

睿语™语音加密技术

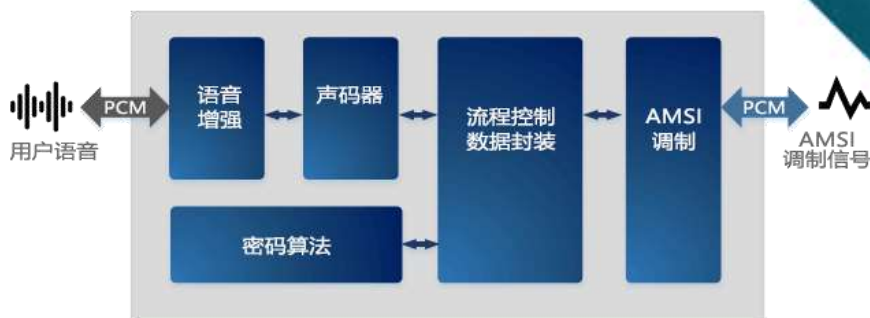
睿语™语音加密方案以睿语公司具有领先地位的 AMSI 调制解调技术为基础，集成高品质声码器算法、高安全等级密码算法、以及高效数据通讯协议，支持高可靠性数据传输、高实时性数据传输两种工作模式，实现了电话加密通讯所需的数字信道训练、加密密钥协商、数字语音编码加密、以及数据通讯等全部功能，是目前国内外唯一采用数字语音加密技术实现座机、手机、卫星电话等各类电话终端加密互通的产品方案。

什么是 AMSI?

AMSI 技术由北京睿语公司研发，其全称是“能够对抗音频压缩算法干扰的带语音激励机制的先进信号调制解调算法”。AMSI 融合了语音编码技术、信号调制技术、信号同步技术、频域/时域补偿技术、信号形变修正技术、纠错算法等多种技术，主要用于在有损语音信道内实现高可靠性数据传输。

AMSI 的工作原理与传统的电话 Modem 类似，在发送端，数字信号经 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 链路进行传送；在接收端，由 AMSI 将模拟调制音解调后还原成数字信号。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语音加密提供了可靠的基础数据通道。

睿语™系统架构



特点

- 集成 700bps/1300bps/2400bps 语音压缩算法，可根据线路质量选择密话音质
- 采用 CTR 加密模式，可选择 AES-256、SM4 等各类高强度加密算法
- 提供 SM9 或 256 位 ECDH 密钥交换算法，支持用户自定义密钥协商协议
- 具备两种数据源传输模式：高可靠性数据传输、高实时性数据传输，可分别用于密钥交换及语音加密数据通讯
- 内置抗语音增强算法，可抵消因电话终端设备内置消噪功能导致的 AMSI 调制信号衰减现象
- 独创 RAEC 线路回声消除算法，有效解决线路回声对双工数据传输的误码影响
- 内置消噪、消回声算法

最安全的加密通话方案

100%数字加密

先对用户语音进行数字化压缩编码，再对编码数据进行加密及调制，密话与白噪声一致，与模拟语音加密产品相比，绝无可懂度残留，从根本上屏蔽了监听者采用音频分析法对语音弱点进行攻击的可能性。

强度符合最严苛的安全标准

采用 CTR 模式 AES-256、SM4 等算法。每秒密钥更换 2 次以上，即使通话 4 小时，密钥也绝无重复。

端到端全程保护

在各种标准语音信道内实现端到端加密通话，无需任何第三方服务商提供特殊的线路或运维支持，密钥完全自主管理，避免了服务商有意或因管理技术漏洞导致的失密事件。



数字语音加密

模拟语音加密技术已完全落后，其无论采用多复杂的变换方法，都无法去除语音特征，为监听者留下可乘之机，通过以下链接，您可以清晰的分辨出通过模拟加密与通过数字加密后的密话语音之间的差别，安全性不辩自明。

<http://www.voclar.com/zh/rstec/#sc>

适用于各种语音通讯线路

睿语™将用户语音加密后再交给普通语音终端进行常规操作，与通话设备及线路无关，可应用于手机、座机电话、VoIP、对讲机、短波/超短波电台、语音短信等，实现通讯类型全覆盖。



可定制化的技术方案

睿语™语音加密方案实现了加密通话的全部功能，方案设计充分考虑应用需求，具备丰富的扩展性、延伸性，既可用做完整的新产品开发方案，又可以作为一个协处理模块集成到各种通用语音通讯产品方案中，全面满足现有资源整合及新产品开发的需求。

我们充分理解不同行业客户对加密通话产品的特殊需求及安全关切，基于先进的 AMSI 技术和完整的睿语™语音加密方案，致力于为行业客户以及产业用户提供最优秀的语音通讯安全解决方案，协助客户快速开发符合业务需求且极具竞争优势的语音通讯安全产品。

实现密话跨网互通

睿语™能够透过普通语音信道实现数字加密通讯，打破了因终端设备不同、通讯技术标准不同、运营商不同等因素造成的数据互通瓶颈，是目前全球唯一具备实用性的，能够实现跨网互通的数字语音加密方案，真正做到：语音通，则密话通。

