J. Cryptology (1996) 9: 111–126

Journal of
CRYPTOLOGY

Correlation Properties of a General Binary Combiner with Memory*

Jovan Dj. Golić
Information Security Research Centre, Queensland University of Technology, GPO Box 2434, Brisbane, Queensland 4001, Australia
golic@fit.qut.edu.au
School of Electrical Engineering, University of Belgrade, Belgrade, Yugoslavia

Communicated by Rainer Rueppel

Received 8 April 1994 and revised 16 January 1995

Abstract. Correlation properties of a general binary combiner with an arbitrary number M of memory bits are derived and novel design criteria proposed. For any positive integer m, the sum of the squares of the correlation coefficients between all nonzero linear functions of m successive output bits and all linear functions of the corresponding m successive inputs is shown to be dependent upon a particular combiner, unlike the memoryless combiners. The minimum and maximum values of the correlation sum as well as the necessary and sufficient conditions for them to be achieved are determined. It turns out that the security of combiners with memory can be considerably improved if M is not small.

An efficient linear sequential circuit approximation (LSCA) method is developed for obtaining output and input linear functions with comparatively large correlation coefficients which is feasible for large M and works for any practical scheme. The method consists in deriving and solving a linear sequential circuit with additional nonbalanced inputs that is based on linear approximations of the output and the component next-state functions. The corresponding correlation attack on combiners with linear feedback shift registers is analyzed and it is shown that every such combiner with or without memory is essentially zero-order correlation immune.

Key words. Keystream generators, Combiners with memory, Correlation properties, Linear sequential circuit approximation.

* A preliminary version of this paper was presented at Eurocrypt '92 and was published in the proceedings. This research was supported in part by the Science Fund of Serbia, Grant #0403, through the Institute of Mathematics, Serbian Academy of Arts and Sciences.

1. Introduction

Linear feedback shift registers (LFSRs) in binary keystream generators for cryptographic applications are commonly combined by memoryless functions. It is shown in [9] and [10] that such structures are vulnerable to divide-and-conquer correlation attacks based on the termwise correlation between the keystream sequence and a set of the LFSR sequences. In [9] the corresponding concept of correlation immunity of Boolean functions is introduced and the tradeoff between the linear complexity and the correlation immunity is pointed out. According to [11], it follows that the output of any Boolean function is correlated to at least one linear function of its inputs. Once such a linear function has been determined, it is in principle possible to apply either the basic [10] or the fast [4] correlation attack in order to reconstruct the initial states of the LFSRs. The attacks are successful only if the corresponding correlation coefficient is large enough in magnitude. Furthermore, it is shown in [5] that the sum of the squares of the correlation coefficients to all the linear functions of the inputs is equal to one for every Boolean function. This implies that for a memoryless combiner with N inputs the largest magnitude of the correlation coefficients cannot be made smaller than $2^{-N/2}$, which provides an upper bound on the security of such schemes against the correlation attacks.

The use of functions with memory in shift-register-based keystream generators is suggested in [8] and [7] in order to overcome the tradeoff between the linear complexity and the correlation immunity. The notion of correlation immunity is extended to combiners with memory and it is shown that it is possible to achieve the maximum-order correlation immunity, regardless of the linear complexity, by using only one bit of memory. Correlation properties of combiners with one bit of memory are further investigated in [6] where the sum of the squares of the correlation coefficients between any output bit and all the linear functions of successive inputs is derived. As a consequence, it is shown that there are combiners with one bit of memory for which each bit of output is statistically independent of all the input sequences. However, it is proved that for such combiners the sum of two successive output bits is a memoryless function of two successive inputs which implies that the corresponding sum of the squares of the correlation coefficients is equal to one. Still, this sum is not determined in the general case when individual output bits need not be statistically independent of the input sequences.

In this paper we study the correlation properties of a general binary combiner with an arbitrary number M of memory bits. We prove that there is a nontrivial (nonzero) linear function of at most $M + 1$ successive output bits that is correlated to a certain linear function of at most $M + 1$ successive inputs. Moreover, for any positive integer m, the sum of the squares of the correlation coefficients between all nontrivial linear functions of m successive output bits and all linear functions of the corresponding m successive inputs is shown to be dependent upon the particular function with memory, unlike the memoryless combiners. It is proved that the minimum value of this sum for all m is achieved if and only if M successive output bits are balanced and statistically independent of the corresponding M successive inputs, which is a new design criterion. For example, the maximum-order correlation immune combiners with one bit of memory defined in [8] satisfy this condition. The minimum correlation sum is equal to zero for $m \leq M$ and to $2^{m-M} - 1$ for $m > M$. In particular, for $m = M + 1$ the minimum correlation sum is equal to one. Consequently, for a combiner with N inputs and M bits of memory, it

turns out that the largest magnitude of the correlation coefficients cannot be smaller than $2^{-(MN+M+N)/2}$, which pertains to the case when $m = M + 1$. This clearly shows the gain in security that could be obtained by using memory. Namely, the total correlation can remain the same as for the memoryless combiners while the number of linear functions among which the correlation is distributed increases exponentially with MN.

When both N and M are relatively small, all the mutually correlated input and output linear functions can be obtained by exhaustive search possibly by employing the Walsh transform technique [7] for Boolean functions. However, when N or M are large this is no longer possible. We develop an efficent procedure for finding input and output linear functions with comparatively large correlation coefficients which is based on the so-called linear sequential circuit approximation of functions with memory. The corresponding divide-and-conquer correlation attack is then examined in more detail and it is shown that the notion of correlation immunity is somewhat artificial for combiners with or without memory based on linear feedback shift registers. More precisely, such combiners essentially prove to be zero-order correlation immune.

A general binary combiner with memory is defined in Section 2, correlation properties of vector Boolean functions are derived in Section 3, and the correlation properties of a general binary combiner with memory are established in Section 4. The linear sequential circuit approximation method is developed in Section 5 and the correlation attack is discussed in Section 6. Conclusions, design criteria, and some open problems are presented in Section 7.

2. General Binary Combiner with Memory

A general binary combiner with M bits of memory and N inputs is a nonautonomous sequential circuit or finite-state machine defined by

$$S_{t+1} = F(X_t, S_t), \qquad t \geq 0, \tag{1}$$

$$y_t = f(X_t, S_t), \qquad t \geq 0, \tag{2}$$

where F: $\mathrm{GF}(2)^N \times \mathrm{GF}(2)^M \to \mathrm{GF}(2)^M$ is a next-state vector Boolean function, f: $\mathrm{GF}(2)^N \times \mathrm{GF}(2)^M \to \mathrm{GF}(2)$ is an output Boolean function, $S_t = (s_{1t}, \ldots, s_{Mt})$ is a state vector at time t, S_0 is an initial state, $X_t = (x_{1t}, \ldots, x_{Nt})$ is an input vector at time t, and y_t is the output bit at time t. We use the notation $F(X, S)$ and $f(X, S)$ for the next-state and output functions, respectively. In the correlation analysis we consider a probabilistic model in which the inputs are assumed to be mutually independent, balanced (uniformly distributed), and independent sequences of binary random variables $\{x_{it}\}_{t=0}^{\infty}$, $1 \leq i \leq N$. For simplicity, the initial state is also assumed to be a balanced random variable independent of all the inputs which is especially appropriate if it is controlled by a secret key. As usual, throughout the paper we use the same notation for the random variables and their values. Consequently, the output $\{y_t\}_{t=0}^{\infty}$ is also a sequence of binary random variables. Our objective is to investigate the statistical dependence between the output and input sequences.

A basic condition to be satisfied for cryptographic applications is that the output sequence is balanced and independent. For memoryless combiners this is true if and only if the output function is balanced. For combiners with memory the situation is

more complicated because memory can introduce statistical dependence. It is easy to see that regardless of the next-state function $F(X, S)$ and for each initial state S_0, the output sequence is balanced and independent if the output function $f(X, S)$ is balanced for each S, that is, balanced and statistically independent of S. For example, the maximum-order correlation immune combiners with one bit of memory from [8] satisfy this condition. The condition is not necessary except when the initial state is not regarded as a random variable, because some of the state sequences can also be balanced and independent. More precisely, let both the input and state variables be divided into two disjoint groups $X = (X', X'')$ and $S = (S', S'')$, respectively, and let $F'(X, S)$ denote the part of the next-state function corresponding to S'. Then the output sequence is balanced and independent if F' is balanced for each X'' and S and if f is balanced for each X' and S''. Both the sufficient conditions are general and easy to control. Note that in both cases the output function f should be balanced.

Another condition which is important for theoretical correlation analysis is that the next-state function F is balanced. Then the state vector S_t is balanced for every $t \geq 0$ provided that the initial state vector is balanced, because X_t and S_t are independent for every $t \geq 0$. Note that our results essentially remain correct even if S_0 is regarded as a fixed rather than a random variable as long as S_t rapidly converges to a balanced random variable as t increases, provided that the Markov chain for the corresponding next-state probability distribution is ergodic. In particular, if $F(X, S)$ is balanced for each S, then S_t is balanced for every $t \geq 1$.

3. Correlation Properties of Vector Boolean Functions

In this section we study the correlation properties of vector Boolean functions which are needed for the correlation analysis of a general binary combiner with memory in the next section. Let F: $\mathrm{GF}(2)^{n_1} \times \mathrm{GF}(2)^{n_2} \to \mathrm{GF}(2)^m$ denote an arbitrary vector Boolean function of $n = n_1 + n_2$ variables. We use the notation $Z = F(X, Y)$, where $X \in \mathrm{GF}(2)^{n_1}$ and $Y \in \mathrm{GF}(2)^{n_2}$. Assume that X and Y are independent and balanced random variables. Our aim is to analyze the statistical dependence between the random variables Z and X. To this end, first define

$$N_{XZ} = \#\{Y\colon Z = F(X, Y)\} \tag{3}$$

and

$$N_Z = \sum_{X \in \mathrm{GF}(2)^{n_1}} N_{XZ}. \tag{4}$$

It follows that

$$\sum_{Z \in \mathrm{GF}(2)^m} N_{XZ} = 2^{n_2}, \qquad X \in \mathrm{GF}(2)^{n_1}. \tag{5}$$

It is clear that Z is statistically independent of X if and only if $N_{XZ} = 2^{-n_1} N_Z$ for every X and Z, and that Z is functionally dependent on X if and only if for each X a value of Z exists for which $N_{XZ} = 2^{n_2}$. In order to express the degree of statistical dependence of Z upon X between these two extreme cases, we now consider the correlation of linear functions of the output to linear functions of the input. Let the dot product $L_W(X) = W \cdot X$

denote a linear function of X determined by $W \in \mathrm{GF}(2)^{n_1}$ and let $L_V(F) = V \cdot F$ denote a linear combination of the component functions of F determined by $V \in \mathrm{GF}(2)^m$. The correlation coefficient [5] between the Boolean functions $L_V(F)$ and L_W is defined by

$$c_{VW} = \frac{1}{2^{n-1}}\#\{(X, Y):\ V \cdot F(X, Y) = W \cdot X\} - 1. \tag{6}$$

Interestingly enough, the following lemma shows that the total correlation between the considered output and input linear functions can be expressed only in terms of the numbers N_{XZ} which are proportional to the corresponding joint probabilities. The lemma can be proved after certain algebraic manipulations with the Walsh transforms of the output linear functions. Note that $\mathbf{0}$ denotes the all zero vector of appropriate dimension.

Lemma 3.1.

$$C_0 \stackrel{\text{def}}{=} \sum_{V \neq \mathbf{0}} c_{V\mathbf{0}}^2 = \frac{1}{2^m} \sum_{Z} \left(\frac{N_Z}{2^{n-m}} \right)^2 - 1, \tag{7}$$

$$C_1 \stackrel{\text{def}}{=} \sum_{V \neq \mathbf{0}} \sum_{W \neq \mathbf{0}} c_{VW}^2 = \frac{1}{2^{n_1+m}} \sum_{X} \sum_{Z} \left(\frac{N_{XZ}}{2^{n_2-m}} - \frac{N_Z}{2^{n-m}} \right)^2, \tag{8}$$

$$C_2 \stackrel{\text{def}}{=} C_0 + C_1 = \sum_{V \neq \mathbf{0}} \sum_{W} c_{VW}^2 = \frac{1}{2^{n_1+m}} \sum_{X} \sum_{Z} \left(\frac{N_{XZ}}{2^{n_2-m}} \right)^2 - 1. \tag{9}$$

A direct consequence of Lemma 3.1 is the following property which covers the extreme cases.

Property 3.1. The correlation sum C_0 is equal to its minimum value zero if and only if F is balanced and is equal to its maximum value $2^m - 1$ if and only if F is constant. The correlation sum C_1 is equal to its minimum value zero if and only if $F(X, Y)$ is statistically independent of X and is equal to its maximum value $2^m - 1 - C_0$, given C_0, if and only if $F(X, Y)$ is functionally dependent on X. The correlation sum C_2 is equal to its minimum value zero if and only if $F(X, Y)$ is balanced and statistically independent of X and is equal to its maximum value $2^m - 1$ if and only if $F(X, Y)$ is functionally dependent on X.

Lemma 3.1 together with Property 3.1 essentially means that the sum C_1 of the squares of the correlation coefficients between all nontrivial (nonzero) linear functions of $F(X, Y)$ and X, respectively, represents the quadratic measure of statistical dependence between $F(X, Y)$ and X. On the other hand, the sum C_0 of the squares of the correlation coefficients between all nontrivial linear functions of $F(X, Y)$ and the constant zero function represents the quadratic measure of the distribution nonuniformity of $F(X, Y)$. The well-known result [5] on the sum of the squares of the correlation coefficients for Boolean functions is a special case of (9) when $m = 1$ and $n_2 = 0$.

The statistical independence case in Property 3.1 can be further developed by using the following two facts regarding the correlation coefficients. First, the correlation coefficient

between a Boolean function and the constant zero function is equal to zero if and only if the function is balanced. Second, the correlation coefficient between two Boolean functions, one of which is balanced, is equal to zero if and only if they are statistically independent and also if and only if their sum is balanced. Accordingly, Lemma 3.1 and Property 3.1 result in the following two properties, the first of which is well known, whereas the second one extends the well-known lemma from [11].

Property 3.2. A vector Boolean function is balanced if and only if all nontrivial linear combinations of its component Boolean functions are balanced.

Property 3.3. A vector Boolean function $F(X, Y)$ is statistically independent of X if and only if each nontrivial linear combination of its component Boolean functions is statistically independent of each nontrivial linear function of X.

Note that nontrivial linear functions are all balanced whereas the vector Boolean function from Property 3.3 need not be balanced.

Property 3.1 shows the conditions under which the correlation sums achieve their minimum or maximum values. While the maximum values are achievable for any n_1, n_2, and m, it may be impossible to attain the minimum values if n_2 is smaller than m. For example, a balanced vector Boolean function $F(X, Y)$ cannot be balanced for each X if $n_2 < m$. This is exactly the case which proves to be important for the correlation analysis of combiners with memory. It follows that in this case the correlation sum C_1, which is equal to C_2 because $C_0 = 0$, is necessarily greater than zero. The problem to be considered is to determine the minimum achievable value of C_2 as well as the conditions under which it is obtained.

Lemma 3.2. *Let $F(X, Y)$ be an m-dimensional vector Boolean function of n_1 variables in X and n_2 variables in Y. Let $n_2 = m - k$ where $0 \le k \le m$. Then the correlation sum C_2 is equal to its minimum value $2^k - 1$ if and only if $F(X, Y)$ is an injective function of Y for each X.*

Proof. The correlation sum C_2 is given by (9) in Lemma 3.1. For a nonnegative integer N_{XZ} we have $N_{XZ}^2 \ge N_{XZ}$ where the equality holds if and only if N_{XZ} is equal either to zero or to one. From (9) in view of (5) we then obtain

$$C_2 \ge \frac{1}{2^{n_1+m}} \sum_X \sum_Z \frac{N_{XZ}}{2^{2n_2-2m}} - 1 = 2^k - 1 \tag{10}$$

with equality if and only if, for every X, Z, N_{XZ} is equal either to zero or to one. Equivalently, the equality holds if and only if for each X and every achievable Z there is exactly one value of Y such that $F(X, Y) = Z$. □

4. Correlation Properties of Combiners with Memory

Consider a general binary combiner with M bits of memory and N inputs defined in Section 2. Let, for any positive integer m and every $t \ge m - 1$, $y_t^m = (y_t, \ldots, y_{t-m+1})$

and $X_t^m = (X_t, \ldots, X_{t-m+1})$ denote blocks of m successive output bits and m successive input binary vectors at time t, respectively. From (1) and (2) it follows that

$$y_t^m = \mathcal{F}_m(X_t^m, S_{t-m+1}), \qquad t \geq m-1, \tag{11}$$

where, for each $m \geq 1$, $\mathcal{F}_m$ is a time-independent vector Boolean function $\mathrm{GF}(2)^{mN} \times \mathrm{GF}(2)^M \to \mathrm{GF}(2)^m$ which can be expressed in terms of the output function f and a self-composition of the next-state function F. We use the notation $\mathcal{F}_m(X^m, S)$. Recall that in the assumed probabilistic model the input $\{X_t\}_{t=0}^{\infty}$ is a sequence of balanced and independent vector random variables and the initial state S_0 is a balanced vector random variable independent of the input. The output sequence $\{y_t\}_{t=0}^{\infty}$ is balanced and independent if and only if the function $\mathcal{F}_m$ is balanced for each $m \geq 1$. Sufficient conditions in terms of f and F for this to hold are given in Section 2. On the other hand, as explained in Section 2, if F is balanced, then the state vector S_t is balanced for every $t \geq 0$. Also, X_t^m and S_{t-m+1} are independent for each m and t. Therefore, for each $m \geq 1$ and $t \geq m-1$, the function $\mathcal{F}_m(X_t^m, S_{t-m+1})$ is of the type analyzed in Section 3. By using the correlation properties of vector Boolean functions established in Section 3, we now prove two correlation theorems, the first of which is of the existence type, while the second one determines the total correlation between the output and input sequences of combiners with memory. Note that the special case of combiners without inputs (autonomous finite-state machines) is analyzed in [3].

Theorem 4.1. *Let the next-state function of a binary combiner with M memory bits and N inputs be balanced. Then for any $m \geq 1$, any linear function L_V of m binary variables, and any linear function L_W of Nm binary variables, the correlation coefficient between the linear functions $L_V(y_t^m)$ of at most m successive output bits and $L_W(X_t^m)$ of at most m successive input binary vectors is the same for each $t \geq m-1$. For any $m \geq 1$, if the correlation coefficient is nonzero and L_V is degenerate in the first variable, then L_W must be degenerate in the first N variables. If the output sequence is balanced and independent, then for $m = M+1$ there is a linear function L_V nondegenerate in the first variable and a nontrivial linear function L_W such that the corresponding correlation coefficient is different from zero. In a special case when the output function $f(X, S)$ is balanced for each S, if the correlation coefficient is nonzero and L_V is nondegenerate in the first variable, then L_W must be nondegenerate in at least one of the first N variables.*

Proof. For an arbitrary binary combiner with memory, a succession y_t^m of output bits should be generally considered as a function of all the corresponding inputs X_t^{t+1} and the initial state S_0. It can also be expressed by (11) in terms of the function $\mathcal{F}_m(X_t^m, S_{t-m+1})$ where X_t^m is balanced and independent of S_{t-m+1}. If the next-state function is balanced and S_0 is a balanced random variable independent of all the inputs, then S_t is balanced for every $t \geq 0$ as well. The correlation coefficient between the functions $L_V(y_t^m)$ and $L_W(X_t^m)$ is therefore equal to the time-independent correlation coefficient between the Boolean functions $L_V(\mathcal{F}_m(X^m, S))$ and $L_W(X^m)$, where (X^m, S) is assumed to be balanced. If L_V is degenerate in the first variable whereas L_W is nondegenerate in at least one of the first N variables, then clearly the linear function $L_W(X^m)$ is statistically independent of $L_V(\mathcal{F}_m(X^m, S))$ and hence the correlation coefficient must be equal to zero.

If the output sequence is balanced and independent, then $\mathcal{F}_m(X^m, S)$ is balanced for each $m \geq 1$. However, for $m = M + 1$ it cannot be balanced for each S because the dimension M of S is less than $M + 1$. Therefore $\mathcal{F}_{M+1}(X^{M+1}, S)$ is not statistically independent of X^{M+1}. By virtue of Property 3.3 it then follows that nontrivial linear functions L_V and L_W exist such the corresponding correlation coefficient is different from zero. Furthermore, as proved above, if L_V is degenerate in the first $k - 1$ variables and nondegenerate in the kth one, then L_W must be degenerate in the first $(k - 1)N$ variables. Accordingly, since the correlation coefficient is time-independent, it follows that by discarding the first $k - 1$ variables of L_V and the first $(k - 1)N$ variables of L_W the desired linear functions are obtained. In particular, if the output function $f(X, S)$ is balanced for each S and L_V is nondegenerate in the first variable while L_W is degenerate in the first N variables, then clearly the function $L_V(\mathcal{F}_m(X^m, S))$ is statistically independent of the linear function $L_W(X^m)$ and hence the correlation coefficient must be equal to zero. □

Theorem 4.2. *Let the next-state function of a binary combiner with M memory bits be balanced. Then, for any $m \geq 1$, the sum $C(m)$ of the squares of the correlation coefficients between all nontrivial linear functions of m successive output bits y_t^m and all linear functions of m successive input binary vectors X_t^m is the same for every $t \geq m - 1$ and satisfies*

$$\underline{C}(m) \leq C(m) \leq \overline{C}(m), \qquad m \geq 1, \tag{12}$$

$$\underline{C}(m) = \begin{cases} 0, & 1 \leq m \leq M, \\ 2^{m-M} - 1, & m \geq M + 1, \end{cases} \tag{13}$$

$$\overline{C}(m) = 2^m - 1, \qquad m \geq 1. \tag{14}$$

The minimum value $\underline{C}(m)$ is achieved for all $m \geq 1$ if and only if, for any $t \geq M - 1$, M successive output bits y_t^M are balanced and statistically independent of M successive input binary vectors X_t^M, that is, if and only if $\mathcal{F}_M(X^M, S)$ is a balanced function of S for each X^M. The maximum value $\overline{C}(m)$ is achieved for any $m \geq 1$ if and only if the output function is degenerate in all the state variables.

Proof. For any $m \geq 1$, by the same argument as in the proof of Theorem 4.1, it follows that the considered sum of the correlation coefficients is equal to the time-independent correlation sum C_2 for the m-dimensional vector Boolean function $\mathcal{F}_m(X^m, S)$ with respect to the binary vector variable X^m. From Property 3.1 it then follows that $C(m) \leq 2^m - 1$ for every $m \geq 1$ where for any m the maximum is achieved if and only if $\mathcal{F}_m(X^m, S)$ is degenerate in S, which is clearly true if and only if the output function $f(X, S)$ is degenerate in S.

On the other hand, from Property 3.1 it also follows that $C(m) \geq 0$ for every $1 \leq m \leq M$ where for any such m the minimum is achieved if and only if the function $\mathcal{F}_m(X^m, S)$ is balanced for each X^m. This is satisfied for every $1 \leq m \leq M$ if it is satisfied for $m = M$, because of the following fundamental property of the family of functions $\{\mathcal{F}_m\}_{m \geq 1}$. For any $m' < m$ and any fixed X^m, the function $\mathcal{F}_{m'}(X^{m'}, S)$ is identical to a subfunction of $\mathcal{F}_m(X^m, S)$ for any fixed X^m such that $X^{m'}$ is an appropriate subvector of X^m. Apart

from that, from Lemma 3.2 we directly obtain that $C(m) \geq 2^{m-M} - 1$ for every $m \geq M$ where for any such m the minimum is achieved if and only if $\mathcal{F}_m(X^m, S)$ is an injective function of S for each X^m. This is true for all $m \geq M$ if it is true for $m = M$, because of the fundamental property of the family of functions $\{\mathcal{F}_m\}_{m \geq 1}$ given above. □

Corollary 4.1. *If the output sequence is balanced and independent, then Theorem* 4.2 *holds for the sum of the squares of the correlation coefficients between all nontrivial linear functions of m successive outputs and all nontrivial linear functions of the corresponding m successive inputs. If the output sequence is statistically independent of the input sequences, that is, if the probability distribution of the set of all achievable (at most* 2^M*) output sequences is the same for all the input sequences, then Theorem* 4.2 *holds for the sum of the squares of the correlation coefficients between all nontrivial linear functions of m successive outputs and the constant zero function.*

Proof. If the output sequence is balanced and independent, then for each $m \geq 1$ the function $\mathcal{F}_m$ is balanced and hence, in view of Property 3.1, the correlation sum C_0 is zero so that C_2 reduces to C_1, and the boundary cases are both achievable. If the output sequence is statistically independent of the input sequences, then for each $m \geq 1$ the correlation sum C_1 is zero so that C_2 reduces to C_0, and both the boundary cases are also achievable. Note that the maximum correlation is attained if and only if the output function is constant. □

Theorem 4.2 together with Corollary 4.1 is a generalization of the result from [5] yielding the total correlation for memoryless combiners. Unlike the memoryless combiners, the total correlation for combiners with memory turns out to be dependent on the choice of the output and next-state functions. Its value is between $2^{m-M} - 1$ and $2^m - 1$ and is divided among $(2^m - 1)2^{mN}$ pairs of output and input linear functions, for each $m > M$. In a special case when $M = 1$ and $m = 2$ the total correlation is not smaller than one and is not greater than three and both the bounds are achievable, which completes the analysis from [6]. Accordingly, the maximum absolute value of the correlation coefficients cannot be smaller than $2^{-(mN+M)/2}$ for each $m > M$ which pertains to the uniform distribution. The largest lower bound is obtained for $m = M + 1$, when the minimum correlation sum is one, and is equal to $2^{-(MN+M+N)/2}$. For a memoryless combiner with the same number of inputs this bound is equal to $2^{-N/2}$. The potential advantage of combiners with memory is significant and can be realized if the distribution of the correlation among all possible pairs of linear functions is approximately uniform. In this calculation the fact that some correlations are not possible by Theorem 4.1 is neglected for simplicity. Of course, it is not proved whether approximately uniform distribution of correlations is achievable at all. In any case, it appears that even if the number of inputs N is very small, which may be the case for high-speed stream cipher applications with LFSR input sequences, the security of combiners with memory against the correlation attacks can be considerable if the memory size M is not small.

Another interesting design criterion is the necessary and sufficient condition for the minimum total correlation provided in Theorem 4.2. Whether a nice and general characterization of this condition in terms of the output and next-state functions can be

determined is still an open question. It follows that a necessary condition to be satisfied is that the output function $f(X, S)$ is balanced for each X. Note that by virtue of Property 3.3 it follows that in this case there is no termwise correlation between the output and input sequences. This condition is also sufficient if $M = 1$. In this case the output function must be of the form $f(X, s) = s + g(X)$. If it is also required that the output function be balanced for each s, which is a sufficient condition for the output sequence to be balanced and independent, then the function $g(X)$ should be balanced. This is satisfied for the maximum-order correlation immune combiners with one bit of memory suggested in [8] where $g(X)$ is linear. As for the next-state function for $M = 1$, the only desired property is that it is balanced. In general, for $M > 1$, the choice of a balanced next-state function $F(X, S)$ that is also balanced for each X seems to be appropriate.

5. Linear Sequential Circuit Approximation Method

For cryptographic purposes it is important to determine the correlation coefficient with the largest absolute value, given a binary combiner with memory, and all the corresponding pairs of mutually correlated input and output linear functions. For cryptanalytic purposes it is desirable to find one or more pairs of correlated linear functions with sufficiently large correlation coefficients. A systematic method to achieve both the goals is the exhaustive search over all possible input and output linear functions. Given an output linear function, the correlation coefficients to all the input linear functions can be obtained by using the Walsh transform technique [7], which for a Boolean function of n variables has $O(n2^n)$ computational complexity. If we consider successions of $m = M + 1$ outputs and inputs, then according to Theorem 4.1 we deal with at most 2^M Boolean functions of $MN + N + M$ variables. Hence, the computational complexity of the basic method is $O((MN + N + M)2^{MN+N+2M})$. This is not feasible for relatively large MN, which according to Theorem 4.2 is needed in order to obtain a sufficiently small value of the largest correlation coefficient.

We now describe the so-called linear sequential circuit approximation (LSCA) of binary combiners with memory, which is a feasible procedure that, with high probability, results in pairs of mutually correlated linear functions of at most $M + 1$ successive output bits and at most $M + 1$ successive input binary vectors, respectively, with comparatively large correlation coefficients. The LSCA method consists in determining and solving a linear sequential circuit (LSC) that approximates a binary combiner with memory. The LSC has additional nonbalanced inputs and is based on linear approximations of the output function and of all the component next-state functions, where a linear approximation of a Boolean function is any linear function to which the Boolean function is correlated. The method generally applies to arbitrary binary combiners with memory without any restrictions regarding the output and next-state functions.

First, find a linear approximation of the output function f and of each of the component functions of the next-state function F. This is equivalent to expressing each of these $M + 1$ functions as a sum of a linear function and a nonbalanced function. If the function being decomposed is already nonbalanced, then the constant zero linear function may be chosen. If the function being decomposed is statistically independent of a subset of variables, then every linear approximation must necessarily involve at least one of

the variables out of this subset, see Property 3.3. So, the basic requirement is that the corresponding correlation coefficients are different from zero. It will be shown that it is also desirable to choose linear approximations with the correlation coefficients whose absolute values are close to maximum. Of course, one can determine by the Walsh transform technique the correlation coefficients to all the linear functions for each of the considered $M + 1$ Boolean functions of $M + N$ variables, which in general requires $O((M + 1)(M + N)2^{M+N})$ computational complexity. Even if M is large, in practical realizations both the output and all the component next-state functions must themselves effectively depend on relatively small numbers of variables or can be expressed in terms of such Boolean functions. In both cases the Walsh transform technique is feasible, although in the latter one it may lead to approximate solutions.

Second, given the linear approximations, put the basic equations (1) and (2) for a combiner with memory into the matrix form

$$S_{t+1} = \mathbf{A}S_t + \mathbf{B}X_t + \Delta(X_t, S_t), \qquad t \geq 0, \tag{15}$$

$$y_t = \mathbf{C}S_t + \mathbf{D}X_t + \varepsilon(X_t, S_t), \qquad t \geq 0, \tag{16}$$

where the vectors are regarded as one-column matrices, $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$, and $\mathbf{D}$ are binary matrices, and ε and each component of $\Delta = (\delta_1, \ldots, \delta_M)$ are nonbalanced Boolean functions, called the noise functions. The main idea now is to regard $\{\varepsilon(X_t, S_t)\}_{t=0}^{\infty}$ and $\{\delta_i(X_t, S_t)\}_{t=0}^{\infty}$, $1 \leq i \leq M$, as the input sequences so that (15) and (16) define a nonautonomous linear finite-state machine or LSC, called the LSCA of a combiner with memory. Then solve this LSC by using the generating function (D-transform) technique, see [1], for example. Precisely, let $\mathbf{S}$, $\mathbf{X}$, $\mathbf{\Delta}$, ε, and $\mathbf{y}$ denote the generating functions in variable z of the sequences $\{S_t\}$, $\{X_t\}$, $\{\Delta(X_t, S_t)\}$, $\{\varepsilon(X_t, S_t)\}$, and $\{y_t\}$, respectively. Then (15) and (16) result in

$$\mathbf{S} = z\mathbf{A}\mathbf{S} + z\mathbf{B}\mathbf{X} + z\mathbf{\Delta} + S_0, \tag{17}$$

$$\mathbf{y} = \mathbf{C}\mathbf{S} + \mathbf{D}\mathbf{X} + \varepsilon. \tag{18}$$

The solution to (17) and (18) is clearly

$$\mathbf{y} = \left(\mathbf{D} - \frac{\mathbf{C}\,\mathrm{adj}(z\mathbf{A} - \mathbf{I})\,\mathbf{B}}{\det(z\mathbf{A} - \mathbf{I})}\right)\mathbf{X} - \frac{\mathbf{C}\,\mathrm{adj}(z\mathbf{A} - \mathbf{I})}{\det(z\mathbf{A} - \mathbf{I})}(z\mathbf{\Delta} + S_0) + \varepsilon, \tag{19}$$

where $\mathbf{I}$ is the identity matrix, $\det(z\mathbf{A} - \mathbf{I}) \stackrel{\text{def}}{=} \varphi(z)$, $\varphi(0) = 1$, is the reciprocal of the characteristic polynomial of the state-transition matrix $\mathbf{A}$ of degree at most $\operatorname{rank} \mathbf{A} \leq M$, and the elements of the matrix $\mathrm{adj}(z\mathbf{A} - \mathbf{I})$ are polynomials in z of degree at most $M - 1$. The computational complexity of obtaining (19) is $O(M^3(N + 1))$. Accordingly, (19) can be put into the form

$$\mathbf{y} = \frac{1}{\varphi(z)} \sum_{i=1}^{N} g_i(z)\mathbf{x}_i + \frac{1}{\varphi(z)} \sum_{j=1}^{M} h_j(z)(z\boldsymbol{\delta}_j + s_{j0}) + \boldsymbol{\varepsilon}, \tag{20}$$

where $\mathbf{x}_i$ and $\boldsymbol{\delta}_j$ denote the generating functions of $\{x_{it}\}$ and $\{\delta_j(X_t, S_t)\}$, and the degrees of the polynomials $g_i(z)$ and $h_j(z)$ are at most M and $M - 1$, $1 \leq i \leq N$, $1 \leq j \leq M$,

respectively. Letting $\varphi(z) = \sum_{k=0}^{M} \varphi_k z^k$, $g_i(z) = \sum_{k=0}^{M} g_{ik} z^k$, and $h_j(z) = \sum_{k=0}^{M-1} h_{jk} z^k$, (20) in the time domain reduces to

$$\sum_{k=0}^{M} \varphi_k \, y_{t-k} = \sum_{i=1}^{N} \sum_{k=0}^{M} g_{ik} \, x_{i,t-k} + e(X_t^{M+1}, S_{t-M}), \qquad t \geq M, \tag{21}$$

$$e(X_t^{M+1}, S_{t-M}) = \sum_{j=1}^{M} \sum_{k=0}^{M-1} h_{jk} \, \delta_j(X_{t-1-k}, S_{t-1-k}) + \sum_{k=0}^{M} \varphi_k \, \varepsilon(X_{t-k}, S_{t-k}), \qquad t \geq M, \tag{22}$$

where it is assumed that the state vector S_{t-k} is a function of $(X_{t-k-1}^{M-k}, S_{t-M})$ for each $0 \leq k \leq M-1$. Interestingly enough, (21) is of the type dealt with in Theorem 4.1. The output and input linear functions in (21) are correlated if and only if the noise function e is nonbalanced. The correlation coefficient is time-independent if the next-state function is balanced. If this is not satisfied, then the correlation coefficient may be time-dependent because S_t need not be a balanced function for every $t \geq 0$ any more. The noise function e in (22) is defined as a sum of individual noise functions that are nonbalanced provided that the next-state function is balanced. Since the individual noise functions need not be independent, it is in principle not impossible that the correlation coefficient of e to the constant zero function is equal to zero or is close to zero. However, it is intuitively clear that this situation is highly unlikely. This is justified by the following probabilistic argument which can be proved by some combinatorial and asymptotic analysis, see [2].

Lemma 5.1. *Consider m Boolean functions of the same n variables with the correlation coefficients c_i to the constant zero function, $1 \leq i \leq m$. If the functions are chosen uniformly and independently at random, then for large 2^n the probability distribution of the correlation coefficient of their sum is asymptotically normal with the expected value $\prod_{i=1}^{m} c_i$ and the variance $O(m/2^n)$.*

In our case the individual noise functions can be regarded as Boolean functions of $n = MN + N + M$ variables in (X_t^{M+1}, S_{t-M}). Consequently, except in some special cases, it may generally be expected with high probability that the overall correlation coefficient is very close to the product of the individual ones and hence different from zero as well. Accordingly, not only does the LSCA method with high probability yield the mutually correlated input and output linear functions, but it also enables estimation of the value of the corresponding correlation coefficient by using the independence or other appropriate probabilistic assumptions. Since ideally we would like to obtain the LSCAs with the correlation coefficients whose absolute values are close to maximum, the individual correlation coefficients should be large in magnitude and the number of noise terms in (22) should be small. Of course, these requirements might be contradictory. Therefore, a good approach is to repeat the LSCA procedure several times, starting from the best linear approximations of the output and component next-state functions. The procedure may also be performed for all possible linear approximations, which seems to be the only systematic way to check all the correlations that might result from the LSCA method. In general, there are at most $(M+1)2^{M+N}$ such linear approximations. However, it is in principle always feasible to examine all possible linear approximations

even if M is large, because in practical realizations the output and the component next-state functions depend on relatively small numbers of variables or are composed of such Boolean functions. It is not difficult to see that the LSCA method can be generalized to deal with the linear approximations of the linear combinations of the component next-state functions as long as the set of the linear combinations is invertible [3]. This means that the best or good linear approximations of such linear combinations could also be checked. For practical combiners with memory this is feasible, but increases the computational complexity.

The output linear function determined by the characteristic polynomial of the state-transition matrix of the corresponding LSC involves at most $M + 1$ successive output bits. Sometimes, it may happen that all the polynomials from (20) contain a common factor. It can be removed, which results in output and input linear functions of necessarily less than $M + 1$ successive outputs and inputs, respectively. Note that the magnitude of the correlation coefficient may thus increase or decrease. On the other hand, all the polynomials from (20) can also be multiplied by an appropriate polynomial and correlated output and input linear functions of more than $M + 1$ successive outputs and inputs, respectively, are thus obtained with a possibly increased correlation coefficient because the number of noise terms may decrease.

The LSCA method works for arbitrary binary combiners with memory, and the output and input linear functions obtained are determined by the matrices $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$, and $\mathbf{D}$ of the corresponding LSC. In the light of Property 3.3, we now examine how the choice of the output and component next-state functions affects these matrices. If the output function $f(X, S)$ is balanced for each S, then $\mathbf{D}$ must be nonzero so that at least one of the coefficients g_{i0}, $1 \leq i \leq N$, is nonzero, which is in accordance with Theorem 4.1. If and only if the output function is not balanced for at least one value of X, then at least one linear approximation exists such that $\mathbf{C}$ is zero, which is the memoryless case. Similar arguments hold for the component next-state functions and rows of the matrices $\mathbf{A}$ and $\mathbf{B}$. Accordingly, if the output function and all the component next-state functions are balanced for each X and S, respectively, then $\mathbf{C}$, $\mathbf{D}$, each row of $\mathbf{A}$, and each row of $\mathbf{B}$ are all nonzero. This may lead to a large number of noise terms in (22), which is desirable for cryptographic purposes. Apart from that, it appears that for immunity against the described LSCA attack on combiners with memory, it is generally good if the memory size is large and if the output function and all the component next-state functions or their nontrivial linear combinations have large distance from affine functions and effectively depend on relatively large sets of variables.

6. Correlation Attack

Consider a binary combiner with M memory bits and N input sequences produced by linear feedback shift registers. Let $\psi_i(z)$ denote the feedback polynomial, possibly irreducible or primitive, of the input sequence $\{x_{it}\}$, $1 \leq i \leq N$. Assume that the secret key controls only the initial contents of the shift registers and possibly the intitial memory state as well. Given a segment of the keystream sequence, the objective is to reconstruct the shift register initial contents based on the correlation between the keystream sequence and the shift register sequences which, according to the correlation

properties of combiners with memory established in Section 4, necessarily exists if the keystream sequence is balanced and independent. A pair of mutually correlated output and input linear functions can be found either by exhaustive search if MN is not large or by the linear sequential circuit approximation method described in Section 5. The correlation coefficient can be computed exactly if MN is not large or determined approximately by using the LSCA method. Another possibility is to obtain an empirical estimate from the keystream sequence of the given length. In any case, the basis of the correlation attack is a correlation equation of the form (21) in the time domain or (20) in the generating functions domain. In principle, the attack can be performed only on the LFSR sequences that appear in (21), that is, for which the polynomial $g_i(z)$ is nonzero. More precisely, the initial state reconstruction is possible only for those LFSR sequences for which the polynomials $\psi_i(z)$ and $g_i(z)$ are relatively prime. Otherwise, the common factors cancel and the complete reconstruction is not possible. In the degenerate case when $\psi_i(z)$ is a factor of $g_i(z)$ the ith LFSR sequence effectively disappears from (21). On the other hand, if the feedback polynomials are not pairwise coprime, then the full initial state reconstruction is not possible, which is natural because in this case equivalent secret keys may exist. Assume for simplicity that the feedback polynomials are pairwise coprime. Then the complete reconstruction of all the corresponding LFSR sequences is possible provided that the observed segment of the keystream sequence is sufficiently long. The minimum necessary length for the successful reconstruction is proportional to the sum of the involved shift register lengths and inversely proportional to the square of the correlation coefficient. With the blind search over all possible initial states, the divide-and-conquer effect is achieved only if the number of the involved LFSR sequences is less than N. However, the fast correlation attacks [4] based on iterative probabilistic decoding algorithms may also be performed if the correlation coefficient is sufficiently large. If the combiner is maximum-order correlation immune, then the number of LFSR sequences in (21) for which $g_i(z)$ is nonzero is always N, provided that the correlation coefficient is nonzero. Note that even in this case the basic divide-and-conquer effect is possible if $\psi_i(z)$ divides $g_i(z)$ for some i. It is an interesting theoretical problem to derive the conditions under which any particular input LFSR sequence does not effectively appear in any nontrivial input linear function that is correlated to the output. This would mean that the corresponding LFSR is resistant against the correlation attack. For memoryless combiners, this is possible if and only if the output function is degenerate in the input variable considered. Unlike memoryless combiners, in a combiner with memory, multiple linear correlations between the keystream sequence and the same subset of the input LFSR sequences may exist. When exploited, they increase the strength of the correlation attack on the same keystream sequence. Also, correlation conditioned on the output [6] is another possibility to be investigated in more detail for a general combiner with memory.

We proceed by showing that every LFSR-based combiner with or without memory is essentially zero-order correlation immune. This is not very surprising because the notion of correlation immunity [8] is defined for balanced and independent input sequences. It is clear that every such combiner with N inputs can be regarded as a combiner with an arbitrarily chosen single input and enlarged memory that encompasses all the other input LFSRs. The correlation theorems from Section 4 which show that each input sequence is correlated to the output one can then be applied. Of course, it is in principle possible that every polynomial specifying the input linear function correlated to the output contains the

considered LFSR feedback polynomial as a factor. The LSCA attack on the single input combiner can be performed as follows. First find the LSCA of the original combiner with N inputs, that is, the correlation equations (20) and (21). Pick any input that effectively appears in (21). Then multiply all the polynomials in (20) by the least common multiple of the feedback polynomials of the other inputs that also effectively appear in (21). This will clearly cause all these inputs to disappear from the corresponding (21), and the new noise function will with high probability remain nonbalanced. The initial state reconstruction of the chosen LFSR is then possible if its feedback polynomial is relatively prime to all the others. Furthermore, proceeding in the same manner all the polynomials in (20) can be multiplied by the product of the feedback polynomials of all the inputs that effectively appear in (21) which then yields a nonbalanced linear function of the successive output bits.

7. Conclusion

Correlation properties of a general binary combiner with an arbitrary number M of memory bits are analyzed, novel design criteria are established, and a so-called LSCA correlation attack on keystream generators is developed. Sufficient conditions for the output sequence to be balanced and independent are first pointed out. Fundamental correlation properties of vector Boolean functions are then derived and used for the correlation analysis of combiners with memory. It is proved that a pair of certain mutually correlated linear functions of at most $M + 1$ successive outputs and inputs, respectively, exists. The correlation coefficient turns out to be time-independent if the next-state function is balanced. Moreover, for any positive integer m, the sum of the squares of the correlation coefficients between all nonzero linear functions of m successive output bits and all linear functions of the corresponding m successive inputs is shown to be dependent upon the output and next-state functions, unlike the memoryless combiners. It is proved that the minimum value of this sum is achieved for all m if and only if any M successive output bits are balanced and statistically independent of the corresponding M successive inputs, which is a new design criterion. A necessary condition for this to hold is that the output function is balanced for each memory state. The minimum correlation sum is equal to zero for $m \leq M$ and to $2^{m-M} - 1$ for $m > M$. It is also proved that the maximum value of the correlation sum is equal to $2^m - 1$ and is achieved for any m if and only if the output function is degenerate in all the state variables, which is essentially the memoryless case. The results show a significant impact of the memory size upon the security of combiners with memory. As a consequence, it follows that for high-speed stream cipher applications any large memory size realizable by look-up tables is appropriate. An open problem is to examine the conditions under which uniform or approximately uniform distribution of the correlation among all possible pairs of output and input linear functions is achievable. Another interesting problem is to investigate whether similar results can be obtained for the correlation conditioned on the output [6].

When M is not large, all the mutually correlated output and input linear functions along with the corresponding correlation coefficients can be found by exhaustive search and the Walsh transform technique. An efficient LSCA method is developed for obtaining output and input linear functions with comparatively large correlation coefficients which

is feasible for large M and, in fact, works for any practical scheme. The method consists in deriving and solving a linear sequential circuit, with additional nonbalanced inputs, that is based on linear approximations of the output and the component next-state functions. Regarding the immunity against the LSCA attack on combiners with memory, it follows that apart from relatively large memory size it is generally good that the output function and all the component next-state functions or their nontrivial linear combinations have a large distance from affine functions and effectively depend on relatively large sets of variables. It also appears desirable that all these functions be balanced for each value of the memory state and each value of the input, respectively. Whether there are other efficient procedures like the LSCA one remains an open question.

The corresponding correlation attack on combiners with linear feedback shift registers is analyzed and it is shown that every such combiner with or without memory is essentially zero-order correlation immune. Since the LSCA method is in principle applicable to arbitrary finite-state machines, it is an interesting research problem to investigate how it works on arbitrary keystream generators, for example, based on clock-controlled shift registers, see [2] and [3].

References

[1] A. Gill, *Linear Sequential Circuits*, McGraw-Hill, New York, 1966.

[2] J. Dj. Golić, Intrinsic statistical weakness of keystream generators, *Advances in Cryptology—Asiacrypt* '94, Lecture Notes in Computer Science, vol. 917, J. Pieprzyk and R. Safavi-Naimi, eds., Springer-Verlag, Berlin, 1995, pp. 91–103.

[3] J. Dj. Golić, Linear models for keystream generators, *IEEE Trans. Comput.*, to appear.

[4] W. Meier and O. Staffelbach, Fast correlation attacks on certain stream ciphers, *J. Cryptology*, 1(3):159–176, 1989.

[5] W. Meier and O. Staffelbach, Nonlinearity criteria for cryptographic functions, *Advances in Cryptology—Eurocrypt* '89, Lecture Notes in Computer Science, vol. 434, J.-J. Quisquater and J. Vandewalle, eds., Springer-Verlag, Berlin, 1990, pp. 549–562.

[6] W. Meier and O. Staffelbach, Correlation properties of combiners with memory in stream ciphers, *J. Cryptology*, 5(1):67–86, 1992.

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

[8] R. A. Rueppel, Correlation immunity and the summation generator, *Advances in Cryptology—Crypto* '85, Lecture Notes in Computer Science, vol. 218, H. C. Williams, ed., Springer-Verlag, Berlin, 1986, pp. 260–272.

[9] T. Siegenthaler, Correlation immunity of nonlinear combining functions for cryptographic applications, *IEEE Trans. Inform. Theory*, 30:776–780, September 1984.

[10] T. Siegenthaler, Decrypting a class of stream ciphers using ciphertext only, *IEEE Trans. Comput.*, 34:81–85, January 1985.

[11] G. Z. Xiao and J. L. Massey, A spectral characterization of correlation-immune combining functions, *IEEE Trans. Inform. Theory*, 34:569–571, May 1988.