4. Мак-Вильямс Ф., Слоэн Н. Теория кодов, исправляющих ошибки / Пер. с англ. под ред. Л.А. Басалыго.–М:Связь, 1979. – 746 с.

5. Урбанович П.П., Романенко Д.М. Свойства и алгоритмы аппаратной реализации нового вида итеративных кодов для систем памяти // Новые информационные технологии: Третья международная конференция NITE'2000. Т. 2. – Мн.: БГЭУ, 2000. – С. 159–164.

УДК 621.3.049.77

А.И. Галабурда, аспирант

МОДЕЛИРОВАНИЕ ПАРАМЕТРОВ НАДЕЖНОСТИ УСТРОЙСТВ КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ ИНФОРМАЦИИ

The main idea of this article – to estimate failure effect of symmetric data encryption algorithms hardware. Were established the most error prone blocks of block chipper algorithms. New methods of improvements of chipper blocks are suggested to enhance stability.

Широкое применение компьютерных технологий в автоматизированных системах обработки информации и управления привело к обострению проблемы защиты информации, циркулирующей в компьютерных системах, от несанкционированного доступа. Радикальное решение проблемы защиты информации может быть получено только на базе использования криптографических методов. При внедрении оборудования, реализующего алгоритмы криптографического преобразования информации, встает вопрос его отказоустойчивости. Данной проблеме и посвящена эта статья.

Сложность схем, разнообразие видов отказов приводят к тому, что аналитические методы расчета надежности схем криптографического преобразования информации обеспечивают лишь приближенную оценку. Метод статистического моделирования надежности позволяет при достаточной длительности моделирования получить более точную, по сравнению с аналитическими методами, оценку показателей надежности с помощью более точных моделей отказов.

Построим дескриптивную модель криптоалгоритма ГОСТ 28147-89 и проанализируем один из вариантов его аппаратной реализации на предмет устойчивости к сбоям оборудования. Сбои оборудования являются следствием сложных физических процессов, происходящих в аппаратуре преобразования данных, а именно в таких компонентах криптосхем, как логические, арифметические элементы, элементы памяти и др., могут появляться [1] статистически независимые отказы и сбои. Следствием влияния сбоев и отказов в криптографических схемах на достоверность преобразуемой информации будем считать ошибки. Структурная схема простейшего устройства, реализующего шифрование информации в режим простой замены, состоит из следующих блоков:

- два 32-разрядных накопителя N_1 и N_2;
- ключевое запоминающее устройство, состоящее из восьми 32-разрядных накопителей;
- 32-разрядный сумматор по модулю 2^{32};
- 32-разрядный сумматор по модулю 2;
- модуль циклического сдвига на одиннадцать шагов в сторону старшего разряда;
- блок подстановки.

Криптографический алгоритм ГОСТ является блочным. Это означает, что данные для шифрования разбиваются на блоки, каждый из которых в дальнейшем подвергается многократным преобразованиям. Рассмотрим алгоритм шифрования блока данных. Блок данных T=(a_1, a_2, …, a_{32}, b_1, b_2, …, b_{32}), состоящий из 64 бит, разбивается на два 32-битных блока. Далее производится ввод информации в накопители N_1 и N_2 таким образом, что значение a_1 вводится в 1-й разряд N_1, a_2 – во 2-й и т.д., а значение b_1 вводится в 1-й разряд N_2, b_2 –во 2-й и т.д. В результате получаем состояние (a_{32}, a_{31} ,…, a_2, a_1) накопителя N_1 и (b_{32}, b_{31} ,…, b_2, b_1) накопителя N_2. Алгоритм зашифровывания 64-разрядного блока открытых данных в режиме простой замены состоит из 32-х циклов. В первом цикле начальное заполнение накопителя N_1 суммируется в сумматоре CM_1 с заполнением накопителя X_0(ключевая информация), при этом содержимое накопителя сохраняется. Результат суммирования преобразуется в блоке подстановки, и полученный вектор поступает на вход регистра, где циклически сдвигается на 11 разрядов в сторону старших разрядов. Результат сдвига суммируется поразрядно по модулю 2 с заполнением накопителя N_2. Полученный в CM_2 результат записывается в N_1, при этом старое заполнение N_1 переписывается в N_2. На этом первый цикл заканчивается. Последующие циклы осуществляются аналогично.

Отдельно следует упомянуть блок замены. Блок состоит из 8-ми составляющих блоков с памятью на 64 бита каждый. Поступающий на блок подстановки 32-разрядный вектор данных разбивается на 8 блоков по 4 бита. Каждый из этих блоков преобразуется соответствующим узлом замены, представляющим собой матрицу из 16 4-битовых строк. Входной вектор определяет адрес строки матрицы, а содержимое строки является выходным вектором. Далее эти выходные вектора последовательно объединяются в 32- разрядный вектор.

Проанализируем работу данной логической схемы на предмет устойчивости к ошибкам. Будем рассматривать ошибки в следующих блоках схемы: сумматор по модулю2^{32}; блок подстановки; блок циклического сдвига; сумматор по модулю 2.

При рассмотрении сумматора по модулю 2^{32} необходимо заметить, что данные могут поступить с искаженными битами или даже целыми группами битов, т.к. данные хранятся в накопителях, а накопители, в свою очередь, могут не содержать механизмов коррекции ошибок. Также сбой может произойти в самом сумматоре. Он называется сумматором с переносом, т.е. если результат суммы больше 2^{32}, то применяется формула результат-2^{32} . Количество искаженных битов после операции суммирования будет зависеть от положения бита ошибки в 32-битном слове. В самом худшем случае, если бит ошибки находится в младших разрядах, может произойти искажение всех битов 32-битного блока.

Блок подстановки чрезвычайно нестоек к возможным ошибкам ввиду того, что изменение любого бита в 4-битовом блоке повлечет выемку результата подстановки из другой строки. Что в общем случае приведет к замене всего 4-битового блока неверными значениями. Следует, однако, заметить, что в 10% случаев это не приведет к потере правильных данных [2]. Данные сведения подтверждаются требованиями к узлам подстановки, т.к. одним из основных критериев является обеспечение размножения ошибок. Любой блок подстановки должен быть составлен таким образом, чтобы изменение одного бита на входе приводило к изменению на выходе, по крайней мере, двух битов [2].

В блоке циклического сдвига сдвиг на неверную величину приведет к полной потере информации в блоке данных.

В сумматоре по модулю 2 ошибка в любом бите затрагивает лишь бит результата в соответствующем разряде, т.к. в данной операции нет переноса.

Анализируя данные по отказоустойчивости, следует заметить, что любые незначительные однобитовые ошибки будут впоследствии многократно размножены размешивающими преобразованиями. Так, например, ошибка в блоке подстановки, приводящая к потере четырех бит информации, приведет при циклическом сдвиге на нечетную величину и на следующей операции замены к потере 8-ми битов информации. И это не учитывая влияние операций сложения. Таким образом, операции рассеивания (распространение влияния одного символа блока на все последующие) и перемешивания (операция разрушения статистических характеристик блока), примененные многократно, одновременно с шифрующими действиями способствуют распространению ошибок.

Для анализа отказоустойчивости криптосхемы алгоритма ГОСТ была разработана программная модель этого алгоритма, основанная на запоминании информационных последствий отказов. Причем в данной модели объекты соответствуют основным блокам криптографических преобразований. Кроме того, в модели присутствует объект «Ошибка», который управляет распределением ошибок в блоках.

В результате работы программы моделировался момент возникновения одиночной ошибки в блоках криптоалгоритма и фиксировалось влияние ошибки на результат. Следует заметить, что под ошибками в регистре сдвига понималась ошибка в единичном бите, которая не влекла изменения в соседних битах. В таблице представлены данные для криптосхемы, составленной из различных элементов, т.е. собранной не на одном кристалле. Полученные результаты приведены в таблице.

Таблица

Количество дефектных битов на выходе криптоалгоритма

Итерация	Блок алгоритма ГОСТ							
	Режим шифрования				Режим расшифровывания			
	Сумматор по мод. 32	Блок подстановки	Блок циклического сдвига	Сумматор по мод. 2	Сумматор по мод. 32	Блок подстановки	Блок циклического сдвига	Сумматор по мод. 2
1	2,61	2,09	1	32,03	32,02	31,95	32,08	32,05
2	6,47	5,39	3,51	31,97	31,95	31,94	32,01	32
3	11,24	9,78	7,37	32,06	31,96	31,99	31,93	31,94
4	16,53	14,92	11,96	31,98	31,98	32	32,06	31,98
5	22,31	21,07	18,01	32,04	32,05	31,91	32,02	32,02
6	27,86	26,89	24,07	31,95	32	32,03	31,97	31,93
7	30,34	29,87	28,64	32,03	31,95	32,07	32,04	31,98
8	31,51	31,33	30,84	31,99	32,04	32,05	32,03	32,02
31	31,87	31,92	31,91	31,97	6,27	5,4	3,57	32,04
32	31,96	32,04	32,04	31,99	2,48	2,11	1	32,07

В среднем после 6 итераций количество ошибок в результате преобразований равно половине всего количества битов информационного слова. Ошибки сумматора по модулю 2 вообще не зависят от итерации. Таким образом, можно с уверенностью сказать, что возникновение ошибки в любом блоке информации будет иметь катастрофические последствия для целостности информации. Исследования проводились с использованием алгоритма ГОСТ в режиме формирования независимых блоков инфор-

мации. При использовании режима гаммирования количество искаженных бит, в случае возникновения ошибки в блоке данных, будет около 50%. В среднем после шести итераций количество ошибок в результате(количествово битов, не совпадающих с правильным результатом) преобразований равно половине всего количества битов информационного слова. Ошибки сумматора по модулю 2 вробще не зависят от итерации. Примем вероятность отказов равной $10 \cdot e^{-4}$ [3]. Прировняв элементы устройства к элементам памяти, получим, что модель состоит из 1024 элементов. Тогда в режиме простой замены количество дефектных битов будет варьироваться от 0,6 до 10%. В режиме гаммирования с обратной связью 50% битов будут не совпадать с правильным результатом, т.е. информация будет потеряна полностью. В случае сбоя – вся информация потеряна в любом режиме работы, т.к. ошибка не устраняется.

Данные анализа и других исследований[1] свидетельствуют о необходимости применения методов повышения эксплуатационной надежности криптосхем.

Для повышения отказоустойчивости криптосхем необходимо применять специальные алгоритмы коррекции ошибок, т.к. здесь широко применяются арифметические и логические операции [3].

Для этой цели не подходят ни код с проверкой на четность, ни код Хемминга, т.к. у них не существует однозначной связи между контрольными разрядами исходных чисел и контрольными разрядами результата операции. Посылочные корректирующие коды не совместимы с арифметическими операциями. Самым простым кодом, позволяющим обнаруживать одиночную ошибку в блоке суммирования по модулю 32, является контроль остатков от деления по модулю. Принципиальная схема блока суммирования, использующего этот принцип коррекции, представлена на рис. 1.

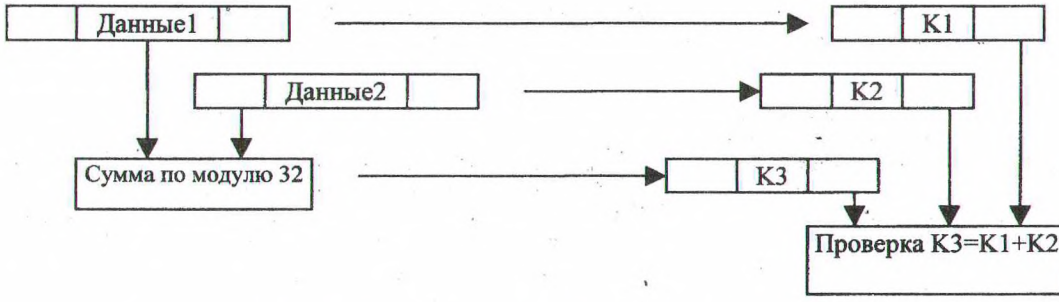

Рис. 1: Отказоустойчивый блок суммирования по модулю 32

Суть метода заключается в вычислении остатков от деления операндов и остатка от деления результата по заранее выбранному модулю. Если сумма остатков деления операндов не равна остатку деления результата, то делают вывод о возникновении ошибки.

Для построения отказоустойчивого блока подстановки можно использовать код Хемминга. Поясняющая данный принцип схема приведена на рис. 2. Для этого необходимо произвести расчет кода Хемминга для данных, а затем использовать вторую подстановочную таблицу для контрольных разрядов. А далее простое вычисление контрольных данных и сравнения с полученными после подстановки позволит установить корректность данных.

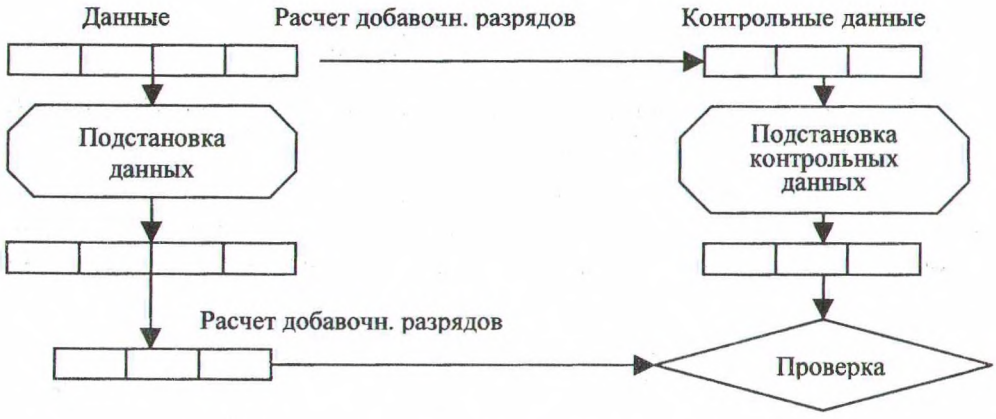

Рис. 2. Отказоустойчивый блок подстановки

Для выявления возникновения ошибок в блоке суммирования по модулю 2 можно использовать следующий метод. Вычислить контрольные разряды кода Хемминга для результата операции суммирования по модулю 2. Произвести суммирование по модулю 2. Вычислить контрольные разряды и сравнить их с полученными данными. В данный метод заложено дублирование, но избыточность все же меньше, чем при использовании трех блоков для определения корректности операции сложения по модулю 2 с использованием принципа большинства. Схема данного блока представлена на рис. 3.

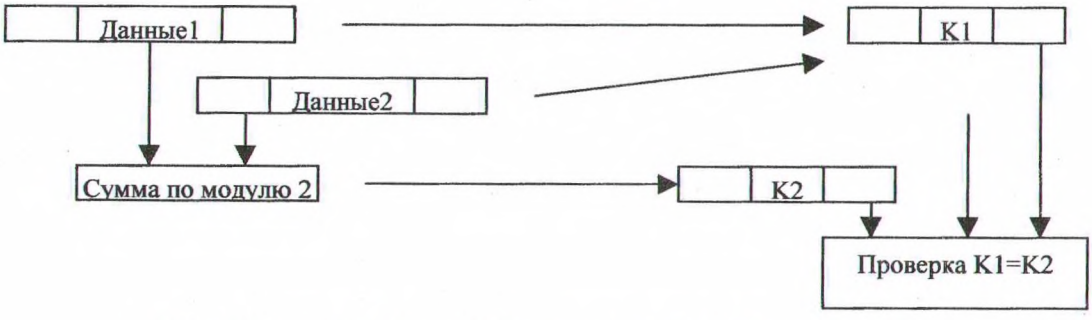

Рис. 3. Отказоустойчивый блок суммирования по модулю 2

Кроме того, следует заметить, что применение методов понижения влияния шумов и излучений и прогнозирование сбоев также повышает устойчивость аппаратуры к отказам.

ЛИТЕРАТУРА

1. Пацей Н.В., Скачков М.С., Урбанович П.П. Некоторые закономерности распределения ошибок в каналах передачи дискретной информации // Известия белорусской инженерной академии. №1(7)/1, IV МНТК. Современные средства связи: Мат. конф. – Минск,1999. – С.18.

2. Пацей Н.В. Метод повышения отказоустойчивости криптографических схем защиты информации // Труды БГТУ. Серия физико-математич. наук и информатики. Вып. 8. – Мн.:БГТУ,2000.

3. Лысиков Б.Г. Арифметические и логические основы цифровых автоматов. – Мн.:Выш.школа,1980. –336 с.