周报 向嘉豪(2025-12-15)

摘要: 本周为 ML-DSA 论文新增 5 幅 TikZ 可视化图示, 系统展示算法流程、系统架构与协议结构。内容涵盖 ML-DSA 签名流程图(Fiat-Shamir with Aborts 范式与拒绝采样循环), MQTT 发布-订阅架构与 ML-DSA 集成图示, 硬件平台架构图(STM32F407VG 与 ESP32 UART 互连), 软件分层架构栈(Application→MQTT/Crypto→FreeRTOS→HAL→Hardware), 以及 TLV 编码消息格式结构图。所有图示遵循 TikZ 相对定位设计原则确保嵌套环境兼容性。

下周计划: 1) 完善 Conclusion 章节撰写 2) 论文整体审校与修改

1 论文可视化元素扩展

完成了 Implementation Architecture 章节与 ML-DSA Algorithm 章节的 TikZ 图示扩展, 共新增 5 幅技术图示系统展示 ML-DSA 在 MQTT 环境中的部署架构与算法特征。图示设计遵循统一的风格规范:采用蓝色(`\color{blue}`)作为主色调增强视觉区分度;使用 TikZ 相对定位语法(`right=of`、`below=of`)确保图示在各种 LaTeX 环境(itemize、minipage、multicol 等)中的稳健渲染;避免使用 anchor 偏移量、绝对坐标与 xshift/yshift 修饰符以提升跨环境兼容性。

图示分布于论文核心章节:ML-DSA 签名流程图(fig:mldsa-signing), 展示 Fiat-Shamir with Aborts 范式的拒绝采样循环结构;MQTT 架构图(fig:mqtt-mldsa)位于 MQTT Protocol and Security Integration 小节, 阐明发布者-代理-订阅者消息流与加密操作分布;硬件架构图(fig:hardware-architecture)与软件架构图(fig:software-stack)位于 Implementation Architecture 章节, 分别展示计算与网络职责分离的硬件设计与模块化软件分层;消息格式图(fig:message-format)位于 Message Format and Signature Integration 小节, 图解 TLV 编码复合消息结构。

2 ML-DSA 签名流程图设计

设计了 ML-DSA 签名流程图展示 Fiat-Shamir with Aborts 范式核心结构。流程图采用紧凑垂直布局, 包含开始/结束节点(圆角矩形、灰色填充)、处理节点(矩形、白色填充)、NTT 操作节点(矩形、浅灰填充突出计算密集特性)与决策节点(菱形)。主流程从私钥sk与消息M输入开始, 经密钥展开(Expand Key)、消息哈希($\mu \leftarrow H(M)$)、掩码向量采样(Sample $\boldsymbol{y}$)、NTT 变换($\hat{\boldsymbol{w}} \leftarrow \boldsymbol{A}\hat{\boldsymbol{y}}$)、挑战计算($c \leftarrow H(\boldsymbol{w}_1, \mu)$)、响应向量计算($\boldsymbol{z} \leftarrow \boldsymbol{y} + c\boldsymbol{s}_1$), 至范数检验决策节点($\|\boldsymbol{z}\|_\infty < \gamma_1 - \beta$)。

拒绝采样循环通过决策节点右侧分支实现, “No”路径返回至 Sample $\boldsymbol{y}$节点形成闭环, 标注“4–5 iter.” 表示期望迭代次数;决策节点下方 “Yes” 路径通向签名输出节点。关键性能标注包括:NTT 节点左侧“60–70% cost”说明 NTT 操作占签名计算 60-70% 开销;Sample 节点右侧“4–5 iter.” 标注期望拒绝采样迭代次数。图示尺寸控制在单栏宽度内, 节点间距 0.55cm 确保紧凑布局同时保持可读性。

3 MQTT 架构与消息格式图示

设计了 MQTT 发布-订阅架构图展示 ML-DSA 签名集成于 IoT 消息流的完整路径。架构图采用水平三节点布局:Publisher(IoT Sensor)、Broker(Route)、Subscriber(Gateway), 通过 PUBLISH 与 FORWARD 箭头连接表示消息流向。各端点下方标注加密操作节点:Publisher 下方 “Sign (657–1150 ms)” 表示签名延迟范围(ML-DSA-44 至 ML-DSA-87), Subscriber 下方

“Verify (416–717 ms)”表示验证延迟范围。Broker 上方消息结构框展示复合消息组成:Payload 10–100 B 与 Sig. 2.4–4.6 KB，直观呈现签名数据相对载荷的尺寸主导地位。端点两侧标注密钥符号(sk、pk)表示私钥与公钥分布。

TLV 编码消息格式图采用水平字段链布局，各字段以紧邻矩形呈现:Type(1B)、Len(2B)构成 Header 区域;Payload(10–100 B)为应用数据区域;Alg(1B)、Key(2B)、Time(4B)、Len(2B)构成 Sig. Metadata 区域;Signature(2.4–4.6 KB)为签名数据区域(深色填充突出尺寸主导)。字段下方使用花括号分组标注 Header 与 Sig. Metadata 区域，上方标注“Data”与“Dominates size”说明功能与尺寸特征，顶部跨越式标注“Total message: 2.4–4.7 KB”显示完整消息尺寸范围。

4 硬件与软件架构图设计

设计了硬件平台架构图展示加密计算与网络协议处理的职责分离设计。架构图采用双核心水平布局:左侧 STM32F407VG 节点(ARM Cortex-M4F、168 MHz、1 MB Flash、192 KB SRAM)负责加密操作(Crypto Operations: ML-DSA Sign/Verify)，右侧 ESP32 节点(WiFi 802.11n、TCP/IP Stack)负责网络协议(Network Protocol: MQTT Transport)。双向箭头标注“UART 115.2k”连接两核心表示串口互连。外围组件包括:左侧 Sensors(ADC/I2C)通过箭头连接 STM32 输入，右侧 WiFi Network 通过箭头连接 ESP32 输出;下方电源子系统 3.3V Regulator 与 INA219 Current 传感器节点以虚线连接表示供电与能耗监测。

软件分层架构图采用垂直栈式布局展示五层模块化设计。顶层 Application Layer(Publish/Subscribe Workflows, Sensor Data Processing)为应用逻辑层;第二层并列 MQTT Client(Paho Embedded C、QoS 0/1/2)与 ML-DSA Crypto(pqm4 Library、Sign/Verify/KeyGen)分别处理协议与加密;第三层 FreeRTOS(Task Scheduling, Queues, Synchronization)提供实时操作系统支持;第四层 ARM Cortex-M4 HAL(Peripheral Access, Clock Config, Interrupts)实现硬件抽象;底层 Hardware(STM32F407VG 规格)为物理硬件。各层采用渐进深色填充区分层级，侧边标注 Network API 与 Crypto API 说明接口边界，顶层至第二层的箭头表示应用层对协议层与加密层的调用依赖。