Atelier « La sécurité informatique et la cryptographie »
12–16 avril 2010

**Workshop on Computer Security and Cryptography**
**April 12–16, 2010**

# Pairing-friendly composite order bilinear groups

Alice Silverberg

Department of Mathematics
University of California, Irvine
Rowland Hall
Irvine, CA 92697-3875
USA

asilverb@math.uci.edu

---

*In joint work with Dan Boneh and Karl Rubin*, we apply the Cocks–Pinch method to obtain pairing-friendly composite order groups with prescribed embedding degree associated to ordinary elliptic curves, and we show that new security issues arise in the composite order setting.