ПДМ. 2012. № 4(18).

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

ДИСКРЕТНЫЕ МОДЕЛИ РЕАЛЬНЫХ ПРОЦЕССОВ

ИСТОРИЧЕСКИЕ ОЧЕРКИ ПО ДИСКРЕТНОЙ МАТЕМАТИКЕ И ЕЁ ПРИЛОЖЕНИЯМ

АНАЛИТИЧЕСКИЕ ОБЗОРЫ

ŋqdqɏəɎ bɆ dədɆbɎзə d ɕɔɑbɔɏ Ɉqdd Ɏqɏè

108–122

Агибалов Г. П., Панкратова И. А. Sibecrypt'12. Обзор докладов // ПДМ. 2012. № 4(18). С. 108–122.

ŋqdqɏeɎ bɆ dədɆbɎɜə d ɕɔɑbɔɏ Ɉqddɏqɏè

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.6

ПОЛОЖИТЕЛЬНЫЕ СВОЙСТВА НЕОТРИЦАТЕЛЬНЫХ МАТРИЦ

К. Г. Когос*, В. М. Фомичев**

**Национальный исследовательский ядерный университет (МИФИ), г. Москва, Россия*
***Финансовый университет при Правительстве Российской Федерации, г. Москва, Россия*

E-mail: fomichev@nm.ru

Дан обзор результатов исследования примитивности графов (неотрицательных матриц) и некоторых направлений обобщения. Приведены оценки экспонентов различных классов графов и систем графов (матриц и систем матриц).

Ключевые слова: *примитивный граф, примитивная матрица, экспонент, субэкспонент.*

Одним из положительных криптографических свойств преобразований векторных пространств является хорошее перемешивание, то есть зависимость каждой координатной функции от всех переменных. Перемешивающие свойства преобразования g пространства P^n над полем P, заданного системой координатных функций $\{g_1(x_1,\ldots,x_n),\ldots,g_n(x_1,\ldots,x_n)\}$, определяются системой множеств $\{S(g_1),\ldots,S(g_n)\}$, где $S(g_j)$ — множество номеров существенных переменных координатной функции $g_j(x_1,\ldots,x_n)$, $j=1,\ldots,n$. Наилучшее перемешивание достигается, если каждая из координатных функций преобразования g зависит от всех переменных, то есть $S(g_j)=\{1,\ldots,n\}$, $j=1,\ldots,n$. Такие преобразования принято называть совершенными. Обобщениями свойства совершенности функций являются такие свойства, как строгий лавинный критерий, критерии распространения, свойство «бент».

Почти все преобразования векторного пространства P^n над конечным полем P являются совершенными при $n\to\infty$. Однако подобный вывод неприменим к функциям, используемым в криптографических системах, так как они выбираются не случайно, а из отображений с рядом заданных свойств. Поэтому изучение перемешивающих свойств криптографических функций — актуальная задача криптографического анализа.

Некоторые функции с полным перемешиванием обладают свойством распространения искажений входных данных, что позволяет использовать их в криптосистемах аутентификации. С другой стороны, к функциям шифрования с неполным перемешиванием входов применимы методы определения ключа типа последовательного опробования, что делает привлекательным использование в криптосистеме шифрования совершенных преобразований.

Аппаратная или программная реализация совершенных преобразований затруднена в связи с необходимостью реализации функций от большого числа переменных. Поэтому для хорошего перемешивания используются итерации (возведение в степень) преобразования с относительно слабыми перемешивающими свойствами. Показатель степени преобразования, при которой достигается хорошее перемешивание, является

ŋqdqayeY bȨ deqȨbYae d ecaqcy Ǝqdqyqè