Journal of Theoretical and Applied Information Technology
31st March 2017. Vol.95. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A SYMMETRIC CRYPTOSYSTEM BASED ON NONDETERMINISTIC FINITE AUTOMATA

[1]GHASSAN KHALEEL, [1]SHERZOD TURAEV, [1]IMAD ALSHAIKHLI
[2]TAMARA ZHUKABAYEVA, [1]M. IZZUDDIN M. TAMRIN

[1]Faculty of Information and Communication Technology
International Islamic University Malaysia, 53100 Gombak, Selangor D.E., Malaysia
[2]Faculty of Information Technology
L.N. Gumilyov Eurasian National University
010008 Astana, Kazakhstan
E-mail: [1]ghassan.khaleel@live.iium.edu.my, [1]{sherzod, imadf, izzuddin}@iium.edu.my,
[2]tamara_kokenovna@mail.ru

ABSTRACT

This paper proposes a new symmetric cryptosystem based on nondeterministic finite automata. It is shown that nondeterminism allows to reduce the dependency of key automata on a large descriptional complexity and irreversibility of automata. Moreover, it is proven that the introduced cryptosystem has higher security and more efficient performance than its deterministic counterparts – Dömösi's cryptosystem and its modified version.

Keywords: *Cryptography, Stream Cipher, Nondeterministic Finite Automata, Dömösi's Cryptosystem*

1. INTRODUCTION

Cryptography is a method or mechanism of storing and transmitting information in a particular form through insecure channels. The main objective of the cryptography is satisfying confidentiality, authentication, data integrity and non-repudiation. The confidentiality means that the information we have in database or in the systems should be out of hands of unauthorized users. The basic element of protecting information confidentiality is encryption. Encryption ensures that only the authorized people can read the information. Whereas, the authentication verifies the user's identity before revealing sensitive information. The data integrity is one of the most important factor in the cryptography, it means that the received message should be exactly the sent message. Cryptographic systems can be classified into two types: symmetric-key and asymmetric-key cryptosystems. Symmetric-key cryptosystems use a single key that both sender and recipient have, whereas public-key systems use two keys, a public key known to everyone and a private key that only the recipient of the messages uses. Symmetric-key systems can be also broadly classified into: block ciphers and stream ciphers. The basic idea of a block cipher is to break a plaintext into fixed length blocks, and encrypt each block separately. A stream cipher encrypts a sequence of data, typically, a bit or byte, by using sequence of keys.

2. RELATED WORKS

The theory of formal languages and automata, the backbone of theoretical computer science, also offers a natural basis for cryptosystems design. Several cryptosystems have been designed based on various types of automata and grammars such as Mealy machines, cellular automata, Lindenmayer systems, etc.

In 1985, Tao and Chen [1] proposed a public-key cryptosystem based on Mealy machine, which is called Finite Automata Public Key Cryptosystem (for short named as FAPKC0). This cryptosystem uses invertible automata for which explicit inverses are known, but such that an inverse of the composition of two automata was computationally unfeasible to compute. Two new variants, called as FAPKC1 and FAPKC2, were introduced in [2]. In 1995, Bao and Igarashi [3] found some security weaknesses in these systems.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

To prevent attacks, a refinement of this system, called FAPKC3, was developed in [4]. But this modification was also broken by Meskaten in [5].

M. Gysin [6] presented a one-key cryptosystem based on non-linear extended Mealy machine. In this system, Mealy automata consist of octuple sets and functions, and n additional internal variables. The key is a part of automaton itself, and hence, the number of states becomes $2^n + k$ states, where k is a long of the key. The ciphetext is generated depending on the key and three additional function to specify the extra states, and assign the next state in the automaton. To recover the plaintext, this process can be reversed. The statistical analysis of the system shows that the proposed cryptosystem has the same statistical proprieties of DES, and the length of the generated ciphertext is the same length of plaintext. However, the performance of the cryptosystem is slower than DES cryptosystem. Moreover, the vulnerability of these cryptosystems is due to the well-known fact that automaton mappings are length and prefix preserving. Knowing a great number of ciphertext, the cryptosystem can be attacked by brute force search.

In 2008, Dömösi [7-9] proposed a new stream cipher based on Rabin-Scott model of automata (i.e., finite automata without outputs), which act as a key for encrypting plaintexts and decrypting ciphertexts. In this way, Dömösi's cryptosystem is similar to Mealy machine: the encoding and decoding are performed using the same key automaton, but it is different from Mealy machine in generating ciphertext: it does not generate the ciphertext by combining the plaintext bit stream a random bit stream using the exclusive **OR** operator. Dömösi's cryptosystem overcomes many drawbacks of the automata based cryptosystems mentioned above. Firstly, the random number generator is independent from the key. Secondly, the weak reversibility of automata does not affect the cryptosystem, so this system cannot be attacked with methods used for defeating FAPKC cryptosystems. Thirdly, the key automaton is chosen randomly from a large set of automata with more than 256 states and more that 256 input signals, i.e., more than $(256!)^{256}$ possible key automata to be randomly generated. Thus, it gives a lot of options for choosing the key automaton. It is obviously impossible to break the system using brute-force approach. In addition to those advantages, it can be implemented in the software and hardware efficiently due to the simplicity of the operations used. Moreover, Dömösi's cryptosystem overcomes some complicated mechanisms in broadcasting/datacasting systems, i.e., this cryptosystem makes frequent key changes unnecessary and it also makes possible to start decoding at any time during service provision (i.e. not only at the beginning).

However, Dömösi's cryptosystem suffers from the practical difficulties in the encryption algorithm, which affects the entire performance of the cryptosystem. In order to solve these difficulties, Dömösi proposed some modifications in the encryption process with appropriate type of key automata. Comparing with some stream ciphers, the proposed Dömösi cryptosystem is rather slow. In the security level, the resistance against attacks depends on the construction of large minimal and maximal block lengths of ciphertexts, which results in producing much longer ciphertexts than given plaintexts. Hence, this expansion in the ciphertext may affect the performance of encryption and decryption algorithms.

In order to overcome the drawbacks and improve the performance of Dömösi's cryptosystem to a better linear time without backtracking, G. Khaleel at al. [10] proposed an additional control system used integrated into the Dömösi's encryption algorithm. This control system prevents backtracking in the encryption algorithm by generating two vectors according to the current state, input signals and final states. The control system consists of the initialization stage and the operation stage. In the initialization stage, the control system generates all the control vectors V_1 and V_2, where V_1 consists of all input signals that take the automaton from the current state to any non-final state, whereas V_2 consists of all input signals that take the automaton from any state to one of the target final states. In the operation mode, first, the algorithm constructs a prefix of ciphertext of length $t-1$ by randomly selecting signals from vectors V_1, and second, it selects a random signal from V_2 finalizing the construction of ciphertext. Since the modification overcomes the backtracking, the ciphertext is constructed in linear time proportional to the maximum length of the ciphertext blocks.

3. PROPOSED CRYPTOSYSTEM

To reduce the dependency of key automata on the size and reversibility of automata, and enhance the security level, we introduce a new stream cipher by replacing deterministic finite automata in the cryptosystems with their nondeterministic counterparts. In nondeterministic

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

finite automata model (NFA), we can use same ciphertext signals to increase numbers of ciphertext blocks, hence increasing the system immunity against many types of attacks such as brute-force attack. However, we cannot directly use the nondeterministic model as a key for encryption and decryption, due to "nondeterminism". Because, in the decryption process, the key automaton cannot uniquely define the next state to move. As it is illustrated in the state diagram in Figure 1, the signal x_0 can take the automaton to different states.

Formally, an NFA is 5-tuple $M = (A, a_0, \delta, \Sigma, F)$ where A is a finite non-empty set of states, Σ is an alphabet of input signals, $a_0 \in A$ is the initial state, $F \subseteq A$ is a set of final states, and $\delta : A \times \Sigma \to P(A)$ is a transition function with the power set $P(A)$ of A.

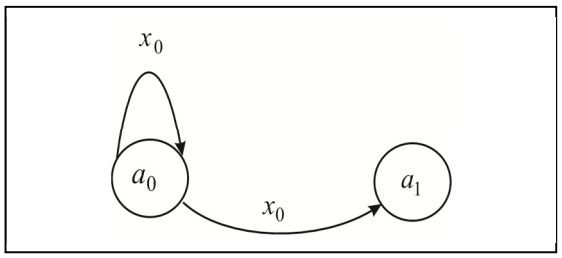

Figure 1: The state diagram of NFA

To use NFA as a key automaton in the encryption and decryption algorithms, we propose the following modified procedure:

1. Let $M = (A, a_0, \delta, \Sigma, F)$ be a nondeterministic automaton. For each signal x in the ciphertext alphabet Σ corresponding to current state $a \in A$, we assign an extra information $i_j \in \{0,1\}^*$ as shown in the Figure 2.

2. To generate these information i_j, we introduce the following procedures:

   - Let a function $\mu : A \times \Sigma \to n$ takes two parameters: the current state a and signal x as an input, and the output parameter is the number of the next state(s). For example, let $\delta(a,x) = \{a_1, a_2\}$, where $a_1, a_2 \in A$, then $\mu(a,x) = 2$.
   - If $\mu(a,x) = 1$ then $i_0 = 0$.
   - If $\mu(a,x) = 2$ then $i_0 = 0$, $i_1 = 1$ etc.

3. We propose a new transition function δ^* takes the key automaton from the current state a to the next state(s) such that $\delta^*(a,x,i_j) \to 2^A$, where the new transition function δ^* takes i_j as an additional argument together with the current state a and ciphertext signal x.

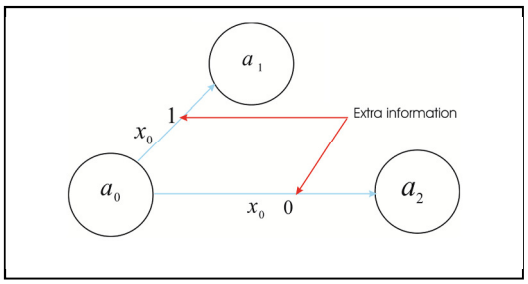

Figure 2: An additional information

4. In order to select an extra information (bits strings) i_j in the encryption and decryption algorithms, we use the same pseudo-random seeds during the encryption and decryption processes, otherwise, the decryption does not produce the same plaintext, and let $i_j = PRNG() \bmod \mu(a,x)$, where a and x are current state and input signal respectively.

New encryption and decryption algorithms based on nondeterministic automata and control system approach are illustrated in the Algorithms 1 and 2.

Journal of Theoretical and Applied Information Technology
31st March 2017. Vol.95. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Algorithm 1: Encryption algorithm

Procedure **MODIFIEDENCRYPTION**

Input: $b_1 b_2 \cdots b_n \in \prod^+$

Output: $w_1 w_2 \cdots w_k \in \Sigma^*$

$p \leftarrow a_0$, $i \leftarrow 1$;

while $i \le k$ **do**

read b_i;

$w_i \leftarrow \lambda$;

select a random t **with** $s_{\min} \le t \le s_{\max}$;

$j \leftarrow 0$;

while $j \le t-1$ **do**

select a random $x \in V_1[p]$

select a random r **with** $\overrightarrow{\hat{\delta}(p, w_i x, r)}$

and $a \notin \phi^{-1}(b_i)$;

$w_i \leftarrow w_i x$;

$p \leftarrow a$;

$j \leftarrow j+1$;

select $x \in V_2[b_i][p]$;

select a random r **with** $\overrightarrow{\hat{\delta}(p, w_i x, r)}$

and $a \in \phi^{-1}(b_i)$;

$w_i \leftarrow w_i x$;

$p \leftarrow a$;

$i \leftarrow i+1$;

return $w_1 w_2 \cdots w_k$;

Algorithm 2: Decryption Algorithm

Procedure **MODIFIEDDECRYPTION**

Input: $x_1 x_2 \cdots x_k \in \Sigma^*$

Output: $b_1 b_2 \cdots b_n \in \prod^+$

$p \leftarrow a_0$, $i \leftarrow 0$; $j \leftarrow 0$;

while $i \le k$ **do**

select a random number r;

$a \leftarrow \hat{\delta}(p, x_i, r)$;

$j \leftarrow j+1$;

if $(a \in F \,\&\, j \ge s_{\min})$ **do**

$j \leftarrow 0$; $i \leftarrow i+1$;

$b_i \leftarrow \phi(a)$;

return $b_1 b_2 \cdots b_n \in \prod^+$;

4. AN EXAMPLE

We consider a small key automaton for our proposed cryptosystem. Let $M = (A, a_0, \delta^*, \Sigma, F)$ be an automaton, where $\Sigma = \{x_0, x_1, x_2, x_3, x_4\}$, and $F = \{a_3, a_4\}$ such that $\phi^{-1}(b_1) = a_3$, where $b_1 \in \prod$ is a plaintext character and the transition function δ^* with the additional information are defined as shown in the Figure 3, and let the length of the ciphertext block is 4.

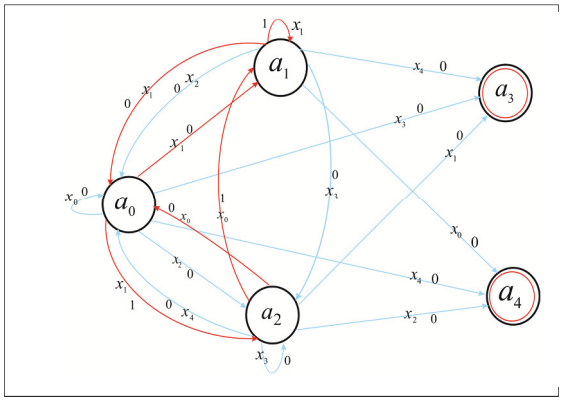

Figure 3: Cryptosystem based on an NFA

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Consider the generation of the ciphertext w_1 corresponding to the plaintext character b_1. Based on the control system approach, we define two vectors V_1 and V_2 for every state, for instance,

$$V_1[a_0] =< x_0, x_1, x_2 >$$
$$V_1[a_1] =< x_1, x_2, x_3 >$$
$$V_1[a_2] =< x_0, x_3, x_4 >$$
$$\ldots$$
$$V_2[a_0, b_1] =< x_3 >$$
$$V_2[a_1, b_1] =< x_4 >$$
$$V_2[a_2, b_1] =< x_1 >$$
$$\ldots$$

First, the encryption algorithm constructs a prefix of ciphertext w_1 by randomly selecting signal x_i from vectors V_1, and at the same time it generates bits string i_j for every signal x_i by using pseudo-random number generator. This process is repeated three times, due to the length of ciphertext block for each plaintext symbol is four. Finally, it selects a signal from V_2 based on the current state and the final state of b_1, finalizing the construction of ciphertext w_1.

Let $\{x_2, x_0, x_3, x_1\}$ and $\{0,1,0,0\}$ be the ciphertext characters and an additional information, respectively, that randomly selected from V_1, V_2 and pseudo-random number generator. Then, the output ciphertext corresponding to the plaintext b_1 is $w_1 = x_2x_0x_3x_1$. Figure 4 shows the produced ciphertext based on the control system and the nondeterministic finite automaton.

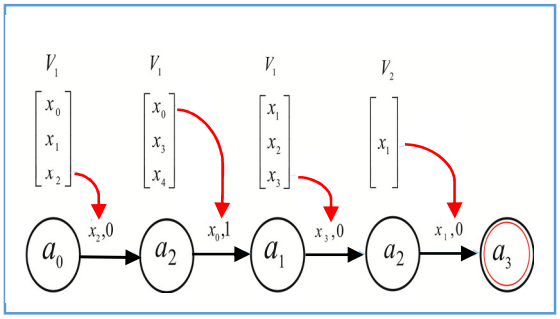

Figure 4: Control system and nondeterministic automata

In the decryption algorithm, the procedure reads the ciphertext characters $\{x_2, x_0, x_3, x_1\}$, at the same time the pseudo-random number generator produces same sequence of the extra control information $\{0,1,0,0\}$ corresponding to the ciphertext characters, then the key automaton goes into states $\{a_0, a_2, a_1, a_2, a_3\}$ under the effect of $\{x_2, x_0, x_3, x_1\}$ and $\{0,1,0,0\}$, hence the state a_3 is the final state, and b_1 is recovered plaintext character, where $\phi(a_3) = b_1$.

5. REDUCING THE DEPENDENCY OF THE LENGTH OF THE CIPHERTEXT BLOCKS

In Dömösi's cryptosystems [2], and also in the modified Dömösi cryptosystem [1], the only way of resisting against various types of attacks is to apply large automata, and relatively large numbers for minimal and maximal length of ciphertext blocks. Therefore, based on Dömösi's method, for every plaintext character, there is at least m^{k-1} ciphertext blocks, where k is the average length of the ciphertext blocks and m is number of signals that take the key automaton to non-final states from the initial state or a final state. For simplicity, consider a small key automaton as shown in Table 1. Let the average length k of all ciphertext blocks is 3 characters.

Table 1: Deterministic key automaton

	a_0	a_1	a_2	a_3
x_0	a_0	a_1	a_2	a_3
x_1	a_1	a_0	a_3	a_0
x_2	a_2	a_3	a_0	a_1
x_3	a_3	a_0	a_1	a_2

Evidenced by Table 1, there are only three input signals take the automaton to non – final state. Hence, the number of the ciphertext blocks corresponding to every plaintext character is $3^2 = 9$. The blocks of the words (accepted strings such that there is no intermediate final states) which take the automaton from initial state to the final state are as follows:

$$\{(x_1x_1x_1), (x_2x_3x_2), (x_1x_0x_2), (x_2x_0x_1), (x_0x_1x_2),$$
$$(x_1x_3x_3), (x_2x_2x_3), (x_0x_0x_3), (x_0x_2x_1)\}.$$

To increase number of the ciphertext blocks, Dömösi already proposed: increasing the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

length of ciphertext blocks (k), for instance, consider $k=5$, then the number of the ciphertext becomes 81 blocks. Some of the samples of the ciphertext blocks are as follows:

$\{(x_1x_0x_0x_1x_1),(x_1x_0x_0x_0x_2),(x_2x_0x_0x_3x_2),(x_0x_0x_0x_0x_3)$
$(x_0x_1x_3x_0x_2),(x_2x_0x_0x_0x_1),(x_2x_3x_0x_0x_2),\ldots\}$.

However, with increased the length of the ciphertext blocks corresponding to given plaintext, the performance of modified Dömösi's encryption algorithm is decreased. Therefore, in this work, we can overcome this weakness as follow. We increased the number of the ciphertext blocks by increasing the numbers of non-final input signals (m). Thus, based on nondeterministic properties, we can use same signals in the ciphertext set (Σ). For instance, we can increase the number of ciphertext blocks in the above example from 9 to 81 blocks by adding 6 identical input signals to the automaton as shown in Table 2. Samples of ciphertext blocks based on nondeterminism way are as follows:

$\{(x_0x_2x_1),(x_0x_0x_1),(x_0x_2x_3),(x_0x_0x_2),(x_0x_3x_2),$
$(x_1x_3x_3),(x_1x_0x_3),(x_1x_1x_1),(x_1x_0x_2),\ldots\}$.

Table 2: Nondeterministic key automaton

	a_0	a_1	a_2	a_3
x_0	a_0,a_2,a_1	a_1,a_0,a_2	a_2,a_1,a_2	a_3
x_1	a_1,a_0,a_2	a_0,a_2,a_1	a_3	a_0
x_2	a_2,a_1,a_0	a_3	a_0,a_2,a_1	a_1
x_3	a_3	a_2,a_1,a_0	a_1,a_2,a_0	a_2

6. Security and Performance Tests

A strong cipher is capable of resisting against all types of attacks such as statistical, differential, brute-force, known-plaintext, chosen-plaintext and adaptive-chosen plaintext attacks. On the other hand, the computational performance of encryption and decryption schemes is very important. In this section, we perform a series of tests to estimate the security and performance of the proposed cryptosystem.

6.1 Key Space

In the proposed stream cipher, a large key automaton is used for encryption and decryption in order to avoid many types of attacks. For instance, brute-force attacks. Consider the number of input signals is $|\Sigma|=m$ and also the number of states is $|Q|=k$ in the key automaton. Based on nondeterminism, each input signal takes the automaton from a current state to a set of states i.e., $\delta: Q\times\Sigma^*\rightarrow 2^Q$, such that each one of these state is non-final states. Thus, that is the number of possible key automata is more than $(2^k!)^m$. For instance, consider $m=256$ and $k=256$, this gives more than $(2^{256}!)^{256}$ option for choosing the key automaton, where each automaton can be filled in with different elements (states). We should mention again that the key space of the modified Dömösi's cryptosystem is $(k!)^m$.

6.2 Cryptanalytic Attacks

This section discusses several standard attacks against the proposed stream cipher, such as brute-force attack, known plaintext attack, adaptive or non-adaptive chosen-ciphertext attack and chosen-plaintext attack, through the following an experimental test.

First, based on Dömösi's method [7], each plaintext character associated with several ciphertext blocks. The number of all the ciphertext blocks corresponding to every plaintext character one is x^{y-1}, where x is the total number of nonfinal states in all the column of the transition matrix, while y is the average of the minimal and maximal length of the ciphertext block. Consider the proposed stream cipher consists of a large key automaton with 256 input signals and 256 states. Let the number of the final states is 16 states, and for each current state and non-final input signal, the next state is an element of the set of two nonfinal states i.e., the number of nonfinal states x in all column of the transition matrix is $(256-16)\times 2=480$ final states. Therefore, the total number of all ciphertext blocks corresponding to every plaintext character is $x^{y-1}=480^{y-1}\approx 2^{8.9(y-1)}$.

Second, based on the above facts, we can conclude the that the brute-force attacks (exhaustive key search), known plaintext attack, chosen plaintext attack and even the adaptive chosen plaintext attack cannot be attacked the proposed cryptosystem, due to the following reasons:

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- A sidereal number of key automata. For example, let $m = 256, k = 256,$ then the number of key automata is more than $(2^{256}!)^{256}$. So, breaking this is infeasible, even with quantum computers.
- A huge number of ciphertext blocks that associated with every plaintext character, let $y \geq 16,$ then the numbers of the ciphertext blocks corresponding to each plaintext character are shown in Table 3.
- The relation between the plaintext and its associated ciphertext is independent (the proposed cryptosystem like Dömösi's cryptosystem is not a standard system [8].
- The relation between the random number generator and the ciphertext is independent.
- The statistical analysis showed that the stream bytes of the ciphertext is random, moreover it has a uniform character distribution.
- With nondeterministic key automaton, more than one plaintext character could be ordered to one ciphertext block as shown in the Figure 5. In this simple example, there are two identical ciphertext blocks corresponding to different plaintext characters, thus $w_0, w_1 \in \Sigma,$ where $w_0 = w_1 = x_0 x_1 x_2.$

Table 3: Number of ciphertext blocks

Length of ciphertext (y)	No. of ciphertext blocks
16	2^{133}
18	2^{151}
20	2^{169}
22	2^{186}
24	2^{204}
30	2^{258}

6.3 Statistical Analysis

In order to test the randomness of proposed cryptosystem, we test the sequence of stream bytes of the output ciphertext, by using ENT 2008 program [11]. To perform these tests, we use a random sample of plaintext of size 5 KB and about 90 KB size of ciphertext, let the minimal length of the ciphertext block is 9, maximal length of ciphertext block is 10 and for each signal there are several additional signals. Table 4 shows that the output ciphertext has high entropy. So, the information is essentially random. In addition, the arithmetic mean value of the proposed cryptosystem reaches to 127.5, thus the information is close to the true randomness. Chi-square distribution test shows that the byte sequences of the ciphertext are random. Moreover, the serial correlation coefficient is close to the zero, which means that the byte sequence of the ciphertext is uncorrelated.

Table 4: Randomness test of the proposed cryptosystem

Extra signals	Entropy	Chi-square	Mean value	Monte Carlo	Serial correlation
2	7.997814	21.99%	127.48	3.1362	0.0008
3	7.998164	89.10%	127.54	3.1517	0.0026
4	7.997949	49.28%	127.88	3.1496	0.0087
5	7.998037	67.38%	127.88	3.1453	0.0023

Moreover, the simulation graphics of character distribution illustrate that characters in the ciphertext have good uniform distribution, the fraction of each character ranges from 0.003 to 0.0037 as shown in Figure 6.

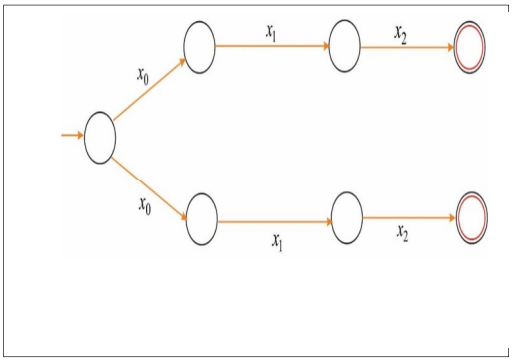

Figure 5: Ciphertext based on NFA

Journal of Theoretical and Applied Information Technology
31st March 2017. Vol.95. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

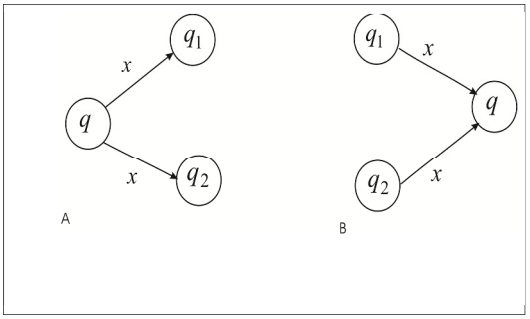

Figure 6: Character Distribution

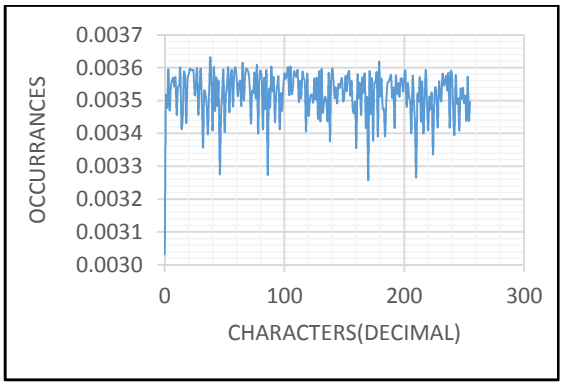

Figure 7: The Prohibited Configuration

Finally, we can say that sequence of stream byte of the output ciphertext is random. Hence, the proposed cryptosystem is strong against statistical attacks.

6.4 Reversibility Versus Nondeterministic Finite Automata

One of the famous results by [12], there exists a polynomial time and linear space algorithm to identify the automaton of k-reversible languages by using characteristic sample sets. So, there is a serious attack against the modified Dömösi's cryptosystem. Therefore, in order to prevent a reversibility attack against the introduced stream cipher, we proposed a nondeterministic finite automaton as a key automaton for encryption and decryption. Therefore, this section presents some definitions and methods to prove that the nondeterministic configuration is forbidden in the construction of reversible automata.

Consider an automaton $M=(Q,q_0,\delta,\Sigma,F)$.

Definition 1. [13] the automaton M that contains neither the configuration given by Figure 7a nor the configuration given by Figure 7b is said to be reversible (injective).

Method 1. [14] Given a non -negative integer k, the automaton M is k-reversible if M is deterministic automaton and the reverse automaton $M^r=(Q,q_0,\delta^r,\Sigma,F)$ is deterministic where $\delta^r=\{b\in Q \mid a\in\delta(b,x)\}$. Figure 8 shows the deterministic automaton and reverse deterministic automaton.

Eventually, based on the above results, it is not difficult to verify that the nondeterministic finite automata are irreversible automata and its configuration cannot be used to generate the k-reversible automata, and all reversible automata are deterministic automata. Thus, this cannot use the famous results by [91] to attack the cryptosystems based on finite nondeterministic automata.

6.5 Performance Tests

The experiments results are taken on Lenovo Notebook E430 machine having Intel(R) Core(TM) i5-3230M CPU 2.6 GHz with 4 GB RAM under 64-bit Operating System Windows 10.

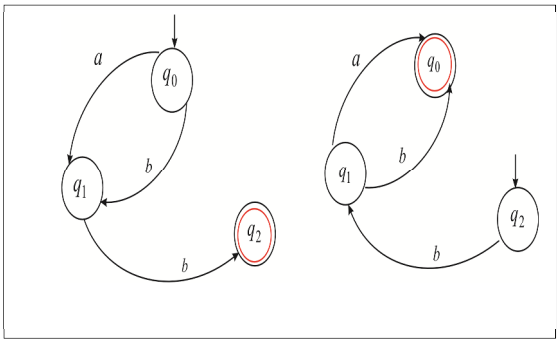

Figure 8: Deterministic automaton and reverse deterministic

The Visual Studio 2013 is used for the implementation of the algorithms. The simulation programs are compiled using C++. In these speed tests, we apply large nondeterministic key automaton $M=(Q,q_0,\delta,\Sigma,F)$, for instance, the number of states and number of input signals are 256. Let the number of final states be 16. Moreover, for each nonfinal input signal $x\in\Sigma$, there is an associated set of nonfinal states consists of two states.

Journal of Theoretical and Applied Information Technology
31st March 2017. Vol.95. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The first performance test is conducted between a novel stream cipher based on NFA and modified Dömösi's cryptosystem. Where, each one of them produces the same number of ciphertext blocks corresponding to each plaintext character. For the modified Dömösi's cryptosystem, consider the average size of the ciphertext block is 10 characters with same above key automaton. Thus, it gives more than 240^{10} cipher blocks. While, in the proposed stream cipher based on NFA, we can generate the same number of the ciphertext blocks by increasing the size (cardinality) of the set of nonfinal states that associated with each nonfinal input signal to 240, in addition to this, decreasing the average length to only 5 characters long.

Figure 9 shows the performance test of a novel stream cipher based on NFA and the modified Dömösi's cryptosystem in terms of the throughput of the ciphertext

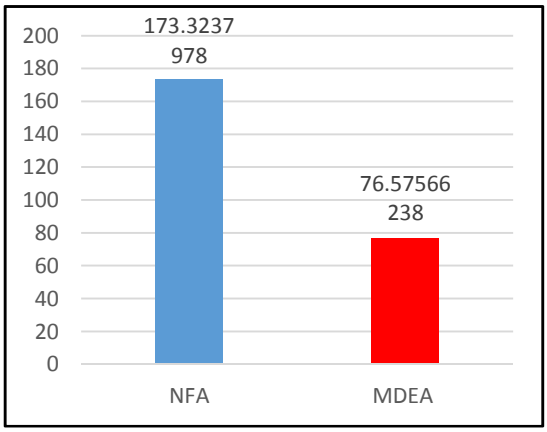

Figure 9: Throughput Of MDEA And Stream Cipher Based On NFA

While, the second speed test is performed between a novel stream cipher based on NFA and second version of Dömösi's cryptosystem. Figure 10 simulates the speed test of stream cipher based on NFA and second version of Dömösi's cryptosystem in terms of throughput.

From above Figures, it is not difficult to see that the throughput of proposed stream ciphers based on NFA has the advantage over MDEA and DEA II.

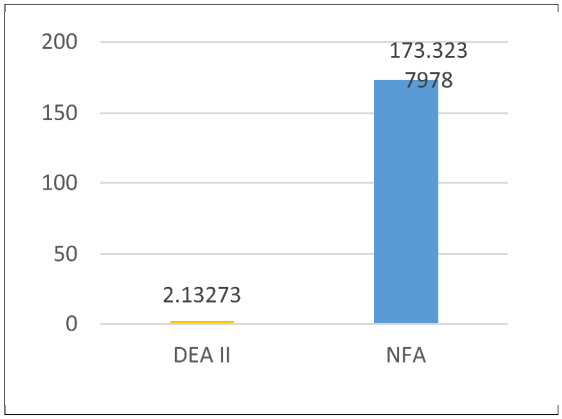

Figure 10: Throughput of DEA II and stream cipher based on NFA

7 CONCLUSIONS

This paper proposed a novel stream cipher based on nondeterministic finite automata as keys for encryption and decryption. Simple example showed how to use a nondeterministic automaton as a key automaton. While, security and performance analyses proved that the proposed novel cryptosystem can resist against many types of attacks, and it has a high performance.

ACKNOWLEDGMENT

This work has been supported through International Islamic University Malaysia Research Initiative Grant Scheme **RIGS16-368-0532**.

REFERENCES

[1] R. Tao, S. Chen, "A finite automaton public key cryptosystem and digital signature", Chinese Journal of Computers 8(6), pp. 401–409, 1985.
[2] R. Tao, S. Chen, "Two varieties of finite automaton public-key cryptosystem and digital signatures", J. of Compt. Sci. and Tech. 1, pp. 9–18, 1986.
[3] F. Bao, Y. Igarashi, "Break finite automata public key cryptosystem", In: International Congress of Mathematicians, pp. 147–158, 1995.
[4] R. Tao, S. Chen, "FAPKC3: a new finite automaton public key cryptosystem", Journal of Computer Science and Technology 12(4), pp. 289–305, 1997.
[5] R. Tao, S. Chen, "The generalization of public-key cryptosystem FAPKC4", Chinese Science Bulletin 44(9), pp. 784–790, 1999.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[6] Gysin, M. "A one–key cryptosystem based on a finite nonlinear automaton". Cryptography, Policy and algorithms. Lecture Notes in computer science, vol.1029, 165-173, Springer, 1996.

[7] P. Dömösi, "A novel cryptosystem based on finite automata without outputs", In: M. Ito, Y. Koboyashi, and K. Shoji (eds.), Automata, Formal Languages and Algebraic Systems, World Scientific, p. 23-32, 2008.

[8] P. Dömösi, "A novel stream cipher based on finite automata", In: IntelliSec – The 1st International Workshop on Intelligent Security Systems. Bucharest, Romania (November 11-14, 2009).

[9] P. Dömösi, P.: US. Pub. No. US 2009/0092251 A1.

[10] Khaleel, S. Turaev, M.I. Mohd Tamrin and I.F. Al-Shaikhli, "A Performance Improvement of Dömösi's Cryptosystem", AIP Conference Proceedings 1705, 020007, 2016.

[11] ENT2008. A pseudorandom number sequence test program. http://www.fourmilab.ch/random

[12] D. Angluin, "Inference of reversible language", J. Assoc. Comput., Mach., 29 (1982), 741-765.

[13] J. Eric. On the languages accepted by finite reversible automata. Vol. 267 of the series Lecture Notes in Computer Science pp. 237-249. Springer. 2005.

[14] J. Falucskai. On the k-reversibility of finite automata. Annales Mathematicae et Informaticae. 36, pp. 71–75. 2. 2009.