А. М. Коренева

СИСТЕМАТИЗАЦИЯ ТЕОРЕТИКО-ГРАФОВЫХ МОДЕЛЕЙ В КРИПТОЛОГИИ

Теория графов активно применяется во многих областях знаний, где предметом изучения являются сложные системы, элементы которых связаны определенным образом.

В статье представлены многообразные связи теории графов [1] с математическими задачами криптологии, направленными на разработку методов построения и анализа криптографических систем.

Известно, что математический базис криптологии образуется рядом дисциплин: теорией групп, полугрупп, теорией автоматов, математическим анализом, теорией чисел, теорией вероятностей, теорией графов и др. Основной задачей выполнения обзора является систематизация теоретико-графовых моделей, применяемых в криптологии [2].

В силу наглядности теория графов используется в качестве удобного и простого языка для построения и исследования математических моделей различных объектов, в том числе криптографических функций и систем.

Связь теории графов и криптологии можно проиллюстрировать рядом примеров. Семейству преобразований любого эндоморфного шифра соответствует помеченный граф, вершинами которого являются шифруемые элементы текста, а дуги помечены используемым ключом. В частности, квадратная таблица размера n x n, определяющая табличный шифр, может быть легко преобразована в n-вершинный граф. Также при помощи графов решаются системы уравнений. Такой способ решения носит название «метод ветвей и границ». Свойство транзитивности полугрупп и групп преобразований, связанных с шифром, может быть интерпретировано как сильная связность соответствующего графа [3]. Задача изоморфизма графов в криптологии связана с задачей выявления эквивалентных криптографических ключей.

Также существует ряд прикладных задач, в решении которых методы теории графов часто связаны с исследованием свойств множества путей в определенных графах. К таким задачам в криптологии относится исследование существенной зависимости функций от переменных. Важными характеристиками перемешивающих свойств системы преобразований являются экспонент и субэкспонент системы соответствующих графов преобразований. Наличие хороших перемешивающих свойств является важным для построения преобразований, распространяющих искажения в криптографических системах аутентификации [4], и для оценки сложности решения систем уравнений относительно методов последовательного опробования ключей.

При выполнении работы, связанной с анализом и систематизацией теоретико-графовых моделей в криптологии, была использована как отечественная, так и зарубежная литература.

Первым рассмотренным классом являются теоретико-графовые модели бинарных отношений. В криптологии часто исследуются бинарные отношения частичного порядка или квазипорядка на множествах, чаще на конечных множествах. Если для элементов x и y множества X выполнено отношение $x \leq y$, то в соответствующем графе Г с множеством вершин X пара (x, y) образует дугу. При таком определении множеству X с линейным порядком соответствует гамильтонов путь. Граф, соответствующий частично упорядоченному множеству, называют диаграммой ч. у. м. Известно, что теория решеток является теоретической основой решения задачи теории кодирования и криптографии, такой как безошибочная передача данных с обеспечением их защиты от несанкционированного доступа [5].

Кроме того, можно выделить теоретико-графовые модели алгебраических систем, в частности графы Кэли и графы, построенные по системе образующих элементов. Граф Кэли

группоида представляет собой помеченный n-вершинный ориентированный граф с множеством вершин $G = \{g_i\}$, с множеством меток G и с множеством дуг $U = \{(g_i,g_ig_j) : (g_i,g_j) \in G^2\}$, где дуга (g_i,g_ig_j) помечена символом g_j. Каждой полугруппе можно сопоставить ее граф Кэли, определяемый полугрупповой операцией. Граф Кэли полугруппы определяется аналогично графу Кэли группоида. Отметим, что в графе Кэли полугруппы могут существовать параллельные дуги. Граф Кэли группы определяется аналогично графу Кэли полугруппы. Вместе с тем все элементы группы G обратимы относительно заданной операции, отсюда следуют свойства графа Кэли:

— граф является полным и не содержит параллельных дуг;

— граф является псевдосимметрическим порядка $|G|$;

— между любыми двумя вершинами имеется пара дуг с противоположными ориентациями и взаимно обратными метками;

— таблица Кэли представляет собой латинский квадрат над множеством G.

Изучение протоколов аутентификации типа «запрос-ответ», в основе которых лежат графы Кэли группы Кокстера, является одной из актуальных задач современной криптографии [6].

Также были проанализированы теоретико-графовые модели криптографических функций, заданных на множестве слов конечной длины, графы преобразований и систем преобразований множества, графы сдвиговых регистров, автоматные графы. Особый интерес в криптологии представляют преобразования множеств слов над конечным алфавитом, т. е. преобразования множества X^n, где X — конечное множество. Среди них важное место занимают преобразования регистров сдвига над кольцами и полями, которые представляет интерес в связи с активным использованием сдвиговых регистров при построении криптографических схем.

Рассмотрен класс графовых моделей полугрупп и групп преобразований, построенных по системе образующих элементов.

При построении криптосистемы важным условием криптографической стойкости является нелинейность реализуемых отображений, а также перемешивающие свойства отображений. Функции с полным перемешиванием входов используются в системах аутентификации, поскольку обладают свойством распространения искажений входных данных. С точки зрения анализа стойкости криптографической системы к функциям шифрования с неполным перемешиванием входов применим метод последовательного опробования при определении ключа [3].

Перемешивающие свойства отображения φ определяются системой множеств $\{S(f_1),\ldots,S(f_m)\}$, где $S(f_i)$ — множество номеров существенных переменных координатной функции $f_j(x_1,\ldots,x_n)$, $j = 1,\ldots m$. Функции φ соответствует двудольный орграф $\Gamma_D(\varphi)$ с множеством вершин $1,\ldots,n + m$ и множеством дуг $U_\varphi = \{(i,j + n)\}$, где $i \in \{1,\ldots,n\}$ и $j \in \{1,\ldots,m\}$ (вершины $1,\ldots,n$ — номера переменных, а вершины $n + 1,\ldots,n + m$ соответствуют координатным функциям $f_1(x_1,\ldots,x_n),\ldots,f_m(x_1,\ldots,x_n)$). Пара $(i,j + n) \in U_\varphi \Leftrightarrow i \in S(f_j)$, что означает существенную зависимость функции f_j от переменной x_i. Граф $\Gamma_D(\varphi)$ называется перемешивающим графом функции φ. Функция φ называется совершенной, или вполне перемешивающей, если двудольный орграф $\Gamma_D(\varphi)$ является полным, т. е. имеет $m{\cdot}n$ дуг. Почти все функции $\varphi{:}X^n \to X^m$ являются совершенными при $n \to \infty$, m,k, ограниченных величиной порядка n. Однако подобный вывод не применим к функциям, используемым в криптографических схемах, так как они выбираются не случайно, а из отображений с рядом заданных свойств. Поэтому изучение перемешивающих свойств криптографических функций — актуальная задача.

В работе систематизирован ряд используемых в криптологии теоретико-графовых моделей, проанализированы их свойства. Показаны некоторые применения графовых моделей в криптографических приложениях.

СПИСОК ЛИТЕРАТУРЫ:

1. *Оре О.* Теория графов: Пер. с англ. 2-е изд. М.: Книжный дом «Либроком», 2009. – 352 с.
2. *Коренева А. М.* О некоторых результатах систематизации теоретико-графовых моделей, используемых для решения задач криптологии // XIV Международная телекоммуникационная конференция студентов и молодых ученых «МОЛОДЕЖЬ И НАУКА». Тезисы докладов. Ч. 3. М.: НИЯУ МИФИ, 2010. С. 239–241.
3. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. – 424 с.
4. *Фомичев В. М.* Свойства путей в графах и мультиграфах // Прикладная дискретная математика. 2010. №1, С. 118–124.
5. *Кутьин А. М.* Коды, композиции и решетки // Прикладная дискретная математика. 2008. № 1, С. 15–20.
6. *Sagols F. and Morales-Luna G.* Two identification protocols based on Cayley graphs of Coxeter groups. URL: http://eprint.iacr.org/2010/470.pdf.