ReliaSpeak

PVR BT Voice Protector

White Book V1.2

Protect call, voice message and recording privacy

Reliaspeak Information Technology Co., Ltd.

Tel：8610-88334733
www.reliaspeak.com
support@reliaspeak.com

Statement

PD：2021/02

Catalog

1. Outline

1.1 Background

Voice, as one of the most common information carriers, can not be replaced by other carriers such as text, picture and image in the aspects of information recording and information exchange, real-time, convenience and uniqueness. With the rapid development and popularization of communication technology, it has become everyone's daily behavior to store voice through electronic media and to transmit voice through the network, but accompanied by the increasing risk of state secrets, business secrets and personal privacy.

How to protect the voice security? How to prevent the private information contained in voice from being stolen by illegal persons during storing and exchange? At present, there are many mature technical solutions and products, for example: audio file encrypted storage, encrypted VoIP system, encrypted landline products based on v.32 and other Modem technologies, 3G or VoLTE encrypted mobile phone provided by telecom carriers, etc.

However, these solutions and products have some following problems more or less:

1. Self-contained, only suitable for a specific region, telecom carrier or communication method, can not implement intercommunication.
2. Have to rely on or trust the specific service provider in terms of security, can not achieve security autonomous.
3. Too narrow security boundary, the security chain has no complete closed loop, and has security vulnerabilities.

Therefore, based on AMSI Modem technology as core, combined with narrow band voice coding technology and high level cryptographic algorithm, Reliaspeak Information Technology Co., Ltd. developed voice encrypted coder solution, provide an encrypted voice product for user with security chain complete closed loop, security autonomous and controlled, suitable for different region, telecom carriers

and communication styles.

1.2 Product Introduction

The core of PVR is voice encrypted coder, it can convert normal voice audio signal to encrypted audio signal by voice coding, digital encrypting, signal modulating and other processes. The encrypted audio signal has the following 3 features:

1. The encrypted audio signal has no any phonetic characteristic and intelligibility, can only be decoded and restored to understandable normal voice audio signal with correct key.
2. The encrypted voice audio signal can be coded and stored by recording programs, and will be decoded and restored when playing.
3. Encrypted voice audio signal can be transmitted through landline channel, cellular voice channel and VoIP channel as the ordinary analog voice, and can be decoded and restored at the receiving end.

PVR can be used with smartphone or other intelligent terminal, to realize **encrypted recording, encrypted voice messages, encrypted mobile calls, encrypted VoIP calls**, etc.

PVR realizes voice source protection, can resist eavesdropping risks at maximum, including telecom carrier, network, SS7, pseudo base station and other lines eavesdropping, and phone spyware, backdoor local eavesdropping.

2. Functions and Specifications

2.1 Appearance

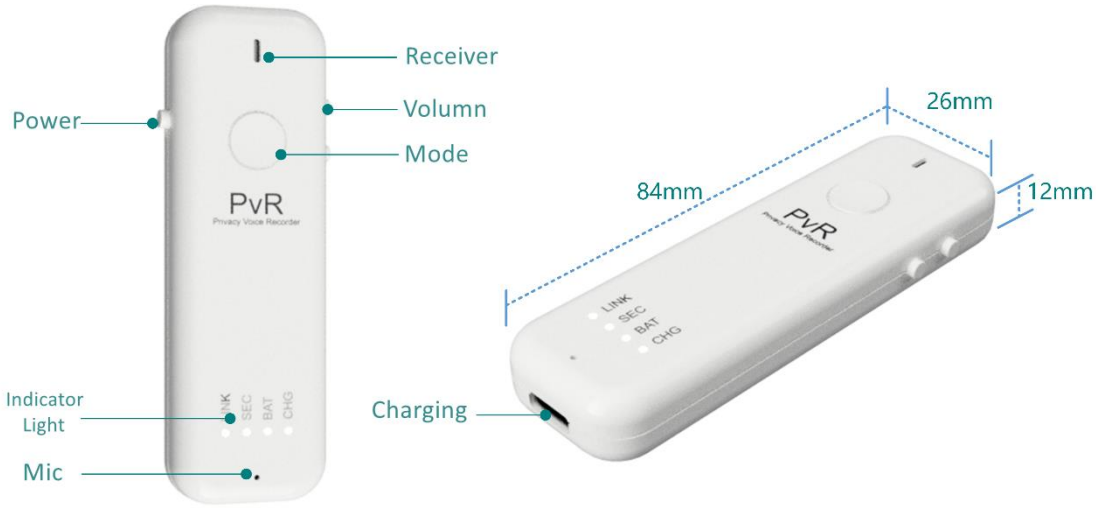

Figure 1 PVR Overview

2.2 Main Functions

1. Working with phone recording Apps[①], can realize voice encrypted recording.
2. Working with phone voice message Apps[②] (for example: the We Chat voice message function), can realize voice encrypted messages.
3. Realize GSM[③], UMTS, VoLTE cellular voice encrypted calls.
4. Working with phone VoIP Apps, to realize VoIP encrypted calls
5. Support to intercommunicate between smartphone and landline using AMSI technology.

2.3 Specifications

1. Encrypted Calls key source: ECDH real-time key agreement

① Recording Apps should support BT sound pick-up and play.

② Voice message Apps should support BT sound pick-up and play.

③ Support EFR or AMR FR coded GSM mobile cellular channel.

2. Recording and voice messages key: Preloaded shared key.
3. Voice coding cryptographic algorithm: AES256
4. Normal/Encrypted switch: One button switching
5. Encrypted call switching time: ≤11s
6. Encrypted call switching success rate: ≥95% (signal strength no lower than -90dBm)
7. Encrypted call intelligibility: ≥90% (signal strength no lower than -90dBm)
8. Charging Port: Micro Type C
9. Dimension: 84mm x 26mm x 12mm
10. Weight: 30g
11. Battery standby: ≥20hs
12. Normal calls time: ≥5hs
13. Encrypted calls time: ≥2hs
14. Charging time: ≤1.2hs

3. Advantages

1. Realize call, voice messages, recording privacy protection at the same time
2. Digital voice encryption modulation technology, recording storage or encrypted voice signal transmitted in the communication line without any phonetic intelligibility residual
3. End to end encrypted calls, without relying on telecom carriers' special services, security can be autonomous and controlled.
4. Voice source encryption, can prevent various eavesdropping such as

lines, Trojans and back doors.

5. Small and portable (disposable lighter size), pairing and working with mobile phones via BT.

6. Only use when need to make encrypted calls, voice messages, recordings, VoIP calls, without changing the daily habit of phone usage.

4. Technical Solution Introduction

4.1 Hardware Framework

PVR hardware is mainly composed by MCU, BT chipset, cryptographic chipset, Power Management, analog silicon MIC, Receiver, rechargeable Li-On battery. It has features of high integrating, strong system reliability and so on.

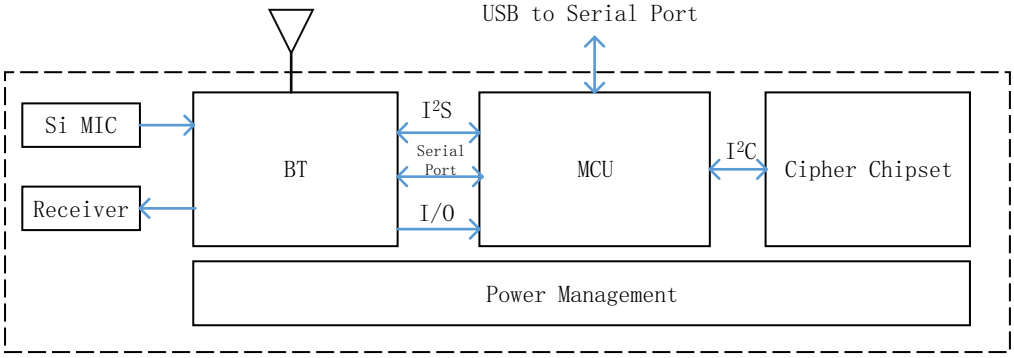

Figure 2 PVR Hardware Frame

4.2 Software Framework

PVR Software is mainly divided to 3 parts: BT processor software, MCU software and cryptographic processor software (cryptographic chipset COS).

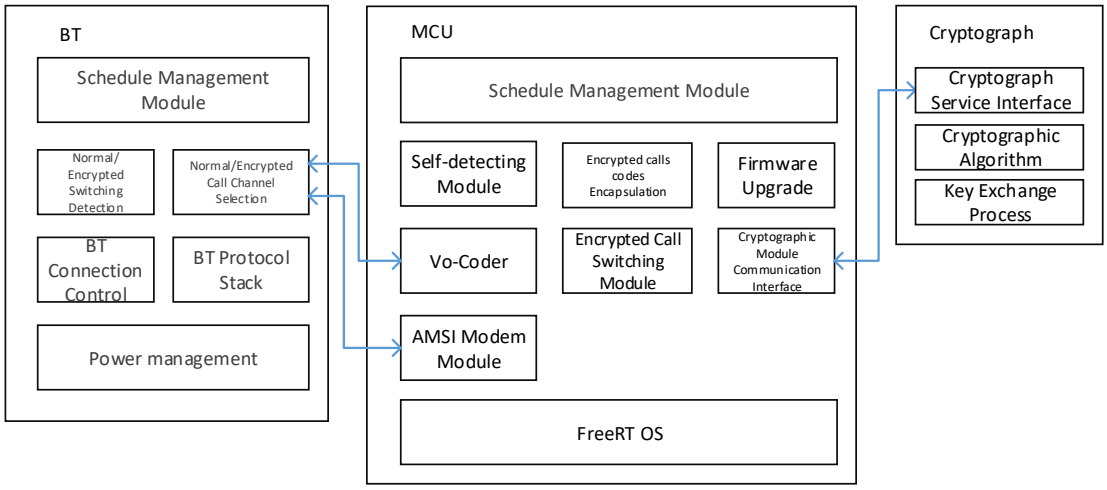

Figure 3 PVR Software Frame

4.3 Encrypted call process

Take encrypted call as an example, after PVR MCU entering to encrypted mode, BT processor opens voice enhancement module (users end audio) and MCU processor audio channel. At this time, MCU will initiate two processes, executing normal call encrypting and encrypted call decrypting. Encrypted call process strictly follow digital voice encryption solution, the specific data process is shown in the figure below. In which, encrypted call decrypting process will also detect normal call signal returned in line, once detected, MCU will stop working, meantime, BT processor will close the audio channel of voice enhancement module (user end audio), BT protocol stack and MCU processor, and open audio channel of voice enhancement module (user end audio) and BT protocol stack, return to normal mode.

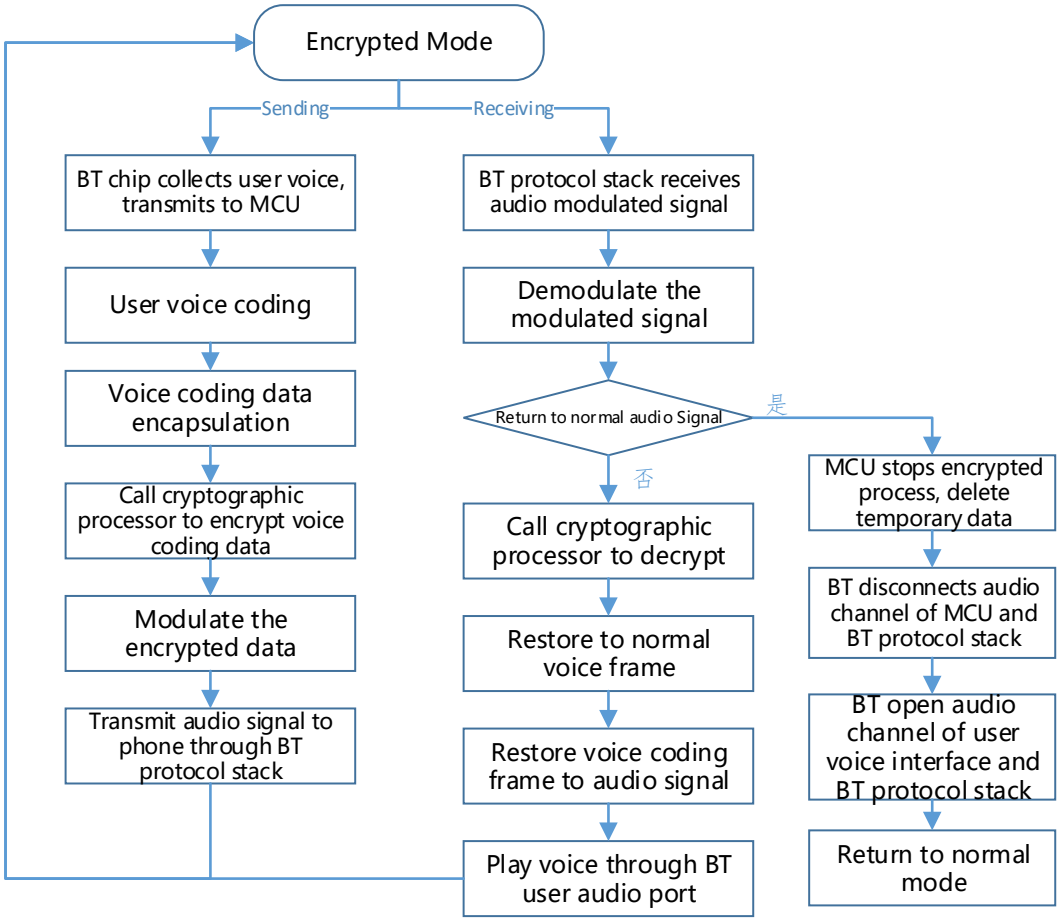

Figure 4 PVR Encrypted Call Process

5. Core Technology

5.1 Based on AMSI MODEM technology to implement digital communication

In order to implement end to end digital voice encrypted communication under cellular mobile network, landline network, or intercommunication between the two networks, firstly it is required to transmit minimum rate of 2kbps to 3bps high reliable data to communicate based on standard voice channel. However, no matter cellular mobile network or landline network soft-switch environment, because of the existence of Vo-coder algorithm, the traditional PSK, QAM, OFDM modulation technology as well as the new speech-like, wavelet modulation, cosine modulation and other solutions can not implement a practical reliable data transmission with a rate of 1.5bps or higher, and have no data communication ability to implement digital voice encrypted communication.

AMSI Modem technology is an advanced digital signal modulation and demodulation technology developed by Reliaspeak Information Technology Co., Ltd. Its work principle is the same as the traditional telephone Modem, at the sending end, data stream is modulated by AMSI and converted to analog modulation voice, transmitted through telephone, mobile phone, VoIP voice channel as the ordinary voice electrical signal. At the receiving end, the analog modulation voice is demodulated by AMSI and restored to data stream. The difference between AMSI and traditional Modem is: the audio signal modulated by AMSI could still be demodulated accurately after being compressed and restored by medium and low rate Vo-coder. That is, AMSI has the sufficient penetration ability for medium and low rate Vo-coder, thereby providing reliable basic data channel for digital voice encryption through mobile phone and other standard voice channels.

- The voice coding channel can be currently penetrated through by AMSI: GSM EFR、UMTS AMR WB、UMTS AMR NB、AMR NB12.2、AMR WB24.4、SILK、OPUS、G.711…
- The basic performance of AMSI: provide 2kbps to 4kbps basic communication bandwidth, and the error rate is less than 0.2%.

5.2 Adopt low-rate Vo-coder to compress user's voice

In order to implement digital voice encryption, meantime considering the low digital communication bandwidth supported by mobile cellular network and landline network, it is required to digitally compress user's analog voice, and decrease the voice coding data quantity as much as possible. Therefore, PVR adopts high quality 1.2kbs voice coding algorithm to implement voice compressing.

5.3 Deep customized BT voice process

Normal BT chipset usually adopts SoC frame. Although its inner processor has some computing power, it is far from being able to do the complicated computing requirement such as real-time voice coding, signal modulation, etc. Meanwhile, if serially connect a MCU to the front side of the BT chipset audio port for encrypted

voice process, the additional component such as Vocoder will be required, and will cause encrypted analog signal, which is transmitted between MCU and BT chipset analog port, attenuation and noise interference, resulting the decreasing of encrypted voice quality.

Therefore, through deeply customization of the BT chipset inner process, implement the interception and resend of BT voice PCM via I^2S port. On the one hand increased the product integration, on the other hand eliminated the noise interference what is caused by analog signal transmission, meantime uses BT chipset inner preloaded advanced noise cancellation and echo cancellation algorithm to enhance the original voice, so that can guarantee the encrypted voice quality maximum.

5.4 Based on audio signal modulation technology to implement key updating

In order to guarantee the security of the encrypted recording and voice messages, user needs to update key periodically, the operation convenience will be very important. As a BT audio terminal, in order for the product convenience, there is no keyboard for user to type in the passwords directly. While it is inconvenient for user to input password using BLE or USB.

Therefore, PVR uses digital MODEM technology, modulate the password characteristic stings input by user through independent mobile App into audio signal, and transmit to PVR through A2DP channel to recognize and demodulate, to implement the key updating function.

6. Security Introduction

6.1 Digital voice encryption

Uses voice source digital encryption solution, based on the compressed voice coding algorithm, digital cryptographic algorithm and signal Modem technology to implement. In the encrypted mode, the “encrypted voice”, which is stored as recording file or transmitted in the mobile cellular network channel, is totally

modulated data signal, and there is no any human phonetic characteristic. The security is totally depends on the strength of the cryptographic algorithm and the randomness of the key. Digital voice encryption solution work flow is shown as the figure 5.

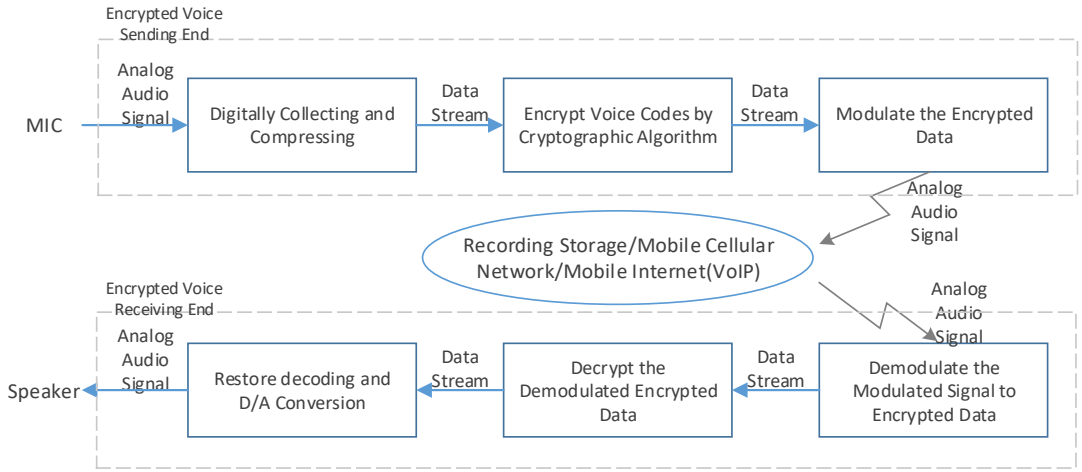

Figure 5 Digital Voice Encryption Communication Work Flow

1. The encrypted voice of the sending end receives the normal voice, do the A/D conversion, compress the normal voice by Vo-coder.
2. Use standard cryptographic algorithm to encrypt the compressed data.
3. Modulate the encrypted voice data which is compressed into audio modulation signal.
4. Store or transmit the audio modulation signal by recording software or mobile cellular network.
5. The receiving end demodulate the audio modulated signal, uses standard cryptographic algorithm to decrypt the demodulated data.
6. Restore the decrypted data and do the D/A conversion by Vo-coder, play the restored voice.

6.2 Key system and management

The key used by PVR includes: basic key, message key and user key.

1. Basic Key

Generated by specified management software, every PVR uses one group, factory preloaded, can be replaced using specified software.

PVR supports ECDH-256 key agreement algorithm.

For ECDH-256 algorithm, basic key mainly includes 256 bit ECC key pair, group shared key. Every cryptograph has the only ECC key pair. The same user group cryptograph has the same group shared key.

2. Message Key

Message key is used to protect the encrypted calls. Before the encrypted call, it can be agreed and obtained online by both PVR sides. The agreement process use both sides basic key as calculation basis, one time pad. Key agreement algorithm uses ECDH-256 to implement.

What's more, PVR also supports user group encrypted voice communication function. When use ECDH-256 algorithm, it could be implemented by verifying group ID of device ID and using group shared keys.

3. User key

User key which is used to protect recording and voice messages, is set by users with specified software. When multiple users communicate with encrypted voice messages, each user should set the same user key.

6.3 Key agreement algorithm

PVR supports ECDH-256 key agreement algorithms.

When use ECDH-256 algorithm to implement key agreement, the basic key used by cryptograph is the preloaded 256 bit ECC key pairs, the device ID (including the

device group ID) will also participate in the calculation, and preloaded group shared keys.

The ECDH-256 key agreement process is shown as the below figure. During the agreement, both sides need to exchange device ID, random number, and the public key of the basic key.

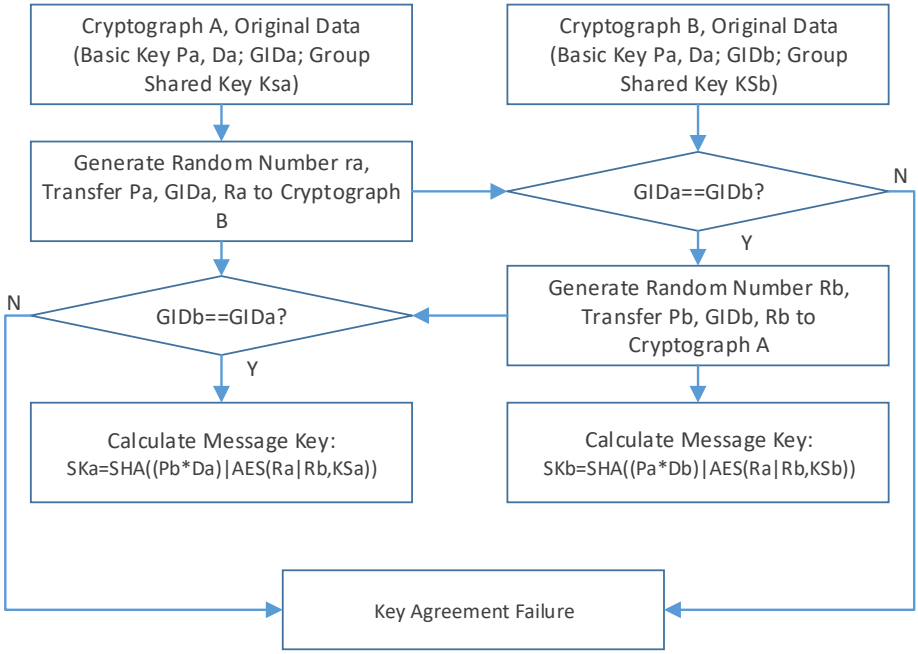

Figure 6 ECDH Algorithm Process

The user group management is implemented by verifying group ID of the other side device ID, that is, if the other side group ID is different from local side, the communication will be terminated. Meanwhile, the solution which uses group shared keys to participate message key calculation, can prevent illegal users from cheating by forging device ID.

During the ECDH-256 key agreement process, random number is used to participate in calculation of message key. The message keys generated by two same users who make encrypted calls each time are different, so as to ensure one time pad.

6.4 Voice data cryptographic algorithm

PVR supports AES-256 cryptographic algorithm to realize encrypted communication due to the high real-time requirement of encrypted communication, and digital

MODEM solution based on cellular mobile network can not guarantee zero error bit of transferring, in the real application, cryptograph uses CTR mode of AES-256 cryptographic algorithm (stream encryption solution) to encrypt and decrypt the voice coding data. The process is:

1. The PVR sending end divides the normal call voice coding data into frames according to the fixed packet, and generate a Kid for each frame.
2. The PVR sending end uses message key to encrypt Kid with AES-256 cryptographic algorithm, and uses encrypted results to calculate the normal call coding data frame with XOR, generates the encrypted voice data.
3. The PVR sending end sends Kid and encrypted coding data to receiving end.
4. The PVR receiving end uses message key to encrypt the received Kid with AES-256 cryptographic algorithm, and uses encrypted results to calculate the encrypted coding data frame with XOR, restore to normal voice coding data.

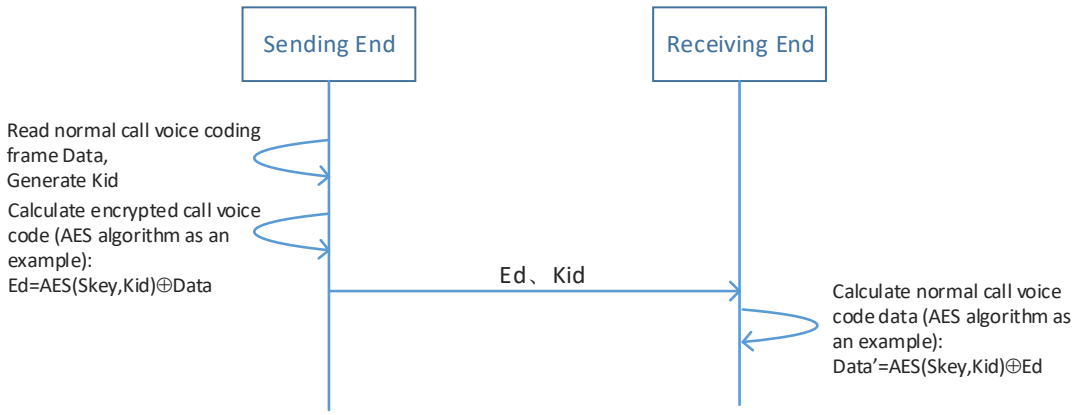

Figure 7 Voice Coding Encryption/Decryption Process During the Encrypted Call

6.5 Pairing

Turn the power on and long press the function button to enter to pairing mode, the BT indicator light will flash quickly. Please use phone to search PVR device to pair

with.

6.6 Security mode switching

PVR has two security mode: **encrypted calls mode and encrypted recording mode.** It is set to **encrypted calls** mode by default when the power is on. It could be switched to the security mode by double pressing the function button quickly.

6.7 Encrypted Calls

PVR will reconnect to the paired device when the power is on. Set to **encrypted calls mode**, PVR could be used to make encrypted calls, and could switch the encrypted and normal mode by pressing the function button.

6.8 Recording and voice messages encryption

PVR will reconnect to the paired device when the power is on. Set to **encrypted recording mode**, the security indicator light will always on. Use the recording or voice messages Apps which support BT sound pick-up and play function to record and play voices, or send and play the voices messages.

Note: in the encrypted recording mode, PVR can not be used for encrypted calls.

6.9 User's key updating.

The User's key is used to encrypt and decrypt when recording or playing the voices, or sending or receiving the voices messages.

Before updating the User's key, please set the PVR to the encrypted recording mode, and download and install the password management App on the paired smartphone. Download the key into PVR by entering the password and sending from the PVR password management interface. When the User's key updates successfully, the PVR security indicator light will flash slowly for 3s and return to always on.

7. Product Limitation

1. When using the encrypted recording and encrypted voice messages

functions of PVR, corresponding Apps must support BT sound pick-up and play.

2. When PVR communicates with smartphone through BT, it may cause loss or deformation of encrypted audio signal due to the interference of external signal (especially for 2.4 Wi-Fi), resulting tone-changing, loss, noise addition, etc. of encrypted voice.

3. The cellular network signal quality will have a great influence on the encrypted voice quality when using PVR for encrypted communication. The poor cellular network signal will increase the AMSI data communication error rate so that the encrypted voice quality will be worse.

4. PVR could not support all the VoIP Apps to realize encrypted communication. The main reason is that some VoIP will do the noise cancellation process for the encrypted voice as noise, what will cause the encrypted signal deformed and can not be decoded.

8. Applicability Indroduction

8.1 Cellular voice encrypted communication function

8.1.1 **Supported Smartphone Brand and Model**

Smartphone	Model
iPhone	iPhone 8/X/11/12
Huawei	Mate20/Mate30/Mate40 series、P30/P40 Series
Samsung	S10/20 Series、Note10/20 Series
Others	Most smartphones with Snapdragon 845/855/865 Chipsets Most smartphones with Kirin 970/980/990 Chipsets

8.1.2 **Cellular Calls Voice Coding Standard Support Condition**

Supported cellular calls voice coding standards by PVR include:

Cellular Network	Coding Method	Support
GSM	GSM EFR	Y
	GSM FR	N
	GSM HR	N
UMTS/WCDMA	UMTS AMR_NB	Y
	UMTS AMR_WB	Y
CDMA	EVRB	N
CDMA2000	EVRB	N
VoLTE	AMR_NB	Y
	AMR_WB	Y

8.1.3 **Overseas Telecom Carriers and Network Support Condition**

PVR has been used under over 40 mobile carriers in over 20 countries (Asia: Philippines, Malaysia, Indonesia, Mongolia, etc. Africa: Egypt, Kenya, Juba, etc. Europe: Russia, Bulgaria. South American: Chile, Peru, etc. ME: Saudi Arab, Iran, etc.) . PVR has the good applicability in abroad from the result:

1. Supports encrypted communication based on local UMTS/VoLTE cellular voice network in all country.
2. Supports encrypted communication cross 2 or more carriers in most of countries.
3. Supports roaming encrypted communication by at least one domestic carrier (China Union, China Mobile or China Telecom).

8.2 Encrypted VoIP Calls

Although most public VoIP Apps could provide enough audio bandwidth for PVR encrypted communication, unfortunately many VoIP Apps' noise cancellation algorithm will eliminate the PVR encrypted audio signal as noise, what will cause a surge of demodulation error rate of encrypted signal, resulting a poor encrypted communication performance.

At present, it can be ensured that FaceTime and WhatsApp have better encrypted communication performance, users need to test for other VoIP Apps.

8.3 Encrypted Voice Messages

Voice Message App	iOS	Android
We Chat	Y	Y
Ding Talk	Y	N
WhatsApp	Y	N

At present, most iOS voice message Apps can support Bluetooth sound pick-up which means most iOS voice message Apps could use PVR to encrypt voice messages. But most Android voice message Apps, except We Chat as we known (maybe some other Apps more), don't support Bluetooth sound pick-up, which means only We Chat (maybe some other Apps more) could use PVR to encrypt voice messages.

8.4 Encrypted Recording

It is found that most built-in recording software of iOS could support Bluetooth sound pick-up after testing, therefore all iPhones support encrypted recording using PVR. However, the original built-in recording software of Huawei, Xiao Mi, Samsung or other brands of smartphones does not support Bluetooth sound pick-up, so the PVR can't be used for encrypted recording for these smartphones.

In order to use Android system smartphone for encrypted recording, users could download the third-party's recording software which support Bluetooth sound pick-up function.

In addition, there are reasons to believe that the original recording software of mainstream smartphone brand will support Bluetooth sound pick-up function gradually as the Bluetooth earphone is used commonly.