Cryptology ePrint Archive: Report 2011/654

Elliptic Curve Cryptography in JavaScript

Laurie Haustenne and Quentin De Neyer and Olivier Pereira

Abstract: We document our development of a library for elliptic curve cryptography in JavaScript. We discuss design choices and investigate optimizations at various levels, from integer multiplication and field selection to various fixed-based EC point multiplication techniques. Relying on a small volume of public precomputed data, our code provides a speed-up of a factor 50 compared to previous existing implementations. We conclude with a discussion of the impact of our work on a concrete application: the Helios browser-based voting system.

Category / Keywords: implementation /

Date: received 3 Dec 2011

Contact author: olivier pereira at uclouvain be