参赛学生姓名：田岳洲

中学：陕西省西安中学

省份：陕西省

国家/地区：中国

指导老师姓名：高洁、吴琼

指导老师单位：陕西省西安中学、

西安工业大学

论文题目：AM-SEV：可验证密码设计的度量理论、 AI 引擎与 Tempest v4 实例

2026 J-1 Yau High School Science Award
仅用于2026丘成桐中学科学奖论文公示

AM-SEV：可验证密码设计的度量理论、AI 引擎与 Tempest v4 实例

田岳洲

摘要—密码学伪随机数生成器支撑密钥生成与随机掩码等安全机制，其可验证设计需要在部署前核查结构条件及实现一致性。对于 AND–XOR–旋转（AND-RX）候选，端口与执行顺序的改变会使旧度量失配，如何保持数学对象、程序语义和证据范围一致是本文研究的问题。本文提出 AM-SEV“结构分析—修复—复核”方法，以可逆更新替换旧算法中合并输入的操作，用秘密子密钥驱动 32 轮顺序计算构建 Tempest v4-R1：16 位缩小模型的 65536 种输入在 9 种轮数下均产生不同输出；C 与独立 Python 实现的 125000 字节输出逐字节一致；八通道字节接口实测吞吐量为 2.646 Gbit/s，核实了结构修复、实现对应与运行效率。这些结果为原创 AND-RX 设计的缺陷定位、版本修订和独立复核提供依据，完整原语的密码学安全性仍待进一步分析。

关键词—结构密码分析；二次布尔映射；极化秩；可复现验证；证据分级；AI 辅助设计。

I. 引言

A. 研究背景与问题价值

从网络通信、软件防护到科学计算，随机数都参与系统的关键决策。不同用途对随机性的要求并不相同：仿真关注统计分布与可重复性，密码系统还要求攻击者难以从已知输出预测未知输出或恢复秘密。伪随机数生成器（PRNG）用确定性程序将短种子扩展成长流；用于密码用途时，种子质量、核心结构和调用规则共同决定其能否满足预期安全条件。因此，研究生成器不能只比较速度与有限样本的统计表现，还需要检查支撑构造的假设是否在具体程序中成立。

实际事故体现了不同层次的风险。Debian OpenSSL（CVE-2008-0166）的错误补丁削弱了熵混入，使受影响 PRNG 主要依赖进程号；常见 PID 配置下，每架构仅有 32767 条候选流[1]。2010 年 PS3 ECDSA 漏洞因复用秘密签名随机数而允许恢复签名私钥[2]；这与本文 CTR 接口所要求的公开 nonce 同密钥唯一，是不同的使用约束。Dual_EC_DRBG 则说明，公开参数也可能隐藏选参者掌握的陷门关系；NIST 于 2015 年正式移除了该生成器[3]。这些事件提示，需要分别检查代码依赖、接口前提和参数来源。本文未对上述漏洞运行检测，也不以常量可复算替代无后门证明。

本文将问题收窄到 AND–XOR–旋转（AND-RX）设计。它以按位 AND 提供非线性，以 XOR 和循环旋转连接字与比特，便于把轮函数写成明确的有限布尔程序。对于这类程序，某些局部性质可以精确求解；但端口、赋值顺序或输出接口一旦改变，原来的结论可能不再对应实际实现。本文研究的具体问题是：**怎样把一个 AND-RX 候选的程序对象、结构查询、缺陷反例与修复证据连接起来，使设计修改后的每条结论仍能独立复核？**这既能发现不满足构造要求的实现，也能避免把局部性质误读为完整密码安全性。

B. 相关研究

已有研究为这一问题提供了不同层次的工具。BBS 与 RSA 类生成器展示了在明确困难性假设下建立伪随机性的路线 [11], [12]；AES-CTR 与 ChaCha20 则是基于已有密码原语的常见生成方式 [3]。这类工作说明了构造级论证的重要性。另一方面，xoshiro 与 PCG 侧重快速生成及统计质量 [1], [2]；它们的状态更新和输出变换须分别分析，不能将统计质量直接等同于计算不可预测性。

在结构分析方面，二次映射的仿射导数、布尔函数的 Walsh 谱以及 SIMON 类轮函数的精确差分与线性表达式，为局部秩计算提供了基础 [15], [16]。SAND、Ascon 等设计表明 AND、XOR 和旋转可以用于构造密

[1]Debian DSA-1571-1：https://www.debian.org/security/2008/dsa-1571；候选流范围：https://wiki.debian.org/SSLkeys。

[2]fail0verflow，*Console Hacking 2010: PS3 Epic Fail*，27C3：https://media.ccc.de/v/27c3-4087-en-console_hacking_2010。

[3]陷门机制：https://projectbullrun.org/dual-ec/back-door.html；NIST 2015 年修订公告：https://www.nist.gov/news-events/news/2015/06/nist-revises-key-computer-security-publication-random-number-generation。

2026 Yau High School Science Award 仅用于2026年决赛科学论文公示

码原语 [13], [14]。多轮分析则需要进一步处理组件之间的传播与依赖；宽轨迹方法以及 MILP/SAT 搜索分别提供了相应的论证与建模手段 [4]–[6]。

自动化工具已将多个分析环节连接起来。CLAASP 以组件图描述原语，并支持代码生成、约束模型、代数分析、统计和神经区分器等功能 [7]；Gohr 的工作展示了学习型区分器在减轮密码分析中的用途 [9]。TestU01 等统计工具从输出样本检查特定偏差 [8]。本文以这些方法为基础，关注它们在本实例的版本修订过程中如何形成可重建的论证链，不将设计时分析、自动搜索或统计检验本身列为首创。

C. 问题与挑战

上述理论与工具并不会自动解决一个持续修改的原创候选的全部安全问题。对本项目，需要直接处理以下三个难点。

第一，精确查询与完整安全之间存在范围差异。二次映射在固定差分或固定输出掩码下可用秩给出精确结果，但这不等于完成全局最优化；实际顺序级联还可能提高次数，使二次公式失去适用前提。高次数、低样本相关或未见碰撞也不能独立转化为攻击复杂度下界。

第二，数学对象与执行语义必须对应。快照读取与顺序读取可以产生不同函数；相同目标字的多次写入可能保留、累加或覆盖前一步贡献。端口调整后，旧矩阵、证书或小模型结果不能仅通过修改版本名而沿用。

第三，不同证据不能相互替代。局部证明、缩小模型穷举、全宽抽样、输出统计与实现测量回答不同问题。分组核心与字节接口的区别，以及失败、超时和筛选记录，都需要随结果保留。本文要补齐的是这些环节在本实例中的对应关系，而非声称现有平台普遍缺少相关能力；与既有工具的等预算效率比较仍未完成。

D. 本文方法与主要贡献

针对上述问题，本文提出 AM-SEV 度量与核查框架，以程序版本、计算对象、输入分布、字宽轮数、查询范围和证据等级共同标识一条结论。局部度量用于定位结构问题，反例决定修复对象，再由独立计算或实现检查复核修复。候选可以来自人工、进化算子或语言模型，提案来源不改变核查条件。Tempest v4-R1 是这一方法的研究实例；v3 保留为缺陷与修复的对照。

本文的主要贡献如下。

1) **限定对象的局部推导。**以经典二次导数和 Walsh 公式为基础，证明完整四字交互图在 $W = 2^m$ 时极化满秩（命题 III.1），给出非二次幂字宽反例，并修正 v4 影子的单字读字秩重叠公式。固定查询的精确值与全局搜索、次数上界与实际达界分别记录。
2) **由反例驱动的结构修复。**从 v3 的非单射字内映射、公开调度退化和依赖覆盖出发，给出 v4-R1 的目标排除顺序剪切、秘密子密钥、32 轮分组置换及完整逆算法，并给出保留未知 PRP 优势项的条件性输出界。置换性修复了相应构造缺陷，不被解释为完整 128 位安全证明。
3) **分层且保留负面结果的核查。**分别对当前分组核心 E_K 和 R1-P4 字节接口 $P \circ E_K$ 报告完整 16 位模型计数、指定掩码谱、全宽抽样、源码一致性、统计电池以及软件和硬件成本。BigCrush 标记、零活动见证及求解超时等与正面结果一并保留，避免跨对象或跨版本合并结论。
4) **候选生成与性质验证分开的引擎。**实现 L1 筛查、L2 指定查询、证书复核及拒绝原因记录，以 v3.1 的真实依赖覆盖错误作为回归控制。现有结果支持这一核查流程的实例化，不宣称已经完成独立候选集上的搜索优势比较。

AM-SEV 的目标是使局部数学结果、程序修复和复核材料相互对应；原创原语的完整密码安全性仍需独立分析。图 1给出方法与实例总览。第二至四节介绍背景、度量和引擎，第五至六节定义并分析 v4，第七至八节报告工程与实验，第九节讨论结果与边界。

a) 代码与复现材料: 项目 GitHub 仓库为https://github.com/paim-creater/prng。随稿源码、常量、证书及实验记录以 v4-R1 标识分组版本、以 R1-P4 标识字节流配置，与历史 v3 工件分别保存。项目的 `tempest-rng` 条目已被 *awesome-cryptography-rust* 的 PRNG 栏目收录[4]；此处只说明软件目录收录事实，不表示经过独立密码安全评估。

II. 背景与威胁模型

A. PRNG 框架与安全游戏

采用三元组 $(\mathcal{S}, \Phi, \varphi)$ 表示发生器：状态空间、状态转移、输出函数；第 t 次输出为 $x_t = \varphi(\Phi^t(s_0))$ [1]。当前 v4 采用四个 64 位字的带密钥分组置换 E_K；公开

[4]收录页面：https://github.com/rust-cc/awesome-cryptography-rust。

2026 5th International Conference on Computer Science and Artificial Intelligence 录用于2026国际计算机科学与人工智能大会

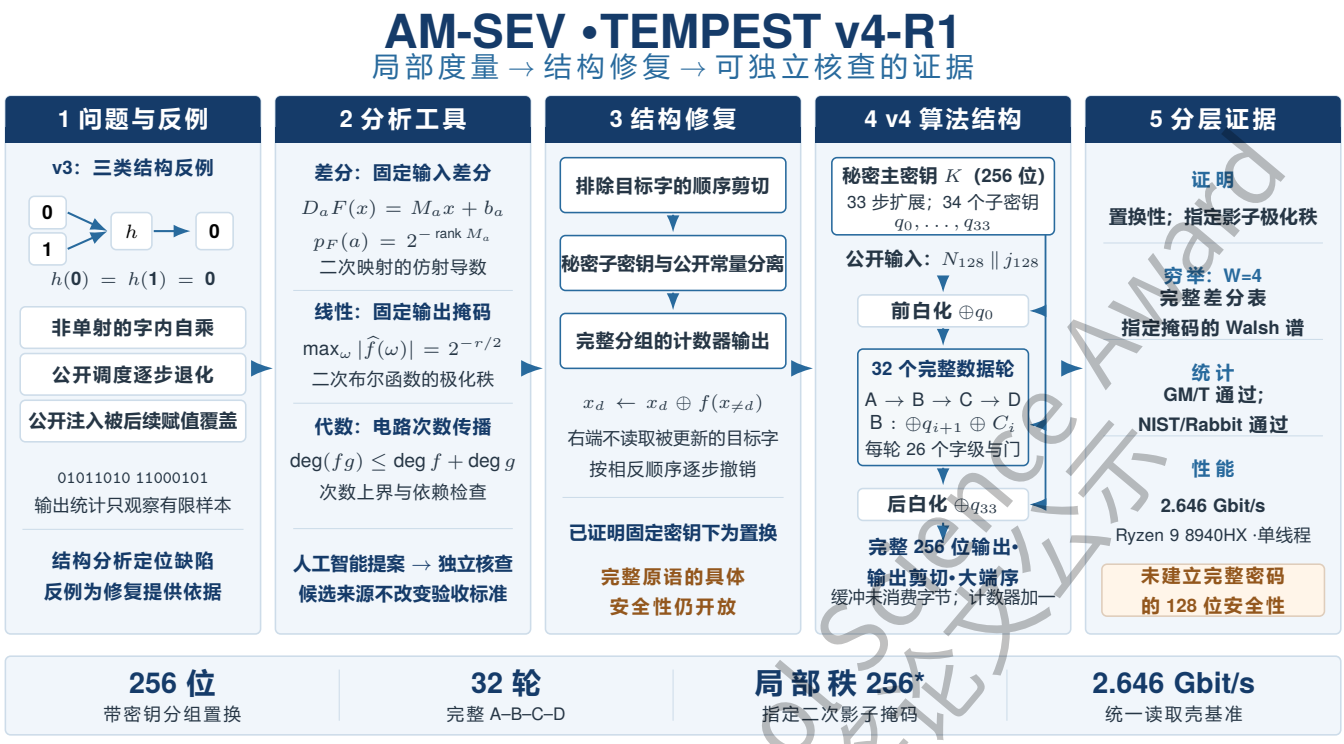


图 1. AM-SEV 的分析、修复与核查流程及 v4-R1 实例。第二栏仅对相应二次对象成立：a 为非零输入差分，M_a 为仿射导数的线性部分，$p_F(a) = \max_b \mathrm{DP}_F(a,b)$；$r$ 为二次布尔函数 f 的极化秩，$\widehat{f}(\omega)$ 为输入掩码 ω 下的归一化 Walsh 系数。第四栏的秘密子密钥与公开输入分别走线；每轮 26 个 AND 均为字级操作。局部影子秩、统计结果与实测吞吐各自保留适用范围，不表示完整密码已达到 128 位安全性。图中 NIST 通过指比例与行级均匀性判据，Rabbit 按其电池 P 值判据验收；标记项在第八节报告。字节接口在 32 轮之后施加公开的 4-AND 输出剪切；每轮 26 个 AND 是分组核心的计数。

输入 $N\|\mathrm{BE}_{128}(j)$ 经 E_K 和公开输出置换 P 后，形成 R1-P4 字节流。初始化保存子密钥、nonce、计数器及余字节缓冲。图 2区分三个查询对象。旧 v3 公开调度的固定点与初始化/提取结构只用于历史反例，不是 v4 的运行规则。

a) 差分概率的三个层次. 为明确后文每个极值的范围，定义

$$\mathrm{DP}_\Phi(a,b) = 2^{-n}\#\{x : D_a\Phi(x) = b\},$$
$$p_\Phi(a) = \max_b \mathrm{DP}_\Phi(a,b),$$
$$\mathrm{DP}(\Phi) = \max_{a\neq 0} p_\Phi(a).$$

本文原记号 $\mathrm{DP}(a)$ 等于 $p_\Phi(a)$。方向 $a = 0$ 不参加全局最大化；固定 a 与遍历全部 $a \neq 0$ 不是同一任务。概率默认基于完整输入空间上的均匀 X。固定密钥的分布、对密钥平均的分布，以及初始化所得状态分布也应分别标注。

表 I统一主要记号。四字核心有 $n = 4W$ 个输入位，旧字内映射 h 只有 W 个输入位；二者的像、导数与秩分别计算。

B. 威胁模型

按 Kerckhoffs 原则，攻击者知道全部算法。主要考虑密钥恢复与统计区分两种游戏，其正式定义放在实例之后。本文给出保留未知 PRP 优势项的条件输出归约，但未得到原创原语的具体优势上界。密钥长度是参数，不是 2^{128} 或 2^{256} 攻击复杂度定理。任意发生器也没有普遍适用的纯生日界，因为输出关系可能更早暴露。选择 nonce、相关密钥、状态恢复、预测抵抗及回溯抵抗需要分别研究。

分析使用代数次数、二次导数 / 相关计算、小状态计数与模型路径搜索。模型最优值只有在编码和概率

2026 5 - 1 (1) Hua Shan Science Award 仅用于2026届华山科学奖公示

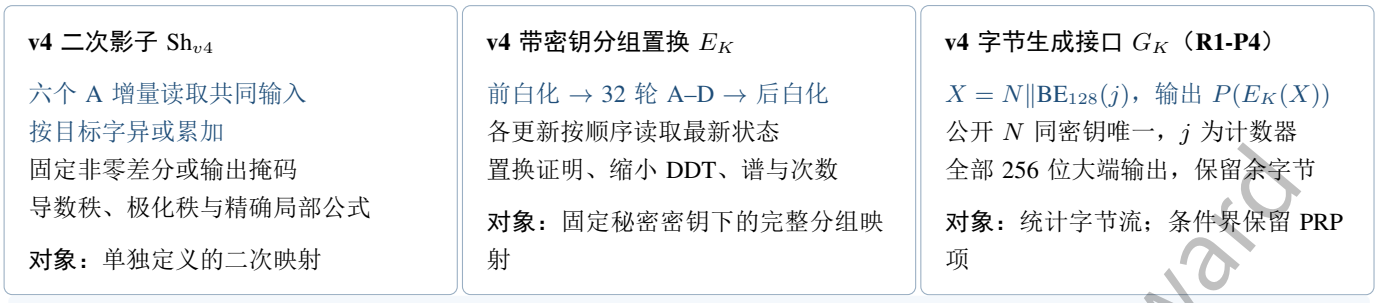


图 2. 当前 v4-R1 的三个分析对象。左侧固定六个 A 增量于共同输入，按目标字异或累加，仅用于二次局部查询；中间是实际顺序执行的带密钥分组置换 E_K；右侧是加上公开输出置换 P 的 R1-P4 字节接口。N 为 128 位公开 nonce，j 为 128 位计数器。分组 DDT、谱与 RTL 针对 E_K，统计电池针对 $P \circ E_K$；各层结论分别核查，不能相互代替。

表 I
主要记号及其对象

记号	含义
W, n	字宽及四字核心位数 $n = 4W$；h 的位数为 W
$\mathbb{F}_2, R_a$	二元域与循环左移 a 位
K, N, j	秘密主密钥、公开 nonce 及分组计数器
E_K, P, G_K	v4 分组置换、公开输出置换及 R1-P4 字节接口
$\mathrm{Sh}_{v4}, \mathrm{Sh}_{v3}$	分别按 v4、v3 端口定义的快照二次影子
Φ, h, Φ_p	一般指定映射；后两者仅指 v3 旧字内映射与固定公开字核心
a, b, u	输入差分、输出差分及输出掩码
B_a, Q_u	仿射导数的线性矩阵及标量二次分量的极化矩阵
$p_\Phi(a)$	固定 a 后对输出差分取最大的概率
$C_\Phi(\omega, u)$	指定输入掩码 ω 与输出掩码 u 的归一化相关
M_t, P_t	像大小与均匀输入的碰撞概率；一般不互为倒数

解释均被证明时，才能解释为真实概率指数。NIST SP 800-90A/B/C 提供标准化生成和熵接口术语[5]；Tempest 是实验性发生器，未获 DRBG 批准，也未证明符合 RBG 构造。提交代码未规定经验证的熵源或重新播种。

C. 证据分级

本文把每条结论归入四类证据，并在正文与表格中保持这一标签。表 II列出每类证据能够支持与不能支持的结论；这一分级是方法的一部分，而不是事后限定。

D. 相关工作

快速非密码发生器。xoshiro / xoroshiro 与 Mersenne Twister 的状态更新是二进制线性的 [1], [10]。

[5]标准原文：https://csrc.nist.gov/pubs/sp/800/90/a/r1/final；https://csrc.nist.gov/pubs/sp/800/90/b/final；https://csrc.nist.gov/pubs/sp/800/90/c/final。

表 II
证据等级与可支持的结论

等级	典型手段	能支持 / 不能支持
定理	代数推导、归纳、构造	全参数范围的确定命题；不包含未建模攻击
穷举	指定宽度与轮数的全枚举	该有限模型的精确计数；不外推到全宽
抽样	固定样本上的频率与相关	样本范围内的观测；不给出全局上界
工程	KAT、综合布线、吞吐	特定实现的一致性与成本；不证明安全强度

PCG 采用同余更新和输出变换 [2]，不能归为同一种 $\mathbb{F}_2$ 线性机制。统计质量不等于密码学不可预测性。

安全证明与成熟设计。BBS 和 RSA 类构造说明了基于假设的可证明安全 [11], [12]。ChaCha20 和 AES-CTR 是已有成熟设计 [3]，但密钥长度也不是排除一切高效攻击的无条件下界。本文未对 Tempest 给出同等安全定理。

$\mathbb{F}_2$ 构造与宽轨迹。SAND、Ascon 等展示 AND、XOR 和旋转可构造密码原语 [13], [14]；具体设计选择仍需分析。宽轨迹在多轮上约束活跃组件，而本项目的固定查询不能包含其全部论证。SIMON 类的精确二次差分与线性分析、自动搜索均已有研究 [15]，原创性应与这些方法比较。

自动与 AI 辅助分析。Gohr 用神经网络寻找减轮密码差分区分器 [9]；这里把类似工具作为校准后的 B 层筛查。CLAASP 等工具链自动产生 SAT / MILP 模型 [7]。本文评估器使用的是熟悉的缩小位宽全差分枚举和全位宽二进制秩计算。本项目把候选生成与性质检

2026 S. T. Yau High School Science Award 仅用于2026丘成桐中学科学奖论文公示

查分开。

二次布尔映射与 FPGA。二次映射的仿射导数性质是经典结论 [16][6]；本文把它系统地用于设计时检查。FPGA 部分记录确定性发生器的功能与成本，未建立经批准的熵源或 DRBG 集成。

III. AM-SEV 框架

AM-SEV 组织 $\mathbb{F}_2$ 上的局部计算、有限测量和复现控制。“度量”在这里指结构指标，不是满足距离公理的度量函数；SEV 是这些指标和实现问题的组织方式。每个指标对应明确对象，工程控制不是新的安全公理。

正确性范围。当前 v4 的实际轮按顺序读取最新值；它的二次影子才读取共同输入快照。本节历史 v3 的精确小位宽数字遵循旧快照语义：A 阶段读取轮开始的 (u_0, v_0, w_0, z_0)。KAT 检查的 C 与向量化 DSL 解释器逐位一致。早期解释器读取了当前寄存器，计算的是另一个轮函数；其 $H_\infty = 7.93$、$\tau = 1.000$ 以及级联表 5.00/8.00/8.00/7.80/7.80 撤回，以以下数字替代。

证据范围。分别记录明确假设下的数学命题、指定有限模型完整计数、采样或历史观察、待证明或测量的提案。回归只检验所选输入。局部证书或统计通过都不证明初始化后的发生器安全。新增检查与修正的日期另见修改清单。

a) 历史结果的适用范围.: 本节出现的 v3、旧字内映射 h、旧影子、秩 38 与像 3501 至 139 等结果只针对原对象。v4 改变了端口与执行顺序，对应性质在第六节重新推导；保留旧推导是为了不丢失修复所针对的反例。表 III逐项记录结构结论的来源；同一版本标签随结论一起出现。

A. 三类攻击维度的精确局部度量

差分、线性和代数是三种维度。矩阵精确公式用于已知二次映射的固定方向或掩码；电路传播给出次数上界。全局优化和高次级联另需工作。

III-A1 导数矩阵的秩与仿射导数.

定义 III.1 (设计空间与二次影子)**.** 设计由 AND、XOR、旋转构成，字宽 W，四字 $(u, v, w, z) \in (\mathbb{F}_2^W)^4$。若每个 AND 的输入都是轮输入的仿射函数，则该“二层”设计的映射至多二次。v3 历史级联的影子 Sh_{v3} 保留快照 A、额外快照 AND 及固定公开注入，删除字内预混合和后续级联。当前 v4 的影子 Sh_{v4} 则采用修订读端口，将 A 的六个增量固定于共同输入并按目标字异或累加（第 VI-C 节）。两者均单独定义；正文简称 Sh 时，以所标版本为准。

对旧 v3，当 $W = 4$ 时，字内预混合因 $22 \equiv 26$、$7 \equiv 19 \pmod 4$ 退化为线性；在测试过的 8、16、32、64 位，其 AND 是非线性的。影子按定义在各位宽均为二次，使用定理时不能暗中把完整预混合算进去。

定理 III.1 (仿射差分定理；经典二次结论)**.** 若 $\Phi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ 的代数次数至多 2，则每个固定非零 Δ 满足

$$\begin{aligned} D_\Delta(s) &= \Phi(s + \Delta) + \Phi(s) \\ &= B_\Delta s + D_\Delta(0), \\ B_\Delta e_j &= D_\Delta(e_j) + D_\Delta(0). \end{aligned}$$

因此，在全空间均匀输入下，

$$\begin{aligned} \mathrm{DP}(\Delta) &= \max_c \Pr[D_\Delta(s) = c] \\ &= 2^{-\operatorname{rank} B_\Delta}, \\ H_\infty(\Phi) &= \min_{\Delta \neq 0} \operatorname{rank} B_\Delta. \end{aligned}$$

固定方向的矩阵构造后，二进制消元为 $O(n^3)$；遍历全部非零差分是另外的搜索，并未被此定理变为多项式时间。

证明. 对单项式 $s_i s_j$ 展开，差分为 $\Delta_i s_j + \Delta_j s_i + \Delta_i \Delta_j$，关于 s 仿射。导数的每个非空纤维是 $\ker B_\Delta$ 的陪集，大小为 $2^{n - \operatorname{rank} B_\Delta}$；除以 2^n 即得概率。 □

这里的 $H_\infty(\Phi)$ 专指最坏非零输入差分下的输出差分最小熵，即 $\min_{a \neq 0} H_\infty(D_a\Phi(X))$，其中 X 在完整输入空间上均匀。它与 $\Phi(X)$ 本身的输出最小熵是不同对象。原记录在 $W = 4$ 覆盖 65,535 个方向，在超过 10^5 个随机二次映射测试及 $W = 8$ 导数测试中未见反例；相关脚本为 `audit_cascade_rank.py` 和 `test_aggregation_conjecture.py`。

推论 III.1 (二阶退化)**.** 二次映射的二阶导数

$$\begin{aligned} D_{a,b}\Phi(s) = \Phi(s) &+ \Phi(s + a) \\ &+ \Phi(s + b) + \Phi(s + a + b) \end{aligned}$$

[6]教材来源：C. Carlet，*Boolean Functions for Cryptography and Coding Theory*，Cambridge University Press，2021，doi: 10.1017/9781108606806。

2026 S. T. Yau High School Science Award 仅用于2026丘成桐中学科学奖论文公示

表 III
结构结论的来源。“v3”表示旧设计上的公式；“v4 新”表示 v3 没有的结果；“v4 修正”表示因端口或执行顺序改变而重推。版本标签不构成安全性迁移。

结果	对象/范围	版本	在 v4-R1 中的状态
仿射导数；$\mathrm{DP}(\Delta) = 2^{-\operatorname{rank} B_\Delta}$	二次影子	经典	仅用于指定版本影子
二次 Walsh 秩公式	固定二次掩码	经典	仅固定掩码
差分映射次数	一般映射	经典	适用一般映射
级联次数律	v3 级联前缀	v3	历史；v4 次数另行推导
无重叠读字秩	v3 快照端口	v3	v4 端口由修正公式取代
RX 极化恒等式	v3 二次类	v3	历史；不作为 v4 安全结论
固定方向 $W = 4$ 比较	v3 缩小模型	v3	修复所针对的缺陷证据
h 的非单射性	v3 核心轮	v3	修复所针对的缺陷证据
非线性残差反例	一般	v3	继承
差分分解界	级联	v3	在 v4 中修正
K_4 满秩	v4 影子	v4 新	用于 v4
修正读字秩（重叠项）	v4 影子	v4 修正	用于 v4
剪切、线性逆、置换	v4 核心	v4 新	用于 v4
条件 CTR 界	v4 接口	v4 应用	用于 v4
子密钥边缘分布	v4 密钥表	v4 新	用于 v4

表 IV
AM-SEV 评估记录：结论与成立条件一并保存

字段	记录内容
程序对象	源码版本、字宽、常量、快照或顺序语义
查询条件	输入分布、公开参数、轮数、差分与掩码
结构指标	次数上界、差分概率与相关；区分精确值和界
核查工件	矩阵、消元、有效见证、完整计数或模型证书
代码核查	KAT、回归、数据流及实际覆盖范围
工程成本	运行环境、吞吐、面积及测量或估计方法
结论状态	已证明、已穷举、有限观察或开放

与 s 无关，等于双线性极化值 $B(a,b)$，所以它恒为零当且仅当 $B(a,b) = 0$。这描述二阶布尔导数，不建立回旋镖连通性或多轮性质。

证明. 常数和线性项各出现偶数次并抵消；二次项 $x_i x_j$ 留下 $a_i b_j + a_j b_i$。逐输出位相加即得结论。 □

原 $W = 4$ 检查抽取 200 对方向，每对 6 个状态点，结果均为常量，脚本 `rx_theory_check.py`。

a) 二阶展开的中间项: 线性项 x_i 对二阶导数的贡献是

$$x_i + (x_i + a_i) + (x_i + b_i) + (x_i + a_i + b_i) = 0.$$

常数同样抵消。乘积项 $x_i x_j$ 的四项展开只留下 $a_i b_j + a_j b_i$；所有含基点 x 的项均抵消，因而二阶导数与基点无关。这是上一段证明的逐项计算，不附带多轮或回旋镖安全结论。

下文使用两个不同的矩阵，不能混用：导数矩阵 B_Δ（等价地 M_a）给出差分概率；极化矩阵 Q_u 给出固定输出掩码下的 Walsh 相关。关于其中一个的秩结论不能直接搬到另一个。

III-A2 Walsh 秩公式. 经典 Dickson 标准形给出二次函数的线性对应 [16]。此处它是评估组件，未作为新定理主张。

定理 III.2 (经典二次 Walsh 公式)**.** 设 $\Phi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ 的代数次数至多 2。固定非零输出掩码 u，令 $g_u(x) = u \cdot \Phi(x)$。极化矩阵

$$(Q_u)_{ij} = g_u(0) + g_u(e_i) + g_u(e_j) + g_u(e_i + e_j)$$

是交替矩阵，秩 r_u 为偶数。若

$$C_\Phi(a,u) = 2^{-n} \sum_x (-1)^{a\cdot x + u\cdot\Phi(x)},$$

则 $\max_a |C_\Phi(a,u)| = 2^{-r_u/2}$，最大概率偏差为 $2^{-1-r_u/2}$。未归一化 Walsh 系数是 0 或 $\pm 2^{n-r_u/2}$。固定掩码的秩计算是多项式时间；对全部非零输出掩码优化仍是另一个搜索。

证明. 可逆二进制换元把二次部分分成 $r_u/2$ 个独立乘积。每对的 Walsh 和绝对值 2，剩余变量贡献 0 或 2^{n-r_u}。相乘再归一化得相关，概率偏差是相关的一半。线性项平移谱支撑。 □

2026 Shi Yau High School Science Award
仅用于2026石成相高中科学奖论文公示

表 V
局部度量及其假设；末两行仅为 v3 历史数值，v4 见第六节

项目	差分	线性	代数
对象	固定 Δ	固定 $u \neq 0$	指定电路
假设	二次映射	二次分量	层语义明确
结果	$p = 2^{-r}$	$\max_a \lvert C\rvert = 2^{-r/2}$	次数上界
全局任务	搜索差分	搜索输出掩码	证明达界
v3 四位轮	1066/65536	见表VIII	次数 16
v3，64 位	影子单比特秩 3	影子全 1 掩码秩 256	次数 ≤ 64

a) 配对求和与归一化的细节: 在极化形式的标准坐标中，写 $r_u = 2k$。每对二次变量的求和为

$$\sum_{s,t\in\{0,1\}} (-1)^{st+\alpha s+\beta t} = 2(-1)^{\alpha\beta}.$$

这可按 $s = 0, 1$ 分组直接验证。不同配对使用不同变量，所以求和相乘，贡献幅度 2^k。其余 $n - r_u$ 个方向没有二次项，每个线性系数为零时贡献 2，否则贡献 0。故非零未归一化幅度为

$$2^{r_u/2}2^{n-r_u} = 2^{n-r_u/2}.$$

再除以 2^n 得相关；事件概率相对 $1/2$ 的偏差再除以 2。输入掩码会随可逆坐标变换重新编号，线性项会改变谱的支撑。可逆输出线性变换也只在对全部输出掩码优化时保持最优值，不能保持某个同名掩码的意义。

对指定二次前缀，$W = 64$ 时全 1 输出掩码的已检查秩为 256。因此只对此输出掩码，遍历输入掩码的最大相关为 2^{-128}，最大概率偏差为 2^{-129}。不能作为完整级联或发生器的全局线性界；原来其他掩码扫描只是有限观察。

III-A3 导数次数与级联次数.

定理 III.3 (差分映射次数；一般映射)**.** 设 $\deg\Phi = d \geq 1$。对每个非零且导数不恒零的方向，$\deg D_\Delta\Phi \leq d-1$；并存在某个非零方向达到 $d-1$。不是每个方向均达到。

证明. 最高次项在 $\Phi(s+\Delta)+\Phi(s)$ 中抵消，给上界。取某坐标中的 d 次单项式 $m = x_{i_1}\cdots x_{i_d}$，沿 e_{i_1} 求导留下 $\prod_{j=2}^{d} x_{i_j}$。只有 m 本身能产生该项，故不能被别的单项式抵消。例 $\Phi = x_1x_2$ 沿 e_3 导数恒零，说明原来的逐方向下界表述错误。 □

在 $W = 4$，完整轮次数 16，方向 $0x1$ 导数次数 15，来自完整 ANF，脚本explore_cascade_degree.py。高次数或非线性残差本身不决定分布集中还是分散。

定理 III.4 (级联次数律；v3)**.** 令 Φ_0 为带字内预混合的指定前缀，每增加一个跨字 AND 层得到 Φ_k，中间线性层按规定放置。则

$$\deg\Phi_k \leq 2^k \deg\Phi_0.$$

此处带预混合的前缀一般不再二次。四位截断原始完整 ANF 记录为 $2, 4, 8, 14, 16$（$k = 0, \ldots, 4$）：前两次达倍增界，随后抵消使次数为 14 而非 16，最后到 16 变量上限。

证明. 使用复合次数界 $\deg(F \circ G) \leq \deg F \deg G$。每个乘积层至多把输入次数加倍，XOR 和旋转不增加次数。小模型具体次数由全部 2^{16} 状态的 Möbius 变换求得。 □

上述截断序列是原小模型记录；完整表审计确认列出轮数处完整映射次数 16、方向 1 导数 15，并未独立证明后来源码注释中的全位宽等式。全位宽实际电路为初始二次层、一个非线性字内预混合、四个乘积层，次数上界序列 $2, 4, 8, 16, 32, 64$，第二预混合线性。因此 $\deg\Phi \leq \min(4W, 64)$。等号、多轮次数下界、攻击复杂度均不随层数自动成立；高阶导数消失也不是积分安全证明。

B. 二次结构的低秩方向与适用边界

对指定二次前缀，可直接核查低秩见证。它促使研究更深映射，但不证明级联是唯一设计选择。

III-B1 二次映射低秩见证.

推论 III.2 (限定范围的秩观察)**.** 在 $W = 4$，所有非零差分的最小导数秩为 3，全局最大差分概率 $1/8$。在 $W = 4, 8, 16, 32, 64$，检查过的所有单比特方向均秩 3。大位宽的秩 3 见证只证明全局最小秩至多 3，不能排除其他方向更低。不主张所有方向、所有位宽下界。

证明. 四位结论来自 65,535 行完整计数和仿射导数定理；大位宽来自参数明确的固定方向矩阵计算。交替双线性搜索找到见证后停止，不能证明最优。 □

III-B2 读字结构与单字差分.

定理 III.5 (受限单比特读字结论；v3，v4 端口下由修正公式取代)**.** 二次快照映射中，读取字 w 的非线性门形如 $d_g \mathrel{+}= R_{r_g}w \wedge R_{s_g}o_g$，且 $o_g \neq w$。若恰有 k 个门读取 w，对单比特方向 $e_{(w,p)}$ 的导数贡献具有不同输入列

2026 S&T Yau High School Science Award
仅用于2026年成都市科学奖论文公示

和不同输出行，则导数矩阵秩为 k。这是带非重合条件的单比特结论，不是全局差分定理。

证明. 每个门在行 $(d_g, p+r_g)$、列 $(o_g, p+r_g-s_g)$ 给一个单位元素，位置模 W。行列互异形成有 k 项的部分置换矩阵，秩为 k。仿射项只贡献常数；后接可逆线性输出变换也保持导数矩阵的秩。多比特、多字时须另查合并与抵消。 □

推论 III.3 (本影子的单字精确秩)**.** 对 v3 A 层（原四字快照层）的六门二次影子，某字 x 上的差分支撑 $P \subseteq \mathbb{Z}_W$，$|P| = t$，则

$$\operatorname{rank} B_\Delta = 3t - |P \cap (P+2)|\mathbf{1}_{x=z}. \tag{1}$$

证明. 读取任一字的三个门有不同配偶字，所以触发的单位列不重复，秩等于触及的不同输出行数。只有读取 z 并写 u 的两门可能行重合，相关旋转 25 和 23 相差 2，故重合计数为 $|P \cap (P+2)|$，每次少一个秩。 □

a) 行重合的定位条件: 若两个门写同一输出字，输入差分位置 p, p' 触及相同输出行的条件为

$$p + r_x \equiv p' + r'_x \pmod{W}.$$

本影子只有读 z 并写 u 的两门可能出现这一重合；其旋转 25、23 给出 $p'-p \equiv 2$。不同配偶字确保输入列不重合，因而这里可通过不同输出行数计秩。这个前提在一般设计中并不自动成立。原检查入口为rx_theory_check.py；原 15 种支撑记录属于旧实验，本轮没有把它重标为新的全域计算。

四位下各字 15 种非空支撑全部吻合。公式只依赖旋转差 2 与模 W 位置。本项目早期曾把相同输出门对的对齐数当作整个双列设计类的秩规律，这是错误的：配偶字重复时还会列合并，甚至同一行列完整重合，故这里仅保留特定影子公式及旧广义版反例。$t \geq 2$ 时该秩至少 $2t \geq 4$，单比特为 3；这仍未覆盖多字差分，不能补齐全位宽全局下界。

III-B3 其他二次实例与宽轨迹. 经典“二次导数仿射”不限于 AND-RX。五位 χ 型示例 $y_i = x_i + (x_{i+1} \wedge x_{i+2})$ 的 31 个非零方向均符合，最小秩 2、最大 DP 为 $1/4$；这只是小型说明映射，并非完整 Ascon S 盒规范。SIMON 型 Feistel 轮 $F(x) = (R_1 x \wedge R_8 x) + R_2 x$ 的 16 位状态的 65,535 个非零差分完整检查得到最小秩 0：透传使 $(\Delta L, 0) \to (0, \Delta L)$ 确定发生，DP 为 1。多轮扩散会改变这些局部关系，不能据此判定完整密码不安全。这些实例说明经典性质的用途，不建立新密码分析方法 [14], [15]。宽轨迹控制多轮活跃组件，固定方向极化给一行局部分布；双方不能替代对方缺失的假设，当前级联完整路径求和仍未解决。

III-B4 旋转对称与 RX 维度. 旋转攻击考察 $(x, R_k x + \delta)$ 类输入对，是 ARX / AND-RX 的标准攻击面 [17]–[19]。前三类度量本身不涵盖旋转；在常数自由部分等变时，可把 RX 转成一阶差分。

去掉常数的二次影子满足 $f(R_k s) = R_k f(s)$：旋转与共同旋转下的 XOR、AND 可交换。四位对全部状态验证过，同一代数论证适用于各位宽。外部常数可能破坏相等关系，但只平移 RX 输出值，不改变最大点概率。

定理 III.6 (RX 极化秩恒等式；v3)**.** 设 $\Phi = f + c$ 二次，$f(R_k x) = R_k f(x)$。令

$$g_{\delta,k}(s) = \Phi(R_k s + \delta) + R_k \Phi(s).$$

则 g 仿射，$\mathrm{RXDP}(\delta) = \mathrm{DP}(R_k^{-1}\delta)$，其中两边均取各自输出值上的最大概率。

证明. 令 $a = R_k^{-1}\delta$，则 $R_k s + \delta = R_k(s+a)$。代入等变性质得

$$g_{\delta,k}(s) = R_k(D_a\Phi(s)) + c + R_k c.$$

导数内部常数抵消，外部 $c + R_k c$ 仍在，但只作平移。输出旋转可逆，保持秩与纤维大小，所以最大概率相同。$\delta = 0$ 时导数恒零，最大概率为 1，可单独处理。 □

a) RX 仿射矩阵与概率的对应: 将 $D_a\Phi(x) = B_a x + c_a$ 代入前式，得到

$$\begin{aligned} g_{\delta,k}(x) &= R_k B_a x + R_k c_a + c + R_k c, \\ \operatorname{rank}(R_k B_a) &= \operatorname{rank} B_a, \\ \max_{\varepsilon} \Pr[g_{\delta,k}(X) = \varepsilon] &= 2^{-\operatorname{rank} B_a} = \mathrm{DP}(a). \end{aligned}$$

最后一行的幂次表达式使用二次假设；输出旋转和平移本身保持纤维大小的事实不限于二次映射。常数只作为末端输出平移时才能这样处理，固定掩码、逻辑移位或内部非线性前的常数须按实际程序判断等变性。

该结论不能排除复合发生器的旋转攻击，也不能在常数进入后续非线性层时自动使用。较大位宽级联扫描只是有限观察，旧 RX 脚本是辅助材料。

2026 S. T. Yau High School Science Award 作品报告 论文公示

表 VI
历史 v3 与其他生成器的对象范围比较

指标	Tempest v3	xoshiro256**	ChaCha20
状态 $\mathbb{F}_2$ 线性	否	是	否
次数	四位 16	状态 1	未评估
核心 DP	四位 1066/65536	1	未评估
核心单射	否	是	未比较
秩分析对象	二次前缀	线性状态	不直接适用
公开注入	单独检查	不适用	未比较
已存输出测试	1 TiB	8 GB	8 GB

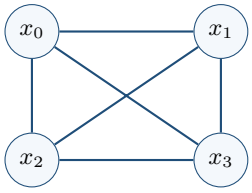


图 3. v4 二次影子的完整四字交互图。边表示含旋转的 AND 乘积配对，仅用于极化分析，不表示实际顺序 A 模块的执行顺序。

线性与 ARX 的范围边界。xoshiro256** 的状态更新只有加载、XOR、移位，是 $\mathbb{F}_2$ 线性的；200 对抽查支持源码论证。状态次数 1，固定方向传播确定、DP 为 1，转移矩阵满秩 256，因此核心为置换。这些结论不自动覆盖其含模乘法的输出扰乱器。XOR 与旋转也不能称为模 2^{64} 整数环上的线性。对 ChaCha20，本框架未给精确全局差分或次数结论。下表是适用范围检查，不是共同安全等级排序。

b) 跨算法检查的来源: 表VI的原辅助入口为baseline_compare.py 及存档输出测试。xoshiro 状态转移的二进制矩阵秩记录为 256/256，线性性和差分确定传播各有 200 对输入的回归支持；普遍结论来自源码的线性组成和矩阵，而非 200 个样本。上述状态结论不覆盖其模乘输出扰乱器；ChaCha20 的全局差分与次数仍未由这张表计算。

C. 完整四字交互图

四字 AND-RX 设计中一个有用的特殊情形是完整交互图：四个字两两之间恰有一个 AND 乘积。它在极化分析中可完全求解，也为后文 v4 影子的满秩结论提供结构解释。图 3给出该图；边表示带旋转的乘积，不表示执行顺序。

命题 III.1 (四字完整交互图的极化满秩；v4 新结果)**.** 设 $W = 2^m$，$x_0, \dots, x_3 \in \mathbb{F}_2^W$。记 $\pi(y) = \sum_{i=0}^{W-1} y_i \in \mathbb{F}_2$，并定义

$$q(x) = \sum_{0 \le a < b < 4} \pi\big((R_{r_{ab}} x_a)(R_{s_{ab}} x_b)\big) + \ell(x),$$

其中各旋转量任意，ℓ 为任意仿射布尔函数。则 q 的极化矩阵在 $\mathbb{F}_2$ 上的秩为 $4W$。对任意输入掩码 $\omega \in \mathbb{F}_2^{4W}$，归一化 Walsh 系数的绝对值均为 2^{-2W}，相应偏差为 2^{-2W-1}。

证明. 把一个字视为环 $\mathcal{R} = \mathbb{F}_2[t]/(t^W - 1)$ 中的多项式，R_r 对应乘以 t^r。极化矩阵可写成 $\mathcal{R}$ 上的 4×4 矩阵 M：对角块为零，(a, b) 块为 $t^{s_{ab} - r_{ab}}$，反向块为其逆移位。仿射项不影响极化。

由于 W 是二次幂，$t^W - 1 = (t+1)^W$。多项式在 $t = 1$ 处取 1，就不含因子 $t+1$，与 $(t+1)^W$ 互素；由多项式的扩展欧几里得算法，它在 $\mathcal{R}$ 中可逆。令 $t = 1$，每个非对角块均变为 1，故 $M(1) = J_4 + I_4$，其中 J_4 为全一矩阵。在特征二下 $J_4^2 = 0$，于是 $(J_4 + I_4)^2 = I_4$。因此 $\det M$ 在 $t = 1$ 处取 1，在 $\mathcal{R}$ 中可逆。由伴随矩阵公式，M 在 $\mathcal{R}$ 上可逆，也就是对应的 $4W$ 维二进制线性映射可逆。秩结论随即得到。最后应用二次布尔函数的 Walsh 秩公式：满秩 $r = 4W$ 时，全部归一化 Walsh 幅值为 $2^{-r/2} = 2^{-2W}$。 □

该命题说明：当 $W = 2^m$ 且六个字对全部出现时，任意旋转参数与任意仿射项都不改变满秩结论。$W = 64$ 时秩为 $4W = 256$，全字奇偶掩码的归一化 Walsh 幅值为 $2^{-2W} = 2^{-128}$。这是局部二次函数的相关性陈述，不直接给出顺序模块或完整密码的安全位数。

字宽条件确实必要。例如在 $W = 3$ 时取

$$q(x) = \pi(x_0x_1 + x_0x_2 + x_0x_3 + x_1x_2) + \pi(x_1R_1x_3 + x_2R_2x_3).$$

其极化矩阵的核恰为 $(a, a, a, 0)$，其中 a 为偶校验的三位字。验证这一点，令 $C = I + R_1 + R_2$：前三行方程给出 $Cx_3 = 0$，最后一行化为 $Cx_2 = x_3$。C 的像为 $\{000, 111\}$，核为偶校验子空间，二者交集仅有零，故 $x_3 = 0$，其余三字相同且偶校验。核维数为 2，12 维极化矩阵的秩因而为 10。完整 4096 点 Walsh 变换进一步核对最大绝对值为 128，即归一化幅值 $1/32$，而非满秩情形的 $1/64$。二次幂字宽下另有 224 组旋转矩阵与 1792 次极化恒等式核对；这些计算检查实现，普遍性来自上述证明。

2026 S&T Young Scientist Award 仅用于2026国防科学技术奖公示

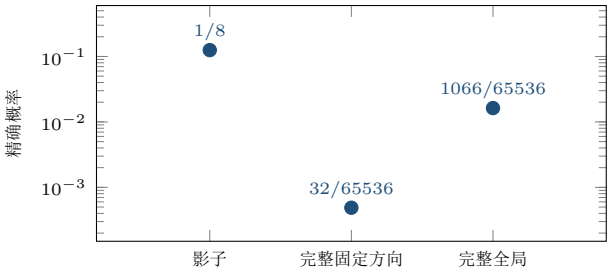


图 4. v3 历史四位级联：固定方向与全局最大

D. 级联效果与状态压缩

此部分比较所选前缀和完整级联，并记录状态压缩；不证明安全设计都必须采用该级联。

III-D1 固定方向的级联比较.

命题 III.2 (固定方向小模型比较；v3 缩小模型)**.** $W = 4$、初始公开字 8、方向 $0x1$ 下，前缀最大概率 $8192/65536 = 1/8$，完整轮为 $32/65536 = 2^{-11}$。完整轮的全局最大却是 $1066/65536$，发生在 $0x5005$。

次数序列 $2, 4, 8, 14, 16$ 不保证差分同步改善，也不给全位宽攻击界。图4在统一模型下比较固定方向与全局极值；用对数纵轴上的独立点表示精确概率。

III-D2 状态像与多轮合并.

命题 III.3 (固定公开调度核心轮非单射；v3 缺陷)**.** 对 $h(x) = x + R_{22}x + R_{26}x + (R_7x \wedge R_{19}x)$，令 $d = \gcd(12, W)$，则

$$|\operatorname{im} h| \le 2^W - 2^{d-1}, \qquad |\operatorname{im} \Phi_p| \le (2^W - 2^{d-1})^4 < 2^{4W}.$$

p 是固定公开输入，像针对全部核心状态。

证明. 全 1 字记为 $\mathbf{1}$，展开有 $h(x + \mathbf{1}) + h(x) = R_7x + R_{19}x$。旋转 12 位不变的字有 2^d 个，构成 2^{d-1} 对互补碰撞。四个并行 h 给乘积像上界，之后确定性组合不能增加像的大小。 □

a) 64 位像上界的加强（本次增补）： 对相同的 h，取

$$a = \texttt{3B3B3B3B3B3B3B3B},$$
$$x_* = \texttt{0110011001100110},$$
$$c_a = h(a) + h(0) = \texttt{8080808080808080}.$$

其仿射导数的线性部分为

$$B_a x = (R_7 a \wedge R_{19} x) + (R_{19} a \wedge R_7 x). \tag{2}$$

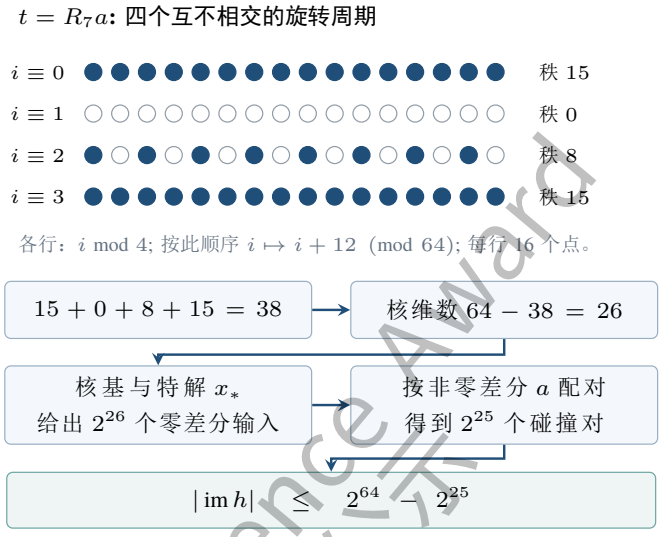


图 5. v3 旧字内映射 h 的秩 38 证书。实心/空心点分别为系数 1/0，核维数与已验证特解确定零差分解集；碰撞仅属于该旧 h。

下面不依赖随机抽样，直接计算其秩。令 $y = R_7x$、$t = R_7a$，则 $B_ax = t \wedge R_{12}y + R_{12}t \wedge y$。旋转 12 在 64 个位置上分成四个长度 16 的循环。t 的 8 位重复模式是 9D；按位置模 4 分组，四个循环上的系数分别为全 1、全 0、交替 1/0、全 1。

全 1 循环对应 $I + R$，核是常量串，秩 15；全 0 循环秩 0；交替循环仅 8 个变量有效，每个进入一对输出，秩 8。因此

$$\operatorname{rank} B_a = 15 + 0 + 8 + 15 = 38.$$

代入上述 x_* 可验证 $B_ax_* = c_a$，等价于 $h(x_* + a) = h(x_*)$。故零差分方程的解集是 $x_* + \ker B_a$，恰有 2^{26} 点。该集合在 $x \mapsto x + a$ 下不变，因 $a \neq 0$ 分成 2^{25} 个互不重叠的碰撞对，得到

$$\begin{aligned} |\operatorname{im} h| &\le 2^{64} - 2^{25}, \\ |\operatorname{im} \Phi_p| &\le (2^{64} - 2^{25})^4. \end{aligned} \tag{3}$$

这加强了前述 $(2^{64} - 8)^4$ 界。独立 C 计算由函数值构造导数矩阵，Python 由乘积展开构造矩阵；两者均得秩 38 及同一特解。发布包保存 64 列矩阵与 26 个核基向量。固定方向的零差分概率 2^{-38} 属于字内 h，不能直接当作经过 A、B 后的完整轮差分概率；也未证明该方向全局最优。像上界不等于初始化后的密钥熵损失，更不等于已构造实用输出流攻击。

一致的小模型规定 $W = 4, p_0 = 8$、旋转模 4、常数截断、移位距离不改；不含初始化与提取，枚举全部

2026 S.T. Yau High School Science Award
仅用于2026丘成桐中学科学奖公示

表 VII
v3 固定公开调度下的完整四位计数；概率均为计数除以 65,536

R	全局最大计数	差分 a	方向 1 计数	像大小
1	1066	5005	32	3501
2	1222	5005	94	2066
4	1362	5005	254	1077
6	1522	5005	380	732
8	1628	5005	460	544
12	1900	0408	798	311
16	2244	0204	1104	210
22	2472	A00A	1352	139

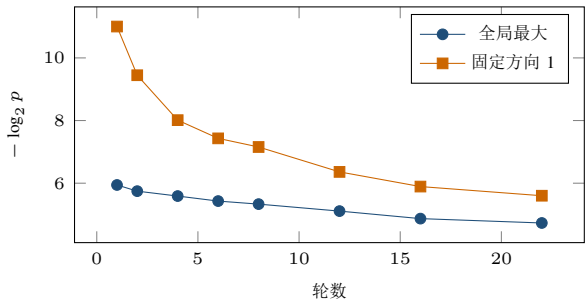


图 6. v3 历史多轮曲线：纵轴越低表示集中越强

65,536 状态及 65,535 非零方向。完整计算于 10 月 28 日执行，本修订采用存档计数，未声称新做长时间重跑。

所列轮数中全局最大概率增加，像从 3501 缩到 139。22 轮为 $2^{-4.7285}$，替换因公开初始化不一致得到的旧 $2^{-4.82}$。更多轮没有改善此模型的全状态指标；大位宽样本未见碰撞不能推出像或差分的全局界。

命题 III.4 (非线性残差未必分散；v3)**.** 非线性导数的仿射部分秩不能决定最大点概率。两位 $H(x) = x + x_0x_1(1,1)$ 线性部分秩 2，最大概率却 $1/2$；三位 $H = (x_0, x_1x_2, 0)$ 线性部分秩 1，最大概率 $3/8 < 1/2$。逐点枚举即可验证。

为使这两个映射成为实际导数，增加一个输入位 t，取 $F(t,x) = (0, tH(x))$，则 $D_{(1,0)}F(t,x) = (0, H(x))$。新增自由位不改变点概率或仿射部分的秩，故反例也适用于导数。这替换原来带普遍意味的“聚集”解释。

命题 III.5 (固定调度复合的零差分单调性)**.** 设 $F_0 = I$、$F_{t+1} = \Phi_{p_t} \circ F_t$，公开序列 p_t 预先固定。对任意固定 a，令

$$Z_t(a) = \Pr_X[F_t(X + a) = F_t(X)],$$

其中 X 在 $N = 2^n$ 个状态上均匀。则 $Z_{t+1}(a) \geq Z_t(a)$。若 $m_{t,y} = |F_t^{-1}(y)|$，则碰撞概率

$$P_t = \frac{\sum_y m_{t,y}^2}{N^2} = \frac{1}{N}\sum_a Z_t(a) \tag{4}$$

也不随 t 下降。写 $M_t = |\operatorname{im} F_t|$，有

$$\max_{a\neq 0,b} \Pr[D_aF_t(X) = b] \geq \frac{NP_t - 1}{N - 1} \geq \frac{N - M_t}{M_t(N - 1)}. \tag{5}$$

证明. 两个轨迹一旦在 t 轮相等，经过同一个下一轮函数后仍相等，因此零差分事件包含于下一轮事件。对全部有序输入对计数得到式(4)。后续映射只会合并纤维；合并大小 s, t 时，平方和增加 $2st \geq 0$。又 $Z_t(0) = 1$，非零方向的平均零差分概率为 $(NP_t - 1)/(N - 1)$，其中至少一个不小于平均值。Cauchy–Schwarz 给 $\sum_y m_{t,y}^2 \geq N^2/M_t$，得到第二个下界。 □

该命题解释了“轨迹合并”如何同时反映到像大小、零差分与谱能量。它不声称任意非零输出差分的概率或完整 DDT 最大值普遍单调；也不能直接移用于再次注入密钥的初始化分布。本文玩具模型存档的所列轮数在最坏行上由零输出差分达界。本次对 22 个核心复合映射重新计数纤维，见表VIII，与原像大小一致。

III-D3 差分分解界.

定理 III.7 (修正的差分分解界；v4 修正)**.** 若 $D_\Delta(x) = B_\Delta x + c + R_\Delta(x)$，$r_\Delta = \operatorname{rank} B_\Delta$，则

$$\mathrm{DP}(\Delta) \geq \frac{1}{2^{r_\Delta}|\operatorname{im} R_\Delta|}.$$

证明. 导数像包含于 $c + \operatorname{im} B_\Delta + \operatorname{im} R_\Delta$，支撑点数至多 $2^{r_\Delta}|\operatorname{im} R_\Delta|$。至少一点概率不小于其倒数。不假设残差与仿射部分独立。 □

旧分母 2^{n-r_Δ} 混淆纤维大小和像大小。例 $F = (x_0x_1, x_0x_2, 0)$、$\Delta = e_0$，导数 $(x_1, x_2, 0)$ 最大概率 $1/4$，旧式误给下界 $1/2$；新式为 $1/4$。对非线性残差也不能无条件推 2^{-r_Δ} 上界。

a) 像大小与碰撞概率. 像大小 M_t 统计可达值，碰撞概率 P_t 还取决于各逆像的重数。二者满足

$$1 \leq \frac{1}{P_t} = \frac{N^2}{\sum_y m_{t,y}^2} \leq M_t. \tag{6}$$

右侧由 Cauchy–Schwarz 不等式得到，等号要求所有非空逆像等大。$1/P_t$ 可以不是整数。例如四个输入的逆像重数为 $(2,2)$ 或 $(3,1)$ 时，像大小同为 2，碰撞概率

2026 CJT Yan Huang School Science Award
仅用于2026年度中学科学奖公示

却分别为 1/2 和 5/8。旧四位模型一轮有 $M_1 = 3501$、$1/P_1 \simeq 2561.16$，22 轮有 $M_{22} = 139$、$1/P_{22} \simeq 48.34$；这些是全状态均匀输入下的量，不是初始化密钥熵或输出安全性。

E. 可复现评估与辅助检查

III-E1 证书与评估控制. 证书必须指定来源、参数和性质，而不是整个发生器的安全认证。

- 对已知二次映射的固定方向，保存导数矩阵、常数和消元结果。低秩见证不是全局最小值证明。
- 最小化模型的可行解给代价上界；下界需正确编码与完整排除更低代价，并提供可核验证书或穷尽。超时不满足要求。
- 电路传播给次数上界；下界 / 精确值需真实程序中的有效单项式或等价证书。仅留若干最高次项并不自动完整。
- 检查固定核心状态时改变公开 p 是否改变转移。旧 `legacy_v31` 先保存 S_0，向 S 注入 p 函数，再从 S_0 重写四字，因此该注入对核心输出始终无效。主密钥仍通过初始化进入；这是公开调度注入被覆盖，不是弱主密钥类别。旧 τ 不再保留为密钥秘密性指标。

A1 保留回归控制、A2 廉价筛查与精确评估分开、A3 提案与检查分开、A4 记录源码版本 / 种子 / 证据，都是工程惯例，不是数学公理，也不证明覆盖所有攻击或具有样本外安全预测能力。

III-E2 差分—谱对偶. 定义 $\mathrm{DP}_0(\Delta) = \Pr[\Phi(x+\Delta) = \Phi(x)]$ 及

$$E(a) = 2^{-n} \sum_u C_\Phi(a,u)^2.$$

由经典 Wiener—Khinchin 恒等式 [20]，

$$\mathrm{DP}_0(\Delta) = \sum_a (-1)^{a\cdot\Delta} E(a),$$

$$E(0) = \langle \mathrm{DP}_0 \rangle_\Delta = \langle C_\Phi(0,u)^2 \rangle_u.$$

式(4)中的 P_t 恰为此处 $E_t(0)$，将多轮纤维合并与谱能量连接。随附数学检查器对小完整映射验证此式。它连接零差分概率与能量，不是新的安全归约，也不是已完成全位宽全掩码评估的声明。

a) 对偶恒等式的归一化步骤: 输出零差分的指示函数可以写成

$$\mathbf{1}_{y=0} = 2^{-n} \sum_u (-1)^{u\cdot y}.$$

表 VIII
v3 一致四位模型的像、碰撞能量与指定掩码精确谱

R	M_R	$\sum_y m_{R,y}^2$	P_R（近似）
1	3501	1676962	0.00039045
2	2066	5610016	0.00130618
4	1077	16068990	0.00374135
6	732	26323378	0.00612889
8	544	32797064	0.00763616
12	311	51721918	0.01204245
16	210	73953594	0.01721866
22	139	88844774	0.02068579

映射（输出掩码集 $\mathcal{U}$）	$\max_{a,b} \lvert\mathcal{W}\rvert$	$\max_{a\neq 0,b} \lvert\mathcal{W}\rvert$
一轮影子	32768	32768
一轮完整核心	9306	1516
22 轮完整核心	18722	1494

$P_R = \sum m^2/2^{32}$，不是最大 DP。下表中 b 只遍历 23 个指定非零输出掩码，a 遍历全部输入掩码；$C = \mathcal{W}/65536$，概率偏差为 $\mathcal{W}/131072$。不含初始化和提取。

此前修正后概览项	数值
一轮 $-\log_2$ DP	5.9420
一轮最坏输入差分	5005
一轮方向 1 最大概率	32/65536
一轮到 22 轮核心像	$3501 \to 139$
全局 DP 整数分子（分母 65536）	$1066 \to 2472$
完整映射 / 方向 1 导数次数	16/15

代入 $y = \Phi(x+\Delta)+\Phi(x)$，再对 x 平均；对每个输出掩码，将自相关展开为归一化 Walsh 系数平方的 Fourier 反演，便得到前述等式。特别地，

$$\sum_a E(a) = 1, \qquad E(0) = 2^{-2n} \sum_y |\Phi^{-1}(y)|^2.$$

这里平均包含 $\Delta = 0$。若只平均非零差分，结果应为 $(2^n E(0) - 1)/(2^n - 1)$。这是碰撞概率的关系；仅有像的点数并不能确定实际分布的 Shannon 熵或最小熵。

III-E3 一致四位数据审计.

旧当前寄存器解释器及控制不正确的“no-key”标记不混入此表。原四位最大 DP 及次数保留为表 VII的完整 DDT 存档；本表新增的 P_R 是碰撞概率，不是最大 DP。高次数与像收缩可以并存，均不直接预测全位宽安全。

III-E4 SEV-5D 与侧信道. SEV 保留为操作检查表，不是安全评分。源码没有秘密分支或查表不代表功耗 / 电磁泄漏与数据无关。掩码保护、目标平台计时和物理测量是单独任务 [21]。

IV. AI 设计引擎

引擎按规范生成候选，经 L1 筛查、L2 深入核查后记录评分并反馈。进化算子改变阶段顺序与旋转常数，

2025 Shanghai High School Science Award
仅用于2026上海市成绩中学科学奖公示

表 IX
实现检查问题，不赋统一安全分数

问题	所需证据
代数非线性	指定映射的实际次数论证
差分 / 线性	明确范围的分布与相关分析
扩散	指标定义、证明或完整计算
时间	目标平台与编译器检查
功耗 / 电磁	泄漏模型、防护及物理评估

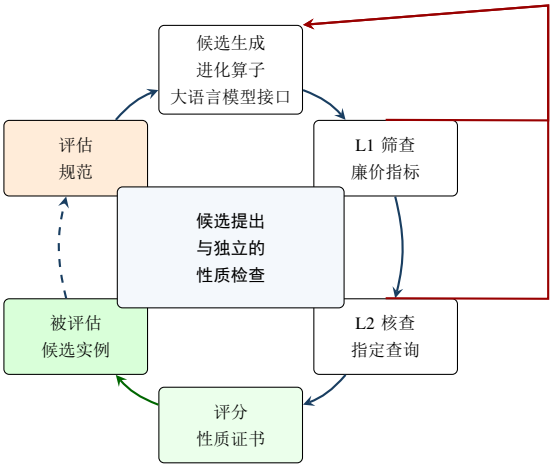


图 7. 候选生成与独立检查的流程示意。通用排序、条件筛选与性质脚本是不同入口；本图不表示每个候选均执行全部检查。

LLM 接口读取外部结构化提案，不自动调用模型。通用搜索、候选族筛选及独立性质脚本分开实现；排序分数、筛选决策和性质证书分别解释。

A. 架构

规范固定程序形式和查询。L1 对候选计算公开参数影响、活动诊断、小位宽神经区分深度、雪崩偏离、统计失败及操作量吞吐模型；L2 对入围者追加检查。通用 `engine.py` 采用有限扣分后排序，并非统一的硬性淘汰；`architect.py` 另按活动数和参数影响条件筛选帕累托前沿，再补入参考对照，故返回族也不等于全部满足验收条件。固定二次查询的秩证书由独立脚本重建。

候选生成和独立性质检查是两个组件。“被评估实例”并非“已证明安全实例”。

a) 证书中应保存的核查信息: 一个可复核记录应包含程序版本、位宽、常数、公开调度、输入状态域、固定方向或掩码，以及计算方法。二次导数证书还应保存 c_a、矩阵列、消元主元和秩。检查者须从程序重建矩阵，而不是仅信任文件中的秩标签。程序确为二次、有限 KAT 一致和矩阵消元回答不同问题；不能相互代替。候选提出、L1 筛查、L2 核查、评分和拒绝原因各自记录；这些记录不自动构成对全部攻击的验证。

表 X
历史校准与当前 v4 的区别；新版统计的标记项见第八节。

检查	归档 v3.1	原提交 v3	当前 v4-R1
公开注入覆盖	存在	A 后注入	顺序 B 注入
核心可逆	未建立	h 碰撞否定	固定密钥置换已证
神经/统计	历史观察	历史观察	第八节，保留标记
完整 PRG 证明	未提供	未提供	PRP 优势项仍未知

B. 校准：复现一个真实依赖错误

归档版本可作回归控制：公开注入被后续赋值覆盖。源码数据流解释比统计失败更具体，但不证明每个旧输出测试失败都由此造成。发展序列与适应度是在同一历史数据上校准，并非密码安全预测的留出检验。

a) 历史校准与新的搜索评估: 原 11 代评分及随机 / LLM 种子搜索记录作为历史工件归档，不计为第 VIII 节的 v4 实验结果。若要比较搜索效率，还需要未用于调参的候选集合、相同提案和核查预算、多组独立种子、无效候选数、停止条件、耗时与不确定性范围。这里列出所缺评估条件，不将这些新评估冒称为已经完成。

C. 性质脚本、历史诊断与规范驱动编译

极化秩、能量谱、2-SAT、单项式不交性及频谱检查由各自脚本实现，并非通用搜索的统一自动验收器。历史 v3 二次影子的端到端示范 `rank_certificate_demo.py` 在 64 位字宽对方向 $0x4$ 输出导数矩阵 C_i、秩 3 及精确 DP 为 1/8 的证书，经两条独立路径检查。同一历史对象的 32 个随机方向扫描未见秩低于 174；这不证明全局最优，且不否定已知低秩方向。

历史活动指标也须区别：通用搜索计数 AND 两输入差分同时为 1 的位，不是第 VI-D 节实际 AND 输出的非零字差分。旧 `exact-W4` 只枚举全部差分，每方向抽取一个状态，不是状态与差分的联合穷举；旧 `verifiers/empirical.py` 的一般 AND 更新还混用了未旋转状态与旋转差分，单门两执行反例即可否定其传播等价性[7]。因此依赖该路径的活动分数、16 常量变体和 LLM 零分提案仅作历史搜索记录，不作为精确性质

[7] $W = 4$，仅执行 $u \leftarrow u + (R_1 v \wedge R_2 w)$，输入 $(0,0,2,0)$、差分 $(0,1,0,0)$，真实输出差分为 $(0,1,0,0)$，旧传播器却给出 $(2,1,0,0)$。

2026 年 High School Science Award 仅用于 2026 届中学科学奖公示

证书或安全排序依据。当前 v4 的两执行、插桩和源码 miter 在第 VI 节独立报告，未复用这一传播器。

a) 历史筛选与本次研究候选: 历史评分不为 v4-R1 提供追溯接受。若将“实际输出正活动数”单列为验收条件，第 VI-D 节的单轮零活动见证即不满足；这与旧输入活动指标不是同一查询。输出剪切前的 NIST 与 Rabbit 标记及第八节的新结果分别保留，不能用其他得分抵消。本文保留 v4-R1 作为已证明可逆、仍有开放诊断与密码分析问题的研究实例；结构修复检查不等于部署批准。

V. 从反例到修复：Tempest v4-R1

A. 修复映射

Tempest v4-R1 是 AM-SEV 框架中的升级实例。论文主体仍然是把 AND–XOR–旋转程序、限定范围的结构查询和可独立检查的证据连接起来；v4 保留四个 64 位字、A–D 模块组织、每轮 26 个字级 AND 门以及原设计的大部分旋转参数。完整版本标识为 `TEMPEST-v4-R1-ANDRX256-CTR32`，下文简写为 v4。字节接口配置记为 `R1-P4`，与较早不含输出剪切的流区分；分组密码与 SHAKE 域标签仍为 R1。公开输出剪切是 v4-R1 字节接口的一部分（第 V-D 节）；不改变分组密码及其 KAT。SHAKE 域标签与分组轮常量保持不变；公开输出剪切本身不含常量项。预期研究目标是 128 位经典安全性，目前没有建立该安全级别。

v3 分析揭示了自乘预混合的非单射性、快照赋值与顺序赋值的语义差异，以及公开调度字与秘密密钥混淆的问题。v4 据此把非线性更新重组为可逆剪切，明确区分秘密轮密钥与公开轮常量，并将原自主状态迭代与非单射输出滤波改为 256 位带密钥置换的计数器输出。因此它是基于 v3 核心的结构修复，但输出接口确实发生了较大改变，不能把 v3 的完整安全分析和测试记录直接改名为 v4。

v3 的教训. 三个结构缺陷直接促成了本次修复。第一，旧字内自乘 $h(x) = x + R_{22}x + R_{26}x + (R_7x \wedge R_{19}x)$ 满足 $h(0) = h(\mathbf{1}) = 0$，核心轮不是单射，22 轮内像从 3501 个状态收缩到 139 个；把一轮用作置换，必须证明其单射性，而不能只做测试。第二，公开调度 $M = I + R_{19}$ 满足 $M^{64} = 0$，任一初值在 64 次更新内收敛到固定点；公开变量不是密钥材料，必须与秘密子密钥分离。第三，归档的 `legacy_v31` 先保存 S_0，注入公开字 p，再用 S_0 覆盖状态，抹去注入；赋值依赖必须直接检查。这三类缺陷都不能由输出统计定位，有利的测试结果也不能修复它们。

表 XI把每个缺陷、直接证据、修复动作与核查方式对应起来。它是第五至六节的索引：后文的技术细节均回指其中一行。

仅修改旋转参数不足以修复旧字内自乘：无论旋转距离如何，旧映射始终满足 $h(0) = h(\mathbf{1}) = 0$。本文保留这一反例和旧像压缩结论，作为设计决策的依据，而不将其误述为已经攻破 v3 实际可见输出。

B. 字操作与完整轮定义

默认字宽 $W = 64$，缩小模型仅使用 $W \in \{1, 2, 4, 8, 16, 32, 64\}$。$R_a$ 表示模 W 的循环左移；下式的加号均为异或，乘号均为逐位 AND。**所有赋值按顺序执行，右端读取最新值。**每个非线性剪切的右端均不读取被更新的目标字。把它们改成同时读取同一快照，会得到另一个算法。

A 模块依次执行：

$$
\begin{aligned}
u &\leftarrow u + R_5 v + R_{17} w + (R_5 v)(R_{25} z) + c_u,\\
v &\leftarrow v + R_{11} w + R_{23} z + (R_{11} w)(R_{29} u) + c_v,\\
w &\leftarrow w + R_{13} z + R_{31} u + (R_9 u)(R_{15} z) + c_w,\\
z &\leftarrow z + R_{17} u + R_7 v + (R_{27} v)(R_{21} w) + c_z,\\
u &\leftarrow u + (R_{23} z)(R_{53} w),\\
z &\leftarrow z + (R_5 u)(R_{25} v).
\end{aligned}
$$

四个固定常数 c_u, c_v, c_w, c_z 的十六进制表示依次为 `9e3779b97f4a7c15`、`3c6ef372fe94f82a`、`5a8279998f1bbd27`、`6ed9eba1f97f3b4c`。缩小模型取其低 W 位。相对 v3，A 中两个 AND 读端口调整，故其二次影子的读字秩公式也必须重推。

B 模块把四字秘密子密钥 q_i 与四字公开常量 C_i 异或进入状态。C 模块先对每个字执行 $L_{22,26} = I + R_{22} + R_{26}$，再执行表XII的 P、G1、G2，随后对每个字执行 $L_{16,14}$，最后执行 G3、G4。表中每个元组 (d, a, r, b, s) 代表

$$x_d \leftarrow x_d + (R_r x_a)(R_s x_b), \quad (x_0, x_1, x_2, x_3) = (u, v, w, z).$$

每组四个元组自左至右依次执行。P 替代旧非单射字内预混合；G3 也去除了目标字自读。D 模块依次更新：

2026 Sixth International Conference on Cryptography, Computer Science and Information Technology (CCSIT 2026) 计算机科学与信息技术国际会议（CCSIT 2026）录用论文公示

表 XI
v3 缺陷到 v4-R1 修复的映射；每行给出直接证据与可执行的核查。

v3 缺陷	直接证据	v4-R1 修复	核查
非单射自乘：$h(0) = h(\mathbf{1})$	像从 3501 收缩到 139；互补碰撞对	顺序目标排除剪切；可逆线性层	剪切引理与置换定理；逆算法 KAT
公开调度在 64 步内固定	调度递推与固定点	公开常量与秘密子密钥分离；SHAKE256 域分离	33 轮密钥扩展；常量周期检查
公开注入被快照覆盖	数据流依赖覆盖	顺序赋值；非线性目标字不自读	C/Python/Z3 源级等价；负证书
影子读字公式因端口改变而失效	$W = 4$、字 v、支撑 0x5：真秩 4，旧式给 6	重新推导单字秩公式	60 个单字方向与 24 个支撑模式核查
二次公式被外推到级联	仿射缺陷见证（第 VI 节）	明确影子边界，只对影子使用公式	反例保留，不因修复而删除

表 XII
v4-R1 C 模块全部非线性剪切。每组四个更新，顺序不能互换。

组	第 1 步	第 2 步	第 3 步	第 4 步
P	(0,1,7,2,19)	(1,2,7,3,19)	(2,3,7,0,19)	(3,0,7,1,19)
G1	(0,1,31,2,53)	(1,2,17,3,43)	(2,3,7,0,23)	(3,0,5,1,19)
G2	(0,1,17,3,43)	(1,2,7,0,23)	(2,3,5,1,19)	(3,0,31,2,53)
G3	(0,3,7,2,23)	(1,0,5,3,19)	(2,1,31,0,53)	(3,2,17,1,43)
G4	(0,1,5,2,19)	(1,2,31,3,53)	(2,3,17,0,53)	(3,0,7,1,23)

$$u \leftarrow u + R_3 v + R_9 w, \qquad v \leftarrow v + R_5 w + R_{11} z,$$
$$w \leftarrow w + R_9 z + R_{13} u, \qquad z \leftarrow z + R_{11} u + R_{17} v.$$

上式每行从左向右，再到下一行。一轮共 42 个字级赋值：A 六步、B 四步、C 的线性更新八步和非线性更新二十步、D 四步。AND 门数为 A 的六个加 C 的二十个。参考实现完整给出正轮与逆轮。生成器的字节接口另加四个公开的输出剪切赋值（第 V-D 节）；它们在分组密码之外，不改变 42 个赋值的轮计数和分组 KAT。

C. 常量生成、密钥扩展与分组加密

记 $\mathcal{R}_{k,c}$ 为上述完整轮，其中 B 模块使用子密钥 k 和公开向量 c。公开常量采用可复算的离线规则：公共 ASCII 前缀

```
AM-SEV/TEMPEST-v4-R1-ANDRX256-CTR32/
```

分别拼接 `data-round`、`key-round`、`key-domain`，不添加空格或换行。对三个标签分别取 SHAKE256 的前 32×32、33×32、1×32 字节，依次按每 32 字节分组，每组按大端序解析为四个 64 位字。无筛选、重试或按结果替换常量的步骤。运行时核心不调用 SHAKE；它只用于公开常量的离线固定。常量文件和脚本随论文提供。域分离区分各类常量的用途，不提供秘密熵；可复算来源也不能单独排除陷门或代替完整 PRP 分析。

数据域向量记作 $C_0, \ldots, C_{31}$，密钥域记作 $J_0, \ldots, J_{32}$，初始密钥域常量记作 D_K。对 256 位主密钥 K，定义

$$q_0 = K + D_K, \qquad q_{i+1} = \mathcal{R}_{0,J_i}(q_i), \quad 0 \le i \le 32.$$

共保存 $q_0, \ldots, q_{33}$ 这 34 个四字子密钥。分组加密为

$$s_0 = X + q_0,$$
$$s_{i+1} = \mathcal{R}_{q_{i+1},C_i}(s_i), \qquad 0 \le i < 32,$$
$$E_K(X) = s_{32} + q_{33}.$$

复用原核心作密钥扩展减少了规范复杂度，但也产生必须分析的相关轮密钥结构，不能据此假设轮密钥相互独立。

D. 完整逆算法与字节接口

对密文 Y，先异或去除 q_{33}，再按 $31, 30, \ldots, 0$ 的顺序执行逆轮，最后去除 q_0。每个逆轮依次：逆序撤销 D；逆序撤销 G4、G3；施加 $L_{16,14}^{-1}$；逆序撤销 G2、G1、P；施加 $L_{22,26}^{-1}$；撤销 B；逆序撤销 A。剪切本身是对合，线性逆的公式在下节证明。Python 检查器另用二进制矩阵求逆，避免两个实现共享同一种逆公式而掩盖错误。

2026 IACR Tsinghua Science Award 公开学术论文公示

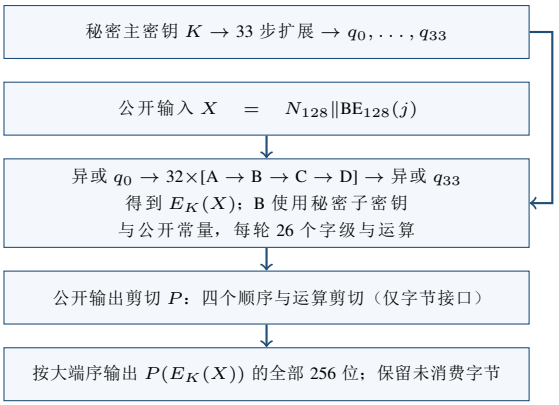


图 8. R1-P4 字节接口与完整轮结构。秘密子密钥直接供给密钥运算，不是公开输入的一部分。分组 KAT 与 RTL 针对 E_K；统计电池针对 $P \circ E_K$。每块执行 32 轮，公开输出剪切另计。

公开输出剪切. 分组密码之后，字节接口对每个 256 位分组施加公开置换 P：

$$\begin{aligned} u &\leftarrow u \oplus (R_5 v \wedge R_{19} w), \\ v &\leftarrow v \oplus (R_{11} w \wedge R_{23} z), \\ w &\leftarrow w \oplus (R_{13} z \wedge R_{29} u), \\ z &\leftarrow z \oplus (R_{17} u \wedge R_{31} v). \end{aligned}$$

四个赋值按顺序执行，右端不读取目标字；P^{-1} 按相反顺序撤销。该层不含秘密，不属于轮函数、分组 KAT 或 RTL 核心。发生器输出

$$P(E_K(N \| \mathrm{BE}_{128}(j))), \qquad j = 0, 1, 2, \ldots$$

由于 P 是公开双射，分组置换性质与条件界中的 PRP 项不变。公开输出剪切是 v4-R1 字节接口的一部分；分组密码及其 KAT 不变。上面的逆算法只撤销 E_K，不撤销 P；若需要分组值，应先对发出的分组施加 P^{-1}。四个输出字全部按大端序发送，未消费字节保留在缓冲区。因此连续请求 a, b 字节与一次请求 $a+b$ 字节完全一致，不丢弃半个输出块。每次初始化最多输出 2^{32} 字节，即 2^{27} 个分组。长度非法或超过预算时返回错误，且不推进状态。同一密钥下 nonce 必须唯一；本接口不要求 nonce 保密或不可预测。4GiB 是单次初始化的输出预算，不替代跨会话的 nonce 唯一性要求。本接口没有熵源采集、重播种、认证或泄露后恢复机制。**发布范围。** v4-R1 代码树提供 C 参考实现、独立 Python 模型、标量与 AVX-512 后端、统计与性能测试工具，以及 C++/GSL、Rust、Go、NumPy/PyPI、OpenSSL 3 provider、wolfSSL 回调和 Homebrew 绑定。各绑定通过兼容层把历史生成器 API 转到 v4 核心；它们属于集成工件，不构成额外安全证据，其测试与统计电池记录分开保存。

a) 字节流参考 KAT: 取 64 位字 $K = (1, 2, 3, 4)$、$N = (5, 6)$，均按大端编码，计数器从零开始。前 32 个输出字节为

```
89b4ccfa3f02997e80aceb8b0aa77592
801ba282f3aeaf6ab23a850e11ac902d。
```

上述是输出字节，不是摘要。前 125000 字节的 SHA-256 为

```
3a49ae552c59bc6d88d24d9ad5e36fc6
5521a90d70c95440c0e3c58cf97906f1。
```

VI. 安全性分析：已证明、已穷举、已抽样与仍开放

A. 安全实验与结论层次

对手知道全部算法和公开 nonce。秘密主密钥均匀抽取；区分实验比较真实输出与具有同样长度及公开输入规则的理想随机比特接口。同一密钥下进入分组置换的完整 256 位输入不得重复。恢复实验另问对手能否得到原先抽取的密钥；仅找到一个符合少量观察的候选，不自动等于恢复原密钥。

本文分开报告四类结论：对所有输入成立的结构定理、缩小模型的完整计数、有限抽样观察、尚未完成的攻击分析。逆算法与源码等价性属于结构检查，统计套件属于有限输出观察。把这些结果合成一个分数，不能得到 128 位安全结论。下文的条件归约把最关键的分组置换假设明确保留。

本节 $\mathrm{Adv}_{\mathrm{out}}$ 和 $\mathrm{Adv}_{\mathrm{PRP}}$ 统一采用接受概率差约定：

$$\begin{aligned} \mathrm{Adv}_{\mathrm{out}}(A) = \big| &\Pr[A(\mathrm{real}) = 1] \\ &- \Pr[A(\mathrm{ideal}) = 1] \big|. \end{aligned}$$

历史 v3 实验的猜测优势是该差值的一半，不能混用两种约定。

B. 可逆性、像与密钥扩展

先证明每个基本操作可逆，再记录其对像、零差分与子密钥的推论。

引理 VI.1 (不读取目标字的剪切；v4)**.** 若 f 不读取目标字 x_d，则仅执行 $x_d \leftarrow x_d + f(x_{\neq d})$ 的映射是对合。

证明. 其他字在两次执行间不变，所以两次计算的 f 相同。目标字变为 $x_d + f + f = x_d$。论证允许 f 非线性，

2026 Shanghai High School Science Award 仅用于公众号评审论文公示

也允许包含公开常数，但不表示不同剪切可以交换顺序。顺序复合必须逆序撤销。 □

引理 VI.2 (三项线性旋转的逆；v4)**.** 对 $W = 2^m$ 和任意旋转距离 a, b，$L = I + R_a + R_b$ 可逆，且

$$L^{-1} = \prod_{t=0}^{m-1} (I + R_{2^t a} + R_{2^t b}).$$

$W = 1$ 时空积为 I。

证明. 令 $A = R_a + R_b$。旋转可交换，特征二下 $A^{2^t} = R_{2^t a} + R_{2^t b}$，所以 $A^W = I + I = 0$。由

$$(I + A) \prod_{t=0}^{m-1} (I + A^{2^t}) = I + A^W = I$$

得到逆式。即使缩小字宽使旋转距离重合，结论仍成立。 □

定理 VI.1 (固定密钥下的置换；v4)**.** 对每个允许字宽及固定子密钥、公开常量，v4 完整轮都是置换；固定主密钥下，带前后白化的完整分组加密也是置换。

证明. 逐项检查完整操作表，A、C 的每个非线性更新和 D 的每个线性剪切都不在右端读取目标字，满足剪切引理。B 是异或平移。C 的两个线性层满足线性逆引理。可逆映射的顺序复合、轮迭代和前后白化均可逆。证明不需要统计测试，也不需要假设密钥随机。 □

该定理精确修复了 v3 固定密钥核心的像压缩，但不能推出差分、线性或恢复攻击安全。例如恒等映射也是置换。公开输出剪切 P 是双射，与 E_K 复合后仍保持输出分组的置换性质。分组 KAT 与影子/DDT/次数分析仍针对 E_K；发生器字节流是 $P(E_K(\cdot))$，统计电池测试的是该字节流。

a) 像、零输出差分与碰撞能量: 令 $n = 4W$，F 为任一固定密钥、包含对应白化的轮前缀。对全空间均匀 X，有

$$|\operatorname{Im} F| = 2^n, \qquad \Pr[F(X) = y] = 2^{-n},$$
$$\sum_y \Pr[F(X) = y]^2 = 2^{-n}.$$

任意 $a \neq 0$ 均满足 $\mathrm{DP}_F(a, 0) = 0$，否则两个不同输入有相同输出，与单射矛盾。后接置换不能把两个不同状态合并，所以旧核心的合并机制在此层面不存在。但真实 nonce 与计数器序列只是结构化输入子集，不能从全空间均匀性直接推出该子集输出的计算伪随机性。

b) 子密钥边缘分布及局限:

命题 VI.1 (子密钥边缘分布；v4)**.** 对每个固定下标 i，$K \mapsto q_i$ 是置换。主密钥均匀时，每个子密钥单独看也是均匀分布。

证明. 初始域平移可逆；其后每个密钥域轮由前述定理可逆；复合保留双射性和均匀分布。 □

34 个子密钥的联合信息仍只由 256 位秘密决定，因此高度相关。边缘均匀不等于独立，不排除相关密钥攻击，也不能证明完整分组置换没有等价密钥。尤其不能仅凭 q_0 不同就断言完整 E_K 不同。对一个固定输入，逐一翻转主密钥 256 个位，输出均发生变化，平均汉明距离 128.15625，范围 102–154；这只是局部影响性检查，不是弱密钥类的穷举。

C. 二次影子：修正的读字秩及其边界

影子保留两个修订读端口，单独定义如下：若 A 第 g 步为 $x_{d_g} \leftarrow x_{d_g} + f_g(x)$，$1 \le g \le 6$，其中 f_g 不含目标字旧值，则对 $0 \le d < 4$ 令

$$(\mathrm{Sh}_{v4}(x))_d = x_d + \sum_{g : d_g = d} f_g(x).$$

各增量均在同一输入 x 上计算；重复目标字累加全部增量，不能用后一次快照赋值覆盖前一次贡献。该映射至多二次；实际顺序 A 读取最新状态，一般已不是此二次映射。第三节的仿射导数公式仅直接用于该影子。

v4 修正。设差分只位于一个输入字，其支撑为 $P \subseteq \mathbb{Z}_W$，$t = |P|$。显式极化矩阵列消元给出

$$\operatorname{rank} B_\Delta = 3t - |P \cap (P + 2)|\, \mathbf{1}_{\{\text{输入字} \in \{v,z\}\}}.$$

证明. 输入字为 u 时，非零导数行分布在输出字 v, w, z 的 $P{+}29, P{+}9, P{+}5$ 位置，自由源字依次为 w, z, v。输入字为 w 时，分布在输出字 v, z, u 的 $P{+}11, P{+}21, P{+}53$ 位置，自由源字依次为 u, v, z。两种情况三组源字互异，每组旋转源坐标只出现一次，故三组共 $3t$ 行独立。输入字为 v 时，行族分别是输出 u 的 $P+5$ 位置（源字 z），及输出 z 的 $P{+}27, P{+}25$ 位置（源字 w, u）。后两组在 $(P{+}27) \cap (P{+}25)$ 处共用输出行，大小为 $|P \cap (P{+}2)|$；每个合并行仍具有不出现在其他行中的源坐标，因此不再发生额外行依赖，秩恰少这一重叠数。输入字为 z 时，对应输出 u 的 $P + 25, P + 23$（源字 v, w），及输出 w

2026 S. T. Yau High School Science Award 仅用于2026年成都市青少年科学实践大赛公开展示

的 $P+15$（源字 u），同理成立。所有位置均模 W。影子的线性项只贡献仿射常数，不进入 B_Δ。 □

该式仅对单字差分成立。已检查四位字宽全部 60 个非零单字方向，以及 8、16、32、64 位字宽各 24 个支撑模式。旧式仅对 z 扣除重叠，不能照搬：$W=4$、输入字 v、支撑 0x5 时，实际秩为 4，旧式误给 6。这一反例说明改变端口后必须重算度量。

五种字宽的全部单比特方向影子秩均为 3。四位字宽对全部 65535 个非零方向穷举，最小秩也是 3，但不能据此证明 64 位全方向最小值。64 位固定方向 $\Delta=e_{u,0}$ 有可重建的秩 3 证书，故该影子导数在其仿射像上的点概率恰为 2^{-3}。64 位全一输出掩码的极化秩为 256，因此固定此输出掩码、遍历输入掩码时最大相关幅度为 2^{-128}，概率偏差为 2^{-129}；二者不能混写，结论也不适用于完整轮。

v4-R1 的 A 影子恰好构成完整四字交互图，因此第三节的满秩命题直接适用：在 $W=64$ 时，全字奇偶掩码的极化秩为 256，归一化 Walsh 幅值为 2^{-128}。该数值只描述该影子与该输出掩码；顺序 A 模块、32 轮密钥置换以及旋转候选的完整安全排序均不在其范围内。

a) 二次公式不能越过顺序级联: $D_aQ(x)=B_ax+c_a$ 要求 Q 至多二次。顺序赋值把新值代回后可以提高次数。在四位完整一轮映射中，取 $a=1,x=2,y=4$，有

$$D_aF(x+y)+D_aF(x)+D_aF(y)+D_aF(0)=37238\neq 0.$$

整数表示按字打包的 16 位向量。这直接否定了把完整轮导数当成仿射映射的做法。框架的残余支撑不等式在其假设下仍是某个可达点概率的下界，不能反过来作为差分安全所需的概率上界。

D. 差分证据：完整计数、抽样与活动

差分证据按三种分辨率报告：缩小模型的完整计数、全宽抽样与门活动诊断。下述计数与谱均针对 E_K；生成器的公开输出剪切 P 在 E_K 之后施加，不属于这些查询。第八节测试的是复合流 $P(E_K(\cdot))$。固定缩小密钥 $(1,2,3,4)$，所有常量取低四位，对 1、2、4、6、8、12、16、22、32 轮逐一枚举 65536 个输入和 65535 个非零输入差分的全部 DDT 行。差分始终包含完整 16 位输出。每个映射的像均为 65536，非零输入差分达到零输出的次数均为零。表XIII分开列出方向 1 的最大计数和遍历全部非零方向的全局最大计数。一轮方向 1 的计数为 12，但全局最大计数为 276。两轮全局最大计数降到 18，随后在 18 与 20 之间波动。即使所有轮都是置换，也不能主张增加轮数必使最大 DP 单调下降。该实验是对完整缩小映射的精确判断，不是 64 位密码全局最优差分的估计。

表 XIII
v4-R1 分组置换 E_K 的完整四位模型（不含输出 P）。DP 与 Walsh 整数的分母均为 65536；Walsh 只覆盖 23 个输出掩码。

轮数	像	次数	方向 1	全局 DP	Walsh
1	65536	15	12	276	1332
2	65536	15	16	18	1260
4	65536	15	10	20	1336
6	65536	15	12	18	1404
8	65536	15	12	20	1288
12	65536	15	10	20	1380
16	65536	15	10	18	1240
22	65536	15	12	20	1288
32	65536	15	12	18	1328

a) 全宽抽样: 在计算结果前固定公开 SHAKE256 输入文件，包含 2^{24} 个 256 位点。固定方向 $e_{u,0}$，分别计算 1、2、22、32 轮的完整 256 位输出差分，排序时包含四个输出字。四组都没有重复差分，也没有零差分，观察最大频率均为 $1/2^{24}$。

若假设独立同分布抽样，对某个真实概率为 p 的输出类别，其样本计数满足

$$\Pr[N_b\le 1]=(1-p)^N+Np(1-p)^{N-1}.$$

对真实最大概率所对应的类别应用此式，可由“未见重复”事件构造条件置信解释，无须遍历所有可能类别再作联合界。但这里的输入是确定性公开测试文件，没有认证为 IID，论文将原始观察与假设性的抽样解释分开。无论哪种解释，都不能把未见重复写成确定的全局 DP $\le 2^{-24}$。

b) 门活动的负面发现: 对 2000 个预先规定的四位状态，各自比较全部 65535 个非零差分，计数一轮 26 个实际 AND 输出中非零的字差分。各状态最小值的总体最小为 0、最大为 15、众数为 8。零活动见证为按低字优先打包的十进制状态 12591、差分 387。插桩执行在全部 65536 个输入上与主 C 轮输出一致。

因此不能声称这个指标始终存在正下界。本文保留零见证，不通过改指标或丢弃输入使它“通过”。继续追踪相同输入对 32 轮的活动轨迹，并对

2026 Shu Yu Huishan Science Award 参赛作品 仅用于2026年舒宇辉山学术奖公示

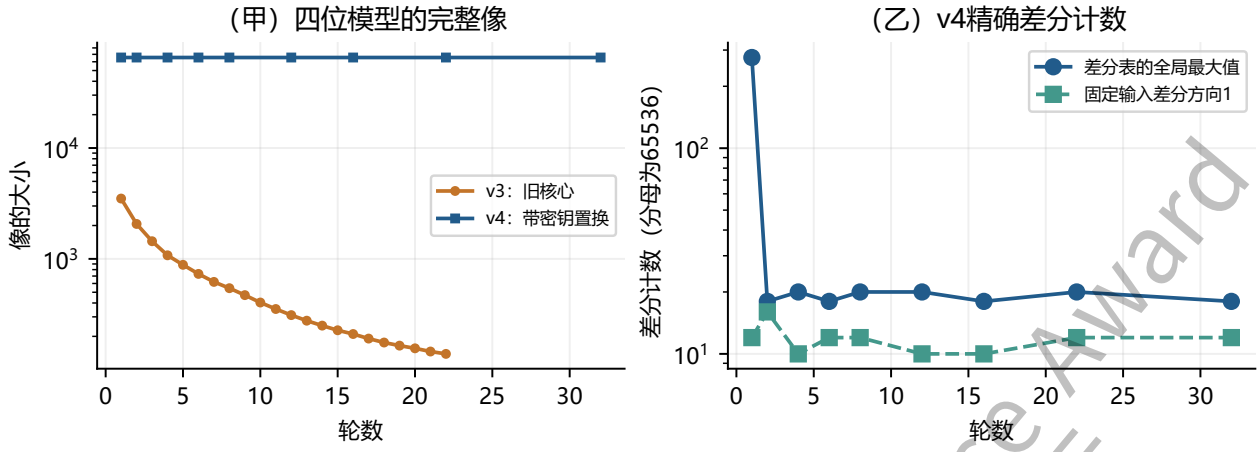


图 9. 完整缩小模型比较。左：v3 内部像收缩，v4 保持满像。右：固定方向与全局 DDT 最大值明显不同，增加轮数不保证单调改善。图中对象及全空间输入分布不等于实际输出接口。

$(1,2),(3,4),\ldots,(31,32)$ 这 16 组连续轮，穷举从全部 16 位输入到 52 个 AND 输出字的联合签名。每组联合签名均无碰撞，而单轮签名确有碰撞。这说明所检查轮对内不存在两轮都零活动的不同输入对，但它仍只是该缩小模型的有限事实，不是全位宽路径概率上界。

后续 64 位检查使用既有冻结全位宽文件前 2000 个点，每点搜索 260 个方向，包括全部 256 个单比特及四个单字全一差分。所选方向最小值为 16–21，插桩与主 C 的 2000 个基点输出均一致。由于只扫描方向子集，这些值是每个状态真实最小值的上界；观察为正不能证明全局活动下界。

c) 路径编码与共享变量约束. 对一位 AND，第一条执行的操作数为 x, y，输入差分为 α, β，精确输出差分约束为

$$\gamma = \alpha y + \beta x + \alpha\beta.$$

忠实 SAT 模型须保留两条执行中的实际值、共享线、旋转和顺序依赖，不能仅编码某处是否非零。两个门若共享同一随机事件，各自概率 $1/2$，联合概率可能仍为 $1/2$，不能相乘成 $1/4$。旧八位支撑模型的 25、58、96、130、166 保留在项目归档中，属于 v3 模型记录，没有转填为 v4 结果。

新的联合签名检查针对实际执行，避免把支撑代价误解成概率指数。完整多轮差分簇的概率上界仍未解决，本文不根据每轮 26 个 AND 宣称 2^{-cR} 安全界。

新的八位字宽精确双执行 SMT 覆盖一至五轮，查询是否存在不同状态，使指定轮内全部实际 AND 输出相同。一轮返回 SAT：两输入为 $(197,46,112,11)$ 与 $(189,111,88,11)$，独立 Python 复核 26 个 AND 字均相同，但最终状态差分为 $(65,20,136,34)$。二至五轮各 25 秒后返回 UNKNOWN，不能据此给出正活动下界。该实验覆盖原来的轮数范围，保留真实操作数约束，但与历史支撑最小化是不同查询，结果不能混在同一概率表中。

E. 线性谱与代数次数

本节谱与次数界均针对 E_K；公开输出剪切 P 不在这些查询范围内。每个缩小轮数对 23 个固定非零输出掩码，遍历全部 65536 个输入掩码计算精确 Walsh 谱，共 207 组完整谱。表XIII列出所选输出掩码集合内的最大绝对整数和，未声称覆盖全部 65535 个输出掩码。固定密钥置换的输出均匀性还直接保证：输入掩码为零、输出掩码非零时相关为零。

64 位实验在 65536 个固定输入上扫描 4096 对预先固定的非零输入/输出掩码。1、2、22、32 轮的最大绝对样本相关依次为 0.01699829、0.01449585、0.01391602、0.01226807；概率偏差是相关的一半。若输入为 IID，对预先确定的 M 个掩码联合使用 Hoeffding 界，得到

$$\Pr[\exists j : |\widehat{C}_j - C_j| > \epsilon] \le 2M\exp(-N\epsilon^2/2).$$

当 $M = 4096, N = 65536, \alpha = .05$ 时，误差半径约 0.01914，大于观察到的最大值。因此样本尚不能分辨更小的真实相关，也不能覆盖未扫描掩码。小数值本身不是全局线性安全界。

2026 Sixth Yau Hing Chi Science Award 决赛于 2026 年成绩中学科学奖公示

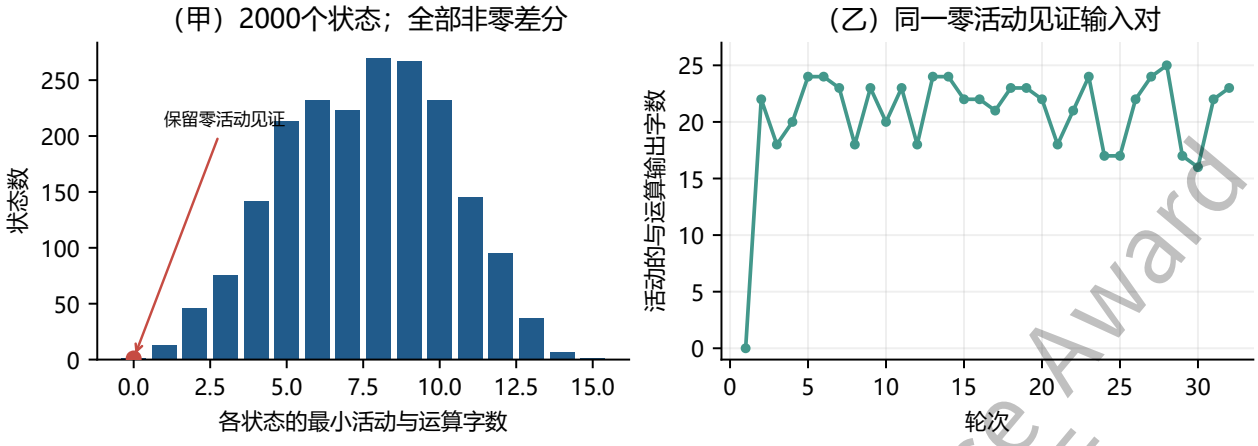


图 10. v4-R1 分组核心的门活动诊断（不含输出置换 P）。左：2000 个状态各自扫描全部差分后的最小活动分布。右：首轮零活动的同一输入对在第二轮有 22 个活动字差分。每点是实际执行计数，不是概率指数。

a) 次数、积分与代数恢复: 精确 Möbius 变换显示，四位模型九个轮数的最大坐标次数均为 15，包括一轮。这达到 16 位置换的 $n-1$ 次数上限，但不代表每个坐标都达到该次数，更不推出完整密钥代数恢复至少需要 2^{256} 工作量。全位宽电路可以按异或取最大、AND 取次数和并截断到输入变量数，传播次数上界；上界大尤其不能替代实达次数证明。

置换在整个输入域上具有非零线性输出组合平衡、全域输出异或固定等平凡积分性质。这不排除低维积分、除法性质区分器、立方关系、稀疏零化子或涉及密钥的低次方程。上述攻击需要专门搜索；次数饱和不能改名为代数安全。

F. 条件性输出界

定理 VI.2 (经典条件输出界；v4 应用)**.** 在均匀秘密密钥下，若总共查询至多 q 个互异的 256 位输入，则可从输出区分器 A 构造 PRP 区分器 B，满足

$$\mathrm{Adv}_{\mathrm{out}}(A) \le \mathrm{Adv}_{\mathrm{PRP}}(B;E) + \frac{q(q-1)}{2^{257}}.$$

归约开销是计数器接口模拟，本文不对右端 PRP 优势给出数值上界。

证明. 先把 E_K 替换为 256 位域上的均匀随机置换。用其预言机模拟计数器接口，就得到 PRP 混合实验，接受概率改变至多 $\mathrm{Adv}_{\mathrm{PRP}}(B;E)$。互异输入下，随机置换的输出是无放回抽样。将它与独立均匀 256 位串耦合，直到独立串首次重复前两者完全相同。任意一对串碰撞的联合上界为 $\binom{q}{2}/2^{256}$，故两类转录的统计距离至多该值。公开置换 P 保持均匀分布；施加 P、截断末块或将字节拆成多次 API 调用均不增加上述距离。用三角不等式合并即得。只要完整输入不重复，证明也允许对手选择不同 nonce。 □

单个 4GiB 会话 $q \le 2^{27}$，切换项小于 2^{-203}。跨会话必须累计总 q，不能每次重置计数器就重新计算安全预算。重复 nonce 会重放完全相同输出，违反定理前提；完整计数输入唯一是 CTR 的标准要求[8]。此处是标准构造级证明，不是新的归约技术，也不是证明原创 AND–RX 置换具有小 PRP 优势。该定理不表示 TEMPEST 获得 NIST 批准，亦不表示它实现了 CTR_DRBG。

G. 实现语义与证书

C 与独立 Python 对 1、2、4、8、16、32、64 位字宽共 11200 组正逆轮、200 组不同字宽/轮数的分组测试一致。三个 1024 字节向量检查完整字节流、分块调用、原地加解密、错误原子性与清理。符号位向量 miter 把 C 的 46 个正向赋值语句与独立 DSL 的 42 个操作对比，输入、子密钥和公开常量均任意。Z3 在 4、8、16、32、64 位下返回 UNSAT。这验证无符号定宽源码表达式，不是编译器或机器码证明。miter 与正逆轮用例针对 E_K；输出剪切 P 由字节流 KAT 与完整样本比对覆盖。

秩证书检查器重新生成矩阵列和仿射常数，不信任证书自报秩。十二类负面证书改变矩阵、方向、常数、字宽或对象范围，均被拒绝，用来检验检查器是否守住

[8]NIST SP 800-38A：https://csrc.nist.gov/pubs/sp/800/38/a/final。

2026 年 Tiyau High School Science 仅用于 2026 江城桐中学科学奖论文公示 Award

查询边界，包括不能把影子证书用于完整轮。大端序和四字差分完整打包同样属于语义检查；漏掉高位可以制造虚假碰撞。

四组真实密钥恢复位向量模型包含全部 33 轮密钥扩展和两对已知完整分组，参数为 $(W,R) = (4,1),(4,32),(8,2),(64,32)$。四组均在 25 秒预算后返回 UNKNOWN。尤其四位实例已经由独立的 65536 密钥完整枚举恢复，说明即使极小实例的求解超时也不是困难性证书，只反映特定编码、求解器和预算。

H. 开放攻击面

以下攻击类尚未被上述结果解决；这里记录每一类目前已有的证据与缺口。

a) 旋转关系、滑动与公开调度: 去掉常量时，AND、异或与公共旋转可交换。v4 的 32 个数据域和 33 个密钥域常量向量各自无重复，且没有一个向量具有非平凡公共字旋转周期。这只排除了向量字面相等与自旋转不变，不能排除跨轮旋转关系、RX 路径或密钥补偿。

v3 在至多 64 次更新后固定的公开递推字已删除；v4 没有演化的 Weyl 字。每个输出块都从新计数器输入开始执行相同规范的 32 轮置换。滑动分析仍须考虑轮函数与相关子密钥，不能仅凭常量不同就宣布不存在滑动攻击。域分离避免直接使用同一常量序列，但不是轮函数独立或子密钥独立的定理。

b) 恢复实验、等价密钥与状态泄露: 在四位 32 轮模型中，对全部 65536 个缩小主密钥穷举已知完整分组对。选定测试密钥的一对分组留一个候选，两对也留同一个候选。这是玩具密钥空间的完整枚举恢复，用来检查密钥和接口方程；它不提供 256 位密钥的攻击下界，也未遍历所有可能密钥与等价类。

因公开 P 可逆，输出完整分组后，观察者可撤销 P 并获得 $(N\|j, E_K(N\|j))$ 这样的已知输入/输出对。旧滤波器多对一逆像的讨论不再适用，普通分组密码分析直接相关；不能以“内部状态不可见”作为额外安全论据。密钥扩展可逆，任一个完整 q_i 泄露即可逆推 K，因此保存的子密钥需要保护。本构造没有宣称前向保密、回溯抵抗、泄露后预测抵抗、相关密钥或 nonce 误用安全。

c) 穷举与时间—内存—数据权衡: 256 位密钥说明枚举空间，而不是攻击工作量下界。若已知分组对足以区分候选，完整枚举给出约 2^{256} 次密钥试探的通用上界，每次还需计入密钥扩展与加密。量子搜索约 2^{128} 次预言机计算同样是通用算法上界，不是该原创原语已经达到的强度 [22]；本文目标和归约均为经典模型。

原稿“内存 $M \le 2^{40}$ 时 $T \ge 2^{216}$”不作为新实例保证。时间—内存—数据权衡依赖预计算预算、目标群体、表项大小、数据访问方式和被求逆的函数 [23]。v4 的计数器与 nonce 公开，子密钥均由同一主密钥决定，不能把旧自主隐藏状态模型直接代入 256 位。对单一固定输入，存储 2^{40} 个不同候选密钥的表覆盖均匀目标密钥的概率为 2^{-216}；这一覆盖概率不是时间下界。本文没有建立完整位宽的权衡下界。

d) 差分线性、转录与困难问题论据: 差分线性攻击的中间差分与线性事件共享同一次执行，缺少依赖论证时不能相乘其边缘概率。窗口或自动搜索方法须保留中间状态、实际 AND 操作数及异或重汇合。新源码 miter 验证操作语义，双执行 SAT 验证指定零活动查询；二者都没有计算差分线性簇或排除全部窗口攻击。

H 系数方法要求真实/理想转录概率比及坏事件界。不能假定原创密码的“好”转录天然等于理想。前述定理 VI.2明确完成标准构造混合，并保留未界定的 PRP 项，从而给出有效的条件论证，也指出原语层仍缺什么。

把 $E_K(X)$ 写作 $AX + N_K(X)$，不会使 $N_K(X)$ 成为独立 Bernoulli 噪声。对确定、密钥相关残差提出 LPN 式假设，仍是在额外假设原创密码本身，不能称为归约到标准 LPN。类似地，高坐标次数、单门输入数有限与轮数较多，都不足以排除分组求解攻击（GAS）。任何适用或排除论证都须从可见的 $(N\|j, E_K(N\|j))$ 关系出发，纳入密钥扩展并量化工作量。因此不再对 v4 宣称 GAS“不构成威胁”。

I. 安全性总体状态

已证明的修复是固定密钥可逆性，条件归约明确了仍需证明或充分分析的 PRP 假设。缩小全局 DDT、指定掩码精确谱与源码 miter 比沿用旧测试更直接，但完整位宽差分/线性簇、代数与相关密钥恢复、弱密钥类、高阶及差分线性攻击仍未解决。在 v4-R1 下，NIST 严格 3σ 比例门槛与 Rabbit 电池通过；单行 $p < 0.01$ 的离群项与有利结果一并保留。表 XIV按攻击面汇总现有证据；空白不表示“安全”，而表示“尚未分析”。当前得到的是规范更完整、分析更充分的研究候选，尚不是已证实 128 位安全的密码。

2026 Si Yuan High School Science Award
仅用于2026年度科学奖公示

表 XIV
攻击面与证据状态；每行只引用其证据等级能够支持的结论。

攻击面	现有证据	状态
固定方向差分	二次影子仿射导数定理；读字秩公式；$W = 4$ 全部 60 个单字方向，以及更大字宽各 24 个支撑模式	已证明（影子）/已穷举（$W = 4$）
全局差分	$W = 4$ 全部 65535 个方向的完整 DDT；2^{24} 全宽抽样	已穷举（16 位）/仅抽样（全宽）
线性	207 组精确 Walsh 谱（23 个掩码）；4096 个全宽掩码对	已穷举（选定掩码）/仅抽样（全宽）
代数	$W = 4$ 次数 15；置换一般上界 $4W - 1$（全宽至多 255）	已穷举（$W = 4$）/仅有上界
相关密钥	子密钥边缘均匀；联合分布高度依赖	未解决
滑动与旋转	公开常量无平凡公共周期；无证明	开放
实现与侧信道	无查表、无秘密索引；无功耗/电磁实测	功能一致/侧信道未验证
完整 PRP	条件性归约 $\mathrm{Adv}_{\mathrm{out}} \le \mathrm{Adv}_{\mathrm{PRP}} + q(q-1)/2^{257}$	开放（保留 PRP 项）

表 XV
ECP5-25K CABGA256；新 v4 串行分组原型。

项目	结果
RTL 功能向量	12/12；3 组密钥
综合 LUT4	12900
布线后 COMB	14832/24288
触发器	1803
RAMW	320
目标/达到频率	50 / 26.63 MHz
50 MHz 时序	未满足
实体上板	未测量

表 XVI
v4-R1 完整分组数据路（E_K，不含输出 P）；HX8K 或 ECP5-85K；未约束 IO 时序，无上板实测。

结构	周期/块	MHz	估计 Gbit/s
HX8K，64 位接口	65	–	–
HX8K，128 位接口	65	–	–
ECP5，完整轮迭代	65	28.02	0.11035
ECP5，单字微步骤	1377	85.32	0.01586
ECP5，六段寄存	225	61.13	0.06955

VII. 硬件实现案例

本轮重新生成 v4 实际轮函数和完整密钥扩展 RTL，没有复用 v3 资源数。组合轮由顺序控制器复用：装载密钥后运行 33 个密钥域轮并保存 34 个子密钥；分组加密运行 32 个数据轮并施加前后白化。低引脚数串行外壳装入 256 位密钥、256 位输入并移出 256 位输出。该外壳是分组密码原型；nonce 管理、4GiB 预算和字节缓存属于软件接口，不能宣称已在这一 RTL 中实现。RTL 实现的是 E_K；公开输出剪切 P 属于输出阶段，不在本次 RTL 原型及其 KAT 中。

Icarus 对三组密钥共 12 个完整分组加密进行仿真，均与独立 Python 结果一致；源文件明确给出复位、忙/就绪和单周期有效信号。Yosys 对同一设计作 ECP5 映射，nextpnr 进行布局布线。表XV记录实际工件与时序结果。没有将综合估计改称上板实测。v3 的流水线与检查器教训保留在项目归档中，但两代的存储量、轮数和成本不同。未流水化的一轮组合路径较长，32 轮数据计算需 32 个时钟，时钟频率受剪切顺序路径限制。串行输入/输出另有明显接口开销。$256f/32$ 只能表示不计串口的理论数据通路速率，不能称为应用实测吞吐。若按模块增加寄存器，须重新检查延迟、控制和端到端等价。

控制器复位不会擦除已保存的子密钥 RAM。生成配置未绑定具体开发板引脚，属于研究工件，不是已验证上板设计或满足 50MHz 的位流。接口与密钥擦除要求独立于功能仿真。

A. 按原文架构类别补充的完整轮实现

另以相同 v4-R1 规范实现 64/128 位输出接口、逐字微步骤与六段寄存数据路，全部保留密钥扩展、32 个数据轮和 256 位输出。每种结构均以三组密钥、12 个分组核对软件模型，并检查完整块周期。ECP5 补测使用 85K 器件，表XV的较早原型使用 25K 器件，两者分别记录。新架构的密钥读取与寄存分段引入不同周期开销，不能沿用旧 32 周期公式。

每个完整块的周期数为表中所列 I，内部数据路估计为 $256f/I$，串行输入和板级接口另计。原文 v3 架构也按单/双接口、k2 截断、半字复用和寄存分段复测；k2 是不同旧算法，结果只作历史对照。综合、容量不足、布线未完成及请求频率未达标分别保存，详细数据随独立报告提供。

2026 Sixth Lion School Science Award
仅用于学术论文公示

VIII. AM-SEV 与修订实例的评估

A. 固定样本与检查条件

先固定算法、常量标签和输出规则，再生成统计样本。输出剪切的旋转参数经过了有记录的 36 组 NIST 100 筛选；该选择过程在此披露。NIST 100 行属于开发筛选结果；NIST 1000 及其余电池是筛选后的检查。严格比例门槛与 p 值离群项一并报告，未把失败项改写成通过。保存的 48000 字节公开文件给出 1000 组 32 字节密钥与 16 字节 nonce，每组初始化后生成恰好 1000000 位。这里公开密钥是复现实验输入，不是部署密钥。GM/T 与 NIST 读取相同字节，观察 P 值后不重采样。长流工具则在同一密钥下拼接 nonce 互异的 4GiB 会话，以遵守单次初始化接口预算。

GM/T 采用公开库 Trisia/randomness 的固定版本[9]及项目 27 分支适配器，v4 样本全部重新生成；这是所列配置的检测记录，不是产品认证。Python 重现第一条完整 125000 字节样本；独立重算 5000 组 P/Q，最大绝对误差 2.22×10^{-16}。全零、交替位负对照及低 P 观察都在原始工件中保留。负对照被拒绝不能证明接近随机的发生器具有密码学安全。

B. 输出统计测试及例外

GM/T 0005–2021[10]规定 15 类方法；本次适配器设置 27 个参数分支，显著性水平 0.01，均匀性阈值 0.0001。全部 27 分支同时满足通过比例和均匀性要求：1000 条中通过 982–995 条，最低要求 981 条，Q 值分布的最小均匀性检验值 $U = 0.0043013$。这些是新生成 v4 样本的结果，不是旧 v3 数值。

NIST STS 2.1.2[11]含 15 族 188 行。通过比例的严格下限为 $\lceil 0.99m - 3\sqrt{0.99 \cdot 0.01m} \rceil$，其中 m 为该行适用样本数。100 条剖面各行均满足此下限：常规分母 100 时通过 97–100 条；1000 条剖面常规分母下通过 982–998 条，严格最低为 981 条。随机游走族另按实际适用分母 614 验收，通过 605–611 条。报告首列是行级均匀性 P 值，其验收阈值为 0.0001，并非单条序列的显著性水平 0.01；两个剖面的最小值分别为 0.000439 和 0.001123，均满足均匀性要求。低于 0.01 的行级均匀性 P 值分别有 6 行与 2 行，作为尾部观察保留，不另行改写成比例缺陷。100 条已用于候选筛选，1000 条包含其中 100 条，故不视为两个独立验证集。统计通过不决定密码安全。

TestU01 [8] SmallCrush 消费 226866076 个 32 位字，15 项统计均通过。可移植与优化实现报告的 P 值及消费字数一致。Crush 完成 144 项统计，无标记分项，跨 32 个互异 nonce 会话消费 33843219826 个 32 位字。Rabbit 在 10^8 位配置的 40 项全部通过（73367232 个 32 位字）；同规模 Alphabit 的 17 项通过。BigCrush 记录于表XVII；其单项尾部标记按原样保留，不用其他电池抵消。PractRand 0.96[12]以开启 Windows 二进制输入的宏重新编译，统计函数未改。1GiB 运行没有 FAIL/SUSPICIOUS，也没有 unusual 项（227 项测试结果）。BigCrush 在最终 v4-R1 流上完成 160 项统计，消费 357112465449 个 32 位字，跨 333 个互异 nonce 会话。TestU01 汇总列出 1 项落在 $[0.001, 0.9990]$ 之外：$r = 0$ 的 SimpPoker，$p = 7.6 \times 10^{-5}$（$\chi^2 = 49.99$，18 自由度）；其余 159 项通过。该标记按原样保留，不改写为通过。快速 PractRand1TiB 运行到 2^{40} 字节，354 项结果无 FAIL、SUSPICIOUS 或 unusual。较早未含输出剪切的流在便携式 256MB 检查点记录过两个 unusual；这是不同输出配置的历史记录，不能与当前 R1-P4 的无标记结果合并为同一次运行。原始日志单独归档。便携 1GiB 与快速长流的初始密钥、nonce 和计数器规则一致，前 32MiB 逐字节相同。

C. 附加筛选与输出剪切修订

在同一冻结开发语料上，先检查 36、40、44、48 轮及四个结构候选，随后提前固定 31 个共享 P 层旋转候选。共 39 个候选均在严格 NIST100 条门槛被拒；后续未运行电池不计为通过，独立复核语料也未用于验收。上述 39 个候选仍全部被拒；v4-R1 的字节接口包含公开输出剪切，是第八节报告的研究实例。此前共享 P 族没有入选的 R2。

同一严格 100 条门槛下，AES-256-CTR 与 ChaCha20 参考对照也出现拒绝项。这些标记需要按其统计含义解释，不能直接称为密码攻击。理想单项按 0.01 水平独立拒绝每条样本时，$F \sim \mathrm{Bin}(100, 0.01)$，严格

[9]源码版本：https://github.com/Trisia/randomness/tree/5baeaa7dbdb5efb87693ce1fd7a72f5c10c71805。

[10]国家密码管理局公告（第 43 号）：https://oscca.gov.cn/sca/xwdt/2021-10/19/content_1060880.shtml。

[11]NIST SP 800-22 Rev. 1a（2010）：https://csrc.nist.gov/pubs/sp/800/22/r1/upd1/final。

[12]工具发布与文档：https://pracrand.sourceforge.net。

2026 Silk Road High School Science Award 仅用于2026丝路高级中学科学奖公示

表 XVII
v4-R1 的 R1-P4 字节输出统计记录。未完成项目不得计作通过；标记项按原样列出，不四舍五入为通过。

测试	规模	结果
GM/T 0005–2021	1000×10^6 bits	27/27 分支
NIST STS	100×10^6 bits	0 个 3σ 比例缺陷；常规行 97–100/100，游走行 66–69/69
NIST STS	1000×10^6 bits	0 个 3σ 比例缺陷；常规行 982–998/1000，游走行 605–611/614
SmallCrush	226866076 个 32 位字	15/15 通过
crush	144 项统计	全部通过；33843219826 个 32 位字
bigcrush	160 项统计	159 项通过；1 项标记（SimpPoker，$r=0$，$p=7.6\times10^{-5}$）；357112465449 个 32 位字
rabbit	40 项统计	全部 40 项通过；73367232 个 32 位字
alphabit	17 项统计	全部通过；28125000 个 32 位字
PractRand	1 GiB	227 项测试无异常
PractRand long	1 TiB	最终 354 项无异常；保留较早标记
滞后诊断	2^{22} words	自定义诊断，区别于 Dieharder

97/100 门槛的剖面拒绝概率为 $\Pr(F\ge4)=0.0183740$。此计算不假定 188 行相互独立。全部失败记录保留，未通过换种子或调整阈值取得通过报告。

D. 自定义滞后诊断与修正方差

在 2^{22} 个 64 位字、即 32MiB 上重做旧自定义诊断：18 个滞后的低 32 位 Pearson 相关、同组滞后的原始乘积和，以及 12 个滞后各 64 个位通道相关。明确区分于 Dieharder 程序。字相关最小 P 值 0.127473，修正协方差后的原始乘积最小 P 值 0.529011；位通道最小未调整 P 值 0.00151643，高于全 804 项 Bonferroni 阈值 $0.05/804\simeq6.22\times10^{-5}$。这里仍使用渐近 P 值诊断，比较之间存在依赖。

旧原始乘积代码漏计了共享操作数的依赖。对 IID 标量字，均值 μ、方差 σ^2、二阶矩 m_2，设 $S=\sum_{i=0}^{n-k-1}X_iX_{i+k}$、$m=n-k$，则

$$\mathbb{E}S=m\mu^2,$$
$$\operatorname{Var}S=m(m_2^2-\mu^4)+2\max(n-2k,0)\mu^2\sigma^2.$$

不相交乘积项独立；共享项满足 $\operatorname{Cov}(X_iX_{i+k},X_{i+k}X_{i+2k})=\mu^2\sigma^2$，这样的无序项对有 $\max(n-2k,0)$ 个，在方差中各计两次。工件分字段保存旧式与修正式的 Z/P，没有把旧统计重新包装为已校准结果。

E. 经验诊断：神经探针与雪崩

以下诊断针对 32 轮分组核心 E_K；公开输出剪切 P 未参与这些诊断。复用历史网络结构，以明确的 NumPy 后端实现两层各 128 单元 ReLU、Adam 学习率 0.001、25 轮训练、批量 512，每组 12000 正例与 12000 负例。八位字宽、1 至 8 轮及 22、32 轮，配合种子 5、6、7，共 30 组预先确定的探测；固定缩小密钥，方向为 $e_{u,0}$。各组平衡留出集 4800 条；输入无序对的代表先去重再划分训练/测试。全部权重、数据哈希和结果保存。向量实现先与独立标量模型核对；恒等控制准确率 1.0，随机分布控制 0.50104。

30 组准确率范围 0.48750–0.522292。最高值是 32 轮种子 6 的 2507/4800；条件 Fisher 参考检验 $p=0.00071697$，对 30 次比较作 Bonferroni 后为 0.0215091。虽然未超过历史 0.55 启发阈值，仍作为标记保留。随后不重训、不搜索另一种子，对保存模型使用另行固定的 100000 正例与 100000 负例，排除原输入代表。确认集准确率 100281/200000，即 0.501405，条件 Fisher 参考 $p=0.095196$，未复现初始显著性，但初始标记没有删除。参考检验依赖所述可交换零假设，不覆盖其他网络，也不建立全位宽输出优势界。

预备数据生成曾在截断前排序输入代表，意外改变抽样范围及训练/测试范围。加入论文结果前的代码复核发现该问题；预备版源码、权重与结果单独归档。正式计算保持随机首次出现顺序，种子和预算不变。这是方法纠错，没有将预备试算称为有效 IID 实验。

a) 雪崩与物理泄漏: 32 轮实验对 1024 个固定基点逐一翻转 256 个输入位，平均输出汉明距离 128.015789。65536 个输入位到输出位的翻转计数格子范围 448–577，分母 1024。这是相关格子上的扩散诊断，

2026 S. T. Yau High School Science Award
仅用于2026丘成桐中学科学奖公示

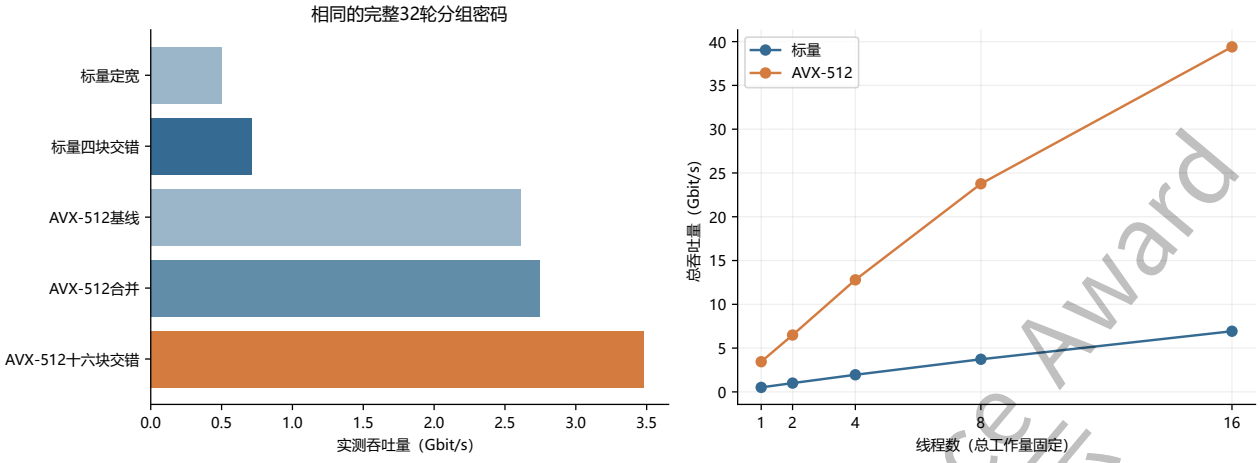


图 11. 完整 32 轮内核的吞吐与固定总工作量下的线程扩展。内核与扩展点来自归档的十六块交错构建；当前八通道适配路径见表XXI。

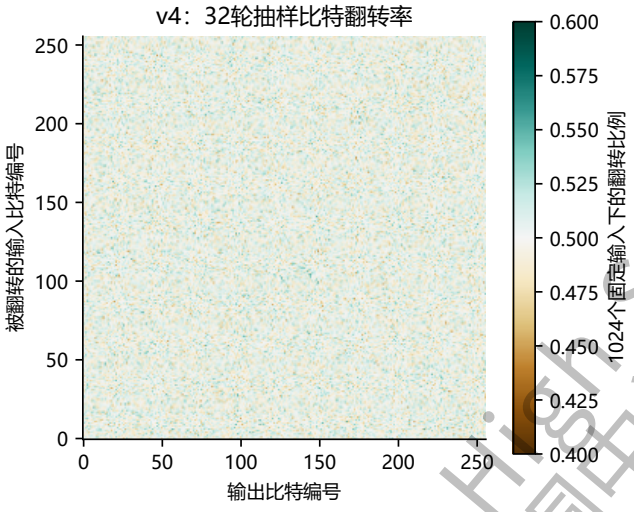


图 12. v4-R1 分组核心 E_K 的扩散抽样热图（不含输出置换 P），色阶 0.4–0.6。这是 32 轮观察，不是安全界。

不是严格雪崩或位独立性证明。均匀的扩散图仍可能隐藏密码关系。

C 轮无秘密索引表，指令结构固定，源代码不存在秘密相关控制分支。这只支持源码控制流观察，不能替代不同编译器和处理器上的恒时测量。本文没有掩码证明、功耗/电磁泄漏、故障注入或实体 FPGA 测量。串行原型用于功能和成本研究，不宣称抗侧信道。

F. 优化实现仍是同一算法

定宽 64 位和八路 AVX-512 实现保持冻结操作与轮数，没有用其他原语生成输出。已对比 256 个分组与可移植 C、前 32768 字节流与独立 Python。引入四线程生成后，完整 256MiB 文件 SHA-256 保持为

表 XVIII

同一主机三次中位数。参考路径行按统一读取壳重测；内核与线程扩展行来自归档的交错构建。内核、字节 API 与线程扩展分别计量。

配置	线程	Gbit/s
参考 API，8 字节	1	0.1532
参考 API，16 字节	1	0.1537
参考 API，16 KiB	1	0.1536
定宽完整块（内核）	1	0.5030
四块标量交错（内核）	1	0.7124
AVX-512 八块（内核，归档）	1	2.6107
AVX-512 八个独立流（归档）	1	2.7633
AVX-512 十六块交错（归档）	1	3.4809
AVX-512 多线程，1 线程（归档）	1	3.4472
AVX-512 多线程，2 线程（归档）	2	6.4928
AVX-512 多线程，4 线程（归档）	4	12.7956
AVX-512 多线程，8 线程（归档）	8	23.7655
AVX-512 多线程，16 线程（归档）	16	39.3977

ce248dddd103b6a7acdd31bd89709faf
d7b96665d51807324436b2e630d9d65c

SmallCrush 也在两种实现间重放一致。这些检查支持用快速生产器完成长统计，同时保存主动停止的慢速重复运行日志，不能把中断解释成算法统计失败或成功。

G. 软件性能与工程成本

参考上下文占 1168 字节。当前 `csprng_bench.c` 的八通道基准适配器包含参考上下文与一个 64 位计数，共 1176 字节；统一读取壳及临时缓存另计。其填充函数要求 256 字节整数倍，报告中的小请求由 16KiB 读取壳提供。这是实测适配路径，不等同于已验证所有参考 API 边界的直接替代实现。此前 11072 字节优化上

2026 S.T. Yau High School Science Award 作品于2026年成稿中学科学奖论文公示

表 XIX

统一 16 KiB 读取壳下的交付字节接口，三次中位数。参考路径调用 v4_read；向量路径使用八通道内核。

路径	8 字节	16 字节	16 KiB	1 MiB 流
	Gbit/s			
参考路径	0.1532	0.1537	0.1536	0.1531
AVX-512	2.5073	2.5834	2.6461	2.6463

表 XX

归档优化后端初始化及首 32 字节，含密钥准备；不是当前八通道适配器的初始化测量。

批量块	ns/次
1	2292.19
4	2301.37
8	3502.23
16	3495.80
32	3496.48

下文、初始化测量及 164 组 API 边界检查均属于归档后端，分别保留其范围。

图11概括了完整内核吞吐与线程扩展。

本轮在 AMD Ryzen9 8940HX 主机上采用 QPC 墙钟计时，三次重复取中位数，保存每次运行和范围。全部长统计及硬件任务结束后再计时；线程由操作系统调度。TSC 只列参考 ticks，不以其频率代替核心执行频率，也不作 5GHz 线性外推。

8 字节与 16 字节情形各调用 5000 万次；16KiB 与 1MiB 情形每次运行交付 1GiB。批量与向量行通过统一读取壳执行同一计划，多线程维持总工作量。初始化测试为 5 万次。论文文字与旧复现源文件的循环量并不完全相同，本轮在原始 JSON 中逐项记录实际次数和交付字节，而不声称逐字运行了全部旧包装。

预合并子密钥与轮常量采用 XOR 结合律；四块标量、两批或四批八通道向量只交错不同块的操作，保留各块全部 42 个顺序赋值和 32 轮。字节接口在每个分组后施加四个公开输出剪切赋值；优化后端同时保留 42 个分组赋值与该输出阶段。归档优化 API 有 164 组字节流与边界检查；当前吞吐适配器完成 1MiB 参考流比对，但不继承该归档后端的完整边界验证声明。优化输出与参考相同，因此输出剪切后的统计结果在各后端间保持一致。

完整块标量内核为 0.5030 Gbit/s，四块交错为 0.7124。八通道交付路径经 16 KiB 字节 API 实测为 2.646 Gbit/s（8 字节请求为 2.507），与表XXI同口径。

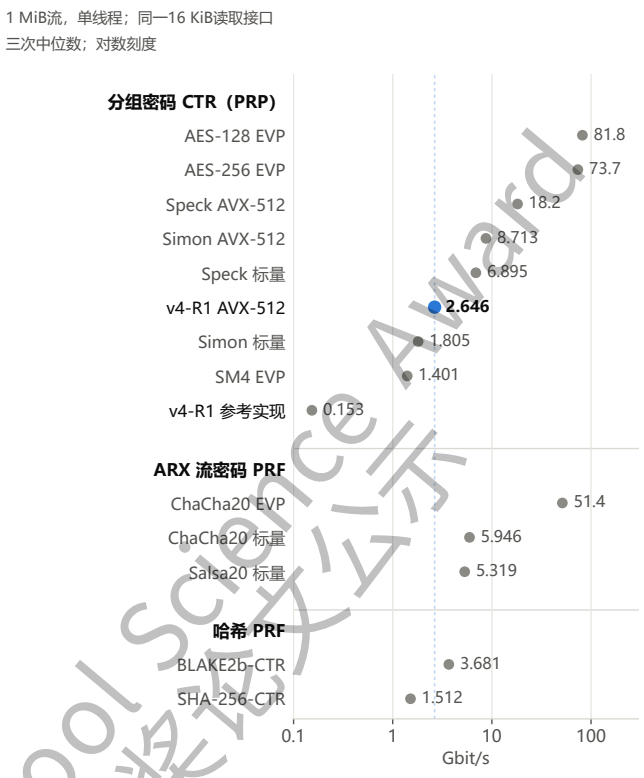


图 13. 同一家族、同一读取壳：1 MiB 流的对数刻度吞吐。交付的 v4-R1 八通道路径高亮，灰色行为语境。数值来自表XXI同一基准的三次中位数；这是实现对比，不是等安全排名。

线程扩展示意所用的十六块交错归档微基准为 3.4809 Gbit/s，它不是交付路径。初始化成本另列，避免用长流吞吐掩盖短请求代价。每输出 256 位需 32 轮，故单块顺序实现的轮速率换算因子为 8 位/轮，与原始轮测试相符。

表XXI把交付路径放进基于 PRF 的 CSPRNG 家族，而不是与线性生成器比较。所有行使用同一 16 KiB 读取壳、同一调用计划和三次中位数；可移植行是同一编译选项下的自实现，EVP 行使用平台 OpenSSL。v4-R1 八通道路径为 2.646 Gbit/s：高于标量 SHA-256-CTR、SM4-CTR 与 Simon-CTR（1.51、1.40、1.81），接近 BLAKE2b-512-CTR（3.68），低于标量 ChaCha20（5.95）以及向量化 Simon/Speck 路径（8.71、18.16）；AES-NI 约快一个数量级。排序反映轮函数成本：Simon 与 Speck 的轮更轻，v4-R1 固定 32 轮、每轮 26 个字级 AND。该表只支持一个窄结论——交付路径位于软件 PRP 区间、不是框架瓶颈——不支持等安全排名。

原 v3 单轮更新后交付 64/128 位，v4-R1 以 32 轮

2026 Silk Road High School Science Award 获奖论文公示 仅用于公示后完成用学术论文

表 XXI
同一主机、同一 16 KiB 读取壳、同一调用计划，三次中位数。可移植行使用同一编译选项下的自实现；EVP 行使用平台 OpenSSL（AES-NI/AVX-512 汇编）。块长与轮函数不同，不构成等安全比较。

实现	原始块 (B)	8 B 接口	16 KiB 接口	1 MiB 流	TSC tick/B
			Gbit/s		
分组密码 CTR（PRP）					
Tempest v4-R1，AVX-512	32	2.507	2.646	2.646	7.24
Tempest v4-R1，参考路径	32	0.153	0.154	0.153	125.14
Simon128/256-CTR，标量	16	1.734	1.807	1.805	10.62
Simon128/256-CTR，AVX-512	16	7.483	8.939	8.713	2.20
Speck128/256-CTR，标量	16	5.987	6.896	6.895	2.78
Speck128/256-CTR，AVX-512	16	12.313	17.439	18.159	1.06
AES-128-CTR，EVP	16	29.401	83.406	81.845	0.23
AES-256-CTR，EVP	16	28.257	74.206	73.668	0.26
SM4-CTR，EVP	16	1.365	1.403	1.401	13.68
ARX 流密码 PRF					
ChaCha20，标量	64	5.360	5.955	5.946	3.22
ChaCha20，EVP	64	24.134	51.473	51.389	0.37
Salsa20/20，标量	64	4.753	5.313	5.319	3.60
哈希 PRF					
SHA-256-CTR，标量	32	1.459	1.510	1.512	12.68
BLAKE2b-512-CTR，标量	64	3.419	3.696	3.681	5.21

交付 256 位；这种构造差异须与实现优化区分。AES-NI 与 OpenSSL 汇编路径不构成等安全排名，新表也不作此声称。

H. 消融与淘汰版本的反例价值

第一项保留旧自乘，仅改变旋转：零与全一仍碰撞，故旋转变体未修复结构缺陷。第二项保留旧公开递推：至多 64 次更新后固定，默认首次固定为第 63 次，即 22 轮初始化后再生成 41 轮；这属于公开调度，不是秘密主密钥的“弱密钥”。

第三项独立传播 v3 四位固定公开序列的像纤维，一轮像 3501，22 轮像 139，最终碰撞能量分子 88844774、分母 2^{32}。第四项把旧读字秩式套到新端口，以 `0x5` 支撑反例拒绝。第五项把二次公式用于完整级联，由非零仿射缺陷拒绝。这些消融说明论据为何失效，而非调整评分来偏爱 v4。

历史上的注入覆盖与半块输出检查器同样保留：先注入公开量后被快照赋值覆盖是数据流错误，只比较半个分组便接受是接口验证错误，二者都不能由统计测试掩盖。项目归档保存完整讨论和原图。AI 候选引擎尚无留出集、等预算的独立对照实验，不能宣称比现有搜索方法更有效。

IX. 讨论与结论

AM-SEV 在 Tempest 实例中连接 AND-RX 候选的程序对象、结构查询、缺陷反例与修复证据，使设计修订后、限定条件下的结论仍可追溯并独立复核。这一结果为可验证密码设计提供了具体的复核起点，使后续分析者能够区分已经建立的性质、依赖的程序条件和仍缺少的证据。本文沿用经典二次函数分析，并对 CLAASP 等自动化分析工作作实例补充：限定 Tempest 各版本结论的适用范围，给出结构推导，保留从边界反例到修复后复核的记录 [7], [15], [16]。完整位宽的多轮差分与线性簇、相关密钥、代数恢复及实现泄漏尚未完整分析，原语 PRP 优势仍未知，AI 引擎也缺少留出候选上的等预算对照，因此尚不能确定 v4-R1 的完整密码安全强度或引擎相对已有方法的搜索效率。后续应建立符合顺序执行语义的多轮模型，针对零活动见证与统计标记开展独立密码分析，并补充目标平台泄漏评估和多种子、等预算搜索实验，逐项缩小这些未知范围。

2026 Si Yuan High School Science Award 仅限于公示成绩的科学类论文公示

参考文献

[1] D. Blackman and S. Vigna, “Scrambled linear pseudorandom number generators,” *ACM Trans. Math. Softw.*, vol. 47, no. 4, 2021.

[2] M. E. O’Neill, “PCG: A family of simple fast space-efficient statistically good algorithms for random number generation,” Technical Report HMC-CS-2014-0905, Harvey Mudd College, 2014.

[3] D. J. Bernstein, “ChaCha, a variant of Salsa20,” 2008.

[4] S. Sun, L. Hu, P. Wang, K. Qiao, X. Ma, and L. Song, “Automatic security evaluation and (related-key) differential characteristic search: application to SIMON, PRESENT, LBlock, DES(L) and other bit-oriented block ciphers,” *ASIACRYPT 2014*, LNCS 8873, pp. 158–178, 2014.

[5] L. Song, Z. Huang, and Q. Yang, “Automatic differential analysis of ARX block ciphers with application to SPECK and LEA,” ACISP 2016, LNCS 9723, pp. 379–394.

[6] J. Daemen and V. Rijmen, “The wide trail design strategy,” in *Cryptography and Coding 2001*, LNCS 2260, pp. 222–238, 2001, doi: 10.1007/3-540-45325-3_20.

[7] E. Bellini, D. Gerault, J. Grados, Y. J. Huang, M. Rachidi, S. Tiwari, and R. H. Makarim, “CLAASP: a cryptographic library for the automated analysis of symmetric primitives,” *IACR Cryptology ePrint Archive*, Paper 2023/622, 2023. https://eprint.iacr.org/2023/622.

[8] P. L'Ecuyer and R. Simard, “TestU01: a C library for empirical testing of random number generators,” *ACM Trans. Math. Softw.*, vol. 33, no. 4, article 22, 2007.

[9] A. Gohr, “Improving attacks on round-reduced Speck32/64 using deep learning,” *CRYPTO 2019*, LNCS 11693, pp. 150–179, 2019.

[10] M. Matsumoto and T. Nishimura, “Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator,” *ACM Trans. Model. Comput. Simul.*, 8(1), 1998.

[11] L. Blum, M. Blum, and M. Shub, “A simple unpredictable pseudo-random number generator,” *SIAM J. Comput.*, 15(2), 1986.

[12] W. Alexi et al., “RSA and Rabin functions: certain parts are as hard as the whole,” *SIAM J. Comput.*, 17(2), 1988.

[13] S. Chen, Y. Fan, L. Sun, Y. Fu, H. Zhou, Y. Li, M. Wang, W. Wang, and C. Guo, “SAND: an AND-RX Feistel lightweight block cipher supporting S-box-based security evaluations,” *Designs, Codes and Cryptography*, vol. 90, pp. 155–198, 2022, doi: 10.1007/s10623-021-00970-9.

[14] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, “Ascon v1.2: lightweight authenticated encryption and hashing,” *J. Cryptol.*, vol. 34, article 33, 2021.

[15] S. Kölbl, G. Leander, and T. Tiessen, “Observations on the SIMON block cipher family,” *CRYPTO 2015*, LNCS 9215, pp. 161–185, 2015.

[16] K. Nyberg, “Differentially uniform mappings for cryptography,” EUROCRYPT 1993, LNCS 765, pp. 55–64, 1994.

[17] T. Ashur and Y. Liu, “Rotational cryptanalysis in the presence of constants,” *IACR Trans. Symmetric Cryptol.*, vol. 2016, no. 1, pp. 57–70, 2016.

[18] A. Biryukov, B. Lambin, and A. Udovenko, “Exact formula for RX-differential probability through modular addition for all rotations,” *IACR Trans. Symmetric Cryptol.*, vol. 2025, no. 1, pp. 542–591, 2025.

[19] S. Yakovliev, “Differential properties of LRX-analogues of small constant multiplication,” *Int. J. Electron. Telecommun.*, vol. 71, no. 1, pp. 95–100, 2025, doi: 10.24425/ijet.2025.153550.

[20] C. Blondeau and K. Nyberg, “New links between differential and linear cryptanalysis,” *EUROCRYPT 2013*, LNCS 7881, pp. 388–404, 2013.

[21] Y. Ishai, A. Sahai, and D. Wagner, “Private circuits: securing hardware against probing attacks,” CRYPTO 2003, LNCS 2729, pp. 463–481.

[22] L. K. Grover, “A fast quantum mechanical algorithm for database search,” STOC 1996, pp. 212–219. https://arxiv.org/abs/quant-ph/9605043.

[23] A. Biryukov and A. Shamir, “Cryptanalytic time/memory/data tradeoffs for stream ciphers,” ASIACRYPT 2000, LNCS 1976, pp. 1–13.

2026 Xiaohu High School Science Award 应用于2026年获得中学科学奖论文公示

致　谢

这篇论文背后的算法经历了十一代设计、超过二十个变体，以及数次深刻的自我修正。回头看，这段旅程最困难的从来不是某个定理，而是学会在每一个数字面前保持诚实。论文最终能够交付，离不开许多人的帮助，谨在此致以诚挚的谢意。我负责了寻找研究方向、构思研究思路、进行计算机实验和撰写论文。

首先要衷心感谢我的指导老师高洁老师与吴琼老师。高洁老师是我在学校的数学竞赛教练，为我打下了数论和代数的知识基础。为了了解专业学术论文的写作规范，我找到了西安工业大学的吴琼教授进行指导。在论文结构组织、图表呈现与论文写作规范方面，老师们提出了许多宝贵的修改意见。指导为无偿性质，两位老师从未参与实验计算、验证代码的编写与论文主体的撰写，全部技术内容均由本人独立完成并负责。

还要感谢 `awesome-cryptography-rust`（rust-cc 组织维护的 Rust 密码学精选开源列表）的维护者们：本论文的代码仓库有幸被该列表收录。感谢 wolfSSL 的 David Garske 先生，感谢他对算法的审阅。开源社区对独立研究者的这份善意，是这项工作的一个重要组成部分——论文反复强调每个声明都应能被任何人独立复核，而正是这样，让社区复核成为可能。谨向维护者的辛勤付出致以诚挚的谢意。

关于本论文的研究过程，在此作如下说明。

选题源于我对随机数构造及其安全问题的关注。研究初期，我较多关注输出是否均匀、算法运行是否足够快；进一步学习后，我认识到，统计测试、结构性质与密码安全回答的是不同问题，不能相互替代。因此，本文把研究问题逐步收敛为：怎样把一个 AND-RX 候选的程序对象、结构查询、缺陷反例与修复证据连接起来，使设计修改后的每条结论仍能独立复核？AM-SEV 围绕这一问题组织分析方法，Tempest v4-R1 作为修订实例，旧版本则作为检验论据和说明修复依据的对照。

本次修订的研究工作也围绕这一问题展开：梳理二次影子、完整分组核心和字节输出接口的区别，核对局部秩公式与程序的对应关系，依据旧结构的反例修改轮函数，并给出逆算法和固定密钥下的置换证明。实验部分分别开展四位字宽模型的完整计数、全位宽指定查询的抽样、C 与独立 Python 实现的一致性检查，以及 NIST、GM/T、TestU01 和 PractRand 等输出统计测试；软件吞吐测量与 FPGA 原型的仿真、综合及布局布线结果也各自注明实现与条件。完整计数、有限观察和条件性论证分别报告，统计标记、零活动见证、求解器超时和硬件尚未上板等情况一并保留，没有把测试通过当作完整密码安全证明。

研究过程中的一段难忘经历，是尝试把算法接入已有软件生态。我曾围绕 Rust 的 rand_core、Go 的 math/rand/v2、C++ 的随机数接口、GSL、NumPy 及 OpenSSL 等开展历史版本的接入验证。特别感谢 wolfSSL 的 David Garske 先生，他在 issue 中说

2026 Shaanxi Youth Undergraduate Science Award
仅用于2026年陕西省青少年科学院论文公示

明了库内接口的限制，并建议使用 crypto callback 这一外部接入路径，帮助我完成了当时版本的 TLS 握手接入实验。这些交流让我更认真地看待接口契约和验证范围：旧版本的接入与已知答案测试不能直接作为 v4 的验证结果，接口能够调用、项目被目录收录，也都不能代替独立的密码安全分析。我会继续通过公开代码和实验记录向社区征求意见。

研究中最困难的部分，是发现已有论据失效后，重新检查它所支撑的结论。早期枚举程序对快照与顺序读取的处理不一致，使部分数字描述了不同的轮函数；旧版本还存在公开注入被后续赋值覆盖、字内映射合并不同输入等问题。修订中，我把这些问题逐一分开，撤回不能成立的推断，并据此引入目标字不参与右端的顺序剪切、秘密子密钥和明确的计数器接口。由各步可逆得到的置换性，只回答结构修复是否成立，没有解决完整原语是否具有足够小的伪随机置换优势。

复核验证工具本身同样带来了教训。历史通用搜索器的一般 AND 差分更新混用了旋转前后的操作数；名为精确枚举的活动检查也只遍历差分，每个方向仍抽样一个状态。因此，相关活动分数和搜索排名只能保留为历史记录，不能继续作为精确性质证据。当前 v4 的两次实际执行比较、插桩诊断和源码等价检查分别说明了对象与范围。这些修正让我逐渐养成一个习惯：不仅检查结果是否符合预期，也检查生成结果的程序是否真正回答了提出的问题。

这段经历使我学会了更具体地表达一项研究的贡献与局限：说明已经证明了什么，保存反例和失败记录，也承认暂时无法回答的问题。全位宽多轮密码分析、实现泄漏与 AI 引擎的独立对照评估仍有待继续开展。能够在老师和开源社区的帮助下完成这些修订，并带着可供复核的材料参加答辩，是这次科研训练留给我的重要收获。

最后，按照竞赛要求如实说明本研究对人工智能工具的使用情况。研究过程中使用了 deepseek v4 flash(通过 claudecode 平台接入)，用途包括三个方面：其一，在 AI 设计引擎中作为提案生成器参与候选算法结构的设计——所有提案均经过校准验证器栈以机器可查的数学度量（秩、代数度、密钥相关性等）裁决，不依赖模型的判断；其二，辅助验证、整理部分验证脚本；其三，论文文字的组织与润色。

参赛者：田岳洲

2026 年 11 月

2026 S. T. Yau High School Science Award
仅用于2026丘成桐中学科学奖公示