CONJURA · OPEN PROBLEM

t-Wise Independence of AES for $t > 2$

Pairwise is done; the next level has no proof and one cautionary counterexample nearby

Status. Statement: AI-written from Tianren Liu, Stefano Tessaro and Vinod Vaikuntanathan, *The t-wise Independence of Substitution-Permutation Networks*, IACR ePrint 2021/507. Not yet checked by a human. The source names this as the first of "the two outstanding open problems that come of this work." It proves almost pairwise independence ($t = 2$) for multi-round AES with independent round keys, and proves an existential t-wise result for key-alternating ciphers with *most* permutations — but nothing for concrete AES beyond $t = 2$. Its own Appendix B gives an attack on 4-wise independence in the width-1 case with the patched-inverse S-box, which is why the round count is the crux.

Category. *Symmetric-Key Cryptography.*

Conjecture (informal). *A family of permutations is t-wise independent if its behaviour on any t distinct inputs is indistinguishable from a random permutation's. For $t = 2$ this already rules out differential and linear cryptanalysis, and the source proves it for real AES with real S-boxes. Higher t rules out more attacks and is the natural next target, and the source names it as an outstanding open problem. There is a warning attached: in the degenerate width-1 case, with the same patched-inverse S-box AES uses, 4-wise independence provably* fails *for a modest number of rounds, by an interpolation attack. So the question is not whether AES gets there, but after how many rounds — and no technique currently reaches any finite answer for $t \geq 3$.*

1 The setting

The programme is to prove, for concrete block-cipher designs with their actual S-boxes rather than idealized ones, that specific well-studied classes of attacks cannot succeed. Almost t-wise independence is the chosen target because, in the source's words, "Sufficiently strong (almost) pairwise independence already suffices to

resist (truncated) differential attacks and linear cryptanalysis, and hence this is a relevant and meaningful target."

What the source establishes splits along a line worth keeping straight.

Concrete, $t = 2$. It proves almost pairwise independence of multi-round SPNs instantiated with concrete S-boxes and a suitable linear mixing layer, and adapts the argument to the actual AES round structure and parameters ($k = 16$, $b = 8$), obtaining that 6 AES rounds with independent sub-keys are ε-close to pairwise independent for some $\varepsilon < 1/2$, hence (Theorem 3.14) that $6r$-round AES is $2^{r-1}(0.472)^r$-close to pairwise independence. Its own assessment: "The bound is likely far from tight, as we expect much better, but non-trivial further work seems required to obtain a substantial improvement."

Existential, general t. Separately, it shows by the probabilistic method that there *exist* permutations instantiating a $(t+1)$-round key-alternating cipher that is almost t-wise independent — in $t + o(t)$ rounds. Those permutations can then be fixed, but they are not AES's S-box, and the result says nothing about any named cipher.

The gap between the two is the statement below.

2 Notation and parameters

- An SPN with word length b, width k and r rounds alternates: XOR the round key; apply an S-box $S : \mathbb{F}_{2^b} \to \mathbb{F}_{2^b}$ to each of the k blocks in parallel; apply an invertible linear mixing layer. A *key-alternating cipher* (KAC) is the special case $k = 1$, where the mixing step can be dropped.
- AES is $k = 16$, $b = 8$, block size 128; S-box the patched inverse $x \mapsto x^{2^b-2}$ composed with an invertible $\mathbb{F}_2$-affine map; mixing layer ShiftRows then MixColumns.
- Round keys are *independent* and uniform. This is an assumption of the whole line; see Remark 4.
- A permutation family is *ε-close to t-wise independent* if its output distribution on any t distinct inputs is within statistical distance ε of a uniformly random permutation's.

3 The conjecture

Conjecture 1 (t-wise independence of AES, $t > 2$, [LTV21, §1.2]). *For every $t > 2$ and every $\varepsilon > 0$ there is a round count $r = r(t, \varepsilon)$ such that r-round AES with independent round keys is ε-close to t-wise independent.*

Remark 1 (How the source states it, and what is being supplied here). Page 7: "the two outstanding open problems that come of this work are (a) to prove t-wise independence of multi-round AES with independent round keys, for $t > 2$; and (b) to formalize and prove security against algebraic attacks." Item (a) is this statement; item (b) is not, and is a programme rather than a proposition.

The source names the goal without fixing t, ε or a target round count, so the quantifier structure in Conjecture 1 — for every t and ε, some finite r — is this statement's choice, and the weakest reading with content. A resolution should report the dependence $r(t, \varepsilon)$ it achieves; a bound polynomial in t and $\log(1/\varepsilon)$ would be far more useful than a merely finite one, and should be stated as such.

Remark 2 (The nearby counterexample, and why it does not settle this). The source's Appendix B is titled "Attack against 4-wise Independence" and shows that for a modest number of rounds $r \ll 2^n$, the key-alternating cipher with permutation $x \mapsto x^{2^n-2}$ — the same patched inverse, but at width 1 over the whole n-bit block — is *not* 4-wise independent. The attack is essentially the interpolation attack of Jakobsen and Knudsen: the output can be written as a rational function of the input with numerator and denominator linear in x.

Two things follow. First, this is not a refutation of Conjecture 1: AES has width 16 with 8-bit S-boxes and a mixing layer, and the source cites Carlitz for the fact that with $2^{\Omega(n)}$ rounds the same KAC *would* be indistinguishable from a random permutation — so the width-1 obstruction is about round count, not about impossibility. Second, it is a real constraint on the shape of any proof: an argument for $t \geq 4$ cannot be insensitive to width and mixing, since the width-1 specialization of the claim is false at modest r. That is a sharper obstruction than one usually gets for an unproved statement, and it

is the reason to be careful with any purported proof that never uses k or M.

Remark 3 (Where $t = 3$ sits). The source's problem is stated for $t > 2$, and the counterexample above is for $t = 4$. Nothing quoted here rules out $t = 3$ being materially easier than general t, and it is the natural first target: it is the smallest case not covered by the pairwise machinery, and it is below the level at which the interpolation attack is known to bite. A resolution for $t = 3$ alone would be genuine progress on this statement and should be reported as a partial result rather than as the whole.

Remark 4 (Independent round keys is load-bearing). The assumption is explicit in the source's problem statement — "with independent round keys" — and is not a technicality: real AES derives round keys from a key schedule. The line's working expectation is that t-wise independence becomes t-wise pseudorandomness under an appropriate key schedule, and the source records that "understanding the precise role of key schedules is an important open problem." So a resolution of Conjecture 1 would not be a statement about AES-128 as deployed.

Remark 5 (Neighbouring questions in the same discussion). The source also asks for a tighter tradeoff between the number of rounds and the statistical distance, and for a direct bound on the differential probability without going through statistical distance. It notes that a 2^{-127} bound on expected differential probability for a 128-bit block does not rule out a distinguisher, which is why closeness parameters in this area have to be pushed to 2^{-128}. None of these is this statement. The companion Conjura statement on 192-round AES concerns $t = 2$ and a concrete round count, and is also not this one.

4 Bibliography

[LTV21] Tianren Liu, Stefano Tessaro and Vinod Vaikuntanathan. *The t-wise independence of substitution-permutation networks.* CRYPTO 2021 (IACR ePrint 2021/507). The source. The two open problems are named on page 7; the AES pairwise bound is Theorem 3.14 on page 31; the existential KAC result is Section 4 and the attack against 4-wise independence is Appendix B, page 46.

[JK97] Thomas Jakobsen and Lars R. Knudsen. *The interpolation attack on block ciphers.* Fast Software Encryption 1997. The attack the source's Appendix B adapts. [UNVERIFIED] — cited in the source as [JK97] under the description "algebraic attacks"; the bibliographic detail here is inferred.

[Car53] Leonard Carlitz. *Permutations in a finite field.* Proceedings of the American Mathematical Society, 1953. Cited by the source for the fact that with $2^{\Omega(n)}$ rounds the key-alternating cipher with the patched inverse would be indistinguishable from a truly random permutation.

[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. Improves the pairwise ($t = 2$) picture substantially and conjectures a concrete round count for AES; the source of the companion Conjura statement. Does not address $t > 2$ for concrete AES.

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