ОСНОВНЫЕ МЕТОДЫ ПРЯМОГО ПРЕОБРАЗОВАНИЯ В МОДУЛЯРНЫЙ КОД

Калмыков И.А., Макарова А.В., Науменко Д.О., Березкина М.В.,
Северо-Кавказский федеральный университет,
Институт информационных технологий и телекоммуникаций,
г. Ставрополь, Россия,
alyonchikMav@yandex.ru

Развитие новых информационных технологий и всеобщая компьютеризация привели к тому, что информационная безопасность не только становится обязательной, она еще и одна из характеристик информационных систем. Существует довольно обширный класс систем обработки информации, при разработке которых, фактор безопасности играет первостепенную роль.

В данной работе рассмотрена разработка блока криптографической системы, способной осуществлять операции прямого преобразования в модулярный код, с использованием полиномиальных систем классов вычетов. С помощью которой возможна организация ортогональных преобразований сигналов в расширенных полях Галуа $GF(p^{\nu})$ [1,2]. Одним из основным достоинств системы класса вычетов является простота выполнения модульных операций (сложения, вычитания, умножения). Формальные правила выполнения таких операций в ПСКВ позволяют существенно повысить скорость работы блока криптографической системы.

Одной из немодульных процедур является реализация прямого преобразования кода позиционной системы счисления (ПСС) в код ПСКВ. В последние годы нашли широкое применение несколько методов перевода из ПСС в ПСКВ. Один из основных методов перевода является метод понижения разрядности числа [1,3]

$$a_i = C_i = \left|2^i\right|_{p_i}^{*} = 2^i, \forall i \in [0,r], . \qquad (1)$$

Из этого следует, что для получения требуемого вычета $\alpha_i = |A|_{Pi}^{+}$ предлагается использовать повторение вычислительной модели

$$|A|_{Pi}^{+} = \sum_{i=0}^{J} \left|2^i\right|_{Pi}^{+} \cdot \{a(j)\}^{[i]}, \text{ где j=0,1,2…,} \qquad (2)$$

При этом для реализации (2) используется позиционный сумматор.

Но для реализации выражения (2) необходимо выполнять проверки условий окончания процесса итераций по контролю знака полученной разницы в операции вычитания, что приводит к понижению быстродействия системы. А при большой размерности входных данных количество итераций может быть чрезмерным, что снижает быстродействие системы в целом.

Ликвидировать указанные недостатки можно отказавшись от обратных связей в нейронных сетях (НС) конечного кольца, реализовав обработку на сети прямого распространения [1]. Число слоев в такой сети определяется количеством итераций *l*, необходимых для преобразования входных данных, а количество нейронов в каждом слое - разрядностью обрабатываемых данных на каждой итерации. Веса, связывающие *i*-й нейрон с *j*-м нейроном

следующего слоя, определяются $\overline{\omega}_{ij} = \left\{ \left| 2^i \right|_p^+ \right\}^{[j]}$. Тогда итеративный алгоритм преобразования А по модулю р определяется выражением

$$A(l+1) = \sum_{i=0}^{\deg A(l)} \left| 2^i \right|_p^+ \cdot \left| \left[\frac{A(l)}{2^i} \right] \right|_2^+, \qquad (3)$$

Замена обратных связей в НС на прямые дает возможность увеличить скорость обработки данных, так как в такой сети одновременно обрабатывается несколько отсчетов и в каждом такте работы сети на входе формируются преобразованные данные.

Повысить скорость реализации прямого преобразования из кода ПСС в код ПСКВ можно с помощью метода непосредственного суммирования [1,3]. Преобразование исходного *A(x)*, заданного в поле $GF(p^{\upsilon})$, в полиномиальную систему класса вычетов осуществляется с помощью набора констант, которые являются эквивалентами степеней оснований 2^i и коэффициентов при соответствующих степенях оснований $a_i(x)$, представленных в ПСКВ

$$A(x) = \sum_{l=0}^{k} a_l(x) \cdot x^l \equiv a_i(x) \bmod p_i(x), i = 1,2,3,...,n. \qquad (4)$$

Для получения значений *A(x)* в системе класса вычетов с основаниями $p_1(x)$, $p_2(x)$,..., $p_n(x)$ необходимо получить в этой системе значения $a_i(x) \bmod p_i(x)$. В этом случае остаток по модулю $p_i(x)$ определяется

$$\alpha_i(x) = \left| \sum_{l=0}^{k} (a_l{}^i \bullet x^l) \bmod p_i(x) \right|_2^+, \qquad (5)$$

где $\mathrm{a}_1^i = a_l \bmod p_i(x), i = 1,2,3,...,n.$

В соответствии с (5), перевод *A(x)* из позиционной системы счисления в непозиционную можно свести к суммированию по модулю два величин $a_l^i \bmod p_i(x)$ в соответствии с заданным полиномом *A(x)*.

Пример. Найти остаток $A(x) = x^{12} + x^7 + x^5 + x^4 + x^3 + x$ по модулю $p(x) = x^4 + x^3 + 1$

Для перевода из ПСС в ПСКВ используем выражение (5). Тогда значения остатков степеней оснований и коэффициентов при них равны

$x^{12} \equiv x + 1 \bmod(x^4 + x^3 + 1)$

$x^7 \equiv x^2 + x + 1 \bmod(x^4 + x^3 + 1)$

$x^5 \equiv x^3 + x + 1 \bmod(x^4 + x^3 + 1)$

$x^4 \equiv x^3 + 1 \bmod(x^4 + x^3 + 1)$

$x^3 \equiv x^3 \bmod(x^4 + x^3 + 1)$

$x \equiv x \bmod(x^4 + x^3 + 1)$

Тогда, согласно (5), получаем

$$\alpha(x) = (x+1) \oplus (x^2 + x + 1) \oplus (x^3 + x + 1) \oplus (x^3 + 1) \oplus x^3 \oplus x = x^3 + x^2$$

Следовательно,

$$x^{12} + x^7 + x^5 + x^4 + x^3 + x \equiv x^3 + x^2 \bmod(x^4 + x^3 + 1)$$

В работе [1] представлена матрица связанности, т. е. синаптические веса нейронной сети, представляются в виде матрицы, строки которой

соответствуют области аксонов предыдущего слоя, а столбцы – рецепторным полям нейронов последующего слоя. Разрабатываемая НС для перевода из ПСС в ПСКВ содержит 2 слоя. Первый слой состоит из 15 нейронов, на входы которых подается исходный полином в двоичном коде. С выходов нейронов первого слоя сигналы поступают на входы нейронов 2-го слоя в соответствии с матрицей T_{12}

$$T_{12} = \begin{vmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 10 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 11 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 10 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 01 & 0 & 1 & 1 & 0 & 0 \end{vmatrix}$$

При этом операция перевода осуществляется всего за одну итерацию, что является существенным преимуществом по сравнению с ранее рассмотренными методами перевода. Структура НС, реализующей перевод по $p(x) = x^4 + x^3 + 1$ в ПСКВ поля $GF(2^4)$, представлена [1].

Таким образом, очевидно, что реализация метода непосредственного суммирования для полиномиальной системы класса вычетов позволяет разрабатывать высокоскоростные преобразователи кодов для вычислительных структур реального масштаба времени.

СПИСОК ЛИТЕРАТУРЫ

1. Элементы компьютерной математики и нейроноинформатики /Червяков Н.И., Калмыков И. А., Галкина В.А., Щелкунова Ю.О., Шилов А.А.. - М.: ФИЗМАТЛИТ, 2003. - 216 с.

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

3. 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.