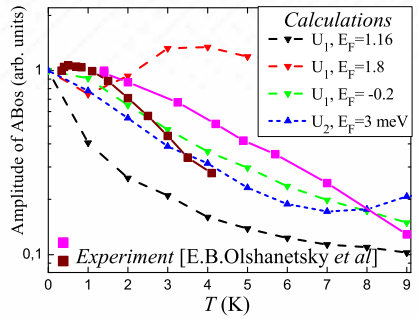

Рис. 4.
Вычисленные и измеренные температурные зависимости амплитуды осцилляций Аронова-Бома. U1, U2– реализации потенциала, отвечающие небольшому (10%) изменению коэффициента связи глубины травления с измеренной высотой рельефа локального анодного окисления. EF – значения химпотенциала. Экспериментальные зависимости измерены в разных криостатах, т.е. отвечают разным распределениям заряда на примесях в слоях легирования

туды осцилляций АБ с изменением химпотенциала [3]. Нестабильность темпа теплового подавления осцилляций действительно обнаружена в измерениях с данной структурой [3]. Заметим, что в основе объяснения эффекта лежало решение задачи двумерного квантового рассеяния для 150 000 пар (E, B), что требовало 6 часов счета на 64 процессорах машины Zahir суперкомпьютерного центра IDRIS (France, http://www.idris.fr). Соответствующее время для решения аналогичной задачи на настольном компьютере было в 300 раз больше.

Дальнейшая работа в обозначенном направлении поддержана Интеграционным проектом ИП-26 СО РАН (блок 1.10) и Программой Президиума РАН №21 "Основы фундаментальных исследований нанотехнологий и наноматериалов" (проект 1.13.6).

СПИСОК ЛИТЕРАТУРЫ

1. *Ткаченко О.А., Ткаченко В.А., Квон З.Д., Латышев А.В., Асеев А.Л.* Интроскопия квантовых наноэлектронных устройств // Российские нанотехнологии. 2010. Т. 5, № 9–10. С. 93–103.
2. *Renard V.T., Tkachenko O.A., Tkachenko V.A., Ota T., Kumada N., Portal J.C., Hirayama Y.* Boundary-Mediated Electron-Electron Interactions in Quantum Point Contacts // Phys. Rev. Lett. 2008. V. 100. P. 186801-1–186801-4.
3. *Tkachenko O. A., Tkachenko V. A., Baksheev D. G., Portal J.*-C. Mesoscopical behavior of Aharonov-Bohm effect in small ring interferometer /Proc. 13th Intl. Symp. Nanostructures: Physics and Technology (St. Petersburg, 2005.). P. 205–206; *Olshanetsky E.B., Tkachenko V.A., Tkachenko O. A., Kvon Z.D., Renard V., Scheglov D.V., Latyshev A.V., Portal J.C.* The effect of microscopic state of a ballistic ring on the Aharonov–Bohm oscillations temperature dependence / Workbook of 16th International Conference on High Magnetic Fields in Semiconductor Physics (Tallahassee, USA, 2004) rep. ThP23.

Вычисления в теории чисел и криптографии

9 Вычисления в теории чисел и криптографии

Необходимость обмена большими массивами конфиденциальной информации (не только государственной и военной, но и банковской, экономической, медицинской, юридической и т.п.), а также возможность такого обмена в связи с появлением и распространением доступных и эффективных компьютерных средств обработки этой информации способствовали появлению и активному развитию открытой криптографии. На суперкомпьютерах «Ломоносов» и «Чебышев» в МГУ проводятся исследования уязвимости некоторых криптографических алгоритмов по отношению к различного вида атакам. В частности, ведутся работы по исследованию так называемых хеш-функций и разложению больших составных чисел на множители.

АВТОРЫ:

Ю.В. Нестеренко — докт. физ.-мат. наук, чл.-корр. РАН, зав.кафедрой механико-математического факультета МГУ имени М.В.Ломоносова;
e-mail:nester@orc.ru

Любой текст может быть закодирован последовательностью чисел. Например, букве "а" можно сопоставить число 1, букве "б" — число 2 и так далее, букве "я"— число 32. Можно сопоставить числа пробелам, точке, другим знакам препинания. После этого процессы зашифрования и расшифрования информации представятся как некоторые алгоритмы, перерабатывающие одни массивы целых чисел в другие.

На суперкомпьютерах «Ломоносов» и «Чебышев» в МГУ проводятся исследования уязвимости некоторых криптографических алгоритмов по отношению к различного вида атакам. В частности, ведутся работы по исследованию так называемых хеш-функций и разложению больших составных чисел на множители.

Коллизии для хеш-функции SHA-1

Хеш-функция есть функция, отображающая сообщения (строки из 0 и 1) произвольной длины в последовательности из 0 и 1 ограниченной длины — значения хеш-функции или хеш-значения. Значение хеш-функции есть как бы отпечаток всего сообщения, а роль его подобна отпечаткам пальцев в процессе идентификации. Используемые в криптографических приложениях хеш-функции определяются стандартами. Есть такой стандарт и в России.

Для любой хеш-функции существуют сообщения, имеющие одинаковые хеш-значения, ведь множество сообщений бесконечно, а множество хеш-значений конечно. Хеш-функция считается скомпроме-тированной, если для нее построены два различных, даже бессмысленных, сообщения, имеющие совпадающее хеш-значение или, иначе говоря, если для этой хеш-функции построена коллизия.

Хеш-функция, обозначаемая SHA-1 (Secure Hash Algorithm), преобразует сколь угодно длинные сообщения в 160-битное хеш-значение. Эта хеш-функция была опубликована NIST (National Institute of Standards and Technolodgy) в США в 1995 г. и в настоящее время используется как важная составная часть различных государственных и индустриальных стандартов безопасности, таких, как электронная цифровая подпись, аутентификация пользователей, обмен ключами, построение псевдослучайных последовательностей. SHA-1 внедрена почти во все коммерческие системы безопасности.

В 2000-х гг. активно стал развиваться разностный (дифференциальный) криптоанализ в применении к хеш-функциям. С его помощью были скомпрометированы такие хеш-функции, как MD5 и SHA-0. В течение ряда лет в различных странах предпринимаются активные попытки компрометации функции

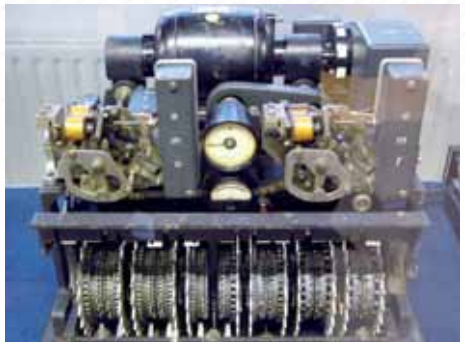

Рис. 1.
Шифровальная машина Lorenz SZ-42

SHA-1, и хотя коллизия все еще не построена, исследователи продвинулись в этой деятельности достаточно далеко. С 2007 г. NIST проводит открытый конкурс на построение новой хеш-функции, которая смогла бы заменить SHA-1. Предполагается ввести новую функцию в действие в 2012 г.

В основе вычисления хеш-значения SHA-1 лежит так называемая сжимающая функция, которая с помощью 80 раундов выполнения близких, но отличающихся операций последовательно «подмешивает» очередной 512-битовый блок сообщения к результатам вычислений, проведенных таким же образом с предыдущими блоками. Исследователи пытаются построить коллизию для упрощенной каким-либо способом хеш-функции SHA-1, последовательно приближаясь при этом к оригиналу. В 2005 г. в Австрии была построена коллизия для хеш-функции, устроенной так же, как и SHA-1, но использующей усеченную до 64 раундов сжимающую функцию. В 2007 г. та же группа ученых нашла коллизию для SHA-1 с усеченной до 70 раундов сжимающей функцией. Все эти конструкции использовали достаточно мощные вычислительные ресурсы.

В июле 2010 г. аспирант кафедры теории чисел механико-математического факультета МГУ Е. Гречников построил коллизию для функции SHA-1 с усеченной до 72, а затем и до 73 раундов сжимающей функцией. Это лучший в мире результат на сегодня. Заключительные вычисления, приведшие к нахождению коллизии, выполнялись на суперкомпьютере «Ломоносов» в МГУ. Время выполнения первого этапа построения этой коллизии составило 18 801 секунд на 8192 ядрах; ожидаемое время выполнения заключительного этапа было примерно в 16 раз больше, но при реальных вычислениях в результате «везения» построение коллизии было выполнено всего за 2693 секунд на 16 384 ядрах. Следует отметить, что при росте числа раундов необходимое время растет экспоненциально. Поэтому применение известных в настоящее время алгоритмов к полноценной 80-раундовой хеш-функции SHA-1, т.е. переход от 73 до 80 раундов, требует недоступных на сегодняшний день вычислительных ресурсов. Построение коллизии в ближайшее время требует либо радикального совершенствования известных, либо создания принципиально новых алгоритмов.

Разложение больших целых чисел на множители.

Стойкость многих криптографических алгоритмов напрямую зависит от того, насколько некоторые задачи теории чисел сложны в вычислительном отношении. Одной из них является задача разложения чисел на множители. Интерес к ней связан с известной криптосистемой RSA. В 1991 г. Лаборатория RSA для поощрения исследований в области вычислительной теории чисел и определения практической сложности задачи факторизации опубликовала ряд чисел размером от 100 до 617 десятичных знаков и объявила конкурс по их разложению. Денежные призы, назначенные за разложение некоторых из этих чисел, были отменены в 2007 г. Но большинство из предложенных чисел до сих пор остаются и, вероятно, останутся неразложенными еще в течение длительного времени. К настоящему моменту разложены все числа от RSA-100 до RSA-200, а также число RSA-768, записываемое 232 десятичными цифрами. Этот рекорд был поставлен в конце 2009 г. после почти 5 лет вычислений объединенной группой ученых из Швейцарии, Японии, Германии, Франции, США и Нидерландов. Самые маленькие из оставшихся неразложенными чисел — это RSA-210 и RSA-220 (десятичная запись), а также RSA-704, записываемое 212 десятичными цифрами.

На базе суперкомпьютеров «Ломоносов» и «Чебышев» в МГУ с использованием пакетов свободного программного обеспечения наши специалисты реализовали параллельную версию алгоритма решета числового поля, самого на сегодняшний день эффективного алгоритма, имеющего субэкспоненциальную оценку времени работы. Его основной принцип восходит еще к идеям Ферма: если представить раскладываемое число в виде разности квадратов целых чисел, то с большой вероятностью разность или сумма этих чисел содержат в своем разложении нетривиальный делитель исходного числа. Для построения пар таких чисел и используется метод решета, который позволяет эффективно набирать множества чисел с известным разложением на заданные малые простые множители (соотношения), а затем при помощи решения линейной системы комбинировать из них искомые пары. В отличие от других алгоритмов, в решете числового поля вместо рациональных чисел рассматриваются алгебраические, а вместо простых делителей — простые идеалы. Это усложняет базовые операции в алгоритме, но, с другой стороны, дает очень весомый асимптотический выигрыш во времени работы.

В период с 10 мая 2010 по 8 ноября 2010 г. И. Поповян (МГУ) и А.Тимофеев (CWI, Нидерланды) нашли разложение на простые множители числа RSA-190,

заполнив тем самым последнюю брешь на участке до RSA-200. Построение многочлена, определяющего числовое поле, было выполнено в МГУ на «Чебышеве» (100 процессоров и 4 дня работы). Нахождение соотношений просеиванием выполнялось в основном на ресурсах CWI (в МГУ выполнено 20% этой работы) и заняло почти все лето 2010 г. В результате было найдено более 1 миллиарда соотношений. После фильтрации была получена матрица размером около 33 млн строк и столбцов. Этот процесс занял порядка 38 часов на 1 процессоре «Чебышева». Получившаяся система уравнений решалась на 900 процессорах «Ломоносова», на что потребовалось около 37 часов. Завершающий этап выполнялся еще примерно 110 часов на 1 процессоре «Чебышева» и потребовал большого количества оперативной памяти, для чего были задействованы узлы с памятью 32 Гб. На «Ломоносове», где узлы по 16 Гб, на этапе фильтрации и построения матрицы памяти не хватало.

RSA-190 = 1907556405060696491061450432646028861081179759533184460647975622318915025587184175754054976155121593293492260464152630093238509246603207417124726121580858185985938946945490481721756401423481.

Два простых сомножителя этого числа равны

p=3171195257690152709485171289740475929805147316029450327784761927832793642798125654241572430961 9

q=6015260020444561641587641685526676183243543359471811072599763828083615704046048162535561940489 9

Деятельность по разложению чисел на множители опирается на фундаментальные знания теории чисел и алгебры. Вместе с тем она сочетает в себе черты инженерной науки, поскольку во многом использует допущения, основанные на опыте и все еще не имеющие теоретических обоснований, а с другой стороны, она сродни искусству, так как зачастую продолжительность работы алгоритма и результат зависят от удачного выбора параметров.

Применение суперкомпьютеров для установления механизмов биохимических реакций