(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

(43) 国际公布日
2017 年 6 月 15 日 (15.06.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/096599 A1

(51) 国际专利分类号:
H04L 9/12 (2006.01)

(21) 国际申请号: PCT/CN2015/097060

(22) 国际申请日: 2015 年 12 月 10 日 (10.12.2015)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: **深圳市大疆创新科技有限公司 (SZ DJI TECHNOLOGY CO., LTD.)** [CN/CN]; 中国广东省深圳市南山区高新区南区粤兴一道 9 号香港科大深圳产学研大楼 6 楼, Guangdong 518057 (CN)。

(72) 发明人: **陈永森 (CHEN, Yongsen)**; 中国广东省深圳市南山区高新区南区粤兴一道 9 号香港科大深圳产学研大楼 6 楼, Guangdong 518057 (CN)。 **谢鹏 (XIE, Peng)**; 中国广东省深圳市南山区高新区南区粤兴一道 9 号香港科大深圳产学研大楼 6 楼, Guangdong 518057 (CN)。 **万日栋 (WAN, Ridong)**; 中国广东省深圳市南山区高新区南区粤兴一道 9 号香港科大深圳产学研大楼 6 楼, Guangdong 518057 (CN)。 **吴军 (WU, Jun)**; 中国广东省深圳市南山区高新区南区粤兴一道 9 号香港科大深圳产学研大楼 6 楼, Guangdong 518057 (CN)。 **龚明 (GONG, Ming)**; 中国广东省深圳市南山区高新区南区粤兴一道 9 号香港科大深圳产学研大楼 6 楼, Guangdong 518057 (CN)。 **尤中乾 (YOU, Zhongqian)**; 中国广东省深圳市南山区高新区南区粤兴一道 9 号香港科大深圳产学研大楼 6 楼, Guangdong 518057 (CN)。

(74) 代理人: **深圳市赛恩倍吉知识产权代理有限公司 (SHENZHEN SCIENBIZIP INTELLECTUAL PROPERTY AGENCY CO., LTD.)**; 中国广东省深圳市龙华新区龙观东路 83 号荣群大厦 9 楼, Guangdong 518109 (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, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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, GH, GM, KE, LR, LS, MW, MZ, NA,

[见续页]

(54) **Title**: SECURE COMMUNICATION SYSTEM, METHOD, AND DEVICE

(54) **发明名称** : 安全通信系统、方法及装置

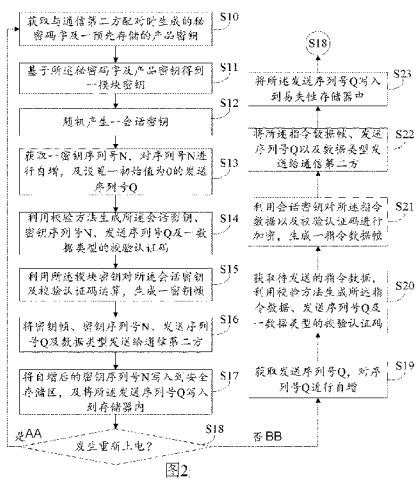

图2

S10OBTAIN A SECRET CODEWORD GENERATED WHEN PAIRING WITH A SECOND COMMUNICATION PARTY AND A PRE-STORED PRODUCT KEY
S11OBTAIN A MODULE KEY ON THE BASIS OF THE SECRET CODEWORD AND THE PRODUCT KEY
S12RANDOMLY GENERATE A SESSION KEY
S13OBTAIN A KEY SERIAL NUMBER N, PERFORM AUTO-INCREMENT ON THE SERIAL NUMBER N, AND SET A TRANSMISSION SERIAL NUMBER Q HAVING AN INITIAL VALUE OF 0
S14GENERATE A CHECK AUTHENTICATION CODE OF THE SESSION KEY, THE KEY SERIAL NUMBER N, THE TRANSMISSION SERIAL NUMBER Q, AND A DATA TYPE BY USING A CHECK METHOD
S15OPERATE ON THE SESSION KEY AND THE CHECK AUTHENTICATION CODE BY USING THE MODULE KEY TO GENERATE A KEY FRAME
S16SEND THE KEY FRAME, THE KEY SERIAL NUMBER N, THE TRANSMISSION SERIAL NUMBER Q, AND THE DATA TYPE TO THE SECOND COMMUNICATION PARTY
S17WRITE THE KEY SERIAL NUMBER N ON WHICH AUTO-INCREMENT HAS BEEN PERFORMED INTO A SECURE STORAGE AREA, AND WRITE THE TRANSMISSION SERIAL NUMBER Q INTO A MEMORY
S18RE-ELECTRIFIED?
S19OBTAIN THE TRANSMISSION SERIAL NUMBER Q AND PERFORM AUTO-INCREMENT ON THE SERIAL NUMBER Q
S20OBTAIN INSTRUCTION DATA TO BE SENT, AND GENERATE A CHECK AUTHENTICATION CODE OF THE INSTRUCTION DATA, THE TRANSMISSION SERIAL NUMBER Q, AND A DATA TYPE BY USING THE CHECK METHOD
S21ENCRYPT THE INSTRUCTION DATA AND THE CHECK AUTHENTICATION CODE BY USING THE SESSION KEY TO GENERATE AN INSTRUCTION DATA FRAME
S22SEND THE INSTRUCTION DATA FRAME, THE TRANSMISSION SERIAL NUMBER Q, AND THE DATA TYPE TO THE SECOND COMMUNICATION PARTY
S23WRITE THE TRANSMISSION SERIAL NUMBER Q INTO A VOLATILE MEMORY
AA YES
BB NO

(57) **Abstract**: A secure communication method, comprising: a first communication party sends a multilevel-encrypted key data packet to a second communication party to execute security authentication between the first communication party and the second communication party; and the first communication party sends a multilevel-encrypted instruction data packet to the second communication party to send instruction data to the second communication party. The present invention also provides a secure communication system and device. The present invention is able to prevent replay attacks in a communication system.

(57) **摘要**: 一种安全通信方法，在该方法中，通讯第一方向通信第二方发送多级加密的密钥数据包，以执行通信第一方与通信第二方之间的安全认证，以及通讯第一方向通信第二方发送多级加密的指令数据包，以向所述通信第二方发送指令数据。本发明还提供一种安全通信系统及装置。本发明能够防止通信系统中的重放攻击。

WO 2017/096599 A1

RW, 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, 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))。

安全通信系统、方法及装置

技术领域

[1] 本发明涉及一种无线通信系统中安全认证以及安全通信技术，尤其是防止重放攻击的安全通信系统及方法。

背景技术

[2] 在安全通信中，往往有以下的基本要求：

[3] 1、保密：必须保证通信的数据只有通信双方可以解读；

[4] 2、认证：必须保证通信的数据是授信方发送出来的；

[5] 3、防止重放攻击：防止攻击者录制以前发送的数据，从而欺骗接收者。攻击者可能使用系统上次运行或者本次运行的数据来欺骗接收者，所以在系统设计时，必须防止这两种攻击。

[6] 无线通信系统很容易遭受中间人攻击，比如对无线系统进行指令注入，达到控制和劫持接收方的目的；修改无线系统的数据，从而欺骗接收方；通过重放攻击，劫持接收方，从而（1）俘获受攻击的对象，从而造成系统所有者的财产损失；（2）操作受劫持的对象完成一些恶意攻击，给他人的生命财产造成损失。

[7] 目前的无线通信系统，有些因为没有对通信双方进行有效认证，并进行数据保护，容易遭受攻击。而就算加入加密和认证，也因为没有有效防止重放攻击，而使系统被劫持。

[8] 在单向通信系统中，上述的问题尤为突出。而在双向通信系统中，上述的问题也存在。

对发明的公开

发明内容

[9] 鉴于以上内容，有必要提出一种安全通信系统、方法及装置，能够防止通信系统中的重放攻击。

[10] 一种安全通信方法，由一通信第一方所执行，该方法包括：

[11] 获取通信第一方与一通信第二方配对时生成的秘密码字，并获取预先存储的产

品密钥；

[12] 基于所述秘密码字及产品密钥得到一模块密钥；

[13] 随机产生一会话密钥；

[14] 获取一密钥序列号N，并对序列号N进行自增，及设置一初始值为0的发送序列号Q；

[15] 利用所述模块密钥对所述会话密钥及所述会话密钥的校验认证码进行运算，生成一密钥帧；

[16] 将所述密钥帧、密钥序列号N、发送序列号Q及一数据类型的数据包发送给通信第二方，其中，所述数据类型指示所述数据包为密钥数据包；

[17] 获取发送序列号Q，并对序列号Q进行自增；

[18] 获取待发送的指令数据，利用所述会话密钥对所述指令数据以及所述指令数据的校验认证码进行加密，生成一指令数据帧；及

[19] 将所述指令数据帧、发送序列号Q以及一数据类型的数据包发送给通信第二方，其中，所述数据类型指示所述数据包为指令数据包。

[20] 优选地，所述通信第一方为控制方及通信第二方为受控方。

[21] 优选地，所述通信第一方为飞行遥控器及所述通信第二方为无人飞行器或者无人飞行器上的一个或者多个模块。

[22] 优选地，所述无人飞行器上的一个或者多个模块包括相机、云台。

[23] 优选地，该方法还包括：重复执行上述获取发送序列号Q的步骤到将所述指令数据帧、发送序列号Q以及一数据类型的数据包发送给通信第二方的步骤直到所述通讯第一方上电重启。

[24] 优选地，所述产品密钥是通讯第一方在生产时，烧录在其安全存储区的。

[25] 优选地，所述模块密钥是对所述秘密码字及产品密钥执行派生算法得到的，所述派生算法包括加密、消息认证码。

[26] 优选地，所述会话密钥是使用随机数发生器动态产生的。

[27] 优选地，对序列号N的自增方法包括每向通信第二方发送一次数据，则N值增加1。

[28] 优选地，所述序列号Q的自增方法包括每向通信第二方发送一次数据，则Q值

增加1，或者每隔预设的时间段Q值增加1。

[29] 优选地，利用所述模块密钥对所述会话密钥及所述会话密钥的校验认证码进行运算的方法包括加密运算及/或消息认证码。

[30] 优选地，所述模块密钥、发送序列号Q以及会话密钥存储于通信第一方的易失性存储器中。

[31] 优选地，所述秘密码字以及密钥序列号N存储于所述通信第一方的非易失性存储器中。

[32] 一种安全通信方法，由一通信第一方所执行，该方法包括：

[33] 获取通信第一方与一通信第二方配对时生成的秘密码字，并获取一预先存储的产品密钥；

[34] 基于所述秘密码字及产品密钥得到一模块密钥；

[35] 随机产生一会话密钥；

[36] 获取一密钥序列号N，对序列号N进行自增，及设置一初始值为0的发送序列号Q；

[37] 利用所述模块密钥对所述会话密钥及所述会话密钥的校验认证码进行运算，生成一密钥帧；

[38] 将所述密钥帧、密钥序列号N、发送序列号Q及一数据类型的数据包发送给通信第二方，其中，所述数据类型指示所述数据包为密钥数据包；及

[39] 每隔预设的时间段执行将所述密钥帧、密钥序列号N、发送序列号Q及一数据类型的数据包发送给通信第二方。

[40] 优选地，所述通信第一方为飞行遥控器及所述通信第二方为无人飞行器或者无人飞行器上的一个或者多个模块。

[41] 优选地，所述产品密钥是通讯第一方在生产时，烧录在其安全存储区的。

[42] 优选地，所述秘密码字及所述密钥序列号N存储于所述通信第一方的非易失性存储器中。

[43] 优选地，所述模块密钥、会话密钥及发送序列号Q存储于所述通信第一方的易失性存储器中。

[44] 优选地，所述钥序列号N在每次生成会话密钥时，该N的值进行自增。

[45] 一种安全通信方法，由一通信第一方所执行，该方法包括：

[46] 获取一发送序列号Q，并序列号Q进行自增；

[47] 获取待发送的指令数据，利用一随机生成的会话密钥对所述指令数据以及所述指令数据的校验认证码进行加密，生成一指令数据帧；及

[48] 将所述指令数据帧、发送序列号Q以及一数据类型的数据包发送给通信第二方，其中，所述数据类型指示所述数据包为指令数据包。

[49] 优选地，所述通信第一方为飞行遥控器及所述通信第二方为无人飞行器或者无人飞行器上的一个或者多个模块。

[50] 优选地，所述发送序列号Q的初始值为0，并在所述会话密钥发生变更时，重新归0，在所述会话密钥没有发生变更时，单调增长。

[51] 优选地，所述会话密钥及发送序列号Q存储于所述通信第一方的易失性存储器中。

[52] 一种安全通信方法，由一通信第二方所执行，该方法包括：

[53] 接收配对的通信第一方传送的密钥数据包；

[54] 读取一密钥序列号n；

[55] 获取密钥数据包中的密钥序列号N，在N<=n时，丢弃所述密钥数据包；

[56] 在N>n时，获取与通信第二方与一通信第一方配对时生成的秘密码字，并获取一产品密钥；

[57] 基于所述秘密码字及产品密钥得到一模块密钥；

[58] 利用所述模块密钥解密所述密钥数据包，得到一会话密钥及校验认证码；

[59] 当利用所述校验认证码验证所述会话密钥不正确时，丢弃所述密钥数据包；

[60] 当所述会话密钥正确时，存储所述会话密钥；

[61] 接收通信第一方传送的指令数据包；

[62] 从获取一发送序列号q；

[63] 获取所述指令数据包中的发送序列号Q，当Q<=q时，丢弃所述指令数据包；

[64] 当Q>q时，获取所述会话密钥；

[65] 利用所述会话密钥解密指令数据包，得到指令数据及校验认证码；

[66] 当利用所述校验认证码验证所述指令数据不正确时，丢弃所述指令数据包；及

[67] 当所述指令数据正确时，执行所述指令。

[68] 优选地，所述通信第一方为控制方及通信第二方为受控方。

[69] 优选地，所述通信第一方飞行遥控器及所述通信第二方为无人飞行器或者无人飞行器上的一个或者多个模块。

[70] 优选地，所述无人飞行器上的一个或者多个模块包括相机、云台。

[71] 优选地，所述产品密钥存储在通讯第二方的安全存储区。

[72] 优选地，所述模块密钥是对所述秘密码字及产品密钥执行派生算法得到的，所述派生算法包括加密、消息认证码。

[73] 优选地，该方法还包括：

[74] 将所述模块密钥以及所接收的发送序列号Q以及会话密钥存储于通信第二方的易失性存储器中，并记发送序列号q=Q。

[75] 优选地，该方法还包括：

[76] 将所述密钥序列号N存储于所述通信第二方的非易失性存储器中，并记密钥序列号n=N。

[77] 一种安全通信方法，由一通信第二方所执行，该方法包括：

[78] 接收配对的通信第一方传送的密钥数据包；

[79] 获取一预先存储的密钥序列号n；

[80] 获取密钥数据包中的密钥序列号N，在N<=n时，丢弃所述密钥数据包；

[81] 在N>n时，获取与通信第二方与一通信第一方配对时生成的秘密码字，及从获取一预先存储的产品密钥；

[82] 基于所述秘密码字及产品密钥得到一模块密钥；

[83] 利用所述模块密钥解密所述密钥数据包，得到一会话密钥及校验认证码；

[84] 当利用所述校验认证码验证所述会话密钥不正确时，丢弃所述密钥数据包；及

[85] 当所述会话密钥正确时，存储所述会话密钥。

[86] 优选地，所述通信第一方飞行遥控器及所述通信第二方为无人飞行器或者无人飞行器上的一个或者多个模块。

[87] 优选地，所述产品密钥是存储在通讯第二方的安全存储区。

[88] 优选地，所述秘密码字及所述密钥序列号n存储于所述通信第二方的非易失性

存储器中。

[89] 一种安全通信方法，由一通信第二方所执行，该方法包括：

[90] 接收配对的通信第一方传送的指令数据包；

[91] 获取一发送序列号q；

[92] 获取所述指令数据包中的发送序列号Q，当Q<=q时，丢弃所述指令数据包；

[93] 当Q>q时，获取一会话密钥；

[94] 利用所述会话密钥解密指令数据包，得到指令数据及校验认证码；

[95] 当利用所述校验认证码验证所述指令数据不正确时，丢弃所述指令数据包；及

[96] 当所述指令数据正确时，执行所述指令。

[97] 优选地，所述通信第一方飞行遥控器及所述通信第二方为无人飞行器或者无人飞行器上的一个或者多个模块。

[98] 优选地，所述会话密钥及发送序列号q存储于所述通信第二方的易失性存储器中。

[99] 一种安全通信方法，由一通信第二方所执行，该方法包括：

[100] 获取一会话密钥；

[101] 获取一发送序列号M，并对发送序列号M进行自增；

[102] 获取待发送的反馈数据，利用所述会话密钥对所述反馈数据以及反馈数据的校验认证码进行加密，生成一反馈数据帧；及

[103] 将所述反馈数据帧、发送序列号M发送给配对的通信第一方。

[104] 优选地，所述通讯第一方为主控方，所述通信第二方为受控方。

[105] 优选地，所述通信第一方飞行遥控器及所述通信第二方为无人飞行器或者无人飞行器上的一个或者多个模块。

[106] 优选地，所述无人飞行器上的一个或者多个模块包括相机、云台。

[107] 优选地，所述会话密钥通过下述方法得到：

[108] 接收所述通信第一方传送的密钥数据包；

[109] 获取一预先存储的密钥序列号n；

[110] 获取密钥数据包中的密钥序列号N，在N<=n时，丢弃所述密钥数据包；

[111] 在N>n时，获取与通信第二方与一通信第一方配对时生成的秘密码字，及从获

取一预先存储的产品密钥；

[112] 基于所述秘密码字及产品密钥得到一模块密钥；

[113] 利用所述模块密钥解密所述密钥数据包，得到一会话密钥及校验认证码；

[114] 当利用所述校验认证码验证所述会话密钥不正确时，丢弃所述密钥数据包；及

[115] 当所述会话密钥正确时，存储所述会话密钥。

[116] 优选地，所述产品密钥是存储在通讯第二方的安全存储区。

[117] 优选地，所述秘密码字及所述密钥序列号n存储于所述通信第二方的非易失性存储器中。

[118] 一种安全通信方法，该方法包括：

[119] 通信第一方利用一模块密钥对一随机产生的会话密钥进行加密，并传送给通信第二方；

[120] 所述通信第二方利用所述模块密钥对所述会话密钥进行解密，得到所述会话密钥。

[121] 优选地，所述模块密钥通过下述方法得到：

[122] 获取通信第一方与一通信第二方配对时生成的秘密码字，并获取一预先存储的产品密钥；及

[123] 基于所述秘密码字及产品密钥，通过派生算法得到所述模块密钥。

[124] 优选地，所述通信第一方为控制方及通信第二方为受控方。

[125] 优选地，所述通信第一方飞行遥控器及所述通信第二方为无人飞行器或者无人飞行器上的一个或者多个模块。

[126] 优选地，所述无人飞行器上的一个或者多个模块包括相机、云台。

[127] 优选地，所述通信第一方及通信第二方均既是信息发送方又是信息接收方。

[128] 优选地，所述通信第一方及通信第二方是两个无人飞行器、或者是无人飞行器的两个模块。

[129] 一种通信装置，该装置包括：

[130] 认证发送模块，用于获取所述通信装置与另一通信装置配对时生成的秘密码字，并获取预先存储的产品密钥；基于所述秘密码字及产品密钥得到一模块密钥；随机产生一会话密钥；获取一密钥序列号N，并对序列号N进行自增，及设置

一初始值为0的发送序列号Q；利用所述模块密钥对所述会话密钥及所述会话密钥的校验认证码进行运算，生成一密钥帧；将所述密钥帧、密钥序列号N、发送序列号Q及一数据类型的数据包发送给通信第二方，其中，所述数据类型指示所述数据包为密钥数据包；及

[131] 指令发送模块，用于获取所述发送序列号Q，并对序列号Q进行自增；获取待发送的指令数据，利用所述会话密钥对所述指令数据以及所述指令数据的校验认证码进行加密，生成一指令数据帧；及将所述指令数据帧、发送序列号Q以及一数据类型的数据包发送给通信第二方，其中，所述数据类型指示所述数据包为指令数据包。

[132] 优选地，所述通信装置为飞行遥控器。

[133] 优选地，所述通信装置包括一个或者多个非易失性存储器，用于存储所述产品密钥、秘密码字以及密钥序列号N。

[134] 优选地，所述通信装置包括一个或者多个易失性存储器，用于存储所述模块密钥、会话密钥以及发送序列号Q。

[135] 优选地，所述模块密钥是对所述秘密码字及产品密钥执行派生算法得到的，所述派生算法包括加密、消息认证码。

[136] 优选地，所述会话密钥是使用随机数发生器动态产生的。

[137] 优选地，对序列号N的自增方法包括每向通信第二方发送一次数据，则N值增加1。

[138] 优选地，所述序列号Q的自增方法包括每向通信第二方发送一次数据，则Q值增加1，或者每隔预设的时间段Q值增加1。

[139] 优选地，利用所述模块密钥对所述会话密钥及所述会话密钥的校验认证码进行运算的方法包括加密运算及/或消息认证码。

[140] 一种通信装置，该通信装置包括：

[141] 认证接收模块，用于接收配对的另一个通信装置传送的密钥数据包；读取一密钥序列号n；获取密钥数据包中的密钥序列号N，在N<=n时，丢弃所述密钥数据包；在N>n时，获取与通信第二方与一通信第一方配对时生成的秘密码字，并获取一产品密钥；基于所述秘密码字及产品密钥得到一模块密钥；利用所述模块

密钥解密所述密钥数据包，得到一会话密钥及校验认证码；当利用所述校验认证码验证所述会话密钥不正确时，丢弃所述密钥数据包；当所述会话密钥正确时，存储所述会话密钥；及

[142] 指令执行模块，用于接收另一通信装置传送的指令数据包；从获取一发送序列号q；获取所述指令数据包中的发送序列号Q，当Q<=q时，丢弃所述指令数据包；当Q>q时，获取所述会话密钥；利用所述会话密钥解密指令数据包，得到指令数据及校验认证码；当利用所述校验认证码验证所述指令数据不正确时，丢弃所述指令数据包；及当所述指令数据正确时，执行所述指令。

[143] 优选地，所述通信装置为无人飞行器或者无人飞行器上的一个或者多个模块。

[144] 优选地，所述无人飞行器上的一个或者多个模块包括相机、云台。

[145] 优选地，所述通信装置包括非易失性存储器，用于存储所述产品密钥、密钥码字以及密钥序列号n。

[146] 优选地，所述认证接收模块还用于将所述密钥序列号N存储于所述非易失性存储器中，并记密钥序列号n=N。

[147] 优选地，所述通信装置包括易失性存储器，用于存储所述模块密钥、会话密钥及发送序列号q。

[148] 优选地，所述指令接收模块还用于将所接收的发送序列号Q以及会话密钥存储于所述通信装置的易失性存储器中，并记发送序列号q=Q。

[149] 优选地，所述模块密钥是对所述秘密码字及产品密钥执行派生算法得到的，所述派生算法包括加密、消息认证码。

[150] 优选地，所述通信装置还包括：

[151] 反馈数据发送模块，用于获取所述会话密钥；

[152] 获取一发送序列号M，并对发送序列号M进行自增；

[153] 获取待发送的反馈数据，利用所述会话密钥对所述反馈数据以及反馈数据的校验认证码进行加密，生成一反馈数据帧；及

[154] 将所述反馈数据帧、发送序列号M发送给配对的通信第一方。

[155] 一种安全通信系统，包括通过无线网络进行通信的通信第一方及通信第二方，其中：

[156] 所述通信第一方利用一模块密钥对一随机产生的会话密钥进行加密，并传送给通信第二方；及

[157] 所述通信第二方利用所述模块密钥对所述会话密钥进行解密，得到所述会话密钥。

[158] 优选地，所述模块密钥通过下述方法得到：

[159] 获取通信第一方与一通信第二方配对时生成的秘密码字，并获取一预先存储的产品密钥；及

[160] 基于所述秘密码字及产品密钥，通过派生算法得到所述模块密钥。

[161] 优选地，所述通信第一方为控制方及通信第二方为受控方。

[162] 优选地，所述通信第一方飞行遥控器及所述通信第二方为无人飞行器或者无人飞行器上的一个或者多个模块。

[163] 优选地，所述无人飞行器上的一个或者多个模块包括相机、云台或遥控器中的一个或多个。

[164] 优选地，所述通信第一方及通信第二方均既是信息发送方又是信息接收方。

[165] 优选地，所述通信第一方及通信第二方是两个无人飞行器、或者是无人飞行器的两个模块。

[166] 相较于现有技术，利用本发明提供的安全通信系统及方法能够实现通信发送方与接收方的安全认证、加密通信以及防止重放攻击。

附图说明

[167] 图1是本发明安全通信系统较佳实施例的硬件架构示意图。

[168] 图2是本发明安全通信方法较佳实施例中单向通信系统的发送方的数据处理方法流程图。

[169] 图3是本发明安全通信方法较佳实施例中单向通信系统的接收方的数据处理方法流程图。

[170] 图4是本发明安全通信方法较佳实施例中单向通信系统的数据流的传输处理示意图。

[171] 图5是本发明安全通信方法较佳实施例中非对称双向通信系统的受控方向主控方传送反馈数据的方法流程图。

[172] 图6是本发明安全通信方法较佳实施例中非对称双向通信系统的主控方接收受控方反馈数据的方法流程图。

主要元件符号说明

[173] 通信第一方 1

[174] 安全存储区 10

[175] 产品密钥 100

[176] 秘密码字 101

[177] 密钥序列号 102

[178] 易失性存储器 11

[179] 模块密钥 110

[180] 会话密钥 111

[181] 发送序列号 112

[182] 认证发送模块 12

[183] 指令发送模块 13

[184] 反馈数据接收模块 14

[185] 通信第二方 2

[186] 安全存储区 20

[187] 产品密钥 200

[188] 秘密码字 201

[189] 密钥序列号 202

[190] 易失性存储器 21

[191] 模块密钥 210

[192] 会话密钥 211

[193] 发送序列 212

[194] 认证接收模块 22

[195] 指令执行模块 23

[196] 反馈数据发送模块 24

[197] 如下具体实施方式将结合上述附图进一步说明本发明。

具体实施方式

[198] 参阅图1所示，是本发明安全通信系统较佳实施例的硬件架构示意图。

[199] 本实施例中，所述安全通信系统1000包括通过无线网络进行通信的通信装置，如通信第一方1及通信第二方2。所述通信第一方1及通信第二方2可以分别是单向通信系统的信息发送方及信息接收方，或者是非对称双向通信系统中的主控方及受控方。例如，所述通信第一方1可以是飞行控制器，如遥控器等，以及所述通信第二方2可以是无人飞行器或者无人飞行器上的相机模块、云台等。

[200] 在其他实施例中，所述通信第一方1及通信第二方2也可以既是信息发送方又是信息接收方。例如，所述通信第一方1及通信第二方2可以是两个无人飞行器、或者无人飞行器的两个相机模块等。

[201] 所述通信第一方1包括一个或者多个安全存储区10以及一个或者多个易失性存储器11。所述安全存储区10可以是通信第一方1的只读存储器（Read-Only Memory，简称：ROM）或者其他类型的非易失性存储器，如可编程只读存储器（erasable programmable read only memory，简称：EPROM）、闪存（Flash Memory）软盘、硬盘、磁盘、光盘、SM卡、CF卡、XD卡、SD卡、MMC卡、SONY记忆棒、eMMC、NAND等。所述易失性存储器11可以是随机存取存储器（Random-Access Memory，简称RAM），包括为静态RAM（SRAM）和动态内存（DRAM）等。

[202] 本实施例中，所述通信第一方1在生产时，会分配一个产品密钥（ProductKey），并将其烧录或固化在所述通信第一方1的安全存储区10，如ROM中。

[203] 相似地，所述通信第二方2也包括一个或者多个安全存储区20以及一个或者多个易失性存储器21。对应的，通信第二方2的安全存储区20中也存储有产品密钥200。所述产品密钥200与所述产品密钥100相同。

[204] 进一步地，所述通信第一方1还包括认证发送模块12以及指令发送模块13。

[205] 所述认证发送模块12用于向通信第二方2发送多级加密的密钥数据包，以执行通信第一方1与通信第二方2之间的安全认证。所述指令发送模块13用于向通信第二方2发送多级加密的指令数据包，以向所述通信第二方2发送指令数据。

[206] 本发明所述认证发送模块12及指令发送模块13可以防止通信过程中的重放攻击

，详细地请参阅下述图2中的描述。

[207] 进一步地，所述通信第二方2还包括认证接收模块22以及指令执行模块23。

[208] 所述认证接收模块22用于接收通信第一方1发送的密钥数据包，执行对通信第一方1的认证。所述指令执行模块23用于接收通信第一方1发送的指令数据包，以执行通信第一方1下达的指令。

[209] 参阅图2所示，是本发明安全通信方法较佳实施例中单向通信系统的发送方的数据处理方法流程图。本实施例中，所述发送方为通信第一方1。根据不同的需求，图2所示数据处理方法中，步骤的执行顺序可以改变，某些步骤可以省略，而并不限于图2所示的步骤及顺序。

[210] 步骤S10，在通信第一方1开机或者上电重启时，通信第一方1的认证发送模块12获取通信第一方1在与通信第二方2配对时生成并写入到安全存储区10的秘密码字（SecretCode）101，并从所述安全存储区10获取预先存储的产品密钥100。本实施例中，所述通信第一方1与通信第二方2的配对一般在安全环境下进行，从而保证该秘密码字101的安全性。所述配对过程可为无人机和遥控器的对频过程。

[211] 步骤S11，所述认证发送模块12基于所述秘密码字101及产品密钥100得到一模块密钥（ModuleKey）110。本实施例中，所述认证发送模块12对所述秘密码字101及产品密钥100执行派生算法，产生所述模块密钥110。所述派生算法可以是加密、哈希、消息认证码 (Message Authentication Code，MAC)或者任意之结合。本实施例中，所述模块密钥110只在上电时生成一次，因此，为了提高安全性，所述认证发送模块12将该模块密钥110存储于易失性存储器11中。

[212] 步骤S12，所述认证发送模块12随机产生一个或者多个会话密钥（SessionKey）111。所述会话密钥111可以使用随机数发生器或者其他生成随机数的方法动态产生。所述会话密钥111也只在上电时生成一次，因此，所述认证发送模块12将该会话密钥111存储于易失性存储器11中。

[213] 步骤S13，所述认证发送模块12从安全存储区10获取一密钥序列号（Key Number）N 102，对所述序列号N进行自增，并设置一初始值为0的发送序列号（Sequence Number）Q 112。本实施例中，所述密钥序列号N 102的初始值可以

设为0或者其他值，并在每次生成会话密钥111时，该N的值进行自增，如增加1，因此，所述认证发送模块12将所述密钥序列号N 102存储于安全存储区10，以在掉电时可以找回。所述发送序列号Q 112在会话密钥111发生变更时，重新归零，在会话密钥111没有发生变更时，单调增长，因此，所述认证发送模块12可以将所述发送序列号Q 112存储于易失性存储器11中。发送序列号Q 112增长的方法可以是每次向通信第二方2发送一条信息时，Q的值增加1，或者每隔一小段时间，如50ms、1s后，Q的值增加1。可以理解，所述密钥序列号N102也可能存储于易失性存储器中，则所述认证发送模块12从所述易失性存储器中获取所述密钥序列号N102。

[214] 步骤S14，所述认证发送模块12利用校验方法生成所述会话密钥111、密钥序列号N 102、发送序列号Q 112及一数据类型的校验认证码。所述校验方法可以是数据摘要算法，如各种哈希值，包括MD5、SHA等，或者校验码，如CRC等，以及消息认证码等。所述数据类型可以是代表认证数据类型的字符。

[215] 步骤S15，所述认证发送模块12利用所述模块密钥110对所述会话密钥111及其校验认证码进行运算，生成一密钥帧。所述运算可以是（1）计算原始消息的校验码（或者摘要），然后使用模块秘钥对会话密钥以及校验码（或者摘要）进行加密；（2）计算原始消息的MAC，然后使用模块秘钥对会话密钥进行加密。

[216] 步骤S16，所述认证发送模块12将所述密钥帧、密钥序列号N 102、发送序列号Q 112及所述数据类型发送给通信第二方2。

[217] 对于单向通信系统，所述认证发送模块12每隔一段时间，如1s，将所述密钥帧、密钥序列号N 102、发送序列号Q 112及所述数据类型发送给通信第二方2一次，以确通信第二方2可以收到所述密钥帧。

[218] 步骤S17，所述认证发送模块12将自增后的密钥序列号N 102写入到安全存储区10，及将所述发送序列号Q 112写入到存储器11内。可以理解，所述发送序列号Q112可被写入易失性存储区，存于易失性存储器中时，可保证及时擦除，保证了信息的安全性；若存储到安全存储区，则需保证通过加密等手段保证信息的足够安全性。

[219] 步骤S18，所述认证发送模块12判断通信第一方1是否发生重新上电。若发生了

重新上电，则重复执行上述的步骤S10至S17。若通信第一方1没有发生重新上电，则执行下述的步骤S19。

[220] 步骤S19，通信第一方1的指令发送模块13从易失性存储器11内获取发送序列号Q 112，并对序列号Q 112进行自增。如上所述，序列号Q增长的方法可以是每次向通信第二方2发送一条信息时，Q的值增加1，或者每隔一小段时间，如50ms、1s后，Q的值增加1。

[221] 步骤S20，所述指令发送模块13获取待发送的指令数据，利用校验方法生成所述指令数据、发送序列号Q 112及一数据类型的校验认证码。所述指令数据可以是，例如控制无人飞行器的相机的旋转方向及旋转角度等。所述校验方法可以是数据摘要算法，如各种哈希值，包括MD5、SHA等，或者校验码，如CRC等，以及消息认证码等。所述数据类型可以是代表指令数据类型的字符。

[222] 步骤S21，所述指令发送模块13利用存储于易失性存储器11中的会话密钥111对所述指令数据以及其校验认证码进行运算，生成一指令数据帧。所述运算可以是加密算法或者消息认证码等。

[223] 步骤S22，所述指令发送模块13将所述指令数据帧、发送序列号Q 112以及所述数据类型发送给通信第二方2。

[224] 步骤S23，所述指令发送模块13将所述发送序列号Q 112写入到易失性存储器11中。

[225] 可以理解，所述产品密钥110、会话密钥111、密钥序列号N102及发送序列号Q 112也可均存储于遥控器或无人机的安全存储区域内。

[226] 可以理解，上述执行操作的模块可合并或拆分，可实现密钥交换和通信功能即可。

[227] 参阅图3所示，是本发明安全通信方法较佳实施例中单向通信系统的接收方。本实施例中，所述接收方为通信第二方2。根据不同的需求，图3所示数据处理方法中，步骤的执行顺序可以改变，某些步骤可以省略，而并不限于图3所示的步骤及顺序。

[228] 步骤S30，所述通信第二方2接收通信第一方1传送的数据包。

[229] 步骤S31，所述通信第二方2判断所述数据包是否为密钥数据包。本实施例中，

所述认证接收模块22根据所述数据包中包括的数据类型判断所述数据包是否为密钥数据包。若所述数据包是密钥数据包，则流程执行下述的步骤S32-S40。否则，若所述数据包不是密钥数据包，且根据所述数据包中包括的数据类型判断所述数据包为指令数据包时，执行下述的步骤S41-S46。

[230] 步骤S32，所述通信第二方2的认证接收模块22从所述通信第二方2的安全存储区20获取一密钥序列号n 202。

[231] 步骤S33，所述认证接收模块22获取所接收的数据包中的密钥序列号N 102，并判断是否N<=n。当N<=n时，说明该数据包可能是通信第一方1重复发送的，或者是攻击者通过重放攻击发送的数据包，则执行步骤S34，认证接收模块22丢弃该数据包。否则，若N>n，则执行下述的步骤S35。

[232] 具体地，因为所述密钥序列号N102在每次生成会话密钥111时一并产生，在同一会话中，此密钥序列号N102可保持不变，故若N<=n时，则说明可能是攻击者使用了上次会话的时运行的数据进行重放攻击。从而，通过比对密钥序列号N102和密钥序列号n202，可防止攻击者使用上次会话的数据进行重放攻击。

[233] 步骤S35，所述认证接收模块22获取所述通信第二方2与通信第一方1配对时生成并写入到安全存储区20的秘密码字201。所述秘密码字201与上述通信第一方1的秘密码字101相同。

[234] 步骤S36，所述认证接收模块22从所述安全存储区20获取一预先存储的产品密钥200。所述产品密钥200与上述通信第一方1的产品密钥100相同。

[235] 步骤S37，所述认证接收模块22基于所述秘密码字201及产品密钥200得到一模块密钥210。本实施例中，所述认证接收模块22对所述秘密码字201及产品密钥200执行如派生算法，产生模块密钥。所述派生算法可以使用加密或者消息认证码 (Message Authentication Code, MAC)。所述认证接收模块22将该模块密钥210存储于易失性存储器21中。

[236] 步骤S38，所述认证接收模块22利用所述模块密钥210解密所述数据包中的密钥帧，得到其中的会话密钥111及校验认证码。

[237] 步骤S39，所述认证接收模块22利用所述校验认证码验证所述会话密钥111是否正确。若会话密钥111不正确，则执行上述的步骤S34，丢弃该数据包。否则，

若会话密钥111正确，则执行下述的步骤S40。

[238] 步骤S40，认证接收模块22存储数据包中的会话密钥111及发送序列号Q 112于易失性存储器21内，并记发送序列号q=Q，及存储数据包中的密钥序列号N 102于安全存储区20，并记密钥序列号n=N。至此，所述通信第二方2获取了通信第一方1传送的会话密钥，完成了密钥交换过程。

[239] 可以理解，也可省去判断所述数据包类型的步骤，即步骤S31。而在上电或重启时，待生成会话密钥后即发送密钥数据包。接收方接收到该密钥数据包之后，若接收成功，则返回接收成功的信息，若不成功，则要求发送方重新发送直至接收成功。后续发送的数据包则均认为是指令数据包。

[240] 若所接收的数据包是指令数据包，则步骤S41，所述通信第二方2的指令执行模块23从易失性存储器21内获取一发送序列号q 212。

[241] 步骤S42，所述指令执行模块23获取所接收的数据包中的发送序列号Q 112，并判断是否Q<=q。当Q<=q时，说明该数据包可能是通信第一方1重复发送的，或者是攻击者通过重放攻击发送的数据包，则执行步骤S34，指令执行模块23丢弃该数据包。否则，若Q>q，则执行下述的步骤S43。

[242] 步骤S43，所述指令执行模块23从易失性存储器21内获取所存储的会话密钥211。

[243] 步骤S44，所述指令执行模块23利用所述会话密钥211解密数据包中的指令数据帧，得到指令数据及校验认证码。

[244] 步骤S45，所述指令执行模块23利用所述校验认证码验证所述指令数据是否正确。若指令数据不正确，则执行步骤S34，指令执行模块23丢弃该数据包。若指令数据正确，则执行下述的步骤S46。

[245] 步骤S46，所述指令执行模块23存储发送序列号Q 112于易失性存储器21内，记发送序列号q=Q，并执行所述指令，如控制无人飞行器的相机模组按指令中的方向或者角度旋转等。

[246] 在图3所述实施例运行时，若通信第二方2发生异常，如掉电重启后，需要通信第一方1重新进行密钥交换。实现方法可以包括使通信第一方1也重新上电或者在双向通信的情况下，通信第二方2主动要求通信第一方1重新进行密钥交换。

[247] 具体地，若通信第二方2发生如掉电或重启异常，可选择两种方案：对通信第一方1进行重启，从而使通信第一方1和通信第二方2重新进行密钥交换；若有从通信第二方2到通信第一方1的回传链路，则在通信第二方2重新启动后，给通信第一方1发送请求，要求通信第一方1重新发送会话密钥或密钥数据包。

[248] 参阅图4所示，是本发明安全通信方法较佳实施例中单向通信系统的数据流的传输处理示意图。

[249] 通信第一方1在开机或者上电重启时，根据预先存储的产品密钥100及配对时产生的秘密码字101派生出一模块密钥110，并从其安全存储区10读取一密钥序列号N 102。在执行与通信第二方2的交换密钥的过程中，通信第一方1对所获取的密钥序列号N 102自增，如每发送一次增加1，将自增后的N写入其安全存储区10，用自增后的N取代原来的N，同时，通信第一方1随机产生一会话密钥111，并设置一初始值为0的发送序列号Q 112。进一步地，通信第一方1利用所述模块密钥110对所述会话密钥111以及会话密钥的验证码进行加密或者其他运算生成一密钥帧，并生成一个包括所述密钥帧、密钥序列号N 102及发送序列号Q 112的密钥数据包，并将该密钥数据包定期发送给通信第二方2。

[250] 通信第二方2在开机或者上电重启时，也会根据预先存储的产品密钥200及配对时产生的秘密码字201派生出一模块密钥210，并从其安全存储区20读取一密钥序列号n 202。在接收到通信第一方1传送的密钥数据包时，首先判断是否N<=n。当N<=n时，丢弃该数据包，及当N>n时，解密并验证所述会话密钥，存储所述会话密钥及发送序列号Q 112于通信第二方2的易失性存储器21中，记q=Q，并存储密钥序列号N 102于通信第二方2的安全存储区20，如非亦失性存储器内，记n=N，从而完成密钥交换过程。

[251] 认证之后，若通信第一方1及通信第二方2均没有上电重启，则可以执行指令数据的发送过程。首先，通信第一方1读取一发送序列号Q 112，对序列号Q进行自增，如每发送一次增加1或者每隔预设时间增加1，并利用所述会话密钥111对待发送的指令数据以及该指令数据的验证码进行加密或者其他运算生成一个指令数据帧，并生成一个包括所述指令数据帧、所述发送序列号Q 112的指令数据包，将该指令数据包传送给通信第二方2。

[252] 通信第二方2接收到所述指令数据包后，从其易失性存储器21内，获取一发送序列q 212，并判断是否Q<=q。当Q<=q时，丢弃密钥数据包；否则，当Q>q时，解密及验证所述指令数据，存储发送序列号Q 112于易失性存储器21内，记q=Q，及执行所述指令数据。

[253] 所述密钥数据包包括数据类型、密钥序列号N、发送序列号Q、会话密钥和验证码，并使用模块密钥对会话密钥和验证码进行加密，而MAC码本身不加密。同样，所述指令数据包包括数据类型、发送序列号Q、指令数据和验证码，并通过会话密钥对指令数据和验证码进行加密。

[254] 以上所述的实施例中，所述产品密钥预先存储在通信第一方及通信第二方的安全存储区，如ROM中，防止攻击者读取到。所述通信第一方与通信第二方的配对一般在安全环境下进行，从而保证该秘密码字的安全性。因此，保证了基于所述产品密钥及秘密码字产生的模块密钥的秘密性及安全性。通信第二方在收到通信第一方发送的数据包时，当N<=n及/或Q<=q时，代表所述数据包可能是通信第一方重复发送的，或者是攻击者通过重放攻击发送的，因此将该数据包丢掉，当N>n及Q>q时，才处理该数据包，保证了防止数据传输过程中的重放攻击。

[255] 其中，所述密钥序列号是每次通信第一方上电重新产生会话密钥时自增一次，因此，为了保障安全性，所述密钥序列号存储于通信第一方及通信第二方的非易失性存储器内。所述的发送序列号在重新产生会话密钥时会清零，因此，所述发送序列号可以存储于通信第一方及通信第二方的易失性存储器内。

[256] 可以理解，所述密钥数据包也可包括数据类型、密钥序列号N、发送序列号Q、会话密钥和MAC码，此种情况中，使用模块密钥对会话密钥进行加密或MAC运算，而MAC码本身不加密。同样，所述指令数据包可包括数据类型、发送序列号Q、指令数据和MAC码，并通过会话密钥对指令数据进行加密或MAC运算。

[257] 以上实施例描述了单向通信系统中的认证及指令传输系统，即通讯第一方为信息发送方及通讯第二方为信息接收方。本领域技术人员应该了解，上述实施例同样适用于非对称双向通信系统，即通信第一方为主控方，通讯第二方为受控

方。在非对称双向通信系统系统中，从主控方到受控方的通信可靠度要求较高，而从受控方到主控方的通信可靠度要求较低。因此，非对称双向通信系统中，从主控方到受控方的通信可以参照如图2到图4的通信过程。从受控方到主控方的通信过程可以参照下述描述的图5及图6。

[258] 参阅图5所示，是本发明安全通信方法较佳实施例中非对称双向通信系统的受控方向主控方传送反馈数据的方法流程图。本实施例中，所述受控方为所述通信第二方2。根据不同的需求，图5所示数据处理方法中，步骤的执行顺序可以改变，某些步骤可以省略，而并不限于图5所示的步骤及顺序。

[259] 步骤S50，通信第二方2的反馈数据发送模块24从其易失性存储器21中获取所存储的会话密钥211。所述会话密钥211是利用如图2所示方法，从通信第一方1接收的。

[260] 步骤S51，所述反馈数据发送模块24从易失性存储器21中获取一发送序列号M，对序列号M进行自增。所述自增的方法可以是每发送一次，增加1，或者每隔预设时间，如50ms或者1s，增加1。

[261] 步骤S52，所述反馈数据发送模块24获取待发送的反馈数据，利用校验方法生成所述反馈数据、发送序列号M的校验认证码。所述校验方法包括可以是数据摘要算法，如各种哈希值，包括MD5、SHA等，或者校验码，如CRC等，以及消息认证码等。

[262] 步骤S53，所述反馈数据发送模块24利用所述会话密钥212对所述反馈数据以及所述校验认证码进行加密或者其他运算，生成一反馈数据帧。

[263] 步骤S54，所述反馈数据发送模块24将所述反馈数据帧、发送序列M发送给通信第一方1。

[264] 参阅图6所示，是本发明安全通信方法较佳实施例中非对称双向通信系统的主控方接收受控方反馈数据的方法流程图。本实施例中，所述主控方为通信第一方1。根据不同的需求，图6所示数据处理方法中，步骤的执行顺序可以改变，某些步骤可以省略，而并不限于图6所示的步骤及顺序。

[265] 步骤S60，通信第一方1的反馈数据接收模块14接收通信第二方2发送的数据包。

[266] 步骤S61，所述反馈数据接收模块14从易失性存储器11内获取一发送序列号m。

[267] 步骤S62，所述反馈数据接收模块14获取数据包中的发送序列号M，并判断是否M<=m。

[268] 若M<=m，则步骤S63，所述反馈数据接收模块14丢弃该数据包。

[269] 若M>m，则步骤S64，所述反馈数据接收模块14利用所述会话密钥111对所述反馈数据帧解密，获取其中的反馈数据及校验认证码。

[270] 步骤S65，所述反馈数据接收模块14利用所述校验认证码判断所述反馈数据是否准确。若所述反馈数据不准确，则执行上述的步骤S63，所述反馈数据接收模块14丢弃该数据包。

[271] 若所述反馈数据准确，则步骤S66，所述反馈数据接收模块14接收所述反馈数据，并将所述发送序列号M存储于易失性存储器内，并记为发送序列号m=M。

[272] 应当说明的是，以上实施例仅用以说明本发明的技术方案而非限制，尽管参照以上较佳实施例对本发明进行了详细说明，本领域的普通技术人员应当理解，可以对本发明的技术方案进行修改或等同替换，而不脱离本发明技术方案的精神和范围。

权利要求书

[权利要求 1] 一种安全通信方法，由一通信第一方所执行，其特征在于，该方法包括：

获取通信第一方与一通信第二方配对时生成的秘密码字，并获取预先存储的产品密钥；

基于所述秘密码字及产品密钥得到一模块密钥；

随机产生一会话密钥；

获取一密钥序列号N，并对序列号N进行自增，及设置一初始值为0的发送序列号Q；

利用所述模块密钥对所述会话密钥及所述会话密钥的校验认证码进行运算，生成一密钥帧；

将所述密钥帧、密钥序列号N、发送序列号Q及一数据类型的数据包发送给通信第二方，其中，所述数据类型指示所述数据包为密钥数据包；

获取发送序列号Q，并对序列号Q进行自增；

获取待发送的指令数据，利用所述会话密钥对所述指令数据以及所述指令数据的校验认证码进行加密，生成一指令数据帧；及

将所述指令数据帧、发送序列号Q以及一数据类型的数据包发送给通信第二方，其中，所述数据类型指示所述数据包为指令数据包。

[权利要求 2] 如权利要求1所述的安全通信方法，其特征在于，所述通信第一方为控制方及通信第二方为受控方。

[权利要求 3] 如权利要求2所述的安全通信方法，其特征在于，所述通信第一方为飞行遥控器及所述通信第二方为无人飞行器或者无人飞行器上的一个或者多个模块。

[权利要求 4] 如权利要求3所述的安全通信方法，其特征在于，所述无人飞行器上的一个或者多个模块包括相机、云台。

[权利要求 5] 如权利要求1所述的安全通信方法，其特征在于，该方法还包括：

重复执行：

获取发送序列号Q，并对序列号Q进行自增；

获取待发送的指令数据，利用所述会话密钥对所述指令数据以及所述指令数据的校验认证码进行加密，生成一指令数据帧；及

将所述指令数据帧、发送序列号Q以及一数据类型的数据包发送给通信第二方，其中，所述数据类型指示所述数据包为指令数据包；

直到所述通讯第一方上电重启。

[权利要求 6] 如权利要求1所述的安全通信方法，其特征在于，所述产品密钥是通讯第一方在生产时，烧录在其安全存储区的。

[权利要求 7] 如权利要求1所述的安全通信方法，其特征在于，所述模块密钥是对所述秘密码字及产品密钥执行派生算法得到的，所述派生算法包括加密、消息认证码。

[权利要求 8] 如权利要求1所述的安全通信方法，其特征在于，所述会话密钥是使用随机数发生器动态产生的。

[权利要求 9] 如权利要求1所述的安全通信方法，其特征在于，对序列号N的自增方法包括每向通信第二方发送一次数据，则N值增加1。

[权利要求 10] 如权利要求1所述的安全通信方法，其特征在于，所述序列号Q的自增方法包括每向通信第二方发送一次数据，则Q值增加1，或者每隔预设的时间段Q值增加1。

[权利要求 11] 如权利要求1所述的安全通信方法，其特征在于，利用所述模块密钥对所述会话密钥及所述会话密钥的校验认证码进行运算的方法包括加密运算及/或消息认证码。

[权利要求 12] 如权利要求1至11中任意一项所述的安全通信方法，其特征在于，所述模块密钥、发送序列号Q以及会话密钥存储于通信第一方的易失性存储器中。

[权利要求 13] 如权利要求1至11中任意一项所述的安全通信方法，其特征在于，所述秘密码字以及密钥序列号N存储于所述通信第一方的非易失性

存储器中。

[权利要求 14] 一种安全通信方法，由一通信第一方所执行，其特征在于，该方法包括：

获取通信第一方与一通信第二方配对时生成的秘密码字，并获取一预先存储的产品密钥；

基于所述秘密码字及产品密钥得到一模块密钥；

随机产生一会话密钥；

获取一密钥序列号N，对序列号N进行自增，及设置一初始值为0的发送序列号Q；

利用所述模块密钥对所述会话密钥及所述会话密钥的校验认证码进行运算，生成一密钥帧；

将所述密钥帧、密钥序列号N、发送序列号Q及一数据类型的数据包发送给通信第二方，其中，所述数据类型指示所述数据包为密钥数据包；及

每隔预设的时间段执行将所述密钥帧、密钥序列号N、发送序列号Q及一数据类型的数据包发送给通信第二方。

[权利要求 15] 如权利要求14所述的安全通信方法，其特征在于，所述通信第一方为飞行遥控器及所述通信第二方为无人飞行器或者无人飞行器上的一个或者多个模块。

[权利要求 16] 如权利要求15所述的安全通信方法，其特征在于，所述产品密钥是通讯第一方在生产时，烧录在其安全存储区的。

[权利要求 17] 如权利要求14或16所述的安全通信方法，其特征在于，所述秘密码字及所述密钥序列号N存储于所述通信第一方的非易失性存储器中。

[权利要求 18] 如权利要求14或16所述的安全通信方法，其特征在于，所述模块密钥、会话密钥及发送序列号Q存储于所述通信第一方的易失性存储器中。

[权利要求 19] 如权利要求14所述的安全通信方法，其特征在于，所述钥序列号N

在每次生成会话密钥时，该N的值进行自增。

[权利要求 20] 一种安全通信方法，由一通信第一方所执行，其特征在于，该方法包括：

获取一发送序列号Q，并序列号Q进行自增；

获取待发送的指令数据，利用一随机生成的会话密钥对所述指令数据以及所述指令数据的校验认证码进行加密，生成一指令数据帧；及

将所述指令数据帧、发送序列号Q以及一数据类型的数据包发送给通信第二方，其中，所述数据类型指示所述数据包为指令数据包。

[权利要求 21] 如权利要求20所述的安全通信方法，其特征在于，所述通信第一方为飞行遥控器及所述通信第二方为无人飞行器或者无人飞行器上的一个或者多个模块。

[权利要求 22] 如权利要求20所述的安全通信方法，其特征在于，所述发送序列号Q的初始值为0，并在所述会话密钥发生变更时，重新归0，在所述会话密钥没有发生变更时，单调增长。

[权利要求 23] 如权利要求20或22所述的安全通信方法，其特征在于，所述会话密钥及发送序列号Q存储于所述通信第一方的易失性存储器中。

[权利要求 24] 一种安全通信方法，由一通信第二方所执行，其特征在于，该方法包括：

接收配对的通信第一方传送的密钥数据包；

读取一密钥序列号n；

获取密钥数据包中的密钥序列号N，在N<=n时，丢弃所述密钥数据包；

在N>n时，获取与通信第二方与一通信第一方配对时生成的秘密码字，并获取一产品密钥；

基于所述秘密码字及产品密钥得到一模块密钥；

利用所述模块密钥解密所述密钥数据包，得到一会话密钥及校验

认证码；

当利用所述校验认证码验证所述会话密钥不正确时，丢弃所述密钥数据包；

当所述会话密钥正确时，存储所述会话密钥；

接收通信第一方传送的指令数据包；

从获取一发送序列号q；

获取所述指令数据包中的发送序列号Q，当Q<=q时，丢弃所述指令数据包；

当Q>q时，获取所述会话密钥；

利用所述会话密钥解密指令数据包，得到指令数据及校验码；

当利用所述校验认证码验证所述指令数据不正确时，丢弃所述指令数据包；及

当所述指令数据正确时，执行所述指令。

[权利要求 25] 如权利要求24所述的安全通信方法，其特征在于，所述通信第一方为控制方及通信第二方为受控方。

[权利要求 26] 如权利要求25所述的安全通信方法，其特征在于，所述通信第一方飞行遥控器及所述通信第二方为无人飞行器或者无人飞行器上的一个或者多个模块。

[权利要求 27] 如权利要求26所述的安全通信方法，其特征在于，所述无人飞行器上的一个或者多个模块包括相机、云台。

[权利要求 28] 如权利要求27所述的安全通信方法，其特征在于，所述产品密钥存储在通讯第二方的安全存储区。

[权利要求 29] 如权利要求24所述的安全通信方法，其特征在于，所述模块密钥是对所述秘密码字及产品密钥执行派生算法得到的，所述派生算法包括加密、消息认证码。

[权利要求 30] 如权利要求24至29中任意一项所述的安全通信方法，其特征在于，该方法还包括：

将所述模块密钥以及所接收的发送序列号Q以及会话密钥存储于通

信第二方的易失性存储器中，并记发送序列号q=Q。

[权利要求 31] 如权利要求24至29中任意一项所述的安全通信方法，其特征在于，该方法还包括：

将所述密钥序列号N存储于所述通信第二方的非易失性存储器中，并记密钥序列号n=N。

[权利要求 32] 一种安全通信方法，由一通信第二方所执行，其特征在于，该方法包括：

接收配对的通信第一方传送的密钥数据包；

获取一预先存储的密钥序列号n；

获取密钥数据包中的密钥序列号N，在N<=n时，丢弃所述密钥数据包；

在N>n时，获取与通信第二方与一通信第一方配对时生成的秘密码字，及从获取一预先存储的产品密钥；

基于所述秘密码字及产品密钥得到一模块密钥；

利用所述模块密钥解密所述密钥数据包，得到一会话密钥及校验认证码；

当利用所述校验认证码验证所述会话密钥不正确时，丢弃所述密钥数据包；及

当所述会话密钥正确时，存储所述会话密钥。

[权利要求 33] 如权利要求32所述的安全通信方法，其特征在于，所述通信第一方飞行遥控器及所述通信第二方为无人飞行器或者无人飞行器上的一个或者多个模块。

[权利要求 34] 如权利要求32所述的安全通信方法，其特征在于，所述产品密钥是存储在通讯第二方的安全存储区。

[权利要求 35] 如权利要求32或34所述的安全通信方法，其特征在于，所述秘密码字及所述密钥序列号n存储于所述通信第二方的非易失性存储器中。

[权利要求 36] 一种安全通信方法，由一通信第二方所执行，其特征在于，该方

法包括：

接收配对的通信第一方传送的指令数据包；

获取一发送序列号q；

获取所述指令数据包中的发送序列号Q，当Q<=q时，丢弃所述指令数据包；

当Q>q时，获取一会话密钥；

利用所述会话密钥解密指令数据包，得到指令数据及校验认证码；

当利用所述校验认证码验证所述指令数据不正确时，丢弃所述指令数据包；及

当所述指令数据正确时，执行所述指令。

[权利要求 37] 如权利要求36所述的安全通信方法，其特征在于，所述通信第一方飞行遥控器及所述通信第二方为无人飞行器或者无人飞行器上的一个或者多个模块。

[权利要求 38] 如权利要求36所述的安全通信方法，其特征在于，所述会话密钥及发送序列号q存储于所述通信第二方的易失性存储器中。

[权利要求 39] 一种安全通信方法，由一通信第二方所执行，其特征在于，该方法包括：

获取一会话密钥；

获取一发送序列号M，并对发送序列号M进行自增；

获取待发送的反馈数据，利用所述会话密钥对所述反馈数据以及反馈数据的校验认证码进行加密，生成一反馈数据帧；及

将所述反馈数据帧、发送序列号M发送给配对的通信第一方。

[权利要求 40] 如权利要求39所述的安全通信方法，其特征在于，所述通讯第一方为主控方，所述通信第二方为受控方。

[权利要求 41] 如权利要求40所述的安全通信方法，其特征在于，所述通信第一方飞行遥控器及所述通信第二方为无人飞行器或者无人飞行器上的一个或者多个模块。

[权利要求 42] 如权利要求41所述的安全通信方法，其特征在于，所述无人飞行器上的一个或者多个模块包括相机、云台。

[权利要求 43] 如权利要求39所述的安全通信方法，其特征在于，所述会话密钥通过下述方法得到：

接收所述通信第一方传送的密钥数据包；

获取一预先存储的密钥序列号n；

获取密钥数据包中的密钥序列号N，在N<=n时，丢弃所述密钥数据包；

在N>n时，获取与通信第二方与一通信第一方配对时生成的秘密码字，及从获取一预先存储的产品密钥；

基于所述秘密码字及产品密钥得到一模块密钥；

利用所述模块密钥解密所述密钥数据包，得到一会话密钥及校验认证码；

当利用所述校验认证码验证所述会话密钥不正确时，丢弃所述密钥数据包；及

当所述会话密钥正确时，存储所述会话密钥。

[权利要求 44] 如权利要求43所述的安全通信方法，其特征在于，所述产品密钥是存储在通讯第二方的安全存储区。

[权利要求 45] 如权利要求43所述的安全通信方法，其特征在于，所述秘密码字及所述密钥序列号n存储于所述通信第二方的非易失性存储器中。

[权利要求 46] 一种安全通信方法，其特征在于，该方法包括：

通信第一方利用一模块密钥对一随机产生的会话密钥进行加密，并传送给通信第二方；

所述通信第二方利用所述模块密钥对所述会话密钥进行解密，得到所述会话密钥。

[权利要求 47] 如权利要求46所述的安全通信方法，其特征在于，所述模块密钥通过下述方法得到：

获取通信第一方与一通信第二方配对时生成的秘密码字，并获取

一预先存储的产品密钥；及

基于所述秘密码字及产品密钥，通过派生算法得到所述模块密钥。

[权利要求 48] 如权利要求46所述的安全通信方法，其特征在于，所述通信第一方为控制方及通信第二方为受控方。

[权利要求 49] 如权利要求48所述的安全通信方法，其特征在于，所述通信第一方飞行遥控器及所述通信第二方为无人飞行器或者无人飞行器上的一个或者多个模块。

[权利要求 50] 如权利要求49所述的安全通信方法，其特征在于，所述无人飞行器上的一个或者多个模块包括相机、云台。

[权利要求 51] 如权利要求46所述的安全通信方法，其特征在于，所述通信第一方及通信第二方均既是信息发送方又是信息接收方。

[权利要求 52] 如权利要求51所述的安全通信方法，其特征在于，所述通信第一方及通信第二方是两个无人飞行器、或者是无人飞行器的两个模块。

[权利要求 53] 一种通信装置，其特征在于，该装置包括：

认证发送模块，用于获取所述通信装置与另一通信装置配对时生成的秘密码字，并获取预先存储的产品密钥；基于所述秘密码字及产品密钥得到一模块密钥；随机产生一会话密钥；获取一密钥序列号N，并对序列号N进行自增，及设置一初始值为0的发送序列号Q；利用所述模块密钥对所述会话密钥及所述会话密钥的校验认证码进行运算，生成一密钥帧；将所述密钥帧、密钥序列号N、发送序列号Q及一数据类型的数据包发送给通信第二方，其中，所述数据类型指示所述数据包为密钥数据包；及

指令发送模块，用于获取所述发送序列号Q，并对序列号Q进行自增；获取待发送的指令数据，利用所述会话密钥对所述指令数据以及所述指令数据的校验认证码进行加密，生成一指令数据帧；及将所述指令数据帧、发送序列号Q以及一数据类型的数据包发送

给通信第二方，其中，所述数据类型指示所述数据包为指令数据包。

[权利要求 54] 如权利要求53所述的通信装置，其特征在于，所述通信装置为飞行遥控器。

[权利要求 55] 如权利要求53所述的通信装置，其特征在于，所述通信装置包括一个或者多个非易失性存储器，用于存储所述产品密钥、秘密码字以及密钥序列号N。

[权利要求 56] 如权利要求53所述的通信装置，其特征在于，所述通信装置包括一个或者多个易失性存储器，用于存储所述模块密钥、会话密钥以及发送序列号Q。

[权利要求 57] 如权利要求53所述的通信装置，其特征在于，所述模块密钥是对所述秘密码字及产品密钥执行派生算法得到的，所述派生算法包括加密、消息认证码。

[权利要求 58] 如权利要求53所述的通信装置，其特征在于，所述会话密钥是使用随机数发生器动态产生的。

[权利要求 59] 如权利要求53所述的通信装置，其特征在于，对序列号N的自增方法包括每向通信第二方发送一次数据，则N值增加1。

[权利要求 60] 如权利要求53所述的通信装置，其特征在于，所述序列号Q的自增方法包括每向通信第二方发送一次数据，则Q值增加1，或者每隔预设的时间段Q值增加1。

[权利要求 61] 如权利要求53所述的通信装置，其特征在于，利用所述模块密钥对所述会话密钥及所述会话密钥的校验认证码进行运算的方法包括加密运算及/或消息认证码。

[权利要求 62] 一种通信装置，其特征在于，该通信装置包括：

认证接收模块，用于接收配对的另一个通信装置传送的密钥数据包；读取一密钥序列号n；获取密钥数据包中的密钥序列号N，在N<=n时，丢弃所述密钥数据包；在N>n时，获取与通信第二方与一通信第一方配对时生成的秘密码字，并获取一产品密钥；基于

所述秘密码字及产品密钥得到一模块密钥；利用所述模块密钥解密所述密钥数据包，得到一会话密钥及校验认证码；当利用所述校验认证码验证所述会话密钥不正确时，丢弃所述密钥数据包；当所述会话密钥正确时，存储所述会话密钥；及

指令执行模块，用于接收另一通信装置传送的指令数据包；从获取一发送序列号q；获取所述指令数据包中的发送序列号Q，当Q<=q时，丢弃所述指令数据包；当Q>q时，获取所述会话密钥；利用所述会话密钥解密指令数据包，得到指令数据及校验认证码；当利用所述校验认证码验证所述指令数据不正确时，丢弃所述指令数据包；及当所述指令数据正确时，执行所述指令。

[权利要求 63] 如权利要求62所述的通信装置，其特征在于，所述通信装置为无人飞行器或者无人飞行器上的一个或者多个模块。

[权利要求 64] 如权利要求63所述的通信装置，其特征在于，所述无人飞行器上的一个或者多个模块包括相机、云台。

[权利要求 65] 如权利要求62所述的通信装置，其特征在于，所述通信装置包括非易失性存储器，用于存储所述产品密钥、密钥码字以及密钥序列号n。

[权利要求 66] 如权利要求65所述的通信装置，其特征在于，所述认证接收模块还用于将所述密钥序列号N存储于所述非易失性存储器中，并记密钥序列号n=N。

[权利要求 67] 如权利要求62所述的通信装置，其特征在于，所述通信装置包括易失性存储器，用于存储所述模块密钥、会话密钥及发送序列号q。

[权利要求 68] 如权利要求67所述的通信装置，其特征在于，所述指令接收模块还用于将所接收的发送序列号Q以及会话密钥存储于所述通信装置的易失性存储器中，并记发送序列号q=Q。

[权利要求 69] 如权利要求62所述的通信装置，其特征在于，所述模块密钥是对所述秘密码字及产品密钥执行派生算法得到的，所述派生算法包

括加密、消息认证码。

[权利要求 70] 如权利要求62所述的通信装置，其特征在于，所述通信装置还包括：

反馈数据发送模块，用于获取所述会话密钥；

获取一发送序列号M，并对发送序列号M进行自增；

获取待发送的反馈数据，利用所述会话密钥对所述反馈数据以及反馈数据的校验认证码进行加密，生成一反馈数据帧；及

将所述反馈数据帧、发送序列号M发送给配对的通信第一方。

[权利要求 71] 一种安全通信系统，包括通过无线网络进行通信的通信第一方及通信第二方，其特征在于：

所述通信第一方利用一模块密钥对一随机产生的会话密钥进行加密，并传送给通信第二方；及

所述通信第二方利用所述模块密钥对所述会话密钥进行解密，得到所述会话密钥。

[权利要求 72] 如权利要求71所述的安全通信系统，其特征在于，所述模块密钥通过下述方法得到：

获取通信第一方与一通信第二方配对时生成的秘密码字，并获取一预先存储的产品密钥；及

基于所述秘密码字及产品密钥，通过派生算法得到所述模块密钥。

[权利要求 73] 如权利要求71所述的安全通信系统，其特征在于，所述通信第一方为控制方及通信第二方为受控方。

[权利要求 74] 如权利要求73所述的安全通信系统，其特征在于，所述通信第一方飞行遥控器及所述通信第二方为无人飞行器或者无人飞行器上的一个或者多个模块。

[权利要求 75] 如权利要求74所述的安全通信系统，其特征在于，所述无人飞行器上的一个或者多个模块包括相机、云台或遥控器中的一个或多个。

[权利要求 76] 如权利要求71所述的安全通信系统，其特征在于，所述通信第一方及通信第二方均既是信息发送方又是信息接收方。

[权利要求 77] 如权利要求76所述的安全通信系统，其特征在于，所述通信第一方及通信第二方是两个无人飞行器、或者是无人飞行器的两个模块。

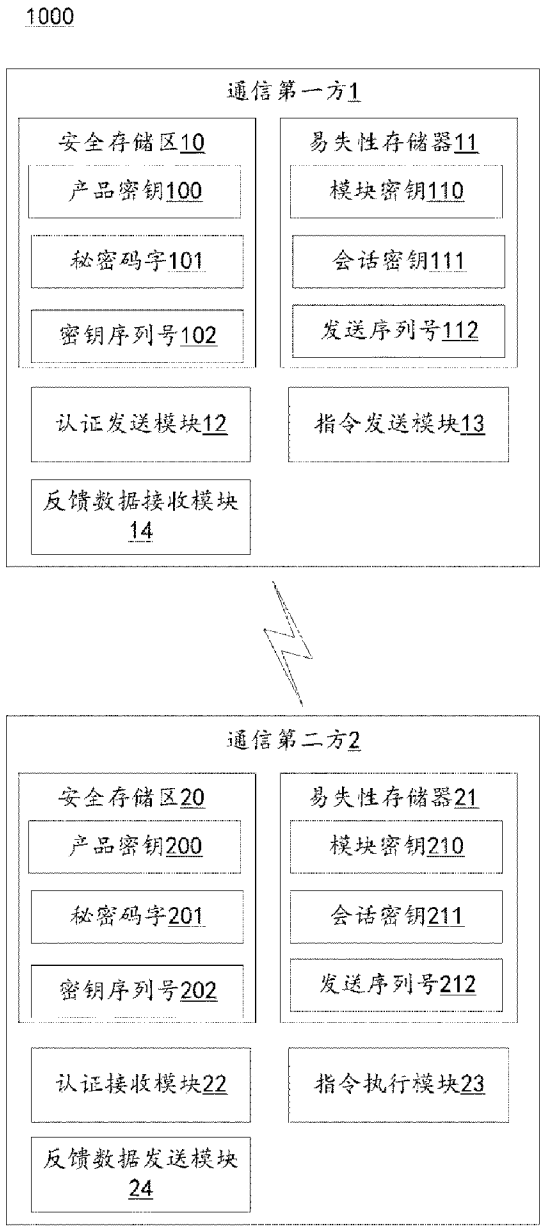
1000
通信第一方1
安全存储区10
产品密钥100
秘密码字101
密钥序列号102
易失性存储器11
模块密钥110
会话密钥111
发送序列号112
认证发送模块12
指令发送模块13
反馈数据接收模块14
通信第二方2
安全存储区20
产品密钥200
秘密码字201
密钥序列号202
易失性存储器21
模块密钥210
会话密钥211
发送序列号212
认证接收模块22
指令执行模块23
反馈数据发送模块24

图1

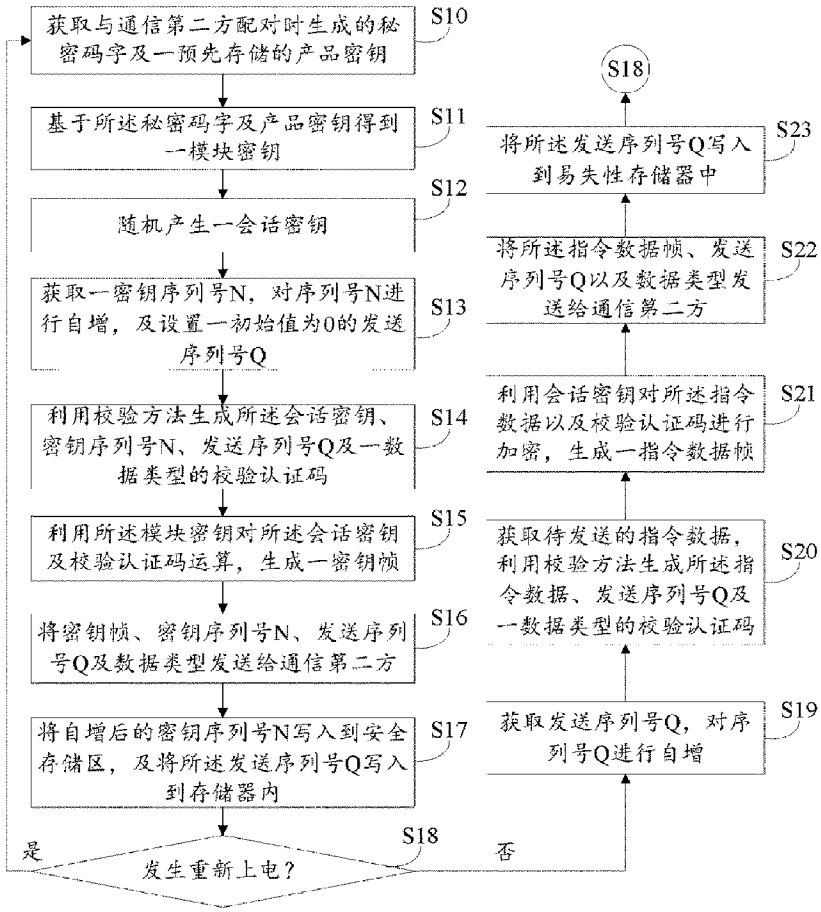
获取与通信第二方配对时生成的秘密码字及一预先存储的产品密钥
S10
基于所述秘密码字及产品密钥得到一模块密钥
S11
随机产生一会话密钥
S12
获取一密钥序列号N，对序列号N进行自增，及设置一初始值为0的发送序列号Q
S13
利用校验方法生成所述会话密钥、密钥序列号N、发送序列号Q及一数据类型的校验认证码
S14
利用所述模块密钥对所述会话密钥及校验认证码运算，生成一密钥帧
S15
将密钥帧、密钥序列号N、发送序列号Q及数据类型发送给通信第二方
S16
将自增后的密钥序列号N写入到安全存储区，及将所述发送序列号Q写入到存储器内
S17
发生重新上电？
S18
是
否
S18
将所述发送序列号Q写入到易失性存储器中
S23
将所述指令数据帧、发送序列号Q以及数据类型发送给通信第二方
S22
利用会话密钥对所述指令数据以及校验认证码进行加密，生成一指令数据帧
S21
获取待发送的指令数据，利用校验方法生成所述指令数据、发送序列号Q及一数据类型的校验认证码
S20
获取发送序列号Q，对序列号Q进行自增
S19

图2

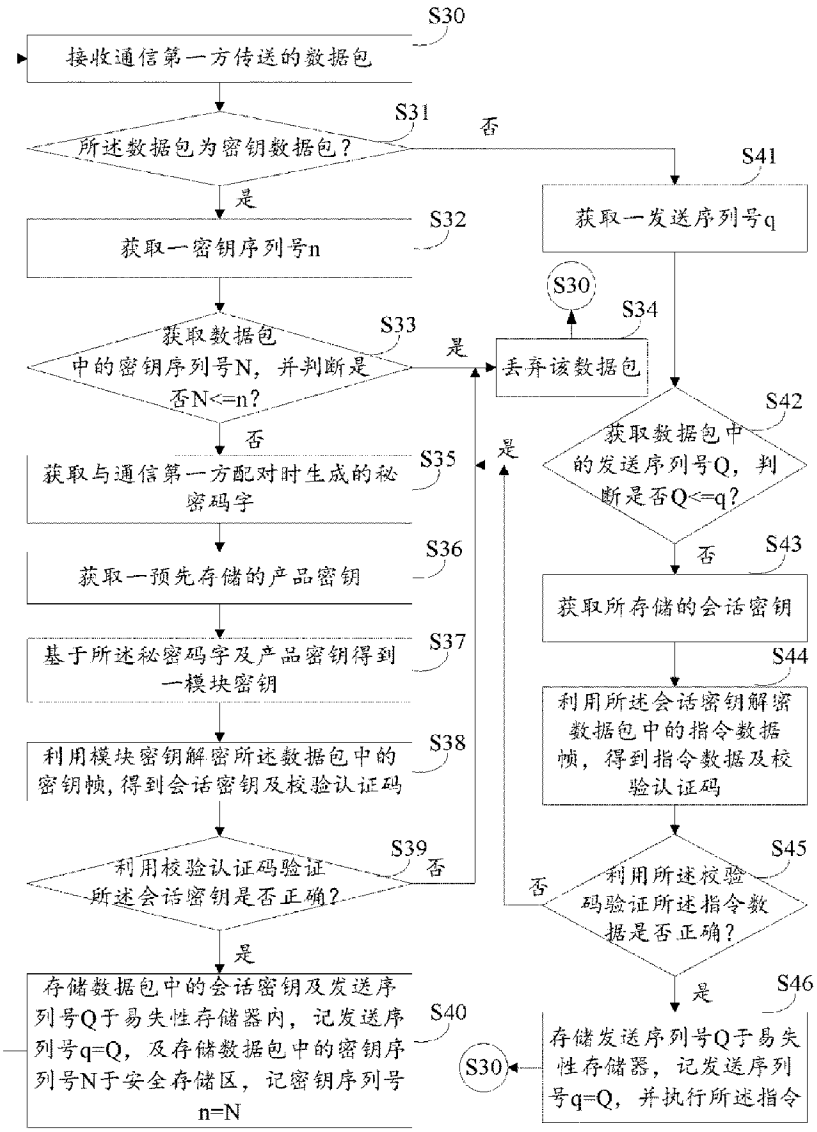
S30
接收通信第一方传送的数据包
S31
所述数据包为密钥数据包?
否
是
S41
获取一发送序列号q
S32
获取一密钥序列号n
S30
S34
S33
获取数据包中的密钥序列号N，并判断是否N<=n?
是
丢弃该数据包
否
S42
获取数据包中的发送序列号Q，判断是否Q<=q?
是
S35
获取与通信第一方配对时生成的秘密码字
否
S43
获取所存储的会话密钥
S36
获取一预先存储的产品密钥
S44
利用所述会话密钥解密数据包中的指令数据帧，得到指令数据及校验认证码
S37
基于所述秘密码字及产品密钥得到一模块密钥
S38
利用模块密钥解密所述数据包中的密钥帧，得到会话密钥及校验认证码
S39
利用校验认证码验证所述会话密钥是否正确?
否
S45
利用所述校验码验证所述指令数据是否正确?
否
是
S46
是
存储数据包中的会话密钥及发送序列号Q于易失性存储器内，记发送序列号q=Q，及存储数据包中的密钥序列号N于安全存储区，记密钥序列号n=N
S40
S30
存储发送序列号Q于易失性存储器，记发送序列号q=Q，并执行所述指令

图3

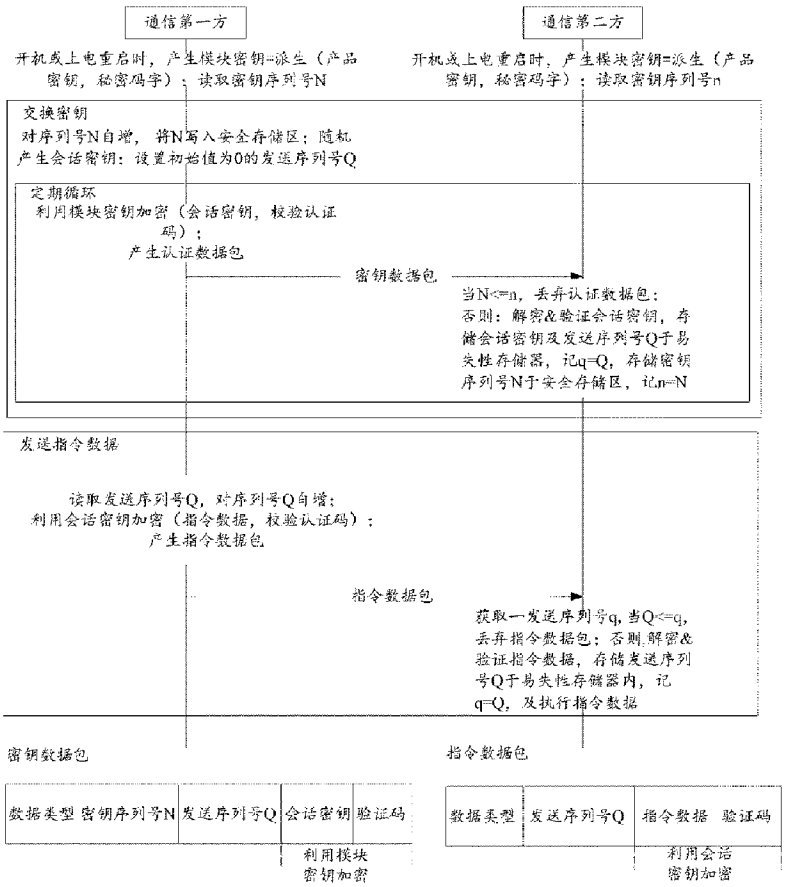
通信第一方
通信第二方
开机或上电重启时，产生模块密钥=派生（产品密钥，秘密码字）；读取密钥序列号N
开机或上电重启时，产生模块密钥=派生（产品密钥，秘密码字）；读取密钥序列号n
交换密钥
对序列号N自增，将N写入安全存储区；随机产生会话密钥；设置初始值为0的发送序列号Q
定期循环
利用模块密钥加密（会话密钥，校验认证码）；
产生认证数据包
密钥数据包
当N<=n，丢弃认证数据包；否则：解密&验证会话密钥，存储会话密钥及发送序列号Q于易失性存储器，记q=Q，存储密钥序列号N于安全存储区，记n=N
发送指令数据
读取发送序列号Q，对序列号Q自增；
利用会话密钥加密（指令数据，校验认证码）；
产生指令数据包
指令数据包
获取一发送序列号q，当Q<=q，丢弃指令数据包；否则解密&验证指令数据，存储发送序列号Q于易失性存储器内，记q=Q，及执行指令数据
密钥数据包
数据类型 密钥序列号N 发送序列号Q 会话密钥 验证码
利用模块密钥加密
指令数据包
数据类型 发送序列号Q 指令数据 验证码
利用会话密钥加密

图4

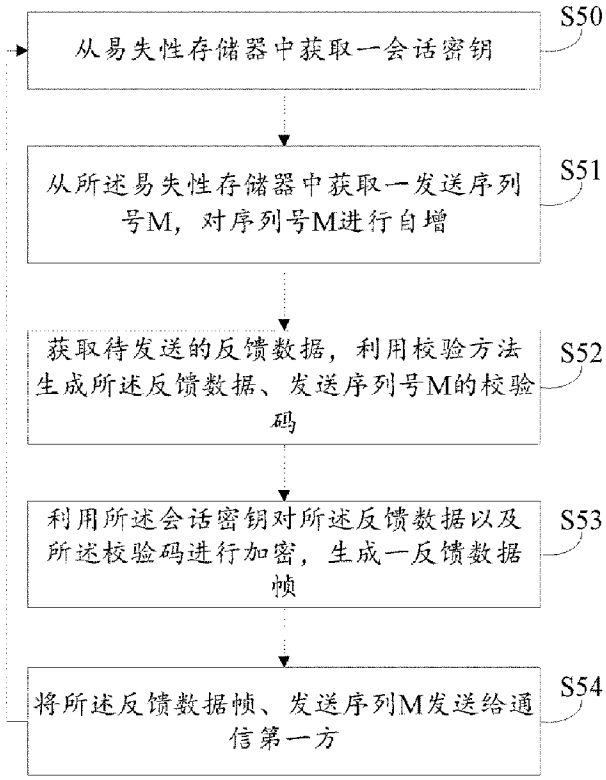
从易失性存储器中获取一会话密钥
S50
从所述易失性存储器中获取一发送序列号M，对序列号M进行自增
S51
获取待发送的反馈数据，利用校验方法生成所述反馈数据、发送序列号M的校验码
S52
利用所述会话密钥对所述反馈数据以及所述校验码进行加密，生成一反馈数据帧
S53
将所述反馈数据帧、发送序列M发送给通信第一方
S54

图5

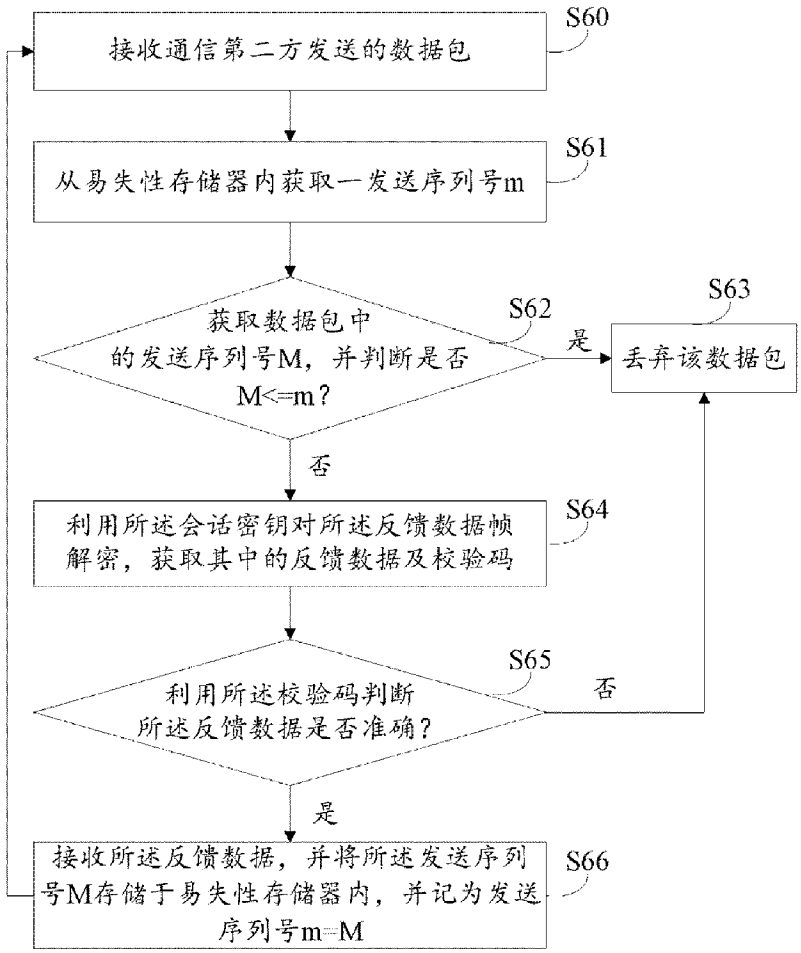
S60
接收通信第二方发送的数据包
S61
从易失性存储器内获取一发送序列号m
S62
获取数据包中的发送序列号M，并判断是否M<=m？
是
S63
丢弃该数据包
否
S64
利用所述会话密钥对所述反馈数据帧解密，获取其中的反馈数据及校验码
S65
利用所述校验码判断所述反馈数据是否准确？
否
是
S66
接收所述反馈数据，并将所述发送序列号M存储于易失性存储器内，并记为发送序列号m=M

图6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/097060

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/12 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; G06F; G01D

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, EPODOC, CNPAT, CNKI: session key, secret code, product key, module key, traffic encryption key, TEK, sequence number, increase, verify, authentication, instruction, encrypt, decrypt

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 103258152 A (THOMSON LICENSING SA), 21 August 2013 (21.08.2013), claims 1-5, and description, paragraphs [0029]-[0042]	20-23, 36-42, 46, 48-52, 71, 73-77
X	US 2014304511 A1 (ROBERT BOSCH GMBH), 09 October 2014 (09.10.2014), description, paragraphs [0019]-[0027]	46, 48-52, 71, 73-77
A	CN 104023013 A (SHANGHAI DNION INFORMATION TECHNOLOGY CO., LTD.), 03 September 2014 (03.09.2014), the whole document	1-77
A	CN 1767429 A (SHANGHAI DATANG MOBILE COMMUNICATIONS EQUIPMENT CO., LTD.), 03 May 2006 (03.05.2006), the whole document	1-77
A	US 2014270166 A1 (QUALCOMM INCORPORATED), 18 September 2014 (18.09.2014), the whole document	1-77

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 April 2016 (21.04.2016)	**24 August 2016 (24.08.2016)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **SUN, Zhifei** Telephone No.: (86-10) **52871153**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/097060

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103258152 A	21 August 2013	US 2014140504 A1	22 May 2014
		EP 2629223 A1	21 August 2013
		JP 2013175179 A	05 September 2013
		KR 20130093557 A	22 August 2013
		EP 2629225 A1	21 August 2013
		TW 201337633 A1	16 September 2013
US 2014304511 A1	09 October 2014	DE 102013206202 A1	30 October 2014
		CN 104101376 A	15 October 2014
CN 104023013 A	03 September 2014	None	
CN 1767429 A	03 May 2006	None	
US 2014270166 A1	18 September 2014	EP 2974340 A1	20 January 2016
		WO 2014159689 A1	02 October 2014
		CN 105009597 A	28 October 2015
		KR 20150129824 A	20 November 2015

国际检索报告

国际申请号 PCT/CN2015/097060

A. 主题的分类

H04L 9/12(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L; G06F; G01D

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

WPI,EPODOC,CNPAT,CNKI:秘密码字，产品密钥，模块密钥，会话密钥，序列号，增加，校验，认证，指令，加密，解密，secret code，product key，module key，traffic encryption key，TEK，sequence number，increase，verify，authentication，instruction，encrypt，decrypt

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN 103258152 A (汤姆森特许公司) 2013年 8月 21日 (2013-08-21) 权利要求1-5，说明书第[0029]-[0042]段	20-23，36-42，46，48-52，71，73-77
X	US 2014304511 A1 (ROBERT BOSCH GMBH) 2014年 10月 9日 (2014-10-09) 说明书第[0019]-[0027]段	46，48-52，71，73-77
A	CN 104023013 A (上海帝联信息科技股份有限公司) 2014年 9月 3日 (2014-09-03) 全文	1-77
A	CN 1767429 A (大唐移动通信设备有限公司) 2006年 5月 3日 (2006-05-03) 全文	1-77
A	US 2014270166 A1 (QUALCOMM INCORPORATED) 2014年 9月 18日 (2014-09-18) 全文	1-77

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2016年 4月 21日	2016年 8月 24日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	孙志飞
传真号 (86-10)62019451	电话号码 (86-10)52871153

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2015/097060

检索报告引用的专利文件			公布日（年/月/日）	同族专利			公布日（年/月/日）
CN	103258152	A	2013年 8月 21日	US	2014140504	A1	2014年 5月 22日
				EP	2629223	A1	2013年 8月 21日
				JP	2013175179	A	2013年 9月 5日
				KR	20130093557	A	2013年 8月 22日
				EP	2629225	A1	2013年 8月 21日
				TW	201337633	A	2013年 9月 16日
US	2014304511	A1	2014年 10月 9日	DE	102013206202	A1	2014年 10月 30日
				CN	104101376	A	2014年 10月 15日
CN	104023013	A	2014年 9月 3日	无			
CN	1767429	A	2006年 5月 3日	无			
US	2014270166	A1	2014年 9月 18日	EP	2974340	A1	2016年 1月 20日
				WO	2014159689	A1	2014年 10月 2日
				CN	105009597	A	2015年 10月 28日
				KR	20150129824	A	2015年 11月 20日