On a bias of Rabbit

Jean-Philippe Aumasson

University of Applied Sciences Northwestern Switzerland
School of Engineering

RABBIT

Design

- Presented at FSE 2003 by Boesgaard *et al.*
- eSTREAM phase 2 candidate (SW & HW), report 2005/024.
- Patented by Cryptico (Denmark), described in RFC 4503.

Analysis

- 9 white papers @ `cryptico.com`:
  - performance evaluation
  - analysis of key and IV setup
  - algebraic and mod n analysis
  - analysis of the core function g (differentials, *etc.*)
- SASC 2004 paper "The Rabbit Stream Cipher - Design and Security Analysis".

KEYSTREAM GENERATION

- 128-bit key, 64-bit IV, 513-bit state:

  32-bit sequences $\{x_{j,t}\}_{0 \leq j \leq 7}$ and $\{c_{j,t}\}_{0 \leq j \leq 7}$ + carry bit

- Each round outputs a 128-bit keystream block s_t, *e.g.*

$$s_t^{[15...0]} = x_{0,t}^{[15...0]} \oplus x_{5,t}^{[31...16]}.$$

  State update:

$$\begin{aligned} x_{0,t+1} &= g_{0,t} + (g_{7,t} \lll 16) + (g_{6,t} \lll 16), \\ x_{5,t+1} &= g_{5,t} + (g_{4,t} \lll 8) + g_{3,t}. \end{aligned}$$

- The main function g:

$$g_{j,t} = (x_{j,t} + c_{j,t+1})^2 \oplus [(x_{j,t} + c_{j,t+1})^2 \gg 32] \mod 2^{32}.$$

THE FUNCTION g

$$g_{j,t} = (x_{j,t} + c_{j,t+1})^2 \oplus [(x_{j,t} + c_{j,t+1})^2 \gg 32] \mod 2^{32}.$$

- g's distribution with random state = distribution of

  $$x \rightarrow x^2 \oplus (x^2 \gg 32)$$

  with random $x \in \{0,1\}^{32}$.
- Consider the function $G_n : \{0,1\}^n \rightarrow \{0,1\}^n$,

  $$x \rightarrow x^2 \oplus (x^2 \gg n).$$

PROPERTIES OF $G_n : x \rightarrow x^2 \oplus (x^2 \gg n)$

Property 1

For all even $n \geq 2$, $G_n(1) = G_n(2^{n/2}) = 1$, so G_n is not bijective for even n's.

Property 2

For all even $n \geq 2$, if $x < 2^{n/2}$, then $G_n(x) = x^2$.

Property 4

For all $n \geq 2$, $G_n(0) = 0$ and $G_n(2^n - 1) = 2^n - 1$.

PROPERTIES OF $G_n : x \longrightarrow x^2 \oplus (x^2 \gg n)$

Property 5

For all even $n \geq 4$, if $x = \sum_{k=n/2-1}^{n-2} 2^k$, then $G_n(x) = x$.

Property 6

For all $n \geq 2$, the number $2^n + 1$ is square-free if and only if any non-null x verifies $G_n(x) \neq 0$.

DISTRIBUTION OF G_8 & G_{32}

- Distribution of $G_8(x)$:

offset	0	1	2	3	4	5	6	7
bias	$2^{-5.0}$	$2^{-5.0}$	$2^{-5.2}$	$2^{-5.0}$	$2^{-4.7}$	$2^{-5.0}$	$2^{-5.0}$	$2^{-5.0}$

(bias at position $i = \frac{1}{2} - P\left(G(x)^{[i]} = 1\right)$)

- For G_{32}'s offsets:

$$2^{-17.35} < \text{bias} < 2^{-16.40}.$$

- Only positive biases
  - $\Rightarrow$ "more zeros than ones" in g's images
  - $\Rightarrow$ **bias in the keystream** $\{s_t\}_{t>0}$.

BIAS OF THE KEYSTREAM $\{s_t\}_{t>0}$

- Example of the first bit of a keystream block:

$$\begin{aligned} s_t^{[0]} &= \mathbf{x_{0,t}^{[0]}} \oplus \mathbf{x_{5,t}^{[16]}} \\ x_{0,t+1} &= g_{0,t} + (g_{7,t} \lll 16) + (g_{6,t} \lll 16) \\ x_{5,t+1} &= g_{5,t} + (g_{4,t} \lll 8) + g_{3,t} \end{aligned}$$

- Distribution of $\mathbf{x_{0,t}^{[0]}}$ easy to compute:

$$P(x_{0,t}^{[0]} = 1) = p_0 \cdot p_{16}^2 + p_0 \cdot q_{16}^2 + 2 \cdot q_0 \cdot p_{16} \cdot q_{16} \leq \frac{1}{2} - 2^{-47.85},$$

with $p_i = P(i\text{-th bit} = 1)$, $q_i = 1 - p_1$.

- Distribution of $\mathbf{x_{5,t}^{[16]}}$?

BIAS OF THE KEYSTREAM $\{s_t\}_{t>0}$

- Bias in the 17-th bit of $x_{5,t+1} = g_{5,t} + (g_{4,t} \lll 8) + g_{3,t}$ computed by
  1. recursively expressing the distribution of $(g_{3,t} + g_{5,t})$,
  2. computing carry bits distribution*.
- Bias of $x_{5,t}$, $0 \leq k < 4$:

0	1	2	3	4	5	6	7
$2^{-48.8}$	$2^{-63.3}$	$2^{-52.7}$	$2^{-55.3}$	$2^{-59.9}$	$2^{-59.3}$	$2^{-60.2}$	$2^{-63.2}$
...	...	...	...	**16**	...	...	...
...	...	...	...	$\mathbf{2^{-76.7}}$	...	...	...
24	25	26	27	28	29	30	31
$2^{-78.9}$	$2^{-80.0}$	$2^{-79.4}$	$2^{-79.8}$	$2^{-87.8}$	$2^{-81.2}$	$2^{-79.6}$	$2^{-80.0}$

* we assume independence between the (random variables of) the carry bit distribution at a given offset and the bits after this offset.

BIAS OF THE KEYSTREAM $\{s_t\}_{t>0}$

- From the previous results:

$$P(s_t^{[0]} = 1) \approx \frac{1}{2} - 2^{-124.50}.$$

- Same bias appears in $s_t^{[k]}$, for $128 > k \equiv 0 \mod 16$.
- Optimal distinguisher requires $\approx 2^{247}$ blocks s_t, with random keys & IV's (exh.search needs 2^{128} blocks).

CONCLUSION

Rabbit is safe, but...

- its core function suffers of several non-desirable properties, and
- a uniform distribution of initial states does not provide a uniform distribution of keystream bits.

CONCLUSION

Rabbit is safe, but. . .

- its core function suffers of several non-desirable properties, and
- a random inital state does not produce a (uniform) random keystream.

Chase the Rabbit ! (see contest at `www.cryptico.com`).