ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 23 МАТЕМАТИКИ Выпуск 4
2016

Ф. Б. Б у р т ы к а (Ростов-на-Дону, ЮФУ)**. Оценка числа диагонализируемых корней односторонних матричных полиномов второго порядка над конечными полями.**

Для проведения глубокого анализа криптостойкости полностью гомоморфного шифра из [1] необходимо хорошо понимать задачу нахождения корней (унитарных) односторонних матричных полиномов (ОМП) над конечным полем $\mathbb{F}_p$. ОМП n-го порядка — это выражения вида:

$$\mathcal{F}(X) = X^d + \mathbf{F}_{d-1}\,X^{d-1} + \cdots + \mathbf{F}_2 X^2 + \mathbf{F}_1\,X + \mathbf{F}_0, \tag{1}$$

где коэффициенты $\mathbf{F}_i$ и переменная X — матрицы размера $n \times n$. Корень (1) — это матрица $\mathbf{S}$ такая, что $\mathcal{F}(\mathbf{S}) = \mathbf{0}$, где $\mathbf{0}$ — нуль-матрица. В данной работе выводятся формулы количества диагонализируемых корней (ДК) (1) для $\mathbb{F}_p$, в этом случае все матрицы будут из множества $\mathsf{M}_n(\mathbb{F}_p)$ матриц размера $n \times n$ с коэффициентами из поля $\mathbb{F}_p$. Ранее в литературе этот вопрос рассматривался лишь для ОМП над полем комплексных чисел $\mathbb{C}$ [2–3]. Однако в случае поля $\mathbb{C}$ (1) может иметь бесконечное число корней, что невозможно для $\mathbb{F}_p$. Основным вопросом данной работы является то, *какое количество ДК будет иметь* (1) *над* $\mathbb{F}_p$ *в тех случаях, когда над* $\mathbb{C}$ (1) *имел бы бесконечное число корней.* Здесь будет проанализирован случай ОМП *второго порядка.* Множество ОМП над полем $\mathbb{F}_p$ обозначим как $(\mathsf{M}_n(\mathbb{F}_p))[X]$. Количество ДК обозначим как $\#\mathsf{Null}_{\mathfrak{D}}(\mathcal{F}(X))$.

Для поиска ДК используем метод из [2–3], который был предложен для случая $\mathbb{C}$, но легко переносится на $\mathbb{F}_p$. Ниже приводятся определения из [2–3], адаптированные для $\mathbb{F}_p$.

О п р е д е л е н и е 1. λ — матрица соответствующая (1) — это полином $\mathcal{F}(\lambda) = \lambda^d + \mathbf{F}_{d-1}\,\lambda^{d-1} + \cdots + \mathbf{F}_2\,\lambda^2 + \mathbf{F}_1\,\lambda + \mathbf{F}_0 \in \mathsf{M}_n(\mathbb{F}_p[\lambda])$, где $\lambda \in \mathbb{F}_p$ — скалярная переменная.

О п р е д е л е н и е 2. Латентный корень (ЛК) $\mathcal{F}(\lambda)$ — это $\lambda_0 \in \mathbb{F}_p$ такое, что $g(\lambda_0) = 0$, где $g(\lambda) = \mathsf{det}(\mathcal{F}(\lambda)) \in \mathbb{F}_p[\lambda]$, $\mathsf{deg}(g) = d\,n$.

О п р е д е л е н и е 3. Латентный вектор (ЛВ), соответствующий $\lambda_0 \in \mathbb{F}_p$, — это $\vec{v}_0 \in \mathsf{Ker}(\mathcal{F}(\lambda_0))$.

Теорема 1. *Пусть* $\mathcal{F}(\lambda)$ *имеет ЛК* $\lambda_1, \ldots, \lambda_n \in \mathbb{F}_p$ *такие, что для всех* $\lambda_i, 1 \leqslant i \leqslant n$ *найдется* $\vec{v}_i \in \mathsf{Ker}(\mathcal{F}(\lambda_i))$ *и* $\{\vec{v}_1, \ldots, \vec{v}_n\}$ *— базис* $\mathbb{F}_p^n$. *Тогда* $\mathbf{S} = \mathbf{V}\,\mathsf{diag}(\lambda_1, \ldots, \lambda_n)\,\mathbf{V}^{-1}$ *— корень* $\mathcal{F}(X)$, *где* i*-й столбец* $\mathbf{V} \in \mathsf{M}_n(\mathbb{F}_p)$ *равен* $\vec{v}_i$.

Теорема 1 была доказана в [2] для $\mathbb{C}$, но тривиально выполняется и для $\mathbb{F}_p$, т. к. следует из того, что все собственные числа и векторы любого корня $\mathcal{F}(X)$ являются ЛК и ЛВ для $\mathcal{F}(\lambda)$. Легко показать, что любой ДК (1) имеет вид, указанный в теореме 1. Это дает алгоритм поиска всех ДК: Сначала вычисляются корни $\lambda_1, \ldots, \lambda_t$ полинома $\mathsf{det}(\mathcal{F}(\lambda))$, затем для $\forall i \in \overline{1,t}$ вычисляются $\vec{v}_i \in \mathsf{Ker}(\mathcal{F}(\lambda_i))$. Из $\vec{v}_i$ и λ_i строятся различные корни (1).

Перейдем к вопросу о количестве ДК (1) для $n = 2$. При $n = 2$ для ЛК λ_0 полинома $\mathcal{F}(\lambda)$ есть только два варианта: 1) $\mathcal{F}(\lambda_0) \neq \mathbf{0}$ и тогда $\mathsf{Ker}(\mathcal{F}(\lambda_0)) = \mathsf{Lin}(\vec{v}_0)$ для некоторого $\vec{v}_0 \in \mathbb{F}_p^2$; 2) $\mathcal{F}(\lambda_0) = \mathbf{0}$ и тогда $\mathsf{Ker}(\mathcal{F}(\lambda_0)) = \mathbb{F}_p^2$.

Теорема 2. *Пусть* $\mathcal{F}(\lambda) \in \mathsf{M}_2(\mathbb{F}_p[\lambda])$ *имеет множество ЛК* $\{\lambda_1, \ldots, \lambda_t\}$ *и для некоторого* $s \leqslant t$ *выполняется* $\mathcal{F}(\lambda_i) = \mathbf{0}$ *для* $1 \leqslant i \leqslant s$, *и* $\mathcal{F}(\lambda_i) \neq \mathbf{0}$ *для* $s+1 \leqslant i \leqslant t$. *И пусть* $\{\lambda_{s+1}, \ldots, \lambda_t\} = \Lambda_1 \cup \ldots \cup \Lambda_m$, *где* $\Lambda_i \cap \Lambda_j = \varnothing$ *при* $i \neq j$, $\Lambda_i = \{\lambda_{i_1}, \ldots, \lambda_{i_{t_i}}\}$, $\sum_{i=1}^{m} t_i = s - t$ *и для всех* $\lambda_{i_l} \in \Lambda_i$ *выполняется* $\mathsf{Ker}(\mathcal{F}(\lambda_{i_l})) = \mathsf{Lin}(\vec{v}_i)$ *и* $\mathsf{Lin}(\vec{v}_i) \cap \mathsf{Lin}(\vec{v}_j) = \varnothing$ *при* $i \neq j$. *Тогда справедливы следующие утверждения о количестве ДК* $\mathcal{F}(X)$:

1) *если* $t = 0$, *то* $\#\mathsf{Null}_{\mathfrak{D}}(\mathcal{F}(X)) = 0$;
2) *если* $t = s = 1$, *то* $\#\mathsf{Null}_{\mathfrak{D}}(\mathcal{F}(X)) = 1$;
3) *если* $t = s$, $s > 1$, *то* $\#\mathsf{Null}_{\mathfrak{D}}(\mathcal{F}(X)) = s + C_s^2\, p\,(p+1)$;
4) *если* $s = 0$, $m = 1$, *то* $\#\mathsf{Null}_{\mathfrak{D}}(\mathcal{F}(X)) = 0$;
5) *если* $s = 0$, $m > 1$, *то* $\#\mathsf{Null}_{\mathfrak{D}}(\mathcal{F}(X)) = \sum_{i=1}^{m-1} \sum_{j=i+1}^{m} t_i\, t_j$;
6) *если* $s = 1$, $m > 1$, *то* $\#\mathsf{Null}_{\mathfrak{D}}(\mathcal{F}(X)) = 1 + p \sum_{i=1}^{m} t_i + \sum_{i=1}^{m-1} \sum_{j=i+1}^{m} t_i\, t_j$;
7) *если* $s > 1$, $m = 1$, *то* $\#\mathsf{Null}_{\mathfrak{D}}(\mathcal{F}(X)) = s + C_s^2\, p\,(p+1) + s\, p\, t_1$;
8) *если* $s > 1$, $m > 1$, *то* $\#\mathsf{Null}_{\mathfrak{D}}(\mathcal{F}(X)) = s + C_s^2\, p\,(p+1) + s\, p \sum_{i=1}^{m} t_i + \sum_{i=1}^{m-1} \sum_{j=i+1}^{m} t_i\, t_j$.

Д о к а з а т е л ь с т в о . Указанные формулы следуют из того, что из данных ЛК и ЛВ можно составить решения четырех видов.

1) $\mathbf{S} = \mathsf{diag}(\lambda_i, \lambda_i), 1 \leqslant i \leqslant s$, если $s \geqslant 1$. Количество различных решений этого вида s.

2) $\mathbf{S} = \mathbf{V}\, \mathsf{diag}(\lambda_i, \lambda_j)\, \mathbf{V}^{-1}$, $1 \leqslant i, j \leqslant s$, $i \neq j$, если $s > 1$. Количество различных решений данного вида $C_s^2\, p\,(p+1)$.

3) $\mathbf{S} = \mathbf{V}\, \mathsf{diag}(\lambda_{i_k}, \lambda_{j_l})\, \mathbf{V}^{-1}$, $\lambda_{i_k} \in \Lambda_i$, $\lambda_{j_l} \in \Lambda_j$, $i \neq j$, если $m > 1$. Количество различных решений этого вида $\sum_{i=1}^{m-1} \sum_{j=i+1}^{m} t_i\, t_j$.

4) $\mathbf{S} = \mathbf{V}\, \mathsf{diag}(\lambda_i, \lambda_{j_l})\, \mathbf{V}^{-1}$, $1 \leqslant i \leqslant s$, $\lambda_{j_l} \in \Lambda_j$, если $s \geqslant 1$, $m \geqslant 1$. Количество различных решений этого вида $s\, p \sum_{i=1}^{m} t_i$. $\square$

Следствие 1. *Пусть* $\mathcal{F}(\lambda) \in \mathsf{M}_2(\mathbb{F}_p[\lambda])$ *имеет* t *различных ЛК кратности* 1, $t \geqslant 2$, *и каждому ЛК соответствует одномерное подпространство ЛВ* V_i. *Тогда* $\#\mathsf{Null}_{\mathfrak{D}}(\mathcal{F}(X)) \leqslant C_t^2$.

Данное следствие справедливо и при $n > 2$. Отметим, что в случаях 3, 6, 7, 8 из теоремы 2, при переходе к $\mathbb{C}$ количество ДК (1) становится бесконечным [3].

Теорема 3. *Пусть* $\mathcal{F}(\lambda) \in \mathsf{M}_n(\mathbb{F}_p[\lambda])$ *с* $\mathsf{deg}(\mathcal{F}) = d$ *имеет ЛК* $\lambda_1, \ldots, \lambda_{n\,d}$, $\lambda_i \neq \lambda_j$. *Если каждому* λ_i *соответствует одномерное подпространство ЛВ* $V_i = \mathsf{Lin}\{\vec{v}_i\}$ *и любой набор* $\{\vec{v}_{i_1}, \ldots, \vec{v}_{i_n}\}$ *является базисом* $\mathbb{F}_p^n$, *то все корни* (1) *являются ДК и их количество* $C_{n\,d}^n$.

Теорема 3 доказана в [2] для поля $\mathbb{C}$. Это доказательство тривиально переносится на случай $\mathbb{F}_p$. Матричные полиномы $\mathcal{F}(X)$, описанные в теореме 3, — это полиномы в случае общего положения [2]. Они имеют лишь ДК. Матричные полиномы не в случае общего положения могут иметь недиагонализируемые решения, которые нужно искать отдельно.

Работа выполнена при финансовой поддержке гранта РФФИ № 16-37-00125 мол-а.

СПИСОК ЛИТЕРАТУРЫ

1. *Буртыка Ф. Б.* Симметричное полностью гомоморфное шифрование с использованием неприводимых матричных полиномов. — Изв. Южного федерального ун-та. Технические науки, 2014, т. 157, № 8, с. 107–122.
2. *Dennis, Jr J. E., Traub J. F., Weber R. P.* The algebraic theory of matrix polynomials. — SIAM Journal on Numerical Analysis, 1976, v. 13, № 6, p. 831–845.
3. *Wilson R. L.* Polynomial equations over matrices. — Rutgers University.