УДК 004.9, 004.56.5

Коляда А.А., Чернявский А.Ф., Шабинская Е.В.

БАЗОВЫЕ НЕЙРОННЫЕ СЕТИ НА КОНЕЧНЫХ КОЛЬЦАХ ДЛЯ МОДУЛЯРНОЙ ПОРОГОВОЙ СХЕМЫ РАЗДЕЛЕНИЯ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ

Научно-исследовательское учреждение «Институт прикладных физических проблем имени А.Н. Севченко» Белорусского государственного университета.
Минск, Республика Беларусь. shabinskaya@rambler.ru

Предложен новый алгоритм позиционно-модулярного кодового преобразования больших чисел, ориентированный на применение в нейросетевых пороговых криптосхемах разделения секретной информации. В качестве базового используется редукционный метод рекурсивного снижения разрядности преобразуемых чисел. Результирующая процедура выполняется не более чем за $\lfloor \log_2 b \rfloor$ итераций (b – разрядность входного числа). Разработанный алгоритм может служить эффективной основой синтеза базовых нейронных сетей конечного кольца для пороговых систем разделения секрета модулярного типа.

Современная применительная практика средств защиты информации в распределенных системах обработки данных указывает на то, что приоритетные позиции в этой области отводятся технологии активной безопасности [1, 2].

Как известно, наиболее уязвимыми местами распределенных вычислительных систем являются места хранения секретной информации и, в частности, криптографических ключей. Основополагающая идея, реализуемая в рамках метода активной безопасности, состоит в периодическом обновлении и пространственном разделении секрета между абонентами, участниками сеансов связи. Поскольку ключи, а также их компоненты – частичные секреты, принадлежащие абонентам, представляют собой большие числа, то базовые реализационные процедуры технологии активной безопасности имеют высокий уровень вычислительной сложности. С одной стороны, это обеспечивает высокую стойкость применяемых криптографических средств, а с другой – выдвигает весьма жесткие требования к их производительности. Перспективным подходом к решению обозначенной проблемы является применение быстродействующих нейроускорителей, реализующих свойственную для нейронных сетей (НС) уникальную возможность массовых параллельных вычислений, в том числе при выполнении трудоемких криптографических преобразований на диапазонах больших чисел (ДБЧ). Особый интерес при этом представляют нейроускорители, построенные на основе модулярных систем счисления (МСС) [1–3]. Сказанное обусловлено идеальной согласованностью модулярной арифметики (МА) с принципами нейросетевой обработки информации.

Ключевую роль в процессе построения модулярных пороговых криптосхем разделения информации нейросетевого типа выполняют НС, определенные на конечных кольцах вычетов по некоторому базису модулей [1, 4–7]. Операционную основу нейронных сетей конечного кольца (НСКК) составляют, главным образом, операции приведения целых чисел (ЦЧ) к остаткам по используемым модулям. Вполне понятно, что НСКК как структурно, так и на операционном уровне в максимальной мере должны быть согласованы с естественным кодовым параллелизмом МА.

Рассмотрим НС конечного кольца по некоторому модулю m. Остановимся подробнее на проблеме вычисления в данной НС остатка $\chi = |X|_m$ от деления входного неотрицательного ЦЧ X, представленного b-разрядным двоичным кодом $(x_{b-1}\ x_{b-2}\ \ldots\ x_0)_2$ $(x_j \in \{0,1\}\ (j = \overline{0, b-1}))$ на m. По критерию простоты компьютерной реализации наиболее приемлемым методом выполнения операции $\chi = |X|_m$, то есть преобразования $(x_{b-1}\ x_{b-2}\ \ldots\ x_0)_2 \to |X|_m$, является метод модулярной редукции суммы взвешенных

операндов по рекурсивной схеме последовательного снижения разрядности получаемых чисел [5, 6].

Положим

$$X^{(0)} = (x^{(0)}_{b_0-1}\ \ x^{(0)}_{b_0-2} \ldots\ x^{(0)}_0)_2 = \sum_{j=0}^{b_0-1} 2^j x_j^0\ \ (b_0 = b,\ \ x_j^{(0)} = x_j) \tag{1}$$

и пусть

$$W_j = \left| 2^j \right|_m^- = \begin{cases} \left| 2^j \right|_m, \text{ если } \left| 2^j \right|_m < \lceil m/2 \rceil, \\ \left| 2^j \right|_m - m, \text{ если } \left| 2^j \right|_m \ge \lceil m/2 \rceil. \end{cases} \tag{2}$$

Тогда применяемая редукционная схема описывается соотношением

$$X^{(s)} = \sum_{j=0}^{b_{s-1}-1} W_j x_j^{(s-1)} = (x^{(s)}_{b_s-1}\ x^{(s)}_{b_s-2} \ldots x^{(s)}_0)_2 = \sum_{j=0}^{b_s-1} 2^j x_j^{(s)}\ \ (b_s = \lceil \log_2 X^{(s)} \rceil; \quad s = \overline{1, S};\ S \ge 1). \tag{3}$$

Из (1)–(3) следует, что $\left|X^{(s)}\right| < \sum_{j=0}^{b_{s-1}-1} \frac{m}{2} = b_{s-1} m/2$. Следовательно, для разрядности b_s ЦЧ $X^{(s)}$ верна оценка: $b_s < \log_2 b_{s-1} + b_\mathrm{mod}$, где $b_\mathrm{mod} = \lceil \log_2 m \rceil$ – длина двоичного кода модуля m. С помощью приведенной оценки легко показать, что в результате преобразования (3), выполняемого на s-й итерации редукционной схемы разрядность b_s получаемого ЦЧ $X^{(s)}$, в сравнении с разрядностью b_{s-1} числа $X^{(s-1)}$ уменьшается, как минимум, в два раза: $b_{s-1}/b_s > 2$. Искомое неравенство для проверки данного утверждения имеет вид: $\frac{1}{2} b_{s-1} > \log_2 b_{s-1} + b_\mathrm{mod}$.

Рекурсивный редукционный процесс, базирующийся на (1)–(3), характеризуется следующими свойствами:

А. Числа $X^{(01)} = X, \left|X^{(1)}\right|, \left|X^{(2)}\right|, \ldots \left|X^{(S)}\right|$ образуют убывающую последовательность. При этом ввиду (2) все $X^{(s)}$ $(s = \overline{0, S})$ являются элементами одного и того же класса вычетов по модулю m, то есть $X^{(s)} \equiv X (\mathrm{mod}\ m)$.

Б. Признаком окончания процесса понижения разрядности ЦЧ $X^{(s)}$ с возрастанием s может служить выполнение условия $b_S \le b_\mathrm{mod}$. Искомое значение остатка $\chi = \left|X\right|_m$ определяется по правилу

$$\chi = \begin{cases} X^{(S)}, \text{ если } b_S < b_\mathrm{mod} \text{ или } X^{(S)} < m, \\ X^{(s)} - m \text{ в противном случае}. \end{cases} \tag{4}$$

В. Количество итераций рекурсивной процедуры, реализующей (3), составляет $S = \lceil \log_2 (b / b_\mathrm{mod}) \rceil$.

Г. Набор необходимых весов W_j для схемы рассчитывается предварительно и хранится в памяти.

Д. Расчетные соотношения (3) и (4) целиком согласуются с принципами нейросетевой вычислительной технологии.

Е. Схема (3) без существенных структурно-функциональных изменений применима для любого числа модулей. Это обеспечивает возможность совместного использования ИНС и МА.

Синтезированный на базе редукционной схемы понижения разрядности входного числа алгоритм позиционно-модулярного кодового преобразования заключается в нижеследующем.

Параметры алгоритма: основания $m_1, m_2, \ldots m_k$ $(k>1)$ базовой МСС.

Входные данные алгоритма: двоичный код $(x_{b-1}\ x_{b-2}\ x_0)_2$ входного ЦЧ X (b – длина кода).

Выходные данные: модулярный код: $\chi_1, \chi_2, \ldots, \chi_k$ числа X.

Предварительно получаемые данные: Рассчитанные по правилу (2) наборы весов $W_i = \left\{ W_{j,i} \middle| W_{j,i} = \left| 2^j \right|_{m_i} \ (j = \overline{0, b-1}) \right\}$ $(i = \overline{1,k})$.

Тело алгоритма позиционно-модулярного кодового преобразования по редукционной схеме понижения разрядности ЦЧ

ПМ_РС.1. Положить $b_0=b$, $X^{(0)} = (x_{b_0-1}^{(0)}\ x_{b_0-2}^{(0)}\ \ldots\ x_0^{(0)})_2 = (x_{b_0-1}\ x_{b_0-2}\ \ldots\ x_0)_2 = X$, $i=1$.

ПМ_РС.2. Номеру итерации редукционного процесса присвоить начальные значения: s=1.

ПМ_РС.3. Вычислить $X^{(s)} = \sum_{j=0}^{b_{s-1}-1} W_{j,i} x_j^{(s-1)}$, сформировав двоичный код $(x_{b_s-1}^{(s)}\ x_{b_s-2}^{(s)}\ \ldots\ x_0^{(s)})_2$ длины b_s бит ЦЧ X^s.

ПМ_РС.4. Если разрядность b_s числа X^s и b_mod= $\lceil \log_2 m_i \rceil$ текущего модуля m_i МСС удовлетворяют условию b_mod<b_s, то s инкрементировать (s=s+1) и перейти к ПМ_РС.3.

ПМ_РС.5. При b_s<b_mod в качестве искомого значения i-й цифры формируемого МК зафиксировать $\chi_i = X^{(s)}$ и перейти к ПМ_РС.7.

ПМ_РС.6. Положить

$$\chi_i = \begin{cases} X^{(s)}, \text{ если } X^{(s)} < m_i, \\ X^{(s)} - m_i, \text{ если } X^{(s)} \ge m_i. \end{cases}$$

ПМ_РС.7. При $i \neq k$ переменную i инкрементировать (i=i+1) и перейти к ПМ_РС.2. По достижении равенства i=k завершить работу алгоритма.

Приведенный алгоритм модулярной редукции с последовательным понижением разрядности чисел весьма прост в реализации и имеет сравнительно высокое быстродействие. Для НСКК по модулю $m \in \{m_1, m_2, \ldots, m_k\}$, выполняющей позиционно-модулярное кодовое преобразование по рассмотренной редукционной схеме обычно употребляется [1, 5] условное графическое обозначение, представленное на рис. 1. В исследованиях по проблематике построения модулярных пороговых криптосхем разделения информации данная НС играет ключевую роль.

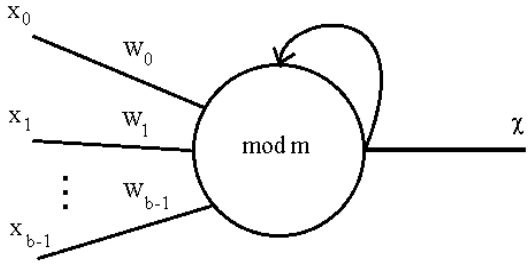

Рисунок 1 – Условное графическое обозначение НСКК по модулю m.

Список литературы

1 Червяков, Н.И. Применение искусственных нейронных сетей и системы остаточных классов в криптографии /Н.И. Червяков, А.И. Галушкин, А.А. Евдокимов, А.В. Лавриненко – М.: Физматлит, 2012. – 280 с.

2 Червяков, Н.И. Нейросетевой генератор криптографических ключей пороговой схемы разделения секрета / Н.И. Червяков, А.А. Евдокимов // Нейрокомпьютеры: разработка, применение. – 2004. – № 10. – С. 62–67.

3 Тихонов, Э.Е. Программно-аппаратная реализация нейронных сетей: Монография / Э.Е. Тихонов, А.А. Евдокимов. – Невинномысск: НИЭУП, 2013. – 116 с.

4 Червяков, Н.И. Нейронные сети конечного кольца для реализации пороговых схем разделения секрета / Н.И. Червяков, А.А. Евдокимов // Нейрокомпьютеры: разработка, применение. – 2007. – № 2–3. – С. 45–50.

5 Пат. №2279132 Россия. МКП G06 H3/04. Нейронная сеть конечного кольца / Ю.А. Стрекалов, Н.И. Червяков, В.А. Галкина, С.В. Лавриненко // Регистрация – 08.07.2003. Опубл. – 27.06.2006.

6 Пат. №2317584 Россия. МКП G06 H3/04. Конвейерная нейронная сеть конечного кольца /Н.И. Червяков // Регистрация – 20.06.2006. Опубл. –2008.

7 Червяков, Н.И. Реализация модулярного умножения нейронной сетью конечного кольца / Н.И. Червяков, В.А. Кучуков // Сборник трудов международной технической конференции “Современные технологии в нефтегазовом деле – 2015”. – Октябрьский, Башкортостан, РФ, 13 марта 2015. – Уфа: Аркаим, 2015. – С. 415–420.