Решение задач криптоанализа генераторов ключевого потока A5/1 и Bivium в проекте добровольных распределенных вычислений SAT@home[1]

О.С. Заикин, А.А. Семенов
zaikin.icc@gmail.com, biclop.rambler@yandex.ru
Институт динамики систем и теории управления СО РАН

Многие важные прикладные задачи могут быть эффективно сведены к задаче о булевой выполнимости (SAT) [1]. Обычно под SAT понимается задача поиска выполняющего набора либо доказательства невыполнимости конъюнктивной нормальной формы (КНФ). Программы, решающие данную задачу, называются SAT-решателями. Несмотря на то, что SAT является NP-полной задачей, за последние 15 лет был достигнут значительный прогресс в алгоритмике SAT-решателей. В частности, речь идет о создании алгоритма CDCL (Conflict Driven Clause Learning). Дальнейшее развитие данного алгоритма, а также разработка новых эффективных структур данных позволило решить трудные задачи из целого ряда прикладных областей, таких как символьная верификация, криптография и биоинформатика.

Поскольку SAT-задачи являются вычислительно трудными, для их решения оправдано применение параллельных вычислений. Существует два похода к параллельному решению SAT-задач. Согласно первому из них, называемому «partitioning-подход», область поиска разбивается на непересекающиеся подобласти с помощи декомпозиции по данным. В итоге решение исходной SAT-задачи сводится к решению семейства подзадач, которые могут быть обработаны независимо друг от друга. Данный подход был впервые изложен в статье [2]. Применение partitioning-подхода для решения SAT-задач в грид-системах было рассмотрено в статье [3]. Для решения независимого семейства подзадач можно также применять интенсивно развивающиеся за последние 15 лет добровольные распределенные вычисления [4], в рамках которых с помощью ресурсов ПК частных лиц решаются масштабные научные задачи.

Второй, т.н. «portfolio-подход», был предложен в статье [5]. Согласно этому подходу решение одной и той же SAT-задачи запускается одновременно в несколько потоков, при этом на каждом потоке могут быть использованы обычные последовательные SAT-решатели. Ключевым моментом данного подхода является обмен накапливаемой информацией о ходе поиска (в виде конфликтных дизъюнктов) между решателями в различных потоках, что позволяет на некоторых классах тестов получить хорошее ускорение по сравнению с последовательными SAT-решателями. Однако, у данного подхода есть существенное ограничение по масштабируемости. На практике portfolio-

[1] Работа выполнена при частичной финансовой поддержке РФФИ (грант № 14-07-00403). Совета по грантам Президента РФ для поддержки молодых ученых (стипендия СП-1855.2012.5), Совета по грантам Президента РФ для государственной поддержки ведущих научных школ (НШ-5007.2014.9).

решатели имеет смысл запускать только на системах с общей памятью, т.к. интенсивный обмен накапливаемой информацией требует больших ресурсов.

Исходя из вышесказанного, для решения некоторых классов трудных SAT-задач более подходит partitioning-подход. Главное преимущество этого подхода заключается в хорошей масштабируемости. При этом эффективность применения partitioning-подхода очень сильно зависит от того, как именно была осуществлена декомпозиция исходной SAT-задачи.

В работе [6] исследуется проблема использования метода Монте Карло для поиска «хороших» декомпозиционных множеств для SAT-задач. Под декомпозиционным множеством понимается подмножество переменных КНФ, варьируя все варианты значений которых формируется декомпозиционное семейство, от решения в общем случае всех SAT-задач которого можно эффективно получить решение исходной SAT-задачи. Реализация данного метода в виде параллельной MPI-программы PDSAT позволила найти декомпозиции для задач логического криптоанализа генераторов A5/1 и Bivium. В случае генератора Bivium полученные декомпозиции оказались лучше (по прогнозному времени решения исходной задачи), чем опубликованные ранее [7]. Для генератора A5/1 подобные декомпозиции в открытых источниках найдены не были. Найденные с помощью PDSAT декомпозиционные множества изображены на рисунках 1 и 2.

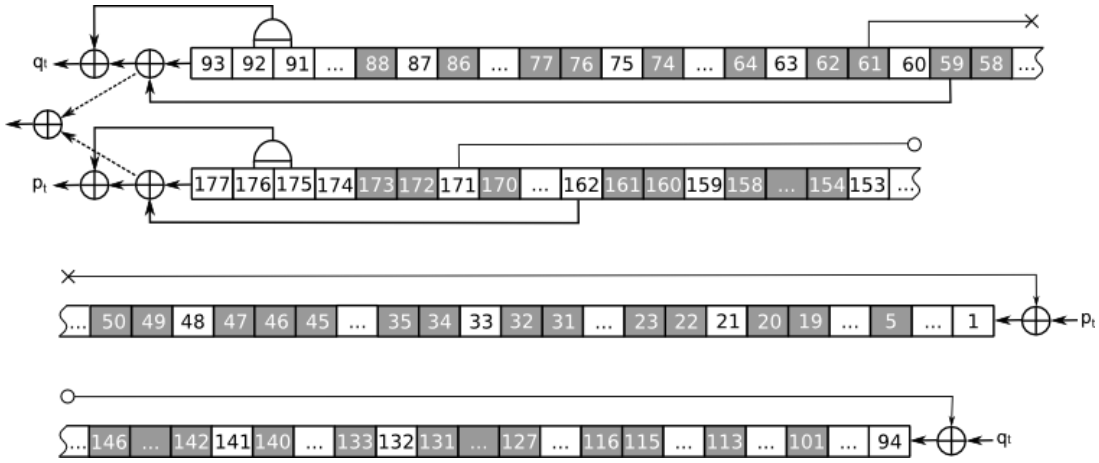

Рис. 1. Декомпозиционное множество, найденное для криптоанализа генератора Bivium.

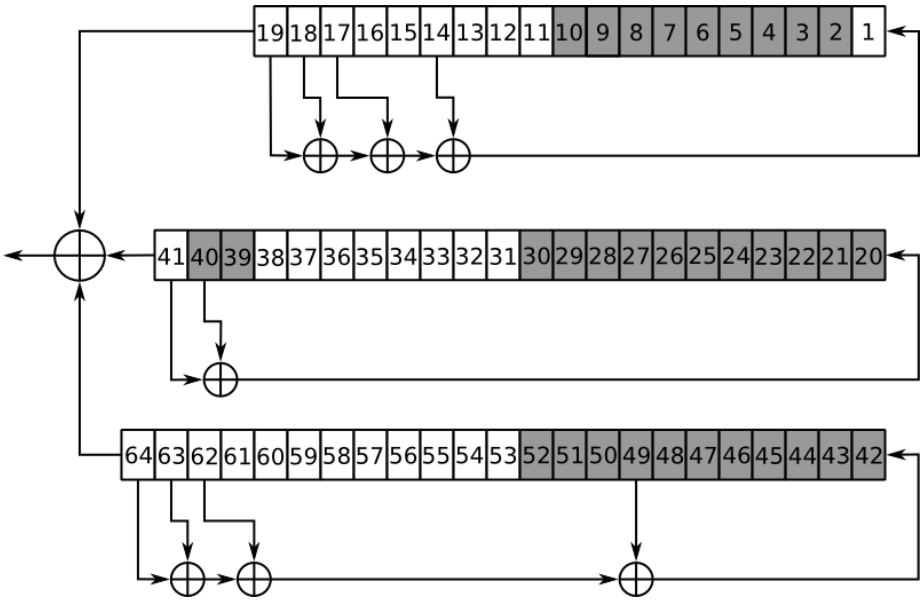

Рис. 2. Декомпозиционное множество, найденное для криптоанализа генератора A5/1.

Найденное декомпозиционное множество было использовано для решения задач криптоанализа генератора A5/1 в проекте добровольных распределенных вычислений SAT@home [8]. Наиболее успешным методом криптоанализа данного генератора является т.н. «rainbow»-метод. Однако известные rainbow-таблицы покрывают ключевое пространство A5/1 примерно на 88% и не дают результатов для тестов, в которых используются оставшиеся 12% ключей. Для решения в рамках проекта SAT@home были построены 10 таких тестов. Все они были успешно решены за полгода работы проекта.

В случае генератора Bivium прогнозное время для обработки декомпозиционного семейства оказалось слишком большим, поэтому был решен ряд ослабленных задач криптоанализа. Ослабление заключалось в том, что были известны несколько бит из искомого начального заполнения регистров Bivium (суммарно два регистра состоят из 177 бит). В проекте SAT@home за 3 месяца были решены 3 ослабленные задачи криптоанализа генератора Bivium, в каждой из которых были известны 10 бит из 177.

Полученные результаты показывают, что добровольные распределенные вычисления позволяют решать трудные SAT-задачи, кодирующие задачи криптоанализа реальных криптографических систем. Это обусловлено, в том числе, высокой производительностью проекта SAT@home. Следует отметить, что в SAT@home использовались не только ресурсы ПК частных лиц, но и узлы нескольких вычислительных кластеров. Эти узлы были подключены с помощью программного средства CluBORun [9], которое позволяет использовать свободные ресурсы вычислительных кластеров в BOINC-расчетах. На рисунке 3 показана динамика производительности проекта SAT@home с октября 2011 года по октябрь 2014 года.

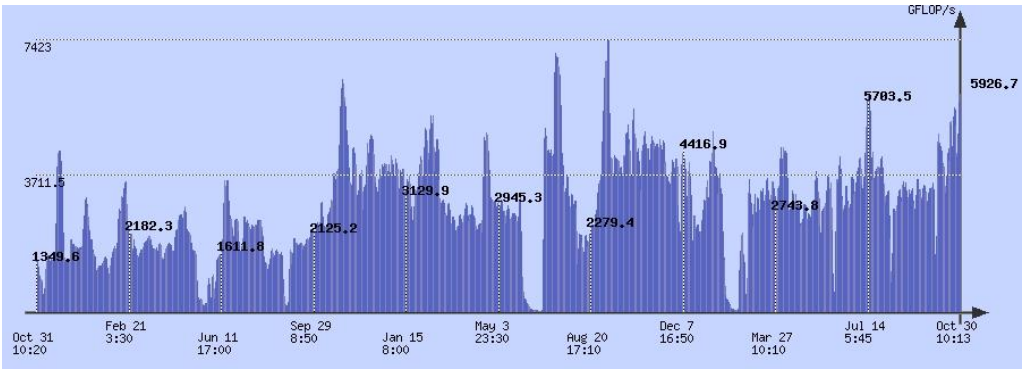

Рис. 3. Динамика производительности проекта SAT@home с октября 2011 года по октябрь 2014 года.

Авторы выражают благодарность всем добровольцам, которые предоставили свои вычислительные ресурсы для проекта SAT@home.

Список литературы

1. Biere, A., Heule, M., van Maaren, H., Walsh, T. (eds.): Handbook of Satisfiability, Frontiers in Artificial Intelligence and Applications, vol. 185. IOS Press, 2009.
2. Bohm M., Speckenmeyer E. A fast parallel SAT solver - efficient workload balancing. Annals of Mathematics and Artificial Intelligence. 1996. 17, № 2. pp. 381-400.
3. Hyvarinen A.E.J., Junttila T.A., Niemela I. A Distribution Method for Solving SAT in Grids. Lecture Notes in Computer Science. 2006. Vol. 4121. 430-435.
4. M. Nouman Durrani and J. A. Shamsi. Review: Volunteer computing: Requirements, challenges, and solutions. J. Netw. Comput. Appl., 39:369–380, 2014.
5. Hamadi, Y., Jabbour, S., Sais, L. Control-based clause sharing in parallel SAT solving. In Proceedings of the 21st International Joint Conference on Artificial Intelligence (IJCAI 2009). pp. 499–504.
6. Заикин О.С., Семенов А.А. Применение метода Монте-Карло к прогнозированию времени параллельного решения проблемы булевой выполнимости // Вычислительные методы и программирование: новые вычислительные технологии. 2014. Т. 15. Вып. 1. С. 22-35.
7. T. Eibach, E. Pilz, G. Volkel. Attacking Bivium Using SAT Solvers. LNCS, vol. 4996, Springer, 2008. pp. 63–76.
8. Заикин О.С., Посыпкин М.А., Семёнов А.А., Храпов Н.П. Опыт организации добровольных вычислений на примере проектов OPTIMA@home и SAT@home // Вестник ННГУ. № 5(2). 2012. С. 338-346.
9. Манзюк М.О., Заикин О.С. CluBORun: средство использования свободных ресурсов вычислительных кластеров для BOINC-расчетов // Труды научной конференции «Высокопроизводительные вычисления на базе BOINC: фундаментальные исследования и разработки». ИПМИ КарНЦ РАН. 2013. С. 9-14.