Волокитин А.А., Коновалова С.С., Титов С.С., Федоров Д.Н.

U(3)-СТОЙКИЕ ШИФРЫ И КОНЕЧНЫЕ ПЛОСКОСТИ

Уральский государственный университет путей сообщения

В настоящей статье рассматривается проблема конструирования $U(3)$-стойких шифров – современных аналогов совершенных шифров, стойких к атакам имитации и подмены сообщения, в том числе с использованием конечных плоскостей.

1. Рассмотрим полуполе Алберта, которое дает пример билинейного немультипликативного совершенного шифра (это утверждение доказано при решении в [1] задачи, сформулированной в [2]). Полуполе – это система Веблена–Веддербёрна, в которой выполняются оба дистрибутивных закона. Умножение в полуполе Алберта $K(p^r)$, где p – простое нечетное число, r – нечетное и $r>1$, определяется формулой $x\circ y=(xA, yA)$, где $x=(u,1)=1/2(u+u^p)$, A: $u=xA$ – это взаимнооднозначное отображение, $(x,y)=1/2(xy^p+x^py)$. Для случая $p=3$, $r=3$ построено полуполе Алберта $GF(3^3)$, задаваемое неприводимым многочленом $f(x)=x^3+x^2+2$, проверено основное свойство неассоциативности умножения, которое позволяет строить на его основе немультипликативные шифры, может быть и $U(3)$-стойкие.

2. Рассмотрим функцию зашифрования на основе суперпозиции подстановок для возможности построения эндоморфного $U(3)$-стойкого шифра:

$$f(x) = g^m(x)a^2 + b, \qquad (1)$$

где сложение и умножение производится по модулю 23; b – произвольный вычет по модулю 23, a – произвольный ненулевой вычет по модулю 23, $m=\{0,1,2,...,6\}$.

Одним из условий построения такого шифра является нахождение семи троек элементов, каждая из которых принадлежит одной прямой, и невозможно перевести изоморфизмом одну тройку в другую. В данной работе рассмотрено следующее разбиение на тройки, удовлетворяющее этому условию:

(0,1,22), (2,5,16), (3,6,14), (7,18,21), (8,11,13), (9,17,20), (10,15,19).

В качестве шифрующей подстановки, которая удовлетворяет свойству: элементы каждой тройки находятся в разных циклах, а оставшиеся два элемента являются неподвижными точками) – возьмем

$$g=(4)(12)(0,9,14,7,16,11,19)(1,20,3,18,5,8,15)(22,17,6,21,2,13,10). \qquad (2)$$

$U(3)$-стойкий шифр с функцией зашифрования (1) и найденной подстановкой (2) существует, если функция $f=f_1^{-1}f_2$ не содержит трех неподвижных точек, неподвижную точку и цикл длины два или цикл длины три. Возьмем $f_1(x)=g^2(x)$ (то есть $a=1$, $b=0$, $m=2$) и $f_2(x)=g^0(x)+2=e(x)+2=x+2$ (то есть $a=1$, $b=2$, $m=0$), получим итоговую функцию $f(x)=f_1^{-1}f_2=g^{-1}(x)(x+2)$, или в виде подстановки

$$f=(3)(5)(16)(0,13)(1,10,4,6)(2,8,20,17,12,14)(7,11,9,21,19,18,22,15).$$

Подстановка f имеет три неподвижные точки, поэтому шифр, построенный на основе формулы зашифрования (1), не обладает свойством $U(3)$-стойкости.

3. Рассмотрим группу Матьё M_{23}, задающую $O(4)$-стойкий шифр, которая порождается подстановками

$$a=(0,1,2,3,4,5,6,7,8,9,10,11,12,13,141,15,16,171,81,9,20,21,22),$$
$$b=(2,16,9,6,8)(3,12,13,18,4)(7,17,10,11,22)(14,19,21,20,15)\ [2].$$

Обозначим

$c=ababa^{-1}b^{-1}$=(0,20,14,12,21,1,16,19,6,4,22)(2,7,10,11,13,15,17,18,9,3,8)(5),
$d=a^2b^{-1}a^{-1}b^{-1}a^{-1}$=(0,21,10,7,19,12,14)(1,3,17,11,9,15,8)(2,6,4,5,18,20,16)(13)(22)
и возьмем две подстановки
$g_1=a^{20}c^4d^6$=(0,8,4,6,21,16,11,17,20,15,7,12,10,9,18,1,2,19,22,14,5,13,3), тогда
$g^{-1}{}_1=d^{-6}c^{-4}a^{-20}=dc^7a^3$;
$g_2=a^{19}c^8d^3$=(0,19,12,2,6,1,20,21,8,4,18,22,13,3)(5,10,11,9,16,7,15)(14,17),
и получим $g^{-1}{}_1g_2=(dc^7a^3)(a^{19}c^8d^3)=$
=(0)(1,22,12,15,21)(2,20,14,13,10)(3)(4)(5,17,9,11,7)(6,18,16,8,19),
которая содержит три неподвижные точки (0, 3 и 4). Таким образом, доказано, что в группе Матье M_{23} нет подгруппы, соответствующей $U(3)$-стойкому шифру с $\lambda=23$ и $\pi=C^3{}_{23}=23\cdot11\cdot7$.

4. В [2] говорится о связи $U(L)$-стойких шифров и соответствующих им массивов $PA_\omega(L, \lambda, \mu)$ с L-схемами L-(μ, λ, ω). L-схемы как комбинаторные конструкции, согласно [3], связаны с конечными геометриями, а точнее – с плоскостью Мёбиуса. Плоскость Мёбиуса – это плоскость, удовлетворяющая системе K из четырех аксиом. Аксиома $K2$ (с любой тройкой точек инцидентен единственный цикл) является необходимым условием $U(3)$-стойкости, поэтому данный тип плоскости представляет интерес в теории совершенных шифров.

В статье на примере 3-(10, 4, 1)-схемы была рассмотрена возможность построения неэндоморфных $U(3)$-стойких шифров. Было замечено, что необходимое число ключей для построения неэндоморфного шифра $\pi=q(q^2+1)\cdot C_\lambda{}^3$ связано с числом $q(q^2+1)$ циклов блок-схемы, если q – это порядок соответствующей плоскости, и с числом ключей для эндоморфного шифра $C_\lambda{}^3= C_\mu{}^3$. Поэтому для того, чтобы построить неэндоморфный $U(3)$-стойкий шифр на основе плоскости Мёбиуса, необходимо каждый ее цикл использовать вместе с соответствующим эндоморфным $U(3)$-стойким шифром. Отметим случай $L=q$: тогда эндоморфный $U(3)$-стойкий шифр задается латинским квадратом. Полученный из плоскости Мёбиуса неэндоморфный шифр удовлетворяет условию $U(3)$-стойкости, так как сама плоскость Мёбиуса согласно ее основной аксиоме.

Таким образом приведены примеры конструкций, которые как могут быт использованы для построения $U(3)$-стойких шифров, так и нет. Дальнейшее изучение таких структур, а особенно конструкций на основе конечных плоскостей, позволит строить шифры с большим параметром стойкости.

Литература

1. Коновалова, С.С. О конструкциях эндоморфных совершенных шифров / С.С. Коновалова, С.С. Титов // Матер. межд. науч. конф. по проблемам безопасности и противодействия терроризму. Интеллектуальный Центр МГУ, 2-3 ноября 2005 г. – М. : МЦНМО, 2006. – С. 168–180.

2. Зубов, А.Ю. Совершенные шифры / А.Ю. Зубов. – М. : Гелиос АРВ, 2003. – 160 с.

3. Картеси, Ф. Введение в конечные геометрии: Пер. с англ. / Ф. Картеси. – М. : Наука. Гл. ред. физ.-мат. лит., 1980. – 320 с.