New Insight into the Isomorphism of Polynomial Problem IP1S and its Use in Cryptography

Gilles Macario-Rat[1], Jérôme Plut[2], and Henri Gilbert[2]

[1] Orange Labs
38–40, rue du Général Leclerc, 92794 Issy-les-Moulineaux Cedex 9, France
gilles.macariorat@orange.com
[2] ANSSI,
51 Boulevard de la Tour-Maubourg, 75007 Paris, France
henri.gilbert@ssi.gouv.fr jerome.plut@ssi.gouv.fr

Abstract. This paper investigates the mathematical structure of the "Isomorphism of Polynomial with One Secret" problem (IP1S). Our purpose is to understand why for practical parameter values of IP1S most random instances are easily solvable (as first observed by Bouillaguet et al.). We show that the structure of the problem is directly linked to the structure of quadratic forms in odd and even characteristic. We describe a completely new method allowing to efficiently solve most instances. Unlike previous solving techniques, this is not based upon Gröbner basis computations.

1 Introduction

Multivariate cryptography is a sub area of cryptography the development of which was initiated in the late 80's [13] and was motivated by the search for alternatives to asymmetric cryptosystems based on algebraic number theory. RSA and more generally most existing asymmetric schemes based on algebraic number theory use the difficulty of solving one univariate equation over a large group (e.g. $x^e = y$ where e and y are known). Multivariate cryptography as for it, aims at using the difficulty of solving systems of multivariate equations over a small field.

A limited number of multivariate problems have emerged that can be reasonably conjectured to possess intractable instances of relatively small size. Two classes of multivariate problems are underlying most multivariate cryptosystems proposed so far, the MQ problem of solving a multivariate system of m quadratic equations in n variables over a finite field $\mathbb{F}_q$ - that was shown to be NP-complete even over $\mathbb{F}_2$ for $m \approx n$ [10]- and the broad family of the so-called isomorphism of polynomials (IP) problems.

Isomorphism of Polynomial problems can be roughly described as the equivalence of multivariate polynomial systems of equations up to linear (or affine)

bijective changes of variables. Two separate subfamilies of IP problems can be distinguished: isomorphism of polynomials with two secrets (IP2S for short) and isomorphism of polynomials with one secret (IP1S for short). A little more in detail, given two m-tuples $a = (a_1, \ldots, a_m)$ and $b = (b_1, \ldots, b_m)$ of polynomials in n variables over $\mathbb{K} = \mathbb{F}_q$, IP2S consists of finding two linear bijective transformations S of $\mathbb{K}^n$ and T of $\mathbb{K}^m$, such that $b = T \circ a \circ S$. Respectively, (computational) IP1S consists of finding one linear bijective transformations S of $\mathbb{K}^n$, such that $b = a \circ S$. Many variants of both problems can be defined depending on the value of the triplet (n, m, q), the degree d of the polynomial equations of a and b, whether these polynomials are homogeneous or not, whether S and T are affine or linear, etc. It turns out that there are considerable security and simplicity advantages in restricting oneself, for cryptographic applications, to instances involving only homogeneous polynomials of degree d and linear transformations S and T. For performance reasons, the quadratic case $d = 2$ is most frequently encountered in cryptography. Due to the existence of an efficient canonical reduction algorithm for quadratic forms, instances such that $m \geq 2$ must then be considered. The cubic case $d = 3$ is also sometimes considered, then instances such that $m = 1$ are generally encountered.

Many asymmetric cryptosystems whose security is related to the hardness of special trapdoor instances of IP2S were proposed in which all or part of the m-tuple of polynomials b plays the role of the public key and is related by secret linear bijections S and T to a specially crafted, easy to invert multivariate polynomial mapping a. Most of these systems, e.g. Matsumoto and Imai's seminal multivariate scheme C* [13], but also reinforced variants such as SFLASH and HFE [18, 16] were shown to be weak because the use of trapdoor instances of IP2S with specific algebraic properties considerably weakens the general IP2S problem. A survey of the status of the IP2S problems and improved techniques for solving homogeneous instances are presented in [1] and [4].

The IP1S problem was introduced in [16] by Patarin, who proposed in the same paper a zero-knowledge asymmetric authentication scheme named the IP identification scheme with one secret (IP1S scheme for short). This authentication scheme is inspired by the well known zero-knowledge proof for Graph Isomorphism by Goldreich et al. [11]. It can be converted into a (less practical) asymmetric signature scheme using the Fiat-Shamir transformation. The IP1S problem and the related identification scheme possess several attractive features:

- the IP1S problem can be reasonably conjectured not to be solvable in polynomial time: it has been shown in [17] that the quadratic version of IP1S (QIP1S for short) is at least as hard as the Graph Isomorphism problem (GI)[3], one of the most extensively studied problems in complexity theory. While the GI problem is not believed to be NP-complete since it is NP and co-NP and hard instances of GI are difficult to construct for small parameter values, GI is generally believed not to be solvable in polynomial time.

[3] However we recently discovered a mistake in the corresponding proof in [17], that makes us think that quadratic IP1S is not indeed as hard as GI. More precisely quadratic IP1S should be solvable in polynomial time.

– unlike the encryption or signature schemes based on IP2S mentioned above, the IP1S scheme does not use special trapdoor instances of the IP1S problem and therefore its security is directly related to the intractability of general IP1S instances.

The IP1S problem also has some loose connections with the multivariate signature scheme UOV [12], that has until now remarkably well survived all advances in the cryptanalysis of multivariate schemes. While in UOV the public quadratic function b is related to the secret quadratic function by the equation $b = a \circ S$, both a and S are unknown whereas only S is unknown in the IP1S problem.

Former results. Initial assessments of the security of practical instances of the IP1S problem suggested that relatively small public key and secret sizes - typically about 256 bits - could suffice to ensure a security level of more than 2^{64}. The IP1S scheme therefore appeared to favorably compare with many other zero-knowledge authentication schemes, e.g [21, 22, 20]. Moreover, despite advances in solving some particular instances of the IP1S problem, in particular Perret's Jacobian algorithm[4] [19], the four challenge parameter values proposed in 1996 [16] (with $q = 2$ or 2^{16}, $d = 2$ and $m = 2$, or $d = 3$ and $m = 1$) remained unbroken until 2011.

Significant advances on solving IP1S instances that are practically relevant for cryptography were made quite recently [2, 1]. Dubois in [7] and the authors of [2] were the first to notice that the IP1S problem induces numerous linear equations in the coefficients of the matrix of S and of the inverse mapping $T = S^{-1}$. When $m \geq 3$, the number mn^2 of obtained linear equations is substantially larger than the number $2n^2$ of variables. While the system cannot have full rank since the dimension of the vector space of solutions is at least 1, it can heuristically be expected to have a very small vector space of solutions that can be tried exhaustively. The authors of [2] even state that they "empirically find one solution (when the polynomials are randomly chosen)".

Therefore the most interesting remaining case appears to be $m = 2$. It is shown in [2] that the vector space of solutions of the linear equations is then isomorphic to the commutant of a non-singular $n \times n$ matrix C and that its dimension r is lower bounded by n in odd characteristic and $2n$ in even characteristic. The reported computer experiments indicate that r is extremely likely to be close to these lower bounds in practice. While for typical values of q^n the vector space of solutions is too large to be exhaustively searched, one can try to solve the equation $b = a \circ S$ over this vector space. This provides a system of quadratic equations in a restricted variable set of $r \approx n$ (resp. $r \approx 2n$) coordinates. The approach followed in [2] in order to solve this system consisted of applying Gröbner basis algorithms such as Faugère's $F4$ [8] and related computer algebra tools such as FGLM [9]. This method turned out to be quite successful: all the IP1S challenges proposed by Patarin were eventually broken in computing times ranging from less than 1 s to 1 month. This led the authors of [2] to

[4] This algorithm recovers mn linear equations in the coefficients of S and is therefore suited for solving IP1S instances such that $m \approx n$.

conclude that "[the] IP1S-Based identification scheme is no longer competitive with respect to other combinatorial-based identification schemes". However, the heuristic explanation suggested in [2], namely that the obtained system was so massively over defined that a random system with the same number of random quadratic equations would be efficiently solvable in time $O(n^9)$ with overwhelming probability, was later on shown to be false by one of the authors of [2], due to an overestimate of the number of linearly independent quadratic equations.

This is addressed in Bouillaguet's PhD dissertation [1] where the results of [2] are revisited. The main discrepancy with the findings of [2] is the observation that in all the reported experiments in odd and even characteristic, the number of linearly independent quadratic equations, that was supposed in [2] to be close to n^2, is actually bounded over by a small multiple of n and only marginally larger than r. The author writes "This means that we cannot argue that solving these equations is doable in polynomial time. An explanation of this phenomenon has eluded us so far." Despite of the surprisingly small number of linearly independent quadratic equations, nearly all instances are confirmed to be efficiently solvable for all practical values of n when the size q of the field is sufficiently small (q=2 or 3) and still solvable efficiently up to values of n of about 20. The author writes "For instance, when $q = 2$ and $n = 128$ we are solving a system of 256 quadratic equations in 256 variables over $\mathbb{F}_2$. When the equations are random this is completely infeasible. In our case, it just takes 3 minutes ! We have no clear explanation of this phenomenon."

Our contribution. The lack of explanation for the success of the attack – more precisely the puzzling fact that the number of linearly independent quadratic equations is close to n in odd characteristic and to $2n$ in even characteristic and the even more puzzling fact that nearly all instances are nevertheless solvable – motivated our research on IP1S. We revisited the former analysis and eventually found an algebraic explanation of why most random instances of the quadratic IP1S problem are efficiently solvable that leads to a new method (not based on Gröbner basis computations) to directly solve these instances. Our analysis shows in particular that in the likely cases where the characteristic is odd and the matrix C is cyclic or the characteristic is even and C is similar to a block-wise diagonal matrix with two equal cyclic $\frac{n}{2} \times \frac{n}{2}$ diagonal blocks, the quadratic equations split up in an appropriate base in small triangular quadratic systems that can be solved efficiently. The highlighted structure of the quadratic equations seems to be the essential reason why Gröbner basis computations behave so well on most instances.

The rest of this paper is organized as follows. In Section 2, we present the problem IP1S, its background and some major mathematical results used in the following sections. We then discuss in Section 3 and 4 the resolution of the problem over finite fieds of odd, resp. even characteristic.

2 The Isomorphism of Polynomial Problem with One Secret

2.1 Notations and first definitions

Let $\mathbb{K}$ be a field; for practical considerations, we shall assume that $\mathbb{K}$ is the finite field $\mathbb{F}_q$ with q elements, although most of the discussion is true in the general case.

A *(homogeneous) quadratic form in n variables* over $\mathbb{K}$ is a homogeneous polynomial of degree two, of the form $q = \sum_{i,j=1\ldots n} \alpha_{i,j} x_i x_j$, where the coefficients $\alpha_{i,j}$ belong to $\mathbb{K}$. For simplicity, we write $x = (x_i)$ for the vector with coordinates x_i. The quadratic form q can be described by the matrix with general term $\alpha_{i,j}$. Note that the matrix representation of a quadratic form is not unique: two matrices represent the same linear form if, and only if, their difference is antisymmetric.

The *polar form* associated to a quadratic form q is the bilinear form $b = \mathcal{P}(q)$ defined by $b(x, y) = q(x + y) - q(x) - q(y)$. This is a symmetric bilinear form. This can be used to give an intrinsic definition of bilinear forms (which is useful to abstract changes of bases from some proofs belows): given a vector space V, a quadratic form over V is a function $q : V \to \mathbb{K}$ such that

(i) for all $x \in V$ and $\lambda \in \mathbb{K}$, $q(\lambda x) = \lambda^2 q(x)$;
(ii) the polar form $\mathcal{P}(q)$ is bilinear.

For any matrix A, let ${}^tA$ be the transpose matrix of A and $\mathcal{P}(A)$ be the symmetric matrix ${}^tA + A$. Then if q is a quadratic form with matrix A, its polar form has matrix $\mathcal{P}(A)$. The quadratic form q is *regular* if its polar form is not singular, i.e. if it defines a bijection from V to its dual. In general, we define the *kernel* of a quadratic form to be the kernel of its polar form.

From the definition of $b = \mathcal{P}(q)$ we derive the *polarity identity*

$$2q(x) = b(x, x). \tag{1}$$

This identity obviously behaves very differently when 2 is a unit in $\mathbb{K}$ and when $2 = 0$ in $\mathbb{K}$. This forces us to use some quite different methods in both cases.

If 2 is invertible in $\mathbb{K}$ then the polarity identity (1) allows recovery of a quadratic form from its polar bilinear form. In other words, quadratic forms in n variables correspond to symmetric matrices.

Conversely, if $2 = 0$, then the polarity identity reads as $b(x, x) = 0$; in other words, the polar form is an alternating bilinear form. In this case, equality of polar forms does not imply equality of quadratic forms. Define $\Delta(A)$ as the matrix of diagonal entries of the matrix A. Then quadratic forms A and B are equal if, and only if, $\mathcal{P}(A) = \mathcal{P}(B)$ and $\Delta(A) = \Delta(B)$.

2.2 The quadratic IP1S problem

We now state the quadratic IP1S problem and give an account of its current status after the recent work of [2] and [1].

Problem 1 (Quadratic IP1S). Given two m-tuples $a = (a_1, \ldots, a_m)$ and $b = (b_1, \ldots, b_m)$ of quadratic homogeneous forms in n variables over $\mathbb{K} = \mathbb{F}_q$, find a non-singular linear mapping $S \in GL_n(\mathbb{K})$ (if any) such that $b = a \circ S$, i.e. $b_i = a_i \circ S$ for $i = 1, \ldots, m$.

Remark 1. In order not to unnecessarily complicate the presentation, our definition of the IP1S problem slightly differs[5] from the initial statement of the problem introduced in [16]. Though the name "quadratic homogeneous IP1S" might be more accurate to refer to the exact class of instances we consider, we will name it quadratic IP1S or IP1S in the sequel.

If we denote by A_i, resp. B_i any $n \times n$ matrices representing the a_i, resp. the b_i and denote by X the matrix representation of S, the conditions for the equality of two quadratic forms given in Section 2.1. allow to immediately translate the quadratic IP1S problem into equivalent matrix equations.

- If the characteristic of $\mathbb{K}$ is odd: the problem is equivalent to finding an invertible matrix X that satisfies the m polar equations: $\mathcal{P}(B_i) = {}^tX\mathcal{P}(A_i)X$
- If the characteristic of $\mathbb{K}$ is even: the problem is equivalent to finding an invertible matrix X that satisfies the polar and the diagonal equations: $\mathcal{P}(B_i) = {}^tX\mathcal{P}(A_i)X$; $\Delta(B_i) = \Delta({}^tXA_iX)$.

In the following sections we will consider IP1S instances such that $m = 2$, that are believed to represent the most "interesting" instances of IP1S as reminded above. Matrix pencils, that can be viewed as $n \times n$ matrices whose coefficients are polynomials of degree 1 of $\mathbb{K}[\lambda]$ represent a convenient way to capture the above equations in a more compact way. If we denote by A and B the matrix pencils $\lambda A_\infty + A_0$ and $\lambda B_\infty + B_0$, and by extension $\mathcal{P}(A)$ and $\mathcal{P}(B)$ the symmetric matrix pencils $\lambda\mathcal{P}(A)_\infty + \mathcal{P}(A)_0$ and $\lambda\mathcal{P}(B)_\infty + \mathcal{P}(B)_0$, the two polar equations can be written in one equation: $\mathcal{P}(B) = {}^tX\mathcal{P}(A)X$. However, as detailed in the next section, the theory of pencils is far more powerful than just a convenient notation for pairs of matrices. See for instance [3].

2.3 Mathematical background

In this Section we briefly outline a few known definitions and results related to the classification of matrices and matrix pencils and known methods for solving matrix equations that are relevant for the investigation the IP1S problem.

[5] While in [16] the isomorphism of two m-tuples quadratic polynomials comprising also linear and constant terms through a non-singular affine transformation was considered, we consider here the isomorphism of two m-tuples of quadratic forms through a non-singular linear transformation. This replacement of the original definition by a simplified definition is justified by the fact that all instances of the initial problem can be shown to be either easily solvable due to the lower degree homogeneous equations they induce or efficiently reducible to an homogeneous quadratic instance.

Basic facts about matrices. Two matrices A and B are *similar* if there exists an invertible matrix P such that $P^{-1}AP = B$ and *congruent* if there exists an invertible P such that ${}^tPAP = B$.

The matrix A is called *cyclic* if its minimal and characteristic polynomials are equal.

For any matrix A, the *commutant* of A is the algebra $\mathcal{C}_A$ of all matrices commuting with A. It contains the algebra $\mathbb{K}[A]$, and this inclusion is an equality if, and only if, A is cyclic.

For any matrix A, let $\prod p_i^{e_i}$ be the prime factorization of its minimal polynomial. Then $\mathbb{K}[A]$ is the direct product of the algebras $\mathbb{K}[x]/p_i(x)^{e_i}$; each of these factors is a local algebra with residual field equal to the extension field $\mathbb{K}[x]/p_i$.

Pencils of bilinear and quadratic forms. Let V be a $\mathbb{K}$-vector space and $Q(V)$ be the vector space of all quadratic forms on V. A *projective pencil of quadratic forms* on V is a projective line in $\mathbb{P}Q(V)$, *i.e.* a two-dimensional subspace of $Q(V)$. As a projective pencil is the image of the projective line $\mathbb{P}^1$ in $Q(V)$, it is determined by the images of the points ∞ and 0 in $\mathbb{P}^1$, which we write A_0 and A_∞.

An *affine pencil of quadratic forms* is an affine line in $Q(V)$, or equivalently a pair of elements of $Q(V)$. The affine pencil with basis (A_∞, A_0) may also be written as a polynomial matrix $A_\lambda = A_0 + \lambda A_\infty$. Given a projective pencil A of $Q(V)$, the choice of any basis (A_∞, A_0) of A determines an affine pencil.

A projective pencil is *regular* if it contains at least one regular quadratic form. An affine pencil (A_∞, A_0) is *regular* if A_∞ is regular; it is *degenerate* if the intersection of the kernels of the quadratic forms A_λ is nontrivial.

If an affine pencil is non-degenerate, then the polynomial $\det A_\lambda$ is non-zero; choosing any λ which is not a root of this polynomial proves that the associated projective pencil is regular (over $\mathbb{K}$ itself if it is infinite, and over a finite extension of $\mathbb{K}$ if it is finite). This gives a basis of the projective pencil which turns the affine pencil into a regular one. We shall therefore assume all affine pencils to be regular.

Two pencils A, B of quadratic forms are *congruent* if there exists an invertible matrix X such that ${}^tXA_\lambda X = B_\lambda$. The case $m = 2$ of the quadratic IP1S problem reduces to the Pencil congruence problem: given two affine pencils A and B, known to be congruent, exhibit a suitable congruence matrix X.

We first note that the IP1S problem easily reduces to the case where both pencils are regular. Namely, if one (and therefore both) is degenerate, then we may quotient out both spaces by the (isomorphic) kernels of the pencils; this define non-degenerate affine pencils on the quotient vector spaces, which are still congruent. Since the associated projective pencils are regular, a change of basis in the pencils (and maybe an extension of scalars) brings us to the case of two regular affine pencils.

We define pencils of bilinear forms in the same way as pencils of quadratic forms. The pencil $b_\lambda = b_0 + \lambda b_\infty$ *regular* if b_∞ is; in this case, the *characteristic endomorphism* of the pencil is the endomorphism $f = b_\infty^{-1} \circ b_0$.

The following lemma allows to decompose pencils as direct sums, with each factor having a power of an irreducible polynomial as its characteristic endomorphism.

Lemma 1. *Let b be a regular pencil of symmetric bilinear forms. Then all primary subspaces of the characteristic endomorphism f are orthogonal with respect to all forms of b.*

Proof. We have to prove the following: given any two mutually prime factors p, q of f and any $x, y \in V$ such that $p(f)(x) = 0$ and $q(f)(y) = 0$, then for all λ, we have $b_\lambda(x, y) = 0$. For this it is enough to show that $b_\infty(x, y) = 0$.

Since p, q are mutually prime, there exist u, v such that $up + vq = 1$. Note that, for all $x, y \in V$, we have $b_\infty(x, fy) = b_0(x, y) = b_0(y, x) = b_\infty(fx, y)$; therefore, all elements of $\mathbb{K}[f]$ are self-adjoint with respect to b_∞. From this we derive the following:

$$\begin{aligned} b_\infty(x, y) &= b_\infty(x,\ u(f)p(f)y + v(f)q(f)y) \\ &= b_\infty(u(f)p(f)x, y)\ +\ b_\infty(x, v(f)q(f)y) \\ &= 0. \end{aligned} \tag{2}$$

□

Explicit similarity of a matrix and its transposed. The next result is intensively used in the sequel to deal with symmetric pencils. Although this result is classic [23], we are interested with the explicit form given below.

Theorem 1. *For any matrix M, there exists a non-singular symmetric matrix T such that ${}^tMT = TM$.*

Proof. Using primary decomposition for M, we may assume that it is of the form

$$M = \begin{pmatrix} M_0 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & M_0 \end{pmatrix}, \tag{3}$$

where M_0 is the companion matrix of an irreducible polynomial $p(\lambda) = \lambda^n + \sum_{i=0}^{n-1} p_i \lambda^i$. (Note that this is not the Frobenius normal form, although it is equivalent to it as long as p is separable). We then define matrices T_0 and T by

$$T_0 = \begin{pmatrix} p_1 & \cdots & p_{n-1} & 1 \\ \vdots & \iddots & \iddots & \\ p_{n-1} & \iddots & & \\ 1 & & & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 0 & & T_0 \\ & \iddots & \\ T_0 & & 0 \end{pmatrix}. \tag{4}$$

One can easily verify that T_0 is invertible, symmetric and ${}^tM_0T_0 = T_0M_0$, and that the same is true for T and M. □

3 IP1S in characteristic different from two

Let $\mathbb{K}$ be a field of characteristic different from two[6]. In this case, the polarity identity (1) identifies quadratic forms with symmetric bilinear forms, or again with symmetric matrices with entries in $\mathbb{K}$. We shall therefore write a quadratic pencil A as $A_\lambda = A_0 + \lambda A_\infty$, where A_0 and A_∞ are symmetric matrices.

Proposition 1. *Let $A_\lambda = A_0 + \lambda A_\infty$, $B_\lambda = B_0 + \lambda B_\infty$ be two regular affine pencils.*

(i) If A_λ is congruent to B_λ, then the characteristic matrices

$$M_A = A_\infty^{-1} A_0 \quad \textit{and} \quad M_B = B_\infty^{-1} B_0$$

are similar.

(ii) Assume that M_A and M_B are similar and choose P such that $P^{-1} M_A P = M_B$. Then ${}^tPA_\lambda P = {}^tPA_\infty P(\lambda + M_B)$.

(iii) Assume that $A_\lambda = A_\infty(\lambda + M)$ and $B_\lambda = B_\infty(\lambda + M)$. Then the solutions of the pencil congruence problem are exactly the invertible X such that

$$XM = MX \quad \textit{and} \quad {}^tXA_\infty X = B_\infty. \tag{5}$$

Proof. (i). Since A_λ is regular, A_∞ is invertible and we may write $A_\lambda = A_\infty(\lambda + A_\infty^{-1}A_0)$; likewise, $B_\lambda = B_\infty(\lambda + B_\infty^{-1}B_0)$. Choose P such that ${}^tPA_\lambda P = B_\lambda$, then

$$B_\infty(\lambda + M_B) \;=\; {}^tPA_\lambda P \;=\; {}^tPA_\infty P(\lambda + P^{-1}M_A P), \tag{6}$$

which implies $P^{-1}M_A P = M_B$ as required. The same computations prove (ii).

The equations (5) follows directly from the equality ${}^tXA_\infty(\lambda + M)X = {}^tXA_\infty X(\lambda + X^{-1}MX)$. □

We now restrict ourselves to the case where the characteristic endomorphism is cyclic.

Proposition 2. *Let $A_\lambda = A_\infty(\lambda + M)$ and $B_\lambda = B_\infty(\lambda + M)$ be two regular symmetric pencils such that the matrix M is cyclic, that is, its minimal and characteristic polynomials are equal.*

Then the solutions X of the pencil congruence problem are the square roots of $A_\infty^{-1}B_\infty$ in the algebra $\mathbb{K}[M]$.

Proof. Since M is cyclic, its commutant is reduced to the algebra $\mathbb{K}[M]$; therefore, all solutions of the congruence problem are polynomials in M.

Since A_λ is symmetric, both matrices A_∞ and $A_0 = A_\infty M$ are symmetric; therefore, ${}^tMA_\infty = A_\infty M$. Since X is a polynomial in M, we deduce that also ${}^tXA_\infty = A_\infty X$.

The relation ${}^tXA_\infty X = B_\infty$ may therefore be rewritten as $A_\infty X^2 = B_\infty$, or $X^2 = A_\infty^{-1}B_\infty$. □

[6] Although this is not used in cryptography, we mention that this section also applies verbatim to the case of characteristic zero.

Theorem 2. *Let $\mathbb{K}$ be a finite field of odd characteristic and A_λ, B_λ be two regular pencils of quadrics over $\mathbb{K}^n$, congruent to each other, such that at least one is cyclic (and therefore both are). Then the pencil congruence problem may be solved using no more than $\widetilde{O}(n^3)$ operations in the field $\mathbb{K}$.*

Proof. The first step is to reduce to the case of primary components of the characteristic endomorphism. This may be done, using for example Frobenius reduction of both matrices $A_\infty^{-1}A_0$ and $B_\infty^{-1}B_0$, with a complexity of $\widetilde{O}(n^3)$ operations. This also provides the change of basis making the characteristic endomorphism of both pencils to have the same matrix.

There remains to compute a square root of $C = A_\infty^{-1}B_\infty$ in $\mathbb{K}[M]$, where now the minimal polynomial of M is p^e, with p irreducible. For this we first write C as a polynomial $g(M)$; this again requires $\widetilde{O}(n^3)$ operations. To solve the equation $y^2 = g(M)$ in the ring $\mathbb{K}[M] = \mathbb{K}[x]/p(x)^e$, we first solve it in the (finite) residual field $\mathbb{K}[x]/p(x)$, with complexity $\widetilde{O}(n^3)$ again; lifting the solution to the ring $\mathbb{K}[M]$ requires only $\widetilde{O}(n^2)$ with Hensel lifting. □

Solutions of the IP1S problem are square roots of an element C of the algebra $\mathbb{K}[M]$; therefore, the number of solutions is 2^s, where s is the number of connected components of $\mathbb{K}[M]$, that is, the number of prime divisors of the minimal polynomial of M.

Summary and Computer Experiments. The case where all the elementary divisors of $\mathcal{P}(A)$ are pairwise co-prime – or equivalently where M is cyclic – represents in practice a quite large fraction of random cases (see for instance [15]). In this case, as shown above, the number of solutions is exactly 2^s where s is the numbers of elementary divisors and solutions can be efficiently computed (in polynomial time $\mathcal{O}(n^3)$) by our method. The highlighted structure of the equations also provides some likely explanations of why Gröbner basis computation methods such as those presented in [2] were successful in this case. We give in next table results (timings) of our MAGMA script SOLVECYCLICODDPC, t is the mean execution time when solving 100 random cyclic IP1S instances, τ is the observed fraction in percent of such "cyclic" instances over random instances.

q	n	t	τ
3	80	5.s.	87.
3	128	34.s.	88.
3^{10}	32	15.s.	100.

q	n	t	τ
5	20	0.07s.	95.
5	32	0.28s.	95.
5	80	7.s.	95.
5^7	32	8.s.	100.

q	n	t	τ
7^6	32	11.s.	100.
65537	8	0.04s.	100.
65537	20	1.s.	100.

4 IP1S in Characteristic Two

Let $\mathbb{K}$ be a finite field of characteristic two. In this case, the polarity identity (1) shows that the polar form $b = \mathcal{P}(q)$ attached to a quadratic form q is an alternating bilinear form.

4.1 Pencils of alternating bilinear forms

This paragraph is a reminder of classical results. We refer the reader to [14] for the proofs.

If b is alternating and nondegenerate, then the vector space V has a *symplectic basis*, i.e. a basis $(e_1, \dots, e_n, f_1, \dots, f_n)$ such that $b(e_i, f_i) = 1$ and all other pairings are zero. In particular, the dimension of V is even. The vector E space generated by the e_i is equal to its orthogonal space $E^\perp$; such a space is called a *Lagrangian* space for b.

We recall that two matrices A and B define the same quadratic form if and only if $\mathcal{P}(A) = \mathcal{P}(B)$ and $\Delta(A) = \Delta(B)$.

Although quadratic forms only produce alternating bilinear forms in characteristic two, the following lemma about alternating forms is true in all characteristics. It proves that there exists a basis of V in which the pencil has the block-matrix decomposition

$$A_\infty = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad A_0 = \begin{pmatrix} 0 & {}^tF \\ F & 0 \end{pmatrix}; \qquad A_\infty^{-1} A_0 = \begin{pmatrix} F & 0 \\ 0 & {}^tF \end{pmatrix}. \tag{7}$$

The matrix F is called the *Pfaffian* endomorphism of A.

Lemma 2. *Let $b = (b_\infty, b_0)$ be a regular pencil of alternating bilinear forms on V. Then there exists a symplectic basis for b_∞ whose Lagrangian is stable by the characteristic endomorphism of b.*

Proof. Let f be the characteristic endomorphism of b. By Lemma 1, we may replace V by one of the primary components of f and therefore assume that the minimal polynomial of f is p^n where p is a prime polynomial. By extending scalars to $\mathbb{K}[\lambda]/p(\lambda)$ and replacing b_0 by $\lambda b_\infty + b_0$ we may assume that $p(t) = t$. We now prove the lemma by induction on $\dim V$.

Since t^n is the minimal polynomial of f and b_∞ is non-degenerate, there exists $x, y \in V$ such that $b_\infty(x, f^{n-1}y) = 1$. Let $W = \mathbb{K}[f]x \oplus \mathbb{K}[f]y$. Then we may write $V = W \oplus W^\perp$ where both W and its b_∞-orthogonal $W^\perp$ are stable by f; since $W^\perp$ satisfies the lemma by the induction hypothesis, we only need to prove it for W.

Let $a(t) = 1 + a_1 t + \cdots + a_{n-1} t^{n-1}$ be a polynomial and $x' = a(f)x$. Then we still have $b_\infty(x', f^{n-1}y) = 1$, and moreover we can choose a so that $b_\infty(x', f^i y) = 0$ for all $i = 0, \dots, n-2$. In other words, $(x', fx', \dots, f^{n-1}x', f^{n-1}y, f^{n-2}y, \dots, fy, y)$ is a symplectic basis for b_∞ on W. By construction, its Lagrangian is $\mathbb{K}[f]x$, which is obviously stable by the characteristic endomorphism f. □

Proposition 3. *Let $\mathbb{K}$ be a binary field. Any regular pencil of alternating bilinear forms is congruent to a pencil of the form*

$$A_\infty = \begin{pmatrix} 0 & T \\ T & 0 \end{pmatrix}, \quad A_0 = \begin{pmatrix} 0 & TM \\ TM & 0 \end{pmatrix}, \tag{8}$$

where M is in rational (Frobenius) normal form and T is the symmetric matrix defined in Theorem 1.

Proof. From the equation 7, choose a matrix P such that $M = P^{-1}FP$ is in rational normal form and define T as in Theorem 1. Then the coordinate change $\begin{pmatrix} P & 0 \\ 0 & {}^tP^{-1}T \end{pmatrix}$ produces the required form. □

Proposition 4. *Let A be a cyclic pencil of alternating bilinear forms. The group of automorphisms $O(A)$ is generated by the elementary transformations*

$$G_1(X) = \begin{pmatrix} 1 & X \\ 0 & 1 \end{pmatrix}, \quad G_2(X) = \begin{pmatrix} 1 & 0 \\ X & 1 \end{pmatrix}, \quad G_3(X) = \begin{pmatrix} X & 0 \\ 0 & X^{-1} \end{pmatrix}, \quad G_4 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{9}$$

where $X \in \mathbb{K}[M]$, X invertible for $G_3(X)$.

The first three transformations generate the subgroup of *positive* automorphisms of A. This is a subgroup of index two of the orthogonal group [6].

Proof. Direct computation shows that the matrices in $O(A)$ are the matrices $\begin{pmatrix} X_1 & X_2 \\ X_3 & X_4 \end{pmatrix}$ such that all X_i commute with M (and therefore, since M is cyclic, belong to the commutative algebra $\mathbb{K}[M]$), and $X_1X_4 + X_2X_3 = 1$. This implies that at least one of X_1X_4 and X_2X_3 is invertible; depending on this, we may write at least one of the two decompositions:

$$\begin{aligned} X &= G_2(X_1^{-1}X_3) \cdot G_3(X_1) \cdot G_1(X_1^{-1}X_2) \\ &= G_2(X_2^{-1}X_4) \cdot G_3(X_2) \cdot G_1(X_2^{-1}X_1) \cdot G_4 \end{aligned} \tag{10}$$

□

4.2 Pencils of quadratic forms

The following proposition deals with the diagonal terms of a quadratic form in the cyclic case. We recall that, using the notations of Theorem 1, $\mathbb{L} = \mathbb{K}[M_0]$ is an extension field of $\mathbb{K}$, and $\mathbb{K}[M]$ is the $\mathbb{L}$-algebra generated by

$$H = \begin{pmatrix} 0 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & 0 \end{pmatrix}. \tag{11}$$

This is a local algebra, whose maximal ideal is generated by H. We write v_H for the valuation in this algebra; for any $X \in \mathbb{K}[M] = \mathbb{L}[H]$, $v_H(X)$ is the unique integer such that $X = H^{v_H(X)}U$ with U invertible.

We write $\varphi(X) = X^2$ for the Frobenius map of $\mathbb{L}$. Since this is a finite field, the Frobenius map is bijective. It extends to $\mathbb{K}[M]$ as $\varphi(\sum x_i H^i) = \sum x_i^2 H^i$.

Proposition 5. *Define matrices M of size n, M_0, T_0 of size $e = n/d$ as in Theorem 1.*

(i) The $\mathbb{K}$-linear map $\mathbb{L} \mapsto \mathbb{K}^e$, $X \mapsto \Delta(T_0X)$ is an isomorphism.

(ii) For any diagonal matrix D of size e, there exists a (unique) matrix $C = \psi_0(D) \in \mathbb{L}$ such that, for all $X \in \mathbb{L}$:

$$\Delta({}^tXDX) \;=\; \Delta(T_0CX^2). \tag{12}$$

(iii) Let D be a diagonal matrix of size n, written as blocks $D_0, \ldots, D_{d-1}$, and write $X \in \mathbb{K}[M]$ as $X = x_0 + \cdots + x_{d-1}H^{d-1}$ with $x_i \in \mathbb{L}$. Also define $\psi(D) = \sum \psi_0(D_i)H^i \in \mathbb{K}[M]$. Then we have the relation in $\mathbb{K}[M]$

$$\psi(\Delta({}^tXDX)) = \varphi(X) \cdot \psi(D). \tag{13}$$

Proof. (i) Since $2 = 0$ in $\mathbb{K}$, for any symmetric matrix A and any X, we have

$$\Delta({}^tX\Delta(A)X) = \Delta({}^tXAX). \tag{14}$$

Since the space $\mathbb{L}$ has dimension e over $\mathbb{K}$, we only have to check injectivity. Assume $\Delta(T_0X) = 0$ with $X \neq 0$; since $\mathbb{L}$ is a field, X is invertible. Let $Y = \varphi^{-1}(X^{-1})$. We then have

$$\Delta(T_0) = \Delta(T_0XY^2) = \Delta({}^tY(T_0X)Y) = \Delta({}^tY\Delta(T_0X)Y) = 0. \tag{15}$$

Let $p(x) = p_0 + \cdots + p_{e-1}x^{e-1} + x^e$ be the minimal polynomial of M_0. From $\Delta(T_0) = 0$ we deduce that $p_{e-1} = p_{e-3} = \cdots = 0$, which contradicts the irreducibility of p.

(ii) Let $C \in \mathbb{L}$ such that $\Delta(C) = D$; applying (14) to the symmetric matrix T_0C and using the symmetry of T_0M_0 yields

$$\Delta(T_0CX^2) = \Delta({}^tXT_0CX) = \Delta({}^tX\Delta(T_0C)X) = \Delta({}^tXDX). \tag{16}$$

(iii) From direct computation we find that the diagonal blocks of ${}^tXDX$ are $B_m = \sum_{i+j=m} {}^tX_iD_jX_i$; hence $\Delta(B_m) = \sum \Delta(T_0\psi_0(D_j)X_i^2)$ and $\psi_0(B_m) = \sum \psi_0(D_j)\,\varphi(X_i)$. □

For any binary field $\mathbb{K}$, we write $\wp(\mathbb{K})$ for the set of elements $x^2 + x \in \mathbb{K}$. This is an additive subgroup of index two of $\mathbb{K}$, and the characteristic-two analogue of the multiplicative group of squares. We fix an element δ of $\mathbb{L} \smallsetminus \wp(\mathbb{L})$.

Proposition 6. *Any regular pencil of quadratic forms is congruent to a pencil of the form*

$$A_\infty = \begin{pmatrix} A_1 & T \\ 0 & A_2 \end{pmatrix}, \quad A_0 = \begin{pmatrix} A_3 & TM \\ 0 & A_4 \end{pmatrix}, \tag{17}$$

where M, T are as in Prop. 3 and A_i are diagonal matrices, such that with $\alpha_i = \psi(A_i)$, the pair (α_1, α_2) is either $(0, 0)$, $(H^m, 0)$, or $(H^m, \delta H^{d-1-m})$ for $0 \leq m \leq (d-1)/2$. Moreover, these cases are mutually exclusive.

We shall say that a pencil in this form is *reduced*, and call the values α_i the *characteristics* of A. The image modulo $\wp(\mathbb{L})$ of the coefficient $\alpha_{2,d-1-m}$ is known as the *Arf invariant* [14] of A_∞.

Proof. By Prop. 3, we may compute bases in which the pencils of polar forms have the form (8). In the same bases the pencils have the form (17) with M, T, M_0, T_0 as in Theorem 1 for some diagonal matrices A_i.

We use the elementary transformations $G_i(X)$ from (9). Let $X = x_0 + \cdots + x_{d-1}H^{d-1} \in \mathbb{K}[M]$. We define

$$\theta(X) = \psi(\Delta(T\,X)) = \sum_{2i \geq (d-1)} x_{2i-(d-1)} H^i. \tag{18}$$

The effects of the elementary transformations $G_i(X)$ on the pair (α_1, α_2) are:

$$\begin{aligned} G_1(X): &\quad \alpha_2 \leftarrow \alpha_2 + \varphi(X)\,\alpha_1 + \theta(X), \quad \alpha_1 \leftarrow \alpha_1; \\ G_2(X): &\quad \alpha_1 \leftarrow \alpha_1 + \varphi(X)\,\alpha_2 + \theta(X), \quad \alpha_2 \leftarrow \alpha_2; \\ G_3(X): &\quad \alpha_1 \leftarrow \varphi(X)\,\alpha_1, \quad \alpha_2 \leftarrow \varphi(X^{-1})\,\alpha_2; \\ G_4: &\quad \alpha_1 \leftrightarrow \alpha_2. \end{aligned} \tag{19}$$

Using transformations G_4 and G_3, we may assume that $\alpha_1 = H^m$ for $0 \leq m \leq d$ and α_2 has valuation $\geq m$. The transformation $G_2(X)$ then reads as:

$$\alpha_{2,d-1-i} \leftarrow \alpha_{2,d-1-i} + x^2_{d-1-i-m} + x_{d-1-2i}, \tag{20}$$

where $x_{d-1-2i} = 0$ for $d-1-2i < 0$. The equation $\alpha_{2,d-1-i} \leftarrow 0$ has a solution for all i except for $i = m$, where it is of the form $x^2_{d-1-2m} + x_{d-1-2m} = C$. Hence, we may assume that α_{d-1-m} is either 0 or δ, and all others α_i are zero.

Finally, note that if $m \geq d/2$, then $\alpha_1 = H^m$ is in the image of θ; therefore, a transformation of the form $G_1(X)$ allows us to replace α_1 with 0 in this case. □

The pencil $A = (A_0, A_\infty)$ is called *semi-vanishing* if $\alpha_1 = 0$, and *vanishing* if both pencils (A_0, A_∞) and (A_{∞,A_0}) are semi-vanishing.

Proposition 7. *Any vanishing pencil of quadrics is isomorphic to a pencil with the characteristics* $(0, 0, H^m, 0)$ *with* $m \geq d/2$.

Proof. Let A be a vanishing pencil. This means that A is isomorphic to a pencil with the characteristics $(0, 0, \alpha_3, \alpha_4)$ with $v_H(\alpha_3), v_H(\alpha_4) \geq d/2$. The transformations preserving $\alpha_1 = \alpha_2 = 0$ are of the form $G_1(x)G_3(\varphi^{-1}(u^{-1}))G_2(y)$ with $\theta(x) = \theta(y) = 0$, and the image of (α_3, α_4) is (α'_3, α'_4) such that

$$\begin{aligned} u\alpha'_3 &= \alpha_3 + \alpha_4\varphi(x) + \theta(H\,x), \\ u\alpha_4 &= \alpha'_4 + \alpha'_3\varphi(y) + \theta(H\,y). \end{aligned}$$

From the second equation, we may assume that $\alpha_4 = 0$, unless $v_H(\alpha_3) = d/2$ where $\alpha_4 \in \{0, \delta H^{d/2}\}$. In this last case however, the first equation allows the change to $\alpha_3 = H^m$ with $m \geq d/2 + 1$. □

Theorem 3. *Let* A, A' *be two congruent cyclic pencils of quadratic forms. Then it is possible to compute an isomorphism between* A *and* A' *in polynomial time.*

Proof. By Prop. 6, we may assume that A, A' are reduced. The vanishing (or semi-vanishing) case is taken care of by Prop. 7. We may therefore assume that A is not semi-vanishing and that $\alpha_1 = \alpha'_1 \mid \alpha_2, \alpha'_3, \alpha_4$. Let $\beta_i \in \mathbb{L}[H]$ be such that

$$\alpha_2 = \alpha'_1\beta_2, \qquad \alpha_3 = \alpha'_1\beta'_3, \qquad \alpha_4 = \alpha'_1\beta_4. \tag{21}$$

According to (19), a transformation of the form $G_2(x)G_3(\varphi^{-1}(u^{-1}))G_1(y)$ is an isomorphism between A and A' if and only if it satisfies the equations

$$\begin{aligned} u\alpha'_1 &= \alpha_1 + \alpha_2\varphi(x) + \theta(x), \\ u\alpha_2 &= \alpha'_2 + \alpha'_1\varphi(y) + \theta(y), \\ u\alpha'_3 &= \alpha_3 + \alpha_4\varphi(x) + \theta(M\,x), \\ u\alpha_4 &= \alpha'_4 + \alpha'_3\varphi(y) + \theta(M\,y). \end{aligned} \tag{22}$$

Since A is reduced, $v_H(\alpha_1) < v_H(\theta(x))$, and therefore the first equation determines an invertible u. Eliminating u and performing a invertible linear combination of the last three equations yields the equations on (x, y):

$$\begin{array}{rrrl} \alpha'_1\beta_2^2\varphi(x) + \alpha'_1\varphi(y) + \beta_2\theta(x) + \theta(y) & & & = \alpha_1\beta_2 + \alpha'_2, \\ \alpha'_1(\beta_2\beta'_3 + \beta_4)\varphi(x) + \beta'_3\theta(x) & & + \theta(Mx) & = \alpha_1\beta'_3 + \alpha_3, \\ \beta_4\theta(x) + \beta'_3\theta(y) & + \beta_2\theta(Mx) & + \theta(My) & = \\ & & & \alpha_1\beta_4 + \alpha'_2\beta'_3 + \alpha_3\beta_2 + \alpha'_4. \end{array} \tag{23}$$

Let $z = y + \varphi^{-1}(\beta_2^2)x$ and let $\alpha = \alpha'_1$, $\beta = \beta'_3 + M_0$ and $\gamma = \beta_4 + \beta_2\beta'_3$. We deduce from (26) that $\varphi(z) = \beta_2^2\varphi(x) + \varphi(y)$ and $\theta(z) = \beta_2\theta(x) + \theta(y)$, and the system (23) becomes

$$\begin{cases} \alpha\varphi(z) + \theta(z) & & = C, \\ \alpha\gamma\varphi(x) + \beta\theta(x) & + \theta(Hx) & = C', \\ \gamma\theta(x) + \beta\theta(z) & + \theta(Hz) & = C''. \end{cases} \tag{24}$$

Proposition 11 explains how to solve such a system in $\mathbb{L}[H]$. □

4.3 Solving the semi-linear equations of the IP1S problem

We consider the algebra $A = \mathbb{L}[H]/H^n$ equipped with the Frobenius endomorphism φ and the linear endomorphisms θ defined in (18) and ω defined by

$$\omega(\sum x_i H^i) = \sum_{2i+1 \le d-1} x_{2i+1} H^i. \tag{25}$$

We check that the operators θ and ω are semi-linear in the sense that

$$\varphi(a)\theta(x) = \theta(a^2x); \qquad \varphi(a)\omega(x) = \omega(a^2x). \tag{26}$$

We also define the *pseudo-inverse* of an element $x = x'H^r \in A$, where x' is invertible, as

$$\widehat{x} = \frac{1}{x'}H^{n-r}. \tag{27}$$

This is well-defined if $r = v_H(x) \leq d/2$. The pseudo-inverse of x generates the annulator ideal of x, and has the following properties:

$$a \cdot \widehat{ab} = \widehat{b}; \qquad \varphi(\widehat{a}) = \widehat{\varphi(a)}; \qquad \theta(\widehat{a^2}\ x) = \varphi(\widehat{a})\,\omega(x). \tag{28}$$

Proposition 8. *For all b, c, $d \in A$, the equation*

$$\varphi(x) \;=\; b\,\theta(x) + c\,\theta(Hx) + d \tag{29}$$

has exactly one solution if b is not invertible, and zero or two solutions if b is invertible. It is possible to compute these solutions using no more than $O(n \log n)$ operations in $\mathbb{L}$.

Proof. The map $x \mapsto \varphi^{-1}(b\theta(x) + c\theta(Hx) + d)$ is contracting for the H-adic valuation on A/H^{n-1}, and has therefore a unique solution modulo H^{n-1}. Solving for the coefficient of H^{n-1} yields an Artin-Schreier equation if b is invertible, and a pseudo-linear equation if H divides b. □

Proposition 9. *For all b, c, $d \in A$ and $r \leq n/2$, the equation*

$$\varphi(x) \;\equiv\; b\,\omega(x) + c\,\omega(Hx) + d \pmod{H^r} \qquad (x \in L/H^{2r}) \tag{30}$$

is solvable using at most $O(r^2)$ operations in $\mathbb{L}$.

Proof. Let $m = \min(v_H(b), v_H(c))$. The first $2m-1$ equations of the system are of the form $x_i^2 = c_i x_0 + d_i x_1 + \cdots + c_m x_{2(i-m)} + d_m x_{2(i-m)+1}$; since $i > 2(i-m)+1$, this is triangular and has therefore unique solutions $x_0, \ldots, x_{2m-2}$. The equations for x_{2m-1} and x_{2m} read

$$\begin{array}{lllll} x_{2m-1}^2 = d_{2m-1} & +c_{2m-1}x_0 + b_{2m-1}x_1 + \ldots & +c_m x_{2m-2} + b_m x_{2m-1}, \\ x_{2m}^2 \;\; = d_{2m} & +c_{2m}x_0 + b_{2m}x_1 + \ldots & +c_m x_{2m} + b_m x_{2m+1}. \end{array} \tag{31}$$

If $b_m \neq 0$, then the first equation is an Artin-Schreier equation on x_{2m-1}; else $c_m \neq 0$ and the second equation is an Artin-Schreier equation on x_{2m}. All the equations for x_{2m+i} with $i \geq 1$ have the free variable x_{2m+2i} or $x_{2m+2i+1}$. □

Proposition 10. *For any a, b, c, $d \in A$, the equation*

$$a\varphi(x) = b\theta(x) + c\theta(Hx) + ad \tag{32}$$

is solvable in A using no more than $O(n^2)$ operations in the field $\mathbb{L}$.

Proof. Assume that x is a root of (32). Then $y = \varphi^{-1}(a^2)x$ is a root of

$$\varphi(y) = b\theta(y) + c\theta(Hy) + d \pmod{\widehat{a}}. \tag{33}$$

Conversely, let y be one of the (at most two) solutions of (33), computed in polynomial time with Prop. 8. Since $v_H(y) \geq 2v_H(a)$, we may write $y = \widehat{\varphi^{-1}(a^2)}x'$ with $x' \in A$, which is then a solution of (32) modulo $\widehat{a}$. Write $x = x' + \widehat{\varphi^{-1}(a^2)}x''$. Equation (18) is then equivalent to an equation of the form $\varphi(x'') = b\omega(x'') + c\omega(Hx'') + C \pmod{a}$, which can be solved via Prop. 9. □

Proposition 11. *The system* (24) *is solvable in* A *using at most* $O(n^2)$ *operations in the field* $\mathbb{L}$.

Proof. By Prop. 10, we can find solutions x' and z' of the first two equations of (24), respectively modulo $\widehat{\alpha}$ and modulo $\widehat{\alpha\gamma}$. Write $x = x' + \varphi^{-1}(\widehat{(\alpha\gamma)^2})x''$ and $z = z' + \varphi^{-1}(\widehat{\alpha^2})z''$: then, using the rules (28), the system (24) is equivalent to the equations on (x'', z'')

$$\begin{cases} \varphi(z'') \equiv \omega(z'') & +F(z') & \pmod{\alpha} \\ \varphi(x'') \equiv \beta\,\omega(x'') + \omega(Hx'') & +F'(x') & \pmod{\alpha\gamma} \\ \quad 0 \quad \equiv \beta\,\omega(z'') + \omega(Hz'') + \omega(x'') & +F''(z', x'), & \pmod{\alpha} \end{cases} \tag{34}$$

where the various $F()$ are constants in A. For any solution z'' of the first equation, the remaining equations on x'' are of the form

$$\varphi(x'') \equiv \omega(Hx'') + C \pmod{\alpha\gamma}, \qquad \omega(x'') \equiv C' \pmod{\alpha}, \tag{35}$$

where both constants C, C' depend on x' and z. Write $x'' = \sum x_i H^i$. The second equation determines all coefficients x_{2i+1}, while the first one is of the form $x_i^2 + x_{2i} = C_i$. For $i = 0$, this is an Artin-Schreier equation; for all $i \geq 1$, this equation uniquely determines the value x_{2i}. □

5 Conclusion and future work

We have shown that special instances of the quadratic homogeneous IP1S problem with $m = 2$ equations can be solved in polynomial time. These instances are those where the characteristic endomorphism of the pencil (or its Pfaffian) is cyclic, and represent in practice a large fraction of generic instances. We have since also studied the case where the characteristic endomorphism is no longer cyclic and found similar results to be published. We also believe that the results may be extended to IP1S problem with more than 2 equations, thus proving that the original (quadratic) IP1S problem is solvable in polynomial time.

References

1. C. Bouillaguet. *Études d'hypothèses algorithmiques et attaques de primitives cryptographiques*. PhD thesis, Université Paris-Diderot – École Normale Supérieure, 2011.
2. Charles Bouillaguet, Jean-Charles Faugère, Pierre-Alain Fouque, and Ludovic Perret. Practical cryptanalysis of the identification scheme based on the isomorphism of polynomial with one secret problem. In Catalano et al. [5], pages 473–493.
3. Charles Bouillaguet, Pierre-Alain Fouque, and Gilles Macario-Rat. Practical key-recovery for all possible parameters of sflash. In Dong Hoon Lee and Xiaoyun Wang, editors, *ASIACRYPT*, volume 7073 of *Lecture Notes in Computer Science*, pages 667–685. Springer, 2011.

4. Charles Bouillaguet, Pierre-Alain Fouque, and Amandine Véber. Graph-theoretic algorithms for the "isomorphism of polynomials" problem. *IACR Cryptology ePrint Archive*, 2012:607, 2012.
5. Dario Catalano, Nelly Fazio, Rosario Gennaro, and Antonio Nicolosi, editors. *Public Key Cryptography - PKC 2011 - 14th International Conference on Practice and Theory in Public Key Cryptography, Taormina, Italy, March 6-9, 2011. Proceedings*, volume 6571 of *Lecture Notes in Computer Science*. Springer, 2011.
6. Jean Dieudonné. Pseudo-discriminant and Dickson invariant. *Pacific J. Math*, 5:907–910, 1955.
7. Vivien Dubois and Jean-Gabriel Kammerer. Cryptanalysis of cryptosystems based on non-commutative skew polynomials. In Catalano et al. [5], pages 459–472.
8. Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases (F4). *Journal of Pure and Applied Algebra*, 139(1–3):61–88, June 1999.
9. Jean-Charles. Faugère, Patrizia Gianni, Daniel Lazard, and Teo Mora. Efficient Computation of Zero-dimensional Gröbner Bases by Change of Ordering. *Journal of Symbolic Computation*, 16(4):329–344, 1993.
10. M.R Garey and D.S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness*. W. H. Freeman & Co, 1979. Ch. 7.2: Algebraic Equations over GF(2).
11. Oded Goldreich. *The Foundations of Cryptography - Volume 1, Basic Techniques*. Cambridge University Press, 2001.
12. Aviad Kipnis, Jacques Patarin, and Louis Goubin. Unbalanced oil and vinegar signature schemes. In Jacques Stern, editor, *EUROCRYPT*, volume 1592 of *Lecture Notes in Computer Science*, pages 206–222. Springer, 1999.
13. Tsutomu Matsumoto and Hideki Imai. Public quadratic polynominal-tuples for efficient signature-verification and message-encryption. In Christoph G. Günther, editor, *EUROCRYPT*, volume 330 of *Lecture Notes in Computer Science*, pages 419–453. Springer, 1988.
14. John W. Milnor and Dale Husemoller. *Symmetric bilinear forms*. Springer-Verlag, 1973.
15. Peter M. Neumann and Cheryl E. Praeger. Cyclic matrices over finite fields. *J. London Math. Soc. (2)*, 52(2):263–284, 1995.
16. J. Patarin. Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. In *Eurocrypt '96*, volume 1070 of *Lecture Notes in Computer Science*, pages 33–48. Springer-Verlag, 1996.
17. Jacques Patarin, Louis Goubin, and Nicolas Courtois. Improved algorithms for isomorphisms of polynomials. In Kaisa Nyberg, editor, *EUROCRYPT*, volume 1403 of *Lecture Notes in Computer Science*, pages 184–200. Springer, 1998.
18. Jacques Patarin, Louis Goubin, and Nicolas Courtois. C^*_{-+} and HM: Variations Around Two Schemes of T. Matsumoto and H. Imai. In Kazuo Ohta and Dingyi Pei, editors, *ASIACRYPT*, volume 1514 of *Lecture Notes in Computer Science*, pages 35–49. Springer, 1998.
19. Ludovic Perret. A fast cryptanalysis of the isomorphism of polynomials with one secret problem. In *Advances in Cryptology - EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 354–370. Springer, 2005.
20. David Pointcheval. A new identification scheme based on the perceptron problem. In *Advances in Cryptology - EUROCRYPT 1995*, volume 921 of *Lecture Notes in Computer Science*, pages 319–328. Springer, 1995.
21. Adi Shamir. An efficient identification scheme based on permuted kernels. In *Advances in Cryptology - CRYPTO 1989*, volume 435 of *Lecture Notes in Computer Science*, pages 606–609. Springer, 1989.

22. Jacques Stern. Designing identification schemes with keys of short size. In *Advances in Cryptology - CRYPTO 1994*, volume 839 of *Lecture Notes in Computer Science*, pages 164–173. Springer, 1994.
23. Olga Taussky and Hans Zassenhaus. On the similarity transformation between a matrix and its transpose. *Pacific J. Math.*, 9:893–896, 1959.

A Complexity, Timings, and Other Considerations

All the experimental results have been obtained with an Opteron 850 2.2GHz, with 32 GBytes of Ram. The systems associated with the instance of the problems and their solutions have been generated using the MAGMA software, version 2.13-15. MAGMA scripts cited in this paper can be obtained from the authors.