Cryptographic Significance of the Carry for Ciphers Based on Integer Addition

Othmar Staffelbach [1)] Willi Meier [2)]

[1)] GRETAG, Althardstrasse 70
CH-8105 Regensdorf, Switzerland

[2)] HTL Brugg-Windisch
CH-5200 Windisch, Switzerland

Abstract

Integer addition has been proposed for use in cryptographic transformations since this operation is nonlinear when considered over GF(2). In these applications nonlinearity or confusion is achieved via the carry. If the carry happens to be biased, there result correlations to linear functions which can be cryptanalytically exploited.

The aim of the present paper is to investigate the probability distribution of the carry for integer addition with an arbitrary number n of inputs. It is shown that asymptotically the carry is balanced for even n and biased for odd n. As a result, for $n = 3$ the carry is strongly biased, whereas for increasing n it is shown that the bias tends to 0.

1 Introduction

Several cryptographic transformations are known which use integer addition as a primitive. In [5,6] the summation principle has been formulated in order to generate cryptographically strong binary sequences out of given (cryptographically weak) sequences. In another direction we mention that knapsack type ciphers are also based on integer addition.

In these ciphers nonlinearity or confusion is achieved via the carry. In fact if the carry happens to be zero, integer addition is linear when considered over $GF(2)$, or there result correlations to linear functions if the carry is biased. Therefore the strength of these ciphers heavily relies on the randomness of the carry. In particular it is required that the least significant bit (l.s.b.) of the carry is balanced or nearly balanced. However it may happen that this postulate is satisfied in the average, but is violated locally. In fact for the summation combiner with $n = 2$ inputs it has been

A.J. Menezes and S.A. Vanstone (Eds.): Advances in Cryptology - CRYPTO '90, LNCS 537, pp. 601-614, 1991.

semi-infinite sequence. The digit z_j is recursively computed by

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

$$\sigma_j = f_1(a_j, b_j, \sigma_{j-1}) = a_j b_j + a_j \sigma_{j-1} + b_j \sigma_{j-1} \tag{2}$$

where in (1) σ_{j-1} denotes the carry bit, and $\sigma_{-1} = 0$.

Suppose that the input to the adder, i.e. the integers a and b, are uniformly distributed. In statistical terms this means that the corresponding input sequences $\mathcal{A}$ and $\mathcal{B}$ are considered as *independent and uniformly distributed* sequences of random variables. Then, as is shown in [4], the probability distribution of the carry bit σ_j converges exponentially to the uniform distribution. Moreover, if the initial carry σ_{-1} is assumed to be uniformly distributed this is also the case for all successive carries σ_j distributed as well. With regard to *correlation immunity*, knowledge of the output z_j does not give any information about the inputs a_j, b_j or the sum $a_j + b_j$. However it is shown in [4] that this is no longer true when z_j is observed in a run of consecutive equal output digits, as in this case the carry bit is expected to be biased.

To recall some results proved in [4], let $q_j(0)$ and $q_j(1)$ denote the probability that the carry bit σ_j is in state 0, or state 1, respectively. According to [4], the probability distributions $\mathbf{q}_j = (q_j(0), q_j(1))$ and $\mathbf{q}_{j-1} = (q_{j-1}(0), q_{j-1}(1))$ are related by

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

However if z_j is known to be 0, the relation between the conditional probabilities $\mathbf{q}_j$ and $\mathbf{q}_{j-1}$ is given by

$$\begin{pmatrix} q_j(0) \\ q_j(1) \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & 0 \\ \frac{1}{2} & 1 \end{pmatrix} \begin{pmatrix} q_{j-1}(0) \\ q_{j-1}(1) \end{pmatrix} \tag{4}$$

Now 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

$$A^s = \begin{pmatrix} \frac{1}{2} & 0 \\ \frac{1}{2} & 1 \end{pmatrix}^s = \begin{pmatrix} \frac{1}{2^s} & 0 \\ 1 - \frac{1}{2^s} & 1 \end{pmatrix} \tag{5}$$

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

$$\mathbf{q}_{j+s}(0) \leq \frac{1}{2^s} \quad \text{and} \quad \mathbf{q}_{j+s}(1) \geq 1 - \frac{1}{2^s} \tag{6}$$

Therefore the carry prefers to be 1 in a run of consecutive 0's, similarly it prefers to be 0 in a run of consecutive 1's. Hence, there result strong correlations between a single output digit z_j and the sum $a_j + b_j$.

2.2 Integer Addition with Three Inputs

Consider the addition of 3 integers $a = a_{m-1}2^{m-1} + \cdots + a_1 2 + a_0$, $b = b_{m-1}2^{m-1} + \cdots + b_1 2 + b_0$ and $c = c_{m-1}2^{m-1} + \cdots + c_1 2 + c_0$. Denote by $\mathcal{A} = (a_0, a_1, a_2, \ldots)$, $\mathcal{B} = (b_0, b_1, b_2, \ldots)$ and $\mathcal{C} = (c_0, c_1, c_2, \ldots)$ the corresponding binary input sequences. Then the integer sum $z = a + b + c$ defines the first m digits of the output sequence $\mathcal{Z} = (z_0, z_1, z_2, \ldots)$. Denote by $I_j = a_j + b_j + c_j$ the integer sum of the inputs a_j,b_j and c_j. For independent and uniformly distributed input sequences, I_j can take the values 0,1,2 or 3 with the following probabilities

I_j	0	1	2	3
p	0.125	0.375	0.375	0.125

(7)

The value of the carry σ_j can be 0, 1 or 2, and is given as a function of σ_{j-1} and I_j as shown in Table 1, where the entries for σ_j in the frames indicate that the corresponding output z_j is 0.

	I_j			
σ_{j-1}	0	1	2	3
0	$\boxed{0}$	0	$\boxed{1}$	1
1	0	$\boxed{1}$	1	$\boxed{2}$
2	$\boxed{1}$	1	$\boxed{2}$	2

Table 1: σ_j as function of σ_{j-1} and I_j

For $j = 0, 1, 2, \ldots$ denote by $q_j(0)$, $q_j(1)$ and $q_j(2)$ the probability that the carry σ_j is in state 0, 1 or 2. From Table 1 and (7) we conclude that the probability vectors $\mathbf{q}_j = (q_j(0), q_j(1), q_j(2))$ and $\mathbf{q}_{j-1} = (q_{j-1}(0), q_{j-1}(1), q_{j-1}(2))$ are related by

$$\begin{pmatrix} q_j(0) \\ q_j(1) \\ q_j(2) \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{1}{8} & 0 \\ \frac{1}{2} & \frac{3}{4} & \frac{1}{2} \\ 0 & \frac{1}{8} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} q_{j-1}(0) \\ q_{j-1}(1) \\ q_{j-1}(2) \end{pmatrix} \tag{8}$$

Therefore $\mathbf{q}_j = A^j \mathbf{q}_0$, where A denotes the transition matrix in (8). This equation describes the propagation of the probability distribution of the carry from a given initial distribution. In this context it is of interest to know how $\mathbf{q}_j$ behaves asymptotically and whether $\lim_{j\to\infty} \mathbf{q}_j$ does exist. To settle this question we observe that the transition matrix A is *diagonalizable*, i.e. it can be written in the form $A = S^{-1}DS$,

where D is a diagonal matrix, namely

$$A = \begin{pmatrix} \frac{1}{2} & \frac{1}{8} & 0 \\ \frac{1}{2} & \frac{3}{4} & \frac{1}{2} \\ 0 & \frac{1}{8} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{1}{6} & 1 & -\frac{1}{2} \\ \frac{2}{3} & 0 & 1 \\ \frac{1}{6} & -1 & -\frac{1}{2} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & 0 \\ 0 & 0 & \frac{1}{4} \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ \frac{1}{2} & 0 & -\frac{1}{2} \\ -\frac{2}{3} & \frac{1}{3} & -\frac{2}{3} \end{pmatrix} \tag{9}$$

Then we have $\mathbf{q}_j = A^j \mathbf{q}_0 = S^{-1} D^j S \mathbf{q}_0$. As the diagonal entries of D are 1, 1/2, 1/4, we arrive at

$$\lim_{j\to\infty} \mathbf{q}_j = \lim_{j\to\infty} A^j \mathbf{q}_0 = S^{-1} \lim_{j\to\infty} D^j S \mathbf{q}_0 = \left(\frac{1}{6}, \frac{2}{3}, \frac{1}{6}\right) \tag{10}$$

Observe that the diagonal entries of D are the eigenvalues of A, and that the limit in (10) is the (normalized) eigenvector to the eigenvalue 1.

Formula (10) implies that (asymptotically) the carry is 0, 1 or 2 with probability 1/6, 2/3 or 1/6, respectively. Therefore the least significant bit of the carry is strongly biased. As a consequence, in the average the output z_j is correlated to $a_j + b_j + c_j + 1$ with probability 2/3. This result contrasts to the addition with 2 inputs, where the carry is balanced in the average.

Our analysis shows that the summation combiner with 3 inputs still has unpleasant properties with respect to correlation. Therefore we are lead to investigate whether the situation improves as n increases.

3 Integer Addition with n Inputs

3.1 The Transition Matrix

Consider n integers $x_1, x_2, \ldots, x_n$, and denote by $\mathcal{X}_k = (x_{k0}, x_{k1}, x_{k2}, \ldots)$, $1 \le k \le n$, the corresponding binary sequences, i.e. $x_k = x_{k,m-1}2^{m-1} + \cdots + x_{k1}2 + x_{k0}$. Then the integer sum $z = x_1 + \cdots + x_n$ defines the first m digits of the output sequence $\mathcal{Z} = (z_0, z_1, z_2, \ldots)$. Denote by $I_j = x_{1j} + \cdots + x_{nj}$ the integer sum of the j–th input digits. Again the $\mathcal{X}_k$'s are assumed to be independent and uniformly distributed sequences of random variables. Then I_j can take the values i, $0 \le i \le n$, with probability

$$P(I_j = i) = \binom{n}{i} \frac{1}{2^n} \tag{11}$$

The values of the output z_j and the carry σ_j are given as a function of the input I_j and the previous carry σ_{j-1}:

$$z_j = f_0(I_j, \sigma_{j-1}) \tag{12}$$

$$\sigma_j = f_1(I_j, \sigma_{j-1}) \tag{13}$$

The carry σ_j can take the values 0, 1, ..., n-1, and is computed according to Table 2, where the entry for σ_j in the frames indicate that the corresponding output z_j is 0.

	I_j								
σ_{j-1}	0	1	2	3	4	5	$\cdots$	$n-1$	n
0	$\boxed{0}$	0	$\boxed{1}$	1	$\boxed{2}$	2	.		
1	0	$\boxed{1}$	1	$\boxed{2}$	2	.			
2	$\boxed{1}$	1	$\boxed{2}$	2	.				
3	1	$\boxed{2}$	2	.					
4	$\boxed{2}$	2	.						
5	2	.							
.	.							.	.
$n-2$							.	$n-2$	$n-2$
$n-1$						.	$n-2$	$\boxed{n-1}$	$\boxed{n-1}$
						.	$n-2$	$\boxed{n-1}$	$n-1$

Table 2: σ_j as function of σ_{j-1} and I_j

For $j = 0, 1, 2, \ldots$, and $0 \le s \le n-1$ denote by $q_j(s)$ the probability that the carry σ_j is in state s, and let $\mathbf{q}_j = (q_j(0), \ldots, q_j(n-1))$. The vectors $\mathbf{q}_j$ and $\mathbf{q}_{j-1}$ are related by the formula

$$q_j(s) = \sum_{\substack{i,t \\ f_1(i,t)=s}} P(I_j = i)\, q_{j-1}(t) \tag{14}$$

Thus we have the linear relation $\mathbf{q}_j = A\mathbf{q}_{j-1}$ where the $n \times n$ transition matrix A, according to Table 2 and formula (11), is computed as follows.

$$A = \frac{1}{2^n} \begin{pmatrix} \binom{n}{1}+\binom{n}{0} & \binom{n}{0} & 0 & 0 & \cdots & 0 \\ \binom{n}{3}+\binom{n}{2} & \binom{n}{2}+\binom{n}{1} & \binom{n}{1}+\binom{n}{0} & \binom{n}{0} & \cdots & 0 \\ \binom{n}{5}+\binom{n}{4} & \binom{n}{4}+\binom{n}{3} & \binom{n}{3}+\binom{n}{2} & \binom{n}{2}+\binom{n}{1} & \cdots & 0 \\ & & \vdots & & & \\ 0 & & \cdots & 0 & \binom{n}{0} & \binom{n}{0}+\binom{n}{1} \end{pmatrix} \tag{15}$$

The entry a_{st} of the matrix A is expressed as

$$a_{st} = \frac{1}{2^n}\left(\binom{n}{2s-t} + \binom{n}{2s-t-1}\right) = \frac{1}{2^n}\binom{n+1}{2s-t} \tag{16}$$

whereby (16) also holds for $2s - t < 0$ or $2s - t > n + 1$, in which case the binomial coefficients are defined to be 0. Therefore the matrix A can be written in the form

$$A = \frac{1}{2^n} \begin{pmatrix} \binom{n+1}{1} & \binom{n+1}{0} & 0 & 0 & 0 & \cdots & 0 \\ \binom{n+1}{3} & \binom{n+1}{2} & \binom{n+1}{1} & \binom{n+1}{0} & 0 & \cdots & 0 \\ \binom{n+1}{5} & \binom{n+1}{4} & \binom{n+1}{3} & \binom{n+1}{2} & \binom{n+1}{1} & \cdots & 0 \\ & & & \vdots & & & \\ 0 & & \cdots & & 0 & \binom{n+1}{0} & \binom{n+1}{1} \end{pmatrix} \tag{17}$$

3.2 Eigenvectors and Eigenvalues of the Transition Matrix

In Section 2.2 the evolution of the probability distribution of the carry is obtained by considering the diagonalization of the transition matrix. In order to find a representation of the matrix A in diagonal form, $A = S^{-1}DS$, one has to find the eigenvalues and the eigenvectors of A. Recall that the eigenvalues of A coincide with the diagonal entries of D, and the columns of the matrix S^{-1} are the corresponding eigenvectors.

Observe that the diagonalization of (9) for $n = 3$ is based on the fact that the eigenvalues of the transition matrix are all distinct. Moreover a unique asymptotic probability distribution (see (10)) of the carry exists as a consequence of the fact that, apart from the eigenvalue 1, all other other eigenvalues have absolute value strictly smaller than 1. Our aim is to generalize both of these facts to the transition matrix in (17) for arbitrary n.

First observe that A is a stochastic matrix, i.e. its satisfies $\sum_{s=1}^{n} a_{st} = 1$. Thus for any vector $\mathbf{x} = (x_1, \ldots, x_n)$ the sum $\sum_s x_s$ is preserved by A, i.e. if $\mathbf{x}' = A\mathbf{x}$ then $\sum_s x'_s = \sum_s x_s$. Suppose that $\mathbf{x}$ is an eigenvector of A to the eigenvalue λ, i.e. $\mathbf{x}' = A\mathbf{x} = \lambda\mathbf{x}$. Then $\sum_s x'_s = \lambda \sum_s x_s = \sum_s x_s$ implies either $\lambda = 1$ or $\sum_s x_s = 0$. Hence all eigenvectors to eigenvalues $\lambda \neq 1$ satisfy $\sum_s x_s = 0$.

The matrix A has an additional symmetry—it is compatible with the the transformation M defined by $M(x_1, \ldots, x_n) = (x_n, \ldots, x_1)$. This means that $MA\mathbf{x} = AM\mathbf{x}$ holds for all $\mathbf{x}$. If $\mathbf{x}$ is an eigenvector, $M\mathbf{x}$ is also an eigenvector to the same eigenvalue λ. For eigenvectors $\mathbf{x}$ with multiplicity 1 this implies that

$$M\mathbf{x} = \mathbf{x} \quad \text{or} \quad M\mathbf{x} = -\mathbf{x}, \tag{18}$$

i.e. the eigenvector is either symmetric or antisymmetric.

Theorem 3.1 *The matrix $A = A(n)$ as given by (17) has n different eigenvalues*

$$\lambda_k = 2^{-k}, \quad 0 \leq k \leq n - 1 \tag{19}$$

and the corresponding eigenvectors $\mathbf{x}_k$ *satisfy*

$$M\mathbf{x}_k = (-1)^k \mathbf{x}_k \tag{20}$$

Moreover the components of the eigenvector $\mathbf{x} = \mathbf{x}_0$ *to the eigenvalue* $\lambda_0 = 1$ *satisfy* $x_s > 0$ *for all* s.

Proof. For $n = 1$ the claim of the theorem is trivial, and for $n > 1$ we proceed by induction on n. Denote by A the matrix in dimension n, and by A' the matrix in dimension $n-1$. According to (16) A and A' are computed as

$$a_{st} = \frac{1}{2^n}\binom{n+1}{2s-t} \quad \text{and} \quad a'_{st} = \frac{1}{2^{n-1}}\binom{n}{2s-t} \tag{21}$$

In the following computations it makes sense to consider a_{st}, as defined in (21), also for values $s < 1$ or $s > n$, and similarly a'_{st} for $s < 1$ or $s > n-1$. To establish a relationship between A and A' consider, for $1 \le t \le n-1$,

$$\begin{aligned}
a_{st} - a_{s,t+1} &= \frac{1}{2^n}\left(\binom{n+1}{2s-t} - \binom{n+1}{2s-t-1}\right) \\
&= \frac{1}{2^n}\left(\binom{n}{2s-t} + \binom{n}{2s-t-1} - \binom{n}{2s-t-1} - \binom{n}{2s-t-2}\right) \\
&= \frac{1}{2^n}\left(\binom{n}{2s-t} - \binom{n}{2s-t-2}\right) \\
&= \frac{1}{2}a'_{st} - \frac{1}{2}a'_{s-1,t}
\end{aligned} \tag{22}$$

Since for $1 \le t \le n-1$, $s = 0$ or $s = n$, we have $a'_{st} = 0$, formula (22) for $s = 1$ or $s = n$ writes as

$$a_{1t} - a_{1,t+1} = \frac{1}{2}a'_{1t} \tag{23}$$

$$a_{nt} - a_{n,t+1} = -\frac{1}{2}a'_{n-1,t} \tag{24}$$

Now suppose that $\mathbf{y} = (y_1, \ldots, y_{n-1})$ is an eigenvector of A' to the eigenvalue λ. Consider the vector $\mathbf{x} = (x_1, \ldots, x_n)$ defined by

$$\begin{aligned}
x_1 &= y_1 \\
x_s &= y_s - y_{s-1}, \quad 2 \le s \le n-1 \\
x_n &= -y_{n-1}
\end{aligned} \tag{25}$$

We claim that $\mathbf{x}$ is an eigenvector of A. The image $\mathbf{x}' = A\mathbf{x}$ is computed as

$$x'_s = \sum_{t=1}^{n} a_{st}x_t = a_{s1}y_1 + \sum_{t=2}^{n-1} a_{st}(y_t - y_{t-1}) - a_{sn}y_{n-1} = \sum_{t=1}^{n-1}(a_{st} - a_{s,t+1})y_t \tag{26}$$

According to (22) one obtains for $2 \leq s \leq n-1$,

$$\begin{aligned} x'_s &= \frac{1}{2}\sum_{t=1}^{n-1}(a'_{st} - a'_{s-1,t})\, y_t = \frac{1}{2}\sum_{t=1}^{n-1} a'_{st}\, y_t - \frac{1}{2}\sum_{t=1}^{n-1} a'_{s-1,t}\, y_t \\ &= \frac{1}{2}\lambda y_s - \frac{1}{2}\lambda y_{s-1} = \frac{\lambda}{2} x_s \end{aligned} \tag{27}$$

Similarly, according to (23) and (24), for $s = 1$ or $s = n$ we get

$$x'_1 = \frac{1}{2}\sum_{t=1}^{n-1} a'_{1t}\, y_t = \frac{\lambda}{2} y_1 = \frac{\lambda}{2} x_1 \tag{28}$$

$$x'_n = -\frac{1}{2}\sum_{t=1}^{n-1} a'_{n-1,t}\, y_t = -\frac{\lambda}{2} y_{n-1} = \frac{\lambda}{2} x_n \tag{29}$$

Thus by (25) we have a (linear) mapping $Q : \mathbf{R}^{n-1} \to \mathbf{R}^n$ which maps an eigenvector (to the eigenvalue λ) in dimension $n-1$ to an eigenvector (to the eigenvalue $\lambda/2$) in dimension n. Moreover if $\mathbf{y}$ is symmetric, $\mathbf{x} = Q\mathbf{y}$ is antisymmetric; if $\mathbf{y}$ is antisymmetric, $\mathbf{x} = Q\mathbf{y}$ is symmetric. By induction hypothesis, A' has $n-1$ eigenvectors $\mathbf{y}_k$, $0 \leq k \leq n-2$, to the eigenvalues $\lambda_k = 2^{-k}$ with $M\mathbf{y}_k = (-1)^k \mathbf{y}_k$. Therefore $\mathbf{x}_k = Q\mathbf{y}_{k-1}$, $1 \leq k \leq n-1$, are $n-1$ eigenvectors of A to eigenvalues $\lambda_k = 2^{-k}$ with $M\mathbf{x}_k = (-1)^k \mathbf{x}_k$.

It remains to consider the eigenvalue $\lambda_0 = 1$. Let $I = (\delta_{st})$ denote the identity matrix. Since A is a stochastic matrix, we have $\sum_s (a_{st} - \delta_{st}) = 0$. Hence $A - I$ is a singular matrix and $\lambda = 1$ is an eigenvalue of A. This completes the proof of (19). Moreover, as the eigenvalues are all distinct, the corresponding eigenvectors are determined up to a scalar factor. It follows that the matrix A is diagonalizable, i.e. it can be written in the form

$$A = S^{-1} D S = S^{-1} \begin{pmatrix} \lambda_0 & & 0 \\ & \ddots & \\ 0 & & \lambda_{n-1} \end{pmatrix} S \tag{30}$$

with $\lambda_k = 2^{-k}$ and where the k–the column in S^{-1} is an eigenvector to the eigenvalue λ_k. It remains to show that the eigenvector $\mathbf{x} = \mathbf{x}_0$ to the eigenvalue $\lambda_0 = 1$ is symmetric, and that its components x_s are strictly positive.

Let $\mathbf{y} \in \mathbf{R}^n$ be any vector, and denote by α the first component of $S\mathbf{y}$. Then by (30)

$$\lim_{m \to \infty} A^m \mathbf{y} = \alpha \mathbf{x} \tag{31}$$

Since $\sum_s y_s$ is preserved by A, we have $\sum_s y_s = \alpha \sum_s x_s$. By choosing $\sum_s y_s \neq 0$, we conclude that $\sum_s x_s \neq 0$. Thus we may normalize the eigenvector $\mathbf{x} = \mathbf{x}_0$ such that $\sum_s x_s = 1$. In this case we have $\alpha = \sum_s y_s$, and hence for any $\mathbf{y}$ with $\sum_s y_s = 1$,

$$\lim_{m \to \infty} A^m \mathbf{y} = \mathbf{x} \tag{32}$$

In order to show that all components x_s of $\mathbf{x}$ are strictly positive, consider the set

$$G = \{\mathbf{y} \in \mathbf{R}^n \mid \sum_{s=1}^{n} y_s = 1,\ y_s > 0\} \tag{33}$$

and its closure in the topological space $\mathbf{R}^n$,

$$\overline{G} = \{\mathbf{y} \in \mathbf{R}^n \mid \sum_{s=1}^{n} y_s = 1,\ y_s \geq 0\} \tag{34}$$

Note that $\overline{G}$ is the set of all probability distributions for n–ary random variables. It is easy to see that the matrix A maps $\overline{G}$ into $\overline{G}$. Thus for any $\mathbf{y} \in \overline{G}$ and for all m, we have $A^m\mathbf{y} \in \overline{G}$ and hence $\mathbf{x} = \lim_{m\to\infty} A^m\mathbf{y} \in \overline{G}$. In order to show that actually $\mathbf{x}$ is in G we observe that $A^m(\overline{G}) \subset G$ for m sufficiently large (e.g. $m \geq n$). This claim follows from the fact that the entries of A in the diagonal and next to the diagonal are strictly positive. Hence for any $\mathbf{y} \in \overline{G}$ with $y_s > 0$, also the components y'_{s-1}, y'_s, y'_{s+1} of the image $\mathbf{y}' = A\mathbf{y}$ are strictly positive. Iterating this argument, we conclude that $A^m\mathbf{y} \in G$ for $m \geq n-1$. In particular for $\mathbf{y} = \mathbf{x}$ we have $\mathbf{x} = A^m\mathbf{x} \in G$, i.e. $x_s > 0$ for all s.

Moreover by (18) either $M\mathbf{x} = \mathbf{x}$ or $M\mathbf{x} = -\mathbf{x}$. As $\mathbf{x} \in G$, we must have $M\mathbf{x} = \mathbf{x}$, which means that the eigenvector to the eigenvalue 1 is symmetric. This completes the proof of the theorem. □

4 Probability Distribution of the Carry

4.1 Asymptotic Probability Distribution

According to (32), for any probability distribution $\mathbf{q}_0$ of the initial carry σ_0, the probability distribution of the j–th carry σ_j converges (exponentially) to a unique asymtotic probability distribution

$$\mathbf{x} = \lim_{j\to\infty} A^j\mathbf{q}_0 \tag{35}$$

where $\mathbf{x} = (x_1, \ldots, x_n)$ is the eigenvector of A to the eigenvalue 1, normalized by $\sum_s x_s = 1$. Since $z_j = x_{1j} + \cdots + x_{nj}$ for even carry σ_j and $z_j \neq x_{1j} + \cdots + x_{nj}$ for odd carry, z_j is correlated to the sum $x_{1j} + \cdots + x_{nj}$ of inputs with probability $p_0 = P(z_j = x_{1j} + \cdots + x_{nj}) = x_1 + x_3 + x_5 + \cdots$, or $p_1 = P(z_j \neq x_{1j} + \cdots + x_{nj}) = x_2 + x_4 + x_6 + \cdots$. The normalized correlation (see [3]) caused by the "bias" of the carry is expressed as the difference

$$\delta(n) = p_0 - p_1 = -\sum_{s=1}^{n}(-1)^s x_s \tag{36}$$

The correlation $\delta(n)$ decreases for larger n as is shown in the following theorem.

Theorem 4.1 *For an even number n of inputs there is no bias of the carry, i.e.*

$$\delta(n) = 0, \tag{37}$$

and for an odd number of inputs we have

$$|\delta(n)| < 2^{-(n-1)/2} \tag{38}$$

and in particular $\lim_{n\to\infty} \delta(n) = 0$.

Proof. According to Theorem 3.1 the eigenvector $\mathbf{x}$ of A to the eigenvalue 1 is symmetric. For even n this implies

$$\sum_{s=1}^{n} (-1)^s x_s = 0$$

and hence $\delta(n) = 0$. For odd n the equality $A\mathbf{x} = \mathbf{x}$ can be applied to estimate $\delta(n)$, e.g. as follows

$$\sum_{s=1}^{n} (-1)^s x_s = \sum_{s=1}^{n} (-1)^s \sum_{t=1}^{n} a_{st}\, x_t = \sum_{t=1}^{n} \left(\sum_{s=1}^{n} (-1)^s a_{st} \right) x_t \tag{39}$$

For the evaluation of $\sum_s (-1)^s a_{st}$ in (39), according to (17) the two sums

$$S_0 = S_0(n+1) \;=\; \binom{n+1}{0} - \binom{n+1}{2} + \binom{n+1}{4} - \cdots \pm \binom{n+1}{n+1} \tag{40}$$

$$S_1 = S_1(n+1) \;=\; \binom{n+1}{1} - \binom{n+1}{3} + \binom{n+1}{5} - \cdots \pm \binom{n+1}{n} \tag{41}$$

are to be computed. Then $\sum_s (-1)^s a_{st}$ is equal to $\pm 2^{-n} S_0$ for even s, and to $\pm 2^{-n} S_1$ for odd s, such that

$$\sum_{s=1}^{n} (-1)^s x_s = 2^{-n} (S_1 x_1 + S_0 x_2 - S_1 x_3 - S_0 x_4 + \cdots \pm S_1 x_n) \tag{42}$$

The values $S_0(n+1)$ and $S_1(n+1)$ are given in the following lemma.

Lemma 4.2 *For even m, $m = 2k$, we have*

$$S_0(2k) = \begin{cases} 2^k & k \equiv 0 \pmod 4 \\ 0 & k \equiv 1 \pmod 4 \\ -2^k & k \equiv 2 \pmod 4 \\ 0 & k \equiv 3 \pmod 4 \end{cases} \qquad S_1(2k) = \begin{cases} 0 & k \equiv 0 \pmod 4 \\ 2^k & k \equiv 1 \pmod 4 \\ 0 & k \equiv 2 \pmod 4 \\ -2^k & k \equiv 3 \pmod 4 \end{cases}$$

This lemma immediately follows from the equation

$$S_0 + S_1 i = (1+i)^m = \left(\sqrt{2} e^{i\pi/4}\right)^m = 2^k \left(e^{i\pi/2}\right)^k = 2^k i^k. \tag{43}$$

Therefore by Lemma 4.2 and (42) we get

$$\sum_{s=1}^{n} (-1)^s x_s = \begin{cases} 2^{-n} S_1 (x_1 - x_3 + x_5 - \cdots \pm x_n) & n \equiv 1 \pmod 4 \\ 2^{-n} S_0 (x_2 - x_4 + x_6 - \cdots \pm x_{n-1}) & n \equiv 3 \pmod 4 \end{cases} \tag{44}$$

Since $|x_1 - x_3 + x_5 - \cdots \pm x_n|$ and $|x_2 - x_4 + x_6 - \cdots \pm x_{n-1}|$ are strictly less than 1, this implies $|\delta(n)| < 2^{-n} 2^{(n+1)/2} = 2^{-(n-1)/2}$, hence the theorem. □

4.2 Probability Distribution of the Carry Conditioned on the Output

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 2. Thus I_j is restricted to either even or odd values depending on whether σ_{j-1} is even or odd. This means that the conditional probability $P(I_j = i)$ is either 0 or the double of the value as given in (11). Therefore the conditional probabilities $\mathbf{q}_j$ and $\mathbf{q}_{j-1}$ are related by the formula $\mathbf{q}_j = C\mathbf{q}_{j-1}$ where the transition matrix C, according to Table 2 is given as

$$C = \frac{1}{2^{n-1}} \begin{pmatrix} \binom{n}{0} & 0 & 0 & 0 & 0 & \cdots & 0 \\ \binom{n}{2} & \binom{n}{1} & \binom{n}{0} & 0 & 0 & \cdots & 0 \\ \binom{n}{4} & \binom{n}{3} & \binom{n}{2} & \binom{n}{1} & \binom{n}{0} & \cdots & 0 \\ & & & \vdots & & & \\ 0 & & \cdots & & 0 & \binom{n}{0} & \binom{n}{1} \end{pmatrix} \tag{45}$$

The matrix (45) is of the form

$$C = \begin{pmatrix} 2^{-(n-1)} & 0 & \cdots & 0 \\ * & & & \\ \vdots & & \boxed{A} & \\ * & & & \end{pmatrix} \tag{46}$$

where A is the transition matrix for the unconditioned probability distribution of the carry for $n-1$ inputs as given in (17). By (46) it follows that $\lambda_{n-1} = 2^{-(n-1)}$ is an eigenvalue of C, and for any eigenvector $\mathbf{y}$ of A the vector $(0, \mathbf{y})$ is an eigenvector of C to the same eigenvalue. Thus Theorem 3.1 implies

Corollary 4.3 *The matrix $C = C(n)$ as given by (45) has n different eigenvalues $\lambda_k = 2^{-k}$, $0 \le k \le n-1$. For $0 \le k \le n-2$ the corresponding eigenvectors $\mathbf{x}_k$ are of the form $\mathbf{x}_k = (0, \mathbf{y}_k)$, where $\mathbf{y}_k$ is an eigenvector to λ_k of the matrix $A(n-1)$ as given in (17).*

If a run of t consecutive output digits $z_{j+1} = z_{j+2} = \ldots = z_{j+t} = 0$ has been observed, the (conditional) probabilities $\mathbf{q}_{j+t}$ and $\mathbf{q}_j$ are related by $\mathbf{q}_{j+t} = C^t\mathbf{q}_j$. Similar as in the proof of Theorem 3.1 we conclude that for any probability distribution $\mathbf{q}_j$, in a run of consecutice output digits 0, the probability distribution of the carry tends to the asymptotic value

$$\mathbf{x}' = \lim_{t\to\infty} C^t\mathbf{q}_j = (0, \mathbf{x}) \tag{47}$$

where $\mathbf{x}$ is the (unconditioned) asymptotic probability distribution of the carry for $n-1$ inputs. In such a run, for $m = j + t$, the output digit z_m is asymptotically correlated to $x_{1m} + \cdots + x_{nm}$ with correlation coefficient

$$\delta'(n) = -\sum_{s=1}^{n}(-1)^s x'_s = \sum_{s=1}^{n-1}(-1)^s x_s = -\delta(n-1) \tag{48}$$

A similar result holds for runs of consecutive output digits 1. In fact if z_j is assumed to be 1, the transition matrix of the conditional probabilities is of the form

$$C = \begin{pmatrix} \boxed{A} & \begin{matrix} * \\ \vdots \\ * \end{matrix} \\ 0 \quad \cdots \quad 0 & 2^{-(n-1)} \end{pmatrix} \tag{49}$$

where $A = A(n-1)$ is the transition matrix for the probability distribution of the carry for $n-1$ inputs. Then Theorem 3.1 is applied as in Corrolary 4.3 to determine eigenvectors and eigenvalues. In particular $\mathbf{x}' = (\mathbf{x}, 0)$ is an eigenvector of C to the eigenvalue 1. Thus in a run of consecutice output digits 1, the probability distribution of the carry tends to the asymptotic value $\mathbf{x}' = (\mathbf{x}, 0)$. Therefore the asymptotic correlation of z_m to $x_{1m} + \cdots + x_{nm}$ in a run of consecutive output digits 1 is obtained as

$$\delta'(n) = -\sum_{s=1}^{n}(-1)^s x'_s = -\sum_{s=1}^{n-1}(-1)^s x_s = \delta(n-1) \tag{50}$$

4.3 Numerical Values of $\delta(n)$ for Small n

For small numbers of inputs n the eigenvectors $\mathbf{x}$ of $A = A(n)$ to the eigenvalue 1 are obtained as shown in Table 3. The eigenvectors are normalized by $x_1 = 1$.

n	*Eigenvectors to the eigenvalue 1*	$\sum_{s=1}^{n} x_s$
1	(1)	1
2	(1, 1)	2
3	(1, 4, 1)	6
4	(1, 11, 11, 1)	24
5	(1, 26, 66, 26, 1)	120
6	(1, 57, 302, 302, 57, 1)	720
7	(1, 120, 1191, 2416, 1191, 120, 1)	5,040
8	(1, 247, 4293, 15619, 15619, 4293, 247, 1)	40,320
9	(1, 502, 14608, 88234, 156190, 88234, 14608, 502, 1)	362,880
10	(1, 1013, 47840, 455192, 1310354, 1310354, 455192, 47840, 1013, 1)	3,628,800

Table 3: Eigenvectors to the eigenvalue 1

To obtain the corresponding asymptotic probability distribution of the carry the eigenvectors have to be divided by $\sum_s x_s$, i.e. by the entry in the last column. For odd n the resulting values of $\delta(n)$ are given in Table 4—by Theorem 4.1 for even n the values $\delta(n)$ are 0.

n	1	3	5	7	9	11
$\delta(n)$	1.0000	−0.3333	0.1333	−0.0540	0.0219	−0.0088

Table 4: Values of $\delta(n)$ for odd n

As already pointed out in Theorem 4.1 the bias of the carry diminishes as n gets larger. This means that the resulting correlation probability approaches 0.5. For example from Table 4 one can deduce that the deviation of $\delta(n)$ from 0.5 decreases from 0.1667 for 3 inputs to 0.0044 for 11 inputs.

A closer look at the last column in Table 3 shows that the eigenvectors to the eigenvalue 1 satisfy the equation

$$\sum_{s=1}^{n} x_s = n! \tag{51}$$

In subsequent work, W.-A. Jackson and K. Martin [1], and independently S. Lloyd and C. Mitchell [2], were able to prove that equation (51) holds for arbitrary n. Furthermore in [2] closed formulas for the eigenvectors and the values of $\delta(n)$, as well as some nice combinatorial interpretations have also been derived.

References

[1] W.-A. Jackson, K. Martin, *Private communication*, 1990.

[2] S. Lloyd, C. Mitchell, *Calculating Some Eigenvectors*, Preprint 1990.

[3] W. Meier, O. Staffelbach, *Nonlinearity Criteria for Cryptographic Functions*, Proceedings of Eurocrypt'89, Springer-Verlag, to appear.

[4] W. Meier, O. Staffelbach, *Correlation Properties of Combiners with Memory in Stream Ciphers*, Journal of Cryptology, to appear.

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

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