АЛГОРИТМЫ ОПРЕДЕЛЕНИЯ ЭЛЕМЕНТОВ ИНКАПСУЛИРОВАННЫХ КОЛЕЦ ВЫЧЕТОВ

А.В. Трепачева

Южный федеральный университет, Большая Садовая 105/42, 344006 Ростов-на-Дону, Россия
alina1989malina@ya.ru

Инкапсулированные (black-box) представления алгебраических структур помогают оценить сложность алгоритмов, которые строятся безотносительно конкретного представления элемента [1, 2, 3].

Практическая ценность инкапсулированных колец состоит в том, что они дают оценки на сложность криптоанализа полностью гомоморфных криптосистем в атаке на основе шифртекстов [4, 5].

Определение 1. *Инкапсулированное кольцо вычетов – это шестерка* (n, k, h, F, G, T) *в которой* $n \in \mathbb{N}$ *– определяет количество элементов в кольце,* $k \in \mathbb{N}$ *– определяет длину битового представления кодировки. Функции* h, F, G, T *определены следующим образом.*

1. *Функция* $h : \{0,1\}^k \to \mathbb{Z}_n$ *сопоставляет элемент из кольца каждой* k*-битной двоичной строке. Функция* h *сюръективна, т. е. каждый элемент кольца представлен по меньшей мере одной битовой строкой.*

2. *Функции* $F, G : \{0,1\}^k \times \{0,1\}^k \to \{0,1\}^k$ *выполняют сложение и умножение. Они удовлетворяют следующим соотношениям* $h(F(x,y)) = h(x) + h(y)$ *и* $h(G(x,y)) = h(x)h(y)$.

3. *Функция* $T : \{0,1\}^k \times \{0,1\}^k \to \{\texttt{true}, \texttt{false}\}$ *проверяет равенство двух инкапсулированных элементов:* $T(x,y) = \texttt{true}$ *тогда и только тогда, когда* $h(x) = h(y)$.

Определение 2. *Пусть*(n, k, h, F, G, T) *– инкапсулированное кольцо вычетов. Обозначим отображение, сопоставляющее элементу* x *некоторое представление* $[x]$ *как* $[]$. ***Проблема инкапсулированного кольца вычетов*** *состоит в следующем: найти алгоритм* $\mathcal{A}$ *который по данному* n *и оракулам* $F, G, T, []$ *и представлению* $\alpha \in \mathbb{Z}_n$ *находит* α *в явном виде.*

Искомый алгоритм $\mathcal{A}$ может быть представлен в виде последовательности ответов на вопросы вида « $f([x]) = 1?$ » , где $f([x])$ – полином, эффективно вычислимый в инкапсулированном кольце (n, k, h, F, G, T).

Определение 3. *Функцию (полином)* $f([x])$ *будем называть эффективно вычислимой в инкапсулированном кольце вычетов* (n, k, h, F, G, T)*, если её можно вычислить, пользуясь оракулами* F*,* G *и* T *лишь* $O(\log n)$ *раз.*

Определение 4. *Полином* $f([x])$ *будем называть разреженным в инкапсулированном кольце вычетов* (n, k, h, F, G, T)*, если количество его ненулевых коэффициентов равно* $O(\log n)$.

Разреженный полином в кольце (n, k, h, F, G, T) всегда является эффективно вычислимой функцией.

Лемма 1. *Если* $f([x])$ *– эффективно вычислимая функция, то* $f([x])^d$ *– также эффективно вычислимая функция.*

Возводить полином в степень, большую чем n не имеет смысла, поэтому достаточно возвести его в степень $d' = d \bmod n$. Для этого можно воспользоваться алгоритмом быстрого возведения в степень: сначала получить двоичное представление числа $d' = d'_{\log_2 n} ... d'_1 d'_0$, далее последовательным возведением в квадрат получаем $f([x])^2, f([x])^4, f([x])^8, f([x])^{16}, ..., f([x])^{2^{\lceil \log_2 n \rceil}}$. Результат получается перемножением тех степеней, при которых в двоичном разложении d' стояла единица, т.е.

Теорема. *В случае кольца вычетов по простому модулю существует такая последовательность эффективно вычислимых функций* $f_i([x]),\ 0 \leq i \leq O(\log_2 n)$ *(которую будем называть классифицирующей), что последовательными ответами на вопросы вида* $f_i([x]) = 1$*? элемент инкапсулированного кольца определяется по своему представлению однозначно.*

Идея доказательства состоит в том, что $x^{\frac{n-1}{2}} \bmod n$ в случае, если n – простое число является символом Лежандра и в половине случаев равен 1, что позволяет удачно классифицировать элемент x.

Свойства разреженных полиномов похожи на свойства случайных перестановок в $\mathbb{Z}_n$ и можно показать что при количестве этих полиномов с подавляющей вероятностью найдется такой, который принимает значение 1 на приблизительно половине элементов произвольно выбранного множества.

Таким образом, получается, что на каждом шаге с помощью некоторого разреженного полинома возможно с подавляющей вероятностью «сузить» область поиска примерно вдвое, что можно представить в виде бинарного дерева поиска в листьях которого находятся элементы инкапсулированного кольца вычетов и это дерево будет сбалансировано.

Работа выполнена при финансовой поддержке гранта РФФИ №15-07-00597 А.

Литература

1. Arvind V., Das B., and Mukhopadhyay P. *The complexity of black-box ring problems.* // Computing and Combinatorics, Springer, 2006. P. 126–135.

2. Boneh D. and Lipton R. J. *Algorithms for black-box fields and their application to cryptography.* // Advances in Cryptology—CRYPTO'96, Springer, 1996. P. 283–297.

3. Zumbragel J., Maze G., and Rosenthal J. *Efficient recovering of operation tables of black box groups and rings.* // IEEE International Symposium on Information Theory, 2008 (ISIT 2008). IEEE, 2008. P. 639–643.

4. Maurer U. *Abstract models of computation in cryptography* // Cryptography and Coding. Springer Berlin Heidelberg, 2005. P. 1-12.

5. Jager T. *Black-Box Models of Computation in Cryptology.* – Springer Science & Business Media, 2012.