PATENTE

I. LUENGO[1]

The $\mathbb{F}_q$-linear isomorphism $L_3 = \ell \circ \tilde{L}_3 \circ \pi_2^{-1}$ is defined as

$$(\mathbb{F}_{q^n})^m \xrightarrow[\sim]{\pi_2^{-1}} (\mathbb{F}_q^n)^m \xrightarrow[\tilde{L}_3]{} (\mathbb{F}_q^n)^m \xrightarrow[\ell^{-1}]{} \mathbb{F}_q^{nm}, \qquad L_3 : (\mathbb{F}_{q^n})^m \to (\mathbb{F}_q^n)^m$$

The morphism $\tilde{L}_3$ is defined as $\tilde{L}_3 = (L_{31}, \ldots, L_{3n})$ where $L_{3j}(x'_j) = x'_j A_{3j}$, $A_{3j} \in \mathscr{M}_{n\times n}(\mathbb{F}_q)$ and $\det(A_{3j}) \neq 0$.

The main part of the design of the system are the two exponential maps G_1 and G_2 build with monomial maps as follows:

$$G_1(x_1, \ldots, x_m) = (x_1^{a_{11}} \cdot \ldots \cdot x_m^{a_{1m}}, \ldots, x_1^{a_{m1}} \cdot \ldots \cdot x_m^{a_{mm}}), \qquad G_1 : (\mathbb{F}_{q^n})^m \to \mathbb{F}_{q^n})^m$$

where $A_1 = (a_{ij}) \in \mathscr{M}_{m\times m}(\mathbb{Z}_{q^n-1})$ such that $d'_1 = \det(A_1)$ is prime with $q^n - 1$;

$$G_2(x'_1, \ldots, x'_n) = ({x'_1}^{b_{11}} \cdot \ldots \cdot {x'_n}^{b_{1n}}, \ldots, {x'_1}^{b_{n1}} \cdot \ldots \cdot {x'_n}^{b_{nn}}), \qquad G_1 : (\mathbb{F}_{q^m})^n \to \mathbb{F}_{q^m})^n$$

where $B_2 = (b_{ij}) \in \mathscr{M}_{n\times n}(\mathbb{Z}_{q^m-1})$ such that $d'_2 = \det(B_2)$ is prime with $q^m - 1$

If $\underline{x} = (x_{11}, \ldots, x_{nm}) \in {\mathbb{F}_q}^{nm}$ are the inicial coordinates, then the composition of the five maps L_1, G_1, L_2, G_2 and G_3 allow us to compute the components of $F(\underline{x})$ as polynomials $F_i \in \mathbb{F}_q[x_{11}, \ldots, x_{nm}]$. In order to keep small the number of monomials, we choose the matrices A_1 and B_2 with the following properties:

(1) The entries of A_1 and B_2 are of the form p^a.
(2) We fix two integers s and t such that the rows of A_1 have at most s non zero entries and the rows of B_2 have at most t non zero entries. One can compute the monomials in the F_i with the algorithm described below, resulting that the total number of monomials is $MON = (b \cdot n^s)^t$ where b depends on the mixing map M.
(3) The inverse maps G_1^{-1} and G_2^{-1} can be computed in the same way from the inverse matrix of A_1 and B_2 respectively and F_1^{-1} is also polynomial.

If the number of monomials in F^{-1} is not very big, one can get the coefficient of the polynomial by computing enough number of pairs $(x, F(x))$. To avoid this attack we tak A_1 such that $d_1 = \frac{1}{\det(A_1)} \mod q^n - 1$ has a expansion in base p with $d_1 = [K_0, \ldots, K_\ell]$ with at least s_1 non vanishing K_i and the same with B_2 and $d_2 = \frac{1}{\det(B_2)}$ (with at least t_1 non vanishing digits). The details of values of t_1, s_1 will be given when discussing the security of the system.

The public key of the system is $K_P = (h, \pi_0, F)$ and the private key is given by h, π_0 and the five maps $L_1, \ldots, L_3$ and their inverses that can be used to encrypt and decrypt. Given an encrypted message $z = F(\underline{x}) = DM(\overline{x})$, one compute $\underline{x} = F^{-1}(z)$ and discard the randow entries with the use of h.

It is possible to get the monomials of the F_i without computing the composition of the five maps as follows: we start with m lists that contain the coordinates of the $\underline{x}_i$, $M_{01} = [x_{11}, \ldots, x_{1n}]$, $\ldots$, $M_{mn} = [x_{m1}, \ldots, x_{mn}]$, and we define the operations on lists: multiplication and exponentiation. If $S = [s_1, \ldots, s_m]$, $T = [t_1, \ldots, t_m]$ then $S \cdot T = [s_i \cdot t_i]$ and $S^a = [s_i^a]$.

With these notations, one can see that the exponential G_1 produce, on each component, polynomials whose list of monomials is $N_{0k} = M_{01}^{a_{k1}} \cdot \ldots \cdot M_{0n}^{a_{kn}}$.

The mixing map M determines that in the list of monomials of each x'_k appears the list N_{0k}, joint with the list N_{0j} of the vectors that are placed at the $m-n$ last entreis of x'_k. If b_k is the number of vectors adjoined to x'_k then, if we denote by P_{0k} $(k = 1, \ldots, n)$ such list, then the final list of monomials of each component after G_2 to each monomial ${x'_1}^{b_{k1}} \cdot \ldots \cdot {x'_n}^{b_{kn}}$ gives $Q_{0k} = P_{01}^{b_{k1}} \cdot \ldots \cdot P_{0n}^{b_{kn}}$.

Notice that when we apply the final $\mathbb{F}_q$-linear bijection $\tilde{L}_3$, each component still have the same monomial, than means that there are n groups of m polynomials $F_{k1}, \ldots, F_{km}$ such that they have the same monomials, namely the list Q_{0k}.

It is clear that the number of monomials of Q_{0k} is at most $((1 + b_k) \cdot n^s)^t$. So if we denote by $b_{\max} = \max_k(1 + b_k)$, we get on each component at most $(b_{\max} \cdot n^s)^t$ monomials.

Departamento de Álgebra, Universidad Complutense, Plaza de las Ciencias s/n, Ciudad Universitaria, 28040 Madrid, SPAIN

E-mail address: iluengo@ucm.es