# The Design and Analysis of Lightweight Block Ciphers

Muhammad Reza Z'aba

Network Security Lab
MIMOS Berhad

**Abstract.** In recent years, research into the design and analysis of lightweight block ciphers has received significant attention by the cryptographic community. Its growth is spurred by the proliferation of ubiquitous devices such as RFID tags and wireless sensor nodes. Such devices have physical constraints such as small area, memory and limited power supply. General-purpose block ciphers such as the Advanced Encryption Standard (AES) are not suitable to be implemented in these devices due to their high hardware footprint. In this talk, we review the design choices made by the designers of lightweight block ciphers and their implications to aspects such as security, efficiency and area requirements.