dr Robert Dryło
IMPAN

Zastosowania w kryptografii krzywych eliptycznych i hipereliptycznych o małych stopniach zanurzeniowych

Dla krzywych eliptycznych i hipereliptycznych o dostatecznie małym stopniu zanurzeniowym można obliczyć iloczyny dwuliniowe Weila lub Tate. Od roku 2000 własność tę wykorzystuje się do tworzenia efektywnych protokołów kryptograficznych (m.in. krótkich podpisów cyfrowych lub szyfrowania opartego na tożsamości). Podstawowym problemem jest skonstruowanie odpowiednich krzywych, dla których można otrzymać bezpieczny i efektywny system.

Podczas referatu przedstawię krótkie wprowadzenie do tej dziedziny oraz nowe metody konstruowania odpowiednich krzywych.