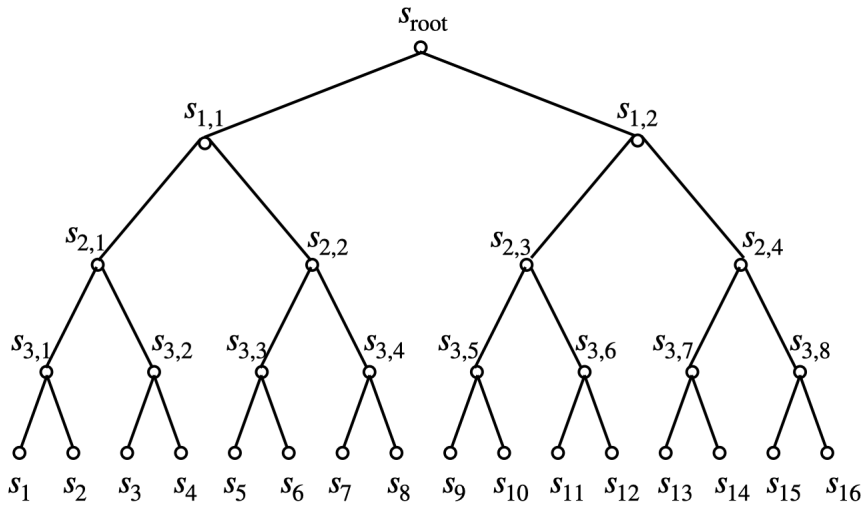
Selected Areas in Cryptology - Part 1: Post-quantum cryptography

Exercise sheet 5, 3 April 2024

1. Consider the MPCitH construction instantiated with the discrete log as an underlying hard problem, with N shares. Explain how a malicious prover can cheat with probability $\frac{1}{N}$.

2. In the following seed tree, what is the *authentication path* (the set of nodes that are sent to the verifier) when the challenge is $c = 5$?



3. **Bonus:** Consider an instance of the syndrome decoding problem over $\mathbb{F}_{13}$, where the length of the code is $n = 7$ and the solution is $\mathbf{x} = (0, 0, 1, 0, 7, 2, 0)$. We need to prove that the hamming weight of $\mathbf{x}$ is $t = 3$, without revealing $\mathbf{x}$. Using Lagrange interpolation, find the polynomial S. Then find the 'complement' polynomial Q, as well as F and P. Finally, check that $S \cdot Q - F \cdot P = 0$ when evaluated on some random inputs. **Hint:** If you get stuck on some step, look at the toy example on slide 18.