# Inverting bijective polynomial maps over finite fields

Antonio Cafure
Depto. de Matemática, FCEyN, UBA,
Ciudad Universitaria, Pabellón I,
(C1428EHA) Buenos Aires, Argentina.
Instituto del Desarrollo Humano,
Universidad Nac. Gral. Sarmiento,
J. M. Gutiérrez 1150
(1613) Los Polvorines, Argentina.

Guillermo Matera
Instituto del Desarrollo Humano,
Universidad Nac. Gral. Sarmiento,
J. M. Gutiérrez 1150
(1613) Los Polvorines, Argentina.
CONICET, Argentina.

Ariel Waissbein
CoreLabs, CORE ST,
Humboldt 1967 (C1414CTU)
Cdad. de Bs. As., Argentina.
Doctorado en Ingeniería, ITBA:
Av. Eduardo Madero 399
(C1106ACD) Cdad. de Buenos Aires,
Argentina.

***Abstract*— We study the problem of inverting a bijective polynomial map $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$ over a finite field $\mathbb{F}_q$. Our interest mainly stems from the case where $F$ encodes a permutation given by some cryptographic scheme. Given $y^{(0)} \in \mathbb{F}_q^n$, we are able to compute the value $x^{(0)} \in \mathbb{F}_q^n$ for which $F(x^{(0)}) = y^{(0)}$ holds in time $O(Ln^{O(1)}\delta^4)$ up to logarithmic terms. Here $L$ is the cost of the evaluation of $F$ and $\delta$ is a geometric invariant associated to the graph of the polynomial map $F$, called its degree.**

## I. Introduction

Let $\mathbb{F}_q$ be the finite field of $q$ elements, let $\overline{\mathbb{F}}_q$ denote its algebraic closure and let $\mathbb{A}^n$ denote the $n$–dimensional affine space $\overline{\mathbb{F}}_q^n$. Let $X := (X_1, \ldots, X_n)$ be a vector of indeterminates and let $F_1, \ldots, F_n$ be polynomials in $\mathbb{F}_q[X]$. Assume that the map $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$ defined by $F(x) := \big(F_1(x), \ldots, F_n(x)\big)$ is bijective. In this paper we exhibit an algorithm which, on input $y^{(0)} \in \mathbb{F}_q^n$, computes the point $x^{(0)} \in \mathbb{F}_q^n$ for which $F(x^{(0)}) = y^{(0)}$ holds.

This problem is tightly related to the classical algebraic geometry problem of finding an $\mathbb{F}_q$–rational solution of a polynomial system and has direct applications in the domain of public–key cryptography (see e.g. [1]).

Algebrists and other computer scientists have tried to tackle this problem (see e.g. [2], [3], [4]). It is well–known that this is a hard problem, even when restricting to quadratic equations ([5], [6]). Indeed, the solutions proposed in [2], [3] have exponential running time, and only [4] achieves a polynomial complexity in the Bézout number of the system (which is nevertheless exponential in worst case). [8], [9] and [10] exhibit efficient algorithms for special cases.

In the setting of cryptography, since [11] researchers have unsuccessfully tried to construct public–key schemes based on the (allegedly) difficult problem of solving polynomial systems over finite fields, but proposals are typically proved to be weak through *ad hoc* attacks (see [12], [9]). This might be seen as an indication that the polynomial maps used in public–key cryptography —typically with underlying quadratic polynomials— are not intrinsically difficult to invert, and calls for the study of parameters to measure such difficulty.

In [8] Sturtivant and Zhang exhibit an algorithm for inverting a bijective polynomial map $F$ over $\mathbb{F}_q$, assuming that $F$ is an automorphism of $\mathbb{F}_q[X]^n$ whose inverse has degree $(dn)^{O(1)}$, with $d := \max_{1 \le k \le n} \deg F_k$. The algorithm performs $(Lnd)^{O(1)}$ arithmetic operations in $\mathbb{F}_q$, where $L$ is the number of arithmetic operations necessary to evaluate $F$.

From the cryptographic point of view, the critical problem is that of computing the inverse image of a given point $y^{(0)} \in \mathbb{F}_q^n$ under a map $F$, rather than that of inverting $F$ itself. In this sense, we solve the former under much less stringent hypotheses than those of [8]. More precisely, we exhibit a (probabilistic) algorithm that, given a point $y^{(0)} \in \mathbb{F}_q^n$ and a straight–line program evaluating $F$ in $\mathbb{F}_q[X]$, computes the point $x^{(0)} \in \mathbb{F}_q^n$ for which $F(x^{(0)}) = y^{(0)}$ holds. For this purpose we make the additional (geometric) hypothesis that the projection of the graph of $F$ on the $Y$–axis is what in algebraic geometry is called a finite morphism. This assures that the fibers $F^{-1}(y)$ are nonempty and finite for every $y \in \mathbb{A}^n$. We remark that this is a reasonable assumption from the cryptographic point of view, because it is typically met in the public–key schemes proposed.

The complexity of our algorithm is roughly of order $O((Ln^4+\delta^2)n\delta^2)$, where $L$ is the complexity of the evaluation of $F$ and $\delta$ is a geometric invariant associated to the map $F$: the (geometric) degree of its graph. This degree is a basic measure of the complexity of the description of the graph of $F$ (see e.g. [13], [14]), which may play a significant role to assess the difficulty of inverting $F$. In this sense, $\delta$ should be taken into account as a *security estimation parameter*. Notice that $\delta$ is upper bounded by the Bézout number $\deg F_1 \cdots \deg F_n$, and this bound is attained in worst case (see e.g. [13]).

Finally, if the hypotheses of [8] hold, then our algorithm meets also the complexity bound $(Lnd)^{O(1)}$ of [8].

## II. Notions and Notations

Let $\mathbb{K}$ be a subfield of $\overline{\mathbb{F}}_q$ containing $\mathbb{F}_q$. Let $V$ be a $\mathbb{K}$–definable affine subvariety of $\mathbb{A}^n$ (a $\mathbb{K}$–variety for short). We denote by $I(V) \subset \mathbb{K}[X]$ its defining ideal and by $\mathbb{K}[V]$ its coordinate ring, namely, the quotient ring $\mathbb{K}[V] := \mathbb{K}[X]/I(V)$.

If $V$ is an irreducible $\mathbb{K}$–variety, we define its *dimension* as the transcendence degree of the field extension $\mathbb{K} \hookrightarrow \mathbb{K}(V)$, where $\mathbb{K}(V)$ is the field of fractions of the domain $\mathbb{K}[V]$, and the *degree* as the maximum number of points lying in the intersection of $V$ with an affine linear subspace $L$ of $\mathbb{A}^n$ of

codimension $\dim V$ for which $\#(V \cap L) < \infty$ holds. More generally, if $V = C_1 \cup \cdots \cup C_N$ is the decomposition of $V$ into irreducible $\mathbb{K}$–components, we define the dimension of $V$ as $\dim V := \max_{1 \le i \le N} \dim C_i$ and the degree of $V$ as $\deg V := \sum_{i=1}^{N} \deg C_i$ (cf. [13]).

A $\mathbb{K}$–variety $V \subset \mathbb{A}^n$ is *absolutely irreducible* if it is an irreducible $\overline{\mathbb{F}}_q$–variety.

Let $V$ be an irreducible $\mathbb{K}$–variety of $\mathbb{A}^n$ and let $\pi : V \to \mathbb{A}^n$ be a finite morphism, that is, a morphism which induces an integral ring extension $\mathbb{K}[\mathbb{A}^n] \hookrightarrow \mathbb{K}[V]$. The degree $\deg \pi$ of $\pi$ is defined as the degree of the field extension $\mathbb{K}(\mathbb{A}^n) \hookrightarrow \mathbb{K}(V)$. We say that $y \in \mathbb{A}^n$ is a *lifting point* of $\pi$ if the number of inverse images of $y$ is equal to the degree of the morphism $\pi$.

### A. Geometric solutions

We shall use a representation of $\mathbb{K}$–varieties which is well suited for algorithmic purposes (cf. [15]). Let $V \subset \mathbb{A}^n$ be a $\mathbb{K}$–variety of dimension $r$ and degree $\delta$ and suppose that the linear projection $\pi : V \to \mathbb{A}^r$ defined by $\pi(x) := (x_1, \ldots, x_r)$ is a finite morphism of degree $D$.

*Definition 2.1:* A *geometric solution* of $V$ consists of the following items:

- a linear form $U \in \mathbb{K}[X]$ which induces a primitive element of the ring extension $\mathbb{K}[X_1, \ldots, X_r] \hookrightarrow \mathbb{K}[V]$, i.e. an element $u \in \mathbb{K}[V]$ whose (monic) minimal polynomial $m \in \mathbb{K}[X_1, \ldots, X_r][T]$ over $\mathbb{K}[X_1, \ldots, X_r]$ satisfies the condition $\deg_T m = D$. Observe that $\deg m \le \delta$ holds.
- the minimal polynomial $m \in \mathbb{K}[X_1, \ldots, X_r][T]$ of $u$.
- a generic "*parametrization*" of the variety $V$ by the zeros of $m$, of the form $(\partial m/\partial T)X_k - v_k$ $(r+1 \le k \le n)$ with $v_k \in \mathbb{K}[X_1, \ldots, X_r][T]$. We require that $\deg_T v_k < D$, $\deg_X v_k \le \delta$ and $(\partial m/\partial T)(U)X_k - v_k(U) \in I(V)$ hold.

The polynomial $m$ can be also defined as follows: consider the linear map $\pi_U : V \to \mathbb{A}^{r+1}$ defined by $\pi_U(x) := (x_1, \ldots, x_r, U(x))$. The Zariski closure of $\pi_U(V)$ is a $\mathbb{K}$–hypersurface $H$ of $\mathbb{A}^{r+1}$, which is indeed defined by $m$.

We remark that in the case $r = 0$, a linear form $U$ induces a primitive element of the ring extension $\mathbb{K} \hookrightarrow \mathbb{K}[V]$ if and only if $U$ separates the points of $V$.

## III. Preparation of the input data

Let $F_1, \ldots, F_n \in \mathbb{F}_q[X]$ be polynomials of degree at most $d$. Let $F : \mathbb{A}^n \to \mathbb{A}^n$ be the polynomial map defined by $F_1, \ldots, F_n$. Observe that the restriction of $F$ to $\mathbb{F}_q^n$ is a well–defined polynomial map from $\mathbb{F}_q^n$ to $\mathbb{F}_q^n$, also denoted by $F$.

Let $Y := (Y_1, \ldots, Y_n)$ be a vector of new indeterminates and let $V \subset \mathbb{A}^{2n}$ be the affine $\mathbb{F}_q$–variety defined by

$$V := \{(x, y) \in \mathbb{A}^{2n} : \ y_i = F_i(x),\ 1 \le i \le n\}.$$

We make the following assumptions on the map $F$ (usually met in the cryptographic situations we are interested in):

$(i)$ $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$ is a bijective map.

$(ii)$ The projection map $\pi : V \to \mathbb{A}^n$ defined by $\pi(y, x) := y$ is a finite morphism. In particular, the fiber $V_y := \pi^{-1}(y)$ is a zero–dimensional subvariety of $V$ for every $y \in \mathbb{A}^n$.

We deduce that $V$ has dimension $n$ and that the image of $F$ is a dense subset of $\mathbb{A}^n$. Thus $Y_1, \ldots, Y_n$ are algebraically independent in $\overline{\mathbb{F}}_q[V]$. We set $\delta := \deg V$ and $D := \deg \pi$.

*Lemma 3.1:* $V$ is an absolutely irreducible $\mathbb{F}_q$–variety.

*Proof:* The ideal $I := (Y_i - F_i(X) : 1 \le i \le n) \subset \overline{\mathbb{F}}_q[X, Y]$ is contained in $I(V)$. Since $\overline{\mathbb{F}}_q[X, Y]/I$ is isomorphic to $\overline{\mathbb{F}}_q[X]$, $I$ is a prime ideal, and thus $I = I(V)$ holds. ∎

Suppose that we are given a geometric solution of $V$. By the remark after Definition 2.1, we see that $V$ is birationally equivalent to the hypersurface $H$ defined by the minimal polynomial $m \in \overline{\mathbb{F}}_q[Y, T]$. Since $V$ is absolutely irreducible, so is $H$ and then $m$.

Suppose that we are given $y^{(0)} \in \mathbb{F}_q^n$ and let $V_{y^{(0)}}$ be the corresponding zero–dimensional fiber. In order to compute the point $x^{(0)} \in \mathbb{F}_q^n$ for which $(x^{(0)}, y^{(0)}) \in V_{y^{(0)}}$ holds, we shall deform the system $F(X) = y^{(0)}$ into a system $F(X) = F(x^{(1)})$ with a point $x^{(1)}$ randomly chosen in a suitable finite field extension $\mathbb{K}$ of $\mathbb{F}_q$ to be determined (cf. [16]). The next two lemmas state suitable bounds on the degree of the genericity conditions underlying the choice of $x^{(1)}$.

*Lemma 3.2:* There exists a polynomial $A \in \overline{\mathbb{F}}_q[X]$ of degree at most $3d\delta^4$ such that for any $x \in \mathbb{A}^n$ with $A(x) \neq 0$, the point $y := F(x)$ satisfies the following conditions:

$(i)$ $y$ is a lifting point of $\pi : V \to \mathbb{A}^n$,

$(ii)$ The curve $\mathcal{C}$ defined by $F(X) = y + (S-1)(y - y^{(0)})$ is absolutely irreducible.

*Proof:* Let $\mathcal{L} \in \overline{\mathbb{F}}_q[X]$ be a linear form inducing a primitive element of the ring extension $\overline{\mathbb{F}}_q[Y] \hookrightarrow \overline{\mathbb{F}}_q[V]$ and let $m_{\mathcal{L}} \in \overline{\mathbb{F}}_q[Y][T]$ be its minimal polynomial.

Let $\tilde{A}_1 \in \overline{\mathbb{F}}_q[Y]$ be the discriminant of $m_{\mathcal{L}}$ with respect to $T$. The absolutely irreducibility of $m_{\mathcal{L}}$ implies $\tilde{A}_1 \neq 0$. Let $A_1 := \tilde{A}_1(F(X)) \in \overline{\mathbb{F}}_q[X]$. Since the image of $F$ is a dense subset of $\mathbb{A}^n$, there exists $x \in \mathbb{A}^n$ such that $A_1(x) \neq 0$. Hence, $A_1$ is a nonzero polynomial of degree bounded by $(2D-1)d\delta$.

Set $\widetilde{m}_{\mathcal{L}}(X, S, T) := m_{\mathcal{L}}(F(X) + (S-1)(F(X) - y^{(0)}), T) \in \overline{\mathbb{F}}_q[X, S, T]$. Since $m_{\mathcal{L}}$ is monic in $\overline{\mathbb{F}}_q[Y][T]$, we see that $\widetilde{m}_{\mathcal{L}}$ is a monic element $\overline{\mathbb{F}}_q[X, S][T]$. This implies that $\widetilde{m}_{\mathcal{L}}(x, 1, T) = m_{\mathcal{L}}(y, T)$ is a separable polynomial of $\overline{\mathbb{F}}_q[X][T]$ for any lifting point $y$ of $\pi$ and any $x \in V_y$.

Following [17, Theorem 5], in the version of [4, Theorem 3.6], there exists a polynomial $A_2 \in \overline{\mathbb{F}}_q[X]$ of degree bounded by $2d\delta^4$ such that for any $x \in \overline{\mathbb{F}}_q^n$ with $A_2(x) \neq 0$ the polynomial $\widetilde{m}_{\mathcal{L}}(x, S, T)$ is absolutely irreducible.

Let $A := A_1 A_2 \in \overline{\mathbb{F}}_q[X]$. Observe that $A$ has degree at most $3d\delta^4$. Let $x \in \mathbb{A}^n$ be any point satisfying $A(x) \neq 0$ and let $y := F(x)$. We claim that conditions $(i)$ and $(ii)$ of the statement of the lemma are satisfied. Indeed, $A_1(x) \neq 0$ implies that $\tilde{A}_1(y) \neq 0$, that is, the discriminant of $m_{\mathcal{L}}(y, T)$ with respect to $T$ is nonzero. We deduce that $m_{\mathcal{L}}(y, T)$ has $D$ distinct roots and therefore, $y$ is a lifting point of $\pi$. Finally, since $y$ is a lifting point of $\pi$ and $A_2(x) \neq 0$, $\widetilde{m}_{\mathcal{L}}(x, S, T)$ is absolutely irreducible and hence, so is $\mathcal{C}$. ∎

Suppose that we have chosen a point $x \in \mathbb{A}^n$ satisfying the conditions of Lemma 3.2 and let $y := F(x)$.

*Lemma 3.3:* Let $\Lambda := (\Lambda_1, \ldots, \Lambda_n)$ be indeterminates. There exists a polynomial $B \in \overline{\mathbb{F}}_q[\Lambda] \setminus \{0\}$ of degree at most

$2D^2$ such that for any $\lambda \in \mathbb{A}^n$ with $B(\lambda) \neq 0$, the linear form $U = \lambda_1 X_1 + \cdots + \lambda_n X_n$ separates the points of $V_y$ and $V_{y^{(0)}}$.

*Proof:* Let $V_y \cup V_{y^{(0)}} := \{P_1, \ldots, P_{D'}\}$. Let $U_\Lambda := \Lambda_1 X_1 + \cdots + \Lambda_n X_n$, and let $B(\Lambda) := \Pi_{1 \leq i < j \leq D'}(U_\Lambda(P_i) - U_\Lambda(P_j))$. Observe that $D' \leq 2D$ holds. Then $B \in \overline{\mathbb{F}}_q[\Lambda]$ is a nonzero polynomial of degree at most $2D^2$. Furthermore, if $\lambda \in \mathbb{A}^n$ satisfies $B(\lambda) \neq 0$ holds, then by construction it is clear that $U$ separates the points of $V_y$ and of $V_{y^{(0)}}$. ∎

Our algorithm works in a finite field extension $\mathbb{K}$ of $\mathbb{F}_q$ such that there exist $\lambda, x \in \mathbb{K}^n$ satisfying the requirements of Lemmas 3.2 and 3.3. Our next result states that we may randomly choose $\lambda$ and $x$.

*Corollary 3.4:* With notations as in Lemmas 3.2 and 3.3, fix $\mu > 0$ and let $\mathbb{K}$ be a finite field extension of $\mathbb{F}_q$ of cardinality greater than $4\mu d\delta^4$. Then a random choice $(x, \lambda) \in \mathbb{K}^{2n}$ satisfies $(AB)(x, \lambda) \neq 0$ with probability at least $1 - 1/\mu$.

*Proof:* The number of zeros in $\mathbb{K}^n$ of the polynomial $A$ is at most $3d\delta^4(\#\mathbb{K})^{n^2-1}$ [18, Theorem 6.13]. Then a random choice of $x \in \mathbb{K}^n$ satisfies $A(x) \neq 0$ with probability at least $1 - 3d\delta^4/\#\mathbb{K} \geq 1 - 3/4\mu$. Given such a choice, a random choice of $\lambda \in \mathbb{K}^n$ satisfies $B(\lambda) \neq 0$ with probability at least $1 - 2D^2/\#\mathbb{K} \geq 1 - 1/4\mu$. This shows that a random choice $(\lambda, x) \in \mathbb{K}^{2n}$ satisfies $(AB)(x, \lambda) \neq 0$ with probability at least $(1 - 3/4\mu)(1 - 1/4\mu) \geq 1 - 1/\mu$. ∎

## IV. The algorithm

In this section we exhibit an algorithm which computes the point $x^{(0)} \in \mathbb{F}_q^n$ for which $F(x^{(0)}) = y^{(0)}$ holds. By Corollary 3.4 we may assume that we are given $(\lambda, x^{(1)}) \in \mathbb{K}^{2n}$ satisfying the requirements of Lemmas 3.2 and 3.3, where $\mathbb{K}$ is a finite field extension of $\mathbb{F}_q$ of cardinality $O(d\delta^4)$. This means that $y^{(1)} := F(x^{(1)})$ is a lifting point of $\pi : V \to \mathbb{A}^n$, the space curve $\mathcal{C}$ of $\mathbb{A}^{n+1}$ defined by

$$y^{(1)} + (S-1)(y^{(1)} - y^{(0)}) = F(X) \tag{1}$$

is absolutely irreducible, and the linear form $U := \lambda_1 X_1 + \cdots + \lambda_n X_n \in \mathbb{K}[X]$ separates the points of $V_{y^{(1)}}$ and $V_{y^{(0)}}$. Let $\pi_S : \mathcal{C} \to \mathbb{A}^1$ be the projection map defined by $\pi_S(s, x) := s$. We have that $\pi_S$ is a finite morphism of degree $D$, the identities $\mathcal{C}_1 := \pi_S^{-1}(1) = V_{y^{(1)}}$ and $\pi_S^{-1}(0) = V_{y^{(0)}}$ hold, and $S = 1$ is lifting point of $\pi_S$. Since $U$ separates the points of $V_{y^{(1)}} = \mathcal{C}_1$ and $S = 1$ is lifting point of $\pi_S$, it follows that $U$ is a primitive element of $\mathbb{K}[S] \hookrightarrow \mathbb{K}[\mathcal{C}]$.

In the first step of this algorithm we compute the minimal polynomial $m_S(S, T)$ of $U$ in the ring extension $\mathbb{K}[S] \hookrightarrow \mathbb{K}[\mathcal{C}]$. This is a monic absolutely irreducible element of $\mathbb{K}[S][T]$ with $\deg_S m_S \leq \delta$ and $\deg_T m_S = D$.

### A. The computation of the polynomial $m_S$

Consider the factorization of $m_S(S, T)$ in $\mathbb{K}[\![S-1]\!][T]$. From the fact that $m_S(1, T)$ is separable of degree $D$, we conclude that $m_S(S, T)$ has a factorization of the form $m_S = \prod_{i=1}^{D}(T - \sigma^{(i)})$ with $\sigma^{(i)} \in \mathbb{K}[\![S-1]\!]$ for $1 \leq i \leq D$. Furthermore, $m_S(1, T)$ can be factored as $m_S(1, T) = \prod_{i=1}^{D}(T - \sigma^{(i)}(1))$, where $\sigma^{(i)}(1)$ represents the constant term of $\sigma^{(i)}$ for $1 \leq i \leq D$. Let $\pi_S^{-1}(1) = \{P_1, \ldots, P_D\}$. We have $m_S(1, T) = \prod_{i=1}^{D}(T - U(P_i))$. Since $x^{(1)}$ belongs to the fiber $\pi_S^{-1}(1)$, we see that there exists $i$ for which $U(x^{(1)}) = \sigma^{(i)}(1)$ holds. For simplicity, we shall denote such $\sigma^{(i)}$ by $\sigma$.

The algorithm that computes the polynomial $m_S(S, T)$ starts computing the power series $\sigma$ truncated up to order $N := 2D\delta$. Let $\sigma_N$ be the polynomial of $\overline{\mathbb{F}}_q[S]$ of degree at most $N$ satisfying $\sigma \equiv \sigma_N \bmod (S-1)^{N+1}$. Our next result shows how to compute $m_S(S, T)$ from $\sigma_N$.

*Lemma 4.1:* Let $g \in \mathbb{K}[S, T]$ be a polynomial with $\deg_S g \leq \delta$ and $\deg_T g \leq D$ such that the congruence relation

$$g(S, \sigma_N) \equiv 0 \bmod (S-1)^{N+1} \tag{2}$$

holds. Then $m_S$ divides $g$ in $\mathbb{K}[S, T]$.

*Proof:* Let $g \in \mathbb{K}[S, T]$ be a solution of (2). The resultant $h \in \mathbb{K}[S]$ of $g$ and $m_S$ with respect to $T$ has degree at most $N$ and belongs to the ideal generated by $m_S$ and $g$. Since $m_S(S, \sigma_N)$ and $g(S, \sigma_N)$ are congruent to 0 mod $(S-1)^{N+1}$, we see that $h(S) \equiv 0 \bmod (S-1)^{N+1}$ holds. Then we have $h = 0$, which implies that $m_S$ and $g$ have a common factor in $\mathbb{K}(S)[T]$. Combining the irreducibility of $m_S$ in $\mathbb{K}(S)[T]$ with the Gauss lemma finishes the proof. ∎

From Lemma 4.1 we conclude that $m_S$ can be characterized as the nonzero solution of (2) of minimal degree.

Notice that (2) is a linear system in the coefficients of $g$. In order to obtain the equations of (2), we need the powers $\sigma_N, \ldots, \sigma_N^D$ truncated at order $N+1$. The computation of $\sigma_N$ is based on a multivariate Newton iteration over the power series ring $\mathbb{K}[\![S-1]\!]$. Substituting 1 for $S$ in (1), we obtain the system $y^{(1)} = F(X)$. Since $y^{(1)}$ is a lifting point of $\pi$, from [4, Lemma 2.1] we see that none of the solutions of $y^{(1)} = F(X)$ annihilates the determinant of the Jacobian matrix $J_F := (\partial F_i)/(\partial X_j)_{1 \leq i,j \leq n}$. In particular, $\det J_F(x^{(1)}) \neq 0$ holds. Let $N_F$ be the Newton–Hensel operator:

$$N_F(X) := X - J_F^{-1}(X) G(S, X),$$

with $G(S, X) := F(X) - y^{(1)} - (S-1)(y^{(1)} - y^{(0)})$ and let $N_F^{(k)}$ denote the $k$–fold iteration of $N_F$. Then, for $\Psi_k := N_F^{(k)}(x^{(1)}) \in \mathbb{K}[\![S-1]\!]^n$, it is well–known that

$$G(S, \Psi_k) \equiv 0 \bmod (S-1)^{2^k} \tag{3}$$

holds. Since $m_S(S, U(X))$ vanishes on $\mathcal{C}$, it belongs to the ideal of $\mathbb{K}[S, X]$ generated by $G$. Therefore, (3) implies that $m_S(S, U(\Psi_k)) \equiv 0 \bmod (S-1)^{2^k}$ holds. From the identity $U(\Psi_k)(1) = U(x^{(1)})$ we deduce that $U(\Psi_k) \equiv \sigma \bmod (S-1)^{2^k}$. Hence, we obtain $\sigma_N$ as the power series $U(\Psi_\kappa)$ with $\kappa := \lceil \log_2(N+1) \rceil$ truncated at order $N+1$. From $\sigma_N$ we easily compute the powers $\sigma_N^2, \ldots, \sigma_N^D$ by successive multiplication and truncation.

In order to state the complexity of this procedure, we shall use the quantity $\mathsf{M}(m) := m \log^2 m \log\log m$. An arithmetic operation in $\mathbb{K}$ requires $O(\mathsf{M}(\log \#\mathbb{K}))$ bit operations, and the number of arithmetic operations in $\mathbb{K}$ necessary to compute the multiplication, division or gcd of univariate polynomials of $\mathbb{K}[T]$ of degree at most $m$ is also of order $O\big(\mathsf{M}(m)\big)$ (cf. [19], [20]). On the other hand, we shall also use the exponent $\omega$

of the complexity $O(n^\omega)$ of the multiplication of two $(n\times n)$–matrices with coefficients in $\mathbb{K}$. We have (theoretically) $\omega < 2.376$, but for practical issues it is usually taken $\omega = \log_2 7 \sim 2.81$ (cf. [20]). We have:

*Proposition 4.2:* $\sigma_N, \ldots, \sigma_N^D \bmod (S-1)^{N+1}$ can be computed with $O\big((L+n^{1+\omega})\mathsf{M}(D\delta)\big)$ operations in $\mathbb{K}$.

*Proof:* The evaluation of the Newton–Hensel iterator $N_F$ requires the inversion of the Jacobian matrix $J_F$. Since the polynomials $F_1, \ldots, F_n$ can be evaluated with $L$ arithmetic operations, from the Baur–Strassen theorem [21] we have that the entries of $J_F$ can be evaluated with $O(L)$ arithmetic operations and its determinant and adjoint matrix can be evaluated with $O(L + n^{1+\omega})$ arithmetic operations [20]. In order to compute $\Psi_{k+1}$ we compute the inverse matrix $J_F^{-1}(\Psi_k)$ as the product $J_F^{-1}(\Psi_k) = \det J_F(\Psi_k)^{-1} \cdot Adj\big(J_F(\Psi_k)\big)$ of the reciprocal of the power series $\det J_F(\Psi_k)$ by the adjoint matrix $Adj\big(J_F(\Psi_k)\big)$. The truncation of $\det J_F(\Psi_k)^{-1}$ can be computed using fast power series inversion ([19], [20]) with $O\big((L+n^{1+\omega})\mathsf{M}(2^k)\big)$ arithmetic operations. With similar cost we compute $Adj\big(J_F(\Psi_k)\big)$ and the product $\det J_F(\Psi_k)^{-1} \cdot Adj\big(J_F(\Psi_k)\big)$. Therefore, the computation of $\Psi_k$ for $2 \le k \le \kappa$ requires $O\big((L + n^{1+\omega}) \sum_{k=0}^{\kappa-1} \mathsf{M}(2^k)\big) = O\big((L + n^{1+\omega})\mathsf{M}(D\delta)\big)$ arithmetic operations. The remaining steps do not change the overall asymptotic complexity. ∎

Next we discuss how we can solve (2). This is a linear system with $N+1$ equations and $D\delta$ indeterminates, namely, the coefficients of the solution $g \in \mathbb{K}[S,T]$ of (2). Best general–purpose algorithms solving a system of size $O(D\delta \times D\delta)$ require $O((D\delta)^\omega)$ arithmetic operations [20]. We shall profit from the structure of (2) in order to improve this complexity estimate to $O\big(D^2\mathsf{M}(D\delta)\big)$.

*Lemma 4.3:* For a suitable ordering of the indeterminates, the matrix defining (2) is block–Toeplitz with $D$ blocks.

*Proof:* Fix $i$ with $0 \le i \le N$ and consider the $i$–th equation of (2), which expresses the condition that the coefficient of $(S-1)^i$ in $g(S,\sigma_N)$ must vanish. Let $g(S,T) := \sum_{j=0}^{\delta}\sum_{k=0}^{D} A_{j,k}(S-1)^j T^k$ and $\sigma_N^k \equiv \sum_{h=0}^{N} \alpha_{h,k}(S-1)^h \bmod (S-1)^{N+1}$. Then the $i$th equation reads

$$\sum_{j=0}^{\delta}\sum_{k=0}^{D} \alpha_{i-j,k} A_{j,k} = 0, \tag{4}$$

with $\alpha_{i-j,k} = 0$ for $i-j<0$. Fix $k_0$ and let $M^{(k_0)}$ be the $(N+1)\times\delta$–submatrix of the matrix $M$ defining (2) formed by the columns of $M$ corresponding to the indeterminates $A_{j,k_0}$ for $0 \le j \le \delta$. From (4) we see that $M^{(k_0)}$ is a Toeplitz matrix. Arranging the indeterminates $A_{j,k}$ according to the inverse lexicographical order on the set of pairs $(k,j)$ we deduce that $M$ is a block–Toeplitz matrix, with $D$ blocks. ∎

Lemma 4.3 enables us to solve (2) using the theory of matrices of fixed displacement rank (cf. [20], [22]). From [22, Chapter 5] it follows that a basis of the null space of a block–Toeplitz $(2D\delta \times D\delta)$–matrix with $D$ blocks can be probabilistically computed with $O\big(D^2\mathsf{M}(D\delta)\big)$ operations in $\mathbb{K}$. From such a basis we easily obtain $m_S$ within the same asymptotic complexity. In conclusion, we have:

*Proposition 4.4:* The polynomial $m_S \in \mathbb{K}[S,T]$ can be computed with $O\big((L+n^{\omega+1}+D^2)\mathsf{M}(D\delta)\big)$ operations in $\mathbb{K}$.

### *B. Computation of a geometric solution of $\mathcal{C}$*

In this section we extend the algorithm of the previous section to an algorithm computing a geometric solution of the curve $\mathcal{C}$ defined in (1). Let $\Lambda := (\Lambda_1, \ldots, \Lambda_n)$ be a vector of new indeterminates and let $\pi_\Lambda : \mathbb{A}^n \times \mathcal{C} \to \mathbb{A}^n \times \mathbb{A}^1$ be the projection map defined by $\pi_\Lambda(\lambda, s, x) := (\lambda, s)$. Since $\pi_S$ is a finite morphism, we deduce that $\pi_\Lambda$ is a finite morphism. Furthermore, the minimal polynomial $m_\Lambda(\Lambda, S, T) \in \mathbb{K}[\Lambda, S, T]$ of the linear form $U_\Lambda := \Lambda_1 X_1 + \cdots + \Lambda_n X_n$ in the ring extension $\mathbb{K}[\Lambda, S] \hookrightarrow \mathbb{K}[\mathbb{A}^n \times \mathcal{C}]$ induced by $\pi_\Lambda$ satisfies $\deg_T m_\Lambda \le D$, $\deg_S m_\Lambda \le \delta$ and $\deg_\Lambda m_\Lambda \le \delta$ (see e.g. [7, Proposition 6.1]). We have that $m_\Lambda$ is a separable element of $\mathbb{K}[\Lambda, S][T]$ and $\partial m_\Lambda/\partial T$ is not a zero divisor of $\mathbb{K}[\mathbb{A}^n \times \mathcal{C}]$ (see e.g. [7, Proposition 6.1]).

Let $\xi_1, \ldots, \xi_n$ be the coordinate functions of $\mathbb{K}[\mathcal{C}]$ defined by $X_1, \ldots, X_n$ and let $\widehat{U}_\Lambda := \sum_{k=1}^n \Lambda_k \xi_k$. Taking the partial derivative with respect to the variable $\Lambda_k$ at both sides of the identity $m_\Lambda(\Lambda, S, \widehat{U}_\Lambda) = 0$ of $\mathbb{K}[\mathbb{A}^n \times \mathcal{C}]$ for $1 \le k \le n$, we see that the following identity holds in $\mathbb{K}[\mathbb{A}^n \times \mathcal{C}]$:

$$(\partial m_V/\partial T)(\Lambda, S, \widehat{U}_\Lambda)\, \xi_k + (\partial m_\Lambda/\partial \Lambda_k)(\Lambda, S, \widehat{U}_\Lambda) = 0. \tag{5}$$

Observe that $\partial m_\Lambda/\partial\Lambda_k(\Lambda, S, T)$ satisfies $\deg_S \partial m_\Lambda/\partial\Lambda_k \le \delta$ and $\deg_T \partial m_\Lambda/\partial\Lambda_k \le D$. Substituting $\lambda_k$ for $\Lambda_k$ in (5) we obtain the parametrizations

$$(\partial m_S/\partial T)(S,T)X_k - v_k(S,T) \quad (1 \le k \le n) \tag{6}$$

we are looking for. In order to compute $v_1, \ldots, v_n$, we observe that the Taylor expansion of $m_\Lambda(\Lambda, S, T)$ in powers of $\Lambda - \lambda := (\Lambda_1 - \lambda_1, \ldots, \Lambda_n - \lambda_n)$ of order one has the expression:

$$m_\Lambda = m_S + \sum_{k=1}^{n} \Big(\frac{\partial m_S}{\partial T} X_k - v_k\Big)(\Lambda_k - \lambda_k) \bmod (\Lambda - \lambda)^2.$$

We shall compute this (truncated) Taylor expansion applying the algorithm underlying Proposition 4.4 to the generic linear form $U_\Lambda$. Each arithmetic operation in this algorithm now becomes an arithmetic operation between two polynomials of $\mathbb{K}[\Lambda]$, truncated at order $(\Lambda-\lambda)^2$. Since adding or multiplying two polynomials of $\mathbb{K}[\Lambda]$ truncated at order $(\Lambda-\lambda)^2$ requires $O(n)$ arithmetic operations in $\mathbb{K}$, we obtain:

*Proposition 4.5:* A geometric solution of $\mathcal{C}$ can be computed with $O\big((L+n^{\omega+1}+D^2)n\mathsf{M}(D\delta)\big)$ operations in $\mathbb{K}$.

### *C. Computation of the point $x^{(0)}$*

In this section we describe the computation of the point $x^{(0)} \in \mathbb{F}_q^n$ for which $F(x^{(0)}) = y^{(0)}$ holds, given a $\mathbb{K}$–definable geometric solution of the curve $\mathcal{C}$ defined in (1).

Set $\pi_S^{-1}(0) =: \{0\} \times \mathcal{C}_0$. Our hypotheses imply that $x^{(0)}$ is the only $\mathbb{F}_q$–rational point of $\mathcal{C}_0$. Since $U$ separates the points of $\pi_S^{-1}(0)$, from a geometric solution of $\mathcal{C}$ we easily obtain a geometric solution of $\mathcal{C}_0$. Indeed, substituting 0 for $S$ in $m_S, v_1, \ldots, v_n$, we obtain polynomials $m_S(0,T), v_1(0,T), \ldots, v_n(0,T) \in \mathbb{K}[T]$

which represent a complete description of $\mathcal{C}_0$, eventually including multiplicities. Such multiplicities are represented by multiple factors of $m_S(0,T)$, which are also factors of $v_1(0,T),\ldots,v_n(0,T)$ (see e.g. [23, §6.5]). Therefore, they may be removed in the following way: first we compute $a(T) := \gcd\big(m_S(0,T),(\partial m_S/\partial T)(0,T)\big)$, and we clean the multiplicities of $m_S(0,T)$ by computing $m_0 := m_S(0,T)/a(T)$. Then we obtain the parametrizations $\big((\partial m_S/\partial T)(0,T)/a(T)\big)X_k - v_k(0,T)/a(T)$ $(1 \le k \le n)$ which form a geometric solution of our input system. Finally, taking into account that $m_0$ and $(\partial m_S/\partial T)(0,T)/a(T)$ are relatively prime in $\mathbb{K}[T]$, we invert $(\partial m_S/\partial T)(0,T)/a(T)$ modulo $m_0$ and obtain parametrizations $X_k - w_k(T)$ for $1 \le k \le n$ which are better suited for our purposes. Computing the dense representation of $m_S(0,T), v_1(0,T),\ldots,v_n(0,T)$ requires $O(nD\delta)$ arithmetic operations in $\mathbb{K}$. The remaining computations involve multiplications, gcd and modular inversions of univariate polynomials of degree at most $D$ and thus require $O\big(n\mathsf{M}(D)\big)$ operations in $\mathbb{K}$. Thus we obtain:

*Proposition 4.6:* Given a geometric solution of $\mathcal{C}$, we can compute a geometric solution $m_0(T), X_1 - w_1(T),\ldots,X_n - w_n(T)$ of $\mathcal{C}_0$ with $O(n\delta\mathsf{M}(D))$ operations in $\mathbb{K}$.

Next, we compute the $\mathbb{K}$–rational points of $\mathcal{C}_0$. Let $h := \gcd(m_0, T^{\#(\mathbb{K})} - T) \in \mathbb{K}[T]$. The computation of $h$ requires $O\big(\mathsf{M}(D)\log\#(\mathbb{K})\big)$ operations in $\mathbb{K}$ [19, Corollary 11.16]. The roots of $h$ are the values $U(P)$ of the $\mathbb{K}$–rational points $P$ of $\mathcal{C}_0$. In particular, $U(x^{(0)}) \in \mathbb{K}$ is a root of $h$.

Since $h$ factors into linear factors in $\mathbb{K}[T]$, its factorization can be probabilistically computed with $O\big(\mathsf{M}(D)\log\#(\mathbb{K})\big)$ operations in $\mathbb{K}$ [19, Theorem 14.9]. We evaluate the polynomials $w_k$ at the roots $\alpha$ of $h$ and obtain $x^{(0)}$ as the only $\mathbb{F}_q$–rational point of the form $\big(w_1(\alpha),\ldots,w_n(\alpha)\big)$.

Putting together these considerations and Propositions 4.5 and 4.6 we obtain our main result:

*Theorem 4.7:* The only $\mathbb{F}_q$–rational solution of the input system $F(X) = y^{(0)}$ can be computed with $O\big((L + n^{1+\omega} + D^2)n\mathsf{M}(D\delta)\mathsf{M}(\log q\delta) + \mathsf{M}(D)\mathsf{M}^2(\log q\delta)\big)$ bit operations.

Since $D \le \delta$ holds, our complexity estimate may be roughly described as polynomial in the complexity $L$ of the evaluation of $F_1,\ldots,F_n$, the quantities $n$ and $\log q$, and a geometric invariant: the degree $\delta$ of the graph of the map $F$. In this sense, we see that the practical convenience of our algorithm, and the subsequent (in)security of cryptosystems based on polynomial maps over a finite field, essentially relies on this geometric invariant. In worst case we have $\delta = \deg F_1 \cdots \deg F_n$, which implies that our algorithm is exponential. Furthermore, adapting the arguments of [14] it is possible to prove that any *universal* algorithm solving $F(X) = y^{(0)}$ has necessarily complexity $(\deg F_1 \cdots \deg F_n)^{\Omega(1)}$, showing thus the security of the corresponding cryptosystem with respect to universal decoding algorithms. A universal algorithm is an algorithm which does not distinguish input systems according to geometric invariants and represents a model for the standard algorithms based on rewriting techniques, such as Gröbner basis algorithms.

Finally, we comment on the behavior of our algorithm under the hypotheses of [8]. Recall that [8] requires the polynomial map $F : \mathbb{A}^n \to \mathbb{A}^n$ to be polynomially invertible, with inverse $G := (G_1,\ldots,G_n)$ of degree $(nd)^{O(1)}$. Then the authors show that $G$ can be computed with $(Lnd)^{O(1)}$ operations. Under these conditions, we have that the projection map $\pi : V \to \mathbb{A}^n$ has degree 1, i.e., $D = 1$ holds. Furthermore, it is easy to see that the minimal polynomial $m_S(S,T)$ has degree bounded by $e := \max_{1\le k\le n}\deg G_k$, and the algorithms underlying Proposition 4.5 and 4.6 have actually complexity $L(nd)^{O(1)}$. This shows that our complexity result meets this polynomial bound under the much stronger hypotheses of [8].

## REFERENCES


[1] I. Shparlinski, *Computational and algorithmic problems in finite fields*, Dordrecht Boston London: Kluwer Academic Publishers, 1992.

[2] M.-D. Huang and Y.-C. Wong, "Solvability of systems of polynomial congruences modulo a large prime," *Comput. Complexity*, vol. 8, no. 3, pp. 227–257, 1999.

[3] M. Bardet, J.-C. Faugère and B. Salvy, "Complexity of Gröbner basis computation for Semi–regular Overdetermined sequences over $\mathbb{F}_2$ with solutions in $\mathbb{F}_2$," Rapport de Recherche INRIA RR–5049, 2003, http://www.inria.fr/rrrt/rr-5049.html.

[4] A. Cafure and G. Matera, "Fast computation of a rational point of a variety over a finite field," To appear in Math. Comput., available at www.arxiv.org/pdf/math.AG/0406085, 2005.

[5] M. Garey and D. Johnson, *Computers and Intractability: A Guide to the Theory of NP–Completeness*. San Francisco: Freeman, 1979.

[6] J. von zur Gathen, M. Karpinski, and I. Shparlinski, "Counting curves and their projections," *Comput. Complexity*, vol. 6, pp. 64–99, 1997.

[7] A. Cafure and G. Matera, "Improved explicit estimates on the number of solutions of equations over a finite field," To appear in Finite Fields Appl., available at www.arxiv.org/pdf/math.NT/0405302, 2005.

[8] C. Sturtivant and Z.-L. Zhang, "Efficiently inverting bijections given by straight line programs," in *Proc. FOCS'90*. IEEE, 1990, pp. 327–334.

[9] A. Kipnis and A. Shamir, "Cryptanalysis of the HFE Public Key Cryptosystem by relinearization," in *Proceedings CRYPTO'99*, ser. Lecture Notes in Comput. Sci., vol. 1666. Berlin: Springer, 1999, pp. 19–30.

[10] N. Courtois, A. Klimov, J. Patarin, and A. Shamir, "Efficient algorithms for solving overdefined systems of multivariate polynomial equations," in *EUROCRYPT 2000*, ser. Lecture Notes in Comput. Sci., B. Preneel, Ed., vol. 1807. Berlin: Springer, 2000, pp. 71–79.

[11] T. Matsumoto and H. Imai, "A class of asymmetric crypto-systems based on polynomials over finite rings," in *IEEE Intern. Symp. Inform. Theory, Abstracts of Papers*, 1983, pp. 131–132.

[12] C. Wolf and B. Preneel, "Taxonomy of public key schemes based on the problem of multivariate quadratic equations," Cryptology ePrint Archive, Report 2005/077, 2005, http://eprint.iacr.org/.

[13] J. Heintz, "Definability and fast quantifier elimination in algebraically closed fields," *Theoret. Comput. Sci.*, vol. 24, no. 3, pp. 239–277, 1983.

[14] D. Castro, M. Giusti, J. Heintz, G. Matera, and L. Pardo, "The hardness of polynomial equation solving," *Found. Comput. Math.*, vol. 3, no. 4, pp. 347–420, 2003.

[15] M. Giusti, K. Hägele, J. Heintz, J. Morais, J. Montaña, and L. Pardo, "Lower bounds for Diophantine approximation," *J. Pure Appl. Algebra*, vol. 117,118, pp. 277–317, 1997.

[16] L. Pardo and J. San Martín, "Deformation techniques to solve generalized Pham systems," *Theoret. Comput. Sci.*, vol. 315, 593–625, 2004.

[17] E. Kaltofen, "Effective Noether irreducibility forms and applications," *J. Comput. System Sci.*, vol. 50, no. 2, pp. 274–295, 1995.

[18] R. Lidl and H. Niederreiter, *Finite fields*. Addison–Wesley, 1983.

[19] J. von zur Gathen and J. Gerhard, *Modern computer algebra*. Cambridge: Cambridge Univ. Press, 1999.

[20] D. Bini and V. Pan, *Polynomial and matrix computations*, ser. Progress in Theoretical Computer Science. Boston: Birkhäuser, 1994.

[21] W. Baur and V. Strassen, "The complexity of partial derivatives," *Theoret. Comput. Sci.*, vol. 22, pp. 317–330, 1983.

[22] V. Pan, *Structured matrices and polynomials. Unified superfast algorithms*. Boston: Birkhäuser, 2001.

[23] M. Giusti, G. Lecerf, and B. Salvy, "A Gröbner free alternative for polynomial system solving," *J. Complexity*, vol. 17, pp. 154–211, 2001.