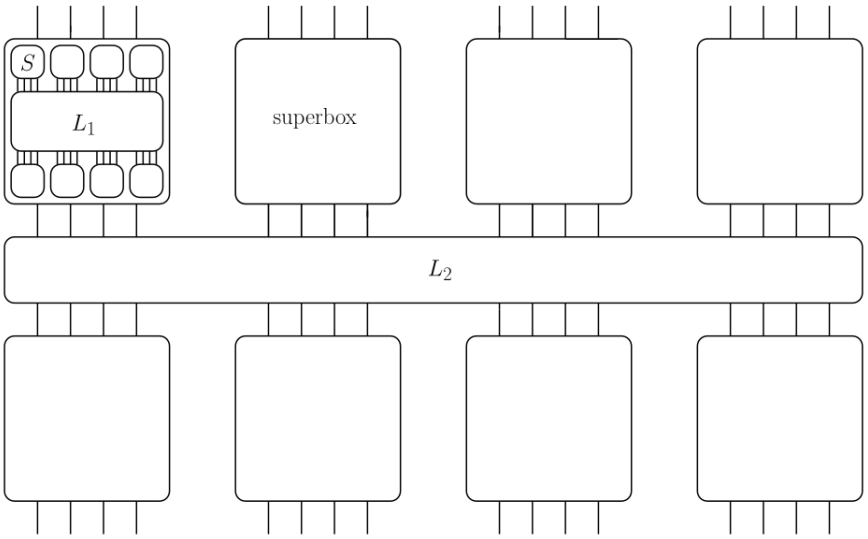
Pairwise independence of the AES



The Advanced Encryption Standard (AES) is one of the most influential block ciphers in modern cryptography. One of the attractive features of the AES is that the arguments for its (conjectured) security are relatively transparent. Although proving the security of AES-like ciphers against general attacks is not feasible with current techniques, recent work has led to security arguments against an important class of attacks. In this internship, you will improve these arguments using computational methods.

More specifically, recent work [1] has established *ε-pairwise independence* for AES-like constructions. Here, the parameter ε quantifies security against a certain class of attacks. If the AES is secure against these attacks, then we expect that $\varepsilon \leq 2^{-128}$. However, the current upper bound on ε is 2^{54-40r} for $4r$ iterations of the AES round function. The standard number of iterations is 10, but this upper bound only drops below 2^{-128} for more than 20 iterations.

The bound on ε is derived from the singular values of a large matrix of size $2^{32} \times 2^{32}$ that is related to a part of the AES (the 'superbox'). Your task in this internship project will be to exploit the structure of this matrix to compute its singular values numerically.

Applicants interested in this project should have some familiarity with numerical linear algebra.

[1] T. Beyne, G. Leander, I. Schütt. *Pairwise independence of AES-like block ciphers.* EUROCRYPT 2026. `https://eprint.iacr.org/2025/1495`.

Practicalities

Supervisors: Tim Beyne tim.beyne@esat.kuleuven.be office B01.03

 © 2025-2026 COSIC