Assignment 4

Q1 (10 points)

Someone decides that to enable themselves to sign more messages with a SPHINCS-like signature scheme, they will generate different random keys at each level, pseudorandomly based on the message. That is, to sign a message m, in Step 4(a) in SPHINCS from the notes, they compute instead

$$(\mathbf{PK}_{\ell,j}, \mathbf{SK}_{\ell,j}) = \mathsf{WOTS.KeyGen}(\mathsf{PRG}(s, \ell, j, m))$$

Explain why this is insecure.

Q2 (10 points)

Suppose you have a signature scheme (KeyGen, Sign, Verify) which can sign up to 3 messages with no loss of security, and it is just as fast and compact as WOTS. Describe how to make a SPHINCS-like signature scheme. Compare the efficiency of the new scheme to SPHINCS itself.

Q3 (10 points)

Show that if an adversary sees N messages signed with FORS (with k blocks of trees with n values in each tree), then they can efficiently forge a signature for a random message m with probability

$$\left(1 - \left(1 - \frac{1}{n}\right)^N\right)^k \tag{1}$$

Q4 (10 points)

Consider a Merkle tree where each node is the hash of 3 child nodes, and suppose we use these Merkle trees in SPHINCS. Describe an authentication path in this new type of Merkle tree. What is the length of a signature in the new scheme?

Q6 (10 points)

Show that for a linear code $C \subseteq \mathbb{F}_2^n$ and a fixed constant d, the following are equivalent:

(1) for any $c_1, c_2 \in C$, $|c_1 - c_2|_{Ham} \geq d$

(2) for any $c \in C$ with $c \neq 0$, $|c|_{Ham} \geq d$

(Don't forget: $\mathbb{F}_2^n$ is a vector space of n-bit strings, where addition and subtraction are done modulo 2, so both are equivalent to XOR)