```
88        C0 = SHA(C0,A0,X0);           C1 = SHA(C1,A1,X1);
89        A0 = SHA(A0,C0,Y0);           A1 = SHA(A1,C1,Y1);
90        i1 = i2;  i2 = i3;  i3 = i;
91      }
92    }
93    X0 = CVHI(A0,C0,0xB1);          X1 = CVHI(A1,C1,0xB1);
94    Y0 = CVLO(A0,C0,0xB1);          Y1 = CVLO(A1,C1,0xB1);
95    X0 = ADD(X0,LOAD(state0+0));  X1 = ADD(X1,LOAD(state1+0));
96    Y0 = ADD(Y0,LOAD(state0+1));  Y1 = ADD(Y1,LOAD(state1+1));
97    STORE(state0+0,X0);           STORE(state1+0,X1);
98    STORE(state0+1,Y0);           STORE(state1+1,Y1);
99  }
```

Listing 1: Implementation of the `Update` function using: 1) SSE vectors; 2) pipelined SHA-NI extensions.

REFERENCES

[1] Onur Aciicmez. 2005. *Fast hashing on Pentium SIMD architecture.* Master's thesis. Oregon State University. http://ir.library.oregonstate.edu/concern/graduate_thesis_or_dissertations/mk61rk723

[2] Elena Andreeva, Andrey Bogdanov, Atul Luykx, Bart Mennink, Elmar Tischhauser, and Kan Yasuda. 2013. Parallelizable and Authenticated Online Ciphers. In *Advances in Cryptology - ASIACRYPT 2013*, Kazue Sako and Palash Sarkar (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 424–443. https://doi.org/10.1007/978-3-642-42033-7_22

[3] ARM. 2017. *ARM Architecture Reference Manual. ARMv8, for ARMv8-A architecture profile.* ARM. https://static.docs.arm.com/ddi0487/ca/DDI0487C_a_armv8_arm.pdf

[4] Daniel J. Bernstein (Ed.). 2013. *CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness.* Cryptographic competitions. https://competitions.cr.yp.to/caesar-submissions.html

[5] Daniel J Bernstein, Daira Hopwood, Andreas Hülsing, Tanja Lange, Ruben Niederhagen, Louiza Papachristodoulou, Michael Schneider, Peter Schwabe, and Zooko Wilcox-O'Hearn. 2015. SPHINCS: practical stateless hash-based signatures. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, Berlin, Heidelberg, 368–397. https://doi.org/10.1007/978-3-662-46800-5_15

[6] Daniel J. Bernstein and Tanja Lange. 2017. eBACS: ECRYPT Benchmarking of Cryptographic Systems. (Dec. 2017). http://bench.cr.yp.to/supercop.html Published: Accessed on 20 December 2017.

[7] Andrey Bogdanov, Martin M. Lauridsen, and Elmar Tischhauser. 2015. Comb to Pipeline: Fast Software Encryption Revisited. In *Fast Software Encryption: 22nd International Workshop, FSE 2015, Istanbul, Turkey, March 8-11, 2015, Revised Selected Papers*, Gregor Leander (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 150–171. https://doi.org/10.1007/978-3-662-48116-5_8

[8] Johannes Buchmann, Erik Dahmen, and Andreas Hülsing. 2011. XMSS - A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions. In *Post-Quantum Cryptography*, Bo-Yin Yang (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 117–129. https://doi.org/10.1007/978-3-642-25405-5_8

[9] Ana Karina D. S. de Oliveira and Julio López. 2015. An Efficient Software Implementation of the Hash-Based Signature Scheme MSS and Its Variants. In *Progress in Cryptology – LATINCRYPT 2015*, Kristin Lauter and Francisco Rodríguez-Henríquez (Eds.). Springer International Publishing, Guadalajara, Mexico, 366–383. https://doi.org/10.1007/978-3-319-22174-8_20

[10] Armando Faz-Hernández and Julio López. 2015. Fast Implementation of Curve25519 Using AVX2. In *Progress in Cryptology – LATINCRYPT 2015 (Lecture Notes in Computer Science)*, Kristin Lauter and Francisco Rodríguez-Henríquez (Eds.), Vol. 9230. Springer International Publishing, Guadalajara, Mexico, 329–345. https://doi.org/10.1007/978-3-319-22174-8_18

[11] Agner Fog. 2017. *Instruction tables: Lists of instruction latencies, throughputs and micro-operation breakdowns for Intel, AMD and VIA CPUs.* Technical University of Denmark. http://www.agner.org/optimize/instruction_tables.pdf.

[12] Vinodh Gopal, Sean Gulley, Wajdi Feghali, Dan Zimmerman, and Ilya Albrekht. 2015. *Improving OpenSSL Performance.* Technical Report. Intel Corporation. https://software.intel.com/en-us/articles/improving-openssl-performance

[13] Vinodh Gopal, Jim Gullford, Wajdi Feghali, Erdinc Ozturk, Gil Wolrich, and Martin Dixon. 2010. *Processing Multiple Buffers in Parallel to Increase Performance on ® Intel Architecture Processors.* Technical Report 324101. Intel Corporation. https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/communications-ia-multi-buffer-paper.pdf

[14] Shay Gueron. 2009. Intel's New AES Instructions for Enhanced Performance and Security. In *Fast Software Encryption: 16th International Workshop, FSE 2009 Leuven, Belgium, February 22-25, 2009 Revised Selected Papers*, Orr Dunkelman (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 51–66. https://doi.org/10.1007/978-3-642-03317-9_4

[15] Shay Gueron. 2010. *Intel® Advanced Encryption Standard (AES) New Instructions Set.* Technical Report. Intel Corporation. http://www.intel.com/content/dam/doc/white-paper/advanced-encryption-standard-new-instructions-set-paper.pdf

[16] Shay Gueron and Michael Kounavis. 2010. Efficient implementation of the Galois Counter Mode using a carry-less multiplier and a fast reduction algorithm. *Inform. Process. Lett.* 110, 14 (2010), 549–553. https://doi.org/10.1016/j.ipl.2010.04.011

[17] Shay Gueron and Vlad Krasnov. 2012. Parallelizing message schedules to accelerate the computations of hash functions. *Journal of Cryptographic Engineering* 2, 4 (01 Nov 2012), 241–253. https://doi.org/10.1007/s13389-012-0037-z

[18] Shay Gueron and Vlad Krasnov. 2012. Simultaneous Hashing of Multiple Messages. *Journal of Information Security* 3, 4 (Oct. 2012), 319–325. https://doi.org/10.4236/jis.2012.34039

[19] S. Gueron and V. Krasnov. 2016. Accelerating Big Integer Arithmetic Using Intel IFMA Extensions. In *2016 IEEE 23nd Symposium on Computer Arithmetic (ARITH)*. IEEE, Santa Clara, CA, USA, 32–38. https://doi.org/10.1109/ARITH.2016.22

[20] Jim Guilford, Kirk Yap, and Vinodh Gopal. 2012. *Fast SHA-256 Implementations on Intel ® Architecture Processors.* Technical Report 327457-001. Intel Corporation. https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/sha-256-implementations-paper.pdf

[21] Sean Gulley, Vinodh Gopal, Kirk Yap, Wajdi Feghali, Jim Gullford, and Gil Wolrich. 2013. *Intel ® SHA Extensions New Instructions Supporting the Secure Hash Algorithm on Intel ® Architecture Processors.* Technical Report. Intel Corporation. https://software.intel.com/sites/default/files/article/402097/intel-sha-extensions-white-paper.pdf

[22] Andreas Hülsing. 2013. W-OTS+ – Shorter Signatures for Hash-Based Signature Schemes. In *Progress in Cryptology – AFRICACRYPT 2013*, Amr Youssef, Abderrahmane Nitaj, and Aboul Ella Hassanien (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 173–188. https://doi.org/10.1007/978-3-642-38553-7_10

[23] Andreas Hülsing, Denis Butin, Stefan-Lukas Gazdag, Joost Rijneveld, and Aziz Mohaisen. 2018. *XMSS: Extended Hash-Based Signatures.* Internet-Draft draft-irtf-cfrg-xmss-hash-based-signatures-12. Internet Engineering Task Force. https://datatracker.ietf.org/doc/draft-irtf-cfrg-xmss-hash-based-signatures Work in Progress.

[24] Andreas Hülsing, Lea Rausch, and Johannes Buchmann. 2013. Optimal Parameters for XMSS^{MT} . In *Security Engineering and Intelligence Informatics*, Alfredo Cuzzocrea, Christian Kittl, Dimitris E. Simos, Edgar Weippl, and Lida Xu (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 194–208. https://doi.org/10.1007/978-3-642-40588-4_14

[25] Intel Corporation. 2009. Define SSE2, SSE3 and SSE4. http://www.intel.com/support/processors/sb/CS-030123.htm. (Jan. 2009).

[26] Intel Corporation. 2011. Intel® Advanced Vector Extensions Programming Reference. https://software.intel.com/sites/default/files/m/f/7/c/36945. (June 2011).

[27] Intel Corporation. 2016. *Intel® Architecture Instruction Set Extensions Programming Reference.* Intel Corporation. https://software.intel.com/sites/default/files/managed/b4/3a/319433-024.pdf

[28] Jérémy Jean, Ivica Nikolić, and Thomas Peyrin. 2014. Tweaks and Keys for Block Ciphers: The TWEAKEY Framework. In *Advances in Cryptology – ASIACRYPT 2014: 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014, Proceedings, Part II*, Palash Sarkar and Tetsu Iwata (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 274–288. https://doi.org/10.1007/978-3-662-45608-8_15

[29] National Institute of Standards and Technology. 2001. *Advanced Encryption Standard (AES).* Technical Report FIPS PUB 197. NIST, Gaithersburg, MD, USA. https://doi.org/10.6028/NIST.FIPS.197

[30] National Institute of Standards and Technology. 2001. *Recommendation for Block Cipher Modes of Operation.* Technical Report NIST SP 800-38A. NIST, Gaithersburg, MD, USA. https://doi.org/10.6028/NIST.SP.800-38A

[31] National Institute of Standards and Technology. 2002. *Secure Hash Standard.* Technical Report FIPS PUB 180-2. NIST, Gaithersburg, MD, USA. https://doi.org/10.6028/NIST.FIPS.180-4

[32] National Institute of Standards and Technology. 2015. *FIPS PUB 202 SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions.* Technical Report. Gaithersburg, MD, USA. https://doi.org/10.6028/NIST.FIPS.202

[33] National Institute of Standards and Technology. 2016. *Post-Quantum Cryptography Standardization.* Technical Report. NIST, Gaithersburg, MD, USA. https://www.nist.gov/pqcrypto

[34] N. Stephens, S. Biles, M. Boettcher, J. Eapen, M. Eyole, G. Gabrielli, M. Horsnell, G. Magklis, A. Martinez, N. Premillieu, A. Reid, A. Rico, and P. Walker. 2017. The ARM Scalable Vector Extension. *IEEE Micro* 37, 2 (Mar 2017), 26–39. https://doi.org/10.1109/MM.2017.35

[35] Hongjun Wu and Bart Preneel. 2014. AEGIS: A Fast Authenticated Encryption Algorithm. In *Selected Areas in Cryptography – SAC 2013: 20th International Conference, Burnaby, BC, Canada, August 14-16, 2013, Revised Selected Papers*, Tanja Lange, Kristin Lauter, and Petr Lisoněk (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 185–201. https://doi.org/10.1007/978-3-662-43414-7_10