STUDIA INFORMATICA
Nr 2(13) Systems and information technology 2009

Cryptosystem Based on Reversible Two-dimensional Cellular Automata

Andrzej Wiśniewski
Institute of Computer Science, University of Podlasie
St. 3 Maja 52, 08-110 Siedlce, Poland

Abstract: Cellular Automata have been successfully applied to several scientific problems such as among others image processing or data encryption. One could find reversibility of dynamics is a fundamental feature of nature. While the most CA are not reversible in nature, one can find some CA with simple behavior could be reversible. Reversible cellular automata (RCA) as efficient encryption and decryption devices was originally conceived by Kari. In this introduction paper, we analyze and develop reversible cellular automata (RCA) based on Kari's idea and some Clarridge's concepts.

Keywords: Cellular automata, reversibility, cryptosystem

1 Introduction

Many fields like financial information, military strategies, business or personal data all require cryptography so as to preserve secrecy or integrity. Cryptography is critical while in sending over untrusted communication medium. It is clear that security of the cryptography systems depends upon the fact that only authorized parties have the complying keys. From the point of view both uniqueness and randomness are necessary components that kind of system. History of cryptography begins thousands of years ago, but when we analyze modern methods of encryption we could find, under basic classification, three follows principal categories of cryptographic algorithms. Firstly encryption function works on a set number of bytes at time (usual called a block cipher) or by encryption individual elements (called a stream cipher). Both of them we direct to symmetric cryptography (because encryption and decryption keys are the same). Some example of popular symmetric algorithms include AES, Blofish, AES. Another, relatively new, cryptographic approach is the use asymmetric key algorithms (based on creation key pair: a private key and published public key). The considered keys are mathematically related and for given public key it is computationally infeasible (factorization problem as the decomposition of an number, a polynomial or a matrix object) to find private key. Well-regard asymmetric key techniques include e.g. DSS, ElGamal, RSA. The third

category, cryptography hush function, includes procedures that takes an arbitrary block of data and returns a fixed-size bit string – the hash value. One can find that any change (accidental or intentional) to the data will change the hash value. The list of cryptographic hash functions is long including, among others, SHA-0, RIPEMD and MD5.

Cellular Automata (CA) has came out as a very practical concept especially for implementing different complex functions (e.g. modeling physic structures). Within cryptography systems cellular automata may be used as a pseudorandom generators. The generating systems based on CA needs initial state which defined the secret key. That kind of systems is known as stream ciphers. The problem considered above was first studied by Wolfram [23], Gutowitz (considering both reversible and irreversible rules) [8] and recently by Tomassini-Perrenou (cit. in [21]), Seredynski [18]). Another cryptosystems were proposed by Kari [10,11], Clarridge [4,5] use reversible CA. In such RCA (reversible cellular automat) system uses two keys, one key for encryption and the other for decryption security depends on difficulty of finding inverse cellular automaton.

From computationally intensiveness point of view symmetric algorithms are in general much less than asymmetric one (such as RSA). That means, in practice, that symmetric key algorithms are hundreds to thousands times faster than asymmetric key algorithms. That stimulate to consider alternative technique like reversible CA, which can be faster than existing techniques. While CA in application mentioned above is very attractive idea, comparing to RSA algorithms one could find some weaknesses of RCA e.g. large number of rules, large grid of cells related to size of plaintext. Cryptography systems based on reversible CA related to security level gain by RSA algorithms needs faster hardware (e.g. parallel computing).

In this paper we present some proposition of extends of Kari's and Clarridge's conceptions for application of reversible CA for asymmetric cryptography.

2 Basic of cellular automata

We define Cellular Automata (CA) as synchronous distributed systems where the next state of each cell only depends, in general, on its own state one time step previously and the current state of its nearby neighbors. This special class of CAs we call totalistic CAs. Notice that all cells on array are updated synchronously in discrete time steps. Under the formal point of view cellular automata is quadruple

$$A = \langle d, Q, N, f \rangle$$

where

$d > 0$ - dimension in integer form,

$Q = \{q_1, ..., q_n\}$ - set of state which is finite and non empty,

$N = \{n_1, ..., n_k\}$ – neighborhood defined as finite subset of Z^d,

$f: Q^N \rightarrow Q$ – transition function of local mapping.

Moreover, formally a d-dimensional CA consist of a d-dimensional (finite or infinite) array of identical cells. State of each cell is changing in discrete step, as we pointed above, according to f - the local rule of the CA. Under basic approach CA-array consists of only cells works under the same rule, so one could call this

kind of array as homogenous. We assume cellular array with periodic boundary condition which is simply the toroidal boundary condition (i.e creating 2-dimensional toroidal array). The special form of set of neighbors around examine cell define type of neighborhood. There are several kind of 1D and 2D neighborhood e.g. Brickwall for 1D, rectangle 2D neighborhood (von Neumann, Moore or Margolus neighborhoods), unaligned (brickwall) rectangular or hexagonal neighborhood. For example the von Neumann neighborhood is the set of neighbors:

$$vN(r) = \{x \in Z^d \mid \Sigma^d_{i=1} | x_i | \leq r \}$$

or in form including rectangular coordinators:

$$N = \{ \{0, -1\}, \{-1, 0\}, \{0,0\}, \{+1,0\}, \{0,+1\} \}.$$

We define *d*-configuration as a map:

$$c : Z^d \rightarrow Q$$

formulating description of states of all the cells in the array.

Let the quadruple, considered above, $A = \langle d, Q, N, f \rangle$ be a cellular automata (CA). The global function mapping of A in form:

$$F_A : Q^Z \rightarrow Q^Z$$

(where symbols $Z \equiv Z^d$) could be defined by

$$(F_A (c) (x) = f (c(x + n_1), \ldots, c(x + n_k))$$

where configuration c is transformed into a new configuration $F_A(c)$ at each time step.

Now we need to apply cellular automata as cryptography system transforming plaintext on cipher form. The receiver of cipher text have to use reversible cellular automata (RCA). Reversibility, in considered sense, is a features of system allowing the system to run backwards and retrace all the steps of previous evolution. We called cellular automata is reversible, if its global map F_A is invertible. The last lemma means that for every possible state of the CA the global function specifies one and only one successor. Alternatively we could say that the global function has to be bijective function i.e. a function F_A from a set X to a set Y with property that, for every y in Y there is exactly one x in X such that F(x) = y and no unmapped element exists in either X or Y. It is obvious that function F_A is bijective (being simultaneously injective and surjective function) if and only if its inverse relation F^{-1}_A is a function. So CA A is irreversible iff the reverse CA exists (i.e. A is invertible and F^{-1}_A is the global evolution function of CA)

The problem considered above is undecidable for 2-dimensional CA, that means there doesn't exist any algorithm that would resolve whether a given CA is reversible or not.

3 Reversible Cellular Automata (RCA)

When we state CA A is injective and thus an RCA so its inverse RCA A^{-1} is as simple as A. Its need to emphasize for given RCA A it is easy to find its inverse A^{-1} only under constructing phase. The outcome RCA for two-dimensional CA can be very hard to invert. The corollary above is directed from Kari's theorem [7]:

"It is undecidable if a given two-dimensional CA is reversible. This is true even when restricted to CA using the von Neumann neighborhood."

As a corollary from theorem above the time for find the inverse A is estimated as function of e.g. number neighborhood. That is theoretical base for applied RCA as a cryptosystem. Let $A= (d, S, N, f)$ be a reversible CA and $A^{-1} = (d, S, N^{-1}, f^{1})$ be its inverse. The input message, called plaintext, is written into e.g. two--dimensional (in general case d-dimensional) array using symbols S (binary, natural language or others). If we denote input configuration created by written plaintext as $p \in Q^{Z} (Z^{d}, S)$ then encryption process would be done after applying RCA A for k time step. As the outcome configuration is recorded we get crypto text $c = F^{k}_{A} (p)$. The original message (plaintext) would be obtained by applying inverse RCA A^{-1} on c for k time steps.

We direct attention on Kari's model and its extension (Clarridge model). The essential idea presents in Kari's paper [10,11] and then develops in Clarridge thesis [5] was to compose together reversible marker cellular automata. The general aim of approach above is to form a more complex automata and its inverse. The way to realize RCA is to define a sequence so-called marker automata defined by state set S, function $f : S \rightarrow S$ and finite set of patterns $P_{1,} P_{2,}...,P_{k}$ around the origin. The function f is applied at time $t+1$ to state of each c if any of the patterns $P_1,P_2,..,P_k$ is present. In the case if any patterns no exist c's state does not change.

As opposed to Kari's model Clarridge defines marker CA where all the patterns use the same neighborhood. Therefore so-called fixed-domain maker cellular automata (FDM CA) may be present as the five-tuple form [4,5]:

FDM CA (d,S, N, A, f)

where:

d – dimension array,

S – state set,

$N = (n_1, n_2,...,n_k), n \in Z^{d},$ for $i=1,2..,k$ - neighborhood vector,

$A \subseteq S^{k}$ active set of elements whose entries correspond to the position defined by N,

f – local rule function.

Applying the FDM CA is similar to model considered above because acting on a cell c the local rule of the marker checks if the neighbors of c are in state configuration corresponding to an element of A. The positive result change state of c under function $f(s)$ on the next generation, otherwise the state of c does not change. However FDM CA checks all patterns in one cycle instead of using sequence markers, as Kari's model.

The both of the analyzed models are used two-dimensional array and different numbers of state and number of markers CA. The example of marker reversible cellular automata (RCA) of Kari's approach is presented on Fig. 3.1.

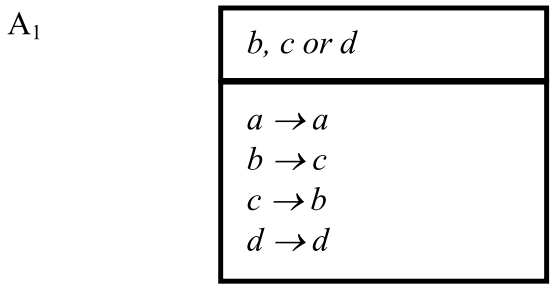

Fig. 3.1 The example of a marker reversible cellular automata (RCA) of Kari's approach [10]

The applied five marker RCA of Kari's approach are all reversible (Fig. 3.1). The patterns enclosed within the RCA define just one cell: top and right neighbor. The two markers CA are defined top cell and three others the right neighbors respectively.

The encryption of input message is obtained by applying $A_1, A_2, ..., A_n$ in the pointed order, which may be present as their composition:

$$A = A_n \circ A_{n-1} \circ ... \circ A_1 .$$

The composition above is the public key of constructed cryptosystem (e.g. that is previously considered mapping of neighborhoods to states after k time steps). The private key is obtained by simply sequentially applied of A_i in reverse order for decryption in the following form

$$A^{-1} = A_1 \circ A_2 \circ ... \circ A_n .$$

Notice that number of markers CA in FDM CA is nearly equal of size of applied array grid on the contrary with only five markers CA of Kari's approach.

4 Security concerning

It is well-know that general aims of cryptanalysis is prepared breaking methods of the secrecy and confidentiality of any communications. The notion of effective security is related to efficiency method which can be found to break the cipher. The one-time-pad cipher pointed by Claude Shannon as unbreakable cipher remains today the only theorize about it. There are considerable number of cryptanalytic attacks, which can classified in any diversity way. Usually the classification is based on two criterion including knowledge of attacker and kind of available capabilities. We can find the following three essential class of attacks [25,27]:

- ciphertext-only, where attacker is assumed to have access only to a set of ciphertexts,
- known-plaintext, where plaintext and ciphertext pairs are available,
- chosen-plaintext, which presumes that cryptanalyst has capability to choose arbitrary plaintext and can obtain their corresponding ciphertexts,

The last one has two forms: batch chosen-plaintext and adaptive chosen plaintext which described different time and form of attacker's access to plaintext.

Others kind of attacks to find some weakness or insecurity in cryptographic system includes side channel and brute force attack. First of them require considerable knowledge of specific operation of the operation system on which crypto sys-

tem works. The side channel attack in general is based on information obtain from physical implementation such crypto system. The second one is general technique includes looking over the search space for possible keys for found the correct. However most of stream ciphers using simple logical operations could be vulnerable to e.g. described brute force attacks. The differential cryptanalysis and known plaintext attacks in that case would be effective on the same level. A considerably different attack is applied to system using public key cryptography (e.g. earlier pointed RSA and of course examined RCA). We can found a few attacks methods like as timing attack, differential power analysis or differential cryptanalysis. The timing attack is based on monitoring the time which is consumed by encryption and encryption processes. The resulting time is support for estimating the key nature. The second one attack is related to observe the power consuming by cryptographic devices. The secret key would be derive from. A well-know differential cryptanalysis attack searches correspondence between the original message (plaintext) and ciphertext [27].

In the case of FDM CA construction the brute force attack requires to revise track of global inputs and outputs in order to invert composed CA. The estimated the number of possible global configuration in this case is $|S|^g$ where g is the number of grid cells [8,15]. The time needed for solving, defined under Big $\boldsymbol{O}$ notation, would be approximately $\boldsymbol{O}(\log g)$. Nevertheless the both of the RCA and RSA algorithms represents the public key cryptography concept. The security of RSA algorithms is based on difficulty of factoring large composite integers. The well-known and particular effective at splitting composite numbers Pollard's rho algorithm was invented by John Polard in 1975. The factorization time calculated under Pollard's algorithm is approximately equal [16,27]:

$$t_F \propto \exp[(64/9)^{1/3} (\ln N)^{1/3} (\ln \ln N)^{2/3}$$

where:

$N = p * q$, p and q are the big prime numbers.

As we mention above Cellular Automata (including reversible version) is one of promising cryptography techniques but comparing times presented above we can find security RCA high not enough.

Due to the properties e.g. number of neighbors, using kind of random generator, fixed size of grid one can discover the RCA might be vulnerable to cryptography attack. The result of forward processing of RCA is the public key, which size would be estimated on the order of $|S|^{|N|}$ (or $S^N \log_2 S$) [3,4,7]. While number of states would be increasing to about 20 and more states which are required for security, a neighborhood size of larger than 2 creates non-acceptable magnitude of increasing of public key.

The number of grid cells needs large value, approximately several hundreds or more, due to the methods of brute force attacks. Another a secure problem is placed within well-designed cryptographic application that as a general rule uses random members. A reliable source of real random bits such as thermal noise in electrical circuits is impossible to get on a computer calculations way only. Instead of we use to create these values a special function called as a Pseudo-Random Number Generator (PRNG). The RCA considered above uses PRNG e.g. to choose transition function f. From the security view point is important using good-designed

PRNGs and use them on ways that make various attack much harder. However the RCA is vulnerable on various form of cryptographic attacks especially of statistic-based or chosen-input attacks distinguish between pseudo-random output and random values.

The several recourses give us some interesting tools against statistical attacks. The proper idea of that approach is based on simply including redundancy in the form "dummy" states into S. The adding states couldn't be used in the plaintext but may be added to working set (e.g. in FDM CA that is an active set) of states. The aim of that is to keep attacker from determining which state was last added to working set. Unfortunately the examined construction of CA which computes one-way function after adding "dummy" inputs (without affect on the output) as well as "dummy" constant outputs doesn't confirm suggestion making above. The proving conclusion states security of most low-level cryptographic algorithms which are frequently used to build computer security systems are not affected by such stuffing [1].

The last not least there exists some proof (Cook's theorem) that even for simply input configuration the inversion problem of two-dimensional CA is NP-hard. The Cook's theorem only suggests that there are a few hard instances but without any information about their frequencies. That is important conclusion in probably case of little fraction of "hard" instance there may be exists efficient algorithm for solving the inversion problem with acceptable probability [1].

5 Discussion of modifications

The problem of building efficient and secure cryptosystems is still open. The RSA algorithm considering earlier is much slower than probably may be RCA or DES and another symmetric cryptosystems. However when we compare the security level of both version of cryptographic applications namely RCA and RSA algorithms one can find that the first could be reviewed in non-acceptable short time (see chapter 4). The RCA cryptosystem achieving high level of security with increasing number of states, size of neighbors, number of iteration are in conflict with high speed and low costs of implementation of the system. With the aim of increasing security level of RCA we apply a transforms the system by coding output product of RCA cryptosystem. The well-know simple XOR cipher operates according to e.g. the principle:

$$(B \oplus A) \oplus A = B.$$

For a given key string of the message may be encrypted by applying XOR operator. Reapplying the key removes the cipher and decrypt the output.

Furthermore the two steps are needed to assure the RCA security cryptosystem on the satisfying level. The first of all the PRNG at series form should be writing in the working table. The input message would be transforming on blocks of the size related to the size of RCA grid of cells. The encryption process of each block (including XOR coding) uses the synchronously pseudo-random series from the working table.

6 Summary

We present two approaches to reversible cellular automata cryptosystem from security view point. The RCA security level in the original form is far away from the acceptable value. Furthermore procedure of the key generation implemented within the FDM CA model makes possibility for attacker to determine which state was last added to "change set". These information would be taking as a starting point to find every elements of compositions in backward order. Increasing of the size of public key seems rather hard (neighborhoods larger than two may be infeasible, accepting larger number of states needs operation on parallel hardware). The interesting idea based on including "dummy" states was proved as ineffective. From that view point we expect higher security level of the composed systems discussed above. We describe some proposition based on the embedded system security. The resulting of estimating security level based on popular cryptographic tools will be presented in the next article.

References

Articles

1. Appelbaum B., Ishai Y., Kushilevitz E., "Cryptography by Cellular Automata or How Fast Can Complexity Emerge in Nature", http://www.wisdom.weizmann.ac.il/~bennyap/pubs/CA.pdf
2. Arcaya I., Romero N., On a Hedlund's theorem and place-dependent cellular automata, http://revistas.luz.edu.ve/index.php/divma/article/viewFile/3117/3002
3. Bao F., "Cryptanalysis of Partially Known Cellular Automata Cryptosystem", IEEE Computer Society 2004, http://scilib.kiev.ua/ieee/tc/2004/11/ty/t1493.pdf
4. Clarridge A., Salomaa K., "A Cryptosystem Based the Composition of Reversible Cellular Automata", http://research.cs.queensu.ca/TechReports/Reports/2008-549.pdf
5. Clarridge A., "Cellular Automata: Algorithms and Applications", 2009, thesis, http://qspace.library.queensu.ca/dspace/bitstream/1974/1724/1/Clarridge_Adam_G_200903_MSc.pdf
6. Durand-Lose J., Representing Reversible Cellular Automata with Reversible Block Cellular Automata, http://www.emis.ams.org/journals/DMTCS/pdfpapers/dmAA0110.pdf
7. Gajardo A. Goles E., Circuit Universality of Two Dimensional Cellular Automata: a Review, http://citeseerx.ist.psu.edu/viewdoc/summery?doi=10.1.1.88.9179
8. Gutowitz H., "Cryptography with Dynamical Systems" 1996, http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.52.7330
9. Kaminski A., Cellular Auotmaa Based Stream Cipher.Lectures notes, www.cs.vit.edu/~arch/lectures/ca/c01/cass01.pdf
10. Kari J., "Cryptosystems based on reversible cellular automata", http://sgldwssr.hp.infoseek.co.jp/kari92cryptosystems
11. Kari J., "Theory of cellular automata: A survey", http://www.lama.univ-savoie.fr/~theyssier/edocs/kariSurvey.pdf
12. Kari J., Undecidable Properties on the Dynamics of Reversible One-Dimensional Cellular Automata, JAC 2008, http://hal.archives-ouvertes.fr/docs/00/27/40/09/PDF/3-14.pdf
13. Kelsey J., Schneier B., Wagner D., Hall Ch. "Cryptoanalytic on Pseudorandom Number Generators" www.eecs.berkeley.edu/~daw/papers/prngs-fse98.ps

14. Morita K., Cellular Automata and Artificial Life, 1998 Summer School on Complex Systems, http://www.iec.hiroshima-u.ac.jp/~morita/pub1.html
15. Philip N.S., Joseph K.B., "Chaos for Stream Cipher",http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.14.1256,
16. Placzek W., „Kwantowy algorytm Shora - czyli jak łamać szyfry", www.if.uj.edu.pl/~placzek/referaty/Shor.pdf
17. Sen S., Hossain Sk.I., Chowdhuri D.R., Chaudhuri P.P., "Cryptosystem Designed for Embedded System Security", Proc. Of the International Conference on VLSI Design (VLSI'03). 2003 IEEE, http://eref.uqu.edu.sa/files/Others/Hardware-Software%20Co-design/Cryptosystem%20designed%20for%20embedded%20system%20security.pdf,
18. Seredynski F., Bouvry P., Zomaya A.Y., "Cellular automata computations and secret key cryptography", http://pascal.bouvry.org/ftp/parco04.pdf
19. Sutner K., The Complexity of Reversible Cellular Automata, http://www.cs.cmu.edu/~sutner/papers/reverse.pdf
20. Taati S., Cellular Automata Reversible over Limit Set?, http://users.utu.fi/staati/articles/AUTOMATA05.pdf
21. Testa II J.S., Investigations of Cellular Automata-based Stream Ciphers, http://ritdml.rit.edu/bitstream/hanadle/1850/7897/JTestaThessis05-2008.pdf....
22. Toffoli T., Computation and Construction Universality of Reversible Cellular Automata, 1976 JCSS, http://pm1.bu.edu/~tt/qcl/pdf/toffolit197718176a6b.pdf
23. Wolfram S., Cryptography with cellular automata, http://dsns.csie.nctu.edu.tw/research/crypto/HTML/PDF/C85/497PDF

Books

1. Koblitz N., Wykład z teorii liczb i kryptografii, Warszawa 1995.
2. Menezes A.J., van Oorschot P.C., Vanstone S.A., Kryptografia stosowana, Warszawa 2005.
3. Schneier B., Kryptografia dla praktyków. Protokoły, algorytmy i programy źródłowe w języku C, Warszawa 1995.

WWW pages

1. www.en.wikipedia.org