Lamport Signature Scheme

**Introduction**

Lamport Signature Scheme (aka Lamport One Time Signature) is a method for creating digital signatures, and typically involves cryptographic hash functions. Since this is a one-time scheme, Lamport can only securely sign one message.

**Method**

If Alice wants to digitally sign a message to Bob, here are the steps for doing so with a Lamport signature scheme:

1. Key Generation:

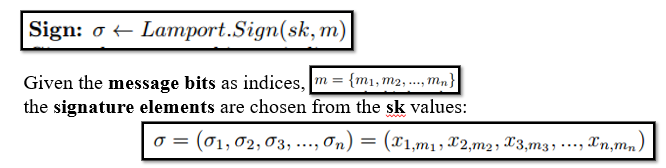
Alice creates the private keys (sk) using a secure random number generator to generate pairs of random numbers. She stores the keys securely. To create the public keys Alice hashes each private key to create the corresponding public key (pk).

A close-up of a math problem

Description automatically generated

1. Signature Generation:

Alice will hash her message (with a function such as SHA-256). Then, each bit in the corresponding message hash, will determine which row to select a private key (sk) from in that position to append. After a private key is selected for each corresponding position, the final product of concatenated private keys will be the signature. Alice sends the hashed message along with her signature to Bob.



1. Signature Verification

Bob hashes the message received from Alice. Then, each bit in the corresponding message hash, will determine which row to select on of Alice’s public keys (pk) from in that position to append. After a public key is selected for each corresponding position, the final product of concatenated public keys will be the verification sequence. Bob hashes the numbers in Alices signature to see if they match the public keys digest that he calculated earlier. If they match the message is verified. Otherwise, the message has been potentially tampered with.

A math equations on a white background

Description automatically generated

**Implementation**

Note: Alice has publicly published half of a private key as her signature. Her remaining private key cannot be used again and must be destroyed.

**References**

Lamport Signature Scheme on geeksforgeeks.org:

* [Lamport One Time Signature Scheme - GeeksforGeeks](https://www.geeksforgeeks.org/lamport-one-time-signature-scheme/) [Lamport One Time Signature Scheme - GeeksforGeeks](https://www.geeksforgeeks.org/lamport-one-time-signature-scheme/)