Journal of Industrial Information Integration 5 (2017) 17–25

Contents lists available at ScienceDirect

Journal of Industrial Information Integration

journal homepage: www.elsevier.com/locate/jii

A cost-efficient one time password-based authentication in cloud environment using equal length cellular automata

Arnab Mitra[a,*], Anirban Kundu[b], Matangini Chattopadhyay[c], Samiran Chattopadhyay[d]

[a] Computer Innovative Research Society (CIRS), Howrah, 711103, India
[b] Netaji Subhash Engineering College, Kolkata, 700152, India
[c] Jadavpur University, Kolkata, 700032, India
[d] Jadavpur University, Kolkata, 700098, India

ARTICLE INFO

Article history:
Received 29 April 2016
Revised 27 November 2016
Accepted 30 November 2016
Available online 2 December 2016

Keywords:
Cellular automata
Equal length cellular automata
Characteristics polynomial
Authentication
One time password
Cloud computing

ABSTRACT

One time password (OTP) scheme has been suggested as an efficient and simple solution for authentication in cloud computing. This paper investigates the nature of characteristics polynomials of Equal Length Cellular Automata (ELCA) and its application in OTP generation for authentication in cloud computing. In this work, primitive characteristics polynomial is identified as a crucial criterion for pseudo-randomness of ELCA cycles generated with linear rules. Novel algorithms are also designed for (i) cost effective generation of OTPs, (ii) flexible generation of equally populated OTP sets, and (iii) generation of controllable number of passwords in OTP sets. Application of linear rules in synthesis of OTPs ensures easy implementation using only modular arithmetic, which makes the proposed method truly cost efficient.

1. Introduction

The importance of cloud computing in today's life is undeniable. Along with cloud computing, Internet of Things (IoT) is also gaining increasing importance among researchers. In cloud computing and IoT, there are several research issues including efficient data communication, energy consumption management, service discovery and selection etc. [1–4]. Although cloud computing has applications in several critical situations, such systems are susceptible to a variety of security threats mounted by intruders [5]. A large number of research papers has attempted to enhance authentication and security in cloud computing and IoT [1,3,7–12]. As a result, several authentication techniques have been presented by researchers to enhance privacy and data security in cloud environment. Authentication based on multiple factors (e.g., identity-based, smartcard-based, remote password-based) [6,7] and one time passwords (OTPs) [8–11] have been presented recently to enhance security in clouds.

Inherent threats in data communications have been categorized in [13,14] as "Host Compromise" and "Communication Compromise". Combination of hardware and software has been suggested as a solution to host compromise [13]. On the other hand, "Communication Compromise" refers to the threat associated with message communication. Loss of privacy in conversations (eavesdropping), arbitrary modification(s) to received message and replay of old messages are common security hazards faced during transmission of message. Authentication is accepted as a solution to this problem. Authentication means an appropriate arrangement of identification and verification. Three different authentication categories are discussed in the literature: (i) authentication of content (ii) authentication of origin (iii) authentication of general identity [13].

During authentication, one node (sender) is verified by another node (receiver). In basic authentication, encrypted messages independently generated by the sender and the receiver using a symmetric key have to match [13]. Building a complex crypto system for authentication purposes is not typical in cloud computing. Smart phone-based authentication in cloud targeting intelligent transportation system has been described in [15]. Multiple factor-based authentication [6,7], OTP-based authentication [10,11,13], attachment of small piece of high-performance trusted hardware with untrusted units [16], anonymous node ID Assignment [17] are some of the different approaches adopted in cloud computing to enhance authentication.

* Corresponding author.
E-mail addresses: mitra.arnab@gmail.com (A. Mitra), anik76in@gmail.com (A. Kundu), matanginic@gmail.com (M. Chattopadhyay), samiranc@it.jusl.ac.in (S. Chattopadhyay).

http://dx.doi.org/10.1016/j.jii.2016.11.002
2452-414X/

It is discussed in [6] that the identity and smartcard-based remote password authentication scheme is susceptible to user and server masquerade attack, insider attack and off-line password guessing attack. OTP scheme has been suggested as an efficient and simple solution for message authentication in cloud computing [13]. OTP is known to be a time synchronized random password which is used in authentications; this password can be used at most once. The list of generated passwords is stored in the client and the server. A single password from the list is used in a sequential manner for every distinct session. OTP protocol is known to be an effective measure for security in cloud to defend against "Replay Attacks" and "Dictionary Attacks" [13]. Several researchers have worked on use of OTP in cloud environment. For instance, OTP-based authentication and delivery of OTP using SMS and email in cloud computing architecture have been discussed in [18,19]. Self-updating OTP-based authentication [8], time synchronized OTP ("DropLock") [9] have also been described as authentication techniques in the cloud environment.

Cellular Automata (CA) [20–22] has been applied in several fields of computing such as distributed computing [23,24] and parallel computing [25-27]. They have also been used for cost efficient and fast data authentication and for building low computation crypto systems [14,20,22,28–31] for their elegant mathematical structure. Another interesting feature of CA is that CA-based models can be realized by low cost, simple VLSI implementation [20,22,28–31]. Like CA, Equal Length CA (ELCA) can also be applied in bio-informatics, protein synthesis and distributed computing in a cost-efficient manner [32,33]. It is shown in [28] that non-maximal length cycles along with CA-based pseudo-random number generator has been applied in cryptography. Non-group CA-based OTP generation using non-reversibility property of such CAs [10] has been described as a solution towards authentication problem in cloud environment. However, generation of equally populated multiple OTP sets using non-group CA has not been addressed in [10]. In fact, we have not come across any simple approach targeting cost-efficient and controllable generation of multiple and equally populated OTP sets. Hence, a cost effective, simple design of equally populated OTP sets is necessary for enhancing authentication in cloud computing. Towards that end, we have explored principles of ELCA generation using finite state machine (FSM) to investigate properties of ELCA cycles for their application in OTP-based authentication.

Major contributions in this paper are as follows.

(i) It provides a cost-efficient algorithm for ELCA-based OTP set generation.
(ii) It provides an algorithm for OTP assignment in cloud scenario.
(iii) It demonstrates that controlled and equally populated one time password (OTP) sets can be generated by the proposed algorithms.

Rest of the paper is organized as follows. In Section 2, the fundamentals of CA and ELCA are discussed. Some background work of ELCA that is required in the remaining part of the paper is also included in Section 2. Empirical analysis of ELCA is presented in Section 3. The proposed design based on ELCA has been described in Section 4. Results are discussed in Section 5. Conclusions have been drawn in Section 6.

2. Cellular automata preliminaries

Cellular Automata (CA) [20–22] is referred to as a collection of 'valued' cells on a grid of specified shape (dimension) that evolves through several discrete time steps according to a set of rules, based on the states of neighbouring cells. Rules are used iteratively for as many stages as chosen. One-dimensional line grid with null-boundary or periodic-boundary CA (also known as Elementary CA (ECA)) is the simplest to construct [22]. Mathematically, CA is defined as a function of sextuples as described in Eq. (1) [34].

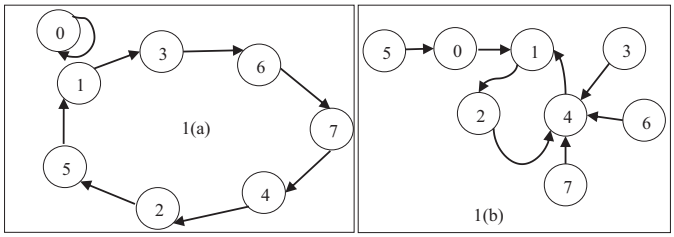

Fig. 1. (a). Typical transition diagram for group CA using ⟨90, 90, 150⟩ (b). Typical transition diagram for non-group CA using ⟨10, 2, 1⟩.

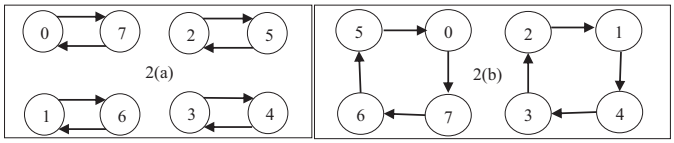

Fig. 2. (a). Four ELCA structures for ⟨51, 51, 51⟩ (b). Two ELCA structures for ⟨153, 153, 153⟩.

$$CA = \langle \Gamma, S, s,\ s_0, N, \Phi \rangle \tag{1}$$

where, countably infinite tessellation of an n-dimensional Euclidean Space R^n is represented by Γ, consisting of cells c_i such that $i \in \mathbb{N}$;

finite set of k states referred as S where often $S \subset \mathbb{N}$;
output mapping function $s : \Gamma \times \mathbb{N} \to S$ produces the state value of cell c_i at the tth discrete time step denoted by $s(c_i,\ t)$;
initial condition for every cell c_i i.e., $s(c_i,\ t)=s_0(c_i)$ is assigned by function s_0: $\Gamma \to S$;
every cell c_i is mapped to a finite sequence $N(c_i) = (c_{ij})_{j=1}^{|N(c_i)|}$ by neighborhood function $N : \Gamma \to \bigcup_{P=1}^{\infty} \Gamma^P$ and $|N(c_i)|$ is the number of all distinct cells c_{ij};
$\Phi = (\phi_i)_{i\in\mathbb{N}}$ is a family of functions $\phi_i : S^{|N(c_i)|} \to S$ such that each ϕ_i is responsible for the dynamics of cell c_i, i.e., $s(c_i, t+1) = \phi_i(\tilde{s}(N(c_i), t))$, as $(\tilde{s}(N(c_i), t)) = (\tilde{s}(N(c_i), t))_{j=1}^{|N(c_i)|}$.
In this paper, we have used three-neighbourhood null boundary ECA for its simplicity.
Following ECA terminologies [22] are needed for subsequent discussions.

Rule Vector- *The set of rules $R = \langle R_1, R_2, \ldots, R_n \rangle$ in a CA is called the rule vector.*

Uniform CA and Hybrid CA- *If the same rule is applied to each cell, it is referred to as a Uniform CA; otherwise it is referred to as a Hybrid CA.*

Group CA and Non-group CA- *If the transition diagrams of a CA are only of circular spaces, it is referred to as Group CA; else it is referred to as Non-group CA.*

Group CA and Non-group CA are depicted in Fig. 1.

In Figs. 1 and 2, CA states are represented by circular/oval shapes. State values are in decimal numbers and are indicated within these circle/oval shapes (states). An arrow shows transition from one state to the next state; ⟨–, –, –,⟩ denotes rule vector responsible for generation of transition diagram for the corresponding ECA.

Linear CA and Non-linear CA- *If the next state of a CA rule can be expressed as a function of 'XOR' or 'XNOR' logic, it is referred to as a Linear CA rule; else it is referred to as a Non-linear CA rule. A CA configuration with all linear rules is referred to as a Linear CA; else, it is referred to as a Non-linear CA.*