

Generalizing Syndrome Decoding problem to the totally Non-negative Grassmannian

Kelechi Chuwkunonyerem Emerole*, Said Boussakta*

*†

* †

Abstract—The syndrome decoding problem has been proposed as a computational hardness assumption for code based cryptosystem that are safe against quantum computing. The problem has been reduced to finding the codeword with the smallest non-zero columns that would satisfy a linear check equation. Variants of Information set decoding algorithms has been developed as cryptanalytic tools to solve the problem. In this paper, we study and generalize the solution to codes associated with the totally non-negative Grassmannian in the Grassmann metric. This is achieved by reducing it to an instance of finding a subset of the plucker coordinates with the smallest number of columns. Subsequently, the theory of the totally non negative Grassmann is extended to connect the concept of boundary measurement map to Tanner graph like code construction while deriving new analytical bounds on its parameters. The derived bounds shows that the complexity scales up on the size of the plucker coordinates. Finally, experimental results on decoding failure probability and complexity based on row operations are presented and compared to Low Density parity check codes in the Hamming metric.

Keywords 1. syndrome,coding, Grasmannian, complexity , cryptography

I. INTRODUCTION

The hardness of decoding the syndrome of a linear code [1] has been useful in designing quantum safe encryption in the Hamming metric using Goppa codes [2] and in the rank metric using Gabidulin [3]. The syndrome decoding problem states that given an instance of parity check matrix H , a syndrome of minimum hamming weight w to find a vector x such that $Hx^T = s$. The syndrome decoding problem is relevant to the cryptanalysis of code based cryptography. This is because on the input of certain code parameters and with the knowledge of the structure of the code, an attacker can decrypt the ciphertext and reveal the message in the process. Furthermore, this can be done by the Adversary, if it can find the a vector of length n and also if it has the ability to correct k errors. Solutions to the problem in the Hamming metric have been presented using information sets [4] and its variants [5] to find the codeword with the smallest weight. Also, these solutions has been extended to the rank metric to guess the support that contains the error coordinates [6].

The Grassmannian can be divided into positive or negative depending whether the maximal minor of the generator matrix which is the determinant is positive or negative. In other words, a negative Grassmannian has a negative minor while a positive Grassmannian has a positive minor. Furthermore, the positive Grassmannian has positive

plucker coordinates as well and the essence of using the positive plucker coordinates as a solution to the syndrome decoding problem is to avoid oscillations that would lead to erroneous results when swapping the columns of the generator matrix. Consequently, in the Grassmann metric, plucker coordinates would replace information sets used in the Hamming metric.

However, to the best of our knowledge, no Post quantum based cryptosystem has been designed using codes associated with the Grassmannian in the Grassmann metric. Nevertheless, there is ample evidence that points to the fact there is a connection between the construction of a cryptosystem using a Grassmann based code or a Hamming based code. This is because of the link between the structure of these two codes as explained in this paper [7]. Also, no solution to the problem in the Grassmann metric has been proposed as regards to its use in cryptography. However, for coding applications, research on finding the minimum weight of codewords in the Grassmann metric has been proposed [8].

The question of importance moving forward is this, are there codes associated to Grassmannian varieties with robust theoretical background that can be categorized as a sub family of Tanner graph codes? The synopsis to this question comes from the implication of using Grassmann support and its mathematical framework [6] on code based based cryptography in the rank metric. This parameter is actually a parameter used for codes associated to Grassmann varieties. This inspires the paper to connect the dot by expounding on the Grassmann support and its derivatives. Finally, in the theory of toric geometry [9], the planar graph that illustrates the totally non negative Grassmannian can be redesigned into a graph similar to a Tanner graph [10] and possessing the properties of such a graph. Consequently, Non-negative Grassmann codes is a graph based code that can be represented with vertices and nodes just like Tanner graph based codes.

The solution of the syndrome decoding problem is generalized to the Grassmann metric by using Plucker coordinate based decoding. This is done by finding the subset of plucker coordinate of codewords of minimum Grassmann weight and with zero error coordinate vectors. This can be seen as a generalization of the birthday attack used in plaintext recovery [5]. The plucker coordinates of the totally positive Grassmannian cells are the the columns of the Generator matrix of the code $C(k, n) \subset G_r(n, k)$ whose maximal minor is non-zero . Families of codes associated to Grassmann

varieties can be employed in the quantum safe code based cryptosystem because of its efficient decoding procedure [11] and probability to correct low weight codewords [12].

The Grassmann graph defines a system of k -dimensional subspaces in an n -dimensional vector space of a finite field of Characteristic 2. The graph also includes a projection of $n-k$ dimensional subspace that form unique pivot positions. These subspaces can be seen as vertices connected by edges, if and only if there is a trivial intersection between the subspaces and in the process producing a unit Grassmann distance. Furthermore, the Graph is characterized by sparse bi-adjacency matrix which can be decomposed into a set of positive Grassmannian Schubert cells [9]. These cells can be represented by a canonical matrix in a row echelon format with a leading one in each row. The missing element in each row can be modelled using Ferrer's diagram [12] which represents it as partitions.

The adversary requires knowledge of the map structure in order to decompose the Generator matrix into its row echelon form. In this paper, an instance of a boundary map would be employed to decompose the Generator matrix. They are used to map the k subset elements of the generator matrix into a point in the Grassmannian in order to find non-negative plucker coordinates with minimum Grassmann distance. Furthermore, an a priori approach can be promoted to find the low Grassmann weight vector by enumerating the basis based on a bound that is expressed as function of the number of positroid cells in the graph $Gr_{k,n}$ with weight k .

A. Contribution

The basic contribution of this paper is to advance the solution of the syndrome decoding problem to the Grassmann metric using Plucker coordinates. First, the theory of plucker coordinates is extended with the transformation of planar graphs to non planar graph with tanner like graph properties. Then, the plucker based decoding based on Gaussian decomposition is presented. Thereafter, analytical bounds on the Grassmann parameters are presented. Finally, Numerical results on the failure probability and the cost of row operations when the solution to the syndrome decoding problem is applied to the Non-negative Grassmann is presented and the result is compared to that of Low Density Parity check codes.

II. PRELIMINARIES

A. Notation

In this section,a brief summary of some of the notation used in this paper is provided. F_q represents finite field of q elements, F_{q^m} represents extension field of degree m , F_q^n represents vector spaces of dimension n over F_q , A represents $n \times m$ matrix, a represents a vector, $G_q(n)$ represents set of subspaces belonging to F_q^n (Grassmann graph), $E \oplus F$ represents smallest subspace , $\langle A \rangle$ represents F_q span of A

B. Coding Theory in the Rank Metric

Assuming a bijective mapping between a vector a and a matrix $A \in F_q^{m \times n}$, the subspace of a size $n - k$, the complexity of a combinatoric solution is given by $n - k)^3 m^3 q^{(n-k)} \left[\frac{(k+1)m}{n} \right] - m$ [6]. Lifting can be performed

on an interleaved code by transforming the linear matrix code to a subspace by multiplying its transpose with an identity matrix. The linear matrix code $C[m \times n, k] \in F_{q^m}$ is a linear code generated by $(m \times n)$ matrices. The linear matrix code can be represented as a function of its basis by $C_j = \sum_{i=1}^m X_{ij} \beta_i \forall j \in \{1, \dots, n\}$ where β_i is a basis of a subspace F over F_{q^m} . The basis of a subspace over F_q multiplies C by a non zero element which does not affect the rank distance between codewords. The basis can also be a row of a generator matrix $G \in F_{q^m}^{k \times n}$ which has the complexity of $k(n - k)m^2 \log_2 q$ bits [13]. The dimension of the subspace determines the weight of the codeword and the number of subspaces is given by the Gaussian coefficient expressed as

$$\binom{n}{w}_q = \prod_{i=0}^{k-1} \frac{q^n - q^i}{q^w - q^i} \quad (1)$$

w is the weight and q^m and q^i are monomials over F_{q^m} . In information set decoding, the probability of finding the codeword given a $[n, k, t + 1]$ matrix code is given by

$$P_{dec} = \frac{\binom{n-k}{t}}{\binom{n}{t}} \quad (2)$$

with complexity $P_{dec} = O(1).2^{nH_2(t/n) - (1-k)H_2(t/(n-k))}$ where $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ [14].If the parity check matrix H is expressed with respect to $(n-k) \times n$ identity matrix, an $m \times k$ zero matrix and $(n-k-n) \times k$ random matrix code chosen uniformly as $H = (I/0/R)$ then the linear matrix code is called a simple code and to decode such a matrix value when $m < \frac{m+n-\sqrt{(m-n)^2+4km}}{2}$ is given by $P_f \sim \frac{1}{q^{m-w+1}}$ as $q \rightarrow \infty$.

The bound on the weight of the error vector is given by the Gilbert-Varshamov bound [15] which is defined as thus

Definition 1. The number of elements of a sphere S given integers n, m, q, t with radius $t \in F_{q^m}^n$ is equal to the number of spaces with $m \times n$ bases of dimension t . For $t \geq 1$ this follows that

$$S = \prod_{j=0}^{t-1} \frac{(q^n - q^j)(q^m - q^j)}{q^t - q^j} \quad (3)$$

For a ball of radius t , the volume of $B = \sum_{i=0}^t S(i)$.Also for a matrix code C , if $B \geq q^{m(n-k)}$ and $\sum_{j=0}^{t-1} \binom{n-1}{j} < 2^{n-k}$ then the smallest integer t is referred to as the Gilbert-Varshamov bound.

C. Syndrome Decoding Problem

The Syndrome decoding problem is defined here in terms of complexity theory

Definition 2. The a priori probability of finding a codeword x_i with non-zero codewords $\leq w$ and an integer which represent the i th column of an error applied to a Code C which transforms it to C' , and in the process satisfying the expression

$H^T x = s$, where $s \in R F_{q^m}^{n-k}$ is a syndrome and H is a parity check matrix over F_{q^m} .

Consequently, to generalize this problem to the Grassmannian metric, it has to be reduced to an instance of finding the plucker coordinates of codewords with lowest Grassmann weight.

Definition 3. Let plucker coordinates be denoted as $\Delta_{I,J}(G) > 0$ which forms the columns of the generator matrix. The syndrome decoding problem is to find linearly dependent subset of plucker coordinate with w columns such that $G_{i,j-k} \wedge v_j = u_i$ were a basis B is defined thus; $B = \{u_i, v_j | i \in I, j \in J\}$, a $k \times n - k$ matrix M_v and a $k \times n - k$ generator matrix G with rank K .

D. Grassmannian theory

Definition 4. Totally non-negative Grassmannian [9] is the point in the Grassmann graph with positive plucker coordinates $\Delta_I \neq 0$

In other words its maximal minor is positive and it can combinatorially analyzed using planar bipartite graph. The matroid of the totally positive Grassmannian is termed a positroid.

Definition 5. The boundary measurement map [9] is defined as $b : R_{>0} \rightarrow G_{L_k} . A \in Gr_{n,k}$ where A is a $k \times n$ biadjacency matrix with a rank k which are represented by incoming boundary edges and the map depends on the coloring of the vertices.

The matrix has a maximal minor $\Delta_I = 1$ that forms the plucker coordinates on $Gr_{n,k}$ with column vectors $\frac{I}{A}$ that gives the basis of the subspace. Furthermore, the coordinates of A can be defined as follows with slight abuse of notation $\varphi(A) = \langle (u_i + \sum_{j=1}^{n-k} A_{ij} v_j) \rangle \forall 1 \leq i \leq k$.

$R_{>0}$ is characterized by the set of all the biadjacency matrix A . The subspace in this set is a graph of a map from a projection to its orthonormal that is $V \rightarrow V^\perp$ and direct sum expression given by $V \oplus V^\perp \cong R^n$ with a basis $V = \{v_1, \dots, v_a\}$.

Let the map of a subspace U to its local diffeomorphism be given as $\phi(u) = (\phi_1, \dots, \phi_n)(u_1, \dots, u_k)$, then it follows that the tangential space at any point of the map has a basis with coordinates $\{\frac{\partial \phi}{\partial u_1}, \dots, \frac{\partial \phi}{\partial u_k}\}$. In other words, the tangential space can also be represented by the derivative of the Grassmann. If there is an open subspace in the Grassmann graph $Gr_{n,k}$, then we have $U = \{W : W \cap V^\perp = \{0\}\} \subset R^k \times R^{n-k}$ for any $W \in U$.

There are complex numbers c_{ij} such that $v_i + \sum_{j=1}^b c_{ij} v_j \in W$ which is linearly isomorphic. Therefore, the graph becomes $U(S) = \{v + Sv : v \in V\}$ such that $v \mapsto (V, S(v))$. If $v = 0$, then $U(C) = 0$ from the nullity of maps. If V is decomposed to subspaces P and Q where $Q \in U_A$ and U_A is a set of all subspace $P \subset V$ such that $V \cap U_A = \{0\}$, then we have $P = (P \cap Q) \oplus P'$ for some P' isomorphic to $P/(P \cap Q)$.

Furthermore, for a direct sum decomposition, the intersection of P and Q is trivial which now becomes $P + ((P \cap Q) \oplus P') = P \oplus Q'$. If the subspace E is decomposed,

we now have $E = (E \cap V) \oplus E'$ for some $E' \subset R^n$ where the intersection $E \cap V$ tends towards the solution [11].

Finally, an injective transformation $F_k(V)$ given by $T : R^k \mapsto V$ is an open subset of $L(R^k, V)$ and a space with $\dim(F_k(V)) = kn$. In other words, $F_k(V)$ is the projective geometry of V and its quotient space generates the Grassmannian space.

Proposition 1. Let V be a linear subspace and V^\perp its orthonormal projection. Let U_A be a set of all projections $P_V \subset V$ through a map $U = v + Sv$. Then U_A lies in $L(V, E)$, if a linear isomorphism $T \in \pi^{-1}(U_A)$ exists.

Proof. If there is an open subspace in the Grassmann graph G_{n-k} , then $U = \{E \cap V^\perp = \{0\}\}$ and $U(S) = \{v + Sv : v \in V\} : v \mapsto (v, S(v))$ where a subspace $S \subset V \oplus E$. This implies that $S \cap E = \{0\}$. Lets define two projections $P_{V'} : V' \mapsto V$ and $P_V : V \mapsto V'$ where $P_V(v)$ is related to $P_{V'}$ by the expression $P_V(v) = (P_{V'})^{-1}(v) - v$. Given U_A a set of all projections $P_V \subset V$, we have a linear isomorphism $T \in \pi^{-1}(U_A)$ and a projective geometry $F_K(v) = \pi^{-1}(U_A)$ where π^{-1} is an invertible function. Then it follows that the intersection of T and the biadjacency A is trivial that is $\pi(U_A \cap A) = \{0\}$, if the function π can be inverted and if a map $f(T) = 0$. For $v \in V$, it is assumed that the k dimensional subspace is equivalent to its transformation for some $v' \in V$ that is $v + S(v) = v' + S'(v')$. It follows that $v - v' = S'(v') - S(v) \in E \cap V^\perp = \{0\}$, $\Rightarrow S(v) = S'(v')$. Concatenating the linear isomorphism T with the projections $P_{V'}$ and P_V , we have $f_T(v) = (P_{V'} \circ T) \circ (P_V \circ T)^{-1} \forall v \in V$ and if f restricts $S = S'$ on $L(V, E)$ then it becomes $f_T : \pi^{-1}(U_A) \mapsto L(V, E) \Rightarrow$ that $P_V(v) = (P_{V'})^{-1}(v) - v = v + Sv$. This results to $P_V(v) = Sv$ and $f_T(v) = (P_{V'} \circ T) \circ (P_V \circ T)^{-1} = id_{V, V^\perp}$ \square

III. EXTENDING THE THEORY ON NON NEGATIVE GRASSMANN

In this section, we would try to link the totally non negative Grassmann to tanner code like constructions by transforming it from its planar structure to non planar structure. This can be seen as intersecting the theory of distance transitive graph and coding theory based on the framework of Grassmann variety. First, we redefine the concept of boundary measurement maps and thereafter present a logical breakdown of how this map can be represented as a binary matrix. The boundary measurement maps are designed as a mapping or transformation of vertex set in a planar bipartite graph to edge weights defined as a set of vertices in a cell in the Grassmannian graph. Given a set $I_f \subset I$, removing an element from the set, an embedding can be constructed from the

bipartite to the Grassmannian as $Gr_{r_k, n}(R) \rightarrow RP^{\binom{n}{k}-1}$ which forms a gauge transformations expressed as a function of matroids $Meas : R_{>0} \rightarrow Gr_{r_k, n}(R)$ where $Gr_{r_k, n}(R)$ is k planes on an n -dimensional space which is not affected by the ratios of $k \times k$ minors of a $k \times n$ code. To decompose the Grassmann, an arbitrary edge function is selected such that

$e : u \rightarrow v$ and if the vertex is coloured, another edge function is selected $e' : v \rightarrow w$ by maximum revolution. Depending on the coloring, this maximum revolution can be clockwise or anticlockwise. This maximum revolution induces self intersections through the path and can define the boundary measurement as $M_{ij} = \sum_{P:e \rightarrow e'} (-1)^{\text{wind}(R)} \text{wt}(P, y)$ where the factor $(-1)^{\text{wind}(R)}$ is bound by the number of connection between sources to the planar bipartite graph which is made up of n external nodes of perfect orientation and k sources of perfect orientation and $\text{wt}(P, y)$ is the weight of the path.

The planar bipartite graph structure with perfect orientation[16],[9] would be employed to buttress the idea. This is shown in Figure 1 and Figure 2. First, the planar bipartite graph is transformed into non planar bipartite graph taking note of the sources and external nodes while labelling them accordingly for convenience purposes. If the row and column are of the same node, the code entry is set to 1, if there is no path connecting the nodes, the map code entry is set to 0. Finally, the condition in literature is modified to support the objective of the idea by stating that if there is a negative sign then the entry is set to 0 and set to 1 if otherwise. Therefore, a boundary measurement mapping A and B produces the Grassmannian $G_{r>0}(2, 4)$ and $G_{r>0}(2, 6)$ respectively which is constructed using the flows as regards to whether it is clockwise or anticlockwise as follows;

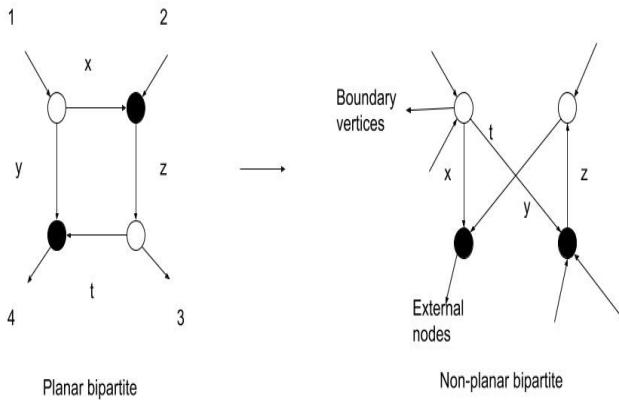


Fig. 1. Non planar bipartite graph with perfect orientation containing 2 boundary vertices, 2 external nodes and a face transformed to its non planar structure

$$A = \begin{bmatrix} 1 & 0 & -t+x & -(y+xzt) \\ 0 & 1 & y & zt \end{bmatrix} \Rightarrow \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix} \rightarrow G_{r>0}(2, 4) \quad (4)$$

The same procedure is extended to B as well

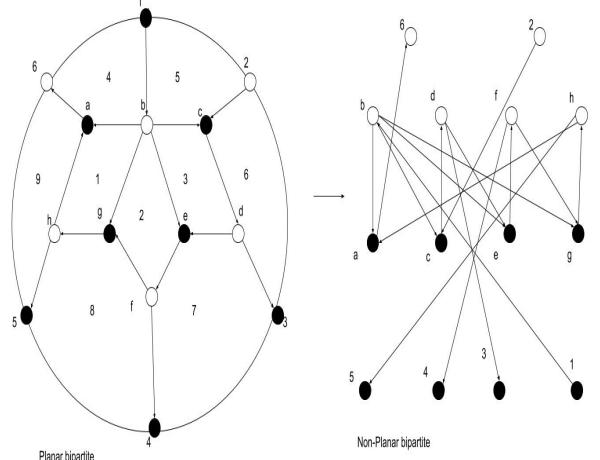


Fig. 2. Non planar bipartite graph with perfect orientation containing 2 boundary vertices, 6 external nodes and 9 faces transformed to its non planar structure

$$B = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \rightarrow G_{r>0}(2, 6) \quad (5)$$

The dimension of the Grassmannian parametrized from $G_{r>0}(2, 4)$ is given as 4, then the number of boundary vertices k is computed as follows $k(n - k) = 4$; $k = 2$ while that of the Grassmannian parametrized $G_{r>0}(2, 4)$ is given as 6, then the number of boundary vertices k is computed as follows $k(n - k) = 6$; $k = 2$

For a set $I = \{1, 2\}$ and a minor $J = 2, 6$, a modified plucker coordinate for $\Delta_{2,6}$ can be computed as follows

$$\Delta_{26} = f/g = \frac{(1b + C2)(1b + ab)}{1 + C2} \quad (6)$$

IV. DECODING WITH PLUCKER COORDINATES

In this section we present the idea of decoding with plucker coordinates as a solution to the Syndrome decoding problem in the Grassmann metric. It is pertinent to note that this method is analogous to an optimized variant of Information set decoding.

Let $C \subset G_r^+(n, k) \in F_2^{k+l}$ be a code associated to the totally non-negative Grassmannian with a generator matrix $G \in F_2^{(k+l) \times l}$ and a subset of the matroid space Mat_+ ,

$$\text{we have } G = \begin{pmatrix} g_0 & g_1 & g_2 & \dots & g_n \\ g_0^q & g_1^q & g_2^q & \dots & g_n^q \\ \vdots & \vdots & \vdots & \dots & \vdots \\ g_0^{q^{k-1}} & g_1^{q^{k-1}} & g_2^{q^{k-1}} & \dots & g_n^{q^{k-1}} \end{pmatrix}.$$

The element of the Grassmannian are the linear span of the columns of the generator matrix which produces the subspace $V = \langle g_i, \dots, g_n^{q^{k-1}} \in R^k \rangle$ and the linear span of the rows of the generator matrix produces the subspace $U = \langle g_i, \dots, g_n \rangle \subset R^n$. By employing Gaussian elimination

and taking an instance of the boundary map $\tau \in b$, we generate an equivalent code $C' = \tau(C)$ with generator matrix G' in row echelon form $G' = \begin{pmatrix} I^l & O^l & H' \\ O^{n-k-l} & I^{n-k-l} & H'' \end{pmatrix}$ were $H' \in F_2^{(k+l) \times (k+l)}$, $H'' \in F_2^{(2k+l) \times (k+l)}$ and I^{n-k-l}, I^l are identity matrices of size $n - k - l$ and l respectively. O^{n-k-l}, O^l are zero matrices of size $n - k - l$ and l respectively. Select plucker coordinates $\Delta_{I,J}(G)$ with size $k+l$ for H' and another plucker coordinate $\Delta_{I,J}$ for H'' were $I = \{i_1 < \dots < i_k\}$ are k elements of G . Applying cycle shift to the columns of H' and removing indices $i \in I$ to form a basis of the subspace $V' = \langle g_2, \dots, (-1)^{k-1}g_n^{q^{k-1}}, g_1 \rangle$ and also cycling shifting the columns of H' and removing indices $i \in I$ to form the basis of the extended subspace $U' = \langle g_2, \dots, g_n, g_i \rangle$. A linear combination of the $k-1$ columns of the subspace V' will form a vector $\tau(V')$ and a linear combination of the n columns of the subspace U' will form a vector $\tau(\Delta_{U'})$ with a pivot centered around $\tau \in b$. Add $\tau(V') + \tau(\Delta_{U'})$ and check if the Grassmann weight $d(V' \cap U') \leq w - n + k - 1$ and stop. if the last condition is not met, then the process is repeated. It can be said that if the cyclic shift is applied, I becomes I' . The Gaussian decomposition operation is a function of the ordering of the plucker coordinate vectors.

A. Correctness

The identity matrix I_u and the zero matrix O_V were both are restricted to $n - k - l$ plucker coordinate positions, $I_U = \begin{bmatrix} I^l \\ I^{n-k-l} \end{bmatrix}$ and $O_U = \begin{bmatrix} O^l \\ O^{n-k-l} \end{bmatrix}$. We transform the matrix I_U and O_V by multiplying by the parity check matrix H as follows $I_U H = \begin{bmatrix} H' & I^l \\ H'' & I^{n-k-l} \end{bmatrix}$ and $O_V H = \begin{bmatrix} H' & O^l \\ H'' & O^{n-k-l} \end{bmatrix}$. Furthermore, multiplying the error vector x to both matrices were x is generated by $k+l$ entries $I_U H x^T = \begin{bmatrix} H' x'^T + x''^T \\ H'' x'^T + x''^T \end{bmatrix}$ and $O_V H x^T = \begin{bmatrix} H' x'^T \\ H'' x'^T \end{bmatrix}$. Concatenating the matrices becomes

$$I_U O_V H x^T = \begin{bmatrix} (H' x'^T \cdot H' x'^T) + (H' x'^T \cdot x''^T) \\ (H'' x'^T \cdot H' x'^T) + (H'' x'^T \cdot x''^T) \end{bmatrix} \quad (7)$$

let $s = (s', s'')$ be the coordinate of the syndrome then

$$I_U O_V s^T = \begin{bmatrix} H' x'^T + O^l \\ H'' x'^T s' + O^l \end{bmatrix} = \begin{bmatrix} H' x'^T \\ H'' x'^T s' \end{bmatrix}$$

Let $B(k, n)$ be the plucker coordinate of all subspaces with restriction in the first k plucker coordinates $g_1, \dots, g_k^{q^{2k-n}}$. The $k \times k$ minor $\Delta_{B(n,k)}$ of the generator matrix G' is the set of k plucker coordinates in $G_r^+(k, n)$. The instance of the boundary measurement map is validated by the Adversary on the condition that $\Delta_{B(n,k)}(G) \neq 0$. It can be said that $B(k, n)$ which is the bounded affine permutations constitute the set of information sequences. The instance of the boundary measurement map can be represented by a Vandermonde matrix such that the plucker coordinate is the column set of $I^{n-k-l} \in G'$. Afterwards, the adversary selects an arbitrary

subspace V with basis $V = \langle 0, v_1, \dots, v_{k+l} \rangle \subset C'$ and choose the codewords with minimum weight $w \leq q^{\frac{k(k-1)}{2}}$. Finally, the Adversary checks if $d(U \cap V) \leq w$ and stops. By induction, it can be seen that there are $q^{\frac{k(k-1)}{2}} \cdot \binom{k}{r}_q$ ways of choosing the basis of the subspace V and $q^{\frac{k(k-1)}{2}} \cdot \binom{n-r}{k-r}_q$ ways of choosing subspace U . The proof of this claim is presented in Theorem 3. Therefore the probability of guessing correctly the error free plucker coordinates is given as $\frac{\binom{n-r}{k-r}_q}{\binom{k}{r}_q}$.

V. ANALYTICAL BOUNDS ON GRASSMANN PARAMETERS

Proposition 2. Let $U, V \in F_{q^m}$. As $q \mapsto 1$ and defining a map $P_v : F_q^n \mapsto F_q^{n-1}/V'$ then $d(U, V) \leq 2q \binom{n}{k}_q$

Proof. k subspaces U, V of F_{q^m} , $d(U, V) = k - \dim(U \cap V)$ and for vector spaces over the same field, we have $\dim(V \cap G) = \dim(V) + \dim(G) - \dim(V \cdot G)$, therefore it follows that

$d(U, V) = k - (\dim(U) + \dim(V) - \dim(U \cdot V)) \leq k - (k + k - (k - r)) = r$. Given a subspace with dimension k , $\binom{n}{k}_q = \prod_{i=0}^{k-1} \frac{q^n - q^i}{q^k - q^i}$, Selecting a $k-1$ dimensional subspace V' of F_q^{n-1} to construct an arbitrary k dimensional subspace such that $V \cap V' = \{0\}$. Selecting a basis $v \in V'$, $v' = \{v_1 < \dots < v_{k-1}\} \subset N$ of a linear map defined thus $P_v : F_q^n \rightarrow F_q^{n-1}/V'$ to construct a bundle $\phi^{-1}(1) = V$. If $\dim V' = r$, then the number of bundles is equivalent to the number of enumerated bases of size $\{1, \dots, n - k\}$ over F_q which is q^{n-k} . This results to the identity

$$\binom{n}{k}_q = \prod_{i=0}^{k-1} \frac{q^n - q^i}{q^k - q^i} = \binom{n-1}{k-1}_q + q^{n-k} \binom{n-1}{k-1}_q \quad (8)$$

(9)

this follows that for $0 < k < n$

$$\leq \frac{q^{n-1} - 1}{q^k - 1} + q^{n-k} \cdot \frac{q^{n-1} - 1}{q^{k-1} - 1} \quad (10)$$

$$\leq \frac{q^{n-1} - 1}{q^k - 1} + \frac{(q^{n-k})(q^{n-1} - 1)}{q^{k-1} - 1} \quad (11)$$

Using a generalized identity [17] and doubling the right hand side of Equation (13), vectors except one of the q multiples of v can be computed as

$$\binom{n}{k}_q = \sum_{i=0}^{k-1} q^{(n-k)(k-i)} \binom{n-i}{i}_q \leq \quad (12)$$

$$\prod_{i=0}^{k-1} \frac{q^{n-i+1} - q}{q^i - 1} = \quad (13)$$

factorize q based on cardinality [18] it becomes

$$\prod_{i=0}^{k-1} q \frac{q^{n-i}-1}{q^i-1} \quad (14)$$

□

Remark 1. Proposition 2 gives the bound on the total number of error patterns with k errors that the enumerator can compute given the size of the plucker coordinate as $\begin{bmatrix} n \\ k \end{bmatrix}_q$.

Lemma 1. The basis of the concatenation of the subspace U and V induces a subgraph with no cycle whose weight of its total path is equivalent to the plucker coordinate of the Grassmannian graph.

Proof. Given a bounded permutation $f_x(i) = \min\{y \geq i/v_i \in \text{span}\{v_{i+1}, v_{i+2}, \dots, v_j\}\}$ where v_i are the columns of the arbitrary space of S , taking basis $\{v_{i+1}, v_{i+2}, \dots, v_j\}$ and extend it to $U \cap V$ as follows $v_{i+1}, v_{i+2}, \dots, v_j, e_{i-m+1}, \dots, e_i$ and $\{v_{i+1}, \dots, v_j, f_{i-m+1}, \dots, f_k\}$ through the path of the disk divided by a face $f \in U$ then we have $P = \{e_{i-m+1}, f_{i-m+1}, \dots, e_i, f_i\}$ which forms a basis. The plucker coordinate now becomes $\Delta_I(G) = \sum \prod_{P_i} \text{wt}(P_i)$, which implies that $\Delta_I(G)$ divides the vertex set Δ_I indexed by I an identity matrix such that each elements $e \in E$ and $f \in F$ induces a subgraph in Δ_I □

Theorem 1. the intersection array is given by $b_{r_k} \leq q^{i(i-1)/2} \begin{bmatrix} n \\ k \end{bmatrix}_q$.

Proof. Connecting k to $k+1$ vertices with a rank r will give the boundary measurement map transformation from the planar bipartite graph G to non-planar Grassmannian G_r if $k+1 \in I$. For $k \notin I$ and with plucker coordinates given as $\Delta_I(G) = \Delta_I(G_r) + r\Delta_I - \{k+1\} \cup \{k\}(G_r)$ this implies that $\Delta_{(I \setminus \{r\}) \cup \{k\}} = (-1)^t b_{r_k} \geq 0$ where $t = |I \cap [r+1, k-1]|$ resulting in the probability

$$(-1)^i \prod_{j=1}^i \frac{q^{j-1}qm - i + 1 - 1}{q^i - 1} = (-1)^i q^{i(i-1)/2} \begin{bmatrix} m \\ i \end{bmatrix} \quad (15)$$

□

Remark 2. It can be seen from Theorem 1, that the intersection array depends on the degree of the extension field m . Increasing the degree extension of the field or the power of the prime increases the intersection array of the Grassmannian graph. Also, each row operation of the Gaussian elimination process preserves the intersection array of the graph. Furthermore, this increases the size of the plucker coordinates thereby reducing the complexity of the solution.

Assuming two codewords C_1 and C_2 have rank weight k_1 and k_2 . C_1 and C_2 have two different subspaces V and U where $V = \{v_1, \dots, v_{k_1}\}$ and $U = \{u_1, \dots, u_{k_2}\}$, then the product of the spaces is bounded by $\langle VU \rangle \leq k_1 k_2$ where k_1 and k_2 are the dimensions of the spaces V and U . if $k_1 k_2 < m$ then the probability holds $\Pr(\dim\langle VU \rangle < k_1 k_2) \leq \frac{q^{k_1 k_2}}{q^m}$. This probability is the probability of enumerating the bases

in order to find the candidate codewords given the dimension

Corollary 1. If A is random and B is fixed then the probability that a space U and A a base that generates a random space with dimension k_1 is at least $1 - k_1 \frac{q^{k_1 k_2}}{q^m}$ where $\dim\langle AU \rangle = k_1 k_2$.

Proof. There exist a codeword $C \in U$ where U is a space and $C \notin F_q$, then given $\dim\langle AU^2 \rangle = k_1 k_2$ and an error $e \in \langle AB \rangle$ with $e \notin A$ then the product CU is an element of the space U . □

Theorem 2. Let A be a base that generates a fixed space with dimension k_1 and B a base that generates a random space with a basis such that dimension $k'_2 = k'_1(1 - k_2)$, if $A \cup \langle AB \rangle = \beta$ with its probability of enumeration given as $1 - k_2 \frac{q^{2k_1 k'_2 + k_2(k_2+1)}}{q^m}$ holds.

Proof. We have $\cap_i \beta_i^{-1} s = A$ then $A \cup \langle AB \rangle = \beta$ where $\langle AB \rangle$ is the product of the space with their attendant bases A and B which gives a new basis β . If A is random the dimension becomes $k'_1 k_2 - k_2 = k_2(k'_1 - 1)$ then a random space with a base B has a dimension $k'_2 = k'_1(1 - k_2)$ as given. If $\langle AB \rangle \cap \langle AB \rangle_{-1} = A$ such that the dimension of a fixed base B is $\dim B = \dim(k_2) + B\beta^{-1}$ which is equivalent to $\frac{k_2(k_2+1)}{2} + B\beta^{-1}$. Multiplying both sides by 2 now becomes $k_2(k_2+1) + 2k_1 k'_2$ with the given probability □

Remark 3. Corollary 1 shows the probability of finding the codewords in plucker coordinates embedded in a space of dimension k_1 when the Code associated to the totally Nonnegative Grassmann is concatenated with a subspace generated by a random basis.

Theorem 2 takes it further by describing the probability of finding the codeword if the subspace is a linear span of a fixed basis and a random basis with random coordinate vectors. It can be seen that the probability scales with increase in the k_2 positions the decoding algorithm searches for.

Theorem 3. Given $U, V \in G_r(n, k)$ and $d(U, V) = \dim(U) + \dim(V) - 2\dim(U \cap V) = k - r$ where k is the dimension of the subspace and r is the rank with integers l, p, m then the bound from the Gaussian coefficient on $d(U, V)$ given by

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \sum_{k=0}^{\infty} \frac{q^{\frac{k(k-1)}{2}}}{(1-q)(1-q^2) \dots (1-q^k)} \cdot \begin{bmatrix} n-r \\ k-r \end{bmatrix}_q \cdot \begin{bmatrix} r \\ k-m \end{bmatrix}_q \cdot \begin{bmatrix} k \\ r \end{bmatrix}_q \quad (16)$$

Proof. Starting with a basis for U , $B_1 = (e_1, \dots, e_m)$, picking randomly linearly independent vector $x_{U_i} \in U$. Then search for a coordinate of x_{U_i} and replace to produce a new basis for U after repeated procedures to give $B_1 = e'_1, \dots, e'_m, x_{U_1}, \dots, x_{U_k}$ and update count as

$$\text{Count}_U = \prod_{k=0}^{U_i-1} q^k = \sum_{k=0}^{U_i} q^{\frac{k(k-1)}{2}} \binom{n}{k} \quad (17)$$

Then the same process follows for V a basis, $B_2 = (f_1, \dots, f_m)$ is selected. Then, random linearly independent vectors $y_{V_i} \in V$ is selected as well and a search for

coordinate of y_{V_i} is conducted which is now replaced to produce a new basis for V after repeated procedures to give $B_2 = f'_1, \dots, f'_m, y_{V_1}, \dots, y_{V_k}$ and updating the count gives

$$\text{Count}_V = \prod_{k=0}^{V_i-1} q^k - q^{k-r} = \sum_{k=0}^{V_i} q^{\frac{k(k-r)}{2}} \binom{k}{r}_q \quad (18)$$

Then, finally starting with a basis for $U \cap V$, $B_3 = (g_1, \dots, g_m)$, then another random linearly independent vector $z_i \in U \cap V$ is selected to produce a new basis after repeated procedures $B_{3'} = (g'_1, \dots, g'_m, x_{U_1}, \dots, x_{U_k})$ and $B_{3''} = (g_1, \dots, g'_m, y_{V_1}, \dots, y_{V_k})$. Sampling an integer $l_i \in L$ where $L = \text{Vect}(x_U)$ and $p_i \in P$ where $P = \text{Vect}(y_V)$ and updating the count as

$$\begin{aligned} \text{Count}_* = & \prod_{k=0}^{U_i-V_i-1} q^k - q^{k-r+t} - q^{k-r+p} = \\ & \sum_{k=0}^{U_i-V_i-1} q^{\frac{k(k-r)}{2}} \left[\begin{matrix} n-r \\ k-r \end{matrix} \right]_q . \\ & \left[\begin{matrix} r \\ k-t \end{matrix} \right]_q \cdot \left[\begin{matrix} k \\ r \end{matrix} \right]_q \end{aligned} \quad (19)$$

From the total of the Counts, $\text{Count} = \text{Count}_U + \text{Count}_V + \text{Count}_*$, the bounds can be computed. It follows that $U = \text{span}\{g_i, x_{U_i}\}$, $V = \text{span}\{g_i, y_{V_i}\}$ and $U \cap V = \text{span}\{g_i\}$

□

Remark 4. The syndrome decoding problem becomes $H'x^T = \sum_{l=1}^n \sum_{j=1}^k \alpha_{ij} H'_l V_j = 0$, we now have

$$\text{Prob}(U \cap V) = \frac{q^{\frac{k-1}{2}} \binom{n}{k}_q}{q^{\frac{k(k-r)}{2}} \binom{k}{r}_q} \propto q^{\frac{k(k-r)}{2}(n-k)} \quad (20)$$

This results in a complexity of $O(\frac{(n-k)^2}{2} q^{\frac{k(k-r)}{2}(n-k)})$.

Theorem 4. if the dimension of the vector space $\forall d \leq 2$, then the complexity of basis enumeration is given by

$$\sum_{\alpha=1}^d \binom{n}{l} \binom{\alpha}{n}^d \left(1 - \frac{\alpha}{n}\right)^{n-l} x^d .$$

Theorem 4 gives a closed form expression for the average number of iterations

VI. FAILURE PROBABILITY AND COMPLEXITY ANALYSIS

We present numerical results on the optimization of plucker set decoding to the totally non negative grassmannian. In order to compare the results with code in the Hamming metric, we optimized our implementation to use information sets rather than plucker coordinates. It is also important we feed the algorithm with as much sets as possible to make the iteration process smooth and efficient. At this juncture it is important to reiterate that simulations of these kind has huge impact on the memory resources of the computing device deployed. In these experiments we used AMD Ryzen 3 2200U laptop with Radeon Vega Mobile Gfx graphic card with processor speed of 2500MHz, 2 cores, 4 logical processors and clock speed of 2.5GHz. Due to the limitation of the memory, the experiments were conducted with little amount of code sizes. However, these experiments can be scaled up without much impact on the result analysis.

A. Probability of failure

In this section, the results of experiments on the probability of decryption failure while using the solution to the syndrome decoding problem to recover the information sequence from totally non negative Grassmannian is presented and compared with the probability of solving the problem using an LDPC code in the Hamming metric. This process was carried out by optimizing the implementation [19] for this purpose. Theoretical analysis on the comparison between two codes has been studied(ref). We go further than this by experimentally analysing the implication of this comparison on the security of a code based cryptosystem. We can recall the importance of this property on the semantic security of Indistinguishability for a Chosen ciphertext attack. This is because of the negligible error patterns present in each vector space. The lower this probability, the higher chance of the quantum adversary to distinguish between random instances of the ciphertext. In this experiment, we set the number of information sets 2^l , for each level of security under investigation were l is the number of indices of the information set. For 128-bit security level, we set $T = 32,768$ and the result is shown in Fig. 3, for 256-bit we set the number of information sets as $l = 1048576$ and the result is shown in Fig 4, for 512-security level we set the number of information sets as $T = 33,554,432$ and the result is shown in Fig.5,finally for 1024-security level, we set the number of information sets to $T = 1073741824$ and the result is shown in Fig. 6. The standard deviation of the distribution σ for all security levels is varied from 0.30 to 0.85 for cryptography purposes. To compute the amount of Gaussian elimination operation carried out, we use the formula $\frac{1}{2}(n-k)k^2$, this is shown in Table 1. This formula relates the number of information sets T to the Gaussian decomposition operations. It can be see from Table 1. that the Gaussian decomposition increases as the security level increases. This is due to size of the information set for each security level which is bounded by $\geq n - k$. The reason for this is to limit the frequent failure of the algorithm due to its probabilistic approach at examining the codewords. However, this comes at a great computational cost. Furthermore, It can be seen that the failure probability of the Non-negative Grassmannian code is smaller than the failure probability of the LDPC code. The implication of this is that the Non-negative Grassmannian code based cryptosystem is more secured than the LDPC code based cryptosystem under the IND-CCA model. This is because in the IND-CCA model, the probability error must be negligible in order for the probability polynomial adversary to find it hard to be able to distinguish a secret sampled from a theoretical distribution from that sampled from an arbitrary distribution. In Fig1. at a standard deviation of 0.50, the failure probability of the Non-negative Grassmann code is less than that of the LDPC code by 1.18 percent, In Fig2. at a standard deviation of 0.50, the failure probability of the Non-negative Grassmann code is less than that of the LDPC code by 3.23 percent. In Fig3. at a standard deviation of 0.50, the failure probability of the Non-negative Grassmann code is less than that of the LDPC code by 2.34 percent and finally in Fig.4 at a standard deviation of

0.50, the failure probability of the Non-negative Grassmann code is less than that of the LDPC code by 3.17 percent. As the security level increases, the size of the intersection array increases which induces some level of randomness on the plucker coordinates and in the process expanding the probability that a zero error pattern is contained in an arbitrary information subspace. This can be seen in the reduction in the error floor as the security level increases.

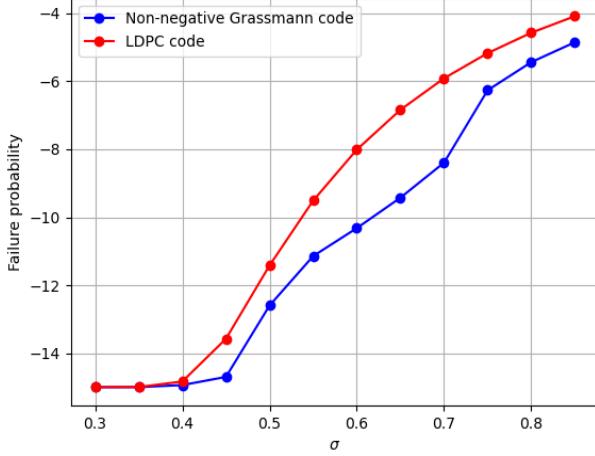


Fig. 3. Probability of failure for 128-bit security, security parameter $l = 15$

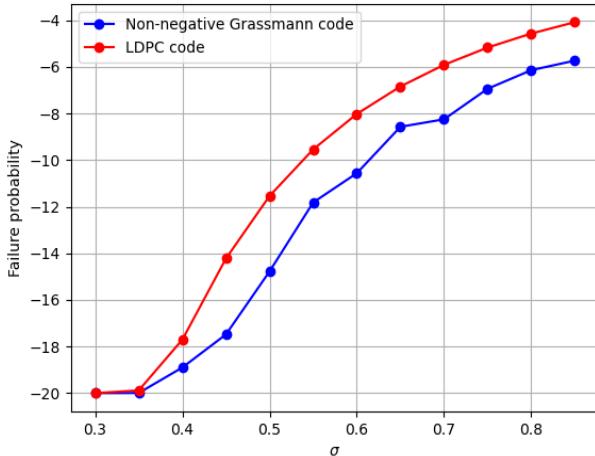


Fig. 4. Probability of failure for 256-bit security, security parameter $l = 20$

B. Complexity

In this section we optimized the implementation [24] to test the cost of iterating over the rows of the Non negative Grassmann code in the Grassmann metric as compared to the LDPC code in the Hamming metric with increase in code length. The results are presented in Fig. 6 for finite field of characteristic 2 and in Fig. 7 for a finite field of characteristic

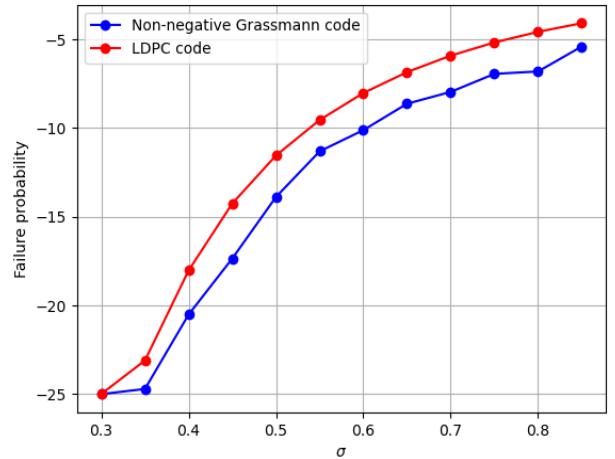


Fig. 5. Probability of failure for 256-bit security, security parameter $l = 25$

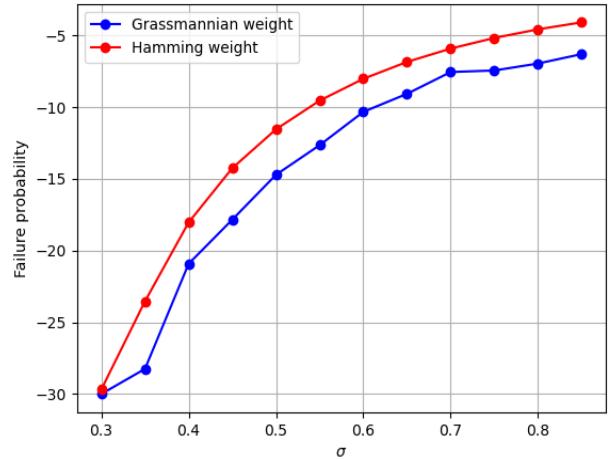


Fig. 6. Probability of failure for 1024-bit security, security parameter $l = 30$

2 and extension 2. From the result it can be seen that cost of iterating over rows of the Non negative Grassmann code is higher than of the LDPC code with increasing code length. At a code length of $n = 100$, the complexity of row operations is higher by 5.81 percent. This shows that Non negative Grassmann code based cryptosystem is stronger against ISD attack than LDPC code. This is good for quantum security. In Fig. 7, the field size was extended by 2 and a difference of 29.4 percent was recorded. The huge difference is a result of the large size of the coefficients of the polynomial linear equations with variable q , the field size which in turn increases the size of the basis of $k + 1$ subspaces of dimension $n = 1$.

Quantum security is obtained by dividing the security bits by 2, that means for 128 bit security the equivalent quantum security is 56 bits and to make the density of the decodable syndrome close to 1, parameters must satisfy [25].

TABLE I
GAUSSIAN DECOMPOSITION OPERATIONS AS A FUNCTION OF SECURITY LEVEL

Security level	Gaussian Decomposition
128	131072
256	1048576
512	8388608
1024	67108864

TABLE II
COMPARISON WITH PARAMETERS IN THE RANK METRIC

n	k	m	q	w	Security	
67	7	89	2	5	128	[20]
100	80	96	2	5	192	[21]
100	80	96	2	5	192	[22]
67	22	71	2	11	133	[23]
110	7	18	2	12	128	This work

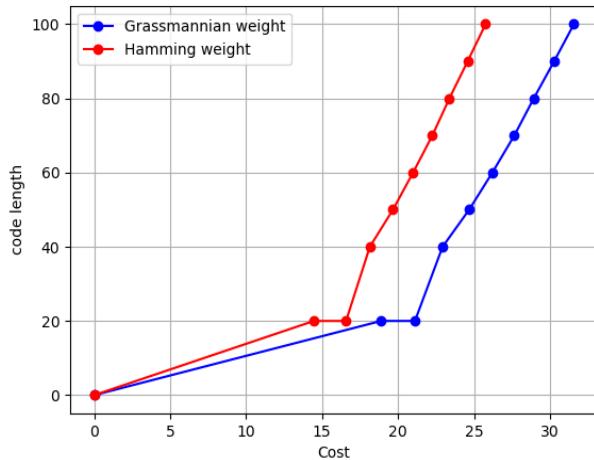


Fig. 7. Cost of row ISD operations,field size $q = 2$

The Grassmannian weight of the Trapdoor function should be large enough to make cryptanalysis through a structural process difficult. The data size and computational time are linear in $\log q$ while the complexity of combinatorics are polynomial on q making it difficult to break encryption key. The decoding error with failure probability is equivalent $\frac{1}{q^{l'-2wr+1}}$ [21] and the key size increase inversely to an increase in the probability of the decoding failure. In the presence of cyclic vectors, classical attacks makes it possible to obtain the plucker coordinates of the permuted codewords. In Table 2 we give suggested parameters were n is the code length, k is the code dimension, m is the degree of extension field, q is the prime, w is the error weight which is compared to other parameters from related works. The works compared in the table were variants of ISD employed in cryptanalyzing Code based cryptography in the rank metric. From the complexity derived from Theorem 3 and Remark 2, it can be deduced

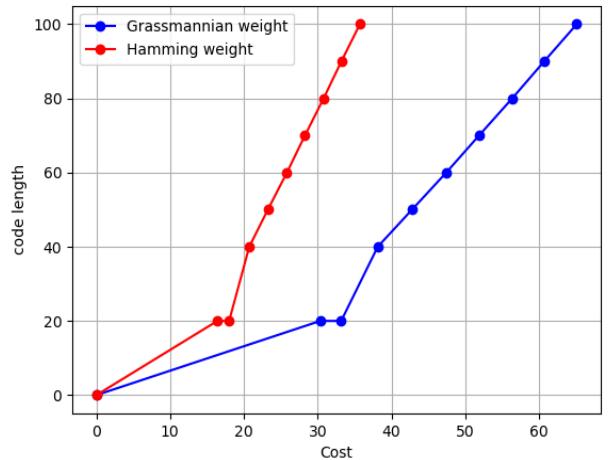


Fig. 8. Cost of ISD row operations,field size $q = 2^2$

that the complexity of the ISD decomposition on the input of the proposed parameters is 2^{23} which is below the claimed security level of 2^{128} . This shows that the complexity of our approach depends on the size of the plucker coordinates as derived from proposition 2.

VII. CONCLUSION

The syndrome decoding problem as a computationally hard primitive has been used in code based cryptosystem to secure information systems from quantum based solutions. In this paper, we generalize solution to the problem using Information set decoding to the Grassmann metric for codes associated with the totally non negative Grassmannian. A new theory linking the planar structure of the totally non negative Grassmannian to Tanner graph like construction was developed using the concept of boundary measurement map was developed. The bounds on the parameters such as the size of the information subspace and intersection array of the

new constructed Non-negative grassmann codes was derived. Thereafter a variant of Information set decoding based on decomposing the Generator matrix into positroid cells using Gaussian elimination to find linearly dependent subsets of the plukcer coordinates with minimal non-zero coordinates and in which the the maximal minor is totally positive was presented. Finally numerical results presented showed that the Non negative Grassmann code had a low decoding probability of failure when compared with an LDPC code. This implies that the error floor of the LDPC code is higher than that of the Non-negative Grassmann code. Also, for increase in the code length, the decoding cost for the totally non negative Grassmann code was higher than the LDPC code. This validates the theory of the Non negative Grassmann code in the Grassmann metric more Indistinguishable secure under the Chosen ciphertext model when compared to the LDPC code in the Hamming metric. Due to its robust security credentials, we recommend this code to construct future post quantum encryption schemes.

REFERENCES

- [1] E. Berlekamp, R. McEliece, and H. Van Tilborg, “On the inherent intractability of certain coding problems (corresp.),” *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 384–386, 1978.
- [2] R. J. McEliece, “A public-key cryptosystem based on algebraic,” *Coding Thv*, vol. 4244, pp. 114–116, 1978.
- [3] P. Gaborit, O. Ruatta, J. Schrek, and G. Zémor, “Ranksign: An efficient signature algorithm based on the rank metric,” in *International Workshop on Post-Quantum Cryptography*, Springer, 2014, pp. 88–107.
- [4] E. Prange, “The use of information sets in decoding cyclic codes,” *IRE Transactions on Information Theory*, vol. 8, no. 5, pp. 5–9, 1962.
- [5] J. Stern, “A method for finding codewords of small weight,” in *International Colloquium on Coding Theory and Applications*, Springer, 1988, pp. 106–113.
- [6] P. Gaborit, O. Ruatta, and J. Schrek, “On the complexity of the rank syndrome decoding problem,” *IEEE Transactions on Information Theory*, vol. 62, no. 2, pp. 1006–1019, 2015.
- [7] T. Etzion and H. Zhang, “Grassmannian codes with new distance measures for network coding,” *IEEE Transactions on Information Theory*, vol. 65, no. 7, pp. 4131–4142, 2019.
- [8] C. T. Ryan and K. M. Ryan, “The minimum weight of the grassmann codes c (k, n),” *Discrete applied mathematics*, vol. 28, no. 2, pp. 149–156, 1990.
- [9] A. Postnikov, D. Speyer, and L. Williams, “Matching polytopes, toric geometry, and the totally non-negative grassmannian,” *Journal of Algebraic Combinatorics*, vol. 30, no. 2, pp. 173–191, 2009.
- [10] R. Tanner, “A recursive approach to low complexity codes,” *IEEE Transactions on information theory*, vol. 27, no. 5, pp. 533–547, 1981.
- [11] R. Koetter and F. R. Kschischang, “Coding for errors and erasures in random network coding,” *IEEE Transactions on Information theory*, vol. 54, no. 8, pp. 3579–3591, 2008.
- [12] T. Etzion and N. Silberstein, “Codes and designs related to lifted mrd codes,” *IEEE Transactions on Information Theory*, vol. 59, no. 2, pp. 1004–1017, 2012.
- [13] F. Chabaud and J. Stern, “The cryptographic security of the syndrome decoding problem for rank distance codes,” in *International Conference on the Theory and Application of Cryptology and Information Security*, Springer, 1996, pp. 368–381.
- [14] G. Kachigar and J.-P. Tillich, “Quantum information set decoding algorithms,” in *International Workshop on Post-Quantum Cryptography*, Springer, 2017, pp. 69–89.
- [15] R. R. Varshamov, “The evaluation of signals in codes with correction of errors,” in *Doklady Akademii Nauk*, Russian Academy of Sciences, vol. 117, 1957, pp. 739–741.
- [16] S. Franco, D. Galloni, and A. Mariotti, “Bipartite field theories, cluster algebras and the grassmannian,” *Journal of Physics A: Mathematical and Theoretical*, vol. 47, no. 47, p. 474004, 2014.
- [17] G. E. Andrews, *q-Series: Their Development and Application in Analysis, Number Theory, Combinatorics, Physics and Computer Algebra: Their Development and Application in Analysis, Number Theory, Combinatorics, Physics, and Computer Algebra*, 66. American Mathematical Soc., 1986.
- [18] E. Gabidulin and N. Pilipchuk, “Subspace network codes with large cardinality,” in *2015 International Conference on Engineering and Telecommunication (EnT)*, IEEE, 2015, pp. 10–13.
- [19] Q. Guo, T. Johansson, E. Mårtensson, and P. S. Wagner, “Some cryptanalytic and coding-theoretic applications of a soft stern algorithm,” *Advances in Mathematics of Communications*, vol. 13, no. 4, p. 559, 2019.
- [20] C. A. Melchor, P.-L. Cayrel, P. Gaborit, and F. Laguillaumie, “A new efficient threshold ring signature scheme based on coding theory,” *IEEE Transactions on Information Theory*, vol. 57, no. 7, pp. 4833–4842, 2011.
- [21] P. Gaborit, A. Hauteville, D. H. Phan, and J.-P. Tillich, “Identity-based encryption from codes with rank metric,” in *Annual International Cryptology Conference*, Springer, 2017, pp. 194–224.
- [22] D. Chang, A. K. Chauhan, S. Kumar, and S. K. Sanadhya, “Revocable identity-based encryption from codes with rank metric,” in *Cryptographers’ Track at the RSA Conference*, Springer, 2018, pp. 435–451.
- [23] T. Lau and C. Tan, “A new technique in rank metric code-based encryption,” *Cryptography*, vol. 2, no. 4, p. 32, 2018.
- [24] W. Beullens, “Not enough less: An improved algorithm for solving code equivalence problems over fq,” Tech. Rep.
- [25] D. J. Bernstein, “Introduction to post-quantum cryptography,” in *Post-quantum cryptography*, Springer, 2009, pp. 1–14.