Abstract: Internet of Things (IoT) consists of low-cost general purpose devices with sensing, actuating, computation, communication and storage capabilities. The challenge becomes: How do we handle (communicate, store, process and secure) the data at this scale using resource limited endpoints? For example, a vast majority of IoT/Mobile devices have a camera attached, and bulky image/video transfers have been estimated to comprise 80% of the Internet traffic by 2019. Technology giants have been advancing communication, storage and processing capacity of their products to keep up with the demand. However, deployment of a new technology may need to wait until the existing one is decommissioned.

The project investigates the problem of combining both compression and encryption so it is possible to achieve both very effective compression (close to optimal) and authenticated encryption. A trivial solution would be to concatenate both algorithms - first we compress and then encrypt, but it is relatively costly. Hence, the objective of this project is to incorporate encryption in compression algorithm - to reduce hardware cost, time and energy consumption. This can be done using "free parameters" of compression, which can be used as a cryptographic key that switches on or off carefully chosen compression parameters. The resulting algorithm is called ComCrypt (a shorthand for compression+encryption). The project applies the ANS compression invented by Jarek Duda who is one of the investigators in this project. The ANS compression has been adopted as a standard by big IT companies as Apple, Facebook and Google, also in Linux kernel and was standardized for HTTP and MIME protocols.