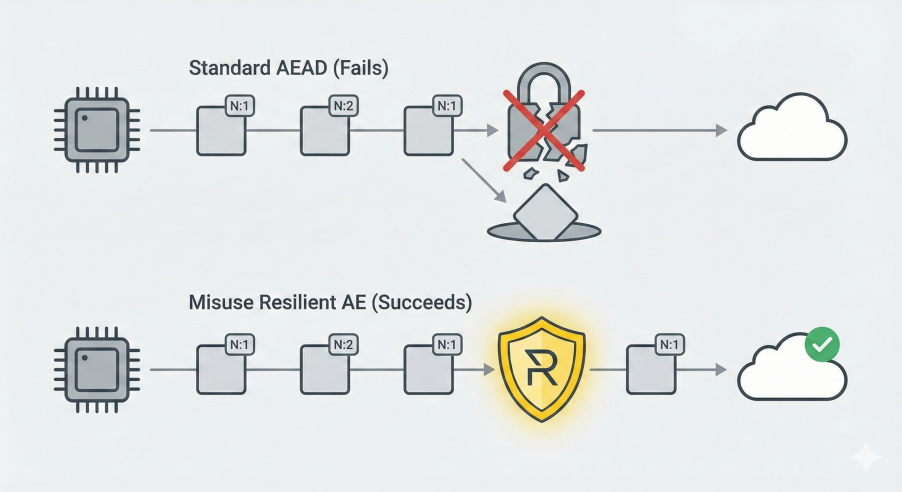
Nonce Misuse Resistance in Out-of-Order and Lightweight Communications



Modern embedded and cyber-physical systems increasingly require confidentiality and integrity for short, frequent messages sent over unreliable links. In practice, the assumptions behind standard AEAD are often violated: devices reboot and counters reset, randomness at boot can be weak, links drop or reorder packets, and timing jitter becomes a safety and availability concern. As a result, engineers either deploy schemes that fail catastrophically under nonce reuse, or disable security because they cannot afford buffering and full message verification. This project aims to design and evaluate a new authenticated encryption mode tailored to these operational realities. The intern will help develop a construction that provides bounded damage under nonce reuse, supports online verification so receivers can detect tampering early, and remains robust under packet loss, duplication, and reordering. The work will balance provable security foundations with deployability on constrained hardware. A key goal is to produce an end-to-end proof of feasibility on real devices, rather than stopping at a paper design.

During the internship, the intern will first map the precise gap between existing AEAD guarantees and the requirements of real-time, lossy, reset-prone deployments. The intern will then implement and evaluate candidate constructions that combine bounded damage under nonce reuse with online verification, so a receiver can detect tampering early without buffering the full message. A core output is an end-to-end feasibility demonstrator on real devices, where the intern measures latency distribution, jitter, energy, code size, RAM footprint, and behaviour under induced resets and packet loss. The evaluation will include careful comparison against representative baselines used in practice, such as AES GCM, AES CCM, ChaCha20 Poly1305, and at least one misuse-resistant baseline, such as an SIV-style construction.

Practicalities

Supervisors:	Sayon Duttagupta	sayon.duttagupta@esat.kuleuven.be	office B01.17
	Amit Singh Bhati	amitsingh.bhati@3milabs.tech	office B01.17

Nature of the work:	20% theoretical work, 80% software (implementation on embedded devices)
Number of students:	1