

ECC 2005 – Rump Session
Monday, September 19th, 2005

19:00	Nigel Smart	More pairing stuff
19:05	Roberto Avanzi	Fast binary field arithmetic for low genus HECC
19:10	Nicolas Thériault	Efficient implementation of low genus binary HECC
19:20	Roberto Avanzi	Cryptography on a Shoestring
	BREAK	
19:45	Announcements	Tanja Lange, Roberto Avanzi, Manfred Lochter
19:55	Colm Ó hÉigenartaigh	Speeding Up Pairing Computation
20:00	Daniel J. Bernstein	Is $2^{255} - 19$ big enough?
20:05	Nigel Smart	An Xmas Treat
20:10	Martijn Stam	Pairing based banana routing in the standard model