Cryptanalysis Techniques for Stream Cipher: A Survey

M. U. Bokhari
Chairman, Department of Computer Science, AMU
Aligarh (India)

Shadab Alam
Research Scholar, Dept. of Computer Science, AMU
Aligarh (India)

Faheem Syeed Masoodi
Research Scholar, Dept. of Computer Science, AMU
Aligarh (India)

ABSTRACT
Stream Ciphers are one of the most important cryptographic techniques for data security due to its efficiency in terms of resources and speed. This study aims to provide a comprehensive survey that summarizes the existing cryptanalysis techniques for stream ciphers. It will also facilitate the security analysis of the existing stream ciphers and provide an opportunity to understand the requirements for developing a secure and efficient stream cipher design.

Keywords
Stream Cipher, Cryptography, Cryptanalysis, Cryptanalysis Techniques

1. INTRODUCTION
Cryptography is the primary technique for data and communication security. It becomes indispensable where the communication channels cannot be made perfectly secure. From the ancient times, the two fields of cryptology; cryptography and cryptanalysis are developing side by side.

Cryptography studies the design of algorithms for information and communication security at the same time cryptanalysis is concerned with the study of different techniques to search weakness in the cryptographic algorithms and try to break these algorithms. The developed designs or ciphers should be secured against any possible attack in an ideal situation, but this is not possible in the practical world. Any cryptographic primitive can only be tested for all the possible known attacks.

Cryptographic algorithms can be divided into two categories, Symmetric (Secret) key algorithms and Asymmetric (Public) key algorithms. In some literature cryptographic algorithms have been divided into three categories; Symmetric key, Asymmetric key and Unkeyed algorithms. In Symmetric key algorithm, both the sender and receiver share the secret key and in asymmetric key algorithms; there are two keys; Public key and Private Key. Public key is made public and private key is kept secret with the receiver. The third category i.e. unkeyed algorithms use the hybrid of these two technologies for e.g. hash functions.

The symmetric key algorithms are further divided into two categories of Block Cipher and Stream cipher. In this paper we are focusing on Stream ciphers.

Cryptanalysis is the technique of deriving the original message from the ciphertext without any prior knowledge of secret key or derivation of key from the ciphertext. A general technique for cryptanalysis, applicable to all cryptographic algorithms is to try all the possible keys until the correct key is matched, it is known as exhaustive key search. With every passing day, the computing ability of hardware is increasing manifold; therefore it becomes necessary to use long keys for avoiding exhaustive key search. All the other attacks applied on stream ciphers are compared to exhaustive key search in terms of data and memory complexity and if its complexity is less than exhaustive key search, then only these are considered as successful. A symmetric key cipher, especially a stream cipher is assumed secure, if the computational capability required for breaking the cipher by best-known attack is greater than or equal to exhaustive key search.

There are different Attack scenarios for cryptanalysis based on available resources:

1. Ciphertext only attack
2. Known plain text attack
3. Chosen plaintext attack
4. Chosen ciphertext attack

On the basis of intention of the attacker, the attacks can be classified into two categories namely key recovery attack and distinguishing attacks. The motive of key recovery attack is to derive the key but in case of distinguishing attack, the attacker's motive is only to derive the original from the ciphertext. There are different attacks known for the stream ciphers. Majority of these attacks have been discussed here. This study is conducted due to significance of stream ciphers in data and communication security and will provide an extensive survey of different cryptanalysis techniques and weaknesses of existing stream cipher designs that need to be overcome for developing a secure and efficient stream cipher.

2. CRYPTANALYSIS TECHNIQUES
Cryptanalysis techniques for stream ciphers are:

1. Exhaustive Key Search Attack
2. Side Channel Analysis Attack
3. Time Memory Trade off Attacks
4. Distinguishing Attacks
5. Algebraic Attack
6. Correlation attacks
7. Guess and Determine attacks
8. Linear Masking attacks
9. Related Key Attack
10. Divide and Conquer Attack

2.1 Exhaustive Key Search Attack:
In an exhaustive key search attack or a brute force attack, the cryptanalyst tries all possible keys to decrypt a ciphertext and can be used against any cryptographic algorithm including stream ciphers except provable secure ciphers [1] though a provable secure cipher is not practically feasible, for e.g. one time pad.

If the key size is n bits, then the attacker has to try on an average 2^{n-1} keys for breaking a cipher and 2^n keys in the worst case. The computational complexity of an attack is often stated as O (2^n). [1] An attack with a higher computational complexity than an exhaustive key search is not considered an attack at all.

2.2 Side Channel Analysis Attack:

Generally there are two steps involved in developing any cryptographic primitive. First, it is defined as an abstract mathematical object. Thereafter this mathematical entity needs to be implemented in form of a program and in some cases these programs are further implemented in some specific hardware. These programs after implementation will be executed in a computing environment on processing units. These executions will present some specific characteristics.

Side channel Analysis (SCA) refers to the attacks based on the physically observable characteristics during execution. Some of the common physical characteristics that are used for Side Channel Analysis are Power and Microprocessor time required for execution, electromagnetic radiation, heat dissipation and noise of the system etc.

On the basis of above characteristics; there are different Side Channel attacks on ciphers in general and on stream cipher in particular. Some of powerful techniques, that generally used for Side Channel Analysis attacks are Simple Power analysis attack, Differential Power Analysis attack [2,3], Timing Analysis attack [4,5], Electromagnetic Analysis attacks [6,7,8] and Acoustic Cryptanalysis [9].

Though there is no general countermeasure to these attacks but some of the possible countermeasures maybe noise addition, buffering of the output sequence, Physical shielding, reduction of signal size, eliminating the branch processing in implemented algorithm that will make the encryption time equivalent [10,11] and few more.

2.3 Time Memory Tradeoff Attacks

A time memory tradeoff attack is a method of cryptanalysis that aims to attack a cryptographic primitive with lower complexity than look up table and an online complexity lower than exhaustive key search. TMTO is an improvement to the exhaustive key search attack that trades off computational time against memory complexity [12].

This attack can be divided into two phases; an offline phase or pre-computation phase and online phase. In offline phase a table is constructed in like lookup table method by selecting different random keys and generating the output for each chosen key. These pairs of output strings and keys are stored in an indexed table by the output strings. In the second phase or online phase, the attacker observes the output generated by unknown keys. Then these outputs are matched with the outputs of the table generated in the offline phase. If a match is found then corresponding key will be the key off the matched output.

Amirazizi and Hellmen were the first to propose Time memory processor trade-off attack [12] on block ciphers and in case of stream ciphers, TMTO was proposed by Babbage [13] in 1995 and Golic [14] in 1997 independently. Later on Biryukov and Samir combined Babbage and Golic scheme with Hellmen attack [15]. This attack was further refined by Birykov, Shamir and Wagner and applied on A5/1 [16].

To avoid TMTO on stream ciphers, Hong and Sarkar [52] suggested that state size should be equal to or greater than sum of key size and size of IV and it should be random. Babbabge [13] and Golic [14] suggested that state size should be at least double the size of key.

2.4 Distinguishing Attack

The most important criterion for a good stream cipher design is that keystream generation should be random. A distinguishing attack tries to identify that if a given keystream is a random sequence or a cipher or generator has created it.

Distinguishing attack tries to identify the relations between internal state variables and output keystream. The internal structure of a cipher has to be analyzed extensively for distinguishing attack. Distinguishing attack is a known keystream attack.

Fluhrer and McGrew introduced the idea of this attack on alleged RC4 key stream generator [18]. Some other works on this attack are Ekdahl and Johansson [19,53]; Goli´c and Menicocci [20]; Junod [21]; Watan-abe et al. [22]; Englund and Johansson [23]; Paul et al. [24]; Rose and Hawkes [25] and many more. In [26] Paul and Preneel unified distinguishing attacks into a single framework. Ciphers are required to use sufficiently long keystreams to avoid distinguishing attacks.

2.5 Algebraic Attack

Algebraic attacks are relatively new attacks for stream ciphers and progress is rapidly taking place in this field. Algebraic attacks are very much effective against LFSR based ciphers[17]. The basic principle of algebraic attacks is to model a cryptographic system in terms of algebraic equations. The first step of this attack is to find the set of algebraic equations that relate the initial state with the output keystream, then keystream bits are observed and these values are substituted into the equations. Attackers try to collect maximum possible keystream bits. Finally, this system of equations is solved to determine the initial state and then derive the secret key from it. Courtois in [27] against Toycrypt first proposed algebraic Attack on stream cipher and later it was used on LILI-128 [28]. This attack was also successfully applied to the stream ciphers with memory that were assumed to be more secure against this attack [29,30]. Later on Courtois further enhanced this attack and proposed Fast Algebraic attack [31] that was further strengthened by Armknecht [32]. The idea behind fast algebraic attack was to get equations of lower degree by linearly combining the equations before solving the system of equation that drastically increases the speed of the attack.

2.6 Correlation Attacks

Correlation attack is a class of known plaintext attack. These attacks are widely applicable to stream ciphers; especially to design based on feedback shift registers. A correlation attack tries to extract some information about the initial state from the output keystream by exploiting the weaknesses in the combining function of the design.

Siegenthaler first introduced the Correlation attack against combination generator [33] in 1985 but Meier and Staffelbach further improved this attack in 1988 as Fast Correlation Attack [34]. Zhang and Feng proposed an improved fast correlation attack on stream ciphers in [35]. This attack was further discussed and applied in [36, 37, 38, 39]. Correlation-immune functions need to be implemented for avoiding such attacks. In the case of LFSRs, the irregular clocking is one of the concepts to avoid linearity that will help countering this attack.

2.7 Guess-and-Determine Attacks

Guess and determine attacks are general attacks on stream ciphers. As it is clear from the name, in Guess and determine

attacks, an attacker guess a part of the internal state and try to recover the full value of internal states by observing the keystream using the guessed part and small amount of known keystream. In the end a part of keystream is generated using the guessed values and then it is compared with the known keystream to check the correctness of the guessed values. In [40] guess and determine attack was given against Polar Bear. Guess and determine attacks were also presented in [41] against SNOW. By irregular clocking, resistance against guess and determine attacks can be increased. Guess and determine attacks are more effective against word oriented stream ciphers [42].

2.8 Linear Masking Attacks

Linear masking attacks can be applied to those ciphers where some non-linear process resembling block cipher design exist and in which linear masking is used to hide this process. In these attacks first of all a non-linear characteristic is distinguished that exhibits some bias. Then we look at linear process and get some missing linear combinations. The same linear combinations are applied to the cipher output and we try to find the traces of distinguishing property. Coppersmith et al. in [43] described a generic attack on stream ciphers using linear masking. Watanabe et al. proposed linear masking attack on SNOW [44]. It is a form of Guess and Determine attack.

2.9 Related Key Attack

To provide a little bit of extra safety or security some of the cryptographic protocol limits the amount of data, which can be encrypted using a single key. In such cases either the new key is generated with using the IV (initialization vector) and with master key or to change the IV which in turns change the cipher key.

In such type of ciphers if the rekeying strategy relates the inputs to the internal states without sufficient non-linearity then cipher may become prone to a related key attack. These types of weaknesses are not very common in case of stream ciphers but there are some examples of related key attacks. Fluhrer et al. shown the related key attack on RC4 in [45] by exploiting a weakness of invariance in the key initialization algorithm. This weakness of RC4 was used by Stubblefield et al. to break the WEP protocol with practical complexity [46]. Sekar et al. presented a related key attack on Py-family of stream ciphers [47,48].

2.10 Divide and Conquer Attack

Divide and conquer is a common technique to divide the problem into small problems and try to solve the problem step by step. The same strategy is applied in case of divide and conquer attack where a cipher is partitioned into components and only a few key bits are determined in each stage. First the most vulnerable components are attacked. Siegenthaler [33] originally pointed out this concept. The attack can be termed as successful only if complexities of all the stages are smaller than the exhaustive key search. Some examples of attack are [49, 50]. High correlation immunity decreases the vulnerability to divide and conquer attack [51].

CONCLUSION

In this paper, we have tried to describe the existing cryptanalytic attacks on stream ciphers and countermeasures to these attacks have been suggested with different examples. These attacks are generally tried against any new cryptographic primitive at first. In order to develop a new secure stream cipher, it is very much necessary that these attacks should be taken into consideration during development and countermeasures of these attacks should be applied in the design, so that the new design is not vulnerable to these attacks. Though these are the available techniques in literature for cryptanalysis of the stream ciphers but generally combinations and variants of these attacks can be used in future and just by overcoming these attacks any cryptographic primitive cannot be assumed secure. We are working in the field of cryptanalysis for further enhancement of available attacks and their applications on available stream ciphers.

3. REFERENCES

[1] Christof Paar and Jan Pelzl. “Understanding Cryptography: A textbook for students and practitioners”, 2010 Springer p.7 ISBN 978-364204100-6

[2] W. Fischer, B. M. Gammel, O. Kniffler and J. Velton, “Differential Power Analysis of Stream Ciphers,” Topics in Cryptology-CT-RSA 2007, Springer-Verlag, LNCS, Vol. 4377, pp. 257–270, 2007.

[3] P. Kocher, J. Jaffe and B. Jun, “Differential Power Analysis”, in the Proceedings of Crypto 1999, LNCS, vol 1666, pp 398–412, Santa-Barbara, CA, USA, August 1999.

[4] J.-F. Dhem, F. Koeune, P.-A. Leroux, P. Mestré, J.-J. Quisquater, and J.-L. Willems, “A practical implementation of the timing attack”, Proc. CARDIS 1998, Smart Card Research and Advanced Applications (J.-J. Quisquater and B. Schneier, eds.), LNCS, Springer, 1998.

[5] P. Kocher, “Timing attacks on implementations of Diffe-Hellman, RSA, DSS, and other systems”, Advances in Cryptology - CRYPTO '96, Sant Barbara, California (N. Koblitz, ed.), LNCS, vol. 1109, Springer, 1996, pp. 104-113.

[6] K. Gandolfi, C. Mourtel and F. Olivier. “Electromagnetic Attacks: Concrete Results”. In the Pro-ceedings of the Workshop on Cryptographic Hardware and Embedded Systems 2001 (CHES 2001), LNCS 2162 Paris, France, May 2001, pp 251–261

[7] Jean–Jacques Quisquater and David Samyde. “Electro Magnetic Analysis (EMA): Measures and Counter-Measures for Smart Cards”. In Smart Card Programming and Security (E-smart 2001), Cannes, France, LNCS 2140, pp.200-210, September 2001.

[8] Agrawal, D., Archambeault, B., Rao and J.R., Rohatgi, P.: “The EM Side-Channel(s): Attacks and Assessment Methodologies”. In: Cryptographic Hardware and Embedded Systems – CHES 2002 (2002)

[9] Adi Shamir and Eran Tromer. "Acoustic cryptanalysis: on nosy people and noisy machines". Available from: http://www.wisdom.weizmann.ac.il/~tromer/acoustic/

[10] Y. Zhou and D. Feng, "Side-channel attacks: Ten years after its publication and the impacts on cryptographic module security testing", NIST Physical Security Testing Workshop, Hawaii, USA, Sep. 2005. Cryptology ePrint Archive, Report 2005/388, 2005, http://eprint.iacr.org

[11] Standaert and Francois-Xavier.: "Introduction to side-channel attacks", In Verbauwhede, I.M.R. (ed.) Secure Integrated Circuits and Systems, pp. 27–42. Springer, Heidelberg (2010) ISBN: 978-0-387-71827-9.

[12] H. R. Amirazizi and M. E. Hellman. "Time-memory-processor trade-offs". IEEE Transactions on Information Theory, 34(3):505–512, 1988.

[13] S. Babbage. "Improved exhaustive search attacks on stream ciphers". In ECOS 95 (European Convention on Security and Detection), 1995.

[14] J. D. Golic. "Cryptanalysis of alleged A5 stream cipher". In EUROCRYPT, pages 239–255, 1997.

[15] A. Biryukov and A. Shamir. "Cryptanalytic time/memory/data tradeoffs for stream ciphers". In T. Okamoto, editor, ASIACRYPT, volume 1976 of Lecture Notes in Computer Science, pages 1–13. Springer, 2000.

[16] A. Biryukov, A. Shamir, and D. Wagner. "Real time cryptanalysis of A5/1 on a pc". In B. Schneier, editor, FSE, volume 1978 of Lecture Notes in Computer Science, pages 1–18. Springer, 2000.

[17] Faheem Masoodi, Shadab Alam and M U Bokhari. "An Analysis of Linear Feedback Shift Registers in Stream Ciphers" .*International Journal of Computer Applications* 46(17):46-49, May 2012. Published by Foundation of Computer Science, New York, USA.

[18] S. Fluhrer and D. McGrew, "Statistical Analysis of the Alleged RC4 Keystream Generator", proceedings of FSE 2000, Lecture Notes in Computer Science 1978, pp. 19-30, Springer-Verlag, 2001.

[19] Ekdahl, P. and Johansson, T., "Distinguishing attacks on SOBER-t16 and SOBER-t32". In: Daemen, J., Rijmen, V. (Eds.), Fast Software Encryption 2002. Vol. 2365 of Lecture Notes in Computer Science. Springer-Verlag, pp. 210–224, 2002.

[20] Goli´c, J. and Menicocci, R., "A new statistical distinguisher for the shrinking generator", available at http://eprint.iacr.org/2003/041,2003 Accessed November 14, 2012.

[21] Junod, P., "On the optimality of linear, differ-ential and sequential distinguishers". In: Advances in Cryptology—EUROCRYPT 2003. Vol. 2656 of Lecture Notes in Computer Science. Springer-Verlag, pp. 17–32.

[22] Watanabe, D., Biryukov and A., Canniere, C. D., "A distinguishing attack of SNOW 2.0 with linear masking method". In: Selected Areas in Cryptography—SAC 2003. To be published in Lecture Notes in Computer Science. Springer Verlag.

[23] Englund, H. and Johansson., T., "A new distinguisher for clock controlled stream ciphers". In: Fast Software Encryption 2005. Lecture Notes in Computer Science. Springer-Verlag.

[24] S. Paul, B. Preneel, and G. Sekar, "Distinguishing Attacks on the Stream Cipher Py", proceedings of Fast Software Encryption 2006, Lecture Notes in Computer Science 4047, pp. 405-421, Springer-Verlag.

[25] G. Rose and P. Hawkes, "On the applicability of distinguishing attacks against stream ciphers", Preproceedings of the 3rd NESSIE Workshop, available online at http://eprint.iacr.org/2002/142.pdf

[26] Souradyuti Paul and Bart Preneel, "On the (In)security of Stream Ci-phers Based on Arrays and Modular Addition", Advances in Cryptology - proceedings of ASIACRYPT 2006, Lecture Notes in Computer Science 4284, pp. 69-83, Springer-Verlag, 2006.

[27] N. Courtois, "Higher order correlation attacks, XL algorithm and Cryptanalysis of Toyocrypt", ICISC 2002, LNCS 2587, Springer-Verlag, pp. 182-199, 2002.

[28] N. Courtois and W. Meier, "Algebraic attacks on stream ciphers with linear feedback", Advances in Cryptology, Eurocrypt 2003, LNCS 2656, Springer-Verlag, pp. 345-359, 2003.

[29] F. Armknecht and M. Krause, "Algebraic attacks on combiners with memory", Advances in Cryptology – Crypto 2003, LNCS 2729, Springer-Verlag, pp. 162-175, 2003.

[30] N. Courtois, Algebraic attacks on combiners with memory and several outputs, E-print archive, http://eprint.iacr.org/2003/125. Accessed November 14, 2012.

[31] N. Courtois, "Fast algebraic attack on stream ciphers with linear feedback", Advances in Cryptology - Crypto 2003, LNCS 2729, Springer-Verlag, pp. 176-194, 2003.

[32] F. Armknecht, "Improving fast algebraic attacks", Fast Software Encryption (FSE) 2004, LNCS 3017, Springer Verlag, pp. 65-82, 2004.

[33] T. Siegenthaler, "Decrypting a class of stream ciphers using ciphertext only," IEEE Trans. Computers, vol. C-34, no. 1, pp. 81–84, 1985.

[34] W. Meier and O. Staffelbach, "Fast Correlation Attacks on Stream Ciphers", Advances in Cryptology-EUROCRYPT'88, Lecture Notes in Computer Science, vol. 330, Springer-Verlag, 1988, pp. 301-314.

[35] B. Zhang and D. Feng, "An Improved Fast Correlation Attack on Stream Ciphers", Selected Areas in Cryptography Lecture Notes in Computer Science Volume 5381, 2009, pp 214-227

[36] M. Mihaljevic, M. Fossorier, and H. Imai, "A low complexity and high-performance algorithm for the fast correlation attack," Fast Software Encryption-FSE'2000, Lecture Notes in Computer Science, Springer-Verlag , vol. 1978 , 2001, pp. 194-212.

[37] A. Canteaut and M. Trabbia. "Improved fast correlation attacks using parity-check equations of weight 4 and 5". In Advances in Cryptology EUROCRYPT 2000, Springer-Verlag, 2000 volume LNCS 1807, pp. 573-588.

[38] T. Johansson, F. Jonsson, "Fast correlation attacks based on turbo code techniques", Advances in Cryptology, CRYPTO'99, Lecture Notes in Computer Science, vol. 1666, Springer-Verlag, 1999, pp. 181-197.

[39] S. Palit, B. Roy and A. De, "A Fast Correlation Attack for LFSR-Based Stream Ciphers", Lecture Notes in Computer Science, Volume 2846, Springer-Verlag, 2003, pp. 331 - 342.

[40] J. Mattsson. "A Guess and Determine Attack on the Stream Cipher Polar Bear". eSTREAM, ECRYPT Stream Cipher Project, Report 2006/017, 2006. http://www.ecrypt.eu.org/stream.

[41] P. Hawkes and G. G. Rose. "Guess-and-Determine Attacks on SNOW". In Selected Areas in Cryptography, pages 37–46, 2002.

[42] Philip Hawkes and Gregory G. Rose. "Exploiting Multiples of the Connection Polynomial in Word-Oriented Stream Ciphers", Proceedings of the 6th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology, p.303-316, December 03-07, 2000.

[43] D. Coppersmith, S. Halevi, and C. Jutla. "Cryptanalysis of stream ciphers with linear masking". In Advances in Cryptology - CRYPTO 2002, volume 2442 of Lecture Notes in Computer Science, pages 515 – 532, January 2002.

[44] D.Watanabe, A. Biryukov, and C. De Canniere. "A Distinguishing Attack of SNOW 2.0 with Linear Masking Method". In Selected Areas in Cryptography (SAC 2003), LNCS 3006, pp. 222{233, Springer-Verlag, 2004.

[45] Scott Fluhrer, Itsik Mantin, and Adi Shamir. "Weaknesses in the key scheduling algorithm of RC4". In Mitsuru Matsui, editor, Proceedings of the 8th International Workshop on Fast Software Encryption, volume 2355 of Lecture Notes in Computer Science, pages 1–24. Springer-Verlag, 2001.

[46] Adam Stubblefield, John Ioannidis, and Avi Rubin. "Using the Fluhrer, Mantin, and Shamir Attack to break WEP". Technical report, TD-4ZCPZZ AT&T Labs Technical Report, 2001.

[47] Sekar, G., Paul, S., & Preneel, B., "Related-key attacks on the Py-family of ciphers and an approach to repair the weaknesses". In LNCS Vol. 4859. Indocrypt'07 (pp. 58–72). Berlin: Springer, 2007.

[48] Bokahri, Shadab and Faheem. "A Review of Py (Roo) Stream Cipher and its Variants". In Proceedings of the 5th National Conference; INDIACom-2011

[49] Kevin Chen, Matt Henricksen, Leonie Simpson, William Millan and Ed Dawson. "A Complete Divide and conquer attack on the Alpha1 stream cipher". ICISC 2003, 6th International Conference, Seoul, November 27-28, 2003, Revised papers, volume 2971, of Lecture Notes In Computer Science page 418-431. Springer 2004.

[50] S. Khazaei, "Divide and Conquer Attack on ABC Stream Cipher". eSTREAM, ECRYPT Available at: http://www.ecrypt.eu.org/stream/papersdir/052.pdf.

[51] T. Siegenthaler, "Design of Combiners to Prevent Divide and Conquer Attacks", Advances in Cryptology-CRYPTO'85, H. C. Williams (Ed.), LNCS 218, Springer-verlag, 1986, pp. 273-279.

[52] J. Hong and P. Sarkar. "Rediscovery of time memory tradeoffs", 2005.

[53] Faheem Masoodi, Shadab Alam and M U Bokhari. "SOBER Family of Stream Ciphers: A Review". *International Journal of Computer Applications* 23(1):1–5, June 2011. Published by Foundation of Computer Science, New York, USA.