Advances in Intelligent Systems and Computing

Volume 538

Series editor

Janusz Kacprzyk, Polish Academy of Sciences, Warsaw, Poland
e-mail: kacprzyk@ibspan.waw.pl

About this Series

The series "Advances in Intelligent Systems and Computing" contains publications on theory, applications, and design methods of Intelligent Systems and Intelligent Computing. Virtually all disciplines such as engineering, natural sciences, computer and information science, ICT, economics, business, e-commerce, environment, healthcare, life science are covered. The list of topics spans all the areas of modern intelligent systems and computing.

The publications within "Advances in Intelligent Systems and Computing" are primarily textbooks and proceedings of important conferences, symposia and congresses. They cover significant recent developments in the field, both of a foundational and applicable character. An important characteristic feature of the series is the short publication time and world-wide distribution. This permits a rapid and broad dissemination of research results.

Advisory Board

More information about this series at http://www.springer.com/series/11156

Editors
Masato Akagi
School of Information Science,
Area of Human Life Design
Japan Advanced Institute of Science
and Technology
Nomi-shi, Ishikawa
Japan

Thanh-Thuy Nguyen
Department of Computer Science
VNU University of Engineering
and Technology
Hanoi
Vietnam

Duc-Thai Vu
Faculty of Information Technology
Thai Nguyen University of Information
and Communication Technology
Thai Nguyen
Vietnam

Trung-Nghia Phung
Thai Nguyen University of Information
and Communication Technology
Thai Nguyen
Vietnam

Van-Nam Huynh
School of Knowledge Science,
Area of Knowledge Management
Japan Advanced Institute of Science
and Technology
Nomi-shi, Ishikawa
Japan

ISSN 2194-5357 ISSN 2194-5365 (electronic)
Advances in Intelligent Systems and Computing
ISBN 978-3-319-49072-4 ISBN 978-3-319-49073-1 (eBook)
DOI 10.1007/978-3-319-49073-1

Library of Congress Control Number: 2016955568

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Low Power ECC Implementation on ASIC

Van-Lan Dao(✉), Van-Tinh Nguyen, and Van-Phuc Hoang

Le Quy Don Technical University, Hanoi, Vietnam
kqha1025@gmail.com, tinh.vxl@gmail.com, phuchv@mta.edu.vn

Abstract. In this paper, the Low power Elliptic Curve Cryptography (ECC) structure over Galois field $GF(2^m)$ is studied and implemented on the Application Specific Integrated Circuit (ASIC) tool for wireless sensor network and Internet of Things (IoT) Applications. Clock gating technique is used for decreasing power consumption. The implementation is conducted by the 180 nm CMOS standard library shows that the proposed ECC structure has the power consumption of 10.4 μW/MHz outweigh than previous designs.

1 Introduction

Recently, the need of using energy-efficient electronic devices, IoT applications and communication networks is more and more emerging. A large number of applications using wireless sensor networks to be used in different areas of life. Wireless sensor networks [2–7] can be utilized in military, agriculture, industry, medicine, sport, environmental monitoring, traffic, smart houses, etc. Figure 1 is the general structure of a wireless sensor network (WSNs) in which the data confidentiality is an essential issue [1].

The objective of this paper is to design a low power ECC structure based on the clock gating technique with area and power constrained condition. The rest of this paper is organized as follows. Section 2 describes the ECC, clock gating technique and Sect. 3 presents the low power ECC structure. Section 4 shows the implementation results and finally, Sect. 5 concludes the paper.

2 ECC and Clock Gating Technique

2.1 Elliptic Curve Cryptography

In 1985, elliptic curve cryptography [15] based on the discrete logarithm problem was proposed by Miller [8] and Koblitz [9] independently. An elliptic curve, over binary field ($GF(2^m)$) can be defined a set of solution to the equation as bellow [10]:

$$y^2 + xy = x^3 + ax^2 + b \tag{1}$$

where $a, b \in GF(2^m), b \neq 0$ and at the same time the point at infinity is $\emptyset$. Thus, if P_1 is a point on the ECC curve then $P_1 + \emptyset = P_1$. Two point operations are used called point addition and point doubling. We consider P_1 and P_2 be points

M. Akagi et al. (eds.), *Advances in Information and Communication Technology*,
Advances in Intelligent Systems and Computing 538, DOI 10.1007/978-3-319-49073-1_36

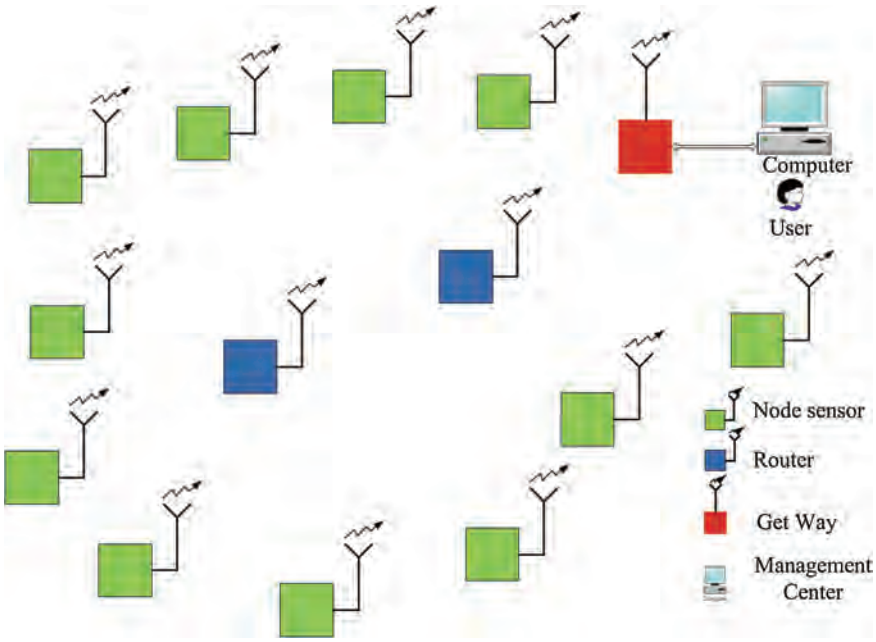


Fig. 1. The general structure of a wireless sensor network.

over ($GF(2^m)$ on the elliptic curve. If the two points are not the same then the adding of the points gives a new point, Q on the elliptic curve called the result of point addition. Again, if the two points are the same, $P_1 = P_2$ then, the addition of the two points gives a new point, Q is called the result of point doubling [10].

The main operation in ECC is point multiplication, where a point, P and a random number, k are considered on an ECC curve and a scalar multiplication is performed to obtain Q, where $Q = k.P$. The basic operation of point multiplication can be obtained by point addition and point doubling. The field arithmetic involved in point addition and point doubling can also be performed in binary fields. The scalar point multiplication $Q = k.P$ can be written as $kP = P + \cdots + P$.

2.2 Clock Gating Technique

Today there are many researches related to clock gating technique [11–13]. Clock gating technique is an efficient power optimization technique that is employed in both ASIC and FPGA designs to eliminate the unnecessary switching activity. This method usually requires the designers to add a small amount of logic to their RTL code to deselect unnecessarily active sequential elements - registers. Figure 2 is the simple classic global clock gating.

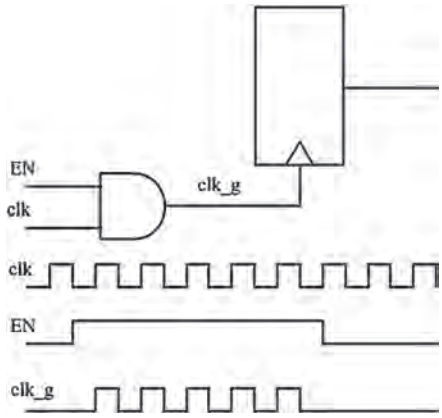


Fig. 2. The simple global clock gating.

3 Low Power ECC Design

In our research, the ECC core architecture as shown in Fig. 3 is used [14]. It includes a FSM control unit, point addition units, point multiplication units and squaring units.

Table 1 lists the function of the signals in the proposed ECC core. On the other hand, clock gating technique is carried out by using the Multiplexer unit.

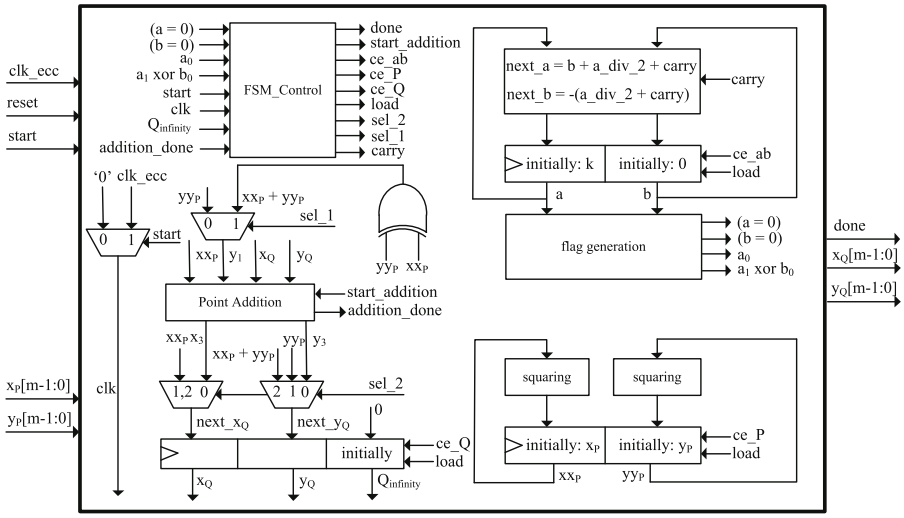


Fig. 3. The ECC core architecture.

Table 1. Signals in the proposed Ecc core.

Signal	Direction	Function
clk_ecc	Input	System clock
reset	Input	System reset
$X_P[m-1:0]$	Input	Data input X_P
$Y_P[m-1:0]$	Input	Data input Y_P
done	Output	To indicate that the output is ready to read
$X_Q[m-1:0]$	Output	Data output X_Q
$Y_Q[m-1:0]$	Output	Data output Y_Q

4 Implementation Results

The ECC core was implemented with VHDL code, simulated in the Modelsim tool and then synthesized by using a 180 nm CMOS standard library in the Synopsys Design Complier. Figure 4 shows the simulation model for the 8-bit ECC core. The input generation block generates the input vector values for the ECC core verification. Figures 5 and 6 present the RTL (pre-synthesis) simulation results in the Modelsim tool and post-synthesis simulation results in the Synopsys VCS-DVE tool, respectively. Table 2 is an example of a test vector for the ECC core verification. It can be seen that the simulation results are the same for pre- and post-synthesis netlists.

Table 2. An example of a test vector for ECC core verification.

K(hexa)	0xFFF030001F0000FFFFF000003800000000
X_P**(hexa)**	0x2FE13C0537BBC11ACAA07D793DE4E6D5E5C94EEE8
Y_P**(hexa)**	0x289070FB05D38FF58321F2E800536D538CCDAA3D9
X_Q**(hexa)**	0x01C14DDAB12BC0D98BF83CE0022F305039F64FC205
Y_Q**(hexa)**	0x006F9B20200EB3CEA80D1DB6C0FB8E6DED4A3C665C

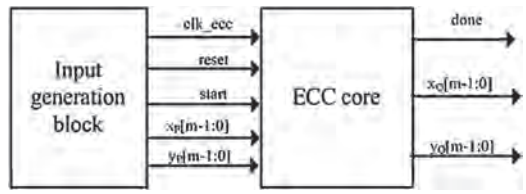
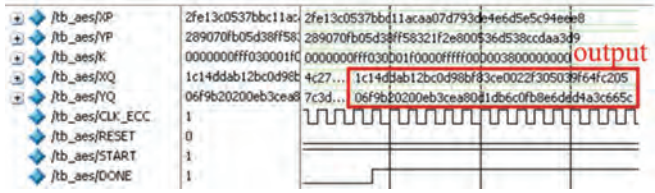


Fig. 4. The simulation model for the ECC core.

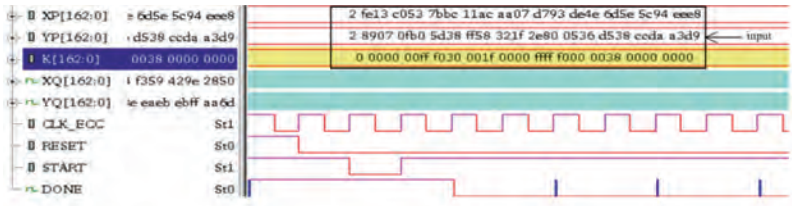
(a) Data and key input



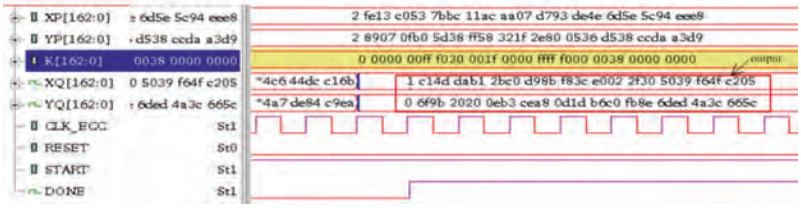
(b) Data output.

Fig. 5. Simulation results in Modelsim tool

The ASIC implementation results are shown in Table 5 in which the proposed ECC core power can be reduced to only 10.4 µW/MHz when $m = 163$. Compared with other designs, the ECC core power consumption can also be reduced significantly while achieving the maximum clock frequency of 59 MHz.



(a) Data and key input



(b) Data output.

Fig. 6. Post-synthesis simulation results in Synopsys VCS-DVE tool

Table 3. Implementation results of ECC core in a 180 nm CMOS ASIC library.

	K163	K233	K283	K409	K571
Area (kgates)	27.5	37.2	47.3	65.5	98
Speed (MHz)	59	56	61	56	55

Table 4. Power consumption of ECC core in a 180 nm CMOS ASIC library (μW).

ECC core	K163	K233	K283	K409	K571
Not clock gating	143	203	246	356	499
Clock gating	10.4	40	58	108	174

Table 5. Comparison of ECC core designs.

Design	Field size (m)	Power	Note
[16]	163	17 µW	4-bit digit multiplier
		305 µW	3-reg. coprocessor
		503 µW	7-reg. coprocessor
		12000 µW	typ. 8-bit processor
[17]	233	20.38 mW	Single Processor
		64.64 mW	Asynchronous MIMD
		49.51 mW	MIMD-SIMD
[18]	192	39.3 µW	-
[19]	192	18.85 µA@100 kHz	-
[20]	134	<15 µW@200 kHz	-
[21]	100	<400 µW@500 kHz	-
[22]	193	42.8 µW/MHz	-
This work	233	40 µW/MHz	-

In this paper, the ECC core is synthesized with two cases of using clock gating techniques and not using clock gating techniques. Area and speed of the ECC core in both cases were similar, synthesis results are shown in Table 3. However, the power consumption of the ECC core with clock gating technique is reduced significantly. For example, $m = 163$, the power consumption of ECC core using clock gating technique decreased by 92.7 % in comparison to the case not using clock gating technique. Other cases of m are shown in Table 4, in which K163 presents the key length of 163-bit. Figure 7 is the synthesized netlist in the 180 nm CMOS standard cell library for the case of clock gating architecture.

Fig. 7. Synthesized netlist of the ECC core in a 180 nm CMOS library.

5 Conclusions

This paper presented a power efficient ECC core for wireless networks and IoT applications. The ASIC implementation results show that using clock gating techniques, the ECC core power can be reduced significantly. Therefore, this ECC core is highly potential to be used in IoT applications and wireless network nodes such as environment monitoring which requires low power and compact encryption cores. In the future, we will optimize the power consumption and area for the proposed ECC core and apply it for wireless network applications.

References

1. Du, X., Chen, H.-H.: Security in wireless sensor networks. IEEE Wireless Commun. **15**(4), 60–66 (2008)
2. Bari, N., Mani, G., Berkovich, S.: Internet of things as a methodological concept. In: 2013 Fourth International Conference on Computing for Geospatial Research and Application (COM.Geo), San Jose, CA, pp. 48–55 (2013)
3. Hac, A.: Wireless Sensor Network Designs. Wiley, New York (2013)
4. Tiwari, A., et al.: Energy-efficient wireless sensor network design and implementation for condition-based maintenance. ACM Trans. Sensor Netw. (TOSN) **3**(1), 1–23 (2007)
5. Yun, D.S., Lee, S.-J., Kim, D.H.: A study on the vehicular wireless base-station for in-vehicle wireless sensor network system. In: Proceedings of 2014 International Conference on Information and Communication Technology Convergence, pp. 609–610, October 2014

6. Ding, R., Hou, J., Xing, B.: Research of wireless sensor network nodes based on ambient energy harvesting. In: Proceedings of 2013 6th International Conference on Intelligent Networks and Intelligent Systems (ICINIS), pp. 286–288, November 2013
7. Liu, Y., Wang, C., Qiao, X., Zhang, Y., Yu, C.: An improved design of ZigBee wireless sensor network. In: Proceedings of 2nd IEEE International Conference on Computer Science and Information Technology (ICCSIT 2009), pp. 515–518, August 2009
8. Miller, V.S.: Use of elliptic curves in cryptography. In: Williams, H.C. (ed.) CRYPTO 1985. LNCS, vol. 218, pp. 417–426. Springer, Heidelberg (1986). doi:10.1007/3-540-39799-X_31
9. Koblitz, N., Menezes, A., Vanstone, S.: The state of elliptic curve cryptography. Des. Codes Crypt. **19**(2–3), 173–193 (2000)
10. Hankerson, D., Menezes, A., Vanstone, S.: Guide to Elliptic Curve Cryptography. Springer, New York (2004)
11. Zhong, W.J., Noh, N.M., Rosdi, B.A.: Clock gating assertion check: an approach towards achieving faster verification closure on clock gating functionality. In: 2015 6th Asia Symposium on Quality Electronic Design (ASQED), Kula Lumpur, pp. 94–101 (2015)
12. Wimer, S., Koren, I.: Design flow for flip-flop grouping in data-driven clock gating. IEEE Trans. Very Large Scale Integr. (VLSI) Syst. **22**(4), 771–778 (2014)
13. Nikolić, M., Katona, M.: Improve the automatic clock gating insertion in ASIC synthesis process using optimal enable function selection. In: 2010 5th European Conference on Circuits and Systems for Communications (ECCSC), Belgrade, pp. 131–134 (2010)
14. Deschamps, J.-P., Imaãa, J.L., Sutter, G.D.: Hardware Implementation of Finite-Field Arithmetic, 1st edn. Publisher of McGraw-Hill Education, New York (2009)
15. National Institute of Standards and Technology (NIST): Digital Signature Standard (DDS). FIPS Publication 186-3, June 2009
16. Bertoni, G., Breveglieri, L., Venturi, M.: ECC hardware coprocessors for 8-bit systems, power consumption considerations. In: Third International Conference on Information Technology: New Generations, 2006, ITNG 2006, Las Vegas, NV, pp. 573–574 (2006)
17. Purnaprajna, M., Puttmann, C., Porrmann, M.: Power aware reconfigurable multiprocessor for elliptic curve cryptography. In: Design, Automation and Test in Europe, 2008, Munich, pp. 1462–1467 (2008)
18. Ahmadi, H.R., Afzali-Kusha, A.: Low-power low-energy prime-field ECC processor based on montgomery modular inverse algorithm. In: 12th Euromicro Conference on Digital System Design, Architectures, Methods and Tools, 2009, Patras, pp. 817–822 (2009)
19. Feldhofer, M., Wolkerstorfer, J.: Strong crypto for RFID tags - comparison of low-power hardware implementations. In: ISCAS 2007, pp. 1839–1842 (2007)
20. Batina, L., et al.: Public-key cryptography on the top of a needle. In: ISCAS 2007, pp. I831–1834 (2007)
21. Gaubatz, G., et al.: State of the art in ultra-low power public key cryptography for wireless sensor networks. In: 3rd IEEE PerCom 2005 Workshops, pp. 146–150 (2005)
22. de Dormale, G.M., Ambroise, R., Bol, D., Quisquater, J.J., Legat, J.D.: Low-cost elliptic curve digital signature coprocessor for smart cards. In: Proceedings of the IEEE 17th International Conference on Application-Specific Systems, Architectures and Processors, ASAP 06, pp. 347–353 (2006)