Question 3

Recall that the FORS scheme uses k Merkle trees $T_1, T_2, \ldots, T_k$ each with n leaf nodes. At signing m is hashed into $1 \leq h_1, h_2, \ldots, h_k \leq n$, and the signature are the authentication paths σ_j of h_j in tree T_j for $1 \leq j \leq k$.

Let $\mathcal{A}$ denote a EF-CMA adversary. Suppose that $\mathcal{A}$ makes N queries: $m_1, m_2, \ldots, m_N$, then the signing oracles will return the authentication paths for:

$$\begin{bmatrix} h_{1,1}, & h_{1,2}, & \ldots, & h_{1,N}, & \text{from } T_1 \\ h_{2,1}, & h_{2,2}, & \ldots, & h_{2,N}, & \text{from } T_2 \\ \ldots & & & & \\ h_{k,1}, & h_{k,2}, & \ldots, & h_{k,N}, & \text{from } T_k \end{bmatrix}$$

Let m^* be some randomly chosen message, and $h_1^*, h_2^*, \ldots, h_k^* = H(m)$. m^* is forgeable if the authentication paths in all k trees are forgeable. An authentication path in tree T_i is forgeable if any of $h_{i,1}, h_{i,2}, \ldots, h_{i,N}$ collides with h_i^*. Therefore:

$$\begin{aligned} P[T_i \text{ auth path forgeable}] &= 1 - P[T_i \text{ auth path unforgeable}] \\ &= 1 - P[h_{i,j} \neq h_i^* \text{ for all } 1 \leq j \leq N] \\ &= 1 - \prod_{j=1}^{N} P[h_{i,j} \neq h_i^*] \\ &= 1 - (1 - \frac{1}{n})^N \end{aligned}$$

Where $P[h_{i,j} \neq h_i^*] = 1 - \frac{1}{n}$ because each hash $H(m)$ must be in the range $1, 2, \ldots, n$, and we assume that hash function to be an ideal pseudorandom function.

Finally:

$$\begin{aligned} P[\text{FORS forgeable}] &= P[T_i \text{ authentication path forgeable for all } 1 \leq i \leq k] \\ &= \prod_{i=1}^{k} P[T_i \text{ auth path forgeable}] \\ &= (1 - (1 - \frac{1}{n})^N)^k \end{aligned}$$