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

Предметом дослідження є симетричний шифр з автентифікацією PAES-8, атаки на основі диференціального криптоаналізу.

Метою даної роботи є дослідження шифру PAES-8, аналіз існуючих атак на нього та створення і реалізація нової атаки. Коректність та оцінка нової атаки була перевірена експериментально.

Науковою новизною даної роботи є створення нової атаки з кращими властивостями, ніж існуючі, а також певні запропоновані модифікації шифру, які роблять його невразливим до вказаної атаки.