Systems of polynomial equations associated to elliptic curve discrete logarithm problems

Claus Diem

Institute for Experimental Mathematics, University of Duisburg-Essen

October 27, 2004

Abstract. We show that the discrete logarithm problem (DLP) in $E(K)$, where E/K is an elliptic curve over a finite field K, can be solved if one can decide whether certain systems of multivariate quadratic polynomial equations over K are consistent, i.e. whether they have a solution in the algebraic closure of K. If the cyclic subgroup of $E(K)$ in which one wants to solve the DLP has a size of N bits, one has to determine whether less than $2N$ systems with each less than N variables are consistent or not.

Keywords. Elliptic curve discrete logarithm problem, multivariate systems of polynomial equations

1 Introduction and main result

The fact that the security of many cryptographic systems would be jeopardized if one could solve certain systems of multivariate polynomial equations has recently received considerable attention of cryptologists (see e.g. [4, 17, 10]). In this paper, we show that in a certain way also the security of elliptic curve cryptography relies on the difficulty of finding solutions to systems of multivariate polynomial equations.

The elliptic curve discrete-logarithm problem (ECDLP) is the following algorithmic problem: Given a finite field K, an elliptic curve E/K (given by an explicit curve equation), a point $P \in E(K)$ and a point $Q \in \langle P \rangle$ (given by explicit coordinates), where $\langle P \rangle$ is the cyclic subgroup generated by P, find a natural number e such that $e \cdot P = Q$. By abuse of terminology, if the field K, the elliptic curve E/K and the points P and Q are fixed, we speak of the (elliptic curve) discrete-logarithm problem with respect to E/K, P and Q.

The best (publicly) known methods to attack the ECDLP which apply to all discrete logarithm problems in all elliptic curves over all finite fields are "generic" methods which only rely on the fact that $E(K)$ is a group: First of all, with the Chinese Remainder Theorem one can easily reduce to the case that the group order is prime. Now (for example) with Pollard's ρ-method one obtains an expected running time of $\Theta(\sqrt{\ell})$ (counted in field operations), where $\ell := \#\langle P \rangle$.

In this paper, we present a completely new approach to attack the ECDLP which also applies to all discrete logarithm problems in all elliptic curves over all finite fields. Our main result is as follows:

Main result. *To the elliptic curve E/K, a point $P \in E(K)$ such that the group $\langle P \rangle$ has bit-length N (i.e. $N = [\log_2(\#\langle P \rangle)] + 1$), a second point $Q \in E(K)$ and an integer s with $3 \leq s \leq N-2$, one can associate a system of quadratic polynomials in $K[X_1, \ldots, X_{s-1}, Y_1, \ldots, Y_{N-s}]$ of the form*

$$f_k := (\sum_{j=1}^{N-s}(\sum_{i=1}^{s-1} a_{i,j}^{(k)} X_i Y_j) + a_{s,j}^{(k)} Y_j) + a^{(k)} \quad (k = 1, \ldots, M,\ a_{i,j}^{(k)}, a^{(k)} \in K)$$

(where $M \geq N$) with the following property: All solutions of the system of equations $f_1 = f_2 = \cdots = f_M = 0$ in the algebraic closure $\overline{K}$ of K lie in K, and they correspond bijectively to tuples $\underline{e} \in \{0,1\}^{\{0,\ldots,N-1\}}$ with $(\sum_{i=0}^{N-1} e_i 2^i) \cdot P = Q$ such that $|\underline{e}| := \sum_{i=0}^{N-1} e_i = s$. (In particular, the associated algebraic set is 0-dimensional.)

Moreover, the calculation of the system of polynomials is very fast from a practical point of view, and counted in field operations, it is polynomial in N from a theoretical point of view. Also, once one has found a solution to the system, one can easily derive the corresponding tuple $\underline{e} \in \{0,1\}^{\{0,\ldots,N-1\}}$.

Let $Q \in \langle P \rangle$. Note that according to the definition of N, there always exists at least one and at most two $\underline{e} \in \{0,1\}^{\{0,\ldots,N-1\}}$ with $(\sum_{i=0}^{N-1} e_i 2^i) \cdot P = Q$. Accordingly, one of the following two possibilities is always satisfied.

1. The union of the sets of solutions to the above systems over K (or – what is the same – over $\overline{K}$) consists of at least one and at most two elements, and each of these elements corresponds to a solution of the DLP given by P and Q.

2. There exists some $\underline{e} \in \{0,1\}^{\{0,\ldots,N-1\}}$ with $|\underline{e}| = 0, 1, 2, N-1, N$ with $(\sum_{i=0}^{N-1} e_i 2^i) \cdot P = Q$.

In the second case one can easily derive the vector $\underline{e}$ by a "brute-force" approach. We can thus conclude that we can solve the DLP given by E/K, P and Q if we can solve the above quadratic systems.

We will see at the end of the following section that there is an alternative to solving the above system which potentially is computationally easier:

By an analogous procedure as the one which we use to construct the above systems, one can construct certain systems with slightly less variables. If one can now check whether these systems are *consistent*, i.e. whether they have a solution in $\overline{K}$, one can also solve the discrete logarithm problem in $E(K)$.

2 Construction of the system

As above, let K be a finite field and E/K an elliptic curve. Let us first fix some notations.

Notations

We denote the *divisor group* of E/K (i.e. the group of K-rational divisors of E/K) by $\mathrm{Div}(E/K)$ and the *(divisor) class group* (sometimes also called Picard group) of E/K by $\mathrm{Cl}(E/K)$. We denote by $\mathrm{Div}^0(E/K)$ and $\mathrm{Cl}^0(E/K)$ the corresponding groups consisting of divisors (resp. divisor classes) of degree 0.

If $P \in E/K$, we denote the corresponding divisor of degree 1 in $\mathrm{Div}(E/K)$ by $[P]$, and if $a \in \mathrm{Div}(E/K)$, we denote the corresponding class in $\mathrm{Cl}(E/K)$ by $\overline{a}$. Let us denote the neutral element in $E(K)$ by $\mathcal{O}$.

If f is a non-trivial element in the function field $K(E)^*$, we denote the corresponding residue class in $K(E)^*/K^*$ by $\overline{f}$. (This notation should not be confused with the above notation for elements in $\mathrm{Cl}(E/K)$.)

If $D \in \mathrm{Div}(E/K)$, we denote the corresponding Riemann-Roch space by $\mathcal{L}(D)$. Recall that by definition $\mathcal{L}(D)$ is the K-vector subspace of the function field $K(E)$ consisting of the zero-element and all rational functions $f \in K(E)^*$ with $(f) \geq -D$.

Note that for $P, Q, R \in E(K)$, we have $P + Q = R$ if and only if $\overline{[P]} + \overline{[Q]} = \overline{[R]} + \overline{[\mathcal{O}]} \in \mathrm{Cl}(E/K)$ *by definition* of the group law on $E(K)$.

If L/K is an extension field, we write E/L if we consider E as an elliptic curve over L. Then $\mathrm{Div}(E/L)$ and $\mathrm{Cl}(E/L)$ will be the divisor group, resp. the class group of E over L. Note that if D is a divisor on E, the notation $\mathcal{L}(D)$ does not indicate whether one considers the Riemann-Roch space of D over K or over L. Because of this, in the following lemma, we state explicitly if we consider the Riemann-Roch space in $K(E)$ or in $\overline{K}(E)$.

Lemma 1. *Let $P_1, P_2, Q \in E(K)$. Then the following assertions are equivalent.*

1. $P_1 + P_2 = Q \in E(K)$.
2. $\overline{[P_1]} + \overline{[P_2]} = \overline{[Q]} + \overline{[\mathcal{O}]} \in \mathrm{Cl}(E/K)$.
3. *There exists some function $f \in K(E)^*$ such that $(f) = [P_1]+[P_2]-[Q]-[\mathcal{O}] \in \mathrm{Div}^0(E/K)$.*
4. *There exists some function $f \in \overline{K}(E)^*$ such that $(f) = [P_1]+[P_2]-[Q]-[\mathcal{O}] \in \mathrm{Div}^0(E/\overline{K})$.*
5. *There exists some function $f \in K(E)^*$ such that f lies in $\mathcal{L}([Q]+[\mathcal{O}]-[P_1]-[P_2]) \subset K(E)$ and f^{-1} lies in $\mathcal{L}([P_1]+[P_2]-[Q]-[\mathcal{O}]) \subset K(E)$.*
6. *There exists some function $f \in \overline{K}(E)^*$ such that f lies in $\mathcal{L}([Q]+[\mathcal{O}]-[P_1]-[P_2]) \subset \overline{K}(E)$ and f^{-1} lies in $\mathcal{L}([P_1]+[P_2]-[Q]-[\mathcal{O}]) \subset \overline{K}(E)$.*

If these conditions are satisfied, the functions f in assertions 3 and 5 are uniquely determined up to multiplication by an element in K^*, and the functions f in assertions 4 and 6 are uniquely determined up to an element in $\overline{K}^*$.

Proof. The assertions 1,2,3 and 5 are equivalent by the definition of the group law on E/K and the definitions of the divisor class group and the Riemann-Roch spaces. The same holds for the assertions 1,4,6. The last assertion can easily be derived from the fact that $\mathcal{L}(0) = K$ ([18, I.4.7]). □

The equivalence between the first and the last two assertions is a first step towards the system of quadratic equations we have in mind.

Lemma 2. *Let $P_1, \ldots, P_a, Q \in E(K)$ such that the P_i are pairwise distinct and all points are different from the neutral element $\mathcal{O}$, and let $s \in \mathbb{N}$. Then there is a natural bijection between the set*

$$\left\{ \underline{e} \in \{0,1\}^a \mid \sum_{i=1}^{a} e_i P_i = Q \wedge |\underline{e}| = s \right\}$$

and the set

$$\left\{ \overline{f} \in K(E)^*/K^* |\ f \in \mathcal{L}([Q] + (s-1)[\mathcal{O}]) \wedge f^{-1} \in \mathcal{L}(\sum_{i=1}^{a} [P_i] - [Q] - (s-1)[\mathcal{O}]) \right\}.$$

Explicitly, this bijection is given as follows:

To every $\underline{e} \in \{0,1\}^a$ *with* $\sum_{i=1}^{a} e_i P_i = Q$ *and* $|\underline{e}| = s$*, we assign the residue class in* $K(E)^*/K^*$ *determined by an* $f \in K(E)^*$ *with* $(f) = \sum_{i=1}^{a} e_i [P_i] - [Q] + (1-s)[\mathcal{O}]$*. Conversely, to a residue class of functions* $\overline{f}$ *lying in the second set, we associate the tuple* $\underline{e} \in \{0,1\}^a$ *which is defined by* $e_i := v_{P_i}(f)$*, where* v_{P_i} *is the valuation of the function field* $K(E)/K$ *at* P_i*.*

In particular, the second set is invariant under the replacement of the field K *by the algebraic closure* $\overline{K}$*.*

For the *proof* one just has to check that the two maps are well-defined. This is straightforward. We just note that a function in any residue class in the second set always has a simple pole at Q, i.e. the valuation at Q is always 1. The "in particular" statement follows from the fact that the first set is invariant under the replacement of K by $\overline{K}$.

For the derivation of the system of quadratic equations, we apply the above lemma to $a = N$, $P_i := 2^{i-1}P$ $(i = 1, \ldots, N)$, where N is the bit-size of $\#\langle P \rangle$ and some s with $3 \leq s \leq N-2$.

We obtain a bijection between

$$\left\{ \underline{e} \in \{0,1\}^{\{0,\ldots,N-1\}} |\ \sum_{i=0}^{N-1} e_i 2^i P = Q \wedge |\underline{e}| = s \right\}$$

and

$$\left\{ \overline{f} \in K(E)^*/K^* \left| \begin{array}{c} f \in \mathcal{L}([Q] + (s-1)[\mathcal{O}]) \\ \wedge \\ f^{-1} \in \mathcal{L}(\sum_{i=0}^{N-1} [2^i P] - [Q] - (s-1)[\mathcal{O}]) \end{array} \right. \right\}.$$

Choosing bases

By the Riemann-Roch Theorem ([18, I.5.15.], [11, IV, Theorem I.3]), the space $\mathcal{L}((s-1)[\mathcal{O}])$ is an $s-1$-dimensional K-vector space; let $\alpha_1, \ldots, \alpha_{s-1}$ be a basis of this space (α_1 can chosen to be 1). As again by the Riemann-Roch Theorem $\mathcal{L}([Q]+(s-1)[\mathcal{O}])$ is an s-dimensional K-vector space, there exists an element α_s in this space such that $\alpha_1, \ldots, \alpha_s$ is a basis of $\mathcal{L}([Q] + (s-1)[\mathcal{O}])$. Furthermore, the space $\mathcal{L}(\sum_{i=0}^{N-1}[2^i P] - [Q] - (s-1)[\mathcal{O}])$ is an $N-s$-dimensional K-vector space; let $\beta_1, \ldots, \beta_{N-s}$ be a basis of this space.

With these definitions, the second set is equal to the following set.

$$\left\{ \overline{f} \in K(E)^*/K^* |\ f \in \langle \alpha_1, \ldots, \alpha_s \rangle_K \wedge f^{-1} \in \langle \beta_1, \ldots, \beta_{N-s} \rangle_K \right\}$$

By definition, every residue class in this set is defined by a function which has a (simple) pole at Q. Together with the definition of $\alpha_1, \ldots, \alpha_s$, this means that the above set is in natural bijection with the set

$$\left\{ f \in K(E) |\ f \in \alpha_s + \langle \alpha_1, \ldots, \alpha_{s-1} \rangle_K \wedge f^{-1} \in \langle \beta_1, \ldots, \beta_{N-s} \rangle_K \right\},$$

and this set is in natural bijection with

$$\left\{ (f,g) \in K(E)^2 |\ f \cdot g = 1 \wedge f \in \alpha_s + \langle \alpha_1, \ldots, \alpha_{s-1} \rangle_K \wedge g \in \langle \beta_1, \ldots, \beta_{N-s} \rangle_K \right\},$$

which in turn is in natural bijection with

$$\left\{ (\underline{x}, \underline{y}) \in K^{s-1} \times K^{N-s} |\ (\alpha_s + \sum_{i=1}^{s-1} x_i \alpha_i) \cdot (\sum_{j=1}^{N-s} y_j \beta_j) = 1 \right\},$$

that is,

$$\left\{ (\underline{x}, \underline{y}) \in K^{s-1} \times K^{N-s} |\ \sum_{j=1}^{N-s} ((\sum_{i=1}^{s-1} x_i y_j \gamma_{i,j}) + \gamma_{s,j} y_j) = 1 \right\},$$

where

$$\gamma_{i,j} := \alpha_i \beta_j \quad (i = 1, \ldots, s, j = 1, \ldots, N-s).$$

Let $K(E) = K(X)[Y]$, where Y satisfies an equation of degree 2 over the rational function field $K(X)$. The idea is now to expand "everything" with respect to the basis $1, Y$ of the $K(X)$-vector space $K(E)$.

For this, first write $\gamma_{i,j} = \gamma_{i,j,1} + Y\gamma_{i,j,2}$ wit $\gamma_{i,j,1}, \gamma_{i,j,2} \in K(X)$. Now let $D(X) \in K[X]$ be the least common multiple of the denominators of all the $\gamma_{i,j,1}, \gamma_{i,j,2}$ (written as reduced fractions). Now we have $\gamma_{i,j} = \frac{\delta_{i,j,1}}{D} + Y\frac{\delta_{i,j,2}}{D}$ with some polynomials $\delta_{i,j,1}, \delta_{i,j,2} \in K[X]$.

With these definitions, the above set is equal to

$$\left\{ (\underline{x}, \underline{y}) \in K^{s-1} \times K^{N-s} \left| \begin{array}{c} \sum_{j=1}^{N-s} (\sum_{i=1}^{s-1} x_i y_j \delta_{i,j,1} + y_j \delta_{s,j,1}) = D(X) \\ \wedge \\ \sum_{j=1}^{N-s} (\sum_{i=1}^{s-1} x_i y_j \delta_{i,j,2} + y_j \delta_{s,j,2}) = 0 \end{array} \right. \right\}.$$

For $k \in \mathbb{N}$, let $\delta_{i,j,1}^{(k)}$ (resp. $\delta_{i,j,2}^{(k)}$) be the k-th coefficient of the polynomial $\delta_{i,j,1} \in K[X]$ (resp. $\delta_{i,j,2} \in K[X]$), and let $D^{(k)}$ be the k-th coefficient of $D \in K[X]$. Then the above set is equal to

$$\left\{ (\underline{x}, \underline{y}) \in K^{s-1} \times K^{N-s} \left| \begin{array}{c} \forall k \in \mathbb{N} : \sum_{j=1}^{N-s} (\sum_{i=1}^{s-1} x_i y_j \delta_{i,j,1}^{(k)} + \delta_{s,j,1}^{(k)} y_j) = D^{(k)} \\ \wedge \\ \forall k \in \mathbb{N} : \sum_{j=1}^{N-s} (\sum_{i=1}^{s-1} x_i y_j \delta_{i,j,2} + \delta_{s,j,2}^{(k)} y_j) = 0 \end{array} \right. \right\}.$$

The system of polynomials in $K[X_1, \ldots, X_{s-1}, Y_1, \ldots, Y_{N-s}]$ we want to derive consists of

$$(\sum_{j=1}^{N-s} (\sum_{i=1}^{s-1} \delta_{i,j,1}^{(k)} X_i Y_j) + \delta_{s,j,1}^{(k)} Y_j) - D^{(k)}$$

and

$$(\sum_{j=1}^{N-s}(\sum_{i=1}^{s-1}\delta_{i,j,2}^{(k)}X_iY_j)+\delta_{s,j,2}^{(k)}Y_j) \qquad (k\in\mathbb{N}).$$

Note that only finitely many of these polynomials are non-trivial.

Algorithmic aspects

To explicitly construct the system of polynomials starting from an explicitly given equation of E/K and two points $P,Q\in E(K)$, one just has to follow the above procedure. The only step which we did not explain in a constructive way is the finding of the bases of the Riemann-Roch spaces in question. For this well-known algorithmic problem, we refer to [12], in particular [12, Algorithm I and Remark 6.2]. Furthermore, if one has found a solution, one can derive the corresponding vector in $\{0,1\}^{\{0,\ldots,N-1\}}$ which gives the solution to the DLP by first constructing the class $\overline{f}\in K(E)^*/K^*$ corresponding to the solution (by inverting the above procedure) and then checking for each $i=0,\ldots,N-1$ whether f has a zero at 2^iP.

A question of consistency

One can reduce the problem of finding solutions to the above systems of quadratic polynomial equations to a question of consistency, i.e. to the question whether certain systems of polynomials have a solution in the algebraic closure $\overline{K}$ of the ground field K. Note that by Hilbert's "Nullstellensatz" a system is consistent if and only if the generated ideal in the surrounding polynomial ring is strictly smaller than the unit ideal.

For this variant, we proceed as follows: First of all, for some s with $3\leq s\leq N-3$, we consider the system obtained by the above method after substituting $\mathcal{L}(\sum_{i=0}^{N-1}[2^iP]-[Q]-(s-1)[\mathcal{O}])$ by $\mathcal{L}(\sum_{i=0}^{N-2}[2^iP]-[Q]-(s-1)[\mathcal{O}])$. Now the union of sets the solutions of the systems contains at most one element (instead of at most 2 elements).

Now we first of all check the systems for consistency to determine the s (if it exists) such that there exists a $\underline{e}\in\{0,1\}^{\{0,\ldots,N-2\}}$ with $(\sum_i e_i2^i)\cdot P_i=Q$ and $|\underline{e}|=s$. (If no such s exists, we replace Q by $Q-2^{N-1}P$ and proceed with this system as just described.)

After we have determined s, we want to find the unique $\underline{e}\in\{0,1\}^{\{0,\ldots,N-2\}}$ with $(\sum_i e_i2^i)\cdot P_i=Q$ and $|\underline{e}|=s$. To do so, we repeatedly replace the Riemann-Roch space $\mathcal{L}(\sum_{i=0}^{N-2}[2^iP]-[Q]-(s-1)[\mathcal{O}])$ by $\mathcal{L}((\sum_{i=0}^{N-2}[2^iP])-[2^{i_0}P]-[Q]-(s-1)[\mathcal{O}])$, where i_0 is any element in the set $\{0,\ldots,N-2\}$. We check whether the system one obtains with the above method is consistent. If it is, we know that in the unique vector $\underline{e}\in\{0,1\}^{\{0,\ldots,N-2\}}$ with $\sum_{i=0}^{N-2}e_i2^iP=Q$, there is a 0 at the index i_0. It it is not, there is a 1 at this index.

3 Testing the systems for consistency

In this section, we want to discuss what complexity one can expect if one tries to determine whether the above systems are consistent (solvable). In contrast to the previous section, this discussion will involve some heuristic considerations.

We have conducted experiments with the above systems. In these experiments, the dimension of the space generated by the equations in the "main result" was always exactly N, i.e. it was equal to the number of variables $+1$. Also the smaller systems described at the end of the previous section had the property that the difference between the dimension of the space generated by the equations and the number of variables present in the system was always 1 (independent of whether or not the systems were consistent).

While we do at present not have a theoretical explanation or a proof for this statement, it seems to be reasonable to make the assumption that the difference between the dimension of the spaces generated by the equations and the number of variables present in the systems is 1.

In the appendix to this work, we present a Monte-Carlo algorithm to test whether a system given by $n+1$ *homogeneous* polynomials in $n+1$ variables is consistent, i.e. whether it has a non-trivial solution. The algorithm could be called a "Monte-Carlo test for consistency via Macaulay matrices"; it is closely related to Lazards' algorithms ([14, 15]), to the F_5-algorithm ([9]), as well as the XL-algorithm ([3]). (See also the subsection "Comparison with F_5" in the appendix.)

If one tries to apply this algorithm (or Lazard's algorithms / the XL-algorithm) to the homogenizations of the system we derived, one encounters however a problem: By the structure of the equations, the algebraic set of solutions at infinity is not empty (and its dimension is quite high), thus in particular, the systems are always consistent. (In principle, it is possible to apply the F_4- or F_5-algorithms, but because of the solutions are infinity, the running time might be quite bad.)

One can however modify the systems and the algorithm such that we can avoid this problem.

For this modification, we start with a system

$$g_k := (\sum_{j=1}^{N-1-s-\epsilon}(\sum_{i=1}^{s-1} a_{i,j}^{(k)} X_i Y_j) + a_{s,j}^{(k)} Y_j) + a^{(k)} \qquad (k = 1, \ldots, M,\ a_{i,j}^{(k)}, a^{(k)} \in K) \tag{1}$$

obtained by the method in the previous section (in the variant described in the subsection "A question of consistency"). Here ϵ is 0 or 1, depending on whether one wants to determine s or if s has already been determined. We want to test this system for consistency.

We introduce a new variable X_s and consider the system

$$\tilde{g}_k := (\sum_{j=1}^{N-1-s-\epsilon} \sum_{i=1}^{s} a_{i,j}^{(k)} X_i Y_j) + a^{(k)} \quad (k = 1, \ldots, M,\ a_{i,j}^{(k)}, a^{(k)} \in K). \tag{2}$$

By the construction of the system in the previous section, every solution $(\underline{x}, \underline{y})$ of this system satisfies $x_s \neq 0$ (see in particular the definition of the basis of

$\mathcal{L}([Q] + (s-1)[\mathcal{O}])$ in the subsection "Choosing bases"). It follows that this system is consistent if and only if the previous one is.

Now we apply a variant of the "relinearization technique" ([13]) once:

Let us consider the map

$$\overline{K}^{N-1-s-\epsilon} \times \overline{K}^{s} \longrightarrow \overline{K}^{(N-1-s-\epsilon)\cdot s}, \quad (\underline{x}, \underline{y}) \mapsto \underline{z} = (z_{ij}) \text{ with } z_{ij} = x_i y_j \quad (3)$$

All elements in the image of this map obviously satisfy the system of equations

$$Z_{ij}Z_{\ell k} - Z_{ik}Z_{\ell j}. \quad (4)$$

It is not hard to see that this set of equations defines the image of the map. Moreover, it is also not hard to see that if $\underline{x} \neq 0$ and $\underline{y} \neq 0$, then exactly the elements of the form $(\lambda\underline{x}, \frac{1}{\lambda}\underline{y})$ with some $\lambda \in \overline{K}^*$ map to the same image. Also, exactly the elements $(\underline{0}, \underline{y})$ and $(\underline{x}, \underline{0})$ map to $\underline{0}$.

Let us consider the system consisting of (4) and the following linear equations.

$$l_k := (\textstyle\sum_{j=1}^{N-1-s-\epsilon} \sum_{i=1}^{s} a_{i,j}^{(k)} Z_{ij}) + a^{(k)} \qquad (k = 1, \ldots, M,\ a_{i,j}^{(k)}, a^{(k)} \in K) \quad (5)$$

The group $\overline{K}^*$ operates on the set of solutions of (2) in $\overline{K}$ via $(\lambda, (\underline{x}, \underline{y})) \mapsto (\lambda\underline{x}, \frac{1}{\lambda}\underline{y})$. By what we said about the map (3), the classes of the solutions $(\underline{x}, \underline{y})$ in $\overline{K}$ with $\underline{x} \neq \underline{0}$ and $\underline{y} \neq \underline{0}$ of (2) modulo this operation correspond bijectively to the non-trivial solutions in $\overline{K}$ of the corresponding "relinearized" system consisting of (4) and (5). As at least one of the $a^{(k)}$ is non-trivial, the solutions $(\underline{x}, \underline{y})$ in $\overline{K}$ of (2) are in bijection with the solutions in $\overline{K}$ of the "relinearized" system.

This implies that system (2) is consistent if and only if the "relinearized" consisting of (4) and (5) system is.

The "relinearized" system has no non-trivial solutions at infinity. This can be seen as follows: The non-trivial solutions at infinity in $\overline{K}$ of the "relinearized system" correspond bijectively to classes of solutions $(\underline{x}, \underline{y})$ in $\overline{K}$ with $\underline{x} \neq \underline{0}$, $\underline{y} \neq \underline{0}$ of the system

$$\sum_{j=1}^{N-1-s-\epsilon} \sum_{i=1}^{s} a_{i,j}^{(k)} X_i Y_j \qquad (k = 1, \ldots, M,\ a_{i,j}^{(k)} \in K).$$

By going through Section 2, one sees that a solution of this system in $\overline{K}$ with $\underline{x} \neq \underline{0}, \underline{y} \neq \underline{0}$ would give rise to a pair $(f, g) \in \overline{K}(E) \times \overline{K}(E)$ with $f \cdot g = 0$, $f \neq 0, g \neq 0$ which does not exist.

We are thus left with the question of deciding whether the homogenization of the "relinearized" system is consistent or not (as a homogeneous system). In the subsection "examples for generalizations" in the appendix, we show that with a generalization of the "Monte-Carlo test for consistency via Macaulay matrices" one can test the consistency of the homogenization of the system in $\tilde{\mathcal{O}}(2^{4N})$ bit operations. This complexity is of course far worse than the complexity of a brute force attack on the ECDLP itself.

4 Conclusions

We have shown that one can solve an N-bit discrete-logarithm problem in an elliptic curve over a finite field K if one can determine whether less than $2N$ systems of multivariate quadratic polynomial equations with at most N variables over K are consistent, that is, whether they have a solution in the algebraic closure $\overline{K}$ of K.

We found no indication that it might be possible to check whether the systems are consistent with a running time which is better than that of a brute force attack on the ECDLP itself.

Even though the proposed attack thus clearly seems to fail and not to pose a threat to elliptic curve cryptography, we find it however interesting that just as the security of many other cryptographic schemes, also the security of elliptic curve cryptography relies on the difficulty of the problem of solving systems of polynomial equations over finite fields (more precisely, determining whether they are consistent). If for example the systems we derived have some unexpected special property (for example concerning Gröbner bases), it might be possible to determine much faster whether they are consistent, and this might also lead a veritable attack on the ECDLP.

We would also like to point out that there is also another approach to associate systems of polynomial equations to the DLP in elliptic curves (and in other algebraic groups): One introduces variables X_i, the i-th variable corresponds to the i-th bit in the unknown (and one introduces equations $X_i(X_i-1)=0$, as the bits are either 0 or 1), and then one uses the group law to construct equations relating the variables X_i (possibly after introducing certain auxiliary variables).

Acknowledgment

I thank Jürgen Herzog and Aldo Conca for discussions on commutative algebra.

Support by the IST Programme "Ecrypt" of the European Union is gratefully acknowledged.

References

[1] M. Bardet, J.-C. Faugère, and B. Salvy. Complexity of Gröbner basis computations for Semi-regular Overdetermined sequences over $\mathbb{F}_2$ with solutions in $\mathbb{F}_2$. INRIA Rapport de recherche No. 5049, 2003.

[2] A. Conca and J. Herzog. personal communication.

[3] N. Courtois, A. Klimov, J. Pararin, and A. Shamir. Solving overdefined multivariate equations. In B. Preneel, editor, *Advances in Cryptology — EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 392–407. Springer-Verlag, Berlin, 2000.

[4] N. Courtois and J. Pieprzyk. Cryptanalysis of block ciphers with overdefined systems of equations. In *Advances in Cryptology — ASIACRYPT 2002*, number 2501 in LNCS, pages 267–287. Springer-Verlag, 2002.

[5] C. Diem. The XL-Algorithm and a Conjecture from Commutative Algebra. In *Proceedings in Cryptology — ASIACRYPT 2004*, Lecture Notes in Computer Science, Berlin. to be published.
[6] W. Eberly and E. Kaltofen. On randomized lanczos algorithms. In W. Küchlin, editor, *Proceedings ISSAC 1997*, pages 176–183. ACM Press, 1997.
[7] D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. Springer-Verlag, New York, 1995.
[8] A. Enge and P. Gaudry. A general framework for subexponential discrete logarithm algorithms. *Acta. Arith.*, 102:83–103, 2002.
[9] J.-C. Faugère. A new efficient algorithm for computing Groebner Bases without reduction to zero (F5). In *Proceedings of ISSAC (2002)*, pages 75–83. ACM Press, 2002.
[10] J.-C. Faugère and A. Joux. Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases. In D. Bonet, editor, *Advances in Cryptography — CRYPTO 2003*, number 2729 in Lecture Notes in Computer Science, Berlin, 2003. Springer-Verlag.
[11] R. Hartshorne. *Algebraic Geometry*. Springer-Verlag, New York, 1977.
[12] F. Heß. Computing Riemann-Roch spaces in algebraic function fields and related topics. *J. Symbolic Computation*, 11, 2001.
[13] A. Kipnis and A. Shamir. Cryptanalysis of the HFE public key cryptosystem by relinearization. In *Advances in cryptology — CRYPTO 1999*, volume 1666 of *Lecture Notes in Comput. Sci.*, pages 19–30, Berlin, 1999. Springer-Verlag.
[14] D. Lazard. Résolution des systèmes d'équations algébriques. *Theoret. Comput. Sci.*, 15(1):77–110, 1981.
[15] D. Lazard. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In *Computer algebra (London, 1983)*, volume 162 of *Lecture Notes in Comput. Sci.*, pages 146–156. Springer-Verlag, Berlin, 1983.
[16] F. Morain. La primalité en temps polynomial. *Séminaire Bourbaki*, 917, 2002-2003.
[17] S. Murphy and M. Robshaw. Essential algebraic structure within the AES. In Moti Yung, editor, *Advances in Cryptology - CRYPTO 2002*, pages 1–16, 2002.
[18] H. Stichtenoth. *Algebraic Function Fields and Codes*. Springer-Verlag, Berlin, 1993.

A A Monte-Carlo test for consistency via Macaulay matrices

In this section we describe an algorithm which could be called a "Monte-Carlo test for consistency of homogeneous systems via Macaulay matrices".

The input of the algorithm are $n+1$ non-trivial *homogeneous* polynomials $F_1, \ldots, F_{n+1} \in K[X_0, \ldots, X_n]$ of degrees $d_1, \ldots, d_{n+1}$, K an "effective" field. We want to determine whether there exists an element $\underline{x} \in \overline{K}^{\{0,\ldots,n\}} \setminus \{\underline{0}\}$ with $F_k(\underline{x}) = 0$ for all $k = 1, \ldots, n+1$. If this is the case, we say that the system is (as a homogeneous system) *consistent*, otherwise we say that it is *inconsistent*.

Note that $K[X_0, \ldots, X_n]/(F_1, \ldots, F_{n+1})$ is a graded $K[X_0, \ldots, X_n]$-algebra; we will denote the d^{th} homogeneous component of this algebra by $(K[X_0, \ldots, X_n]/(F_1, \ldots, F_{n+1}))_d$.

The algorithm is based on the following lemma:

Lemma 3. *The following conditions are equivalent:*

1. *The system $F_1, \ldots, F_{n+1}$ is inconsistent.*
2. *The ring $K[X_0, \ldots, X_n]/(F_1, \ldots, F_{n+1})$ is 0-dimensional.*
3. *The K-algebra $K[X_0, \ldots, X_n]/(F_1, \ldots, F_{n+1})$ is a finite-dimensional K-vector space.*
4. *The system $F_1, \ldots, F_{n+1}$ forms a regular sequence, i.e. each F_{i+1} is a non-zerodivisor in $K[X_0, \ldots, X_n]/(F_1, \ldots, F_i)$.*
5. *$(K[X_0, \ldots, X_n]/(F_1, \ldots, F_{n+1}))_D = 0$, where $D = d_1 + \cdots d_{n+1} - n$.*

Sketch of the Proof. The equivalence of the first two items follows from Hilbert's "Nullstellensatz". For the equivalence of the second and third item note that both statements are equivalent to $K[X_0, \ldots, X_n]/(F_1, \ldots, F_{n+1})$ being artinian.

We now show that 2. $\longrightarrow$ 4., 4. $\longrightarrow$ 5. and 5. $\longrightarrow$ 2.

The implication 2. $\longrightarrow$ 4. is essentially a special case of [7, Corollary 17.7.]. (Note that this corollary is only stated for local rings, but it is easy to derive from the statement on local rings the corresponding statement on graded rings.)

Let 4. be satisfied. It is rather straightforward that the Hilbert series of $K[X_0, \ldots, X_n]/(F_1, \ldots, F_{n+1})$ is $\frac{\prod_{i=1}^{n+1}(1-T^{d_i})}{(1-T)^{n+1}}$, in particular the degree of the Hilbert series is $d_1 + \cdots d_n - n - 1$. This implies 5. (For more information on Hilbert series and a proof of the statement concerning the Hilbert series of $K[X_0, \ldots, X_n]/(F_1, \ldots, F_{n+1})$ see (e.g.) [5, Section 4].)

Let 5. be satisfied. Then for all $d > D$, the K-vector space $(K[X_0, \ldots, X_n]/(F_1, \ldots, F_{n+1}))_d$ is also trivial; it follows that $K[X_0, \ldots, X_n]/(F_1, \ldots, F_{n+1})$ is a finite-dimensional K-vector space, i.e. 3. is satisfied. □

The algorithm is based on the equivalences between assertions 1. and 5. A brief description of the algorithm is: Consider the set P of all polynomials of the form $X^{\underline{i}} \cdot F_k$, where $i \in \mathbb{N}_0^{\{0,\ldots,n\}}$ is a multiindex and $\deg(X^{\underline{i}}) + d_k = D$ with $D = d_1 + \cdots d_n - n$, $d_k = \deg(F_k)$. Now the system $F_1, \ldots, F_{n+1}$ is consistent if and only if the K-vector space $\langle P \rangle_K$ is strictly smaller than $K[X_0, \ldots, X_n]_D$. To check whether this is the case, use some method from linear algebra.

To apply methods from linear algebra, one should first construct a matrix. To do this, one chooses an order on the set of all monomials of degree $D = d_1 + \cdots d_n - n$ (this order might for example be given via an admissible monomial order on $K[X_0, \ldots, X_n]$). With respect to this order, one can associate a *coefficient vector* to each polynomial of degree D. Now the rows of the matrix we want to consider consist of the coefficient vectors of the polynomials of the form $X^{\underline{i}} \cdot F_k$ as above. In order to define the matrix rigorously, one also has to define an order on the tuples of the form $(X^{\underline{i}}, j)$ with $\deg(X^{\underline{i}}) + k = d_1 + \cdots d_n - n$. Let us assume that we have chosen such an order. Say that with respect to this order, $(X^{\underline{i}}, j)$ is tuple number a. Then the a-th row of the matrix consists of the coefficient vector of the polynomial $X^{\underline{i}} \cdot F_k$.

The matrix we just defined is in fact exactly the so-called *Macaulay matrix* $\mathcal{M}_{D,m}^{\text{acaulay}}$ with $D = d_1 + \cdots d_n - n$ considered for example in Section 2.2. of [1].

A first description of the algorithm (which still lacks quite a bit of determinacy) is as follows:

The algorithm (Outline)

Input: An effective field K and a system of forms (homogeneous polynomials) $F_1, \ldots, F_{n+1} \in K[X_0, \ldots, X_n]$
Output: A statement on the consistency of the system.

Let $\mathcal{M}$ be the Macaulay matrix to degree $D = d_1 + \cdots + d_n - n$ (with respect to some order) corresponding to the system $F_1, \ldots, F_{n+1}$.
Let $c := \binom{D+n}{n} = \binom{d_1+\cdots+d_n}{n}$ be the number of columns of $\mathcal{M}$.
Test whether the rows of $\mathcal{M}$ do not generate K^c. If the outcome of the test is "yes", output "consistent", otherwise output "inconsistent".

The question is now of course how one should test whether the rows of $\mathcal{M}$ generate the surrounding space. Depending on this method, one obtains a deterministic or a randomized test.

One can for example use structured Gaussian elimination. Like this, one obtains a deterministic test. As the Macaulay matrix is however very sparse, a randomized (Monte-Carlo) test based on sparse linear algebra is much more efficient.

Note that the following statements are equivalent:

- The rows of $\mathcal{M}$ generate the surrounding space K^c.
- The rank of $\mathcal{M}$ is equal to c.
- The columns of $\mathcal{M}$ are linearly independent.
- The kernel of $\mathcal{M}$ is trivial.

One can use a randomized algorithm to check whether the last condition is satisfied. Let us assume that the field K is finite. Then we can (for example) use a variant of the randomized Lanczos algorithm presented in [6] to check whether $\ker(\mathcal{M}) \neq 0$. The following proposition is an easy corollary of [8, Theorem 3] which relies on the algorithm in [6].

Proposition 1. *There exists a Monte-Carlo test on the non-triviality of the kernel of a matrix $A \in \mathbb{F}_q^{r \times c}$ given in sparse form with ω non-zero entries which has an expected running time of $\mathcal{O}(c \cdot (\omega + c) \cdot \log^2(c\,q))$ bit operations.*

Recall that by definition, a Monte-Carlo test on a property $\mathcal{P}$ is a randomized algorithm which outputs "yes" / "no" and has the following properties: If the input does not satisfy $\mathcal{P}$, it always outputs "no", and if the input satisfies $\mathcal{P}$, it outputs "yes" with a probability of $\geq \frac{1}{2}$. A brief description of this and related notions can for example be found in [16, Section 2].

We can apply this algorithm to test whether the Macaulay matrix has trivial kernel. We obtain the following proposition.

Proposition 2. *There exists a Monte-Carlo test on the question whether a system of forms (homogeneous polynomials) $F_1, \ldots, F_{n+1} \in \mathbb{F}_q[X_1, \ldots, X_n]$ is consistent which has the following property:*

Let $d_k := \deg(F_k)$, let T_k the number of (non-trivial) terms in F_k, and let $T := \sum_{k=1}^{n+1} T_k$. Then the algorithm has an expected running time of

$$\mathcal{O}\Big(\tbinom{d_1+\cdots+d_n}{n} \cdot \big(\big(\sum_{j=1}^{n+1} T_k \cdot \tbinom{d_1+\cdots+d_n-d_k}{n}\big) + \tbinom{d_1+\cdots+d_n}{n}\big) \cdot (d_1+\cdots+d_n+\log(q))^2\Big)$$

$$\subset \mathcal{O}\Big((T+1) \cdot \tbinom{d_1+\cdots+d_n}{n}^2 \cdot (d_1+\cdots+d_n+\log(q))^2\Big)$$

bit operations.

In particular, if all polynomials are quadratic, the algorithm has an expected running time of $\tilde{\mathcal{O}}(2^{4n})$.

Comparison with F_5

The F_5-algorithm ([9]) is an algorithm to calculate Gröbner bases of homogeneous systems of multivariate polynomials. One might think that the F_5-algorithm could lead to substantially better running times than our above "Monte-Carlo test for non-consistency via Macaulay matrices". This is however not the case if one wants to check whether "randomly generated" / "sufficiently general" systems are consistent.

If one wants to use the F_5-algorithm to test whether a system is consistent, one has to calculate Gaussian normal forms of various matrices, the largest being (generally) a quadratic matrix of size $\binom{d_1+\cdots d_n}{n}$. The system is consistent if and only if the kernel of this quadratic matrix is non-trivial.

Being quadratic, the final matrix in the F_5-algorithm is smaller than the Macaulay matrix we consider, but it is reasonable to assume that the Macaulay matrix has less non-zero entries than the final matrix in the F_5-algorithm.

As said, the F_5-algorithm relies on the calculation of Gaussian normal forms of various matrices. It is not obvious if one can modify the algorithm in such a way that one can apply any of the "standard" algorithms to solve sparse linear systems. (These algorithms can be used to test whether the final matrix in the F_5-algorithm has a non-trivial kernel, but the usage of the Gaussian normal forms of the intermediate matrices seems to be inherent in the algorithm.) If one compares the F_5-algorithm with structured Gaussian elimination with our test with randomized Lanczos' algorithm, then asymptotically our algorithm is clearly faster.

Generalization

One can generalize the above algorithm in the following way: Let $R_1, \ldots, R_r$ be a system of forms in the polynomial ring $K[Z_0, \ldots, Z_a]$, and suppose that the ring $R := K[Z_0, \ldots, Z_a]/(R_1, \ldots, R_r)$ is Cohen-Macaulay and $n+1$-dimensional. (See [7, Sections 17 and 18], in particular [7, Section 18.2] for information on

Cohen-Macaulay rings.) Let $F_1, \ldots, F_{n+1}$ be system of forms in $K[Z_0, \ldots, Z_a]$ with $\deg(F_k) = d_k$. Then a generalization of the above algorithm can be used to decide whether the system $R_1, \ldots, R_r, F_1, \ldots, F_{n+1}$ is consistent.

This generalization is based on the following lemma which generalizes Lemma 3.

Lemma 4. *Let* $D := \deg(\prod_{i=1}^{n+1}(1 - T^{d_i}) \cdot H_R) + 1$, *where* H_R *is the Hilbert series of* R. *Then the following conditions are equivalent:*

1. *The system* $R_1, \ldots, R_r, F_1, \ldots, F_{n+1}$ *is inconsistent.*
2. *The ring* $K[Z_0, \ldots, Z_a]/(R_1, \ldots, R_r, F_1, \ldots, F_{n+1}) \simeq R/(F_1, \ldots, F_{n+1})$ *is 0-dimensional.*
3. *The* K*-algebra* $R/(F_1, \ldots, F_{n+1})$ *is a finite-dimensional* K*-vector space.*
4. *The system* $F_1, \ldots, F_{n+1}$ *forms a regular sequence in* R, *i.e. each* F_{i+1} *is a non-zerodivisor in* $R/(F_1, \ldots, F_i)$ $(i = 0, \ldots, n)$.
5. $(K[Z_0, \ldots, Z_a]/(R_1, \ldots, R_r, F_1, \ldots, F_{n+1}))_D \simeq (R/(F_1, \ldots, F_{n+1})_D = 0$.

The *proof* of this lemma is analogous to the one of Lemma 3. We just note that by the Cohen-Macaulay property the ring $R/(F_1, \ldots, F_{n+1})$ is 0-dimensional if and only if $F_1, \ldots, F_{n+1}$ defines a regular sequence in R. (This follows again from [7, Corollary 17.7.].) Also, if $F_1, \ldots, F_{n+1}$ is a regular sequence, then the Hilbert series of $R/(F_1, \ldots, F_{n+1})$ is $\prod_{i=1}^{n+1}(1-T^{d_i})H_R$, and thus $(R/(F_1, \ldots, F_{n+1}))_D = 0$.

The general outline of our test on the consistency of the system $R_1, \ldots, R_r$, $F_1, \ldots, F_{n+1}$ is analogous to the above algorithm: One calculates the Macaulay matrix $\mathcal{M}$ of degree D of the system $R_1, \ldots, R_r, F_1, \ldots, F_{n+1}$, and one tests whether $\ker(\mathcal{M}) \neq 0$. The correctness of the algorithm is guaranteed by the above lemma.

Let us assume that we have an explicit K-basis B of R consisting of homogeneous elements such that if $P, Q \in B$, then $P \cdot Q \in B$, and this element is easily computable. Under this condition, there is a variant of the algorithm which can be substantially faster:

For some $d \in \mathbb{N}$, let B_d be the elements of the fixed basis B of degree d. Now instead of considering the system of all polynomials $X^{\underline{i}} \cdot R_k, X^{\underline{i}} \cdot F_k$ with $\deg(X^{\underline{i}}) + \deg(R_k) = D, \deg(X^{\underline{i}}) + \deg(F_k) = D$, one considers the system consisting of all $H \cdot F_k \in R_D$, where for some j, H runs through $B_{D-\deg(F_k)}$, the set of basis elements of degree $D - \deg(F_k)$.

Then analogously to above, one represents each $H \cdot F_k \in R_d$ by its coefficient vector with respect to B, and one forms a matrix $\mathcal{M}$ (which could be called a *generalized Macaulay matrix*) whose rows consist of these coefficient vectors. Again, by the equivalences of the assertions 1 and 5 in the above lemma, the system is consistent if and only if $\ker(\mathcal{M}) \neq 0$. If the field K is finite, condition $\ker(\mathcal{M}) \neq 0$ can again be tested with the randomized algorithm of Proposition 1.

The advantage of this variant is that the size of the vectors is equal to the dimension of R_D (and not the dimension of $K[Z_0, \ldots, Z_a]_D$ which can be much larger), and the number of rows can also be substantially smaller.

Examples for generalizations

Two Cohen-Macaulay rings are particularly important from a practical point of view.

The first one is the ring $R^{(n)}$ given by $(n+1)^2$ indeterminates Z_{ij} $(i,j = 0,\ldots,n)$ modulo the relations $Z_{ij} - Z_{ji}$ for all i,j and $Z_{ij}Z_{\ell k} - Z_{ik}Z_{\ell j}$ for all i,j,ℓ,k. That is,

$$R^{(n)} := K[\{Z_{ij}\}_{i,j=0,\ldots,n}]/(\{Z_{ij} - Z_{ji}, Z_{ij}Z_{\ell k} - Z_{ik}Z_{\ell j}\}).$$

This ring is canonically isomorphic to the subring of $K[X_0,\ldots,X_n]$ generated by all X_iX_j (where X_iX_j corresponds to Z_{ij}), and it is $n+1$-dimensional. Note that a single application of the "relinearization technique" ([13]) to a homogeneous system $F_1,\ldots,F_{n+1} \in K[X_0,\ldots,X_n]$ corresponds to considering the F_i as linear forms in $R^{(n)}$.

The second one is the ring

$$R^{(a,b)} := K[\{Z_{ij}\}_{i=0,\ldots,a,j=0,\ldots,b}]/(\{Z_{ij}Z_{\ell k} - Z_{ik}Z_{\ell j}\}).$$

This ring is canonically isomorphic to the subring of the polynomial ring $K[X_0,\ldots,X_a,Y_0,\ldots,Y_b]$ generated by all monomials of the form X_iY_j (where X_iY_j corresponds to Z_{ij}), and it is $a+b+1$-dimensional.

For both rings, one has homogeneous K-bases such that the products of basis elements are again (easily computable) basis elements: In the ring $R^{(n)}$ (considered as subring of $K[X_0,\ldots,X_n]$), the monomials of even degree in $K[X_0,\ldots,X_n]$ form such a basis; in the ring $R^{(a,b)}$ (considered as subring of $K[X_0,\ldots,X_a,Y_0,\ldots,Y_b]$), all monomials of the form $X^{\underline{i}}\cdot Y^{\underline{j}}$, where $\underline{i} \in \mathbb{N}_0^{\{0,\ldots,a\}}$, $\underline{j} \in \mathbb{N}_0^{\{0,\ldots,b\}}$ and $i_0 + \cdots + i_a = j_0 + \cdots + j_b$ form such a basis.

Note also that if R is a Cohen-Macaulay ring, so is the polynomial ring $R[Z]$ ([7, Proposition 18.9]). This fact can in particular be applied to the above two rings.

Because of the application in Section 3 we have in mind, we now concentrate on the following question:

We suppose we are given a system of $a+b+2$ polynomials of the form

$$F_k = \sum_{i=0}^{a}\sum_{j=0}^{b} a_{i,j}^{(k)} X_iY_j + a^{(k)}Z \qquad (a_{i,j}^{(k)}, a^{(k)} \in K). \tag{6}$$

over a finite field K. Similarly to Section 3, we want to find out whether there exists a solution $(\underline{x},\underline{y},z) \in \overline{K}^{a+b+3}$ to this system with $\underline{x} \neq \underline{0}, \underline{y} \neq \underline{0}$. To study this question, we study whether the homogeneous system consisting of the linear equations

$$L_k = \sum_{i=0}^{a}\sum_{j=0}^{b} a_{i,j}^{(k)} Z_{i,j} + a^{(k)}Z \qquad (a_{i,j}^{(k)}, a^{(k)} \in K). \tag{7}$$

and the quadratic equations

$$Z_{ij}Z_{\ell k} - Z_{ik}Z_{j\ell} \tag{8}$$

is consistent. (These two questions are equivalent by the arguments of Section 3.)

To study this question, we can apply the generalization of our algorithm to systems in the Cohen-Macaulay ring $R^{(a,b)}[Z]$.

The d-th component of the ring $R^{(a,b)}$ has dimension $\binom{a+d}{d} \cdot \binom{b+d}{d}$ (because the polynomials $X^{\underline{i}} \cdot Y^{\underline{j}}$ with $i_0 + \cdots i_a = j_0 + \cdots + j_b = d$ form a basis). We have

$$(1-T)^{a+b+1} H_{R^{(a,b)}} = \sum_{i \in \mathbb{N}_0} \binom{a}{i}\binom{b}{i} T^i;$$

the degree of this polynomial is thus $\min\{a,b\}$ ([2]). It follows that $(1-T)^{a+b+2} H_{R^{(a,b)}[Z]} = (1-T)^{a+b+1} H_{R^{(a,b)}}$ also has degree $\min\{a,b\}$.

Let $a \leq b$ and $n := a+b$. Note that

$$\dim_K(R_d^{(a,b)}) = \binom{a+d}{d} \cdot \binom{b+d}{d} \leq \binom{\frac{n}{2}+d}{d}^2$$

by the inequality of the arithmetic-geometric mean. This implies that

$$\dim_K(R_{a+1}^{(a,b)}) \leq \binom{\frac{n}{2}+a+1}{a+1}^2 \leq \binom{n+1}{\frac{1}{2}n+1}^2 \leq 2^{2n+2}$$

which in turn implies that

$$\dim_K(R^{(a,b)}[Z]_{a+1}) \leq (\frac{n}{2}+2) \cdot 2^{2n+2}.$$

Together with the algorithm of Proposition 1, one obtains a Monte-Carlo test on the consistency of system consisting of (7) and (8) which has a running time of

$$\tilde{\mathcal{O}}(2^{4n})$$

bit operations (for $n = a+b$). (Note the similarity of this result with Proposition 2).

The work described in this paper has been supported in part by the European Commission through the IST Programme under Contract IST-2002-507932 ECRYPT.