

НЕЙРОСЕТЕВЫЕ ОПЕРАЦИОННЫЕ БЛОКИ, РЕАЛИЗУЮЩИЕ ВЗАИМНО-ОБРАТНЫЕ УПРАВЛЯЕМЫЕ ПЕРЕСТАНОВКИ, И ИХ ПРИМЕНЕНИЕ ДЛЯ ОРГАНИЗАЦИИ БЛОЧНОГО ШИФРОВАНИЯ

© 2012 В. Н. Лопин¹, О. И. Лапшиков²

¹докт. техн. наук, профессор каф. программного обеспечения
и администрирования информационных систем
e-mail: kzis3@yandex.ru

²аспирант каф. программного обеспечения
и администрирования информационных систем
e-mail: woodlin@mail.ru

Курский государственный университет

Приведено описание нейросетевых логических модулей, построенных на основе иерархических нейросетей, реализующих операцию подстановки в бинарном информационном потоке. Рассмотрена организация блочного шифрования с использованием взаимно-обратных управляемых перестановок.

Ключевые слова: бинарный поток, нейросетевые логические модули, блочный шифр, управляемые перестановки.

В работах [Лопин, Захаров 2004, 2004a] были рассмотрены вопросы шифрования бинарного потока с использованием нейросетевых логических модулей. Для реализации шифрования была предложена система шифрования (рис. 1) с иерархической структурной организацией управляемых нейросетевых логических модулей NET^m, NET^n .

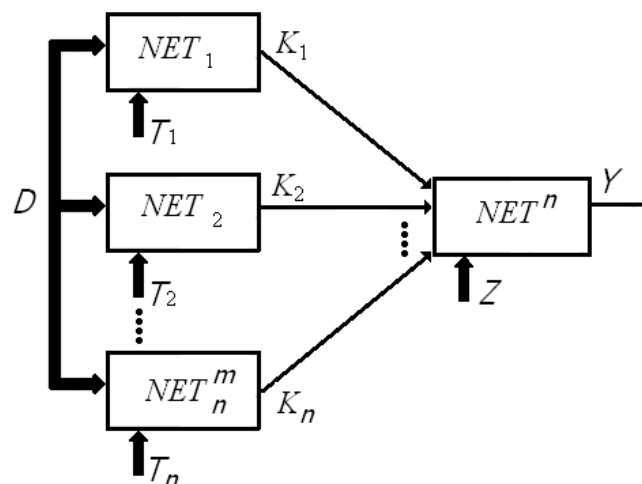


Рис. 1. Система шифрования

В соответствии с алгоритмом функционирования системы, исходный бинарный поток Z представлялся последовательностью блоков длиной 2^n бит, к которым периодически применялся некоторый фиксированный набор операций подстановки для реализации перестановок в этих блоках. Особенностью этого подхода [Лопин, Захаров 2004a] являлась возможность формирования любой последовательности периодических

перестановок для блоков бинарного потока Z путем задания соответствующих функций активации структуры с помощью настроек (T_1, \dots, T_n) .

В работах [Молдовян, Молдовян, Советов 2001; Молдовян, Молдовян, Еремеев 2004] была показана эффективность использования различных управляемых операций для проектирования блочных шифров. Дальнейшее развитие подхода, основанного на использовании нейросетевых управляемых логических модулей, позволило предложить вариант блочного шифрования с использованием взаимно-обратных управляемых перестановок, описанный в данной работе.

На рисунке 2 представлена схема одного раунда такого блочного шифрования.

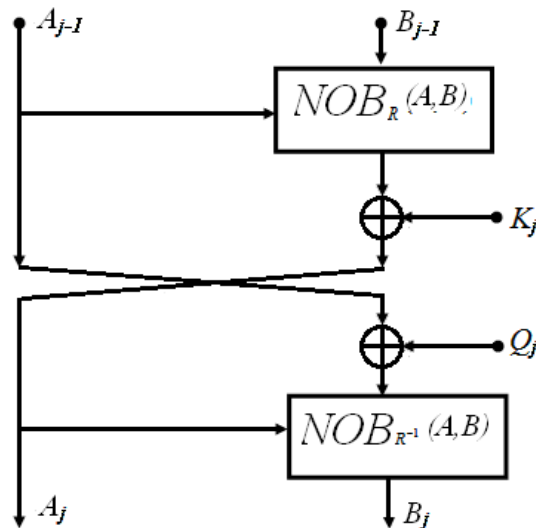


Рис. 2. Схема раунда

В этой схеме используется перенастраиваемый нейросетевой операционный блок, представленный функцией $Y = NOB_M(A, B)$ и предназначенный для реализации двух взаимно-обратных управляемых перестановок:

$$(F_A(B), F_A^{-1}(B)) : F_A(F_A^{-1}(B)) = F_A^{-1}(F_A(B)). \quad (1)$$

Здесь: $M \in (R, R^{-1})$ – матрица настройки блока, определяющая настройку операционного блока на управляемую перестановку $F_A(B)$ при $M=R$ или на управляемую перестановку $F_A^{-1}(B)$ при $M=R^{-1}$; A – вектор управления перестановками; B – вектор входа; Y – вектор выхода. В раунде шифрования используются ключи K_j и Q_j .

Можно доказать, что процедуры шифрования и расшифрования отличаются лишь распределениями (расписаниями) этих ключей по раундам шифрования и расшифрования. Очевидно, что независимо от числа раундов такое доказательство достаточно рассмотреть на двух раундах, выполняющих соответственно шифрование и расшифрование.

Для этого доказательства рассмотрим некоторую гипотетическую систему, включающую в свой состав последовательно раунд шифрования и раунд расшифрования, определяемые схемой на рисунке 2. Для раундовых ключей такой системы введем следующее распределение:

$$(K_j, Q_j, Q_{j+1}, K_{j+1}) : (Q_{j+1} = Q_j, K_{j+1} = K_j).$$

Докажем, что на втором раунде такой системы будет выполнена процедура расшифрования, то есть будут выполнены условия:

$$A_{j+1} = A_{j-1}, B_{j+1} = B_{j-1}. \quad (2)$$

Действительно, для первого раунда шифрования в соответствии со схемой раунда можно записать следующие преобразования:

$$A_j = F(A_{j-1}, B_{j-1}) \oplus K_j, B_j = F^{-1}(A_j, A_{j-1} \oplus Q_j).$$

Для второго раунда расшифрования выполняются преобразования:

$$A_{j+1} = F(A_j, B_j) \oplus Q_{j+1}, B_{j+1} = F^{-1}(A_{j+1}, A_j \oplus K_{j+1}).$$

Таким образом, на втором раунде, учитывая свойства (1) взаимно-обратных управляемых перестановок, можно записать:

$$A_{j+1} = F(A_j, B_j) \oplus Q_{j+1} = F(A_j, F^{-1}(A_j, A_{j-1} \oplus Q_j)) \oplus Q_{j+1} = A_{j-1};$$

$$B_{j+1} = F^{-1}(A_{j+1}, A_j \oplus K_{j+1}) = F^{-1}(A_{j+1}, F(A_{j-1}, B_{j-1}) \oplus K_j \oplus K_{j+1}) = B_{j-1}.$$

Следовательно, условия расшифрования (2) на втором раунде предлагаемой системы блочного шифрования выполняются.

Нейросетевой операционный блок $NOB_M(A, B)$, как и приведенная ранее на рисунке 1 система шифрования, может быть реализован в базисе управляемых нейросетевых логических модулей NET^m, NET^n .

В работе [Лопин, Захаров 2004а] было показано, что в любом нейросетевом логическом модуле $NET^k, k \in (n, m)$, представленном на рисунке 3, управление перестановками в бинарном потоке Z можно задавать графом переходов вектора X .

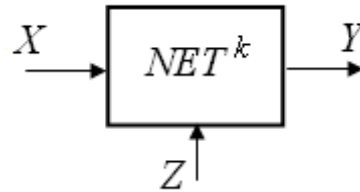


Рис. 3. Нейросетевой логический модуль: $X = (x_1, \dots, x_n); Z = (z_1, \dots, z_{2^n}); Y = (y_1, \dots, y_{2^n})$

Действительно, как следует из [Лопин, Захаров 2004, 2004а], любой граф переходов $GX_j[c_{ij}]; i \in (0, 1, \dots, 2^n - 1); j \in (1, 2, \dots, 2^n!)$, представленный на рисунке 4, однозначно определяет соответствующую операцию подстановки для 2^n разрядного блока в бинарном потоке Z .

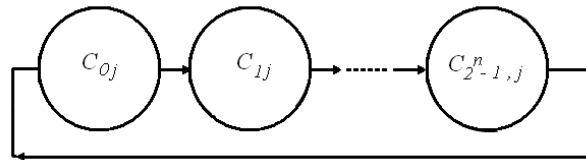


Рис. 4. Граф переходов вектора $X: c_{ij} = (x_{1ij}, x_{2ij}, \dots, x_{nij})$

Таким образом, любому графу $GX_j[c_{ij}]$ можно поставить в соответствие некоторую операцию подстановки P_j и наоборот. Известно, что иерархический нейросетевой модуль NET^k может реализовать любую булеву функцию k переменных $Y = f_z(X)$, где $Z = (z_1, \dots, z_{2^m})$ – вектор настройки модуля [Там же]. Следовательно,

оказывается возможным в базе иерархических нейросетевых модулей организовать управление графами переходов $GX_j[c_{ij}]$ и, соответственно, операциями подстановки P_j . На рисунке 5 представлена структура операционного блока $NOB_M(A, B)$ в базе нейросетевых модулей NET^k . На данном рисунке изображены векторы $A = (a_1, \dots, a_n)$, $B = (b_1, \dots, b_n)$, $Y = (y_1, \dots, y_n)$, $M = (R; R^{-1}) = (R_{1j}, \dots, R_{nj}, R_{1j}^{-1}, \dots, R_{nj}^{-1})$, $j = (1, \dots, d)$.

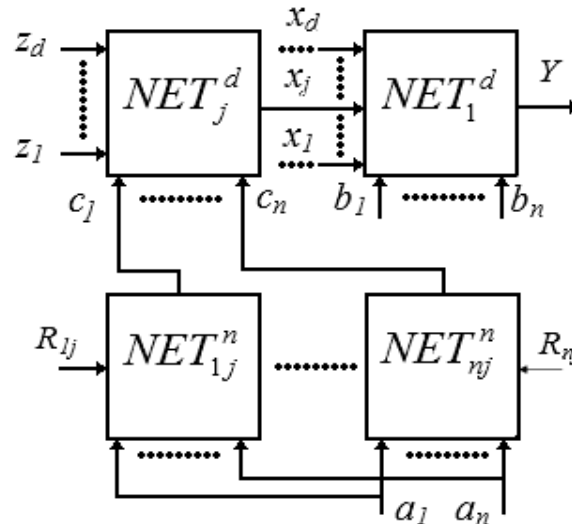


Рис. 5. Структура операционного блока $NOB_M(A, B)$

Вектор инициализации $Z = (z_1, \dots, z_d)$ задается фиксированным графом переходов $GZ[k_i]$; $k_i = i$, $i \in (0, 1, \dots, 2^d - 1)$, который изображен на рисунке 6.

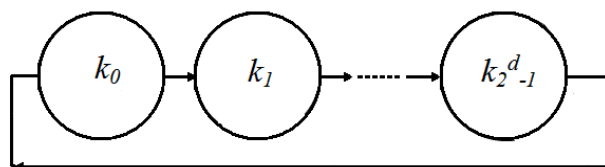


Рис. 6. Граф переходов вектора Z

Представленный операционный блок $NOB_M(A, B)$ реализует перестановку $F_A(B)$ при $M=(R)=(R_{1j}, \dots, R_{nj})$ и перестановку $F_A^{-1}(B)$ при $M=(R^{-1})=(R_{1j}^{-1}, \dots, R_{nj}^{-1})$. Таким образом, обе взаимно-обратные управляемые перестановки реализуются одним операционным блоком, допускающим перенастройку двух возможных режимов.

Из структуры, представленной на рисунке 6, следует, что для реализации операционного блока $NOB_M(A, B)$ при $A=(a_1, \dots, a_n)$ и $B=(b_1, \dots, b_n)$ необходимо использовать $S_d = (1 + \log_2 n)$ модулей NET^d и $S_n = (n \cdot \log_2 n)$ модулей NET^n .

Учитывая, что аппаратная реализация раунда преобразования блока длиной n требует применения двух операционных блоков $NOB_M(A, B)$, можно определить структурную сложность S аппаратной реализации раунда следующим выражением:

$$S = (2S_d + 2S_n); S_d = (1 + \log_2 n), S_n = (n \cdot \log_2 n).$$

Таким образом, в операционном блоке $NOB_M(A, B)$ можно использовать однородные базисные нейросетевые модули двух типов NET^d и NET^n , отличающиеся лишь числом информационных и настроечных входов.

Очевидно, что предлагаемая структурная организация операционных блоков, основанная на применении однородных базисных нейросетевых модулей двух типов, в значительной степени отвечает возможности их аппаратной реализации в виде СБИС.

Библиографический список

Лопин В. Н. Захаров И. С. Применение иерархических нейросетей для шифрования бинарного информационного потока // Телекоммуникации. М.: Наука и технологии, 2004. №11. С. 36–40.

Лопин В. Н. Захаров И. С. Шифрование бинарного информационного потока методом периодических перестановок на основе нейросетевых логических модулей // Телекоммуникации. М.: Наука и технологии, 2004а. №12. С. 31–35.

Молдовян Н. А., Молдовян А. А., Еремеев М. А. Криптография от примитивов к синтезу алгоритмов. СПб.: БХВ-Петербург, 2004. 448 с.

Молдовян Н. А., Молдовян А. А., Советов Б. Я. Криптография. СПб.: Лань, 2001. 224 с.