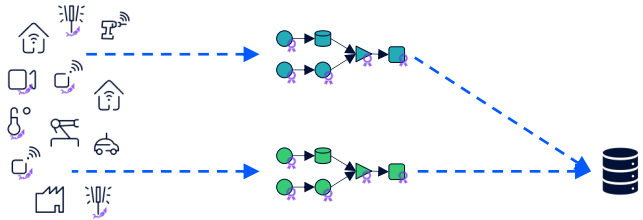
zkStream: a framework for trustworthy stream processing

A **trustworthy** stream processing framework, relying on two ingredients:

- **Signatures** on sensor inputs
- **Zero-Knowledge Proofs** for operator code

in an **architecture** that supports typical **streaming features** and with optimized **gadgets for aggregation operations**.



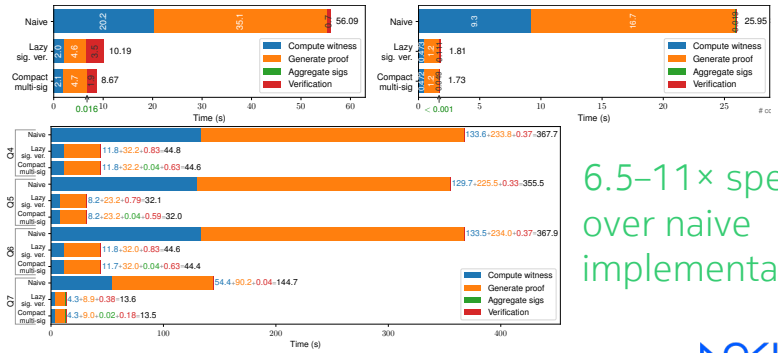
Optimizations:

1. **Lazy signature verification**
2. **Compact multi-signatures**

to make this feasible for practical applications.

Guarantees:

- ✓ **Confidentiality**: Data owner does not leak sensor data nor intermediate results.
- ✓ **Computational integrity**: Data consumer knows algorithm ran as specified.
- ✓ **Provenance**: Inputs are guaranteed to come from trusted sensors.



6.5–11× speed-up over naive implementation

