Achterbahn-128/80: Design and Analysis

Berndt Gammel Rainer Göttfert Oliver Kniffler

Infineon Technologies AG
Germany

berndt.gammel@infineon.com
rainer.goettfert@infineon.com
oliver.kniffler@infineon.com

Abstract. We determine the imbalances of the keystreams produced by Achterbahn-80 and Achterbahn-128 in two different ways. The number of cyclically inequivalent keystreams produced by the keystream generators of Achterbahn-80 and Achterbahn-128 is determined. An abstract model for the keystream generator of a primitive NLFSR combination generator is used to justify the correlation attack introduced in [6] and generalized in [8]. A common error in a guess and determine attack is discussed. The optimal decision rule for finding the correct initial state of the target shift register in the guess and determine attack is described in the coin tossing model. The reliability of results derived from the abstract keystream generator model and the coin tossing model is demonstrated by running an actual guess and determine attack on a cipher that could be called Baby-Achterbahn. Two attacks against Achterbahn-128/80 found by Naya-Plasencia [8] and Hell and Johansson [5] are shown to be equivalent.

1 Introduction

Achterbahn-128 and Achterbahn-80 are two NLFSR based additive stream ciphers [2]. The keystream generator of the first cipher deploys 13 shift registers denoted by A_0 through A_{12}. All shift registers are nonlinear, fix the allzero state, and produce a sequence of maximum period for every nonzero initial state. We call such shift registers primitive. The lengths N_j of the shift registers are $N_j = 21 + j$ for $0 \leq j \leq 12$. The least periods of the nonzero output sequences of the shift registers A_j are denoted by p_j. Thus $p_j = 2^{21+j} - 1$ for $0 \leq j \leq 12$.

The keystream generator of Achterbahn-80 deploys the shift registers A_1 through A_{11}. The Boolean combining function G of Achterbahn-80 is a subfunction of the combining function F of Achterbahn-128. We have $G(x_1, \ldots, x_{11}) = F(0, x_1, \ldots, x_{11}, 0)$. Because of this Achterbahn-128 is downward compatible to Achterbahn-80. We use the name Achterbahn-128/80 for a stream cipher that can produce both keystreams. The design size of Achterbahn-128/80 is therefore slightly larger than the design size of Achterbahn-128, due to the enhanced control logic. The design size of Achterbahn-80 at frequencies below 400 MHz amounts to about 2188 NAND gate equivalents (GE). The design size of Achterbahn-128/80 has 2538 GE. The design promotes parallel implementations up to a factor of eight. (This property is the reason for the name: Achterbahn = eigth liner.) In an 8-bit implementation of Achterbahn, a throughput of 8 Gigabit/s is achieved.

The frame lengths for both keystream generators in Achterbahn-128/80 were declared by the designers to be 2^{64} (see page 2 in [2]). Recently Naya-Plasencia [8] and Hell and Johansson [5] showed that the cipher can be broken with complexities below the complexity of an brute force attack if the attackers have more than 2^{56} respectively 2^{60} keystream bits at their proposal. Due to these findings, the new recommended frame length for Achterbahn-80 is 2^{52} bits. The recommended frame length for Achterbahn-128 is 2^{56} bits.

2 Number of keystreams

A primitive feedback shift register combination generator consists of a Boolean combining function F of n variables and n primitive binary feedback shift registers. At each time unit each shift register produces one output bit, and the n output bits of the n shift registers are compressed into one keystream bit. The primitive combination generator in which all feedback shift registers are linear is probably the most studied keystream generator. Achterbahn-80 and Achterbahn-128 are realizations of a primitive feedback shift register combination generator in which all shift registers are nonlinear. If the lengths of the n shift registers are pairwise relatively prime, then for every admissible initialization of the keystream generator, the same periodic sequence is produced. Different initializations correspond to different positions in this sequence. If the lengths of the shift registers are not pairwise relatively prime, then it can happen that different initializations give rise to different keystreams. We call an initialization of the keystream generator admissible if all shift registers are in a nonzero state.

Theorem 1. *If all admissible initializations are used, then Achterbahn-80 produces* $470\,624\,175$ *different keystreams each of which has least period* $> 2^{268.18}$ *and linear complexity* $> 2^{100.46}$. *Under the same provision, Achterbahn-128 will produce* $5\,995\,037\,111\,378\,175$ *cyclically inequivalent keystreams. Each keystream has least period* $> 2^{298.58}$ *and linear complexity* $> 2^{100.92}$.

Proof. It has been proved in [2, Sec. 4.2] that for each admissible initialization the corresponding keystream produced by Achterbahn-80 has least period $v = \operatorname{lcm}(p_1, \ldots, p_{11})$. In particular, all keystreams have the same least period. The number of admissible initializations is $u = \prod_{j=1}^{11} p_j$. It follows that there are $u/v = 470\,624\,175$ cyclically inequivalent keystreams. The assertion for Achterbahn-128 is proved similarly. The lower bounds for the linear complexities have been derived in [2, Sec. 4.3, p. 37]. □

In order to be able to prove lower bounds for the linear complexity of the keystream, to pass statistical tests, and to resist correlation attacks, it is necessary that the shift registers in a primitive combination generator have distinct lengths. It is, however, not necessary that the lengths are pairwise relatively prime. The most efficient hardware implementation will use shift registers whose lengths cover all integer values in some interval. The design of Achterbahn-128/80 follows this principle. Figure 2 in Appendix B shows the design size of an Achterbahn-128/80 implementation as a function of various throughput values.

3 Imbalance of keystream

Let X be a binary-valued random variable with $\Pr(X = 0) = p$. The magnitude $\varepsilon = 2p - 1$ is called the *imbalance* of X. The name was introduced in [3, Definiton 2], although the authors were only interested in the absolute value of the imbalance. The bias δ of X is usually defined by $\Pr(X = 1) = \frac{1}{2} + \delta$. Then $\varepsilon = -2\delta$, so that the absolute value of the imbalance is twice the absolute value of the bias.

We define the imbalance of a binary periodic sequence as follows: Let σ be a binary (purely) periodic sequence of least period $r \geq 1$ containing k zeros among its first r terms. Then the imbalance ε of σ is defined to be $\varepsilon = (2k - r)/r$.

When discussing properties of a Boolean function $F(x_1, \ldots, x_n)$, it is convenient to make use of probabilistic terminology. For instance, the fact that F is balanced, which means that $F(\mathbf{a}) = 0$ holds for exactly 2^{n-1} input vectors $\mathbf{a} \in \mathbb{Z}_2^n$, can be expressed by the equation $\Pr(F = 0) = 1/2$. In this setting, the input variables $x_1, \ldots, x_n$ are (tacitly) treated as independent symmetrically distributed binary-valued random variables. In the sequel we shall consider Boolean functions whose original variables $x_1, x_2, \ldots$ are replaced by arbitrary binary random variables $X_1, X_2, \ldots$, which are not necessarily independent or symmetrically distributed. In this case, we shall always use capital letters to distinguish the two cases.

Lemma 1. *Let F be an m-resilient Boolean function of n variables ($1 \leq m < n$). Let $X_1, \ldots, X_n$ be statistically independent binary random variables with $\Pr(X_j = 0) = \frac{1}{2}(1+\varepsilon_j)$, $1 \leq j \leq n$. The random variable $Z = F(X_1, \ldots, X_n)$ satisfies*

$$\Pr(Z = 0) = \frac{1}{2} + \sum_{k=m+1}^{n} \sum_{1 \leq j_1 < \cdots < j_k \leq n} c_{j_1,\ldots,j_k} \prod_{l=1}^{k} \varepsilon_{j_l}, \tag{1}$$

where the coefficients $c_{j_1,\ldots,j_k} \in \mathbb{Q}$ satisfy $|c_{j_1,\ldots,j_k}| \leq 1/2$.

Proof. Let $\mathbf{x} = (x_1, \ldots, x_n)$. Since F is correlation immune of order m,

$$\Pr(F(\mathbf{x}) = 0 |\, x_{j_1} = e_1, \ldots, x_{j_k} = e_k) = \Pr(F(\mathbf{x}) = 0)$$

for $1 \leq k \leq m$, $1 \leq j_1 < \cdots < j_k \leq n$, and all $(e_1, \ldots, e_k) \in \mathbb{Z}_2^k$. Using Bayes's formula $\Pr(B|A) = \Pr(A|B)\Pr(B)\Pr(A)^{-1}$ if $\Pr(A) \neq 0$ and $\Pr(B) \neq 0$, we get

$$\Pr(x_{j_1} = e_1, \ldots, x_{j_k} = e_k |\, F(\mathbf{x}) = 0) = \frac{1}{2^k}$$

for $1 \leq k \leq m$, $1 \leq j_1 < \cdots < j_k \leq n$, and $(e_1, \ldots, e_k) \in \mathbb{Z}_2^k$. It follows that

$$\Pr(x_{j_1} + \cdots + x_{j_k} = 0 |\, F(\mathbf{x}) = 0) = \frac{1}{2} \tag{2}$$

for $1 \leq k \leq m$ and all $\binom{n}{k}$ possibilities $1 \leq j_1 < \cdots < j_k \leq n$.

Since F is balanced there are exactly $h = 2^{n-1}$ row vectors $\mathbf{a}_i = (a_{i1}, a_{i2}, \ldots, a_{in}) \in \mathbb{Z}_2^n$ with $F(\mathbf{a}_i) = 0$. Let $A = \{\mathbf{a}_1, \ldots, \mathbf{a}_h\} = F^{-1}(\{0\})$. According to (2), for $1 \leq k \leq m$ and $1 \leq j_1 < \cdots < j_k \leq n$, we have

$$a_{i,j_1} + \cdots + a_{i,j_k} = \begin{cases} 0 & \text{for exactly } h/2 \text{ vectors } \mathbf{a}_i \in A; \\ 1 & \text{for the remaining } h/2 \text{ vectors } \mathbf{a}_i \in A. \end{cases} \tag{3}$$

Let $\mathbf{X}$ denote the random vector $(X_1, \ldots, X_n)$ whose components are the given random variables.

$$\begin{aligned}
\Pr(Z=0) &= \sum_{i=1}^{h} \Pr(\mathbf{X} = \mathbf{a}_i) = \sum_{i=1}^{h} \Pr(X_1 = a_{i1}, \ldots, X_n = a_{in}) \\
&= \sum_{i=1}^{h} \prod_{j=1}^{n} \Pr(X_j = a_{ij}) = \frac{1}{2^n} \sum_{i=1}^{h} \prod_{j=1}^{n} (1 + (-1)^{a_{ij}} \varepsilon_j) \\
&= \frac{1}{2} + \frac{1}{2^n} \sum_{i=1}^{h} \sum_{k=1}^{n} \sum_{1 \le j_1 < \cdots < j_k \le n} (-1)^{a_{i,j_1} + \cdots + a_{i,j_k}} \prod_{l=1}^{k} \varepsilon_{j_l} \\
&= \frac{1}{2} + \frac{1}{2^n} \sum_{k=1}^{n} \sum_{1 \le j_1 < \cdots < j_k \le n} \sum_{i=1}^{h} (-1)^{a_{i,j_1} + \cdots + a_{i,j_k}} \prod_{l=1}^{k} \varepsilon_{j_l}.
\end{aligned}$$

Using (3), we obtain

$$\Pr(Z=0) = \frac{1}{2} + \sum_{k=m+1}^{n} \sum_{1 \le j_1 < \cdots < j_k \le n} \left(\frac{1}{2^n} \sum_{i=1}^{h} (-1)^{a_{i,j_1} + \cdots + a_{i,j_k}} \right) \prod_{l=1}^{k} \varepsilon_{j_l}.$$

The coefficient

$$c_{j_1,\ldots,j_k} = \frac{1}{2^n} \sum_{i=1}^{h} (-1)^{a_{i,j_1} + \cdots + a_{i,j_k}} \tag{4}$$

of the product $\varepsilon_{j_1} \cdots \varepsilon_{j_k}$ satisfies $-h2^{-n} \le c_{j_1,\ldots,j_k} \le h2^{-n}$ implying that $|c_{j_1,\ldots,j_k}| \le 1/2$. □

Formula (1) is also true for $m = 0$, that is, if F is just balanced. In the other extreme case $m = n - 1$, we have $F = x_1 + \cdots + x_n$. The only nonzero coefficient in (1) now is $c_{1,\ldots,n} = 1/2$. Thus, in the case $m = n - 1$, Lemma 1 boils down to the piling-up lemma:

$$\Pr(Z=0) = \frac{1}{2}\left(1 + \prod_{j=1}^{n} \varepsilon_j\right).$$

We applied Lemma 1 to the keystream generators of Achterbahn-128/80 and obtained the imbalance $\varepsilon_{80} \simeq -2^{-185.94}$ for the keystreams of Achterbahn-80, and the imbalance $\varepsilon_{128} \simeq -2^{-237.06}$ for the keystreams of Achterbahn-128. In this derivation, we used $\varepsilon_j = 1/(1-2^{N_j})$ for the imbalances of the driving shift registers A_j, $0 \le j \le 12$. Furthermore, we used equation (4) to compute the exact values of the coefficients $c_{j_1,\ldots,j_k}$. These coefficients are derived from the Boolean combining functions $F(x_0, \ldots, x_{12})$ and $G(x_1, \ldots, x_{11})$ of Achterbahn-128 and Achterbahn-80, respectively.

Since the output bits of the various shift registers A_j, $0 \le j \le 12$, are not realizations of statistically independent random variables (as presupposed in Lemma 1), we have to check the applicability of Lemma 1 to primitive feedback shift register combination generators. To this end we used a small combination generator consisting of four primitive NLFSRs of lengths 7, 8, 9, and 11, and the 1-resilient Boolean combining function $H(x_1, \ldots, x_4) = x_1 + x_2 + (x_1 + x_4)(x_2 + x_3)$. Using Lemma 1 along with formula (4) we obtained the imbalance $\varepsilon = \frac{800257}{33875260545}$. For a randomly selected initialization of the keystream generator, we counted the number of zeros among the first n keystream bits for $n = 2^{30}$, 2^{31}, 2^{32}, 2^{33}, and 2^{34}. We then compared these numbers with the theoretically expected number of zeros given by np, where $p = \frac{1}{2}(1+\varepsilon)$. The differences between the true number of zeros and the theoretically expected number of zeros was -70, $+6$, $+111$, $+259$, and $+173$.

We shall now present another way to determine the imbalances of the keystreams produced by Achterbahn-128 and Achterbahn-80. The idea in this alternative approach is to count the number of zeros produced by the keystream generator if the internal state of the keystream generator runs through all admissible internal states.

Theorem 2. *The average imbalance ε_{80} of the keystreams of Achterbahn-80 is*

$$\varepsilon_{80} = -1 + 2\sum_{i=1}^{1024}\prod_{j=1}^{11}\frac{2^{20+j}+a_{ij}-1}{2^{21+j}-1} \simeq -2^{-185.94},$$

where $A = \{\mathbf{a}_1, \ldots, \mathbf{a}_{1024}\} \subset \mathbb{Z}_2^{11}$ with $G(\mathbf{a_i}) = 0$ and $\mathbf{a_i} = (a_{i1}, a_{i2}, \ldots, a_{i\,11})$. The average imbalance ε_{128} of the keystreams of Achterbahn-128 is

$$\varepsilon_{128} = -1 + 2\sum_{i=1}^{4096}\prod_{j=0}^{12}\frac{2^{20+j}+b_{ij}-1}{2^{21+j}-1} \simeq -2^{-237.06},$$

where $B = \{\mathbf{b}_1, \ldots, \mathbf{b}_{4096}\} \subset \mathbb{Z}_2^{13}$ with $F(\mathbf{b_i}) = 0$ and $\mathbf{b_i} = (b_{i0}, b_{i1}, \ldots, b_{i\,12})$.

Proof. The full period of a primitive binary N-stage feedback shift register contains $2^{N-1}-1$ zeros and 2^{N-1} ones. Consider the combining function G of Achterbahn-80. Let $\mathbf{a} = (a_1, \ldots, a_{11}) \in \mathbb{Z}_2^{11}$ be an input vector to G with $G(\mathbf{a}) = 0$. If the keystream generator of Achterbahn-80 runs through all $u = \prod_{j=1}^{11}(2^{N_j}-1)$ admissible internal states, the input vector $\mathbf{a} = (a_1, \ldots, a_{11})$ is produced exactly $\prod_{j=1}^{11}(2^{N_j-1}+a_j-1)$ times. Let Z_k be a keystream bit. Then

$$\Pr(Z_k = 0) = \frac{1}{u}\sum_{i=1}^{1024}\prod_{j=1}^{11}(2^{N_j-1}+a_{ij}-1) = \sum_{i=1}^{1024}\prod_{j=1}^{11}\frac{2^{20+j}+a_{ij}-1}{2^{21+j}-1}.$$

For Achterbahn-128 the assertion in proved in the same way. □

4 Analysis

Let $G(\mathbf{x})$, $\mathbf{x} = (x_1, \ldots, x_{11})$, be the Boolean combining function of Achterbahn-80, and consider its quadratic approximation

$$Q(\mathbf{x}) = x_1 + x_3 + x_5 + x_4x_{10} + x_6x_7. \tag{5}$$

We have $\Pr(G = Q) = 31/64 = \frac{1}{2}(1+\varepsilon)$, where the correlation coefficient $\varepsilon = -2^{-5}$. The polynomial

$$g(x) = (x^{p_4p_{10}}-1)(x^{p_6p_7}-1) \tag{6}$$

is a characteristic polynomial of $\sigma = \sigma_4\sigma_{10} + \sigma_6\sigma_7$, so that $g(T)\sigma = \mathbf{0}$, the zero sequence. Here $T : \mathbb{Z}_2^\infty \to \mathbb{Z}_2^\infty$ denotes the shift operator defined by $T(c_i)_{i=0}^\infty = (c_{i+1})_{i=0}^\infty$ for all binary sequences $(c_i)_{i=0}^\infty$.

Since for an arbitrary input vector $\mathbf{x} \in \mathbb{Z}_2^{11}$, the function values $G(\mathbf{x})$ and $Q(\mathbf{x})$ agree with probability 31/64, it is reasonable to assume that an arbitrary term z_i of the keystream $\zeta = (z_i)_{i=0}^\infty$ agrees with the ith term of the sequence $\sigma_1 + \sigma_3 + \sigma_5 + \sigma_4\sigma_{10} + \sigma_6\sigma_7$ with probability 31/64. For this we write

$$\zeta \overset{\varepsilon=-2^{-5}}{\approx} \sigma_1 + \sigma_3 + \sigma_5 + \sigma_4\sigma_{10} + \sigma_6\sigma_7 \tag{7}$$

since $31/64 = \frac{1}{2}(1 - 2^{-5})$. In other words, the terms of the sequence $\omega = \zeta + \sigma_1 + \sigma_3 + \sigma_5 + \sigma_4\sigma_{10} + \sigma_6\sigma_7$ are biased towards 1.

Applying the linear operator $g(T)$ to this sequence yields the sequence

$$g(T)\omega = g(T)\zeta + g(T)\sigma_1 + g(T)\sigma_3 + g(T)\sigma_5. \tag{8}$$

Since the polynomial $g(x)$ has four terms, the application of $g(T)$ to the sequence ω means that we add together termwise four sequences: the original sequence ω and three shifted versions of ω. It was assumed in [6], [4] that the terms of the sequence $g(T)\omega$ are biased towards 0 with imbalance $\varepsilon' = \varepsilon^4 = 2^{-20}$. Recently, Hell and Johansson [5] found a more accurate value for the imbalance by evaluating the truth table of a 36-variable Boolean function derived from the Boolean combining function G of Achterbahn-80. (The paper says that a Boolean function of 32 variables has been examined to determine the correct value of the imbalance. But that must be a typographical error.) They found that the actual imbalance is 256 times greater than the previously assumed value, namely 2^{-12} rather than 2^{-20}. It is save to conjecture that this observation made their day.

Naya-Plasencia [8] grounds her cryptanalysis of Achterbahn-80 (and Achterbahn-128) on linear approximations. She used the linear approximation

$$L(\mathbf{x}) = x_1 + x_3 + x_4 + x_5 + x_6 + x_7 + x_{10}.$$

We have $\Pr(G = L) = 7/16 = \frac{1}{2}(1 - \frac{1}{8})$. The functions G and L are stronger correlated than the functions G and Q. This is not just a coincidence. Canteaut and Trabbia [1] proved that the best approximation (i.e., an approximation maximizing the absolute value of the correlation coefficient) to a given m-resilient Boolean function by an $m+1$-variable Boolean function is always an affine function. We have

$$\zeta \overset{\varepsilon=-2^{-3}}{\approx} \sigma_1 + \sigma_3 + \sigma_4 + \sigma_5 + \sigma_6 + \sigma_7 + \sigma_{10}. \tag{9}$$

Comparing the approximations in (7) and (9) with each other, it seems that (9) has the advantage of having a larger correlation coefficient (in absolute value) while (7) has the advantage of being shorter. The simple but far reaching idea of Naya-Plasencia was to interpret approximation (9) as the sum of five (rather than seven) sequences making it equally short: [1]

$$\zeta \overset{\varepsilon=-2^{-3}}{\approx} \sigma_1 + \sigma_3 + \sigma_5 + (\sigma_4 + \sigma_{10}) + (\sigma_6 + \sigma_7). \tag{10}$$

[1] In reality, Naya-Plasencia used the approximation $\zeta \approx \sigma_1 + \sigma_3 + \sigma_{10} + (\sigma_4 + \sigma_7) + (\sigma_5 + \sigma_6)$. We use approximation (10) in our discussion because it compares better to (7).

The sequence $\tau_1 = \sigma_4 + \sigma_{10}$ has $p_4 p_{10}$ as a period, and $\tau_2 = \sigma_6 + \sigma_7$ has $p_6 p_7$ as a period. (In both cases these are actually the least periods.) Therefore, the polynomial $g(x)$ in (6) is also a characteristic polynomial of $\tau = (\sigma_4 + \sigma_{10}) + (\sigma_6 + \sigma_7)$. Applying the linear operator $g(T)$ to both sides in (10) yields

$$g(T)\zeta \overset{\varepsilon'=2^{-12}}{\approx} g(T)\sigma_1 + g(T)\sigma_3 + g(T)\sigma_5.$$

Applying the "imbalance-multiplication-rule", Naya-Plasencia finds for the imbalance $\varepsilon' = (-2^{-3})^4 = 2^{-12}$. The same value as has been found in [5] with the help of a computer. Since in both approaches the same linear operator $g(T)$ is used, the keystream is processed in the same way. Thus the two attacks described in [8] and [5] against Achterbahn-80 are equivalent.

5 An abstract model of the keystream generator

We have seen in the preceding section that the method introduced in [6] can lead to incorrect values for the imbalance. We shall now investigate under which circumstances this can happen. Instead of dealing with the actual keystream generator, we work in a simplified model. The aim of the model is that we can draw precise conclusions and provide rigorous proofs within the model. In Section 8 we shall compare the conclusions derived from the model with a real keystream generator consisting of six primitive shift registers of lengths between 15 and 20.

Let $F(x_1, \ldots, x_n)$ be an m-resilient Boolean function of n variables. For $j = 1, \ldots, n$ let $\mathbf{X}_j$ be a periodic sequence of symmetrically distributed binary-valued random variables of period p_j:

$$\mathbf{X}_j = (X_{ji})_{i=0}^{\infty} = (X_{j,0}, X_{j,1}, \ldots, X_{j,p_j-1})^{\infty}.$$

The random variables within one period are assumed to be statistically independent. The random variables belonging to different sequences are also assumed to be statistically independent. The Boolean function F and the sequences $\mathbf{X}_j$, $1 \leq j \leq n$, define a sequence $\mathbf{Z} = (Z_i)_{i=0}^{\infty}$ of new random variables by

$$Z_i = F(X_{1,i}, X_{2,i}, \ldots, X_{n,i}), \qquad i = 0, 1, \ldots .$$

Let L be a linear approximation of F containing exactly $m+1$ different variables. W.l.o.g., assume that

$$L(\mathbf{x}) = x_1 + x_2 + \cdots + x_{m+1}. \tag{11}$$

Let ε be the correlation coefficient of L and F, that is $\Pr(F = L) = \frac{1}{2}(1 + \varepsilon)$. Consider the polynomial

$$g(x) = \prod_{k=1}^{m+1} (x^{p_k} - 1) = \sum_{d \in D} x^d.$$

The set of exponents $D = \{0, p_1, p_2, \ldots, p_1 + \cdots + p_{m+1}\}$ has cardinality 2^{m+1}.

Applying the linear operator $g(T)$ to the sequence $\mathbf{Z} = (Z_i)_{i=0}^{\infty}$ yields a sequence $\mathbf{Y} = (Y_i)_{i=0}^{\infty} = g(T)\mathbf{Z}$ whose terms are given by $Y_i = \sum_{d \in D} Z_{i+d}$ for $i = 0, 1, \ldots$. Since the Y_i are identically distributed it suffices to consider

$$Y := Y_0 = \sum_{d \in D} Z_d.$$

We wish to determine the imbalance of Y. To this end we consider 2^{m+1} auxiliary random variables W_d, $d \in D$. We set $q = p_1 + \cdots + p_{m+1}$ and $q_i = q - p_i$ for $1 \leq i \leq m+1$. Then

$$\begin{aligned}
W_0 &= F(X_{1,0},\, X_{2,0},\, X_{3,0},\, \ldots,\, X_{n,0}) \;+\; X_{1,0} + X_{2,0} \;+\; \cdots + X_{m+1,0};\\
W_{p_1} &= F(X_{1,0}, X_{2,p_1}, X_{3,p_1}, \ldots, X_{n,p_1}) + X_{1,0} + X_{2,p_1} + \cdots + X_{m+1,p_1};\\
W_{p_2} &= F(X_{1,p_2}, X_{2,0}, X_{3,p_2}, \ldots, X_{n,p_2}) + X_{1,p_2} + X_{2,0} + \cdots + X_{m+1,p_2};\\
&\;\;\vdots\\
W_q &= F(X_{1,q_1}, X_{2,q_2}, X_{3,q_3}, \ldots, X_{n,q}) + X_{1,q_1} + X_{2,q_2} + \cdots + X_{m+1,q_{m+1}}.
\end{aligned}$$

We have

(i) $\sum_{d \in D} W_d = \sum_{d \in D} Z_d = Y$;

(ii) $\Pr(W_d = 0) = \frac{1}{2}(1 + \varepsilon)$ for $d \in D$.

Furthermore, it can be shown that the random variables W_d, $d \in D$, are statistically independent (which is the nontrivial part of the proof). Therefore, we can apply the piling-up lemma and obtain

$$\Pr(Y = 0) = \frac{1}{2}\left(1 + \varepsilon^{2^{m+1}}\right).$$

The total number of independent random variables X_{ji} appearing in the above system of equations is given by $f'(1)$, where

$$f(x) = x^{n-m-1}(x+1)^{m+1}.$$

For instance, for $n = 8$ and $m = 4$, the system contains 176 independent random variables.

For lack of space we shall not give the complete proof for the fact that the random variables W_d, $d \in D$, are statistically independent. We mention, however, the lemma that plays a crucial role in the proof.

Lemma 2. *Let F be an m-resilient Boolean function of n variables. For $1 \leq k \leq m+1$ and $1 \leq j_1 < \cdots < j_k \leq n$, consider the Boolean function $G(x_1, \ldots, x_n) = F(x_1, \ldots, x_n) + x_{j_1} + \cdots + x_{j_k}$. Then*

$$\Pr(G = 0 | X_{j_1} = e_1, \ldots, X_{j_k} = e_k) = \Pr(G = 0)$$

for all $(e_{j_1}, \ldots, e_{j_k}) \in \mathbb{Z}_2^k$.

The assertion in the lemma does not hold if the sum $x_{j_1} + \cdots + x_{j_k}$ contains more than $m+1$ terms or if the sum is replaced by any non-affine expression like a quadratic or cubic Boolean function of $m+1$ or more variables. This is the reason why the "imbalance-multiplication-rule" yields wrong results in such cases.

In the abstract keystream generator model, Naya-Plasencia's generalization of the heuristic correlation attack of Johansson, Meier, and Muller [6] can also be justified. Her generalization reads:

Reconsider the linear approximation (11). Decompose the set $\{1, 2, \ldots, m+1\}$ into t mutually disjoint subsets $\{S_1, \ldots, S_t\}$, where $1 \leq t \leq m+1$. (For $t = m+1$ one obtains the original algorithm introduced in [6].) For $j = 1, \ldots, t$, let q_j be the least common multiple of all periods p_i with $i \in S_j$. Consider the polynomial

$$h(x) = \prod_{j=1}^{t} (x^{q_j} - 1).$$

Then, in the abstract keystream generator model, the terms Y_i of the sequence $\mathbf{Y} = h(T)\mathbf{Z}$ satisfy

$$\Pr(Y_i = 0) = \frac{1}{2}\left(1 + \varepsilon^{2^t}\right) \qquad \text{for } i = 0, 1, \ldots .$$

6 Analysis of the guess and determine attack

Let us continue the discussion of the cryptanalysis of Achterbahn-80. Reconsider

$$g(T)\zeta \overset{\varepsilon'=2^{-12}}{\approx} g(T)\sigma_1 + g(T)\sigma_3 + g(T)\sigma_5. \tag{12}$$

If the abstract model in the preceding section is a good approximation of the keystream generator of Achterbahn-80, then the imbalance ε' should indeed be close to 2^{-12}.

For $r \geq 1$, the decimation operator D_r defined by $D_r\sigma = (s_0, s_r, s_{2r}, \ldots)$ for all binary sequences $\sigma = (s_i)_{i=0}^{\infty}$ is a linear operator on $\mathbb{Z}_2^{\infty}$. Set $D = D_{p_5}$, where p_5 is the least period of the sequence σ_5. Clearly, $D\sigma_5$ is a constant sequence, and so is $Dg(T)\sigma_5$. Applying D to both sides of (12) yields

$$Dg(T)\zeta \overset{\varepsilon'=2^{-12}}{\approx} Dg(T)\sigma_1 + Dg(T)\sigma_3 + \text{const.} \tag{13}$$

The application of the decimation operator was introduced in [4]. (Notice that the stream cipher concept investigated in [4] was not an eSTREAM submission, as claimed by the authors of [4].) Next the sequences σ_1 and σ_3 are determined. That is, the initial states of the shift registers A_1 and A_3 are (systematically) guessed. Write (13) in the equivalent form

$$Dg(T)[\zeta + \sigma_1 + \sigma_3] \overset{\varepsilon'=2^{-12}}{\approx} \text{const.}$$

For the correct initial states the sequence $\zeta + \sigma_1 + \sigma_3$ has imbalance $\varepsilon = \pm 2^{-12}$. For all other initial states the sequence $\zeta + \sigma_1 + \sigma_3$ should be roughly balanced.

It was assumed by Naya-Plasencia [8] that $1/\varepsilon'^2 = 2^{24}$ keystream bits are sufficient to determine the correct initial states. In reality, about 2^{30} keystream bits are needed. (The same error was made by Johansson, Meier, and Muller in [6] and by Hell and Johansson in [4]. As a consequence in all cases the claimed complexities for the attacks are underestimated.)

Suppose we are given a collection of 2^N sequences of independent identically distributed Bernoulli random variables. The terms X_i of one sequence have imbalance $\varepsilon \neq 0$. The terms of all other sequences are balanced. Then a statistical analysis will show that one needs to observe about $(N \ln 4)/\varepsilon^2$ terms in order to identify the biased sequence.

7 The coin tossing model

A sequence of independent identically distributed Bernoulli random variables can be seen as the mathematical description of a sequence of coin tosses. Assume that we are given M fair coins $C_1, \ldots, C_M$, and one biased coin C_0. Identify 'head' with 0 and 'tail' with 1. Then, $\Pr(C_j \text{ falls } 0) = 1/2$ for $1 \leq j \leq M$, and $\Pr(C_0 \text{ falls } 0) = p \neq 1/2$. Let us assume that $p > 1/2$. (The case $p < 1/2$ is treated similarly.)

The coin tossing model is a simplification of the situation described in the preceding section: The coin C_0 corresponds to the correct initial state of the shift register. The fair coins $C_1, \ldots, C_M$ correspond to wrong initial states.

Each coin C_t, $0 \leq t \leq M$, is flipped n times. Let l_t be the number of times coin C_t falls 0. Based on the value of l_t, a decision is made, whether the coin should be regarded as fair or as biased. In the latter case the probability $p = \Pr(C_t \text{ falls } 0) > 1/2$ is known. In the sequel, we set $q = 1 - p$ and use $\log(x)$ to denote the base-2 logarithm of $x > 0$. The best strategy makes use of the following decision rule:

$$\text{If } l_t \geq \lambda_n, \text{ decide that } C_t \text{ is biased.}$$
$$\text{If } l_t < \lambda_n, \text{ decide that } C_t \text{ is fair.}$$

The number $\lambda_n \in \{0, 1, \ldots, n\}$ is given by

$$\lambda_n = \begin{cases} \lfloor pn \rfloor & \text{for } n \leq n_0; \\ \left\lceil \frac{\log M - n(1+\log q)}{\log p - \log q} \right\rceil & \text{for } n > n_0. \end{cases}$$

The number n_0 is determined by

$$n_0 = \left\lceil \frac{\log M}{1 + p \log p + q \log q} \right\rceil. \tag{14}$$

The probability that the biased coin C_0 is misjudged as a fair coin is

$$\alpha_n = \Pr(l_0 < \lambda_n) = \sum_{k=0}^{\lambda_n - 1} \binom{n}{k} p^k q^{n-k}.$$

The probability that a fair coin C_t, $1 \leq t \leq M$, is (erroneously) interpreted as the biased coin is

$$\beta_n = \Pr(l_t \geq \lambda_n) = \sum_{k=\lambda_n}^{n} \binom{n}{k} 2^{-n}.$$

The expected number of fair coins that will be misjudged as biased (the number of false alarms) is

$$\gamma_n = M\beta_n = M2^{-n} \sum_{k=\lambda_n}^{n} \binom{n}{k}.$$

The probability that no fair coin in misjudged as biased is $\delta_n = (1 - \beta_n)^M$. The decision rule has the following properties:

1. The probability to identify the biased coin is $> 1/2$.

2. For $n > n_0$, we have $\gamma_n < 1/2$.

Remark. (i) If n is close to n_0, then α_n is close to $1/2$ and the cryptanalyst should be able to successfully identify the correct initial state of the target shift register on the average at the second try. (ii) If n is close to $1/\varepsilon^2$, there will be about $0.1587M$ false alarms.

Furthermore, we mention that

$$\frac{1}{1 + p\log p + q \log q} \rightarrow \frac{2\ln 2}{\varepsilon^2}$$

as p approaches $1/2$. This explains the claim made at the end of Section 6.

8 A simulation of the guess and determine attack

We have to check the validity of the above derived results in a practical attack. Along the way several idealizations (or simplifications) were made. The results obtained in the coin tossing model apply to sequences which are realizations of independent and identically distributed Bernoulli random variables. But the sequences in question are pseudorandom sequences with strong dependencies among their terms. Furthermore, the validity of the "imbalance-multiplication-rule" can be rigorously proved only within the abstract keystream generator model. It is not a priori clear whether the rule yields reliable results for the analysis of a true keystream generator.

To shed some light on these issues, we ran an actual guess and determine attack on a primitive NLFSR combination generator that consists of six shift registers $B_1, \ldots, B_6$. The lengths of the shift registers are 15, 16, 17, 18, 19, and 20, respectively. The feedback functions of the shift registers and the initial states used in the simulation can be found in Appendix A. The Boolean combining function is given by

$$\begin{aligned} S(x_1, \ldots, x_6) = {} & x_1x_2 + x_1x_3 + x_1x_4 + x_1x_5 + x_1x_6 + x_2x_3 + x_2x_4 + x_2x_5 + x_2x_6 \\ & + x_3x_4 + x_3x_5 + x_3x_6 + x_4x_5 + x_4x_6 + x_5x_6 + x_1x_2x_5 + x_1x_2x_6 + x_1x_3x_4 \\ & + x_1x_3x_6 + x_1x_4x_5 + x_2x_3x_4 + x_2x_3x_5 + x_2x_4x_6 + x_3x_5x_6 + x_4x_5x_6. \end{aligned}$$

The Boolean function S is balanced, has order of correlation immunity 2 and nonlinearity 24.

We approximate S by $L = x_1 + x_2 + x_3$. We have $\Pr(S = L) = \frac{1}{2}(1 + \frac{1}{4})$. Let $r_2 = 2^{16} - 1$ and $r_3 = 2^{17} - 1$ the least periods of the output sequences of the shift registers B_2 and B_3. Apply $g(T) = (T^{r_2} - 1)(T^{r_3} - 1)$ to

$$\zeta \overset{\varepsilon=1/4}{\approx} \sigma_1 + \sigma_2 + \sigma_3.$$

Then, by the "imbalance-multiplication-rule",

$$g(T)[\zeta + \sigma_1] \overset{\varepsilon=1/256}{\approx} \mathbf{0}.$$

Thus, $\varepsilon = 1/256$ and $p = \frac{1}{2}(1 + \varepsilon) = 257/512 \simeq 0.50195$.

We generated for all $2^{15} - 1$ nonzero initial states of the shift register B_1 the sequence σ_1 corresponding to one such initial state. Then, for $2^{16} \leq n \leq 2^{22}$, and for all $2^{15} - 1$ sequences

σ_1, we counted the number of zeros within the first n terms of the sequence $g(T)[\zeta+\sigma_1]$. The ratio of the number of counted zeros to the number n of considered bits has been plotted in Figure 1. In this manner each initial state creates a curve. The curves corresponding to five (randomly selected) initial states are depicted in Figure 1, as well as the curve corresponding to the correct initial state.

The curves that correspond to the $2^{15}-2$ wrong initial states lie all within the colored envelope. We observe that the curve corresponding to the correct initial state leaves the envelope at about $n = 2^{20.5} \simeq 1.5N/\varepsilon^2$, where $N = 15$ is the length of the target shift register B_1. From the coin tossing model, we would expect that the correct initial state can be determined by investigating a number of n keystream bits close to n_0 (with $n > n_0$). In fact, we have

$$n_0 \simeq \frac{N \ln 4}{\varepsilon^2} \simeq \frac{1.4N}{\varepsilon^2}.$$

Next, for $n = 1/\varepsilon^2 = 2^{16}$, we counted the number of initial states of the shift register B_1 whose graphs lie above the horizontal line $y = p$. We found that 5203 initial states fulfilled that criterion, while the correct initial state lies below the line $y = p$. In other words, in the guess and determine attack one gets 5203 false alarms if only $n = 1/\varepsilon^2$ keystream bits are processed.

The theoretically expected number of false alarms is $0.1587M = 5200$, where $M = 2^{15}-2$. Thus the simulation confirms that the widely used "$1/\varepsilon^2$ rule of thumb" is inadequate in a guess and determine attack. Furthermore, the above results show that the theoretical models yield reliable results despite the imposed simplifications.

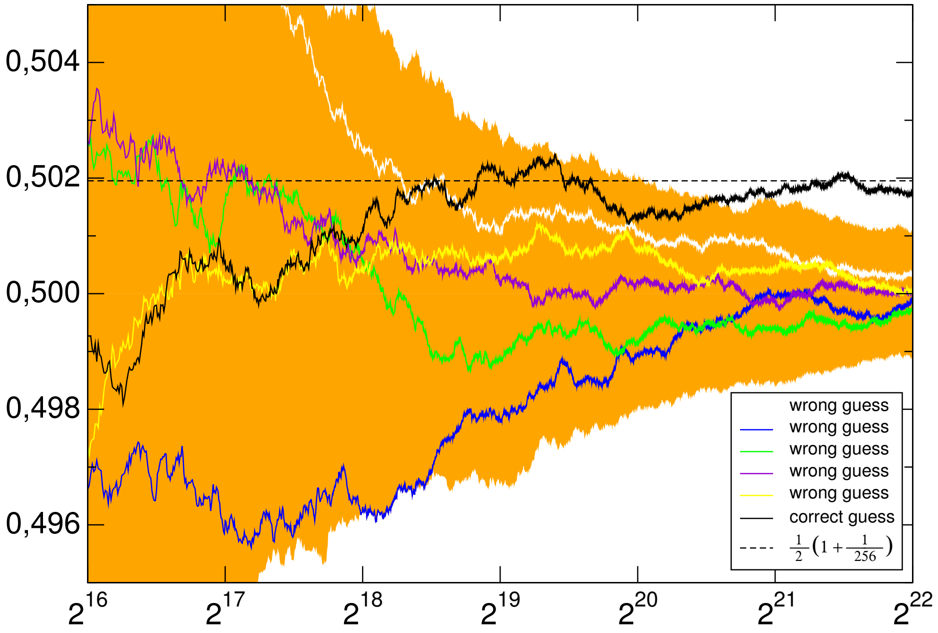

Fig. 1. Simulation of a guess and determine attack

References

1. A. Canteaut and M. Trabbia: Improved fast correlation attacks using parity-check equations of weight 4 and 5. In B. Preneel (Ed.): *EUROCRYPT 2000*, LNCS 1807, pp. 573–588, Springer-Verlag, Berlin-Heidelberg, 2000.
2. B. M. Gammel, R. Göttfert, and O. Kniffler: Achterbahn-128/80, eSTREAM, ECRYPT Stream Cipher Project, 2006, http://www.ecrypt.eu.org/stream/p2ciphers/achterbahn/achterbahn_p2.pdf.
3. C. Harpes, G. G. Kramer, and J. L. Massey: A generalization of linear cryptanalysis and the applicability of Matsui's piling-up lemma, *Advances in Cryptology — EUROCRYPT '95* (C. Guillou and J.-J. Quisquater, eds.), Lecture Notes in Computer Science, vol. 921, pp. 24–38, Springer-Verlag, Berlin, 1995.
4. M. Hell and T. Johansson: Cryptanalysis of Achterbahn-Version 2, eSTREAM, ECRYPT Stream Cipher Project, report 2006/042, http://www.ecrypt.eu.org/stream.
5. M. Hell and T. Johansson: Cryptanalysis of Achterbahn-128/80, eSTREAM, ECRYPT Stream Cipher Project, report 2006/054, http://www.ecrypt.eu.org/stream.
6. T. Johansson, W. Meier, and F. Muller: Cryptanalysis of Achterbahn. In M.J.B. Robshaw (Ed.): *FSE 2006*, LNCS 4047, pp. 1–14, Springer-Verlag, Berlin-Heidelberg, 2006.
7. Z. Kukorelly: The piling-up lemma and dependent random variables. *IMA—Crypto & Coding '99* (M. Walker, ed.), Lecture Notes in Computer Science, vol. 1746, pp. 186–190, Springer-Verlag, Berlin, 1999.
8. M. N. Plasencia: Cryptanalysis of Achterbahn-128/80, eSTREAM, ECRYPT Stream Cipher Project, report 2006/055, http://www.ecrypt.eu.org/stream.

9 Appendix A

$$\begin{aligned}B_1(x_0,x_1,\ldots,x_{14}) = {} & x_0+x_3+x_4+x_{10}+x_{12}+x_{13}+x_9x_{14}+x_{10}x_{13}+x_{11}x_{12}+x_5x_8x_{11}+x_5x_{11}x_{12}\\ & +x_6x_9x_{12}+x_8x_{11}x_{12}+x_9x_{11}x_{12}+x_5x_6x_8x_9+x_5x_6x_9x_{12}+x_5x_8x_9x_{11}+x_5x_9x_{11}x_{12}\\ & +x_6x_8x_9x_{12}+x_8x_9x_{11}x_{12};\end{aligned}$$

Initial state of B_1: 010110001010001

$$\begin{aligned}B_2(x_0,x_1,\ldots,x_{15}) = {} & x_0+x_1+x_3+x_5+x_{12}+x_{10}x_{15}+x_2x_3x_9+x_3x_5x_9+x_2x_3x_{11}+x_3x_5x_{11}\\ & +x_2x_9x_{11}+x_5x_9x_{11}+x_2x_3x_6x_9+x_3x_4x_6x_9+x_2x_3x_6x_{11}+x_3x_4x_6x_{11}\\ & +x_2x_6x_9x_{11}+x_4x_6x_9x_{11};\end{aligned}$$

Initial state of B_2: 1011010100010001

$$\begin{aligned}B_3(x_0,x_1,\ldots,x_{16}) = {} & x_0+x_3+x_6+x_9+x_{15}+x_3x_4+x_4x_8+x_4x_9+x_7x_9+x_1x_3x_4+x_2x_4x_5\\ & +x_1x_3x_9+x_1x_4x_9+x_2x_3x_4x_5+x_2x_4x_5x_9+x_2x_3x_4x_5x_9;\end{aligned}$$

Initial state of B_3: 00110111110110011

$$\begin{aligned}B_4(x_0,x_1,\ldots,x_{17}) = {} & x_0+x_7+x_8+x_{14}+x_{17}+x_1x_9+x_2x_4+x_2x_8+x_3x_9+x_8x_9+x_2x_3x_9\\ & +x_2x_4x_{11}+x_2x_8x_9+x_2x_8x_{11}+x_4x_{11}x_{15}+x_8x_{11}x_{15}+x_2x_3x_9x_{11}+x_2x_8x_9x_{11}\\ & +x_3x_9x_{11}x_{15}+x_8x_9x_{11}x_{15};\end{aligned}$$

Initial state of B_4: 101101100101100110

$$\begin{aligned}B_5(x_0,x_1,\ldots,x_{18}) = {} & x_0+x_2+x_3+x_5+x_8+x_{12}+x_1x_6+x_2x_6+x_2x_9+x_4x_7+x_5x_6+x_9x_{10}\\ & +x_9x_{11}+x_2x_4x_6+x_2x_4x_{10}+x_2x_6x_9+x_4x_9x_{10}+x_6x_9x_{10}+x_9x_{10}x_{11}+x_2x_4x_6x_9\\ & +x_2x_4x_9x_{10}+x_4x_6x_9x_{10};\end{aligned}$$

Initial state of B_5: 1001101010000001010

$$\begin{aligned}B_6(x_0,x_1,\ldots,x_{19}) = {} & x_0+x_1+x_3+x_5+x_{12}+x_{16}+x_{18}+x_{19}+x_1x_5+x_5x_8+x_6x_{10}+x_{11}x_{18}\\ & +x_4x_6x_{16}+x_4x_9x_{14}+x_6x_{15}x_{16}+x_1x_9x_{14}x_{17}.\end{aligned}$$

Initial state of B_6: 10010011011101101111

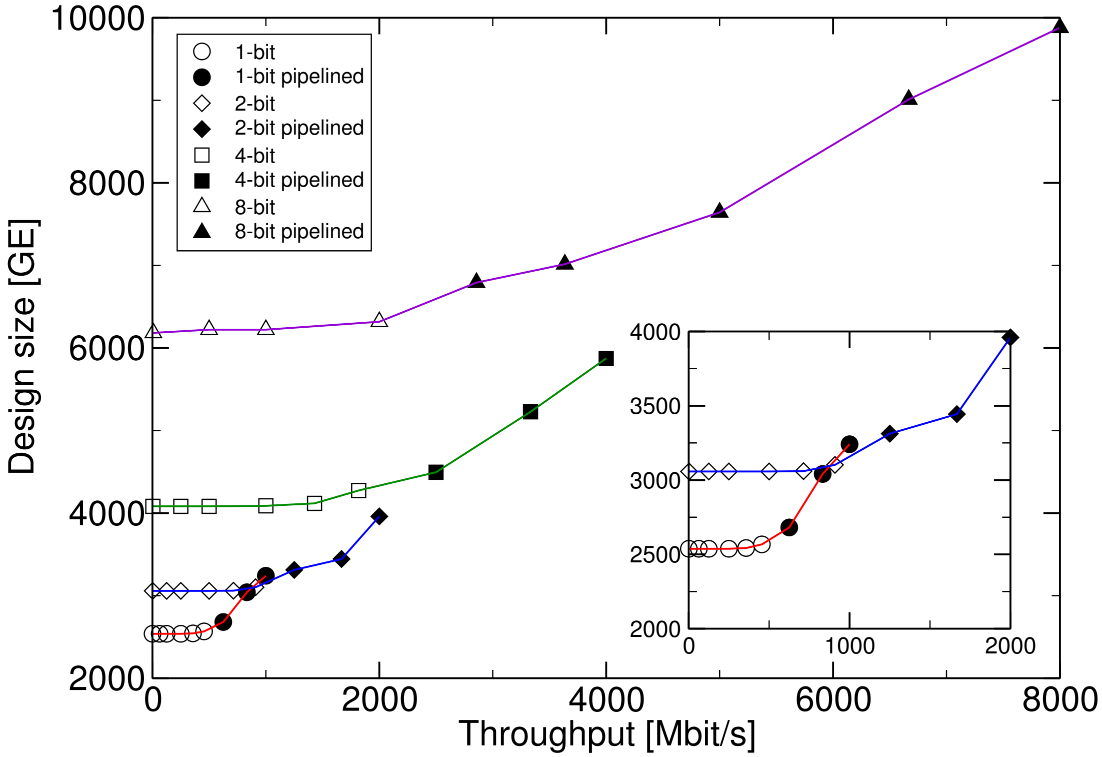

Fig. 2. Throughput versus design size for ACHTERBAHN-128/80 without SPA countermeasures