АНАЛИЗ ЭФФЕКТИВНОСТИ ПРИМЕНЕНИЯ ПРЕДСТАВЛЕНИЙ БОЛЬШИХ ЦЕЛЫХ ЧИСЕЛ ПО МНОЖЕСТВЕННЫМ ОСНОВАНИЯМ В НЕСИММЕТРИЧНОЙ КРИПТОГРАФИИ

Шепляков Р.И.
Научный руководитель – к.т.н., доц. Мельникова О. А.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, пр. Ленина,14, каф. безопасности информационных технологий, тел. (057) 702-14-25

The efficiency of using double base and multiple base number representations in public-key cryptography is considered.

При реализации несимметричных криптопреобразований одним из критичных параметров является, как известно, вычислительная сложность базовых арифметических операций, в частности, операции скалярного умножения для криптосистем в группах точек эллиптических кривых (ЭК). Для уменьшения вычислительной сложности операций могут использоваться комбинации различных подходов, как меняющих характеристики исходных операндов за счет специальных систем их представления или интерпретации, так и подразумевающих использование обновленного алгоритмического/математического аппарата. В докладе анализируются возможности уменьшения вычислительной сложности базовых операции за счет применения представления операндов по множественным основаниям.

Представление по множественным основаниям (1) подразумевает преобразование большого целого числа в сумму термов, где термом является произведение чисел 2 и 3 в некоторых степенях.

$$T= \quad , \qquad (1)$$

где $c_i \in S$, $S = \{1,0,-1\}$ знаково-цифровой набор; a_i и b_i – целые числа, степени 2 и 3 соответственно.

Если при реализации операции умножения точки на скаляр, представить его по множественным основаниям используя основание (2,3), то к базовым операциям удвоения (2P) и сложения (P+Q) добавляется операция утроения (3P), а общее количество операций уменьшается. Теоретически обосновано, что операция утроения точки (3P) может иметь меньшую вычислительную сложность, чем аналогичная операция 2P+Q. Формулы для эффективной реализации операции утроения точки разработаны для большинства применяемых в криптографии координат (аффинны, якобиановых и т.д.) и видов эллиптических кривых (Вейерштрасса, Эдвардса, Коблица и т.д.).

Увеличение количества оснований позволяет уменьшить количество слагаемых в (1), а следовательно уменьшить количество операций сложения точек при реализации эллиптического скалярного умножения.