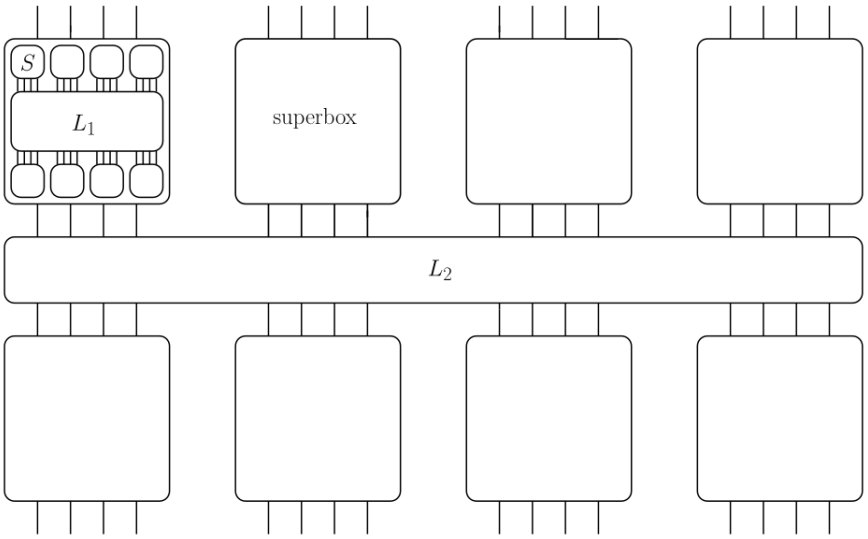
Paarsgewijze onafhankelijkheid van AES



De *Advanced Encryption Standard* (AES) is een van de meest invloedrijke blokcijfers in de moderne cryptografie. Een van de aantrekkelijke eigenschappen van AES is dat argumenten voor de (veronderstelde) veiligheid ervan relatief transparant zijn. Hoewel het met de huidige technieken niet haalbaar is om de veiligheid van AES-achtige cijfers tegen algemene aanvallen te bewijzen, is recent werk er wel in geslaagd om veiligheidsargument tegen een belangrijke klasse van aanvallen te geven. In deze stage zal je deze argumenten verbeteren met computationele methodes.

Meer specifiek heeft recent werk [1] *ε-paarsgewijze onafhankelijkheid* aangetoond voor AES-achtige constructies. Hierbij kwantificeert de parameter ε de veiligheid tegen een bepaalde klasse van aanvallen. Als AES tegen deze aanvallen veilig is, dan verwachten we dat $\varepsilon \leq 2^{-128}$. De huidige bovengrens voor ε is echter 2^{54-40r} voor $4r$ iteraties van de AES-rondefunctie. Het standaard aantal iteraties is 10, maar pas bij meer dan 20 iteraties ligt deze bovengrens onder 2^{-128}.

De bovengrens op ε is afgeleid uit de singuliere waarden van een grote matrix van grootte $2^{32} \times 2^{32}$ die verband houdt met een deel van AES (de 'superbox'). Jouw taak in dit stageproject bestaat erin de structuur van deze matrix uit te buiten om die singuliere waarden numeriek te berekenen.

Kandidaten die geïnteresseerd zijn in dit project hebben bij voorkeur enige vertrouwdheid met numerieke lineaire algebra.

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

Praktische informatie

Begeleiding Tim Beyne tim.beyne@esat.kuleuven.be kantoor B01.03

 © 2025-2026 COSIC