1016-11-253 **Daniel J. Bernstein*** (djb@math.uic.edu), PMB 346, 2038 N. Clark Street, Chicago, IL 60614.

Differential addition chains.

Differential addition chains (also known as strong addition chains, Lucas chains, and Chebyshev chains) are addition chains in which every sum is already accompanied by a difference. Low-cost differential addition chains are used to efficiently exponentiate in groups where the operation $a, b, a/b \mapsto ab$ is fast: in particular, to perform x-coordinate scalar multiplication $P \mapsto mP$ on an elliptic curve $y^2 = x^3 + Ax^2 + x$. Similarly, low-cost *two-dimensional* differential addition chains are used to efficiently compute the function $P, Q, P - Q \mapsto mP + nQ$ on an elliptic curve. I will present two new constructive upper bounds on the costs of two-dimensional differential addition chains. My new "binary" chain is very easy to compute and uses 3 additions (14 field multiplications in the elliptic-curve context) per exponent bit, with a uniform structure that helps cryptographers protect against side-channel attacks. My new "extended-gcd" chain takes more time to compute, does not have the uniform structure, and is not easy to analyze, but experiments show that it takes only about 1.77 additions (9.97 field multiplications) per exponent bit. (Received February 14, 2006)