Design of Encrypted Packets for Identification of Missing objects using RF Tags and 32 -Bit Microcontroller

Randeep Singh Taggad
ECE Department
Lingaya's University
Faridabad

S.V.A.V.Prasad,Ph.D
Dean
Lingaya's University
Faridabad

Arvind Pathak
Assistant Professor
Lingaya's University
Faridabad

ABSTRACT
RFID technology enables us to identify each object and even the container itself. The RFID readers can be placed up to a few meters away from RFID tagged objects.[8] However, current RFID gives all information related to the objects present in the group but they do not provide information on IDs missing from a group. The work mentioned in this paper proposes a method and it will design a system which will determine the unique IDs of objects missing from a group. The proposed methodologically will find out the identification of the missing objects and transmit the desired information in encrypted packet format for secured communication of the information.. Encrypted packets will be of 8-bit size and will be transferred to a remote analyzer through UART of ARM7. The analysis work will be done using serial monitoring software and the information will be displayed on a embedded user interface in encrypted form which will further be decrypted to get the desired information about the missing tags.

Keywords
ARM7, RF-ID Tags, LCD, UART

1. INTRODUCTION
The proposed work is based on 32 - bit Microcontroller. Here the system is designed using LPC2148 microcontroller which has on chip support for serial communication. The system is based on radio frequency identification technology and will find missing objects from a group of many objects. It will identify RFID tags which are having unique number for every different object. The proposed method will identify 10-bit unique IDs of missing objects from a group of objects by writing group-related information into the on chip flash memory. Retrieved information is encrypted for secured transmission and secured data packets are designed for the system which will send encrypted information in the form of packets for the missing objects from the given group of the objects and received packets will be analyzed after decryption and will give the correct information about the missing objects. Identification of missing objects also find out with the help of Group coding [1]. There are fundamental and False-positiveness group coding [2] but They are doing with the secured way and They design packet in encrypted form. This application is mainly used in very sensitive or highly confidential area, like military, defense etc. All information regarding missing objects is shown on LCD. It can not show any animated display on screen but characters and numbers can be displayed on the same LCD. User interface is designed using 16X2 character LCD which will show the mode of the device i.e. active or inactive and will also show the status of the scanned tags. Information regarding missing objects or tags will be transmitted in the form of secured packets using RS232 protocol. For secured transmission They will design encryption algorithm Using RSA algorithm. RSA Algorithm is the strongest algorithm for secured data transmission. Packet transmission will be done after encryption using encryption algorithm and key for encryption. Transmission of encrypted packets is done through serial communication. Packet analysis for received commands is done using X-CTU packet monitoring software. All transmitted data will be send to the analyzer for analysis using on-chip UART module.

In the block diagram They have used ARM7 microcontroller to design the complete system which is based on LPC2148 member of the given family. A character LCD display is used to design a display unit which will give details of the tags such as mode of operation, tag no., item code, item quantity, item type etc. The display panel will be interfaced with ARM7 microcontroller. The data bus and control bus of the LCD will be connected to the I/O pins of ARM7 microcontroller. Pin numbers P0.16 to P0.23 are used to be connected for data bus of the LCD. Data bus will be used to send data to the display panel and the control bus will be used to send commands to the display panel. A complete panel for control inputs will be designed which will be used to give control inputs to the systems. Depending upon the inputs from the control switch panel desired operations can be performed. Mode selection for operation will also be done using the same control switch panel. The bus size for the control switch panel will be four if They are using four input switches. There is not a linear relation between number of wires used for interfacing and number of control switches. A RF ID tag reader linear relation between number of wires used for interfacing and number of control switches. A RF ID tag reader module is also interfaced with ARM7 micro controller which will detect presence of RF tags around it. It has a constraint that tags should be in close vicinity of the reader module. This is a

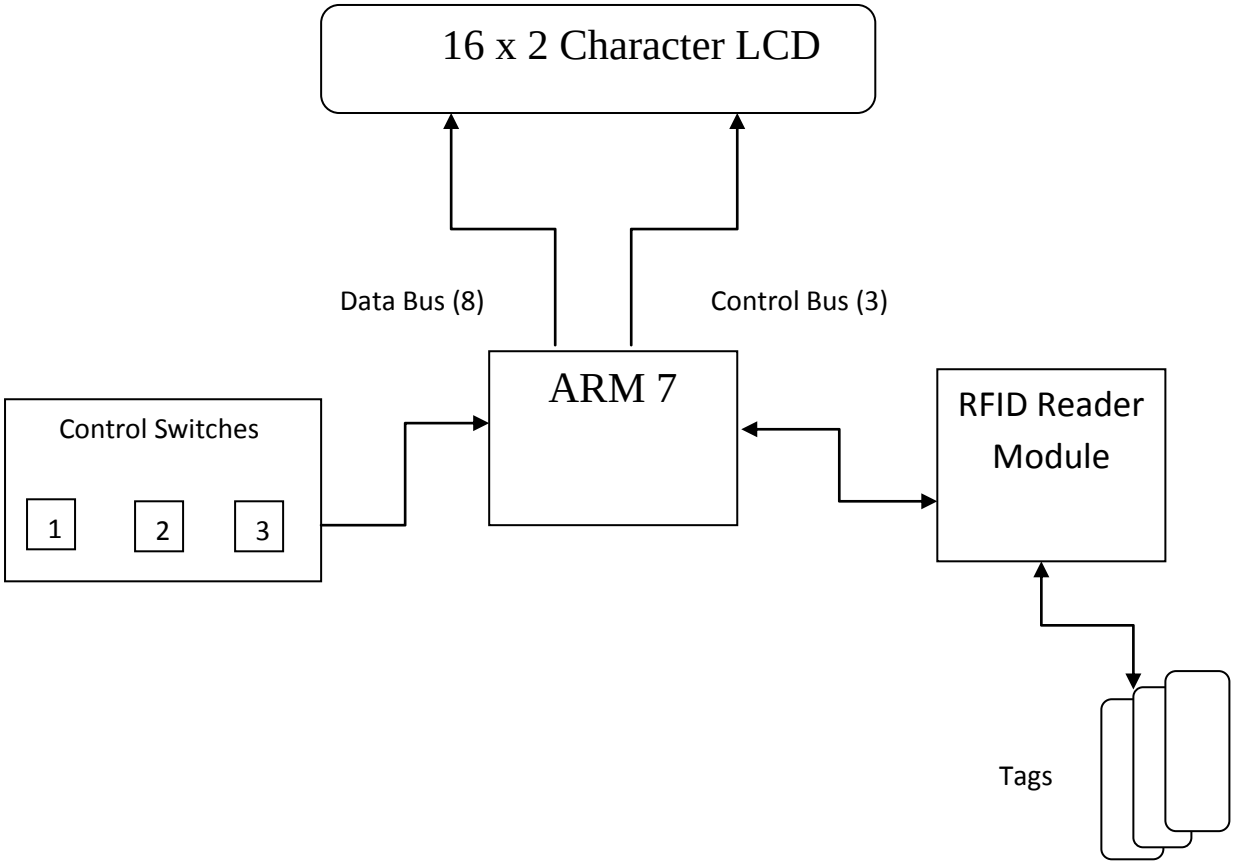

Figure1: Block Diagram of System Design

contactless RF tag reader module so no actual contact of the tags is required in this case. They have option for both types of tag readers i.e. contact based and contactless based tag readers but They have selected for contactless type tag readers since it suits our design.

2. RF IDENTIFICATION

Here They are using RF-Tags which are contact less so it can be easily read with the help of RFID reader module and no actual contact is required. In RFID reader module for data transmission They are using RS-232 connector. RS-232 is used for serial communication and is connected to Rx and Tx pins of ARM7 microcontroller. There are 9 pins on D- type connector for RS232 communication RFID reader module. RFID tag reader pin configuration as shown in below figure. [6] They are using passive tags as it suits our application.

A passive tag is an RFID tag that does not contain a battery; the power is supplied by the reader module. When radio waves from the reader are encountered by a passive RFID tag, the coiled antenna within the tag forms a magnetic field. The tag draws power from it, energizing the circuits in the tag. The tag then sends the information encoded in the tag's memory. [5]

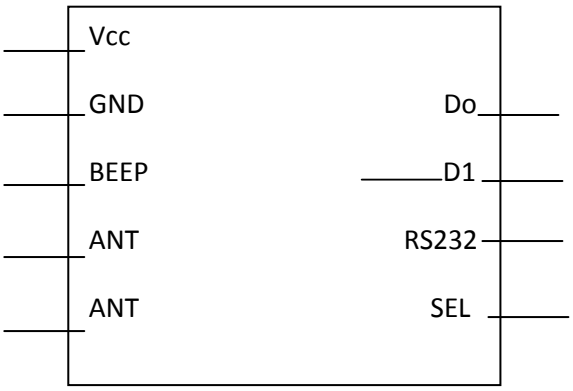

Figure2: RFID tag reader pin configuration

3. RSA ENCRPYTION ALGORITHM

RSA implements a public-key cryptosystem as well as digital signature. RSA implemented two important ideas, these are:

3.1 Public-key encryption. This idea omits the need for a "courier" to deliver keys to recipients over another secure channel before transmitting the originally - intended message. In RSA, encryption keys are public, while the decryption keys are not, so only the person with the correct decryption key can decipher an encrypted message. Everyone has their own encryption and decryption keys. The keys must be made in

such a way that the decryption key may not be easily deduced from the public encryption key.

3.2 Digital signatures. The receiver may need to verify that a transmitted message actually originated from the sender (signature), and didn't just come from there (authentication). This is done using the sender's decryption key, and the signature can later be verified by anyone, using the corresponding public encryption key. Signatures therefore cannot be forged. Also, no signer can later deny having signed the message.

This is not only useful for electronic mail, but for other electronic transactions and transmissions, such as fund transfers. The security of the RSA algorithm has so far been validated, since no known attempts to break it have yet been successful, mostly due to the difficulty of factoring large numbers n = p*****q, where p and q are large prime numbers. Here, They are using this algorithm for military or defense uses.

- **Secured RSA Algorithm**

The RSA algorithm is strongest algorithm. There is no encryption technique which is even perfectly secure from an attack by a realistic cryptanalyst. RSA Algorithm Methods are simple but lengthy and may crack a message, but not likely an entire encryption scheme. A probabilistic approach has to be considered, meaning there's always a chance someone may get the "one key out of a million". It is difficult to know that how to prove whether an encryption scheme is unbreakable not. If there is no way to prove it, it will be analyzed that at least if someone can break the code. This is how the RSA were essentially certified. Despite years of attempts, no one has been known to crack this algorithm. Such a resistance to attack makes RSA secure in practice. [4]

- **Public Key & Private key Selection**

Key Generation	
Select p.q	p,q both prime, p≠q
Calculate n=pxq	
Calculate $\phi(n)=(p-1)x(q-1)$	
Select integer e	$gcd(\phi(n),e)=1; 1<e<\phi(n)$
Calculate d	
Public key	KU = {e,n}
Private key	KR = {d,n}
Encryption	
Plain text	M<n
Ciphertext	C=Me (mod n)
Decryption	
Ciphertext	C
Plain text	M=Cd(modn)

Figure3: Encryption Algorithm Key selection [5]

Key Selection Procedure:

- Select two large prime numbers : p and q
  Let p=17 and q=11
- Now calculate n
  n = p x q
  n = 17 x 11 = 187
- Now calculate ϕ
  $\phi = (p-1)(q-1) = 16 \times 10 = 160$
- Now select e, lcd $(\phi,e) = 1; 0 < e < \phi$
  let e = 7.
- Now calculate d such that de mod $\phi = 1$
  for calculating this $\phi*k +1$ where k = 1,2,.....N
- 160k + 1 = 161, 321,481.....
- now this answer check which is divisible by 7
- 161 is divisible by7 giving us to d = 161/7 = 23
- Key 1 = {e , n } & Key 2 = {d , n}
- Key 1 = {7 , 187} & Key 2 = {23 , 187}

Now Key 1 is Public Key and Key 2 is Private Key.

4. PACKET DESIGNING

These packets will contain all the information related to tags. At the time of packet designing various issues have to be considered such as size of the packet, data to be sent in the packet, control information to be sent in the packets. Following figure gives a brief idea about the data bits and their position which They will be sending in the final packet to be transferred.

R1	R2	F1	F2	P1	P2	T1	T2

Figure4: Bit Pattern of transmitted packets

In Above figure R1 and R2 define regions like east, west, north, south. F1 and F2 define Factory or makers in regions respectively. P1 and P2 define product of the material. T1 and T2 define type of products.

For example

0	0	0	1	1	1	1	0

- Its first 2-bits stand for region, which is 00 for East region,
- Next 2-bits for factory which is 01 for CHD,
- Next 2-bits for product which is 11 for bullets and,
- Last 2-bits for Type of product which is 10 for size of bullets (in mm).

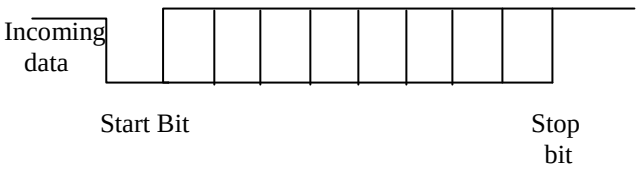

Figure5: Start and Stop bit identification in transmitted packets

Transmission of packets will be done with two synchronization bit – START BIT and STOP BIT. An eight

bit data packet will be transmitted through UART available inside LPC2148 microcontroller. The data transmission will be achieved through Tx pin of ARM7 controller. There is no need to keep track of start and stop bit but the UART itself will look after synchronization bits. The serial transmitted data will be analyzed using serial monitoring software X-CTU.

- **ENCRYPTION OF DATA PACKET**

Encryption of designing packets has been performed using RSA encryption algorithm. The packets contain 8 bit which is applied to the encryption algorithm using two keys denoted by p and q. These two keys are used as public key and private key which will enable us to encrypt the data packets securely. The encryption of the packets can be verified using RCA calculator and values of data packets can be taken from it after performing calculations.

5. ANALYSIS OF ENCRPYTED PACKETS

Packet analysis is the most important part in the proposed design since it will give information regarding the missing tags from the given set of goods. Packet analysis will be done using X-CTU packet monitoring software. In our case They will be using X-CTU packet monitoring software for packet analysis. All transmitted data will be sent to the analyzer for analysis using on-chip UART module. The received packets can be seen in the terminal window in hexadecimal formats. These packets can be decoded to analyze the plain text which will give the desired information.

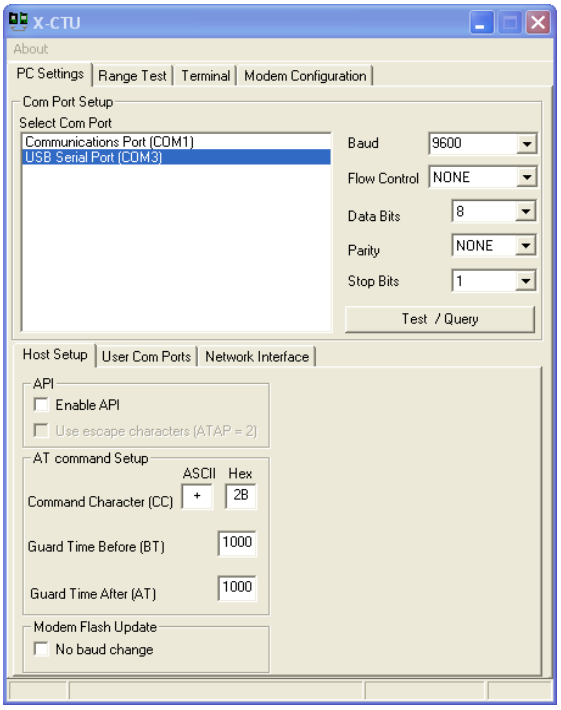

Figure6: Terminal window for serial data analyses

6. IDENTIFICATION OF MISSING OBJECTS

After decryption of the received packets the information regarding missing objects will be displayed on the LCD and simultaneously it will be displayed on the sent on the serial port which can further be analyzed on the serial monitoring software.

7. COMPARISON STUDY BETWEEN DIFFERENT ENCRYPTION ALGO.

The following give table represents the speed of three different encryption algorithms, i.e. DES, triple DES and RSA. In this table throughput of the encryption algorithm is calculated by dividing the total plaintext in Megabytes encrypted on total encryption time for each algorithm.

Input Size(KB)	3 DES	DES	RSA
45	50	25	55
55	44	29	46
96	76	45	89
236	113	39	119
319	155	89	157
560	171	131	169
899	299	240	309
5345	1166	1296	1441
Throughput (MB/Sec.)	2.08	3.01	1.67

Table1: Execution Time (Milliseconds) of Encryption of Different data packet size [11]

8. RESULT

The missing tags are identified from a group of tags and the corresponding information is displayed on the embedded user interface. The encrypted information is also transmitted on the serial port of ARM7 microcontroller and is analyzed on serial monitoring software i.e. X-CTU.

Following table gives the received packets which They have received after encryption

S. No	Tag Number	Missing Item
1.	5647834897	A # # >
2.	5672894305	A # # B
3.	6547890362	A # # !
4.	6689564537	A # # Z

9. CONCLUSION AND FUTURE SCOPE

Finally encrypted packets and embedded system has been designed which will identify the missing tags from a group of RFID tags and display the tag information on the display screen. The relevant information is displayed on the screen and it can be analyzed on X-CTU software and corrective measures can be taken to handle missing objects from a group.

The designed embedded system can be used for future applications in which it can have multiple RFID reader module for identification of missing tags simultaneously at two different locations and the same information can be send to a remote site using GSM technology.

10. ACKNOWLEDGEMENT

Special thanks to Mr. Arvind Pathak for the guidance and all the other faculty members for their support. At last special

thanks to Lingaya's University for its support and also providing labs with all the required equipments.

11. REFERENCES

[1] Yuki Sato,Yuki Igarshi, Jin Mitsugi, Osamu Nakamura and Jin Murai , "Identification of Missing Objects with Group Coding of RF tags", IEEE International Conference on RFID, pp. 95-101, june. 2012.

[2] Yuki Sato,Yuki Igarshi, Jin Mitsugi, Osamu Nakamura and Jin Murai , "Group Coding of RF tags to Verify the Integrity of Group of Objects", IEEE International Conference on RFID, pp. 200-206, aug. 2011.

[3] I.D Robertson and I. Jalaly S "RFID Tagging Explained" IEEE conference pp53-58, june. 2003.

[4] http://www.math.washington.edu/~morrow/336_09/papers/Yevgeny.pdf

[5] http://www.engineersgarage.com/embedded/pic-microcontroller-projects/rfid-interfacing-circuit-code.

[6] http://www.engineersgarage.com/embedded/pic-microcontroller-projects/rfid-interfacing-circuit-code.

[7] Muhammad Muazzem Hossain and Victor R. Prybutok "Consumer Acceptance of RFID Technology " IEEE Transaction of Engineering Management, pp. 316-327, may.2008

[8] Chiao-Tzu Huang, Li-Wen Lo, Wei-Ling Wang and Hsin-Lin Chen "A Study for Optimizing the Reading rate of RFID Tagged Cartons in Palletizing Process" IEEE conference pp. 1138-1142, aug. 2008.

[9] Jin-Sup Kim, Sang-Gi Byeon, Won-kyu Choi, Young-Cheol Kang and Eun-Ju Lee "An Active RFID Tag for Container Management" IEEE conference oct, 2005

[10] http://www.datasheetarchive.com/ARM7+LPC2148+block+diagram+of+lpc2148+microcontroller-datasheet.html.

[11] Aman Kumar, Dr. Sudesh Jakhar, and Mr. Sunil Makkar, "Comparative analysis between DES and RSA Algorithms", International Journal of Advanced Research in Computer Science and Software Engineering, July, 2012.