Field Programmable gate array based Radio Frequency identification with Cryptography-Review

Neelappa

Department of E & C

Govt. Engineering College Kushlangar, Karnataka,India -571234

Email:neel.m.dy@gmail.com

Abstract: In this paper review on RFID system and cryptography is carried out. Many authors have proposed architectures for passive tag and reader and reported the performance. Aauthors have also proposed architectures for ECC processor and algorithm for scalar multiplication at different bit size and different frequency to optimize parameters. Various proposals have been suggested by researchers for the design of low-power/energy ECC processors. The objective seen in many of these publications is reaching lower power consumption. The focus of the researchers is on minimizing calculation time and simultaneously getting their implementations relevant for applications of a wide range like RFID and WSNs.

Key words: FPGA, ECC,EEPROM,HF,UHF,LF,WSNs

1. Introduction

RFID ipso facto deals with identification of objects through radio waves. It's use started during World War II in the identification of "Friend-or-Foe" for targets used by the military, such as aircraft and forces. It was only in 1990s, that large scale use of RFID started. Areas of use were supply management, for tracking articles, inventory and also for identification of animals. The role of identifier is to serve a tag in RFID. It contains an UID of the object to which it is tagged. Transmission of the ID is done to a reader through wireless medium[1].

The technology is considered as an improvement over barcodes apart from increased storage capacity and reprogramming capability. There is no need for RFID to be in line-of-sight for the purpose of identification. Technology is able to ensure automatic and wireless identification of objects without the need of any physical contact. Small size of tags makes for convenience in their embedding into consumer items, credit cards, with the possibility of implanting them into humans and animals. A significant difference between barcodes and RFID is that the latter have the EPC which has the additional feature of identification of the item that is known for universal uniqueness.

Speedy identification of objects was the purpose of designing RFID. The technology does not have the provision for validating the parties of a communication. viz., tags and readers. An important feature of the tags is their ability to reveal their indenties to readers who have queries. Eavesdroppers are able to intercept messages. This is a corollary of the feature of the openbroad cast of wireless communication. However, there is the problem of the confidentiality of communication being lost, there by getting

exposed to serious security and privacy attacks resulting in unauthorized access to resources and collection of the confidential information relating to the object.

Security and privacy issues explain why barcodes still remain without getting eased out by RFID. There is also another fact to contend with additional cost which is more than for barcodes.

There are limitations in the area of technical capabilities. Current research in RFID authentication works on the objective of low power, low cost EPC tags which can be embedded into consumer items. This has to be offset against the limited capabilities of tags [2].

The focus of attention during the last few years has been to ensure security and privacy issues to increase the opportunities in the area of consumer applications. Research work is focused towards finding a secure way of identification that would protect the privacy of users and is robust against unauthorized usage.

1.1 Overview of RFID system

Reader, tag and a back-end database are the main components of an RFID system. Back-end database is used to store data related with tag contents. This is shown in Figure 1.1. The reader is connected to a workstation via network. RFID tags have UID. The RFID reader reads the UID of the tag. An RFID reader can read a number of tags [3].

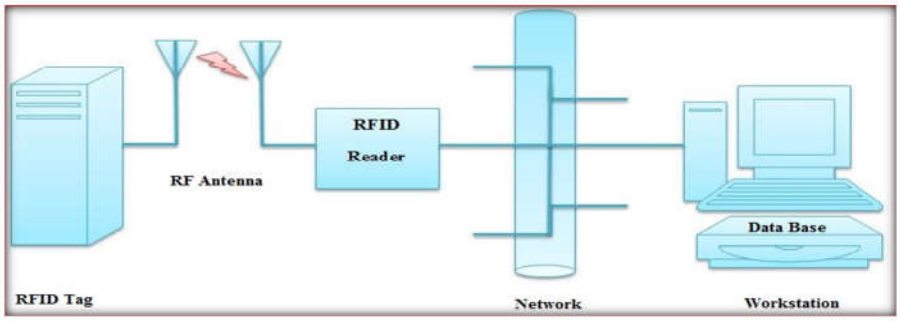

Figure 1.1 RFID system

RFID tag contains an antenna, analog front end, base band-processor and EEPROM (Figure 1.2). The base-band processor is an important part of the tag, performing read/write operation of EEPROM. It is difficult to reduce power consumption of analog front end and EEPROM. Therefore, it is important to design a low power base-band processor. RFID module can be programmed for the manufacturing. The volume of data to be stored depends on the chip and ascertaining an UID programmed during chip production [4].

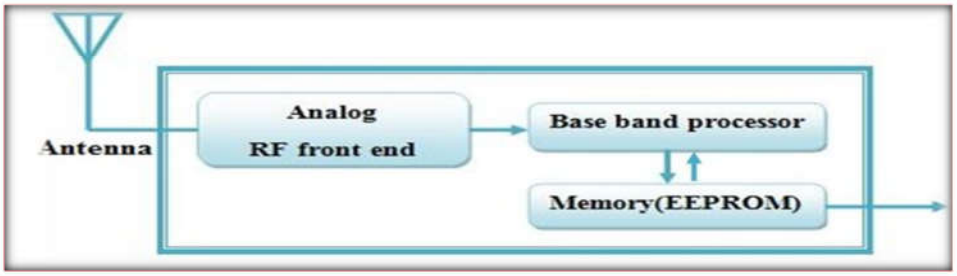

Figure 1.2 RFID tag blocks

The RFID reader consists of a base-band processor, antenna, interface module and analog front end (Figure 1.3). The antenna is connected with the analog front end and tuned to detecting a tag that gets close to the reader field. Detection and decoding of the data read from the tag by the front end are done by the base-band processor. The data is later sent to the interface. The interface connector could be USB, SPI etc. Interfacing with the user is possible through the use of LED and beeper for indicating the status of the tag read [5].

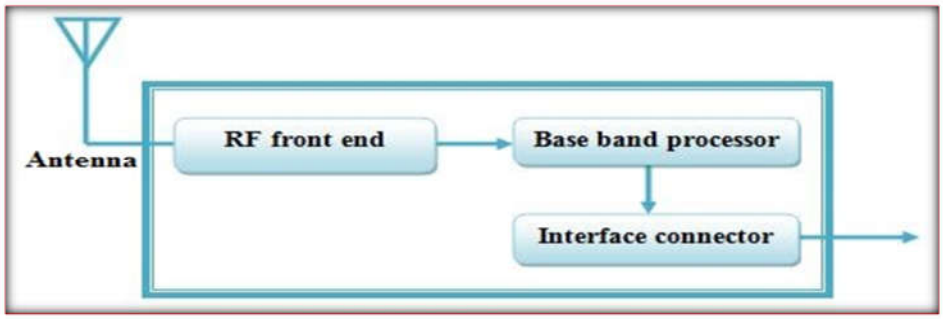

Figure 1.3 RFID reader blocks

It is possible for readers to use tag contents as a lookup key into a database. The database is associated with product information and key management information with a specific tag. It is possible for anyone to build independent databases with access to tag contents.

1.2 RFID tags

RFID tags are electronic devices of smaller size consisting of a memory connected to an integrated antenna. The memory has the ability to provide storage and computatinal capabilities. The antenna provides communication with the reader. Tags can be categorized into active, semi-passive and passive depending on the power source. Passive tags use energy from the reader to generating a response. An internal battery supplies energy to active tags. A small battery on board is attached to semi-passive tags. But their response is possible only to a request from the reader[1][2]. The source of power is a significant feature of a tag considering the fact it decides the possible reading range, lifetime, cost and functionalities of the tag.

Active tags are alone can initiate communication with the reader. They can constantly beacon their ID's. Active tags of highly advanced type have the ability to communicate with other active tags forming ad hoc networks. Active tags have power source of their own. Hence, they can operate over long distances. They also have

better computational capability compared to other types of tags. This has, however, to be viewed against the limited life-time of the battery that shows rapid draining as a result of constant beaconing. Active tags find use in localization of cattle over long distances, live tracking of high value assets etc. These have reasonably bigger size. They are more expensive than tags of other types.

Semi-passive tags too have a power source on board. But, they have no communication with the reader. They indulge in generation of a respone only in the event of introgation from the reader. They conserve and retain power and ensure better longevity**.** They provide good computational and storage characteristics. Provision of power source makes semi-passive tags more expenive and larger in size compared to passive tags. They often are used for sensing functionality.

Passive tags are known to be inexpensive. They are also the most common type of RFID tags. They have no power source of their own. They gather energy from the electromagnetic signals from the reader. This necessitates the location of the reader in the close proximity and results in a short range operation. The advantage of being powered by the external sources provides the facility of the information being stored longer in their memory, giving rise to an almost unlimited life time.

There is also another advantage arising from the absence of a battery. It is the flexibility in the design of the tags, enabling the application of convenient form factors for incorporation into items, from RFID chips known for the rice grain size implemented into pets. RFID labels, that are thin, neat and flexible can be incorporated into packing materials and paper. Passive tags functionalities have their own limlitation in the area of storage of an ID number and arithmetic operations.

Passive tags have a large variety of applications. This is naturally so considering their low cost and lower maintenance requirements. The applications include wireless payments, electronic documents, animal identification, theft detection etc. A comparison of the summary of RFID tags is provided in Table 1.1.

Table 1.1 Summary of RFID tags

Tag Type	**Communication Mode**	**Storage capabilities**	**Power source**	**Operating Range (meters)**	**life duration**	**Costs**
Passive	Response only	Simple	Getting energy from reader	10	Unlimited	Cheapest
Semi-active	Response only	More advanced	On board Battery	>100	Less	More expensive
Active	Response or Initiate (Beaconing	Most advanced	On board battery	>100	Least	Most expensive

	)					

Over and above the different type of power source, there is fact of RFID systems operating in different regions of radio spectrum considered for communication between readers and tags. Performance is defined in terms of signal strength and tolerance to obstacles of varying nature, the size of the tag, and the applications areas.

The Table 1.2 summarizes classes of radio bands and their application areas by different wavebands used in RFID systems:

Table 1.2 Summary of classes of radio bands and applications areas

Classes Radio bands	**Frequency range**	**Application**	**Bandwidth**	**Distance**
UWB	3–30 GHz	Vehicle Identification	< 200 kb/s	ca. 15 m
UHF	300MHz–3 GHz	Range Counting	< 200 kb/s	3–12 m
HF	3–30 MHz	Access Control	< 100 kb/s	0.05–1 m
MF	300kHz– 3 MHz	Contactless Payments	< 50 kb/s	0.2–0.8 m
LF	30–300 kHz	Animal Identification	< 10 kb/s	0.1–0.2 m

1.3 RFID readers

RFID readers provide wireless connection with RFID tags, query and identify them too. Points of interaction between tags and the RFID system do exist. They are involved in the collection and analysis of data that readers are known to collect. Identification procedure is defined with the help of protocol used in a specific RFID environment. It may be a multi-round or a simple request-reply exchange protocol. Depending on the protocol, tags can transfer tasks to readers which are computationally complex and require more power. RFID readers could be either mobile or stationary. The mobile readers are generally in the form of hand held devices. At the entrance of the supermarkets or warehouses stationary readers are usually located.

Several tags are located close to the reader known for simultaneous response on the same frequency, thereby causing collision in communication. In environments where multiple tags have simultaneous presence, RFID readers use anti-collision protocols of exclusive variety [06] [07][08][09][10].

A reader's request for data from the tag initiates the communication in RFID. Such a communication link goes by nomenclature of a forward channel. The transmission of the request is sent on the frequency which is defined by the standard format. The tag, on receipt of reader's request, forwards its ID in the format conforming to the definition provided by the authentication protocol. Dissemination of response from the tag to the reader is done over the backward channel. The reader processes the reply from the tag and extracts the ID of the tag. It is followed by a check in the database with the set of valid ID's. A decision on this made on the basis of the tag being authorized. Figure. 1.4.illustrates this communication process.

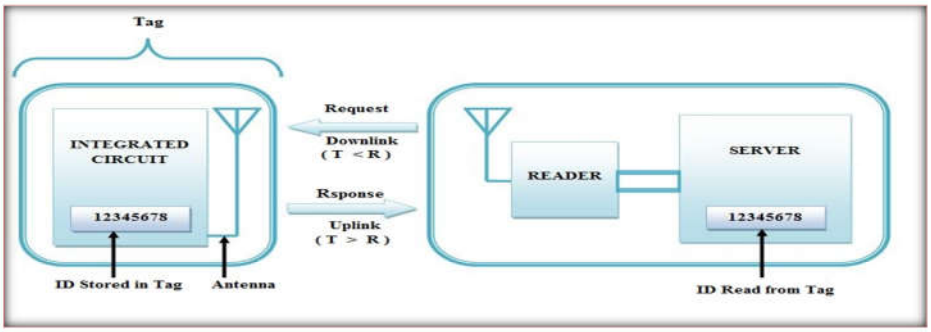

Figure 1.4 Communication process in RFID system

1. 4 Antenna

In RFID system antennas are indispensable elements. They are passive devices that make use of power available with the reader for generating a field meant for the forwarding and receipt of signals from the RFID tags. Antennas have variations in size, gain, rating, polarization and connector type. Selecting the right antenna for the specific RFID application is crucial.

2. Cryptography

Cryptography is used for ensuring the security in information. Cryptographic encryption algorithms are classified under two heads, namely, symmetric key and asymmetric key. In the case of the former, a key is communicated by the dispatcher and the beneficiary. The latter employs a solitary key for encryption and another for decryption respectively.

The feasibility of public-key (PK) solutions for RFID's has been stated in the subject matter for research. This arises from limitations in areas of cost, area and power. RFID have the requirement of security solutions. Implementation of PKC faces some problems in these environments considering the deployment of computationally demanding operations. Passive RFID tags are well known for implementations of reports. ECC has used for been implementations for RFID tags.

ECC is a public key cryptography method. It is an important feature of the data security system. The algebraic structure of elliptic curve over finite fields forms its basis and offering security analogous to RSA algorithm. ECC is implemented under extreme resource constraints. Algorithm for ECC and architecture at RTL level in affine and projective coordinates have been proposed for mitigating hardware complexity and reducing power consumption.

In this paper section 1 describes introduction, in section 2 cryptography is explained literature review is explained in section 3. In section 4 conclusion is presented.

3. Literature Survey

In the literature survey, techniques and different architectures for implementing low power DBBP passive tag, digital base-band processor RFID reader and ECC are explored. In particular, the subjects of low power techniques, encryption algorithms, dedicated elliptic curve processors**,** versatile and general scalar multipliers are been given special attention. The summary of the literature review is presented in the Tables 3.1 and 3.2.

Table 3.1 Literature Survey summary Without ECC

Ref. No.	Technology	Frequency	Power	Area
[18]	-	-	6.7mW @ 1.2 V	-
[19]	UMC 0.18 µm CMOS	83 MHz	-	4 mm^2
[22]	0.18 µm CMOS	2.56 MHz	6.4 µW	0.3mm^2 @ 1 V
[23]	0.18 µm 6 layer CMOS	3.55 MHz	3.436 µW	892µm x 260µm
[24]	0.18 µm CMOS	2.56 MHz	1.25 µW	300 µm x 300µm @ 1 V
[25]	0.35 µm CMOS	2.56MHZ	7.5 µW	800 µm x 800µm @ 0.96V
[26]	0.35 µm 1p4M CMOS	-	8.9 µW @ 2V	-
[28]	0.18 µm CMOS	1.92 MHz	2.7 µW @ 1 V	0.11 mm^2

Table 3.2 Literature Survey summary With ECC

Ref No.	Technology	Frequency	Field size	Power	Gate Area	# Clock Cycles	Energy	Time*
[30]	TSMC 0.18µm CMOS	1.28 MHz	226	6.607 µW	16.9K	36,174	NA	-
[31]	UMC 0.18 µm CMOS	13.56MHz	-	14.7µW @423KHz 208.4µW @13.56 MHz	25.7K	NA	NA	12.52ms

[32]	0.13µm CMOS	500 KHz		Gate area-30.76K		NA	NA	7.35ms
[28]	0.35µm CMOS	1.92 MHz		2.9µA @1.2 V	NA	NA	NA	
Ref. No	**Technology**	**Frequency**	**Field size**	**Power**	**Gate Area**	**Clock Cycles**	**Energy**	**Time***
[33]	TSMC 65 nm CMOS	1130 KHz	NA	NA	12,102	52,012	NA	46 ms
[38]	UMC 0.13 µm CMOS	13.56MHz	168	23.1µW @1MHz	NA	NA	NA	0.72 s
			192	26.3µW @1 MHz				1.15 s
[40]	UMC0.13 µm CMOS	13.56MHz		253 µW	NA	13.7K	3.31µJ	13.1 ms
[41]	ASIC 120nm CMOS	312 MHz	256	NA	1.29 mm^2			0.85 ms
[43]	0.13µm CMOS	1130 KHz	NA	36.63 µW	12.5 K	275,816	8.94µJ	244 ms
[44]		45.87MHz	131	NA	5945*	NA	NA	11.3 ms
		43.38MHz	163		6913*			14.9 ms
[45]	0.13µm CMOS	1 MHz	168	NA	NA	NA	12.9µJ	0.4 s
[48]	FPGA (Vertex-4)	251 MHz	163	Area Slices-19604 LUTs -36727		2993	Time -11.92µS	
[49]		100KHz	192	18.85 µW	23.6K	NA	NA	
[51]		274 MHz	128	Area-1552 Slices		65000	0.24ms	
[52]	FPGA (Vertex-4)	131 MHz	163	LUTs-14507 Slices-8095		Latency -1429	10.70 µS	
	FPGA (Verte	147 MHz	163	LUTs-8095 Slices-3513		Latency -1429	9.70 µS	

	x-5)					
[53]	FPGA (Vertex-4)	154 MHz	55	Flip flops-7962 LUTs-26364 Slices-16209	Latency -3010	19.5 µS
[54]	FPGA (Vertex-5)	250 MHz	81 bit digit serial	LUTs-22936 Slices-6150	Latency -1371	5.48 µS
[55]	FPGA (Vertex-4)	185 MHz	82	Slices-20807	Latency -1428	7.72 µS
[56]		143 MHz	3G NB	Slices-24363	Latency -1446	10 µS
[57]		167 MHz	163	LUTs-10176 Slices-3446	Latency -1429	8.60 µS
	FPGA (Vertex-5)	147 MHz	163	LUTs-14265 Slices-8070	Latency -1429	9.70 µS
[58]	FPGA (Vertex-4)	121 MHz	163	Slices-10417	Latency -1091	9.0 µS
[59]		133 MHz	163	Slices-27889	Latency -2128	16 µS
[60]		290 MHz		Flip flops-1870, LUTs-6672, Slices-3536	Latency -4168	14.39 µS
[61]		210 MHz	163	Flip flops-3077 LUTs-23468 Slices-12964	Latency -1119	5.32 µS

*** For one Scalar multiplication**

4. Conclusion

From the literature survey it can be concluded that the majority of the authors have proposed architectures RFID system and presented the performance. Through performance comparison between tag with ECC and without ECC it can be concluded that most of the authors have proposed architectures for ECC processor and algorithm for scalar multiplication at different bit size and different frequency to optimize parameters. The objective seen in many of these proposals is reaching lower power consumption.

References

[1] Roman Zharinov, UliaTrifonova and Alexey Gorin, "Using RFID Techniques for a Universal Identification Device", Proceeding of the 13th Conference of Fruct Association.

[2] A. Juels and S. Weis, "Authenticating Pervasive Devices with Human Protocols,"in *Advances in Cryptology – CRYPTO 2005 SE – 18*, ser. Lecture Notes in Computer Science, V. Shoup, Ed. Springer Berlin Heidelberg, 2005,vol. 3621, pp. 293–308.

[3] P. Suresh and R.Kesavan, "Design of Dynamic RFID System using 89C51 Microcontroller based Embedded System for Effective Supply Chain Management", International Conference on Industrial Engineering and Operations Management Kuala Lumpur, Malaysia, January2011, pp. 22–24.

[4] Klaus Finkenzeller, "RFID Handbook: Fundamentals and Applications in contactless Smart Cards and Identification", Second Edition John Wiley and Sons, Ltd.

[5] NSK electronics RFID reader 125 KHz datasheet web - http://www.nskelectronics.in/files/rfid_edk_kit.pdf.

[6] N. Abramson, "The Aloha System: another alternative for computer communications", Proceedings of the November 17-19, fall joint computer conference. ACM, 1970, pp. 281–285.

[7] L. G. Roberts, "ALOHA packet system with and without slots and capture", ACM SIGCOMM Computer Communication Review, Vol. 5, No. 2,1975, pp. 28–42.

[8] J. Myung, W. Lee, and J. Srivastava, "Adaptive binary splitting for efficient RFID tag anti-collision", IEEE Communications Letters, Vol. 10, No. 3,2006, pp. 144–146.

[9] J. R. Cha and J. H. Kim, "Novel anti-collision algorithms for fast object identification in RFID system," in Parallel and Distributed Systems, 2005.Proceedings.11th International Conference on, IEEE, vol. 2.,2005, pp. 63–67.

[10] D. H. Shih, P. L. Sun, D. C. Yen and S. M. Huang, "Taxonomy and survey of RFID anti-collision protocols, Computer communications", Vol. 29, No. 11, 2006, pp. 2150–2166.

[11] F. Armknecht, M. Hamann and V. Mikhalev, "Lightweight Authentication Protocols on Ultra-Constrained RFIDs-Myths and Facts, in Radio Frequency Identification: Security and Privacy Issues". Springer, 2014, pp. 1–18.

[12] C. A. Repec, Regulatory status for using RFID in the EPC Gen 2 band (860 to 960 MHz) of the UHF spectrum, 2014. [Online].http://www.gs1.org/docs/epc/UHF_Regulations.pdf.

[13] K. Finkenzeller and D. Müller, "Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field communication", Wiley, 2010.

[14] D.M. Dobkin, “The RF in RFID: passive UHF RFID in practice”, Newnes, 2007.

[15] EPC Global. EPC Class 1 Generation 2 UHF Air Interface Protocol Standard "Gen 2", 2008.

[16] Xin Li and Chunhua Wang, “Design and FPGA verification of UHF RFID reader digital baseband”, 2011 International conference on electrical and control engineering, Sept. 2011, pp.2100–2103.

[17] LiyanXu, Lingling Sun and Xiaoping Hu, “Design and realization of a UHF RFID interrogator”, International Journal on Smart Sensing and Intelligent Systems, Vol. 6,Jun. 2013, pp.1012-1031.

[18] Jing Liu, Yihao Chen, Bin Gu, Runxi Zhang, Feng Ran and Zong sheng Lai, “ASIC design of UHF RFID digital baseband”, Asia pacific conference on postgraduate research on micrco electronics and electronics, Sept. 2010, pp. 263–266.

[19] Shuang Zhao,Wengeing Lu, Chao Lu, Xiaofang Zhou and Dian Zhou, “An Efficient Multi-protocol RFID Interrogator Baseband Processor based on a Reconfigurable Architecture”, International conference on embedded software and systems,2008**,** pp.264-270.

[20] Chang Seok Yoon, Sung Ho Cho and Ki Yong Jeon, “A design of UHF-band RFID reader using FPGA”, 2014.

[21] Pradeep Basappa Khannur, Xuesong Chen, Dan Li Yan, Danshen and Bin Zhao, “A Universal UHF RFID Reader IC in 0.18-µm CMOS Technology”, IEEE journal of solid state circuits, Vol.43, May 2008, pp.1146–1155.

[22] Vahid Roostaie,ValiNajafi, Siamak Mohammadi and Ali Folowat-Ahmady, “A Low Power Baseband Processor for a Dual Mode UHF EPC Gen 2 RFID Tag”, 3rd International Conference on Design and Technology of Integrated Systems in Nano scale Era,2008, pp.1-5.

[23] Adam S.W.Man, Edward S.Zhang, H.T.Chan,Vincent K.N. Lau,C.Y.Tsui and Howard C.Luong, Design and Implementation of low power baseband system for RFID tag, IEEE transactions, 2007.

[24] Tian Jiayin, He Yan and Min Hao, A Novel baseband processor for LF RFID tag, IEEE transactions, 2007.

[25] ShenJinpeng, Wang Xinan,Liu Shan Zong Hongqiang, Huang Jinfeng, YangXin, Feng Xiaoxing and GeBinjie, Design and implementation of an ultra-low power passive UHF RFID tag, Journal of Semi-conductor, Chinese institute of electronics, Vol. 33, No.11, 2012.

[26] Guohua Chen, Linan Li, Hongwei Shen and Yumei Zhou, Design of a Low-Power digital core for passive UHF RFID sensor, IEEE transactions, 2007.

[27] Ismarani Ismail and Azlina Ibrahim, Modelling and Simulation of Base band Processor for UHF RFID Reader on FPGA, International journal of electrical and electronic systems research, Vol.6, 2013.

[28]Dingguo Wei, Chun Zhang, Yan Cui, Hong Chen and Zhihua Wang, Design of a Low-cost Low-power Baseband-processor for UHF RFID Tag with Asynchronous Design Technique, Institute of Microelectronics, Tsinghua University, Beijing, 100084, PR. China, 2010.

[29] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede,

Public-Key cryptography for RFID Tags, 2006.

[30] PengLuo, Xinan Wang, Jun Feng and Ying Xu, Low-Power Hardware Implementation of ECC processor suitable for Low cost RFID Tags, The key labs of Integrated Micro system, Shemhen Graduate school of Poking university,China,2008.

[31] Dongsheng Liu, Zilong Liu, Zhenqiang Yong,XuechengZou, and Jian Cheng, Design and Implementation of An ECC-Based Digital Baseband Controller for RFID Tag Chip, IEEE transactions on industrial electronics, Vol. 62, No. 7, July 2015.

[32] Lili Wei, ZhaotongLuo, QiangQu, Qing He and JingweiXu, A Low-cost PKC-based RFID Authentication Protocol and Its Implementation, Tenth International Conference on Computational Intelligence and Security, 2014.

[33] Jose A. Rodriguez-Rodriguez, Manuel Delgado-Restituto and Angel

Rodriguez- Vazquez, Baseband-Processor for a Passive UHF RFID Transponder, 2010.

[34] Tuy Tan Nguyen and Hanho Lee, Efficient Algorithm and Architecture for Elliptic Curve Cryptographic Processor, Journal of semiconductor technology and science, Vol. 16, No. 1, February 2016, pp. 1598-1657.

[35] Gustavo D. Sutter, Jean-Pierre Deschamps and José Luis Imaña, Efficient Elliptic Curve Point Multiplication Using Digit-Serial Binary Field Operations, IEEE transactions on industrial electronics, Vol. 60, No. 1, January 2013.

[36] Hsin-Yu Ting and Chih-Tsun Huang, Design of Low-Cost Elliptic Curve Cryptographic Engines for Ubiquitous Security, National Tsing Hua University, Taiwan, 2014.

[37] Yiran Lin,Kaige Kang,Yue Shi, Research on Encryption Model Based on AES andECC in RFID, International Conference on Computer Sciences and Applications, 2013.

[38] Bijan Ansari and M. Anwar Hasan, High-Performance Architecture of Elliptic Curve Scalar Multiplication, IEEE transactions on computers, Vol. 57, No. 11, November 2008.

[39] Hamid Reza Ahmadi and Ali Afzali-Kusha, Very Low-Power Flexible GF (p) Elliptic-Curve Crypto-Processor for Non-Time-Critical Applications, School of Electrical and Computer Engineering, University of Tehran, Iran, 2009.

[40] Zilong Liu, Dongsheng Liu, XuechengZou, Hui Lin and Jian Cheng, Design of an Elliptic Curve Cryptography Processor for RFID Tag Chips, Sensors, 2014.

[41] Z. Guitouni, R.Chotin-Avot, M. Machhout, H. Mehrez and R. Tourki, High Performances ASIC based Elliptic Curve Cryptographic Processor over GF(2^m),IJCA Special Issue on Network Security and Cryptography, 2011.

[42] Sunil Devidas Bobade and Vijay R. Mankar, Area Efficient Implementation of Elliptic Curve Point Multiplication Algorithm, International Journal of Advanced Computer Science and Applications, Vol. 6, No. 4, 2015.

[43] Yong Ki Lee, Kazuo Sakiyama, Lejla Batina and Ingrid Verbauwhede, Elliptic-

Curve- Based Security Processor for RFID, IEEE transactions on computers, Vol. 57, No. 11, November 2008.

[44] M. B. I. Reaz, J. Jalil, H. Husain and F. H. Hashim, FPGA Implementation of Elliptic Curve Cryptography Engine for Personal Communication Systems,WSEAS TRANSACTIONS on circuits and systems, Issue 3, Vol. 11, March 2012.

[45] Hamid Reza Ahmadi and Ali Afzali-Kusha, Low-Power Low-Energy Prime-Field ECC Processor Based on Montgomery Modular Inverse Algorithm, 12th Euromicro Conference on Digital System Design, Architectures, Methods and Tools, 2009.

[46] Jing Guo, Liyi Xiao, Zhigang Mao and Qiang Zhao,Enhanced Memory Reliability Against Multiple Cell Upsets Using Decimal Matrix Code, IEEE transactions on very large scale Integration(VLSI) systems, Vol. 22, No. 1, January 2014.

[47] R. Azarderakhsh and A. Reyhani-Masoleh, Efficient FPGA implementations of point multiplication on binary Edwards and generalized Hessian curves using Gaussian normal basis,IEEE Trans. VLSI Systems, Vol. 20, No. 8, Aug. 2012, pp. 1453-1466.

[48] H. Mahdizadeh and M. Masoumi, Novel Architecture for Efficient FPGA Implementation of Elliptic Curve Cryptographic Processor Over GF(2163),IEEE Trans. on Very Large Scale Integration(VLSI) Systems, Vol. 21, No. 12, Dec. 2013, pp. 2330-2333.

[49] M.Feldhofer and J.Wolkerstorfer, Strong Crypto for RFID Tags - A Comparison of Low-Power Hardware Implementations, ISCAS, 2007, pp. 1839-1842.

[50] J. Goodman and P.Chandrakasan, An energy-efficient reconfigurable public-key cryptography processor, IEEE Journal of Solid-State Circuits, Vol. 36, No. 11, 2001,pp. 1808-1820.

[51] Burak Govemet al, A Fast and Compact FPGA Implementation of Elliptic Curve Cryptography Using Lambda Coordinates, Volume 9646 of the series Lecture Notes in Computer Science, April 2016, pp. 63-83.

[53] W. Chelton and M. Benaissa, Fast Elliptic Curve Cryptography on FPGA, IEEE Trans. VLSI Systems, Vol. 16, No. 2, Feb.2008,pp. 198–205.

[54] G. Sutter, J. Deschamps and J. Imana, Efficient Elliptic Curve Point Multiplication Using Digit Serial Binary Field Operations, IEEE Trans. Ind. Electron, Vol. 60, No. 1, 2013, pp. 217-225.

[55] Y. Zhang, D. Chen, Y. Choi, L. Chen and S. B. Ko, A high performance ECC hardware implementation with instruction-level parallelism over GF(2163), Micro process. Microsystems, Vol. 34, No. 6, Oct.2010, pp. 228–236.

[56] H. M. Choi, C. P. Hong and C. H. Kim, High Performance Elliptic Curve Cryptographic Processor Over GF(2163), In proc. 4th IEEE Intl. Symposium on Electronic Design, Test & Applications, DELTA,2008, pp. 290–295.

[57] C. Rebeiro, S. Roy and D. Mukhopadhyay, Pushing the Limits of High- Speed GF(2m) Elliptic Curve Scalar Multiplication on FPGAs, Lecture Notes in Comp. Sc.–CHES, vol. 7428,2012, pp. 496-511.

[58] S. Liu, L. Ju, X. Cai, Z. Jia and Z. Zhang, High Performance FPGA Implementation of Elliptic Curve Cryptography over Binary Fields,In proc. 13th IEEE Int. Conf. on Trust, Security and Privacy in Comp. and Communications(Trust Com), 2014, pp.148-155.

[59] A. P. Fournaris, J. Zafeirakis and O. Koufopavlou, Designing and Evaluating High Speed Elliptic Curve Point Multipliers, In proc. 17th Euro micro Conf. on Digital System Design (DSD), 2014, pp.169-174.

[60] Z. Khan and M. Benaissa, Throughput Area Efficient ECC Processor on FPGA, IEEE Transactions on Circuits and Systems II: Express Briefs, Vol. 62, No.11,Nov. 2015, pp. 1078-1082.

[61] Z. Khan and M. Benaissa, High Speed ECC Implementation on FPGA over GF(2m), In Proc.25th Int. Conf. on Field-programmable Logic and Applications (FPL), Sept. 2015, pp.1-6.