WYKŁAD WYDZIAŁOWY

w ramach seminarium

ARYTMETYCZNA GEOMETRIA ALGEBRAICZNA

(organizatorzy: Grzegorz Banaszak, Piotr Krasoń)

Środa **21 marca 2018**, godz. **12:00**, sala **A1-33**

Wydział Matematyki i Informatyki UAM w Poznaniu

dr Janusz Szmidt

UAM Poznań

Wybór kryptograficznie bezpiecznych krzywych eliptycznych

Streszczenie: Krzywe eliptyczne nad ciałami skończonymi mają zastosowanie w konstrukcji protokołów klucza publicznego (wymiana kluczy kryptograficznych, podpis cyfrowy). Istnieją standardy krzywych eliptycznych, które zawierają ustalone krzywe. W zastosowaniach specjalnych (np. dla wojska) zalecany jest wybór własnych krzywych eliptycznych. W referacie przedstawione będą kryteria matematyczne wyboru bezpiecznych kryptograficznie krzywych eliptycznych. Ponadto omówione będą poglądy, czy standardy krzywych zostały wybrane tak, aby instytucje odpowiedzialne za ich wybór miały możliwość łamania protokołów opartych na tych krzywych.