

MoonGuard 项目申报书

一、项目名称

MoonGuard — MoonBit 供应链安全工具链

二、项目简介

MoonGuard 是用纯 MoonBit 实现的供应链安全工具链，提供 Ed25519 包签名与验签、SHA-256 清单完整性校验、JSON+PEM 可信公钥管理、Levenshtein 与同形 (homoglyph) 双模式 typosquat 检测、CVSS 风格 0-10 风险评分的 JSON 安全审计报告，附带 9 子命令的 moon_guard CLI。

三、项目方向与适用场景

方向：MoonBit 包供应链安全（包来源可信 + 清单完整性 + typosquat 检测）。适用：开发者发布前签名验证、用户安装前审计、CI/CD 集成、批量仓库风险扫描。

四、核心功能

lib/manifest	纯 MoonBit SHA-256、清单生成与校验
lib/crypto	Ed25519 (RFC 8032) + SHA-512 + field 算术
lib/trust	Full / Partial / Untrusted 分级 + PEM / JSON 持久化
lib/verify	audit 全链路 (integrity + signature + trust) + typosquat 严格检测
lib/report	0-10 风险评分 + JSON 安全报告
cmd/main	9 子命令 CLI: keygen / sign / verify / trust / typosquat / manifest / hash / audit / version

五、项目属性

原创项目 — SHA-256 / Ed25519 / Levenshtein 全部按公开 RFC (6234 / 8032) 与算法规范独立实现，不移植自其他项目，无闭源代码，无授权争议。

六、GitHub / Gitlink 仓库

GitHub: <https://github.com/chenzehao00/MoonGUARD>

Gitlink: <https://gitlink.org.cn/sharp/MoonGuard>

默认分支: main

七、交付物

核心 lib + CLI + 83+ 单元 / 端到端 / fuzz / bench 测试 + 跨平台 CI (ubuntu/macos/windows × wasm/native) + examples/basic_audit 可复现 demo; 通过 moon check / moon info / moon test 三连验证。

八、编译与运行验证

本地命令: moon run cmd/main -- keygen 生成密钥对; moon run examples/basic_audit 跑通端到端审计; moon run cmd/main -- audit pkg ver "src/main.mbt:fn main {}" 产出包含风险评分与 JSON 报告的标准输出。

本申报书内容限定在一页 PDF (按章程要求)，完整技术细节见 README.zh.md、docs/API.zh.md 与 PROJECT_PROPOSAL.md。