Military Technical College
Kobry Elkobbah,
Cairo, Egypt

8th International Conference
on Aerospace Sciences &
Aviation Technology

# A New Generation of Message Authentication Code Using Symbolic Dynamics

**Alaa Fahmy***

## ABSTRACT

Authentication plays an important role in data security. It informs the receiver much more about the integrity of the received message to decide whether it is genuine or forge message. Verifying the correctness of the message authentication code can authenticate the message's contents. In this paper, we introduce a novel method, based on symbolic dynamic, to generate the message authentication code (MAC).

## 1. INTRODUCTION

Cryptography provides solutions to the two major problems of data security: the privacy problem, preventing an opponent from extracting information from a communication channel, and the authentication problem, preventing an opponent from injecting false data into the channel or altering messages. The authentication problem can be solved either by using conventional cryptosystem or the public key cryptosystem [1,2]. The eavesdropper does not only listen on the communication channel, but he may also inject a forge message or alter the cryptograms flowing on the communication channel to deceive the receiver. Therefore, the communicator has to have an authentication scheme to protect himself from being deceived by forge messages.

Message authentication is a procedure established between two ends (sender and receiver) allows each end to verify the integrity of the received message. The message authentication enables the receiver to authenticate the message's contents, message's origin, and message's timeliness. In this paper, we discuss the authentication of message's contents. Verifying the correctness of message authentication code (MAC), which is computed by the sender and appended to the message (M), authenticates the contents of a message.

## 2. SYMBOLIC DYNAMICS OF UNIMODAL CHAOTIC MAPPING

### 2.1 Preliminaries

The complete description of the discrete time evolution of the map $X_{n+1} = f(X_n, \mu)$, $X_n \in I$, and $\mu$ is a non-linear parameter, would require the knowledge of the whole set $\{X_i, i=0,1,...\}$ for all possible initial choices of $X_0$.

---

* Ph.D , Dpt. of Electrical Engineering, Military Technical College, Cairo, Egypt.

Therefore, one can develop a coarse-grained description by ignoring the actual numbers in the set, but retaining the essential feature of the evolution [3]. One of the simplest discrete unimodal chaotic maps is called the logistic map and it is given by the following equation [3]:

$$\mathbf{X}_{n+1} = \mu \mathbf{X}_n (1 - \mathbf{X}_n), \qquad \mathbf{X} \in \mathbf{I}. \tag{1}$$

The interval, I, can be divided into two segments, according to the monotonic branches of the map. These segments are separated by critical points of the map. Each segment needs a letter to label (R or L), and the critical point is labeled by a letter C, where $L < C < R$. Replace each number $X_i$ by the label of the interval into which it falls, every set $\{X_i\}$ will become a sequence of letters. Using a finite number of symbols, one can form infinitely many symbolic sequences.

### 2.2 Definitions

- **Stable periodic orbit:** an orbit of period n is said to be stable if [3]:

$$\left| \prod_{i=1}^{n} \mathbf{f}'(\mu, \mathbf{x}_i) \prec 1. \right| \tag{2}$$

Where f′ represents the first derivative of the map $X_{n+1}$.

- **Admissible word:** a word is said to be admissible, if it does correspond to a stable periodic orbit of the unimodal map [3].
- **Parity of a word:** a word made of a certain number of letters R and L is said to be odd (even), if it contains an odd (even) number of R's [3].
- **Harmonic of a word:** if we have a word W, we can construct another word H(W) called the harmonic of W [3].

$$\begin{aligned} \mathbf{H(W)} = \mathbf{W}\sigma\mathbf{W}, \quad & \sigma = \mathbf{R}, \quad \textbf{if W even}; \\ & \sigma = \mathbf{L}, \quad \textbf{if W odd}. \end{aligned} \tag{3}$$

- **Antiharmonic of a word:** the antiharmonic of a word A(W) is constructed according to a rule opposite to that for the harmonic [3].

$$\begin{aligned} \mathbf{A(W)} = \mathbf{W}\sigma\mathbf{W}, \quad & \sigma = \mathbf{L}, \quad \textbf{if W even}; \\ & \sigma = \mathbf{R}, \quad \textbf{if W odd}. \end{aligned} \tag{4}$$

If the word W is an admissible word, then the harmonic of the word W is also admissible and corresponds to the period-doubled cycle of word W. The antiharmonic of a word W is not admissible word, and does not corresponds to a real orbit of the map.

## 3. MESSAGE AUTHENTICATION CODE GENERATION

The process of generating MAC consists of the following main steps:

**(1) Encoding process:** assigning letter R and L to the plaintext corresponding to the binary digit '1' and '0' respectively. Therefore, we get a symbolic sequence of R and L. Then, we divide this symbolic sequence into blocks of length 8-digits each.

**(2) Message's selection:** we select all the admissible and inadmissible words (but starts with letter "R") from the plaintext.

**(3) Message's ordering:** the selected message's words can be ordered by comparing them, letter by letter from left to right, and denote the largest common part by $W^*$. The order is defined on the basis of the natural order on the interval I (L < C < R). For example, let

$$\mathbf{W}_1 = \mathbf{W} * \sigma_1\sigma_2 \ldots\ldots; \qquad \mathbf{W}_2 = \mathbf{W} * \tau_1\tau_2\ldots\ldots \tag{5}$$

If $W^*$ is even, $\sigma_1 > \tau_1$, therefore, $W_1 > W_2$. If $W^*$ is odd, $\sigma_1 < \tau_1$, therefore, $W_1 > W_2$.

**(4) Find the median words Φ(M):** In this way, we use the symbolic dynamics of unimodal chaotic map given by eq. (1) to generate the median words between every two words, in the selected message, with maximum word length ($L_{max}$) as follows:

(i) Suppose we have two words $W_1$ and $W_2$, where $W_1 < W_2$, $W_1$ has length $n_1$;
(ii) Construct $H(W_1)$ and $A(W_2)$, denote their leading common part of length $n^*$ by $W^*$;
(iii) if $n^* > 2n_1$, then the median word Φ(M) is given by the harmonic of $W_1$ and if $n^* < 2n_1$, then the median word Φ(M) is given by $W^*$ itself.

$$\mathbf{H}(\mathbf{W}_1) = \mathbf{W} * \sigma_1\sigma_2\ldots\ldots; \qquad \mathbf{A}(\mathbf{W}_2) = \mathbf{W} * \tau_1\tau_2\ldots\ldots \tag{6}$$

**(5) Encipherment process:** The cryptosystem presented by Sobhy and Alaa [4] can be used to encipher both the plaintext M and the median Φ(M). The encipherment of the median represents the message authentication code.

$$\mathbf{MAC} = \mathbf{E}_k(\Phi(\mathbf{M})), \qquad \mathbf{k} \in \mathbf{K}, \tag{7}$$

where E is the encryption algorithm used, and K is the key space. The receiver deciphers the received ciphertext, following the previous procedures to reproduce the MAC, and check the integrity of the received message by comparing the received MAC with the calculated one. If they are equal then the message is genuine otherwise, it is forge message.

## 4. DISCUSSIONS

The MAC is a function of the entire message and has the following properties:

- It is computationally infeasible for an opponent to find a different message M` such that Φ (M`) = Φ (M).
- For M`≠ M, the probability that: Φ (M`) = Φ (M) is $1/2^c$, where c is the number of bits in MAC.

One of the basic ideas of any authentication algorithm is to add redundancy to the message, and to spread this redundancy all over the message. This method of MAC generation can control the amount of redundancy in a way to compromise between the security and message expansion requirements. Specifying the median words with a certain maximum word length ($L_{max}$) can control the amount of redundancy.

Table 1 illustrates a simple example for the steps of generating the MAC for a plaintext "SEQUENCE" with $L_{max}$ = {3, 4, 5, 6, 2, 2}, and $L_{max}$ = {2, 3, 4, 2, 2, 2}. Moreover, it emphases how this method control the amount of redundancy. For the maximum word length $L_{max}$ = {3, 4, 5, 6, 2, 2}, the MAC's length is 43-bit while with $L_{max}$ = {2, 3, 4, 2, 2, 2}, it is 13-bit. In addition, a single bit change in the ciphertext results in a failure to reproduce the message authentication code. That is, the algorithm used for generating the MAC rotates in a closed loop trying to find the median words.

## 5. CONCLUSION

A novel method, based on a new application of symbolic dynamic in cryptography, is introduced to generate the message authentication code. It is based on the idea of finding the median words between two given words. This novel method can control the amount of redundancy in a way to compromise between the security and message expansion requirements. Moreover, a single bit change in the ciphertext results in a failure to reproduce the message authentication code (system rotate in a closed loop trying to find the median words).

## REFERENCES

[1] Carl H. Meyer, Stephen M. Matyas, Cryptography, A New Dimension in Computer Data Security, New York: Wiley, 1982.

[2] Kellogg S. Booth, "Authentication of Signatures using Public Key Encryption", Communication of the ACM, Nov. 1981, Vol.24, No.11, P772- 774.

[3] Hao Bai-Lin, Elementary Symbolic Dynamics and Chaos in Dissipative Systems, World Scientific, 1989.

[4] Sobhy M.I. and Alaa Fahmy, "Cryptographic Algorithm Based on Chaotic Behavior", Proceedings of the 10th National Radio Science Conference, Feb. 16-18, 1993.

## Plaintext (M)

SEQUENCE

## Symbolic sequence

RRLLRLRL RLRLLLRL RLLLRLRL RLRLRLRL RLRLLLRL LRRRLLRL RRLLLLRL RLRLLLRL

## Message's selection (Admissible & inadmissible words)

RRLLRLRL RLRLLLRL RLLLRLRL RLRLRLRL RLRLLLRL RRLLLLRL RLRLLLRL

## Message's ordering & median words with $L_{max}$ = {3, 4, 5, 6, 2, 2}

| Word/median no. | Period (n+1) | Word (length n) |
|---|---|---|
| W1 | 9 | RRLLRLRL |
| | 3 | RR |
| M1 | 2 | R |
| W2 | 9 | RLRLLLRL |
| W2 | 9 | RLRLLLRL |
| | 4 | RLR |
| | 3 | RL |
| M2 | 4 | RLL |
| W3 | 9 | RLLLRLRL |
| W4 | 9 | RLRLRLRL |
| | 4 | RLR |
| | 5 | RLRR |
| | 3 | RL |
| M3 | 5 | RLLR |
| | 4 | RLL |
| W3 | 9 | RLLLRLRL |
| W5 | 9 | RLRLLLRL |
| | 6 | RLRLL |
| | 5 | RLRL |
| M4 | | |
| | 6 | RLRLR |
| W4 | 9 | RLRLRLRL |
| W6 | 9 | RRLLLLRL |
| M5 | 2 | R |
| W5 | 9 | RLRLLLRL |

| Word/median no. | Period (n+1) | Word (length n) |
|---|---|---|
| W5 | 9 | RLRLLLRL |
| | 6 | RLRLL |
| | 5 | RLRL |
| M4 | | |
| | 6 | RLRLR |
| W4 | 9 | RLRLRLRL |
| W6 | 9 | RRLLLLRL |
| M5 | 2 | R |
| W5 | 9 | RLRLLLRL |
| W6 | 9 | RRLLLLRL |
| M6 | 2 | R |
| W7 | 9 | RLRLLLRL |

**The median words (with 43-bit length)**

$\Phi(M) = \{M_i, i = 1, 2, 6\}$

$\Phi(M)$ = RRRRLRRLRLLRLRRLRRRLRLLRRLLRLRLLRLRLRLRLRRR

**$MAC = E_k(\Phi(M))$**

**Table 1-a Generation of MAC using the median words between every two words with $L_{max} = \{3, 4, 5, 6, 2, 2\}$**

| Word/median no. | Period (n+1) | Word (length n) |
|---|---|---|
| W1 | 9 | RRLLRLRL |
| M1 | 2 | R |
| W2 | 9 | RLRLLLRL |
| W2 | 9 | RLRLLLRL |
| M2 | 3 | RL |
| W3 | 9 | RLLLRLRL |
| W4 | 9 | RLRLRLRL |
| | 4 | RLR |
| | 3 | RL |
| M3 | | |
| | 4 | RLL |
| W3 | 9 | RLLLRLRL |
| W5 | 9 | RLRLLLRL |
| | No Median Word | |
| W4 | 9 | RLRLRLRL |
| W6 | 9 | RRLLLLRL |
| M4 | 2 | R |
| W5 | 9 | RLRLLLRL |
| W6 | 9 | RRLLLLRL |
| M5 | 2 | R |
| W7 | 9 | RLRLLLRL |

**The median words (with 13-bit length)**

$\Phi(M) = \{M_i, i = 1, 2, 5\}$

$\Phi(M)$ = RRLRLRRLRLLRR

**MAC = $E_k$ ($\Phi$(M))**

**Table 1-b Generation of MAC using the median words between every two words with $L_{max}$ = {2, 3, 4, 2, 2, 2}**