物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

基于Bell态粒子和单光子混合的量子安全直接通信方案的信息泄露问题

刘志昊　陈汉武

Information leakage problem in quantum secure direct communication protocol based on the mixture of Bell state particles and single photons

Liu Zhi-Hao　Chen Han-Wu

引用信息 Citation: Acta Physica Sinica, 66, 130304 (2017)　DOI: 10.7498/aps.66.130304
在线阅读 View online: http://dx.doi.org/10.7498/aps.66.130304
当期内容 View table of contents: http://wulixb.iphy.ac.cn/CN/Y2017/V66/I13

基于Bell态粒子和单光子混合的量子安全直接通信方案的信息泄露问题*

刘志昊[1)2)3)] 陈汉武[1)2)†]

1) (东南大学计算机科学与工程学院, 南京 211189)

2) (计算机网络和信息集成教育部重点实验室 (东南大学), 南京 211189)

3) (Centre for Quantum Software and Information, Faculty of Engineering and Information Technology, University of Technology Sydney, NSW 2007, Australia)

(2016 年 12 月 30 日收到; 2017 年 3 月 14 日收到修改稿)

最近, 一种基于 Bell 态粒子和单光子混合的量子安全直接通信方案 [物理学报 **65** 230301(2016)] 被提出. 文章宣称一个量子态可以编码 3 比特经典信息, 从而使得协议具有很高的信息传输效率. 不幸的是, 该协议存在信息泄露问题: 编码在单光子上的 3 比特经典信息有 2 比特被泄露, 而编码在 Bell 态上的 3 比特经典信息有 1 比特被泄露, 所以它不是一个安全的直接量子通信方案. 在保留原协议思想且尽可能少地更改原协议的基础上, 我们提出一种改进的消息编码规则, 从而解决信息泄露问题, 使之成为一个高效、安全的量子通信协议. 衷心希望研究者能对量子安全通信协议中信息泄露问题引起足够重视, 设计真正安全的量子通信协议.

关键词: 信息泄露, 单光子, Bell 态, 量子安全直接通信

PACS: 03.67.Hk, 03.67.Dd **DOI:** 10.7498/aps.66.130304

1 引 言

现在我们已经步入了云计算和大数据时代[1−8], 数据的安全性显得尤为重要. 通常, 人们使用加密的方法来确保数据的安全或者将相关信息进行隐藏[9,10]. 在使用加密的方法中, 密钥往往需要频繁更换, 而距离遥远的双方如何产生真正安全的密钥在经典密码学中是一个比较难以解决的问题, 所以密钥的产生往往建立在暂未证明的数学困难问题的计算复杂性上. 不同于经典密码学, 量子密码学提供了一套完全不同的思路和方法, 它以物理基本原理为基础, 具有理论上无条件安全性. 当然, 如果设计者考虑不周, 设计的量子密码协议就有可能被窃听者主动攻击[11−20]. 信息泄露[21−25]是另一种安全性问题, 指窃听者在不采取主动攻击的情况下, 只要获得了公共信道的信息, 就可以推导出关于秘密的部分消息, 是一种被动攻击类型. 在设计量子安全通信协议时, 大家既要考虑如何防范主动攻击, 又要防止信息泄露问题的存在. 信息泄露问题往往存在于量子对话或双向量子安全直接通信协议中[21−23,25]. 然而, 我们发现在某些 (单向) 量子安全通信协议中, 此问题同样存在[24].

量子安全直接通信是一种不需要事先建立密钥而直接在量子信道上安全地传输秘密信息的量子通信模式[26]. 它可以使用量子纠缠[26,27], 也可以不使用量子纠缠[28]. 量子安全直接通信最近在实验上有很大发展, 实现了噪声环境下的基于单光子的量子安全直接通信[29], 并且利用先进的量子存储, 演示了文献 [26, 27] 中基于纠缠的量子安全直接通信[30]. 最近, 曹正文等[31]提出了利用块传

* 国家自然科学基金 (批准号: 61502101, 61170321)、江苏省自然科学基金 (批准号: BK20140651, BK20140823)、PAPD 和 CICAEET 资助的课题.

† 通信作者. E-mail: hw_chen@seu.edu.cn

输思想[26,27] 基于Bell态粒子和单光子混合的量子安全直接通信方案. 他们宣称, 光源使用Bell态粒子和单光子的混合, 是为了达到更高的编码容量, 即一个量子态可以加载3 比特的经典信息, 从而可以提高信道容量和通信传输效率. 然而, 经过仔细思考, 我们发现该协议存在信息泄露问题: 编码在单光子上的3比特经典信息有2比特被泄露, 而编码在Bell态上的3 比特经典信息有1比特被泄露. 平均来说, 一次消息编码有1.5比特的信息被确定地泄露, 所以该方案不是一个安全的直接量子通信方案. 在保留原协议思想且尽可能少地更改原协议的基础上, 我们提出了一种改进的消息编码规则, 使之成为一个高效、安全的量子通信协议.

2 原协议描述

原协议[31] 可描述如下.

1) Alice制备一串单光子序列$S_{\rm s}$和一串Bell态(即EPR纠缠粒子对)序列. 每个单光子随机地处于 $|H\rangle(|0\rangle)$, $|V\rangle(|1\rangle)$, $|L\rangle(|+\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle))$, $|R\rangle(|-\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle))$ 四个态中的其中一个, 每对Bell态随机地处于$|\varphi^-\rangle$, $|\psi^+\rangle$, $|\psi^-\rangle$, $|\varphi^+\rangle$四个态中的其中一个. Alice抽取所有Bell 态中的第一个粒子构成序列$S_{\rm A}$, 所有剩余的第二个粒子构成序列$S_{\rm B}$.

2) Alice将$S_{\rm B}$发给Bob而将$S_{\rm A}$保留. Bob收到序列$S_{\rm B}$后随机地选取部分粒子进行单光子测量, 即Bob随机选取Z基$\{|0\rangle, |1\rangle\}$或X基$\{|+\rangle, |-\rangle\}$对抽样粒子进行测量, 并将其测量结果、位置及其测量基信息通过不能被篡改的经典信道发给Alice.

3) Alice收到Bob发送的信息后, 利用和Bob相同的测量基对在$S_{\rm A}$中与Bob抽样粒子对应的粒子进行单光子测量, 并将自己的测量结果与Bob发送过来的测量结果做对比, 分析错误率. Alice根据错误率判断量子信道是否存在窃听. 若错误率高于初期定好的可容忍的阈值, 抛弃已接收序列且终止通信, 如果低于该阈值则说明量子信道不存在窃听, 可以进行下一步通信.

4) Alice按照之前约定好的编码规则, 将信息序列M编码在序列$S_{\rm A}$(去除用于安全检测的粒子)和单光子序列$S_{\rm s}$上, 形成混合量子态编码序列$S_{\rm A\text{-}S}$. 编码规则为: $|H\rangle \to 000$, $|V\rangle \to 001$, $|L\rangle \to 010$, $|R\rangle \to 011$, $|\varphi^+\rangle \to 100$, $|\varphi^-\rangle \to 101$, $|\psi^+\rangle \to 110$, $|\psi^-\rangle \to 111$. 注: 此处需用到酉操作将在步骤1制备的初始态转化为对应的编码信息后的状态, 否则无法完成消息编码, 但原文没有明确说明. 如在步骤1制备的某一初始态为$|R\rangle$, 但欲传输的信息为010, 则编码信息后的量子态应为$|L\rangle$, 这需要酉操作将$|R\rangle$转化为$|L\rangle$. 当然, 在步骤1时, 就可根据欲传输的消息来制备相应的态.

5) Alice先将已编码序列$S_{\rm A\text{-}S}$顺序重排构成新序列S_1, 再加入部分用于窃听检测的单光子构成发送序列S_2发给Bob.

6) Bob收到序列S_2后利用光纤中的光延时对其进行延迟, 以防公布位置后部分量子态未发送完导致信息泄露. Alice公布检测粒子的位置信息和测量基, Bob对这些检测粒子利用Alice公布的测量基进行单光子测量. Bob将测量结果告知Alice. Alice将自己制备的初始粒子状态与Bob告知的测量结果做对比, 分析错误率. 注: 此步骤原论文描述为: "Bob收到序列S_2后利用光纤中的光延时对其进行延迟, 以防公布位置后部分量子态未发送完导致信息泄露. Alice公布检测粒子的位置信息, Bob对这些检测粒子进行单光子测量, 如同步骤2. Alice利用Bob告知的测量基信息对序列S_2中的检测粒子进行测量, 并将测量结果与Bob告知的测量结果做对比, 分析错误率, 如同步骤3." 事实上, 原文描述存在问题, 既然序列S_2已经从Alice发送给Bob, 那么Alice手中再无其他光子, 也就不可能测量S_2中的检测粒子.

7) Alice将序列S_1中各粒子原来的顺序、位置和测量基信息发给Bob. Bob按照Alice告知的信息恢复原编码序列$S_{\rm A\text{-}S}$, 并结合序列$S_{\rm B}$(去除用于安全检测的粒子), 对其中粒子或粒子对进行相应的Z基测量或X基测量或Bell基联合测量, 将测量结果结合编码规则进行译码, 最终得到原信息序列M.

3 信息泄露问题及其改进策略

表面上看, 该量子安全直接通信协议具有编码容量高、信息传输效率高等特点[31], "光源使用Bell态粒子和单光子的混合, 是为了达到更高的编码容量, 即一个量子态可以加载3比特的经典信息, 从而可以提高信道容量和通信传输效率." 但是, 如果

仔细思考, 人们不难发现, 该量子安全直接通信方案存在严重的信息泄露问题. 为了方便Bob进行信息解码, Alice必须在协议第7步公布序列S_1中各粒子原来的顺序、位置和测量基. 这样, Bob才可以恢复序列$S_{\text{A-S}}$, 并进行正确的单粒子或者Bell基联合测量. 现在我们将重点放在协议是否存在信息泄露问题上. 事实上, 当Alice公布哪些粒子需要进行Z基测量、哪些粒子需要进行X基测量、哪些粒子需要进行Bell基联合测量时, 窃听者(Eve)能获得一部分Alice发送的秘密消息. 具体为: 当Alice公布某一编码粒子需进行Z基测量时, Eve知道此粒子状态为$|H\rangle$或$|V\rangle$, 即可知Alice编码的消息为000或者001, 也就是说, Eve可以确切知道对应编码消息的第一和第二比特必为00; 当Alice公布某一编码粒子需进行X基测量时, Eve知道此粒子状态为$|L\rangle$或$|R\rangle$, 即可知Alice编码的消息为010或者011, 也就是说, Eve可以确切知道对应编码消息的第一和第二比特必为01; 当Alice公布某粒子对需进行Bell基联合测量时, Eve知道Alice编码的消息为100, 101, 110或者111, 也就是说, Eve可以确切知道对应编码信息的第一比特必为1. 平均来说, Eve可以确切知道Alice发送的一半消息.

事实上, 传输n量子比特, 最多可携带n经典比特的信息[32]. 在原量子安全直接通信方案中, 一次消息编解码平均传输了1.5量子比特, 所以平均最多只能保密传输1.5比特信息, 否则将存在安全性漏洞. 在尽量保留原协议思想和尽可能少改动原协议的前提下, 我们可以更改消息编码规则, 将其改造为信息传输量最大且无信息泄露的协议. 改进后的消息编码规则为(见表1): $|H\rangle \to 0$, $|V\rangle \to 1$, $|L\rangle \to 0$, $|R\rangle \to 1$, $|\varphi^+\rangle \to 00$, $|\varphi^-\rangle \to 01$, $|\psi^+\rangle \to 10$, $|\psi^-\rangle \to 11$.

表1 改进后的消息编码方案

Table 1. The improved message encoding scheme.

消息比特	单粒子态	消息比特	Bell态
0	$\|H\rangle$	00	$\|\varphi^+$
1	$\|V\rangle$	01	$\|\varphi^-$
0	$\|L\rangle$	10	$\|\psi^+$
1	$\|R\rangle$	11	$\|\psi^-$

从改进后的消息编码规则可以看出, 即使Alice在协议第7步将序列S_1中各粒子原来的顺序、位置和测量基信息发给Bob, Eve获得这些信息后并不能推导出任何有关秘密消息的信息. 例如, Eve即使知道, Alice公布信息后, Bob需对某消息编码粒子进行X基测量, 但Eve并不知道该粒子编码的比特为0还是1. 显然, 在改进消息编码方案的量子安全直接通信中, 平均1量子比特编码1经典比特信息, 编码效率达到Helovo界[32], 且不存在信息泄露问题.

由于只改进了消息编码规则, 所以改进后的协议与原协议具有应对主动攻击相同的能力. 故在此不在赘述.

4 结 论

总之, 曹正文等[31]提出的基于Bell态粒子和单光子混合的量子安全直接通信方案存在信息泄露问题: 编码在单光子上的3比特经典信息有2比特被泄露, 而编码在Bell态上的3比特经典信息有1比特被泄露. 所以该方案不是一个安全的量子直接通信方案. 在保留原协议思想且尽可能少更改原协议的基础上, 我们提出了一种改进的消息编码规则, 使之成为一个高效、安全的量子通信协议. 我们希望研究者能对量子安全通信协议中信息泄露问题引起足够重视, 设计真正安全的量子通信协议.

参考文献

[1] Fu Z, Sun X, Liu Q, Zhou L, Shu J 2015 *IEICE Trans. Commun.* **E98B** 190

[2] Ma T, Zhou J, Tang M, Tian Y, Al-Dhelaan A, Al-Rodhaan M, Lee S 2015 *IEICE Trans. Inf. Syst.* **E98D** 902

[3] Fu Z, Huang F, Sun X, Vasilakos A, Yang C-N 2016 *IEEE Transactions on Services Computing* DOI: 10.1109/TSC.2016.2622697

[4] Fu Z, Ren K, Shu J, Sun X, Huang F 2016 *IEEE Trans. Parallel Distrib. Syst.* **27** 2546

[5] Fu Z, Sun X, Ji S, Xie G 2016 *The 35th Annual IEEE International Conference on Computer Communications (IEEE INFOCOM 2016)*, San Francisco, CA, 10–14 April, 2016 p1

[6] Fu Z, Wu X, Guan C, Sun X, Ren K 2016 *IEEE Trans. Inf. Foren. Sec.* **11** 2706

[7] Xia Z, Wang X, Sun X, Wang Q 2016 *IEEE Trans. Parallel Distrib. Syst.* **27** 340

[8] Xia Z, Wang X, Zhang L, Qin Z, Sun X, Ren K 2016 *IEEE T. Inf. Foren. Sec.* **11** 2594

[9] Chen X, Chen S, Wu Y 2017 *J. Internet Technol.* **18** 91

[10] Yuan C, Xia Z, Sun X 2017 *J. Internet Technol.* **18** 209
[11] Zhang Y S, Li C F, Guo G C 2001 *Phys. Rev. A* **6303** 036301
[12] Cai Q Y 2003 *Phys. Rev. Lett.* **91** 109801
[13] Gao F, Wen Q Y, Zhu F C 2007 *Phys. Lett. A* **360** 748
[14] Song J, Zhang S 2007 *Phys. Lett. A* **360** 746
[15] Gao F, Wen Q Y, Zhu F C 2008 *Chin. Phys. B* **17** 3189
[16] Hao L, Li J, Long G 2010 *Sci. China: Phys. Mech. Astron.* **53** 491
[17] Liu Z H, Chen H W, Liu W J, Xu J, Li Z Q 2011 *Int. J. Quantum. Inf.* **9** 1329
[18] Liu Z H, Chen H W, Wang D, Li W Q 2014 *Quantum Inf. Process.* **13** 1345
[19] Liu Z H, Chen H W 2016 *Chin. Phys. B* **25** 080308
[20] Liu Z, Chen H, Liu W 2016 *Int. J. Theor. Phys.* **55** 4564
[21] Gao F, Guo F Z, Wen Q Y, Zhu F C 2008 *Sci. China Ser. G: Phys. Mech. Astron.* **51** 559
[22] Tan Y G, Cai Q Y 2008 *Int. J. Quantum. Inf.* **6** 325
[23] Liu Z H, Chen H W 2013 *Chin. Phys. Lett.* **30** 079901
[24] Liu Z H, Chen H W, Liu W J 2016 *Chin. Phys. Lett.* **33** 070305
[25] Liu Z H, Chen H W, Liu W J 2016 *Int. J. Theor. Phys.* **55** 4681
[26] Long G L, Liu X S 2002 *Phys. Rev. A* **65** 032302
[27] Deng F G, Long G L, Liu X S 2003 *Phys. Rev. A* **68** 042317
[28] Deng F G, Long G L 2004 *Phys. Rev. A* **69** 052319
[29] Hu J Y, Yu B, Jing M Y, Xiao L T, Jia S T, Qin G Q, Long G L 2016 *Light: Sci. Appl.* **5** e16144
[30] Zhang W, Ding D S, Sheng Y B, Zhou L, Shi B S, Guo G C 2016 arXiv:1609.09184
[31] Cao Z W, Zhao G, Zhang S H, Feng X Y, Peng J Y 2016 *Acta Phys. Sin.* **65** 230301 (in Chinese) [曹正文, 赵光, 张爽浩, 冯晓毅, 彭进业 2016 物理学报 **65** 230301])
[32] Nielsen M A, Chuang I L 2000 *Quantum Computation and Quantum Information (10th Anniversary Edition)* (New York: Cambridge University Press) p535

Information leakage problem in quantum secure direct communication protocol based on the mixture of Bell state particles and single photons*

Liu Zhi-Hao[1)2)3)] Chen Han-Wu[1)2)†]

1) (*School of Computer Science and Engineering, Southeast University, Nanjing 211189, China*)

2) (*Key Laboratory of Computer Network and Information Integration (Southeast University), Ministry of Education, Nanjing 211189, China*)

3) (*Centre for Quantum Software and Information, Faculty of Engineering and Information Technology, University of Technology Sydney, NSW 2007, Australia*)

(Received 30 December 2016; revised manuscript received 14 March 2017)

Abstract

Recently, a quantum secure direct communication (QSDC) protocol based on the mixture of Bell state particles and single photons [*Acta Phys. Sin.* **65** 230301(2016)] was put forward. In this QSDC protocol, the single photons and the Bell states were both used as information carriers. To be specific, each Bell state as well as single photon was encoded by three bits of classical information. After the sender told the receiver how to measure the particles, the receiver could read out the secret message sent by the sender. Speciously, the information transmission efficiency of this protocol was high. Unfortunately, there exists the information leakage problem in this protocol. When the sender announces that the receiver uses the Z-basis to measure a single photon, everyone knows that the sent secret message is 000 or 001, that is, the first two bits are leaked out; when the sender announces that the receiver uses the X-basis to measure a single photon, everyone knows that the sent secret message is 010 or 011, that is, the first two bits are leaked out too; when the sender announces that the receiver uses the Bell-basis to measure a pair of particles from a Bell state, everyone knows that the sent secret message is 100, 101, 110 or 111, that is, the first bit is leaked out. In a word, two of the three bits of classical information encoded in a single photon, and one of the three bits of classical information encoded in a Bell state are leaked out. Therefore, this scheme is not secure. On the basis of keeping the original idea and changing the contents of the protocol as less as possible, we put forward an improved message encoding rule to solve the information leakage problem, that is, the single photon is only encoded by one bit of classical information, and the Bell state is only encoded by two bits of classical information. In fact, this makes the information capacity of the improved protocol achieves the Helovo bound. So it has high coding capacity. We hope researchers pay more attention to the information leakage problem in quantum secure communication protocols, and thus design truly secure ones.

Keywords: information leakage, single photon, Bell state, quantum secure direct communication

PACS: 03.67.Hk, 03.67.Dd **DOI:** 10.7498/aps.66.130304

* Project supported by the National Natural Science Foundation of China (Grant Nos. 61502101, 61170321), Natural Science Foundation of Jiangsu Province, China (Grant Nos. BK20140651, BK20140823), PAPD and CICAEET.

† Corresponding author. E-mail: hw_chen@seu.edu.cn