УДК 681.36

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ КАК ПРОЦЕДУРА КОДИРОВАНИЯ

Ю.Г. САВЧЕНКО, Т.В. ЧИЧ

Рассмотрены задачи криптографического шифрования двоичной информации в терминах алгебраической теории кодов с коррекцией ошибок. Показано единство процедур шифрования и кодирования, на основе чего может быть получен обширный класс новых алгоритмов криптозащиты.

В настоящее время независимо друг от друга существуют и развиваются две специфические ветви преобразования двоичной информации: помехозащищенное кодирование и криптографическое шифрование. Эти ветви базируются на различных подходах: кодирование использует, главным образом, чисто алгебраический подход; шифрование (в зависимости от класса процедур — разные методы — от комбинаторных до таких, как эллиптические функции, арифметику в остаточных классах, вычисления в поле Галуа и др.). В то же время термины «шифрование» и «кодирование» по своей сути являются почти синонимами, что непосредственно следует из классической работы К. Шеннона [1], где рассмотрены основные известные к тому времени шифры, в том числе близкие к предлагаемому ниже подходу матричные системы Л. Хилла. Как при кодировании, так и при шифровании речь идет о процедуре (алгоритме, правиле, формуле) преобразования одной двоичной комбинации $\mathbf{X}$ в другую $\mathbf{Y}$, т.е.

$$\mathbf{Y} = F(\mathbf{X}). \qquad (1)$$

Для описания такой процедуры в стандарте AES (Rijdael) [2], который призван заменить широко распространенный стандарт DES, используется матричный подход. Двоичные последовательности представляются в виде полиномов в поле Галуа (точно так, как и при построении циклических помехозащищенных кодов), а отдельные шаги (раунды) шифрования — матричными операциями. Вхождениями матриц выступают отдельные *байты* информационной последовательности или ключа, что позволяет существенно облегчить программную реализацию соответствующих процедур.

Предлагаемый подход базируется также на матричном описании, но на *битовом* уровне, т.е. в виде двоичных матриц аналогично процедурам кодирования и декодирования групповых кодов, что позволяет сблизить, а в некоторых случаях и совместить помехозащищенное кодирование и криптографическое шифрование.

В общем случае (по крайней мере, при двоичном представлении $\mathbf{X}$ и $\mathbf{Y}$) зависимость (1) должна, очевидно, задаваться соответствующими автоматными уравнениями. Однако, учитывая реально используемые в настоящее время процедуры кодирования и шифрования, можно ограничиться лишь булевыми уравнениями вида

$$y_i = f_i(x_1, x_2, ..., x_k),\ i = 1, ..., n;\ n \geq k\ , \qquad (2)$$

где x_i и y_j — компоненты, соответственно, двоичного вектора $\mathbf{X}$ и $\mathbf{Y}$.

При помехозащищенном кодировании чаще всего все f_i — линейные булевы функции относительно операции сложения по модулю 2, т.е. каждый символ y_i — это некоторая сумма по модулю 2 избранной совокупности входных символов. Для групповых кодов, включая циклические, процедура кодирования математически может быть задана умножением слева исходной комбинации $\mathbf{X}$ в виде вектор-строки $\mathbf{X} = (x_1, x_2, ..., x_k)$ на так называемую порождающую матрицу вида

$$\mathbf{Q} = \mathbf{I}_k \mathbf{A}_{k,n-k}\ ,$$

где $\mathbf{I}_k$ — единичная матрица ранга k; $\mathbf{A}_{k,n-k}$ — матрица размерности $k \times (n-k)$, которая задает $(n-k)$ уравнений кодирования

$$y_{k+j} = \varphi(x_1, x_2, ..., x_k)\ .$$

Важно отметить принципиальную для нашего рассмотрения особенность: при таком выборе матрицы $\mathbf{Q}$ значения первых k разрядов в слове $\mathbf{Y}$ совпадают со значениями соответствующих разрядов в слове $\mathbf{X}$. И это понятно, поскольку решается задача защиты от помех, а поэтому процедура восстановления исходного сообщения $\mathbf{X}$ должна быть максимально простой и быстрой.

Совсем иное дело шифрование. В этом случае основная цель — максимально скрыть не только исходное сообщение $\mathbf{X}$, но и замаскировать статистику появления отдельных символов в совокупности сообщений, поступающих (перехваченных) от конкретного источника. Поэтому, если для шифрования использовать такую же процедуру, как и для кодирования, то требования к порождающей матрице должны быть коренным образом изменены. В частности, в большинстве случаев $n = k$, т.е. $\mathbf{Q}$ — квадратная матрица ранга k. Кроме того, поскольку именно эта матрица определяет конкретный способ преобразования $\mathbf{X}$ в $\mathbf{Y}$, то в случае шифрования она должна однозначно определяться на основе ключа шифрования $\mathbf{K} = (k_1, k_2, ..., k_k)$ и соответствующего фрагмента открытого текста. Отметим, что длина ключа не обязательно должна совпадать с длиной исходного текста. На основе этих простых соображений можно утверждать, что матрица $\mathbf{Q}$ содержит в качестве вхождений либо компоненты ключа $\mathbf{K}$, либо некоторые функции ψ_{ij}, зависящие от ключа и от значений разрядов исходного текста $\mathbf{X}$, т. е.

$$q_{ij} = \psi_{ij}(\mathbf{K}, \mathbf{X})\ .$$

Вопрос выбора функций, с помощью которых определяются вхождения матрицы $\mathbf{Q}$, с одной стороны, достаточно сложный процесс, поскольку кроме всего прочего необходимо обеспечить возможность однозначного вычисления каждого q_{ij} получателем сообщения, т.е. должно существовать преобразование

$$\psi_{ij}(\mathbf{K},\mathbf{X}) \Rightarrow \psi'_{ij}(\mathbf{K},\mathbf{Y}).$$

Однако можно предполагать, что матрица $\mathbf{Q}$ получена любым доступным способом, включая случайный выбор, при выполнении некоторых простых ограничений, и заранее известна как отправителю, так и получателю.

В наиболее простом случае $\mathbf{Q}$ должна однозначно определяться только на основе известного ключа $\mathbf{K}$, например, некоторой перестановкой его компонент либо функциями от их двоичных значений.

Рассмотрим элементарные квадратные матрицы с двоичными элементами и их очевидные свойства.

1. Нулевая квадратная матрица $\mathbf{Y}$ ранга m. Очевидно, что умножение на такую матрицу дает в результате нулевой вектор-столбец.

2. Единичная диагональная матрица $\mathbf{I}$. Умножение $\mathbf{X}$ слева на $\mathbf{I}$ не изменяет $\mathbf{X}$, т.е. $\mathbf{X} \times \mathbf{I} = \mathbf{X}$.

3. Единичная правая диагональная матрица $\mathbf{J}$. Умножение $\mathbf{X}$ слева на $\mathbf{J}$ изменяет порядок (нумерацию) разрядов в $\mathbf{X}$ на обратный.

4. Умножение на матрицу

$$\mathbf{A} = \begin{Vmatrix} 0 & 1 & 0 & 0 & \ldots & 0 & 0 \\ 1 & 0 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 0 & 1 & \ldots & 0 & 0 \\ 0 & 0 & 1 & 0 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & 0 & \ldots & 0 & 1 \\ 0 & 0 & 0 & 0 & \ldots & 1 & 0 \end{Vmatrix}$$

меняет местами четные и нечетные разряды в $\mathbf{X}$.

5. Матрица

$$\mathbf{B} = \begin{Vmatrix} 0 & 0 & \ldots & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & \ldots & 0 & 0 & 1 & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{Vmatrix}$$

соответствует «зеркальной» перестановке позиций слова $\mathbf{X}$: левая половина становится правой и наоборот.

Перечень примеров аналогичных элементарных матриц можно продолжать достаточно долго. Легко показать, что любая двоичная матрица, содержащая точно по одной единице в каждом столбце, при умножении на нее осуществляет некоторую перестановку разрядов $\mathbf{X}$, а произведение произвольного подмножества таких матриц даст в результате также элемен-

тарную матрицу, содержащую в каждом столбце не более одной единицы. Поэтому такие матрицы для шифрования представляют ограниченный интерес и могут быть использованы, в основном, для маскирования статистики («забеливания» и так называемого гаммирования).

Матрицы же, столбцы которых содержат больше одной единицы, представляют большой интерес для построения процедур шифрования. Рассмотрим некоторые общие свойства таких матриц, которые могут быть полезными для шифрования.

Возникает естественный вопрос: любая ли двоичная матрица ранга k пригодна для построения процедуры шифрования? Чтобы ответить на него, целесообразно рассмотреть процедуру дешифрования принятого сообщения в предположении, что получателю известна матрица $\mathbf{Q}$.

Каждому столбцу такой матрицы можно поставить в соответствие уравнение вида (2). В случае использования алгоритма, аналогичного процедуре кодирования для групповых кодов, эти уравнения имеют вид

$$y_i = \oplus\sum_{\alpha} x_\alpha, \ \alpha \in U_i, \ i = \overline{1,k}, \tag{3}$$

где U_i — совокупность номеров позиций i-го столбца матрицы, значения которых равны 1.

Очевидно, система уравнений (3) разрешима относительно x_α, $\alpha = \overline{1,k}$ тогда и только тогда, когда эти уравнения линейно независимы относительно операции поразрядного сложения по модулю 2. Отсюда непосредственно следует, что и строки матрицы $\mathbf{Q}$ должны быть линейно независимыми. Иными словами, все строки матрицы $\mathbf{Q}$ должны быть различными, и ни одна из них не может быть представлена в виде суммы любой совокупности остальных строк. Очевидно также, что выполнить это требование не очень сложно, используя известные из теории кодирования приемы. По крайней мере, можно обоснованно предполагать, что комбинаторного разнообразия матриц достаточно, чтобы обеспечить криптографическую стойкость полученных таким способом шифров. В пользу такого предположения можно привести матричное представление одного из широко применяемых алгоритмов, например, DES [3]. В этом случае шифрующую матрицу представим следующим образом:

$$\mathbf{Q} = \begin{Vmatrix} \mathbf{Y} & \mathbf{Y} & \mathbf{Y} & \mathbf{W} & \mathbf{Y} & \mathbf{Y} & \mathbf{Y} & \mathbf{Y} \\ \mathbf{Y} & \mathbf{Y} & \mathbf{Y} & \mathbf{Y} & \mathbf{Y} & \mathbf{Y} & \mathbf{Y} & \mathbf{W} \\ \mathbf{Y} & \mathbf{Y} & \mathbf{W} & \mathbf{Y} & \mathbf{Y} & \mathbf{Y} & \mathbf{Y} & \mathbf{Y} \\ \mathbf{Y} & \mathbf{Y} & \mathbf{Y} & \mathbf{Y} & \mathbf{Y} & \mathbf{Y} & \mathbf{W} & \mathbf{Y} \\ \mathbf{Y} & \mathbf{W} & \mathbf{Y} & \mathbf{Y} & \mathbf{Y} & \mathbf{Y} & \mathbf{Y} & \mathbf{Y} \\ \mathbf{Y} & \mathbf{Y} & \mathbf{Y} & \mathbf{Y} & \mathbf{Y} & \mathbf{W} & \mathbf{Y} & \mathbf{Y} \\ \mathbf{W} & \mathbf{Y} & \mathbf{Y} & \mathbf{Y} & \mathbf{Y} & \mathbf{Y} & \mathbf{Y} & \mathbf{Y} \\ \mathbf{Y} & \mathbf{Y} & \mathbf{Y} & \mathbf{Y} & \mathbf{W} & \mathbf{Y} & \mathbf{Y} & \mathbf{Y} \end{Vmatrix}, \tag{4}$$

где $\mathbf{Y}$ — нулевые матрицы ранга 8, а

$$\mathbf{W} = \begin{Vmatrix} 0 & 0 & 0 & \psi_{ij} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \psi_{ij} \\ 0 & 0 & \psi_{ij} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \psi_{ij} & 0 \\ 0 & \psi_{ij} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \psi_{ij} & 0 & 0 \\ \psi_{ij} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \psi_{ij} & 0 & 0 & 0 \end{Vmatrix}, \qquad (5)$$

где, в свою очередь, вхождения ψ_{ij} определяются как значения булевых функций (0 или 1), которые зависят от соответствующих битов ключа $\mathbf{K}$ и входного слова $\mathbf{X}$. В частности,

$$\psi_{ij}(\mathbf{K}, \mathbf{X}) = L_i \oplus f(\mathbf{R}_i, \mathbf{K}_{i+1}),$$

где $\mathbf{L}_i \cup \mathbf{R}_i = \mathbf{X}$; $f(\mathbf{R}_i, \mathbf{K}_{i+1}) = \mathbf{R}'_i \oplus \mathbf{K}_i$. Здесь знак $\cup$ соответствует простому соединению (объединению) двух 32-разрядных комбинаций (левой и правой половин) в одну 64-разрядную, а $\mathbf{R}'$ — расширение 32-розрядного вектора $\mathbf{R}_i$ до 48 разрядов путем добавления нулей. В окончательном (рабочем) виде запись (5) — это двоичная матрица, разная для различных шифруемых блоков. Однако ее структура остается неизменной и всегда соответствует виду (4), (5).

В заключение приведенного краткого изложения рискнем утверждать, что преобразование двоичных последовательностей с помощью матричных операций образует широкий класс легко реализуемых процедур шифрования. Соответствующие аппаратные и программные решения давно используются при помехозащищенном кодировании и могут быть применены и для криптографической защиты в телекоммуникационных системах. Важно также, что в этом случае легко совместить шифрование с помехозащищенным кодированием не только для циклических [4, 5], но и в целом для групповых кодов.

ЛИТЕРАТУРА

1. *Шеннон К.* Теория связи в секретных системах // В сб.: Работы по теории информации и кибернетике. — М.: Изд. иностр. лит., 1963. — С. 333–413.
2. *Зендин О.С., Иванов М.А.* Стандарт криптографической защиты AES. — Кн. 1. — М.: Кудиц-Образ, 2002.— 274 с.
3. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке С. — М.: Триумф, 2002. — 816 с.
4. *Горовой И.М., Савченко Ю.Г.* Коды с коррекцией ошибок как средство криптозащиты // УСиМ. — 2002. — №5. — С. 74–79.
5. *Савченко Ю.Г., Горовой И.М.* Централизованное управление связью как средство криптозащиты // Связь. — 2004. — № 7. — С. 32–34.

Поступила 16.03.2006