LIGHTWEIGHT CRYPTOGRAPHY FOR RESOURCE-CONSTRAINED DEVICES

Andrea Visconti

Università degli Studi di Milano

Resource-Constrained Devices are widely used in specific context such as sensor networks, healthcare, Internet of Things (IoT), and so on. In order to carry out some activities, these devices (1) have to be highly interconnected and (2) need to offload the execution and workload to powerful computers. Indeed, they have to address the well-known physical constraints of smart devices such as limited processing capabilities, limited battery lifetime, and limited storage capacity. Unfortunately, current cryptographic standards were developed to exploit the computational resources of desktops and servers, therefore usually do not fit into resource-constrained devices. Since 2007 several lightweight ciphers have been proposed – to date none of them is considered an international standard – and in 2018 NIST initiated a process of evaluation and standardization of lightweight cryptographic algorithms. In this talk we will introduce the issues addressed by researchers and some ciphers published in the literature.