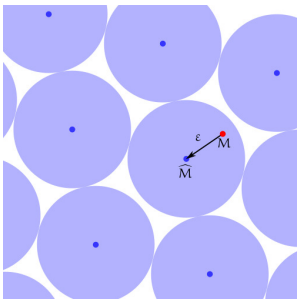
Understanding Recent Structural Attacks on the McEliece Cryptosystem



Recent research has introduced new structural and algebraic cryptanalytic techniques against the McEliece cryptosystem, including improved distinguishers and heuristic key-recovery methods [1, 2, 3]. Recent work has also analyzed the concrete cost of such key-recovery approaches against Classic McEliece [4]. These results differ substantially in their assumptions, objectives, complexity, and practical relevance. In particular, distinguishing a public code, recovering an equivalent secret key, and practically breaking Classic McEliece are distinct objectives.

This thesis will systematically compare recent structural attacks on McEliece, considering their assumptions, recovered information, theoretical and concrete complexity, experimental evidence, and applicability to practical parameters. One selected attack will be studied in greater depth, focusing on the connection between distinguishing a public code and recovering a valid or equivalent secret key. A focused experimental component will reproduce or test part of the selected attack on reduced parameter sets. The objective is to clarify what has been formally established, what remains heuristic, and what recent cryptanalytic developments imply for the security of Classic McEliece.

Practicalities

Promotor:	Prof. Bart Preneel		
Daily supervisor:	Kevin Bogner	kevin.bogner@esat.kuleuven.be	office B01.20
	Varesh Mishra	varesh.mishra@esat.kuleuven.be	office B01.23
Nature of the work:	40% literature, 40% theoretical work, 20% software		
Number of students:	1		

[1] H. Randriambololona, "The Syzygy Distinguisher," Cryptology ePrint Archive, Paper 2024/1193, 2024. https://eprint.iacr.org/2024/1193

[2] A. Ghoshal, Y. Ishai, A. Jain, and N. Sun, "Quasipolynomial Cryptanalysis of the McEliece Cryptosystem (or: PIR Meets McEliece)," Cryptology ePrint Archive, Paper 2026/1630, 2026. https://eprint.iacr.org/2026/1630

[3] T. Hemmert, "Key Recovery for the McEliece Cryptosystem Using Higher-Order Vanishing," Cryptology ePrint Archive, Paper 2026/1339, 2026. https://eprint.iacr.org/2026/1339

[4] M.-J. O. Saarinen, "Bit Operation Cost of 'Holdout' Key-Recovery Attacks Against Classic McEliece," Cryptology ePrint Archive, Paper 2026/1786, 2026. https://eprint.iacr.org/2026/1786

Image: Fabrice Mouhartem, "Error Correcting Code Balls." CC BY-SA 4.0.

 © 2026 – 2027 COSIC