УДК 681.3

НЕКОТОРЫЕ УСЛОВИЯ КРИПТОГРАФИЧЕСКОЙ СТОЙКОСТИ КРИПТОСИСТЕМ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Магистрант Короткевич О.С.,
кандидат техн. наук, доцент Артамонов В.А.
Белорусский национальный технический университет

В современной криптографии широко используются криптографические преобразования в группе точек эллиптических кривых (ЭК). Стойкость криптоалгоритмов, использующих преобразования в группах точек ЭК, основывается на сложности решения задачи дискретного логарифма на эллиптической кривой.

В криптографии используются ЭК двух видов [1]:

− ЭК над конечным полем $F_p, p > 3$:

$$y^2 + xy = x^3 + ax^2 + b, \text{ где } a, b \in F_{2m}, b \neq 0 (\mathrm{mod}\, p).$$

− ЭК над конечным полем F_{2m}:

$$y^2 + xy = x^3 + ax^2 + b, \text{ где } a, b \in F_{2m}, b \neq 0.$$

Проведенный анализ исследований в описываемой области показывает, что для обеспечения высокого уровня криптографической стойкости группа точек эллиптической кривой E над конечным полем F, где $q = p^k$, p – простое число, должна удовлетворять следующим требованиям:

1. Либо k = 1, либо k должен быть простым числом;
2. $\#E(F_q) = c \cdot n$, где n большое простое число, нод(n, p) = 1, а положительный кофактор $c \leq 4$ [2];
3. (MOV – условие): $q^k \neq 1 (\mathrm{mod}\, n)$ для $1 \leq k \leq B$;
4. (условие аномальности): $n \neq q$; Если $k > 1$, то $a, b \notin F_p$.

Таким образом, в докладе сформирован и обоснован список условий налагаемых на эллиптическую кривую при использовании ее в криптографических целях. Данный список является минимально-необходимым и строго рекомендуется для соблюдения при построении любых криптографических систем на эллиптических кривых.

Литература

1. Ростовцев А.Г., Маховенко Е.Б., Введение в криптографию с открытым ключом – СПб.: Мир и семья, 2001. – 336 с.
2. Baier H., Buchmann J., Efficient construction of crypto-graphically strong elliptic curves, Progress in Cryptology –INDOCRYPT'2000, LNCS Vol.1977, Springer-Verlag, 2000, pp.191-202.