УДК 519.6

О БЛОЧНЫХ ШИФРАХ, ПОСТРОЕННЫХ НА ОСНОВЕ РЕГИСТРОВ СДВИГА С ДВУМЯ ОБРАТНЫМИ СВЯЗЯМИ

А. М. Коренева

Получены условия биективности и инволютивности алгоритма блочного шифрования, построенного на основе регистра сдвига с двумя обратными связями над пространством двоичных векторов. Построен пример алгоритма блочного шифрования с указанными свойствами на основе регистра сдвига длины 4.

Ключевые слова: *биективность, итеративные симметричные блочные шифры, инволютивность алгоритма шифрования, регистры сдвига.*

При построении и анализе блочных шифров Фейстеля и более общих моделей регистрового типа необходимо ответить на ряд актуальных вопросов. К таким вопросам относятся определение инволютивности алгоритма шифрования (инволютивность важна для удобства технической и программной реализации), перемешивающих свойств алгоритма (важных с точки зрения противодействия методам последовательного опробования элементов ключа и дифференциального криптоанализа) и др. При усложнении модели алгоритма блочного шифрования необходимо сохранить биективность шифрующих преобразований. В продолжение исследований алгоритмов блочного шифрования, обобщающих шифры Фейстеля [1], в работе рассмотрены алгоритмы, построенные на основе регистров сдвига с двумя обратными связями над пространством двоичных векторов. Такие алгоритмы представляют интерес в связи с тем, что имеют более сильные перемешивающие свойства по сравнению с регистрами с одной обратной связью [2]. Получены условия биективности преобразования регистра сдвига с двумя обратными связями и условия инволютивности соответствующего алгоритма блочного шифрования. На примере алгоритма блочного шифрования на базе регистра сдвига длины 4 показана практическая возможность обеспечения ряда положительных криптографических свойств блочного шифра.

Рассмотрим функции $\varphi_i(x_1,\ldots,x_n) : X^n \to X$, $i = 1, 2$, X — конечное множество. Система функций $\varphi = \{\varphi_1(x_1,\ldots,x_n), \varphi_2(x_1,\ldots,x_n)\}$ биективна по множеству переменных $\{x_i, x_j\}$, если φ реализует биективное преобразование множества X^2 при любой фиксации переменных $\{x_1,\ldots,x_n\}\backslash\{x_i, x_j\}$. Далее X — векторное пространство.

Утверждение 1. Если $\varphi_1 = x_i + f_1(x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n)$, $\varphi_2 = x_j + f_2(x_1,\ldots, x_{i-1},x_{i+1},\ldots,x_{j-1},x_{j+1},\ldots,x_n)$, то система φ биективна по множеству переменных $\{x_i, x_j\}$.

Автономным регистром сдвига длины n над X с обратными связями $\varphi_m(x_1,\ldots,x_n)$ и $\varphi_n(x_1,\ldots,x_n)$ назовём преобразование g_φ множества X^n, задаваемое системой координатных функций $\{\varphi_1(x_1,\ldots,x_n),\ldots,\varphi_n(x_1,\ldots,x_n)\}$, где $\varphi_i(x_1,\ldots,x_n) = x_{i+1}$ для всех $i \in \{1,\ldots,n-1\}\backslash\{m\}$, $\varphi = \{\varphi_m(x_1,\ldots,x_n), \varphi_n(x_1,\ldots,x_n)\}$. Здесь m — параметр регистрового преобразования, $1 \leqslant m \leqslant n-1$.

Теорема 1. Преобразование регистра сдвига g_φ биективно, если и только если система φ биективна по множеству переменных $\{x_1, x_{m+1}\}$.

В соответствии с утверждением 1 преобразование g_φ биективно, если при $m < n-1$ имеет место $\varphi_m = x_{m+1} + f_m(x_2,\ldots,x_m,x_{m+2},\ldots,x_n)$, $\varphi_n = x_1 + f_n(x_2,\ldots,x_n)$ или при $m = n-1$ выполняется $\varphi_m = x_n + f_m(x_2,\ldots,x_{n-1})$, $\varphi_n = x_1 + f_n(x_2,\ldots,x_n)$.

Пусть $X = V_r$ — множество двоичных r-мерных векторов. Рассмотрим блочный шифр $C(g_{\varphi,q})$ с раундовой подстановкой $g_{\varphi,q}$ множества X^n, задаваемой системой координатных функций $\{\varphi_1(x_1,\ldots,x_n,q),\ldots,\varphi_n(x_1,\ldots,x_n,q)\}$, где $\varphi_i(x_1,\ldots,x_n) = x_{i+1}$ для всех $i \in \{1,\ldots,n-1\}\backslash\{m\}$, $1 \leqslant m < n-1$; q — бинарный раундовый ключ; координатные функции φ_m и φ_n имеют вид $\varphi_m = x_{m+1} \oplus f_m(x_2,\ldots,x_m,x_{m+2},\ldots,x_n,q)$, $\varphi_n = x_1 \oplus f_n(x_2,\ldots,x_n,q)$.

Определим условия инволютивности рассматриваемого шифра — условия, при которых расшифрование отличается от зашифрования только порядком использования раундовых ключей. Обозначим через I_n инволюцию степени n вида $I_n(x_1,\ldots,x_n) = (x_n,\ldots,x_1)$. Функцию f_n назовем инвариантной относительно инволюции I_{n-1}, если $f_n(x_2,\ldots,x_n,q) = f_n(x_n,\ldots,x_2,q)$. Функцию f_m назовем инвариантной относительно инволюции I_{n-2}, если $f_m(x_2,\ldots,x_m,x_{m+2},\ldots,x_n,q) = f_m(x_n,\ldots,x_{m+2},x_m,\ldots,x_2,q)$.

Лемма 1. Если функция f_n инвариантна относительно инволюции I_{n-1}, а функция f_m инвариантна относительно инволюции I_{n-2}, то для раундовой подстановки выполнено равенство $(g_{\varphi,q})^{-1} = I_n g_{\varphi,q} I_n$.

Теорема 2. Пусть h-раундовый блочный шифр $C(g_{\varphi,q})$ при шифровании реализует произведение раундовых подстановок $g_{\varphi,q_1},\ldots,g_{\varphi,q_h}$ и инволюции I_n. Тогда если функция f_n инвариантна относительно инволюции I_{n-1} и функция f_m инвариантна относительно инволюции I_{n-2}, то алгоритм шифрования инволютивен и расшифрование отличается от зашифрования использованием раундовых ключей в обратном порядке.

Пример (инволютивный алгоритм блочного шифрования на основе регистра сдвига с двумя обратными связями). Пусть $n = 4$, $m = 2$, $r = 16$. Рассмотрим алгоритм, который реализует произведение h раундовых подстановок (с раундовыми ключами $q_1,\ldots,q_h$) и инволюции I_4. Функция усложнения раундовой подстановки представлена парой функций $f_4(x_2,x_3,x_4,q)$ и $f_2(x_2,x_4,q)$. Раундовая подстановка $g_{\varphi,q}$ при использовании ключа q имеет вид $g_{\varphi,q} = (x_2, x_3 \oplus f_2(x_2,x_4,q), x_4, x_1 \oplus f_4(x_2,x_3,x_4,q))$.

Из теоремы 2 следует, что для обеспечения инволютивности рассматриваемого алгоритма шифрования функции $f_4(x_2,x_3,x_4,q)$ и $f_2(x_2,x_4,q)$ должны быть инвариантны относительно инволюций I_3 и I_2 соответственно, иначе говоря, инвариантны относительно перестановки переменных x_2 и x_4. Рассмотрим варианты построения функций $f_4(x_2,x_3,x_4,q)$ и $f_2(x_2,x_4,q)$.

Используемый 32-битовый раундовый ключ q разобъём на два 16-битовых подключа: $q = (q_1,q_2)$. Тогда указанным требованиям удовлетворяют, в частности, функции вида $f_4(x_2,x_3,x_4,q) = (y_2 \vee y_4) \oplus S_4(y_3)$, $f_2(x_2,x_4,q) = S_2(x_2 \oplus x_4) \oplus q_2$, где $(y_2,y_3,y_4) = (x_2 \oplus q_1, x_3 \oplus q_2, x_4 \oplus q_1)$, $\vee$ — покоординатная дизъюнкция 16-битовых векторов, S_2, S_4 — нелинейные преобразования множества V_{16} (например, четвёрки s-боксов $V_4 \to V_4$). Применяя h раундов шифрования открытого текста $(x_1(0),x_2(0),x_3(0),x_4(0))$ и инволюцию I_4, получаем шифрованный текст в режиме ECB, равный $(x_4(h),x_3(h),x_2(h),x_1(h))$. В соответствии с теоремой 2 данный алгоритм шифрования инволютивен, расшифрование отличается от зашифрования использованием раундовых ключей в обратном порядке. Другие положительные криптографические свойства шифра могут быть обеспечены с помощью выбора числа циклов шифрования h, преобразований S_2, S_4, ключевого расписания и др.

ЛИТЕРАТУРА

1. *Коренева А. М., Фомичев В. М.* Об одном обобщении блочных шифров Фейстеля // Прикладная дискретная математика. 2012. № 3. С. 34–40.

2. *Коренева А. М., Фомичев В. М.* Криптографические свойства блочных шифров, построенных на основе регистров сдвига // Прикладная дискретная математика. Приложение. 2012. № 5. С. 49–51.

УДК 519.151, 519.725, 519.165

КОНСТРУКЦИИ ИДЕАЛЬНЫХ СХЕМ РАЗДЕЛЕНИЯ СЕКРЕТА

Н. В. Медведев, С. С. Титов

Работа посвящена исследованию вопросов разграничения доступа к информации при помощи линейных идеальных однородных схем разделения секрета. Приведена конструкция таких схем над любым полем $\mathrm{GF}(q)$. Путём добавления участников показано, что такие схемы сводятся к схемам на проективных пространствах.

Ключевые слова: *однородные схемы разделения секрета, структуры доступа, матроиды, код Рида — Маллера, идеальные схемы.*

Неотъемлемыми атрибутами современных компьютерных систем и сетей передачи данных являются криптографические протоколы защиты информации. На этом пути часто возникают сложные проблемы, требующие привлечения серьёзного математического аппарата. Одна из таких актуальных и активно исследуемых западными специалистами областей — разграничение доступа [1] при помощи протоколов (схем) разделения секрета (СРС) [2, 3].

Механизм работы СРС заключается в предоставлении участникам долей секрета таким образом, чтобы заранее заданные коалиции участников (разрешённые коалиции) могли однозначно восстановить секрет [4]. Особый интерес вызывают однородные СРС [5 – 7], которые допускают идеальную реализацию. При этом ограничиваются рассмотрением разделяющих СРС, т. е. таких, где нет незаменимых участников [6].

Разрешённые коалиции идеальной совершенной схемы разделения секрета определяются циклами некоторого связного матроида, изучение которого и даёт структуру доступа [8]. В терминах циклов аксиом всего две. Представляется естественным рассмотреть двойственный вариант аксиоматизации матроида, а именно использовать не циклы C матроида M, а его нуль-множества Z, т. е. $Z = M \setminus C$, которые можно назвать «антициклами». Тогда аксиомы матроида в терминах антициклов имеют следующий вид: 1) нет антицикла в антицикле, т. е. если Z_1, Z_2 — антициклы и $Z_1 \subset Z_2$, то $Z_1 = Z_2$; 2) если $e \in M$, $e \notin Z_1 \cup Z_2$ и Z_1, Z_2 — антициклы, причём $Z_1 \neq Z_2$, то существует такой антицикл Z, что $(\{e\} \cup (Z_1 \cap Z_2)) \subset Z$.

Перейдём к рассмотрению матроидов в проективном m-мерном пространстве M над $\mathrm{GF}(q)$. Возьмём в качестве нуль-множеств Z гиперпространства в M. Как известно [9], $|M| = (q^{m+1} - 1)/(q - 1)$ и $|Z| = (q^m - 1)/(q - 1)$. Поскольку любые два гиперпространства Z_i и Z_j всегда пересекаются, т. е. $(Z_i \cap Z_j) \neq \varnothing$, причём $\dim Z = m - 1$, $\dim(Z_i \cap Z_j) = m - 2$, то для любой точки $e \notin (Z_i \cap Z_j)$ существует единственное гиперпространство Z, натянутое на $\{e\}$ и на пересечение гиперпространств Z_i и Z_j, так что $Z = \langle \{e\}, Z_i \cap Z_j \rangle$. А это — не что иное, как вторая аксиома матроида в терминах антициклов, которую можно назвать усиленной, так как существует единственное такое гиперпространство. Следовательно, вторая аксиома матроида выполняется. Первая аксиома матроида с очевидностью выполняется, так как размерности гиперпространств одинаковы и антицикла в антицикле быть не может.