

(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
2018 年 5 月 24 日 (24.05.2018)



(10) 国际公布号
WO 2018/090339 A1

- (51) 国际专利分类号:
H04L 9/00 (2006.01)
- (21) 国际申请号: PCT/CN2016/106451
- (22) 国际申请日: 2016 年 11 月 18 日 (18.11.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (71) 申请人: 海能达通信股份有限公司(HYTERA COMMUNICATIONS CORPORATION LIMITED) [CN/CN]; 中国广东省深圳市南山区高新技术产业园北区北环路海能达大厦, Guangdong 518057 (CN)。
- (72) 发明人: 罗正华(LUO, Zhenghua); 中国广东省深圳市南山区高新技术产业园北区北环路海能达大厦, Guangdong 518057 (CN)。 马琰(MA, Yan);

中国广东省深圳市南山区高新技术产业园北区北环路海能达大厦, Guangdong 518057 (CN)。 张颖哲(ZHANG, Yingzhe); 中国广东省深圳市南山区高新技术产业园北区北环路海能达大厦, Guangdong 518057 (CN)。 徐燕(XU, Yan); 中国广东省深圳市南山区高新技术产业园北区北环路海能达大厦, Guangdong 518057 (CN)。 左银丽(ZUO, Yinli); 中国广东省深圳市南山区高新技术产业园北区北环路海能达大厦, Guangdong 518057 (CN)。 刘洋(LIU, Yang); 中国广东省深圳市南山区高新技术产业园北区北环路海能达大厦, Guangdong 518057 (CN)。

(74) 代理人: 深圳市威世博知识产权代理事务所(普通合伙)(CHINA WISPRO INTELLECTUAL PROPERTY LLP.); 中国广东省深圳市南山区高

(54) Title: WIRELESS COMMUNICATION METHOD AND DEVICE, AND COMMUNICATION APPARATUS

(54) 发明名称: 无线通信方法、装置及通信设备

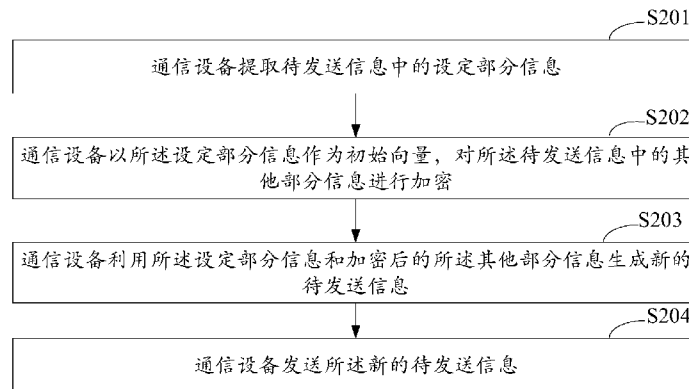


图2

- S201 A communication apparatus extracting set partial information in information to be sent
- S202 The communication apparatus taking the set partial information as an initial vector to encrypt other partial information in the information to be sent
- S203 The communication apparatus using the set partial information and the encrypted other partial information to generate new information to be sent
- S204 The communication apparatus sending the new information to be sent

(57) Abstract: Disclosed in the present application are a wireless communication method and device, and a communication apparatus. The method comprises: a communication apparatus extracting set partial information in information to be sent; taking the set partial information as an initial vector to encrypt other partial information in the information to be sent; using the set partial information and the encrypted other partial information to generate new information to be sent; and sending the new information to be sent. By means of the method, security of wireless communication can be ensured.



新区粤兴三道8号中国地质大学产学研基地中
地大楼A806, Guangdong 518057 (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, DJ, 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, KW, 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, 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))。

(57) 摘要: 本申请公开了无线通信方法、装置及通信设备。其中, 该方法包括: 通信设备提取待发送信息中的设定部分信息; 以所述设定部分信息作为初始向量, 对所述待发送信息中的其他部分信息进行加密; 利用所述设定部分信息和加密后的所述其他部分信息生成新的待发送信息; 发送所述新的待发送信息。通过上述方式, 能够保证无线通信的安全性。

无线通信方法、装置及通信设备

[1] 【技术领域】

[2] 本申请涉及无线技术领域，特别是可实现通信安全的无线通信方法、装置及通信设备。

[3] 【背景技术】

[4] 在目前无线通信标准如DMR/PDT中，信息均是以明文的形式在空中传输。任何一个通信设备，只要遵循对应的无线通信标准，就能加入到该无线通信系统，在相应的物理信道上与其他通信设备进行相互通信。

[5] 显然，现有的无线通信标准中，缺乏对无线通信系统中传输的信息进行保护，使得任何一个遵循对应无线通信标准的通信设备均可在相应的物理信道上进行监听，导致通信信息被窃取，信息泄密。

[6] 【发明内容】

[7] 本申请提供无线通信方法、装置及通信设备，能够保证无线通信的安全性。

[8] 本申请第一方面提供一种无线通信方法，包括：通信设备提取待发送信息中的设定部分信息；以所述设定部分信息作为初始向量，对所述待发送信息中的其他部分信息进行加密；利用所述设定部分信息和加密后的所述其他部分信息生成新的待发送信息；发送所述新的待发送信息。

[9] 其中，所述设定部分信息为所述待发送信息中的校验数据和/或信令。

[10] 其中，所述待发送信息为信令，所述设定部分信息为所述信令的校验数据，所述其他部分信息为所述信令的信令内容；或所述待发送信息为语音呼叫信息，所述设定部分信息为所述语音呼叫信息中的语音头帧和/或语音结束帧，所述其他部分信息为所述语音呼叫信息中的语音帧；或所述待发送信息为数据业务信息，所述设定部分信息为所述数据业务信息的数据头帧和/或数据结束帧，所述其他部分信息为所述数据业务信息的数据帧。

[11] 其中，在所述利用所述设定部分信息和加密后的所述其他部分信息生成新的待发送信息之前，还包括：对所述设定部分信息按照设定加密规则进行加密处理

- 。
- [12] 其中，所述以所述设定部分信息作为初始向量，对所述待发送信息中的其他部分信息进行加密，包括：以所述设定部分信息作为初始向量，按照设定加密公式和设定数据对所述待发送信息中的其他部分信息进行运算，将运算结果作为加密后的所述其他部分信息。
- [13] 本申请第二方面提供一种无线通信方法，包括：通信设备提取已接收信息中的设定部分信息；以所述设定部分信息作为初始向量，对所述已接收信息中的其他部分信息进行解密；对由所述设定部分信息和解密后的所述其他部分信息组成的新的已接收信息进行处理。
- [14] 其中，所述设定部分信息为所述已接收信息中的校验数据和/或信令。
- [15] 其中，所述已接收信息为信令，所述设定部分信息为所述信令的校验数据，所述其他部分信息为所述信令的信令内容；所述对由所述设定部分信息和解密后的所述其他部分信息组成的新的已接收信息进行处理，包括：由解密后的所述信令内容生成新校验数据；比较所述信令中的校验数据与所述新校验数据是否相同；若相同，则对由所述校验数据和解密后的所述信令内容生成新信令，并响应所述新信令；否则丢弃所述信令。
- [16] 其中，所述已接收信息为语音呼叫信息，所述设定部分信息为所述语音呼叫信息中的语音头帧和/或语音结束帧，所述其他部分信息为所述语音呼叫信息中的语音帧。
- [17] 其中，所述已接收信息为数据业务信息，所述设定部分信息为所述数据业务信息的数据头帧和/或数据结束帧，所述其他部分信息为所述数据业务信息的数据帧；
- [18] 所述对由所述设定部分信息和解密后的所述其他部分信息组成的新的已接收信息进行处理，包括：由解密后的所述数据帧生成新校验数据；比较所述解密后的数据帧中的校验数据与所述新校验数据是否相同；若相同，则对解密后的新数据业务信息进行处理；否则丢弃所述数据业务信息。
- [19] 其中，在所述以所述设定部分信息作为初始向量，对所述已接收信息中的其他部分信息进行解密之前，还包括：对所述设定部分信息按照设定解密规则进行

解密处理。

- [20] 其中，所述以所述设定部分信息作为初始向量，对所述已接收信息中的其他部分信息进行解密，包括：以所述设定部分信息作为初始向量，按照设定解密公式和设定数据对所述待发送信息中的其他部分信息进行运算，将运算结果作为解密后的所述其他部分信息。
- [21] 本申请第三方面提供一种无线通信装置，包括：提取模块，用于提取待发送信息中的设定部分信息；加密模块，用于以所述设定部分信息作为初始向量，对所述待发送信息中的其他部分信息进行加密；生成模块，用于利用所述设定部分信息和加密后的所述其他部分信息生成新的待发送信息；发送模块，用于发送所述新的待发送信息。
- [22] 本申请第四方面提供一种无线通信装置，包括：提取模块，用于提取已接收信息中的设定部分信息；解密模块，用于以所述设定部分信息作为初始向量，对所述已接收信息中的其他部分信息进行解密；处理模块，用于对由所述设定部分信息和解密后的所述其他部分信息组成的新的已接收信息进行处理。
- [23] 本申请第五方面提供一种通信设备，包括发送器、存储器及处理器；所述存储器用于存储被配置为被所述处理器执行的计算机指令；所述处理器执行所述计算机指令，用于：提取待发送信息中的设定部分信息；以所述设定部分信息作为初始向量，对所述待发送信息中的其他部分信息进行加密；利用所述设定部分信息和加密后的所述其他部分信息生成新的待发送信息；通过所述发送器发送所述新的待发送信息。
- [24] 本申请第六方面提供一种通信设备，包括接收器、存储器及处理器；所述存储器用于存储被配置为被所述处理器执行的计算机指令；所述处理器执行所述计算机指令，用于：提取所述接收器接收到的已接收信息中的设定部分信息；以所述设定部分信息作为初始向量，对所述已接收信息中的其他部分信息进行解密；对由所述设定部分信息和解密后的所述其他部分信息组成的新的已接收信息进行处理。
- [25] 上述方案中，通信设备采用待发送信息或已接收信息的设定部分信息作为初始向量对其他部分信息进行加密或解密处理，故非法设备无法窃取到该无线通信

系统内传输的信息且其发送的消息无法得到该无线通信系统的正确响应，从而保证了该无线通信的安全性，避免了非法设备的信息干扰，另外，由于通信设备直接利用待发送信息的部分信息作为初始向量进行加密，无需额外初始向量，故无需增加空口开销。

[26] **【附图说明】**

[27] 图1是本申请无线通信系统一实施方式的结构示意图；

[28] 图2是本申请无线通信方法一实施方式的流程图；

[29] 图3是图1所示实施例一应用场景的通信流程框图；

[30] 图4是图1所示实施例另一应用场景的通信流程框图；

[31] 图5是本申请无线通信方法另一实施方式的流程图；

[32] 图6是图5所示实施例一应用场景的通信流程框图；

[33] 图7是图5所示实施例另一应用场景的通信流程框图；

[34] 图8是本申请无线通信装置一实施方式的结构示意图；

[35] 图9是本申请无线通信装置另一实施方式的结构示意图；

[36] 图10是本申请通信设备一实施方式的结构示意图。

[37] **【具体实施方式】**

[38] 以下描述中，为了说明而不是为了限定，提出了诸如特定系统结构、接口、技术之类的具体细节，以便透彻理解本申请。然而，本领域的技术人员应当清楚，在没有这些具体细节的其它实施方式中也可以实现本申请。在其它情况中，省略对众所周知的装置、电路以及方法的详细说明，以免不必要的细节妨碍本申请的描述。

[39] 为便于理解本申请，先对本申请无线通信系统进行说明。

[40] 该无线通信系统为设备间可根据如数字移动无线电（英文：Digital Mobile Radio，简称：DMR）、警用数字集群（英文Police Digital Trunking，简称：PDT）等无线通信标准进行通信的系统，其通信模式可以为直通模式、中转模式或集群模式，直通模式即设备间直接通过无线信道进行通信；中转模式即设备发送的信息需经过中转台转发到其他设备；集群模式即设备发送的信息需经过系统或基站转发到其他设备。

- [41] 请参阅图1，图1是本申请无线通信系统一实施方式的结构示意图。以集群模式的无线通信系统举例，该无线通信系统10包括多个通信设备11、12、多个基站13、14（图1仅示范性示出两个通信设备和基站，但实际上无线通信系统中的通信设备和基站的数目是不受限制，可根据实际需求设置）。其中，通信设备11、12通过基站13、14与集群核心网15连接，集群核心网15可用于移动性管理和呼叫管理。
- [42] 该无线通信系统10中的通信设备之间可通过基站和集群核心网进行无线通信，如通话、数据交互等。具体，该通信设备可以为任意可进行无线通信的设备，例如手机、电脑等终端。
- [43] 本实施例中，通信设备11、12在发送信息时对其信息进行加密处理，并在接收到信息时对其信息进行相应解密，以保证该系统10无线通信的安全性。具体，为了保证该系统10的通信设备的正常通信，该系统10设置有统一的内部加密标准，加入该系统10的通信设备获取该内部加密标准，并按照该标准对通信信息进行正确的加/解密处理，从而保证系统内部的有效通信，同时，由于未经系统10认证的外部非法通信设备无法获取该加密标准，故无法对系统内的通信信息进行正确的加/解密，从而避免其非法窃取系统内的通信信息或向系统发送信息，保证系统内部通信的安全性。
- [44] 具体地，系统中的通信设备在发送和接收信息时的加/解密处理请对应参阅以下实施例。
- [45] 请参阅图2，图2是本申请无线通信方法一实施方式的流程图。该方法由无线通信系统中的通信设备执行，用于在发送信息时对信息进行加密处理。具体，该方法包括：
- [46] S201：通信设备提取待发送信息中的设定部分信息。
- [47] 例如，当通信设备需要向该无线通信系统的其他通信设备发送数据时，生成原始的待发送信息，并根据所在系统的内部加密标准，从待发送信息中提取设定部分信息。
- [48] 其中，根据实际通信需求，系统内部加密标准可设置该待发送信息的任一部分作为该设定部分信息。由于该设定部分信息用于作为加密的初始向量，为了进

一步保证加密的安全性，优选将待发送信息的非敏感且非恒定信息设置为该设定部分信息，例如，该待发送信息中的校验数据和/或信令，对于不同的待发送信息，其校验部分、信令部分通常也是不同的，即每条待发送信息加密都是不同的，故保证了加密的变化性，进一步提高了通信安全。

[49] 具体，本申请所述的信令包括语音链路帧、数据链路帧、控制信令块等。该语音链路帧如语音头帧、语音结束帧，进一步地，该语音链路帧按照不同的设置方式分为嵌入式和非嵌入式，嵌入式语音链路帧即该语音链路帧划分为若干部分插入至语音帧中，非嵌入式语音链路帧即该语音链路帧作为整体设置在语音帧的前面或后面；该数据链路帧如数据头帧、数据结束帧。

[50] S202：通信设备以所述设定部分信息作为初始向量，对所述待发送信息中的其他部分信息进行加密。

[51] 例如，通信设备以提取的设定部分信息作为初始向量，按照设定加密公式和设定数据对所述待发送信息中的其他部分信息进行运算，将运算结果作为加密后的所述其他部分信息。该设定加密公式可为现有的加密算法，或者自定义的任意运算公式。通信设备根据该系统的内部加密标准可确定该设定加密公式和设定数据。

[52] 可以理解的是，该所述其他部分信息为该待发送信息中除该设定部分信息外的剩余信息的全部或部分信息。

[53] S203：通信设备利用所述设定部分信息和加密后的所述其他部分信息生成新的待发送信息。

[54] 例如，若该其他部分信息为该待发送信息的中除该设定部分信息外的剩余信息的全部信息，则通信设备将设定部分信息和该其他部分信息组成新的待发送信息；若该其他部分信息为该待发送信息的中除该设定部分信息外的剩余信息的部分信息，则通信设备将设定部分信息、该其他部分信息以及另一部分信息组成新的待发送信息，该另一部分信息即为该待发送信息的中除该设定部分信息和该其他部分信息外的剩余信息。

[55] 在另一实施例中，为进一步提高通信信息的安全性，通信设备可以在S203之前，对该设定部分信息按照设定加密规则进行加密处理，在S203中再利用加密后

的设定部分信息和加密后的其他部分信息生成信息的待发送消息。其中，该设定加密规则为系统内部加密标准中指定的，该设定加密规则可以为任何数据处理算法，例如为现有的加密算法、或者如本实施例所述的加密方法。可以理解的是，该设定部分信息的加密处理也可以在S202之前执行，在S202及之后的步骤中采用加密后的设定部分信息进行相应处理。

[56] S204: 通信设备发送所述新的待发送信息。

[57] 例如，通信设备通过空口将该新的待发送信息发射出去。

[58] 具体地，以下提供对三种不同的待发送信息对本实施例方法进行进一步举例说明。

[59] 1) 所述待发送信息为信令，所述设定部分信息为所述信令的校验数据，所述其他部分信息为所述信令的信令内容。该校验数据具体可为校验和、循环冗余校验码（英文简称：CRC）、奇偶校验位等。该信令内容为用于承载该信令需传递的信息的数据，例如为该信令中的控制数据、管理数据等。

[60] 具体如，当需要向其他通信终端发送信令如控制信令块时，通信设备按照无线通信标准生成原始的待发送的信令，然后使用信令中的校验数据作为初始向量，将系统内部加密标准指定的设定数据和该信令中信令内容代入至系统内部加密标准指定的加密公式中进行运算，并将运算结果作为新的信令内容，并将该新的信令内容和校验数据通过空口发送出去。

[61] 如图3所示，为该待发送信息为嵌入式链路帧的应用场景中的通信流程框图，通信设备生成信令内容和对应的第一校验数据如校验和，并经过前向纠错（英文：Forward Error Correction，简称：FEC）信道编码后，生成信令数据A，然后以信令数据A中第二校验数据如奇偶校验位作为初始向量，对信令数据A中除第二校验数据外的剩余部分数据按照设定加密算法和密钥进行加密，生成信令数据B，通过空口发射。

[62] 如图4所示，为该待发送信息为非嵌入式链路帧的应用场景中的通信流程框图，通信设备生成信令内容A和对应的校验数据如CRC，然后以校验数据作为初始向量，对信令内容A按照设定加密算法和密钥进行加密，生成信令内容B，将信令内容B和校验数据经过FEC信道编码后生成信令数据，通过空口发射。

- [63] 2) 所述待发送信息为语音呼叫信息, 所述设定部分信息为所述语音呼叫信息中的语音头帧和/或语音结束帧, 所述其他部分信息为所述语音呼叫信息中的语音帧。
- [64] 在如DMR/PDT等无线通信标准中, 一次语音呼叫信息包含语音头帧、语音帧和语音结束帧。通信设备可按照系统内部加密标准将所述语音头帧或/或语音结束帧作为该设定部分信息。
- [65] 具体如, 通信设备在进行语音呼叫时, 生成语音呼叫信息, 并使用语音呼叫信息中的语音头帧作为初始向量, 按照设定加密算法和密钥对语音帧进行加密, 从而生成新的语音帧, 通过空口将由该语音头帧、新的语音帧、语音结束帧组成的新的语音呼叫信息发送出去。
- [66] 3) 所述待发送信息为数据业务信息, 所述设定部分信息为所述数据业务信息的数据头帧和/或数据结束帧, 所述其他部分信息为所述数据业务信息的数据帧。
- [67] 在如DMR/PDT等无线通信标准中, 一次数据业务信息包含数据头帧和数据帧, 在有些数据业务信息中还包含数据结束帧。通信设备可按照系统内部加密标准将所述数据头帧和/或数据结束帧作为该设定部分信息。
- [68] 具体如, 通信设备在与其他通信设备进行数据业务时, 生成数据业务信息, 并使用数据业务信息中的数据头帧作为初始向量, 按照设定加密算法和密钥对数据帧进行加密, 从而生成新的数据帧, 通过空口将由该数据头帧、新的数据帧组成的新的数据业务信息发送出去。
- [69] 在其他实施例, 上述作为初始向量的语音头帧和/或语音结束帧、数据头帧和/或数据结束帧在作为初始向量之前, 可采用如上述信令实施例加密方法对其进行加密。
- [70] 本实施例中, 通信设备采用待发送信息设定部分信息作为初始向量对其他部分信息进行加密或解密处理, 故非法设备无法窃取到该无线通信系统内传输的信息, 从而保证了该无线通信的安全性, 另外, 由于通信设备直接利用待发送信息的部分信息作为初始向量进行加密, 无需额外初始向量, 故无需增加空口开销。

- [71] 请参阅图5，图5是本申请无线通信方法另一实施方式的流程图。该方法由无线通信系统中的通信设备执行，用于在接收到信息时对信息进行解密处理。具体，该方法包括：
- [72] S501：通信设备提取已接收信息中的设定部分信息。
- [73] 例如，通信设备在接收到其他通信设备发送的信息时，根据所在系统的内部加密标准，从在已接收信息中提取设定部分信息。
- [74] 如上一实施例所述，系统内部加密标准可设置该已接收信息的任一部分作为该设定部分信息，例如，该设定部分信息为该已接收信息中的校验数据和/或信令。可以理解的是，内部加密标准对该无线通信系统中的待发送数据和已接收信息的设定部分信息是相同的，以保证系统内部的通信信息可正确被解密。
- [75] S502：通信设备以所述设定部分信息作为初始向量，对所述已接收信息中的其他部分信息进行解密。
- [76] 例如，通信设备以提取的设定部分信息作为初始向量，按照设定解密公式和设定数据对所述已接收信息中的其他部分信息进行运算，将运算结果作为解密后的所述其他部分信息。该设定解密公式与该无线通信系统的上述设定加密公式是对应的，可为现有的解密算法，或者自定义的任意运算公式。通信设备根据该系统的内部加密标准可确定该设定解密公式和设定数据。其中，上述设定加密公式、设定解密公式、设定数据均存储在通信设备本地，并限制无法通过空口传输，以保证非法设备无法对该系统的信息进行正确加/解密。
- [77] 可以理解的是，该所述其他部分信息为该已接收信息中除该设定部分信息外的剩余信息的全部或部分信息。同样地，为保证系统内部的通信信息可正确被解密，内部加密标准对该无线通信系统中的待发送数据和已接收信息的该其他部分信息的设置是相同的。
- [78] 进一步地，在另一该设定部分信息被加密处理的实施例中，在该S502之前或之后，通信设备对所述设定部分信息按照设定解密规则进行解密处理，并在后续步骤中采用该解密后的设定部分信息进行相应处理。其中，该设定解密规则与上述设定加密规则对应，为系统内部加密标准中指定的。具体，当设定部分信息的加密在上述S202之前执行，则上述设定部分信息的解密在S502之后执行，

当设定部分信息的加密在上述S203之前执行，则上述设定部分信息的解密在S502之前执行。

[79] S503: 通信设备对由所述设定部分信息和解密后的所述其他部分信息组成的新的已接收信息进行处理。

[80] 本实施例中，该已接收信息的类型及其设定部分信息和其他部分信息的划分可对应为上述实施例所述的信令、语音呼叫信息、数据业务信息及其设定部分信息和其他部分信息的划分。

[81] 具体地，以下提供对三种不同的已接收信息对本实施例方法进行进一步举例说明。

[82] 1) 当该已接收信息为信令如控制信令块时，通信设备使用信令中的校验数据作为初始向量，将系统内部加密标准指定的设定数据和该信令中信令内容代入至系统内部加密标准指定的解密公式中进行运算，并将运算结果作为解密后的信令内容，并对由所述校验数据和解密后的所述信令内容组成的新的已接收信息进行处理，具体包括：由解密后的所述信令内容生成新校验数据；比较所述信令中的校验数据与所述新校验数据是否相同；若相同，则对由所述校验数据和解密后的所述信令内容生成新信令，并响应所述新信令；否则丢弃所述信令，也即对该信令不做响应。

[83] 如图6所示，为该已接收信息为嵌入式链路帧的应用场景中的通信流程框图，通信设备在收到一条嵌入式链路帧信令数据B时，先以信令数据B中的第二校验数据如奇偶校验位作为初始向量，对信令数据B的另一部分数据按照设定解密算法和密钥进行解密，得到信令数据A，对该信令数据A和第二校验数据进行FEC信道解码后，得到新的信令内容和第一校验数据如校验和，接着将新的信令内容按无线通信标准规定的校验和计算规则计算出校验和，当计算得到的校验和与接收到的信令中的校验和相同时，则表示信令内容是正确的，按无线通信标准对信令内容进行后续处理；否则表示信令内容是不合法的，直接丢弃。

[84] 如图7所示，为该已接收信息为非嵌入式链路帧的应用场景中的通信流程框图，通信设备在收到一条信令数据时，先对信令数据进行FEC信道解码，得到信令内容B和校验数据如CRC，然后以CRC作为初始向量，对信令内容B按照设定解

密算法和密钥进行解密，生成信令内容A，接着将信令内容A按无线通信标准规定的CRC计算规则计算出CRC，当计算得到的CRC与接收到的信令中CRC相同时，则表示信令内容A是正确的，按无线通信标准对信令内容A进行后续处理；否则表示信令内容A是不合法的，直接丢弃。

[85] 2) 当该已接收信息为语音呼叫信息时，通信设备可用该语音呼叫信息中的语音头帧作为初始向量，按照设定解密算法和密钥对该语音呼叫信息中的语音帧进行解密，得到原始的语音帧，然后进行后续处理，如将该语音帧进行播放。若该语音呼叫信息为非法设备发送的，则解密后的语音帧并非为非法设备原始发送的信息，故无法正确播放信息，例如会出现播放的是杂音。

[86] 3) 当该已接收信息为数据业务信息时，通信设备可用数据业务信息的数据头帧作为初始向量，按照设定解密算法和密钥对数据业务信息的数据帧进行解密，得到解密后的数据帧，然后对由所述设定部分信息和解密后的所述数据帧组成的新的已接收信息进行处理，具体包括：由解密后的所述数据帧生成新校验数据；比较所述解密后的数据帧中的校验数据与所述新校验数据是否相同；若相同，则对由所述设定部分信息和解密后的数据帧生成新数据业务信息，并响应所述新数据业务信息；否则丢弃所述数据业务信息，也即对该数据业务信息不做响应。

[87] 本实施例中，通信设备采用已接收信息的设定部分信息作为初始向量对其他部分信息进行解密处理，故非法设备发送的消息无法得到该无线通信系统的正确响应，从而保证了该无线通信的安全性，避免了非法设备的信息干扰。

[88] 请参阅图8，图8是本申请无线通信装置一实施方式的结构示意图。该无线通信装置80用于无线通信系统的通信终端具体包括提取模块81、加密模块82、生成模块83和发送模块84。

[89] 提取模块81用于提取待发送信息中的设定部分信息；

[90] 加密模块82用于以所述设定部分信息作为初始向量，对所述待发送信息中的其他部分信息进行加密；

[91] 生成模块83用于利用所述设定部分信息和加密后的所述其他部分信息生成新的待发送信息；

- [92] 发送模块84用于发送所述新的待发送信息。
- [93] 可选地，所述设定部分信息为所述待发送信息中的校验数据和/或信令，具体可如上述实施例所述。
- [94] 可选地，加密模块82还用于对所述设定部分信息按照设定规则进行加密处理。
- [95] 可选地，加密模块82具体用于以所述设定部分信息作为初始向量，按照设定加密公式和设定数据对所述待发送信息中的其他部分信息进行运算，将运算结果作为加密后的所述其他部分信息。
- [96] 请参阅图9，图9是本申请无线通信装置另一实施方式的结构示意图。该无线通信装置90用于无线通信系统中的通信设备，具体包括：提取模块91、解密模块92和处理模块93。
- [97] 提取模块91用于提取已接收信息中的设定部分信息；
- [98] 解密模块92用于以所述设定部分信息作为初始向量，对所述已接收信息中的其他部分信息进行解密；
- [99] 处理模块93用于对由所述设定部分信息和解密后的所述其他部分信息组成的新的已接收信息进行处理。
- [100] 可选地，所述设定部分信息为所述已接收信息中的校验数据和/或信令，具体可如上述方法实施例所述。
- [101] 可选地，处理模块83具体用于当所述已接收信息为信令时，由解密后的所述信令内容生成新校验数据；比较所述信令中的校验数据与所述新校验数据是否相同；若相同，则对由所述校验数据和解密后的所述信令内容生成新信令，并响应所述新信令；否则丢弃所述信令。
- [102] 可选地，处理模块93具体用于当所述已接收信息为数据业务信息时，由解密后的所述数据帧生成新校验数据；比较所述解密后的数据帧中的校验数据与所述新校验数据是否相同；若相同，则对解密后的新数据业务信息进行处理；否则丢弃所述数据业务信息。
- [103] 可选地，解密模块92还用于对所述设定部分信息按照设定解密规则进行解密处理。
- [104] 可选地，解密模块92具体用于以所述设定部分信息作为初始向量，按照设定解

密公式和设定数据对所述待发送信息中的其他部分信息进行运算，将运算结果作为解密后的所述其他部分信息。

[105] 上述装置的模块可对应用于执行上述方法实施例中的步骤，具体说明请参阅上述方法实施例的描述。

[106] 可以理解的是，图8和图9所示实施例中的无线通信装置可设置在同一通信设备中。

[107] 参阅图10，图10是本申请通信设备一实施方式的结构示意图。本实施方式的通信设备100，包括发送器101、接收器102、处理器103、存储器104以及总线105。

[108] 发送器101用于向外部设备如无线通信系统中的其他通信设备发送消息。

[109] 接收器102用于接收外部设备如无线通信系统中的其他通信设备发送的消息。

[110] 存储器104用于存储被配置为被所述处理器103执行的计算机指令以及在处理器103工作过程中所需保存或缓存的数据。

[111] 在本实施例中，处理器103通过调用存储器104存储的计算机指令，用于执行以下两方面的至少一个：

[112] 第一方面：对待发送数据的加密处理；

[113] 提取待发送信息中的设定部分信息；

[114] 以所述设定部分信息作为初始向量，对所述待发送信息中的其他部分信息进行加密；

[115] 利用所述设定部分信息和加密后的所述其他部分信息生成新的待发送信息；

[116] 通过发送器101发送所述新的待发送信息。

[117] 可选地，所述设定部分信息为所述待发送信息中的校验数据和/或信令，具体可如上述实施例所述。

[118] 可选地，处理器103还用于对所述设定部分信息按照设定规则进行加密处理。

[119] 可选地，处理器103具体用于以所述设定部分信息作为初始向量，按照设定加密公式和设定数据对所述待发送信息中的其他部分信息进行运算，将运算结果作为加密后的所述其他部分信息。

[120] 第二方面：对已接收数据的解密处理；

- [121] 提取接收器102接收到的已接收信息中的设定部分信息；
- [122] 以所述设定部分信息作为初始向量，对所述已接收信息中的其他部分信息进行解密；
- [123] 对由所述设定部分信息和解密后的所述其他部分信息组成的新的已接收信息进行处理。
- [124] 可选地，所述设定部分信息为所述已接收信息中的校验数据和/或信令，具体可如上述方法实施例所述。
- [125] 可选地，处理器103具体用于当所述已接收信息为信令时，由解密后的所述信令内容生成新校验数据；比较所述信令中的校验数据与所述新校验数据是否相同；若相同，则对由所述校验数据和解密后的所述信令内容生成新信令，并响应所述新信令；否则丢弃所述信令。
- [126] 可选地，处理器103具体用于当所述已接收信息为数据业务信息时，由解密后的所述数据帧生成新校验数据；比较所述解密后的数据帧中的校验数据与所述新校验数据是否相同；若相同，则对解密后的新数据业务信息进行处理；否则丢弃所述数据业务信息。
- [127] 可选地，处理器103还用于对所述设定部分信息按照设定解密规则进行解密处理。
- [128] 可选地，处理器103具体用于以所述设定部分信息作为初始向量，按照设定解密公式和设定数据对所述待发送信息中的其他部分信息进行运算，将运算结果作为解密后的所述其他部分信息。
- [129] 可以理解的是，在不同实施例中，该处理器103可仅用于执行第一方面或第二方面，或可用于执行以上两方面。
- [130] 上述处理器103还可以称为CPU（Central Processing Unit，中央处理单元）。存储器104可以包括只读存储器和随机存取存储器，并向处理器103提供指令和数据。存储器104的一部分还可以包括非易失性随机存取存储器（NVRAM）。具体的应用中，移动终端的上述各个组件通过总线105耦合在一起，其中总线105除包括数据总线之外，还可以包括电源总线、控制总线和状态信号总线等。但是为了清楚说明起见，在图中将各种总线都标为总线105。

[131] 上述本发明实施例揭示的方法可以应用于处理器103中，或者由处理器103实现。处理器103可能是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法的各步骤可以通过处理器103中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器103可以是通用处理器、数字信号处理器（DSP）、专用集成电路（ASIC）、现成可编程门阵列（FPGA）或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本发明实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本发明实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器104，处理器103读取存储器104中的信息，结合其硬件完成上述方法的步骤。

[132] 采用上述方案可实现以下有益效果：

[133] 1、非法设备无法窃取该无线通信系统内传输的信息，提高了专网通信的信息安全，确保通信的安全性。

[134] 无线通信系统内的通信设备对该通信信息进行上述加密后，非法设备由于无法获知其解密规则，故即使获取到该无线通信系统内的通信信息，也无法正确解密进而无法窃取到该无线通信系统内传输的信息，非法设备无法窃取该无线通信系统内传输的信息，提高了专网通信的信息安全，确保通信的安全性。

[135] 2、避免了非法设备的信息干扰，确保信息的可靠性。

[136] 非法设备由于无法获知其加密规则，故无法将信息正确加密，无线通信系统内的通信设备即使接收到该非法设备发送的信息，经解密后则可发现其信息非法发送或者无法还原成非法设备发送的信息，故避免了非法设备的信息干扰，确保信息的可靠性。

[137] 3、限制非法设备使用该无线通信系统资源，确保系统安全性。

[138] 如2所述，非法设备发送的信息会被无线通信系统中的设备发现，故不做响应，如无线通信系统的中转台接收到该非法设备的信息后则丢弃不再转发，故限

制非法设备使用该无线通信系统资源，确保系统安全性。

[139] 4、不增加任何的空口开销。

[140] 由于通信设备直接利用待发送信息的部分信息作为初始向量进行加密，无需额外初始向量，故无需增加空口开销。

[141] 在本申请所提供的几个实施方式中，应该理解到，所揭露的系统，装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施方式仅仅是示意性的，例如，所述模块或单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

[142] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施方式方案的目的。

[143] 另外，在本申请各个实施方式中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

[144] 所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）或处理器（processor）执行本申请各个实施方式所述方法的全部或部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器（ROM，Read-Only Memory）、随机存取存储器（RAM，Random Access Memory）、磁碟或者光盘等各种可以存储程序代码的介质。

权利要求书

- [权利要求 1] 一种无线通信方法，其特征在于，包括：
- 通信设备提取待发送信息中的设定部分信息；
- 以所述设定部分信息作为初始向量，对所述待发送信息中的其他部分信息进行加密；
- 利用所述设定部分信息和加密后的所述其他部分信息生成新的待发送信息；
- 发送所述新的待发送信息。
- [权利要求 2] 如权利要求1所述的无线通信方法，其特征在于，所述设定部分信息为所述待发送信息中的校验数据和/或信令。
- [权利要求 3] 如权利要求2所述的无线通信方法，其特征在于，
- 所述待发送信息为信令，所述设定部分信息为所述信令的校验数据，所述其他部分信息为所述信令的信令内容；或
- 所述待发送信息为语音呼叫信息，所述设定部分信息为所述语音呼叫信息中的语音头帧和/或语音结束帧，所述其他部分信息为所述语音呼叫信息中的语音帧；或
- 所述待发送信息为数据业务信息，所述设定部分信息为所述数据业务信息的数据头帧和/或数据结束帧，所述其他部分信息为所述数据业务信息的数据帧。
- [权利要求 4] 如权利要求1所述的无线通信方法，其特征在于，在所述利用所述设定部分信息和加密后的所述其他部分信息生成新的待发送信息之前，还包括：
- 对所述设定部分信息按照设定加密规则进行加密处理。
- [权利要求 5] 如权利要求1所述的无线通信方法，其特征在于，所述以所述设定部分信息作为初始向量，对所述待发送信息中的其他部分信息进行加密，包括：
- 以所述设定部分信息作为初始向量，按照设定加密公式和设定数据对所述待发送信息中的其他部分信息进行运算，将运算结果作

为加密后的所述其他部分信息。

[权利要求 6]

一种无线通信方法，其特征在于，包括：

通信设备提取已接收信息中的设定部分信息；

以所述设定部分信息作为初始向量，对所述已接收信息中的其他部分信息进行解密；

对由所述设定部分信息和解密后的所述其他部分信息组成的新的已接收信息进行处理。

[权利要求 7]

如权利要求6所述的无线通信方法，其特征在于，所述设定部分信息为所述已接收信息中的校验数据和/或信令。

[权利要求 8]

如权利要求7所述的无线通信方法，其特征在于，所述已接收信息为信令，所述设定部分信息为所述信令的校验数据，所述其他部分信息为所述信令的信令内容；

所述对由所述设定部分信息和解密后的所述其他部分信息组成的新的已接收信息进行处理，包括：

由解密后的所述信令内容生成新校验数据；

比较所述信令中的校验数据与所述新校验数据是否相同；

若相同，则对由所述校验数据和解密后的所述信令内容生成新信令，并响应所述新信令；否则丢弃所述信令。

[权利要求 9]

如权利要求7所述的无线通信方法，其特征在于，所述已接收信息为语音呼叫信息，所述设定部分信息为所述语音呼叫信息中的语音头帧和/或语音结束帧，所述其他部分信息为所述语音呼叫信息中的语音帧。

[权利要求 10]

如权利要求7所述的无线通信方法，其特征在于，所述已接收信息为数据业务信息，所述设定部分信息为所述数据业务信息的数据头帧和/或数据结束帧，所述其他部分信息为所述数据业务信息的数据帧；

所述对由所述设定部分信息和解密后的所述其他部分信息组成的新的已接收信息进行处理，包括：

由解密后的所述数据帧生成新校验数据；
比较所述解密后的数据帧中的校验数据与所述新校验数据是否相同；
若相同，则对解密后的新数据业务信息进行处理；否则丢弃所述数据业务信息。

[权利要求 11] 如权利要求6所述的无线通信方法，其特征在于，在所述以所述设定部分信息作为初始向量，对所述已接收信息中的其他部分信息进行解密之前，还包括：

对所述设定部分信息按照设定解密规则进行解密处理。

[权利要求 12] 如权利要求6所述的无线通信方法，其特征在于，所述以所述设定部分信息作为初始向量，对所述已接收信息中的其他部分信息进行解密，包括：

以所述设定部分信息作为初始向量，按照设定解密公式和设定数据对所述待发送信息中的其他部分信息进行运算，将运算结果作为解密后的所述其他部分信息。

[权利要求 13] 一种无线通信装置，其特征在于，包括：

提取模块，用于提取待发送信息中的设定部分信息；

加密模块，用于以所述设定部分信息作为初始向量，对所述待发送信息中的其他部分信息进行加密；

生成模块，用于利用所述设定部分信息和加密后的所述其他部分信息生成新的待发送信息；

发送模块，用于发送所述新的待发送信息。

[权利要求 14] 一种无线通信装置，其特征在于，包括：

提取模块，用于提取已接收信息中的设定部分信息；

解密模块，用于以所述设定部分信息作为初始向量，对所述已接收信息中的其他部分信息进行解密；

处理模块，用于对由所述设定部分信息和解密后的所述其他部分信息组成的新的已接收信息进行处理。

- [权利要求 15] 一种通信设备，其特征在于，包括发送器、存储器及处理器；
所述存储器用于存储被配置为被所述处理器执行的计算机指令；
所述处理器执行所述计算机指令，用于：
提取待发送信息中的设定部分信息；
以所述设定部分信息作为初始向量，对所述待发送信息中的其他部分信息进行加密；
利用所述设定部分信息和加密后的所述其他部分信息生成新的待发送信息；
通过所述发送器发送所述新的待发送信息。
- [权利要求 16] 如权利要求15所述的通信设备，其特征在于，
所述待发送信息为信令，所述设定部分信息为所述信令的校验数据，所述其他部分信息为所述信令的信令内容；或
所述待发送信息为语音呼叫信息，所述设定部分信息为所述语音呼叫信息中的语音头帧和/或语音结束帧，所述其他部分信息为所述语音呼叫信息中的语音帧；或
所述待发送信息为数据业务信息，所述设定部分信息为所述数据业务信息的数据头帧和/或数据结束帧，所述其他部分信息为所述数据业务信息的数据帧。
- [权利要求 17] 如权利要求15所述的通信设备，其特征在于，
所述处理器还用于对所述设定部分信息按照设定加密规则进行加密处理。
- [权利要求 18] 一种通信设备，其特征在于，包括接收器、存储器及处理器；
所述存储器用于存储被配置为被所述处理器执行的计算机指令；
所述处理器执行所述计算机指令，用于：
提取所述接收器接收到的已接收信息中的设定部分信息；
以所述设定部分信息作为初始向量，对所述已接收信息中的其他部分信息进行解密；
对由所述设定部分信息和解密后的所述其他部分信息组成的新的

已接收信息进行处理。

[权利要求 19]

如权利要求18所述的通信设备，其特征在于，

所述已接收信息为信令，所述设定部分信息为所述信令的校验数据，所述其他部分信息为所述信令的信令内容；或

所述已接收信息为语音呼叫信息，所述设定部分信息为所述语音呼叫信息中的语音头帧和/或语音结束帧，所述其他部分信息为所述语音呼叫信息中的语音帧；或

所述已接收信息为数据业务信息，所述设定部分信息为所述数据业务信息的数据头帧和/或数据结束帧，所述其他部分信息为所述数据业务信息的数据帧。

[权利要求 20]

如权利要求18所述的通信设备，其特征在于，

所述处理器还用于对所述设定部分信息按照设定解密规则进行解密处理。

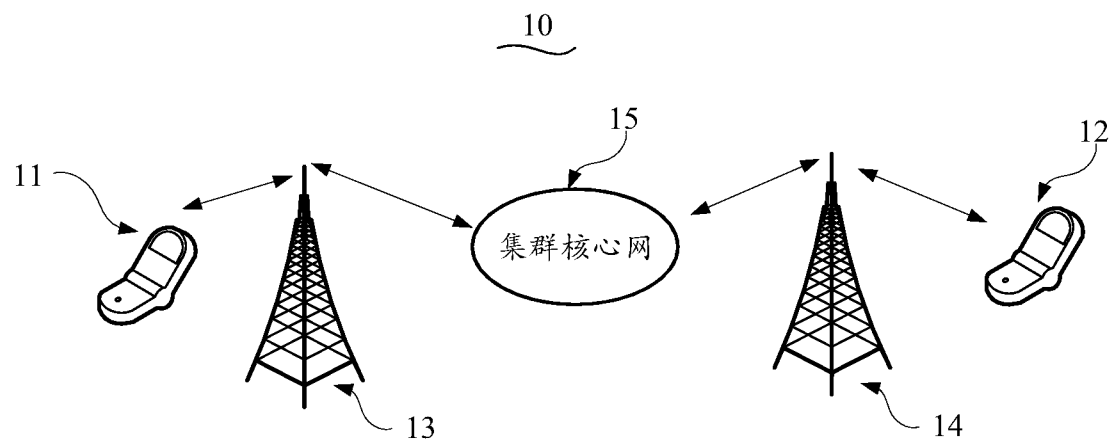


图1

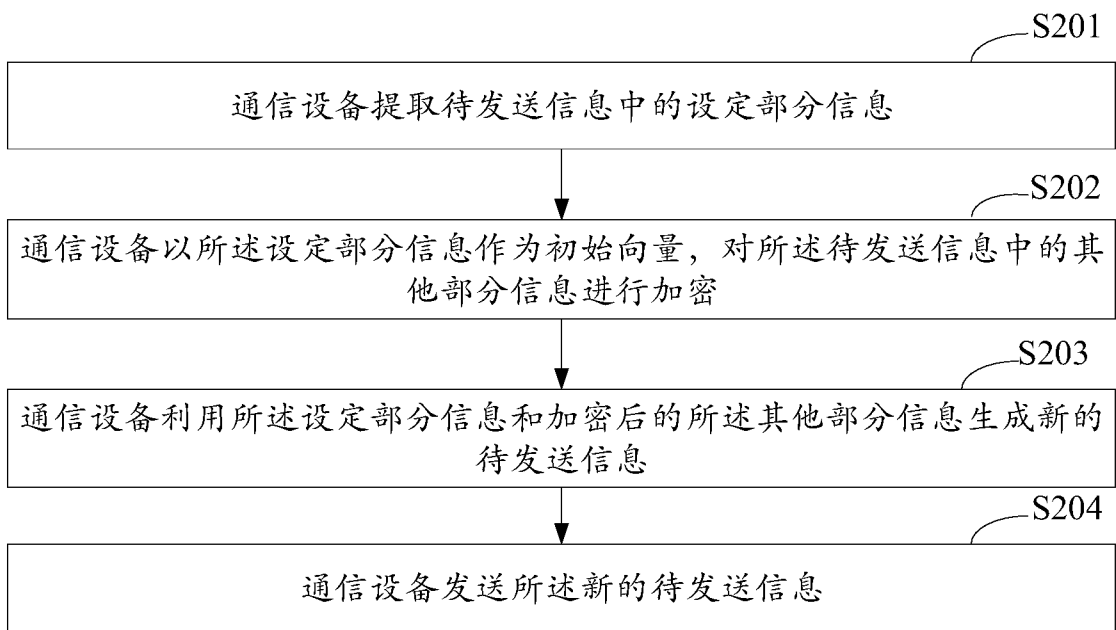


图2

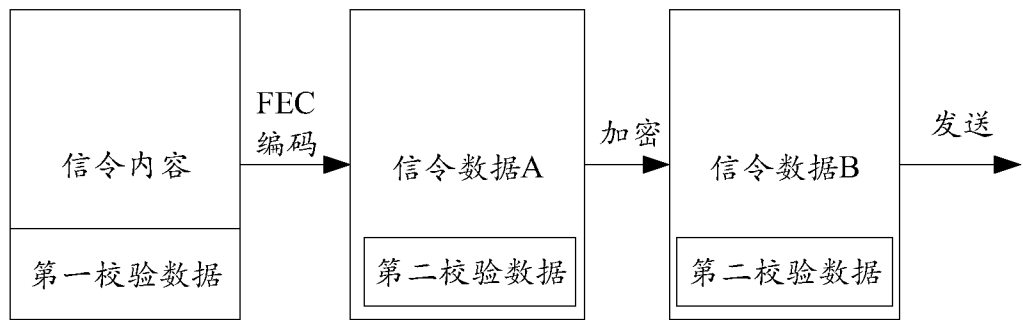


图3

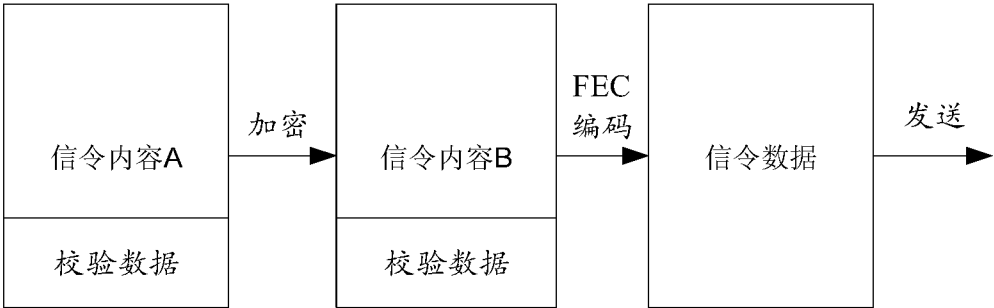


图4

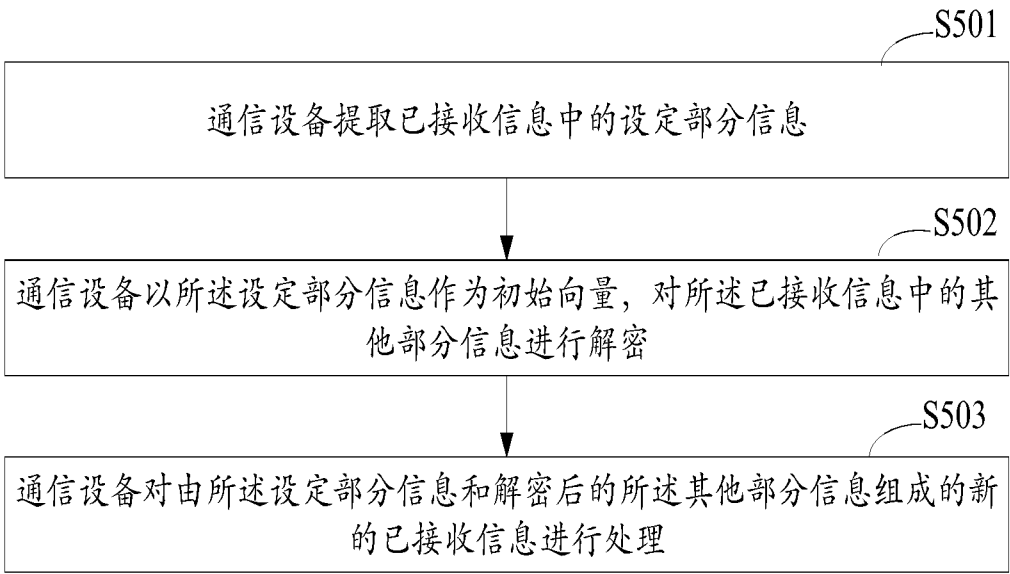


图5

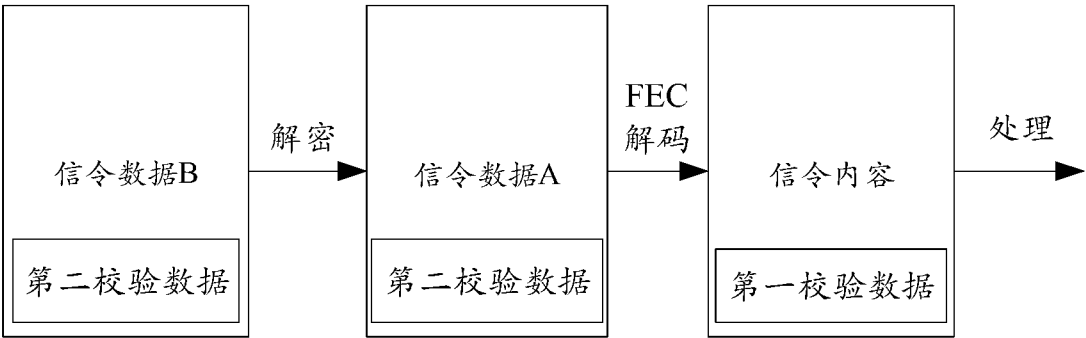


图6

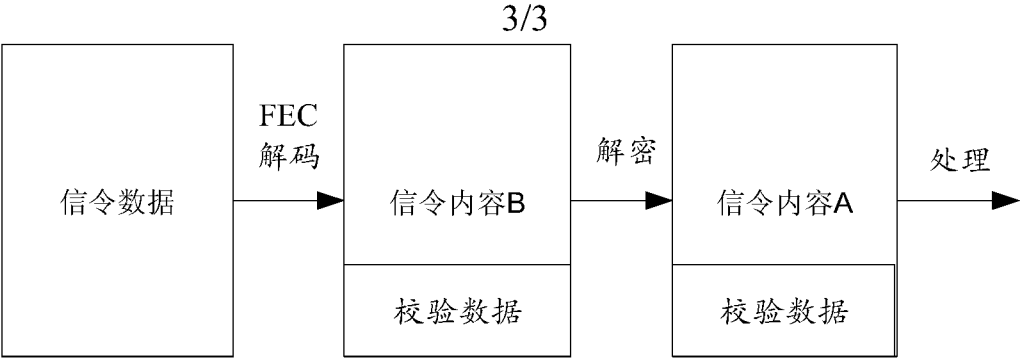


图7

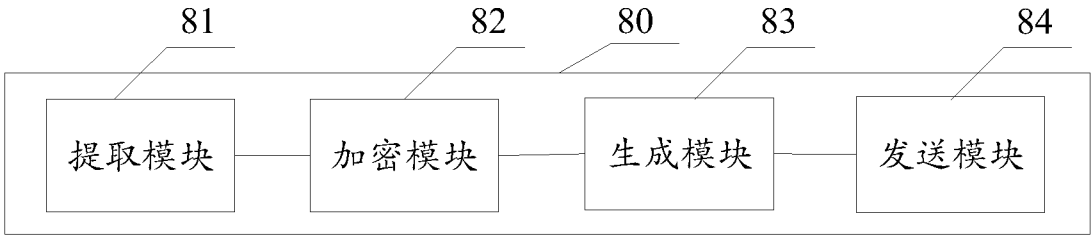


图8

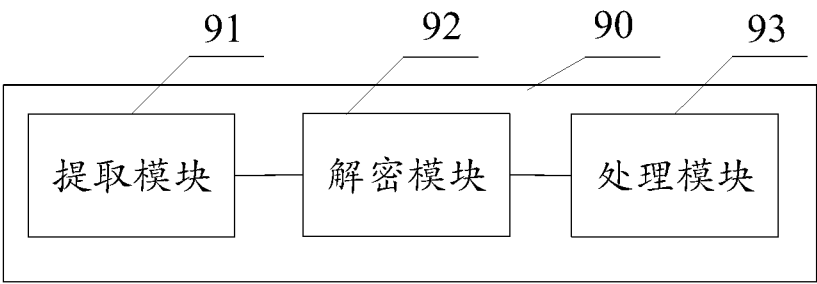


图9

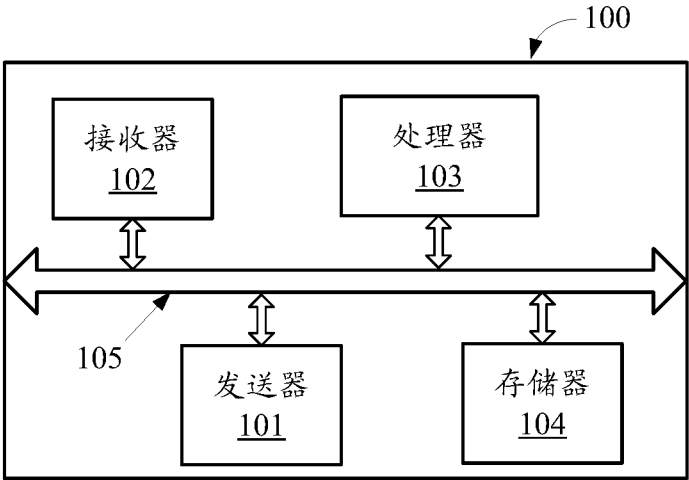


图10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/106451

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/00 (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

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)

CNABS, CNTXT, CNKI, VEN: 初始向量, 初始化向量, 加密, 校验, 控制, 发送, 帧, initializ+ vector, encrypt???, verificat???, control+, transmit+, frame

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 102144370 A (FUJITSU LIMITED), 03 August 2011 (03.08.2011), description, paragraphs [0012]-[0013] and [0038]-[0054]	1-20
Y	WO 2007059558 A1 (UNIV SYDNEY et al.), 31 May 2007 (31.05.2007), claims 1-20	1-20
Y	CN 101542961 A (INTELLON CORPORATION), 23 September 2009 (23.09.2009), claims 1-2 and 5-6	1-20
A	CN 102136904 A (INSTITUTE OF SOFTWARE, CHINESE ACADEMY OF SCIENCES), 27 July 2011 (27.07.2011), entire document	1-20

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search 03 March 2017	Date of mailing of the international search report 20 March 2017
Name and mailing address of the ISA 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 LI, Fan Telephone No. (86-10) 62089572

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/106451

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102144370 A	03 August 2011	CN 102144370 B WO 2010026637 A1 JP 5338816 B2 US 2011138173 A1 US 8538021 B2 JP 5423916 B2 JP 2013102547 A	15 April 2015 11 March 2010 13 November 2013 09 June 2011 17 September 2013 19 February 2014 23 May 2013
WO 2007059558 A1	31 May 2007	None	
CN 101542961 A	23 September 2009	KR 20080040732 A MX 2008001252 A CA 2616855 A1 JP 2009504023 A WO 2007086934 A3 EP 1922635 A2 JP 4981802 B2 US 2007112972 A1 US 7684568 B2 CN 101542961 B CA 2616855 C WO 2007086934 A2 AU 2006336351 A1 BRPI 0614124 A2	08 May 2008 01 March 2008 02 August 2007 29 January 2009 30 April 2009 21 May 2008 25 July 2012 17 May 2007 23 March 2010 10 October 2012 24 February 2015 02 August 2007 20 March 2008 09 March 2011
CN 102136904 A	27 July 2011	None	

国际检索报告

国际申请号

PCT/CN2016/106451

A. 主题的分类

H04L 9/00(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

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))

CNABS, CNTXT, CNKI, VEN:初始向量, 初始化向量, 加密, 校验, 控制, 发送, 帧, initializ+ vector, encrypt???, verificat???, control+, transmit+, frame

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 102144370 A (富士通株式会社) 2011年 8月 3日 (2011 - 08 - 03) 说明书第[0012]-[0013]、[0038]-[0054]段	1-20
Y	WO 2007059558 A1 (UNIV SYDNEY等) 2007年 5月 31日 (2007 - 05 - 31) 权利要求1-20	1-20
Y	CN 101542961 A (因特隆公司) 2009年 9月 23日 (2009 - 09 - 23) 权利要求1-2、5-6	1-20
A	CN 102136904 A (中国科学院软件研究所) 2011年 7月 27日 (2011 - 07 - 27) 全文	1-20

☐ 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

2017年 3月 3日

国际检索报告邮寄日期

2017年 3月 20日

ISA/CN的名称和邮寄地址

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

传真号 (86-10)62019451

受权官员

李凡

电话号码 (86-10)62089572

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/106451

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	102144370	A	2011年 8月 3日	CN	102144370	B	2015年 4月 15日
				WO	2010026637	A1	2010年 3月 11日
				JP	5338816	B2	2013年 11月 13日
				US	2011138173	A1	2011年 6月 9日
				US	8538021	B2	2013年 9月 17日
				JP	5423916	B2	2014年 2月 19日
				JP	2013102547	A	2013年 5月 23日
WO	2007059558	A1	2007年 5月 31日	无			
CN	101542961	A	2009年 9月 23日	KR	20080040732	A	2008年 5月 8日
				MX	2008001252	A	2008年 3月 1日
				CA	2616855	A1	2007年 8月 2日
				JP	2009504023	A	2009年 1月 29日
				WO	2007086934	A3	2009年 4月 30日
				EP	1922635	A2	2008年 5月 21日
				JP	4981802	B2	2012年 7月 25日
				US	2007112972	A1	2007年 5月 17日
				US	7684568	B2	2010年 3月 23日
				CN	101542961	B	2012年 10月 10日
				CA	2616855	C	2015年 2月 24日
				WO	2007086934	A2	2007年 8月 2日
				AU	2006336351	A1	2008年 3月 20日
				BRPI	0614124	A2	2011年 3月 9日
CN	102136904	A	2011年 7月 27日	无			

表 PCT/ISA/210 (同族专利附件) (2009年7月)