A post-quantum key exchange protocol from the intersection of quadric surfaces

Daniele Di Tullio1 · Manoj Gyawali1

Accepted: 26 February 2023 / Published online: 28 April 2023
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2023

Abstract
In this paper, we present a new key exchange protocol in which Alice and Bob have secret keys given by quadric surfaces embedded in a large ambient space by means of the Veronese embedding and public keys given by hyperplanes containing the embedded quadrics. Both of them reconstruct the isomorphism class of the intersection which is a curve of genus 1, and is uniquely determined by the $j$-invariant. An eavesdropper, to find this $j$-invariant, has to solve problems which are conjecturally quantum-resistant.

Keywords Post-quantum cryptography · Quadric surfaces · Veronese embedding · Segre embedding

1 Introduction

Bringing difficult mathematical problems to cryptography is required not only to connect abstract mathematics to the real-world applications but also to make cryptography stronger and applicable. Many classical mathematical problems like factorization and discrete logarithm are vulnerable to quantum attack after the algorithm by Shor [20] in 1994. The algorithm by Shor created a threat to the cryptographic world, and then, the necessity of the post-quantum system was realized. In 2016, the US government agency National Institute of Standards and Technology (NIST) put a call for new post-quantum cryptographic algorithms to systematize the post-quantum candidates in near future [24], and its third and fourth rounds suggested many candidates for public-key encryption, key establishment algorithms and digital signatures based on various mathematical problems. Currently, there are five major
post-quantum areas of research are carried out, and four of them are discussed in [4] including lattice-based cryptography based on lattice problems, code-based cryptography based on a problem of distinguishing a random code from a masked Goppa code, 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 an NP-hard problem, hash-based cryptography based on one-way hash functions and isogeny-based cryptography based on isogeny problems, see for ex. [8, 9].

In a research community, many researchers believe to have quantum supremacy in near future where high-performance computer and network system known as quantum internet [12–14] could exist. A research towards post-quantum cryptography is aimed to maintain possible security in such a scenario.

In this paper, we propose a key exchange protocol whose security relies on various problems in computational algebraic geometry, like solving large system of polynomial equations with high degree in many variables, or finding the primary decomposition of an ideal generated by many polynomials in many variables, which we conjecture to be quantum-safe problems.

In a nutshell, Alice chooses a quadric surface embedded in a large projective space by the means of the Segre and the Veronese map. She gives some informations like an embedding and an automorphism of the variety so that Bob can generate an embedding which is required to agree on a common key. Both Bob and Alice have their respective embeddings by which they hide their secret quadric surfaces; instead, they publish their corresponding hyperplanes containing the images of their respective embeddings. Now, by using their private embeddings they compute the pullback of each other’s hyperplanes, recover a (2, 2) homogeneous curve and finally compute the $j$-invariant of the components. Under some heuristic assumptions, both parties are able to get such components with high probability. The $j$-invariants are equal, which is the common keys for both Alice and Bob. Notwithstanding the availability of the public data, an attacker is not able to recover information on private data because of the assumptions on the underlying problems.

2 Preliminaries

In this section, we discuss briefly a background of Segre and Veronese embeddings. These terminologies are already common in the literature such as in [18, 19, 25], and we consider that they are taken from those references unless otherwise stated.

2.1 Quadratic hypersurface

Let $\mathbb{P}^n = \mathbb{P}^n_{\kappa} = (\kappa^{n+1} \setminus \{0\}) / \sim$ be the projective space of dimension $n$ for any field $\kappa$.

**Definition 1** A quadratic hypersurface or quadric surface in the projective space $\mathbb{P}^n$ is the zero set of a homogeneous polynomial $G \in \kappa[z_0, \ldots, z_n]$ of the form
A post-quantum key exchange protocol from the intersection…

Elliptic curve arises as an intersection of two quadric surfaces. For a general choice of two quadric surfaces $Q_1, Q_2 \subset \mathbb{P}^3$, the intersection $Q_1 \cap Q_2$ is isomorphic to an elliptic curve, whose isomorphism class is determined by the j-invariant.

We will observe quadric surfaces as the images of Segre embeddings. Segre embedding embeds the product of two projective spaces into a bigger projective space.

**Definition 2** The standard Segre embeddings are the morphisms of the projective varieties

$$
\mathbb{P}^n \times \mathbb{P}^m \xrightarrow{s_{n,m}} \mathbb{P}^{(m+1)(n+1)-1} \ni ([x_0 : \ldots : x_n], [y_0 : \ldots : y_m])
$$

where $x_i, y_j$'s are ordered according to the standard lexicographical order. The images of these embeddings are called standard Segre varieties and are denoted by $\Sigma_{n,m}$.

**Example 1** For the Segre embedding

$$
\mathbb{P}^1 \times \mathbb{P}^1 \xrightarrow{s_{1,1}} \mathbb{P}^3 \ni ([x_0 : x_1], [y_0 : y_1]) \mapsto [x_0 y_0 : x_0 y_1 : x_1 y_0 : x_1 y_1],
$$

we have $s_{1,1}(\mathbb{P}^1 \times \mathbb{P}^1) = \Sigma_{1,1} \subset \mathbb{P}^3$ and $\Sigma_{1,1}$ is a smooth quadric surface defined by the equation

$$
z_0 z_3 = z_1 z_2,
$$

where $[z_0 : z_1 : z_2 : z_3]$ is the coordinate of $\mathbb{P}^3$.

Smooth quadric hypersurface are unique up to projective isomorphism.

**Lemma 1** All the smooth quadric hypersurfaces of $\mathbb{P}^n$ are projectively isomorphic.

**Proof** See in [15, Exercise 5.12].

2.2 Curve as an intersection of quadric surfaces

By a bi-homogeneous polynomial of bi-degree $(u, v)$ in $n + m$ variables: $F(x_1, \ldots , x_n, y_1, \ldots , y_m)$, we mean $F$ is homogeneous in $x_i$ of degree $u$ and homogeneous in $y_j$ of degree $v$.

The intersection of two quadric surfaces in $\mathbb{P}^3$ is a curve of bi-degree $(2, 2)$. 

\[ G = \sum_{i=0}^{n} c_i z_i^2 + \sum_{i=0}^{n} \sum_{j=i+1}^{n} c_{i,j} z_i z_j. \]
Suppose we have two smooth quadric surfaces $Q_1, Q_2$. From Lemma 1, we can choose a projective isomorphism $f : \mathbb{P}^3 \to \mathbb{P}^3$ such that $f(Q_1) = \Sigma_{1,1}$. Assume that $Q_1 = \Sigma_{1,1}$, then $Q_1 \cap Q_2 \cong s_{1,1}^{-1}(Q_2) \subset \mathbb{P}^1 \times \mathbb{P}^1$. Let
\[
G(z_0, z_1, z_2, z_3) := a_1 z_0^2 + a_2 z_1^2 + a_3 z_2^2 + a_4 z_3^2 + a_5 z_0 z_1 + \ldots + a_{10} z_2 z_3
\]
be the quadratic form defining $Q_2$, then $s_{1,1}^{-1}(Q_2)$ is defined in $\mathbb{P}^1 \times \mathbb{P}^1$ by a bi-homogeneous polynomial of bi-degree $(2,2)$
\[
F(x_0, x_1; y_0, y_1) := G(x_0 y_0, x_0 y_1, x_1 y_0, x_1 y_1),
\]
which is called the pullback of the polynomial $G$ through $s_{1,1}$.

Since $Q_1 \cap Q_2$ is isomorphic to an elliptic curve, let us denote it by $C$, we consider $C$ up to isomorphism. We want to find its $j$-invariant.

A standard result in the theory of algebraic curves is that there is the bijection
\[
\begin{align*}
\{ \text{genus 1 curves up to isomorphism} \} & \quad \leftrightarrow \quad \{ \text{4-tuples of distinct points of } \mathbb{P}^1 \text{ up to automorphism} \}
\end{align*}
\]
See, for example, in [25, 19.5].

Let $\pi : C \to \mathbb{P}^1$ be any degree 2 morphism. Then the 4-tuple of points associated with $C$ are the branch locus of $\pi$ that are, by definition, the points $P \in \mathbb{P}^1$ such that $\#\pi^{-1}(P) = 1$.

**Example 2** Let $E$ be the elliptic curve defined by the equation $y^2 z = f(x, z)$, where $f(x, z) = (x - az)(x - bz)(x - cz)$, let
\[
E \xrightarrow{\pi} \mathbb{P}^1, \quad [x : y : z] \xrightarrow{\pi} [x : z]
\]
be a degree 2 map. The branch locus of $\pi$ is the set $\{[1 : 0], [a : 1], [b : 1], [c : 1]\}$.

We have $C \subset \mathbb{P}^1 \times \mathbb{P}^1$ and suppose
\[
C \xrightarrow{\pi} \mathbb{P}^1, \quad (P, Q) \mapsto P
\]
be the projection in the first coordinate. Then the 4-tuple of points in $\mathbb{P}^1$ corresponding to $C$ are the points $P \in \mathbb{P}^1$ such that $\#\pi^{-1}(P) = 1$. Now, we write Eq. 1 in the following form
\[
F(x_0, x_1; y_0, y_1) = y_0^2 F_0(x_0, x_1) + y_0 y_1 F_1(x_0, x_1) + y_1^2 F_2(x_0, x_1),
\]
which is the defining polynomial of $C$. Then the branch locus of $\pi$ is the set of points $P = [X_0, X_1]$ such that the equation
\[
F(X_0, X_1; Y_0, Y_1) = 0
\]
has single but repeated solution.
Therefore, the discriminant of \( F(X_0, X_1; y_0, y_1) \) is zero, and hence, \([X_0, X_1]\) is the solution of the polynomial
\[
H(x_0, x_1) := F_1(x_0, x_1)^2 - 4F_0(x_0, x_1)F_2(x_0 x_1).
\]
Writing
\[
H(x_0, x_1) = q_0 x_0^4 + q_1 x_0^3 x_1 + q_2 x_0^2 x_1^2 + q_3 x_0 x_1^3 + q_4 x_1^4
\]
and defining
\[
S := q_0 q_4 - \frac{q_1 q_3}{4} + \frac{q_2^2}{12}
\]
\[
T := \frac{q_0 q_2 q_4}{6} + \frac{q_1 q_2 q_3}{48} - \frac{q_2^3}{216} - \frac{q_0 q_4^2}{16} - \frac{q_1^2 q_4}{16},
\]
we get \( j(C) = \frac{S^3}{S^3 - 27T^2} \), the \( j \)-invariant of the \((2, 2)\) curve \( C \). Also, \( H \) is invariant under the action of \( GL(2) \), see, for example, in \([1, 11, 18]\).

### 2.3 Segre and veronese embeddings

We will define a non-standard Segre embedding as the composition of the standard Segre embedding and a projective automorphism of the ambient space of the codomain, which is represented by a square matrix.

**Definition 3** Let \( n, m \in \mathbb{N} \). The non-standard Segre embedding and the Segre variety represented by the matrix \( M \) in the general linear group \( GL((m + 1)(n + 1)) \) are, respectively, defined as
\[
\Sigma_{n,m}^M := M \circ \Sigma_{n,m}, \quad \Sigma_{n,m}^M := M \Sigma_{n,m}.
\]

The smooth quadric surfaces of \( \mathbb{P}^3 \) are projectively isomorphic; therefore, they are \( \Sigma_{n,m}^M \) for some \( m \) and \( n \).

**Example 3** Consider a non-standard Segre embedding
which is represented by the matrix

\[
M = \begin{bmatrix}
1 & 0 & 0 & -4 \\
0 & 0 & -7 & 1 \\
1 & 2 & -1 & 5 \\
0 & 8 & 1 & 0
\end{bmatrix}.
\]

We also define the standard and non-standard Veronese embedding.

**Definition 4** For \( n, m \in \mathbb{N} \), the standard Veronese embedding are the morphisms

\[
P^n \longrightarrow \mathbb{P}^{(n+m)-1}
\]

where the monomials \((x_0^i \cdots x_n^i)_{0 \leq i \leq m}\) with \( \sum_{j=0}^{n} i_j = m \) (of degree \( m \)) are ordered by the lexicographical order. The images of these embeddings are called standard Veronese varieties and they are denoted by \( V_{n,m} \).

Suppose \( z_{i_1, \ldots, i_n} \) be the variable in \( \mathbb{P}^{(m+3)}{3} - 1 \) corresponding to the monomial \( x_0^{i_0} \cdots x_n^{i_n} \) in the Veronese map. Suppose 

\[
C = c_0, \ldots, c_n, D = d_0, \ldots, d_n, E = e_0, \ldots, e_n, \text{ and } F = f_0, \ldots, f_n
\]

be the indices of the coordinates of \( \mathbb{P}^{(n+m)}{m} - 1 \) such that \( C + D = E + F \), i.e. \( c_0 + d_0 = e_0 + f_0, \ldots, c_n + d_n = e_n + f_n \), then in the images of the Veronese map, we have the following relation of coordinates:

\[
z_C \cdot z_D - z_E \cdot z_F = 0
\]

(2)

**Proposition 1** The standard Veronese variety is defined by the quadratic equations given in Equation (2).

**Proof** See in [19, Example 1.28].

**Example 4** For the Veronese embedding

\[
P^1 \longrightarrow \mathbb{P}^3
\]

we have, \( \nu_{1,3}(\mathbb{P}^1) = V_{1,3} \subset \mathbb{P}^3 \), the image is defined by the following quadratic equations
where \([z_0 : z_1 : z_2 : z_3]\) is the coordinate of \(\mathbb{P}^3\).

Similarly we define non-standard Veronese embedding as the composition of the standard Veronese embedding and a projective automorphism of the ambient space of the variety.

**Definition 5** Let \(n, m \in \mathbb{N}\). Let \(M \in \mathcal{GL}(\binom{n+m}{m})\). Then

\[
v^M_{n,m} := M \circ v_n, m, \quad V^M_{n,m} := M V_{n,m}
\]

are defined, respectively, as the Veronese embedding and the Veronese variety represented by the matrix \(M\).

We use the composition of the Segre embedding \(s^M_{1,1}\) and the Veronese embedding \(v^M_{3,m}\) in the application to cryptography. We define the composition \(v^M_{3,m} \circ s^M_{1,1}\) as a \(\sigma\)-embedding represented by a \(\binom{m+3}{3} \times (m+1)^2\) matrix.

**Example 5** Let \(\kappa = \mathbb{F}_3 = \{0, 1, 2\}\) and \(m = 2\) then \(\binom{m+3}{3} = 10\). Consider a non-standard Segre embedding

\[
\mathbb{P}^1 \times \mathbb{P}^1 \xrightarrow{s^M_{1,1}} \mathbb{P}^3
\]

\[
\begin{pmatrix} x_0 \\ x_1 \end{pmatrix}, \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} \xrightarrow{v^M_{3,2}} \begin{pmatrix} -x_0y_0 + x_0y_1 + x_1y_1 \\ x_1y_0 + x_0y_1 - x_1y_1 \\ x_0y_0 - x_1y_0 + x_1y_1 \\ -x_0y_0 + x_0y_1 + x_1y_1 \end{pmatrix}
\]

which is represented by the matrix

\[
M = \begin{bmatrix} 2 & 1 & 0 & 1 \\ 0 & 1 & 1 & 2 \\ 1 & 0 & 2 & 1 \\ 2 & 1 & 0 & 1 \end{bmatrix}.
\]

Suppose

\[
v^M_{3,2} := M \circ v_{3,2},
\]

where the map \(v_{3,2} \circ s^M_{1,1}\)
Now applying the automorphism of $\mathbb{P}^9$ given by

$$M' = \begin{bmatrix}
2 & 1 & 1 & 1 & 1 & 2 & 1 & 2 & 1 & 2 \\
2 & 1 & 0 & 0 & 1 & 2 & 1 & 2 & 1 & 1 \\
2 & 1 & 0 & 0 & 2 & 1 & 2 & 1 & 2 & 1 \\
2 & 1 & 2 & 1 & 1 & 1 & 0 & 2 & 2 & 1 \\
2 & 1 & 0 & 0 & 1 & 0 & 0 & 2 & 0 & 2 \\
1 & 0 & 2 & 0 & 2 & 1 & 0 & 1 & 0 & 0 \\
0 & 2 & 0 & 0 & 2 & 1 & 1 & 2 & 1 & 0 \\
2 & 0 & 2 & 1 & 1 & 0 & 2 & 0 & 2 & 1 \\
1 & 1 & 0 & 0 & 2 & 2 & 1 & 1 & 1 & 0 \\
1 & 1 & 0 & 2 & 1 & 1 & 1 & 1 & 1 & 1 \\
\end{bmatrix}$$

we get the $\sigma$-embedding $\iota_{3,m}^M \circ s_{1,1}^M$, which maps to

$$\begin{align*}
[x_0y_0^2 + x_0^2y_0y_1 + x_0x_1y_0y_1 + x_0^2y_1^2 - x_0x_1y_1^2 + x_1^2y_1^2 : -x_0x_1y_0^2 - x_0^2y_0y_1 - x_0x_1y_0y_1 + x_0^2y_1^2 - x_0x_1y_1^2 + x_1^2y_1^2 : -x_0x_1y_0^2 + x_0^2y_0y_1 + x_0x_1y_0y_1 + x_0^2y_1^2 - x_0x_1y_1^2 + x_1^2y_1^2 : x_0^2y_0^2 - x_0^2y_0y_1 - x_0x_1y_0y_1 + x_0^2y_1^2 - x_0x_1y_1^2 + x_1^2y_1^2 : x_0^2y_0^2 - x_0^2y_0y_1 - x_0x_1y_0y_1 + x_0^2y_1^2 - x_0x_1y_1^2 + x_1^2y_1^2] \\
\end{align*}$$
A post-quantum key exchange protocol from the intersection...

and its $10 \times 9$ matrix representation

$$M'' = \begin{bmatrix}
1 & 0 & 0 & 1 & 1 & 0 & 1 & 2 & 1 \\
0 & 2 & 0 & 2 & 2 & 1 & 1 & 0 & 2 \\
2 & 1 & 0 & 1 & 2 & 2 & 0 & 1 & 1 \\
1 & 0 & 0 & 1 & 1 & 0 & 1 & 2 & 1 \\
0 & 1 & 0 & 2 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 2 & 1 & 1 & 2 & 0 & 1 & 2 \\
0 & 2 & 0 & 2 & 2 & 1 & 1 & 0 & 2 \\
1 & 1 & 1 & 0 & 2 & 1 & 0 & 0 & 1 \\
2 & 1 & 0 & 1 & 2 & 2 & 0 & 1 & 1 \\
1 & 0 & 0 & 1 & 1 & 0 & 1 & 2 & 1
\end{bmatrix}.$$

is obtained with respect to the monomial basis

$$\{x_0^2y_0^2, x_0x_1y_0^2, x_1^2y_0^2, x_0^2y_0^1, x_0x_1y_0y_1, x_1^2y_0y_1, x_0^2y_1^2, x_0x_1y_1^2, x_1^2y_1^2\}.$$

2.4 Automorphism of veronese variety

It is easy to construct the automorphisms of the Veronese variety. This can be obtained by using the homomorphism of general linear groups. Suppose we have the standard Veronese embedding $v_{n,m} : \mathbb{P}^n \rightarrow \mathbb{P} \left( \begin{pmatrix} n+m \\ m \end{pmatrix} \right) - 1$.

Consider an action of $A = (a_{ij})_{0 \leq i, j \leq n} \subseteq GL(n + 1)$ on the coordinates of $\mathbb{P}^n$ as

$$x_i \mapsto L_i := \sum_{j=0}^{n} a_{ij}x_j, \quad 0 \leq i \leq n$$

This action on coordinates induces a natural action on the monomials of degree $\sum_{k=0}^{n} e_k = m$ as

$$x_0^{e_0} \cdots x_n^{e_n} \mapsto L_0^{e_0} \cdots L_n^{e_n}$$

and can be represented by a matrix in $GL \left( \begin{pmatrix} n+m \\ m \end{pmatrix} \right)$. More precisely, this matrix is obtained by the action of $A$ on the homogeneous polynomials of degree $m$, written with respect to the monomial basis of the Veronese map.

This gives a natural group homomorphism

$$\phi_{n,m} : GL(n + 1) \rightarrow GL \left( \begin{pmatrix} n+m \\ m \end{pmatrix} \right).$$

Example 6 Take $n = 1$ and $m = 2$. Then the Veronese map is
Consider \( A = \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \in \GL(2) \) acting on the coordinates \([x_0 : x_1] \in \mathbb{P}^1\) as

\[
\begin{align*}
x_0 &\mapsto ax_0 + bx_1 \\
x_1 &\mapsto cx_0 + dx_1.
\end{align*}
\]

This corresponds to an action on the monomials of degree 2 as

\[
\begin{align*}
x_0^2 &\mapsto a^2x_0^2 + 2abx_0x_1 + b^2x_1^2 \\
x_0x_1 &\mapsto acx_0^2 + (ad + bc)x_0x_1 + bdx_1^2 \\
x_1^2 &\mapsto c^2x_0^2 + 2cdx_0x_1 + d^2x_1^2.
\end{align*}
\]

This gives the following matrix with respect to the monomial basis \(\{x_0^2, x_0x_1, x_1^2\}\)

\[
\phi_{n,m}(A) = \left( \begin{array}{ccc} a^2 & 2ab & b^2 \\ ac & ad + bc & bd \\ c^2 & 2cd & d^2 \end{array} \right).
\]

The image of \(\phi_{n,m}\) is a subgroup of \(\GL\left(\binom{n + m}{m}\right)\), which contains the automorphisms of the ambient space \(\mathbb{P}^{n + m}\) that fix the Veronese variety \(V_{n,m}\).

The automorphisms of the Veronese variety \(V_{n,m}^M\) are given by the following proposition.

**Proposition 2** \(\text{Aut}(V_{n,m}^M) = M\text{Im}(\phi_{n,m})M^{-1}\) for any \(M \in \GL\left(\binom{m + 3}{3}\right)\).

**Proof** It follows from the equality

\[
\text{Aut}(MV) = M\text{Aut}(V)M^{-1}
\]

for any projective subvariety \(V\).

\[
\square
\]

### 3 Relevant works

Isogeny-based post-quantum key exchange schemes SIDH [9] and CSIDH [8] use supersingular elliptic curves, where both parties make a random walk in an isogeny graph, and they manage to reach to a common supersingular elliptic curve. The common key is the invariant associated with the common curve, i.e. the \(j\)-invariant of the curve. They are based on the problem of finding an isogeny between supersingular...
elliptic curves. However, there are polynomial time classical attacks [7, 16, 17] for SIDH.

In our case, the communicating parties embed quadric surfaces in a large ambient space by means of the Veronese embedding; then, the intersection of the quadric surfaces will be an elliptic curve whose \( j \)-invariant is the common key.

4 New key exchange

In this section, we present a new key exchange scheme, which we call quadratic surface intersection (QSI) key exchange.

4.1 QSI algorithm

Let \( \mathbb{P}^n_\kappa = \mathbb{P}^n \) be the projective space of dimension \( n \), where \( \kappa = \mathbb{F}_q \) is a finite field with \( q \) elements and \( m \in \mathbb{N}^+ \) be the degree of the Veronese embedding \( v_{3,m}^{M_A} \).

- Alice chooses a non-standard Veronese embedding
  \[
  v_{3,m}^{M_A} : \mathbb{P}^3 \to M_A \cdot V_{3,m} \subset \mathbb{P} \left( \begin{array}{c} m+3 \\ 3 \end{array} \right) - 1
  \]
  represented by a random matrix \( M_A \in \mathcal{GL} \left( \begin{array}{c} m+3 \\ 3 \end{array} \right) \).

- Alice constructs some automorphisms of the variety \( M_A \cdot V_{3,m} \). These automorphisms of the variety are chosen by the map \( \phi_{n,m} \) as described in Subsection 2.4. Precisely, she selects some automorphisms of \( \mathbb{P}^3 \), i.e. \( A_1', \ldots, A_r' \in \mathcal{GL}(4) \) of order \( q^4 - 1 \) (with the characteristic polynomials irreducible over \( \mathbb{F}_q \)), and then, she computes
  \[
  A_i : = M_A \phi_{n,m}(A_i')M_A^{-1}
  \]
  as some automorphisms of the variety. For example, we fix \( r = 2 \).

- Alice selects a secret quadric surface inside \( M_A \cdot V_{3,m} \), equivalently a \( \sigma \)-embedding
  \[
  \sigma_A^{(s)} : \mathbb{P}^1 \times \mathbb{P}^1 \to M_A \cdot V_{3,m} \subset \mathbb{P} \left( \begin{array}{c} m+3 \\ 3 \end{array} \right) - 1
  \]
  represented by a \( \left( \begin{array}{c} m+3 \\ 3 \end{array} \right) \times (m+1)^2 \) matrix \( M_A^{(s)} \) as described in Example 5, because a choice of a quadric surface in \( \mathbb{P}^3 \) and its embedding to the large
projective space \( \mathbb{P}\left(\frac{m+3}{3}\right) \) are done through the composition of Veronese and Segre embeddings.

- She constructs a hyperplane \( H_A \subset \mathbb{P}\left(\frac{m+3}{3}\right) \) containing the \( \text{Im}(\sigma^{(s)}_A) \), which can be obtained by choosing a vector in \( \text{coker}(M^{(s)}_A) \subset \mathbb{F}_q^{m+3} \).

- She constructs a public quadric surface inside \( M_A \cdot V_{3,m} \), equivalently a \( \sigma \)-embedding

\[
\sigma^{(p)}_A : \mathbb{P}^1 \times \mathbb{P}^1 \to M_A \cdot V_{3,m} \subset \mathbb{P}\left(\frac{m+3}{3}\right) - 1,
\]

which is represented by a \( \left(\frac{m+3}{3}\right) \times (m+1)^2 \) matrix \( M^{(p)}_A \).

**Alice’s public key:**

- Two automorphisms of the variety given by matrices \( A_1, A_2 \in \mathcal{G}\mathcal{L}\left(\left(\frac{m+3}{3}\right)\right) \).

- The \( \left(\frac{m+3}{3}\right) \times (m+1)^2 \) matrix \( M^{(p)}_A \).

- The hyperplane \( H_A \).

**Alice’s secret key:**

- The \( \sigma \)-embedding \( \sigma^{(s)}_A \) or equivalently its representing matrix \( M^{(s)}_A \) of size \( \left(\frac{m+3}{3}\right) \times (m+1)^2 \).

**Bob’s key generation**

- Bob chooses \( b_1, b_2, b_3, b_4 \in \{0, \ldots, q^4 - 1\} \) and then computes

\[
M'_B = A_1^{b_1} A_2^{b_2} A_1^{b_3} A_2^{b_4}.
\]

- Bob computes the matrix \( M_B := M'_B \cdot M^{(p)}_A \) as a matrix of a \( \sigma \)-embedding

\[
\sigma^{(s)}_B : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}\left(\frac{m+3}{3}\right) \]

which is, in fact, the private quadratic surface of Bob lying in the Veronese variety chosen by Alice.

- Bob computes a hyperplane \( H_B \subset \mathbb{P}\left(\frac{m+3}{3}\right) \) containing the \( \text{Im}(\sigma^{(s)}_B) \).
Bob keeps $\sigma_B^{(s)}$ or $M_B$ as a private key and publishes $H_B$.

**Key Exchange:**

- Bob computes the pullback $\sigma_B^{(s)*}H_A$. It is a curve of bi-degree $(m, m)$ in $\mathbb{P}^1 \times \mathbb{P}^1$.
- He uses a factorization algorithm to find a component of bi-degree $(2, 2)$ and computes its $j$-invariant $j_B \in \mathbb{F}_q$.
- The probability that the residue curve of bi-degree $(m - 2, m - 2)$ is reducible is negligible, so the $j_B$ is well determined except for $m = 4$, in which case there are two bi-degree $(2, 2)$ curve.
- Alice computes the pullback $\sigma_A^{(s)*}H_B$. She finds the component of bi-degree $(2, 2)$, then she computes its $j$-invariant $j_A \in \mathbb{F}_q$.

$j_A = j_B$ is the common key of Alice and Bob.

**Lemma 2** Two $j$-invariants are equal, i.e. $j_A = j_B$.

**Proof** Since $\mathbb{P}^3$ is isomorphic to the Veronese variety in $\mathbb{P}\left(\frac{m + 3}{3}\right)$, an embedding $\mathbb{P}^1 \times \mathbb{P}^1$ in $\mathbb{P}\left(\frac{m + 3}{3}\right)$ contained in the Veronese variety is equivalent to giving an embedding of $\mathbb{P}^1 \times \mathbb{P}^1$ into $\mathbb{P}^3$, whose image is a quadric surface.

Alice and Bob have two different embeddings $\sigma_A^{(s)}$ and $\sigma_B^{(s)}$ whose images are contained in the Veronese variety, viewing these images as quadric surfaces, denote them as $Q_A$ and $Q_B$, respectively. We need to find the intersection $Q_A \cap Q_B$ which is a genus 1 curve and is isomorphic with the curves of Alice and Bob. Thus, identifying the Veronese variety as $\mathbb{P}^3$, the embedding of Alice can be assumed as

$$\sigma_A^{(s)} : \mathbb{P}^1 \times \mathbb{P}^1 \to Q_A \subset \mathbb{P}^3$$

and similarly quadratic surface of Bob as

$$\sigma_B^{(s)} : \mathbb{P}^1 \times \mathbb{P}^1 \to Q_B \subset \mathbb{P}^3.$$

The pullback of $Q_B$ through the $\sigma$-embedding of Alice: $\sigma_A^{(s)*}Q_B$, which is isomorphic to $Q_A \cap Q_B$ as in the discussion of Subsection 2.2. Providing a hyperplane section of the Veronese variety is equivalent to giving a surface $S_A$ or $S_B$ of $\mathbb{P}^3$ of degree $m$ and having $Q_A$ or $Q_B$ as the component. The pullback gives the $(2, 2)$ bi-degree component and is isomorphic to $Q_A \cap Q_B$ at least in the general case.

4.2 Toy example

**Example 7 Key Generation:** A finite field $\mathbb{F}_q$ with $q = 16411$, $m = 2$. Then $\left(\frac{m + 3}{3}\right) = 10$. Alice chooses a Veronese embedding
represented by a random $10 \times 10$ matrix

$$M_A = \begin{bmatrix}
6434 & 8624 & 1442 & 8172 & 13226 & 12669 & 9492 & 11160 & 2354 & 14514 \\
5392 & 9365 & 1565 & 3457 & 14505 & 8874 & 9738 & 9536 & 4162 & 7052 \\
9995 & 3409 & 12388 & 2962 & 13538 & 3814 & 8079 & 14920 & 2982 & 3167 \\
3655 & 8237 & 1820 & 12771 & 15351 & 11681 & 6626 & 463 & 12211 & 10377 \\
9818 & 15886 & 11814 & 11548 & 8164 & 7285 & 3865 & 4837 & 15330 & 12963 \\
1377 & 7570 & 10743 & 8013 & 3980 & 6998 & 6942 & 13032 & 13042 & 13066 \\
13067 & 8075 & 8684 & 6162 & 11588 & 10876 & 8172 & 40 & 2874 & 5514 \\
1420 & 11397 & 14649 & 7628 & 9902 & 5803 & 4539 & 9387 & 13157 & 6504 \\
5479 & 12138 & 680 & 8772 & 5036 & 11603 & 4928 & 6922 & 7011 & 15716 \\
5020 & 14199 & 11398 & 13653 & 6829 & 2800 & 2834 & 10248 & 7818 & 1773
\end{bmatrix}.$$  

In order to choose automorphisms of the Veronese variety $M_A \cdot V_{3,m}$, she takes two random matrices $A'_1, A'_2 \in GL(4)$, where

$$A'_1 = \begin{bmatrix}
15790 & 6966 & 6845 & 4231 \\
8011 & 3668 & 8257 & 831 \\
605 & 3986 & 7888 & 1157 \\
4462 & 16388 & 7343 & 14432
\end{bmatrix} \quad \text{and} \quad A'_2 = \begin{bmatrix}
5758 & 201 & 14881 & 3246 \\
1376 & 211 & 9310 & 7851 \\
9861 & 13210 & 1243 & 15 \\
5776 & 13711 & 9047 & 5442
\end{bmatrix}.$$  

and computes

$$A_i = M_A \phi_{n,m}(A'_i)M^{-1}_A \quad \text{for} \ i = 1, 2.$$  

Therefore,
A post-quantum key exchange protocol from the intersection…

\[
A_1 = \begin{bmatrix}
15018 & 7379 & 11744 & 11490 & 10844 & 10009 & 12890 & 11191 & 1666 & 16235 \\
436 & 6517 & 11689 & 1035 & 3948 & 8946 & 795 & 15753 & 3926 & 15920 \\
15677 & 6798 & 4533 & 4266 & 490 & 14025 & 13668 & 860 & 5535 & 8840 \\
4283 & 6514 & 6363 & 9652 & 12681 & 11618 & 16094 & 12376 & 12056 & 7575 \\
2808 & 61 & 193 & 4741 & 9627 & 2813 & 12310 & 15657 & 4608 & 2378 \\
2978 & 16021 & 5513 & 1185 & 10587 & 13067 & 8342 & 4232 & 16273 & 7589 \\
11071 & 12641 & 1141 & 2329 & 8739 & 2990 & 13833 & 8438 & 11187 & 13591 \\
6272 & 9096 & 12928 & 788 & 2799 & 10686 & 9829 & 7755 & 14429 & 7948 \\
7864 & 1517 & 6114 & 9107 & 13263 & 4237 & 1312 & 4171 & 11821 & 3308 \\
15726 & 7489 & 1756 & 8055 & 8245 & 4124 & 8820 & 10566 & 13627 & 1083
\end{bmatrix}
\]

and

\[
A_2 = \begin{bmatrix}
13369 & 15770 & 9803 & 10390 & 15295 & 14706 & 12527 & 9354 & 7794 & 14856 \\
8447 & 9124 & 6458 & 12871 & 9932 & 6220 & 10477 & 9907 & 7816 & 6399 \\
12520 & 9907 & 5244 & 11892 & 8717 & 12287 & 6801 & 7262 & 1980 & 2350 \\
10666 & 2429 & 10820 & 3502 & 4264 & 1076 & 3684 & 4255 & 13409 & 12313 \\
9194 & 4290 & 4445 & 14167 & 4100 & 3093 & 4026 & 5614 & 5983 & 2029 \\
14093 & 2842 & 14268 & 7988 & 4402 & 10580 & 5060 & 12625 & 14393 & 10063 \\
420 & 664 & 11556 & 7209 & 13025 & 8693 & 4869 & 550 & 15038 & 5438 \\
14547 & 11245 & 7577 & 13783 & 8462 & 16111 & 3996 & 6680 & 8069 & 5781 \\
8898 & 8774 & 15705 & 3270 & 11632 & 6559 & 12836 & 13643 & 12300 & 8008 \\
8574 & 2669 & 14730 & 14024 & 11160 & 13511 & 7697 & 10874 & 9888 & 12951
\end{bmatrix}
\]
She keeps the secret embedding

$$\sigma_A^{(s)} : \mathbb{P}^1 \times \mathbb{P}^1 \to M_A \cdot V_{3,m} \subset \mathbb{P}^9$$

whose representing matrix is the following $10 \times 9$ matrix

$$M_A^{(s)} = \begin{bmatrix}
1320 & 2620 & 11135 & 2352 & 4340 & 5297 & 416 & 12442 & 1908 \\
1896 & 1525 & 6976 & 10295 & 15677 & 5531 & 8803 & 13595 & 11350 \\
3114 & 3038 & 4343 & 4194 & 3410 & 3268 & 13487 & 885 & 11904 \\
3276 & 2264 & 7342 & 15211 & 11771 & 8806 & 11059 & 11378 & 10608 \\
1196 & 15628 & 8778 & 15495 & 1815 & 7911 & 12916 & 4073 & 12975 \\
13875 & 3785 & 8803 & 1247 & 7024 & 6443 & 9817 & 502 & 9134 \\
10985 & 6007 & 1464 & 12419 & 1703 & 1835 & 15245 & 12758 & 14087 \\
8343 & 11091 & 10245 & 1960 & 13606 & 6551 & 14556 & 5822 & 8517 \\
3923 & 6315 & 11634 & 7502 & 6454 & 3700 & 13878 & 10216 & 4533 \\
1295 & 11283 & 2418 & 1477 & 15007 & 7063 & 15300 & 5917 & 2092
\end{bmatrix}.$$ 

Alice’s public keys consist of a hyperplane $H_A$ in $\mathbb{P}^9$:

$$x_0 + 1469x_1 - 8066x_2 + 2363x_3 + 2680x_4 - 1980x_5 + 5540x_6 + 2285x_7 - 5203x_8 + 7674x_9$$

containing the image of $\sigma_A^{(s)}$, the embedding

$$\sigma_A^{(p)} : \mathbb{P}^1 \times \mathbb{P}^1 \to M_A \cdot V_{3,m} \subset \mathbb{P}^9$$

represented by the $10 \times 9$ matrix
A post-quantum key exchange protocol from the intersection…

Bob chooses random integers $b_1 = 6739, b_2 = 6338, b_3 = 14612, b_4 = 6950$; and computes an automorphism

$$M^{(p)}_A = \begin{bmatrix}
8590 & 8461 & 6748 & 15978 & 3543 & 12505 & 3129 & 627 & 16239 \\
15293 & 13594 & 10715 & 12397 & 46 & 4798 & 12438 & 13145 & 14163 \\
7602 & 769 & 5417 & 3304 & 7795 & 14719 & 15833 & 6416 & 11489 \\
7632 & 13392 & 10345 & 322 & 10751 & 5896 & 16313 & 16225 & 14235 \\
7749 & 15238 & 12591 & 2855 & 5074 & 771 & 2812 & 8788 & 8135 \\
4852 & 11438 & 4357 & 5462 & 371 & 5418 & 13730 & 14255 & 12231 \\
14594 & 176 & 15387 & 2185 & 3097 & 6726 & 16198 & 1553 & 99 \\
9265 & 15959 & 1594 & 16353 & 16183 & 13447 & 3785 & 11208 & 1609 \\
1115 & 10396 & 2580 & 1153 & 531 & 10719 & 8208 & 11221 & 4900 \\
8475 & 15417 & 15063 & 16139 & 16064 & 5343 & 11934 & 5658 & 15627
\end{bmatrix}$$

and automorphisms $A_1, A_2$.

Bob chooses a random integers $b_1 = 6739, b_2 = 6338, b_3 = 14612, b_4 = 6950$; and computes an automorphism

$$M^{(p)}_B = A_1^{b_1} A_2^{b_2} A_1^{b_3} A_2^{b_4} = \begin{bmatrix}
8402 & 8088 & 3256 & 9623 & 16339 & 15102 & 7293 & 12071 & 15793 & 8979 \\
12150 & 13336 & 594 & 3969 & 7180 & 2239 & 11310 & 9534 & 5091 & 13870 \\
14874 & 5084 & 13249 & 12808 & 7354 & 2911 & 2559 & 165 & 5762 & 4748 \\
11762 & 12983 & 12932 & 6250 & 14281 & 9673 & 573 & 6454 & 5011 & 909 \\
13865 & 3904 & 4003 & 2096 & 5504 & 5870 & 13008 & 7737 & 5252 & 11114 \\
4497 & 14177 & 10640 & 5234 & 10054 & 11048 & 2128 & 7427 & 14868 & 13717 \\
7523 & 13487 & 7464 & 796 & 10253 & 2102 & 8736 & 10399 & 1582 & 5422 \\
13783 & 10771 & 1723 & 3461 & 68 & 14176 & 15622 & 2233 & 3743 & 15586 \\
8951 & 14717 & 6121 & 4899 & 9838 & 10902 & 2187 & 13328 & 3436 & 12577 \\
2073 & 1183 & 13888 & 4233 & 12205 & 6095 & 15837 & 9761 & 15699 & 5154
\end{bmatrix}$$
of the variety $M_A \cdot V_{3,m}$. He calculates

$$M_B = M'_B M''_A = \begin{bmatrix}
10316 & 70 & 5132 & 5007 & 2548 & 7354 & 732 & 15368 & 4469 \\
5158 & 10610 & 12687 & 4020 & 10647 & 12187 & 7885 & 10061 & 12566 \\
3263 & 3196 & 12137 & 3814 & 6090 & 10420 & 105 & 4761 & 15514 \\
6142 & 8180 & 13169 & 2750 & 15611 & 14046 & 14894 & 6055 \\
15633 & 4970 & 9093 & 14779 & 7475 & 15556 & 8779 & 451 & 14227 \\
14863 & 3370 & 2268 & 920 & 369 & 9234 & 10790 & 2659 & 8773 \\
9388 & 1235 & 8573 & 3814 & 6090 & 10420 & 105 & 4761 & 15514 \\
15445 & 12709 & 8615 & 5043 & 11409 & 2875 & 2516 & 11029 & 9782 \\
11591 & 10626 & 11760 & 10191 & 7664 & 14341 & 10404 & 8175 & 12554 \\
13748 & 3883 & 2870 & 8980 & 15814 & 12948 & 9672 & 8447 & 276
\end{bmatrix}$$

as a representing matrix of the secret $\sigma$-embedding

$$\sigma^{(s)}_B : \mathbb{P}^1 \times \mathbb{P}^1 \to M_A \cdot V_{3,m} \subset \mathbb{P}\left(\binom{m+3}{3}\right).$$

He also computes a hyperplane $H_B$ in $\mathbb{F}_q^9$ given by

$$x_0 - 5404x_1 + 3650x_2 + 465x_3 + 6073x_4 + 7863x_5 - 162x_6 - 7294x_7 - 7707x_8 + 8095x_9$$

containing the image of $\sigma^{(s)}_B$.

**Key Exchange:**

Bob computes the pullback

$$C_1 := \sigma^{(s)*}_B H_A = 4094x_0^2x_2^2 + 433x_0x_1x_2^2 + 262x_1^2x_2^2 + 1048x_0^2x_2x_3 + 5309x_0x_1x_2x_3 - 4413x_1^2x_2x_3 + 5200x_0^2x_3^2 - 4806x_0x_1x_3^2 - 1129x_1^2x_3^2,$$

which is a bi-degree (2,2) curve and computes its $j$-invariant $j_B = j(C_1) = 4026 \in \mathbb{F}_q$.

Alice computes the pullback

$$C_2 := \sigma^{(s)*}_A H_B = -7091x_0^2x_2^2 - 5735x_0x_1x_2^2 - 2687x_1^2x_2^2 + 1479x_0^2x_2x_3 + 6077x_0x_1x_2x_3 + 8150x_1^2x_2x_3 + 1351x_0^2x_3^2 + 7198x_0x_1x_3^2 + 4625x_1^2x_3^2$$

and computes its $j$-invariant $j_A = j(C_2) = 4026 \in \mathbb{F}_q$, which is the common key.
5 Public-key encryption

The QSI key exchange technique can be used to design a public-key crypto-system, similar to the ElGamal public-key encryption scheme.

Suppose Bob wants to send a message $m$ to Alice.

- **Public parameters to both parties**
  A finite field $\mathbb{F}_q$, $m \in \mathbb{N}^+$ and a family of hash functions $\mathcal{H} = \{H_k : k \in \mathcal{K}\}$ from the finite field $F_q$ to the message space $\{0, 1\}^w$, and $\mathcal{K}$ be a finite set.

- **Encryption**
  Bob has access to the Alice’s public data $(A_1, A_2, M_{A}^{(p)}, H_{A}, k)$. He computes a random ephemeral key, a $\sigma$ embedding $\sigma^{(s)}_B : \mathbb{P}^1 \times \mathbb{P}^1 \rightarrow M_{A} \cdot V_{3,m} \subset \mathbb{P}\left(\frac{m+3}{3}\right) - 1$. He first computes the $j$-invariant of the bi-degree $(2,2)$ curve $j_B$ as described before. Then he encrypts the message $m \in \{0, 1\}^w$ as

  $$c = H_k(j_B) \oplus m.$$  

The ciphertext is $(H_B, c)$.

- **Decryption**
  Alice gets the ciphertext $(H_B, c)$ and using her private embedding $\sigma^{(s)}_A : \mathbb{P}^1 \times \mathbb{P}^1 \rightarrow M_{A} \cdot V_{3,m} \subset \mathbb{P}\left(\frac{m+3}{3}\right) - 1$, she first recovers the $(2, 2)$ curve and its $j$-invariant $j_A$, and recovers the message $m$ as

  $$m = H_k(j_A) \oplus c.$$  

6 Cost and security analysis of QSI

6.1 Underlying cost of the key exchange

We first observe the space complexity of public and private keys.

**Keys of Alice:**

- Two public square matrices $A_1, A_2$ of size $\left(\frac{m+3}{3}\right)$ require $\mathcal{O}(m^6 \log q)$ space.
- Public matrix $M_A^{(p)}$ of size $\left(\frac{m+3}{3}\right) \times (m+1)^2$ requires $\mathcal{O}(m^5 \log q)$.  

\[\text{Springer}\]
• Public hyperplane $H_A$, a vector of length \( \binom{m+3}{3} \), requires $O(m^3 \log q)$.

• Private $\sigma$-embedding $\sigma_A^{(s)}$ or its matrix $M_A^{(s)}$ of size \( \binom{m+3}{3} \times (m+1)^2 \) requires $O(m^5 \log q)$.

Keys of Bob:

• Private $\sigma$-embedding $\sigma_B^{(s)} : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P} \binom{m+3}{3}$ or its matrix $M_B$ of size \( \binom{m+3}{3} \times (m+1)^2 \) requires $O(m^5 \log q)$.

• Public hyperplane $H_B$, a vector of length \( \binom{m+3}{3} \), occupies $O(m^3 \log q)$.

Now, we analyze asymptotic steps required to share a common key.

• Number of steps to produce $A_1, A_2, \sigma_A^{(s)}$ is bounded by $O(M(\log q)m) + O(m^n)$, where $M(x)$ denote the number of steps required to multiply two $x$-bits integers.

• To compute the hyperplanes $H_A$ and $H_B$, it requires to solve a system of linear equation which takes at most $O(m^{2\omega})$ steps [21], where $2 < \omega \leq 3$ is the matrix multiplication exponent.

• For private $\sigma$-embedding of Bob $\sigma_B^{(s)}$, it needs $O(m^{3\omega} \log m)$.

• To both Alice and Bob
  - Pull back of hyperplane by private $\sigma$-embeddings in $O(M(\log q)m^3)$.
  - Factorization of bi-degree $(m, m)$ can be computed efficiently by the method given in [3].

6.2 Brute force attempts

We give the approximate steps needed to attack the keys.

• The number of quadric hypersurfaces contained in $H_A$, i.e. amount of brute force needed to find $\sigma_A^{(s)}$.

  We count $M_A^{(s)}$ such that $H_A$ is in $\text{coker}M_A^{(s)}$, i.e. $H_A M_A^{(s)} = 0$. This implies that the columns of $M_A^{(s)}$ are in the kernel of $H_A$, which is isomorphic with
\[
\mathbb{F}_q\left(\frac{m+3}{3}\right) - 1; \text{ therefore, choosing } (m+1)^2 \text{ elements of } \mathbb{F}_q\left(\frac{m+3}{3}\right) - 1
\]
requires total of \(q\left(\frac{m+3}{3}\right)^{-1}(m+1)^2\) attempts.

- Possible number of \(\sigma_B^{(s)}\) (necessarily depending on \(r\)):
  For \(r = 2\), choices of \(b_i\) for \(i = 1, \ldots, 4\) determine \(\sigma_B^{(s)}\) therefore, there are \(q^{16}\) choices.
- Running over all possibilities for \(\sigma_B^{(s)}\), the number of distinct options for \(\sigma_B^{(s)} H_A\) is \(q^{16}\).
- Similarly, the number of distinct options for \(\sigma_B^{(s)} H_A\) is \(q\left(\frac{m+3}{3}\right)^{-1}(m+1)^2\).
- Valid \(j\)-invariants (i.e. amount of brute force needed to find \(j_A = j_B\)):
  Since \(j\)-invariants are defined in \(\mathbb{F}_q\) so there are \(q\) choices.

Since the \(j\)-invariants belong to the base field \(\mathbb{F}_q\), we have to choose \(q \approx 2^{128}\) for the classical 128-bit security level. This attack suggests that small values of \(m\) could work but we will see that the brute force is not the best attack.

### 6.3 Other possible attack strategies

Here we summarize other possible attack strategies against QSI. One of the possibilities is a direct key recovery attack targeting the private keys, more precisely, to the secret \(\sigma\)-embeddings or the Veronese variety hidden by the automorphism of the ambient space. We state the following underlying problem of the proposed key exchange scheme.

**Problem 1** Let \(\kappa = \mathbb{F}_q\) be the field of cardinality \(q\). Suppose

\[
\nu_{3,m}^M : \mathbb{P}^3 \to M \cdot V_{3,m} \subset \mathbb{P}\left(\frac{m+3}{3}\right)_{-1}
\]
be a non-standard Veronese embedding represented by a random matrix \(M \in GL\left(\frac{m+3}{3}\right)\) with its variety \(M \cdot V_{3,m}\) and let
be $\sigma$-embeddings represented by $\binom{m+3}{3} \times (m+1)^2$ matrices $M^{(p)}$ and $M^{(s)}$, respectively. A hyperplane $H$ containing $\text{Im}(\sigma^{(s)})$ is represented by a vector in \( \text{coker}(M^{(s)}) \subset \mathbb{F} \left( \binom{m+3}{3} \right) \). Furthermore, let $A_1$ and $A_2$ in $GL\left( \binom{m+3}{3} \right)$ be two matrices representing automorphisms of the variety $M \cdot V_{3,m}$. Given:

- the finite field $\mathbb{F}_q$,
- the degree of the Veronese embedding $m \in \mathbb{N}^+$,
- two automorphisms of the variety given by matrices $A_1, A_2$,
- the matrix $M^{(p)}$ and
- a hyperplane $H$ containing the image of $\sigma^{(s)}$,

determine $\sigma^{(s)}$ (equivalently its corresponding matrix) or the matrix $M$ representing the non-standard Veronese variety $M \cdot V_{3,m}$.

Problem 1 of determining the Veronese variety, say $V = M \cdot V_{3,m}$ and the $\sigma$-embedding $\sigma^{(s)}$ reduce to a problem of solving multivariate and high-degree polynomial equations. Since $A_i$ are automorphisms of $V$, we have

$$A_i M = M \phi_{3,m}(A)$$

(4)

for some matrix $A \in GL(4)$. Consider $A = (a_{ij})$ be $4 \times 4$ and $M = (m_{ij})$ be $\binom{m+3}{3} \times \binom{m+3}{3}$ matrices of unknowns. Substituting these matrices in Eq. 4, we get a system of multivariate polynomial equations of bi-degree $(1, m)$ in variables $m_{ij}$ and $a_{ij}$, and elimination of the variables $a_{ij}$ changes the system into a system with very high-degree equations and large number of variables as $m$ gets bigger.

Likewise, an attempt to find $\sigma^{(s)}$ such that $\text{Im}(\sigma^{(s)}) \subset V$ also reduces to the similar multivariate problem. The condition $\text{Im}(\sigma^{(s)}) \subset V$ implies that

$$\sigma^{(s)} = M_{\circ} V_{3,m} \circ A_{\circ} S_{1,1}$$

for some $A \in \text{Aut}(\mathbb{P}^3)$ since $\sigma^{(s)}$ is a composition of non-standard Segre and Veronese. As before, the matrix $M_{\sigma^s}$, representing the embedding $M_{\circ} V_{3,m} \circ A_{\circ} S_{1,1}$, is a matrix whose components are bi-homogeneous polynomials of bi-degree $(1, m)$ in the set of variables $\{m_{ij}\}$ and $\{a_{ij}\}$, where $a_{ij}$ and $m_{ij}$ are as above. Now, imposing the
A post-quantum key exchange protocol from the intersection…

Shared Secret Recovery: Another underlying problem of the QSI key exchange is a problem of recovering the common secret, which is the bi-degree \((2, 2)\) homogeneous curve embedded as a curve of degree \(4m\) in the Veronese variety.

**Problem 2** Let \(\kappa = \mathbb{F}_q\) be the finite field with \(q\) elements. Suppose that \(V \subset \mathbb{P}\left(\binom{m+3}{3} - 1\right)\) is a three-dimensional non-standard Veronese variety. Assume the homogeneous ideal of \(V\) is known but its isomorphism with \(\mathbb{P}^3\) is not known. Let \(H_1\) and \(H_2\) be two hyperplanes of \(\mathbb{P}\left(\binom{m+3}{3} - 1\right)\). Find the irreducible decomposition of the curve \(V \cap H_1 \cap H_2\) as a curve of degree \(4m\) and a curve of degree \(m^3 - 4m\).

The equivalent problem in terms of defining ideals can be stated as the problem of primary decomposition of the ideal \(I = (I_V, L_{H_1}, L_{H_2})\) where \(I_V\) is the homogeneous ideal of \(V\); \(L_{H_1}\) and \(L_{H_2}\) are the linear equations defining the hyperplanes \(H_1\) and \(H_2\). Here, the Gröbner basis of the ideal \(I\) gives the information of the shared secret.

The Veronese variety \(V\) is defined by \(m(m^2 - 1)(m^3 + 12 m^2 + 59 m + 66)\) homogeneous polynomials of degree 2.

**Proposition 3** The Veronese variety \(V_{3,m}\) is an intersection of \(N(V_{3,m}) = m(m^2 - 1)(m^3 + 12 m^2 + 59 m + 66)\) linearly independent quadric hypersurfaces in \(\binom{m+3}{3}\) variables.

**Proof** See in Appendix C.

These defining polynomials can be obtained by some linear algebra. Therefore, the main difficulty lies in the computation of irreducible components of the variety \(V \cap H_1 \cap H_2\), or equivalently to find the primary decomposition of the ideal generated by the quadratic polynomials defining \(V\) and the two linear polynomials defining \(H_1\) and \(H_2\).

The Veronese variety \(V\) is of degree \(m^3\).

**Proposition 4** The Veronese variety \(V_{3,m} \subset \mathbb{P}\left(\binom{n+m}{3} - 1\right)\) is a three-dimensional projective variety of degree \(m^3\).

**Proof** In general, \(\deg(V_{n,m}) = m^n\), see, for example, in [19, 4.2.7]
It follows that the curve $V_{3,m} \cap H_1 \cap H_2$ is a curve of degree $m^3$ and it is reducible with a component of degree $4m$ because of the following proposition.

**Proposition 5** The image of a curve of bi-degree $(2, 2)$ through a $\sigma$-embedding $\mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^{(m+3)/3-1}$ is a curve of degree $4m$.

**Proof** See in Appendix C. \qed

Once the irreducible component of $V_{3,m} \cap H_1 \cap H_2$ of degree $4m$ is known, then one can evaluate the $j$-invariant of the component of degree $4m$, which is the common secret to both Alice and Bob.

**Attack to the Private Keys:** Suppose Eve wants to attack Bob’s private key. She chooses $e_1, e_2, e_3, e_4 \in \{0, \ldots, q^4 - 1\}$ and then computes

$$M'_E = A_{1}^{e_1}A_{2}^{e_2}A_{1}^{e_3}A_{2}^{e_4}.$$  

She further computes the matrix $M_E := M'_E \cdot M_A^{(p)}$ as a matrix of a $\sigma$-embedding $\sigma_E : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^{(m+3)/3}$ and imposes the condition

$$H_B \in \text{coker}(M_E).$$

This may require $q^{16}$ attempts. But, the possible quadric surfaces of $\mathbb{P}^3$ form a nine-dimensional projective space; therefore, the brute force attack requires only $q^{9}$ attempts. This shows $q^9$ trials can generate a $\sigma$-embedding say $\sigma_E$ such that its image coincide with the image of the private $\sigma$-embedding of Bob, i.e. $\text{Im}(\sigma_E) = \text{Im}(\sigma_B^{(s)})$. 

---

**Table 1** Gröbner basis computation

| $m$ | Time 1(sec) | Time 2(sec) | Time 3(sec) | Time(sec) |
|-----|-------------|-------------|-------------|-----------|
| 3   | 0.440       | 0.450       | 0.449       | 3         |
| 4   | 20.519      | 19.629      | 20.359      | 4         |
| 5   | 613.620     | 608.470     | 623.980     | 5         |
|     | Aborted (after 6 hrs) |          |             |           |

**Table 2** Key size comparison

| Schemes          | sk    | pk    |
|------------------|-------|-------|
| Classic McEliece | 6492  | 261120|
| Kyber            | 1632  | 800   |
| QSI key Exchange | 2448000 | 10880 |

$q = \text{NextPrime}(2^{128})$
6.4 Gröbner basis computation

In general, Gröbner basis computation may take exponential time but it depends heavily on the nature of the problem. Faugère’s $F_4$ and $F_5$ [10] are currently the best algorithm to compute Gröbner basis. In our context, we estimate according to our experimental evidences.

We have posted a code to compute the Gröbner basis of the ideal $I = (I_{V_1}, L_{H_1}, L_{H_2})$ described in Paragraph 6.3 at https://github.com/mgyawali/QSI-Key-Exchange, which is written for Magma [6].

Our experiment was done on the computer of the University of L’Aquila [22].

Finite field is $\mathbb{F}_q$ and $m$ is the degree of the Veronese embedding.

Algorithm used: Faugère F4

Monomial basis order: Graded Reverse Lexicographical

Magma V2.24-2

Time required for some values of $m$ is given in Table 1.

Large values of $m$ makes the key exchange excessively slow. We believe that some variants or some technique to accelerate the system could be possible in future. Therefore, we leave the complete security analysis and development of some possible variants for the future research.

6.5 Comparison with some post-quantum schemes

A rigorous security analysis is required to understand the size of parameters; however, we propose a parameter set according to an experimental analysis. For AES-128 bit security level, we set $m = 14, q \approx 2^{128}$. The size of public and private keys (in bytes) are presented in Table 2. In this table we have computed the key size of Bob.

Currently, key sizes are larger than the other established schemes. However, we believe that use of sparse matrices could decrease key sizes or there might be an efficient method to represent the matrices.

7 Security proof

We have adopted the computational Diffie–Hellman and decisional Diffie–Hellman problem in the case of QSI key exchange.

**Problem 3** (Quadratic Surface Computational Diffie–Hellman (QSCDH) Problem)

Consider a non-standard Veronese embedding

$$v_{3,m}^{M_A} : \mathbb{P}^3 \rightarrow M_A \cdot V_{3,m} \subset \mathbb{P} \left( \begin{array}{c} m + 3 \\ 3 \end{array} \right) - 1$$

which is represented by a matrix $M_A$. Furthermore, suppose the $\sigma$-embeddings
\[ \sigma_A^{(s)} : \mathbb{P} \times \mathbb{P} \to M_A \cdot V_{3,m} \subset \mathbb{P} \left( \begin{array}{c} m + 3 \\ 3 \end{array} \right)^{-1}, \sigma_A^{(p)} : \mathbb{P} \times \mathbb{P} \to M_A \cdot V_{3,m} \text{ and } \sigma_B^{(s)} : \mathbb{P} \times \mathbb{P} \to \mathbb{P} \left( \begin{array}{c} m + 3 \\ 3 \end{array} \right) \]

are represented, respectively, by matrix \( M_A^{(s)} \), \( M_A^{(p)} \) and \( M_B \), where \( M_B := M'_B \cdot M_A^{(p)} \), \( M'_B = A_1^{b_1} A_2^{b_2} A_1^{b_3} A_2^{b_4} \) and \( b_1, b_2, b_3, b_4 \in \{0, \ldots, q^4 - 1\} \). Let \( H_A \) and \( H_B \) are hyperplanes containing the \( \text{Im}(\sigma_A^{(s)}) \) and \( \text{Im}(\sigma_B^{(s)}) \), respectively.

Given,

- Two Automorphisms \( A_1, A_2 \) of the variety \( M_A \cdot V_{3,m} \).
- \( H_A, H_B, M_A^{(p)} \)

Find an irreducible curve of degree 4 in \( M_A \cdot V_{3,m} \cap H_1 \cap H_2 \) and its \( j \)-invariant.

**Problem 4** (Quadratic Surface Decision Diffie–Hellman (QSDDH) Problem) Let \( C_1 \) be a curve of degree 4 in \( M_A \cdot V_{3,m} \cap H_1 \cap H_2 \) as in QSCDH problem and \( C_2 \) be a curve of degree 4 in \( M_A \cdot V_{3,m} \cap H'_1 \cap H'_2 \), where \( H'_1 \) and \( H'_2 \) are hyperplanes containing the images \( \text{Im}(\sigma_A^{(s)}) \) and \( \text{Im}(\sigma_B^{(s)}) \) respectively, for a random choice of \( M_A \) as in QSCDH problem, decide whether \( j(C_1) = j(C_2) \).

We believe that these problems are computationally infeasible. The following theorem can be proved under the QSDDH problem following the Canetti and Krawczyk (CK) security model.

**Theorem 6** QSI key scheme is secure in the Canetti and Krawczyk (CK) [5] security model under the QSDDH assumption.

---

**Appendix A: Probability that a random curve of bi-degree (2,2) in \( \mathbb{P} \times \mathbb{P} \) is singular**

Let \( \kappa \) be an algebraically closed field, then a general curve \( C \subset \mathbb{P} \times \mathbb{P} \) of bi-degree (2, 2) is non-singular. More precisely:

**Proposition 7** Let

\[ \mathcal{S} := \{ a_{ij} x_0^{2-i} x_1^i y_0^{2-j} y_1^j = 0 : i, j \in \{0, 1, 2\}, a_{ij} \in \kappa \} \]

be the set of curves of bi-degree (2,2) defined over \( \kappa \). Identify \( C \in \mathcal{S} \) with its coefficients (up to scalar multiplication) \( [a_{ij}] \in \mathbb{P}^8 \). Then the condition of being singular is closed in the Zariski topology of \( \mathbb{P}^8 \), i.e. is defined by a set of homogeneous polynomial equations in \( [a_{ij}] \).
The above proposition states that singular curves are very few compared to the smooth ones. You may imagine sets defined by polynomial equations in $\mathbb{R}^n$ or $\mathbb{C}^n$: these sets have a smaller dimension than the one of the ambient space, so their measure is 0. A similar situation occurs for algebraically closed fields. If we consider curves defined over a finite field $\mathbb{F}_q$, then the probability of being singular is not 0, but it should decrease when $q$ increases and it should be negligible when $q$ is very large.

**Appendix B: Irreducibility of curves of bi-degree $(d, d)$**

The pullback of a hyperplane $H$ through a $\sigma$-embedding is a curve of bi-degree $(m, m)$ in $\mathbb{P}^1 \times \mathbb{P}^1$, which has a component of bi-degree $(2, 2)$. An important task is to have a well defined key exchange is to know if the residual $(m - 2, m - 2)$ curve is irreducible or not. We can assume that this residual curve is randomly chosen among the curves of bi-degree $(m - 2, m - 2)$, so a general question is: what is the probability that a curve of bi-degree $(d, d)$ in $\mathbb{P}^1 \times \mathbb{P}^1$ is irreducible?

**Appendix C: Irreducible components of $V \cap H_A \cap H_B$**

The next proposition gives the implicit description of any Veronese variety as intersection of quadric hypersurfaces of the ambient space. Without loss of generality, we can suppose that it is the standard Veronese variety. In this section, some technical terms from algebraic geometry are used.

**Proposition 8** The Veronese variety $V_{3,m}$ is an intersection of

$$h_m := m(m^2 - 1)(m^3 + 12m^2 + 59m + 66)$$

linearly independent quadric hypersurfaces.

**Proof** First of all we need to compute $h^0(I_{V_{3,m}}(2))$. Since $V_{3,m}$ is projectively normal, then

$$h^0(I_{V_{3,m}}(2)) = h^0(\mathcal{O}_{\mathbb{P}^{N_{3,m}}}(2)) - h^0(\mathcal{O}_{V_{3,m}}(2))$$

$$= h^0(\mathcal{O}_{\mathbb{P}^{N_{3,m}}}(2)) - h^0(\mathcal{O}_{\mathbb{P}^3}(2m))$$

$$= \frac{1}{2} \left[ \binom{m + 3}{3} + 1 \right] \binom{m + 3}{3} - \binom{2m + 3}{3}$$

which is equal to the desired value. \hfill \Box

**Example 8** For $m = 8$ there are 12726 linearly independent quadric hypersurfaces containing $V_{3,m}$. It is the condition in the linear system of quadric surfaces of $\mathbb{P}^{N_{3,m}}$ of codimension 969.
A possible approach to find the quadratic equations defining \( V \) is to generate \( d_m - h_m \) points of \( V \), where \( d_m \) is the dimension of the space of all quadric hypersurfaces, sufficiently random points inside \( V \); this can be done easily using the knowledge of the \( \sigma \)-embedding and of some of its automorphisms. After that one can find a basis of the family of quadratic polynomials vanishing on those points. These quadratic polynomials generate the ideal \( I_V \).

**Proposition 9** \( V_{3,m} \subset \mathbb{P}^{N_{3,m}} \) is a three-dimensional projective variety of degree \( m^3 \).

**Proof** In general, \( \deg(V_{n,m}) = m^n \), see, for example, [19, 4.2.7] \( \square \)

After the computation of the primary components of \( V_{3,m} \cap H_A \cap H_B \), Eve has to find the \( j \)-invariant of the component of degree \( 4m \). This is explained by the next proposition.

**Proposition 10** The image of a curve of bi-degree \( (2, 2) \) through a \( \sigma \)-embedding \( \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^{(m+3)^2 - 1} \) is a curve of degree \( 4m \).

**Proof** In fact it is projectively equivalent to the image of a curve of bi-degree \( (2,2) \) under the map

\[
\mathcal{O}_{\mathbb{P}^1 \times \mathbb{P}^1}(m, m) : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^{(m+1)^2 - 1}. 
\]

The degree of the image is \((2, 2) \cdot (m, m) = 4m\) \( \square \)

In conclusion, \( V_{3,m} \cap H_A \cap H_B \) is reducible curve of degree \( m^3 \) with a component of degree \( 4m \). In order to break the system with this information, the eavesdropper needs to find

1. the irreducible decomposition of \( V_{3,m}^{M_A} \cap H_A \cap H_B \);
2. the irreducible component of degree \( 4m \) and compute its \( j \)-invariant.

**Acknowledgements** We are thankful to Luca De Feo, Pierre-Jean Spaenlehauwe, Chloe Martindale and Ankan Pal for useful suggestions in the earlier versions of the paper.

**Author contributions** Both authors have reviewed the manuscript.

**Funding** The first author was supported by the PhD fellowship of Department of Mathematics, Università degli Studi di Roma Tre, and the second author was supported by INdAM Fellowship Programs in Mathematics and/or Applications cofunded by Marie Skłodowska-Curie Actions (2015 INdAM-DP-COFUND fellowships).

**Availability of data and materials** Data not used.

**Declarations**

**Conflict of interest** Not applicable
A post-quantum key exchange protocol from the intersection…

Ethical approval  Not applicable

References

1. Abdesselam A (2006) A computational solution to a question by Beauville on the invariants of the binary quintic. J Algebra 303:771–788
2. Berlekamp ER, McEliece RJ, van Tilborg HCA (1978) On the inherent intractability of certain coding problems. IEEE Trans Inf Theory 24(3):384–386
3. Bernardin L, Monagan MB (1997) Efficient multivariate factorization over finite fields. In: Mora T, Mattson H (eds) Applied algebra, algebraic algorithms and error-correcting codes. AAECC 1997. Lecture notes in computer science 1225. Springer 15–28
4. Bernstein DJ, Buchmann J, Dahmen E (2009) Post-Quantum Cryptography. Springer-Verlag, Berlin Heidelberg
5. Canetti R, Krawczyk H (2001) Analysis of Key-Exchange Protocols and their Use for Building Secure Channels. In: Pfitzmann B (ed) EUROCRYPT 2001, vol 2045. LNCS. Springer, Heidelberg, pp 453–474
6. Cannon J, Bosma W, Fieker C, Steel A (eds) (2013) Handbook of Magma Functions, Version 2.19. https://www.math.uzh.ch/sepp/magma-2.19.8-cr/Handbook.pdf
7. Castryck W, Decru T (2022) An efficient key recovery attack on SIDH (preliminary version). Cryptology ePrint Archive, Paper 2022/975 https://eprint.iacr.org/2022/975
8. 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
9. De Feo L, Jao D, Plût J (2014) Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. J Math Cryptol 8:209–247
10. Ding J, Petzoldt A, Schmidt DS (2020) Multivariate Public Key Cryptosystems. Advances in Information Security 80 http://www.springer.com/series/5576
11. Dolgachev I (2003) Lectures on invariant theory. CUP
12. Gyongyosi L, Imre S (2022) Advances in the quantum internet. Commun ACM 65(8):52–63
13. Gyongyosi L, Imre S (2019) A Survey on quantum computing technology. Comput Sci Rev 31:51–71
14. Gyongyosi L, Imre S (2021) Scalable distributed gate-model quantum computers. Sci Rep 11:5172
15. Hartshorne R (1997) Algebraic geometry. Springer https://link.springer.com/book/10.1007/978-1-4757-3849-0
16. Maino L, Martindale C (2022) An attack on SIDH with arbitrary starting curve. Cryptology ePrint Archive, Paper 2022/1026 https://eprint.iacr.org/2022/1026
17. Robert D (2022) Breaking SIDH in polynomial time. Cryptology ePrint Archive, Paper 2022/1038 https://eprint.iacr.org/2022/1038
18. Salmon G (1964) Higher Algebra, fifth ed., 1885, reprinted by Chelsea, New York. https://archive.org/details/lessonintrosalmoog/page/n210/mode/2up
19. Shafarevich IR (2013) Basic algebraic geometry 1, 3rd edn. Springer, New York
20. Shor PW (1994) Algorithms for quantum computation: Discrete logarithms and factoring. In: Robshaw M, Katz J (eds) Foundations of ComputerScience, CONFERENCE 1994, Proceedings., 35th Annual Symposium, pp 124–134
21. Peng R, Vempala S (2021) Solving sparse linear systems faster than matrix multiplication. In: Proceedings of the 2021 ACM-SIAM symposium on discrete algorithms (SODA) 504-521 https://epubs.siam.org/doi/pdf/10.1137/1.9781611976465.31
22. Pera D (2018) Design and Performance Evaluation of a Linux HPC Cluster. Task Quarterly 22:113–123
23. The National Institute of Standards and Technology (NIST).PQC standardization process: second round candidate announcement. (2019)
24. The National Institute of Standards and Technology (NIST). Submission requirements and evaluation criteria for the post-quantum cryptography standardization process (2016)
25. Vakil R The rising sea - Foundations of Algebraic Geometry. http://math.stanford.edu/~vakil/216blog/FOAGnov1817public.pdf

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.