

Об'єктом дослідження є інформаційні процеси в системах криптографічного захисту.

Предметом дослідження є шифр HIGHT та його стійкість до диференціального криптоаналізу.

В роботі проводиться оцінювання стійкості ARX-шифрів до диференціального криптоаналізу на прикладі шифру HIGHT.