УДК 519.689

А.А. Смагин, П.И. Смикун

О ВОЗМОЖНОСТИ СОВМЕЩЕНИЯ ФУНКЦИЙ ШИФРОВАНИЯ И КОНТРОЛЯ ОШИБОК В СИСТЕМЕ КОДИРОВАНИЯ

Смагин Алексей Аркадьевич, *доктор технических наук, профессор, окончил радиотехнический факультет Ульяновского политехнического института. Заведующий кафедрой телекоммуникационных технологий и сетей Ульяновского государственного университета. Имеет свыше 100 статей, изобретения, монографию в области разработки информационных систем различного назначения. [Тел.: (8422) 32-01-00 / E-mail: AlSmagin@ulsu.ru].*

Смикун Петр Иванович*, окончил факультет автоматики и вычислительной техники Таганрогского радиотехнического института. Начальник научно-исследовательского отделения - заместитель главного конструктора ФНПЦ ОАО «НПО «Марс». Имеет статьи в области разработки информационных систем различного назначения. [Тел.: (8422) 26-28-98 / E-mail: smikun@mail.ru].*

Аннотация

В настоящей статье рассмотрены вопросы совмещения матричного шифрования/дешифрования данных и контроля ошибок, неизбежно возникающих в процессе передачи данных по каналам связи.

Ключевые слова: шифрование, кодирование, матрично-ранговое кодирование, контроль ошибок.

Abstract

The present article deals with issues of combination of matrix encoding/decoding of data and error control, which emerge inevitably during data communication via communication channel.

Key words: encryption, encoding, matrix and rank encoding, error control.

Построение методов кодирования данных для передачи их по зашумленным каналам и каналам, обладающим свойствами защиты информации, способностью обнаруживать, исправлять ошибки, является актуальной задачей. Область применения таких методов — это системы регистрации импульсной информации о сбоях специальной аппаратуры, различного рода телеметрические системы, системы обработки битовых потоков.

Одним из методов кодирования, который имеет такие свойства, является метод матрично-рангового кодирования, исследованный в [1, 2, 3]. В основу метода положена модифицированная матрица биноминальных коэффициентов Паскаля, которая позволяет при определенной организации выборки из нее целых чисел [1] формировать двоичный код. Характерной особенностью матрицы кодирования является возможность манипулирования выбором получения одного из множества вариантов матричного преобразования. Другими словами, одному и тому же входному слову можно поставить во взаимно-однозначное соответствие множество кодовых комбинаций, получаемых по правилу матричного кодирования.

Манипуляция опирается на выбор по определенной стратегии одного из n-входов в матрицу кодирования, где n - целое число, ограниченное величиной блочного разбиения исходного потока данных.

Возможность многовариантного выбора, который связан с понятием ранга (номера входа в матрицу кодирования), позволяет обеспечить защиту передаваемых данных на определенном уровне, а в комбинации с другими примитивами шифрования — повысить секретность до приемлемого уровня. Достаточно подробный анализ вероятностей криптозащиты данных выполнен в работах [3, 6]. Показано, что матричное кодирование можно использовать как систему предшифра, в котором ранг играет роль предключа. При этом предшифр может в композиции с методом шифрования на основе циклического сдвига (например, RC5, RC6, MAPS) образовывать новый криптографический примитив, стойкий к линейному и дифференциальному криптоанализу, с достаточно простой схемотехнической или программной реализацией.

Структура предложенных композиционных шифров отвечает общим принципам построения шифров и включает работу с закрытыми симметричными ключами, процедуру порождения множества подключей по заданному правилу.

Второе свойство метода матричного коди-

рования, а именно возможность обнаружения ошибок, рассмотрено в [1, 4, 5]. Доказано [5], что двоичные коды целых неотрицательных десятичных чисел, полученные методом матрично-рангового кодирования, позволяют обнаружить по меньшей мере одну ошибку. Указанное свойство базируется на способности выявлять наличие неверной передачи данных, основываясь на учете двух факторов:

- данные передаются по каналу, кодированные двоичными словами постоянной длины;

- вес всех кодовых слов одинаков и равен выбранному режиму кодирования.

Исходя из структуры матричного кода, можно не только обнаруживать ошибки, но и исправлять их. Эффект применения предлагаемого подхода состоит в использовании особенностей кода наряду с реализацией возможности одновременного диагностирования полос связи параллельных каналов.

Так для случая несимметричного канала передачи данных в структуру кодовой комбинации, полученной матричным способом, вводится в начало кода один нулевой избыточный бит. Длина кодового слова L увеличивается и становится равной $L+1$. Поскольку матричный код всегда начинается с единицы, то появляется возможность контролировать комбинацию 01: на позиции $i \ mod \ (L+1)$ — ноль, а на позиции $(i+1) \ mod \ (L+1)$ - единицу.

$P_1 = i \ mod \ (L+1)$ и $P_2 = (i+1) \ mod \ (L+1)$,

где i — номер блока;

L — длина блока.

Процедура контроля наличия ошибок в двух проверяемых разрядах кода может быть реализована с использованием циклического сдвига в зависимости от его порядкового номера i.

Метод обнаружения ошибок на основе подсчета единиц ранга, который известен получателю, и учет комбинации 01 в старших разрядах матричного кода можно объединить. Это позволяет улучшить распознающие свойства метода.

При совмещении функций шифрования/дешифрования и обнаружения ошибок возникает следующая проблема. Шифрование на основе матричного кода включает в себя необходимость смены подключа (ранга) всякий раз при появлении нового блока, полученного при разбиении входного потока данных.

При обнаружении ошибок, основываясь на структуре матричного кода, ранг не меняется (остается неизменным). Это необходимое условие. Образовавшееся противоречие порождает задачу — как удовлетворить требованиям вариативности ранга при шифровании и сохранить его неизменность при контроле ошибок в рамках одной системы подготовки данных для передачи по параллельному каналу связи.

Вторая часть проблемы заключается в том, что необходимо определить, какая операция «шифрование» или «формирование кода» для контроля ошибок будет первой в очереди преобразований исходного блока, а какая — второй.

Если операция шифрования будет первой, то контроль ошибок обязан иметь постоянный для всех блоков ранг, что по условиям шифрования является недопустимым. К тому же, не проверенный на достоверность полученный код не позволит осуществить правильное его дешифрование.

Если операция шифрования будет второй в очереди преобразований, то обнаружить ошибку не представляется возможным.

Отсюда требуется компромиссное решение. С этой целью предлагается идея двойного матричного кодирования, общая схема которого представлена на рисунке 1.

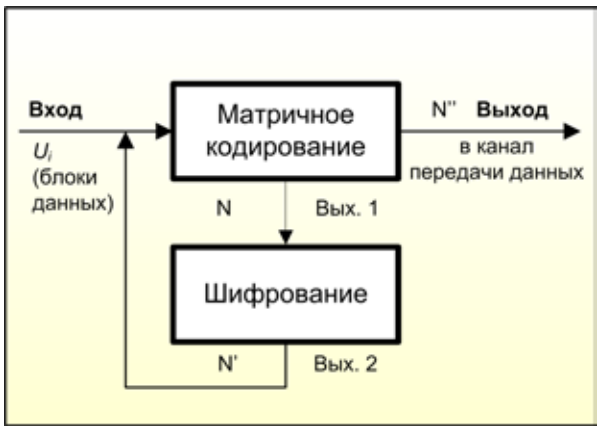

Рис. 1. Схема двойного матричного кодирования

В представленной на рисунке 1 схеме *i*-блок данных *Ui* поступает на вход подсистемы матричного кодирования (программа, аппаратура), где формируется матричный код N

$N = \varphi(U_i)$,

где φ - матричное преобразование;

i — номер блока данных.

Полученный код N служит предшифром для собственно второго уровня шифрования (в композиционном шифре в качестве операции второго уровня может быть выбран циклический сдвиг или суммирование единиц). Далее матричный код $N = (U_k^i)$ поступает на вход подсистемы шифрования второго уровня, где образуется шифрматричный код со своим переменным рангом $R_ш$, т.е.

$N' = f_ш(Nk^t)$,

где k^t — ключ шифрования.

На третьем шаге необходимо сформировать код, пригодный для проведения операции контроля ошибок с новым рангом $R_п$, который позволит обнаруживать ошибки. Для этого шиф-

рматричный код подается на вход подсистемы матричного кодирования, где вновь вырабатывается преобразование

$$N'' = \varphi(U_i).$$

Таким образом, для обеспечения требуемого эффекта необходимо выполнить два матричных преобразования и одно шифрование.

Достижение поставленной цели, а именно совмещение двух функций: шифрование и контроль ошибок, в рамках одного способа кодирования влечет за собой дополнительные временные издержки, которые можно минимизировать, например, за счет схемного варианта построения матричного преобразователя с хранимой матрицей чисел и использованием достаточно простого циклического сдвига на быстрых регистрах.

В [2] приведены оценки скорости передачи разработанных матричных кодов и их связь с корректирующей способностью; здесь же показано, что при минимальном хеммингговом расстоянии, равном двум, скорость передачи кода ниже верхней границы Плоткина и близка к ней.

Предложенная схема формирования обобщенного кода относится к передающей (входной) части канала передачи данных и на ее основе может быть построена приемная (выходная) часть канала.

Общая модель системы подготовки, прохождения по каналу и обработки полученных данных представлена в виде коммутативной диаграммы (см. рис. 2), на которой вершинам графа приписаны соответствующие преобразования, а дугам — получаемые результаты. В модели использованы следующие обозначения:

- ИК- исходный код (блок);
- М — матрица преобразований;
- ПК1 — первый предключ;
- МК1 — матричный код, полученный на первом шаге матричного преобразования;
- К — ключ шифрования;

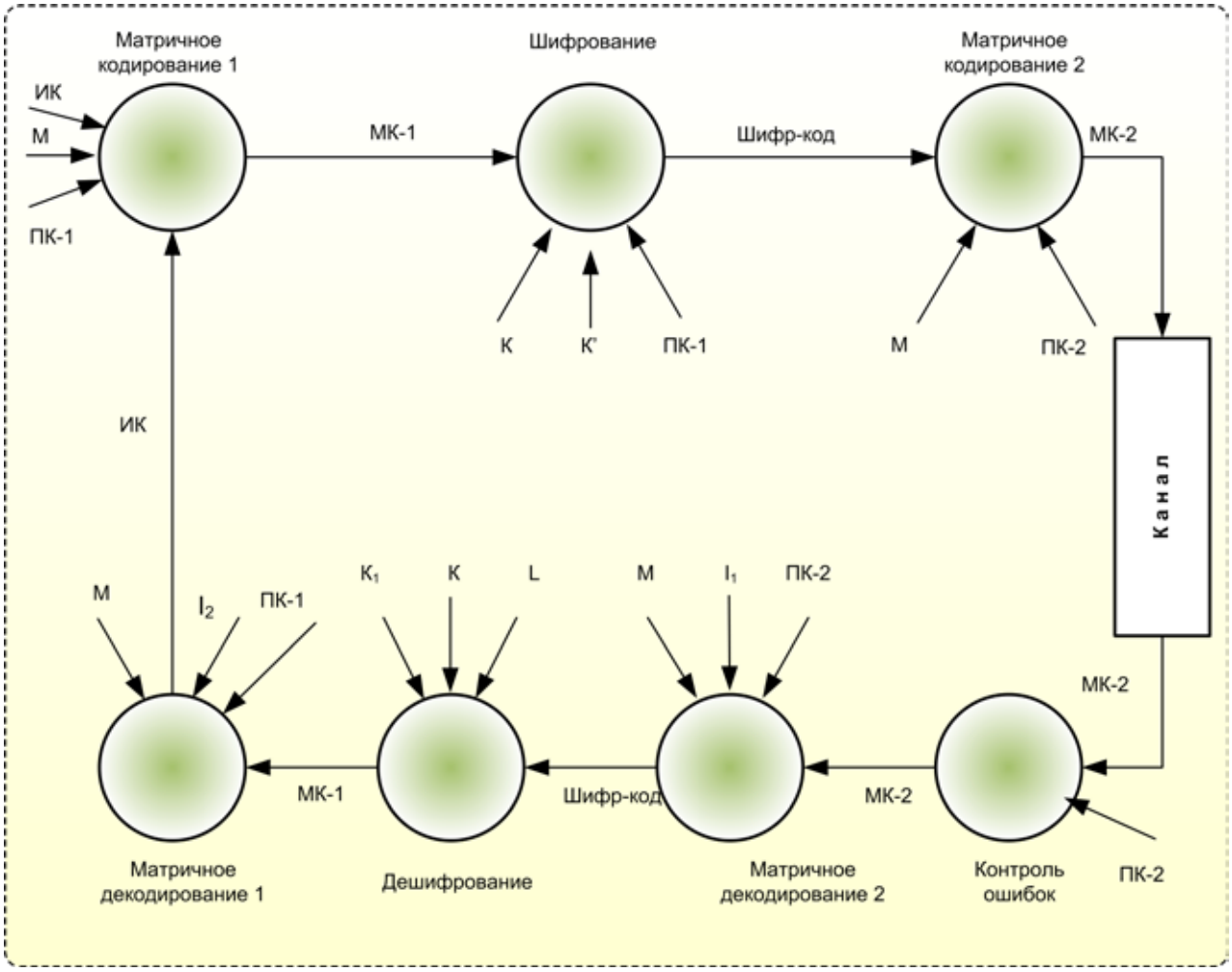

Рис. 2. Схема передачи блоковых кодов с использованием матрично-рангового преобразования

- k′ — подключ шифрования для второго шага преобразований;
- ПК2 — второй подключ;
- МК2 - матричный код, полученный на втором шаге матричного преобразования;
- I — некоторая вспомогательная информация.

Процессы контроля ошибок изложены выше, процедура матричного декодирования — в [1], процедура дешифрования — в [6]. Таким образом, все необходимые действия в модели — коммутативной диаграмме определены. Проведены экспериментальные проверки отдельно по процедурам кодирования/декодирования, шифрования/дешифрования и контроля ошибок, которые подтвердили правильность исходных посылок.

Предложенное совмещение функций «шифрование/дешифрование» и «контроль ошибок» может найти применение в несимметричных параллельных каналах связи для передачи блоковых кодов, построение которых для матрично-рангового преобразования изложено в [1].

СПИСОК ЛИТЕРАТУРЫ

1. Смагин А.А., Терентьева Ю.Ю. Математическая модель счетчика, построенная на основе кода Линча-Дэвисона // Известия ВУЗов. Приборостроение. - 2000. - № 3. - С. 28-32.

2. Смагин А.А., Терентьева Ю.Ю. Способ преобразования дискретной информации. Фундаментальные проблемы математики и механики // Ученые записки УлГУ. - Ульяновск: УлГУ, 1996. - Вып. 1. - Часть 2. - С. 101-108.

3. Смагин А.А., Терентьева Ю.Ю., Капитанчук В.В. Метод построения криптографического примитива. Международная конференция «Информационные технологии и безопасность» (ИТБ-2004), Украина, Крым, Партенит, 22-24 июня 2004 г.

4. Смагин А.А., Смикун П.И., Терентьева Ю.Ю. Об одном способе построения блоковых кодов. Спец. выпуск «Четверть века изысканий и экспериментов по созданию уникальных технологий и материалов для авиастроения». УНТЦ-ФГУП-ВИАМ// Известия Самарского НЦ РАН. - 2008. - Том 4. - С. 99-102.

5. Смагин А.А., Смикун П.И., Терентьева Ю.Ю. Алгоритм помехоустойчивой передачи потока данных // Известия научного центра Российской академии наук. — 2008. - Т.4. - С. 96-98.

6. Смагин А.А., Капитанчук В.В. Разработка двухуровневого композиционного шифра // Ученые записки Ульяновского государственного университета. Серия «Информационные технологии». - Ульяновск, 2005. - № 2. - С. 46-52.