Инженерный вестник Дона, №1 (2018)
ivdon.ru/ru/magazine/archive/n1y2018/4726

Метод переменной окрестности для задачи факторизации целых чисел в сочетании с байесовским подходом

Ю.Ю.Огородников[1], *А.П.Плёнкин*[2]

[1] *Институт математики и механики имени Н.Н.Красовского Уро РАН, Екатеринбург*

[2] *Южный федеральный университет, г.Таганрог*

Аннотация: В статье рассматривается приближённый алгоритм поиска решения задачи факторизации целых чисел путём сведения к оптимизационному варианту задачи выполнимости булевых формул, содержащей в каждом дизъюнкте ровно 3 литерала (MAX-3SAT). Для последней задачи строится непрерывный вещественнозначный функционал, глобальный минимум которого совпадает с решением MAX-3SAT. Показано использование метода простой итерации в сочетании с методом переменной окрестности и байесовским округлением. Изложено, что глобального минимума не всегда удаётся достигнуть из-за наличия на траектории поиска локальных экстремумов, однако точки, соответствующие локальным оптимумам, могут быть проанализированы на предмет совпадения отдельных компонент решения с точным. Приведены результаты численных экспериментов, которые показали, что разработанный гибридный метод определяет верно на 7% бит выполняющего набора больше чем предшествующие разработки авторов. Также представленный метод поиска задачи факторизации рассмотрен с позиции защищенности квантовых каналов связи в системах квантового распределения ключа. Описана типовая структура системы квантового распределения ключа.

Ключевые слова: задача факторизации целых чисел, оптимизационный вариант задачи выполнимости булевых формул (MAX-3SAT), метод переменой окрестности, вещественнозначный функционал представления MAX-3SAT, квантовое распределение ключа.

Введение

Актуальной задачей для современных телекоммуникационных систем является вопрос обеспечения защищенности каналов связи. С появлением первых образцов квантовых компьютеров, надежность существующих криптографических алгоритмов приобретает вероятностный характер. Проблема надежности при шифровании сообщений сводится к проблеме распределения секретного ключа между корреспондентами. Эту проблему решает квантовая криптография, принципы которой реализуются в системах квантового распределения ключа (КРК). Уже созданы действующие коммерческие образцы систем квантового распределения ключа. Напомним, что система квантового распределения ключа состоит из двух станций,

которые соединены между собой волоконно-оптической линией связи. Распределение квантового ключа обеспечивается посредством кодирования фазового состояния фотона.

Разработки и исследования в данной области ведутся многими мировыми лабораториями, однако только несколько компаний реализуют готовую продукцию. Устойчивой работоспособностью при изменяющихся внешних условиях выделяются системы квантового распределения ключа с фазовым кодированием состояний фотонов [1-5]. Такие системы работают по схеме с автоматической компенсацией поляризационных искажений. В системах КРК применяются симметричные методы шифрования [6, 7]. Однако, в силу несовершенства систем квантовой связи, зачастую используются гибридные сочетания методов шифрования. Последнее показывает, что поиск новых методов и алгоритмов, направленных на усиление задач факторизации является актуальной задачей. Рассмотрим подробнее суть данной задачи и пути её решения.

Задача факторизации целых чисел (англ. Integer Factorization Problem, IFP) - одна из наиболее важных и интересных задач в дискретной математике [8]. Несмотря на то, что близкая ей задача проверки числа на простоту полиномиально разрешима [9], вычислительный статус IFP до сих пор не определён. Пользуясь этим обстоятельством, задача IFP активно используется в различных криптографических протоколах, самым распространённым из которых является алгоритм асимметричного шифрования RSA [10]. Современными методами (в частности, общим методом решета числового поля) удалось получить за полиномиальное время разложения чисел, содержащих в двоичной записи до 768 бит включительно [11]. Тем не менее, дальнейшее повышение размерности существенно повышает трудоёмкость операции декомпозиции составного числа. В связи с этим разрабатываются иные подходы к решению задачи

факторизации целых чисел. Одним из таких является сведение IFP к хорошо известной NP-трудной задаче 3-SAT.

Приведём её формулировку.

Пусть дана булева формула, представленная в виде КНФ

$$L(y) = \wedge_{i=1}^{m} C_i \quad (1)$$

где C_i – элементарные дизъюнкции вида

$$y_{j1}^{\sigma 1} \vee \ldots \vee y_{jk}^{\sigma k}$$

$1 \le k \le n, \sigma_j \in \{0,1\}, y^1 = y, y^0 = \bar{y}$

Задача заключается в следующем: можно ли назначить переменным $y_1,\ldots,y_n$ значения *true* и *false* так, чтобы формула (1) приняла значение *true*?

Алгоритм полиномиального сведения IFP к 3-SAT, основанный на представлении в терминах булевой алгебры операции умножения двух чисел “столбиком”, описан в работах [12, 13]. Получаемый экземпляр 3-SAT содержит единственный выполняющий набор. Таким образом, если удастся найти заданный выполняющий набор, то решение исходной задачи IFP можно будет также восстановить. Более того, алгоритм сведения IFP к 3-SAT устроен так, что для каждого бита выполняющего набора известен его смысл в схеме кодирования операции умножения “столбиком”. Получается, что отдельно можно выделить биты сомножителей, биты промежуточных сумм и биты переносов, и для исходной задачи IFP значимыми будут являться, вообще говоря, лишь биты сомножителей.

К сожалению, в настоящее время не известно полного (т.е. находящего выполняющий набор в любом случае) полиномиального алгоритма для задачи 3-SAT. Однако, в силу того что для задачи IFP важны лишь биты, отвечающие за сомножители, представляет интерес использование оптимизационного варианта 3-SAT, который носит название MAX-3SAT. Суть MAX-3SAT заключается в максимизации числа выполнимых дизъюнктов (или, что то же самое, минимизации числа невыполнимых).

Очевидно, что наилучшее решение MAX-3SAT (все дизъюнкты выполнены) является также решением для 3-SAT. Таким образом, встаёт вопрос о поиске приближённого решения MAX-3SAT.

Для данных целей предлагается использовать непрерывную модель задачи 3-SAT, которая носит название UniSAT7 [14]. Приведём её описание.

Пусть имеется непрерывная вещественнозначная гладкая функция *F(x):*

$$F(x) = \sum_{i=1}^{m} P_i(x), \tag{2}$$

где $P_i(x) = \prod_{j=1}^{n} p_{ij}(x), p_{ij}(x) = \begin{cases} x_j^2, \text{если } \bar{y} \text{ содержится в } C_i \\ (1-x_j)^2, \text{если } y_j \text{ содержится в } C_i \\ 1, \text{иначе} \end{cases}$.

В работе [15] показано, что глобальный минимум данной функции соответствует искомому выполняющему набору.

Для нахождения глобального минимума дифференцируем функцию *F(x)* по каждой переменной и приравняем каждую к нулю.

$$\frac{\partial F(x)}{\partial x_i} = 0, \quad (i = 1..n) \tag{3}$$

Рассмотрим систему (3). После дифференцирования функции по (2) по i-й переменной производные членов $P_j = \prod_{k=1}^{3} x_k^2$, не содержащих x_i, обращаются в 0, поэтому уравнения (3) могут быть представлены в виде

$$2x_i \sum_{j=1}^{m} R_{ij}(x) - 2(1-x_i) \sum_{j=1}^{m} \overline{R}_{ij}(x) = 0 \quad (i = 1..n), \tag{4}$$

где $R_{ij}(x) = P_j(x)/x_i^2$, $\overline{R}_{ij}(x) = P_j(x)/(1-x_i)^2$.

Применим к системе (4) метод простой итерации [14] (англ. Simple Iteration Method, SIM)

$$\Phi_i(x) = \sum_{j=1}^{m} \overline{R}_{ij}(x) \Big/ \left(\sum_{j=1}^{m} R_{ij}(x) + \sum_{j=1}^{m} \overline{R}_{ij}(x) + \alpha \right) \tag{5}$$

В формуле (5) α - коэффициент регуляризации, экспериментально установлен в 0.5.

Для итераций будем использовать метод Зейделя $x_i^{(k+1)} = \Phi_i(x_1^{(k+1)}, x_2^{(k+1)} \ldots x_{i-1}^{(k+1)}, x_i^{(k)} \ldots x_n^{(k)})$ с условием остановки $\max\limits_{i=1..n} | x_i^{(k+1)} - x_i^{(k)} | < \varepsilon$.

К сожалению, метод простой итерации далеко не всегда находит глобальный минимум из-за наличия на траектории поиска локальных экстремумов. Тем не менее, можно попытаться преодолеть локальный экстремум. Для этого предлагается использовать метод переменных окрестностей (англ. Variable Neighborhood Search, VNS), предложеннный Младеновичем и Хансеным в 1997 году [16].

Главной идеей, лежащей в основе VNS, является то, что точка $x^{(l)}$, являющаяся экстремумом в некоторой окрестности, совершенно необязательно будет являться экстремумом в большей окрестности. В общей схеме метода предлагается использовать заранее заданный список окрестностей $N_1(x) \subset N_2(x) \ldots \subset N_{kmax}(x)$ с определённой структурой. При попадании в локальный экстремум следует начать перебор окрестностей до тех пор, пока в очередной окрестности $N_j(x)$ точка $x^{(l)}$ экстремумом являться не будет. После этого следует продолжить поиск.

В применении к задаче 3-SAT воспользуемся схемой построения окрестностей, предложенной в работах [16, 17] для задачи MAX-SAT.

Обозначим через $N_0(\tilde{x})$ окрестность решения целочисленной точки $\tilde{x}$ с координатами 1 и 0. Все точки $N_0(\tilde{x})$ получаются инвертированием одной переменной, входящей в $\tilde{x}$ (под инвертированием понимается изменение значения $\tilde{x}_i$ на противоположное).

Точки окрестности $N_1(\tilde{x})$ получаются слиянием переменных, входящих в формулу (1), с помощью рандомизированного алгоритма. Так, если переменная l_i ещё не просмотрена, то случайным образом выбирается другая непросмотренная переменная l_j, и создаётся новая переменная l_k (в дальнейшем называемая кластером), состоящая из l_i и l_j. При этом если

происходит назначение кластеру l_k значений 1 и 0, то это означает, что происходит назначение соответствующих значений 1 и 0 входящим в него переменным l_i и l_j.

Таким образом окрестность $N_1(\bar{x})$ состоит из точек, полученных инвертированием кластеров, каждый из которых содержит 2 переменные. Дальнейшие окрестности $N_i(\bar{x}), i = 2..kmax$ получаются слиянием кластеров, использованных в предыдущих окрестностях $N_{i-1}(\bar{x})$ по вышеописанной схеме. Если же кластеров нечётное количество, то один из новых сформированных кластеров будет содержать 3 кластера с предыдущей окрестности.

Данный процесс повторяется до тех пор, пока не будет достигнуто максимальное значение числа окрестностей kmax. В работе [17] рекомендовано выбирать kmax так, что число формируемых кластеров равняется 10% от размерности задачи. Так, если число переменных равняется 100, то получается 4 окрестности и kmax=3 (100 переменных в окрестности $N_0(\bar{x})$, 50 в $N_1(\bar{x})$, 25 в $N_2(\bar{x})$ и 13 в $N_3(\bar{x})$ (в последнем случае число 12,5 округляется в большую сторону).

Опишем алгоритм поиска приближённого решения $\bar{x}$ для функции (2).

Алгоритм 1. Метод простой итерации в сочетании с методом переменных окрестностей (SIM + VNS).

Вход: Булева формула в виде 3-КНФ.

Шаг 1. Произвести переход от булевой формулы (1) к задаче минимизации непрерывного вещественнозначного функционала F(x) (2).

Шаг 2. Задать структуру окрестностей $N_i(\bar{x}), i = 1..kmax$.

Шаг 3. Задать стартовое приближение $x^{(0)} \in [0,1]^n$.

Шаг 4. Выполнять итерирование до попадания в локальный экстремум. Зафиксировать точку $x^{(l)}$, соответствующую локальному оптимуму $F(x^{(l)})$.

Шаг 5. Преобразовать $x^{(l)}$ в точку с целочисленными координатами $y^{(l)}$ по правилу $y_i^{(l)} = \begin{cases} 1, \text{если } x_i^{(l)} \geq 0.5 \\ 0, \text{иначе} \end{cases}$

Шаг 6. Положить k=1.

Шаг 7. Выбрать точки $z_k \in N_k\left(y^{(l)}\right), k = 1 \ldots |N_k\left(y^{(l)}\right)|$ и посчитать для каждой из них значение $F(z_k)$. Если $F(z_k) < F(x^{(l)})$, то положить $x^{(0)} = z_k$ и перейти к шагу 4. Если такой точки не нашлось, то положить k=k+1.

Шаг 8. Если k=kmax, то прекратить выполнение алгоритма и выдать ответ: $\tilde{x} = x^{(l)}$.

Выход. Приближённое решение $\tilde{x}$.

Конец алгоритма 1.

К сожалению, даже с применением эвристики VNS метод простой итерации не находит точное решение, однако позволяет ближе подобраться к глобальному оптимуму. Кроме того, данный метод можно сочетать с разыми другими эвристиками.

Применим к методу SIM + VNS модифицированную схему округления с использованием формулы Байеса, описанную в статье [18]. Для этого введём два события H_i^0 и H_i^1, заключающиеся в округлении $\tilde{x}_i$ в 0 и в 1 на l-й итерации, соответствующей локальному экстремуму (после применения SIM+VNS), и положим $P\left(H_i^0\right) = 0.5$ и $P(H_i^1) = 0.5$. Введём далее условные вероятности $P(A|H_i^0)$ и $P(A|H_i^1)$. Нетрудно показать, что $P(A|H_i^0)$ и $P(A|H_i^1)$ равны $P([y_i^* = 0])$ и $P([y_i^* = 1])$ по построению (здесь и далее y^* обозначает эталонное решение).

Полная вероятность события A_i вычисляется по хорошо известной формуле $P(A_i) = P\left(H_i^0\right)P\left(A_i|H_i^0\right) + P(H_i^1)P(A_i|H_i^1)$.

Далее, вычисляются две апостериорные вероятности

$$P(H_i^0 \mid A_i) = \frac{P(H_i^0)P(A_i \mid H_i^0)}{P(A_i)}, P(H_i^1 \mid A_i) = \frac{P(H_i^1)P(A_i \mid H_i^1)}{P(A_i)}, \quad (6)$$

и совершается округление вещественного вектора $\tilde{x}$ в целочисленный $\tilde{y}$ по формуле

$$\tilde{y}_i = \begin{cases} 0, \text{если } P(H_i^0|A_i) \geq P(H_i^1|A_i) \\ 1, \text{иначе} \end{cases} \quad (7)$$

Округление по формуле (7) будем проводить в конце работы алгоритма 1. Полученный комбинированный метод назовём SIM+VNS+Bayesian (по задействованным в нём компонентам).

Исследуем статистически, насколько хорошо определяет SIM+VNS+Bayesian биты выполняющего набора. Для этого проведём серию экспериментов множестве экземпляров $U = \{I_1, \ldots, I_d\}$ размера d . Пусть $y^*(I)$ точное решение для экземпляра I, а $\hat{y}(I)$ – приближение, полученное в результате выполнения алгоритма SIM+VNS+Bayesian. Введём функцию потерь $L(\hat{y}(I), y^*(I)) = \frac{1}{n} \| \hat{y}(I) - y^*(I) \|_1$. Тогда функционал качества примет вид

$$\overline{L} = \frac{1}{d} \sum_{j=1}^{d} L(\hat{y}(I_j), y^*(I_j)) \quad (8)$$

Аналогично, введём функции потерь $L^0(\hat{y}(I), y^*(I)) = \frac{|\{i : \hat{y}_i(I) = 1 \text{ and } y_i^*(I) = 0\}|}{|\{i : y_i^*(I) = 0\}|}$, $L^1(\hat{y}(I), y^*(I)) = \frac{|\{i : \hat{y}_i(I) = 0 \text{ and } y_i^*(I) = 1\}|}{|\{i : y_i^*(I) = 1\}|}$, и с их помощью определим функционалы качества $\overline{L^0} = \frac{1}{d} \sum_{j=1}^{d} L^0(\hat{y}(I_j), y^*(I_j))$, и $\overline{L^1} = \frac{1}{d} \sum_{j=1}^{d} L^1(\hat{y}(I_j), y^*(I_j))$ для единичных и нулевых бит соответственно.

Для оценки точности алгоритма будем использовать кросс-валидацию. Для этих целей будем использовать обучающую выборку размера n_ed=999 и контрольную выборку размера n_control=1 (сумма размеров контрольной и обучающей выборки равняется 1000 - именно столько экземпляров было использовано при тестировании).

Для упрощения дальнейшего изложения приведём в таблице 1 соотношение размерностей исходной задачи (размер факторизуемого числа, обозначен через *k*), числа переменных в эквивалентной 3-КНФ (обозначен *n*) и число дизъюнктов *m* в 3-КНФ.

Таблица №1

Размеры экземпляров задачи IFP

k	64	100	200	300	400	500	600	1024
n	5952	14700	59400	134100	238800	373500	538200	1569792
m	23424	58200	236400	534600	952800	1491002	2149200	6273026

В дальнейших таблицах будет представлен только параметр *n*.

Здесь и далее во всех экспериментах для всех вычисленных данных приведены нижние и верхние границы с уровнем доверия 90%. Оценка уровня доверия проводилась следующим образом: считались доли верно определённых нулевых и единичных бит на контрольной выборке, затем подобная операция проводилась для всех контрольных выборок (всего 1000 экземпляров), затем полученные данные сортировались по возрастанию, и находилось то значение, для которого 90% данных оказывались больше него.

В таблице 2 приведены данные по сравнению частот верно определённых бит алгоритмом SIM+VNS+Bayesian (SVB) и методом простой итерации в сочетании с байесовским округлением, описанным в статье [18] (обозначения далее SIM+Bayesian и SB).

Таблица 2

Сравнение частот верно определённых бит методами SB и SVB

n	$\overline{L^0}$		$\overline{L^1}$		$\overline{L}$	
	SB	SVB	SB	SVB	SB	SVB
5952	(0.13;0.36)	(0.09;0.28)	(0.08;0.23)	(0.05;0.19)	(0.11;0.3)	(0.07;0.24)
14700	(0.14;0.38)	(0.11;0.34)	(0.11;0.25)	(0.09;0.21)	(0.13;0.31)	(0.1;0.27)
59400	(0.13;0.38)	(0.09;0.33)	(0.1;0.24)	(0.06;0.19)	(0.125;0.31)	(0.08;0.25)

134100	(0.12;0.39)	(0.07;0.33)	(0.14;0.27)	(0.11;0.22)	(0.15;0.335)	(0.09;0.28)
238800	(0.14;0.41)	(0.1;0.36)	(0.15;0.28)	(0.08;0.23)	(0.155;0.33)	(0.06;0.3)
373500	(0.17;0.4)	(0.12;0.25)	(0.15;0.27)	(0.09;0.22)	(0.18;0.33)	(0.11;0.23)
538200	(0.18;0.4)	(0.13;0.29)	(0.16;0.27)	(0.19;0.33)	(0.18;0.33)	(0.15;0.31)
1569792	(0.17;0.4)	(0.12;0.27)	(0.16;0.27)	(0.13;0.22)	(0.17;0.32)	(0.12;0.24)

Как может быть видно из содержимого таблицы 2, метод SIM+VNS+Bayesian превосходит SIM+Bayesian.

В таблице 3 приведено сравнение расстояний Хэмминга и времени вычисления двух рассматриваемых методов.

Таблица 3

Сравнение расстояний Хэмминга и времени выполнения методов SB и SVB

n	Расстояние Хэмминга		Время выполнения	
	SB	SVB	SB (hh:mm:ss)	SVB (hh:mm:ss)
5952	(654;1763)	(562;1544)	3:43	8:25
14700	(1911;4502)	(1686;4085)	8:15	22:07
59400	(7722;17998)	(6975;16865)	15:35	48:36
134100	(17433;43448)	(15706;41260)	42:15	1:32:13
238800	(35820;80833)	(31705;75847)	59:16	2:30:05
373500	(59760;22694)	(52306;104725)	1:12:47	3:44:56
538200	(96876;176798)	(91605;172540)	1:48:02	4:50:05
1569792	(282562;511360)	(273564;503104)	2:17:47	6:27:10

Как видно из данных таблицы 3, приближения, получаемые методом SIM+VNS+Bayesian в среднем оказываются ближе к точному, нежели определяемые SIM+Bayesian.

Таким образом можно говорить об эффективности описанного приближённого алгоритма поиска решения задачи факторизации целых чисел путём сведения к оптимизационному варианту задачи выполнимости булевых формул, содержащей в каждом дизъюнкте ровно 3 литерала (MAX-3SAT). Показано, что для такой задачи строится непрерывный веществennозначный фукционал, глобальный минимум которого совпадает с решением MAX-3SAT. Приведено использование метода простой итерации в сочетании с методом переменной окрестности и байесовским округлением.

Видно, что глобального минимума не всегда удаётся достигнуть из-за наличия на траектории поиска локальных экстремумов, однако точки, соответствующие локальным оптимумам, могут быть проанализированы на предмет совпадения отдельных компонент решения с точным. Приведены результаты численных экспериментов, которые показали, что разработанный гибридный метод определяет верно на 7% бит выполняющего набора больше чем предшествующие разработки авторов. Рассмотрены вопросы применения алгоритма поиска задачи факторизации с позиции защищенности квантовых каналов связи в системах квантового распределения ключа. Показано, что разработанный метод может быть применен в системах квантовой связи для оценки защищенности последних.

Благодарности

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 17-32-50001\17 мол_нр.

Литература

1. Румянцев К.Е., Плёнкин А.П. Повышение эффективности алгоритма вхождения в синхронизм системы квантового распределения ключей. Известия ЮФУ. Технические науки. 2015. Т. 8, № 169. С. 6–19.

2. Румянцев К.Е., Плёнкин А.П. Синхронизация системы квантового распределения ключа в режиме однофотонной регистрации импульсов для повышения защищенности. Радиотехника. 2015. Т. №2. С. 125–134.

3. Pljonkin A., Rumyantsev K. Single-photon synchronization mode of quantum key distribution system. International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT). India, New Delhi. 2016. pp. 531–534. DOI: 10.1109/ICCTICT.2016.7514637. WOS: 000389774600096. IDS: BG5UT.

4. Rumyantsev K. E.; Pljonkin A. P. Preliminary Stage Synchronization Algorithm of Auto-compensation Quantum Key Distribution System with an Unauthorized Access Security. International Conference on Electronics, Information, and Communications (ICEIC). 2016. Vietnam, Danang. pp. 1–4. DOI: 10.1109/ELINFOCOM.2016.7562955. WOS: 000389518100035. IDS: BG5KP.

5. Pljonkin A., Rumyantsev K. Quantum-cryptographic network. East-West Design & Test Symposium (EWDTS), 2016 IEEE. Electronic ISSN: 2472-761X. DOI: 10.1109/EWDTS.2016.7807623. ISBN: 978-150900693-9.

6. Плёнкин, А.П. Симметричное шифрование квантовыми ключами. Инженерный вестник Дона, 2016, №3. URL: ivdon.ru/ru/magazine/archive/n3y2016/3705

7. Зикий, А.Н., Плёнкин, А.П. Смеситель дециметрового диапазона на комбинации линий передачи. Инженерный вестник Дона, 2016, №3. URL: ivdon.ru/ru/magazine/archive/n3y2016/3701

8. Crandall, R.: Pomerance, C.: Prime Numbers: A Computational Perspective. Chapter 5: Exponential Factoring Algorithms. Springer-Verlag New York, 2nd edition (2005), pp. 2-6.

9. A Generalized Prime Factor FFT Algorithm for any $N = 2^p 3^q 5^r$. SIAM Journal on Scientific and Statistical Computing, 13(3), 676-686 (1992).

10. RSA laboratories - The RSA Challenge Factoring FAQ. URL: emc.com/emc-plus/rsa-labs/historical/the-rsa-factoring-challenge-faq.htm.

11. The factorization, found using the Number Fiels Sieve (NFS). URL: documents.epfl.ch/users/l/le/lenstra/public/papers/rsa768.txt (date of access: 25.12.2017).

12. Дулькейт В.И. Сведение задач факторизации, дискретного логарифмирования и логарифмирования на эллиптической кривой к

решению ассоциированных задач «ВЫПОЛНИМОСТЬ». Компьютерная оптика. – 2010. – Т.34(1). – С. 118-123.

13.Дулькейт В.И., Файзуллин Р.Т., Хныкин И.Г. Непрерывные аппроксимации решения задачи «ВЫПОЛНИМОСТЬ» применительно к криптографическому анализу асимметричных шифров // Компьютерная оптика. – 2009. – Т. 33 (1). – С. 86-91.

14. Gu, J., Purdom, P.W., Franco, J., Wah, B.W.: Algorithms for the Satisfiability Problem. Cambridge University Press (1999), pp. - 12-53.

15. Mladenovic Nenad, Hansen Pierre (1997). "Variable neighborhood search". Computers and Operations Research. 24 (11), pp. - 1097–1100.

16. Bouhmala N. A Variable Neighborhood Walksat-Based Algorithm for MAX-SAT Problems. The Scientific World Journal, V. 2014, 11p., doi:10.1155/2014/798323.

17. Bouhmala N., Overgard K.I. Combining Genetic Algorithm with Variable Neighborhood Search for MAX-SAT. Innovative Computing, Optimization and Its Applications, pp.73-92. doi: 10.1007/978-3-319-66984-7_5.

18. Khachay M., Ogorodnikov Y. Combining Fixed-point Iteration Method and Bayesian Rounding for Approximation of Integer Factorization Problem // 2nd International Conference on Artificial Intelligence: Techniques and Applications (AITA 2017). September 17-18, 2017, Shenzhen, China, pp. 1-6.

Gratitude

The study was carried out with the financial support of the Russian Foundation for Basic Research in the framework of the scientific project No. 17-32-50001 \ 17 mol_nr.

References

1. Rumjancev K.E., Pljonkin A.P. Izvestija JuFU. Tehnicheskie nauki. 2015. T. 8, № 169. pp. 6–19.

2. Rumjancev K.E., Pljonkin A.P. Radiotehnika. 2015. T. №2. pp. 125–134.

3. Pljonkin A., Rumyantsev K. Single-photon synchronization mode of quantum key distribution system. International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT). India, New Delhi. 2016. pp. 531–534. DOI: 10.1109/ICCTICT.2016.7514637. WOS: 000389774600096. IDS: BG5UT.

4. Rumyantsev K. E.; Pljonkin A. P. Preliminary Stage Synchronization Algorithm of Auto-compensation Quantum Key Distribution System with an Unauthorized Access Security. International Conference on Electronics, Information, and Communications (ICEIC). 2016. Vietnam, Danang. pp. 1–4. DOI: 10.1109/ELINFOCOM.2016.7562955. WOS: 000389518100035. IDS: BG5KP.

5. Pljonkin A., Rumyantsev K. Quantum-cryptographic network. East-West Design & Test Symposium (EWDTS), 2016 IEEE. Electronic ISSN: 2472-761X. DOI: 10.1109/EWDTS.2016.7807623. ISBN: 978-150900693-9.

6. Pljonkin, A.P. Inženernyj vestnik Dona (Rus), 2016, №3. URL: ivdon.ru/ru/magazine/archive/n3y2016/3705

7. Zikij, A.N., Pljonkin, A.P. Inženernyj vestnik Dona (Rus), 2016, №3. URL: ivdon.ru/ru/magazine/archive/n3y2016/3701

8. Crandall, R., Pomerance, C.: Prime Numbers: A Computational Perspective. Chapter 5: Exponential Factoring Algorithms. Springer-Verlag New York, 2nd edition (2005). pp. 2-6.

9. A Generalized Prime Factor FFT Algorithm for any $N = 2^p 3^q 5^r$. SIAM Journal on Scientific and Statistical Computing, 13(3), pp. - 676-686 (1992).

10. RSA laboratories - The RSA Challenge Factoring FAQ. URL: emc.com/emc-plus/rsa-labs/historical/the-rsa-factoring-challenge-faq.htm.

11. The factorization, found using the Number Fiels Sieve (NFS). URL: documents.epfl.ch/users/l/le/lenstra/public/papers/rsa768.txt (date of access: 25.12.2017).

12. Dulkeyt V.I. Komp'juternaja optika. 2010. T.34 (1). pp. 118-123.

13. Dulkeyt V.I., Faizullin R.T., Khnykin I.G. Komp'juternaja optika. 2009. T. 33 (1). pp. 86-91.

14. Gu, J., Purdom, P.W., Franco, J., Wah, B.W.: Algorithms for the Satisfiability Problem. Cambridge University Press (1999), pp. 12-53.

15. Mladenovic Nenad, Hansen Pierre (1997). "Variable neighborhood search". Computers and Operations Research. 24 (11), pp. 1097–1100.

16. Bouhmala N. A Variable Neighborhood Walksat-Based Algorithm for MAX-SAT Problems. The Scientific World Journal, V. 2014, 11p., doi:10.1155/2014/798323.

17. Bouhmala N., Overgard K.I. Combining Genetic Algorithm with Variable Neighborhood Search for MAX-SAT. Innovative Computing, Optimization and Its Applications, pp.73-92. doi: 10.1007/978-3-319-66984-7_5.

18. Khachay M., Ogorodnikov Y. 2nd International Conference on Artificial Intelligence: Techniques and Applications (AITA 2017). September 17-18, 2017, Shenzhen, China, pp. 1-6.