Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 46 (2015) 697 – 705

Procedia Computer Science

International Conference on Information and Communication Technologies (ICICT 2014)

RC4 Encryption-A Literature Survey

Poonam Jindal*, Brahmjit Singh

Electronics and Communication Engineering Department, National Institute of Technology, Kurukshetra 136119, India

Abstract

A chronological survey demonstrating the cryptanalysis of RC4 stream cipher is presented in this paper. We have summarized the various weaknesses of RC4 algorithm followed by the recently proposed enhancements available in the literature. It is established that innovative research efforts are required to develop secure RC4 algorithm, which can remove the weaknesses of RC4, such as biased bytes, key collisions, and key recovery attacks on WPA. These flaws in RC4 are still offering an open challenge for developers. Hence our chronological survey corroborates the fact that even though researchers are working on RC4 stream cipher since last two decades, it still offers a plethora of research issues. The attraction of community towards RC4 is still alive.

Peer-review under responsibility of organizing committee of the International Conference on Information and Communication Technologies (ICICT 2014)

Keywords: Biases; Symmetric key encryption; Stream cipher; RC4; WEP;

1. Introduction

The concept of security is generally interpreted as the idea of confidentiality of data being transmitted, particularly the digital information transmitted over the wireless network. However the need of confidentiality of information is indeed a social paradigm. Security is provided using cryptographic primitives. As shown in Fig. 1, the cryptographic primitives are classified into three main categories; not using key, symmetric key and asymmetric

* Corresponding author. Tel.: +91-9466620527.
E-mail address: poonamjindal81@nitkkr.ac.in

Peer-review under responsibility of organizing committee of the International Conference on Information and Communication Technologies (ICICT 2014)
doi:10.1016/j.procs.2015.02.129

key[1]. Although Fig. 1 is not presenting an exhaustive list of these primitives but is highlighting the important and relevant areas.

In this paper, we have focused on symmetric key ciphers which are also known as secret key or single key ciphers. Secret key ciphers are further classified as stream ciphers and block ciphers. In stream ciphers, one bit or a byte is processed/encrypted at a time, a key stream is produced which is a pseudorandom sequence of bits. A plaintext (a sequence of bits/bytes) is converted into ciphertext (again a sequence of bits/bytes of same length as that of plaintext) by hiding the plaintext with a keystream, using a simple XOR operation. Whereas in block ciphers, a block of bits/bytes/words is processed at a time. We have worked on stream ciphers which are further classified as synchronous and self-synchronous stream ciphers. Synchronous stream ciphers (SSC) are prominently discussed in literature. However, generally due to the design problems, self-synchronizing stream cipher (SSSC) are not much explored in literature and are less used in practice[2]. Different synchronous stream ciphers available in the literature are RC4, E0 (a stream cipher used in Bluetooth), A5/1 and A5/2 (stream ciphers used in GSM), SNOW 3G, ZUC (4G stream ciphers), Rabbit, FISH, and HC-256 etc.[3-6].

The strength of stream ciphers is the random keystream which ensures the computational security of the cipher. In cryptographic primitives non-random events which can be computationally recognized either in the internal states and in the output keystream are generally not desirable. Thus the cryptanalysis of stream ciphers is imperatively focused on the identification of non-random events and hence extensive analysis of stream ciphers is done till date to identify the occurrence of non-random events. Table 1 and Figs. (2, 3) demonstrates the overview of various cryptanalytic attack models, modes of attacks and goals of intruder in stream ciphers respectively. The general classification of the cryptanalytic attacks on stream ciphers with the assumption that what is known to the intruder is shown in Table. 1. These cryptanalytic attacks are also known as attack models. Further on the basis of these attack models and the knowledge of intruder (what is known to intruder), Fig. 2 presents the different modes in which the intruder can attack the cipher. Intruder mount these models and modes of attack on stream ciphers with the goals as shown in Fig. 3. In this paper we have presented the chronological comprehensive survey of the most prevalent and commercially used RC4 stream cipher. We have focused on RC4 because it outperforms amongst all the modern stream ciphers. Though the algorithm is publicly revealed in 1994 through internet but due to its simplicity everyone gets attracted towards it and has been adopted worldwide. The cipher has gained immense popularity due to its design simplicity and has been widely adopted in various software and web applications. It is used in various network protocols such as WEP (Wireless equivalent privacy), WPA (Wi-Fi protected access), and SSL (Secure socket layer). Also it is extensively used in Microsoft windows, Apple OCE (*Apple Open Collaboration Environment*), secure SQL (a server for database management and data warehousing solution) etc. It is found that regardless of many efforts made by researchers in improving the flaws of RC4 cipher, still there are number of biases exist in the keystream, key recovery can be made from state and certain sets of keys do exist that can generate similar states. It corroborate the fact that even after the decades of research, the RC4 stream cipher continues to offer research problems ofinterest to the researchers.

Rest of the paper is organized as follows. Related work is presented in section 2. Section 3 describes the various weaknesses observed in RC4 stream cipher. Existing proposals for the enhancement of the cipher are given in section 4. Conclusion and future scope is drawn in section 5.

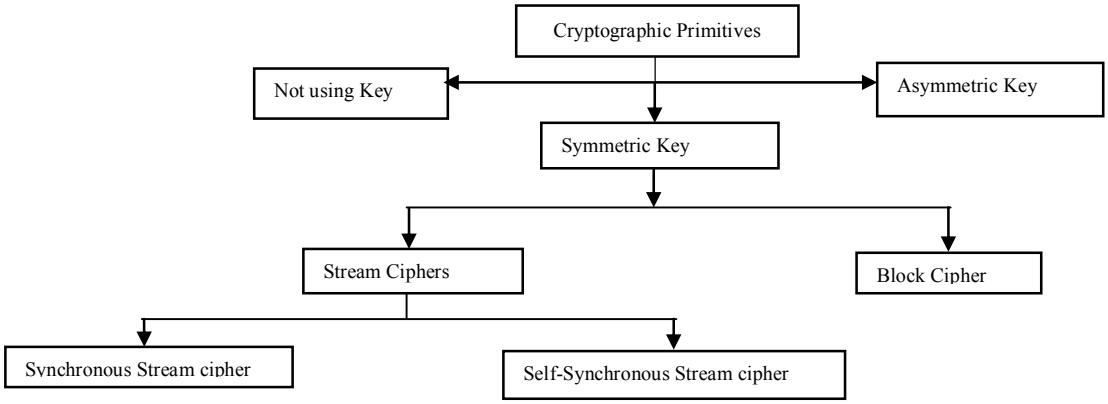


Fig. 1. Cryptographic primitives

Table 1. Broad Classification of the Cryptanalytic attacks on Stream ciphers (RC4)

Type of Cryptanalytic Attacks	**Information known to cryptanalytic**
Ciphertext only	Intruder has partial knowledge of some ciphertext (CT) messages but does not know anything about plaintext message (PT)
Known plaintext	Intruder has some knowledge of the PT-CT pairs
Chosen plaintext	Intruder knows the encryption algorithm that produces CT for the PT messages chosen by intruder using a secret key
Known initialization vector (IV)	Intruder either has some knowledge of IV or choose some IV and obtains the corresponding output keystream with the secret key. This is also known as re-synchronization attack and follows known plaintext attack for obtaining keystream and CT.
Chosen ciphertext	Intruder knows the encryption algorithm that produces PT for the CT messages chosen by intruder using a secret key

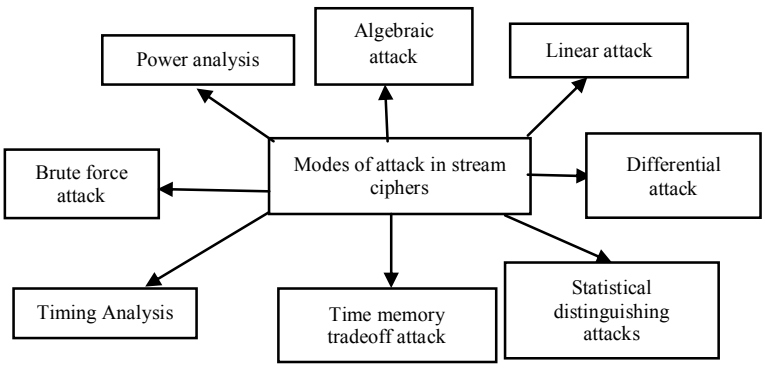


Fig. 2 Modes of attack in stream ciphers

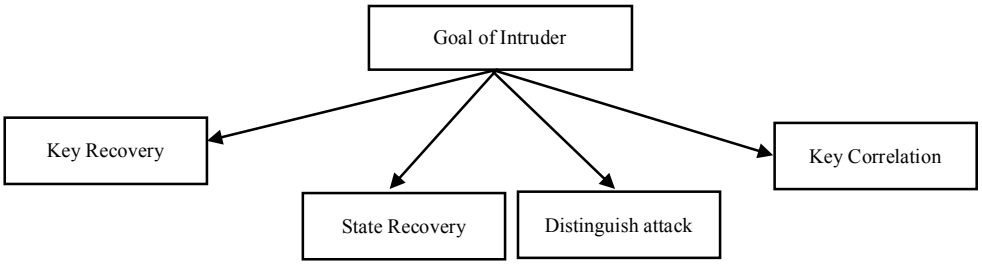
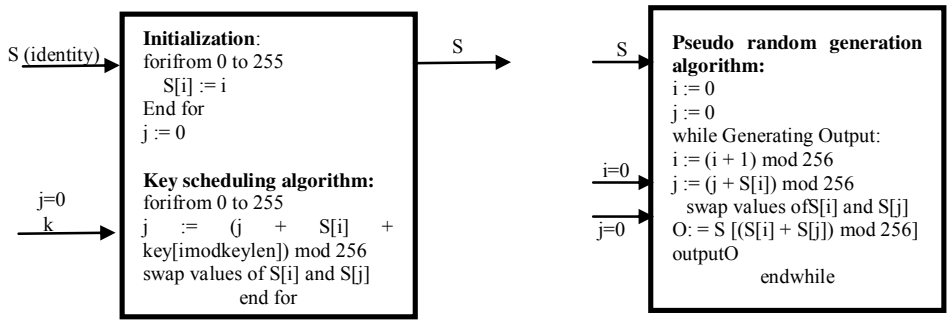


Fig. 3 Goal of Intruder



a) RC4 Key scheduling algorithm b) RC4 Pseudo random generation algorithm

Fig. 4 RC4 encryption

2. Related Work

RC4 is known to be one of the simplest and widely adopted cipher. However, the simplicity of RC4 makes it vulnerable to different security attacks. The cipher was designed in 1984 and was anonymously released on mails and news groups in 1994. Since then many cryptanalysts have worked on the weaknesses of the cipher. The basic functioning of RC4 is shown in Fig. 4 and shows that RC4 has two basic constituents; Key scheduling algorithm (KSA), Pseudo random number generator (PRGA). It is observed that PRGA generates a pseudorandom output sequence (bytes) from the permuted internal state which itself is a random sequence. The cryptanalyst is always in search of the statistical weaknesses of the output sequence. Statistical weaknesses are the biases in the random keystream that can be exploited with a very high probability of success, to differentiate the generated RC4 keystream from a truly random sequence of bytes.

Hence the main goal of an intruder while attacking RC4 is to investigate the non-random behavior either in the internal state or in the output keystream. The brief summary of security attacks on RC4 since its first public appearance to date is shown in Table 2. We have elaborated our discussion with the main focus on the security weaknesses of RC4 in WLAN protocols. For security provisioning RC4 is extensively used in WLAN security protocols. WEP (Wired equivalent privacy) was the first security protocol used for Wi-Fi security in IEEE 802.11 LANs and is based on RC4 encryption algorithm. Due to the number of attacks on WEP such as; related key attacks[7], Fluhrer, Mantin and Shamir attack (FMS)[8], Korek practical attacks[9], Mantin attack on RC4 [10] and WEP,

Klien attack[11], Tews, Weinmann and Pyshkin (TWP) attack[12], Vaudenay and Vuagnoux (VV) attacks[13], Tews and Beck (TB) attack[14], Shepehrdad, Vaudenay and Vuagnoux (SVV) attack[15-17], and Shepehrdad, Susil, Vaudenay and Vuagnoux (SSVV) attack[18], WEP was declared as an insecure protocol. Later it is replaced by WPA (Wi-Fi protected access) which also make use of RC4 as its core element. WPA defended against many attacks in WEP. WPA has again proved to be a weak protocol due to TB data injection attacks[14], and SVV attacks[17]. Further a new protocol WPA2 was proposed by the Wi-Fi alliance which uses AES block cipher as an encryption algorithm instead of RC4. Though WPA2 is a secure protocol, removing many weaknesses of WEP and WPA but its hardware based applications are not cost effective as compare to WEP and WPA where RC4 was used as a basic module. Inspite of so many attacks and weaknesses in WEP, it is enormously opted in large number of applications due to its simplicity over WPA and WPA2. RC4 is also broadly accepted in web security. It is used in TLS (Transport layer security) /SSL to offer security over the internet. The RC4 is known to the best choice for TLS/SSL as it can mitigate many attacks on the protocol. However recently in 2013 and 2014, a new security attack[19-22] on RC4 of TLS and WPA protocol has been proposed, but still RC4 is considered to be the most popular algorithm for protocol. Although there had been many successful security breaches in the protocols using RC4, but the striking combination of robustness and design elegance of RC4 has made it most preferred protocol for last two decades. Different researchers have proposed variety of its implementations to make the cipher more secure, but the available literature demonstrate the insecurity of RC4 till date. The most recent literature[19-22] on RC4 and its applications in WEP, WPA and TLS reveals the fact that the RC4 is still an attraction for community and also offer many research issues. It is the simplest protocol to date and offering variety of research issues even after years of analysis.

3. Weaknesses of RC4

KSA and PRGA are the two major constituents of RC4. A simple scrambling of input keystream and the initial state is performed in KSA and results in a new state, which is nothing more than an initial state permutation. A pseudorandom output byte sequence is generated from internal permutation after PRGA. Intruder attack the cipher with the intention, either to recover the original key or the internal state or the output keystream to have an access on the input message and the future messages. From the available literature, based on these two components of RC4 we have briefly summarized some of the weaknesses of RC4 as below:

- *Weak keys in RC4:*Weak keys are the small set of keys in RC4 which leaves some traces in the keystream generated after KSA or in the output bytes after PRGA. If such traces are followed by the intruder he/she can easily recover the key from the internal state or the output stream.
- *Biased bytes:* In stream ciphers the event or bytes are said to be biased if an event occurs with different probability as that from the uniformly random sequence of bits/bytes. To study the non-random behaviour of bytes is the goal of attacker. Several biases or correlation related to secret key, state variables, and short term and long term biases related to keystream bytes are there in RC4 KSA and PRGA.
- *Distinguishers:* if the events in RC4 are biased and are solely based on keystream bytes then such biased events are referred to as distinguishers.
- *Key collisions:* In RC4 KSA, it may be possible to generate a similar state even if two different keys are used and a similar output keystream will be produced. Such a scenario is known as key collision or related key pairs. Construction of such key pairs is the goal of attacker.
- *Key recovery from state:* RC4 PRGA is reversible in nature. From any given state of PRGA it is easy to reach the internal state and it is quite easy to recover the secret key from the internal state.
- *Key recovery from keystream:* Key can be easily recovered from output keystream and this weakness of RC4 was exploited in WEP and WPA.
- *State recovery:* the state-space size in RC4 is $N! \times N^2$, where N! is the space of N bytes in the internal state S and N^2 comes from the all possible combinations of indices *i andj*. Hence in RC4, for N=256 the total

state-space available is, $256! \times 265^2 \approx 2^{1700}$. Inspite of such a big state-space, the state recovery is possible in the cipher.

Table 2. Cryptanalysis on RC4 stream cipher

Year	Weak keys* and key recovery from state	Key recovery from key stream	State recovery attack	Biases and distinguishers
1995	-Roos [23] -Wagner weak keys[24]	-	-	-Roos biases[23]
1996	-	-	-	-Glimpse bias[20]
1997	-	-	-	-Golic long term bias[29]
1998	-	-	- KMP branch and bound approach [31]	
2000	-Related key-pairs[25]	-	-Iterative probabilistic cryptanalysis[32]	-Digraph biases [30]
2001	-	FMS WEP attack[8]	-	Broadcast attack[31]
2002	-	-	-	-
2003	-	-	State part known attack[32]	
2004	-	Korek WEP attack[9]	-	
2005	-	Mantin WEP attack[10]	-	
2006	-	Klein WEP attack[11]	-	-
2007	- short related keys attack	-TWP WEP attack[12] -VV WEP attack[13]	Hill climb search attack[33]	
2008	-Difference equations -key byte -bit by bit approach attack	-	-generative pattern[34] -iterative probabilistic attack[35]	Maitra and Paul conditional Bias[37]
2009	-key collision attacks -bidirectional search attacks	-TB WEP and WPA attacks[14]	-	-
2010		SVV WEP attack[15]	-	SVV biases in key and state variables[17]
2011	-New key collisions	SVV WEP and WPA attack[16]	-	-keylength biases[37]
2012	-	SVV WEP and WPA attack[17]	-	
2013	-Near colliding keys	SSVV passive attack on WEP[18]	-	-TLS and WPA attack[38]
2014	-	-	-	-biased bytes [22]

4. Enhancements in RC4 stream cipher

Due to the cryptanalytic attempts, many variants of RC4 have been proposed by researchers. We have reported some recent papers on the enhancements of RC4 algorithm. In[39] authors have studied theoretically the RC4 KSA. It is found that the expected number of times each value of the state permutation is moved by the indices *i, j* is not uniform. A modified RC4 with three layer scrambling is proposed. Analysis of RC4+ illustrates that the modified algorithm avoids some of the existing weaknesses of RC4. To increase the security of RC4, a new PRGA, based on conventional RC4 is proposed in[40-41]. It is revealed that the proposed RC4 has two internal states and has removed the foundation of many security attacks on RC4 and is also faster than the existing conventional RC4. In[42] authors have proposed a new variant of RC4 called Quad-RC4 without changing the basic structure of conventional RC4. The proposed RC4 structure promises the reasonable security and a high throughput. In term of speed the proposed cipher performs much better in comparison with HC-128, the fastest software stream cipher amongst the e-STREAM finalists.A new variant of RC4 known as FJ-RC4 is proposed by authors[43]. In FJ-RC4 is designed in a manner such that in KSA input key is divided into three parts and the structure of PRGA is same as with conventional RC4. A new keystream after KSA is generated in three rounds whereas PRGA performs only single round.Another variant of RC4 known as effective RC4 cipher is proposed[44] where the security analysis is performed by using Shannon's Secrecy theory and numerical values are obtained to analyse the secrecy. It is proposed that the improved RC4 cipher can be used in software applications where there is requirement of both the throughput and secrecy. Further a new PRGA RC4B is proposed in[45], which provides better immunity against the known attacks. The new variant of RC4 is proposed in[46] which provides high security along with long period of KSA keystream,

large complexity and having good statistical properties. In[47] authors have proposed a modified RC4 (MRC4) by modifying both KSA and PRGA. From the available literature it is found that many recent RC4 variants have been proposed by researchers. Some are targeted towards achieving better security by removing the non-uniformity of bytes or by removing the correlation between key and the state bytes and some towards better performance in terms of time or throughput. Some of the proposals have entirely changed the basic structure of RC4 which is generally not desirable because the robust design of RC4 is the basic strength of the cipher. However, inspite of so many proposals on RC4, many open issues related to the searches of more biases, key collisions in keystream, and key recovery attack on WPA exists on RC4 till date. Therefore there is a strong need of the modifications of RC4 without changing the basic structure of RC4. It is recommended that while considering these existing weaknesses of RC4 one can design a new enhanced RC4 stream cipher exhibiting a sufficient resistance against the existing weaknesses of the cipher.

5. Conclusion

In this paper, we have presented the chronological survey of the cryptanalysis on the RC4 since its first public appearance to date. It is found that the simple and robust structure of RC4 is still attracting the community. It is extensively deployed in wireless network and internet protocols. We have presented a broad classification of the existing weaknesses in RC4 followed by the measure taken by various researchers to improve the security of the cipher by removing the existing weaknesses. Although many improved variants of RC4 which removes the existing weaknesses and enhance the security of the cipher may be found in the literature, but the question about which is the best solution still remain unanswered, since each of them focus on specific attack or weakness. Further inspite of all the developments reported in the literature, there are still many open research challenges and issues related to searches of more biases, key collisions in keystream, and key recovery attack on WPA. Therefore it is concluded that there is ample scope to further investigate the issues in RC4 particularly the non-random behavior of bytes in the state permutation, and to develop a new, more efficient and effective RC4 encryption algorithm.

References

1. Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. Hand- book of Applied Cryptography. CRC Press, August 2011 edition, 1996. Fifth Printing.
2. Douglas R. Stinson. *Cryptography: Theory and Practice*. CRC Press, third November 2005) edition, 1995.
3. Alex Biryukov, Adi Shamir, and David Wagner. Real time cryptanalysis of A5/1 on a PC. In Bruce Schneier, editor, *FSE*, volume 1978 of *Lecture Notes in Computer Science*, p. 1–18. Springer, 2000.
4. Marc Briceno, Ian Goldberg, and David Wagner. A pedagogical implementation of the GSM A5/1 and A5/2 “voice privacy” encryption algorithms. Available online at http://www.scard.org/gsm/a51.html, 1998.
5. 3rd Generation Partnership Project. Specification of the 3GPP confidentiality and integrity algorithms UEA2 & UIA2. ETSI/SAGE Specification Document 2: SNOW 3G Specification, v1.1, September 6, 2006.
6. ECRYPT Stream Cipher Project eSTREAM. Software performance results from the eSTREAM project. Available online at http://www. ecrypt.eu.org/stream/perf/#results.
7. Ronald L. Rivest. RSA security response to weaknesses in key scheduling algorithm of RC4. Technical note, RSA Data Security, Inc., 2001.
8. Scott R. Fluhrer, Itsik Mantin, and Adi Shamir. Weaknesses in the key scheduling algorithm of RC4. In Serge Vaudenay and Amr M. Youssef, editors, *Selected Areas in Cryptography*, volume 2259 of *Lecture Notes in Computer Science*, p. 1–24. Springer, 2001.
9. Korek. Need security pointers. Published online at http://www.netstumbler.org/showthread.php?postid=89036#pos%t89036, 2004.
10. Itsik Mantin. A practical attack on the fixed RC4 in the WEP mode. In Bimal K. Roy, editor, *ASIACRYPT*, volume 3788 of *Lecture Notes in Computer Science*, p. 395–411. Springer, 2005.
11. Andreas Klein. Attacks on the RC4 stream cipher. *Des. Codes Cryptography*, 48(3):269–286, 2008. Published online in 2006, and accepted in WCC 2007 workshop.
12. Erik Tews, Ralf-Philipp Weinmann, and Andrei Pyshkin. Breaking 104 bit WEP in less than 60 seconds. In Sehun Kim, Moti Yung, and Hyung- Woo Lee, editors, *WISA*, volume 4867 of *Lecture Notes in Computer Science*, p 188–202. Springer, 2007.
13. Serge Vaudenay and Martin Vuagnoux. Passive-only key recovery attacks on RC4. In Carlisle M. Adams, Ali Miri, and Michael J. Wiener, editors, *Selected Areas in Cryptography*, volume 4876 of *Lecture Notes in Computer Science*, p. 344–359. Springer, 2007.
14. Erik Tews and Martin Beck. Practical attacks against WEP and WPA. In David A. Basin, Srdjan Capkun, and Wenke Lee, editors, *WISEC*, p. 79–86. ACM, 2009.

15. Pouyan Sepehrdad. *Statistical and Algebraic Cryptanalysis of Lightweight and Ultra-Lightweight Symmetric Primitives*. PhD thesis No. 5415, École Polytechnique Fédérale de Lausanne (EPFL), 2012. Available online at http://lasecwww.epfl.ch/~sepehrdad/Pouyan_Sepehrdad_PhD_Thesis.pdf.
16. Pouyan Sepehrdad, Serge Vaudenay, and Martin Vuagnoux. Discovery and exploitation of new biases in RC4. In Alex Biryukov, Guang Gong, and Douglas R. Stinson, editors, *Selected Areas in Cryptography*, volume 6544 of *Lecture Notes in Computer Science*, p. 74–91. Springer, 2010.
17. Pouyan Sepehrdad, Serge Vaudenay, and Martin Vuagnoux. Statistical attack on RC4 - distinguishing WPA. In Kenneth G. Paterson, editor, *EUROCRYPT*, volume 6632 of *Lecture Notes in Computer Science*, p. 343–363. Springer, 2011.
18. Pouyan Sepehrdad, Petr Susil, Serge Vaudenay, and Martin Vuagnoux. Smashing WEP in a passive attack. In *Fast Software Encryption (FSE)*, 2013.
19. Santanu Sarkar, Sourav Sen Gupta, Goutam Paul, and Subhamoy Maitra. Proving TLS-attack related open biases of RC4. *IACR Cryptology ePrint Archive*, 2013:502, 2013.
20. Subhamoy Maitra and Sourav Sen Gupta. New long-term glimpse of RC4 stream cipher. In Aditya Bagchi and Indrakshi Ray, editors, *ICISS*, volume 8303 of *Lecture Notes in Computer Science*, p. 230–238. Springer, 2013.
21. Kenneth G. Paterson, Bertram Poettering, and Jacob C.N. Schuldt. Plaintext recovery attacks against WPA/TKIP.IACR Cryptology ePrint Archive, 2013:748, 2013
22. Sourav Sen Gupta, Subhamoy Maitra, Goutam Paul, Santanu Sarkar: (Non-) Random Sequences from (Non-) Random Permutations - Analysis of RC4 Stream Cipher.J. Cryptology 27(1): 67-108 (2014)
23. Andrew Roos. A class of weak keys in the RC4 stream cipher. Two posts in sci.crypt, message-id 43u1eh$1j3@hermes.is.co.za and 44ebge$llf@hermes.is.co.za, 1995. Available online at http://www.impic.org/papers/WeakKeys-report.pdf.
24. David A. Wagner. My RC4 weak keys. Post in sci.crypt, messageid 447o1l$cbj@cnn.Princeton.EDU, 1995. Available online at http://www.cs.berkeley.edu/~daw/my-posts/my-rc4-weak-keys.
25. Alexander L. Grosul and Dan S. Wallach. A related-key cryptanalysis of RC4. Technical Report TR-00-358, Department of Computer Science, Rice University, 2000.
26. Robert J. Jenkins Jr. ISAAC and RC4. Published on the Internet at http://burtleburtle.net/bob/rand/isaac.html, 1996.
27. Jovan Dj. Golic. Linear statistical weakness of alleged RC4 keystream generator. In Walter Fumy, editor, *EUROCRYPT*, volume 1233 of *Lecture Notes in Computer Science*, p. 226–238. Springer, 1997.
28. Lars R. Knudsen, Willi Meier, Bart Preneel, Vincent Rijmen, and Sven Verdoolaege. Analysis methods for (alleged) RC4. In Kazuo Ohta and Dingyi Pei, editors, *ASIACRYPT*, volume 1514 of *Lecture Notes in Computer Science*, p. 327–341. Springer, 1998.
29. Jovan Dj. Golic. Iterative probabilistic cryptanalysis of RC4 keystream generator. In Ed Dawson, Andrew Clark, and Colin Boyd, editors, *ACISP*, volume 1841 of *Lecture Notes in Computer Science*, p. 220– 233. Springer, 2000.
30. Scott R. Fluhrer and David A. McGrew. Statistical analysis of the alleged RC4 keystream generator. In Bruce Schneier, editor, *FSE*, volume 1978 of *Lecture Notes in Computer Science*, p. 19–30. Springer, 2000.
31. Itsik Mantin and Adi Shamir. A practical attack on broadcast RC4. In Mitsuru Matsui, editor, *FSE*, volume 355 of *Lecture Notes in Computer Science*, p. 152–164. Springer, 2001.
32. Yoshiaki Shiraishi, Toshihiro Ohigashi, and Masakatu Morii. An improved internal-state reconstruction method of a stream cipher RC4. In M.H. Hamza, editor, *Communication, Network, and Information Security, Track 440–088*, New York, USA, December 2003.
33. Violeta Tomasevic, Slobodan Bojanic, and Octavio Nieto-Taladriz. Finding an internal state of RC4 stream cipher. *Inf. Sci.*, 177(7):1715–1727, 2007.
34. Alexander Maximov and Dmitry Khovratovich. New state recovery attack on RC4. In DavidWagner, editor, *CRYPTO*, volume 5157 of *Lecture Notes in Computer Science*, p. 297–316. Springer, 2008.
35. Jovan Dj. Golic and Guglielmo Morgari. Iterative probabilistic reconstruction of RC4 internal states. *IACR Cryptology ePrint Archive*, 2008:348, 2008.
36. Riddhipratim Basu, Shirshendu Ganguly, Subhamoy Maitra, and Goutam Paul. A complete characterization of the evolution of RC4 pseudo random generation algorithm. *J. Mathematical Cryptology*, 2(3):257–289, 2008.
37. Sourav Sen Gupta, Subhamoy Maitra, Goutam Paul, and Santanu Sarkar. Proof of empirical RC4 biases and new key correlations. In Ali Miri and Serge Vaudenay, editors, *Selected Areas in Cryptography*, volume 7118 of *Lecture Notes in Computer Science*, p. 151–168. Springer, 2011.
38. Nadhem AlFardan, Dan Bernstein, Kenneth G. Paterson, Bertram Poettering, and Jacob C.N. Schuldt. On the security of RC4 in TLS. In *USENIX Security Symposium*, 2013. Presented at FSE 2013 as an invited talk [14] by Dan Bernstein. Full version of the research paper and relevant results are available online at http://www.isg.rhul.ac.uk/tls/.
39. Maitra, S., & Paul, G. Analysis of RC4 and proposal of additional layers for better security margin. In *Progress in Cryptology-INDOCRYPT 2008* (p. 27-39). Springer Berlin Heidelberg.
40. Xie, J., & Pan, X. An improved RC4 stream cipher. In *Computer Application and System Modeling (ICCASM), 2010 International Conference on* (Vol. 7, p. V7-156). IEEE.
41. Hammood, M. M., Yoshigoe, K., & Sagheer, A. M. (2013). RC4-2S: RC4 Stream Cipher with Two State Tables. In *Information Technology Convergence* (p. 13-20). Springer Netherlands.
42. Paul, G., Maitra, S., & Chattopadhyay, A. Quad-RC4: Merging Four RC4 States towards a 32-bit Stream Cipher. *IACR Cryptology ePrint Archive*, *2013*, 572.
43. Kherad, F. J., Naji, H. R., Malakooti, M. V., & Haghighat, P. A new symmetric cryptography algorithm to secure e-commerce transactions. In *Financial Theory and Engineering (ICFTE), 2010 International Conference on* (p. 234-237). IEEE.
44. Weerasinghe, T. D. B. An Effective RC4 Stream Cipher. *IACR Cryptology ePrint Archive*, *2014*, 171.
45. Lv, J., Zhang, B., & Lin, D. Distinguishing Attacks on RC4 and A New Improvement of the Cipher. *IACR Cryptology ePrint Archive*, *2013*, 176.

46. Khine, L. L. A New Variant of RC4 Stream Cipher. *World Academy of Science, Engineering and Technology*, *50*.
47. Jindal, P., & Singh, B. (2014, May). Performance analysis of modified RC4 encryption algorithm. In *Recent Advances and Innovations in Engineering (ICRAIE), 2014* (p. 1-5). IEEE.