CIPHERING USING GENERALIZED QUADRANGLES

PAVEL E. BLUMOV ASSISTANT PROFESSOR OF MATHEMATICS
DEPARTMENT OF MATHEMATICS AL-QUSA UNIVERSITY GAZA
PALESTINE

ABSTRACT In this paper we describe a method of making a cryptosystem using generalized quadrangles following a method set in [2]. We examine the system showing that it is secure, and we introduce several examples.

1 INTRODUCTION

Generalized quadrangles arose in two separate areas as special cases of two different theories. They were introduced by J. Tits in 1958 as a special case of what is called generalized polygons. They also arose again in the work of Bose in 1962 in his work about partial geometries. Several classical examples of generalized quadrangles can be defined algebraically; however, the theory is still under investigation. New ones on families of ones are discovered every now and then. In this paper we will define them geometrically then we will introduce the classical ones algebraically and use them to build up a cryptosystem. This paper is follows the theme as in [2].

2 DEFINITIONS AND PRELIMINARIES

For the following definitions we use [3-4]

Definition 2.1: A point-line geometry \( G = (P, L, I) \) is a pair of sets \( P \) and \( L \) is called the set of points and \( L \) is called the set of lines, where members of \( L \) and \( P \) are just subsets of \( P \). If \( P \) is a point belongs to a line \( L \), we say that \( P \) lies on \( L \), and \( L \) passes through \( P \). If \( P \) and \( L \) are incident with \( L \) \( I \) and \( L \) are two points and \( P \) and \( L \) are said by \( P \) and \( L \) are collinear, and this is denoted by \( P \) \( I \) \( L \). Two lines \( L \) and \( L \) are called opposite if there is no common point.
incident point \( P - P.L \) is called linear singular space because each pair of distinct points has exactly one line and it is called partial linear if each pair of points has at most one line.

A subspace of a point-line geometry \( P.L \) is a subset \( M \) of points together with all lines \( \ell \) such that \( \ell \) has at least two points in \( M \) and \( M \) has entirely in \( M \).

A path of length \( k \) from \( P \) to \( Q \) is a set of \( k + 1 \) points \( P = x_0, x_1, x_2, \ldots, x_k = Q \), such that \( x_i \) is collinear with \( x_{i+1} \) \( 0 \leq i \leq k - 1 \).

A geodesic is a shortest path between two points. We define the distance function \( d \) on the set \( X \) by \( d(x, y) \) - the length of any geodesic from \( x \) to \( y \). A subspace \( A \) is called convex if it contains all geodesics between any two points in \( A \). The smallest subspace containing a set \( A \) is called the subspace generated by \( A \) and is denoted by \( \langle A \rangle \). If \( x \) is a point in \( X \), then \( \langle x \rangle \) is an empty subset of \( X \). In addition to \( \langle x \rangle \) itself, a point-line geometry \( P.L \) is called a gamma space if \( \mathbb{R}^2 \) is a subspace for every point \( x \). A polar space is a point-line geometry that satisfies the following:\n
- For each point \( x \) and incident with \( x \), \( \mathbb{R}^2 \) is collinear with \( x \) on all points of \( \mathbb{R}^2 \).

If \( P \) - \( P.L \) is a point-line geometry, then \( Rad(P) \) - \( P.L \) \( A \) \( P.L \) is called the largest integer \( a \) for which there is a chain of singular subspaces \( A = A_1 = A_2 = \cdots = A_A \). Where \( A \) \( A_1 \) \( A_2 \) \( A_3 \) and \( A_A \) \( A_{A_1} \) \( A_{A_2} \) \( A_{A_3} \) are the largest integers for which there is a chain of singular subspaces \( A_1 = A_2 = \cdots = A_A \). Where \( A \) \( A_1 \) \( A_2 \) \( A_3 \) and \( A_A \) \( A_{A_1} \) \( A_{A_2} \) \( A_{A_3} \) are the largest integers for which there is a chain of singular subspaces \( \mathbb{R}^2 \) - \( P.L \) is called a point-line geometry where the familiar terminology used in the frame of geometry is that two lines are called parallel if they have empty intersection.

**Definition** \( A \) - a point-line geometry \( P.L \) is called a generalized quadrangle if it satisfies the following:

- (GQ1) Every point of \( P \) is contained in at most one line \( \ell \) of \( P.L \).
- (GQ2) For each point \( x \) of \( \mathbb{R}^2 \) there is \( \ell \) with \( x \) and \( \ell \) implies that \( x \) is collinear with \( x \) on all points of \( \mathbb{R}^2 \).
Sphering using generalized quadrangles

In a classical finite point set \( P \),

\( G(0) \) defines non-collinear points and non-concurrent lines.

\( G(1) \) is finite.

The classical examples are defined here:

\[ \text{FINITE CLASSICAL GENERALIZED QUADRANGLES} \]

Let \( \Pi = (P, L) \) be a finite classical polar space of rank \( n \) with \( n \geq 2 \).

We shall use the following notation as in [2]:

- \( \text{THE SYMPLECTIC CASE } W_n(q) \) - the polar space arising from a symplectic polarity on \( PG(n, q) \) in \( n \) and \( n \leq 3 \) here \( n = \frac{n-1}{2} \).

- \( \text{THE ORTHOGONAL CASE } Q(2n, q) \) - the polar space arising from a non-degenerate quadric in \( PG(2n, q) \) in \( n \geq 2 \) here \( n = \frac{n-1}{2} \).

- \( \text{THE HYPERBOLIC CASE } Q^-(2n+1, q) \) - the polar space arising from a non-degenerate hyperbolic quadric in \( PG(2n+1, q) \) in \( n \geq 2 \) here \( n = \frac{n-1}{2} \).

- \( \text{THE ELLIPTIC CASE } Q^+(2n+1, q) \) - the polar space arising from a non-degenerate elliptic quadric in \( PG(2n+1, q) \) in \( n \geq 2 \) here \( n = \frac{n-1}{2} \).

- \( \text{THE UNITARY CASE } U(n, q^2) \) - the polar space arising from a non-degenerate Hermitean form on \( PG(n, q^2) \) in \( n \geq 3 \) here \( n = \frac{n-1}{2} \).

Let \( P \) denote the number of points of \( P \) and let \( S(P) \) be the set of all maximal totally singular subspaces of \( P \). All members of \( S(P) \) have projective dimension \( n-1 \). Let the following theorem state [2]:

**Theorem 3.** The numbers of points of the finite classical polar spaces are given by the formulae:

\[
\begin{align*}
W_n(q) &= q^{n+1} - 1 \quad \frac{1}{q-1} \\
Q(2n, q) &= q^n - 1 \quad \frac{1}{q-1} \\
Q^-(2n+1, q) &= q^n - 1 \quad \frac{1}{q-1} \\
Q^+(2n+1, q) &= q^n - 1 \quad \frac{1}{q-1} \\
\end{align*}
\]
Theorem 3.2] The numbers of maximal totally singular subspaces of the finite classical polar space are given by the formulae:

\[
S(W_2(q)) \quad - \quad q = 1, \quad \frac{q - q^2}{(q - 1)^2} \quad \text{if } q \neq 2
\]

\[
S(Q(2n, q)) \quad - \quad q = 1, \quad \frac{(q^n - 1)(q^2 + 1)}{(q + 1)} \quad \text{if } q \neq 2
\]

\[
S(Q(2n + 1, q)) \quad - \quad q = 1, \quad \frac{(q^n - 1)(q^2 + 1)}{(q + 1)} \quad \text{if } q \neq 2
\]

\[
S(H(2n, q^2)) \quad - \quad q = 1, \quad \frac{(q^n - 1)(q^2 + 1)}{(q + 1)} \quad \text{if } q \neq 2
\]

\[
S(H(2n + 1, q^2)) \quad - \quad q = 1, \quad \frac{(q^n - 1)(q^2 + 1)}{(q + 1)} \quad \text{if } q \neq 2
\]

**Corollary 3.3** In the case \( q = 2 \) we get a generalized quadrangle. It follows that the number of points and number of lines in respecting cases are:

\[
W_2(q) : \quad q + 1 \quad \frac{q - q^2}{(q - 1)^2} \quad \text{if } q \neq 2
\]

\[
Q(4, q) : \quad q + 1 \quad \frac{q - q^2}{(q - 1)^2} \quad \text{if } q \neq 2
\]

\[
Q^+(3, q) : \quad q + 1 \quad \frac{q - q^2}{(q - 1)^2} \quad \text{if } q \neq 2
\]

\[
Q^-(3, q) : \quad q + 1 \quad \frac{q - q^2}{(q - 1)^2} \quad \text{if } q \neq 2
\]

**Definition 3.5** A spread of a CQ is a collection of pairwise non-intersecting lines whose union is the whole set of points of the CQ.

**Remark 3.6** Note that \( W_2(q) \) and \( Q(4, q) \) are dual to each other and that any selection \( q \neq 2 \) of \( q \neq 2 \) is in \( H(3, q^2) \) if \( Q(3, q) \) is also in \( H(3, q^2) \) and \( Q(3, q) \) has a spread.

**IV. MAIN RESULT**

We will use a generalized quadrangle to build a cryptosystem that can stand by itself and if can be combined with other systems to get a more-resistant system.

**The Cryptosystem** Let \( Q = \{ P, L \} \) be a generalized quadrangle and \( L \) be a line in \( Q \). Let \( P \) be a point not on line \( L \) such that \( P \) is opposite to \( L \) and \( L \) is opposite to \( P \) and the line \( L \) is a point on line \( L \) and \( P \). Then by the definition of \( CQ \), there is a unique point \( P \) on the line \( L \) that
Ciphersing using generalized quadrangles

It will mean to say last iteration to being the sequence where \( i \) is the point on \( L \) that is collinear to \( u \).

**Definition 1.** Let \( L = \{l_1, l_2, \ldots, l_n\} \) be a system of consecutive-opposite lines (in short co-system). The path \( \{x_0, x_1, \ldots, x_n\} \) generated using the system of lines \( L \) where \( x_0 \rightarrow l_1 \rightarrow x_1 \rightarrow l_2 \rightarrow \ldots \rightarrow x_n \rightarrow l_1 \), \( l_n \) and \( l_0 \) are taken modulo \( n = 1 \) is called the path \( [x_0, x_n] \) in the system \( L \) and is denoted by \( (x_0, x_n) \). The function \( f : x \rightarrow f(x) \) defined by \( f(x) = x + 1 \) \( \mod n \) is called the function of the system \( L \).

**Lemma 1.** Let \( L \) be a co-system then the function of the system \( L \) is injective.

**Proof:** For any pair of opposite lines \( l_1 \) and \( l_2 \), if \( x_1 \) and \( x_2 \) are both on \( L \), \( \{x_1, x_2\} \) is a point and \( x_1 \neq x_2 \). Therefore, by (Q2), there is a unique point \( x \) such that \( f(x) = x \). Thus, the function \( f : x \rightarrow f(x) \) defined by \( f(x) = x + 1 \mod n \) for \( x \rightarrow l_1 \) \( \mod n \) is all injective. \( f \) is the composition of all the \( f_{x_i} \)’s times \( f \) is injective.

**Definition 2.** A \( GC \) is called regular with parameters \( s, t \) if every point is incident with \( s + 1 \) lines and every line is incident with \( s \) \( \geq 1 \) points.

Some numerical facts about regular \( GCs \)

**Lemma 2.** Let \( L \) be a regular \( GC \) with parameters \( s, t \). Then we have the following:

1. \( p > 1 \) if \( p = 1 \) for any pair of non-collinear points \( x, y \).
2. \( p = t = 1 \) if \( s = 1 \) and \( s = 1 \) and \( p = 1 \) if \( s = 1 \).
3. \( s = 1 \) if \( s = 1 \).
4. \( s = 1 \) if \( s = 1 \) and \( s = 1 \) and \( s = 1 \).

**Proof:** See 1.

**Lemma 3.** Let \( y \) be a point \( y \) not on \( L \) at least \( t + 1 \) times opposite to \( x \).

**Proof:** It is collinear to exactly one point \( x \) if \( y \) has exactly one line \( y \) intersecting \( L \) and since there are \( s \) \( \leq 1 \) times \( x \) has \( s \) \( \leq 1 \) times opposite to \( y \).
Lemma 4.1.6. Let $\ell$ be a line and $A$ a point on $\ell$ such that there are $a$ lines opposite to $\ell$.

Proof. Each line $l$ has $a = 1$ points on $\ell$ such that every point outside $\ell$ has $a$ lines opposite to $\ell$. But every line has $a = 1$ points. Therefore we have $a^2$ lines opposite to $\ell$.

Example 4.1.7. Let $\ell = \{1, 2, 3, 4, 5\}$ and $A = \{1, 2, 3\}$. Then $\ell$ has $a = 1$ points on $\ell$. Every point outside $\ell$ has $a = 1$ lines opposite to $\ell$.

Among these $a^2$ lines there are $b$ lines parallel to each other.

Example 4.1.8. Let $\ell = \{1, 2, 3\}$ and $A = \{4, 5\}$. Then $\ell$ has $a = 1$ points on $\ell$. Every point outside $\ell$ has $a = 1$ lines opposite to $\ell$. It follows that $a = -2$, $a = -2$, and $a = -2$. Thus $\ell$ is parallel to $A$.

Of course, the last example is not an example of real lines that can be used for the purpose of encryption, but it is more complicated.

Lemma 4.1.9. Let $\ell$ be a line and $A$ a point on $\ell$. Then there is a co-system such that $f(\ell) = A$.

Proof. If $\ell$ is collinear to $A$, then choose a line $\ell_1$ on $\ell$, and by the previous lemma there are $a$ lines on $\ell$ that are opposite to $\ell_1$. It follows that there is a line $\ell_2$ opposite to $\ell_1$ with $f(\ell) = A$.

If $\ell$ is not collinear to $A$, let $\ell_1$ and $\ell_2$ be two opposite lines on $\ell$. Then the existence of these lines was possible by previous lemma. Now since $\ell_1$ is not collinear to $\ell$, there are $a = 1$ points on $\ell_1$. Choose a point $x \in \ell_1 \cap A$. There are $a$ lines altogether. Since $\ell_1$ is not collinear to $\ell$, there are at least $a$ lines on $\ell_1$. Intersecting $\ell_1$ and $\ell_2$, there is a common opposite line to both, $\ell_1$ and $\ell_2$.

What is good about this system?

1. It is not easily analyzed statistically.
2. It withstands any plaintext-ciphertext attacks.
3. The key-space is very large.
4. The plaintext and ciphertext spaces are very large.
5. The unpredictability of the system is high.

Explanation
Ciphering using generalized quadrangles

1. Since the whole message is being inserted in one point there is no meaning of doing letter frequency.
2. Knowing $z, f(z)$ in some point $a$, will not determine $f$. If $\mathcal{G}$ is a genus, the space consists of all possible cosystems which is very large, space of genus for large parameters $s \geq 1$.
3. The plantext and ciphertext spaces are the set of points of the line $\mathcal{G}$ of cardinality $s = 1$. Thus the large space is large and in addition to the fact that the whole message is encoded in one point.
4. The whole $\mathcal{G}$ might be brand new Since there is no classification of $\mathcal{G}$ Thus the best one can not be predicted.

5. THE CLASSICAL CASES

In all the classical cases we may calculate the function $f$ in the following way.

We know that the line is a totally isotropic 2-dimensional vector space. It means that any line is a projective space and its points can be represented by $[u, v] = [x, y]$. Where $[x, y]$ is a basis of the 2-space corresponding to the line $[u, v]$, an element $\alpha$ of the field on which the vector space is defined, or we may suppose that the lines are $[u_0, v_0], [u_1, v_1], [u_2, v_2], \ldots, [u_n, v_n]$.

Now we find the point $1, a_1$ that corresponds to $1, a_0$ we have to have

$B(u_0, v_0) = a_0 B(v_0, u_0)$
$B(u_0, u_1) = B(a_0 v_0, u_1) = B(u_0, a_1 v_1) = B(v_0, a_1 v_1) = B(v_0, v_1) = 1$
$B(u_0, u_1) = a_0 B(v_0, u_1) = a_0 B(u_0, v_1) = 1$

Thus $z = -\frac{B(u_0, v_1) + a_0 B(v_0, u_1)}{B(v_0, u_1) + a_0 B(v_0, v_1)}$

Note that the denominator can be made not to equal zero by careful
The choice of the system

It follows that we have the general inductive relation

\[
2^n = \frac{B(u_{n-1},u_1) + B(u_{n-1},u_0)}{B(u_{n-1},u_1) + B(u_{n-1},u_0)}
\]

Then implement this system i.e. for the classical example of \( \mathbb{Q} \) see \( \mathbb{Q}^2(0,0) \) this means that we have a vector space \( \mathbb{V} \) of dimension \( n \) over the finite field \( \mathbb{GF}(q) \) equipped with a hyperbolic bilinear form \( \langle u, v \rangle = \langle u, v \rangle_{\mathbb{V}} \), where the points \( \mathbb{Q} \) of \( \mathbb{GF}(q) \) are the \( n \)-dimensional isotropic subspaces of \( \mathbb{V} \) and the lines of \( \mathbb{Q} \) are the \( (n-1) \)-dimensional subspaces of \( \mathbb{V} \). Parallel lines mean that the intersection of the corresponding 2-subspaces is the zero vector. Two points are collinear if the corresponding two 1-spaces form a totally isotropic 2-dimensional subspace.

In addition the question: how to insert the plaintext in the point \( \mathbb{Q}^2 \) has to be addressed. To answer this question we refer to the classical examples of where points are vector subspaces so it is easy to insert the plaintext inside the vector as a component. To make this idea clear let us consider the following example: let \( \mathbb{Q}^2 \) be the vector space of dimension 2 defined over the field \( \mathbb{GF}(2) \) equipped with the scalar product \( \langle, \rangle \). It follows that \( \mathbb{Q}^2 \) becomes an orthogonal space \( \mathbb{Q}^2(5,2) \) if it has 15 points and 16 lines.

Let our plaintext be \( \text{pt} = (1, 0, 0, 0) \) and let the 1-dimensional spaces of the 2-dimensional subspace \( \{1 1, 0 0, 0 0, 1 0\} \) be arranged in the following way:

1. \( \langle 1, 1, 0, 0 \rangle = 0 \times (0, 0, 1, 0) \)
2. \( \langle 0, 1, 0, 0 \rangle = 0 \times (0, 0, 1, 0) \)
3. \( \langle 0, 1, 1, 0 \rangle = 0 \times (0, 0, 1, 0) \)
4. \( \langle 1, 1, 1, 0 \rangle = 0 \times (0, 0, 1, 0) \)

Let our plaintext be \( \text{pt} = (1, 1, 0, 0) \) and let the 1-dimensional subspaces \( \{1 1, 0 0, 0 0, 1 0\} \) be arranged in the following way:

1. \( \langle 1, 0, 0, 0 \rangle = \alpha \times (0, 0, 1, 0) \)
2. \( \langle 0, 1, 0, 0 \rangle = \alpha \times (0, 0, 1, 0) \)
3. \( \langle 0, 1, 1, 0 \rangle = \alpha \times (0, 0, 1, 0) \)
4. \( \langle 1, 1, 1, 0 \rangle = \alpha \times (0, 0, 1, 0) \)

It follows that:

\( \text{pt} = (1, 1, 1, 0) \)
Ciphering using generalized quadrangles

\[ \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix} \]

which corresponds to the ciphertext \([1, 0, 1, 0, 1] \). Therefore \( x = 1 \).

In fact the last two examples are isomorphic since both represent the generalized quadrangle \( G_q(4, 2) \).

For real examples we take a large field for example \( GF(C) \) where \( C \) consists of 100 digits, then we write \( n \) plaintext as blocks of length less than 100 digits each.

This system may work by itself or in conjunction with RSA cryptosystem.

Warning: Although this cryptosystem can be implemented for any number of parallel lines however there are cases that should be avoided such as the cases where the parallel lines are a grid.

Remark: Let \( C \) be a set in the corollary that shows the number of points on lines in each \( G_q \), there are many possibilities of choices for parallel lines they represent the key for this system.

REFERENCES

2. Muhammad EI-Attar, *Ciphering using \( P_{2n}(4) \) and \( P_{2n}(2) \)*, Australian Information Warfare and Security Conference (AUSIWSEC 2001)
4. Cohen A. 1993 *Handbook of incidence geometry*