Н. А. Каленикова, В. А. Минаев, В. П. Хренов

УЛУЧШЕНИЕ МЕТОДА ФЕРМА: НОВЫЙ АЛГОРИТМ ФАКТОРИЗАЦИИ

Алгоритм факторизации был получен П. Ферма в 1643 г. Основная его идея состоит в том, что составное число C является разностью квадратов, т. е. $C = \rho \cdot q = a^2 - b^2 = (a - b)(a + b)$, где $a = \frac{p+q}{2}$, а $b = \frac{p-q}{2}$.

Поэтому значение a находится последовательным перебором чисел из множества $\{E(\sqrt{C})+1, E(\sqrt{C})+2, E(\sqrt{C})+3,...\}$[1] до тех пор, пока не встретится такое a, что значение $a^2 - C$ будет являться точным квадратом, т. е. b^2.

Метод Ферма относится к способу факторизации с экспоненциальной сложностью. Р. Леман усовершенствовал алгоритм факторизации Ферма таким образом, что в худшем случае для его выполнения требуется $o(C^{\frac{1}{3}})$ операций [1].

В 1982 г. Х.Уильямс предложил метод факторизации с помощью последовательностей чисел Люка. В том же году Д. Поллард предложил свой метод факторизации с $o(B \log B \log^2 N)$ действий (B — максимальный простой делитель). В те же годы А. Ленстра предложил метод факторизации с помощью эллиптических кривых, появились и другие подходы [2].

В связи со сказанным сложность проблемы факторизации до некоторого времени делала алгоритм шифрования RSA, основанный на произведении двух простых чисел, весьма надежным.

Важно отметить, что знание закона образования простых чисел [3] дает возможность создавать новые методы факторизации, не прибегая к помощи достаточно трудоемких тестов проверки простоты чисел. Это существенно ускорит разработку новых алгоритмов факторизации.

Именно на знании закона образования простых чисел и основан изложенный в настоящей статье алгоритм факторизации, улучшающий метод Ферма.

Согласно работе [4], в которой описывается закономерность образования простых чисел, множество натуральных чисел образовано единицей, подмножеством из двух простых чисел ${}_1P = \{2, 3\}$, подмножеством простых чисел вида ${}^-P$ {5, 11, 17, …}, полученных путем вычитания единицы из чисел, кратных 6 {6n — 1}, n = 1,2,3,… (назовем их минус-простыми числами ${}^-\rho$ — МПЧ), подмножеством ${}^+P$ простых чисел {7, 13, 19, …}, образованным при помощи прибавления единицы к числам, кратным 6 {6n — 1}, n = 1,2,3,… (назовем их плюс-простыми числами ${}^+\rho$ — ППЧ), подмножествами четных ${}_2C$ и нечетных чисел ${}_3C$ и подмножествами ${}^-C$ и ${}^+C$ составных чисел, также получаемых вычитанием либо прибавлением единицы к числам, кратным 6. По аналогии назовем их минус-составными числами (МСЧ) и плюс-составными числами (ПСЧ).

Числа, к которым может быть эффективно применим метод Ферма, — это элементы множеств МСЧ и ПСЧ. По определению [4], ПСЧ ${}^+C$ может быть получено произведением как двух ППЧ ${}^+C = {}^+\rho \cdot {}^+q$, так и двух МПЧ ${}^+C = {}^-\rho \cdot {}^-q$, а МСЧ ${}^-C$ образуется произведением МПЧ и ППЧ ${}^-C = {}^+\rho \cdot {}^-q = {}^-\rho \cdot {}^+q$ [3].

Новый алгоритм факторизации

Разложения на множители МСЧ:

Если имеется МСЧ ${}^-C = {}^+\rho \cdot {}^-q = {}^-\rho \cdot {}^+q$, то метод факторизации Ферма можно улучшить не менее, чем в 6 раз, руководствуясь следующей процедурой:

1. Вычислить значение $g = \frac{{}^-C+1}{6}$ и, если оно четно, перейти к указанию 2, а если нечетно, то к указанию 3;

2. Среди чисел вида $E(\sqrt{{}^-C})+1, E(\sqrt{{}^-C})+2, E(\sqrt{{}^-C})+3,...$ исследовать на полный квадрат только числа, делящиеся нацело на 6;

[1] Обозначение $E(x)$ введено Лежандром в 1798 г. для функции «целая часть от x».

3. Среди чисел вида $E(\sqrt{{}^{-}C})+1, E(\sqrt{{}^{-}C})+2, E(\sqrt{{}^{-}C})+3,...$ исследовать на полный квадрат только числа, имеющие в остатке 3 при делении на 6.

В общем виде это утверждение выглядит так:

Утверждение 1: Если составное число — число вида ${}^{-}C={}^{+}p\cdot{}^{-}q={}^{-}p\cdot{}^{+}q$, то среднее арифметическое $a=\frac{{}^{+}p+{}^{-}q}{2}$ нацело делится на 6 при четном значении g или имеет в остатке 3 при нечетном значении g.

Доказательство:

Для произведения ППЧ и МПЧ, например, при ${}^{+}\rho = 6x + 1$, ${}^{-}q = 6y - 1$, где x, y натуральные, a и g примут вид:

$$a=\frac{{}^{+}p+{}^{-}q}{2}=\frac{6x+1+6y-1}{2}=3x+3y;$$

$$g=\frac{(6x+1)(6y-1)+1}{6}=6xy-x+y.$$

В зависимости от значений x и y возможны следующие случаи:

1. x и y — четные числа, $x = 2m$ и $y = 2n$, имеем $a=3x+3y=6m+6n$, следовательно, a делится на 6 нацело, а число $g = 6 \cdot 2m \cdot 2n - 2m + 2n = 2\,(12\,mn - m + n)$ — четное.

2. x и y — нечетные числа вида $x = 2m - 1$ и $y = 2n - 1$

$a=3x+3y=3\cdot(2m-1)+3\cdot(2n-1)=6(m+n-1)$, т. е. a нацело делится на 6.

Так как $g = 6 \cdot (2m - 1)(2n - 1) - 2m + 1 + 2n - 1 = 2\,(12\,mn - 7m - 5n + 3)$, то оно, так же как и в случае 1, четное.

3. x — четное, а y — нечетное (или наоборот, что равносильно) числа вида $x = 2m$ и $y = 2n - 1$, тогда $a=3\cdot 2m+3\cdot(2n-1)=6m+6n-3$ имеет при делении на 6 в остатке 3.

$g = 6 \cdot 2m(2n - 1) - 2m + 2n - 1 = 24mn - 14m + 2n - 1 => g$ — нечетное число.

Пример 1:

Рассмотрим составное число $C = 70098131$. Выяснить, составное оно или простое, легко можно с помощью линейного генератора простых чисел подряд [5].

Поскольку g = 11683022 — число целое и четное, значит, исходя из выше приведенного доказательства, C является МСЧ.

Согласно доказанному выше алгоритму, если число g — четное, то на полный квадрат необходимо исследовать только числа, делящиеся нацело на 6.

Вывод: решая задачу факторизации методом Ферма, необходимо вычислить 93 значения $a^2 - {}^{-}C$ и проверить, является ли каждое из них полным квадратом. Используя предложенное улучшение метода, достаточно вычислить и проверить лишь 15 значений $a^2 - {}^{-}C$.

Пример 2: Для разложения на простые сомножители МСЧ ${}^{-}C = 58420049$ методом Ферма необходимо вычислить 213 значений $a^2 - {}^{-}C$ и проверить, является ли каждое из них полным квадратом. Используя предложенное улучшение метода, достаточно вычислить и проверить лишь 35 значений $a^2 - {}^{-}C$.

Разложение на множители ПСЧ:

В случае, если раскладывать на множители методом Ферма составное число вида ${}^{+}C$, то возможных остатков от деления a на 6 будет больше. Это связано с тем, что оно может быть образовано двумя способами: ${}^{+}C = {}^{-}\rho \cdot {}^{-}q$ и ${}^{+}C = {}^{+}\rho \cdot {}^{+}q$. В таком случае улучшить скорость работы факторизации Ферма можно в 3 раза. Соответствующее описание алгоритма выглядит следующим образом:

1. Вычислить значение $f = \frac{^{+}C - 1}{6}$ и, если оно четно, перейти к указанию 2, а если нечетно, то к указанию 3;

2. Среди всех возможных значений $a = \frac{^{-}p + ^{-}q}{2}$ для нахождения значения, являющегося полным квадратом, необходимо рассматривать только числа, имеющие при делении на 6 в остатке 1 или 5;

3. Среди всех возможных значений $a = \frac{^{-}p + ^{-}q}{2}$ для нахождения значения, являющегося полным квадратом, необходимо рассматривать только числа, имеющие при делении на 6 в остатке 2 или 4.

Утверждение 2: Если $^{+}C = ^{-}p \cdot ^{-}q$, то остаток от деления среднего арифметического $a = \frac{^{-}p + ^{-}q}{2}$ на 6 равен 5 при четном значении f и 2 при нечетном f.

Доказательство:

Для произведения МПЧ и МПЧ

$^{-}\rho = 6x - 1$ и $^{-}q = 6y - 1$, где x, y — натуральные,

$$a = \frac{^{-}p + ^{-}q}{2} = \frac{6x - 1 + 6y - 1}{2} = 3x + 3y - 1;\ f = 6xy - x - y.$$

В зависимости от значений x и y возможны следующие случаи:

1. x и y — четные числа: $x=2m$, $y=2n$, имеем: $a = 6m + 6n - 1$.

Таким образом, остаток от деления a на 6 равен 5. При этом $f = 6 \cdot 2m \cdot 2n - 2m - 2n = 2(12\ mn - m - n)$, т. е. f — четное число.

2. Когда x и y — нечетные числа вида $2m - 1$ и $2n - 1$ соответственно: $a = 6m + 6n - 7$ и остаток от деления a на 6 равен 5. При этом

$f = 6\ (2m - 1)(2n - 1) - 2m + 1 - 2n + 1 = 2\ (12\ mn - 7m - 7n + 4)$ — четное число.

3. Для сочетания, когда x — четное, а y — нечетное или наоборот: $a = 6m + 6n - 4$. При делении a на 6 остаток равен 2. При этом

$f = 6 \cdot 2m(2n - 1) - 2m - 2n + 1 = 24mn - 14m - 2n + 1$ — нечетное число, так как при делении на 2 имеет в остатке единицу.

Утверждение 3: Если $^{+}C = ^{+}\rho \cdot ^{+}q$, то среднее арифметическое $a = \frac{^{+}p + ^{+}q}{2}$ имеет в остатке 1 при делении на 6, если значение f четно, или остаток равен 4 при нечетном значении f.

Доказательство утверждения аналогично двум предыдущим.

Пример 3:

Для разложения на простые сомножители ПСЧ $^{+}C = 71396707$ методом Ферма необходимо вычислить 116 значений $a^2 - C$ и проверить, является ли каждое из них полным квадратом. Используя предложенное улучшение метода, достаточно вычислить и проверить лишь 39 значений $a^2 - C$.

Стоит отметить, что в алгоритме RSA простые ρ и q рекомендуется выбирать таким образом, чтобы задача разложения числа C была достаточно сложна в вычислительном плане. Одним из требований, предъявляемых к используемым в RSA простым числам, является небольшая величина наибольшего общего делителя чисел $\rho - 1$ и $q - 1$; желательно, чтобы НОД($\rho - 1$, $q - 1$) = 2 [10].

Легко показать, используя закон формирования простых чисел [3], что НОД($\rho - 1$, $q - 1$) = 2 только в двух случаях: когда ρ представимо в виде $6n + 1$ и q — в виде $6m - 1$ или при $\rho = 6n - 1$ и $q = 6m - 1$, т. е. составное число может быть как ПСЧ, так и МСЧ, но ПСЧ в этом случае формируется только как произведение МПЧ и МПЧ.

Таким образом, из рассмотренных выше утверждений практическое приложение для алгоритма факторизации применительно к RSA могут иметь только первые два. Их можно объединить в следующую систему указаний:

1) Выяснить, элементом какого множества является число C: ПСЧ или МСЧ.
2) Если C – МСЧ, воспользоваться утверждением 1, иначе утверждением 2.

Итак, в связи с тем, что в шифровании методом RSA не участвуют одновременно два ППЧ, предложенный в работе алгоритм, применимый к криптосистеме RSA, эффективнее метода факторизации Ферма не менее чем в 6 раз.

В заключение необходимо отметить, что при последовательном вычислении скорость работы предложенного алгоритма не может конкурировать со способами факторизации с субэкспоненциальной сложностью. Наиболее эффективным из них на данный момент считается алгоритм решета числового поля, эвристическая оценка сложности которого составляет $e^{(k+o(1))(\log C)^{\frac{1}{3}}(\log\log C)^{\frac{2}{3}}}$ арифметических операций при некоторой постоянной k [2]. Но, в отличие от последнего, предложенный нами алгоритм может быть легко распараллелен, что дает возможность существенно увеличить его эффективность по мере подключения вычислительных мощностей при осуществлении факторизации.

СПИСОК ЛИТЕРАТУРЫ:

1. *Lehman R. S.* Factoring Large Integers // Math. Comp. 1974. V. 28. P. 637–646.
2. *Василенко О. Н.* Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО, 2003.
3. *Минаев В. А., Хренов В. П.* Безопасность в сфере конфиденциальной информации и закон формирования простых чисел // Спецтехника и связь. 2008. № 3 (ноябрь–декабрь). С. 45–48.
4. *Минаев В. А., Хренов В. П.* Открытые закономерности образования простых чисел и некоторые прикладные аспекты открытия // Вестник Российского нового университета. Сборник научных трудов – Управление, вычислительная техника и информатика. Вып. 3. М.: РосНОУ, 2008. С. 49–59.
5. *Хренов В. П.* Свидетельство № 2005613012 от 22 сентября 2005 г. О регистрации программы «Линейный генератор простых чисел подряд».
6. *Кнут Д.* Искусство программирования. Т. 2. Получисленные методы. 3-е изд. М.: Вильямс, 2007.
7. *Коблиц Н.* Курс теории чисел и криптографии. М.: Научное издательство ТВП, 2001.
8. *Фомичев В. М.* Дискретная математика и криптология. Курс лекций. М.: Диалог-МИФИ, 2003.
9. *Minaev V. A., Khrenov V. P., Zernov V. A.* Discovery of Natural Number Laws and Some Applied Aspects of Discovery. Recent Advanced in Management and Information Security // 1st International Conference on Management of Technologies & Information Security. 21–24 January, 2010. New Delhi, Shree Publishers & Distributors, 2010.
10. *Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.* Основы криптографии. М.: Гелиос АРВ, 2002.