State of the Art Realistic Cryptographic Approaches for RC4 Symmetric Stream Cipher

Disha Handa and Bhanu Kapoor

Department of Computer Science Engineering, Chitkara University, Himachal Pradesh

ABSTRACT

In many of today's computer application needs, faster operation is essential to the efficient implementation of information security algorithm. RC4 has been used as the data encryption algorithm for many applications and protocols including the Wi-Fi, Skype, and Bit Torrent to name a few. Several efficient approaches to the implementation of RC4 have been proposed and we review some of those. More recently some parallel approaches to faster implementation of RC4 have been presented and we include those in our survey of efficient approaches to RC4. This paper presents an analysis of available hardware/software parallel implementations of RC4 symmetric key-based algorithm and some security approaches which make it more secure.

KEYWORDS

Parallel cryptography, Cryptography, Security, RC4, Parallel RC4, Stream Cipher

1.INTRODUCTION

The Internet is the worldwide interconnection of networks operated by industry, academia, government and private parties. Initially the Internet is used to interconnect laboratories affianced in government research projects, and since 1994 it has been expanded to serve millions of users for simple routine as well as complex tasks. The Internet, as no other communication medium, has become the Universal source of information for millions of people at school, at home and at work. But the other side of the coin is we have to make sure that our communications are safe while transmitting over the internet. It is sensible to suppose that at some point someone may capture and alter your transmissions. So we should use some form of encoding at the sender level and decoding at receiver to protect the data from unauthenticated parties. To safeguard the data from unauthorized use over the channel encryption/decryption process is used. It allows data to be transmitted that will be ineffective to anyone who intercepts it.

Different encryption algorithms have been used to secure information communications over the network. Furthermore the encryption algorithms are categorized into two categories: Public key infrastructure based known as Asymmetric algorithm and private key infrastructure based also known as symmetric algorithm. In private key algorithms, same key is used for both encryption and decryption process. It's called private key encryption because sender and receiver must know before the message is sent how to interpret the message. RC4 [1-4] is a very popular symmetric stream cipher algorithm. Some other algorithms include DES, 3-DES, and AES [1][12]. Public key algorithms use different keys for encryption and decryption process. Public key means that anyone can publish his or her method of encryption publish a key for his or her messages, and only the recipient can read the messages. This type of encryption is based on the mathematical logic of finding two prime factors of a very large number. In general it is easy to multiply two

DOI:10.5121/ijcsa.2014.4403

very large numbers together, but it is very difficult to take a very large number and find its two prime factors. RSA [1] is the commonly used asymmetric encryption algorithm.

Although security algorithms have many advantages like security of data transmitted over the channel yet there are some disadvantages involved in these algorithms. Intensive computation and their sequential structure affect the speed of the cipher. The speed of the encryption and decryption is a very important aspect of security algorithms [1-4] in working with applications. A slow cryptographic algorithm can slow the speed of an application and reduce its effectiveness. Sequential security algorithms can be made faster using parallelization. Fortunately, with the advent of parallel processors in computing, we now have easily available means to parallelize the algorithms to make them faster. It is possible to use parallel algorithms for any of the cryptographic techniques [8] currently in use.

RC4 has been used as the data encryption algorithm for many applications and protocols. Some of the protocols and applications using RC4 include the Wi-Fi, Skype, and Bit Torrent, to name a few. Several efficient approaches to the implementation of RC4 have been proposed and we review some of those. Our survey on RC4 is based on two common categories: Security and Speedup. This paper presents an analysis of latest work been done on RC4 to attain speedup using multi core technology and to achieve more security with modification in structure.

In Section 2, we discuss some of the basics of cryptography along with the classification of the cryptographic algorithms. Section 3 describes the RC4 symmetric stream cipher algorithm along with its key steps. Section 4 discusses some of the state of the art approaches to the implementation of RC4 that improves security and throughput of the algorithm. Section 5 discusses some of the parallel approaches to improve the performance of the RC4 algorithm followed by the conclusion of the survey paper.

2. BASICS OF CRYPTOGRAPHY

Cryptography is the art of information security. This word is derivative of the Greek *kryptos*, which means *to hide*. Cryptography includes methodologies such as merging words with images, microdots and other ways to hide information in transit or storage. In today's computer-centric world, cryptography converts the ordinary text into an unreadable format so that unauthorized parties cannot read the data. The ordinary text is referred as the plaintext and the scrambled text is known as the cipher text. The whole process of this conversion is known as encryption and the reverse process is known as decryption. Modern cryptography [3][4] concerns itself with the following objectives:

1) **Confidentiality** refers to restrictive information access and revelation to authorized users and preventing access to unauthorized users.
2) **Integrity** refers to the reliability of information resources.
3) **Non-repudiation** means at a later stage the source of the information cannot refuse his or her intentions in the transmission of the information.
4) **Authentication** refers to the process of confirming the identities of the sender and the receiver as well as the source and the destination of the information.

In general, two major cryptographic schemes are used to encrypt data transmitted over the internet: symmetric and asymmetric encryption schemes. In the symmetric technique, both the sender and the receiver use the same key. Symmetric techniques are broadly divided into two sub-categories: stream ciphers and block ciphers. Stream ciphers operate on streams of plaintext and cipher text one bit or byte at a time. The length of the key is same as the length of the data. On the other hand, block ciphers

operate on a specific length block of data at a time and keys are much shorter. The common classification of cryptography techniques is shown in Figure 1.

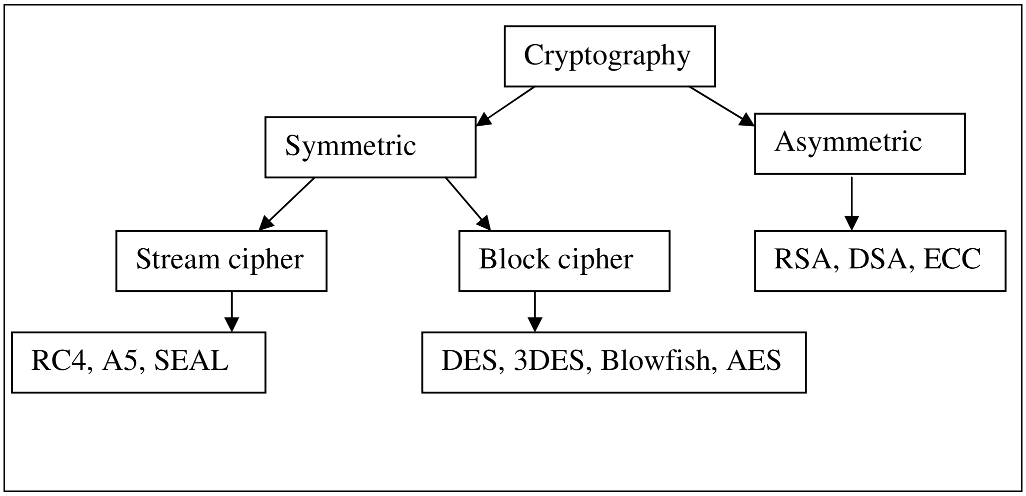

Figure 1: Classification of Cryptography Techniques

Asymmetric algorithms use different keys for encryption and decryption process. One of the keys is a public key. Public key means that anyone can publish his or her method of encryption publish a key for his or her messages, and only the recipient can read the messages. The other key is a private and only the receiver of the data has that key. Any data encrypted with his/her public key can be decrypted using the private key. Commonly used asymmetric algorithms are RSA, DSA and ECC.

3. RC4 METHOD

RC4 [1][2] is a stream cipher algorithm that has been used as the data encryption algorithm for many applications and protocols. Some of the protocols and applications using RC4 include the Wi-Fi, Skype, and Bit Torrent. RC4 generates a key-stream. This key-stream is used to encrypt data by combining it with the plaintext using bit-wise Xor (Exclusive-or) operation. The same way decryption can be performed as exclusive-or is the symmetric operation. To produce the key-stream, the algorithm makes use of an internal state which consists of two parts:

1) A transformation of all 256 possible bytes (denoted "S" below).
2) Two 8-bit index-pointers (denoted "i" and "j").

The transformation is initialized with a variable length key using Key Scheduling Algorithm (KSA).

Afterwards, the stream of bits is generated using the pseudo-random generation algorithm (PRGA).

3.1 Key Scheduling Algorithm (KSA)

The key-scheduling algorithm is used to initialize the “S” array. The "key-length" is defined as the number of bytes in the key. First, the array "S" is initialized with values from 0 to 255. Then 256 times the swap functionality is used to scramble the array elements. This is shown in Figure 2.

```
for i from 0 to 255
    S[i] := i
endfor
j := 0
for i from 0 to 255
    j := (j + S[i] + key[i mod key-length]) mod 256
    swap values of S[i] and S[j]
End for
```

Figure 2. Key scheduling in RC4

3.2 Pseudo-Random Generation Algorithm (PRGA)

After KSA generates the key-stream, the PRGA modifies the state and produces a byte as an output. In every iteration, the PRGA increments i, looks up the i^{th} element of S, in S[i], and adds that to j, afterwards exchanges the values of S[i] and S[j], and then uses the sum of S[i] , S[j] (modulo 256) as an index to obtain a next element of S, which is XORed with the next byte of the message to generate the next byte of either cipher text or plaintext. The whole process is dependent on the swap functionality. This is shown in Figure 3.

```
i := 0
j := 0
while Generating Output:
    i := (i + 1) mod 256
    j := (j + S[i]) mod 256
    swap values of S[i] and S[j]
    K := S[(S[i] + S[j]) mod 256]
  output K
  End While
```

Figure 3. Generation of pseudo-random output stream

4. STATE OF THE ART SYMMETRIC CRYPTOGRAPHIC APPROACHES TO ACHIEVE SECURITY AND THROUGHPUT

Due to its simplicity, RC4 has remained a focus area for many researchers over the years. Despite its weaknesses, it is a widely used algorithm and also used in SSL/TLS protocol. Researchers have suggested many different methods to implement RC4. We have listed some of the different approaches for RC4 that have been presented in the recent years since 2004. Each of these approaches has its own strengths and weaknesses. Table 1 lists and summarizes some of these recently presented approaches to make RC4 more efficient in terms of security.

Table-1: State of the art approaches to make RC4 more secure and fast

Sr.No	***Author***	***Technique***	***Publication year***	***Outcome***
1	Souradyuti Paul and Bart Preneel	Software approach	2004	Security Improvements
2	Peisong Ye and Guangxue Yue2	Software/Hardware approach	2010	WLAN security enhancements
3	Seifedine Kadry and Mohamad Smaili	Software approach	2010	Security improvements
4	Pardeep and Pushpendra Kumar Pateriya	Software approach	2012	Security improvements but key overhead
5	Laxmi Mounika et al	Software approach	2012	Security improvements
6	Prabhudesai Keval Ketan et al	Software approach	2012	Secure and fast hybrid cipher
7	Chandramouli et al	Software/Hardware approach	2006	Low power execution
8	Sourav Sen Gupta et al	Software/Hardware approach	2011	High throughput
9	Nadhem J. et al	Software approach	2013	The results are based on attacks.
10	Jagdeep Singh, Kundan Munjal	Software approach	2013	Enhanced security
11	R.Prabu	Software/Hardware approach	2014	Faster execution
12	Sivalingham Latchmanan et al	Comparative study of RC4 and E0	2012	Reduction of energy consumption while encryption took place.

Souradyuti Paul and Bart Preneel presented "*A New Weakness in the RC4 Key stream Generator and an Approach to Improve the Security of the Cipher*" [15]. RC4A uses fewer operations per output byte and offers the prospect of implementations that can exploit its inherent parallelism to improve its performance further. The paper is appeared in Fast Software encryption, FSE 2004, Lecture Notes in Computer Science, Springer-Verlag, pp. 245–259, 2004 and it improved the security of RC4 by introducing more random variables in the output generation process.

Peisong Ye and Guangxue Yue2 presented "*Security Research on WEP of WLAN*" [20]. This paper introduces the software and hardware based simulative platform to crack RC4 keys. Authors also provide some improvements to enhance the WLAN security as results shows that WLAN based on WEP and RC4 is insecure. The paper is presented in the Proceedings of the Second International Symposium on Networking and Network Security China, 2-4, April. 2010, pp. 039-042 and the final result show that the WLAN based on WEP is insecure and they give some improvements to enhance the WLAN security.

Seifedine Kadry and Mohamad Smaili presented "*An Improvement of RC4 Cipher Using Vigenère Cipher*" [19]. This paper presents the new algorithm named VRC4 which is the combination of RC4 and poly alphabetic cipher Vigenère. The technique is based on the double encryption method. That means the message is encrypted using the original RC4 cipher then re-encrypt the resulted cipher text using Vigenère cipher. The paper is published in International Journal of

Computational Intelligence and Information Security, Vo. 1 No. 3, May 2010 and the approach improves the security of RC4 due to the use of double encryption.

Pardeep and Pushpendra Kumar Pateriya presented "*PC1-RC4 and PC2-RC4 Algorithms: Pragmatic Enrichment Algorithms to Enhance RC4 Stream Cipher Algorithm*" [16].This paper introduces the improved RC4 algorithm named as ""PC1-RC4" and "PC2-RC4".The purpose of the development is to improve the security of the algorithm. The paper is published in International Journal of Computer Science and Network (IJCSN), Volume 1, Issue 3, June 2012 and the outcome is more secure but key management overhead increases as two keys are used.

Laxmi Mounika et al presented "*Remodelling RC4 Algorithm for Secure Communication for WEP/WLAN Protocol*" [18].The paper is based on the security analysis and presenting a way to improve security of RC4 stream cipher algorithm. The paper is published in Global Journal of researches in engineering Electrical and electronics engineering Volume 12 Issue 5 Version 1.0 April 2012 and the resultant output is improvements on linear and IV weaknesses.

Prabhudesai Keval Ketan et al presented "*A hybrid approach to achieve more security*". The purpose of the paper is to present a new algorithm which is the combination of two common symmetric ciphers (AES known for its security) and (RC4 known for its speed)[12]. The paper is published in International Journal of Computer Applications (0975 – 8887), 2012.

Chandramouli et al presented "*Battery Power-Aware Encryption*"[24]. In this paper, a hardware/software set-up to measure the battery power consumption of encryption algorithms through real-life experimentation has been discussed. The paper is published in ACM Transactions on Information Systems and Security, 9 (2), 162-180, 2006.The focus of the paper is Low power execution of cryptography algorithms.

Sourav Sen Gupta et al presented "*Proof of empirical RC4 biases and new key correlations*"[23].Authors presented the method which is the combination of hardware pipeline and loop unrolling to design an architecture that generate two RC4 key-stream bytes per clock cycle. The implemented is based on VHDL description, synthesized with 130, 90, and 65 nm fabrication technologies at clock frequencies 625 MHz, 1.37 GHz, and 1.92 GHz. The paper is part of Lecture Notes in Computer Science, pages 151–168. Springer, 2011 and the output is High throughput, hardware implementation of PC4 to improve upon the RC4 biases.

Nadhem J. et al presented "*recovery attacks against Transport Layer Security*" when RC4 is elected for encryption. Attacks put together on recent advances in the arithmetical analysis of RC4 [21]. The paper is the part of the proceedings of the USENIX Security Symposium, 2013 and the results are supported by an investigational evaluation of the feasibility of the attacks.

Jagdeep Singh, Kundan Munjal presented the implementation of two additional key matrices Key1 and Key2 created on the behalf of key size mentioned by the user and two state matrices having 256 bytes to enhance security in RC4. Author named the algorithm as "Robust RC4"[22]. The paper is published in International Journal of Engineering Research & Technology (IJERT), 2013.

R.Prabu presented "*loop unrolling approach implemented using VHDL*" [13]. This paper proposes the RC4 implementation with the help of loop unrolling and hardware pipeline. Author has implemented the proposed architecture using VHDL description Synthesized with 65nm fabrication technology at clock frequency of 1.37 GHz. The paper is published in International Journal of Innovative Research in Computer and Communication Engineering, 2014.

Sivalingham Latchmanan et al introduced RC4 encryption algorithm as a strong replacement of E0 to overcome the power limitations that mobile devices exhibit in 2012. Authors presented a simulated study to confirm the applicability of RC4 by comparing execution time and memory usage by RC4 and E0 [17].

5.STATE OF THE ART PARALLEL IMPLEMENTATIONS OF RC4 SYMMETRIC STREAM CIPHER

As we have seen in Table-1 that many researchers have done significant work on the RC4 algorithm to achieve better security in the algorithm. Although RC4 is provides faster execution but with the advent of parallel processing era, the requirement of scalable security algorithm increases so that these security algorithms can be executed using multi core processors to achieve faster execution. There have been different parallel approaches for RC4 that is summarized in Table 2.

Table-2: State of the art parallel symmetric cryptographic approaches

Sr.No	*Type of Implementation*	*Author*	*Presentation year*
1	FPGA Implementation	Tsoi, K.H. et al	2002
2	Hardware Implementation	Duhyun Bae et al	2005
3	Software implementation (GPU)	Changxin Li, Hongwei Wu, et al	2009
4	Software Implementation	T.D.B Weerasinghe	2012
5	Embedded(hardware/software) Implementation	Goutam Paul, Subhamoy Maitra et al	2012
6	Embedded(hardware/software) Implementation	Rourab Paul	2012
7	Hardware Implementation	S.S Gupta et al	2013
8	Software implementation (SIMD model)	D.Handa and B.kapoor	2014
9	Embedded(hardware/Software)	R.Prabu	2014

T. Soi presents "*An Extremely Parallel RC4 Key Search Engine*" and is presented in the proceedings of Field-Programmable Custom Computing Machines; 2002[7]. The implementation is based on FPGA hardware. The design uses parallelism at the logic level to execute many operations per cycle. To achieve high memory bandwidth, it uses on-chip memories and floor planning to condense routing delays and several decryption units to achieve more parallelism. Overall, 96 RC4 decryption engines were incorporated on a single Xilinx Virtex XCV1000-E field programmable gate array (FPGA).

The resulting model operates at a 50 MHz clock rate and gains a search speed of 6.06 × 106 keys/second, which is a speedup of 58 over a 1.5 GHz Pentium 4 PC.
Duhyun Bae presents "*Implementation of High performance Rc4 cipher engine for IEEE 802.11i*" This research was supported by the Ministry of information and communication (MIC), Korea under the chung-Ang university and published as chapter in springer-verlag Berlin Heidelberg, 2005[25]. The paper focuses on the reduction of response time using parallel hardware architecture for IEEE 802.11i to support new methods. Authors were able to decrease the

processing overhead of RC4 key arrangement by means of using the double S-Box method. The proposed model condenses the processing time to half in contrast with the sequential. Additionally, it also helps to reduce power consumption in CMOS design process as the clock frequency decreases to 1/5 and the area doubles compared to the typical designs.

Changxin Li presents "*An Efficient implementation of MD5-RC4 encryption using GPU with CUDA*" This paper is presented at ASID 2009[9]. Compute unified device architecture (CUDA) introduced by NVIDIA and graphics processing unit (GPU) is an emerging area for parallel implementations of applications. Changxin Li et al had presented an efficient implementation for MD5-RC4 encryption using NVIDIA GPU with CUDA framework. The MD5-RC4 algorithm was implemented on NVIDIA GeForce 9800GTX card. The results show that this GPU-based technique evince a performance gain of about 3-5 times accelerate for the MD5-RC4 algorithm.

T.D.B Weerasinghe presents "*RC4 Implementation using multithreading techniques in multi-core processors"* and this paper is being published in International Journal of Computer Applications (0975 – 8887), 2012[10] .The paper introduced a mechanism to improve the speed of RC4 algorithm in multi core processors using multithreading. For this research java (JDK version:1.6.0_21) is used to write source code. In this model, Java Executors were used and the Java Virtual Machine decided the number of threads was used in the parallelization process. As per the theoretical concepts available it is one of the most cost effective ways of using of Executors in multithreading. Experiments were done in an Intel® P4 machine (O/S: Windows XP), Core 2 Duo machine (O/S: Windows XP) and Core i3 machine (O/S: Windows 7) to analyze the throughput. The speed of the RC4 cipher can be accelerated using multi core processors.

Goutam Paul presents "*Merging Four RC4 States towards a 32-bit Stream Cipher*" and this work is in progress which started in May 2012[5]. In this paper, Four RC4 states are combined tacitly to devise a high speed stream cipher that produces 32-bit output at each round. The storage requisite for the internal state is 1024 bits only. As RC4 cannot have instruction level parallelism due to intensive swap functionality, the authors selected a simple-scalar RISC processor having sixteen 32-bit registers, six pipeline stages, fully by-passed arithmetic logic unit. The design is scalable to modern processors of large word-width and is at least as secure as RC4. In terms of speed, this cipher performs much faster than normal RC4 and is comparable with HC-128, the fastest software stream cipher amongst the eSTREAM_nalists

Rourab Paul presents "*An efficient one byte one clock RC4 design and implementation in FPGA coprocessor*". This paper is presented in the Proceedings of National Workshop on Cryptology 2012 Organized by CRSI in 2012. In this paper a design methodology which is processing of 1 byte in 1 clock is proposed using VHDL features. The mentioned design is implemented in a custom co-processor working in parallel with a main processor having FPGA architecture -Xilinx Spartan3E XC3S500e-FG320. Data communication between two FPGA boards all the way through their own Ethernet ports and each of the two boards performs encryption and decryption engines using RC4 independently. The clock gating technology is used to save dynamic power. In said design two sequential tasks are executed as two independent events during rising and falling edges of the same clock and the swapping is executed using a MUX-DEMUX combination. With mentioned design the power consumed in behavioural and structural designs of RC4 are estimated and a power optimization technique is proposed. The performance of this design in terms of number of clocks proved to be better than the previous works. The NIST statistical test suite is executed on RC4 key streams so as to know its arbitrariness property.

S.S Gupta presents "*High Performance Hardware Implementation*". The paper is published in IEEE Transactions on Computers [Volume 62, issue 4] in 2013[26]. The paper proposes the fastest hardware implementation for RC4 cipher and this is achieved by combining two key facts one is hardware pipeline and another is loop unrolling. This structural design produces two RC4 key stream bytes for each clock cycle. The proposed architecture is being implemented using VHDL , amalgamate with 130 , 90,65 nm manufacture technologies at clock frequencies 625 MHz, 1.37 GHz, and 1.92 GHz, correspondingly. With the help of this architecture authors succeeded to attain the high throughput of 10, 21.92, and 30.72 Gbps for RC4 key stream.

D. Handa and B.Kapoor Presents "*PARC4: Parallel Implementation of RC4 using SIMD model and multi-core processors*" and this paper is presented in International Conference on Optimization, Reliability, and Information Technology (ICROIT), 2014[8]. This paper introduces an efficient parallel implementation to the compute intensive PRGA that is pseudo-random generation algorithm portion of the RC4 algorithm and the resulted algorithm will be named as PARC4. As per the algorithm, input message is divided into fix sized large blocks and the algorithm encrypts these blocks concomitantly on multi core processor architecture. This is a scalable approach as the number of increases in cores will enhance the speed up without requiring any change in algorithm. According to the paper, the parallelism in RC4 is based on the following fundamentals.

1. ***Algorithm's Architecture***: Rc4 falls in the category of Single Instruction Multiple Data. In SIMD architecture only one instruction is being executed by the CPU during one clock cycle. But multiple data streams can be used as input data during one clock cycle. In Rc4 the input data is huge and the instructions over that data remain same [8].

2. ***Decomposition technique***: Rc4 follows domain decomposition as we can't decompose the tasks because of intensive swap functionality. In this algorithm, First instruction will calculate values and the second one will interchange the values. So we cannot consider both the instructions as independent tasks [8].

3. ***Mapping for load balancing***: The input data set for RC4 at a specific point of time is unknown and, as a result, the dynamic mapping is used here [8].

This approach sees about 5X speed up using 8 core processor and block size 256. We have used the ideas of profiling, data decomposition, and the dynamic mapping as the key means to parallelize and make the algorithm faster. OpenMP is used to parallelize the algorithm on shared memory multi core architecture such as a 8-core machine that we have used for implementation. PARC4 is the scalable approach. That means adding more number of cores in hardware will not require any change in algorithm.

R.prabu presents "*Architecture of High Performance Rc4 Cipher For safe Communication*".
Authors presented the method which is the combination of hardware pipeline and loop unrolling to design an architecture that generates two RC4 key-stream bytes per clock cycle [13]. The implementation is based on VHDL description, 65nm fabrication technology at clock frequency of 1.37 GHz to be obtained a final key stream throughput 30.72Gbps. The method provides high throughput in this hardware-based approach.

6. CONCLUSION

Although RC4 is having weak set of keys [15] but it is still in market and used by many organizations and protocols with some modifications to make it stronger. The paper has divided the survey on RC4 in two sections: one type of approaches to achieve security in RC4 and another type of approaches to execute RC4 in parallel using multi core technology. Table-1 shows recent approaches to attain security and Table-2 shows recent parallel approaches. Both tables reflect that this algorithm is still the point of attraction for researchers. The focus of the paper is to provide ample idea to researchers (new to this area) about all types of implementations on RC4 specifically as this is very simple and can definitely benefit from the emerging areas like FPGA implementations for security and multi core parallelization. The objective of this paper is to bring into notice to new researchers that rc4 is not untouched from parallel implementation and enhancements.

REFERENCES

1) Stallings et al,"Computer security: principles and practice", Upper Saddle River, N.J, Prentice Hall, 2008.
2) Kessler, G. (n.d.). An Overview of Cryptography, Retrieved June 18, 2014, from http://www.garykessler.net/library/crypto.html
3) Federal Information Processing Standards (FIPS) 140-2. (2001, May 25). Security Requirements for Cryptographic Modules. Gaithersburg, MD: National Institute of Standards and Technology (NIST). Retrieved from http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
4) Federal Information Processing Standards (FIPS) 199. (2001, May 25). Standards for Security Categorization of Federal Information and Information Systems. Gaithersburg, MD: National Intitute of Standards and Technology (NIST). Retrieved from http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
5) Goutam Paul et al,"Quad-RC4: Merging Four RC4 States towards a32-bit Stream Cipher, presented atINDOCRYPT, 2012
6) M.vanitha,"hardware and software implementation for highly secured modified wired equivalent privacy (mdwep)", JATIT,Vol 48,no- 2,2013
7) K.H.Tsoi et al, "A massively parallel RC4 key search engine (With FPGA)", 10 Annual IEEE Symposium on Field-Programmable Custom Computing Machines, 2002.
8) D.Handa and B.Kapoor,"PARC4: High Performance Implementation of RC4 Cryptographic Algorithm using Parallelism", International Conference on Reliability Optimization & Information Technology, Feb,2014
9) Changxin Li et al," Efficient implementation for MD5-RC4 encryption using GPU with CUDA", 3rd International Conference,2009
10) T.D.B Weerasinghe," Improving throughput of RC4 algorithm using multithreading techniques in multi core processors", International Journal of Computer Applications(0975 – 8887) Volume 51– No.22, August 2012
11) M Damrudi et al.," State of the Art Practical Parallel Cryptographic Approaches", Aus. Journal of Basic and Applied Sciences,2011,ISSN 1991-8178
12)Prabhudesai Keval Ketan and Vijayarajan V "An Amalgam Approach using AES and RC4 Algorithms for Encryption and Decryption", IJCA, Vol 54,no 12, sep 2012
13) R. Prabu,"Design Of High Performance Rc4 Stream Cipher For Secured Communication", International Journal of Innovative Research in Computer and Communication Engineering, Volume 2,Special issue 1,March 2014
14) Maytham M. Hammood et al,"RC4-2S: RC4 Stream Cipher with Two State Tables", Lecture Notes in Electrical Engineering 253, DOI: 10.1007/978-94-007-6996-0_2
15) Souradyuti Paul and Bart Preneel,"A New Weakness in the RC4 Keystream Generator and an Approach to Improve the Security of the Cipher" Lecture Notes in Computer Science, Springer-Verlag, pp. 245-259, 2004.
16) Pardeep, Pushpendra Kumar Pateriya,"PC1-RC4 and PC2-RC4 Algorithms: Pragmatic Enrichmen Algorithms to Enhance RC4 Stream Cipher", International Journal of Computer Science and Network (IJCSN),Vol-1,issue-3,june 2012
17) Sivalingham Latchmanan and Dr.Sharmin Parveen,"applicability of rc4 algorithm in blue tooth data encryption method for achieving better energy efficiency of mobile devices", http://informatics.fsktm.um.edu.my/cameraready/Informatics_003.pdf
18) Laxmi Mounika et al," Remodelling RC4 Algorithm for Secure Communication for WEP/WLAN Protocol", Global Journal of researches in engineering Electrical and electronics engineering, Volume 12 Issue 5 Version 1.0 April 2012
19) Seifedine Kadry, M. Smaili ,"An Improvement of RC4 Cipher Using Vigenère Cipher", International Journal of Computational Intelligence and Information Security Vo. 1 No. 3, May 2010

20) Peisong Ye and Guangxue Yue,"Security Research on WEP of WLAN", Proceedings of the Second International Symposium on Networking and Network Security (ISNNS '10) Jinggangshan, P. R. China, 2-4, April. 2010, pp. 039-042
21) Nadhem J. AlFardan1,"On the Security of RC4 in TLS and WPA_", proceedings of the USENIX Security Symposium 2013.
22) Jagdeep Singh and Kundan Munjal ,"A New Robust Enrichment Symmetric Stream Cipher Approach for Confidentiality Based on RC4 Stream Cipher Algorithm", International Journal of Engineering Research & Technology (IJERT), Vol. 2 Issue 3, March – 2013
23) Sourav Sen Gupta et al, 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, pages 151–168. Springer, 2011.
24) R. Chandramouli et al "Battery Power-Aware Encryption", ACM Transactions on Information Systems and Security, 9 (2), 162-180,2006
25) Duhyun Bae et al," Design and implementation of efficient cipher engine for IEEE 802.11i compatible with IEEE 802.11n and IEEE 802.11e", Proc. of the 2005 international conference on Computational Intelligence and Security, pp 439-444,Springer-verlag.
26) S.S.Gupta et al,"High-Performance Hardware Implementation for RC4 Stream Cipher", IEEE Transactions on computers, pp: 730 - 743 Volume: 62, Issue: 4, April 2013

Authors

Disha Handa started her career in 2007 with saber corp (An HP Company) as a software developer. She worked in two major projects MPAS (Maryland Pension Administration System) and DMV (Department of Motor Vehicle) for U.S state government. Her expertise areas include C# .net, BIZTALK , ILOG, SSRS, SSIS and Parallel APIs such as OPENMP. She is a member of ACM. Currently she is working as Assistant Professor in Computer Science & engineering department in Chitkara University. Her research area is parallel cryptographic algorithms.

Dr. Bhanu Kapoor started his technical career in 1987 with Texas Instruments, where he held various roles in the company's research and development labs. Since 1996, he has taught several undergraduate and graduate courses in the areas of computer science and electrical engineering, including graduate-level security engineering courses at companies such as L-3, Lockheed Martin, and Rayth eon. He is a senior member of the IEEE and the ACM. He has received six U.S. patents, has participated in various industry panels, and has served as an IEEE conference chairperson. His written works include more than 50 papers that have been presented at IEEE/ACM conferences or published in journals.