МОДЕЛИРОВАНИЕ АЛГЕБРО-КОМБИНАТОРНЫХ КРИПТОСИСТЕМ С ОТКРЫТЫМ КЛЮЧОМ, ОСНОВАННЫХ НА ДВУХ ЗАДАЧАХ ТЕОРИИ ГРАФОВ

И. Б. Просвирнина
Кафедра математического анализа, дифференциальных уравнений и алгебры, ГрГУ им. Я. Купалы
Гродно, Республика Беларусь
E-mail: i.prosvirnina@grsu.by

В настоящей работе изучаются две реализации алгебро-комбинаторной криптосистемы Polly Cracker, основанные на NP-сложной задаче о трехцветной раскраске графа и на NP-сложной задаче о построении гамильтонова пути в графе.

Криптосистема Polly Cracker

Опишем криптосистему с открытым ключом, которую принято называть Polly Cracker [1]. Пусть F – конечное поле, а $T = \{t_i\}_{i=1}^{n}$ – множество переменных. Алиса хочет получить сообщение $m \in F$ от Боба. Секретный ключ криптосистемы – вектор $y \in F^n$, а открытый ключ – множество полиномов $B = \{q_i\}$ из $F[T]$ таких, что

$$q_j(y) = 0.$$

Чтобы отослать сообщение m , Боб генерирует полином

$$p = \sum h_j q_j$$

идеала $I \subset F[T]$, порожденного множеством полиномов B, и отсылает Алисе полином

$$c = p + m.$$

Когда Алиса получает зашифрованный полином c, она находит m, вычисляя значение зашифрованного полинома в точке y:

$$c(y) = p(y) + m = m.$$

I. Криптосистема, основанная на задаче о трехцветной раскраске графа

Открытый ключ – граф $\Gamma = (V, E)$. Секретный ключ – правильная раскраска графа Γ в три цвета.

Объясним, как реализовать криптосистему Polly Cracker в этом случае с помощью техники базисов Гребнера.

Все построения будем проводить над алгебраически замкнутым полем комплексных чисел C. Пусть $e^{2\pi i/3} = \epsilon$ – корень третьей степени из единицы. Представим три цвета раскраски графа тремя различными корнями третьей степени из единицы $1, \epsilon, \epsilon^2$. Далее, пусть $x_1, x_2, \ldots, x_n$ – переменные, поставленные в соответствие различным вершинам графа Γ. Каждой вершине графа Γ сопоставляется один из трёх цветов $1, \epsilon, \epsilon^2$. Это даёт следующие n уравнений:

$$x_i^3 - 1 = 0, \quad 1 \le i \le n.$$

Кроме того, если вершины x_i и x_j соединены ребром, они должны быть раскрашены в разные цвета.

Так как $x_i^3 = x_j^3$, то

$$(x_i - x_j)(x_i^2 + x_i x_j + x_j^2) = 0.$$

Таким образом, вершины x_i и x_j раскрашены в разные цвета тогда и только тогда, когда

$$x_i^2 + x_i x_j + x_j^2 = 0.$$

Рассмотрим идеал I кольца полиномов $C[x_1, x_2, \ldots, x_n]$, порожденный полиномами

$$x_i^3 - 1, \quad 1 \le i \le n,$$

$$x_i^2 + x_i x_j + x_j^2 = 0, \quad 1 \le i, j \le n.$$

Вычислим редуцированный базис Грёбнера Γ идеала I с помощью системы компьютерной алгебры Maple, задав лексикографическое упорядочение термов в кольце полиномов $C[x_1, x2, \ldots, x_n]$, для которого

$$x_1 > x_2 > \ldots > x_n.$$

Рассмотрим многообразие $V(I)$, содержащееся в C^n. Ясно, что граф Γ имеет правильную вершинную раскраску в три цвета тогда и только тогда, когда многообразие $V(I)$ не пусто. По теореме Гильберта о нулях [1] $V(I)$ не пусто в том и только в том случае, когда 1 не принадлежит редуцированному базису Грёбнера Γ идеала I.

Итак, выяснив для конкретного графа, что правильная трёхцветная вершинная раскраска у него существует, продолжаем работу. (В противном случае, выбираем новый граф.) Наша цель: найти какую-нибудь правильную трёхцветную раскраску вершин данного графа. Такая раскраска может быть найдена комбинаторными методами, если известен базис Гребнера Γ идеала I. Решив систему полиномиальных уравнений, тем самым находим секретный ключ криптосистемы – вектор $y \in C^n$, и открытый ключ – множество полиномов базиса Грёбнера Γ идеала I из $C[x_1, x_2, \ldots, x_n]$. Далее – всё по схеме. Чтобы отослать сообщение m, Боб генерирует полином

$$p = \sum h_j q_j$$

идеала I, порожденного множеством полиномов G, и отсылает Алисе полином

$$c = p + m$$

Когда Алиса получает зашифрованный полином c , она находит m , вычисляя значение зашифрованного полинома в точке y:

$$c(y) = p(y) + m = m.$$

II. Криптосистема, основанная на задаче о построении гамильтонова пути

Открытый ключ – граф $\Gamma = (V, E)$ и две его различные вершины s и t. Секретный ключ – гамильтонов путь в графе Γ из вершины s в вершину t.

Объясним, как реализовать криптосистему Polly Cracker в этом случае с помощью техники базисов Гребнера.

Простой путь в графе Γ – это последовательность различных вершин $v_1, v_2, \ldots, v_n$, такая, что $\{v_i, v_{i+1}\} \in E$, $1 \le i \le n$. Гамильтонов путь в графе Γ из вершины s в вершину t – это простой путь из s в t, который включает все вершины графа Γ.

Как и для предыдущей задачи, все построения будем проводить над алгебраически замкнутым полем комплексных чисел C . Поставим в соответствие вершинам $v_1, v_2, \ldots, v_n$ графа Γ переменные $x_1, x_2, \ldots, x_n$ и введём две вспомогательные переменные w и z . Можно считать, что $s = v_1$ и $t = v_n$. Чтобы решить задачу о построении гамильтонова пути в графе Γ из вершины s в вершину t, достаточно найти биективное отображение f из множества вершин графа Γ на множество натуральных чисел $\{1, 2, \ldots, n\}$, сопоставляющее вершине v_i число i и обладающее следующим свойством: если f отображает две вершины в натуральные числа k, $k + 1$, то эти вершины должны быть смежными в графе Γ. Отображение f с указанными свойствами существует тогда и только тогда, когда разрешима следующая система полиномиальных уравнений:

$$x_1 - 1 = 0, \ldots, x_n - n = 0,$$

$$(x_i - 1)(x_i - 2)\ldots(x_i - n) = 0, \quad 1 < i < n,$$

$$1 - z \prod_{1 \le i < j \le n} (x_i - x_j) = 0,$$

$$1 + y - (x_i - x_j)^2 y = 0, \quad 1 \le i < j \le n, \{v_i, v_{i+1}\} \notin E.$$

Рассмотрим идеал I кольца полиномов $C[x_1, x_2, \ldots, x_k, z, w]$, порожденный полиномами:

$$x_1 - 1, \ldots, x_n - n;$$

$$(x_i - 1)(x_i - 2)\ldots(x_i - n), 1 < i < n;$$

$$1 - z \prod_{1 \le i < j \le n} (x_i - x_j),$$

$$1 + w - (x_i - x_j)^2 w = 0, 1 \le i < j \le n, \{v_i, v_{i+1}\} \notin E.$$

Вычислим редуцированный базис Грёбнера G идеала I с помощью системы компьютерной алгебры Maple, задав лексикографическое упорядочение термов в кольце полиномов $C[x_1, x_2, \ldots, x_k, z, w]$, для которого

$$x_1 > x_2 > \ldots > x_n > z > w.$$

Рассмотрим многообразие $V(I)$, содержащееся в C^{n+2} . Ясно, что граф Γ имеет гамильтонов путь из вершины s в вершину t, тогда и только тогда, когда многообразие $V(I)$ не пусто. По теореме Гильберта о нулях [1] $V(I)$ не пусто в том и только в том случае, когда 1 не принадлежит редуцированному базису Грёбнера G идеала I. Итак, выяснив для конкретного графа, что гамильтонов путь у него существует, продолжаем работу. (В противном случае, выбираем новый граф.) Наша цель: найти какой-нибудь гамильтонов путь в данном графе из вершины s в вершину t. Такой путь может быть найдена комбинаторными методами, если известен базис Гребнера G идеала I. Решив систему полиномиальных уравнений, тем самым находим секретный ключ криптосистемы – вектор $y \in C^{n+2}$, и открытый ключ – множество полиномов базиса Грёбнера G идеала I из $C[x_1, x_2, \ldots, x_k, z, w]$. Далее – всё по схеме. Чтобы отослать сообщение m, Боб генерирует полином

$$p = \sum h_j q_j$$

идеала I , порожденного множеством полиномов G, и отсылает Алисе полином

$$c = p + m$$

Когда Алиса получает зашифрованный полином c , она находит m, вычисляя значение зашифрованного полинома в точке y:

$$c(y) = p(y) + m = m.$$

В заключение заметим, что данные алгебро-комбинаторные криптосистемы с открытым ключом могут использоваться как элементы гибридных криптосистем.

1. Koblitz Neal. Algebraic Aspects of Criptography / Neal Koblitz. – Berlin: Springer, 1991. – 206 p.
2. Mishra Bhubaneswar. Algorithmic Algebra / Bhubaneswar Mishra. – New York: Springer, 1993 – 417 p.