A Time-Memory Tradeoff Attack Against LILI-128

Helsinki University of Technology
Laboratory for Theoretical Computer Science
P.O. Box 5400, FIN-02015 HUT, Finland
mjos@tcs.hut.fi

Abstract. In this note we discuss a novel and simple time-memory tradeoff attack against the stream cipher LILI-128. The attack defeats the security advantage of having an irregular stepping function. The attack requires 2^{46} bits of keystream, a lookup table of 2^{45} 89-bit words and computational effort which is roughly equivalent to 2^{48} DES operations.

1 Introduction

2^{112}

1.1 Previous Work

– 2^{71}
2^{79} 2^{30}
2^{40}

–

1.2 Time/Memory/Data Tradeoffs

x_i

N *Step* *Output*

x_0 $z(i)$

Output *Step*

$$z(i) = Output(x_{i-1})$$
$$x_i = Step(x_{i-1})$$

Off-line preprocessing stage. x_i
$z(i), z(i+1), \ldots, z(i+O(\log N))$
x_i

On-line computation phase. $O(\log N)$

Step

$O(\sqrt{N})$ $O(\log N\sqrt{N})$
$O(\log N\sqrt{N})$ x_i

2 Description of LILI-128

$LFSR_c$ $LFSR_d$ $LFSR_c$
$LFSR_d$
$LFSR_c$
$128 = 39 + 89$
[1]
$t_0, t_1, \ldots, t_{38}$ $LFSR_c$ t_0
t_{38}

[1] In [6] the authors also discuss other keying methods for LILI-128.

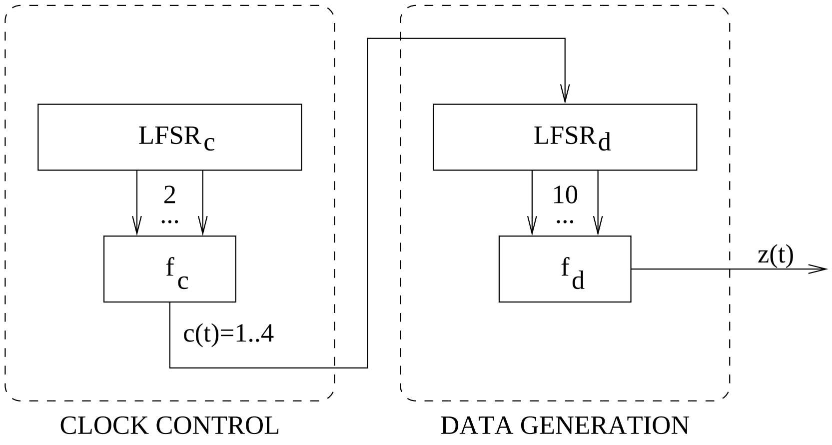

Fig. 1. Overview of the LILI-128 keystream generator.

$u_0, u_1, \ldots, u_{88}$ $LFSR_d$
$LFSR_c$

$$x^{39} + x^{35} + x^{33} + x^{31} + x^{17} + x^{15} + x^{14} + x^2 + 1$$

$LFSR_d$

$$x^{89} + x^{83} + x^{80} + x^{55} + x^{53} + x^{42} + x^{39} + x + 1.$$

$LFSR_d$ $f_d, f_d : \mathbb{F}_2^{10} \to \mathbb{F}_2$
$z(t)$ [2]

$$z(t) = f_d(u_0, u_1, u_3, u_7, u_{12}, u_{20}, u_{30}, u_{44}, u_{65}, u_{80}).$$

$LFSR_c$ $f_c : \mathbb{F}_2^2 \to \mathbb{F}_2$
$c(t)$

$$c(t) = f_c(t_{12}, t_{20}) = 2t_{12} + t_{20} + 1$$

$LFSR_c$
$LFSR_d$ $c(t)$

before

[2] The f_d function is specified as a 1024-entry table in the original specification [5], and is excluded from this paper since it is irrelevant to the present attack.

Lemma 1. *For each* $\Delta_c = 2^{39} - 1$ *times* $LFSR_c$ *is clocked,* $LFSR_d$ *is clocked exactly* $\Delta_d = 5 * 2^{38} - 1$ *times.* [3]

Proof. t

$$\sum_{i=1}^{2^{39}-1} c(t+i) = \Delta_d$$

$LFSR_c$ $2^{39} - 1 = \Delta_c$

$t_0 = t_1 = \ldots = t_{38} = 0$ (t_{12}, t_{20}) $(0,0)$ $2^{37} - 1$ $(0,1)$ $(1,0)$ $(1,1)$ 2^{37} $1*(2^{37}-1)+(2+3+4)*2^{37} = 1374389534719 = \Delta_d$

Lemma 2. $LFSR_d$ *can be stepped by* Δ_d *number of positions forward or backward by performing a vector-matrix multiplication with a precomputed* 89×89 *bit matrix over* $GF(2)$*. The matrix can be constructed with roughly* 2^{28} *bit operations using a binary matrix exponentiation algorithm.*

Proof. $GF(2^{89})$ Δ_d $3949 \approx 2^{11.4}$

3 The Attack

3.1 Constructing the Lookup Table

2^{45} 2^{46} $LFSR_d$ f_d Δ_d

Analysis. $1-e^{-2} = 0.8647$ $2^{51.48}$ 2^{48}

[3] This lemma follows implicitly from Theorem 2 in [5]

3.2 Lookup Stage

2^{46} $z(0), z(1), \ldots, z(2^{46}-1)$

$2^{46} - 44\Delta_c - 1$
$z(i) \mid z(i+\Delta_c) \mid \ \ldots \ \mid z(i+44\Delta_c)$
$LFSR_d$
$LFSR_d$ $\Delta_d \lfloor \frac{i}{\Delta_c} \rfloor$

$f_d(LFSR_d) \neq z(j\Delta_c + (i \bmod \Delta_c))$
$LFSR_d$ Δ_d
$LFSR_d$

$LFSR_d$
$LFSR_d$ Δ_d
$z(i \bmod \Delta_d)$
$LFSR_d$ Δ_d Δ_c
$LFSR_d$

$LFSR_c$

Analysis. $LFSR_d$

$$1 - \left(1 - \frac{0.8647 * 2^{45}}{2^{89}}\right)^{2^{46} - 44\Delta_c} \approx 90\%.$$

2^{45}
2^{48}

4 Conclusions

2^{46}

2^{45} $2^{51.48}$
2^{48}

5 Acknowledgments

References

1. S. Babbage. *Cryptanalysis of LILI-128.* NESSIE Public Report, `https://www.cosic.esat.kuleuven.ac.be/nessie/reports`, 2001.
2. S. Babbage. *A Space/Time Tradeoff in Exhaustive Search Attacks on Stream Ciphers*, European Convention on Security and Detection, IEE Conference Publication No. 408, 1995.
3. A. Biryukov and A. Shamir, *Cryptanalytic Time/Memory/Data Tradeoffs for Stream Ciphers*, Proceedings of ASIACRYPT 2000, LNCS 1976, pp. 1–13, Springer-Verlag, 2000.
4. A. Biryukov, A. Shamir, and D. Wagner, *Real Time Cryptanalysis of A5/1 on a PC*, Proceedings of FSE '2000, LNCS 1978, pp. 1–18, Springer-Verlag, 2001.
5. E. Dawson, J. Golić, W. Millan and L. Simpson, *The LILI-128 Keystream Generator*, Proceedings of the Seventh Annual Workshop on Selected Areas in Cryptology - SAC 2000, LNCS 2012, Springer-Verlag, 2000.
6. E. Dawson, J. Golić, W. Millan and L. Simpson, *Response to Initial Report on LILI-128*, Submitted to Second NESSIE Workshop, 2001.
7. M. E. Hellmab, *A Cryptanalytic Time-Memory Trade-Off*, IEEE Transactions on Information Theory, Vol. IT-26, N 4, pp. 401–406, 1980.
8. F. Jönsson and T. Johansson, *A Fast Correlation Attack on LILI-128.*, Information Processing Letters Vol 81, N. 3, Pages 127-132, 2001.
9. J. White, *Initial Report on the LILI-128 Stream Cipher*, NESSIE Public Report, `https://www.cosic.esat.kuleuven.ac.be/nessie/reports`, 2001.