УДК 511.215

Мохор В.В., д.т.н., профессор, ИССЗИ НТУУ “КПИ”, Киев
Жилин А.В. ИССЗИ НТУУ “КПИ”, Киев

ПРЕДПОСЫЛКИ УЧЕТА СТРУКТУРНЫХ ОСОБЕННОСТЕЙ ПРОСТЫХ ЧИСЕЛ ПРИ РЕШЕНИИ ЗАДАЧИ ФАКТОРИЗАЦИИ В КОНТЕКСТЕ ПОСТРОЕНИЯ АТАКИ НА ШИФРОТЕКСТ, КОТОРЫЙ ЗАШИФРОВАН АСИММЕТРИЧНЫМ МЕТОДОМ ШИФРОВАНИЯ.

Pre-conditions of account of structural features of prime numbers are grounded at the decision of task of factorization. It is assumed that by offered approach it is possible to organize an attack on shifrotekst, calculable complication of which will be below exponential.

Асимметрические методы шифрование широко используются в наше время. Их популярность основана на том, что они решают проблему передачи секретного ключа. На основе этих методов построены многие алгоритмы шифрования, самый известный и широко применяемый из них это RSA. Стойкость этого алгоритма основана на трудоемкости разложения на множители (факторизации) больших чисел [2].

В общем случае вычислительная сложность процесса факторизации имеет экспоненциальный характер [3]. Оценка сложности обусловлена числом переборов возможных вариантов простого числа в двоичной форме на интервале:

$$1..\sqrt{2^n}\ , \qquad (1)$$

где n – разрядность факторизируемого числа

Количество таких простых чисел на интервале определяется формулой Чебышёва [1]:

$$\pi(a) = \frac{a}{\ln(a)}\ , \qquad (2)$$

где a - простое число.

Применяя ограничение (1) к формуле (2) имеем верхнюю границу оценки сложности процесса факторизации:

$$O_h(n) = \frac{\sqrt{2^n}}{\ln(\sqrt{2^n})} = \frac{2^{\frac{n}{2}+1}}{n * \ln 2} \qquad (3)$$

Если представить случай факторизации, реализованный определенным способом, который будет иметь вычислительную сложность ниже

экспоненциальной, то можно будет утверждать, что в общем случае процесс факторизации также будет имеет вычислительную сложность ниже экспоненциальной.

Представим факторизируемое число в двоичной форме $Z = z_0 z_1 z_2 ... z_n$, где z_0 - старший разряд числа, z_n - младший разряд числа. Оно является произведением двух простых чисел $X = x_1 x_2 x_3 x_4 ... x_k$ и $Y = y_1 y_2 y_3 y_4 ... y_k$, где x_1, y_1 - старшие разряды, x_k, y_k - младшие разряды чисел X и Y соответственно:

$$Z = X * Y.$$

$$z_i, x_j, y_j \in \{0,1\}, i = 0...n, j = 1...k, k = (n+1)/2$$

Умножим число X на Y, которые имеют по 5 разрядов ($x_1 x_2 x_3 x_4 x_5$ и $y_1 y_2 y_3 y_4 y_5$) согласно правилам умножения чисел:

$$\begin{array}{ccccccccccc}
 & & & & & x_1 & x_2 & x_3 & x_4 & x_5 & \\
 & & & & & y_1 & y_2 & y_3 & y_4 & y_5 & \\
 & & & & y_5 x_1 & y_5 x_2 & y_5 x_3 & y_5 x_4 & y_5 x_5 & & \\
 & & & y_4 x_1 & y_4 x_2 & y_4 x_3 & y_4 x_4 & y_4 x_5 & & & \\
 & & y_3 x_1 & y_3 x_2 & y_3 x_3 & y_3 x_4 & y_3 x_5 & & & & \\
 & y_2 x_1 & y_2 x_2 & y_2 x_3 & y_2 x_4 & y_2 x_5 & & & & & \\
y_1 x_1 & y_1 x_2 & y_1 x_3 & y_1 x_4 & y_1 x_5 & & & & & & \\
z_0 & z_1 & z_2 & z_3 & z_4 & z_5 & z_6 & z_7 & z_8 & z_9 &
\end{array}$$

Основываясь на этих правилах, получаем приведенную ниже систему уравнений:

$$\begin{aligned}
z_0 &= \{0,1\} = P_1 \\
z_1 &= y_1 x_1 + P_2 \\
z_2 &= y_1 x_2 + y_2 x_1 + P_3 \\
z_3 &= y_1 x_3 + y_2 x_2 + y_3 x_1 + P_4 \\
z_4 &= y_1 x_4 + y_2 x_3 + y_3 x_2 + y_4 x_1 + P_5 \\
z_5 &= y_1 x_5 + y_2 x_4 + y_3 x_3 + y_4 x_2 + y_5 x_1 + P_6 \\
z_6 &= y_2 x_5 + y_3 x_4 + y_4 x_3 + y_5 x_2 + P_7
\end{aligned} \qquad (4)$$

$$z_7 = y_3x_5 + y_4x_4 + y_5x_3 + P_8$$

$$z_8 = y_4x_5 + y_5x_4$$

$$z_9 = y_5x_5$$

где P_t - разрядный перенос.

Определим, что система в заданном виде будет иметь старшие и младшие разрядные уравнения. Старшинство уравнений определяется между ними в соответствии тому, к какому разряду факторизируемого числа оно приравнивается. Вследствие этого P_t будет представлять собой разрядный перенос с младшего разрядного уравнения. Он выражает возможное количество единиц, которые могут быть перенесены.

Необходимо заметить, что последние разряды чисел *X* и *Y* всегда равны 1 (y_5 , x_5 =1), так как эти числа простые, а простые числа нечетные и в двоичной системе счисления заканчиваются на единицу (кроме числа 2, но согласно условия берутся большие простые числа). z_0 будет принимать однозначное значение 0 или 1 (зависит от значения составных чисел).

Возьмем частный случай, когда числа *X* и *Y* равны между собой. Тогда разряды этих чисел, представленных в двоичной форме, также равны между собой. Исходя из этого, получаем систему уравнений вида:

$$z_0 = \{0,1\} = P_1$$

$$z_1 = x_1x_1 + P_2$$

$$z_2 = x_1x_2 + x_2x_1 + P_3$$

$$z_3 = x_1x_3 + x_2x_2 + x_3x_1 + P_4$$

$$z_4 = x_1x_4 + x_2x_3 + x_3x_2 + x_4x_1 + P_5$$

$$z_5 = x_1x_5 + x_2x_4 + x_3x_3 + x_4x_2 + x_5x_1 + P_6 \qquad (5)$$

$$z_6 = x_2x_5 + x_3x_4 + x_4x_3 + x_5x_2 + P_7$$

$$z_7 = x_3x_5 + x_4x_4 + x_5x_3 + P_8$$

$$z_8 = x_4x_5 + x_5x_4$$

$$z_9 = x_5x_5$$

Применим к системе следующие правила:

$$x_i * x_i = x_i$$

$x_i + x_i = 0$ с переносом x_i в старший разряд. (6)

Они основываются на Булевой алгебре и правиле умножения чисел в столбик. Используя эти правила, получаем следующую систему уравнений:

$$z_0 = \{0,1\} = P_1$$
$$z_1 = x_1 + x_2 x_1 + P_2$$
$$z_2 = x_3 x_1 + P_3$$
$$z_3 = x_2 + x_3 x_2 + x_4 x_1 + P_4$$
$$z_4 = x_1 + x_4 x_2 + P_5$$
$$z_5 = x_2 + x_3 + x_4 x_3 + P_6 \qquad (7)$$
$$z_6 = x_3 + x_4$$
$$z_7 = 0$$
$$z_8 = 0$$
$$z_9 = 1$$

Возьмем число Z, значение которого будет равно 10 0001 0001. Подставим данное значение в систему уравнений и решим ее. Разрядный перенос уберем из исходного уравнения, находя его по ходу решения системы, используя для этого правила (6). Для удобства рассмотрения системы пронумеруем ее уравнения. Исходная система уравнений будет иметь вид:

$$0:1 = P_1$$
$$1:0 = x_1 + x_2 x_1$$
$$2:0 = x_3 x_1$$
$$3:0 = x_2 + x_3 x_2 + x_4 x_1$$
$$4:0 = x_1 + x_4 x_2$$
$$5:1 = x_2 + x_3 + x_4 x_3 \qquad (8)$$
$$6:0 = x_3 + x_4$$
$$7:0 = 0$$
$$8:0 = 0$$
$$9:1 = 1$$

Решить данную систему возможно путем выражения неизвестных друг через друга и подстановку их в систему уравнений.

В (6) уравнении выразим x_3 через x_4:

$$x_3 = x_4 \qquad (9)$$

Подставим данную зависимость в систему уравнений (8).

$$0:1 = P_1$$

$$1:0 = x_1 + x_2 x_1$$
$$2:0 = x_4 x_1$$
$$3:0 = x_2 + x_4 x_2 + x_4 x_1$$
$$4:0 = x_1 + x_4 x_2$$
$$5:1 = x_2 + x_4 + x_4 x_4 \qquad (10)$$
$$6:0 = x_4 + x_4$$
$$7:0 = 0$$
$$8:0 = 0$$
$$9:1 = 1$$

Основываясь на правилах (6) получим:

$$0:1 = P_1$$
$$1:0 = x_1 + x_2 x_1$$
$$2:0 = x_4 x_1$$
$$3:0 = x_2 + x_4 x_2 + x_4 x_1$$
$$4:0 = x_1 + x_4 x_2 + x_4$$
$$5:1 = x_2 + x_4 \qquad (11)$$
$$6:0 = 0$$
$$7:0 = 0$$
$$8:0 = 0$$
$$9:1 = 1$$

Обратим внимание на то, что в системе (10) шестая строка имела вид $6:0 = x_4 + x_4$. Основываясь на правилах (6) получился разрядный перенос разряда x_4 с шестого разрядного уравнения на пятое, что учитывает вероятность наличия переносов в системе, которые полностью зависят от значений разрядного уравнения, с которого делается перенос.

В 5 уравнении выразим x_2 через x_4:

$$x_2 = (1 - x_4) \qquad (12)$$

Подставим данную зависимость в систему уравнений (11).

$$0:1 = P_1$$
$$1:0 = x_1 + (1 - x_4) x_1$$
$$2:0 = x_4 x_1$$
$$3:0 = (1 - x_4) + x_4 (1 - x_4) + x_4 x_1$$

$$4:0 = x_1 + x_4(1 - x_4) + x_4$$
$$5:1 = (1 - x_4) + x_4 \quad (13)$$
$$6:0 = 0$$
$$7:0 = 0$$
$$8:0 = 0$$
$$9:1 = 1$$

Упростим систему (13):

$$0:1 = P_1$$
$$1:0 = x_1 + (1 - x_4)x_1$$
$$2:0 = x_4 x_1$$
$$3:0 = 1 - x_4 + x_4 x_1$$
$$4:0 = x_1 + x_4$$
$$5:1 = 1 \quad (14)$$
$$6:0 = 0$$
$$7:0 = 0$$
$$8:0 = 0$$
$$9:1 = 1$$

В 4 уравнении выразим x_1 через x_4:

$$x_1 = x_4 \quad (15)$$

Подставим данную зависимость в систему уравнений (14).

$$0:1 = P_1$$
$$1:0 = x_4 + (1 - x_4)x_4$$
$$2:0 = x_4 x_4$$
$$3:0 = 1 - x_4 + x_4 x_4$$
$$4:0 = x_4 + x_4$$
$$5:1 = 1 \quad (16)$$
$$6:0 = 0$$
$$7:0 = 0$$
$$8:0 = 0$$
$$9:1 = 1$$

Основываясь на правилах (6) получим:

$$0:1 = P_1$$
$$1:0 = x_4$$

$$2:0=x_4$$
$$3:0=1+x_4$$
$$4:0=0$$
$$5:1=1 \qquad (17)$$
$$6:0=0$$
$$7:0=0$$
$$8:0=0$$
$$9:1=1$$

Анализируя систему уравнений (17) можно сделать выводы, что $x_4=1$. Подставим полученное значение равенства в равенства (15), (12) и (9):

$$x_1=x_4=1 \qquad (18)$$
$$x_2=(1-x_4)=1-1=0 \qquad (19)$$
$$x_3=x_4=1 \qquad (20)$$

Согласно условия x_5=1. Число X принимает вид:

$$X_{10}=x_1x_2x_3x_4x_{5_2}=10111_2=23_{10}$$

Возведя в квадрат вычисленный результат, получим заданное условием значение числа Z, что подтверждает правильность решения системы уравнений.

В общем виде система уравнений при равных числах *X* и *Y* будет иметь вид:

$$z_0=\{0,1\}$$
$$z_1=x_1+x_2x_1$$
$$z_2=x_3x_1$$
$$z_3=x_2+x_3x_2+x_4x_1$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$z_{k-5}=x_{n-4}+x_{n-3}x_{n-1}$$
$$z_{k-4}=x_{n-2}+x_{n-3}+x_{n-1}x_{n-2} \qquad (21)$$
$$z_{k-3}=x_{n-2}+x_{n-1}$$
$$z_{k-2}=0$$
$$z_{k-1}=0$$
$$z_k=1\ ,$$

где k – разрядность факторизируемого числа, а n – разрядность простого числа. Представим алгоритм построения этой системы, записанный формальным языком программирования:

m:=0: i:=1:
для j от 1 до n делать1 Mas[m+2,1]:=X[j]*X[j]:
пока i+j<=n делать2 Mas[m+i+1,j+1]:=X[j]*X[i+j]: i:=i+1 конец2: m:=m+2: i:=1
конец1
для i от 1 до 2*n делать1 Mas[i,n+1]:=Z[i] конец1

где Mas[ ] – массив, который определяет структуру системы уравнений вида (21).

Обобщая приведенный порядок действий над системой уравнений, можем представить алгоритм нахождения разрядов простого числа:

1. Основываясь на значении факторизируемого числа, представляем систему уравнений вида (21).
2. Выражаем некоторый старший разряд x_i в $q-ой$ строке через младший и разряд факторизируемого числа.
3. Подставляем x_i в систему уравнений.
4. Упрощаем систему, используя правила (6).
5. Шаги 2-4 проделываем до строки под номером $(n-1)/2$.

В итоге получается система с одним неизвестным x_{k-1}. Из вида системы делаем вывод, чему равен x_{k-1}. Подставляем полученное значение в выражения, которые были получены на втором шаге алгоритма. Вычисляем значения всех неизвестных разрядов простого числа.

Рассмотрим систему (7) начиная с младших разрядных уравнений. Последние три разряда факторизируемого числа всегда будут иметь однозначное значение 001, так как это определено структурой системы уравнений, которую определяют множители.

Строка 6 имеет вид $z_6 = x_3 + x_4$. Можно утверждать, что x_3 зависит от z_6, x_4. Это можно записать как:

$$x_3 = f(x_4, z_6) \qquad (22)$$

Применяя те же изыскания и основываясь на проведенных вычислениях, можно утверждать что:

$$x_2 = f(x_3, x_4, z_5, P_6) \qquad (23)$$

$$x_1 = f(x_2, x_4, z_4, P_5) \qquad (24)$$

Рассмотрим разрядные переносы P_6 и P_5. Они, как и другие в системе уравнений такого типа, выражают возможное количество единиц, которые

могут быть перенесены с младшей разрядной строки. Вследствие этого они полностью зависят от неизвестных, которые и формируют значения переносов. Значит можно утверждать, что

$$P_6 = f(x_3, x_4, z_6) \quad (25)$$

$$P_5 = f(x_2, x_3, x_4, z_5, P_6) =$$

$$= f(x_2, x_3, x_4, z_5, z_6) \quad (26)$$

Как видно из зависимости (26), переносы в старшем разрядном уравнении определенно зависят от неизвестных, которые определяются в нижних разрядных уравнениях и которые предопределяются за условием (z_5, z_6).

В зависимости (23) имеем $x_2 = f(x_3, x_4, z_5, P_6)$. Основываясь на утверждениях (22) и (25) можно записать:

$$x_2 = f(f(x_4, z_6), x_4, z_5, f(x_3, x_4, z_6))$$

$$x_2 = f(f(x_4, z_6), x_4, z_5, f(f(x_4, z_6), x_4, z_6))$$

$$x_2 = f(x_4, z_5, z_6) \quad (27)$$

Равность (27) показывает, что x_2 зависит от возможных вариантов действий над x_4, z_5, z_6. Т.е. x_2 однозначно определяется через x_4, z_5, z_6.

В зависимости (22) имеем $x_1 = f(x_2, x_4, z_4, P_5)$. Основываясь на утверждениях (27), (26) и (22) можно записать:

$$x_1 = f(f(x_4, z_5, z_6), x_4, z_4, f(x_2, x_3, x_4, z_5, z_6))$$

$$x_1 = f(f(x_4, z_5, z_6), x_4, z_4, f(f(x_4, z_5, z_6),\ f(x_4, z_6), x_4, z_5, z_6))$$

$$x_1 = f(x_4, z_4, z_5, z_6) \quad (28)$$

Равность (28) показывает, что x_1 зависит от возможных вариантов действий над x_4, z_4, z_5, z_6. Т.е. x_1 однозначно определяется через x_4, z_4, z_5, z_6.

Проанализировав приведенные утверждения, и проведя аналитические исследования зависимостей значений разрядов простых чисел друг от друга и от значений разрядов факторизируемого числа, основываясь на системе уравнений вида (21) и ее алгоритме построения, можно привести обобщенные выводы.

Обозначим:

k – разрядность простого числа

x_i – разряд простого числа

$X\{x_i\} \mid i = 1...k$ – множество значений разрядов простого числа.

$Z\{z_q\} \mid q = 0...n$ – множество значений разрядов факторизируемого числа

$P\{P_l\} \mid l = 1...n-1$ – множество значений переносов

$XZ\{x_i, z_q, P_l\} = X\{\} + Z\{\} + P\{\}$

$X_i\{\} \subset XZ\{\}$

$x_i = f(X_i\{\})$ - x_i зависит от элементов множества $X_i\{\}$

Вывод зависимостей значений разрядов простых чисел друг от друга и от значений разрядов факторизируемого числа приобретает вид:

$i = 1...k-2$

если i нечетное, то $x_i = f(X_i\{x_j, z_q, P_{q+1}\})$,

где $j = i+1...k-1, q = k-2+i..n-4$

если i четное, то $x_i = f(X_i\{x_j, z_q, P_{q+1}\})$,

где $j = i+1...k-1, j \neq (n-i)/2, q = k-2+i...n-4$ если $i = k-2$, то $x_i = f(X_i\{x_j, z_q\})$,

где $q = 2*i$.

Раскрывая зависимости, приходим к утверждению:

$$x_i = f(X_i\{x_{k-1}, z_q\}), \qquad (29)$$

где $q = \frac{n-1}{2} + i - 1...n-3 = k+i-2...2*k-4$.

С утверждения (29) видно, что любой разряд простого числа однозначно зависит от возможных вариантов действий над предпоследним разрядом этого же простого числа и разрядами числа, которое факторизируется. Это дает право утверждать, что возможно математическое выражение любого разряда простого числа от предыдущих и от значений разрядов факторизируемого числа.

Так как на каждом шаге данного алгоритма имеет место выражение неизвестной и подстановку ее в каждое разрядное уравнение, то вычислительная сложность алгоритма будет равна:

$$O(k) = k^2 \qquad (30)$$

Формула (30) показывает нижнюю границу процесса факторизации, который сведен к частному случаю, когда простые числа равны между собой.

Представленная зависимость (29), алгоритм и его вычислительная сложность (30) дают основания предполагать, что в общем случае процесс

факторизации может иметь вычислительную сложность ниже экспоненциальной. Значит, учитывая структурные особенности простых чисел при решении задачи факторизации, можно организовать атаку на шифротекст, который зашифрован асимметричным методом шифрования, и вычислительная сложность данной атаки будет ниже экспоненциальной. Также представленный алгоритм программно реализован с помощью программного пакета символьных вычислений Maple. В качестве эксперимента было вычислено значения 3030 простых чисел, имея в качестве входных данных их квадраты. В ходе эксперимента не было ни одного неправильного решения, что подтверждает правильность приведенных выше выводов.

1. *Ингам А.Е*. Распределение простых чисел. – М: 1936 – 159с.
2. *Шнайер Б.* Прикладная криптография. – М.: Издательство ТРИУМФ, 2003 – 816 с.: ил.
3. *Василенко О.Н.* Теоретико-числовые алгоритмы в криптографии. — М.:МЦНМО, 2003.—328 с.