New insight into the Isomorphism of Polynomials problem IP1S and its use in cryptography

G. Macario-Rat[1], J. Plût[2], H. Gilbert[3]

[1]Orange Labs, gilles.macario-rat@orange.fr

[2]ANSSI, jerome.plut@ssi.gouv.fr

[3]ANSSI, henri.gilbert@ssi.gouv.fr

2013-12-02

Isomorphism of polynomials with one secret

We consider a field K and the algebra $K[x_1, \ldots, x_n]$ of polynomials in n variables.

Definition (Isomorphic polynomials)

Two families of polynomials $(a_1, \ldots, a_m)$ and $(b_1, \ldots, b_m)$ are *isomorphic* if they are related by a bijective linear transformation s of the variables $(x_1, \ldots, x_n)$:

$$a_i(x_1, \ldots, x_n) = b_i(s_1(x_1, \ldots, x_n), \ldots, s_n(x_1, \ldots, x_n)).$$

In cryptographical applications,the families a and b are public and the transformation s is the secret (e.g. the identification protocol of [Patarin 1996]).

The IP1S problem

Definition (Isomorphism of polynomials with one secret)

Given two families of polynomials (a_i) and (b_i):

Decisional IP1S Determine if they are isomorphic.

Computational IP1S If the polynomials are known in advance to be isomorphic, compute an isomorphism s.

Other common related problems:

MQ Find a common root to a family of multivariate quadratic equations (NP-complete).

IP2S Allow a linear combination of the polynomials: $t \circ a \circ s = b$.

Parameters of the IP1S problem

m	Number of polynomials	(1 or 2)
n	Number of variables	(large)
d	Degree of the polynomials	(2 or 3)
K	Base field	

- The IP1S problem is easier (overdetermined) with more than 2 polynomials.
- Key size depends on the number of polynomials and on their degree.
- The complexity of attacks depends on the number of variables.

This work focuses on the case of **two homogeneous quadratic polynomials** over a finite field **of any characteristic**.

Previous algorithms

- [Bouillaguet, Faugère, Fouque, Perret 2011]: transform the problem to an overdetermined system of quadratic and linear equations.
  - Solve experimentally the systems with Gröbner bases in time $\widetilde{O}(n^6)$.
  - Solved all the quadratic IP1S challenges from [Patarin 1996]:

q	n
2	16
2^4	6
2	32

- This work: use structure theorems on (pairs of) quadratic forms to reduce them to canonical forms.
  - Uses mainly linear algebra and polynomial algebra (no Gröbner bases).
  - Requires separate treatment depending on the characteristic.

Quadratic IP1S for $m = 1$

What about IP1S for **one** polynomial?

- The case $m = 1$ corresponds to isomorphism of quadratic forms of n variables.
- To a quadratic form q we associate the *polar form* b defined by

$$b(x, y) = q(x + y) - q(x) - q(y).$$

- This is a symmetric bilinear form. It satisfies the *polarity identity*

$$2\,q(x) = b(x, x).$$

- If $2 \neq 0$ in K, then this means that quadratic and symmetric bilinear forms are really the same. The bilinear forms are classified by their Gauß reduction.

Regularity of bilinear pencils

What about IP1S for **two** polynomials?

- A *bilinear pencil* is an affine line in the space of bilinear forms:

$$\lambda \longmapsto b_\lambda = b_0 + \lambda b_\infty$$

defined by two bilinear forms b_∞, b_0. It is called

degenerate if $\det b_\lambda = 0$ for all λ,

regular if b_∞ is regular (= invertible).

- Any pencil is a direct sum

$$\text{(non-degenerate pencil)} \quad \oplus \quad \text{(zero pencil)}.$$

- If (b_∞, b_0) is not degenerate, then by replacing b_∞ by b_λ where $\det b_\lambda \neq 0$, we may assume that it is regular.
(this may require a (small) extension of scalars).

Isomorphism of regular bilinear pencils

- If (b_λ) is a regular pencil, then $m_b = b_\infty^{-1} b_0$ is an endomorphism of K^n, which we call the *characteristic automorphism* of b. We may then write
$$b_\lambda = b_\infty(\lambda + m_b).$$
- An isomorphism between the pencils (a_λ) and (b_λ) is a bijective linear map s such that ${}^t s \cdot a_\lambda \cdot s = b_\lambda$, which is equivalent to
$${}^t s \cdot a_\infty \cdot s = b_\infty \qquad \text{and} \qquad s^{-1} \cdot m_a \cdot s = m_b.$$
- If (a_λ) and (b_λ) are isomorphic, then m_a and m_b are similar, and we may assume that they are equal.
- The IP1S problem becomes:
$${}^t s \cdot a_\infty \cdot s = b_\infty \qquad \text{and} \qquad s \text{ commutes with } m.$$

where a_∞, b_∞ and $a_0 = a_\infty m$, $b_0 = b_\infty m$ are symmetric.

Isomorphism of cyclic bilinear pencils

The pencil (a_λ) is *cyclic* if the characteristic endomorphism m_a is cyclic (its characteristic polynomial is equal to its minimal polynomial).

- Random instances of IP1S are generally cyclic.
- The commuting space of m_a is reduced to the ring of polynomials $K[m_a]$.
- The fact that $a_\infty\, m = {}^{\mathrm{t}}m\, a_\infty$ means that, for all s commuting with a_∞, the same equation $a_\infty\, s = {}^{\mathrm{t}}s\, a_\infty$ holds.
- The relation ${}^{\mathrm{t}}s\, a_\infty\, s = b_\infty$ simplifies to

$$a_\infty\, s^2 = b_\infty, \qquad \text{or} \qquad s^2 = a_\infty^{-1}\, b_\infty, \quad s \in K[m].$$

- When K is a finite field, this is easy to solve.

Cyclic IP1S when $2 \neq 0$

Theorem (Solving cyclic IP1S in odd characteristic)

Let K be a finite field with odd characteristic and (a_λ), (b_λ) be two isomorphic cyclic pencils of quadratic forms of dimension n.
It is possible to compute an isomorphism between (a_λ) and (b_λ) using no more than $\widetilde{O}(n^3)$ operations in K.

- Computing the minimal polynomial of $m = m_a$.
- Computing square roots in the residual fields of $K[m]$.
- Lifting (Hensel) to the localizations of $K[m]$.
- Chinese remainders to compute the solution of $s^2 = a_\infty^{-1} b_\infty^{-1}$ in $K[m]$.

Moreover, we know the exact number of solutions to the IP1S problem.

Computer experiments for random instances

q	n	t (s)	% cyclic
3	80	5	87
3	128	34	88
3^{10}	32	15	100

q	n	t (s)	% cyclic
5	20	0.07	95
5	32	0.28	95
5	80	7	95

q	n	t (s)	% cyclic
7^6	32	11	100
65537	8	0.04	100
65537	20	1	100

- Opteron 850 2.2 GHz, 32 GB RAM.
- MAGMA version 2.13-15.

Quadratic forms in characteristic two

- When $2 = 0$ in K, the polarity identity reads $b(x, x) = 0$, *i.e.* the polar form is an **alternating** bilinear form.
- The polarity map is not a bijection.
- In general, a quadratic form has the decomposition

$$\underbrace{(\text{regular quadratic form})}_{\text{even dimension}} \quad \oplus \quad (\text{sum of squares}).$$

  The sum of squares is easy (semi-linear). Thus we may assume that the polar pencil is regular.
- We first compute all possible isomorphisms for the polar pencils, and then look for an isomorphism that has the right action on the diagonal coefficients.

Pencils of alternating bilinear forms

Theorem (Classification of alternating pencils)

Any regular pencil of alternating forms may be written, in a suitable basis

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

where T is an invertible symmetric matrix such that TM is symmetric.

- The endomorphism M is the *Pfaffian* of (A_λ). We may select an appropriate representative of M in its conjugacy class (so that for IP1S, we again have $M = M_A = M_B$), and T depends only on M.
- If the quadratic pencils (A_λ) and (B_λ) are isomorphic, we may assume that both polar pencils are equal, and of the above form.
- The pencil is called *cyclic* if M is cyclic.

Automorphisms of alternating pencils

Theorem (Structure of the orthogonal group)

The automorphisms of a cyclic pencil of alternating forms are generated by the matrices

$$G_1(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \quad G_2(x) = \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix},$$

$$G_3(x) = \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}, \quad G_4 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

where $x \in K[M]$.

We actually have a LU decomposition: any (positive) automorphism is of the form $G_2(y)G_3(u)G_1(x)$ for $x, y \in K[M]$ and $u \in K[M]^\times$.

Normal form for alternating pencils

- We may assume that the minimal polynomial f of M is of the form $f = f_0^d$, where f_0 is irreducible.
- In this case, M is similar to $\begin{pmatrix} M_0 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & \\ 0 & & & M_0 \end{pmatrix}$, where M_0 is the companion matrix of f_0. (This is almost the Frobenius normal form).
- For simplicity, we present here only the case where $M_0 = 0$. In this case, T is the anti-diagonal matrix.
- We map diagonal matrices to $K[M]$ in the following way:

$$A = \mathrm{diag}(a_0, \ldots, a_{n-1}) \longmapsto \alpha = \sum a_i M^i \in K[M].$$

Quadratic pencils in characteristic two

The IP1S problem reduces to: given the matrices T and M as above and diagonal matrices A_i and B_i, compute an isomorphism between

$$\begin{pmatrix} A_1 & T \\ 0 & A_2 \end{pmatrix}, \begin{pmatrix} A_3 & TM \\ 0 & A_4 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} B_1 & T \\ 0 & B_2 \end{pmatrix}, \begin{pmatrix} B_3 & TM \\ 0 & B_4 \end{pmatrix}.$$

We represent the diagonal matrices by elements α_i and β_i of $K[M]$.

Action of the orthogonal group on the diagonal coefficients

- Let A be diagonal, $x \in K[M]$, and A' be the diagonal of ${}^t x\, A\, x$. Then
$$\alpha' = \varphi(x)\,\alpha,$$
where φ is the Frobenius map on $K[M]$: $\varphi(\sum x_i M^i) = \sum x_i^2 M^i$.
- For $x = \sum x_i M^i \in K[M]$, we define
$$\theta(x) = \psi(\text{diagonal}(TX)) = \sum x_{d-1-2i} M^{d-1-i}.$$

Local equations for IP1S in $K[M]$

Let $s = G_2(x)\, G_3(u)\, G_1(y)$ be an orthogonal map. The action of s on the diagonal coefficients is described by **four semi-linear equations** equations on x, y, u in the algebra $K[M]$.

We can eliminate u and perform a linear change of variables to reduce IP1S to a system of the form

$$\begin{cases} \alpha\varphi(z) & + & \theta(z) & & & = & C, \\ \alpha\gamma\varphi(x) & + \beta\theta(x) & & & +\theta(Mx) & = & C', \\ & & \gamma\theta(x) + \beta\theta(z) & & +\theta(Mz) & = & C''. \end{cases}$$

We note that

- φ is bijective and preserves the valuation on $K[M]$;
- θ is a contracting map (modulo M^{d-1}).

In most cases, $\alpha\gamma$ $(= \alpha_1\alpha_4 + \alpha_2\alpha_3)$ is invertible in $K[M]$, and using a fixed point theorem, we can solve the system in $O(d \log d)$ operations in K.

Solving the local equations for IP1S

In the general case, we can study equations of the form

$$M^e \varphi(x) = a\,\theta(x) + b$$

to prove the following result:

Proposition

The local equations for IP1S may be solved using no more than $O(d^2)$ operations in the field K.

Solving cyclic IP1S

Theorem (Cyclic IP1S in characteristic two)

Let K be a binary field and (A_λ), (B_λ) be two isomorphic cyclic pencils of quadratic forms on K^n. It is possible to compute an isomorphism from (A_λ) to (B_λ) using no more than $\widetilde{O}(n^3)$ operations in K.

- Computing the characteristic polynomials.
- Primary decomposition of (A_λ) and (B_λ).
- Solving the local equations.
- Patching via Chinese remainders to a solution of the IP1S problem.

Moreover, we can count the solutions to the IP1S problem.

Computer experiments for random instances

q	n	t (s)	% cyclic
2	32	0.07	96
2	128	2	95
2	256	33	94
2^4	32	0.3	100
2^7	32	0.5	100

In most cases, the determinant $\alpha_1\alpha_4 + \alpha_2\alpha_3$ is invertible in $K[M]$, so that the quadratic convergence of the fixed point theorem allows us to solve the local equations in $O(d \log d)$.

Conclusion and future work

Cyclic case:

- Proof of polynomiality of IP1S in all characteristics.
- Uses classification of quadratic forms.
- Complexity dominated by linear algebra.

Non-cyclic case:

- The commutant of the characteristic endomorphism is harder to manipulate.
- The IP1S problem has more solutions than in the cyclic case.
  - For example: in the extremely non-cyclic case where $b_0 = 0$, the solutions are parametered by the full orthogonal group of b_∞.
  - Giving a parametrization of the space of solutions would help solving the problem for more than two polynomials.