Тема по квантова информатика:
Квантова Криптография
Quantum Cryptography

Иван Михов
ФН:82139

2023-02-18

Съдържание

1 Основни принципи на Криптографията

Криптографията е наука за предпазване на частна информация от неоторизиран достъп, за осигуряване на цялостта и автентичността на данните. За да се постигне тази цел, се използва криптиране: съобщение се комбинира по алгоритъм с допълнителна секретна информация, за да се получи криптограма.
В традиционната терминология Алис е страната, която криптира и предава съобщението, Боб - този, който го получава, а Eve - злонамереният подслушвач. Но криптографската технология, която се използва днес, разчита на трудността на някои математически задачи. Класическата криптография е изправена пред следните два проблема. Първо, сигурността на много класически криптосистеми се основава на трудността на проблеми като факториране на цели числа или задачата за дискретния логаритъм. Но тъй като тези проблеми обикновено не са доказано трудни, съответните криптосистеми са потенциално несигурни. Например, известната и широко разпространена използваната криптосистема с публичен ключ RSA би могла лесно да бъде разбита, ако големите цели числа са лесни за факториране. Трудността на факторирането на цели числа обаче не е доказан факт, а по-скоро хипотеза.
Второ, теорията на квантовите изчисления даде нови методи за справяне с тези математически проблеми по много по-ефективен начин . Въпреки, че все още има многобройни предизвикателства, които трябва да бъдат преодолени, преди да бъде създаден работещ квантов компютър с достатъчна мощност, на теория много класически шифри могат да бъдат разбити от такава мощна машина.
Квантовата Криптография (КК), докато квантовите изчисления изглеждат сериозно предизвикателство за класическата криптография във възможно не толкова далечно бъдеще, в същото време то предлага нови възможности за изграждане на методи за криптиране, които са безопасни дори срещу атаки, извършени с помощта на квантов компютър. Квантовата Криптография (КК) разширява възможностите на класическата криптография, като защитава тайната на съобщения, използвайки физическите закони на квантовата механика.
Идеята за QC е предложена за първи път едва през 70-те години на миналия век от Stephen Wiesner (1983 г.) и от Чарлз Х. Бенет от IBM и Жил Брасар от университета в Монреал (1984, 1985 г.) QC използва принципите на квантовата механика за реализиране на криптографска система. Ключовият проблем, който се решава чрез използване на квантови техники, е откриването на подслушване. Квантовите принципи могат да се използват за вероятностно откриване на подслушване, когато то се случи. В QC битовете се представят като кюбити, които могат да бъдат моделирани като фотони или електрони и се предават по квантов канал. Обикновено поляризационните състояния на кюбитовити представляват 0 и 1.

2 Хилбертови пространства

За да разберем по-добре квантовата криптография, първо трябва да разбираме математическите принципи, на които тя се уповава.
Затова нека започнем от Хилбертови пространства. Хилбертовото пространство не е нищо друго освен векторно пространство над комплексните числа $\mathbb{C}$ с комплексно оценено вътрешно произведение, определено от :

$$(\_,\_) \ : \ \mathbb{H} \ \times \ \mathbb{H} \ \rightarrow \ \mathbb{C}$$

който е пълен по отношение на нормата : $||u|| = \sqrt{(u,u)}$
Трите основни аксиоми, на които отговаря едино вътрешено произвединие, са следните:
1. Позитивна определеност : $(u,u) = 0$ и $(u,u) = 0$, ако $u = 0$
2. Конюгатна симетрия : $(u,v) = (v,u)^*$
3. Линейност по втория аргумент: $(u, v+w) = (u,v) + (u,w)$
В квантовата система елементите на хилбертовото пространство $\mathbb{H}$ се наричат вектори на състояние. Те биват обозначавани с $|$етикет$>$, където "етикет"е просто някакъв избран елемент. Можем да дефинираме $\mathbb{H}^*$ като множеството от всички възможни хомоморфизми на $\mathbb{H}$ в Хилбертовото пространство на всички комплексни числа.

$$\mathbb{H}^* \ = \ Hom_c(\mathbb{H} \ , \ \mathbb{C})$$

Елементите на $\mathbb{H}^*$ се наричат bra вектори или за по-кратко просто bra.

3 Базиси на Хилбертово пространство

Състоянията на една квантова система се представят чрез вектори на състоянието в Хилбертово пространство $\mathbb{H}$. Два вектора $|\alpha>$ и $|\beta>$ в Хилбертовото пространство се предполага, че представят едни и същи квантовомеханични състояния ако съществува ненулево комплексно число λ , такова че :
$|\alpha>=\lambda|\beta>$.
За всяко Хилбертово пространство можем да дефинираме ортогонален базис и всяко състояние в Хилбертовото пространство може да се изрази като линейна комбинация от този базис. И също така за определено Хилбертово пространство могат да съществуват няколко ортогонални базиса. За пример - да разгледаме пространството на Хилберт представящо поляризацията на един фотон. Всеки различен вектор на състояние символизира равнина на поляризация на светлината. Това Хилбертово пространство може да има различни възможни ортогонални базиси, като например праволинейния базис ($|\updownarrow>, |\longleftrightarrow>$), базис на въртене ($|\curvearrowright>, |\curvearrowleft>$), диагонален базис ($|\ \nearrow>, |\nwarrow>$) и така нататък.

4 Кюбитове

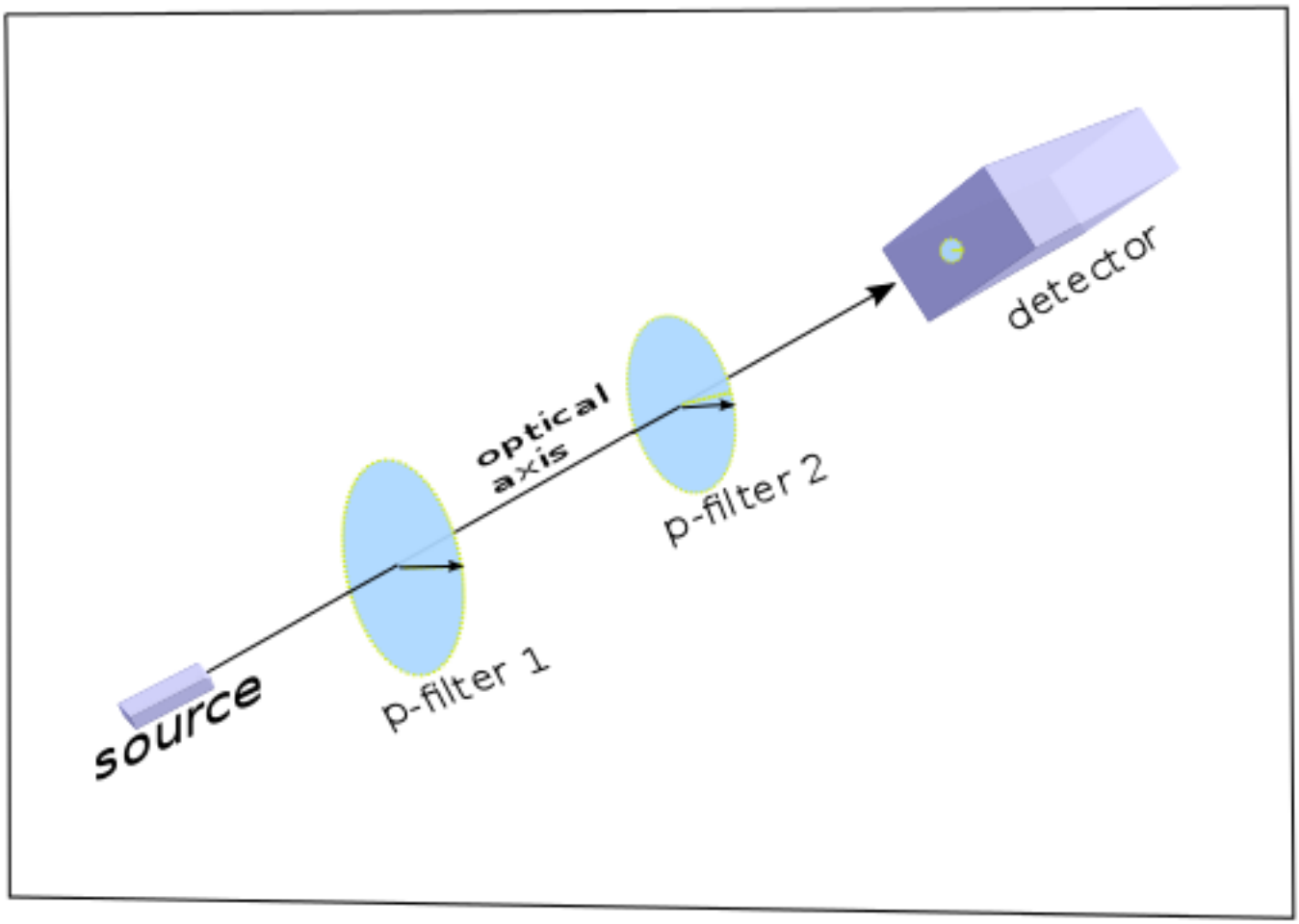
Най-значимата единица информация в компютърните науки е бит. Съществуват два възможни стойности, които могат да бъдат записани в един бит: битът е равен на "0"или на "1". На практика тези две различни състояния могат да бъдат представени по различни начини, например чрез прост превключвател или чрез кондензатор.
Квантовият аналог на бита се нарича кюбит, който произлиза от квантов бит.
Кюбитът ($|\alpha>$) е елемент от двуизмерното Хилбертово пространство $\mathbb{H}^*$, в което можем да въведем ортонормиран базис, състоящ се от двете основни състояния $|0>$ и $|1>$. Това е основната изчислителна единица в квантовия компютър.Физически кюбитът може да се разглежда като електрон във водороден атом или поляризацията на светлинна частица. Съществуват две възможни състояния, в които може да се намира електронът във водородния атом: заземено и възбудено състояние.Заземеното състояниесъответства на стойността на кюбита, когато е 0, а възбуденото състояние съответства на 1, което може да бъдат последователно представени като $|0>$ и $|1>$.

$$|\alpha>= a_0|0> +a_1|1>$$

където a_0 и a_1 са комплексни коефициенти и $|a_0|^2+|a_1|^2 = 1$, което обозначава абсолютната стойност. Това означава, че ако се направи измерване на състоянието на електрона, то вероятността да е $|0>$ е равна $|a_0|^2$, а вероятността да е $|1>$ е $|a_1|^2$.

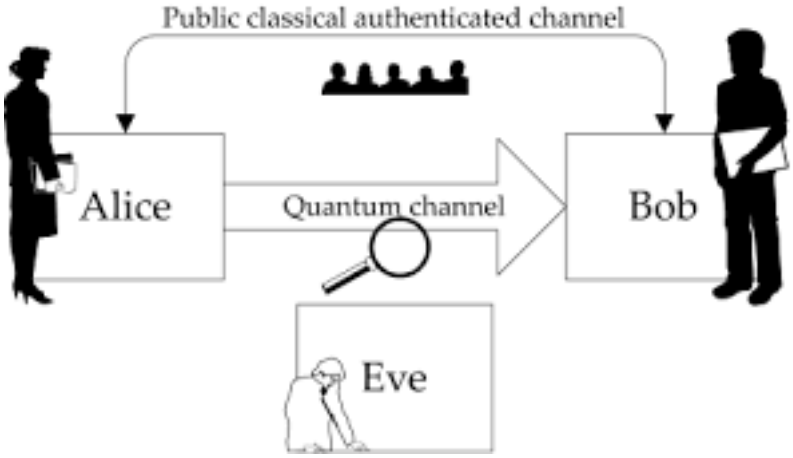
5 Квантова Криптография

Преди да пристъпим към самия алгоритъм за квантово криптиране първо трябва да обясним как работи то.
Затова нека дефинираме нужната информация за криптографията.
Фотоните във физиката са светлинни частици, но тук ще ги разглеждаме като носители на електромагнитно поле.
Хилбертово пространство $\mathbb{H} = \mathbb{H}_{ext} \bigoplus \mathbb{H}_{int}$, където $\mathbb{H}_{ext}$ описва външната информация на фотона, а $\mathbb{H}_{int} = \mathbb{C}^2$ описва вътрешната информация на фотона.
Поляризация - Степента на свобода на светлината, наречена поляризация, е ефект, свързан със пречупването на фотона, и е квантовомеханичен ефект.

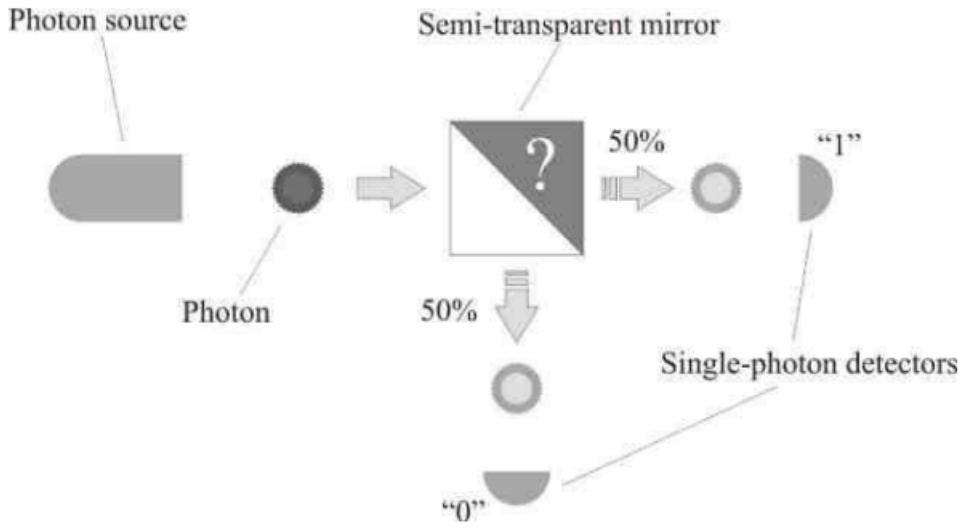


Квантово състояние:= фотон с линейна поляризация по произволна ос в равнината определена от векторите $\vec{E}$ и $\vec{H}$
Базиси на Хилбертовото пространство $\mathbb{H}$:
първи базис: „+“ $= \{|0>, |1>\}$, правоъгълен базис
$\psi = \alpha|0> + \beta|1>, \alpha \ \& \ \beta \in \mathbb{C}, \ |\alpha|^2 + |\beta|^2 = 1$
$|0>$ - фотон с поляризация по оста x
$|1>$ - фотон с поляризация по оста y
Втори базис "x" $= \{|+>, |->\}$
$|+> = \frac{1}{\sqrt{2}}(|0> + |1>)$
$|-> = \frac{1}{\sqrt{2}}(|0> - |1>)$
$|+>=$ фотон с поляризация под ъгъл 45°
$|->=$ фотон с поляризация под ъгъл 135°
Ако фотонът е поляризиран хоризонтално или вертикално, а измерването е направено в базиса "$\times$ то всички получени вероятности не могат да различат състоянията с хоризонтална поляризация от тези с вертикална, т.е., не може да се каже дали състоянието е било $|0>$или $|1>$
В допълнение, след измерването на фотон описван с $|+->$ в базиса „+“ поляризацията му става хоризонтална, ако е настъпило събитието P_0, или вертикална ако е настъпило P_1, т.е., фотонът напълно „забравя“ своята начална поляризация и преминава респективно в състоянието $|0>$или $|1>$

6 QKD протокол Bennett-Brassard 1984 (BB84)



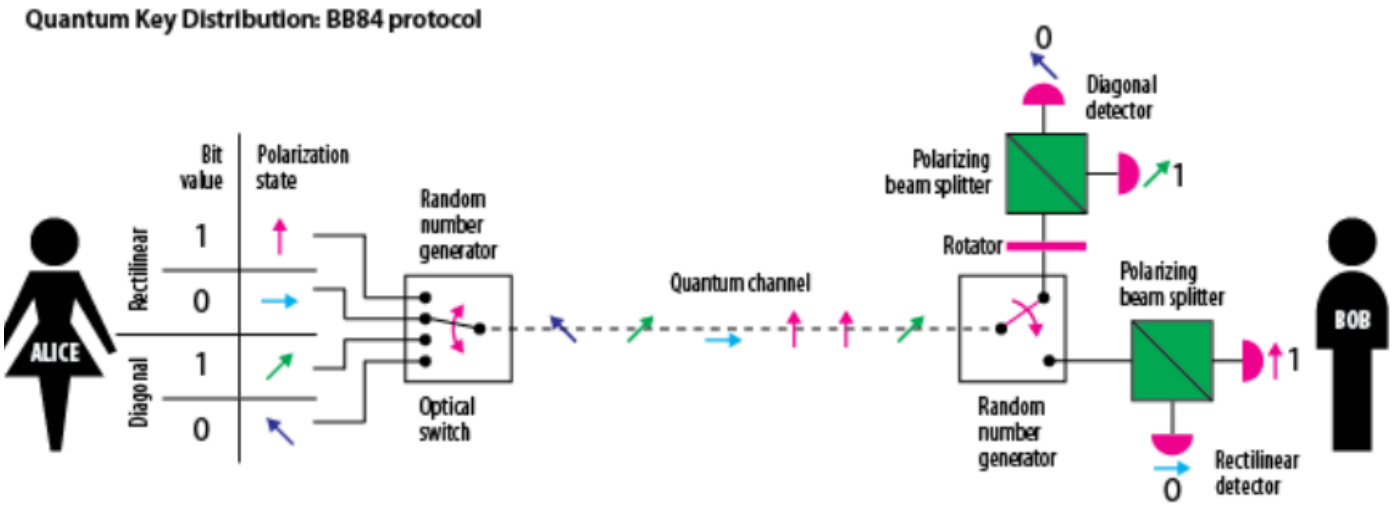
Квантов генератор на случайни числа : Генераторите на случайни числа, които използват квантови източници, за да създадат надежден източник на случайност, са известни като квантови генератори на случайни числа.



:
Това са стъпките на криптографския алгоритъм BB84:

1. Alice използва квантов генератор на случайни числа за да генерира случайна последователност
01100111000101010001110001110 0
За всеки бит Alice избира случайно в кой от двата базиса "+"или "×"да поляризира фотоните, които изпраща на Bob.
2.Ако базисът е "+ тогава поляризацията е:
$0 = \leftrightarrow$ или $1 = \updownarrow$
3. Ако базисът е ×, тогава поляризацията е
$0 = \nwarrow\searrow$ или $1 = \nearrow\swarrow$
Стъпки на Боб
1. Bob приема фотоните изпратени по квантовия канал от Alice и за всеки от тях решава случайно дали да ги измери в базис + или × чрез завъртане на поляризатора пред детектора

2. Bob записва резултатите от измерванията за всеки фотон заедно с типа + или × на поляризатора; резултатите са:
• 0 ако е регистрирал детектора за хоризонтална поляризация при поляризатор в базис +
• 1 ако е регистрирал детектора за вертикална поляризация при поляризатор в базис +
• 0 ако е регистрирал детектора за поляризация 135° при поляризатор в базис ×
• 1 ако е регистрирал детектора за поляризация 45° при поляризатор в базис ×
Bob се обажда на Alice по телефона и за всеки бит съобщава в кой базис е мерил, без да споменава резултатът от измерванията
Alice потвърждава номерата на битовете, за които базисът на Bob съвпада с нейния и тези битове стават основата на секретния ключ



Quantum transmission & detection	ALICE sends photons	↖	↗	→	↑	↑	↗	↖	↑
	ALICE's random bits	0	1	0	1	1	1	0	1
	BOB's detection events	↑	↗	↖	↑	↗	↗	↖	↖
	BOB's detected bit values	1	1	0	1	1	1	0	0
Public discussion (i.e., sifting)	BOB tells ALICE the basis choices he made	Rect	Diag	Diag	Rect	Diag	Diag	Diag	Diag
	ALICE tells BOB which bits to keep		✔		✔		✔	✔	
	ALICE and BOB's shared sifted key	–	1	–	1	–	1	0	–

• Eve измерва ∀ фотони с номера от 1 до 8
  • Базиси: +, × , + , ×, +, ×, +, ×
• Резултат: 1, 1 , 0 , 0 , 1 , 1, 1, 0
• Споделен ключ A & B: - , 1 , - , 1 , - , 1, 0, -
• Проектирано състояние (Bob): ↕ , ↗ ,↔, ↖ , ↕ , ↗, ↕ , ↖
• Резултат Bob and E: 1 , 1 , 0 , 0 , 1 , 1, 0 , 0
• Намесата на Eve: 25 % разминаване

Тест за подслушване
Alice и Bob се договарят и споделят по публичния канал подредица на вече установения секретен ключ, която след публикуването се изважда от ключа.
• Идеален канал: ако подредицата избрана от Alice и Bob е идентична, останалата част от споделената редица се приема за окончателен споделен ключ. Ако подредиците не са идентични - налице е подслушване. Процедурата започва отначало.

• Шумен канал: ако подредицата избрана от Alice и Bob съдържа повече грешки от допустимата грешка на канала (която се определя от характеристиките на квантовия канал), се предполага, че е имало подслушване. В противен случай остатъка от редицата от битове се приема за окончателен ключ.

Корекция на грешките
• В реалността квантовият канал е „шумен“ и тогава може да се окаже, че Alice и Bob притежават различни ключове след споделянето на ключа.
• Един възможен изход е Alice да използва класически методи за корекция на грешки (напр. Repetition code) преди да изпрати битовете по квантовия канал.
• По време на фазата за корекция на грешки Alice изпраща на Bob информация за начина на кодиране,така че Bob също да може да приложи метода за декодиране.
• Накрая Alice и Bob би трябвало да споделят един и същи секретен ключ.

Забрана за копиране
• Измерване: проекционен постулат необратима пертурбация на квантовото състояние
• Предаване на измереното състояние: загуба на първоначалната информация
• Копиране преди измерването
• No-cloning theorem:
Не може да бъде копирано неизвестно квантово състояние.
• Не е възможно да се придобие информация разграничаваща неортогонални състояния без да бъдат пертурбирани (само разложими състояния)
Но остава един проблем :
Eve все още може да има доста информация за ключа, който Алис и Боб споделят. Усилването на поверителността е инструмент за справяне с такъв случай.
То работи по следния начин :
Избираме по кратък двоичен низ s от по-дълъг, но по-малко секретен низ s'.

7 Заключение

Криптографията е наука, която е много важна за нашия онлайн и ежедневен живот. Тя ни дава сигурност, че имуществото ни, личната ни информация и важни за нас неща няма да бъдат достъпени от неприятели. Със зараждането на квантовите компютри всяка една защита, която сме имали, ще падне, затова макар и да не е в краен стадий на развитие Квантовата криптография е изключително важна за бъдещето на нашето общество, защото как бихме живели, ако знаем че всичко най-важно за нас не е защитено?