J. Cryptology (1989) 1: 185–188

Journal of Cryptology

Linear Ciphers and Spreads[1]

Fred Piper
Department of Mathematics, Royal Holloway and Bedford New College (University of London), Egham, Surrey TW20 0EX, England

Michael Walker
Racal Research Ltd., Worton Drive, Worton Grange Industrial Estate, Reading, Berks RG2 0SE, England

Abstract. The purpose of this paper is to point out a correspondence between certain types of linear ciphers and projective planes. With the aid of this correspondence we are then able to answer a number of questions posed in [3].

Key words. Block ciphers, Linear ciphers, Spreads, Translation planes.

1. Introduction

In a recent paper [3], Massey *et al.* study nonexpanding, key-minimal, robustly perfect block ciphers. They define the concepts of linearity, bilinearity, and multiplication for these ciphers but then raise questions about whether or not these three concepts are different. The purpose of this paper is to point out that these three types of ciphers correspond to special types of projective planes; specifically translation, semifield, and desarguesian planes, respectively. Recognition of this correspondence enables us to answer the questions, posed in [3], concerning the existence of the different types of ciphers and the relationships between them.

2. Linear Block Ciphers

Following the terminology and notation in [3], a block cipher with finite plaintext set S_x, finite key set S_z, and (finite) ciphertext set S_y is defined to be a function f of the direct product of S_x and S_z onto S_y:

$$f: S_x \times S_z \to S_y.$$

Throughout most of this paper, we are concerned with a special class of block

[1] Date received: April 1, 1988. Date revised: March 20, 1989.

ciphers which the authors of [3] call nonexpanding, key-minimal, robustly perfect ciphers; abbreviated to NEKMRP ciphers. For a precise definition of these terms, the reader is referred to [3]. As far as an understanding of this paper is concerned, it is however adequate to note that an NEKMRP cipher is combinatorily characterized by the following two properties:

(1) The sets S_x, S_y, and S_z all have the same cardinality.
(2) Given any plaintext, ciphertext pair (x, y), there is a (necessarily unique) key z such that $f(x, z) = y$.

A cipher is said to be *linear* if S_x and S_y are vector spaces over some field, and for each key z the enciphering mapping

$$f_z: S_x \to S_y; \qquad f_z(x) = f(x, z)$$

is a linear transformation of S_x onto S_y. To be a little more precise, let F be a finite field, and denote by F^n the vector space of all n-tuples over F. Then a linear cipher may be defined as a cipher f such that $S_x = F^m$, $S_y = F^n$, and for each key $z \in S_z$

$$f(\alpha x_1 + \beta x_2, z) = \alpha f(x_1, z) + \beta f(x_2, z)$$

for all $\alpha, \beta \in F$ and $x_1, x_2 \in F^m$. Thus, for a linear cipher, the enciphering transformation determined by the key z may be written in the form

$$y = xM_z,$$

where M_z is the $m \times n$-matrix which represents f_z with respect to the standard bases for F^m and F^n.

This definition of a linear cipher is not entirely satisfactory because, irrespective of the key, the plaintext word which is the all zero m-tuple is always enciphered to the all zero n-tuple ciphertext word. To counter this, it is usual to exclude the all zero tuples and consider the plaintext set of a linear cipher to be $F^m - \{0\}$ and the ciphertext set to be $F^n - \{0\}$. With this definition of a linear cipher, an NEKMRP linear cipher may be characterized as a linear cipher which satisfies the property:

If $|F| = q$, then $|S_x| = |S_y| = |S_z| = q^n - 1$. Furthermore, for any $x \in F^n - \{0\}$ and any distinct $i, j \in S_z$, $xM_i \neq xM_j$. This last property can be restated as:

(3) $M_iM_j^{-1}$ fixes no vector of $F^n - \{0\}$.

Following the definition given in [3], a cipher with key set F^k, or the restricted set $F^k - \{0\}$, is said to be *bilinear* if it is linear and if in addition the enciphering mapping f satisfies the condition

$$f(x, \alpha z_1 + \beta z_2) = \alpha f(x, z_1) + \beta f(x, z_2)$$

for all $\alpha, \beta \in F$, $x \in F^m$, and $z_1, z_2 \in F^k$. An NEKMRP bilinear cipher may be characterized as a linear cipher for which both property (3) and the following property hold:

(4) The set $\{M_z | z \in S_z\}$ of $n \times n$ nonsingular matrices which represent the enciphering transformations, together with the all zero $n \times n$ matrix, forms a vector space under matrix addition and scalar multiplication by elements in F.

Observe that, if F is a prime field, this last property is equivalent to closure of the set of matrices which represent the enciphering transformations under matrix addition.

Note further that if $|F| = q$, then the elements of F^n can be identified with the elements of $\mathrm{GF}(q^n)$. If the enciphering rule $y = f(x, z)$ corresponds to the equation $y = xz$ in $\mathrm{GF}(q^n)$, then the cipher is called a *multiplication cipher.*

3. Spreads

Having briefly reviewed the concepts of linear and bilinear ciphers, we now discuss spreads of finite-dimensional vector spaces over finite fields. Spreads correspond to a class of finite projective planes known as translation planes and it is this correspondence, and the relationship between spreads and NEKMRP linear ciphers, which enables us to answer some of the questions posed by Massey *et al.* in [3].

We begin first with the concept of a spread. If V is a vector space of dimension $2n$ over a field F (with $|F| = q$), then a spread of V is a set of $q^n + 1$ n-dimensional subspaces $W_1, W_2, \ldots, W_{q^n+1}$ of V such that $W_i \cap W_j = \{0\}$ for $i \neq j$. In order to understand the relationship of spreads to linear block ciphers we need to represent them in terms of linear transformations.

If W is a vector space of dimension n over F, and if $V = W \oplus W$, then V has dimension $2n$. We can now define $W_1 = \{(x, 0) | x \in W\}$, $W_2 = \{(0, y) | y \in W\}$, and, for $i = 3, 4, \ldots, q^n + 1$, $W_i = \{(x, xT_i) | x \in W$ and T_i is a nonsingular linear transformation of $W\}$. It is then straightforward to show that:

(5) The set of subspaces $W_1, W_2, \ldots, W_{q^n+1}$ forms a spread of V if and only if, for all $i \neq j$, the transformation $T_i T_j^{-1}$ does not fix any nonzero vector of W.

Moreover, every spread may be represented in this way. Thus we can identify a spread of $V = W \otimes W$ with a set $T = \{T_3, T_4, \ldots, T_{q^n+1}\}$ of $q^n - 1$ nonsingular linear transformations of W. Furthermore, from (3) and (5), it is clear that we can also regard T as the set S_z of keys of an NEKMRP linear cipher with plaintext and ciphertext sets both equal to $W - \{0\}$.

If we let $P(T)$ denote the translation plane associated with the set of transformations T, and let $C(T)$ denote the corresponding block cipher, then algebraic properties of T will be reflected in properties of $P(T)$ and $C(T)$. For translation planes, these properties are well known and are discussed in [1] and [2]; whilst, for linear block ciphers, they are discussed in [3]. The correspondence between the planes and ciphers is given in the following table:

Block cipher	Projective plane
Linear	Translation plane
Bilinear	Semifield plane
Multiplication	Desarguesian plane

For the purpose of this paper the precise meanings of semifield plane and desarguesian plane are not important. All that is relevant is that there exist (many)

examples of translation planes which are neither semifield nor desarguesian planes, and that there are (many) semifield planes which are not desarguesian. (Examples can be found in [1] or [2].) Thus we can answer two of the questions posed in [3] and assert:

(a) An NEKMRP linear cipher need not be bilinear.
(b) An NEKMRP bilinear cipher need not be a multiplication cipher.

In addition to the two questions answered by (a) and (b), the authors of [3] also ask whether an NEKMRP bilinear cipher obtained using a specific construction involving shift registers (construction 1 in [3]) is always a multiplication cipher. To answer this question, we begin by considering the concept of a multiplicative spread, that is, a spread for which the set T of transformations representing it is closed under multiplication (i.e., the product $T_i T_j$ belongs to T for all $T_i, T_j \in T$). Multiplicative spreads correspond to a class of translation planes called nearfield planes which, in general, are different from semifield and desarguesian planes. However, it is well known that a spread which is both multiplicative and additive always represents a desarguesian plane (i.e., a multiplication cipher). This result can be used to show that:

(c) Construction 1 in [3] always yields a multiplication cipher.

This answers the third question posed in [3].

Finally, we must emphasize that the intention of this paper is only to point out the correspondence between linear ciphers, spreads, and translation planes, and to indicate that recognition of this correspondence allows us to answer a number of questions concerning linear ciphers. This correspondence and its relevance to cryptography will be discussed in greater detail in a subsequent paper.

References

[1] Hughes, D. R., and Piper, F. C., *Projective Planes*, Graduate Texts in Mathematics, Vol. 6, Springer-Verlag, New York, 1973.
[2] Lüneberg, H., *Translation Planes*, Springer-Verlag, New York, 1980.
[3] Massey, J. L., Maurer, U., and Wang, M., Non-expanding key-minimal, robustly-perfect, linear and bilinear ciphers, *Proceedings of EUROCRYPT 87*, pp. 237–248, Lecture Notes in Computer Science, Vol. 304, Springer-Verlag, Berlin, 1988.