(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 107113169 B
(45)授权公告日 2020.12.18

(21)申请号 201680005112.3
(22)申请日 2016.01.08
(65)同一申请的已公布的文献号
申请公布号 CN 107113169 A
(43)申请公布日 2017.08.29
(30)优先权数据
15305017.4 2015.01.09 EP
15187905.3 2015.10.01 EP
(85)PCT国际申请进入国家阶段日
2017.07.06
(86)PCT国际申请的申请数据
PCT/EP2016/050305 2016.01.08
(87)PCT国际申请的公布数据
WO2016/110582 EN 2016.07.14
(73)专利权人 巴黎矿业电信学院
地址 法国巴黎
(72)发明人 R·阿洛姆
(74)专利代理机构 北京戈程知识产权代理有限公司 11314
代理人 程伟 王锦阳
(51)Int.Cl.
H04L 9/08(2006.01)
(56)对比文件
US 2010239250 A1,2010.09.23
US 2013089206 A1,2013.04.11
US 2013089204 A1,2013.04.11
CN 103490879 A,2014.01.01
CN 101268644 A,2008.09.17
Matthew Campagna.Quantum Safe Cryptography and Security;An introduction,benefits,enablers and challengs.《ETSI World Class Standards》.2014,全文.
Christian Weedbrook.Gaussian Quantum Information.《REVIEWS OF MODERN PHYSICS》.2011,全文.
Cosmo Lupo.Robust quantum data locking from phase modulation.《MIT Open Access Artical》.2014,全文.
审查员 谭菲菲

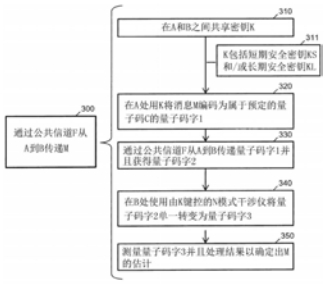
权利要求书3页 说明书18页 附图3页

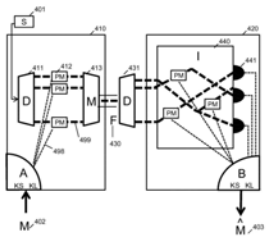
(54)发明名称

来自于短期安全加密量子通信的具有永久安全性的通信

(57)摘要

一种通过公共信道F在第一方A和遥远的第二方B之间传递经典消息M的方法(300),其包括如下步骤:在所述各方之间共享密钥(310),所述共享密钥K包括短期安全密钥KS和/或长期安全密钥KL;在A处,将M编码为量子码字,A利用K将M编码为属于公知量子码的第一加密码字(320);将第一加密码字通过输出为第二码字的F从A传递到B(330);通过利用由B控制的、放置在F的输出的、并且由K键控的N模式干涉仪单一地将第二码字转变为第三码字(340);在B处,通过执行对第三码字的测量,并且通过利用K处理所述测量来确定出M的估计(350)。





CN 107113169 B

1.一种通过连接A和B的有损和/或含噪的公共信道F在遥远的A方和B方之间传递经典消息M的方法,其包括以下步骤:

-在A和B之间共享密钥K,所述密钥K包括短期安全密钥KS和/或长期安全密钥KL;

-在A处将经典消息M编码为量子码字,A使用共享密钥将经典消息M编码为属于公知量子码C的加密码字rho1(M,K);

-通过输出为码字rho2(M,K)的信道F将加密码字rho1(M,K)从A传递到B;

-通过使用由B控制的、放置于信道F的输出并且由K键控的N模式干涉仪I将rho2(M,K)单一地转变为rho3(M,K);

-通过对rho3(M,K)进行测量,并通过使用共享密钥K处理所述测量来确定在B处本地的成熟的M的估计。

2.根据权利要求1所述的方法,

-其中,将M编码到加密码字rho1(M,KS,KL)中的步骤包括以下步骤:将M编码为属于公知量子码C的码字c(M,KL);使用短期安全密钥KS在c(M,KL)上执行逐字加密U(KS),生成加密码字rho1(M,K);

-其中,由KS键控的干涉仪I通过逐字解密来实施U(KS)的反转,随后是独立于短期安全密钥KS的另一个单一转变。

3.根据权利要求1或2所述的方法,

-其中,所述长期安全密钥KL用于选择密码C',所述密码C'与公知码C的子集相关联;

-其中,所述短期安全密钥KS用于在c(M,KL)上执行逐字加密。

4.根据权利要求1所述的方法,其中,将经典消息M编码到rho1(M,K)中的步骤在光量子态中进行,其中所述光量子态与多个特征相关联,所述特征包括:

-C中的码字是在N个玻色子模式中的N个相干态的结果状态,所述玻色子模式选自包括时间模式、频率模式和空间模式的列表;

-代码C的字母表由m=2^p的m进制相移键控相干态组成,其中,每个字母的形式为{|exp(i 2 Pi k/m)alpha>,k=0..m-1},具有远小于1的固定的光子数|alpha^2|;

-使用KS对c(M,KL)的逐字加密包括相位加密步骤,其中短期安全密钥KS用于导出N个独立相移的值,逐字应用在码字的N个相干态上,其中所述相移用p=log2(m)比特进行编码,因此KS的尺寸为p*N。

5.根据权利要求1所述的方法,其中,由B控制的干涉仪I与以下特征中的至少一个相关联,其特征包括:

-I是由分束器和移相器组成的N模式玻色子干涉仪;

-至少一个相移由相位调制器控制,所述相位调制器配置为应用m=2^p的所述m进制相移,以及取决于短期安全密钥KS的值;

-给予短期安全密钥KS,所述干涉仪I配置为实施相位加密并且将rho2(M,K)转变为rho3(M,KL);

-选择干涉仪I的结构,使得在公共信道F上没有噪声的情况下,rho3(M,KL)对应于单模式状态,从而允许使用单模式光学检测器对rho3(M,KL)进行测量。

6.根据权利要求4所述的方法,其中,包括放置在量子信道上的放大器的中继站补偿传播损耗,其中所述中继站或者不了解K=(KS,KL),或者被给予对短期安全密钥KS的部分访

问。

7.根据权利要求5所述的方法,其中:

-M是1比特消息b;

-量子信道是功率透射率为T=tˆ2的玻色子有损信道;

-所使用的代码C是m=2或者4的m进制相移键控字母表的[N,2,D]重复码,其中,N表示长度,2表示码字数,D表示最小距离;

-使用KS的逐字相位加密在于使用KS的log2(m)*N比特对每个相干态的相位执行单次密本加密,所述相位由每个相干态的log2(m)比特来描述;

-干涉仪I是深度为log2(N)的二叉树,将N个相干态的振幅相干地增加到一个单一模式中;

-所述光学检测器包括与A锁相的相位敏感检测器,所述相位敏感检测器选自包括零差检测器、外差检测器、Kennedy接收机、Bondurant接收机或者Dolinar接收机的组;

-在中继站中所使用的放大器包括与A和B锁相的敏感放大器PSA;

-对alpha、N的值,放大器的位置和增益进行优化用于给定的T值。

8.根据权利要求4所述的方法,其中:

-M是1比特消息b;

-量子信道是功率透射率为T=tˆ2的玻色子有损信道;

-所使用的代码C由两个码字组成,来自于单一等价于两个输出上的脉冲位置编码的长度为N的Hadamard码,C的字母表是m=2或者4的m进制相移键控字母表;

-使用KS的逐字相位加密在于使用KS的log2(m)*N比特对每个相干态的相位执行单次密本加密,所述相位由每个相干态的log2(m)比特来描述;

-干涉仪I是深度为log2(N)的二叉树,将N个相干态的振幅相干地增加到功率为tˆ2 N alpha的模式中;

-光学检测器在于相位不敏感检测器,所述相位敏感检测器选自包括单光子检测器、光电二极管或者外差检测器的组;

-在中继站中所使用的放大器是补偿传播损耗的相位不敏感放大器PIA;

-对alpha、N的值,放大器的位置和增益进行优化用于给定的T值。

9.根据权利要求1所述的方法,其中,在A和B之间共享短期安全密钥KS的步骤,其使用计算安全技术通过利用包括密钥密码机制和/或公开密钥机制的一个或者更多个机制来执行。

10.根据权利要求1所述的方法,其中,在A和B之间共享长期安全密钥KL的步骤通过使用长期安全机制来执行,所述机制包括:使用先前在A和B之间交换的长期秘密随机消息或者密钥,使用根据权利要求1所述的步骤,用于具有永久安全性和/或量子密钥分配和/或信任的信使的密钥分配。

11.一种计算机可读存储介质,其上存储有代码指令,当由处理器执行时,所述代码指令执行根据权利要求1至10中的任一项所述的步骤。

12.一种系统,其包括执行根据权利要求1至10中任一项所述的方法的步骤的装置。

13.根据权利要求12所述的系统,其包括以下一个或者更多个:

-存储安全数据(KS,KL)的A的安全边界;

-存储安全数据(KS,KL)的B的安全边界；

-至少以N个模式发射的相干光源；

-信号分离器配置为分离N个模式的每一个或者部分；

-由A控制的至少一个单模式相位调制器设备作用在N个模式中的每一个上；

-配置为组合N个模式中的每一个或者部分的N模式多路复用器；

-从A到B至少一个光量子信道F；

-信号分离器配置为分离N个模式的每一个或者部分；

-由分束器和/或移相器组成的N模式干涉仪I,至少一个由B控制；

-单模式光学检测器。

14.根据权利要求12所述的系统,其包括：

-以N个模式发射相干光的激光器；

-放置在N个模式中的每一个上的相位调制器,其在相干态的m进制相移键控星座图中调制每个模式的状态;所应用的相位调制取决于KS和KL,其生成N模式加密码字rho1(M,K)；

-从A到B至少一个光量子信道；

-由分束器和主动控制的移相器组成的N模式干涉仪；

-在B处的光学检测器；

-在A处和B处的计算装置。

15.一种系统,其包括执行根据权利要求4至5所述的方法的装置,其中,所述系统包括以下一个或者更多个：

-锁模激光器、脉冲激光器和/或连续波激光器；

-相位调制器和/或振幅调制器；

-光开关；

-相位敏感放大器和/或相位不敏感放大器；

-波分多路复用滤波器和/或组合器,和/或分插多路复用器；

-时间延迟干涉仪和/或光学快速傅里叶变换干涉仪；

-选自包括单光子检测器、零差检测器、外差检测器、Kennedy接收机、Dolinar接收机、Bondurant接收机或者量子归零接收机的组中的一个或者更多个检测器。

来自于短期安全加密量子通信的具有永久安全性的通信

技术领域

[0001] 本发明涉及量子密码学领域。

背景技术

[0002] 密钥的创建和分配是加密通信的先决条件。量子密码学(QKD)可以用于产生并且分配密钥,但是不用于传输任何信息数据。相比较计算安全密钥分配技术,量子密码学的一个明显的优点是存在量子密码学协议,其安全性可以在理论信息设置中形式上地建立。即便当一些计算技术用于经典信道的鉴定目的,量子密码学可以保证永久的安全性。

[0003] 对于密钥建立协议,永久的安全性特别地意味着一旦协议终止并且密钥已分配,其安全性不能在将来的任何时候受到损坏,不论计算能力,或者是任何潜在的攻击者所进行的密码分析的发展。如此强大的安全性的保证是不能通过计算技术来获得的。

[0004] 尽管能够提供永久的安全性,量子密码学在性能和资源需求方面仍表现出局限性。到今天为止,量子密码学可以可靠地部署在城市距离内(80公里以下)。长距离量子密码学可以通过光纤用于直到数百公里的距离,但是可实现的密钥速率很低或者不足以用于特定用途。此外,因为检测器噪声、后加工效率以及系统稳定性的要求都随着距离而增加,很难部署具有可靠性的超长距离量子密码学。

[0005] 作为明显的限制,量子密码学不能与光学放大器兼容。因此,在没有可靠的量子中继器的情况下,利用量子密码学可实现的距离仅仅可以延伸到利用经典可信任的中继器的单个量子密码学链路的范围之外。这样的中继器通常要求复杂并且昂贵的具体措施来保证其安全性。因此,具有可信任的中继器的量子密码学不符合端对端安全性范例,因此构成了局限性。量子密码学还表现出其他局限性。

[0006] 在2005年公布的标题为“通过光学放大波分复用通信网络的基于量子数据加密的相干态”的专利文件WO2005046114公开了利用光学放大的双模式相干态的量子加密协议,其结果是与现有的波分复用基础设施相兼容的极化的独立系统,并且其提供了适合于通过串联放大线路的波分复用网络的安全数据加密。该方案的安全性本质上与计算安全的潜在密码的安全性相关。这样的通过计算安全加密的方案的安全性优点,尤其是永久安全性不能够建立。因此该方法表现出局限性。

[0007] 需要方法和系统用于在遥远的A方和B方之间传递具有永久安全性的消息M,特别是可以实现非可信任的中继器。

发明内容

[0008] 本发明公开了一种通过公共信道在第一方和遥远的第二方之间传递经典消息的方法,其包括在所述各方之间共享密钥的步骤,所述共享密钥包括短期安全密钥(KS)和/或长期安全密钥(KL);在第一方将经典消息编码为量子码字,第一方利用共享密钥将经典消息编码为属于公知的量子码的第一加密码字;将第一加密码字通过公共信道从第一方传递到第二方,该公共信道的输出为第二码字;通过利用由第二方控制的、放置在公共信道输出

并且由共享密钥来键控的N模式干涉仪单一地将第二码字转变为第三码字;在第二方通过执行对第三码字的测量并且通过利用共享密钥处理所述测量来确定出经典消息的估计。

[0009] 在实施方案中,公开了一种在遥远的A(Alice)和B(Bob)之间通过在A和B之间共享短期安全经典密钥K,并且通过利用公共量子信道和经典已认证信道来传递长期安全经典消息M的方法。在实施方案中,如果关于消息的任何窃听者E(Eve)的可访问信息可以以任意选择的接近0的数量为上限,并且如果所述界限总是保持有效,则经典消息是长期安全的;并且如果关于消息的任何窃听者E的可访问信息可以以接近0的可以任意选择的数量为上限,并且如果该界限在至少为tau的持续时间间隔期间有效,则经典消息在持续时间tau期间是短期安全的。所描述的进展包括以下步骤:在A和B之间通过经典认证信道共享短期安全密钥K;使用短期安全密钥K将在A处的经典消息M编码为量子态,并且通过量子信道向B处发送量子态;使用K和在量子信道的输出所接收的量子态在B处将信息M进行解码。实施方案进一步包括:使用计算安全公钥和/或对称密钥加密、使用纠错码、在输入使用相干态的结果、使用单模式(自适应或者非自适应)相干或者直接检测接收机。上述为系统和软件方面的描述。

[0010] 有利地,所公开的量子加密协议,即混合经典和量子密码学,其提供了一种全面的安全模型,针对具有给定资源和攻击策略的攻击者,根据该模型可以明确地定义出在给定信道上的协议可实现的性能。

[0011] 有利地,在一些实施方案中,如果在所交换的密钥K短期安全的、大于时间tau的期间内,窃听者不能相干地存储量子信息,与计算安全加密相比,使用量子信道和短期安全密钥K的A和B可以实现长期安全性,甚至可组合的信息理论安全性。

[0012] 有利地,在一些实施方案中,与共享安全随机密钥的量子密码学相比,A和B可以安全地共享确定的消息M。

[0013] 有利地,本发明的实施方案可以实现“扩展安全性”:在量子编码期间使用纠错码使得达到与量子密码学相比提高的性能:更大的可容忍的信道损耗、较高的可容忍的信道误码率、较大的编码器和接收机噪声、无需反馈的信道。

[0014] 有利地,在一些实施方案中,特别是当与量子密码学相比时,A和B甚至不需要在B处执行测量,以便对由E所捕获的信息进行上限处理,因为该界限仅取决于由A所发送的状态。

[0015] 有利地,在一些实施方案中,特别是当与量子密码学相比时,该方法与包含光学放大器的光学信道和波分多路复用光网络相兼容。

[0016] 在一些实施方案中,所公开的方法和系统有利地实现一些可控性。例如,可以调整与所述方法的一些实施方案相关联的,例如(n,alpha)的参数,以优化在给定信道(以损耗率和误码率为特征)上的性能(例如,给出正确性参数epsilon的可实现的通信速率R)。

[0017] 有利地,本发明的实施方案可以在没有过多努力和成本的情况下实施,同时对现有电信组件和系统进行最小的硬件改变(例如通过使用现在广泛地用于长距离相干经典通信的相干态的相位调制和零差检测)。

[0018] 有利地,本发明的实施方案允许执行最佳测量,并达到或者接近用于通过A和B之间的量子信道进行通信的经典容量,同时可以实施为实际的现有接收机,即可以实施为当前技术。

[0019] 在一些实施方案中，所公开的发明可以直接实施为现有的相干通信发射器、相位调制器和接收机。

[0020] 有利地，本发明的实施方案使得“飞行中的数据”(例如数据传输期间的数据流)的安全性具有“静止数据”(例如在数据中心、云计算数据库等中的数据存储的密钥管理)的安全性的应用。

[0021] 有利地，本发明的一些实施方案可以实施在包括波分多路复用光网络和包含光学放大器的网络的光纤网络中，或者实施在卫星网络中。应用范围从军事目的到常规和国内目的(例如银行、政府、投票机、加密货币、电子商务等)。

[0022] 在实施方案中，公开了一种在遥远的A方和B方之间传递消息的方法，其包括使用计算安全加密函数Enc来加密结果状态或者非纠缠的量子码字的步骤，其中，在至少为tau_enc的时间内，Enc是短期安全的，而存储在量子存储器中的任何信息在严格低于tau_enc的tau_Q时间内完全退相干。进展包括使用长期安全对称密钥、量子数据锁定、短期安全短暂屏蔽、二进制相移键控编码、输入信号能量的物理限制L、二进制相移键控字母表上的Hadamard码、以及传播损耗的补偿。系统方面描述了使用干涉仪、单符号接收机、单光子检测器、零差和外差检测器、Kennedy接收机、Dolinar接收机和量子归零接收机。

[0023] 有利地，本发明的实施方案能够实现“后量子”安全模型，即，允许具有永久安全性，并且特别是具有针对操作量子计算机的攻击者的安全性的密钥分配协议。

[0024] 有利地，本发明的实施方案将结构性代码的超加性的性能和量子数据锁定相结合。

[0025] 有利地，本发明的实施方案解除了现有量子数据锁定方案的主要限制中的其中一个，其依赖于不能有效解码的随机码。

[0026] 有利地，本发明的实施方案能够实现长距离安全通信或者具有永久安全性的密钥分配。

[0027] 有利地，本发明的实施方案可以实施为对现有电信组件和系统的最小硬件改变。

[0028] 本发明公开了一种通过有损和/或含噪的公共量子信道F在遥远的A方和B方之间安全地传递经典消息M的方法和显式协议，其包括：在N个模式下，使用经典量子编码C将M编码为光学码字的步骤，该光学码字作为具有被视为量子位的低光子数的N个相干态的结果，以及通过使用计算安全机制，通过执行由A和B之间共享的密钥流KS索引的单模式单一转变将量子位上携带的信息加密的步骤。一经接收(含噪)量子码字，B使用由分束器和移相器组成的N模式光学干涉仪来组合N个所接收的模式。B使用KS在干涉仪路径内应用一些单模式单一转变。这种KS键控干涉仪I的整体效果用于撤销量子位级别的加密并且获得多模式干涉，使得由A使用的多模式码字所组成的代码C单一地映射到由单模式码字组成的代码C’，因此可以用现有检测器实际检测。

[0029] 根据本发明，在名为“爱斯基摩人(ESQUIMO)”(即“强于量子含噪存储器的加密”)的框架中，根据该框架，量子存储时间为tau_Q(N)，在此期间，编码在长度为N的量子码字上的可检索经典消息的小部分以至少1/2衰减，使得对于一些N、tay_Q(N)<<tau_enc，作为计算加密技术用于导出KS的时间的所述时间tau_enc可以被认为是安全的。

[0030] 本发明公开了显式协议(消息M、编码C、使用KS的光学码字的相位加密、干涉仪I、光接收机和由Bob进行的后处理)，使得在爱斯基摩人框架(或者模式)下，M上的Eve信息IE

可以被限制在通过信道F在Alice和Bob之间共享的信息之下。

[0031] 在相干态的多模式的结果上的可能的编码C包括:通过二进制移相键控或者M进制移相键控调制的相干态的重复码;通过二进制移相键控调制的相干态的Hadamard码。

[0032] 本发明公开了一种协议和显式设计,以实现用于编码C的非可信任中继器,该编码C在于通过M进制移相键控调制的重复码。这样的中继器例如可以放置在信道F上以补偿损耗。在本发明的一方面,对于(编码、中继器、解码的)适当参数,尽管中继器不被信任,A与B之间的通信相对于攻击者(包括恶意接收机)的安全性也不会妥协。

[0033] 所公开的方法和协议允许在Alice和Bob之间建立有效的经典窃听信道。然后经典窃听编码(外码)可以用于以取决于量子信道F的特性和协议(编码C、干涉仪I、光学接收机和Bob的解码策略)的速率在A和B之间可靠并且安全地传递经典消息。

[0034] 系统方面描述了使用相位调制器、相位敏感放大器(PSA)、相位不敏感放大器(PIA)、由移相器和分束器组成的多模式玻色子干涉仪、单光子检测器、零差和外差检测器、Kennedy接收机、Dolinar接收机和量子归零接收机。

[0035] 有利地,本发明的实施方案仅仅依赖于用于推导出短期秘密的对称加密技术,因此能够实现针对“后量子”攻击者的永久安全通信。

[0036] 有利地,本发明的实施方案可以使用短期安全加密来模糊不同模式之间的相干关系,以限制Eve在M上的可访问信息。

[0037] 有利地,本发明的实施方案可以组合结构性代码的超加性和短期安全加密的性能,从而限制Eve的可访问信息。

[0038] 有利地,本发明的实施方案可以将量子数据锁定码的性能与短期安全加密结合,从而限制Eve的可访问信息。

[0039] 有利地,本发明的实施方案可以解除现有量子数据锁定方案的主要限制中的一个,并且同时实施为结构化量子数据锁定码。

[0040] 有利地,本发明的实施方案可以实现具有永久安全性的安全通信。

[0041] 有利地,本发明的实施方案可以使用相位敏感放大器或者相位不敏感放大器来实现非可信任的中继器,其能够补偿损耗,并且因此能够在无限距离上实现具有永久安全性和非零速率的安全通信。

[0042] 有利地,本发明的实施方案可以实施为对现有电信组件和系统的有限硬件改变,并且特别实施为与长距离量子密码学所需的检测器相比,具有更多噪声的检测器。

[0043] 有利地,本发明的实施方案使得“飞行中的数据”(例如数据传输期间的数据流)的安全性具有“静止数据”的安全性的应用(例如在数据中心、云计算数据库等中的数据存储的密钥管理)。

[0044] 有利地,本发明的一些实施方案可以实施在包括波分多路复用光网络和包含光学放大器的网络的光纤网络中,或者实施在卫星网络中。应用范围从军事目的到常规和国内目的(例如银行、政府、投票机、加密货币、电子商务等)。

[0045] 本发明公开了在遥远的各方之间安全地传递消息的具有永久安全性的实用系统和方法。

[0046] 有利地,可以正式建立(即根据数学逻辑证明)所公开的方法和系统的永久安全性。

[0047] 有利地，本发明的实施方案使得能够实现超越量子密码学所针对的无条件安全性标准的新的安全模型。

[0048] 有利地，所公开的方法和系统可以被认定为“实际”，即实施为现有硬件，和/或能够用更少的资源获得与量子密码学相当或者更好的性能。

附图说明

[0049] 本发明的实施方案参考附图以示例的方式进行描述，其中相似的附图标记表示相似的元素，并且其中：

[0050] 图1提供了根据本发明的安全模型的总体视图；

[0051] 图2显示了根据本发明的示例性系统的某些方面；

[0052] 图3显示了本发明的实施方案；

[0053] 图4显示了本发明的示例性实施方案的某些方面。

具体实施方式

[0054] 本专利申请的题目为“来自于短期安全加密量子通信的具有永久安全性的通信”，是2015年10月1日提交的题目为“具有永久安全性的实用量子密码学”的改进专利申请，该申请是2015年1月9日提交的题目为“混合经典量子密码学”的专利申请No.EP15305017.4的改进专利，其内容在此合并。

[0055] “可访问信息”或者lacc(M;rho)由最大经典交互信息(在量子态rho下所有可能的局部测量的最大化)来定义，该最大经典交互信息可以从关于经典消息M的量子态rho中获悉。

[0056] 如果关于消息的任何窃听者E的可访问信息可以以接近0的可以任意选择的数量为上限，并且如果该界限总是保持有效，该经典消息是长期安全的。

[0057] 如果关于消息的任意窃听者E的可访问信息可以以接近0的可以任意选择的数量为上限，并且如果该界限在至少为tau的持续时间间隔期间有效，则经典消息在持续时间tau期间是短期安全的。

[0058] 在现实的假设下，持有量子态rho_E的窃听者E不具有量子存储器，或者具有在短时间内退相干的量子存储器，然后长期安全的通信协议(由窃听者获得的可忽略的可访问信息所量化)可以转变为可组合的信息理论安全所适用的通信协议。

[0059] “计算安全(CS)”系统是一种安全系统，其假设任何敌对者从计算方面讲是受限的，因为所有的敌对者是在实际中的。因为问题的困难程度难以证明，所以实际上某些问题是“假设”困难(计算困难假设)。一些常见的密码困难假设或者问题的非详细清单，例如包括：整数因式分解、RSA问题(强于因式分解)、二次剩余问题(强于因式分解)、确定性复合剩余假设(强于因式分解)、高剩余问题(强于因式分解)、Phi隐藏假设(强于因式分解)、离散对数问题(DLP)、计算Diffie-Hellman假设(CDH;强于离散对数问题)、确定性Diffie-Hellman假设(DDH;强于计算Diffie-Hellman假设)、以及最短向量问题。

[0060] 在非正交状态之间区分的不可能性是量子力学的基本原则。

[0061] 在物理学中，在量子力学中，“相干态”相当于谐振子汉密尔顿函数的特征向量。这样的状态非常重要，尤其在光学上，因为激光器(大大超过阈值来操作的)代表性地产生可

以描述为光的相干态的光的状态。

[0062] 将经典消息(x)在量子态Psi上“编码”的步骤意为将单一运算Ux(取决于x)应用于量子态Psi上。

[0063] 将在量子态rho上编码的信息X解码的步骤指的是,在rho上执行测量(可能的联合测量)并且在所获得的测量结果上可能执行随后的经典后处理以建立X的估计的步骤。

[0064] 公开了一种在遥远的A方和B方之间通过在A和B之间共享短期安全经典密钥K并且通过利用公共量子信道和经典已认证信道来传递长期安全经典消息M的(计算机实施的)方法。

[0065] 根据本发明的一方面,公开了一种“混合”安全模型(即将经典密码学和量子密码学结合到特定的方式中)。所公开的发明的实施方案,例如,能够建立安全的双方密码原语。这样的进展包括:例如,比特承诺、抛硬币或者异或计算。相关地,这样的双方密码协议可以用于建立任何安全多方协议。

[0066] 进一步地,如果关于消息的任何窃听者E的可访问信息可以以接近0的可以任意选择的数量为上限,并且如果所述界限总是保持有效,该经典消息是长期安全的。

[0067] 进一步地,如果关于消息的任意窃听者E的可访问信息可以以接近0的可以任意选择的数量为上限,并且如果该界限在至少为tau的持续时间间隔期间有效,则经典消息在持续时间tau期间是短期安全的。

[0068] 进一步地,所述方法包括以下步骤:在A和B之间通过经典已认证信道来共享短期安全密钥K;利用短期安全密钥K将在A处的经典消息M编码为量子态,并且通过量子信道向B处发送量子态;利用K和在量子信道的输出所接收的量子态在B处可靠地解码消息M。

[0069] 进一步地,所述短期安全密钥K可以定期更新。A可以利用安全的随机发生器(例如量子随机数发生器)来产生密钥流S,然后可以利用前述的方法向B安全地发送密钥流S。然后该密钥流S可以用于替换K。

[0070] 进一步地,从A到B共享短期安全密钥K的步骤依赖于或者包括计算安全公共密钥加密。

[0071] 在实施方案中,A可以利用B的公共密钥来加密K,并且可以通过经典已认证信道来将其发送到B。在实施方案中,A和B可以首先共享预共享长期安全密钥Kseed。A和B都可以利用计算安全对称密钥加密算法来将Kseed扩大到K中。

[0072] 进一步地,计算安全加密方案包括分组密码和/或流密码。在实施方案中,运用了高级加密标准(AES)128。在实施方案中,运用了高级加密标准256。在一些实施方案中,可以运用例如双鱼算法、Serpent、高级加密标准(Rijndael)、Blowfish、CAST5、RC4、3DES、Skipjack、Safer+/++和IDEA(以及其组合)的算法。

[0073] 进一步地,从A到B共享短期安全密钥K的步骤包括:利用计算安全公共密钥加密来分配|Kseed|<<|K|的密钥Kseed的步骤;以及利用对称密钥加密来将Kseed扩大到K中的步骤。

[0074] 进一步地,在A处将M编码到量子态中的步骤通过将M编码到尺寸为n的结果状态来进行,该结果状态利用量子信道经由n来通信,并且其中,在解码的步骤期间在B处所进行的测量是每个n信道输出的单独的或者逐项的测量。

[0075] 根据本发明的一方面,来自于协议的安全性可以基于窃听者受使用期限短的量子

存储器所限的事实,其不能够获悉相干信息并且因此受限于模糊态的可访问信息。该可访问信息可以以少量为上限。另一方面,B可以利用可能适用的本地操作来反模糊并且测量连续的信道输出,并且可以估计或者确定A发送的信息。在一些实施方案中,所述信息可以接近最佳信息。

[0076] 进一步地,在A处将消息M编码的步骤包括利用等于n*alpha^2的光量子总数将消息M光学编码到n个光的量子相干态的结果中。

[0077] 进一步地,在A处将消息M编码到n个光的量子相干态的结果中的步骤,包括将在A处的每个相干态进行相位和/或振幅调制的步骤。

[0078] 进一步地,密钥K由n*p比特构成,其中p是大于1的整数;所述短期安全密钥K用于确定具有解析度2Pi/2^p的n个角度{Theta1,Theta2,…,Thetan}。进一步地,所述消息M与|M|的不同值有关,其以比特为单位,长度等于$k=\log_2|M|$。进一步地,在A处利用短期安全密钥K将消息M编码到光量子码字中的步骤,包括以下步骤:应用秘密共享方案S和随后的纠错码C将k比特的消息M编码到l比特的经典码字c(M)中的步骤;将l比特的经典码字c(M)光学编码到n个相位编码脉冲的结果中,其中l=n*m,每个相位编码脉冲是振幅alpha和选自M进制相位星座图中的相位的相干态,将m比特进行编码;以及将角度Theta_i(i=1…n)的相位旋转应用到n个脉冲的每一个。

[0079] 所述步骤定义了将M编码到长度为n的光量子码字中,即通过使用n个信道发送到量子信道上的n个相干态、n个光脉冲的结果状态。

[0080] 进一步地,在B处通过利用短期安全密钥K将所接收的光量子码字解码到M的估计中的步骤包括如下步骤:

[0081] 将角度Theta_i(i=1…n)的反相位旋转应用到所接收的ith光脉冲;随后在n个光脉冲的每一个上执行单独的或者适合的相干测量;并且从n个测量中确定消息M。

[0082] 进一步地,该方法进一步包括生成ns份的消息M的步骤,其根据秘密共享方案S(t,ns)被认为是输入,因此ns份中至少t个的信息对恢复消息M来说是有必要的。

[0083] 秘密共享(也称为秘密分隔)指的是在一组n个参与者(例如,A、B、C、D等)中分配秘密的方法,其中每一个被分配一份秘密。该秘密仅当可能的不同类型、足够数量的份数结合在一起时才可以被重建;单独的一份本身是无用的。每个参与者被给予一份秘密,以这种方式,t(用于阈值)中的任意组或者更多的参与者可以一起重建秘密,但是少于t个参与者的组不可以重建秘密。这样的系统成为(t,n)阈值方案。根据本发明的实施方案,增加t会增加要攻击的量子存储器所要求的尺寸,因此会增加这样的攻击的难度。在一些实施方案中,运用了理论上安全的信息秘密共享方案。在一些实施方案中,运用了计算上安全的秘密共享方案。在实施方案中,运用了同态秘密共享。在一些实施方案中,运用了Blakley方案(几何方案)和/或Shamir方案(例如多项式内插法)和/或中国剩余定理(例如Mignotte和Asmuth-Bloom)。在实施方案中,秘密共享方案是有前瞻性的。在实施方案中,秘密共享方案是可验证的。

[0084] 需要强调的是,秘密共享是用于安全的多方计算的几种协议中最原始的。

[0085] 进一步地,所述方法进一步包括利用纠错码C来将消息M编码到更大的消息M2中的步骤。

[0086] 例如,纠错码可以利用冗余使得消息M恢复到要求的正确度,即使信道是含噪的。

在一些实施方案中，纠错码C的参数可以适用于量子信道参数(例如损耗和噪声)。可选择地运用达到能力并且有效解码的码族，例如低密度奇偶校验码或者Turbo码(例如具有低解码复杂度)、卷积码或者极化码(以及其组合)。

[0087] 进一步地，消息M的长度为1比特；秘密共享方案包含一份；纠错码C是长度为1或者n的重复码，并且M进制相位编码是二进制相位编码。

[0088] 在实施方案中，k等于1即消息M是1比特。微不足道的秘密方案的意思是，例如只有一份秘密。所述重复码可以是长度1等于n。二进制相位编码的意思是，对于M进制编码，m等于1。例如，二进制相位可以是二进制相移键控。

[0089] 进一步地，计算安全加密方案包括分组和/或流密码。

[0090] 进一步地，用于从A到B传递log2|M|(比特)经典消息M的协议的性能与4个参数(R、n、alpha、epsilon)有关，其中：n是在协议的一个运行中所使用的量子信道的数量；R是传输速率，安全信息可以以该速率从A发送到B；R＝log2|M|/n；alpha^2是在协议的一个运行中在量子信道上发送的光量子的平均数；epsilon是协议的正确性，其中在B处的消息M的解码的步骤以大于1-epsilon的机率来执行，而窃听者E关于消息M的可访问信息以epsilon为上限。

[0091] 一方面，增加光量子alpha^2的平均数不但会典型地增加与B共享的信息的数量，而且会增加向E泄露的信息。另一方面，增加n仅仅减少向E泄露的信息。因此，为了确保所规定的安全水平(参数epsilon)，当alpha^2增加时，n必须增加；n*alpha^2的结果以1为上限。为了确定的n*alpha^2的结果，增加n使得距离增加，可靠并且安全的通信(具有正确性epsilon)可以通过该距离来进行。这些是根据公开的方法和系统，可以用于控制通信协议的参数的示例。

[0092] 对于确定的量子信道N_{AB}，其以传输T和规定的误差模型(在此由参数Xi来量化)为特征。可实现的速率R随着减少的T和增加的误差参数Xi而减少。可实现的速率R随着减少的epsilon而减少。可实现的epsilon随着n而减少。

[0093] 例如，通信速率可以用每信道所使用的比特来表示。通信速率(例如每秒所发送的消息的安全比特)可以低于在相同信道上与相同硬件进行相位调制的经典通信可实现的速率。特别地，这些可以由于冗余(参数n)。

[0094] 在此公开了一种计算机程序，当所述计算机程序在合适的计算机设备上执行时，其包括用于实施所述方法的一个或者更多个步骤的指令。

[0095] 在此公开了一种系统，其包括适合于实施所述方法的一个或者更多个步骤的装置。

[0096] 进一步地，该系统在A处包括以连续波形动态来工作的激光器；振幅调制器放置在激光器的后面对n个脉冲进行调制，每个脉冲是振幅alpha的相干态；相位调制器放置在激光器的后面，将相移Theta1、Theta2、…Thetan进行调制，以及将二进制的二进制相移键控进行调制；从A到B至少一个光量子信道；从A到B至少一个经典信道；在B处的相位调制器；在B处的相干接收机(其可以为自适应的或者非自适应的)；以及在A和B处的计算装置。

[0097] 在实施方案中，在A处的激光器的时间相干性可以足够高，以确保通过n个信道所使用的稳定相位关系。在实施方案中，在B处的相干接收机是自适应的。在实施方案中，相干接收机是非自适应的。

[0098] 进一步地，多重相干态与二进制调制的区分包括自适应的个体测量。

[0099] 进一步地，多重相干态与二进制调制的区分由Dolinar接收机来执行，其包括自适应位移和光子计数。这样的Dolinar接收机对于相干态的二进制调制之间的区分是最佳的。

[0100] 进一步地，自适应的个体测量由Dolinar接收机、或者BondurantII接收机、或者Becerra接收机、或者连续波形调零接收机、或者其组合来执行。

[0101] 进一步地，多重相干态与二进制调制的区分包括非自适应的个体测量。

[0102] 进一步地，非自适应个体测量由零差接收机、或者外差接收机、或者Kennedy接收机、或者BondurantI接收机、或者其组合来执行。

[0103] 在实施方案中，公开了一种用于量子密码学的安全模型，其开发了假设：任何量子存储器在限定的时间T_{enc}中势必会退相干，在此期间对称加密可以被认为是完美的，即不能区别于随机函数，而其可以当$t>T_{enc}$时损坏。

[0104] 图1提供了根据本发明的安全模型的总体视图。

[0105] 该模型(或者框架)100称为爱斯基摩人(比量子含噪存储器更强的加密)，可以看作为延时释放加密101和含噪量子存储器模型102的结合。

[0106] 尽管该模型背离理论信息安全(仅在短时间范围内假设保持计算安全)，其表现出至少两个有趣的地方：

[0107] 1)其基于合理假设，即高级加密标准式加密功能不能够在短于最好的量子存储器的退相干时间的时间内损坏。

[0108] 2)其为“后量子”安全模型，因为只假设了对称加密的(短期)安全性，并且其允许建立具有永久安全性的密钥分配协议。

[0109] 爱斯基摩人框架对于量子密码学开放了有利的并且未开发的可能性。可以通过提出密钥分配协议来说明其实际上实施为现今的技术，并且可以通过利用结构性代码的超加性111和量子数据锁定112通过量子密码学的基本交换损耗率来极大地改进。

[0110] 近期在量子数据锁定方面的工作，其安全性基于考虑到可访问信息，该可访问信息清楚地说明了目前常用于量子密码学的可组合安全性标准的放宽可以允许设计用于安全通信的具有改进性能的新的量子密码协议。

[0111] 此外，可以使用有限时间量子存储器，因此在爱斯基摩人框架中可以获得量子数据锁定的可组合安全性。

[0112] 此外，存在完美的短期(短暂的)对称加密功能的假设允许进一步，并且解除了现有的量子数据锁定方案的主要限制的其中一个：这样的方案依赖于随机码结构，为此不清楚如何设计实际的解码器。

[0113] 相反，公开了使用有损的玻色子信道的超加性代码的显式结构，并且公开了通过二进制相移键控(BPSK)字母表，利用脉冲位置调制(PPM)代码来开发这种代码的单一等值。可以利用所述短暂加密来模糊(通过单次密本)二进制相移键控密码本并且确保一致性。所述模糊仅仅是短暂的，但是留给窃听者Eve(在爱斯基摩人中其量子存储器对于$t>T_{enc}$退相干)没有比在信道的输入上执行直接的单符号测量更好的策略。Eve因此受限于用于单符号测量的可访问信息Iacc(M,Q)，而Bob(其可以使得短暂加密反模糊)可以使用结构化的超加性接收机。

[0114] 此外，量子数据锁定可以用于减少Eve的可访问信息，即利用k个秘密比特来隐藏

代码的结构，所提供的m(每个码字所传输的比特数)大于密钥K的比特数k，该密钥K用于将应用到每个码字的单一体进行编码。

[0115] 在此公开了一种优化的并且显式的“实用”量子数据锁定的结构，其依赖于$(2^m-1, 2^m, 2^{m-1})$(长度，码字数，最小距离)Hadamard码。所提出的结构利用用于锁定的k比特，并且可以假设其可以通过2^k因子来减少lacc(M;Q)。对于可实现的但是具有挑战性的值m＝16，通过由Bob lacc(M,K,Q)可解码的信息的超加性增益的组合，以及通过在lacc(M;Q)上的锁定的减少来提高在有损的玻色子信道上最大可达到的距离，但是速率受限于以指数减少的具有m的Hadamard码的速率。对于可达160公里的距离，其导致每二进制相移键控符号可达到10^{-10}比特密钥，等同于相对含噪雪崩光电二极管$(pd＝10^{-5})$。

[0116] 用于密钥分配的改进的编码和调制方式可以用在爱斯基摩人框架中。

[0117] 在此公开了本发明的实施方案。

[0118] 公开了一种方法，其包括以下步骤：

[0119] -对于有损的玻色子信道，运用超加性代码的显式结构；

[0120] -通过二进制相移键控(BPSK)字母表，以及脉冲位置调制(PPM)编码来开发超加性代码的单一等值。

[0121] 进一步地，所述方法还包括运用短暂加密的步骤。在此提供了“短暂”的定义。

[0122] 进一步地，所述短暂加密通过单次密本来模糊，二进制相移键控密码本因此确保了一致性。

[0123] 进一步地，所述方法还包括运用量子数据锁定的步骤。

[0124] 进一步地，运用量子数据锁定的步骤包括利用k个秘密比特来隐藏代码的结构的步骤，所提供的比特数m(每个码字所传输的比特数)大于密钥K的比特数k，该密钥K用于将应用到每个码字的单一体进行编码。

[0125] 进一步地，运用量子数据锁定的步骤包括运用Hadamard码的步骤。

[0126] 图2显示了根据本发明的示例性系统的某些方面。

[0127] 关于本发明的硬件(系统)方面，本发明的一些具体的实施方案(例如下文所述的进展C5和C6)可以有利地依赖于在B处的检测器的超加性的性能(而E只能按符号测量)。然而，如在进展C1中所公开的，B可以运用检测器来按符号测量，但是B可以在运用了干涉仪I(该干涉仪将多个符号合并到一个符号中)之后执行所述测量。具体的硬件方面构成了实施方案(例如C5或者C6)，其可以相对容易地实施。

[0128] 换句话说，在实施方案中，在B处的接收机可以将干涉仪、检测器(单符号)、和经典(标准)解码器(和后处理)组合。换句话说，在B处的接收机可以被认定为超加性接收机，然而实际上可以用单符号检测器来制造。

[0129] 图2显示了系统200的总体视图，其使得遥远的A方和B方相互连接。A涉及光电子元件201以及计算、存储和通信资源280。B同样涉及光电子元件202以及计算、存储和通信资源290。

[0130] 这样的光电子元件可以包括，例如：在A101以连续波形动态来运行的激光器(源)210；位于激光器后面，用于将每个都为振幅alpha的相干态的n个脉冲进行调制的振幅调制器220；位于激光器后面，用于将相移Theta1，Theta2，…Thetan进行调制和二进制的二进制相移键控调制的相位调制器230；从A 101到B102至少一个光量子信道240；从A 101到B102

至少一个经典信道250;在B102,相位调制器260;以及在B102,相干接收机270(自适应或者非自适应的)。

[0131] 如先前所描述的,在有利的实施方案中,B可以包括结构化的超加性接收机(例如由单符号接收机和干涉仪构成)。

[0132] 通常,在A处的计算、存储和通信资源280,或者在B处的计算、存储和通信资源290可以包括:处理装置(281、291)(例如,一个或者更多个CPU)、存储装置(282、292)、输入/输出(I/O)装置(283、293)、存储装置(284、294)、以及网络接入装置(285、295)。所述装置可能彼此相互作用(缓存、交换、分布式计算、负载平衡等)。所述处理装置(281、291)可以包括中央处理器(CPU,多核或者众核)、现场可编程门阵列(FPGA)、专用集成电路(ASIC)、或者其组合。所述存储装置(282、292)包括:例如,一个或者更多个闪存或者随机存储器。附着于A或者B的光电子硬件经由输入/输出装置(283、293)与经典计算、存储和通信装置(280、290)相互作用。所述输入/输出装置(283、293)可以包括:例如,数模转换器(DAC)或者模数转换器(ADC)。该数模转换器(DAC、D/A、D2A或者D-to-A)将数字数据(通常为二进制)转换为模拟信号(电流、电压、或者电荷)。该模数转换器(ADC)执行逆向功能。所述存储装置(284、294)可以包括一个或者更多个的硬盘驱动器或者固态硬盘。

[0133] 可选择地,所述计算、存储和通信装置280或者290可以包括能够实现(图形的)用户界面的(即能够人机交互的)装置。例如,该系统可以进一步包括输出外设(例如显示器)和输入外设(例如鼠标或者键盘,其可以用于经由所关联的图形用户界面来控制通信速率)。

[0134] 在一些实施方案中,也可以使用其他硬件设备(未显示),例如一个或者更多个光开关、光多路复用器、光信号分离器、光放大器、分束器、光非线性进制件、光隔离器、滤波器、光引信、和其他设备。所使用的硬件可以适应于(或者适合于)处理高速度(例如从每秒百万字节到每秒兆兆字节)和/或高调制深度(例如10比特或者以上)。

[0135] 将A和B相互连接的网络(即已认证信道250和量子信道240)可以是有线的和/或无线的。在一些实施方案中,这样的网络是无线网络(例如无线保真和/或卫星)。在一些实施方案中,所述网络是有线网络(例如光纤和/或非对称数字用户线路,例如通过互联网)。有利地,有线网络(即在A和B之间的有线通信线路)表现出可靠的连接性。在一些其他的实施方案中,将A和B相互连接的网络可以包括无线和有线网络(例如,当量子信道由光纤来执行时,已认证信道可以是无线的)。

[0136] 在实施方案中,A(B分别)装备有由现场可编程门阵列来控制的光电子器件。有利地,这样的实施方案是紧凑的。在一些实施方案中,可以使用特定的专用集成电路(例如提供非常高速度的畅销产品)。可以使用多核处理器和众核处理器。

[0137] 在一些实施方案中,本发明实施为高度集成光电子芯片,例如嵌入在小型的终端上或者终端设备上(如智能手机或者智能手表)。

[0138] 所公开的实施方案可以表现为完整的硬件实施方案(例如包括现场可编程门阵列)、完整的软件实施方案(例如以控制根据本发明的系统)、或者包括硬件和软件元素的实施方案的形式。所述软件实施方案包括但不限于固件、常驻软件、微码等。本发明的一些实施方案可以表现为可从计算机可用或者计算机可读介质访问的计算机程序产品的形式,该介质提供计算机或者指令执行系统使用或者与其相关联的程序代码。所述计算机可用或者

计算机可读介质可以是任何装置，其可以包括：存储、通讯、传播、或者传递供指令执行系统、装置或者设备使用或者与其相关联的程序。所述介质可以是电子的、磁性的、光学的、电磁的、红外线的、或者半导体的系统(或者装置、设备)或者传播介质。

[0139] 在此探讨更进一步的实施方案。

[0140] 在此公开了一种方法M，一种新的适用于改进长期安全密码原语的实用性和/或性能和/或可实现性的安全模型，为其提供了一种新的通用结构或者新的显式协议。

[0141] 所述方法M包括运用计算安全加密函数Enc将结果状态(非纠缠)加密为量子码字的步骤。

[0142] 根据称为爱斯基摩人(强于量子含噪存储器的加密)的本安全模型的一个极限情况，Enc对于至少为tau_enc的时间是短期安全的，而存储在量子存储器中的任何信息在tau_Q<tau_enc时间内完全退相干。这符合于本发明的更高抽象水平(C0)。

[0143] 在第一进展中(C0的C1)，公开了用于发送者A和接受者B之间的消息m的实际的、长距离的、长期安全的通信，或者密钥分配(新)的显式协议。

[0144] 在这样的第一进展中：

[0145] -A和B共享长期安全对称密钥K＝K1||K2||Kauth；

[0146] -A和B可以经由公共经典信道和公共量子信道来通信；

[0147] -A和B用Kauth来认证其经典通信；

[0148] -A和B可以从K取得长期安全对称子密钥K1，以用于量子数据锁定；

[0149] -A向B发送已认证报告；

[0150] -A和B运用加密算法Enc、K2和n来取得短期安全短暂屏蔽S，其包括大的伪随机位串S；

[0151] -A将消息m编码为多符号结果状态经典量子码C(m,K1,S)；其中所述符号取自包括一组低能耗、非正交相干态的字母表，例如特别是二进制相移键控编码，每个脉冲的光量子数小于或者约等于1；并且其中屏蔽S用于通过执行对相应符号的经典索引的按符号单次密本加密来完全地模糊代码结构。

[0152] 所述多符号码字可以利用单一的U被单一地转变为单字母码字，并且接收机B可以建立可重构的干涉仪系统I来执行对应于去除屏蔽S的单一的转变，然后执行单一转变U的反转。

[0153] 为了解码，Bob运用I将进入的光学码字去屏蔽并且单一地转变，并且用实际可实现的检测器(例如单光子检测器、零差检测器、外差检测器、Kennedy接收机、Dolinar接收机、量子归零接收机)来执行单符号测量。

[0154] 在第二进展中(C0的C2)，所述方法M可以用于在爱斯基摩人模型中为长期安全密钥分配/长期安全通信建立中继器，实现了如下的功能：

[0155] -中继站不可信任，但是可以利用发送者所使用的短期秘密用方法M将量子码字加密；

[0156] -中继站可以用于补偿传播损耗；

[0157] -显而易见地，所述中继器不使用纠缠，也不使用量子存储器。

[0158] 在更进一步的进展中(C1的C4)，所述长期安全子密钥K1用于量子数据锁定，即从具有适当的锁定性能的适当的2^|K1|个单一体集合中安全地选择一个单一的转变Ulock_

K1。存在适当的集合，例如在大尺寸的码字的极限下，尺寸为|K1＝O(log(n))|的锁定密钥足够将关于尺寸为n的消息的可访问信息减少到接近0的任意值。

[0159] 利用量子数据锁定和方法M，任何人可以建立依赖于结构性代码的切实可行的方案，使得能够在A和B之间可靠地发送消息m，而锁定和联合解码增益可以用于确保安全性。

[0160] 在这样的方案中，密钥分配和安全消息传递一起完成，并且选择代码参数以使得密钥速率足以更新用于量子数据锁定的长期安全秘密比特。

[0161] 在进一步的进展中(C1的C5)，公开了一种通过二进制相移键控编码具有重复码的秘密消息传递的显式结构。例如，公开了一种用于秘密消息传递的显式结构，其中：

[0162] -量子信道是透射率为T＝t^2(功率)的玻色子有损信道；

[0163] -所使用的经典量子码是通过二进制相移键控字母表{alpha>,|-alpha>}得到的(r,2,d)(长度，尺寸，最小距离)重复码；

[0164] -干涉仪I使得Bob连续地增加r个接收信号，并且用接收功率t^2r^2|alpha|^2以速率1/r对单符号进行测量。Alice Bob每符号的容量因此随着r按比例增加。

[0165] 在爱斯基摩人框架中，攻击者受限于单符号可访问信息IE<1-h(phell(|alpha|^2)。

[0166] 其中phell(|alpha^2|＝1/2(1-sqrt(1-exp(-4*|alpha|^2))是对于二进制相移键控符号的最佳误差鉴别概率。

[0167] Eve在M上的可访问信息大约为sqrt(n)|alpha^2|。

[0168] 内部经典量子代码引出Alice和Bob之间的经典窃听信道，为此可以运用有效的、经典的外部设备以执行安全的消息传递。

[0169] 对于任意距离和相应的透射率T，增加r总是使得具有正的私有容量，尽管该容量规模为1/r(缺乏中继器)。

[0170] 在确定的距离，增加r提高信噪比，并且允许使用非常嘈杂的检测器来执行安全的消息传递。

[0171] 在进一步的进展中(C1的C6)，公开了一种用于秘密消息传递的显式结构，其中：

[0172] -量子信道是透射率为T＝t^2(功率)的玻色子有损信道；

[0173] -所使用的经典量子码是通过二进制相移键控字母表得到的(2^m-1,2^m,2^(m-1))(长度，码字数，最小距离)的Hadamard码，单一等价于(2^m,m,(2^m-1))。

[0174] 干涉仪I是由m个对数分束器和m个对数相移器构成的绿色机器，其允许Bob将接收到的单个符号的集中2^m相干地增加到一个模式中，并且用接收功率t^2|2^m*alpha|^2，以速率m/2^m来执行单个符号的测量。

[0175] 每个码字所发送的m比特中的kl部分用于锁定。

[0176] 公开了一种在遥远的A方和B方之间传递消息的方法，其包括：利用计算安全加密函数Enc将结果状态或者非纠缠量子码字加密的步骤；其中Enc对于至少为tau_enc的时间是短期安全的，而存储在量子存储器中的任何信息在严格小于tau_enc的时间tau_Q内完全退相干。

[0177] 进一步地，该方法包括如下步骤：A和B共享长期安全对称密钥K＝K1||K2||Kauth；A和B经由公共经典信道和公共量子信道来通信；A和B用Kauth来认证其经典通信；A和B从K导出长期安全对称子密钥k1以用于量子数据锁定；A向B发送认证报告n；A和B运用加密算法

Enc、K2和n来导出短期安全短暂屏蔽S,其包括大的伪随机位串S;A将消息m编码为多符号结果状态经典量子码C(m,K1,S),其中符号是从包括一组低能量并且非正交相干态的字母表中获得的,例如二进制相移键控编码,每个脉冲的光子数小于或者大约为1;并且其中屏蔽S用于通过按符号执行相应符号的经典索引的单次密本加密来完全地模糊码的结构。

[0178] 进一步地,所述方法还包括:利用单一的U将多符号码字转变为单字母码字的步骤;接收机B运用可重构的干涉仪系统I来执行单一转变的步骤;所述单一转变包括去除屏蔽S和执行单一转变U的反转的步骤。

[0179] 进一步地,该方法还包括:B利用I来去除屏蔽并且将进入的光学码字单一转变的步骤,以及执行单符号测量的步骤。

[0180] 进一步地,该方法还包括步骤:模糊光电路结构;对仅有A知道的长期安全密钥kpriv实施秘密的单一U(kpriv);因此施加输入信号的能量的物理限制L;该方法包括如下步骤:A使用具有强制限制L的硬件测量的光学电路C来实施Ukp;A公开广播公钥kpub的认证值;其中电路C可以通过本地接收密钥k的输入而适应于仅A可以反转的实施单一转变U(kpriv异或k)的电路。

[0181] 进一步地,长期安全子密钥K1用于量子数据锁定,以从适当的具有选定的锁定性能的2^|K1|个单一体的组中安全地选择一个单一转变Ulock_K1,所述选定的锁定性能是,例如,关于尺寸为n的消息的可访问信息减少到接近0的任意值。

[0182] 进一步地,对于通过二进制相移键控编码的具有重复代码的秘密消息传递,量子信道是透射率为T=t^2(功率)的玻色子有损信道;所使用的经典量子码是二进制相移键控字母表{alpha>,|-alpha>}中的(r,2,d)(长度,尺寸,最小距离)重复码。干涉仪I允许B相干地增加r个接收信号,并且以1/r的速率以接收功率t^2r^2|alpha|^2执行单符号测量,其中攻击者受限为单符号可访问信息IE<1-h(phell(|alpha|^2);其中phell(|alpha^2|=1/2(1-sqrt(1-exp(-4*|alpha|^2))是二进制相移键控符号的最佳误差辨别概率;并且其中E的可访问信息与r无关,并且通过选择|alpha^2|～1/r来限制。

[0183] 进一步地,量子信道是透射率为T=t^2(功率)的玻色子有损信道;所使用的经典量子码是二进制相移键控字母表{alpha>,|-alpha>}中的(2^m-1,2^m,2^(m-1))(长度,码字数,最小距离)Hadamard码,单一等价于(2^m,m,(2^m-1));其中每码字所发送的m比特中的kl部分用于量子锁定。

[0184] 所公开的系统包括执行所述方法的步骤的装置,其中该系统包括一个或者更多个中继站,所述站的至少一个是非可信任的,但是其利用发送者所使用的短期秘密根据所述方法将量子码字进行加密;其中所述一个或者更多个中继站根据所述方法补偿传播损耗。

[0185] 进一步地,所述系统包括一个或者更多个单光子检测器、零差检测器、外差检测器、Kennedy接收机、Dolinar接收机或者量子归零接收机。

[0186] 进一步地,所述系统包括干涉仪I,例如由m个对数分束器和m个对数相移器构成的绿色机器,其允许Bob将接收到的单个符号的集中的2^m个相干地增加到一个模式中,并且用接收功率t^2|2^m*alpha|^2,以速率m/2^m来执行单个符号的测量。

[0187] 图3图示了本发明的实施方案。

[0188] 本发明公开了一种通过公共信道在第一方和遥远的第二方之间传递经典消息的方法(300),其包括以下步骤:在所述各方之间共享密钥(310),所述共享密钥包括短期安全

密钥和/或长期安全密钥;在第一方将经典消息编码为量子码字,第一方利用共享密钥将经典消息编码为属于公知量子码的第一加密码字(320);将第一加密码字通过输出为第二码字的公共信道从第一方传递到第二方(330);通过利用由第二方控制的、放置在公共信道的输出并且由共享密钥来键控的N模式干涉仪单一地将第二码字转变为第三码字(340);在第二方通过执行对第三码字的测量并且通过利用共享密钥处理所述测量来确定出经典消息的估计(350)。

[0189] 图4图示了本发明的示例性实施方案的某些方面。该示意图显示了激光器401;A方安全边界410;B方安全边界420;公共信道F 430;经典消息M 402;消息M的估计403;信号分离器411、431;多路复用器413;相位调制器412;干涉仪I 440;粗虚线的量子信道499;细虚线的经典消息信道498;单模式光学检测器441。第一方A通过N相调制器将具有KL和/或KS的M编码到多模式经典消息光量子码字中,在B的输入的N模式干涉仪I由分束器和移相器组成,相移值由KS和KL键控。干涉仪I将所接收的码字进行转变,使得具有单模式光学检测器的单模式测量足以进行测量。遥远的B方从测量结果、KS和KL来确定M的估计。

[0190] 公开了一种通过连接A和B的有损和/或含噪的公共信道F在遥远的A方和B方之间传递经典消息M的方法,其包括以下步骤:在A和B之间共享密钥K,所述密钥K包括短期安全密钥KS和/或长期安全密钥KL;在A处将经典消息M编码为量子码字,A使用共享密钥K=(KL,KS)将经典消息M编码为属于公知量子码C的加密码字rho1(M,K);通过输出为码字rho2(M,K)的信道F将加密码字rho1(M,K)从A传递到B;通过使用由B控制的、放置在信道F的输出的、并由K来键控的N模式干涉仪I将rho2(M,K)单一转变为rho3(M,K);通过对rho3(M,K)进行测量,并通过使用共享密钥K处理所述测量来确定出在B本地的成熟(Mest)的M的估计。

[0191] 进一步地,将M编码到加密码字rho1(M,KS,KL)中的步骤,包括以下步骤:将M编码为属于公知量子码C的码字c(M,KL);利用短期安全密钥KS在c(M,KL)上执行逐字加密U(KS),生成加密的码字rho1(M,K);并且,由KS键控的干涉仪I通过逐字解密来实现U(KS)的反转;然后是独立于短期安全密钥KS的另一个单一转变。

[0192] 进一步地,使用长期安全密钥KL来选择密码C',所述秘密码C'与公知码C的子集相关联;并且使用短期安全密钥KS来对c(M,KL)执行逐字加密。

[0193] 长期安全密钥的功能是量子数据锁定。对于适当的代码C和C'、以及大尺寸的消息M,如果解码器忽略长期安全密钥KL(可以是尺寸为O(log|M|),由于量子数据锁定,则可以大大减少来自给出KS和长期安全密钥KL的rho1的M上的可访问信息,因此导致A和B之间的私有容量。

[0194] KS的功能是量子码字C(M,KL)的逐字加密。为了获悉M,这种加密模糊了任何攻击者E的码字c(M,KL)的结构,并限制了其对rho1(M,K)进行联合测量的能力。相反,B可以使用干涉仪I执行联合检测,并可以从超加性增益中受益。

[0195] 有利的是,将量子数据锁定与KL结合、以及将逐字加密与KS结合,简化了爱斯基摩人框架中量子数据锁定的实施,因为可以选择结构化、有效的可解码代码C'=C(KL),仍然具有永久的安全性。

[0196] 有利的是,将量子数据锁定与KL结合、以及将逐字加密与KS组合,使得在爱斯基摩人框架中以高于量子信道的私有容量的速率执行具有永久安全性的安全通信。

[0197] 进一步地,将经典消息M编码到rho1(M,K)中的步骤在光量子态中进行,其中所述

光量子态与多个特征相关联，所述特征包括：C中的码字是在N个玻色子模式中的N个相干态的结果状态，从包括时间模式、频率模式和空间模式的列表中选择玻色子模式；代码C的字母表由m＝2^p的m进制相移键控相干态组成，每个字母的形式为{|exp(i 2Pi k/m)alpha>，k＝0..m-1}，固定的光子数|alpha^2|比1小得多；用KS对c(M,KL)的逐字加密包括相位加密步骤，其中短期安全密钥KS用于导出逐字地应用在码字的N个相干态上的N个独立相移的值，其中所述相移用p＝log2(m)比特编码，因此KS的尺寸为p*N。

[0198] 进一步地，由B控制的干涉仪I与至少一个特征相关联，其包括：I是由分束器和移相器组成的N模式玻色子干涉仪；至少一个相移由相位调制器控制，所述相位调制器配置为应用m＝2^p的所述m进制相移，以及应用取决于短期安全密钥KS的值；给予短期安全密钥KS，干涉仪I配置为实施相位解密并将rho2(M,K)转变为rho3(M,KL)，选择干涉仪I的结构，使得rho3(M,KL)对应于在公共信道F上没有噪声的单模式状态，从而允许使用单模式光学检测器在rho3(M,KL)上执行测量。

[0199] 进一步地，所述方法包括使用中继站，所述中继站包括放置在量子信道上的放大器，该放大器补偿传播损耗，其中在实施方案中，所述中继站或者不了解K＝(KS,KL)，或者在另一个实施方案中给予对短期安全密钥KS的部分访问。

[0200] 这样的放大器构成非可信任的中继器。给与rho1(K,M)和对KS的部分访问，M上的中继器的可访问信息被限制在M的可访问信息之下，导致A和B之间的秘密容量，至于包括中继站的任何攻击者，因此不需要被信任。在一些实施方案中，所述字母表是对应于p＝2的四进制相移键控(QPSK)，并且字母可以由两个比特来描述，b1编码Pi相移，b2编码Pi/2相移。相反，对于码字C(M,KL)中的N个相干态中的每一个，Ks包含两个比特c1和c2来加密相位。在这种情况下，并且当在中继器中使用相位敏感放大器时，必须将c2的N个值发送到中继站，使得在执行N模式下的相位敏感放大之前，可以在c2＝1的每个模式下实施Pi/2相移。

[0201] 在实施方案中(特定协议)：M是1比特消息b；量子信道是透射率T＝t^2(功率)的玻色子损耗信道；所使用的代码C是m＝2或者4的m进制相移键控字母表的[N,2,D](长度，码字数，最小距离)重复码；用KS逐字相位加密在于使用KS的log2(m)*N比特对每个相干态的相位进行单次密本加密，所述相位由用于每个相干态的log2(m)比特来描述；干涉仪I是深度为log2(N)的二叉树，将N个相干态的振幅相干地增加到一个单一模式中；所述光学检测器包括与A锁相的相位敏感检测器，所述相位敏感检测器选自包括零差检测器、外差检测器、Kennedy接收机、Bondurant接收机或者Dolinar接收机的组；在中继站中所使用的放大器包括与A和B锁相的敏感放大器PSA；对alpha、N的值，放大器的位置和增益进行优化用于给定的T值。当m＝4时，KS的一半比特(PI/2相位的编码)被发送到中继器，使得在放大之前可以应用适当的Pi/2相位旋转。

[0202] 当适当地设置O(N)相移时，干涉仪可以将N个相干态的振幅相干地增加到一个模式中，导致输出状态[(-1)^b t sqrt(N)alpha>)。

[0203] 如果使用一个中继站，相位敏感放大器有利地放置在A-B信道的中间(等效损耗sqrt(T))，并且其强度增益设置为1/sqrt(T)。

[0204] 在实施方案中(特定协议)：M是1比特消息b；量子信道是透射率T＝t^2(功率)的玻色子损耗信道；所使用的代码C由两个码字组成，来自于单一等价于两个输出上的脉冲位置编码的长度为N的Hadamard码，C的字母表是m＝2或者4的m进制相移键控字母表；使用KS的

逐字相位加密在于使用KS的log2(m)*N比特对每个相干态的相位进行单次密本加密，所述相位由用于每个相干态的log2(m)比特来描述；干涉仪I是深度为log2(N)的二叉树，将N个相干态的振幅相干地增加到功率为t^2N alpha的模式中；光学检测器在于相位不敏感/敏感检测器，所述相位敏感检测器选自包括单光子检测器、光电二极管或者外差检测器的组；在中继站中所使用的放大器是补偿传播损耗的相位不敏感放大器PIA；对alpha、N的值，位置和增益进行优化用于给定的T值。

[0205] 当适当地设置0(N)相移时，干涉仪可以将N个相干态的振幅相干地增加，导致将输出功率t^2N alpha集中到模式b中。

[0206] 进一步地，在A和B之间共享短期安全密钥KS的步骤，利用计算安全技术通过使用包括密钥密码机制和/或公开密钥机制的一个或者更多个机制来执行。

[0207] 在实施方案中，所述机制是密钥机制。初始共享密钥，K＝K1||Kauth在A和B之间共享，并在此时保密。A和B认证其通信，并且KS通过使用对称技术(例如在计数器模式下使用AES_K1)执行密钥扩展来从K1导出。

[0208] 在实施方案中，所述机制是公开密钥机制。假设公钥密码学、公钥加密的短期安全性可以用于KS的密钥分配。根据权利要求1所述的方法，其可以用于公开网络，仍然具有永久安全性。

[0209] 进一步地，在A和B之间共享长期安全密钥KL的步骤通过使用长期安全机制来执行，所述机制包括使用先前在A和B之间交换的长期秘密随机消息或者密钥，利用根据权利要求1所述的步骤，用于具有永久安全性和/或量子密钥分配和/或信任的信使的密钥分配。

[0210] 本发明公开了一种包括代码指令的计算机程序产品，当其在计算机上运行时，其执行根据权利要求1至10中的任一项所述的步骤。

[0211] 本发明公开了一种系统，其包括用于执行所述方法的一个或者更多个步骤的装置。

[0212] 进一步地，所述系统包括：存储安全数据(KS,KL)的A(A)的安全边界；存储安全数据(KS,KL)的B(B)的安全边界；至少以N个模式发射的相干光源(S)；可选的信号分离器(D)，其可以分离N个模式的每一个或者部分；由A控制的单模式相位调制器设备(PM)作用在N个模式中的每一个上；可以组合N个模式的每一个或者部分的可选的N模式多路复用器(M)；从A到B至少一个光量子信道F；可选的信号分离器(D)，其可以分离N个模式的每一个或者部分；由分束器和移相器组成的N模式干涉仪I，一些由B主动控制；和单模式光学检测器(SMD)。

[0213] 进一步地，所述系统包括：以N个模式发射相干光的激光器；放置在N个模式中的每一个上的相位调制器，其在相干态的m进制相移键控星座图内调制每个模式的状态；所应用的相位调制取决于KS和KL，其导致N模式加密码字rho1(M,K)；从A到B的至少一个光量子信道；由分束器和主动控制的移相器组成的N模式干涉仪；在B处的光学检测器；以及在A和B处的计算装置。

[0214] 进一步地，根据本发明并且实施所述方法的一个或者更多个步骤的系统，其包括以下一个或者更多个：在N个模式下发射相干光的激光器；放置在N个模式中的每一个上的相位调制器，其将由KS、{Theta1,Theta2,...ThetaN}以及c(M,KL)的二进制相移键控编码一起加密的相移进行调制，导致N模式码字rho1(M,K)；从A到B至少一个光量子信道；由分束

器和主动控制的移相器组成的N模式干涉仪;在B处的光学检测器;在A处和B处的计算装置。

[0215] 在一些实施方案中,光学的码分多址技术可以用于实施本发明的实施方案。在一些实施方案中,正交频分复用技术可以用于,特别地依赖于频谱编码和锁模激光器。在一些实施方案中,光学编码可以与空间光调制器结合,在多个空间模式下执行。

[0216] 进一步地,根据本发明的系统包括以下一个或者更多个:锁模激光器、脉冲激光器和/或连续波激光器;相位调制器和/或振幅调制器;光开关;相位敏感放大器和/或相位不敏感放大器;波分多路复用滤波器和/或组合器,和/或分插多路复用器;时间延迟干涉仪和/或光学快速傅里叶变换干涉仪;选自包括单光子检测器、零差检测器、外差检测器、Kennedy接收机、Dolinar接收机、Bondurant接收机或者量子归零接收机的组中的一个或者更多个检测器。

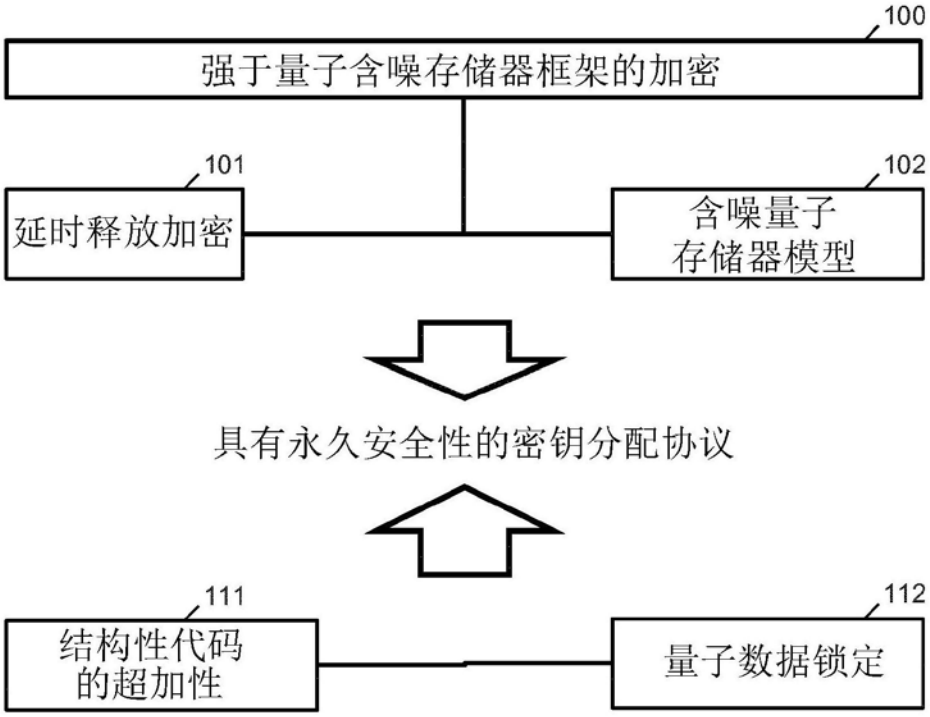

100
强于量子含噪存储器框架的加密
101
延时释放加密
102
含噪量子
存储器模型
具有永久安全性的密钥分配协议
111
结构性代码
的超加性
112
量子数据锁定

图1

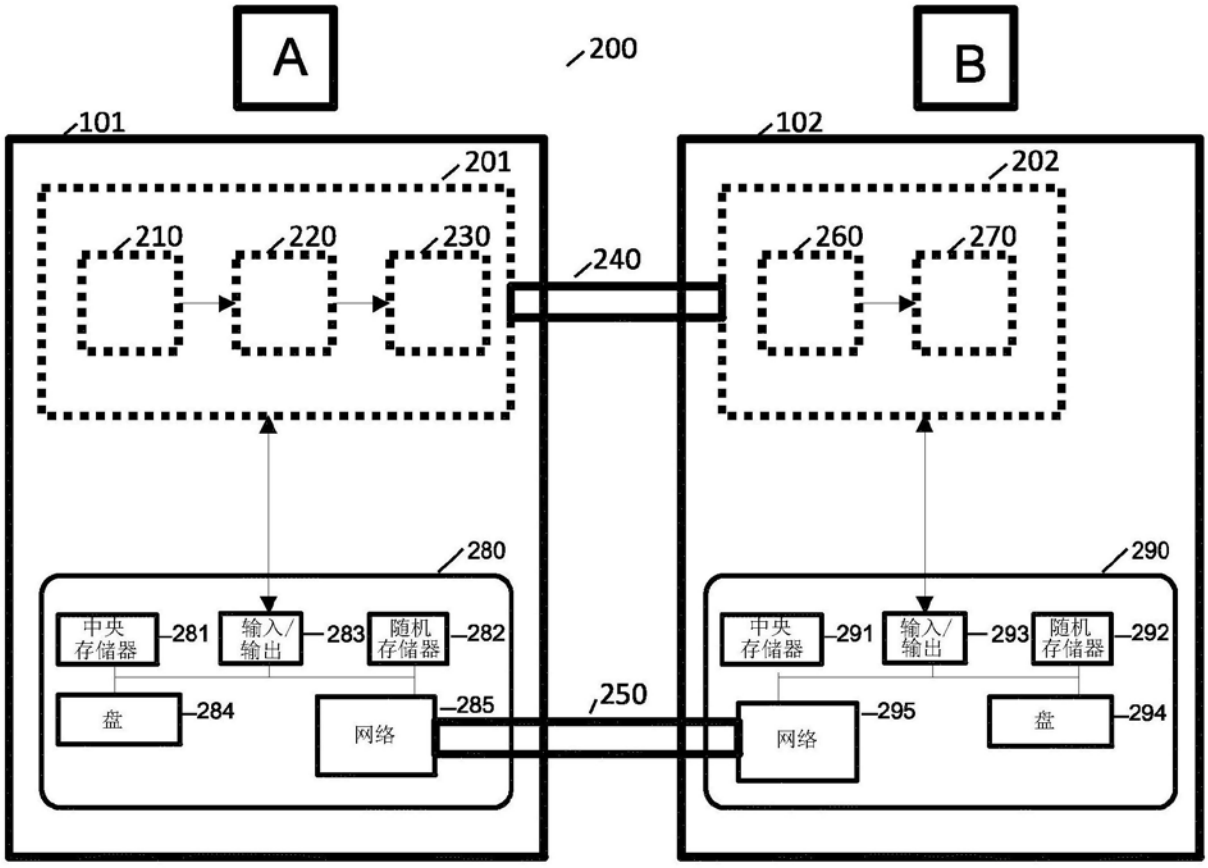

A
200
B
101
102
201
202
210
220
230
240
260
270
280
290
中央
存储器
281
输入/
输出
283
随机
存储器
282
盘
284
网络
285
250
中央
存储器
291
输入/
输出
293
随机
存储器
292
网络
295
盘
294

图2

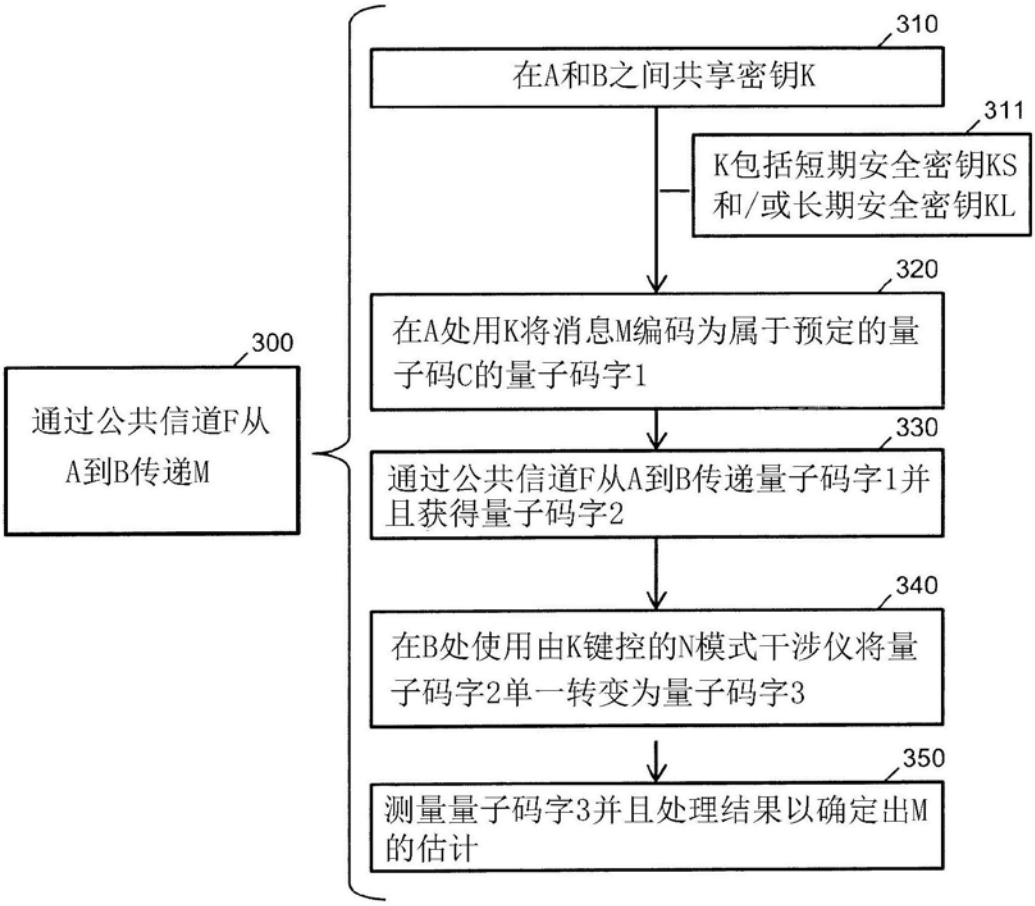

310
在A和B之间共享密钥K
311
K包括短期安全密钥KS和/或长期安全密钥KL
320
在A处用K将消息M编码为属于预定的量子码C的量子码字1
300
通过公共信道F从A到B传递M
330
通过公共信道F从A到B传递量子码字1并且获得量子码字2
340
在B处使用由K键控的N模式干涉仪将量子码字2单一转变为量子码字3
350
测量量子码字3并且处理结果以确定出M的估计

图3

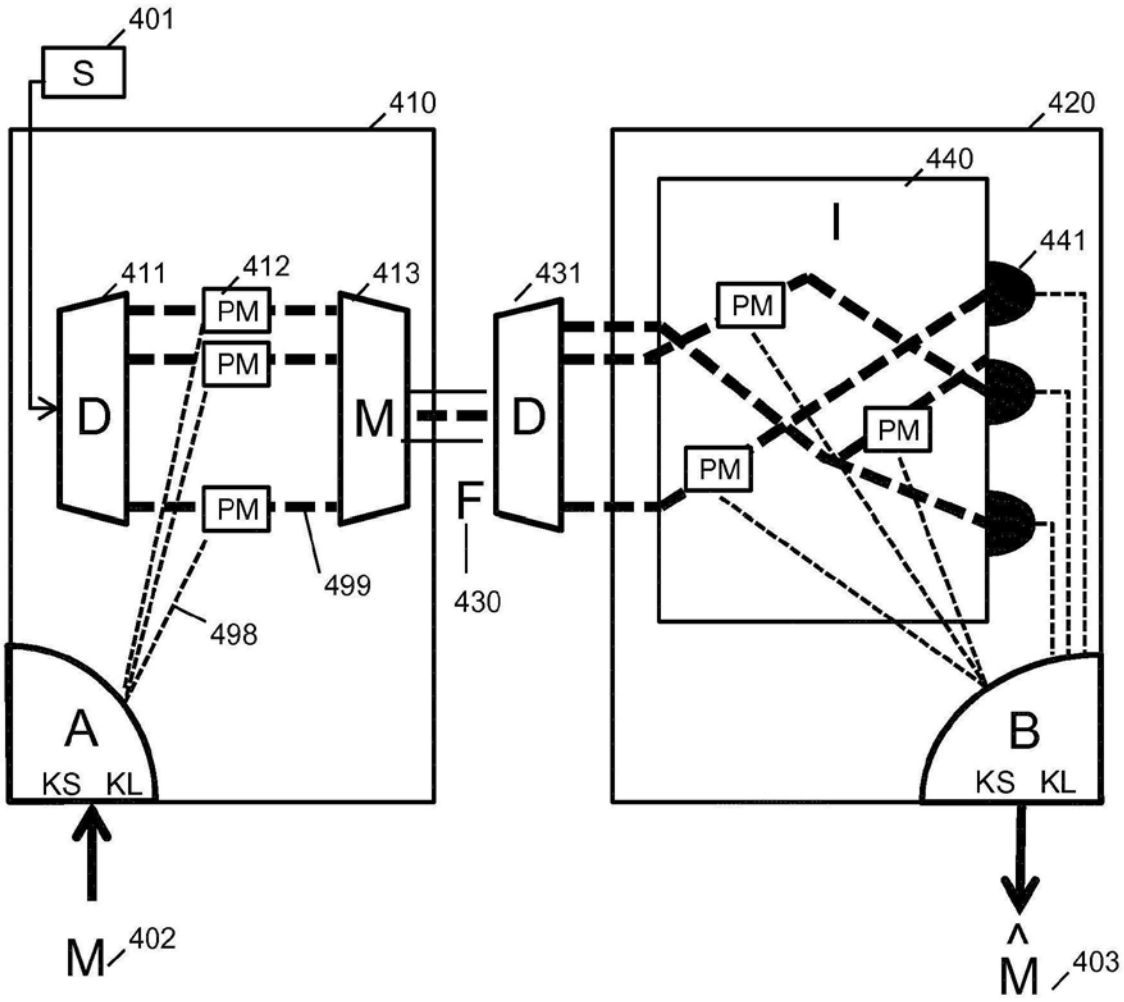

401
S
410
420
440
I
441
411
412
413
431
PM
PM
PM
PM
PM
D
M
D
F
430
499
498
A
KS KL
B
KS KL
M
402
M
403

图4