BB84 KVANT KALITINI TAQSIMLASH PROTOKOLI

Kurbanova F.CH
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari Universiteti magistiri

https://doi.org/10.5281/zenodo.11164054

Annotatsiya: Mazkur tadqiqot ishida kvant texnologiyasidagi BB84 protokoli, kvant elementlari haqida tushunchalar keltirilgan. Kvant texnologiyasining BB84 protokoli tahlil qilingan.

Kalit so‘zlar: BB84, protocol, kriptografiya, protokol sxemalari, protocol sxemasi, klassik protsedura.

BB84 QUANTUM KEY DISTRIBUTION PROTOCOL

Abstract: This research paper presents the concepts of BB84 protocol, quantum elements in quantum technology. The BB84 protocol of quantum technology is analyzed.

Keywords: BB84, protocol, cryptography, protocol schemes, protocol scheme, classical procedure.

ПРОТОКОЛ РАСПРЕДЕЛЕНИЯ КВАНТОВЫХ КЛЮЧЕЙ BB84

Аннотация: В данной исследовательской работе представлены концепции протокола BB84, квантовых элементов в квантовых технологиях. Анализируется протокол квантовой технологии BB84.

Ключевые слова: BB84, протокол, криптография, схемы протоколов, схема протоколов, классическая процедура.

KIRISH

1984 yilga kelib kvant kriptografiyasi tamoyillarini shakllantirish va hatto o'sha paytda kalitlarni taqsimlashning ushbu usulining maxfiyligi foydasiga qat'iy, ammo intuitiv dalillarni taqdim etish uchun yetarli bo'lgan. Keyin kvant kriptografiyasining haqiqiy formalizmini rivojlantirish vaqti keldi: qonuniy foydalanuvchilarning talab qilinadigan harakatlari tavsiflandi, hujumchi harakatlari rasmiylashtirildi va BB84 deb nomlangan birinchi kvant kalitlarini taqsimlash protokolining maxfiyligi isbotlandi.

Kvant kriptografiyasiga asoslangan kvant axborot nazariyasining asosiy faktlari bu o'zboshimchalik bilan kvant holatlarini nusxalashning mumkin emasligi va ortogonal bo'lmagan holatlarni ishonchli farqlashning mumkin emasligi haqidagi bir-biriga bog'liq bo'lgan bayonotlardir. Birgalikda, bu faktlar shuni ko'rsatadiki, ortogonal bo'lmagan to'plamdan kvant holatlarini ajratish urinishlari shovqinlarga olib keladi, ya'ni tutuvchining harakatlari qabul qilish tomonidagi xato kattaligi bilan aniqlanishi mumkin.

ASOSIY QISM

Shuni ta'kidlash kerakki, kvant kriptografiyasi tinglovchining harakatlarining tabiati va u uchun mavjud bo'lgan resurslar miqdori to'g'risida hech qanday taxmin qilmaydi: hujumchi har qanday resurslarga ega bo'lishi va bugungi kunda ma'lum bo'lgan tabiat qonunlari doirasida barcha mumkin bo'lgan harakatlarni amalga oshirishi mumkin. Bu kvant kriptografiyasini tinglovchining hisoblash quvvatidagi cheklovlarga tayanadigan klassikadan sezilarli darajada ajratib turadi.

Umumiy protokol sxemasi

Norasmiy ravishda, kvant kriptografiyasining barcha protokollarining ishlash printsipini quyidagicha ta'riflash mumkin: uzatuvchi tomon (Alisa) har bir qadamda ularning ortogonal bo'lmagan to'plamidan davlatlardan birini yuboradi va qabul qiluvchi tomon (Bob) shunday o'lchov hosil qiladiki, tomonlar o'rtasida klassik ma'lumotlarning qo'shimcha almashinuvidan so'ng, ular mukammal kanal va hujumchi yo'qligi holatiga to'liq mos keladigan bit satrlariga ega bo'lishi kerak. Ushbu satrlardagi xatolar kanalning nomukammalligini ham, tinglovchining harakatlarini ham ko'rsatishi mumkin. Xato ma'lum bir chegaradan oshib ketganda, protokol harakati to'xtatiladi, aks holda qonuniy foydalanuvchilar o'zlarining (bir-biriga mos keladigan) bit qatorlaridan to'liq maxfiy kalitni olishlari mumkin.

Signal holatini uzatish

BB84 protokoli ikkita bazisdan foydalanadi:

$$+: |x\rangle = |0\rangle, \qquad |y\rangle = |1\rangle,$$
$$x: |u\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |v\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \qquad (1)$$

Bu bazislar xolis shartni qondirishini tekshirish oson

$$|\langle x|u\rangle|^2 = |\langle x|v\rangle|^2 = \frac{1}{2},$$
$$|\langle y|u\rangle|^2 = |\langle y|v\rangle|^2 = \frac{1}{2}. \qquad (2)$$

bu norasmiy ravishda bitta bazis nuqtai nazaridan, boshqasidagi holatlar nosimmetrik tarzda joylashganligiga bog'liq.

Holatlarni tayyorlash bosqichida Alisa tasodifiy ravishda ko'rsatilgan bazislardan birini tanlaydi (1) va keyin tasodifan bit qiymatini tanlaydi: 0 yoki 1 va ushbu tanlovga muvofiq to'rtta signaldan birini yuboradi:

- $|x\rangle$ agar bu bazis “+” bo'lsa va bit qiymati 0,
- $|y\rangle$ xuddi shu bazisda va bit qiymati 1 ga teng,
- $|u\rangle$ “×” bazisga tushganda va bit 0 ga teng bo‘lganda,
- $|u\rangle$ agar 1-bit “×” bazisida tushirilsa.

Ushbu signallarning har birini yuborishda Alisa o'zining asosiy tanlovini va bitni tanlashni eslab qoladi, natijada uning tomonida ikkita tasodifiy bit satr paydo bo'ladi.

Bob Alisa tomonidan yuborilgan signallarning har birini qabul qilib, uning ustida tasodifiy ravishda ikkita o'lchovdan birini ishlab chiqaradi, ularning har biri Alisaning har bir bazisidagi holatlarning ortogonalligi tufayli ishonchli natija berishga qodir:

$$M_0^+ = |x\rangle\langle x|, \qquad M_1^+ = |y\rangle\langle y|,$$
$$M_0^x = |u\rangle\langle u|, \qquad M_1^x = |v\rangle\langle v|. \qquad (3)$$

Natijada, u ikkita chiziqqa ega: o'lchov uchun bazislardan qaysi biri bilan tanlangan va bu o'lchovlar natijalari bilan.

Shunday qilib, barcha holatlar o'tkazilgandan va o'lchovlar o'tkazilgandan so'ng, Alisa va Bob har biri ikkita qatorga ega. Bu yerda bazislarni muvofiqlashtirish sodir bo’ladi: ochiq kanalda Alisa va Bob o'zlarining satrlarini bir-birlariga bazalarni tanlash bilan e'lon qilishadi va ular o'zlarining bazislariga mos kelmaydigan xabarlarnilarni tashlashadi. Shuni ta'kidlash kerakki, Agar Alisaning holatini yuborish uchun ishlatiladigan bazis Bobni o'lchash asosiga to'g'ri kelgan bo'lsa, u holda aloqa kanalida shovqin bo'lmasa, ularning bit satrlaridagi natijalar tegishli

pozitsiyada mos keladi, shuning uchun bazisni muvofiqlashtirish bosqichidan keyin ideal kanal va hujumchi tomonidan harakatlar bo'lmasa, Alisa va Bob bir xil bit satrlarga ega bo'lishi kerak.

Ammo, agar kanalda xatolar bo'lsa yoki hujumchi ma'lumotni tinglashga harakat qilsa, Alisa va Bobning bit satrlari mos kelmasligi mumkin, shuning uchun tekshirish uchun ular bit satrlarining taxminan yarmini izchil ravishda ochishlari kerak. Markaziy chegara teoremasiga ko'ra, ochilgan bit ketma-ketligidagi xato butun ketma-ketlikdagi xatoni yetarlicha aniq baholaydi va undan qolgan pozitsiyalarda xato ehtimolini aniq baholash mumkin. Agar xato miqdori ma'lum bir qiymatdan (protokol parametri) kattaroq bo'lsa, ma'lumotlarni uzatish to'xtaydi: bu shuni anglatadiki, tutuvchi kalit haqida juda ko'p ma'lumotga ega. Aks holda, Alisa va Bobga umumiy maxfiy kalitni olish vazifasi yuklatilgan. Ushbu vazifani ikki bosqichga bo'lish mumkin: birinchidan, xatolarni tuzatish amalga oshiriladi, natijada Alisa va Bobning ixtiyorida bir-biriga mos keladigan bit satrlari bo'ladi. Maxfiylikni kuchaytirish deb nomlangan ikkinchi bosqich, ishlatilgan kvant holatlari bo'yicha harakatlar yoki xatolarni tuzatish jarayonida hujumchiga yetib borishi mumkin bo'lgan kalit ma'lumotlarini chiqarib tashlashni maqsad qiladi. Ushbu qadam natijasida hujumchi Alisa va Bobning umumiy bit qatori haqida ma'lumotga ega bo'lmasligi kerak.

Xatoni tuzatish

Shunday qilib, xatolarni tuzatish protsedurasining maqsadi Alisa va Bobning bir-biriga mos keladigan bit qatorlaridan butunlay bir xillarni olishdir. Bu klassik protsedura, chunki u faqat klassik bitlar va ochiq aloqa kanallari bilan shug'ullanadi.

Xatolarni tuzatishning eng samarali protsedurasi tasodifiy kodlardan foydalanishga to'g'ri keladi. Q xatosi ehtimoli bo'lgan klassik kanalning o'tkazuvchanligi

$$C_{clas}(Q) = 1 - h(Q),$$

bu yerda $h(Q)$ ikkilik Shennon entropiyasi. Kanaldagi xatolik ehtimolini bilgan va n uzunlikdagi ketma-ketlikka ega bo'lgan Alisa $2^{n(C_{clas}-\delta)}$ tasodifiy kodli so'zlarni yaratadi. Parametr δ ning katta qiymatlari uchun kichik bo'lishi mumkin. Alisa ham bunga o'z bitlar ketma-ketligini qo'shadi. Ro‘yxatni tuzadi, shundan so‘ng u Bobga kod so‘zlari to‘plamini ochiqchasiga yetkazadi. Olingan kodli so'zlar ro'yxatidan Bob Hamming metrikasidagi ketma-ketligiga eng yaqinini tanlaydi. Shovqinli kanalni kodlash teoremasiga ko'ra, kod so'zlarning bunday tanlovi bilan Bob ehtimollik bilan Alisaning bit qatorini tanlaydi.

Ammo shuni yodda tutingki, mutlaqo tasodifiy kodlarni amalda qo'llash qiyin, chunki ulardan foydalanish xotirada eksponensial darajada ko'p sonli kod so'zlarini (n bit qatorining uzunligiga qarab) saqlashni talab qiladi. Odatda, haqiqiy sxemalarda samaradorligi pastroq bo'lgan boshqa, konstruktiv kodlar qo'llaniladi.

Maxfiylikni oshirish

Ushbu bosqichda Alisa va Bob mos keladigan bit satrlari va Eva uchun mavjud bo'lgan ma'lumotlarning taxminiga ega. Bu taxmin “xom” kalitdagi xatolar sonidan olingan (esda tutingki, bu xatolar aloqa kanalidagi shovqin bilan bog'liq va ularning barchasi Evaning faoliyati tufayli yuzaga kelgan. Uning ma'lumotlarini qanday aniq baholash mumkin. Xatolar soniga keying o’rinlarda ko'rsatiladi) va xatolarni to'g'rilash protsedurasidan boshlab, ma'lumotlarning bir qismi, ta'kidlanganidek, tutuvchiga ham o'tadi.

Maxfiylikni kuchaytirish bosqichining vazifasi Alisa va Bobning qisman maxfiy umumiy uy satrlaridan Evaga umuman noma'lum bo'lgan maxfiy kalitni olishdir. Odatda, bunday protsedura davomida kalit uzunligi sezilarli darajada kamayadi.

Maxfiylikni oshirishning asosiy usuli $\mathcal{G}$ universal Xesh funksiyalari sinfidan foydalanishdir. Bu tasodifiy tanlangan Xesh funksiyasi uchun $g \in \mathcal{G}$ va har qanday mos kelmaydigan elementlar uchun $a_1 a_2 \in \mathcal{G}$ va ularning $g(a_1) = g(a_2)$ rasmlarining mos kelish ehtimoli $1/|B|$ dan oshmaydigan tarzda b bit qatorlari to'plamiga n-bitli m-qatorlari to'plamini aks ettiruvchi funksiyalardir. Ya'ni, B dagi ikki xil elementning prototiplarini topish muammosi qo'pol kuch ishlatish yoki taxmin qilishdan ko'ra samaraliroq hal etilmaydi.

Evaning yakuniy kalit haqidagi ma'lumotlarini qisman maxfiy kalit haqidagi dastlabki ma'lumotlari va yakuniy kalit uzunligi m orqali baholaydi:

Teorema. *X* taqsimoti *p(x)* bo‘lgan tasodifiy o‘zgaruvchi bo‘lsin, G esa X alifbosini $\{0, 1\}^m$ ga xaritalashtiruvchi xesh funksiyalarning universal sinfidan xesh-funksiyalarning teng ehtimolli tasodifiy tanlanishiga mos keladigan tasodifiy o‘zgaruvchi bo‘lsin. Shunda

$$H(G(X)G) \geq m - 2^{m-H_c(X)}, \quad (4)$$

Qayerdaki

$$H_c(X) = -\log\left[\sum_x p(x)^2\right]$$

to'qnashuv entropiyasi deb ataladi.

Uning qo'llanilishi shundan kelib chiqadiki, qonuniy foydalanuvchilar Eva haqidagi ma'lumotni baholaydilar (bu qiymat bilan beriladi), har doim yakuniy kalitning uzunligini tanlashi mumkin m shunchalik kichikki, Evaning yakuniy kalitga nisbatan noaniqligi (4) ning chap tomoni tomonidan berilgan oddiy taxminning noaniqligiga yaqin bo'lgan har qanday joyda bo'ladi, bu uning to'liq maxfiyligiga mos keladi.

Uning qo'llanilishi shundan iboratki, qonuniy foydalanuvchilar Evaning ma'lumotlarini ($H_c(X)$ qiymati bilan berilgan) baholab, har doim yakuniy kalit m uzunligini shunchalik kichik tanlashlari mumkinki, Evaning yakuniy kalitga nisbatan noaniqligi (chap tomonda berilgan (4)) o'zboshimchalik bilan unga mos keladigan oddiy taxminning noaniqligiga yaqin bo'ladi to'liq maxfiylik.

XULOSA

Shunday qilib, Alisa va Bobning o'zaro ma'lumotlari Alisa va Evaning o'zaro ma'lumotlaridan ustun bo'lgan vaziyatda, har doim universal xesh funksiyasi yordamida uni siqib, asl qisman maxfiy kalitdan to'liq maxfiy kalitni olish har doim mumkin.

Foydalanilgan adabiyotlar

1. Acin A., Gisin N., and Scarani V. Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks // Phys. Rev. A-2004. - Vol. 69, 012309.
2. Bennett C.H. Quantum Cryptography using any Two Nonortogonal States // Phys. Rev. Lett. - 1992. -Vol.68, 3121.
3. Bennett C.H., Brassard G. Quantu Cryptography: Public Key Distribution and Coin Tossing // Proc.of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India, - 1984. - Pp. 175 -179.
4. Carter J.L., Wegman M.N. Universal classes of hash functions // Journal of Computer and System Sciences - 1979. - Vol. 18, 143.
5. Diffic W., Hellman M.E. New Directions in Cryptography IEEE Transactions on Information Theory 1976. - Vol. 22, 644.
6. Einstein A., Podolsky B., Rosen N. Can quantum-mechanical description of physical reality be considered complete? // Phys. Rev. A - 1935. - Vol. 47, 777.