dr Robert Dryło
Instytut Matematyczny PAN

Konstruowanie krzywych eliptycznych dla zastosowań w kryptografii

Celem referatu jest omówienie metod konstruowania krzywych eliptycznych nad ciałami skończonymi o danym rzędzie oraz krzywych z małym stopniem zanurzeniowym, dla których można efektywnie obliczyć iloczyn Weila. Omówimy również wybrane protokoły oparte na krzywych drugiego typu, takie jak przydzielanie klucza publicznego na podstawie tożsamości (IBE) oraz podpisy cyfrowe.

Praca naukowa finansowana ze środków na naukę w latach 2008–2010 jako projekt rozwojowy Nr R00 0031 06.