УДК 519.876.5

ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ СТОЙКОСТИ ПОЛИНОМИАЛЬНОЙ СХЕМЫ РАЗДЕЛЕННОЙ ПЕРЕДАЧИ ДАННЫХ

Н. С. Могилевская, П. П. Простяков
Южный федеральный университет (г. Ростов-на-Дону, Российская Федерация)

Рассмотрена полиномиальная схема разделенной передачи данных, основанная на использовании кодов Рида–Маллера и дифференцировании полиномов нескольких переменных, заданных над различными полями Галуа. В системе предполагается, что отправитель разделяет исходные данные на несколько частей, а затем передает эти части независимо друг от друга по различным каналам связи. Получатель сообщений исправляет непреднамеренные ошибки, внесенные каналом связи, и восстанавливает исходные данные из принятых частей. Интересен вопрос, что может узнать нелегальный пользователь системы, если он сумеет организовать перехват данных из одного или нескольких каналов связи. Авторами схемы построены теоретические оценки стойкости схемы передачи данных к некоторым атакам в случае использования полей Галуа нечетной мощности. Проведено экспериментальное исследование возможностей нелегального пользователя. Реализовано специальное программное средство, которое моделирует процесс восстановления данных или ключа наблюдателем системы по перехваченным значениям. С применением этого средства проведен ряд экспериментов по оценке стойкости системы при различных атаках. Результаты проведенного экспериментального исследования согласуются с оценками авторов системы в случае ее реализации в полях Галуа нечетной мощности, а также показывают, что полиномиальная схема разделенной передачи данных, построенная над бинарными полями Галуа, не является стойкой.
Ключевые слова: атака на ключ, атака на шифротекст, разделенная передача данных, коды Рида–Маллера, каналы связи.

UDC 519.876.5

EXPERIMENTAL RESEARCH OF THE STABILITY OF A POLYNOMIAL SCHEME OF DIVIDED DATA TRANSMISSION

N. S. Mogilevskaya, P. P. Prostyakov
Southern Federal University (Rostov-on-Don, Russian Federation)

The paper considers a polynomial scheme of divided data transmission based on the use of Reed-Muller codes and differentiation of polynomials of several variables defined over different Galois fields. The system assumes that the sender splits the source data into several parts, and then transmits these parts independently from each other through various communication channels. The message recipient corrects unintentional errors made by the communication channel, and restores the original data from the received parts. An interesting question is what an illegal user of a system can find out if he manages to intercept data from one or more communication channels. The authors of the scheme have constructed theoretical estimates of the resistance of the data transmission scheme to certain attacks in the case of using Galois fields of odd power. In this work, an experimental study of the possibilities of an illegal user is carried out. A special software tool that simulates the process of data or key recovery by an observer of the system from intercepted values has been implemented. A number of experiments has been carried out to assess the stability of the system in various attacks. The results of the experimental study are consistent with

the estimates of the authors of the system in case of its implementation in Galois fields of odd power, and show that the polynomial split data transmission scheme constructed over the Galois binary fields is not stable.

Keywords: key attack, ciphertext attack, split data transmission, Reed-Muller codes, communication channels.

Введение. В работах [1–2] построена система разделенной передачи данных (РПД), основанная на использовании теории квадратичных форм, дифференцировании полиномов нескольких переменных над полями Галуа и кодах Рида–Маллера. Основное отличие работ [1–2] в мощности использованных полей Галуа. В работе [2] рассмотрен один вариант атаки на систему РПД. Работа [3] полностью посвящена теоретической оценке стойкости системы РПД, построенной над полями Галуа нечетной мощности, в зависимости от возможностей нелегального пользователя этой системы.

Целью работы является проведение экспериментального исследования стойкости системы разделенной передачи данных из [1–2].

1. Идея организации систем разделенной передачи данных. В литературе [1, 4–9] представлены некоторые известные системы распределенного хранения и передачи данных. Системы разделенного хранения и передачи данных организуются с использованием схожих методов, далее для определенности следует говорить о системах передачи данных. В таких системах отправитель некоторым образом разделяет исходные данные на несколько частей, а затем передает эти части независимо друг от друга по различным каналам связи. Получатель сообщений восстанавливает исходные данные из принятых частей. Для передачи могут быть использованы как несколько отдельных каналов, так и многоканальная система передачи [10]. Целью использования разделенной передачи может быть повышение скорости или надежности связи, а также обеспечение конфиденциальности передаваемых данных за счет усложнения задачи перехвата из нескольких каналов связи. Если в системе используется секретный ключ, то обычно каждому каналу соответствует свой частичный ключ, вырабатываемый из общего ключа по какому-либо правилу.

В системах РПД принято называть наблюдателем нелегитимного пользователя, который обнаружил уязвимость в технической защите одного или нескольких каналов легальных пользователей и организовал перехват данных. Канал, созданный наблюдателем, называют отводным каналом. Целью нелегитимного участника является как получение исходных данных, так и получение секретного ключа системы или частичного ключа, соответствующего тому каналу системы связи, из которого организован отводной канал. От количества организованных каналов наблюдения, а также от длительности их использования зависит результативность атаки, организованной наблюдателем.

2. Необходимые сведения о полиномиальной системе РПД. Введем необходимые обозначения [1–2]. F_p – конечное поле Галуа, p – простое число, $F_p^{(r)}[x_1, x_2, ..., x_m]$ – кольцо полиномов от m переменных над полем F_p, при этом степень полиномов из этого кольца не превышает r. F_p^m – m-мерное линейное пространство над F_p.

Производной полинома $f \in F_p^{(r)}[x_1, x_2, ..., x_m]$ по направлению $\bar{b} \in F_p^m$ называется

$$(D_b f)(\bar{x}) = f(\bar{x} + \bar{b}) - f(\bar{x}). \quad (1)$$

Если $f \in F_p^{(r)}[x_1, x_2, ..., x_m]$, то для результата дифференцирования верно $D_{\bar{b}} f \in F_p^{(r-1)}[x_1, x_2, ..., x_m]$.

В векторном пространстве F_p^m зафиксируем некоторое упорядочение

$$\{\bar{\alpha}_1, \bar{\alpha}_2, ..., \bar{\alpha}_n\},\ \bar{\alpha}_i \in F_p^m,\ n = p^m. \quad (2)$$

Коды Рида–Маллера (РМ-коды) над конечным полем F_p (см. [1–2]) с информационными полиномами из $f \in F_p^{(r)}[x_1, x_2, ..., x_m]$ и соответствующими информационными векторами $\bar{f}$ определяются натуральными параметрами r и m, $m \geq r > 0$, $m \geq 2$ и задаются выражением:

$$RM_p(r,m) = \{(f(\bar{\alpha}_1), f(\bar{\alpha}_2), ..., f(\bar{\alpha}_n)) \mid f(x) \in F_p^{(r)}[x_1, x_2, ..., x_m]\} \subset F_p^n.$$

Параметр r называется порядком кода. РМ-коды образуют семейство линейных $[n,k,d]_p$-кодов, где длина кода $n = p^m$, размерность кода вычисляется по формулам

$$k = 1 + m, \text{ при } r = 1;\ k = 1 + m + \frac{m(m+1)}{2}, \text{ при } r = 2. \quad (3)$$

Способ вычисления минимального кодового расстояния d кода можно найти, например, в [1–2].

Информационный полином $f \in F_p^{(r)}[x_1, x_2, ..., x_m]$ кодируется с помощью вычисления его значений в точках пространства F_p^m, при этом точки используют из упорядочения (2):

$$C(f) = (f(\bar{\alpha}_1), f(\bar{\alpha}_2), ..., f(\bar{\alpha}_n)).$$

В полиномиальной схеме [1–2] для разделения и восстановления данных используются $[n,k_1,d_1]_p$-коды Рида–Маллера первого порядка и $[n,k_2,d_2]_p$-коды Рида–Маллера второго порядка, заданные над полем Галуа F_p простой мощности p. Значения p и m являются параметрами схемы. Основными этапами работы схемы являются разделение исходного сообщения на m частей, передача этих частей по m различным каналам и восстановление исходного сообщения. Секретным ключом системы является упорядоченный набор базисных векторов $\beta = \{\bar{b}_i \in F_p^m\}_{i=1,...,m}$.

Опишем упрощенно часть схемы разделенной передачи, связанной с разделением сообщений и отправкой данных в каналы связи. Исходным сообщением является информационный полином $f(\bar{x}) \in F_p^{(2)}[x_1, x_2, ..., x_m]$ $[n,k_2,d_2]_p$-кода $RM_p(2,m)$, затем этот полином кодируется и строится вектор $C(f(\bar{x})) \in F_p^n$. Далее для каждого вектора b_i, $i = \overline{1,m}$ из секретного ключа β схемы вычисляется производный вектор $\overline{D_{\bar{b}_i}(C(f(\bar{x}))}$ от кодового вектора $C(f(\bar{x}))$. Производный вектор составляется из коэффициентов производного полинома $D_{\bar{b}_i}(C(f(\bar{x}))$. По каждому из m различных каналов связи передаются соответствующие векторы $\overline{D_{\bar{b}_i}(C(f(\bar{x}))}$ В [1–2] показано, что $D_{\bar{b}}(C(f(\bar{x})) = C(D_{\bar{b}}(f(\bar{x}))$.

Атакующий по перехваченному вектору $\bar{S} = C(D_{\bar{b}}(f(\bar{x})) + \bar{e}$, где $\bar{e} \in F_p^n$ – вектор непреднамеренных ошибок, внесенный каналом связи, может с помощью произвольного декодера кода $RM_p(1,m)$ восстановить $D_{\bar{b}}(f(\bar{x}))$. Затем ему нужно решить задачу нахождения информационного полинома $f(\bar{x}) \in F_p^{(2)}[x_1, x_2, ..., x_m]$ и вектора $\bar{b} \in F_p^m$. Очевидно, что кроме искомых $f(\bar{x})$ и $\bar{b}$ мо-

гут отыскаться и другие значения полинома $\varphi(\bar{x}) \in F_p^{(2)}[x_1, x_2, ..., x_m]$ и вектора $\bar{v} \in F_p^m$, для которых $D_{\bar{b}}(f(\bar{x})) = D_{\bar{v}}(\varphi(\bar{x}))$. Такие значения $(\varphi, \bar{v})$ называют подходящей парой.

Рассмотрим теоретические оценки длин списков подходящих пар, получаемых наблюдателем при различных атаках из [3]. Длина списка в результате однократного перехвата одного канала оценивается в $p^{m+m(m+1)/2}$. При t-кратном перехвате одного канала наблюдатель построит t различных списков из $p^{m+m(m+1)/2}$ подходящих пар. При однократном перехвате из одного канала при известном частичном ключе $\bar{b}$ этого канала наблюдатель получит список из $p^{m(m+1)/2}$ подходящих пар.

3. Программное средство. Для исследования возможностей нелегального наблюдателя в полиномиальной системе РПД сделаем предположение, что наблюдатель перехватил вектор $S = C(D_{\bar{b}}(f(\bar{x})) + \bar{e}$, восстановил из него значение $D_{\bar{b}}(f(\bar{x}))$ и затем пытается подобрать подходящие пары $(\varphi, \bar{v})$. Обратим внимание, что для исследования возможностей наблюдателя нет необходимости реализовывать всю схему целиком, достаточно программного средства, которое позволяет моделировать процесс восстановления данных или ключа наблюдателем системы по перехваченным значениям $D_{\bar{b}}(f(\bar{x}))$.

Рассмотрим необходимый функционал такого программного средства:

а) построение по входным параметрам схемы p и m всех возможных полиномов кольца $F_p^{(2)}[x_1, x_2, ..., x_m]$ и всех их производных $(D_{\bar{b}} f)(\bar{x})$ по направлениям $\bar{b} \in F_p^m$;

б) сохранение построенных полиномов в табличный процессор Excel следующим образом: в верхней строке, начиная со второго столбца, сохраняются полиномы $f(\bar{x}) \in F_p^{(2)}[x_1, x_2, ..., x_m]$, в первом столбце со второй строки содержатся векторы $\bar{b} \in F_p^m$. В основной части таблицы содержатся производные $(D_{\bar{b}_i} f_j)(\bar{x})$, где i и j зависят от текущих строки и столбца. В табл. 1 схематично представлена структура хранения результатов.

Таблица 1

Структура хранения результатов

	$f_1(\bar{x}) \in F_p^{(2)}[x_1, x_2, ..., x_m]$	…	$f_k(\bar{x}) \in F_p^{(2)}[x_1, x_2, ..., x_m]$
$\bar{b}_1 \in F_p^m$	$(D_{\bar{b}_1} f_1)(\bar{x})$	…	$(D_{\bar{b}_1} f_k)(\bar{x})$
…	…	…	…
$\bar{b}_n \in F_p^m$	$(D_{\bar{b}_n} f_1)(\bar{x})$	…	$(D_{\bar{b}_n} f_k)(\bar{x})$

Рассмотрим алгоритм работы программы.

Вход: параметры схемы p и m.

Выход: табл. Excel полиномов $f(\bar{x}) \in F_p^{(2)}[x_1, x_2, ..., x_m]$ и их производных $(D_{\bar{b}} f)(\bar{x})$, $\bar{b} \in F_p^m$.

Шаг 1. Создать массив M длины p^m для записи векторов из $F_p^{p^k}$.

Шаг 2. Создать файл Excel.

Шаг 3. Для каждого $f(\bar{x}) \in F_p^{(2)}[x_1, x_2, ..., x_m]$ выполнить.

Начало цикла для каждого $i = \overline{1, p^k}$, k – размерность кода выполнить.

Шаг 3.1. Генерация полинома $f_i(\bar{x}) \in F_p^{(2)}[x_1, x_2, ..., x_m]$.

Шаг 3.2. Начало цикла для каждого $j = \overline{1, p^m}$ выполнить.

Шаг 3.2.1. Сгенерировать вектор $\bar{b}_j \in F_p^m$.

Шаг 3.2.2. Вычислить производный полином $(D_{\bar{b}_j} f_i)(\bar{x})$.

Шаг 3.2.3. Записать $(D_{\bar{b}_j} f_i)(\bar{x})$ в j-тую позицию массива M.

Шаг 3.3. Вывод элементов массива M в i-ый столбец таблицы Excel.

Шаг 3.4. Очистить массив M.

Конец цикла.

Шаг 4. Сохранить и закрыть файл Excel.

Конец алгоритма.

Программное средство, реализующее описанный алгоритм, построено в среде разработки Visual Studio на языке программирования C++. Исходный программный код реализован в виде одного программного модуля и содержит один класс *RingDifferentation*. Опишем три основных метода программного средства.

Метод *Polynom_generator(intm,intp)* получает на вход p — мощность поля и m — количество переменных. Метод генерирует все возможные полиномы $f(\bar{x}) \in F_p^{(2)}[x_1, x_2, ..., x_m]$.

Метод *Diff(vector<int>polin)* вычисляет для заданного полинома $f_i(\bar{x})$ его производные по всем возможным направлениям $\bar{b}_j \in F_p^m$. На выходе формируется массив M производных вида $(D_{\bar{b}_j} f_i)(\bar{x})$, $j = \overline{1, p^m}$.

Метод Output_Data(vector<vector<int>>differen, vector<int>polin) выводит в необходимые позиции таблицы Excel значения из массива M.

4. Экспериментальное исследование. В работе сделано предположение, что за системой разделенной передачи данных следит нелегальный наблюдатель, цель которого восстановить полностью или частично секретный ключ β и информационные сообщения $f(\bar{x})$, передаваемые по каналам связи. Согласно принятым в криптографии подходам, при оценке стойкости систем защиты данных разделяют атаки на ключ и атаки на данные [11], однако специфика рассматриваемой системы РПД такова, что эти атаки разделить не удается [3]. Будем считать, что нелегальный наблюдатель при перехвате данных из каналов связи умеет определять начало и окончание передаваемых производных векторов, а также у него есть возможность синхронизировать данные, полученные из нескольких линий связи.

Далее рассмотрим несколько атак на систему РПД и оценим результативность нелегального наблюдателя системы. Предположим, что наблюдатель отыскивает подходящие пары методом полного перебора всех возможных полиномов $\varphi(\bar{x}) \in F_p^{(2)}[x_1, x_2, ..., x_m]$ и векторов $\bar{v} \in F_p^m$, а также нахождении тех из них, для которых $D_{\bar{b}}(f(\bar{x})) = D_{\bar{v}}(\varphi(\bar{x}))$, где $D_{\bar{b}}(f(\bar{x}))$ – перехваченное значение.

Полиномы из колец $F_p^{(r)}[x_1, x_2, ..., x_m]$, $r = 1, 2$, содержат k_r коэффициентов, где k_r определяется формулой (3). Следовательно, легко вычислить мощность пространства $F_p^{(r)}[x_1, x_2, ..., x_m]$, $r = 1, 2$, формулой $M_r = p^{k_r}$. Наблюдателю системы РПД для поиска подходящих пар необходимо

рассмотреть $M_2 = p^{k_2}$ полиномов из $F_p^{(2)}[x_1,...,x_m]$ и вычислить производные этих полиномов во всех p^m направлениях линейного пространства F_p^m, т. е. $p^{k_2} p^m = p^{1+2m+m(m+1)/2}$ значений производных может быть вычислено. В табл. 2 указаны некоторые значения параметров схем РПД, которые будут использованы для дальнейших рассуждений.

Таблица 2

Некоторые значения параметров схем РПД, использованных в экспериментах

Основные параметры схемы, p, m	**Мощность пространства**			**Общее число производных** $p^{1+2m+m(m+1)/2}$
	$F_p^{(1)}[x_1,...,x_m]$	$F_p^{(2)}[x_1,...,x_m]$	F_p^m	
p=2, m=3	16	1024	8	8192
p=2, m=4	32	32768	16	524288
p=3, m=2	27	729	9	6561
p=3, m=3	81	59049	27	1594323

Рассмотрим случай системы РПД с параметрами $p=3$ и $m=2$. Для выполнения атаки на ключ и данные методом полного перебора потребуется 6561 раз вычислить значения различных производных (см. табл. 2) и составить таблицу производных, структура которой повторяет табл. 1. После проведения дифференцирования в основной части таблицы производных имеются только полиномы из кольца $F_3^{(1)}[x_1,x_2]$, всего существует 27 таких полиномов. Таким образом, вычисление 6561 производных дает в результате только 27 различных значений. Зафиксируем каждый из 27 полиномов кольца $F_3^{(1)}[x_1,x_2]$ и вычислим, какое количество раз он встречается в каждый строке таблицы. Результат учета встречаемости производных оформлен в виде табл. 3. В этой таблице строки помечены значениями векторов-направлений $\bar{b} = (b_1,b_2) \in F_p^m$, используемых для вычисления производных. Столбцы помечены значениями полиномов из кольца $F_3^{(1)}[x_1,x_2]$. Строки этой таблицы, соответствующие ненулевым векторам $\bar{b}$, содержат одинаковые значения, поэтому таблица представлена частично.

Таблица 3

Результат поиска подходящих пар для системы
с параметрами $p=3$ и $m=2$

	Полиномы $F_3^{(1)}[x_1,x_2]$						
$\bar{b}$	*0*	*1*	*2*	x_1	$2x_1$	…	$2x_1x_2$
(0,0)	729	0	0	0	0	…	0
(0,1)	27	27	27	27	27	…	27
…	…	…	…	…	…	…	…
(2,2)	27	27	27	27	27	…	27

Ненулевое значение $D_{\bar{b}}(f(\bar{x}))$, имеющееся у наблюдателя, встречается в каждой строке, кроме строки, соответствующей $\bar{b} = \bar{0}$, и наблюдатель может построить список из $27 \cdot 8$ подходящих пар $(\varphi,\bar{v})$, таких, что $D_{\bar{b}}(f(\bar{x})) = D_{\bar{v}}(\varphi(\bar{x}))$. Если известно значение частичного ключа $\bar{b}$, то будет получено 27 вариантов значений $f(\bar{x})$. В случае двукратного перехвата из одного канала

связи наблюдатель для каждого из 8 возможных значений частичного ключа $\bar{b} \in F_p^m$ получит 27^2 вариантов $f_1(x)$ и $f_2(x)$. Итого, общий список составит $27^2 \cdot 8$ возможных вариантов исходных сообщений. Без каких-либо знаний об исходном сообщении уменьшить количество подходящих пар наблюдатель не имеет возможности.

Рассмотрим систему РПД с параметрами $p = 3$ и $m = 3$. В ходе выполнения исследования для схемы с этими параметрами была построена таблица, аналогичная табл. 3. Не будем ее приводить в работе из-за ее громоздкости, а также из-за легко описываемой структуры. Строки этой таблицы, соответствующие ненулевым векторам $\bar{b}$, содержат одинаковые значения, в каждой ячейке таблицы для ненулевого значения вектора-направления для дифференцирования $\bar{b} \in F_p^m$ расположено число 729. Следовательно, при однократном перехвате из одной линии связи наблюдатель сможет построить список из $26 \cdot 729$ подходящих пар $(\varphi, \bar{v})$, таких, что $D_{\bar{b}}(f(x)) = D_{\bar{v}}(\varphi(x))$. Если известно значение частичного ключа $\bar{b}$, то будет получено 729 вариантов значений $f(x)$. В случае двукратного перехвата из одного канала связи наблюдатель для каждого из 26 возможных значений частичного ключа $\bar{b} \in F_p^m$ получит по 729^2 вариантов $f_1(\bar{x})$ и $f_2(x)$. Итого, общий список составит $729^2 \cdot 26$ возможных вариантов исходных сообщений.

Кроме приведенных выше примеров, в исследовании были рассмотрены и другие поля Галуа нечетной мощности, например, F_5, F_7, F_9. Во всех случаях были получены таблицы учета встречаемости производных с аналогичным содержанием. Сравнительный анализ длин списков подходящих пар, полученных в экспериментах, а также теоретических оценок из [3] показал следующее:

1) для случая перехвата с известным значением частичного ключа $\bar{b} \in F_p^m$, при $\bar{b} \neq \bar{0}$, длина экспериментально полученного списка подходящих пар полностью согласуются с теоретически вычисленным значением $p^{m(m+1)/2}$ длины списка;

2) в результате однократного перехвата из одного канала длина списка теоретически оценивается в $p^{m+m(m+1)/2}$, эксперименты показали значение $(p^m - 1)p^{m(m+1)/2}$. Различие в результатах возникает из-за вектора-направления $\bar{b} = \bar{0}$ При получении теоретической оценки этот вектор был учтен как любой другой вектор $\bar{b} \in F_p^m$, $\bar{b} \neq \bar{0}$, однако любая производная в нулевом направлении дает нулевой результат. Это же отличие в оценках длины списков подходящих пар сохраняется и при рассмотрении t-кратного перехвата одного канала.

Рассмотрим далее два случая схемы РПД, построенной над бинарным полем Галуа. В работе [3] теоретические оценки для такого случая не получены.

Табл. 4 построена для схемы с параметрами $p = 2$ и $m = 3$, ее содержимое аналогично табл. 3. По данным таблицы видно, что все полиномы, кроме $f(x) = 0$ и $f(x) = 1$, могут появиться только в результате дифференцирования по некоторым направлениям, при этом каждый из них может получиться точно в трех случаях для восьми возможных значений векторов-направлений. При однократном перехвате из одного канала связи наблюдатель сможет определить три возможных вектора-направления и построить список из $16 \cdot 3$ подходящих пар. При однократном перехвате из двух разных каналов значений $D_{\bar{b}_i}(f(\bar{x}))$ и $D_{\bar{b}_j}(f(x))$ или при двукратном перехвате из одного канала значений $D_{\bar{b}_i}(f_1(\bar{x}))$ и $D_{\bar{b}_i}(f_2(x))$ количество возможных векторов-направлений, яв-

ляющихся ключами системы, резко уменьшается, что позволяет сразу восстановить полный ключ системы или частичный ключ, соответствующий одному каналу.

Увеличим параметры системы и рассмотрим случай $p = 2$ и $m = 4$. В этом случае таблица производных имеет структуру, сходную со случаем из табл. 4. Опишем словесно ее содержимое. В каждом столбце таблицы для всех полиномов, кроме $f(\bar{x}) = 0$ и $f(\bar{x}) = 1$, 7 раз встречается число 128 и 9 раз встречается число ноль. При однократном перехвате из одного канала наблюдатель сможет определить 7 возможных значений частичного ключа и построить список из $128 \cdot 7$ подходящих пар. Если наблюдатель при повторном перехвате перехватил $f(\bar{x}) = 0$ или $f(\bar{x}) = 1$, то нелегальный наблюдатель не сможет уменьшить список возможных частичных ключей. При повторном перехвате полинома, отличного от предыдущего, наблюдатель сможет уменьшить количество возможных вариантов частичного ключа. Наблюдателю потребуется от трех до девяти перехватов из одного канала связи, чтобы однозначно определить соответствующий частичный ключ и по 128 возможных значений для полиномов $f_i(\bar{x})$, соответствующих каждому перехвату.

Таблица 4

Результат поиска подходящих пар для системы с параметрами $p = 2$ и $m = 3$

	Полиномы $F_2^{(1)}[x_1, x_2, x_3]$							
$\bar{b}$	0	1	x_1	$1 + x_1$	x_2	$1 + x_2$	…	$1 + x_1 + x_2 + x_3$
(0,0,0)	128						…	
(0,0,1)	16	16			16	16	…	
(0,1,0)	16	16	16	16			…	
(0,1,1)	16	16					…	16
(1,0,0)	16	16	16	16	16	16	…	
(1,0,1)	16	16			16	16	…	16
(1,1,0)	16	16	16	16			…	16
(1,1,1)	16	16					…	

Из экспериментов, проведенных для схемы РПД, определенной над бинарным полем Галуа, видно, что ее стойкость по сравнению со случаями использования схемы над полями Галуа нечетной мощности чрезвычайно понижается.

Заключение. В работе рассмотрена система разделенной передачи данных из [1–2]. Построено программное средство, позволяющее исследовать возможности нелегального пользователя системы по восстановлению данных, полученных из каналов при перехвате. Проведен ряд исследований системы с различными параметрами. В случае полей Галуа нечетной мощности результаты исследования согласуются с оценкой сложности из [3]. В случае бинарных полей Галуа схема разделенной передачи данных не обладает стойкостью к рассмотренным атакам, следовательно, ее использование для обеспечения конфиденциальности передаваемых данных становится нецелесообразным.

Библиографический список

1. Деундяк, В. М. Дифференцирование полиномов нескольких переменных над полями Галуа нечетной мощности и приложения к кодам Рида–Маллера / В. М. Деундяк, Н. С. Могилевская // Вестник Дон. гос. техн. ун-та. — 2018. — Т. 18, № 3. — С. 339–348.

2. Деундяк, В. М. Схема разделенной передачи конфиденциальных данных на основе дифференцирования полиномов нескольких переменных над простыми полями Галуа / В. М. Деундяк, Н. С. Могилевская // Вопросы кибербезопасности. — 2017. — № 5 (24). — С. 64–71.

3. Деундяк, В. М. Стойкость полиномиальной схемы разделенной передачи конфиденциальных данных / В. М. Деундяк, Н. С. Могилевская // Вопросы кибербезопасности. — 2018. — № 4 (28). — С. 38–45.

4. Мищенко, В. А. Ущербные тексты и многоканальная криптография / В. А. Мищенко, Ю. В. Виланский. — Минск : Энциклопедикс, 2007. — 292 с.

5. Тормасов, А. Г. Обеспечение отказоустойчивости в распределенных средах / А. Г. Тормасов, М. А. Хасин, Ю. И. Пахомов // Программирование. — 2001. — Т. 27, № 5. — С. 26.

6. Sharma R., Subramanian D., Srirama S. DAPriv: Decentralized architecture for preserving the privacy of medical data — Режим доступа: arxiv.org/abs/1410.5696 (дата обращения: 10.04.2019)

7. Kong Z, Salah A., Soljanin E. Decentralized Coding Algorithms for Distributed Storage in Wireless Sensor Networks — Режим доступа: arxiv.org/abs/0904.4057 (дата обращения: 10.04.2019)

8. Могилевская, Н. С. О применении порогового разделения данных для организации разделенной передачи на примере метода битовых масок / Н. С. Могилевская // Инженерный вестник Дона. — 2017. — № 2 (45). — 39 с.

9. Могилевская, Н. С. Имитационная модель цифрового канала передачи данных и алгебраические методы помехоустойчивого кодирования / Н. С. Могилевская, Р. В. Кульбикаян, Л. А. Журавлёв // Вестник Дон. гос. техн. ун-та. — 2011. — Т. 11, № 10 (61). — С. 1749–1755.

10. Скляр, Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр. — Москва : Издательский дом «Вильямс», 2003. — 1104 с.

11. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. — Москва : Триумф, 2016. — 816 с.

Об авторах:

Могилевская Надежда Сергеевна, доцент кафедры «Алгебра и дискретная математика» Института механики, математики и компьютерных наук им. Воровича Южного федерального университета (344058, РФ, г. Ростов-на-Дону, ул Мильчакова, 8а), кандидат технических наук, nadezhda.mogilevskaia@yandex.ru

Простяков Павел Павлович, студент кафедры «Алгебра и дискретная математика» Института механики, математики и компьютерных наук им. Воровича Южного федерального университета (344058, РФ, г. Ростов-на-Дону, ул Мильчакова, 8а), pasha-pro2014@yandex.ru