Comb to Pipeline: Fast Software Encryption Revisited

AES-NI, or Advanced Encryption Standard New Instructions, is an extension of the x86 architecture proposed by Intel in 2008. With a pipelined implementation utilizing AES-NI, parallelizable modes such as AES-CTR become extremely efficient. However, out of the four non-trivial NIST-recommended encryption modes, three are inherently sequential: CBC, CFB, and OFB. This inhibits the advantage of using AES-NI significantly. Similar observations apply to CMAC, CCM and a great deal of other modes. We address this issue by proposing the comb scheduler – a fast scheduling algorithm based on an efficient look-ahead strategy, featuring a low overhead – with which sequential modes profit from the AES-NI pipeline in real-world settings by filling it with multiple, independent messages.

We apply the comb scheduler to implementations on Haswell, Intel’s latest microarchitecture, for a wide range of modes. We observe a drastic speed-up of factor 5 for NIST’s CBC, CFB, OFB and CMAC performing around 0.88 cpb. Surprisingly, contrary to the entire body of previous performance analysis, the throughput of the authenticated encryption (AE) mode CCM gets very close to that of GCM and OCB3, with about 1.64 cpb (vs. 1.63 cpb and 1.51 cpb, resp.), despite Haswell’s heavily improved binary field multiplication. This suggests CCM as an AE mode of choice as it is NIST-recommended, does not have any weak-key issues like GCM, and is royalty-free as opposed to OCB3. Among the CAESAR contestants, the comb scheduler significantly speeds up CLOC/SILC, JAMBU, and POET, with the mostly sequential nonce-misuse resistant design of POET, performing at 2.14 cpb, becoming faster than the well-parallelizable COPA.

Finally, this paper provides the first optimized AES-NI implementations for the novel AE modes OTR, CLOC/SILC, COBRA, POET, McOE-G, and Julius.

General information
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Cryptology
Contributors: Bogdanov, A., Lauridsen, M. M., Tischhauser, E. W.
Pages: 150-171
Publication date: 2015

Host publication information
Title of host publication: Revised Selected Papers of the 22nd International Workshop on Fast Software Encryption (FSE 2015)
Publisher: Springer
Editor: Leander, G.
ISBN (Print): 978-3-662-48115-8
(Lecture Notes in Computer Science, Vol. 9054).
Keywords: AES-NI, pclmulqdq, Haswell, Authenticated encryption, CAESAR, CBC, OFB, CFB, CMAC, CCM, GCM, OCB3, OTR, CLOC, COBRA, JAMBU, SILC, McOE-G, COPA, POET, Julius
DOIs: 10.1007/978-3-662-48116-5_8
Source: PublicationPreSubmission
Source ID: 117990600
Research output: Chapter in Book/Report/Conference proceeding › Article in proceedings – Annual report year: 2015 › Research › peer-review