УДК 621. 391.7

МУЛЬТИПОЛИНОМИАЛЬНЫЙ ВАРИАНТ МЕТОДА "КВАДРАТИЧНОГО РЕШЕТА" ФАКТОРИЗАЦИИ RSA МОДУЛЯ СИСТЕМЫ АУТЕНТИФИКАЦИИ

д.т.н., проф. Ю.В. Стасев, к.т.н., проф. Л.С. Сорока, А.А. Смирнов

В статье рассматриваются каналы уязвимости RSA систем аутентификации с точки зрения факторизации модуля. Даётся описание мультиполиномиального варианта одного из методов факторизации - метода "Квадратичного решета".

Стойкость системы RSA обеспечивается за счёт выбора в качестве составляющих модуля **N** таких больших сильных простых чисел **p** и **q** [1], для которых процедура разложения на сомножители числа **N** (процедура факторизации числа **N**) в вычислительном отношении оказывается практически не реализуемой (требуемый объём вычислительных затрат превосходит реальные практические возможности) [2]. Большинство алгоритмов факторизации базируются на квадратичном сравнении [3]:

$$\mathbf{X^2 \equiv Y^2 (mod\ N)} \qquad (1)$$

со свойством

$$\mathbf{X \not\equiv \pm Y (mod\ N)}.$$

Если выполнено:

$$\mathbf{N \mid X^2 - Y^2 = (X+Y)\cdot(X-Y)};$$

$$\mathbf{N \not\mid (X-Y)} \text{ и } \mathbf{N \not\mid (X+Y)},$$

то **НОД (X+Y, N)** и **НОД(X-Y, N)** есть делители **N**.

Алгоритмы, основанные на квадратичном сравнении, различаются лишь по способу действия, как находится или образовывается сравнение (1).

В общем случае в "квадратичном решете" это сравнение образовывается путем комбинации [4] сравнений $\mathbf{r_i}$ вида

$$\mathbf{X_i^2 \equiv Y_i (mod\ N)}. \qquad (2)$$

Сравнение такого вида описываются в дальнейшие как отношения. Когда находят несколько таких отношений, определяют подмножество **S**, удовлетворяющее условию

$$\prod_{r_i \in S} Y_i \equiv Y^2 \pmod{N}.$$

Для определения этого, подмножества разлагаются на простые сомножители Y_i. Таким образом

$$X^2 \equiv \prod_{r_i \in S} X_i^2 \equiv \prod_{r_i \in S} Y_i \equiv Y^2 \pmod{N}.$$

На основе принципа действия разделяют алгоритм на 2 фазы. В первой фазе находятся отношения вида (2), во второй фазе найденные отношения приводятся к квадратичному сравнению.

Для нахождения отношений выбирают полином $Q(z)$ второй степени, значение функции квадрата по модулю N которого равно:

$$\forall_{z \in Z} \exists_{H \in Z} \; Q(z) \equiv H^2 \pmod{N}.$$

При реализации классического метода “квадратичного решета” используются полиномы вида

$$Q(z) := \left(z + \left\lfloor \sqrt{N} \right\rfloor\right)^2 - N.$$

Последовательность величин значений функции важна, так как требуется их разложение на простые сомножители.

Выбор полиномов осуществляется последовательным увеличением размера решета до тех пор, пока не обнаружат необходимые отношения (больше чем элементов фактор-базы). Вероятность того, что значение функции целиком разложится по фактор - базе, может исчисляться с помощью ρ - функции.

Для постоянного $L \in N$, случайно избранного числа $Y \in [1...L]$ и $\alpha \geq 1$ со свойствами

$$p_i > p_{i+1},\ p_i \in P \text{ и } p_i \mid Y$$

$\rho(\alpha)$ определяют как вероятность того, что самый большой простой сомножитель p_i числа Y меньше $L^{1/\alpha}$:

$$\rho(\alpha) := \lim_{L \to \infty} P\left(p_1 < L^{1/\alpha}\right).$$

Для ρ - функции выполняется сравнение

$$\alpha \rho'(\alpha) + \rho(\alpha - 1) = 0$$

и может решаться путем численного интегрирования [5] :

$$\rho(\alpha) = \begin{cases} 1, & \text{для } 0 \le \alpha \le 1; \\ \dfrac{1}{\alpha} \displaystyle\int_{\alpha-1}^{\alpha} \rho(t)dt, & \text{для } \alpha > 1. \end{cases}$$

Для $5 < \alpha < 11$ может использоваться следующее приближение [3]:

$$\rho(\alpha) \approx \exp\left(-\alpha \cdot \left(\log(\alpha) + 0.56 - \frac{1}{\log(\alpha)}\right)\right).$$

При этом из ряда размеров значений функции выбирается L, а после определяется α, так что

$$L^{\frac{1}{\alpha}} = p_{max} := \max\{p \in FB\}.$$

Для того, чтобы разложить значения функции $Q(z)$, выбирают постоянное множество простых чисел, называемое фактор-базой (ФБ), и границу $M \in Z$. С помощью "решета" находят периодические значения функции полинома $Q(z)$ (для $z \in [-M, M]$), который раскладывается этой фактор - базой и получают отношение вида

$$Q(z_j) = \prod_{p_i \in FB} p_i^{e_{ij}} (= Y_j) \equiv X_j^2 \pmod N, \text{ для } e_{ij} \in N \cup \{0\}. \qquad (3)$$

Увеличение интервала "решета" (и вместе с ним значений функции, подлежащих разложению) ведет к быстрому уменьшению этой вероятности. Для пояснения этого эффекта рассматривают фиктивную факторизацию числа $N \approx 10^{100}$ основной версией квадратичного решета. Это приводит, при реалистичном размере фактор-базы $|FB| \approx 10^5$, к интервалу решета $[1, 5 \cdot 10^{15}]$. Найденная вероятность, оценивает то, что значение функции которая целиком разложилось по фактор-базе, находится в интервале $[1, 2*10^{11}]$. В интервале $[1, 10^8]$ эта вероятность в 50 раз выше. Эти наблюдения проведены для того, чтобы попробовали получить как можно меньший интервал решета. Это достигается путем применения нескольких полиномов, которые удовлетворяют поставленным к оригинальному полиному условиям. В противоположность относительно основной версии квадратичного решета выбирают постоянную длину интервала решета и варьируют количеством применяемых полиномов.

Мультиполиномиальная модификация имеет также влияние на раздел алгоритма на фазы. Если учитывают функциональность модифицированного алгоритма, то образовывается следующий утонченный раздел на фазы, вернее на модули. При этом шаги (1) - (5) относятся к более ранней, приблизительной фазе сбора отношений, а шаг (6) представляет комбинацию отношений.

Алгоритм мультиполиномиальной модификации метода ”квадратичного решета” заключается в следующем.

Составляем фактор-базу (1)
пока (найдено недостаточно отношений для вида (3)) (2)
начало цикла
Выбираем новый полином (3)
Проходим фазу “решета” (4)
Обрабатываем данные фазы “решета” (5)
конец цикла
Решить линейную систему сравнений (6)

На практике линейная система сравнений решается только тогда, когда $\mathbf{k < F + c}$ (при этом $\mathbf{c \in N}$ есть малой константой). Как только **c>10**, существуют несколько различных решений, с помощью которых находят все нетривиальные делители $\mathbf{N}$.

После решения системы линейных сравнений, которая строится по найденным отношениям, конструируем квадратичное сравнение

$$\mathbf{X^2 \equiv Y^2 (mod\ N)}.$$

Чтобы обнаружить делители числа **N**, вычисляем

$$\mathbf{НОД(X - Y, N)} \text{ и } \mathbf{НОД(X + Y, N)}.$$

При этом обходят вычисление корня при вычислении **X** и **Y,** в котором **X** и **Y** вычисляют непосредственно, а не сперва $\mathbf{X^2}$ и $\mathbf{Y^2}$.

Пусть $\boldsymbol{l}$ - число отношений, которые использовались при построении линейной системы сравнений. Система сравнений имеет $\boldsymbol{l}$ строк и решением является вектор

$$\boldsymbol{\lambda} = (\lambda_1, ..., \lambda_l) \text{ такие что } \lambda_j \in \{0,1\}, \text{ для } j \in \{1, ..., l\}.$$

Для вычисления **X** и **Y** перемножают те отношения, которые относятся к ним и равны 1. **Y** вычисляют из

$$\mathbf{Y^2 \equiv \prod_{p_i \in FB} p_i^{\sum_{j=1}^{l} (e_{i,j} \cdot \lambda_j)} (mod\ N)}$$

с тем, чтобы

$$\mathbf{Y \equiv \prod_{p_i \in FB} p_i^{\frac{\sum_{j=1}^{l} (e_{i,j} \cdot \lambda_j)}{2}} (mod\ N)}.$$

Составляют все степени элементов фактор - базы и делят это значение пополам, перед тем как возводят с ним в степень элементы фактор-базы. Это возможно, поскольку после конструирования, степени каждого элемента фактор - базы будут четными.

При записи в память **j**-го отношения вида (3) записывается каждый раз только $\mathbf{X_j}$, так что **X** может вычисляться из

$$\mathbf{X \equiv \prod_{j=1}^{l} (X_j)^{\lambda_j} (mod\ N)}.$$

Теперь тестируют, есть ли $\mathbf{НОД(X-Y,N)}$ и $\mathbf{НОД(X+Y,N)}$ делителями **N**. Если никакого делителя не обнаружили, то проверяют, приводит ли следующее решение системы сравнений к делителям. Для каждого решения системы сравнений вероятность нахождения делителей составляет в среднем 50 %. Если **N** имеет больше чем 2 делителя, то получают все делители путем рассмотрения следующих решений.

Таким образом, рассмотрен мультиполиномиальный вариант "квадратичного решета" факторизации RSA модуля.

Вывод. Мультиполиномиальная версия метода "квадратичного решета" в отличие от классической версии требует меньших временных затрат. Это является основным параметром для определения стойкости RSA модуля или эффективности данного математического аппарата при решении задачи факторизации больших простых чисел. При практической реализации метода 256 битовое число было факторизовано за 70 минут. Если не будет открыто принципиально новых методов, то 2048 - битный RSA - ключ будет всегда оставаться безопасным от угрозы факторизации, но, к сожалению, никто не может предсказать этого точно.

ЛИТЕРАТУРА

1. *Jonh Gordon. Strong Primes are Easy to Find. - Advances in Cryptology. EUROCRYPT'85.*
2. *Диффи У. Первые десять лет криптографии с открытым ключом // ТИИЭР. – 1988. – Т.76, №5. – С. 54 - 74.*
3. *Wunderlich M.C. Computational Methods for factoring large integers // Abacus 5. – 1988. – No. 2. – P. 19 - 33.*
4. *Виноградов И.М. Основы теории чисел. – М.: Наука, 1987. – 176 с.*
5. *Пискунов Н.С. Дифференциальное и интегральное исчисление. – М.: Наука, 1985. – 431 с.*

Поступила 15.01.2002

СТАСЕВ Юрий Владимирович, *доктор техн. наук, профессор, начальник факультета ХВУ. Закончил ХВВКИУ в 1981 году. Область научных интересов – защита информации в автоматизированных системах управления и сетях.*

СОРОКА Леонид Степанович*, канд. техн. наук, профессор. Закончил ХВВКУ в 1974 году. Область научных интересов – методы и средства обработки информации.*

СМИРНОВ Алексей Анатольевич*, адъюнкт Харьковского военного университета. В 1999 году закончил Харьковский военный университет. Область научных интересов – защита информации в автоматизированных системах управления и сетях.*