1116-11-1345 **Ping Ngai Chung*** (briancpn@math.uchicago.edu), **Craig Costello** and **Benjamin Smith**.
Fast, uniform, and compact scalar multiplication for elliptic curves and genus 2 Jacobians with applications to signature schemes. Preliminary report.

We introduce a method to compute multi-dimensional scalar multiplication on a given one or two dimensional abelian variety using pseudo-multiplication algorithms on its Kummer variety (the abelian variety modulo the inverse map). The latter is typically more efficient and is exception-free, both desirable for cryptographic protocols for speed and security reasons, yet the former is required for some cryptographic protocols, for instance digital signatures. As an application, we introduce an efficient, uniform and compact digital signature scheme on genus 2 curves, using the efficient pseudo-addition formulae on its Kummer surface first introduced to cryptography by Pierrick Gaudry in 2007. (Received September 18, 2015)