Технические науки

УДК 004.04

Коряков Игорь Витальевич

Начальник отдела разработки и производства технических средств

ООО Научно-внедренческая фирма «Криптон»

ШИФРЫ КАК ФИЛЬТРЫ

Аннотация. *Если представить шифры структурно в виде фильтров, в которых регистры с задержанными отсчётами будут хранить состояние шифра, а умножение на коэффициенты будет заменено некоторыми функциональными преобразованиями, то окажется, что шифр SPN эквивалентен БИХ фильтру первого порядка, а шифр на основе сети Фейстеля – БИХ фильтру второго порядка с коэффициентом $a_2 = 1$. Причём вместо отсчётов входного сигнала на фильтр будет поступать последовательность подключей.*

Обратимость канонической структуры фильтров (КСФ) позволяет построить класс шифров, в которых шифратор и дешифратор отличаются переменой мест функций БИХ и КИХ ветвей. Такие шифры обладают рядом интересных свойств, описываемых ниже.

Ключевые слова: *цифровой фильтр, каноническая структура фильтра, криптография, блочный шифр, потоковый шифр.*

Цифровые фильтры

Передаточная функция цифрового фильтра имеет вид [1, с.141]:

$$H(z) = \frac{B(z)}{A(z)} = \frac{\sum_{m=0}^{M} b_m z^{-m}}{1 - \sum_{n=1}^{N} a_n z^{-n}}, \quad (1)$$

где z^{-t} – задержка сигнала на t отсчётов, b_m – коэффициенты нерекурсивной секции фильтра (фильтр с конечной импульсной характеристикой

КИХ), a_n – коэффициенты рекурсивной секции (фильтр с бесконечной импульсной характеристикой БИХ).

Разностное уравнение фильтра может быть представлено в форме:

$$y(k) = x(k) - \sum_{n=1}^{N} a_n D_n(k-1) + \sum_{n=1}^{N} b_n D_n(k-1),$$

где y_k – выходной отсчёт фильтра, x_k – входной отсчёт фильтра, D_n () – значение на n-том выходе линии задержки, определяемой как

$$D_n(k) = D_{n-1}(k-1) | n = N,...,2$$

и

$$D_1(k) = x(k) - \sum_{n=1}^{N} a_n D_n(k-1).$$

Каноническая структура фильтра (КСФ), соответствующая этому уравнению, может быть представлена в форме, приведённой на рисунке 1.

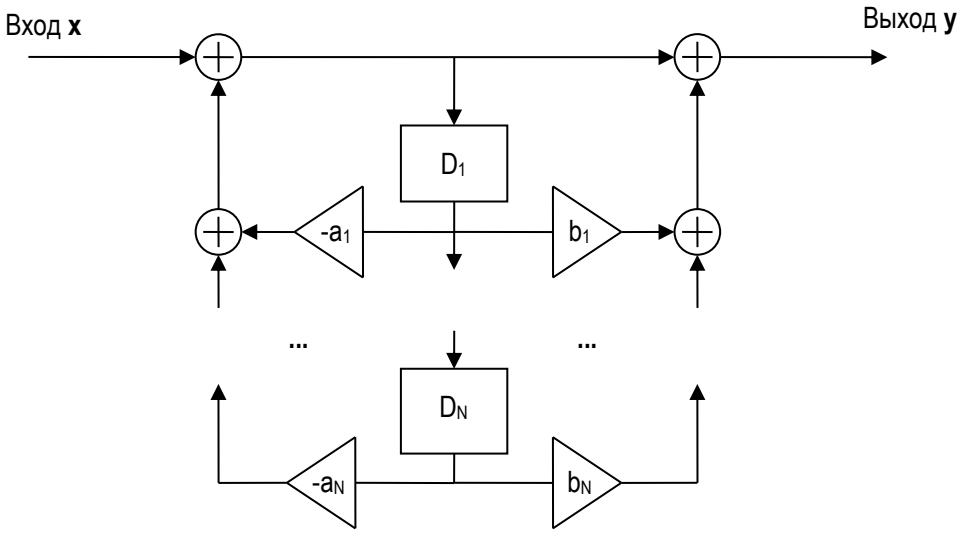

Рис. 1. Каноническая структура цифрового фильтра

Сходство структур

Существует множество разнообразных объектов с одинаковыми структурными признаками, аналоги деления или умножения на некий полином. Например, аналоги деления на полином:

– интегратор,

– фильтр с бесконечной импульсной характеристикой (БИХ).

– самосинхронизирующийся скремблер,

– шифратор в режиме гаммирования с обратной связью (Cipher Feedback, CFB),

Объекты – аналоги умножения на полином:

– дешифратор в режиме CFB,

– самосинхронизирующийся дескремблер,

– дифференциатор,

– фильтр с конечной импульсной характеристикой (КИХ).

Децимирующий CIC фильтр (cascaded integral-comb, каскадный интегрально-гребенчатый фильтр) – сначала деление, затем умножение на полином.

Интерполирующий CIC фильтр – сначала умножение, затем деление на полином.

Переход к структуре цифрового фильтра

Традиционно принято изображать структуры блочных шифров в виде последовательности операций. Например, раунд шифра AES отображается в виде 4-х последовательных операций, изображённых на рисунке 2 в виде прямоугольников со стрелками:

1. Текущее состояние шифра S_i является входом преобразования и подвергается табличной подстановке: SubBytes(state);
2. Перестановка: ShiftRows(state);
3. Перестановка: MixColumns(state);
4. Сложение с подключём: AddRoundKey(state) образует следующее состояние шифра S_{i+1}.

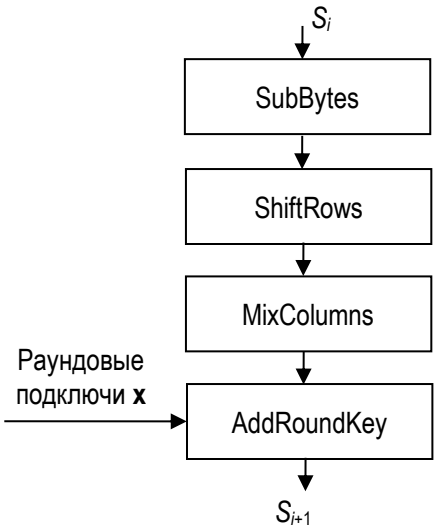

Рис. 2. Структура раунда шифра AES

А теперь посмотрим, что собой представляет шифр AES с точки зрения цифрового фильтра. Он содержит некий регистр состояния (128 бит), некое преобразование подстановки-перестановки F и сложение с подключом k_r.

Итеративный блочный шифр типа SPN (substitution-permutation network), к которому относится стандарт AES, можно представить структурой БИХ фильтра с делением на полином. На рисунке 3 представлена структура БИХ фильтра первого порядка с передаточной функцией

$$H(z) = \frac{1}{A(z)} = \frac{1}{1 - a_1 z^{-1}}. \qquad (2)$$

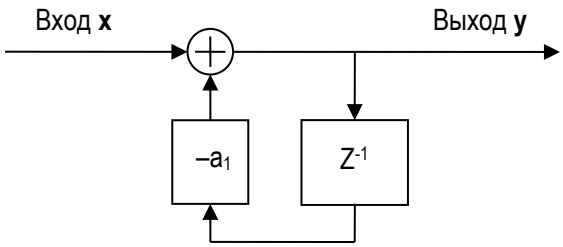

Рис. 3. Структура БИХ фильтра 1-го порядка

Здесь Z^{-1} – элемент задержки на один отсчёт (обычно параллельный регистр), $-a_1$ – умножитель на коэффициент a_1, + – сумматор. На вход фильтра поступают отсчёты сигнала x, на выходе фильтра формируются отсчёты y.

Теперь рассмотрим в общем виде структуру шифра SPN, представленную на рисунке 4.

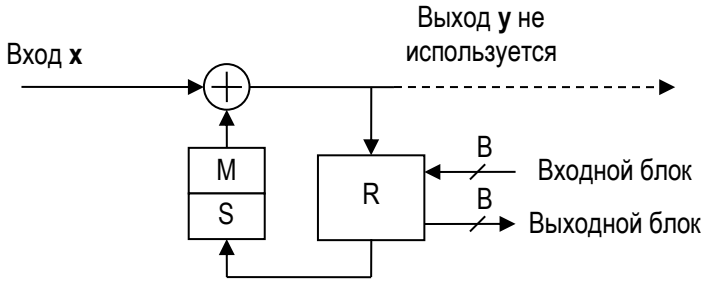

Рис. 4. Структура SPN шифратора

Здесь R– параллельный регистр, хранящий текущее состояние шифра B бит, S и M – раундовая функция (подстановка и перестановка, соответственно), + – сумматор. Если проводить аналогию с БИХ фильтром, то вместо умножителя стоит функциональный преобразователь, на вход фильтра поступают подключи x, начальное состояние – это входной блок, конечное состояние после некоторого числа тактов – результирующий блок, а выход фильтра y не используется.

На рисунке 5 представлен БИХ фильтр второго порядка с передаточной функцией

$$H(z) = \frac{1}{A(z)} = \frac{1}{1 - a_1 z^{-1} - a_2 z^{-2}}. \qquad (3)$$

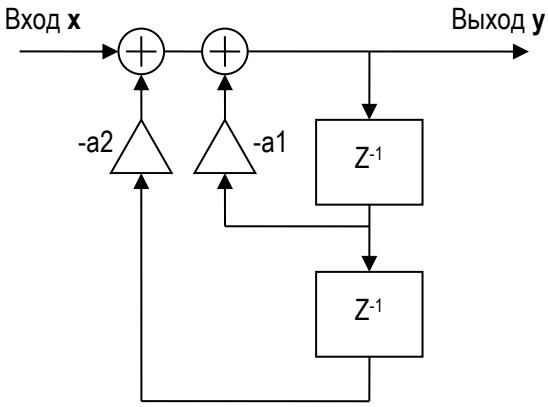

Рис. 5. Структура БИХ фильтра 2-го порядка

Здесь изображён фильтр 2-го порядка с двумя элементами задержки Z^{-1} и двумя постоянными коэффициентами – a_1 и – a_2.

Это фактически схема Фейстеля, реализованная в ГОСТ 28147 (см. рисунок 6), у которой коэффициент – $a_2 = 1$, а – a_1 представлен последовательными преобразованиями S (узлы замены) и M (циклический сдвиг).

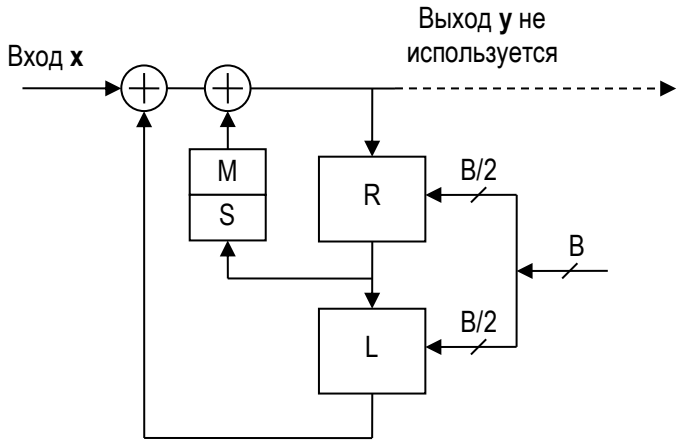

Рис. 6. Сеть Фейстеля как фильтр 2-го порядка

При этом входом является не сигнал x, а состояние элементов задержки R и L как правой и левой частей шириной B/2 входного блока шириной B, а x является последовательностью подключей. Выход фильтра y не используется. Выходом преобразования является состояние элементов

задержки после фильтрации r отсчётов (число раундов) входного вектора x. На примере ГОСТ 28147 вход B составляет 64 разряда, регистры R и L – 32-х разрядные, S – это восемь 4-х разрядных таблиц, M – циклический сдвиг. Подключи – это 32 целых 32-х разрядных отсчёта. Сложение с подключами делается в несколько другой точке (не после задержки в регистре R, а до неё), место этой точки не влияет на свойства шифра.

Рассмотрим ещё один БИХ фильтр с двумя единичными коэффициентами a_i =1 и a_j =1 и остальными коэффициентами, равными нулю.

Такой фильтр будет иметь один полюс, расположенный на единичной окружности в z-плоскости и будет неустойчивым, то есть его импульсная характеристика не будет убывать. Реализация фильтра в виде линии задержки, на вход которой поступает сумма отводов i и j и будет представлять собой генератор при ненулевом начальном состоянии ЛЗ. Достаточно быстро такой генератор (при обычной целочисленной арифметике без насыщения) выйдет из линейного режима и будет переполняться по модулю разрядности арифметики. Если i = 24 и j =55, то получится один из вариантов задержанного генератора Фибоначчи, широко применяемого в криптографии.

Обратимость канонической структуры

Для фильтра, определяемого в соответствии с формулой (1), при условии $N = M$ и $b_0 = 1$, возможен обратный фильтр с заменой местами числителя и знаменателя:

$$H^{-1}(z) = \frac{A(z)}{B(z)} = \frac{\sum_{n=1}^{N} a_n z^{-n}}{1 - \sum_{m=1}^{M} b_m z^{-m}}. \qquad (4)$$

Обратный фильтр по выходной последовательности y прямого фильтра точно восстанавливает его входную последовательность x.

Свойство обратимости КСФ (восстановления входного сигнала по выходному) при перестановке коэффициентов a_n и b_n сохраняется, даже

если сложение заменить любой коммутативной операцией, а умножение – любым функциональным преобразованием, в том числе – необратимым.

На основе КСФ возможно построение шифра, в котором схемы зашифрования и расшифрования будут отличаться переменой мест преобразований a_n и b_n.

Если мы зафиксируем размер внутреннего состояния шифра (например, 128 бит), то могут быть масштабируемыми порядок фильтра N и ширина шифра B (разрядность регистров линии задержки). Вплоть до $N = 1$ и $B = 128$ и до $N = 128$ и $B = 1$. Например, если мы задаём элемент, подвергающийся шифрованию, как байт, то получим шифр с $N = 16$ и $B = 8$.

При этом, в определённом смысле, N является аналогом числа раундов блочного шифра, а преобразования a_n и b_n – аналогом раундовых функций.

И если для $B = 1$ функции задаются простейшими подстановками: значение входа, инверсное значение входа, константа «0» и константа «1» (это приводит к классическим потоковым шифрам с одноразрядными регистрами), то для $B = 8$ наиболее разумными представляются фиксированные случайные перестановки 8 х 8, заданные таблично, а для $B = 128$ – вопрос требует особого изучения.

Рассмотрим конкретный вариант КСФ шифра с $N = 1$ и $B = 128$, схема зашифрования и расшифрования которого приведены на рисунке 7.

Здесь D_1 – элемент задержки в виде 128-ми разрядного параллельного регистра, a_1 и b_1 – функциональные преобразования, приближённые к фиксированным случайным подстановкам 128 х 128. Операции сложения представлены 128-разрядными сумматорами по модулю 2.

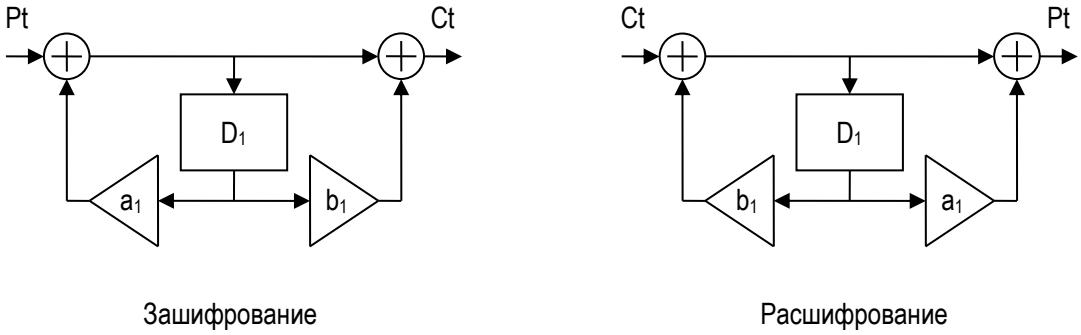

Рис. 7. Схема КСФ шифра с $N = 1$ и $B = 128$

Зависимость преобразований от ключа может быть введена либо в начальное состояние (как в потоковых шифрах), либо в функциональные преобразования, например, как представлено на рисунке 8.

При этом ключ K длиной 256 бит разделяется на две половины K_1 и K_2, которые складываются по модулю 2 с входами и выходами функциональных преобразователей a_1 и b_1 в соответствии с шифром Ивен-Мансура [2] с доказуемой стойкостью.

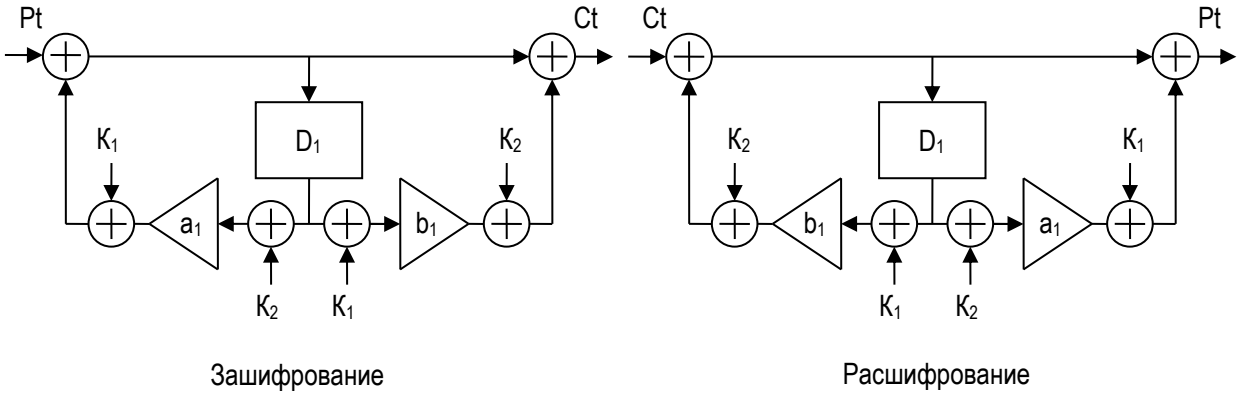

Рис. 8. Пример схемы ввода подключей в функциональные преобразования

Функциональные преобразователи a_1 и b_1 могут быть реализованы в виде «широких» S-блоков, содержащих, например, по 16 таблиц фиксированных случайных подстановок S_0 – S_{15} размером 8 x 128, конкатенация 16-ти входов которых образует 128-ми разрядный вход преобразования, а сумма по модулю 2 всех 16-ти 128-ми разрядных выходов таблиц образует

выход преобразования. Структура таких функциональных преобразователей приведена на рисунке 9.

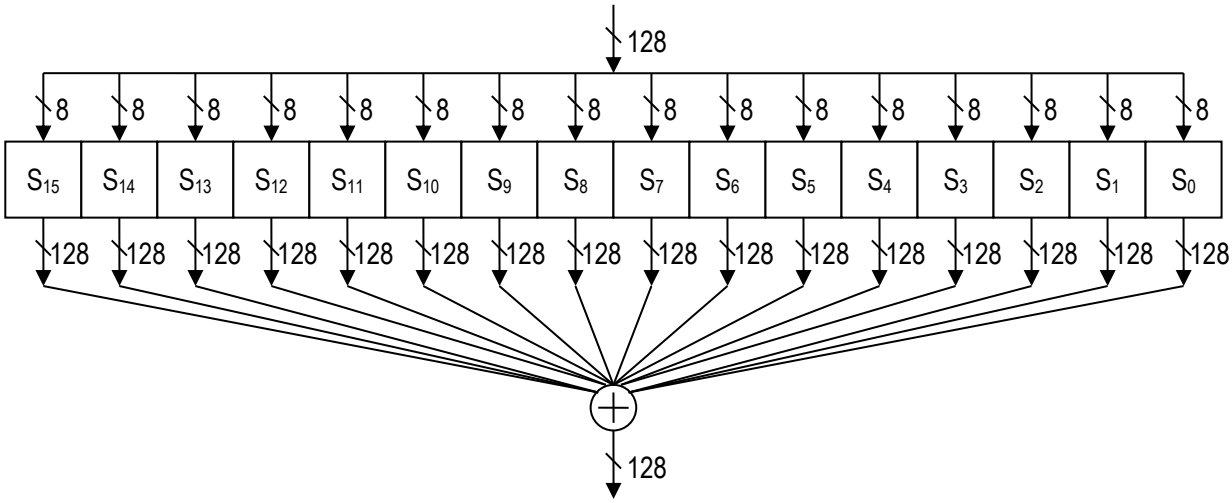

Рис. 9. Схема «широкого» S-блока

Какой-либо отбор S-блоков скорее всего не потребуется, поскольку комбинаторная мощность такого блока очень велика (2 в степени порядка 500000) и вероятность получения случайным образом «плохого» блока исчезающе мала. Такие S-блоки при шифровании $N*B$ бит применяются однократно, в то время как в SPN шифрах один S-блок применяется повторно сотни раз при шифровании одного блока данных, что требует очень строгого подхода к его формированию. Конечно, объём памяти для реализации «широких» S-блоков довольно значителен – 128К байт для конкретного примера, но в настоящее время такой объём является вполне доступным ресурсом.

Предполагаемым преимуществом класса шифров КСФ будет являться монотонная масштабируемость по N и B, что помимо адаптации шифра к конкретным задачам позволит исследовать уменьшенные версии шифров. Кроме того, аппаратная реализация шифра позволяет сократить время шифрования одного блока до одного такта.

Литература

1. Оппенгейм А. В., Шафер Р. В. Цифровая обработка сигналов. М.: Связь, 1979. 416 с.
2. Even S., Mansour Y. A Construction of a Cipher From a Single Pseudorandom Permutation. In: Imai, H., Rivest, R.L., Matsumoto, T. (eds.): ASIACRYPT 1991. LNCS, vol. 739. Springer, Heidelberg. 1993. P. 210–224.