FIBEMATE · 项目简介

让工程文档里的每个数字都有据可查

一套可复现的后量子密码工程参考实现，以及围绕它的证据链工具。
目标不是“声称安全”，而是让“声称”可以被逐条复核。

版本：2026-10 快照 · 联系：research@fibemate.net · 代码：github.com/Lennonhaha

一、我们要解决的问题

在密码工程与安全评审中，最常见的失效不是算法被攻破，而是**文档与实现之间没有任何可执行的对应关系**：文档写“10,000 次交叉验证通过”，实现里找不到那 10,000 次的输出；文档写“常数时间”，代码里没有任何时序检测记录。

审阅者因此只有两个选择：相信，或者不信。两者都不专业。我们做的是第三种：**把每个数字指回一个产物，把指不回去的明确标出来。**

二、三个可独立复核的交付物

1. 后量子密码参考实现（ML-KEM / ML-DSA 及衍生方案）

JavaScript、C、WebAssembly、FPGA 四端实现与跨语言互操作验证；KAT/TVLA 测试向量入库；算法参数、序列化格式、边界条件有对应测试。定位是**互操作与教学用的参考实现**，不是经认证的密码模块。

2. 数字溯源工具 verifact（本次样例报告的对象）

只读扫描代码库文档，抽出带数字的断言，逐条绑定到仓库内产物，输出“一致 / 不一致 / 无产物 / 多候选”四态账本，并作为 CI 门禁运行。**它不判断谁对，只判断“能不能对上”和“对上了没有”。**

3. 形式化验证与时间戳存证

关键协议不变量以 Isabelle 建模并给出机器可检的证明义务账本；发布物用 RFC 3161 时间戳（TSA）固定，任何人可用公开哈希复核。存证文件本身禁止被注释修改——工具对这类目录设有独立的“哈希存证”类别。

三、当前状态：数字，含不好看的那些

FIBEMATE 全仓扫描快照 · 2026-10-30 12:31 · 范围：按 `verifact.json` 全仓配置扫描（379 个文档）。

项目	实测值	说明
文档中的数字断言	2,347	含叙事、存证、豁免条目
应当有产物的断言	2,137	覆盖率的分母
逐条绑定成功	137	6.4%（2,137 分母）
暂无产物	1,768	**诚实缺口，不隐藏**
与产物不一致	0	CI 门禁当前通过
显式豁免	21	每条写明理由与失效条件
形式化：证明义务	6	已登记、未关闭，宽松构建下通过

口径说明：`claimsTotal` 含被分类、被忽略与被拒绑的条目，所以它与“应当有产物”的分母不等；两个百分比的分母不同，不可互相引用。与 2026-10-26 那份 `docs/` 子集快照（314 条断言）不是同一分母，不构成趋势比较。

> **必须说明的三件事**：① 未做全量硬件级物理侧信道评估（当前仅为软件级 TVLA 自评），文档已按此修正声明；② 未通过任何第三方安全审计或密评认证；③ 形式化验证的“严格模式”目前会按设计失败——6 条证明义务尚未完成，我们不把它包装成“已验证”。

四、为什么这些数字值得相信

不是因为我们说它们可信，而是因为每一条都有可复现的检查方式：

主张	复核方式
文档数字与产物一致	运行 verifact，逐条给出文件、行号、产物路径
形式化证明可复现	容器内 `isabelle build`；严格入口单独提供，失败即为失败
发布物未被改动	RFC 3161 时间戳 + 公开哈希
测试真实通过	测试脚本与 CI 日志公开；关键用例做了变异验证（改坏实现必须变红）

> **一条我们自己踩过的教训**：工具曾把 X25519 keygen 5.97ms 与 SM2 verify 50ms 绑定成功（相似度 0.57），因为两者形状相近。这条被隐藏在一份“豁免清单”里很久。现在的规则是：**形状相似在密码学语义面前不算证据**，任何豁免都必须署名。

五、可以怎么合作

场景	交付形态
存量系统文档审计	只读扫描 + 数字溯源报告（哪些数字有据、哪些无据、哪些冲突）
PQC 迁移评估	CBOM（CycloneDX 标准）生成与差异分析
交付物可复核性	把“文档—产物”对账接入 CI，交付时附可复核账本
教学与实训	参考实现 + 验证容器 + 失败案例集（含本文提到的错绑案例）

我们不做的事：不做安全认证代办，不出具“符合某标准”的结论，不宣称未经第三方验证的安全性质。**我们提供的是证据，结论应由评审方自己下。**

六、附件

- 《文档数字溯源样例报告》（对 liboqs 与 FIBEMATE 两个真实仓库的只读扫描）：https://fibemate.net/docs/verifact-sample-report-20261030.pdf
- 本文（项目简介 PDF）：https://fibemate.net/docs/fibemate-intro-20261030.pdf
- 工具与规则源码、门禁配置（开源，可自行复跑）：https://github.com/Lennonhaha/fibemate-tools

本文所有数字均来自 2026-10-30 的本地实测输出，可要求提供原始 JSON。