Устименко Василь Олександрович

Професор, доктор фізмат наук

Інститут телекомунікацій та глобального інформаційного простору НАН України та Royal Holloway of University of London, UK

Алгебраїчна геометрія та нові алгоритми постквантової криптографії.

У доповіді будуть представлені групи перетворень векторного простору довільної розмірності, визначені через символічні обчислення з використанням комірок Шуберта проективної геометрії. Деякі модифікації цих перетворень у випадку скінченних полів великого розміру характеристики два дозволяють визначити квадратичні бієктивні відкриті ключі багатовимірної криптографії так, що обернені публічні перетворення мають великий поліноміальний ступінь. Також буде представлено симбіотичну комбінацію протоколу на основі цих груп із новим інструментом шифрування багатоваріантної криптографії.