J. Cryptology (1992) 5: 67–86

Journal of Cryptology

Correlation Properties of Combiners with Memory in Stream Ciphers[1]

Willi Meier
HTL Brugg-Windisch, CH-5200 Windisch, Switzerland

Othmar Staffelbach
Gretag Data Systems AG, CH-8105 Regensdorf, Switzerland

Abstract. For pseudo-random generators where one or several LFSRs are combined by a memoryless function, it is known that the output sequences are correlated to certain LFSR-sequences whose correlation coefficients c_i satisfy the equation $\sum_i c_i^2 = 1$. In this paper it is proved that a corresponding result also holds for generators whose LFSRs are connected to a combiner with memory.

If correlation probabilities are conditioned on side information, e.g., on known output digits, it is shown that new or stronger correlations may occur. This is exemplified for the summation cipher with only two LFSRs where such correlations can be exploited in a known plaintext attack. A cryptanalytic algorithm is given which is shown to be successful for LFSRs of considerable length and with arbitrary feedback connection.

Key words. Stream cipher, Correlation, Cryptanalysis, Boolean functions.

1. Introduction

Cryptographic transformations are usually designed by appropriate composition of nonlinear functions. In the design of stream ciphers such functions have been applied to combine the output of linear feedback shift registers (LFSRs) in order to produce the key stream. In this design, the combining functions should not leak information about the individual LFSR-sequences into the key stream in order to prevent divide-and-conquer correlation attacks. For this purpose, the concept of correlation immunity has been introduced in [8] and [5]. For nonlinear combiners, there is a tradeoff between the nonlinear order of the Boolean function and its order of correlation immunity. As has been pointed out in [5], this tradeoff can be avoided if the function is allowed to have memory.

For a memoryless combiner, the output always has correlation to certain linear

[1] Date received: September 1, 1990. Date revised: December 19, 1990. A preliminary version of this paper was presented at Eurocrypt '90, May 21–24, Århus, Denmark, and has appeared in the proceedings, pp. 204–213.

functions of the inputs, and the "total correlation" is independent of the combining function. In fact, it has been shown in [4] that the sum of the squares of the correlation coefficients is always 1. If such a combiner is applied to the output of LFSRs, there result correlations to sums of certain LFSR-sequences such that the correlation coefficients c_i satisfy

$$\sum_i c_i^2 = 1. \tag{1}$$

Choosing the combiner to be correlation-immune of some order means that certain of these c_i's vanish. In particular, to prevent divide-and-conquer attacks, we ensure that there is no correlation to sums of outputs of only a few LFSRs. However, by (1) there must be stronger correlation to certain other sums of LFSR-sequences that must be considered with regard to the cryptanalytic algorithms described in [3]. A first goal of the present paper is to show that a result similar to (1) remains valid for combiners with memory. In fact, the total correlation appears to be independent of the combining functions as for memoryless combiners. Therefore memory does not reduce the total correlation, but offers more flexibility in handling the individual correlation coefficients.

The summation combiner has been proposed in [5] as an example of a combiner that avoids the tradeoff between nonlinear order and correlation immunity. This combiner is based on integer addition which, when viewed over GF(2), defines a nonlinear function with memory whose correlation immunity is maximum.

In Section 2, all correlations between the output of the basic summation combiner and linear functions of the inputs are computed. For inputs a_j and b_j, the output z_j is given by $z_j = a_j + b_j + \sigma_{j-1}$ where σ_{j-1} denotes the carry bit. If $\mathscr{A} = (a_0, a_1, a_2, \ldots)$ and $\mathscr{B} = (b_0, b_1, b_2, \ldots)$ are independent and uniformly distributed sequences of random variables, the output sequence $\mathscr{Z} = (z_0, z_1, z_2, \ldots)$ is also uniformly distributed. Moreover, z_j is independent of a_j, b_j, and the sum $a_j + b_j$. However, it is shown in Section 2.2 that z_j is correlated to both $a_j + b_j + a_{j-1}$ and $a_j + b_j + b_{j-1}$ with probability $p = P(z_j = a_j + b_j + a_{j-1}) = P(z_j = a_j + b_j + b_{j-1}) = 0.75$. The corresponding correlation coefficients are obtained as $c = 2p - 1 = 0.5$. More generally, in Theorem 1 it is shown that for every i, $1 \leq i \leq j$, there are correlations to $N = 2^{i+1} - 2$ linear functions of the form $s = \sum_{k=j-i}^{j} \alpha_k a_k + \beta_k b_k$ and the corresponding correlation coefficients c_h satisfy

$$\sum_{h=1}^{N} c_h^2 = 1 - \frac{1}{2^i}. \tag{2}$$

Note that the right side of (2) tends to 1 as i tends to ∞. This means that the total correlation for the basic summation combiner approaches 1, similar to the case of memoryless combiners. It is shown in Section 3 that this property holds for completely general combiners with 1 bit memory. Such a combiner is described by two balanced functions f_0 and f_1,

$$z_j = f_0(x_{1j}, \ldots, x_{nj}, \sigma_{j-1}), \tag{3}$$

$$\sigma_j = f_1(x_{1j}, \ldots, x_{nj}, \sigma_{j-1}), \tag{4}$$

where σ_j denotes the state of the memory and where the input sequences $\mathscr{X}_m = (x_{m0}, x_{m1}, x_{m2}, \ldots)$, $1 \leq m \leq n$, are assumed to be independent and uniformly distributed. (By definition a function is balanced if it takes on the values 0 and 1 the same number of times.) In Theorem 2, a method is described in order to determine all possible correlations of z_j to linear functions of the inputs, i.e., to linear functions of the form $s = \sum_{k \le j} \sum_{m=1}^{n} w_{mk} x_{mk}$. It is shown that the sum of the squares of the correlation coefficients approaches 1 for every choice of the functions f_0 and f_1, except in a singular case where a similar statement holds for $z_j' = z_j + z_{j-1}$. Therefore the total correlation is independent of the combiner.

These results can be applied to analyze key stream generators where several LFSRs are connected to a combiner with memory. In this analysis, the output of an LFSR can be modeled by a sequence of independent and uniformly distributed binary random variables. If the input sequences $\mathscr{X}_m = (x_{m0}, x_{m1}, x_{m2}, \ldots)$ to the combiner are generated by LFSRs, correlation of z_j to a linear function leads to correlation of the output sequence to a certain sum of phase shifts of the input LFSR-sequences, which is again an LFSR-sequence. With regard to these correlations, Theorem 2 provides a criterion for maximum-order correlation immunity of combiners with memory generalizing that obtained in [4] for memoryless combiners. Theorem 2 also generalizes the treatment of maximum-order correlation immunity in [6] as it covers every kind of correlation to LFSR-sequences originating from the given LFSRs. Such correlations exist even if the combiner is chosen to be maximum-order correlation immune. For stream cipher design, these correlations have to be taken into account not only in view of the cryptanalytic algorithms described in [3] but also with regard to the new algorithm introduced in Section 5 of this paper.

The correlation coefficients in (2) and in Theorem 2 are derived from unconditional probabilities. However, it is often the case that the cryptanalyst has access to side information, e.g., he may know portions of the output sequence. In fact, if correlation is conditioned on the output, new or much stronger correlations may occur. This is exemplified for the basic summation combiner with two inputs where knowledge of portions of the output sequence can considerably reduce the uncertainty about the carry bit. This affects correlation of z_j to the input sum $a_j + b_j$, although z_j and $a_j + b_j$ are uncorrelated in the average.

It is shown in Section 4, that in a run of s consecutive output digits 1, the carries tend to be 0. For example, assume that $z_{j+1} = z_{j+2} = \cdots = z_{j+s} = 1$. Then at the end of the run the carry bit σ_{j+s} is 0 with probability at least $1 - 2^{-s}$. More generally, for every t with $1 \le t \le s$, the corresponding conditional probability satisfies $P(\sigma_{j+s} = \sigma_{j+s-1} = \cdots = \sigma_{j+t} = 1) \ge 1 - 2^{-t}$. As a consequence it is shown in Theorem 3 that, for given t, $1 \le t \le s$, and for every i with $j + t + 1 \le i \le j + s + 1$, the equations

$$z_i = a_i + b_i \tag{5}$$

and $z_{j+s+2} = a_{j+s+2} + b_{j+s+2} + a_{j+s+1}$ *simultaneously* hold with probability at least $1 - 2^{-t}$. A similar statement holds for a run of consecutive output digits 0 where the carries tend to be 1.

This result can be cryptanalytically exploited in a known plaintext attack on the basic summation cipher with only two LFSRs, where the key size k is the sum of the two LFSR-lengths. A cryptanalytic algorithm is given which is shown to be successful for LFSRs of considerable length and with arbitrary feedback connection.

As a consequence for the design of summation ciphers, it is recommended to take several LFSRs of moderate length rather than just a few long LFSRs. The algorithm is based on a general cryptanalytic idea. Observe that satisfaction of (5) for d values of i reduces the uncertainty about the key by d bits. Therefore blocks of d key bits can be tested simultaneously. The resulting procedure is comparable with an exhaustive search over only k/d bits instead of k bits, i.e., it effectively reduces the key size by the factor d.

2. Summation Cipher

2.1. *Basic Summation Principle*

Integer addition has been proposed by R. A. Rueppel and J. L. Massey in [7] for use in cryptographic transformations since this operation is nonlinear when considered over GF(2). In [2] they formulated the summation principle in order to generate cryptographically strong binary sequences out of given (cryptographically weak) sequences. To understand this principle, consider two binary sequences $\mathscr{A} = (a_0, a_1, a_2, \ldots)$ and $\mathscr{B} = (b_0, b_1, b_2, \ldots)$. For every n, the first n digits are viewed as the binary representation of an integer, i.e., $a = a_{n-1}2^{n-1} + \cdots + a_1 2 + a_0$ and $b = b_{n-1}2^{n-1} + \cdots + b_1 2 + b_0$. Then the integer sum $z = a + b$ defines the first n digits of the resulting sequence $\mathscr{Z} = (z_0, z_1, \ldots, z_{n-1}, \ldots)$. If $\mathscr{A}$ and $\mathscr{B}$ are semi-infinite, then $\mathscr{Z}$ is also defined as a semi-infinite sequence. The digit z_j is recursively computed by

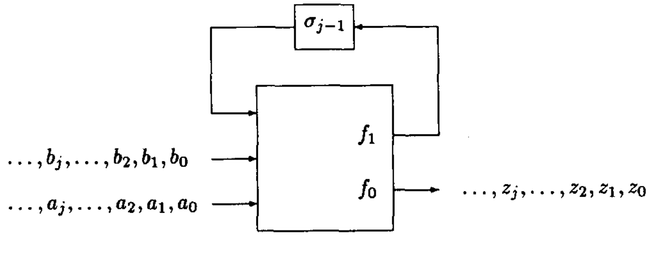
$$z_j = f_0(a_j, b_j, \sigma_{j-1}) = a_j + b_j + \sigma_{j-1}, \tag{6}$$

$$\sigma_j = f_1(a_j, b_j, \sigma_{j-1}) = a_j b_j + a_j \sigma_{j-1} + b_j \sigma_{j-1}, \tag{7}$$

where in (6) σ_{j-1} denotes the carry bit and $\sigma_{-1} = 0$. The generation of the sequence $\mathscr{Z}$ is illustrated in Fig. 1 by a circuit with 1 *bit memory*.

2.2. *Summation Principle and Correlation*

It has been shown in [5] that (besides nonlinearity) the summation principle effects correlation immunity in the following sense. Suppose that $\mathscr{A}$ and $\mathscr{B}$ are *independent and uniformly distributed* sequences of random variables. Then the output z_j is



σ_{j-1}
f_1
f_0
$\ldots, b_j, \ldots, b_2, b_1, b_0$
$\ldots, a_j, \ldots, a_2, a_1, a_0$
$\ldots, z_j, \ldots, z_2, z_1, z_0$

Fig. 1. Summation principle.

statistically independent of both a_j and b_j. Moreover, as the function f_1 in (7) is balanced, for increasing j the carry σ_j becomes arbitrarily close to a balanced random variable. For this reason we consider the initial carry σ_{-1} to be a uniformly distributed random variable. This implies that all carries σ_j, $j \geq -1$, are balanced, and that z_j is independent of the sum $a_j + b_j$. However, σ_{j-1} depends on a_k and b_k for $k \leq j - 1$. In particular, from (7) one sees that σ_{j-1} is correlated (with probability 0.75) to a_{j-1}, b_{j-1}, and σ_{j-2}. This implies, e.g., that f_1 has a representation as

$$\sigma_{j-1} = f_1(a_{j-1}, b_{j-1}, \sigma_{j-2}) = a_{j-1} + g(a_{j-1}, b_{j-1}, \sigma_{j-2}),$$

where g is a function with $\text{Prob}(g = 0) = 0.75$. The computation of z_j according to (6) yields

$$z_j = a_j + b_j + a_{j-1} + g(a_{j-1}, b_{j-1}, \sigma_{j-2}).$$

Hence

$$\text{Prob}(z_j = a_j + a_{j-1} + b_j) = 0.75,$$

which shows that z_j is correlated to certain sums of a_k and b_k for $k \leq j$. If the sequences $\mathscr{A}$ and $\mathscr{B}$ are produced by LFSRs (as suggested in [6]), the output sequence $\mathscr{Z}$ is correlated to LFSR-sequences. Therefore we investigate all possible correlations between z_j and finite sums s of random variables of the form

$$s = \sum_{k \leq j} \alpha_k a_k + \beta_k b_k \tag{8}$$

for $\alpha_k, \beta_k \in \text{GF}(2)$.

The *normalized* correlation between two functions f, g: $\text{GF}(2)^n \rightarrow \text{GF}(2)$ is defined as

$$c(f, g) = \frac{\#\{\mathbf{x} \mid f(\mathbf{x}) = g(\mathbf{x})\} - \#\{\mathbf{x} \mid f(\mathbf{x}) \neq g(\mathbf{x})\}}{2^n}. \tag{9}$$

Replacing the arguments of f and g by binary random variables $X_1, \ldots, X_n$, we obtain random variables $Z_f = f(X_1, \ldots, X_n)$ and $Z_g = g(X_1, \ldots, X_n)$. Suppose that the random variables $X_1, \ldots, X_n$ are uniformly distributed. Then by (9) the probability $P(Z_f = Z_g)$ is related to $c(f, g)$ by

$$c(f, g) = 2P(Z_f = Z_g) - 1.$$

Moreover, for balanced functions f and g the random variables Z_f and Z_g are uniformly distributed.

In general, the correlation coefficient between two random variables X and Y is defined by $\text{cor}(X, Y) = \text{cov}(X, Y)/\sqrt{\text{var}(X)\,\text{var}(Y)}$. If X and Y are uniformly distributed binary random variables, their correlation coefficients can be computed by the following steps:

$$\text{var}(X) = E(X^2) - E(X)^2 = 0.5 - 0.25 = 0.25,$$

$$\text{cov}(X, Y) = E(XY) - E(X)E(Y) = P(X = 1, Y = 1) - 0.25 = P(X = Y)/2 - 0.25,$$

$$\text{cor}(X, Y) = 4\,\text{cov}(X, Y) = 2P(X = Y) - 1.$$

This implies

$$\text{cor}(Z_f, Z_g) = 2P(Z_f = Z_g) - 1 = c(f, g), \tag{10}$$

Table 1. Correlation of z_j to linear functions (Step 1).

Correlation of σ_{j-1} to	Resulting correlation of z_j to	Correlation coefficient
a_{j-1}	$a_j + b_j + a_{j-1}$	0.5
b_{j-1}	$a_j + b_j + b_{j-1}$	0.5
σ_{j-2}	$a_j + b_j + \sigma_{j-2}$	0.5
$a_{j-1} + b_{j-1} + \sigma_{j-2}$	$a_j + b_j + a_{j-1} + b_{j-1} + \sigma_{j-2}$	−0.5

which means that $c(f, g)$ as defined in (9) agrees with $\mathrm{cor}(Z_f, Z_g)$ as defined in statistics.

The recursions (6) and (7) can be applied to compute the correlation coefficients $c(z_j, s)$ where s is a sum of the form (8). In a first step, we use the fact that the function $\sigma_{j-1} = f_1(a_{j-1}, b_{j-1}, \sigma_{j-2})$ of (7) has correlation to exactly the following four linear functions: a_{j-1}, b_{j-1}, σ_{j-2} and $a_{j-1} + b_{j-1} + \sigma_{j-2}$. Substituting σ_{j-1} in (6) as above, these correlations lead to correlations of z_j to sums of certain a_k, b_k, and σ_k as shown in Table 1.

The first two sums in Table 1 are already of the form (8) whereas σ_{j-2}, which appears in the other two sums, is again correlated to the four linear functions a_{j-2}, b_{j-2}, σ_{j-3} and $a_{j-2} + b_{j-2} + \sigma_{j-3}$. This in turn leads to correlation of z_j to sums as shown in Table 2.

The correlation coefficients can be obtained by a product formula, e.g., $c(z_j, a_j + b_j + a_{j-2}) = c(z_j, a_j + b_j + \sigma_{j-2})c(\sigma_{j-2}, a_{j-2}) = 0.5^2 = 0.25$, as specified in the following lemma.

Lemma 1. *Let A_1, A_2, A_3, and X be binary random variables. Suppose that A_1, A_3, X, $A_2 + A_3$, and $A_2 + X$ are uniformly distributed. If A_1 is correlated to $A_2 + X$ and X is correlated to A_3, then A_1 is correlated to $A_2 + A_3$ with correlation coefficient*

$$c(A_1, A_2 + A_3) = c(A_1, A_2 + X)c(X, A_3). \tag{11}$$

Table 2. Correlation of z_j to linear function (Step 2).

Correlation of σ_{j-2} to	Resulting correlation of z_j to	Correlation coefficient
a_{j-2}	$a_j + b_j + a_{j-2}$	0.25
	$a_j + b_j + a_{j-1} + b_{j-1} + a_{j-2}$	−0.25
b_{j-2}	$a_j + b_j + b_{j-2}$	0.25
	$a_j + b_j + a_{j-1} + b_{j-1} + b_{j-2}$	−0.25
σ_{j-3}	$a_j + b_j + \sigma_{j-3}$	0.25
	$a_j + b_j + a_{j-1} + b_{j-1} + \sigma_{j-3}$	−0.25
$a_{j-2} + b_{j-2} + \sigma_{j-3}$	$a_j + b_j + a_{j-2} + b_{j-2} + \sigma_{j-3}$	−0.25
	$a_j + b_j + a_{j-1} + b_{j-1} + a_{j-2} + b_{j-2} + \sigma_{j-3}$	0.25

Proof. Let $c = c(A_1, A_2 + A_3)$, $c' = c(A_1, A_2 + X)$, and $c'' = c(X, A_3)$. We introduce the probabilities $p = P(A_1 = A_2 + A_3)$, $p' = P(A_1 = A_2 + X)$, and $p'' = P(X = A_3)$. By hypothesis and from (10), we have $p' = (1 + c')/2$ and $p'' = (1 + c'')/2$. Therefore

$$\begin{aligned} p &= P(A_1 = A_2 + X)P(X = A_3) + \mathrm{P}(A_1 \neq A_2 + X)P(X \neq A_3) \\ &= p'p'' + (1 - p')(1 - p'') \\ &= \left(\frac{1 + c'}{2}\right)\left(\frac{1 + c''}{2}\right) + \left(\frac{1 - c'}{2}\right)\left(\frac{1 - c''}{2}\right) = \frac{1}{2} + \frac{c'c''}{2}. \end{aligned}$$

This implies $c = 2p - 1 = c'c''$, which proves the lemma. □

The computation of the correlation coefficients in Table 2 according to Lemma 1 is based on the assumption that the random variables invoked in (11) are uniformly distributed. The random variables in Tables 1 and 2 are of the form

$$s = \sum_{k=j-i}^{j} (\alpha_k a_k + \beta_k b_k) \tag{12}$$

or

$$s' = \sum_{k=j-i}^{j} (\alpha_k a_k + \beta_k b_k) + \sigma_{j-i-1}. \tag{13}$$

The sums of type (12) are uniformly distributed, provided only that they are nonzero, whereas the sums of type (13) are also uniformly distributed since σ_{j-i-1} is balanced and independent of $\sum_{k=j-i}^{j} \alpha_k a_k + \beta_k b_k$. Thus the hypothesis of Lemma 1 is satisfied.

From Table 2, we get four additional sums of the form (8), all correlated to z_j with $|c| = 0.25$. This process can be iterated. By induction, in step i we get 2^i sums of the form (12) with $|c| = 2^{-i}$. Hence, for $i \leq j$, we have obtained N sums $s_1, s_2, \ldots, s_N$ of the form (12) where N is given as

$$N = N(i) = \sum_{k=1}^{i} 2^k = 2^{i+1} - 2.$$

The sum of the squares of the corresponding correlation coefficients $c_1, c_2, \ldots, c_N$ satisfies an invariance property similar to that for memoryless combiners in [4], namely

$$\sum_{h=1}^{N} c_h^2 = \sum_{k=1}^{i} 2^k \frac{1}{2^{2k}} = \sum_{k=1}^{i} \frac{1}{2^k} = 1 - \frac{1}{2^i}.$$

This proves the following theorem.

Theorem 1. *Let $1 \leq i \leq j$. Then the output digit z_j of the basic summation combiner is correlated to linear functions $s_1, s_2, \ldots, s_N$ of the form* (12) *where $N = N(i) = 2^{i+1} - 2$, and the corresponding correlation coefficients c_h satisfy*

$$\sum_{h=1}^{N} c_h^2 = 1 - \frac{1}{2^i}. \tag{14}$$

Moreover, for every k, $1 \leq k \leq i$, there are exactly 2^k functions s_h with correlation coefficient $c_h = 2^{-k}$.

Note that the right side of (14) tends to 1 as i (or j) → ∞. This result will be generalized to arbitrary combiners with 1 bit memory.

3. General Combiner with 1 Bit Memory

3.1. *Main Theorem on Correlation Coefficients*

A general combiner with 1 bit memory is described by two functions f_0 and f_1 as follows:

$$z_j = f_0(x_{1j}, \ldots, x_{nj}, \sigma_{j-1}), \tag{15}$$

$$\sigma_j = f_1(x_{1j}, \ldots, x_{nj}, \sigma_{j-1}). \tag{16}$$

It is assumed that $\mathscr{X}_m = (x_{m0}, x_{m1}, x_{m2}, \ldots)$, $1 \leq m \leq n$, are independent and uniformly distributed sequences of random variables. Furthermore, it is supposed that the functions f_0 and f_1 are balanced and that σ_{-1} is uniformly distributed. Then, for every j, σ_j and z_j as defined in (15) and (16) are also uniformly distributed. The generation of the sequence $\mathscr{Z} = (z_0, z_1, z_2, \ldots)$ is illustrated in Fig. 2.

In order to study the correlation properties of this combiner, we investigate correlations of the combining functions f_0, f_1: $\mathrm{GF}(2)^{n+1} \rightarrow \mathrm{GF}(2)$ to linear functions. The correlation of an arbitrary function f: $\mathrm{GF}(2)^{n+1} \rightarrow \mathrm{GF}(2)$ to the linear function $L_{\mathbf{w}}(x) = \mathbf{w} \cdot \mathbf{x}$ ($\mathbf{w}, \mathbf{x} \in \mathrm{GF}(2)^{n+1}$) is readily found from the Walsh coefficient

$$\hat{F}(\mathbf{w}) = \sum_{\mathbf{x} \in \mathrm{GF}(2)^{n+1}} \hat{f}(\mathbf{x})(-1)^{\mathbf{w} \cdot \mathbf{x}}. \tag{17}$$

where $\hat{f}(\mathbf{x}) = (-1)^{f(\mathbf{x})}$ is the Boolean function with values in the multiplicative group $\{1, -1\}$. The correlation coefficient $c(f, L_{\mathbf{w}})$ is thus

$$c(f, L_{\mathbf{w}}) = \frac{\hat{F}(\mathbf{w})}{2^{n+1}}. \tag{18}$$

For the combining functions $f_0(\mathbf{x}, \sigma)$ and $f_1(\mathbf{x}, \sigma)$, $\mathbf{x} \in \mathrm{GF}(2)^n$, we distinguish be-

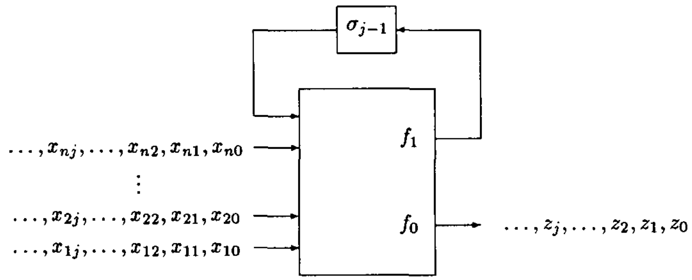

σ_{j-1}
f_1
$\ldots, x_{nj}, \ldots, x_{n2}, x_{n1}, x_{n0}$
$\vdots$
$\ldots, x_{2j}, \ldots, x_{22}, x_{21}, x_{20}$
f_0
$\ldots, z_j, \ldots, z_2, z_1, z_0$
$\ldots, x_{1j}, \ldots, x_{12}, x_{11}, x_{10}$

Fig. 2. General combiner with 1 bit memory.

tween correlation to linear functions of the form

$$L(\mathbf{x}, \sigma) = \mathbf{w} \cdot \mathbf{x} \tag{19}$$

and

$$L(\mathbf{x}, \sigma) = \mathbf{w} \cdot \mathbf{x} + \sigma. \tag{20}$$

For the function f_0, the corresponding correlation coefficients are given by $c_0(\mathbf{w}) = \hat{F}_0(\mathbf{w}, 0)/2^{n+1}$ and $c_1(\mathbf{w}) = \hat{F}_0(\mathbf{w}, 1)/2^{n+1}$, where $\hat{F}_0$ denotes the Walsh transform of $\hat{f}_0$. In order to distinguish between functions of the form (19) and (20), we introduce

$$C_0^2 = \sum_{\mathbf{w} \in \mathrm{GF}(2)^n} c_0(\mathbf{w})^2, \qquad C_1^2 = \sum_{\mathbf{w} \in \mathrm{GF}(2)^n} c_1(\mathbf{w})^2. \tag{21}$$

In a similar way, for the function f_1, we introduce $d_0(\mathbf{w}) = \hat{F}_1(\mathbf{w}, 0)/2^{n+1}$, $d_1(\mathbf{w}) = \hat{F}_1(\mathbf{w}, 1)/2^{n+1}$, and

$$D_0^2 = \sum_{\mathbf{w} \in \mathrm{GF}(2)^n} d_0(\mathbf{w})^2, \qquad D_1^2 = \sum_{\mathbf{w} \in \mathrm{GF}(2)^n} d_1(\mathbf{w})^2. \tag{22}$$

Then, by Parseval's theorem,

$$C_0^2 + C_1^2 = 1 \qquad \text{and} \qquad D_0^2 + D_1^2 = 1. \tag{23}$$

For a generalization of Theorem 1, we compute the correlation of the output z_j of the general combiner (15), (16) to linear functions of the form

$$s = \sum_{k=j-i}^{j} \sum_{m=1}^{n} w_{mk} x_{mk}. \tag{24}$$

In total there are $N = 2^{(i+1)n}$ such functions.

Theorem 2. *Let $1 \le i \le j$. Then the output digit z_j of the general combiner with* 1 *bit memory is correlated to linear functions $s_1, s_2, \ldots, s_N$ of the form* (24) *and the corresponding correlation coefficients c_h satisfy*

$$\sum_{h=1}^{N} c_h^2 = C_0^2 + C_1^2(1 - (D_1^2)^i), \tag{25}$$

where C_0, C_1, and D_1 are defined in (21) *and* (22) *above.*

Proof. Let $\mathbf{x}_j = (x_{1j}, \ldots, x_{nj})$ and $\mathbf{w}_j = (w_{1j}, \ldots, w_{nj})$. Then (24) can be expressed as

$$s = \sum_{k=j-i}^{j} \mathbf{w}_k \cdot \mathbf{x}_k, \tag{26}$$

and similarly

$$z_j = f_0(\mathbf{x}_j, \sigma_{j-1}), \qquad \sigma_j = f_1(\mathbf{x}_j, \sigma_{j-1}).$$

Then, for every $\mathbf{w}_j \in \mathrm{GF}(2)^n$, the output $z_j = f_0(\mathbf{x}_j, \sigma_{j-1})$ is correlated to the linear functions $\mathbf{w}_j \cdot \mathbf{x}_j$ and $\mathbf{w}_j \cdot \mathbf{x}_j + \sigma_{j-1}$. The corresponding correlation coefficients are

$$c(z_j, \mathbf{w}_j \cdot \mathbf{x}_j) = c_0(\mathbf{w}_j), \tag{27}$$

$$c(z_j, \mathbf{w}_j \cdot \mathbf{x}_j + \sigma_{j-1}) = c_1(\mathbf{w}_j). \tag{28}$$

The linear functions in (27) are already of the form (24). The correlation to the

Table 3. Exploiting the correlation of z_j to $\mathbf{w}_j \cdot \mathbf{x}_j + \sigma_{j-1}$.

Correlation of σ_{j-1} to	Correlation coefficient	Resulting correlation of z_j to	Correlation coefficient
$\mathbf{w}_{j-1} \cdot \mathbf{x}_{j-1}$	$d_0(\mathbf{w}_{j-1})$	$\mathbf{w}_j \cdot \mathbf{x}_j + \mathbf{w}_{j-1} \cdot \mathbf{x}_{j-1}$	$c_1(\mathbf{w}_j)d_0(\mathbf{w}_{j-1})$
$\mathbf{w}_{j-1} \cdot \mathbf{x}_{j-1} + \sigma_{j-2}$	$d_1(\mathbf{w}_{j-1})$	$\mathbf{w}_j \cdot \mathbf{x}_j + \mathbf{w}_{j-1} \cdot \mathbf{x}_{j-1} + \sigma_{j-2}$	$c_1(\mathbf{w}_j)d_1(\mathbf{w}_{j-1})$

functions in (28) can be exploited as in Theorem 1, since $\sigma_{j-1} = f_1(\mathbf{x}_{j-1}, \sigma_{j-2})$ is correlated to the linear functions $\mathbf{w}_{j-1} \cdot \mathbf{x}_{j-1}$ and $\mathbf{w}_{j-1} \cdot \mathbf{x}_{j-1} + \sigma_{j-2}$. This leads to correlation of z_j to the functions

$$\mathbf{w}_j \cdot \mathbf{x}_j + \mathbf{w}_{j-1} \cdot \mathbf{x}_{j-1}, \tag{29}$$

$$\mathbf{w}_j \cdot \mathbf{x}_j + \mathbf{w}_{j-1} \cdot \mathbf{x}_{j-1} + \sigma_{j-2}, \tag{30}$$

where in (29) $\mathbf{w}_{j-1}$ is assumed to be nonzero—the functions (29) with $\mathbf{w}_{j-1} = 0$ are already covered in (27). The correlation coefficients are computed according to the product formula (11) and are listed in Table 3. The hypotheses of Lemma 1 are satisfied as all random variables involved in the product formula are uniformly distributed. In particular, $\mathbf{w}_{j-1} \cdot \mathbf{x}_{j-1}$ and $\mathbf{w}_j \cdot \mathbf{x}_j + \mathbf{w}_{j-1} \cdot \mathbf{x}_{j-1}$ in the first row of Table 3 are balanced since $\mathbf{w}_{j-1}$ is assumed to be nonzero. (Note, however, that $\mathbf{w}_{j-1}$ in the second row is allowed to be zero.)

Furthermore, the correlation of σ_{j-2} to $\mathbf{w}_{j-2} \cdot \mathbf{x}_{j-2}$ and $\mathbf{w}_{j-2} \cdot \mathbf{x}_{j-2} + \sigma_{j-3}$ leads to correlation of z_j to $\mathbf{w}_j \cdot \mathbf{x}_j + \mathbf{w}_{j-1} \cdot \mathbf{x}_{j-1} + \mathbf{w}_{j-2} \cdot \mathbf{x}_{j-2}$, where $\mathbf{w}_{j-2} \neq 0$, and to $\mathbf{w}_j \cdot \mathbf{x}_j + \mathbf{w}_{j-1} \cdot \mathbf{x}_{j-1} + \mathbf{w}_{j-2} \cdot \mathbf{x}_{j-2} + \sigma_{j-3}$. The corresponding correlation coefficients are $c_1(\mathbf{w}_j)d_1(\mathbf{w}_{j-1})d_0(\mathbf{w}_{j-2})$ and $c_1(\mathbf{w}_j)d_1(\mathbf{w}_{j-1})d_1(\mathbf{w}_{j-2})$, respectively. By induction, after i steps, we obtain all linear functions of the form (24) correlated to z_j. As a summary, all these functions and their correlation coefficients are listed in Table 4.

Denote by S_0 the set of functions in the first row of Table 4, by S_1 the set of functions in the second row, etc., and by S_i the set of functions in the last row of Table 4. Then $S_0, S_1, \ldots, S_i$ is a partition of the set of functions of the form (24). For the evaluation of (25), we first compute $\sum_{s \in S_p} c(z_j, s)^2$ for each value of p, $0 \leq p \leq i$. For $p = 0$, $\sum_{s \in S_0} c(z_j, s)^2 = C_0^2$ and, for $1 \leq p \leq i$,

$$\sum_{s \in S_p} c(z_j, s)^2 = \sum_{\{\mathbf{w}_{j-k} | 0 \leq k \leq p,\, \mathbf{w}_{j-p} \neq 0\}} c_1(\mathbf{w}_j)^2 d_0(\mathbf{w}_{j-p})^2 \prod_{k=1}^{p-1} d_1(\mathbf{w}_{j-k})^2 = C_1^2 D_0^2 D_1^{2(p-1)}.$$

Table 4. Correlation of z_j to linear functions.

Correlation of z_j to		Correlation coefficient
$\mathbf{w}_j \cdot \mathbf{x}_j$		$c_0(\mathbf{w}_j)$
$\mathbf{w}_j \cdot \mathbf{x}_j + \mathbf{w}_{j-1} \cdot \mathbf{x}_{j-1}$,	$\mathbf{w}_{j-1} \neq 0$	$c_1(\mathbf{w}_j)d_0(\mathbf{w}_{j-1})$
$\mathbf{w}_j \cdot \mathbf{x}_j + \mathbf{w}_{j-1} \cdot \mathbf{x}_{j-1} + \mathbf{w}_{j-2} \cdot \mathbf{x}_{j-2}$,	$\mathbf{w}_{j-2} \neq 0$	$c_1(\mathbf{w}_j)d_1(\mathbf{w}_{j-1})d_0(\mathbf{w}_{j-2})$
$\vdots$	$\vdots$	$\vdots$
$\mathbf{w}_j \cdot \mathbf{x}_j + \mathbf{w}_{j-1} \cdot \mathbf{x}_{j-1} + \cdots + \mathbf{w}_{j-i} \cdot \mathbf{x}_{j-i}$,	$\mathbf{w}_{j-i} \neq 0$	$c_1(\mathbf{w}_j)d_1(\mathbf{w}_{j-1}) \cdots d_1(\mathbf{w}_{j-i+1})d_0(\mathbf{w}_{j-i})$

To explain the last equality, we note that $d_0(\mathbf{w}) = 0$ for $\mathbf{w} = 0$ as f_1 is balanced, and therefore $D_0^2 = \sum_{\mathbf{w}\neq 0} d_0(\mathbf{w})^2$. Thus

$$\sum_{h=1}^{N} c_h^2 = C_0^2 + \sum_{p=1}^{i} C_1^2 D_0^2 D_1^{2(p-1)} = C_0^2 + C_1^2 D_0^2 \frac{1 - D_1^{2i}}{1 - D_1^2} = C_0^2 + C_1^2(1 - D_1^{2i}),$$

which completes the proof of the theorem. □

3.2. *Applications to Stream Ciphers Using LFSRs Components*

In stream ciphers, LFSRs are commonly used for pseudo-random sequence generation since their output typically has good statistical properties. In particular, this holds for maximum-length LFSRs. Therefore, in the analysis of stream ciphers, the output of an LFSR can be modeled by a sequence of independent and uniformly distributed binary random variables. In this framework we can apply our results to key stream generators where several LFSRs are connected to a combiner with memory.

If the input sequences $\mathcal{X}_m = (x_{m0}, x_{m1}, x_{m2}, \ldots)$, $1 \leq m \leq n$, to a combiner with memory are generated by LFSRs, then the correlation of z_j to linear functions, as described in Theorem 2, leads to correlation to sums of LFSRs-sequences and their phase shifts. By (23) and (25), the sum of the squares of the corresponding correlation coefficients converges to 1 as i tends to ∞, except in the (singular) case $D_1 = 1$ (i.e., when $D_0 = 0$). Therefore we make a distinction between the two cases $D_0 \neq 0$ and $D_0 = 0$.

3.2.1. *The Case $D_0 \neq 0$.* According to (24), the linear functions in Table 4 are given by

$$s = \sum_{m=1}^{n} \left(\sum_{k=j-i}^{j} w_{mk} x_{mk} \right). \tag{31}$$

Then, for each m, the inner sum

$$s_m = \sum_{k=j-i}^{j} w_{mk} x_{mk} \tag{32}$$

is a phase of the mth LFSR-sequence. If certain of these s_m's vanish, a divide-and-conquer correlation attack is possible. To prevent such divide-and-conquer attacks *maximum-order correlation immunity* has been postulated in [4], [5], and [6]. According to Theorem 2, the combiner is maximum-order correlation immune if for every linear function in Table 4 with nonvanishing correlation coefficient and for every m, $1 \leq m \leq n$, there is at least one index k with $w_{mk} \neq 0$. Note that this coincides with condition MCI as introduced in [4].

In this framework, Theorem 2 extends Rueppels's treatment of maximum-order correlation immunity in [5] as it covers every kind of correlation to LFSR-sequences originating from the given LFSRs. Such correlations exist even if the combiner is chosen to be maximum-order correlation immune. In fact, in the case $D_0 \neq 0$, the "total correlation" is independent of the combiners f_0 and f_1 as (25) converges to 1. This generalizes a corresponding result in [4] for memoryless combiners.

3.2.2. *The Case $D_0 = 0$.* Motivated by the results for $D_0 \neq 0$, we might be tempted to choose a maximum-order correlation immune combiner in (15) and (16) satisfying $D_0 = 0$. Maximum order correlation immunity implies in particular, that the function $z = f_0(\mathbf{x}, \sigma)$ is not correlated to linear functions $L(\mathbf{x}) = \mathbf{w} \cdot \mathbf{x}$ for $\mathbf{w} \neq \mathbf{1} = (1, \ldots, 1)$. By (18) this means that $\hat{F}_0(\mathbf{w}, 0) = 0$ for $\mathbf{w} \neq \mathbf{1}$. Then the formula for the inverse of the Walsh transform of the function $\hat{f}_0(\mathbf{x}, \sigma) = (-1)^{f_0(\mathbf{x}, \sigma)}$ decomposes as

$$\begin{aligned} \hat{f}(\mathbf{x}, \sigma) &= \frac{1}{2^{n+1}} \sum_{\mathbf{w}} \hat{F}_0(\mathbf{w}, 0)(-1)^{\mathbf{w} \cdot \mathbf{x}} + \frac{1}{2^{n+1}} \sum_{\mathbf{w}} \hat{F}_0(\mathbf{w}, 1)(-1)^{\mathbf{w} \cdot \mathbf{x} + \sigma} \\ &= \hat{g}_0(\mathbf{x}) + (-1)^{\sigma} \hat{h}_0(\mathbf{x}). \end{aligned} \tag{33}$$

The first term in (33) is of the form

$$\hat{g}_0(\mathbf{x}) = d(-1)^{\mathbf{1} \cdot \mathbf{x}} \tag{34}$$

where $d = 2^{-(n+1)} \hat{F}_0(\mathbf{1}, 0)$ is a constant. Since $\hat{f}_0$ is ± 1-valued, we have $|\hat{f}_0(\mathbf{x}, 0)| = |\hat{f}_0(\mathbf{x}, 1)| = 1$, i.e.,

$$|\hat{g}_0(\mathbf{x}) + \hat{h}_0(\mathbf{x})| = |\hat{g}_0(\mathbf{x}) - \hat{h}_0(\mathbf{x})|.$$

Hence, for any $\mathbf{x}$, either $\hat{g}_0(\mathbf{x}) = 0$ or $\hat{h}_0(\mathbf{x}) = 0$. If the coefficient d in (34) is nonzero, then $\hat{h}_0 = 0$. This implies $\hat{f}_0(\mathbf{x}) = d(-1)^{\mathbf{1} \cdot \mathbf{x}}$. Therefore $f_0(\mathbf{x}, \sigma) = x_1 + \cdots + x_n + c$ with $d = (-1)^c$, which means that f_0 is linear or affine. In the case $d = 0$ we have $\hat{f}_0(\mathbf{x}, \sigma) = (-1)^{\sigma} \hat{h}_0(\mathbf{x})$, or in additive notation

$$f_0(\mathbf{x}, \sigma) = h_0(\mathbf{x}) + \sigma, \tag{35}$$

where $\hat{h}_0(\mathbf{x}) = (-1)^{h_0(\mathbf{x})}$. The case of a linear or affine f_0 is not interesting, so we concentrate on functions f_0 of the form (35). A similar decomposition as in (33), applied to the function $\hat{f}_1$, yields

$$\hat{f}_1(\mathbf{x}, \sigma) = \hat{g}_1(\mathbf{x}) + (-1)^{\sigma} \hat{h}_1(\mathbf{x}). \tag{36}$$

Since D_0 is assumed to be zero (i.e., $\hat{F}_1(\mathbf{w}, 0) = 0$ for all $\mathbf{w}$), the first term $\hat{g}_1(\mathbf{x})$ in (36) vanishes for all $\mathbf{x}$. Hence $\hat{f}_1(\mathbf{x}, \sigma) = (-1)^{\sigma} \hat{h}_1(\mathbf{x})$, i.e.,

$$f_1(\mathbf{x}, \sigma) = h_1(\mathbf{x}) + \sigma, \tag{37}$$

where $\hat{h}_1(\mathbf{x}) = (-1)^{h_1(\mathbf{x})}$. Thus by (35) and (37), $z_j = h_0(\mathbf{x}_j) + \sigma_{j-1}$ and $\sigma_{j-1} = h_1(\mathbf{x}_{j-1}) + \sigma_{j-2}$, and therefore $z_j = h_0(\mathbf{x}_j) + h_1(\mathbf{x}_{j-1}) + \sigma_{j-2}$. On the other hand, $z_{j-1} = h_0(\mathbf{x}_{j-1}) + \sigma_{j-2}$, which implies

$$z_j + z_{j-1} = h_0(\mathbf{x}_j) + h_0(\mathbf{x}_{j-1}) + \mathbf{h}_1(\mathbf{x}_{j-1}). \tag{38}$$

This means that the sequence $z_j' = z_j + z_{j-1}$ is generated by a memoryless combiner. Hence by a result in [4], z_j' is correlated to LFSR-sequences with correlation coefficients c_i with the property that

$$\sum_i c_i^2 = 1.$$

Thus, by choosing the combiner according to (35) and (37), we can cause all the correlation coefficients in Theorem 2 to vanish. However, the sequence $\mathscr{X}'$, which is easily obtained from $\mathscr{X}$, has correlation to LFSR-sequences as in the case where $D_0 \neq 0$.

4. Correlation Conditioned on Known Output Sequence

4.1. *Basic Summation Combiner*

The basic summation combiner (see (6) and (7))

$$z_j = f_0(a_j, b_j, \sigma_{j-1}) = a_j + b_j + \sigma_{j-1}$$
$$\sigma_j = f_1(a_j, b_j, \sigma_{j-1}) = a_j b_j + a_j \sigma_{j-1} + b_j \sigma_{j-1},$$

is maximum-order correlation immune in the sense of the previous section. In addition, on average, the output z_j and the sum $a_j + b_j$ are uncorrelated as the carry σ_{j-1} is balanced. However, it is shown in this section that, under certain conditions, knowledge of portions of the output sequence can considerably reduce the uncertainty about the carry bit. This affects correlation of z_j to $a_j + b_j$ (or to other sums of input digits). These correlations may be much stronger than those described in Theorems 1 and 2.

Denote by $I_j = a_j + b_j$ the integer sum of a_j and b_j. Then the probability distribution of I_j is given by

I_j	0	1	2
p	0.25	0.5	0.25

(39)

The carry σ_j as a function of σ_{j-1} and I_j is shown in Table 5, where the entries for σ_j in the frames indicate that the corresponding output z_j is 0.

For $j = 0, 1, 2, \ldots$, denote by $q_j(0)$ and $q_j(1)$ the probability that the carry bit σ_j is in state 0 and state 1, respectively. From Table 5 and (39), we conclude that the carry bit changes with probability 0.25 and remains unchanged with probability 0.75, and therefore

$$\begin{pmatrix} q_j(0) \\ q_j(1) \end{pmatrix} = \begin{pmatrix} \frac{3}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{3}{4} \end{pmatrix} \begin{pmatrix} q_{j-1}(0) \\ q_{j-1}(1) \end{pmatrix}. \tag{40}$$

The transition matrix A in (40) can be written in the form $A = S^{-1}DS$ where D is a

Table 5. The carry σ_j as function of σ_{j-1} and I_j.

	I_j		
σ_{j-1}	0	1	2
0	$\boxed{0}$	0	$\boxed{1}$
1	0	$\boxed{1}$	1

diagonal matrix, namely

$$A = \begin{pmatrix} \frac{3}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{3}{4} \end{pmatrix} = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix}.$$

The probability distribution $\mathbf{q}_j = (q_j(0), q_j(1))$ of σ_j is related to the probability distribution $\mathbf{q}_0 = (q_0(0), q_0(1))$ of σ_0 by the equation $\mathbf{q}_j = A^j\mathbf{q}_0 = S^{-1}D^jS\mathbf{q}_0$. Thus $\mathbf{q}_j$ is easily obtained as

$$q_j(0) = \frac{1}{2} + \frac{1}{2^{j+1}}(q_0(0) - q_0(1)),$$

$$q_j(1) = \frac{1}{2} - \frac{1}{2^{j+1}}(q_0(0) - q_0(1)),$$

which shows that, for any initial value $\mathbf{q}_0$, the probability distribution $\mathbf{q}_j$ converges to the uniform distribution.

Now suppose that the output z_j is known to be 0. Then the input I_j and the carry σ_{j-1} are restricted to the values as indicated by the frames in Table 5. Therefore the carry bit changes with probability 0.5 if $\sigma_{j-1} = 0$ and remains unchanged if $\sigma_{j-1} = 1$. Thus, instead of (40), the relation between the probabilities $\mathbf{q}_j$ and $\mathbf{q}_{j-1}$ (conditioned on $z_j = 0$) is given by

$$\begin{pmatrix} q_j(0) \\ q_j(1) \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & 0 \\ \frac{1}{2} & 1 \end{pmatrix} \begin{pmatrix} q_{j-1}(0) \\ q_{j-1}(1) \end{pmatrix}. \tag{41}$$

Assume that a run of s consecutive output digits 0 has been observed, e.g., $z_{j+1} = z_{j+2} = \cdots = z_{j+s} = 0$. Then the (conditional) probabilities $\mathbf{q}_{j+s}$ and $\mathbf{q}_j$ are related by $\mathbf{q}_{j+s} = A^s\mathbf{q}_j$, where the transition matrix A^s is obtained as

$$A^s = \begin{pmatrix} \frac{1}{2} & 0 \\ \frac{1}{2} & 1 \end{pmatrix}^s = \begin{pmatrix} 1/2^s & 0 \\ 1 - 1/2^s & 1 \end{pmatrix}. \tag{42}$$

Therefore, for any value of $\mathbf{q}_j$, the probability distribution $\mathbf{q}_{j+s}$ satisfies the inequalities

$$q_{j+s}(0) \le \frac{1}{2^s} \quad \text{and} \quad q_{j+s}(1) \ge 1 - \frac{1}{2^s}. \tag{43}$$

Moreover, for $1 \le t \le s$, we have $P(\sigma_{j+s} = \sigma_{j+s-1} = \cdots = \sigma_{j+t+1} = 1 | \sigma_{j+t} = 1) = 1$ since $\sigma_{j+s} \cdots \sigma_{j+t+1}$ remain unchanged if $\sigma_{j+t} = 1$. By (43), $P(\sigma_{j+t} = 1) \ge 1 - 2^{-t}$. This implies

$$P(\sigma_{j+s} = \sigma_{j+s-1} = \cdots = \sigma_{j+t} = 1) \ge 1 - \frac{1}{2^t}. \tag{44}$$

Similarly, assume that in the output of the basic summation combiner a run of s consecutive digits $z_{j+1} = z_{j+2} = \cdots = z_{j+s} = 1$ has been observed. Then the carries tend to be zero; more precisely, for every t with $1 \le t \le s$, the conditional probability

$P(\sigma_{j+s} = \sigma_{j+s-1} = \cdots = \sigma_{j+t} = 0)$ satisfies

$$P(\sigma_{j+s} = \sigma_{j+s-1} = \cdots = \sigma_{j+t} = 0) \geq 1 - \frac{1}{2^t}. \tag{45}$$

Since by (44) and (45) the carries are biased, the output z_{j+t} is correlated to sums of inputs $a_{j+t} + b_{j+t}$ and to other sums of inputs as shown in the following theorem.

Theorem 3.

(1) *Suppose that the output of the basic summation combiner satisfies* $z_{j+1} = z_{j+2} = \cdots = z_{j+s} = 0$ *and* $z_{j+s+1} = 1$. *Then, for every* t *with* $1 \leq t \leq s$, *the* $s - t + 2$ *equations*

$$\begin{aligned} z_{j+t+1} &= a_{j+t+1} + b_{j+t+1} + 1 = 0, \\ z_{j+t+2} &= a_{j+t+2} + b_{j+t+2} + 1 = 0, \\ &\vdots \\ z_{j+s+1} &= a_{j+s+1} + b_{j+s+1} + 1 = 1, \\ z_{j+s+2} &= a_{j+s+2} + b_{j+s+2} + a_{j+s+1}, \end{aligned} \tag{46}$$

are simultaneously satisfied with probability at least $1 - 2^{-t}$.

(2) *Suppose that the output of the basic summation combiner satisfies* $z_{j+1} = z_{j+2} = \cdots = z_{j+s} = 1$ *and* $z_{j+s+1} = 0$. *Then, for every* t *with* $1 \leq t \leq s$, *the* $s - t + 2$ *equations*

$$\begin{aligned} z_{j+t+1} &= a_{j+t+1} + b_{j+t+1} = 1, \\ z_{j+t+2} &= a_{j+t+2} + b_{j+t+2} = 1, \\ &\vdots \\ z_{j+s+1} &= a_{j+s+1} + b_{j+s+1} = 0, \\ z_{j+s+2} &= a_{j+s+2} + b_{j+s+2} + a_{j+s+1}, \end{aligned} \tag{47}$$

are simultaneously satisfied with probability at least $1 - 2^{-t}$.

Proof. The first $s - t + 1$ equations in (46) and (47) follow from (44) and (45). For the verification of the last equation in (46), recall the assumption $z_{j+s+1} = 1$ and $z_{j+s} = 0$. Then by (44), with probability at least $1 - 2^{-t}$, we have $\sigma_{j+s} = 1$. Under this hypothesis, $1 = z_{j+s+1} = I_{j+s+1} + 1 \pmod 2$. Thus either $I_{j+s+1} = 0$ and $\sigma_{j+s+1} = 0$, or $I_{j+s+1} = 2$ and $\sigma_{j+s+1} = 1$. In either case, $\sigma_{j+s+1} = a_{j+s+1}$ (or $\sigma_{j+s+1} = \mathrm{b}_{j+s+1}$). Hence, with probability at least $1 - 2^{-t}$, we have $z_{j+s+2} = a_{j+s+2} + b_{j+s+2} + a_{j+s+1}$. The relations (47) are proved similarly. □

Observe that Theorem 3, which states that (46) and (47) are simultaneously satisfied with a certain probability, is much stronger than the statement that these equations are individually satisfied with the same probability. This fact can be cryptanalytically exploited as described in Section 5. Note also that the last relation in (46) or (47) has already been encountered in Table 1. However, stronger (as well as new) correlations may result when the output is known.

4.2. *Summation Combiner with More than Two Inputs*

For a summation combiner with $n \geq 3$ inputs, the carry can take on the values 0, $1, \ldots, n - 1$. Therefore this combiner has more than 1 bit memory. With regard to Section 4.1, we are led to investigate the probability distribution of the carry in this more general setting. If the carries turn out to be biased, there will be correlation between the output and the sum of the inputs.

The computation of the probability distribution of the carry in the general case is beyond the scope of the present paper. This is the subject of a subsequent publication [9]. In particular, it is shown in [9] that the weakness, as found in Theorem 3, does not appear if $n > 2$ inputs are added. However, there remains a bias of the carry if n is odd and a bias for even n if the probabilities are conditioned on the output. Furthermore, it is shown in [9] that this bias diminishes as n increases.

5. Cryptanalysis of the Summation Cipher with Two LFSRs

5.1. *A Cryptanalytic Algorithm*

In an implementation of the basic summation cipher, the two input sequences to the adder are produced by LFSRs. Then the systems of equations in Theorem 3 can be cryptanalytically exploited in a known plaintext attack.

Suppose that a run $z_{j+1}, \ldots, z_{j+s}$ of s consecutive 0's or 1's has been observed in the key stream sequence. Then, by considering the digits $z_{j+t+1}, \ldots, z_{j+s+2}$, we obtain $s - t + 2$ equations of the form (46) or (47) that are simultaneously satisfied with probability at least $1 - 2^{-t}$. The actual value of t, which is a parameter for the reliability of the equations, may be chosen depending on the length of the known portion of the key stream. Since the digits a_j and b_j in (46) and (47) are linearly expressed in terms of the initial state of the two LFSRs, we obtain a system of $s - t + 2$ linear equations for the initial digits of the LFSRs. Our aim is to find sufficiently many such systems with highest reliability that can be suitably combined to a system of linear equations for the initial digits.

For a more precise description of our analysis, we introduce the following notation. Let N be the length of the known key stream sequence and let k be the key size (which is the sum of the LFSR-lengths). The key stream is scanned for runs of at least s consecutive 0's or 1's. Suppose that a total number n of such runs have been found. According to the desired reliability, we choose the parameter t and we obtain, as described above, a "block" of $d = s - t + 2$ equations for each run. Thus we get at least nd equations for the initial digits. We assume that $nd > k$, i.e., that $nd = \alpha k$ where $\alpha > 1$. To solve for the key, we need only $m = \lceil k/d \rceil \approx \alpha^{-1} n$ "correct" blocks of equations. In order to find m correct blocks, we proceed as follows.

1. Randomly choose m out of the n available blocks and solve the resulting system of linear equations for the k unknowns.
2. Test all possible solutions obtained in Step 1 to see whether they produce the correct key stream. If there is a correct solution terminate, else go to Step 1.

The complexity of this cryptanalytic algorithm is dominated by the total number of trials. To get an estimate of this number, we observe that each block has probability ρ of being incorrect where $\rho \leq 2^{-t}$. Then the expected number of trials needed is the reciprocal value of the probability q that, by sampling without replacement, m randomly chosen blocks are correct. We estimate this probability in a typical situation where ρn blocks are incorrect. (Assume here for simplicity that ρn is an integer.) Then q is estimated as

$$q = \left(1 - \frac{\rho n}{n}\right)\left(1 - \frac{\rho n}{n-1}\right)\cdots\left(1 - \frac{\rho n}{n-(m-1)}\right) \tag{48}$$

$$> \left(1 - \frac{\rho n}{n-m}\right)^m = \left(1 - \frac{\alpha\rho}{\alpha - 1}\right)^m. \tag{49}$$

As an illustration, we consider the following example.

Example. Consider a basic summation cipher with two LFSRs of length approximately 200, i.e., $k = 400$. Suppose that we have $N = 50{,}000$ digits of the key stream sequence. If this sequence is scanned for runs then, on average,

$$n \approx \frac{N}{2^s} \tag{50}$$

runs of length at least s are to be expected (see [1, p. 322ff.]). If we choose $s = 7$, we obtain $n = 390$ runs of length at least 7. Take $t = 4$. Then $d = s - t + 2 = 5$ is the length of a block and $\rho = 2^{-4} = 1/16$ is the probability of a block being incorrect. Moreover, $m = k/d = 80$ blocks of equations are needed to solve for the key. The value of α is obtained as $\alpha = n/m = 390/80 = 4.88$. Thus

$$q > \left(1 - \frac{4.88}{3.88}\cdot\frac{1}{16}\right)^{80} = 0.0014 \qquad \text{and} \qquad q^{-1} < 699.$$

Therefore, less than 700 trials are sufficient in this typical situation.

This example shows that the summation cipher with only two LFSRs can be successfully cryptanalyzed for LFSRs of considerable length with arbitrary feedback connection. For given N and k, the parameters s and t can be chosen to minimize the number of trials. If, in the above example, N is larger, the average number of trials can be decreased by choosing longer runs (i.e., larger s and t) in order to get blocks with higher reliability. Note that our algorithm also works if the known portion of the key stream has some (but not too many) gaps.

5.2. *Comments on the Cryptanalytic Algorithm*

The success of our algorithm rests on the property of the basic summation combiner as observed in Theorem 3. It is shown in [9] that a similar cryptanalysis is no longer possible for a summation cipher with more than two LFSRs. From this point of view, it is recommended to take several LFSRs of moderate length rather than just a few long LFSRs.

The method of our algorithm can be described in more general terms. Basically, the cryptanalytic problem consists in finding a k-bit key. Observing that this key is determined by a number $m = k/d$ of (correct) blocks of equations, we search for $m = k/d$ such blocks instead of the k unknown bits. Since a block is correct, with probability at least $1 - 2^{-t} \geq 0.5$, this procedure may be compared with an exhaustive search over only k/d bits instead of k bits. This is similar to the effect of a reduction of the key size by the factor d. However, if certain blocks are incorrect they cannot be corrected like a single bit. Therefore a set S of more than m blocks is required in order to find m correct blocks.

Let n denote the total number of available blocks and ρ the probability of a block being incorrect. Then $n - \rho n$ blocks are expected to be correct. Hence it is necessary that $n - \rho n$ is larger than m. Therefore it is favorable to have ρ small and $\alpha = n/m$ large. In fact, already for $\alpha \approx 5$ and ρ only slightly smaller than 0.5, our cryptanalytic algorithm is much faster than an exhaustive search even if the blocks consist of single bits, i.e., if $d = 1$ and $k = m$.

In the case $d = 1$, our method leads to a procedure to find k correct bits out of a set of n bits, where each bit in the set is assumed to be incorrect with probability ρ. This is exactly the situation one is faced with in the general correlation problem in cryptanalysis. In this direction, our method applies to increase the efficiency of a cryptanalytic algorithm described in [3].

Algorithm A in [3] addresses the problem of determining the initial digits of a k-bit LFSR (with few feedback taps) from a disturbed output sequence of the LFSR. The algorithm describes a method to find k digits with the highest probability of being undisturbed. These digits are taken as an estimate of the LFSR-sequence at the corresponding positions. Then the correct sequence is found by testing modifications of this estimate. Again, denote by ρ the probability of a selected bit to be incorrect. It is shown in [3] that, on average,

$$W_0 = 2^{h(\rho)k} \tag{51}$$

trials are necessary where $h(\rho)$ denotes the binary entropy function.

We can improve algorithm A by applying the method as introduced in Section 5.1. According to this method, we start with a set S of more than k digits having a high probability of being undisturbed. Then we choose k digits from this set randomly and test these whether they are correct, i.e., whether they determine the correct LFSR-sequence. This process is repeated until k correct digits have been found.

We express the cardinality of the set S as a multiple of k, i.e., $|S| = \alpha k$ where $\alpha > 1$. According to (49) it is favorable to choose S (or α) as large as possible. On the other hand, for increasing cardinality of S, the reliability of the selected digits will decrease (see [3]). However, for moderate α (e.g., $\alpha = 4$ or 5), the error probability ρ turns out to be roughly the same as for $\alpha = 1$. Therefore, according to (49), in a typical situation the average number of trials is less than

$$W_1 = \left(1 - \frac{\alpha}{\alpha - 1}\rho\right)^{-k} = 2^{-\log_2(1-(\alpha/(\alpha-1))\rho)k}. \tag{52}$$

For a comparison of the two work factors W_0 and W_1, we may assume that the

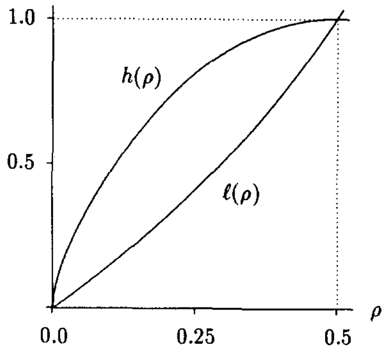


Fig. 3. Comparison of $h(\rho)$ and $l(\rho)$.

fraction $\alpha/(\alpha - 1)$ in (52) is close to 1. Thus (52) can be replaced by

$$W_1 = 2^{l(\rho)k}, \tag{53}$$

where $l(\rho) = -\log_2(1 - \rho)$. Formulas (51) and (53) show that both methods have exponential complexity. However, the exponent in (53) is smaller than that in (51), as is illustrated in Fig. 3. In particular, for small ρ, the value $l(\rho)$ is a small fraction of $h(\rho)$. In fact,

$$\lim_{\rho \to 0} \frac{h(\rho)}{l(\rho)} = \infty. \tag{54}$$

Thus the method of Section 5.1 leads to a substantial improvement of algorithm A, as is also illustrated in the following example. (A similar improvement has independently been found by R. Haefelin.)

Example. Consider an LFSR of length $k = 200$ with few feedback taps. Then, with the method of algorithm A, it is feasible to find, e.g., a set S of 1000 digits with error probability lower than 0.1, i.e., with $\alpha = 5$ and $\rho \leq 0.1$. Then, in order to find the LFSR-sequence with a search as in the original algorithm A, (51) shows that 2^{94} trials would be necessary on the average. However, if the improved algorithm A is applied, the number of trials according to (48) can be estimated as 2^{34}.

In order to find sufficiently many digits with small ρ, it has to be assumed (as in [3]) that the number of feedback taps is small. In fact, for LFSRs with more than ten feedback taps, the feasibility of the improved algorithm is roughly limited to the same conditions as the original algorithm A.

References

[1] W. Feller, *An Introduction to Probability Theory and its Applications*, Vol. 1, Wiley, New York, 1968.

[2] J. L. Massey, R. A. Rueppel, Method of, and Apparatus for, Transforming a Digital Data Sequence into a Encoded Form, U.S. Patent No. 4,797,922, 1989.

[3] W. Meier, O. Staffelbach, Fast correlation attacks on certain stream ciphers, *Journal of Cryptology*, Vol. 1, No. 3 (1989), pp. 159–176.

[4] W. Meier, O. Staffelbach, Nonlinearity criteria for cryptographic functions, *Advances in Cryptology —Eurocrypt '89, Proceedings*, Springer-Verlag, Berlin, 1990, pp. 549–562.

[5] R. A. Rueppel, Correlation immunity and the summation generator, *Advances in Cryptology—Crypto '85, Proceedings*, Springer-Verlag, Berlin, 1986, pp. 260–272.

[6] R. A. Rueppel, *Analysis and Design of Stream Ciphers*, Springer-Verlag, Berlin, 1986.

[7] R. A. Rueppel, J. L. Massey, The knapsack as a non-linear function, *IEEE Int. Symp. Inform. Theory*, Brighton, England, Abstracts of Papers, 1985, p. 46.

[8] T. Siegenthaler, Correlation-immunity of nonlinear combining functions for cryptographic applications, *IEEE Trans. Inform. Theory*, Vol. 30 (1984), pp. 776–780.

[9] O. Staffelbach, W. Meier, Cryptographic significance of the carry for ciphers based on integer addition, *Proceedings of Crypto '90*, Springer-Verlag, Berlin (to appear).