Устименко Василь Олександрович
Професор, доктор фізмат наук
Інститут телекомунікацій та глобального інформаційного простору НАН України та Royal Holloway of University of London, UK

Проєктивні Геометрії, Постквантові Криптосистеми від багатьох змінних та схеми типу Ель Гамаля.

Анотація. Дослідження лінійних кодів, визначених у термінах скінчених проєктивних геометрій становлять традиційний напрямок у Теорії Кодування. Деякі застосування проєктивних геометрій до симетричної криптографії також розглядалися. Некомутативні групи та напівгрупи, визначені в термінах цих геометрій, можуть служити платформами протоколів постквантової криптографії. У доповіді ми пропонуємо ідею відкритих ключів багатовимірної криптографії, заданих квадратичними перетвореннями, згенерованими шляхами напідструктурах інцидентності проективної геометрії з вершинами з двох найбільших комірок Шуберта. Будуть запропоновані деякі схеми перетворення цих відкритих ключів у криптосистеми типу Ель Гамаля.

Projective Geometries, Postquantum Multivariate Cryptosystems and El Gamal type schemes.

Abstract. Studies of linear codes defined in terms of finite projective geometries form traditional direction in Coding Theory. Some applications of projective geometries to Symmetric Cryptography were considered. Noncommutative groups and semigroups defined in terms of these geometries can serve as platforms of protocols of Post Quantum Cryptography. In the talk we suggest an idea of public keys of Multivariate Cryptography given by quadratic transformations generated via walks on incidence substructures of projective geometry with vertexes from two largest Schubert cells. Some schemes of conversion of these public keys to El Gamal type cryptosystems will be proposed.