(Preprint of a Paper to appear in the Proceedings of EUROCRYPT 87, in Advances in Cryptology, Lecture Notes in Computer Science, published by Springer-Verlag.)

NON-EXPANDING, KEY-MINIMAL, ROBUSTLY-PERFECT, LINEAR AND BILINEAR CIPHERS

James L. Massey, Ueli Maurer & Muzhong Wang

Institute for Signal and Information Processing
Swiss Federal Institute of Technology
CH-8092 Zürich, Switzerland

1. INTRODUCTION

The purposes of this paper are: (1) to give appropriate definitions of robustly-perfect ciphers, linear ciphers and bilinear ciphers; (2) to give two general constructions of robustly-perfect bilinear block ciphers that do not expand the plaintext and that have the smallest possible amount of secret key; (3) to give some isolated examples of robustly-perfect linear stream ciphers that use less key than had been earlier conjectured to be necessary; and (4) to suggest some possible useful applications for robustly-perfect linear and bilinear ciphers.

Section 2 introduces the notion of a robustly-perfect block cipher and shows the connection of such ciphers to Latin squares. Linear and bilinear block ciphers are defined in Sections 3 and 4, respectively. Two general constructions of non-expanding, key-minimal robustly-perfect bilinear ciphers are also given in Section 4, and some as-yet-unanswered questions about such ciphers are raised. Section 5 gives a tentative general definition of a linear stream cipher, and exhibits some counterexamples to a conjecture by Massey and Rueppel on the amount of key required in such ciphers. Finally, Section 6 suggests some possible practical applications for robustly-perfect linear and bilinear ciphers and points out some further open questions about such ciphers.

2. KEY-MINIMAL ROBUSTLY-PERFECT BLOCK CIPHERS

In a deterministic secret-key cipher, the ciphertext Y can be written in terms of the plaintext X and the key Z in the manner

$$Y = f(X, Z)$$

where f is a mapping from $S_x \times S_z$ to S_y where S_x is the set of allowed plaintexts, S_z is the set of allowed keys and S_y is the set of possible ciphertexts. The probability distribution P_X of X is determined by the plaintext source, but P_Z is chosen by the cryptographer. It is always assumed that X and Z are statistically independent. The pair (f, P_Z) can be called the cipher system. The only essential requirement on f is that the enciphering must be decipherable by one who knows the key, i.e., $f(x_1, z) = f(x_2, z)$ must imply $x_1 = x_2$.

Until further notice, we shall be concerned only with block ciphers, which can be defined as ciphers for which S_x, S_y and S_z are all finite sets.

Shannon [1, p.679] has defined a cipher system (f, P_Z) to be perfect if X and Y are statistically independent. In this definition, P_X is assumed to be specified. It is natural to extend Shannon's definition and to say that the cipher system (f, P_Z) is robustly perfect if it is perfect for all probability distributions P_X on the set S_x.

The Vernam cipher or "one-time pad", in which $S_x = S_y = S_z = \{0, 1, 2, ..., m-1\}$,

$$Y = f(X, Z) = X \bigoplus Z,$$

where the addition is modulo m, and P_Z is the uniform distribution on $\{0, 1, ..., m-1\}$, is robustly perfect. This follows from the fact that $P_{Y|X}(j|i) = \frac{1}{m}$ for all i and j, and hence $P_{Y|X}(j|i) = P_Y(j) = \frac{1}{m}$ independently of the choice of P_X.

Shannon [1, p.681] has shown that, in a perfect cipher system, the number of keys $\#(S_z)$ must be at least as great as the number of plaintexts with non-zero probability. Thus, a robustly-perfect cipher system must have $\#(S_z) \geq \#(S_x)$. We shall say that a robustly-perfect cipher system is key-minimal if $\#(S_z) = \#(S_x)$. A block cipher is non-expanding if $\#(S_y) = \#(S_x)$. The one-time pad is thus seen to be a non-expanding key-minimal robustly-perfect cipher system.

Shannon [1, p.681] has stated a proposition equivalent to the following:

Proposition 1: *A cipher system (f, P_Z) with $\#(S_x) = \#(S_y) = \#(S_z)$ is robustly-perfect if and only if (1) P_Z is the uniform distribution on S_z and (2) for every x and y in S_x and S_y, respectively, there is a unique z in S_z such that $y = f(x, z)$.*

Shannon observed that condition (2) of the above proposition shows that the essential feature of a non-expanding key-minimal robustly-perfect cipher is that, with the rows indexed by the plaintexts and the columns indexed by the keys, the array of corresponding ciphertexts forms a Latin square. A Latin square [2] (of size $n \times n$) is an $n \times n$ array, whose entries are drawn from an alphabet of n letters, with the property that each letter of the alphabet appears exactly once in each row and once in each column. The name "Latin square" comes from the fact that their first systematic investigator, L. Euler, chose the first n Latin letters as his alphabet, but most investigators today use the alphabet $\{1,2,...,n\}$. The following two examples of 7×7 Latin squares will be of interest in Section 3:

1	2	3	4	5	6	7
2	3	4	5	6	7	1
3	4	5	6	7	1	2
4	5	6	7	1	2	3
5	6	7	1	2	3	4
6	7	1	2	3	4	5
7	1	2	3	4	5	6

1	2	3	4	5	6	7
4	1	5	6	2	7	3
5	3	6	2	7	1	4
6	4	2	7	1	3	5
7	6	1	3	4	5	2
2	5	7	1	3	4	6
3	7	4	5	6	2	1

If we take $S_x = S_y = S_z = \{1,2,...,7\}$, then the second of these Latin squares specifies, for instance, that the ciphertext y corresponding to the plaintext $x=3$ and the key $z=5$ can be found in the third row and fifth column of this array and is thus $y=7$, i.e. $f(3,5)=7$.

Because P_Z must be the uniform distribution in a non-expanding, key-minimal, robustly-perfect (NEKMRP) cipher system (f, P_Z), we can and will speak of the cipher f alone as NEKMRP. It is interesting to note that if the roles of the plaintext x and the key z are interchanged in an NEKMRP cipher, then the new cipher is also NEKMRP, as follows from the fact that the transpose of a Latin square is another Latin square. But x and y can also be interchanged in an NEKMRP cipher and the new cipher remains NEKMRP, as follows immediately from Proposition 1. Thus there is a complete <u>interchangeability of variables</u> in an NEKMRP cipher $y=f(x,z)$ in the sense that any one of x, y and z can be taken as the "key" and either of the two remaining quantities can be taken as the "plaintext". This interchangeability is quite obvious for the one-time pad, but rather less so for the NEKMRP ciphers that will be given later.

3. LINEAR BLOCK CIPHERS

The notion of a "linear" cipher requires that the plaintext set, S_x, and ciphertext set, S_y, be vector spaces. The notion of a "block" cipher (to which our discussion is still restricted) demands that these same sets be finite. Thus, the notion of a "linear block" cipher demands that S_x and S_y be finite-dimensional vector spaces over a finite field.

Here and hereafter, let F denote an arbitrary <u>finite field</u> and let F^n denote the vector space of n-component "column vectors" over F, i.e., vectors of the form $\underline{v} = (v_1, v_2, ..., v_n)$ where $v_i \in F$ for all i. Then a <u>linear cipher</u> can be defined as a cipher f such that $S_x = F^m$, $S_y = F^n$, and, for each $z \in S_z$,

$$f(c_1\underline{x}_1 + c_2\underline{x}_2, z) = c_1 f(\underline{x}_1, z) + c_2 f(\underline{x}_2, z) \tag{1}$$

for all $c_1 \in F$, $c_2 \in F$, $\underline{x}_1 \in F^m$ and $\underline{x}_2 \in F^m$. A linear cipher is <u>non-expanding</u> if $m=n$.

Our interest will be in "robustly-perfect" linear ciphers. Some subtlety is required for an appropriate definition of a "robustly-perfect" linear cipher, however, for the reason made clear by the following fact.

Proposition 2: *If f is a linear cipher and if the cipher system (f, P_Z) is perfect for the plaintext distribution $P_{\underline{X}}$ (where $P_{\underline{X}}(\underline{0}) \neq 1$ is assumed to avoid trivialities), then $P_{\underline{X}}(\underline{0}) = 0$.*

Proof: Because the cipher system is perfect,

$$P_{\underline{XY}}(\underline{0}, \underline{0}) = P_{\underline{X}}(\underline{0}) P_{\underline{Y}}(\underline{0}).$$

Because the cipher is linear, $P_{\underline{Y}|\underline{X}}(\underline{0}|\underline{0}) = 1$ and thus

$$P_{\underline{XY}}(\underline{0}, \underline{0}) = P_{\underline{Y}|\underline{X}}(\underline{0}|\underline{0}) P_{\underline{X}}(\underline{0}) = P_{\underline{X}}(\underline{0}).$$

Hence it follows that

$$P_{\underline{X}}(\underline{0}) = P_{\underline{X}}(\underline{0}) P_{\underline{Y}}(\underline{0}),$$

which, because $P_{\underline{Y}}(\underline{0}) \neq 1$, implies that $P_{\underline{X}}(\underline{0}) = 0$.

Remark: When $P_{\underline{X}}(\underline{0}) = 1$, every cipher is trivially perfect since every $\underline{Y}$ is then statistically independent of $\underline{X}$. Thus, excluding the case $P_{\underline{X}}(\underline{0}) = 1$ excludes only this triviality.

Proposition 2 shows the appropriateness of defining a linear cipher to be robustly-perfect if it is a robustly-perfect cipher for the restricted plaintext set $F^m - \{\underline{0}\}$. In any linear cipher, the required decipherability of the enciphering transformation $\underline{y} = f(\underline{x}, z)$ for every key z is equivalent to the requirement that $\underline{y} = \underline{0}$ implies $\underline{x} = \underline{0}$. Thus, the plaintext restriction to the set $F^m - \{\underline{0}\}$ automatically implies a corresponding ciphertext restriction to the set $F^n - \{\underline{0}\}$.

If $F = GF(q)$, the finite field of q elements, then there are $q^m - 1$ plaintexts in the restricted plaintext set $F^m - \{\underline{0}\}$. A robustly-perfect linear cipher is thus appropriately defined to be key-minimal if also $\#(S_z) = q^m - 1$. It follows that in a non-expanding key-minimal robustly-perfect (NEKMRP) linear cipher, the restricted plaintext set, the restricted ciphertext set, and the key set all have cardinality $q^m - 1$. It thus follows from Proposition 1 that the array of restricted ciphertexts for an NEKMRP cipher, with the rows indexed by the keys and the columns indexed by the restricted plaintexts, forms a $(2^m - 1) \times (2^m - 1)$ Latin square and, conversely, that any linear cipher for which this array is a Latin square becomes an NEKMRP cipher when the keys are chosen to be equiprobable. Because (1) implies that the enciphering transformation $\underline{y} = f(\underline{x}, z)$ of a linear cipher can be written as

$$\underline{y} = M_z \underline{x} \tag{2}$$

where M_z is an $n \times m$ matrix determined by the key z, and because decipherability implies that M_z must have rank m, the Latin square characterization of an NEKMRP linear cipher is equivalent to the following matrix characterization.

Proposition 3: *The linear cipher $\underline{y} = M_z \underline{x}$, where $\underline{x} \in F^m - \{\underline{0}\}$ and $F = GF(q)$, is non-expanding key-minimal and robustly-perfect if and only if (1) there are $q^m - 1$ different keys z and these are chosen to be equiprobable and (2) every matrix M_z is a nonsingular $m \times m$ matrix and, for each $\underline{x} \in F^m - \{\underline{0}\}$ and every $\underline{y} \in F^m - \{\underline{0}\}$, there is exactly one matrix M_z such that $\underline{y} = M_z \underline{x}$.*

The following example shows that NEKMRP linear ciphers exist.

Example 1: $F = GF(2)$, $m = 2$, $S_z = \{1, 2, 3\}$,

$$M_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad M_2 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \qquad M_3 = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}.$$

For $\underline{x} = (1,0)$, $M_1\underline{x} = (1,0)$, $M_2\underline{x} = (0,1)$ and $M_3\underline{x} = (1,1)$. For $\underline{x} = (0,1)$, $M_1\underline{x} = (0,1)$, $M_2\underline{x} = (1,1)$ and $M_3\underline{x} = (1,0)$. For $\underline{x} = (1,1)$, $M_1\underline{x} = (1,1)$, $M_2\underline{x} = (1,0)$ and $M_3\underline{x} = (0,1)$. Thus, by Proposition 3, this linear cipher is NEKMRP when the keys each have probability 1/3.

This example is the $q = 2$, $m = 2$ special case of the first of two general constructions of NEKMRP linear ciphers that will be given in the next section.

4. BILINEAR BLOCK CIPHERS

In order to define a "bilinear" cipher, we must require that S_z, as well as S_x and S_y, be a vector space. It would seem natural then to define a "bilinear" cipher as a cipher such that (i) $S_x = F^m$, $S_y = F^n$ and $S_z = F^k$, (ii) f satisfies (1), i.e., f is a linear cipher, and (iii) for every $\underline{x} \in F^m$

$$f(\underline{x}, c_1\underline{z}_1 + c_2\underline{z}_2) = c_1 f(\underline{x}, \underline{z}_1) + c_2 f(\underline{x}, \underline{z}_2) \tag{3}$$

for all $c_1 \in F$, $c_2 \in F$, $\underline{z}_1 \in F^k$ and $\underline{z}_2 \in F^k$. However, (3) implies that $f(\underline{x}, \underline{0}) = \underline{0}$ for all $\underline{x} \in F^m$ so that the decipherability condition cannot be satisfied for $\underline{z} = \underline{0}$. Thus, the key $\underline{z}$ must belong to the restricted key set $F^k - \{\underline{0}\}$ in order to have a valid cipher; hereafter, we assume this restriction to hold and we then take conditions (i), (ii) and (iii) above together with the condition (iv) that the mapping $\underline{y} = f(\underline{x}, \underline{z})$ be invertible for every fixed $\underline{z}$, $\underline{z} \neq \underline{0}$, as our definition of a bilinear cipher.

Equations (1) and (3) and condition (iv) imply that the enciphering transformation $\underline{y} = f(\underline{x}, \underline{z})$ of a bilinear cipher can be written as

$$\underline{y} = M_{\underline{z}}\underline{x} \tag{4}$$

where $M_{\underline{z}}$ is an $n \times m$ matrix of rank m when $\underline{z} \neq \underline{0}$ such that

$$M_{c_1\underline{z}_1 + c_2\underline{z}_2} = c_1 M_{\underline{z}_1} + c_2 M_{\underline{z}_2}. \tag{5}$$

But (5) is just the condition that each entry in $M_{\underline{z}}$ where $\underline{z} = (z_1, z_2, ..., z_k)$ be a linear combination of the key components $z_1, z_2, ..., z_k$.

Example 2: $q = 2$, $m = n = k = 2$,

$$M_{\underline{z}} = \begin{bmatrix} z_1 & z_2 \\ z_2 & z_1 + z_2 \end{bmatrix}$$

defines a bilinear cipher because

$$M_{(1,0)} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad M_{(0,1)} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \qquad M_{(1,1)} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

all have rank 2, i.e., are all nonsingular matrices. We see in fact that this bilinear cipher is precisely the NEKMRP linear cipher of Example 1 with an obvious mapping between the key space $F^2 - \{\underline{0}\}$ and the key set $\{1, 2, 3\}$.

For any $F = GF(q)$ and any m, an NEKMRP bilinear cipher may be constructed as follows.

Construction 1:

(1) Let $(z_1, z_2, ..., z_m)$ be the initial state of an m-stage q-ary maximal-length (ML) linear feedback shift-register (LFSR), i.e., an LFSR whose output sequence has period $q^m - 1$ when started in any nonzero initial state.

(2) Compute symbolically each of the next $m-1$ digits $z_{m+1}, z_{m+2}, ..., z_{2m-1}$ of the LFSR output sequence as a linear combination of the variables $z_1, z_2, ..., z_m$.

(3) Choose the i-th column of $M_{\underline{z}}$ to be the column vector $(z_i, z_{i+1}, ..., z_{i+m-1})$ where each z_j for $j > m$ is written as the linear combination determined in step (2).

Example 3: The two-stage binary LFSR

is an MLLFSR such that $z_3 = z_1 + z_2$. Thus, Construction 1 uses the sequence $(z_1, z_2, z_3) = (z_1, z_2, z_1 + z_2)$ to obtain the matrix

$$M_{\underline{z}} = \begin{bmatrix} z_1 & z_2 \\ z_2 & z_1 + z_2 \end{bmatrix},$$

which is that of the NEKMRP bilinear cipher of Examples 1 and 2.

Example 4: The three-stage binary LFSR

is an MLLFSR such that $(z_1, z_2, z_3, z_4, z_5) = (z_1, z_2, z_3, z_1 + z_3, z_1 + z_2 + z_3)$. Construction 1 thus gives the bilinear cipher with

$$M_{\underline{z}} = \begin{bmatrix} z_1 & z_2 & z_3 \\ z_2 & z_3 & z_1 + z_3 \\ z_3 & z_1 + z_3 & z_1 + z_2 + z_3 \end{bmatrix}.$$

The reader is invited to check that with the mapping from the binary vector (c_1, c_2, c_3) to the integer $c_1 + 2c_2 + 4c_3$, this bilinear cipher corresponds exactly to the second of the two 7×7 Latin squares exhibited in Section 2, and is thus an NEKMRP cipher when the 7 keys are chosen to be equiprobable.

That the bilinear cipher produced by Construction 1 is indeed NEKMRP (when the $q^m - 1$ keys are equally likely) can be seen as follows. In one period of the output sequence of an m-stage q-ary MLLFSR, the state of the shift-register takes on each of the $q^m - 1$ possible non-$\underline{0}$ values exactly once. But the columns of $M_{\underline{z}}$, by construction, consist of m consecutive states of the MLLFSR. For any fixed $\underline{x} \neq \underline{0}$, by the well-known shift-and-add property of ML sequences, cf. [3, Theorem 4.3], $M_{\underline{z}}\underline{x}$ is a state at a fixed number of shifts later on the same MLLFSR state sequence as the state $(z_1, z_2, ..., z_m)$ corresponding to the first column of $M_{\underline{z}}$. Thus, as $\underline{z}$ runs over all values in $F^m - \{\underline{0}\}$, so also does $M_{\underline{z}}\underline{x}$. Thus, for each $\underline{x} \neq \underline{0}$ and every $\underline{y} \neq \underline{0}$, there is exactly one choice for $\underline{z} = (z_1, z_2, ..., z_m)$ such that $\underline{y} = M_{\underline{z}}\underline{x}$. That this bilinear cipher is thus NEKMRP now follows from Proposition 3.

Because the finite field $GF(q^m)$ can be considered as a vector space of dimension m with respect to the "scalar" field $F = GF(q)$ [4, p.54], the elements of $GF(q^m)$ can be represented as vectors in F^m in the manner that if β_1 and β_2 in $GF(2^m)$ are represented by $\underline{v}_1$ and $\underline{v}_2$, respectively, in F^m, then $\beta_1 + \beta_2$ is represented by $\underline{v}_1 + \underline{v}_2$. If α is an element of $GF(q^m)$ whose minimal polynomial over $GF(q)$ has degree m, then a commonly used such representation of $GF(q^m)$ takes the representation of the so-called "canonical basis" $1, \alpha, \alpha^2, ..., \alpha^{m-1}$ in $GF(q^m)$ to be the "unit vectors" $(1, 0, 0, ..., 0)$, $(0, 1, 0, ..., 0)$, ... , $(0, 0, 0, ..., 1)$.

Example 5: Let α be an Element of $GF(2^2)$ whose minimal polynomial over $GF(2)$ is $X^2 + X + 1$, i.e., $\alpha^2 + \alpha + 1 = 0$ and thus $\alpha^2 = \alpha + 1$. Representing 1 and α by $(1, 0)$ and $(0, 1)$, respectively, the multiplication rule for $GF(2^2)$ is readily checked to be

$$(x_1 + x_2\alpha)(z_1 + z_2\alpha) = (x_1z_1 + x_2z_2) + (x_1z_2 + x_2z_1 + x_2z_2)\alpha,$$

which can be written more suggestively as

$$(x_1, x_2) \times (z_1, z_2) = (x_1z_1 + x_2z_2, x_1z_2 + x_2z_1 + x_2z_2).$$

For any $F = GF(q)$ and any m, an NEKMRP bilinear cipher may be constructed as follows.

Construction 2:

(1) Take $\underline{x} = (x_1, x_2, ..., x_m)$, $\underline{y} = (y_1, y_2, ..., y_m)$ and $\underline{z} = (z_1, z_2, ..., z_m)$ to be the representations of non-zero elements x, y and z, respectively, of $GF(q^m)$ as described above.

(2) Take the ciphering rule $\underline{y} = f(\underline{x}, \underline{z})$ to correspond to the $GF(q^m)$ equation

$$y = xz. \tag{6}$$

Example 6: Taking $F = GF(2)$, $m = 2$, and using the representation of Example 5, Construction 2 gives the bilinear cipher

$$(y_1, y_2) = (x_1z_1 + x_2z_2, x_1z_2 + x_2z_1 + x_2z_2) = \begin{bmatrix} z_1 & z_2 \\ z_2 & z_1 + z_2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix},$$

which we now recognize to be (accidentially) the NEKMRP cipher of Example 4.

That Construction 2 always gives an NEKMRP bilinear cipher can be seen as follows. ¿From (6) and the fact that

$$(x_I + x_{II})z = x_Iz + x_{II}z$$

and

$$x(z_I + z_{II}) = xz_I + xz_{II},$$

it follows that the cipher is indeed bilinear. For each $x \in GF(q^m)$–$\{\underline{0}\}$ and every $y \in GF(q^m)$–$\{\underline{0}\}$, there is a unique $z \in GF(q^m)-\{\underline{0}\}$ such that (6) is satisfied. It thus follows from Proposition 3 that the cipher is NEKMRP.

If one takes $F = GF(2)$, $m = 3$, and uses the mapping from $GF(2^3)-\{\underline{0}\}$ to $\{1, 2, 3, 4, 5, 6, 7\}$ such that α^i is mapped to $i+1$ where α is a primitive element of $GF(2^3)$, then the bilinear cipher (6) corresponds to the first of the two Latin squares exhibited in Section 3.

Construction 2 can be generalized somewhat as follows. Let A, B and C be nonsingular $m \times m$ matrices over $GF(q)$, let $\hat{x}$, $\hat{y}$ and $\hat{z}$ be the elements of $GF(q^m)$ represented by $A\underline{x}$, $B\underline{y}$ and $C\underline{z}$, respectively, and replace equation (6) by

$$\hat{y} = \hat{x}\hat{z}. \tag{7}$$

It is easily seen that this new cipher is again NEKMRP and, in fact, corresponds just to a change in basis for the representations of $GF(q^m)$ used for $\underline{x}$, $\underline{y}$ and $\underline{z}$. We shall call any bilinear cipher constructed in this manner a multiplication cipher.

Some questions that as yet we have not been able to answer are: (1) Is an NEKMRP bilinear cipher obtained from Construction 1 always a multiplication cipher? (2) Is every NEKMRP bilinear cipher a multiplication cipher? (3) With an appropriate representation of the set of keys, is every NEKMRP linear cipher a bilinear cipher?

5. LINEAR AND BILINEAR STREAM CIPHERS

In this section we will be concerned with stream ciphers, which can be defined as ciphers for which S_x and S_y (and also generally S_z) are infinite sets. We shall take S_x, S_y and S_z to be F^∞, the vector space of all one-sided infinite sequences $\tilde{v} = (v_0, v_1, v_2, ...)$ with $v_i \in F = GF(q)$. We define a non-expanding additive stream cipher to be a cipher such that the ciphertext sequence $\tilde{Y} = (Y_0, Y_1, Y_2, ...)$ is determined as

$$Y_i = X_i + W_i, \qquad i \geq 0 \tag{8}$$

where $\tilde{W} = (W_0, W_1, W_2, ...)$ is the running key sequence and where we allow W_i to depend both on the secret key $\tilde{Z}$ (as is customary) and on the plaintext digits X_j with $j < i$ (as is not customary but is required for interesting definitions of "linear" and "bilinear" stream ciphers). Equation (8) ensures the decipherability of the cipher since

$$X_i = Y_i - W_i$$

and W_i can be found with knowledge of the secret key $\tilde{Z}$ and the previously deciphered plaintext digits. For later convenience, we take the plaintext sequence $\tilde{X}$ to be $\tilde{X} = (X_{-M}, ..., X_{-1}, X_0, X_1, ...)$, where $X_{-M}, ..., X_{-1}$ are "dummy plaintext digits" known in advance at the receiving site, and we take the secret key to be $\tilde{Z} = (Z_{-L}, ..., Z_{-1}, Z_0, Z_1, ...)$. The parameters M and L will soon be specified.

We shall say that a non-expanding additive stream cipher has plaintext-memory M and key-rate r, where r is a nonnegative real number, if each digit of the running-key sequence can be written as

$$W_i = g_i(X_{i-1}, ..., X_{i-M}, Z_{\lceil ri \rceil}, Z_{\lceil ri \rceil - 1}, ..., Z_{-L}), \tag{9}$$

where $\lceil . \rceil$ denotes the smallest integer equal to or greater than the enclosed number. We shall further say that such a cipher is linear if, when $\tilde{Z}$ is fixed, each function g_i is linear in its plaintext variables, and to be bilinear if it is linear and, when $\tilde{X}$ is fixed, each function g_i is also linear in its key variables.

A non-expanding additive stream cipher is robustly-perfect if, for any choice of statistics for the plaintext sequence $\tilde{X}$, the running-key sequence $\tilde{W}$ is statistically independent of the plaintext sequence $\tilde{X}$, and $\tilde{W}$ is a sequence of statistically independent uniformly-distributed (i.u.d) random variables.

Because (9) implies that $W_i = 0$ when $X_{i-1} = ... = X_{i-M} = 0$ and the cipher is linear, it follows that a linear additive stream cipher with plaintext memory M cannot be robustly-perfect unless we enforce the plaintext M-restriction that no M consecutive digits in $\tilde{X}$ can all be zeros. We shall later consider a somewhat more severe plaintext restriction.

By an easy argument based on the entropies of the $\tilde{W}$ and $\tilde{Z}$ sequences, one sees that if the cipher (9) is robustly-perfect then the key-rate r is at least 1; we shall say the cipher is key-minimal if $r = 1$. Massey and Rueppel [5] have constructed linear ciphers of the form (9) that are robustly-perfect for the plaintext M-restriction and have key rate $r = 2$. Their ciphers are given by

$$W_i = X_{i-1}Z_{2i-1} + X_{i-2}Z_{2i-2} + \ldots + X_{i-M}Z_{2i-M} \tag{10}$$

where $\tilde{Z}$ is i.u.d.; we see from (10) that this Massey-Rueppel robustly-perfect additive stream cipher is in fact bilinear. Massey and Rueppel [5] also conjectured that no robustly-perfect linear cipher (9) exists (for the plaintext M-restriction) with $r < 2$ for any $M \geq 2$, (which implies that key-minimal robustly-perfect ciphers of this type do not exist). We will show this conjecture to be false by exhibiting key-minimal (i.e., $r = 1$), robustly-perfect for the plaintext M-restriction, additive bilinear stream ciphers for $M = 2$ and $M = 3$, namely, the binary [i.e., F=GF(2)] ciphers

$$W_i = X_{i-1}(Z_{i-1} + Z_{i-4}) + X_{i-2}(Z_{i-2} + Z_{i-3}) \tag{11}$$

and

$$W_i = X_{i-1}Z_{i-1} + X_{i-2}Z_{i-3} + X_{i-3}(Z_{i-2} + Z_{i-3}) \tag{12}$$

when $\tilde{Z}$ is i.u.d.. To show that these ciphers are robustly-perfect we require two additional facts, the first of which should be quite obvious.

<u>Proposition 4</u>: *A bilinear additive stream cipher satisfying (9) is robustly-perfect for a specified plaintext restriction if and only if, for every admissible plaintext sequence $\tilde{x}$, an i.u.d. key sequence $\tilde{Z}$ produces an i.u.d. running-key sequence $\tilde{W}$.*

Because in a bilinear additive stream cipher satisfying (9), given that $\tilde{X} = \tilde{x}$, we can write for every $i \geq 0$

$$(W_0, W_1, ..., W_i) = M_{ix}(Z_{-L}, Z_{-L+1}, ..., Z_{\lceil ri \rceil}) \tag{13}$$

where M_{ix} is an $(i+1) \times (L+\lceil ri \rceil+1)$ matrix whose components are each a linear combination of the digits $x_{-M}, x_{-M+1}, ..., x_{i-1}$, it follows that Proposition 4 is equivalent to the following proposition.

<u>Proposition 5</u>: *A bilinear additive stream cipher satisfying (9) is robustly-perfect for a specified plaintext restriction if and only if, for every $i \geq 0$ and for every admissible plaintext sequence $\tilde{x}$, the matrix M_{ix} of (13) has linearly independent rows.*

This equivalence follows from the facts that if the i+1 rows of M_{ix} are linearly dependent then the column space of M_{ix} has dimension less than $i+1$ and hence $(W_0, W_1, ..., W_i)$ cannot take on all q^{i+1} possible values; and conversely, if the i+1 rows are linearly independent then $(W_0, W_1, ..., W_i)$ takes on all q^{i+1} values and, by linearity, the same number of keys produce each possible value so that the random variables $W_0, W_1, ..., W_i$ are i.u.d. when $Z_{-L}, Z_{-L+1}, ..., Z_{\lceil ri \rceil}$ are i.u.d..

For the binary bilinear ciphers of (11) and (12),

$$M_{ix} = \begin{bmatrix} x_{-1} & x_{-2} & x_{-2} & x_{-1} & 0 & 0 & \dots & 0 \\ 0 & x_0 & x_{-1} & x_{-1} & x_0 & 0 & \dots & 0 \\ & & & & & & & \\ & & & & & & & \\ 0 & 0 & \dots & \dots & x_{i-1} & x_{i-2} & x_{i-2} & x_{i-1} \end{bmatrix} \tag{14}$$

and

$$M_{ix} = \begin{bmatrix} x_{-2}+x_{-3} & x_{-3} & x_{-1} & 0 & 0 & \dots & 0 \\ 0 & x_{-1}+x_{-2} & x_{-2} & x_0 & 0 & \dots & 0 \\ & & & & & & \\ & & & & & & \\ 0 & \dots & & 0 & x_{i-2}+x_{i-3} & x_{i-2} & x_{i-1} \end{bmatrix}, \tag{15}$$

respectively. The M-restriction on $\tilde{x}$ in both cases is equivalent to the condition that the matrix M_{ix} has no all-zero rows. By a straightforward but somewhat tedious induction, one shows that the matrices in (14) and (15) do indeed have linearly independent rows when the plaintext M-restriction is satisfied, which by Proposition 5 proves the claim that these binary bilinear additive stream ciphers are key-minimal robustly-perfect.

It is quite easy, as we now show, to construct key-minimal robustly-perfect bilinear additive stream ciphers if one relaxes the plaintext M-restriction somewhat. Choose a positive integer m and define $\underline{X}_j = (X_{jm}, X_{jm+1}, ..., X_{jm+m-1})$ to be an m digit segment of $\tilde{X}$. Define $\underline{Z}_j$, $\underline{W}_j$ and $\underline{Y}_j$ in a similar fashion. Now consider the bilinear additive stream cipher such that

$$\underline{Y}_j = \underline{X}_j + \underline{W}_j \tag{16}$$

where

$$\underline{W}_j = M_{\underline{Z}_{j-1}} \underline{X}_{j-1} \tag{17}$$

where $M_{\underline{Z}}$ is the matrix of a NEKMRP bilinear block cipher as discussed in Section 4. This cipher has plaintext-memory $M = 2m - 1$ as follows from the fact that Y_{jm+m-1}, the "newest" digit in $\underline{Y}_j$, depends on X_{jm-m}, the "oldest" digit in $\underline{X}_{j-1}$. We now claim that, for the "strong plaintext restriction" that $\tilde{X}$ contains no run of m consecutive zeroes (and hence that $\underline{X}_j \neq \underline{0}$ for all j), this bilinear additive cipher is key-minimal robustly-perfect. To prove this claim, we suppose that $\tilde{X} = \tilde{x}$ where $\tilde{x}$ is some admissible plaintext sequence. We recall from Proposition 3 that then $\underline{Z}_{j-1} \neq \underline{0}$ in (17) implies $\underline{W}_j \neq \underline{0}$. But $\underline{Z}_{j-1} = \underline{0}$ implies by bilinearity that $M_{\underline{Z}_{j-1}}$ is the zero matrix and hence that $\underline{W}_j = \underline{0}$. Thus because $\tilde{Z}$ is i.u.d., $\underline{W}_j$ equals $\underline{0}$ with probability q^{-m} independent of the value of $\underline{W}_0, \underline{W}_1, ..., \underline{W}_{j-1}$. Proposition 3 further implies that $\underline{W}_j$ equals all $q^m - 1$ non-zero values with equal probability, which must also be q^{-m}, independent of the values of $\underline{W}_0, \underline{W}_1, ..., \underline{W}_{j-1}$. It now follows from Proposition 4 that this bilinear additive stream cipher is robustly-perfect and, since the key-rate $r = 1$, it is also key-minimal.

6. POSSIBLE APPLICATIONS AND SOME REMARKS

As any experienced cryptographer is aware, "linearity" in a cipher is generally one of the greatest assists to the enemy cryptanalyst who attacks it. Thus, we would not seriously propose using directly any of the linear or bilinear ciphers developed in this paper for any practical application where generally only a small amount of secret key (compared to the amount of plaintext) can be tolerated. The real point of this work is the fact that a robustly-perfect linear or bilinear cipher provides a mechanism by which one sequence (the "key") effectively randomizes another sequence (the "plaintext"). Indeed, Massey and Rueppel [5] used their robustly-perfect bilinear additive stream cipher (10) as a mechanism to combine two LFSR sequences to produce a cryptographically strong running-key sequence. The key-minimal robustly-perfect bilinear additive stream ciphers constructed in Section 5 should be even better sequence combiners. The key-minimal robustly-perfect bilinear block ciphers constructed in Section 4 might make excellent component ciphers, when interleaved with nonlinear transpositions, in a product cipher.

It is still a very open question whether, for any $r < 2$, one can for every M construct a plaintext-memory M bilinear (or just linear) additive stream cipher that is robustly-perfect for the plaintext M-restriction and has key-rate at least r. Although, we have not yet succeeded for any $M > 3$, our intuition now is that $r = 1$ is possible for every M. The possibly great potential of such $r = 1$ ciphers as sequence combiners suggests that this open question deserves some serious attention. It is also far from clear that our definitions of "linear" and "bilinear" additive stream ciphers are the most appropriate ones, and some attention should be paid to alternative definitions that might be still more natural.

REFERENCES

[1] C. E. Shannon, "Communication Theory of Secrecy Systems", Bell Sys. Tech. J., vol. 28, pp. 656-715, Oct. 1949.

[2] J. Dénes and A. D. Keedwell, Latin Squares and their Applications. Budapest: Akadémiai Kiadó, 1974.

[3] S. W. Golomb, Shift Register Sequences. San Francisco: Holden-Day, 1967.

[4] R. Lidl and H. Niederreiter, Finite Fields (Vol. 20, Encyclopedia of Math. and its Appl.). Englewood Cliffs, NJ: Addison-Wesley, 1983.

[5] J. L. Massey and R. A. Rueppel, "Linear Ciphers and Random Sequence Generators with Multiple Clocks", pp. 74-87 in Advances in Cryptology (Proceedings of EUROCRYPT 84, Lecture Notes in Computer Science No. 209). Heidelberg and New York: Springer 1985.