1016-11-137 **Andy Chan**, **Vassil Dimitrov**, **Laurent Imbert** and **Michael Jacobson***
(jacobs@cpsc.ucalgary.ca), Department of Computer Science, University of Calgary, 2500 University Drive NW, Calgary, Alberta T2N 1N4, Canada. *Improved Point Multiplication on Koblitz Curves Using Double-base Expansions.*

Point multiplication, adding a point to itself k times, is a central operation of elliptic curve cryptosystems. Koblitz curves are a special class of curves defined over $GF(2^m)$ for which the usual "double-and-add" algorithm can be improved significantly by replacing the point doublings with applications of the Frobenius map. The key to this technique is computing a τ-adic expansion of the integer k, where τ is a root of the characteristic polynomial of the Frobenius. The resulting point-multiplication algorithms require a number of point additions that is linear in $\log k$.

In this talk, we describe how recent ideas involving double-base expansions of integers can be applied in this context to obtain a point-multiplication algorithm that, at least empirically, requires a sub-linear number of point additions. The key to our improvement is an algorithm that expresses k as a sum of terms of the form $\pm\tau^a(\tau-1)^b$. We describe our method and present empirical results demonstrating its efficiency as compared to existing techniques. We also present data indicating that the number of point additions required is indeed sub-linear and discuss the state of our efforts to prove that sub-linear expansions of this form exist for any integer k. (Received February 08, 2006)