УДК 681:519

Е.В. ЗАГУМЕННАЯ[1], С.О. МОРОЗ[1], В.О. ЖАДАН[2], В.А. КРАСНОБАЕВ[2]

[1] *Харьковский национальный технический университет сельского хозяйства им. П. Василенко, Украина*

[2] *Полтавский национальный технический университет им. Ю. Кондратюка, Украина*

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ПРОЦЕССА ТАБЛИЧНОЙ РЕАЛИЗАЦИИ ОПЕРАЦИЙ АЛГЕБРАИЧЕСКОГО УМНОЖЕНИЯ В КЛАССЕ ВЫЧЕТОВ

В литературе уже были представлены математические модели, на основании которых реализованы табличные методы и алгоритмы модульного умножения чисел в непозиционной системе счисления класса вычетов. Недостаток этих математических моделей состоял в том, что их использование не дает возможности создать табличный метод реализации операции алгебраического умножения в классе вычетов. В статье предлагается математическая модель процесса табличной реализации операции алгебраического умножения в классе вычетов. Данная модель рекомендована к практическому применению при разработке методов и процедур быстрой обработки криптографических алгоритмов.

Ключевые слова: *система обработки криптографической информации, табличная реализации модульных операции, класс вычетов.*

Введение

Масштабы и сложность задач, которые решаются современными системами и средствами обработки целочисленной информации (СОИ), обуславливает к ним повышенные требования по качеству обработки информации. Решение широкого круга сложных вычислительных задач требует (например, реализация несимметричных криптографических алгоритмов, основанных на использовании операций над эллиптическими кривыми) значительных объемов расчетов, которые проводятся в реальном времени функционирования СОИ. В этом аспекте поиск методов и средств повышения производительности обработки цифровой информации, является актуальным [1, 2].

В любой позиционной системе счисления (ПСС) выполнение арифметических операций предполагает последовательную обработку всех разрядов операндов по правилам, определяемым содержанием данной операции, и не может быть закончено до тех пор, пока не будут последовательно определены значения всех промежуточных результатов с учетом всех межразрядных связей операндов. Таким образом, ПСС, в которых представляется и обрабатывается информация в современных вычислительных машинах, обладают существенным недостатком – наличием логических связей между двоичными разрядами в обрабатываемых операндах. Данный недостаток оказывает существенное влияние на методы реализации арифметических операций, усложняют аппаратуру и ограничивают быстродействие. Поэтому естественно изыскание такой машинной арифметики, в которой бы поразрядные связи были бы ослаблены, либо отсутствовали вообще. Отметим, любая система счисления в большей степени влияет на структуру и принципы функционирования операционного устройства (ОУ) СОИ.

Поиск путей повышения производительности обработки информации позиционных СОИ реального времени привел к необходимости проведения исследований возможности использования табличного метода (табличной арифметики) реализации модульных операций. В общем случае табличное ОУ СОИ, предназначенное для реализации арифметических операций (которые реализуется в унитарном коде), представляет собой двухвходовое постоянное запоминающее устройство (ПЗУ). Для каждого из входов ПЗУ количество входных шин для l-байтового (8l двоичных разряда) ОУ равно 2^{8l}. При этом общее количество логических схем совпадения "И" в узлах ПЗУ (которое в основном и определяет общее количество оборудования табличного ОУ СОИ) равно $N_{l\,ПСС} = 2^{8l} \times 2^{8l} = 2^{16l}$. Исходя из этого, очевидно, что табличная реализация целочисленных модульных арифметических операций в ПСС может быть целесообразна только для значения l=1. Действительно, в этом случае $N_{1ПСС} = 2^{16} = 65536$, что является приемлемым количеством оборудования ОУ для современного развития элементной базы. Однако, как отмечалось выше, тенденция развития систем и средств обработки криптографической информации (СОКИ) направлена на увеличение длины разрядной сетки СОИ. Уже сейчас необходимо для

практического использования СОКИ с l=4 и l=8. В этом случае $N_{4ПСС}=2^{32}\times2^{32}=2^{64}$ и $N_{8ПСС}=2^{64}\times2^{64}=2^{128}$. Если учесть, например, что $2^{32}=4294967296$, $2^{64}=18446744073709551616$, а $2^{128}\approx3{,}4\times10^{38}$, то очевидно, что табличный метод реализации арифметических операций в ПСС практически не применим.

Иные результаты использования табличного метода реализации арифметических операций можно получить, если рассмотреть СОКИ в непозиционной системе счисления класса вычетов (КВ). Класс вычетов обладает уникальным свойством независимости друг от друга остатков по принятой системе оснований. Эта независимость открывает широкие возможности в построении не только новой машинной арифметики, но и принципиально новой схемной реализации СОКИ, которая в свою очередь заметно расширяет применение табличной арифметики [3, 4].

Действительно, в общем случае для l-байтовых машинных слов, при реализации алгоритмов модульной обработки информации для табличного ОУ СОИ в КВ не обходимо $N_{lKB}=\sum_{i=1}^{n} m_i^2$ схем совпадения И, а для ОУ СОИ в КВ с $l=4$ и $l=8$ соответственно имеем $N_{4KB}=2397$ и $N_{8KB}=13275$, что вполне приемлемо при реализации арифметических операций сложения, вычитания и умножения тем более используя современную элементную микроэлектронную базу. Вышеизложенное обстоятельство подтверждает важность, целесообразность и эффективность проведения практических исследований и разрабки табличных методов и алгоритмов реализации модульных операций в КВ. Отметим основные достоинства табличного метода построения ОУ СОИ в КВ:

Во-первых, высокое быстродействие выполнения арифметических операций. Результат операции может быть получен в момент поступления входных операндов в табличный вычислитель, т.е. практически за один такт работы СОИ. Таким образом, время выполнения арифметических операций в КВ сравнимо с тактовой частотой вычислителя, что принципиально невозможно для позиционных вычислительных машин при существующей элементной базе.

Во-вторых, табличные ОУ имеют высокую надежность, так как реализуются в виде набора, по числу n модулей m_i КВ, компактных ПЗУ. В этом случае весь тракт, состоящий из n (по числу модулей m_i КВ), обработки информации ОУ строится по блочному принципу, что улучшает безотказность и ремонтопригодность СОИ.

В-третьих, отметим простоту технической реализации ОУ СОИ в КВ, состоящего в основном из регистров, табличных сумматоров, шифраторов и дешифраторов и унификацию его оборудования для произвольного модуля $\{m_i\},(i=\overline{1,n})$

Отметим, необходимость разработки методов и алгоритмов арифметического умножения чисел необходимо предварительно иметь и в дальнейшем использовать математическую модель (ММ) процесса табличной реализации операции модульного умножения в КВ.

В литературе описаны математические модели, на основании которых реализованы табличные методы и алгоритмы модульного умножения чисел в непозиционной системе счисления класса вычетов [3-4]. Поиск путей упрощения структуры табличного ОУ СОИ обусловил необходимость совершенствования ММ, методов и алгоритмов реализации модульных операций, позволяющих повысить эффективность применения табличной арифметики в КВ. Так в [4] представлена математическая модель процесса табличной реализации операции арифметического модульного умножения в КВ. Особенностью реализации данной модели является возможность уменьшения количества оборудования ОУ СОИ за счет сокращения на (50-70)% логических элементов "И" в узлах таблицы ПЗУ, непосредственно реализующих операцию модульного умножения по произвольному m_i модулю КВ. Это возможно за счет использования свойств симметрии таблицы реализации $a_i b_i (\mathrm{mod}\, m_i)$ модульной операции умножения.

В КВ число А представляется в виде совокупности остатков $\{a_i\}$ по n модулям (основаниям) $\{m_i\}$, где $a_i=A-[A/m_i]\cdot m_i$; $M=\prod_{i=1}^{n} m_i$. В этом случае число А в КВ представляется в следующем виде $A=(a_1,a_2,...,a_n)$.

Пусть задана пара операндов $A=(a_1,...,a_n)$ и $B=(b_1,...,b_n)$ в КВ с попарно взаимно простыми основаниями $m_1,\ldots,m_n$. В соответствии с правилами выполнения арифметических операций в КВ каждой паре остатков a_i и b_i ставится в соответствие величина $(a_i \otimes b_i)\bmod m_i$.Таким образом, весь машинный тракт вычислительной операции $(A\otimes B)\bmod M$ в КВ можно представить в виде n независимых однотипных ПЗУ.

Рассмотрим процедуру реализации операции модульного умножения (наиболее трудоемкую арифметическую операцию). Составим таблицу из числовых значений $a_i b_i (\mathrm{mod}\, m_i)$.

Эта таблица симметрична относительно диагоналей, вертикали и горизонтали, проходящих между числами $\frac{(m_i-1)}{2}$ и $\frac{(m_i+1)}{2}$ для m_i – нечетного числа.

Симметричность относительно левой диагонали определяется коммутативностью операции $a_i\cdot b_i=b_i\cdot a_i$ умножения.

Симметричность относительно правой диагонали определяется тем, что

$$a_i \cdot b_i \equiv [(m_i - b_i)(m_i - a_i)] \bmod m_i.$$

Симметричность относительно вертикали и горизонтали определяется из условия кратности по модулю m_i суммы симметричных чисел:

$$a_i b_i \equiv [m_i - a_i(m_i - b_i)] \bmod m_i,$$
$$a_i b_i \equiv [m_i - b_i(m_i - a_i)\}] \bmod m_i.$$

Используя свойства симметрии можно полностью восстановить таблицу данных модульного умножения $a_i b_i (\bmod m_i)$. Для этого достаточно иметь числовую информацию только ее восьмой части. Отсюда возникает возможность упростить таблицу (уменьшить количество схем совпадения ПЗУ) модульного умножения. Для реализации операции $a_i b_i (\bmod m_i)$ представляется наиболее эффективным, с точки зрения быстродействия выполнения операции умножения, в четыре раза уменьшить таблицу модульного умножения. Для решения поставленной задачи необходимо ввести признак, определяющий местоположение входных чисел в каждом из четырех квадрантов таблицы $a_i b_i (\bmod m_i)$.

Рассмотрим один из возможных вариантов кодирования входных операндов a_i и b_i таблицы по модулю m_i посредством кода информационного сжатия данных (КИСД). Пусть даны входные операнды a_i и b_i. Значения a_i (или b_i), лежащие в диапазоне $\left[0, \frac{m_i - 1}{2}\right)$, могут быть закодированы произвольным образом, а значения a_i (или b_i), лежащие в диапазоне $\left[\frac{m_1 + 1}{2}, m_i - 1\right)$, кодируются, как $m_i - a_i$ (или $m_i - b_i$). Для отличия диапазонов вводится признак γ_a (γ_b) КИСД, определенный следующим образом:

$$\gamma_a\ (\gamma_b) = \begin{cases} 0, \text{ если } 0 \le a_i (b_i) \le \dfrac{m_i - 1}{2}, \\ 1, \text{ если } \dfrac{m_i + 1}{2} \le a_i (b_i) \le m_i - 1, \end{cases}$$

где $0 \le a^*(b^*) \le (m_i - 1)/2$.

Процедура определения результата операции модульного умножения, посредством введенного кода информационного сжатия данных, следующий: если заданы два операнда в КИСД вида $a_i = (\gamma_a, a_i^*)$, $b_i = (\gamma_b, b_i^*)$, то для, того чтобы получить произведение этих чисел по модулю m_i, достаточно получить произведение $a_i^* b_i^* (\bmod m_i)$ и инвертировать его обобщенный признак γ_i в случае, если γ_a отлично от γ_b, т.е.

$$a_i b_i (\bmod m_i) = (\gamma_i, a_i^* b_i^* (\bmod m_i)),$$

где $\gamma_i = \begin{cases} \overline{\gamma_i}, \text{ если } \gamma_a \ne \gamma_b, \\ \gamma, \text{ если } \gamma_a = \gamma_b. \end{cases}$

Предложенный вариант реализации модульных операций в КВ позволяют оптимизировать структуру СОИ путем повышения эффективности использования табличной арифметики. Сокращение количества оборудования ПЗУ, составляющих основную часть ОУ, позволяет повысить надежностные показатели (увеличить вероятность безотказной работы P(t), уменьшить время восстановления $T_в$) и улучшить эксплуатационно-технические показатели (уменьшить массу и габаритные размеры, уменьшить потребляемую мощность и улучшить техническое обслуживание СОИ в КВ).

Учитывая КИСД, математическая модель процесса табличной реализации в положительном числовом диапазоне двух чисел в КВ представится следующими математическими соотношениями:

$$\begin{aligned} C = A \cdot B (\bmod M) &= [(a_1, a_2, ..., a_i, ..., a_n) \cdot (b_1, b_2, \\ &,..., b_i, ..., b_n)] \bmod M = [(a_1 \cdot b_1) \bmod m_1, (a_2 \cdot \\ &\cdot b_2) \bmod m_2, ..., (a_i \cdot b_i) \bmod m_i, ..., (a_n \cdot \\ &\cdot b_n) \bmod m_n] = \{[(\gamma_{a_1}, a_1^*) \cdot (\gamma_{b_1}, b_1^*)] \bmod m_1, \\ &[(\gamma_{a_2}, a_2^*) \cdot (\gamma_{b_2}, b_2^*) \bmod m_2], ..., (\gamma_{a_i}, a_i^*) \cdot (\gamma_{b_i}, \\ &b_i^*) \bmod m_i], ..., [(\gamma_{a_n}, a_n^*) \cdot (\gamma_{b_n}, b_n^*)] \bmod m_n\} \\ &= \{[\gamma_1, (a_1^* \cdot b_1^*) \bmod m_1], [\gamma_2, (a_2^* \cdot \\ &\cdot b_2^*) \bmod m_2], ..., [\gamma_i, (a_i^* \cdot b_i^*) \bmod m_i], ..., \\ &..., [\gamma_n, (a_n^* \cdot b_n^*) \bmod m_n]\} = \\ &= (c_1, c_2, ..., c_i, ..., c_n). \end{aligned} \quad (1)$$

При этом признак γ_{a_i} (γ_{b_i}) кода (γ_{a_i}, a_i^*) ((γ_{b_i}, b_i^*)) КИСД таблицы модульного умножения для произвольного m_i модуля КВ определяется следующим образом. Для m_i - четного

$$\gamma_{a_i}(\gamma_{b_i}) = \begin{cases} 0, \text{ если } 0 \le a_i (b_i) \le m_i / 2, \\ 1, \text{ если } m_i / 2 < a_i (b_i) \le m_i - 1. \end{cases} \quad (2)$$

Для m_i - нечетного

$$\gamma_{a_i}(\gamma_{b_i}) = \begin{cases} 0, \text{ если } 0 \le a_i (b_i) \le (m_i - 1)/2, \\ 1, \text{ если } (m_i - 1)/2 < a_i (b_i) \le m_i - 1. \end{cases} \quad (3)$$

при чем $0 \le a_i (b_i) \le m_i - 1$

Числовая часть a_i^* (b_i^*) КИСД определяется так.

Для m_i - четного это будет

$$a_i^*(b_i^*) = \begin{cases} a_i (b_i), \text{если } 0 \le a_i (b_i) \le m_1 / 2, \\ \overline{a_i}(\overline{b_i}) = m_1 - a_i (b_i), \text{если } m_1 / 2 < a_i (b_i) \le m_1, \end{cases} \quad (4)$$

при этом $0 \le a_i^*(b_i^*) \le m_i / 2$.

Для m_i -нечетного

$$a_i^*(b_i^*)=\begin{cases} a_i(b_i), \text{если } 0\le a_i(b_i)\le (m_i-1)/2, \\ \overline{a_i}(\overline{b_i})=m_i-a_i(b_i), \text{если } (m_i-1)/2<a_i(b_i)\le m_i-1, \end{cases} \quad (5)$$

при этом $0 \le a_i^*(b_i^*) \le (m_i - 1)/2$.

Если результат $(a_i \cdot b_i) \bmod m_i$ модульного умножения определяется в КИСД как $[\gamma_i, (a_i^* \cdot b_i^*) \bmod m_i]$, тогда

$$(a_i \cdot b_i) \bmod m_i = \begin{cases} (a_i^* \cdot b_i^*) \bmod m_i, \\ \text{если } (\gamma_{a_i} + \gamma_{b_i}) = 0 \pmod 2; \\ m_i - (a_i^* \cdot b_i^*) \bmod m_i, \\ \text{если } (\gamma_{a_i} + \gamma_{b_i}) = 1 \pmod 2, \end{cases} \quad (6)$$

при этом $0 \le (a_i^* \cdot b_i^*) \bmod m_i \le m_i - 1$.

Таким образом, совокупность выражений (2)-(6) представляет собой ММ процесса табличной реализации модульного арифметического умножения в КВ.

Недостаток рассмотренной ММ состоит в том, что ее использования не дает возможности создать табличный метод реализации операции алгебраического умножения в КВ.

Цель статьи – разработать ММ процесса табличной реализации умножения в КВ как для положительного, так и для отрицательного числовых диапазонов.

Основная часть

Для построения ММ процесса табличной реализации умножения в КВ, как для положительного, так и для отрицательного числовых диапазонов представим входные числа A и B в следующем виде (искусственная форма представления чисел в КВ [4])

$A' = A + m/2$ и $B' = B + m/2$, для m – четных чисел;

$A' = A + (m-1)/2$ и $B' = B + (m-1)/2$,

для m – нечетных чисел.

Если, например, m четное число, тогда выполняются следующие соотношения

$$\begin{cases} -m/2 \le A(B) < m/2, \\ 0 \le A'(B') < m-1, \\ -m/2 \le A \cdot B < m/2, \\ 0 \le (A \cdot B)' < m-1. \end{cases}$$

Очевидно, что

$$(A \cdot B)' = A \cdot B + m/2. \quad (7)$$

Тогда имеем

$$(A' \cdot B') \bmod m = \left[(A + m/2)(B + m/2) \right] \bmod m =$$
$$= \left[AB(\bmod m/2) + m/2 \cdot (A + B + m/2) \right] \bmod m. \quad (8)$$

Из выражения (7) очевидно, что

$$A \cdot B = A' \cdot B' - m/2 \cdot (A + B + m/2). \quad (9)$$

Подставим выражение (9) в формулу (7). Получим, что

$$(A \cdot B)' = A' \cdot B' - m/2 \cdot (A + B + m/2) + m/2. \quad (10)$$

В выражении (10) есть член, который имеет численное значение m/2. Он и обуславливает ошибку в вычислении значения $A' \cdot B' (\bmod m)$. Таким образом формулы для вычисления AB(mod m) имеют следующий вид для m четных чисел

$$\left[(A \cdot B) \bmod m/2 \right]' = (A' \cdot B') \bmod m + m/2, \quad (11)$$

или

$$\left[(A \cdot B) \bmod m/2 \right]' = (A' \cdot B') \bmod m. \quad (12)$$

Для m нечетного имеем

$$\left[(A \cdot B) \bmod (m-1)/2 \right]' = (A' \cdot B') \bmod m + (m-1)/2, \quad (13)$$

или

$$\left[(A \cdot B) \bmod (m-1)/2 \right]' = (A' \cdot B') \bmod m. \quad (14)$$

Учитывая выражения (7) ÷ (14), построим ММ процесса модульного умножения для положительного и отрицательного (алгебраическое умножение) целочисленных числовых диапазонов.

$$\begin{aligned} &a_i' = a_i + m_i/2, a_i' = a_i' + (m_i - 1)/2; \\ &a_i' = [\gamma_{a_i}', (a_i')^*]; \\ &b_i' = b_i + m_i/2, b_i' = b_i' + (m_i - 1)/2; \\ &b_i' = [\gamma_{b_i}', (b_i')^*]. \end{aligned} \quad (15)$$

Для m_i - четного

$$\gamma_{a_i}'(\gamma_{b_i}') = \begin{cases} 0, \text{ если } 0 \le a_i'(b_i') \le m_i/2, \\ 1, \text{ если } m_i/2 < a_i'(b_i') \le m_i - 1. \end{cases} \quad (16)$$

Для m_i - нечетного

$$\gamma_{a_i}'(\gamma_{b_i}') = \begin{cases} 0, \text{ если } 0 \le a_i'(b_i') \le (m_i - 1)/2, \\ 1, \text{ если } (m_i - 1)/2 < a_i'(b_i') \le m_i - 1. \end{cases} \quad (17)$$

Числовая часть $(a_i')^* [(b_i')^*]$ КИСД определяется следующим образом.

Для m_i – четного

$$(a_i')^*[(b_i')^*] = \begin{cases} a_i'\ (b_i'), \\ \text{если } 0 \le a_i'(b_i') \le m_i / 2; \\ \overline{a_i'}\ (\overline{b_i'}) = m_i - a_i'(b_i'), \\ \text{если } m_i / 2 < a_i'(b_i') \le m_i - 1. \end{cases} \quad (18)$$

при этом $0 \le (a_i')^*\ [(b_i')^*] \le m_i / 2.$

Для m_i – нечетного числа

$$(a_i')^*[(b_i')^*] = \begin{cases} a_i'\ (b_i'), \\ \text{если } 0 \le a_i'(b_i') \le (m_i - 1) / 2; \\ \overline{a_i'}\ (\overline{b_i'}) = m_i - a_i'(b_i'), \\ \text{если } (m_i - 1) / 2 < a_i'(b_i') \le m_i - 1. \end{cases} \quad (19)$$

при этом $0 \le (a_i')^*\ [(b_i')^*] \le (m_i - 1) / 2.$

Результат $(a_i' \cdot b_i') \bmod m_i$ операции представляется в КИСД, т.е. в виде $\left\{\gamma_i', [(a_i')^*(b_i')^*] \bmod m_i\right\}$, тогда

$$(a_i' \cdot b_i') \bmod m_i = \begin{cases} [(a_i')^* \cdot (b_i')^*] \bmod m_i, \\ \text{если } (\gamma'_{a_i} + \gamma'_{b_i}) = 0 \ (\text{mod } 2); \\ m_i - [(a_i')^* \cdot (b_i')^*] \bmod m_i, \\ \text{если } (\gamma'_{a_i} + \gamma'_{b_i}) = 1 \ (\text{mod } 2). \end{cases} \quad (20)$$

при этом $0 \le [(a_i')^* \cdot (b_i')^*] \bmod m_i \le m_i - 1.$

Формула для определения произведения двух чисел в КВ имеет следующий вид

$$\begin{aligned} &(A \cdot B) \bmod M = (A' \cdot B') \bmod M = \\ &= [(a_1', a_2', ..., a_i', ..., a_n') \cdot \\ &\cdot (b_1', b_2', ..., b_i', ..., b_n')] = \\ &= [(a_1' \cdot b_1') \bmod m_1, (a_2' \cdot b_2') \bmod m_2, ..., \\ &, ..., (a_i' \cdot b_i') \bmod m_i, ..., (a_n' \cdot b_n') \bmod m_n]. \end{aligned} \quad (21)$$

Так, как все модули $\{m_i\}$, $i = \overline{1, n}$ КВ, (за исключением возможно только одного основания), нечетные числа, то в дальнейшем, без потери общности рассуждений, будем считать что основание КВ нечетные числа. Формула (21) с учетом КИСД имеет следующий вид

$$\begin{aligned} &(A' \cdot B') \bmod M = \\ &= (\{[\gamma'_{a_1}, (a_1')^*] \cdot [\gamma'_{b_1}, (b_1')^*]\} \bmod m_1, \\ &\{[\gamma'_{a_2}, (a_2')^*] \times [\gamma'_{b_2}, (b_2')^*]\} \bmod m_2, ..., \\ &..., \{[\gamma'_{a_i}, (a_i')^*] \cdot [\gamma'_{b_i}, (b_i')^*]\} \bmod m_i, ..., \\ &..., [\gamma'_{a_n}, (a_n')^*] \cdot [\gamma'_{b_n}, (b_n')^*]\} \bmod m_n) = \\ &= (\{\gamma_1', [(a_1')^* \cdot (b_1')^*] \bmod m_1\}, \\ &\{\gamma_2', [(a_2')^* \cdot (b_2')^*] \bmod m_2\}, ..., \\ &..., \{\gamma_i', [(a_i')^* \cdot (b_i')^*] \bmod m_i\}, ..., \\ &...., \{\gamma_n', [(a_n')^* \times (b_n')^*] \bmod m_n\}), \end{aligned} \quad (22)$$

где

$$\begin{aligned} &(a \cdot b_i') \bmod m_i = \{[\gamma'_{a_i}, (a_i')^*] \cdot \\ &\cdot [\gamma_{b_s}, (b_i')^*]\} \bmod m_i = \\ &= \{\gamma_i', [(a_i')^* \cdot (b_i')^*]\} \bmod m_i. \end{aligned} \quad (23)$$

Исходя из (22) ÷ (23) где, а также учитывая, что (15) ÷ (21), для m – нечетного получим следующие соотношение для реализации модульной операции алгебраического умножения в КВ

$$\begin{cases} \{(a_i \cdot b_i) \bmod [(m_i - 1) / 2]\}' = \\ = \{[(\gamma_{a_i}, a_i) \cdot (\gamma_{b_i}, b_i)] \bmod [(m_i - 1) / 2]\}' = \\ = (a_i' \cdot b_i') \bmod m_i + (m_i - 1) / 2 = \\ = \{[\gamma'_{a_i}, (a_i')^*] \cdot [\gamma'_{b_i}, (b_i')^*]\} \bmod m_i + \\ + (m_i - 1) / 2 = \{\gamma_i', [(a_i')^* \cdot (b_i')^*] \bmod m_i + \\ + (m_i - 1) / 2; \\ \{(a_i \cdot b_i) \bmod [(m_i - 1) / 2]\}' = \\ = \{[(\gamma_{a_i}, a_i) \cdot (\gamma_{b_i}, b_i)] \bmod [(m_i - 1) / 2]\}' = \\ = (a_i' \cdot b_i') \bmod m_i = \{[\gamma'_{a_i}, (a_i')^*] \cdot \\ \cdot [\gamma'_{b_i}, (b_i')^*]\} \bmod m_i = \\ = \{\gamma_i', [(a_i')^* \cdot (b_i')^*] \bmod m_i\}. \end{cases} \quad (24)$$

Для m_i – четного числа получим

$$\begin{cases} (a_i \cdot b_i) \bmod [m_i / 2]\}' = \{[(\gamma_{a_i}, a_i) \cdot \\ \cdot (\gamma_{b_i}, b_i)] \bmod [m_i / 2]\}' = \\ = (a_i' \cdot b_i') \bmod m_i + m_i / 2 = \\ = \{[\gamma'_{a_i}, (a_i')^*] \cdot [\gamma'_{b_i}, (b_i')^*]\} \bmod m_i + \\ + m_i / 2 = \{\gamma_i', (a_i')^* \cdot (b_i')^*]\} \bmod m_i + m_i / 2; \\ \{(a_i \cdot b_i) \bmod [m_i / 2]\}' = \{[(\gamma_{a_i}, a_i) \cdot \\ \cdot (\gamma_{b_i}, b_i)] \bmod [m_i / 2]\}' = \\ = (a_i' \cdot b_i') \bmod m_i = \{[\gamma'_{a_i}, (a_i')^*] \cdot \\ \cdot [\gamma'_{b_i}, (b_i')^*]\} \bmod m_i = \\ = \{\gamma_i', [(a_i')^* \cdot (b_i')^*] \bmod m_i. \end{cases} \quad (25)$$

Соотношения (24) ÷ (25) представляет собой математическую модель процесса табличной реализации операций алгебраического умножения в КВ.

Заключение

Таким образом, на основании свойств КВ в статье синтезирована математическая модель процесса табличной реализации модульного умножения, как для положительных, так и для отрицательных числовых диапазонов обработки информации СОИ. Данная модель рекомендована к практическому применению при разработке методов и алгоритмов быстрой обработки криптографической информации.

Литература

1. Качко, Е.Г. Параллельные вычисления в криптографических алгоритмах на основе эллиптических кривих [Текст]/ Е.Г. Качко, С.С. Батюшко // Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения безопасности информации. – 2010. – Т. 9, № 3. – С. 370 – 373.

2. Бессалов, А.В. Изоморфизм дивизоров и параллельных точек гиперэллиптической кривой рода два [Текст] / А.В. Бессалов, А.В. Неласая. // Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения безопасности информации. – 2010. – Т. 9, № 3. – С. 418 – 420.

3. Method of bit-by-bit tabular realization of arithmetic operations in the system of residual classes [Текст] / S.A. Koshman, V.I. Barsov, V.A. Krasnobayev, K.V. Yaskova, N.S. Derenko // Радіоелектронні і комп'ютерні системи. – 2009. – № 5 (39). – С. 44 – 48.

4. Акушский, И.Я. Машинная арифметика в остаточных классах [Текст] / И.Я. Акушский, Д.И. Юдицкий. – М.: Советское радио, 1968. – 440 с.

Поступила в редакцию 21.12.2011

Рецензент: д-р техн. наук, проф., зав. каф. автоматизации и компьютерных технологий И.А. Фурман, Харьковский национальный технический университет сельского хозяйства имени Петра Василенка, Харьков.

МАТЕМАТИЧНА МОДЕЛЬ ПРОЦЕСУ ТАБЛИЧНОЇ РЕАЛІЗАЦІЇ ОПЕРАЦІЇ АЛГЕБРОЇЧНОГО МНОЖЕННЯ В КЛАСІ ВИЧЕТІВ

К.В. Загуменна, С.О. Мороз, В.О. Жадан, В.А. Краснобаєв

У літературі вже були представлені математичні моделі, на підставі яких реалізовані табличні методи і алгоритми модульного множення чисел в непозиційній системі числення класів залишків. Недолік цих математичних моделей полягав в тому, що їх використання не дає можливості створити табличний метод реалізації операції алгебраїчного множення в класі залишків. У статті пропонується математична модель процесу табличної реалізації операції алгебраїчного множення в класі залишків. Дана модель рекомендована до практичного вживання при розробці методів і процедур швидкої обробки криптографічних алгоритмів.

Ключові слова: система обробки криптографічної інформації, таблична реалізації модульних операції, клас вичетів.

A MATHEMATICAL MODEL OF PROCESS OF TABULAR REALIZATION OF OPERATION OF ALGEBRAIC INCREASE IS IN THE CLASS OF TAKE OUTS

K.V. Zagumenna, S.O. Moros, V.O. Zhadan, V.A. Krasnobaev

Mathematical models on the basis of which tabular methods and algorithms of module increase of numbers are realized in the unposition number of class of take-outs system were already presented in literature. The lack of these mathematical models consisted of that their use does not enable to create the tabular method of realization of operation of algebraic increase in the class of take-outs. In the article the mathematical model of process of tabular realization of operation of algebraic increase is offered in the class of take-outs. This model is recommended to practical application at development of methods and procedures of rapid treatment of cryptographic algorithms.

Key words: system of treatment of cryptographic information, tabular to realization of module operations, class of take-outs.

Загуменная Екатерина Викторовна – ассистент кафедры автоматизации и компьютерно-интегрированных технологий, Харьковский национальный технический университет сельского хозяйства им. Петра Василенка, Харьков, Украина

Мороз Сергей Александрович – аспирант кафедры автоматизации и компьютерно-интегрированных технологий, Харьковский национальный технический университет сельского хозяйства им. Петра Василенка, Харьков, Украина.

Жадан Валентина Олеговна – магистрант кафедры компьютерной инженерии, Полтавский национальный технический университет им. Ю. Кондратюка, Полтава, Украина.

Краснобаев Виктор Анатольевич – д-р техн. наук, профессор, заведующий кафедры компьютерной инженерии, Полтавский национальный технический университет им. Ю. Кондратюка, Полтава, Украина.