The Journal of Supercomputing (2025) 81:1183
https://doi.org/10.1007/s11227-025-07657-1

Key exchange based on three-dimensional Segre products and their projections

Alberto Alzati[1] · **Alfonso Tortora**[1]

Accepted: 2 July 2025

Abstract
In this paper we present a key exchange protocol in which Alice and Bob use a three-dimensional Segre product embedded in a large projective space by mean of the Veronese embedding. Public keys are given by hyperplanes cutting pairs of Segre products containing a common plane. Alice and Bob consider the residual curve which is projectively equivalent to a smooth plane curve of genus 1, whose j-invariant is the exchanged key. When the dimension of the above projective space increases very much, HPC capabilities are required.

Keywords Quadrics · Veronese embedding · Segre embedding

1 Introduction

In [1] the authors use intersections of generic quadrics in projective space to define a key exchange protocol. In brief: Alice chooses a pair of quadrics and tells to Bob how to define another pair of quadrics, known only by Bob, in such a way that the smooth elliptic quartic curves, which are intersections of the two pairs of quadrics, are projectively equivalent. Hence the two curves have the same j-invariant, which is in fact the exchanged key. The procedure is made safe by transferring the above mechanism into a high dimensional projective space $\mathbb{P}^N$ by using a suitable Veronese embedding of high degree.

The above technique is a good example of applications of difficult mathematical problems to cryptography. To find the intersection of two quadrics $Q_1, Q_2 \subset \mathbb{P}^3$ embedded in a sufficiently large ambient space is computationally infeasible if the embedding is unknown, which is conjecturally a quantum-safe problem.

Alberto Alzati and Alfonso Tortora are members of GNSAGA of the Italian CNR.

✉ Alberto Alzati
alberto.alzati@unimi.it

[1] Department of Mathematics, University of Milano, via C. Saldini 50, 20133 Milan, Italy

Published online: 23 July 2025

Moreover this approach is different from the previously known promising post-quantum algorithms:

- Lattice-based cryptography based on lattice problems,
- Code-based cryptography based on decoding a generic linear code, which is a NP-complete problem [2],
- Multivariate cryptography based on the difficulty of inverting a multivariate quadratic map or equivalently to solving a set of quadratic equations over a finite field which is a NP-hard problem,
- Hash-based cryptography based on one way hash functions,
- Isogeny-based cryptography based on isogeny problems for example computing isogeny between elliptic curves see [3, 4].

However, recently, some possible attacks to the protocols based on Veronese embeddings have been announced by W. Castryck during the 2023 SIAM Conference at Eindhoven. The weak point consists in the fact that the safety of these protocols is based on the choice of a secret linear isomorphism $\psi : \mathbb{P}^N \to \mathbb{P}^N$, hence in a $(N+1, N+1)$ non-singular matrix V representing ψ, but the knowledge of V allows to break the method. In fact ψ, hence V, can be recovered in principle by the standard well-known polynomial equations of the embedding $\mathcal{X}$ in $\mathbb{P}^N$ and by the polynomial equations of $\psi(\mathcal{X})$, which can be written by a third part by using the public information of the protocol. Fortunately it is very difficult to operate in this way: deep computations in Lie Algebras are required (see [5]) and, as far as we know, an explicit algorithm has not been yet published. In any case it would be better to modify the protocol in such a way that Castryck's attack is impossible. One way to do it is to use fields of very low characteristic, (for instance 2) because the required computations use partial derivatives which vanish in low characteristics.

In this paper we suggest another idea: instead of using only d-Veronese embeddings in $\mathbb{P}^N$ we also use secret linear projections in $\mathbb{P}^{N-1}$ (eventually in lower dimensional spaces), in this way the polynomial equations defining $\mathcal{X}$ and $\psi(\mathcal{X})$ are not known, depending on the used secret projections, this fact makes impossible to recover V by using the above attack.

To illustrate this strategy here we will use a case with $d = 2$ and $N = 20$. We preferred to use the smallest possible value for d so that anyone can easily follow the various calculations, the examples, and verify the correctness of the innovative proposed method. However the method also works for $d \gg 0$, in this case the use of HPC/real-time power is required to make the encoding and decoding of the key you want to exchange sufficiently fast. From what follows it will be clear that when $d \gg 0$ the time required to perform the calculations grows rapidly and would become excessive for practical purposes if a Supercomputer were not used.

In Sect. 2 we recall the definition and some properties of the embedding of the Segre product $\mathbb{P}^1 \times \mathbb{P}^2$ in $\mathbb{P}^5$ and describe some intersection curves of two of these embeddings and their suitable projections. In Sect. 3 we explain how to calculate the projective j-invariant for smooth plane cubic curves. In Sect. 4 we give a key exchange protocol without worrying about security issues. In Sect. 5 we encrypt the

protocol by using 2-Veronese embeddings. In Sect. 6 we discuss possible attacks to the system and countermeasures. In Sect. 7 we give a toy example.

2 Segre product $\mathbb{P}^1 \times \mathbb{P}^2$

Let us fix a finite base field $\mathbb{K}$ of characteristic $\mathrm{p} \geq 2$ and order $|\mathbb{K}|$, let us tacitly assume that $|\mathbb{K}| \gg 0$. Let us recall the notion of standard Segre embedding.

Definition 2.1 The standard Segre embeddings are a family of morphisms of projective varieties

$$\begin{array}{c} \mathbb{P}^n \times \mathbb{P}^m \xrightarrow{\quad s_{n,m} \quad} \mathbb{P}^{N_{n,m}} \\ ([X_0 : \ldots : X_n], [Y_0 : \ldots : Y_m]) \longmapsto [X_0Y_0 : X_0Y_1 : \ldots : X_nY_m] \end{array}$$

where $N_{n,m} = (m+1)(n+1) - 1$ and the sequence $[X_iY_j]$ is ordered by the standard lexicographical order. The images of these embeddings are called standard Segre varieties and they are denoted by the symbol $\Sigma_{n,m}$. They are essentially isomorphic copies of $\mathbb{P}^n \times \mathbb{P}^m$ inside $\mathbb{P}^{N_{n,m}}$.

In this paper we are mainly interested to $\Sigma_{1,2} \subset \mathbb{P}^5$, so that we will choose particular symbols for our variables. Let $(s : t)$ and $(u : v : w)$ be coordinates in $\mathbb{P}^1$ and $\mathbb{P}^2$ respectively. Let $(a : b : c : d : e : f)$ be coordinates in $\mathbb{P}^5$. Then $s_{1,2}$ is given by:

$$\begin{aligned} a &= su \\ b &= sv \\ c &= sw \\ d &= tu \\ e &= tv \\ f &= tw. \end{aligned} \tag{1}$$

and in $\mathbb{P}^5$ we can define the smooth threefold

$$X := s_{1,2}(\mathbb{P}^1 \times \mathbb{P}^2)$$

whose equations are:

$$\begin{aligned} bf - ce &= 0 \\ cd - af &= 0 \\ ae - bd &= 0. \end{aligned} \tag{2}$$

Note that X can be also defined as the locus of points in $\mathbb{P}^5$ such that the following matrix N has rank at most 1:

$$N := \begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix}.$$

Note also that if we fix a point $(s : t)$ in $\mathbb{P}^1$ we get a uniquely determined plane in $\mathbb{P}^5$ contained in X. For instance if we choose $(1 : 0)$ we get the plane having equations $d = e = f = 0$. All these planes are two by two disjoint in $\mathbb{P}^5$.

Every linear isomorphism

$$\omega : \mathbb{P}^5 \to \mathbb{P}^5$$

is defined by a (6, 6) non-singular matrix Ω such that

$$\mathbf{y} = \Omega\mathbf{x}$$

where $\mathbf{y}$ and $\mathbf{x}$ are, respectively, the column vectors of the coordinates of points $\omega(P)$ and $P \in \mathbb{P}^5$. If we want to get the equations of $\omega(X)$ we have only to substitute in N the variables $a, b..., f$ with the corresponding linear forms given by the rows of Ω^{-1}. For instance (indicating the substitution with an arrow):

$$\begin{cases} ca \to [\textit{first row of } \Omega^{-1}] \times \mathbf{x} \\ b \to [\textit{second row of } \Omega^{-1}] \times \mathbf{x} \\ ... \end{cases}$$

where here $\times$ denotes the usual rows/columns product among matrices.

By any Computer Algebra System, as Macaulay, it is easy to see that, if we choose a generic linear isomorphism ω, the intersection between X and $\omega(X)$ is a smooth curve $\mathcal{C}$ of degree 9 and genus 4, but if we choose a generic linear isomorphism ω fixing a plane π contained in X, then $X \cap \omega(X)$ is the union of π and a smooth curve $\mathcal{C}$ of degree 6 and genus 1, i.e.:

$$X \cap \omega(X) = \mathcal{C} \cup \pi.$$

Moreover $\mathcal{C}$ intersects π at three distinct points with multiplicity 1 in such a way that, if we project $\mathcal{C}$ from π onto a disjoint plane in $\mathbb{P}^5$ (for instance a plane contained in X, different from π), we get a smooth plane curve Γ of degree 3 and genus 1.

Now, let us call π the plane having equations $d = e = f = 0$ and let us determine Γ as a function of ω. It is easy to see that all matrices Ω representing linear isomorphisms of $\mathbb{P}^5$ fixing π are of the following type:

$$\begin{bmatrix} * & * \\ 0 & * \end{bmatrix}$$

where $*$ are (3, 3) matrices and 0 is the (3, 3) zero matrix. Hence we have that Ω^{-1} is of the following type:

$$\Omega^{-1} = \begin{bmatrix} A & B \\ 0 & C \end{bmatrix}$$

where A and C are (3, 3) nonsingular matrices and B is any (3, 3) matrix. The product of Ω^{-1} with the coordinates of any point of $\mathbb{P}^5$ is the following:

$$\begin{aligned} \alpha_1(a:b:c) + \beta_1(d:e:f) \\ \alpha_2(a:b:c) + \beta_2(d:e:f) \\ \alpha_3(a:b:c) + \beta_3(d:e:f) \\ \gamma_1(d:e:f) \\ \gamma_2(d:e:f) \\ \gamma_3(d:e:f) \end{aligned}$$

where $\alpha_i(a:b:c)$ is a linear form whose coefficients are the entries of the $i-th$ row of A; $\beta_i(a:b:c)$ is a linear form whose coefficients are the entries of the $i-th$ row of B and similarly for γ_i and C. Hence $\omega(X)$ is defined as the locus of points in $\mathbb{P}^5$ such that the following matrix N_ω has rank at most 1:

$$N_\omega := \begin{bmatrix} \alpha_1 + \beta_1 & \alpha_2 + \beta_2 & \alpha_3 + \beta_3 \\ \gamma_1 & \gamma_2 & \gamma_3 \end{bmatrix}.$$

Now let us intersect X and $\omega(X)$ by using the parametric equations of X given by $s_{1,2}$ and we get the following three equations:

$$\begin{aligned} &(\alpha_1(su:sv:sw) + \beta_1(tu:tv:tw))\gamma_2(tu:tv:tw) = \\ &= (\alpha_2(su:sv:sw) + \beta_2(tu:tv:tw))\gamma_1(tu:tv:tw); \\ &(\alpha_1(su:sv:sw) + \beta_1(tu:tv:tw))\gamma_3(tu:tv:tw) = \\ &= (\alpha_3(su:sv:sw) + \beta_3(tu:tv:tw))\gamma_1(tu:tv:tw); \\ &(\alpha_2(su:sv:sw) + \beta_2(tu:tv:tw))\gamma_3(tu:tv:tw) = \\ &= (\alpha_3(su:sv:sw) + \beta_3(tu:tv:tw))\gamma_2(tu:tv:tw). \end{aligned} \tag{3}$$

Of course the solution $t = 0$ gives rise to the plane π. Dividing all equations by t and forgetting to write $(u:v:w)$ we get the following equations defining the residual curve $\mathcal{C}$ in $\mathbb{P}^1 \times \mathbb{P}^2$

$$\begin{aligned} s\alpha_1\gamma_2 + t\beta_1\gamma_2 - s\alpha_2\gamma_1 - t\beta_2\gamma_1 = 0 \\ s\alpha_1\gamma_3 + t\beta_1\gamma_3 - s\alpha_3\gamma_1 - t\beta_3\gamma_1 = 0 \\ s\alpha_2\gamma_3 + t\beta_2\gamma_3 - s\alpha_3\gamma_2 - t\beta_3\gamma_2 = 0 \end{aligned}$$

or:

$$\begin{aligned} s(\alpha_1\gamma_2 - \alpha_2\gamma_1) + t(\beta_1\gamma_2 - \beta_2\gamma_1) = 0 \\ s(\alpha_1\gamma_3 - \alpha_3\gamma_1) + t(\beta_1\gamma_3 - \beta_3\gamma_1) = 0 \\ s(\alpha_2\gamma_3 - \alpha_3\gamma_2) + t(\beta_2\gamma_3 - \beta_3\gamma_2) = 0. \end{aligned}$$

To project $\mathcal{C}$ into the "factor" $\mathbb{P}^2$, (which is projectively equivalent to project $\mathcal{C}$ into any plane of $\mathbb{P}^1 \times \mathbb{P}^2$ skew with π) it suffices to eliminate s, t from the above equations. It is very simple because they are three linear homogeneous equations in $(s : t)$ so that it suffices to impose that the above linear system has solutions. Apparently we get three conditions but they coincide with the following one:

$$(\alpha_1\beta_2 - \alpha_2\beta_1)\gamma_3 - (\alpha_1\beta_3 - \alpha_3\beta_1)\gamma_2 + (\alpha_2\beta_3 - \alpha_3\beta_2)\gamma_1 = 0$$

which is in turn the following one (recall that α_i, β_i and γ_i are linear forms in $(u : v : w)$):

$$det \begin{bmatrix} \alpha_1 & \beta_1 & \gamma_1 \\ \alpha_2 & \beta_2 & \gamma_2 \\ \alpha_3 & \beta_3 & \gamma_3 \end{bmatrix} = 0. \tag{4}$$

In conclusion of this section we can state the following Proposition whose proof is given by the above simple calculations.

Proposition 2.2 *Let X be the Segre embedding of $\mathbb{P}^1 \times \mathbb{P}^2 = (s : t) \times (u : v : w)$ in $\mathbb{P}^5$ with coordinates $(a : b : c : d : e : f)$. Let A, B, C be the three $(3, 3)$ matrices (A, C nonsingular) defining the inverse matrix Ω^{-1}:*

$$\begin{bmatrix} A & B \\ 0 & C \end{bmatrix}$$

of a linear isomorphism ω of $\mathbb{P}^5$ fixing the plane π: $d = e = f = 0$. Then the smooth projection Γ into $\mathbb{P}^2$ of the curve $\mathcal{C}$, residual with respect to π of $X \cap \omega(X)$, is the plane cubic having equation

$$det \begin{bmatrix} AL & BL & CL \end{bmatrix} = 0$$

where L is the transpose of $[u \;\; v \;\; w]$.

In what follows we will be interested in determining Γ without knowing Ω. Note that the above calculations prove also that this is possible from the equations defining $\omega(X)$: see the following Remark.

Remark 2.3 Let X, ω and Γ be as above for some unknown linear isomorphism ω of $\mathbb{P}^5$. Assume that we know the three quadratic equations defining $\omega(X)$, that is to say the three minors of matrix N_ω, then it is possible to get the equation of Γ in $\mathbb{P}^2$ simply:

- intersecting X and $\omega(X)$ by using (1) and getting three equations as in (3)
- dividing the three equations by t
- eliminating s, t as above from the three new equations.

We conclude this section with a last consideration. In our assumptions we have:

$$X \cap \omega(X) = \mathcal{C} \cup \pi.$$

If we apply ω^{-1}, recalling that ω fixes π, we get:

$$\omega^{-1}(X) \cap X = \omega^{-1}(\mathcal{C}) \cup \pi.$$

Obviously $\omega^{-1}(\mathcal{C})$ is projectively equivalent to $\mathcal{C}$, hence, if we project it in the same plane $\mathbb{P}^2$ as above, we get another smooth plane cubic curve, which is projectively equivalent to Γ.

Remark 2.4 All calculations made in this Section are based only on linear Algebra, without using inverse matrices. In particular they can be executed in every field with any characteristic. It follows that it is possible to get a homogeneous polynomial of degree three defining the smooth plane cubic curve Γ in any case.

3 Projective invariants for smooth cubic plane curves

In Sect. 2 we have seen that, if we consider the standard Segre embedding X of $\mathbb{P}^1 \times \mathbb{P}^2$ with coordinates $(s : t) \times (u : v : w)$ in $\mathbb{P}^5$ with coordinates $(a : b : c : d : e : f)$, and we choose any linear isomorphism ω of $\mathbb{P}^5$ fixing the plane π, then we get two smooth, projectively equivalent, cubic curves in the projective plane $(u : v : w)$.

One of them, say Γ_ω, is the projection of (the residual with respect to π of) $X \cap \omega(X)$, and the other one, say $\Gamma_{\omega^{-1}}$, is analogously the projection of $X \cap \omega^{-1}(X)$. If we know the matrices representing ω and ω^{-1} we can write down the polynomials in $(u : v : w)$ defining the two cubics as in (4). Otherwise, we can write down these polynomials in any case by starting with the three degree two equations defining $\omega(X)$ and $\omega^{-1}(X)$.

When we have two smooth, projectively equivalent, plane cubics we know that their j-invariants are the same. This invariant is an element of the base field $\mathbb{K}$, but in literature there are many different ways to calculate it, moreover the most part of the used formulas assume that the equation of the curve is written in a particular form, called "normal", which is always possible when $\mathbb{K}$ has zero characteristic, but not in any case.

Let us see how to get the j-invariant in our situation. Firstly let us write any polynomial defining a plane cubic curve in the following way (Greek letters are elements of $\mathbb{K}$) :

$$F := \begin{bmatrix} u & v & w \end{bmatrix} \begin{bmatrix} \alpha & \delta & \eta \\ \beta & \epsilon & \theta \\ \gamma & \zeta & \lambda \end{bmatrix} \begin{bmatrix} u^2 \\ v^2 \\ w^2 \end{bmatrix} + (\mu)uvw. \tag{5}$$

If $\mathrm{p} \neq 2$ and $\mathrm{p} \neq 3$, then we can assume that

$$F := \begin{bmatrix} u & v & w \end{bmatrix} \begin{bmatrix} \alpha' & 3\delta' & 3\eta' \\ 3\beta' & \epsilon' & 3\theta' \\ 3\gamma' & 3\zeta' & 3\lambda' \end{bmatrix} \begin{bmatrix} u^2 \\ v^2 \\ w^2 \end{bmatrix} + 6(\mu')uvw. \tag{6}$$

and in this case, depending on $\alpha'...\mu'$, there is a formula for calculating the j-invariant of the curve defined by $F = 0$ on the book of Sturmfels [6].

In fact, the above (6) is the same as (4.4.13) in [6] pag. 166. From this you can calculate a degree 4 projective invariant S as in Proposition 4.4.7 of [6]. Of course, as in the definition of S appears the number $18630 = 23 \cdot 5 \cdot 3^4 \cdot 2$, p must be different from 2, 3, 5, 23. Then, from (6), you can calculate a degree 6 invariant T as in Example 4.5.3 of [6], pag. 171. Note that S and T generate all projective invariants for F thanks to Theorem 4.4.6 of [6]. In any case we can calculate the j-invariant as follows (see [6] formula (4.5.8) pag. 173):

$$j(F) = \frac{S^3}{T^2 - 64S^3}. \tag{7}$$

Note that when the plane cubic curve defined by $F = 0$ is smooth, as we are assuming, $T^2 - 64S^3 \neq 0$ so that (7) can be used (see [6] pag 171).

Unfortunately S has 25 monomials and T has 203 monomials, whose coefficients are nonzero when $\mathrm{p} \neq 2, 3, 5$. However there are many Computer Algebra packages that can calculate the j-invariant for a polynomial F. For instance MAPLE; however, as the j-invariant can be defined in different ways identical (except for a constant factor) it is necessary to be careful. For instance, if we call Mj the j-invariant calculated by MAPLE, we have that $Mj(F) = -48^3 \cdot j(F)$; as $48 = 3 \cdot 2^4$ we see that our assumptions on characteristic p make this relation always meaningful.

If in (5) we have: $\beta = \delta = \epsilon = 0$ and $\alpha + \zeta = 0$, with $\alpha \neq 0$, then F/α is in "normal form", see [7] pag. 319, Proposition 4.6. In this case the j-invariant can be calculated in an easier way: see [7] pag. 317. However to put an arbitrary degree three polynomial in $(u : v : w)$, defining a smooth plane curve, in "normal form" requires to get at least a flex on the curve. It is not possible without solving some polynomial equations which could be a difficult problem when $\mathrm{p} > 0$, although it would be in principle always possible for $\mathrm{p} \neq 2$ (see [7], Proposition 4.6), but we prefer to avoid any nonlinear equation in this paper.

In what follows we will find it useful to calculate the j-invariant also when $\mathrm{p} = 2$. Previous formulas cannot help, so we will resort to Glynn's article [8]. Let us call (M, μ) the pair (matrix, element of $\mathbb{K}$) arising from (5). In Theorem 3.2 of [8] is defined a new pair (M', μ') as follows:

$$M' := \begin{bmatrix} \alpha\lambda + \theta\zeta & \beta\lambda + \theta\gamma & \beta\zeta + \epsilon\gamma \\ \delta\lambda + \eta\zeta & \alpha\lambda + \eta\gamma & \alpha\zeta + \delta\gamma \\ \delta\theta + \eta\epsilon & \alpha\theta + \eta\beta & \alpha\epsilon + \beta\delta \end{bmatrix} + \mu \begin{bmatrix} 0 & \eta & \delta \\ \theta & 0 & \beta \\ \zeta & \gamma & 0 \end{bmatrix}$$

$$\mu' := \mu^2.$$

Now let us consider another pair (M'', μ'') where $M'' := (M')'$ and $\mu'' := \mu^4$. Then the j-invariant can be calculated as follows (see Theorem 3.9 of [8]):

$$j(F) = \frac{\mu^{12}}{det(\mu^3 M + M'')}. \tag{8}$$

We were unable to find a single formula that is valid for every characteristic, unless F is in "normal form" and we cannot assume this fact: let us see why. As we have explained in Sect. 2 our degree three polynomials will depend on linear isomorphisms of $\mathbb{P}^5$ fixing the particular plane π. As we will see, such maps will be often the composition of other similar maps. It is possible to define isomorphisms (i.e. triples of matrices A, B, C as in Proposition 2.2), such that the polynomial F given by (4) is in "normal form", but the composition of such isomorphisms does not give an isomorphism with the same property. For instance, to get F in "normal form" it is necessary that $\epsilon = det(B) = 0$, and this property is not preserved by composing such isomorphisms.

4 A new type of key exchange

In this Section we will describe a key exchange based on the Segre product $\mathbb{P}^1 \times \mathbb{P}^2$, a slight generalization of the method suggested in [1] for $\mathbb{P}^1 \times \mathbb{P}^1$ with the aim of making it even safer. To explain the method as clearly as possible, here we do not consider security issues which will be postponed to next Section. As usual we call Alice and Bob two imaginary characters who exchange a key. Charlie will be the name of a third part trying to intercept the key.

Firstly let us recall the 2-Veronese embedding $\nu_5 : \mathbb{P}^5 \to \mathbb{P}^{20}$ given by

$$(a : b : c : d : e : f) \to (x_0 : x_1 : ... : x_{20}) \tag{9}$$

where: $x_0 = a^2$;$x_1 = ab$;....;$x_{20} = f^2$ in lexicographic order. For a brief discussion of Veronese's maps see the Appendix of [9], here is sufficient to say that the dual of the projective space $\mathbb{P}^{20}$ parametrizes all quadrics of $\mathbb{P}^5$. For instance the hyperplanes of $\mathbb{P}^{20}$ having coefficients

$$\begin{gathered}(0:0:0:0:1:0:0:0:0:-1:0:0:0:0:0:0:0:0:0:0:0:0)\\(0:0:0:0:0:1:0:0:0:0:0:0:-1:0:0:0:0:0:0:0:0)\\(0:0:0:0:0:0:0:0:0:0:0:1:0:0:-1:0:0:0:0:0:0)\end{gathered} \tag{10}$$

correspond to the three quadrics: $ae - bd, af - cd, bf - ce$ defining X. In the sequel we will call ν_n the 2-Veronese map defined on $\mathbb{P}^n$. Note that, from the above Appendix, the target of a d-Veronese map defined on $\mathbb{P}^5$ has dimension $\binom{d+5}{5}$, hence HPC is required for calculations when $d \gg 0$.

For any linear isomorphism $\omega : \mathbb{P}^5 \to \mathbb{P}^5$ represented by a (6, 6) matrix Ω there is a unique linear isomorphism $\tilde{\omega} : \mathbb{P}^{20} \to \mathbb{P}^{20}$ represented by a nonsingular (21, 21) matrix $\tilde{\Omega}$ such that $\tilde{\omega} \circ \nu_5 = \nu_5 \circ \omega$. In other words the following diagram is commutative:

$$\begin{array}{ccc} \mathbb{P}^5 & \xrightarrow{\omega} & \mathbb{P}^5 \\ \downarrow{\scriptstyle \nu_5} & & \downarrow{\scriptstyle \nu_5}. \\ \mathbb{P}^{20} & \xrightarrow{\tilde{\omega}} & \mathbb{P}^{20} \end{array}$$

Obviously, not all linear isomorphisms of $\mathbb{P}^{20}$ can be obtained in this way. In particular, if we choose a generic non singular (21, 21) matrix V it defines a linear isomorphism of $\mathbb{P}^{20}$ not coming from a linear isomorphism of $\mathbb{P}^5$, this fact will be crucial in the sequel.

Let us call $\underline{B}$ the (21, 1) matrix given by monomials $a^2, ab, ..., f^2$ in lexicographic order as above. Using the above notations we get that $\nu_5 \circ s_{1,2}$ is given by

$$\begin{aligned} &a^2 = s^2u^2; ab = s^2uv; ac = s^2uw; ad = stu^2; ae = stuv; af = stuw; \\ &b^2 = s^2v^2; bc = s^2vw; bd = stuv; be = stv^2; bf = stvw; \\ &c^2 = s^2w^2; cd = stuw; ce = stvw; cf = stw^2; \\ &d^2 = t^2u^2; de = t^2uv; df = t^2uw; e^2 = t^2v^2; ef = t^2vw; f^2 = t^2w^2. \end{aligned}$$

Now let us consider $s_{2,5} \circ (\nu_1 \times \nu_2)$, where $\nu_1 \times \nu_2 : \mathbb{P}^1 \times \mathbb{P}^2 \to \mathbb{P}^2 \times \mathbb{P}^5$ is the Segre product of the two 2-Veronese embeddings:

$$\begin{aligned} &(s : t) \to (s^2 : st : t^2) \\ &(u : v : w) \to (u^2 : uv : uw : v^2 : vw : w^2), \end{aligned}$$

and $s_{2,5} : \mathbb{P}^2 \times \mathbb{P}^5 \to \mathbb{P}^{17}$ is another Segre embedding. It is immediate to see that $s_{2,5} \circ (\nu_1 \times \nu_2)$ is given by the (18, 1) matrix $\underline{b}$ obtained by flattening the following one:

$$\begin{bmatrix} s^2 \\ st \\ t^2 \end{bmatrix} \begin{bmatrix} u^2 & uv & uw & v^2 & vw & w^2 \end{bmatrix}.$$

Then $\nu_5 \circ s_{1,2} = m \circ s_{2,5} \circ (\nu_1 \times \nu_2)$, where $m : \mathbb{P}^{17} \to \mathbb{P}^{20}$ is a suitable linear morphism represented by a maximal rank (21, 18) matrix M such that

$$M\underline{b} = \underline{B}. \tag{11}$$

Straightforward calculations show that M is a matrix given by three blocks: $M_1 := I_3$, $M_3 := I_6$ (I_n denotes the identity matrix of order n) and

$$M_2 := \begin{bmatrix} 0&0&0&1&0&0&0&0&0 \\ 0&0&0&0&1&0&0&0&0 \\ 0&0&0&0&0&1&0&0&0 \\ 1&0&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0&0 \\ 0&0&0&0&1&0&0&0&0 \\ 0&0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&1&0 \\ 0&0&1&0&0&0&0&0&0 \\ 0&0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&0&1 \end{bmatrix}. \tag{12}$$

Now, let $\mathbf{v}$ be any vector in $\mathbb{K}^{21}$. If we look for the solutions of the linear system (here $(..)^t$ means transposition; vectors are always column vectors):

$$\mathbf{v}^t M = \mathbf{0}^t \tag{13}$$

we get a three-dimensional vector space generated by $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$, the (column) vectors given by coefficients in (10); in fact we know that $\mathbf{v}_1^t \underline{B} = \mathbf{v}_2^t \underline{B} = \mathbf{v}_3^t \underline{B} = 0$ are the equations of X.

The key remark is that if we consider any fixed $\mathbf{u}$ in $\mathbb{K}^{21}$ and the corresponding quadric Q in $\mathbb{P}^5$ having equation $\mathbf{u}^t \underline{B} = 0$ then the equation $\mathbf{u}^t M \underline{b} = 0$ given by (11) and (13) allows to get a bidegree (1, 2) equation in $\mathbb{P}^1 \times \mathbb{P}^2$ defining $X \cap Q$, i.e. the divisor of $\mathbb{P}^1 \times \mathbb{P}^2$ cut by Q on X in $\mathbb{P}^5$.

Remark 4.1 Let $\mathbf{u}^t \underline{B} = 0$ be the equation of a quadric $Q \subset \mathbb{P}^5$ and let Ω and $\tilde{\Omega}$ be as above; then $\mathbf{u}^t \tilde{\Omega}^{-1} \underline{B} = 0$ is the equation of $\omega(Q)$, while $\mathbf{u}^t \tilde{\Omega} \underline{B} = 0$ is the equation of $\omega^{-1}(Q)$. Moreover $\mathbf{u}^t \tilde{\Omega}^{-1} M \underline{b} = 0$ defines of $X \cap \omega(Q)$ in $\mathbb{P}^1 \times \mathbb{P}^2$, while $\mathbf{u}^t \tilde{\Omega} M \underline{b} = 0$ defines $X \cap \omega^{-1}(Q)$.

In general, if Q_1, Q_2, Q_3 are three quadrics in $\mathbb{P}^5$, having equations respectively $\mathbf{u}_i^t \underline{B} = 0$ with $i = 1, 2, 3$, whose intersection is some variety $\mathcal{V}$, then $\mathbf{u}^{\mathbf{t}}{}_i M \underline{b} = 0$ with $i = 1, 2, 3$ defines the intersection $X \cap \mathcal{V}$ in $\mathbb{P}^1 \times \mathbb{P}^2$.

Now we can prove the following

Proposition 4.2 *Let $\omega : \mathbb{P}^5 \to \mathbb{P}^5$ be a linear isomorphism fixing plane π and let Ω and $\tilde{\Omega}$ be the matrices representing ω and, respectively, its induced isomorphism on $\mathbb{P}^{20}$ as explained above. Then the solutions of the linear system*

$$\mathbf{v}^t \tilde{\Omega} M = \mathbf{0}^t$$

give rise to a three-dimensional vector space, say $\langle \mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_3 \rangle$, such that the three bidegree (1, 2) equations $\mathbf{w}_i^t M \underline{b} = 0$ in $\mathbb{P}^1 \times \mathbb{P}^2$ define $X \cap \omega(X)$, and allow to determine an equation for Γ_ω as explained in Sect. 2.

Proof By recalling 4.1 we have that, for any quadric $Q \subset \mathbb{P}^5$ having equation $\mathbf{u}^t B = 0$, the equation of $\omega(Q)$ is $\mathbf{u}^t \tilde{\Omega}^{-1} \underline{B} = 0$. Then the equations of $\omega(X)$ are $\mathbf{v}_i^t \tilde{\Omega}^{-1} \underline{B} = 0$ for $i = 1, 2, 3$, where vectors $\mathbf{v}_i$ are the vectors in (10). Such vectors $\mathbf{v}_i^t \tilde{\Omega}^{-1}$ are solutions of $\mathbf{v}^t \tilde{\Omega} M = \mathbf{0}^t$ because $\mathbf{v}_i$ are solutions of $\mathbf{v}^t M = \mathbf{0}^t$. Then we can use Remark 4.1 with $\mathcal{V} = \omega(X)$. Last property comes from the fact that ω fixes π.

□

Now we can define an algorithm for exchanging keys inspired from the one in [1].

(1) Alice chooses a generic linear isomorphism φ_a of $\mathbb{P}^5$ fixing π, determines the matrix $\tilde{\Phi}_a$ representing the induced isomorphism in $\mathbb{P}^{20}$ and solves the linear system:

$$\mathbf{v}^t \tilde{\Phi}_a M = \mathbf{0}^t. \tag{14}$$

Then chooses another pair ϕ_1 and ϕ_2 of linear morphisms of $\mathbb{P}^5$ fixing π and determines the matrices $\tilde{\Delta}_1$ and $\tilde{\Delta}_2$ of the induced morphisms in $\mathbb{P}^{20}$.

(2) Alice publishes three independent solutions $\mathbf{v}_{a1}, \mathbf{v}_{a2}, \mathbf{v}_{a3}$ of (14) and the matrices $\tilde{\Delta}_1$ and $\tilde{\Delta}_2$.

(3) Bob chooses a random string of $2n$ integers $j_1, j_2, ..., j_{2n}$ and calculates $\tilde{\Phi}_b := \tilde{\Delta}_1^{j_1} \tilde{\Delta}_2^{j_2} ... \tilde{\Delta}_2^{j_{2n}}$ (representing in $\mathbb{P}^{20}$ the linear isomorphism $\varphi_b := \phi_1^{j_1} \phi_2^{j_2} .... \phi_2^{j_{2n}}$ fixing π). Then solves the linear system:

$$\mathbf{v}^t \tilde{\Phi}_b M = \mathbf{0}^t. \tag{15}$$

(4) Bob publishes three independent solutions $\mathbf{v}_{b1}, \mathbf{v}_{b2}, \mathbf{v}_{b3}$ of (15).

(5) For $i = 1, 2, 3$, Alice considers $\mathbf{v}^{\mathbf{t}}{}_{bi} \tilde{\Phi}_a M \underline{b} = 0$, which are three bidegree (1, 2) equations in $\mathbb{P}^1 \times \mathbb{P}^2$ defining $X \cap \varphi_a^{-1}(\varphi_b(X)) = \pi \cup \mathcal{C}_a$. In fact $\mathbf{v}_{bi}^t$ are the coefficients of the quadrics defining $\varphi_b(X)$; if they are multiplied by $\tilde{\Phi}_a$ you get the coefficients of quadrics defining $\varphi_a^{-1}(\varphi_b(X))$. Then Alice determines the j-invariant of the smooth plane cubic curve Γ_a which is the projection of $\mathcal{C}_a$ in $\mathbb{P}^2$ with coordinates $(u : v : w)$ as we explained in Sect. 3.

(6) For $i = 1, 2, 3$, Bob considers $\mathbf{v}^{\mathbf{t}}{}_{ai} \tilde{\Phi}_b M \underline{b} = 0$, which are three bidegree (1, 2) equations in $\mathbb{P}^1 \times \mathbb{P}^2$ defining $X \cap \varphi_b^{-1}(\varphi_a(X)) = \pi \cup \mathcal{C}_b$ (similarly to 5)). Then Bob determines the j-invariant of the smooth plane cubic curve Γ_b which is the projection of $\mathcal{C}_b$ in $\mathbb{P}^2$ with coordinates $(u : v : w)$ as we explained in Sect. 3.

The two above j-invariants are equal because $X \cap \varphi_a^{-1}(\varphi_b(X))$ is projectively equivalent in $\mathbb{P}^5$ to $\varphi_a(X) \cap \varphi_b(X)$ by φ_a, which is in turn equivalent to $X \cap \varphi_b^{-1}(\varphi_a(X))$ by φ_b. It follows that $\mathcal{C}_a$ is projectively equivalent to $\mathcal{C}_b$ and therefore the same happens for the two plane curves Γ_a and Γ_b. The element of $\mathbb{K}$ which is the common j-invariant of the two curves is in fact the key exchanged between Alice and Bob.

Remark 4.3 For generic choices of $\varphi_a; \phi_1; \phi_2; j_1 ... j_{2n}$; $\mathcal{C}_a$ and $\mathcal{C}_b$ are smooth and the same happens for Γ_a and Γ_b. However, if for some unlucky choice, Γ_a or Γ_b are singular the j-invariant cannot be calculated: if $\mathrm{p} \neq 2$ recall that for singular cubics $T^2 - 64S^3 = 0$ hence formula (7) cannot be used; if $\mathrm{p} = 2$, for singular cubics $det(\mu^3 M + M'') = 0$ (see [8], Cor. 3.12) hence formula (8) cannot be used. In any

case it is not possible to get a mistake; if some singular curve occurs it suffices to make other choices.

5 Encrypt of the key exchange

The key exchange algorithm defined in Sect. 4 is not secret. A third part, say Charlie, knows the equations of $\varphi_a(X)$ i.e. $\mathbf{v}_{ai}^t \underline{B} = 0$ and the equations of $\varphi_b(X)$ i.e. $\mathbf{v}_{bi}^t \underline{B} = 0$ in $\mathbb{P}^5$ from steps 2) and 4) of the algorithm. Hence Charlie knows the equations of the curve $\mathcal{C}$, the residual with respect to π in $\varphi_a(X) \cap \varphi_b(X)$. $\mathcal{C}$ is a smooth sextic curve of genus 1 and in principle it can be possible to calculate its j-invariant, which is the same as the j-invariant of Γ_a and Γ_b. Of course it is not easy: Charlie must project $\mathcal{C}$ from a 3-secant generic plane to a generic disjoint plane to get a smooth plane cubic curve and then use formulas (7) or (8). Or Charlie could be define a double covering $\mathcal{C} \to \mathbb{P}^1$ and calculate the j-invariant from it (see [7], pag. 317). Although there is not a simple way to calculate $j(\mathcal{C})$, however *in principle* it is possible, so the key exchange algorithm defined in Sect. 4 cannot be considered safe. To this aim we can proceed more or less as in [1] and we modify the above algorithm as follows.

5.1 Non-standard embedding of $\mathbb{P}^1 \times \mathbb{P}^2$

The fundamental relation (11) relies on matrix M, which is known. As we will see in Sect. 6 to make safe the algorithm it is useful to change this relation. It depends on the standard embedding (1), but Alice can use a non-standard one.

Let us choose generic linear isomorphisms $\lambda : \mathbb{P}^1 \to \mathbb{P}^1$ and $\theta : \mathbb{P}^2 \to \mathbb{P}^2$ to get the map $\lambda \times \theta : \mathbb{P}^1 \times \mathbb{P}^2 \to \mathbb{P}^1 \times \mathbb{P}^2$. Then let us consider the composition $\nu_5 \circ s_{1,2} \circ (\lambda \times \theta) : \mathbb{P}^1 \times \mathbb{P}^2 \to \mathbb{P}^{20}$. We have the following

Proposition 5.1 *Let $\nu_5 \circ s_{1,2} \circ (\lambda \times \theta)$ be the above defined map. Then*

(*i*) $\nu_5 \circ s_{1,2} \circ (\lambda \times \theta) = m \circ s_{2,5} \circ (\nu_1 \times \nu_2) \circ (\lambda \times \theta)$ *where m is the same map introduced in Sect. 4 and represented by M*;

(*ii*) *the* (21, 18) *matrix $\bar{M}$ satisfying the relation* (*corresponding to* (11) *in such embedding*)

$$\bar{M} \underline{b} = \underline{B} \tag{16}$$

is such that $\bar{M} = MR$ where R is a suitable (18, 18) *nonsingular matrix, hence $\bar{M}$ has maximal rank*;

(*iii*) *the equations of X in $\mathbb{P}^5$ are the same as when using standard embedding*.

Proof (i) Obvious because we know that $\nu_5 \circ s_{1,2} = m \circ s_{2,5} \circ (\nu_1 \times \nu_2)$ from Sect. 4.

(ii) Let Λ and Θ be the matrices representing λ and θ respectively. Such maps induce two isomorphisms $\tilde{\lambda} : \mathbb{P}^2 \to \mathbb{P}^2$ and $\tilde{\theta} : \mathbb{P}^5 \to \mathbb{P}^5$, via 2-Veronese embeddings, such that

$$(\tilde{\lambda} \times \tilde{\theta}) \circ (\nu_1 \times \nu_2) = (\nu_1 \times \nu_2) \circ (\lambda \times \theta)$$

The matrices representing $\tilde{\lambda}$ and $\tilde{\theta}$ can be computed taking into account that now

$$\begin{bmatrix} s \\ t \end{bmatrix} \to \Lambda^{-1} \begin{bmatrix} s \\ t \end{bmatrix} \qquad \begin{bmatrix} u \\ v \\ w \end{bmatrix} \to \Theta^{-1} \begin{bmatrix} u \\ v \\ w \end{bmatrix} \tag{17}$$

and their determinants are $det(\Lambda)^{-3} \neq 0$ and $det(\Theta)^{-5} \neq 0$ respectively, so that $\tilde{\lambda}$ and $\tilde{\theta}$ are isomorphisms. In turn $\tilde{\lambda} \times \tilde{\theta}$ induces a linear isomorphism $\rho : \mathbb{P}^{17} \to \mathbb{P}^{17}$, represented by a (18, 18) matrix R, such that the following diagram is commutative:

$$\begin{array}{ccccc} \mathbb{P}^1 \times \mathbb{P}^2 & \xrightarrow{\nu_1 \times \nu_2} & \mathbb{P}^2 \times \mathbb{P}^5 & \xrightarrow{s_{2,5}} & \mathbb{P}^{17} \\ \downarrow{\scriptstyle \lambda \times \theta} & & \downarrow{\scriptstyle \tilde{\lambda} \times \tilde{\theta}} & & \downarrow{\scriptstyle \rho} \\ \mathbb{P}^1 \times \mathbb{P}^2 & \xrightarrow{\nu_1 \times \nu_2} & \mathbb{P}^2 \times \mathbb{P}^5 & \xrightarrow{s_{2,5}} & \mathbb{P}^{17} \end{array}$$

moreover $det(R) = det(\Lambda)^{-3} det(\Theta)^{-5} \neq 0$. Putting all things together we have that:

$$\nu_5 \circ s_{1,2} \circ (\lambda \times \theta) = m \circ \rho \circ s_{2,5} \circ (\nu_1 \times \nu_2);$$

therefore the maximal rank matrix $\bar{M}$ defined in (16) is such that $\bar{M} = MR$.

(iii) When the embedding of $\mathbb{P}^1 \times \mathbb{P}^2$ is standard the equations of X in $\mathbb{P}^5$ are defined by the solutions of (13). If not, they are defined by $\mathbf{v}^t \bar{M} = \mathbf{0}^t$. As $\bar{M} = MR$ and $det(R) \neq 0$ we have the same solutions.

□

Although equations of X are the same by using non-standard embedding the same is not true for the equation of the curve Γ_ω which is the projection in $\mathbb{P}^2$ of the residual with respect to π of the intersection $X \cap \omega(X)$ where ω is a linear isomorphism of $\mathbb{P}^5$ fixing π as in Sect. 2. However the two curves are projectively equivalent under the action of θ.

Proposition 5.2 *Let us consider a non-standard embedding $\mathbb{P}^1 \times \mathbb{P}^2$ in $\mathbb{P}^5$ as above. Let $\omega : \mathbb{P}^5 \to \mathbb{P}^5$ be a linear isomorphism fixing π defined by three matrices A, B, C as in Sect. 2). Let Γ_ω be the degree 3 plane cubic curve as recalled above.*

Then the equation of this curve is given by

$$det \left[A\bar{L}\ B\bar{L}\ C\bar{L} \right] = 0$$

where $\bar{L} = L\Theta^{-t}$ *and* L *is the transpose of* $[u \ v \ w]$.

Proof Let us proceed as in Sect. 2 until equations (3). Now we have to change variables according to (17). As a first step let us change only s and t. It is possible to divide the new equations (3) by a linear form in $(s : t)$ corresponding to π (in standard embedding the form is simply t). Then we get a linear system S of three equations in s, t whose (3, 2) matrix is the product of the same matrix in $\alpha_i, \beta_i, \gamma_i$ of the standard case and the nonsingular matrix Λ^{-1}.

Of course the conditions under which S has solutions are exactly the same as in standard case. So we get the same as (4). Now if we substitute the variables (u, v, w) as in (17) we get the equation

$$det\left[A\bar{L} \ B\bar{L} \ C\bar{L}\right] = 0.$$

□

5.2 The algorithm

In this subsection we describe the algorithm we propose for exchanging a key, which will be an element of $\mathbb{K}$. It will be a safe version of the algorithm defined in Sect. 4. We assume that the field $\mathbb{K}$ is known to both Alice and Bob.

I) Firstly Alice chooses (secretly):

- a generic nonsingular (2, 2) matrix Λ defining a linear isomorphism $\lambda : \mathbb{P}^1 \to \mathbb{P}^1$;
- a generic nonsingular (3, 3) matrix Θ representing a linear isomorphism $\theta : \mathbb{P}^2 \to \mathbb{P}^2$;
- a generic nonsingular (21, 21) matrix V defining a linear isomorphism $\psi : \mathbb{P}^{20} \to \mathbb{P}^{20}$.

Then she determines a secret matrix $\bar{M}$ as explained in Sect. 5.1 by using λ and θ. Matrix V allows to define a new secret base $\hat{\underline{B}} := V\underline{B}$ for the 21-dimensional vector space of degree two monomials in $(a : b : c : d : e : f)$ such that the fundamental relation (11) becomes:

$$V\bar{M}\underline{b} = V\underline{B} = \hat{\underline{B}}. \tag{18}$$

Alice chooses a generic linear isomorphism φ_a of $\mathbb{P}^5$ fixing π, determines the matrix $\tilde{\Phi}_a$ as before, but now she considers the matrix $V\tilde{\Phi}_a V^{-1}$ representing the induced isomorphism in $\mathbb{P}^{20}$ with respect the new and secret base $\hat{\underline{B}}$. Then Alice solves the linear system

$$\mathbf{v}^t(V\tilde{\Phi}_a V^{-1})V\bar{M} = \mathbf{v}^t V\tilde{\Phi}_a\bar{M} = \mathbf{0}. \tag{19}$$

As a last thing Alice chooses another pair ϕ_1 and ϕ_2 of linear morphisms of $\mathbb{P}^5$ fixing π and determines the matrices $\tilde{\Delta}_1$ and $\tilde{\Delta}_2$ of the induced morphisms in $\mathbb{P}^{20}$.

(II) Alice publishes three independent solutions $\hat{\mathbf{v}}_{a1}, \hat{\mathbf{v}}_{a2}, \hat{\mathbf{v}}_{a3}$ of (19) and the matrices $V\tilde{\Delta}_1 V^{-1}$ and $V\tilde{\Delta}_2 V^{-1}$ and moreover the matrix $V\bar{M}$. Obviously $\hat{\mathbf{v}}_{ai}^t V = \mathbf{v}_{ai}^t$ for any i.

(III) Bob chooses a random string of $2n$ integers $j_1, j_2, ..., j_{2n}$ and calculates

$$\begin{aligned} & V\tilde{\Phi}_b V^{-1} \\ & := (V\tilde{\Delta}_1 V^{-1})^{j_1}(V\tilde{\Delta}_2 V^{-1})^{j_2}...(V\tilde{\Delta}_2 V^{-1})^{j_{2n}} \\ & = (V\tilde{\Delta}_1^{j_1} V^{-1})(V\tilde{\Delta}_2^{j_2} V^{-1})...(V\tilde{\Delta}_2^{j_{2n}} V^{-1}) \\ & = V(\tilde{\Delta}_1^{j_1}\tilde{\Delta}_2^{j_2}...\tilde{\Delta}_2^{j_{2n}})V^{-1} \end{aligned}$$

representing in $\mathbb{P}^{20}$ the linear isomorphism $\varphi_b := \phi_1^{j_1}\phi_2^{j_2}....\phi_2^{j_{2n}}$, fixing π, with respect to the new and secret base $\underline{\hat{B}}$. Then solves the linear system:

$$\mathbf{v}^t(V\tilde{\Phi}_b V^{-1})V\bar{M} = \mathbf{v}^t V\tilde{\Phi}_b\bar{M} = \mathbf{0}^t. \tag{20}$$

Note that to solve the above system Bob needs not to know matrices V and $\bar{M}$. It suffices to know the public matrix $V\bar{M}$ and the matrix $V\tilde{\Phi}_b V^{-1}$ he has defined.

A comment regarding Bob's choice of $2n$ integers. For the functioning of the algorithm this choice is irrelevant however it has consequences on the time needed to perform the necessary calculations, in particular if d-Veronese embeddings are used. Another reason to require the use of HPC.

IV) Bob publishes three independent solutions $\hat{\mathbf{v}}_{b1}, \hat{\mathbf{v}}_{b2}, \hat{\mathbf{v}}_{b3}$ of (20). Obviously $\hat{\mathbf{v}}_{bi}^t V = \mathbf{v}_{bi}^t$ for any i.

V) For $i = 1, 2, 3$, Alice considers

$$\hat{\mathbf{v}}_{bi}^t(V\hat{\Phi}_a V^{-1})(V\bar{M})\underline{b} = \mathbf{v}_{bi}^t\tilde{\Phi}_a\bar{M}\underline{b}$$

which are three bidegree (1, 2) equations in $\mathbb{P}^1 \times \mathbb{P}^2$, as in 5) of the previous algorithm, defining $X \cap \varphi_a^{-1}(\varphi_b(X)) = \pi \cup \mathcal{C}_a$ although these varieties have been embedded in $\mathbb{P}^{20}$ by ν_5. Then she determines the j-invariant of the smooth plane cubic curve Γ_a which is the projection of $\mathcal{C}_a$ in $\mathbb{P}^2$ with coordinates $(u : v : w)$ as we explained in Sect. 3. As we have seen in Sect. 5.1 this curve is not the same as in 5) of the previous algorithm, but the two plane curves are projectively equivalent via θ.

VI) For $i = 1, 2, 3$, Bob considers

$$\hat{\mathbf{v}}_{ai}^t(V\hat{\Phi}_b V^{-1})(V\bar{M})\underline{b} = \mathbf{v}_{ai}^t\tilde{\Phi}_b\bar{M}\underline{b}$$

which are three bidegree (1, 2) equations, as in 6) of the previous algorithm, defining $X \cap \varphi_b^{-1}(\varphi_a(X)) = \pi \cup \mathcal{C}_b$ although these varieties have been embedded in $\mathbb{P}^{20}$ by ν_5. Then he determines the j-invariant of the smooth plane cubic curve Γ_b which is the projection of $\mathcal{C}_b$ in $\mathbb{P}^2$ with coordinates $(u : v : w)$ as we explained in Sect. 3. As we have seen in Sect. 5.1 this curve is not the same as in 6) of the previous algorithm, but the two plane curves are projectively equivalent via θ.

5.3 The algorithm works

In this brief subsection we want to explain why the above algorithm is safer than the previous one.

Note that, contrary to what happens with the algorithm of Sect. 4, now Charlie cannot recover the equations of $\varphi_a(X)$ and $\varphi_b(X)$. In fact everyone knows the public coefficients ($\hat{\mathbf{v}}_{ai}$ and $\hat{\mathbf{v}}_{bi}$ respectively, see steps II) and IV)) of the quadrics defining $\varphi_a(X)$ and $\varphi_b(X)$ with respect to the base $\underline{\hat{B}}$, but nobody knows this secret base except Alice.

The crucial point is that, as V is generic, ψ is a linear isomorphism of $\mathbb{P}^{20}$ not induced by a linear isomorphism of $\mathbb{P}^5$, otherwise the public coefficients $\hat{\mathbf{v}}_{ai}$ and $\hat{\mathbf{v}}_{bi}$ would define two varieties W_a and W_b (both intersection of three quadrics) projectively equivalent in $\mathbb{P}^5$ to $\varphi_a(X)$ and $\varphi_b(X)$ respectively. Hence Charlie could determine a curve $\mathcal{D}$, projectively equivalent to that contained in $\varphi_a(X) \cap \varphi_b(X)$, simply considering $W_a \cap W_b$ and then he could calculate $j(\mathcal{D}) = j(\mathcal{C})$. As ψ is not induced by a linear isomorphism of $\mathbb{P}^5$ the intersection $W_a \cap W_b$ is not projectively equivalent to $\varphi_a(X) \cap \varphi_b(X)$.

Obviously the knowledge of V would break the method because $\underline{\hat{B}} = V\underline{B}$ and base $\underline{\hat{B}}$ would become known. We will deal with this fact in the next Section.

6 Security analysis

6.1 Possible attacks

Of course the secretness of the key exchange algorithm defined in Sect. 5 relies only on matrix V, because all the mathematical background is supposed to be known.

If Alice chooses a standard Segre embedding $\mathbb{P}^1 \times \mathbb{P}^2 \to \mathbb{P}^5$, i.e. $\bar{M} = M$, then, as matrix VM is public (step II), it is possible to solve a linear system of $21 \times 18 = 378$ equations in $21 \times 21 = 441$ unknowns to get V.

Such linear system has infinitely many solutions (the rank of its associated matrix is maximal because V is generic) more precisely the solutions give rise to a vector space of dimension 63 in $\mathbb{K}^{441}$: a number of cases to examine much too big with respect to $|\mathbb{K}|$. In any case this strategy is not possible if Alice chooses a non-standard embedding because, in this case, $\bar{M}$ is not known.

However there is a more insidious attack that can be performed to know V. In fact V represents a linear isomorphism $\psi : \mathbb{P}^{20} \to \mathbb{P}^{20}$. By knowing the equations of a variety $\mathcal{X} \subset \mathbb{P}^{20}$ (not contained in projective space of smaller dimension i.e. $\langle \mathcal{X} \rangle = \mathbb{P}^{20}$) and the equations of $\psi(\mathcal{X})$ *in principle* it is possible to recover matrix V of ψ, simply transforming all equations of $\mathcal{X}$ with the rows of an unknown matrix V and then imposing that such new equations coincide with the known equations of $\psi(\mathcal{X})$.

In our case the above strategy leads to a nonlinear system of a huge number of equations, so it is not practicable. But there exists another way to recover V by using the *Lie Algebras method* (see [5, 10, 11]). In short, this technique provides to determine the Lie Algebras associated to $\mathcal{X}$ and to $\psi(\mathcal{X})$, to determine a suitable

isomorphism I between them and to calculate V from I. Although the method is not completely clear in details (at least to the authors) especially with regard to determine I, we think that it should be taken in serious consideration in all cases when embedded projective varieties are used to exchange keys.

In our situation we have two candidates for the role of $\mathcal{X}$: $\nu_5(X)$ and $\nu_5(\mathbb{P}^5)$ because the equations of both of them are public (recall that the equations of $X \in \mathbb{P}^5$ are known, see (2), and they are not changed by non-standard embeddings), however $\nu_5(X)$ is the intersection of $\nu_5(\mathbb{P}^5)$ with three hyperplanes, corresponding to quadrics defining $X \subset \mathbb{P}^5$, hence $\langle \nu_5(X) \rangle \neq \mathbb{P}^{20}$ (here $\langle .. \rangle$ means the linear span); hence the Lie Algebra method can be applied only to $\mathcal{X} := \nu_5(\mathbb{P}^5)$. The equations of $\mathcal{X}$ are known: it easy to see they are 105 degree two polynomials. *A priori* the equations of $\psi(\mathcal{X})$ are not known, however there exists a way to get them. The idea is due to W. Castryck (see [9] for a similar case):

- pick random points in $\mathbb{P}^1 \times \mathbb{P}^2$ with their coordinates $(s : t)$ and $(u : v : w)$ and map them into $\psi(\mathcal{X})$ using $V\bar{M}$, known by step II). Note that these points are confined inside $\psi(\nu_5(X)) \subset \psi(\nu_5(\mathbb{P}^5)) = \psi(\mathcal{X})$.
- Move the above mapped points from $\psi(\nu_5(X))$ to $\psi(\mathcal{X})$ by using random compositions of matrices $V\tilde{\Delta}_1 V^{-1}$ and $V\tilde{\Delta}_2 V^{-1}$, known by step II). Note that, as the linear isomorphisms represented by $\tilde{\Delta}_1$ and $\tilde{\Delta}_2$ come from ϕ_1 and ϕ_2 respectively, these isomorphisms fix $\mathcal{X} \subset \mathbb{P}^{20}$ but not pointwise, hence the morphisms represented by $V\tilde{\Delta}_1 V^{-1}$ and $V\tilde{\Delta}_2 V^{-1}$ can be used to move points inside $\psi(\mathcal{X})$.
- Starting with a degree two polynomial (a quadric in $\mathbb{P}^{20}$) 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 105: any base of this space defines $\psi(\mathcal{X})$.

Due to the above procedure we have to assume that the equations of $\psi(\mathcal{X})$ are known too, hence the Lie Algebras method could be unfortunately applied.

A simple choice making our proposed algorithm unassailable by this method is to use very low $\mathtt{p}$. To associate a Lie Algebra to $\mathcal{X}$ requires calculation of some derivatives which cannot performed with low $\mathtt{p}$. For instance if $\mathtt{p} = 2$ the attack surely fails; this is why we spent time to get formulas for j-invariants of cubic plane curves with $k = 2$ in Sect. 3. However low characteristics are not always desirable for various reasons, especially $k = 2$, therefore here we give a countermeasure that will likely run in other cases, not only in this one, when the Lie Algebra method could pose a danger.

6.2 Projections of algebraic varieties

Let us define projections from points in projective spaces and let us recall some properties. Let us fix a point $\mathbf{p}$ in some projective space $\mathbb{P}^n$ (here $\mathbf{p}$ denotes both the point and the column vector of its coordinates) and a hyperplane $H \simeq \mathbb{P}^{n-1}$ disjoint from $\mathbf{p}$. Let $W \in \mathbb{P}^n$ be any smooth projective variety. Let $\langle \mathbf{p}, \mathbf{q} \rangle$ be the

line passing through two distinct points $\mathbf{p}, \mathbf{q} \in \mathbb{P}^n$. The projection $p : \mathbb{P}^n \backslash \mathbf{p} \to H$ is defined as follows for any point $\mathbf{q} \neq \mathbf{p}$:

$$\mathbf{q} \to \langle \mathbf{p}, \mathbf{q} \rangle \cap H. \tag{21}$$

Let us collect in the following list some properties of p (see for instance [12]):

(i) If we restrict p to W we get a map $p_{|W} : W \to p(W)$. The fibers of $p_{|W}$, the smoothness/singularities of $p(W)$, the degree of $p(W)$ and the equations defining $p(W)$ depend on the secant lines to W passing through $\mathbf{p}$ (a secant line is a line intersecting W in at least two points, eventually coincident).

(ii) $p(W)$ is smooth if no secant line to W passes through $\mathbf{p}$; as secant lines give rise to a variety of dimension at most $2dim(W) + 1$ if $2dim(W) + 1 < n$ then $p(W)$ is smooth for generic $\mathbf{p}$.

(iii) It is possible to find matrices representing p: any $(n, n+1)$ matrix P with maximal rank such that $P\mathbf{p} = \mathbf{0}$ is fine. By using such a matrix P we have that $p(\mathbf{q}) = P\mathbf{q}$.

(iv) Let $\phi : \mathbb{P}^n \to \mathbb{P}^n$ be a linear isomorphism such that $\phi(\mathbf{p}) = \mathbf{p}$ and let Φ be a $(n+1, n+1)$ matrix representing ϕ, then ϕ induces a linear isomorphism $\phi' : \mathbb{P}^{n-1} \to \mathbb{P}^{n-1}$ such that $\phi' \circ p = p \circ \phi$ (see the following commutative diagram)

$$\begin{array}{ccc} \mathbb{P}^n & \xrightarrow{\phi} & \mathbb{P}^n \\ \downarrow p & & \downarrow p \\ \mathbb{P}^{n-1} & \xrightarrow{\phi'} & \mathbb{P}^{n-1} \end{array}$$

if PP^t is a nonsingular (n, n) matrix, then the following matrix Φ' represents ϕ':

$$\Phi' := (P\Phi P^t)(PP^t)^{-1}.$$

We can summarize up in the following commutative diagram the relations between any projection $p : \mathbb{P}^{20} \to \mathbb{P}^{19}$ and some previously defined maps:

$$\begin{array}{ccccccccc} \mathbb{P}^1 \times \mathbb{P}^2 & \xrightarrow{\lambda \times \theta} & \mathbb{P}^1 \times \mathbb{P}^2 & \xrightarrow{s_{1,2}} & \mathbb{P}^5 & \xrightarrow{\nu_5} & \mathbb{P}^{20} & \xrightarrow{p} & \mathbb{P}^{19} \\ \downarrow id & & \downarrow id & & \downarrow \varphi & & \downarrow \tilde{\varphi} & & \downarrow \tilde{\varphi}' \\ \mathbb{P}^1 \times \mathbb{P}^2 & \xrightarrow{\lambda \times \theta} & \mathbb{P}^1 \times \mathbb{P}^2 & \xrightarrow{s_{1,2}} & \mathbb{P}^5 & \xrightarrow{\nu_5} & \mathbb{P}^{20} & \xrightarrow{p} & \mathbb{P}^{19} \end{array}$$

where φ fixes π and some generic point $\mathcal{P} \in \mathbb{P}^5$, $\tilde{\varphi}$ fixes $\mathbf{p} := \nu_5(\mathcal{P})$ and $\tilde{\varphi}'$ is defined as the map ϕ' above.

To illustrate what was said in (i) we give the following example (for the properties of Veronese surface see [13] or [12]):

Example 6.1 Assume that p $\neq 2$ and let us consider $\nu_2 : \mathbb{P}^2 \to \mathbb{P}^5$; let S be $\nu_2(\mathbb{P}^2)$. $S \subset \mathbb{P}^5$ is a smooth surface of degree 4, called Veronese surface, which has the following equations in the standard embedding:

$$ad - b^2 = ae - bc = be - cd = df - e^2 = af - c^2 = bf - ce = 0.$$

A remarkable property of S is that its secant variety $Sec(S)$ is a hypersurface of degree 3 having equation:

$$adf + 2bce - c^2d - ae^2 - b^2f = 0.$$

If we project S from a generic point $\mathbf{p} \in \mathbb{P}^5$ we get a smooth surface in $\mathbb{P}^4$ of degree 4; for instance if $\mathbf{p} = (0 : 1 : 0 : 0 : 0 : 1)$ we get the following equations on the left, if $\mathbf{p} = (1 : 0 : 0 : 1 : 0 : 1)$ we get the following equations on the right:

$$\begin{cases} cd^2 - bde - e^3 = 0; \\ c^2d - ae^2 = 0; \\ bcd - ade + ce^2 = 0; \\ b^2d - ad^2 + cde + be^2 = 0; \\ acd - abe - c^2e = 0; \\ abc + c^3 - a^2e = 0; \\ ab^2 + bc^2 - a^2d + ace = 0; \end{cases} \qquad \begin{cases} c^3 + acd - cd^2 - abe + bde - ce^2 = 0 \\ bcd - b^2e + c^2e = 0 \\ bc^2 - ace + cde - be^2 = 0 \\ b^2c - abe - ce^2 = 0 \\ b^3 - abd - ace - be^2 = 0 \\ abc - a^2e - b^2e + ade + e^3 = 0 \\ ab^2 - ac^2 - a^2d - b^2d + ad^2 + de^2 = 0. \end{cases}$$

If we project S from a generic point $\mathbf{p} \in Sec(S)\backslash S$ we get a singular surface in $\mathbb{P}^4$ of degree 4; for instance if $\mathbf{p} = (0 : 1 : 0 : 0 : 0 : 0)$ we get:

$$df - e^2 = af - c^2 = 0$$

which is singular along the line $c = e = f = 0$. If we project S from a generic point $\mathbf{p} \in S$ we get a smooth surface in $\mathbb{P}^4$ of degree 3; for instance if $\mathbf{p} = (4 : 2 : 2 : 1 : 1 : 1)$ we get:

$$cd - be - ce + 2e^2 = bc - c^2 - ae + 2ce = b^2 - c^2 - ad + 4ce - 4e^2 = 0.$$

All above computations were made by the help of *Macaulay*. As we see, the number, the degree and the equations themselves defining the projection of S depend on the chosen point $\mathbf{p}$.

6.3 A safer version of the algorithm

Taking into account the possible attack described in Sect. 6.1 and what we have seen in Sect. 6.2 now we can give a refined version of the algorithm suggested in Sect. 5.2. Firstly we make the following remarks.

- The Veronese embedding $\mathcal{X} = \nu_5(\mathbb{P}^5) \subset \mathbb{P}^{20}$ does not contain lines. Hence, if we project $p : \mathbb{P}^{20} \to \mathbb{P}^{19}$ from a point $\mathbf{p} \in \mathcal{X}$, $\mathbf{p} = \nu_5(\mathcal{P})$, with $\mathcal{P} \notin X$ generic in $\mathbb{P}^5$, then we have that $p(\nu_5(X))$ is smooth and isomorphic to X. The same is true also for the projection of any intersection $\nu_5(X) \cap \nu_5(\omega(X))$ where ω is a linear morphism of $\mathbb{P}^5$ such that $\omega(\mathcal{P}) = \mathcal{P}$, hence $\mathcal{P} \notin \omega(X)$.
- Moreover, if we call P the matrix representing p as in Sect. 6.2 and we consider any $\mathbf{u}$ in $\mathbb{K}^{20}$ such that $\mathbf{u}^t P \underline{B} = 0$ is the equation of a quadric Q in $\mathbb{P}^5$,

then $\mathbf{u}^t PM\underline{b} = 0$ is a bidegree (1, 2) equation in $\mathbb{P}^1 \times \mathbb{P}^2 = 0$ defining $X \cap Q$, ($\mathbf{u}^t P\bar{M}\underline{b} = 0$ for non-standard embedding).
- If $\psi : \mathbb{P}^{19} \to \mathbb{P}^{19}$ is a linear isomorphism represented by a (20, 20) matrix V, then the previous item is true replacing $\mathbf{u}^t$ with $\mathbf{u}^t V$.

From the properties recalled above it follows that we can define $X \cap \omega(X) \simeq p(\nu_5(X) \cap \nu_5(\omega(X)))$ as in Remark 4.1.

Here is the refined version of the algorithm.

(I) Alice chooses (secretly):

- a generic nonsingular (2, 2) matrix Λ defining a linear isomorphism $\lambda : \mathbb{P}^1 \to \mathbb{P}^1$;
- a generic nonsingular (3, 3) matrix Θ defining a linear isomorphism $\theta : \mathbb{P}^2 \to \mathbb{P}^2$;
- a generic point $\mathcal{P} \in \mathbb{P}^5$ with $\mathcal{P} \notin X$ and the point $\mathbf{p} := \nu_5(\mathcal{P}) \in \nu_5(\mathbb{P}^5) \subset \mathbb{P}^{20}$;
- a generic (20, 21) matrix P such that $P(\mathbf{p}) = 0$ defining a secret projection $p : \mathbb{P}^{20} \to \mathbb{P}^{19}$ as in 6.2; in particular P have to be chosen such that PP^t is nonsingular (and this is generically true);
- a generic nonsingular (20, 20) matrix V representing a linear isomorphism $\psi : \mathbb{P}^{19} \to \mathbb{P}^{19}$.

Then Alice determines a secret matrix $\bar{M}$ as explained in Sect. 5.1 by using λ and θ and she multiplies $P\bar{M}$. Now the fundamental relation (11) becomes:

$$VP\bar{M}\underline{b} = VP\underline{B} = \underline{\hat{B}'} \tag{22}$$

Note that now $\underline{\hat{B}'}$ is a base of a 20-dimensional subspace of degree two monomials in $(a : b : c : d : e : f)$.

Alice chooses a generic linear isomorphism φ_a of $\mathbb{P}^5$ fixing π and $\mathcal{P}$ so that the induced linear isomorphism $\tilde{\varphi}_a$ of $\mathbb{P}^{20}$ fixes $\mathbf{p}$ and gives rise to a linear isomorphism $\tilde{\varphi}'_a$ in $\mathbb{P}^{19}$. Then she determines the matrix $\tilde{\Phi}_a$ as before and the (20, 20) matrix $\tilde{\Phi}'_a$, defining the induced linear morphism in $\mathbb{P}^{19}$, as explained in 6.2, and she considers the matrix $V\tilde{\Phi}'_a V^{-1}$ representing the induced isomorphism in $\mathbb{P}^{19}$ by ψ. Then Alice solves the linear system:

$$\mathbf{v}^t(V\tilde{\Phi}'_a V^{-1})VP\bar{M} = \mathbf{v}^t V\tilde{\Phi}'_a P\bar{M} = \mathbf{0}^t. \tag{23}$$

As a last thing Alice chooses another pair ϕ_1 and ϕ_2 of linear morphisms of $\mathbb{P}^5$ fixing π and $\mathcal{P}$ and determines the (20, 20) matrices $\tilde{\Delta}'_1$ and $\tilde{\Delta}'_2$ of the induced morphisms in $\mathbb{P}^{19}$, as above.

II) Alice publishes three independent solutions $\hat{\mathbf{v}}_{a1}, \hat{\mathbf{v}}_{a2}, \hat{\mathbf{v}}_{a3}$ of (23), the matrices $V\tilde{\Delta}'_1 V^{-1}$ and $V\tilde{\Delta}'_2 V^{-1}$ and moreover the (20, 18) matrix $VP\bar{M}$.

III) Bob chooses a random string of $2n$ integers $j_1, j_2, ..., j_{2n}$ and calculates (note that now they are all (20, 20) matrices):

$$
\begin{aligned}
&V\tilde{\Phi}'_b V^{-1}\\
&:= (V\tilde{\Delta}'_1 V^{-1})^{j_1}(V\tilde{\Delta}'_2 V^{-1})^{j_2}...(V\tilde{\Delta}'_2 V^{-1})^{j_{2n}}\\
&= (V\tilde{\Delta}'^{j_1}_1 V^{-1})(V\tilde{\Delta}'^{j_2}_2 V^{-1})...(V\tilde{\Delta}'^{j_{2n}}_2 V^{-1})\\
&= V(\tilde{\Delta}'^{j_1}_1\tilde{\Delta}'^{j_2}_2...\tilde{\Delta}'^{j_{2n}}_2)V^{-1}
\end{aligned}
$$

representing in $\mathbb{P}^{19}$ the linear isomorphism induced (via p, as in 6.2, and by ψ), by $\tilde{\varphi}_b := \tilde{\phi}_1^{j_1}\tilde{\phi}_2^{j_2}....\tilde{\phi}_2^{j_{2n}} : \mathbb{P}^{20} \to \mathbb{P}^{20}$, fixing π and $\mathbf{p}$. Then Bob solves the linear system:

$$\mathbf{v}^t(V\tilde{\Phi}'_b V^{-1})VP\bar{M} = \mathbf{v}^t V\tilde{\Phi}'_b P\bar{M} = \mathbf{0}^t. \tag{24}$$

Note that to solve the above system Bob needs not to know matrices V, P and $\bar{M}$. It suffices to know the public matrix $VP\bar{M}$ and the matrix $V\tilde{\Phi}'_b V^{-1}$ he has defined. Of course, the same considerations on HPC made in point III of the original algorithm apply.

IV) Bob publishes three independent solutions $\hat{\mathbf{v}}_{b1}, \hat{\mathbf{v}}_{b2}, \hat{\mathbf{v}}_{b3}$ of (24).

V) For $i = 1, 2, 3$, Alice considers

$$\hat{\mathbf{v}}^t_{bi}(V\hat{\Phi}'_a V^{-1})(VP\bar{M})\underline{b} = \hat{\mathbf{v}}^t_{bi} V\tilde{\Phi}'_a P\bar{M}\underline{b} = 0 \tag{25}$$

which are three bidegree (1, 2) equations in $\mathbb{P}^1 \times \mathbb{P}^2$ defining the intersection $X \cap \varphi_a^{-1}(\varphi_b(X)) = \pi \cup \mathcal{C}_a$ as explained in previous items. Then Alice determines the j-invariant of the smooth plane cubic curve Γ_a in $\mathbb{P}^2$ with coordinates $(u : v : w)$ as we explained in Sect. 3.

VI) For $i = 1, 2, 3$, Bob considers

$$\hat{\mathbf{v}}^t_{ai}(V\hat{\Phi}'_b V^{-1})(VP\bar{M})\underline{b} = \hat{\mathbf{v}}^t_{ai} V\tilde{\Phi}'_b P\bar{M}\underline{b} = 0 \tag{26}$$

which are three bidegree (1, 2) equations as in 6) of the previous algorithm defining $X \cap \varphi_b^{-1}(\varphi_a(X)) = \pi \cup \mathcal{C}_b$. Then Bob determines the j-invariant of the smooth plane cubic curve Γ_b in $\mathbb{P}^2$ with coordinates $(u : v : w)$ as we explained in Sect. 3.

The above refinement of the algorithm acts like the previous one, but the morphism represented by V now is defined in $\mathbb{P}^{19}$, via projection p. This fact makes it impossible to use the attack described in 6.1. As we have seen, it would be necessary to know the equations of $p(\mathcal{X})$ and $\psi(p(\mathcal{X}))$ where $\mathcal{X} = \nu_5(\mathbb{P}^5)$. The equations of $\psi(p(\mathcal{X}))$ can be recovered by arguing as in items of Sect. 6.1, but now the equations of $p(\mathcal{X})$ depend on the secret choice of $\mathcal{P} \in \mathbb{P}^5$. They can be determined only by Alice, knowing p, but she needs not do it.

6.4 Key size comparison and computational complexity

In this Subsection we give an estimate of the size (in bytes) of the keys used in the algorithm proposed in 6.3. Of course we assume that the order of $\mathbb{K}$ is sufficiently large $\approx 2^{32}$ to satisfy standards of AES-128 bit security level.

The public keys pk are only the published vectors, three each for Alice and Bob. Each of them has 20 entries, so we get 180 entries. The secret keys sk are given by the (20, 18) matrices of the linear systems (23) and (24), hence we get 720 entries.

In the following Table 1 we collect some other values (see [9]).

As far concerning the computational complexity we remark that the above method does not depend on some variable integer, hence we have precise values. We need only to multiply matrices, determine the inverse of some matrices and solve linear systems. It is not required to solve nonlinear equations.

Taking into account that:

- to multiply two matrices of size (α, β) and (β, γ) requires $\alpha\beta\gamma$ products;
- to calculate the inverse of a (n, n) matrix requires n^3 products;
- to solve a linear systems of N equations in $N + h$ unknowns requires $max(N^3, N^2h)$ products;

we have that every calculation in our algorithm requires at most $20^2 \cdot 21$ products (to calculate $P^t(PP^t)^{-1}$).

7 Toy example

Here we show how the algorithm in Sect. 6.3 works using a very simple example over a field $\mathbb{K}$ with $\mathrm{p} \gg 0$. We use a different Segre product to avoid too big matrices in our paper and, by the way, this proves that our method could also work with other Segre products. For products of large projective spaces it may be necessary to use HPC capabilities.

Let us consider:

$$\mathbb{P}^1 \times \mathbb{P}^1 \xrightarrow{s_{1,1}} \mathbb{P}^3 \xrightarrow{\nu_3} \mathbb{P}^9 \xrightarrow{p} \mathbb{P}^8$$

where we use coordinates $(s : t)$ and $(v : w)$ in $\mathbb{P}^1 \times \mathbb{P}^1$, coordinates $(x : y : z : u)$ in $\mathbb{P}^3$, coordinates $(x_0 : x_1 : ... : x_9)$ and $(y_0 : y_1 : ... : y_8)$ in $\mathbb{P}^9$ and $\mathbb{P}^8$ respectively; $s_{1,1}$ is the standard Segre embedding:

$$x = sv; \quad y = sw; \quad z = tv; \quad u = tw;$$

Table 1 Key size comparison

Schemes	sk	pk
Classic Mc Eliace	6492	261120
Kyber	1632	800
QSI key exchange	2448000	10880
CSI	13920	960
This paper	720	180

whose image is the quadric $X \subset \mathbb{P}^3$ having equation $xu - zy = 0$. ν_3 is the standard 2-Veronese embedding of $\mathbb{P}^3$:

$$x_0 = x^2; \quad x_1 = xy \quad x_2 = xz; \quad x_3 = xu; \quad x_4 = y^2;$$
$$x_5 = yz; \quad x_6 = yu; \quad x_7 = z^2; \quad x_8 = zu; \quad x_9 = u^2.$$

Let us choose point $\mathbf{p} := (0 : 0 : 1 : 1) \in X$ and its image $\mathcal{P} := \nu_3(\mathbf{p}) = (0 : 0 : 0 : 0 : 0 : 0 : 1 : 1 : 1)$; p is the projection from $\mathcal{P}$:

$$y_0 = x_0; \quad y_1 = x_1 \quad y_2 = x_2; \quad y_3 = x_3; \quad y_4 = x_4$$
$$y_5 = x_5; \quad y_6 = x_6; \quad y_7 = x_7 - x_9; \quad y_8 = x_8 - x_9.$$

Note that here we have chosen a point $\mathbf{p} \in X$ such that $\mathcal{P} \in \nu_3(X)$ which is the intersection of $\nu_3(\mathbb{P}^3)$ and a hyperplane H in $\mathbb{P}^9$, otherwise $p(H) = \mathbb{P}^8$ and the systems as (23) and (24) would have only $\mathbf{0}$ as solution. In this toy example, for any generic linear isomorphism $\omega : \mathbb{P}^3 \to \mathbb{P}^3$ fixing $\mathbf{p}$ here we have that $X \cap \omega(X)$ is a smooth elliptic quartic curve $\mathcal{C}$ passing through $\mathbf{p}$, but the method allows to recover the bidegree (2, 2) divisor corresponding to $\mathcal{C}$ in $\mathbb{P}^1 \times \mathbb{P}^1$.

On consequence of the above choices we have:

$$P = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \end{bmatrix} \quad M = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Now Alice chooses a generic (9, 9) matrix V defining a linear isomorphism $\psi : \mathbb{P}^8 \to \mathbb{P}^8$ and two (4, 4) matrices defining two linear isomorphisms $\varphi_a : \mathbb{P}^3 \to \mathbb{P}^3$ and $\phi : \mathbb{P}^3 \to \mathbb{P}^3$ fixing $\mathbf{p}$:

$$V = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 & 0 \\ 3 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 1 & -1 & 1 & 1 \\ 1 & -1 & 1 & 1 & 0 & 0 & 2 & 1 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 & 1 & -1 \\ 4 & 7 & -1 & 1 \\ -12 & -23 & 5 & -1 \\ -4 & -4 & 4 & 0 \end{bmatrix} \qquad \begin{bmatrix} -1 & 2 & 1 & -1 \\ 1 & 2 & -1 & 1 \\ 1 & 2 & 3 & 1 \\ -3 & 6 & 3 & 1 \end{bmatrix}.$$

Then Alice determines: the (10, 10) matrix $\tilde{\Phi}_a$ representing the induced isomorphism by φ_a in $\mathbb{P}^9$; the (9, 9) matrix $\tilde{\Phi}'_a = P\tilde{\Phi}_a P^t(PP^t)^{-1}$ representing the induced isomorphism in $\mathbb{P}^8$ by the projection p and the matrix $V\tilde{\Phi}'_a V^{-1}$ representing the induced isomorphism in $\mathbb{P}^8$ by ψ. At the end Alice gets the following (9, 9) matrix $A_s := (V\tilde{\Phi}'_a V^{-1})VPM$:

$$A_s = \begin{bmatrix} 16 & 44 & 29 & -20 & -26 & 2 & 5 & -6 & 1 \\ -48 & -172 & -153 & 36 & 46 & -38 & -5 & 6 & -1 \\ 0 & -12 & -23 & -12 & -6 & 22 & 5 & -6 & 1 \\ 0 & -32 & -54 & -32 & -4 & 52 & 18 & -20 & 2 \\ 16 & 56 & 52 & -8 & 0 & 8 & 4 & -8 & 4 \\ 176 & 664 & 603 & -136 & -2548 & 66 & 15 & -18 & 3 \\ 96 & 412 & 424 & -68 & -120 & 68 & 12 & -16 & 4 \\ 176 & 696 & 676 & -120 & -212 & 72 & 16 & -20 & 4 \\ 32 & 116 & 90 & -28 & -72 & -8 & 2 & 0 & -2 \end{bmatrix}$$

and solves the linear system $\mathbf{v}^t A_s = \mathbf{0}^t$ having the unique solution (up to a constant):

$$\mathbf{v}_a^t = (10/9, -7/36, 35/9, -31/24, -1/9, -25/18, -5/36, 41/36, 1).$$

Then Alice determines: the (10, 10) matrix $\tilde{\Delta}$ representing the induced isomorphism by ϕ in $\mathbb{P}^9$; the (9, 9) matrix $\tilde{\Delta}' = P\tilde{\Delta}P^t(PP^t)^{-1}$ representing the induced isomorphism in $\mathbb{P}^8$ by the projection p and the matrix $V\tilde{\Delta}'V^{-1}$ representing the induced isomorphism in $\mathbb{P}^8$ by ψ.

Alice publishes the above solution and the two (9, 9) matrices $V\tilde{\Delta}'V^{-1}$ and VPM, where $7V\tilde{\Delta}'V^{-1} =$

$$\begin{bmatrix} 112 & 42 & -84 & 7 & -56 & 0 & 14 & 14 & -28 \\ -22 & 7/2 & 0 & 33/4 & 33 & 17 & -5/2 & -71/2 & -3 \\ -26 & 105/2 & 0 & -17/4 & -17 & 15 & -11/2 & 23/2 & -29 \\ 36 & 154 & 1148 & -17 & -40 & 88 & 34 & -38 & -144 \\ -96 & 70 & -112 & 57/11 & 4 & 36 & -58 & 50 & -92 \\ -552 & 441/2 & 28 & 975/4 & -103 & -87 & -667/2 & 883/14 & 45 \\ -310 & 119 & 112 & 201/2 & -4 & 20 & -145 & 139 & -48 \\ -90 & 833/2 & 56 & 401/4 & -103 & -31 & -261/2 & 2751/4 & -11 \\ -146 & 49 & 112 & 99/2 & -40 & -24 & -99 & -109 & 52 \end{bmatrix}$$

$$VPM = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 \\ 3 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 1 & -1 & 1 & 1 & -2 \\ 1 & -1 & 0 & 1 & 1 & 2 & 1 & 0 & -1 \\ 2 & 0 & 0 & 0 & -1 & 0 & 1 & 0 & -1 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \end{bmatrix}.$$

In this toy example Bob simply chooses $\varphi_b = \phi^2$, hence he calculates $V\tilde{\Phi}'_b V^{-1} := V\tilde{\Delta}'^2 V^{-1}$ and the (9, 9) matrix $B_s := (V\tilde{\Phi}'_b V^{-1})VPM$:

$$B_s = \begin{bmatrix} 76 & -64 & -176 & -24 & 72 & -160 & 12 & -8 & -4 \\ 25 & 4 & 164 & -74 & 102 & 84 & 1 & -18 & 17 \\ 7 & 124 & -36 & 74 & -38 & 44 & -33 & 18 & 15 \\ 140 & 464 & -144 & 136 & 40 & 144 & -84 & -24 & 108 \\ 156 & -144 & 112 & -120 & 136 & -16 & 28 & -56 & 28 \\ -101 & -692 & 300 & 18 & 50 & -452 & 131 & 122 & -253 \\ 6 & -88 & 312 & -44 & 132 & 40 & 70 & -12 & -58 \\ 21 & -300 & -172 & -82 & 94 & -380 & 141 & -10 & -131 \\ -114 & 86 & -40 & 52 & -92 & -88 & 30 & 68 & -98 \end{bmatrix}$$

then Bob solves the linear system $\mathbf{v}^t B_s = \mathbf{0}^t$ having the unique solution (up to a constant):

$$\mathbf{v}_b^t = (47/31, -61/31, -118/31, 1/2, 5/31, -1/31, 1, -44/31, 1)$$

and he publishes the above solution.

Now Alice gets the (2, 2) bidegree polynomial $DA := \mathbf{v}_b^t V\tilde{\Phi}'_a PM\underline{b}$:

$$\begin{aligned} 31DA = &-192s^2v^2 - 1160s^2vw - 1580s^2w^2 + 184stv^2 \\ &+ 248stvw - 712stw^2 - 36t^2v^2 + 112t^2vw - 76t^2w^2 \end{aligned}$$

and Bob gets the (2, 2) bidegree polynomial $DB := \mathbf{v}_a^t V\tilde{\Phi}'_b PM\underline{b}$:

$$9DB = -378s^2v^2 - 4200s^2vw - 8008s^2w^2 + 476stv^2 \\ - 2044stvw - 952stw^2 - 98t^2v^2 - 84t^2vw + 182t^2w^2.$$

From the above bidegree polynomials it is possible to calculate the j-invariant of the corresponding elliptic curves by using, for instance, the method in [1], appendix B. Both Alice and Bob get

$$J = 1541199117151/656233710075 \in \mathbb{K}.$$

which is the exchanged key in this example.

Acknowledgements We wish to thank: W. Castryck for discussions about the Lie algebra attack; G. Ottaviani for having pointed out Sturmfel's book and its formulas for calculating j-invariant of projective smooth plane cubic curves; the anonymous referees for their comments and suggestions.

Author contributions A.A and A.T. wrote the entire manuscript and reviewed it.

Data availability No datasets were generated or analysed during the current study.

Declarations

Conflict of interest The authors declare no competing interests.

References

1. Di Tullio D, Gyawali M (2023) A post quantum key-exchange protocol from the intersection of quadric surfaces. J Supercomput 79:16529–16558
2. Berlekamp ER, McEliece RJ, van Tilborg H (1978) On the inherent intractability of certain coding problems. IEEE Trans Inform Theory 24(3):384–386
3. De Feo L, Jao D, Plût J (2014) Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. J Math Cryptol 8:209–247
4. Castryck W, Lange T, Martindale C, Panny L, Renes J (2018) 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
5. Pilnikova J Parametrizing algebraic varieties using Lie Algebras. arxiv:math/0610727
6. Sturmfels B (2008) Algorithms in invariant theory. Springer, Wien, New York
7. Hartshorne R (1997) Algebraic geometry GTM 52. Springer, New York
8. Glynn DG (1998) On cubic curves in projective planes of Characteristic two Australas. J Combin 17:1–20
9. Alzati A, Di Tullio D, Gyawali M, Tortora A (2025) A post quantum key-exchange protocol from the intersection of conics. J Symbol Comput 126:102343
10. de Graaf W, Harrison M, Pilnikova J, Schicho J (2006) A Lie Algebra method for rational parametrization of Severi Brauer surfaces. J Algebra 303:514–529
11. Castryck W (2023) Private communication based on the talk. On the hardness of cryptosystems based on disguised Veronese varieties. In: SIAM Conference on Applied Algebraic Geometry, Eindhoven
12. Harris J (1992) Algebraic geometry, a first course GTM 133. Springer, Berlin Heidelberg

13. Ciliberto C (2021) An undergraduate primer in algebraic geometry. Unitext. Springer-Verlag, Berlin Heidelberg