

$(Q_i, \Sigma, \delta_i)$  to be isomorphic to  $\mathcal{A}$  for any  $i \in \mathbb{N}$ . First we describe a construction that is a ciphertext.

Define an automaton  $\mathcal{P} = (\{p_1, p_2, \dots, p_{|u|+1}\}, \{0, 1\}, \gamma)$  where  $\gamma$  is defined as follows: for  $i \in \{1, \dots, |u| + 1\}$  set  $\gamma(p_{i-1}, u_i) = p_i$ , where  $u_i$  is  $i$ -th letter of a word  $u$ . In other words we encode our plaintext in the form of a directed path, where consecutive edges correspond to the consecutive letters of the word  $u$ . Encryption consists of four steps:

1. Compute  $\mathcal{B} = \bigcup_{i=1}^{|u|+1} \mathcal{A}_i$  and denote  $\bigcup_{i=1}^{|u|+1} \delta_i = \rho$ ,  $P = \bigcup_{i=1}^{|u|+1} Q_i$
2. for any transition  $(p_i, p_j)$  in  $\mathcal{P}$ , labelled with a letter  $x \in \{0, 1\}$  choose any pair of states  $q^i \in Q_i$  and  $q^j \in Q_j$ , and set  $\rho(q^i, x) = q^j$ ,
3. for all  $i \in \{1, \dots, |u| + 1\}$  and for every letter  $a \in \Sigma$ , if  $q^i \in Q_i$  and  $\delta(q^i, a)$  is undefined, then choose any  $j$  and any state  $q^j \in Q_j$  and set  $\rho(q^i, a) = q^j$ ,
4. for all  $i \in \{1, \dots, |u| + 1\}$  choose  $k_i \in \mathbb{N}$ . Choose  $k_i$  pairs  $(q_p^i, q_r^i)$  and a letter  $x \in \{0, 1\}$  and define  $\rho(q_p^i, x) = q_r^i$

Automaton  $\mathcal{B}$  is our ciphertext. It is straightforward from the construction, that computing such automaton is polynomial in terms of  $Q, \Sigma$  and length of the plaintext. We also state two obvious observations.

**Fact 2.** *After removing letters  $x \in \{0, 1\}$  from automaton  $\mathcal{B}$  we obtain a DFA over  $\Sigma$ .*

**Fact 3.** *After removing letters  $a \in \Sigma$  from automaton  $\mathcal{B}$  we obtain a digraph labelled with letters  $x \in \{0, 1\}$  with longest path between the vertices of length 1.*

Procedure of encrypting the word 01 is depicted on figures 3, 4, 5 and 6. As a public key we take the automaton depicted on Figure 2.