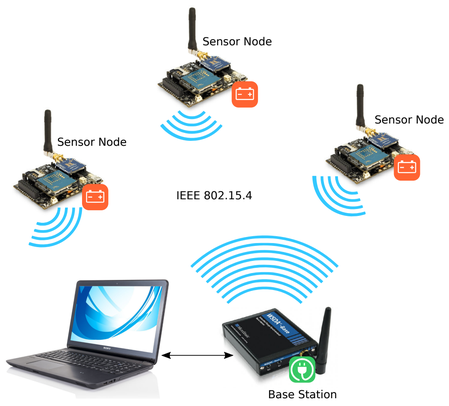
# Lightweight Cryptography for the IoT

Carlos Andres Lara-Niño, (carlos.lara@cinvestav.mx)

## The IoT ecosystem

The Internet of Things (IoT) uses a series of underlying technologies which focus on particular tasks:

- Wireless Sensor Networks
- Radiofrequency Identification
- Supervisory Control and Data Acquisition
- Machine to Machine communications

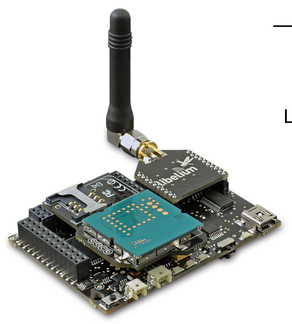



## Wireless Sensor Networks (WSN)

Networked *sensor nodes*, which are devices of restricted capabilities, often operate with sensitive information that ought to be obfuscated. In some cases, the sheer information volume can provide insights on the user's behavior. Security services are required for protecting these data.

## Sensor Nodes (motes)

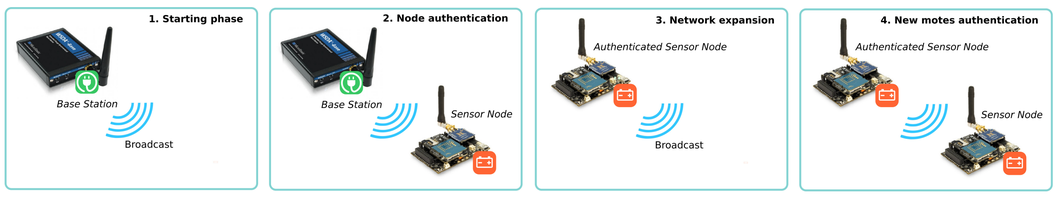
The characteristics of WSN motes impose restrictions on the design of their underlying algorithms.



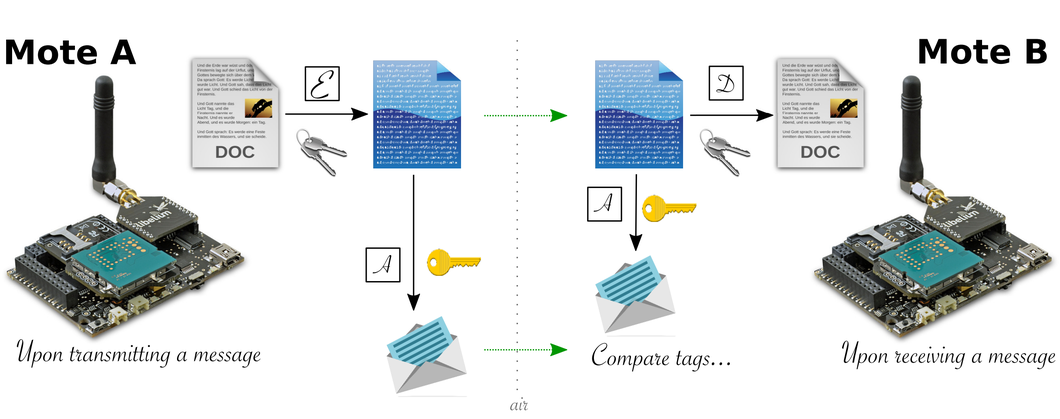
| Characteristics | Which cause that |
|---|---|
| Reduced physical size | The implementation **size** must be reduced |
| Limited processing power | The **efficiency** and **performance** of the algorithms must be improved |
| Reduced bandwidth | The amout of **transmitted data** must be limited |
| Battery powered | The **energy consumption** must be low |
| Deployed in unsecure environments | **Security services** need to be provided |

## Securing an WSN

A WSN can be formed parting from the *base station* as motes join the network.




A secure channel can provide different security services. These generally include **confidentiality**—by using ciphers $(\mathcal{E}, \mathcal{D})$—, and **integrity or authentication**—by adding an authentication tag to the message $(\mathcal{A})$.

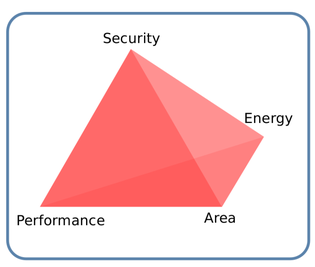



## Challenges:

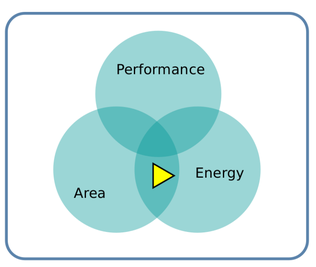
- The encryption, decryption, and authentication functions must be efficient!
- The shared keys required must be obtained somehow!

## Lightweight Cryptography

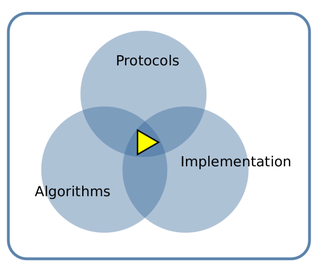
Is the set of algorithms and techniques tailored for providing security services to highly constrained devices.




Development trade-offs.




Development goals.




Solution approaches.

Lightweight algorithms must offer adequate **security** levels with balanced tradeoffs regarding **runtime** or processing power, **hardware** usage, **power** dissipation, **energy** consumption, and **bandwidth**.

### Symmetric algorithms

**Types:** Block ciphers, Hash functions, MAC functions, Authenticated cihpers.
Characteristics:

- A single *key* is used to 'protect' and to 'retrieve' the data.
- This key is said to be *symmetric*.
- Designed to process large volumes of data.
- Rely on data transformations such as permutations and substitutions.

**Examples:** PRESENT, SIMON, SPECK, Midori, GIFT, QUARK, SPONGENT, PHOTON, GLUON, Hummingbird, ALE, FIDES, APE.

### Asymmetric constructions

**Types:** Ciphers, Digital Signatures, Key Exchange, Key Encapsulation.
Characteristics:

- The key used to 'protect' the data differs from the one used to 'retrieve' it.
- This key is said to be *asymmetric*.
- Designed to process small messages.
- Rely on arithmetic transformations which are costly to perform.

**Examples:** Elliptic Curve Cryptography (TinyECCK, MicroECC, MoTE-ECC).

## Realization costs

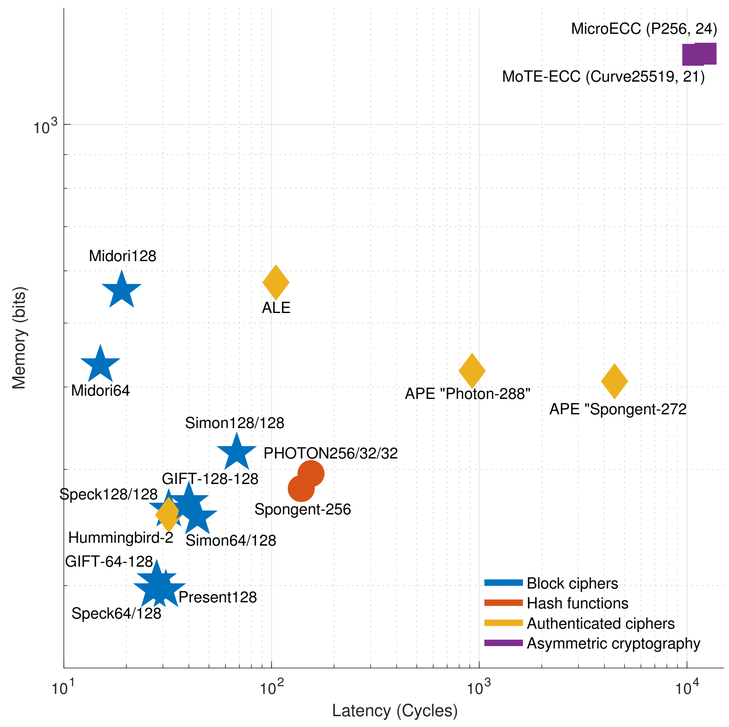



**Figure:** Storage and latency requirement for popular lightweight algorithms with 128-bit security.

## Further reading


- "Report on Lightweight Cryptography," NISTIR 8114, March 2017, [DOI] 10.6028/NIST.IR.8114
- "Energy and Area Costs of Lightweight Cryptographic Algorithms for Authenticated Encryption in WSN," in *Security and Communication Networks*, vol. 2018, Article ID 5087065, 14 pages, 2018.
- "Elliptic Curve Lightweight Cryptography: A Survey,in *IEEE Access*, vol. 6, pp. 72514-72550, 2018.


Cinvestav Tamaulipas