基于单光子的多方半量子秘密共享方案

李雪杨 昌 燕* 张仕斌 代金鞘 郑 涛
(成都信息工程大学网络空间安全学院 四川 成都 610225)

摘 要 基于半量子理论,提出一种易于实现的基于单光子的多方半量子秘密共享方案,降低了量子秘密共享网络的构建成本,完成了多方秘密共享。以单光子作为初始资源,减少了对纠缠粒子的依赖,且并不要求各方具备完备的量子能力,仅需秘密分发者 Alice 拥有完备量子能力,参与者 Bob_i 拥有受限的量子能力。通过基于半量子理论的秘密共享网络完成了秘密分发者与多个参与者之间的秘密共享。安全性分析表明,该方案可以抵抗内部攻击和外部纠缠攻击,对于当前技术是安全可行的。

关键词 量子秘密共享 半量子密码学 单粒子

中图分类号 TP3 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2020.12.046

MULTI-PARTY SEMI-QUANTUM SECRET SHARING BASED ON SINGLE PARTICLES

Li Xueyang Chang Yan* Zhang Shibin Dai Jinqiao Zheng Tao
(*School of Cybersecurity*, *Chengdu University of Information Technology*, *Chengdu 610225*, *Sichuan*, *China*)

Abstract Based on the semi-quantum theory, we propose an easy-to-implement multi-party semi-quantum secret sharing scheme using single particles, which reduces the construction cost of quantum secret sharing network and completes the multi-party secret sharing. The scheme uses single particles as the initial resource to reduce the dependence on entangled particles, and does not require all parties of complete quantum capabilities. Only the secret distributor Alice has complete quantum capabilities, and the participant Bob_i has limited quantum capabilities. The secret sharing network based on semi-quantum theory completes the secret sharing between the secret distributor and multiple participants. Security analysis shows that the scheme can resist internal attacks and external entanglement attacks and is safe and feasible for current technologies.

Keywords Quantum secret sharing Semi-quantum cryptography Single particles

0 引 言

量子秘密共享是量子密码学的一个重要分支,它是经典秘密共享和量子理论的结合,它使得秘密信息(经典信息或量子编码信息)通过量子操作分发、传输和恢复。量子秘密共享的安全性基于量子力学的基本原理,这使得量子秘密共享比传统的秘密共享更为安全。

最早的量子秘密共享方案由 Hillery 等[1]提出,该方案采用 Greenberger-Horne-Zeilinger(GHZ)纠缠态粒子完成了秘密共享。此后,越来越多的基于 Bell 纠缠态或多粒子纠缠态的量子秘密共享方案被提出[2-8]。然而,Bell 态或多粒子纠缠态制备的困难性表明基于纠缠态的量子秘密共享方案在某些情况下是不值得的,毕竟实用性是量子信息论的重要追求,这些技术障碍使得此类量子秘密共享方案的实用性大大降低。对此,Guo 等[9]提出一种无纠缠的量子秘密共享方案,该

收稿日期:2019-07-17。国家自然科学基金项目(61572086,61402058);国家重点研发计划项目(2017YFB0802302);四川省高校科研创新团队项目(17TD0009);四川省学术和技术带头人培养支持经费资助项目(2016120080102643);四川省应用基础项目(2017JY0168);四川省重点研发计划项目(2018TJPT0012);四川省科技支撑计划项目(2016FZ0112,2018GZ0204);四川省重点研发项目(2018GZ0232);四川省科技成果转化平台项目(2018CC0060)。**李雪杨**,硕士生,主研领域:量子通信,信息安全。**昌燕**,教授。**张仕斌**,教授。**代金鞘**,硕士生。**郑涛**,硕士生。

方案利用单粒子完成了经典信息的秘密共享。Yan 等[10]提出一种无纠缠的多方和多方之间的量子秘密共享方案,但随后文献[11]指出该方案在粒子传输上存在安全隐患,造成秘密信息泄露,并给出了相应改进措施。此类量子秘密共享方案虽然没有采用纠缠态粒子的纠缠特性完成秘密共享,但很难保证粒子传输的安全性。且现有的量子秘密共享协议大都要求通信双方具有完备量子能力,成本和量子资源的限制严重阻碍了量子秘密共享实现商业化和大众化。

半量子密码通信是量子通信的一个研究分支,指具有完备量子能力和存在限制量子能力的通信者间的通信。它不要求通信双方都具有完备的量子能力,却又通过量子力学特性提升了通信过程的安全性,同时减少了对量子设备资源的依赖。Boyer 等[12]提出了半量子协议的定义和应用思路,并基于半量子思想提出了第一个基于 BB84 的半量子密码协议。此后,研究人员开始研究基于半量子思想的量子密码协议,将半量子密码概念应用于量子密钥分发、量子直接通信、量子隐私比较、量子秘密共享等量子密码学任务[13-16]。Li 等[17]将半量子思想扩展到量子秘密共享,提出了两个基于类 GHZ 态的半量子秘密共享方案。Wang 等[18]提出了一种基于两粒子纠缠态的半量子秘密共享方案。Li 等[19]提出了一种两粒子乘积态的半量子秘密共享方案,用$|+\rangle|+\rangle$态作为初始态,完成了三方秘密共享,这使得量子秘密共享方案更具有实用性且减少了量子资源的消耗。Xie 等[20]提出了一种基于类 GHZ 态的半量子秘密共享协议;Ye 等[21]提出了一种基于单光子的环形半量子秘密共享协议。可见,半量子通信是一种具有实践意义的通信方案,它在保证通信安全性的同时大大减少了对量子资源的依赖。受半量子密码启发,本文提出一种基于单光子的多方半量子秘密共享方案,仅采用单粒子完成多方之间的秘密共享,且降低了对量子设备的依赖,便于在实践中实施。

1　预备知识

1.1　量子秘密共享

量子秘密共享是经典秘密共享与量子密码的结合,它基于量子力学的特性来提升秘密共享的安全性。量子秘密共享中秘密分发者将经典信息编码拆分为量子态,参与者通过量子通信收到量子态后,通过量子操作恢复出秘密信息的一部分,每个参与者只能通过诚实合作才能恢复出原始秘密信息。

1.2　半量子密码通信

半量子密码通信指通信双方中一方拥有完备量子能力(量子方),另一方拥有受限的量子能力(经典方),规定经典方只能进行如下操作:

(1) 用 Z 基测量粒子;

(2) 不测量粒子,将粒子直接反射给量子方;

(3) 以 Z 基制备粒子发送给量子方;

(4) 重新对收到的粒子序列进行排序。

半量子密码通信不严格要求通信双方具有完备量子能力,减少了对量子资源的依赖,却又具备量子密码的特性,提升了安全性。

2　方案设计

假设秘密分发者 Alice 准备和 n 个接收者 Bob_i 完成长度为 M 的秘密信息共享。Alice 拥有量子能力,而 Bob_i 只拥有经典能力。为完成与 Bob_i 共享 Alice 密钥的任务,本文采用单光子构造了多方半量子秘密共享方案。

定义经典方 Bob_i 拥有的两种操作:

(1)用 Z 基($\{|0\rangle,|1\rangle\}$)测量收到的粒子,并制备一个相同量子态的新粒子发送给 Alice(简称为 MEASURE)。

(2) 将粒子没有干扰地返回给 Alice(简称为 REFLECT)。

简单起见,本文中,将测量基$\{|0\rangle,|1\rangle\}$记为 Z 基,测量基$\{|+\rangle,|-\rangle\}$记为 X 基,其中$|\pm\rangle=\frac{1}{\sqrt{2}}(|0\rangle\pm|1\rangle)$,粒子$|0\rangle$和$|1\rangle$的测量结果表示经典比特 0 和 1。

方案具体步骤如下:

步骤 1　秘密分发者 Alice 制备一串长度为 $M+T$ 的单光子序列$|S\rangle$,其中每个单光子$|S_i\rangle$随机处于四个量子态$\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$之一。

步骤 2　Alice 将$|S\rangle$发送给接收方 Bob_1。Bob_1 收到来自 Alice 的所有粒子后,Bob_1 随机的选择 M 个粒子进行 MEASURE,并对剩下的 T 个粒子进行 REFLECT。Bob_1 将 M 个粒子的测量结果表示为经典信息,记为 K_{B1}。

步骤 3　Alice 确认收到 Bob_1 的 $M+T$ 个粒子后,Bob_1 向 Alice 公布他选择 MEASURE 和选择 REFLECT 的粒子的位置。

步骤 4　Alice 开始进行窃听检测,由于 Alice 知道 Bob_1 选择 MEASURE 和选择 REFLECT 的粒子的位

置,她可以区分哪些粒子是被反射回来的,哪些粒子是被测量的。对于 T 个被反射的粒子,即 Bob_1 执行 REFLECT的粒子,Alice 使用原始的制备基去测量它们。对于 M 个被测量的粒子,即 Bob_1 执行 MEASURE 的粒子,Alice 使用 Z 基去测量它们,并将测量结果表示为经典信息 K'_{B1}。Alice 计算被 REFLECT 的粒子的错误率以及被 MEASURE 的粒子中那些原本采用 Z 基制备的粒子的错误率,如果两个错误率低于阈值,Alice 继续执行下一步骤。否则,Alice 重新开始与接收方 Bob_1 的通信。

步骤 5 重复步骤 2 - 步骤 4,Alice 将$|S\rangle$发送给接收方 $Bob_2, Bob_3, \cdots, Bob_n$,在进行窃听检测之后,Alice完成与接收方 $Bob_2, Bob_3, \cdots, Bob_n$的秘密共享。记 $Bob_2, Bob_3, \cdots, Bob_n$手中执行 MEASURE 的粒子测量结果的经典信息为 $K_{B2}, K_{B3}, \cdots, K_{Bn}$,Alice 手中对应粒子的测量结果的经典信息为 $K'_{B2}, K'_{B3}, \cdots, K'_{Bn}$。Alice对 $K'_{B1}, K'_{B2}, \cdots, K'_{Bn}$做异或运算,得到 $K_A = K'_{B1}$ XOR K'_{B2} XOR K'_{B3} XOR$\cdots$XOR K'_{Bn}。此时,Alice 建立了她与 $Bob_1, Bob_2, \cdots, Bob_n$的秘密共享关系,即长度为 M 的秘密信息 $K_A = K_{B1}$ XOR K_{B2} XOR K_{B3} XOR$\cdots$XOR K_{Bn}。只有当 $Bob_1, Bob_2, \cdots, Bob_n$通过诚实合作,他们才能共同恢复 Alice 的秘密信息 K_A。

下面以 Alice 与 Bob_1、Bob_2、Bob_3、Bob_4 的秘密共享为例,举例了 $M = 10$、$T = 5$ 时的五方半量子秘密共享过程,$K_A = K_{B1}$ XOR K_{B2} XOR K_{B3} XOR K_{B4},其中 MEASURE 和 REFLECT 操作简记为 M 和 R:

Alice 发送的粒子序列$|S\rangle$

$|+ - + + +1, -0 +10, 011 +0\rangle$

Bob_1 对接收粒子执行的操作

MRMMR,MMMMR,MRRMM

Bob_1 的测量结果的经典信息 K_{B1}

101,1011,010

Bob_1 发送以及反射给 Alice 的粒子序列

$|1 -011, 10110, 01110\rangle$

Bob_2 对接收粒子执行的操作

RMRRM,MMRRM,MMMMM

Bob_2 的测量结果的经典信息 K_{B2}

11,000,01110

Bob_2 发送以及反射给 Alice 的粒子序列

$|+1 + +1, 00 +10, 01110\rangle$

Bob_3 对接收粒子执行的操作

MMRRM,MRRMM,RMMMM

Bob_3 的测量结果的经典信息 K_{B3}

111,010,1100

Bob_3 发送以及反射给 Alice 的粒子序列

$|11 + +1, 00 +10, 01100\rangle$

Bob_4 对接收粒子执行的操作

RRMMM,MRMMM,RMMMR

Bob_4 的测量结果的经典信息 K_{B4}

001,0010,111

Bob_4 发送以及反射给 Alice 的粒子序列

$|+ -001, 00010, 01110\rangle$

Alice 的秘密信息 K_A

1011101111

3 安全性分析

本方案可以有效抵御内部参与者和外部攻击,保证量子秘密信息共享的安全性。

3.1 内部攻击

任意内部参与者 Bob_i 无法通过截获/重发攻击来获取利益。

假设 Bob_i 截获 Alice 发送给 Bob_j 的粒子序列,然后 Bob_i 制备一串新的长度为 $M + T$ 的粒子序列发送给 Bob_j,如根据自己的利益制备由$|0\rangle$或$|1\rangle$构成的粒子序列发送给 Bob_j。由于 Bob_i 不知道 Bob_j 选择 MEASURE 和 REFLECT 的位置,Alice 收到 Bob_j 的粒子后,可以通过窃听检测发现异常,因为 Bob_i 制备的粒子序列不与 Alice 制备的粒子序列相同,Alice 可以通过检查 Bob_j 执行 REFLECT 操作的粒子来发现异常。

假设 Bob_i 截获 Bob_j 发送给 Alice 的粒子序列,然后 Bob_i 制备一串新的长度为 $M + T$ 的粒子序列发送给 Alice。同样,Bob_i 不知道 Bob_j 选择 MEASURE 和 REFLECT 的位置,此后,Alice 根据 Bob_j 选择MEASURE和 REFLECT 的位置测量粒子后,可以在窃听检测中发现异常。此外,这种情况下 Alice、Bob_i、Bob_j 也无法建立秘密共享关系,因为 Alice 测得的 K'_{Bj} 不等于 K_{Bj}。

任意内部参与者 Bob_i 无法通过测量/重发攻击来窃取他人的测量结果的经典信息 K_{Bj}。

假设 Bob_i 截获并测量 Bob_j 发送给 Alice 的粒子序列,并将测量后的粒子序列重新发送给 Alice,企图在 Bob_j 公布选择 MEASURE 和 REFLECT 的粒子的位置后确定 K_{Bj}。但此前 Bob_i 不知道 Bob_j 选择 MEASURE 和 REFLECT 的位置,因此 Alice 可以通过检查 Bob_j 执行 REFLECT 操作的粒子来发现异常。

此外,任意内部参与者 Bob_i 无法通过猜测其他参与者测量结果的经典信息推测出 Alice 的完整秘密信息 K_A。

长度为 M 的秘密信息 K_A 由 $K_{B1},K_{B2},\cdots,K_{Bn}$ 按位异或得到。对于每一位异或值,假设 Bob_i 有 50% 的概率猜对其他参与者测量结果的经典信息的异或值,可以根据统计数据定量评估 Bob_i 成功推断整个消息秘密信息 K_A 的概率 P_{infer}。

$$P_{infer}=\binom{M}{k}\left(\frac{1}{2}\right)^{k}\left(\frac{1}{2}\right)^{M-k} \tag{1}$$

式中:k 表示 Bob_i 正确猜测的异或值的总数;M 表示整个秘密信息 K_A 的长度。概率 P_{infer} 符合二项分布和二项式系数。

$$\binom{M}{k}=\frac{M!}{k!(M-k)!} \tag{2}$$

通过计算 $M=256$、$M=512$、$M=1\ 024$、$M=2\ 048$ 时 Bob_i 正确猜测异或值的数量 k 下的概率 P_{infer} 可知,对于不同的 M,P_{infer} 在区间 $(0,k)$ 上存在它的最大值($P_{max}(M=256)\approx0.057\ 5$,$P_{max}(M=512)\approx0.040\ 7$,$P_{max}(M=1\ 024)\approx0.028\ 8$,$P_{max}(M=2\ 048)\approx1.480\ 4\times10^{-102}$),并且随着 M 的增大而减小。因此任意内部参与者 Bob_i 无法通过猜测推测出完整秘密信息 K_A。

3.2　外部攻击

外部窃听者 Eve 或任意内部参与者无法通过纠缠/测量攻击来获取利益。

假设攻击者 Eve 截获秘密共享过程中 Alice 发送给 Bob 的粒子串 $|S\rangle$ 以及 Bob 执行 MEASURE 和 REFLECT操作后发送给 Alice 的粒子串 $|B\rangle$,并通过单一操作矩阵运算 $\boldsymbol{E}$ 将新的辅助粒子 e 与 $|S\rangle$ 或 $|B_i\rangle$($|S_i\rangle=\{|0\rangle、|1\rangle、|+\rangle、|-\rangle\}$,$|B_i\rangle=\{|0\rangle、|1\rangle\}$)缠绕在一起形成一个更大的希尔伯特空间,那么可能出现的 4 种系统态如下:

$$\boldsymbol{E}\otimes|0e\rangle=a|0e_{00}\rangle+b|1e_{01}\rangle \tag{3}$$

$$\boldsymbol{E}\otimes|1e\rangle=b'|0e_{10}\rangle+a'|1e_{11}\rangle \tag{4}$$

式中:a、a'、b、b' 是概率幅度参数。

$$\begin{aligned}\boldsymbol{E}\otimes|+e\rangle=&\frac{1}{\sqrt{2}}(a|0e_{00}\rangle+b|1e_{01}\rangle+b'|0e_{10}\rangle+a'|1e_{11}\rangle=\\&\frac{1}{2}[|+\rangle(a|e_{00}\rangle+b|e_{01}\rangle+b'|e_{10}\rangle+\\&a'|e_{11}\rangle)+|-\rangle(a|e_{00}\rangle-b|e_{01}\rangle+\\&b'|e_{10}\rangle-a'|e_{11}\rangle)]\end{aligned} \tag{5}$$

$$\begin{aligned}\boldsymbol{E}\otimes|-e\rangle=&\frac{1}{\sqrt{2}}(a|0e_{00}\rangle+b|1e_{01}\rangle-b'|0e_{10}\rangle-a'|1e_{11}\rangle=\\&\frac{1}{2}[|+\rangle(a|e_{00}\rangle+b|e_{01}\rangle-b'|e_{10}\rangle-\\&a'|e_{11}\rangle)+|-\rangle(a|e_{00}\rangle-b|e_{01}\rangle-\\&b'|e_{10}\rangle+a'|e_{11}\rangle)]\end{aligned} \tag{6}$$

其中,$\boldsymbol{E}$ 是 Eve 的单一操作矩阵,表示为:

$$\boldsymbol{E}=\begin{pmatrix}a & b'\\ b & a'\end{pmatrix} \tag{7}$$

由 $\boldsymbol{E}$ 运算符决定的四个 $\{e_{00},e_{01},e_{10},e_{11}\}$ 纯状态满足归一化条件:

$$\sum_{\alpha,\beta\in\{0,1\}}\langle e_{\alpha,\beta}|e_{\alpha,\beta}\rangle=1 \tag{8}$$

因为 $\boldsymbol{E}\boldsymbol{E}^{*}=1$,$a,b,a',b'$ 满足以下关系:

$$\begin{gathered}|a|^2+|b|^2=1\quad|a'|^2+|b'|^2=1\\ ab^{*}=(a')^{*}b'\end{gathered} \tag{9}$$

可以获得结果:

$$|a|^2=|a'|^2\quad|b|^2=|b'|^2 \tag{10}$$

如果 Eve 的攻击粒子处于纠缠态,这种窃听者的干扰最终将不可避免地引入错误,Alice 可以通过 P_E 的概率在窃听检测过程中检测到窃听者的存在。

$$P_E=|b|^2=1-|a|^2=|b'|^2=1-|a'|^2 \tag{11}$$

如果 Eve 不想引入误差,则总粒子必须与 Eve 的辅助粒子以直积态相关。然而,在直积态下,辅助粒子 e 与 $|S_i\rangle$ 粒子或 $|B_i\rangle$ 粒子之间没有任何相关性,因此 Eve 没有得到任何有用信息,这证明了纠缠/测量攻击是徒劳的。

4　结　语

本文分析了之前主要的基于纠缠态的量子秘密共享方案,以及半量子秘密共享方案,并提出一种基于单光子的多方半量子秘密共享方案。该方案仅采用单粒子完成了量子方与多个半量子方之间的秘密共享,可以应用在更贴近实际的量子通信网络中,如 Alice 作为量子方,由网络信息服务供应商来充当,Bob_i 等经典方代表网络中的普通客户,达成安全可靠的多方秘密共享。

与以前的量子秘密共享方案不同,本文方案的优点归纳如下:(1) 本文秘密共享方案不依赖于纠缠态粒子,而是采用单粒子,在实际中具有更强的实用性。(2) 本文协议不需要经典方具备完备量子能力,降低了量子设备资源的需求。(3) 本文完成了秘密分发者与多方间的秘密共享,而不仅限于三方间的秘密共享。安全性分析表明,本文方案能够抵御内部攻击和外部纠缠攻击,在当前技术下是安全可行的。

参　考　文　献

[1] Hillery M, Buzek V, Berthiaume A. Quantum secret sharing [J]. Physical Review A, 1999, 59(3): 1829 - 1834.

[2] Bai C M, Li Z H, Xu T T, et al. A generalized information theoretical model for quantum secret sharing[J]. International Journal of Theoretical Physics, 2016, 55(11): 4972 -

4986.
[3] Deng F G, Long G L, Zhou H Y. An efficient quantum secret sharing scheme with Einstei-Podolsky-Rosen pairs[J]. Physics Letters A, 2005, 340(1-4): 43-50.
[4] 邵婷婷,张仕斌,昌燕. 基于 Bell 态的(3,3)量子秘密共享方案[J]. 计算机工程与设计, 2019, 40(5): 1210-1213, 1224.
[5] Karlsson A, Koashi M, Imoto N. Quantum entanglement for secret sharing and secret splitting[J]. Physical Review A, 1999, 59(1): 162-168.
[6] Man Z X, Xia Y J, An N B. Quantum state sharing of an arbitrary multiqubit state using nonmaximally entangled GHZ states[J]. The European Physical Journal D, 2007, 42(2): 333-340.
[7] Wang X J, An L X, Yu X T, et al. Multilayer quantum secret sharing based on GHZ state and generalized Bell basis measurement in multiparty agents[J]. Physics Letters A, 2017, 381(38): 3282-3288.
[8] Liu C J, Li Z H, Bai C M, et al. Quantum-Secret-Sharing scheme based on local distinguishability of orthogonal seven-qudit entangled states[J]. International Journal of Theoretical Physics, 2017, 57(2): 428-442.
[9] Guo G P, Guo G C. Quantum secret sharing without entanglement[J]. Physics Letters A, 2003, 310(4): 247-251.
[10] Yan F L, Gao T. Quantum secret sharing between multiparty and multiparty without entanglement[J]. Physical Review A, 2005, 72(1): 12304.
[11] Han L F, Liu Y M, Shi S H, et al. Improving the security of a quantum secret sharing protocol between multiparty and multiparty without entanglement[J]. Physics Letters A, 2007, 361(1-2): 24-28.
[12] Boyer M, Kenigsberg D, Mor T. Quantum key distribution with classical Bob[C]//2007 First International Conference on Quantum, Nano, and Micro Technologies (ICQNM'07), 2007.
[13] Boyer M, Gelles R, Kenigsberg D, et al. Semiquantum key distribution[J]. Physical Review A, 2009, 79(3): 032341.
[14] Shukla C, Thapliyal K, Pathak A. Semi-quantum communication: protocols for key agreement, controlled secure direct communication and dialogue[J]. Quantum Information Processing, 2017, 16(12): 295.
[15] Yan L L, Sun Y H, Chang Y, et al. Semi-quantum protocol for deterministic secure quantum communication using Bell states[J]. Quantum Information Processing, 2018, 17(11): 315.
[16] Sun Y H, Yan L L, Chang Y, et al. Two semi-quantum secure direct communication protocols based on Bell states[J]. Modern Physics Letters A, 2019, 34(1): 1950004.
[17] Li Q, Long D Y, Chan W H. Semi-quantum secret sharing using entangled states[J]. Physical Review A, 2010, 82(2): 2422-2427.
[18] Wang J, Zhang S, Zhang Q, et al. Semiquantum secret sharing using two-particle entangled state[J]. International Journal of Quantum Information, 2012, 10(5): 1250050.
[19] Li L, Qiu D, Mateus P. Quantum secret sharing with classical Bobs[J]. Journal of Physics A: Mathematical and Theoretical, 2013, 46(4): 045304.
[20] Xie C, Li L, Qiu D. A novel semi-quantum secret sharing scheme of specific bits[J]. International Journal of Theoretical Physics, 2015, 54(10): 3819-3824.
[21] Ye C Q, Ye T Y. Circular semi-quantum secret sharing using single particles[J]. Communications in Theoretical Physics, 2018, 70(6): 661-671.

(上接第 243 页)

[15] Wang H, Cen Y, He Z, et al. Robust generalized low-rank decomposition of multimatrices for image recovery[J]. IEEE Transactions on Multimedia, 2017, 19(5): 969-983.
[16] Zhao X, An G, Cen Y, et al. Robust generalized low rank approximations of matrices for video denoising[C]//2016 IEEE 13th International Conference on Signal Processing(ICSP), 2016.
[17] Boyd S, Parikh N, Chu E, et al. Distributed optimization and statistical learning via the alternating direction method of multipliers[M]. Now Foundations and Trends, 2011.
[18] 史加荣,郑秀云,魏宗田,等. 低秩矩阵恢复算法综述[J]. 计算机应用研究, 2013, 30(6): 1601-1605.

(上接第 259 页)

[12] 尹国强. 基于改进人工势场法的移动机器人路径规划研究[D]. 天津:天津理工大学, 2017.
[13] 侯翔. 基于人工势场和量子遗传算法的移动机器人路径规划方法[J]. 计算机应用与软件, 2018, 35(6): 263-266, 333.
[14] Boor V, Overmars M H, Stappen A FVD. The gaussian sampling strategy for probabilistic roadmap planners[C]//1999 IEEE International Conference on Robotics and Automation, 1999.
[15] Hsu D, Jiang T, Reif J, et al. The bridge test for sampling narrow passages with probabilistic roadmap planners[C]//2003 IEEE International Conference on Robotics and Automation, 2003.
[16] Missiuro P E, Roy N. Adapting probabilistic roadmaps to handle uncertain maps[C]//2006 IEEE International Conference on Robotics and Automation, 2006.
[17] Bohlin R, Kavraki L E. Path planning using lazy PRM[C]//2000 IEEE International Conference on Robotics and Automation, 2000.