Techniques for Low Power ECC in Embedded Systems

Ben Terner

1 Abstract

Elliptic curves offer strong computational security for public key cryptography while requiring far smaller keys than RSA. In a world where interconnected devices trend toward miniaturization and security threats become more frequent, elliptic curves are especially appealing to implementors of embedded devices with strong security requirements and few computing resources.

This survey will investigate techniques for implementing elliptic curve cryptography in embedded systems. In particular, we will investigate algorithmic approaches to low power elliptic curve cryptography. Techniques used towards this end require efficient multiplication and inversion of elements within a finite field [2] [5], and extend to efficient point multiplication [2] and [3] and parallelized modular operations on multiple cores [1].

References

[1] J. Fan, K. Sakiyama, and I. Verbauwhede, "Elliptic curve cryptography on embedded multicore systems," *Design Automation for Embedded Systems*, vol. 12, no. 3, pp. 231–242, 2008.

[2] R. Afreen and S. Mehrotra, "A review on elliptic curve cryptography for embedded systems," *arXiv preprint arXiv:1107.3631*, 2011.

[3] J. Dams, "Portable elliptic curve cryptography for medium-sized embedded systems," *University of Vaasa, Faculty of Technology Department of Computer Science, Vaasa*, 2008.

[4] A. Liu and P. Ning, "Tinyecc: A configurable library for elliptic curve cryptography in wireless sensor networks," in *Information Processing in Sensor Networks, 2008. IPSN'08. International Conference on.* IEEE, 2008, pp. 245–256.

[5] E. Öztürk, B. Sunar, and E. Savaş, "Low-power elliptic curve cryptography using scaled modular arithmetic," in *Cryptographic Hardware and Embedded Systems-CHES 2004.* Springer, 2004, pp. 92–106.