Cryptology ePrint Archive: Report 2012/730

Twisted Edwards-Form Elliptic Curve Cryptography for 8-bit AVR-based Sensor Nodes

Dalin Chu and Johann Gro{\ss}sch{\"a}dl and Zhe Liu

Abstract: Wireless Sensor Networks (WSNs) pose a number of unique security challenges that demand innovation in several areas including the design of cryptographic primitives and protocols. Despite recent progress, the efficient implementation of Elliptic Curve Cryptography (ECC) for WSNs is still a very active research topic and techniques to further reduce the time and energy cost of ECC are eagerly sought. This paper presents an optimized ECC implementation that we developed from scratch to comply with the severe resource constraints of 8-bit sensor nodes such as the MICAz and IRIS motes. Our ECC software uses Optimal Prime Fields (OPFs) as underlying algebraic structure and supports two different families of elliptic curves, namely Weierstra{\ss}-form and twisted Edwards-form curves. Due to the combination of efficient field arithmetic and fast group operations, we achieve an execution time of $5.9 \cdot 10^6$ clock cycles for a full 160-bit scalar multiplication on an 8-bit ATmega128 microcontroller, which is 2.78 times faster than the widely-used TinyECC library. Our implementation also shows that the energy cost of ephemeral ECDH key exchange between two MICAz (or IRIS) motes amounts to only 38.7 mJ per mote (including radio communication). A mote with a standard AA battery pack could theoretically perform up to 174,278 ECDH key exchanges before running out of energy.

Category / Keywords: implementation / elliptic curve cryptosystem

Date: received 31 Dec 2012

Contact author: johann groszschaedl at uni lu