# ИМИТОСТОЙКИЕ ШИФРЫ И ЭЛЛИПТИЧЕСКИЕ КРИВЫЕ НАД ПОЛЯМИ ХАРАКТЕРИСТИКИ ДВА

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

Уральский государственный университет путей сообщения,

Колмогорова 66, 620034, Екатеринбург, Россия

sergey.titov@usaaa.ru

В $U(3)$-стойких шифрах параметр стойкости три и буква $U$ (от слова Unordered — неупорядоченный) означает следующее: для любого трехэлементного подмножества $X_3 = \{x_1, x_2, x_3\} \subset X$ и любого трехэлементного подмножества $Y_3 = \{y_1, y_2, y_3\} \subset Y = X$ существует единственная подстановка $E_k$ с ключом $k$ — одним из минимального числа $\pi = C^3_\lambda$, такая, что $E_k$ зашифровывает $X_3$ в $Y_3$.

Удобный аппарат для параметризации трехэлементных множеств — кубические уравнения, корнями которых являются элементы этих множеств в полях $GF(2^n)$. Рассмотрим уравнение

$$x^3 + \sigma_1 x^2 + \sigma_2 x + \sigma_3 = 0.$$

где, согласно стандартным обозначениям, $\sigma_1, \sigma_2, \sigma_3$ — базисные симметричные многочлены, которые по теореме Виета выражаются через корни $x_1, x_2, x_3$ уравнения. После преобразование получаем, что $(u, v)$ — точка на стандартной эллиптической суперсингулярной кривой $E_1$ с уравнением $v^2 + v = u^3$.

Эндоморфизмом кривой $E_1$ является отображение кратности $\varphi_s(P) : P \to s \cdot P$ для $P \in E_1$, $s \in Z$.

1. Сложение. $u_3 = \lambda^2 + u_1 + u_2$, $v = (\lambda(u_1 + u_2) + v_1 + 1)$.
2. Удвоение. При $P_1 = P_2 = P = (u, v)$ имеем, очевидно $2P = (u^4, v^4 + 1)$.
3. Утроение.

$$u_3 = \lambda^2 + u_1 + u_2 = \frac{u^9 + u^3 + 1}{u^2 \cdot (u^3 + 1)^2}, v_3 = \lambda \cdot (u + u_3) + v + 1 = \frac{u^6 + u^3 + 1}{(u^4 + u)^3} + v + 1.$$

4. Упятерение.

$$u_5 = \frac{u^{33} + u^{24} + u^{18} + u^{12} + u^6 + u^3}{(u^{16} + u)^2} = \frac{u^3 + (u^3)^2 + ((u^3)^2)^2 + (((u^3)^2)^2)^2 + u^{2^n+1} + u^{2^{n-1}+2}}{(u^{2^n-1} + u)^2},$$

$$v_5 = \frac{v^{33} + v^{28} + v^{26} + v^{24} + v^{23} + v^{22} + v^{19} + v^{18} + v^{16} + v^{15} + v^{12} + v^{11} + v^{10} + v^8 + v^6 + v}{v^{32} + v^{22} + v^{21} + v^{20} + v^{19} + v^{16} + v^{14} + v^{13} + v^{11} + v^{10} + v^8 + v^6 + v^2 + v}.$$

5. Усемерение.

$$u_7 = \frac{u^{129} + u^{96} + u^{66} + u^{48} + u^{24} + u^{12} + u^6 + u^3}{(u^{64} + u)^2}.$$

6. Эндоморфизм Фробениуса $\tau$ -многократное удвоение: $\tau(P) = 2^{(n+1)/2} \cdot P$.

Порядок группы кривой $E_1$ при $q = 2^n$, где $n$ — нечетно, равен $2^n+1$. Получаем $2^n+1 = q + 1 - t \Leftrightarrow t = 0$, откуда следует, что эта группа циклическая, так как $2^n = q \neq 3(\bmod 4)$. Поскольку $n$ нечетно, то $2^n + 1$ делится на три. Группа автоморфизмов кривой изоморфна, поэтому мультипликативной группе взаимно простых с $2^n + 1$ чисел. Двойка взаимно проста с $2^n + 1$, и поэтому удвоение — автоморфизм (т. е. обратимый эндоморфизм) Фробениуса. Приведенные выше формулы показывают, что может быть предложена следующая

**Конструкция.** Пусть $n > 2$ — простое число, такое, что $p = (2^n + 1)/3$ $f_s(x)$ тоже простое число. Тогда в качестве функций $f_s(x)$ можно взять ординату отображения кратности $\varphi_s(P) : P \to s \cdot P$ для всех $s$, являющихся квадратами по модулю $p : sP = (g_s(u, v), f_s(v))$, $P = (u, v)$, $s \equiv t^2(\bmod p)$.