$U(3)$-СТОЙКИЕ ШИФРЫ И ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ

Д.С. Гутарин, Л.Е. Пашнина, В.И. Тимин, С.С. Титов, А.В. Торгашова

Уральский государственный университет путей сообщения,

Колмогорова 66, 620034 Екатеринбург, Россия

denis.gutarin@gmail.com, Ludochka_524@mail.ru, sergey.titov@usaaa.ru

Данная работа основана на книге А.Ю. Зубова [1], посвященной подробному изложению теории совершенных шифров. Объектом исследования являются эндоморфные $U(3)$-стойкие шифры с уравнением [2]

$$y = kf_m(x) + l.$$

Цель работы — расширить знания о эндоморфных $U(3)$-стойких шифрах такого вида.

Если взять подматрицу из 3 столбцов $U(3)$-стойкого шифра, то каждая строка ее будет содержать некоторое трехэлементное множество. Удобный аппарат для параметризации таких множеств — кубические уравнения, корнями которых являются элементы полей $GF(q)$, $q = p^n$. Рассматривались случаи, когда $p = 2$, $\omega = 1$ [3] и $q > 3$, $\omega = 2$, где ω - параметр соответствующего $U(3)$-стойкому шифру перпендикулярного массива $PA_\omega(3, \lambda, \lambda)$, где $\lambda = q$ [1].

В работе была установлена связь между трехэлементными множествами корней уравнения и точками суперсингулярной эллиптической кривой E_1 с уравнением $v^2 + v = u^3$ [4]. При этом каждому множеству соответствует свои шесть уникальных точек на кривой. Однако, такая связь найдена только при устранении всех циклических сдвигов на l и растяжений на k, то есть соответствующие точкам кривой множества нельзя получить друг из друга посредством умножения на k и сдвига на l. Таким образом каждой тройке корней соответствует функция $f_m(x)$, и каждой функции $f_m(x)$ соответствует множество шести точек суперсингулярной эллиптической кривой E_1.

Выяснилось, что для полей с характеристикой $p > 3$ и параметром $\omega = 2$ количество функций $f_m(x)$ меньше чем количество необходимых для построения массива по формуле $y = kf_m(x) + l$.

$$\frac{\lambda - 2}{6} < \frac{\lambda - 2}{3}$$

Если строить массив в поле с характеристикой $p = 2$, то функций $f_m(x)$ достаточно для построения $U(3)$-стойкого шифра.

Результаты работы имеют научную и методическую ценность, так как расширяют существующую теорию $U(3)$-стойких шифров и открывает перспективы дальнейшего изучения связи между совершенными шифрами и эллиптическими кривыми.

Литература

1. *Зубов А. Ю.* Совершенные шифры. М. : Гелиос АРВ, 2003. 160 с.

2. *Гутарин Д.С., Коновалова С.С., Тимин В.И., Титов Е.С., Титов С.С.* Комбинаторные проблемы существования совершенных шифров // Труды Института математики и механики. Екатеринбург: УрО РАН. Т. 13, № 4. 2007. С. 61–73.

3. *Пашнина Л.Е., Тимин В.И., Титов С.С., Торгашова А.В.* U(3)-стойкие шифры над полями характеристики два и эллиптические кривые // Молодежь – будущее атомной промышленности России: Сборник научных трудов конференции. Снежинск: СГФТА, 2007. С. 86–89.

4. *Болотов А,А,, Гашков С.Б., Фролов А.Б., Часовских А.А. и др.* Элементарное введение в эллиптическую криптографию: алгебраические и алгоритмические основы. М.: КомКнига, 2006. 328 с.