Abstract:

The NTRU cryptosystem is one of the main alternatives for practical implementations of post-quantum, public-key cryptography. In this work, we analyze the feasibility of employing the NTRU encryption scheme, NTRUEncrypt, in resource constrained devices such as those used for Internet-of-Things endpoints. We present an analysis of NTRUEncrypt’s advantages over other cryptosystems for use in such devices. We describe four different NTRUEncrypt implementations on an ARM Cortex M0-based microcontroller, compare their results, and show that NTRUEncrypt is suitable for use in battery-operated devices. We present performance and memory footprint figures for different security parameters, as well as energy consumption in a resource constrained microcontroller to backup these claims. Furthermore, to the best of our knowledge, in this work we present the first time-independent implementation of NTRUEncrypt.