Dan Bernstein

Edwards coordinates for elliptic curves

The standard elliptic-curve addition laws are annoying! They force the user to distinguish doublings from generic additions; they have other exceptional cases; and they aren't very fast. One can eliminate the doubling distinction, and with more work one can eliminate all of the exceptional cases over a finite field, but the resulting addition laws are even slower. I'll explain a new coordinate system that eliminates the need for the doubling distinction, that eliminates all of the exceptional cases for some curves, and that achieves remarkable speed. I'll then discuss applications to elliptic-curve cryptography. This is joint work with Tanja Lange.

Moti Yung

Cryptography and Virology Inter-Relationships

Cryptography can influence the design of computer viruses, and the existence of viruses, in turn, influences the way cryptographic systems should be designed. In this talk I will cover some of these inter-relationships between the two disciplines.