Network Security Project
Draft Literature Review

Nicholas Capo - Nicholas.Capo@Gmail.com

February 18, 2012

1 Draft Literature Review

1.1 Overview

"Serpent is a symmetric key block cipher which was a finalist in the Advanced Encryption Standard (AES) contest, where it came second to Rijndael. Serpent was designed by Ross Anderson, Eli Biham, and Lars Knudsen."[6]

1.2 Design Methodology

A significant portion of Serpent was based on the extensive cryptanalysis completed on the Data Encryption Standard (DES). [3] This allows the authors to design a a stronger cipher while still maintaining the known advantages of DES. The original submission to AES actually used the same S-Boxes as DES[3, p. 5], but later it was determined that suitably complex S-Boxes could be created using a deterministic method (thereby avoiding the potential for built-in trapdoors). [3, pp. 7, 15]

1.3 Parallelism

By using a bit-slice implementation, Serpent can be efficiently implemented on a "processor with two 32-bit integer ALUs (such as the popular Intel MMX series)".[3, p. 2] From Wikipedia: "Serpent was designed so that all operations can be executed in parallel, using 32 1-bit slices. This maximizes [the] parallelism [of the algorithm]"[6]

1.4 Conservative Approach

Using the cryptanalysis of DES as a basis the authors of Serpent took a conservative approach to the design of the algorithm.[6] Since it was expected (and we now know) that AES would be employed for many years after the competition, Serpent has been designed with an eye to the future. The authors believe that as few as 16 rounds of permutation-substitution would be secure for many years, however the design proposes 32 rounds as a precaution against feature advances in cryptanalysis. [3, pp. 4, 8]

1.5 Reference Implementations

During the AES selection process, several references implementations were developed in several languages: Specifically, Ada, Assembler, C, Java, and Python.[3, p. 16] Several of these implementations are available for download from the Serpent Homepage [1].

1.6 Patents and Licensing

The authors of Serpent have applied for a U.K. Patent (Application 9722798.9. Filed October 30, 1997) [2] but to quote the Serpent Homepage:

> Serpent is now completely in the public domain, and we impose no restrictions on its use. This was announced on the 21st August at the First AES Candidate Conference. The optimised implementations in the submission package are now under the General Public License (GPL), although some comments in the code still say otherwise.

[1]

References

[1] Ross J. Anderson. *Serpent Home Page*. [Online; accessed 26-January-2012]. URL: https://www.cl.cam.ac.uk/~rja14/serpent.html (cit. on p. 2).

[2] David Hopwood david.hopwood@zetnet.co.uk. *SCAN – Standard Cryptographic Algorithm Naming*. [Online; accessed 26-January-2012]. 2002. URL: http://www.users.zetnet.co.uk/hopwood/crypto/scan/cs.html#Serpent (cit. on p. 2).

[3] 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 pp. 1, 2).

[4] Ross Anderson, Eli Biham, and Lars Knudsen. *The Case for Serpent*. [Online; accessed 18-February-2012]. 2000. URL: http://www.cl.cam.ac.uk/~rja14/Papers/serpentcase.pdf.

[5] Frank Stajano. *Serpent reference implementation*. [Online; accessed 26-January-2012]. URL: https://www.cl.cam.ac.uk/~fms27/serpent/.

[6] 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).