Секция 7

ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

УДК 519.7

ИСПОЛЬЗОВАНИЕ ГРАФИЧЕСКИХ УСКОРИТЕЛЕЙ В РЕШЕНИИ ЗАДАЧ КРИПТОАНАЛИЗА

Д. В. Беспалов, В. Г. Булавинцев, А. А. Семёнов

Первые идеи использования для решения трудоемких (переборных) задач специализированных вычислительных архитектур возникали еще в 70-х годах прошлого века. В качестве одного из наиболее ярких примеров можно привести предложенный У. Диффи и М. Хеллманом проект вычислительного устройства (см. [1, 2]), предназначенного для криптоанализа шифра DES простым перебором (метод «грубой силы»). Стоимость устройства на тот момент составляла около 20 млн долларов. На сегодняшний день стоимость криптоанализа DES методом «грубой силы» понижена до $\approx$ 10 тыс. долларов. Соответствующие атаки используют специальные вычислители на ПЛИСах [3]. Следует отметить, что само по себе «программирование» ПЛИС требует определенных навыков, относящихся не столько к собственно программированию, сколько к схемотехнике.

Другой перспективной в плане применимости к криптоанализу архитектурой являются активно развивающиеся в последние годы графические ускорители (GPU), специализированные под потоковые вычисления. Понимание серьезных вычислительных возможностей GPU (пусть даже на немногочисленных пока классах задач) мотивирует их производителей постоянно совершенствовать архитектуру и программное обеспечение.

В работе сообщаются результаты применения метода «грубой силы» к криптоанализу известных систем шифрования: A5/1 и DES. На примере решения этих задач демонстрируются трудности реализации даже весьма примитивных алгоритмов на современных GPU. Описывается ряд техник и приемов организации вычислений, позволяющих частично или полностью обходить ограничения GPU-архитектур при решении переборных задач. В частности, детально описывается технология замены условных переходов арифметико-логическими выражениями. Ее применение к криптоанализу методом «грубой силы» генератора A5/1 дает существенный прирост производительности по сравнению с «обычной схемой». При решении этой задачи также был использован простейший препроцессинг: независимо сгенерированные 64 сдвига для каждого из РСЛОСов генератора A5/1 загружались в память GPU, после чего запускался процесс перебора. В применении к криптоанализу шифра DES методом «грубой силы» предложена новая техника реализации на GPU дискретных функций S-блоков: для построения максимально компактных представлений данных функций формулами используются двоичные диаграммы решений (BDD).

Из полученных в ходе исследований результатов можно сделать следующие выводы. Описанная атака на DES, реализованная на GPU, по стоимости превосходит подобные атаки, реализованные на ПЛИСах. Однако рост производительности GPU

оставляет в этом направлении существенные перспективы. Атака на A5/1 методом «грубой силы» бесперспективна из-за большей, в сравнении с DES, длины ключа. Кроме этого, данная атака по эффективности более чем в 200 раз проигрывает известной SAT-атаке [3], реализация которой на GPU невозможна вследствие целого комплекса ограничений современных GPU-архитектур: отсутствие поддержки рекурсии, неэффективная обработка условных переходов, ограниченные возможности адресации памяти. Можно надеяться, что огромный интерес в мире к GPU-вычислениям позволит в ближайшее время в значительной степени преодолеть эти ограничения.

ЛИТЕРАТУРА

1. *Diffie W., Hellman M.* Exhaustive cryptanalysis of NBS data encryption standard // Computer. 1977. V. 10. P. 74–84.
2. *Hellman M.* A cryptanalytic time-memory trade-off // IEEE Trans. Inf. Theory. 1980. V. IT-26. P. 401–406.
3. *Kumar S., Paar C., Pelzl J., et al.* How to Break DES for Euro 8,980 // II Workshop on Special-purpose Hardware for Attacking Cryptographic Systems (SHARCS). Germany. 2006.
4. *Семенов А. А., Заикин О. С., Беспалов Д. В., и др.* Решение задач обращения дискретных функций на многопроцессорных вычислительных системах // Труды IV Междунар. конф. PACO'2008 (Москва, 26–29 октября 2008). 2008. С. 152–176.

УДК 519.7

ЭКСПЕРИМЕНТАЛЬНАЯ ОЦЕНКА СКОРОСТИ ПРОГРАММНОЙ РЕАЛИЗАЦИИ НЕКОТОРЫХ ПРЕОБРАЗОВАНИЙ, ИСПОЛЬЗУЮЩИХСЯ ПРИ СИНТЕЗЕ БЛОЧНЫХ КРИПТОСХЕМ

А. А. Дмух

Основными параметрами современных блочных криптосхем являются линейные преобразования, действующие на блоке, и нелинейные преобразования, представляющие собой параллельное применение нелинейных преобразований (подстановок) на блоках меньшей длины. В [1] указывается, что для обеспечения стойкости блочной криптосхемы линейные преобразования должны обладать достаточно хорошими рассеивающими свойствами. При этом основная трудоемкость одной итерации блочной криптосхемы, как правило, приходится на вычисление линейного преобразования.

При синтезе линейных преобразований разработчики пытаются достичь «золотой середины» между такими относительно противоречивыми требованиями к линейному преобразованию блочной криптосхемы, как максимизация скорости вычисления, минимизация памяти, необходимой для хранения, и достаточно хорошие рассеивающие свойства.

На данный момент в криптографической практике для реализации на ЭВМ одной итерации блочной криптосхемы используют подход (см., например, [2]), который заключается в использовании заранее вычисленных таблиц, в которых хранится результат композиции нелинейного и линейного преобразований. Результат применения одной итерации (после наложения ключа) представляет собой сумму по модулю 2 содержимого таблицы, взятого по байтам-адресам. Наилучшие показатели по скорости шифрования и количеству тактов процессора, необходимых для зашифрования одного байта, достигаются в случае, если таблица может быть целиком помещена в кэш-память процессора.