3. Нагорный Л.Я., Лебедев П.А. Устройство для решения системы линейных уравнений с разреженной матрицей. №813444 А.С. СССР. Опубл. 15.03.81. Бюл. №10.

4. Егоров Ф.И., Орленко В.С., Хорошко В.А. Вычислительные модули для системы защиты информации / Зб. наук. праць ВІ КНУ ім. Т.Шевченка. Вип. №11, 2008. –С.117-124.

Ковальова Ю.С., Плус Д.В., Хорошко В.О. Розподіл ресурсів у багаторубіжній системі захисту / Правове, нормативне та метрологічне забезпечення СЗІ, НТЗ. Вип. 8, 2004. –С.39-43.

Поступила 29.01.2009

УДК 511

Мохор В.В., Жилин А.В.

СВЕДЕНИЕ ЗАДАЧИ ФАКТОРИЗАЦИИ ЧИСЛА К РЕШЕНИЮ СИСТЕМЫ НЕЛИНЕЙНЫХ УРАВНЕНИЙ В АЛГЕБРЕ ЖЕГАЛКИНА

Одним из направлений в развитии современных средств защиты информации является использование асимметричных методов/алгоритмов шифрования. Классическим представителем таких алгоритмов является алгоритм RSA. При этом, как отмечает Б. Шнайер [1], «безопасность алгоритма RSA основана на трудоемкости разложения на множители (факторизации) больших чисел» и далее «предполагается, что восстановление открытого текста по шифртексту и открытому ключу равносильно разложению числа на два больших простых множителя». В этом контексте общие результаты в решении задачи факторизации представляют не только теоретический, но и практический интерес для сферы технической защиты информации

Представленный в работе [2] метод факторизации предполагает работу со структурой числа, которое представлено в двоичной форме, и основывается на правиле умножения чисел в двоичной системе счисления. Факторизуемое число Z представляется в виде вектора: $Z= \{ z_0, z_1, z_2,\ldots, z_i,\ldots, z_n\}$, где z_0 - старший разряд числа, z_n, - младший разряд числа. Факторизуемое число Z является произведением двух простых чисел X и Y, представляемых векторами $X= \{x_1, x_2,\ldots, x_j,\ldots, x_m\}$, и $Y= \{y_1, y_2,\ldots, y_j,\ldots, y_m\}$, где x_0, y_0 - старшие разряды, а x_m, y_m - младшие разряды чисел X и Y соответственно. Задача состоит в том, чтобы по известным значениям компонент вектора $Z= \{z_0, z_1, z_2,\ldots, z_i,\ldots, z_n\}$ найти неизвестные компоненты для векторов $X= \{x_0, x_1, x_2,\ldots, z_j,\ldots, x_m\}$, и $Y= \{y_0, y_1, y_2,\ldots, y_j,\ldots, y_m\}$. Классический метод умножения чисел «в столбик» $Z= X^* Y$ представим следующим образом:

						x_1	x_2	…	x_k	…	x_{m-1}	x_m
						y_1	y_2	…	y_k	…	y_{m-1}	y_m
						$x_1 y_m$	$x_2 y_m$	…	$x_k y_m$	…	$x_{m-1} y_m$	$x_m y_n$
					$x_1 y_{m-1}$	$x_2 y_{m-1}$	…	$x_k y_{m-1}$	…	$x_{m-1} y_{m-1}$	$x_m y_{m-1}$	
					…	…	…	…	…	…	…	
			$x_1 y_k$	$x_2 y_k$	…	$x_k y_k$	…	$x_{m-1} y_k$	$x_m y_k$			
		…	…	…	…	…	…	…	…			
		$x_1 y_2$	$x_2 y_2$	…	$x_k y_2$	…	$x_{m-1} y_2$	$x_m y_2$				
	$x_1 y_1$	$x_2 y_1$	…	$x_k y_1$	…	$x_{m-1} y_1$	$x_m y_1$					
z_0	z_1	z_2	…	…	…	…	z_m	…	…	…	…	z_{n-1}	z_n

Из этого представления следует, что можно связать между собой компоненты векторов X, Y и Z системой уравнений вида (1). При этом условимся считать, что для уравнений системы в заданном виде установлено отношение порядка, определяющее отношение «старший-младший» в соответствии с номером индекса переменной z в правой части. Так, например, уравнение системы (1), правая часть которого равна z_1 является старшим по отношению к уравнению, правая часть которого равна z_2, а уравнение для z_n является младшим по отношению к уравнению для z_{n-1}.

$$
\begin{array}{cccccccccccc}
 & & & & & & & & P_1 & = & z_0 \\
y_1x_1 & & & & & & & & P_2 & = & z_1 \\
y_1x_2 & +y_2x_1 & & & & & & & P_3 & = & z_2 \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
y_1x_m & +y_2x_{m-1} & & +y_kx_{m-k+1} & +y_kx_{m-k+2} & \dots & +y_{m-1}x_2 & +y_mx_1 & P_m & = & z_m \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
 & & & y_kx_m & +y_kx_{m-k+1} & \dots & +y_{m-1}x_{k-1} & +y_mx_k & P_k & = & z_{n-k} \\
 & & & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
 & & & & & & y_{m-1}x_m & +y_mx_{m-1} & & = & z_{n-1} \\
 & & & & & & & y_mx_m & & = & z_n
\end{array}
\qquad (1)
$$

В системе (1) фигурирует P_k – разрядный перенос из уравнений k-й строки в уравнения (k-1)-й строки. Сразу укажем, что перенос P_k может рассматриваться в качестве критерия порядка между уравнениями системы (1): если в уравнении некоторой строки с номером (i) формируется перенос P_i, то данное уравнение является младшим по отношению к тому уравнению, в которое осуществляется трансфер данного значения переноса P_i. Соответственно, если уравнение принимает в себя значение переноса P_i, то оно является старшим, по отношению к тому уравнению, из которого данный перенос P_i получен.

Система (1) не является инвариантной к перестановкам уравнений, т.к. разрядные переносы P_k не определены в явном виде. Наличие неопределенных разрядных переносов является основной причиной, из-за которой решение системы уравнений (1) в общем случае невозможно. Если найти способ представления значений P_k в явном виде, то есть надежда, что, во-первых, система уравнений (1) будет разрешима и, во-вторых, полученное решение будет единственным. В этом случае задача факторизации числа Z может быть сведена к задаче решения системы уравнений, в которую переходит система (1) после учета значений разрядных переносов в явном виде.

Покажем на примере, как такая постановка задачи может иметь решение. Прежде всего, будем считать, что X, Y – нечетные, простые числа. Из этого следует, что самые младшие разряды X, Y равны единице:

$$y_5=1,\ x_5=1. \qquad (2)$$

Очевидно, что такое предположение не является ограничением на общность результатов в нашей задаче. Для определенности и простоты изложения положим m=5 и зададимся конкретным значением правой части: Z= { 0, 1, 1, 0, 0, 0, 0, 1, 1, 1}. Тогда система уравнений (1) принимает вид:

$$
\begin{array}{cccccccccc}
(0) & & & & & & & P_1 & = & 0 \\
(1) & y_1x_1 & & & & & & +P_2 & = & 1 \\
(2) & y_1x_2 & +y_2x_1 & & & & & +P_3 & = & 1 \\
(3) & y_1x_3 & +y_2x_2 & +y_3x_1 & & & & +P_4 & = & 0 \\
(4) & y_1x_4 & +y_2x_3 & +y_3x_2 & +y_4x_1 & & & +P_5 & = & 0 \\
(5) & y_1 & +y_2x_4 & +y_3x_3 & +y_4x_2 & +x_1 & & +P_6 & = & 0 \\
(6) & & y_2 & +y_3x_4 & +y_4x_3 & +x_2 & & +P_7 & = & 0 \\
(7) & & & y_3 & +y_4x_4 & +x_3 & & +P_8 & = & 1 \\
(8) & & & & y_4 & +x_4 & & & = & 1 \\
(9) & & & & & 1 & & & = & 1
\end{array}
\qquad (3)
$$

Для удобства дальнейшего изложения в левой колонке системы (3) приведена нумерация строк. Нумерация выбраны таким образом, чтобы номер строки k был равен индексу элемента z_k вектора правой части. На номера k мы будем в дальнейшем ссылаться, когда нам нужно будет выделить какое-либо одно уравнении системы. А именно, будем указывать «уравнение в строке номер k системы», «уравнение с номером k системы» или просто «k-е уравнение системы», имея в виду номер соответствующей строки в крайней левой колонке соответствующей системы.

Учитывая, что числа X и Y представлены в двоичном виде, компоненты векторов X и Y принимают значения из множества {0, 1}.

Приведем правила преобразований, которые в дальнейшем будут использованы при выкладках. Пусть v и w – некоторые переменные, принимающие значения из множества {0, 1}. Тогда выполняются следующие правила:

A) $v \cdot v \equiv v$.

B) $v \cdot 1 \equiv v$.

C) $v \cdot 0 \equiv 0$.

D) $v \cdot 2 \equiv 0 + P(v)$,
где P(v) обозначает трансфер (т.е. перенос) переменной v в старший разряд.

E) $(v \oplus v) \equiv 0 \cdot$

F) $(1 \oplus v) \cdot w \equiv w \oplus v \cdot w$

G) $(1 \oplus v) \cdot v \equiv 0$.

H) Если $(v \oplus w) = 1$, то $v = 1 \oplus w$.

I) Если $(v \oplus w) = 0$, то $v = w$.

J) Если $v + w = 1$, то это справедливо тождество $(v + w = 1) \equiv (v \oplus w = 1)$.
Следствие. Из правила F) на основании правила D) следует: если $(v + w = 1)$ то $v = 1 \oplus w$.

K) Если v+w=0, то справедливо тождество:

$$(v + w = 0) \equiv (v \oplus w + 2\, v \cdot w = 0) \equiv [v \oplus w + P(v \cdot w) = 0].$$

Выражение в правой части предыдущего тождества имеет следующую интерпретацию: равенство $(v + w = 0)$ представляет собой сумму переменных v и w по mod2 $(v \oplus w)$ с учетом трансфера в старший разряд выражения $(v \cdot w)$.

L) Если $v \cdot w = 1$, то $v = w = 1$;
Следствие: если $v \cdot w = 1$, то $v \oplus w = 0$.

M) Если для элемента v существует элемент $v^{-1} = w$ такой, что $v \cdot w = v \cdot v^{-1} = 1$, то согласно следствию из правила J) вытекает $v \oplus v^{-1} = 0$, откуда, в свою очередь, согласно правилу I) следует $v = v^{-1}$.
Следствие: если $v \cdot w = u$, то $w = u \cdot v^{-1} = u \cdot v$. При этом если u=1, то v=w=1, а если u=0, то w=0 при том, что v может быть произвольным, а именно, либо 0 либо 1.

N) $v \cdot (1 \oplus w) + w \cdot (1 \oplus v) \equiv (v \oplus w)$

С учетом приведенных правил проведем последовательность преобразований системы (3). Начнем с уравнения в строке (8) системы (3):

$$y_4 + x_4 = 1. \quad (4)$$

Согласно правилу J) это уравнение тождественно уравнению

$$y_4 \oplus x_4 = 1. \quad (5)$$

В соответствии со следствием правила J) из уравнения (5) имеем

$$y_4 = 1 \oplus x_4. \quad (6)$$

Поскольку структура уравнения (4) такова, что ни при каких условиях в нем не может быть сформировано значение переноса в старшие уравнения, аналитическое значение переноса P_8, учитываемое в уравнении строки (7) системы (3), тождественно равно нулю

$$P_8 \equiv 0. \quad (7)$$

С учетом выражений (6) и (7) для уравнения строки (7) системы (3) можно построить следующую цепочку преобразований:

$y_3+y_4x_4+x_3+P_8=1 \Rightarrow y_3+(1\oplus x_4)x_4+x_3=1 \Rightarrow$

$$\Rightarrow y_3+x_3=1 \quad (8)$$

Получили выражение (8), аналогичное соотношению (4), которое было проанализировано выше. По аналогии с результатами, полученными в отношении выражения (4), можно сразу записать:

$$y_3 =1\oplus x_3 \quad (9)$$

и

$$P_7 \equiv 0. \quad (10)$$

С учетом вышеизложенного, система (3) примет следующий вид:

(0)						P_1	=	0
(1)	y_1x_1					$+P_2$	=	1
(2)	y_1x_2	$+y_2x_1$				$+P_3$	=	1
(3)	y_1x_3	$+y_2x_2$	$+(1\oplus x_3)x_1$			$+P_4$	=	0
(4)	y_1x_4	$+y_2x_3$	$+(1\oplus x_3)x_2$	$+(1\oplus x_4)x_1$		$+P_5$	=	0
(5)	y_1	$+y_2x_4$	$+(1\oplus x_3)x_3$	$+(1\oplus x_4)x_2$	$+x_1$	$+P_6$	=	0
(6)		y_2	$+(1\oplus x_3)x_4$	$+(1\oplus x_4)x_3$	$+x_2$		=	0
(7)			y_3				=	$1\oplus x_3$
(8)				y_4			=	$1\oplus x_4$
(9)					1		=	1

(11)

Рассмотрим уравнение строки (6) системы (11):

$$y_2 + (1\oplus x_3)x_4 +(1\oplus x_4)x_3 +x_2 = 0 \quad (12)$$

Прежде всего, отметим, что в это уравнение входит подвыражение

$$(1\oplus x_3)x_4 +(1\oplus x_4)x_3,$$

которое можно упростить по правилу N):

$$(1\oplus x_3)x_4 +(1\oplus x_4)x_3 \equiv (x_3 \oplus x_4).$$

Тогда уравнение (12) примет вид:

$$y_2 + (x_3\oplus x_4) +x_2 = 0 \quad (13)$$

Для удобства положим $(x_3\oplus x_4)= t$ и рассмотрим таблицу значений выражения (13):

(1)	(2)	(3)	(4)	(5)	(6)	(7)
y_2	x_2	t	$S =y_2 + t +x_2$	s	p	$y_2 + t +x_2=0$
0	0	0	0			Истина
0	0	1	1	1		
0	1	0	1	1		
0	1	1	2		***1***	***Истина***
1	0	0	1	1		
1	0	1	2		***1***	***Истина***
1	1	0	2		***1***	***Истина***
1	1	1	3	1	1	

В столбцах (1) - (3) этой таблицы представлены значения независимых переменных.

Столбец (4) содержит значения S, которые принимает выражение $(y_2 + t +x_2)$ на соответствующих наборах значений переменных y_2, x_2 и t. В столбцах (5) и (6) представлены одноразрядные значения первого (младшего) разряда (s) и второго (старшего) разряда (p) двоичного представления значения суммы $S = y_2 + t +x_2$. В столбце (7) представлено логическое значение предиката $(y_2 + t +x_2 = 0)$ в категориях «истина»-«ложь».

Анализируя таблицу можно видеть, что значения переносов, равные единице (p=1), формируются на множестве $П_6$ из четырех наборов переменных – это наборы (0,1,1), (1,0,1), (1, 0,1) и (1,1,1). Из таблицы также следует, что предикат ($y_2 + t + x_2 = 0$) принимает значение «истина» на множестве $И_6$ из четырех наборов переменных - это наборы (0,0,0), (0,1,1), (1,0,1), (1, 0,1). Множества $П_6$ и $И_6$ не совпадают между собой, но очевидно, что аналитическое выражение переноса P_6 из уравнения (6) в уравнение (5) системы (11) может быть представлено формулой, возвращающей единицу на наборах, входящих в пересечение множеств $П_6$ и $И_6$. В данном случае такая формула имеет вид:

$$P_6 = y_2x_2x_3 \oplus y_2x_2 \oplus y_2x_2x_4 \oplus y_2x_3 \oplus y_2x_4 \oplus x_2x_3 \oplus x_2x_4 \qquad (14)$$

С учетом выражения (14) уравнение (5) системы (11) приводится к следующему виду

$$y_1 + y_2x_4 + (1 \oplus x_3)x_3 + (1 \oplus x_4)x_2 + x_1 + (y_2x_2x_3 \oplus y_2x_2 \oplus y_2x_2x_4 \oplus y_2x_3 \oplus y_2x_4 \oplus x_2x_3 \oplus x_2x_4) = 0 \qquad (15)$$

Так как переносы, которые могут быть сформированы в уравнении (6) системы (11) уже учтены аналитическим выражением трансфера P_6 , все знаки операции сложения (+) в уравнении (13) должны быть заменены знаками операции ($\oplus$) сложения по mod2:

$$y_2 \oplus (x_3 \oplus x_4) \oplus x_2 = 0.$$

Отсюда следует

$$y_2 = x_4 \oplus x_3 \oplus x_2 \qquad (16)$$

Подставим значения y_2 из выражения (16) в выражение (15). После приведения подобных членов получим:

$$y_1 + (x_4 \oplus x_3 \oplus x_2)x_4 + (1 \oplus x_4)x_2 + x_1 + (x_3 \oplus x_4 \oplus x_2 \oplus x_3x_2 \oplus x_4x_2) = 0 \qquad (17)$$

Тогда система уравнений (11) примет следующий вид:

(0)							P_1	= 0	
(1)	y_1x_1						$+P_2$	= 1	
(2)	y_1x_2	$+y_2x_1$					$+P_3$	= 1	
(3)	y_1x_3	$+y_2x_2$	$+(1 \oplus x_3)x_1$				$+P_4$	= 0	
(4)	y_1x_4	$+y_2x_3$	$+(1 \oplus x_3)x_2$	$+(1 \oplus x_4)x_1$			$+P_5$	= 0	
(5)	y_1	$+(x_4 \oplus x_3 \oplus x_2)x_4$		$+(1 \oplus x_4)x_2$	$+x_1$		$(x_3 \oplus x_4 \oplus x_2 \oplus x_3x_2 \oplus x_4x_2)$	= 0	(18)
(6)		y_2						= $x_4 \oplus x_3 \oplus x_2$	
(7)			y_3					= $1 \oplus x_3$	
(8)				y_4				= $1 \oplus x_4$	
(9)					1			= 1	

Для уравнения в строке (5) системы (18) необходимо сформировать два множества $П_5$ и $И_5$. Множество $И_5$ должно представлять собой множество наборов значений переменных y_1, x_1, x_2, x_3, x_4, на которых предикат уравнения строки (5) системы (18)

$$y_1 + (x_4 \oplus x_3 \oplus x_2)x_4 + (1 \oplus x_4)x_2 + x_1 + (x_3 \oplus x_4 \oplus x_2 \oplus x_3x_2 \oplus x_4x_2) = 0$$

принимает значение «истина». Множество $П_5$ должно представлять собой множество наборов значений переменных y_1, x_1, x_2, x_3, x_4, на которых в уравнении строки (5) системы (18) формируются значения переноса, отличные от нуля.

Построив соответствующую таблицу можно показать, что множество $П_5$ включает в себя следующие наборы: { (0,0,0,0,1); (0,0,1,1,0); (0,0,1,1,1); (0,1,0,1,0); (0,1,1,0,1); (1,0,0,1,0); (10101); (11000); (11001); (11011); (11100); (11110); (11111) }. При этом на наборах (11001); (11100); (11110); (11111) перенос p принимает значение p=2, а на остальных наборах – значение p=1. По этому признаку множество $П_5$ может быть разбито на два подмножества $П_5^{(1)}$ и $П_5^{(2)}$. Подмножество $П_5^{(1)}$ включает в себя наборы значений переменных, на которых в уравнении строки (5) системы (18) формируются значения переносов в уравнение строки, показатель старшинства которой на 1 единицу больше, чем показатель старшинства строки (5). Соответственно, подмножество $П_5^{(2)}$ включает в себя наборы значений переменных, на

которых в уравнении строки (5) системы (18) формируются значения переносов в уравнение строки, показатель старшинства которой на 2 единицы больше, чем показатель старшинства строки (5). Таким образом, множество $П_5^{(1)}$ имеет вид:

$П_5^{(1)}$ = { (0,0,0,0,1); (0,0,1,1,0); (0,0,1,1,1); (0,1,0,1,0); (0,1,1,0,1); (1,0,0,1,0); (10101); (11000); (11011) },

а множество $П_5^{(2)}$

$П_5^{(2)}$ = { (11001); (11100); (11110); (11111) }.

При этом множество $И_5$ имеет следующий вид:

$И_5$ = { (00000); (00001); (00011); (00100); (00110); (00111); (01010); (01101); (10010); (10101); (11000); (11001); (11011); (11100); (11110); (11111) }

Аналитическое выражение переноса $P_5^{(1)}$ из уравнения (5) в уравнение (4) системы (18) может быть представлено формулой, возвращающей единицу на наборах, входящих в пересечение множеств $П_5^{(1)}$ и $И_5$. В данном случае такая формула имеет вид:

$$P_5^{(1)} = x_1x_2x_3y_1 \oplus x_1x_2x_4y_1 \oplus x_1x_3x_4y_1 \oplus x_1x_2x_3 \oplus x_2x_3y_1 \oplus x_1x_2x_4 \oplus x_2x_4y_1 \oplus x_1x_3y_1 \oplus x_1x_2 \oplus x_2y_1 \oplus x_3x_4 \oplus x_1x_3 \oplus x_3y_1 \oplus x_1x_4 \oplus x_4y_1 \oplus x_1y_1 \oplus x_2 \oplus x_4.$$

Аналогично, аналитическое выражение переноса $P_5^{(2)}$ из уравнения (5) в уравнение (3) системы (18) может быть представлено формулой, возвращающей единицу на наборах, входящих в пересечение множеств $П_5^{(2)}$ и $И_5$. Эта формула имеет вид:

$$P_5^{(2)} = x_1x_3x_4y_1 \oplus x_1x_2y_1 \oplus x_1x_4y_1.$$

Так как переносы, которые могут быть сформированы в уравнении (5) системы (18) уже учтены аналитическими выражениями трансферов $P_5^{(1)}$ и $P_5^{(2)}$, то все знаки операции сложения (+) в уравнении (17) должны быть заменены знаками операции ($\oplus$) сложения по mod2. Тогда взамен уравнения (17) будем иметь уравнение следующего вида:

$$y_1 \oplus (x_4 \oplus x_3 \oplus x_2)x_4 \oplus (1 \oplus x_4)x_2 \oplus x_1 \oplus (x_3 \oplus x_4 \oplus x_2 \oplus x_3x_2 \oplus x_4x_2) = 0, \quad (19)$$

из которого, после раскрытия скобок и приведения подобных членов, можно получить явное выражение для y_1:

$$y_1 = x_1 \oplus x_3 \oplus x_2x_4 \oplus x_3x_2 \oplus x_3x_4 \quad (20)$$

Подставим значение y_1 из выражения (20) в формулы трансферов $P_5^{(1)}$ и $P_5^{(2)}$. После раскрытия скобок и приведения подобных членов будем иметь:

$$P_5^{(1)} = x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_1x_3 \oplus x_2x_3 \oplus x_2x_4 \oplus x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_3x_4, \quad (21)$$

$$P_5^{(2)} = x_1x_2 \oplus x_1x_4 \oplus x_1x_3x_4 \quad (22)$$

В результате система уравнений (18) примет следующий вид:

$$\begin{array}{lllll}
(0) & & & P_1 = 0 \\
(1) & y_1x_1 & & +P_2 = 1 \\
(2) & y_1x_2 + y_2x_1 & & +P_3 = 1 \\
(3) & y_1x_3 + y_2x_2 + (1 \oplus x_3)x_1 & & P_5^{(2)} + P_4 = 0 \\
(4) & y_1x_4 + y_2x_3 + (1 \oplus x_3)x_2 + (1 \oplus x_4)x_1 & & + P_5^{(1)} = 0 \\
(5) & y_1 & & = x_1 \oplus x_3 \oplus x_2x_4 \oplus x_3x_2 \oplus x_3x_4 \\
(6) & y_2 & & = x_4 \oplus x_3 \oplus x_2 \\
(7) & y_3 & & = 1 \oplus x_3 \\
(8) & y_4 & & = 1 \oplus x_4 \\
(9) & 1 & & = 1
\end{array} \quad (23)$$

Рассмотрим уравнение строки (4) системы (23):

$$y_1x_4 + y_2x_3 + (1 \oplus x_3)x_2 + (1 \oplus x_4)x_1 + P_5^{(1)} = 0 \quad (24)$$

Подставим в это уравнение значения y_1 , y_2 и $P_5^{(1)}$, определенные выражениями (20), (16) и (21) соответственно. В результате получим следующее уравнение

$$(x_3x_4 \oplus x_2x_4 \oplus x_1x_4 \oplus x_3x_4 \oplus x_3x_2x_4) + (x_4x_3 \oplus x_3 \oplus x_2x_3) + (1 \oplus x_3)x_2 + (1 \oplus x_4)x_1 +$$

$$+(x_4 \oplus x_1 \oplus x_3 \oplus x_1x_3x_4 \oplus x_1x_3 \oplus x_2 \oplus x_1x_2x_4 \oplus x_2x_4 \oplus x_2x_3 \oplus x_1x_2x_3)=0 \quad (25)$$

Построив множества $П_4$ и $И_4$ для этого уравнения и найдя их пересечение получим наборы значений переменных x_1, x_2, x_3, x_4, на которых, с одной стороны, в уравнении (25) формируются ненулевые значения переносов в уравнения старших строк, и, с другой стороны, выполняется истинность предиката, заданного тем же уравнением (25). По этому набору можно реконструировать формулу трансфера переноса из уравнения строки (4) в уравнение строки (3) системы (23), которая после упрощения принимает вид:

$$P_4 = x_1 \oplus x_2 \oplus x_3 \oplus x_1x_2 \oplus x_1x_4 \oplus x_2x_4 \oplus x_3x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4 \quad (26)$$

Учет в строке (3) системы (23) полученного аналитическое значение трансфера P_4 дает возможность провести в уравнении (25) замену знаков операции сложения (+) на знаки операции сложения по mod2 ($\oplus$). В результате уравнение (25) переходит в следующее выражение:

$$x_3 \oplus x_1x_3 \oplus x_2x_3 \oplus x_2x_4 \oplus x_3x_4 \oplus x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_3x_4 = 0, \quad (27)$$

а система уравнений (23) принимает вид

$$\begin{array}{lllll}
(0) & & P_1 & = & 0 \\
(1) & y_1^1 x & +P_2 & = & 1 \\
(2) & y_1^2 x + y_2 x_1 & +P_3 & = & 1 \\
(3) & y_1^3 x + y_2 x_2 + (1 \oplus x_3)x_1 & P_5^{(2)} + P_4 & = & 0 \\
(4) & & 0 & = & x_3 \oplus x_1x_3 \oplus x_2x_3 \oplus x_2x_4 \oplus x_3x_4 \oplus x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_3x_4 \\
(5) & y_1 & & = & x_1 \oplus x_3 \oplus x_2x_4 \oplus x_3x_2 \oplus x_3x_4 \\
(6) & y_2 & & = & x_4 \oplus x_3 \oplus x_2 \\
(7) & y_3 & & = & 1 \oplus x_3 \\
(8) & y_4 & & = & 1 \oplus x_4 \\
(9) & 1 & & = & 1
\end{array} \quad (28)$$

Последовательно применяя подобные рассуждения и аналогичные выкладки для уравнений в строках (3), (2), (1) и (0) системы (28) получим в итоге систему уравнений следующего вида:

$$\begin{array}{lll}
(0) & 0 & = 0 \\
(1) & x_1 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1x_3x_4 & = 1 \\
(2) & x_1 \oplus x_2 \oplus x_3 \oplus x_1x_3 \oplus x_1x_4 \oplus x_3x_4 & = 1 \\
(3) & 0 & = 0 \\
(4) & x_3 \oplus x_1x_3 \oplus x_2x_3 \oplus x_2x_4 \oplus x_3x_4 \oplus x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_3x_4 & = 0 \\
(5) & y_1 & = x_1 \oplus x_3 \oplus x_2x_4 \oplus x_3x_2 \oplus x_3x_4 \\
(6) & y_2 & = x_4 \oplus x_3 \oplus x_2 \\
(7) & y_3 & = 1 \oplus x_3 \\
(8) & y_4 & = 1 \oplus x_4 \\
(9) & 1 & = 1
\end{array} \quad (29)$$

Уравнения этой системы представляют собой уравнения в алгебре Жегалкина и не содержат неопределенных значений переносов. Таким образом, система (29) оказывается инвариантной к упорядочиванию уравнений в системе и, следовательно, допускает применение в дальнейшем известных методов для ее решения.

Для завершенности изложения рассмотрим решение системы (29). В уравнении строки (1) вынесем за скобки переменную x_1:

$x_1(1 \oplus x_2 \oplus x_3 \oplus x_3x_4)=1$.

Из этого выражения, согласно правилу L) следует одновременное выполнение двух условий:

$$x_1=1 \tag{30}$$

$$1\oplus x_2\oplus x_3\oplus x_3x_4=1. \tag{31}$$

В выражении (31) можно сократить единицу в левой и правой части:

$$x_2\oplus x_3\oplus x_3x_4=0. \tag{32}$$

Уравнение (32) дает возможность представить нелинейный член x_3x_4 в виде суммы:

$$x_3x_4= x_2\oplus x_3 \tag{33}$$

Подставим в систему (29) вместо x_1 и x_3x_4 их значения согласно выражениям (31) и (33) соответственно. В результате получим

$$\begin{array}{lll}
(0) & 0 & = 0 \\
(1) & 1 & = 1 \\
(2) & 1\oplus x_4\oplus x_3 & = 1 \\
(3) & 0 & = 0 \\
(4) & 0 & = 0 \\
(5) & y_1 & = 1\oplus x_3\oplus x_2x_4 \oplus x_3x_2\oplus x_3x_4 \\
(6) & y_2 & = x_4 \oplus x_3 \oplus x_2 \\
(7) & y_3 & = 1\oplus x_3 \\
(8) & y_4 & = 1\oplus x_4 \\
(9) & 1 & = 1
\end{array} \tag{34}$$

В уравнении строки (2) системы (34) можно сократить единицу в левой и правой части. Тогда получим уравнение

$$x_4\oplus x_3=0,$$

из которого следует

$$x_4=x_3. \tag{35}$$

Полученное значение x_4 подставим в уравнение (33) и получим:

$$x_3= x_2\oplus x_3,$$

из чего следует, что

$$x_2=0. \tag{36}$$

Соберем вместе выражения, представленные формулами (2), (35), (35) и (30):

$$\begin{array}{l}
x_1=1, \\
x_2=0, \\
x_4=x_3, \\
x_5=1
\end{array} \tag{37}$$

и формулами (2), (6), (9), (16) и (20):

$$\begin{array}{l}
y_1= (x_1 \oplus x_3\oplus x_2x_4 \oplus x_3x_2\oplus x_3x_4) \\
y_2= (x_4\oplus x_3\oplus x_2) \\
y_3= (1\oplus x_3), \\
y_4= (1\oplus x_4), \\
y_5= 1,
\end{array} \tag{38}$$

Полученная система результатов допускает две интерпретации: первая - при $x_4=x_3=0$, и вторая – при $x_4=x_3=1$.

Рассмотрим первую интерпретацию:

$$x_4=x_3=0 \tag{39}$$

Тогда согласно выражениям системы результатов (37) и (38) имеем $x_1=1$, $x_2=0$, $x_3=0$, $x_4=0$, $x_5=1$ и, соответственно, $y_1=1$, $y_2=0$, $y_3=1$, $y_4=1$, $y_5=1$, что отвечает значениям сомножителей X=10001 и Y=10111, которые являются сомножителями факторизованного числа Z=0110000111.

Рассмотрим вторую интерпретацию:

$$x_4=x_3=1. \tag{40}$$

Тогда согласно выражениям системы результатов (37) и (38) имеем $x_1=1$, $x_2=0$, $x_3=1$, $x_4=1$, $x_5=1$ и, соответственно, $y_1=1$, $y_2=0$, $y_3=0$, $y_4=0$, $y_5=1$. Таким образом, имеем значения X=10111 и Y=10001.

Очевидно, что обе интерпретации представляют собой один и тот же результат; сомножители X и Y просто меняются местами. В действительности так и должно быть – решение должно допускать два варианта именования сомножителей, что, впрочем, не влияет на единственность полученного решения.

На рассмотренном примере сведения задачи факторизации числа мы проиллюстрировали метод, который является достаточно общим и состоит в следующем:

1. Изначально, задача факторизации числа Z формулируется в виде задачи решения системы нелинейных алгебраических уравнений, неинвариантной к перестановкам уравнений из-за наличия неопределенных значений переносов между уравнениями системы. В качестве вектора правых частей такой системы уравнений используется вектор разрядов двоичного представления числа Z. На множестве уравнений системы определено отношение порядка в категориях «старший-младший».
2. Известно, что уравнение системы, имеющее самый младший порядок, не формирует переносов в уравнения старших порядков. Из этого следует, что в системе существует уравнение минимального порядка старшинства, в котором может быть сформировано аналитическое выражение для первого переноса – перенос самого низшего порядка. Как только такой перенос сформирован, наступает определенность со всеми слагаемыми следующего по старшинству уравнения. Это, в свою очередь, дает возможность сформировать аналитическое выражение для переноса следующего порядка и так далее вплоть до самого старшего уравнения. В результате последовательного включения в уравнениях системы аналитических выражений для переносов удается устранить из системы уравнений неопределенные значения переносов.
3. Построение аналитических выражений для функций переносов может быть выполнено в виде полиномов в алгебре Жегалкина. При этом, уравнение, которое порождает переносы, автоматически преобразуется в уравнение в алгебре Жегалкина путем замены символов операции сложения символом операции сложения по модулю два.

Подводя итог всему вышеизложенному можно утверждать, что задача факторизации числа, может быть сведена к системе уравнений в алгебре Жегалкина путем последовательного (начиная с младших строк) применения к каждой строке системы уравнений вида (1) последовательной процедуры трансфера переносов, представленных формулами алгебры Жегалкина, реконструированных на наборах, множество которых, в свою очередь, представляет собой, например, пересечение множества наборов для ненулевых значений переносов данной строки со множеством наборов, возвращающих значение «истина» предикату, представленному уравнением данной строки.

Решение полученной системы уравнений в алгебре может быть выполнено известными методами.

Список литературы

1. *Шнайер Б.* Прикладная криптография. – М.: Издательство ТРИУМФ, 2003 – 816 с.: ил.

2. *Жилин А.В., Мохор В.В.* Структурный метод факторизации больших целых чисел// Моделювання та інформаційні технології. Спец. випуск зб. наук. пр. ІПМЕ НАН України – К.:2008. - С.49 – 57

Поступила 12.01.2009