УДК 004.052

А.И. Галабурда, ассистент

РЕАЛИЗАЦИЯ ОТКАЗОУСТОЙЧИВЫХ ЭЛЕМЕНТОВ, ВЫПОЛНЯЮЩИХ ЭЛЕМЕНТАРНЫЕ ОПЕРАЦИИ БЛОЧНЫХ КРИПТОАЛГОРИТМОВ

In this article new method of fault-tolerant operation block building. Considered operations: of bitwise summation, summation by modulo 2^{32}, substitution. As error correcting code the Hamming code is used.

Шифрование – один из самых эффективных и распространенных способов защиты информации. В свою очередь, аппаратная реализация криптографического алгоритма надежней программного исполнения. В число основных достоинств аппаратных шифраторов входят следующие [1]:

– гарантия неизменности алгоритма шифрования (криптографическое программное обеспечение по определению не защищено от воздействия враждебных программ, способных модифицировать его код);

– наличие аппаратного датчика случайных чисел, используемого при создании криптографических ключей. Для этих целей в аппаратном датчике задействованы физические процессы, что обеспечивает выдачу действительно случайных чисел, распределение которых близко к равновероятному. Аппаратный датчик случайных чисел, как правило, применяется при генерации ключей не только шифрования, но и электронной цифровой подписи;

– возможность прямой (минуя системную шину компьютера) загрузки ключей шифрования в специализированный процессор аппаратного шифратора с персональных идентификаторов – носителей типа смарт-карт и модулей Touch Memory. Тем самым снимается угроза перехвата ключей, которые при использовании программных шифраторов циркулируют в оперативной памяти компьютера;

– хранение ключей шифрования не в оперативном запоминающем устройстве компьютера (как в случае с программной реализацией), а в памяти шифропроцессора;

– идентификация и аутентификация пользователя до загрузки операционной системы; запрет на изменение процесса загрузки компьютера (когда, скажем, вход зарегистрированного пользователя осуществляется только по предъявлении идентификатора с ключами, а остальные варианты – с загрузочной дискеты, компакт-диска и т. п. – блокированы); возможности контроля целостности операционной системы и прикладного программного обеспечения, позволяющие, к примеру, отследить действия вирусов; ведение доступного лишь администратору безопасности журнала действий пользователей, регистрирующего все (в том числе и безуспешные) попытки доступа к компьютеру. Эти опции обобщенно именуются функциями "электронного замка";

– обеспечение наряду со всеми перечисленными достоинствами сопоставимой с программными продуктами скорости шифрования. Не менее важно, что шифраторы, конструктивно выполненные в виде плат расширения разъема PCI, способны использовать для выполнения криптографических преобразований свой собственный процессор, не загружая процессор компьютера. Понятно, что при программной реализации добиться разгрузки центрального процессора невозможно.

Важной характеристикой средства защиты информации является его надежность, так как аппаратный шифратор из эффективного средства защиты информации может превратиться в не менее эффективное средство ее гарантированного уничтожения: потеря или сбой единственного носителя с ключами означает, что зашифрованная информации утеряна навсегда. Поэтому целесообразно отдать предпочтение системам криптографического преобразования информации, использующим элементы увеличения функциональной надежности. Повысить надежность функционирования системы можно при помощи дубли-

рования узлов устройства с применением мажоритарных элементов. Этот метод обладает рядом достоинств, наиболее значимым из которых является простота реализации. С другой стороны, недостатком этого метода является большая избыточность. Этот метод получил широкое распространение.

Другой подход к увеличению функциональной надежности предполагает использование отказо- и сбоеустойчивых блоков для реализации устройств. В этом случае аппаратные затраты будут меньше, чем при реализации схем дублирования. Однако реализация этого метода требует разработки унифицированной элементной базы отказоустойчивых элементов, что требует дополнительных затрат [2].

Рассмотрим способ увеличения функциональной надежности блока суммирования по модулю 2. В качестве корректирующего кода будем использовать код Хемминга [3].

Обозначим через функцию F(x) операцию вычисления проверочных разрядов.

Допустим, матрица кода Хемминга (7, 4) имеет вид

$$H_{7,4} = \begin{vmatrix} x4 & x3 & x2 & x1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{vmatrix}.$$

Вычисление контрольных разрядов проводится по формулам:

$$x_5 = x_4 + x_2 + x_1; \quad (1)$$

$$x_6 = x_4 + x_3 + x_1; \quad (2)$$

$$x_7 = x_4 + x_3 + x_2, \quad (3)$$

где + операция суммирования по модулю 2.

Выпишем уравнения для расчета проверочных разрядов кода Хемминга для случая сложения аргументов по модулю 2:

обозначим операнды как x' и x '', а результат – y, индексами будем указывать положение бит.

Так,

$$y_1 = x_1' + x_1''; \quad (4)$$

$$y_2 = x_2' + x_2''; \quad (5)$$

$$y_3 = x_3' + x_3''; \quad (6)$$

$$y_4 = x_4' + x_4''. \quad (7)$$

Проверочные разряды в этом случае вычисляются по формулам

$$y_5 = y_4 + y_2 + y_1; \quad (8)$$

$$y_6 = y_4 + y_3 + y_1; \quad (9)$$

$$y_7 = y_4 + y_3 + y_2. \quad (10)$$

Преобразуем выражения 8 –10 с использованием 4–7:

$$y_5 = x_4' + x_4'' + x_2' + x_2'' + x_1' + x_1''; \quad (11)$$

$$y_6 = x_4' + x_4'' + x_3' + x_3'' + x_1' + x_1''; \quad (12)$$

$$y_7 = x_4' + x_4'' + x_3' + x_3'' + x_2' + x_2''. \quad (13)$$

Перегруппируем:

$$y_5 = (x_4' + x_2' + x_1') + (x_4'' + x_2'' + x_1''); \quad (14)$$

$$y_6 = (x_4' + x_3' + x_1') + (x_4'' + x_3'' + x_1''); \quad (15)$$

$$y_7 = (x_4' + x_3' + x_2') + (x_4'' + x_3'' + x_2''). \quad (16)$$

С учетом формул 1–3

$$y_5 = x_5' + x_5''; \quad (17)$$

$$y_6 = x_6' + x_6'';\quad (18)$$

$$y_7 = x_7' + x_7''.\quad (19)$$

Таким образом, выражения 17–19 можно записать:

$$F(X') + \text{mod } 2\ F(X'') = F(X' + \text{mod } 2\ X''). \quad (20)$$

Для исправления возникающих ошибок в блоке суммирования по модулю 2 необходимо [4]:

1) вычислить контрольные разряды кода Хемминга для исходных данных операции суммирования по модулю 2;
2) произвести суммирование по модулю 2 для исходных данных;
3) произвести суммирование по модулю 2 для контрольных разрядов;
4) произвести процедуру коррекции, если необходимо.

Схема данного блока представлена на рис. 1.

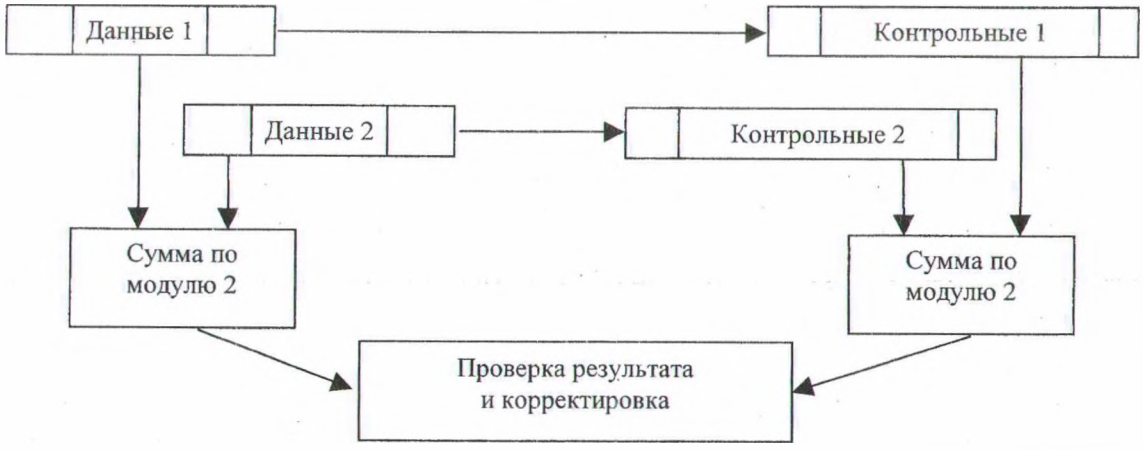

Рис. 1

Рассмотрим работу элемента, выполняющего суммирование по модулю 2^{32}.

Предположим, что для суммирования с переносом выполняется следующее условие:

$$F(X') + \text{mod } 2^{32}\ F(X'') = F(X' + \text{mod } 2^{32}\ X''), \quad (21)$$

где mod 2^{32} – операция суммирования по модулю 2^{32}.

Проверим выполнение этого уравнения для произвольных данных.

Пусть

$X' = 2_{10}, (0010_2)$; $F(X') = 5_{10}, (101_2)$;

$X'' = 6_{10}, (0110_2)$; $F(X'') = 3_{10}, (011_2)$.

В этом случае $X' + \text{mod } 2^{32}\ X'' = 8_{10}, (1000_2)$; $F(X' + \text{mod } 2^{32}\ X'') = 7_{10}, (111_2)$.

В то же время $F(X') + \text{mod } 2^{32}\ F(X'') = 8_{10}, (1000_2)$.

Как видно из приведенного расчета,

$$F(X') + \text{mod } 2^{32}\ F(X'') \neq F(X' + \text{mod } 2^{32}\ X'').$$

Следовательно, гипотеза о возможности применения уравнения 21 для отказоустойчивой реализации операции суммирования по модулю 2^{32} неверна.

Выпишем уравнения для расчета проверочных разрядов кода Хемминга, для случая сложения аргументов по модулю 2^{32}, обозначим операнды как x' и x '', а результат – y, индексами будем указывать положение бит.

Так,

$$Y\ 1 = x\ 1' + x\ 1'' + П\ 1, \quad (22)$$

где П 1 – флаг переноса, П 1 = 0.

$$Y\,2 = x\,2' + x\,2'' + П\,2; \quad (23)$$

$$Y\,3 = x\,3' + x\,3'' + П\,3; \quad (24)$$

$$y\,4 = x\,4' + x\,4'' + П\,4. \quad (25)$$

Согласно уравнению 1, вычисление пятого проверочного бита описывается уравнением

$$Y\,5 = y\,4 + y\,2 + y\,1. \quad (26)$$

Подставим выражения 25, 23 и 22 в формулу 26:

$$Y\,5 = x\,4' + x\,4'' + П\,4 + x\,2' + x\,2'' + П\,2 + x\,1' + x\,1'' + П\,1. \quad (27)$$

Перегруппируем операнды

$$Y\,5 = x\,4' + x\,2' + x\,1' + x\,4'' + x\,2'' + x\,1'' + П\,4 + П\,2 + П\,1.$$

Однако, согласно уравнению 1, сумма $x\,4 + x\,2 + x\,1$ равна $x\,5$, тогда

$$Y\,5 = x\,5' + x\,5'' + П\,4 + П\,2 + П\,1. \quad (28)$$

Для других проверочных бит значения получаются аналогично.

Таким образом, проверочные разряды кода Хемминга результата операции суммирования по модулю 2^{32} можно вычислить, используя проверочные разряды исходных операндов и значения бит переноса.

Схема отказоустойчивой реализации блока операции суммирования по модулю 2^{32} представлена на рис. 2.

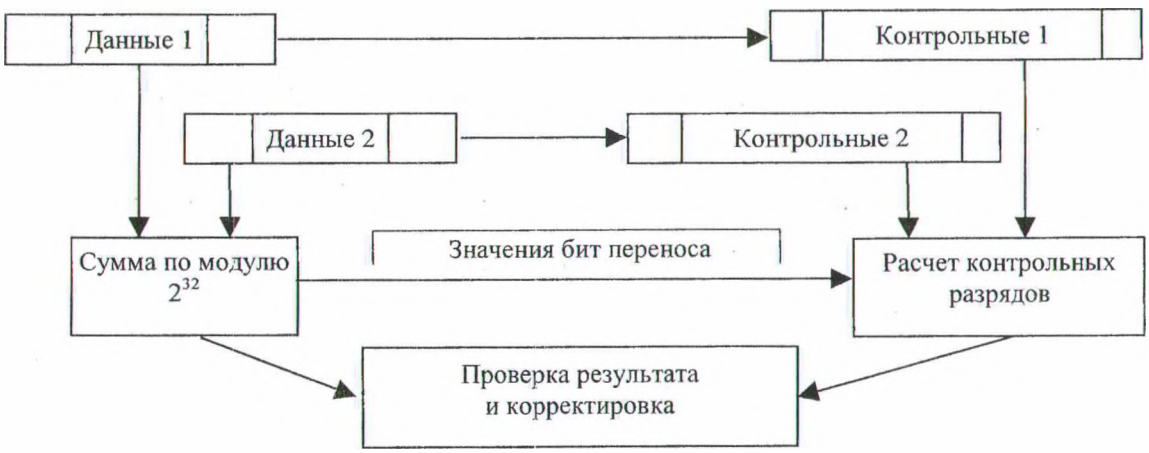

Рис. 2

Увеличение параметров отказоустойчивости блока подстановки может быть достигнуто введением дополнительного элемента, осуществляющего подстановку над проверочными разрядами кода Хемминга. Схема реализации блока подстановки представлена на рис. 3.

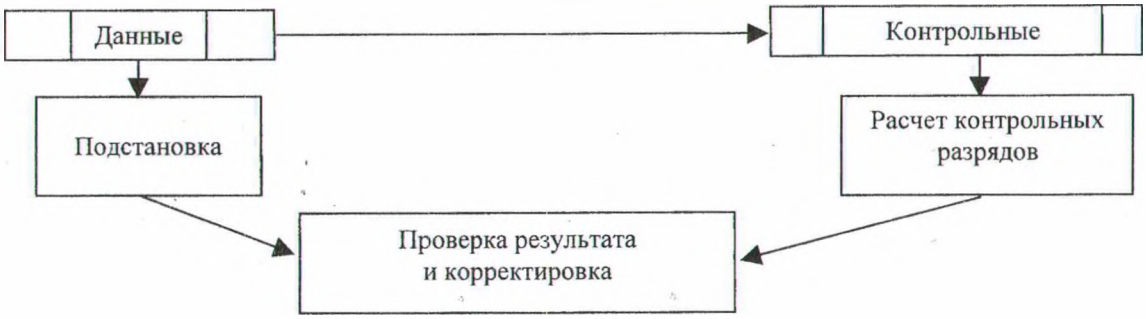

Рис. 3

Использование разработанных элементов возможно в большом количестве вычислительных устройств, требующих обеспечения высокой отказоустойчивости. Но наиболее перспективным является применение таких элементов в устройствах криптопреобразования. Например, с использованием разработанных элементов возможно реализовать устройство, работающее по алгоритму ГОСТ 28147-89. Разработка унифицированных отказоустойчивых элементов позволит удешевить аппаратные средства защиты информации.

ЛИТЕРАТУРА

1. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. – СПб.: Лань, – 2001. – 218 с.

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

3. Галабурда А.И. Некоторые аспекты увеличения отказоустойчивости устройств, реализующих блочные алгоритмы шифрования // Материалы I международной конференции «Информационные системы и технологии». – Минск: БГУ, 2002. – Т. 2.–С. 30 – 33.

4. Галабурда А.И., Урбанович П.П. Методы повышения функциональной надежности блоков криптографического преобразования информации (на примере криптоалгоритма ГОСТ 28147-89) // Доклады III международной конференции «Цифровая обработка информации и управление в чрезвычайных ситуациях». – Минск: Ин-т техн. кибернетики НАН Беларуси, 2002. – Т. 2. – С. 200 –205.