IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Novel Coding Scheme for Security in Communications in Passive RFID Systems

T.Renuka [1] ,D.Anitha Kumari[2]

Associate Lecturer[1 2]

Department of Electronics and Communication Engineering.[1 2]

Sir C. Ramalinga Reddy Polytechnic[1 2], Eluru[1 2], Andhra Pradesh[1 2], India[1 2].

ABSTRACT—Radio Frequency Identification (RFID) is an electronic tagging technology that allows objects to be automatically identified at a distance without a direct line-of-sight using an electromagnetic challenge-and- response exchange of data. Due to the computational power constraints of passive tags, non-encryption- based singulation protocols have been recently developed, in which wireless jamming is used. In this project, we are proposing a novel coding scheme, namely Random Flipping Random Jamming (RFRJ), to protect tags' content. Further, as an enhancement, we are implementing low power memory organization coding which provides more robust and reliable low power data as output.

INDEX TERMS — Electronic tagging technology, passive tags ,Radio Frequency Identification (RFID), Random Flipping Random Jamming (RFRJ).

I INTRODUCTION

In October 1999, the United States Federal Communications Commission (FCC) allocated 75 MHz of spectrum in the 5.9 GHz band to be used by intelligent transportation systems (ITS).[2] In August 2008, the European Telecommunications Standards Institute (ETSI) allocated 30 MHz of spectrum in the 5.9 GHz band for ITS By 2003, it was used in Europe and Japan in electronic toll collection DSRC systems in Europe, Japan and U.S. are not compatible and include some very significant variations (5.8 GHz, 5.9 GHz or even infrared, different baud rates, and different protocols).Singapore's Electronic Road Pricing scheme uses DSRC technology for road use measurement. [2] Other possible applications were:

- Emergency warning system for vehicles
- Cooperative Adaptive Cruise Control
- Cooperative Forward Collision Warning
- Intersection collision avoidance
- Approaching emergency vehicle warning (Blue Waves)
- Vehicle safety inspection
- Transit or emergency vehicle signal priority
- Electronic parking payments
- Commercial vehicle clearance and safety inspections
- In-vehicle signing
- Rollover warning
- Highway-rail intersection warning
- Electronic toll collection

II METHODOLOGY

RFID (Radio Frequency Identification) is an ADC (Automated Data Collection) technology that:

1Uses radio-frequency waves to transfer data between a reader and a movable item to identify, categorize, track...

2Is fast and does not require physical sight or contact between reader/scanner and the tagged item.

3. Performs the operation using low cost components.

4. Attempts to provide unique identification and backend integration that allows for wide range of applications.

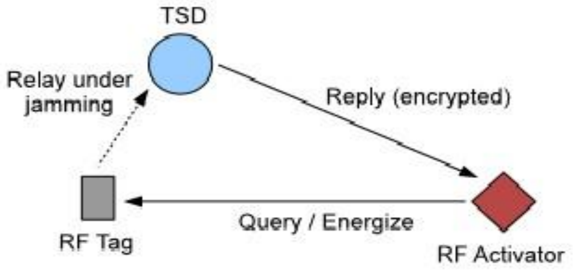


Fig.1: Proposed design

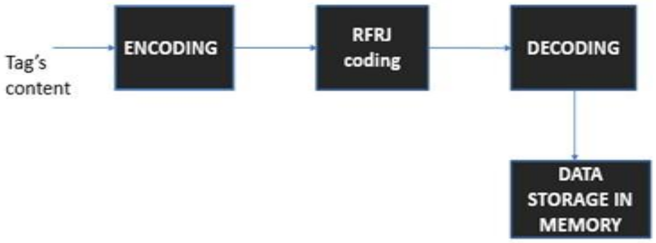


Fig.2: Block diagram

Coding rules:

Table: 1 Coding rules

	$b_k = 0$	$b_k = 1$
$b_{k-4}b_{k-3}b_{k-2}b_{k-1}$	c	c'
0000	0000	1111
0001	0011	1100
0010	0001	1110
0011	1101	0010
0100	0101	1010
0101	1001	0110
0110	1000	0111
0111	1011	0100
1000	1111	0000
1001	1100	0011
1010	1110	0001
1011	0010	1101
1100	1010	0101
1101	0110	1001
1110	0111	1000
1111	0100	1011

The tag‟s content is encoded generally and some of the bits of encoded data are randomly flipped and randomly jammed. The resultant data is transmitted by the TSD from tag to reader. After reception, the reader decodes the original data from a set of code rules. Next, the decoded data is stored in the memory.

[1]

III DETAILED DESIGN 1-To-4- RFRJ Coding Scheme:

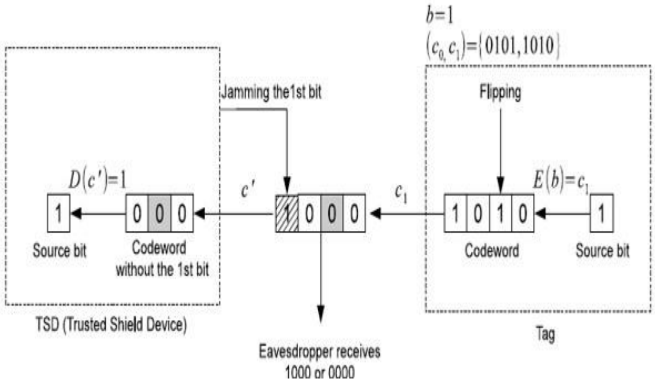

$b=1$
$(c_0, c_1)=\{0101,1010\}$
Jamming the1st bit
Flipping
$D(c')=1$
c'
c_1
$E(b)=c_1$
1
0 0 0
1 0 0 0
1 0 1 0
1
Source bit
Codeword without the 1st bit
Codeword
Source bit
TSD (Trusted Shield Device)
Eavesdropper receives 1000 or 0000
Tag

Fig.3: RFRJ coding Scheme

For source bit 1”1010” (c1) is selected

For source bit 0”0101” (c0) is selected

In general, we call lb-to-lc, the RFRJ coding scheme. For instance, the coding with lb=1 and lc=4 is said to be the 1-to-4 RFRJ coding scheme. A source bit is encoded into a 4-bit codeword. The tag flips the third bit in the codeword, which is colored gray, and the TSD selects the first bit for jamming, which is crossed off. Assume the original code-word is 1010.

Since the tag flips the third bit, it will send 1000 over the backward channel. Meanwhile, the TSD jams the first bit. Hence, the TSD and the eavesdropper will receive X000, where X could be decoded to either 0 or 1.For the eavesdropper, two out of the 4 bits may contain errors. Thus, the TSD and the eavesdropper have a different amount of information to decode the original codeword. [4]

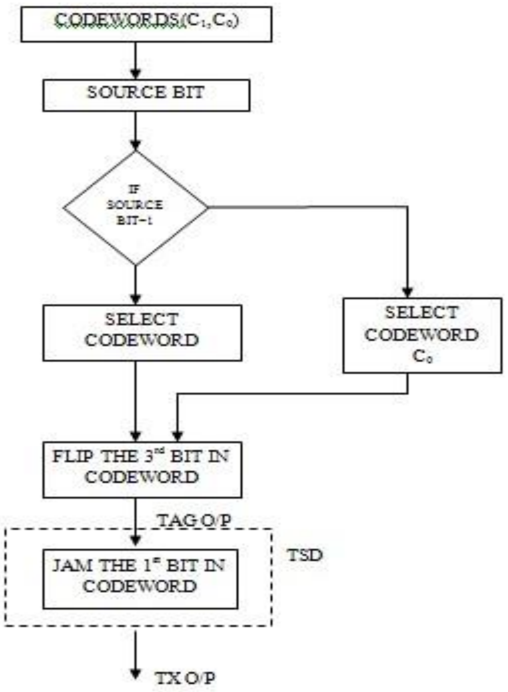


Fig. 4: Flow chart for transmitter section

IV RING COUNTER WITH CLOCK GATED BY SR FLIP-FLOP

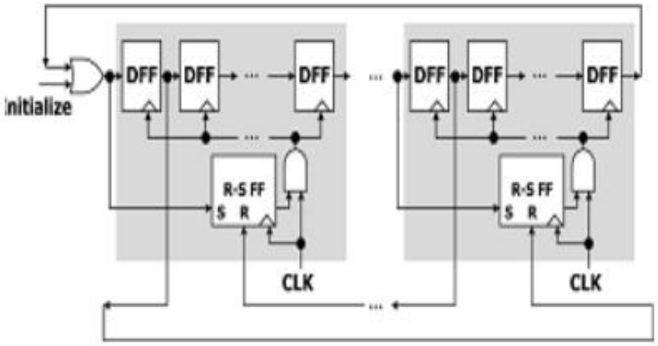


Fig.5: Ring Counter With Clock Gated By SR Flip-Flop

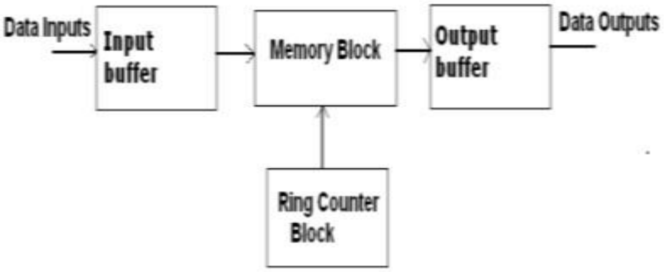


Fig.6: Block diagram of delay buffer existing technique After receiving the data, the receiver stores the information of tag in the memory which is present at the back-end infrastructure. In order to store a data in a memory, the buffers in the memory should be selected sequentially. Thus, we are presenting the circuit design of a low power delay buffer.

V RING COUNTER WITH CLOCK GATED BY CELEMENTS

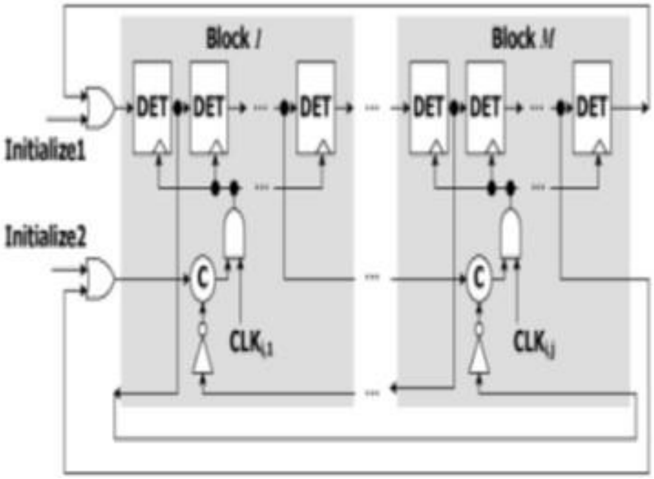
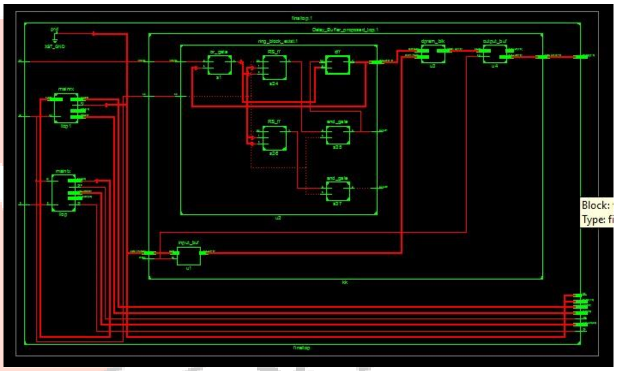


Fig.7: Ring Counter With Clock Gated By C-Elements

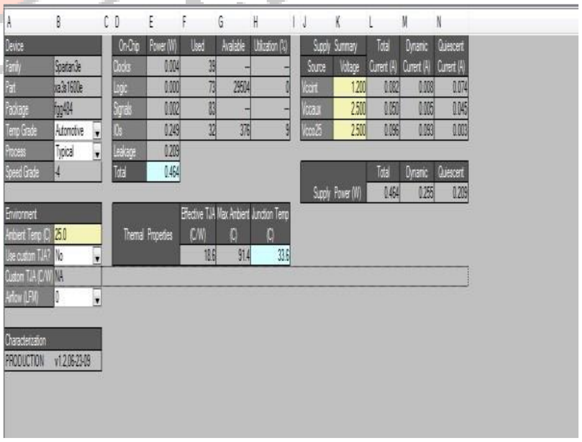
Logic of C-element= AC+AB+BC

VI RESULTS

RTL schematic of existing technique:



Power results of existing technique:



Device	
Family	Spartan3e
Part	xa3s1600e
Package	fgg484
Temp Grade	Automotive
Process	Typical
Speed Grade	-4

On-Chip	Power (W)	Used	Available	Utilization (%)
Clocks	0.004	39	---	---
Logic	0.000	73	29504	0
Signals	0.002	83	---	---
IOs	0.249	32	376	9
Leakage	0.209			
Total	0.464			

Supply Summary		Total	Dynamic	Quiescent
Source	Voltage	Current (A)	Current (A)	Current (A)
Vccint	1.200	0.082	0.008	0.074
Vccaux	2.500	0.050	0.005	0.045
Vcco25	2.500	0.096	0.093	0.003

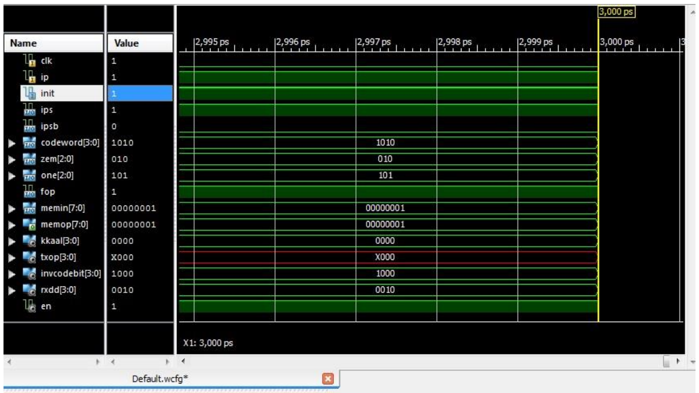
	Total	Dynamic	Quiescent
Supply Power (W)	0.464	0.255	0.209

Environment	
Ambient Temp (C)	25.0
Use custom TJA?	No
Custom TJA (C/W)	NA
Airflow (LFM)	0

Thermal Properties	Effective TJA (C/W)	Max Ambient (C)	Junction Temp (C)
	18.6	91.4	33.6

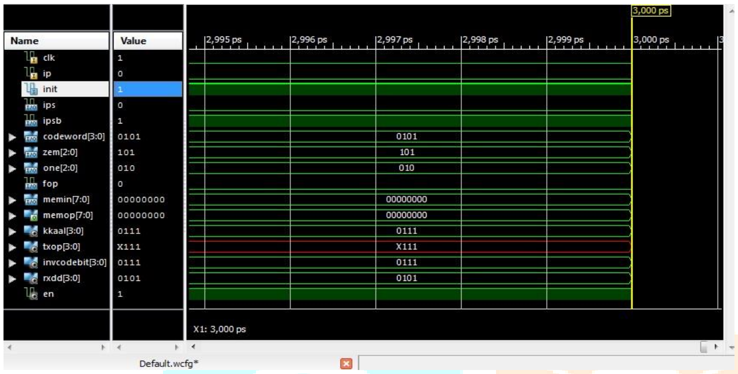
Characterization	
PRODUCTION	v1.2,06-23-09

Simulation output for input „1":



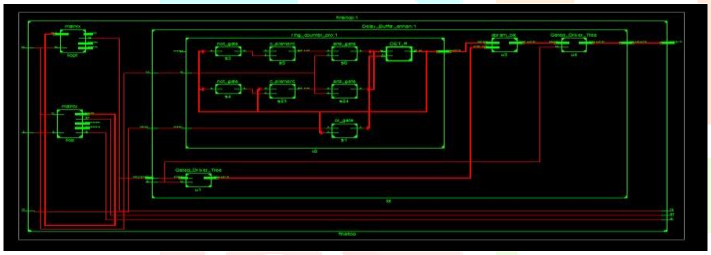
Name	Value
clk	1
ip	1
init	1
ips	1
ipsb	0
codeword[3:0]	1010
zem[2:0]	010
one[2:0]	101
fop	1
memin[7:0]	00000001
memop[7:0]	00000001
kkaal[3:0]	0000
txop[3:0]	X000
invcodebit[3:0]	1000
rxdd[3:0]	0010
en	1

Simulation output for input „0‟:

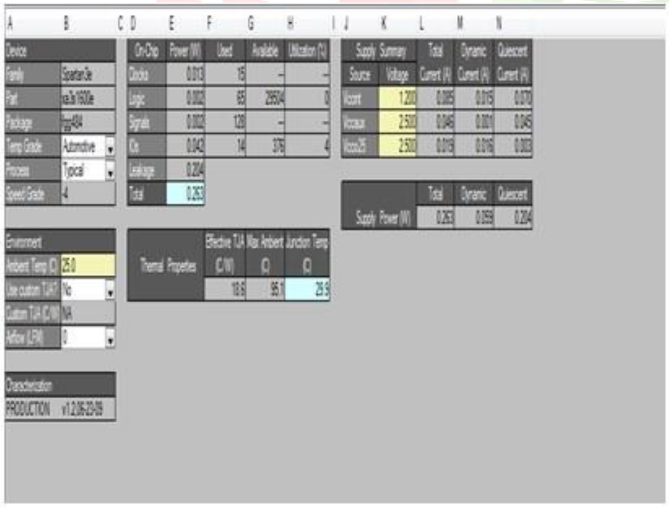


Name	Value
clk	1
ip	0
init	1
ips	0
ipsb	1
codeword[3:0]	0101
zem[2:0]	101
one[2:0]	010
fop	0
memin[7:0]	00000000
memop[7:0]	00000000
kkaal[3:0]	0111
txop[3:0]	X111
invcodebit[3:0]	0111
rxdd[3:0]	0101
en	1

RTL schematic of proposed technique:



Power results of proposed technique:



Device	
Family	Spartan3e
Part	xa3s1600e
Package	fgg484
Temp Grade	Automotive
Process	Typical
Speed Grade	-4

On-Chip	Power (W)	Used	Available	Utilization (%)
Clocks	0.013	15	---	---
Logic	0.002	65	29504	0
Signals	0.002	128	---	---
IOs	0.042	14	376	4
Leakage	0.204			
Total	0.263			

Supply Summary		Total	Dynamic	Quiescent
Source	Voltage	Current (A)	Current (A)	Current (A)
Vccint	1.200	0.085	0.015	0.070
Vccaux	2.500	0.046	0.001	0.045
Vcco25	2.500	0.019	0.016	0.003

	Total	Dynamic	Quiescent
Supply Power (W)	0.263	0.059	0.204

Environment	
Ambient Temp (C)	25.0
Use custom TJA?	No
Custom TJA (C/W)	NA
Airflow (LFM)	0

Thermal Properties	Effective TJA (C/W)	Max Ambient (C)	Junction Temp (C)
	10.6	95.1	25.9

Characterization	
PRODUCTION	v1.2,06-23-09

VII CONCLUSION

In this project, we presented a new architecture of RFID systems which provides security and a low power delay buffer architecture using a ring counter with clock gated by the C-elements to reduce power consumption

REFERENCES:

[1] Y. Li and X. Ding, "Protecting RFID communications in supply chains," in Proc. 2nd ACM Symp. Inf., Comput. Commun. Security, 2007, pp. 234–241.

[2] H. K. H. Chow, K. L. Choy, W. B. Lee, and K. C. Lau, "Design of a RFID case-based Resource management system for warehouse operations," Expert Syst. Appl., vol. 30, no. 4, pp. 561–576, Feb. 2006.

[3] A. Juels, "RFID security and privacy: A research survey," IEEE J. Sel. Areas Comm., vol. 24, no. 2, pp. 381–394, 2006.

[4] K. Sakai, W.-S. Ku, R. Zimmermann, and M.-T. Sun, "Dynamic bit encoding for privacy protection against correlation attacks in RFID backward channel," IEEE Trans. Comput., vol. 62, no. 1, pp. 112–123, Jan. 2013.

[5] M. Jain, J. L. Choi, T. M. Kim, D. Bharadia, S. Seth, K. Srinivasan, P. Levis, S. Katti, and P. Sinha, "Practical, realtime, full duplex wireless," in Proc. 17th Annu. Int. Conf. Mobile Comput. Netw. 2011, pp. 301–312.

[6] D. D. Donno, F. Ricciato, L. Catarinucci, A. Coluccia, and L. Tarricone, "Challenge: Towards distributed RFID sensing with software-defined radio," in Proc. 16th Annu. Int. Conf. Mobile Comput. Netw. 2010, pp. 97–104.

[7] L. Sang and A. Arora, "Capabilities of low-power wireless jammers," in Proc. INFOCOM, 2009, pp. 2551–2555.

[8] J. Myung, W. Lee, J. Srivastava, and T. K. Shih, "Tagsplitting: Adaptive collision arbitration protocols for RFID tag identification," IEEE Trans. Parallel Distrib. Syst., vol. 18, no. 6, pp. 763–775, Jun. 2007.

[9] A. Juels, R. Pappu, and B. Parno, "Unidirectional key distribution across time and space with applications to RFID Security," in Proc. USENIX Secur. Symp ., 2008, pp. 75–90.

[10]S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," in Proc. 1st Int. Conf. Security Pervasive Comput., 2003, pp. 201–212.

[11]A. Czeskis, K. Koscher, J. R. Smith, and T. Kohno, "RFIDs and secret handshakes: Defending against ghost-andleech attacks and unauthorized reads with context-aware communications," in Proc. 15th ACM Conf. Comput. Commun. Security, 2008, pp. 479–490.