On public key cryptosystem based on the problem of solving a non linear system of polynomial equations

NACER GHADBANE
Laboratory of Pure and Applied Mathematics , Department of Mathematics, University of M'sila, BP 166 Ichebilia, 28000, M'sila, ALGERIA.

Abstract: The basic idea behind multivariate cryptography is to choose a system of polynomials which can be easily inverted (central map). After that one chooses two affine invertible maps to hide the structure of the central map. Fellows and Koblitz outlined a conceptual key cryptosystem based on the hardness of POSSO.
Let F_{p^s} be a finite field of p^s elements, where p is a prime number, and $s \in N, s \geq 1$. In this paper, we used the act of $GL_n\left(F_{p^s}\right)$ on the set $F_{p^s}^n$ and the transformations group, to present the public key cryptosystems based on the problem of solving a non-linear system of polynomial equations.

Key-Words: Group,Finite field, Group action on a set, General linear group, Linear transformation, Public key cryptography.

Received: March 15, 2020. Revised: September 12, 2020. Re-revised: September 23, 2020. Accepted: October 3, 2020. Published: October 24, 2020

1 Intoduction

Cryptographic techniques are essential for the security of communication in modern society. The asymmetric encryption methods based on difficult problems in mathematics. Today, nearly all cryptographic schemes used in practice are based on the two problems of factoring large integers and solving discrete logarithms. However, schemes based on these problems will become insecure when large enough quantum computers are built. The reason for this is Shor's algorithm. which solves number theoretic problems such as integer factorization and discret logarithms in polynomial time on a quantum computer. Therefore one needs alternatives to those classical public key schemes. Besides lattice, code and hash based cryptosystems, multivariate cryptography seems to be a candidate for this.

In 1994, Fellows and Koblitz outlined a conceptual key cryptosystem based on the hardness of the problem of solving a non-linear system of polynomial equations.

The remainder of this paper is organized as follows. In Section 2, we begin with some elementary material concerning of group, finite field, group action on a set, general linear group, linear transformation, and public key cryptography. In Section 3, we prove that the general linear group $GL_n\left(F_{p^s}\right)$ acts on the set $F_{p^s}^n$. In Section 4, we used the computational hardness of the Polynomial System Solving (POSSO) to present the public-key cryptosystems, we draw our conclusions in Section 5.

2 Preliminaries

A group is a non-empty set G on which there is binary operation
$(a, b) \longmapsto ab$ such that
• if a and b belong to G then ab is also in G (closure).
• If a, b and c in G, then $(ab)\,c = a\,(bc)$ (associativity).
• there exists an element 1_G in G such that
$1_G a = a 1_G = a$ for all $a \in G$ (identity).
• if $a \in G$, then there is an element $a^{-1} \in G$ such that
$a^{-1}a = aa^{-1} = 1_G$ (inverse).

The order of a group G, denoted by $|G|$, is the cardinality of G, that is the number of elements in G. A subset H of a group G is a subgroup of G, if and only if $H = \emptyset$ and for all a, b in H, ab in H and a^{-1} in H. The subgroup H of a group G is denoted by $H \leq G$.

Given two groups G and H, a group homomorphism is a map $f : G \longrightarrow H$ such that $f\,(ab) = f\,(a)\,f\,(b)$ for all $a, b \in G$. Note that this definition immediately implies that the identity 1_G of G is mapped to the identity 1_H of H. The same is true for the inverse, that is $f\left(a^{-1}\right) = f\,(a)^{-1}$.

Recall that if $f : G \longrightarrow H$ is a group homomorphism, the kernel of f is defined by $Ker\,(f) = \{a \in G : f\,(a) = 1_H\}$, $[1], [2], [9]$.

The group G acts on the set X if for all $g \in G$, there is a map
$G \times X \longrightarrow X, (g, x) \longmapsto g.x$ such that
(i) $h.\,(g.x) = (hg)\,.x$ for all $g, h \in G$, for all $x \in X$.
(ii) $1.x = x$ for all $x \in X$.

The kernel of an action $G \times X \longrightarrow X, (g, x) \longmapsto g.x$ is given by

$Ker = \{g \in G, g.x = x forall x \in X\}$.

The orbit $O(x)$ of x under the action of G is defined by $O(x) = \{g.x, g \in G\}$. It is important to notice that orbits partition X. Clearly, one has that $X =_{x \in X} O(x)$. The stabilizer of an element $x \in X$ under the action of G is defined by $Stab(x) = \{g \in G, g.x = x\}$. One may check that this is a subgroup of G. Note that, The size of the orbit is the index of the stabiliser, that is $|O(x)| = |G : Stab(x)|$. If G is finite, then $|O(x)| = \frac{|G|}{|Stab(x)|}$.
In particular, the size of an orbit divides the order of the group.

Let the finite group G act on the finite set X, and denote by X^g the set of elements of X that are fixed by g, that is $X^g = \{x \in X, g.x = x\}$.
Then the number of orbits is $\frac{1}{|G|}{}_{g \in G} |X^g|$, [4].
A ring is a set R with two binary operations $+$ and $\times$ such that
(i) $(R, +)$ is a commutative group;
(ii) $\times$ is associative, and there existe an element 1_R such that
$a \times 1_R = a = a1_R \times a$ for all $a \in R$;
(iii) the distributive law holds: for all a, b, and c in R,

$$(a + b) \times c = a \times c + b \times c$$
$$a \times (b + c) = a \times b + a \times c.$$

A field is a set F with two composition laws $+$ and $\times$ such that
(i) $(F, +)$ is a commutative group;
(ii) $(F - \{0\}, \times)$ is a commutative group;
(iii) the distributive law holds.
A field E containing a field F is called an extension field of F.
Let $f(X) \in F[X]$ be a monic polynomial of degree m, and let (f) be the ideal generated by f. Consider the quotient ring $F[X] / (f(X))$, and write x for the image of X in $F[X] / (f(X))$, i.e, x is the coset $X + (f(X))$.
The map $F[X] \longrightarrow F[x], P(X) \longmapsto p(x)$ is a homomorphism sending $f(X)$ to 0. Therefore, $f(x) = 0$.
The division algorithm shows that each element g of $F[X] / (f(X))$ is represented by a unique polynomial r of degree $< m$. Hence each element of $F[x]$ can be expressed uniquely as a sum $a_0 + a_1 x + ... + a_{m-1} x^{m-1}, a_i \in F \quad (*)$.
To add two elements, expressed in the form $(*)$, simply add the corresponding coefficients. To multiply two elements expressed in the form $(*)$, multiply in the usual way, and use the relation $f(x) = 0$ to express the monomials of degree $\geq m$ in x in terms of lower degree monomials.
Recall that, if $f(X)$ is a monic irreductible polynomial of degree m in $F[X]$, then $F[x] = F[X] / (f(X))$ is a field of degree m over F.

Let F_{p^s} be a finite field of p^s elements, where p is a prime number, and $s \in N, s \geq 1$. We consider vectors of length n with entries in F_{p^s}. We denote this by $F_{p^s}^n$. This becomes an abelian group under vector addition: $(x_1, ..., x_n) + (y_1, ..., y_n) = (x_1 + y_1, ..., x_n + y_n)$, [7], [8].
Let $GL_n(F_{p^s})$ be the general linear group over the field F_{p^s}, is the group of invertible $n \times n$ matrices with cofficients in F_{p^s}. Note that, the columns of an invertible matrix give a basis of $F_{p^s}^n$. Conversely, if $u_1, u_2, ..., u_n$ is a basis of $F_{p^s}^n$ then there is an invertible matrix with these vectors as columns.
Let $A \in GL_n(F_{p^s})$. The linear transformation associated with A is the function $T_A : F_{p^s}^n \longrightarrow F_{p^s}^n$ defined by $T_A(U) = AU^t$ for all $U \in F_{p^s}^n$.
Recall that, if $T : F_{p^s}^n \longrightarrow F_{p^s}^n$ be a linear transformation, then the columns of the matrix corresponding to T are the vectors $T(e_1), ..., T(e_n)$, where $e_1, ..., e_n$ denote the standard basis vectors for $F_{p^s}^n$.
Let A and B be in $GL_n(F_{p^s})$, and let T_A and T_B be the corresponding linear transformations. Then,
(i) The composition $T_A \circ T_B$ is a linear transformation, corresponding to the matrix AB.
(ii) T_A is bijective, and $(T_A)^{-1}$ is the linear transformation corresponding to the matrix A^{-1}.
A transformations group is a group whose elements are linear transformations, and whose operation is composition.
Let G be a transformation group, and let H be the corresponding set of $n \times n$ matrices. Then H is a subgroup of $GL_n(F_{p^s})$, and G and H are isomorphic.
Public-key cryptography, also called asymmetric cryptography, was invented by Diffie And Hellman more than forty years ago. In public-key cryptography, a user U has a pair of related keys (pK, sK): the key pK is public and should be available to everyone, while the key sK must be kept secret by U. The fact that sK is kept secret by a single entity creates an asymmetry, hence the name asymmetric cryptography, [6], [10], [13].

3 Results

In the following proposition we prove that the general linear group $GL_n(F_{p^s})$ acts on the set $F_{p^s}^n$. Also we show some results about this notion.

Let F_{p^s} be a finite field of p^s elements, where p is a prime number, and $s \in N, s \geq 1$. Let $GL_n(F_{p^s})$ be the group of $n \times n$ invertible matrices entries in the field F_{p^s}. Consider $\{e_1, ..., e_n\}$ the standard basis vectors for $F_{p^s}^n$, where $n \in N, n \geq 1$. Then,
• $GL_n(F_{p^s})$ acts on the set $F_{p^s}^n$ by
$GL_n(F_{p^s}) \times F_{p^s}^n \longrightarrow F_{p^s}^n, (A, u) \longmapsto A.u = Au^t$.
• for all $1 \leq i \leq n$, $|O(e_i)| = p^{sn} - 1$.

• for all $u \in F_{p^s}^n - \left\{0_{F_{p^s}^n}\right\}, |O(e_i)| = p^{sn} - 1$ and $O\left(0_{F_{p^s}^n}\right) = \left\{0_{F_{p^s}^n}\right\}$.
• for all $1 \leq i \leq n$, $|Stab(e_i)| = |GL_{n-1}(F_{p^s})| p^{s(n-1)}$.
• $|GL_n(F_{p^s})| = p_{i=1}^{sn^2 n}\left(1 - \frac{1}{p^{is}}\right)$.

• Let us check the action is actually well defined. First, we have that $A.(B.u) = A.(Bu^t) = A(Bu^t) = (AB)u^t$.
As for the identity, we get $I_n.u = I_n u^t = u$.
• Let $a_i = (a_{1i}, ..., a_{ni}) \in F_{p^s}^n$ be a nonzero vector. Then we can extend this vector to a basis of $F_{p^s}^n$, that is, there is $a_1, ..., a_{i-1}, a_{i+1}, ..., a_n \in F_{p^s}^n$ such that $a_1, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n$ is a basis of $F_{p^s}^n$. Since they are a basis the matrix $A = \begin{pmatrix} a_{11} & . & . & . & a_{1i} & . & . & . & a_{1n} \\ . & & & & . & & & & . \\ . & & & & . & & & & . \\ . & & & & . & & & & . \\ a_{n1} & & & & a_{ni} & & & & a_{nn} \end{pmatrix}$ is invertible, that is, $A \in GL_n(F_{p^s})$. We have $Ae_i^t = \begin{pmatrix} a_{11} & . & . & . & a_{1i} & . & . & . & a_{1n} \\ . & & & & . & & & & . \\ . & & & & . & & & & . \\ . & & & & . & & & & . \\ a_{n1} & & & & a_{ni} & & & & a_{nn} \end{pmatrix} \begin{pmatrix} 0 \\ . \\ 1 \\ 0 \\ 0 \end{pmatrix} = a_i$.
Thus $a_i \in O(e_i)$. It is clear that $0_{F_{p^s}^n} \notin O(e_i)$.
Then $|O(e_i)| = \left|F_{p^s}^n\right| - 1 = p^{sn} - 1$.
• Note that $A \in Stab(e_i)$ if and only if $Ae_i^t = e_i$. Thus A is of the form $\begin{pmatrix} A_1 & 0 & A_2 \\ A_3 & 1 & A_4 \\ A_5 & 0 & A_6 \end{pmatrix}$ where $\begin{pmatrix} A_1 & A_2 \\ A_5 & A_6 \end{pmatrix}$ is an $(n-1) \times (n-1)$ matrix, $\begin{pmatrix} A_3 & 1 & A_4 \end{pmatrix}$ is a $1 \times n$ matrix. Since A is invertible, the matrix $\begin{pmatrix} A_1 & A_2 \\ A_5 & A_6 \end{pmatrix}$ must be invertible as well, hence $\begin{pmatrix} A_1 & A_2 \\ A_5 & A_6 \end{pmatrix} \in GL_{n-1}(F_{p^s})$. The matrix $\begin{pmatrix} A_3 & 1 & A_4 \end{pmatrix}$ can be anything. Thus there are $|GL_{n-1}(F_{p^s})|$ choices for $\begin{pmatrix} A_1 & A_2 \\ A_5 & A_6 \end{pmatrix}$ and $p^{s(n-1)}$ choices for $\begin{pmatrix} A_3 & 1 & A_4 \end{pmatrix}$. In total, there are $|GL_{n-1}(F_{p^s})| p^{s(n-1)}$ possible choices for $A \in Stab(e_i)$.
• We prove that $|GL_n(F_{p^s})| = p_{i=1}^{sn^2 n}\left(1 - \frac{1}{p^{is}}\right)$, by induction on n.
When $n = 1$, we have $|GL_1(F_{p^s})| = |F_{p^s} - \{0_{F_{p^s}}\}| = p^s - 1$
$= p_{i=1}^{s\,1}\left(1 - \frac{1}{p^{is}}\right) = p^s\left(1 - \frac{1}{p^s}\right)$.
Now we assume that the formula is true for $n-1$. By the orbit-stabilizer theorem, we have $|GL_n(F_{p^s}) : Stab(e_i)| = |O(e_i)|$. Since $GL_n(F_{p^s})$ is finite, we have
$|GL_n(F_{p^s})| = |O(e_i)| |Stab(e_i)| = (p^{sn} - 1) |GL_{n-1}(F_{p^s})| p^{s(n-1)}$
$= (p^{sn} - 1) p_{i=1}^{s(n-1)^2 n-1}\left(1 - \frac{1}{p^{is}}\right) p^{s(n-1)} = p_{i=1}^{s(n^2-2n+1+n-1+n)n}\left(1 - \frac{1}{p^{is}}\right)$
$= p_{i=1}^{sn^2 n}\left(1 - \frac{1}{p^{is}}\right)$.

Let F_p be the finite field of p elements, where p is a prime number. Let $GL_n(F_p)$ be the group of $n \times n$ invertible matrices with entries in the field F_p. Let $e_1 \in F_p^n$ be the vector $(1, 0, ..., 0)$. Then
• $O(e_1) = F_p^n - \left\{0_{F_p^n}\right\}$, hence $|O(e_1)| = p^n - 1$.
• $|Stab(e_1)| = |GL_{n-1}(F_p)| p^{n-1}$.
• $|GL_n(F_p)| = p_{i=1}^{n^2 n}\left(1 - \frac{1}{p^i}\right)$.

4 Application on the hardness of POSSO in public key cryptography

Multivariate cryptography is usually defined as the set of cryptographic schemes using the computational hardness of the Polynomial System Solving (POSSO). The POSSO problem over the field F_{p^s} is then following:
given a system $S = (f_1, ..., f_m$ of m nonlinear polynomial equations in the variables $x_1, ..., x_n$, find values $z_1, ..., z_n$ such that
$f_1(z_1, ..., z_n) = ...f_1(z_1, ..., z_n) = 0$. It is undecidable in general, [15] , [16]

The POSSO protocol :

The basic idea behind multivariate cryptography is to choose a system S of m polynomials in n variables which can be easily inverted (central map). After that one chooses two affine invertible maps ϕ and ψ to hide the structure of the central map. The public key of the cryptosystem is the composed map $P = \phi \circ S \circ \psi$ which is difficult to invert. The private key consistes of S, ϕ, and ψ and therefore allows to invert P, [11] , [12] , [14].

Secret Key (sk) : we choose a particular system of algebraic equations
$S = (f_1, ..., f_m) \in (F_{p^s}[x_1, ..., x_n])^m$, which the POSSO problem is easy to solve. That is, for all $(\mu_1, ..., \mu_m) \in (F_{p^s})^m$, we can solve in polynomial-time: $\begin{cases} f_1 - \mu_1 = 0 \\ . \\ . \\ . \\ f_m - \mu_m = 0 \end{cases}$

And we choose $(M,U) \in GL_n(F_{p^s}) \times F_{p^s}^n$, and $(N,V) \in GL_m(F_{p^s}) \times F_{p^s}^m$.
$(S,(M,U),(N,V))$ constitute a secret key.
Public Key(pk): we construct the public-key as:
for all $(x_1,...,x_n) \in F_{p^s}^n$, $P(x_1,...,x_n)$
$= N\left(f_1\left(M(x_1,...,x_n)^t + U\right),...,\right.$
$\left. f_m\left(M(x_1,...,x_n)^t + U\right)^t + V\right.$
$= (p_1(x_1,...,x_n),...,p_m(x_1,...,x_n))$, which the POSSO problem is undecidable to solve. $\left(F_{p^s}, F_{p^s}^n, P\right)$ constitut a public key.
Encreption: to encrypt a message $M = (m_1,...,m_n) \in F_{p^s}^n$, we evaluate its components on the public-key, i.e. $C = P(m_1,...,m_n)$
$= (p_1(m_1,...,m_n),...,p_m(m_1,...,m_n)) = (c_1,...,c_m)$.
$(c_1,...,c_m)$
$= N\left(f_1\left(M(m_1,...,m_n)^t + U\right),...,\right.$
$\left. f_m\left(M(m_1,...,m_n)^t + U\right)^t + V\right.$.
Decryption: we can decrypt by to solve, $(c_1,...,c_m) =$
$N\left(f_1\left(M(m_1,...,m_n)^t + U\right),...,\right.$
$\left. f_m\left(M(m_1,...,m_n)^t + U\right)^t + V\right.$

Security of POSSO protocol

The security of multivariate cryptography is based on two mathematical problems:
1. Solve the system $f_1 = ... = f_m = 0$, where each f_i is a polynomial in the n variables $x_1,...,x_n$ with cofficients and variables in $F_{p^s}^n$.
2. Given a class of central maps C and a map P expressible as $P = \phi \circ S \circ \psi$, where ϕ and ψ are affine maps and $S \in C$, find a decomposition of P of the form $P = \phi' \circ S' \circ \psi'$, with affine maps ϕ' and ψ' and $S' \in C$, [17].

An attack against the public-key cryptosystem based on the problem of solving a non-linear system of polynomial equations does not allow to find exactly the Secret-Key. We will get rather a key that is equivalent to it in the following direction:

We say that $(S',(M',U'),(N',V'))$ is an equivalent key to the Secret-key $(S,(M,U),(N,V))$ if any message encrypted with the Public-Key $\left(F_{p^s}, F_{p^s}^n, P\right)$ can be decrypted with $(S',(M',U'),(N',V'))$. This is the case for example if $(S',(M',U'),(N',V'))$ checks the following condition:
$N'\left(f'_1\left(M'(m_1,...,m_n)^t + U'\right),...,\right.$
$\left. f'_m\left(M'(m_1,...,m_n)^t + U'\right)^t + V'\right.$
$= N\left(f_1\left(M(m_1,...,m_n)^t + U\right),...,\right.$
$\left. f_m\left(M(m_1,...,m_n)^t + U\right)^t + V\right.$
for all $(m_1,...,m_n) \in F_{p^s}^n$.

5 Conclusion

In this work, we present the public-key cryptosystem based on the problem of solving a non-linear system of polynomial equations.

References:

[1] M. R. Adhikari, A. Adhikari, "Basic Modern Algebra With Applications, Springer (2014).

[2] B. Baumslag and B. Chandler. "Theory and Problems of Group Theory", New York University, (1968).

[3] L. Bettale, "Cryptanalyse algébrique: outils et applications", thèse de doctorat, Université de Paris 6, (2011).

[4] O. Bogopolski, "Introduction to Group Theory", European Mathematical Society, (2008).

[5] L. Changming, Z. Lei and S. Yanjun, "The Design of Public Key Cryptography fo Key Exchange Base on Multivariate Equations, Applied Mechanics and Materials, Vol. 513-517, No.6, pp. 552-554, (2014).

[6] W. Diffie, M. E. Hellman, "New Direction in Cryptography," IEEE Trans, on Inform Theory, 22(6), P. 644-665, (1976).

[7] D. Guin et T. Hausberger, "Algèbre Tome 1 Groupes, Corps et Théorie de Galois", EDP Sciences, (2008).

[8] W. Ledermann, "Introduction to Group Theory", Longman Group Limited, London, (1973).

[9] J. M. Howie, "Fundamentals of Semigroup Theory", Oxford Science Publications, (1995).

[10] C. Paar and J. Pelzl, "Understanding Cryptography", Springer, (2009).

[11] Z. Peng and S. Tang, "Circulant UOV: a new UOV variant with shorter private key and faster signature generation", KSII Transactions on Internet and Information Systems , Vol. 12, No.3, pp. 1376-1395, (2018).

[12] A. Petzoldt, "Selecting and Reducing Key Sizes for Multivariate Cryptography, Technischen Universitàt Darmastadt, (2013).

[13] H. Phan, P. Guillot," Preuves de sécurité des schémas cryptographiques," université Paris 8, (2013).

[14] J. Porras, J. Baena and J. Ding, "ZHFE, a New Multivariate Public Key Encryption Scheme", 6th international workshop, PQCrypto, Waterloo, Canada, Proceedings, pp.229-245, (2014).

[15] H. Rosen, "Cryptography Theory and Practice," Third Edition, Chapman and Hall/CRC, (2006).

[16] X. Wang and B. Yang, "An improved signature model of multivariate polynomial public key cryptosystem against key recovery attack", Mathematical Biosciences and Engineering, Vol. 16, No.6, pp. 7734-7750, (2019).

[17] T. Yasuda, X. Dahan, Y. Huang, T. Takagi and K. Sakurai, "A Multivariate Quadratic challenge toward post-quantum generation", ACM Communications in Computer Algebra, Vol. 49, No. 3, pp. 105-107, (2015).