

TABLE I
THE NUMBERS OF FALSE ALARMS OBTAINED WITH THE NEW LCT
ATTACK (SEE TEXT)

	N	n_f	$n_f\%$	n_s	f_s	$f_s\%$
$t = 1$	20	1	5	2	1	5
$t = 2$	190	62	33	5	2	1

algorithm) n_s are given together with the numbers of cases f_s , in which the false alarms were generated with the maximum number of solutions (that would be the worst possible case for the cryptanalyst). In the table, N represents the total number of possible combinations for complementing the bits of the intercepted sequence.

From the Table I it can be noted that for $t = 2$ the number of false alarm cases is quite high, approx. 33% of all the cases. The maximum number of solution initial states of LFSR_s offered by the attack algorithm in that case is $n_s = 5$, which is 1/3 of the possible number of initial states of that register. This number is also quite high, but to recover from such a situation, ordering of these solution states according to the corresponding numbers of consistent systems obtained in the attack is possible to perform, which in most cases places the right initial state to the second position. This eliminates the problem of too many solutions offered by the attack algorithm and also makes the problem of too many false alarms easier. The greatest advantage of the new attack compared with the attack from [1] and [6] is in the fact that the new algorithm always produces the right solution, even when it is accompanied by a false alarm.

V. CONCLUSION

In this paper, a new Linear Consistency Test (LCT)-based attack against a noised pseudorandom generator scheme employing irregular clocking is described and analyzed. The attack was applied against a specific representative of this class of generators known as The Binary Rate Multiplier (BRM). The attack first assigns a system of linear equations to the BRM based on a guessed initial state of its clocking LFSR. This system is then checked for consistency and if consistent, the right initial state of the clocking LFSR was guessed. If the obtained system is inconsistent, the equations involving complemented bits of the intercepted sequence are eliminated from the system and then the consistency of the system is checked again. Which bits of the intercepted sequence are complemented is also guessed. If the guess of those bits is right, the obtained system will surely become consistent. Otherwise, if the guess of the initial state of the clocking LFSR was right, there is a significant chance that the newly obtained system becomes consistent. In a contrary case, the new system will be inconsistent with high probability. The attack always gives the right solution for the initial state of the clocking LFSR, but that solution may be accompanied by other solutions (false alarms). The recovery procedure in those cases is proposed as well. The attack is feasible if the number of possible combinations for the bits of the intercepted

sequence complemented by noise is small, which means that the level of noise is up to moderate.

REFERENCES

- [1] G. Bu, "Linear consistency test (LCT) in cryptanalysis of irregularly clocked LFSRs in the presence of noise," Master thesis, Gjøvik University College, Gjøvik, Norway, 2011.
- [2] W. Chambers and S. Jennings, "Linear equivalence of certain BRM shift-register sequences," *Electronics Letters*, vol. 20, no. 24, pp. 1018–1019, 1984.
- [3] J. Golić and M. Mihaljević, "A generalized correlation attack on a class of stream ciphers based on the Levenshtein distance," *Journal of Cryptology*, vol. 3, no. 3, pp. 201–212, 1991.
- [4] T. Johansson, "Reduced complexity correlation attacks on two clock-controlled generators," in: Ohta K. (Ed.), *Advances in Cryptology: Proceedings of ASIACRYPT '98*, Lecture Notes in Computer Science LNCS 1514, pp. 342–356, Springer-Verlag, 1998.
- [5] H. Molland, T. Helleseeth, "An improved correlation attack against irregular clocked and filtered keystream generators," in *Proceedings of CRYPTO 2004*, Lecture Notes in Computer Science LNCS 3152, pp. 373–389, Springer-Verlag, 2004.
- [6] S. Petrović, "Application of linear consistency test in a ciphertext-only attack on irregularly clocked linear feedback shift registers," in *Proceedings of XII Spanish Conference on Cryptography and Information Security (RECSI2012)*, U. Zurutuza, R. Uribeetxeberria, I. Arenaza-Nuño, Eds. Arrasate - Mondragon: Servicio Editorial de Mondragon Unibertsitatea, pp. 113–117, 2012.
- [7] K. Zeng, C. Yang, and T. Rao, "On the linear consistency test (LCT) in cryptanalysis with applications," in *Advances in Cryptology, Proceedings of CRYPTO '89*, Lecture Notes in Computer Science LNCS 435, pp. 164–174, Springer-Verlag, 1990.