АНАЛІЗ ТА ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ НОВИХ МЕТОДІВ ЕЛІПТИЧНОГО СКАЛЯРНОГО МНОЖЕННЯ

Танцура Д.В.
Науковий керівник – к.т.н., доцент Мельникова О.А.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Леніна,14, каф. БІТ, тел. (057) 702-14-25)

During realization of electronic digital signature (DSA) standards, using cryptotransformation in the groups of points of elliptic curves (EC), are more frequent than all used in the modern systems of defence of commercial and other valuable information.

При реалізації електронного цифрового підпису (ЕЦП) в сучасних системах захисту комерційної і іншої цінної інформації найчастіше використовуються стандарти, що використовують криптоперетворення в групах точок еліптичних кривих (ЕК). Одним з критичних параметрів при реалізації ЕЦП є час виконання криптоперетворень, яке визначається обчислювальною складністю операцій еліптичного скалярного множення.

Для зменшення часу криптоперетворень рекомендується використання нових методів скалярного множення точок а саме: метод подвоєння і складання (Double-and-Add method) і метод ділення та складання (Halve-and-Add method). Приведені вище методи засновані на побітовому переборі скаляра. Коли в скалярі зустрічається одиниця, в обох методах проводиться складання точок. Якщо в скалярі зустрічається нуль, то в першому методі проводиться подвоєння точки, а в другому – її ділення на два.

Проте, для методу ділення і складання перед використанням алгоритму, скаляр необхідно перетворити таким чином:

$$k = k_t 2^t + \ldots + k_1 t + k_0 \equiv k'_t / 2^t + \ldots + k'_1 / 2 + k'_0 (\mathrm{mod}\, n),$$

де:

$$2^t k \bmod n = k'_0 2^t + k'_1 2^{t-1} + \ldots + k'_t$$

Проведений аналіз дозволяє скоротити час виконання криптоперетворень еліптичного скалярного множення.