Network Security Project
Draft Problem Statement and Proposed Solution

Nicholas Capo - Nicholas.Capo@Gmail.com

February 18, 2012

1 Problem Statement

According to and [2]: "Serpent was designed so that all operations can be executed in parallel, using 32 1-bit slices. This maximizes [the] parallelism [of the algorithm]". However, the context of these (and other) statements seem to imply that it would only be efficient to parallelize Serpent in hardware (or very close to hardware, e.g. Assembly). But the efficiency gains of a parallelized implementation in software are not addressed.

2 Proposed Solution

Construct a cipher-text compatible implementation of the Serpent Algorithm in both C and Python. Each implementation shall be capable of encryption and decryption using a single thread[1] as well as 32 parallel threads as described in [1]. These implementations can then be compared for speed and efficiency, in threaded and non-threaded modes, and the results analyzed to determine if there is any advantage to implementing parallelism in Serpent.

References

[1] Ross Anderson, Eli Biham, and Lars Knudsen. *Serpent: A proposal for the Advanced Encryption Standard*. [Online; accessed 18-February-2012]. URL: http://www.cl.cam.ac.uk/~rja14/Papers/serpent.pdf (cit. on p. 1).

[2] Wikipedia. *Serpent (cipher) — Wikipedia, The Free Encyclopedia*. [Online; accessed 18-February-2012]. 2012. URL: http://en.wikipedia.org/w/index.php?title=Serpent_(cipher)&oldid=469573199 (cit. on p. 1).

[1] `pThread` in the case of C, and the `multiprocessing` module in the case of Python (see the note at http://docs.python.org/library/threading.html for why `multiprocessing` was chosen over `threading`)