On the frame length of Achterbahn-128/80

Rainer Göttfert
Infineon Technologies AG
Am Campeon 1–12
D-85579 Neubiberg, Germany
rainer.goettfert@infineon.com

Berndt M. Gammel
Infineon Technologies AG
Am Campeon 1–12
D-85579 Neubiberg, Germany
berndt.gammel@infineon.com

Abstract— **In this paper we examine a correlation attack against combination generators introduced by Meier et al. in 2006 and extended to a more powerful tool by Naya-Plasencia. The method has been used in the cryptanalysis of the stream ciphers Achterbahn and Achterbahn-128/80. No mathematical proofs for the method were given. We show that rigorous proofs can be given in an appropriate model, and that the implications derived from that model are in accordance with experimental results obtained from a true combination generator. We generalize the new correlation attack and, using that generalization, show that the internal state of Achterbahn-128 can be recovered with complexity 2^{119} using $2^{48.54}$ consecutive keystream bits. In order to investigate a lower bound for the frame length of Achterbahn-128 we consider another application of the generalized correlation attack. This attack has complexity 2^{136} (higher than brute force) and requires $2^{44.99}$ keystream bits. Similar results hold for Achterbahn-80. Due to these findings our new recommendation for the frame length of Achterbahn-128 and Achterbahn-80 is 2^{44} bits.**

I. Introduction

Consider a keystream generator (KSG) that consists of n devices producing binary periodic sequences and a Boolean combining function which combines these sequences to generate the keystream. If the input sequences have relatively short periods—in comparison to the keystream—then a certain correlation attack comes into play. This heuristic correlation attack was introduced by Johansson, Meier, and Muller [4] and later on generalized by Naya-Plasencia [5]. The method is in the spirit of linear cryptanalysis. No proof has been given for the method. We shall generalize this correlation attack and present a rigorous proof for the attack in a simplified model.

We give a brief description of the correlation attack as introduced in [4]. Let $F(x_1, \dots, x_n)$ be a balanced Boolean combining function that is correlation immune of order 4, say. Let $L = x_1 + x_2 + x_3 + x_4 + x_5$ be a linear approximation to F, so that $\Pr(F = L) = \frac{1}{2}(1 + \epsilon)$ with a nonzero correlation coefficient ϵ. Let $\sigma_1, \dots, \sigma_n$ be the input sequences to F and let $\zeta = (z_i)_{i=0}^{\infty}$ be the keystream. Since F and L are correlated, the sequences ζ and $\sigma = \sigma_1 + \sigma_2 + \sigma_3 + \sigma_4 + \sigma_5$ are correlated. Let p_j be the least period of σ_j, $1 \le j \le 5$, and let $T : (b_i)_{i=0}^{\infty} \to (b_{i+1})_{i=0}^{\infty}$ be the shift operator, defined on the vector space of all binary sequences under termwise operations on sequences. The polynomial $g(x) = \prod_{j=1}^{5}(x^{p_j} - 1)$ is a characteristic polynomial of σ, so that $g(T)\sigma = \mathbf{0}$. Since the polynomial $g(x)$ has 32 terms, $g(T)[\zeta + \sigma] = g(T)\zeta$ is the termwise sum of 32 sequences. It has been assumed in the heuristic method that the sequence $g(T)\zeta$ reflects the probability distribution $\Pr(Y = 0) = \frac{1}{2}(1 + \epsilon^{32})$.

II. The Simplified Keystream Generator Model

Instead of working with a true combination generator in which the sequences to be combined are, e.g., shift register sequences, we shall work in a simplified model. In this model the input sequences to the Boolean combiner are replaced by periodic sequences of binary-valued random variables which are assumed to be independent and symmetrically distributed.

We shall use the following notation. If M is a set, then $|M|$ denotes the cardinality of M. If D is a subset of the set of integers $\mathbb{Z}$ and n is a nonnegative integer, then $D_{\operatorname{mod} n}$ is the corresponding subset of $\mathbb{Z}/n\mathbb{Z}$ consisting of the elements of D reduced modulo n.

Theorem 1: Let F be a balanced Boolean function of $n \ge 1$ variables having order of correlation immunity c with $0 \le c \le n - 1$. Let $p_1, \dots, p_n$ be n distinct nonnegative integers. For each $k = 1, \dots, n$, let

$$\mathbf{X}_k = (X_{ki})_{i=0}^{\infty} = (X_{k,0}, X_{k,1}, \dots, X_{k,p_k-1})^{\infty} \qquad (1)$$

be a periodic sequence of binary-valued balanced random variables of least period p_k such that the random variables X_{ki}, $1 \le k \le n$, $0 \le i \le p_k - 1$, are statistically independent. Let $\mathbf{Z} = (Z_i)_{i=0}^{\infty}$ be the sequence of binary-valued random variables defined by

$$Z_i = F(X_{1,i}, X_{2,i}, \dots, X_{n,i}) \quad \text{for } i = 0, 1, \dots .$$

Let

$$L = x_{i_1} + x_{i_2} + \cdots + x_{i_m} + a \qquad (2)$$

be an affine Boolean function of m variables, $1 \le m \le n$. Select an integer h with $1 \le h \le m$ and decompose the set $M = \{i_1, i_2, \dots, i_m\}$ into h mutually disjoint subsets $M_1, \dots, M_h$. Compute the least common multiples

$$q_j = \operatorname{lcm}(p_i : i \in M_j), \quad 1 \le j \le h.$$

Choose nonnegative integers $t_1, \dots, t_h$, and set $r_j = t_j q_j$ for $1 \le j \le h$. Consider the binary polynomial

$$g(x) = \prod_{j=1}^{h}(x^{r_j} - 1) = \sum_{d \in D} x^d.$$

The linear operator $g(T)$ and the sequence $\mathbf{Z} = (Z_i)_{i=0}^{\infty}$ define a new sequence $\mathbf{Y} = g(T)\mathbf{Z}$ with terms $Y_i = \sum_{d \in D} Z_{i+d}$.

If $m \le c+1$ and $|D_{\bmod p_j}| = 2^h$ for all $1 \le j \le n$ with $j \notin M$, then

$$\Pr(Y_i = 0) = \frac{1}{2}\big(1 + \epsilon^{2^h}\big) \qquad \text{for } i = 0, 1, \dots, \tag{3}$$

where ϵ is the correlation coefficient between F and L, that is, $\epsilon = 2\Pr(F = L) - 1$.

The special case $m = c+1$ and $t_j = 1$ for $1 \le j \le h$ corresponds to the method of Naya-Plasencia suggested in [5, page 5]. The special case $m = c+1$, $h = m$, and $t_j = 1$ for $1 \le j \le m$, corresponds to the method of Meier et al. described in [4, page 10].

Formula (3) need not hold if the stated assumptions in Theorem 1 are not fulfilled.

Example 1. The Boolean Function $F(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_2x_3$ is balanced and correlation immune of order $c = 0$. The linear function $L = x_1 + x_2$ is uncorrelated to F, that is $\epsilon = 0$. We have $m = 2$, so that the assumption $m \le c+1$ is not fulfilled. Let $g(x) = (x^{p_1} - 1)(x^{p_2} - 1)$ and $D = \{0, p_1, p_2, p_1 + p_2\}$. Assume that $|D_{\bmod p_3}| = 4$. One readily checks that the random variable Y_0 satisfies $\Pr(Y_0 = 0) = 9/16$. This result clearly contradicts formula (3).

Example 2. Let F be the Boolean function from Example 1. We use the linear approximation $L = x_1$. We have $\Pr(F = L) = 3/4$ so that $\epsilon = 1/2$. Assume that the periods p_1, p_2, p_3 are distinct with p_3 dividing p_1. Let $g(x) = x^{p_1} - 1$. Then $D = \{0, p_1\}$ and $D_{\bmod p_3} = \{0\}$, so that the second assumption in Theorem 1 is not fulfilled. In fact, we find for $Y_0 = F(X_{10}, X_{20}, X_{30}) + F(X_{10}, X_{2p_1}, X_{30})$ that $\Pr(Y_0 = 0) = 3/4$. This again contradicts formula (3).

For the proof of Theorem 1 we need some auxiliary results. The proof of the next lemma is straightforward and can be skipped.

Lemma 1: Let R_{ij}, $1 \le i \le k$, $1 \le j \le n$, be a collection of $k \times n$ statistically independent binary-valued random variables, and let F be an arbitrary Boolean function of n variables. Then the k random variables $S_1, \dots, S_k$ defined by

$$S_i = F(R_{i1}, R_{i2}, \dots, R_{in}) \qquad \text{for } 1 \le i \le k$$

are statistically independent.

Lemma 2: Let F be a balanced Boolean function of n variables. For $j \in \{1, \dots, n\}$, let $G_j(x_1, \dots, x_n) = F(x_1, \dots, x_n) + x_j$. Then

$$\Pr(G_j = e | x_j = 0) = \Pr(G_j = e | x_j = 1) = \Pr(G_j = e)$$

for $e \in \{0, 1\}$ and $1 \le j \le n$.

Proof: It suffices to treat the case $j = 1$. For ease of notation we write G instead of G_1. Let

$$\begin{aligned} U &= \{\mathbf{x} = (0, x_2, \dots, x_n) : x_2, \dots, x_n \in \{0,1\}\}, \\ V &= \{\mathbf{x} = (1, x_2, \dots, x_n) : x_2, \dots, x_n \in \{0,1\}\}. \end{aligned}$$

Consider the following subsets of U:

$$\begin{aligned} U_0 &= \{\mathbf{x} \in U : G(\mathbf{x}) = 0\} = \{\mathbf{x} \in U : F(\mathbf{x}) = 0\}, \\ U_1 &= \{\mathbf{x} \in U : G(\mathbf{x}) = 1\} = \{\mathbf{x} \in U : F(\mathbf{x}) = 1\}, \end{aligned}$$

and similar subsets of V:

$$\begin{aligned} V_0 &= \{\mathbf{x} \in V : G(\mathbf{x}) = 0\} = \{\mathbf{x} \in V : F(\mathbf{x}) = 1\}, \\ V_1 &= \{\mathbf{x} \in V : G(\mathbf{x}) = 1\} = \{\mathbf{x} \in V : F(\mathbf{x}) = 0\}. \end{aligned}$$

It suffices to show that $\Pr(G = 0 | x_1 = 0) = \Pr(G = 0 | x_1 = 1)$. Equivalently, that $|U_0| = |V_0|$. Since F is balanced,

$$|U_0| + |V_1| = 2^{n-1}.$$

We trivially have $|V_0| + |V_1| = |V| = 2^{n-1}$. Hence, $|U_0| = 2^{n-1} - |V_1| = 2^{n-1} - (2^{n-1} - |V_0|) = |V_0|$. ■

Lemma 3: Let the Boolean function $F(x_1, \dots, x_n)$ be balanced and correlation immune of order c. For $1 \le k \le c+1$ and $1 \le j_1 < \dots < j_k \le n$, consider the Boolean function $G(x_1, \dots, x_n) = F(x_1, \dots, x_n) + x_{j_1} + \dots + x_{j_k}$. Then

$$\Pr(G = e | x_{j_1} = e_1, \dots, x_{j_k} = e_k) = \Pr(G = e)$$

for all $e \in \{0, 1\}$ and $(e_{j_1}, \dots, e_{j_k}) \in \{0, 1\}^k$.

Proof: It suffices to proof the assertion for

$$G(x_1, \dots, x_n) = F(x_1, \dots, x_n) + x_1 + \dots + x_{c+1}.$$

Since F is balanced and correlation immune of order c, any subfunction of F obtained by replacing arbitrary c variables of F with arbitrary binary constants is balanced. It follows (compare the proof of Lemma 2) that

$$\begin{aligned} &\Pr(F = 0 | x_1 = e_1, \dots, x_{c+1} = e_{c+1}) \\ &\qquad = \begin{cases} a/b & \text{if } e_1 + \dots + e_{c+1} = 0 \\ (b-a)/b & \text{if } e_1 + \dots + e_{c+1} = 1 \end{cases} \end{aligned}$$

with $b = 2^{n-c-1}$, for some $a \in \{0, 1, \dots, b\}$, and for all $(e_1, \dots, e_{c+1}) \in \{0, 1\}^{c+1}$. It follows that

$$\Pr(G = 0 | x_1 = e_1, \dots, x_{c+1} = e_{c+1}) = a/b$$

for all $(e_1, \dots, e_{c+1}) \in \{0, 1\}^{c+1}$. ■

We are now ready for the proof of Theorem 1.

Proof: All random variables of the sequence $(Y_i)_{i=0}^{\infty} = g(T)(Z_i)_{i=0}^{\infty}$ have the same probability distribution. It therefore suffices to examine one of those random variables, say Y_0. Let us denote Y_0 by Y. Thus, $Y = \sum_{d \in D} Z_d$.

The case $m = n$ is trivial. Because in this case the assumption $m \le c+1$ together with $c+1 \le n$ implies that F is affine. It follows that $\mathbf{Y}$ is the zero sequence. Since $\Pr(F = L)$ is either 1 or 0, the correlation coefficient ϵ is either 1 or -1. Formula (3) holds in both cases. We shall assume in the rest of the proof that $m < n$.

Without loss of generality we may assume that the function L in (2) is linear and has the form $L = x_1 + \dots + x_m$. Again, without loss of generality, we can assume that the decomposition of the set $M = \{1, \dots, m\}$ into h pairwise disjoint nonempty subsets $M_1, \dots, M_h$ is of the form

$$M_j = \{c_j, c_j + 1, \dots, n_j\}, \quad 1 \le j \le h,$$

with integers n_j satisfying $1 < n_1 < \dots < n_h = m$, and integers c_j defined by $c_1 = 1$ and $c_j = n_{j-1} + 1$ for $2 \le j \le h$.

Because of the periodicity properties, the random variables Z_d, $d \in D$, have the form

$$\begin{aligned}
Z_0 &= F(X_{1,0}, \dots, X_{n_1,0}, \dots, X_{c_h,0}, \dots, X_{m,0}, \dots, X_{n,0}),\\
Z_{r_1} &= F(X_{1,0}, \dots, X_{n_1,0}, \dots, X_{c_h,r_1}, \dots, X_{m,r_1}, \dots, X_{n,r_1}),\\
&\vdots\\
Z_{r_h} &= F(X_{1,r_h}, \dots, X_{n_1,r_h}, \dots, X_{c_h,0}, \dots, X_{m,0}, \dots, X_{n,r_h}),\\
&\vdots\\
Z_s &= F(X_{1,s_1}, \dots, X_{n_1,s_1}, \dots, X_{c_h,s_h}, \dots, X_{m,s_h}, \dots, X_{n,s}),
\end{aligned}$$

where $s = r_1 + \dots + r_h$ and $s_j = s - r_j$ for $1 \le j \le h$.

Notice that each random variable X_{kd}, $1 \le k \le m$, $d \in D$, appears exactly twice in the above system of equations, whereas each random variable X_{kd}, with $m+1 \le k \le n$, $d \in D$, appears exactly once. It follows that Y depends on

$$\frac{m|D|}{2} + (n-m)|D| = (2n-m)2^{h-1}$$

independent symmetrically distributed random variables.

The random variables Z_d, $d \in D$, are not statistically independent. The idea of our proof is to alter the random variables Z_d in such a way that the modified random variables will be statistically independent. The modified random variables are:

$$\begin{aligned}
W_0 &= Z_0 + X_{1,0} + \dots + X_{n_1,0} + \dots + X_{c_h,0} + \dots + X_{m,0},\\
W_{r_1} &= Z_{r_1} + X_{1,0} + \dots + X_{n_1,0} + \dots + X_{c_h,r_1} + \dots + X_{m,r_1},\\
&\vdots\\
W_{r_h} &= Z_{r_h} + X_{1,r_h} + \dots + X_{n_1,r_h} + \dots + X_{c_h,0} + \dots + X_{m,0},\\
&\vdots\\
W_s &= Z_s + X_{1,s_1} + \dots + X_{n_1,s_1} + \dots + X_{c_h,s_h} + \dots + X_{m,s_h}.
\end{aligned}$$

We have

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

Furthermore,

$$\Pr(W_d = 0) = \Pr(F = L) = \frac{1}{2}\bigl(1 + \epsilon\bigr) \qquad \text{for all } d \in D.$$

Since the random variables W_d, $d \in D$, are statistically independent, the piling-up lemma can be applied to them. This yields

$$\Pr(Y = 0) = \frac{1}{2}\bigl(1 + \epsilon^{|D|}\bigr) = \frac{1}{2}\bigl(1 + \epsilon^{2^h}\bigr).$$

It remains to show that the random variables W_d are indeed statistically independent. That is, we have to verify that any nonempty subset $\{V_1, \dots, V_k\}$ of the set $\{W_d : d \in D\}$ satisfies

$$\Pr(V_1 = e_1, \dots, V_k = e_k) = \prod_{j=1}^{k} \Pr(V_j = e_j)$$

for all $(e_1, \dots, e_k) \in \{0,1\}^k$.

We shall carry out the details of the proof only for the largest such subset, i.e., for the set $\{W_d : d \in D\}$. The proofs for the other subsets are similar and somewhat simpler. For convenience, let us rename the elements of the set $\{W_d : d \in D\}$ by $W_1, W_2, \dots, W_t$ with $t = |D| = 2^h$. Let us denote the $u = m2^{h-1}$ random variables that appear twice in the above system of equations by $A_1, A_2, \dots, A_u$.

Using the formula for the *total probability*, we get

$$\Pr(W_1 = e_1, \dots, W_t = e_t) = \sum_{(a_1,\dots,a_u) \in \{0,1\}^u} \Pr(W_1 = e_1, \dots, W_t = e_t | A_1 = a_1, \dots, A_u = a_u) \frac{1}{2^u}.$$

By Lemma 1, the sum is equal to

$$\frac{1}{2^u} \sum_{(a_1,\dots,a_u) \in \{0,1\}^u} \prod_{i=1}^{t} \Pr(W_i = e_i \,| A_1 = a_1, \dots, A_u = a_u).$$

Each W_i depends only on m random variables of the set $\{A_1, \dots, A_u\}$. Therefore, Lemma 3 implies that

$$\Pr(W_i = e_i \,| A_1 = a_1, \dots, A_u = a_u) = \Pr(W_i = e_i)$$

for $1 \le i \le t$ and for all $(a_1, \dots, a_u) \in \{0,1\}^u$. It follows that

$$\begin{aligned}
&\Pr(W_1 = e_1, \dots, W_t = e_t)\\
&\qquad = \frac{1}{2^u} \sum_{(a_1,\dots,a_u) \in \{0,1\}^u} \prod_{i=1}^{t} \Pr(W_i = e_i)\\
&\qquad = \prod_{i=1}^{t} \Pr(W_i = e_i).
\end{aligned}$$

■

III. The Coin Tossing Model

In preparation for the subsequent sections we discuss a problem in the simplest of all probabilistic models, the coin tossing model.

Consider a collection of S coins. One coin is biased. All other coins are fair. Identify head with 0 and tail with 1. The biased coin falls head, i.e., shows 0, with probability $p > 1/2$. The value of p is known, but the coin that is biased is not. To distinguish the biased coin from the fair coins we toss each coin n times recording the number of observed zeros for each coin.

Theorem 2: Toss each of the S coins n_0 times where

$$n_0 = \left\lceil \frac{\log_2 S}{1 + p\log_2 p + (1-p)\log_2(1-p)} \right\rceil. \tag{4}$$

Then, the probability that the biased coin shows at least $\lfloor p\, n_0 \rfloor$ zeros is greater than $1/2$. The probability that each fair coin shows less than $\lfloor p\, n_0 \rfloor$ zeros is also greater than $1/2$.

We omit the proof. Problems of this kind are typically investigated in the framework of hypothesis testing. (Notice that the denominator of the above fraction is the relative entropy—or Kullback-Leibler distance—between a symmetrically distributed Bernoulli random variable and a Bernoulli random variable with parameter p.)

IV. Cryptanalysis of Achterbahn-128 using $2^{48.54}$ keystream bits

The KSG of Achterbahn-128 consists of 13 binary nonsingular nonlinear feedback shift registers A_k of lengths $N_k = k + 21$, $0 \le k \le 12$. The shift registers are *primitive*. This means that the shift register A_k will output a sequence $\sigma_k = (s_n^{(k)})_{n=0}^{\infty}$ of least period $p_k = 2^{N_k} - 1$ for every nonzero initial state. The produced sequences $\sigma_0, \ldots, \sigma_{12}$ are then combined by a balanced Boolean combining function $F(x_0, \ldots, x_{12})$ to produce the keystream $\zeta = (z_n)_{n=0}^{\infty}$. Thus,

$$z_n = F(s_n^{(0)}, \ldots, s_n^{(12)}) \qquad \text{for } n = 0, 1, \ldots .$$

Using a more compact notation, we also write $\zeta = F(\sigma_0, \ldots, \sigma_{12})$. The function F is correlation immune of order 8 and has nonlinearity 3584. See [2] for more information on this stream cipher.

The frame length of a stream cipher defines the maximum amount of keystream that can be used before resynchronization or re-keying becomes necessary. The initial frame length recommendation for Achterbahn-128 was 2^{64} bits (see [2, page 2]). However, Naya-Plasencia [5] found an attack with complexity 2^{80} that requires only $2^{60.26}$ keystream bits. In [6], she describes an attack of complexity 2^{104} requiring $2^{55.61}$ keystream bits. The following attack with complexity 2^{119} requires $2^{48.54}$ keystream bits.

We start our attack in the simplified KSG model. Recall that in this model the shift register sequences σ_k are replaced by the sequences $\mathbf{X}_k$ introduced in (1). The keystream ζ is replaced by $\mathbf{Z} = F(\mathbf{X}_0, \ldots, \mathbf{X}_{12})$. We use the linear approximation

$$L = x_0 + x_1 + x_2 + x_3 + x_4 + x_7 + x_9 + x_{10} + x_{12}.$$

Since F is balanced and correlation immune of order 8, the function $F' = F + x_4 + x_9 + x_{10}$ is balanced and correlation immune of order 5. Furthermore, the linear function

$$L' = x_0 + x_1 + x_2 + x_3 + x_7 + x_{12}$$

approximates F'. We have $\Pr(F' = L') = \Pr(F = L) = \frac{1}{2}(1 + \epsilon)$ with $\epsilon = 2^{-3}$. Define $q_1 = \operatorname{lcm}(p_0, p_7) \simeq 2^{42}$, $q_2 = \operatorname{lcm}(p_1, p_{12}) \simeq 2^{44}$, and $q_3 = \operatorname{lcm}(p_2, p_3) \simeq 2^{47}$. Consider the family of polynomials

$$g_{ij}(x) = (x^{iq_1} - 1)(x^{jq_2} - 1)(x^{q_3} - 1),$$

$1 \le i \le 38$, $1 \le j \le 10$. Let $D^{(ij)}$ be the set

$$\{0, iq_1, jq_2, q_3, iq_1 + jq_2, iq_1 + q_3, jq_2 + q_3, iq_1 + jq_2 + q_3\}.$$

Then $|D^{(ij)}_{\operatorname{mod} p_k}| = 8$ for $1 \le i \le 38$, $1 \le j \le 10$, and $k = 4, 5, 6, 8, 9, 10, 11$. Consider

$$\mathbf{Y} = g_{ij}(T)[\mathbf{Z} + T^a\mathbf{X}_4 + T^b\mathbf{X}_9 + T^c\mathbf{X}_{10}] \qquad (5)$$

with $0 \le a \le p_4 - 1$, $0 \le b \le p_9 - 1$, $0 \le c \le p_{10} - 1$.

If $a = b = c = 0$ (this corresponds to the correct guess), then $\mathbf{Y} = g_{ij}(T)\mathbf{Z}'$, where $\mathbf{Z}' = \mathbf{Z} + \mathbf{X}_4 + \mathbf{X}_9 + \mathbf{X}_{10} = F'(\mathbf{X}_0, \ldots, \mathbf{X}_{12})$. Applying Theorem 1 to F', L', and $\mathbf{Z}'$, we conclude that the terms of the sequence $\mathbf{Y} = (Y_n)_{n=0}^{\infty}$ are identically distributed with

$$\Pr(Y_n = 0) = p = \frac{1}{2}\left(1 + 2^{-24}\right) \qquad \text{for } n = 0, 1, \ldots .$$

For $a + b + c > 0$ (this corresponds to a wrong guess), the Y_n are balanced, that is $\Pr(Y_n = 0) = 1/2$. (This too can be rigorously proved in the simplified KSG model. However, we omit the proof for lack of space.)

We now change from the simplified KSG model to the true KSG. The equivalents of the sequences in (5) are

$$\eta = g_{ij}(T)[\zeta + \alpha + \beta + \gamma], \qquad (6)$$

where α, β, and γ are output sequences of the three target shift registers A_4, A_9, and A_{10}. It is a consequence of the key-loading algorithm of Achterbahn-128/80 that from the $2^{N_k} - 1$ nonzero output sequences of the shift register A_k only $2^{N_k - 1}$ are actually used (see Step 5 on page 21 in [2]). It follows that there are 2^{83} possibilities for the triple (α, β, γ). The sequences α, β, and γ can, of course, be represented by their initial states which are row vectors of lengths N_4, N_9, and N_{10}, respectively.

We impose another simplification. We treat the sequences η in (6) as if they were realizations of sequences of *independent* and identically distributed Bernoulli random variables. Notice that even in the simplified KSG model this is not true: The terms of the sequences $\mathbf{Y}$ in (5) are statistically dependent.

This simplification allows us to invoke Theorem 2. The correct triple $(\alpha, \beta, \gamma) = (\sigma_4, \sigma_9, \sigma_{10})$ corresponds to the biased coin. Wrong triples correspond to fair coins. Using formula (4) with $S = 2^{83}$ and $p = \frac{1}{2}(1 + 2^{-24})$, we get $n_0 = 32\,387\,195\,359\,857\,782 < 2^{54.847}$.

By applying all 380 linear operators $g_{ij}(T)$ to a segment of the sequence $\zeta + \alpha + \beta + \gamma$ consisting of $2^{48.54}$ bits, we gain

$$\sum_{i=1}^{38} \sum_{j=1}^{10} \left(2^{48.54} - \deg(g_{ij})\right) > 2^{54.847}$$

samples y_i. The triple (α, β, γ) producing the greatest number of zeros is the primary candidate for the correct initial states of the three registers A_4, A_9, A_{10}. Once we know the initial states of the three registers, the initial states of the remaining ten registers can be computed. This task is computationally less expensive.

V. Guessing the Initial States of Four Registers

In the above attack we guessed the initial states of three shift registers. Any attack against Achterbahn-128 that guesses more than three shift registers has complexity greater than 2^{128} and, therefore, does not make sense. Nonetheless, we consider such an "attack" to get an idea for a secure frame length recommendation. The complexity of the following "attack" is about 2^{136}. We use the linear approximation

$$L = x_0 + x_1 + x_3 + x_4 + x_5 + x_6 + x_7 + x_{10} + x_{12}.$$

The correlation coefficient between F and L is again $\epsilon = 1/8$. We guess the registers A_3, A_4, A_5, and A_6. There are 2^{98} possibilities for the initial states. Consider the polynomials

$$g_k(x) = (x^{q_1} - 1)(x^{q_2} - 1)(x^{kp_{10}} - 1)$$

for $1 \leq k \leq 10\,000$. Let $D^{(k)}$ be the corresponding set of exponents. Then $|D^{(k)}_{\bmod p_j}| = 8$ for all $1 \leq k \leq 10\,000$ with $k \neq 4098$ and for $j = 2, 3, 4, 5, 6, 8, 9, 11$, whereas $|D^{(4098)}_{\bmod p_{11}}| = 6$. Using (4) with $S = 2^{98}$ and $p = \frac{1}{2}(1+2^{-24})$, we obtain $n_0 < 2^{55.086}$. Let f be the minimum amount of keystream needed to collect $2^{55.086}$ samples using the linear operators $g_k(T)$. We make the Ansatz

$$2^{55.086} = \sum_{k=1}^{t+1}{}^{*} [f - \deg(g_k)],$$

where the asterisk indicates that the sum is extended only over values $k \neq 4098$. It follows that

$$2^{55.086} = [f - q_1 - q_2]\, t - p_{10} \left[\frac{(t+2)(t+1)}{2} - 4098 \right].$$

Equivalently,

$$f(t) = \frac{2^{55.086} - 4097 p_{10}}{t} + \frac{1}{2} p_{10} t + q_1 + q_2 + \frac{3}{2} p_{10}.$$

Solving $f'(t) = 0$ for t, we find as the nearest integer solution $t = 5967$. Since the second derivative is positive, f has a local minimum near $t = 5967$. Therefore, the best strategy is to use the 5967 linear operators $g_k(T)$, $1 \leq k \leq 5968$ with $k \neq 4098$ on a keystream segment of length $f(5967) \simeq 2^{44.99}$.

VI. Theory Versus Experiment

We need to check whether we are still in touch with reality. We want to know whether the results derived from the simplified KSG model and the coin tossing model are in accordance with experimental results obtained from a true KSG. To this end we consider a combination generator similar to the KSG of Achterbahn but with smaller design parameters so that a guess and determine attack can be simulated on the computer. This KSG consists of eight primitive nonlinear shift registers of lengths $N_j = j + 14$, $1 \leq j \leq 8$. The periods are $p_j = 2^{N_j} - 1$. The combining function $F(x_1, \ldots, x_8)$ is balanced, correlation immune of order 3, and has nonlinearity 64.

$$\begin{aligned} F(x_1, \ldots, x_8) = {} & x_1 + x_3 + x_5 + x_8 + x_1x_7 + x_1x_8 + x_2x_4 \\ & + x_2x_6 + x_2x_7 + x_2x_8 + x_3x_6 + x_4x_8 + x_5x_6 + x_6x_7 \\ & + x_1x_4x_7 + x_1x_4x_8 + x_1x_6x_7 + x_1x_6x_8 + x_2x_4x_6 \\ & + x_2x_4x_7 + x_2x_4x_8 + x_2x_6x_7 + x_2x_6x_8 + x_4x_6x_8 \\ & + x_1x_4x_6x_7 + x_1x_4x_6x_8 + x_2x_4x_6x_7 + x_2x_4x_6x_8 \end{aligned}$$

The best linear approximation to F is $L = x_1 + x_2 + x_7 + x_8$. We have $\Pr(F = L) = 3/4$ so that $\epsilon = 1/2$. We guess the initial state of the second shift register of length $N_2 = 16$ considering all $2^{16} - 1$ nonzero initial states. We make use of the following 1024 polynomials:

$$g_k(x) = (x^{kp_1} - 1)(x^{p_7} - 1)(x^{p_8} - 1),$$

$k \in K = \{1, 2, \ldots, 1030\} \setminus \{8, 20, 62, 64, 126, 188\}$. The assumption $|D^{(k)}_{\bmod p_j}| = 8$ is fulfilled for $2 \leq j \leq 6$ and for all $k \in K$. Let ζ be the keystream and β any nonzero output sequence of the target shift register. For each $k \in K$ we compute the first 2^{12} terms of the sequence $g_k(T)[\zeta + \beta]$. Let η_k denote the sequence consisting of those 2^{12} terms. We piece together the sequences η_k to create a sequence $\eta = (\eta_1 | \eta_2 | \cdots | \eta_{1030})$ of $r = 2^{22}$ terms. Associate with $\eta = (y_i)_{i=0}^{r-1}$ the sequence $\gamma = (c_n)_{n=0}^{r-1}$ whose terms are defined by $c_n = \frac{1}{n} |\{i : 0 \leq i \leq n-1,\ y_i = 0\}|$. In this manner each nonzero initial state of the target shift register gives rise to a sequence γ. We plotted the graphs of six of those sequences—among them the sequence corresponding to the correct initial state—over the interval $2^{16} \leq n \leq 2^{22} - 1$. See Figure 1. The graphs of all $2^{16} - 1$ sequences lie within the colored envelope. The graph of the sequence that corresponds to the correct initial state leaves the envelope about at $n = 2^{20.65}$. Using Theorem 1, we find $p = \frac{1}{2}(1 + 2^{-8}) = 257/512$. Using Theorem 2 with $S = 2^{16} - 1$ and $p = 257/512$, we get $n_0 = 2^{20.47}$. Thus, the theoretically predicted result comes close to the true result.

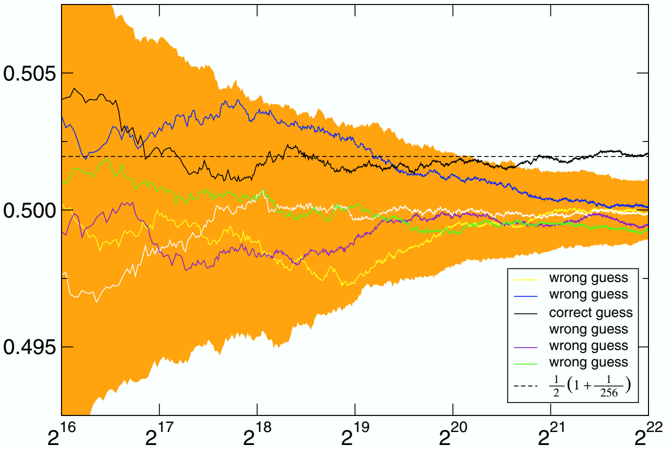

Fig. 1. Simulation of a guess and determine attack

References

[1] B. M. Gammel, R. Göttfert, and O. Kniffler: The Achterbahn stream cipher, eSTREAM, ECRYPT Stream Cipher Project, 29 April 2005. `http://www.ecrypt.eu.org/stream/ciphers/achterbahn/achterbahn.pdf`

[2] B. M. Gammel, R. Göttfert, and O. Kniffler: Achterbahn-128/80, eSTREAM, ECRYPT Stream Cipher Project, 30 June 2006. `http://www.ecrypt.eu.org/stream/p2ciphers/achterbahn/achterbahn_p2.pdf`

[3] B. M. Gammel, R. Göttfert, and O. Kniffler: Achterbahn-128/80: Design and Analysis, *SASC 2007—The State of the Art of Stream Ciphers* (Bochum, Jan. 31 - Feb. 1, 2007), Workshop Record, pp. 152–165.

[4] T. Johansson, W. Meier, and F. Muller: Cryptanalysis of Achterbahn. *FSE 2006*, LNCS 4047, pp. 1–14, Springer-Verlag, Berlin-Heidelberg, 2006.

[5] M. Naya-Plasencia: Cryptanalysis of Achterbahn-128/80, *SASC 2007—The State of the Art of Stream Ciphers* (Bochum, Jan. 31 - Feb. 1, 2007), Workshop Record, pp. 139–151.

[6] M. Naya-Plasencia: Cryptanalysis of Achterbahn-128/80 with a new keystream limitation, eSTREAM, ECRYPT Stream Cipher Project, Report 2007/004, 5 February 2007, `http://www.ecrypt.eu.org/stream/papersdir/2007/004.pdf`