N^{th} internal state of the cipher, then the key recovery algorithm recovers the secret key by performing $N+160$ iterations in the 'while loop' of the on-line phase of the algorithm.

IX. CONCLUSION

In this paper, we presented a new class of cryptanalytic attacks, which are applicable against those ciphers whose analysis theory depends on the properties of 2-adic numbers. The new class of cryptanalytic attacks is referred to as 'Linearisation Attacks'. This class consists of three variants, namely, 'Conventional Linearisation Attacks', 'Fast Linearisation Attacks' and the 'Improved Linearisation Attacks'. All these variants provide a tradeoff between data, time and memory complexities when compared with each other. These attacks are demonstrated against the F-FCSR family of stream ciphers by cryptanalysing two important members of this family, which are known as F-FCSR-H v2 and the F-FCSR-H. To cryptanalyse these ciphers, we presented state recovery algorithms based on the three different variants of the linearisation attacks. These algorithms recover the internal secret state of the ciphers. A comparative analysis of different attacks on F-FCSR-H v2 and F-FCSR-H stream ciphers is also presented, which shows various tradeoffs between these variants in terms of data, time and memory complexities. This analysis shows that CLA is easy to implement, but requires more resources such as known key-stream, processing time, etc. The FLA is the most efficient attack in terms of running time complexity. The ILA is the most efficient attack in terms of data and memory complexities. The paper also presented a key recovery algorithm, which works in conjunction with the state recovery algorithms and recovers the effective key used in the ciphers.

X. REFERENCE

[1] A.Ali, "New Most Efficient State Recovery Attacks on an eSTREAM Candidate F-FCSR-H v2 and F-FCSR-H Stream Ciphers," In Proceedings of the World Congress on Internet Security (WorldCIS-2011), London, UK, 2011.

[2] A. Ali, "New Results on FCSRs and Their Applications for FCSR-based Stream Ciphers," PhD Annual Review Report, RHUL, UK, 28 October 2010.

[3] F. Arnault and T. Berger, "Design and Properties of a New Pseudo-random Generator Based on a Filtered FCSR Automaton," IEEE Transactions on computers 54(11), 2005, pp.1374–1384.

[4] F. Arnault and T. Berger, "F-FCSR: Design of a new class of stream ciphers," In: H. Gilbert and Fast Software Encryption 2005, Lecture Notes in Computer Science, 3557, 2005, pp. 83-97.

[5] F. Arnault, T. Berger, and C. Lauradoux, "Update on F-FCSR stream cipher," eSTREAM, ECRYPT stream cipher project, Report 2006. http://www.ecrypt.eu.org/stream/, 2006.

[6] J. Evertse, "Linear structures in block ciphers," Advances in Cryptology – EUROCRYPT'87, Lecture Notes in Computer Science 304, 1988.

[7] M. Goresky and A. Klapper, "Periodicity and Distribution Properties of Combined FCSR Sequences," Sequences and Their Applications – SETA'06, Lecture Notes in Computer Science 4086, 2006, pp. 334-341.

[8] M. Hell and T. Johansson, "Breaking the F-FCSR-H Stream Cipher in Real Time," Proceedings of 14th International Conference on the Theory and Applications of Cryptology and Information Security, Advances in Cryptology, Lecture Notes in Computer Science 5350, 2008, pp. 557-569.

[9] M. Hell and T. Johansson, "Breaking the Stream Ciphers F-FCSR-H and F-FCSR-16 in Real Time," Journal of Cryptology, 2009, pp. 1-19.

[10] A. Kerkhoffs, "La cryptographie militaire," Journal des Sciences Militaires, 1883, pp. 161-191.

[11] A. Klapper and M. Goresky, "Fibonacci and Galois Representations of Feedback –With-Carry Shift Registers," IEEE Transactions on Information Theory 48(11), 2002, pp. 2826-2836.

[12] M. Saarinen, "Linearisation attacks against syndrome based hashes," In: K. Srinathan, C. Pandu, M. Yung (eds.), Indocrypt'07, Lecture Notes in Computer Science 4859, 2007, pp. 1-9.

[13] S. Babbage, C.D. Canniere, A. Canteaut, C. Cid, H. Gilbert, T. Johansson, M. Parker, B. Preneel, V. Rijmen, and M. Robshaw, "The eSTREAM Portfolio", April 15, 2008, Available at: http://www.ecrypt.eu.org/stream/portfolio.pdf (Access Date: March 7, 2011).

[14] S. Babbage, C.D. Canniere, A. Canteaut, C. Cid, H. Gilbert, T. Johansson, M. Parker, B. Preneel, V. Rijmen, and M. Robshaw, "The eSTREAM Portfolio (rev. 1)", September 8, 2008, Available at: http://www.ecrypt.eu.org/stream/portfolio-revision1.pdf (Access Date: March 7, 2011).

Copyright © 2012, Infonomics Society