массива позволяет построить n различных отображений для разделения секрета. Любая комбинация из t различных отображений позволяет построить алгоритм восстановления.

Оценка защищенности алгоритма.

Предположим, требуется восстановить массив данных с помощью (t, n)-схемы. При этом используется конструкция из m полиномов. Каждый полином использует t неизвестных коэффициентов. Пусть имеется только $(t-1)$ отображений массива, что позволяет построить систему из $(t-1)$ уравнений. В данной ситуации невозможно вычислить точно i-й корень системы из $(t-1)$ уравнений. Возможно только вероятностное угадывание правильного результата. Вероятность правильного восстановления полного массива без

$$\left(1/p\right)$$

ошибок в этом случае можно оценить как .

Векторные схемы обеспечивают защиту в распределенной системе хранения информации и могут быть рекомендованы для применения в системах, обеспечивающих безопасность инфраструктуры открытых ключей

СХЕМА РАЗДЕЛЕНИЯ СЕКРЕТА НА АЛГЕБРО-ГЕОМЕТРИЧЕСКИХ КОДАХ

Т.М. Казубович, С.Б. Саломатин

Схема разделения секрета (СРС) включает в себя центр, формирующего секрет, и участников сети, получающих часть от этого секрета. Только объединившись в коалиции, *n* участников пороговой схемы «*n* из *N*» могут восстановить секрет. В СРС участники параметризуются элементами конечного поля, что геометрически означает ось абсцисс, а так же еще одного «несобственного» участника, соответствующего «бесконечно удаленной» точке.

С геометрической точки зрения для реализации СРС удобно использовать коды, построенные на кривых и точки на них для параметризации участников.

Для произвольной ненулевой рациональной функции f над кривой C и произвольной точки *P* этой кривой можно определить целое число $ord_P(f)$, называемое порядком этой функции в точке P.

Если в коалиции участников меньше чем n, то такая коалиция будет неразрешенной. Если в коалиции участников ровно n, и сумма точек-участников не равна 0, то это – разрешенная коалиция. Если в коалиции участников ровно n, и сумма точек-участников равна 0, то это – неразрешенная коалиция. Если в коалиции более чем n участников, то она будет неразрешенной тогда и только тогда, когда сумма любых ее n точек-участников равна нулю.

Основой описания минимальных разрешенных коалиций и циклов является понятия матроида. При случайном выборе коалиций они будут разрешенными с очень большой вероятностью. Число всех коалиций определяется латинским N-мерным квадратом, при этом вероятность неразрешимости коалиции участников можно оценить как $n!/N$.

$$\frac{N^{n-1}}{C_N^n} = O(N^{-1}) \approx \frac{k}{N} \sim \frac{n!}{N}$$

КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ, БАЗИРУЮЩИЕСЯ НА МАТЕМАТИЧЕСКОЙ КОНЦЕПЦИИ ГЕОМЕТРИЧЕСКОЙ НЕПРЕРЫВНОСТИ

С. Б. Саломатин, В.В. Панькова

Геометрические криптосистемы используют непрерывность метрики. Суть непрерывных криптосистем состоит в том, что открытые тексты и крипто-тексты являются элементами таких областей как действительные (комплексные) числа или действительные

векторные пространства, процедуры процесса шифрования и расшифрования используют непрерывное преобразование этих областей.

Каждый открытый текст представляется как точка топологии пространства X, каждый криптотекст является точкой топологии Y, каждая процедура шифрования/расшифрования рассматривается как непрерывный изоморфизм между X и Y.

При рассмотрении непрерывных криптосистем можно использовать понятие дискретизации непрерывных объектов. Дискретизация предполагает введение в рассмотрение точных раундовых процедур преобразования.

Метрическая система с точки зрения информационного подхода определяется как непрерывная криптосистема со следующими свойствами:

– определено точное конечное подмножество P для X как пространство открытых текстов;

– точно определено конечное подмножество C для Y как пространство криптотекстов;

– каждая процедура шифрования/расшифрования выполняется итеративно в виде раундов преобразований, гарантирующих отображение $P \to C$.

Обнаружение ошибки при передаче криптотекстов. Рассмотрим ситуацию, когда открытый текст представляется как дискретная точка в $\mathbf{R}^n$ (точка, принадлежащая решетке $\mathbf{Z}^n$ в $\mathbf{R}^n$, где $\mathbf{Z}$ – множество всех целых чисел), а криптотекст получается в результате непрерывного не обязательно везде дискретного преобразования. Любая ошибка, произошедшая при передаче криптотекста, делает маловероятным, событие размещения результата расшифрования в дискретной точке. Следовательно, результат расшифрования, размещенный не в дискретный точке, может свидетельствовать об ошибке при передаче криптотекста.

МОДИФИЦИРОВАННЫЙ АЛГОРИТМ ШИФРОВАНИЯ И ЕГО КРИПТОАНАЛИЗ

А.В. Сидоренко, Д.А. Жуковец

В современном мире информационный ресурс стал одним из наиболее мощных рычагов экономического развития.

Наряду с традиционными алгоритмами шифрования, которые постоянно разрабатываются и совершенствуются, все большую популярность в криптографическом сообществе приобретают алгоритмы шифрования на основе систем динамического хаоса.

Целью работы является разработка алгоритма и программных средств для шифрования на основе динамического хаоса, а также исследование его устойчивости к различным видам криптоатак.

В результате проведенных исследований нами был разработан алгоритм, а также программа для шифрования и расшифрования открытого текста с использованием динамического хаоса. Для доказательства стойкости алгоритма шифрования проведено определение количественных параметров, таких как информационная энтропия, числовых характеристик распределения значений байт в открытом и зашифрованном тексте, корреляция, процент бит изменивших значение (лавинный эффект), процент пикселей изменивших значение (Number of Pixels Change Rate), среднее изменение интенсивности (Unified Average Changing Intensity). Проведен линейный и дифференциальный криптоанализ алгоритма шифрования

Литература

1. Chaos-based secure satellite imagery cryptosystem / M. Usama et al. // Computers and Mathematics with Applications 60 (2010) 326-337

2. A chaos-based image encryption scheme using 2D rectangular transform and dependent substitution / Xuanping Zhang, Xing Fan, JiayinWang, Zhongmeng Zhao // Springer (2014)