RFID Encryption Performance Verify

By
Chih-Cheng Ou Yang
503590352

Abstract

Encrypted confidential data might cause the effectiveness accuracy rate for writing data into tag. But encryption for RFID confidential data is necessary for industrial, including healthcare, supply chain, etc. The project is to verify the performance of encrypted data during transmitting, and also help industry to find the balance between efficiency and security.

Encryption methods which are used in the project will be introduced, and the designed interface of verifying program will be illustrated. DES and Rijndael (AES) are two symmetric encryption methods used in the project. Different key lengths of these two encryption methods are the difference which the project needs to use for generating different encrypted data length. Multi-functions interface is designed to help user to verify the performance easily. Not only automatically executing the verifying cycles repeatedly but also generate the test report instantly which include tag information, accuracy rate, average execution time and data information.

1. Project Overview:

Plain data transferring without security encryption between RFID reader and tag is happened in most of the protocols of RFID transmission, so the safety is concerned all the time. RFID technology is applied in supply chain industry, healthcare, specimen track, library system and smart shelf, etc [1]. Some of the industry and applications need security protection of their data during transmission and in memory. These kind of data includes personal privacy information and non-public information, so these data can not be leaked to unauthorized devices or prying people. Encryption applying on these privacy data is obviously essential. Encrypted data apparently will be longer than plain text, so the accuracy and efficiency during transmission will be affected. In this project, symmetric and asymmetric encryption methods will be used to encrypt plain text data and using MD5 hash code to verify data accuracy. Find a balance between security and efficiency will be discussed in this report.

1.1 RFID Equipments:

- RFID Reader Module:
  Texas Instruments S6500 Long Range Reader Module
  Part Number: RI-STU-650A -- ISO 15693 compliant with a relay output and an asynchronous interface which can be configured as RS232 [2].

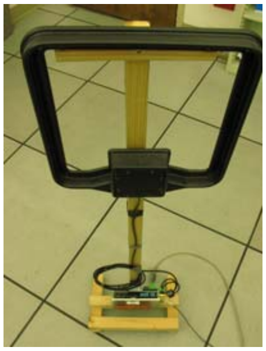


Fig 2: RFID Reader Module

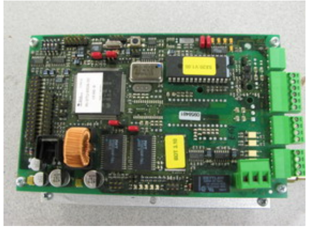


Fig3: S6500 Long Range Reader Module

- RFID Reader Antenna:
  Texas Instruments Series 6000 Gate Antenna
  Part Number: RI-ANT-T01A -- Single-loop antenna with transmitting frequency of 13.56 MHz and an output impedance of 50 Ohm [3].

Fig 4: Series 6000 Gate Antenna [4]

- RFID Tag:
  Zebra's RFID wristbands RFID Z-Band® 4000
  Size: 1" x 11“
  Memory Size: 128 Bytes [5]

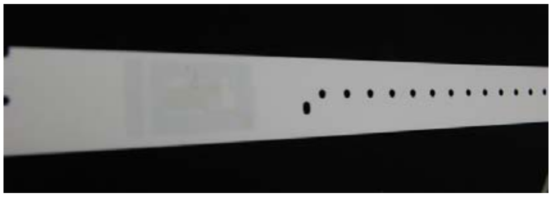


Fig 5: RFID Tag

- Programming Software:
  Microsoft Visual Studio 2005 C#

2. Encryption Methods:

2.1 Symmetric Encryption Method:

The encryption methods used in the test are DES and Rijndael (AES) of symmetric encryption method for encryption and decryption the data and also used MD5 Hash encryption to verify the data accuracy of writing and reading process. Symmetric encryption method is used for long time. The particular point of symmetric encryption method is the administrator and the clients both have the same secret key to encrypt and decrypt the confidential data. The most common way to encrypt the data is called Cipher Block Chaining (CBC), which works as follow [6]:

1. The plain text will be broken into blocks of same size as the input for the cipher function.
2. Process the first message block:
   a. XOR the message block with the “seed” data to create a combined data block.
   b. Encrypt the result to produce the first block of cipher text.
3. Process remaining message blocks in turn:
   a. XOR the plaintext block with most recently created cipher text block to create a combined data block.
   b. Encrypt the combined data block and append the result to the cipher text.

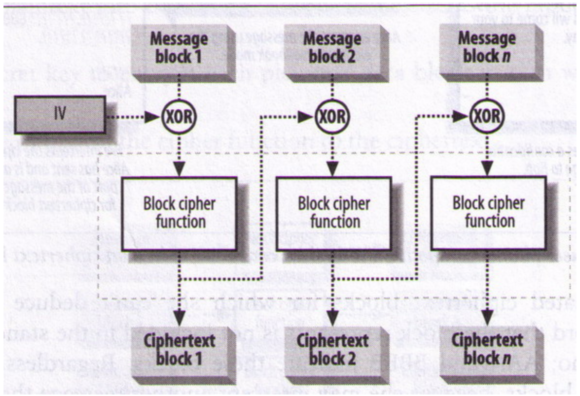


Fig 6: CBC mode [7]

Generating static initialization vector (IV) and DES key in the program will be done in this project. They will be used as the elements to encrypt the confidential data.

2.1.1 Comparison:

Two methods of symmetric encryption way are used in this project, DES and Rijndael (AES). The differences between these two methods are the key length and the block size. The comparison of these two methods as shown in Table 1 and the result of encryption plain text as shown in Table 2:

Name	Block Size	Key Length
DES	**64**	**56**
Rijndael(AES)	**128, 192,256**	**128, 192,256**

*Table 1: Comparison between DES and Rijndael(AES)***.**

	Plain Text Length (Bytes)	Encrypted Length (Bytes)
DES	0~7	12
	8~15 (GTIN, SGTIN)	24
	32~39	56
	88~95	128
AES	0~15(GTIN, SGTIN)	24
	16~31	44
	32~47	64
	80~95	128

Table 2: Comparison between two encryption

2.2 Hashing Verification:

Hashing encryption method is used to verify the data accuracy during transmission. It is more like a common verification code between two stream data. Original encrypted data uses the hashing method to generate a hashing code and keeps it in memory. After receiving the data which is read from reader's memory, then generate another hashing code with the new data from reader's memory. Comparing these two hashing code to make confirmation if the data is altered or not. It is also like check sum verification.

3. Programming and Designed interface:

The functions of the designed program are encoding plain data into encrypted data with desired encryption methods, transmitting encrypted data to the tag, reading encrypted data from RFID tag, decoding data into plain data, verifying the accuracy and efficiency in desired cycles automatically and generating test report.

3.1 Write Process:

After encrypted the plain data, the program can transmit the encrypted data to the tag and confirming the data is written correctly or not. First, generate the hash code of encrypted data as verification testimony. Second, writing the encrypted data into the tag memory and wait for reader feedback. If it returns success signal, then read the same data from the memory, and verifying the read back data's hash code with original hash code is match or not. If the verification is true, the writing process will be announced as successful. Because the data might be revised during transmission, and if only checks the error message from the reader, the revised data will not be known as program. So the double testimony of the process is definitely needed. This strict verifying step cause the writing accuracy rate will be affected by reading accuracy rate, but it can not be eliminated from the progress. The logic flow chart of writing process as shown in Fig 7:

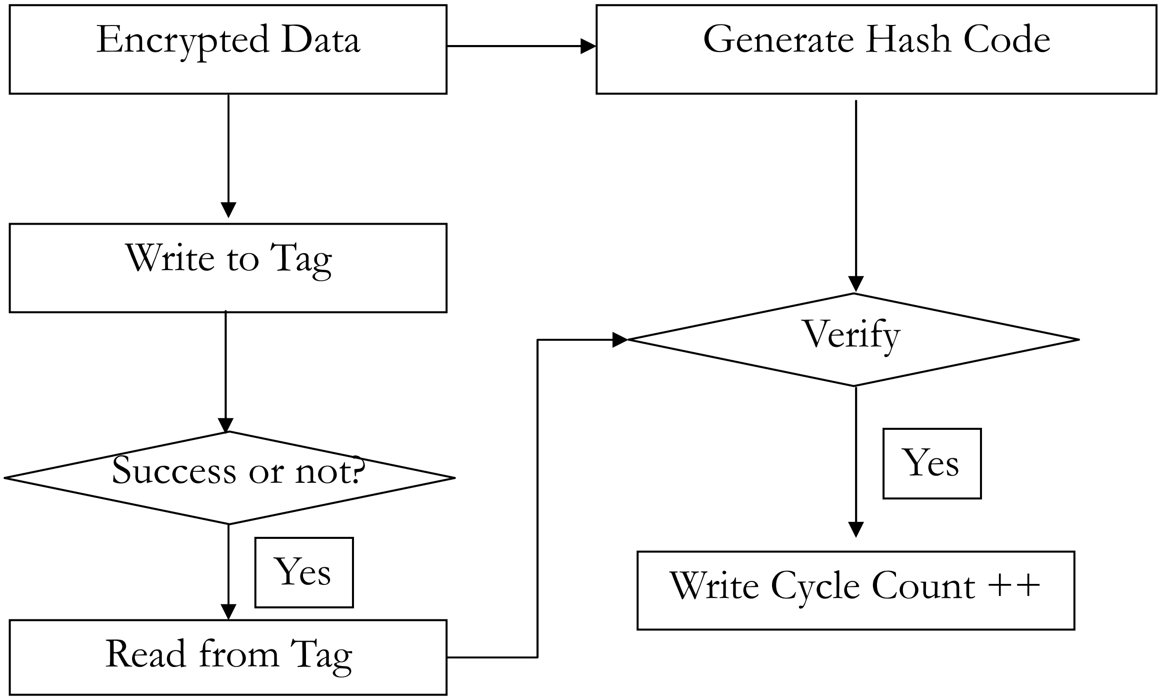


Fig 7: Writing process flow chart

3.2 Read Process:

Reading process will be simpler than writing process. Generating the hash code of original encrypted data and making comparison of the hash code from the read back data.

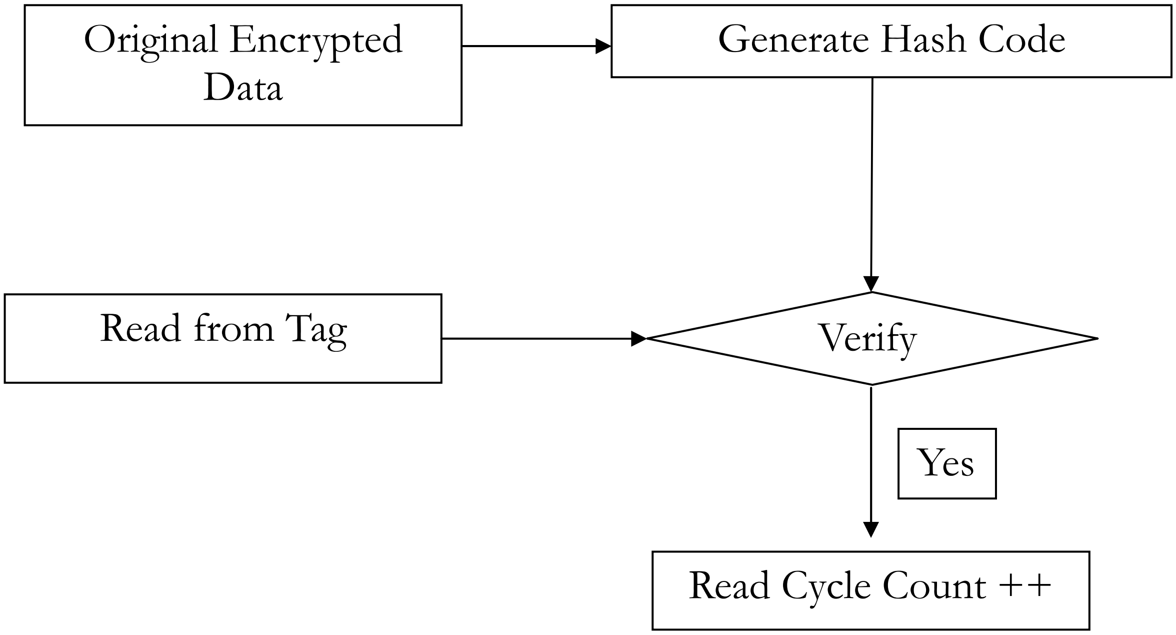
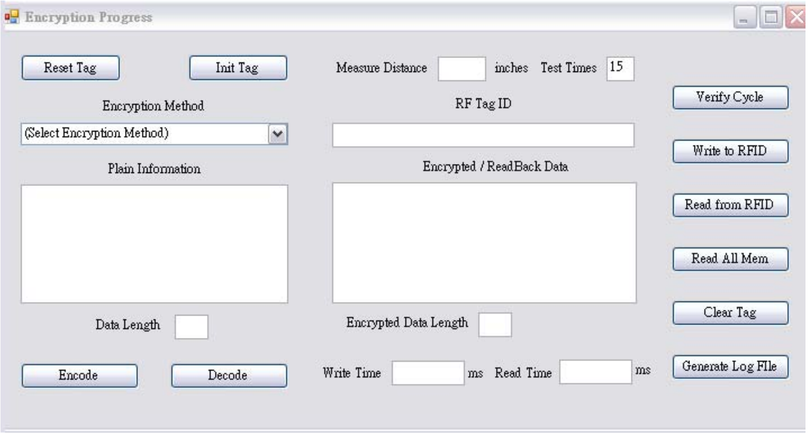


Fig 8: Reading process flow chart

3.3 Interface:

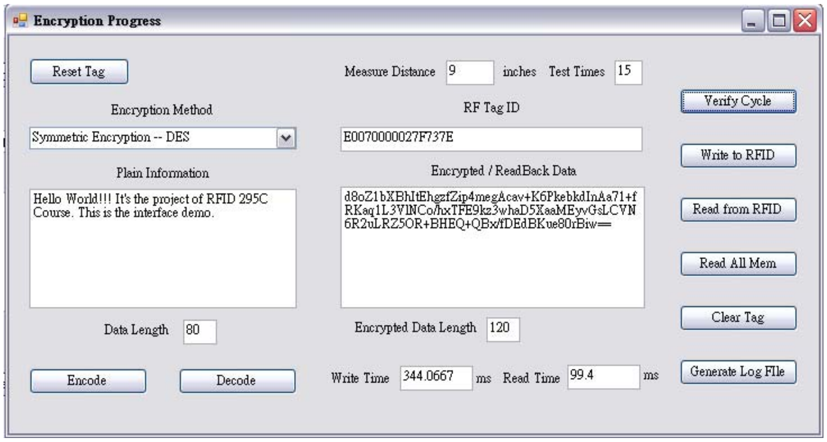
The interface is designed with multi-functions for testing and single step test, including read tag ID, encode and decode data with different encryption methods, write the data into memory of tag, read the data from tag, clear tag memory, measuring the writing and reading time, generating the test log file and verifying the test cycle with desired times. The designed interface is shown as Fig 7 and Fig 8:



Test Times 15

Encryption Method (Select Encryption Method)

Fig 9: Interface of verifying program



Measure Distance 9 inches

Test Times 15

Encryption Method: Symmetric Encryption -- DES

RF Tag ID: E0070000027F737E

Plain Information:

Hello World!!! It's the project of RFID 295C Course. This is the interface demo.

Encrypted / ReadBack Data:

```
d8oZ1bXBhItEhgzfZip4megAcav+K6PkebkdInAa71+f
RKaq1L3VlNCo/hxTFE9kz3whaD5XaaMEyvGsLCVN
6R2uLRZ5OR+BHEQ+QBx/fDEdBKue80rBiw==
```

Data Length 80

Encrypted Data Length 120

Write Time 344.0667 ms

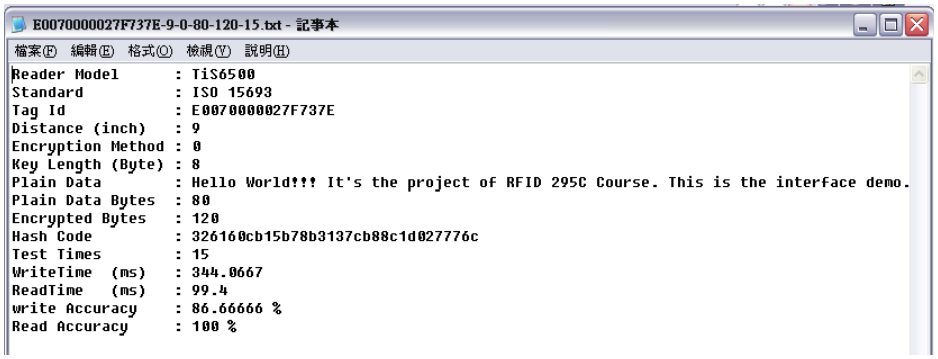
Read Time 99.4 ms

Fig 10: Demonstrate of verifying cycle

After the verifying cycle is over the test report will be generated as a text file automatically. The information of the test report including:

1. Reader Model
2. Standard
3. Tag Id
4. Test Distance (inch)
5. Encryption Method
6. Key Length (Byte)
7. Plain Data
8. Plain Data Bytes
9. Encrypted Bytes
10. Hash Code
11. Test Times

12. Average Write Time (ms)
13. Average Read Time (ms)
14. Write Accuracy Rate
15. Read Accuracy Rate


E0070000027F737E-9-0-80-120-15.txt - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)

```
Reader Model        : TiS6500
Standard            : ISO 15693
Tag Id              : E0070000027F737E
Distance (inch)     : 9
Encryption Method : 0
Key Length (Byte) : 8
Plain Data          : Hello World!!! It's the project of RFID 295C Course. This is the interface demo.
Plain Data Bytes  : 80
Encrypted Bytes   : 120
Hash Code           : 326160cb15b78b3137cb88c1d027776c
Test Times          : 15
WriteTime  (ms)   : 344.0667
ReadTime   (ms)   : 99.4
write Accuracy    : 86.66666 %
Read Accuracy     : 100 %
```

Fig 11: Test report

2. Testing Reports:

The test parameter is set as verifying the write accuracy rate and read accuracy rate with different distance (3 inches interval) with 128 bytes to discover what distance will perform the best representation of writing and reading.

The parameter of this test is set as:

1. Distance: 3 ~ 15 inches with every 3 inches interval.
2. Plain Text Data: 88 bytes
3. Encryption Method: DES
4. Encrypted Data Length: 128 bytes
5. Numbers of Test Times for each distance cycle: 1000

The performance is shown facts of:

1. Average writing time: 366.27 ms
2. Average reading time: 103.57 ms
3. Writing and reading data with 128 bytes at 15 inches performance approximate zero.
4. The majority of writing accuracy rate locates at 86.8% (12 inches) ~ 90.4% (3 inches).
5. The majority of reading accuracy rate locates at 97% (12 inches) ~ 98.3% (3 inches).
6. Relationship between performance and distance is positive related.

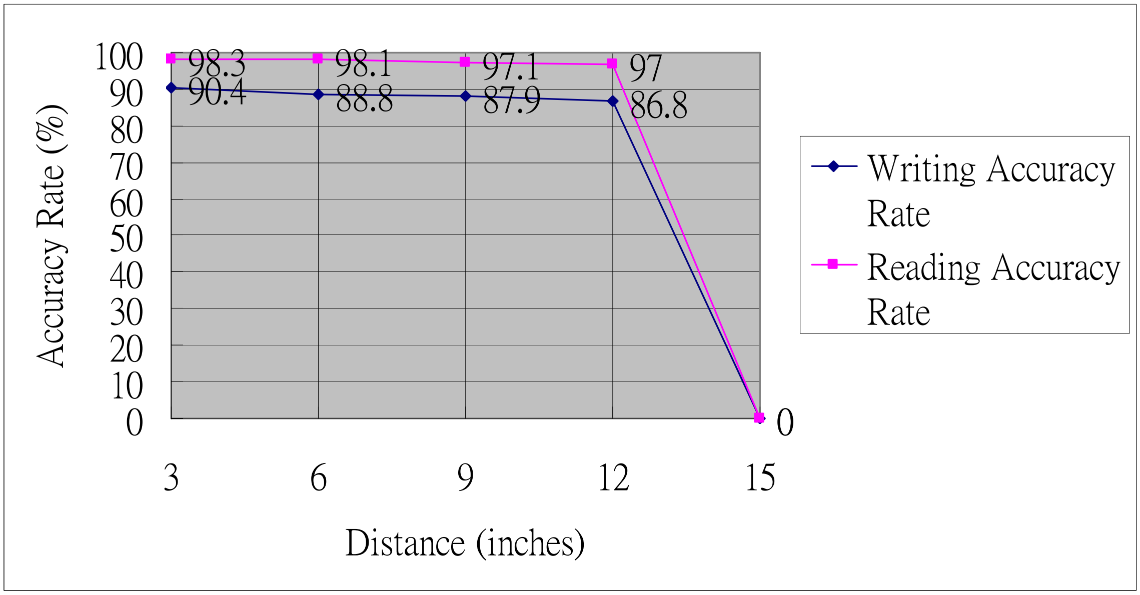


Chart 11: Verifying Performance Test report

3. Conclusion:

According to the test report, the writing accuracy is getting more accurate when closing to the reader. But the best accuracy rate locates on around 90%, it's much lower than reading accuracy rate for 8% difference. The difference could be caused by these facts: (1) Data bytes are too large which cause the accuracy rate fall (2) The stability of reader or tag (3) Writing accuracy rate is bound by reading accuracy rate, because of strict verifying step. So the writing accuracy rate is inevitable affected by the reading accuracy rate, and cause the difference.

The relationship between data accuracy rate, distance, different reader and tag, different data length and writing stability still can be verified in future work. These test report can be a useful reference as choosing encryption methods for confidential data and as finding the best efficient distance range for writing data.

References:

[1] WINMEC LAB, UCLA:
http://www.winmec.ucla.edu/

[2] Texas Instruments:
http://www.ti.com/rfid/shtml/prod-readers-RI-STU-650A.shtml

[3] Texas Instruments:
http://www.ti.com/rfid/shtml/prod-ant-RI-ANT-T01A.shtml

[4] Texas Instruments:
http://www.ti.com/rfid/graphics/productImages/ant-t01a.jpg

[5] Zebra:
http://www.zebra.com/id/zebra/na/en/index/products/supplies/rfid_supplies/rfid_wristbands.html

[6] Adam Freeman & Allen Jones 2003, “Programming .NET Security”, O’Reilly, pp. 341.

[7] Adam Freeman & Allen Jones 2003, “Programming .NET Security”, O’Reilly, pp. 342.