Universal Hash Designs for an Accordion Mode

Talk Abstract Submission to the NIST Workshop on Requirements for an Accordion Mode Cipher 2024

Jean Paul Degabriele[1], Jan Gilcher[2], Jérôme Govinden[3] and Kenneth G. Paterson[2]

[1] Technology Innovation Institute, Abu Dhabi, United Arab Emirates
[2] ETH Zurich, Zurich, Switzerland
[3] TU Darmstadt, Darmstadt, Germany

Variable-Length Strong Pseudorandom Permutations have been studied extensively by the cryptographic community for the past two decades, and several such constructions have been proposed. These constructions can be classified according to their structure and properties into four groups:

[2B1M] Constructions like CMC, EME, and AEZ where two layers of processing with a blockcipher are applied, sandwiched around one very efficient mixing layer [10]–[12]. In CMC and EME every block of data requires two blockcipher evaluations, whereas in AEZ this blockcipher processing is instantiated with four rounds of AES for better performance.

[2H1B] Constructions like XCB, HCTR, HCTR2, TET, TCT1 (a blockcipher instantiation of PIV), and HEH which process the input twice with a universal hash and once with a blockcipher [1], [4], [9], [14]–[16]. Although these constructions consist of three layers they can still be implemented in two passes over the input and typically offer better performance than the [2B1M] group.

[BBB] Constructions that achieve beyond-birthday-bound security. To the best of our knowledge, the only two known constructions in the literature are Tweakable HCTR and TCT2 (an instantiation of PIV using Cascaded LRW2) [7], [16].

[PBC] Constructions from Permutation Based Cryptography, such as Double decker, Docked Double decker, and Adiantum [3], [8].

We note, however, that NIST's proposal for requirements for an Accordion mode [2] states that the mode should be based on a blockcipher which rules out the last category [PBC]. Furthermore, the constructions in the third category achieve beyond birthday bound security either if instantiated with a 'from scratch' tweakable blockcipher such as Deoxys-TBC or SKINNY, which is also out of scope, or tweakable blockcipher instantiations using Cascaded LRW2 [13] requiring two blockcipher evaluations per tweakable blockcipher evaluation, which degrades performance. As such, for higher security, it might be more viable to instantiate a birthday-bound-security construction with a 256-bit blockcipher rather than use a construction from group [BBB]. This leaves categories [2B1M] and [2H1B], where constructions in [2H1B] are likely to offer better performance than those in [2B1M], with the exception of AEZ. However AEZ relies on significantly stronger assumptions on AES and cannot readily be replaced with another blockcipher. As such, it is questionable whether AEZ can be considered a mode of operation.

Our focus here is on the group [2H1B] where both the security and performance of the constructions rely crucially on the availability of a suitable universal hash function. Different constructions impose different security requirements on the universal hash function, but they can almost always be realised from some variation of a polynomial hash function. The two most popular polynomial hash functions in use today are GHASH (along with its close sibling POLYVAL) and Poly1305. Motivated by the fact that the multiuser security of ChaCha-Poly1305 is strongly dominated by the security of Poly1305 [6], in recent work we reconsidered the design of Poly1305 [5]. In particular we studied the landscape of possible design choices and optimisations to explore the different tradeoffs between performance and security for polynomial hash functions over prime fields. As a result we identified new designs that significantly outperform Poly1305 in offering either better security without degrading performance or better performance without degrading security. In the case of an Accordion mode construction from group [2H1B], a good choice of a universal hash function is at least *twice* as important when compared to AEAD schemes like GCM or ChaCha-Poly1305. In particular, a good choice of hash function should offer a good tradeoff between the following desiderata:

- Exploit superscalar CPU architectures wherein the hash function is evaluated in parallel with the blockcipher by running on different processing units of the CPU. This is the case, for instance, with GHASH/POLYVAL and AES when using the AES-NI and PCLMULQDQ instructions.
- Offer good performance on a variety of hardware platforms, even ones without specialised instruction sets.
- Achieve its top performance as quickly as possible. Typical benchmarks for AEAD schemes often quote their asymptotic performance which might be reached at message lengths well above 16 kBytes—the maximum TLS packet size. Thus the actual performance in an Internet application may be quite far off from the quoted benchmark, see Figure 1. In the case of an Accordion mode used for disk encryption, this aspect is even more critical since typical disk sector sizes are in the range between 512 Bytes and 4 KBytes.
- Offer an adequate security bound that matches the security of the construction, i.e., the security of the Accordion mode should not be dominated (heavily) by the security of the hash function. Otherwise the choice of hash function would be limiting the Accordion mode from reaching its full security potential.
- Not be significantly harder to implement in software than existing universal hash designs that are deployed in practice.

In this Talk We will present our view on the requirements of universal hash functions for an Accordion mode cipher. We will then report on our universal hash constructions from [5] and how they can be integrated in Accordion mode constructions. We will conclude with other new universal hash designs that we are currently exploring in follow-up work.

References

[1] D. Chakraborty and M. Nandi, "An improved security bound for HCTR," in *FSE 2008*, K. Nyberg, Ed., ser. LNCS, vol. 5086, Springer, Heidelberg, Feb. 2008, pp. 289–302. DOI: 10.1007/978-3-540-71039-4_18.

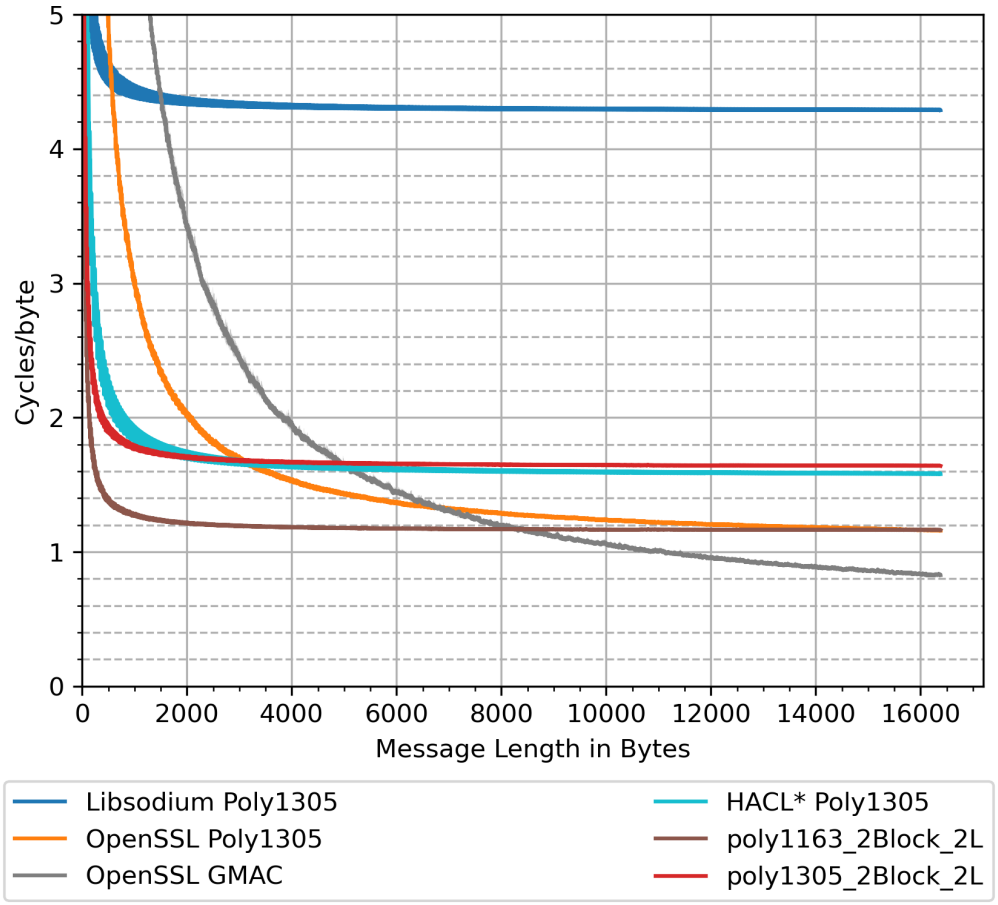

Figure 1: Performance comparison of (non-vectorised) Poly1163 [5] and various Poly1305 (vectorised and non-vectorised) implementations on an arm processor.

[2] Y. L. Chen, M. Davidson, M. Dworkin, J. Kang, J. Kelsey, Y. Sasaki, M. S. Turan, D. Chang, N. Mouha, M. Largo, *et al.*, "Proposal of requirements for an accordion mode," 2024.

[3] P. Crowley and E. Biggers, "Adiantum: Length-preserving encryption for entry-level processors," *IACR Trans. Symm. Cryptol.*, vol. 2018, no. 4, pp. 39–61, 2018, ISSN: 2519-173X. DOI: 10.13154/tosc.v2018.i4.39-61.

[4] P. Crowley, N. Huckleberry, and E. Biggers, *Length-preserving encryption with HCTR2*, Cryptology ePrint Archive, Report 2021/1441, https://eprint.iacr.org/2021/1441, 2021.

[5] J. Degabriele, J. Gilcher, J. Govinden, and K. G. Paterson, "SoK: Efficient design and implementation of polynomial hash functions over prime fields," in *2024 IEEE Symposium on Security and Privacy (SP)*, Los Alamitos, CA, USA: IEEE Computer Society, May 2024, pp. 131–131. DOI: 10.1109/SP54263.2024.00132. [Online]. Available: https://doi.ieeecomputersociety.org/10.1109/SP54263.2024.00132.

[6] J. P. Degabriele, J. Govinden, F. Günther, and K. G. Paterson, "The security of ChaCha20-Poly1305 in the multi-user setting," in *ACM CCS 2021*, G. Vigna and E. Shi, Eds., ACM Press, Nov. 2021, pp. 1981–2003. DOI: 10.1145/3460120.3484814.

[7] A. Dutta and M. Nandi, "Tweakable HCTR: A BBB secure tweakable enciphering scheme," in *INDOCRYPT 2018*, D. Chakraborty and T. Iwata, Eds., ser. LNCS, vol. 11356, Springer, Heidelberg, Dec. 2018, pp. 47–69. DOI: 10.1007/978-3-030-05378-9_3.

[8] A. Gunsing, J. Daemen, and B. Mennink, *Deck-based wide block cipher modes and an exposition of the blinded keyed hashing model*, Cryptology ePrint Archive, Report 2022/247, https://eprint.iacr.org/2022/247, 2022.

[9] S. Halevi, "Invertible universal hashing and the TET encryption mode," in *CRYPTO 2007*, A. Menezes, Ed., ser. LNCS, vol. 4622, Springer, Heidelberg, Aug. 2007, pp. 412–429. DOI: 10.1007/978-3-540-74143-5_23.

[10] S. Halevi and P. Rogaway, "A tweakable enciphering mode," in *CRYPTO 2003*, D. Boneh, Ed., ser. LNCS, vol. 2729, Springer, Heidelberg, Aug. 2003, pp. 482–499. DOI: 10.1007/978-3-540-45146-4_28.

[11] S. Halevi and P. Rogaway, "A parallelizable enciphering mode," in *CT-RSA 2004*, T. Okamoto, Ed., ser. LNCS, vol. 2964, Springer, Heidelberg, Feb. 2004, pp. 292–304. DOI: 10.1007/978-3-540-24660-2_23.

[12] V. T. Hoang, T. Krovetz, and P. Rogaway, "Robust authenticated-encryption AEZ and the problem that it solves," in *EUROCRYPT 2015, Part I*, E. Oswald and M. Fischlin, Eds., ser. LNCS, vol. 9056, Springer, Heidelberg, Apr. 2015, pp. 15–44. DOI: 10.1007/978-3-662-46800-5_2.

[13] W. Landecker, T. Shrimpton, and R. S. Terashima, "Tweakable blockciphers with beyond birthday-bound security," in *CRYPTO 2012*, R. Safavi-Naini and R. Canetti, Eds., ser. LNCS, vol. 7417, Springer, Heidelberg, Aug. 2012, pp. 14–30. DOI: 10.1007/978-3-642-32009-5_2.

[14] D. A. McGrew and S. R. Fluhrer, "The security of the extended codebook (XCB) mode of operation," in *SAC 2007*, C. M. Adams, A. Miri, and M. J. Wiener, Eds., ser. LNCS, vol. 4876, Springer, Heidelberg, Aug. 2007, pp. 311–327. DOI: 10.1007/978-3-540-77360-3_20.

[15] P. Sarkar, *Efficient tweakable enciphering schemes from (block-wise) universal hash functions*, Cryptology ePrint Archive, Report 2008/004, https://eprint.iacr.org/2008/004, 2008.

[16] T. Shrimpton and R. S. Terashima, "A modular framework for building variable-input-length tweakable ciphers," in *ASIACRYPT 2013, Part I*, K. Sako and P. Sarkar, Eds., ser. LNCS, vol. 8269, Springer, Heidelberg, Dec. 2013, pp. 405–423. DOI: 10.1007/978-3-642-42033-7_21.