Post-quantum cryptography with polynomials

Ignacio Luengo
U. Complutense de Madrid

Lahore, August 2018

Outline

- Shor's algorithm and quantum computers
- Quantum safe Cryptography
- Public Key Cryptography (PKC)
- Multivariate PKC
- Algebraic cryptoanalisys of MPKC
- Algebraic Geometry
- DME
- NIST call proposals
- Open questions

References

- J. Ding, D. Schmidt, J. Gower. Multivariate Public Key Cryptography, Advances in Information Security series, Springer, 2006
- J. Ding, B. Yang. Multivariate public key cryptography (with Bo-yin Yang), Chapter in Post-Quantum Cryptography by D . Bernstein , J. Buchmann, E. Dahmen (Editors), Springer, 2009
- DME preprint :http://www.mat.ucm.es/ iluengo/DME
- NIST contest: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions

Post-quantum cryptography: public-key cryptography resistant to future quantum computers.

Shor's algorithm (1994): Factorization and discrete Logarithm in polynomial time on a quantum computer.

Backward security

Post-quantum cryptography: public-key cryptography resistant to future quantum computers.

Shor's algorithm (1994): Factorization and discrete Logarithm in polynomial time on a quantum computer.

Backward security: today's internet traffic in 15/20 years?

NSA (2015): Change to quantum safe cryptography.

NIST (2016) open call: proposals for standarization of quantum safe PKC.

November 2017 : end of the call, 83 proposal for KEM/Encryption and Signature.

Public Key Cryptography: It uses two keys PK (public key) for encription and SK (secret key) for decription.
The secret key SK can not be deduced from the public key PK.

Mathematical challenge: To find families of biyections $\{e_K\}$ with two ways of invert them. One difficult way **(public)** and one easy way **(secret)** .

Cryptosystem: A family of biyections $e_k : P \to C$, $d_k : e_k^{-1}$
x message, $y = e_k(x)$ cypher text, $d_k(e_k(x)) = x$

Public Key Cryptosystem: It uses two keys pk (public key) for encription and sk (secret key) for decription.
The secret key sk can not be deduced from the public key pk.

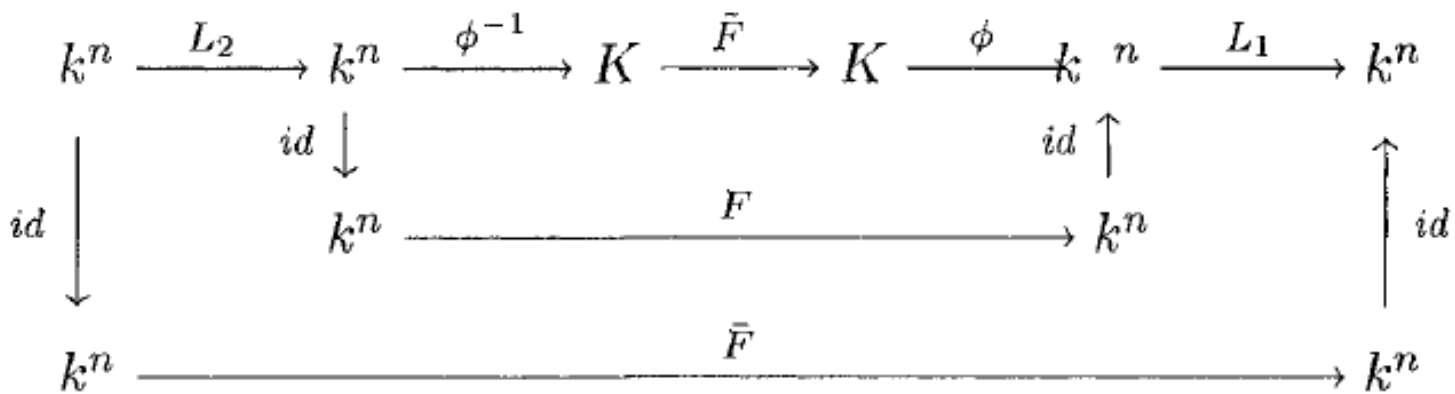
Mathematical challenge: To find families of biyections $\{e_{pk}\}$ with two ways of invert them. One difficult way **(public)** and one easy way **(secret)** .

Signature: Encript with the secret key SK. The map e_{KS} need not to be biyective, only need to be surjective.

- Lattices.
- Error correcting codes.
- Multivariate systems
- Mixed : Isogenies, hash, braid..

The public key is a (cuadratic) map $F : k^n \to k^m$, $k = \mathbb{F}_q$, $q = p^e$ and $K = k^n$ compossed with two generic linear maps $L1$ and $L2$.

The first MPKC was the Imai-Matsumoto (1988), $\tilde{F}(z) = z^{q^a+1}$
On $k = \mathbb{F}_q \setminus \{0\}$ we have $z^{q-1} = 1$,
if $d = (q^a + 1)^{-1} mod \quad q - 1$ then $\tilde{F}^{-1}(u) = z^d$
- Imai-Matsumoto system was broken by Patarin in 1995



- Patarin(1996) propossed the HDE(Hidden Field Equations) the central map is

$$\tilde{F}(z) = \sum_{q^i+q^j \leq D} a_{ij} z^{q^i+q^j}$$

- To invert F one has to solve the $F_i(x) = y_i$ by Grobner basis.

- Faugere (F4, F5), XL, MinRank.... broke HFE (2005...)

Modifications of HFE: oil and vinegar (ov), uov, plus(+), minus(-),....HFEv-

- Quadratic multivariate systems can only be used for signature.

Monomial maps

Let A be a matrix $A = (a_{ij}) \in \mathscr{M}_{n\times n}(\mathbb{Z})$ one can define a monomial map G_A associated to the matrix A as follows:
$G_A : K^n \to K^n : \quad G_A(x_1, \ldots, x_n) = (x_1^{a_{11}} \cdot \ldots \cdot x_n^{a_{1n}}, \ldots, x_1^{a_{n1}} \cdot \ldots \cdot x_n^{a_{nn}})$.
If $\det(A) = \pm 1$, the inverse matrix $A^{-1} \in \mathscr{M}_{n\times n}(\mathbb{Z})$, then G_A is invertible on $(K \setminus \{0\})^n$ and the inverse is given by $G_{A^{-1}}$

Now if we take $A \in M_{n\times n}(\mathbb{Z}_{q-1})$ then,

Exponential maps (called monomial in algebraic geometry)

A matrix

$$A = (a_{ij}) \in M_{n\times n}(\mathbb{Z}_{q-1})$$

defines an exponential map

$$G_A : {\mathbb{F}_q}^n \to {\mathbb{F}_q}^n$$

given by

$$G_A(x_1, \ldots, x_n) = (x_1, \ldots, x_n)^A = (x_1^{a_{11}} \cdot \ldots \cdot x_n^{a_{n1}}, \ldots, x_1^{a_{1n}} \cdot \ldots \cdot x_n^{a_{nn}})$$

Exponential maps (called monomial in algebraic geometry)

A matrix

$$A = (a_{ij}) \in M_{n\times n}(\mathbb{Z}_{q-1})$$

defines an exponential map

$$G_A : {\mathbb{F}_q}^n \to {\mathbb{F}_q}^n$$

given by

$$G_A(x_1, \ldots, x_n) = (x_1, \ldots, x_n)^A = (x_1^{a_{11}} \cdot \ldots \cdot x_n^{a_{n1}}, \ldots, x_1^{a_{1n}} \cdot \ldots \cdot x_n^{a_{nn}})$$

and satisfying

$$((x_1, \ldots, x_n)^A)^B = (x_1, \ldots, x_n)^{A\cdot B}$$

Exponential maps (called monomial in algebraic geometry)

A matrix

$$A = (a_{ij}) \in M_{n\times n}(\mathbb{Z}_{q-1})$$

defines an exponential map

$$G_A : {\mathbb{F}_q}^n \to {\mathbb{F}_q}^n$$

given by

$$G_A(x_1, \ldots, x_n) = (x_1, \ldots, x_n)^A = (x_1^{a_{11}} \cdot \ldots \cdot x_n^{a_{n1}}, \ldots, x_1^{a_{1n}} \cdot \ldots \cdot x_n^{a_{nn}})$$

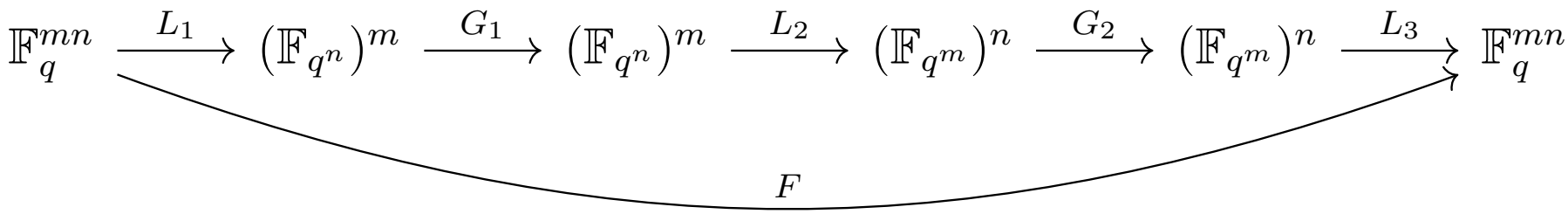
and satisfying

$$((x_1, \ldots, x_n)^A)^B = (x_1, \ldots, x_n)^{A\cdot B}$$

Theorem : If $\gcd(\det(A), q-1) = 1$, then G_A is invertible on $(\mathbb{F}_q \setminus \{0\})^n$ and the inverse of G_A is given by $G_{A^{-1}}$

DME stands for double matrix exponentiation

The public key is $K_P = F$, where $F : \mathbb{F}_q^{nm} \to \mathbb{F}_q^{nm}$ is a map obtained as composition of five maps, $F = L_3 \circ G_2 \circ L_2 \circ G_1 \circ L_1$, and $q = 2^e$.



The map F is designed to be injective on $(\mathbb{F}_q^n \setminus \{0\})^m$ and

$$\forall x \in (\mathbb{F}_q^n \setminus \{0\})^m,\ F(x) \in (\mathbb{F}_q^m \setminus \{0\})^n.$$

-The maps G_1 and G_2 are monomial maps given by **(public)** matrices with two non zero entries (powers of 2)

-The maps L_1, L_2 and L_3 are $\mathbb{F}_q$-linear **(secret)** isomorphisms

-In order to keep the final number of monomials small we take $(n = 2, m = 3, \ldots 6)$,

-The maps G_1 and G_2 are monomial maps given by **(public)** matrices with two non zero entries (powers of 2)

-The maps L_1, L_2 and L_3 are $\mathbb{F}_q$-linear **(secret)** isomorphisms

-In order to keep the final number of monomials small we take $(n = 2, m = 3, \ldots 6)$,

NIST proposal: $n = 2, m = 3, q = 2^{48}, (288 bits)$

Each component of F has 64 monomials and F^{-1} has at least 2^{100}.

-The maps G_1 and G_2 are monomial maps given by **(public)** matrices with two non zero entries (powers of 2)

-The maps L_1, L_2 and L_3 are $\mathbb{F}_q$-linear **(secret)** isomorphisms

-In order to keep the final number of monomials small we take $(n = 2, m = 3, \ldots 6)$,

NIST proposal: $n = 2, m = 3, q = 2^{48}, (288 bits)$

-Each component of F has 64 monomials and F^{-1} has at least 2^{100}.

$$x_1^{8388608} x_3^{131072} x_4^{8589934592} x_6^{1048576}$$

Implementated by

- Martín Avendaño (CUD, Zaragoza)
- Miguel Ángel Marco (Univ. Zaragoza)

	Encr.	*Decr.*	*SK*	*PK*	*CyphText*
Lattices	$0.22M$ 465.6	$0.17M$ 488.09	$32B$ 2565055	$826B$ 1357824	$253B$ 334640
Codes	$0.45M$ 112.24	$0.15M$ 681.89	$40B$ 41802	$564B$ 2563260	$226B$ 17778
Multivariable	$2.11M$	$1.08M$	$288B$	$2304B$	$36B$
Isogen(*SIKE*)	$55.82M$	$0.38M$	$1572B$	$8679B$	$8710B$

	Key Gen.	Encr.	Decr.	SK	PK	CT	bytes
DME	13.5 M	2.11 M	10.8 M	288 B	2304 B	36 B	33 B

	Key Gen.	Encr.	Decr.	SK	PK	CT	bytes
DME	13.5 M	2.11 M	10.8 M	288 B	2304 B	36 B	33 B

Total number of proposals remaining:

	Lattices	*Codes*	*Multivariable*	*Mixed*
KEM/Encrypt	21	16	1	1
Signature	4	2	7	4 (3*hash*, 1*braid*)

www.safecrypto.eu/pqclounge/

Pros:

- Very simple design

Pros:

- Very simple design
- Flexibility

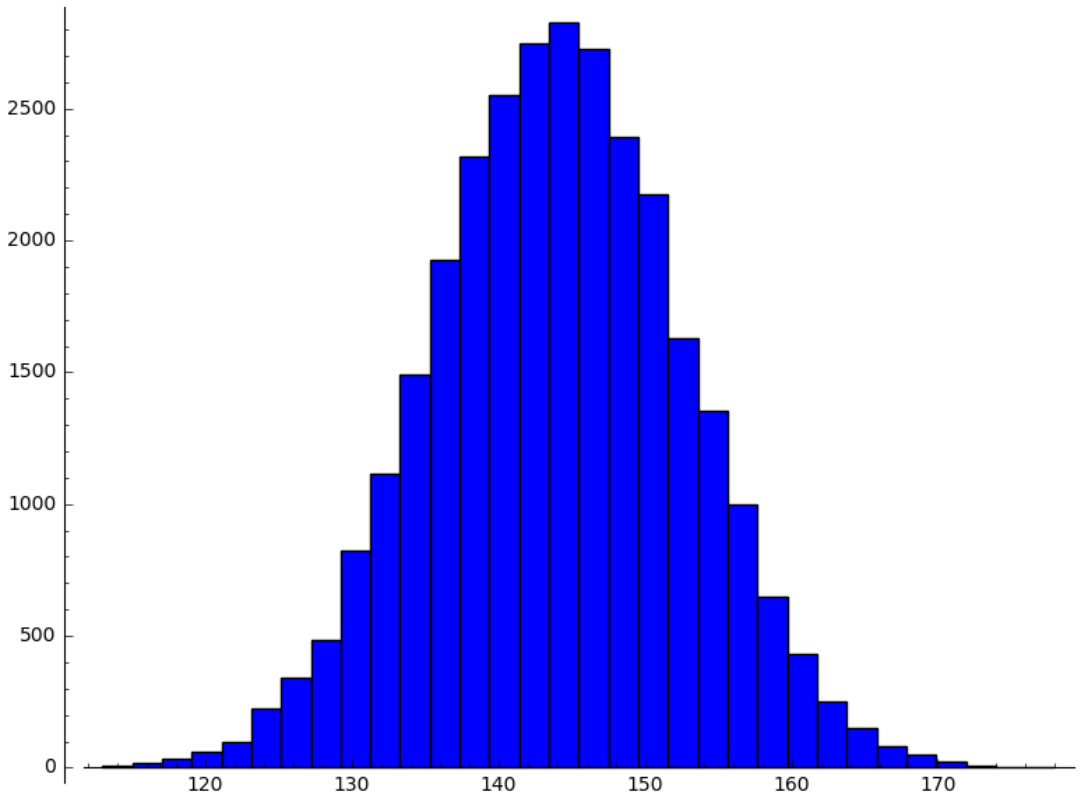
Pros:

- Very simple design
- Flexibility
- Constant time evaluation (timing side-channel attacks)

Pros:

- Very simple design
- Flexibility
- Constant time evaluation (timing side-channel attacks)
- Immune to Grobner basis attack over $\mathbb{F}_{2^{48}}$
- Randomness: similar behavior as a block cypher : PRNG,

Randomness



Cons:

- Very new system (2017)

Cons:

- Very new system (2017)
- Proof of security: reduction to a hard problem

Cons:

- Very new system (2017)
- Proof of security: reduction to a hard problem
- Estructural attacks to find the secret linear maps L_i

Cons:

- Very new system (2017)
- Proof of security: reduction to a hard problem
- Estructural attacks to find the secret linear maps L_i

Cryptoanalisys: Weil descent over $\mathbb{F}_2$

- Over $\mathbb{F}_2$, F can be written as a system $\tilde{F}$ of quartic polynomials in 288 variables.

Cons:

- Very new system (2017)
- Proof of security: reduction to a hard problem
- Estructural attacks to find the secret linear maps L_i

Cryptoanalisys: Weil descent over $\mathbb{F}_2$

- Over $\mathbb{F}_2$, F can be written as a system $\tilde{F}$ of quartic polynomials in 288 variables.
- Attack(Ward Buellens): use Fauguere-Perret decomposition algorithm (does not work for small fields)

Cons:

- Very new system (2017)
- Proof of security: reduction to a hard problem
- Estructural attacks to find the secret linear maps L_i

Cryptoanalisys: Weil descent over $\mathbb{F}_2$

- Over $\mathbb{F}_2$, F can be written as a system $\tilde{F}$ of quartic polynomials in 288 variables.
- Attack(Ward Buellens): use Fauguere-Perret decomposition algorithm (does not work for small fields)
- Degree of regularity of $\tilde{F}$

New proposed parameters for the second round:

- $n = 2$, $m = 4$, $N = 6$ variables, $q = 2^{48}$

New proposed parameters for the second round:

- $n = 2$, $m = 4$, $N = 6$ variables, $q = 2^{48}$
- $h(x_1, \ldots, x_6) = (x_1, x_2, x_3, x_4, x_5, x_6, x_2x_4x_6, 0)$
  $F : (\mathbb{F}_q)^6 \to (\mathbb{F}_q)^8$

New proposed parameters for the second round:

- $n = 2$, $m = 4$, $N = 6$ variables, $q = 2^{48}$
- $h(x_1, \ldots, x_6) = (x_1, x_2, x_3, x_4, x_5, x_6, x_2x_4x_6, 0)$
  $F : (\mathbb{F}_q)^6 \to (\mathbb{F}_q)^8$
- ct= 48 bytes, 32 monomials

New proposed parameters for the second round:

- $n = 2$, $m = 4$, $N = 6$ variables, $q = 2^{48}$
- $h(x_1, \ldots, x_6) = (x_1, x_2, x_3, x_4, x_5, x_6, x_2x_4x_6, 0)$
  $F : (\mathbb{F}_q)^6 \to (\mathbb{F}_q)^8$
- ct= 48 bytes, 32 monomials
- Typical monomials

$$x_1^{2^{\alpha_1}} x_2^{b_1} x_3^{2^{\alpha_3}} x_4^{b_4} x_5^{2^{\alpha_5}} x_6^{b_6}$$

New proposed parameters for the second round:

- $n = 2$, $m = 4$, $N = 6$ variables, $q = 2^{48}$
- $h(x_1, \ldots, x_6) = (x_1, x_2, x_3, x_4, x_5, x_6, x_2x_4x_6, 0)$
  $F : (\mathbb{F}_q)^6 \to (\mathbb{F}_q)^8$
- ct= 48 bytes, 32 monomials
- Typical monomials

$$x_1^{2^{\alpha_1}} x_2^{b_1} x_3^{2^{\alpha_3}} x_4^{b_4} x_5^{2^{\alpha_5}} x_6^{b_6}$$

- On $\mathbb{F}_2$ the PK, $\tilde{F}$ can have degree > 100 and more than 2^{256} monomials

Open questions

- Proof of security: reduction to a hard problem (NP-complete)
- Security against Grobner basis attacks
- Estimate the degree of regularity
- Algebraic cryptoanalisys over F_2
- Resistence to structural attacks
- Find the best exponent matrices

Thank you for your attention!

Thank you for your attention!

Questions?