An Encryption Technique for Measurement and Display of Radar Parameters

Xiaofei Zhu [a], Weizhong Yu [b], Guodong Jin [c]

The high tech research institute of Xi'an, China

[a]Zhuxf101@163.com, [b]zhouenlai2002-1@sohu.com, [c]18578031@qq.com

Keywords: encryption method of AES, encryption display, key management.

Abstract. The secrecy of emission frequency is prerequisite for securely working of radar. This paper proposes an encryption test program based on encryption algorithm of AES focusing on the need for the encryption test of radar parameters, and then analyses the designing method of AES algorithm, finally completes the system designing. The test results show that, the proposed program can effectively enhance the confidentiality of emission frequency test of radar, it can also be applied in the security management for parameters measurement of radar.

Introduction

Some key test data of radar like the transmitting frequency are required to be kept secret, even to the operating personnel and the testers in order to avoid malicious attacks. To ensure the measurements to be safely developed, it is a key issue to ensure the testers to be able to identify the test data and manage the test record.

Currently, the absolute confidentiality of key data of radar like the transmitting frequency is mastered and tested by specially-assigned person. There are no effective technical control means in the work of safeguarding secret information, which could easily lead to the leakage of key data parameters. There are two key points to realize encryption test. One is to ensure the testers can test under the condition of not being aware of the frequency, so as to efficiently control the range of knowing the confidentiality. The other is that the measured frequency value cannot be directly displayed until the secrecy frequency is transformed, which is to ensure the testers do not know the secret. These problems will be solved in this paper through using the data encryption technology.

Realization of data encryption algorithm (DDA)

Advance Encryption Standard, simply AES, was started by the National Institute of Standards and Technology (NIST) in 1997. The NIST has collected algorithms since 1997 and then decided to adopt Randel as the final algorithm in 2000. Moreover, in the year of 2001, it was approved to be the new federal information encryption standard by the US Department of Commerce (FIPS PUB 197). AES, as the substitute of DES, features security and high efficiency. Besides, AES can always well perform in the hardware and software operating environment. Therefore, it is suitable to be used in this design and to encrypt the confidential information [1].

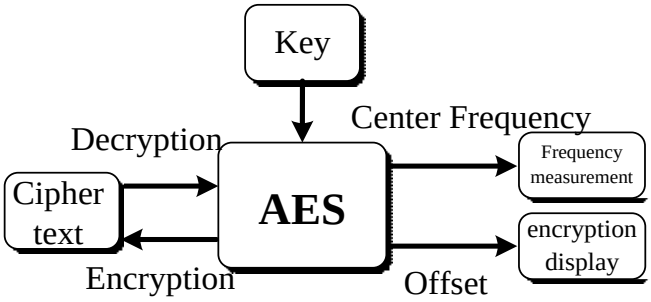

Figure 1: Encryption test functional block diagram

Figure 1 shows the overall design. Encrypt the confidential information by AES and then store the cipher text in the external storage device, being separately stored with the test instrument. When tested, it is connected with the test instrument and then read the cipher text. At this time, it can decrypt and get the confidential information together with the encryption key in the instrument. The confidential information include the offset which is added when carrier frequency value of the transmitter and the measuring frequency display. And then the carrier frequency is transmitted to frequency measurement and the offset is applied to encryption display. Thus the operating personnel can test under the condition of being unaware of the frequency of the fuse machine.

Encryption and measurement of radar parameters

Hardware designing Because the information which should be encrypted are only the carrier wave frequency of transmitter and the offset value of encryption display, and both of them are very low, high encrypting or deciphering speed for the whole system are not necessary, which is also the same for the reading and writing speed or the storage of memorizer used to store the encryption data.
From the above analysis, STM32F103ZET6 produced by ST is selected for computing core in system designing, which is a 32-bits micro controller based on an ARM core of Cortex-M3 with an maximum frequency of 72MHz. The AES algorithm is realized on STM32, EEPROM is selected to store the encrypted data. When radar parameters is being tested, we should just combine the equipment with EEPROM internally installed and the test instrument together to decode the data. After the decryption done we can get the frequency value and offset value, which is the whole process of encryption measurement.

EEPROM is a serial chip with a 64K I2C, its chip type is 24LC64, the range of power supply for this chip is 1.8V to 5.5V, it also uses the low-power dissipation CMOS technology, therefore the working current is only 1mA with a clock frequency of 4000kHz, the chip has adopted two lines of serial communication protocols I2C to transmit data. Vcc should be connected with a power source of +1.8V~5.5V, and Vss should be connected with the ground. SDA is used to transmit address and data in two direction, SCL is a pin of synchronous clock, WP (Write-Protect) is a pin of write-protect. It is invalid when connected with Vss or null. If WP in connected to Vcc, writing is forbidden, but reading is not affected.

Software designing STM32 has an I2C port inside, when it is in master mode, I2C port will start data transmission and generate a clock signal. Serial data transmission always starts under the start conditions and stops under the stop conditions. Both the start and stop conditions are controlled by software in master mode.

When it is in slave mode, I2C port can recognizes its own address (7 or 10 bits). Data and address are transmitted on 8 bits per byte with high bit ahead. The one (7 bits) or two (10 bits) bytes followed the start conditions is the address. The address is transmitted only in master mode. To transmit a byte will take 8 clock periods, and in the ninth clock period, the receiver must answer an ACK to the sender.

Here STM32 is the master, and EEPROM is the slave, the addressing mode for EEPROM is showed in figure 2.

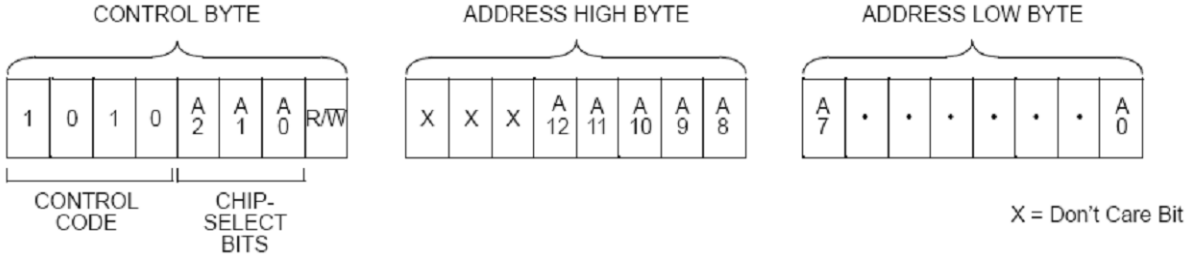

Fig 2 addressing mode of 24LC64

Firstly, the master computer should send a control byte, as for 24LC64, CONTROL CODE should be set as ‘1010’, the A2, A1 and A0 are chip selection pin, which can be used to expand to 8 24LC64 in the same bus. If the last bit of control byte is set to 1, it means to write, if it is set to 0, it means to read. With the above I2C bus communication rules between EEPROM and STM32, the encrypted data transmission in one bus between EEPROM and STM32 can be realized.

Test and analysis

Firstly, we verify the AES algorithm on MATLAB by a case of AES code, which is encrypted and decrypted on MATLAB, the results are as follows:

Step 1: suppose that the confidentiality frequency is 2GHz, which can be transferred to 77359400 in hexadecimal system, this is the clear text, the round key is “000102030405060708090a0b0c0 d0e0f”, on STM32 we can get the cryptograph as “1bcd9983afce67c2b5d40c9e55fc911 6”. Decrypt the cryptograph above and we can get the clear as “00112233445566778899aabbccddeeff”, which is the same as the clear we input, so we can get the conclusion that the proposed AES algorithm is correct and effective to encrypt the confidential frequency.

Secondly, we should transplant the AES algorithm to STM32 to verify its correctness,

Step 2: Decode the cryptograph above on STM32, we can get the clear text as “00000000000000000000000077359400”, which is the same as the initial clear, so we can come to the conclusion that the proposed AES algorithm is feasible on STM32.

Key management

In the dedicated parameter tester designed for radar, the tested data should be encrypted. Then the cryptograph is stored in the external storage device, and the storage device should be placed separately from the tester. It can be used to store the testing result data, history data and the comparison analysis between them. Before the test starts, the storage device should be connected with the tester to read the cryptograph and key to decode the cryptograph, after that the confidential information is got. Key and linear transmission function used to display the data are stored in the dedicated radar tester which adopts authorization and key management. The key and cryptograph are stored separately in order to guarantee the security of key data testing for radar.

Conclusion

This paper has introduced the math and transmission principles of AES algorithm, and the encryption and decryption design of AES on STM32.Then a case has been tested. The results showed that the desirable confidential effect has been realized and it the security of confidential information can be enhanced by technical means.

References

[1] HE Ming Xing FAN Pingzhi. Advances and analysis of the advanced encryption standard [J] Java World, 2000, 12(4): p. 47-51.

[2] National Institute of Standards and Technology. Advanced encryption standard [DB/OL]. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, 2001.

[3] Joan Diemen, Vincent Ragmen. Advanced encryption standard (AES) algorithm—Randel designing [M]. Peking: Tsinghua University, 2003.

[4]Joan D, Vincent R. AES proposal: Randel [DB/OL]. http://csrc.nist.gov/encryption/aes/rijndael /Rijndael.pdf, 2001.

[5]Kurekin, A. ; Marshall, D. ; Radford, D. ; Lever, K. ; Kulemin, G. Assessment of Soil Parameter Estimation Errors for Fusion of Multichannel Radar Measurements. 2006 9th International Conference on Information Fusion, 2006: p.1 - 8

[6]Gulum, T.O. Erdogan, A. Y. Yildirim, T. Pace, P.E. A parameter extraction technique for FMCW radar signals using Wigner-Hough-Radon transform.2012 IEEE Radar Conference (RADAR), 2012: p.0847 – 0852.