УДК 517.51

Д. С. Лукомский, С. Ф. Лукомский

ВСПЛЕСКОВЫЕ БАЗИСЫ И КРИПТОГРАФИЯ

В последние десятилетия криптография оформилась в новую математическую теорию и стала объектом интенсивного математического изучения. Основой современных криптографических систем являются теоретико-числовые методы. Мы хотим рассмотреть непрерывные методы.

Основная идея непрерывных методов в криптографии заключается в использовании дискретных ортогональных систем. Классическим примером такой системы является система Хаара. Если мы имеем вектор $\mathbf{f} = (f_0, f_1, \ldots, f_{2^n-1})$, то мы можем по нему построить вектор-преобразование Фурье – Хаара $\hat{f} = (\hat{f}(0), \hat{f}(1), \ldots, \hat{f}(2^n-1))$. Преобразование $\hat{f}(n)$ и есть зашифрованное сообщение $\mathbf{f}$. Но этот метод бесполезен, так как, зная информацию, что зашифрованное сообщение есть преобразование Фурье – Хаара, можно сразу восстановить исходное сообщение f. В последние годы, в связи с развитием теории КМА на нуль-мерных группах, появилась возможность строить бесконечно много дискретных ОНС, каждая из которых определяется конечным набором комплексных чисел $(\mu_k)_{k=0}^N$ с единственным условием $\mu_0 = 1$, $|\mu_k| = 1$ при $k \geq 1$. Таким образом, появляется возможность, используя в качестве ключа последовательность чисел $(\mu_k)_{k=0}^N$, строить криптографические алгоритмы как разложения конечномерного вектора по ортонормированной системе. Мы ограничимся простейшим примером, который объяснит суть происходящего. В нашем примере рассмотрим ОНС, которые не зависят от групповой операции и являются начальным шагом в построении целого класса ОНС.

Пусть $(G, \dot{+})$ – нуль-мерная локально компактная Абелева группа с основной цепочкой подгрупп

$$\cdots \subset G_n \subset \cdots \subset G_1 \subset G_0 \subset G_{-1} \subset \cdots \subset G_{-n} \subset \ldots, \quad (G_n/G_{n+1})^\sharp = p,$$

где p – простое, $g_n \in G_n \setminus G_{n+1}$ – базисная последовательность. Известно [1], что любой элемент $x \in G$ единственным образом представим в виде суммы ряда

$$x = \sum_{n=-\infty}^{+\infty} x_n g_n \quad (x_n = \overline{0, p-1}).$$

Отображение $\psi:\ G \to \mathbb{R}^+$, определенное равенством

$$\psi(x) = \sum_{n=-\infty}^{+\infty} \frac{x_n}{p^{n+1}},$$

переводит каждую подгруппу G_n в модифицированный отрезок $\left[0, \frac{1}{p^n}\right]^*$. Это позволяет рассматривать группу G на модифицированной полупрямой, в которой топология определяется сдвигами отрезков $\left[0, \frac{1}{p^n}\right]^*$. Через $G_n^\perp$ будем обозначать аннуляторы подгруппы G_n. Характеры $r_n \in \in\ G_n^\perp \setminus G_{n+1}^\perp$ будем называть *функциями Радемахера*. Значение характера χ на элементе x будем обозначать (χ, x).

Пусть $r_{-1} \in G_0^\perp \setminus G_{-1}^\perp$ – функция Радемахера. Так как $r_{-1} \in G_0^\perp$, то $r_{-1}(G_0) = 1$. Так как p – простое, то (r_{-1}, g_{-1}) есть корень из 1 степени p, т.е. $(r_{-1}, g_{-1}) = e^{\frac{2\pi i}{p}\nu}$. Базисный элемент g_{-1} можно выбрать так, что $(r_{-1}, g_{-1}) = e^{\frac{2\pi i}{p}}$, и поэтому можно считать, что $r_{-1}(G_0 \dot{+} j g_{-1}) = e^{\frac{2\pi i}{p} j}$ $(j = \overline{0, p-1})$. Пусть

$$\varphi(x) = \frac{1}{p} \mathbf{1}_{G_{-1}}(x) \sum_{j=0}^{p-1} \mu_j (r_{-1}, x)^j \tag{1}$$

масштабирующая функция и μ_j – комплексные числа такие, что $\mu_0 = 1$, $|\mu_j| = 1$. Отметим свойства функции φ [2].

1. $\varphi(x) = 0$ вне G_{-1}, это очевидно.

2. $\varphi(x)$ постоянна на смежных классах $G_0 \dot{+} j g_{-1}$. Это было проверено выше.

3. Если $x \in G_0 \dot{+} \lambda g_{-1}$ $(\lambda \neq 0)$, то $\varphi(x) = \varphi(\lambda g_{-1})$, $\varphi(x \dot{-} \nu g_{-1}) =$ $= \varphi(\lambda g_{-1} \dot{-} \nu g_{-1})$, т.е. сдвиг $\varphi(x \dot{-} \nu g_{-1})$ есть функция, принимающая на смежных классах $G_0 \dot{+} \lambda g_{-1}$ значения $\varphi_{\lambda,\nu} = \varphi(\lambda g_{-1} \dot{-} \nu g_{-1})$.

4. Смежные классы $G_0 \dot{+} j g_{-1}$ можно рассматривать как модифицированные отрезки $[j, j+1]^*$.

Предложение 1. *Любая функция, принимающая постоянные значения на смежных классах $G_0 \dot{+} \lambda g_{-1} = [\lambda, \lambda + 1]^*$, есть линейная комбинация сдвигов $\varphi(x \dot{-} \nu g_{-1})$.*

Доказательство. Пусть $f = (f_0, f_1, \ldots, f_{p-1})$ функция, постоянная на смежных классах $G_0 \dot{+} \lambda g_{-1}$ и $f_0, f_1, \ldots, f_{p-1}$ ее значения на этих смежных классах. Надо доказать, что найдутся числа c_ν $(\nu = \overline{0, p-1})$ такие, что

$$\sum_{nu=0}^{p-1} c_\nu \varphi(x \dot{-} \nu g_{-1}) = f. \tag{2}$$

Обозначим через Φ матрицу с элементами $\varphi_{\lambda,\nu}$, т.е. $\Phi = (\varphi_{\lambda,\nu})_{\lambda,\nu=\overline{0,p-1}}$. Тогда равенство (2) равносильно системе

$$\Phi \cdot (c_0, c_1, \ldots, c_{p-1})^T = (f_0, f_1, \ldots, f_{p-1})^T. \tag{3}$$

Так как матрица Φ унитарна, то система (3) имеет единственное решение $(c_0, c_1, \ldots, c_{p-1})^T = \overline{\Phi^T} \cdot (f_0, f_1, \ldots, f_{p-1})^T$, и, значит, $f = \sum\limits_{\nu=0}^{p-1} c_\nu \varphi(x \dot{-} \nu g_{-1})$. $\square$

Теперь мы можем выписать алгоритм шифровки сообщения.

1. Выбираем последовательность $(\mu_j)_{j=0}^{p-1}$ такую, что $\mu_0 = 1$, $|\mu_j| = 1$ при $j = \overline{1, p-1}$.

2. По формулам (1) строим функцию $\varphi(x)$.

3. Образуем матрицу $\Phi = \left(\varphi(\lambda g_{-1} \dot{-} \nu g_{-1})\right)_{\lambda,\nu}$.

4. По сообщению $f = (f_0, f_1, \ldots, f_{p-1})^T$ строим коэффициенты $C = (c_0, c_1, \ldots, c_{p-1})^T$ по формулам $C = \Phi f$.

5. Вместо сообщения f передаем зашифрованное сообщение

$$C = (c_0, c_1, \ldots, c_{p-1})^T.$$

Этот метод следует отнести к классическим методам. По своим принципам он близок к методу Хилла [3]. Ключом в рассматриваемом методе является последовательность (μ_j). В отличие от метода Хилла ключей может быть бесконечно много. Так как $|\mu_j| = 1$, то $\mu_j = e^{\frac{2\pi i}{p}\kappa_j}$, $\kappa_j = \overline{0, p-1}$, и, значит, вектор $\kappa = (\kappa_0, \kappa_1, \ldots, \kappa_{p-1})$ можно выбирать в качестве ключа.

Предложение 2. *Если $\kappa = \alpha \cdot (0, 1, \ldots, p-1)$, т.е. $\kappa_j = \alpha \cdot j$, то вектор $(c_k)_{k=0}^{p-1}$ получается из сообщения f α-й итерацией циклической перестановки.*

Доказательство. Вначале отметим, что функции

$$\psi_j = \frac{1}{\sqrt{p}} \left(e^{\frac{2\pi i}{p} 0 j}, e^{\frac{2\pi i}{p} 1 j}, \ldots, e^{\frac{2\pi i}{p}(p-1)j} \right),$$

определенные на дискретном множестве $X = \{0, 1, \ldots, p-1\}$, образуют ОНС на X. Поэтому равенство

$$\hat{f}(j) = \sum_{\nu=0}^{p-1} \frac{1}{\sqrt{p}} e^{-\frac{2\pi i}{p}\nu j} f_\nu$$

определяет на X дискретное преобразование Фурье.

Согласно предложению 1 и определению функции φ имеем

$$c_\nu = \sum_{\lambda=0}^{p-1} \bar{\varphi}_{\lambda\nu} f_\lambda = \sum_{\lambda=0}^{p-1} \frac{1}{p} \sum_{j=0}^{p-1} e^{-\frac{2\pi i}{p}\alpha j} (r_{-1}, g_{-1})^{-\lambda j} (r_{-1}, g_{-1})^{\nu j} f_\lambda =$$

$$= \frac{1}{\sqrt{p}} \sum_{j=0}^{p-1} e^{-\frac{2\pi i}{p}(\alpha j - \nu j)} \sum_{\lambda=0}^{p-1} \frac{1}{\sqrt{p}} e^{-\frac{2\pi i}{p}\lambda j} f_\lambda = \sum_{j=0}^{p-1} \frac{1}{\sqrt{p}} e^{\frac{2\pi i}{p} j(\nu-\alpha)} \hat{f}(j) = f_{\nu-\alpha},$$

откуда и следует предложение 2, так как разность $\nu - \alpha$ в $f_{\nu-\alpha}$ понимается как вычитание по $\bmod 2$. $\square$

Замечание. Если ключ κ есть произвольный вектор, принадлежащий множеству $[0, p-1]^p$, то зашифрованное сообщение $C = (c_k)_{k=0}^{p-1}$ не обязано быть перестановкой исходного сообщения. Например, при $p = 11$, $f = (c\,o\,e\,f\,f\,i\,c\,i\,e\,n\,t)$ зашифрованное сообщение $C = (g\,h\,k\,g\,i\,g\,g\,j\,o\,c\,l)$.

При шифровке сообщение следует разбить на слова длиной p, и шифровать каждое слово отдельно. Слово длины p, очевидно, шифруется одинаково независимо от его положения в сообщении. Детальное изучение криптоустойчивости данного и близких к нему алгоритмов предполагается в дальнейшем.

Работа выполнена при финансовой поддержке гранта Президента РФ (проект НШ-4383.2010.1) и РФФИ (проект 10-01-00097-а).

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Агаев Г. Н., Виленкин Н. Я., Джафарли Г. М., Рубинштейн А. И.* Мультипликативные системы функций и гармонический анализ на нуль-мерных группах. Баку : Элм, 1981.

2. *Лукомский С. Ф.* Кратномасштабный анализ на нуль-мерных абелевых группах и всплесковые базисы // Мат. сб. 2010. Т. 201, № 5. С. 41–46.

3. *Саломаа А.* Криптография с открытым ключом. М. : Мир, 1995.

УДК 517.984

Т. В. Мазур

АЛГОРИТМ РЕШЕНИЯ ОБРАТНОЙ ЗАДАЧИ ШТУРМА — ЛИУВИЛЛЯ НА ЗВЕЗДООБРАЗНОМ ГРАФЕ

В статье предлагается алгоритм решения обратной задачи Штурма — Лиувилля на звездообразном графе, использующий ряд соотношений метода спектральных отображений и требующий относительно небольшого количества операций.