5.1 Extended encryption

The extension consists of adding two stages between the 1 and 2 stage of encryption method, defining sets Q'_i and substitute them for Q_i in latter stages. Let us state two additional stages:

1. add l a-clusters with depth 1 to automaton obtained in stage 1 and define letters b for centers of those clusters to fulfill assumptions of lemma 4 in ρ function (defined in section 3)

2. for each copy $\mathcal{A}_i$ of public key in automaton obtained in previous stage add k_i states and define transitions as in lemma 3 and note the set of the added states in this stage as A_i for each $\mathcal{A}_i$

Now let us define sets Q'_i. For clusters $\mathcal{C}_1 = (S_1, \{a\}, \gamma_1), \ldots, \mathcal{C}_l = (S_l, \{a\}, \gamma_l)$ (from stage 1) with centers $K_1, \ldots, K_l$ respectively we define sets $C_1, \ldots, C_{|u|+1}$, such that if for $q \in K_i$ it holds $\rho(q, b) \in B_j$ (notation from lemma 4), then q and its branch belong to the set C_j. Then define $Q'_i = Q_i \cup A_i \cup C_i$. It is a simple exercise to prove that the sets $Q'_1, \ldots, Q'_{|u|+1}$ form a partition of $P = \bigcup_{i=1}^{|u|+1} Q_i \cup A_i \cup C_i$ which is the set of all states of our ciphertext. The latter stages remain as in section 3.

5.2 Extended decryption

Algorithm of deciphering is similar to the one described in section 4. We state lemmas being in a strict correspondence with those proven in section 4.

Lemma 5. *Let $\mathcal{B}$ be a ciphertext computed by extended encryption method using public key $\mathcal{A} = (Q, \Sigma, \delta)$ and $Q.w = q_l$. After removing letters $x \in \{0, 1\}$ from automaton $\mathcal{B}$ we have that $P.w = \{q_l^1, q_l^2, \ldots, q_l^{|u|+1}\}$.*

Proof. Observe that after stage 1 we can apply Lemma 4 and we obtain that $(\bigcup_{i=1}^{|u|+1} Q_i \cup C_i).w = \{q_l^1, q_l^2, .., q_l^{|u|+1}\}$. Notice that after stage 2 we can apply Lemma 3 to any copy of public key that was modified by that stage and also $P.w = \{q_l^1, q_l^2, .., q_l^{|u|+1}\}$. The rest of the proof is similar to the proof of Lemma 1. □

Lemma 6. *There exist an algorithm with polynomial time complexity (depending on $|P|$ and $|w|$) which computes a partition of P on sets Q'_1, Q'_2, ..., $Q'_{|u|+1}$.*

Proof. Using approach from the proof of Lemma 2 we can compute similar matrix, say M, in time $O(|P||w|)$. From Lemma 6 we know the last row contains only the states from the set $\{q_l^1, q_l^2, \ldots, q_l^{|u|+1}\}$ and we can compute sets $\bar{Q}_1, \ldots, \bar{Q}_{|u|+1}$ such if column of the first row containing q is the same as the column of the last row containing q_l^i, then $q \in \bar{Q}_i$. Notice that there are three cases, when $q \in \bar{Q}_i$:

- $q \in Q_i$