

UDK 519.71

KVANT PARALELLASHTIRISHDA KVANT ALGORITMLARNI OPTIMALLASHTIRISH USULLARI

Toirov Sh.A.¹, Kudratov R.B.¹, Xamdamov F.B.², Xonimqulov J. B.¹

¹ Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Samarqand filiali, Samarqand, O'zbekiston

² Samarqand viloyati hokimligi huzuridagi fuqarolarning o'zini o'zi boshqarish organlari xodimlarining malakasini oshirish o'quv kursi, Samarqand, O'zbekiston
tshuxrat@mail.ru, firuz-0405@mail.ru, rustamkudratov4@gmail.com

Annotatsiya. Ushbu maqolada kvant algoritmlarni yechishda qo'llaniladigan QCL (quantum computation language), uning operatorlari va Deutsch algoritmi orqali yechish prinsiplari keltirib o'tilgan. Kvant jarayonlarning asosiy tamoyillari, fizikaviy va algoritmik talqinlari hisobga olingan. Ushbu jarayonlar tizimli tahlil qilishda global optimallashtirish muammolariga samarali yechimlarni qidirishda va kutilmagan holatlarni oqilona boshqarishda qo'llaniladigan algoritmlarning tasniflari keltirilib o'tilgan.

Kalit so'zlar: kvant, genetik va immun algoritmlar, qcl (quantum computation language), global optimallashtirish, intellektual boshqarish.

I. KIRISH

Global (umumiy holda ko'pmezonli) optimallashtirish masalasining yechimini qidirish tizimli tahlil uchun odatiy hisoblanadi. Axborotning noaniqligi va xatarli (riskli) shartlarda optimal yechimlarni qabul qilish va murakkab tizimlarni boshqarish har xil yo'nalishlarda ko'p yillardan buyon rivojlanib kelmoqda. So'nggi yillarda mazkur masalaning yechimi intellektual hisoblashlarning yangi ko'rinishlari bilan muvaffaqiyatli topilmoqda.

Kvant algoritmlarning yordami bilan yechimni topish uchun, daslabki holatni daslabki superpozitsiya maqsadiga muvofiq ravishda o'zgartirib, kvant operatorlarini ketma-ket ko'rsatilgan turlari qo'llaniladi.

Odatdagi an'anaviy dasturlashda bir parametrlilik funksiya quyidagicha amalga oshiriladi:

• parametr kiruvchi registrga joylashtiriladi;

• funksiya tanasini tashkil etuvchi komandalar bu parametr ustida biror manipulyatsiyalar (o'zgartirishlar) amalga oshiradi, so'ngra natija chiqish registriga joylashtiriladi, bunda parametrning ilgarigi holati yo'qotiladi.

Kvantli dasturlashda esa so'nggi amal (operatsiya) imkonsiz, chunki bu amal qaytarilmasdir. Buning o'rniga natijalar bitlari chiquvchi registrlarning (\oplus) 2 modul bo'yicha bo'linishi natijasiga qo'shiladi. Boshqacha aytganda, ular ustida XOR (istisnoli yoki) amali bajariladi. Bu amal, aniqki, qaytariluvchi: uni ikkinchi marta qo'llash yetarli va xotira boshlang'ich holatiga qaytadi [1].

II. ASOSIY QISM

Kvant paralellashtirish kvant hisoblashning asosiy xususiyatlaridan biri hisoblanadi. Bu xususiyat kvantli kompyuterlarga f ning turli qiymatlari uchun $f(x)$ funksiyasini bir vaqtning o'zida hisoblash imkonini beradi. Kvant paralellizmini tasvirlash uchun x

o'zgaruvchisining funksiyasini hisoblashni ko'rib chiqamiz va u quyidagi ko'rinishda tasvirlanadi.

$$f(x) : \{0, 1\} \rightarrow \{0, 1\}. \quad (1)$$

Kvant kompyuterda bu funksiyani hisoblashning maqbul usuli - ikki qubitli kvantli kompyuterni ko'rib chiqishdan iborat va u $|xy\rangle$ holat bilan ishlaydi. Mantiqiy eshiklar ketma-ketligini qo'llash orqali, boshlang'ich $|xy\rangle$ holatni $|x, y \otimes f(x)\rangle$ holatga o'zgartirishi mumkin. Bu yerda x, y - kvant kompyuterining registrlari deb ayta olamiz. Bunday holatda, birinchi registr ma'lumotlar registri deb ataladi va ikkinchisi - nishon (metka) registr. Bu yerda $|x, y\rangle \rightarrow |x, y \otimes f(x)\rangle$ o'zgaruvchilarni U unitar o'zgaruvchi orqali amalga oshiriladi.

Ularning har biri unitar operator bilan bog'liq. Ya'ni $Uf|x, y\rangle = |x, y \oplus f(x)\rangle$.

Bunday holatlarda funksiya to'rtta holatda bo'ladi: ya'ni $f(x) = 0$ va $f(x) = 1$ bo'lgan holatlarda $f(x)$ funksiya doimiy, $f(x) = x$ va $f(x) = 1 - x$ bo'lgan holatlarda $f(x)$ funksiya muvozanatlashgan bo'ladi (chunki 0 va 1 qiymatlarini teng sonli nuqtalarda oladi) [4].

Bu masalani yechishda $f(0) \otimes f(1)$ ikki modul bo'yicha ko'paytmasi qaraladi. Bu jarayonni hisoblash uchun $|x\rangle = \frac{(|0\rangle + |1\rangle)}{\sqrt{2}}$ (1) ni $f(0)=0$ va $f(1)=1$ bo'lgan holatda yechimlarini topish yetarlidir. U holda, agar $x=0$ va $x=1$ bo'lganda (1) ning ko'rinishi quyidagicha $\frac{(|00\rangle - |01\rangle)}{\sqrt{2}}$ va $\frac{(|10\rangle - |11\rangle)}{\sqrt{2}}$ bo'ladi.

Agar $f(0)=1$ va $f(1)=1$ bo'lgan holatda esa, $x=0$ va $x=1$ bo'lganda (1) ning ko'rinishi quyidagicha $| - 1 \rangle = \frac{(|00\rangle - |01\rangle)}{\sqrt{2}}$ va $| - 1 \rangle = \frac{(|10\rangle + |11\rangle)}{\sqrt{2}}$ bo'ladi.

Yuqoridagi ikki holatni Uf unitar o'zgaruvchi orqali quyidagicha yozish mumkin

$$U_f \left[|x\rangle = \frac{(|0\rangle - |1\rangle)}{\sqrt{2}} \right] = (-1)^{f(x)} |x\rangle = \frac{(|0\rangle - |1\rangle)}{\sqrt{2}} \quad (2)$$

bu yerda $| - \rangle = \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$ belgilashni kiritamiz. Endi dastlabki holatni ko'rib chiqamiz ya'ni $|+\rangle * | - \rangle$. U holda $|\psi\rangle = \frac{(|0\rangle)}{2} | - \rangle + \frac{(|1\rangle)}{2} | - \rangle$ teng bo'ladi. Endi $Uf|\psi\rangle$ unitar o'zgaruvchini hisoblasak, u quyidagicha bo'ladi [3].

$$U_f |\psi_1\rangle = (-1)^{f(0)} \frac{(|0\rangle)}{2} | - \rangle + (-1)^{f(1)} \frac{(|1\rangle)}{2} | - \rangle \quad (3)$$

(3) formuladan ko'rinib turibdiki, agar $f(x)$ funksiya doimiy bo'ladi, qachonki $(-1)^{f(1)} = (-1)^{f(0)}$ bo'lsa, va natija $(-1)^{f(0)} | + \rangle \otimes | - \rangle$ bo'lganda. Agar $f(x)$ funksiya muvozanatlashgan bo'ladi, qachonki $(-1)^{f(1)} = -(-1)^{f(0)}$ bo'lsa, va natija $(-1)^{f(0)} | - \rangle \otimes | - \rangle$ bo'lganda [2].

Yuqoridagilardan ko'rinib turibdiki M ni birinchi bitga qo'llaganda. Doimiy funksiya uchun $|0\rangle$ va muvozanatlashgan funksiya uchun $|1\rangle$ bo'ladi.

Endi yuqorida ko'rib chiqqan funksiyani QCL Quantum Computation Language dasturlash tili yordamida ko'rib chiqamiz.

Kerakli tavsiflar:

$qcl > qureg x[1]; qureg y[1]; int r;$

Uf operatorini yozib chiqamiz:

- $n = 0$ - uchun $f(x) = 0$ (bu operator hech narsa bajarmaydi);
- $n = 1$ - uchun $f(x) = 1$ bo'lsin;
- $n = 2$ - uchun $f(x) = x$ bo'lsin;
- $n = 3$ - uchun $f(x) = 1 - x$ bo'lsin.

Endi QCL Quantum Computation Language dasturlash tilida quyidagi jarayonni yozib chiqamiz [2].

```

qcl> procedure U(int n, qureg x, qureg y)
{ if n==1 { Not(y); } /* f(x)=1 */
else { if n==2 { x->y; } /* f(x)=x */
else { if n==3 { Not(x); x->y; Not(x); }}}
/* f(x)=1-x */

```

Bu jarayonni kiritganimizdan so'ng, y bitga $|-\rangle$ holatni ko'rib chiqamiz va quyidagi natijaga ega bo'ladi:

```

qcl> Not(y)
[2/32] 1 |0, 1>
qcl> Mix(y)
[2/32] 0.70711 |0, 0> - 0.70711 |0, 1>

```

Endi $|+\rangle \otimes |-\rangle$ holat ko'rib chiqilganda uning natijaga quyidagi ko'rinishni oladi.

```

qcl> Mix(x)
[2/32] 0.5 |0, 0> + 0.5 |1, 0> - 0.5 |0, 1> -
0.5 |1, 1>

```

Endi $f(x) = 1$ funksiyaga mos keladigan Uf operator qo'llanilganda Uf operatorining ko'rinishi quyidagicha bo'lishini ko'ramiz. Natijasi pastki qatorda ko'rsatilgan.

```

qcl> U(1,x,y)
[2/32] -0.5 |0, 0> - 0.5 |1, 0> + 0.5 |0, 1> +
0.5 |1, 1>

```

Yuqoridagilardan kelib chiqib, x bitga Adamar funksiyani qo'llaganda quyidagi ko'rinishga ega bo'ladi.

```

qcl> Mix(x)
[2/32] -0.70711 |0, 0> + 0.70711 |0, 1>
qcl> measure x,r
[2/32] -0.70711 |0, 0> + 0.70711 |0, 1>
qcl> print r
0

```

natija nolga teng bo'lgan holatni olamiz. Bundan ko'rinadiki, x bit $|0\rangle$ holatda albatta funksiya doimiy bo'ladi. x bitni qiymat natijasini o'zgartmaydigan r ga yoziladi va chop etadi [2].

Endi boshqa funksiyalarni ham natijasi qanaqa bo'lishligini ko'rib chiqish uchun xotirani asl holiga keltiramiz va $f(x)$ ning yana bitta funksiyasi uchun yuqoridagi

holatlarni takrorlaymiz $f(x)=x$ bo'lganda. Bu yerda *reset* xotirani asl holiga keltirish operatori.

```

qcl> reset
[2/32] 1 |0, 0>
qcl> Not(y)
[2/32] 1 |0, 1>
qcl> Mix(y)
[2/32] 0.70711 |0, 0> - 0.70711 |0, 1>
qcl> Mix(x)
[2/32] 0.5 |0, 0> + 0.5 |1, 0> - 0.5 |0, 1> -
0.5 |1, 1>
qcl> U(2,x,y)
[2/32] 0.5 |0, 0> - 0.5 |1, 0> - 0.5 |0, 1> +
0.5 |1, 1>
qcl> Mix(x)
[2/32] 0.70711 |1, 0> - 0.70711 |1, 1>
qcl> measure x,r
[2/32] 0.70711 |1, 0> - 0.70711 |1, 1>
qcl> print r
1

```

$f(x)=1-x$ bo'lganda ham natijasi 1 ga teng holat chiqayapdi.

```

qcl> reset
[2/32] 1 |0,0>
qcl> Not(y)
[2/32] 1 |0,1>
qcl> Mix(y)
[2/32] 0.70711 |0,0> - 0.70711 |0,1>
qcl> Mix(x)
[2/32] 0.5 |0,0> + 0.5 |1,0> - 0.5 |0,1> - 0.5
|1,1>
qcl> U(3,x,y)
[2/32] -0.5 |0,0> + 0.5 |1,0> + 0.5 |0,1> - 0.5
|1,1>
qcl> Mix(x)
[2/32] -0.70711 |1,0> + 0.70711 |1,1>
qcl> measure x,r
[2/32] -0.70711 |1,0> + 0.70711 |1,1>
qcl> print r
1

```

Olingan natijadan ko'rinib turibdiki, x bit 1 ga teng bo'lyapdi, u holda albatta $f(x) = x$ va $f(x) = 1 - x$ funksiyalar muvozanatlashgan bo'ladi [1].

Keyingi ish butun algoritmni avtomatlashagan jarayonni yozishimiz

mumkin. Bu jarayonda n parametr $f(x)$ funksiyani ishlatadi.

```

qcl> procedure Deutsch( int n)
{ reset; Not(y); Mix(y); Mix(x); /* |+> *|-> */
  U(n,x,y); Mix(x);
  measure x,r; print r; }
qcl> Deutsch(0)
0
[2/32] 0.70711 |0, 0> - 0.70711 |0, 1>
qcl> Deutsch(1)
0
[2/32] -0.70711 |0, 0> + 0.70711 |0, 1>
qcl> Deutsch(2)
1
[2/32] 0.70711 |1, 0> - 0.70711 |1, 1>
qcl> Deutsch(3)
1
[2/32] -0.70711 |1, 0> + 0.70711 |1, 1>
qcl> exit

```

Bundan biz ko‘ramizki, algoritm haqiqatdan ham 0 ga teng bo‘lganda birinchi ikkita $f(x)$ funksiyalar doimiy ($f(x)=0$, $f(x)=1$) va 1 ga teng bo‘lganda qolgan ikkita ($f(x)=x$ va $f(x)=1-x$) uchun funksiya muvozanatlashgan bo‘ladi [11-12].

Klassik analogdan farqli o‘laroq, kvant algoritmi yacheyka ishlatiladigan hisoblash asosiga qarab universal elementlarning turli sinflarida bajarilishi mumkin. Kvant algoritmi yacheykasi kvant hisoblash jarayoniga mos keladigan ba‘zi bir unitar operator U ning evolyutsiyasini tavsiflaydi.

Kvant axborot nazariyasining asosiy tushunchalari. Kvant axborot nazariyasi kvant holatlari bilan ishlaydi, ularning xususiyatlari va qonuniyatlarini o‘rganadi. Ushbu fan kvant holatlari va to‘lqin funksiyasi tushunchalari asosida qurilgan. Ularning asosida qubit, to‘lqin funksiyasining qulashi va klonlashni taqiqlash kabi tushunchalar shakllanadi.

Tushunchalarning har biriga batafsil to‘xtalib o‘tsak.

Kvant va an’anaviy axborot nazariyasi o‘rtasida sezilarli farqlar mavjud. Avvalo, kvant zarrachasi va zarrachalar tushunchalari bir-biridan farq qiladi. Agar fazodagi ba‘zi bir jismlar sifatida qaraladigan zarracha uchun klassik fizikada koordinatalar, massa va kattalik kabi xususiyatlar mavjud bo‘lsa, u holda kvant fizikasida ularning qaysi qismida joylashganligini aniqlash mumkin emas (Geyzenbergning noaniqlik prinsipi). Shunga qaramay, ularning xatti-harakatlarini ma’lum bir ehtimollik bilan taxmin qilish mumkin edi, bu faqat tizimning klassik fizik xususiyatlarini to‘liq rad etgandan so‘ng tasvirlanishi mumkin. Bu prinsipial yangi kontseptsiya – “kvant holati” ning kiritilishiga olib keldi [13-14].

Kvant holati - bu N gilbert fazosidagi musbat Ermit operatoridir. Boshqacha qilib aytganda, bu tizimning xususiyatlarini aniqlaydigan to‘liq ma’lumotlar to‘plami (fizik kattaliklar). Tizim tomonidan aniqlanadigan ma’lumotlar to‘g‘ridan-to‘g‘ri tizimning o‘ziga bog‘liqdir.

Murakkab kvant tizimining tavsifi superpozitsiya prinsipiga asoslanadi. Holat - bu vektor kattaligi, bu kvant nazariyasida $|\psi\rangle$ belgisi bilan belgilanadi.

Kvant kriptografiyasida kalitlarni taqsimlash tizimlarini rivojlantirishning ikkita asosiy yo‘nalishi aniqlangan.

Birinchi yo‘nalish bitta zarrachaning kvant holatini kodlashga asoslangan va ikkita ortogonal bo‘lmagan kvant holatini mutlaqo ishonchli tarzda ajratib bo‘lmaydigan prinsipga asoslanadi [14].

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

bu yerda $|0\rangle$ va $|1\rangle$ holatning α va β murakkab koeffitsientlari bilan, bundan tashqari

$$|\alpha|^2 + |\beta|^2 = 1$$

Agar $\langle \psi_1, \psi_2 \rangle = 0$ shart bajarilmasa, ya'ni agar holatlar ortogonal bo'lsa u holda kvant mexanikasining qonunlari, ikkita kvant holatini ishonchli ajratishga imkon bermaydi

$$|\psi_1\rangle = \alpha|0\rangle + \beta|1\rangle$$

va

$$|\psi_2\rangle = \alpha|0\rangle + \beta|1\rangle$$

Birinchi yo'nalish xavfsizligi noma'lum kvant holatini klonlashni taqiqlovchi teorema asoslanadi. Kvant mexanikasining yaxlitligi va chiziqchilik tufayli, boshlang'ich holatiga ta'sir qilmasdan, noma'lum kvant holatining aniq nusxasini yaratish mumkin emas. Jo'natuvchi va qabul qiluvchisi ushbu tizimlarning holatini kodlovchi ma'lumotlarni uzatish uchun ikki darajali kvant tizimlaridan foydalanadilar deylik.

Agar tajovuzkor, jo'natuvchi tomonidan yuborilgan saqlash vositasini buzsa, uning holatini o'lchaydi va uni qabul qiluvchiga yuboradi, unda bu vositaning holati o'lchov oldingisiga qaraganda boshqacha bo'ladi. Shunday qilib, kvant kanalini tinglash qonuniy foydalanuvchilar tomonidan aniqlanishi mumkin bo'lgan uzatishda xatolariga olib keladi [5-7].

BB84 protokolida esa fotonlarning to'rtta kvant holatidan foydalanadi, polarizatsiya vektorining yo'nalishi, ulardan biri jo'natuvchi uzatiladigan bitga qarab tanlaydi: "1" uchun 90° yoki 135° , "0" uchun 45° yoki 0° . Bir juft kvant

holati $0(|0(+)\rangle)$ va $1(|1(+)\rangle)$ ga to'g'ri keladi va "+" asosiga tegishli. Boshqa juft kvant holati $0(|0(\times)\rangle)$ va $1(|1(\times)\rangle)$ ga to'g'ri keladi va "x" asosiga tegishli. Ikkala bazisning ichida ham holatlar ortogonaldir, ammo turli xil bazislardagi holatlar juft bo'lmagan ortogonaldir (ma'lumotni olishga urinishlarni aniqlash uchun ortogonalizm zarur).

Bizning ishimizning BB84 protokolidan farqi shundaki, kalitlarni yaratish jarayoni quyidagi bosqichlarda ishlab chiqiladi.

Birinchi mijoz tomonidan tasodifiy sonlar generatsiyasi tanlanadi va maxsus IP va portlar orqali Serverga yuboriladi.

Ikkinchi tomon ham serverga yuqoridagi bir xil IP va port orqali ulanganda birinchi mijoz yuborgan tasodifiy sonlar generatsiyasi tanlagan raqamlar hosil bo'ladi. Hosil bo'lgan raqamlar ikkinchi tomondan tasodifiy sonlar generatsiyasi asosida yaratilgan raqamlar bilan solishtirilib yagona kalit yaratiladi. Shu yaratilgan yagona kalit ikkala tomon uchun ham kalit hosoblanadi.

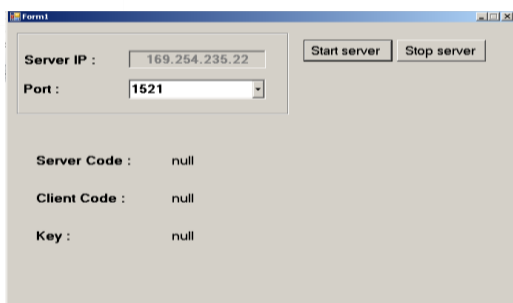
Tanlangan kalitlar bir-biriga mos keladigan holatlar soni asl ketma-ketlikning o'rtacha uzunligiga, ya'ni $n = \frac{1}{2}$ ga teng bo'ladi [15].

Kvant kriptografiyasi orqali kalitlarni taqsimlash quyidagi ko'rinishda bo'ladi.

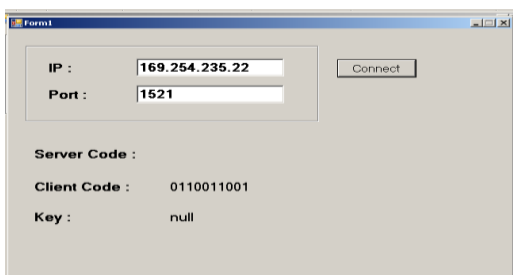
Protokolimiz orqali yaratilgan kalitlarni taqsimlash va tahlil qiluvchi dasturiy vositaning ishlash prinsipi quyidagicha.

Dasturning IP va port maydonida qiymati hisoblanishi zarur bo'lgan manzil tanlanadi [16].

Server qismida *Start server*, *Stop server* bo'limlari joylashgan.

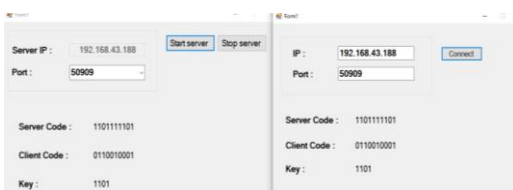


1-rasm. Server dasturni kalitni taqsimlashi.



2-rasm. Adireslash va portni aniqlash.

Mijoz bo'limida IP va shu IP ga mos Port bo'limlari joylashgan. Server Code qismida *Server Code* tanlagan tasodifiy sonlar generatsiyasi asosida kalitlar hosil bo'ladi. *Client Code* bo'limida mijoz tomonidan tasodifiy sonlar generatsiyasi asosida hosil bo'lgan sonlar yoziladi. *Key* qimida esa *Server* va *Mijoz*lar kalitlari solishtirishdan hosil bo'lgan umumiy yagona kalit hosil qilinadi [8-10].



3-rasm. Ikkalasi uchun umumiy kalitlar.

III. XULOSA

Xulosa qilib aytadigan bo'lsak ushbu maqolada kvant algoritmlarni yechishda qo'llaniladigan qcl (quantum computation language) tili, uning operatorarining ishlash jarayonlari va Deutsch algoritmini ishlash prinsiplari keltirib o'tilgan. Kvant jarayonlarning asosiy tamoyillari,

fizikaviy va algoritmik talqinlari hisobga olingan. Ushbu jarayonlar tizimni tahlil qilishda global optimallashtirish muammolariga samarali yechimlarni qidirishda va kutilmagan holatlarni oqilona boshqarishda qo'llaniladigan algoritmlarning tasniflari keltirilib o'tilgan.

Hozirgi vaqtda kalitlarni taqsimlash muammosida kvant kriptografiyasi assimetrik shifrlash tizimlariga yagona muqobildir. Yuqoridagilarni hisobga olgan holda, assimetrik shifrlash tizimlarini buzish murakkabligi sezilarli darajada pasaygan taqdirda, kvant kriptografiyasi rivojlanish uchun potentsialga ega.

Biroq, kvant kriptografiyasining tamoyillari va usullaridan foydalangan holda tizimlarni tashkil qilishning yuqori texnologik murakkabligi, hatto zamonaviy texnologiyalarning etarlicha yuqori darajada rivojlanishi bilan ham assimetrik tizimlarni siqib chiqarishga imkon bermaydi.

ADABIYOTLAR

- [1] B. Omer, Structured Quantum Programming, Ph. D. Thesis, Technical University of Vienna (2003).
- [2] A. Г. Грозин, Квантовый компьютер для чайников, Новосибирск (2004).
- [3] J. van der Hoeven, GNU TEXmacs, <http://www.texmacs.org/>
- [4] A.G. Grozin, TEXmacs interfaces to Maxima, MuPAD and REDUCE, Proc. 5 Int. workshop on Computer algebra and its applications to physics, Dubna, JINR E5,11-2001-279; cs.SC/0107036
- [5] D. Deutsch and R. Jozsa, Rapid solution of problems by quantum computer, Proc. Roy. Soc. A 439 (1992) 553.

- [6] P.W. Shor, Algorithms for quantum computation: Discrete logarithms and factoring, Proc. 35 Annual Symposium on Foundations of Computer Science, IEEE Press (1994).
- [7] R. Rivest, A. Shamir, and L. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Comm. ACM 21 (2) (1978) 120.
- [8] C.H. Bennett, G. Brassard, and N.M. Mermin, Quantum cryptography without Bell's theorem, Phys. Rev. Lett. 68 (1992) 557.
- [9] S. Wiesner, Conjugate coding, написано в 1970, опубликовано в SIGACT News 15 (1) (1983) 78.
- [10] C.H. Bennett, G. Brassard, C. Cr'epeau, R. Jozsa, A. Peres, and W.K. Wootters, Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels, Phys. Rev. Lett. 70 (1993) 1895.
- [11] Кронберг Д.А., Ожигов Ю.И., Чернявский А.Ю. Квантовая криптография. Москва, Изд-во МГУ им. М.В. Ломоносова, 2006, с. 23–40.
- [12] Вялый М. Квантовые алгоритмы: возможности и ограничения. Санкт-Петербург, 2011.
- [13] Постулаты квантовой теории. ВГУ, 2012. URL: <http://www.rec.vsu.ru>
- [14] Bennett C.H. Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett., 1992, vol. 68, no. 21, pp. 3121–3124.
- [15] Ш. Тоиров. “Подходы и алгоритмы квантовой криптографии” журнал “Информатика и энергетика”. Ташкент 2020.
- [16] Sh. Toirov. Efficient methods for solving functions using quantum genetic algorithms. XI International Scientific and Practical Conference “Theoretical approaches of Fundamental Sciences. Theory, Practice and prospects ”, April 26-28, 2021, Geneva, Switzerland

Поступила в редакцию 15.10.2022

Citation: Toirov Sh.A., Xamdamov F.B., Xonimqulov J. B. (2022). Kvant paralellashtirishda kvant algoritmlarni optimallashtirish usullari. Raqamli texnologiyalarning nazariy va amaliy masalalari xalqaro jurnali. 2(2). – B. 77-84.

OPTIMIZATION METHODS OF QUANTUM ALGORITHMS IN QUANTUM PARALLELIZATION

Toirov Sh.A.¹, Kudratov R.B.¹, Xamdamov F.B.², Xonimqulov J. B.¹

¹ Samarkand branch of Tashkent University of information technologies named after Muhammad al-Khwarizmi, Samarkand, Uzbekistan

² Training course for employees of self-government bodies of citizens under the administration of the Samarkand region, Samarkand, Uzbekistan
tshuxrat@mail.ru, firuz-0405@mail.ru, rustamkudratov4@gmail.com

Abstract. In this article, *qcl* (quantum computation language), its operators, and the principles of solving using Deutsch's algorithm, used in solving quantum algorithms, are presented. The basic principles, physical and algorithmic interpretations of quantum

processes are considered. Classifications of algorithms used in the search for effective solutions to global optimization problems and rational management of unexpected situations in the analysis of these processes are given.

Keywords: *Quantum, genetic and immune algorithms, qcl (quantum computation language), global optimization, intelligent management.*

МЕТОДЫ ОПТИМИЗАЦИИ КВАНТОВЫХ АЛГОРИТМОВ ПРИ КВАНТОВОЙ ПАРАЛЛЕЛИЗАЦИИ

Toirov Sh.A.¹, Kudratov R.B.¹, Xamdamov F.B.², Xonimqulov J.B.¹

¹Самаркандский филиал Ташкентского университета информационных технологий имени Мухаммада ал-Хорезми, Самарканд, Узбекистан

²Учебный курс для работников органов самоуправления граждан при администрации Самаркандской области, Самарканд, Узбекистан
tshuxrat@mail.ru, firuz-0405@mail.ru, rustamkudratov4@gmail.com

Аннотация. *В данной статье представлены qcl (язык квантовых вычислений), его операторы и принципы решения с использованием алгоритма Дойча, применяемого при решении квантовых алгоритмов. Рассмотрены основные принципы, физические и алгоритмические интерпретации квантовых процессов. Приведены классификации алгоритмов, используемых при поиске эффективных решений задач глобальной оптимизации и рационального управления непредвиденными ситуациями при анализе этих процессов.*

Ключевые слова: *квантовые, генетические и иммунные алгоритмы, qcl (язык квантовых вычислений), глобальная оптимизация, интеллектуальное управление.*