ReliaSpeak

PVR 蓝牙语音保密器

技术白皮书 V1.2

保护通话隐私、语音消息隐私、录音隐私

北京睿语信息技术有限公司

北京西城区瑞得大厦 905 室
电话：8610-88334733
www.reliaspeak.com
support@reliaspeak.com

声明

PD：2021/02

目录

1、概述

1.1 背景

语音作为一种最普通的信息载体，在信息记录和信息交换方面，在实时性、便捷性、唯一性等方面，都是文字、图像、影像等其它载体所无法取代的，随着通讯技术的快速发展和普及应用，通过电子介质存储语音、通过网络传送语音也成为所有人的日常行为，但伴随而来的却是国家机密、商业机密、个人隐私与日俱增的失密风险。

如何保护语音安全？如何让语音中所包含的私密信息在存储和交换时不被非法人员窃取？目前，已有很多成熟的技术方案及产品，例如：对音频文件进行加密存储、加密 VoIP 系统、基于 v.32 等 Modem 技术的保密固话产品、运营商提供的 3G 或 VoLTE 加密手机，等等…

然而，这些技术方案和产品或多或少都存在以下几方面问题：

（1） 自成体系，仅适用于某个特定的地域、运营商或通讯方式，无法实现多态互通；

（2） 在安全性上必须依赖和信任特定的服务商，无法做到安全自主；

（3） 安全边界过窄，安全链没有完整闭环，存在安全弱点。

为此，北京睿语公司以独有的 AMSI 调制解调技术为核心，结合窄带语音编码技术和高等级密码技术，创建了语音加密编码器技术方案，实现了对音源的数字编码、加密和调制，并应用于 PVR 蓝牙语音保密器产品，为用户提供了一个安全链完全闭环、安全自主可控、能广泛适用于各个区域、运营商及通讯方式的语音保密产品。

1.2 产品简介

PVR 蓝牙语音保密器的核心是语音加密编码器，其可以将普通的明话音频信号通过语音编码、数字加密、信号调制等处理转换为密话音频信号。该密话音频信号具备以下三个特点：

（1） 密话音频信号不具备任何语音特征和可懂性，且只有使用正确的密钥才能被解码还原为可懂的明话音频；

（2） 密话音频信号可被录音程序进行编码存储，并在播放时进行解码还原；

（3） 密话音频信号可以像普通的模拟语音一样，通过有线电话信道、蜂窝语音信道、VoIP 信道进行传输，并可以在接收端被解码还原；

PVR 蓝牙语音保密器与手机等智能终端设备配合使用，可实现**录音加密**、**语音消息加密**、**移动通话加密**、**VoIP 通话加密**等功能。

PVR 蓝牙语音保密器实现了音源保护，能够在最大程度上抵抗窃听风险，包括运营商窃听、网络窃听、7 号信令窃听、伪基站窃听等线路窃听，以及手机间谍软件、后门等本地窃听。

2、 产品功能及性能指标

2.1 产品外形结构

图 1 PVR 蓝牙语音保密器产品外观

2.2 产品主要功能

（1） 配合手机录音软件[①]，实现语音加密录音；

[①] 录音软件应支持蓝牙拾音和播放

（2） 配合手机语音短信息软件[②]（如：微信中的语音消息功能），实现语音消息加密；

（3） 实现 GSM[③]、UMTS、VoLTE 蜂窝语音加密通话；

（4） 配合手机 VoIP 软件，实现 VoIP 通话加密通话；

（5） 支持与采用 AMSI 技术的固定电话保密产品实现手机/固话加密互通。

2.3 产品技术指标

（1） 加密通话密钥来源： ECDH 算法或 SM9 算法实时协商密钥；

（2） 录音及语音消息密钥：预置共享密钥；

（3） 语音编码加密算法：AES256 算法或 SM4 算法；

（4） 明密切换方式：按键一键切换；

（5） 密话建立时间：≤11s；

（6） 密话建链成功率：≥95%（手机信号强度不低于-90dBm）；

（7） 密话语音可懂度：≥90%（手机信号强度不低于-90dBm）；

（8） 电源接口：Micro Type C；

（9） 外部尺寸： 84mm x 26mm x 12mm；

（10） 整机重量：30g；

（11） 电池待机时间：≥20 小时；

（12） 连续明话通话时间：≥5 小时；

（13） 连续密话通话时间：≥2 小时；

（14） 电池充电时间：≤1.2 小时；

[②] 语音短消息应支持蓝牙拾音和播放

[③] 支持 EFR 或 AMR FR 编码的 GSM 移动蜂窝信道

3、 产品优势

（1） 同时实现通话保护、语音消息保护、录音保护三大隐私保护；

（2） 数字语音加密调制技术，录音存储或通话线路中传输的密话信号无任何语音特征残留；

（3） 端到端加密通话，无需依赖运营商特殊服务，安全自主可控；

（4） 对音源进行加密，可防范线路、木马、后门等各种窃听手段；

（5） 产品小巧便携(一次性打火机大小)，通过蓝牙功能与手机配对使用；

（6） 仅在需要时开机并进行保密通话，不改变日常手机接听电话习惯；

4、 产品技术方案简介

4.1 产品硬件架构

PVR 蓝牙语音保密器硬件主要由主控处理器、蓝牙芯片、密码芯片、电源管理、模拟硅麦、听筒、充电锂电池等组成。具备产品集成度高、系统可靠性强等特点。

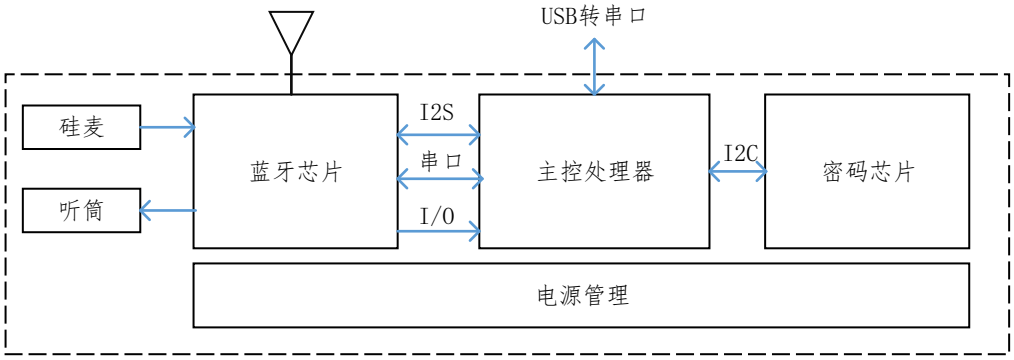

图 2 PVR 蓝牙语音保密器硬件架构

4.2 产品软件架构

PVR 蓝牙语音保密器的软件主要分为三部分：蓝牙处理器软件、主控处理器软件、以及密码处理器软件（密码芯片 COS）。

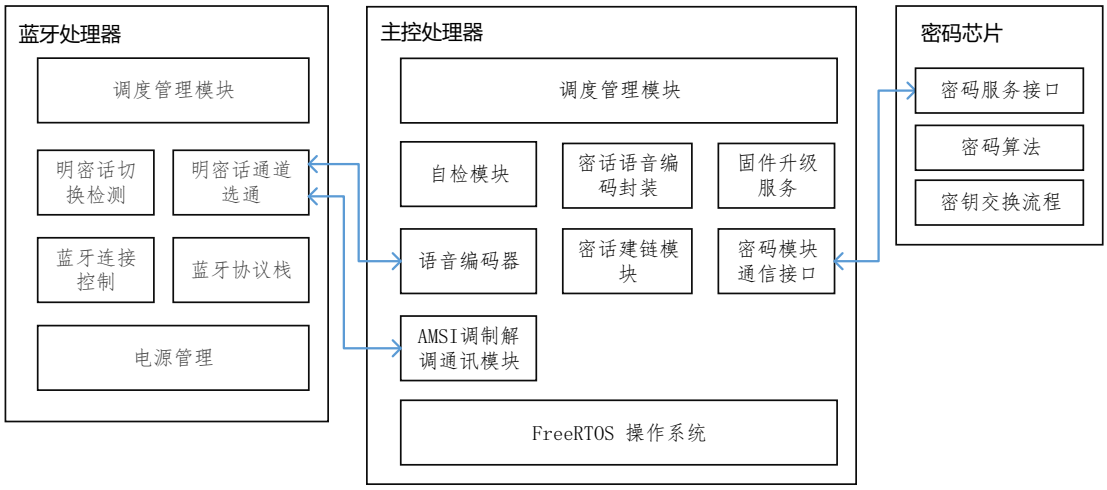

图 3 PVR 蓝牙语音保密器硬件架构

4.3 密话处理流程

以语音加密通话为例，PVR 蓝牙语音保密器的主控处理器进入密话态后，蓝牙处理器打开语音增强模块（用户端音频）与主控处理器的音频通路。此时，主控处理器启动两个处理进程，分别执行明话加密进程和密话解密进程，密话流程严格遵循数字话音加密方案，具体数据处理流程如下图所示。其中，密话解密进程还负责检测线路中的返回明话信号，一旦检测到该信号，主控处理器将停止工作，同时，蓝牙处理器将关闭语音增强模块（用户端音频）、蓝牙协议栈与主控处理器之间的音频通道，并打开语音增强模块（用户端音频）与蓝牙协议栈之间的音频通路，返回明话状态。

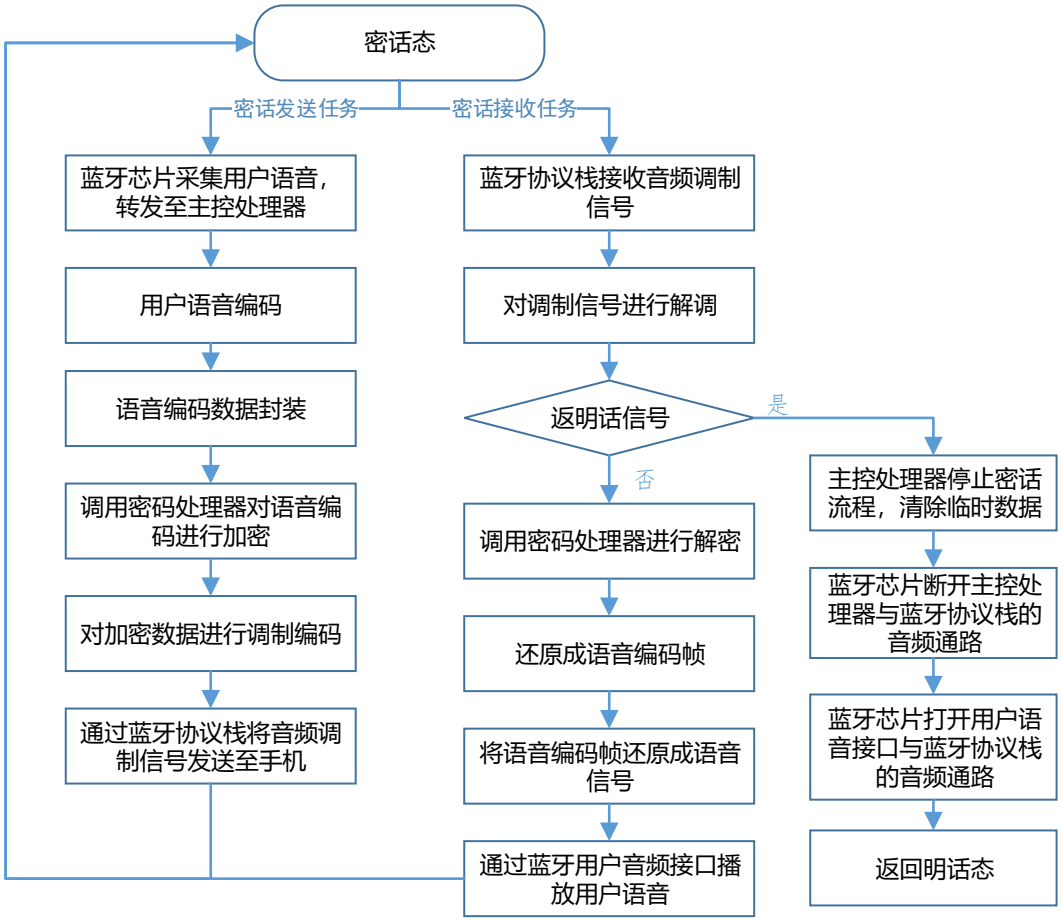

图 4 PVR 蓝牙语音保密器密话处理流程

5、 核心技术

5.1 基于 AMSI 调制解调技术实现数字通讯

为实现在蜂窝移动网络、固定电话网络、以及二者互通环境下的端到端数字话音加密通讯，首先需要基于标准语音信道实现最低 2kbps 至 3kbps 传输速率的高可靠性数据通讯。而目前无论是蜂窝移动网络还是固定电话网的软交换环境，由于声码器算法的存在，传统的 PSK、QAM、OFDM 等调制技术以及近期新出现的类语音、小波调制、余弦调制等方案都无法实现 1.5kbps 以上速率且具备实用性的可靠性数据传输，不具备实现数字话音加密通讯的数据通讯能力。

AMSI 调制解调技术是北京睿语信息技术有限公司研发的一种先进的数字信号调制解调技术，其工作原理与传统的电话 Modem 类似，在发送端，数据流经 AMSI 调制后被转换为模拟调制音，像普通语音电信号一样通过电话、手机、VoIP 语音信道进行传送；在接收端，由 AMSI 将模拟调制音解调后还原成数据流。AMSI

与传统电话 Modem 的区别在于：AMSI 所调制的音频信号在经过中低速率语音声码器压缩还原后依然能够被准确解调，即 AMSI 对中低速率语音声码器有足够穿透能力，从而为通过手机等标准语音信道进行数字话音加密提供了可靠的基础数据通道。

- AMSI 技术目前可穿透的语音编码信道：GSM EFR、UMTS AMR WB、UMTS AMR NB、AMR NB12.2、AMR WB24.4、SILK、OPUS、G.711… ；
- AMSI 技术基本性能：可提供 2Kbps 至 4Kbps 基础通讯带宽，误码率小于 0.2%。

5.2 采用低速率声码器对用户语音进行压缩编码

为实现数字话音加密，同时考虑到移动蜂窝网络以及固定电话网络可支持的数据通信带宽较低，故需要对用户模拟语音进行数字化压缩编码，并尽可能降低语音编码的数据量。因此，PVR 蓝牙语音保密器采用高质量的 1.2kbps 语音编码算法实现语音压缩编码。

5.3 深度定制化的蓝牙语音处理流程

普通蓝牙芯片一般采用 SoC 架构，其内置处理器虽然有一定运算能力，但远远无法满足实时语音编码、信号调制等复杂运算需求，同时，如果在蓝牙芯片音频接口前端串联一个 MCU 用于密话处理，则需要额外增加声码器等器件，同时会造成密话模拟信号在主 MCU 与蓝牙芯片模拟接口传输过程中的衰减及噪声干扰，从而影响密话语音质量。

为此，PVR 蓝牙语音保密器通过对蓝牙芯片内部处理流程的深度定制，通过 I2S 接口实现对蓝牙语音 PCM 的截获与回送，一方面增加了产品的集成度，另一方避免了模拟信号传输引入的噪声干扰，同时利用了蓝牙芯片内置的先进的消噪、消回声算法对原始语音进行增强处理，最大限度保证密话语音音质。

5.4 基于音频信号调制技术实现密钥更新

为了保证录音加密和语音消息加密的安全性，用户需要随时更换密钥，其操作便捷性十分重要。作为蓝牙音频终端，为保证产品的便携性，没有键盘，无法

让用户直接输入密码；而通过 BLE 或 USB 输入密钥，用户在使用上都十分不便。

为此，PVR 蓝牙语音保密器采用了数据调制解调技术，通过独立的手机 APP 将用户输入的密钥字符串调制成音频信号，并通过 A2DP 信道传输至 PVR 蓝牙语音保密器进行识别和解调，实现密钥更新功能。

6、 安全性说明

6.1 数字语音加密

采用音源数字语音加密方案，基于语音压缩编码算法、数据加密算法、以及信号调制解调技术实现。密话时，在录音文件中存储或在移动蜂窝网络信道中传输的“密话语音”完全是数据调制信号，没用任何人声特征，其安全性完全取决于密码算法的强度和密钥的随机性。数字语音加密方案的工作流程如下图所示：

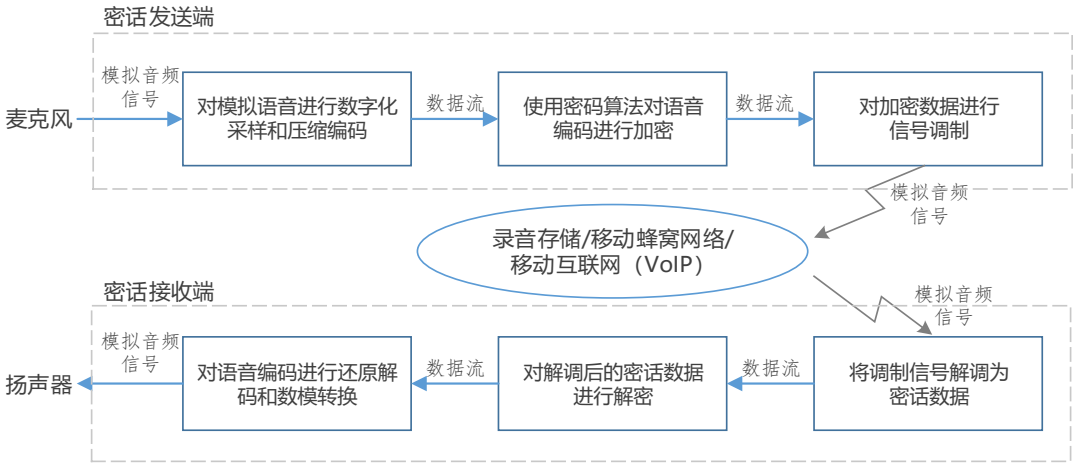

图 5 数字语音加密通讯工作流程

（1） 密话发送端接收用户明话，进行模数转换，并通过声码器对明话语音进行压缩编码；

（2） 使用标准密码算法对语音压缩编码后的数据进行加密；

（3） 将加密后的语音压缩编码密文进行信号调制，产生音频调制信号；

（4） 通过录音软件存储或在移动蜂窝网络传输音频调制信号；

（5） 接收端对音频调制信号进行解调，并使用标准密码算法对解调后的数据进行解密；

（6） 通过声码器算法对解密后的数据进行还原并进行数模转换，最终播放还原后的话音。

6.2 密钥体系及管理

PVR 蓝牙语音保密器所使用的密钥包括：基本密钥、消息密钥、以及用户密钥。

（1） **基本密钥**

由专用管理软件产生，每个 PVR 使用一组，出厂时预置，并可以使用专用软件进行更换；

PVR 蓝牙语音保密器支持 ECDH-256 和 SM9 两种密钥协商算法，两种算法对应的基本密钥也不相同。

对于 ECDH-256 算法，基本密钥主要包含 256 位 ECC 密钥对、组共享密钥。每个密码机具有唯一的 ECC 密钥对，同一用户组的密码机具有相同的组共享密钥。

对于 SM9 算法，基本密钥主要包含 SM9 主加密公钥、设备标识、加密私钥。所有密码机具有相同的 SM9 主加密公钥，每个密码机具有唯一的加密私钥。

（2） **消息密钥**

用于保护电话通话的密钥。在密话通信前，通过在线方式由双方 PVR 协商获得，协商过程使用双方基本密钥作为计算基础，一话一密。密钥协商算法采用 ECDH-256 或 SM9 算法实现。

此外，PVR 还支持用户分组话音保密通信功能，采用 ECDH-256 算法时，此功能通过检测设备标识中的组标志并利用组共享密钥实现；采用 SM9 算法时，此功能通过检测设备标识中的组标志实现。

（3） **用户密钥**

用于保护录音和语音消息的密钥，由用户通过专用软件进行设置。当多个用户在使用加密语音消息进行交流时，各方都应设置相同的用户密钥。

6.3 密钥协商算法

PVR 蓝牙语音保密器支持 ECDH256 及 SM9 两种密钥协商算法，用户可根据需要进行选择。

6.3.1 ECDH 密钥协商算法

采用 ECDH-256 算法实现密钥协商时，密码机所使用的基本密钥是预存的 256 位 ECC 密钥对，同时参与计算的还有设备标识 ID（其中包含该设备的组标记 GID），以及预置的组共享密钥。

ECDH-256 密钥协商流程如下图所示。在协商过程中，双方需要交换设备标识、随机数、以及基本密钥中的公钥。

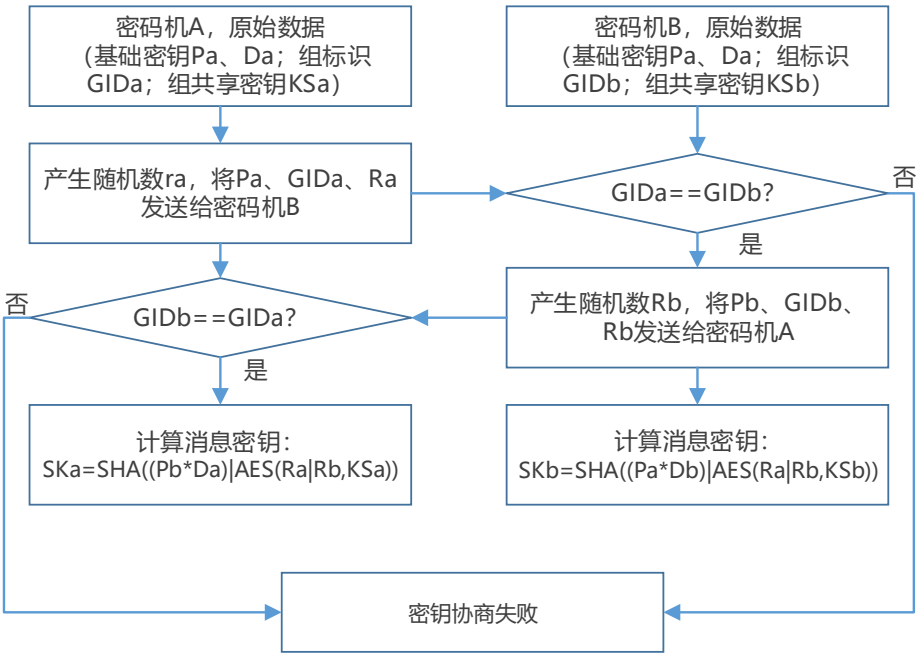

图 6 ECDH 算法流程

用户分组管理是通过验证对方设备标识 ID 中的组标记 GID 来实现的，即：如对方的组标识 GID 与本方不相同，则终止通信；同时，通过使用组共享密钥参与消息密钥计算的方案，防止非法用户通过伪造设备标识进行欺骗。

在 ECDH-256 密钥协商过程中，使用随机数参与消息密钥计算，即使是相同的两个用户，每次进行话音保密通信所产生的消息密钥也均不相同，以此保证一话一密。

6.3.2 SM9 密钥协商算法

采用 SM9 算法实现密钥协商时，密码机所使用的基本密钥是预存的 SM9 的加密主公钥、加密私钥，参与计算的还有设备标识 ID（其中包含该设备的组标记）。

SM9 密钥协商流程如下图所示。在协商过程按照 SM9 算法标准执行。

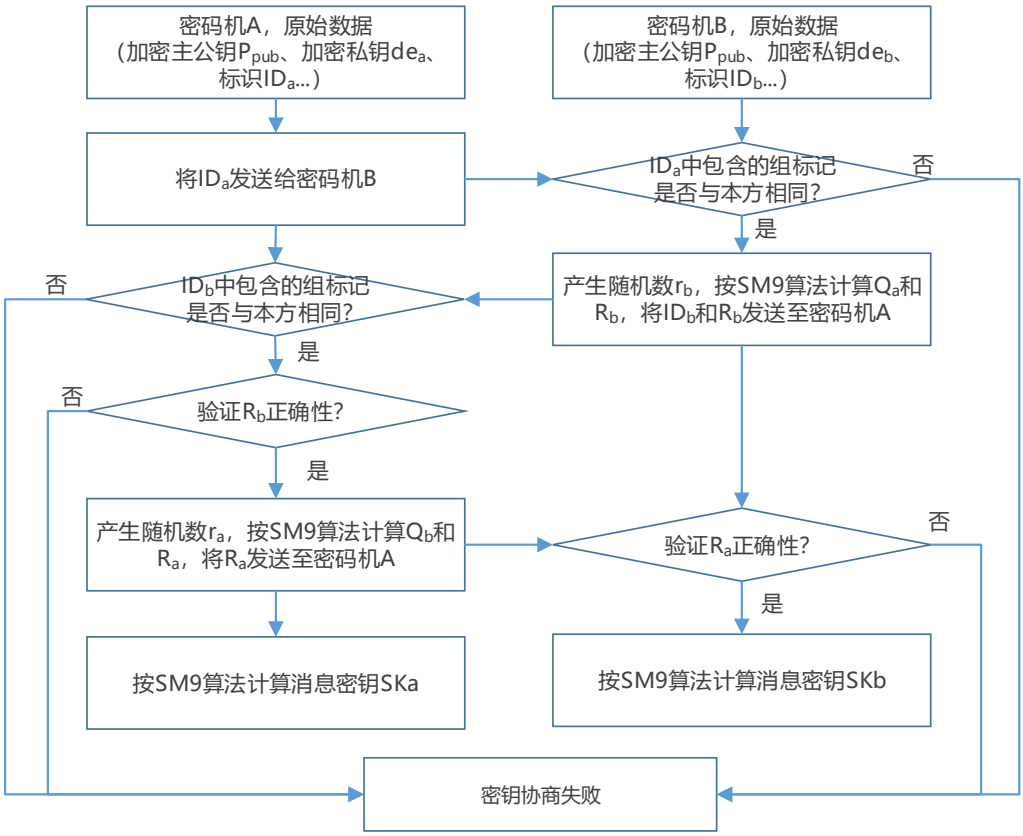

图 7 SM9 算法流程

用户分组管理是通过验证对方设备标识中的组标记来实现的，即：如对方的组标识与本方不相同，则终止通信。由于 SM9 算法本身杜绝了设备标识被篡改的可能性，所以可以防止非法用户通过伪造设备标识进行欺骗。

同时，SM9 算法使用随机数参与消息密钥计算，即使是两个相同用户每次进行话音保密通信所产生的消息密钥也均不相同，以此保证一话一密。

6.4 语音数据加密算法

PVR 蓝牙语音保密器支持 AES-256 及 SM4 两种密码算法实现话音加密，用户可根据需要进行选择。

由于密话通信对实时性要求高，且基于蜂窝移动网络的数据调制解调方案无法保证密话数据传输零误码，所以实际应用时，密码机采用 CTR 模式的 AES-256/SM4 算法（流加密方案）对语音编码数据进行加解密计算，流程如下：

（1） 发送端 PVR 按固定分包方式对明话语音编码数据流进行分帧，并为每一帧数据产生一个 Kid；

（2） 发送端 PVR 使用消息密钥对 Kid 进行 AES-256/SM4 算法加密，并使用加密后的结果对明话编码数据帧进行异或计算，生成密话语音数据；

（3） 发送端 PVR 将 Kid 及密话编码数据一起发送给接收端 PVR；

（4） 接收端 PVR 使用消息密钥对收到的 Kid 进行 AES-256/SM4 算法加密，并使用加密后的结果对密话编码数据帧进行异或计算，还原成明话语音编码数据。

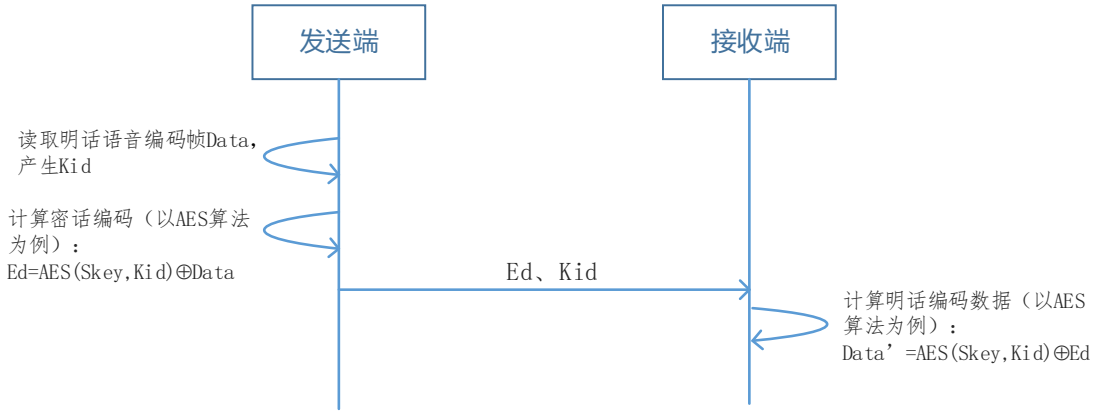

图 8 加密通话过程中语音编码加解密流程

7、 产品使用说明

7.1 配对

打开电源开关，长按 5 秒功能键，进入配对状态，此时蓝牙指示灯快闪，使用手机搜索 PVR 设备进行配对。

7.2 切换设备安全模式

PVR 蓝牙语音保密器具有两种安全模式：***通话保密模式***、***录音保密模式***，PVR 开机后默认为***通话保密模式***，用户可以通过快速双按功能键来切换安全模式。

7.3 通话加密

打开电源开关，PVR 自动回连已配对设备，将设备设置为***通话保密模式***，在***通话保密模式***下，用户可以使用 PVR 进行明话通话，并在明话过程中通过按下功能键切换明密话状态。

7.4 录音及语音消息加密

打开电源开关，PVR 自动回连已配对设备，将设备设置为***录音保密模式***，此时安全指示灯常亮，使用支持蓝牙拾音/播放功能的录音或语音消息软件，即可执行加密录音/解密播放，以及语音消息加密发送/收听。

注意：在***录音保密模式***下，用户无法使用 PVR 进行明话通话。

7.5 更新用户密钥

用户密钥用于对在录音/放音时，以及语音消息发送/接听时对语音进行加解密处理。

更新用户密钥前，首先需要将 PVR 设置为***录音保密模式***，同时在与 PVR 配对的手机上安装 PVR 密码管理 APP。通过 PVR 密码管理界面输入密钥，并执行发送操作，即可将密钥下载到 PVR 设备中，用户密钥更新成功后，PVR 的安全指示灯将慢闪 3 秒，然后恢复常亮。

8、 产品限制性说明

（1） 在使用 PVR 蓝牙语音保密器的录音加密及语音消息加密功能时，相应的应用软件必须支持蓝牙设备拾音和放音；

（2） PVR 蓝牙语音保密器通过蓝牙功能与手机通讯时，因外界信号干扰（尤其是 2.4G WiFi），可能导致密话音频信号丢失或变形，从而使密话出现变调、丢音、加入噪音等现象；

（3） 通过 PVR 蓝牙语音保密器进行蜂窝语音通话时，蜂窝网络信号质量对密话音质影响很大，蜂窝网络信号质量差将导致 AMSI 数据通讯误码增加，从而使密话音质变差；

（4） PVR 蓝牙语音保密器无法支持所有的 VoIP 应用实现加密通话，主要原因是有些 VoIP 会将密话语音作为噪音进行消噪处理，导致密话信号变形而无法解码。

9、 产品适用性说明

9.1 蜂窝语音加密通话功能

9.1.1 支持的手机品牌型号

品牌	型号
苹果	iPhone 8/X/11/12
华为	Mate20/Mate30/Mate40 系列、P30/P40 系列
三星	S10/20 系列、Note10/20 系列
其他	大部分采用骁龙 845/855/865 芯片的手机 大部分采用麒麟 970/980/990 芯片组的手机

9.1.2 蜂窝电话语音编码制式支持情况

PVR 蓝牙语音保密器所支持的蜂窝电话语音编码制式包括：

蜂窝网络	编码方式	支持程度
GSM	GSM EFR	支持
	GSM FR	不支持
	GSM HR	不支持
UMTS/WCDMA	UMTS AMR_NB	支持
	UMTS AMR_WB	支持
CDMA	EVRB	不支持
CDMA2000	EVRB	不支持
VoLTE	AMR_NB	支持
	AMR_WB	支持

9.1.3 国内运营商及网络支持情况

2020 年 11 月，按有关单位要求，我公司在北京、上海、广州、沈阳、西安、拉萨、新疆、成都 8 个城市对 PVR 蓝牙语音保密器进行了跨网络、跨地域、跨手机平台的通联性测试，测试内容涵盖了建链成功率、建连时间、密话可懂度、密话稳定性等各个方面。测试结果如下所示，显示出 PVR 具备很好的线路适应性和稳定性。

通话 A 端 / 通话 B 端		中国移动		中国联通		中国电信
		2G	VoLTE	3G	VoLTE	VoLTE
中国移动	2G	部分支持	支持	部分支持	部分支持	部分支持
	VoLTE	支持	最佳	支持	支持	支持
中国联通	3G	部分支持	支持	支持	支持	支持
	VoLTE	部分支持	支持	支持	最佳	支持
中国电信	VoLTE	部分支持	支持	支持	支持	最佳

目前，国内移动、联通、电信已基本做到了 VoLTE 全覆盖，为用户使用 PVR 进行加密通话提供了良好的线路基础。

9.1.4 境外运营商及网络支持情况

PVR 蓝牙语音保密器已在全球 20 多个国家（亚洲：菲律宾、马来西亚、印度尼西亚、蒙古等，非洲：埃及、肯尼亚、朱巴等，欧洲：俄罗斯、保加利亚，南美洲：智利、秘鲁，中东：沙特阿拉伯、伊朗等）的 40 余家移动运营商有过实用案例，从结果来看，PVR 在境外同样具备良好的适用性：

（1） 在所有国家,都支持基于当地 UMTS/VoLTE 蜂窝语音网络进行加密通话；

（2） 在大部分国家，支持两个以上的运营商之间实现跨运营商加密通话；

（3） 在多数国家，支持一种以上的国内卡（联通、移动、电信）实现漫游加密通话；

9.2 VoIP 通话加密功能

虽然大多数公共 VoIP 应用都能够为 PVR 加密通话提供足够的音频带宽，但不幸的是，很多 VoIP 软件的消噪算法会将 PVR 的密话音频信号作为噪音进行消除，导致密话信号在解调时误码激增，从而使加密通话效果变差。

目前，我们能够确认 PVR 加密通话效果较为优异的 VoIP 应用是 FaceTime 和 WhatsApp，对于其它 VoIP 应用，需要客户自行测试。

9.3 语音消息加密功能

语音消息应用	iOS	Android
微信	支持	支持
钉钉	支持	不支持
WhatsApp	支持	不支持

目前，对于 iOS 系统，多数语音消息应用可以支持蓝牙拾音功能，即能够使用 PVR 加密语音消息；而对于 Android 系统，除微信以外，其它语音消息应用都不支持蓝牙拾音功能，故在 Android 系统下仅微信可支持 PVR 加密语音消息。

9.4 录音加密功能

经测试发现，目前 iOS 系统内置的录音软件可以支持蓝牙拾音，故 iPhone 手机都支持使用 PVR 进行加密录音；然而，华为、小米、三星等手机，其系统原生的录音软件都不支持蓝牙拾音功能，也就无法使用 PVR 进行加密录音。

为了使用 Andorid 系统手机进行加密录音，用户可以下载第三方支持蓝牙拾音功能的“录音机”软件。

另外，我们有理由相信，随着蓝牙耳机被普遍使用，主流品牌手机的原生语音应用会逐步支持蓝牙拾音功能。