CONJURA · OPEN PROBLEM

192-Round AES Is 2^{-128}-Close to Pairwise Independent

Proved for AES with most mixing layers removed; conjectured for AES itself

Status. Statement: AI-written from Anastasiya Pelecanos, Stefano Tessaro and Vinod Vaikuntanathan, *Layout Graphs, Random Walks and the t-wise Independence of SPN Block Ciphers*, IACR ePrint 2024/083. Not yet checked by a human. Their Theorem 7 proves the bound for "192-round censored AES" — real AES S-boxes, real AES mixing layer, but a subset of the mixing layers removed. The source conjectures the same round count suffices for AES itself, and calls proving it "an outstanding open problem." The best proved bound for actual AES is Liu, Tessaro and Vaikuntanathan's, which needs more than 9000 rounds.

Category. *Symmetric-Key Cryptography.*

Conjecture (informal). *Pairwise independence is a security property strong enough to rule out differential and linear cryptanalysis, and weak enough that one can hope to prove it for a real cipher with its real S-box, rather than for an idealized model. For AES the question is how many rounds are needed before the cipher is within 2^{-128} of pairwise independent. The source gets to* 192 *rounds — but only after* removing *most of the mixing layers, which is what lets it substitute repeated S-box applications for a random S-box. Nobody expects removing mixing layers to help a cipher. The conjecture says so:* 192 *rounds of real AES should do at least as well.*

1 The setting

A substitution-permutation network with word length b, width k and r rounds alternates three steps: XOR the round key into the state; apply an invertible S-box $S : \mathbb{F} \to \mathbb{F}$, where $\mathbb{F} = \mathbb{F}_{2^b}$, to each of the k blocks in parallel; apply an invertible linear mixing layer $M : \mathbb{F}^k \to \mathbb{F}^k$. AES is the case $k = 16$, $b = 8$, with the patched inverse S-box composed with an $\mathbb{F}_2$-affine map, and the mixing layer

given by ShiftRows followed by MixColumns.

Two idealizations are usually needed to say anything provable, and the source removes one of them. Analyses in the "large S-box" model treat the S-box as random or as a public random permutation, which is unrealistic when $b = 8$. The source instead proves results for random, independent S-boxes (calling the resulting cipher AES*) and then converts them to results about the *concrete* AES S-box by replacing one random S-box with several sequential applications of the real one, each preceded by a fresh key XOR. That substitution is what costs the mixing layers: the resulting cipher is AES with a subset of mixing layers removed, which the source calls *censored AES*. The other idealization, independent round keys, is retained here and throughout the line.

Where this leaves the numbers:

- AES* — random independent S-boxes, real AES mixing — is 2^{-128}-close to pairwise independent after 7 rounds (the source's Theorem 6), and $2^{-23.42}$-close after 3 (its Theorem 5).
- 192-round censored AES is 2^{-128}-close to pairwise independent (its Theorem 7).
- For real AES, the best proved bound is Liu, Tessaro and Vaikuntanathan's, that $6r$-round AES is $2^{r-1}(0.472)^r$-close to pairwise independence, which reaches 2^{-128} only past 9000 rounds.

2 Notation and parameters

- $b = 8$ is the S-box input length, $k = 16$ the width, so the block is 128 bits.
- Round keys are independent and uniform, as throughout this line; Remark 4 says why that matters.
- *ε-close to pairwise independent* means the joint distribution of the cipher's outputs on any two distinct inputs is within statistical distance ε of the corresponding distribution for a uniformly random permutation.
- *Censored AES* on r rounds means an $(r-1)$-round SPN (thus r layers of S-boxes), independent keys, the true AES S-box (patched inverse composed with an affine map) and the AES mixing layer, but with a subset of the mixing layers removed;

which ones remain is determined by the source's proof.

3 The conjecture

Theorem 1 (What is proved, [PTV24, Theorem 7]). 192-*round censored AES is* 2^{-128}*-close to pairwise independent.*

Conjecture 1 (Censoring never helps, [PTV24, §1]). 192-*round AES is* 2^{-128}*-close to pairwise independent.*

Remark 1 (How the source states it, and its reason). Page 7: "We give a censored variant of AES which is 2^{-128}-close to pairwise independent after 192 rounds. We conjecture that 192-round of AES itself is also 2^{-128}-close to pairwise independent, i.e., the censoring mixing layers never increases security." And on page 29, the rationale: "If one believes that the mixing layers are useful for AES to achieve pseudorandomness, then it is natural to expect that removing a large fraction of them should only hurt the convergence to pairwise independence." The source then records: "We view proving this conjecture formally to be an outstanding open problem."

Remark 2 (The conjecture is a monotonicity claim, not a new bound). What is being asserted is not that some argument gives 192 rounds for AES, but that adding back the removed mixing layers cannot make the cipher converge more slowly. That is intuitive and, as far as the source says, unproved even in weak forms. The clean sub-question is whether inserting a single invertible linear layer into an SPN can ever *increase* the distance from pairwise independence; a proof of that in the generality needed would give the conjecture, and a counterexample — even an artificial one, for some mixing layer and some round count — would show the intuition cannot be used as stated.

Remark 3 (Why 192 and not 7). The gap between Theorem 6 (7 rounds for AES*) and Theorem 1 (192 rounds for censored AES) is entirely the price of replacing a random S-box by real ones. The source computes that an 8-fold sequential composition of the AES S-box with independent key bytes is $2^{-29.39}$-close to pairwise independent, so simulating four random S-box layers costs $16 \cdot 4$ times that; a 32-round partial censored AES is then ε-close

for $\varepsilon < 2^{-22.39}$, and amplification with $r = 6$ repetitions gives $2^5 \cdot (2^{-22.39})^6 < 2^{-128}$ over 192 rounds. A resolution of Conjecture 1 that also brought the round count near 7 would be a substantially stronger result, and should be reported as such.

Remark 4 (Independent round keys is an assumption, not a detail). Every result in this line assumes independent round keys, a modelling choice rooted in Lai, Massey and Murphy's Markov ciphers and adopted by Nyberg. Real AES derives its round keys from a key schedule. The expectation in the field is that t-wise independence becomes t-wise pseudorandomness under an appropriate key schedule, and Liu, Tessaro and Vaikuntanathan record that "understanding the precise role of key schedules is an important open problem." A resolution of Conjecture 1 says nothing about AES-128 as deployed.

Remark 5 (What pairwise independence does and does not rule out). Sufficiently strong almost-pairwise independence suffices to resist truncated differential attacks and linear cryptanalysis, which is why it is the target. It is not a proof of pseudorandomness, and the same line names algebraic attacks as a separate class it does not address. Also worth keeping in mind: a differential-probability bound of 2^{-127} for a 128-bit block does not rule out a distinguisher, so the closeness parameter has to be pushed to 2^{-128} for the statement to mean what it appears to mean — which is why the conjecture names that number.

4 Bibliography

[PTV24] Anastasiya Pelecanos, Stefano Tessaro and Vinod Vaikuntanathan. *Layout graphs, random walks and the t-wise independence of SPN block ciphers.* IACR ePrint 2024/083. The source. The conjecture is stated on page 7 and repeated with its rationale on page 29; Theorems 5 and 6 are on page 28 and Theorem 7 on pages 28–29. Source code for the computations is linked from Section 6.

[LTV21] Tianren Liu, Stefano Tessaro and Vinod Vaikuntanathan. *The t-wise independence of substitution-permutation networks.* CRYPTO 2021 (IACR ePrint 2021/507). The prior bound for actual AES — Theorem 3.14 there, $6r$-round AES is $2^{r-1}(0.472)^r$-close to pairwise independence — and the source of the key-schedule remark. Also the source of the companion Conjura statement on t-wise independence for $t > 2$.

[LMM91] Xuejia Lai, James L. Massey and Sean Murphy. *Markov ciphers and differential cryptanalysis.* EUROCRYPT 1991. The origin of the independent-round-keys model this line works in.

[KNR09] Eyal Kaplan, Moni Naor and Omer Reingold. *Derandomized constructions of k-wise (almost) independent permutations.* Algorithmica, 2009. One of the two amplification results the source uses to turn a constant closeness into 2^{-128} by sequential composition. [UNVERIFIED] — cited in the source as [KNR09a]; the bibliographic detail here is inferred, not read off the source's reference list.

[BV05] Thomas Baignères and Serge Vaudenay. *Proving the security of AES substitution-permutation network.* Selected Areas in Cryptography 2005. Describes the random walk on layouts for the special case of AES* and $t = 2$, which the source notes is related to but not sufficient for its results.