The $\mathbb{F}_q$-linear isomorfism $L_3 = \ell \circ \tilde{L}_3 \circ \Pi_2^{-1}$

$$\begin{tikzcd}
(\mathbb{F}_{q^n})^m \arrow[r, "\Pi_2^{-1}"] \arrow[rr, bend right, "L_3"'] & (\mathbb{F}_q^{\,n})^m \arrow[r, "\tilde{L}_3"'] & (\mathbb{F}_q)^{nm} \arrow[r, "\ell^{-1}"'] & \mathbb{F}_q^{\,nm}
\end{tikzcd}$$

$\tilde{L}_3$ is defined as $\tilde{L}_3 = (L_{31}, -, L_{3n})$ with

$L_{3j}(x'_j) = x'_j A_{3j}$, $A_{3j} \in \mathcal{M}_{n\times n}(\mathbb{F}_q)$ and $\det(A_{3j}) \neq 0$.

The main part of the design of the system are the two ~~maps G~~ exponential maps G_1 and G_2 build with monomial maps as folows

$$G_1(x_1 \,--\, x_n) = (x_1^{a_{11}} \cdots x_n^{a_{1n}}, \,—\,, x_1^{a_{n1}} \;\; x_n^{a_{mn}}).$$

$$G_1 : (\mathbb{F}_{q^n})^m \longrightarrow (\mathbb{F}_{q^n})^*,$$

with $A_1 \in \mathcal{M}_{m\times m}(\mathbb{Z}_{q^m-1})$ such that $d_1 = \det(A_1)$ is prime with q^m-1.

$$G_2(x'_1 \,\cdots\, x'_m) = (x_1'^{\,b_{11}} \cdots x_m'^{\,b_{1m}}, \ldots, x_1'^{\,b_{m1}} \;\; x_m'^{\,b_{mm}}$$

$G_2 : (\mathbb{F}_{q^m})^n \longrightarrow (\mathbb{F}_{q^m})^n$, $B_2 = (b_{ij}) \in \mathcal{M}_{n\times n}(\mathbb{Z}_{q^m-1})$

and $d_2 = \det(B_2)$ is prime with q^m-1.

If $\underline{x}=(x_{11} -- x_{nm})\in \mathbb{F}_q^{nm}$ are the inicial coordinates then the compositión of the five maps L_1, G_1, L_2, G_2 an G_3 alow us to compute the components of $F(\underline{x})$ as polinomials $F_i \in \mathbb{F}_q[x_{11} -- x_{nm}]$. In order to keep small The ~~number~~ number of monomials we choose the matri as 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 ~~and~~ 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 fim the same way from the inverse matrix of A_1 and B_2 respectively. ~~As we~~ and F_1^{-1} is also a polynomial.

~~In order to avoid that The~~

If the number of monomial of F^{-1} is not very big one can ~~compute~~ get the coeficient of the polinomial by computing enough number of pairs, $(X, F(X))$. To avoid this attack. ~~We~~ take A_1 ~~and~~ such $d_1 = \frac{1}{\det(A_1)} \mod q^n - 1$ has ~~an p-adic exp~~ expansion in base p with $d_1 = [k_0 \cdots k_i]$ with ~~many~~ at least s_1 non vanishing k_i. and the same with B_2 and $d_2 = \frac{1}{\det(B_2)}$. ~~We will~~ such tha d_2 has at leas t_1. non vanishing digits. We will give the details of values of t_1 and s_1 whne we discuss the sequrity of the system.

The public key of the system is $K_P = (h, n_0, F)$, and the private key is given by ~~the~~ h, n_0, and the five maps $L_1 - - L_3$, and its inverses, that can be used to encript and decrypt. Given a encripted message $z = F(\underline{x}) = DM(\bar{x})$, one compute $\underline{x} = F^{-1}(z)$ and discard the random 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 ~~the~~ n list that contain the coordinates of the $\underline{x}_i$, $Mo_1 = [x_{11} \quad x_{1n}]$, - — $Mo_n = [x_{m1} \; - - x_{mn}]$ and we define to operation on list, multiplication and exponentiation ~~$= [h_1 - h_n]$, $= [$~~ the $S = [s_1 - - s_n]$, $T = [t_1 — t_n]$, the $S \cdot T = [s_i \cdot t_i]$, an $S^a = [s_1^a, - -, s_n^a]$.

With this notations one can see that the exponential G_1 produce in each component polynomials whose list of monomial is $N_{0k} = M_{01}^{a_{k1}} \cdots M_{0n}^{a_{kn}}$.

The mixing map M determine that in the list of monomials of each x'_k apears the list N_{0k} ~~ao~~ joint with the list N_{0j} of the vector that are placed at the $m-n$ ~~entr~~ las entries of x'_k. If b_k is the number of vectors adjoined to x'_k then. If we denote by P_{0k}, $k=1 \cdots n$, such list. then final list of monomials of each components after we aply G_2 each monomial ~~x_1~~ $x_1'^{b_{k1}} \cdots x_n'^{b_{kn}}$ gives $Q_{0k} = P_{01}^{b_{k1}} \cdots P_{0n}^{b_{kn}}$.

Notice that ~~who~~ when ~~we~~ we aply the final $\mathbb{F}_q$-linear ~~isom~~bryection $\tilde{L}_3$, each component stil have the same monomial, that means that The ~~m polinomial~~ There are ~~group~~ n groups of the m polynomial $F_{k1} \cdots F_{km}$ ~~st~~hat have the same monomials, namely the list Q_{0k}. ~~St~~It is clear that the number of monomial of Q_{0k} is at most $((1+b_k)\cdot n^5)^t$. So if we ~~co~~denote by $b_{max} = \max_k (1+b_k)$ we get on each component at most $(b_{max}\cdot n^5)^t$ monomials.

Once one gets the list of monomials of the F_i one gets the coefficient of each group of polynomials. $F_{K1} - - - F_{Km}$ by evaluating on a set of pairs $(x, F_{Ki}(x))$ ~~for~~ big enough ~~for the c~~ to gavantee that the correspon ding linear equations are independents.

That is if