SCIENTIFIC JOURNAL

3(70)/2014

INFORMATSIONNO-UPRAVLIAIUSHCHIE SISTEMY (INFORMATION AND CONTROL SYSTEMS)

REFEREED EDITION

Contact information
The Editorial and Publishing Center, SUAI
67, B. Morskaia, 190000, St. Petersburg, Russia
Website: http://i-us.ru/en, E-mail: ius.spb@gmail.com
Tel.: +7 - 812 494 70 02

The Journal was registered in the Ministry of Press, Broadcasting and Mass Media of the Russian Federation. Registration Certificate JD № 77-12412 from April, 19, 2002. Re-registration in the Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications (ROSKOMNADZOR) due to change of the founder: «Information and Control Systems», Ltd., JD № FS77-49181 from March, 30, 2012.

The journal is distributed by subscription. Subscription can be made in the Editorial and publishing center, SUAI as well as in any post office based on «Rospechat» catalogue:
№ 48060 — annual subscript, № 15385 — semiannual subscript.

Submitted for publication 07.04.14. Passed for printing 17.06.14. Format 60×841/8.
Offset paper. Phototype SchoolBookC. Offset printing.

Layout original is made at the Editorial and Publishing Center, SUAI.
67, B. Morskaia, 190000, St. Petersburg, Russia
Printed from slides at the Editorial and Publishing Center, SUAI.
67, B. Morskaia, 190000, St. Petersburg, Russia

НАУЧНЫЙ ЖУРНАЛ

3(70)/2014

РЕЦЕНЗИРУЕМОЕ ИЗДАНИЕ

ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ

Учредитель
ООО «Информационно-управляющие системы»

Адрес редакции: 190000, Санкт-Петербург,
Б. Морская ул., д. 67, ГУАП, РИЦ
Тел.: (812) 494-70-02, e-mail: ius.spb@gmail.com, сайт: http://i-us.ru

Журнал зарегистрирован в Министерстве РФ по делам печати, телерадиовещания и средств массовых коммуникаций. Свидетельство о регистрации ПИ № 77-12412 от 19 апреля 2002 г. Перерегистрирован в Роскомнадзоре. Свидетельство о регистрации ПИ № ФС77-49181 от 30 марта 2012 г.

Журнал входит в «Перечень ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные научные результаты диссертации на соискание ученой степени доктора и кандидата наук».

Журнал распространяется по подписке. Подписку можно оформить через редакцию, а также в любом отделении связи по каталогу «Роспечать»: № 48060 — годовой индекс, № 15385 — полугодовой индекс.

Сдано в набор 07.04.14. Подписано в печать 17.06.14. Формат 60×84 1/8.
Бумага офсетная. Гарнитура SchoolBookC. Печать офсетная.
Усл. печ. л. 16,0. Уч.-изд. л. 20,1. Тираж 1000 экз. Заказ 258.

Оригинал-макет изготовлен в редакционно-издательском центре ГУАП.
190000, Санкт-Петербург, Б. Морская ул., 67.

Отпечатано с готовых диапозитивов в редакционно-издательском центре ГУАП.
190000, Санкт-Петербург, Б. Морская ул., 67.

УДК 004.056.2

ОБ ОБНАРУЖЕНИИ АЛГЕБРАИЧЕСКИХ МАНИПУЛЯЦИЙ С ПОМОЩЬЮ ОПЕРАЦИИ УМНОЖЕНИЯ

М. О. Алексеев[a, 1], *ведущий программист*
[a]*Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, РФ*

Постановка проблемы: *известно, что реализации криптографических алгоритмов подвержены атакам по сторонним каналам. Одной из наиболее эффективных является атака по привнесенным помехам с последующим линейным или дифференциальным анализом ошибок. Атака заключается в нестандартном воздействии на криптографическое устройство в целях внесения помех в его работу. Модель такой атаки получила название алгебраической манипуляции. Целью работы являются исследование и развитие одного из методов защиты от рассматриваемой атаки.* ***Результаты:*** *исследуемая контрмера заключается в построении нелинейного помехоустойчивого кода, кодирующей функцией которого выбирается операция умножения в конечном поле. Разработаны и описаны два варианта модификации кодовой конструкции, основанные на расширении случайной величины и на разбиении информационного сообщения. Данные модификации позволяют варьировать такие параметры кода, как скорость и вероятность обнаружения атаки, во многих случаях уменьшая избыточность кода. При этом вторая модификация также позволяет снизить аппаратные затраты на реализацию кодека.* ***Практическая значимость:*** *полученная гибкая и просто реализуемая кодовая конструкция обнаруживает любую ошибку в передаваемой информации с заданной вероятностью даже при условии коррелированности значения ошибки и кодируемых данных.*

Ключевые слова *— помехоустойчивые коды, нелинейные коды, атаки по сторонним каналам, алгебраические манипуляции, умножение в поле.*

Введение

Использование линейных помехоустойчивых кодов является эффективным методом борьбы с искажениями, возникающими в канале [1]. Естественным требованием для обеспечения высокого уровня защищенности от помех является условие согласованности параметров используемого кода с характеристиками канала. Если же характеристики канала не могут быть точно определены (например, для каналов со случайной структурой), кодирование линейным кодом в общем случае является неэффективным.

Случайная структура канала может быть обусловлена многими факторами, имеющими как естественную, так и искусственную природу. Примерами естественных воздействий, приводящих к изменению характера возникающих ошибок, являются, например, случайное изменение состояния канала, накопление статического заряда, воздействие заряженных частиц, износ оборудования. Искусственные методы изменения характеристик канала часто заключаются в нестандартном физическом воздействии на канал. Примерами таких воздействий являются электромагнитное излучение, когерентное излучение (например, лазер), подавление и зашумление данных [2].

Уязвимость классических методов защиты со стороны каналов со случайной структурой может быть использована злоумышленником. В частности, преобразование исходного канала, с которым согласована информационная система, в канал со случайной структурой может быть осуществлено с помощью атак по сторонним каналам, называемых атаками по привнесенным ошибкам [2, 3]. Целью данного типа атак является вычисление секретных параметров систем обработки данных, например ключей шифрования. Как правило, атаки состоят из двух этапов: атакуемое устройство (канал) подвергается нестандартному внешнему физическому воздействию, после чего производится анализ результатов работы устройства. На основе полученных данных злоумышленник зачастую способен либо напрямую восстановить значение секретных ключей, либо заметно уменьшить мощность перебора.

Для работы с каналами со случайной структурой были разработаны классы нелинейных кодов — надежные коды и коды, обнаруживающие алгебраические манипуляции [4–7]. Требование нелинейности обусловлено тем, что у любого q-ичного линейного кода существует как минимум $q^k - 1$ необнаруживаемых ошибок, соответствующих кодовым словам, где k — размерность кода. Это приводит к ситуации, когда, имея возможность определенным образом воздействовать на канал, злоумышленник способен провоцировать такое его состояние (и возникающую конфигурацию ошибок), при котором ошибки и атаки не могут быть обнаружены. Существуют классы нелинейных кодов, которые не имеют необнаруживаемых ошибок, любая ошибка обнаруживается с ненулевой вероятностью.

Надежные нелинейные коды предназначены для обнаружения ошибок (как естественного, так

[1] Научный руководитель — доктор технических наук, профессор *Е. Т. Мирончиков*.

и искусственного происхождения) при условии, что злоумышленник (источник ошибок в канале) не обладает знанием о передаваемых данных [4, 5]. Надежные коды гарантируют заданную ненулевую вероятность обнаружения любой конфигурации ошибок.

Нелинейные коды, обнаруживающие алгебраические манипуляции, позволяют обнаруживать любые ошибки с заданной вероятностью даже при условии, что злоумышленник обладает знанием о передаваемой информации [4, 6]. Это обеспечивается за счет рандомизации результата кодирования.

Защищенные коды, обнаруживающие алгебраические манипуляции

Рассмотрим следующую модель атаки [6, 7]:

— злоумышленник способен контролировать значение ошибок, возникающих в канале;

— ошибка аддитивна;

— злоумышленник способен контролировать передаваемое информационное сообщение.

Такая модель атаки называется сильной. Сильной модели атаки соответствует атака, при которой злоумышленник не только способен генерировать заданную ошибку, но и имеет возможность контролировать значение кодируемого сообщения. В этой ситуации злоумышленник, зная информационное сообщение, вычисляет получаемое кодовое слово, после чего выбирает значение ошибки, при внедрении которой текущее кодовое слово преобразуется в другое кодовое слово. Даже надежные нелинейные коды не могут гарантировать защиту от такой модели атаки.

Для защиты от сильных атак были предложены защищенные коды, обнаруживающие алгебраические манипуляции (strongly secure algebraic manipulation detection codes, strongly secure AMD codes). Для краткости будем называть их AMD-кодами.

Очевидно, что процесс кодирования должен иметь недетерминированный характер. В противном случае злоумышленник гарантированно вносит необнаруживаемую ошибку. Естественным путем решения этой проблемы является привнесение случайности в процесс кодирования, когда каждому сообщению соответствует множество кодовых слов, а выбор конкретного кодового слова из этого множества определяется некоторой случайной величиной, которую злоумышленник не способен контролировать. В этом случае, зная информационное сообщение, злоумышленник способен вычислить набор кодовых слов, одно из которых, в зависимости от значения случайной величины, может стать результатом кодирования. Далее атакующий выбирает значение ошибки, которое имеет наименьшую вероятность обнаружения для заданного набора возможных кодовых слов. Другими словами, выбирается такая ошибка, которая не будет обнаружена при наибольшем количестве значений случайной величины для заданного исходного сообщения.

Для построения AMD-кодов используются различные математические объекты: коды аутентификации, разностные структуры, помехоустойчивые коды [4, 7]. Одной из наиболее исследованных и эффективных конструкций AMD-кодов является конструкция, основанная на полиномах. Наиболее полно этот класс AMD-кодов описан в работе [6], где значительная часть предлагаемых конструкций являются оптимальными в смысле вероятности обнаружения ошибки.

Далее будут рассматриваться систематические коды над полями характеристики 2. Кодовые слова систематического AMD-кода представляют собой конкатенацию информационного сообщения $y \in GF(2^k)$, некоторой случайной величины $x \in GF(2^m)$ и значения нелинейной функции $f(y, x) \in GF(2^r)$. Сами AMD-коды определяются как коды, для которых не существует такой конфигурации ошибок

$$\mathbf{e} = (e_y \in GF(2^k), e_x \in GF(2^m), e_f \in GF(2^r))$$

и такого значения y, при возникновении которых равенство

$$f(y, x) + e_f = f(y + e_y, x + e_x)$$

выполнится при всех возможных значениях x. Данное равенство называется уравнением маскирования ошибки (УМО). Легко заметить, что проверка выполнения этого равенства является аналогом вычисления синдрома принятого слова линейного кода.

Способность AMD-кода обнаруживать ошибки напрямую зависит от вида его УМО: максимальное количество решений УМО относительно x среди всех возможных комбинаций y, e_x, e_y, e_f и будет максимальным количеством необнаруживаемых кодом ошибок. Вероятность обнаружения ошибки ограничена снизу выражением

$$P_{\text{det}} \geq 1 - \max_{y,e} \frac{|\{x : f(y,x) + e_f = f(y + e_y, x + e_x)\}|}{|\{x\}|}, \quad (1)$$

которое непосредственно следует из сценария сильной атаки.

Код на основе умножения

Одной из конструкций AMD-кодов является конструкция, основанная на умножении в конечном поле [8]. Кодовое слово такого AMD-кода выглядит следующим образом:

$$(y \,|\, x \,|\, f(x, y) = xy),$$

где x, y, $f(y, x) \in GF(2^k)$ (т. е. $m = r = k$), операция умножения выполняется в поле $GF(2^k)$, а символом «|» обозначена операция конкатенации. УМО такого кода выглядит следующим образом:

$$xy + e_f = (x + e_x)(y + e_y).$$

Легко заметить, что максимальное количество решений данного УМО относительно x при фиксированных y и **e** равно единице, так как

$$e_f = xe_y + ye_x + e_xe_y, \quad x = \frac{e_f + ye_x + e_xe_y}{e_y}.$$

Правая часть последнего выражения при фиксированной величине ошибки представляет собой константу; если случайная величина x равна этой константе, то привнесенная ошибка $e = (e_y, e_x, e_f)$ останется необнаруженной. Случайная величина x распределена равномерно, следовательно, вероятность обнаружения любой ошибки e при фиксированном y равна

$$P_{\text{det}} = 1 - \frac{|\{x : f(y, x) + e_f = f(y + e_y, x + e_x)\}|}{|\{x\}|} = 1 - \frac{1}{2^m} = 1 - 2^{-m} = 1 - 2^{-k}.$$

Тут необходимо обратить внимание на то, что данный код неприменим при $e_y = 0$, что накладывает ограничение на множество обнаруживаемых ошибок. Кроме того, это противоречит определению AMD-кодов, которое дано в работе [6]. Однако стоит отметить, что в некоторых других работах (например, в [7]) AMD-код определяется как код, который гарантированно обнаруживает ошибки только в информационной части кодового слова, т. е. когда $e_y \neq 0$. Данное определение обусловлено требованиями многих практических задач, в которых важна целостность только информационной части y кодового слова [7]. Далее будем рассматривать лишь вероятность обнаружения ошибки e, у которой $e_y \neq 0$.

Необходимо указать, что о целесообразности использования умножения в поле для обнаружения ошибок в каналах со случайной структурой писали еще В. И. Коржик и Л. М. Финк [8]. Предложенный ими универсальный метод стохастического кодирования для каналов со случайной структурой обеспечивает более низкую вероятность обнаружения ошибок. Кроме того, в их модели подразумевается, что приемник и передатчик имеют точно синхронизированную случайную величину x, что ограничивает область применения данного метода кодирования.

Использование AMD-кода, основанного на умножении, позволяет обеспечить максимально возможную вероятность обнаружения ошибки даже при условии искажения случайной величины. Случайная величина x является частью кодового слова, передается по каналу и не требует дополнительной синхронизации передатчика и приемника.

Основным недостатком данной кодовой конструкции является отсутствие гибкости при выборе параметров кода [7]. Фактически, размер информационного сообщения k полностью определяет длину кода $n = 3k$, размер случайной величины k бит, а также вероятность обнаружения ошибки $P_{\text{det}} = 1 - 1/2^k$. Ниже будут представлены два варианта модификаций данной конструкции, которые предоставляют большую гибкость при выборе параметров кода.

Модификация на основе расширения случайной величины

Наиболее естественным методом модификации описанной конструкции является использование случайной величины из меньшего поля Галуа, т. е. $x \in GF(2^m)$, $m < k$. Для выполнения умножения формируется вектор $\bar{x} \in GF(2^k)$ путем дополнения двоичного представления элемента x $k - m$ нулями, т. е. выполняется отображение $g(x) = \bar{x}$, $\bar{\mathbf{x}} = (0, \ldots, 0, x_{m-1}, \ldots, x_0)$, где x_{m-1}, ..., x_0 есть двоичное представление элемента поля x. Полученный элемент большего поля $\bar{x} \in GF(2^k)$ используется для выполнения операции кодирования согласно оригинальной конструкции. Кодовое слово выглядит следующим образом:

$$\mathbf{c} = (y \in GF(2^k) \,|\, x \in GF(2^m) \,|\, \bar{x} \cdot y \in GF(2^k)),$$

т. е. длина кода уменьшается на $k - m$ бит.

На приемной стороне перед проверкой УМО полученная из канала случайная величина $x + e_x \in GF(2^m)$ еще раз подвергается отображению $g(x + e_x) = \overline{x + e_x}$.

Теорема 1. Вероятность обнаружения сильной атаки ограничена снизу выражением

$$P_{\text{det}} \geq 1 - 2^{-m}.$$

Доказательство: Рассмотрим формулу (1). Мощность множества значений случайной величины x, стоящая в знаменателе дроби, равна 2^m. Необходимо определить значение числителя дроби из (1). Легко заметить, что для данной модификации исходной кодовой конструкции числитель дроби приобретает вид

$$|\{x : f(y, \bar{x}) + e_f = f(y + e_y, \overline{x + e_x}),\ g(x) = \bar{x}\}| = |\{\bar{x} : f(y, \bar{x}) + e_f = f(y + e_y, \overline{x + e_x}),\ \exists g^{-1}(\bar{x})\}|$$

т. е. добавляется условие, что для получаемого решения УМО должен существовать прообраз

среди $x \in GF(2^m)$. Дополнительное ограничение на мощность множества приводит к тому, что обнаруживающая способность кода становится неравномерной. Если для оригинальной конструкции значение числителя было равно 1 для всех возможных y и $e \neq 0$, то при данной модификации некоторая часть комбинаций y и $e \neq 0$ приведет к решениям УМО, которые не имеют прообраза относительно отображения $g(x)$, т. е. значение числителя будет равно 0. Таким образом, часть ошибок будет обнаруживаться с вероятностью $P_{\text{det}}(\mathbf{e}) = 1 - 0/2^m = 1$, в то время как остальные — с $P_{\text{det}}(\mathbf{e}) = 1 - 1/2^m = 1 - 2^{-m}$, где через $P_{\text{det}}(\mathbf{e})$ обозначена вероятность обнаружения конкретной ошибки $\mathbf{e}$ при сильной атаке.

Таким образом, вероятность обнаружения сильной атаки для данной кодовой конструкции $P_{\text{det}} \geq 1 - 2^{-m}$.

Вывод по конструкции. Как видно, данная модификация кодовой конструкции AMD-кодов, основанной на умножении в поле, предоставляет возможность гибкого выбора длины кода и соответствующей вероятности обнаружения сильных атак. Зависимость вероятности обнаружения сильной атаки от размера случайной величины x аналогична оригинальной конструкции. Аппаратная сложность реализации данной модификации соответствует сложности оригинальной кодовой конструкции.

Модификация на основе разбиения информационного сообщения

Вторым вариантом модификации оригинальной кодовой конструкции является следующий: пусть $k = mu$ (в противном случае либо уменьшается разрядность m случайной величины x, либо размер k информационного вектора y увеличивается до необходимого значения за счет добавления, например, нулей). Далее информационный вектор делится на u частей по m бит: $\mathbf{y} = (y_1|y_2|...|y_u)$, где $y_i \in GF(2^m)$, $i = 1, ..., u$. Каждый y_i на основе случайной величины x подвергается процедуре кодирования согласно оригинальной конструкции, т. е. получаем набор из u кодовых слов:

$$\mathbf{c}_i = (y_i \in GF(2^m) \,|\, x \in GF(2^m) \,|\, y_i \cdot x \in GF(2^m)), \quad i = 1, \ldots, u,$$

т. е. выполняется u процедур кодирования сообщений y_i на основе фиксированной случайной величины x. Далее полученные промежуточные кодовые слова c_i объединяются в одно слово следующим образом:

$$\mathbf{c} = (y \,|\, x \,|\, f(x,y)),$$
$$\mathbf{c} = (y_1 \,|\, y_2 \,|\, \ldots \,|\, y_u \,|\, x \,|\, y_1 \cdot x \,|\, y_2 \cdot x \,|\, \ldots \,|\, y_u \cdot x).$$

Полученное кодовое слово имеет длину $n = k + m + k = 2k + m$. На приемнике данное кодовое слово раскладывается в u кодовых слов

$$\mathbf{c}_i + \mathbf{e}_i = (y_i + e_{y_i} \,|\, x + e_x \,|\, y_i \cdot x + e_{f_i}),\ i = 1, \ldots, u,$$

после чего выполняется u проверок их УМО. При обнаружении ошибки хотя бы в одном кодовом слове весь набор $\mathbf{y} = (y_1|y_2|...|y_u)$ признается ошибочным. Рассмотрим вероятность обнаружения сильных атак с помощью данной модификации AMD-кода.

Теорема 2. Вероятность обнаружения сильной атаки равна $P_{\text{det}} \geq 1 - 2^{-m}$.

Доказательство: Очевидно, что чем больше блоков y_i (и, соответственно, кодовых слов c_i) подвергается атаке, тем меньше вероятность того, что ошибка не будет выявлена (предполагается, что вероятность успешной атаки меньше единицы). Таким образом, с позиции злоумышленника наиболее разумно атаковать один из u блоков y_i. При этом вероятность успеха атаки будет максимальна. Рассмотрим эту вероятность, так как именно она определяет нижнюю границу P_{det}.

Атаку одного из блоков y_i можно рассматривать как атаку одного из кодовых слов оригинальной конструкции с параметрами $y \in GF(2^m)$, $x \in GF(2^m)$, $f(y, x) \in GF(2^m)$, $n = 3m$. Получаем, что вероятность обнаружения сильной атаки одного блока $P_{\text{det}} = 1 - 2^{-m}$. Отсюда вероятность обнаружения сильной атаки кодового слова ограничена снизу:

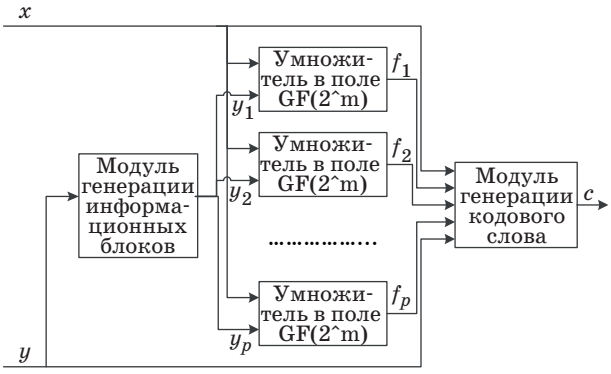
$$P_{\text{det}} \geq 1 - 2^{-m}.$$

Необходимо отметить, что тот факт, что все u кодовых слов c_i получены на основе одной и той же случайной величины x, не может быть использован для успешной атаки кодового слова $\mathbf{c}$ при данном методе декодирования. Если бы решение о наличии ошибок принималось независимо на уровне каждого блока, а не на уровне целого слова, то в этом случае злоумышленник был бы способен проводить атаку с более высокой вероятностью успеха. Для этого он бы для каждого из $\mathbf{c}_i$ случайно выбирал некоторые неповторяющиеся числа $\widetilde{x_i} \in GF(2^m)$, которые считал бы соответствующим значению x. Исходя из $\widetilde{x_i}$ рассчитывались бы такие значения ошибок $\mathbf{e}_i$, чтобы выполнялось УМО. Таким образом, злоумышленник смог бы перебрать u возможных значений случайной величины. В этом случае вероятность успешного внедрения ошибки в один из u блоков (т. е. успешная атака кодового слова $\mathbf{c}$ при таком методе декодирования) равнялась бы $P_{\text{undet}} = u/2^m$ при $u < 2^m$ и $P_{\text{undet}} = 1$ при $u \geq 2^m$. Соответственно, вероятность обнаружения ошиб-

ки на уровне кодового слова при $u < 2^m$ была бы равна $P_{\text{det}} = 1 - u/2^m$.

Вывод по конструкции. Данная модификация позволяет достигнуть тех же характеристик, что и первая модификация. Аппаратная реализация умножения в конечном поле имеет квадратичную зависимость от степени расширения поля. Благодаря этому данная модификация позволяет значительно снизить сложность кодека за счет того, что умножение вычисляется в меньшем поле. Схема одного из вариантов реализации кодера приведена на рисунке.

На схеме изображено p умножителей в поле $GF(2^m)$. Их количество может варьироваться от 1 до u в зависимости от требуемой производительности. При $p < u$ умножители будут использоваться повторно для различных y_i, что приведет к увеличению временных затрат кодирования. При $p = u$ сложность реализации кодера будет максимальна и составит порядка $uO(m^2)$, в то время как в других конструкциях, где умножение выполняется в $GF(2^k)$, она имеет порядок $O(k^2)$, что сопоставимо со сложностью $u^2O(m^2)$ данной модификации.



■ Общая схема кодера для модификации AMD-кода, основанного на умножении

Заключение

В данной работе описан класс AMD-кодов, основанный на умножении в конечном поле. Приведена вероятность обнаружения сильных атак с помощью данного кода. Предложены две модификации этой конструкции, которые обеспечивают гибкость при выборе характеристик кода за счет варьирования размера случайной части в кодовом слове. Вероятность обнаружения сильной атаки для обеих модификаций имеет такую же зависимость от размера случайной величины, как и вероятность для оригинальной конструкции. Аппаратная сложность реализации второй модификации может быть значительно уменьшена за счет повторного использования имеющихся умножителей.

Литература

1. **MacWilliams J., Sloane N. J. A.** The Theory of Error-Correcting Codes. — Amsterdam: North-Holland, 1977. — 762 p.
2. **Zhou Y., Feng D.** Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing. http://eprint.iacr.org/2005/388.pdf (дата обращения: 07.04.2014).
3. **Chen C. N., Yen S. M.** Differential Fault Analysis on AES Key Schedule and Some Countermeasures // Proc. of the 8th Australasian Conf., ACISP 2003, Wollongong, Australia, July 9–11, 2003. P. 118–129. DOI:10.1007/3-540-45067-X_11
4. **Jongsma E.** Algebraic Manipulation Detection Codes. Bachelorscriptie, Mathematisch Instituut, Universiteit Leiden, 6 maart 2008. https://www.math.leidenuniv.nl/scripties/JongsmaBachelor.pdf (дата обращения: 07.04.2014).
5. **Akdemir K. D., Wang Z., Karpovsky M. G., Sunar B.** Design of Cryptographic Devices Resilient to Fault Injection Attacks Using Nonlinear Robust Codes// Fault Analysis in Cryptography/Ed. M. Joye. — Springer, 2011. — P. 171–200.
6. **Wang Z., Karpovsky M. G.** Algebraic Manipulation Detection Codes and Their Application for Design of Secure Cryptographic Devices // Proc. of Intern. Symp. on On-Line Testing (IOLTS), Athens, July 13–15, 2011. P. 234–239. DOI:10.1109/IOLTS.2011.5994535.
7. **Cramer R., Dodis Y., Fehr S., Padro C., Wichs D.** Detection of Algebraic Manipulation with Applications to Robust Secret Sharing and Fuzzy Extractors // Proc. of the Theory and Applications of Cryptographic Techniques 27th Annual Intern. Conf. on Advances in Cryptology, ser. EUROCRYPT'08, 2008. P. 471–488.
8. **Финк Л. М., Коржик В. И.** Помехоустойчивое кодирование дискретных сообщений в каналах со случайной структурой. — М.: Связь, 1975. — 272 с.

UDC 004.056.2

On the Detection of Algebraic Manipulations by Means of Multiplication Operation

Alekseev M. O.[a], Lead Programmer, alexeev@vu.spb.ru
[a]Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation

Purpose: It is well known that implementations of cryptographic algorithms are subject to side-channel attacks. One of the most effective attacks is a fault-injection attack followed by simple or differential fault. The attack involves a non-standard impact on a cryptographic device in order to inject faults in its operation. A model of the attack is called an algebraic manipulation. The goal of this paper is to study and to develop a countermeasure against this attack. **Results:** The countermeasure under consideration implies constructing a nonlinear error-control code which encoding function is a multiplication operation in a Galois field. There have been developed and described two modifications of a code structure based on extension of a random value and on information message splitting. These modifications allow varying such parameters as a code rate and an error detection probability, in many cases it leads to decrease of code redundancy. At the same time the second modification also tends to decrease hardware overheads of codec implementation. **Practical relevance:** Therefore, there has been obtained a flexible and easily implementable code structure which detects any error of transferred information with fixed probability even when an error value and coded data are correlated.

Keywords – Error Control Codes, Nonlinear Codes, Side-Channel Attacks, Algebraic Manipulations, Multiplication in Galois Field.

References

1. MacWilliams J., Sloane N. J. A. *The Theory of Error-Correcting Codes*. Amsterdam, North-Holland, 1977. 762 p.
2. Zhou Y., Feng D. *Side-Channel Attacks: Ten Years After its Publication and the Impacts on Cryptographic Module Security Testing*. Available at: http://eprint.iacr.org/2005/388.pdf (accessed 7 April 2014).
3. Chen C. N., Yen S. M. Differential Fault Analysis on AES Key Schedule and Some Countermeasures. *Proc. of the 8th Australasian Conf., ACISP 2003*, Wollongong, Australia, July 9–11, 2003, pp. 118–129. DOI:10.1007/3-540-45067-X_11
4. Jongsma E. *Algebraic Manipulation Detection Codes*. Bachelorscriptie, Mathematisch Instituut, Universiteit Leiden, 6 maart 2008. Available at: https://www.math.leidenuniv.nl/scripties/JongsmaBachelor.pdf (accessed 7 April 2014).
5. Akdemir K. D., Wang Z., Karpovsky M. G., Sunar B. Design of Cryptographic Devices Resilient to Fault Injection Attacks Using Nonlinear Robust Codes. *Fault Analysis in Cryptography*. M. Joye Ed. Springer, 2011. P. 171–200.
6. Wang Z., Karpovsky M. G. Algebraic Manipulation Detection Codes and Their Application for Design of Secure Cryptographic Devices. *Proc. of Intern. Symp. on On-Line Testing (IOLTS)*, Athens, July 13–15, 2011, pp. 234–239. DOI:10.1109/IOLTS.2011.5994535
7. Cramer R., Dodis Y., Fehr S., Padro C., Wichs D. Detection of Algebraic Manipulation with Applications to Robust Secret Sharing and Fuzzy Extractors. *Proc. of the Theory and Applications of Cryptographic Techniques 27th Annual Intern. Conf. on Advances in Cryptology, ser. EUROCRYPT'08*, 2008, pp. 471–488.
8. Fink L. M., Korzhik V. I. *Pomekhoustoichivoe kodirovanie diskretnykh soobshchenii v kanalakh so sluchainoi strukturoi* [Error Correcting Coding of Discrete Messages in Channels with Random Structure]. Moscow, Sviaz' Publ., 1975. 272 p. (In Russian).