

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局



(10) 国际公布号
WO 2024/198393 A1

(43) 国际公布日
2024 年 10 月 3 日 (03.10.2024)

(51) 国际专利分类号:
H04L 9/08 (2006.01) **H04B 10/54** (2013.01)
H04B 10/556 (2013.01)

(21) 国际申请号: PCT/CN2023/132375

(22) 国际申请日: 2023 年 11 月 17 日 (17.11.2023)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202310341896.9 2023 年 3 月 31 日 (31.03.2023) CN

(71) 申请人: 清华大学 (TSINGHUA UNIVERSITY) [CN/
CN]; 中国北京市海淀区清华园 1 号,
Beijing 100084 (CN)。

(72) 发明人: 马雄峰 (MA, Xiongfeng); 中国北京市海淀区清华园 1 号, Beijing 100084 (CN)。黄溢智 (HUANG, Yizhi); 中国北京市海淀区清华园 1 号, Beijing 100084 (CN)。

(74) 代理人: 北京亿腾知识产权代理事务所 (普通合伙) (E-TONE INTELLECTUAL PROPERTY FIRM (GENERAL PARTNERSHIP)); 中国北京市海淀区中关村紫金数码园 3 号楼 707, Beijing 100190 (CN)。

(81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ,

(54) Title: QUANTUM KEY DISTRIBUTION METHOD, APPARATUS AND SYSTEM

(54) 发明名称: 一种量子密钥分发方法、装置和系统

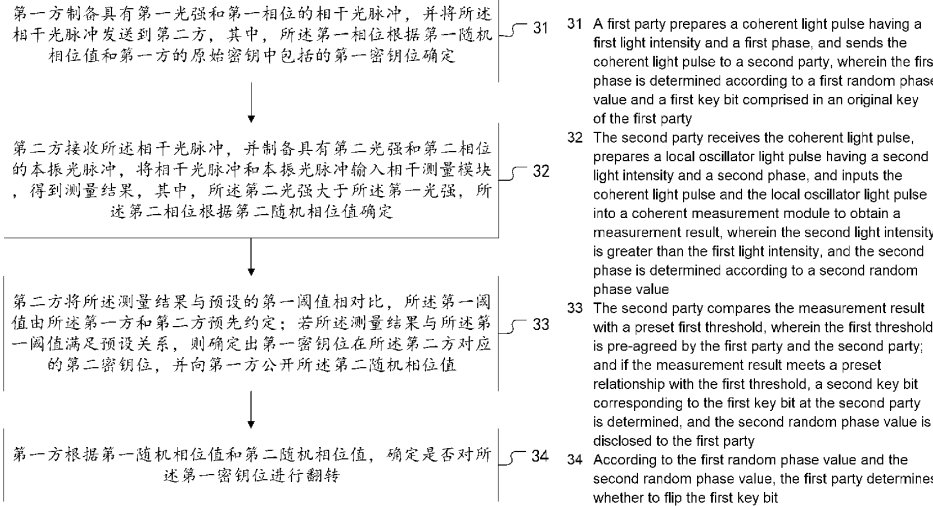


图 3

(57) Abstract: Embodiments of the present invention provide a quantum key distribution method, apparatus and system. Participants of quantum key distribution comprise a first party and a second party, and the method comprises: the first party preparing a coherent light pulse having a first light intensity and a first phase, and sending the coherent light pulse to the second party, wherein the first phase is determined according to a first random value and a first key bit; the second party preparing a local oscillator light pulse having a second light intensity and a second phase, and inputting the coherent light pulse and the local oscillator light pulse into a coherent detection module to obtain a measurement result, wherein the second phase is determined according to a second random value; the second party comparing the measurement result with a preset first threshold, wherein the first threshold is pre-agreed by the first party and the second

[见续页]

LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN,
MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA,
PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD,
SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ,
UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国(除另有指明, 要求每一种可提供的地区
保护): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ,
NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚
(AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE,
BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR,
HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO,
PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF,
CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN,
TD, TG)。

本国际公布:
— 包括国际检索报告(条约第21条(3))。

party; if the measurement result meets a preset relationship with the first threshold, determining a second key bit corresponding to the first key bit at the second party, and disclosing the second random value to the first party; and according to the first random value and the second random value, the first party determining whether to flip the first key bit.

(57) 摘要: 本发明实施例提供了一种量子密钥分发方法、装置和系统, 量子密钥分发的参与方包括第一方和第二方, 方法包括: 第一方制备具有第一光强和第一相位的相干光脉冲, 并将相干光脉冲发送到第二方, 第一相位根据第一随机值和第一密钥位确定; 第二方制备具有第二光强和第二相位的本振光脉冲, 将相干光脉冲和本振光脉冲输入相干探测模块, 得到测量结果, 第二相位根据第二随机值确定; 第二方将测量结果与预设的第一阈值相对比, 第一阈值由第一方和第二方预先约定; 若测量结果与第一阈值满足预设关系, 则确定出第一密钥位在第二方对应的第二密钥位, 并向第一方公开第二随机值; 第一方根据第一随机值和第二随机值, 确定是否对第一密钥位进行翻转。