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

Daniele Di Tullio Manoj Gyawali*

May 27, 2020

Università degli Studi di Roma Tre, Department of Mathematics. Largo S. Leonardo Murialdo 1, Rome, Italy.
danieleditullio@hotmail.it
manoj.gyawali@ncit.edu.np

Abstract

In this paper we present a 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, which is uniquely determined by the j-invariant. An eavesdropper, to find this j-invariant, has to solve problems which are conjecturally quantum resistant.

Keywords: Quadric surfaces Veronese embedding Segre embedding Post-quantum cryptography.

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 [9] in 1994. The algorithm

*This author is supported by INdAM Fellowship Programs in Mathematics and/or Applications cofunded by Marie Skodowska-Curie Actions.

by Shor created a threat to the cryptographic world and then the necessity of the post-quantum system was realized. In 2016, the United States 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 [11] and in 2019 declared the 17 candidates for public-key encryption and key-establishment algorithms and 9 candidates for digital signatures [10] based on various mathematical problems. Currently, there are five major post-quantum areas of research are carried out, four of them are discussed in [3] including lattice-based cryptography based on lattice problems, code-based cryptography based on decoding a generic linear code, which is an 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 an NP-hard problem, hash-based cryptography based on one way hash functions and isogeny based cryptography based on isogeny problems, see for ex. [5, 4].
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 information 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.

In section 2 and section 3 we recall some terminologies that are used everywhere in this paper. In section 4 we give a key exchange protocol called Quadratic Surface Intersection (QSI) key exchange and a variant of

it. In section 5 we present the QSI key exchange protocol in a scenario of a trusted third party. In section 6 we discuss some underlying mathematical problems and hardness assumptions. We also give appendices to fulfill some extra arguments.

2 Intersection of quadric surfaces

The intersection of two quadric surfaces in $\mathbb{P}^3$ is a curve of degree 4. The geometric properties of this curve are well known. In this section, we have taken most of the terminologies from [12, 7, 8] unless otherwise stated.

Proposition 2.1. *Let κ be an algebraically closed field. Then, for a general choice of two quadric surfaces $Q_1, Q_2 \subset \mathbb{P}^3_\kappa$, $Q_1 \cap Q_2$ is a smooth curve of genus 1.*

The proposition 2.1 suggests that the intersection of two quadric surfaces is expected to be isomorphic to an elliptic curve, whose isomorphism class is determined by the j-invariant. We describe a way to compute the j-invariant of an intersection of two quadric surfaces.

Definition 2.2. *The standard Segre embeddings are a family of morphisms of projective variety*

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

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 $\mathbb{P}^{N_{n,m}}$.

Example 2.3. *$\Sigma_{1,1} \subset \mathbb{P}^3$ is the smooth quadric surface defined by the equation*

$$X_0X_3 = X_1X_2$$

Example 2.3 gives an easy characterization of the intersection of two smooth quadric surfaces Q_1, Q_2. We recall a basic result in Algebraic Geometry.

Lemma 2.4. *All the smooth quadric hypersurfaces of $\mathbb{P}^n$ are projectively isomorphic.*

Suppose we have two smooth quadric surfaces Q_1 and Q_2. From lemma 2.4 and example 2.3 we can choose a projectivity $f : \mathbb{P}^3 \to \mathbb{P}^3$ such that $f(Q_1) = \Sigma_{1,1}$. Assume that $Q_1 = \Sigma_{1,1}$, then $s_{1,1}^{-1}(Q_2) \cong Q_1 \cap Q_2$. Let $F_2(Z_0, Z_1, Z_2, Z_3)$ 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)

$$G(X_0, X_1; Y_0, Y_1) := F_2(X_0Y_0, X_0Y_1, X_1Y_0, X_1Y_1)$$

which is called the "pullback" of the polynomial F_2 through $s_{1,1}$. Hence, in particular every intersection of two smooth quadric surfaces is isomorphic to the zero locus of a polynomial of bi-degree (2,2) in $\mathbb{P}^1 \times \mathbb{P}^1$. The next proposition explains how to compute the j-invariant of a curve defined in that way.

Proposition 2.5. *Let $C \subset \mathbb{P}^1 \times \mathbb{P}^1$ be a smooth curve defined by a bi-homogeneous polynomial of bi-degree (2,2) over a field of characteristic different from 0 and 3.*

$$F(X_0, X_1; Y_0, Y_1) = Y_0^2 F_0(X_0, X_1) + Y_0 Y_1 F_1(X_0, X_1) + Y_1^2 F_2(X_0, X_1).$$

Define $G(X_0, X_1) := F_1^2 - 4F_0F_2$ and write

$$G(X_0, X_1) = q_0 X_0^4 + q_1 X_0^3 X_1 + q_2 X_0^2 X_1^1 + q_3 X_0 X_1^3 + q_4 X_1^4$$

Define

$$\begin{aligned} S &:= q_0q_4 - \frac{q_1q_3}{4} + \frac{q^2}{12} \\ T &:= \frac{q_0q2q_4}{6} + \frac{q_1q_2q_3}{48} - \frac{q_2^3}{216} - \frac{q_0q_3^2}{16} - \frac{q_1^2q_4}{16} \end{aligned}$$

Then $j(C) = \dfrac{S^3}{S^3 - 27T^2}$.

Proof. See appendix B. □

3 Segre and Veronese embeddings

We recall here the general notion of Segre and Veronese embeddings. We already defined the standard Segre embeddings in section 2. A general Segre embedding is a 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 3.1. *Let $n, m \in \mathbb{N}$, $N_{n,m} := (m+1)(n+1)-1$ and $M \in \mathrm{GL}(N_{n,m}+1)$. Then we define*

$$s_{n,m}^M := M \circ s_{n,m}, \quad \Sigma_{n,m}^M := M\Sigma_{n,m}$$

to be respectively the Segre embedding and the Segre Variety represented by the matrix M.

Remark 3.2. *Since all the smooth quadric surfaces of $\mathbb{P}^3$ are projectively isomorphic, then each of them is equal to some $\Sigma_{n,m}^M$.*

Example 3.3. *Let*

$$M := \begin{bmatrix} 1 & -2 & 3 & 0 \\ 0 & -1 & 1 & -5 \\ 8 & 3 & 1 & -1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

be a matrix, then it represents the non-standard Segre embedding

$$\begin{array}{ccc} \mathbb{P}^1 \times \mathbb{P}^1 & \xrightarrow{\quad S_{1,1}^M \quad} & \mathbb{P}^3 \\ \left(\begin{bmatrix} X_0 \\ X_1 \end{bmatrix}, \begin{bmatrix} Y_0 \\ Y_1 \end{bmatrix} \right) & \longmapsto & \begin{bmatrix} X_0Y_0 - 2X_0Y_1 + 3X_1Y_0 \\ -X_0Y_1 + X_1Y_0 - 5X_1Y_1 \\ 8X_0Y_0 + 3X_0Y_1 + X_1Y_0 - X_1Y_1 \\ X_0Y_0 + X_1Y_1 \end{bmatrix} \end{array}$$

We now define Veronese embeddings, which are copies of $\mathbb{P}^n$ in a larger ambient space.

Definition 3.4. *Let $n, m \in \mathbb{N}$, then the standard Veronese embedding is the morphism*

$$\begin{array}{ccc} \mathbb{P}^n & \xrightarrow{\quad v_{n,m} \quad} & \mathbb{P}^{\binom{n+m}{m}-1} \\ [X_0 : \cdots : X_n] & \longmapsto & [X_0^m : \cdots : X_n^m] \end{array}$$

where the sequence $[X_0^m : \cdots : X_n^m]$ is ordered by the lexicographical order. The images of these embeddings are called standard Veronese varieties and they are denoted by $V_{n,m}$.

Definition 3.5. *Let $n, m \in \mathbb{N}$, $N_{n,m} := \binom{n+m}{m} - 1$ and $M \in \mathrm{GL}(N_{n,m}+1)$. Then we define*

$$v_{n,m}^M := M \circ v_{n,m}, \quad V_{n,m}^M := MV_{n,m}$$

to be respectively the Veronese embedding and the Veronese variety represented by the matrix M.

For our purposes we are interested in Segre embeddings $s^M_{1,1}$, the Veronese embeddings $v^{M'}_{3,m}$. We give a name to their composition.

Definition 3.6. *We call σ-embedding any composition $v^{M'}_{3,m} \circ s^M_{1,1}$.*

Any σ-embedding is represented by a $(N_{3,m}+1) \times (m+1)^2$ matrix M. It is defined by the condition

$$\sigma([X_0, X_1], [Y_0, Y_1]) = M \cdot \begin{bmatrix} X_0^m Y_0^m \\ \vdots \\ X_1^m Y_1^m \end{bmatrix}$$

We now describe how to construct automorphisms of the Veronese varieties. First of all we describe a natural multiplicative group homomorphism

$$\mathrm{GLEmb}(n, m) : \mathrm{GL}(n+1) \to \mathrm{GL}(N_{n,m})$$

arising from the standard Veronese embedding $v_{n,m}$. Let $A := (a_{ij})_{i,j \in \{0,\dots,n\}} \in \mathrm{GL}(n+1)$. It corresponds to an action on the coordinates

$$X_i \mapsto L_i := \sum_{j=0}^{n} a_{ij} X_j, \quad i \in \{0, .., n\}$$

There is a natural action induced on the monomials of any fixed degree, in fact

$$X_0^{e_0} \cdots X_n^{e_n} \mapsto L_0^{e_0} \cdots L_n^{e_n}$$

We denote by $\mathrm{GL}(n, m)(A)$ the matrix representing the action of A on the homogeneous polynomials of degree m with respect to the monomial basis with the standard lexicographical order.

Definition 3.7. *We call general linear group embedding associated to the standard Veronese embedding $v_{n,m}$ the function* $\mathrm{GLEmb}(n, m)$*, which is defined above.*

Example 3.8. *In the case $n = 1, m = 2, N_{n,m} = 2$ a general matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{GL}(2)$ acts on the coordinates*

$$\begin{aligned} X_0 &\mapsto aX_0 + bX_1 \\ X_1 &\mapsto cX_0 + dX_1 \end{aligned}$$

Then the action on the monomials of degree 2 is the following

$$\begin{aligned} X_0^2 &\mapsto a^2X_0^2 + 2abX_0X_1 + b^2X_1^2 \\ X_0X_1 &\mapsto acX_0^2 + (ad + bc)X_0X_1 + bdX_1^2 \\ X_1^2 &\mapsto c^2X_0^2 + 2cdX_0X_1 + d^2X_1^2 \end{aligned}$$

$$So\ \mathrm{GLEmb}(1,2)\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a^2 & 2ab & b^2 \\ ac & ad+bc & bd \\ c^2 & 2cd & d^2 \end{pmatrix}$$

The subgroup $\mathrm{Im}(\mathrm{GLEmb}(n,m)) \subset \mathrm{GL}(N_{n,m}+1)$ corresponds to the set of automorphisms of $\mathbb{P}^{N_{n,m}}$ which fix $V_{n,m}$. We can construct matrices representing automorphisms of any Veronese variety $V_{n,m}^M$.

Proposition 3.9. $\mathrm{Aut}(V_{n,m}^M) := M\,\mathrm{Im}(\mathrm{GL}(n,m))M^{-1}$

Proof. It is a general fact

$$\mathrm{Aut}(MX) = M\,\mathrm{Aut}(X)M^{-1}$$

for any $X \subset \mathbb{P}^N$ projective subvariety, for any $M \in \mathrm{GL}(N+1)$. □

4 Quadratic Surface Intersection (QSI) Key Exchange

In the proposed key exchange protocol both Alice and Bob choose random quadric surfaces. The common key is the isomorphism class of the curve intersection of those quadrics, namely its j-invariant. To make the exchange secure the quadric surface is embedded in a large projective space through a non-standard Veronese embedding. Any user U has a private data given by a non-standard Veronese embedding of $\mathbb{P}^3$ represented by a $N_{n,m} \times N_{n,m}$ matrix. The user has also a private data given by the isomorphic copy of quadric surface inside the chosen Veronese variety. U also needs to publish some data in order to allow anyone who wants to contact him to produce a distinct and random quadric surface: for this purpose he publishes some automorphisms of the Veronese variety and the user chooses another quadric surface (distinct from the private one) inside it. These information should not allow any eavesdropper to recover the Veronese embedding chosen by U.

4.1 QSI algorithm first version.

The algorithm is comprised of key generation and the key exchange.
User key construction:

1. U chooses a finite field $\mathbb{F}_q$.
2. U chooses $m \in \mathbb{N}^+$ and computes $N = \binom{m+3}{3} - 1$.

3. U chooses a non-standard Veronese embedding

$$v_{3,m}^{M_U} : \mathbb{P}^3 \to M_U \cdot V_{3,m} \subset \mathbb{P}^N$$

represented by the matrix $M_U \in \mathrm{GL}(N+1)$.

4. U constructs some automorphisms of $M_U \cdot V_{3,m}$ by using the homomorphism $\mathrm{GLEmb}(3, m)$. U chooses a set of automorphisms of $\mathbb{P}^3$ of order $q^4 - 1$ (with a characteristic polynomial irreducible over $\mathbb{F}_q$) $\{U_i'\}_{1 \le i \le t} \subset \mathrm{GL}(4)$ and then he computes

$$U_i := M_U \, \mathrm{GLEmb}(3, \mathrm{m})(\mathrm{U_i'}) \, M_U^{-1}$$

we assume that $t = 2$ is the most appropriate one.

5. U constructs a secret quadric surface inside $M_U \cdot V_{3,m}$, more precisely a σ-embedding

$$\sigma_U^{(s)} : \mathbb{P}^1 \times \mathbb{P}^1 \to M_U \cdot V_{3,m} \subset \mathbb{P}^N$$

represented by a $(N+1) \times (m+1)^2$ matrix $M_U^{(s)}$. U constructs also a hyperplane $H_U \subset \mathbb{P}^N$ containing $\mathrm{Im}(\sigma_U^{(s)})$, which is represented by a vector in $\mathrm{coker}(M_U^{(s)}) \subset \mathbb{F}_q^{N+1}$.

6. U constructs a public quadric surface inside $M_U \cdot V_{3,m}$, more precisely a σ-embedding

$$\sigma_U^{(p)} : \mathbb{P}^1 \times \mathbb{P}^1 \to M_U \cdot V_{3,m} \subset \mathbb{P}^N$$

represented by a $N + 1 \times (m+1)^2$ matrix $M_U^{(p)}$.

The key exchange is asymmetric since the common keys are different depending on if Alice wants to contact Bob or vice versa. Suppose that Bob wants to contact Alice.

Alice public keys:

- The field $\mathbb{F}_q$.
- $m \in \mathbb{N}^+$.
- Two matrices $A_1, A_2 \in \mathrm{GL}(N+1)$, where $N = \binom{m+3}{3} - 1$.
- The $(N+1) \times (m+1)^2$ matrix $M_A^{(p)}$.

- The hyperplane $H_A \in \mathbb{F}_q^{N+1}$.

Alice secret keys:

- The matrix $M_A^{(s)}$.

Key Exchange:

1. Bob chooses $m_1, m_2, m_1', m_2' \in \{0, ..., q^4 - 1\}$ and then computes $M_B' := A_1^{m_1} A_2^{m_2} A_1^{m_1'} A_2^{m_2'}$.

2. Bob computes the matrix $M_B := M_B' \cdot M_A^{(p)}$. This corresponds to a choice of a σ-embedding $\sigma_B : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^N$.

3. Bob computes a random $H_B \in \text{coker}(M_B)$ and sends it to Alice. This corresponds to a hyperplane containing $\text{Im}(\sigma_B)$.

4. Bob computes the pullback $\sigma_B^* H_A$. It is a curve in $\mathbb{P}^1 \times \mathbb{P}^1$ defined by a curve of bi-degree (m, m). He uses a factorization algorithm to find a component of bi-degree (2,2) then he 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 (see appendix B for more details), so the j_B is well determined except for $m = 4$.

5. 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.

Example 4.1. *(Toy Example)* ***Key Generation:*** *A finite field $\mathbb{F}_q$ with $q = 67$, $m = 3$. Alice chooses a random matrix*

$$M_A = \begin{bmatrix}
56 & 21 & 22 & 46 & 19 & 30 & 54 & 59 & 17 & 23 & 35 & 17 & 18 & 60 & 13 & 54 & 27 & 43 & 55 & 16 \\
42 & 1 & 54 & 49 & 3 & 29 & 9 & 1 & 34 & 65 & 35 & 65 & 34 & 47 & 27 & 4 & 25 & 53 & 27 & 17 \\
29 & 3 & 59 & 56 & 50 & 44 & 36 & 27 & 63 & 33 & 3 & 15 & 4 & 36 & 28 & 32 & 3 & 50 & 29 & 56 \\
62 & 53 & 21 & 31 & 23 & 50 & 28 & 37 & 13 & 62 & 16 & 27 & 29 & 27 & 66 & 44 & 40 & 42 & 60 & 55 \\
9 & 2 & 58 & 4 & 50 & 2 & 63 & 34 & 10 & 1 & 27 & 34 & 14 & 17 & 11 & 61 & 4 & 48 & 36 & 61 \\
35 & 63 & 13 & 66 & 50 & 14 & 23 & 42 & 23 & 58 & 22 & 14 & 6 & 29 & 52 & 58 & 36 & 9 & 42 & 0 \\
61 & 64 & 15 & 65 & 57 & 44 & 54 & 60 & 11 & 4 & 25 & 37 & 29 & 5 & 56 & 9 & 9 & 11 & 57 & 31 \\
40 & 42 & 2 & 48 & 28 & 26 & 31 & 9 & 8 & 15 & 62 & 31 & 53 & 46 & 12 & 39 & 46 & 52 & 30 & 8 \\
29 & 28 & 40 & 29 & 36 & 62 & 32 & 57 & 47 & 25 & 11 & 10 & 55 & 8 & 39 & 43 & 3 & 66 & 64 & 29 \\
61 & 63 & 24 & 42 & 43 & 15 & 18 & 63 & 21 & 64 & 60 & 14 & 26 & 8 & 12 & 0 & 23 & 61 & 28 & 66 \\
55 & 21 & 48 & 0 & 47 & 17 & 20 & 22 & 61 & 65 & 49 & 5 & 24 & 43 & 51 & 24 & 62 & 14 & 41 & 42 \\
34 & 25 & 43 & 37 & 36 & 11 & 16 & 11 & 65 & 59 & 61 & 54 & 22 & 66 & 66 & 49 & 28 & 20 & 26 & 3 \\
0 & 38 & 53 & 16 & 44 & 46 & 21 & 64 & 54 & 5 & 39 & 2 & 64 & 28 & 61 & 30 & 53 & 1 & 34 & 58 \\
18 & 65 & 52 & 54 & 6 & 31 & 43 & 3 & 46 & 7 & 5 & 26 & 29 & 55 & 39 & 65 & 12 & 4 & 33 & 63 \\
49 & 59 & 43 & 54 & 46 & 14 & 16 & 4 & 30 & 40 & 29 & 1 & 48 & 59 & 22 & 2 & 8 & 14 & 30 & 33 \\
34 & 46 & 63 & 8 & 14 & 51 & 1 & 29 & 6 & 52 & 46 & 47 & 25 & 9 & 13 & 28 & 8 & 33 & 25 & 34 \\
48 & 31 & 6 & 62 & 34 & 49 & 16 & 60 & 32 & 21 & 55 & 22 & 2 & 23 & 35 & 20 & 62 & 0 & 64 & 15 \\
33 & 45 & 48 & 62 & 5 & 0 & 1 & 65 & 66 & 35 & 43 & 34 & 5 & 18 & 11 & 57 & 41 & 6 & 53 & 41 \\
12 & 24 & 28 & 36 & 4 & 18 & 31 & 34 & 1 & 21 & 65 & 13 & 1 & 31 & 43 & 9 & 23 & 43 & 66 & 13 \\
41 & 9 & 45 & 49 & 6 & 38 & 40 & 4 & 50 & 45 & 10 & 14 & 13 & 18 & 40 & 23 & 6 & 33 & 13 & 39
\end{bmatrix}$$

which represents a choice of a Veronese embedding

$$v_A : \mathbb{P}^3 \to V_A \subset \mathbb{P}^{19}.$$

She produces a random automorphism of the Veronese variety V_A which is given by a matrix

$$A_1 = \begin{bmatrix}
60 & 55 & 21 & 17 & 53 & 5 & 30 & 53 & 30 & 25 & 36 & 1 & 40 & 46 & 14 & 36 & 27 & 7 & 54 & 54 \\
0 & 59 & 51 & 65 & 25 & 62 & 57 & 4 & 23 & 55 & 8 & 53 & 8 & 34 & 36 & 24 & 36 & 33 & 55 & 60 \\
56 & 34 & 7 & 35 & 10 & 39 & 18 & 64 & 62 & 49 & 23 & 10 & 41 & 28 & 0 & 12 & 1 & 52 & 51 & 51 \\
61 & 42 & 35 & 43 & 29 & 44 & 30 & 35 & 28 & 61 & 6 & 48 & 30 & 54 & 21 & 37 & 8 & 21 & 48 & 0 \\
37 & 20 & 42 & 4 & 23 & 25 & 26 & 47 & 3 & 46 & 31 & 49 & 13 & 12 & 40 & 21 & 10 & 66 & 12 & 38 \\
27 & 39 & 26 & 35 & 4 & 43 & 35 & 48 & 5 & 57 & 56 & 28 & 55 & 65 & 15 & 23 & 27 & 43 & 41 & 53 \\
54 & 9 & 7 & 15 & 21 & 21 & 8 & 57 & 40 & 22 & 50 & 55 & 29 & 46 & 39 & 42 & 44 & 21 & 39 & 32 \\
3 & 17 & 9 & 43 & 3 & 48 & 38 & 49 & 24 & 5 & 20 & 60 & 56 & 57 & 31 & 18 & 53 & 57 & 21 & 43 \\
63 & 20 & 4 & 44 & 2 & 30 & 16 & 26 & 21 & 23 & 40 & 42 & 6 & 28 & 26 & 23 & 40 & 62 & 54 & 1 \\
23 & 6 & 0 & 50 & 47 & 46 & 29 & 17 & 62 & 62 & 32 & 55 & 26 & 22 & 27 & 65 & 29 & 25 & 65 & 11 \\
66 & 16 & 65 & 60 & 8 & 34 & 21 & 43 & 49 & 64 & 3 & 20 & 37 & 49 & 1 & 9 & 58 & 39 & 20 & 5 \\
38 & 19 & 30 & 22 & 11 & 15 & 20 & 9 & 16 & 1 & 65 & 12 & 17 & 1 & 56 & 41 & 4 & 21 & 44 & 19 \\
15 & 16 & 16 & 4 & 26 & 61 & 62 & 16 & 6 & 36 & 33 & 33 & 30 & 2 & 35 & 56 & 65 & 59 & 33 & 46 \\
44 & 22 & 9 & 56 & 57 & 11 & 10 & 6 & 14 & 22 & 24 & 58 & 49 & 32 & 35 & 58 & 4 & 14 & 53 & 48 \\
65 & 26 & 24 & 24 & 48 & 57 & 14 & 44 & 0 & 39 & 18 & 45 & 35 & 19 & 21 & 59 & 56 & 63 & 1 & 3 \\
39 & 24 & 5 & 34 & 46 & 14 & 31 & 14 & 59 & 40 & 1 & 38 & 43 & 46 & 40 & 21 & 33 & 65 & 20 & 36 \\
54 & 55 & 41 & 7 & 17 & 58 & 13 & 30 & 1 & 66 & 53 & 41 & 15 & 47 & 66 & 65 & 58 & 34 & 0 & 41 \\
55 & 37 & 41 & 32 & 11 & 42 & 38 & 25 & 43 & 9 & 33 & 7 & 31 & 25 & 59 & 3 & 45 & 61 & 36 & 36 \\
39 & 26 & 46 & 66 & 50 & 5 & 52 & 14 & 2 & 3 & 15 & 25 & 22 & 27 & 65 & 4 & 56 & 58 & 27 & 60 \\
46 & 35 & 61 & 39 & 20 & 51 & 21 & 50 & 55 & 29 & 18 & 38 & 12 & 46 & 59 & 51 & 2 & 43 & 15 & 31
\end{bmatrix}$$

and she keeps the secret embedding

$$\sigma_A^{(s)} : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^{19}$$

represented by the matrix

$$M_A^{(s)} = \begin{bmatrix}
9 & 17 & 23 & 59 & 50 & 10 & 11 & 36 & 64 & 56 & 27 & 16 & 40 & 62 & 8 & 6 \\
34 & 48 & 49 & 26 & 25 & 58 & 16 & 33 & 36 & 2 & 43 & 4 & 62 & 39 & 17 & 34 \\
3 & 49 & 33 & 24 & 26 & 64 & 66 & 46 & 63 & 17 & 61 & 49 & 14 & 43 & 65 & 23 \\
37 & 45 & 12 & 60 & 27 & 5 & 29 & 3 & 33 & 51 & 7 & 30 & 11 & 47 & 40 & 44 \\
54 & 57 & 19 & 25 & 13 & 14 & 37 & 23 & 24 & 39 & 21 & 41 & 58 & 41 & 65 & 64 \\
40 & 18 & 2 & 44 & 64 & 32 & 17 & 15 & 42 & 15 & 27 & 30 & 45 & 22 & 39 & 49 \\
46 & 10 & 38 & 59 & 31 & 36 & 1 & 28 & 18 & 51 & 46 & 19 & 5 & 8 & 31 & 26 \\
45 & 65 & 39 & 32 & 35 & 6 & 18 & 65 & 12 & 0 & 17 & 59 & 65 & 4 & 26 & 5 \\
4 & 14 & 13 & 27 & 43 & 58 & 63 & 66 & 41 & 57 & 39 & 12 & 30 & 43 & 25 & 7 \\
4 & 1 & 6 & 25 & 49 & 11 & 40 & 48 & 20 & 30 & 52 & 29 & 35 & 23 & 35 & 3 \\
31 & 5 & 63 & 25 & 63 & 2 & 20 & 62 & 32 & 13 & 43 & 24 & 18 & 14 & 40 & 14 \\
21 & 38 & 7 & 31 & 46 & 50 & 3 & 27 & 8 & 59 & 47 & 21 & 29 & 53 & 22 & 1 \\
9 & 55 & 21 & 31 & 48 & 5 & 20 & 66 & 9 & 33 & 28 & 0 & 45 & 25 & 7 & 48 \\
19 & 48 & 3 & 13 & 6 & 20 & 1 & 33 & 37 & 12 & 61 & 63 & 36 & 34 & 55 & 35 \\
21 & 9 & 62 & 15 & 20 & 7 & 24 & 62 & 64 & 9 & 30 & 31 & 1 & 46 & 62 & 60 \\
37 & 52 & 30 & 58 & 33 & 46 & 63 & 28 & 38 & 22 & 14 & 36 & 12 & 30 & 10 & 59 \\
33 & 36 & 36 & 55 & 66 & 15 & 15 & 56 & 17 & 56 & 62 & 21 & 7 & 39 & 20 & 29 \\
30 & 40 & 53 & 59 & 8 & 9 & 62 & 28 & 13 & 31 & 4 & 41 & 44 & 24 & 47 & 51 \\
50 & 41 & 5 & 5 & 42 & 40 & 62 & 20 & 36 & 59 & 2 & 41 & 23 & 62 & 25 & 42 \\
24 & 66 & 52 & 46 & 24 & 23 & 64 & 8 & 45 & 52 & 59 & 29 & 10 & 4 & 33 & 12
\end{bmatrix}.$$

For a public key, she computes a hyperplane H_A, which is a closed subscheme of projective space $\mathbb{P}^{19}$ over $\mathbb{F}_q$ defined by:

$$x_0 - 21x_3 - 15x_5 - 32x_6 + 16x_7 - 10x_8 + 5x_9 + 11x_{10} + 16x_{11} + x_{12} - 4x_{13} \\ -28x_{14} - 20x_{15} + 18x_{16} + 8x_{17} + x_{18} + 32x_{19}$$

containing the image of $\sigma_A^{(s)}$ *and also computes an embedding*

$$\sigma_A^{(p)} : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^{19}$$

represented by the matrix

$$M_A^{(p)} = \begin{bmatrix}
28 & 32 & 4 & 38 & 26 & 36 & 6 & 20 & 1 & 2 & 22 & 27 & 23 & 35 & 10 & 24 \\
29 & 3 & 48 & 59 & 19 & 11 & 17 & 23 & 10 & 61 & 12 & 50 & 21 & 17 & 46 & 35 \\
27 & 21 & 45 & 43 & 33 & 48 & 4 & 43 & 64 & 37 & 34 & 46 & 60 & 3 & 41 & 27 \\
4 & 45 & 65 & 55 & 6 & 40 & 11 & 30 & 41 & 31 & 19 & 23 & 42 & 41 & 11 & 1 \\
53 & 14 & 44 & 37 & 15 & 49 & 57 & 26 & 55 & 22 & 29 & 45 & 44 & 9 & 59 & 30 \\
45 & 60 & 22 & 66 & 26 & 27 & 60 & 60 & 54 & 63 & 62 & 64 & 4 & 18 & 44 & 18 \\
42 & 33 & 47 & 53 & 52 & 65 & 45 & 28 & 5 & 21 & 58 & 45 & 49 & 31 & 22 & 27 \\
30 & 13 & 6 & 6 & 37 & 40 & 38 & 51 & 2 & 43 & 61 & 6 & 52 & 4 & 48 & 34 \\
66 & 54 & 47 & 64 & 13 & 20 & 66 & 23 & 31 & 36 & 55 & 42 & 11 & 27 & 39 & 17 \\
29 & 28 & 31 & 44 & 54 & 9 & 60 & 44 & 64 & 1 & 59 & 12 & 38 & 41 & 57 & 32 \\
10 & 18 & 2 & 58 & 38 & 5 & 35 & 14 & 55 & 16 & 22 & 61 & 18 & 13 & 55 & 46 \\
28 & 53 & 39 & 66 & 55 & 0 & 46 & 21 & 7 & 49 & 30 & 1 & 60 & 15 & 37 & 63 \\
54 & 24 & 9 & 29 & 24 & 42 & 51 & 50 & 35 & 10 & 50 & 18 & 16 & 44 & 10 & 7 \\
64 & 24 & 63 & 33 & 49 & 14 & 47 & 35 & 33 & 30 & 59 & 4 & 20 & 24 & 66 & 1 \\
59 & 37 & 43 & 25 & 55 & 7 & 21 & 26 & 62 & 44 & 64 & 45 & 66 & 4 & 46 & 62 \\
7 & 47 & 2 & 13 & 0 & 40 & 21 & 1 & 11 & 7 & 56 & 14 & 60 & 41 & 21 & 62 \\
51 & 20 & 31 & 4 & 55 & 36 & 27 & 22 & 61 & 42 & 32 & 51 & 56 & 20 & 26 & 5 \\
36 & 46 & 36 & 42 & 59 & 65 & 33 & 58 & 43 & 20 & 40 & 50 & 15 & 7 & 11 & 63 \\
18 & 15 & 53 & 12 & 3 & 8 & 50 & 66 & 55 & 39 & 42 & 8 & 10 & 31 & 1 & 29 \\
66 & 34 & 55 & 50 & 26 & 57 & 3 & 35 & 30 & 41 & 39 & 55 & 35 & 40 & 40 & 27
\end{bmatrix}$$

Bob chooses a random integer $m_1 = 70$ *(for sake of brevity, in the present example, we have chosen only one automorphism instead of two), computes an automorphism* $M_B = A_1^{m_1}$ *of the variety* V_A *and then a* σ*-embedding*

$$\sigma_B : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^{19}$$

represented by the matrix

$$M_B = \begin{bmatrix}
46 & 26 & 7 & 53 & 4 & 8 & 3 & 63 & 15 & 66 & 49 & 2 & 4 & 9 & 56 & 4 \\
61 & 24 & 1 & 50 & 17 & 19 & 48 & 28 & 38 & 45 & 44 & 35 & 36 & 49 & 4 & 48 \\
22 & 28 & 65 & 20 & 18 & 24 & 4 & 65 & 37 & 17 & 57 & 7 & 29 & 59 & 20 & 35 \\
58 & 21 & 5 & 64 & 66 & 8 & 17 & 20 & 27 & 17 & 14 & 50 & 53 & 40 & 28 & 18 \\
25 & 56 & 30 & 19 & 39 & 62 & 44 & 21 & 37 & 1 & 22 & 43 & 8 & 13 & 30 & 19 \\
43 & 14 & 16 & 44 & 60 & 60 & 21 & 10 & 48 & 65 & 53 & 20 & 46 & 12 & 35 & 44 \\
27 & 52 & 64 & 40 & 51 & 25 & 13 & 62 & 48 & 57 & 53 & 14 & 43 & 25 & 42 & 50 \\
38 & 56 & 61 & 42 & 26 & 42 & 29 & 20 & 23 & 34 & 56 & 34 & 29 & 60 & 25 & 24 \\
15 & 35 & 27 & 50 & 4 & 7 & 56 & 25 & 66 & 36 & 47 & 38 & 38 & 41 & 3 & 28 \\
10 & 38 & 43 & 46 & 56 & 37 & 28 & 48 & 44 & 51 & 23 & 52 & 5 & 48 & 22 & 50 \\
34 & 50 & 50 & 37 & 12 & 29 & 11 & 40 & 31 & 5 & 52 & 13 & 53 & 58 & 29 & 52 \\
37 & 20 & 40 & 22 & 49 & 37 & 58 & 0 & 8 & 19 & 26 & 34 & 52 & 35 & 19 & 53 \\
19 & 39 & 22 & 65 & 5 & 7 & 62 & 35 & 51 & 43 & 16 & 35 & 48 & 43 & 38 & 44 \\
60 & 3 & 49 & 48 & 44 & 9 & 39 & 26 & 39 & 50 & 24 & 53 & 52 & 4 & 0 & 43 \\
0 & 23 & 54 & 63 & 27 & 26 & 59 & 23 & 8 & 50 & 62 & 42 & 37 & 48 & 26 & 60 \\
5 & 14 & 33 & 28 & 36 & 24 & 17 & 18 & 15 & 47 & 30 & 49 & 37 & 34 & 55 & 16 \\
59 & 57 & 9 & 62 & 38 & 57 & 61 & 30 & 5 & 13 & 58 & 64 & 36 & 40 & 18 & 61 \\
38 & 48 & 39 & 43 & 40 & 9 & 35 & 51 & 14 & 40 & 60 & 61 & 50 & 2 & 25 & 22 \\
38 & 51 & 37 & 66 & 26 & 25 & 40 & 6 & 64 & 22 & 62 & 16 & 12 & 57 & 14 & 9 \\
21 & 15 & 48 & 53 & 36 & 20 & 29 & 25 & 18 & 18 & 2 & 0 & 62 & 64 & 36 & 63
\end{bmatrix}$$

He also computes a hyperplane H_B*, which is again the closed subscheme of projective space of dimension over* $\mathbb{F}_q$ *defined by:*

$$x_0 + 4400x_1 + 4433x_2 + 8909x_3 + 26482x_4 + 3162x_5 - 4113x_6 + 24289x_7 \\ -15946x_8 + 4813x_9$$

and is identifed by an element of coker(M_B).

Key Exchange:

Bob computes the pullback

$$\begin{aligned}\sigma_B^* H_A = {} & 12x_0^3x_2^3 + 2x_0^2x_1x_2^3 + 13x_0x_1^2x_2^3 - 7x_1^3x_2^3 + 26x_0^3x_2^2x_3 + 29x_0^2x_1x_2^2x_3 \\ & - 19x_0x_1^2x_2^2x_3 + 16x_1^3x_2^2x_3 + 29x_0^3x_2x_3^2 - 30x_0x_1^2x_2x_3^2 + 9x_1^3x_2x_3^2 \\ & - 26x_0^3x_3^3 + 12x_0^2x_1x_3^3 - 22x_0x_1^2x_3^3 - 24x_1^3x_3^3\end{aligned}$$

and finds a component of bi-degree (2,2)

$$\begin{aligned}C_1 = {} & -x_0^2x_2^2 + 6x_0x_1x_2^2 + x_1^2x_2^2 + 28x_0^2x_2x_3 - 12x_0x_1x_2x_3 + 30x_1^2x_2x_3 - 4x_0^2x_3^2 \\ & - 24x_0x_1x_3^2 - 9x_1^2x_3^2\end{aligned}$$

and computes the j-invariant $j_B = j(C_1) = 57 \in \mathbb{F}_q$. Alice computes the pullback

$$\begin{aligned}\sigma^{(s)_A^*} H_B = {} & -32x_0^2x_1x_2^3 - 15x_0x_1^2x_2^3 + 24x_1^3x_2^3 - 7x_0^2x_1x_2^2x_3 - 16x_0x_1^2x_2^2x_3 \\ & - 29x_0^3x_2x_3^2 + 19x_0^2x_1x_2x_3^2 - 11x_0x_1^2x_2x_3^2 - 16x_1^3x_2x_3^2 - 27x_0^3x_3^3 \\ & - 5x_0^2x_1x_3^3 - 7x_0x_1^2x_3^3 + 26x_1^3x_3^3\end{aligned}$$

and finds a component of bi-degree (2,2)

$$C_2 = 33x_0x_1x_2^2 + x_1^2x_2^2 - 23x_0x_1x_2x_3 - 2x_1^2x_2x_3 + 32x_0^2x_3^2 - 19x_1^2x_3^2$$

and computes the j-invariant $j_A = j(C_2) = 57 \in \mathbb{F}_q$, which is the common key.

This version of the algorithm has some practical issues: the memory required to reach a good level of security is remarkably larger than the one needed by some of the most practical existing post-quantum cryptosystems, like lattice based ones and SIDH. In fact each user has a public key comprehensive of matrices of large size over $\mathbb{F}_q$. Another issue is the speed of the key exchange, in particular the bottleneck is the computation of products of big matrices.

4.2 QSI algorithm second version

In this section we describe some modifications of the previous algorithm which significantly improve the speed of the key exchange. It is not clear that whether this makes the protocol prone to some attacks by the extra information revealed.

Experimental evidence shows that the computationally heavy part of the key exchange is the calculation of M'_B: it is required to compute powers of matrices of large size. By choosing A_1, A_2 to be generalized permutation matrices, Alice can dramatically speed up the computations of this product of matrices. This can be achieved by choosing A'_1, A'_2 and M_A to be generalized permutation matrices. A drawback is that the order of A_i is bounded by $4(q-1)$. So in this context, Alice should use a much larger value of q to reach the same level of security.

Besides the improvement in the speed of the key exchange, the main issue remains the size of the public key. The major contribution to this size is by the matrix $M_A^{(p)}$, which requires around $l \cdot (m+1)^2 \cdot \binom{m+3}{3}$ bits, where l is the binary length of q. For example in the case $l = 64, m = 8$ this values is 855360, which is unpractical. A problem is to reduce the size of $M_B^{(p)}$, which can be achieved by taking sparse or small entry matrices.

5 QSI Key Exchange with TTP

In this section we describe a variation of the key exchange where a trusted third party is allowed. TTP are not used in the design of the most common key exchange protocols, on the other hand they are required in several real-life applications. The advantage of the TTP (which will be called "Trent") in the case of the QSI key exchange protocol is that it allows the users to have a high level of security with a considerably short public key size and less time in common key generation.

Trent secret data:

- A Veronese variety $V_T \subset \mathbb{P}^{\binom{m+3}{3}-1}$ for $m \in \mathbb{N}$.

Trent public data:

- A finite field $\mathbb{F}_q$.
- A positive integer m.
- A matrix M_T of size $\binom{m+3}{3} \times (m+1)^2$ representing a σ-embedding of $\mathbb{P}^1 \times \mathbb{P}^1$ into V_T.
- Two $\binom{m+3}{3} \times \binom{m+3}{3}$ matrices T_1, T_2 representing automorphisms of V_T of order $q^4 - 1$.

Suppose that a user U wants to register to Trent's key exchange system. Then U has to:

1. Download Trent's public data.
2. Choose random integers $1 \leq m_1^U, m_2^U, m_1'^U, m_2'^U \leq q^4 - 1$ and to compute $M_U := T_1^{m_1^U} T_2^{m_2^U} T_1^{m_1'^U} T_2^{m_2'^U}$. This corresponds to the choice of a σ-embedding $\sigma_U : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^{\binom{m+3}{3}-1}$ such that $\mathrm{Im}(\sigma_U) \subset V_T$.
3. Compute a random $H_U \in \mathrm{coker}(M_U)$. This corresponds to the choice of a hyperplane containing $\mathrm{Im}(\sigma_U)$.

Suppose that Alice and Bob want to generate a common key, then:

1. Alice downloads Bob's public key H_B, she computes $\sigma_A^* H_B$ and she finds a component of bi-degree $(2,2)$. Then she computes its j-invariant j_A.
2. Bob downloads Alice's public key H_A, he computes $\sigma_B^* H_A$ and he finds a component of bi-degree $(2,2)$. Then he computes its j-invariant j_B.

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

Remark 5.1. *H_U is the public key. Its binary length is $\binom{m+3}{3} \cdot l$, where l is the binary length of q. For example, imposing $\binom{m+3}{3} - (m+1)^2 - 1$ coefficients equal to 0 and one coefficient equal to 1, H_U can be described by $l(m+1)^2$ bits. For $l = 64$ and $m = 8$ it is equal to 5184 bits: shorter than in SIDH or NTRU at 128-bit security level.*

6 Underlying mathemtical problems

Suppose that an eavesdropper Eve wants to break the protocol. Then she has the following possible options:

1. She can try to find explicitly the Veronese variety, i.e. the $\binom{m+3}{3} \times \binom{m+3}{3}$ matrix M_U in the version without TTP or M_T in the TTP version. Note that, in the case of TTP version, if Eve is able to solve this problem, then she is able to break any communication between two users of the Trent system.
2. She can try to find $M_U^{(s)}$ in the version without TTP, or M_U in the version with TTP. Note that, in the case of TTP version, if Eve is able to solve this problem, then she is able to break any communication between U and other users of the Trent system.

3. She can find the explicit equations of $V_A = M_A V_{3,m}$ in the version without TTP, or of V_T in the version with TTP. Then she can try to attack the single communication between Alice and Bob by searching the primary components of $V_A \cap H_A \cap H_B$ (without TTP) or $V_T \cap H_A \cap H_B$ (with TTP).

Suppose that Eve wants to follow the first option. Also, suppose that we are in the case of the TTP version (in the other case, the problem is completely analogous). A possible attempt is to find M_T by solving a system of polynomial equations: she writes M_T as a matrix of $\binom{m+3}{3}^2$ unknowns. The condition that T_i is an automorphism of V_T means that

$$T_i M_T = M_T \,\mathrm{GLEmb}(3, \mathrm{m})(A)$$

for some matrix $A \in \mathrm{GL}(4)$. If Eve eliminates the variables $\{a_{ij}\}$, then she gets polynomial conditions of extremely high degree on $m_{i,j}$ (note that $M_T \,\mathrm{GLEmb}(3, \mathrm{m})(A)$ is a matrix whose components are bi-homogeneous polynomials whose bi-degree is $(1, m)$ in the set of variables $\{m_{ij}\}$ and $\{a_{ij}\}$). The condition that σ_U is a σ-embedding such that $\mathrm{Im}(\sigma_U) \subset V_T$ means that

$$\sigma_U = M_T \circ v_{3,m} \circ A \circ s_{1,1}$$

for some $A \in \mathrm{Aut}(\mathbb{P}^3)$. Note that, like above, the matrix M_E representing the σ-embedding $M_T \circ v_{3,m} \circ A \circ s_{1,1}$ is a matrix whose components are bi-homogeneous polynomials whose bi-degree is $(1, m)$ in the set of variables $\{m_{ij}\}$ and $\{a_{ij}\}$. If Eve eliminates the variables $\{a_{ij}\}$, then she gets polynomial conditions of extremely high degree on $\{m_{ij}\}$.

Suppose that Eve chooses the second option to attack the system. Then she wants to find $m_1^U, m_2^U, m_1'^U, m_2'^U$ such that

$$H_U \in \mathrm{coker}\left(T_1^{m_1^U} T_2^{m_2^U} T_1^{m_1'^U} T_2^{m_2'^U}\right).$$

Since the product of matrices is non-commutative, it seems that methods similar to Pollard rho or baby-step giant-step are not possible in this case. Since the family of quadric surfaces of $\mathbb{P}^3$ is a 9-dimensional projective space, using a brute force attack (just choosing random values of $m_1^U, m_2^U, m_1'^U, m_2'^U$), Eve should find a σ-embedding σ_E such that $\mathrm{Im}(\sigma_E) = \mathrm{Im}(\sigma_U)$ in around q^9 trials (instead of q^{16} as one would expect).

Suppose that Eve wants to choose the third option: she has first to compute the polynomial equations defining V_T. This is not a hard problem because V_T is defined by $m(m^2-1)(m^3+12m^2+59m+66)$ degree-2

homogeneous polynomials by proposition D.1 and that can be found by the methods of linear algebra. After this, one needs to find the irreducible components of the variety $V_T \cap H_A \cap H_B$, this corresponds to find the primary decomposition of the ideal generated by the quadratic polynomials defining V_T and the two linear polynomials defining respectively H_A and H_B.

Acknowledgements

We would like to thank Ankan Pal for his constructive suggestions on an earlier version of this paper.

References

[1] A. Abdesselam: A computational solution to a question by Beauville on the invariants of the binary quintic. Journal of Algebra 303, 771–788(2006)

[2] Berlekamp E. R., McEliece R. J., van Tilborg H. C. A.: On the inherent intractability of certain coding problems. IEEE Trans. Information Theory IT-24(3), 384–386(1978)

[3] Bernstein D. J., Buchmann J., Dahmen E. :Post-Quantum Cryptography, Springer-Verlag Berlin Heidelberg (2009)

[4] Castryck W., Lange T., Martindale C., Panny L., Renes J.:CSIDH: An Efficient Post-Quantum Commutative Group Action. In: Peyrin T., Galbraith S. (eds) Advances in Cryptology - ASIACRYPT 2018. Lecture Notes in Computer Science, vol 11274. Springer, Cham, (2018)

[5] De Feo L., Jao D.,Plût J. :Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. J. Math. Cryptol., 8, 209 – 247(2014)

[6] Dolgachev, I. (2003) Lectures on Invariant Theory. CUP.

[7] Salmon G.: Higher Algebra, fifth ed., 1885, reprinted by Chelsea, New York. `https://archive.org/details/lessonsintroduc00salmgoog/page/n210/mode/2up` (1964)

[8] Shafarevich I. R.: Basic Algebraic Geometry 1, third ed. Springer, New York (2013)

[9] Shor P. W.:Algorithms for quantum computation: Discrete logarithmsand factoring. In: M. Robshaw and J. Katz, editors, Foundations of ComputerScience, CONFERENCE 1994, Proceedings., 35th Annual Symposium, pp. 124–134 (1994)

[10] The National Institute of Standards and Technology (NIST).PQC Standardization Process: Second Round Candidate Announcement. (2019)

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

[12] Vakil R.: The rising sea - Foundations of Algebraic Geometry. `http://math.stanford.edu/~vakil/216blog/FOAGnov1817public.pdf`

A Probability that a random curve of bi-degree (2,2) in $\mathbb{P}^1 \times \mathbb{P}^1$ is singular.

Let κ be an algebraically closed field, then a general curve $C \subset \mathbb{P}^1 \times \mathbb{P}^1$ of bi-degree $(2,2)$ is non-singular. More precisely:

Proposition A.1. *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 $\mathbb{K}$*. 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.

B j-invariant of a $(2,2)$-curve in $\mathbb{P}^1 \times \mathbb{P}^1$

A standard result in the theory of algebraic curves is that there is a bijection

$$\left\{\begin{array}{c}\text{genus 1 curves up}\\ \text{to isomorphism.}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{4-tuples of distinct points of } \mathbb{P}^1\\ \text{up to automorphism.}\end{array}\right\}$$

see for example [12, 19.5]. Let $[C]$ be an isomorphism class of genus 1 curves. Let $\pi : C \to \mathbb{P}^1$ be any degree 2 morphism. Then the 4-tuple of points associated to C is the branch locus of π, which are by definition the points $P \in \mathbb{P}^1$ such that $\#\pi^{-1}(P) = 1$.

Example B.1. *Let E be the elliptic curve defined by the equation $Y^2Z = f(X,Z)$, where $f(X,Z) = (X - aZ)(X - bZ)(X - cZ)$, let*

$$\begin{array}{ccc} E & \xrightarrow{\quad\pi\quad} & \mathbb{P}^1 \\ [X:Y:Z] & \longmapsto & [X:Z] \end{array}$$

be the degree 2 map to $\mathbb{P}^1$. The branch locus of π is the set $\{[1:0],[a:1],[b:1],[c:1]\}$.

Example B.2. *Let $C \subset \mathbb{P}^1 \times \mathbb{P}^1$ be a smooth curve of bi-degree (2,2) and let*

$$\begin{array}{ccc} C & \xrightarrow{\pi} & \mathbb{P}^1 \\ (P,Q) & \longmapsto & P \end{array}$$

be the first projection map. Let

$$F(X_0,X_1;Y_0,Y_1) = Y_0^2F_0(X_0,X_1) + Y_0Y_1F_1(X_0,X_1) + Y_1^2F_2(X_0,X_1)$$

be the defining polynomial of C. Then the branch locus of π is the set of points $P = [p_0,p_1]$ for which the equation

$$F(p_0,p_1;Y_0,Y_1) = 0$$

has one (double) solution. Equivalently $F(p_0,p_1,Y_0,Y_1)$ is a quadratic binary form with vanishing discriminant. So $[p_0 : p_1]$ is a root of the binary quartic form

$$G(X_0,X_1) := F_1(X_0,X_1)^2 - 4F_0(X_0,X_1)F_2(X_0X_1)$$

The invariants of a binary quartic form under the action of $\mathrm{GL}(2)$ is classically well known (see for example [7, 199,p.189], [1, 2.2], or [6, 10.2]): if we write

$$G(X_0,X_1) = q_0X_0^4 + q_1X_0^3X_1 + q_2X_0^2X_1^1 + q_3X_0X_1^3 + q_4X_1^4$$

and we define

$$\begin{aligned} S &:= q_0q_4 - \frac{q_1q_3}{4} + \frac{q_2^2}{12} \\ T &:= \frac{q_0q_2q_4}{6} + \frac{q_1q_2q_3}{48} - \frac{q_2^3}{216} - \frac{q_0q_3^2}{16} - \frac{q_1^2q_4}{16} \end{aligned}$$

then $\dfrac{S^3}{S^3 - 27T^2}$ *is the invariant of* G *under the action of* $\mathrm{GL}(2)$ *or equivalently the invariant of the set of points given by the roots of* G *under the action of* $\mathrm{PGL}(2)$. *This is equal to the j-invariant of the curve* C.

C Irreducibility of curves of bi-degree (d, d).

The pullback of a hyperplane H through a σ-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?

D Irreducible components of $V_T \cap H_A \cap H_B$

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 D.1. *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 $h^0(\mathcal{I}_{V_{3,m}}(2))$. Since $V_{3,m}$ is projectively normal, then

$$\begin{aligned} h^0(\mathcal{I}_{V_{3,m}}(2)) &= h^0(\mathcal{O}_{\mathbb{P}^{N_{3,m}}}(2)) - h^0(\mathcal{O}_{V_{3,m}}(2)) \\ &= h^0(\mathcal{O}_{\mathbb{P}^{N_{3,m}}}(2)) - h^0(\mathcal{O}_{\mathbb{P}^3}(2m)) \\ &= \frac{1}{2}\left[\binom{m+3}{3} + 1\right]\binom{m+3}{3} - \binom{2m+3}{3} \end{aligned}$$

which is equal to the desired value. □

Example D.2. *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_T is to generate $d_m - h_m$ points of V_T, where d_m is the dimension of the space of all quadric hypersurfaces, sufficiently random points inside V_T: this can be done easily using the knowledge of the σ-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_T}.

Proposition D.3. *$V_{3,m} \subset \mathbb{P}^{N_{3,m}}$ is a 3-dimensional projective variety of degree m^3.*

Proof. In general $\deg(V_{n,m}) = m^n$, see for example [8, 4.2.7] □

After the computation of the primary components of $V_T \cap H_A \cap H_B$, Eve has to find the j-invariant of the component of degree $4m$. This is explained by the next proposition.

Proposition D.4. *The image of a curve of bi-degree $(2,2)$ through a σ-embedding $\mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^{\binom{m+3}{3}-1}$ 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 $(2,2)\cdot(m,m) = 4m$. □

In conclusion, $V_T \cap H_A \cap H_B$ 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.