УДК 681.3

М.А. Еремеев, И.Е. Горбачев

СВОЙСТВА УПРАВЛЯЕМЫХ ПОДСТАНОВОЧНО-ПЕРЕСТАНОВОЧНЫХ СЕТЕЙ ДЛЯ БЛОЧНЫХ АЛГОРИТМОВ ШИФРОВАНИЯ НА ОСНОВЕ ОДНОГО КЛАССА ПОДСТАНОВОК

Еремеев М.А., Горбачев И.Е. **Свойства управляемых подстановочно-перестановочных сетей для блочных алгоритмов шифрования на основе одного класса подстановок.**

Аннотация. Статья посвящена исследованию управляемых подстановочно-перестановочных сетей на основе управляемых элементов $F_{4/2}$ в качестве примитива блочных алгоритмов шифрования. Актуальность исследований связана с их ориентацией на проектирование скоростных аппаратных шифров. Научная и практическая значимость полученных результатов заключается в повышении эффективности аппаратной реализации скоростных алгоритмов шифрования, предназначенных для защиты информации в информационно-телекоммуникационных системах и сетях.

Ключевые слова: защита информации, блочные шифры, управляемые подстановочно-перестановочные сети, криптографический примитив.

Eremeev M.A., Gorbachev I.E. **Properties of the Controlled Substitution-Permutation Network for Block Encryption Algorithm Based on One Class of Permutations.**

Abstract. Article is devoted to investigation of the controlled substitution-permutation network based on managed elements $F_{4/2}$ as a primitive block encryption algorithms. Relevance of research is related to their focus on the design of high-speed hardware ciphers. The scientific and practical significance of the results is to improve the efficiency of high-speed hardware implementation of encryption algorithms, designed to protect information in information and telecommunication systems and networks.

Keywords: information security, block ciphers, controlled substitution-permutation network, cryptographic primitive.

1. Введение. Постоянно увеличивающийся объем конфиденциальной информации, циркулирующей в информационно-телекоммуникационных сетях (ИТКС), предъявляет повышенные требования к современным шифрам. Характерным является повышение требований одновременно по стойкости, скорости и простоте реализации.

Любой блочный шифр представляет собой большое множество подстановок заданного размера, выбираемых в зависимости от секретного ключа. Однако такое непосредственное задание шифра на практике не реализуется, поскольку требует неимоверно большого количества памяти. Но такие подстановки можно генерировать. Соответствующий генератор и представляет собой блочный алгоритм шифрования. Построение блочных шифров на практике осуществляется путем многократного применения относительно простых криптографических преобразований (примитивов). В современных блочных шифрах наиболее широко используются

следующие примитивы: перестановки, подстановки, циклический сдвиг, побитовое сложение по модулю 2 (гаммирование), сложение по модулю 2^n. Использование управляемых операций в качестве криптографического примитива давно привлекает внимание разработчиков шифров. Под управляемой операцией преобразования понимается операция, управляемая некоторым двоичным вектором. При фиксированном значении управляющего вектора реализуются преобразования, относящиеся к одному из вариантов (модификаций) операции. Иными словами, управляемую операцию можно охарактеризовать как множество различных модификаций, каждая из которых соответствует конкретному значению управляющего вектора. Управляющий вектор в таких операциях может формироваться по секретному ключу и/или по преобразуемому блоку данных. Использование такого рода операций открывает большие перспективы для построения стойких и высокоскоростных блочных шифров.

В работах [1–6] была показана эффективность использования управляемых подстановочно-перестановочных сетей (УППС) для синтеза блочных шифров, ориентированных на программную реализацию, в том числе и реализацию в программируемых интегральных схемах. В настоящее время в массовом масштабе выпускаются программируемые логические интегральные схемы (ПЛИС - FPGA) нового поколения, которые предоставляют потенциальную возможность для существенного повышения эффективности аппаратной реализации блочных шифров, оцениваемую по показателю отношения производительности к используемым вычислительным ресурсам. Реализация этой возможности предполагает проектирование УППС, ориентированных на максимальное использование ресурсов типовых логических блоков, содержащихся в новых ПЛИС. Это делает актуальным вопрос о поиске новых типов операций, зависящих от преобразуемых данных (ОЗПД) и реализуемых с помощью УППС, построенных с использованием управляемых элементов (УЭ), более полно использующих объем памяти элементарных ячеек памяти в логических матрицах FPGA, по сравнению с ранее пользованными типами УЭ $F_{2/1}$ [1], $F_{2/2}$ [2].

Программируемые логические матрицы, широко распространенные в настоящее время (к примеру, Virtex-6), содержат типовые логические блоки, включающие два SLICE-узла, каждый из которых включает четыре логические ячейки LUT (LOOP UP TABLE), представляющие собой 64-битовые элементы памяти (ячейки). Каждая такая ячейка позволяет реализовать произвольную булеву функцию (БФ) от шести переменных. Это обеспечивает эффективную реализацию УЭ типов $F_{2/3}$ и $F_{2/4}$, задающих, соответственно, выполнение 8 и 16 подстановок размера 2×2 в зависимости от значения двоичного вектора на управляющем входе, что показано в работах [3–5].

Заметим, что эффективность ОЗПД связана с увеличением размера подблока преобразуемых данных, над которыми они задают некоторую подстановку. Если модификации данной ОЗПД задают преобразование n-битовых векторов и число этих модификаций M, то сама ОЗПД определяет преобразование над N-битовыми векторами, где $N=n+\log_2 M$. Из последнего соотношения видно, что для повышения эффективности ОЗПД необходимо увеличивать число модификаций (размерность управляющего вектора) и размер подблока преобразуемых данных. Таким образом, интерес представляет управляемый элемент $F_{4/2}$, который позволяет на 100% использовать ресурс ячейки памяти. При этом, в отличие от УЭ с двухбитовым входом данных (таким как $F_{2/4}$), для УЭ $F_{4/2}$ возможно построение УППС, обеспечивающих нелинейность преобразования данных при фиксировании управляющего подблока данных. Разумно предположить, что при соответствующем выборе УЭ типа $F_{4/2}$ можно обеспечить существенное повышение криптографических показателей синтезируемого операционного блока. Это позволит сократить число раундов преобразования при сохранении высокой стойкости алгоритмов.

В данной работе рассматривается задача разработки критериев выбора УЭ $F_{4/2}$ и их использования для синтеза УППС и скоростных блочных шифров, ориентированных на эффективную аппаратную реализацию с использованием ПЛИС.

2. Варианты представления, критерии построения и проектирование УЭ $F_{4/2}$. Управляемый элемент $F_{4/2}$ обладает 4-х битовым входом и выходом и 2-х битовым управляющим входом. Схемное представление УЭ $F_{4/2}$ представлено на рисунке 1.

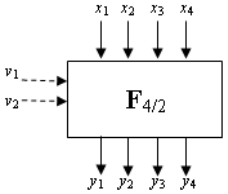

Рис. 1. Управляемый элемент $F_{4/2}$

В общем случае УЭ $F_{4/2}$ удобно представлять в следующих двух видах:

1) В виде четырех булевых функций от 6-ти переменных;

2) В виде упорядоченного набора из четырех подстановок размером 4×4, каждая из которых выполняется над входным 4-х битовым двоичным вектором $X=(x_1, x_2, x_3, x_4)$ при одном из четырех возможных значений управляющего вектора $V=(v_1, v_2)=(0,0), (0,1), (1,0), (1,1)$.

Для синтеза эффективных многослойных УППС требуется

сформулировать некоторые критерии выбора конкретных вариантов УЭ вида $F_{4/1}$. На основании вышеизложенного и результатов, полученных в работе [1], сформулируем следующие базовые критерии отбора и проектирования УЭ $F_{4/2}$:

1) Любой из четырех выходов блока $F_{4/2}$ должен представлять собой нелинейную БФ от шести переменных: $y_i=f_i(x_1, x_2, x_3, x_4, v_1, v_2)$, $i=1, ..., 4$, каждая из которых имеет значение нелинейности близкое к максимально возможному значению для сбалансированных БФ от шести переменных;

2) Каждая из четырех элементарных модификаций УЭ $F_{4/2}$, а именно $F^{(0)}$, $F^{(1)}$, $F^{(2)}$, $F^{(3)}$ должна осуществлять биективное преобразование $(x_1, x_2, x_3, x_4) \rightarrow (y_1, y_2, y_3, y_4)$;

3) Каждая из четырех модификаций УЭ $F_{4/2}$ должна быть инволюцией;

4) Все линейные комбинации БФ: $f_5= y_1 \oplus y_2$, $f_6= y_1 \oplus y_3$, $f_7= y_1 \oplus y_4$, $f_8= y_2 \oplus y_3$, $f_9= y_2 \oplus y_4$, $f_{10}= y_3 \oplus y_4$, $f_{11}= y_1 \oplus y_2 \oplus y_3$, $f_{12}= y_1 \oplus y_2 \oplus y_4$, $f_{13}= y_1 \oplus y_3 \oplus y_4$, $f_{14}= y_2 \oplus y_3 \oplus y_4$ *и* $f_{15}= y_1 \oplus y_2 \oplus y_3 \oplus y_4$ должны иметь значения нелинейности близкие к $NL(y_1)$, $NL(y_2)$, $NL(y_3)$, $NL(y_4)$.

Используя эти критерии и перебирая различные варианты УЭ $F_{4/2}$, можно найти множество конкретных элементов $F_{4/2}$, представляющих интерес для использования в проектировании блочных шифров. Для оценки возможности полного перебора всех возможных вариантов УЭ $F_{4/2}$ могут быть использованы два варианта поиска УЭ.

Первый состоит в переборе всех возможных четверок булевых функций $y_1=f_1(x_1,x_2,x_3,x_4,v_1,v_2)$, $y_2=f_2(x_1,x_2,x_3,x_4,v_1,v_2)$, $y_3=f_3(x_1,x_2,x_3,x_4,v_1,v_2)$, $y_4=f_4(x_1,x_2,x_3,x_4,v_1,v_2)$. Но объем вычислений, требующихся для реализации этого варианта, очень велик. В самом деле, существует 2^{64} различных булевых функций от 6 переменных, следовательно, необходимо перебрать $2^{64}\cdot(2^{64}-1)\cdot(2^{64}-2)\cdot(2^{64}-3)\approx \approx 11{,}5\cdot10^{76}$ различных четверок булевых функций. Мы можем существенно ограничить количество вариантов перебора, воспользовавшись следствием из второго критерия выбора БФ, а именно тем, что выход операции, реализующей биективное преобразование, описывается сбалансированной БФ. Количество сбалансированных БФ от n переменных равно числу сочетаний $C_{2^n}^{2^{n-1}}$, которое при $n=6$ приблизительно равняется $1{,}8\cdot10^{18}$, что также достаточно велико и не позволяет выполнить полный перебор.

Минимальное количество вариантов перебора достигается при втором подходе, так как в этом случае проектирование УЭ $F_{4/2}$ сводится к формальному выбору модификаций $F^{(0)}$, $F^{(1)}$, $F^{(2)}$, $F^{(3)}$, каждая из

которых является подстановкой размера 4×4. Количество подстановок размера 4×4 определяется по формуле $2^n!$, что при n=4 равняется $2{,}092 \cdot 10^{13}$. Причем существует $4{,}621 \cdot 10^7$ вариантов таких подстановок удовлетворяющих третьему критерию. Следовательно, проектирование сводится к выбору четверок подобных модификаций. Однако и в этом случае полный перебор является сложной вычислительной задачей.

Рассмотрим возможность сокращения числа рассматриваемых подстановок. Итак, наименьшее число вариантов подстановок обеспечивает требование номер три. Построение всего множества подстановок 4×4 являющихся инволюциями представляется вычислимой задачей. Каждую инволюцию можно представить в виде векторной булевой функции - совокупности БФ, каждая из которых будет описывать по одному выходу УЭ $F_{4/2}$. Для обеспечения максимальной нелинейности преобразования, при фиксированных битах управляющего вектора следует отфильтровывать только те инволюции, в векторную БФ которых входят БФ с максимально возможным значением нелинейности. Хотя максимальное значение нелинейности для БФ от 4-х переменных и равняется 6, для сбалансированных БФ (следствие 2-го критерия) этот показатель не превышает значения 4.

Существенным является влияние всех входных битов на каждый выходной бит, для этого БФ описывающая выход должна зависеть от каждого входного бита, иными словами ее алгебраическая нормальная форма должна иметь в своей записи столько различных переменных, сколько входов у УЭ. В нашем случае это 4.

Для противодействия попыткам проведения криптоанализа немаловажную роль играет также показатель корреляционной эффективности БФ.

В целях проведения исследования была разработана программа, позволяющая отсеивать инволюции по значению характеристик векторных БФ соответствующих конкретной инволюции. Она позволяет отсеивать инволюции по приведенным критериям и выводит результат в файл с некоторой сопутствующей информацией. С учетом вышеизложенных требований остается всего 32256 инволюций. Перебор всех четверок модификаций требует анализа $1{,}08 \cdot 10^{18}$ вариантов, что существенно меньше полученного ранее значения, но также велико.

Для практического применения УЭ $F_{4/2}$ достаточно найти сравнительно малое число таких элементов представляющих их основные подклассы, удовлетворяющие сформулированным критериям. Поэтому можно применить полный перебор по некоторой репрезентативной выборке УЭ $F_{4/2}$, генерируя варианты $F_{4/2}$ путем равновероятной случайной выборки модификаций $F^{(0)}$, $F^{(1)}$, $F^{(2)}$, $F^{(3)}$. В таблице 1 приведена небольшая выборка из множества инволюций,

удовлетворяющих описанным выше критериям. Каждая строчка этой таблицы задает инволюцию.

Таблица 1. Выборка из множества инволюций

№ п/п	f_1	f_2	f_3	f_4
1	$x_4 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1$	$x_3 \oplus x_1x_4 \oplus x_1x_3 \oplus x_1x_2$	$x_2 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1 \oplus x_1x_4 \oplus x_1x_3 \oplus x_1x_2$	$x_2x_4 \oplus x_2x_3 \oplus x_1x_4 \oplus x_1x_3 \oplus x_1x_2$
2	$x_4 \oplus x_3 \oplus x_3x_4 \oplus x_2x_3 \oplus x_1x_3$	$x_3 \oplus x_1x_4 \oplus x_1x_3 \oplus x_1x_2$	$x_2 \oplus x_1x_4 \oplus x_1x_3 \oplus x_1x_2$	$x_3 \oplus x_3x_4 \oplus x_2x_3 \oplus x_1 \oplus x_1x_3$
3	$x_3 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1x_4 \oplus x_1x_3$	$x_4 \oplus x_2 \oplus x_2x_3 \oplus x_1 \oplus x_1x_3$	$x_3x_4 \oplus x_2 \oplus x_2x_4 \oplus x_1x_4$	$x_3x_4 \oplus x_2x_4 \oplus x_1 \oplus x_1x_4$
4	$x_4 \oplus x_1x_4 \oplus x_1x_3 \oplus x_1x_2$	$x_3x_4 \oplus x_2 \oplus x_2x_4 \oplus x_1 \oplus x_1x_4$	$x_4 \oplus x_2 \oplus x_1x_3 \oplus x_1x_2$	$x_3 \oplus x_3x_4 \oplus x_2 \oplus x_2x_4 \oplus x_1x_4$
5	$x_4 \oplus x_3x_4 \oplus x_2x_4 \oplus x_1x_3 \oplus x_1x_2$	$x_4 \oplus x_3x_4 \oplus x_2 \oplus x_2x_4 \oplus x_1x_3 \oplus x_1x_2$	$x_4 \oplus x_2 \oplus x_1x_4 \oplus x_1x_3 \oplus x_1x_2$	$x_3 \oplus x_2 \oplus x_1x_4 \oplus x_1x_3 \oplus x_1x_2$
6	$x_4 \oplus x_3 \oplus x_1 \oplus x_1x_4 \oplus x_1x_2$	$x_3x_4 \oplus x_2x_3 \oplus x_1 \oplus x_1x_4 \oplus x_1x_2$	$x_3 \oplus x_2 \oplus x_1 \oplus x_1x_4 \oplus x_1x_2$	$x_1x_2 \oplus x_3x_4 \oplus x_2x_3 \oplus x_1x_4 \oplus x_2x_4 \oplus x_3$
7	$x_4 \oplus x_2 \oplus x_2x_3 \oplus x_1x_2$	$x_4 \oplus x_3x_4 \oplus x_2x_4 \oplus x_1 \oplus x_1x_4$	$x_3 \oplus x_3x_4 \oplus x_2 \oplus x_1 \oplus x_1x_4$	$x_4 \oplus x_3 \oplus x_3x_4 \oplus x_2x_4 \oplus x_1x_4$
8	$x_4 \oplus x_2 \oplus x_2x_3 \oplus x_1x_2$	$x_3x_4 \oplus x_2 \oplus x_1x_4 \oplus x_1x_3$	$x_4 \oplus x_3 \oplus x_2 \oplus x_2x_4 \oplus x_1x_2$	$x_4 \oplus x_3 \oplus x_2 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1$
9	$x_3 \oplus x_2x_4 \oplus x_1 \oplus x_1x_4 \oplus x_1x_2$	$x_4 \oplus x_2 \oplus x_2x_4 \oplus x_2x_3 \oplus x \oplus x_1x_4 \oplus x_1x_3$	$x_4 \oplus x_3 \oplus x_2x_4 \oplus x_2x_3 \oplus x \oplus x_1x_4 \oplus x_1x_3$	$x_4 \oplus x_3 \oplus x_2 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1x_4 \oplus x_1x_3$
10	$1 \oplus x_4 \oplus x_3 \oplus x_2 \oplus x_2x_4 \oplus x_1 \oplus x_1x_4$	$x_3 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1x_4 \oplus x_1x_3$	$x_2 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1x_4 \oplus x_1x_3$	$x_3x_4 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1 \oplus x_1x_4 \oplus x_1x_3$
11	$1 \oplus x_4 \oplus x_3 \oplus x_2 \oplus x_1 \oplus x_1x_4 \oplus x_1x_3$	$x_2 \oplus x_1 \oplus x_1x_4 \oplus x_1x_3$	$x_3x_4 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1x_4 \oplus x_1x_3$	$x_3 \oplus x_2 \oplus x_1x_4 \oplus x_1x_3$
12	$1 \oplus x_4 \oplus x_3x_4 \oplus x_2 \oplus x_2x_3 \oplus x_1x_3$	$x_3 \oplus x_3x_4 \oplus x_2 \oplus x_2x_3 \oplus x_1x_3$	$x_3 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1x_2$	$x_3 \oplus x_2 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1 \oplus x_1x_2$
13	$x_3x_4 \oplus x_2x_4 \oplus x_1 \oplus x_1x_3 \oplus x_1x_2$	$1 \oplus x_4 \oplus x_3 \oplus x_2 \oplus x_2x_4 \oplus x \oplus x_1x_4 \oplus x_1x_3$	$x_2 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1x_4 \oplus x_1x_3$	$x_4 \oplus x_3x_4 \oplus x_2x_3 \oplus x_1x_4 \oplus x_1x_2$
14	$x_3x_4 \oplus x_2 \oplus x_2x_3 \oplus x_1x_4 \oplus x_1x_2$	$1 \oplus x_3 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1x_2$	$x_4 \oplus x_2x_3 \oplus x_1x_2$	$x_4 \oplus x_2 \oplus x_2x_3 \oplus x_1 \oplus x_1x_2$
15	$1 \oplus x_3 \oplus x_2 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1x_4 \oplus x_1x_3$	$1 \oplus x_4 \oplus x_2 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1 \oplus x_1x_2$	$x_4 \oplus x_3 \oplus x_2 \oplus x_1 \oplus x_1x_2$	$x_2 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1$
16	$1 \oplus x_3 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1 \oplus x_1x_2$	$1 \oplus x_3 \oplus x_2 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1x_4 \oplus x_1x_3$	$x_2x_4 \oplus x_2x_3 \oplus x_1x_4 \oplus x_1x_3 \oplus x_1x_2$	$x_4 \oplus x_3 \oplus x_2 \oplus x_1x_4 \oplus x_1x_3$
17	$1 \oplus x_4 \oplus x_2 \oplus x_1x_4 \oplus x_1x_3$	$1 \oplus x_3 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1x_2$	$x_4 \oplus x_3 \oplus x_1x_2$	$x_4 \oplus x_3 \oplus x_2 \oplus x_1 \oplus x_1x_2$
18	$x_4 \oplus x_3 \oplus x_1 \oplus x_1x_4 \oplus x_1x_2$	$x_3 \oplus x_3x_4 \oplus x_2x_3 \oplus x_1$	$1 \oplus x_3 \oplus x_2 \oplus x_1 \oplus x_1x_4 \oplus x_1x_2$	$x_3 \oplus x_1x_4 \oplus x_1x_2$
19	$x_3x_4 \oplus x_2x_3 \oplus x_1 \oplus x_1x_3$	$x_3 \oplus x_3x_4 \oplus x_2x_4 \oplus x_1 \oplus x_1x_3 \oplus x_1x_2$	$1 \oplus x_3 \oplus x_3x_4 \oplus x_2 \oplus x_2x_4 \oplus x_1x_4$	$x_4 \oplus x_3 \oplus x_3x_4 \oplus x_2x_3 \oplus x_1 \oplus x_1x_4 \oplus x_1x_2$
20	$1 \oplus x_4 \oplus x_3x_4 \oplus x_2x_3 \oplus x_1 \oplus x_1x_4 \oplus x_1x_2$	$x_4 \oplus x_3x_4 \oplus x_2 \oplus x_2x_3 \oplus x_1$	$1 \oplus x_4 \oplus x_3 \oplus x_1x_4 \oplus x_1x_3 \oplus x_1x_2$	$x_3x_4 \oplus x_2x_3 \oplus x_1x_4 \oplus x_1x_3 \oplus x_1x_2$

В целях проведения анализа свойств УЭ $F_{4/2}$ по заданным модификациями $F^{(0)}$, $F^{(1)}$, $F^{(2)}$, $F^{(3)}$ получим алгебраическую нормальную форму, реализующих его БФ f_1, f_2, f_3, f_4.

Пусть $\left\{f_1^1(x_1,x_2,x_3,x_4), f_2^1(x_1,x_2,x_3,x_4), f_3^1(x_1,x_2,x_3,x_4), f_4^1(x_1,x_2,x_3,x_4)\right\}$ – БФ, реализующая модификацию $F^{(0)}$ при значении V=(0,0), $\left\{f_1^2(x_1,x_2,x_3,x_4), f_2^2(x_1,x_2,x_3,x_4), f_3^2(x_1,x_2,x_3,x_4), f_4^2(x_1,x_2,x_3,x_4\right\}$, реализующие модификацию $F^{(1)}$ при значении V=(0,1), $\left\{f_1^3(x_1,x_2,x_3,x_4), f_2^3(x_1,x_2,x_3,x_4), f_3^3(x_1,x_2,x_3,x_4), f_4^3(x_1,x_2,x_3,x_4\right\}$, реализующие модификацию $F^{(2)}$ при значении V=(1,0), $\left\{f_1^4(x_1,x_2,x_3,x_4), f_2^4(x_1,x_2,x_3,x_4), f_3^4(x_1,x_2,x_3,x_4), f_4^4(x_1,x_2,x_3,x_4\right\}$, реализующие модификацию $F^{(3)}$ при значении V=(1,1).

Тогда конкретный вид четырех БФ, реализующих УЭ $F_{4/2}$, можно получить следующим образом:

$$y_1 = (v_1 \oplus 1)(v_2 \oplus 1) f_1^1(x_1,x_2,x_3,x_4) \oplus (v_1 \oplus 1)(v_2) f_1^2(x_1,x_2,x_3,x_4) \oplus (v_1)(v_2 \oplus 1) f_1^3(x_1,x_2,x_3,x_4) \oplus (v_1)(v_2) f_1^4(x_1,x_2,x_3,x_4);$$

$$y_2 = (v_1 \oplus 1)(v_2 \oplus 1) f_2^1(x_1,x_2,x_3,x_4) \oplus (v_1 \oplus 1)(v_2) f_2^2(x_1,x_2,x_3,x_4) \oplus (v_1)(v_2 \oplus 1) f_2^3(x_1,x_2,x_3,x_4) \oplus (v_1)(v_2) f_2^4(x_1,x_2,x_3,x_4);$$

$$y_3 = (v_1 \oplus 1)(v_2 \oplus 1) f_3^1(x_1,x_2,x_3,x_4) \oplus (v_1 \oplus 1)(v_2) f_3^2(x_1,x_2,x_3,x_4) \oplus (v_1)(v_2 \oplus 1) f_3^3(x_1,x_2,x_3,x_4) \oplus (v_1)(v_2) f_3^4(x_1,x_2,x_3,x_4);$$

$$y_4 = (v_1 \oplus 1)(v_2 \oplus 1) f_4^1(x_1,x_2,x_3,x_4) \oplus (v_1 \oplus 1)(v_2) f_4^2(x_1,x_2,x_3,x_4) \oplus (v_1)(v_2 \oplus 1) f_4^3(x_1,x_2,x_3,x_4) \oplus (v_1)(v_2) f_4^4(x_1,x_2,x_3,x_4).$$

3. Основные криптографические свойства. В таблице 2 представлены некоторые наборы модификаций, которые удовлетворяют критериям 1–4.

Таблица 2. Представительные наборы модификаций

№	Значение нелинейности БФ	Набор модификаций
1	16-20-24-20-24-20-16-16-16-16-16-20-20-20-16	3-4-5-7
2	20-16-20-20-20-16-24-20-20-16-24-20-20-16-20	5-6-9-15
3	16-20-24-16-24-16-16-16-16-16-16-20-20-16-24	9-14-17-18

3.1. Дифференциальные характеристики. Одними из важных характеристик криптографических примитивов являются дифференциальные, которые отражают подверженность дифференциальному криптоанализу в целом алгоритма шифрования,

построенного на этих примитивах [1, 2, 5]. Их также можно получить для самого УЭ. Рассмотрим дифференциальные характеристики типового конструктивного элемента $F_{4/2}$ которые определят для заданной топологии операционного блока дифференциальные характеристики последнего. На рисунке 2 представлены варианты весов Хэмминга всех возможных разностей, относящихся к УЭ $F_{4/2}$.

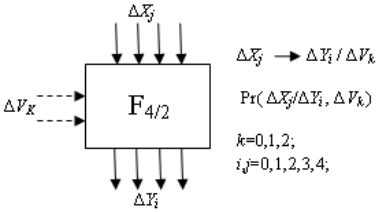

Рис. 2. Варианты разностей для УЭ $F_{4/2}$

Управляемые элементы $F_{4/2}$, удовлетворяющие заданным критериям отбора, обладают хорошими дифференциальными свойствами. Например, дифференциальные характеристики УЭ $F_{4/2}$ (см. вариант 2 в таблице 2) приведены в таблице 3.

Таблица 3. Дифференциальные характеристики

k	*i*	*j*	*Pr*	*k*	*i*	*j*	*Pr*	*k*	*i*	*j*	*Pr*
0	0	0	0.016	1	0	0	0.004	2	0	0	0.003
0	0	1	0.004	1	0	1	0.012	2	0	1	0.008
0	0	2	0.006	1	0	2	0.023	2	0	2	0.01
0	0	3	0.006	1	0	3	0.019	2	0	3	0.007
0	0	4	0	1	0	4	0.004	2	0	4	0.002
0	1	0	0	1	1	0	0.011	2	1	0	0.007
0	1	1	0.024	1	1	1	0.043	2	1	1	0.023
0	1	2	0.04	1	1	2	0.071	2	1	2	0.036
0	1	3	0.024	1	1	3	0.05	2	1	3	0.024
0	1	4	0.005	1	1	4	0.012	2	1	4	0.004
0	2	0	0	1	2	0	0.012	2	2	0	0.003
0	2	1	0.025	1	2	1	0.05	2	2	1	0.023
0	2	2	0.039	1	2	2	0.071	2	2	2	0.037
0	2	3	0.027	1	2	3	0.043	2	2	3	0.024
0	2	4	0.002	1	2	4	0.011	2	2	4	0.007
0	3	0	0	1	3	0	0.004	2	3	0	0.002
0	3	1	0.009	1	3	1	0.019	2	3	1	0.008
0	3	2	0.009	1	3	2	0.023	2	3	2	0.011
0	3	3	0.005	1	3	3	0.012	2	3	3	0.007
0	3	4	0.009	1	3	4	0.004	2	3	4	0.002
0	4	0	0	1	4	0	0	2	4	0	0
0	4	1	0	1	4	1	0	2	4	1	0
0	4	2	0	1	4	2	0	2	4	2	0
0	4	3	0	1	4	3	0	2	4	3	0
0	4	4	0	1	4	4	0	2	4	4	0

3.2 Линейные свойства УЭ $F_{4/2}$. Также важными характеристиками криптографических примитивов являются линейные, которые отражают подверженность линейному криптоанализу [1, 2, 5].

Чтобы вычислить смещение для линейных характеристик УЭ вида $F_{4/2}$, используем следующую формулу:

$$P(a,b,c)=|Pr(\mathrm{XOR}(X\bullet a,F_{4/2}(X,c)\bullet b)=0)-1/20|,$$

где $0 \le a,b \le 15$ и $0 \le c \le 3$. По этой форме, просто вычислять смещения, результаты вычисления смещения для набора модификаций номер 2 в таблице 2, представлены в таблице 4.

Таблица 4. Фрагмент таблицы линейных характеристик для УЭ $F_{4/2}$

a	*b*	*c*	*P*	*a*	*b*	*c*	*P*	*a*	*b*	*c*	*P*	*a*	*b*	*c*	*P*
0	0	0	0.5	0	0		0.5	0	0	2	0.5	0	0	3	0.5
0	1	0	0	0	1	1	0	0	1	2	0	0	1	3	0
0	2	0	0	0	2	1	0	0	2	2	0	0	2	3	0
0	3	0	0.25	0	3	1	0.25	0	3	2	0.25	0	3	3	0.25
0	4	0	0	0	4	1	0	0	4	2	0	0	4	3	0
0	5	0	0.25	0	5	1	0.25	0	5	2	0.25	0	5	3	0.25
1	0	0	0	1	0	1	0	1	0	2	0	1	0	3	0
1	1	0	0.25	1	1	1	0	1	1	2	0	1	1	3	0
1	2	0	0.25	1	2	1	0.25	1	2	2	0.25	1	2	3	0.125
1	3	0	0.125	1	3	1	0.125	1	3	2	0.25	1	3	3	0.25
1	4	0	0.25	1	4	1	0.25	1	4	2	0.25	1	4	3	0.25
1	5	0	0.125	1	5	1	0.25	1	5	2	0.375	1	5	3	0.25
2	0	0	0	2	0	1	0	2	0	2	0	2	0	3	0
2	1	0	0.25	2	1	1	0.25	2	1	2	0.25	2	1	3	0.125
2	2	0	0.25	2	2	1	0.25	2	2	2	0.25	2	2	3	0.25
2	4	0	0.125	2	4	1	0.25	2	4	2	0.25	2	4	3	0.25
3	0	0	0.25	3	0	1	0.25	3	0	2	0.25	3	0	3	0.25
3	1	0	0.125	3	1	1	0.125	3	1	2	0.25	3	1	3	0.25
3	3	0	0.25	3	3	1	0	3	3	2	0	3	3	3	0.25
4	1	0	0.25	4	1	1	0.25	4	1	2	0.25	4	1	3	0.25
4	2	0	0.125	4	2	1	0.25	4	2	2	0.25	4	2	3	0.25
4	4	0	0	4	4	1	0	4	4	2	0	4	4	3	0.25
4	5	0	0.125	4	5	1	0.25	4	5	2	0.25	4	5	3	0.375
5	0	0	0.25	5	0	1	0.25	5	0	2	0.25	5	0	3	0.25
5	1	0	0.125	5	1	1	0.25	5	1	2	0.375	5	1	3	0.25
5	3	0	0.25	5	3	1	0.3125	5	3	2	0.4375	5	3	3	0.3125

5	4	0	0.125	5	4	1	0.25	5	4	2	0.25	5	4	3	0.375
5	5	0	0	5	5	1	0	5	5	2	0.25	5	5	3	0.25
6	6	0	0.25	6	6	1	0	6	6	2	0.25	6	6	3	0.25
7	7	0	0.25	7	7	1	0	7	7	2	0.25	7	7	3	0.25
8	8	0	0	8	8	1	0.25	8	8	2	0.25	8	8	3	0.25
8	9	0	0.375	8	9	1	0.375	8	9	2	0.125	8	9	3	0.375
8	10	0	0.25	8	10	1	0.375	8	10	2	0.125	8	10	3	0.375
9	8	0	0.375	9	8	1	0.375	9	8	2	0.125	9	8	3	0.375
9	9	0	0	9	9	1	0.25	9	9	2	0.25	9	9	3	0.25
10	12	0	0.312	10	12	1	0.4375	10	12	2	0.25	10	12	3	0.4375
10	14	0	0.375	10	14	1	0.375	10	14	2	0.25	10	14	3	0.375
11	11	0	0.25	11	11	1	0.25	11	11	2	0.25	11	11	3	0.25
11	13	0	0.312	11	13	1	0.4375	11	13	2	0.4375	11	13	3	0.4375
11	15	0	0.375	11	15	1	0.375	11	15	2	0.375	11	15	3	0.375
12	12	0	0.25	12	12	1	0.25	12	12	2	0.25	12	12	3	0.25
13	11	0	0.312	13	11	1	0.4375	13	11	2	0.4375	13	11	3	0.4375
13	12	0	0.375	13	12	1	0.375	13	12	2	0.375	13	12	3	0.375
13	13	0	0.25	13	13	1	0.25	13	13	2	0.5	13	13	3	0.25
13	15	0	0.375	13	15	1	0.375	13	15	2	0.5	13	15	3	0.375
14	12	0	0.375	14	12	1	0.375	14	12	2	0.375	14	12	3	0.375
14	14	0	0.25	14	14	1	0.25	14	14	2	0.5	14	14	3	0.25
14	15	0	0.375	14	15	1	0.375	14	15	2	0.5	14	15	3	0.375
15	14	0	0.375	15	14	1	0.375	15	14	2	0.5	15	14	3	0.375
15	15	0	0.25	15	15	1	0.25	15	15	2	0.5	15	15	3	0.25

4. Блочный шифр на основе управляемых операций. Покажем пример использования УЭ $F_{4/2}$ при разработке блочного шифра на основе управляемых операций.

Необходимо определить критерии построения:

1) Блочный шифр должен быть итеративным, обеспечивающим высокую скорость преобразования данных при относительно недорогой аппаратной реализации. Блок данных определим в 128 бит;

2) Для выполнения процедур зашифрования и расшифрования должен использоваться один и тот же алгоритм, а смена режима преобразования должна обеспечиваться сменой расписания

использования ключей;

3) В целях сохранения высокой производительности шифра в приложениях, требующих частой сменой ключа, будем использовать простое расписание ключа.

Схема итеративного шифрования представлена на рисунке 3, где $\mathrm{Crypt}^{(e)}$ – раундовое преобразование, а значение $e \in GF(2)$ определяет режим преобразования.

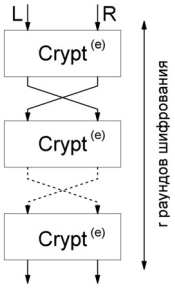

Рис. 3. Схема итеративного шифрования

На рисунке 4 приведен вариант реализации раундового преобразования $\mathrm{Crypt}^{(e)}$.

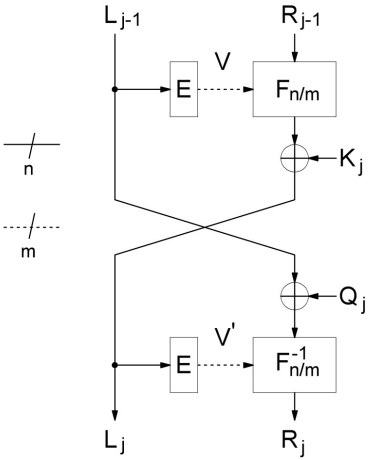

Рис. 4. Вариант раундового преобразования $\mathrm{Crypt}^{(e)}$ в общем виде

Преобразование Crypt можно представить в виде функции:

$$(L_j, R_j)=\text{Crypt}(L_{j-1},R_{j-1}, K_j, Q_j),$$

или в виде

$$L_j \leftarrow \text{F}_{n/m}(R_{j-1}, \text{E}(L_{j-1})) \text{ XOR } \text{K}_\text{j}$$

$$R_j \leftarrow \text{F}^{-1}{}_{n/m}(L_{j-1} \text{ XOR } Q_j, \text{E}(\text{F}_{n/m}(R_{j-1}, \text{E}(L_{j-1})) \text{ XOR } K_j)),$$

здесь (L_{j-1}, R_{j-1}) и (L_j, R_j) входной и преобразованные блоки данных, представленные в виде конкатенации подблоков одного размера. (K_j, Q_j) – j раундовый ключ, состоящий из двух раундовых подключей одного размера и равных по размеру подблокам L_j и R_j. E – блок расширения, необходимый для формирования управляющего вектора V и представляющий собой простое разветвление проводов, что практически не вносит временную задержку.

Данное раундовое преобразование обращается простой перестановкой раундовых подключей:

$$\text{Crypt}(L, R, K, Q) = (L', R');$$

$$\text{Crypt}(L', R', Q, K) = (L, R).$$

Таким образом, при использовании простого расписания ключей для которого $(K_j, Q_j)=(Q_{r-j+1}, K_{r-j+1})'$, где штрихом обозначен $(r-j+1)$ раундовый ключ процедуры расшифрования, шифрование является корректным, т.е. процедура расшифрования обратна процедуре шифрования.

Дальнейшее проектирование шифра сводится к выбору конкретной реализации блока расширения, выбору числа раундов R, формированию расписания ключа, и разработке конкретной пары управляемых операций F и F^{-1}.

Блок $\text{F}_{n/m}$ построенный на основе УЭ $\text{F}_{4/2}$ представляет несколько слоев параллельно расположенных и не пересекающихся между собой УЭ $\text{F}_{4/2}$. Между соседними слоями используются фиксированные коммутаторы π, основной принцип коммутации – обеспечение влияния каждого входного бита на каждый выходной бит. Общий вид блока $\text{F}_{n/m}$ представлен на рисунке 5.

Мы определили размер блока данных в 128 бит, отсюда следует, что n для нашего блока равно 64. Один слой нашего блока будет состоять из 16 УЭ $\text{F}_{4/2}$. Для того чтобы каждый входной бит влиял на все выходные потребуется $\log_4 16+1=3$ слоя. Соответственно размер управляющего вектора равен $3 \cdot 16 \cdot 2=96$ бит, а размер управляющего подблока данных всего 64, поэтому необходимо использовать блок расширения E. Реализация $\text{F}_{64/92}$ представлена на рисунке 6.

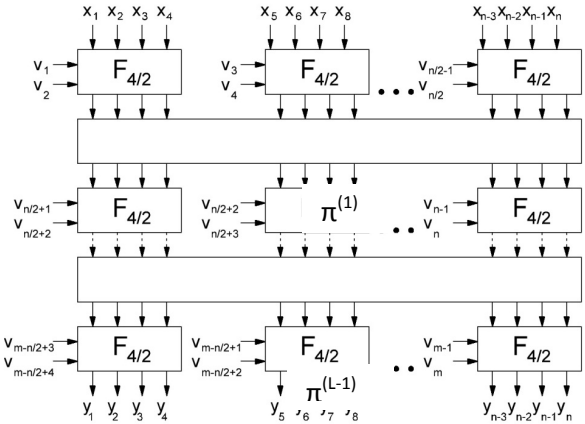

Рис.5. Общий вид блока $F_{n/m}$ на основе $F_{4/2}$ с послойной структурой

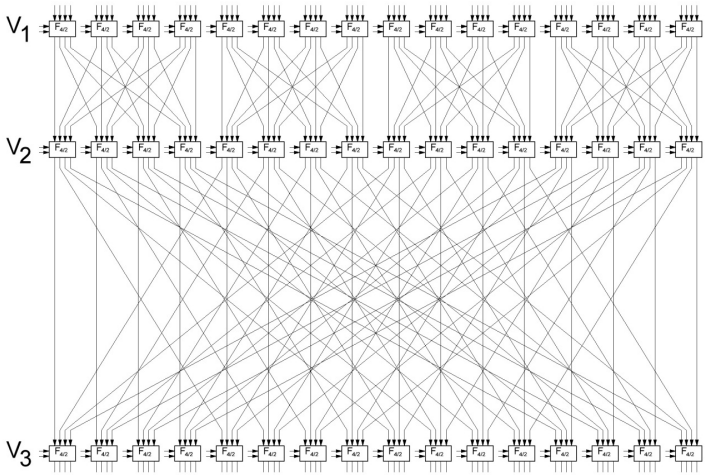

Рис. 6. Структура блока $F_{64/92}$

Для построения обратного преобразования F^{-1} достаточно в блоке F поменять местами вход и выход а управляющий вектор, представленный в виде конкатенации векторов размера *m*/*l*, записать в обратном порядке.

Вероятность прохождения разницы минимального веса через один раунд шифрования равняется $2^{-13,6}$. Таким образом, 10 раундов будет достаточно для успешного противодействия дифференциальному криптоанализу.

Результаты сравнительного анализа сложности аппаратной

реализации [6] и скорости преобразования современных блочных алгоритмов шифрования приведены в таблице 5.

Таблица 5. Сравнение аппаратной реализации различных блочных шифров ПЛИС Xilinx Virtex-6

Шифр	#CLB	Скорость Mbps	Эффективность Mbps / #CLB
AES	2358	259	0,11
IDEA	2878	600	0,21
DES	722	181	0,25
Шифр на основе $F_{4/2}$	*96*	*1119*	*11,65*

4. Заключение. На настоящий момент использование управляемых операций прошло достаточную практическую апробацию на примере блочных шифров DES, RC5, RC6 и MARS и др.. Исследования показывают, что применение управляемых операций позволяет эффективно противостоять дифференциальному и линейному криптоанализу. Использование управляемых операций позволяет строить стойкие и высокоскоростные блочные шифры. В настоящей работе приведено описание УЭ $F_{4/2}$, сформулированы основные требования к проектированию УЭ, показаны основные методы построения таких элементов, и приведены дифференциальные и линейные характеристики для конкретного примера реализации УЭ.

Результаты могут быть использованы при проектировании скоростных блочных шифров на основе управляемых операций, предназначенных для защиты информации, циркулирующей в ИТКС.

Литература

1. *Молдовян А.А., Еремеев М.А., Молдовян Н.А., Морозова Е.В.* Полная классификация и свойства нелинейных управляемых элементов минимального размера и синтез криптографических примитивов // Вопросы защиты информации. 2003. №3. С.15–27.
2. *Еремеев М.А., Молдовян А.А., Молдовян Н.А.* Шифры на основе управляемых операций: комбинирование сетей различного типа // Вопросы защиты информации. 2004. №3. С.17–23.
3. *Хо Н.З.* Разработка и исследование нового класса управляемых элементов $F_{2/3}$ // Инновационная деятельность в Вооруженных силах Российской Федерации: Труды всеармейской научно-практической конференции. СПб.: ВАС. 2010. С. 419–424.
4. *Хо Н.З., Молдовян А.А.* Разработка управляемых подстановочно-перестановочных сетей на основе управляемых элементов $F_{2/3}$ для синтеза скоростных блочных шифров // Известия СПбГЭТУ ‹‹ЛЭТИ››. 2011. №6. С. 25–30.
5. *Еремеев М.А., Молдовян А.А., Молдовян Н.А.* Разработка и исследование подстановочно-перестановочных сетей для блочных алгоритмов шифрования на основе одного класса управляемых элементов $F_{2/2}$ // Вопросы защиты информации. 2003. №4. С.14–22.
6. *Еремеев М.А., Коркишко Т.А., Мельник А.А., Молдовян А.А., Молдовяну П.А.* Аппаратная поддержка программных шифров // Вопросы защиты информации. 2002. №2. С.26–34.

References

1. Moldovjan A.A., Eremeev M.A., Moldovjan N.A., Morozova E.V. [Complete classification and properties of nonlinear control elements of the minimum size and synthesis of cryptographic primitives]. *Voprosy zashhity informacii – Information security questions*. Moscow: Federal Informational and Analytical Center of the Defense Industry (VIMI). 2003. vol. 3. pp. 15–27. (In Russ).
2. Eremeev M.A., Moldovjan A.A., Moldovjan N.A. [Ciphers based on controlled operations: combining different types of networks]. *Voprosy zashhity informacii - Information security questions*. Moscow: Federal Informational and Analytical Center of the Defense Industry (VIMI). 2004. vol. 3. pp. 17–23. (In Russ).
3. Ho N.Z. [Development and research of a new class of managed elements $F_{2/3}$]. *Innovacionnaja dejatel'nost' v Vooruzhennyh silah Rossijskoj Federacii: Trudy vsearmejskoj nauchno-prakticheskoj konferencii* [Innovative activity in the Armed Forces of the Russian Federation: Proceedings of the All-Army scientific and practical conference]. SPB: Military Academy of Telecommunications. 2010. pp. 419–424. (In Russ).
4. Ho N.Z., Moldovjan A.A. [Development of controlled substitution-permutation network based on managed elements $F_{2/3}$ for the synthesis of high-speed block ciphers]. *Izvestija SPbGJeTU «LJeTI» – News of the SPbGJeTU «LJeTI»*. SPB: Saint Petersburg Electrotechnical University "LETI". 2011. vol. 6. pp. 25–30. (In Russ).
5. Eremeev M.A., Moldovjan A.A., Moldovjan N.A. [Development and research of controlled substitution-permutation network for block encryption algorithms based on a class of controlled elements $F_{2/2}$]. *Voprosy zashhity informacii – Information security questions*. Moscow: Federal Informational and Analytical Center of the Defense Industry (VIMI). 2003. vol. 4. pp. 14–22. (In Russ).
6. Eremeev M.A., Korkishko T.A., Mel'nik A.A., Moldovjan A.A., Moldovjanu P.A. [Hardware support for software ciphers]. *Voprosy zashhity informacii – Information security questions*. Moscow: Federal Informational and Analytical Center of the Defense Industry (VIMI). 2002. vol. 2. pp. 26–34. (In Russ).

Еремеев Михаил Алексеевич — д-р техн. наук, профессор, начальник кафедры систем сбора и обработки информации, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: информационная безопасность, криптография, моделирование конфликтующих систем, автоматизированные системы сбора и обработки информации. Число научных публикаций — 200. mae1@rambler.ru; ул. Ждановская, д. 13, Санкт-Петербург, 197198; р.т.: +7(812) 237-19-60.

Eremeev Mikhail Alekseevich — Ph.D., Dr. Sci., professor, head of system for collecting and processing information department, Mozhaisky Military Space Academy. Research interests: information security, cryptography, modeling of the conflicting systems. The number of publications — 200. mae1@rambler.ru; 13, Zhdanovskaya street, St.-Petersburg, 197198, Russia; office phone: +7(812) 237-19-60.

Горбачев Игорь Евгеньевич — к-т техн. наук, доцент, докторант кафедры систем сбора и обработки информации, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: исследование операций, информационная безопасность, искусственный интеллект, информационные конфликты в инфотелекоммуникационном пространстве. Число научных публикаций — 60. gie1976@mail.ru; ул. Ждановская, д. 13, Санкт-Петербург, 197198; р.т.: +7(812) 347-96-87.

Gorbachev Igor' Evgen'evich — Ph.D., associate professor, doctoral student of system for collecting and processing information department, Mozhaisky Military Space Academy. Research interests: research of operations, artificial intelligence, information security, the information conflicts in infotelekommunikatsionny space. The number of publications — 60. gie1976@mail.ru; 13, Zhdanovskaya street, St.-Petersburg, 197198, Russia; office phone: +7(812) 347-96-87.

РЕФЕРАТ

Еремеев М.А., Горбачев И.Е. **Свойства управляемых подстановочно-перестановочных сетей для блочных алгоритмов шифрования на основе одного класса подстановок.**

Постоянно увеличивающийся объем конфиденциальной информации, циркулирующей в информационно-телекоммуникационных сетях, предъявляет повышенные требования к современным шифрам. Характерным является повышение требований одновременно по стойкости, скорости и простоте реализации.

Статья посвящена исследованию управляемых подстановочно-перестановочных сетей на основе управляемых элементов $F_{4/2}$ в качестве примитива блочных алгоритмов шифрования. Показано, что применение управляемых операций позволяет эффективно противостоять дифференциальному и линейному криптоанализу, а также строить стойкие и высокоскоростные блочные шифры. В работе рассматривается задача разработки критериев выбора управляемых элементов $F_{4/2}$ и их использования для синтеза управляемых подстановочно-перестановочных сетей и скоростных блочных шифров, ориентированных на эффективную аппаратную реализацию с использованием программируемых логических интегральных схем.

Результаты могут быть использованы при проектировании скоростных блочных шифров на основе управляемых операций, предназначенных для защиты информации, циркулирующей в критической инфраструктуре.

SUMMARY

Eremeev M.A., Gorbachev I.E. **Properties of the Controlled Substitution-Permutation Network for Block Encryption Algorithm Based on One Class of Permutations.**

An ever-increasing amount of confidential information circulating in the information and telecommunications networks, has high requirements for modern ciphers. Characteristic is the increasing demands concurrently for durability, speed and ease of implementation.

Article is devoted to investigation of the controlled substitution-permutation network based on managed elements $F_{4/2}$ as a primitive block encryption algorithms. It is shown that the use of controlled operations allows to effectively resist differential and linear cryptanalysis, as well as build resistant and high-speed block ciphers. The paper examines the problem of the development of criteria for the selection of managed elements $F_{4/2}$ and their use for the synthesis of controlled substitution-permutation networks and block ciphers, focused on efficient hardware implementation using programmable logic integrated circuits.

The results can be used in the design of high-speed block ciphers based on managed operations designed to protect the information circulating in the critical infrastructure.