Lab 1-2

Carl Benson

May 21, 2018

1 Lab 1

With $k = 8$, there is next to no slowdown for the connecting client. $k = 10$ took approximately a second to process. $k = 12$ ran for approximated 93 seconds before finding the solution. $k = 16$ took 244 seconds. After letting the client run for 30 minutes with $k = 20$ I quit the client without finding a solution.

A relatively small increase in k leads to an exponential increase in the time required for a client to solve the puzzle.

2 Lab 2

2.1 Main Idea

The main idea behind this algorithm is a verification with a smaller public key than HORS through the use of HORS with a Merkle Hash Tree.

2.2 Trade-Offs

Standard HORS has a larger public key and signature than this construction, however the computation time is shorter.

2.3 Execution Time Difference

2.4 SPHINCHS

Both this construction and SPHINCS utilize HORS with trees (HORST). By using HORST rather than HORS, the size of the public key and signature are reduced. [1]

References

[1] D. J. Bernstein, D. Hopwood, A. Hülsing, T. Lange, R. Niederhagen, L. Papachristodoulou, M. Schneider, P. Schwabe, and Z. Wilcox-O'Hearn,

“Sphincs: Practical stateless hash-based signatures,” *Advances in Cryptology – EUROCRYPT 2015 Lecture Notes in Computer Science*, p. 368–397, 2015.