Meeting: 998, Houston, Texas, SS 17A, Special Session on Coding Theory and Cryptography

998-11-381 **Jerome A. Solinas** (jasolin@orion.ncsc.mil), National Security Agency, Suite 6511, 9800 Savage Rd., Ft. Meade, MD 20755-6511. *Custom Elliptic Curves for Fast Public-Key Cryptography.* Preliminary report.

The basic operation in elliptic curve cryptography is scalar multiplication, *i.e.* taking a large multiple of a given point. The efficiency of elliptic curve based public key protocols depends heavily on that of scalar multiplication. The best general-purpose algorithm for this operation is a binary method based on an optimal signed binary expansion of the coefficient. If 4 extra coordinates are precomputed and stored, this method can perform a k-bit scalar multiplication with k point doublings and $\sim k/4$ point additions. With 6 extra coordinates, the number of point additions drops to $\sim 2k/9$.

We discuss a family of curves defined over $\mathbb{F}_p$ (p prime) on which scalar multiplication is significantly faster than in the general case. The method requires precomputing and storing 5 extra coordinates and performs a k-bit scalar multiplication with $k/2$ point doublings and $\sim k/4$ point additions. The curves have complex multiplication by a cube root ω of unity and an additional property that allows the ordinary scalar multiplication to be replaced by the computation of an expression of the form $aP + bQ$. The latter computation is carried out using a recently discovered optimization of the signed binary technique. We discuss the occurrence of these particular curves, and present examples of various sizes of cryptographic interest. We also discuss the performance of the algorithm on these curves. (Received March 02, 2004)