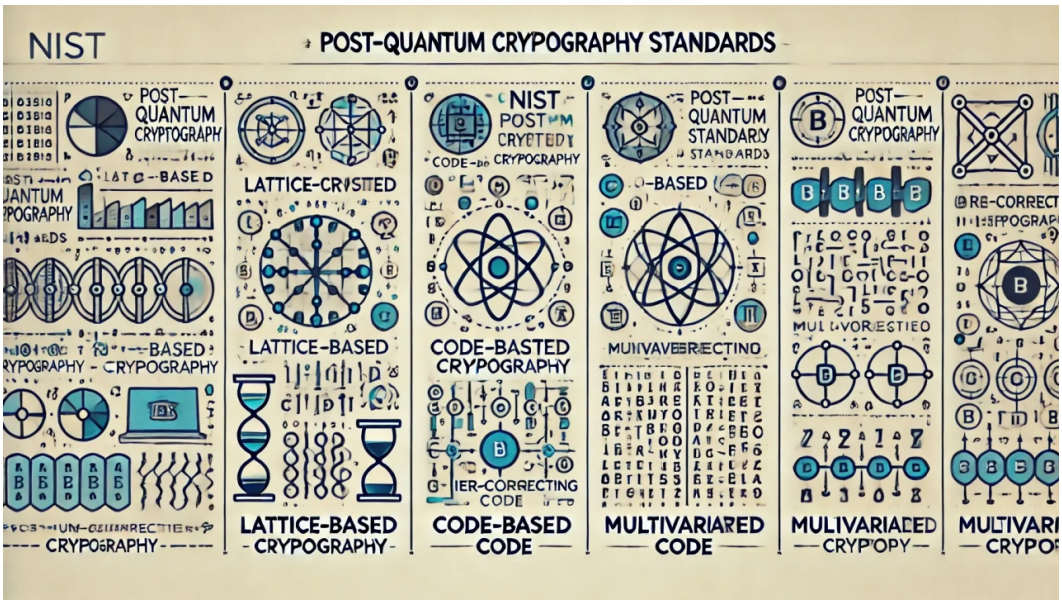
# Problem 9. «Post-quantum signature»

## Problem for a special prize!

Represent any of widely known (by your choice) post-quantum digital signature schemes as a Mealy finite-state machine with minimum resource consumption of its hardware implementation as well as adequate cryptographic strength. Describe the state diagram of the machine and substantiate your solution.




This nice picture is taken from
https://www.linkedin.com/pulse/understanding-nists-post-quantum-cryptography-shadab-hussain-wxt9e