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

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

Breaking ECC2K-130 on cell processors and GPUs

Peter Schwabe

Department of Mathematics and Computer Science
Eindhoven University of Technology
Den Dolech 2
5600 MB Eindhoven
THE NETHERLANDS

peter@cryptojedi.org

In 1997, Certicom published a list of elliptic-curve discrete-logarithm challenges. Some excercise challenges were soon solved ; currently all challenges over fields of 109 bits or less but none of the larger challenges have been solved.

A cluster of research groups is currently trying to solve the specific challenge ECC2K-130 which consists in solving the ECDLP on a Koblitz curve over a 131-bit binary field. In my talk I will give the necessary background on the iteration function used in the parallel Pollard rho algorithm and then focus on platform specific optimization techniques for Cell processors and (NVIDIA) graphics processing units.