УДК 681.3:681.04

Методы реализации криптографических RSA преобразований на основе использования модулярной системы счисления

В. А. Краснобаев, С. О. Мартыненко, Л. С. Сорока
Харьковский национальный университет имени В.Н. Каразина, Украина

С целью уменьшения времени реализации криптографических RSA преобразований в статье рассматриваются методы быстрой обработки информации. Разработанные методы основываются на использовании принципа кольцевого сдвига в модулярной системе счисления (МСС). Применение МСС позволило эффективно, с точки зрения повышения быстродействия реализации криптографических преобразований с открытым ключом, организовать процесс реализации модульных целочисленных арифметических операций.

Ключевые слова: *быстрая обработка информации, криптографические RSA преобразования, открытый ключ, кольцевой сдвиг, модулярная система счисления.*

З метою зменшення часу реалізації криптографічних перетворень RSA в статті розглядаються методи швидкої обробки інформації. Розроблені методи грунтуються на використанні принципу кільцевого зрушення в модулярної системі числення (МСЧ). Застосування МСЧ дозволило ефективно, з погляду підвищення швидкодії реалізації криптографічних перетворень з відкритим ключем, організувати процес реалізації модульних цілочисельних арифметичних операцій.

Ключові слова: *швидка обробка інформації, криптографічні перетворення RSA, відкритий ключ, кільцеве зрушення, модулярна система числення, цілочисельні арифметичні операції.*

With the purpose of diminishing of time of realization of cryptographic RSA transformations to the article the methods of rapid treatment of information are examined. The developed methods are based on the use of principle of circular change in the modular number system (MNS). Application of MNS allowed effectively, from point of increase of fast-acting of realization of cryptographic transformations with the opened key, to organize the process of realization of module integer-valued arithmetic operations.

Key words: *rapid treatment of information, cryptographic RSA transformations, opened key, circular change, modular number system, integer-valued arithmetic operations.*

1. Общая постановка задачи и ее актуальность

В настоящее время современные криптопреобразования с открытым ключом основываются на преобразованиях на алгебраических кривых (эллиптические кривые (ЭК), гиперэллиптические кривые (ГЭК), кривые Пикарда (КП) и суперэллиптические кривые (СУ)), а также на RSA системах. Существующая тенденция развития криптографических методов обработки информации направлена на увеличения длины ключей, что в свою очередь приводит к снижению быстродействия криптографических преобразований с открытым ключом. Это особенно критично для обеспечения заданного уровня стойкости при реализации криптопреобразований на ЭК в специальных системах и устройствах с существующими ограничениями по объему памяти и массогабаритным характеристикам, т.е. в тех случаях, где нет возможности использовать мощные стационарные высокопроизводительные вычислители с большой разрядной сеткой. Данное обстоятельство обуславливает важность и

актуальность поисков методов повышения производительности, надежности и достоверности криптопреобразований [1-3].

2. Истоки исследования авторов

Анализ методов повышения производительности СУ в якобиане ГЭК позволил теоретически обосновать и практически показать зависимость производительности реализации операций СУ в якобиане ГЭК от совокупности следующих основных характеристик: от вида реализации криптопреобразований (программная, аппаратная или программно-аппаратная); от вида алгоритма СУ дивизоров; от заданного базового поля, над которым задается данная кривая; от типа кривой; от значений коэффициентов кривой; от выбранной системы координат, в которой представлены дивизоры якобиана ГЭК (аффинная, проективная, взвешенная и смешанная); от принятого метода арифметических преобразований в якобиане и пр. Известные методы реализации алгоритмов СУ (метод сложения дивизоров Кантора, метод Коблица, методы арифметических преобразований дивизоров в якобиане ГЭК второго, третьего и четвертого рода, методы сложения дивизоров различного веса, метод Карацубы для умножения и приведения по модулю в поле полиноминальных функций, метод основанный на некоторых результатах “Китайской теоремы об остатках” и пр.) не всегда удовлетворяют требованиям по производительности криптопреобразований. В тоже время, в литературе [4-7] показана высокая эффективность применения кодов модулярной арифметики – модулярной системы счисления (МСС) - при решении отдельных задач быстрой обработки цифровой информации (решение задач цифровой фильтрации, задачи реализации БПФ, ДПФ и пр.).

3.Нерешенность проблемы и цели работы

Вышеизложенное обстоятельство и обуславливает важность и актуальность поиска методов и средств повышения производительности, в первую очередь, RSA криптопреобразований на основе использования МСС. Это обусловлено тем, что предложенная в 1977 году система RSA наиболее широко используемая сейчас криптосистема с открытым ключом [2, 3, 8].

Цель статьи – разработка метода быстрой реализации криптографических преобразований с открытым ключом, а также структурной схемы операционного устройства (ОУ) спецпроцессора обработки криптографической информации (СОКИ) на основе использования МСС.

В [4, 6, 7] исследовано влияние основных свойств (независимость, равноправность и малоразрядность остатков, представляющих операнд) МСС на структуру и принципы функционирования СОКИ в МСС. В частности, показано, что малоразрядность остатков в представлении чисел в модулярной арифметике дает возможность широкого выбора вариантов системотехнических решений при реализации целочисленных модульных арифметических операций.

Известно [5], что существует четыре принципа реализации арифметических операций в МСС: сумматорный принцип (на базе малоразрядных двоичных сумматоров по модулю m_i МСС [1]); табличный принцип (на основе использования ПЗУ); прямой логический принцип реализации арифметических операций, основанный на описании и реализации модульных операций на уровне систем переключательных функций,

посредством которых формируются значения результата модульной операции (в качестве элементной базы для технической реализации данного принципа целесообразно использовать систолические и программируемые логические матрицы, а также ПЛИС); принцип кольцевого сдвига (ПКС), основанный на использовании кольцевых регистров сдвига (КРС).

Отсутствие процесса переноса между остатками числа, представленного в МСС (внутри каждого остатка по модулю m_i между двоичными разрядами переносы существуют) в обрабатываемых в СОКИ операндах в процессе криптопреобразований (при реализации модульных операций) на основе ПКС является одной из главных и наиболее привлекательных особенностей МСС.

4. Используемый метод решения задачи

В позиционной системе счисления (ПСС) выполнение арифметической операции предполагает последовательную обработку разрядов операндов по правилам, определяемым содержанием данной операции, и не может быть закончена до тех пор, пока не будут последовательно определены значения всех промежуточных результатов с учетом всех связей между разрядами.

Таким образом ПСС, в которой представляется и обрабатывается информация в современных СОКИ, обладает существенным недостатком – наличием межразрядных связей, которые накладывают свой отпечаток на методы реализации арифметических операций, усложняют аппаратуру, снижает достоверность вычислений и ограничивают быстродействие реализации криптографических преобразований. Поэтому естественно изыскание возможностей построения такой арифметики, в которой бы поразрядные связи отсутствовали. В этом плане обращает на себя внимание МСС. Данная непозиционная система счисления обладает ценным 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 машинной арифметики. Во многих литературных источниках отмечается, что одним из практических направлений повышения пользовательской производительности вычислительных средств является внедрение нетрадиционных методов представления и обработки информации в числовых системах с параллельной структурой, и в частности, в так называемых модулярных системах счисления, обладающих максимальным уровнем внутреннего параллелизма в организации процесса переработки информации. К таким системам счисления относится и МСС.

5. Общий подход к решению задачи

Рассмотрим существующие предпосылки к эффективному использованию в качестве системы счисления СОКИ модулярной системы счисления: в СОКИ обработка цифровой информации, как и в МСС, производится только с целочисленными числами; в СОКИ осуществляется реализация только модульных арифметических операций; реализация целочисленных модульных арифметических операций в СОКИ осуществляется в положительном числовом диапазоне; основными

операциями при реализации криптосистемы RSA (более 95%) являются операция модульного умножения и операция возведения чисел в квадрат по модулю m_i, наиболее эффективно (с точки зрения быстродействия выполнения модульных арифметических операций) реализуемых в МСС; с увеличением длины l машинного слова (разрядной сетки вычислителя (embedded processor, processor node) криптосистем), что характерно для современной тенденции развития СОКИ криптосистемы RSA, эффективность использования МСС возрастает; широкое использование КРС в СОКИ при реализации криптопреобразований RSA; нерешенность в ПСС задачи существенного повышения производительности и отказоустойчивости СОКИ; положительные предварительные результаты эффективности использования МСС для повышения пользовательской производительности и отказоустойчивости СОКИ реального времени.

В [9] сформулирован принцип реализации целочисленных арифметических операций в МСС - принцип кольцевого сдвига (ПКС), особенность которого заключается в том, что результат арифметической операции $(a_i \pm b_i) \bmod m_i$ по произвольному m_i модулю МСС, заданной совокупностью $\{m_j\}$ $(j = \overline{1,n})$ оснований, определяется без вычисления значений величин частичных сумм S_i и значений C_i переносов двоичного сумматора в ПСС, а только за счет циклических сдвигов заданной цифровой структуры. Действительно, известная теорема Кэли устанавливает изоморфизм между элементами конечной абелевой группы и элементами группы перестановок. В этом случае матрица сложения для произвольного m_i модуля МСС будет задана таблицей 1 (для m_i= 5 – таблицей 2).

Таблица 1. Таблица Кэли для произвольного значения m_i

β_i	α_i				
	0	1	2	...	$m_i - 1$
0	0	1	2	...	$m_i - 1$
1	1	2	3	...	0
2	2	3	4	...	1
...	...	...	...	...	...
$m_i - 1$	$m_i - 1$	0	1	...	$m_i - 2$

Таблица 2. Таблица Кэли для m_i = 5

β_i	α_i				
	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Одно из следствий теоремы Кэли является вывод о том, что отображение элементов абелевой группы на группу всех целых чисел является гомоморфным. Это обстоятельство позволяет организовать процесс определения результата арифметических операций в МСС посредством использования ПКС. Так, операнд в МСС представляется набором из n остатков $\{a_i\}$, образованных путем последовательного деления исходного числа A на n попарно простых чисел $\{\mathrm{m_i}\}$, для $(\mathrm{i}=\overline{1,\mathrm{n}})$. В этом случае совокупность остатков $\{\mathrm{m_i}\}$ непосредственно отождествляется с суммой n простых полей Галуа вида $\sum_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{GF}(\mathrm{m_i})$.

При рассмотрении метода реализации арифметических операций в МСС удобно и достаточно рассмотреть вариант для произвольного конечного поля Галуа $GF(m_i)$ при i=const, т. е. для конкретной приведенной системы вычетов по модулю $\mathrm{m_i}$. Пусть для заданной операции модульного сложения $(a_i + b_i) \bmod m_i$ в поле $\mathrm{GF}(\mathrm{m_i})$ составлена таблица Кэли (табл. 1). Из существования нейтрального элемента в поле $\mathrm{GF}(\mathrm{m_i})$ следует, что в таблице 1 есть строка (столбец), в которой элементы данного поля стоят в порядке возрастания, а из того факта, что в поле вычетов $\mathrm{GF}(\mathrm{m_i})$ эти элементы различны (порядок группы равен $\mathrm{m_i}$), следует, что в каждой строке (столбце) таблицы 1 содержатся все элементы поля ровно по одному разу. Использование перечисленных свойств позволяет реализовать операции модульного сложения и вычитания в МСС на основе использования ПКС, посредством n кольцевых $\mathrm{M} = \mathrm{m_i}([\log_2(\mathrm{m_i}-1)]+1)$ - разрядных сдвигающих регистров.

Пусть произвольная алгебраическая система представлена в виде $\mathrm{S} = \langle \mathrm{G}, \otimes \rangle$, где G - непустое множество; $\otimes$ - тип операции, определенной для любых двух элементов a_i, $b_i \in G$. Операция $\oplus$ сложения в множестве классов вычетов R, порожденных идеалом J, образует новое кольцо, называемое кольцом классов вычетов $\mathrm{R/J}$. Его можно представить в виде $\mathrm{Z/m_i}$, где Z - множество целых чисел $0,\ \pm1,\ \pm2,\ldots$. (Если основание $\mathrm{m_i}$ МСС - простое число, то $\mathrm{Z/m_i}$ - поле). Данное обстоятельство обусловливает возможность реализации арифметической операции сложения в МСС без межразрядных переносов путем кольцевого сдвига содержимого разрядов КСР.

6. Методы реализации криптографических преобразований

На основе предложенного в [9] ПКС в статье предлагается метод реализации арифметических операций в МСС - метод двоичного представления остатков (МДПО). Суть разработанного метода состоит в том, что исходная цифровая

структура для каждого модуля (основания) m_i МСС представляется в виде содержимого первой строки (столбца) таблицы Кэли модульного сложения (вычитания) $(a_i \pm b_i) \bmod m_i$ вида (рис. 1)

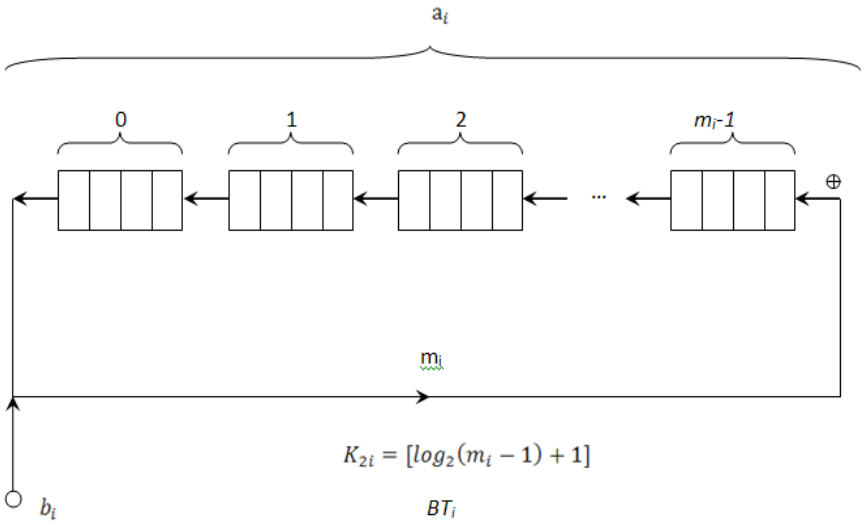

Рис. 1. Сумматор по модулю m_i в МСС

Исходную цифровую структуру содержимого КРС для каждого модуля m_i можно представить в виде (1), где $\|$- операция конкатенации (присоединения, склеивание); $P_v(a_v)$- k-разрядный двоичный код, соответствующий значению a_v-го остатка $(a_v = \overline{0, m_i - 1})$ числа по модулю m_i ; $k = \left[\log_2(m_i - 1) + 1\right]$

$$P_{\text{исх}}^{(m_i)} = \left[P_0(\alpha_0) \| P_1(\alpha_1) \| \ldots \| P_{m_i - 1}(\alpha_{m_i - 1}) \right]. \quad (1)$$

Для заданного конкретного модуля m_i=5, исходная цифровая структура содержимого КСР имеет вид

$$P_{\text{ñõ}}^{(5)} = \left[000 \| 001 \| 010 \| 011 \| 100 \right].$$

Таким образом, посредством используемых в ПСС кольцевых регистров сдвига легко реализовать арифметические операции в МСС. При этом степени циклических перестановок, исходя из (1), определяется следующими выражениями:

$$\left[P_0(\alpha_0)\left\|P_1(\alpha_1)\right\|...\left\|P_{m_i-1}(\alpha_{m_i-1})\right.\right]=\left[P_z(\alpha_z)\left\|P_{z+1}(\alpha_{z+1})\right\|...\left\|P_0(\alpha_0)\right\|...\left\|P_{m_i-1}(\alpha_{m_i-1})\right.\right]^Z, \quad (2)$$

$$\begin{aligned}\left[P_0(\alpha_0)\left\|P_1(\alpha_1)\right\|...\left\|P_{m_i-1}(\alpha_{m_i-1})\right.\right]^{-z}&=\left[P_{m_i-1-z}(\alpha_{m_i-1-z})\right\|...\left\|P_{m_i-z}(\alpha_{m_i-z1})\right\|\\&\left\|...\left\|P_0(\alpha_0)\right\|P_1(\alpha_1)\right\|...\left\|P_{m_i-z-2}(\alpha_{m_i-z-2})\right.\right].\end{aligned} \quad (3)$$

Отметим, что $\left[\mathrm{P_0(\alpha_0)}\left\|\mathrm{P_1(\alpha_1)}\right\|...\left\|\mathrm{P_{m_i-1}(\alpha_{m_i-1})}\right.\right]^{\mathrm{m_i}}=\varepsilon$, т.е. при $z = m_i$ все элементы упорядоченного множества $\left\{\mathrm{P_j(\alpha_i)}\right\}$ $(\mathrm{j}=\overline{0,\mathrm{m_i}-1})$ остаются на исходном месте.

При технической реализации данного метода первый операнд a_i определяет номер a_{a_i} разряда $P_{a_i}(a_{a_i})$, с содержимым результата модульной операции по модулю m_i, а второй операнд b_i - число разрядов КРС ($b_i k$ -двоичных разрядов), на которые необходимо провести сдвиги исходного (1) содержимого КРС. На рисунках 2 и 3 представлены схемы возможных ОУ СОКИ в МСС, где: $КОИ_i$ - канал обработки информации ОУ по модулю m_i МСС; $КРС_i$ – кольцевой регистр по модулю m_i.

Исходя из [4-6] время сложения двух остатков $(a_i+b_i)\bmod m_i$ в МСС определится математическим выражением

$$T^{(+)}_{\substack{мсс\\ m_i}}=K_{1i}\cdot K_{2i}\cdot t_{сдв}, \quad (4)$$

где: K_{1i} – значение второго b_i слагаемого в сумме $(a_i+b_i)\bmod m_i$ (количество разрядов КРС на которое в положительном (против часовой стрелки) направлении сдвигается исходное содержимое КРС), т.е $K_{1i}=\overline{0,m_i-1}$; K_{2i} – количество двоичных разрядов в одном разряде КРС по модулю m_i, т.е $K_{2i}=\left[\log(m_i-1)\right]+1$; $K_{1i}\cdot K_{2i}$ – количество сдвигаемых в положительном направлении двоичных разрядов КРС; $t_{сдв}=3\cdot\tau_B$ – время сдвига одного двоичного разряда; τ_B – время срабатывания одного логического вентиля (элемента И, ИЛИ).

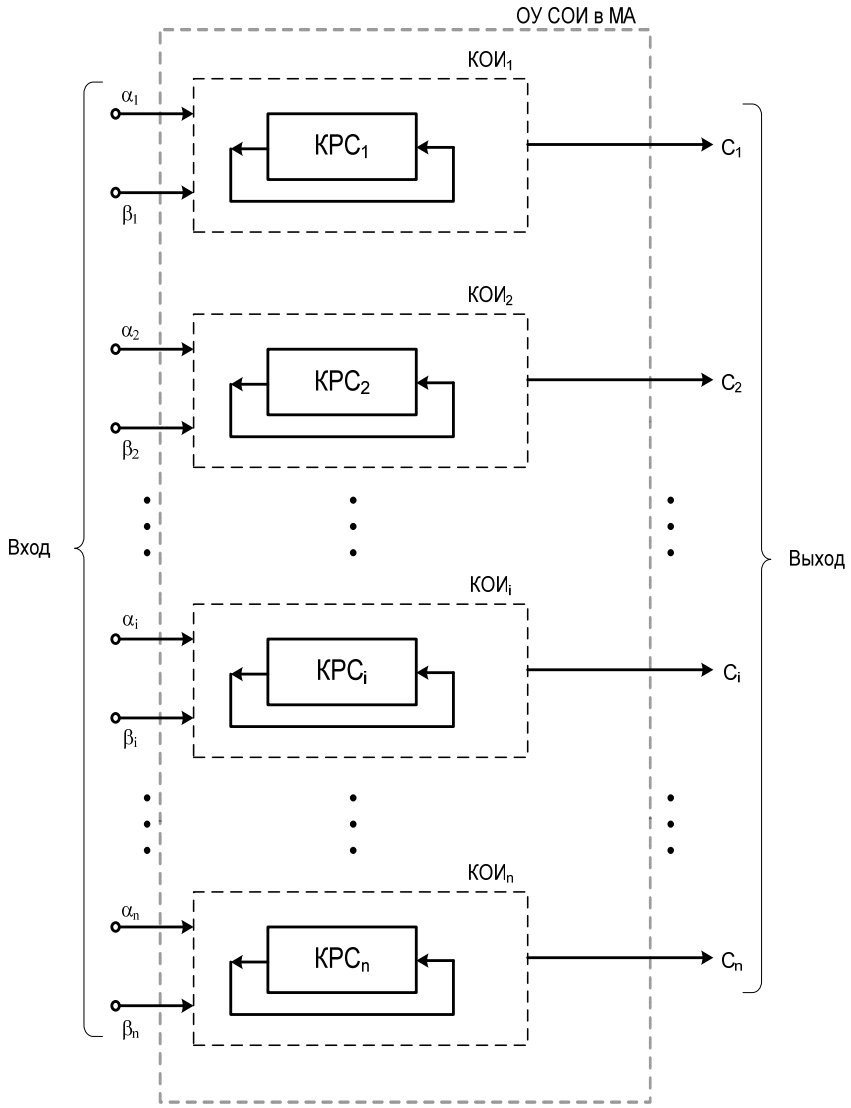

Рис. 2. Структурная схема операционного устройства СОКИ в МСС

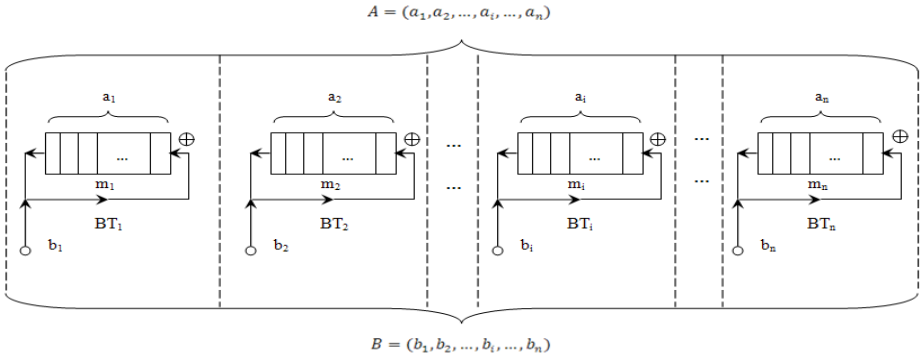

Рис. 3. Схема операционного устройства СОКИ для произвольной МСС

Таким образом, для произвольного модуля m_i МСС время сложения двух остатков a_i и b_i по модулю равно

$$T^{(+)}_{\substack{мсс \\ m_i}} = 3 \cdot K_{1i} \cdot \left\{ \left[\log_2 (m_i - 1) \right] + 1 \right\} \cdot \tau_B. \qquad (5)$$

В этом случае максимально возможное значение $T^{(+)}_{\substack{мсс \\ m_i}}$ для произвольного модуля m_i МСС равно

$$T^{(+)}_{\substack{мсс \\ m_i \\ \max}} = 3 \cdot (m_i - 1) \cdot \left\{ \left[\log_2 (m_i - 1) \right] + 1 \right\} \cdot \tau_B, \qquad (6)$$

а для данной МСС максимальное время сложения двух чисел $A = (a_1, a_2, \cdots, a_{\text{n}})$ и $B = (b_1, b_2, \cdots, b_{\text{n}})$ равно

$$T^{(+)}_{\substack{мсс \\ m_n \\ \max}} = 3 \cdot (m_n - 1) \cdot \left\{ \left[\log_2 (m_n - 1) \right] + 1 \right\} \cdot \tau_B, \qquad (7)$$

В общем случае время сложения двух чисел $A = (a_1, a_2, \cdots, a_{\text{n}})$ и $B = (b_1, b_2, \cdots, b_{\text{n}})$ в МСС определится временем $T^{(+)}_{\substack{мсс \\ m_i}}$ реализации модульной операции $(a_i + b_i) \bmod m_i$ в вычислительном тракте (BT_i), т.е. в КОИ$_i$, для которого выполняется условие $K_{1i} \cdot K_{2i} = \max$ из всех $BT_j (j = \overline{1, n};\ i \neq j)$.

Приведем примеры конкретного выполнения операции сложения двух чисел в МСС для однобайтового $(l = 1)$ процессора. Для $l = 1$ основания МСС могут быть следующие $m_1 = 3,\ m_2 = 4,\ m_3 = 5$ и $m_4 = 7$. На рис. 4 представлена упрощенная схема операционного устройства для однобайтового $(l = 1)$ процессора в МСС.

Пример 1. Пусть второй операнд равен $B = (10,10,100,001)$. Тогда:

-для $BT_1 (m_1 = 3)$ имеем $b_1 = 10,\ K_{11} = 2,\ K_{21} = \left[\log (m_i - 1) \right] + 1 = 2,$ и $K_{11} \cdot K_{21} = 2 \cdot 2 = 4$;

- для $BT_2 (m_2 = 4)$ имеем $b_2 = 10,\ K_{12} = 2,\ K_{22} = 2,$ и $K_{12} \cdot K_{22} = 2 \cdot 2 = 4$;

- для $BT_3 (m_3 = 4)$ – $b_3 = 100,\ K_{13} = 4,\ K_{23} = 3,$ и $K_{13} \cdot K_{23} = 4 \cdot 3 = 12$;

- для $BT_4 (m_4 = 7)$ – $b_4 = 001,\ K_{14} = 1,\ K_{24} = 3,$ и $K_{14} \cdot K_{24} = 1 \cdot 3 = 3.$

Как видно наибольшее количество сдвигаемых двоичных разрядов производится в третьем BT_3, а именно 12.

Таким образом, время реализации двух чисел *A* и *B*, определяемое в МСС на основе принципа кольцевого сдвига, определяется значением второго слагаемого *B*, равно

$$T^{(+)}_{\substack{мсс \\ m_3}} = K_{13} \cdot K_{23} \cdot 3 \cdot \tau_B = 12 \cdot 3 \cdot \tau_B = 36 \cdot \tau_B.$$

Пример 2. Пусть $B = (10,11,001,001)$. Тогда имеем:

– для $BT_1(m_1 = 3)$, $b_1 = 2(10)$, $K_{11} = 2$, $K_{21} = 2$ и $K_{11} \cdot K_{21} = 2 \cdot 2 = 4$;

– для $BT_2(m_2 = 4)$, $b_2 = 3(11)$, $K_{12} = 3$, $K_{22} = 2$ и $K_{12} \cdot K_{22} = 3 \cdot 2 = 6$;

– для $BT_3(m_3 = 5)$, $b_3 = 1(001)$, $K_{13} = 1$, $K_{23} = 3$ и $K_{13} \cdot K_{23} = 1 \cdot 3 = 3$;

– для $BT_4(m_4 = 7)$, $b_4 = 1(001)$, $K_{14} = 1$, $K_{24} = 3$ и $K_{14} \cdot K_{24} = 1 \cdot 3 = 3$.

Таким образом, время сложения чисел A и B определяется временем реализации операции $(a_2 + b_2) \bmod m_2$ во втором вычислительном тракте BT_2 и равно

$$T^{(+)}_{\substack{мсс \\ m_2}} = K_{12} \cdot K_{22} \cdot 3 \cdot \tau_B = 3 \cdot 2 \cdot 3 \cdot \tau_B = 18 \cdot \tau_B.$$

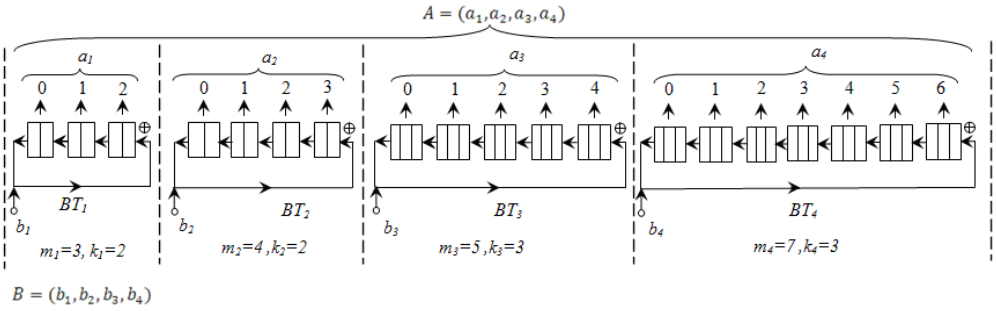

Рис. 4. Упрощенная схема операционного устройства в МСС для однобайтового $(l = 1)$ *СОКИ*

Недостатком предложенного метода реализации арифметических операций в МСС является относительно большое время выполнения целочисленных арифметических модульных операций, что снижает эффективность использования ПКС. Этот недостаток обусловлен тем, что структура $P^{(m_i)}_{исх}$ (см. (2)) представлена набором исходных остатков первой строки (столбца) матрицы $(\alpha_i + \beta_i) \bmod m_i$, отображаемых двоичным кодом. В этом случае время реализации модульного сложения двух операндов $A = (\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, \alpha_n)$ и $B = (\beta_1, \beta_2, \ldots, \beta_{n-1}, \beta_n)$, в МСС определяется выражением (7).

Рассмотрим метод реализации арифметических операций в МСС, основанный на ПКС и лишенный указанного недостатка. Это метод унитарного представления остатков (МУПО), согласно которому информационная структура $P^{(m_i)}_{исх}$ числа по произвольному модулю m_i МСС представляется в виде унитарного (m_i-1)-разрядного кода:

$$P^{(m_i)}_{исх} = \left[P(\alpha_{i-1}) \| P(\alpha_{i-2}) \| \ldots \| P(1) \| P(0) \right] \qquad (8)$$

где $P(\alpha_j)$ - двоичный разряд цифровой структуры (8), единичное состояние которого соответствует значению операнда α_j, представленного унитарным кодом $(\alpha_j = \overline{0, m_i - 1})$. В этом случае исходное содержимое КРС состоит из $(m_i\text{-}1)$-го нулевых двоичных разрядов и схематически может быть представлено в виде (рис. 5)

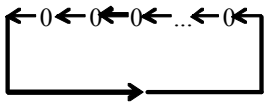

Рис. 5. Исходное содержимое КРС при МУПО

При этом первый операнд α_j, отображаемый унитарным кодом по произвольному модулю m_i МСС, заносится в j-й разряд КРС, т.е переводит j-й двоичный разряд в единичное состояние. Второй операнд β_i указывает на число сдвигов z содержимого КРС, определяя время реализации арифметических операций по модулю m_i МСС, т.е.

$$t_{сл} = \beta_i \tau. \tag{9}$$

Отметим, что время реализации арифметической операции (A + B)mod m в СОК будет определяться временем выполнения операции для максимального значения $(\beta_{\max\ i} \quad (i = \overline{1, n})$ остатка из совокупности $\{\beta_i\}$ для данного операнда $B = (\beta_1, \beta_2, ..., \beta_n)$, т.е.

$$t_{сл} = \beta_{\max\ i} \tau. \tag{10}$$

Проведем сравнительный анализ времени реализации операции сложения двух чисел A и B в ПСС и в МСС. Известно [9], что время $T^{(+)}_{ПСС}$ сложения чисел A и B в ПСС равно

$$T^{(+)}_{ПСС} = (2 \cdot \rho - 1) t_c = (16 \cdot l - 1) \cdot 3 \cdot \tau_B, \tag{11}$$

где: $\rho = 8 \cdot l$ – l-байтовое машинное слово (разрядная сетка СОКИ для $l = \overline{1, 4, 8}$); $t_c = 3 \cdot \tau_B$ – время суммирования в $(i+1)$-м двоичном разряде позиционного сумматора значений $a_{i+1} + b_{i+1} + c_i$, т.е время определения значений C_{i+1} и S_{i+1} [10].

Учитывается, что существует метод уменьшения в два раза максимального времени реализации операции модульного сложения в МСС [9] имеем для ПКС

$$T^{(+)}_{\substack{мсс \\ \max}} = T^{(+)}_{\substack{мсс \\ m_n}} / 2. \tag{12}$$

Введем коэффициент α отношения времени реализации операции сложения в ПСС и в МСС, т.е.

$$\alpha = T^{(+)}_{ПСС} / T^{(+)}_{\substack{мсс \\ \max}} = \frac{(16 \cdot l - 1) \cdot 3 \cdot \tau_B \cdot 2}{(m_n - 1) \cdot \{[\log_2(m_n - 1)] + 1\} \cdot 3 \cdot \tau_B} = \\ = \frac{2 \cdot (16 \cdot l - 1)}{(m_n - 1) \cdot \{[\log_2(m_n - 1)] + 1\}}. \quad (13)$$

Анализ выражений (9) и (10) показывает, что разработанный МУПО примерно в $k = [\log_2(m_i - 1) + 1]$ раз сокращает время выполнения арифметических операций по сравнению с МДПО.

Расчет и сравнительный анализ времени выполнения арифметических операций при криптографических преобразований показал высокую эффективность применения МДПО и МУПО, основанных на использовании ПКС, по сравнению с методом, применяемыми в ПСС (таблица 3). Это без учета дополнительной возможности применения существующих алгоритмов, использование которых позволяет уменьшить время реализации модульных арифметических операций. Полученные аналитические выражения (4), (5), (6), (7), (9), (10), (13) и результаты расчетов времени реализации арифметических операций в МСС могут быть использованы также при оценке и сравнительном анализе вычислительной сложности алгоритмов RSA криптопреобразований.

Таблица 3. Данные сравнительного анализа времени операции сложения

l (ρ)	Двоичная ПСС	Модулярная система счисления				Выигрыш в [%]	
	$T^{(+)}_{ПСС} / 3 \cdot \tau_B$	m_n	K	$T^{(+)}_{\substack{i \\ \max}} / 3 \cdot \tau_B$			
				МДПО	МУПО	МДПО	МУПО
1 (8)	15	7	3	9	3	40	80
2 (16)	31	13	4	24	6	22	80
3 (24)	47	19	5	45	9	5	81
4 (32)	63	29	5	70	14	–	78
8 (64)	127	53	6	159	27	–	71

7. Выводы по результатам и направления дальнейших исследований

В данной статье рассмотрено новые методы повышения быстродействия реализации криптографических преобразований в полях Галуа, в частности, повышения производительности RSA криптопреобразований с открытым ключом. Данные методы основаны на использовании ПКС в МСС. Использование основных теоретических свойств МСС позволяет эффективно организовать процесс реализации модульных операций в криптографических задачах. К практическому использованию предложены два метода реализации арифметических операций в МСС, основанных на ПКС: метод двоичного представления остатков и метод унитарного представления остатков. Проведенный анализ эффективности использования данных методов и примеры конкретной технической реализации модульных арифметических операций

показал их практическую реализуемость. Данные методы обработки информации рекомендованы к практическому использованию в СОКИ реального времени. Однако, принимая во внимания тот факт, что тенденция развития криптографии направлена на увеличения длины разрядной сетки СОКИ, предпочтительно, использовать МУПО. Результаты, изложенных исследований целесообразно также использовать в системах и устройствах обработки больших массивов цифровой информации реального времени.

ЛИТЕРАТУРА

1. Шнайер Б. Прикладная криптография. М.: Изд-во. “Триумф”, 2002. – 797с.
2. Горбенко И.Д., Збитнев С.И., Поляков А.А. Криптоанализ криптографических преобразований в группах точек эллиптических кривых методом Полларда // Радиотехника: Всеукр. межвед. научн-тех. сб. 2001. Вып. 119. – С. 43-50.
3. V.A. Krasnobayev. Method for Realization of Transformations in Public-Key Cryptography, Telecommunications and Radio Engineering (USA), 2007, Vol. 66, Issue 17, pp. 1559-1572.
4. Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. – М.: Сов. радио, 1968. – 440 с.
5. Коляда А.А., Пак И.Т. Модулярные структуры конвейерной обработки цифровой информации. Минск: Университетское, 1992. – 256с.
6. Барсов В.И., Сорока Л.С., Краснобаев В.А., Хери Али Абдуллах. Модели и методы повышения отказоустойчивости и производительности управляющих вычислительных комплексов специализированных систем управления реального времени на основе применения непозиционных кодовых структур модулярной арифметики. Монография. - Х.: УИПА, 2008. - 147с.
7. Барсов В.И., Сорока Л.С., Краснобаев В.А. Методология параллельной обработки информации в модулярной системе счисления: Монография.-Х.: МОН, УИПА, 2009. - 268с.
8. Вербіцький О. В. Вступ до криптології. –Львів.: ВНТЛ, 1998. - 248с.
9. Жихарев В.Я., Илюшко Я.В., Кравець Л.Г., Краснобаев В.А. Методы и средства обработки информации в непозиционной системе счисления в остаточных классах. Монография.–Житомир: Изд-во “Волынь”, 2005. – 220с.
10. В. А. Краснобаев, С.О. Мартыненко, Ж.В. Дейнеко, А.А. Замула, А.А. Баклыков. Метод обработки криптографической информации в модулярной системе счисления, основанный на принципе кольцевого сдвига // Прикладная радиоэлектроника. Научно-технический журнал. Тематический выпуск, посвященный проблемам обеспечения безопасности информации. Том 8. 2009. № 3. С. 343-350.

Надійшла у першій редакції 25.02.2010, в останній - 04.04.2010.