انجمن رمز ایران
Iranian Society of Cryptology

Lightweight/Low-Energy/Low-Latency Cryptography

We are surrounded by yet-rapidly-increasing embedded devices, as a trend of ubiquitous computing, in which information related to our everyday activities are processed. Such devices often communicate and store our private information, ignoring the fact that this technology has not been necessarily designed with security in mind. Naturally, cryptography is the first choice to fulfill the essential requirements with respect to confidentiality, privacy protection, and many other security objectives. Thanks to hard mathematical problems, cryptography often achieves the required strength. On the other hand, cryptographic algorithms require highly intensive computations, which leads to the main restriction for their wide application in embedded devices. This fact motivated the field of lightweight cryptography, and several schemes and algorithms have been proposed in public literature to ease their integration into embedded systems. Further, by increasing the number of different applications - where cryptography is required - more criteria are added to the desired algorithms. Amongst them are: i) low-power and low-energy features which are essential for pervasive (usually battery-operated) applications, e.g., Internet of Things, and ii) low-latency feature that has become a major challenge in applications with disk/memory encryption feature. In this talk, an overview about the activities in these areas of research is given. We will discuss on a couple of practices for hardware design of lightweight, low-energy, and low-latency cryptographic primitives, that hopefully clarifies the gaps which still need to be filled.