УДК 519.7 https://doi.org/10.26160/2541-8637-2020-5-130-135

ВЫСОКОТОЧНЫЕ ВЫЧИСЛЕНИЯ В МОДУЛЯРНО-ПОЗИЦИОННОЙ ИНТЕРВАЛЬНО-ЛОГАРИФМИЧЕСКОЙ АРИФМЕТИКЕ

Коржавина А.С.
Вятский государственный университет, г.Киров

Ключевые слова: система остаточных классов, высокоточные вычисления, масштабирование, целочисленная интервальная арифметика, сравнение чисел.
Аннотация. Для решения многих задач, включая задачи гомоморфной криптографии, требуется высокая точность представления числовой информации, в несколько десятков раз превышающая размер машинного слова, в связи с чем требуется создание аппаратно-программных комплексов высокоточных вычислений, обеспечивающих приемлемое для практики быстродействие. В настоящей работе рассматривается новый, более эффективный по сравнению с аналогами метод выполнения немодульных операций за счет применения интервальных вычислений с фиксированной точкой.

HIGH-PRECISION RESIDUE POSITIONAL INTERVAL LOGARITHMIC ARITHMETIC

Korzhavina A.S.
Vyatka State University, Kirov

Keywords: residue number system, high-precision computations, scaling, integer interval arithmetic, comparison.
Abstract. A high accuracy of the presentation of numerical information is required to solve many scientific problems including homomorphic cryptography. The precision of tens to hundreds times larger than a machine word requires creating hardware-software complexes of high-precision computations that provide acceptable performance for practice. In this paper, we consider a new, more efficient method for non-modular operations using fixed-point intervals.

В современном мире повсеместного использования облачных сервисов и нейросетевых технологий для обработки медицинской и другой персональной информации, все большее значение приобретают технологии защиты личных данных людей, что требует создания систем защиты информации нового поколения. Для построения таких систем требуются специальные аппаратно-программные средства, обеспечивающие проведение массовых вычислений над данными сверхвысокой точности в режиме реального времени. Наиболее актуальным направлением является гомоморфная криптография, изучающая схемы шифрования, допускающие выполнение арифметических и логических вычислений над зашифрованными данными без предварительного дешифрования. Для построения полностью гомоморфных схем шифрования требуется точность в диапазоне 2048-32768 бит [1, 2]. Подобные диапазоны требуются не только для криптографических задач, но и для некоторых задач высокоточного моделирования, например, экспериментальной вычислительной математики [3, 4], математической физики [5], биохимии [6].

Использование позиционной длинной арифметики приводит к резкому увеличению времени выполнения арифметических операций над длинными

числами. Например, при выполнении операции умножения Монтгомери, необходимо выполнить 36 стандартных команд процессора для операндов разрядности 192 бит, а при разрядности операндов в 2048 бит – свыше 4000 [7].

Одной их базовых операций в задачах криптографии является алгоритм Монтгомери с использованием систем остаточных классов, в котором ключевым шагом выступает немодульная операция расширения базиса. В настоящее время, основной целью исследований в области СОК является построение эффективных методов выполнения немодульных операций для модулярной арифметики в сверхбольших числовых диапазонах, применяемой в большинстве задач криптографии. Таким образом, актуальной является задача сравнения, расширения базиса и масштабирования сверхбольших чисел (соответствующих двоичной точности в 1024-32768 бит), представленных в системе остаточных классов.

Большинство быстрых методов выполнения немодульных операций разработаны для наборов модулей малой разрядности с использованием подстановочных таблиц или специальных наборов модулей, при использовании таких наборов модулей диапазон представления длинных чисел, как правило, не превышает 128-256 бит [8]. Разработанные ранее методы не применимы для произвольных наборов модулей средней и большой разрядности (свыше 15-16 бит) для представления чисел в сверхбольших диапазонах, поскольку объем используемых подстановочных таблиц увеличивается экспоненциально с ростом разрядности и количества модулей.

Целью данной работы является разработка эффективного метода выполнения немодульных операций сравнения, расширения базиса и масштабирования чисел, представленных в СОК с произвольным набором модулей средней разрядности (16-18 бит) с использованием двоичных целочисленных интервалов, который не требует выполнения табличных операций и операций с плавающей точкой.

В работе предлагается новый способ представления целых и вещественных чисел для вычислений в сверхбольших диапазонах – гибридная модулярно-позиционная интервально-логарифмическая форма:

$$X \xrightarrow{МПИЛ-СС} \left[\left\langle m_1, m_2, ..., m_n \right\rangle, \underline{L}, \overline{L}, \lambda, \sigma \right],$$

где $M = \left\langle m_1, m_2, ..., m_n \right\rangle$ – модулярная мантисса числа, λ – масштаб (порядок) числа, $\underline{L}, \overline{L}$ – границы интервальной логарифмической характеристики мантиссы числа, σ – знак числа.

Согласно КТО, позиционное значение числа $X \in \left[0, P\right)$, представленного в СОК остатками $\left\langle x_1, x_2, ..., x_n \right\rangle$ по основаниям $\left\{ p_1, p_2, ..., p_n \right\}$ вычисляется по формуле:

$$X = \left| \sum_{i=1}^{n} \left| x_i \cdot \left| P_i^{-1} \right|_{p_i} \right|_{p_i} \cdot P_i \right|_P = \sum_{i=1}^{n} \left| x_i \cdot \left| P_i^{-1} \right|_{p_i} \right|_{p_i} \cdot P_i - R \cdot P,$$

где $P_i = \frac{P}{p_i}$, $\left|P_i^{-1}\right|_{p_i}$ – мультипликативная инверсия P_i по модулю p_i, $i \in [1,n]$, n – количество модулей, R – позиционный индекс.

Для вычисления коэффициента R был разработан алгоритм с использованием целочисленных интервалов на основе приближенной интервальной оценки величины:

$$W_X = \left[\sum_{i=1}^{n} \left| X_i \cdot P_i^{-1} \right|_{p_i} \cdot \underline{w_i}, \sum_{i=1}^{n} \left| X_i \cdot P_i^{-1} \right|_{p_i} \cdot \overline{w_i} \right].$$

Процесс вычисления коэффициента R с использованием вещественных интервалов с направленным округлением, а также необходимые условия корректности вычислений, представлены в [9], метод вычисления коэффициента R с использованием целочисленных интервалов описан в патенте [10].

Величины $\underline{w_i}, \overline{w_i}$ вычисляются заранее с точностью s двоичных знаков.

Целочисленная оценка модулярного числа W_X – положительное целое число разрядностью $q+s-1+\log_2 n$, где n – количество модулей в базисе. Путем умножения на масштабирующий коэффициент 2^{q+s-1} вычисляются значения позиционного индекса R и значение относительной величины модулярного числа X/P.

Обозначим $S_i = \left| X_i \cdot P_i^{-1} \right|_{p_i}$.

Целочисленный интервал $\left[\underline{W_X}, \overline{W_X}\right]$ назовем целочисленной интервальной оценкой модулярного числа.

По значениям R_{min} (минимальное значение позиционного индекса) и R_{max} (максимальное значение позиционного индекса) определяется корректность вычисления целочисленной интервальной оценки: если числа равны, то целочисленная интервальная оценка вычислена корректно.

Были проведены серии вычислительных экспериментов для различных значений разрядности модулей q (от 5 до 16) и количества модулей n (от 8 до 32). Для каждого конкретного значения q и n были сформированы выборки чисел из диапазона $[0,P-1]$. Количество чисел в каждой выборке – 10^{10}, выборка производилась равномерно из диапазона представления модулярных чисел. Для каждого из чисел выборки были вычислены модулярное представление, значение целочисленной интервальной оценки и коэффициента R. Определялись количество случаев, для которых значения верхней и нижней оценок коэффициентов R были равны (количество попаданий), и для которых значения этих коэффициентов были не равны (количество промахов).

В ходе экспериментов выявлено, что вероятность корректного вычисления величины R не зависит от разрядности модулей, а зависит от их количества, то есть при фиксированном значении $r=s-\log_2 n$ (где s – разрядность коэффициентов) доля чисел из выборки, для которых корректно вычислено значение R приблизительно одинакова вне зависимости от количества и разрядности модулей. На рис. 1 изображен график зависимости вероятности корректного вычисления целочисленной оценки модулярного числа для различных значений

разрядности модулей и их количества. Серым обозначены значения, вычисленные по формуле $y = 1 - \frac{1}{2^{s-\log_2 n}}$.

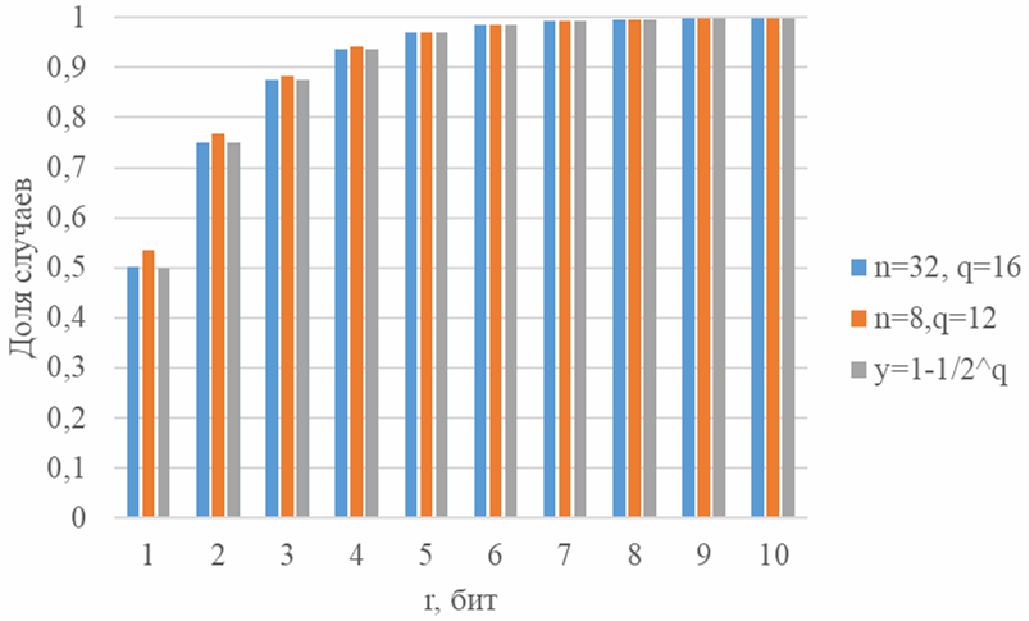

Рис. 1. Зависимость относительной доли попаданий при различных значениях разрядности *r*

При увеличении разрядности коэффициентов w_i увеличивается доля случаев корректного вычисления коэффициента *R*, т.е. точность вычисления коэффициента *R* и соответственно точность приближенных методов сравнения, масштабирования, расширения базиса.

Схема устройства вычисления нижней границы целочисленной интервальной характеристики приведена на рис. 2. Верхняя граница вычисляется аналогичным образом.

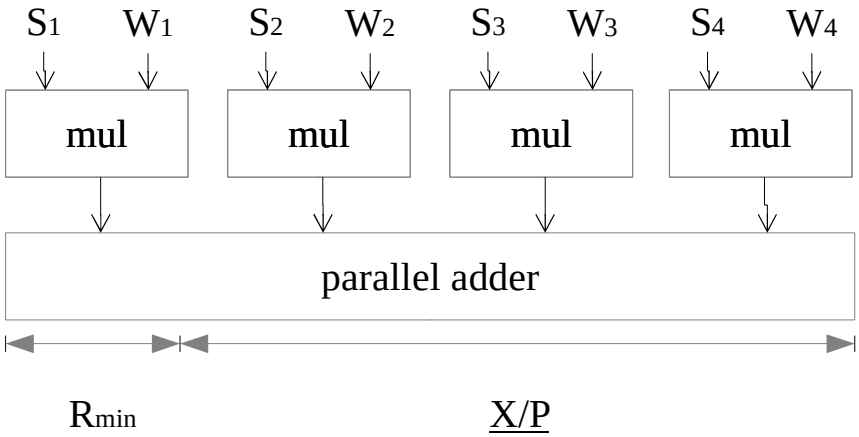

Рис. 2. Схема вычисления позиционного индекса R

Разработанные устройства вычисления целочисленных интервальных характеристик были синтезированы для ПЛИС *Altera Cyclone V* для различных значений разрядностей коэффициентов w. Результаты представлены в таблице 1.

Табл. 1. Результаты вычисления целочисленных интервальных характеристик

***r*, бит**	***Схема R_{min}***		***Схема R_{max}***		***Вероятность Rmin=Rmax, %***
	Площадь, модулей	***Время, нс***	***Площадь, модулей***	***Время, нс***	
9	128	12,816	180	13,004	98,44
10	126	13,946	321	14,045	99,22
11	312	14,344	317	14,351	99,61
12	360	14,276	334	14,673	99,81
13	363	14,723	387	13,310	99,90
14	391	14,28	408	14,962	99,95
15	427	14,45	420	15,10	99,98

Результаты моделирования на ПЛИС показывают линейный рост площади схемы вычисления целочисленной интервальной оценки, а также незначительный линейный рост времени выполнения. Таким образом, при увеличении разрядности коэффициентов w_i, и, как следствие, вероятности корректного вычисления коэффициента R среднее время стремится к времени выполнения немодульной операции с использованием разработанного метода. Однако, при увеличении разрядности сумматоров и умножителей в схеме вычисления целочисленной интервальной оценки возрастает площадь схемы и задержки на элементах (так как используются обычные позиционные сумматоры).

Таким образом, в данной работе был предложен новый метод выполнения немодульных операций систем остаточных классов; проведена оценка временной и аппаратной сложности разработанного метода, выполнено моделирование блоков немодульных операций. Показано, что для достижения приемлемой точности и быстродействия при выполнении немодульных операций достаточно использования целочисленных интервалов малой разрядности.

Работа выполнена при финансовой поддержке РФФИ в рамках научного проекта № 18-37-00278 мол_а.

Список литературы

1. High-precision arithmetic in homomorphic encryption / H. Chen et al. // Cryptographers' Track at the RSA Conference. Springer. 2018. P. 116-136. DOI: 10.1007/978-3-319-76953-0_7.
2. Improved security for a ring-based fully homomorphic encryption scheme / J. W. Bos et al. // IMA International Conference on Cryptography and Coding. Springer. 2013. P. 45-64. DOI: 10.1007/978-3-642-45239-0_4.
3. Iakymchuk R., Defour D., Collange S., Graillat S. Reproducible and accurate matrix multiplication // International Symposium on Scientific Computing, Computer Arithmetic and Validated Numerics. 2015: 126-137. DOI: /10.1007/ 978-3-319-31769-4_11.
4. Voros A. Discretized Keiper/Li approach to the Riemann Hypothesis. Experimental Mathematics. 2018: 1-18. DOI: 10.1080/10586458.2018.1482480.
5. Yang L., Ma D., Ebrahim A., Lloyd C. J., Saunders M. A., Palsson B. O. solveME: fast and reliable solution of nonlinear ME models BMC bioinformatics. 2016; 17: 391. DOI: 10.1186/s12859-016-1240-1.

6. Panzer E. Algorithms for the symbolic integration of hyperlogarithms with applications to Feynman integrals Computer Physics Communications. 2015; 188: 148-166. DOI: 10.1016/j.cpc.2014.10.019.
7. Fast Montgomery Modular Multiplication and Squaring on Embedded Processors / Y. Li et al. // IEICE Transactions on Communications. 2016. DOI: 10.1587/transcom.2016EBP3189.
8. Czyzak M., Smyk R., Ulman Z. Pipelined scaling of signed residue numbers with the mixed-radix conversion in the programmable gate array // Poznan University of Technology Academic Journals. Electrical Engineering. 2013. № 2. P. 89-99. URL: https://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-5d0a87e2-2459-476f-8c7e-2d72d07072f2/c/Czyzak.pdf.
9. Isupov K., Knyazkov V. Interval estimation of relative values in Residue Number System // Journal of Circuits, Systems and Computers. 2018. Vol. 27, no. 01. P. 1850004. DOI: 10.1142/S0218126618500044.
10. Патент №2666285 РФ. МПК G06F 7/483 (2006.01), G06F 7/487 (2006.01). Способ организации выполнения операции умножения двух чисел в модулярно-логарифмическом формате представления с плавающей точкой на гибридных многоядерных процессорах / В.С. Князьков, А.С. Коржавина – №2017135775/22; заявл.06.10.2017; опубл. 06.09.2018, Бюл. №25.

Сведения об авторе:
Коржавина Анастасия Сергеевна – старший преподаватель, ВятГУ, г. Киров.