efficiently reduces the design and development time and cost, and achieves flexible and efficient way.

The MAC layer processes communication commands. A reader communicates to tag populations using three basic operations: Select, Inventory, Access. There are 14 commands to communicate with tag, including Select, Query, Query_adjust, Query_rep, Ack, Nak, Req_rn, Read, Write, Kill, Lock, Access, Block_write and Block_erase.

According to select command, the particular tag population based on user defined criteria will be selected. Query command initiates an inventory round and decides which tags will participate in the round query .Query command contains a slot-count parameter Q ,which make the tags to produce a random time slot. Query_adjust command repeats a previous query and may increment or decrement Q, but does not introduce new tags into the round. Query_rep command repeats a previous query without changing any parameters and introducing new tags into the round. Ack command is to acknowledge the tag. Nak command causes all tags in the inventory round to return to arbitrate without changing their inventoried flag. Rq_rn command is to obtain a new RN16. Read, Write, Kill, Lock,Block_write and Block_erase commands are to write or erase tags memory.

Figure 6 shows the implementation of the inventory procedure. First, the baseband CPU configures reader's mode, which including modulator and encoder configuration. The reader sends 5ms continues carrier wave to wake up the tags, then it sends Select command to select particular tag populations. After waiting for 300us carrier wave, the reader sends Query command. Query command initiates an inventory round, and the reader waits for the 16bit random number response. Reader sends Select command repeatedly when it is timeout. After getting RN16 from the tag, the reader sends ACK command to request tag's EPC. If reader could receive the EPC from the tag, then it will get the EPC from the buffer memory. Otherwise it sends Select command again.

As RFID tag is stored with a unique Electronic Product Code (EPC) and related product information, which raises important security and privacy issues. RFID tag and reader use wireless communication and the channel is considered not secure. In most standards, authentication feature are based on a simple password system or access control password, where security can be easily cracked by eavesdropping a password. In EPC global C1G2, the standard specifies that a tag has four memory banks: Reserved, EPC, TID, and User. 32-bit Access Password (APwd) and

32-bit Kill Password (KPwd) are stored in Reserved memory bank, and EPC number is stored in EPC memory.

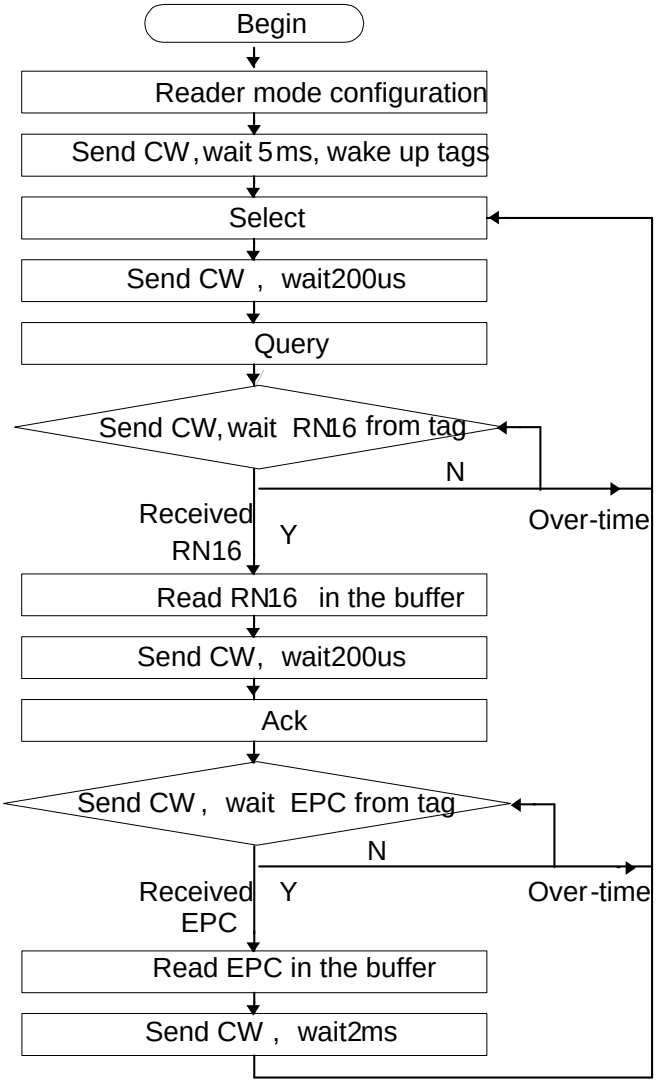

Figure 6. Inventory procedure

APwd and KPwd are protected because the reserved memory bank is not allowed to be read or written by any reader. APwd is used when data are needed to be exchanged between a reader and a tag. A compliant RFID reader can use KPwd to permanently disable the tag.

It is very easy to understand the multi-step procedure shown in Figure 7. RT1 and RT2 are random number, they use XOR operation to obscure APwd, which is known as Cover-Coding APwd (CCPwd). XOR operation shall be performed on APwd's 16-bit Most Significant Bits

(MSB) APwdM firstly, then be performed by 16-bit Least Significant Bits (LSB) APwdL. The cover-coding make the reader-to-tag communications more safety, as a reader performs an XOR operation for data encryption. Then, a tag can recover the received messages by doing another XOR operation. Assuming that the signals from a tag to a reader are too weak to be eavesdropped by the attacker, this cover coding scheme is an effective encryption scheme. However, an enhanced receiver or an implanted receiver near to a tag can make the cover-coding scheme useless.

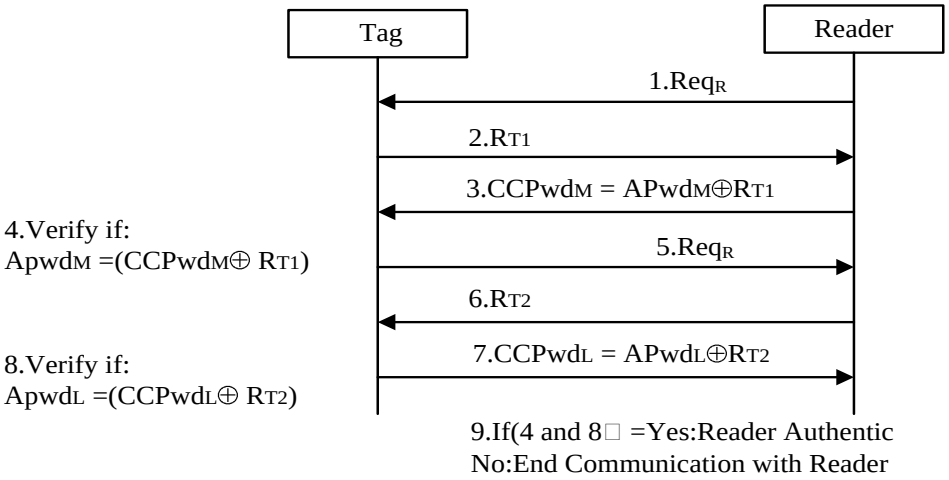

Figure 7. Authentication scheme between a reader and a tag

IV. EXPERIMENTAL RESULTS

The development platform Quartus II is embedded in Signaltap II Logic Analyzer. We could use Signaltap II Logic Analyzer to observe the function of FPGA internal circuits and capture the signals of the baseband circuit. Some verification results of baseband modules are shown below. The verification results of ASK demodulator are shown in Figure 8, When I signal is stronger than Q signal, I signal can be demodulated successfully. The verification results of FM0 decoder are shown in Figure 9 and the results of Miller decoder are shown in Figure 10. The verification results of bit synchronization module are shown in Figure 11. Synchronous data can be successfully extracted from the input data and clock signal.

In RF transmitter, the signal generator generates RFID baseband PIE coded signals, such as Read command 1100001011100111110000001. Zero symbol length of time of Tari is set to 25us and

transmission rate is 40Kbps. When the signals is encoded and input to RF system, the rate is 80Kbps. Access by the differential I/Q quadrature signals to the up-conversion, after a pre-amplifier and power amplifier, the output RF signals go through a 30dB attenuator and enter into the spectrum analyzer. The spectrogram of RF signal is shown in figure 12. The spectrum Span is set to 1MHz and channel width is 500KHz. Channel power is about 24dBm. Power spectral density is 65.24dBm/Hz and the coaxial cable loss is about 2dB. The power of the RF output signal is less than the expected power approximately 3dB, but it is still in the adjustable range of the output power.

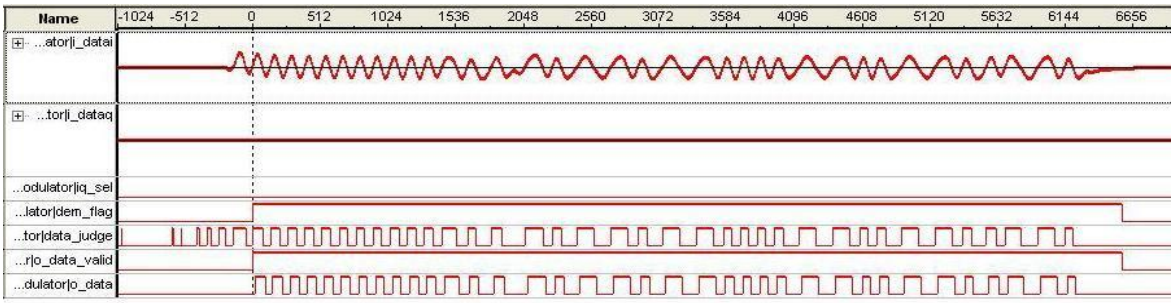

Figure 8. The verification results of ASK demodulator

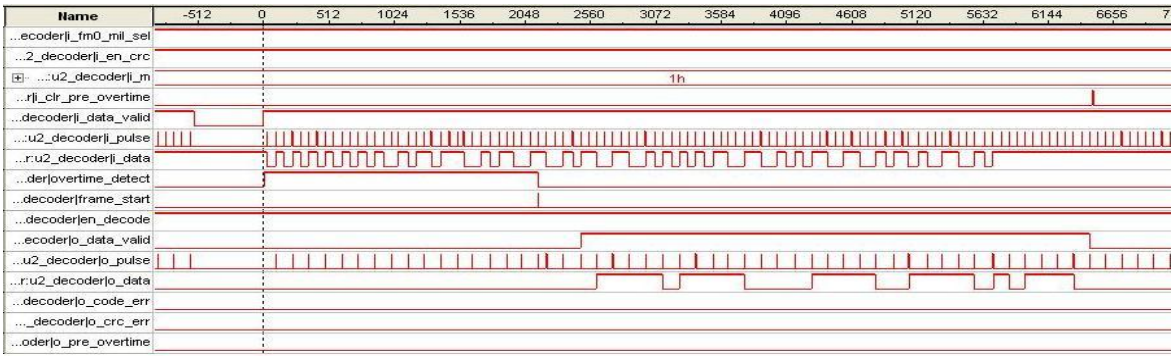

Figure 9. The verification results of FM0 decoder

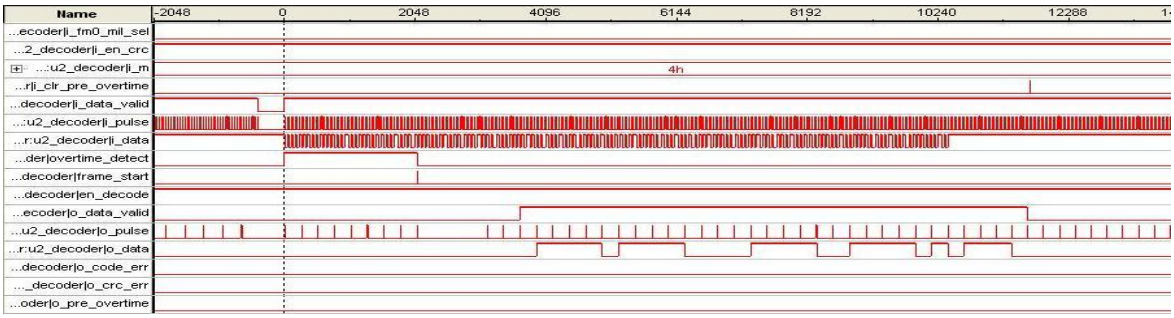

Figure 10. The verification results of Miller decoder

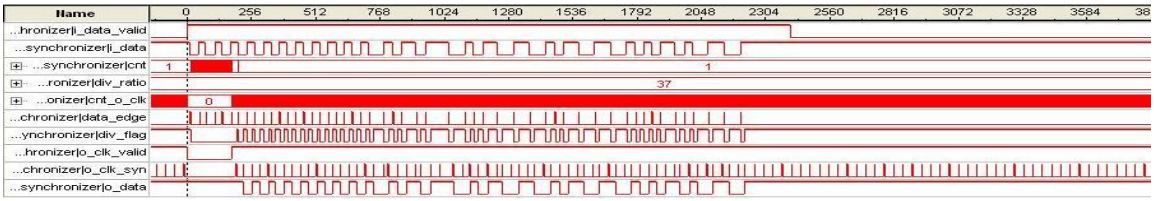

Figure 11. The verification results of bit synchronization

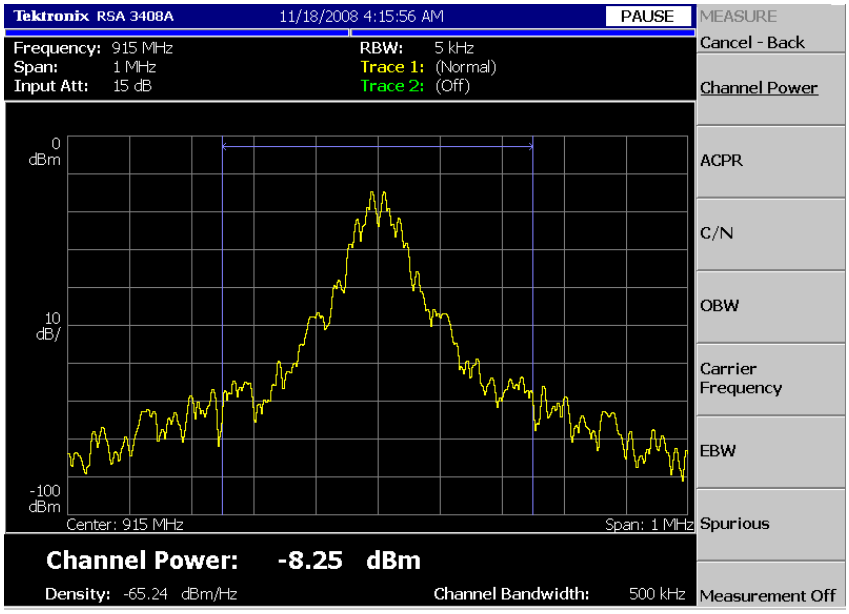

Figure 12. The spectrogram of RF transmission signal

In the RF receiver, the reader receives the backscatter signals of the tag. The signals are encoded in FM0 with a rate of 80kbps.After frequency conversion by the 915MHz signal generator ,the power of received signal is -70dBm,as shown in figure 13.

The received RF signals are down converted to the baseband frequency by the quadrature demodulator, and then amplified by an operational amplifier and filtered by the low pass filter. After FM0 decoding, the received data are 000000000000(12 preamble codes) 1010V1 (synchronous preamble codes) 0100010000000101 (the RN16 returned by tag). The final baseband waveforms of received signals are shown in figure 14. The demodulated signals are completely match with original command and the signals' amplitude is satisfied with the sampling requirements of the ADC.

The waveform of transmitting signal from reader and the waveform of backscatter signal from tag could be captured by the spectrum analyzer. The communication process between the reader

and tag is shown in Figure 15. Select and Query commands are sent by reader, then the tag responses with RN16.When the reader sends ACK, it will get EPC from the tag.

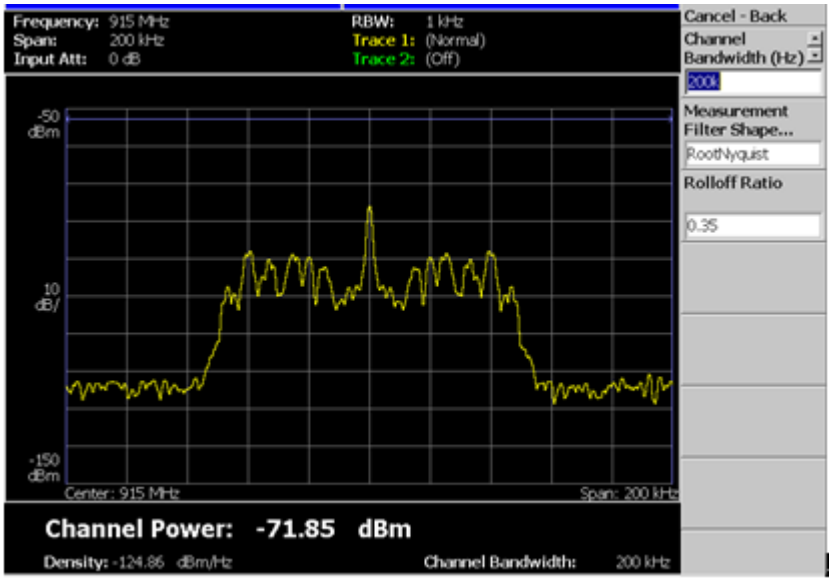

Figure 13. The spectrogram of RF received signal

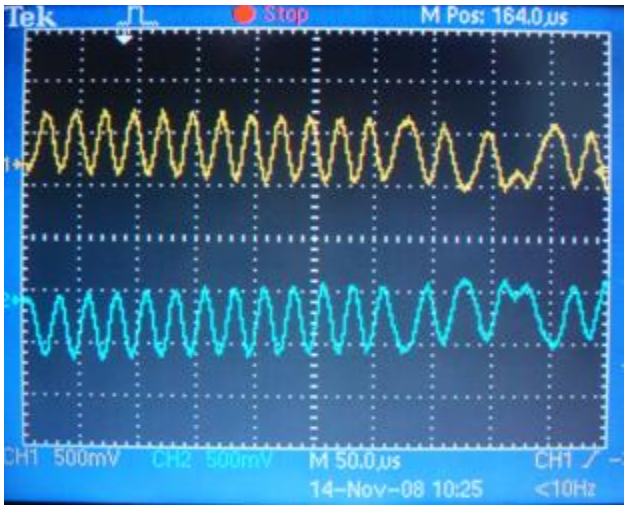

Figure 14. The baseband waveforms of received signals

Software in NIOS II continuous read the tag's EPC information and sends the tag's EPC to the host computer via an RS232 interface. Computer uses UART software to responsible for receiving from the NIOS II information. If the reader correctly reads the tag's EPC Information, then it displays the EPC data and length. If the reader can not correctly read the tag EPC information, it displays an error. For example, when waiting timeout, violations of FM0/Miller coding rules error or CRC checksum error happened, it displays an error. During the debug

process, adjusting the distance between the reader and the tag, the reader can correctly read the tag's EPC information within 3 meters .The results verify the reader could meet the design requirements.

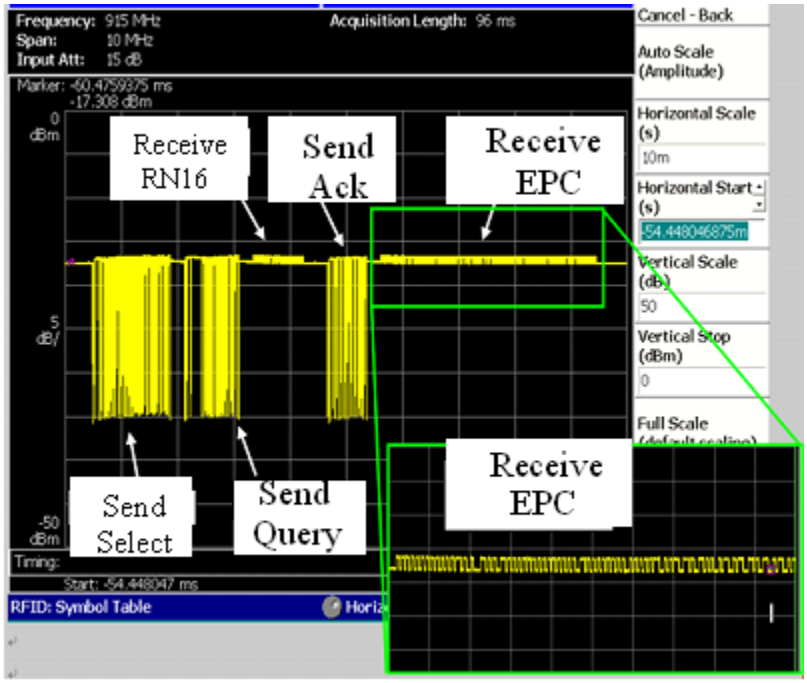

Figure 15. Communication between the reader and tag

V. CONCLUSIONS

This paper presents design and realization of a UHF RFID reader, which is compatible with EPC C1G2 Standard. The experimental results demonstrated that the reader could send commands and receive data from the tag correctly. The designed reader's architecture is not only applicable for EPC C1G2 protocol, but also applicable for other RFID standards. The ISO18000 6A/6B/6C protocols share the same uplink configuration, which is similar with EPC C1G2, but they differ in the downlink modulation and anti collision approach, however they could also be realized in this platform. The FPGA is a system controller and baseband processor .It could be flexible adjusted to implement physical layer of different protocol. The NiosII core in FPGA performs all commands and controls and could achieves rapid, flexible and efficient development. Since all standard dependent properties could be mapped into reconfigurable hardware components in FPGA. We use verilog HDL language to implement the MAC layer of EPC C1G2 protocol with all the states, commands and functions. We will focus on the development of a framework

supporting multiple receive and transmit antennas to enable MIMO RFID systems in future work. By this means it is expected to greatly improve the detection range and the data rate. We observe that EPC C1G2 protocol lacks the security features to make the EPC-ID secure or to have a mutual authentication between the tags and reader. Hence there is a need to integrate security protocol with the EPC C1G2 to have a secure communication.

ACKNOWLEDGEMENTS

The work is supported by zhejiang provincial natural science foundation of china (No.Y1110992)and zhejiang provincial key innovative team foundation of china(No.2010R50010).

REFERENCES

[1] K. Finkenzeller, “RFID Handbook”, Wiley ,2nd,pp.7-9, 2004.

[2] K. V. S. Rao, “An overview of backscattered radio frequency identification system (RFID)” IEEE Microwave Conference, Vol. 3, pp. 746-749, November 1999.

[3] EPCglobal, “EPC Radio-Frequency Identity Protocol,Class-1 Generartion-2 UHF RFID Protocol for Communications at 860-960MHz”,ver 1.1.0,2005.

[4] Huihui Li, Xuanqin Mou,“A New Implementation of UHF RFID Reader”,TENCON 2009 IEEE Region 10 Conference , pp.1-4, Singapore, January 2009.

[5] N. Roy, A. Trivedi, and J. Wong, “Designing an FPGA-Based RFID Reader”,XCell Journal, Vol.2, No.26, pp. 26-29,2006.

[6] C. Angerer, B. Knerr, M. Holzer, A. Adalan, and M. Rupp, “Flexible Simulation and Prototyping for RFID Designs”, Proceedings of the first international EURASIP Workshop on RFID Technology, pp.51-54, September 2007.

[7] X. D. Pang, X. S. Yao and C. P. Liang, “Design and Realization of a Highly Integrated UHF RFID Reader Module”, Microwave and Millimeter Wave Technology, Vol. 3,pp. 1506-1508, 2008.

[8] J. M. Zhang, S. L. Lai and Y. T. Chen, “The Application of DSP Sampling and Identifying in UHF RFID Reader”, Science Technology and Engineering, Vol. 6, No. 8,pp. 956-959, 2006.

[9] C. Floerkemeier and S. Sarma, "RFIDSim-A Physical and Logical Layer Simulation Engine for Passive RFID", IEEE Trans. on Automation Science and Engineering, Vol. 6,No. 1,pp. 33-43, 2009.

[10] S.R. Banerjee, R. Jesme, and R.A. Sainati, " Performance analysis of short range UHF propagation as applicable to passive RFID", In the Proceedings of the IEEE International Conference on RFIDpp.30-36, USA,March 2007.

[11] Christoph Angerer, Robert Langwieser, Markus Rupp, "Evaluation and exploration of RFID systems by rapid prototyping", Personal and Ubiquitous Computing, Vol.16, Issue 3, pp.309-321, March 2012.

[12] P. V. Nikitin, K. V. S. Rao, "Theory and Measurement of backscattering from RFID tags", IEEE Antennas and Propagation Magazine,Vol.48,pp.212-218, 2006.

[13] D.M. Dobkin, "The RF in RFID: Passive UHF RFID in Practice", Elsevier, pp.110-137,2007.

[14] P.V. Nikitin and K.V.S. Rao, "Performance Limitations of Passive UHF RFID Systems", Antennas and Propagation Society International Symposium 2006, pp.1011-1014, Albuquerque, USA, July,2006.

[15] P.V. Nikitin , K.V.S. Rao, "Antennas and Propagation in UHF RFID Systems", in IEEE Int. Conf. on RFID, pp. 277-288, Las Vegas, USA, April 2008.

[16] Byung-Jun Jang. "Phase diversity and optimal I/Q signal combining methods on an UHF RFID reader's receiver", Microwave Journal(Web Exclusive), Vol. 51, No. 4, April 2008.

[17] H. Yoon,B.J. Jang, "Link budget calculation for UHF RFID systems", Microwave Journal, Vol. 51, No. 12, pp. 78-77, December 2008.

[18] Koswatta, V. Randika, Karmakar, C.Nemai, "A Novel Reader Architecture Based on UWB Chirp Signal Interrogation for Multiresonator-Based Chipless RFID Tag Reading" ,IEEE Transactions on Microwave Theory and Techniques, Vol. 60,No.9, pp.2925-2933,September 2012.

[19] Ji-Noon Bae, WonKyu Choi,Chan-Won Park, "Design of Reader Baseband Receiver Structure for Demodulating Backscattered Tag Signal in a Passive RFID Environment ",ETRI Journal,Vol. 34 ,No. 2, pp.147-158 , April 2012.

[20] O. Bjelica, D Mijic," Hardware design of a reader device in RFID-based class-attendance system",Proc. TELFOR 2012, pp. 1068-71, Serbia, November 2012.

[21] Zheng Wang,Haifeng Zhang. Yubo Wang, "UHF RFID reader with separate central frequencies for forward and reverse links",2012 IEEE International Conference on RFID Technologies and Applications , pp. 212-215, France ,November 2012.

[22] Boyang Zhang,Guangjun Wen,Liu Yang, " Single chip UHF RFID reader digital baseband design ", 2012 International Conference on Wavelet Active Media Technology and Information Processing ,pp.203-206,Chengdu, China, December 2012.

[23] Hongyi Wang, Yang Qing, Wu Jian-fei,"A Novel Implementation of UHF RFID Reader ",3rd International Conference on Digital Manufacturing and Automation ,Vol.190-191,pp.642-646, Guangxi,China,Auguest 2012.

[24] S. Merilampi, T. Björninen, L. Sydänheimo, and L. Ukkonen, "Passive UHF RFID strain sensor tag for detecting limb movement",International Journal on Smart Sensing and Intelligent Systems,Vol.5,No.2, pp.315-328, June 2012.