DAN BROWN, Certicom (subsidiary of Research in Motion)
Cryptography in Diophantine Cloak

Some important cryptographic problems can be easily expressed as Diophantine problems: quite simply for public-key cryptography, or using the notion of straight line program for symmetric-key cryptography. This talk will review some theorems about solving the factoring and Rivest–Shamir–Adleman (RSA) problems using a straight line program. This talk will also relate the security U.S. Federal Information Processing Standard (FIPS) 186-3 Digital Signature Algorithm (DSA) to the well-known discrete logarithm problem, and a not-so-well-known problem Diophantine problem: the one-up problem.