1. PROBLEM AND OVERVIEW

Overview:
- Traditional signature schemes are not designed for uncertain settings with unpredictable resource constraints.
- Can one design a signature scheme that quantifies the validity of the signature based on a fraction of the number of computations performed during the verification?

Proposed Solution: Use Hash-based Digital Signature Schemes like Lamport-Diffie One-Time-Signature and Merkle Authentication Tree. The confidence level is determined by the number of computations passed during verification.

2. FLEXIBLE LAMPORT-DIFFIE SIGNATURE

Idea: Randomly verify different positions of the signature. The more the number of computations passed, the more confident one can be about the validity of the signature.

Security: Security of the scheme relies on the problem of finding an $\ell$-near-collision pair. Thus, for a smaller $\ell$ (e.g., more computations performed on the signature), more effort is required for attacker to forge the signature.

3. FLEXIBLE MERKLE SIGNATURE

Idea: Use Merkle authentication tree to convert one-time signature scheme to a many-time signature scheme.

New Signing and Verifying Algorithms:
- Require signer to send more authentication nodes.
- Verifier can verify authenticity of Public key on different levels of the tree. By doing this, the confidence for the authenticity of the one-time public key increases linearly.

4. EVALUATION

To evaluate both schemes, we constructed a Merkle signature scheme of height $h=20$ using SHA256, and compared the results for the number of computations $k = 32, 64, 128, 192, \text{max}$ where max is the number of computations needed for a complete verification.

Security Level:

Performance: