一种基于树型网络的可验证多方量子密钥分配协议

沙倚天[1] 李天一[1] 贾 玮[2,3] 姚铭艺[1]

[1](国网江苏省电力有限公司南京供电分公司 江苏 南京 210024)

[2](南京南瑞国盾量子技术有限公司 江苏 南京 210016)

[3](南瑞集团有限公司(国网电力科学研究院有限公司) 江苏 南京 210016)

摘 要 借助可信中心的协助,引入用户身份验证和密钥验证机制,提出一种适用于电力通信系统的树型网络可验证多方量子密钥分配协议。利用带密钥的单向 hash 函数技术同时对每个用户进行身份验证和密钥验证,保证两者可以在同一个步骤中完成。发送者和接收者之间无需进行公开讨论,节省了资源,降低了成本。和其他利用纠缠资源的协议相比,该协议采用单光子作为量子信息载体,且单光子不需要存储,在技术上更容易实现。通过对该协议进行安全性分析,表明该协议在理论上是安全的。

关键词 多方量子密钥分配 树型网路 身份验证 密钥验证

中图分类号 TP309 **文献标识码** A DOI:10.3969/j.issn.1000-386x.2019.08.054

A VERIFIABLE MULTI-PARTY QUANTUM KEY DISTRIBUTION PROTOCOL BASED ON TREE NETWORK

Sha Yitian[1] Li Tianyi[1] Jia Wei[2,3] Yao Mingyi[1]

[1](*Nanjing Power Supply Company, State Grid Jiangsu Electric Power Co., Ltd., Nanjing 210024, Jiangsu, China*)

[2](*NRGD Quantum Technology Co., Ltd., Nanjing 210016, Jiangsu, China*)

[3](*NARI Group Corporation / State Grid Electric Power Research Institute, Nanjing 210016, Jiangsu, China*)

Abstract With the help of Trust Center, we introduced user authentication and key authentication mechanism, and proposed a verifiable multi-party quantum key distribution protocol based on tree network for power communication system. Using one-way hash function with key to simultaneously authenticate and verify each user ensured that both can be completed in the same step. There is no need for open discussion between sender and receiver, saving resources and reducing costs. Compared with other protocols using entanglement resources, this protocol used single photon as quantum information carrier, and single photon did not need to be stored, so it was easier to implement technically. The security analysis of the protocol shows that the protocol is theoretically secure.

Keywords Multi-party quantum key distribution Tree network Identity authentication Key authentication

0 引 言

2016 年 8 月,世界上第一颗量子科学实验卫星“墨子”在中国成功发射。2017 年 9 月,建立了连接北京和上海,总长度超过 2 000 公里的量子通信骨干网“量子京沪干线”。量子通信骨干网将推动量子安全通信在金融、政务、国防和电子信息领域的大规模应用。量子密钥分配(QKD)是量子信息安全领域中最重要的应用之一。在电力行业,将 QKD 与电力通信系统相结合逐渐成为电网企业关注的焦点。

QKD 以经典密码学和量子力学为基础,利用量子力学原理来实现通信双方共享一组随机序列组成的密钥。1984 年,Bennett 等提出了第一个著名的量子密钥

收稿日期:2018 - 11 - 12。国网江苏省电力有限公司科技项目(J2018023)。**沙倚天**,工程师,主研领域:电力信息技术,信息安全。**李天一**,工程师。**贾玮**,工程师。**姚铭艺**,工程师。

分配协议——BB84[1],在协议中两个用户通过交换单粒子来创建一个共享密钥。随后,人们提出了一系列基于单粒子或纠缠态的 QKD 协议[2-5],其中大部分协议是点对点之间的密钥分配。而在实际中,一个量子网络[6]由多个节点组成,要求节点(用户)之间进行密钥分配。为此,人们提出了多用户量子密钥分配协议(Multi-User Quantum Key Distribution, MQKD)。1995 年,Phoenix 等[7]提出了第一个基于单光子的 MQKD 协议,展示了如何利用单光子的特性在光网络上实现密钥分配。为了提高传输效率,2010 年,Hong 等[8]提出基于 Bell 态的 MUQKD 协议,利用纠缠交换实现密钥分配,并且对于 n 个用户的通信系统,仅需要 n 个量子信道,Guo 等[9]提出了一种基于 GHZ 态网络量子密钥分配的 MQKD 协议,其中,一种方案以概率方式在合法用户之间分配密钥,而另一种方案以确定性方式发送确定性消息。上述协议中的纠缠制备和量子存储并不容易实现,并且上述协议一般仅实现了密钥验证,身份验证[10]的问题函待解决。

2014 年,Guan 等[11]提出了一个基于单光子的三方可验证量子密钥分配协议,在星型网络拓扑结构上实现身份验证和密钥验证。该协议仅适用于星型网络拓扑结构,并不适用树型网络拓扑结构。2016 年,Lin 等[12]提出适用于树型网络拓扑结构的单光子可验证 MQKD 协议,其中身份验证和密钥验证是分阶段执行的,其成本开销会更大,且面临一些安全隐患。为了解决以上问题,本文提出一个基于树型网络的可验证多方量子密钥分配协议,同时对每个用户进行身份验证和密钥验证,两者在一个步骤中完成,而无需发送者和接收者之间的公开讨论,节省了资源。此外,本协议利用单光子作为量子信息载体,且单光子不需要存储,更容易实现。

1　预备知识

1.1　电力通信系统网络

电力通信系统网络一般体现为树型拓扑结构。例如,江苏电网安全稳定实时预警及协调防御系统(Electric Power Alarming and Coordinated Control System, EACCS)具有典型的树型拓扑结构,如图 1 所示,该图充分展示了中心站与主站、主站与子站、子站与执行站之间的上下层次关系。

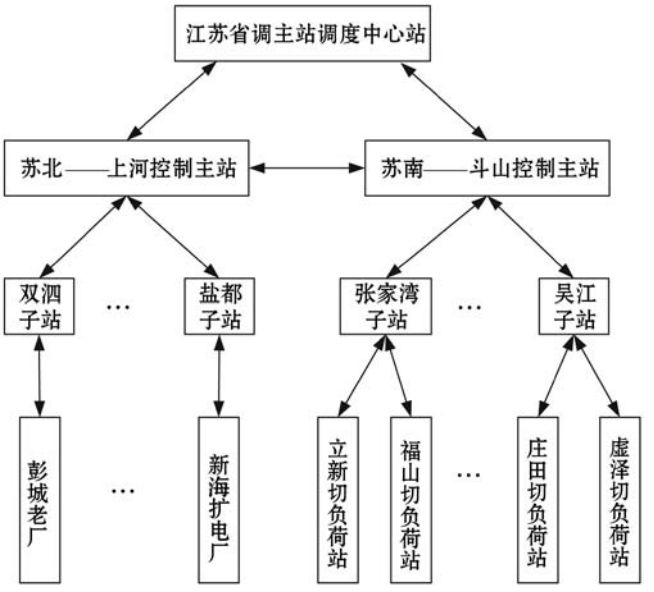

图 1　EACCS 系统控制结构

1.2　量子态

比特是经典计算和经典信息里的基本概念,其状态或 0 或 1。类似地,在量子计算中,量子比特的两个可能状态是 $|0\rangle$ 和 $|1\rangle$,此外,量子比特可以是状态的线性组合,常称为叠加态:

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1}$$

式中:α 和 β 是复数且满足 $|\alpha^2| + |\beta|^2 = 1$。向量 $|0\rangle$ 和 $|1\rangle$ 可以被表示为:

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \quad |1\rangle = \begin{pmatrix}0\\1\end{pmatrix} \tag{2}$$

量子比特 $|\varphi\rangle$ 用向量的形式表示为 $|\varphi\rangle = \begin{pmatrix}\alpha\\\beta\end{pmatrix}$。

1.3　量子测量

量子测量由一组测量算子 $\{M_m\}$ 描述,这些算子作用在被测系统状态空间上,指标 m 表示实验中可能的测量结果。若在测量前,量子系统的最新状态是 $|\psi\rangle$,则结果 m 发生的可能性由下式给出:

$$p(m) = \langle\psi|M_m^+ M_m|\psi\rangle \tag{3}$$

且测量后系统的状态为:

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^+ M_m|\psi\rangle}} \tag{4}$$

测量算子满足完备性方程:

$$\sum_m M_m^+ M_m = I \tag{5}$$

2　协议设计

从图 1 可知,电力通信系统网络结构可以抽象成树型拓扑结构图,如图 2 所示。

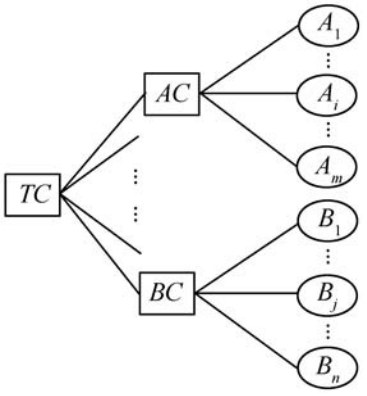

图 2 电力通信系统树型拓扑结构图

假设树型网络中任意两个不同的终端用户 A_i 和 B_j 希望生成一个安全的会话密钥。假设根节点 TC 及 A_i 和 B_j 所属的中间节点 AC、BC 为可信的；A_i、AC、BC、B_j 的身份 U_{Ai}、U_{AC}、U_{BC}、U_{Bj} 是公开的，长度均为 k 比特；AC 与 A_i 共享一个长度为 n 比特的安全主密钥 K_{TAi}，BC 与 B_j 共享一个长度为 n 比特的安全主密钥 K_{TBj}，K_{TAi} 和 K_{TBj} 对无关的第三方是保密的。中间节点 $AC(BC)$ 和用户 $A_i(B_j)$ 根据预先共享的主密钥 $K_{TAi}(K_{TBj})$ 约定测量基。如果 $(K_{TAi})_s=0$，就选择基 $D=\{|+\rangle,|-\rangle\}$，否则选择基 $R=\{|0\rangle,|1\rangle\}$，其中，$(K_{TAi})_s$ 表示密钥 K_{TAi} 的第 s 位，$s=1,2,\cdots,n$。本文协议描述如图 3 所示。

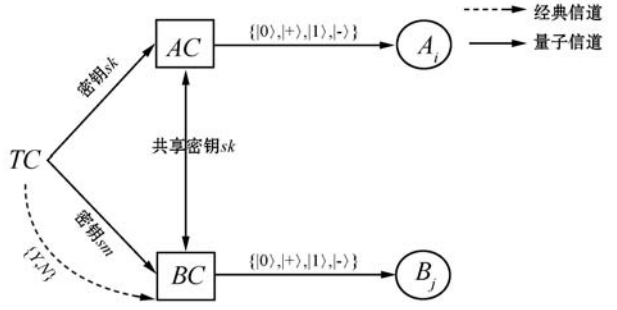

图 3 本文协议的密钥分配过程

步骤 1 根节点 TC 与中间节点 $AC(BC)$ 利用文献[13]中的方法生成一个 u 比特安全的密钥 $sk(sm)$。TC 将 sk 与 sm 进行对比分析，若对应的比特相同记为“Y”不同记为“N”。TC 通过公开的信道将所得的比较结果告诉 AC 和 BC，这样，AC 和 BC 可以共享彼此的量子密钥 sm 和 sk。

步骤 2 TC 生成长度为 l 比特的随机数 r_{TAC}、r_{TBC}。$AC(BC)$ 生成长度为 l 比特的随机数 $r_{TAi}(r_{TBj})$ 并计算中间量：

$$R_{TAi}=h(K_{TAi},r_{TAi},r_{TAC})\oplus(sk\|U_{Ai}\|U_{AC}\|U_{BC}\|U_{Bj})$$

$$(R_{TBj}=h(K_{TBj},r_{TBj},r_{TBC})\oplus(sk\|U_{Bj}\|U_{BC}\|U_{AC}\|U_{Ai}))$$

式中：$h(\cdot):\{0,1\}^*\rightarrow\{0,1\}^m$ 是输出为 m 比特的单向哈希函数，并且有等式 $n=m+2l$ 和 $m=u+4k$ 成立。注意，$(K_{TAi})_s((K_{TBj})_s)$ 中长度为 n 比特，sk 长度为 u 比特，U_{AC}、U_{BC}、U_{Ai}、U_{Bj} 长度均为 k 比特。

步骤 3 $AC(BC)$ 根据 $(r_{TAi}\|r_{TAC}\|R_{TAi})_s$（$(r_{TBj}\|r_{TBC}\|R_{TBj})_s$）和 $(K_{TAi})_s$（$(K_{TBj})_s$）制备量子比特 Q_{TAi}（Q_{TBj}）并发送给，制备规则如下：

$$(Q_{TAi})_s=\begin{cases}|+\rangle & (r_{TAi}\|r_{TAC}\|R_{TAi})_s=0 \text{ and}(K_{TAi})_s=0\\ |-\rangle & (r_{TAi}\|r_{TAC}\|R_{TAi})_s=1 \text{ and}(K_{TAi})_s=0\\ |0\rangle & (r_{TAi}\|r_{TAC}\|R_{TAi})_s=0 \text{ and}(K_{TAi})_s=1\\ |1\rangle & (r_{TAi}\|r_{TAC}\|R_{TAi})_s=1 \text{ and}(K_{TAi})_s=1\end{cases} \tag{6}$$

式中：$s=1,2,\cdots,n$。

步骤 4 $A_i(B_j)$ 根据 $K_{TAi}(K_{TBj})$ 来测量接收到的量子比特 $Q_{TAi}(Q_{TBj})$。如果 $(K_{TAi})_s=0((K_{TBj})_s=0)$，则用 D 基进行测量；否则，用 R 基进行测量。

步骤 5 $A_i(B_j)$ 得到测量结果 $r'_{TAi}\|r'_{TAC}\|R'_{TAi}(r'_{TBj}\|r'_{TBC}\|R'_{TBj})$ 后，若 $h(K_{TAi},r'_{TAi},r'_{TAC})\oplus R'_{TAi}(h(K_{TBj},r'_{TBj},r'_{TBC})\oplus R'_{TBj})$ 的后 $4k$ 比特与 $U_{Ai}\|U_{AC}\|U_{BC}\|U_{Bj}(U_{Bj}\|U_{BC}\|U_{AC}\|U_{Ai})$ 相同，则说明中间节点和用户均合法，否则，通信终止。接下来，$A_i(B_j)$ 选取 $h(K_{TAi},r'_{TAi},r'_{TAC})\oplus R'_{TAi}(h(K_{TBj},r'_{TBj},r'_{TBC})\oplus R'_{TBj})$ 前 u 比特作为密钥 sk'（sk''）。

3 协议分析

3.1 正确性分析

不失一般性，选取两个用户 A_i 与 B_j 来验证协议的正确性。假设 $U_{AC}=100$，$U_{BC}=001$，$U_{Ai}=101$，$U_{Bj}=011$；$K_{TAi}=10001100100000101010001110100011$，$K_{TBj}=01011000111101011110001110000100$；$AC(BC)$ 和 $A_i(B_j)$ 根据预先共享的主密钥 $K_{TAi}(K_{TBj})$ 约定测量基。如果 $(K_{TAi})_s=0$，就选择基 $D=\{|+\rangle,|-\rangle\}$，否则选择基 $R=\{|0\rangle,|1\rangle\}$，其中，$(K_{TAi})_s$ 表示密钥 K_{TAi} 的第 s 位，$s=1,2,\cdots,n$。TC 与 AC、BC 的共享密钥分别为 $sk=1010100000010111$、$sm=0011100101111011$。

步骤 1 中，$AC(BC)$ 可以得到彼此的密钥 $sm(sk)$。

步骤 2 中，TC 生成随机数 $r_{TAC}=00$，AC 生成随机数 $r_{TAi}=10$，计算 $h(K_{TAi},r_{TAi},r_{TAC})=110100110101000101011101000$ 和 $R_{TAi}=h(K_{TAi},r_{TAi},r_{TAC})\oplus(sk\|U_{Ai}\|U_{AC}\|U_{BC}\|U_{Bj})=011110110100011000011110011$。同理，$TC$ 生成随机数 $r_{TBC}=01$，BC 生成随机数 $r_{TBj}=11$，计算 $h(K_{TBj},r_{TBj},r_{TBC})=01011010001100011111110110001$ 和 $R_{TBj}=h(K_{TBj},r_{TBj},r_{TBC})\oplus(sk\|U_{Bj}\|U_{BC}\|U_{AC}\|U_{Ai})=111100100010011010011101010$1。

步骤 3 中，AC 根据 $(r_{TAi}\|r_{TAC}\|R_{TAi})_s$ 和 $(K_{TAi})_s(s=1,\cdots,n)$，制备量子比特 $(Q_{TAi})_s=|1\rangle|+\rangle|+\rangle$

$|+\rangle|0\rangle|1\rangle|-\rangle|-\rangle|1\rangle|+\rangle|-\rangle|-\rangle|+\rangle|-\rangle|0\rangle|+\rangle|0\rangle|-\rangle|1>|+\rangle|+\rangle|+\rangle|0\rangle|1\rangle|1\rangle|-\rangle|1\rangle|+\rangle|+\rangle|+\rangle|1\rangle|1\rangle$并发送给 A_i。同理,BC 制备量子比特$(Q_{TBj})_s = |-\rangle|1\rangle|+\rangle|1\rangle|1\rangle|-\rangle|1\rangle|-\rangle|-\rangle|-\rangle|0\rangle|0\rangle|1\rangle|0\rangle|+\rangle|0\rangle|-\rangle|0\rangle|0\rangle|1\rangle|1\rangle|+\rangle|-\rangle|+\rangle|0\rangle|1\rangle|1\rangle|-\rangle|+\rangle|-\rangle|+\rangle|1\rangle|+\rangle|-\rangle$并发送给 B_j。

步骤 4 中,A_i根据 K_{TAi}来测量接收到的量子比特,得到结果 $r'_{TAi}\|r'_{TAC}\|R'_{TAi}$ = 10000111101101000110000111100011。同理,B_j得到测量结果 $r'_{TBj}\|r'_{TBC}\|R'_{TBj}$ = 11011111001000100110100111010101。

步骤 5 中,A_i得到测量结果 $r'_{TAi}\|r'_{TAC}\|R'_{TAi}$后,若 $h(K_{TAi},r'_{TAi},r'_{TAC})\oplus R'_{TAi}$的后 $4k$ 比特与 $U_{Ai}\|U_{AC}\|U_{BC}\|U_{Bj}$ = 101100001011 相同,则说明中间节点和用户均合法,否则,通信终止。接下来,A_i选取 $h(K_{TAi},r'_{TAi},r'_{TAC})\oplus R'_{TAi}$前 u 比特得到密钥 sk' = 1010100000010111。同理,B_j可判断中间节点和用户是否合法,若合法,得到密钥 sk'' = 1010100000010111,否则,协议终止。

以上过程中,密钥串数值、测量基和量子态变换情况如表 1 所示。

表 1　本文协议中密钥串数值、测量基和量子态对应关系

编号	(1)	(2)	(3)	(4)	(5)	(6)	(7)
K_{TAi}	1	0	0	0	1	1	0
Base	*R*	*D*	*D*	*D*	*R*	*R*	*D*
$(r_{TAi}\|r_{TAC}\|R_{TAi})_i$	1	0	0	0	0	1	1
Q_{TAi}	$\|1\rangle$	$\|+\rangle$	$\|+\rangle$	$\|+\rangle$	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$
Base	*R*	*D*	*D*	*D*	*R*	*R*	*D*
$r'_{TAi}\|r'_{TAC}\|R'_{TAi}$	1	0	0	0	0	1	1
sk'	1	0	1	0	1	0	0
编号	(8)	(9)	…	(16)	(17)	…	(32)
K_{TAi}	0	1	…	0	1	…	1
Base	*D*	*R*	…	*D*	*R*	…	*R*
$(r_{TAi}\|r_{TAC}\|R_{TAi})_i$	1	1	…	0	0	…	1
Q_{TAi}	$\|-\rangle$	$\|1\rangle$	…	$\|+\rangle$	$\|0\rangle$	…	$\|1\rangle$
Base	*D*	*R*	…	*D*	*R*	…	*R*
$r'_{TAi}\|r'_{TAC}\|R'_{TAi}$	1	1	…	0	0	…	1
sk'	0	0	…	1	–	…	–

3.2　安全性分析

本文主要从以下 5 种常见攻击情形来分析所提协议的安全性。它们分别是假冒根节点攻击,即假冒 *TC* 攻击;假冒中间节点攻击,即假冒 $AC(BC)$ 攻击;假冒用户攻击,即假冒 $A_i(B_j)$ 攻击;在线猜测攻击;离线猜测攻击。

(1) *假冒 TC 攻击*　在步骤 1 中,根节点 *TC* 与中间节点 $AC(BC)$利用文献[13]方法生成一个 u 比特安全的密钥 $sk(sm)$。该方法已被证明 $AC(BC)$可以有效地对 *TC* 进行身份验证和密钥验证[13]。因此,攻击者假冒 *TC* 会在 $AC(BC)$对 *TC* 的身份验证和密钥验证中被检测到。

(2) *假冒 AC(BC) 攻击*　本协议中,假冒 $AC(BC)$攻击可分为两种情形:在中间节点 $AC(BC)$与根节点 *TC* 进行密钥分配时;在中间节点 $AC(BC)$与用户 $A_i(B_j)$进行密钥分配时。第一种情形与假冒 *TC* 攻击类似,其安全性已在上面方法中被证明。第二种情形,因为攻击者不知道 $K_{TAi}(K_{TBj})$,在步骤 3 和步骤 4 中单比特将以$\frac{1}{4}$的概率出错,密钥串被发现的概率为 $1-\left(\frac{3}{4}\right)^n$,$n$ 为比特串长度。总而言之,假冒 $AC(BC)$攻击将会被检测到。

(3) *假冒 $A_i(B_j)$ 攻击*　在步骤 4 中,在用户 $A_i(B_j)$测量接受到的量子比特 $Q_{TAi}(Q_{TBj})$时,如果一个攻击者假冒用户 $A_i(B_j)$,因为攻击者不知道 $K_{TAi}(K_{TBj})$,在步骤 4 中单比特将以$\frac{1}{4}$的概率出现错误,密钥串被发现的概率为 $1-\left(\frac{3}{4}\right)^n$,$n$ 为比特串长度。因此,假冒 $A_i(B_j)$将会被检测到。

(4) *在线猜测攻击*　在线猜测攻击在现有的密钥分配协议中是不可避免的,尽管攻击者可以在本文协议上执行在线猜测攻击,但他必须花费大量精力来验证他对主密钥 $K_{TAi}(K_{TBj})$的猜测,即在目标协议上多次执行在线猜测攻击。这使得中间节点 $AC(BC)$和用户可以采取一些对付这种攻击的对策。例如,一旦中间节点和用户注意到一定数量的本文协议执行失败,则应该更新预共享密钥,这样就可以避免在线猜测攻击。

(5) *离线猜测攻击*　在步骤 2 中,哈希值 $h(K_{TAi},r_{TAi},r_{TAC})(h(K_{TBj},r_{TBj},r_{TBC}))$被用来加密序列 $sk\|U_{Ai}\|U_{AC}\|U_{BC}\|U_{Bj}(sk\|U_{Bj}\|U_{BC}\|U_{AC}\|U_{Ai})$。因此,即使重发相同的会话密钥,接收者也不会收到相同的量子比特。这也使得窃听者不能够执行离线猜测攻击来猜测量子信道上的基。

4　协议比较

通过选取加密机制、量子信道、易受中间人攻击、

易受被动攻击、易受重放攻击、信息载体、身份验证、密钥验证和网络等指标,将本文协议与其他多方密钥分配协议[14-17]进行了比较,相关参数如表 2 所示。

表 2 本文协议与其他协议比较

指标	协议 1[14]	协议 2[15]	协议 3[16]	协议 4[17]	本协议
加密机制	经典	量子	量子 + 经典	量子 + 经典	量子 + 经典
量子信道	N	Y	Y	Y	Y
易受中间人攻击	N	N	Y	Y	N
易受被动攻击	Y	N	N	N	N
易受重放攻击	Y	N	N	N	N
信息载体	经典载体	纠缠态	纠缠态	N	N
身份验证	Y	N	Y	Y	Y
密钥验证	N	Y	N	N	Y
网络	星型网络	星型网络	星型网络	星型网络	树形网络

由表 2 可知,与经典的多方密钥分配协议 1[14]相比,所提协议更有效抵抗重放和被动攻击,具有更高的安全性。本协议采用单光子实现,且单光子无需存储,协议 2 和协议 3 需要存储纠缠态,这在当前技术条件下很难实现。与协议 3 和协议 4 相比,所提协议可以避免中间人攻击,不仅可以实现身份验证还可以实现密钥验证。总而言之,本协议可以同时对每个用户进行身份验证和密钥验证,两者可以在一个步骤中完成,而无需发送者和接收者之间的公开讨论,节省了资源,降低了成本。和其他利用纠缠资源的协议相比,本协议采用单光子作为量子信息载体,且单光子不需要存储,在技术上更容易实现。

5 结 语

本文将经典密码学和量子密码学的优点相结合,提出了一种适用于电力通信系统的密钥分配协议。与经典的三方密钥分配协议相比,本协议更容易抵抗重放和被动攻击。与其他三方量子密钥分配协议相比,本协议不仅实现了用户身份验证还实现了密钥验证,并且两者可以在一个步骤中同时完成,而无需发送者和接收者之间的公开讨论,节省了资源,降低了成本。安全性分析表明,本协议在理论上是安全的。在方案实现方面,和其他利用纠缠资源的协议相比,本协议采用单光子作为量子信息载体,且单光子不需要存储,这在当前技术下更容易实现。

当然,本协议仍有一些不足可以改进。例如,本协议不考虑量子信道中的噪声,但在实际环境中这不可避免,下一步工作会考虑存在量子信道噪声的情形下,使用纠错码和密钥演化来设计一种适用于电力通信系统的树型网络可验证多方量子密钥分配协议。

参 考 文 献

[1] Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing[J]. Theoretical Computer Science, 2014, 560: 7-11.

[2] Scarani V, Bechmann-Pasquinucci H, Cerf N J, et al. The Security of Practical Quantum Key Distribution[J]. Review of Modern Physics, 2009, 81(3): 1301.

[3] Meslouhi A, Hassouni Y. Cryptanalysis on authenticated semi-quantum key distribution protocol using Bell states[J]. Quantum Information Processing, 2017, 16(1): 18.

[4] Zhu K N, Zhou N R, Wang Y Q, et al. Semi-Quantum Key Distribution Protocols with GHZ States[J]. International Journal of Theoretical Physics, 2018, 57(12): 3621-3631.

[5] 颛孙少帅, 陈红, 蔡晓霞. 基于 GHZ 态纠缠交换的量子确定性密钥分发方案[J]. 量子电子学报, 2015, 32(1): 83-89.

[6] 吴华, 赵于康, 赵勇, 等. 实用化光纤量子加密电话网络和高速数据传输系统——现场应用与安全管理[J]. 中国科学:信息科学, 2014, 44(3): 312-321.

[7] Phoenix S D, Barnett S, Townsend P, et al. Multi-user Quantum Cryptography on Optical Networks[J]. Optica Acta International Journal of Optics, 1995, 42(6): 1155-1163.

[8] Hong C H, Heo J O, Khym G L, et al. N quantum channels are sufficient for Multi-user Quantum Key Distribution protocol between n users[J]. Optics Communications, 2010, 283(12): 2644-2646.

[9] Guo Y, Shi R, Zeng G. Secure networking quantum key distribution schemes with Greenberger-Horne-Zeilinger states[J]. Physica Scripta, 2010, 81(4): 045006.

[10] Renuka D, Chenna Reddy P. Integrated Classical and Quantum Cryptography Scheme Using Three Party Authenticated Key Distribution Protocols[J]. Materials Today: Proceedings, 2018, 5(1): 1017-1023.

[11] Guan D J, Wang Y J, Zhuang E S. A practical protocol for three-party authenticated quantum key distribution[J]. Quantum Information Processing, 2014, 13(11): 2355-2374.

[12] Lin S, Wang H, Guo G D, et al. Authenticated multi-user quantum key distribution with single particles[J]. International Journal of Quantum Information, 2016, 14(1): 1650002.

[13] 王映康, 朱鹏. 基于 BB84 的量子密钥分发和身份认证[J]. 电气应用, 2015(S1): 143-146.

(下转第 333 页)

电极利用率、提高液滴操作的并行处理和减小生化实验完成时间的影响能力越高,比如,在 3 min 时限内,用 TS 在 10×10、11×11 和 12×12 芯片完成生化实验的时间分别比 TS* 减少了 10.58%、7.12% 和 4.19%。

5 结　语

本文利用功能模块的动态重构特性,在某个操作执行的过程中,适时改变其绑定的功能模块在片上的位置,增大液滴操作的并行处理,同时结合改进的禁忌搜索算法来实现功能模块的动态移位以及数字微流控生化检验的架构级调度和几何级布局,以达到提高电极利用率,最小化生化检验完成时间的目的。通过人体体液体外诊断实验的仿真,对多个算法进行比较,仿真结果验证了本文算法的有效性和可行性。而且该算法同样也可用于其他生化实验的实施,对数字微流控生化检验的系统综合具有一定的参考价值。

参 考 文 献

[1] Choi K, Ng A H C, Fobel R, et al. Digital Microfluidics [J]. Annual Review of Analytical Chemistry, 2012, 5(1): 413 – 440.

[2] Srinivasan V, Pamula V K, Fair R B. An integrated digital microfluidic lab-on-a-chip for clinical diagnostics Oil human physiological fluids [J]. Lab Chip, 2004, 4(4): 310 – 315.

[3] Kaler K, Prakash R. Droplet Microfluidics for Chip-Based Diagnostics[J]. Sensors, 2014, 14(12):23283 – 23306.

[4] Jebrail M J, Bartsch M S, Patel K D. Digital microfluidics: a versatile tool for applications in chemistry, biology and medicine[J]. Lab on a Chip, 2012, 12(14):2452 – 2463.

[5] Chakrabarty K. Design, testing, and applications of digital microfluidics-based biochips [C]//Proceedings of the 18th International Conference on VLSI Design held jointly with 4th International Conference on Embedded Systems Design, Washington, DC, USA, January 3 – 7, 2005: 221 – 226.

[6] Chakrabarty K, Su F. Design automation challenges for microfluidics-based biochips [C]//Design, Test, Integration, and Packaging of MEMS/MOEMS. Montreux, Switzerland, Jun 1 – 3, 2005: 260 – 265.

[7] Chakrabarty K, Su F. System-level design automation tools for digital [C]//CODES + ISSS, Jersey City, New Jersey, USA, 2005: 201 – 206.

[8] Chakrabarty K, Zeng J. Design automation for microfluidics-based biochips[J]. ACM Journal on Emerging Technologies in Computing Systems, 2005, 1(3): 186 – 223.

[9] Ren H, Fair R B. Micro/nano liter droplet formation and dispensing by capacitance metering and electro wetting actuation [C]//Proceedings of the 2nd IEEE Conference on Nanotechnology, 2002 IEEE-NANO Munich: IEEE, 2002: 369 – 372.

[10] Paik P, Pamula V K, Fair R B. Rapid droplet mixers for digital microfluidic systems[J]. Lab on a Chip, 2003, 3(4): 253 – 259.

[11] Pollack M G, Shenderov A D, Fair R B. Electrowetting-based actuation of droplets for integrated microfluidics[J]. Lab on a Chip, 2002, 2(2):96 – 101.

[12] Glover E. Tabu search: Part I[J]. ORSA Journal on Computinn, 1989, 1(3): 190 – 206.

[13] 贺一. 禁忌搜索及其并行化研究[D]. 重庆:西南大学, 2006.

[14] Su F, Hwang W L, Chakrabarty K. Droplet Routing in the Synthesis of Digital Microfluidic Biochips[C]//Proceedings of the Conference on Design, Automation and Test in Europe, DATE 2006, Munich, Germany, March 6 – 10, 2006. IEEE, 2006: 73 – 78.

[15] Ding J, Chakrabarty K, Fair R B. Scheduling of microfluidic operations for reconfigurable two-dimensional electrowetting arrays[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits, and Systems, 2001, 20(12):1463 – 1468.

[16] Su F, Chakrabarty K. Architectural-Level Synthesis of Digital Microfluidics-Based Biochips [C]//Proceedings of the 2004 IEEE/ACM International conference on Computer-aided design. IEEE, 2004: 223 – 228.

(上接第 319 页)

[6] 景鹏. 天地一体化网络中深度包检测应用开发[D]. 北京:北京交通大学,2017.

[7] 刘永明,王渊. 基于 DPI 和 DFI 的非法业务识别技术[J]. 软件导刊,2015,14(12):177 – 179.

[8] Deri L, Martinelli M, Bujlow T, et al. nDPI: Open-source high-speed deep packet inspection[C]// 2014 International Wireless Communications and Mobile Computing Conference (IWCMC). IEEE, 2014.

[9] 卓中流. 匿名网络追踪溯源关键技术研究[D]. 成都:电子科技大学,2018.

(上接第 324 页)

[14] 钟成, 李兴华, 宋园园, 等. 无线网络中基于共享密钥的轻量级匿名认证协议[J]. 计算机学报, 2018, 41(5): 191 – 205.

[15] 江英华, 张仕斌, 昌燕, 等. 具有双向身份认证的量子密钥分发协议[J]. 量子电子学报, 2018(1):49 – 53.

[16] 陈晓峰. 基于纠缠交换的具有双向认证的多方量子密钥分发[J]. 韶关学院学报, 2016, 37(10): 20 – 24.

[17] 陈晓峰, 刘晓芬. 基于单粒子态的双向认证多方量子密钥分发[J]. 量子电子学报, 2017, 34(3): 369 – 373.