**Lightweight Swarm Attestation: a Tale of Two LISA-s**

Xavier Carpent\(^1\), Karim ElDefrawy\(^2\), Norrathep Rattanavipanon\(^1\) and Gene Tsudik\(^1\)

\(^1\)University of California, Irvine and \(^2\)SRI International

---

### Contributions

- Define a new metric that captures the type of information offered by a swarm attestation technique.
- Construct two practical attestation protocols with different QoSA features and communication and computation complexities.
- Investigate the impact of proposed protocols on the underlying security architecture.
- Assess their performance using the open-source Common Open Research Emulator (CORE) [1].

### Security Architecture

A swarm device adheres to SMART+ ([4], [3]) architecture. Key aspects are as follows:

- **AttCode** in ROM does not leak info.
- Execution of **AttCode** is atomic and complete.
- A key is stored in ROM and can only be read from within **AttCode**.
- A fixed-size block of secure RAM.

### Comparison

- **LISA** - Asynchronous
  - Minimal change from single-prover RA
  - Device collaboration only for propagating attestation requests and reports

- **LISA** - Synchronous
  - Aggregate many reports into a single report
  - Wait for all children’s reports before constructing own report

### Experimental Results

- **Attestation Runtime:** **LISA** is better.
- **Bandwidth Usage:** **LISAs** is better.

### Conclusion

This paper brings swarm RA closer to reality by designing two simple and practical protocols: **LISAs** and **LISA**s. To analyze and compare multiple protocols, we introduced a new metric, called Quality of Swarm Attestation (QoSA) which captures the type of information offered by swarm RA.

### References