- $q \in A_i$
- $q \in S_m$ such that there exist $p \in C_i \cap S_m$ (notation from Lemma 4)

First two cases are straightforward. To prove the theorem for the third case observe that if $q \notin Q_i \cup A_i$, then $q \notin A_j$ and $q \notin Q_k$ for any $j, k \neq i$ otherwise $\mathcal{B}$ would be non-deterministic. So we deduce that $q \in S_m$ for some m. For the sake of contradiction suppose that $C_i \cap S_m = \varnothing$. But that means, that $q.a^m b \in B_j$ for $j \neq i$ and further $q.ab^m w' = q.w = q_l^j$ what is a contradiction. From these considerations we are able to determine for each i the sets A_i and Q_i that are subsets of the set Q_i'. In order to compute the sets C_i we first compute $S_1', .., S_n'$ inducing all a-clusters in $\mathcal{B}$ by removing $b, 0, 1$ transitions and determine all connected components of the resulting structure. Now we examine three cases for a cluster S_j':

- $S_j' \cap \bar{Q}_i = \varnothing$
- $S_j' \subseteq \bar{Q}_i$
- $S_j' \cap \bar{Q}_i \neq \varnothing$ and $S_j' \not\subset \bar{Q}_i$

Notice, that if the first case holds we know that no state of S_j' belongs to C_i. If the second case holds, we must check if $S_j' \subseteq Q_i \cup A_i$. If this is not true, then we have found a cluster $\mathcal{C}_m$, such that for all $q \in K_m$ it holds $\rho(q, b) \in B_i$ and we determined the a-cluster that belongs to C_i. In the third case we know that some of the states of the cluster S_j' are in C_i and some are not. To compute those that are let us take the center of the a-cluster S_j', say K_j', and observe that $q \in C_i$ if, and only if $q \in \{p \in K_j' : \rho(p, b) \in B_i\} = K_j''$ or q belongs to some branch with destination in K_j''. That concludes the proof. □

Using two former lemmas, decryption method is similar as in 4. Extended step is depicted on Figure 7. If we choose the public key to be the automaton on Figure 2, then notice, that in Lemma 4 we have $m = 2$, and $Q.a^2 b = \{2, 3, 7, 12, 13\}$.