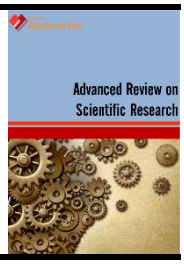
Penerbit Akademia Baru

Journal of Advanced Review on Scientific Research

Journal homepage: www.akademiabaru.com/arsr.html
ISSN: 2289-7887



An overview of cryptosystems based on finite automata

Open Access

G. Khaleel, S. Turaev [1,*], I. Al-Shaikhli, M.I. Mohd Tamrin

Department of Computer Science, Kulliyah of Information and Communication Technology, International Islamic University Malaysia, 53100 Kuala Lumpur, Malaysia

ARTICLE INFO

Article history:
Received 20 September 2016
Received in revised form 3 November 2016
Accepted 5 November 2016
Available online 11 November 2016

Keywords:
Formal languages, Finite automata, cryptosystem, Dömösi's cryptosystem

ABSTRACT

Finite automata are backbones of the cryptosystems based on language theory. Most of the cryptosystems based on grammars and word problems are either insecure or do not satisfy digital signature prosperities. Basically, the cryptosystems based on automata are classified into cryptosystems based on: transducers, cellular automata and acceptors (i.e., finite automata without outputs). In this paper, we discuss the advantages and disadvantages of the important cryptosystems based on finite automata such as FAPKC, Gysin, Wolfram, Kari, Dömösi's cryptosystems and modified Dömösi's cryptosystems.

1. Introduction

A cryptography is a method or mechanism to protect the transmitting information in a particular form through insecure channels. The aim of cryptography is to provide: authentication, confidentiality (privacy), integrity and non-repudiation. Authentication is the procedure of proving the identity. It means that before transmitting sensitive information, the sender and receiver identity should be confirmed. While, a confidentiality means that the information should be out of hands of unauthorized users, or only the intended receiver can read this information. Therefore, encryption and decryption are used to achieve the confidentiality. The data integrity is an important factor in the cryptography, it means that the received message should be exactly the sent message. A checksum or hash function may be used to find corruption errors and evaluate overall data integrity. Non repudiation is the ability of a system to confirm that a sender cannot refuse having sent message.

Based on the key type, the cryptosystems can be classified into symmetric key (private key) and asymmetric key (public key) cryptosystem. In a symmetric cryptosystem, a system depends on using the same key for encryption and decryption. While, in an asymmetric cryptosystem there are two types of keys: public key can be used to encrypt the messages and private key to decrypt the encoded

* *Corresponding author.*
E-mail address: sherzod@iium.edu.my (S. Turaev)

messages. Also, based on the length of plaintext, we can classify the symmetric cryptosystem into block ciphers and stream ciphers.

The basic idea of cryptosystems based finite automata is quite simple: the encryption key consists of an automaton and its inverse is the decryption key. Therefore, and in many cases it is difficult to find the automaton that inverts the function of a given automata. Moreover, these systems have been designed in order to overcome the biggest drawbacks of the cryptosystems based on grammars and word problems, i.e., insecurity, ciphertext expansion and lack of digital signature. Most of finite automata based cryptosystems use transducers machines (Mealy and Moore machines), cellular automata, and automata without output (acceptors).

2. Cryptosystems based on cellular automata

2.1 Wolfram's Cryptosystem

The first cellular automata (CA) based cryptosystem was introduced by S. Wolfram in 1985 [1]. The cryptosystem is based on a simple one-dimensional cellular automaton, which consist of a circular register with cells, where each cell has a value a_i equal to 0 or 1. The values are changed synchronously in discrete time steps based on the rule $a_i' = f(a_{i-1}, a_i, a_{i+1})$, (for instance, the rules: 30,90,150). Where the function f is the next state based on itself state and on its two neighbours' states left and right. The key or the seed of the key is the initial state, and the ciphertext output can be generated from binary plaintext based on the relation $C_i = P_i \oplus a_i'$. By repeating same operation, plaintext can be recovered, but if the sequence a_i' is known. This system has been successfully attacked by known - plaintext, due to lack of the key. The weaknesses of this cryptosystem were shown by Meier and Staffelback [2]. Many random number generators and also linear feedback shift registers depend on Wolfram's system concept.

2.2 Kari's cryptosystem

In order to improve the security and performance of the cryptosystems introduced in [1], J. Kari [3] proposed the use of reversible cellular automata (RCA) as efficient encryption and decryption devices. The security of this system depends on the difficulty of finding the inverse of given cellular automaton. This system consists of multi-dimensional array of cells, and can be used as a symmetric key, and also as a public-key cryptosystem. In the symmetric key, the encryption is done by applying RCA on plaintext. The plaintext can be recovered from the ciphertext by applying the inverse of RCA. Moreover, Kari designed a public key cryptosystem based on RCA, and consist of at least two dimensional of states, due to all the one-dimensional RCA can be inverted. The main problem is that the size of the public key is very big. On the other hand, the most advantages of the two types of RCA cryptosystem is both the encryption and decryption can be performed in parallel manner.

3. Cryptosystems based on mealy machine

3.1 FAPKC cryptosystems

In 1985, Tao and Chen [4,5] proposed a public key cryptosystem based on Mealy machine, which is called finite automata public key cryptosystem (FAPKC). The idea of this cryptosystem depend on difficulties in inversion of composed of finite automata. These systems have many advantages, first, these systems are very fast and can be implemented in both software and hardware, and second,

they also can be used for confidentiality and digital signature. In these systems, the public key consists of combination of two finite automata, while the private key consists of the inverse of these automata. The first automaton is non-linear weakly invertible with delay 0, while the second one is linear invertible with delay τ. Obviously, it is hard to invert the combined automata without knowledge of the private key automata. However, after 10 years, in 1995, Bao and Igarashi [6] found some security weakness in the system. FAPKC (0, 1 and 2) cannot resist against chosen plaintext attacks. Thus, to prevent attacks, a refinement of this system, called FAPKC3, was developed in [7]. But this modification was broken by Meskanen [8]. Finally, Tao et al. introduced FAPKC4 in [9], which is secure and still retains merits of the early FAPKC's such as the fast speed, relatively short public key and can be easily implemented, since it includes only logic operations. FAPKC4 was practically used in some local networks in China.

Another modification on FAPKC was conducted in 2010 by S. Chopuryan, G. Margarov [10]. To improve the security of FAPKC against chosen plaintext attacks, the authors proposed a modified FAPKC: the successful chosen plaintext attack is conditioned by usage of nonlinear weakly invertible finite automata (WIFA) with delay 0 and linear weakly invertible finite automata with delay τ. The task of chosen plaintext attacks is reduced the number of arguments of a system of nonlinear equations. Therefore, to increase the number of these arguments (i.e., increase the length of public key), the authors introduced two ways. First way, by increasing the encryption automaton delay τ to the nonlinear component automaton into a WIFA with delay τ_1. Second way, by making the component linear WIFA automaton's delay longer by adding new states to its state alphabet. Where, delay τ_1 proportional to number of states of linear WIFA. The security analysis proved the modified FAPKC is secure against brute force attacks and also chosen ciphertext attacks, due the growth of public key size.

3.2 Gysin's cryptosystem

Since several cryptosystems based on Mealy machine with different approaches have been developed: M. Gysin [11] 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 also 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.

4. Cryptosystems based on finite automata without outputs

4.1 Dömösi's cryptosystem

In 2008, P. Dömösi [13] proposed a new stream cipher based on Rabin-Scott model of finite 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 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 implement the cryptosystem 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) [4]. 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 also affect the performance of encryption and decryption algorithms.

4.2 Horvath and Dömösi's cryptosystem

In 2015, G. Horvath and P. Dömösi [12] designed a novel block cipher based on Gluskov product of automata (permutation automata). The system consists of two main parts, the pseudorandom generator, and a collection of permutation automata. The first part, the pseudorandom generator produces two blocks of signals each time, one is constant, secret and part of the key (core vector), and the other block is changed each time when using the encryption (initialization vector). The recent seed can be calculated as a function of these two blocks. These blocks have been designed in order to create different ciphertext each time when encrypting the same plaintext. The encoding depends on an encryption function, which has been created in order to improve the security of the cryptosystem. This function first receives three parameters: the plaintext block and two pseudorandom blocks, then after many round, the ciphertext is generated. Decoding done with the same function, but it has different parameters: ciphertext block and the two pseudorandom blocks in the opposite order, and the output is the plaintext. The results of the performance tests showed that the encoding time is more than 7 MB per second, and decoding time is about the same. On the other hand, the system has the optimal avalanche effect.

4.3 Modified Dömösi's cryptosystem

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. [14, 15] proposed an additional control system used together with 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. The performance test showed that the throughput of the modified Dömösi's encryption algorithm reaches to 100MB/s.

Regarding to the security level of modified Dömösi's cryptosystem, the system has the same security of Dömösi's cryptosystem. Moreover, the statistical analysis showed that byte sequence of the encoded messages is random.

4.4 A stream cipher based on nondeterministic finite automata

To reduce the dependency of key automaton on the size of the length of the ciphertext blocks and reversibility of automata and enhance the performance and security levels, [16] introduced a new stream cipher based, replacing as deterministic finite automata in the system with their nondeterministic counterparts. The authors used a specific nondeterministic finite automaton accepter model as a secret key for encryption and decryption. However, the one cannot directly use the nondeterministic model as a key automaton, due to "nondeterminism". Because, in the decryption process, the key automaton cannot uniquely define the next state to move. Therefore, to solve the nondeterminism issue, the authors proposed some modifications in the structure of the transition function as well as assigned some extra information (bits string) for each signal in the ciphertext alphabet based on a pseudorandom number generator. The authors used the identical ciphertext signals to increase numbers of the ciphertext blocks corresponding to each plaintext character, consequently, improving the system immunity against many types of attacks such as brute-force attacks and analytical attacks. Then, no need to increase the size of the ciphertext blocks, hence, the performance of the proposed stream cipher is improved.

4.5 A block cipher based on finite automata systems

For further security and performance improvements, a new block cipher based on finite automata system is proposed [17]. The authors exploited the idea of parallel computations in order to design a new block cipher to achieve high security as well high performance. The idea of this block cipher depends on executing several different machines (automata) for encryption and decryption concurrently. Therefore, they proposed two main parallel models, one for encryption scheme, and the other for decryption scheme. The procedure involves dividing the plaintext or the ciphertext into more than one part based on the number of cores in the CPU/GPU and sending different parts to different cores for execution (encryption/decryption) concurrently and independently. Where the encryption and decryption algorithms used in these models are the counterparts of the encryption and decryption algorithms of the stream cipher based on nondeterministic finite automata. Moreover, in this work, the authors suggested a diffusion round (permutation box) in the encryption algorithm to increase the complexity of the proposed encryption scheme. The security of this block cipher depends on many levels: the number of cores, each core executes different key automaton and the permutation box. While, in the performance part, the proposed block cipher depended on number of cores in CPU/GPU.

5. Conclusion

This paper is devoted to present some important cryptosystems based on finite automata. The structure, strength points and weaknesses of these cryptosystems are illustrated. Most of systems based on Mealy machine and cellular automata are either insecure or unpractical. Though, Dömösi's cryptosystems have many advantages over many others stream ciphers, however, this cryptosystem suffers from security weaknesses and the practical difficulties in the encryption algorithm. Eventually, in order to improve the performance of Dömösi's cryptosystem, the modified Dömösi's cryptosystem has been designed. This system uses control vectors together with the second version of Dömösi's cryptosystem to overcome the backtracking search, and improve the performance to a better linear time. However, this system still depends on length of the ciphertext block to reach a high security of the deterministic version. Thus, to reduce the dependency on the length of the ciphertext blocks and also on the deterministic automata, a novel stream cipher based on nondeterministic finite automata has been introduced. Moreover, for further security and performance improvements, a new block cipher based on finite automata system has been designed.

Acknowledgement
This work has been supported through Fundamental Research Grant Scheme FRGS13-066-0307, Ministry of Education, Malaysia.

References

[1] Wolfram, Stephen. "Cryptography with cellular automata." In *Conference on the Theory and Application of Cryptographic Techniques*, pp. 429-432. Springer Berlin Heidelberg, 1985.
[2] Meier, Willi, and Othmar Staffelbach. "Analysis of pseudo random sequences generated by cellular automata." In *Workshop on the Theory and Application of of Cryptographic Techniques*, pp. 186-199. Springer Berlin Heidelberg, 1991.
[3] Kari, Jarkko. "Cryptosystems based on reversible cellular automata." *Manuscript, August* (1992).
[4] Tao, Renji, and Shihua Chen. "A finite automaton public key cryptosystem and digital signatures." *Chinese Journal of Computers* 8, no. 6 (1985): 401-409.
[5] Tao, Renji, and Shihua Chen. "Two varieties of finite automaton public key cryptosystem and digital signatures." *Journal of computer science and technology* 1, no. 1 (1986): 9-18.
[6] Bao, Feng, and Yoshihide Igarashi. "Break finite automata public key cryptosystem." In *International Colloquium on Automata, Languages, and Programming*, pp. 147-158. Springer Berlin Heidelberg, 1995.
[7] Tao, Renji, Shihua Chen, and Xuemei Chen. "FAPKC3: a new finite automaton public key cryptosystem." *Journal of Computer science and Technology* 12, no. 4 (1997): 289-305.
[8] Meskanen, Tommi. *On finite automaton public key cryptosystems*. Turku Centre for Computer Science, 2001.
[9] Tao, Renji, and Shihua Chen. "The generalization of public key cryptosystem FAPKC4." *Chinese science bulletin* 44, no. 9 (1999): 784-790.
[10] Chopuryan, Siranush, and Gevorg Margarov. "Modification of Finite Automata Public Key Cryptosystem." *Journal of Information Security Research* 1, no. 2 (2010): 39-54.
[11] Gysin, Marc. "A one-key cryptosystem based on a finite nonlinear automaton." In *Cryptography: Policy and Algorithms*, pp. 165-173. Springer Berlin Heidelberg, 1996.
[12] Dömösi, Pál, and Géza Horváth. "A novel cryptosystem based on abstract automata and Latin cubes*." *Studia Scientiarum Mathematicarum Hungarica*52, no. 2 (2015): 221-232.
[13] Dömösi, P. "A Novel Cryptosystem Based on Finite Automata Without Outputs." *Ito, M., Kobayashi, Y., Shoji, Kunitaka, S., eds., AFLAS* 8 (2010): 23-32.
[14] Khaleel, Ghassan, Sherzod Turaev, and Tamara Zhukabayeva. "A Novel Stream Cipher Based on Nondeterministic Finite Automata." *AIP Conference Proceedings* 1705, 020007, 2016.
[15] Khaleel, Ghassan, Sherzod Turaev, M. Izzuddin M. Tamrin, and Imad F. Al-Shaikhli. "Performance and Security Improvements of Dömösi's Cryptosystem." *International Journal of Applied Mathematics and Statistics™* 55, no. 2 (2016): 32-45.

[16] Khaleel G., Turaev, S., Zhukabayeva T. “A novel stream cipher based on nondeterministic finite automata”. In: Information Technologies in Science, Management, Social Sphere and Medicine (ITSMSSM 2016), 23-26 May, 2016, Tomsk, Russia, Atlantis Press, 110-191. 2016.

[17] Khaleel, Gh, SHERZOD TURAEV, and M. I. M. Tamrin. "A New Block Cipher Based on Finite Automata Systems." *International Journal on Perceptive and Cognitive Computing* 2, no. 1 (2016).