The University of Texas at Austin

EXPLORATORY CANDIDATE ALGORITHM PERFORMANCE CHARACTERISTICS IN COMMERCIAL SYMMETRIC MULTIPROCESSING (SMP) ENVIRONMENTS FOR THE ADVANCED ENCRYPTION STANDARD (AES)

January 30, 1999

Primary Researcher Larry Leibrock, Ph.D.

(Corrected)

SUMMARY OF ONGOING RESEARCH: Evaluation techniques, performance metrics, and comparative algorithms should be investigated in the typical distributed server environments used in modern enterprise settings. The present baseline systems are single processor systems typically employed as client platforms. These single processor client systems may be insufficient in terms of scale, current computational efficiency, or commercial reliability to serve as an adequate baseline reference in many enterprise settings. This paper takes the position that SMP-based servers should be explored and perhaps considered in regeneration of the AES baseline, as many new Public Key Infrastructures (PKI) (directory-based) are being envisioned as server-centric, enterprise deployed systems.

Given this envisioned deployment, it is sensible to explore performance characteristics of the candidate algorithms in symmetric multiprocessor servers with typical commercial-off-the-shelf operating systems (Windows NT) and software development tools (Microsoft C). Candidate algorithms, in

standard ANSI C codes, have been obtained from NIST and recompiled using commercial off-the-shelf ANSI C – integrated development environments. The executable algorithms in the form of C programs are tested and timed both as single processor as well as multiple processor Windows NT ® servers using the commercially available Pentium III ® processors. Performance data derived from the NIST test-harness is compared to the timings of the present AES baseline single processor client systems,

VALUE OF RESEARCH: Computational efficiency of commercial SMP Servers. The evaluation of computational efficiency will be applicable to both hardware and software implementations. This work will provide more knowledge and perhaps a better baseline for analysis of prevailing commercial hardware implementations during Round 2 AES analysis. This research is believed to have relevance in the use of AES-based technology in public key infrastructures. A second value is crosscutting analysis among the AES candidate set.

CANDIDATE SET: All AES candidate algorithms meeting the minimum acceptability criteria have been announced by NIST. The candidate algorithms are derived from the NIST CDROM, which contains the ANSI C and Java™ referenced and optimized implementations. These are available for algorithm testing purposes. No hand-optimization or hand reordering to enhance parallelism will be part of this exploration. Algorithms implemented in Java™ and SMP systems performance will be the focus of successive research work as part of AES Round 2.

These AES algorithms, which meet minimum acceptable criteria, will be the candidate set. Exploratory test results and any recompiled codes will be made available electronically at the address listed below.

TIMING AND PROFILING PROGRAMS: The NIST timing harness and methods will be utilized and Intel processor execution profiles will be presented. Results and codes will be made available electronically at the address listed below.

PUBLICATION DATES: Final report will be on or before **March 10, 1999**. The required interval has been the requisite time necessary to install test and analyze the results derived from the systems test-bed.

PROPRIETARY RIGHTS: Since this research paper or any digest of the submitted paper will be made available to the public, it will not contain any

proprietary information. All NIST Copy rights have been sent (via facsimile) to NIST.

ADDRESS AND FURTHER INFORMATION CONTACT: Larry Leibrock Ph.D. The University of Texas at Austin, M/S B6003, Austin Texas 78712-1172 leibrock@mail.utexas.edu ; telephone 512-471-1650 or via fax at 512-232-1831. http://niim.bus.utexas.edu