Security of Encryption Modes and an Exposition of Proof Techniques

Bart Mennink

Radboud University, Nijmegen, The Netherlands
b.mennink@cs.ru.nl

Abstract. An important building block in cryptography is the AES block cipher [DR20]. It is a function that, on input of a secret key K, bijectively transforms 128-bit input blocks to 128-bit output blocks. Such a block cipher can be put in a *mode of operation* to be able to perform data encryption, data authentication, authenticated encryption, and many more. Security of such modes is typically reduced to the security of the underlying building block. Depending on the mode that is being investigated, such proofs range from simple to very complex, and also the proof techniques vary greatly.

In this talk, I will elaborate on how security of encryption modes is typically argued. I will start with the simplest example, namely counter mode. This mode evaluates the underlying block cipher on input of a nonce N (unique for each message) concatenated with a counter and uses the resulting 128-bit output blocks as keystream. Then, I will extend the ideas to modes that are more complex but achieve higher security, such as CENC [Iwa06], and explain what complications surface when proving security of such modes. This discussion, among others, may include a high-level exposition of the H-coefficient technique [Pat08,CS14] and the mirror theory [Pat05,MN17,CDN+23].

If time permits, I extend the discussion to a new concept in encryption world, called accordion modes [CDD+24].

References

CDD+24. Yu Long Chen, Michael Davidson, Morris Dworkin, Jinkeon Kang, John Kelsey, Yu Sasaki, Meltem Sönmez Turan, Donghoon Chang, Nicky Mouha, and Alyssa Thompson. Proposal of Requirements for an Accordion Mode: Discussion Draft for the NIST Accordion Mode Workshop 2024. https://csrc.nist.gov/pubs/other/2024/04/10/proposal-of-requirements-for-an-accordion-mode-dis/iprd, 2024.

CDN+23. Benoît Cogliati, Avijit Dutta, Mridul Nandi, Jacques Patarin, and Abishanka Saha. Proof of Mirror Theory for a Wide Range of $\xi_{\max}$. In Carmit Hazay and Martijn Stam, editors, *Advances in Cryptology - EUROCRYPT 2023 - 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part IV*, volume 14007 of *Lecture Notes in Computer Science*, pages 470–501. Springer, 2023.

CS14. Shan Chen and John P. Steinberger. Tight Security Bounds for Key-Alternating Ciphers. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*, volume 8441 of *Lecture Notes in Computer Science*, pages 327–350. Springer, 2014.

DR20. Joan Daemen and Vincent Rijmen. *The Design of Rijndael - The Advanced Encryption Standard (AES), Second Edition.* Information Security and Cryptography. Springer, 2020.

Iwa06. Tetsu Iwata. New Blockcipher Modes of Operation with Beyond the Birthday Bound Security. In Matthew J. B. Robshaw, editor, *Fast Software Encryption, 13th International Workshop, FSE 2006, Graz, Austria, March 15-17, 2006, Revised Selected Papers*, volume 4047 of *Lecture Notes in Computer Science*, pages 310–327. Springer, 2006.

MN17. Bart Mennink and Samuel Neves. Encrypted Davies-Meyer and Its Dual: Towards Optimal Security Using Mirror Theory. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part III*, volume 10403 of *Lecture Notes in Computer Science*, pages 556–583. Springer, 2017.

Pat05. Jacques Patarin. On Linear Systems of Equations with Distinct Variables and Small Block Size. In Dongho Won and Seungjoo Kim, editors, *Information Security and Cryptology - ICISC 2005, 8th International Conference, Seoul, Korea, December 1-2, 2005, Revised Selected Papers*, volume 3935 of *Lecture Notes in Computer Science*, pages 299–321. Springer, 2005.

Pat08. Jacques Patarin. The "Coefficients H" Technique. In Roberto Maria Avanzi, Liam Keliher, and Francesco Sica, editors, *Selected Areas in Cryptography, 15th International Workshop, SAC 2008, Sackville, New Brunswick, Canada, August 14-15, Revised Selected Papers*, volume 5381 of *Lecture Notes in Computer Science*, pages 328–345. Springer, 2008.