УДК 621.391

ОПТИМИЗАЦИЯ МЕТОДОВ ЗАЩИТЫ НАУКОЕМКИХ ТЕХНОЛОГИЙ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

А. И. Астайкин, А. А. Курочкин, А. П. Мартынов, В. Б. Профе
Российский федеральный ядерный центр – ВНИИ экспериментальной физики, Саров, Россия

Предложен метод устранения избыточности информации при дискретном представлении одного из основных законов криптографии – закона перестановки.

Одна из важнейших задач прикладной физики – создание наукоемких технологий. Ожидается, что в XXI веке международный коммерческий обмен наукоемкими технологиями в финансовом выражении может превысить объем торговли сырьем, оружием и т. д. При этом наукоемкие технологии должны быть признаны стратегическим ресурсом страны, а требования к защите коммерческой тайны в этой области становятся по уровню соизмеримыми к требованиям по защите государственной и военной тайны.

Информация о новейших технологиях возникает еще на этапе физических исследований, и по мере ее продвижения к формированию конкретных технологических решений становится все более привлекательным объектом промышленного шпионажа. При этом ученым-физикам с неизбежностью приходится овладевать методами защиты информации от несанкционированного доступа.

Защита конфиденциальной информации требует применения тех или иных криптографических законов или алгоритмов. Очевидно, что чем большей избыточностью будет обладать зашифрованная информация, тем легче ее конфиденциальность может быть нарушена потенциальным злоумышленником.

Одним из основных законов криптографии является закон перестановки (рис. 1). Входные символы информации A_1, ..., A_n перемешиваются определенным (неслучайным) образом. В результате образуется выходная комбина-

ция символов B_1, ..., B_n. Перестановку можно осуществлять на уровне слов, символов или отдельных бит информации. Существует несколько способов представления закона перестановки [2]: графический, аналитический и табличный.

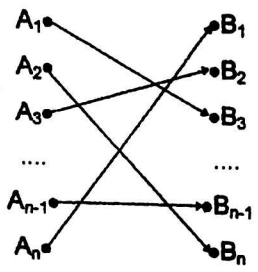

Рис. 1. Закон перестановки

Табличный способ является наиболее удобным и наглядным для представления на ЭВМ в дискретной форме, когда каждый элемент перестановки представляется соответствующим ему определенным числом. Однако, наряду с неоспоримыми преимуществами, этот способ обладает информационной избыточностью, которая в свою очередь ведет не только к увеличению используемых ресурсов памяти, но и к снижению криптостойкости всей системы. Последнее особенно критично в вычислительных системах обработки и хранения конфиденциальной информации, полученной в результате проведения ряда физических экспериментов.

Рассмотрим количественную оценку избыточности.

Перестановка из N элементов представляется табличным способом в дискретной форме в виде последовательности N дискретных значений, соответствующих элементам. Последовательность имеет разрядность R_1 бит:

$$R_1 = N \cdot \mathrm{ROUND}\ (\log_2 N), \qquad (1)$$

где ROUND(A) – наименьшее целое число, не меньшее числа A.

С другой стороны, перестановка из N элементов может быть однозначно представлена в дискретной форме соответствующим ей натуральным числом разрядности R_2:

$$R_2 = \mathrm{ROUND}(\log_2 (N!)). \qquad (2)$$

Из выражений (1) и (2) видно, что $R_1 > R_2$ при любом значении N, и при табличном способе дискретного представления перестановки из N элементов возникает избыточность.

Следует отметить, что табличное представление перестановки из N элементов имеет избыточность при любом значении N, а не только для N, некратных 2, как может показаться на первый взгляд. Это объясняется тем, что число возможных перестановок из N элементов равно $N!$, в то время как для выражения (1) максимальное двоичное число разрядности R равно N^N, для N, кратных 2 и не менее N^N, для N, некратных 2, которое больше $N!$ для любого натурального $N>1$.

График зависимости избыточности табличного способа представления от количества элементов перестановки приведен на рис. 2.

Анализ способов представления перестановок в целях сокращения избыточности информации в их дискретной форме привел к созданию авторами метода факториального сжатия.

Суть метода заключается в представлении перестановки в виде однозначно соответствующего ей натурального числа. Исходная перестановка представляется табличным способом.

Рис. 2. График зависимости избыточности табличного способа представления от количества элементов перестановки

График зависимости коэффициента сжатия дискретного информационного блока по методу факториального сжатия от числа элементов перестановки приведен на рис. 3.

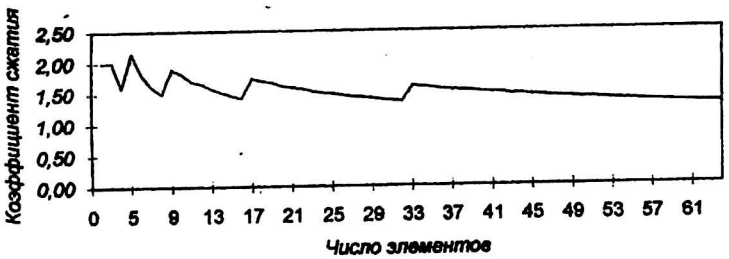

Рис. 3. График зависимости коэффициента сжатия дискретного информационного блока по методу факториального сжатия от количества элементов перестановки

Как видно из графиков, представленных на рис. 2 и 3, разработанный метод позволяет практически полностью исключить информационную избыточность, возникающую при дискретном представлении перестановки из N элементов, и достигает, таким образом, максимального теоретически возможного сжатия дискретных информационных блоков, соответствующих перестановкам.

Метод факториального сжатия информации включает в себя следующие процедуры преобразования:

упаковку произвольной перестановки (процедура преобразования неупакованной перестановки в упакованную форму);

распаковку предварительно упакованной перестановки (процедура преобразования упакованной формы перестановки в неупакованную).

Процедура упаковки исходной произвольной перестановки из N элементов в упакованную форму осуществляется в три этапа:

представление перестановки последовательностью модифицированных численных значений;

формирование элементарных слагаемых;

формирование итоговой упакованной формы перестановки.

Процедура преобразования упакованной формы перестановки в неупакованную осуществляется в три этапа:

формирование элементарных остатков от деления;

формирование последовательности модифицированных численных значений, представляющей перестановку;

преобразование последовательности модифицированных численных значений в последовательность предварительно фиксированных численных значений.

Дальнейшая детализация метода, по понятным причинам, представляется нецелесообразной.

Следует отметить, что метод факториального сжатия информации не зависит от размерности исходного блока информации, представляющего перестановку и подвергаемого сжатию, так как изначально не привязан к определенной размерности информационного блока. Это делает его универсальным. Размер исходного блока информации является входным параметром, который настраивает рабочие параметры алгоритма преобразования. Кроме того, разработанный метод является несложным в реализации и может быть практически реализован на любом персональном компьютере или микропроцессоре, обладающем минимальным набором математических функций.

Разработанное авторами программное обеспечение для обработки результатов физических экспериментов реализует на практике метод факториального сжатия и подтверждает работоспособность предлагаемого метода для любой размерности информационного блока.

Литература

1. *Хоффман Л.* Современные методы защиты информации: Пер. с англ./ Под ред. В. А. Герасименко. – М.: Сов. радио, 1980. – 264 с.

2. *Конхейм А. Г.* Основы криптографии: Пер. с англ. – М.: Радио и связь, 1987. – 412 с.

Optimization of guard methods of higt-end technologies from unauthorized access

A. I. Astaikin, A. A. Kurochkin, A. P. Martynov, V. B. Profe
All-Russia Scientific Research Institute of Experimental Physics, Sarov, Russia

The method of redundancy reduction of the information is offered at discrete representation of one of fundamental laws of cryptography – law of transposition.