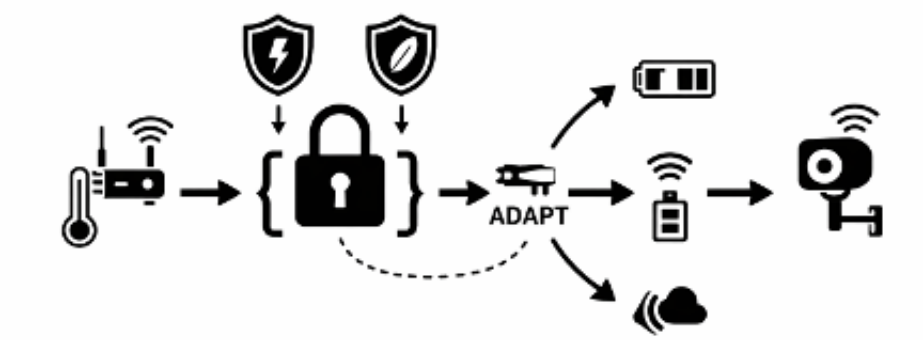
Adaptive Lightweight Cryptography for Resource-Constrained IoT Devices



Many IoT and edge devices operate under strict constraints in terms of processing power, memory, and energy consumption. At the same time, these devices often exchange sensitive data or control signals that require strong cryptographic protection. Traditional cryptographic protocols designed for general computing systems can introduce significant overhead, making them difficult to deploy on constrained devices.

To address this challenge, lightweight cryptographic algorithms have been developed specifically for embedded systems. Recent standardization efforts, such as the NIST lightweight cryptography competition, have introduced new algorithms designed for efficient operation on constrained hardware. However, most current implementations rely on static cryptographic configurations, where the same algorithm and security parameters are used regardless of the system's context or threat level.

The goal of this thesis is to investigate adaptive lightweight cryptographic mechanisms for IoT and edge environments. The student will explore approaches that dynamically adjust cryptographic parameters or algorithms based on device capabilities, communication conditions, or security requirements. A prototype implementation will be developed to evaluate how adaptive cryptography can balance security, performance, and energy efficiency in constrained systems.

Practicalities

Promotor:	Bart Preneel		
Daily supervisor:	Farhad Aghili	farhad.aghili@sirris.be	office Sirris-Heverlee
	Laurens Le Jeune	laurens.lejeune@sirris.be	office Sirris-Heverlee
	Roozbeh Sarenche	roozbeh.sarenche@kuleuven.be	office B01.13
Nature of the work:	30% literature, 30% theoretical work, 40% implementation		
Number of students:	1		

 © 2026 – 2027 COSIC