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