Fact 1. Let \mathcal{A} be a PFA and $\mathcal{P}(\mathcal{A})$ be its power automaton. Then \mathcal{A} is carefully synchronizing if and only if for some state $q \in Q$ there exists a path in $\mathcal{P}(\mathcal{A})$ from Q to $\{q\}$. The shortest synchronizing word for \mathcal{A} corresponds to the shortest such path in $\mathcal{P}(\mathcal{A})$.

An example of a carefully synchronizing automaton \mathcal{A}_{car} is depicted in Fig. 2. One of its carefully synchronizing words is $aa(ba)^3bbab$.

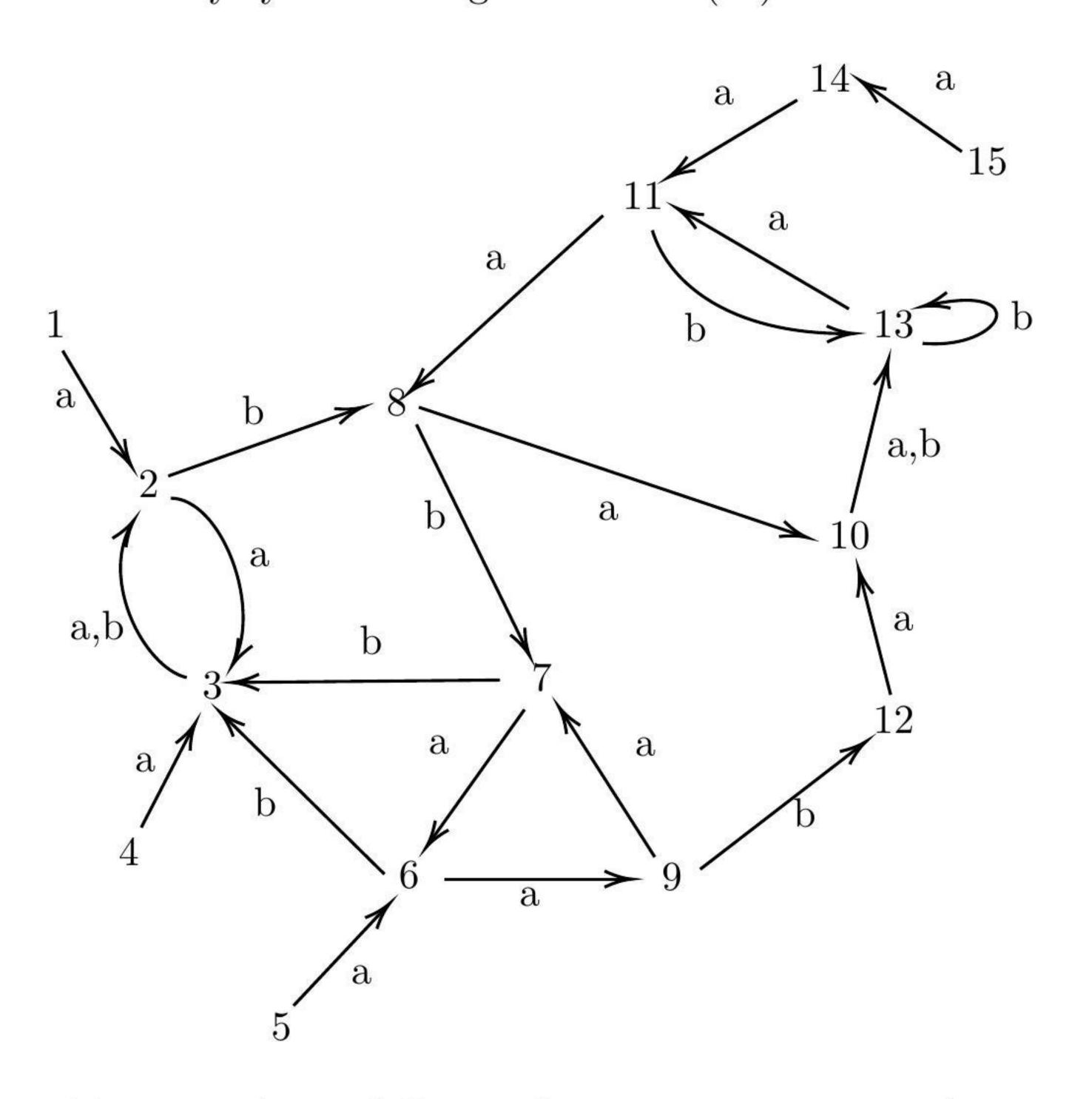


Figure 2: A carefully synchronizing automaton \mathcal{A}_{car} .

We recall the result of Vorel [26] about the complexity of deciding whether a PFA is carefully synchronizing.

Theorem 1. Given a PFA $\mathcal{A} = (Q, \Sigma, \delta)$, checking if \mathcal{A} is carefully synchronizing is PSPACE-complete even for $|\Sigma| = 2$.

Further we assume that $\Sigma = \{a, b\}$ and the letter a is defined for all the states wherever not mentioned otherwise. Having that we can go to the description of our method.

3 Basic encryption

Let a plain text be the word $u \in \{0,1\}^*$. Choose a public key to be a carefully synchronizing PFA $\mathcal{A} = (Q, \Sigma, \delta)$ and a private key to be any word w that carefully synchronizes \mathcal{A} . For simplicity of further statements we note $\mathcal{A}_i =$