Low Power VLSI Design for a RFID Passive Tag baseband System Enhanced with an AES Cryptography Engine

Adam S.W. Man, Edward S. Zhang, Vincent K.N. Lau, C.Y. Tsui, and Howard C. Luong
Department of Electronic and Computer Engineering
The Hong Kong University of Science and Technology
Email: adamman@ust.hk

Abstract— **This paper describes a low power implementation of a secure EPC UHF Passive RFID Tag baseband system. To ensure the secure information transaction of the tag, traditionally the focus is on directly applying a low-complexity encryption engine. However, this approach could lead to the problem of known-plaintext attack (KPA). The attacker could make use of the known header to reveal the secret key. Our contributions are proposing a novel dataflow solution enforced by an AES cryptography engine embedded inside the passive RFID tag. Also, various low power design techniques are proposed to reduce the power consumption of the baseband of the passive tag. In particular, we propose a moving window PIE decoding algorithm and an improved Tausworthe sequence generator to reduce the power consumption. Other low power design techniques such as clock gating, optimal clock driving and parallel operations are extensively used in the design of the tag. The complete RFID tag which consists of an analog frontend, 136 bits one-time programmable (OTP) memory, charge pump, rectifier, clock divider, and the proposed baseband system, was designed using TSMC 0.18μm process and verified. The area of the proposed baseband system is 0.446mm^2 and from the power simulation, the overall power consumption of the baseband system with the AES encryption is about 4.695 uW.**

Index Terms —RFID, Tag, AES, Low Power

I. Introduction

RFID is an automatic identification technology which can be applied in many applications, such as supply chains management, product tracing, building access control and automatic product checkout [1]. The cost of a passive RFID tag has been dropped to the range from 0.05 to 0.1 USD, and this stimulates the growth of its usage [2]. With RFID technology, fast and accurate recognition of objects could be achieved with a very low cost.

At the same time, the mass usage of RFID has raised concerns regarding security and privacy issues [3]. One of the primary security concerns regarding RFID technology is the illicit tracking of RFID tags. For examples, thieves with RFID readers could scan and track crowds for high-value banknotes. Police could also abuse a convenient method of cradle-to-grave surveillance. Existing passive tag is small, highly mobile, and there is no agreed security solution for low cost RFID systems in the market. Therefore, a passive tag is easily to be trailed, monitored and even copied by adversaries [4]. Conventionally the simplest way to enhance privacy is directly "kill" the tag after purchasing, but the drawback is that the clients could not use the tag anymore. Another approach is to use hash-lock schemes to authenticate the readers [5]. However, this method does not eliminate the threat of passive eavesdropping. If an adversary hears commands during the authentication communication between the reader and tag, adversary could get the sensitive information.

In order to achieve a secure transaction, which should have confidentiality, authorization and authentication, we propose a symmetric encryption algorithm in our passive RFID tag design. A new data flow solution is suggested to prevent known plain text attack by using three random numbers to scramble the data. Also, identifying the trustful readers and authorizing the suitable rights for them are achieved in our scheme.

In this work, we design a complete baseband system which provides sufficient security level for the passive RFID tag. At the same time, the power consumption of the system is minimized. Also, our system is fully compatible with the EPC C1G2 standard [6]. The baseband system also serves as the central controller of the tag. It is responsible for encrypting and decrypting data, decoding PIE data, reading and writing to the OTP memory, adjusting the clock generator and controlling the state transitions. With a novel baseband system, all individual analogy units could utilize their potential to the best to constitute a high performance tag. All the subsystems in the complete baseband system are designed using low power techniques

The paper is organized as follows. Section II describes the specification of the RFID system. Section III discusses the overall architecture for the Baseband system and Section IV gives a discussion on the AES algorithm and presents our proposed encryption architecture. Section V describes the suggested data flow solution. Section VI presents the low-power design techniques used in the tag. Section VII shows the experimental results and Section VIII gives the concluding remarks.

II. RFID requirement

In each communication round, the reader transmits data embedded in a continuous wave in a frequency ranging from 860MHz to 960MHz. The received signal is extracted from the antenna and demodulated by the analog frontend. The baseband system then performs the decoding, CRC checking,

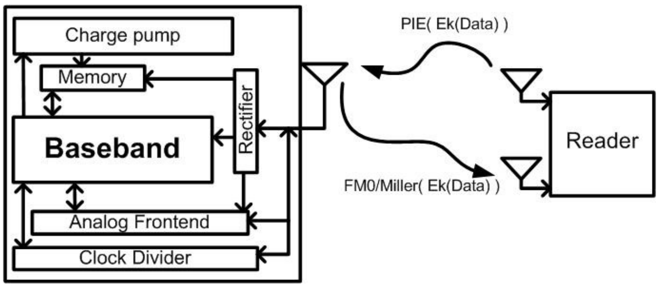

Fig.1. RFID system

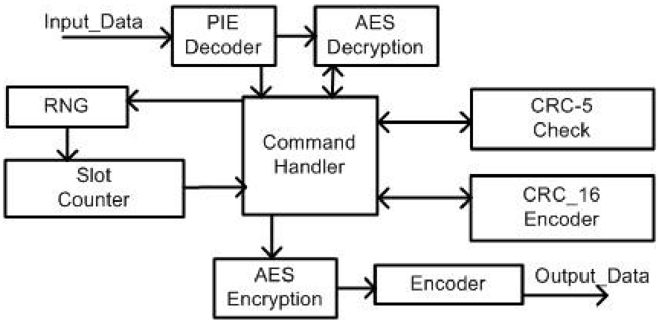

Fig.2. Architecture of the Tag

accessing the memory for receiving the command. It then executes the adjustment of the clock divider, encoding of the message and sends back the message to the reader. The details of a RFID tag system are shown in fig.1.

Apart from the compulsory operations required by the specification, our baseband system also performs an extra function to enhance the security level. In designing for a security transition, there are three constraints we have to consider. The first constraint is related to the insufficient size of the non-volatile memory. In our system, the memory is a one-time-programmable memory with 136 bits which restricts the size of key length to be stored in the tag. The second constraint is the computational power. Since the cost of a tag has to be very low, it can only afford to have a few thousand gates for the security engine. The third constraint is related to the system response time. There are minimum response time requirements for the tag to output random numbers and reply a message for successful writing operation. The overall response latency should be less than the timing requirement even with encryption and decryption operations.

There are many encryption standards available in the market, our strategy is to choose the most suitable one by finding the optimal tradeoff between cost and encryption performance. For high security strength, public key encryption, such as RSA and NTRU, are the best choice [7]. However, it is too expensive for RFID passive tag system to implement. Public Key algorithm requires at least a few hundred bits for the secret key and a few hundred thousand gates for computational processing [8]. There is an RFID active tag developed by Atmel which contains an NTRU public key encryption engine [9]. However, the cost is much higher than what we can afford for a passive tag.

Among all symmetric key standards, AES-128 is the most suitable one to be adopted in RFID system. AES is fast for both software and hardware implementation. It is relatively easy to be implemented with little memory usage. In addition, strong security strength can be provided by AES. Unlike most other block ciphers, AES has a very neat mathematical characteristic. The US government has announced that the design and strength of all key lengths of the AES algorithm are sufficient to protect classified information up to SECRET level in 2003 [10]. In [11], a low complexity implementation of the Sbox, which used only combination logic, was proposed. Based on this, the AES encryption and decryption engine can be implementation with lower gate count and smaller die-size.

III. Overall System Architecture

Figure 2 shows the block diagram of our baseband system. It, consists of 9 modules, and is driven by 3 different clocks, which are Clk_Dectect, Clk_Data and Clk_VCO. Clk_Detect is the fastest clock, used by the PIE Decoder. It is directly generated and divided from the carrier frequency. Clk_Data is used to drive most of the modules and is eight time slower than Clk_Detect. Clk_VCO is responsible for the data encoding. The AES decryption unit is used for data decryption and it could be bypassed in the normal mode if the system does not support encryption. The PIE decoder and Encoder interface with the analog frontend. The Command Handler controls the operation of charge pump which is used for accessing the OTP memory. It also controls the clock divider, the AES unit and OTP memory R/W. The random number generator RNG and Slot Counter are used for the anti-collision scheme. The encoder supports both FM0 and Miller encoding method.

IV. AES Algorithm and Architecture

In this work, we use 128 bits AES algorithm. Here the input key, the data input and the output length are all 128 bits. There are seven major operations in the encryption and decryption processes, which are SubBytes, ShiftRows, MixColumns, AddRoundKey, InvShiftRows, InvSubbytes and InvMixColumns [12]. Fig.3 and fig. 4 shows the process or AES encryption and decryption, respectively. For encryption, the loop will be executed for nine times, following by the last round which bypasses MixColumns or InvMixColumns transformation. For decryption, the process is just reversed. For both encryption and decryption, resource sharing could be achieved as the AES algorithm uses a round function that is composed of four different byte-oriented transformations.

Conventional AES cryptography engine has high complexity in order to maintain high throughput, but in RFID system, the throughput requirement is much lower. Also, the overall response time required by the RFID specification is much lower than other applications (less than 20ms in writing). Therefore a much slower AES engine can be used. Thus we focus on the reduction of the complexity when we design the AES architecture for RFID system. An 8-bit AES encryption and decryption architecture is adopted in our system. This proposed

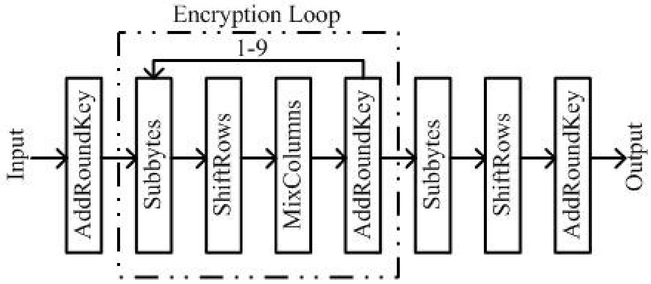

Fig.3. AES Encryption Algorithm

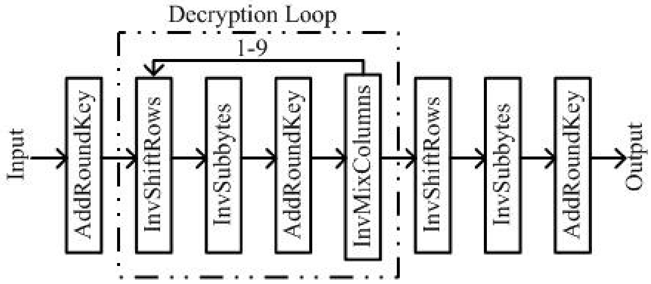

Fig.4. AES Decryption Algorithm

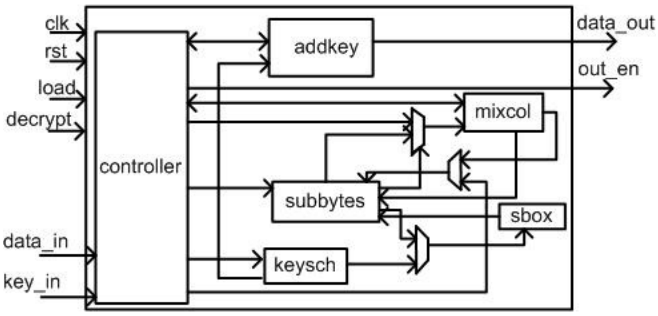

Fig.5. Proposed AES Architecture

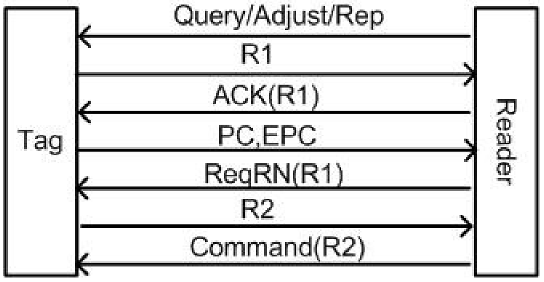

Fig. 6 Inventory and Access Process of a Tag

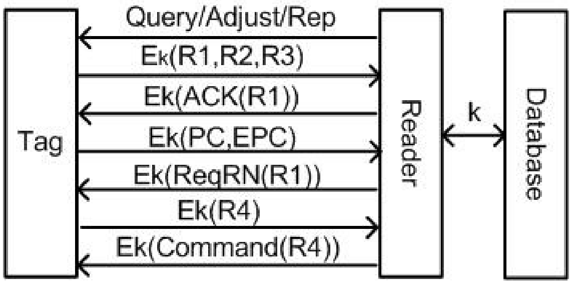

Fig. 7 Improved Encryption Data Flow

architecture is shown in fig.5. It consists of 6 modules, including an 8-bit Sbox, an addKey unit, a subbytes unit, a keysch unit, a mixcol unit and a controller. By executing the Sbox operation in the KeyExpansion and Subbytes operation in the same hardware, a single 8-bit Sbox is enough for the whole AES engine. The controller is responsible for activating the different modules in different rounds. The mixcol unit is responsible for mixing the data within each column of the state array. The keysch unit is used for generating the section key.

V. PROPOSED COMMUNICATION FLOW BETWEEN THE READER AND TAG TO ENHANCE SECURITY

The typical communication flow specified in the C1G2 standard [6] is shown in fig.6. The reader first sends out a Query command to start the communication. Once the tag receives a Query, it generates a random number R0 and start to count down from R0. Once the counter reaches zero, it replies to the reader with a 16 bits random number R1. Within a specified period, if the tag receives the acknowledgement with a matched R1, it will start to transmit the actual data, such as the PC and EPC. The reader will send back a ReqRN command after receiving the tag data. Finally, the tag will send back another 16 bits random number R2 for the usage of other commands. Under this flow, the tag can be accessed by any reader who follows this communication flow.

If we add security on the tag by using AES encryption, we need to modify the communication flow in order to enhance the security strength level. We assume that the secret key is securely delivered to the reader from the database before the communication starts between the reader and the tag. Every step in the communication flow is the same as that shown in figure 6 except that all commands are encrypted. However, this new communication flow suffers from a potential secure hazard, known as plain text (KPA) attack. For most of the mandatory commands, there are predefined headers in the commands. Adversaries can use this information to help in cracking the secret key.

We propose an improved communication flow scheme which makes use of the existing resource in the tag. Moreover, the existing communication flow does not need to be changed. Since AES-128 has a fixed input and output size of 128bits, the transmitted and received data have to be 128 bit long. In the existing RFID system, normally the length of the actual data communicated between the reader and the tag is less than 128 bits. We need to fill up the data with other data to form a 128 bit word for transmission. We can pack the word with all zero or all one at the tail of the data but this will significantly reduce the security strength because of KPA. In our scheme, instead of using constant zero or one, we use random number to fill up the transmitted word. Also to avoid KPA, during the send of the command from the reader to the tag, we randomly shift the location of the header of the command and also scramble the data with another random number. The random shift and the random numbers used for the scrambling are generated from the tag and are communicated to the reader in an encrypted form after receiving the Query command from the reader.

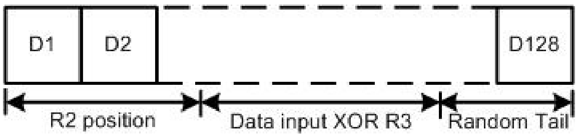

Fig. 8 Suggested Data Format

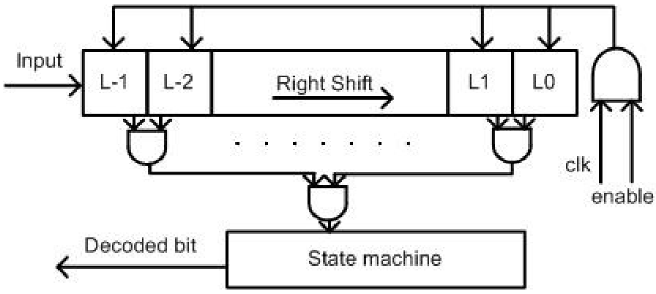

Fig.9. PIE decoder

Fig. 7 shows the proposed communication flow scheme. , All commands are encrypted even they do not contain any private information because we want to authorize the access rights to the trustful readers only. After the reader sends out a Query command to the tag, the tag generates a 128 bits random data and send back to the reader. In these 128 bits, the first 16 bits is used as the R1 similar to the original communication flow. The next second 7 bits determines the length of the random shifting used by the reader. The rest of the data is the third random number which is used to scramble the header and the data. When the reader receives this packet, it uses the information to generate the command packet of which the format is shown in fig. 8. By doing so, KPA is much harder. The data is first shifted according to the value of R2, and then XORed with R3. Random tail is added if necessary. By shifting the know plaintext with a random position and performing an XOR operation with another random number, there is no hint for adversaries to guess the text.

The implementation of this solution does not require additional hardware resource as the random number generator is already implemented and can be shared. Since the throughput of RNG is high enough to output a random number in a clock cycle, the extra latency of encryption caused by this scheme is less than 8 clock cycles. Since all commands are encrypted before transmission, confidentiality on sensitive information is achieved. Moreover, only the reader who has the secret key can decrypt the message. Thus authorization and authentication are ensured. Our system does not suffer from illegal tracing as the response for the first command Query is a 128 bits encrypted random number.

VI. Low Power Design Methodologies

Since the energy of a passive Tag is extracted from the continuous wave sent by the reader, it is a power limited device. To ensure the correct operation of the tag and to increase the range of operation, the power consumption of the tag has to be minimized.

There are two main components of power consumption in digital CMOS circuits, namely the static power and the dynamic power consumption [13]. Dynamic power dissipation is the result of the charging and discharging of the loading capacitances and short circuit power due to non-zero rise and fall time of input signals. Static power dissipation results from the leakage current when the logic gate is idle. To reduce the power consumption in RFID system, we need to consider both power consumption components

In our design, we focus on the following two directions to reduce the power consumption,, minimizing the switching activity and slowing the driving clock frequency as much as possible. The following are some approaches that we use in reducing the power consumption in our design.

A. *Optimizing the Driving Clock Frequency*

The data sent from a reader are in PIE format. There are two kinds of data, Data-0 or Data-1. The length of Data 0, Data 1, PW, Tari, Trcal and Rtcal are changed in each communication round by the reader, which means the tag needs to measure a varying length signal within certain accuracy. Tari is selected from the value of {6.25us, 12.5us, and 25us}. Either Preamble or Frame-Sync is transmitted before the payload. The reader can also require the tag response in a specified backscatter frequency LF. For different length of Trcal specified in the preamble, there are different percentages of allowable frequency tolerance which set constraints in the baseband decoder and clock divider.

The LF tolerance requires a relatively high sampling clock frequency to measure the Trcal, but the overall response time required by the specification is relatively long (less than 20ms in writing). It is possible to reduce the power consumption if we use two clocks instead of a single system clock. Our first scheme is to divide the clock frequency into Clk_Detect (measurement) and Clk_Data (controlling) so that most of the logic gates are driven by a slower clock.

The internal driving clocks are divided from the carrier wave which is in the range of 860MHz to 960MHz. This restricts the internal clock frequency options to be $f/2^N$. N should be chosen according to the Trcal measurement and PIE decoding performance.

To determine N, the ability of detecting the minimum PW, which is 2us, is essential. An effective Moving-Window Decoding algorithm is proposed to decode and measure the Trcal, and it is shown fig.9. There is no timing synchronization and channel estimation requirement in this algorithm and most importantly it is easy to implement in the hardware with accurate decoding results.

The moving window in the PIE decoder contains L shift registers, which store the received bit in each clock cycle. Once the sum of the L registers is less than a threshold L/2, a transition from high to low is detected. When the sum of the L registers is larger than the threshold, a transittion from low to high is detected. By counting the number of clock cycles in between, the length of a signal can be measured. We simulated the decoding performance with different Signal-to-Noise ration value and the results are shown in fig.10. Here L equals to 7 and N equals to 7 also. From fig. 10, we can see that the

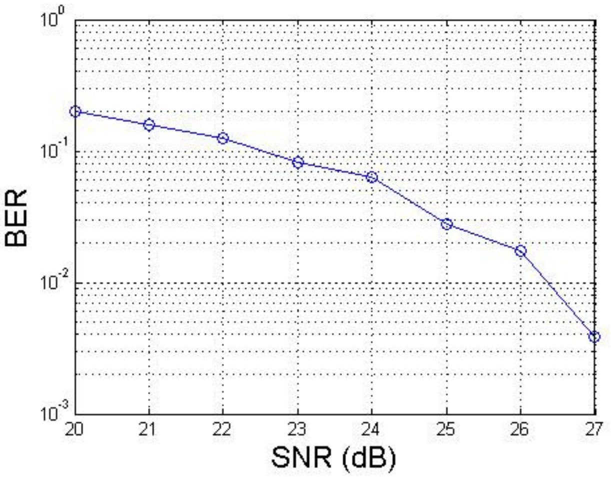

Fig.10. Simulation result of PIE decoding

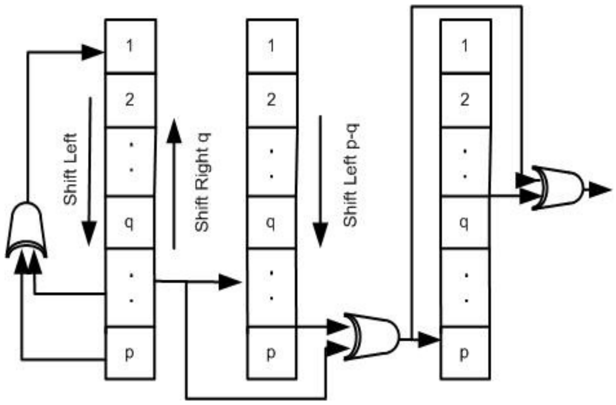

Fig.11. Improved Tausworthe sequence generator

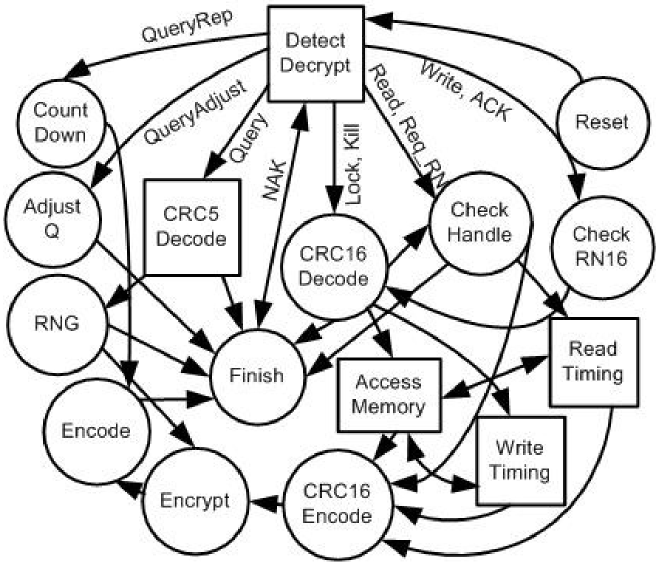

Fig.12. State transition diagram of the baseband system

BER is less than 10^{-2}. The corresponding Clk_Detect is in the range of 3.35M to 3.75M.

Once Clk_Detect is fixed, we then choose Clk_Data with the slowest allowable frequency. For a fixed response time requirement, we can reduce the clock frequency if we can reduce the number of clock cycle required to complete the computation. In our tag design, the frequency of Clk_Data is reduced to 8 times slower than Clk_Detect by applying advanced techniques to reduce the number of clock cycle required in each module. As most of the logic gates are driven by Clk_Data, the dynamic power consumption is reduced significantly.

In the anti-collision scheme and our proposed communication flow solution, a random number generator is required. An uniformly distributed random number is used to determine the waiting time of a tag before responding to the reader. Conventional design normally employs the Tausworthe sequence generator, which uses feedback shift register for generating uniformly random numbers. Although it is easy to implement in circuit and has good randomness property, it takes K clock cycles to generate a K-bit random number. This latency is critical when we need to use the AES encryption operation. It is one of the bottlenecks in reducing the latency.

A new method is employed by using an improved Tausworthe sequence generator proposed by [13]. By adding two level XOR elements to form a concurrent network, a P-bit random number is generated during each shift operation, which is shown in fig.11. Therefore, the throughput of this design is about P time faster than the traditional Tausworthe sequence generator. In our system, 31 bits seed is long enough to meet the randomness requirement and generate 16 bits uniformly distributed random number. By doing this, the clock cycle requirement of RNG is reduced and a slower clock can then be used.

Another approach to reduce the latency is to use parallel processing technique. Fig. 12 shows the state transition of the system. Every state with a rectangular shape means that more than one module is activated in this state. In the state Detect/Decrypt, instead of receiving PIE decoded bit and keeping other modules idle, the bit is fetched into the CRC 5 decoder and AES decryption engine at the same time. By doing this the latency of CRC decoding would be reduced. In the state “Write Timing” and “Read Timing”, the CRC encoder is also activated. Once the data is extracted from the memory bit by bit, it would also be sent to the CRC encoder at the same time. By doing so, the latency of CRC encode and decode would be reduced.

B. *Reducing switching event*

Extensive clock-gating is used to reduce the switching activity of the idling modules. For example, the RNG should be activated only when the command Query is received and decoded. Also, the reader should not send another command while the previous one has not yet been finished. Therefore, PIE decoder should remain idle when the handler is executing the received command.

Another scheme is to have a power efficient accessing method for the memory. Fig. 12 shows the memory access scheme. In Write operation, data is sent to the memory bit by bit. Since the memory is one time programmable, each bit value could only be modified once. Whenever there are more than one write operations at the same memory location, the tag should send out an error message. Our scheme is to eliminate

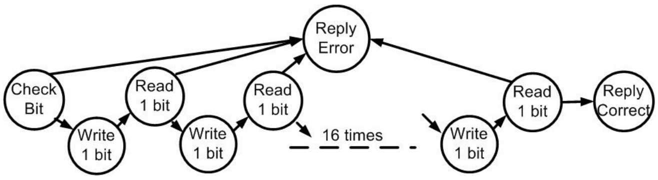

Fig.13. Memory access scheme in write command

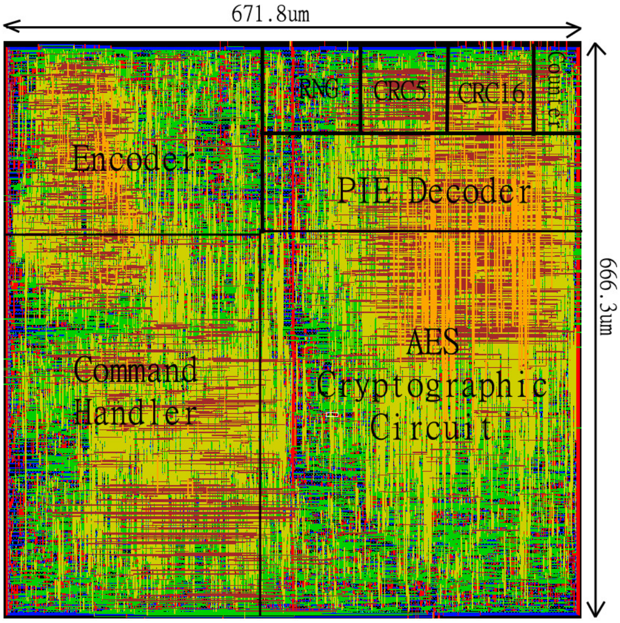

Fig. 14 Floor plan for the baseband system

the continuous writing into the memory when an error is detected because writing into memory consumes a huge amount of power. For each group of two bytes in the memory, one extra bit is used to indicate whether this group has been written or not. Whenever there is a write operation, the first operation is to check this bit. If it is zero, the write operation could continue. In between any two bits writing, a Read operation is performed. This accessing scheme can guarantee that the tag responds to an error message in the fastest way. Moreover, the number of time of switching the address is minimized as it is writing and reading at the same address bit by bit.

VII. Experimental Results

We have designed the whole baseband system in TSMC 0.18μm CMOS process. The design is modeled in Verilog and synthesized using Synopsys Design Compiler. The supply voltage is 1.8V and clock frequency of Clk_Detect is set at 3.55MHz. The layout of the baseband system is shown in fig. 14. The largest module is the AES cryptographic circuit, followed by the Command handler, the Encoder and the PIE decoder, the overall area of the chip is 671.8um x 666.3 um. We used Power Compiler to simulate the power consumption of the design. The total power consumption is equal to 4.7uW.

VIII. Conclusion

In this paper, the design of a complete baseband system for RFID Passive Tag is presented. AES engine is included in the design to ensure secure communication. Our security goals, confidentiality, authorization and authentication are achieved by using a new communication flow. In order to reduce the power consumption, advanced low power design schemes are adopted in this system. Simulation results verify that the design is fully compatible with EPC C1G2 standard and demonstrate that low power consumption can be achieved.

References

[1] K.Finkenzeller: *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*, 2nd Ed, Wiley, 2003

[2] RFID Journal, "The EPC tag and reader maker has dropped the price of its Class 1 label to less than 20 cents each for orders of 1 million", April 1, 2004.
http:/ /www.rfidjournal.com/article/articleview/857/1/1

[3] A. Juels, "RFID Security and Privacy: A Research Survey", *IEEE Journal on Selected Areas in Communications,* Vol. 24, pp.381 – 394, February 2006

[4] R. Rieback, B. Crispo, S.Tanenbaum, "The Evaluation of RFID Security", *IEEE Pervasive Computing*, Vol. 5, pp. 62 – 69, March 2006.

[5] D. Henrici, P. Muller, "Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers," in *Pervasive Computing and Communication Workshops*, 2004 pp. 149-153.

[6] EPCglobal IncTM, EPCTM Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860MHz -960MHz Version 1.0.9 , January 2005.

[7] RSA Laboratories Technical Staff, *RSA Hardware Implementation*, RSA Laboratories, 1996.
http://www.rsasecurity.com/rsalabs/

[8] Nibouche, O.; Belatreche, A.; Nibouche, M, "Speed and area trade-offs for FPGA-based implementation of RSA architectures," in *NEWCAS*, 2004, pp.217 – 220.

[9] Available at: http://www.ntru.com/

[10] *National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information*, CNSS Policy No. 15, Fact Sheet No. 1, Jun 2003.
http://www.cnss.gov/Assets/pdf/cnssp_15_fs.pdf

[11] J. Wolkerstorfer, E. Oswald, M. Lamberger, "An ASIC Implementation of the AES SBox," in *CT-RSA 2002*, vol. 2271 of *Lecture Notes in Computer Science*, pp. 67-78. Springer, 2002

[12] Federal Information, Processing Standards Publication 197, "Advanced Encryption Standard", November 2001.
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[13] M. Rabaey, M. Pedram, *Low Power Design Methodologies*, 1st Ed. Kluwer Academic Publishers, 1996.

[14] Wei Cui; He Chen; Yueqiu Han, "VLSI Implementation of Universal Random number generator," in *APCCAS*, 2002, pp. 465-470.