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.

Details

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

WOTS

Explain and go through the example.

WOTS+

Go through example here.

Lamport+

Lamport+ essentially is Lamport with pieces of WOTS+ integrated.

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.

Conclusion

References