Note on cipher hypersystem

S. Innamorati, Dip. di Matematica, Politecnico di Milano
F. Zuanni, Dip. di Ingegneria Elettrica, Università degli Studi, L'Aquila

Abstract.- Recently, see [2], cryptographic structures derived from generalized designs and hyperstructures have been investigated. In this paper we deal with cipher-hypersystems constructed by using finite geometry.

1. - Introduction.

Cryptography is the study of methods of sending messages that cannot be read by an unauthorized person. An old problem is the frequency analysis of the occurrences in the ciphertext. In the history of cryptography considerable efforts have been performed towards the construction of cryptosystems which have only few statistical information on the occurrences. A famous example is the homophones which are different symbols with the same meaning. As it is well-known, classical cipher-systems, such as the ancient Vigenere's square, are algebraic structures. In recent years, (cfr.[2]) algebraic hyperstructures have been considered in order to avoid frequency analysis. The aim of this paper is to look at cipher hypersystems constructed by using finite geometry.
The reason of using such structures is that it is very hard to discover the geometric connection of a pattern of points.

2. - Geometric spaces, hypergroupoids and cipher systems

Firstly, we recall some definitions.

A geometric space is a pair $(P,\mathcal{B})$, where P is a non-empty set of elements called points and $\mathcal{B}$ is a non-empty family of subsets of P called blocks.

A c-set C of a geometric space $(P,\mathcal{B})$ is said to be a c-arc if

1) $|B \cap C| \leq 2 \quad \forall B \in \mathcal{B}$;

2) $\exists B \in \mathcal{B} : |B \cap C| = 2$.

Moreover a c-set C is said to be an intersection set if

$$B \cap C \neq \emptyset \quad \forall B \in \mathcal{B} .$$

Of course, if each subset B of $\mathcal{B}$ has at least three points then the complementary set of a c-arc is an intersection set. An intersection set whose complementary set is an intersection set too is called a blocking set. Since many of today's applications deal with discrete geometric structures, the study of c-sets having graphic properties, such as arcs, intersection and blocking sets, is of interest to many authors (see [1],...,[14]).

Let t, v, k and λ be non-negative integers, with $v>k>t\geq 2$.

A geometric space $(\mathcal{P},\mathcal{B})$ is said to be a t-(v,k,λ) design if

1) $|P| = v$;

2) $|B| = k \quad \forall B \in \mathcal{B}$;

3) each t-set of P is contained in exactly λ blocks of $\mathcal{B}$.

A t-(v,k,1) design is also called a Steiner system S(t,k,v).

Let A be a non-empty finite set called alphabet. Let us consider two subsets T and K of A, which are the set of the letters of the cleartext and the set of the keywords, respectively.

Moreover we suppose that the ciphertext symbols are elements of a family $\mathcal{C}$ of subsets of A.

A cipher system is a pair (A,f) where f is a function

$$f: T \times K \longrightarrow \mathcal{C}$$

such that

$$\forall C \in \mathcal{C} , \forall k \in K \quad \exists! t \in T \quad : \quad f(t,k) = C .$$

Let P be a non empty v-set. A function

$$o : P \times P \longrightarrow 2^P - \{\emptyset\}$$

is said to be a hyperoperation on P. The pair (P,o) is called a Marty hypergroupoid.

We will show that such three structures have a strict mutual relationship.

A geometric space $(P,\mathcal{B})$ defines a hypergroupoid (P,o) in the following natural way by setting for each $x,y\in P$

$$xoy = \bigcup_{\substack{B\in\mathcal{B}\\ x,y\in B}} B .$$

Let (P,o) be a Marty hypergroupoid. As with the previous notation, let A, T and K be three subsets of P. The pair $(A,o_{|_A})$ is an algebraic cipher hypersystem if
$\forall t\in T,\ k\in K,\ C\in\mathcal{C}$ the equation $tok = C$ has a unique solution.

Now it is clear how to deduce a cipher hypersystem from a geometric space, passing through a hyperstructure. To complete the scheme, the final step is to consider cipher hypersystems deduced directly from geometric spaces.

Let $(P,\mathcal{B})$ be a geometric space. The sets A, T and K, introduced before, will be subsets of P. Let us consider a family of subsets of A $\mathcal{C} = (C_{tk})_{t\in T,k\in K}$ such that

1) $(t_1,k_1)\neq(t_2,k_2) \Rightarrow C_{t_1k_1} \neq C_{t_2k_2}$.

Then it is naturally defined a function f

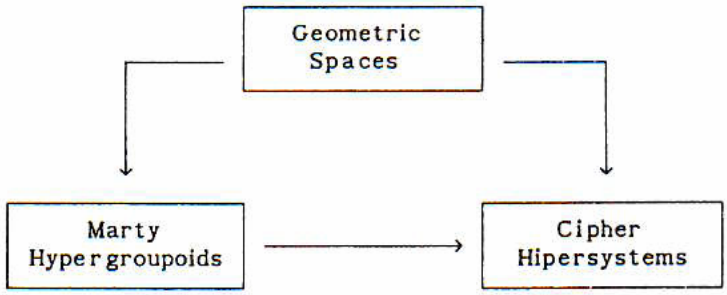
$$f : T\times K \longrightarrow \mathcal{C}$$

$$(t,k)\in T\times K \longrightarrow C_{tk}\in\mathcal{C}$$

such that

$$\forall C\in\mathcal{C},\ \forall k\in K\ \ \exists! t\in T\ :\ f(t,k) = C .$$

So the pair (A,f) is a cipher hypersystem.
We observe that 1) is a strong condition, in fact in section 3 we present an example of cipher hypersystem in which 1) doesn't hold.
The mutual relationship between the structures introduced before can be summarized in the following diagram



3. - An example of cipher hypersystem

In this section we will present an example of cipher hypersystem obtained by a geometric space.

Let $\mathcal{D}=(S,\mathcal{B})$ be a S(t,k,v) Steiner system, t>2. It is well-known that $\mathcal{D}$ is a (t-1)-(v,k,λ) design where λ=(v-t+1)/(k-t+1). Fix a c-arc $\mathcal{T}$. A cipher system can be obtained by considering the set S as the alphabet and the arc $\mathcal{T}$ as the cleartext set T and as the keywords set K.

Let us suppose that we want to send a message consisting of several points and denote one of these by m. In order to cipher m by a key h we choose at random one of the blocks through m and h. Let B denote this block. The ciphertext C is a set of (t-1) points chosen at random by B-{h,m}. The receiver knows the key h of the system. When he receives C he computes the unique block B through the t-set C∪{h}. The message is $\mathcal{T}\cap B-\{h\}$. If $\mathcal{T}\cap B-\{h\}=\emptyset$ then the system assumes the key h as the message m.

Since an unauthorized person doesn't know the correct key h he has 1/λ possibilities to guess the block B.

To increase the security we assume that the users of the cryptographic system have access to a fixed sequence of c-arcs.

An ideal cipher system is the one that the ciphertext contains no statistical information.

The two previous choices have been introduced in order to avoid fequency analysis of the ciphertext occurrences.

References

[1] L.BERARDI, *Constructing 3-designs from spreads and lines*, Discrete Math. 74 (1989), 331-332.

[2] L.BERARDI, F.EUGENI and S.INNAMORATI, *Generalized designs, linear spaces, hypergroupoids and algebraic cryptography*, Proc. IV int. congress on AHA, World Scientific, 1990, 55-65.

[3] A.BEUTELSPACHER and F.EUGENI, *Geometrie finite e crittosistemi*, Atti del II Simposio Naz. "Stato e prospettive della ricerca crittografica in Italia", Roma Novembre 1989.

[4] A.BICHARA and G.KORCHMAROS, n^2*-sets in a projective plane which determine exactly* n^2+n *lines*, J. of Geometry, Vol. 15/2, 1980, 175-181.

[5] M.CERASOLI, F.EUGENI and M.PROTASI, *Elementi di Matematica Discreta*, Zanichelli Bologna, 1986.

[6] P.CORSINI, *Prolegomeni alla Teoria degli Ipergruppi*, Quad. dell'Istituto di Informatica e Sistemistica, Udine 1982.

[7] F.EUGENI, *Combinatorics and Cryptography*, Lecture given at the Int. Conf. "COMBINATORICS '90", Gaeta (Italy), May 1990.

[8] F.EUGENI and M.GIONFRIDDO, *On the minimum number of blocks of a maximal partial spread in* STS(v) *and* SQS(v), Journal of Geometry 36 (1989), 37-48.

[9] M.GIONFRIDDO, *Hypergroups associated with multihomomorphisms between generalized graphs*, Atti del Convegno su "Sistemi binari e loro applicazioni", Taormina (Italy) 1978, 161-174.

[10] B.SEGRE, *Lectures on modern geometry*, Cremonese Roma, 1961.

[11] G.TALLINI, *Strutture grafiche proiettive*, Liguori Napoli, 1967.

[12] G.TALLINI, *Geometric hyperquasigroups and line space*, Acta Univ. Carolinae 25 (1984), 69-73.

[13] G.TALLINI, *On Steiner hypergroups and linear codes*, Atti del Convegno su "Ipergruppi, altre strutture multivoche e loro applicazioni", Udine (Italy) 1985, 87-91.

[14] M. TALLINI SCAFATI, *Sui (k;n)-archi di un piano grafico finito, con particolare riguardo a quelli con due caratteri*, Nota I e II, Rend. Acc. Naz. Lincei, 8, 40 (1966), 812-818, 1020-1025.