

生成应用层密钥

技术领域

[01]本说明书一个或多个实施例涉及蓝牙技术领域，尤其涉及生成应用层密钥的方法和装置。

背景技术

[02]蓝牙技术是一种支持设备短距离通信的无线电技术。建立蓝牙连接的设备之间可以进行无线数据通信，为保证通信数据的安全性，除了在链路层使用链路层密钥对通信数据进行加密以外，还可以在应用层利用应用层密钥对通信数据进行加密，以实现通信数据的双层加密。

[03]目前，该应用层密钥是预置在蓝牙设备的固件中的，且各个蓝牙设备内预置的应用层密钥相同，应用层密钥容易被攻击者逆向破解。因此，需要提供一种更可靠的应用层密钥生成方案。

发明内容

[04]本说明书一个或多个实施例描述了一种生成应用层密钥的方法和装置，以降低应用层密钥被攻击者破解的可能性。

[05]根据第一方面，提供了一种生成应用层密钥的方法，包括：确定与外部蓝牙设备建立蓝牙连接时使用的连接模式；根据所述连接模式，确定应用层密钥生成函数；根据所述应用层密钥生成函数，确定在链路层使用的链路层动态参数；获取与所述外部蓝牙设备约定的应用层密钥标识；根据所述应用层密钥生成函数、所述链路层动态参数和所述应用层密钥标识，生成应用层密钥。

[06]在一个实施例中，所述连接模式为：基本速率/增强数据速率模式；所述根据所述连接模式确定应用层密钥生成函数，包括：将生成链路层密钥时使用的 f_2 函数，确定为应用层密钥生成函数；所述确定在链路层使用的链路层动态参数，包括：将所述 f_2 函数在计算链路层密钥时使用的各密钥参数中的随机数确定为所述链路层动态参数；所述生成应用层密钥，包括：将所述 f_2 函数在计算链路层密钥时使用的各密钥参数中的链路层密钥标识替换为所述应用层密钥标识；利用所述 f_2 函数对替换后得到的各密钥参数进行计算，得到所述应用层密钥。

[07]在一个实施例中，所述应用层密钥标识与所述链路层密钥标识不相同。

[08]在一个实施例中,所述连接模式为:基本速率/增强数据速率模式,或者低功耗模式;所述根据所述连接模式确定应用层密钥生成函数,包括:将 h6 函数,确定为应用层密钥生成函数;所述确定在链路层使用的链路层动态参数,包括:获取与外部蓝牙设备建立所述蓝牙连接时生成的链路层密钥;将所述链路层密钥确定为所述链路层动态参数;所述生成应用层密钥,包括:利用所述 h6 函数对所述应用层密钥标识和所述链路层密钥进行计算,得到所述应用层密钥。

[09]在一个实施例中,当所述连接模式为基本速率/增强数据速率模式时;所述链路层密钥是利用 f2 函数以及链路层密钥标识生成的;所述应用层密钥标识与所述链路层密钥标识相同或不相同。

[10]在一个实施例中,当所述连接模式为低功耗模式时;所述链路层密钥是利用 f5 函数生成的。

[11]第二方面,还提供了一种生成应用层密钥的装置,包括:连接模式确定单元,被配置为确定与外部蓝牙设备建立蓝牙连接时使用的连接模式;应用层密钥生成函数确定单元,被配置为根据所述连接模式,确定应用层密钥生成函数;链路层动态参数获取单元,被配置为根据所述应用层密钥生成函数,确定在链路层使用的链路层动态参数;应用层密钥标识获取单元,被配置为获取与所述外部蓝牙设备约定的应用层密钥标识;应用层密钥生成单元,被配置为根据所述应用层密钥生成函数、所述链路层动态参数和所述应用层密钥标识,生成应用层密钥。

[12]在一个实施例中,所述连接模式为:基本速率/增强数据速率模式;所述应用层密钥生成函数确定单元被配置为:将生成链路层密钥时使用的 f2 函数,确定为应用层密钥生成函数;链路层动态参数获取单元被配置为:将所述 f2 函数在计算链路层密钥时使用的各密钥参数中的随机数确定为所述链路层动态参数;所述应用层密钥生成单元被配置为:将所述 f2 函数在计算链路层密钥时使用的各密钥参数中的链路层密钥标识替换为所述应用层密钥标识;利用所述 f2 函数对替换后得到的各密钥参数进行计算,得到所述应用层密钥。

[13]在一个实施例中,所述应用层密钥标识与所述链路层密钥标识不相同。

[14]在一个实施例中,所述连接模式为:基本速率/增强数据速率模式,或者低功耗模式;所述应用层密钥生成函数确定单元被配置为:将 h6 函数,确定为应用层密钥生成函数;所述链路层动态参数获取单元被配置为:获取与外部蓝牙设备建立所述蓝牙连接时生成的链路层密钥;将所述链路层密钥确定为所述链路层动态参数;所述应用层密钥生成单元被配置为:利用所述 h6 函数对所述应用层密钥标识和所述链路层密钥进行计算,得

到所述应用层密钥。

[15]在一个实施例中，当所述连接模式为基本速率/增强数据速率模式时；所述链路层密钥是利用 f2 函数以及链路层密钥标识生成的；所述应用层密钥标识与所述链路层密钥标识相同或不相同。

[16]在一个实施例中，当所述连接模式为低功耗模式时；所述链路层密钥是利用 f5 函数生成的。

[17]根据第三方面，提供了一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现本说明书任一实施例所述的方法。

[18]在本说明书实施例提供的一种生成应用层密钥的方法和装置，蓝牙设备根据与外部蓝牙设备建立蓝牙连接时使用的连接模式，确定应用层密钥生成函数，并根据确定的应用层密钥生成函数，确定在链路层使用的链路层动态参数，根据应用层密钥生成函数、链路层动态参数和与外部蓝牙设备约定的应用层密钥标识，生成应用层密钥。由于链路层使用的链路层动态参数是动态生成的，因此，利用该链路层动态参数生成的应用层密钥也是动态变化的，所以可以降低应用层密钥被攻击者破解的可能性。

附图说明

[19]为了更清楚地说明本说明书实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图是本说明书的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[20]图 1 是本发明一个实施例提供的生成应用层密钥的方法所应用的系统架构的示意图；

[21]图 2 是本说明书一个实施例提供的生成应用层密钥的方法的流程图；

[22]图 3 是本说明书一个实施例提供的生成应用层密钥的装置的示意图。

具体实施方式

[23]下面结合附图，对本说明书提供的方案进行描述。

[24]目前，应用层密钥是由应用开发者编写，并将该应用层密钥预置在蓝牙设备的固件中或者硬编码在蓝牙设备的应用 APP 中，该应用层密钥是固定不变的，且各个蓝牙设备内预置的应用层密钥相同，一旦被攻击者逆向破解出来，攻击者就可以获取到各个蓝牙设备内的应用层密钥，对蓝牙设备之间数据通信的安全性造成影响。

[25]如果需要提高蓝牙设备之间数据通信的安全性，可以考虑每次生成的应用层密钥是动态变化的，该应用层密钥可以通过使用函数对一些参数进行计算的方式来生成，但需要保证建立蓝牙连接的两个蓝牙设备都能够获知到每一次生成应用层密钥所使用的的函数和参数。

[26]其中，每一次生成应用层密钥所使用的的函数，可以通过每次建立蓝牙连接时使用的连接模式来确定。

[27]而对于生成应用层密钥所使用的参数，如果由其中一个蓝牙设备生成该参数后，再分发给另一个蓝牙设备，该分发过程不仅复杂，而且不安全。如此，可以考虑利用链路层使用的链路层动态参数，因为在每次建立蓝牙连接时，链路层本身就会产生链路层动态参数，且两端的蓝牙设备在链路层使用的链路层动态参数相同，因此，如果将该链路层使用的链路层动态参数作为生成应用层密钥时所使用的参数，不需要参数的分发过程，两端的蓝牙设备就会获知到该链路层动态参数。并且，每一次蓝牙连接时该链路层动态参数都是动态变化的，从而可以满足每次使用链路层动态参数生成的应用层密钥是动态变化的。

[28]下面描述以上构思的具体实现方式。

[29]为了方便对本说明书的理解，首先对本说明书所应用的系统架构进行描述。如图 1 中所示，该系统架构主要包括两个蓝牙设备。比如，一个蓝牙设备是蜻蜓主机，另一个蓝牙设备是蓝牙键盘。

[30]其中，每一个蓝牙设备中均设置有蓝牙芯片，用于利用该蓝牙芯片与另一个蓝牙设备的蓝牙芯片之间建立蓝牙连接，成功建立蓝牙连接的两个蓝牙设备之间可以实现短距离的无线数据通信。在无线数据通信过程中，蓝牙设备会在应用层和链路层分别对通信数据进行一次加密，将两次加密后的通信数据发送给另一端蓝牙设备，另一端蓝牙设备在接收到加密的通信数据后，会通过对应的两次解密来获取到该通信数据，从而保证通信数据的传输安全性。由于链路层密钥是在建立蓝牙连接的过程中生成的，下面描述生成应用层密钥的方法的具体实现过程。

[31]图 2 示出根据一个实施例的生成应用层密钥的方法的流程图。可以理解，该方法可以通过任何具有计算、处理能力的装置、设备、平台、设备集群来执行。参见图 2，此后，具体的实现包括：步骤 200：确定与外部蓝牙设备建立蓝牙连接时使用的连接模式；步骤 202：根据所述连接模式，确定应用层密钥生成函数；步骤 204：根据所述应用层密钥生成函数，确定在链路层使用的链路层动态参数；步骤 206：获取与所述外部蓝牙设备约定的应用层密钥标识；步骤 208：根据所述应用层密钥生成函数、所述链路层动

态参数和所述应用层密钥标识，生成应用层密钥。

[32]在图 2 所示的生成应用层密钥的方法中，蓝牙设备可以根据与外部蓝牙设备建立蓝牙连接时使用的连接模式，确定应用层密钥生成函数，并根据确定的应用层密钥生成函数，确定在链路层使用的链路层动态参数，根据应用层密钥生成函数、链路层动态参数和与外部蓝牙设备约定的应用层密钥标识，生成应用层密钥。由于链路层使用的链路层动态参数是动态生成的，因此，利用该链路层动态参数生成的应用层密钥也是动态变化的，所以可以降低应用层密钥被攻击者破解的可能性。并且，该链路层使用的链路层动态参数是在建立蓝牙连接的过程中本身就会产生的，因此，将该已有参数作为生成应用层密钥所使用的参数，可以避免复杂的参数分发过程。

[33]下面描述图 2 所示的各个步骤的实现方式。

[34]在步骤 200，确定与外部蓝牙设备建立蓝牙连接时使用的连接模式。

[35]可以实现蓝牙连接的电子设备有很多类型，例如，手机、平板电脑、笔记本电脑、相机、鼠标、键盘、手环等。不同类型的设备在建立蓝牙连接时使用的连接模式不同。

[36]本步骤中，确定出的蓝牙连接的连接模式可以包括两种：第一种是基础速率/增强数据速率（BR/EDR）模式，第二种是低功耗（LE）模式。其中，BR/EDR 模式主要用于音频和流媒体应用，是以点对点网络拓扑结构创建一对一设备通信；LE 模式多用于依靠电池工作的设备，使用点对点、广播和网络等多种网络拓扑结构。

[37]在步骤 202，根据确定出的连接模式，确定应用层密钥生成函数。

[38]在本说明书实施例中，该应用层密钥生成函数是用来生成应用层密钥的，而生成的应用层密钥需要满足如下三个条件：

[39]条件一、每次生成的应用层密钥是动态变化的。

[40]条件二、两个蓝牙设备需要能够获知到每一次使用的应用层密钥生成函数以及应用层密钥生成函数中使用的密钥参数。

[41]条件三、每次生成的应用层密钥与本次蓝牙连接中使用的其他密钥不相同。

[42]其中，上述条件二中两个蓝牙设备需要能够获知到每一次使用的应用层密钥生成函数，可以通过与外部蓝牙设备建立蓝牙连接时使用的连接模式来确定，下面针对上述两种连接模式，分别对确定的应用层密钥生成函数进行说明。

[43]一、连接模式为 BR/EDR 模式。

[44]由于蓝牙标准中存在有多个计算函数，为节省研发成本，可以直接使用蓝牙标准中

的计算函数来作为应用层密钥生成函数。在本说明书的一个实施例中,在该 BR/EDR 模式下,至少可以将蓝牙标准中的生成链路层密钥时使用的 f2 函数或将蓝牙标准中的 h6 函数作为应用层密钥生成函数,下面针对这两种函数分别进行说明。

[45]方式 A: 将生成链路层密钥时使用的 f2 函数确定为应用层密钥生成函数。

[46]在该 BR/EDR 模式下,蓝牙芯片在建立蓝牙连接完成后,会使用 f2 函数生成链路层密钥,该 f2 函数的表达式如下式(1)所示:

$$LK=f2(DHkey,N_master,N_slave,"btlk",BD_ADDR_master,BD_ADDR_slave) \quad (1)$$

[47]其中, LK 用于表征在 BR/EDR 模式下利用 f2 函数生成的链路层密钥, DHkey 是蓝牙芯片建立蓝牙连接过程中生成的密钥, N_master 是建立蓝牙连接的两个蓝牙设备中主蓝牙设备生成的随机数, N_slave 是建立蓝牙连接的两个蓝牙设备中从蓝牙设备生成的随机数, "btlk"为链路层密钥标识, 长度为 32bit, BD_ADDR_master 是建立蓝牙连接的两个蓝牙设备中主蓝牙设备的私有地址, BD_ADDR_slave 是建立蓝牙连接的两个蓝牙设备中从蓝牙设备的私有地址。

[48]根据上述 f2 函数的表达式可知, 在利用 f2 函数计算链路层密钥时使用的密钥参数中包括两个随机数 N_master 和 N_slave, 由于这两个随机数是在每一次建立蓝牙连接过程中随机生成的, 因此, 在本说明书实施例中, 可以将这两个随机数确定为步骤 204 中的在链路层使用的链路层动态参数。由于该链路层动态参数是动态变化的, 那么在步骤 208 中利用 f2 函数和该链路层动态参数生成应用层密钥时, 可以使得每次生成的应用层密钥是动态变化的, 从而满足了上述条件一。

[49]另外, 在利用 f2 函数计算链路层密钥时使用的密钥参数, 均已经在蓝牙连接建立过程中存储在了两端的蓝牙设备中。因此, 可以将该利用 f2 函数计算链路层密钥时使用的密钥参数作为应用层密钥生成函数中所使用的的密钥参数。如此, 不需要对密钥参数进行分发, 两端的蓝牙设备就能够获知到应用层密钥生成函数中所使用的密钥参数。以及, 应用层密钥生成函数通过连接模式来确定, 从而满足了上述条件二。

[50]可以理解, 如果生成的应用层密钥与本次蓝牙连接中使用的其他密钥相同, 比如, 与链路层密钥相同, 那么对通信数据使用两个相同的密钥进行加密, 其安全性会受到影响, 因此, 可以将 f2 函数在计算链路层密钥时使用的密钥参数中的链路层密钥标识 "btlk" 替换为步骤 206 中获取的应用层密钥标识, 使得利用 f2 函数在计算应用层密钥时使用的密钥参数与在利用 f2 函数计算链路层密钥时使用的密钥参数不同, 那么生成的应用层密钥就会与链路层密钥不相同, 从而满足了上述条件三。

[51]基于上述描述，可以得出该应用层密钥生成函数的表达式如下式(2)所示：

$$\text{APP_AES_Key} = f2(\text{DHkey}, \text{N_master}, \text{N_slave}, \text{KeyID}, \text{BD_ADDR_master}, \text{BD_ADDR_slave}) \quad (2)$$

[52]其中，APP_AES_Key 为利用 f2 函数生成的应用层密钥，KeyID 为应用层密钥标识。

[53]方式 B：将 h6 函数确定为应用层密钥生成函数。

[54]在蓝牙标准中存在一个 h6 函数，该 h6 函数的表达式如下式(3)所示：

$$\text{Key} = h6(\text{W}, \text{KeyID0}) \quad (3)$$

[55]其中，Key 用于表征利用 h6 函数生成的密钥，W 用于表征一个加密密钥，KeyID0 是该函数中的一个密钥标识，长度为 32bit。

[56]由于该 h6 函数是对加密密钥和密钥标识进行计算生成密钥 Key，那么可以考虑将该 h6 函数中使用的密钥参数进行更换，来生成本说明书实施例的应用层密钥，在本说明书实施例中，可以对式(3)进行密钥参数的更换，得到如下式(4)所示的 h6 函数的表达式：

$$\text{App_AES_Key} = h6(\text{LK}, \text{KeyID}) \quad (4)$$

[57]其中，APP_AES_Key 为利用 h6 函数生成的应用层密钥，LK 为在 BR/EDR 模式下通过式(1)利用 f2 函数以及链路层密钥标识生成的链路层密钥，KeyID 为应用层密钥标识。

[58]在利用该 h6 函数计算应用层密钥时使用的密钥参数中包括链路层密钥 LK，根据对上述方式 A 的描述可知，由于在利用 f2 函数计算链路层密钥时使用的密钥参数中包括两个随机数，因此每一次建立蓝牙连接时生成的链路层密钥 LK 是动态变化的。在本说明书实施例中，可以将该链路层密钥确定为步骤 204 中的在链路层使用的链路层动态参数。由于该链路层动态参数是动态变化的，那么在步骤 208 中利用 h6 函数和该链路层动态参数生成应用层密钥时，可以使得每次生成的应用层密钥是动态变化的，从而满足了上述条件一。

[59]另外，在每次建立蓝牙连接过程中，两端的蓝牙设备均生成并存储了该链路层密钥 LK，因此，直接将该链路层密钥作为应用层密钥生成函数中所使用的的密钥参数，从而可以不需要对密钥参数进行分发，两端的蓝牙设备就能够获知到应用层密钥生成函数中所使用的密钥参数。以及，应用层密钥生成函数通过连接模式来确定，从而满足了上述条件二。

[60]可以理解，在利用 h6 函数计算应用层密钥时使用的密钥参数（LK、KeyID）与蓝

牙标准中 h6 函数计算 Key 时使用的密钥参数 (W、KeyID0) 不相同, 因此, 计算得到的应用层密钥与 Key 不相同, 从而满足了上述条件三。

[61] 二、连接模式为 LE 模式。

[62] 在本说明书实施例中, 在该 LE 模式下, 至少可以将蓝牙标准中的 h6 函数作为应用层密钥生成函数。

[63] 根据对连接模式为 BR/EDR 模式下的方式 B 的描述可知, 可以对式(3)进行密钥参数的更换, 得到得到如下式(5)所示的 h6 函数的表达式:

$$\text{App_AES_Key} = \text{h6}(\text{LTK}, \text{KeyID}) \quad (5)$$

[64] 其中, APP_AES_Key 为利用 h6 函数生成的应用层密钥, LTK 为在 LE 模式下利用 f5 函数生成的链路层密钥, KeyID 为应用层密钥标识。

[65] 其中, f5 函数的表达式如下式(6)所示:

$$\text{LTK} = \text{f5}(\text{DHKey}, \text{Na}, \text{Nb}, \text{A}, \text{B}) \quad (6)$$

[66] 其中, DHKey 为蓝牙芯片建立蓝牙连接过程中生成的密钥, Na 是建立蓝牙连接的两个蓝牙设备中主蓝牙设备生成的随机数, Nb 是建立蓝牙连接的两个蓝牙设备中从蓝牙设备生成的随机数, A 是建立蓝牙连接的两个蓝牙设备中主蓝牙设备的私有地址, B 是建立蓝牙连接的两个蓝牙设备中从蓝牙设备的私有地址。

[67] 在利用该 h6 函数计算应用层密钥时使用的密钥参数中包括链路层密钥 LTK, 是根据上述 f5 函数计算得到的, 根据 f5 函数可知, 在计算该链路密钥时使用的密钥参数中包括两个随机数 Na 和 Nb, 因此每一次建立蓝牙连接时生成的链路层密钥 LTK 是动态变化的。在本说明书实施例中, 可以将该链路层密钥确定为步骤 204 中的在链路层使用的链路层动态参数。由于该链路层动态参数是动态变化的, 那么在步骤 208 中利用 h6 函数和该链路层动态参数生成应用层密钥时, 可以使得每次生成的应用层密钥是动态变化的, 从而满足了上述条件一。

[68] 另外, 在每次建立蓝牙连接过程中, 两端的蓝牙设备均生成并存储了该链路层密钥 LTK, 因此, 直接将该链路层密钥作为应用层密钥生成函数中所使用的的密钥参数, 从而可以不需要对密钥参数进行分发, 两端的蓝牙设备就能够获知到应用层密钥生成函数中所使用的密钥参数。以及, 应用层密钥生成函数通过连接模式来确定, 从而满足了上述条件二。

[69] 可以理解, 在利用 h6 函数计算应用层密钥时使用的密钥参数 (LTK、KeyID) 与蓝牙标准中 h6 函数计算 Key 时使用的密钥参数 (W、KeyID0) 不相同, 因此, 计算得到

的应用层密钥与 Key 不相同，从而满足了上述条件三。

[70]在步骤 204，根据应用层密钥生成函数，确定在链路层使用的链路层动态参数。

[71]在本说明书实施例中，在步骤 202 中，确定的应用层密钥生成函数不同，那么获取的该链路层动态参数也不同，具体地：

[72]如果在步骤 202 中，将生成链路层密钥时使用的 f2 函数确定为了应用层密钥生成函数，那么在本步骤 204 中，将 f2 函数在计算链路层密钥时使用的各密钥参数中的随机数确定为该链路层动态参数。

[73]如果在步骤 202 中，将 h6 函数确定为了应用层密钥生成函数，那么在本步骤 24 中，首先获取与外部蓝牙设备建立蓝牙连接时生成的链路层密钥，然后将该链路层密钥确定为该链路层动态参数。

[74]在步骤 206，获取与外部蓝牙设备约定的应用层密钥标识。

[75]根据步骤 202 可知，f2 函数中的链路层密钥标识的长度以及 h6 函数中的密钥标识的长度均为 32bit，那么为了便于计算，该应用层密钥标识的长度也可以为 32bit。

[76]在本说明书实施例中，该应用层密钥标识需要建立蓝牙连接的两个蓝牙设备预先约定好。例如，在一个可以实现的方式中，可以将应用层密钥标识预置在蓝牙设备的固件中，或者硬编码在蓝牙设备上安装的应用程序中。蓝牙设备可以从固件或硬编码中获取到该预置的应用层密钥标识。

[77]在本说明书实施例中，该预置的应用层密钥标识的个数可以为一个或多个。在预置的应用层密钥标识为多个时，两个蓝牙设备就需要预先约定好应用层密钥标识的选取规则，以使两个蓝牙设备选择相同的应用层密钥标识。

[78]根据步骤 202 中可知，需要生成的应用层密钥至少满足上述条件三。基于此，在如下两种前提下，应用层密钥标识需要满足的条件不同：

[79]前提一，连接模式为 BR/EDR 模式，且应用层密钥生成函数为 f2 函数。

[80]在该前提一下，应用层密钥标识需要满足的条件为：应用层密钥标识与链路层密钥标识不相同。

[81]只有在应用层密钥标识与链路层密钥标识不相同，在利用 f2 函数计算应用层密钥和链路层密钥时，所使用的密钥参数不完全相同，如此，生成的应用层密钥和链路层密钥不相同。

[82]前提二，连接模式为 BR/EDR 模式，且应用层密钥生成函数为 h6 函数。

[83]在该前提二下，应用层密钥标识需要满足的条件为：应用层密钥标识与链路层密钥标识相同或不相同。

[84]由于在该前提二下，计算应用层密钥和计算链路层密钥使用的函数不同，因此，无论应用层密钥标识与链路层密钥标识相同还是不相同，计算得到的应用层密钥与链路层密钥都不相同。

[85]在步骤 208，根据所述应用层密钥生成函数、所述链路层动态参数和所述应用层密钥标识，生成应用层密钥。

[86]在本说明书实施例中，步骤 202 中确定的应用层密钥生成函数不同，那么在生成应用层密钥时的计算过程不同，具体地：

[87]情况一：应用层密钥生成函数为 f2 函数。

[88]此种情况下，在步骤 204 中，是将 f2 函数在计算链路层密钥时使用的各密钥参数中包括的随机数确定为链路层动态参数。

[89]相应地，步骤 208 的实现过程包括：将所述 f2 函数在计算链路层密钥时使用的各密钥参数中的链路层密钥标识替换为所述应用层密钥标识；利用所述 f2 函数对替换后得到的各密钥参数进行计算，得到所述应用层密钥。

[90]情况二：应用层密钥生成函数为 h6 函数。

[91]此种情况下，在步骤 204 中，是获取与外部蓝牙设备建立蓝牙连接时生成的链路层密钥；将链路层密钥确定为该链路层动态参数；相应地，步骤 208 的实现过程包括：利用 h6 函数对应用层密钥标识和链路层密钥进行计算，得到应用层密钥。

[92]以上完成了应用层密钥的生成过程。

[93]在本说明书实施例中，应用层密钥在生成之后，可以存储在蓝牙设备中，以便蓝牙设备之间在数据通信时可以直接使用该应用层密钥。

[94]而为了进一步提高数据通信的安全性，降低被攻击者破解的可能性，两个蓝牙设备之间可以执行一种应用层密钥的更新机制，以实现对应用层密钥的更新，以使更新后的应用层密钥与更新前的应用层密钥不同，在对应用层密钥更新后，蓝牙设备使用更新后的应用层密钥对接下来进行通信的数据进行加密解密。下面对应用层密钥的更新机制进行说明。

[95]对应用层密钥进行更新的方式至少可以包括如下三种；

[96]方式 1、周期性更新。

[97]在该方式下，可以设定一个更新周期，每当达到设定的更新周期后，则重新生成应用层密钥，将重新生成的应用层密钥对本地存储的应用层密钥进行更新。

[98]方式 2、跟随链路层密钥的更新机制。

[99]在该方式下，每当链路层密钥需要重新生成时，则重新生成应用层密钥，并将重新生成的应用层密钥对本地存储的应用层密钥进行更新。

[100]方式 3、蓝牙设备重启后更新。

[101]在该方式下，可以将应用层密钥记录在内存中，蓝牙设备在每次重启后该内存中的应用层密钥会被清除，此时就需要重新生成一个应用层密钥。

[102]在上述说明书实施例中，蓝牙设备可以根据与外部蓝牙设备建立蓝牙连接时使用的连接模式，确定应用层密钥生成函数，并根据确定的应用层密钥生成函数，确定在链路层使用的链路层动态参数，根据应用层密钥生成函数、链路层动态参数和与外部蓝牙设备约定的应用层密钥标识，生成应用层密钥。由于链路层使用的链路层动态参数是动态生成的，因此，利用该链路层动态参数生成的应用层密钥也是动态变化的，所以可以降低应用层密钥被攻击者破解的可能性。并且，该链路层使用的链路层动态参数是在建立蓝牙连接的过程中本身就会产生的，因此，将该已有参数作为生成应用层密钥所使用的参数，可以避免复杂的参数分发过程。

[103]另一方面的实施例，还提供了一种生成应用层密钥的装置。如图 3 示出一个实施例的生成应用层密钥的装置。可以理解，该装置可以通过任何具有计算、处理能力的装置、设备、平台和设备集群来实现。如图 3 所示，该装置 30 包括：连接模式确定单元 31，被配置为确定与外部蓝牙设备建立蓝牙连接时使用的连接模式；应用层密钥生成函数确定单元 32，被配置为根据所述连接模式，确定应用层密钥生成函数；链路层动态参数获取单元 33，被配置为根据所述应用层密钥生成函数，确定在链路层使用的链路层动态参数；应用层密钥标识获取单元 34，被配置为获取与所述外部蓝牙设备约定的应用层密钥标识；应用层密钥生成单元 35，被配置为根据所述应用层密钥生成函数、所述链路层动态参数和所述应用层密钥标识，生成应用层密钥。

[104]一个可能的实现方式中，所述连接模式为：基本速率/增强数据速率模式；所述应用层密钥生成函数确定单元被配置为：将生成链路层密钥时使用的 f2 函数，确定为应用层密钥生成函数；链路层动态参数获取单元被配置为：将所述 f2 函数在计算链路层密钥时使用的各密钥参数中的随机数确定为所述链路层动态参数；所述应用层密钥生成单元被配置为：将所述 f2 函数在计算链路层密钥时使用的各密钥参数中的链路层密钥标识替换为所述应用层密钥标识；利用所述 f2 函数对替换后得到的各密钥参数进行计

算，得到所述应用层密钥。

[105] 一个可能的实现方式中，所述应用层密钥标识与所述链路层密钥标识不相同。

[106] 一个可能的实现方式中，所述连接模式为：基本速率/增强数据速率模式，或者低功耗模式；所述应用层密钥生成函数确定单元被配置为：将 h6 函数，确定为应用层密钥生成函数；所述链路层动态参数获取单元被配置为：获取与外部蓝牙设备建立所述蓝牙连接时生成的链路层密钥；将所述链路层密钥确定为所述链路层动态参数；所述应用层密钥生成单元被配置为：利用所述 h6 函数对所述应用层密钥标识和所述链路层密钥进行计算，得到所述应用层密钥。

[107] 一个可能的实现方式中，当所述连接模式为基本速率/增强数据速率模式时；所述链路层密钥是利用 f2 函数以及链路层密钥标识生成的；所述应用层密钥标识与所述链路层密钥标识相同或不相同。

[108] 一个可能的实现方式中，当所述连接模式为低功耗模式时；所述链路层密钥是利用 f5 函数生成的。

[109] 本说明书一个实施例提供了一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现执行说明书中任一个实施例中的方法。

[110] 可以理解的是，本说明书实施例示意的结构并不构成对生成应用层密钥的装置的具体限定。在说明书的另一些实施例中，生成应用层密钥的装置可以包括比图示更多或者更少的部件，或者组合某些部件，或者拆分某些部件，或者不同的部件布置。图示的部件可以以硬件、软件或者软件和硬件的组合来实现。

[111] 上述装置、系统内的各模块之间的信息交互、执行过程等内容，由于与本说明书方法实施例基于同一构思，具体内容可参见本说明书方法实施例中的叙述，此处不再赘述。

[112] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于装置实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[113] 本领域技术人员应该可以意识到，在上述一个或多个示例中，本发明所描述的功能可以用硬件、软件、挂件或它们的任意组合来实现。当使用软件实现时，可以将这些功能存储在计算机可读介质中或者作为计算机可读介质上的一个或多个指令或代码进

行传输。

[114] 以上所述的具体实施方式，对本发明的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本发明的具体实施方式而已，并不用于限定本发明的保护范围，凡在本发明的技术方案的基础之上，所做的任何修改、等同替换、改进等，均应包括在本发明的保护范围之内。

权利要求书

1、生成应用层密钥的方法，包括：

确定与外部蓝牙设备建立蓝牙连接时使用的连接模式；

根据所述连接模式，确定应用层密钥生成函数；

根据所述应用层密钥生成函数，确定在链路层使用的链路层动态参数；

获取与所述外部蓝牙设备约定的应用层密钥标识；

根据所述应用层密钥生成函数、所述链路层动态参数和所述应用层密钥标识，生成应用层密钥。

2、根据权利要求1所述的方法，其中，所述连接模式为：基本速率/增强数据速率模式；

所述根据所述连接模式确定应用层密钥生成函数，包括：

将生成链路层密钥时使用的f2函数，确定为应用层密钥生成函数；

所述确定在链路层使用的链路层动态参数，包括：

将所述f2函数在计算链路层密钥时使用的各密钥参数中的随机数确定为所述链路层动态参数；

所述生成应用层密钥，包括：

将所述f2函数在计算链路层密钥时使用的各密钥参数中的链路层密钥标识替换为所述应用层密钥标识；

利用所述f2函数对替换后得到的各密钥参数进行计算，得到所述应用层密钥。

3、根据权利要求2所述的方法，其中，所述应用层密钥标识与所述链路层密钥标识不相同。

4、根据权利要求1所述的方法，其中，所述连接模式为：基本速率/增强数据速率模式，或者低功耗模式；

所述根据所述连接模式确定应用层密钥生成函数，包括：

将h6函数，确定为应用层密钥生成函数；

所述确定在链路层使用的链路层动态参数，包括：

获取与外部蓝牙设备建立所述蓝牙连接时生成的链路层密钥；

将所述链路层密钥确定为所述链路层动态参数；

所述生成应用层密钥，包括：

利用所述h6函数对所述应用层密钥标识和所述链路层密钥进行计算，得到所述应用层密钥。

5、根据权利要求4所述的方法，其中，当所述连接模式为基本速率/增强数据速率模式时；

所述链路层密钥是利用 f2 函数以及链路层密钥标识生成的;

所述应用层密钥标识与所述链路层密钥标识相同或不相同。

6、根据权利要求 4 所述的方法,其中,当所述连接模式为低功耗模式时;所述链路层密钥是利用 f5 函数生成的。

7、生成应用层密钥的装置,包括:

连接模式确定单元,被配置为确定与外部蓝牙设备建立蓝牙连接时使用的连接模式;

应用层密钥生成函数确定单元,被配置为根据所述连接模式,确定应用层密钥生成函数;

链路层动态参数获取单元,被配置为根据所述应用层密钥生成函数,确定在链路层使用的链路层动态参数;

应用层密钥标识获取单元,被配置为获取与所述外部蓝牙设备约定的应用层密钥标识;

应用层密钥生成单元,被配置为根据所述应用层密钥生成函数、所述链路层动态参数和所述应用层密钥标识,生成应用层密钥。

8、根据权利要求 7 所述的装置,其中,所述连接模式为:基本速率/增强数据速率模式;

所述应用层密钥生成函数确定单元被配置为:将生成链路层密钥时使用的 f2 函数,确定为应用层密钥生成函数;

链路层动态参数获取单元被配置为:将所述 f2 函数在计算链路层密钥时使用的各密钥参数中的随机数确定为所述链路层动态参数;

所述应用层密钥生成单元被配置为:将所述 f2 函数在计算链路层密钥时使用的各密钥参数中的链路层密钥标识替换为所述应用层密钥标识;利用所述 f2 函数对替换后得到的各密钥参数进行计算,得到所述应用层密钥。

9、根据权利要求 8 所述的装置,其中,所述应用层密钥标识与所述链路层密钥标识不相同。

10、根据权利要求 7 所述的装置,其中,所述连接模式为:基本速率/增强数据速率模式,或者低功耗模式;

所述应用层密钥生成函数确定单元被配置为:将 h6 函数,确定为应用层密钥生成函数;

所述链路层动态参数获取单元被配置为:获取与外部蓝牙设备建立所述蓝牙连接时生成的链路层密钥;将所述链路层密钥确定为所述链路层动态参数;

所述应用层密钥生成单元被配置为:利用所述 h6 函数对所述应用层密钥标识和所述链路层密钥进行计算,得到所述应用层密钥。

11、根据权利要求 10 所述的装置，其中，当所述连接模式为基本速率/增强数据速率模式时；

所述链路层密钥是利用 f2 函数以及链路层密钥标识生成的；

所述应用层密钥标识与所述链路层密钥标识相同或不相同。

12、根据权利要求 10 所述的装置，其中，当所述连接模式为低功耗模式时；所述链路层密钥是利用 f5 函数生成的。

13、一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现权利要求 1-6 中任一项所述的方法。