ПОВЫШЕНИЕ НАДЕЖНОСТИ ФУНКЦИОНИРОВАНИЯ СПЕЦПРОЦЕССОРОВ АДАПТИВНЫХ СРЕДСТВ ЗАЩИТЫ НА ОСНОВЕ ПРИМЕНЕНИЯ ПОЛИНОМИАЛЬНОЙ СИСТЕМЫ КЛАССОВ ВЫЧЕТОВ

Калмыков И.А., Лободин М.В., Резеньков Д.Н., Петлеванный С.В.

Ставропольский военный институт связи Ракетных войск,

Северо-Кавказский государственный технический университет

г. Ставрополь, Россия

kia762@yandex.ru , miklob@mail.ru

Проблема исследований: Применение адаптивных средств защиты информации (АСЗИ) позволит повысить эффективность защиты информации от НСД. В то же самое время обеспечение надежности функционирования спецпроцессоров (СП) АСЗИ является одной в ряду наиболее важных задач.

Решение проблемы:

При хранении, передаче и обмене электронной информацией в сетях и системах возникают проблемы обеспечения ее конфиденциальности и целостности. Решить данную задачу можно за счет применения адаптивных средств защиты информации. Применение алгебраических систем, определяемых в расширенных полях Галуа, является одним из наиболее перспективных направлений в построении АСЗИ. В таких системах основными криптографическими преобразованиями являются сложение, умножение и возведение элементов по модулю порождающего полинома $g(z)$. Применение полиномиальной системы классов вычетов (ПСКВ) позволяет повысить не только скорость проведения криптографических преобразований, но и обеспечить высокую надежность работы СП АСЗИ.

Согласно [1-3] в данной алгебраической системе полином $A(z)$, удовлетворяющий условию $A(z) \in P_{пол}$, где $P_{пол} = \prod_{i=1}^{n} p_i(z) = z^{p^n - 1} - 1$, представляется в виде вектора

$$A(z) = (a_1(z), a_2(z), \ldots, a_n(z)), \qquad (1)$$

где $a_i(z) = rest(A(z)/p_i(z))$, $p_i(z)$ - минимальные многочлены расширенного поля $GF(p^n)$, $i = 1,2,...,n$.

Тогда операции сложения, вычитания и умножения можно свести к операциям, проводимым над соответствующими остатками, что повышает быстродействие. Кроме того операции проводятся над малоразрядными операндами, что позволяет сократить аппаратурные затраты.

Однако применение ПСКВ позволяет не только повысить скорость обработки данных, но и обеспечить высокую надежность работы СП [1-3]. Если на диапазон возможного изменения кодируемого множества полиномов наложить ограничения, то есть выбрать k из n оснований ПСКВ ($k < n$), то это определит рабочий диапазон

$$P_{раб}(z) = \prod_{i=1}^{k} p_i(z), \qquad (2)$$

Многочлен $X(z)$ будет считаться разрешенным, если он принадлежит рабочему диапазону $X(z) \in P_{раб}(z)$. Если полином не принадлежит этому диапазону, то он содержит ошибки.

Для коррекции ошибок в немодулярных кодах широко используются позиционные характеристики [3]. Среди множества алгоритмов определения позиционной характеристики непозиционного кода полиномиальной системы класса вычетов особое место принадлежит алгоритму обнаружения ошибки, базирующемуся на процедуре расширения оснований ПСКВ.

$$A(z) = a_1(z)B_1(z) + a_2(z)B_2(z) + ... + a_k(z)B_k(z), \qquad (3)$$

где $B_i(z)$ – ортогональный базис по i-ому основанию; $i=1,\ldots,k$.

Для расширенной системы оснований $p_1(z), p_2(z),..., p_{k+1}(z)$ справедливо

$$A(z) = \sum_{i=1}^{k+1} a_i(z) \cdot B_i^*(z) - r_A^*(z) \cdot P_{раб}(z) \cdot p_{k+1}(z), \qquad (4)$$

где $B_i^*(z)$ -ортогональный базис в расширенно системе оснований; r_A^* - ранг. $P_{раб}(z) = \prod_{i=1}^{k} p_i(z)$ - рабочий диапазон.

Если положить условие, что $A(z) \in P_{раб}(z)$, то

$$\left[\frac{A(z)}{P_{раб}(z)}\right] = 0. \qquad (5)$$

Тогда, подставив в равенство (4) выражение (5) получаем

$$S = \left[\frac{\sum_{i=1}^{k+1} a_i(z) \cdot B_i^*(z) - r_A^*(z) P_{раб}(z) p_{k+1}(z)}{P_{раб}(z)}\right] = \left|\frac{\sum_{i=1}^{k+1} a_i(z) \cdot B_i(z)}{P_{раб}(z)}\right|^{+}_{p_{k+1}(z)}, \qquad (6)$$

где S - номер интервала.

Исходя из условия взаимной простоты оснований имеем

$$\frac{B_i^*(z)}{P_{раб}(z)} = \frac{m_i^*(z) \cdot P_{раб}(z) \cdot p_{k+1}(z)}{p_i(z) \cdot P_{раб}(z)} == \left[\frac{B_i^*(z)}{P_{раб}(z)}\right] \cdot P_{раб}(z) + \left|B_i^*(z)\right|^{+}_{P(z)} = R_i(z) + \left|B_i^*(z)\right|^{+}_{P(z)} \qquad (7)$$

Так как $B_i^*(z) mod P_{раб}(z) \equiv B_i(z)$, то выражение (4) можно представить

$$S = \left| r_a(z) + \sum_{i=1}^{k+1} a_i(z) \cdot \left[\frac{B_i^*(z)}{P_{раб}(z)}\right] \right|^{+}_{p_{k+1}(z)}. \qquad (8)$$

Положив, что $a_{k+1}(z) = 0$, получаем

$$S = \left| r_a(z) + \sum_{i=1}^{k+1} a_i(z) \cdot R_i(z) \right|^{+}_{p_{k+1}(z)}. \qquad (9)$$

Если $S = 0$, то значение $a_{k+1}(z) = 0$. В противном случае

$$a_{k+1}(z) = S(z) \cdot C(z), \qquad (10)$$

где $C(z) = \left|R_{k+1}(z)^{-1}\right|^{+}_{p_{k+1}(z)}$.

Тогда

$$a_{k+1}(z) = C(z) \cdot \left| r_a(z) + \sum_{i=1}^{k} a_i(z) \cdot R_i(z) \right|^{+}_{p_{k+1}(z)}. \qquad (11)$$

Затем значение остатка по контрольному основанию, вычисленное согласно (11), сравниванию с остатком, полученным в процессе работы СП АСЗИ. Если данные значения совпадают, то это свидетельствует о том, что исходная комбинация ПСКВ не содержит ошибки. В противном случае – комбинация ПСКВ содержит ошибку, вызванную отказом оборудования СП.

Применение алгоритма расширения оснований позволяет исправлять однократные ошибки, возникающие в результате отказов работы спецпроцессора криптографических преобразований.

Литература

1. Калмыков И.А. Математические модели нейросетевых отказоустойчивых вычислительных средств, функционирующих в полиномиальной системе классов вычетов/ Под ред. Н.И. Червякова. – М.: ФИЗМАТЛИТ, 2005. - 276 с.

2. Калмыков И.А., Червяков Н.И., Щелкунова Ю.О., Бережной В.В. Математическая модель нейронных сетей для исследования ортогональных преобразований в расширенных полях Галуа/Нейрокомпьютеры: разработка, применение. №6, 2003. с.61-68с.

3. Элементы применения компьютерной математики и нейроинформатики /Н.И. Червяков, И.А. Калмыков И.А., В.А. Галкина, Ю.О. Щелкунова, А.А. Шилов; Под ред. Н.И. Червякова. – М.: ФИЗМАТЛИТ, 2003. – 216с.