одной или более частей сообщения (но не всех) и ее расшифровывание не дает возможности получить все сообщение целиком.

Литература

1. Freier A. The Secure Sockets Layer (SSL) Protocol Version 3.0 – August 2011.

МОДЕЛИРОВАНИЕ АКУСТИЧЕСКИХ ЗАДАЧ С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОГО СРЕДСТВА

И.В.Савченко

Одним из подходов к решению проблема защиты речевой информации от утечек по акустическому каналу является разработка базовой программной модели, которая основана на адаптации физической модели под программную реализацию. Для разработки программного средства определены входные и выходные параметры базовой физической модели, критерии выбора среды разработки и непосредственно сама среда разработки программного средства, а также предложена архитектура программного средства.

Входные величины и параметры, которыми будет оперировать разрабатываемая программная реализация акустической модели, основываются на наборе математических формул и уравнений акустики, описывающих физические процессы в рамках заданного класса акустических задач.

С учетом требований к программной реализации и исследуемой физической модели, оптимальным языком программирования является Java, позволяющий создавать программы в соответствии с концепциями объектно-ориентированного программирования в рамках распространенных паттернов проектирования.

Архитектура программного средства представлена в виде набора шаблонов проектирования, оптимальным из которых является шаблон проектирования «Мост». При реализации базовой архитектуры приложения через шаблон «Мост», изменение структуры интерфейса не мешает изменению структуры реализации.

На основании разработанной архитектуры реализован прототип программного средства, демонстрирующий работу описанного выше алгоритма в рамках выбранной математической модели. В качестве входных параметров заданы: размер помещения и взаимное расположение стен; источник звука, являющийся центром исходящих лучей; точность расчета, включающая в себя количество лучей и количество отражений. Чтобы иттерационно продемонстрировать принцип работы алгоритма, при работе с программой изменялись значения, определяющие точность заданных параметров.

ЗАЩИТЫ ДАННЫХ НА ОСНОВЕ ВЕКТОРНОЙ СХЕМЫ РАЗДЕЛЕНИЯ СЕКРЕТА В РАСПРЕДЕЛЕННОЙ СИСТЕМЕ ХРАНЕНИЯ ИНФОРМАЦИИ

С.Б. Саломатин, Т.А. Андриянова

Распределенные системы хранения информации широко используются в современных инфокоммуникационных системах. При этом появляется возможность использовать пространственно-временную избыточность распределенных систем для защиты информации.

Один из методов защиты данных может быть основан на схеме разделения секрета среди группы пользователей (агентов) распределенной информационной сети.

Векторная пороговая схема, использующая геометрию точек в пространстве.

Сообщение определяется как точка в n-мерном пространстве. Каждое уравнение в пороговой схеме – это уравнение $(n-1)-$ мерной гиперплоскости, содержащей эту точку.

Защищаемые массивы данных, разбиваются на несколько отображений. Коэффициенты отображений выбираются случайным образом из множества целых чисел меньших модуля p или используются элементы массива данных. Матричное представление

Библиотека БГУИР

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

Библиотека БГУИР