ОБ ОДНОМ СПОСОБЕ ГИПЕРСЕТЕВОГО КОДИРОВАНИЯ С УЧЕТОМ КРИПТОЗАЩИТЫ И ИМИТОСТОЙКОСТИ

Д. С. Легкий, В. К. Попков*

Сибирский государственный университет телекоммуникаций и информатики,
630102, Новосибирск, Россия
* Институт вычислительной математики и математической геофизики СО РАН,
630090, Новосибирск, Россия

УДК 004.056.55

Рассматриваются вопросы создания принципа шифрования на основе сложной многоуровневой сетевой структуры — гиперсети. Предлагаемый принцип включает непосредственную защиту от различных видов нарушения целостности данных.

Ключевые слова: гиперсеть, блочный алгоритм шифрования, гиперсетевая основа, защита информации, имитостойкость.

The article deals with the creation of the principle of encryption based on a complex multilayered network structure hypernet. Moreover, this principle includes the direct protection from various types of data integrity.

Key words: hypernetwork, block cipher algorithm, hypernetwork basis, information protection, imitation resistance.

Введение. Шифрование данных не является гарантией их целостности, поэтому в криптографии используются дополнительные методы обеспечения целостности данных. Под нарушениями целостности данных понимаются инверсия битов, добавление новых битов (в частности, новых данных) третьей стороной, удаление битов данных, изменение порядка следования битов или их групп.

В криптографии решение задачи целостности информации предполагает применение мер, позволяющих обнаруживать не столько случайные искажения информации, сколько целенаправленное изменение информации активным криптоаналитиком. Процесс контроля целостности обеспечивается введением в передаваемую информацию избыточности [1].

Теория гиперсетей позволяет моделировать любой математический процесс, связанный с описанием и применением структур, поскольку обеспечивает наглядность процесса моделирования. Решение задачи защиты информации в процессе шифрования на основе сложной структуры позволяет не только надежно защитить данные, но и упростить аппаратно-программную реализацию алгоритма шифрования, так как процесс шифрования совпадает с процессом дешифрования, отличием является только порядок выполнения “раундов”.

Большинство современных блочных шифров, таких как Blowfish, Camellia, CAST-128, CAST-256, CIPHERUNICORN-A, CIPHERUNICORN-E и др. [1], в качестве основы используют сеть Фейстеля.

Альтернативой сети Фейстеля является подстановочно-перестановочная сеть, на основе которой построены такие шифры, как 3-Way, ABC, AES (Rijndael), Akelarre. Anubis, ARIA, BaseKing, BassOmatic и др.

Рассмотрим вариант алгоритма, в котором основой служит гиперсетевая структура и который является еще одной альтернативой блочным шифрам.

Описание алгоритма. Разобьем сообщение Z, записанное в двоичном коде, на блоки $b_j = \{k^l i\}$, где $\{k^l i\}$ – матрица из q столбцов и g строк, в которой $|b_j| = N$. Каждый блок b_j, в свою очередь, разобьем на d частей.

Пусть задана гиперсеть $S = (X, V, R)$, являющаяся долгосрочным ключом. Каждой вершине x_i из множества вершин $X = (x_1, x_2, ..., x_n)$ гиперсети S и каждой ветви v_p из множества ветвей $V = (v_1, v_2, ..., v_g)$ гиперсети S присваивается вес d, а именно часть секретного ключа (в двоичном виде). Во множестве $R = (r_1, r_2, ..., r_f)$ каждому ребру r_j ставится в соответствие цепь в графе первичной сети $PS = (X, V)$.

Пусть матричное представление гиперсети S задано матрицами инциденций $M^{xv}(S) = \{a_{ij}\}$, $M^{vr}(S) = \{b_{jk}\}$, $M^{xr}(S) = \{c_{ik}\}$, данные из которых будут использованы в процессе шифрования [2].

С использованием данных, описанных в $\{k^l i\}$, текущего ключа $K(Z) = (h_{1...}h_{(q\times g)})$ и гиперсети S построим кодировку следующим образом.

1. Первый раунд формирования шифротекста. Имеется три типа матриц:

1) N матриц $b_j = \{k^l i\}_j$, соответствующих исходным данным размерностей $n \times q$ (n — число столбцов; q — число строк);

2) матрица гиперсети S размерностей $M^{xv} - (n \times g)$;

3) матрица $K(Z)$ временного ключа размерностью $g \times q$.

Для каждой строки z очередного блока $\{k^l i\}_j$ матрицы b_j выполним следующую операцию: каждой ее строке поставим в соответствие строку того же размера новой матрицы $\{h^l i\}_j$ по следующему правилу:

1) выполнив сложение по модулю 2 строки z матрицы M^{xv} с соответствующим столбцом матрицы $K(Z)$, получаем матрицу D размерностью $n \times g$;

2) полученную матрицу D складываем по модулю 2 с матрицей $b_j = \{k^l i\}_j$.

В результате для всего сообщения Z получаем систему матриц $H_j = \{h^l i\}_j$ размерностью $n \times q$.

2. Второй раунд формирования шифротекста. Определим веса ребер вторичной сети по следующему правилу: вес ребра равен сумме весов инцидентных данному ребру ветвей. Результат данной операции — матрица весов ребер графа вторичной сети WM размерностью $q \times g$.

3. Третий раунд формирования шифротекста. Выполним операции, аналогичные операциям первого раунда, для следующих матриц:

1) N матриц $H_j = \{h^l i\}_j$ — матрицы размерностей $q \times n$;

2) матрица M^{xr} гиперсети S размерностей $n \times f$;

3) матрица WM весов ребер размерностью $q \times f$.

В результате получаем матрицу $WH_j = \{h^l i\}_j$ размерностью $q \times n$.

Аналогичные операции можно выполнить для гиперсетей S произвольного вида, что позволит увеличить криптостойкость данного алгоритма шифрования.

Процесс дешифрования полученного шифротекста осуществляется с помощью аналогичных операций.

Процесс шифрования с помощью гиперсети имеет следующие особенности:

1. Важным отличием гиперсети от сетей Фейстеля и подстановочно-перестановочных сетей является то, что гиперсетевая основа влияет на длину блока исходного текста: существует четкая зависимость длины исходного блока от количества вершин используемой гиперсети.

2. За счет введения в первичную сеть мультиветвей для блока исходного сообщения произвольной длины длина ключа может быть сколь угодно большой, но не меньше $n - 1$ (n — число вершин гиперсети).

3. Условием достижения максимального "лавинного эффекта" [3] с помощью гиперсети является включение в нее максимально возможного количества вторичных сетей.

4. При шифровании очередной блок шифротекста полностью определяется только соответствующим блоком открытого текста и значением секретного ключа, поэтому одинаковые блоки открытого текста будут преобразовываться в одинаковые блоки шифротекста. Данный эффект нежелателен, так как может дать подсказку при анализе содержания сообщения. Необходимо использовать режим шифрования, отличный от режима ECB (electronic code book). В качестве примера, требующего подробного исследования, рассмотрим следующий режим обратной связи: зашифрованный блок сообщения суммируется по модулю 2 с предыдущим блоком, точнее, с его исходной (незашифрованной) формой. В итоге работы такого режима получаем зашифрованное сообщение, в котором каждый блок (кроме первого) зависит от предыдущего и любая ошибка в единичном бите влияет на сообщение в целом. Таким образом, за счет чувствительности даже к единичным ошибкам данный режим предоставляет исходному сообщению имитозащиту от нежелательной информации.

Заключение. Описанная в данной работе основа блочного симметричного шифрования на базе гиперсети является безызбыточной, что позволяет использовать данный метод шифрования в режиме он-лайн. Предлагаемый метод предоставляет возможность создания новых гибких алгоритмов шифрования, которые можно применять в различных системах защиты информации.

Список литературы

1. Feistel H. Cryptography and computer privacy // Sci. Amer. 1973. V. 228, N 5. P. 15–23.

2. Попков В. К. Математические модели связности. Новосибирск: ИВМиМГ СО РАН, 2006.

3. Шеннон К. Теория связи в секретных системах // Работы по теории информации и кибернетике. М.: Иностр. лит., 1963.

Легкий Дмитрий Сергеевич — магистрант Сибирского государственного университета телекоммуникаций и информатики; e-mail: dmitriy1990@ngs.ru;
Попков Владимир Константинович — д-р физ.-мат. наук, проф., гл. науч. сотр. Института вычислительной математики и математической геофизики СО РАН; e-mail: popkov@sscc.ru

Дата поступления — 20.03.13