LILI-II is not Broken

William Millan and Ed Dawson

Information Security Institute
Queensland University of Technology
Brisbane, Queensland, Australia
{millan, dawson}@isrc.qut.edu.au

Abstract. In this note we point out that a recently published attack on the LILI-II stream cipher does *not* do better than generic time-memory tradeoff techniques (which generalise exhaustive search and apply to any 128-bit key cipher). Thus we assert that LILI-II remains unbroken.

1 Introduction

At FSE'05, a paper by Englund and Johansson [1] discussed techniques for the cryptanalysis of irregularly clocked LFSR filter stream ciphers, and hence they find a distinguishing attack (requiring 2^{103} memory and 2^{103} time) on the 128-bit key LILI-II stream cipher [2] and they claim this is "better than exhaustive search". However they have *ignored* the (by now well known) generic time-memory tradeoff (TMTO) attacks that apply to any and all ciphers for which the algorithm is known. Here we recall the performance of key-recovery TMTO attacks and compare these approaches with the attack from [1], concluding that their attack does *not* (in any way) improve over standard generic attacks on LILI-II. Furthermore, we note that the recent ECRYPT process for stream ciphers seems happy [5] for 128-bit stream ciphers to impose an upper bound of 2^{96} on the number of bits output before mandatory re-keying, and we support this strategy. Hence the (hardware efficient) LILI-II cipher should still be considered unbroken.

2 TMTO attacks

Time memory tradeoff attacks exploit the birthday paradox by using collision search techniques to achieve key recovery for any cipher with a published algorithm. The history of the development of these attacks is nicely covered by [3], so we need not repeat all those details here. Briefly, TMTO attacks have been known since 1980 and several advances were made since the mid-1990's. TMTO attacks targeting the internal state size imply that the security level of any cipher cannot be more than half the state size in bits, and this observation has motivated several designers to increase the internal state of their designs. However, it is interesting to note that these TMTO attacks are not discussed at all in [4] from January 2005.

It seems fair to say that the cryptographic community was surprised (perhaps even embarressed) when [3] reminded us (in late March 2005) that TMTO attacks can just as easily target the secret key directly, rather than the larger internal state, and that internal state size gives no protection to this approach. These key-targeting TMTO attacks are completely generic, apply to any known-algorithm cipher, and allow recovery of a k bit key with effort of $2^{\frac{k}{2}}$ memory and $2^{\frac{k}{2}}$ time. Clearly any publicly proposed 128-bit key stream cipher can be broken with effort of 2^{64} memory and 2^{64} time, regardless of the details of the algorithm. These values are now the benchmark that cryptanalysis must beat in order to be considered a certificational weakness in the cipher. Basically an attack is better than TMTO if and only if the sum of the resource consumption exponents is strictly less than the keysize. This condition is not satisfied for any known attack on LILI-II, including [1].

3 Conclusion

LILI-II remains unbroken. The best known attack on LILI-II is the generic TMTO which applies to all 128-bit key ciphers. The attack from [1] requires a factor of 2^{39} more memory and a factor of 2^{39} more time than the now standard generic key-targeting TMTO attack, and it is only a distinguisher, which is far less powerful than key-recovery. Furthermore, their attack completely fails if the output is limited to the (ECRYPT recommended) 2^{96} bits, which is surely enough for any application. We encourage further analysis of the LILI-II cipher.

References

1. H. Englund and T. Johansson "A New Distinguisher for Clock Controlled Stream Ciphers", Fast Software Encryption 2005, LNCS vol 3557, pages 181-195, Springer, 2005.
2. A. Clark, E. Dawson, J. Fuller, J. Golic, H.J. Lee, W. Millan, S.J. Moon and L. Simpson "The LILI-II Keystream Generator", ACISP 2002, LNCS vol 2384, pages 25-39, Springer, 2002.
3. J. Hong and P. Sarkar "Rediscovery of Time Memory Tradeoffs", IACR ePrint Archive, Report 2005/090, available from http://eprint.iacr.org
4. ECRYPT D.STVL.3 "Ongoing Research Areas in Symmetric Cryptology", 31 January 2005, available online via https://www.cosic.esat.kuleuven.ac.be/ecrypt/documents/D.STVL.3-2.5.pdf
5. B. Preneel, "A Call for Stream Ciphers by ECRYPT", presentation at Asiacrypt'04 rump session, available at http://www.iris.re.kr/ac04/data/Asiacrypt2004/Rump_Session/A3_preneel_rump.pdf