility for use or optimizations.
- Advantages of MPKC
  - Simplicity of Operations (matrices and vectors).
  - Small fields avoid multiple-precision arithmetic.
  - Long term security. (prevention against spying)
  - Efficiency

    Signature generation in 804 cycles by Ding [ASAP 2008].
- Main Challenge
  - Relatively large key sizes.

- MPKC Constructions

Multivariate Public Key Cryptography

- Basic Property:
  - Cryptosystems whose public keys are a set of multivariate polynomials.

Multivariate Public Key Cryptography

- Basic Property:
  - Cryptosystems whose public keys are a set of multivariate polynomials.

- Notation: the public key is given as:

$$P(x_1, \cdots, x_n) = (p_1(x_1, \cdots, x_n), p_2(x_1, \cdots, x_n), \cdots, p_m(x_1, \cdots, x_n))$$

MPKC Encryption

- Given a plaintext $M = (x_1, \cdots, x_n)$.

MPKC Encryption

- Given a plaintext $M = (x_1, \cdots, x_n)$.
- Ciphertext is simply a polynomial evaluation:

$$P(M) = (p_1(x_1, \cdots, x_n), \cdots, p_m(x_1, \cdots, x_n)) = (c_1, \cdots, c_m)$$

MPKC Encryption

- Given a plaintext $M = (x_1, \cdots, x_n)$.
- Ciphertext is simply a polynomial evaluation:

$$P(M) = (p_1(x_1, \cdots, x_n), \cdots, p_m(x_1, \cdots, x_n)) = (c_1, \cdots, c_m)$$

- To decrypt one needs to know a trapdoor so that it is feasible to invert the quadratic map to find the plaintext:

$$(x_1, \cdots, x_n) = P^{-1}(c_1, \cdots, c_m)$$

MPKC Signature

- Public Key:

$$P(x_1, \cdots, x_n) = (p_1(x_1, \cdots, x_n), \cdots, p_m(x_1, \cdots, x_n))$$

MPKC Signature

- Public Key:

$$P(x_1, \cdots, x_n) = (p_1(x_1, \cdots, x_n), \cdots, p_m(x_1, \cdots, x_n))$$

- Private Key: a trapdoor for computing P^{-1}.

MPKC Signature

- Public Key:

$$P(x_1, \cdots, x_n) = (p_1(x_1, \cdots, x_n), \cdots, p_m(x_1, \cdots, x_n))$$

- Private Key: a trapdoor for computing P^{-1}.

- Sign: given a hash $(h_1, \cdots, h_m)$, compute

$$(x_1, \cdots, x_n) = P^{-1}(h_1, \cdots, h_m)$$

MPKC Signature

- Public Key:

$$P(x_1, \cdots, x_n) = (p_1(x_1, \cdots, x_n), \cdots, p_m(x_1, \cdots, x_n))$$

- Private Key: a trapdoor for computing P^{-1}.

- Sign: given a hash $(h_1, \cdots, h_m)$, compute

$$(x_1, \cdots, x_n) = P^{-1}(h_1, \cdots, h_m)$$

- Verify: $(h_1, \cdots, h_n) = P(x_1, \cdots, x_m)$

Departamento de Engenharia de Computação
e Sistemas Digitais

MPKC Signature

- Public Key:

$$P(x_1, \cdots, x_n) = (p_1(x_1, \cdots, x_n), \cdots, p_m(x_1, \cdots, x_n))$$

- Private Key: a trapdoor for computing P^{-1}.

- Sign: given a hash $(h_1, \cdots, h_m)$, compute

$$(x_1, \cdots, x_n) = P^{-1}(h_1, \cdots, h_m)$$

- Verify: $(h_1, \cdots, h_n) = P(x_1, \cdots, x_m)$

- All vars. and coeffs. are in the small field k.

Security

- Direct attack is to solve the set of equations:

$$P(M) = P(p_1(x_1, \cdots, x_n), \cdots, p_m(x_1, \cdots, x_n)) = (c_1, \cdots, c_m)$$

Security

- Direct attack is to solve the set of equations:

$$P(M) = P(p_1(x_1, \cdots, x_n), \cdots, p_m(x_1, \cdots, x_n)) = (c_1, \cdots, c_m)$$

- Solving a set of m randomly chosen (nonlinear) equations with n variables is NP-complete.

Security

- Direct attack is to solve the set of equations:

$$P(M) = P(p_1(x_1, \cdots, x_n), \cdots, p_m(x_1, \cdots, x_n)) = (c_1, \cdots, c_m)$$

- Solving a set of m randomly chosen (nonlinear) equations with n variables is NP-complete.

- **But this does not necessarily ensure the security of the systems.**

Security

- Most of the schemes do not use exactly random maps.

Security

- Most of the schemes do not use exactly random maps.
- Many systems have the structure

$$P(x_1, \cdots, x_n) = L_1 \circ F \circ L_2(x_1, \cdots, x_n)$$

Security

- Most of the schemes do not use exactly random maps.
- Many systems have the structure

$$P(x_1, \cdots, x_n) = L_1 \circ F \circ L_2(x_1, \cdots, x_n)$$

- F is a quadratic map with certain structure. (central map)

Security

- Most of the schemes do not use exactly random maps.
- Many systems have the structure

$$P(x_1, \cdots, x_n) = L_1 \circ F \circ L_2(x_1, \cdots, x_n)$$

- F is a quadratic map with certain structure. (central map)
- This structure enables computing F^{-1} easily.

Security

- Most of the schemes do not use exactly random maps.
- Many systems have the structure

$$P(x_1, \cdots, x_n) = L_1 \circ F \circ L_2(x_1, \cdots, x_n)$$

- F is a quadratic map with certain structure. (central map)
- This structure enables computing F^{-1} easily.
- L_1 and L_2 are full-rank linear maps used to hide F.

Security

- **MQ-Problem**: Given a set of m **quadratic** polynomials in n variables $\mathrm{x} = (x_1, \cdots, x_n)$, solve the system:

$$p_1(x) = \cdots = p_m(x) = 0$$

Security

- **MQ-Problem**: Given a set of m **quadratic** polynomials in n variables $\mathrm{x} = (x_1, \cdots, x_n)$, solve the system:

$$p_1(x) = \cdots = p_m(x) = 0$$

- **IP-Problem**: Given two polynomial maps $F_1, F_2: K^n \longrightarrow K^m$. The problem is to look for two linear transformations $L_1\ and$ L_2 (if they exist) s.t.:

$$F_1(x_1, \cdots, x_n) = L_1 \circ F \circ L_2(x_1, \cdots, x_n)$$

Multivariate Quadratic Construction

- MQ system with m equations in n vars, all coefs. in $\mathbb{F}_q$:

Polynomial notation:

$$p_k(x_1, \dots, x_n) \coloneqq \sum\nolimits_{i,j} P_{ij}^{(k)} x_i x_j + \sum\nolimits_{i} L_i^{(k)} x_i + c^{(k)}$$

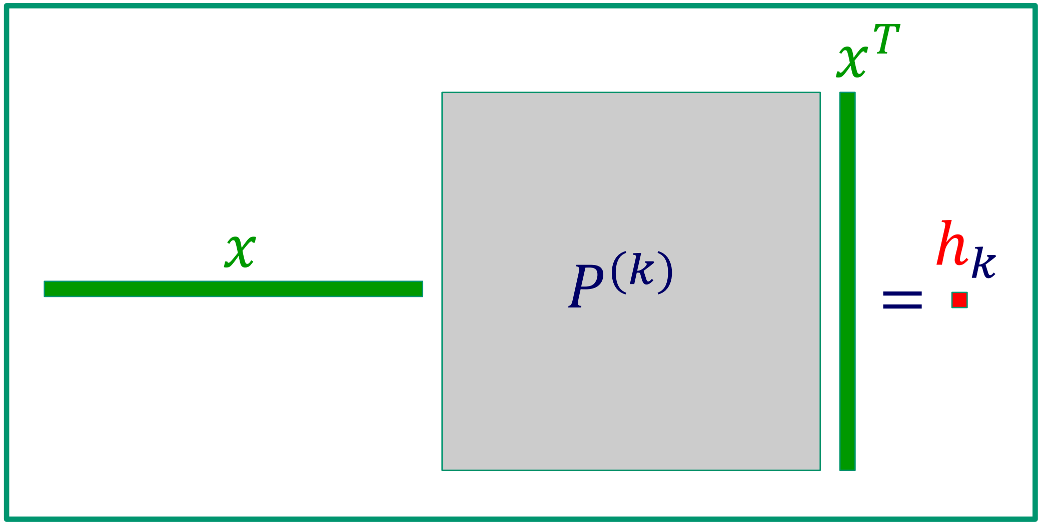
Vector notation:

$$p_k(x_1, \dots, x_n) = x P^{(k)} x^T + L^{(k)} x + c^{(k)}$$

(Pure) Quadratic Map

$$\mathcal{P}(x) = h \iff$$

$$x\, P^{(k)}\, x^T = h_k \ \ (k = 1, \ldots, m)$$



Matsumoto-Imai Cryptosystem

- Previously, many unsuccesfull attempts to construct an encryption scheme.
    - Small number of variables.
    - Huge key sizes.
- In 1988, Matsumoto and Imai adopted a “Big” Field in their C* construction.

Matsumoto-Imai Cryptosystem

- k is a small finite field with $|k| = q$.

Matsumoto-Imai Cryptosystem

- k is a small finite field with $|k| = q$.
- $\overline{K} = k[x]/(g(x))$ a degree n extension of k.

Matsumoto-Imai Cryptosystem

- k is a small finite field with $|k| = q$.
- $\overline{K} = k[x]/(g(x))$ a degree n extension of k.
- The linear map $\phi: \overline{K} \to k^n$ and $\phi^{-1}: k^n \to \overline{K}$.

$$\phi(a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}) = (a_0, a_1, \cdots, a_{n-1})$$

Matsumoto-Imai Cryptosystem

- k is a small finite field with $|k| = q$.
- $\bar{K} = k[x]/(g(x))$ a degree n extension of k.
- The linear map $\phi: \bar{K} \to k^n$ and $\phi^{-1}: k^n \to \bar{K}$.

$$\phi(a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}) = (a_0, a_1, \cdots, a_{n-1})$$

- Build a map $\bar{F}$ over $\bar{K}$:

$$\bar{F} = L_1 \circ \phi \circ F \circ \phi^{-1} \circ L_2$$

where the L_i are randomly chosen invertible maps over k^n

Matsumoto-Imai Cryptosystem

- k is a small finite field with $|k| = q$.
- $\bar{K} = k[x]/(g(x))$ a degree n extension of k.
- The linear map $\phi: \bar{K} \rightarrow k^n$ and $\phi^{-1}: k^n \rightarrow \bar{K}$.

$$\phi(a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}) = (a_0, a_1, \cdots, a_{n-1})$$

- Build a map $\bar{F}$ over $\bar{K}$:

$$\bar{F} = L_1 \circ \phi \circ F \circ \phi^{-1} \circ L_2$$

where the L_i are randomly chosen invertible maps over k^n

- Inversion of $\bar{F}$ is related to the IP Problem

Matsumoto-Imai Cryptosystem

- The map F adopted was:

$$F \ : \overline{K} \longrightarrow \overline{K}$$

$$X \longmapsto X^{q^{\theta}+1}$$

Matsumoto-Imai Cryptosystem

- The map F adopted was:

$$F \ : \overline{K} \longrightarrow \overline{K}$$

$$X \longmapsto X^{q^{\theta}+1}$$

- Let

$$\tilde{F}(x_1, \cdots, x_n) = \phi \circ F \circ \phi^{-1}(x_1, \cdots, x_n) = (\widetilde{F_1}(x_1, \cdots, x_n), \cdots, \tilde{F}_m(x_1, \cdots, x_n))$$

Matsumoto-Imai Cryptosystem

- The map F adopted was:

$$\begin{aligned} F\ &: \overline{K} \longrightarrow \overline{K} \\ X &\longmapsto X^{q^{\theta}+1} \end{aligned}$$

- Let

$$\tilde{F}(x_1,\cdots,x_n) = \phi \circ F \circ \phi^{-1}(x_1,\cdots,x_n) = (\widetilde{F_1}(x_1,\cdots,x_n),\cdots,\tilde{F}_m(x_1,\cdots,x_n))$$

- $\widetilde{F_i}$ are quadratic polynomials because the map $X \longmapsto X^{q^{\theta}}$ is linear (it is the Frobenius automorphism of order θ).

Matsumoto-Imai Cryptosystem

- Encryption is done by the quadratic map over k^n

$$\bar{F} = L_1 \circ \phi \circ F \circ \phi^{-1} \circ L_2$$

where L_i are affine maps over k^n.

Matsumoto-Imai Cryptosystem

- Encryption is done by the quadratic map over k^n

$$\bar{F} = L_1 \circ \phi \circ F \circ \phi^{-1} \circ L_2$$

where L_i are affine maps over k^n.

- Decryption is the inverse process

$$\bar{F}^{-1} = L_2^{-1} \circ \phi \circ F^{-1} \circ \phi^{-1} \circ L_1^{-1}$$

Matsumoto-Imai Cryptosystem

- Requirement: G.C.D. $\left(q^{\theta}+1, q^{n}-1\right)=1$

to ensure the invertibility of the decryption map $\bar{F}^{-1}$

Matsumoto-Imai Cryptosystem

- Requirement: G.C.D. $\left(q^{\theta}+1, q^{n}-1\right)=1$

to ensure the invertibility of the decryption map $\bar{F}^{-1}$

- $F^{-1}(X)=X^{t}, X \in \bar{K}$ where $t \times \left(q^{\theta}+1\right) \equiv 1\, mod(q^{n}-1)$.
- The public key includes k and $\bar{F} = (\bar{F}_1, \cdots, \bar{F}_n)$
- The private key includes L_1, L_2 and $\bar{K}$.

UOV Signature

- Trapdoor to invert F [Patarin]

UOV Signature

- Trapdoor to invert F [Patarin]
- $h = Hash(M)$

UOV Signature

- Trapdoor to invert F [Patarin]
- $h = Hash(M)$
- Split vars. into 2 sets: *oil* variables: $\mathrm{O} \coloneqq (x_1, \cdots, x_o)$
  vinegar variables: $V \coloneqq (x'_1, \dots, x'_v)$

UOV Signature

- Trapdoor to invert F [Patarin]
- $h = Hash(M)$
- Split vars. into 2 sets: *oil* variables: $0 := (x_1, \cdots, x_o)$
  vinegar variables: $V := (x'_1, \ldots, x'_v)$

$$f_k(x_1, \cdots, \mathrm{x}_o, x'_1, \ldots, x'_v\ ) = h_k =$$

$$= \sum_{O \times V} F_{ij}^{(k)} x_i x'_j + \sum_{V \times V} F_{ij}^{(k)} x'_i x'_j + \sum_{O} L_i^{(k)} x_i + \sum_{V} L_i^{(k)} x'_i + c^{(k)}$$

UOV Signature

- Trapdoor to invert F [Patarin]
- $h = Hash(M)$
- Choose uniformly at random *vinegars:* $V \coloneqq (x'_1, \dots, x'_v)$

$$f_k(x_1, \cdots, \mathrm{x}_o, x'_1, \dots, x'_v) = h_k =$$

$$= \sum_{O\times V} F_{ij}^{(k)} x_i {x'}_j + \sum_{V\times V} F_{ij}^{(k)} {x'}_i {x'}_j + \sum_{O} L_i^{(k)} x_i + \sum_{V} L_i^{(k)} {x'}_i + c^{(k)}$$

UOV Signature

- Trapdoor to invert F [Patarin]
- $h = Hash(M)$
- Fix vinegars: $V \coloneqq (x'_1, \dots, x'_v)$

$$f_k(x_1, \cdots, \mathrm{x}_o, x'_1, \dots, x'_v\ ) = h_k$$

$$= \sum_{O \times V} F_{ij}^{(k)} x_i x'_j + \sum_{V \times V} F_{ij}^{(k)} x'_i x'_j + \sum_{O} L_i^{(k)} x_i + \sum_{V} L_i^{(k)} x'_i + c^{(k)}$$

- This becomes an oxo system of linear equations.

UOV Signature

- Trapdoor to invert F [Patarin]
- $h = Hash(M)$
- Fix *vinegars:* $V \coloneqq (x'_1, \ldots, x'_v)$

$$f_k(x_1, \cdots, \mathrm{x}_o, x'_1, \ldots, x'_v) =$$

$$= \sum_{O \times V} F_{ij}^{(k)} x_i x'_j + \sum_{V \times V} F_{ij}^{(k)} x'_i x'_j + \sum_{O} L_i^{(k)} x_i + \sum_{V} L_i^{(k)} x'_i + c^{(k)}$$

- This becomes an oxo system of linear equations.

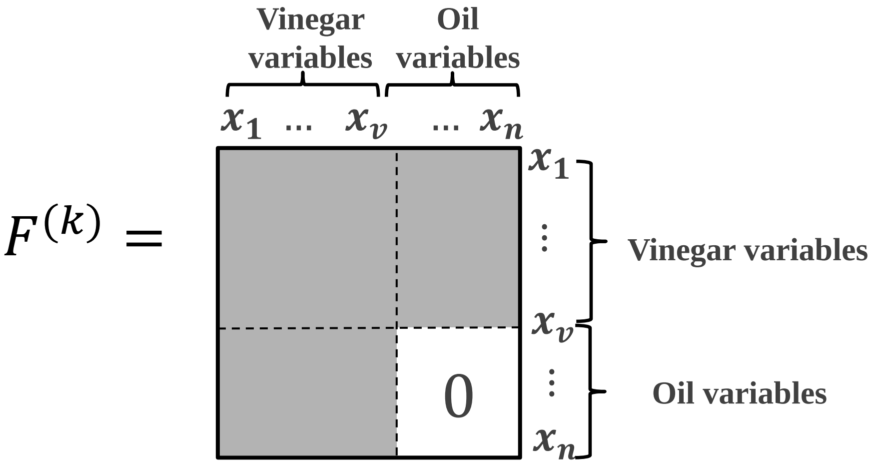
- It has a solution with high probability ($\approx 1 - 1/q$).

Departamento de Engenharia de Computação
e Sistemas Digitais

UOV Signature

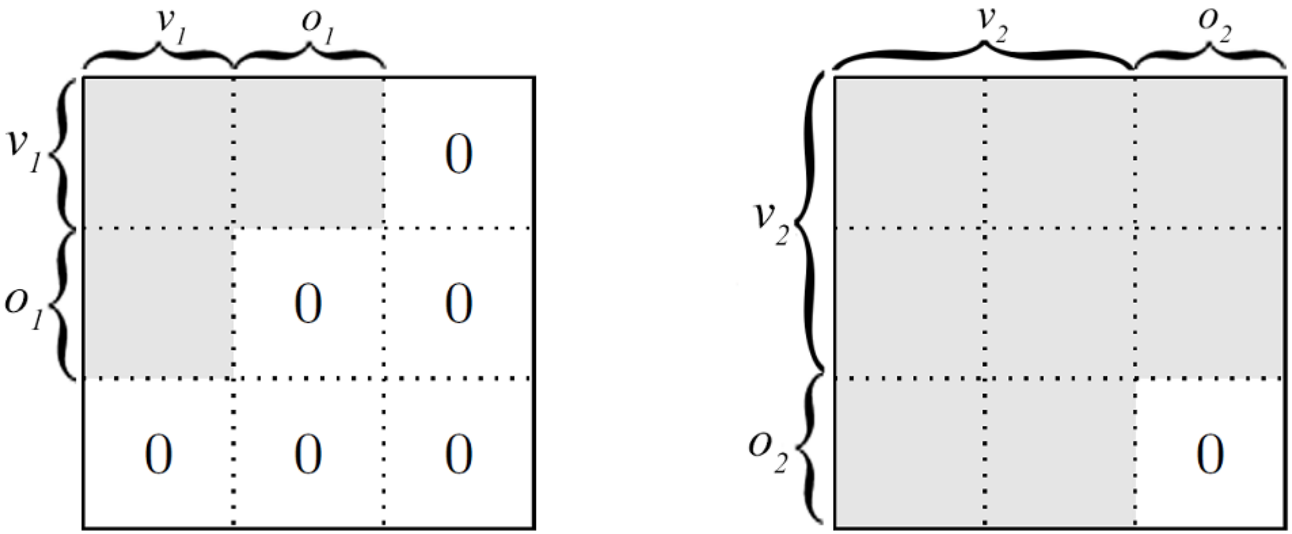
- Trapdoor to invert F [Patarin]

- Oil variables not mixed.



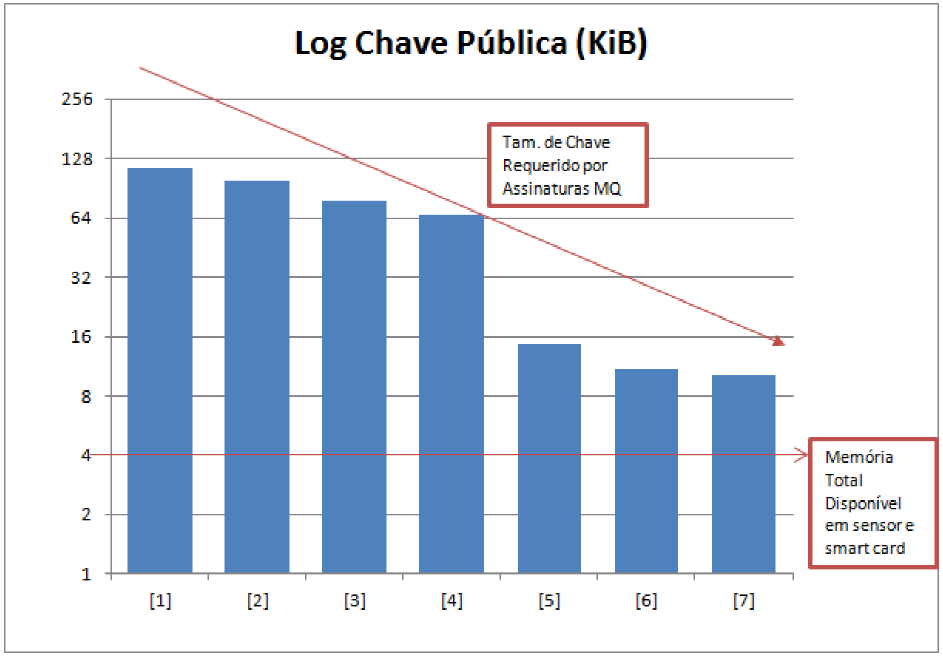
Rainbow Signature

- Rainbow Quadratic Map



MQ Signatures

- UOV key sizes.



Scheme	Public Key (KiB)
Rainbow($\mathbb{F}_{2^4}$, 30,29,29)	113.4
Rainbow($\mathbb{F}_{2^8}$, 29,20,20)	99.4
Rainbow($\mathbb{F}_{31}$, 25,24,24)	77.7
NC-Rainbow($\mathbb{F}_{2^8}$, 17,13,13)	66.7
CyclicUOV($\mathbb{F}_{2^8}$, 26,25)	14.5
UOVLRS($\mathbb{F}_{2^8}$, 26,52,26)	11.0
CyclicRainbow($\mathbb{F}_{2^8}$, 17,13,13)	10.2

- Technique for Key Size Reduction

MQ Signatures - Cyclic UOV

- Technique for reduction of UOV public keys.

MQ Signatures - Cyclic UOV

- Technique for reduction of UOV public keys.

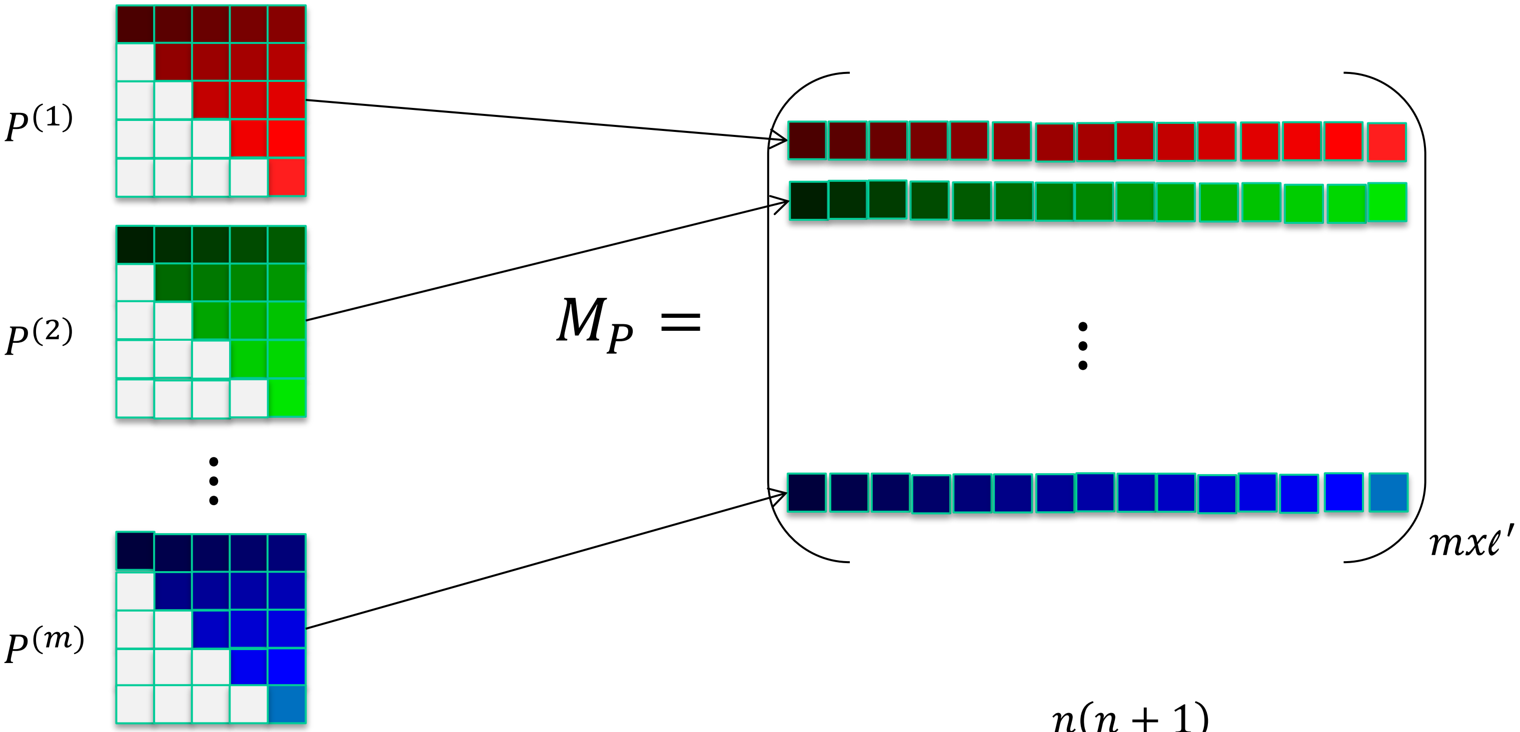
- Part of the public key with short representation.

MQ Signatures - Cyclic UOV

- Technique for reduction of UOV public keys.
- Part of the public key with short representation.
- Achieves a 6x reduction factor for 80-bit security.

MQ Signatures - Cyclic UOV

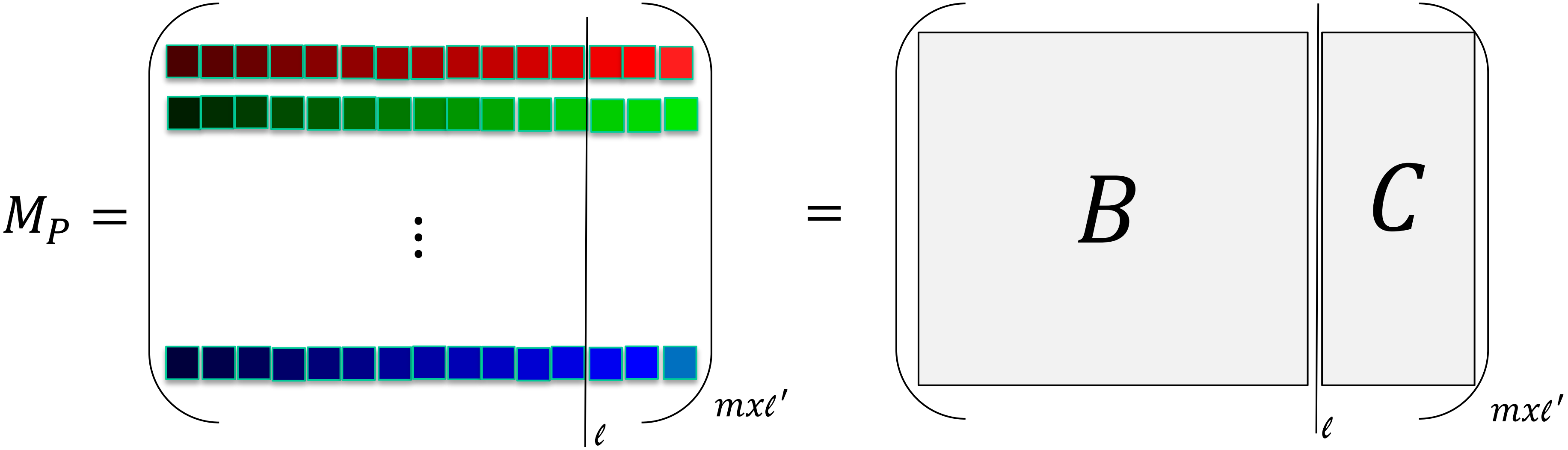
Public matrix of coefficients M_P



$$\ell' = \frac{n(n+1)}{2}$$

MQ Signatures - Cyclic UOV

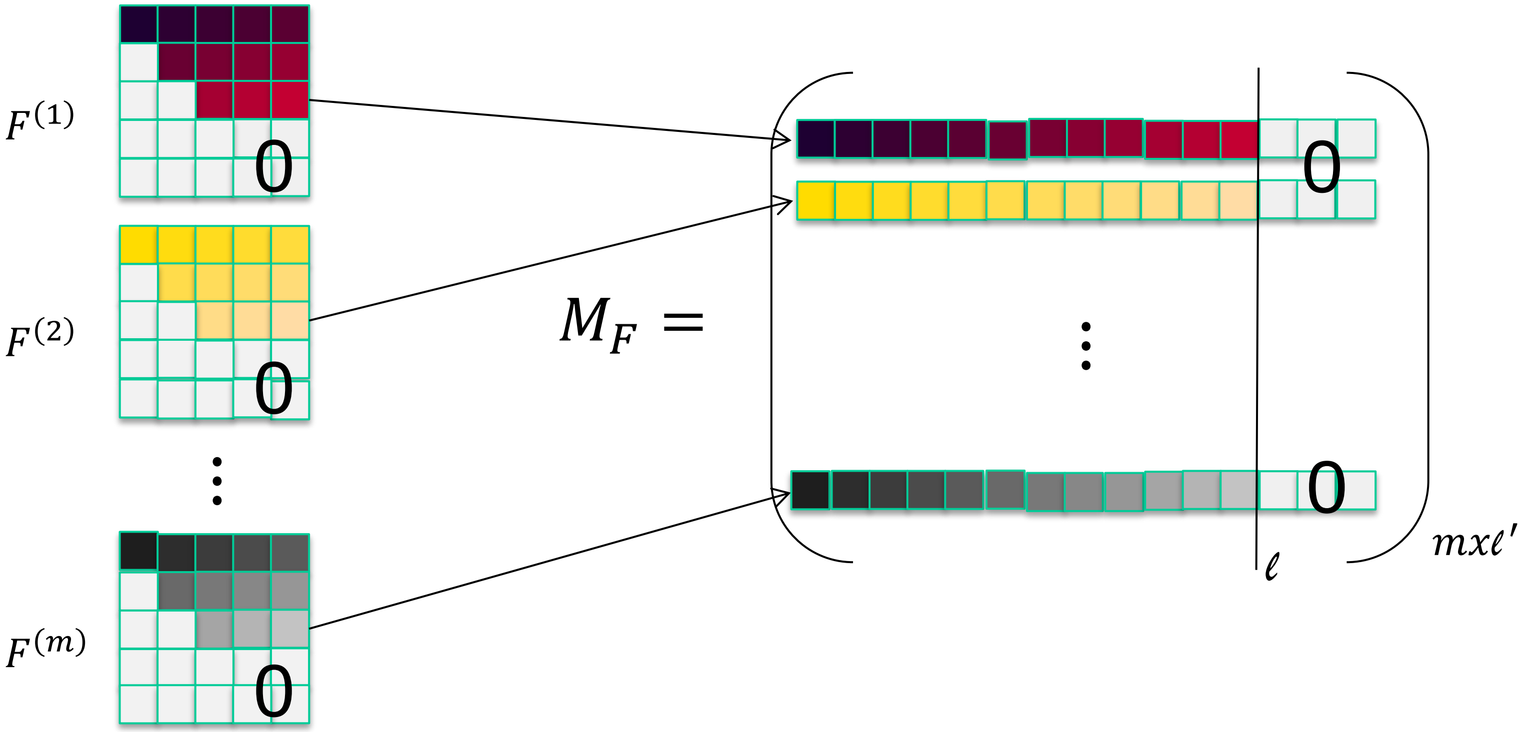
Public matrix of coefficients M_P



$$\ell = \frac{v(v+1)}{2} + mv, \qquad \ell' = \frac{n(n+1)}{2}$$

MQ Signatures - Cyclic UOV

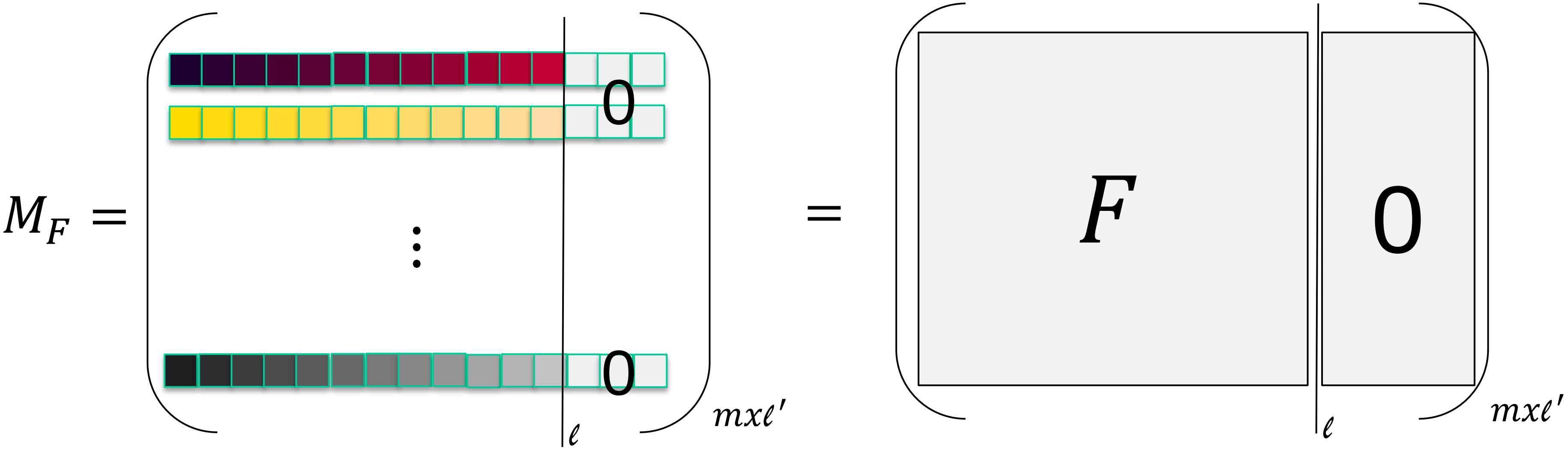
Private matrix of coefficients M_F



$$\ell = \frac{v(v+1)}{2} + mv, \qquad \ell' = \frac{n(n+1)}{2}$$

MQ Signatures - Cyclic UOV

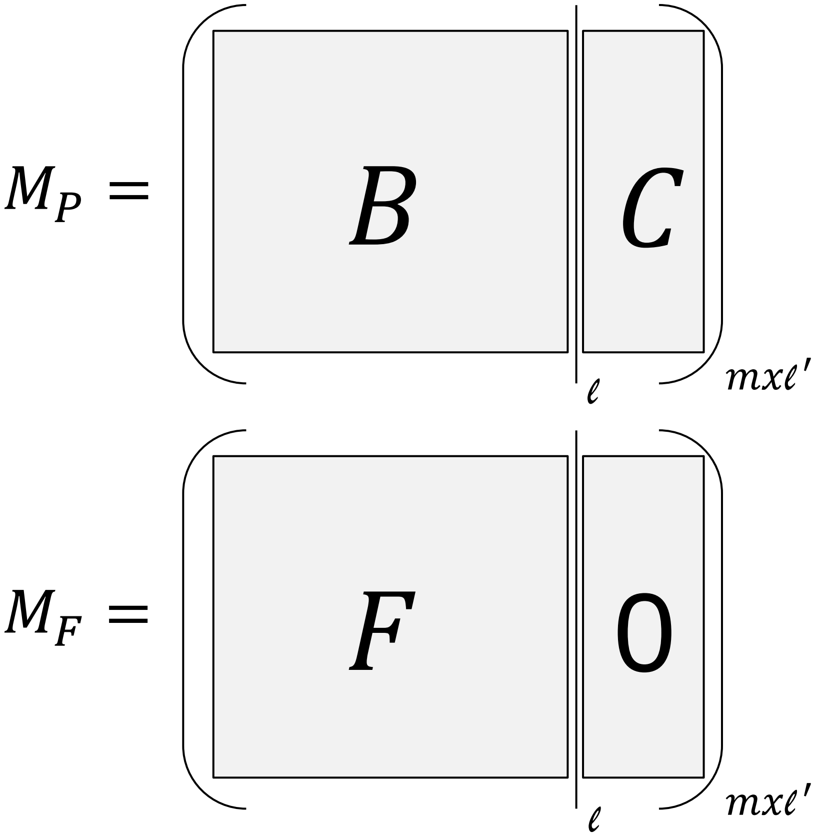
Private matrix of coefficients M_F



$$\ell = \frac{v(v+1)}{2} + mv, \qquad \ell' = \frac{n(n+1)}{2}$$

MQ Signatures - Cyclic UOV

- There is a linear relation between B and F which only depends on B,F and S [Petzoldt et. al, 2010]



$$B = F \cdot A_{UOV}(\mathrm{S})$$

$$a_{ij}^{rs} = \begin{cases} s_{ri}.s_{si}, & i = j \\ s_{ri}.s_{sj} + s_{rj}.s_{si}, & i \neq j \end{cases}$$

$$1 \leq i \leq v, i \leq j \leq n$$

$$1 \leq r \leq v, r \leq s \leq n$$

MQ Signatures - Cyclic UOV

By choosing $A_{UOV}(S)$ invertible:

- F can be computed from B and A_{UOV}^{-1}

  $F = B \cdot A_{UOV}^{-1}$

MQ Signatures - Cyclic UOV

By choosing $A_{UOV}(S)$ invertible:

- F can be computed from B and A_{UOV}^{-1}

  $F = B \cdot A_{UOV}^{-1}$

- Thus, the choice of B becomes flexible.

MQ Signatures - Cyclic UOV

By choosing $A_{UOV}(S)$ invertible:

- F can be computed from B and A_{UOV}^{-1}

  $F = B \cdot A_{UOV}^{-1}$

- Thus, the choice of B becomes flexible.
- In particular:
  $B = 0$ does not result in a valid F,
  B = Identity blocks, reveals too much info of A_{UOV}^{-1},
  B circulant was adopted by [Petzoldt et. al, 2010]

MQ Signatures - Cyclic UOV

By choosing $A_{UOV}(S)$ invertible:

- F can be computed from B and A_{UOV}^{-1}

  $F = B \cdot A_{UOV}^{-1}$

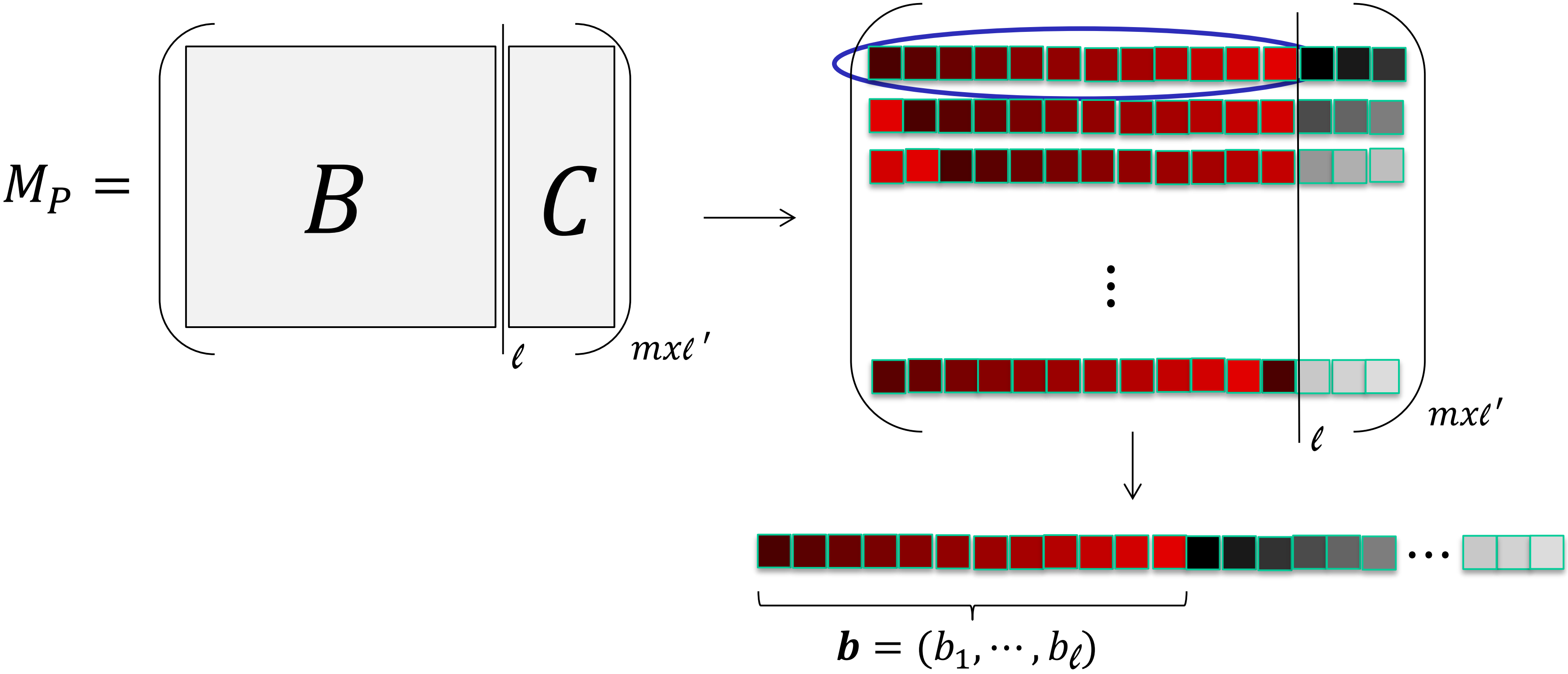
- Thus, the choice of B becomes flexible.
- In particular:

  $B = 0$ does not result in a valid F,
  B = Identity blocks, reveals too much info of A_{UOV}^{-1},
  B circulant was adopted by [Petzoldt et. al, 2010]

Petzoldt et. al. showed by theorem that the choice of a circulant B provides consistent UOV signatures.

MQ Signatures - Cyclic UOV

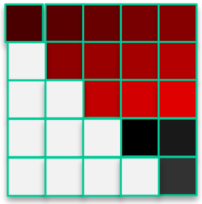
Adopting B circulant:



$$|\boldsymbol{M_P}| = \ell + m(\ell' - \ell)$$

MQ Signatures - Cyclic UOV

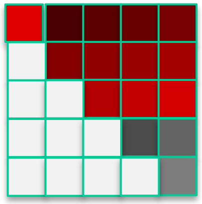
Public matrices $P^{(k)}$



$P^{(1)}$

MQ Signatures - Cyclic UOV

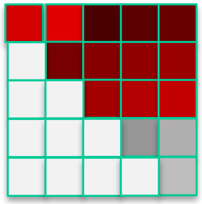
Public matrices $P^{(k)}$



$P^{(2)}$

MQ Signatures - Cyclic UOV

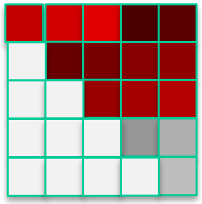
Public matrices $P^{(k)}$



$P^{(3)}$

MQ Signatures - Cyclic UOV

Public matrices $P^{(k)}$



$P^{(4)}$

MQ Signatures - Cyclic UOV

Public matrices $P^{(k)}$

$$\dots$$

Equivalent Keys in UOV

- Idea: Find equivalent private keys that enables solving any given public key system.

Equivalent Keys in UOV

- Idea: Find equivalent private keys that enables solving any given public key system.
- A class of equivalent private keys with a simpler structure.

Equivalent Keys in UOV

- Idea: Find equivalent private keys that enables solving any given public key system.
- A class of equivalent private keys with a simpler structure.
- Thus, private keys can be built using this short structure.

Equivalent Keys in UOV

- UOV public key:

$$P^{(i)} = SF^{(i)}S^T, 1 \leq i \leq m$$

Equivalent Keys in UOV

- UOV public key:

$$P^{(i)} = SF^{(i)}S^T, 1 \leq i \leq m$$

- Question: Are there classes of keys $S'$and F' s.t.

$$P^{(i)} = SF^{(i)}S^T = S'F'^{(i)}S'^T, 1 \leq i \leq m$$

where matrices $F'^{(i)}$ share with $F^{(i)}$ the same trapdoor structure?

Equivalent Keys in UOV

- Idea: Introduce a matrix Ω in $P^{(i)}$:

$$P^{(i)} = S\Omega^{-1}\Omega F^{(i)}\Omega^{T}{\Omega^{T}}^{-1}S^{T}$$

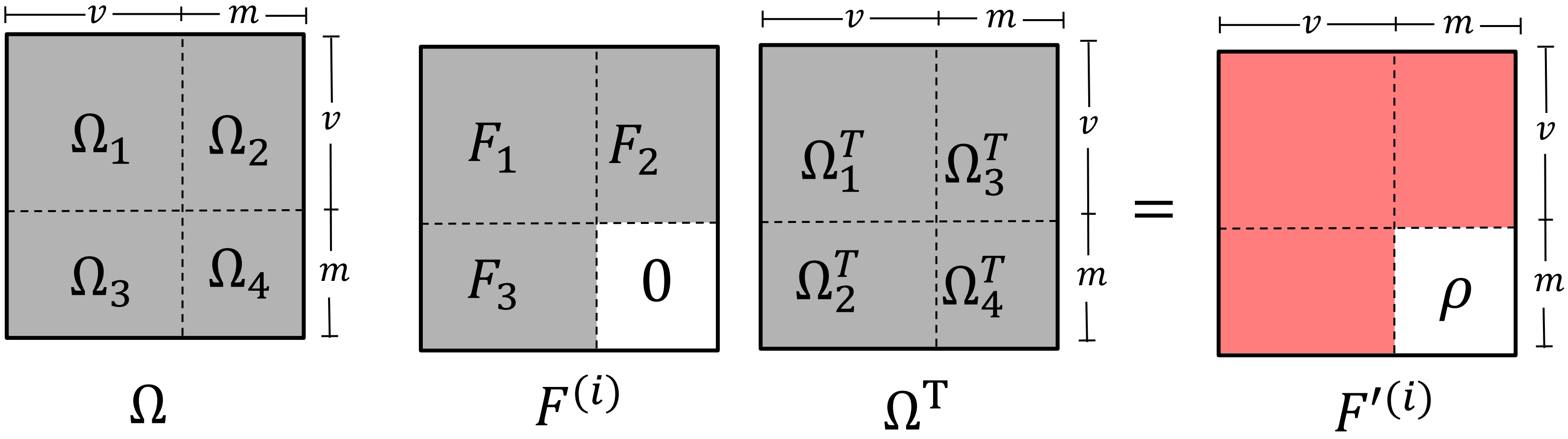
- Define $F'^{(i)} := \Omega F^{(i)}\Omega^{T}$

Equivalent Keys in UOV

- Idea: Introduce a matrix Ω in $P^{(i)}$:

$$P^{(i)} = S\Omega^{-1}\Omega F^{(i)}\Omega^T {\Omega^T}^{-1} S^T$$

- Define $F'^{(i)} := \Omega F^{(i)} \Omega^T$
- We want Ω that keeps the original F structure in F':

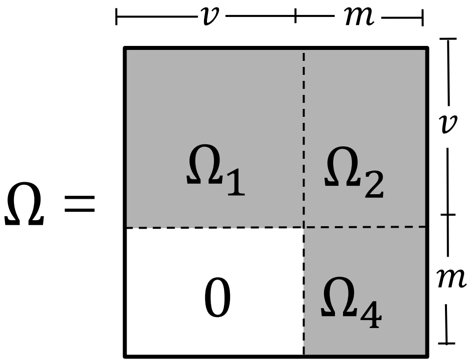


Equivalent Keys in UOV

- From the previous equality we obtain:

$$\rho = (\Omega_3 F_1 + \Omega_4 F_3)\Omega_3^T + \Omega_3 F_2 \Omega_4^T = 0$$

and $\Omega_3 = 0$ is a solution.



Equivalent Keys in UOV

- Thus, $F'^{(i)} = \Omega F^{(i)} \Omega^T$ has the same structure of $F^{(i)}$.
- Going back to definition

$$P^{(i)} = S\Omega^{-1}(\Omega F^{(i)} \Omega^T){\Omega^{T}}^{-1}S^T$$

Equivalent Keys in UOV

- Thus, $F'^{(i)} = \Omega F^{(i)} \Omega^T$ has the same structure of $F^{(i)}$.
- Going back to definition

$$P^{(i)} = S\Omega^{-1}(F'^{(i)})\Omega^{T^{-1}}S^T$$

Departamento de Engenharia de Computação e Sistemas Digitais

Equivalent Keys in UOV

- Thus, $F'^{(i)} = \Omega F^{(i)} \Omega^T$ has the same structure of $F^{(i)}$.

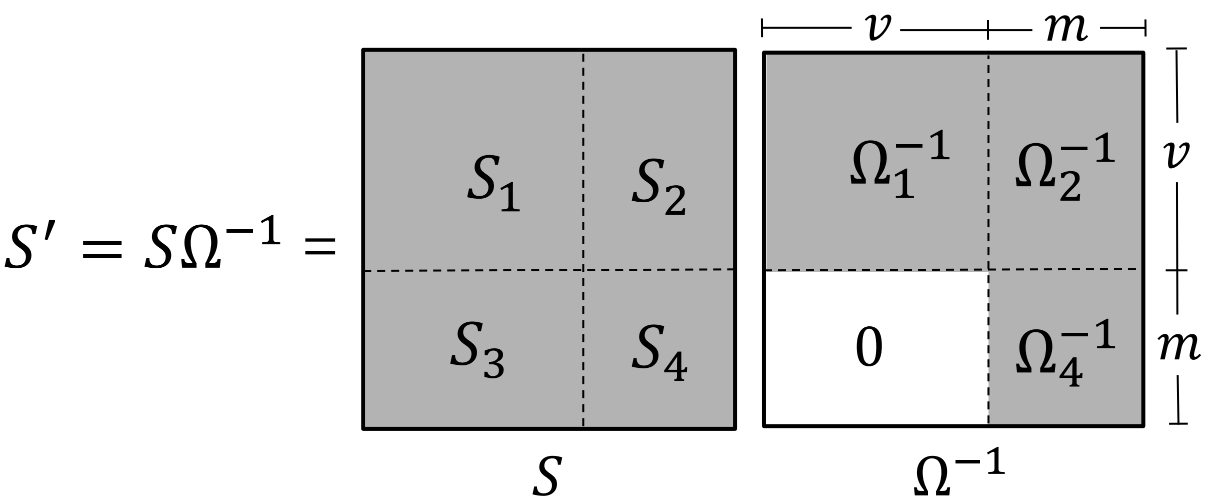
- Going back to definition

$$P^{(i)} = S\Omega^{-1}(F'^{(i)})\Omega^{T^{-1}}S^T$$

- So, defining $S' \coloneqq S\Omega^{-1}$ one finally gets:

$$P^{(i)} = S'F'^{(i)}S'^T$$

Equivalent Keys in UOV



- Note that Ω^{-1} has the same structure of Ω.

Equivalent Keys in UOV

- By choosing suitable values of Ω_i^{-1}, it is possible to get:

$$S_1' = I_{vxv}$$
$$S_2' = 0_{vxm}$$
$$S_4' = I_{mxm}$$

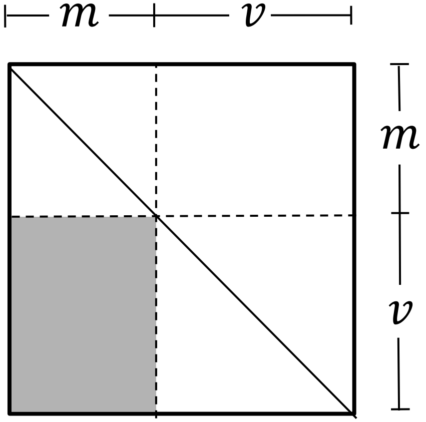
what implies

$$S_3' = S_3 S_1^{-1} S^2 S_1^{-1} + S_4 (S_4 - S_3 S_1^{-1} S_2)^{-1}$$

Equivalent Keys in UOV

- Structure of S':

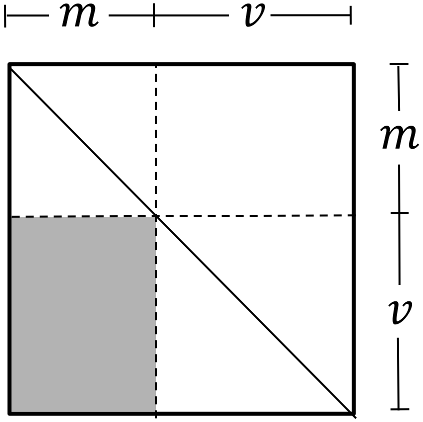
$S' =$



Equivalent Keys in UOV

- Structure of S':

$S' =$

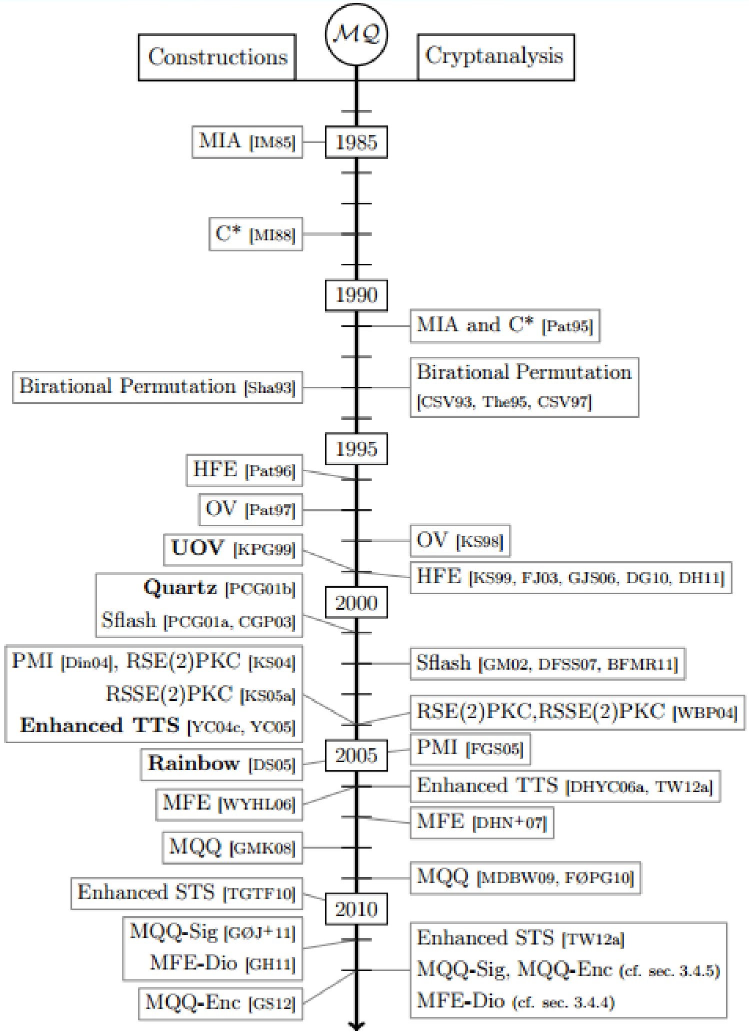


- So, the answer is **yes**, there exist equivalent $S', F'^{(i)}$ s.t.

$$S'F'^{(i)}(S')^T = (S\Omega^{-1})\left(\Omega F^{(i)}\Omega^T\right)(S\Omega^{-1})^T = P^{(i)}$$

and $F'^{(i)}$ have the desired trapdoor structure.

Recap. MQ Schemes



Departamento de Engenharia de Computação e Sistemas Digitais

Thanks!

Questions?