МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ТА ОБЧИСЛЮВАЛЬНІ МЕТОДИ

doi:https://doi.org/10.15407/emodel.41.02.003

УДК 511:003.26.09

С.Д. Винничук, д-р техн. наук, **В.М. Міська**, аспірант
Інститут проблем моделювання в енергетиці ім. Г.Е. Пухова НАН України.
(Україна, 03164, Київ, вул. Генерала Наумова, 15,
тел. +380734095726, e-mail: vynnychuk@i.ua; vitalii.misko@gmail.com

Метод множинного квадратичного *k*-решета з використанням сигнальних остач при просіюванні пробних значень

Описано алгоритм методу множинного квадратичного *k*-решета, який є модифікацією методу квадратичного решета. У даній модифікації зпропоновано при просіюванні пробних значень виконувати попереднє їх просіювання на основі порівняння остач $y_k(X) = X^2 - kN$ $(k \geq 1)$ з сигнальними остачами $y_k^*(X)$, де $y_k^*(X)$ — добуток перших степенів множників $y_k(X)$. Серед пробних значень відсіюють ті, для яких $\log(y_k(X)) < h \log(y_k^*(X))$, де дійсне число $h \in [0,1]$ — це параметр, що обирається. Встановлено, що при зростанні значення N збільшується значення h, при якому досягається найменший час розрахунку. Встановлено також, що зменшення часу отримання достатньої кількості B-гладких відбувається при обмеженні для показників степенів дільників B-гладкого, які перевищують одиницю, для множини елементів загальної факторної бази, більших певного значення, визначеного за параметром *kff*. На основі чисельних експериментів з відносно малими числами порядку 10^m при $m = 20 \div 32$ показано, що час розрахунку достатньої кількості B-гладких є функцією параметра *kff*. Описано кроки алгоритму методу та ідеї їх реалізації. Наведено евристичну оцінку складності запропонованого методу для ряду значень параметра *pla*.

Ключові слова: цілочисельна факторизація, метод квадратичного решета, множинне решето.

Постановка задачі. На даний час криптоалгоритм RSA використовується у web-серверах, браузерах, електронній пошті та є ключовою технологією у системах електронних платежів. Найпоширеніша атака на цей криптоалгоритм заснована на факторизації ключа N, що є добутком двох простих чисел [1—3]. Серед методів факторизації метод квадратичного решета (QS) займає друге місце у списку найшвидших алгоритмів, поступаючись тільки методу решета числового поля [4]. Відносна простота алгоритму

сприяла появі багатьох його модифікацій, серед яких методи множинного квадратичного решета (MPQS) [5] та метод квадратичного *k*-решета (MQkS) [6].

У методі QS формують пару чисел A і B таких, що $A^2 = B^2 (\mathrm{mod}\, N)$, де число A — це добуток ряду пробних значень X, а B — добуток відповідних їм остач,

$$y(X) = X^2 - N, \tag{1}$$

які розкладаються в добуток простих чисел p і називаються B-гладкими.

Нехай $X = X_0 + x = |\sqrt{N} + 1| + x$. При зростанні значень x кількість B-гладких суттєво зменшується. Тому в методах MPQS використовують множину поліномів:

$$y_{a,b}(X) = (aX + b)^2 - N = a^2 X^2 + 2abX + b^2 - N, \tag{2}$$

де a, b — спеціально підібрані цілі числа. Необхідно зауважити, що в порівнянні з методом QS при $a > 1$ для поліномів (2) в a раз зменшується кількість можливих значень пробних X при тому ж радіусі просіювання. У роботах [7, 8] зазначено, що такі поліноми не слід міняти часто, оскільки це потребує значного обсягу попередніх обчислень та може зумовити збільшення обчислювальної складності.

У роботі [6] запропоновано метод MQkS, в якому для пошуку B-гладких використовується множина поліномів:

$$y_k(X) = X^2 - kN, \tag{3}$$

де множники k є довільними натуральними числами, які не діляться без остачі на квадрат більше одного простого числа (k не дорівнює 36, 72, 100, 108 і т.д.). Якщо множники k діляться без остачі на квадрат єдиного простого числа q, то з інтервалу просіювання виключаються значення X, для яких $X (\mathrm{mod} q) = 0$.

На відміну від запропонованих раніше методів MPQS для більшості значень k множина пробних X, визначених на основі величини радіусу просіювання, залишається незмінною. Тому при зміні значень k більшою є кількість пробних X, близьких до $\lfloor \sqrt{kN} + 1 \rfloor$. На основі чисельних експериментів з числами порядку 10^{20} — 10^{30} було встановлено [6], що в методі MQkS кількість аналізованих пробних X, на основі яких отримано L^a+3 B-гладкі числа, менша за їх кількість в базовому методі QS в шість і більше разів. При цьому для кожного значення k формується своя поточна факторна база (ФБ) з числом елементів *pfa*, а розмір *fa* загальної ФБ (ЗФБ) такий же, як в методі QS.

У роботі [6] для порівняння методів QS та MQkS використано ділення остач (1) і (3) на елементи ФБ. Експериментально встановлено, що за допомогою алгоритму методу MQkS час пошуку достатньої кількості B-гладких у 1,5—2 рази менше. Зазначимо, що при застосуванні методу MQkS виконувалася часта зміна поліномів (3), що потребувало додаткових попередніх обчислень. Тому можна очікувати, що при використанні більш ефективної процедури просіювання метод MQkS зможе забезпечити більш суттєве зменшення обчислювальної складності процесу просіювання та загального часу вирішення задачі факторизації.

Оцінка кількості B-гладких, що втрачаються при попередньому просіюванні на основі порівнянь $y_k(X)$ і $y^*(X)$. Нехай ЗФБ є множиною всіх найменших простих чисел починаючи з 2, яка містить fa елементів, $fa=(L^a)^{pla}$, де $L^a=\exp\left(\frac{\sqrt{2}}{4}\sqrt{\ln N\ln\ln N}\right)$ — розмір ФБ, рекомендований в [9]; pla — параметр, значення якого міститься в межах від 0,5 до 1,5. Оскільки для остач $y_k(X)$ при різних значеннях k множини можливих дільників є різними, в методі MQkS для кожного k формується поточна ФБ, число елементів у якій позначено через pfa.

Визначимо розмір радіусу просіювання $fb=(L^a)^{plb}$, де plb — параметр, значення якого міститься в межах від 0,5 до 4,0; $fb=L^b$ при $plb=3$, а L^b є рекомендованою в [9] величинию радіусу просіювання. В чисельних експериментах у більшості випадків використовувалося значення $plb=1{,}4$, оскільки час отримання достатньої кількості B-гладких при $h=0$ та $pla=0{,}8\div1{,}0$ був близький до мінімального. Вважаємо, що при пошуку B-гладких остач $y_k(X)$ пробне X не буде відсіюватися, якщо виконано умову

$$\log(y_k^*(X))\ge h\log(y_k(X)), \tag{4}$$

де h — деяке число $h\in[0,1]$. Множину пробних X, для яких виконано умову (4), позначимо через MV(h). Тоді факт, що пробне X відсіюється, позначимо як $X\notin$ MV(h), а в інших випадках $X\in$ MV(h). Слід зазначити, що при $h=1$ до множини B-гладких ввійдуть остачі тільки $y_k(X)$, для яких виконано умову

$$y_k(X)=y_k^*(X), \tag{5}$$

тобто $y_k(X)$ є добутком простих чисел з поточної ФБ, показник степеня яких дорівнює одиниці.

Вплив параметру h на час визначення достатньої кількості B-гладких оцінимо за даними чисельних експериментів при фіксованих значеннях

параметрів $pla = 1{,}0$ та $plb = 1{,}4$ на множині чисел N порядку 10^m ($m = 20 \div 32$), сформованих за такими правилами:

кожне число N є добутком двох простих;

кожне просте число задається як сума опорного (зазвичай складеного числа) та одного з п'яти найменших значень приростів до нього;

для першого з простих множників числа N значення опорного обирається як випадкове число в діапазоні від $0{,}35\sqrt{N}$ до $0{,}9\sqrt{N}$;

для другого з простих множників числа N значення опорного — це ціле число, найближче до частки від ділення N на перше з опорних.

Значення опорних та прирости до них наведено в табл. 1. Результати чисельних експериментів з визначення $fa + 3$ B-гладких для кожного з 25 варіантів чисел N порядку 10^m($m = 20 \div 32$) та визначення серед них кількості тих, для яких

$$\log(y_k^*(X)) < h \log(y_k(X)) \tag{6}$$

при $h = 0{,}1j$ ($j = 0 \div 10$), наведено в табл. 2, де окремо виділено ті B-гладки, які отримано при $X = X_0 = \lfloor \sqrt{N} + 1 \rfloor$ та $X = X_0 - 1 = \lfloor \sqrt{N} \rfloor$. Інформацію про їх кількість подано у стовпчику D_0. Значення пробних X, які дорівнюють X_0 та $X_0 - 1$, не відсіюються при довільних значеннях параметра h. За такої умови виявилося, що при $h < 0{,}3$ відсутні B-гладкі, для яких виконано умову (6). Тобто жодне з B-гладких не втрачено при виконанні умови (6)

Таблиця 1

m	Опорне число 1	Приріст					Опорне число 2	Приріст				
		1	2	3	4	5		1	2	3	4	5
20	6 471 594 853	16	36	54	96	120	15 452 141 593	58	76	78	106	118
21	27 749 160 899	32	42	54	92	140	36 037 125 721	42	88	100	112	120
22	87 614 993 781	8	82	86	110	116	114 135 715 457	2	12	14	36	54
23	274 858 909 339	34	54	94	114	130	363 823 025 568	1	25	29	43	79
24	651 133 587 339	4	14	58	98	104	1 535 783 162 540	53	63	83	149	219
25	2 095 629 580 239	142	160	184	248	292	4 771 835 678 545	28	46	48	108	118
26	6 787 809 030 482	39	41	77	111	195	14 732 294 257 385	24	78	122	158	194
27	22 126 102 809 573	8	16	34	58	76	45 195 487 366 502	131	167	195	215	225
28	72 582 191 787 419	14	32	68	108	222	137 774 841 923 874	89	107	119	133	137
29	239 604 396 594 260	47	81	209	293	357	417 354 612 108 130	21	39	67	123	133
30	687 691 741 189 047	100	104	176	184	244	1 454 139 900 343 951	16	22	130	162	190
31	2660737903883030	101	153	219	243	329	3758355900220833	20	28	38	70	80
32	8950030870996722	5	31	119	149	167	11173145818307493	4	20	26	86	104

для $h < 0{,}3$. Дані про число втрачених B-гладких внаслідок відсіювання пробних X при $h = 0{,}1j$ для $j = 4 \div 10$ наведено у стовпчиках D_j для відповідних значень j, у стовпчику D_{sum} наведено сумарну кількість B-гладких. У табл. 3 наведено значення відношень D_j / D_{sum} для $h = 0{,}1j$ ($j = 4 \div 10$).

Для оцінки можливості використання обмежень (4) при пошуку B-гладких в чисельних експериментах визначалася кількість $XX(j)$ пробних X, для яких виконуються обмеження

$$0{,}1\, j \log(y_k(X)) \le \log(y_k^*(X)) \le 0{,}1(j+1) \log(y_k(X)) \; (j = 0 \div 9).$$

При отриманні таких даних для кожного з пробних X обчислювалися значення $y_k(X)$ та $y_k^*(X)$, їх логарифми та відношення $\log(y_k^*(X)) / \log(y_k(X))$. Сумарне фактичне число X_{sum} пробних обчислювалося для 25 варіантів чисел N порядку 10^m ($m = 20 \div 32$). В табл. 4 наведено значення відношень $xd(j) = XX(j) / X_{\text{sum}}$ при $j = 0 \div 9$, що відповідає значенням $h = 0{,}1j$.

На основі даних, наведених у табл. 2—4, можна зробити наступні висновки.

1. При зростанні значення параметру h у співвідношенні (4) збільшується кількість відсіяних X та суттєво зменшується кількість тих пробних X, серед яких слід шукати B-гладкі остачі $y_k(X)$. Обчислювальні витрати на попереднє просіювання є меншими, ніж витрати на перевірку,

Таблиця 2

m	Кількість втрачених B-гладких при обмеженні (4)								
	D_4	D_5	D_6	D_7	D_8	D_9	D_{10}	D_0	D_{sum}
20	9	43	180	495	1224	1966	2 728	72	2800
21	2	19	135	490	1366	2274	3 184	66	3250
22	6	22	118	488	1472	2553	3 654	71	3725
23	2	18	110	506	1617	2904	4 209	66	4275
24	0	17	116	479	1725	3346	4 809	91	4900
25	0	13	106	552	1817	3685	5 506	94	5600
26	0	12	89	482	1962	4140	6 314	86	6400
27	0	11	86	542	2197	4822	7 209	91	7300
28	0	9	82	465	2204	5388	8 176	99	8275
29	1	9	73	491	2451	6094	9 306	94	9400
30	0	7	82	548	2549	6777	10 551	99	10650
31	0	3	70	480	2801	7660	11 942	108	12050
32	0	3	52	491	2903	8565	13 498	102	13600

Таблиця 3

m	Значення відношень D_j / D_{sum} для d_j						
	d_4	d_5	d_6	d_7	d_8	d_9	d_{10}
20	0,003214	0,015357	0,064286	0,176786	0,437143	0,702143	0,974286
21	0,000615	0,005846	0,041538	0,150769	0,420308	0,699692	0,979692
22	0,001611	0,005906	0,031678	0,131007	0,395168	0,685369	0,98094
23	0,000468	0,004211	0,025731	0,118363	0,378246	0,679298	0,984561
24	0	0,003469	0,023673	0,097755	0,352041	0,682857	0,981429
25	0	0,002321	0,018929	0,098571	0,324464	0,658036	0,983214
26	0	0,001875	0,013906	0,075313	0,306563	0,646875	0,986563
27	0	0,001507	0,011781	0,074247	0,300959	0,660548	0,987534
28	0	0,001088	0,009909	0,056193	0,266344	0,651118	0,988036
29	0,000106	0,000957	0,007766	0,052234	0,260745	0,648298	0,99
30	0	0,000657	0,0077	0,051455	0,239343	0,636338	0,990704
31	0	0,000249	0,005809	0,039834	0,232448	0,635685	0,991037
32	0	0,000221	0,003824	0,036103	0,213456	0,629779	0,9925

Таблиця 4

m	Відношення XX_j / X_{sum} при h									
	0	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9
20	0,4654	0,225	0,1832	0,1414	0,0786	0,0532	0,0289	0,0168	0,0114	0,0029
21	0,4563	0,2222	0,1763	0,1366	0,0729	0,0465	0,0311	0,02	0,0114	0,004
22	0,4282	0,2097	0,171	0,1251	0,0585	0,0365	0,0228	0,014	0,0102	0,0038
23	0,4311	0,2028	0,1635	0,0931	0,0536	0,0335	0,0208	0,0126	0,0075	0,0023
24	0,4071	0,1973	0,1578	0,0888	0,0514	0,0322	0,0198	0,0143	0,0096	0,0027
25	0,4259	0,185	0,145	0,105	0,0539	0,0325	0,0196	0,012	0,0071	0,0018
26	0,3973	0,192	0,1591	0,1148	0,0498	0,03	0,0208	0,0131	0,0061	0,0016
27	0,3819	0,179	0,1458	0,1052	0,0456	0,0312	0,0211	0,0122	0,0071	0,0032
28	0,3674	0,1679	0,1344	0,0721	0,0358	0,0218	0,0135	0,0094	0,0057	0,0017
29	0,3679	0,1694	0,1338	0,073	0,0364	0,0233	0,0135	0,0077	0,0039	0,001
30	0,3561	0,1593	0,1286	0,0729	0,0355	0,0207	0,0126	0,0066	0,0039	0,0018
31	0,3915	0,1546	0,1191	0,0767	0,0324	0,0204	0,0124	0,0079	0,0049	0,0021
32	0,3543	0,1617	0,1093	0,0752	0,0387	0,0223	0,014	0,0063	0,003	0,0012

чи буде $y_k(X)$ B-гладким для всіх пробних X. Тому можна сподіватися, що при використанні процедури попереднього просіювання зменшиться час пошуку достатньої кількості B-гладких.

2. Загальний час розрахунку достатньої кількості B-гладких для чисел N порядку 10^m, де $m = 20 \div 32$, повинен зменшуватися при $h < 0{,}3$ і умові (6), оскільки жодне з B-гладких не втрачається. Але і при подальшому зростанні значення h серед відсіяних X можуть бути ті, для яких остача $y_k(X)$ буде B-гладким числом. Тоді для отримання достатньої кількості B-гладких буде необхідно розширювати область просіювання, що може зумовити зростання обчислювальної складності та часу розрахунку. Тому доцільно отримати оцінки такого часу при різних значеннях h.

3. Із даних табл. 2 випливає, що зростає відносна кількість B-гладких, для яких справедлива рівність (5), та для переважної більшості B-гладких виконується умова (4) при $h \geq 0{,}7$. Крім того, в результаті аналізу даних про показники степенів множників можна зробити припущення, що більші від одиниці показники степеня простих множників p остач $y_k(X)$ притаманні відносно малим значенням простих p та рідко зустрічаються при більших значеннях p. Це дає змогу зробити припущення, що при пошуку B-гладких доцільно обмежувати величину дільників p в остачах $y_k(X)$, для яких показник степеня може перевищувати одиницю. Це, безперечно, спричинить розширення області просіювання, але спростить його процедуру. Зважаючи на це доцільно визначити час отримання достатньої кількості B-гладких в залежності від ступеня такого обмеження.

Вплив обмежень (4) на час t пошуку достатньої кількості B-гладких при різних значеннях параметру h визначено по результатам чисельних експериментів з множинами чисел, наведених у табл. 1. Дані про час розрахунків наведено в табл. 5 при фіксованих параметрах $pla = 1{,}0$ та $plb = 1{,}4$. Згідно з даними, наведеними у табл. 5, кращий час отримано при $h = 0{,}7$ та $h = 0{,}8$, коли час розрахунку виявився майже вдвічі меншим за відповідний час розрахунку у випадку $h = 0$, коли B-гладкі шукали серед остач $y_k(x)$ для всіх пробних X. Тому надалі в чисельних експериментах було використано параметр $h = 0{,}7$.

Характер розподілу більших за одиницю показників степеня множників B-гладких. Згідно висновку 3 можна очікувати, що більші від одиниці показники степеня простих множників p для остач $y_k(X)$ рідко зустрічаються при більших значеннях p, однак при пошуку B-гладких доцільно обмежувати величину дільників p в остачах $y_k(X)$, для яких показник степеня перевищує одиницю. Справедливість такого припущення підтверджено даними про час отримання достатньої кількості B-гладких в залежності від ступеня такого обмеження, отриманими за результатами чисельних експериментів, у яких:

1). Допустимими *B*-гладкими вважалися такі, для яких показники степеня їх дільників p можуть бути більшими за одиницю при виконанні умови

$$f_p \le ff = (L^a)^{kff}, \qquad (7)$$

де f_p — порядковий номер простого p у списку простих чисел; *kff* — дійсне число, значення якого змінюються в діапазоні 0—1, при *kff* = 1 відсутні обмеження для f_p, а при *kff* = 0 до *B*-гладких будуть віднесені тільки такі остачі $y_k(X)$, для яких справедлива рівність (5).

2). Серед множини *B*-гладких, визначених за умови відсутності обмежень для f_p, визначалося число *B*-гладких, для яких виконувалися умови (7) при $kff = j/10$ ($j = 1 \div 10$).

Результати експериментів стосовно часу отримання достатньої кількості *B*-гладких для 25 варіантів чисел N порядку 10^m при $m = 20 \div 32$ наведено в табл. 6, де $pla = 1{,}0$, $plb = 1{,}4$, $h = 0{,}7$. Отримані дані підтвердили, що при збільшенні значення p зменшується відносне число *B*-гладких, для яких показник степеня множників p *B*-гладкого перевищує одиницю, тобто зростає відносна величина *B*-гладких, для яких виконано умову (7). Тому при фіксованому деякому значенні *kff* < 1 отримуватимемо меншу кількість

Таблиця 5

m	Час розрахунку t (с) *B*-гладких при h									
	0	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9
20	2,219	2,047	1,86	1,531	1,328	1,203	1,14	1,109	1,125	1,203
21	3,422	3,125	2,812	2,453	2,017	1,828	1,86	1,704	1,71	1,922
22	4,953	4,516	4,142	3,394	3,031	2,844	2,593	2,64	2,593	2,687
23	7,702	6,945	6,156	5,209	4,609	4,194	3,86	3,844	3,828	3,993
24	11,171	10,265	8,906	7,437	6,534	6,281	5,75	5,609	5,546	5,812
25	15,812	14,594	12,672	10,516	9,281	8,531	8,03	8	7,931	8,375
26	23,046	21,476	18,453	15,567	13,523	12,281	12,542	11,835	11,765	11,921
27	33,843	31,28	27,046	22,514	19,906	18,203	17,797	17,218	17,218	17,547
28	49,436	45,437	39,445	32,999	29,077	26,999	25,906	25,603	25,421	26,24
29	71,698	65,341	56,342	47,255	41,702	38,608	37,468	36,999	36,905	60,826
30	103,58	97,341	80,981	68,31	60,404	56,279	54,701	53,92	53,858	68,357
31	145,03	130,92	113,37	96,122	85,895	80,31	77,919	77,059	77,039	92,513
32	210,07	188,74	160,91	136,73	122,12	115,3	112	110,9	110,86	129,67

Примітка: підкреслено мінімальні значення.

B-гладких, ніж при *kff* =1. Проте їх отримання потребуватиме меншого числа операцій, оскільки для всіх множників p остач $y_k(X)$, порядкові номери f_p яких більші за *ff*, не допустиме значення показника степеня вище одиниці, а те, що він є дільником $y_k(X)$, визначається на основі попереднього просіювання.

Таким чином, як бачимо із табл. 6, найкращий час розрахунку отримано для $m = 20 \div 23$ при $kff = 0{,}7$; для $m = 24 \div 26$ при $kff = 0{,}6$; для $m = 27 \div 32$ при $kff = 0{,}5$. Відтак, при збільшенні значення N доцільно зменшувати значення параметра *kff*. Слід звернути увагу на те, що при збільшенні значення N мінімальний час розрахунку зміщується в сторону менших значень *kff*.

Вплив розміру загальної ФБ на час отримання достатньої кількості *B*-гладких. Відомо, що для методів QS і MPQS при зменшенні розміру ФБ збільшується радіус просіювання та може зростати час пошуку достатньої кількості *B*-гладких. Оскільки це характерно і для методу MQkS, важливо оцінити вплив значення *fa* ЗФБ на час пошуку достатньої кількості *B*-гладких. Для отримання таких оцінок проведено чисельні експерименти, в яких постійними були значення параметрів $plb = 1{,}4$ та $h = 0{,}7$. Для ряду фіксованих значень параметру *pla* визначалися пара-

Таблиця 6

m	Час t (с) розрахунку при *kff*									
	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1
20	1,794	1,531	1,36	1,156	1,079	0,969	0,953	0,969	1,031	1,125
21	2,688	2,244	1,984	1,719	1,578	1,468	1,422	1,468	1,562	1,718
22	3,593	3	2,703	2,344	2,125	2,016	2,000	2,063	2,25	2,5
23	5,453	4,578	3,859	3,405	3,171	3,015	3,000	3,125	3,37	3,813
24	7,641	6,469	5,414	4,844	4,469	4,328	4,5	4,515	4,906	5,609
25	10,37	9,093	7,703	6,687	7,814	5,969	6,156	6,344	6,906	7,922
26	14,89	13,053	11,14	9,422	8,812	8,64	8,702	9,14	10,047	11,546
27	21,968	18,702	15,656	13,421	12,687	12,614	12,678	13,25	14,765	17,093
28	30,499	26,203	21,277	19,389	18,490	17,921	18,281	19,392	21,859	25,265
29	42,871	36,537	30,233	27,233	25,514	25,171	25,843	27,5	31,435	36,514
30	58,936	50,655	42,608	38,15	36,389	35,811	36,483	39,561	44,722	53,022
31	81,075	69,575	58,534	51,53	50,077	50,092	51,94	55,654	63,353	76,013
32	111,871	90,857	80,607	75,091	71,731	71,937	73,664	80,34	97,621	110,512

Примітка: підкреслено мінімальні значення.

метри *kff* (*kff* = *j*/10, *j* > 3, але *kff* ≤ *pla*), при яких розрахунковий час *t* отримання достатньої кількості *B*-гладких для *N* порядку 10^m (*m* = 20÷32) був найменшим (табл. 7).

Згідно з даними, наведеними в табл. 7, при зменшенні значення параметра *pla* зростає час розрахунку для всіх аналізованих чисел *N* порядку 10^m при *m* = 20÷32. Спостерігається зростання часу при збільшенні значення *m*, при цьому темп зростання збільшується при зменшенні параметра *pla*. Зменшується також параметр *kff* при збільшенні значення *m*. Тому для вибору розміру ЗФБ та параметра *kff* доцільно визначити обчислювальну складність алгоритму пропонованого методу MQkS з просіюванням на основі сигнальних остач.

Алгоритм А1 методу MQkS з проріджуванням пробних *X* на основі сигнальних остач. У роботі [6] описано алгоритм **А** методу MQkS, в якому не передбачалося попереднє просіювання пробних *X*, а для кожного з пробних значень *X* обчислювалася остача $y_k(X)$ та перевірялося, чи буде вона *B*-гладкою. В алгоритмі **А1**, що пропонується, додатково враховано спосіб попереднього просіювання на основі сигнальних остач. При використанні алгоритму **А1** час визначення достатньої кількості *B*-гладких для тієї ж множини значень *N* при *m* = 20÷30 зменшився у 14—22 рази для

Таблиця 7

m	Найменший час *t* (с) в залежності від *kff* при *pla*									
	1		0,95		0,9		0,85		0,8	
	kff	*t* (с)	*kff*	*t* (с)	*kff*	*t* (с)	*kff*	*t* (с)	*kff*	*t* (с)
20	0,7	0,953	0,8	1,344	0,9	2,312	0,85	4,234	0,8	8,719
21	0,7	1,422	0,8	2,078	0,8	3,672	0,85	6,753	0,8	15,343
22	0,7	2	0,7	2,906	0,8	4,969	0,8	10,14	0,8	22,625
23	0,7	3	0,7	4,5	0,7	7,922	0,8	15,293	0,8	35,858
24	0,6	4,328	0,7	6,656	0,7	11,75	0,7	23,64	0,8	58,607
25	0,6	5,969	0,6	9,359	0,7	17,547	0,7	34,64	0,8	89,247
26	0,6	8,64	0,6	13,54	0,7	24,431	0,7	54,107	0,8	138,225
27	0,6	12,614	0,6	19,749	0,7	36,39	0,7	80,31	0,8	201,019
28	0,5	18,49	0,6	28,405	0,7	52,611	0,7	118,652	0,7	321,223
29	0,5	25,514	0,6	41,171	0,6	82,833	0,7	170,076	0,7	455,547
30	0,5	36,389	0,6	58,623	0,6	112,5	0,6	268,829	0,7	702,967
31	0,5	50,077	0,6	83,538	0,6	162,32	0,6	362,158	0,7	1051,68
32	0,5	71,731	0,6	114,969	0,6	243,98	0,6	563,7	0,7	1538,51

$plb = 1{,}4$, $h = 0{,}7$, $kff = 1{,}0$ та $pla = 1{,}0$, $pla = 0{,}95$ і $pla = 0{,}9$. Порівнюючи дані роботи [6, табл. 5] та дані, наведені в табл. 7, бачимо, що час розрахунку зменшився в 16—30 разів, при цьому більші зменшення відповідають більшим значенням N. Це свідчить про високу ефективність процедури попереднього просіювання.

Оскільки використання процедури попереднього просіювання суттєво змінило алгоритм методу MQkS, наведемо загальний алгоритм **A1** методу MQkS, в якому враховано процедуру попереднього просіювання.

А л г о р и т м **A1**.

1. Для заданого N та параметрів pla, plb, h, kff визначити:

кількість елементів fa ЗФБ за формулою

$$fa = \exp\left(pla\frac{\sqrt{2}}{4}\sqrt{\ln N \ln\ln N}\right);$$

базовий розмір радіусу просіювання fb за формулою

$$fb = \exp\left(plb\frac{\sqrt{2}}{4}\sqrt{\ln N \ln\ln N}\right);$$

границю гладкості B з урахуванням значення fa;

граничне значення ff порядкового номера простого числа, яке визначає множину можливих простих дільників p в остачах $y_k(X)$, показники степенів яких можуть перевищувати одиницю;

обчислити значення логарифмів для всіх елементів ЗФБ, дані запам'ятати в масиві p_log[fa].

1.1. Для всіх простих чисел, порядкові номери яких не перевищують ff, визначити їх степені, які не перевищують обраного значення, наприклад границю гладкості B чи обмеження на тип даних. Дані запам'ятати в масиві mpb[ff] (наприклад, при $B > 256$ і $B < 300$ для числа 2, порядковий номер якого в списку простих дорівнює одиниці, mpb[1] = 256, для числа 3 mpb[2] = 243 і т.д.). Лічильнику k присвоїти значення нуль.

2. $k = k + 1$.

3. Якщо k ділиться на квадрат двох чи більше різних простих чисел, перейти до кроку 2.

4. Для числа kN виконати:

4.1. Сформувати множину елементів поточної ФБ, до якої будуть віднесені прості p, що є елементами ЗФБ, а саме

для яких $(kN / p) = 1$;

які є дільниками k при $k \pmod{p^2} > 0$. Якщо для деякого простого p справедливо $k \pmod{p^2} = 0$, виключити таке p з множини елементів поточної ФБ незалежно від значення символу Лежандра (kN / p).

4.2. Визначити число *pfa* елементів поточної ФБ.

4.3. При $(2pfa/fa)^5 < 0{,}75$, перейти до кроку 2, якщо $(2pfa/fa)^5 \geq 0{,}75$ обчислити значення поточного (залежного від k) радіусу просіювання $pfb = fb\,(2pfa/fa)^5$ та перейти до кроку 4.4.

4.4. Визначити $x_0 = \left\lfloor \sqrt{kN} \right\rfloor + 1$ і присвоїти значення: $xp = x_0, xm = x_0 - 1$, $yp = xp^2 - kN, ym = kN - xm^2$. Визначити коефіцієнти розкладання xp, xm, yp, ym за основою 1000. Результати розкладання записати в масиви, наприклад *xp*0[], *xm*0[], *yp*0[], *ym*0[]. Визначити перші п'ять коефіцієнтів розкладання чисел xp, xm, yp, ym за основами степенів простих чисел, записаних у масиві mpb[*ff*] (кількість коефіцієнтів може розглядатися як параметр, а їх число 5 обрано експериментально). Результати розкладання записати в масиви, наприклад *xpp*[], *xmp*[], *ypp*[], *ymp*[].

4.5. Обчислити значення логарифму *lxp* = log (*xp*).

4.6. Для всіх простих чисел з поточної ФБ знайти корені рівняння

$$(y_k(X))\,(\mathrm{mod}\,p) = 0, \tag{8}$$

використавши алгоритм Шенкса. Значення меншого кореня запам'ятати в масиві, наприклад mx1[f_p], де f_p — порядковий номер простого p в списку простих.

5. $c = 0$. Пробні $X = x_0$ та $X = x_0 - 1$ вважати елементами множини MV(h). Перевірити, чи будуть B-гладкими остачі $y_k(x_0)$ та $y_k(x_0 - 1)$.

6. Виділити дві підмножини з інтервалу просіювання: $(x_0 + c, x_0 + c + z]$, $[x_0 - c - z, x_0 - c)$, де $z = \min(1000, (pfb - x_0 - c))$.

7. Для $t = 1 \div z$ присвоїти значення 0 елементам масивів $mzp[t]$, $mzm[t]$ та знайти наближене значення логарифму

$$\log(y_k(x_0 + c + t)) \approx lxp + \log(2c + t) = mlp[t].$$

8. Для кожного елемента p поточної ФБ визначити такі значення пробних $X = x_0 + c + t$ з підмножини $(x_0 + c, x_0 + c + z]$, для яких справедлива рівність (8), і для них додати значення логарифму від p, записане в p_log[f_p], до елементу масиву $mzp[t]$.

9. Порівнюючи значення $mzp[t]$ та $mlp[t]$ з урахуванням параметра h, визначити пробні X, які належать множині MV(h).

10. Для $X \in$ MV(h) перевірити, чи існують дільники p з показником степеня s вище одиниці для остачі $y_k(X)$ серед простих чисел з поточної ФБ, для яких $f_p \leq ff$. Якщо такі існують, то для кожного з них при $X = x_0 + c + t$ до елемента масиву $mzp[t]$ додати значення $(s - 1)\,p$_log[f_p], якщо $|mzp[t] - mlp[t]| < 0{,}1$, то $y_k(X)$ буде B-гладкою остачею.

11. Для кожного елемента p поточної ФБ визначити значення пробних $X = x_0 - c - t$ з підмножини $[x_0 - c - z, x_0 - c)$, для яких справедлива рівність

(8), і для них додати значення логарифму від p, записане в $p\_\log[f_p]$, до елемента масиву $mzm[t]$.

12. Порівнюючи значення $mzm[t]$ та $mlm[t]$ з урахуванням параметра h, визначити пробні X, що належать множині MV(h).

13. Для $X \in$ MV(h) і $X = x_0 - c - t$ перевірити, чи існують дільники p з показником степеня s більше одиниці для остачі $y_k(X)$ серед простих чисел з поточної ФБ, для яких $f_p \le ff$. Якщо такі існують, то для кожного з них до елемента масиву $mzm[t]$ додати значення $(s - 1)\ p\_\log[f_p]$, якщо $|mzm[t] - mlm[t]| < 0{,}1$, то $y_k(X)$ буде B-гладкою остачею.

14. Якщо знайдене число B-гладких перевищує fa, перейти до п. 16, а інакше — до п. 15.

15. $c = c + z$. Якщо $c = pfb$, перейти до п. 2, а інакше — до п. 6.

16. Діагоналізувати матрицю та знайти нульовий рядок. Якщо нульовому рядку відповідає тривіальний корінь рівняння $A^2 (\mathrm{mod}\, N) = B^2 (\mathrm{mod}\, N)$, де A — це добуток ряду пробних значень X, а B — добуток відповідних їм остач (3), замінити його іншим B-гладким за наявності, а інакше — перейти до кроку 2. Якщо отримано нетривіальний корінь, то вивести значення множників числа N і закінчити роботу алгоритму.

В алгоритмі **A1** передбачено, що матриця вирішується тільки тоді, коли знайдено достатнє число B-гладких. Проте такий пошук можна здійснювати на основі діагоналізації матриці «на ходу», що запропоновано у роботі [10], і тоді діагоналізацію матриці можна здійснювати кожен раз після виконання кроку 13.

Оцінка обчислювальної складності алгоритму A1. В описаному методі формування достатньої кількості B-гладких з проріджуванням пробних X на основі сигнальних остач використано параметри pla, plb, h та kff. Згідно зі значенням pla визначено розмір fa ЗФБ за формулою

$$fa = \exp\left(pla \frac{\sqrt{2}}{4} \sqrt{\ln N \ln\ln N} \right),$$

а базовий розмір радіусу просіювання fb — за формулою

$$fb = \exp\left(plb \frac{\sqrt{2}}{4} \sqrt{\ln N \ln\ln N} \right).$$

Такі варіанти визначення fa та fb корелюють з оцінкою обчислювальної складності виду $T(N) = O(\exp(C\sqrt{\ln N \ln\ln N}))$ для методу QS та його модифікацій, включаючи і метод MQkS. Тому, оцінюючи обчислювальну

складність, можна скористатися наближеною формулою для розрахунку часу:

$$T(m) \approx Ae^{C\sqrt{\ln N \ln\ln N}} = A(e^{\sqrt{\ln N \ln\ln N}})^C = A(L^a)^{2\sqrt{2}C}, \quad (9)$$

де A, C — деякі постійні коефіцієнти. При логарифмуванні правої та лівої частин співвідношення (9) отримаємо

$$\log_2(T(m)) \approx \log_2(A) + C\sqrt{\ln N \ln\ln N} = \log_2(A) + 2\sqrt{2}C\log_2(L^a).$$

Якщо позначити $v_1 = \log_2(A)$, $v_2 = 2\sqrt{2}C$, $a(m) = \log_2(L^a)$, $b(m) = \log_2(T(m))$, то для множини m можна записати рівняння

$$v_1 + a(m)v_2 = b(m), \quad (10)$$

корені якого v_1 та v_2 будуть визначатися за умови мінімального квадратичного відхилення. Для визначення коефіцієнта C (змінна v_2 в (10)) було проведено чисельні експерименти для параметрів *pla* та *kff*, наведених у табл. 8. При розрахунку прийнято *pla* = 1,4, h = 0,7. Результати чисельних експериментів для варіанту 1 наведено у табл. 9.

При формуванні системи лінійних алгебраїчних рівнянь (СЛАР) (10) обчислювалися значення логарифму за основою два для рекомендованого в [9] розміру ФБ:

$$L^a(m) = \exp\left(\frac{\sqrt{2}}{4}\sqrt{\ln N(m)\ln\ln N(m)}\right),$$

де $N(m)$ — числа порядку 10^m при $m = 20 \div 32$. Для значень часу, наведених у табл. 9, також обчислювався логарифм за основою два від отриманого часу розрахунку. При різній кількості лінійних рівнянь з двома та більшою кількістю невідомих у СЛАР (10) можна отримати різні значення коефіцієнта C. Тому для кожного стовпчика табл. 9 формувалися системи рівнянь, починаючи з рядка, що відповідає початковому значенню m_0, до рядка, що відповідає m = 32. При різних значеннях m_0 та *pla* отримано різні значення коефіцієнта C. Серед них обирали те, при якому різниці між даними табл. 9 та розрахунковими значеннями часу постійно змінювали свій знак. Порівнюючи значення C, обирали такі, при яких розрахунко-

Таблиця 8

Варіант	*pla*	*kff*
1	1	0,4—1,0
2	0,95	0,4—0,95
3	0,9	0,4—0,9
4	0,85	0,4—0,85
5	0,8	0,4—0,8

вий час для $m = 32$ менший, C (–), та більший, C (+), за табличне значення. Отримані значення C (–) та C (+) при $pla = 1{,}0$ наведено в табл. 10.

Результати чисельних експериментів для варіанту 2 (див. табл. 8) наведено у табл. 11. Значення C (–) та C (+), отримані на основі даних табл. 11, наведено в табл. 12, а значення C (–) та C (+), для варіантів 3—5 (див. табл. 8) — у табл. 13. Відсутність значень C (–) у табл. 9 та 12 означає, що при різних варіантах формування системи рівнянь (10) не було жодного, в якому прогнозований час розрахунку достатньої кількості B-гладких для чисел порядку 10^{32} перевищував би отримане значення часу. Це свідчить про те, що значення коефіцієнта C, яке використовується при оцінці обчислювальної складності, є більшим за C (+).

Аналізуючи дані, наведені в табл. 9, 11 та 12, приходимо до висновку про те, що коефіцієнт C може мати середнє значення між C (+) та C (–) і бути меншим за одиницю, що підтверджено результатами розрахунків для відносно малих чисел. Узагальнити такий висновок на довільні числа N

Таблиця 9

m	Час розрахунку t (с) при *kff*						
	0,4	0,5	0,6	0,7	0,8	0,9	1
20	1,156	1,079	0,969	0,953	0,969	1,031	1,125
21	1,719	1,578	1,468	1,422	1,468	1,562	1,718
22	2,344	2,125	2,016	2	2,063	2,25	2,5
23	3,405	3,171	3,015	3	3,125	3,37	3,813
24	4,844	4,469	4,328	4,5	4,515	4,906	5,609
25	6,687	7,814	5,969	6,156	6,344	6,906	7,922
26	9,422	8,812	8,64	8,702	9,14	10,047	11,546
27	13,421	12,687	12,614	12,678	13,25	14,765	17,093
28	19,389	18,49	17,921	18,281	19,392	21,859	25,265
29	27,233	25,514	25,171	25,843	27,5	31,435	36,514
30	38,15	36,389	35,811	36,483	39,561	44,722	53,022
31	51,53	50,077	50,092	51,94	55,654	63,353	76,013
32	75,091	71,731	71,937	73,664	80,34	97,621	110,512

Таблиця 10

kff	0,4	0,5	0,6	0,7	0,8	0,9	1,0
C (–)	—	—	—	—	—	—	1,04598
C (+)	0,95765	0,97725	0,995949	0,990047	1,01645	1,07049	1,04163

немає можливості, оскільки його оцінки отримано на основі чисельних експериментів над обмеженою множиною відносно малих чисел. Проте плавний характер зміни *C* (+) і *C* (–) при зміні *kff* та *pla* дозволяє вважати можливим отримання модифікованого методу квадратичного решета, у алгоритмі якого коефіцієнт *C* буде меншим за одиницю. Так, для

Таблиця 11

m	Час розрахунку *t* (с) при *kff*						
	0,4	0,5	0,6	0,7	0,8	0,9	0,95
20	1,781	1,61	1,406	1,375	1,344	1,407	1,484
21	2,641	2,484	2,156	2,188	2,078	2,187	2,297
22	3,656	3,219	2,984	2,906	2,937	3,172	3,315
23	5,516	4,925	4,563	4,5	4,551	4,92	5,234
24	7,905	7,078	6,656	6,656	6,734	7,281	7,765
25	10,891	10,109	9,359	9,577	9,812	10,734	11,531
26	15,64	14,375	13,54	13,901	14,328	15,828	16,972
27	22,39	21,225	19,749	20,39	20,962	23,202	25,202
28	32,561	30,843	28,405	29,026	30,592	34,35	37,686
29	47,123	43,23	41,171	42,03	45,03	51,467	57,042
30	65,029	59,373	58,623	58,748	63,04	71,7	79,528
31	92,685	85,601	83,538	85,341	90,814	105,998	115,653
32	125,293	117,658	114,969	119,825	129,433	149,511	165,775

Таблиця 12

kff	0,4	0,5	0,6	0,7	0,8	0,9	0,95
C (–)	0,957962	0,960859	0,985946	1,00466	1,02279	1,04022	1,05352
C (+)	0,950964	0,958305	0,979411	1,00113	1,01919	1,03619	1,05073

Таблиця 13

Вариант	*C*	Значення *C* (–) та *C* (+) при *kff*						
		0,4	0,5	0,6	0,7	0,8	0,85	0,9
3	*C* (–)	—	—	—	1,07631	1,06094	—	1,06763
	C (+)	1,05159	1,04601	1,05925	1,07416	1,06032	—	1,01483
4	*C* (–)	—	—	—	1,12124	—	1,13575	—
	C (+)	1,01827	1,03077	1,09658	1,10882	1,12937	1,12172	—
5	*C* (–)	1,03691	1,04564	—	1,13696	1,15366	—	—
	C (+)	1,02762	1,04291	1,07915	1,12591	1,15128	—	—

аналізованих чисел N при $pla = 0{,}94$ отримуємо $C(+) = 0{,}989129$, $C(-) = 0{,}99512$. При цьому розмір матриці визначається так:

$$(L^a)^{0,94} = \exp\left(0{,}94\frac{\sqrt{2}}{4}\sqrt{\ln N \ln\ln N}\right),$$

а обчислювальна складність методу Гауса для матриці становить

$$O\left(\exp\left(3\cdot 0{,}94\frac{\sqrt{2}}{4}\sqrt{\ln N \ln\ln N}\right)\right) = O\left(\exp\left(0{,}997021\sqrt{\ln N \ln\ln N}\right)\right).$$

Тобто при використанні методу MQkS в цілому значення C виявляється меншим за одиницю, хоча таку оцінку слід вважати евристичною.

Висновки

В методі QS найбільш затратною за часом є процедура пошуку B-гладких чисел, в ході якої шукають такі пробні X, що для остач $y(X)$ достатньо близькими будуть значення $\log(y(X))$ та $\sum_{j=1}^{pfa} s_j \log p_j$, де p_j — прості числа (елементи ФБ). Оскільки при цьому можливі значення $s_j > 1$, необхідно перевіряти виконання умови $y(X) \bmod (p^{S_j}) = 0$, що спричиняє зростання обчислювальних затрат.

Запропонований спосіб просіювання, заснований на використанні сигнальних остач, потребує пошуку коренів рівняння $y_k(X) \bmod (p^{S_j}) = 0$ тільки при $s_j = 1$. Тоді замість виконання умови практичної рівності значень $\log(y_k(X))$ та $\sum_{j=1}^{pfa} s_j \log p_j$ вимагається виконання умови (4), де $h \in [0,1]$. Цей параметр можна обирати, що дозволяє суттєво скоротити час розрахунку. Подальше скорочення часу розрахунків здійснюється при використанні обмеження (7) для множини елементів загальної ФБ, для яких показники степенів дільників B-гладкого можуть перевищувати одиницю.

Зазначимо, що при використанні розміру ФБ L^a та радіусу просіювання L^b [9] для чисел N порядку 2^{1024} число елементів матриці перевищить $9\cdot 10^{20}$, а кількість пробних X може перевищити $27\cdot 10^{30}$. На даний час такий обсяг пам'яті недоступний для сучасних обчислювальних систем. В найближчому майбутньому проблематичним також є виконання за прийнятний час числа операцій, яке перевищує $27\cdot 10^{30}$. Тому є потреба в зниженні кількості елементів ФБ (для методу MQkS ЗФБ) та інтервалу просіювання. В методі MQkS число елементів ЗФБ визначається на основі

параметра *pla*, а розмір інтервалу просіювання — на основі параметра *plb*. Проте зменшення розміру ФБ призводить до збільшення часу пошуку *B*-гладких. Тому одночасне зменшення *fa* та *fb* практично неможливе.

Для методу QS та його модифікацій обчислювальна складність оцінюється величиною $O\left(\exp\left(C\sqrt{\ln N \ln\ln N}\right)\right)$, де $C \geq 1$. На основі проведених чисельних експериментів встановлено, що при $pla \leq 0{,}94$ та $pla > 0{,}9$ для аналізованої множини чисел, наведеної в табл. 1, коефіцієнт C у формулі (9) менший за одиницю. Проте не можна стверджувати, що це буде спостерігатися для довільних N. В той же час, можна стверджувати, що при використанні ідеї діагоналізації матриці «на ходу» [10] є принципово можливим розкладання чисел N порядку 2^{1024}.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. *Горбенко И.Д., Долгов В.И., Потий А.В., Федорченко В.Н.* Анализ каналов уязвимости системы RSA // Безопасность информации, 1995, № 2, с. 22—26.
2. *Brown Daniel R.L.* Breaking RSA May Be As Difficult As Factoring. [Электронный ресурс]. Режим доступа: http://www.pgpru.com/novosti /2005/1026vzlomrsabezfaktorizaciirealennoneeffektiven. Название с экрана.
3. *Kannan Balasubramanian, M. Rajakani.* Algorithmic strategies for solving complex problems in cryptography // Advances in information security, privacy, and ethics (AISPE) book series. Hershey, Pennsylvania (701 E. Chocolate Avenue, Hershey, Pennsylvania, 17033, USA) : IGI Global, 2018.
4. *Quadratic* sieve. [Электронный ресурс]. Режим доступа: https://en.wikipedia.org/wiki/Quadratic_sieve. Название с экрана.
5. *Silverman R.D.* The multiple polynomial quadratic sieve // Math. Comp., 1987, Vol. 48 (177), p. 329—339.
6. *Винничук С.Д., Місько В.М.* Метод множинного *k*-решета цілочисельної факторизації // Електрон. моделювання, 2018, **40**, № 5, с. 3—26. [Электронный ресурс]. Режим доступа: https://doi.org/10.15407/emodel.40.05.003.
7. *Василенко О.Н.* Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО, 2003, с. 328.
8. *Ишмухаметов Ш.Т.* Методы факторизации натуральных чисел. Казань: Казанский ун-т., 2011, с. 190.
9. *Landquist Eric.* The Quadratic Sieve Factoring Algorithm // MATH: Cryptographic Algorithms, 2001, No. 488, p. 1—11.
10. *Vynnychuck S., Misko V.* Acceleration analysis of the quadratic sieve method based on the online matrix solving // Mathematics and cybernetics — applied aspects, 2018, Vol. 2, No. 4 (92) p. 33—38. DOI: 10.15587/1729-4061.2018.133603.

Отримано 27.02.19

REFERENCES

1. Gorbenko, I.D., Dolgov, V.I., Potiy, A.V. and Fedorchenko, V.N. (1995), "Channel analysis of the RSA system vulnerability", *Bezopansost informasii*, no. 2, pp. 22-26.
2. Brown Daniel, R.L. "Breaking RSA May Be As Difficult As Factoring", available at: http://www.pgpru.com/novosti /2005/1026vzlomrsabezfaktorizaciirealennoneeffektiven.
3. Kannan, B. and Rajakani, M. (2018), "Algorithmic strategies for solving complex problems in cryptography. Advances in information security, privacy, and ethics (AISPE) book series", *IGI Global*, Hershey, Pennsylvania, USA.
4. "Quadratic sieve", available at: https://en.wikipedia.org/wiki/Quadratic_sieve.
5. Silverman, R.D (1987), "The multiple polynomial quadratic sieve", *Math. Comp*, Vol. 48 (177), pp. 329-339.
6. Vynnychuk, S.D. and Misko, V.M. (2018), "Method of multiple quadratic k-sieve integer factorization", *Elektron. modelirovanie*, Vol. 40, no. 5, pp. 3-26, available at: https://doi.org/10.15407/emodel.40.05.003.
7. Vasilenko, O.N. (2003), *Teoretiko-chislovyie algoritmy v kriptografii* [Number-Theoretic Algorithms in Cryptography], MTsNMO, Moscow, Russia.
8. Ishmukhametov, Sh.T. (2011), *Metody faktorizatsii naturalnykh chisel* [Methods of natural numbers factorization], Kasanskiy Universitet, Kasan, Russia.
9. Landquist, E. (2001), "The Quadratic Sieve Factoring Algorithm", *MATH: Cryptographic Algorithms*, no. 488, pp. 1-11.
10. Vynnychuck, S. and Misko, V. (2018), "Acceleration analysis of the quadratic sieve method based on the online matrix solving", *Eastern-European Journal of Eenterprise Technologies / Mathematics and cybernetics*, Vol. 2, no. 4 (92), pp. 33-38, DOI: 10.15587/1729-4061.2018.133603.

Received 27.02.19

С.Д. Винничук, В.Н. Мисько

МЕТОД МНОЖЕСТВЕННОГО КВАДРАТИЧНОГО *k*-РЕШЕТА
С ИСПОЛЬЗОВАНИЕМ СИГНАЛЬНЫХ ОСТАТКОВ
ПРИ ПРОСЕИВАНИИ ПРОБНЫХ ЗНАЧЕНИЙ

Описан алгоритм метода множественного квадратичного *k*-решета, который является модификацией метода квадртатичного решета. В предложенной модификации при просеивании пробных значений рекомендуется выполнять предварительное их просеивание на основе сравнения остатков $y_k(X) = X^2 - kN$ $(k \geq 1)$ с сигнальными остатками $y_k^*(X)$, где $y_k^*(X)$ — произведение первых степеней множителей $y_k(X)$. Из пробных значений отсевают те, для которых $\log(y_k(X)) < h \log(y_k^*(X))$, где действительное число $h \in [0,1]$ — это выбираемый параметр. Установлено, что при возрастании значения N увеличивается и значение h, при котором достигается наименьшее время расчета. Установлено также, что уменьшение времени получения достаточного числа B-гладких можно достичь при ограничении на показатели степеней делителей B-гладкого, превышающих еденицу, для множества элементов общей факторной базы, больших некоторого значения, определяемого на основе параметра *kff*. На основе численных экспериментов с относительно малыми числами порядка 10^m при m = 20÷32 показано, что время рачета достаточного числа B-гладких является функцией введеного параметра *kff*. Описаны шаги алгоритма метода и идеи их реализации. Дана эвристическая оценка сложности предложенного метода для ряда значений параметра *pla*.

К л ю ч е в ы е с л о в а: целочисленная факторизация, метод квадратичного решета, множественное решето.

S.D. Vynnychuk, V.M. Misko

METHOD OF MULTIPLE POLINOMIAL *k*-SIEVE
WITH USING OF SIGNAL REMINDERS
DURING SIEVING OF PROBABLE VALUES

An algorithm for the method of a Multiple Quadratic *k*-Sieve (MQkS) is proposed, which is a modification of the quadratic sieve method (QS), in which, when sieving test values, it is proposed to perform a preliminary sieving on the basis of the comparison, the remainder $y_k(X) = X^2 - kN$ $(k \geq 1)$ with signaling residues $y_k^*(X)$, where $y_k^*(X)$ is the product of the first powers of the factors $y_k(X)$. Among the test values, the ones for which $\log(y_k(X)) < h \log(y_k^*(X))$, where a real number $h \in [0,1]$ is a parameter that can be selected. It is established that at growth N the value of h increases, at which the lowest value of the calculation time is reached. It is also established that a decrease in the time of obtaining a sufficient number of *B*-smooth ones can be obtained by limiting the parameters of powers of the *B*-smooth divisors exceeding the unit for a plurality of elements of a common factor base, greater than a certain value, which is determined on the basis of the value of the parameter *kff*. On the basis of numerical experiments with relatively small numbers of order 10^m at $m = 20 \div 32$, it is shown that the time of calculating a sufficient number of *B*-smooth is a function of the introduced parameter *kff*, with a monotonically increasing ratio of calculation time with the value of the parameter *kff* = 1 (no restriction) to the minimum time. The steps of the algorithm of the method and the ideas of their implementation are described. A heuristic estimation of the complexity of the MQkS method for a number of values of the parameter *pla* is given.

K e y w o r d s: integer factoring, quadratic sieve, multiple sieve.

ВИННИЧУК Степан Дмитрович, д-р техн. наук, зав. відділом Ін-ту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. В 1977 р. закінчив Чернівецький госуніверситет. Область наукових досліджень — моделі, методи і програмні засоби для аналізу систем рідини, що стискається та не стискається, теорія алгоритмів.

МІСЬКО Віталій Миколайович, аспірант Ін-ту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. В 2013 р. закінчив Ін-т спеціального зв'язку і захисту інформації НТУУ «КПІ». Область наукових досліджень — чисельні методи та алгоритми факторизації.