Мета роботи — розробка нових моделей та методів, що зможуть зменшити складність диференціального криптоаналізу шляхом заміни складної задачі на більш легку із додатковими обмеженнями.

Об’єкт дослідження: інформаційні процеси в системах криптографічного захисту.

Предмет дослідження: рівняння першого степеня із різними алгебраїчними операціями та їх диференціальні властивості.

В роботі проведено детальний аналіз двох типів рівнянь, запропоновано ефективні алгоритми для обчислення диференціальних імовірностей операцій у них, описані обчислювальна складність та необхідна кількість пам'яті.

Отримані результати можуть бути застосовані для криптоаналізу блокових та потокових шифрів, геш-функцій, ARX-криптосистем та в інших криптографічних задачах.