Параллелизация решения систем уравнений как инструмент в схеме разделения секрета

Р.Т. Файзуллин, Д.А. Волков

Омский Государственный Технический Университет

Передача вычислений в центры обработки данных (ЦОД), а так же параллелизация алгоритмов дает, во-первых, ускорение вычислений по времени, а во-вторых, уменьшение финансовых затрат на решение какой-либо вычислительной задачи. Однако возникают сомнения о безопасности данных, переданных в ЦОД, которые являют собой объект, представленный в удобной для обработки форме. Поскольку шифрование данных не спасает от мафиозной угрозы, а так же от законных оснований правительства других стран о запросе на получение расшифрованных данных, то предлагается применение схем разделения секрета. При использовании таких схем малая, но информативная часть будет обрабатываться на вычислительных ресурсах клиента, тогда как большая часть данных, которая не несет никакой информации об объекте, будет передана для обработки в ЦОД.

Рассмотрим две односвязные области Ω, Ξ, где $\Xi \subset \Omega$ и задачу Дирихле для уравнения Лапласа:

$$\Delta u = 0,\ (x, y) \in \Omega - \Xi \tag{2}$$

$$u|_{\partial\Xi} = \varphi(x, y), \quad u|_{\partial\Omega} = \psi(x, y) \tag{3}$$

Разобьём кольцо Ω - Ξ на два непересекающихся вложенных кольца Θ_1, Θ_2, так что $\Omega - \Xi = \Theta_1 \cup \Theta_2$. Кольцо Θ_1 примыкает к Ξ. Зная решение в области $\Omega - (\Theta_1 \cup \Xi)$, невозможно получить какую-либо информацию о границе Ξ и значениях функции или её производных на $\partial\Xi$, что позволяет использовать данный метод для передачи вычислений в публичное облако.

Для получения численного решения данной задачи используется метод конечных разностей и альтернирующий метод Шварца. Полученная матрица, которая кодирует объект, разбивается по вычислителям. Каждый вычислитель получает свою часть матрицы, в этих частях строки и столбцы, соседние с граничными, называют перехлёстами. При синхронизации вычислители обрабатывающие соседние части матрицы обмениваются между собой перехлёстами. Более наглядно перехлёсты можно увидеть на рис. 1.

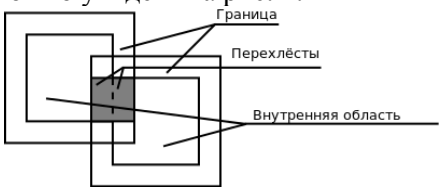

Рис. 1. Схематичное изображение перехлёста между двумя частями матрицы.

Передача перехлёстов проходит через программу-сервер, запущенную на любом компьютере с достаточной шириной интернет канала и доверенном клиенту. В таблице 1 представлены результаты экспериментов на кластере, который состоит из 4-х узлов, содержащих по два четырёхядерных процессора Intel Xeon X5472 3.0GHz Quad Core и по 8 Гб оперативной памяти PC2-5300 ECC. Узлы соединены между собой каналом в 1 Гбит.

Таблица 1. Результаты экспериментов

Размер задачи	Количество ядер	Время полное, с	Время вычислений, с	Время синхронизации, с	Ускорение
1000x1000	16	14041.019	983.865	13017.801	0.046
2000x2000	16	21519.828	4504.495	16976.26	0.328
4000x4000	16	67954.636	41078.507	26849.413	1.536