Механика Транспорт Комуникации

Научно списание

ISSN 1312-3823

том 12, брой 3/2, 2014 г.

статия № 1026

http://www.mtc-aj.com

АСПЕКТИ НА ПРИЛОЖЕНИЯТА НА КВАНТОВАТА КРИПТОГРАФИЯ ЗА ЗАЩИТА НА ДАННИ

Христина Спиридонова, Антонио Андонов
hristinaspiridonova@abv.bg, andonov@vtu.bg

Висше транспортно училище „Тодор Каблешков”
бул. Гео Милев 158, София
БЪЛГАРИЯ

Ключови думи: *информационна сигурност, квантова криптография*

Резюме: *През последните двадесет гадини квантовите свойства на материята и енергията се прилагат в областта на информационната сигурност .В предложената статия са дискутирани основните свойства на квантовия компютър, на тяхна база е обоснован алгоритъм за квантова криптография и е анализирана криптоустойчивостта му.*

1. Въведение.

Съвременните технологични достижения и тяхното бързо развитие в такива области като космически изследвания, радиоелектронна, компютърна и рентгенова техника, квантова физика постоянно изменят ситуацията в областта на защита на конфиденциалната информация, като позволяват създаването на високоефективни средства за несанкциониран достъп до нея. Защитата от тях е възможна само на същото технологично ниво. Създаването на глобални мрежи от системи с различно предназначение: военни, банкови, за електронно банкиране и търговия, ведомствени за специални задачи и други, изискват все по-бързи темпове за обмен и достъпност на информацията в условия на мобилност. Обменяната в тях информация е в основната си част класифицирана, затова основен фактор при тях е защитата и сигурността на информационния обмен. Най-уязвими елементи на информационите системи са оборудването и апаратурата, предназначени за обработка, съхранение и предаване на конфиденциалната информация.

2. Квантова информация

Една от най-бързо развиващите се области в съвременната физика е квантовата информация. Силен тласък на нейното развитие беше даден през 1994 г. от Питър Шор, който предложи първия квантов алгоритъм за факторизиране. В неговата прочута статия той показа, че квантовият компютър може да факторизира числа експоненциално по-бързо от класическия компютър. Предложеният от Гровер през 1997 г. втори квантов алгоритъм за намиране на маркиран елемент в неструктурирана база данни отново демонстрира превъзходството на квантовия компютър спрямо класическия. Тези алгоритми, заедно с експерименталните успехи свързани с контрола и манипулирането на единични квантови частици станаха причина за огромния интерес

към физичната реализация на квантовия компютър. Квантовата информация се състои от три основни области: квантови компютри, квантова криптография и квантови комуникации. Най-голямата от тези области са квантовите компютри, които предлагат не само значително ускоряване на решаването на редица класически бавни задачи, но и на някои класически нерешими задачи. . Това устройство няма да изисква кой знае колко много клетки работна памет за обработка на информацията : Ще са достатъчни само няколкостотин такива. Да кажем – 300 клетки ще стигнат, за да може информационният ресурс на този компютър да превиши 10 пъти броя на частиците във Вселената ($2^{300} = 10^{90}$). Целият този гигантски масив от информация може да се променя съгласувано само с един работен такт. Това поразяващо различие между обикновения и квантовия компютър се обяснява с факта, че ефективността на последния нараства експоненциално с увеличаване броя на клетките на неговата памет

Броят на различните състояния на клетките памет на класическия компютър е същият като на квантовия. Така класическият компютър с памет от 300 бита може последователно да премине през същите 2^{300} състояния, но във всеки един момент той може да се намира само в едно от тях. От друга страна, квантовият компютър може да се намира едновременно във всички тези състояния (в тяхната суперпозиция1). Когато в паметта на класически компютър се промени един бит, останалите битове в нея не реагират по никакъв начин – те не се променят. Когато в квантовия компютър се промени един бит (нарича се квантов бит – кубит), заедно с него съгласувано се променят и всички останали, по този начин цялата суперпозиция се пренастройва мигновено. Така се постига гигантска скорост на действие и според оценката на специалистите излиза, че изчислителната мощност на квантовия компютър
расте експоненциално спрямо тази на класическия компютър. За онагледяване на невероятно голямото предимство на квантовия компютър може да послужи и следния пример. Да си представим, че имаме квантов компактдиск, който за разлика от обикновения съдържа информация в кубити, а не в битове. В квантовия CD кубитите се намират в състояние на суперпозиция, което съдържа всички възможни дискретни последователности от 0 и 1 едновременно. Квантовият CD представлява нещо като универсална матрица, от която може да се „отпечатва“ всеки класически CD, с каквато и да е информация и последователност на битовете. Единственото ограничение е невъзможността да се надвиши обема на битовете на изходния CD. По такъв начин един квантов CD съдържа едновременно всички възможни класически CD – стари, настоящи или бъдещи, с всякаква възможна информация – осмислена или не, и с всякаква двоична последователност, съставена от 0 и 1.. От теоретична гледна точка създаването на квантовия компютър не представлява особена сложност – достатъчно е клетките памет (кубитите) да могат да взаимодействат по-между си и ние да можем целенасочено да въздействаме върху тяхното състояние. Въпросът бил в това, че докато всички съвременни прибори и компютри работят по квантовите закони, но в класически режим, квантовият компютър би трябвало да работи и в квантов режим. В този случай в играта влиза основният принцип на квантовата теория – принципът за суперпозицията на състоянията. Така компютърът получава възможност да оперира с кохерентните (съгласувани) състояния на клетките памет. До този момент човечеството никога не е разполагало с подобни квантово-корехентни устройства, които функционират чрез суперпозиционните състояния. Когато те започнат да навлизат от научните лаборатории в масовото производство и в нашето всекидневие, това е началото на втора квантова революция.

Основният носител на квантова информация е квантовата система с две нива, наречена кюбит. Хилбертовото пространство на ансамбъл от N кюбита има размерност 2^N, което е огромно число дори и за малък брой кюбити. Обработката на квантова

информация от квантовите компютри се осъществява чрез два типа унитарни операции – едночастични и двучастични. Те са достатъчни за реализирането на всяка произволна многочастична операция. Едночастичните унитарни операции имат за цел променянето на състоянието на кюбитите, т.е. реализирането на контролирани квантови преходи между различни суперпозиционни състояния. Многочастичните унитарни операции над кюбити водят до появата на квантови корелации между тях и създаването на така наречените сплетени състояния. Тези състояния са в основата на много от интригуващите аспекти на квантовата информация като проверка на неравенствата на Бел, квантовата телепортация, квантовата криптография и др.

3. Процедура на алгоритъм за квантова криптография

Базова задача на криптографията е шифрирането на данни и автенфикация на потребителя. Това е лесно изпълнимо, ако предаваната страна и получателя разполагат с псевдослучайни последователности, наречени ключове. Пред началото на информационния обмен всеки от участниците трябва да получи ключа, при което тази процедура трябва да се изпълни с най-висока степен на конфинденциалност .

Тук е най-разпространеното в настоящия момент приложение на квантовата механика. Надеждността на метода за квантово разпространение на ключа QKD(Quantum Key Distribution) се основава на ненарушението на квантовата механика. Атака върху сигнала не може да бъде осъществена, тъй като не може да се раздели електронния квант на части. В основата на квантовата криптография лежи даването на квантовите състояния на фотоните. Предаващата страна задава тези състояния, а получаващата ги регистрира. Тук се използва квантовия принцип на неопределеността, когато две квантови величини не могат да бъдат измерени едновременно с необходимата точност. Поляризацията на фотоните може да бъде ортогонална, диагонална или циркулярна. Измерването на един вид поляризация рандомизира другата съставна. Следователно, ако предаващата и приаемащата страни не са се договарили предварително, полуачателя може да разруши сигнала без да извлича информация.

Изпращащата страна кодира изпращаните данни, задава определени квантови състояния, получателя регистрира тези състояния. Същевременно получателя и изпращача съвместно обсъждат резултатите от наблюденията.В крайна сметка с произволно висока достоверност може да се постигне увереност, че изпратените и приети последователности са тъждествени. Обсъждането на резултатите се отнася до грешките внесени от шумове или външни атаки и нито в най-малка степен не разкрива съдържанието на предаваното съобщение. При предаване на данни се контролира поляризацията на фотоните. Поляризацията може да бъде (хоризонтална или вертикална), циркулярна (лява или дясна) и диагонална (45°и 135°).

В качеството на светлинен източник се използва светодиод или лазер. Светлина се филтрира, поляризира и формира във вида на кратки импулси с малка интензивност. Поляризацията на всеки се модулира от изпращащата страна по пройзволен начин в съответствие с едно от четирите посочени състояния (хоризонтално, вертикално, ляво и дясно – циркулярна).

Получателя измерва поляризацията на фотоните, като използва пройзволна последователност базови състояния (ортогонална или циркулярна)

Получателя открито съобщава каква последователност е използвал. Изпращащата страна открито съобщава каква каква последователност той е използвал не уведомява получателя за това, кои базови състояния са използвани коректно. Всички измервания, използвани при неверни базови състояния се отхвърлят. Измерванията се

интерпретират съгласно двойчната схема: ляво- циркулираща поляризация или хоризонтална-„0”, дясно – циркулярната поляризация или вертикална- „1”

Висока надеждност се постига на база, ефекти APR(Айнщайн – Подолски – Росен) Този ефект възниква когато атома излъчва два фотона с неопределена поляризация, но в следствие на симетрията на тяхната поляризация, тя винаги е противоположна. Важна особенност на този ефект, е че поляризацията на фотоните става известна само след измерване. Тогава изпращащата страна генерира определено количество АПР фотонни двойки. Единия фотон от всяка двойка той остава за себе си, втория изпраща на своя партньор. При това, ако ефективността на регистриращия е близка до «1», то то неговия партньор регистрира 0 и обратно. По този начин партньорите получават идентични (инвентирани) кодови последователности.

4. Заключение

Новата физическа дисциплина “Квантова информация” дава реален пример за процесите на диференциация и интеграция в съвременната наука.

Същевременно показва появата на напълно нова и неподозирана предна линия и открито поле за експерименти и теории, нова област от реалността и човешкото знание, която също така обещава и поразителни технически приложения.

Квантовата криптография също така е основана на теоремата за неклониране на квантов обект. Теоремата за неклонирането, според която всеки квантов обект е уникален в смисъл, че е невъзможно да му се създаде точно копие, “клонинг”, има важни фундаментални, така и приложни – в областта на квантовата криптография – импликации. Следствие от теоремата за неклониране или еквивалентна на нея е теоремата за неизчистване, т.е. квантовият обект не може да бъде унищожен, “изчистен”, точно както не може да бъде и дублиран: при унищожаването му тук, той само се премества някъде другаде. Подслушването, за чието затрудняване или осуетяване, се въвежда криптографирането, т.е. зашифроването на едно съобщение, в крайна сметка се базира на факта, че класическата информация може да бъде дублирана: подслушаната информация е тъкмо такова точно копие на предаваната по тайни канали информация. Следователно, ако в качеството на таен канал се използва квантов (т.е. основаващ се на явленията сдвояване, на топологичната неотделимост), то, поради теоремата за неклонирането, той не може да бъде подслушван, или по-точно, всяко подслушване има за следствие изкривяване на предаваното съобщение, поради което детектирането на такива изкривявания води до разкриване на подслушването. Квантова криптография е единствената област от квантовата информация, за която се твърди, че е достигнала степен на практическо приложение.

ЛИТЕРАТУРА

[1]. Баргатин И. В. Запутаннье квантовье состояния в атамньх систем, УФН 171, 2001

[2]. Бауместер Д. Физика квантовой информации. М. Постмаркет 2002

[3]. Доронин С. И. Квантовая магия, С. Петербург,2007

[4]. Stela Ruseva, Distributed attacks denial of service type. Nature of these attacks and Defense against them, computerScience ’08 2008 conference, Kavala, Greece, September 17-20 2008

[5]. Zarek W. H. Decoherence, einselection and the quantum origins of the classical. Rev. Mod. Phys. 75, 2003

ASPECTS OF THE APPLICATION OF QUANTUM CRYPTOGRAPHY TO PROTECT DATA IN INFORMATICS

Hristina Spiridonova, Antonio Andonov
hristinaspiridonova@abv.bg, andonov@vtu.bg

Todor Kableshkov University of Transport
158 Geo Milev Str., Sofia 1574
BULGARIA

Key words: *information security, quantum cryptografy*

Abstract*: In the past twenty years, the quantum properties of matter and light have been applited to the field of information security. Research has advanced to the point that actual daveced using quantum properties are transmitting information over considerable distances. At this time, transmission speeds and hardware expense have generally limited the use of quantum devices to distribute keys rather than entire messages. These is controversy about how secure quantum messages are. It is possible to prove that the probability of message interception by an adversary is arbitrarily small, under ideal conditions. People and machines, however, can never be perfect so ther are many approaches to defeating quantum encryption. Some computer security experts have wondered why making the strongest link in a system event stronger will improwe security overall. Since public key cryptography is so hard to decipher now why spend so much time and money on an even more secure quantum encryption scheme. If deciphering is nearly impossible, why not use other techniques, sudi as social engineering, to eavesdrop. This paper will attempt to answer those questions*