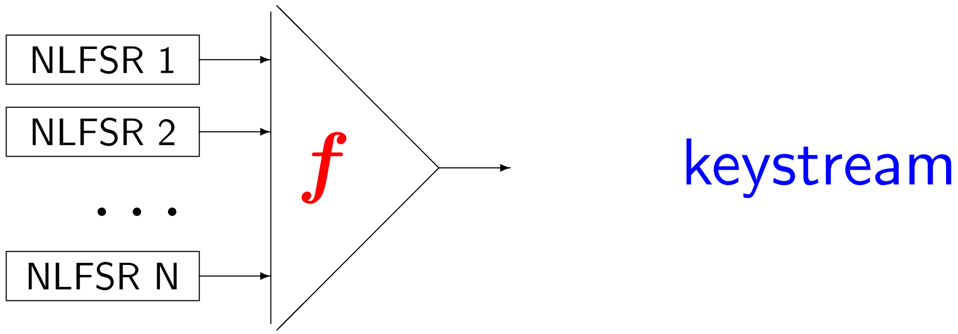
Cryptanalysis of Achterbahn-128/80

Maria Naya-Plasencia

INRIA-Projet CODES
FRANCE

Outline

Achterbahn [Gammel-Göttfert-Kniffler05]



- Achterbahn version 1, version 2, 128-80.
- version 1 cryptanalysed by Johansson, Meier, Muller.
- version 2 cryptanalysed by Hell, Johansson.

Achterbahn-128/80 (July 2006)

Achterbahn-128: key size = 128 bits

- 13 primitive NLFSRs of length $L_i = 21 + i$, $0 \leq i \leq 12$
- Least significant bit of each NLFSR forced to 1 at the initialization process.
- Boolean combining function F:
  - balanced
  - correlation immunity order = 8
- Inputs of $F \leftarrow$ shifted outputs of NLFSRs.
- Keystream length limited to 2^{63}.

Achterbahn-128/80 (July 2006)

Achterbahn-80: key size = 80 bits

- 11 primitive NLFSRs of length $L_i = 21 + i$, $1 \leq i \leq 11$
- Least significant bit of each NLFSR forced to 1 at the initialization process.
- Boolean function $G(x_1, \ldots, x_{11}) = F(0, x_1, \ldots, x_{11}, 0)$:
  - balanced
  - correlation immunity order = 6
- Inputs of $G \leftarrow$ shifted outputs of NLFSRs.
- Keystream length limited to 2^{63}.

Tools used in our cryptanalysis

- Parity checks
- Exhaustive search for the internal states of some registers
- Decimation by the period of a register
- Linear approximations
- Speeding up the exhaustive search

Parity checks

Let $(s_1(t))_{t\geq 0}, \ldots, (s_n(t))_{t\geq 0}$ be n sequences of periods $T_1, \ldots, T_n$, and $\forall t \geq 0,\; S(t) = \sum_{i=1}^{n} s_i(t)$.

- Then, for all $t \geq 0$,

$$\sum_{\tau \in \langle T_1, \ldots, T_n \rangle} S(t+\tau) = 0,$$

$\langle T_1, \ldots, T_n \rangle$: set of all 2^n possible sums of $T_1, \ldots, T_n$.

- Example: $(s_1(t)), (s_2(t))$ with periods T_1 and T_2

$$S(t) + S(t+T_1) + S(t+T_2) + S(t+T_1+T_2) = 0$$

Cryptanalysis with parity checks

- Linear approximation $\ell(t) = \sum_{j=1}^{m} x_{i_j}(t)$ where:

$$\Pr[S(t) = \ell(t)] = \frac{1}{2}(1 + \varepsilon)$$

- Parity check: $\sum_{\tau \in \langle T_{i_1}, \ldots, T_{i_m} \rangle} \ell(t + \tau) = 0$

$$\Pr\left[\sum_{\tau \in \langle T_{i_1}, \ldots, T_{i_m} \rangle} S(t + \tau) = 0\right] \geq \frac{1}{2}\left(1 + \varepsilon^{2^m}\right)$$

Exhaustive search over some registers

- Exhaustive search for the initial states of m' registers

$$\Pr\left[S(t) = \sum_{j=1}^{m'} x_{i_j}(t) + \sum_{j=m'+1}^{m} x_{i_j}(t)\right] = \frac{1}{2}(1+\varepsilon).$$

- The parity check has $2^{m-m'}$ terms and satisfies:

$$\Pr\left[\sum_{\tau \in \langle T_{i_{m'+1}},\dots,T_{i_m}\rangle} \left(S(t+\tau) + \sum_{j=1}^{m'} x_{i_j}(t+\tau)\right) = 0\right] = \frac{1}{2}\left(1+\varepsilon^{2^{m-m'}}\right)$$

Required keystream length

Decoding problem $= 2^{\sum_{j=1}^{m'}(L_{i_j}-1)}$ sequences of length N transmitted through a binary symmetric channel of capacity

$$C(p) = C\left(\frac{1}{2}(1+\varepsilon^{2^{m-m'}})\right) \approx \frac{(\varepsilon^{2^{m-m'}})^2}{2\ln 2}$$

$$N \approx \frac{\sum_{j=1}^{m'}(L_{i_j}-1)}{C(p)} \approx \frac{2\ln 2\sum_{j=1}^{m'}(L_{i_j}-1)}{(\varepsilon^{2^{m-m'}})^2}$$

- Keystream bits needed:

$$(\varepsilon^{2^{m-m'}})^{-2} \times 2\ln 2 \times \sum_{j=1}^{m'}(L_{i_j}-1) + \sum_{i=m'+1}^{m} T_{i_j}$$

Decimation [Hell-Johansson06]

- Parity check:

$$pc(t) = \sum_{\tau \in \langle T_{i_{m'+1}}, \ldots, T_{i_m} \rangle} \left(S(t+\tau) + \sum_{j=1}^{m'} x_{i_j}(t+\tau) \right)$$

- Decimate by the periods of p linear terms $i_1, \ldots, i_p$:

$$pc_p(t) = pc(tT_{i_1} \ldots T_{i_p})$$

- Exhaustive search for the remaining $(m' - p)$ terms

Complexity

- Keystream bits needed:

$$(\varepsilon^{2^{m-m'}})^{-2} \times 2\ln 2 \times \sum_{j=p+1}^{m'} (L_{i_j} - 1) \times 2^{\sum_{j=1}^{p} L_{i_j}} + \sum_{j=m'+1}^{m} 2^{L_{i_j}}$$

- Time complexity:

$$(\varepsilon^{2^{m-m'}})^{-2} \times 2\ln 2 \times \sum_{j=p+1}^{m'} (L_{i_j} - 1) \times 2^{\sum_{j=p+1}^{m'} (L_{i_j} - 1)}$$

Cryptanalysis of Achterbahn-80

- We use a linear approximation: as G has correlation immunity order 6, the best approximation by a 7-variable function is affine [Canteaut-Trabia00]

- We use the following one:

$g_2(x_1, \ldots, x_{10}) = x_1 + x_3 + x_4 + x_5 + x_6 + x_7 + x_{10}$ with $\varepsilon = 2^{-3}$.

Cryptanalysis of Achterbahn-80

- Linear approximation:

$$g_2(x_1, \dots, x_{10}) = (x_4 + x_7) + (x_5 + x_6) + x_1 + x_3 + x_{10} \text{ with } \varepsilon = 2^{-3}.$$

- Parity check:

$$\ell\ell(t) = \ell(t) + \ell(t + T_4 T_7) + \ell(t + T_6 T_5) + \ell(t + T_4 T_7 + T_6 T_5)$$

- Decimate by the period of the register 10.
- Exhaustive search over registers 1 and 3.

Cryptanalysis of Achterbahn-80

- Keystream bits needed:

$$(\varepsilon^4)^{-2} \times 2 \ln 2 \times (L_1 + L_3 - 2) \times 2^{L_{10}} + 2^{L_4 + L_7} + 2^{L_5 + L_6} = 2^{61} \text{ bits.}$$

- Time complexity:

$$(\varepsilon^4)^{-2} \times 2 \ln 2 \times (L_1 + L_3 - 2) \times 2^{L_1 - 1} 2^{L_3 - 1} = 2^{74} \text{ operations.}$$

- Time complexity can be reduced: final complexity 2^{61}.
- We recover the initial states of registers 1 and 3.

Cryptanalysis of Achterbahn-128

- Linear approximation:

$$\ell(x_0,\ldots,x_{12}) = (x_0+x_3+x_7)+(x_4+x_{10})+(x_8+x_9)+x_1+x_2 \text{ with } \varepsilon = 2^{-3}.$$

- Parity check:

$$\ell\ell\ell(t) = \sum_{\tau \in \langle T_{0,3,7}, T_{4,10}, T_{8,9} \rangle} \ell(t+\tau),$$

where $T_{0,3,7} = lcm(T_0, T_3, T_7)$

- Exhaustive search over registers 1 and 2 $\rightarrow$ we can reduce this complexity making profit of the independence of the registers

Improving the exhaustive search

$$\varphi = \sum_{t'=0}^{2^{54}-2^8-1} \sum_{\tau \in \langle T_{0,3,7}, T_{4,10}, T_{8,9} \rangle} (S(t') \oplus x_1(t') \oplus x_2(t'))$$

$$= \sum_{k=0}^{T_2-1} \sum_{t=0}^{2^{31}+2^8-1} \sigma(tT_2+k) \oplus \sigma_1(tT_2+k) \oplus \sigma_2(tT_2+k)$$

$$= \sum_{k=0}^{T_2-1} \left[(\sigma_2(k) \oplus 1) \left(\sum_{t=0}^{2^{31}+2^8-1} \sigma(tT_2+k) \oplus \sigma_1(tT_2+k) \right) + \right.$$

$$\left. \sigma_2(k) \left((2^{31}+2^8) - \sum_{t=0}^{2^{31}+2^8-1} \sigma(tT_2+k) \oplus \sigma_1(tT_2+k) \right) \right]$$

Improving the exhaustive search

for $k = 0$ to $T_2 - 1$ **do**

  $V_2[k] = \sigma_2(k)$ for the all-one initial state.

end for

for each possible initial state of $R1$ **do**

  for $k = 0$ to $T_2 - 1$ **do**

    $V_1[k] = \sum_{t=0}^{2^{31}+2^8-1} \sigma(T_2 t + k) \oplus \sigma_1(T_2 t + k)$

  end for

  for each possible initial state i of $R2$ **do**

  $\sum_{k=0}^{T_2-1}\left[(V_2[k+i \bmod T_2] \oplus 1)\, V_1[k] + V_2[k+i \bmod T_2]\left(2^{31}+2^8-V_1[k]\right)\right]$

    if we find the bias **then**

      return the initial states of $R1$ and $R2$

    end if

  end for

end for

Reducing complexity with an FFT

- $\sum_{k=0}^{T_2-1}\left[(V_2[k+i]\oplus 1)\,V_1[k]+V_2[k+i]\left(2^{31}+2^{8}-V_1[k]\right)\right]$

$$2^{L_2-1}\times T_2\times 2\times 2^{5}$$

- $\sum_{k=0}^{T_2-1}(-1)^{V_2[k+i]}\left(V_1[k]-\frac{2^{31}+2^{8}}{2}\right)+T_2\frac{2^{31}+2^{8}}{2}$

$T_2\log_2 T_2$ with an FFT.

Cryptanalysis of Achterbahn-128

- Keystream bits needed:

$$(\varepsilon^8)^{-2} \times 2\ln 2 \times (L_1 + L_2 - 2) + T_{0,3,7} + T_{4,10} + T_{8,9} < 2^{61} \text{ bits.}$$

- Time complexity:

$$2^{L_1-1} \times \left[2^{31} \times T_2 \times \left(2^4 + 31\right) + T_2 \log T_2\right] + T_2 \times 2^3 = 2^{80.58}.$$

Achterbahn-128 limited to 2^{56} bits

- The same attack as before using the linear approximation:

$$\ell(x_0, \ldots, x_{12}) = (x_3+x_8)+(x_1+x_{10})+(x_2+x_9)+x_0+x_4+x_7$$

- Improved exhaustive search over registers 0,4 and 7, considering R_0 and R_4 together.
  - keystream bits needed $< 2^{56}$
  - time complexity: 2^{104} operations.

Achterbahn-80 limited to 2^{52} bits

- Linear approximation:

$$\ell(x_1, \ldots, x_{11}) = (x_3 + x_7) + (x_4 + x_5) + x_1 + x_6 + x_{10}$$

- With the same attack as before, we need more than 2^{52} keystream bits.

- We can adapt the algorithm in order to reduce the data complexity.

Achterbahn-80 limited to 2^{52} bits

- Instead of one decimated sequence of parity checks of length L, 4 decimated sequences of length $L/4$:

$$S(t(T_1)+i)+S(t(T_1)+i+T_7T_3)+S(t(T_1)+i+T_4T_5)$$

$$+S(t(T_1)+i+T_7T_3+T_4T_5),$$

for $i \in \{0,\ldots,3\}$.

- Keystream bits needed $< 2^{52}$
- Time complexity: 2^{67} operations.

Recovering the key

From the previously recovered initial states of some registers:

- Meet-in-the-middle attack on the key-loading.
- No need to invert all the clocking steps.

Additional complexity:

- Achterbahn-80: 2^{40} in time and 2^{41} in memory.
- Achterbahn-128: 2^{73} in time and 2^{48} in memory.

Conclusions

Attacks complexities against all versions of Achterbahn

version	data complexity	time complexity	references
v1 (80-bit)	2^{32}	2^{55}	[JMM06]
v2 (80-bit)	2^{64}	2^{67}	[HJ06]
v2 (80-bit)	2^{52}	2^{53}	
v80 (80-bit)	2^{61}	2^{55}	
v128 (128-bit)	2^{60}	$2^{80.58}$	