Last Fall Degree, HFE, and Weil Descent Attacks on ECDLP

Ming-Deh A. Huang[1], Michiel Kosters[2(✉)], and Sze Ling Yeo[3]

[1] USC, Los Angeles, California
mdhuang@usc.edu
[2] TL@NTU, Singapore, Singapore
kosters@gmail.com
[3] I2R, Singapore, Singapore
slyeo@i2r.a-star.edu.sg

Abstract. Weil descent methods have recently been applied to attack the Hidden Field Equation (HFE) public key systems and solve the elliptic curve discrete logarithm problem (ECDLP) in small characteristic. However the claims of quasi-polynomial time attacks on the HFE systems and the subexponential time algorithm for the ECDLP depend on various heuristic assumptions.

In this paper we introduce the notion of the last fall degree of a polynomial system, which is independent of choice of a monomial order. We then develop complexity bounds on solving polynomial systems based on this last fall degree.

We prove that HFE systems have a small last fall degree, by showing that one can do division with remainder after Weil descent. This allows us to solve HFE systems unconditionally in polynomial time if the degree of the defining polynomial and the cardinality of the base field are fixed. For the ECDLP over a finite field of characteristic 2, we provide computational evidence that raises doubt on the validity of the first fall degree assumption, which was widely adopted in earlier works and which promises sub-exponential algorithms for ECDLP. In addition, we construct a Weil descent system from a set of summation polynomials in which the first fall degree assumption is unlikely to hold. These examples suggest that greater care needs to be exercised when applying this heuristic assumption to arrive at complexity estimates.

These results taken together underscore the importance of rigorously bounding last fall degrees of Weil descent systems, which remains an interesting but challenging open problem.

Keywords: HFE · ECDLP · Weil descent · Solving equations · First fall degree · Last fall degree

R. Gennaro and M. Robshaw (Eds.): CRYPTO 2015, Part I, LNCS 9215, pp. 581–600, 2015.
DOI: 10.1007/978-3-662-47989-6_28

1 Introduction

1.1 Zero-Dimensional Polynomial Systems and Weil Descent Attacks

Zero-dimensional multivariate polynomial systems over finite fields arise in many practical areas of interest including in cryptography and coding theory. As such, solving these systems has both practical and theoretical interest. For instance, a major application is in the design of multivariate cryptosystems. One of the earliest proposals for the multivariate cryptosystem was the HFE public-key cryptosystem [21]. In recent years, polynomial solving also arises in elliptic curve cryptography, specifically in the index calculus approach to solve the elliptic curve discrete logarithm problem (ECDLP).

Many different approaches had been proposed to solve multivariate polynomial equations over finite fields. The most common approach for generic polynomial systems is via Gröbner basis algorithms [1,9,10]. Typically, a Gröbner basis with respect to the degree reverse lexicographical ordering is first computed via algorithms F_4 or F_5 [9,10]. It is then converted to a Gröbner basis with respect to the lexicographical ordering by algorithms such as the FGLM algorithm [11] which contains equations where variables are eliminated. This enables the variables to be solved one at a time. In general, it is very difficult to determine the complexity of the Gröbner basis algorithm. Various authors have used the term "the degree of regularity" to describe properties of a system that can be used to obtain complexity results. However not all definitions of this term are equivalent.

Another approach to solve multivariate polynomial systems is the XL algorithm and its variants [2–5,17]. This class of algorithms performs well when the system under consideration is overdetermined, that is, the number of equations far exceeds the number of variables.

In this present paper, we first introduce the notion of the last fall degree of a polynomial system over a finite field. Our definition is intrinsic to the polynomial system itself, independent of the choice of a monomial order. With this notion at our disposal, we present an explicit algorithm to find all the roots of a zero-dimensional multivariate polynomial system, bounding the complexity by the last fall degree.

When the polynomial systems are over a field of cardinality q^n, where q is a prime power and n a positive integer, one can convert this system via Weil descent to a system over its subfield with q elements (see Sect. 3 for more details). This results in a polynomial system over a smaller field, but at the expense of more variables. For example, Weil descent has been adopted to solve the HFE system as well as the index calculus method for ECDLP. In this paper, we will describe Weil descent systems arising from a polynomial in one variable and study the relations among various polynomial systems. Analogous definitions hold for a multivariate polynomial system.

1.2 The HFE Cryptosystem

Let k be a finite field of cardinality q^n, with subfield k' of cardinality q. Let $f \in k[X]$ be a polynomial over k with a relatively small degree. Using factorization

algorithms, one can easily factorize this polynomial to find its roots in k. One can transform this system using Weil descent and two transformations into a system in n variables over k'. At first glance, this system seems to be hard to solve and this is the basis of the Hidden Field Equations (HFE) cryptosystem (see [21] and Subsect. 4.1). Computational and heuristic evidence show that such a system is not secure [7,8,16]: the degree of regularity of a Weil descent systemis small and does not depend on n and hence the system can be solved efficiently using Gröbner basis algorithms. In particular in [16], the authors claimed that the HFE system can be solved efficiently under a heuristic assumption on the complexity of the Gröbner basis computations to solve the system. More recently, Christophe Petit, in a preprint [22], gives a proof of this observation by doing manipulations using his successive resultant algorithm on the descent side. In this article, we prove that HFE systems have a small last fall degree, by showing that one can do division with remainder after Weil descent. This allows us to solve the HFE systems unconditionally in polynomial time if the degree of the defining polynomial and the cardinality of the base field are fixed.

We have a natural right action of $\mathrm{Aff}_n(k') = k'^n \rtimes \mathrm{GL}_n(k')$ on the ring $R' = k'[Y_0, \ldots, Y_{n-1}]$ by acting as affine change of coordinates. If $M \in \mathrm{Aff}_n(k')$ and $g \in R'$ we write gM for this action. The main theorem is the following, which allows one to solve HFE systems efficiently. We stress that our results hold for a larger class of polynomial systems as we do not require the resulting Weil descent system to be quadratic.

For $r \in \mathbb{Z}_{\geq 0}$ and $c \in \mathbb{Z}_{\geq 1}$, we set

$$\psi(r, c) = \max\left(\lfloor 2(c-1)\left(\log_c(r) + 1\right)\rfloor, 0\right).$$

Main Theorem 1. *Let q be a prime power and let k be a finite field of cardinality q^n with subfield k' of cardinality q. Let $f \in k[X]$ nonzero which has at most e different roots over k and let $\mathcal{F} = \{f\}$. Let $\mathcal{F}'_f \subset k'[Y_0, \ldots, Y_{n-1}]$ be a Weil descent system of $\mathcal{F}$ (Subsect. 3.1). Let $M \in \mathrm{Aff}_n(k')$, $N \in \mathrm{GL}_n(k')$. Define g_i, $i = 0, \ldots, n-1$, by*

$$\begin{pmatrix} g_0 \\ \vdots \\ g_{n-1} \end{pmatrix} = N \begin{pmatrix} [f]_0 M \\ \vdots \\ [f]_{n-1} M \end{pmatrix}.$$

Set $d = \max(\psi(\deg(f), q), q, e)$. Then given $\mathcal{G} = \{g_0, \ldots, g_{n-1}, Y_0^q - Y_0, \ldots, Y_{n-1}^q - Y_{n-1}\} \subset k'[Y_0, \ldots, Y_{n-1}]$, one can deterministically find all solutions to $\mathcal{G}$ in time polynomial in $(n+d)^d$.

If one fixes q and $\deg(f)$, then the complexity to solve systems in Main Theorem 1 is polynomial in n. Note that $e \leq \deg(f)$, but usually it is much smaller. Furthermore, in practical applications, one wants e to be small, say bounded by a constant: in this case one can solve the above system in quasi-polynomial time if q is fixed and $\deg(f)$ grows like n^α.

It is an open question whether variants of HFE, such as HFEv-, can be attacked by our approach.

1.3 Polynomial Systems from ECDLP

A major application of solving multivariate polynomial equations over a finite field k of cardinality q^n is in the relation search step of the index calculus algorithm for elliptic curves over the field [6,14,23]. Indeed, let $E : y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6$, where $a_1, a_2, a_3, a_4, a_6 \in k$, be an elliptic curve defined over k. Let P be a point on E and let Q be a point in the cyclic group generated by P. The elliptic curve discrete logarithm problem seeks for an integer a such that $Q = aP$.

The most important step in the index calculus approach is to generate sufficiently many relations among suitable points on the elliptic curve E. To this end, summation polynomials provide a way to achieve this (see Subsect. 5.1). In particular, this transforms the problem of finding relations among points to solving a system of polynomial equations over k via the summation polynomials.

Cryptographic applications of Weil descent were first suggested by Frey [12], and Weil descent attacks were initially applied to elliptic curves of composite degrees over $\mathbb{F}_2$ [12,15]. In [6,14], Weil descent was exploited to solve the ECDLP by applying the Weil descent to the summation polynomials over k. In [6], for instance, sub-exponential time estimates via this Weil descent approach were obtained for certain classes of q and n. Here, the author relied on a geometric approach by Rojas to solve a Weil descent system.

In [23], Petit et al. studied Weil descent systems arising from polynomial systems over fields of characteristic 2. Their results are based on a certain heuristic assumption, called the first fall degree assumption, which asserts that the first fall degree of a polynomial system is close to the degree of regularity. More specifically, they obtained a sub-exponential time complexity of $2^{O(n^{2/3}\log n)}$ on the basis of this assumption.

In this article, we provide computational evidence that raises doubt on the validity of the first fall degree assumption when applied to elliptic curves over fields of characteristic 2. In addition, we construct a Weil descent system from a set of summation polynomials in which the first fall degree assumption is unlikely to hold. These examples suggest that greater care needs to be exercised when applying this heuristic assumption to arrive at complexity estimates.

1.4 Our Contributions

The contributions of this paper are three-fold.

– First, we introduce the notion of the last fall degree for a finite set of polynomials. Intuitively, this last fall degree determines the minimum degree at which operations on the generating polynomials need to be performed for all other polynomials to be generated. Our definition is intrinsic to the generating system and is independent of any monomial order. This allows us to provide an explicit and generic algorithm to find all the zeroes of a zero-dimensional set of polynomials whose time complexity depends on this last fall degree. While our approach may be similar to existing Gröbner basis algorithms, we stress

that we have developed a generic framework that applies to any multivariate zero-dimensional polynomial system with a time complexity dependent on a well-defined parameter.
- Second, we prove that the polynomials from the HFE system can be solved in polynomial time if the degree of the defining polynomial and the cardinality of the base field are fixed. Our proof is elementary and complete, without relying on any unproved assumptions or results. We do this by bounding the last fall degree of the zero-dimensional system and then exploit the aforementioned algorithm to solve the system. Besides, our proof works for any univariate polynomial $f(X)$ bounded by some degree in contrast to the original HFE system which restricts the monomials in $f(X)$ to be of a certain form. More importantly, our approach can be applied to analyze zero-dimensional polynomial systems of other types (see [20]).
- Finally, we consider an important application of solving a zero-dimensional multivariate polynomial system, namely in finding relations for index calculus algorithms to solve the elliptic curve discrete logarithm problem. Here, we revisit the first fall degree assumption adopted in [23] to derive a subexponential time estimate to solve the ECDLP. We illustrate two examples which raise some doubts on the correctness of this assumption on Weil descent systems arising from summation polynomials. From such examples, we believe that more evidence has to be presented before applying the first fall degree assumption to make complexity claims on the ECDLP.

1.5 Organization of the Paper

The rest of this article is organized as follows. We begin in Sect. 2 by defining a vector space of polynomials obtained with operations within a certain degree starting from a set of polynomials. We then use this set to define the notion of the last fall degree of a polynomial system. With these notions, we present an algorithm to find all the zeros of a zero-dimensional multivariate polynomial system over a finite field. Next in Sect. 3, we define the notion of a Weil descent system and of a fake Weil descent system arising from a system of univariate polynomials over a field of cardinality q^n and we discuss the relations between both systems. This is followed by our attack on the HFE system in Sect. 4. The main result in this section is Main Theorem 1. In the final section, we provide a brief discussion and some comments on Weil descent attacks on ECDLP.

2 Constructible Polynomials

Let k be a field and let $R = k[X_0, \ldots, X_{n-1}]$ be a polynomial ring. Let $\mathcal{F}$ be a finite subset of R and let $I \subseteq R$ be the ideal generated by $\mathcal{F}$. We set $\deg(\mathcal{F}) = \max(\deg(f) : \ f \in \mathcal{F})$.

Definition 1. *For $i \in \mathbb{Z}_{\geq 0}$, we let $V_{\mathcal{F},i}$ be the smallest k-vector space of R such that*

1. $\{f \in \mathcal{F} : \deg(f) \leq i\} \subseteq V_{\mathcal{F},i}$;
2. *if* $g \in V_{\mathcal{F},i}$ *and if* $h \in R$ *with* $\deg(hg) \leq i$, *then* $hg \in V_{\mathcal{F},i}$.

We set $V_{\mathcal{F},\infty} = I$. *For convenience, we set* $V_{\mathcal{F},-1} = \emptyset$. *If* $\mathcal{F}$ *is fixed, we often write* V_i *instead of* $V_{\mathcal{F},i}$.

Intuitively, V_i is the largest subset of I which can be constructed from $\mathcal{F}$ by doing ideal operations without exceeding degree i.

Note that V_i is a finite-dimensional k-vector space of dimension $\dim_k(V_i) \leq \binom{n+i}{i} \leq (n+i)^i$.

If $\mathcal{F}$ is fixed and $g_1, g_2 \in R$, then we write $g_1 \equiv_i g_2$ whenever $g_1 - g_2 \in V_i$. Note that for $h_1, h_2, h_3 \in R$ with $h_1 \equiv_r h_2$, one has

$$h_1 h_3 \equiv_{\max(r,\deg(h_1 h_3),\deg(h_2 h_3))} h_2 h_3.$$

We write $g_1 \equiv g_2$ if $g_1 - g_2 \in I$.

Definition 2. *Let* $\mathcal{F}$ *be a finite subset of* R *and let* I *be the ideal generated by* $\mathcal{F}$. *The minimal* $c \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$ *such that for all* $f \in I$ *one has* $f \in V_{\max(c,\deg(f))}$, *is called the* last fall degree *of* $\mathcal{F}$, *and is denoted by* $d_{\mathcal{F}}$.

A monomial order $\leq$ on R is called degree refining if for monomials M, N with $\deg(M) < \deg(N)$, one has $M < N$.

Lemma 1. *The following hold:*

1. *One has* $d_{\mathcal{F}} \in \mathbb{Z}_{\geq 0}$.
2. *Let* $\mathcal{B}$ *be a Gröbner basis of* I *with respect to some degree refining monomial order on* R. *Then there is an integer* $c \in \mathbb{Z}_{\geq 0}$ *such that* $\mathcal{B} \subseteq V_{\mathcal{F},c}$ *and one has* $d_{\mathcal{F}} \leq c$.

Proof. Since (1) follows from (2), we will prove (2). Let $\{g_1, \ldots, g_s\}$ be a Gröbner basis of I with respect to some monomial order which refines the degree. Set c to be the minimal i such that $g_j \in V_i$ for all j. Let $f \in I$. Since $\mathcal{B}$ is a Gröbner basis of I with respect to a degree refining order, we can write $f = \sum_{i=1}^{s} a_i g_i$ with $\deg(a_i g_i) \leq \deg(f)$ for $i = 1, \ldots, s$. Then one easily finds $f \in V_{\max(\deg(f),c)}$.

Note that the bound c on $d_{\mathcal{F}}$ given in Lemma 1 is constructed with respect to a fixed monomial order. However, the last fall degree $d_{\mathcal{F}}$ is intrinsic to the set $\mathcal{F}$ and independent of the choice of a monomial order.

Let $\mathcal{G}$ be obtained from $\mathcal{F}$ through an invertible linear transformation of equations. Then one has $\max(d_{\mathcal{F}}, \deg(\mathcal{F})) = \max(d_{\mathcal{G}}, \deg(\mathcal{F}))$. Note that $\deg(\mathcal{F}) = \deg(\mathcal{G})$. Further, since any affine transformation of the variables $X_0, \ldots, X_{m-1}$ is degree-preserving, the last fall degree is invariant under such transformations. Finally, enlarging the field k does not change the last fall degree.

Remark 1. The name last fall degree has been chosen because there is a similar concept called the first fall degree, which is used to heuristically bound the complexity of Gröbner basis algorithms, see [23]. The *first fall degree* of a system

$\mathcal{F}$ is the smallest $d \geq \deg(\mathcal{F})$ such that there exists $g_f \in R$ for $f \in \mathcal{F}$ such that $d = \max_{f\in\mathcal{F}}(\deg(g_f f))$ and $\deg(\sum_{f\in\mathcal{F}} g_f f) < d$ and $\sum_{f\in\mathcal{F}} g_f f \neq 0$.

An equivalent definition of the last fall degree is the following: $d_{\mathcal{F}}$ is the largest $c \in \mathbb{Z}_{\geq 0}$ such that $V_c \cap R_{\leq c-1} \neq V_{c-1}$, where $R_{\leq c-1}$ denotes the set of all polynomials in R with degree less than or equal to $c-1$. This definition has the same flavour as the definition of the first fall degree. This equivalent definition of the last fall degree allows one to compute the last fall degree if an upper bound, for example from Lemma 1, is known. It would be of great interest to find a direct method for computing the last fall degree.

2.1 An Explicit Construction of V_i

Next, we describe an algorithm to construct V_i explicitly.

Let V be a finite-dimensional k-vector subspace of $k[X_0, \ldots, X_{n-1}]$. We say that B is a reduced basis of V if B is a basis of V and for all $h = \sum_{g\in B} a_g g, a_g \in k$, we have $\deg(h) = \max_{g\in B} \deg(a_g g)$. For instance, a reduced basis can be constructed if we order the monomials with respect to their degrees and apply linear algebra operations to obtain a basis with different leading monomials.

Fix an integer $i \geq 0$ and let $\mathcal{F} = \{f_1, \ldots, f_r\} \subset k[X_0, \ldots, X_{n-1}]$. We construct V_i inductively as follows.

Let W_0 be the k-linear span of $\{f_j : j = 1, \ldots, r, \deg(f_j) \leq i\}$. By linear algebra operations, construct a reduced basis B_0 of W_0. For $j = 1, 2, \ldots$, define $W_j = \mathrm{Span}_k\{tg : g \in B_{j-1}, t \text{ is a monomial and } \deg(tg) \leq i\}$. Construct a reduced basis B_j of W_j from using linear algebra. Note that W_j contains W_{j-1}. Since $W_0 \subseteq W_1 \subseteq \ldots \subseteq V_i$, this process must terminate and we conclude that there exists some l such that $W_l = W_{l+1}$.

We claim that $W_l = V_i$. Suppose not. Then there must exist some $g \in W_l$ and $h \in k[X_0, \ldots, X_{n-1}]$ such that $gh \notin W_l$ and $\deg(gh) \leq i$. Let $B_l = \{g_1, \ldots, g_s\}$ be a reduced basis of W_l. Then one has $g = a_1 g_1 + a_2 g_2 + \ldots + a_s g_s$ with $a_1, a_2, \ldots, a_s \in k$. Since B_l is a reduced basis of W_l, $\max_j(\deg(a_j g_j)) = \deg(g)$. Hence, $gh = \sum_j g a_j g_j$ and $\max_j(g a_j g_j) \leq i$ so that $W_{l+1} \neq W_l$.

Assume k is a finite field of cardinality q. Since l is bounded by $(n+i)^i$, it follows from the above arguments that one can compute V_i in time polynomial in $r, \log(q)$ and $(n+i)^i$. Furthermore, using linear algebra, one can determine if a polynomial f with $\deg(f) \leq i$ lies in V_i with the same time bound.

2.2 Solving a Zero-Dimensional Polynomial System

Consider a system of r multivariate polynomial equations over a field k of cardinality q, namely, $f_1 = f_2 = \ldots = f_r = 0$ in n variables $X_0, X_1, \ldots, X_{n-1}$. Suppose that the algebraic set defined by this system is zero-dimensional, that is, there are finitely many solutions over an algebraic closure $\overline{k}$ of k. The next proposition gives a generic approach to solve the system via the above construction of V_i.

Proposition 1. *Let k be a finite field of cardinality q. Let $\mathcal{F} \subset R$ be a finite subset and let I be the ideal generated by $\mathcal{F}$. Assume that I is radical and that the system has at most e solutions over $\overline{k}$. Set $d = \max(d_{\mathcal{F}}, e)$. Then one can find all solutions of I in k*

- *probabilistically in time polynomial in the input size of $\mathcal{F}$, $\log(q)$ and $(n+d)^d$;*
- *deterministically in time polynomial in the input size of $\mathcal{F}$, q and $(n+d)^d$.*

Proof. First, note that one can factor a polynomial of degree s over k deterministically in time polynomial in q and s, and probabilistically in time polynomial in $\log(q)$ and s [13].

Compute V_d in time polynomial in the input size of $\mathcal{F}$, $\log(q)$ and $(n+d)^d$ (Subsect. 2.1).

Assume that all solutions over $\overline{k}$ of the system are

$$(a_{0,0}, \ldots, a_{0,n-1}), \ldots, (a_{t,0}, \ldots, a_{t,n-1}) \in \overline{k}^n$$

with $t < e$. Since I is a radical ideal, by the Nullstellensatz and Galois theory, one has

$$h_0 = \prod_{a \in \{a_{i,0}:\ i=0,\ldots,t\}} (X_0 - a) \in I.$$

Using linear algebra, one can find h_0 as the nonzero polynomial of minimal degree d_0 in $V_d \cap \mathrm{Span}_k\{1, X_0, \ldots, X_0^e\}$. Factor h_0. Assume that a_0 is a root of h_0 in k. We will find all solutions over k with $X_0 = a_0$. Set $h_0' = h_0/(X_0 - a_0)$ of degree $d_0 - 1$. By the Nullstellensatz and Galois theory, one has

$$h_1 = h_0' \prod_{a \in \{a_{i,1}:\ i=0,\ldots,t,\ a_{i,0}=a_0\}} (X_1 - a) \in I.$$

Using linear algebra, one finds h_1 as the polynomial of minimal degree d_1 in $V_d \cap \mathrm{Span}_k\{h_0', X_1 h_0', \ldots, X_1^{e-d_0+1} h_0'\}$. Factor h_1/h_0' over k. Pick a solution a_1 over k and find all solutions with $X_0 = a_0$, $X_1 = a_1$ using the similar recursive procedure. Hence one can find all solutions over k as required.

Remark 2. See [20] for a comparison between our approach for solving systems, MutantXL and Gröbner basis algorithms.

3 Weil Descent

Let q be a prime power. Let $n \in \mathbb{Z}_{\geq 1}$ and let k be a finite field of cardinality q^n with subfield k' of cardinality q. Let $\mathcal{F}$ be a finite subset of $k[X]$. In this section, we introduce a Weil descent system of $\mathcal{F}$, which is a system in $k'[Y_0, \ldots, Y_{n-1}]$. Furthermore, we introduce the fake Weil descent system of $\mathcal{F}$, which is a system in $k[X_0, \ldots, X_{n-1}]$. The analysis in this section can be easily extended to m variables for any positive integer m (see Remark 3).

Let $\mathcal{F} \subset k[X]$ be a finite set of polynomials. Suppose we want to find the common zeros of these polynomials in k. Let I be the ideal generated by

$$\mathcal{F}_f = \mathcal{F} \cup \{X^{q^n} - X\}.$$

3.1 Weil Descent

Let $\alpha_0, \ldots, \alpha_{n-1}$ be a basis of k/k'. Write $X = \sum_{i=0}^{n-1} \alpha_i Y_i$ and for $f \in k[X]$, define $[f]_j \in k'[Y_0, \ldots, Y_{n-1}]$ by

$$f(\sum_{j=0}^{n-1} \alpha_j Y_j) \equiv \sum_{j=0}^{n} [f]_j \alpha_j \pmod{Y_0^q - Y_0, \ldots, Y_{n-1}^q - Y_{n-1}}$$

where $[f]_j \in k'[Y_0, \ldots, Y_{n-1}]$ is chosen of minimal degree, that is, $\deg_{Y_i}([f]_j) < q$. Consider the systems

$$\mathcal{F}' = \{[f]_j : f \in \mathcal{F},\ j = 0, \ldots, n-1\}$$

and

$$\mathcal{F}'_f = \{[f]_j : f \in \mathcal{F},\ j = 0, \ldots, n-1\} \cup \{Y_i^q - Y_i : i = 0, \ldots, n-1\}.$$

The latter is called a Weil descent system of $\mathcal{F}$. Notice that the ideal generated by $\mathcal{F}'_f$ is always a radical ideal, as $k'[Y_0, \ldots, Y_{n-1}]/(Y_i^q - Y_i : i = 0, \ldots, n-1)$ is isomorphic to a product of fields (Chinese remainder theorem). One easily sees that solutions of $\mathcal{F}$ or $\mathcal{F}_f$ in k correspond to solutions of $\mathcal{F}'$ or $\mathcal{F}'_f$ over k'.

A different choice of α_i merely results in a linear change of the variables Y_i and the polynomials $[f]_i$. An interesting choice for the α_i is a normal basis, that is, a basis with $\alpha_i = \theta^{q^i}$ for some $\theta \in k$.

3.2 Fake Weil Descent

To study the complexity of solving a Weil descent system, we relate a Weil descent system to another system in $k[X_0, \ldots, X_{n-1}]$, which we refer to as the fake Weil descent system.

Let $R = k[X_0, \ldots, X_{n-1}]$. Let $e \in \mathbb{Z}_{\geq 0}$. Let $X^{e'}$ be the remainder of division of X^e by $X^{q^n} - X$ in $k[X]$. Write $e' = \sum_{j=0}^{n-1} e'_j q^j$ in base q with $e'_j \in \{0, 1, \ldots, q-1\}$. We set

$$\overline{X^e} = X_0^{e'_0} \cdots X_{n-1}^{e'_{n-1}} \in R.$$

We extend this definition k-linearly for all polynomials in R. This gives a map $^-$: $k[X] \to R$. We set, where by convention $X_n = X_0$,

$$\overline{\mathcal{F}} = \{\overline{f} : f \in \mathcal{F}\}$$

and

$$\overline{\mathcal{F}}_f = \{\overline{f} : f \in \mathcal{F}\} \cup \{X_0^q - X_1, \ldots, X_{n-1}^q - X_n\}.$$

We let $\overline{I}$ be the ideal generated by $\overline{\mathcal{F}}_f$. We call $\overline{\mathcal{F}}_f$ the fake Weil descent system of $\mathcal{F}$. Note that $\overline{I}$ is a radical ideal. Indeed the k-algebra morphism

$R/(X_0^q - X_1, \ldots, X_{n-1}^q - X_n) \to k[X_0]/(X_0^{q^n} - X_0)$ which sends X_i to $X_0^{q^i}$ is an isomorphism, because it is a surjective morphism on k-vector spaces of the same dimension. The latter ring is isomorphic to k^k by the Chinese remainder theorem. In the ring k^k all ideals are radical.

There is a bijection between the set of solutions of I and those of $\overline{I}$ over k (or $\overline{k}$). If $X = a \in \overline{k}$ is a zero of I, then $(X_0, \ldots, X_{n-1}) = (a, a^q, \ldots, a^{q^{n-1}})$ is a zero of $\overline{I}$. Conversely, if $(X_0, \ldots, X_{n-1}) = (a_0, \ldots, a_{n-1})$ is a solution of $\overline{I}$, then $X = a_0$ is a solution of I.

We will now prove a couple of lemmas which will be useful later.

Lemma 2. *Let $h_1, h_2 \in R$, $g \in k[X]$. One has, where $\equiv_i$ is defined with respect to $\overline{\mathcal{F}}_f$:*

1. $\overline{h_1 + h_2} \equiv_{\max(\deg(\overline{h_1}), \deg(\overline{h_2}))} \overline{h_1} + \overline{h_2}$;
2. $\overline{h_1} \cdot \overline{h_2} \equiv_{\deg(\overline{h_1}) + \deg(\overline{h_2})} \overline{h_1 h_2}$;
3. *There is $h_3 \in k[X]$ with $\deg(h_3) < q^n$ such that $g \equiv_{\deg(g)} \overline{h_3}$.*

Proof. One reduces to the case of monomials and the result then follows easily.

We have a morphism of k-algebras $\varphi : R \to k[X]$ which maps X_i to X^{q^i}. This map has the following properties.

Lemma 3. *Let $h \in k[X]$. The following statements hold:*

1. $\varphi(\overline{h}) \equiv h \pmod{X^{q^n} - X}$;
2. *$h \in I$ if and only if $\overline{h} \in \overline{I}$.*

Proof. 1: Follows directly.

2: Let $h \in I$. We will show $\overline{h} \in \overline{I}$. One can write $h = b(X^{q^n} - X) + \sum_{f \in \mathcal{F}} a_f f$. Modulo $\overline{I}$ we find with Lemma 2:

$$\overline{h} = \overline{b(X^{q^n} - X) + \sum_{f \in \mathcal{F}} a_f f} \equiv \overline{b}(X_0 - X_0) + \sum_{f \in \mathcal{F}} \overline{a_f}\,\overline{f} \equiv 0.$$

Conversely, let $h \in k[X]$ and assume $\overline{h} \in \overline{I}$. Write $\overline{h} = \sum_{j=0}^{n-1} c_j(X_j^q - X_{j+1}) + \sum_{f \in \mathcal{F}} b_f \overline{f}$. One finds, using 1,

$$\begin{aligned}\varphi(\overline{h}) &= \sum_{j=0}^{n-1} \varphi(c_j)\varphi(X_j^q - X_{j+1}) + \sum_{f \in \mathcal{F}} \varphi(b_f)\varphi(\overline{f}) \\ &\equiv \varphi(c_{n-1})(X^{q^n} - X) + \sum_{f \in \mathcal{F}} \varphi(b_f) f \pmod{X^{q^n} - X}.\end{aligned}$$

We conclude $\varphi(\overline{h}) \in I$.

3.3 Summary of Notation

Let us recall some notation we have introduced thus far. Let $\mathcal{F} \subset k[X]$ be a finite subset, where k is a finite field of cardinality q^n and let k' be its subfield of cardinality q with an implicit choice of basis of k over k'. We let I be the ideal generated by

$$\mathcal{F}_f = \mathcal{F} \cup \{X^{q^n} - X\}.$$

We have systems in $k'[Y_0, \ldots, Y_{n-1}]$ defined by

$$\mathcal{F}' = \{[f]_j : f \in \mathcal{F},\ j = 0, \ldots, n-1\}$$

and a Weil descent system

$$\mathcal{F}'_f = \{[f]_j : f \in \mathcal{F},\ j = 0, \ldots, n-1\} \cup \{Y_i^q - Y_i : i = 0, \ldots, n-1\}.$$

Finally, we have systems in $k[X_0, \ldots, X_{n-1}]$ defined by

$$\overline{\mathcal{F}} = \{\overline{f} : f \in \mathcal{F}\}$$

and the fake Weil descent system

$$\overline{\mathcal{F}}_f = \{\overline{f} : f \in \mathcal{F}\} \cup \{X_0^q - X_1, \ldots, X_{n-1}^q - X_n\}.$$

We let $\overline{I}$ be the ideal generated by $\overline{\mathcal{F}}_f$.

3.4 Relating Both Types of Descent

This subsection seeks to connect the last fall degrees of a Weil descent system and the fake Weil descent system presented in Subsects. 3.1 and 3.2. We follow the formulation in [16] which essentially shows that the two systems are linked by suitable transformations. We have the following result.

Proposition 2. *One has*

$$\max(d_{\mathcal{F}'_f}, q, \deg(\mathcal{F}')) \leq \max(d_{\overline{\mathcal{F}}_f}, q, \deg(\mathcal{F}')).$$

Proof (Sketch). We follow [16]. The details can be found in [20]. One has $\deg(\mathcal{F}') = \deg(\overline{\mathcal{F}})$. After a linear change, we may assume that a Weil descent in $\mathcal{F}'$ is with respect to a normal basis $\{\theta^{q^i} : i = 0, \ldots, n-1\}$. Consider the system $\mathcal{F}' \subseteq k[Y_0, \ldots, Y_{n-1}]$, which has the same last fall degree as considered over k'. Using some linear changes of the polynomials and linear changes of variables as in Sect. 4 of [16], we obtain the system $\mathcal{F}'' = \{\overline{f}, \overline{f^q}, \ldots, \overline{f^{q^{n-1}}} : f \in \mathcal{F}\} \cup \{Y_0^q - Y_1, \ldots, Y_{n-1}^q - Y_n\}$. One has

$$\max(d_{\mathcal{F}'_f}, q, \deg(\mathcal{F}')) = \max(d_{\mathcal{F}''}, q, \deg(\mathcal{F}')).$$

Note that $\overline{\mathcal{F}} \subseteq \mathcal{F}''$ and that both sets generate the same ideal (Lemma 2(2)). Hence the result follows.

Remark 3. In this section, we have presented a Weil descent system and its related fake Weil descent system corresponding to a polynomial system in one variable X over k. This definition can be easily extended to a system of r polynomials in m variables over k such that each variable corresponds to n descent variables. This gives rise to rn polynomials in mn variables and all the results follow accordingly.

4 Solving the HFE System

In this section, our primary goal is to prove that the HFE system and its variants can be solved efficiently by employing the tools we have developed so far. Although such results were shown previously (see for example [16]), their proofs were based on some heuristics. Our proof, on the other hand, is rigorous and free from any unproven conjecture or heuristics. Another claim for a proof can be found in [22].

We begin by reviewing the general description of the HFE system. Throughout this section, k will denote a field of cardinality q^n, while k' will denote its subfield of cardinality q.

4.1 Description of the HFE Encryption

The HFE public key cryptosystem was first introduced by Patarin [21]. Briefly, let $f(X)$ be a univariate polynomial in $k[X]$ with degree bounded by q^t. In practice, the nonconstant monomials in f are chosen to be either of the form $X^{q^i+q^j}$ or X^{q^i} for integers $i, j \geq 0$. However, we will remove this restriction in this paper and allow f to be an arbitrary polynomial with degree bounded by q^t.

Let $\mathcal{F} = \{f\} \subset k[X]$ and consider the Weil descent system

$$\mathcal{F}'_f = \{[f]_0, \ldots, [f]_{n-1}\} \cup \{Y_i^q - Y_i : i = 0, \ldots, n-1\} \subseteq k'[Y_0, \ldots, Y_{n-1}]$$

as in Subsect. 3.1 with respect to some basis of k/k'. We have a natural right action of $\mathrm{Aff}_n(k')$ on $R' = k'[Y_0, \ldots, Y_{n-1}]$ by an affine transformation of variables. Let $M \in \mathrm{Aff}_n(k')$. For $g \in k'[Y_0, \ldots, Y_{n-1}]$, we write gM for this action. Let $N \in \mathrm{GL}_n(k')$. Define

$$\begin{pmatrix} g_0 \\ \vdots \\ g_{n-1} \end{pmatrix} = N \begin{pmatrix} [f]_0 M \\ \vdots \\ [f]_{n-1} M \end{pmatrix}.$$

The public key of the system is the set of equations $\{g_0, g_1, \ldots, g_{n-1}\} \subset k'[Y_0, \ldots, Y_{n-1}]$ while the private key comprises f, the basis choice k/k' and the transformations M and N. To encrypt a message, $(m_0, m_1, \ldots, m_{n-1}) \in k'^n$, one computes

$$(c_0, \ldots, c_{n-1}) = (g_0(m_0, \ldots, m_{n-1}), \ldots, g_{n-1}(m_0, \ldots, m_{n-1})).$$

Using the private key and a factorization algorithm, one can find the message efficiently.

Let $\mathcal{G} = \{g_0 - c_0, \ldots, g_{n-1} - c_{n-1}\} \cup \{Y_i^q - Y_i : i = 0, 1, \ldots, n-1\}$. Observe that the message $(m_0, \ldots, m_{n-1})$ can be recovered if we can solve $\mathcal{G}$. This can be achieved deterministically via Proposition 1 in time polynomial in q and $(n+d)^d$, where d is bounded by the maximum of the last fall degree of $\mathcal{G}$ and the number of solutions e of $\mathcal{G}$. Notice that we are now in the situation of the main theorem (Main Theorem 1) which we now proceed to prove.

4.2 An Upper Bound on the Last Fall Degree

Let q be a prime power and let k be a finite field of cardinality q^n. Let $\mathcal{F} \subset k[X]$ be a finite set. Consider a fake Weil descent system $\overline{\mathcal{F}}_f$ to the subfield of cardinality q. Define $\equiv_j$ with respect to $\overline{\mathcal{F}}_f$. For $e \in \mathbb{Z}_{\geq 0}$ with $e = \sum_i a_i q^i$ in base q, we set $w(e) = \sum_i a_i$. For $f = \sum_i b_i X^i$, we set $w(f) = \max(w(i) : b_i \neq 0)$. Note that $w(f) \leq \deg(f)$, with equality if $\deg(f) < q^n$.

We start with a technical lemma. Recall the following. For $r \in \mathbb{Z}_{\geq 0}$ and $c \in \mathbb{Z}_{\geq 1}$, we set

$$\psi(r, c) = \max\left(\lfloor 2(c-1)\left(\log_c(r) + 1\right)\rfloor, 0\right).$$

Let $g \in k[X] \setminus k$. Then one has

$$\deg(\overline{g}) \leq (q-1)\left(\log_q(\deg(g)) + 1\right).$$

It follows that $\deg(\overline{g}) \leq \psi(\deg(g), q)/2$.

Lemma 4. *Let $h_2 \in k[X]$ nonzero of degree d. Set $u = \psi(d, q)$. Assume $\overline{h_2} \equiv_u 0$. Let $h_1 \in k[X]$. Let h_3 be the remainder of division of h_1 by h_2. Then one has $\overline{h_1} \equiv_{\max(u, w(h_1))} \overline{h_3}$.*

Proof. If $d = 0$, the result follows easily. Assume $d > 0$.

Fix h_2 and write $h_2 = \sum_{i=0}^{d} b_i X^i$ where $b_d \neq 0$. Since taking remainders is additive, it suffices to prove the result for $h_1 = X^e$. Let r_e be the remainder of division of X^e by h_2. For $g \in k[X]$ with $\deg(g) \leq d$, one has $\deg(\overline{g}) \leq u/2$. In particular, we have $\deg(\overline{r_e}) \leq u/2$.

We will prove the following statements successively:

1. for $e \in \{0, 1, \ldots, qd-1\}$, we have $\overline{X^e} \equiv_u \overline{r_e}$;
2. if $e, e' \in \mathbb{Z}_{\geq 0}$ satisfy $w(e) + w(e') \leq u$, $\overline{X^e} \equiv_u \overline{r_e}$ and $\overline{X^{e'}} \equiv_u \overline{r_{e'}}$, then $\overline{X^{e+e'}} \equiv_u \overline{r_{e+e'}}$;
3. for $e \in \mathbb{Z}_{\geq 0}$ with $w(e) \leq u$, we have $\overline{X^e} \equiv_u \overline{r_e}$;
4. for all $e \in \mathbb{Z}_{\geq 0}$ one has $\overline{X^e} \equiv_{\max(u, w(e))} \overline{r_e}$.

1: For $e = 0, \ldots, d-1$, the remainder is X^e itself and the result follows. One has $r_d = \frac{-1}{b_d} \sum_{i=0}^{d-1} b_i X^i$ and this gives $\overline{X^d} \equiv_u \overline{r_d}$. We continue by induction. Assume the statement holds for cases smaller than e and that $e \leq qd - 1$. We will prove the statement for e. Write $r_{e-1} = \sum_{j=0}^{d-1} c_j X^j$. Note that r_e is the

remainder of division of Xr_{e-1} by h_2, which gives $r_e = \sum_{j=0}^{d-1} c_j r_{j+1}$. Note that $e-1 \leq qd-2 = q^{\log_q(d)+1}-2$. Hence we have (as $d>0$):

$$\begin{aligned}\deg(\overline{X}) + \deg(\overline{X^{e-1}}) &\leq 1 + \lfloor (q-1)\left(\log_q(d)+2\right) - 1 \rfloor \\ &= \lfloor (q-1)\left(\log_q(d)+2\right) \rfloor \leq u.\end{aligned}$$

Using Lemma 2 and the induction hypothesis, we find

$$\overline{X^e} \equiv_u \overline{X} \cdot \overline{X^{e-1}} \equiv_u \overline{X} \cdot \overline{r_{e-1}} \equiv_u \overline{\sum_{j=0}^{d-1} c_j X^{j+1}} \equiv_u \overline{\sum_{j=0}^{d-1} c_j r_{j+1}},$$

and this gives the required remainder.

2: Assume without loss of generality that $w(e') \leq u/2$. Then one has $u \geq \max(w(e)+w(e'), \deg(\overline{r_e})+w(e'), \deg(\overline{r_e})+\deg(\overline{r_{e'}}))$ and one has $\deg(r_e r_{e'}) \leq 2d-2 \leq qd-1$. Lemma 1 and 2 give

$$\overline{X^{e+e'}} \equiv_u \overline{X^e} \cdot \overline{X^{e'}} \equiv_u \overline{r_e} \cdot \overline{X^{e'}} \equiv_u \overline{r_e} \cdot \overline{r_{e'}} \equiv_u \overline{r_e r_{e'}} \equiv_u \overline{r_{e+e'}}.$$

3: Using 2 and induction, we easily reduce to the case where $e = q^i$, $i \geq 0$. Note that for $i \geq 1$, $q^i = q \cdot q^{i-1}$ and that $u \geq q$. We can then apply 2 and the proof follows by induction.

4: We prove this statement by induction on $w(e) > u$. Write $e = e_1 + e_2$ with $u \leq w(e_1) < w(e)$, and $w(e_1) + w(e_2) = w(e)$. One has (Lemma 2 and part 3)

$$\begin{aligned}\overline{X^e} &\equiv_{\max(u,w(e))} \overline{X^{e_1}} \cdot \overline{X^{e_2}} \equiv_{\max(u,w(e))} \overline{r_{e_1}} \cdot \overline{X^{e_2}} \\ &\equiv_{\max(u,w(e))} \overline{r_{e_1}} \cdot \overline{r_{e_2}} \equiv_{\max(u,w(e))} \overline{r_e}.\end{aligned}$$

Proposition 3. *Assume $\mathcal{F} = \{f\}$ with $f \in k[X]$ nonzero. Set $u = \psi(\deg(f), q)$ and set $g = \gcd(f, X^{q^n} - X)$. Then we have $\overline{g} \in V_u$.*

Proof. Let f_1 be the remainder of division of $X^{q^n} - X$ by f. By Lemma 4, we have $\overline{f_1} \equiv_u 0$. Let f_2 be the remainder of division of f by f_1. Similarly, we find $\overline{f_2} \equiv_u 0$. Hence we can follow the Euclidean algorithm and we obtain $\overline{g} \in V_u$.

4.3 Proof of the Main Theorem

We can finally prove Main Theorem 1.

Proof. [of Main Theorem 1] We first study the last fall degree of $\mathcal{G}$. One has (Proposition 2)

$$d_{\mathcal{G}} \leq \max(d_{\mathcal{G}}, q, \deg(\mathcal{F}')) = \max(d_{\mathcal{F}'_f}, q, \deg(\mathcal{F}')) \leq \max(d_{\overline{\mathcal{F}}_f}, q, \deg(\mathcal{F}')).$$

Hence we study the last fall degree of $\overline{\mathcal{F}}_f$. Set $g = \gcd(f, X^{q^n} - X)$. From Proposition 3, we have $\overline{g} \in V_u$ with $u = \psi(\deg(f), q)$.

Let $h \in \overline{I}$, the ideal generated by $\overline{\mathcal{F}}_f$. Define the relations $\equiv_i$ with respect to $\overline{\mathcal{F}}_f$. By Lemma 2(3), one has $h \equiv_{\deg(h)} \overline{h_2}$ for some $h_2 \in k[X]$ with $\deg(h_2) < q^n$.

Since $\overline{h_2} \in \overline{I}$, it follows from Lemma 3(2) that $h_2 \in I$. Hence h_2 has remainder 0 when divided by g. From Lemma 4, we conclude (as $\deg(\overline{h_2}) \leq \deg(h)$),

$$h \equiv_{\max(\deg(h),u)} \overline{h_2} \equiv_{\max(\deg(h),u)} 0.$$

This shows $d_{\overline{\mathcal{F}}} \leq u$. Hence one finds, as $\deg(\mathcal{F}') \leq u$,

$$d_{\mathcal{G}} \leq \max(d_{\overline{\mathcal{F}}_f}, q, \deg(\mathcal{F}')) \leq \max(u, q, \deg(\mathcal{F}')) = \max(u, q).$$

Notice that $u \geq q$. Apply Proposition 1 to solve the system $\mathcal{G}$ in the required time.

5 Weil Descent Attacks on ECDLP

5.1 ECDLP and Summation Polynomials

Let E be an elliptic curve over a field k of cardinality q^n and let k' be its subfield of cardinality q. One possible approach to solve the elliptic curve discrete logarithm problem (ECDLP) is via the index calculus method. Essentially, sufficiently many relations between k-points on the curve E need to be generated and the time to construct such relations has a direct impact on the complexity of the entire index calculus approach.

In [6,24], summation polynomials were used to find relations between points on the curve. Here, we recall the definition of a summation polynomial.

Let F be a field. Let $A = (a_1, a_2, a_3, a_4, a_6) \in F^5$. Set

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= a_1 a_3 + 2a_4, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 + 4a_2 a_6 - a_4^2. \end{aligned}$$

We define

$$S_{A,2} = X_0 - X_1 \in F[X_0, X_1].$$

We define the third summation polynomial $S_{A,3} \in F[X_0, X_1, X_2]$ of degree 4 by:

$$\begin{aligned} S_{A,3} = &(X_0^2 X_1^2 + X_0^2 X_2^2 + X_1^2 X_2^2) - 2 \cdot (X_0^2 X_1 X_2 + X_0 X_1^2 X_2 + X_0 X_1 X_2^2) \\ &- b_2 \cdot (X_0 X_1 X_2) - b_4 \cdot (X_0 X_1 + X_0 X_2 + X_1 X_2) - b_6 \cdot (X_0 + X_1 + X_2) - b_8. \end{aligned}$$

We will quite often write S_A instead of $S_{A,3}$. For $r \in \mathbb{Z}_{>3}$, we recursively define the rth summation polynomial by

$$S_{A,r} = \mathrm{Res}_X \left(S_{A,r-1}(X_0, \ldots, X_{r-3}, X), S_{A,3}(X_{r-2}, X_{r-1}, X) \right) \in F[X_0, \ldots, X_{r-1}],$$

where Res_X denotes the resultant with respect to X.

We have the following proposition.

Proposition 4. *Let F be a field and let E/F be an elliptic curve given by $Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$. Let $r \in \mathbb{Z}_{\geq 2}$ and let $x_0, \ldots, x_{r-1} \in \overline{F}$. Then there are $P_0, \ldots, P_{r-1} \in E(\overline{F}) \setminus \{0\}$ with $x(P_i) = x_i$ $(i = 0, \ldots, r-1)$ such that $P_0 + \ldots + P_{r-1} = 0$ if and only if $S_{(a_1,a_2,a_3,a_4,a_6),r}(x_0, \ldots, x_{r-1}) = 0$.*

It follows that given a point $Q \neq 0$ and a positive integer m, we can represent a point Q as a sum of m points by solving $S_{m+1}(x(Q), X_0, \ldots, X_{m-1}) = 0$.

Assume that $F = k$. Further linear constraints were introduced so as to restrict the X_i's to a subspace V of k of dimension n' over k'. Let $L(X) \in k[X^q] \subset k[X]$ be the additive polynomial whose roots are precisely the elements of the subspace V. We obtain a system $\mathcal{F}$ of equations in $k[X_0, \ldots, X_{m-1}]$, namely,

$$\mathcal{F} = \{S_{m+1}(x(Q), X_0, \ldots, X_{m-1}), L(X_0), L(X_1), \ldots, L(X_{m-1})\}.$$

Using this set-up and Weil descent (Remark 3), Diem showed that there exist sub-exponential time index calculus algorithms for ECDLP for some families of q and n.

The authors of [23] adopted a similar approach and considered ECDLP for $q = 2^n$. To solve the system $\mathcal{F}$, they considered a Weil descent system $\mathcal{F}'$ over $\mathbb{F}_2$ (notation as in Subsect. 3.1). With $m = O(n^{1/3})$, the authors claimed that this system can be solved via Gröbner basis algorithms in sub-exponential time of $2^{O(n^{2/3} \log n)}$. Essentially, their claim was based on the so-called "first fall degree assumption" which asserts that the first fall degree (see Remark 1) of a Weil descent polynomial system is close to the degree of regularity, the largest degree reached during Gröbner basis computations. More precisely, as the first fall degree of this system is $O(m^2)$, they conjectured that the degree of regularity is $O(m^2)$ as well, thereby giving their heuristic result. According to the authors, they justified this heuristic assumption based on the following:

- The assumption of a constant gap between the first fall degree and the degree of regularity is widely believed to hold for Weil descent systems arising from HFE systems;
- The assumption is verified with experimental data for some multivariate polynomial systems for small parameters of n and m.

5.2 Discussion on the First Fall Degree Assumption

Here, we wish to highlight some examples where the first fall degree assumption is unlikely to hold.

One Bivariate Summation Polynomial. Let k be a finite field of cardinality 2^n. Let E/k be a random elliptic curve in Weierstrass form with a random nonzero point $Q \in E(k)$. The following table records the degree of regularity for a Weil descent system comprising the bivariate polynomial $S_3(X_0, X_1, x(Q))$. Following the formulation in [23], we include linear constraints on X_0 and X_1 to

restrict their values to be in a random $\mathbb{F}_2$-subspace of k with dimension $\lceil n/2 \rceil$. Note that in this case, a Weil descent system $\mathcal{F}'$, after eliminating variables using the linear constraints, is a system in about n variables and has about n quadratic equations together with field equations of the form $Y_i^2 + Y_i$. We performed our computations using the "GroebnerBasis()" function in the Magma computer Algebra System and the degree of regularity is read off as the largest step degree where new polynomials are generated while the first fall degree is the smallest step degree at which a new lower-degree polynomial is generated. Here, the last column in the table records the degree of regularity of a system of n random quadratic equations in n variables over $\mathbb{F}_2$ together with the n field equations. By a quadratic equation over $\mathbb{F}_2$, we mean an equation whose terms are a product of at most 2 variables.

n	First fall degree	Degree of regularity	Random
12	2	3	4
16	2	3	5
18	2	4	5
20	2	4	5
24	2	4	6
30	2	4	–
40	2	≥ 5	–

As the computations require more than 38 GB for $n = 40$, we are not able to carry out more experiments for larger values of n. However, the behaviour of the step degrees, another observable parameter from the Gröbner basis computations, suggests that the degree of regularity follows an increasing pattern as n increases. The above table raises doubt to the evidence of Assumption 2 from the article [23]: the gap between the degree of regularity and the first fall degree might be dependent on n.

Remark 4. Notice that our $n = 40$ computation did not terminate. After the submission of this paper, with the help of the Caramel team from Nancy (France), we managed to terminate similar computations: the degree of regularity does seem to increase. See [19] for the details. This paper also contains a proof that the first fall degree in general is 2.

Note that in all our computations, the first fall degree is 2. One can prove that this is almost always the case when E is ordinary ($a_1 \neq 0$) and Q is not the point of order 2. After some mathematics, the result follows from the following proposition where a complete proof can be found in [18, Chapter 7, Proposition 5.4]. The result is partially found in [25] as well.

Proposition 5. *Let E/k be an elliptic curve given by $Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$. Assume that E is ordinary ($a_1 \neq 0$). Then we have a*

surjective group morphism

$$\begin{aligned} E(k) &\to \mathbb{F}_2 \\ 0 &\mapsto 0 \\ P &\mapsto \mathrm{Tr}_{k/\mathbb{F}_2}\left(\frac{x(P)+a_2}{a_1^2}\right) \end{aligned}$$

with kernel $2E(k)$.

Note that knowledge of this map can speed up the summation polynomial approach for solving ECDLP, but probably only by a constant.

Multiple Summation Polynomials. Let k be a finite field of cardinality 2^n and let E/k be an elliptic curve. Let $Q \in E(k)$ be a nonzero point. Let $m \in \mathbb{Z}_{\geq 3}$. Instead of working with the $(m+1)$st summation polynomial, we consider the following sequence of m sums:

$$\begin{aligned} Q &= P_1 + Q_1, \\ Q_1 &= P_2 + Q_2, \\ &\dots \quad \dots \\ Q_{m-2} &= P_{m-1} + P_m. \end{aligned}$$

Observe that when this system is satisfied, we have $Q = P_1 + \ldots + P_m$.

Once again, we let the x-coordinates of P_i be restricted in some subspace of dimension $O(n/m)$. Consider the set

$$\mathcal{F} = \{S_3(x(Q), X_1, Y_1), \ldots, S_3(Y_{m-2}, X_{m-1}, X_m)\},$$

where the X_i's are restricted to the subspace and the Y_i are unrestricted. We perform Weil descent to obtain a system $\mathcal{F}'$ of equations in $\mathbb{F}_2$, where each equation has degree at most 3. According to [23], the first fall degree of this system is no greater than 5 (in fact, it is usually 2). Under the first fall degree assumption, this system will have a constant degree of regularity. In particular, it can be solved in time polynomial in m. Now, take $m = O(n)$. Letting the P_i's take some specific points, say $P_i = 2^i P, i = 1, \ldots, m$, this system will allow us to solve the ECDLP for a large proportion of points Q and thus, for all points Q. Consequently, we have a polynomial-time algorithm to solve ECDLP, which is highly improbable. We conclude that the first fall degree assumption is unlikely to hold for this system as well. In a similar way, using the first fall degree assumption, one can prove P=NP [19].

5.3 Open Problem on the Last Fall Degree

From the discussion in the preceding subsection, we believe that greater justification needs to be provided before one applies the first fall degree assumption to

a Weil descent system arising from a multivariate polynomial system. Nonetheless, as the above table demonstrates, the degree of regularity of a Weil descent system tends to grow more slowly than a random system with the same number of equations and variables. The big question is, how slowly does it grow. The slower it grows, the better algorithms there will be for ECDLP using Gröbner basis algorithms. As such, we believe that it remains worthwhile to analyze such systems in greater detail in order to get a more rigorous estimate to solve the ECDLP.

In this article, we defined the notion of a last fall degree of a multivariate polynomial system and describe an explicit algorithm to solve a zero-dimensional polynomial system whose time complexity depends on this last fall degree. As the last fall degree is independent of monomial orders, it enables us to give a rigorous bound on the time to solve a Weil descent system coming from univariate polynomials. We believe that this framework will be useful to help us investigate Weil descent systems from multivariate polynomials as well and will hopefully allow us to rigorously bound last fall degrees.

Remark 5. After submitting this paper, the authors continued their work in [20], and showed that the last fall degree of a Weil descent system arising from a zero-dimensional system also does not depend on the Weil descent parameter n. Unfortunately, the results of [20] do not apply to summation polynomials, because such systems are not zero-dimensional without adding field equations.

Acknowledgements. The authors would like to thank Bagus Santoso, Chaoping Xing and Yun Yang for their help and support in preparing this manuscript. We are grateful to Steven Galbraith and the anonymous reviewers for their valuable comments. Finally, we would like to thank the Caramel team from Nancy (France) for allowing us to use their computers to do experiments.

References

1. Buchberger, B.: Ein Algorithmus zum Auffffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. Ph.D. thesis, University of Innsbruck (1965)
2. Buchmann, J.A., Ding, J., Mohamed, M.S.E., Mohamed, W.S.A.E.: Mutantxl: solving multivariate polynomial equations for cryptanalysis. In: Handschuh, H., Lucks, S., Preneel, B., Rogaway, P. (eds.) Symmetric Cryptography (Dagstuhl, Germany, 2009). Dagstuhl Seminar Proceedings, vol. 09031. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, Germany (2009)
3. Courtois, N.T., Klimov, A.B., Patarin, J., Shamir, A.: Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 392–407. Springer, Heidelberg (2000)
4. Courtois, N.T., Pieprzyk, J.: Cryptanalysis of block ciphers with overdefined systems of equations. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 267–287. Springer, Heidelberg (2002)

5. Courtois, N.T., Patarin, J.: About the XL algorithm over $GF(2)$. In: Joye, M. (ed.) CT-RSA 2003. LNCS, vol. 2612, pp. 141–157. Springer, Heidelberg (2003)
6. Diem, C.: On the discrete logarithm problem in elliptic curves. Compositio Math. **147**, 75–104 (2011)
7. Ding, J., Hodges, T.J.: Inverting HFE systems is quasi-polynomial for all fields. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 724–742. Springer, Heidelberg (2011)
8. Faugère, J.-C., Joux, A.: Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 44–60. Springer, Heidelberg (2003)
9. Faugère, J.C.: A new efficient algorithm for computing Gröbner bases (F_4). J. Pure Appl. Algebra **139**, 61–88 (1999)
10. Faugère, J.C.: A new efficient algorithm for computing Gröbner bases without reduction to zero F_5. In: Proceedings of ISSAC, pp. 75–83. ACM Press (2002)
11. Faugère, J.C., Gianni, P.M., Lazard, D., Mora, T.: Efficient computation of zero-dimensional Gröbner bases by change of ordering. J. Symb. Comput. **16**(4), 329–344 (1993)
12. Galbraith, S.D., Smart, N.P.: A cryptographic application of Weil descent. In: Walker, M. (ed.) Cryptography and Coding 1999. LNCS, vol. 1746, pp. 191–200. Springer, Heidelberg (1999)
13. von zur Gathen, J., Panario, D.: Factoring polynomials over finite fields: a survey. J. Symbolic Comput. **31**(1–2), 3–17 (2001). Computational algebra and number theory, (1996)
14. Gaudry, P.: Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem. J. Symb. Comput. **44**(12), 1690–1702 (2009)
15. Gaudry, P., Hess, F., Smart, N.P.: Constructive and destructive facets of Weil descent on elliptic curves. J. Cryptology **15**(1), 19–46 (2002)
16. Granboulan, L., Joux, A., Stern, J.: Inverting HFE is quasipolynomial. In: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 345–356. Springer, Heidelberg (2006)
17. Kipnis, A., Shamir, A.: Cryptanalysis of the HFE public key cryptosystem by relinearization. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 19–30. Springer, Heidelberg (1999)
18. Kosters, M.: Groups and fields in arithmetic. Ph.D. thesis, Universiteit Leiden (2014)
19. Kosters, M., Yeo, S.L.: Notes on summation polynomials. Preprint (2015). http://arxiv.org/abs/1503.08001
20. Huang, M.-D.A., Kosters, M., Yang, Y., Yeo, S.L.: On the last fall degree of zero-dimensional Weil descent systems. Preprint (2015). http://arxiv.org/abs/1505.02532
21. Patarin, J.: Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of asymmetric algorithms. In: Maurer, U.M. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 33–48. Springer, Heidelberg (1996)
22. Petit, C.: Bounding HFE with SRA. Preprint (2013). http://www0.cs.ucl.ac.uk/staff/c.petit/files/SRA_GB.pdf
23. Petit, C., Quisquater, J.-J.: On polynomial systems arising from a Weil descent. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 451–466. Springer, Heidelberg (2012)
24. Semaev, I.: Summation polynomials and the discrete logarithm problem on elliptic curves. Preprint (2004). https://eprint.iacr.org/2004/031.pdf
25. Seroussi, G.: Compact representation of elliptic curve points over $\mathbb{F}_2^n$ research contribution to IEEE P1363 (1998)