A post-quantum signature scheme from the secant variety of the Grassmannian

Daniele Di Tullio Manoj Gyawali*

September 19, 2020

Università degli Studi di Roma Tre, Department of Mathematics. Largo S. Leonardo Murialdo 1, Rome, Italy.
danieleditullio@hotmail.it
manoj.gyawali@uniroma3.it

Abstract

In this paper we present a signature scheme based on the difficulty of finding a point in a shifted Grassmannian variety or on its secant variety from a knowledge of its defining polynomials. An advantage of using the secant variety of the Grassmannian is that it is defined by sparse cubic equations, which are in general more difficult to solve than quadratic ones, thereby reducing the size of the public key.

Keywords: Multivariate cryptography Grassmannian secant variety digital signature

1 Introduction

Most of the currently used public key cryptosystems are based on the well known mathematical problems namely integer factorization and discrete logarithm problems. But, after the widely acclaimed algorithm by Shor [13], these problems have been considered unsafe from the possible large scale quantum computers in near future. That gave a challenge to design the cryptosystems that are strong enough to face quantum computers and

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

at the same time these should be efficient enough for practical purposes. Many efforts have been pursued toward the quantum resistant cryptosystems that include lattice-based, code-based, multivariate, hash-based [4, 8] and isogeny based cryptography see for example [6, 5, 10] .

Multivariate public key authentication scheme like Rainbow [7], one of the three NIST post-quantum signature finalists [15], is known for relatively fast signing and verification but large public key size in comparison to other post quantum signature schemes. In this paper, we purpose a multivariate signature scheme based on the difficulty of finding points inside the shifted secant variety of the Grassmannian when only the implicit equations are known.

The main idea of the signature scheme can be summarized as follows:

1. Alice chooses a secret projective variety Y, which is a shifted (through an automorphism of the ambient space) Secant variety of the Grassmannian.
2. She publishes a set of equations vanishing on the variety.
3. A document is a linear subspace of the ambient space. A signature is a point lying in the intersection.
4. Alice can quickly sign a document by using the Plücker embedding of the Grassmannian and her secret automorphism.

2 Preliminaries

In this section, we describe some background required to explain the signature scheme. There are good references for the materials covered in this section, for example see in [12, 11, 9, 16, 1].

2.1 Affine Varieties

We begin our description by recalling the notion of affine n-space and its subsets defined by zeros of polynomials.

Definition 2.1. *The affine n-space (over a field κ) is the set of n-tuples*

$$\mathbb{A}^n = \mathbb{A}^n(\kappa) = \{P = (x_1, \ldots, x_n) : x_i \in \kappa\}.$$

Let $\kappa[x] = \kappa[x_1, \ldots, x_n]$ be a polynomial ring in n variables and let $I \triangleleft \kappa[x]$ be and ideal. Then to each such I it is associated a subset of $\mathbb{A}^n$:

$$V(I) = \{P \in \mathbb{A}^n : f(P) = 0 \ \ \forall f \in I\}.$$

Definition 2.2. *An affine algebraic set is any set of the form $V(I)$. If V is an algebraic set, the ideal of V is given by*

$$I(V) = \{f \in \kappa[x] : f(p) = 0 \ \ \forall P \in V\}.$$

The affine varieties are indecomposable affine algebraic sets.

Definition 2.3. *An affine variety is an algebraic set V which can not be written as a non-trivial union of other algebraic sets:*

$$V = V_1 \cup V_2 \Rightarrow V = V_1 \text{ or } V = V_2.$$

2.2 Projective Varieties

The projective space is historically constructed by adding "points at infinity" to the affine space. It can be characterized as the lines of the affine space passing through the origin.

Definition 2.4. *The projective n-space (over a field κ), denoted by $\mathbb{P}^n$, is the set of all the $(n+1)$-tuples*

$$(X_0, \ldots, X_n) \in \mathbb{A}^{n+1}$$

such that at least one X_i is non-zero, modulo the equivalence relation

$$(X_0, \ldots, X_n) \sim (Y_0, ..., Y_n)$$

if and only if there exists $c \in \kappa^*$ such that $X_i = cY_i$ for all $i \in \{0, ..., n\}$. The equivalence class of the point $(X_0, ..., X_n)$ is denoted by $[X_0, ..., X_n]$.

Projective algebraic sets are defined similarly as affine algebraic sets. Observe that it is not well defined the vanishing of a general polynomial $f \in \kappa[X_0, ..., X_n]$ on a point $P \in \mathbb{P}^n = [p_0, ..., p_n]$ since it may happens that $f(cp_0, ..., cp_n) = 0$ and $f(c'p_0, ..., c'p_n) \neq 0$ for $c \neq c'$. The vanishing on a point $P \in \mathbb{P}^n$ is defined only for homogeneous polynomials.

Definition 2.5. *A polynomial $f \in \kappa[X_0, ..., X_d]$ is homogeneous of degree d if all its monomials have degree d. An ideal $I \triangleleft \kappa[X_0, ..., x_n]$ is homogeneous if it is generated by homogeneous polynomials.*

Remark 2.6. *For a polynomial f homogeneous and of degree d, a $(n+1)$-tuple $(x_0, ..., x_n) \in \mathbb{A}^{n+1}$ and $c \in \kappa$, the following relation holds:*

$$f(cx_0, ..., cx_n) = c^d f(x_0, ..., x_n).$$

It follows that the vanishing of f in $[x_0, ..., x_n]$ is well defined.

The projective algebraic sets can now be defined.

Definition 2.7. *A projective algebraic set is any set of the form*

$$V(I) = \{P \in \mathbb{P}^n : f(P) = 0 \quad \textit{for all homogeneous} f \in I\},$$

where $I \lhd \kappa[X]$ is a homogeneous ideal.

The ideal of a projective algebraic set is defined in the similar way.

Definition 2.8. *Let $V \subset \mathbb{P}^n$ be a projective algebraic set. The ideal of V is*

$$I(V) = (\{f \in \kappa[X] : f \textit{ is homogeneous }, f(P) = 0 \ \ \forall P \in V\}).$$

Similar to affine algebraic sets, there exist indecomposable projective algebraic sets.

Definition 2.9. *A projective variety is a projective algebraic set V which can not be written as a non-trivial union of other algebraic sets:*

$$V = V_1 \cup V_2 \Rightarrow V = V_1 \textit{ or } V = V_2.$$

$\mathbb{P}^n$ contains many copies of $\mathbb{A}^n$. The most special ones are so called affine charts. For each $0 \leq i \leq n$ denote by $U_i = \{X_i \neq 0\} \subset \mathbb{P}^n$, then we have a natural identification

$$\begin{array}{c} \mathbb{A}^n_\kappa \xrightarrow{\qquad \phi_i \qquad} U_i \\ (x_1, .., x_n) \longmapsto [x_1, ..., x_{i-1}, 1, x_i, ..., x_n], \end{array}$$

which is a bijection since it has an inverse map

$$\begin{array}{c} U_i \xrightarrow{\qquad \phi_i^{-1} \qquad} \mathbb{A}^n_\kappa \\ [X_0, .., X_n] \longmapsto \left(\frac{X0}{X_i}, ..., \frac{X_{i-1}}{X_i}, \frac{X_{i+1}}{X_i}, ..., \frac{X_n}{X_i} \right). \end{array}$$

Note that the affine charts U_i covers $\mathbb{P}^n$. For any projective algebraic set $V \subset \mathbb{P}^n$, the sets $\phi_i^{-1}(V)$ are affine algebraic sets: they are defined by dehomogenize the polynomials defining $I(V)$ with respect to the variable X_i. If V is a projective variety, then $V \cap U_i$ is an affine variety for $0 \leq i \leq n$.

A simple example of projective varieties are the ones defined by linear equations.

Definition 2.10. *A linear subspace $L \subset \mathbb{P}^n$ is a projective variety defined by homogeneous polynomials of degree 1. The codimension of L, denoted by* $\operatorname{codim}_{\mathbb{P}^n}(L)$*, is the minimum number of generators of $I(L)$. The dimension of L is the quantity* $\dim(L) = n - \operatorname{codim}_{\mathbb{P}^n}(L)$.

Other easy examples of projective algebraic sets are the varieties cut by one equation.

Definition 2.11. *An hypersurface is a projective algebraic set $V \subset \mathbb{P}^n$ defined by a single equation $F(X_0, ..., X_n) = 0$.*

Remark 2.12. *Note that an hypersurface is a projective variety if F has only one prime factor.*

To any projective algebraic set (not just to linear subspaces), the notion of dimension is associated. Here we present a definition which is the most intuitive and less technical, though not so commonly used in the literature. We assume that κ is algebraically closed.

Definition 2.13. *Let $V \subset \mathbb{P}^n$ be a projective algebraic set. Let d be the maximum dimension of a linear subspace $L \subset \mathbb{P}^n$ such that $L \cap V = \emptyset$. Then codimension of V in $\mathbb{P}^n$ is the quantity*

$$\operatorname{codim}_{\mathbb{P}^n}(V) = d + 1.$$

The dimension of V is the quantity

$$\dim(V) = n - \operatorname{codim}_{\mathbb{P}^n}(V).$$

Remark 2.14. *Note that the codimension of a hypersurface is 1, as one could expect.*

2.3 Maps between varieties

In this subsection, we discuss about algebraic maps between varieties.

Definition 2.15. *Let $Y_1 \subset \mathbb{P}^m$, $Y_2 \subset \mathbb{P}^n$ be two projective varieties. A rational map from Y_1 to Y_2 is a map of the form*

$$\begin{array}{ccc} Y_1 & \xrightarrow{\quad\phi\quad} & Y_2 \\ [X_0, ..., X_m] & \longmapsto & [F_0(X), ..., F_n(X)], \end{array}$$

where $F_0, ..., F_n \in \kappa[X] = \kappa[X_0, ..., X_n]$ are homogeneous polynomials of the same degree, satisfying the property that $[F_0(P), ..., F_n(P)] \in Y_2$ for any $P \in Y_1$ such that $F_0(P), ..., F_n(P)$ are not simultaneously 0.

In general rational maps have different representative sequence of polynomials.

Definition 2.16. *Two sequences of polynomials $(F_0, ..., F_n)$ and $(G_0, ..., G_n)$ represent the same rational map*

$$Y \to \mathbb{P}^n$$

if $[F_0(P), ..., F_n(P)] = [G_0(P), ..., G_n(P)]$ for all $P \in Y$ such that both the two sequences do not vanish on P.

A morphism is a rational map defined at every point.

Definition 2.17. *A rational map $\phi : Y \to \mathbb{P}^n$ is regular in P if there exists a representing sequence of polynomials $(F_0, ..., F_n)$ such that*

$$(F_0(P), ..., F_n(P)) \neq (0, ..., 0).$$

ϕ is a morphism if it is regular at every point of Y.

Definition 2.18. *A birational map between projective varieties Y_1 and Y_2 is a map*

$$\phi : Y_1 \to Y_2,$$

for which there exist another rational map

$$\psi : Y_2 \to Y_1$$

such that $\psi \circ \phi = \mathrm{id}_{Y_1}$ and $\phi \circ \psi = \mathrm{id}_{Y_2}$. ϕ is an isomorphism if both ϕ and ψ are morphisms.

2.4 Grassmannian

$\mathbb{P}^n$ paramatrizes the lines through the origin contained in $\mathbb{A}^{n+1}$. Equivalently, it parametrizes the 1-dimensional subspaces of a κ-vector space V of dimension $n + 1$. The Grassmannian is an immediate generalization of this concept.

Definition 2.19. *Let V be a n dimensional vector space over κ. For $1 \leq d \leq n$, the Grassmannian of d-subspaces of V is the set*

$$G(d, V) = \{W \leq V : \dim(W) = d\}.$$

When $V = \kappa^n$, this is denoted by $G(d, n)$.

Recall, from basic linear algebra, that two ordered set of linearly independent vectors of V, $\mathcal{B} = \begin{pmatrix} \vec{v}_1 \\ \vdots \\ \vec{v}_d \end{pmatrix}$ and $\mathcal{B}' = \begin{pmatrix} \vec{w}_1 \\ \vdots \\ \vec{w}_d \end{pmatrix}$, generate the same subspace $W \subset V$ if and only there is an invertible matrix $M \in \mathrm{GL}(d)$ such that

$$\mathcal{B}' = M \cdot \mathcal{B}.$$

It follows that, like the projective space, the Grassmannian can be identified as a quotient by an equivalence relation.

Proposition 2.20. *Let $\mathcal{G}(d, n)$ be the set of $d \times n$ matrices A of rank d modulo the equivalence relation*

$$A \sim A' \iff \exists M \in \mathrm{GL}(d) : A = MA'.$$

Then there is a bijection

$$\mathcal{G}(d, n) \leftrightarrow G(d, n),$$

which maps the class of a matrix A to the vector space spanned by the rows of A.

From now on we will not distinguish between $\mathcal{G}(d, n)$ and $G(d, n)$. Similar to the case of the projective space, affine charts are also defined for the Grassmannian. Let S any subset of $\{1, ..., n\}$ such that $\#S = d$ and denote by $U_S \subset G(d, n)$ the subset of matrices for which the minor $d \times d$ corresponding to S is non-zero. Note that $G(d, n)$ is covered by these subsets U_S. Furthermore any $[M] \in U_S$ admits a unique representative for which the $d \times d$ sub-matrix corresponding to S is the identity matrix: in fact if M_S is such a sub-matrix, then we have just to consider $M_S^{-1} M$ as a representative. It follows that U_S is identified with $\mathbb{A}^{d(n-d)}$.

Example 2.21. *Suppose that $S = \{1, ..., d\}$, then, denoting by* HJ *the operator of horizontal joint of two matrices (having the same number of rows), we have the following characterization*

$$U_S = \{\mathrm{HJ}(I_d, B) : B \in \mathrm{Mat}_{d \times (n-d)}(\kappa)\}.$$

We want now to characterize $G(d,n)$ as a projective variety, i.e. as an object defined by polynomial equations in a projective space. The first aim is to find the projective space on which it lies. Recall first the notion of exterior power of a vector space.

Definition 2.22. *Let V be an n-dimensional κ-vector space, $0 < d \leq n$. Then the d-th exterior power of V, denoted by $\bigwedge^d V$, is the vector space spanned by the tensors of the form $v_1 \wedge v_2 \cdots \wedge v_d$, where $\wedge$ satisfies the following properties:*

- *it is d-linear:*

$$a \cdot (v_1 \wedge ... \wedge v_d) = (av_1) \wedge v_2 ... \wedge v_d = ... = v_1 \wedge ... \wedge v_{d-1} \wedge (av_d),$$

$$v_1 \wedge ... \wedge (v_i + v_i') \wedge ... \wedge v_d = v_1 \wedge ... \wedge v_i \wedge ... \wedge v_d + v_1 \wedge ... \wedge v_i' \wedge ... \wedge v_d;$$

- *it is antisymmetric:*

$$v_{\sigma(1)} \wedge ... \wedge v_{\sigma(d)} = (-1)^{\mathrm{sgn}(\sigma)} v_1 \wedge ... \wedge v_d,$$

for any $\sigma \in \mathcal{S}_d$, where $\mathcal{S}_d$ denotes the d-th symmetric group.

Remark 2.23. *Note that the antisymmetric condition implies, for characteristic > 2, that*

$$\dim(\mathrm{Span}(v_1, ..., v_d)) < d \Rightarrow v_1 \wedge ... \wedge v_d = 0. \tag{1}$$

In characteristic 2, when there is no distinction between symmetry and antisymmetry, it is possible to define the "antisymmetric" property by requiring the symmetric one and the condition 1.

Fix a basis $\{e_1, \ldots, e_n\}$ of the vector space V, the set

$$\{e_{i_1} \wedge \cdots \wedge e_{i_d} : 1 \leq i_1 < \ldots \leq i_d \leq n\} \tag{2}$$

forms a basis for $\bigwedge^d(V)$, whose dimension is then $\binom{n}{d}$.

Lemma 2.24. *Let W be a d-dimensional subspace of a n-dimensional vector space V over κ. Let $\mathcal{U} = \begin{bmatrix} u_1 \\ \vdots \\ u_d \end{bmatrix}$ and $\mathcal{W} = \begin{bmatrix} w_1 \\ \vdots \\ w_d \end{bmatrix}$ be two bases of W and M be a $d \times d$ invertible matrix such that*

$$\mathcal{U} = M\mathcal{W}.$$

Then

$$u_1 \wedge \cdots \wedge u_d = \det(M) \cdot w_1 \wedge \cdots \wedge w_d.$$

This lemma shows that whatever the bases we choose for W, the corresponding wedge product is uniquely determined up to a scalar multiplication. Therefore, the following map

$$\iota : G(d, V) \to \mathbb{P}(\bigwedge^d V)$$

given by $W \mapsto [v_1 \wedge \cdots \wedge v_d]$, where $\{v_1, \dots v_d\}$ is a basis of $W \in G(d, V)$, is well defined.

Proposition 2.25. *The map $\iota : G(d, V) \to \mathbb{P}(\bigwedge^d V)$ defined above is an isomorphism onto the image, called Plücker embedding.*

By the proposition 2.25, the Grassmannian $G(d, V)$ can be seen a subset of a projective space.

Fix a basis $\{e_1, ..., e_n\}$ of V and consider on $\bigwedge^d V$ the basis in 2. Then, in coordinates, the Plücker embedding maps $[M]$ to the sequence of its minors of rank d.

The image $\iota(G(d, V))$ is a projective variety defined by a set of quadratic equations.

Theorem 2.26. *The image of the Plücker embedding $\iota(G(d, V)) \subset \mathbb{P}(\bigwedge^d(V))$ is a projective variety defined by quadratic equations, called Plücker relations. Call $\{X_{i_1,...,i_d}\}_{1 \le i_1 < ... < i_d \le n}$ the coordinates of $\mathbb{P}(\bigwedge^2 V)$, then for any couple of ordered sequences*

$$1 \le i_1 < i_2 < ... < i_{d-1} \le n, \;\; 1 \le j_1 < j_2 < ... < j_{d+1} \le n$$

the following equations hold:

$$\sum_{l=1}^{d+1} X_{i_1,...,i_{d-1},j_l} X_{j_1,...,\hat{j_l},...,j_{d+1}} = 0$$

where $j_1, ..., \hat{j_l}, ..., j_{d+1}$ is the sequence obtained by discarding j_l by the sequence $j_1, ..., j_{d+1}$.

2.5 Grassmannian of planes and its secant variety.

In this section we focus the attention on the case $d = 2$. This case is interesting since both the Grassmannian and its secant variety are defined by sparse equations.

Definition 2.27. *Let $X \subset \mathbb{P}^n$ be a projective variety. The secant variety of X, denoted by $\mathrm{Sec}(X)$ is the smallest projective variety containing the locus*

$$\bigcup_{P,Q \in X} l_{P,Q},$$

where $l_{P,Q}$ denotes the line joining P and Q.

The definition implies that $\mathrm{Sec}(X)$ contains elements of the form $[ax_1 + b_2]$, where $x_1, x_2 \in \mathbb{A}^{n+1}$ are such that $[x_1], [x_2] \in X$, $a, b \in \kappa$. When $X = G(d, n)$, $\mathrm{Sec}(X)$ parametrizes the tensors which can be written as sum of two indecomposable tensors.

Definition 2.28. *Let A be an antisymmetric matrix, then the square root of its determinant i.e. $\sqrt{\det(A)}$ is called the Pfaffian of A.*

Observe that there exists a correspondence between elements of $\bigwedge^2 V$ and $n \times n$ antisymmetric matrices: for any $t \in \bigwedge^2 V$, write $t = \sum_{1 \le i < j \le n} t_{ij} e_i \wedge e_j$. Then the corresponding $n \times n$ antisymmetric matrix is $M_t = (m_{ij})$, where

$$m_{ij} = \begin{cases} t_{ij} \text{ if } i < j \\ 0 \text{ if } i = j \\ -t_{ij} \text{ if } i > j. \end{cases}$$

The rank of the matrix M_t is strictly related to the minimum number of simple tensors in which t can be decomposed.

Proposition 2.29. *Let $t \in \bigwedge^2 V$ and M_t be its associated antisymmetric matrix. Then*

$$\mathrm{rank}(M_t) = 2n_t,$$

where n_t is the minimum number of simple tensors in which t can be decomposed.

Remark 2.30. *An antisymmetric matrix can have only an even rank. For antisymmetric matrices there is an alternative criteria for detecting its rank.*

Definition 2.31. *Let $A = (a_{ij})$ be an $n \times n$ matrix, let $B = (b)_{ij}$ be a sub-matrix $m \times m$ of A. B is centred at the diagonal if there exist a sequence $1 \le s_1 < ... < s_m \le n$ such that*

$$b_{ij} = a_{s_i, s_j}.$$

A minor of A is called centred at the diagonal if it is the determinant of a sub-matrix of A centred at the diagonal.

Remark 2.32. *If A is (anti)symmetric, then so is any sub-matrix centred at the diagonal.*

Proposition 2.33. *Let M be an antisymmetric matrix. Then* $\operatorname{rank}(M) \leq r-2$ *if and only if all the $r \times r$ minors that are centered at the diagonal vanish.*

There is an immediate consequence for the description of $G(2,n)$ and $\operatorname{Sec}(G(2,n))$.

Corollary 2.34. *Let $[t] \in \mathbb{P}(\bigwedge^2 V)$. Then:*

- *$t \in G(2,V)$ if and only if* $\operatorname{rank}(M_t) = 2$ *if and only the Pfaffians of the 4×4 centered at the diagonal sub-matrices vanish;*
- *$t \in \operatorname{Sec}(G(2,V))$ if and only if* $\operatorname{rank}(M_t) \leq 4$ *if and only the Pfaffians of the 6×6 centered at the diagonal sub-matrices vanish.*

In particular $\operatorname{Sec}(G(2,V))$ is defined by $\binom{n}{6}$ cubic polynomials, which are quite spars. For example,

$$\operatorname{pf}\begin{pmatrix} 0 & X_0 & X_1 & X_2 & X_3 & X_4 \\ -X_0 & 0 & X_5 & X_6 & X_7 & X_8 \\ -X_1 & -X_5 & 0 & X_9 & X_{10} & X_{11} \\ -X_2 & -X_6 & -X_9 & 0 & X_{12} & X_{13} \\ -X_3 & -X_7 & -X_{10} & -X_{12} & 0 & X_{14} \\ -X_4 & -X_8 & -X_{11} & -X_{13} & -X_{14} & 0 \end{pmatrix}$$

is a polynomial with 15 non zero monomials. So one expects that if we shift $\operatorname{Sec}(G(2,n))$ with a sparse automorphism of $\mathbb{P}^n$ then we will have a variety defined by sparse cubic equations.

The dimension of $\operatorname{Sec}(G(2,n))$ is known.

Proposition 2.35. *Let $d = G(2,n)$ be the dimension of $G(2,n)$ (so $d = 2(n-2)$), then* $\dim(\operatorname{Sec}(G(2,n))) = 2d-3$.

2.6 Points in linear sections of the Grassmannian

A better approach for generating random points inside a linear section of $G(d,n)$ is not by using Gröbner bases, but by using the affine charts and the Plucker embedding. If we fix a subset $S \subset \{1,...,n\}$ of cardinality d, then the Plücker map restricts to an embedding

$$\mathbb{A}^{d(n-d)} \to \mathbb{P}^{\binom{n}{d}-1}.$$

Let $L \subset \mathbb{P}^{\binom{n}{d}-1}$ be a linear subspace of codimension $n-d$. Then it is possible to find points inside $L \cap G(2,n)$ by just using linear algebra. To illustrate the procedure we consider the case in which $S = \{1,...,d\}$. Suppose

that

$$L = \begin{cases} L_1(X) = 0 \\ \vdots \\ L_{n-d}(X) = 0 \end{cases}$$

then we can choose a vector of unknowns

$$\vec{x} = (1, 0, ..., 0, x_{d+1}, ..., x_n)$$

and $d-1$ random vectors of κ^n

$$\begin{aligned} \vec{a}_1 =& (0, 1, ..., 0, a_{1,d+1}, ..., a_{1,n}) \\ & \vdots \\ \vec{a}_{d-1} =& (0, ..., 0, 1, a_{d-1,d+1}, ..., a_{d-1,n}) \end{aligned}$$

and solve the linear system in $x_{d+1}, ..., x_n$:

$$\begin{cases} L_1(\vec{x} \wedge \vec{a}_1 \wedge \cdots \wedge \vec{a}_{d-1}) = 0 \\ \vdots \\ L_{n-d}(\vec{x} \wedge \vec{a}_1 \wedge \cdots \wedge \vec{a}_{d-1}) = 0. \end{cases}$$

In general this system has a unique solution $\vec{x}_0$, then

$$P = [\vec{x}_0 \wedge \vec{a}_1 \wedge \cdots \wedge \vec{a}_{d-1}]$$

is a point of $G(d, n) \cap L$.

3 New signature scheme

In this section we present a signature scheme, which consists of three parts: key generation, signing and verification. We propose a signature scheme using $\mathrm{Sec}(G(2, n))$, but it can be easily adapted to $G(d, n)$ as well. We use a vector space V of dimension n over a finite field $\kappa = \mathbb{F}_{2^\ell}$ of characteristic 2 then V is identified with κ^n.

3.1 Key generation

The private key consists of a random automorphism ϕ of $V = \kappa^n$, which is sparse and defined over $\mathbb{F}_2$. The public key is a set of cubic equations vanishing on $\phi(\mathrm{Sec}(G(2, n)))$.

Private key generation:

1) Alice chooses a random upper triangular, invertible and sparse $\binom{n}{2} \times \binom{n}{2}$ matrix M'_A.
2) Alice chooses two random $\binom{n}{2} \times \binom{n}{2}$ permutation matrices A_1, A_2;
3) Alice defines $M_A = A_1 M'_A A_2$ and then the private key is

$$K_A^{\text{pri}} = (M_A, M_A^{-1}).$$

If a polynomial $F(X)$, where $X = \begin{pmatrix} X_0 \\ \vdots \\ X_n \end{pmatrix}$, vanishes on a variety $Y \subset \mathbb{P}^n$ and M is an invertible $(n+1) \times (n+1)$ matrix, then $F(M^{-1}X)$ vanishes on MY. This observations makes easy to generate the public key.
Public key generation:

1) Alice chooses a random subset $\{F_1(X), ..., F_m(X)\}$ of the set of $\binom{n}{6}$ Pfaffians defining $\text{Sec}(G(2,n))$.
2) She computes $G_i(X) = F_i(M_A X)$ for i in $\{1, ..., m\}$ and set

$$K_A^{\text{pub}} = \{G_1(X), ..., G_m(X)\}$$

denoting the public key. Note that G_i vanishes on $M_A^{-1}\,\text{Sec}(G(2,n))$ for $i \in \{1, ..., m\}$.

3.2 Signature generation an verification

The document D is assumed to be a linear subspace of $\mathbb{P}^{\binom{n}{2}-1}$ cut by $n-2$ linear equations $\{L_1 = 0, ..., L_{n-2} = 0\}$ defined over $\mathbb{F}_2$.

1) Alice choose a random vector $\vec{a} \in \kappa^n$ of the form $\vec{a} = (0, 1, a_3, ..., a_n)$ and a vector of unknowns $\vec{x} = (1, 0, x_3, ..., x_n)$;
2) Alice computes

$$L'_1(X) = L_1(M_A^{-1}X), ..., L'_{n-2}(X) = L_{n-2}(M_A^{-1}X)$$

and imposes the condition

$$L'_i(\vec{x} \wedge \vec{a}) = 0, \quad \forall i \in \{1, ..., n-2\}.$$

Here $\vec{x} \wedge \vec{a}$ is identified with its coordinates with respect to the basis $\{e_i \wedge e_j : 1 \leq i < j \leq n\}$. It is a linear system in $\{x_3, ..., x_n\}$ which has, in general, a unique solution $(b_3, ..., b_n) \in \kappa^{n-2}$;

3) Let $\vec{b} = (1, 0, b_3, ..., b_n)$, then $P = [M_A^{-1}(\vec{a} \wedge \vec{b})] \in D \cap (M_A^{-1}G(2, n))$. So the point P satisfies the system of equations:

$$\begin{cases} G_1(X) = 0 \\ \quad \vdots \\ G_m(X) = 0 \\ L_1(X) = 0 \\ \quad \vdots \\ L_{n-2}(X) = 0 \end{cases}$$

and $P \in G(2, n) \cap D$.

4) Alice repeats the procedure in $1) - 3)$ and finds another point $Q \in (M_A^{-1}G(2, n)) \cap D$;

5) Alice chooses two random vectors of $\vec{v}_P, \vec{v}_Q \in \kappa^{\binom{n}{2}}$ such that $[v_P] = P, [v_Q] = Q$ and defines $S_A = [v_P + v_Q] \in D \cap (M_A^{-1}\,\mathrm{Sec(G(2,n))})$ to be the signature of D.

If Bob wants to verify the validity of a signature, he has to verify that $G_i(S_A) = 0$ for $i \in \{1, ..., m\}$, $L_i(S_A) = 0$ for $i \in \{1, ..., n-2\}$.

3.3 A toy example

Here we give a toy example with $n = 6, \kappa = \mathbb{F}_2$. The ambient space of $G(2, 6)$ is $\mathbb{P}^{14}$, $\mathrm{Sec}(G(2, 6))$ is a degree 3 hypersurface defined by the equation

$$\begin{aligned} &X_4X_7X_9 + X_3X_8X_9 + X_4X_6X_{10} + X_2X_8X_{10} + X_3X_6X_{11} + \\ &X_2X_7X_{11} + X_4X_5X_{12} + X_1X_8X_{12} + X_0X_{11}X_{12} + X_3X_5X_{13} + \\ &X_1X_7X_{13} + X_0X_{10}X_{13} + X_2X_5X_{14} + X_1X_6X_{14} + X_0X_9X_{14} = 0 \end{aligned} \tag{3}$$

The private key is given by the two matrices:

$$M_A = \begin{bmatrix} 0&0&0&0&0&0&0&0&1&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&0&0 \\ 1&0&0&0&0&0&1&1&0&0&0&1&0&0&0 \\ 0&0&0&0&0&0&0&0&1&0&0&0&1&0&0 \\ 0&1&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&0&0&0&0&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&1&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&0&0&0&0&1&1&0&1&0&0 \\ 0&0&0&0&0&1&0&0&1&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&1&0&0&0&0&0&0&0&0 \\ 1&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 1&0&0&0&0&0&0&0&0&1&0&0&0&0&1 \end{bmatrix}$$

and

$$M_A^{-1} = \begin{bmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&1&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&1&0&1&0&0&0&0&1&0&1&0&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&1&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&1&1\\
0&1&0&0&0&0&0&0&1&1&0&0&0&1&1\\
0&0&1&0&0&0&0&1&0&0&0&0&1&1&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0
\end{bmatrix}.$$

The transformation of coordinates $X \mapsto M_A X$ gives K_A^{pub}, which in this example is the single equation

$$\begin{aligned}
&X_0^2X_4 + X_1X_2X_5 + X_2^2X_5 + X_0X_4X_6 + X_1X_4X_6 +\\
&X_2X_4X_6 + X_0X_3X_7 + X_0X_4X_7 + X_3X_6X_7 + X_3X_7^2 +\\
&X_1X_2X_8 + X_2^2X_8 + X_2X_3X_8 + X_0X_4X_8 + X_0X_5X_8 +\\
&X_3X_6X_8 + X_0X_8^2 + X_1X_2X_9 + X_2^2X_9 + X_0X_4X_9 +\\
&X_4X_6X_9 + X_1X_7X_9 + X_2X_7X_9 + X_4X_7X_9 + X_8X_9^2 +\\
&X_1X_7X_{10} + X_2X_7X_{10} + X_0X_8X_{10} + X_8X_9X_{10} + X_0X_4X_{11} +\\
&X_3X_7X_{11} + X_4X_9X_{11} + X_0X_2X_{12} + X_2X_3X_{12} + X_0X_4X_{12} +\\
&X_0X_7X_{12} + X_1X_7X_{12} + X_2X_7X_{12} + X_0X_8X_{12} + X_2X_9X_{12} +\\
&X_8X_9X_{12} + X_0X_5X_{13} + X_3X_6X_{13} + X_0X_8X_{13} + X_9^2X_{13} +\\
&X_0X_{10}X_{13} + X_9X_{10}X_{13} + X_0X_{12}X_{13} + X_9X_{12}X_{13} + X_0X_4X_{14} +\\
&X_0X_5X_{14} + X_4X_6X_{14} + X_5X_6X_{14} + X_4X_7X_{14} + X_5X_7X_{14} +\\
&X_0X_8X_{14} + X_6X_8X_{14} + X_7X_8X_{14} + X_0X_9X_{14} + X_6X_9X_{14} +\\
&X_7X_9X_{14} + X_4X_{11}X_{14} + X_5X_{11}X_{14} + X_8X_{11}X_{14} + X_9X_{11}X_{14} +\\
&X_2X_{12}X_{14} + X_6X_{12}X_{14} + X_9X_{12}X_{14} + X_{10}X_{12}X_{14} + X_{12}^2X_{14} +\\
&X_9X_{13}X_{14} + X_{10}X_{13}X_{14} + X_{12}X_{13}X_{14} = 0.
\end{aligned} \tag{4}$$

Suppose that Alice wants to sign a document D, corresponding to the system of linear equations:

$$\begin{cases}
L_1 = X_0 + X_2 + X_3 + X_4 + X_5 + X_7 + X_{10} + X_{11} + X_{12} &= 0\\
L_2 = X_2 + X_4 + X_6 + X_{13} + X_{14} &= 0\\
L_3 = X_3 + X_4 + X_{10} + X_{11} + X_{13} + X_{14} &= 0\\
L_4 = X_1 + X_2 + X_3 + X_4 + X_5 + X_6 + X_9 + X_{12} + X_{13} + X_{14} &= 0.
\end{cases}$$

Alice shifts the document D through the matrix M_A^{-1}, by computing $L_i'(X) = L_i(M_A^{-1}X)$. She obtains the system

$$D_A : \begin{cases} X_1 + X_4 + x_6 + X_9 + X_{10} + x_{12} + X_{13} & = 0 \\ X_0 + X_1 + X_3 + X_5 + X_6 + X_7 + X_8 + X_9 + X_{10} + X_{14} & = 0 \\ X_0 + X_2 + X_3 + X_4 + X_5 + X_6 + X_7 + X_8 + X_9 + X_{13} + X_{14} & = 0 \\ X_1 + X_2 + X_3 + X_4 + X_5 + X_6 & = 0. \end{cases}$$

Alice chooses a vector of unknowns $\vec{x} = (1, 0, x_3, x_4, x_5, x_6)$ and two random vectors $\vec{a}_1 = (0, 1, 1, 1, 1, 1), \vec{a}_2 = (0, 1, 1, 0, 0, 1)$. The condition that $\vec{x} \wedge \vec{a}_1 \in D_A$ corresponds to the linear system

$$\begin{cases} x_6 & = 0 \\ x_3 + x_5 + 1 & = 0 \\ x_4 + x_6 & = 0 \\ x_3 + x_4 & = 0 \end{cases}$$

whose solution is $(0, 0, -1, 0)$. Call $x_1 = (1, 0, 0, 0, -1, 0), P_1 = [x_1 \wedge a_1]$. Similarly, the condition that $\vec{x} \wedge \vec{a}_2 \in D_A$ corresponds to the linear system

$$\begin{cases} x_4 + x_5 & = 0 \\ x_3 + x_5 + x_6 & = 0 \\ x_3 + x_4 + x_5 & = 0 \\ x_3 + x_4 & = 0 \end{cases}$$

whose solution is $(0, 0, 0, 0)$. Call $x_2 = (1, 0, 0, 0, 0, 0), P_2 = [x_2 \wedge a_2]$. Then

$$P_1 = [1, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1],$$

$$P_2 = [1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0].$$

$P_1, P_2 \in G(2, 6) \cap D_A$. Call $P = [x_1 \wedge a_1 + x_2 \wedge a_2]$, then

$$P = [0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1]$$

is a point of $\mathrm{Sec}(G(2, 6)) \cap D_A$. It follows that

$$S_A = M_A^{-1} \cdot P = [0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0]$$

is a point of $M_A^{-1}\,\mathrm{Sec}(G(2, 6)) \cap D$. Therefore, in particular, it satisfies the equation 4 and $L_i(S_A) = 0$ for $i \in \{1, 2, 3, 4\}$.

4 Security analysis

Suppose that Frank wants to forge a signature of Alice for a document $D = \{L_1, ..., L_{n-2}\}$. In general, finding a solution of the system

$$\begin{cases} G_i = 0 \text{ for } i \in \{1, ..., m\} \\ L_i = 0 \text{ for } i \in \{1, ..., n-2\} \end{cases}$$

is an NP-hard problem. Nevertheless, if Alice produces around $\binom{n}{6}$ signatures, Frank is able to compute a basis of the vector space of cubic equations vanishing on $M_A^{-1}\,\mathrm{Sec}(G(2,n))$. This fact allows Frank to use two possible approaches:

1) Trying to reconstruct the matrix M_A;

2) Using a Gröbner basis approach, having a full set of equations defining $\mathrm{Sec}(G(2,n))$ makes the computations easier. The complexity of the Gröbner basis computation is related to the CM-regularity of the variety.

We study the complexity of the second approach: in general it is possible to give just a very rough upper bound of it, so it is preferable an empirical analysis.

Note that κ has to be greater than $\mathbb{F}_2$. In fact, if we have a valid signature P defined over κ for a document D, then the probability that it is a valid signature also for another document D' is $\frac{1}{(\#\kappa)^{n-2}}$. So signatures defined over a smaller field must be considered invalid.

5 Estimated key sizes

5.1 Private key size

The private key consists of the two matrices M_A and M_A^{-1}, which are, by construction, sparse binary matrices with around $2n$ components equal to 1. So they require a storage of around $4n$ bits.

5.2 Public key size

The public key is given by a set of m equations of the form

$$\{F_i(M_A X) : i \in \{1, ..., m\}\},$$

where $\{F_1, ..., F_m\}$ is a subset of the $\binom{n}{6}$ Pfaffian cubic polynomials defining $\mathrm{Sec}(G(2, n))$. The Pfaffians have 15 non-zero terms, which are square-free. The number of non-zero terms of the shifted Pfaffians is in general variable. Since the matrix M_A is sparse, we expect that they are also sparse. In the particular case when all the rows of M_A have exactly two components equal to 1, each shifted Pfaffian has a number of non-zero terms which is less than or equal to $120 = 15 \cdot 2^3$. Therefore, it is expected that the size of the public key is around $120m$ bits.

5.3 Document size

If $\kappa = \mathbb{F}_{2^\ell}$ then the size of the document, which is a set of $n-2$ hyperplanes of $\mathbb{P}^{\binom{n}{2}-1}$, is $\binom{n}{2} \cdot (n-2)$ bits.

5.4 Signature size

The signature is a point of $\mathbb{P}^{\binom{n}{2}-1}$ defined over κ, so it depends on $\ell \cdot \left(\binom{n}{2} - 1\right)$ bits.

References

[1] ABDELKERIM R. J: PhD thesis on Geometry of the Dual Grassmannian. University of Illinois at Chicago, 2011.

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

[3] 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)

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

[5] 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)

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

[7] Ding J., Schmidt D.: Rainbow, a new multivariate polynomial signature scheme. In Ioannidis, J., Keromytis, A.D., Yung, M. (eds.) ACNS 2005. LNCS vol. 3531, pp. 164175 Springer, Heidelberg(2005).

[8] Di Tullio D. and Gyawali M. *IACR Cryptology ePrint Archive*, 2020 `https://eprint.iacr.org/2020/628.pdf`

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

[10] Kohel D., Lauter K., Petit C., Tignol J. P. *On the quaternion l-isogeny path problem*, *LMS Journal of Computation and Mathematics*, 17A(2014), 418-432.

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

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

[13] 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)

[14] The National Institute of Standards and Technology (NIST), PQC Standardization Process: Third Round Candidate Announcement 2020. `https://csrc.nist.gov/News/2020/pqc-third-round-candidate-announcement`

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

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

A Magma code

A.1 Code for signature scheme

Here we present a MAGMA code which simulates the signature scheme proposed above. Note that the computation of the equations of the standard secant variety takes a bit long, but this is not a problem since they are known and they don't need to be computed everytime.

```
Plucker:=function(v,w)
        n:=#v;
        N:=Binomial(n,2);
        F:=Parent(v[1]);
        y:=[F!0: i in [1..N]];
        m:=1;
        for i in [1..n-1] do
                for j in [i+1..n] do
                        y[m]:=v[i]*w[j]-v[j]*w[i];
                        m:=m+1;
                end for;
        end for;
        return(y);
end function;

RandomPermutation:=function(S)
        n:=#S;
        v:=[v: v in S];
        S0:=S;
        for i in [1..n] do
                v[i]:=Random(S0);
                S0:=S0 diff {v[i]};
        end for;
        return(v);
end function;

RandomLinearForm:=function(R)
        F:=BaseRing(R);
        mon:=MonomialsOfDegree(R,1);
        f:=R!0;
        for i in [1..#mon] do
                f:=f+Random(F)*mon[i];
        end for;
        return(f);
end function;
```

```
/* *******Function generating a nxn matrix with around 2n
components equal to 1 and the remaining equal to 0 *** */
RandomSparseMatrix:=function(F,n)
        N:=Binomial(n,2);
        v:=[F!0: i in [1..N]];
        m:=Floor(N/n);
        for i in [1..N] do
                r:=Random(0,m-1);
                if r eq 0 then
                        v[i]:=1;
                end if;
        end for;
        M:=UpperTriangularMatrix(v);
        M:=HorizontalJoin(ZeroMatrix(F,n-1,1),M);
        M:=VerticalJoin(M,ZeroMatrix(F,1,n));
        M:=M+IdentityMatrix(F,n); //Random Sparse upper triangular matrix
        S:={s: s in [1..n]};
        A:=PermutationMatrix(F,RandomPermutation(S));
        B:=PermutationMatrix(F,RandomPermutation(S));
        M:=A*M*B;
        return(M);
end function;

F:=GF(2);
K:=GF(2^13);
n:=12;
d:=2*(n-2);
N:=Binomial(n,2);
R:=PolynomialRing(K,N,"grevlex");
Ad:=AffineSpace(K,n-2);
Rd:=CoordinateRing(Ad);

/* Equations defining the Sec(G(2,n)) */
M:=UpperTriangularMatrix(R,[R.i: i in [1..N]]);
M:=HorizontalJoin(ZeroMatrix(R,n-1,1),M);
M:=VerticalJoin(M,ZeroMatrix(R,1,n));
M:=M-Transpose(M);
S:=[1..n];
S:={s: s in S};
S:=Subsets(S,6);
eqSec:={};
for s in S do
        t:=[i:i in s];
```

```
        pf:=Pfaffian(Submatrix(M,t,t));
        eqSec:=eqSec join {pf};
end for;

/* *****The document***** */
Rtemp:=PolynomialRing(F,N);
D:={R!RandomLinearForm(Rtemp): i in [1..n-2]};

/* ***Alice private key*** */
MA:=RandomSparseMatrix(F,N);
MAinv:=MA^(-1);
MA:=ChangeRing(MA,R); //Private key
MAinv:=ChangeRing(MAinv,R); //Private key

/* ***Alice public key*** */
m:=20;
KA:=RandomSubset(eqSec,m);
X:=[R.i: i in [1..N]];
X:=Matrix(R,N,1,X);
MAX:=Eltseq(MA*X);
KA:={ Evaluate(f,MAX) : f in KA }; //Public key

/* ***Signing*** */
MAinvX:=Eltseq(MAinv*X);
time DA:={Evaluate(f,MAinvX) : f in D};
a:=[Rd!0: i in [1..n]];
a[1]:=1;
SA:=[[K!0: i in [1..N]]: j in [1,2]];
for i in [3..n] do
        a[i]:=Rd.(i-2);
end for;
for j in [1,2] do //Generating two points in D cap K_A^pub
        b:=[Random(K): i in [1..n]];
        b[1]:=0; b[2]:=1;
        y:=Plucker(a,b);
        YA:=[Rd!Evaluate(f,y): f in DA];
        YA:=Scheme(Ad,YA);
        YA:=Points(YA)[1];
        YA:=Eltseq(YA);
        SA[j]:=[Evaluate(y[i],YA): i in [1..N]];
end for;
r:=[Random(K): i in [1,2]];
SA:=[r[1]*SA[1][j]+r[2]*SA[2][j]: j in [1..N]]; //Random linear combination of
```

```
                                                    the two points
MAinv:=ChangeRing(MAinv,K);
SA:=Eltseq(MAinv*Matrix(K,N,1,SA)); //Digital signature

/* ***Verification*** */
{Evaluate(f,SA): f in D}; //It is the set {0}
{Evaluate(f,SA): f in KA}; // It is the set {0}
```

A.2 Code for Gröbner basis computation

$M_A^{-1}\,\mathrm{Sec}(G(2,n))$ has dimension $2d-3$, where $d = 2(n-2) = \dim(G(2,n))$. So, if we want to find points on $(M_A^{-1}\,\mathrm{Sec}(G(2,n))) \cap D$, where D is a codimension $n-2$ linear subspace of $\mathbb{P}^{\binom{n}{2}-1}$, in general, we need to intersect with other $2d-3-(n-2) = 2d-n-1$ hyperplanes. In the code below we will consider hyperplanes of the form $X_i = c_i X_{i_0}$, where $c_i \in \kappa$. If we dehomogenize with respect to the variable X_{i_0} (i.e. we set $X_{i_0} = 1$), it is equivalent to put $2d-n$ conditions of the form $X_i = c_i$. The code below is a prosecution of the one in A.1. We assume that the forger Frank knows a basis of the vector space of cubic forms vanishing on $M_A^{-1}\,\mathrm{Sec}(G(2,n))$.

```
eqSec := { Evaluate(f, Eltseq(MAX) ): f in eqSec }; // Polynomials defining MA^(-1)*Sec
H:={i: i in [1..N]};
H:=RandomSubset(H,2*d-n);
H:={R.h-Random(K): h in H}; //Choice of 2d-n-1 hyperplanes and dehomogenization
H:=H join (eqSec join D);
I := ideal<R|H>;
time G := GroebnerBasis(I);
```