(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102938696 B
(45)授权公告日 2015.08.12

(21)申请号 201110232769.2

(22)申请日 2011.08.15

(73)专利权人 国民技术股份有限公司
地址 518057 广东省深圳市南山区高新技术产业园区深圳软件园 3 栋 301、302

(72)发明人 杨贤伟

(74)专利代理机构 北京轻创知识产权代理有限公司 11212
代理人 杨立

(51)Int.Cl.
H04L 9/08(2006.01)

(56)对比文件
US 2010153727 A1,2010.06.17, 说明书第[0023]-[0025],[0032]-[0033]段、图 1.
CN 101222320 A,2008.07.16, 全文 .
CN 101847199 A,2010.09.29, 全文 .
中国石油化工股份有限公司等编著 . 密钥分散算法 .《中国石化加油集成电路 IC 卡应用规范 V1.0》. 中国石化出版社 ,2001,165-178.

审查员 楼芃雯

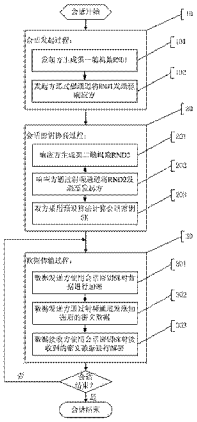
权利要求书2页 说明书8页 附图5页

(54)发明名称

一种会话密钥的生成方法及模块

(57)摘要

本发明涉及一种会话密钥的生成方法及模块。其中,会话密钥的生成方法包括:生成第一随机数;通过磁通道发送会话请求消息,该会话请求消息携带所述第一随机数;通过射频通道接收响应消息,所述响应消息携带第二随机数;根据所述第一随机数和所述第二随机数生成会话密钥。本发明的会话密钥的生成方法及模块,利用磁通道和射频通道共同完成射频会话密钥协商,充分利用了磁通道的近距离传输特性,使得射频通道在数据安全性上等同于近距离磁通道的安全性,提高了会话密钥的安全性,从而提高了使用该会话密钥的通讯过程的安全性。



CN 102938696 B

1. 一种会话密钥的生成方法，其特征在于，包括：

生成第一随机数；

通过磁通道发送会话请求消息，该会话请求消息携带所述第一随机数；

通过射频通道接收响应消息，所述响应消息携带第二随机数；

根据所述第一随机数和所述第二随机数生成会话密钥；

根据所述第一随机数和所述第二随机数生成会话密钥，包括：

以所述第一随机数和/或基于所述第一随机数的变换得到的值为主密钥，以所述第二随机数和/或基于所述第二随机数的变换而得到的值为分散参数，按照设定的密钥分散算法对所述主密钥和分散参数进行密钥分散，得到所述会话密钥。

2. 根据权利要求 1 所述的会话密钥的生成方法，其特征在于：

所述设定的密钥分散算法为：以长度为 16 字节的主密钥为加密密钥，以长度为 8 字节的分散参数为被加密明文，进行三重数据加密标准 3DES 加密运算，将得到的 8 字节密文作为长度为 16 字节的会话密钥的前半部分；以所述长度为 16 字节的主密钥为加密密钥，以所述长度为 8 字节的分散参数的按位取反为被加密明文，进行三重数据加密标准 3DES 加密运算，将得到的 8 字节密文作为所述长度为 16 字节的会话密钥的后半部分。

3. 根据权利要求 2 所述的会话密钥的生成方法，其特征在于：

所述长度为 16 字节的主密钥通过如下方式得到：取长度为 14 字节的第一随机数序列，在每 7 比特数据后插入 1 比特对该 7 比特数据的奇校验位或偶校验位，得到所述长度为 16 字节的主密钥。

4. 根据权利要求 2 所述的会话密钥的生成方法，其特征在于：

所述长度为 8 字节的分散参数通过如下方式得到：直接取长度为 8 字节的第二随机数作为分散参数。

5. 根据权利要求 1 所述的会话密钥的生成方法，其特征在于：

所述第一随机数的长度大于或等于 2 字节，且小于或等于 14 字节。

6. 一种会话密钥的生成模块，其特征在于，包括：

第一生成单元，用于生成第一随机数；

第一发送单元，用于通过磁通道发送会话请求消息，该会话请求消息携带所述第一随机数；

第一接收单元，用于通过射频通道接收响应消息，所述响应消息携带第二随机数；

密钥生成单元，用于根据所述第一随机数和所述第二随机数生成会话密钥。

7. 根据权利要求 6 所述的会话密钥的生成模块，其特征在于：

所述密钥生成单元包括第一密钥生成子单元，用于以所述第一随机数和/或基于所述第一随机数的变换得到的值为主密钥；第二密钥生成子单元，用于以所述第二随机数和/或基于所述第二随机数的变换而得到的值为分散参数；第三密钥生成子单元，用于按照设定的密钥分散算法对所述主密钥和分散参数进行密钥分散，得到所述会话密钥。

8. 根据权利要求 7 所述的会话密钥的生成模块，其特征在于：

所述第三密钥生成子单元包括第一密钥分散算法子单元，用于以长度为 16 字节的主密钥为加密密钥，以长度为 8 字节的分散参数为被加密明文，进行三重数据加密标准 3DES 加密运算，将得到的 8 字节密文作为长度为 16 字节的会话密钥的前半部分；第二密钥分散

算法子单元，用于以所述长度为 16 字节的主密钥为加密密钥，以所述长度为 8 字节的分散参数的按位取反为被加密明文，进行三重数据加密标准 3DES 加密运算，将得到的 8 字节密文作为所述长度为 16 字节的会话密钥的后半部分。

9. 根据权利要求 8 所述的会话密钥的生成模块，其特征在于：

所述第一密钥生成子单元包括主密钥获取子单元，用于取长度为 14 字节的第一随机数序列，在每 7 比特数据后插入 1 比特对该 7 比特数据的奇校验位或偶校验位，得到所述长度为 16 字节的主密钥。

10. 根据权利要求 8 所述的会话密钥的生成模块，其特征在于：

所述第二密钥生成子单元包括分散参数获取子单元，用于直接取长度为 8 字节的第二随机数作为分散参数。

11. 根据权利要求 6 所述的会话密钥的生成模块，其特征在于：

所述第一随机数的长度大于或等于 2 字节，且小于或等于 14 字节。

12. 一种会话密钥的生成方法，其特征在于，包括：

通过磁通道接收会话请求消息，所述会话请求消息携带第一随机数；

生成第二随机数；

通过射频通道发送响应消息，该响应消息携带所述第二随机数；

根据所述第一随机数和所述第二随机数生成会话密钥。

13. 一种会话密钥的生成模块，其特征在于，包括：

第二接收单元，用于通过磁通道接收会话请求消息，所述会话请求消息携带第一随机数；

第二生成单元，用于生成第二随机数；

第二发送单元，用于通过射频通道发送响应消息，该响应消息携带所述第二随机数；

密钥生成单元，用于根据所述第一随机数和所述第二随机数生成会话密钥。

一种会话密钥的生成方法及模块

技术领域

[0001] 本发明涉及无线通讯领域，尤其涉及一种会话密钥的生成方法及模块。

背景技术

[0002] 随着电子支付技术的发展，支付手段的电子化和移动化是不可避免的必然趋势。移动支付将移动终端的便携性和电子支付的自主性相结合，庞大的移动用户数量为移动支付的发展提供了良好的基础，可见移动支付所蕴藏的市场潜力巨大。

[0003] 目前各种无线射频（Radio Frequency，RF）通讯应用十分广泛，尤其是 2.4GHz 作为全球通用的 ISM（Industrial Scientific Medical，工业科学医学）频段，在无线局域网 WLAN、蓝牙、ZigBee 等无线通讯方面有着广泛的应用。由带磁通道的 2.4GHz 射频智能卡及其读卡器所组成的近距离射频通讯系统属于一种典型的移动支付应用系统。由带磁通道的 2.4G 射频智能卡及其读卡器所组成的近距离射频通讯系统采用磁通道进行距离控制，采用射频通道完成交易过程。2.4GHz 的频段具有传输速率高和传输距离较远的优势，但也正因为其通讯数据传输距离较远，使得通过 2.4GHz 频段传输的数据很容易在空中被非法截获和利用，从而给通讯带来一定的安全隐患。

发明内容

[0004] 本发明所要解决的技术问题是提供一种会话密钥的生成方法及模块，能够获得安全性更高的会话密钥，从而提高使用该会话密钥的通讯过程的安全性。

[0005] 为解决上述技术问题，本发明提出了一种会话密钥的生成方法，包括：

[0006] 生成第一随机数；

[0007] 通过磁通道发送会话请求消息，该会话请求消息携带所述第一随机数；

[0008] 通过射频通道接收响应消息，所述响应消息携带第二随机数；

[0009] 根据所述第一随机数和所述第二随机数生成会话密钥。

[0010] 进一步地，上述方法还可具有以下特点，根据所述第一随机数和所述第二随机数生成会话密钥，包括：

[0011] 以所述第一随机数和 / 或基于所述第一随机数的变换得到的值为主密钥，以所述第二随机数和 / 或基于所述第二随机数的变换而得到的值为分散参数，按照设定的密钥分散算法对所述主密钥和分散参数进行密钥分散，得到所述会话密钥。

[0012] 进一步地，上述方法还可具有以下特点，所述设定的密钥分散算法为：以长度为 16 字节的主密钥为加密密钥，以长度为 8 字节的分散参数为被加密明文，进行三重数据加密标准 3DES 加密运算，将得到的 8 字节密文作为长度为 16 字节的会话密钥的前半部分；以所述长度为 16 字节的主密钥为加密密钥，以所述长度为 8 字节的分散参数的按位取反为被加密明文，进行三重数据加密标准 3DES 加密运算，将得到的 8 字节密文作为所述长度为 16 字节的会话密钥的后半部分。

[0013] 进一步地，上述方法还可具有以下特点，所述长度为 16 字节的主密钥通过如下

方式得到：取长度为 14 字节的第一随机数序列，在每 7 比特数据后插入 1 比特对该 7 比特数据的奇校验位或偶校验位，得到所述长度为 16 字节的主密钥。

[0014] 进一步地，上述方法还可具有以下特点，所述长度为8字节的分散参数通过如下方式得到：直接取长度为 8 字节的第二随机数作为分散参数。

[0015] 进一步地，上述方法还可具有以下特点，所述第一随机数的长度大于或等于 2 字节，且小于或等于 14 字节。

[0016] 为解决上述技术问题，本发明还提出了一种会话密钥的生成模块，包括：

[0017] 第一生成单元，用于生成第一随机数；

[0018] 第一发送单元，用于通过磁通道发送会话请求消息，该会话请求消息携带所述第一随机数；

[0019] 第一接收单元，用于通过射频通道接收响应消息，所述响应消息携带第二随机数；

[0020] 密钥生成单元，用于根据所述第一随机数和所述第二随机数生成会话密钥。

[0021] 进一步地，上述模块还可具有以下特点，所述密钥生成单元包括第一密钥生成子单元，用于以所述第一随机数和 / 或基于所述第一随机数的变换得到的值为主密钥；第二密钥生成子单元，用于以所述第二随机数和 / 或基于所述第二随机数的变换而得到的值为分散参数；第三密钥生成子单元，用于按照设定的密钥分散算法对所述主密钥和分散参数进行密钥分散，得到所述会话密钥。

[0022] 进一步地，上述模块还可具有以下特点，所述第三密钥生成子单元包括第一密钥分散算法子单元，用于以长度为 16 字节的主密钥为加密密钥，以长度为 8 字节的分散参数为被加密明文，进行三重数据加密标准 3DES 加密运算，将得到的 8 字节密文作为长度为 16 字节的会话密钥的前半部分；第二密钥分散算法子单元，用于以所述长度为 16 字节的主密钥为加密密钥，以所述长度为 8 字节的分散参数的按位取反为被加密明文，进行三重数据加密标准 3DES 加密运算，将得到的 8 字节密文作为所述长度为 16 字节的会话密钥的后半部分。

[0023] 进一步地，上述模块还可具有以下特点，所述第一密钥生成子单元包括主密钥获取子单元，用于取长度为 14 字节的第一随机数序列，在每 7 比特数据后插入 1 比特对该 7 比特数据的奇校验位或偶校验位，得到所述长度为 16 字节的主密钥。

[0024] 进一步地，上述模块还可具有以下特点，所述第二密钥生成子单元包括分散参数获取子单元，用于直接取长度为 8 字节的第二随机数作为分散参数。

[0025] 进一步地，上述模块还可具有以下特点，所述第一随机数的长度大于或等于 2 字节，且小于或等于 14 字节。

[0026] 为解决上述技术问题，本发明还提出了一种会话密钥的生成方法，包括：

[0027] 通过磁通道接收会话请求消息，所述会话请求消息携带第一随机数；

[0028] 生成第二随机数；

[0029] 通过射频通道发送响应消息，该响应消息携带所述第二随机数；

[0030] 根据所述第一随机数和所述第二随机数生成会话密钥。

[0031] 为解决上述技术问题，本发明还提出了一种会话密钥的生成模块，包括：

[0032] 第二接收单元，用于通过磁通道接收会话请求消息，所述会话请求消息携带第一

随机数；

[0033] 第二生成单元，用于生成第二随机数；

[0034] 第二发送单元，用于通过射频通道发送响应消息，该响应消息携带所述第二随机数；

[0035] 密钥生成单元，用于根据所述第一随机数和所述第二随机数生成会话密钥。

[0036] 本发明的会话密钥的生成方法及模块，利用磁通道和射频通道共同完成射频会话密钥协商，充分利用了磁通道的近距离传输特性，使得射频通道在数据安全性上等同于近距离磁通道的安全性，提高了会话密钥的安全性，从而提高了使用该会话密钥的通讯过程的安全性。

附图说明

[0037] 图 1 为本发明实施例中会话密钥的生成方法的一种流程图；

[0038] 图 2 为本发明实施例中会话密钥的生成模块的一种结构图；

[0039] 图 3 为本发明实施例中会话密钥的生成方法的另一种流程图；

[0040] 图 4 为本发明实施例中会话密钥的生成模块的另一种结构图；

[0041] 图 5 为本发明实施例中带磁通道的射频通讯系统会话过程的整体流程图。

具体实施方式

[0042] 本发明的主要构思是：利用磁通道和射频通道共同完成射频会话密钥协商。这样可以充分利用磁通道的近距离传输特性，提高会话密钥的安全性，从而提高使用该会话密钥的通讯过程的安全性。

[0043] 以下结合附图对本发明的原理和特征进行描述，所举实例只用于解释本发明，并非用于限定本发明的范围。

[0044] 图 1 为本发明实施例中会话密钥的生成方法的一种流程图。图 1 所示流程是带磁通道的射频通讯系统中会话发起方所执行的会话密钥生成方法流程。如图 1 所示，本实施例中，会话发起方所执行的会话密钥生成方法流程包括：

[0045] 步骤 401，生成第一随机数 RND1；

[0046] 第一随机数 RND1 的长度可以为大于等于 2 字节且小于等于 14 字节。优选地，第一随机数 RND1 的长度可以为 14 字节。

[0047] 本文中，随机数可以采用任何一种现有的或以后可能出现的随机数生成方式生成。

[0048] 步骤 402，通过磁通道发送会话请求消息，该会话请求消息携带第一随机数 RND1；

[0049] 会话请求消息的目的地是会话发起方和响应方之中的响应方。

[0050] 步骤 403，通过射频通道接收响应消息，响应消息携带第二随机数 RND2；

[0051] 响应消息的来源是会话发起方和响应方之中的响应方。优选地，第二随机数 RND2 的长度可以为 8 字节。

[0052] 响应方在接收到会话请求消息之后的通讯接入和建立连接过程中，但在会话数据开始传输之前，可以通过射频通道在通讯接入和建立连接过程中的任何一个响应消息中将第二随机数 RND2 发送给发起方，而不仅仅是在会话请求消息的响应消息中携带第二随机

数 RND2。

[0053] 步骤 404，根据第一随机数 RND1 和第二随机数 RND2 生成会话密钥 SK。

[0054] 根据第一随机数 RND1 和第二随机数 RND2 生成会话密钥的具体过程可以是：以第一随机数 RND1 和 / 或任何基于 RND1 的变换而得到的值为主密钥 Km，以第二随机数 RND2 和 / 或任何基于 RND2 的变换而得到的值为分散参数 X，按照某种指定的密钥分散算法 F 对主密钥 Km 和分散参数 X 进行密钥分散，从而得到会话密钥 SK。

[0055] 优选地，主密钥 Km 的长度可以为 16 字节。该 16 字节长的主密钥 Km 可以通过如下方式得到：取长度为 14 字节（即 112bits，1 字节等于 8 比特）的 RND1 序列，在每 7bits（比特）数据后插入 1 比特对该 7bits 数据的奇校验位或偶校验位，从而得到 16 字节长的主密钥 Km。

[0056] 优选地，第二随机数 RND2 的长度可以为 8 字节。则分散参数 X 可以通过如下方式得到：直接使用 8 字节的 RND2 作为分散参数 X。

[0057] 其中，密钥分散算法 F 可以是：以 16 字节长的主密钥 Km 为加密密钥，以 8 字节长的分散参数 X 为被加密明文，进行 3DES（Triple Data Encryption Standard，3 重数据加密标准）加密运算，将得到的 8 字节密文作为 16 字节会话密钥 SK 的前半部分；以 16 字节长的主密钥 Km 为加密密钥，以 8 字节长的分散参数 X 的按位取反（~X）为被加密明文，进行 3DES 加密运算，将得到的 8 字节密文作为 16 字节会话密钥 SK 的后半部分。其中，这里的加密算法 3DES 也可以用其他的加密算法代替，例如 AES（Advanced Encryption Standard，先进加密标准）算法等。

[0058] 本发明实施例的会话密钥的生成方法，利用磁通道和射频通道共同完成射频会话密钥协商，充分利用了磁通道的近距离传输特性，使得射频通道在数据安全性上等同于近距离磁通道的安全性，提高了会话密钥的安全性，从而提高了使用该会话密钥的通讯过程的安全性。

[0059] 图 2 为本发明实施例中会话密钥的生成模块的一种结构图。图 2 所示第一会话密钥生成模块 50 用以执行图 1 所示的会话密钥生成方法流程。图 2 所示第一会话密钥生成模块应用于带磁通道的射频通讯系统的会话发起方。

[0060] 如图 2 所示，本实施例中，第一会话密钥生成模块 50 包括第一生成单元 51、第一发送单元 52、第一接收单元 53 和第一密钥生成单元 54。第一密钥生成单元 54 分别与第一生成单元 51 和第一接收单元 53 相连。第一发送单元 52 与第一生成单元 51 相连。

[0061] 第一生成单元 51 用于生成第一随机数 RND1。第一发送单元 52 用于通过磁通道发送会话请求消息，该会话请求消息携带第一生成单元 51 生成的第一随机数 RND1。第一接收单元 53 用于通过射频通道接收会话请求消息的响应消息，该响应消息携带第二随机数 RND2。密钥生成单元 54 用于根据第一生成单元 51 生成的第一随机数 RND1 和第一接收单元 53 接收的第二随机数 RND2 生成会话密钥。

[0062] 其中，第一密钥生成单元 54 可以进一步包括第一密钥生成子单元、第二密钥生成子单元和第三密钥生成子单元。第一密钥生成子单元用于以第一随机数 RND1 和 / 或基于第一随机数 RND1 的变换得到的值为主密钥 Km。第二密钥生成子单元用于以第二随机数 RND2 和 / 或基于第二随机数 RND2 的变换而得到的值为分散参数 X。第三密钥生成子单元用于按照设定的密钥分散算法对主密钥 Km 和分散参数 X 进行密钥分散，得到会话密钥 SK。

[0063] 其中，第三密钥生成子单元还可以进一步包括密钥分散算法子单元。密钥分散算法子单元用于以长度为 16 字节的主密钥 Km，为加密密钥，以长度为 8 字节的分散参数 X 为被加密明文，进行 3DES 加密运算，将得到的 8 字节密文作为长度为 16 字节的会话密钥的前半部分；以长度为 16 字节的主密钥 Km 为加密密钥，以长度为 8 字节的分散参数 X 的按位取反（~X）为被加密明文，进行 3DES 加密运算，将得到的 8 字节密文作为长度为 16 字节的会话密钥的后半部分。

[0064] 其中，第一密钥生成子单元可以进一步包括主密钥获取子单元。主密钥获取子单元用于取长度为 14 字节的第一随机数序列，在每 7 比特数据后插入 1 比特对该 7 比特数据的奇校验位或偶校验位，得到长度为 16 字节的主密钥 Km。

[0065] 其中，第二密钥生成子单元可以进一步包括分散参数获取子单元，用于直接取长度为 8 字节的第二随机数作为分散参数。

[0066] 其中，第一随机数的长度可以大于或等于 2 字节，且小于或等于 14 字节。

[0067] 本发明实施例的会话密钥的生成模块，利用磁通道和射频通道共同完成射频会话密钥协商，充分利用了磁通道的近距离传输特性，使得射频通道在数据安全性上等同于近距离磁通道的安全性，提高了会话密钥的安全性，从而提高了使用该会话密钥的通讯过程的安全性。

[0068] 图 3 为本发明实施例中会话密钥的生成方法的另一种流程图。图 3 所示流程是带磁通道的射频通讯系统中会话响应方所执行的会话密钥生成方法流程。如图 3 所示，本实施例中，会话响应方所执行的会话密钥生成方法流程包括：

[0069] 步骤 601，通过磁通道接收会话请求消息，该会话请求消息携带第一随机数 RND1；

[0070] 会话请求消息的来源是会话发起方和响应方之中的发起方。第一随机数 RND1 的长度可以为大于等于 2 字节且小于等于 14 字节。优选地，第一随机数 RND1 的长度可以为 14 字节。

[0071] 步骤 602，生成第二随机数 RND2；

[0072] 优选地，第二随机数 RND2 的长度可以为 8 字节。

[0073] 步骤 603，通过射频通道发送响应消息，该响应消息携带第二随机数 RND2；

[0074] 响应消息的目的地是会话发起方和响应方之中的发起方。响应方在接收到会话请求消息之后的通讯接入和建立连接过程中，但在会话数据开始传输之前，可以通过射频通道在通讯接入和建立连接过程中的任何一个响应消息中将第二随机数 RND2 发送给发起方，而不仅仅是在会话请求消息的响应消息中携带第二随机数 RND2。

[0075] 步骤 604，根据第一随机数 RND1 和第二随机数 RND2 生成会话密钥 SK。

[0076] 根据第一随机数 RND1 和第二随机数 RND2 生成会话密钥的具体过程可以是：以第一随机数 RND1 和 / 或任何基于 RND1 的变换而得到的值为主密钥 Km，以第二随机数 RND2 和 / 或任何基于 RND2 的变换而得到的值为分散参数 X，按照某种指定的密钥分散算法 F 对主密钥 Km 和分散参数 X 进行密钥分散，从而得到会话密钥 SK。

[0077] 优选地，主密钥 Km 的长度可以为 16 字节。该 16 字节长的主密钥 Km 可以通过如下方式得到：取长度为 14 字节（即 112bits，1 字节等于 8 比特）的 RND1 序列，在每 7bits（比特）数据后插入 1 比特对该 7bits 数据的奇校验位或偶校验位，从而得到 16 字节长的主密钥 Km。

[0078] 优选地，第二随机数 RND2 的长度可以为 8 字节。则分散参数 X 可以通过如下方式得到：直接使用 8 字节的 RND2 作为分散参数 X。

[0079] 其中，密钥分散算法 F 可以是：以 16 字节长的主密钥 Km 为加密密钥，以 8 字节长的分散参数 X 为被加密明文，进行 3DES（Triple Data Encryption Standard，3 重数据加密标准）加密运算，将得到的 8 字节密文作为 16 字节会话密钥 SK 的前半部分；以 16 字节长的主密钥 Km 为加密密钥，以 8 字节长的分散参数 X 的按位取反（^X）为被加密明文，进行 3DES 加密运算，将得到的 8 字节密文作为 16 字节会话密钥 SK 的后半部分。

[0080] 本发明实施例的会话密钥的生成方法，利用磁通道和射频通道共同完成射频会话密钥协商，充分利用了磁通道的近距离传输特性，使得射频通道在数据安全性上等同于近距离磁通道的安全性，提高了会话密钥的安全性，从而提高了使用该会话密钥的通讯过程的安全性。

[0081] 图 4 为本发明实施例中会话密钥的生成模块的另一种结构图。图 4 所示第二会话密钥生成模块 70 用以执行图 3 所示的会话密钥生成方法流程。图 4 所示第二会话密钥生成模块应用于带磁通道的射频通讯系统的会话响应方。

[0082] 如图 4 所示，本实施例中，第二会话密钥生成模块 70 包括第二生成单元 71、第二发送单元 72、第二接收单元 73 和第二密钥生成单元 74。第二密钥生成单元 74 分别与第二生成单元 71 和第二接收单元 73 相连。第二发送单元 72 与第二生成单元 71 相连。

[0083] 图 4 中，第二接收单元 73 用于通过磁通道接收会话请求消息，该会话请求消息携带第一随机数 RND1。第二生成单元 71 用于生成第二随机数 RND2。第二发送单元 72 用于通过射频通道发送会话请求消息的响应消息，该响应消息携带第二生成单元 71 生成的第二随机数 RND2。第二密钥生成单元 74 用于根据第二接收单元 73 接收的第一随机数 RND1 和第二生成单元 71 生成的第二随机数 RND2 生成会话密钥 SK。

[0084] 其中，第二密钥生成单元 74 的结构与图 2 中第一密钥生成单元 54 的结构相同。第二密钥生成单元 74 可以进一步包括第一密钥生成子单元、第二密钥生成子单元和第三密钥生成子单元。第一密钥生成子单元用于以第一随机数 RND1 和 / 或基于第一随机数 RND1 的变换得到的值为主密钥 Km。第二密钥生成子单元用于以第二随机数 RND2 和 / 或基于第二随机数 RND2 的变换而得到的值为分散参数 X。第三密钥生成子单元用于按照设定的密钥分散算法对主密钥 Km 和分散参数 X 进行密钥分散，得到会话密钥 SK。

[0085] 其中，第三密钥生成子单元可以进一步包括密钥分散算法子单元。密钥分散算法子单元用于以长度为 16 字节的主密钥 Km，为加密密钥，以长度为 8 字节的分散参数 X 为被加密明文，进行 3DES 加密运算，将得到的 8 字节密文作为长度为 16 字节的会话密钥的前半部分；以长度为 16 字节的主密钥 Km 为加密密钥，以长度为 8 字节的分散参数 X 的按位取反（^X）为被加密明文，进行 3DES 加密运算，将得到的 8 字节密文作为长度为 16 字节的会话密钥的后半部分。

[0086] 其中，第一密钥生成子单元可以进一步包括主密钥获取子单元。主密钥获取子单元用于取长度为 14 字节的第一随机数序列，在每 7 比特数据后插入 1 比特对该 7 比特数据的奇校验位或偶校验位，得到长度为 16 字节的主密钥 Km。

[0087] 其中，第二密钥生成子单元可以进一步包括分散参数获取子单元，用于直接取长度为 8 字节的第二随机数作为分散参数。

[0088] 其中，第一随机数的长度可以大于或等于 2 字节，且小于或等于 14 字节。

[0089] 本发明实施例的会话密钥的生成模块，利用磁通道和射频通道共同完成射频会话密钥协商，充分利用了磁通道的近距离传输特性，使得射频通道在数据安全性上等同于近距离磁通道的安全性，提高了会话密钥的安全性，从而提高了使用该会话密钥的通讯过程的安全性。

[0090] 图 5 为本发明实施例中带磁通道的射频通讯系统会话过程的整体流程图。这里，带磁通道的射频通讯系统可以是背景技术中所述的、由带磁通道的 2.4GHz 射频智能卡及其读卡器所组成的近距离射频通讯系统。如图 5 所示，本实施例中，带磁通道的射频通讯系统会话过程的整体流程包括会话发起过程 10、会话密钥协商过程 20 和数据传输过程 30 三个基本过程。具体如下。

[0091] 会话发起过程 10 包括 ：

[0092] 步骤 101，发起方生成第一随机数 RND1 ；

[0093] 优选地，第一随机数 RND1 的长度可以为大于或等于 2 字节，且小于或等于 14 字节。

[0094] 步骤 102，发起方通过磁通道将第一随机数 RND1 发送至响应方。

[0095] 会话发起方首先通过磁通道向响应方发送会话请求消息，该会话请求消息中包含发起方生成的第一随机数 RND1。

[0096] 会话密钥协商过程 20 包括 ：

[0097] 步骤 201，响应方生成第二随机数 RND2 ；

[0098] 步骤 202，响应方通过射频通道将第二随机数 RND2 发送至发起方 ；

[0099] 步骤 203，发起方和响应方双方采用预设算法计算会话密钥 SK（Session Key）。

[0100] 响应方在接收到会话请求消息之后的通讯接入和建立连接过程中，但在会话数据开始传输之前，通过射频通道在通讯接入和建立连接过程中的任何一个响应消息中将第二随机数 RND2 发送给发起方。

[0101] 最后，通讯双方按照预设的会话密钥算法对第一随机数 RND1 和第二随机数 RND2 进行运算，从而生成本次射频通讯会话的会话密钥 SK。

[0102] 预设的会话密钥算法可以是 ：以第一随机数 RND1 和 / 或任何基于 RND1 的变换而得到的值为主密钥 Km，以第二随机数 RND2 和 / 或任何基于 RND2 的变换而得到的值为分散参数 X，按照某种指定的密钥分散算法 F 对主密钥 Km 和分散参数 X 进行密钥分散，从而得到会话密钥 SK。

[0103] 优选地，主密钥 Km 的长度可以为 16 字节。该 16 字节长的主密钥 Km 可以通过如下方式得到 ：取长度为 14 字节（即 112bits，1 字节等于 8 比特）的 RND1 序列，在每 7bits（比特）数据后插入 1 比特对该 7bits 数据的奇校验位或偶校验位，从而得到 16 字节长的主密钥 Km。

[0104] 优选地，第二随机数 RND2 的长度可以为 8 字节。则分散参数 X 可以通过如下方式得到 ：直接使用 8 字节的 RND2 作为分散参数 X。

[0105] 其中，密钥分散算法 F 可以是 ：以 16 字节长的主密钥 Km 为加密密钥，以 8 字节长的分散参数 X 为被加密明文，进行 3DES（Triple Data Encryption Standard，三重数据加密标准）加密运算，将得到的 8 字节密文作为 16 字节会话密钥 SK 的前半部分 ；以 16 字节

长的主密钥 Km 为加密密钥，以 8 字节长的分散参数 X 的按位取反(~X)为被加密明文，进行 3DES 加密运算，将得到的 8 字节密文作为 16 字节会话密钥 SK 的后半部分。

[0106] 数据传输过程 30 包括：

[0107] 步骤 301，数据发送方使用会话密钥 SK 对数据进行加密；

[0108] 步骤 302，数据发送方通过射频通道发送加密后的密文数据；

[0109] 步骤 303，数据接收方使用会话密钥 SK 对接收到的密文数据进行解密。

[0110] 最后判断会话是否结束，若是则整个会话过程结束，否则返回数据传输过程 30。

[0111] 由上可见，会话发起方和响应方之间在射频通讯系统接入和连接过程中，利用磁通道和射频通道共同完成射频会话密钥协商，且在后续通讯过程中使用该会话密钥进行数据加密，使得射频通道在数据安全性上等同于近距离磁通道的安全性。这样充分利用了磁通道的近距离传输特性，提高了会话密钥的安全性，从而提高使用该会话密钥的通讯过程的安全性。

[0112] 以上所述仅为本发明的较佳实施例，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

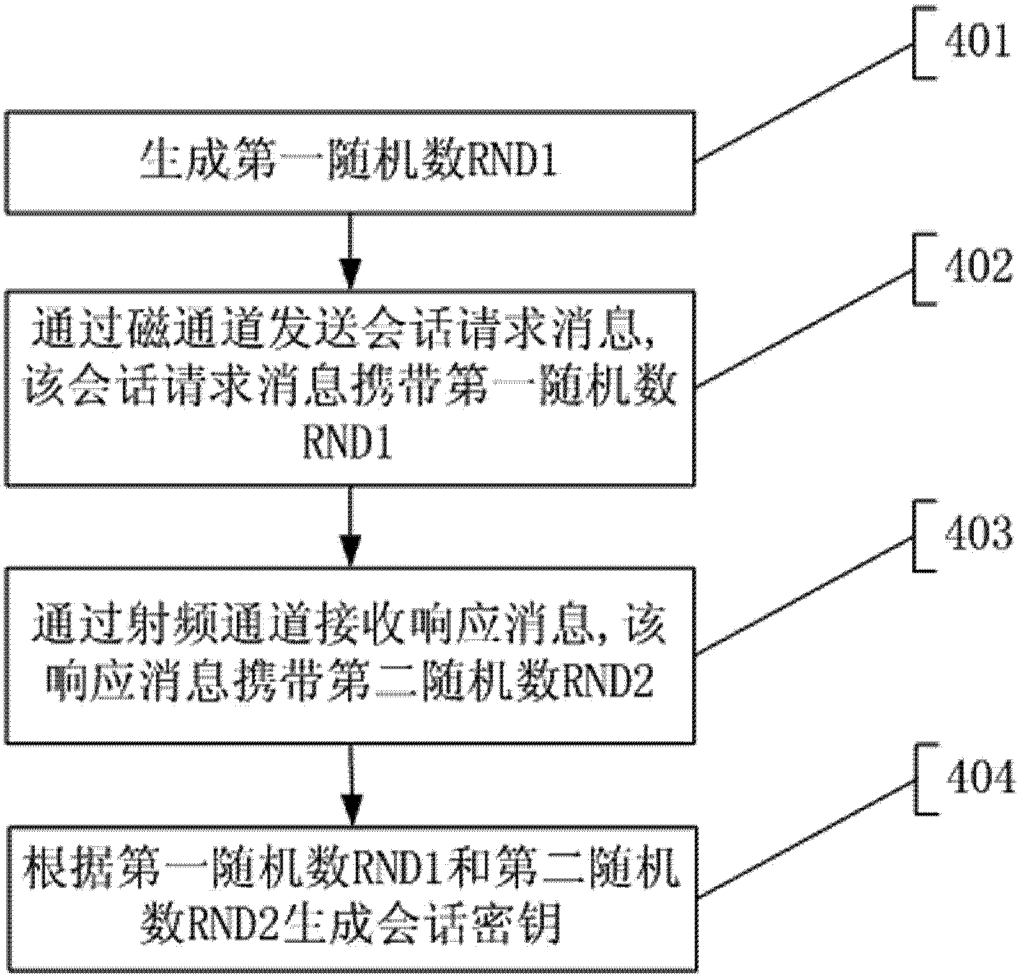

401
生成第一随机数RND1
402
通过磁通道发送会话请求消息，该会话请求消息携带第一随机数RND1
403
通过射频通道接收响应消息，该响应消息携带第二随机数RND2
404
根据第一随机数RND1和第二随机数RND2生成会话密钥

图 1

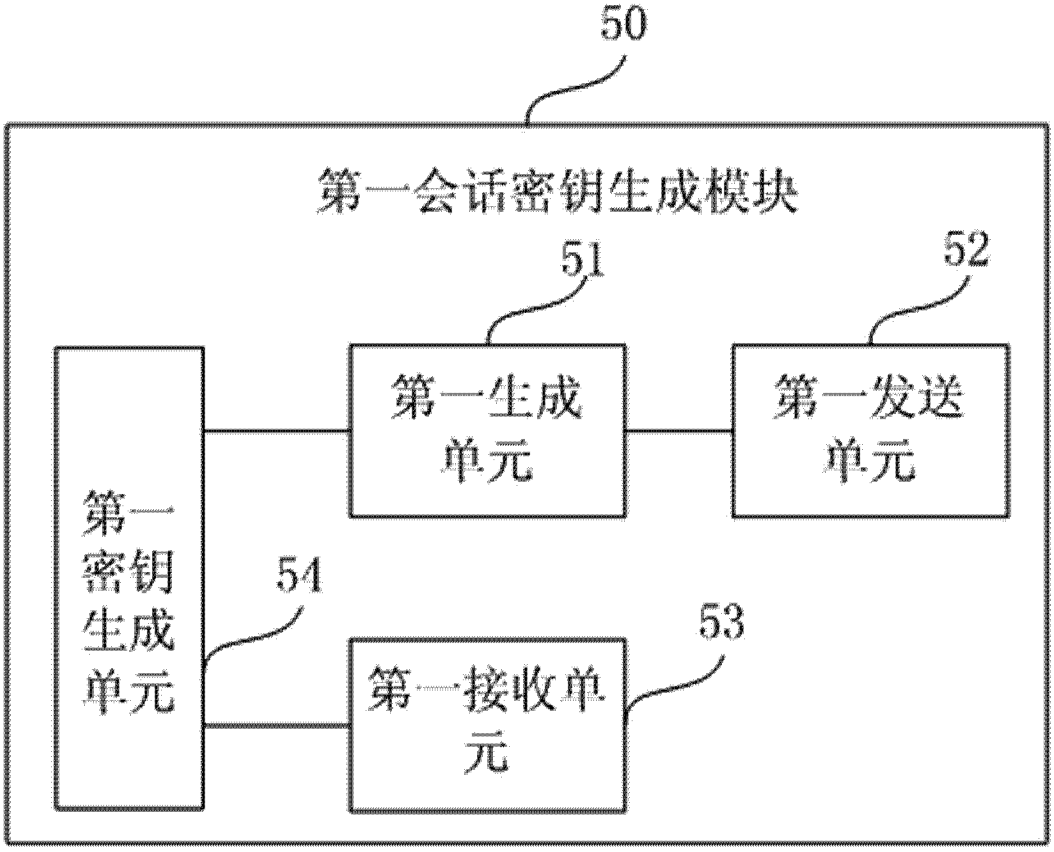


图 2

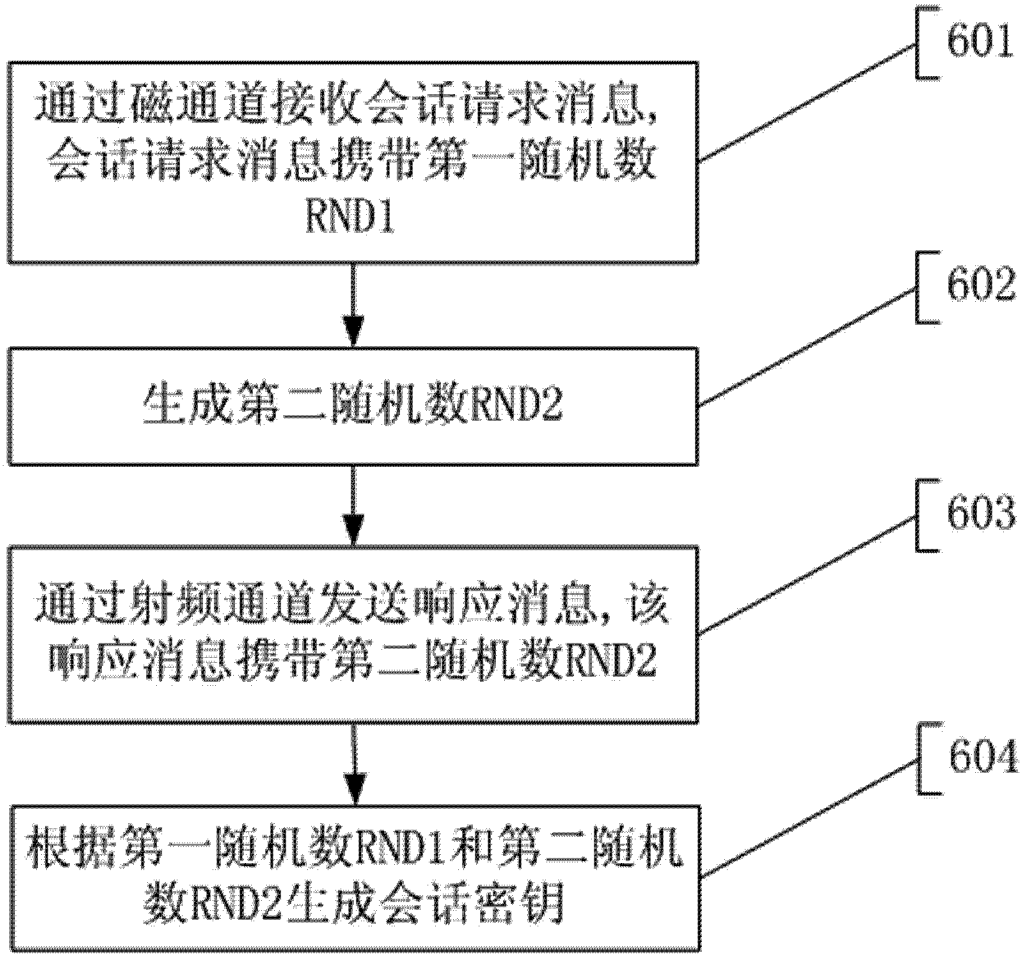

601
通过磁通道接收会话请求消息，会话请求消息携带第一随机数RND1
602
生成第二随机数RND2
603
通过射频通道发送响应消息，该响应消息携带第二随机数RND2
604
根据第一随机数RND1和第二随机数RND2生成会话密钥

图 3

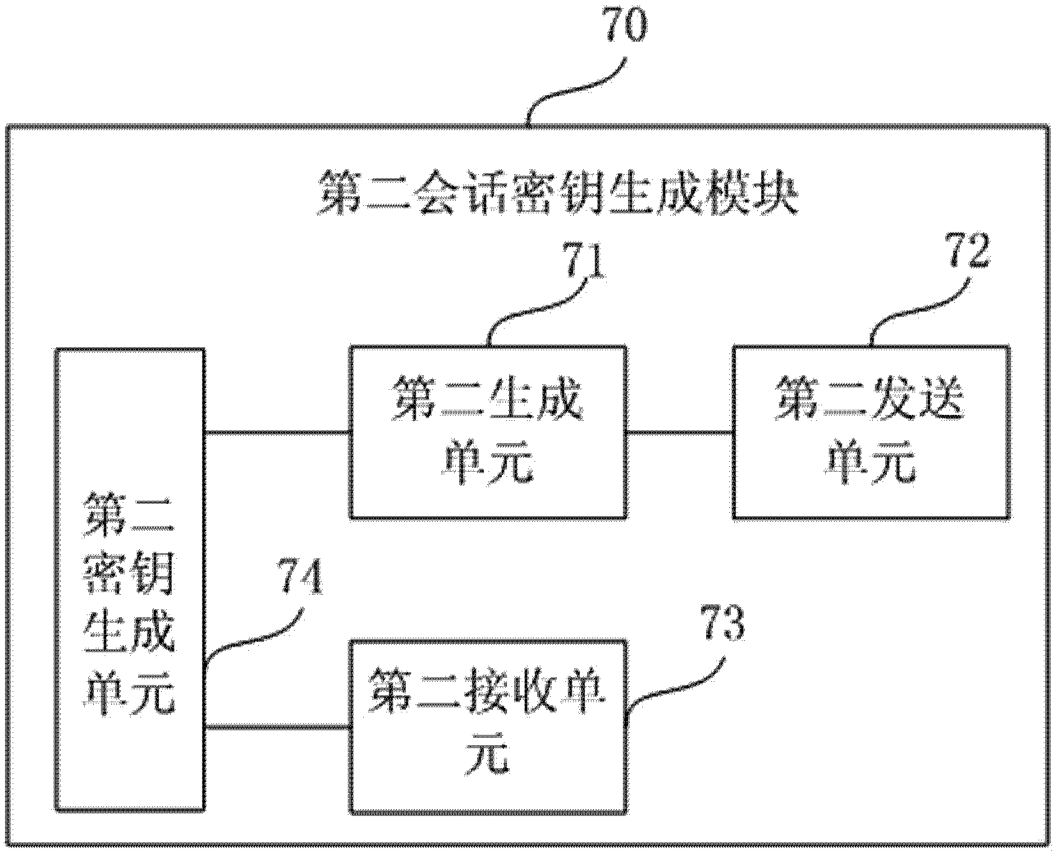


图 4

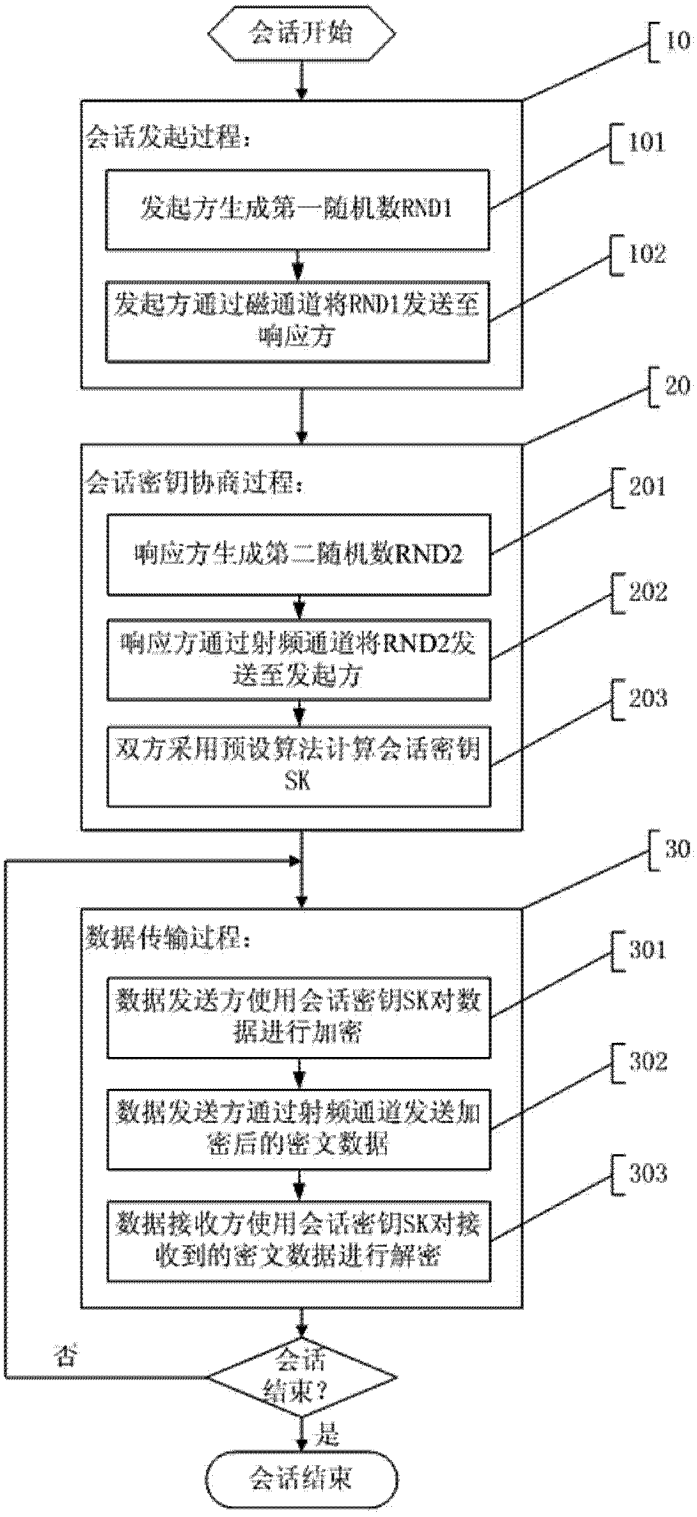

会话开始
10
会话发起过程：
101
发起方生成第一随机数RND1
102
发起方通过磁通道将RND1发送至响应方
20
会话密钥协商过程：
201
响应方生成第二随机数RND2
202
响应方通过射频通道将RND2发送至发起方
203
双方采用预设算法计算会话密钥SK
30
数据传输过程：
301
数据发送方使用会话密钥SK对数据进行加密
302
数据发送方通过射频通道发送加密后的密文数据
303
数据接收方使用会话密钥SK对接收到的密文数据进行解密
否
会话结束？
是
会话结束

图 5