SPHINCS Interim Report

Daniel Kirkpatrick
Vedanth Narayanan
February 17, 2016

Introduction

Have a brief intro about Digital Signatures. Then talk about the relevance of SPHINCS. Important to make note of how SPHINCS integrates multiple technologies and wraps it all together. T

Details

List out the technologies, along with the different dependencies.
Afterwards talk about the ideas that are getting tested out, e.g Lamport+.

WOTS

Firstly, it's important to note that the Winternitz signature scheme is one-time. Any amount more and the security of the scheme cannot be promised. The primal idea behind the scheme is having an input run through a hash function several times. The number of iterations entirely depends on the message that needs to be signed.
WOTS was built on top of the Lamport signature scheme, and the expectation is for it to be intuitive in its logic, but it's not the case. The complexity of the scheme is heavily influences by the logic in figuring out the number of iterations necessary for a value to go through the hash function.
The scheme will be briefly be run through here so future references to the scheme are not ambiguous.
Key Pair Generation: A Winternitz parameter w ≥ 2 is chosen. The parameter signifies the number of bits that'll get processed at a time. The following

$$t_1 = \left\lceil \frac{n}{w} \right\rceil, t_2 = \left\lceil \frac{\lfloor log_2 t_1 \rfloor + 1 + w}{w} \right\rceil, t = t_1 + t_2 \tag{1}$$

Signature Generation:
Signature Verification:

WOTS+

Like one would expect, WOTS+ is very similar to WOTS, expect for

Lamport+ Signature Scheme

Lamport+ Signature Scheme is a new scheme that we are proposing. It not only brings the simplicity of the original Lamport scheme, but also pulls in elements of the WOTS+ scheme. Our hope is that the original scheme's security is withheld, if not enhanced. Please note that the security of the proposed scheme has not been proven, but it can very well be inferred from the previous.
Similar to how WOTS+ introduces XORing of randomized elements to WOTS, the same principle is introduced to Lamport. In the Key generation process,

Lamport+ Hash Chain

Explain how Lamport+ Hash Chain works. It's very, very similar to a normal Hash Chain.

Lamport+ Hash Tree

This piece is not fully developed, but explain how it is headed.

Benchmark

This section is for a little graph of RSA and ECDSA times.

Challenges

The single biggest challenge for us was primarily getting acquainted with the material. To properly, and throughly, understand SPHINCS we needed to get caught up with a lot of reading. There were multiple papers that required time and dedication to fully understand. Understanding the tools and technologies is crucial if we want to be successful. On top of this, we had the added challenge of figuring out how to piece together the technologies, and how SPHINCS uses them.

Conclusion

References