Lemma 3. *Let $\mathcal{A} = (Q, \Sigma, \delta)$ be a PFA with carefully synchronizing word w. Further, let $q \in Q$ be such that there exists $p \in Q$ such that $q \in p.a^{-1}$. Let also $\mathcal{A}' = (Q \cup \{q'\}, \Sigma, \delta')$ where δ' is defined as δ on Q and $\delta'(q', a) = q$. Then w carefully synchronizes $\mathcal{A}'$.*

Proof. Since a is defined for all states of Q', and $|\Sigma| = 2$, then the first letter of w must be a. Let w' be the word w without the first letter. Since $\delta'(q', a) = q$ and we assumed that there exist $p \in Q$ such that $q \in p.a^{-1}$ it is straightforward, that $Q'.a = Q.a$. Since we have not added any other transitions to $\mathcal{A}'$ and δ' is defined as δ on Q, we obtain that $Q'.aw' = Q.aw' = Q.w$ and that concludes the proof. □

For the next lemma we assume notation as in former part of the paper.

Lemma 4. *Let $\mathcal{B} = \bigcup_{i=1}^{k} \mathcal{A}_k$ and $m \in \mathbb{N}$ be the smallest integer such that $Q.a^m = Q.a^{m+1}$. Define $B_i = Q_i.a^m b$ and let $\mathcal{C}_1 = (S_1, \{a\}, \eta_1), \ldots, \mathcal{C}_l = (S_l, \{a\}, \eta_l)$ be a-clusters with depth 1 and centers $K_1, \ldots, K_l$ respectively. Let $\mathcal{B}' = \mathcal{B} \cup \bigcup_{i=1}^{l} \mathcal{C}_i = (P', \Sigma, \rho')$. If we define b transitions for all states $q \in \bigcup_{i=1}^{l} K_i$ such that there exists $0 < j < k + 1$ such that $\rho'(q, b) \in B_j$ then $P'.w = \{q_l^1, ..., q_l^k\}$.*

Proof. Since a is the only letter defined for all states in $\mathcal{A}$ and $Q.a^m = Q.a^{m+1}$ then w starts with a word $a^{m_1}b$ for $0 < m_1 < m+1$. Note $w = a^{m_1}bw'$ Observe that $Q.a^{i+1} \subseteq Q.a^i$ for all $i \geq 0$. From that we have, that $Q.a^m \subseteq Q.a^{m_1}$ and further for all copies of $\mathcal{A}$ in $\mathcal{B}'$ we obtain that $B_i \in Q_i.a^{m_1}.b$. Also, since the depth of any cluster $\mathcal{C}_i$ is 1, we have that $P_j.a^{m_1} = K_j$ for all $0 < j < m + 1$. Notice that $P' = \bigcup_{i=1}^{k} Q_i \cup \bigcup_{i=1}^{l} S_i$, so

$$P'.w = \bigcup_{i=1}^{k} Q_i.w \cup \bigcup_{i=1}^{l} S_i.w = \bigcup_{i=1}^{k} Q_i.a^{m_1}bw' \cup \bigcup_{i=1}^{l} S_i.a^{m_1}bw'$$

which gives

$$P'.w = \bigcup_{i=1}^{k} B_i w' \cup \bigcup_{i=1}^{l} K_i b w'.$$

But we know, that for all $q \in \bigcup_{i=1} K_i$ there exists $0 < i < k + 1$ such that $\delta'(q, b) \in B_i$. From that we obtain

$$P'.w = \bigcup_{i=1}^{k} B_i w',$$

and since each $B_i = Q_i.a^m b$ then $B_i.w' = Q_i.a^m bw' = Q_i.w = \{q_l^i\}$ and that concludes the proof. □

Using these two lemmas we can move on to the description of the extended method of encryption and decryption. In the next two subsections we follow the notation provided in sections 3 and 4.