量子计算理论和应用的初步调研报告

孙晋茹,王霓,董宇

(Dated: 2013年5月28日)

人类跨入了21世纪,信息科学面临着新的挑战.计算机是否存在极限的运算速度?能否实现不可破译、不可窃听的保密通信?诸如此类的问题成为科学家们关注的重要课题.创建新一代高性能的、安全的计算工具和通信技术当前研究的热点,其中量子计算成为了最被关注的领域,无论是从学术的角度还是发展的角度,了解其基本的原理和应用都是很有必要的.

I. 引言

Alan Turing于1936年提出通用计算机即Turing机的概念,宣告了现代计算机科学的产生.最近几十年,计算机伴随着半导体工业的发展在性能上有突飞猛进的进展.然而在有限体积中所容纳的器件数量增加时它的功能开始受到量子效应的干扰.同时,随机性算法对传统的确定性的Turing机构成了挑战,认为任何算法过程均可以用Turing机有效模拟这一命题的正确性受到质疑.因此,未来计算机的方向必然是寻找与传统不同的计算模式.1985 年,David Deutsch 试图提出了一种能够有效模拟任意物理系统的计算装置,这一装置考虑了量子力学原理.不仅如此,Deutsch还举出了一个例子,其中采用了基于量子力学原理的算法,指出量子计算机可能在计算能力上超过经典计算机.虽然量子计算/量子信息目前仍处于起步阶段,但已经有了许多重要的进展,并且必将随着技术水平的发展占据更加重要的地位.

本报告的前两部分分别介绍了量子计算机的基本原理和初步的量子算法简介,概括性地展示了现代量子计算领域的方向和特点.第三部分则选择量子计算最为重要和最引人注目的课题之一,即量子加密进行了简要说明,作为一个量子计算/量子信息的应用性实例.

II. 量子计算机

如果像摩尔定律指出的那样,微处理器上的晶体管数目保持每18个月翻一番,那么到2020或2030年微处理器上的线路就会到达原子水平了,顺理成章的下一步将是建造量子计算机,充分驾驭原子和分子的能力,将其用于存储和计算工作,量子计算机在进行某些计算的时候可以比任何硅基计算机快出很多.

量子计算机是一类遵循量子力学规律进行高速数学和逻辑运算、存储及处理量子信息的物理装置.当某个装置处理和计算的是量子信息,运行的是量子算法时,它就是量子计算机.量子计算机的概念源于对可逆计算机的研究.研究可逆计算机的目的是为了解决计算机中的能耗问题.

早在六七十年代,人们发现，能耗会导致计算机芯片的发热,影响芯片的集成度,限制了计算机的运行速度,能耗产生于计算过程中的不可逆操作.例如,对2比特的异或操作,因为只有1 比特的输出,这一过程损失了一个自由度,因此是不可逆的,按照热力学,必然会产生一定的热量.但这种不可逆性是不是不可避免的呢?事实上,只要对异或门的操作如左图所示的简单改进,即保留一个无用的比特,该操作就变为可逆的.因此物理原理并没有限制能耗的下限,消除能耗的关键是将不可逆操作改造为可逆操作.后来Bennett证明了所有经典不可逆的计算机都可以改造为可逆计算机,而不影响其计算能力.

因为计算机中的每步操作都可以改造为可逆操作,在量子力学中,它就可以用一个幺正变换来代表.Benioff最早用量子力学来描述可逆计算机.在量子可逆计算机中,比特的载体成为二能级的量子体系,体系处于$|0>$和$|1>$上,但不处于它们的叠加态,量子可逆计算机的研究,其核心任务为,对应于具体的计算,寻找合适的哈密顿量来描述.

早期的量子可逆计算机,实际上是用量子力学语言表述出来的经典计算机,它没有利用量子力学的本质特性,如量子叠加性和相干性.这些量子特性可能在未来的量子计算机中起本质作用,如用来模拟量子系统,量子计算机存在多项式算法(多项式算法指运算完成的时间与输入二进制数据的长,即比特的位数存在多项式关系),而经典计算机则需要指数算法.但最具轰动性的结果却是Shor给出的关于大数因子分解的量子多项式算法,因为此问题在经典公钥体系中有重要应用.Shor的发现掀起了研究量子计算机

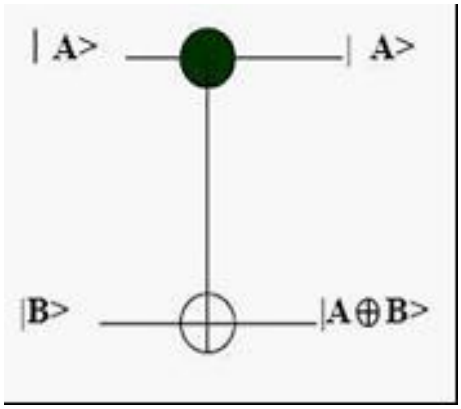

FIG. 1. 量子门

的热潮,从此后,量子计算机的发展日新月异.

在计算机的经典模型中,最基础的构建要素-比特,只能存在于两种截然不同的状态之一:0或是1.在量子计算机中,规则改变了.一个原子比特-经常被简称为“量子比特”(quantum bit) -不仅仅存在于传统的0和1状态中,还可以是一种两者连续或重叠状态.当一个量比处于这种状态时,它可以被认为存在于两种领域中:一种为0,而另外一种为1, 一个基于这种量比的操作能够同时有效地影响两个值。因此，极为重要的一点是：当我们在量比上实行单一操作时，我们是在针对两种不同的值进行的。类似的，一个双量比系统能对4个值进行操作，而一个三量比系统就是8个值.因此,增加量比的数目能够以指数方式增加我们从系统获得的“量子并行效应”.在拥有正确算法类型的情况下,它能通过这种并行效应以远低于传统计算机所花费的时间内解决特定的问题.根据这一性质,量子计算机的输入态和输出态为一般的叠加态,其相互之间通常不正交.量子计算机中的变换为所有可能的幺正变换.得出输出态之后,量子计算机对输出态进行一定的测量,给出计算结果,从另一个角度讲,在经典计算机里,一个二进制位只能存储一个数据,n个二进制位只能存储n个一位二进制数或者1个n位二进制数;而在量子计算机里,一个量子位可以存储两个数据,n个量子位可以同时存储2n个数据,从而大大提高了存储能力.

由此可见,量子计算对经典计算作了极大的扩充.

但量子计算机依赖于原子尺度的运动也带来了一些问题,量子计算机对受量子机械规律决定的奇异的亚原子事件的依赖很大,而这也使它非常脆弱和难以控制.例如,假想一个处于连续状态的量比,一旦它和环境发生了可调节的相互影响,它就将脱散并落入两种传统状态中的一种,这就是脱散性问题.它已经成为了量子计算机作为建立在由连续性状态所带来的量子并行效应上的潜在力量的绊脚石.

目前,量子计算机的研发主要涉及如下三项关键技术:量子编码、量子算法和量子硬件技术.

（1）量子编码

量子编码用于解决可靠性、纠错、避错、防错问题.量子信息论中,信息的载体不再是经典比特,而是一个一般的二态量子体系,这二态量子体系,可以是一个二能级的原子或离子,也可以是一自旋为1/2的粒子或具有两个偏振方向的光子,所有这些体系,均称为量子比特.区别于经典比特,量子比特可以处于0、1两个本征态的任意叠加态,而且在对量子比特的操作过程中,两态的叠加振幅可以相互干涉,这就是所谓

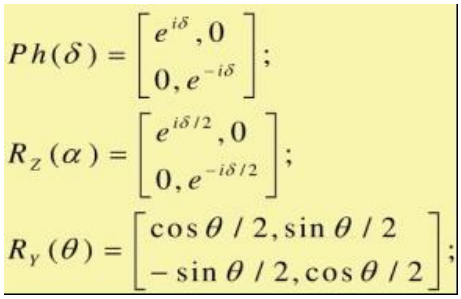

FIG. 2. 量子逻辑门的矩阵表示

的量子相干性.已经发现,在量子信息论的各个领域,包括量子计算机、量子密码术和量子通信等,量子相干性都起着本质性的作用.可以说,量子信息论的所有优越性均来自量子相干性.但受环境的影响,量子状态十分不稳定,不管是外部噪音还是观测都会形成对量子状态的干涉,使存储在量子计算机内的信息崩溃,导致计算错误.比如,当观测一个量子状态时,该状态会立即塌陷为某个确定传值(0或1).这种现象在量子物理上叫做脱散,是量子的固有性质.由此可见,量子计算非常脆弱,非常容易出错,并且随着机器规模的增大,计算的可靠性急剧下降,使制造规模大的量子计算机变得十分困难,研究人员必须设计一种方法,将脱散和其它潜在错误源控制在可接受的水平.这就是困扰整个量子信息论的消相干问题.因此，要使量子计算成为现实,一个核心问题就是克服消相干.

量子编码是迄今发现的克服消相干最有效的方法.主要的几种量子编码方案是:量子纠错码、量子避错码和量子防错码.量子纠错码是经典纠错码的类比,是目前研究的最多的一类编码,其适用范围广,但效率不高.量子避错码和量子防错码有别于量子纠错编码,这些方案防错而不纠错,它们本质性地利用了量子比特消相干过程中的合作效应.

（2）量子算法

量子算法是加速运算的关键(主要不靠器件速度与集成度).到目前为止,人们才找到两个比较成功的量子算法:Shor算法和Grover算法.未来还需要更多能解决实际重大问题的量子算法,以证明在哪些问题上量子计算机的确比传统计算机要优越.

下面举一个例子来说明量子算法的优越性,假设现在我们想求一个函数f(n),(n＝0 7)的值,采用经典计算的办法至少需要下面的步骤:

存储器清零→赋值运算→保存结果→再赋值运算→再保存结果... 对每一个n都必须经过存储器的赋值和函数f(n)的运算等步骤,而且至少需要8个存储器来保存结果.如果是用量子计算机来做这个题目则在原理上要简洁的多.只需用3个量子存储器,把各q-bit制备到$(|0>+|1>)/(\sqrt{2})$态上就一次性完成了对8个数的赋值,此时存储器成为态$|\phi>$,然后对其进行相应的幺正变换以完成函数f(n)的功能,变换后的存储器内就保存了所需的8个结果.这种能同时对多个态进行操纵,所谓“量子并行计算”的性质正是量子计算机巨大威力的奥秘所在.

（3）量子硬件技术

要实现量子计算机,最重要的一点就是量子门的应用.在量子计算和特别是量子线路的计算模型里面,一个量子门是一个基本的,操作一个量子比特的量子线路.它是量子线路的基础,就像传统逻辑门跟一般数字线路之间的关系.但十分重要的一点是,与多数传统逻辑门不同,量子逻辑门是可逆的.例如恒等变换、求非变换、相位移动变换及异或变换量子门的作用等都可以通过矩阵形式表示出来,如FIG.2.所示.将量子门按某种方式连接,构成量子网路,以进行复杂的运算.

近几年,科学界已研发了多种量子器件,新品迭出,为量子计算机的研制创造了条件.这些量子器件有如下种类:①量子晶体管,②量子存储器,③量子阱激光器,④量子效应器件等.

III. 量子算法的初步介绍

量子算法目前仅仅处于起步阶段,甚至找到一个能够实际解决的问题都很困难.然而,目前所提出的量子算法在复杂度上的优越性已经让人认识到其巨大的潜力.总的来说,有三类由于已知的经典算法的量子算法.其一是基于量子情况下的Fourier变换的一类算法,代表为Deutsch-Jozsa算法;第二类是量子搜索算法;第三类是用量子计算机模拟量子系统的量子仿真.由于这里是对量子算法的初步介绍,因此仅仅介绍和量子算法基本思想关联比较紧密的前两类算法.然而,并不是说量子仿真并不重要,实际上,量子仿真的过程有可能大大拓展已知的计算模型,并且可以启发我们发现新的量子算法.

量子算法比起经典算法的优势最突出的一点就是并行性,量子并行性也因此是许多的量子算法的基本特征.下面首先说明量子门和量子并行性的概念.

量子比特可以直接对应于某个状态,可以用Dirac符号表示.量子门可以对量子比特进行作用,对量子门唯一的要求是必须满足幺正性.单比特量子门有很多种,用得最多的两种是Z门和Hadamard门.Z门的作用是保持$|0>$不变,而使$|1>$变为$-|1>$.写成矩阵形式为:

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$$

Hadamard门把$|0>$变为$|0>$和$|1>$之间的中间状态$(|0>+|1>)/\sqrt{2}$, 把$|1>$变为$|0>$和$|1>$之间的中间状态$(|0>-|1>)/\sqrt{2}$.Hadamard 门可以写作矩阵形式:

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$$

对于多量子比特量子逻辑门,其原型为受控非门.如果控制量子比特置0,则目标量子比特保持不变.若控制量子比特置为1,则目标量子比特将翻转.即$|00>\rightarrow|00>$,$|01>\rightarrow|01>$,$|10>\rightarrow|11>$,$|11>\rightarrow|10>$.它可以看作是经典异或门的推广,总结为$|A,B>\rightarrow|A,A\oplus B>$.

设$f(x):0,1\rightarrow 0,1$.在量子计算机上表示这一函数的方法是,考虑初态为$|x,y>$的双量子比特的量子计算机,通过某种逻辑门序列,把状态变换为$|x,y\oplus f(x)>$.考虑FIG.3.的量子线路,数据寄存器中是叠

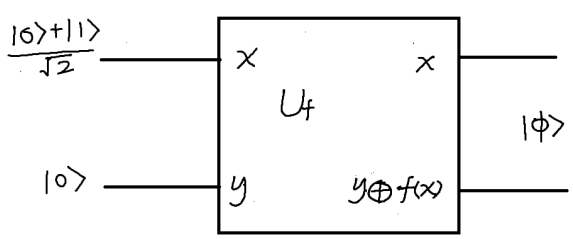

FIG. 3. 同时计算f(0)和f(1)的量子线路

加态$\frac{(|0,f(0)>+|1,f(1)>)}{\sqrt{2}}$,由Hadamard门作用到$|\ 0>$态上得到.

同样考虑多量子态,利用Hadamard变换,即n个Hadamard门同时作用到n个量子比特上,可以产生所有计算基态的平衡叠加,并且效率很高,我们以$H^{\otimes n}$表示n个Hadamard门的并行作用.这样,n 比特输入x 和单比特输出f(x)的函数表示可以利用n+1量子比特的状态$|\ 0>^{\otimes n}|\ 0>$,对前n位进行Hadamard变换,紧接着经过实现映射f(x)的量子线路U_f,产生状态$\frac{1}{2^n}\sum_x |\ x>|\ f(x)>$.

首先介绍Deutsch算法和Deutsch-Jozsa算法.

输入状态$|\ \phi_0>=|\ 01>$,通过并列的Hadamard门,得到状态$|\ \phi_1>=[\frac{|0>+|1>}{\sqrt{2}}][\frac{|0>-|1>}{\sqrt{2}}]$.$U_f$作用在$|\ \phi_1>$得到$|\ \phi_2>$.为了得到$|\ \phi_2>$的值,考虑$U_f$对状态$|\ x>(|\ 0>-|\ 1>)/\sqrt{2}$作用,得到状态$(-1)^{f(x)}\times|\ x>(|\ 0>-|\ 1>)/\sqrt{2}$.所以:

$$|\ \phi_2>=\begin{cases}\pm[\frac{|0>+|1>}{\sqrt{2}}][\frac{|0>-|1>}{\sqrt{2}}] & f(0)=f(1)\\ \pm[\frac{|0>-|1>}{\sqrt{2}}][\frac{|0>-|1>}{\sqrt{2}}] & f(0)\neq f(1)\end{cases} \tag{1}$$

Hadamard门作用在并列的两个量子比特中的前一个上.得到:

$$|\ \phi_3>=\begin{cases}\pm|\ 0>[\frac{|0>-|1>}{\sqrt{2}}] & f(0)=f(1)\\ \pm|\ 1>[\frac{|0>-|1>}{\sqrt{2}}] & f(0)\neq f(1)\end{cases} \tag{2}$$

或者:$|\ \phi_3>=\pm|\ f(0)\oplus f(1)>[\frac{|0>-|1>}{\sqrt{2}}]$.这个结果充分展现了量子并行性和经典算法的区别.经典计算机尽管可能实现一半的概率计算f(0),一半的概率计算f(1),然而这两者不会同时出现.但是对于量子计算机就不同了,这里展现的是一个相互干涉的结果.仅通过一次计算,就可以了解体系的某些整体特征.

Deutsch-Jozsa算法是用来解决Deutsch问题的量子算法,也是表现出量子算法优越性的例子之一.Deutsch问题可以描述为这样的游戏.Alice从0到2^n-1的数中任意选取一个x,把它寄给Bob.Bob根据这个数,通过一个算法得出f(x),并把它寄给Alice.Bob的算法这可能是以下两者之一:其一是f(x)对于所有

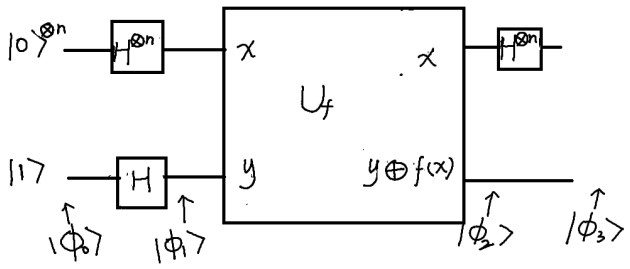

FIG. 4. Deutsch-Jozsa算法的量子线路

的x都是常数;其二是f(x)恰好使一半的x取1,使另一半的x取0,称为平衡的.Alice最快能在几次通信后判断Bob使用的是何种算法?

经典情形下,Alice一次只能发给Bob一个x,因此最坏情况下,Alice至少要询问Bob$2^n/2-1$次,才能判断出Bob是否使用的是平衡算法.但是如果Alice和Bob交换的是量子比特,并且Bob使用的是量子线路U_f来进行f(x)操作,一次通信就可以达到目的.

类似于Deutsch算法,只是Alice使用的是n+1量子比特.前n个量子比特作为寄存器存储她的输入,而最后一个单量子比特寄存器用来存储Bob的答案.Bob用并行性量子线路得到答案后并放入寄存器后,Alice利用Hadamard变换查询寄存器的状态.

具体过程如FIG.4.所示.最初输入的的量子态$|\ \phi_0\ >=|\ 0\ >^{\otimes n}|\ 1\ >$,经过了并列的Hadamard变换后,变为$|\ \phi_1\ >=\sum_{x\in\{0,1\}^n}\frac{|x>}{\sqrt{2^n}}[\frac{|0>-|1>}{\sqrt{2}}]$.经过$U_f$的作用后,给出$|\ \phi_2\ >=\sum_{x\in\{0,1\}^n}\frac{(-1)^{f(x)}|x>}{\sqrt{2^n}}[\frac{|0>-|1>}{\sqrt{2}}]$.

Alice想要从这个状态得到Bob的算法是什么,再次利用了Hadamard变换.先单纯地考察Hadamard变换的数学性质,有如下的结论.对于单量子比特,有$H\mid x>=\sum_z(-1)^{xz}\mid z>/\sqrt{2}$.那么多量子比特的情况也是类似的:

$$H^{\otimes n}\mid x_1,\cdots,x_n>=\sum_{z_1,\cdots,z_n}(-1)^{x_1z_1+\cdots+x_nz_n}\mid z_1,\cdots,z_n>/\sqrt{2^n} \tag{3}$$

或者写成$H^{\otimes n}\mid x>=\sum_z(-1)^{xz}\mid z>/\sqrt{2^n}$.得到这个结果后,可以知道Alice使用Hadamard变换后得到的状态为:

$$|\ \phi_3\ >=\sum_z\sum_x\frac{(-1)^{x\cdot z+f(x)}\mid z>}{\sqrt{2^n}}[\frac{|\ 0>-|\ 1>}{\sqrt{2}}] \tag{4}$$

Alice对她得到的状态进行查看,发现$|\ 0\ >^{\otimes n}$的幅度为$\sum_x(-1)^{f(x)}/2^n$.f为常数,$|\ 0\ >^{\otimes n}$的系数平方为1,所以其他所有幅度为0.所以测量到的所有量子比特位均为0.如果测量到的量子比特位存在不为0的

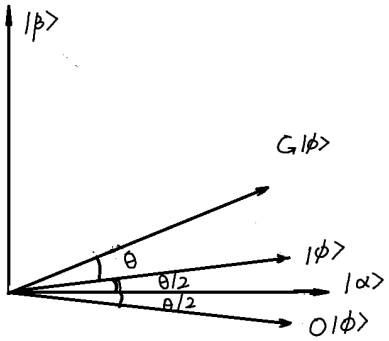

FIG. 5. 一次Grover迭代的示意图

情况,则函数是平衡的.

量子搜索算法和Deutsch算法有所不同,为了较为普遍地描述这一问题而引入了被称为oracle的黑箱机制.在避免讨论oracle的内部机制的前提下,只需知道对于满足某些条件的x,oracle会给出相应的输出值.在量子搜索算法中,oracle的作用可以简化为:$\mid x>\rightarrow o(-1)^{f(x)} \mid x>$.oracle通过改变解的相位标记了搜索问题的解.

算法从计算机的初态$\mid 0>^{\otimes n}$,用Hadamard变化使得计算机处于均匀叠加态:

$$\mid \phi>=\frac{1}{N^{1/2}}\sum_{x=0}^{N-1}\mid x> \tag{5}$$

量子搜索算法反复使用如下被称为Grover迭代的步骤.(1)应用oracle O;(2)应用Hadamard变换$H^{\otimes n}$;(3)执行使$\mid 0>$之外的每个计算基态获得-1的相位移动的条件相移;(4)再次应用Hadamard变化.

容易证明,Grover迭代可以写成$(2\mid \phi><\phi\mid -I)O$,并且是由开始向量$\mid \phi>$和搜索问题解组成的均匀叠加态张成的二维空间中的一个旋转.采用$\sum_x'$表示所有x上搜索问题解之和,$\sum_x''$表示所有x上非搜索问题之和.定义$\mid \alpha>=\frac{1}{\sqrt{N-M}}\sum_x''\mid x>$,$\mid \beta>=\frac{1}{\sqrt{M}}\sum_x'\mid x>$.

$$\mid \phi>=\sqrt{\frac{N-M}{N}}\mid \alpha>+\sqrt{\frac{M}{N}}\mid \beta> \tag{6}$$

如FIG.5.所示,在$\mid \alpha>$和$\mid \beta>$张成的平面上,运算O对向量$\mid \alpha>$进行了一次反射,$O(a\mid \alpha>+b\mid \beta>)=a\mid \alpha>-b\mid \beta>$;然后$2\mid \phi><\phi\mid -I$执行了对$\mid \phi>$的一次反射.这两个反射的积相当于一次旋转.令$\cos\frac{\theta}{2}=\sqrt{(N-M)/N}$,可以算出转角实际上是$\theta$.容易发现,每次应用G,把$\mid \phi>$向$\mid \beta>$的方向旋转$\theta$的角度.

为了使得$\mid \phi>$接近$\mid \beta>$,必须旋转$\arccos\sqrt{M/N}$的弧度,至少要迭代$R=\lfloor\frac{\arccos\sqrt{M/N}}{\theta}\rfloor$次.假设$M\leq N/2$, 可以得出R 的上界为$R\leq\lceil\frac{\pi}{4}\sqrt{\frac{N}{M}}\rceil$.也就是算法复杂度为$O(\sqrt{N/M})$,而经典算法要求的复

杂度为$O(N/M)$.

IV. 量子密码

1、量子密码的诞生

一般认为量子密码协议诞生于1984年.那一年,来自IBM的Bennett和蒙特利尔大学的Brassard教授合作发表了一篇论文[5].该论文明确提出了第一个也是目前实验上和工程上使用最为广泛的量子密钥分发（QKD）协议,俗称BB84协议.就现在来看,这篇论文的影响是深远的.然而在论文发表后的将近七年里,它几乎无人问津,量子密码的诞生并未引起人们多少注意.笔者认为原因有二:第一,经典密码体制早已广泛流行开来,并且还未受到重大安全性威胁,人类还未找到量子密码的实用价值;第二,BB84协议虽然将貌似毫不相关的量子物理和密码学联系起来,但是它只是用到了人们接受已久的海森堡测不准原理,从学术的角度来说该工作不具有足够的科研本身的趣味性.

直到1991年,牛津大学博士生A. Ekert在物理界权威期刊Physical Review Letter上发表了另一篇影响深远的文章[6].该论文提出了一个不同的量子密钥分发协议,俗称E91协议.该协议令人震惊地使用了鬼魅而著名的EPR纠缠对,让世人第一次认识到令包括爱因斯坦在内的无数科学家迷惑不解的量子纠缠竟然可以应用到实用的密钥分发任务当中.虽然后来发生了不和谐的插曲,Bennett和Brassard教授批评性地指出E91协议本质上与BB84协议一样,但是后来他们又重归于好.更重要的是E91协议中所以所用的纠缠资源目前被认为是实现无条件安全量子密钥分发的必须品,也就是说量子纠缠在量子密钥分发中的地位是不可或缺的.

即便如此,量子密码真正引起人们注意是在1994年,那一年MIT数学系教授Peter Shor提出了著名的量子素数分解算法[7],将该问题的时间复杂度从指数级降到了多项式级,将原本需要上千年完成的任务简化到只需要几分钟就可以搞定.而该任务的难解性恰好是许多经典密码体制的基石.但是该算法的执行需要量子计算机,也就是说如果人类能造出量子计算机,那么传统的密码体制将会受到极大的威胁.另一方面,量子密码不受量子计算机的威胁,他的基石是量子物理理论的正确性,于是量子密码安全通信正式引起了科学家的广泛关注,它被认为是下一代安全通信的唯一武器.

值得一提的是,量子计算机虽然原则上可以破解经典密码体制,但是至少在1994年很少人对他的未来持乐观态度,其主要原因是量子计算机相比于经典计算机有着一个貌似致命的缺点:抗噪性极差.很多人认为量子计算机根本不可能造出来.但是量子纠错码的诞生[8, 9]改变了量子计算机的现状.现在看来,量子计算机的实现没有原则上的困难,并且我们能够清晰地看到它过去十几年发展和美好的未来[10].

2、量子密钥的发布

量子密钥分发协议有很多,各有各的特点,但从历史的角度来说BB84协议和E91协议最具代表性,他们内容简洁,容易实现,BB84协议是目前实验上使用最多的协议,而E91协议衍生出来的设备无关量子密钥分发协议将会越来越多的出现在实验室里甚至得到广泛的应用.

2.1 BB84协议

下面是协议的具体步骤[5]:
1)Alice从集合{$|0>,|1>,|+>,|->$}中随机选取并制备一个态$|\alpha>$发送给Bob.
2)Bob随机选择{$|0>,|1>$}基或者{$|+>,|->$}基对$|\alpha>$测量，测量结果r=0表示测得{$|0>$}或{$|+>$},测量结果为表示测得{$|1>$} 或{$|->$}.
3)重复步骤1)和2)若干次，每一次称为一个事件.
4)Alice和Bob对所有的事件公开比较所选的测量基,其中Alice所选的测量基指的是含有$|\alpha>$的正交基,丢弃测量基不一样的事件,对于测量基一样的事件,随机选择一部分出来公开比较,如果有发现Bob的测量结果与Alice发送的态不一致,那么说明检测到窃听者,协议终止,否则,协议产生的密钥就是余下事件的测量结果.

Alice和Bob合作经过经典纠错和保密放大,生成最终密钥.

从资源的角度来说,BB84协议主要使用了非正交的单量子比特,其安全性由量子不可克隆原理和海森堡测不准原理保证,而这是经典世界所缺少的.

2.2 E91协议

下面是协议的具体步骤[6]:
1)Alice制备一个纠缠单态$|\phi>=\frac{|0>_A|1>_B-|1>_A|0>_B}{2}$,发送粒子B给Bob.
2)Alice和Bob分别独立地对手中的粒子进行测量,测量基在{$|0>,|1>$}基和{$|+>,|->$}基之间随机选择.
3)重复步骤1)和2)若干次，每一次称为一个事件.
4)Alice和Bob随机选择一部分事件,公布测量基和测量结果并代入CHSH不等式进行验证,如果不违背CHSH不等式,那么说明检测到窃听者,协议终止,否则,对余下的事件公开比较所选的测量基,协议产生的密钥就是测量基一样的事件的测量结果.

Alice和Bob合作经过经典纠错和保密放,生成最终密钥.

E91协议则使用了EPR纠缠对,其安全性由违背CHSH不等式来保证,只要违背CHSH不等式,就说明双方共享了一定的纠缠,利用这些纠缠就可以产生密钥.注意原始的E91协议使用了三个测量基而不是这里的两个,但是他们本质上都没有太大的区别,只是密钥率不同而已,这里使用两个测量基是为了方便与BB84协议比较.

2.3基于纠缠的BB84协议

下面是协议的具体步骤:
1)Alice制备一个纠缠态$|phi>=\frac{|0>_A|1>_B+|1>_A|0>_B}{2}$,发送粒子B给Bob.
2)Alice和Bob分别独立地对手中的粒子进行测量,测量基在{$|0>,|1>$}基和{$|+>,|->$}基之间随机选择.
3)重复步骤1)和2)若干次,每一次称为一个事件.
4)Alice和Bob对所有的事件公开比较所选的测量基.对所有测量基不一样的事件和随机选择的部分测量基一样的事件,公开比较测量结果,如果满足:

$$P(00 \mid 00) = P(11 \mid 00) = P(00 \mid 11) = P(11 \mid 11) = \frac{1}{2} \tag{7}$$

$$P(00 \mid 01) = P(01 \mid 01) = P(10 \mid 01) = P(11 \mid 01) = P(00 \mid 10) = P(01 \mid 10) = P(10 \mid 10) = P(11 \mid 10) = \frac{1}{4} \tag{8}$$

那么说明检测到窃听者,协议终止,否则,协议产生的密钥就是余下事件的测量结果.这里,$P(ab \mid cd)$中的a和b分别表示Alice和Bob的测量结果a(b)=0表示测得$\{\mid 0 >\}$或态$\{\mid + >\}$, a(b)=1表示测得$\{\mid 1 >\}$或态$\{\mid - >\}$,c 和d 分别表示Alice 和Bob的测量基c(d)=0表示使用的是基$\{\mid 0 >, \mid 1 >\}$,表示使用的是基$\{\mid + >, \mid - >\}$.

Alice和Bob合作经过经典纠错和保密放大,生成最终密钥.

将该协议与E91协议比较可以发现,他们只在第四步检测窃听的方法不同,前者使用的是测量基和测量结果的条件概率分布,后者则是Bell不等式.

3、实验分析与展望

作为量子信息领域最为成熟的一员,量子密码已经在实验室甚至是在工程上取得了一系列的成果.量子通信的距离已经从早期实验室里的几厘米到现在的几百公里,这得益于实验设备的更新和理论方法的改进(如诱骗态的使用)甚至还出现了商用量子密码机.

但就目前来说,使用的协议几乎都是BB84协议,主要原因可能在于它用到的资源只有由单光子实现的单量子比特,而上面讲到的其他方案都是以较难制备的EPR纠缠态来实现的.

另外Bell不等式的验证阶段面临着两个漏洞:探测性漏洞和局域性漏洞.

探测性漏洞指的是在探测量子比特信号的时候,由于噪声的存在通常会丢失一些信号,最后产生的测量结果相当于是完整事件测量结果的一个子集,而这个子集对Bell不等式的违背与否不一定能够代表全集的情况.关闭这个漏洞的方法有两条途径,第一是提高光子探测器的探测效率,目前的超导光子探测器可达到47%的探测效率,但是距离关闭探测性漏洞的条件85%还有一定距离:第二是使用原子作为量子比特的载体,因为原子比特的探测率可接近100%.

局域性漏洞指的是在Alice和Bob探测量子信息的时间间隔如果大于信息以光速从Alice发送到Bob的时间,那么即便违背Bell不等式,也不能排除先测量的一方将测量信息发送给后测量的一方,从而伪造违背Bell不等式的测量结果.关闭这个漏洞的方法就是加快探测器的响应速度,一般来说光子探测器能达到极快的速度,但是原子比特探测器的速度就较慢了.

总的来说同时关闭两个漏洞的途径有两个:一是研发并使用高效的光子探测器,并用光子作为信息载体;二是用光学腔耦合光子比特和原子比特,结合光子探测器和原子探测器各自的优点,同时解决这两个漏洞.

V. 总结

本文概括性地展示了现代量子计算领域的方向和特点,并对目前量子信息领域最为重要的应用,量子加密进行了简要说明.值得注意的是,人类目前对于量子计算机知之甚少,系统地归纳量子计算机和经典计算机之间的差别,或是找出可以实际应用的量子算法,目前都做不到.这些问题将是未来量子计算领域的发展方向.

VI. 参考文献

[1] 周正威,黄运锋,张永生,郭光灿 2005 量子计算的研究进展 物理学进展Vol. 25,No. 4.2005.12

[2] Nielsen等 2003 量子计算和量子信息（北京：清华大学出版社）

[3] Jurgen Audretsch 纠缠的世界——量子信息与量子计算机的魅力

[4] 莫露洁,颜源 2008 量子计算机与经典计算机的比较 电脑应用技术二零零八年总第七十三期

[5] Bennett, C. H. and G. Brassard 1984 Quantum cryptography: Public key distribution and coin tossing, Proceedings IEEE International Conference on Computers, Systems and Signal Processing p175.

[6] Ekert, A. K. 1991 Quantum cryptography based on Bell's theorem, Phys. Rev. Lett. 67, 661.

[7] Shor, P. W. 1994 Algorithms for quantum computation: discrete logarithms and factoring, Proceedings of the 35th Annual Symposium on the Foundations of Computer Science p124.

[8] W.Shor, Peter 1995 Scheme for reducing decoherence in quantum computer memory, Phys. Rev, A. 52, p2493.

[9] A Steane 1996 Multiple-particle interference and quantum error correction, Proc. R. Soc. Lond. A. 452, 1954 p2551-2577.

[10] qist.lanl.gov/qcomp_map.shtml/