Journal of Information Hiding and Multimedia Signal Processing ©2016 ISSN 2073-4212
Ubiquitous International Volume **7**, Number **1**, January **2016**

Audio Packet Encryption of Flow Control Based on Stop-and-Wait Protocol

Gaoling Li*, Yingli Wang, and Hongbin Ma

Department of Electronic Engineering
Heilongjiang University
Harbin, Heilongjia, China
*Corresponding author
midaspeking@sina.com

Received March, 2015; revised October, 2015

Abstract. *The paper chooses the cyclone the second generation of the FPGA chip as the gate array (FPGA) used by AES encryption algorithm. The paper also uses speech codec WM8731 chip to realize eight voice and data coding. Then the paper refers to the PCM frame structure TS0 times lot function design code word synchronization. At last, the paper also uses AES128 grouping encryption algorithm to encrypt digital signal, and voice encryption is realized on the FPGA hardware.*
Keywords: Encryption algorithm; Stop-and-wait protocol; FPGA chip; Speech coding; Encryption synchronization.

1. **Introduction.** With the development of mobile network applications, the personal privacy security about speech information is becoming more and more attention. In this paper, the new design of a circuit can ensure information security by grouping encryption technology[1,2] based on FPGA. However, the routing of IP network transmission and delay characteristics make the received packet disorder, and affect the decryption key synchronization. Therefore, The paper designs a code word synchronization unit of voice pre-treatment and coding unit with stop-and-waiting protocol. This module can ensure the encrypted declassified audio data synchronization. The grouping encryption technology is embedded in the FPGA kernel. The safety of voice communications is guaranteed by grouping encryption circuit.

2. **Speech Data A/D and D/A Conversion.** The WM8731 speech codec chip is used in the paper. It can collect voice data. When gathered, the data stream is transmitted bit by bit. The WM8731 chip inside integrates A/D conversion mode[3], and the analog signal data is converted digital signal in the A/D conversion mode. Figure 1 is data collection format. BCLK refers to the speech coding clock signal. ADCLRC refers to control signal of A/D conversion. The LEFT CHANNEL refers to the left sound channel, and the RIGHT CHANNEL refers to the right sound channel. Left sound channel and the right sound channel completely control signals for ADCLRC. ADCDAT refers to data signals of A/D conversion, including ADCDAT 32 bits of data. LEFT CHANNWL refers to 16 bits of data and RIGHT CHANNEL 16 is bits of data. But the MSB is high data and LSB refers to low signal. Speech signal input from the MIC[4], transfer to the WM8731 speech coding chip, then the data is in A/D conversion. Figure 1 shown is data forma after A/D conversion. The data are commonly controlled by the BCLK clock signal and ADCLRC control signal. BCLK refers to speech coding clock, and ADCLRC refers to

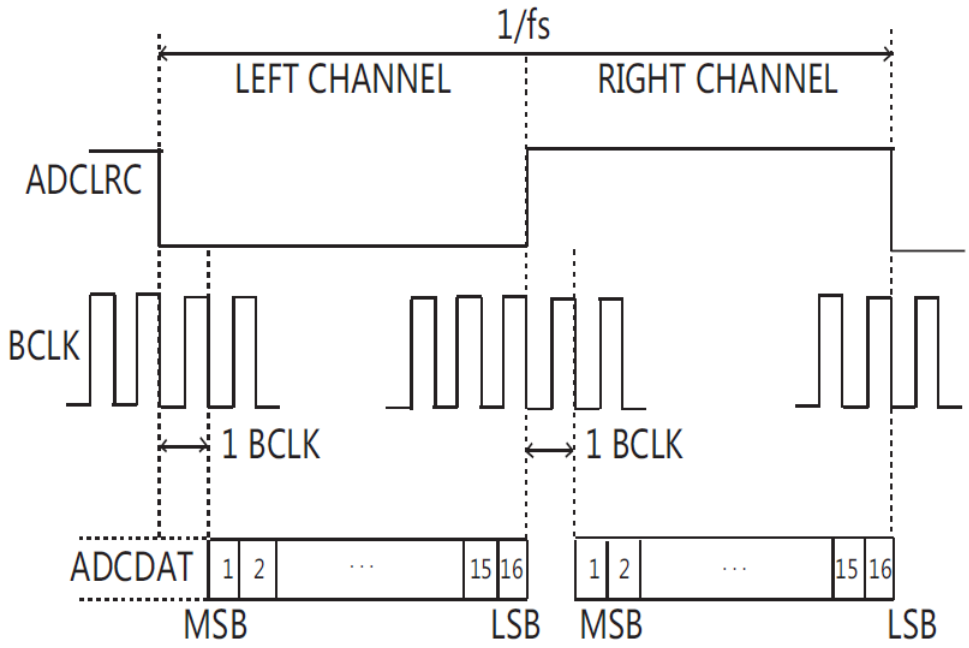

FIGURE 1. The format of data collection

control signal. When ADCLRC falling edge and the BCLK clock signal falling edge arrive at the same time and the BCLK next falling edge comes, it is time to begin collecting 16-bit data to the left sound channel (LEFT CHANNEL) speech signal. First collected data is on high bit, the latter collected data is in low bit. When ADCLRC rise along with the falling edge BCLK synchronous arrival and BCLK next falling edge comes, right sound channel began collecting 16-bit data (RIGHT CHANNEL). The clock signal BCLK

nishes 32-bit data collection after 34 clock signal in the process. This is a collection signal and it sends 32-bit data. A serial ADCDAT send 32 bits of data. The signals are sent to the FPGA, and the data is encrypted. D/A conversion is the inverse of the A/D conversion. When digital signal converts the analog signal, data transmission on DACDAT is by the form of 32- bit data stream. Figure 2 is the data form of D/A conversion. However, through the DACDAT port, the data was sent to phone port bit by bit, then sound was played.

3. **Code Word Synchronization.** It is the very important problem to consider synchronization codeword at re- ceiving end for communication system. It will directly related to the decryption feature of the whole system. The paper solve this problem by stop-and-wait protocol. After sending a packet data, the sender have to stop sending data and wait. Then the sender could not send the next packet data until it receives conformation from the receiver. According to the structure of PCM frame, the paper takes the TS0 time slot as tag of the audio data. The way to archive audio synchronization is that a special bit could be set aside in collected 32-bit code. The audio data is collected through bit by bit in this paper. After the data pass through the A/D conversion, it could be transformed into serial 32-bit data. At last, the two of 32-bit data could be marked. As shown in figure 3, the left and right channel first bit data is '00'. The next 32-bit data is '01' and so on. The fourth 32-bit data is '11'. The above data transmission could comply with stop-and-wait protocol. After the four 32-bit data are finished, these will be encrypted at the receiving end. At the receiving end, if the 10 data is missing, the decryption end

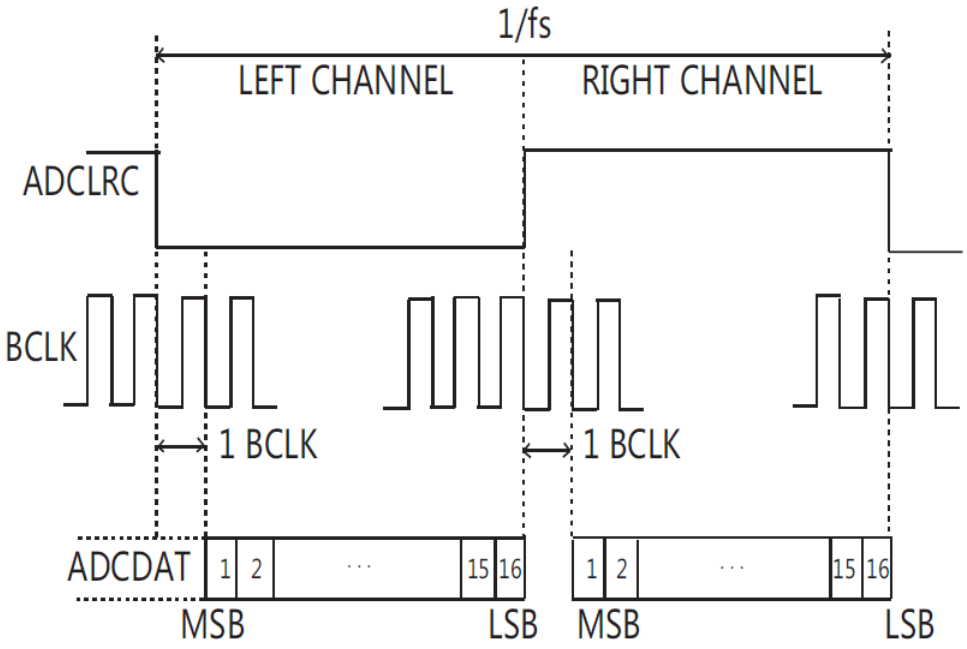

FIGURE 2. The date structure of D/A

would automatically use the key , which is need in the decryption process to solution the next data. As we know, the data is decrypted at the decoding end. The decoding order need rely on the labeling bit. In the process of data transmission, network congestion, or

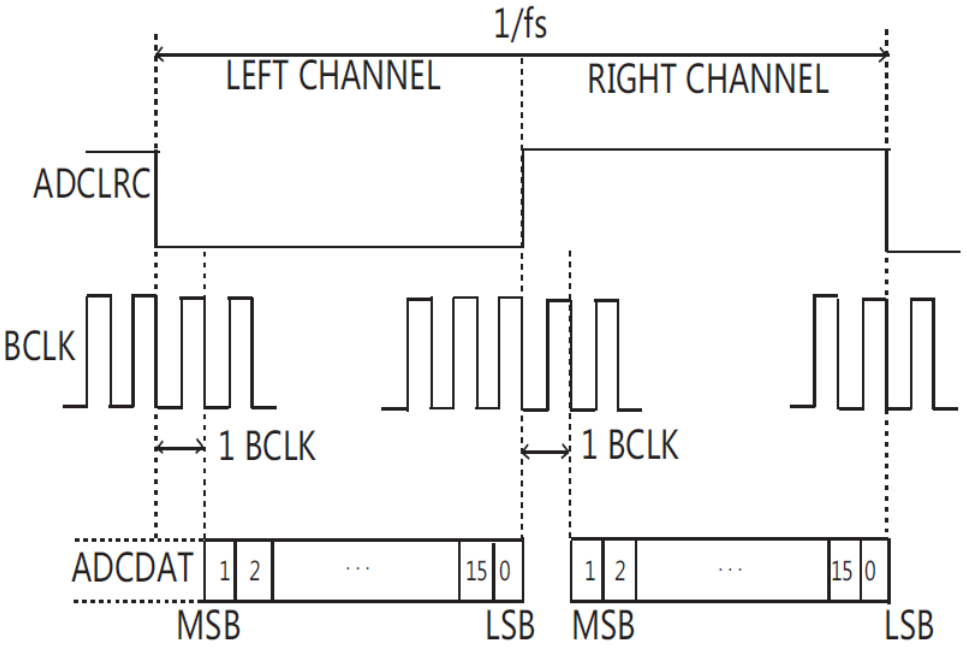

FIGURE 3. The flag first bit of collection

no signal will make the data miss. The missing data won't be code in the decoding end. Then it is necessary to use the mark bit to decide. The lost data, joining the 0010 mark bits on ag bit, will send a request. The sender will give back to the data with 10 mark. It

can solve the problem of speech signal data loss in the process of transmission, realizing audio synchronicity.

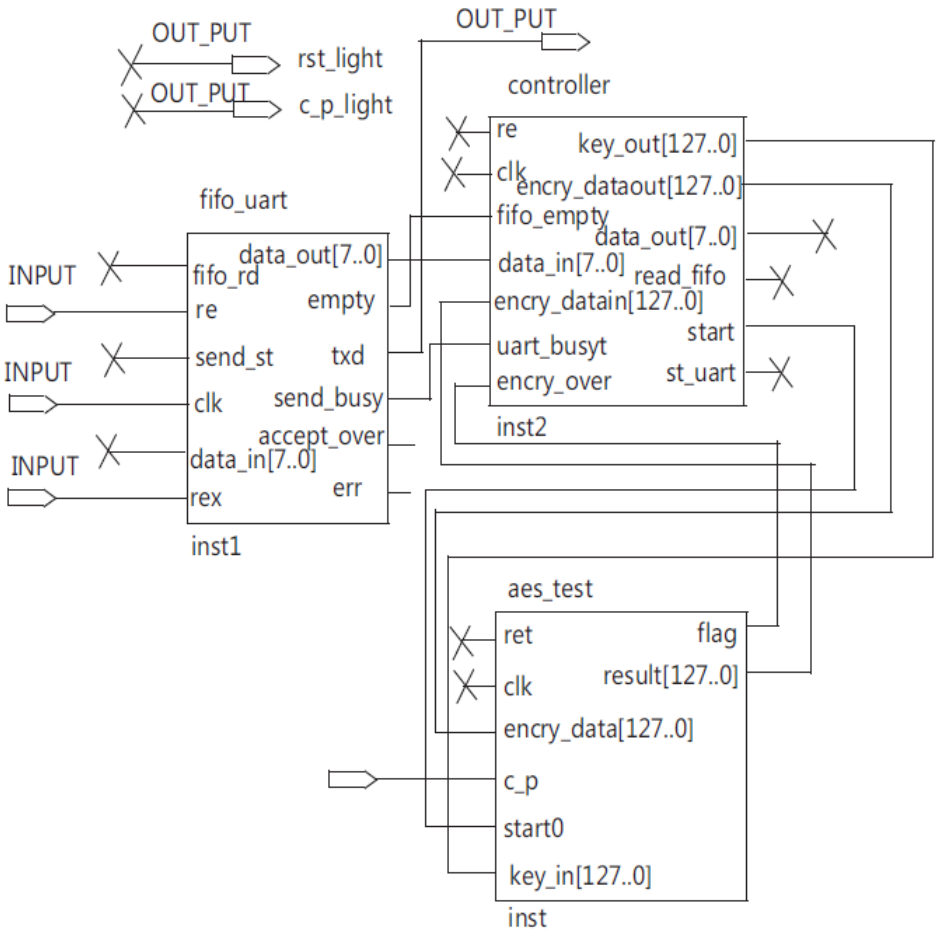

FIGURE 4. AES encryption top nuclear

4. **Encryption Module Design and Implementation.** The chipper realizes the AES algorithm[5,6,7] encryption through fast look-up table method in the verilog programming. The method could complete follow process under the case statement. For example, S-box, the hybrid column table, and simple cyclic shift in the encryption process. By the way, the design of circuit diagram AES encryption algorithm in the FPGA[8] is shown in Figure 4. The function of AES encryption: the speech digital signal could be encrypted through the encryption module, then it would be sent by the wireless. At last, it is decrypted at receiving end. But AES encryption mainly consists with encryption module, key rotation, decryption module, key extension, etc. These modules can encrypt the receiving data with 128 - bit data. This is the function of encryption. The principle of the encryption process is shown in Figure 5. Encryption principle is shown in Figure 6. The encryption part is divided into four modules: the encryption module, decryption module, key extension module and RAM module. The AES encryption module contains 8 I/O ports. Six of the 8 I/O parts is input ports and other two ports is output ports. The encry data[127..0] port can receive the 128 - bit digital signal of the voice signal. When coding data flow bit by bit is stored in AD_fifo, and it is converted to 32-bit data transmission. Before a 128 - bit AES encryption algorithm in the process of transmission, the data is stored in cache, namely in the fifo of theencryption algorithm. When the data arrives 128 bits

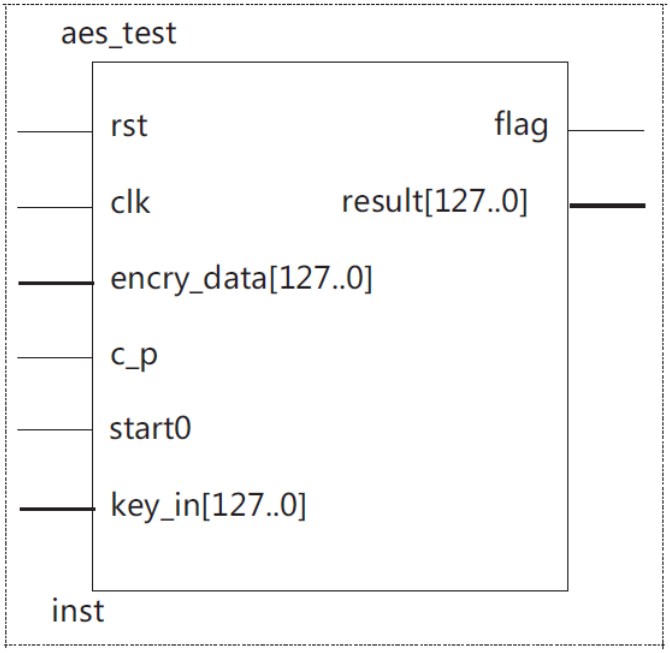

FIGURE 5. The principle diagram of the encryption part of the main frame

of data, start0 port begins to work, the data is stored in SDRAM. After pressing the button for voice broadcast, the data need to be decrypted in the process of play, restoring previous digital signal. Then through the WM8731 decoding, voice encryption process is finished. The encryption part contains 6 input port: rst refers to clock reset signal, and it is effective under the high level. clk port mainly refers to the clock signal in the system. And encry data [127..0] refers to the 128 data come clear speech signal input port. cp signal primarily refers to selective encryption. When cp is high electricity at ordinary times, the whole system is the encryption process. When cp is low electricity at ordinary times, the whole system is the decryption process. It is like the equivalent of buttons. When the button is not pressed, voice encryption process begins. When the button is pressed, the voice decryption process begins. start0 port refers to the start signal. The audio encryption of he whole system begins, It is effective high electricity at ordinary times. key in [127..0] port is a key input port. At the beginning of the whole system, firstly inputting key, the system will automatically take the first data as the key data. After the data reaches 128 bits, the latter data is clear data. The system began to encrypt the latter 128 - bit data. Two output port: ag output port is signal that the add/decryption is over. Its effective level is high level effectively. When the ag is high level, data encryption process is finished. And result [127..0] port is the output result of add/decryption of the 128 speech signal.

5. **Software Process and the Environment.** The system test environment mainly applies Quartus 9.0 software simulation [9] and is encoded in the platform. The speech coding of audio WM8731 and the acquisition of voice data are base on Quartus software. The collected data through the WM8731 chip convert other data, namely the A/D conversion. The converted data through FPGA is under the encryption [10] of data. Then it is transmitted to the wireless network and received on the other side. Software process: design input, design, build, function simulation and timing simulation, hardware configuration and verification. The ow chart of the software overall design is shown as Figure 7.

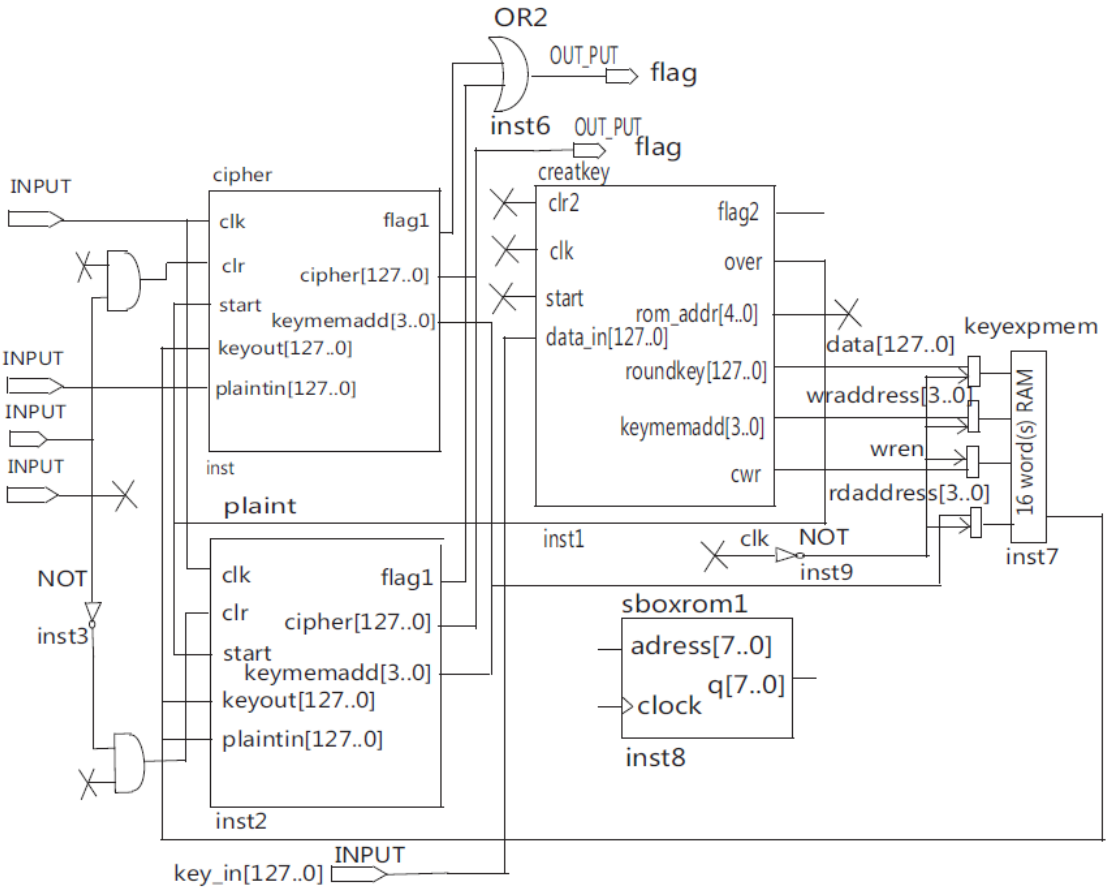

FIGURE 6. The part diagram of Encryption principle

6. **The Result and Stochastic Analysis.** Set the initial key as hexadecimal 000102030405060708090A0B0C0D0E0F0 results of ten rounds of key are as follows:
Round1:D6AA74FDD2AF72FADAA678F1D6B76FE;
Round2:B692CF0B643DBDF1BE9BC5006830B3FE;
Round3:B6FF744ED2C2C9BF6C590CBF0469BF41;
Round4:47F7F7BC95353E03F96C32BCFD058DFD;
Round5:3CAAA3E8A99F9DEB50F3AF57ADF622AA;
Round6:5E390F7DF7A69296A7553DC10AA341F6B;
Round7:14F9701AE35FE28C440ADF4D4EA9C1026;
Round8:47438735A41C65B9E016BA1F4AEBF7AD2;
Round9:549932D1F085577681093ED9CBE2C974E;
Round10:13111D7FE3944A17F307A78B4D2B30C5.
From ten key rotation wheel key extension, it will be found that the key of each round is different. The degree of data encryption is greatly increased in the encryption process. The round keys write number of round keys itself in the program. The key is 10 rounds in the paper. After key rotation, it is time to encrypt data. For captured data, because the intercept is not clear to key rotation, they can not to decrypt the data. By Quartus software simulation data captures part of the AD conversion after the data. The data is passed to the encryption, the data for the cipher is text data. Then the cipher text data is put into a binary code, namely the 0 1 sequence. Through Matlab simulates 0 1 sequence randomness, the number of run, inverse cumulative value of the standard normal distribution and the test results can be known.

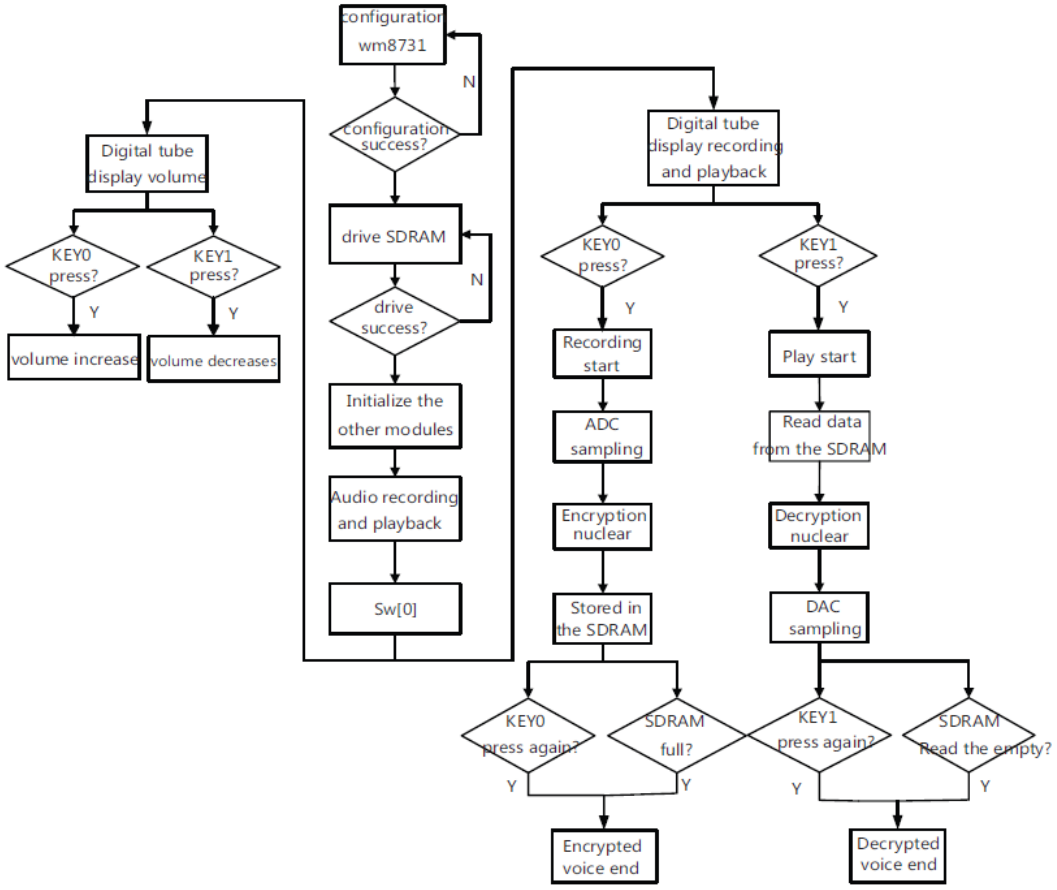

FIGURE 7. The flow chart of software

01101000000100101010101100010100110101111001001111011111011110100101011100101001110100000100101101011101110010000101101000010001101
The above data is a voice encryption data and could be used as the input sequence. It is a result of test with principle of the ow control. Setting parameters: r refers to the number of runs. Randomness refers to the input sequence. zr refers to test results. The inverse cumulative function value of the standard normal distribution is taken as a measure of random sequence by using Norminv. The test sets up several special clear text input in the process. Such as, clear data of full 1:
1111111 11111111111111111111111,
clear data of the whole 0:
00000000000000000000000000000000,
01 evenly distributed data:
01010101010101010101010101010101,
F all the data:
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF,
The normal voice data:
11111010110010001111101011001000.
The above five clear data is encrypted, then the cipher text data full 1 cipher text data:
35D14E6D3E3A279CF01E343E34E7DED3,
All the zero cipher:
C6A13B37878F5B826F4F8162A1C8D879
01 distributed evenly cipher text data:

C352805754237F311AC0FFF4E3E03E78
All F the cipher text data:
3C441F32CE078 22364D7A2990E50BB13
voice cipher data:
6812AB14D793DEF4AE53A0 B5DC85A11B.
The cipher text is converted to binary. Then 0 1 series is under the discussion through the principle of runs test. It is a random sequence or not. The inspection is that the value of the inverse cumulative of standard normal distribution is 1.96, proving that the encrypted cipher text sequence is random sequence.

Acknowledgment. This work is supported by the National Natural Science Foundation of China (No.61302074). Many thanks to the anonymous reviewers, whose insightful comments made this a better paper.

REFERENCES

[1] S. G. Lian,On the Secure Multimedia Distribution Scheme Based on Partial Encryption. *J. International Conference on Taylor and Francis Group*, vol. 9, pp. 23–27, 2010.
[2] H.Martin, P. Oliver, ADPCM with Adaptive Pre-and Post Filtering for-Delay free Audio Coding, *J. ICASSP2007,* vol. 3, pp. 269-272, 2007.
[3] D. Y. Chang, Design Techniques for a Low-Power Low-Cost CMOS A/D Converter, *J. Journal of Solid State Circurts*, vol. 33, pp. 1244–1248, 1998.
[4] M. U. Salamci, M. K. Ozgoren, S. P. Banks, Sliding Mode Control with Optimal Sliding surfaces for Missile Autopilot Design, *J. Journal of Guidance Control and Dynamics*, vol. 23, pp. 719–727, 2000.
[5] C. Nalini, Nagaraj, An FPGA Based Performance Analysis of Pipe-lining and Unrolling of AES Algorithm, *J. International Conference on Source,* vol. 24, pp. 477–482, 2006.
[6] R. L. Lang, Y. Xia, G. Z. Dai, Study of Advanced Encryption A standard (AES) Algorithm, *J. Small Microcomputer Mystem*, vol. 24, pp. 905-908, 2003.
[7] D. Orr, K. Nathan, The effects of the omission of last round's Mix columns on AES., *J. Information Processing Letters*, vol. 11, pp. 304–308, 2010.
[8] H. W. Li, S. H. Yuan, Based on Quartus FPGA/CPLD Design, *Publishing House of Electronics Industry*, Beijing, 2006.
[9] Altera Cyclone II Device Handbook, *http://www.altera.com.*
[10] B. Jiang, Reduction of Primavera Digital System Design and PLD Application Technology, *Publishing House of Electronics Industry*, Beijing, 2010.