# A post-quantum key exchange protocol from the intersection of conics

Alberto Alzati, Daniele Di Tullio,
Manoj Gyawali, Alfonso Tortora

February 5, 2024

**Abstract**

In this paper we present a key exchange protocol in which Alice and Bob have secret keys given by two conics embedded in a large ambient space by means of the Veronese embedding and public keys given by hyperplanes containing the embedded curves. Both of them construct some common invariants given by the intersection of two conics.

***Keywords:*** Conics, Veronese embedding, post-quantum cryptography

## 1 Introduction

After the celebrated algorithm of Shor [13] in 1994, public key cryptography based on the most popular problems called factorization and discrete logarithm are considered to be unsafe for quantum computers. As a consequences of this algorithm, a research is flourishing towards the post-quantum cryptography in order to prevent a possible crisis in near future. To standardize the post-quantum candidates, the United States government agency National Institute of Standards and Technology (NIST) launched the first round of a competition for the post-quantum cryptographic algorithms [14] in 2016 with the following remark:

*"In recent years, there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will compromise the*

*security of many commonly used cryptographic algorithms. In particular, quantum computers would completely break many public-key cryptosystems, including RSA, DSA, and elliptic curve cryptosystems. These cryptosystems are used to implement digital signatures and key establishment and play a crucial role in ensuring the confidentiality and authenticity of communications on the Internet and other networks."*

*NIST -2016.*

During the period from the NIST's first round in 2016 to the fourth round in 2022, we have witnessed many schemes based on various mathematical problems classifying the post-quantum cryptography as lattice-based, code-based, multivariate, hash-based, and isogeny based cryptography [1, 6, 4]. We have also witnessed the powerful attacks for the post quantum schemes. The multivariate schemes known as Rainbow can be broken in a weekend time on a classical laptop due to Ward Beullen [2]. Furthermore, an isogeny based key encapsulation mechanism known as SIKE encountered polynomial time classical attacks [3, 10, 12].

In 2020 a key exchange scheme called quadratic surface intersection (QSI) key exchange was proposed by D. Di Tullio and M. Gyawali [8] based on a new problems in computational algebraic geometry, for example solving large system of high degree polynomial equations in many variables, or finding the primary decomposition of an ideal generated by many polynomials in many variables, which were conjectured to be quantum resistant.

In this work, we propose a new key exchange scheme which resembles QSI key exchange but unlike quadratic surface we use plane conics embedded in a high degree surface $\mathcal{S}$ contained in a high-dimensional space. By using conics, we have smaller key size in a higher security level than the QSI scheme. Two parties A and B choose a plane conic embedded, in two different ways, in a high degree surface $\mathcal{S}$ contained in a high dimensional space. Let us call $\mathcal{C}_A$ and $\mathcal{C}_A$ these curves, respectively. More precisely,

- The secret keys of A and B are respectively embeddings $f_{\mathsf{A}}, f_{\mathsf{B}} : \mathbb{P}^1 \to \mathcal{S}$, whose images are isomorphic copies of plane conics $\mathcal{C}_{\mathsf{A}}, \mathcal{C}_{\mathsf{B}}$.
- The public key of A is a pair of hyperplanes $(\mathcal{H}_{A,1}, \mathcal{H}_{A,2})$ containing $\mathcal{C}_A$ and the same is for B.

The exchanged key will be a set of invariants associated to the "areas" of the four triangles constructed using the four points of intersection of the

"non-embedded versions" of $\mathcal{C}_A$ and $\mathcal{C}_B$. These "areas" can be computed only if the trapdoor (the explicit embedding $\mathbb{P}^1 \to \mathcal{S}$) is known for one of the conics. Obviously here "area" is a suitable generalization in any affine plane of the usual definition of area for triangles in real affine planes $\mathbb{A}^2(\mathbb{R})$.

For a proof of concept, we implemented our algorithm in SAGE [15] and is publicly available in

`https://github.com/mgyawali/CSI_key_exchange`.

In section 2, we give a brief background materials which will be used in the following sections. We present the new key exchange scheme and its detailed description in sections 3 and 4. In section 5, we provide a toy example which further describes the main idea of the scheme. In section 6 we try to give a brief security analysis. We propose a parameter set in section 7 and provide some open problems in section 8.

# 2 Invariants for sets of four points on affine planes

Firstly we give a very informal definition of an invariant.

**Definition 2.1.** *For any family of geometric objects $\mathcal{F}$ and for any group $G$ acting on $\mathcal{F}$, an invariant $\iota$ is an element of a fixed field $\mathbb{F}$ associated to any object $\wr \in \mathcal{F}$ which is preserved by the action of $G$, i.e.*

$$\iota(g \cdot \wr) = \iota(\wr) \text{ for any } g \in G.$$

**Example 2.2.** *A familiar example is the j-invariant belonging to the complex numbers: in this case we can take $\mathcal{F}$ = {smooth plane cubics in the projective plane over complex numbers}, $G$ = {group of linear plane automorphisms} (see [8]).*

In this section we want to define suitable invariants for a set of four distinct points belonging to any affine plane. Before doing this, we need some facts about symmetric functions. Let us start by fixing any field $\mathbb{F}$. Let us consider the four symmetric elementary functions $\mathbb{F}^4 \to \mathbb{F}$ as follows:

$\sigma_1(a,b,c,d) = a+b+c+d$
$\sigma_2(a,b,c,d) = ab+ac+ad+bc+bd+cd$
$\sigma_3(a,b,c,d) = abc+abd+acd+bcd$
$\sigma_4(a,b,c,d) = abcd.$

Here "symmetric" means that the values of the above functions are invariant under the action of the symmetric group $S_4$ over the four elements $a,b,c,d$. It is well known that every symmetric function $\mathbb{F}^4 \to \mathbb{F}$ is in fact

a polynomial function on $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ and that there exists a well known algorithm allowing to detect such polynomial.

Moreover, by any computer algebra system, it is easy to prove that:

- if we define a map $\varphi : \mathbb{F}^4 \to \mathbb{F}^4$ by using the above four functions $\sigma_i$ in this way:

$(a, b, c, d) \to (\sigma_1(a, b, c, d), \sigma_2(a, b, c, d), \sigma_3(a, b, c, d), \sigma_4(a, b, c, d))$

such map is dominant;

- if we restrict $\varphi$ to the elements $a, b, c, d$ satisfying a linear relation, then $Im(\varphi)$ has dimension 3.

For instance, if we assume that $a + b = c + d$ then $Im(\varphi)$ is the hypersurface of $\mathbb{F}^4$ having equation: $\sigma_1^3 - 4\sigma_1\sigma_2 + 8\sigma_3 = 0$.

Now let us consider the affine plane $\mathbb{A}^2(\mathbb{F})$ over $\mathbb{F}$. Let $P, Q, R, S$ be four distinct points, belonging to the plane, in general position; this means that no three of them are collinear. It is known that, in any affine plane, all the triple of non-collinear points are equivalent under affine transformations. I. e., for any ordered triples of distinct points, in general position, $P, Q, R$ and $P', Q', R'$ there exists a unique affine transformation $\alpha$ such that $\alpha(P) = P', \alpha(Q) = Q', \alpha(R) = R'$.

In real affine planes $\mathbb{A}^2(\mathbb{R})$ it is possible to calculate the area of any triangle $\tau$ whose vertices have coordinates $(x_1, y_1), (x_2, y_2), (x_3, y_3)$ by using the following formula:

$$\text{Area}(\tau) = \frac{1}{2} \left| \det \begin{pmatrix} 1 & 1 & 1 \\ x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \end{pmatrix} \right|.$$

Note that, for any affine transformation $\alpha(\vec{v}) = M \cdot \vec{v} + \vec{c}$, from the above formula we can easily deduce that:

$$\text{area}(\alpha(\tau)) = |\det(M)| \cdot \text{area}(\tau)$$

where $M$ is the $(2, 2)$ matrix taking into account the linear part of the affine transformation $\alpha$. Therefore, if we consider the subgroup $G$ of affine transformations with matrix $M$ such that $det(M)^2 = 1$ and let it act on the plane, we get that the areas of triangles are invariant according our definition. Note that this is obviously an invariant for triangles, (i.e. for unordered triple of distinct non collinear points) because the area is independent by the order of the vertices of the triangle. From now on the elements of $G$ will be called *equiaffinities*.

Now we want to use the above real invariant to define invariants for objects in any affine plane. We have to get off the factor $1/2$ and the absolute value; however, in this case, the determinant is sensitive about the

order of the three points. To avoid this problem we can define the following invariant for any set of three distinct non collinear points $P, Q, R$ belonging to any affine plane $\mathbb{A}^2(\mathbb{F})$, assuming that the three points have coordinates, respectively, $(x_1, y_1), (x_2, y_2), (x_3, y_3)$:

$$\mathrm{Ar}(P, Q, R) = (\det \begin{pmatrix} 1 & 1 & 1 \\ x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \end{pmatrix})^2.$$

As we explained before, $Ar(P, Q, R)$ is invariant under the action of any $\alpha \in G$. However we need invariants for 4-ples of points, so we have to use more complex definitions as follows.

Let $P, Q, R, S$ be any set of four distinct points in $\mathbb{A}^2(\mathbb{F})$, in general position, having coordinates, respectively $(x_1, y_1), (x_2, y_2), (x_3, y_3)(x_4, y_4)$; let us put

$a = Ar(P, Q, R)$
$b = Ar(P, Q, S)$
$c = Ar(P, R, S)$
$d = Ar(Q, R, S)$;

and let $A, B, C, D$ be the four values of the four elementary symmetric functions of $a, b, c, d$:

$A = \sigma_1(a, b, c, d) = a + b + c + d$
$B = \sigma_2(a, b, c, d) = ab + ac + ad + bc + bd + cd$
$C = \sigma_3(a, b, c, d) = abc + abd + acd + bcd$
$D = \sigma_4(a, b, c, d) = abcd.$

Then $A, B, C, D$ are four invariants of the set $P, Q, R, S$ under the action of $G$ over the affine plane.

In fact:

- every $\alpha \in G$ sends $P, Q, R, S$ into another set $P', Q', R', S'$ having the same properties,

- the four values $Ar(-, -, -)$ are preserved, as we have seen above,

- the symmetric functions $\sigma_i$ allow to define elements of $\mathbb{F}$ not depending on the order of the considered four points.

For future use we need to know whether, in this way, we can obtain all the elements of $\mathbb{F}^4$ or not. Unfortunately the answer is negative. Firstly we know that the map $\varphi$ is only dominant. Secondly we know that, if there exists a linear relation among $a, b, c, d$ then $dim(Im(\varphi)) = 3$. In this case we have no linear relations of this type, however $dim(Im(\varphi)) = 3$ too. Let us explain why: up to affine transformations in $G$ we can assume that the coordinates of the four points $P, Q, R, S$ give rise the the following $(3, 4)$ matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & p & 0 & h \\ 0 & 0 & q & k \end{pmatrix},$$

where all entries $p, q, h, k$ are different from zero because the points are in general position. Now $a, b, c, d$ are exactly the squares of the four minors of the matrix:

$a = (pq)^2$
$b = (pk)^2$
$c = (-hq)^2$
$d = (pq - hq - pk)^2$,

so that the four elements of $\mathbb{F}$ are in fact squares (in arbitrary fields this means that not all elements of $\mathbb{F}$ can be joined) of four elements among which there is a linear relation. By a computer algebra system you can prove that $dim(Im(\varphi)) = 3$; in fact $Im(\varphi)$ is a singular quartic hypersurface in $\mathbb{P}^3$. This means that the points of $Im(\varphi)$ depend only on three parameters.

In the sequel the set of points under consideration will be the intersections of two affine conics in general position, and one of them will have equation: $y = x^2$. A priori this would give the following problem: the coordinates of the four points could be defined only on a suitable extension of $\mathbb{F}$. However this does not matter. In this case the above $(3, 4)$ matrix will be

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ x_1 & x_2 & x_3 & x_4 \\ x_1^2 & x_2^2 & x_3^2 & x_4^2 \end{pmatrix},$$

and $a, b, c, d$ will be Vandermonde determinants. Note that this is true, whatever extension needed, because one of the conic has equation $y = x^2$. These assumptions implies some important facts:

- The four functions $A, B, C, D$ are symmetric functions of the four values $x_1, x_2, x_3, x_4$, hence they can be expressed as polynomials in the four elementary symmetric functions of the four elements of $\mathbb{F}$: $x_1, x_2, x_3, x_4$. These elements are distinct as the two conics are in general position.

- These four values are the distinct roots of a unique monic degree four polynomial $p(t)$ of $\mathbb{F}[t]$ obtained by eliminating $y$ among the equations of the two conics. Hence the four values of the four elementary symmetric functions of $x_1, x_2, x_3, x_4$ are the coefficient of $p(t)$.

- In conclusion the values $A, B, C, D$ can be computed directly from the polynomial $p(t)$, without passing through the coordinates of the four points, avoiding to use any extension of $\mathbb{F}$.
- For instance, if $p(t) = t^4 + \sigma_1 t^3 + \sigma_2 t^2 + \sigma_3 t + \sigma_4$, then

$$A = 2\sigma_1^2\sigma_2^2 - 6\sigma_1^3\sigma_3 - 8\sigma_2^3 + 28\sigma_1\sigma_2\sigma_3 - 12\sigma_1^2\sigma_4 + 36\sigma_3^2 + 32\sigma_2\sigma_4.$$

# 3 General description of the model

**Trusted setup:** Suppose a trusted third party generates the following information (or by Alice if there is no trusted third party):

- A finite field $\mathbb{F}$ of order $q$.
- A surface $\mathcal{S} \subset \mathbb{P}^n(\mathbb{F})$ for which there exists a **secret** isomorphism to the plane $\sigma : \mathbb{P}^2(\mathbb{F}) \to \mathcal{S}$. This isomorphism will be the composition of a public embedding $\sigma_{\mathcal{B}} : \mathbb{P}^2 \to \mathbb{P}^n$ and a secret isomorphism $\phi$ of $\mathbb{P}^n$.
- A public embedding $\phi \circ \sigma_{\mathcal{B}} \circ f := f_{\text{pub}} : \mathbb{P}^1(\mathbb{F}) \to \mathcal{S}$ for which $\sigma^{-1}(f_{\text{pub}}(\mathbb{P}^1))$ is a smooth public conic $\Gamma = f(\mathbb{P}^1)$ where $f$ is a public embedding of $\mathbb{P}^1$ in $\mathbb{P}^2$.
- At least three **secret** automorphisms $\overline{\alpha_1}, \overline{\alpha_2}, \overline{\alpha_3} \in \text{Aut}(\mathcal{S}_0)$, where $\mathcal{S}_0 := \sigma_{\mathcal{B}}(\mathbb{P}^2)$ under the identification $\mathcal{S}_0 \to \mathbb{P}^2$, and where $\alpha_i$ are linear isomorphism of $\mathbb{P}^2$, (see Appendix A).

**Key generation:** The first user A (Alice) computes an embedding $f_{\mathsf{A}} : \mathbb{P}^1 \to \mathcal{S} = \phi(\mathcal{S}_0)$ of the form

$$f_{\mathsf{A}} = \phi \circ \overline{\alpha}_1 \circ \sigma_{\mathcal{B}} \circ f.$$

A then computes two hyperplanes $\mathcal{H}_{\mathsf{A},1}, \mathcal{H}_{\mathsf{A},2}$ containing $f_{\mathsf{A}}(\mathbb{P}^1)$. Then we have that [pk means public key, sk means secret key]:

$$\mathsf{pk}_{\mathsf{A}} = (\mathcal{H}_{\mathsf{A},1}, \mathcal{H}_{\mathsf{A},2}), \qquad \mathsf{sk}_{\mathsf{A}} = f_{\mathsf{A}}.$$

The second user B (Bob), after choosing a **secret** composition (for some positive integers $\epsilon_1 ... \epsilon_{2q}$):

$$\overline{\beta} = \overline{\alpha_2^{\epsilon_1}\alpha_3^{\epsilon_2} ... \alpha_2^{\epsilon_{2q-1}}\alpha_3^{\epsilon_{2q}}},$$

computes an embedding $f_{\mathsf{B}} : \mathbb{P}^1 \to \mathcal{S} = \phi(\mathcal{S}_0)$ of the form

$$f_{\mathsf{B}} = \phi \circ \overline{\beta} \circ \sigma_{\mathcal{B}} \circ f.$$

B then computes two hyperplanes $\mathcal{H}_{\mathsf{B},1}, \mathcal{H}_{\mathsf{B},2}$ containing $f_{\mathsf{B}}(\mathbb{P}^1)$. The public and private keys of B are

$$\mathsf{pk}_{\mathsf{B}} = (\mathcal{H}_{\mathsf{B},1}, \mathcal{H}_{\mathsf{B},2}) \text{ and } \mathsf{sk}_{\mathsf{B}} = f_{\mathsf{B}}$$

respectively.

**Key exchange:** A and B can compute a common key in the following way:

- A computes $f_{\mathsf{A}}^{-1}(\mathcal{H}_{\mathsf{B},1} \cap \mathcal{H}_{\mathsf{B},2})$ which are points of $\mathbb{P}^1$. The pullback of a hyperplane is rather easy to be computed: it is just a polynomial substitution, while the intersection is just a g.c.d. between two univariate polynomials. At the end the pullback is described by a monic polynomial of degree 4. We will see in the next section how to compute the invariants of the set of 4 points $f(f_{\mathsf{A}}^{-1}(\mathcal{H}_{\mathsf{B},1} \cap \mathcal{H}_{\mathsf{B},2}))$.
- B computes $f_{\mathsf{B}}^{-1}(\mathcal{H}_{\mathsf{A},1} \cap \mathcal{H}_{\mathsf{A},2})$ and analogously he is able to recover the invariants.

# 4 Concrete instantiation

In what follows, all projective spaces will be projective spaces over the fixed finite field $\mathbb{F}$. Let us choose projective coordinates $(t : v)$ for $\mathbb{P}^1$ and $(X : Y : U)$ for $\mathbb{P}^2$; moreover let us choose, once for all, the affine plane $U \neq 0$ and let $x := X/U, y := Y/U$ be affine coordinates in this plane. Let us define $f : \mathbb{P}^1 \to \mathbb{P}^2$ by $f(t : v) = (tv : t^2 : v^2)$. Let us call $\Gamma$ the corresponding smooth plane conic, having projective equation $YU - X^2 = 0$ and affine equation $y - x^2 = 0$.

Fix a degree $d$ and then define $\mathcal{B}$ to be the set of homogeneous monomials of degree $d$ in $\mathbb{F}[X, Y, U]$:

$$\mathcal{B} = \{X^d, X^{d-1}Y, ..., Y^d, Y^{d-1}U, ..., U^d\}.$$

Let $\underline{b}$ be the set of homogeneous monomials of degree $2d$ in $\mathbb{F}[t, v]$

$$\underline{b} = \{t^{2d}, t^{2d-1}v, ..., v^{2d}\}.$$

The set $\mathcal{B}$ defines a polynomial map

$$\sigma_{\mathcal{B}} : \mathbb{P}^2 \to \mathbb{P}^n, \text{ where } n = \binom{d+2}{2} - 1.$$

The image of this map $\mathcal{S}_0 = \sigma_{\mathcal{B}}(\mathbb{P}^2)$ is called *Veronese surface* and it has degree $d^2$. Obviously, this map send $\Gamma$ into a smooth rational normal curve $\sigma_{\mathcal{B}}(\Gamma)$ of degree $2d$ whose span is a projective space of dimension $2d$. The embedding of $\Gamma$ in $\mathcal{S}_0$, hence in $\mathbb{P}^n$, is given by a unique $(n+1, 2d+1)$ sparse matrix $M_{\mathcal{B}}$ such that

$$M_{\mathcal{B}}\underline{b} = \mathcal{B}.$$

Be careful: the above equality is true when we substitute the vector $\sigma_{\mathcal{B}}(f(t:v))$ to the vector $\mathcal{B}$.

Note that any projective isomorphism $\mathbb{P}^2 \to \mathbb{P}^2$ induces a corresponding isomorphism $\mathbb{P}^n \to \mathbb{P}^n$ and a corresponding isomorphism $\mathcal{S}_0 \to \mathcal{S}_0$, which remains fixed as a surface in $\mathbb{P}^n$, but not every projective isomorphism $\mathbb{P}^n \to \mathbb{P}^n$ comes from some projective isomorphism $\mathbb{P}^2 \to \mathbb{P}^2$; in such cases $\mathcal{S}_0$ is not fixed, in general, however the curve $\sigma_{\mathcal{B}}(\Gamma)$ is transformed in another smooth curve of the same degree in $\mathbb{P}^n$ (see Appendix A).

## 4.1 Computation of embeddings and automorphisms

**Generation of $\mathbf{f}_{\text{pub}}$:** the first user (Alice) chooses a random projective invertible transformation $\phi : \mathbb{P}^n \to \mathbb{P}^n$. In practical this means to chose a generic, invertible $(n+1, n+1)$ matrix $V_\phi$. According to what we have remarked above, this transformation does not come from $\mathbb{P}^2$, hence it does not fix $\mathcal{S}_0$, however we can consider the $2d$-degree curve $\phi(\sigma_{\mathcal{B}}(\Gamma))$, which is given by the $(n+1, 2d+1)$ matrix $V_\phi M_{\mathcal{B}}$ such that

$$V_\phi M_{\mathcal{B}}\underline{b} = V_\phi \mathcal{B}.$$

Then Alice computes $f_{\text{pub}} = \phi \circ \sigma_{\mathcal{B}} \circ f$. The secret $\sigma$ of the general setting is $\phi \circ \sigma_{\mathcal{B}}$. Alice can publish the matrix $V_\phi M_{\mathcal{B}}$.

**Generation of $\alpha_i$** : Alice chooses random projective plane isomorphisms $\alpha_i$, with $i = 1, 2, 3$, such that they are area preserving affine transformations from the affine point of view. In our coordinates this means to choose random invertible $(3, 3)$ matrices of the following type (up to a non constant factor), having determinant equal to 1.

$$\begin{pmatrix} * & * & * \\ * & * & * \\ 0 & 0 & 1 \end{pmatrix}.$$

where $*$ is any element of $\mathbb{F}$. For any such matrix it is easy to get the corresponding $(n+1, n+1)$ matrix $A_i$ describing the induced projective isomorphism $\overline{\alpha}_i$ in $\mathbb{P}^n$ such that $\overline{\alpha}_i \circ \sigma_{\mathcal{B}} = \sigma_{\mathcal{B}} \circ \alpha_i$.

Now Alice considers the rational $2d$-degree curves which are the transformed of $\overline{\alpha}_i(\sigma_{\mathcal{B}}(\Gamma))$ under the action of $\phi$. These curves are given by the $(n+1, 2d+1)$ matrix $V_\phi A_i M_{\mathcal{B}}$ such that

$$V_\phi A_i M_{\mathcal{B}} \underline{b} = V_\phi A_i \mathcal{B}.$$

Alice keeps secret the first matrix ($i = 1$), hence the corresponding rational $2d$-degree curve in $\mathbb{P}^n$, say $\mathcal{C}_A$, and publishes the matrices $V_\phi A_2 V_\phi^{-1}$ and $V_\phi A_3 V_\phi^{-1}$.

The second user (Bob) chooses a random sequence of integers $\epsilon_1 ... \epsilon_{2q}$ and a secret matrix of the following type:

$$V_\phi B V_\phi^{-1} = V_\phi A_2^{\epsilon_1} A_3^{\epsilon_2} ... A_2^{\epsilon_{2q-1}} A_3^{\epsilon_{2q}} V_\phi^{-1}$$

by multiplying powers of the matrices published by Alice; of course:

$$B = A_2^{\epsilon_1} A_3^{\epsilon_2} ... A_2^{\epsilon_{2q-1}} A_3^{\epsilon_{2q}}.$$

Then Bob considers the following matrix

$$[V_\phi B V_\phi^{-1}][V_\phi M_{\mathcal{B}}].$$

Note that it is equal to $V_\phi B M_{\mathcal{B}}$ (note also that Bob does not know $B$) hence it defines another rational $2d$-degree curve, say $\mathcal{C}_B$, which is the transformed of $\overline{\beta}(\sigma_{\mathcal{B}}(\Gamma))$ under the action of $\phi$, where $\overline{\beta}$ is defined as in section 3 and $\beta = \alpha_2^{\epsilon_1} \alpha_3^{\epsilon_2} ... \alpha_2^{\epsilon_{2q-1}} \alpha_3^{\epsilon_{2q}}$. Note that $\mathcal{C}_A$ is unknown to Bob and $\mathcal{C}_B$ is unknown to Alice.

$\mathcal{C}_A$ and $\mathcal{C}_B$ have four distinct common points, say $\{P'_1, P'_2, P'_3, P'_4\}$ which are the intersection among these two curves. In fact

$$\overline{\alpha}_1(\sigma_{\mathcal{B}}(\Gamma)) = \sigma_{\mathcal{B}}(\alpha_1(\Gamma))$$

because the isomorphism $\overline{\alpha}_1$ comes from $\mathbb{P}^2$. Analogously:

$$\overline{\beta}(\sigma_{\mathcal{B}}(\Gamma)) = \sigma_{\mathcal{B}}(\beta(\Gamma))$$

for the same reason. In the projective plane $\alpha_1(\Gamma)$ and $\beta(\Gamma)$ intersect at four distinct points $\{P, Q, R, S\}$ and the same is true in our affine plane, thanks to the choice of $\Gamma$ and the fact that the projective isomorphisms of $\mathbb{P}^2$ are random. Therefore $\{P, Q, R, S\}$ are sent in $\mathbb{P}^n$ by $\sigma_{\mathcal{B}}$ into the four common points $\{P_1, P_2, P_3, P_4\}$ between $\overline{\alpha}_1(\sigma_{\mathcal{B}}(\Gamma))$ and $\overline{\beta}(\sigma_{\mathcal{B}}(\Gamma))$. Such points are sent by $\phi$ into $\{P'_1, P'_2, P'_3, P'_4\}$.

**Key exchange** : after Alice has published the above matrices she solves the following linear system of $2d + 1$ equations in $n + 1$ unknowns ($[..]_t$ means transposition):

$$[\mathbf{w}]_t V_\phi A_1 M_{\mathcal{B}} = [\mathbf{0}]_t.$$

Every generic solution gives rise to the $n + 1$ coefficients of a hyperplane in $\mathbb{P}^n$ containing $\mathcal{C}_A$; such hyperplanes cut $\mathcal{C}_B$ at $2d$ distinct points, among which there are $\{P'_1, P'_2, P'_3, P'_4\}$.

Alice publishes two generic solutions of the above linear system.

On the other hand, Bob solves the analogous linear system

$$[\mathbf{v}]_t V_\phi B M_{\mathcal{B}} = [\mathbf{0}]_t.$$

Every generic solution gives rise to the $n + 1$ coefficients of a hyperplane in $\mathbb{P}^n$ containing $\mathcal{C}_B$; such hyperplanes cut $\mathcal{C}_A$ at $2d$ distinct points, among which there are $\{P'_1, P'_2, P'_3, P'_4\}$.

Bob publishes two generic solutions of the above linear system.

## 4.2 Invariants computation

After Alice has received two solutions $\mathbf{v}_1$ and $\mathbf{v}_2$ of Bob's linear system, she calculates, for $i = 1$ and $i = 2$:

$$[\mathbf{v_i}]_t (V_\phi A_1 V_\phi^{-1})(V_\phi M_{\mathcal{B}})\underline{b}$$

which are $2d$-degree homogeneous polynomials of $\mathbb{F}[t, v]$ such that, among their roots, there are four values sent in the four points: $\Gamma \cap [\alpha_1^{-1}(\beta(\Gamma))]$ by $f$. The roots of these polynomials are

$$f^{-1}(\sigma_{\mathcal{B}}^{-1}\{\sigma_{\mathcal{B}}(\alpha_1(\Gamma)) \cap HBob_i\}),$$

where $HBob_i$ are Bob's hyperplanes. To detect what are the four roots corresponding to the above points it is sufficient to calculate the g.c.d. of the two polynomials. Let $p_A(t)$ be the monic g.c.d. of the two polynomials with respect to $t$.

After Bob has received two solutions $\mathbf{w}_1$ and $\mathbf{w}_2$ of Alice's linear system, he calculates, for $i = 1$ and $i = 2$:

$$[\mathbf{w_i}]_t(V_\phi B V_\phi^{-1})(V_\phi M_\mathcal{B})\underline{b}$$

which are $2d$-degree homogeneous polynomials of $\mathbb{F}[t, v]$ such that, among their roots, there are four values sent in the four points $\Gamma \cap [\beta^{-1} \circ \alpha_1(\Gamma)]$ by $f$. The roots of these polynomials are

$$f^{-1}(\sigma_\mathcal{B}^{-1}(\{\sigma_\mathcal{B}(\beta(\Gamma)) \cap HAlice_i\}),$$

where $HAlice_i$ are Alice's hyperplanes. To detect what are the four roots corresponding to the above points it is sufficient to calculate the g.c.d. of the two polynomials. Let $p_B(t)$ be the monic g.c.d. of the two polynomials with respect to $t$.

Now Alice knows a monic polynomial $p_A(t)$ whose roots are the abscissas of four points of $\Gamma$ and Bob knows a monic polynomial $p_B(t)$ whose roots are the abscissas of other four points of $\Gamma$. The two sets of four points are equivalent under an equiaffine map (see section 2): $\beta^{-1} \circ \alpha_1$ (and its inverse), hence the four invariants defined at the end of section 2 are the same for Alice and Bob.

# 5 Toy example

In this section we want to describe in details a very simple example by using $d = 3$ and a finite field of characteristic $p$ sufficiently high such that the following integers need not to be considered *mod* $p$. Let us fix some notation as in section 4. Let $(X : Y : U)$ be coordinates in $\mathbb{P}^2$ and let $x := X/U, y := Y/U$ be affine coordinates in the plane $U \neq 0$. Let

$$(X^3 : X^2Y : X^2U : XY^2 : XYU : XU^2 : Y^3 : Y^2U : YU^2 : U^3)$$

be a standard base of plane cubics. Let $(t : v)$ be coordinates in $\mathbb{P}^1$ and let $(t^2 : tv : v^2)$ be a standard base of degree two homogeneous polynomials in $(t : v)$. Let us call $\mathcal{B}$ the above base of cubics and let us consider it as a $(10, 1)$ vector.

Let us embed $\mathbb{P}^2$ in $\mathbb{P}^9$ (the space of plane cubics) with coordinates

$$(x_0 : x_1 : x_2 : x_3 : x_4 : x_5 : x_6 : x_7 : x_8 : x_9),$$

by using the 3-Veronese embedding: $x_0 = X^3, x_1 = X^2Y$ ... and so on. Let us choose the conic $\Gamma$ given by the following embedding of $\mathbb{P}^1$ in $\mathbb{P}^2$ :

$X = tv, Y = t^2, U = v^2$ so that the equation of $\Gamma$ in $\mathbb{P}^2$ is $YU - X^2$ ($y = x^2$ in the affine coordinates) and the corresponding sextic curve $\overline{\Gamma} := \sigma_{\mathcal{B}}(\Gamma)$ in $\mathbb{P}^9$ is

$x_0 = t^3v^3, x_1 = t^4v^2, x_2 = t^2v^4, x_3 = t^5v, x_4 = t^3v^3, x_5 = tv^5, x_6 = t^6, x_7 = t^4v^2, x_8 = t^2v^4, x_9 = v^6$.

Note that this curve is contained in the intersection of these hyperplanes: $x_7 - x_1 = 0, x_8 - x_2 = 0, x_4 - x_0 = 0$, in fact it is a rational normal curve of degree 6, hence its span is a $\mathbb{P}^6$.

If we call $\underline{b}$ the following base of homogeneous polynomials of degree 6 in two variables:

$$(t^6 : t^5v : t^4v^2 : t^3v^3 : t^2v^4 : tv^5 : v^6)$$

and we consider it as a $(7, 1)$ vector, we can describe the above embedding by using a unique $(10, 7)$ sparse matrix $M$ in this way:

$$M\underline{b} = \mathcal{B}.$$

with

$$M := \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

The above choices are public. Now let us assume that Alice chooses a secret non singular $(10, 10)$ matrix $V$ describing a linear automorphism of the 9-dimensional projective space of plane cubics. For instance:

$$V := \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Note that $det(V) = -1$ and that the above autormorphism is not induced by a projectivity of the plane. For instance in the above automorphism the cubic $X^3$ corresponds to $X^2Y$: the first one is a triple line, the second one not, and this is not possible for two projectively equivalent plane cubics. This fact is crucial for our aim: see at the end of this section.

Now Alice picks up the following secret equiaffinity $\alpha$ in the affine plane coordinates $(x, y)$:

$x \to x/2 - y/3 - 2/3$

$y \to 2y + 2$,

$\alpha$ induces a projectivity on the space of plane cubics which is described by the following $(10, 10)$ matrix $A$ by using the standard base $\mathcal{B}$

$$A := \begin{pmatrix} 1/8 & -1/4 & -1/2 & 1/6 & 2/3 & 2/3 & -1/27 & -2/9 & -4/9 & -8/27 \\ 0 & 1/2 & 1/2 & -2/3 & -2 & -4/3 & 2/9 & 10/9 & 16/9 & 8/9 \\ 0 & 0 & 1/4 & 0 & -1/3 & -2/3 & 0 & 1/9 & 4/9 & 4/9 \\ 0 & 0 & 0 & 2 & 4 & 2 & -4/3 & -16/3 & -20/3 & -8/3 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & -2/3 & -2 & -4/3 \\ 0 & 0 & 0 & 0 & 0 & 1/2 & 0 & 0 & -1/3 & -2/3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 8 & 24 & 24 & 8 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 8 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

but it is described by the following different matrix by using the secret base $V\mathcal{B}$:

$$VAV^{-1}.$$

The sextic rational curve, transformed of $\overline{\Gamma} := \sigma_{\mathcal{B}}(\Gamma)$ under the isomorphism of $\mathbb{P}^9$ induced by $\alpha$ and then by the isomorphism of $\mathbb{P}^9$ defined by $V$, which is in fact the secret conic of Alice, is:

$$[x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9]_t = VAV^{-1}VM\underline{b} = VAM\underline{b}$$

(where $[..]_t$ means transposition), so that if Alice solves the following linear system:

$$[\mathbf{w}]_t VAM = [\mathbf{0}]_t$$

she gets coefficients of hyperplanes of $\mathbb{P}^9$ containing the transformed of $\overline{\Gamma}$. In this example it is easy to see that the solutions are generated by:

$[\mathbf{w_1}]_t := [-24, -72, -48, -2, 1, 0, -26, 0, 0, 0]$

$[\mathbf{w_2}]_t := [8100, 24192, 17064, 684, 0, 1, 9360, 51/2, 338, 0]$

$[\mathbf{w_3}]_t := [-576, -1728, -1224, -48, 0, 0, -672, -2, -26, 1]$.

Now Alice picks up another secret equiaffinity $\beta$. To get very simple computations let us assume that $\beta$ in the affine plane coordinates $(x, y)$ is:

$x \to x/2 - 2y/3 + 2/3$

$y \to 2y + 2$;

$\beta$ induces a projectivity on the space of plane cubics which is described by the following $(10, 10)$ matrix $B$ by using the standard base $\mathcal{B}$

$$B := \begin{pmatrix} 1/8 & -1/2 & 1/2 & 2/3 & -4/3 & 2/3 & -8/27 & 8/9 & -8/9 & 8/27 \\ 0 & 1/2 & 1/2 & -4/3 & 0 & 4/3 & 8/9 & -8/9 & -8/9 & 8/9 \\ 0 & 0 & 1/4 & 0 & -2/3 & 2/3 & 0 & 4/9 & -8/9 & 4/9 \\ 0 & 0 & 0 & 2 & 4 & 2 & -8/3 & -8/3 & 8/3 & 8/3 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & -4/3 & 0 & 4/3 \\ 0 & 0 & 0 & 0 & 0 & 1/2 & 0 & 0 & -2/3 & 2/3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 8 & 24 & 24 & 8 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 8 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

but which is described by the following matrix by using our secret base $V\mathcal{B}$:

$$VBV^{-1}.$$

Now Alice is ready to publish her public keys: $VM$, $VBV^{-1}$, $\mathbf{w_i}$ and Bob can come into play: in this toy example Bob uses simply the matrix $VBV^{-1}$ and he solves the following linear system:

$$[\mathbf{v}]_t VBV^{-1}VM = [\mathbf{v}]_t VBM = [\mathbf{0}]_t.$$

The solutions of this linear systems are coefficients of hyperplanes of $\mathbb{P}^9$ containing the transformed of $\overline{\Gamma}$ under the projectivity induced by $\beta$ and then under the isomorphism of $\mathbb{P}^9$ defined by $V$. Such curve, which is in fact the secret conic of Bob, is

$$[x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9]_t = VBV^{-1}VM\underline{b} = VBM\underline{b}.$$

In this example it is easy to see that the solutions are generated by
$[\mathbf{v_1}]_t := [6, 9, -24, 1, -73/8, 0, 73/4, 0, 0, 0]$
$[\mathbf{v_2}]_t := [-27, -54, 1809/8, 0, 171/2, 1, -657/2, 0, 5329/32, -4161/64]$
$[\mathbf{v_3}]_t := [0, 0, 9, 0, 6, 0, -24, 1, 73/4, -73/8]$.
Now Bob is ready to publish his public keys: $\mathbf{v_i}$.
The exchange of public keys is complete.
To get Bob's information Alice calculates: $[\mathbf{v_i}]_t(VAV^{-1})(VM)\underline{b}$ and, to get Alice's information, Bob calculates: $[\mathbf{w_i}]_t(VBV^{-1})(VM)\underline{b}$. Not that all public keys are necessary to do these calculations.
They get polynomials of degree 6 in $(t : v)$. More precisely, Alice gets:
$-1/6(16v^4 - 12tv^3 - 8t^2v^2 + 3t^3v + t^4)(4v^2 - 3tv + 2t^2)$
$1/8(16v^4 - 12tv^3 - 8t^2v^2 + 3t^3v + t^4)(121v^2 - 24tv + 32t^2)$
$(16v^4 - 12tv^3 - 8t^2v^2 + 3t^3v + t^4)v^2$
and Bob gets:
$4/3(16v^4 + 12tv^3 - 8t^2v^2 - 3t^3v + t^4)(-4v^2 - 3tv + 4t^2)$
$-8(16v^4 + 12tv^3 - 8t^2v^2 - 3t^3v + t^4)(-238v^2 - 168tv + 223t^2)$
$8(16v^4 + 12tv^3 - 8t^2v^2 - 3t^3v + t^4)(-17v^2 - 12tv + 16t^2)$.
Alice and Bob consider the g.c.d. of their polynomials (of course two polynomials i.e. two hyperplanes are sufficient), which have degree 4, and the roots of the g.c.d. In this way they get the first coordinates, in the affine plane (x,y), of four points belonging to $\Gamma$; the second ones are determined by the known equation of $\Gamma$ which is $y = x^2$.
Alice gets: $(1, 1), (2, 4), (-2, 4), (-4, 16)$.
Bob gets: $(-1, 1), (2, 4), (-2, 4), (4, 16)$.
These two sets of four points are sent each other by the plane equiaffinity $\beta^{-1} \circ \alpha$ ( and $\alpha^{-1} \circ \beta$ ) but, of course, neither Alice nor Bob knows these transformations (actually, in this toy example, Alice knows $\alpha$ and $\beta$ because Bob has used simply $VBV^{-1}$, but in general $\beta$ is unknown to Alice) and moreover there is no possibility for them to pair points correctly, so that they have to calculate the symmetric invariants described in section 2. For instance, for Alice the four symmetric functions of the first coordinates of her points have the following values: $\sigma_1 = 3, \sigma_2 = -8, \sigma_3 = -12, \sigma_4 = 16$. For Bob we have, respectively: $-3, -8, 12, 16$. In both cases the invariant A of section 2 is 4248.

It is useful to explain why the above g.c.d. appears. In the $\mathbb{P}^9$ of plane cubics we have two rational normal curves of degree 6: $\overline{\alpha(\Gamma)} := \sigma_{\mathcal{B}}(\alpha(\Gamma))$ and $\overline{\beta(\Gamma)} := \sigma_{\mathcal{B}}(\beta(\Gamma))$. Their spans are 6-dimensional and intersect in a $\mathbb{P}^3$. In the plane $(X : Y : U)$ the two conics $\alpha(\Gamma)$ and $\beta(\Gamma)$ intersect at four points which are sent by the 3-Veronese embedding into four points of $\mathbb{P}^9$, say $P_1, P_2, P_3, P_4$. These points generate the $\mathbb{P}^3$ which is the intersection of the two above 6-dimensional spans, hence their belong to both sextics. Every hyperplane containing one of the two sextics, intersected with the other one, gives rise to 6 points, among which there are $P_1, P_2, P_3, P_4$. This situation is isomorphically transformed by the linear automorphism of $\mathbb{P}^9$ induced by $V$, but this does not affect the argument.

When Alice considers $[\mathbf{v_i}]_t VAM\underline{b} = 0$ she gets her $(t : v)$ coordinates of the 6 points of intersection between the $i-th$ Bob's hyperplane with $\overline{\beta(\Gamma)}$. Among them there are always Alice's $(t : v)$ coordinates of $P_1, P_2, P_3, P_4$.

When Bob considers $[\mathbf{w_i}]_t VBM\underline{b} = 0$ he gets his $(t : v)$ coordinates of the 6 points of intersection between the $i-th$ Alice's hyperplane with $\overline{\alpha(\Gamma)}$. Among them there are always Bob's $(t : v)$ coordinates of $P_1, P_2, P_3, P_4$.

Neither Alice nor Bob are interested in the unknown coordinates of $P_1, P_2, P_3, P_4$ in $\mathbb{P}^9$, but both of them, via the $(t : v)$ coordinates, can recover the personal (and different) pull back on $\Gamma$ of $P_1, P_2, P_3, P_4$.

To conclude the example we remark that Alice can also consider the plane cubics: $[\mathbf{v_i}]_t VA\mathcal{B} = 0$. Every Alice's cubic is broken into a line (depending from the chosen Bob's hyperplane) and the common conic

$$9X^2 + 12XY + 4Y^2 - 48XU - 41YU + 64U^2 = 0$$

which is $\alpha^{-1}(\beta(\Gamma))$. If Alice intersects this conic with $\Gamma$ she gets the four points $(1, 1), (2, 4), (-2, 4), (-4, 16)$.

Bob cannot do the same, because he does not know $V$, however if we consider the plane cubics: $[\mathbf{w_i}]_t VB\mathcal{B} = 0$ we have that they are broken into a line (depending from the chosen Alice's hyperplane) and the common conic

$$9X^2 - 12XY + 4Y^2 + 48XU - 41YU + 64U^2 = 0$$

which is $\beta^{-1}(\alpha(\Gamma))$. If we intersect this conic with $\Gamma$ we get the four Bob's points $(-1, 1), (2, 4), (-2, 4), (4, 16)$.

# 6 A brief security analysis

A detailed security analysis is beyond the scope of this paper, however in this section we give an outline. First of all let us remark that the previous Toy Example has no security claims because Bob uses the public matrix $VBV^{-1}$, given by Alice, hence whoever can do Bob's calculation and get Bob's four points.

Now let us try to give an estimate of the computational complexity needed to use our protocol. Alice and Bob have to multiply $(n+1, n+1)$ matrices (or matrices of smaller size), recall that $n+1 = \binom{d+2}{2}$ and to calculate an inverse, hence the computational complexity is of order $O(d^6)$. Moreover they have to solve linear systems of $2d+1$ equations in $n+1$ variables, but this imply a computational complexity of order only $O(d^4)$, in the end the overall order is $O(d^6)$.

It is more difficult to determine the computational complexity needed to break the protocol. In our method there is not an obvious problem such that, if a third part, say Charlie, solves it then he gets the secret key. From this point of view the method is different from the ones based on the factorization of a big integer number $N$, where the underlying problem is to find the prime factors of $N$.

It follows that, to break the method, it is necessary to find the secret key using only publicly available informations.

The public vectors $\mathbf{w_i}$ (or $\mathbf{v_i}$) can be used to determine plane curves of degree $d$ by using the known base $\mathcal{B}$ hoping to get a common conic, to intersect it with $\Gamma$ and to get four points equivalent to Alice's or Bob's points under an equiaffinity. In this case Charlie can calculate the same invariants as Alice and Bob. But this is not possible because these vectors identify curves with respect to the secret base $V\mathcal{B}$ and not $\mathcal{B}$. For instance, in the Toy Example it is easy to see that, as $V$ defines a linear automorphism in the space of cubics not coming from a projectivity of $\mathbb{P}^2$, Charlie's cubics are irreducible.

Knowledge of $VM$ does not help either: if Charlie calculates

$$[\mathbf{w_i}]_t VM\underline{b} = 0$$

he gets degree $2d$ polynomials whose g.c.d. is a polynomial of degree 4 giving the first coordinates of the four points $\alpha(\Gamma) \cap \Gamma$, but they are not equivalent to $\alpha(\Gamma) \cap \beta(\Gamma)$ by an equiaffinity. The same if Charlie uses $\mathbf{v_i}$, with $\beta$ instead of $\alpha$.

On the other hand, knowledge of matrix $V$ is sufficient to break the method. This fact was remarked in a private communication from W. Cas-

tryck (see [16]) who made an in-depth analysis of [8] on which our ideas are based.

If Charlie knows $V$, finding the common conic component among curves

$$[\mathbf{w_i}]_t V\mathcal{B} = 0$$

he gets $\alpha(\Gamma)$, and, similarly, using curves

$$[\mathbf{v_i}]_t V\mathcal{B} = 0$$

he gets $\beta(\Gamma)$. The intersection of these two conics consists of four points which are equivalent with $\Gamma \cap [\beta^{-1} \circ \alpha(\Gamma)]$ and with $[\alpha^{-1} \circ \beta(\Gamma)] \cap \Gamma$, respectively, by equiaffinities. Hence Charlie can calculate the secret key by using these four points as Alice anb Bob do.

To break the method Charlie could try to determine matrix $V$ knowing $VM$ (recall that $M$ is public), but this leads to a maximal rank linear system of $(2d+1)(n+1)$ equations in $(n+1)^2$ variables. The solutions depend on $(n+1)^2 - (n+1)(2d+1)$ parameters, which are too many for a brute force attempt.

However there is another possibility to find $V$. The $d-$Veronese embedding of $\mathbb{P}^2$ is a smooth surface $\mathcal{S}_0$ of $\mathbb{P}^n$ defined by

$$D(d) := d(d^2-1)(d+6)/8$$

linearly independent quadrics. Our surface $\mathcal{S}$ is $\phi(\mathcal{S}_0)$ where $\phi$ is the linear isomorphism represented by $V$ (recall Section 3). The quadrics defining $\mathcal{S}_0$ are known, while a set of quadrics defining $\mathcal{S}$ can be determined in the following way (see [16]):

- pick random points in $\mathbb{P}^1(\mathbb{F})$ and map them into $\mathcal{S}$ using $f_{\text{pub}}$;
- move the points around $\mathcal{S}$ using random combinations of $V_\phi A_2 V_\phi^{-1}$ and $V_\phi A_3 V_\phi^{-1}$ ;
- starting from a quadric with indeterminate coefficients, for any sampled point obtain a linear condition on these coefficients;
- repeat previous step until you are left with a solution which is a vector space of quadrics of dimension $D(d)$: any base of this space defines $\mathcal{S}$.

The heaviest calculation contained in the previous algorithm is a linear system of $O(d^2)$ equations in $O(d^4)$ variables; the complexity is of order

$O(d^8)$ because the computational complexity of a linear system with $N$ equations in $N+h$ variables is the maximum among $O(N^3)$ and $O(N^2h)$.

Now, let us determine the Lie algebras $A_{\mathcal{S}_0}$ and $A_{\mathcal{S}}$ associated to $\mathcal{S}_0$ and $\mathcal{S}$, respectively. Recall that the Lie algebra associated to the smooth intersection of $r$ quadrics in $\mathbb{P}^n(\mathbb{F})$, defined by $r$ symmetric matrices $A_1, ..., A_r$ of type $(n+1, n+1)$, *as set*, is the set of $(n+1, n+1)$ invertible matrices $Y$ such that

$$Y_t A_i + A_i Y \in \langle A_1, ...A_r \rangle \quad i = 1, ..., r.$$

The computational complexity of such calculations is of order $O(d^{16})$ because it must be solved a linear systems in $(n+1)^2 + r^2$ variables, where $r = D(d)$, with $(n+1)^2$ equations.

In our case, both algebras are isomorphic to the Lie algebra of $\mathbb{P}^2(\mathbb{F})$ which is $\mathfrak{sl}_3(\mathbb{F})$ with the standard bracket product; moreover matrix $V$ induces an isomorphism: $(..) \to V(..)V^{-1}$ among the two algebras.

It can be shown (see [16]) that, up to a constant, matrix $V$ represents also an isomorphism between

$\mathbb{F}\langle X^d, X^{d-1}Y, ..., U^d \rangle$ as right $A_{\mathcal{S}_0}$-module

and

$\mathbb{F}\langle x_0, x_1, ..., x_n \rangle$ as right $A_{\mathcal{S}}$-module.

Obviously it is not easy to find the above isomorphism (see for instance [7] and [11]), however Castryck suggests a strategy in [16], based on the partial derivatives of degree $d$ polynomials, generic elements of $\mathbb{F}\langle X^d, X^{d-1}Y, ..., U^d \rangle$. However this strategy does not work very well when $\mathrm{char}(\mathbb{F}) < \mathrm{d}$.

In conclusion, the computational complexity of Castryck's attack is at least of order $O(d^{16})$ plus a part whose complexity is difficult to evaluate, but which in any case does not run when $\mathrm{char}(\mathbb{F})$ is low. On the other hand, we do not know other methods to determine $V$.

To make the method even safer, with a little effort, we could keep the matrix $M$ secret, i. e. the conic $\Gamma$.

# 7 Key size comparison

A detailed security analysis is required to understand the difficulty of underlying problem. In our case, we propose a parameter set according to an experimental evidence. For AES-128 bit security level, we set $d = 14, q \approx 2^{32}$. The size of public and private keys (in bytes) are presented in Table 1.

Table 1: Key size comparison

| Schemes | sk | pk |
|---|---|---|
| Classic McEliece | 6492 | 261120 |
| Kyber | 1632 | 800 |
| QSI key Exchange | 2448000 | 10880 |
| CSI (This work) | 13920 | 960 |

For QSI and CSI, we have computed the key size of Bob. In CSI, the public and private keys of Bob are

$$\mathsf{pk}_\mathsf{B} = (\mathcal{H}_{\mathsf{B},1}, \mathcal{H}_{\mathsf{B},2}) \text{ and } \mathsf{sk}_\mathsf{B} = f_\mathsf{B}$$

respectively. The hyperplanes $\mathcal{H}_{\mathsf{B},1}, \mathcal{H}_{\mathsf{B},2}$ are vectors of length $n+1$, where $n = \binom{d+2}{2} - 1$ and the embedding $f_\mathsf{B}$ is represented by a matrix of size $(n+1, 2d+1) = (120, 29)$.

# 8 Conclusion

We have proposed a new key exchange scheme based on a new mathematical problem. We conjectured that the underlying problem is difficult for the large scale quantum computer, therefore the key exchange is expected to fit in the post-quantum scenario. We leave a detailed study of the problem for future work.

# References

[1] Daniel J. Bernstein, Johannes Buchmann, Erik Dahmen. *Post-Quantum Cryptography*, *Springer-Verlag Berlin Heidelberg*, 2009.

[2] Ward Beullens. *Breaking Rainbow Takes a Weekend on a Laptop*, Cryptology ePrint Archive 2022/214, `https://eprint.iacr.org/2022/214`

[3] Wouter Castryck, Thomas Decru *An efficient key recovery attack on SIDH (preliminary version)*, Cryptology ePrint Archive 2022/975 `https://eprint.iacr.org/2022/975`

[4] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. *CSIDH: An Efficient Post-Quantum Commutative Group*

*Action*, *In: Peyrin T., Galbraith S. (eds) Advances in Cryptology - ASIACRYPT 2018. Lecture Notes in Computer Science, vol 11274. Springer, Cham*, 2018.

[5] Ciro Ciliberto. *An Undergraduate Primer in Algebraic Geometry*, *Springer-Verlag Berlin Heidelberg*, Unitext 129, 2021.

[6] Luca De Feo, David Jao, Jérôme Plût. *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*, *J. Math. Cryptol.*, 8 (2014), 209 - 247.

[7] Willem A. de Graaf, Michael Harrison, Jana Pilnikova, Josef Schicho *A Lie algebra method for rational parametrization of Severi Brauer surfaces j. of Algebra*, 303 (2006), 514 - 529.

[8] Daniele Di Tullio and Manoj Gyawali. *A post-quantum key exchange protocol from the intersection of quadric surfaces*, The Journal of Supercomputing, 2023.

[9] Joe Harris. *Algebraic Geometry, A First Course*, *Springer-Verlag Berlin Heidelberg*, 1992.

[10] Luciano Maino, Chloe Martindale. *An attack on SIDH with arbitrary starting curve*, Cryptology ePrint Archive 2022/1026 `https://eprint.iacr.org/2022/1026`

[11] Jana Pilnikova *Parametrizing algebraic varieties using Lie algebras* arXiv:math/0610727

[12] Damien Robert. *Breaking SIDH in polynomial time*, Cryptology ePrint Archive 2022/1038 `https://eprint.iacr.org/2022/1038`

[13] Peter W. Shor. *Algorithms for quantum computation: Discrete logarithmsand factoring*, *In M. Robshaw and J. Katz, editors, Foundations of ComputerScience, 1994 Proceedings., 35th Annual Symposium*, (1994), 124-134.

[14] *The National Institute of Standards and Technology (NIST). Submission requirements and evaluation criteria for the post-quantum cryptography standardization process*, 2016.

[15] The Sage Developers, *The Sage Mathematics Software System*, 2020, `https://www.sagemath.org`,

[16] Private communication from Wouter Castryck, based on the talk, *On the hardness of cryptosystems based on disguised Veronese varieties*, SIAM Conference on Applied Algebraic Geometry, Eindhoven, July 2023.

# A Veronese surfaces

For ease of references, we collect here the definitions and a few basic facts about Veronese mappings; for a more complete discussion see [5] section 6.4 or [9] chap. 2.

The Veronese mapping $v_{m,d} : \mathbb{P}^m \to \mathbb{P}^n$, where $n = \binom{m+d}{d} - 1$, is an embedding given via monomials of degree $d$. To define it, we need some preliminaries.

Denote the monomials in $\mathbb{F}[x_0, ..., x_m]$ as $m_I := x_0^{i_0} \cdot ... \cdot x_m^{i_m}$ with $I = (i_0, ..., i_m)$ and $|I| = i_0 + ... + i_m$. The lexicographic order on monomials is defined as follows:

$$m_I > m_J \iff \exists h : i_0 = j_0, ..., i_{h-1} = j_{h-1}, i_h > j_h.$$

It is a well known fact that the number of monomials of degree $d$ in $m+1$ variables is $\binom{m+d}{d}$. With this notation, the Veronese embedding is given by

$$v_{m,d} : (x_0 : ... : x_m) \in \mathbb{P}^m \to (m_I)_{|I|=d} \in \mathbb{P}^n,$$

with monomials listed in lexicographic order in $(m_I)_{|I|=d}$. The image of the Veronese map is the Veronese variety $\mathcal{V}_{m,d} := \mathrm{Im}(v_{m,d})$; it is an $m-$dimensional variety isomorphic to $\mathbb{P}^m$; in particular $\mathcal{V}_{1,2}$ is a smooth conic in $\mathbb{P}^2$.

We are mainly interested in Veronese surfaces, i.e. the case $m = 2$, where we use variables $X, Y, U$. Then $\mathcal{V}_{2,d}$ is a surface of degree $d^2$, isomorphic to $\mathbb{P}^2$ and embedded in $\mathbb{P}^n$, with $n = \binom{d+2}{2} - 1$.

A generic projectivity $\phi : \mathbb{P}^n \to \mathbb{P}^n$, given by a matrix $V_\phi \in \mathrm{GL}(n+1, \mathbb{F})$ does not leave $\mathcal{V}_{2,d}$ invariant, i.e. $\phi(\mathcal{V}_{2,d}) \neq \mathcal{V}_{2,d}$; however, any projectivity $\alpha : \mathbb{P}^2 \to \mathbb{P}^2$, induces a suitable projectivity $\overline{\alpha} : \mathbb{P}^n \to \mathbb{P}^n$, such that $v_{2,d} \circ \alpha = \overline{\alpha} \circ v_{2,d}$, hence $\overline{\alpha}$ leaves $\mathcal{V}_{2,d}$ invariant, i.e. $\overline{\alpha}(\mathcal{V}_{2,d}) = \mathcal{V}_{2,d}$.

We can determine the matrix $\mathbf{A} \in \mathrm{GL}(n+1, \mathbb{F})$ representing $\overline{\alpha}$, in terms of the entries of $\mathcal{A} \in \mathrm{GL}(3, \mathbb{F})$ representing $\alpha$, in the following way. The place of the monomial $m_I = X^{i_1} Y^{i_2} U^{i_3}$, $I = (i_1, i_2, i_3)$, $i_1 + i_2 + i_3 = d$, among the monomials of degree $d$ in lexicographic order is

$$p(I) := \frac{(i_2 + i_3)(i_2 + i_3 + 1)}{2} + i_3 + 1.$$

For instance, if $d = 6$ and $I = (1, 2, 3)$, $p(I) = 19$.

Let $l_r := a_{r1}X + a_{r2}Y + a_{r3}U$, $r = 1, 2, 3$, the linear polynomial given by the $r-$th row of $\mathcal{A}$ then $D_I := l_1^{i_1} l_2^{i_2} l_3^{i_3}$ is a homogeneous polynomial of degree $d$ in the variables $X, Y, U$, hence it is a linear combination of the monomials $m_J$ of degree $d$; the coefficients of this linear combination (in lexicographic order) are the entries of the $p(I)-$th row of $\mathbf{A}$.