Correlation Properties of the Bluetooth Combiner

Miia Hermelin and Kaisa Nyberg

Nokia Research Center, Helsinki, Finland
miia.hermelin@nokia.com, kaisa.nyberg@nokia.com

Abstract. In its intended usage the lengths of the key stream sequences produced by the Bluetooth stream cipher E_0 are strictly limited. In this paper the importance of this limitation is proved by showing that the Bluetooth stream cipher with 128 bit key can be broken in $\mathcal{O}(2^{64})$ steps given an output key stream segment of length $\mathcal{O}(2^{64})$. We also show how the correlation properties of the E_0 combiner can be improved by making a small modification in the memory update function.

1 Introduction

Bluetooth™ is a standard for wireless connectivity specified by the Bluetooth™ Special Interest Group in [1]. The specification defines a stream cipher algorithm E_0 to be used for point-to-point encryption between the elements of a Bluetooth network. The structure of E_0 is a modification of a summation bit generator with memory. In this paper we call it the Bluetooth combiner and analyze its correlation properties. A few correlation theorems originating from [4] are stated and exploited in the analysis. Also a new kind of divide-and-conquer attack is introduced, which shows the importance of limiting the lengths of produced key stream sequences.

As a consequence of these results, we propose a modification to the Bluetooth combiner. This modification could be done at no extra cost, that is, it does not increase the complexity of the algorithm. But, on the other hand, it would improve the correlation properties of the Bluetooth combiner to some extent. However, as long as no practical attack is known against the current version of the Bluetooth combiner, the results given in this paper remain theoretical.

2 Correlation Theorems

2.1 Definitions and Notation

Let us introduce the notation to be used throughout this paper. We shall consider the field $GF(2^n)$ as a linear space with a given fixed basis, and denote by x_t an n-dimensional vector in $GF(2^n)$ as $x_t = (x_t^1, x_t^2, \ldots, x_t^n)$. The inner product "$\cdot$" between two vectors $w = (w_1, w_2, \ldots, w_n)$ and $x = (x_1, x_2, \ldots, x_n)$ of the space $GF(2^n)$ is defined as

$$w \cdot x = w_1 x_1 \oplus w_2 x_2 \oplus \ldots \oplus w_n x_n.$$

The linear function $L_u(x)$ is then

$$L_u(x) = u \cdot x, \ u, x \in GF(2^n).$$

We use the same definition of correlation between two Boolean functions as in [3], where it is also referred to as "normalized correlation".

Definition 1. Let $f, g : GF(2^n) \to GF(2)$ be Boolean functions. The correlation between f and g is

$$c(f,g) = 2^{-n}(\#\{x \in GF(2^n) \mid f(x) = g(x)\} - \#\{x \in GF(2^n) \mid f(x) \neq g(x)\}).$$

Sometimes the notation $c_x(f(x), g(x))$ is used to emphasize the variable with respect to which the correlation is to be calculated.

Finally, we recall Parseval's theorem, which implies, in particular, that any Boolean function is correlated to some linear functions.

Theorem 2. *(Parseval's Theorem)*

$$\sum_{w \in GF(2^n)} c(f, L_w)^2 = 1.$$

2.2 Correlation Theorems

Iterated structures and combinations of transformations with common input are frequently seen building blocks of cryptographic algorithms. The following correlation theorems are useful in the analysis of propagation of correlations over such structures. The proofs of the theorems can be found in [4].

Theorem 3. *Given functions $f : GF(2^n) \times GF(2^k) \to GF(2)$ and $g : GF(2^m) \to GF(2^k)$ we set*

$$h(x,y) = f(x, g(y)), \ x \in GF(2^n), \ y \in GF(2^m).$$

Then, for all $u \in GF(2^n)$, $v \in GF(2^m)$,

$$c_{x,y}(h(x,y), u \cdot x \oplus v \cdot y) = \sum_{w \in GF(2^k)} c_{x,z}(f(x,z), u \cdot x \oplus w \cdot z) c_y(w \cdot g(y), v \cdot y).$$

We note that Theorem 3 can be considered as a generalization of Lemma 2 of [3]. In the second correlation theorem a Boolean function, which is a sum of two functions with partially common input, is considered.

Theorem 4. *Let $f : GF(2^n) \times GF(2^k) \to GF(2)$ and $g : GF(2^k) \times GF(2^m) \to GF(2)$ be Boolean functions. Then, for all $u \in GF(2^n)$, $w \in GF(2^m)$,*

$$\begin{aligned} & c_{x,y,z}(f(x,y) \oplus g(y,z), u \cdot x \oplus w \cdot z) \\ = & \sum_{v \in GF(2^k)} c_{x,y}(f(x,y), u \cdot x \oplus v \cdot y) c_{y,z}(g(y,z), v \cdot y \oplus w \cdot z). \end{aligned}$$

If here the two functions f and g, and the two linear combinations u and w are the same, we have the following corollary.

Corollary 5. *Let $f : GF(2^n) \times GF(2^k) \to GF(2)$ be a Boolean function. Then, for all $u \in GF(2^n)$,*

$$c_{x,y,\xi}(f(x,y) \oplus f(\xi,y), u \cdot (x \oplus \xi)) = \sum_{v \in GF(2^k)} c_{x,y}(f(x,y), u \cdot x \oplus v \cdot y)^2.$$

3 Combination Generators

In [3] an example of a summation bit generator with one bit of memory is introduced and analyzed. The combiner of the Bluetooth key stream generator can be considered as a variation of the thoroughly analyzed basic summation bit generator, see [3] and [2]. A general class of combination generators with memory giving the generators of [3] and [1] as special cases is defined as follows:

$$z_t = \bigoplus_{i=1}^{n} x_t^i \oplus c_t^0 \tag{1}$$

$$c_t = f(x_{t-1}, c_{t-1}, \ldots, c_{t-d}). \tag{2}$$

Here $x_t = (x_t^1, \ldots, x_t^n) \in GF(2^n)$ is the fresh input to the combiner at time t and $c_t^0 \in GF(2)$ is the one-bit input from the memory, $t = 0, 1, 2, \ldots$. The fresh input is formed by n independent sequences $x^i = (x_0^i, x_1^i, \ldots)$, $i = 1, 2, \ldots, n$, which are typically generated by n linear feedback shift registers.

The memory constitutes of md bits arranged as a register of d consecutive cells of m bits each. The memory is updated by computing a new m-bit $c_t = (c_t^0, \ldots, c_t^m)$ using a function f from the fresh input and from the contents of the memory saving the new c_t in the memory and discarding c_{t-d}. The output bit z_t is computed as an xor-sum of the fresh input x_t and the previously computed update c_t of the memory.

Correlation attacks aimed at recovering the keys, which determine the generation of the fresh input, are based on correlations between a number of fresh input bits and the output bits. For the type of generators defined by (1) such correlations relations can be derived from correlations between consecutive "carry" bits c_t^0.

Such correlations are usually found by exhaustive search. This is the case also with the Bluetooth combiner which is such a relatively small system that this kind of "trial and error"-search is possible. In larger systems, however, some more sophisticated means for finding these correlation equations should be used. One such method is presented in [2].

4 Bluetooth Combiner

Bluetooth chips are small components capable of short range communication with each other. The Bluetooth specification is given in [1]. In the security part

of [1] an encryption algorithm E_0 is specified to be used for protection of the confidentiality of the Bluetooth communication.

The algorithm E_0 is of the form specified by (1)and (2). It consists of four LFSRs of length 128 in total, a non-linear memory update function f, which is a composition of a nonlinear f_1 and a linear mapping T.

The functions define the following recursive equations. The output key sequence z_t, used to encipher the plaintext, is

$$z_t = x_t^1 \oplus x_t^2 \oplus x_t^3 \oplus x_t^4 \oplus c_t^0,$$

where $(x_t^1, x_t^2, x_t^3, x_t^4)$ is the fresh input at time t produced by the four LFSRs. Non-linearity is represented in the sequence s_t, defined by the following formula, where "+" means the ordinary integer sum:

$$s_{t+1} = (s_{t+1}^1, s_{t+1}^0) = f_1(x_t, c_t) = \left\lfloor \frac{x_t^1 + x_t^2 + x_t^3 + x_t^4 + 2c_t^1 + c_t^0}{2} \right\rfloor.$$

The function f_1 introduces the necessary non-linearity in the system, as integer summation is non-linear in $GF(2)$. The memory bits c_t are then defined with the aid of s_t as

$$c_{t+1} = (c_{t+1}^1, c_{t+1}^0) = T(s_{t+1}, c_t, c_{t-1}) = T_0(s_{t+1}) \oplus T_1(c_t) \oplus T_2(c_{t-1}).$$

Here T_0, T_1 and T_2 are linear transformations. Although non-linearity is crucial for security, the choice of the linear mapping T has also certain influence to the security of the E_0 algorithm, as we will see later.

4.1 The Mapping T

The linear mapping T of E_0 mix the old bits from the memory to the new updated memory bits. The main focus of this work is to investigating its role in the correlation properties. For the given f_1 we see (c.f. Table 1) that $c(s_t^0, c_{t-1}^0 \oplus u \cdot x_t) = 0$, for all $u \in GF(2)$. Hence these are not useful in correlation attacks. On the other hand, $c(s_t^i, c_{t-1}^1 \oplus v^0 c_{t-1}^0 \oplus u \cdot x_t') \neq 0$, $i = 0, 1$.

The mapping T consists of three mappings, T_0, T_1 and T_2, as

$$\begin{aligned} c_{t+1} &= T(s_{t+1}, c_t, c_{t-1}) \\ &= T_0(s_{t+1}) \oplus T_1(c_t) \oplus T_2(c_{t-1}). \end{aligned}$$

In matrix form, $T_0 = T_1 = I$, where I is a 2×2 identity matrix. Further,

$$T_2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

This means, the bits of $c_t = (c_t^1, c_t^0)$ are

$$c_t^1 = s_t^1 \oplus c_{t-1}^1 \oplus c_{t-2}^0 \tag{3}$$

$$c_t^0 = s_t^0 \oplus c_{t-1}^0 \oplus c_{t-2}^1 \oplus c_{t-2}^0. \tag{4}$$

With different choices of T_0, T_1 and T_2 the correlation properties of the system become different. This shall be analyzed in section 5.

4.2 Correlation Analysis of the Bluetooth Combiner

The memory in Bluetooth has four bits, two bits for each two consecutive time steps t and $t-1$. The function, which is used to form a new term z_t of the keys stream, is linear. The non-linearity is gained from the function f_1, which is used to calculate s_t. As argued in [3], and in more general terms in [2], there remain always some correlations in such a system. They shall be analyzed next.

The analysis exploits the correlations of the form

$$c(w \cdot s_{t+1}, u \cdot x_t \oplus v \cdot c_t)$$

where $u \in GF(2^4)$ and $v = (v^1, v^0) \in GF(2^2)$. Different choices of u and v correspond to different linear combinations of $x_t^1, x_t^2, x_t^3, x_t^4, c_t^1$ and c_t^0. In the following Table 1 all the correlations are presented.

v^1	v^0	weight of u	s_{t+1}^1	s_{t+1}^0	$s_{t+1}^1 \oplus s_{t+1}^0$
0	0	0	0	0	$-\frac{5}{8}$
		1	$\frac{1}{4}$	0	0
		2	0	0	$\frac{1}{8}$
		3	0	0	0
		4	0	0	$-\frac{1}{8}$
0	1	0	$\frac{1}{4}$	0	0
		1	0	0	$\frac{1}{8}$
		2	0	0	0
		3	0	0	$-\frac{1}{8}$
		4	$-\frac{1}{4}$	0	0
1	0	0	$\frac{5}{8}$	$-\frac{1}{4}$	0
		1	0	0	$\frac{1}{4}$
		2	$-\frac{1}{8}$	$\frac{1}{4}$	0
		3	0	0	0
		4	$\frac{1}{8}$	$-\frac{1}{4}$	0
1	1	0	0	0	$\frac{1}{4}$
		1	$-\frac{1}{8}$	$\frac{1}{4}$	0
		2	0	0	0
		3	$\frac{1}{8}$	$-\frac{1}{4}$	0
		4	0	0	$-\frac{1}{4}$

Table 1. The correlations for s_{t+1}^1, s_{t+1}^0 and $s_{t+1}^1 \oplus s_{t+1}^0$.

We note that, since the system is symmetric with respect to each x_t^j, only the Hamming weight of u is of importance. We also see that for s_{t+1}^0, the correlation is zero, if $v_1 = 0$. Next we present derivation of the strongest correlation relation we found within the Bluetooth combiner.

Add c^0_{t-3} to the both sides of (4) and rearrange the terms to get

$$c^0_t \oplus c^0_{t-1} \oplus c^0_{t-3} = s^0_t \oplus c^1_{t-2} \oplus c^0_{t-2} \oplus c^0_{t-3}. \tag{5}$$

Next we use Theorem 3 to get

$$\begin{aligned} & c(c^0_t \oplus c^0_{t-1} \oplus c^0_{t-3}, 0) = c(s^0_t, c^1_{t-2} \oplus c^0_{t-2} \oplus c^0_{t-3}) \\ = & \sum_{w \in GF(2^2)} c(s^0_t, w \cdot c_{t-1}) c(w \cdot c_{t-1}, c^0_{t-2} \oplus c^1_{t-2} \oplus c^0_{t-3}), \end{aligned}$$

with $u = 0$, $v = (0,0,1,1,1,0)$ and $y = (s^0_{t-1}, s^1_{t-1}, c^0_{t-2}, c^1_{t-2}, c^0_{t-3}, c^1_{t-3})$. Now from Table 1 we know, that the terms of the sum are zero for $w = (0,1), w = (1,1)$ and $w = (0,0)$. Only the term with $w = (1,0)$ remains. So, the correlation equation is simplified to

$$\begin{aligned} & c(c^0_t \oplus c^0_{t-1} \oplus c^0_{t-3}, 0) \\ = & c(s^0_t, c^1_{t-1}) c(c^1_{t-1}, c^0_{t-2} \oplus c^1_{t-2} \oplus c^0_{t-3}) \\ = & c(s^0_t, c^1_{t-1}) c(s^1_{t-1}, c^0_{t-2}). \end{aligned}$$

Here the last equation is obtained by moving back in time for one step in equation (3), so that

$$c^1_{t-1} = c^1_{t-1} \oplus s^1_{t-1} \oplus c^0_{t-3}.$$

Using the values of Table 1, we finally get

$$c(c^0_t \oplus c^0_{t-1} \oplus c^0_{t-3}, 0) = -\frac{1}{4} \cdot \frac{1}{4} = -\frac{1}{16}. \tag{6}$$

After this we notice that

$$z_t \oplus z_{t-1} \oplus z_{t-3} = \bigoplus_1^4 x^i_t \oplus \bigoplus_1^4 x^i_{t-1} \oplus \bigoplus_1^4 x^i_{t-3} \oplus c^0_t \oplus c^0_{t-1} \oplus c^0_{t-3}.$$

We conclude by equation (6) that

$$c(z_t \oplus z_{t-1} \oplus z_{t-3}, \bigoplus_1^4 x^i_t \oplus \bigoplus_1^4 x^i_{t-1} \oplus \bigoplus_1^4 x^i_{t-3}) = -\frac{1}{16}. \tag{7}$$

Since the output function of the Bluetooth combiner is XOR, it is maximum order correlation immune. Hence divide and conquer attacks in their standard form are not useful for determining the initial states of the LFSR's. In section 6 it is shown how the achieved correlation relation can be utilized to determine a theoretical upper-bound of the level of the security of the Bluetooth combiner.

5 Alternative Mappings for Mixing the Carry Bits

The goal of this section is to investigate, how the choice of the mapping T affects the correlation properties of the Bluetooth combiner. In particular, we show that the mapping T can be selected in such a way that more than two linear approximations are needed when establishing a correlation relation between consecutive carry bits.

Our method exploits a matrix which makes it possible to consider all possible linear approximations of the function f_1 simultaneously.

Let T_0, T_1 and T_2 be arbitrary 2×2 matrices:

$$T_0 = \begin{pmatrix} t_0^1 & t_0^2 \\ t_0^3 & t_0^4 \end{pmatrix}, \; T_1 = \begin{pmatrix} t_1^1 & t_1^2 \\ t_1^3 & t_1^4 \end{pmatrix}, \text{ and } T_2 = \begin{pmatrix} t_2^1 & t_2^2 \\ t_2^3 & t_2^4. \end{pmatrix}$$

Then

$$c_t = T_0 s_t \oplus T_1 c_{t-1} \oplus T_2 c_{t-2}. \tag{8}$$

We write $T_1 = A \oplus B$. Here the analyst can choose A and B in which way ever is convenient, as long as their sum is T_1. The equation (8) can be written as

$$c_t = T_0 s_t \oplus A c_{t-1} \oplus B c_{t-1} \oplus T_2 c_{t-2}. \tag{9}$$

We perform one iteration by inserting equation (8), applied for $t-1$ instead of t, to the equation (9) and get

$$c_t = T_0 s_t \oplus B c_{t-1} \oplus A T_0 s_{t-1} \oplus A T_1 c_{t-2} \oplus A T_2 c_{t-3} \oplus T_2 c_{t-2}. \tag{10}$$

Now, A may be chosen. Let D be a matrix of the form

$$D = \begin{pmatrix} d_1 & d_2 \\ 0 & d_4 \end{pmatrix}.$$

As the analyst wishes to minimize the number of correlation approximations, she wants c_t^0 not to depend on c_{t-3}^1. Therefore, she chooses $AT_2 = D$. If we assume that T_2 is invertible then such a choice is always possible. Inserting $B = T_1 \oplus A$ into equation (10), as well as $A = DT_2^{-1}$, we have

$$c_t = T_0 s_t \oplus (T_1 \oplus D T_2^{-1}) c_{t-1} \oplus (D T_2^{-1} T_0) s_{t-1} \oplus (D T_2^{-1} T_1 \oplus T_2) c_{t-2} \oplus D c_{t-3}. \tag{11}$$

In order to take the correlation approximations into consideration, we write them in matrix form as

$$s_t = X_t c_{t-1},$$

where

$$X_t = \begin{pmatrix} e_t^1 & e_t^2 \\ e_t^3 & e_t^4 \end{pmatrix},$$

and s_t and c_{t-1} are taken as vertical vectors.

We see from Table 1, that if $e_t^3 = 0$ the correlations for s_t^0

$$c(s_t^0, e_t^3 \cdot c_{t-1}^1 \oplus e_t^4 \cdot c_{t-1}^0 \oplus u \cdot x_t),$$

are always zero. Therefore we can presume $e_t^3 = 1$. The choice of u does not affect the best non-zero values of the correlations. Therefore, we shall drop $u \cdot x_t$ and merely study the combinations of s_{t+1}^i and c_t^j.

We approximate twice by inserting $s_t = X_t c_{t-1}$ into equation (11), which yields

$$c_t = (T_0 X_t \oplus T_1 \oplus D T_2^{-1}) c_{t-1} \oplus (D T_2^{-1} T_0 X_{t-1} \oplus D T_2^{-1} T_1 \oplus T_2) c_{t-2} \oplus D c_{t-3}. \quad (12)$$

In Bluetooth the generated key-sequence z_t does not depend on c_t^1 but merely on c_t^0. Hence, similarly as above in section 4.2, we aim at establishing a correlation relation between zero components of c_t.

Theorem 6. *Let in the Bluetooth combiner generator $T_0 = T_1 = I$ and T_2 an arbitrary invertible 2×2 matrix. If $t_2^3 = 1$, then two correlation approximations suffices to establish a correlation between the input and output.*

Proof. Substitute $T_0 = T_1 = I$ and the general form of T_2 into (12) and obtain the following correlation relation for c_t^0:

$$\begin{aligned} c_t^0 = {} & (1 \oplus d_4, e_t^4 \oplus 1 \oplus d_4 t_2^1) \cdot c_{t-1} \\ & \oplus (d_4 e_{t-1}^1 \oplus d_4 t_2^1 \oplus d_4 \oplus 1, d_4 e_{t-1}^2 \oplus d_4 t_2^1 e_{t-1}^4 \oplus d_4 t_2^1 \oplus t_2^4) \cdot c_{t-2} \\ & \oplus d_4 c_{t-3}^0 \end{aligned}$$

To have only two approximations means that there must be neither c_{t-1}^1 nor c_{t-2}^1 in the equation above, i.e.

$$1 \oplus d_4 = 0 \quad (13)$$

and

$$d_4 e_{t-1}^1 \oplus d_4 t_2^1 \oplus d_4 \oplus 1 = 0. \quad (14)$$

If $d_4 = 0$, then the other approximation will cancel out, so that equation (11) transforms into the initial equation

$$c_t^0 = s_t^0 \oplus c_{t-1}^0 \oplus c_{t-2}^1 \oplus c_{t-2}^0.$$

As this is not what the analyst wants, she chooses $d_4 = 1$ and equation (13) is true. From (14) we then get that

$$e_{t-1}^1 \oplus t_2^1 = 0.$$

Now we check from Table 1 that $c(s_{t-1}^1, c_{t-2}^0 \oplus u \cdot x_{t-2}) \neq 0$ for some u. Hence it is possible to use this correlation if $t_2^1 = 0$. Similarly, if $t_2^1 = 1$, we see that $e_{t-1}^1 = 1$ is possible, as $c(s_{t-1}^1, c_{t-2}^1 \oplus v^0 \cdot c_{t-2}^0 \oplus u \cdot x_{t-2}) \neq 0$ for some choice of u and v^0. □

In the case of the initial choice of Bluetooth T_2, we have $t_2^3 = 1$. So, as we saw earlier in section 4.2, only two iteration approximations are needed. The approximation matrices X_t in the case of (6) were

$$X_{t-1} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \quad X_t = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

From Table 1 we see that $c(s_{t-1}^1, c_{t-2}^1) = \frac{5}{8}$. Hence

$$T_2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

with $t_2^1 = 1$ would have been still a weaker choice than the current T_2 in Bluetooth. Next we show that a stronger choice would have been possible.

Theorem 7. *Let $t_2^3 = 0$. Then at least three approximation rounds are needed.*

Proof. If $t_2^3 = 0$, and T_2 is invertible as assumed, then $t_2^1 = t_2^4 = 1$. Also $T_2^{-1} = T_2$. Let

$$D = \begin{pmatrix} d_1 & d_2 \\ d_3 & d_4 \end{pmatrix}.$$

Then, as in (12) we have

$$c_t = (X_t \oplus I \oplus DT_2)c_{t-1} \oplus (DT_2X_{t-1} \oplus DT_2X_{t-1} \oplus DT_2 \oplus T_2)c_{t-2},$$

and further,

$$\begin{aligned} c_t^0 &= (1 \oplus d_3, e_t^4 \oplus 1 \oplus t_2^2 d_3 \oplus d_4) \cdot c_{t-1} \\ &\quad \oplus [d_3 e_{t-1}^1 \oplus e_{t-1}^3 (t_2^2 d_3 \oplus d_4) \oplus d_3, \\ &\qquad d_3 e_{t-1}^2 \oplus e_{t-1}^4 (t_2^2 d_3 \oplus d_4) \oplus t_2^2 d_3 \oplus d_4 \oplus 1] \cdot c_{t-2} \\ &\quad \oplus (d_3, d_4) \cdot c_{t-3} \end{aligned}$$

Now, if $d_3 = 1$, then we have c_{t-3}^1 in the equation, so we need to do at least one more approximation, hence two approximations is not enough. If $d_3 = 0$, then c_{t-1}^1 is within the equation of c_t^0 and again more than two approximations are needed. □

An example of a matrix T_2, which requires at least three approximations to get correlation relations between the carry bits c_t^0 from different time instances, is $T_2 = I$. We consider, for example, the correlation between c_t^0 and c_{t-4}^0. The correlation relation could involve some x_t variables at appropriate moments t, but in what follows we restrict to the case where the Hamming weight of u is always zero.

Corresponding to the equations (3) and (4) we now have

$$\begin{aligned} c_t^1 &= s_t^1 \oplus c_{t-1}^1 \oplus c_{t-2}^1 \\ c_t^0 &= s_t^0 \oplus c_{t-1}^0 \oplus c_{t-2}^0. \end{aligned}$$

Since no x_{t-1} is involved, we have by Theorem 3 and with the aid of Table 1

$$\begin{aligned} c(c_t^0, c_{t-4}^0) &= c(s_t^0, c_{t-1}^0 \oplus c_{t-2}^0 \oplus c_{t-4}^0) \\ &= \sum_w c(s_t^0, w \cdot c_{t-1}) c(w \cdot c_{t-1}, c_{t-1}^0 \oplus c_{t-2}^0 \oplus c_{t-4}^0) \\ &= c(s_t^0, c_{t-1}^1) c(c_{t-1}^1, c_{t-1}^0 \oplus c_{t-2}^0 \oplus c_{t-4}^0). \end{aligned}$$

The second equality follows from Theorem 3, and in the third we noted that the only non-zero correlation for $c(s_t^0, w \cdot c_{t-1})$ is due to $w = (1, 0)$. We continue in the same manner to obtain:

$$\begin{aligned} & c(c_t^0, c_{t-4}^0) \\ &= -\frac{1}{4} c(s_{t-1}^1 \oplus s_{t-1}^0, c_{t-2}^1 \oplus c_{t-3}^1 \oplus c_{t-3}^0 \oplus c_{t-4}^0) \\ &= -\frac{1}{4} \sum_w c(s_{t-1}^1 \oplus s_{t-1}^0, w \cdot c_{t-2}) c(w \cdot c_{t-2}), c_{t-2}^1 \oplus c_{t-3}^1 \oplus c_{t-3}^0 \oplus c_{t-4}^0) \\ &= -\frac{1}{4} (c(s_{t-1}^1 \oplus s_{t-1}^0, 0) c(c_{t-2}^1 \oplus c_{t-3}^1 \oplus c_{t-3}^0 \oplus c_{t-4}^0, 0) \\ &+ c(s_{t-1}^1 \oplus s_{t-1}^0, c_{t-2}^1 \oplus c_{t-2}^0) c(c_{t-2}^0, c_{t-3}^1 \oplus c_{t-3}^0 \oplus c_{t-4}^0)). \end{aligned} \tag{15}$$

From the two terms inside the brackets only the last one is non-zero. To see this we calculate the first term

$$\begin{aligned} & c(c_{t-2}^1 \oplus c_{t-3}^1 \oplus c_{t-3}^0 \oplus c_{t-4}^0, 0) \\ &= c(s_{t-2}^1, c_{t-3}^0 \oplus c_{t-4}^1 \oplus c_{t-4}^0) \\ &= \sum_w c(s_{t-2}^1, w \cdot c_{t-3}) c(w \cdot c_{t-3}, c_{t-3}^0 \oplus c_{t-4}^1 \oplus c_{t-4}^0) \\ &= c(s_{t-2}^1, c_{t-3}^0) c(c_{t-4}^1 \oplus c_{t-4}^0, 0) + c(s_{t-2}^1, c_{t-3}^1) c(c_{t-3}^1, c_{t-3}^0 \oplus c_{t-4}^1 \oplus c_{t-4}^0). \end{aligned}$$

In the last equality the first term in the sum is zero, since the memory bits on the same moment are assumed to be statistically independent. We continue with the second part of the sum:

$$\begin{aligned} & c(c_{t-3}^0 \oplus c_{t-3}^1, c_{t-4}^1 \oplus c_{t-4}^0) \\ &= c(s_{t-3}^1 \oplus s_{t-3}^0, c_{t-5}^1 \oplus c_{t-5}^0) \\ &= \sum_w c(s_{t-3}^1 \oplus s_{t-3}^0, w \cdot c_{t-4}) c(w \cdot c_{t-4}, c_{t-5}^1 \oplus c_{t-5}^0) \\ &= -\frac{5}{8} (c(s_{t-3}^1 \oplus s_{t-3}^0, 0) c(c_{t-5}^1 \oplus c_{t-5}^0, 0) \\ &+ c(s_{t-3}^1 \oplus s_{t-3}^0, c_{t-4}^1 \oplus c_{t-4}^0) c(c_{t-4}^1 \oplus c_{t-4}^0, c_{t-5}^1 \oplus c_{t-5}^0)) \\ &= -\frac{5}{8} \cdot \frac{1}{4} c(c_{t-4}^1 \oplus c_{t-4}^0, c_{t-5}^1 \oplus c_{t-5}^0). \end{aligned}$$

These calculations are easy to generalize to any moment $t - j$, $j = 0, 1, 2, \ldots$, so actually we have

$$c(c_{t-3}^0 \oplus c_{t-3}^1, c_{t-4}^1 \oplus c_{t-4}^0)$$

$$= \left(-\frac{5}{32}\right)^k c(c^1_{t-3-k} \oplus c^0_{t-3-k}, c^1_{t-4-k} \oplus c^0_{t-4-k}).$$

Hence, infinitely many approximations should be done, and so the correlation can be regarded as zero:

$$c(c^0_{t-3} \oplus c^1_{t-3}, c^1_{t-4} \oplus c^0_{t-4}) = \lim_{k\to\infty} \left(-\frac{5}{32}\right)^k = 0.$$

Let us now return to the equation 15. We have, that

$$\begin{aligned} & c(c^0_t, c^0_{t-4}) \\ &= -\frac{1}{4} \cdot \frac{1}{4} c(c^0_{t-2}, c^1_{t-3} \oplus c^0_{t-3} \oplus c^0_{t-4}) \\ &= -\frac{1}{16} c(s^0_{t-2}, c^1_{t-3}) = -\frac{1}{64}, \end{aligned}$$

which is significantly smaller than $\frac{1}{16}$ in equation 6. In this manner, the correlation can be calculated for other weights of u, too. The resulting values degenerate to a single product, as above, so that the product of the correlations is always significantly smaller than $\frac{1}{16}$.

The Bluetooth combination generator is a strengthened version of the basic summation bit generator. By increasing the size of the memory the correlations have been reduced. We have shown that with the same memory size, by making a small modification in the memory update function, it would be possible to further reduce the correlations.

6 Ultimate Divide and Conquer

In this section it is shown that divide and conquer attack becomes possible if the length of the given keystream is longer than the period p of the shortest (say, the first) LFSR used in the key stream generation. Assume that there is a relation with a non-zero correlation ρ between a linear combination of the shift register output bits

$$(u^1_0 x^1_t \oplus \ldots \oplus u^n_0 x^n_t) \oplus \ldots \oplus (u^1_d x^1_{t-d} \oplus \ldots \oplus u^n_d x^n_{t-d})$$

and the key stream bits

$$w_0 z_t \oplus w_1 z_{t-1} \oplus \ldots \oplus w_d z_{t-d},$$

over a number of $d+1$ time steps. Then it follows by Corollary 5 that we have a correlation relation between a linear combination of the keystream bits

$$w_0(z_t \oplus z_{t+p}) \oplus w_1(z_{t-1} \oplus z_{t+p-1}) \oplus \ldots \oplus w_d(z_{t-d} \oplus z_{t+p-d})$$

and a linear combination of the LFSR output bits

$$\begin{aligned} & u^2_0(x^2_t \oplus x^2_{t+p}) \oplus \ldots \oplus u^n_0(x^n_t \oplus x^n_{t+p}) \oplus \ldots \\ & \oplus u^2_d(x^2_{t-d} \oplus x^2_{t+p-d}) \oplus \ldots \oplus u^n_d(x^n_{t-d} \oplus x^n_{t+p-d}), \end{aligned}$$

where the output bits from the first (the shortest) shift register cancel, since they are equal.

By Corollary 5, the strength of the correlation over the period p is at least ρ^2. Further, Corollary 5 shows how this lower bound can be improved. We state this result in a form of a theorem as follows.

Theorem 8. *For a combination generator, assume that we have the following correlation*

$$c(w_0 z_t \oplus w_1 z_{t-1} \oplus \ldots \oplus w_d z_{t-d}, \\ (u_0^1 x_t^1 \oplus \ldots \oplus u_0^n x_t^n) \oplus \ldots + (u_d^1 x_{t-d}^1 \oplus \ldots \oplus u_d^n x_{t-d}^n)) = \rho \neq 0.$$

Let the lengths of the registers be $L_1, \ldots, L_n$ and the periods $p_1, \ldots, p_n$. Then given a keystream of length $p_1 p_2 \cdots p_k + \frac{1}{\rho^4} + d$ one can do exhaustive search over the $L_{k+1} + \ldots + L_n$ bits which form the initial contents of $n - k$ registers.

If the LFSR registers have primitive feedback polynomials, then $p_i = 2^{L_i} - 1$. In most applications n is even and the lengths L_i are about the same. Then given a sufficiently strong correlation between the input bits and the output bits of a combination generator, the complexity to determine the complete initial state of length L is about $\mathcal{O}(2^{L/2})$. In other words, by generating key stream of length $\mathcal{O}(2^{L/2})$ one can successfully carry out exhaustive search over $L/2$ bits of the initial state.

6.1 Periodic Correlations in Bluetooth

Computation of the correlations for the Bluetooth E_0 combiner is somewhat complicated due to multiple iteration. We make use of the relation $c_t^0 + c_{t-1}^0 + c_{t-3}^0 = 0$, see (6). Applying Theorem 3 we get

$$\begin{aligned} & c(c_t^0 \oplus c_{t-1}^0 \oplus c_{t-3}^0 \oplus c_{t+p}^0 \oplus c_{t+p-1}^0 \oplus c_{t+p-3}^0, 0) \\ & = c(s_t^0 \oplus s_{t+p}^0, c_{t-2}^0 \oplus c_{t-2}^1 \oplus c_{t-3}^0 plus c_{t+p-2}^0 \oplus c_{t+p-2}^1 + c_{t+p-3}^0) \\ & = \sum_{w,w' \in GF(2^2)} c(s_t^0 \oplus s_{t+p}^0, w \cdot c_{t-1} \oplus w' \cdot c_{t+p-1}) \\ & \quad \cdot c(w \cdot c_{t-1} \oplus w' \cdot c_{t+p-1}, c_{t-2}^0 \oplus c_{t-2}^1 \oplus c_{t-3}^0 \oplus c_{t+p-2}^0 \oplus c_{t+p-2}^1 \oplus c_{t+p-3}^0). \end{aligned}$$

Now we apply Theorem 4 to the first correlation in the product and get

$$\begin{aligned} & c(s_t^0 \oplus s_{t+p}^0, w \cdot c_{t-1} \oplus w' \cdot c_{t+p-1}) \\ & = \sum_{u \in GF(2^2)} c(s_t^0, w \cdot c_{t-1} \oplus u \cdot x) c(s_t^0, w' \cdot c_{t-1} \oplus u \cdot x). \end{aligned}$$

Here x has one, two, or three coordinates, depending on whether p is the least common period of of one, two, or three LFSRs, respectively.

Let us now consider the case where p is the least common period of two LFSRs. From Table 1 we see that these correlations are nonzero if and only if

$u = (0,0)$ and $w = w' = (1,0)$, or $u = (1,1)$ and $w = w' = (1,0)$, or $u = (0,1)$ and $w = w' = (1,1)$, or finally, $u = (1,0)$ and $w = w' = (1,1)$.

The value $w = w' = (1,1)$ leads to a longer correlation relation extending over at least two rounds, and hence are expected be of less in amount, but still non-negative. Therefore, we discard the corresponding terms, and get a lower bound to the correlation from the remaining terms with $w = w' = (1,0)$ as follows

$$\begin{aligned}
&c(c_t^0 \oplus c_{t-1}^0 \oplus c_{t-3}^0 \oplus c_{t+p}^0 \oplus c_{t+p-1}^0 \oplus c_{t+p-3}^0, 0) \\
&\geq (c(s_t^0, c_{t-1}^1)^2 + c(s_t^0, c_{t-1}^1 \oplus x_t^1 \oplus x_t^2)^2) \\
&\quad \cdot c(c_{t-1}^1 \oplus c_{t+p-1}^1, c_{t-2}^0 \oplus c_{t-2}^1 \oplus c_{t-3}^0 \oplus c_{t+p-2}^0 \oplus c_{t+p-2}^1 \oplus c_{t+p-3}^0) \\
&= (c(s_t^0, c_{t-1}^1)^2 + c(s_t^0, c_{t-1}^1 \oplus x_t^1 \oplus x_t^2)^2) \cdot \sum_{u \in GF(2^2)} c(s_{t-1}^1, c_{t-2}^0 \oplus u \cdot x)^2 \\
&= ((-1/4)^2 + (1/4)^2)(1/4)^2 = 2^{-7},
\end{aligned}$$

using the correlation values given in Table 1.

It should be stressed, however, that the presented ultimate divide and conquer attack is of theoretical nature, and practical only if the analyzer is given access to key stream extending over periods of partial input. For example, the Bluetooth E_0 algorithm in its intended use generates only short segments of keystream to encrypt each plaintext frame starting from a new independent initial state.

7 Conclusions

We have seen how the correlations in the Bluetooth combiner could be reduced by making a small modification in its memory update function. This improvement is, however, rather theoretical in nature, but quite interesting as such. The methods used in finding this modification are specific to Bluetooth, but could be easily adapted to other similar combiner generators. The technique involves a matrix describing potential approximations based on known non-zero linear correlations over the non-linear part of the memory update function.

We also showed how any significant correlations over a combiner can be used to launch a divide and conquer attack against any combiner generator provided that sufficient amount of the output keystream is given. If the input to the combiner is produced using a certain number of LFSRs with primitive feedback polynomials, and the number of bits of the total initial state is L, then the complexity of this attack is upper bounded by $\mathcal{O}(2^{L/2})$. This will require the amount of same magnitude $\mathcal{O}(2^{L/2})$ of the output bits.

We conclude that if the effective key length of a combiner generator is required to be about the same magnitude as the size of the initial state, then the usage of the generator must be restricted in such a way that the length of any keystream block ever produced by this generator never exceeds the shortest period of the input sequences.

References

1. Bluetooth^{TM} SIG. *Bluetooth Specification*, Version 1.0 A, 24 July 1999.
2. J. Dj. Golić. Correlation properties of a general binary combiner with memory, *Journal of Cryptology*, Vol 9 Number 2, 1996, pp. 111-126.
3. W. Meier and O. Staffelbach. Correlation properties of combiners with memory in stream ciphers, *Journal of Cryptology*, Vol 5 Number 1, 1992, pp. 67-86.
4. K. Nyberg. Correlation theorems in cryptanalysis (submitted)

This article was processed using the LaTeX macro package with LLNCS style