# 周报

2025-12-15

# 本周研究摘要

## 为 ML-DSA 论文新增 5 幅 TikZ 可视化图示

- 系统展示算法流程、架构与协议结构

# ML-DSA 签名流程图

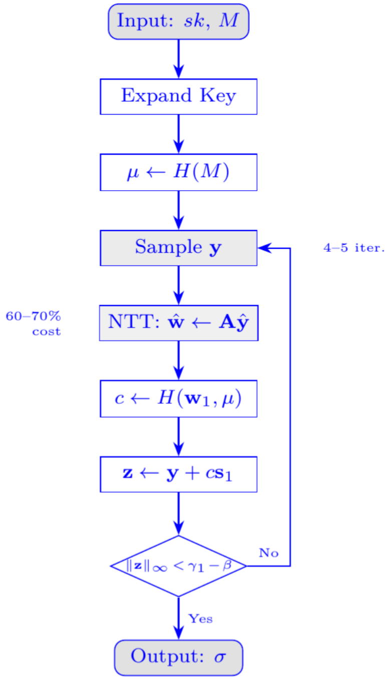

Input: $sk$, $M$
Expand Key
$\mu \leftarrow H(M)$
Sample $\mathbf{y}$
4–5 iter.
60–70% cost
NTT: $\hat{\mathbf{w}} \leftarrow \mathbf{A}\hat{\mathbf{y}}$
$c \leftarrow H(\mathbf{w}_1, \mu)$
$\mathbf{z} \leftarrow \mathbf{y} + c\mathbf{s}_1$
$\|\mathbf{z}\|_\infty < \gamma_1 - \beta$
No
Yes
Output: $\sigma$

**Figure 1:** ML-DSA signing procedure with Fiat-Shamir with Aborts. The rejection sampling loop (4–5 expected iterations) and NTT operations (60–70% of cost) are primary performance bottlenecks.

# MQTT 架构图

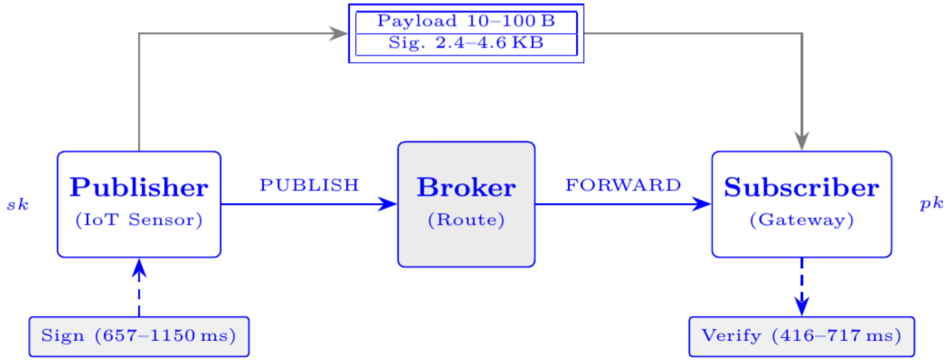


**Figure 2:** MQTT publish-subscribe architecture with ML-DSA integration. Publishers sign sensor data, transmit signed payloads through the broker, and subscribers verify authenticity. Signatures (2.4–4.6 KB) dominate message size relative to payloads (10–100 B).

# 硬件平台架构图

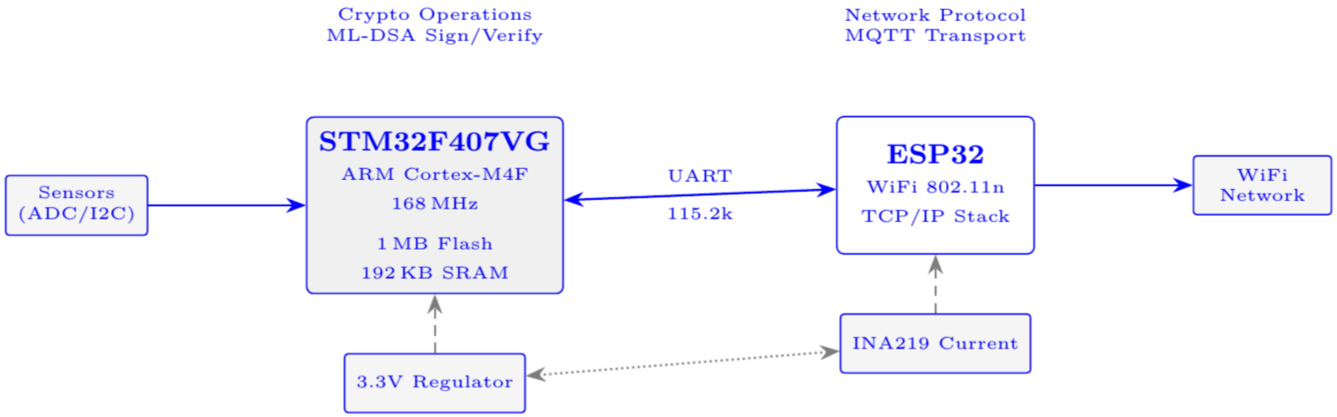


**Figure 3:** Hardware platform architecture with ARM Cortex-M4 microcontroller (STM32F407VG) for cryptographic computation and ESP32 wireless module for network protocol handling. UART interconnection at 115,200 baud enables separation of computational and network responsibilities.

# 软件分层架构图

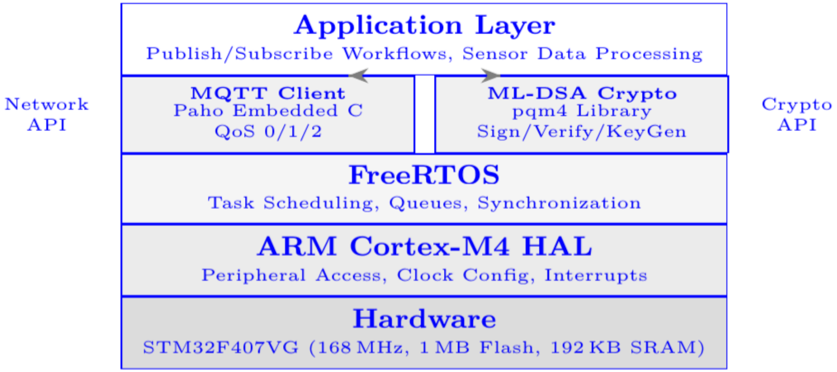
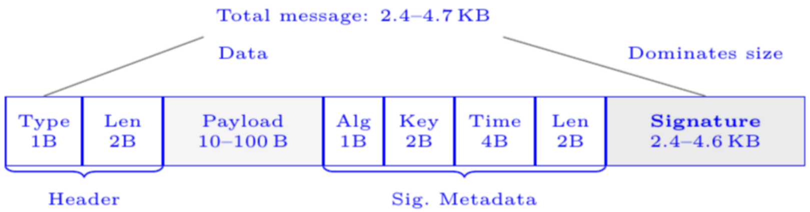

Application Layer
Publish/Subscribe Workflows, Sensor Data Processing
Network API
MQTT Client
Paho Embedded C
QoS 0/1/2
ML-DSA Crypto
pqm4 Library
Sign/Verify/KeyGen
Crypto API
FreeRTOS
Task Scheduling, Queues, Synchronization
ARM Cortex-M4 HAL
Peripheral Access, Clock Config, Interrupts
Hardware
STM32F407VG (168 MHz, 1 MB Flash, 192 KB SRAM)

**Figure 4:** Layered software architecture separating application logic, protocol handling (MQTT), cryptographic operations (ML-DSA), real-time operating system (FreeRTOS), and hardware abstraction (HAL). This modular design enables independent optimization of cryptographic and network components.

# TLV 消息格式图



Total message: 2.4–4.7 KB

Data

Dominates size

Type 1B

Len 2B

Payload 10–100 B

Alg 1B

Key 2B

Time 4B

Len 2B

**Signature** 2.4–4.6 KB

Header

Sig. Metadata

**Figure 5:** Composite MQTT message format with TLV encoding. Fixed-size header (3 bytes) and signature metadata (9 bytes) frame the variable-length payload and ML-DSA signature. Signature data (2,420–4,627 bytes) dominates total message size for typical IoT payloads (10–100 bytes).

# 总结

# 下周计划

论文完善：

- 完善 Results 章节实验数据
- 补充 Conclusion 章节撰写

# 老师评语

**你这图标蓝是给我看证明做了修改是不？如果是这样可以，否则是不能标蓝，就用黑白图。**

是的，标蓝色表示本周修改。

**再个论文长度现在已经 30 页了，即使是会议这也基本到极限长度了，注意精简语言突出重点，不冗余**

后精简部分章节，控制论文长度。