# О СИММЕТРИЧНЫХ ШИФРАХ НА ОСНОВЕ УПРАВЛЯЕМЫХ ОПЕРАЦИЙ

**Винокуров Д.В.**
**Оренбургский государственный университет, г. Оренбург**

Современные симметричные программно-ориентированные и аппаратно-ориентированные шифры используют алгоритмы преобразования данных с предвычислениями, которые вносят существенные ограничения по быстродействию и зачастую требуют значительных вычислительных затрат. В связи с этим в настоящее время существуют различные алгоритмы, в которых реализуются управляемые операции. Данная проблема нашла отражение в работах Молдовяна А. А., Молдовян Н.А., Гуц Н.Д., Нгуен Минь, Шниперова А.Н. и других.

Под управляемой операцией понимается множество некоторых более простых операций, выбираемых в зависимости от значения некоторого управляющего кода. Например, управляющая подстановочная операция (УПО) представляет собой две простые алгебраические операции над двоичными векторами: побитовое сложение по модулю *2* и сложение по модулю $2^n$ [1].

Различают средства аппаратной и программной реализации рассматриваемых шифров. Целью данной работы является поиск и рассмотрение основных скоростных шифров, созданных на основе управляемых операций и зарегистрированных на территории РФ.

SPECTR-H64 является блочным шифром и обрабатывает информацию с 32-разрядной шиной обмена данных [2].

Схема блочного шифрования имеет следующий вид:

$$Y = F\left(X, Q^{(e)}\right), \tag{1}$$

где $Q^{(e)} = H(K, e)$ является расширенным ключом – функцией от 256-битного секретного ключа $K$ и режима шифрования $e$, который принимает значение *0* и *1* (шифрование и расшифровка соответственно). Шифрование проходит в *12* раундов. $X$ является исходным блоком двоичных данных (открытым текстом) в режиме шифрования, а в режиме расшифровки – преобразованным блоком двоичных данных (шифртекстом). В режиме шифрования результирующее значение $Y$ является шифртекстом, а в режиме расшифровки – открытым текстом.

Секретный ключ $K$ является объединения восьми 32-разрядных подключей и имеет следующий вид:

$$K = K_1 \| K_2 \| .. \| K_8 \in GF(2)^{32}. \tag{2}$$

Стоит отметить, что $Q^{(e)}$ является последовательностью семидесяти четырех 32-разрядных двоичных векторов, каждый из которых является одним из восьми секретных подключей $K_i$.

SPECTR-128 является блочным шифром и обрабатывает информацию с 32-разрядной шиной обмена данных.

Секретный ключ в данной случае будет являться объединением четырех 64-разрядных подключей и иметь следующий вид:

$$K = K_1 \| K_2 \| K_3 \| K_4 \in GF(2)^{64}. \quad (3)$$

$Q^{(e)}$ в данном шифре является последовательностью пятидесяти 64-разрядных двоичных векторов, каждый из которых является одним из четырех секретных подключей $K_i$.

CIKS-128 является одним из итеративных блочных шифров и использует схемы патента РФ № 2140714 в качестве базовой схемы одного раунда [1]. Главным отличием CIKS-128 от SPEKTR-128 является использование двух идентичных нелинейных векторных булевых функций вместо блока управляемых перестановок и нелинейной векторной булевой функции.

Секретный ключ также является объединением четырех 64-разрядных подключей и иметь следующий вид:

$$K = K_1 \| K_2 \| K_3 \| K_4 \in GF(2)^{64}. \quad (4)$$

Расширенный ключ $Q^{(e)}$ представляет собой последовательность пятидесяти двух 64-разрядных двоичных векторов, каждый из которых является одним из четырех секретных подключей $K_i$.

Рассмотрим команду DDP32, которая является 32-разрядной перестановкой и ориентирована для применения в криптографических приложениях. Входными параметрами такой команды являются: 32-разрядный преобразуемый бинарный вектор *X*, 32-разрядный управляющий вектор U и одноразрядный управляющий вектор e, принимающий значения *0* (прямая перестановка) и *1* (обратная перестановка). В результате выполнения данной команды получается перестановка 32-разрядного бинарного вектора

$$X : Y = P_{32/32}(X, U, e). \quad (5)$$

Команду DDP32 можно использовать для создания скоростных программных хэш-функций.

Программный шифр SPECTR-SZ использует команду управляемых перестановок DDP32. Он ориентирован на использование в компьютерах с 32-разрядным процессором и является блочнопоточным шифром. При шифровании и расшифровке первый и последний раунды реализуют схему

поточного шифра, а остальные реализуют схему блочного шифра. SPECTR-SZ реализуется в виде модуля инициализации и резидентного модуля, который обслуживает запросы других программ на шифрование и расшифровку данных. Шифрование происходит в 6 раундов, 1 и 6 из которых являются полными, а 2-4 – сокращенными. Сокращенные раунды позволяют обеспечить реализацию сильного лавинного эффекта.

Расширенный ключ шифрования $Q$ представляет собой последовательность из 2051 байта:

$$Q = \{q_0, q_1, q_2, \ldots, q_{2049}, q_{2050}\} \tag{6}$$

Секретный ключ в данном случае имеет вид

$$K = (k_0, k_1, k_2, \ldots, k_s), \tag{7}$$

где $8 \le s \le 2050$.

COBRA-F64a и COBRA-F64b являются блочными шифрами с малым размером входного блока данных, что позволяет строить на их основе микропрограммы. Данные шифры используют команду DDP32. Общая схема шифрования может быть задана следующей формулой:

$$Y = F^{(e)}\left(X, Q^{(e)}\right), \tag{8}$$

где $Q^{(e)} = H(K, e)$ расширенный ключ, который является функцией от 128-рарядного секретного ключа K и режима шифрования e ($F^{(0)}$ – шифрование, $F^{(1)}$ – расшифровка). В режиме шифрования $X$ является исходным блоком двоичных данных, т.е. открытым текстом, а в режиме расшифровки – преобразованным блоком двоичных данных (шифртекстом). В режиме шифрования $Y$ является шифртекстом, а в режиме расшифровки – открытым текстом. Заметим, что $X, Y \in GF(2)^{32}$. В алгоритмах COBRA-F64a и COBRA-F64b используются два 32-разрядных подключа, а именно

$$Q^{(e)} = (Q_j^{(1,e)}, Q_j^{(2,e)}). \tag{9}$$

Секретный ключ $K$ представлен в виде объединения 32-разрядных слов:

$$K = K_0 \| K_1 \| .. \| K_n \in GF(2)^{32}. \tag{10}$$

В программных шифрах DDP-S64 и DDP-S128 также используется полууниверсальная схема шифрования, представленная в формуле 8, однако, ключ $K$ имеет 256-разрядность. Функция шифрования проходит в 3 этапа: начально преобразование, $r$ раундов преобразования с использованием

установленной алгоритмом процедуры, заключительное преобразование. Для DDP-S64 значение r принимается равным 10, а для DDP-S128 – 12. Оба шифра являются стойким к дифференциальному криптоанализу.

Шифр CryptoStar был разработан на основе аппаратно-ориентированного алгоритма COBRA-H6 и является стойким к линейному и дифференциальному аналитическим анализам. В рассматриваемом шифре используется новый криптографический примитив – переключаемая операция. Смеха шифрования и расшифровки, рассчитанная на 14 раундов, имеет вид:

$$Y = T^{(0)}(X, K), \tag{11}$$

$$X = T^{(1)}(Y, K) \tag{12}$$

где $X$ – открытый текст, $Y$ – шифртекст, $K$ – секретный ключ, $T^{(e)}$ – функция для преобразования блока данных, e = 0 (шифрование) или e = 1 (расшифровка). Кроме того, $X, Y \in \{0,1\}^{256}$ $K \in \{0,1\}^{512}$ [3]. Секретный ключ рассматривается как объединение четырех подключей (формула 13), а на их основе формируется раундовый ключ $Q_j^{(e)}$.

$$K = (K_1, K_2, K_3, K_4) \tag{13}$$

Рассмотренные нами шифры несут практическую пользу для их применения. Таким образом, актуальной задачей в области компьютерных методов защиты информации является разработка и реализация скоростных шифров, которые сохраняют высокую скорость шифрования, являются криптостойкими и содержат в себе управляемые операций.

*Список литературы*

*1 Молдовян А. А., Молдовян Н. А., Гуц Н.Д., Изотов Б. В. Криптография: скоростные шифры. [Текст] / А. А. Молдовян. – СПб.: БХВ-Петербург, 2002. – 496 с.*

*2 Гуц Н. Д., Изотов Б. В., Молдовян Н. А. Скоростной алгоритм шифрования SPECTR-H64 // Безопасность информационных технологий. – 2000. – № 4. – С. 37-50.*

*3 Шниперов, А. Н. Высокоскоростная симметричная криптосистема на основе управляемых операций CryptoStar / А. Н. Шниперов // Современные информационные технологии в науке, образовании и практике: сб. науч. тр. – Оренбург: ИПК ГОУ ОГУ, 2007. – С. 154-156.*