УДК 621.391.7 + 681.3.067

С.Д. Винничук, д-р техн. наук
Ин-т проблем моделирования в энергетике
им. Г.Е. Пухова НАН Украины
(Украина, 03164, Киев, ул. Генерала Наумова, 15,
тел. (044) 4249171, e-mail: vynnychuk@i.ua)

Метод удвоения последовательности весов предметов в задаче Меркля—Хеллмана шифрования ранцами

Для криптосхемы Меркля—Хеллмана шифрования ранцами разработан алгоритм формирования обычной последовательности из сверхвозрастающей, основанный на введенных понятиях непрямых модульных преобразований и частичных инверсий, в котором для формирования «лазейки» применяются удвоенные последовательности весов предметов. Показано, что при таком подходе для k-кратно итерируемой ранцевой системы каждому элементу сверхвозрастающей последовательности может соответствовать 2^k вариантов элемента обычной последовательности, а число вариантов обычной последовательности, при всех одинаковых параметрах модульных преобразований, может достигать 2^{kL}, где L — число бит в блоке информации. При этом обратная задача определения сверхвозрастающей последовательности по обычной может быть сведена к задаче целочисленного линейного программирования как вариантная при большом числе вариантов.

Для криптосхеми Меркля—Хеллмана шифрування рюкзаками розроблено алгоритм формування звичайної послідовності із надзростаючої, що ґрунтується на введених поняттях непрямих модульних перетворень і часткових інверсій, в якому при формуванні «люка» використовуються подвоєні послідовності ваг предметів. Показано, що при такому підході для k-кратно ітерованої системи кожному з елементів надзростаючої послідовності може відповідати 2^k варіантів елемента звичайної послідовності, а число варіантів звичайної послідовності при всіх однакових параметрах модульних перетворень, може досягати 2^{kL}, де L — число біт в блоці інформації. При цьому обернена задача визначення надзростаючої послідовності по звичайній може бути зведена до задачі цілочисельного лінійного програмування як варіантна при значному числі варіантів.

Ключевые слова: криптография с открытым ключом, криптосхема Меркля—Хеллмана, шифрование ранцами.

Постановка задачи. Первым известным способом асимметрического шифрования с открытым ключом был способ шифрования ранцами [1, 2]. При таком способе шифрованная информация разбивалась на блоки равной длины, где каждому биту информации, равному единице, ставился в соот-

ветствие определенный вес предмета. Шифрованное сообщение для блока информации фиксированной длины являлось суммой весов предметов, которым в блоке соответствуют биты, равные единице.

В общем виде задача определения веса предметов по их известному суммарному весу считается чрезвычайно сложной и относится к классу *NP*-полных. При этом для возможности расшифрования информации требуется специальный способ построения обычной последовательности. Такой способ был предложен Р. Мерклем [2] как односторонняя функция с «лазейкой», в которой сверхвозрастающая последовательность весов $\{v_i\}_{i=1}^{L}$ такая, что сумма весов первых k предметов меньше веса $k+1$-го предмета ($1 \le k < L$) преобразуется к обычной $\{w_i\}_{i=1}^{L}$ в результате модульного преобразования (определения остатка от деления)

$$w_i = (v_i n) (\mathrm{mod} m), \;\; i = 1 \div L, \tag{1}$$

где n и m — константы модульного преобразования; L — длина информационного блока (число двоичных символов). Тогда для произвольного слова $A = (a_1, a_2, ..., a_L)$ можно определить суммарный вес по правилу

$$W(A) = \sum_{i=1}^{L} a_i w_i. \tag{2}$$

Определение слова A по сумме $W(A)$ возможно на основании обратного модульного преобразования (ОМП)

$$v_i = (w_i \; n^{-1}) (\mathrm{mod} m) = (w_i \; d) (\mathrm{mod} m), \;\; i = 1 \div L, \tag{3}$$

и определения веса $V(A)$ по элементам сверхвозрастающей последовательности:

$$V(A) = (W(A)\, d) (\mathrm{mod} m) = \sum_{i=1}^{L} a_i (w_i d) (\mathrm{mod} m)_i = \sum_{i=1}^{L} a_i v_i. \tag{4}$$

Бесспорное преимущество такого способа шифрования — его простота и скорость. Соотношения (1)—(4) — простейший вариант зашифрования и расшифрования для криптосхемы Меркля—Хеллмана. При таком подходе используется единообразное модульное преобразование сверхвозрастающей последовательности весов в обычную, и для раскрытия кода достаточно определить числа d и m. Задача определения d и m может быть сведена к задаче линейного программирования [2], для которой характерна полиномиальная сложность, тогда как способ раскрытия грубой силой имеет экспоненциальную сложность.

После раскрытия простейшей криптосхемы (1)—(4) было предложено множество других ее вариантов, которые также были раскрыты. В настоящее время такой способ шифрования, несмотря на его простоту и скорость, практически не используется. Более того, в статье У. Диффи, опубликованной в [2], речь идет о «крахе ранцевой системы», и, по мнению автора, «никто не должен возлагать больших надежд на ранцевую систему, если под ее функционирование не подведена намного более глубокая теория, чем та, которая имеется в настоящее время».

Вероятно, такая теория должна препятствовать формированию задачи линейного целочисленного программирования. Именно такой подход реализован в предлагаемых способах получения обычной последовательности весов из сверхвозрастающей с использованием непрямых модульных преобразований (НМП), а также частичных инверсий (ЧИ), при которых «лазейка» формируется на основании удвоенных последовательностей (УП) весов предметов.

Удвоенные последовательности весов предметов и их свойства.

Определение 1. Удвоенная последовательность весов предметов — это последовательность, в которой вес присваивается как биту 1, так и биту 0.

В случае УП правило определения веса ранца при зашифровании блока информации длиной L бит состоит в следующем: каждому i-му информационному биту ставится в соответствие число (вес w_i, $i=1\div L$), как для бита информации, равного единице (w_{i1}), так и для бита, равного нулю (w_{i0}). Тогда суммарный вес предметов, соответствующих слову A, будет определяться по формуле, более сложной, чем (2):

$$W(A)=\sum_{a_i=0} w_{i0}+\sum_{a_i=1} w_{i1}=\sum_{i=1}^{L} a_i w_{i1}+\sum_{i=1}^{L}(1-a_i)w_{i0}. \qquad (5)$$

В общем виде данные, используемые в УП, представлены в табл. 1. Очевидно, что УП требуют увеличения в два раза объема данных при зашифровании и расшифровании информации, что не является положительным фактом. Однако они позволяют проводить ряд дополнительных операций над данными, что в большинстве случаев невозможно для традиционных ранцевых систем. Покажем это на примерах.

Пусть задана некоторая сверхвозрастающая последовательность $\{v_i\}_{i=1}^{L}$. Простейший вариант ее представления в виде УП следующий: всем битам со значением 0 соответствует значение 0, а битам со значением 1 — значение соответствующего элемента сверхвозрастающей последовательности. Обозначим такую последовательность $П2_0$.

Удвоенный объем данных в УП по сравнению со сверхвозрастающей последовательностью позволяет реализовать ряд преобразований. Опишем их и покажем на примере сверхвозрастающей последовательности {4, 5, 10, 20}, последовательность $П2_0$ которой представлена в табл. 1.

Преобразование П1. ***Частичная инверсия.*** Во всех случаях, когда для последовательности $П2_0$ ненулевой элемент соответствует биту 0, будем считать, что для соответствующего бита информации выполняется инверсия. Относительно всей УП может осуществляться как полная инверсия (ПИ) (каждый из ненулевых элементов УП соответствует биту 0), так и ЧИ, когда использована инверсия только для части элементов. Общее число вариантов ЧИ равняется 2^L. Такую сформированную последовательность весов обозначим $П2_1$. Пример ЧИ для последовательности $П2_0$ приведен в табл. 1.

Преобразование П2. ***Перестановка уровней.*** Столбцы УП произвольно меняются местами. Такой способ перестановки использовался и ранее для элементов сверхвозрастающих и обычных последовательностей. Сформированную последовательность весов обозначим $П2_2$. Вариант перестановок для последовательности $П2_1$ приведен в табл. 1.

Преобразование П3. ***Синхронное увеличение веса.*** К элементам произвольного столбца УП одновременно прибавляем одно и то же число, т.е. синхронно на одно и то же число увеличиваем вес одного бита.

В результате преобразования П3 при зашифровании вес ранца и в дальнейшем будет уникальным, так как для произвольного информационного слова соответствующая ему сумма всегда будет синхронно увеличиваться на одно и то же число, которое обозначим S_1. Полученную новую последовательность обозначим $П2_3$. Такое преобразование можно применять к произвольному числу столбцов УП. Например, если для УП $П2_1$ вес столбцов синхронно увеличить соответственно на величину 8, 10, 3, 4 (S_1 = = 8 + 10 + 3 + 4 = 25), то получим новую УП $П2_3$ (см. табл. 1).

В результате выполненных преобразований начальная сверхвозрастающая последовательность $П2_0$ перестала быть сверхвозрастающей еще до ее преобразования на основе модульной арифметики.

Преобразуем последовательность $П2_3$ на основе модульной арифметики.

Преобразование П4. ***Прямые модульные преобразования (ПМП) УП*** реализуются с помощью зависимости (1), для которой следует выбрать взаимно простые числа m и n.

Удвоенную последовательность, полученную после ПМП (1), обозначим $П2_4$. Заметим, что при выборе числа m следует исходить из того, что вес числа m больше любого из весов соответствующих информационных

Таблица 1. **Варианты УП**

Номер бита	w_{i0} для бита 0	w_{i1} для бита 1
Общий вид данных		
1	w_{10}	w_{11}
2	w_{20}	w_{21}
⋮	⋮	⋮
l	w_{l0}	w_{l1}
Общий вид последовательности $П2_0$ *при* $w_{i1} = v_i$		
1	0	v_1
2	0	v_2
⋮	⋮	⋮
l	0	v_l
Пример последовательности $П2_0$		
1	0	4
2	0	5
3	0	10
4	0	20
Вариант размещения элементов последовательности $П2_1$		
1	4	0
2	0	5
3	0	10
4	20	0
Последовательность $П2_2$ *после перестановок в последовательности* $П2_1$		
1	0	10
2	0	5
3	20	0
4	4	0
Последовательность $П2_3$		
1	12	8
2	10	15
3	3	13
4	24	4
Последовательность $П2_4$ *после преобразования* $П2_3$ *согласно (1)*		
1	42	28
2	35	19
3	44	12
4	17	14

Окончание таблицы

Номер бита	w_{i0} для бита 0	w_{i1} для бита 1
Последовательность П2$_5$ после изменения данных в последовательности П2$_4$		
1	25	11
2	20	4
3	38	6
4	5	2
Специальный вариант последовательности П2$_5$		
1	14	0
2	16	0
3	32	0
4	3	0

слов, т.е. число m превысит сумму всех бóльших значений в строках. Поэтому для последовательности $П2_3$ (см. табл. 1) число m выберем из условия $m > 12 + 15 + 13 + 24$, т.е. $m > 64$, например $m = 67$, и взаимно простое с ним число $n = 37$. В результате преобразований получим УП $П2_4$ (см. табл.1).

Преобразование П5. ***Синхронное изменение веса после ПМП.*** От элементов произвольного столбца УП можно одновременно вычесть одно и то же число, т.е. синхронно на одно и то же число изменить вес бита при его значениях 0 и 1.

Такую УП обозначим $П2_5$, а общую величину суммарного синхронного изменения весов — S_2. Пусть для $П2_4$ (см. табл. 1) преобразование П5 реализуется посредством вычитания из битов 1—4 соответственно чисел 17, 15, 6 и 12. Для приведенного примера $S_2 = 17 + 15 + 6 + 12 = 50$. Полученная УП $П2_5$ представлена в табл. 1.

Суммарный вес кодового слова для произвольного информационного блока уменьшен на величину $S_2 = 50$, что следует учитывать при расшифровании информации. Следует заметить, что преобразованя П1, П3 и П5 можно реализовать только при использовании УП.

Рассмотрим примеры зашифрования и расшифрования информации при использовании $П2_5$, представленной в табл. 1, для информационных блоков 1001 и 0010 .

Информационный блок 1001. Зашифрование информации:

$$1001 \rightarrow 11 + 20 + 38 + 2 = 71.$$

Информационный блок 1001. Расшифрование информации:

Ш а г 1. $71 + S_2 = 71 + 50 = 121$.

Ш а г 2. $(121 \cdot 37^{-1})(\text{mod } 67) = (121 \cdot 29)(\text{mod } 67) = 25$.

Ш а г 3. $25 - S_1 = 25 - 25 = 0$.

Ш а г 4. Расшифрование суммы 0 с использованием данных последовательности $П2_2$ (см. табл. 1). Последовательность расшифрования представлена в табл. 2.

Информационный блок 0010. Зашифрование информации:

$$0010 \rightarrow 25 + 20 + 6 + 5 = 56.$$

Информационный блок 0010. Расшифрование информации:

Ш а г 1. $56 + S_2 = 56 + 50 = 106$.

Ш а г 2. $(106 \cdot 37^{-1})(\text{mod } 67) = (106 \cdot 29)(\text{mod } 67) = 59$.

Ш а г 3. $59 - S_1 = 59 - 25 = 34$.

Ш а г 4. Расшифрование суммы 34 (см. табл. 2) с использованием данных последовательности $П2_2$ из табл. 1.

Таблица 2. **Последовательности расшифрования**

Номер бита	Условие определения значения бита	Значение бита
	Расшифрование суммы 0	
4	0 < 20	1
3	0 < 10	0
2	0 < 5	0
1	0 < 4	1
	Расшифрование суммы 34	
4	34 > 20 (34 – 20 = 14)	0
3	14 > 10 (14 – 10 = 4)	1
2	4 < 5	0
1	4 = 4 (4 – 4 = 0)	0
	Расшифрование суммы 39	
4	39 > 20 (39 – 20 = 19)	0
3	19 > 10 (19 – 10 = 9)	1
2	9 > 5 (9 – 5 = 4)	1
1	4 = 4 (4 – 4 = 0)	0
	Расшифрование суммы 5	
4	5 < 20	1
3	5 < 10	0
2	5 = 5 (5 – 5) = 0	1
1	0 < 4	1

Теперь рассмотрим специальный вариант УП — $П2_5$, в котором окажутся равными нулю либо w'_{i0}, либо w'_{i1}, $i = 1 \div l$ (см. табл. 1). Как видно из табл. 3, из данных последовательности $П2_4$ вычитаются соответственно числа 28, 19, 12 и 14 ($S_2 = 28 + 19 + 12 + 14 = 73$). Если к такой последовательности применить ПИ (перестановку значений весов, соответствующих значениям битов 0 и 1), то получим УП, аналогичную $П2_0$, которая однозначно соответствует обычной последовательности (14, 16, 32, 3). Таким образом, от УП можно переходить к обычным последовательностям, учитывая это при расшифровании информации.

Покажем, что используя обычные последовательности, построенные таким способом, можно как зашифровать, так и расшифровать информацию.

Информационный блок 1001. Зашифрование информации:

$$1001 \rightarrow 14 + 0 + 0 + 3 = 17.$$

Информационный блок 1001. Расшифрование информации:

Ш а г 1. $17 + S_2 = 17 + 73 = 90$.

Ш а г 2. $(90 \cdot 37^{-1})(\text{mod } 67) = (90 \cdot 29)(\text{mod } 67) = 64$.

Ш а г 3. $64 - S_1 = 64 - 25 = 39$.

Ш а г 4. Расшифрование суммы 39 (см. табл. 2) с использованием данных последовательности $П2_2$ (см. табл. 1).

Ш а г 5. Полная инверсия (согласно табл. 3) для полученного слова: $0110 \rightarrow 1001$. Инвертированное слово совпало с исходным.

Информационный блок 0010. Зашифрование информации:

$$0010 \rightarrow 0 + 0 + 32 + 0 = 32.$$

Информационный блок 0010. Расшифрование информации:

Ш а г 1. $32 + S_2 = 32 + 73 = 105$.

Ш а г 2. $(105 \cdot 37^{-1})(\text{mod } 67) = (105 \cdot 29)(\text{mod } 67) = 30$.

Таблица 3. **Анализ модульных преобразований**

Номер строки	Последовательность	Преобразование	Вес битов			
			1	2	3	4
1	Обычная	Модуль разности $w_i^* = \lvert w_{i1} - w_{i0} \rvert$	14	16	32	3
2	Обычная	ОМП строки 1 $(w_i^* d)(\text{mod } 67)\ (d = 29)$	4	62	57	20
3	Исходная сверхвозрастающая последовательность	v_i	4	5	10	20
4	Обычная	$67 - v_i = m - v_i$	63	62	57	47

Ш а г 3. $30 - S_1 = 30 - 25 = 5$.

Ш а г 4. Расшифрование суммы 5 (см. табл. 2) с использованием данных последовательности $П2_2$ (см. табл. 1).

Ш а г 5. Полная инверсия (согласно табл. 3) для полученного слова: $1101 \to 0010$. Инвертированное слово совпало с исходным.

Приведенные примеры позволяют убедиться, что такой способ шифрования возможен, но при расшифровании может потребоваться полная или частичная инверсия. Однако остается неясным, увеличивается ли при этом возможность раскрытия способа шифрования.

Из табл. 1 видно, что для последовательности $П2_0$, $П2_1$, $П2_2$ и $П2_3$ постоянным является модуль разности элементов одного и того же столбца. Такой модуль разности позволяет сразу определять значение одного из элементов сверхвозрастающей последовательности. Поэтому использование только преобразований П1—П3 нельзя считать усилением способа шифрования ранцами. Проанализируем далее, что при этом добавляет модульное преобразование УП.

Для последовательностей $П2_4$ и $П2_5$ (см. табл. 1) характерно одинаковое значение модуля разности элементов одного столбца: $w_i^* = |w_{i1} - w_{i0}|$. Поэтому логично проверить возможность получения элементов сверхвозрастающей последовательности (4, 5, 10, 20) по обычной последовательности (14, 16, 32, 3) с использованием ОМП (3) (см. табл. 3).

Из данных табл. 3 следует, что только для определенной части случаев (биты 1, 4) таким способом можно найти элементы сверхвозрастающей последовательности v_i. Для другой части случаев (биты 2, 3) будут определены разности $m - v_i$, а это не позволяет расшифровать информацию, используя только ОМП. Следовательно, преобразования П1—П5 при использовании УП позволяют строить новые обычные последовательности по сверхвозрастающим, для которых не существует ОМП, восстанавливающего все элементы сверхвозрастающей последовательности.

Непрямые модульные преобразования. Как видно из табл. 3, при построении обычных последовательностей по сверхвозрастающим с использованием УП и их преобразований П1—П5 возможны случаи, когда при однократном использовании ПМП (1) формируется такая обычная последовательность, что ее ОМП (3) позволяет найти либо элементы сверхвозрастающей последовательности v_i, либо разности $m - v_i$. В последнем случае требуется отдельное рассмотрение, в связи с чем введено понятие НМП.

Определение 2. Непрямым модульным преобразованием будем называть преобразование вида

$$w^* = m - (v\ n) (\mathrm{mod}\, m), \tag{6}$$

где $0 < v < m$.

Согласно определению 2 в результате преобразований базовой сверхвозрастающей последовательности в ряде случаев получены как ПМП (1), так и НМП (6) (табл. 4). Выясним условия, при которых возникают НМП в случаях преобразований П1—П5.

Пусть задан некоторый элемент сверхвозрастающей последовательности, например $y = 10$. Для последовательностей $П2_0$—$П2_3$ (см. табл. 1) ему соответствует пара чисел 0 и $y = 10$. Допустим, что к этим числам одновременно прибавляется одно и то же число x. Полученные числа преобразуем согласно (1), найдем модуль их разности и сравним такие величины со значением w_{02} ПМП числа $y = 10$, где $w_0 = (y\,37)(\mathrm{mod}67) = (10\cdot37)(\mathrm{mod}67) = 35$, $m - w_0 = 67 - 35 = 32$.

Результаты таких преобразований для различных значений x приведены в табл. 4, из которой видно, что при $x = 0, 2, 4$ w_i^* определяется как ПМП, а при $x = 1, 3, 5$ — как НМП. Следовательно, на изменение модуля разности результатов ПМП элементов в УП может повлиять синхронное изменение весов. Поэтому можно предположить, что получение результата НМП (6) для элемента y возможно при нахождении хотя бы одного значения x, такого, при котором справедливо неравенство

$$((y + x)\,n)(\mathrm{mod}\,m) < (x\,n)(\mathrm{mod}\,m). \qquad (7)$$

В результате анализа различных значений y, x, m, n, d установлено, что для всех случаев модуль разности $|((x + y)\,n)(\mathrm{mod}\,m) - (x\,n)(\mathrm{mod}\,m)\|$ равняется $(y\,n)(\mathrm{mod}\,m)$ или $m - (y\,n)(\mathrm{mod}\,m)$. Исключением является случай $y = d = n^{-1}$, когда для любого значения x разность равняется единице, кроме случая, когда $x + y = m$. Следовательно, подбором числа x всегда можно добиться того, чтобы модуль разности равнялся $m - (y\,n)(\mathrm{mod}\,m)$.

Следует заметить, что при ОМП (2) числа $m - (y\,n)(\mathrm{mod}\,m)$ всегда получим $((m - (y\,n)(\mathrm{mod}\,m))\,d)(\mathrm{mod}\,m) = (md - (y\,n\,d)(\mathrm{mod}\,m))(\mathrm{mod}\,m) = (-(y\,n\,d)(\mathrm{mod}\,m))(\mathrm{mod}\,m) = -m(y\,n\,d)(\mathrm{mod}\,m) = m - (y)(\mathrm{mod}\,m) = m - y$.

Таблица 4. **Анализ ПМП при синхронном изменении весов бита**

Преобразование	Вес бита при изменении элемента сверхвозрастающей последовательности на величину x					
	0	1	2	3	4	5
ПМП при $v_i = x$: $w_{i1} = (v_i 37)(\mathrm{mod}\,67)$	0	37	7	44	14	51
$v_i = 10 + x$	10	11	12	13	14	15
ПМП при $v_i = 10 + x$: $w_{i2} = (v_i 37)(\mathrm{mod}\,67)$	35	5	42	12	49	19
Модуль разности $w_i^* = \|w_{i1} - w_{i2}\|$	35	32	35	32	35	32

Таким образом, используя УП, можно получить НМП как разность ПМП.

Построение обычной последовательности с использованием однократной НМП. Рассмотрим варианты построения способов шифрования, которые, в конечном итоге, дают возможность получить одну обычную последовательность как полный аналог последовательности $П2_0$. При этом возможны различные варианты начальных преобразований П1—П5 сверхвозрастающей последовательности на основе УП.

Алгоритм построения обычной последовательности основан на определении одного из корней неравенства (7). Шаги алгоритма приведены в табл. 5 и 6. На основании анализа данных табл. 5 можно сделать следующие выводы.

1. Способ построения обычной последовательности по сверхвозрастающей позволяет использовать преобразования УП, при которых результат НМП сверхвозрастающей последовательности ($w_i^* = w'_{i0}$, $i = 1 \div 6$) можно получить как разность результатов обычных ПМП элементов столбца УП.

2. Элементам сверхвозрастающей последовательности соответствуют значения информационного бита, равного единице, а элементам полученной обычной последовательности — значения информационного бита, равного нулю. Поэтому при традиционном способе шифрования, когда вес ранца определяется как сумма весов обычной последовательности, которые соответствуют равным единице значениям информационных бит блока, к расшифрованному двоичному тексту следует применять ПИ, т.е. замену информационных символов, равных нулю, единицей и наоборот.

3. Расшифрование текста возможно при использовании ПМП.

Вывод 3 вытекает из следующих преобразований для суммарного веса W:

$$W = \sum_{i=1}^{L} a_i w_i^* = \sum_{i=1}^{L} a_i (m - (v_i n) (\mathrm{mod} m) =$$

$$= s_0 m - \sum_{i=1}^{L} a_i (v_i n) (\mathrm{mod} m) = s_0 m - \sum_{i=1}^{L} a_i w_i,$$

где s_0 — число нулей в информационном блоке, который соответствует информационному блоку $(c_1, c_2, \ldots, c_L)$ длиной L,

$$(W\ d) (\mathrm{mod} m) = \left(\left(s_0 m - \sum_{i=1}^{L} a_i w_i \right) d \right) (\mathrm{mod} m) =$$

$$= \left(-\sum_{i=1}^{L} a_i (w_i d) (\mathrm{mod} m) \right) (\mathrm{mod} m) = \left(-\sum_{i=1}^{L} a_i v_i \right) (\mathrm{mod} m) =$$

$$= m - \left(\sum_{i=1}^{L} a_i v_i \right) (\mathrm{mod}\, m).$$

На основании анализа данных табл. 6 можно сделать следующие выводы.

1. Найденные значения x_i обеспечивают выполнение неравенства

$$w'_{i0} > w_{i1}, \quad i = 1 \div L, \tag{8}$$

как в случае НМП, так и при инверсиях, когда нулевые значения x_i являются наименьшими из возможных, для которых выполняется неравенство (8). Различная природа чисел x_i при наличии инверсий и без них приводит к тому, что при всех инверсиях $w_{i0} = w'_{i0} \neq w^*_i$, $i = 2, 3, 5$.

2. Элементам сверхвозрастающей последовательности соответствуют значения информационного бита, равного единице ($i = 1, 4, 6$) и нулю ($i = 2, 3, 5$), а элементам полученной обычной последовательности — только значения бита, равные нулю. Поэтому при традиционном способе шифрования, когда вес ранца определяется как сумма весов обычной последовательности согласно (2) к расшифрованному двоичному тексту для ряда бит следует применять ЧИ.

Таблица 5. **Способ построения обычной последовательности по сверхвозрастающей на основе НМП для $П2_0$**

Номер строки	Шаг алгоритма	Переменная	Элементы последовательностей для битов					
			1	2	3	4	5	6
0	Исходная сверхвозрастающая последовательность v_i, $i = 1 \div 6$ УП для исходной сверхвозрастающей	v_i	1	2	4	8	16	32
		v_{i0}	0	0	0	0	0	0
		v_{i1}	1	2	4	8	16	32
1	Определение корней неравенства (7) при ПМП $w_{ik} = (v_{ik}\, 84) \pmod{131}$, $k = 0, 1$, $i = 1 \div 6$	x_i	1	3	1	3	3	1
2	Синхронное увеличение весов бит на корни неравенства (7), $v1_{ik} = v_{ik} + x_i$, $i = 1 \div 6$, $k = 0, 1$	$v1_{i0}$	1	3	1	3	3	1
		$v1_{i1}$	2	5	5	11	19	33
3	ПМП $w_{ik} = (v_{1ik}\, 84) \pmod{131}$ для элементов строки 2	w_{i0}	84	121	84	121	121	84
		w_{i1}	37	27	27	7	24	21
4	Синхронное уменьшение весов бит:	w'_{i0}	47	94	57	114	97	63
	$w'_{i0} = w_{i0} - w_{i1}$, $w'_{i1} = w_{i1} - w_{i1} = 0$, $i = 1 \div 6$	w'_{i1}	0	0	0	0	0	0
5	НМП $w^*_i = 131 - (v_i\, 84) \pmod{131} = w'_{i0}$, $i = 1 \div 6$	w^*_i	47	94	57	114	97	63
6	Обычная последовательность весов $w_i = w'_{i0} = w^*_i$, $i = 1 \div 6$	w_i	47	94	57	114	97	63

3. Расшифрование шифротекста невозможно при использовании только ОМП.

Вывод 3 вытекает из следующих соображений. Суммарный вес ранца для слова A является суммой произведений элементов обычной последовательности на значение бит слова:

$$W = \sum_{k=1}^{L} a_i w_i .$$

Эта сумма может быть представлена в виде

$$W'_s = \sum_{k=1}^{L} a_i w_i = \sum_{e_i=1} a_i (m-(v_i\ n)(\mathrm{mod} m)) + \sum_{e_i=0} a_i ((v_i\ n)(\mathrm{mod} m)),$$

где индекс e_i определяет условие выполнения инверсии для i-го элемента последовательности ($e_i = 1$, если преобразование не выполнялось, $e_i = 0$,

Таблица 6. **Способ построения обычной последовательности по сверхвозрастающей на основе НМП для $П2_0$ с использованием ЧИ**

Номер строки	Шаг алгоритма	Переменная	Элементы последовательностей для битов					
			1	2	3	4	5	6
0	Исходная сверхвозрастающая последовательность v_i, $i = 1 \div 6$	v_i	1	2	4	8	16	32
	УП для исходной сверхвозрастающей	v_{i0} v_{i1}	0 1	0 2	0 4	0 8	0 16	0 32
1	ЧИ для базовой УП	v'_{i0} v'_{i1}	0 1	2 0	4 0	0 8	16 0	0 32
2	Определение корней неравенства (7) при ПМП $w_{ik} = (v_{ik}\ 84)(\mathrm{mod}\ 131)$, $k = 0, 1$, $i = 1 \div 6$	x_i	1	0	0	3	0	1
3	Синхронное увеличение весов бит на число x_i: $v1_{ik} = v'_{ik} + x_i$, $i = 1 \div 6$, $k = 0, 1$, $S_1 = 27$	$v1_{i0}$ $v1_{i1}$	1 2	2 0	4 0	3 11	16 0	1 33
4	ПМП $w_{ik} = (v1_{ik}\ 84)\ (\mathrm{mod}\ 131)$, $k = 0, 1$, $i = 1 \div 6$, для элементов строки 3	w_{i0} w_{i1}	84 37	37 0	74 0	121 7	34 0	84 21
5	Синхронное уменьшение весов бит: $w'_{i0} = w_{i0} - w_{i1}$, $w'_{i1} = w_{i1} - w_{i1} = 0$, $i = 1 \div 6$, $S_2 = 65$	w'_{i0} w'_{i1}	47 0	37 0	74 0	114 0	34 0	63 0
6	НМП $w^*_i = 131-(v_i\ 84)\ (\mathrm{mod}\ 131)$ $i = 1 \div 6$	w^*_i	47	94	57	114	97	63
7	Обычная последовательность $w_i = w'_{i0} \neq w^*_i$, $i = 1 \div 6$	w_i	47	37	74	114	34	63

если оно выполнено). Тогда при использовании обычного ОМП получим

$$(W\ d)\,(\mathrm{mod}\,m)=\left(\sum_{e_i=1}a_i(m-(v_i\ n)\,(\mathrm{mod}\,m))+\sum_{e_i=0}a_i((v_i\ n)\,(\mathrm{mod}\,m)\,d)\right)(\mathrm{mod}\,m)=$$

$$=\left(-\sum_{e_i=1}a_i v_i+\sum_{e_i=0}a_i v_i\right)(\mathrm{mod}\,m), \qquad (9)$$

где последнее выражение в скобках может быть как положительным, так и отрицательным числом. Это выражение отображает сумму элементов сверхвозрастающей последовательности только тогда, когда первая из сумм в скобках равна нулю.

Для такого варианта шифрования информации также существует способ расшифрования на основе УП. Пусть известна обычная последовательность $\{w_i\}_{i=1}^{n}$. Тогда суммарный вес S, соответствующий слову A, согласно обозначениям переменных, принятым в табл. 6, можно записать в виде

$$S=\sum_{a_i=1}w_i=\sum_{a_i=1}w'_{i0}+\sum_{a_i=0}w'_{i1}.$$

Как видно из табл. 6, элементам обычной последовательности строки 7 соответствуют элементы УП, представленные в строке 5. Переход от строки 7 к строке 5 не изменяет значения суммарного веса S.

Рассмотрим УП, представленную в строке 4 табл. 6. При этом переходе суммарный вес S возрастет на величину $S_2 = 65$, которая равняется сумме элементов w_{i1}, а общая сумма увеличится на число S_2 и будет равна $S + S_2$:

$$S_{01}=S+S_2=\sum_{a_i=1}w_{i0}+\sum_{i=1}^{n}w_{i1}.$$

Элементы УП строки 3 можно получить с помощью ОМП строки 4. Это значит, что его можно применить и к сумме элементов. Тогда из (8) получим

$$((S+S_2)\,d)\,(\mathrm{mod}\,m)=\left(\left(\sum_{c_i=1}w_{i0}+\sum_{i=1}^{n}w_{i1}\right)d\right)(\mathrm{mod}\,m)=\sum_{c_i=1}v1_{i1}+\sum_{c_i=0}v1_{i0}=S_{02}.$$

Если от суммы S_{02} вычесть сумму S_1 (элементы v_{i0} — корни неравенства (8)), то получим вес S_{03}, рассчитанный по сверхвозрастающей последовательности, преобразованной на основе ЧИ:

$$S_{03}=\sum_{a_i=1}v'_{i1}+\sum_{a_i=0}v'_{i0}=\sum_{a_i=1}(v1_{i1}-x_i)+\sum_{a_i=0}(v1_{i0}-x_i)=$$

$$= \sum_{a_i=0} v1_{i0} + \sum_{a_i=1} v1_{i1} - \sum_{i=1}^{n} x_i = S_{02} - S_1.$$

Теперь информационное слово можно расшифровать, используя известные данные об УП, полученной в результате ЧИ исходной сверхвозрастающей последовательности, представленной в табл. 6.

Следовательно, при расшифровании информации с помощью увеличения исходной суммы S на S_2 становится возможным ОМП полученной суммы, после чего ее уменьшение на S_1 образует сумму элементов сверхвозрастающей последовательности при ЧИ. Таким образом, использование сумм S_1 и S_2 формирует «лазейку» для однократных НМП с использованием ЧИ.

Рассмотрим пример зашифрования и расшифрования информации с использованием обычной последовательности для блока 100111.

Информационный блок 100111. Зашифрование информации:

$$100111 \rightarrow 47, 37, 74, 114, 34, 63,$$

$$S = 47 + 114 + 34 + 63 = 258.$$

Информационный блок 100111. Расшифрование информации:

Ш а г 1. $S_{03} = S_{02} + S_1 = 258 + 63 = 323$.

Ш а г 2. $S_{02} = ((S + S_2)\ 39) \pmod{131} = (323 \cdot 39) \pmod{131} = 21$.

Ш а г 3. $S_{03} = S_{02} - S_1 = 21 - 5 = 16$.

Ш а г 4. Расшифрование суммы 16 с использованием последовательности $П2_1$ (табл. 7). Если бы при расшифровании была использована исходная сверхвозрастающая последовательность, то потребовалась бы инверсия бит 1, 4 и 6.

На основании изложенного можно сделать вывод о том, что в случае шифрования на основе обычных последовательностей, построенных с помощью ЧИ и НМП, для расшифрования шифротекста требуется знание сверхвозрастающей последовательности, сумм S_1 и S_2 и варианта ЧИ.

Таблица 7. **Расшифрование суммы 16**

Номер бита	Условие определения значения бита	Значение бита
6	16 < 32	1
5	16 < = 16 (16 – 16 = 0)	1
4	0 < 8	1
3	0 < 4	0
2	0 < 2	0
1	0 < 1	1

Использование однократных инверсий и однократных НМП при формировании ОМП. Выше было указано, что при использовании только однократных НМП в случае формирования обычной последовательности возникает необходимость ПИ расшифрованного информационного сообщения. Такое утверждение вытекает из определения НМП при его реализации через УП, когда в результате ПМП получены такие преобразованные числа, среди которых меньшим будет число, соответствующее начальному элементу, увеличенному на корень неравенства (7), а большим — соответствующее корню неравенства (7). Следовательно, однократное НМП всех элементов сверхвозрастающей последовательности при водит к необходимости инверсии каждого бита информации, т.е. к ПИ.

В случае использования НМП и ЧИ на основе УП расшифрование зашифрованной информации возможно, но при этом требуется более полная информация, чем сверхвозрастающая последовательность. Действительно, как видно из табл. 7, использование только сверхвозрастающей последовательности приводит к тому, что после расшифрования вместо информационного блока 100111 получаем блок 000010, т.е. расшифрованная информация отличается от начальной в первом, четвертом и шестом бите. Таким же будет отличие для любого другого информационного блока, т.е. в тех битах информации, в которых не была применена ЧИ.

Следовательно, при использовании ЧИ нейтрализуется действие НМП относительно инверсии информационных бит данных. В то же время, для обычных последовательностей, полученных с использовнием одного НМП, необходима полная инверсия бит информационного блока.

Суть механизма действия ЧИ заключается в следующем. При инверсии бита данных значение разности чисел больше нуля, полученных посредством ПМП УП, достигается при $x_i = 0$ и ряде других значений x_i. Поэтому при инверсии и ПМП элементов УП происходит двойная инверсия, в связи с чем справедливо следующее утверждение.

Утверждение. Необходимость инверсии информационного бита после его расшифрования на основе сверхвозрастающей последовательности определяется суммой по модулю два общего числа модульных преобразований и числа инверсий для этого бита, которые были использованы при формировании обычной последовательности по сверхвозрастающей.

Согласно этому утверждению возможным является следующий способ расшифрования текста: после выполнения всех этапов расшифрования вплоть до использования сверхвозрастающей последовательности необходимая инверсия для бит информационного блока реализуется посредством побитового сложения по модулю два полученного слова с некоторым балансирующим словом длиной, равной длине блока. Такой способ воз-

можен, так как сумма по модулю два для числа инверсий (значение 0 или 1), побитовое двоичное добавление которой в случае значения 1 реализует инверсию, а при сумме, равной 0, не изменяет результата. Поэтому при обычной последовательности $П2_5$ (см. в табл. 3) балансирующим словом будет 1111. Для обычной последовательности $П2_1$ (см. табл. 7) балансирующее слово — 100101.

Повторное использование НМП. Для построения обычной последовательности по сверхвозрастающей можно использовать кратные ПМП и НМП и кратные инверсии. Покажем это на примере сверхвозрастающей последовательности $П2_0$ (см. табл. 1), шаги алгоритма построения которой приведены в табл. 8.

Для рассматриваемого варианта построения обычной последовательности НМП применяются четное число раз ко всем информационным битам. При кратном двум числе НМП реализуется двойная инверсия: $0 \rightarrow \rightarrow 1 \rightarrow 0$ и $1 \rightarrow 0 \rightarrow 1$. В этом случае не требуются дополнительные операции инверсии при расшифровании бит информации, т.е. не требуется хранение балансирующего слова. В рассмотренном примере суммы S_1 и S_2 определялись на каждом уровне итерирования. Именно они (а также балансирующее слово) являются результатом формирования «лазейки», позволяющей расшифровать информацию.

Приведенные примеры построения обычных последовательностей из сверхвозрастающих не являются уникальными. Для проверки корректности подхода разработано несколько компьютерных программ, реализующих формирование обычных последовательностей из случайных вариантов сверхвозрастающих с последующей проверкой всех вариантов зашифрования и расшифрования. По результатам их работы получено дополнительное условие на этапе расшифрования данных: если на какомлибо уровне расшифрования сумма окажется отрицательной, то ее необходимо увеличить на число $m1$ из этого же уровня (определить значение по модулю $m1$). При выполнении этого условия во всех случаях расшифрованная информация была правильной.

Следует заметить, что на каждом этапе преобразования обычной последовательности в сверхвозрастающую ОМП суммарный вес ранца S_1 отображает разность двух сумм, характеризующих информационный блок, а не сумму элементов последовательности предыдущего уровня (при многократном итерировании) или сверхвозрастающей последовательности. Поэтому при определении последовательности предыдущего уровня для многократно итерируемых систем или сверхвозрастающей последовательности невозможно сформировать систему уравнений линейного программирования, а только ее варианты.

При формировании обычных последовательностей с использованием НМП и инверсий каждый бит для k-кратно итерируемой системы может принимать 2^k различных значений. Теоретически это вытекает из следующего условия: на каждом уровне итерирования новое значение элемента обычной последовательности может принимать одно из двух значений, получаемых либо согласно (1), либо согласно (6). Рассмотрим пример практического подтверждения такого теоретического положення.

Каждое из чисел $i = 1 \div 9$ будем рассматривать как элемент сверхвозрастающей последовательности при трехкратном итерировании для $m_1 = 20$, $n_1 = 11$, $m_2 = 60$, $n_2 = 37$, $m_3 = 181$, $n_3 = 101$. Пусть информация о способе

Таблица 8. **Способ построения обычной последовательности при использовании трехкратных модульных преобразований и инверсии**

Номер шага	Шаг алгоритма	Переменная	Элементы последовательностей для битов					
			1	2	3	4	5	6
0	Базовая последовательность v_i, $i = 1 \div 6$	v_i	1	2	4	8	16	32
1.1	Первая инверсия для УП	v_{i0} v_{i1}	0 1	2 0	0 4	0 8	16 0	0 32
2.1	Корни (7) и их сумма $S_{11} = 4$	$x1_i$	1	0	1	1	0	1
3.1	ПМП ($m1 = 67$, $n1 = 47$, $d1 = 10$) $w1_{ik} = ((v_{ik} + x_i)\, n1) \pmod{m1}$ и получение суммы $S_{21} = 92$	$w1_{i0}$ $w1_{i1}$	47 27	27 0	47 34	47 21	15 0	47 10
4.1	Первая обычная последовательность в виде УП	$w1'_{i0}$ $w1'_{i1}$	20 0	27 0	13 0	26 0	15 0	37 0
1.2	Вторая инверсия для УП	$v2_{i0}$ $v2_{i1}$	20 0	27 0	13 0	0 26	0 15	37 0
2.2	Корни (7) и их сумма $S_{12} = 4$	$x2_i$	0	0	0	2	2	0
3.2	ПМП ($m1 = 149$, $n1 = 71$, $d1 = 21$) $w2_{ik} = ((v_{ik} + x_i)\, n1) \pmod{m1}$ и получение суммы $S_{22} = 66$	$w2_{i0}$ $w2_{i1}$	79 0	129 0	29 0	142 51	142 15	94 0
4.2	Вторая обычная последовательность в виде УП	$w1'_{i0}$ $w1'_{i1}$	79 0	129 0	29 0	91 0	127 0	94 0
1.3	Третья инверсия для УП	$v3_{i0}$ $v3_{i1}$	0 79	129 0	0 29	91 0	0 127	0 94
2.3	Корни (7) и их сумма $S_{13} = 13$	$x3_i$	5	0	5	0	2	1
3.3	ПМП ($m1 = 563$, $n1 = 101$, $d1 = 262$) $w2_{ik} = ((v_{ik} + x_i)\, n1) \pmod{m1}$ и получение суммы $S_{23} = 199$	$w3_{i0}$ $w3_{i1}$	505 39	80 0	505 56	183 0	202 80	101 24
4.3	Третья обычная последовательность	w_i	466	80	449	183	122	77

Таблица 9. **Веса элементов обычной последовательности для элемента *v* сверхвозрастающей последовательности**

Число *v*	Значение *w* элемента обычной последовательности для различных вариантов преобразования							
	111	110	101	100	011	010	001	000
1	41	140	46	135	75	106	12	169
2	147	34	121	60	63	118	24	157
3	101	80	167	14	109	72	159	22
4	113	68	155	26	3	178	84	97
5	67	114	20	161	143	38	125	56
6	79	102	8	173	37	144	50	131
7	33	148	54	127	83	98	4	177
8	45	136	42	139	71	110	16	165
9	180	1	88	93	117	64	151	30

формирования обычной последовательности на каждом уровне представляется так: индексу 1 соответствует ПМП (согласно (1)), индексу 0 — НМП (согласно (6)). Тогда трем ОМП будет соответствовать обозначение 111, а трем НМП — 000. Всего таких вариантов восемь. Значения весов битов обычной последовательности приведены в табл. 9.

Следовательно, при условии, что параметры модульных преобразований (числа m и n в соотношениях (1) и (6)) независимы от варианта преобразований на каждом из уровней итерирования, общее число вариантов обычных последовательностей, построенных по одной и той же сверхвозрастающей, будет равняться 2^{kL}.

Выводы

Предложенный способ получения обычной последовательности из сверхвозрастающей в задаче формирования многократно итерированной ранцевой системы шифрования с открытым ключом, основан на операции НМП и инверсиях, при которых построение односторонней функции с «лазейкой» реализуется с использованием понятия удвоенной последовательности весов предметов, а при расшифровании информации дополнительно используется балансирующее слово. На основании проведенных исследований можно утверждать, что этот способ является усилением криптосхемы Меркля—Хеллмана. В то же время, полученные усиления в задаче шифрования ранцами требуют дополнительного детального криптографического анализа и оценки криптостойкости.

The algorithm for forming the normal sequence of eccessively ascending one, based on the introduced concepts of indirect modular transformations and partial inversions with the «loophole» formation on the basis of duplicate sequences of the items weights has been developed as part of the Merkle-Hellman cryptoscheme of knapsack encryption . It is shown that under such an approach 2^k options of the element of normal sequence may correspond to each element above the ascending sequence for the k-fold iterated backpack system, and the number of options of normal sequence, with all the same parameters of the modular transformations, may achieve 2^{kL}, where L is the number of bits in the data block. In this case, the inverse problem of determining the excessively ascending sequence of the normal one can be reduced to the problem of integer linear programming only as a variant with the great number of options.

СПИСОК ЛИТЕРАТУРЫ

1. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си: Пер. с англ. — М. : изд-во Триумф, 2002. — 816 с.
2. *Защита* информации. Малый тематический выпуск // ТИИЭР. — 1988. —**76**, № 5. — С. 24—94.

Поступила 21.05.13

ВИННИЧУК Степан Дмитриевич, д-р техн. наук, вед. науч. сотр. Ин-та проблем моделирования в энергетике им. Г.Е. Пухова НАН Украины. В 1977 г. окончил Черновицкий госуниверситет. Область научных исследований — разработка методов, моделей и программных средств для анализа распределительных систем сжимаемой и несжимаемой жидкостей, авиационные системы кондиционирования воздуха; противоаварийная частотная автоматика электроэнергетических систем.