УДК 004.4
І. Вітрук, А. Луцків
(Тернопільський національний технічний університет імені Івана Пулюя)

ПІДХОДИ ДО РОЗВ'ЯЗАННЯ ЗАДАЧ ВИКОНУВАНОСТІ БУЛЕВИХ ФУНКЦІЙ У ПРКС

Задача виконуваності (Satisfiability problem) – дано правильний логічний вираз, чи є спосіб присвоїти правильні значення змінним цього виразу, так, щоб весь вираз став істинним, є *NP*-повною. Засоби для розв'язання даної задачі називаються SAT-солверами й на даний час набувають все більшої актуальності в галузі криптоаналізу. Даний вид програм має велике прикладне значення у алгебраїчному криптоаналізі для атаки на блокові та потокові шифри. SAT-солвери працюють з задачами, які описані в кон'юнктивній нормальній формі (КНФ). КНФ-файли є вхідними даними для задач здійсненності булевих функцій. На виході таких програм отримується набір розв'язків системи рівнянь. Екземпляром задачі SAT є булева формула, що складається тільки з імен змінних, дужок та операцій І, АБО і НЕ. Задача SAT-солвера полягає в наступному: чи можна призначити всім змінним у логічному виразі, значення хибність та істина так, щоб формула стала істинною.

Оскільки, SAT-задача є *NP*-повною, то в загальному випадку її розв'язання є важкообчислюваним. Однак, на практиці, в ряді випадків доводиться користуватися «методами грубої сили». Вирішувати таку складну задачу набагато легше на паралельних та розподілених системах з великою обчислювальною потужністю.

Авторами пропонується три підходи до розподілу SAT-задачі в ПРКС:

а) Програмне розпаралелення – використовуючи технології паралельного програмування, зокрема, MPI-інтерфейс, створювати ПЗ для ПРКС з розподіленою пам'яттю. Авторами здійснено обчислювальний експеримент, що показує ефективність такого способу розпаралелення при збільшенні кількості змінних системи булевих рівнянь. Для цього, як приклад, розв'язано класичну задачу про *N* ферзів: спочатку в послідовній програмі, а потім у паралельній, використовуючи технологію MPI. Загальна оцінка трудомісткості алгоритму в ПРКС може бути отримана наступним чином:

$$T_p = \frac{C_n^N}{p}\left(1 + 2\left(N + N(N-2)(N+1) + \frac{2}{3}N(4N^2-1)\right)\right)\tau + \log_2 p(\alpha + \frac{\omega}{\beta}) + \log_2 p(\alpha + \frac{w(N + N(N-2)(N+1) + \frac{2}{3}N(4N^2-1))}{\beta})$$

де C_n^N - кількість перевірок, які потрібно здійснити, N — кількість суб'єктів (шахових фігур) задачі, n — кількість змінних системи КНФ-рівнянь, p — кількість процесорів.

б) Декомпозиція за даними - незалежне розв'язання окремих систем булевих рівнянь на вузлах кластера. Такий спосіб розв'язання доцільний для систем криптоаналізу та представлення даних за допомогою програм підготовки систем КНФ-файлів, зокрема Grain Of Salt, що генерує незалежні системи рівнянь. Кожен вузол ПРКС займається розв'язанням паралельно. За n секунд вузлом кластера розв'язано SAT-задачу, що утворена з шифротексту довжиною k біт. Тоді за n секунд увесь кластер може розв'язати згенеровану з шифротексту задачу довжиною $K = kp$ біт, де p – кількість вузлів кластера.

в) Спосіб розв'язання задачі, який полягає у розпаралеленні її на ядрах GPU, або іншого обчислювального елементу ПРКС (FPGA, CPU), використовуючи, зокрема, технологію та фреймворк OpenCL.