Ciphering Using residue of metasymplectic space $F_{4,1}(q)$

Dr. Osama A. Al-Absi *
Prof. Mohammed El-Atrash **

ABSTRACT

Let Q_0, Q_1,…, Q_n be a family of n+1 quads in parapolar space that satisfies the following:

For each point x in a quad Q_i, we have $x^{\perp} \cap Q_j$ is a single point, $i \neq j$.

Let x_0 be a point in Q_0 then there is a point $x_1 \in Q_1$, with $x_1 = x_0^{\perp} \cap Q_1$, define by induction $x_{i+1} = x_i^{\perp} \cap Q_{i+1}$, $i = 0, 1, \ldots, n$, (indices are taken modulo n). To encipher we match x_0, to x_{n+1}, and to decipher we go back from x_{n+1} to x_1 using the corresponding quad.

One geometry that satisfies the rule is the residue of metasymplectic space (a dual polar space). In this work we construct the dual polar space and explain how to make up the cipher system using this geometry.

* Department of Mathematics - Al-Aqsa University Gaza, Palestine, Email: osama-absi@hotmail.com.

** Department of Mathematics - Islamic University of Gaza- Gaza, Palestine.

INTRODUCTION:

Ciphering has existed for thousands of years. One of the first known uses in about 1900 BC. An Egyptian scribe used non-standard hieroglyphs while inscribing. Simple substitutions by scribes in Mesopotamia dating about 1500 BC were discovered long time ago. Writing was a safe means of communication because few people could read. Julius Caesar used simple substitutions by shifting letters in the alphabet, off setting (or shifting) 3-letters. But now, in the era of information technology. One of the means to protect information from any person is to encipher this information. Many authors have written many papers about information and computer security, by using various methods of algebra. This is one to add to the literature in this field. What is special about this paper is the use of geometric properties instead of algebraic ones to implement the cipher system. This paper is meant to be self-contained. Some of the material contained here can be found in other sources. The geometric properties that we will use can be derived from the algebraic structure. For more information about the metasymplectic space see [Uzal], [Co] [JT] [CC].

2.1 Basic geometry Definitions:

Given a set *I*, a geometry Γ over *I* is an ordered triple $\Gamma = (X, *, D)$, where X is a non-empty set, D is a partition $\{X_i\}$ of X indexed by *I*. X_i are called components, and it satisfies the following condition:

$x * y$ implies that either x and y belong to distinct components of X or $x = y$.
Elements of X are called objects of geometry, and the objects within one component X_i of the partition are called the object of type i. The subscripts, which index the components, are called types. The obvious mapping $\tau : X \to I$ that takes each object to the index of the component of the partition containing it is called the *type map* τ.

A point-line geometry $\Gamma = (P, L)$ is a pair of sets, P is called the set of "*points*" and L is called the set of "*lines*", where members of L are just subsets of P. If *p* is a point belongs to a line *l* we say that *p lies on l* or *l passes* through *p* or *p* is *incident* with *l*. If *p, q* are two points on one line *l* we say that *p* and *q* are *collinear* and this is denoted by $p \sim q$. $\Gamma = (P, L)$ is called *linear* (*singular*) space if each pair of distinct points lie exactly on one line. Γ is called *partial* (or *near*) linear if each pair of points lie on at most one line. A *subspace* of a point-line geometry $\Gamma = (P, L)$ is a subset X of points together with all lines *l* in L such that if *l* has at least two points of

X then l lies entirely in X. A *path* of length k from x_0 to x_k is a set of k +1 points $x_0, x_1, x_2, \ldots, x_k$, such that x_i is collinear with x_{i+1}, i = 1, 2, 3, ..., k-1. A *geodesic* is a shortest path between two points. We define the *distance function d*: $P \times P \rightarrow Z^+$ **(**non-negative integers**)** by d(x, y) = the length of any geodesic from x to y. A subspace X is called *convex* if it contains all geodesics between any two points of X. The smallest subspace containing a set X is called the *subspace generated* by X and is denoted by $\langle X \rangle$. If p is a point, $p^{\perp}$ means all point collinear with p in addition to p itself. $\Delta_k(p) = \{x \in P \mid x$ is at distance k from $p\}$. $\Delta^*_k(p) = \{x \in P \mid x$ is of distance at most k from $p\}$. Let Γ be point-line geometry. A *geometric hyperplane* of Γ is a proper subspace with the property that every line of Γ meets it in at least one point. A hyperplane of Γ is a maximal proper subspace of Γ.

2.2 Some basic space

$\Gamma = (P, L)$ is called a gamma space if $x^{\perp}$ is a subspace for every point $x \in P$ **.**

A *polar space* is a point-line geometry that satisfies the following Buekenhout- Shult axiom:

(B-S) *For each point p not incident with a line l; p is collinear with one or all points of l.*

If $\Gamma = (P, L)$ is a point-line geometry; $Rad(\Gamma) = \{ q \in P \mid p$ collinear to q for all $p \in P\}$. *Rank* of Γ is the largest integer n for which there is a chain of singular subspaces $\{X_i\}$, i = 1, 2, ..., n. such that:

$X_1 \subset X_2 \subset \ldots \subset X_n$, where $X_i \neq X_j$, $i \neq j$.

If there is no such integer; the rank of Γ is infinite. If Γ is a polar space and $Rad(\Gamma) = \varnothing$, then Γ is called *non-degenerate* polar space; otherwise Γ is called *degenerate* polar space. A point-line geometry is called a *parapolar space* of rank $r + 1$, $r \geq 2$; if it satisfies the following conditions:

(PP1) Γ is a connected gamma space.

(PP2) for every line l; $l^{\perp}$ is not a singular space.

(PP3) for every pair of distinct points x, y; $x^{\perp} \cap y^{\perp}$ is either empty, a point, or a non-degenerate polar space of rank r.

A *strong parapolar* space is a parapolar space in which $x^{\perp} \cap y^{\perp}$ is a polar space for every pair of points distinct x, y of distance 2 apart.

If x, y are two points of a parapolar space; (x, y) is called a *special pair* if $x^{\perp} \cap y^{\perp}$ is just one point, and (x, y) is called a polar pair if $x^{\perp} \cap y^{\perp}$ is a non-degenerate polar space of rank at least 2.

Let *p* be a point in a point-line geometry Γ = (P, L**)**; *Residue* of Γ at *p* denoted by Γ_p or Res(*p*); is a point-line geometry (P_p, L_p) defined as follows: P_p is the set of all lines containing *p*; a member of L_p is the set of all lines containing *p* and contained in a plane (singular space of rank 3).

2.3 Definition:

(Metasymplectic space). A metasymplectic space is a set P in which some subsets called lines, planes, and symplecta are distinguished, and satisfy the following axioms:
(M1) the intersection of distinct symplecta is empty, a point, a line, or a plane.
(M2) A symplecton S together with its "singular spaces"; points, lines, and planes contained in S is a polar space of rank 3.

(M3) Considering the set x* of all symplecta containing a given point $x \in P$, and calling lines (resp. Planes) of x*. The subset of x* consists of all symplecta of x* containing a plane (resp. a line) through x, we obtain a polar space of rank 3.

2.4 Basic Algebraic Definitions and Notations:

Let V be a vector space of finite dimension n over an arbitrary field F.

A *bilinear form* B on V is a mapping
$B: V \times V \rightarrow F$, such that for $\alpha, \beta \in F$; $x, y, z \in V$ we have :
$B(\alpha x + \beta y, z) = \alpha B(x, z) + \beta B(y, z)$.
$B(z, \alpha x + \beta y) = \alpha B(z, x) + \beta B(z, y)$
Thus a bilinear form is a linear functional in each of this coordinate.
If $B = \{e_1, e_2, \ldots, e_n\}$ is a finite basis for a finite-dimensional vector space V, and if B is a bilinear form on V, the matrix of B relative to the ordered basis *B* is the $n \times n$ matrix with entries $b_{ij} = b(e_i, e_j)$. We shall denote this by $[B]_B$ and is called the *grammian matrix* of B, relative to *B.*
For a subspace W of V; we set
$W^{\perp}_L = \{u \in V: B(u, v) = 0$, for all vector $v \in V\}$
$W^{\perp}_R = \{u \in V: B(v, u) = 0$, for all vector $v \in V\}$
$W^{\perp}_L$, $W^{\perp}_R$ are called left and right radicals respectively of W with respect to B.
A bilinear form B is called *symmetric* if B(u, v) = B(v, u) for all vector u, v $\in$ V. A bilinear form B is called *alternate form* iff B(u, u) = 0 , $u \in V$. B is called a *skew-symmetric form* if B(u, v) = - B(v, u) for every $u, v \in V$.

Let B be a symmetric or alternate bilinear form defined on a vector space V over an arbitrary field F. For (a subspace) $W \subset V$; we set
$W^{\perp} = \{u \in V: B(u, v) = 0, \text{ for all vectors } v \in V\}$. $V^{\perp}$ is called *radical* of V with respect to B. A bilinear form B on a vector space V is called *non-degenerate* iff $V^{\perp} = \{0\}$. Otherwise B is called *degenerate*.
Two forms B_1, B_2 on V are said to be equivalent if there is a one-to-one and onto linear transformation $\psi : V \to V$ such that: $B_1(u, v) = B_2(\psi(u), \psi(v))$.

A vector $u \in V$ is called an *isotropic* vector, if $B(u, u) = 0$, and a subspace W of V is called *totally isotropic* (abbreviated TI) subspace of V if $B(u, v) = 0$ for all $u, v \in W$. If a TI subspace W of V is not contained properly in any TI subspace of V; W is called *maximal totally isotropic* (abbreviated MTI) subspace of V.

It can be shown (see Bierbrauer (1997)) that all the MTI subspaces have the same dimension it is called witt index of V and is denoted by ind(V). Two vectors u, v are called orthogonal if $B(u, v) = 0$.

A 2-dimensional vector space with non-degenerate bilinear form B, in which there is an isotropic vector u is called a *hyperbolic plane*, otherwise it is called *anisotropic* plane.

A vector space V of dimension 2n is called *hyperbolic* if V is endowed with a symmetric bilinear form of witt index n, and is called *elliptic* if witt index is n –1.

The following two Theorems explain the structure of vector spaces endowed with bilinear forms. [see Bierbrauer (1997)].

2.4.1 Theorem [Bj]:

Let B be a non-degenerate symmetric bilinear form on a vector space V of dimension 2n over a finite field F. Then B is a hyperbolic form on V iff V has a basis A, such that $V = H_1 \perp H_2 \perp \ldots \perp H_n$, *where all* H_i *are hyperbolic planes,* $i = 1, 2, \ldots, n$ *with ind(V) = n.*

It shows that all hyperbolic non-degenerate symmetric bilinear forms on a certain vector space are equivalent.

2.4.2 Theorem: [Bj]:

For n = 2r, r odd integer, let (,) be the Euclidean scalar on a vector space of dimension n over the finite field of odd order k. Then
(i) (,) is a hyperbolic form iff k = 1 (mod4)
(ii) (,) is an elliptic form iff k = 3 (mod4)
And for n = 2r, r even integer, or q is even (,) is always a hyperbolic form.

3.1 Dual polar spaces [CC]

From the definition of the Metasymplectic space the residue of Metasymplectic space at any point is dual polar space (C_3).

The dual polar space is the space whose point are maximal singular spaces of classical polar space of rank at least two, line are all totally singular subspaces of dimension one less than the dimension of a maximal singular space. All symplecta of these geometries are generalized quadrangles (Quads) **[Uzal]**

(p) : In a parapolar space $\Gamma = (P, L)$, if x_0, x_1, x_2, x_3, x_4, are five points in P, we say that $(x_0, x_1, x_2, x_3, x_4)$ is a *pentagon* if x_i is collinear with x_{i+1}. We say that $(x_0, x_1, x_2, x_3, x_4)$ is **a** *pentagon with no diagonals*, if $(x_0, x_1, x_2, x_3, x_4)$ is a pentagon such that x_i is neither collinear with x_{i+2} nor to x_{i+3}, $i = 0, 1, 2, 3, 4$ (indices are taken mod. 5). We say that Γ satisfy *pentagon property***,** (p) If x_0, x_1, x_2, x_3, x_4 are five points in a parapolar space $\Gamma = (P, L)$, with no diagonals then x_i is collinear to one point on the line $x_{i+2}x_{i+3}$ (indices are taken modulo 5).

3.2 Lemma: [CC]:

Let Γ (P, L) dual polar space, of rank 3 the following holds.

(a) Γ is a gamma space whose lines are maximal cliques

(b) (P) holds.

(c) Each pair of points at mutual distance 2 is contained in a unique quad.

(d) Each pair of quads has either empty intersection or meets in a line.

(e) For any point $x \notin Q \Rightarrow x^{\perp} \cap Q = \varnothing$ or one point.

(f) The diameter of Γ is 3.

Note: This lemma is true for the dual polar space that comes from thick polar space of rank 3.

4.1EXAMPLES OF FINITE CLASSICAL POLAR SPACES:[JT]

Let V be a vector space over a finite field F = GF(q), q is a prime power.

Symplectic Geometry:

$W_n(q)$ is the point-line geometry (P, L), where P is the set of all one dimensional subspaces $\langle x \rangle$ of V, and L is the set of all two dimensional subspaces $\langle x, y \rangle$ for which $B(x, y) = 0$, for a symplectic bilinear form B. In this case n is even, the polar space is of rank n/2.

Hyperbolic Geometry:

$\Omega^{+}_{n}(q)$ is the point-line geometry (P, L), where P is the set of all one dimensional subspaces $\langle x \rangle$ of V for which $B(x, x) = 0$, and L is the set of all two dimensional subspaces $\langle x, y \rangle$ for which

$B(x, y) = 0$, for a hyperbolic bilinear form B. In this case n is even, the polar space is of rank n/2.

Elliptic Geometry:

$\Omega^-_n(q)$ is the point-line geometry (P, L), where P is the set of all one dimensional subspaces $\langle x \rangle$ of V for which B(x, x) = 0, and L is the set of all two dimensional subspaces $\langle x, y \rangle$ for which B(x, y) = 0, for a elliptic bilinear form B. In this case n is even, the polar space is of rank (n/2) - 1.

ORTHOGONAL GEOMETRY:

$\Omega_n(q)$ is the point-line geometry (P, L), where P is the set of all one dimensional subspaces $\langle x \rangle$ of V for which B(x, x) = 0, and L is the set of all two dimensional subspaces $\langle x, y \rangle$ for which B(x, y) = 0, for an orthogonal bilinear form B. In this case n is odd, the polar space is of rank (n-1)/2.

Hermitian Geometry:

$H^+_n(q^2)$ is the point-line geometry (P, L), where P is the set of all one dimensional subspaces $\langle x \rangle$ of V for which B(x, x) = 0, and L is the set of all two dimensional subspaces $\langle x, y \rangle$ for which B(x, y) = 0, for a Hermitian bilinear form B. In this case n is even, the polar space is of rank n/2.

Hermitian Geometry:

$H^-_n(q^2)$ is the point-line geometry (P, L), where P is the set of all one dimensional subspaces $\langle x \rangle$ of V for which B(x, x) = 0, and L is the set of all two dimensional subspaces $\langle x, y \rangle$ for which B(x, y) = 0, for a Hermitian bilinear form B. In this case n is odd, the polar space is of rank (n-1)/2.

4.2 Theorem: [Th]

The number of points of the finite classical polar spaces are given by the following formulae:

$|W_{2n}(q)| = (q^{2n} - 1) / (q - 1)$,
$|\Omega(2n + 1, q)| = (q^{2n} - 1) / (q - 1)$,
$|\Omega^+(2n, q)| = (q^{2n} + 1)(q^n - 1) / (q - 1)$,
$|\Omega^-(2n, q)| = (q^{n-1} - 1)(q^n + 1) / (q - 1)$,
$|H^-(2n + 1, q^2)| = (q^{2n+1} + 1)(q^{2n+1} - 1) / (q^2 - 1)$,
$|H^+(2n, q^2)| = (q^{2n} - 1)(q^n + 1) / (q^2 - 1)$,

4.3 Theorem: [Th]

The numbers of maximal totally isotropic subspaces or maximal singular subspaces of the finite classical polar spaces are given by the following:

$|W_{2n}(q)| = (q + 1)(q^2 + 1)\ldots(q^{(n+1)/2} + 1)$,
$|\Omega(2n + 1, q)| = (q + 1)(q^2 + 1)\ldots(q^n + 1)$

$|\Omega^{+}(2n, q)| = 2(q + 1)(q^2 - 1) \ldots (q^n + 1)$,
$|\Omega^{-}(2n, q)| = (q^2 + 1)(q^3 + 1) \ldots (q^{2n+1} + 1)$,
$|H^{-}(2n +1, q^2)| = (q^3 + 1)(q^5 + 1) \ldots (q^{2n+1} + 1)$,
$|H^{+}(2n, q^2)| = (q + 1)(q^3 + 1) \ldots (q^{2n+1} + 1)$,

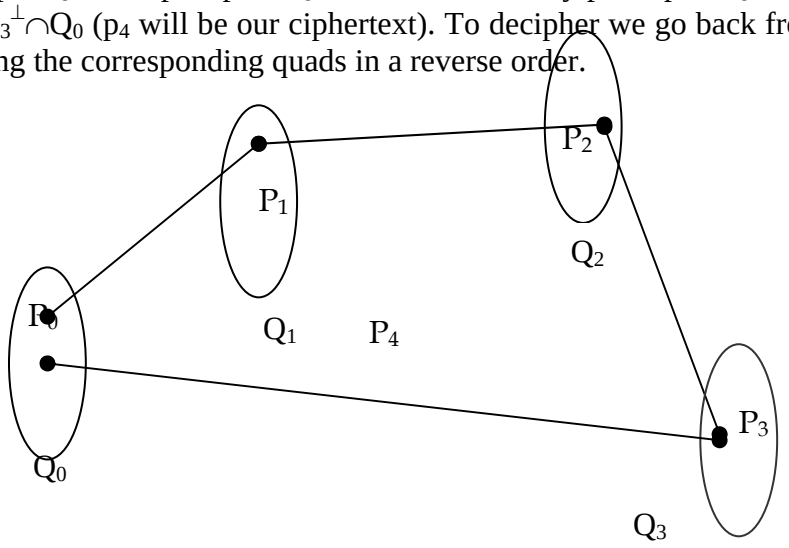
Table 1. The table below lists the number of point, quad and the numbers of points in each quad in dual polar space of rank 3.

Type	# of points	# of quad	# of points in each quads
$W_6(q)$	$(q+1)(q^2+1)(q^3+1)$	$(q^6 - 1) / (q - 1)$	$(q^4 - 1) / (q - 1)$
$\Omega(7, q)$	$(q+1)(q^2+1)(q^3+1)$	$(q^6 - 1) / (q - 1)$	$(q^4 - 1) / (q - 1)$
$\Omega^{+}(6, q)$	$2(q+1)(q^2+1)(q^3+1)$	$(q^2+1)(q^3-1) / (q - 1)$	$(q+1)(q^2-1) / (q - 1)$
$\Omega^{-}(6, q)$	$(q^2+1)(q^3+1)(q^4+1)$	$(q^2-1)(q^3+1) / (q - 1)$	$(q-1)(q^2+1) / (q - 1)$
$H^{-}(7, q^2)$	$(q^3+1)(q^5+1)(q^7+1)$	$(q^7+1)(q^7-1) / (q^2 - 1)$	$(q^5+1)(q^5-1) / (q^2 - 1)$
$H^{+}(6, q^2)$	$(q+1)(q^3+1)(q^5+1)$	$(q^6 - 1)(q^6+1) / (q^2 - 1)$	$(q^4 - 1)(q^4+1) / (q^2 - 1)$

5. Construction of the cipher system:

5.1 Definition:

Two distinct quads are called parallel, if $x \in Q_1 \Rightarrow x^{\perp} \cap Q_2$ = one point. Let Q_0, Q_1, Q_2 Q_3, be four parallel quads in dual polar space $C_{3,3}(q)$, let p_0 be a point in Q_0 (p_0 will be our plaintext). It follows by lemma, that there is a point $p_1 \in Q_1$, with $p_1 = p_0^{\perp} \cap Q_1$. Define inductively $p_{i+1} = p_i^{\perp} \cap Q_i$, $1 \le i \le 3$, $p_4 = p_3^{\perp} \cap Q_0$ (p_4 will be our ciphertext). To decipher we go back from p_4 to p_0 using the corresponding quads in a reverse order.



Next, we will discuss several aspects of this crypto system including implementation of the system, level of security of the system, complexity of the system.

Clearly, the system is a private key system, in which the sequence of quad Q_1, Q_2 Q_3, must be kept secret as the key of the system.

The message space and the ciphertext space is Q_0.

5.2 Example:

Let q = 2, then points of $C_{3,3}(2)$ are totally isotropic 3-space of 7-dimensional vector space, lines are totally isotropic 2-space and quads are totally isotropic 1-spaces.

So, points can be represented by 3x7, matrix containing as rows the basis of totally isotropic space, and a quad is 1-dimension space so it can be represented by 1x7 matrix. M.

It is enough to show how to calculate p_1 from p_0, Q_0 and Q_1. In a similar fashion we calculate the rest of p_2, p_3, p_4.

We know that, both p_0, p_1 corresponds to two maximal totally isotropic 3-subspace of a 7-space. It follows that both that can be represented by tow 3x7 matrices N_0, N_1 respectively, where rows of N_i represent a basis for p_i, i = 0, 1.

We know also that Q_0 corresponds to a totally isotropic 1-space $\{u_0\}$, and Q_1 corresponds to a totally isotropic 1-space $\{u_1\}$. We may assume without loss of generality that rows of N_0 are $\{w_1, w_2, w_3\}$, and rows of N_1 are $\{u_1, u_2, u_3\}$.The line that passing through p_0, p_1 corresponds to a totally isotropic 2-space

$$X = u_1^{\perp} \cap \langle w_1, w_2, w_3 \rangle.$$

It follows that the line p_0 p_1 corresponds to a totally isotropic 3-space $\langle u_1, X \rangle$.

To determine X, we need to find a two totally isotropic 2-spaces $\{u_2, u_3\}$.

This can be achieved by finding a basis of the solution set of the following equation

$$w.w_4 = 0, \quad (1),$$

where $w = aw_1 + bw_2 + cw_3$.

Thus, we are looking for two independent solution of the equation (1) that can be rewritten as:

$a(w_1.u_1) + b(w_2.u_2) + c(w_3.u_3) = 0.$ (2)

Coefficients of equation (2) are known.

It follows that the whole system turned out to be finding out 2 solutions of a system of equation (2). The solution can be calculated by any method like Gauss elimination method.

As for the complexity of the system, not much should be said about that, since clearly from the computations that this system, is as complex as DES system. To break such system it requires the solution of equation in n variables of degree 3, which is considered as a hard problem as the DES system. In fact we can add that the security level of such system is very high, because of huge key space, and the arbitrariness of u_1,q.

For example let $p_0 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}$

$Q_1 = (0\ 0\ 1\ 1\ 1\ 0\ 1) = u_1$

Now, $w = aw_1 + bw_2 + cw_3$,

$u_1.w = a(w_1.u_1) + b(w_2.u_2) + c(w_3.u_3) = 0$

$= a + b + c = 0$

So let $a = 0, b = 1 \rightarrow c = 1$

$a = 1, b = -0 \rightarrow c = 1$

It mean that $u_2 = (0\ 0\ 1\ 1\ 1\ 1\ 0) + (1\ 1\ 0\ 0\ 1\ 1\ 0) = (1\ 1\ 1\ 1\ 0\ 0\ 0)$,

And $u_3 = (1\ 0\ 1\ 0\ 1\ 0\ 1) + (1\ 1\ 0\ 0\ 1\ 1\ 0) = (0\ 1\ 1\ 0\ 0\ 1\ 1)$.

It follows that $p_1 = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}$

Let $Q_2 = (1\ 1\ 1\ 0\ 0\ 1\ 0)$ then $p_2 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$

Let $Q_3 = (1\ 1\ 0\ 1\ 0\ 1\ 0)$ then $p_3 = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$

Let $Q_0 = (1\ 0\ 1\ 0\ 1\ 0\ 1)$ then $p_4 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$

This point is the ciphertext not equal to point p_0, which is plaintext.

REFERENCES:

1. El-Atrash, M., Al-azb, S. and Al-absi, U. "Constant-weight codes using metasymplectic space $F_{4,1}(q)$ and residue" Islamic university Journal Volume13, Number1(2005), Palestine.

2. Tits. J. Building of spherical type and Finite BN-Paris. Number 386 in Lecture Notes in Math. Springer, Berlin, first edition, 1974.
3. Cohen M. Arjeh. Points and lines in Metasymplectic spaces. Annals of Discr. Math., 18:193-196, 1983.
4. Buekenhaut, F. and Cohen, A., Diagram Geometry, Available online at www.win.tue.nl/~amc/buek .
5. Thas, J. "Old and new results on spreads and ovoids of finite classical polar space", Ann. Discrete Math. (1992) 52 pp. 529-544.
6. Cohen A. M. and B. N. Cooperstein " on the local recognition of finite metasymplectic space "J. Algebra 125(1989),348-366.
7. Rieuwert Jan Blok, “On geometries related to buildings”, Ph.D., Thesis, May (1999), Technische Universities Delft, Amsterdam.
8. Jurgen Bierbrauer, , Groups and geometries, May 6,(1997). Personal webpage.