Journal of ELECTRICAL ENGINEERING, VOL. 60, NO. 3, 2009, 155–160

EVALUATION OF THE RC4 ALGORITHM AS A SOLUTION FOR CONVERGED NETWORKS

Alaa M. Riad [*] — **Alaa R. Shehata** [*] — **Elminir K. Hamdy** [**] — **Mohammed H. Abou-Alsouad** [*] — **Taha R. Ibrahim** [*]

Converging of all traffic types into a single multi-service network is a hot topic in the networking industry. Network designers have selected IP as the common infrastructure for this new converged network for its popularity and scalability. But due to the increased number of protocols and applications running on converged networks, new vulnerabilities are emerging and therefore new opportunities to break into the network are added, and so many security mechanisms are needed. Encryption solution based on RC4 algorithm will fit all types of application running over converged network, specially the real time applications and cause an acceptable delay. We will apply the NIST suite of statistical tests to RC4 output to test its randomness and security. The testing results illustrates that RC4 is secure and random enough to be used within the converged network.

K e y w o r d s: converged networks, VOIP security, RC4, stream ciphers, RNG, PRNG

1 INTRODUCTION AND OBJECTIVES

Converged network or NGN (Next Generation Network) is a networking infrastructure that accommodates data, voice, and multimedia communications, converged network can reduce costs for enterprises while providing enhanced functionality and increased flexibility. Benefits of integrating all types of communications include more efficient communication services; extended access to corporate resources for mobile workers; a solid base for deploying more sophisticated, integrated and potentially revenue-generating applications; and increased productivity levels overall. As a result, enterprises that use convergence can experience increased profits and grow revenue to gain a competitive advantage. With right strategy and adaptive network architecture, enterprises can confidently and successfully create a powerful, standard-based multi-service network that sufficiently handles a variety of traffic types simultaneously.

Data network had chosen to be the infrastructure for the NGN, which offers the opportunity for cost savings by migrating to a data network infrastructure, as Internet is everywhere and Internet Protocol (IP) is the most widely used protocol and exists throughout LANs, computer networks, enterprise intranets and the Internet. Its popularity makes IP the unifying protocol for converged network solutions. Converged IP-based architectures are gaining widespread acceptance and adoption by leading technology vendors and contact centre operators alike [1], so the real time traffic (streaming audio and video) or traditional voice will migrate to the data network and will traverse the network as packets. The converged network will involve components from two disparate worlds (circuit switching and packet switching networks) that have different objectives, for example the voice network has always been separated from the data network as the characteristics of voice application differs from those for data applications.

While voice traffic is sensitive to delay, packet misorder and jitter, and needs high reliability, data traffic is less sensitive to delay and jitter but more sensitive to packet loss. In order for a converged network to function well, extra care must be directed to the characteristics of the different traffic types that coexists within it to insure good quality of service and avoid problems like delay, echo, packet loss and jitter, for example network must be able to give priority to voice packets (which is delay sensitive) over data packets.

1.1 Converged Network Security

Security is a very important topic in converged networks implementation, as combining different communication types will combine their vulnerabilities and threats, so the challenge of securing converged communication has become the central issue of discussion and a new barrier to accept the technology. In a converged network every voice port, telephone, IP phone or IP based device is a potential open door [3], which gives hackers the opportunity to access data through voice system or using the data known hacking techniques to manipulate the voice system. For example, in the traditional telephone network, physical access to a switch or wiring closet is required to intercept communications between two parties. In a converged environment, widely available hacker tools can trivially capture voice traffic as it travels

[*] Mansoura University, Faculty of Computer and Information Systems, Mansoura, Egypt; [**] National Research Institute of Astronomy and Geophysics, El-Marsad Street, Helwan, Cairo, Egypt; hamdy_elminir@hotmail.com

ISSN 1335-3632

through a large data network. There are many security problems that are concerned with converged networks as call interception, Denial of Service (DoS) attacks, Signal Protocol Tampering, Spoofing or Presence Theft and Theft of Service and Toll Fraud.

While many existing security disciplines and techniques can effectively be implemented in the converged network, others will require revision, updating or replacement with new controls that reduce risks and fill the gaps between traditional data network and telephone network security. The converged network requires converged security that integrates, enhances supplements and expands traditional data security techniques and policies to provide protection for converged communications carried in the data network. There are many security techniques that can be used to secure converged networks, but Cryptography is probably the most important aspect of communication security and is becoming increasingly important as a basic building block for computer security generally [4], so we will concentrate on the encryption technique that will be used as the solution of many of the converged network problems, like call interception and signal protocol tampering. Encryption if not implemented correctly, can do the potential to delay voice (or video) packets and adversely affect the performance of VoIP on the converged network, especially if there are multiple encryption points. The overhead of the encryption should have little impact on the performance of converged networks, as we stated earlier that real time packets like VoIP packets are more sensitive to delay than data packets, hence if we utilized the traditional encryption techniques used within the data network like block ciphers, the voice quality will be degraded because of the resulting delay. From the prospective of converged security, we can minimize the risk to voice quality even more by employing streaming ciphers like RC4 instead of using block ciphers that is used with data encryption mechanisms. Stream encipherment combines the plaintext x0, x1, ... , xn21 letter-by-letter with a key stream of 0's and 1's. For ASCII plaintext, each letter xi might first be coded into its 7-bit ASCII ordinal value xi and then enciphered by the exclusive-OR (XOR) with the key stream [5].

$$x_0, x_1, ..., x_{n-1} \rightarrow x_0, x_1, ..., x_{n-1}$$

RC4 is the most widely used stream cipher. It is part of the SSL/TLS (Secure Sockets Layer/Transport Layer Security) standards that have been defined for communication between web browsers and servers. It is used in the WEP (Wired Equivalent Privacy) protocol that is a part of the IEEE 802.11 wireless LAN standard, [6]. RC4 is a variable size stream cipher developed by Ron Rivest for RSA Data Security, Inc., it is used also in other applications as Lotus Notes, Apple computers' AOCE and Oracle secures SQL. The IEEE 820.11i uses the Temporal Key Integrity Protocol (TLIP) and the Advanced Encryption Standards (AES), TKIP uses the RC4 stream cipher as the encryption and decryption algorithm and all involved parties must share the same secret key [7]. Many papers have been published analyzing methods of attacking RC4. None of these approaches is practical against RC4 with a reasonable key length, such as 128 bits. A more serious problem is reported in [8].

The authors demonstrate that the WEP protocol, intended to provide confidentiality on 802.11 wireless LAN networks, is vulnerable to a particular attack approach. In essence, the problem is not with RC4 itself but the way in which keys are generated for use as input to RC4. This particular problem does not appear to be relevant to other applications using RC4 and can be remedied in WEP by changing the way in which keys are generated [6]. In our paper we will use the statistical tests to prove that RC4 is secure and random enough to be used within the converged network.

2 RC4 STRUCTURE

RC4 like as a streaming cipher encrypts plaintext one byte at a time, but also can be designed to encrypt one bit a time or even units larger than a byte at a time. In this structure a key is input to a pseudorandom bit generator that produces a stream of 8-bit numbers that are supposed to be truly random, the pseudorandom stream can't be predicted without knowledge of the input key. The output of the generator is called a key stream .It is combined one byte a time with the plain text stream using the bitwise exclusive-OR (XOR) operation.

Table 1. Speed Comparisons of Symmetric Ciphers on a Pentium II

Cipher	Key Length	Speed (Mbps)
DES	56	9
3DES	168	3
RC2	Variable	0.9
RC4	Variable	45

Using RC4 (or stream ciphers generally) is desirable in converged network environment especially for real-time applications than block ciphers, as it is always faster and uses far less code than do block ciphers. Table 1 illustrates this advantage by comparing the execution speed time of RC4 with three well-known symmetric block ciphers [6].

2.1 How do the RC4 Works?

The RC4 is simple and easy to be explained. The algorithm is based on the use of random permutation. A variable length key $K[\,]$ of from 1 to 256 bytes (8 to 2048 bits) is used to initialize a 256-byte state vector $S[\,]$, with elements S [0] S[255]. At all times S [ ] contains a permutation of all 8-bit numbers from 0 to 255. For encryption and decryption, a byte K is generated from

S [ ] by selecting one of the 255 entries in a systematic fashion. As each value of K is generated, the entries in S[ ] is again permuted. Figure 1 shows the block diagram of the RC4 two phases. To encrypt, XOR the value K with the next byte of plaintext, To decrypt, XOR the value K with the next byte of ciphertext, it is clearly here that if we use different keys for encryption and decryption we will never restore our plain text again, even if we use different keys for encryption the resulted ciphertext would not be the same.

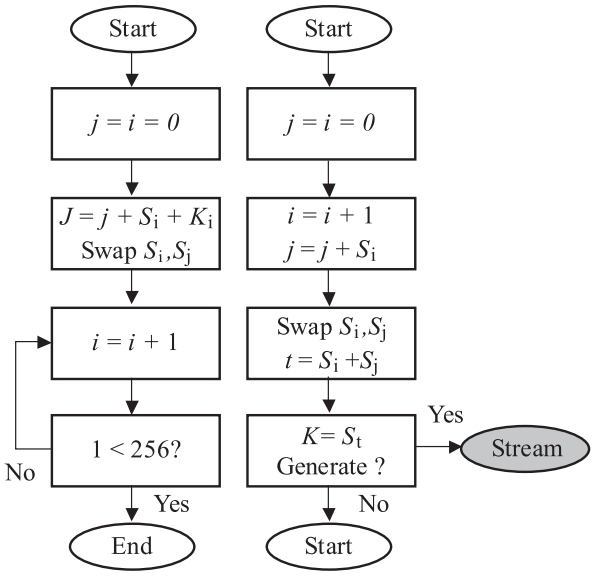

Fig. 1. Block Diagrams of RC4 Phases. [7]

RC4 like any other stream cipher depends on the strength of its key stream, which in turns depends on the degree of randomness of its pseudo random bit generator (throughout this paper the term pseudo random number generator refers to PRBG).The output of such generator needs to meet stronger requirements than for other applications. In particular, their output must be unpredictable in the absence of knowledge of the inputs. If the key (seed) is unknown, the next output number in the sequence should be unpredictable in spite of any knowledge of previous random numbers in the sequence. This property is known as forward unpredictability. It should also not be feasible to determine the key (seed) from knowledge of any generated values (*ie*, backward unpredictability is also required). No correlation between a seed and any value generated from that seed should be evident; each element of the sequence should appear to be the outcome of an independent random event whose probability is 1/2.

3 STATISTICAL TESTING

Suitable metrics are needed to investigate the degree of randomness for binary sequences produced by RC4, statistical testing will be used to gather evidence whose output sequences are truly random, and can be used safely in the converged network applications. There are many statistical test suites that can be used in analyzing the output sequence of RC4 (or any PSRBG), we will use the NIST (The National Institute of Standards and technology) statistical test suite for its flexibility, accuracy and popularity. While it is impossible to give a mathematical proof that any sequence is indeed random, the tests will help to detect certain kinds of weaknesses the RC4's PRBG generator may have. This is accomplished by taking a sample output sequence of the generator and subjecting it to various statistical tests. Each statistical test determines whether the sequence possesses a certain attribute that a truly random sequence would be likely to exhibit; the conclusion of each test is not definite, but rather probabilistic. An example of such an attribute is that the sequence should have roughly the same number of 0's as 1's. If the sequence is deemed to have failed any one of the statistical tests, the generator may be rejected as being non-random; alternatively, the generator may be subjected to further testing. On the other hand, if the sequence passes all of the statistical tests, the generator is accepted as being random, since passing the tests merely provides probabilistic evidence that the generator produces sequences which have certain characteristics of random sequences and in accordance the RC4 algorithm will be accepted.

3.1. The NIST Statistical Test Suite

Let us proceed to describe the NIST test suite in more detail. We begin by highlighting our evaluation framework and then list the defects that each test was designed to detect.

3.1.1 THE NIST Framework

The NIST framework, like many tests, is based on hypothesis testing. A hypothesis test is a procedure for determining if an assertion about a characteristic of a population is reasonable. In this case, the test involves determining whether or not a specific sequence of zeroes and ones (RC4 resulted binary sequence) is random. Table 2 illustrates the step by step process that is followed in the evaluation of a single binary sequence.

3.1.2 The NIST Statistical Tests

The NIST designed a set of different statistical tests to test randomness of (arbitrarily long) binary sequences produced by either hardware or software based cryptographic random or pseudorandom number generators. These tests focus on a variety of different types of non-randomness that could exist in a sequence. The mathematical description of each test can be found at: "A Statistiical Test Suiite for Random and Pseudorandom Number Generators for Cryptographiic Appliicatiions- NIST Special Publication 800-22" [9]. Some tests are decomposable into a variety of subtests. Each test focuses on

Table 2. Evaluation Procedure for a Single Binary Sequence [9]

	Step By Step Process	Comments
(1)	State your null hypothesis	Assume that the binary sequence is random
(2)	Compute a sequence test statistic	Testing is carried out at the bit level
(3)	Compute the P-value	P-value $\in [0, 1]$
(4)	Compare the P-value to []	Fix [], where [] $\in (0.001, 0.01]$ Success is declared whenever P-value >> [][] otherwise, failure is declared

Table 3. Summary of NIST statistical tests characteristics

	Statistical test	Defect detected
(1)	The Frequency (Monobit) Test	Too many zeros or ones for the entire sequence
(2)	The Frequency Test within a block	Too many zeros or ones within M-bit blocks
(3)	Runs Test	Large (small) total number of runs indicates that the oscillation in the bit stream is too fast (too slow)
(4)	Longet Runs of Ones in a block	Deviation of the distribution of long runs of ones within M-bit block
(5)	The Binary Matrix Rank Test	Deviation of the rank distribution from corresponding random sequencedue to periodicity of sub-sequences that repeats
(6)	Discrete Fourier Transform (Spectral) Test	Periodic features in the bit stream
(7)	Non-overlapping template Matching	Too many occurrences of non-periodic templates
(8)	Overlapping Template Matching	Too many occurrences of m-bit runs of ones
(9)	Maurer's "Universal Statistical" Test	Compressibility (regularity). "The sequence can be significantly compressed without loss of information."
(10)	The Lempel-Ziv Compression Test	More compressed than a truly random sequence
(11)	Linear complexity Test	Sequence is not complex enough to be considered random
(12)	The serial test	Non-uniform distribution of m-length words
(13)	The Approximate Entropy Test	Non-uniform distribution of m-length words Small values of ApEn (m) imply strong regularity
(14)	The cumulative Sums Test	Too many zeros or ones at the beginning of the sequences
(15)	The random Excursions Test	Deviation from the distribution of the number of visits of a random walk to a certain state
(16)	The Random Excursions Variant Test	Deviation from the distribution of the total number of visits (across many random walks) to a certain state

a specific type of defect. Table 3 describes the general characteristics of each statistical test.

4 TESTING RESULTS

RC4 will be applied to four different types of converged network traffic (audio, video, image and text), then each resulted sequence will be applied to the NIST statistical tests, and then the result of each test will be analyzed to determine if it passes the randomness properties. Success will be declared whenever P-values (which resulted from testing each sequence) $>$ [][] where [] $\in (0.001, 0.01]$. Otherwise, failure will be declared. After all the statistical tests will be implied , we will decide if the resulted sequences from the RC4 is random enough , and so we will decide if the RC4 itself will be used securely as a security solution for converged networks or not.

4.1 Decision Rule (At 1 % Level)

In all subsequent tests if the computed P-value is ¡ 0.01, then conclude that the sequence is non-random. Otherwise, conclude that the sequence is random.

4.2 Testing Video Files

Figure 2 illustrates the mean values of the resulted P-values after applying NIST statistical tests to the RC4 encrypted video sequences, and it is clear that our video sequences passes all the statistical tests, and their P-Values is much higher than 0.01.

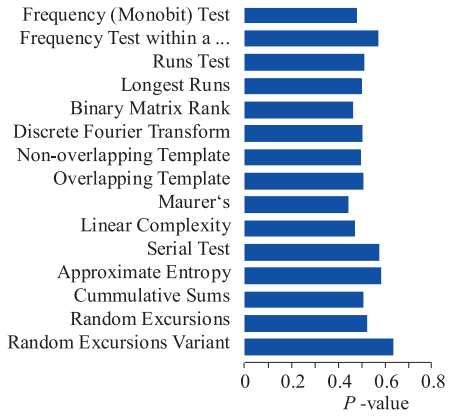

Fig. 2. Video file testing results

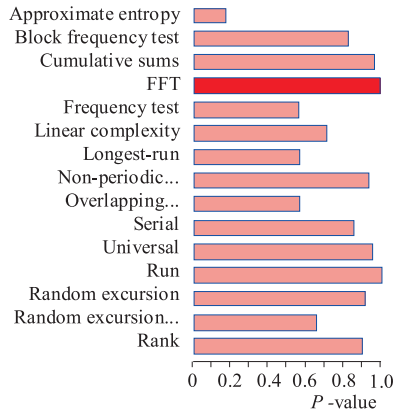

Fig. 3. Video file maximum values

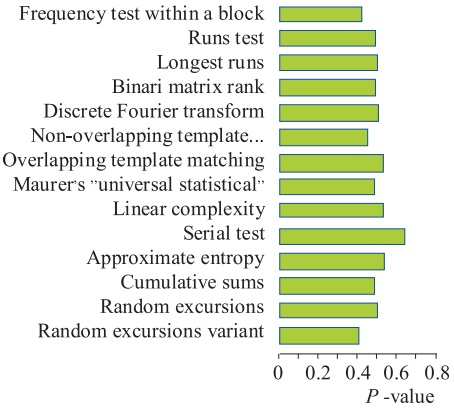

Fig. 4. Audio file testing results

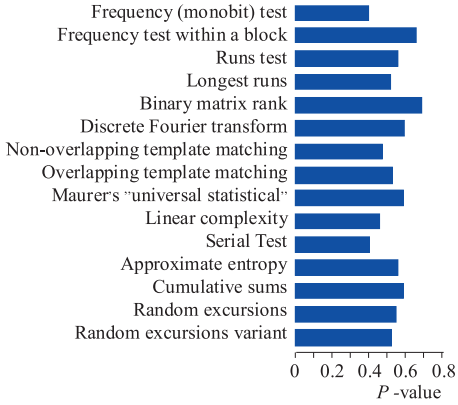

Fig. 5. Audio file maximum values

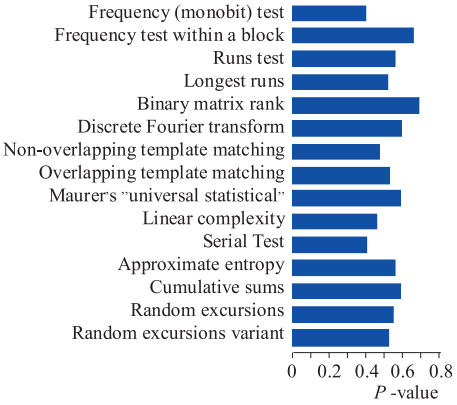

Fig. 6. Image file testing results

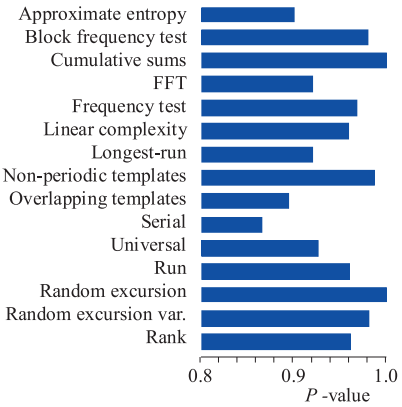

Fig. 7. Image file maximum values

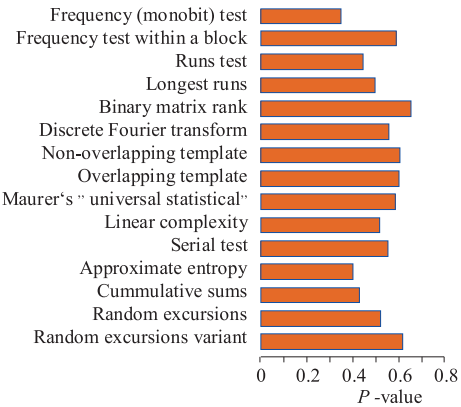

Fig. 8. Text file testing results

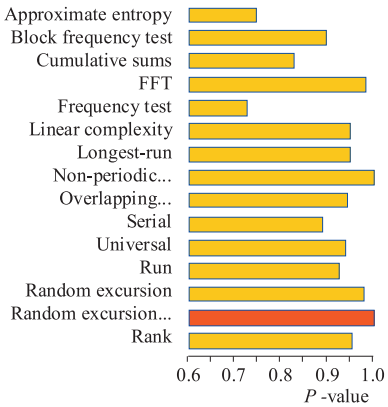

Fig. 9. Text file maximum values

Figure 3 illustrates the maximum value for each test, we can see that our video sequences reached very high P-values at all tests, even they reached one (the most high value) at the Discrete Fourier Transform test, which means good statistical properties as would be expected from truly random sequences, and hence we will accept all the RC4 video sequences as random.

4.3 Testing Audio Files

From Fig. 4 we can notice that our audio sequence passes all the statistical tests with good values which mean that our sequences have no defect at all.

Figure 5 illustrates that the maximum values for our audio sequences at all tests are much higher than 0.01 (all of them are more greater than 0.969) which indicates good statistical properties for our resulted RC4 sequences, and then we will accept them as random.

4.4 Image File Test

From Fig. 6 it is illustrated that our image sequences encrypted by RC4 have no defect and pass all the statistical tests with high values.

From Fig. 7 we can see that our Image sequences reach a very high values which means high randomness , and so we will accept it as random.

4.5 Text File Test

From Fig. 8 we can deduce that our text file is random as it passes all the statistical tests with high values.

Figure 9 illustrates the high values reached by the resulted RC4 text sequences; even we reached one (the absolute highest value) at the Random Excursion Variant test which in turn indicates a good statistical properties and high degree of randomness.

CONCLUSIONS

In this paper we discussed the security problems of the converged networks. RC4 algorithm was introduced as a solution for converged networks security problems. NIST statistical test suite was used to test the security of RC4 algorithm running over converged networks , all traffic types that are running over converged networks (video, audio, image and text) were tested after encrypting them with RC4, the resulted sequences passed all the statistical tests with high values, which indicates high statistical properties for all of them As a result RC4 sequences are random and can't be predicted. Hence RC4 is applicable with converged networks traffic, and can work as a security solution for them, with a very fast performance and strong degree of security.

References

[1] IP for Contact Centers, Guideline for IP Deployment, the ContactCentres.be - IP Convergence Workgroup, Version 1.01, June 2006.

[2] COLLIERM. : The Current State of VoIP Security, VOIP magazine, October 2005.

[3] Steven Sullivan, Securing a Converged Network, infosecwriters, 2007.

[4] Computers at Risk: Safe computing in the information age, USA National Research Council, 1991.

[5] ALANGG. KONHEIM : Computer Security and Cryptography, John Wiley & Sons, Inc,, 2007.

[6] WILLIAMSTALLING : Cryptography and Network Security, Prentice Hall, 2005.

[7] P. KITSOSETAL : Hardware Implementation of The RC4 Stream Cipher, Proceedings of the 46-th IEEE International Midwest Symposium on Circuits and Systems, MWSCAS '03, 2003.

[8] FLUHRER, S.—MANTIN, I.—SHAMIR, A. : Weakness in the Key Scheduling Algorithm of RC4, in Proceedings, Workshop in Selected Areas of Cryptography, 2001.

[9] A Statiistiical Test Suiite for Random and Pseudorandom Number Generators for Cryptographiic Applications, NIST Special Publication 800-22, 2001.

Received 15 November 2008

A. M. Riad (Prof, Dr) is Head of Information Systems Department, Faculty of Computers and Information Sciences, Mansoura University, Egypt, Web site: http://www.amriad.com

Alaa R. Shehata — biography not supplied.

Hamdy K. Elminir was born in EI-Mahala, Egypt in 1968. He received the BSc in Engineering from Monofia University, Egypt in 1991 and completed his master degree in automatic control system in 1996. He obtained his PhD degree from the Czech Technical University in Prague in 2001. Currently he is an associate professor in the National Research Institute of Astronomy and Geophysics, Helwan, Cairo, Egypt.

Mohammed H. Abou-Alsouad — biography not supplied.

Taha R. Ibrahim was born in El-Mahalla, Egypt in 1974.He received the BSc in electronic engineering from faculty of electronic engineering in Menouf, Egypt, he is applying for the master degree in converged network security in El Mansoura University-Egypt, now he is working as a security specialist in Arab Open University-Egypt.