International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 05, May 2015
Available at http://internationaljournalofresearch.org

VLSI Modelling of Side Channel Attacks on Modern Cache Based Processors

[1]mukku Dinesh Kumar, [2]g.Dilli Rani,3 Dr.V.Trimurthulu.
[1]II M.Tech VLSI SD Student, CR Engineering College, Tirupathi, Chittoor, (Dist) A.P, India,
[2] Assistant Professor of ECE Dept CREngineering College, Tirupathi (A.P), India.
3 HOD of Department of ECE,CREngineering College ,Titupati(A.P),India.
mukkudinesh@gmail.com, gdillirani@gmail.com

Abstract—
Current processor architectures are advances as the technology swifts to new dimensional era, as performance optimization is one of the key factor and to attain this up to the market demands modern processors have resources like non blocking and pipelined caches along with hold up for content pre fetching. On the other hand, some of these features accidentally frustrate cautiously considered attacks on cryptographic and security algorithms. The attacks fit in to the category of side channel attacks wherein slight leakage of information through side channels such as power and timing can be demoralized to negotiate secret keys in susceptible applications. This paper further expands and modifies the current work in the field of cache-based side channel attacks targeting the software and hardware implementation of side channel attacks. With this document, we have proposed a simulation model to identify the attack on Public key and Private Key Cryptographic devices The Verilog RTL description of proposed work is successfully implement on Virtex -5 FPGA.

Index Terms —
Performance Optimization; Side Channel Attacks; RTL Description ; Virtex -5 FPGA

INTRODUCTION

Side-channel attacks on cryptographic devices have been explained practically against a variety of cryptographic systems. Side-channel attacks uses the fact that in reality, a cipher is not a pure mathematical function $E_K[P] \rightarrow C$, but a function $E_K[P] \rightarrow (C, t)$ where t is any supplementary information produced by the physical execution. Public-key cryptographic devices are susceptible to side-channel attacks. As countermeasures, a number of protected architectures based on linear and nonlinear detecting codes were proposed. Linear codes provide protection only in antagonism to primitive adversaries with defective attack capabilities, on the other hand nonlinear codes provides defense against strong adversaries, but at the price of high area overhead (200% - 400%).The projected plan is a novel side channel attacker modeling technique based on defense methodology of a basic building block of many public-key cryptographic devices which is under nonlinear code error detection, Cryptographic devices are mainly suffers with various side channel attacks includes for timing analysis, power analysis and fault injection attacks. The current Deep Sub Micron technology is flexible to introduce timing attacks and power attacks but the probability to the interloper are to introduce fault injection attacks over the Cryptographic devices is becoming a new dispute to identify and it must need to be model to enhance the security for Cryptographic areas.

Since the multiplier which is a basic building block of all cryptographic applications and it plays a crucial and critical role in all major Cryptographic algorithms, and also as per the design concerns it occupies much more area so as to consumes more power therefore the multiplier design parameters such as speed, area and power must count into account for reliability issues of the Cryptographic devices and thereby to encounter the side channel attacks. A variety of multiplier architectures have been proposed for security algorithms to guarantee the security of the devices, in this regards various error detecting techniques are also anticipated some of them are, linear arithmetic codes, includes parity codes, Hamming codes, AN-codes etc. Non linear arithmetic codes like, Robust Codes and Multi linear arithmetic codes, each class has their advantages and limitations, therefore an appropriate study and scrutiny is required to select a suitable detection algorithm to model a side channel attack especially in the case of advanced cached based processor architecture.

MUKKU DINESH KUMAR is a Student of VLSI System Design at Chadalawada Ramanamma Engineering College, Tirupati (A.P), India. (Phone: +91 9618344921; email: mukkudinesh@gmail.com).

G DILLI RANI Assistant Professor of ECE Dept Chadalawada Ramanamma Engineering College, Tirupathi (A.P), India. (Phone: +91 9701426399; email: gdillirani@gmail.com).

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 05, May 2015
Available at http://internationaljournalofresearch.org

Usually multiplier consumes more design space when physical design is concerned and also as the increased data length results more consumption of chip area, the other factor which affects the effectiveness of the multiplier is its partial product, as a result there is a strong reason that multiplier design for applications like Cryptography is always serious issue. Hence there is a strong desire to get good tradeoff between area, power and speed particularly for Deep Sub Micron era.

DESIGN DEVELOPMENT

Because of Advent development of VLSI trends these days we had encouraged with very high speed FPGA units which makes them to sustain implementation of high speed cryptographic applications and becomes sophisticated environment for real time scientific applications. The proposed architecture is designed with large amount of data base and its controls so that it could accumulate more than eight million test input data of each 64 bit. The suggested design is implemented in verilog HDL and synthesized for Xilinx virtex-5 device. The design is synthesized using Xilinx 14.4 Vivado ISE tool

TABLE 1
SUMMARY OF DESIGN CONSIDERATIONS

Sno	Design consideration	Selection
1	Compiler	Xilinix14.4Vivado
2	Programming Language	Verilog
3	Standard	Cryptography
4	FPGA	Virtex -5
5	Interface	USB

I. MODELING OF SIDE CHANNEL ATTACK ON FPGA

As we are familiar that the cryptographic algorithm are major dependable on AES(Advanced Encryption Standard), before design discussion of the proposed method a brief description of the cipher's properties that were utilized in this study has to be discussed. This paper will spotlight exclusively on AES with a 128 bit key. 192 and 256 bit versions use a different key expansion algorithm and more iteration. AES is an iterated cipher: Each round i takes a 16-byte block of input Xi and a 16-byte block of key ingredient Ki, producing a 16-byte block of output Xi+1. Each round is carried out by computing the algebraic calculations on Sub Bytes, Shift Rows, and Mix Columns on Xi, then taking the exclusive-or with the round key Ki. Computational based software implementations of AES combine all above procedures and initially calculate the values. The values are stored in large lookup tables, T0; T1; T2; T3, each plotting one byte of input to four bytes of output. Each round is carried out by splitting up Xi into 16 bytes xi 0; xi 1; : : : ; xi15, and Ki into 16 bytes ki0 ; ki1; : : : ; ki15. The encryption round is then carried out as shown in the figure1.

$$X^{i+1} = \{T_0[x_0^i] \oplus T_1[x_5^i] \oplus T_2[x_{10}^i] \oplus T_3[x_{15}^i] \oplus \{k_0^i, k_1^i, k_2^i, k_3^i\},$$
$$T_0[x_4^i] \oplus T_1[x_9^i] \oplus T_2[x_{14}^i] \oplus T_3[x_3^i] \oplus \{k_4^i, k_5^i, k_6^i, k_7^i\},$$
$$T_0[x_8^i] \oplus T_1[x_{13}^i] \oplus T_2[x_2^i] \oplus T_3[x_7^i] \oplus \{k_8^i, k_9^i, k_{10}^i, k_{11}^i\},$$
$$T_0[x_{12}^i] \oplus T_1[x_1^i] \oplus T_2[x_6^i] \oplus T_3[x_{11}^i] \oplus \{k_{12}^i, k_{13}^i, k_{14}^i, k_{15}^i\}\}.$$

Figure1: Encryption Rounds of Cryptographic algorithm

The entire round calculation can be computed successfully with a special king of encoding technique in software this manner, with just up to 16 table lookups and 16 word-lengths
x-or's the last round may not be computed Mix Column technique since it might be immaterially be inverted by an attacker and would apparently slow down hardware implementations of Cache based processors and there by Cryptographic Devices.

Side-channel attacks have been verified in opposition to implementations of many cryptosystems, which includes timing attacks, power supply attacks, injection of electromagnetic radiation, etc. Public key algorithms have proved the most susceptible to timing attacks because they characteristically execute lengthy mathematical procedures, and the corresponding execution time is a direct function of the input data. And also lot of Cache based attacks are also demonstrated with plenty of literature. Their attack requires a very low (» 50) number of encryptions, but need physical access to a machine's power supply. Cache access patterns also cause timing variation, which can be used to construct a timing attack against AES software devoid of direct surveillance of the cache accesses. Which lead to a great challenge especially at deep sub micron area of applications like Electronic Gadgets, Smartphone and high speed super computers, security systems etc.

PROPOSED ALGORITHM and ARCHITECTURE:

By considering all above mentioned principles the proposed scheme whose execution is planned with the algorithm as shown in the following figure2 and the relevant implementation structure is shown in the figure3.

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 05, May 2015
Available at http://internationaljournalofresearch.org

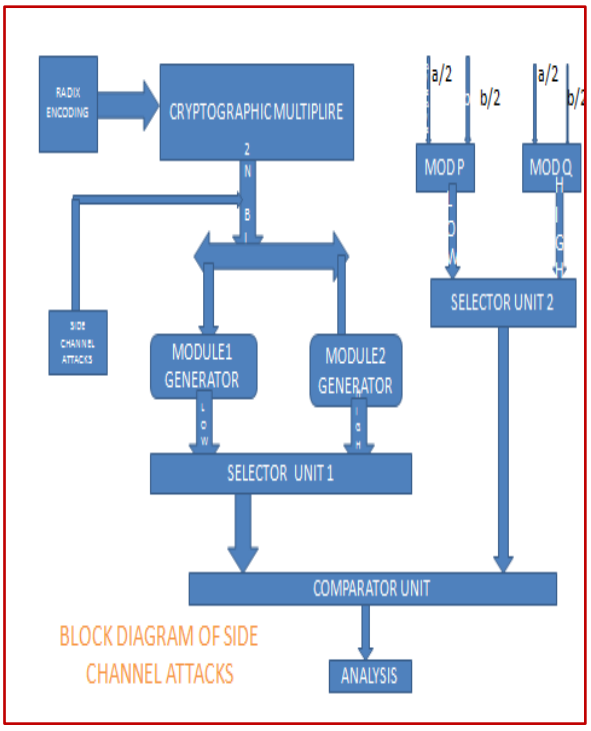

Figure2: Proposed Attacker model architecture

Front-End Modeling:

This phase of implementation contains the following stages simulation using Xilinx 14.4 Vivado suite, synthesis using Xilinx 14.4 XST and verifying on Virtex – 5 FPGA board. The intention of attacker model on cache based processor unit is to create a fully suggested VLSI architecture for advanced processor architectures. The proposed architecture has the above implementation diagram.

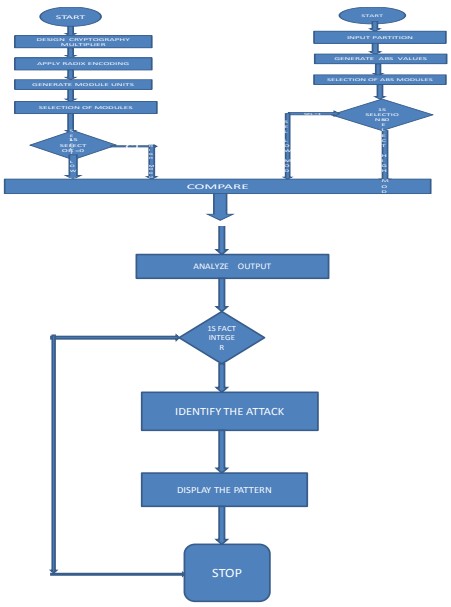

Figure3: Proposed Algorithm

II. SIMULATION AND SYNTHESIS RESULTS

The Verilog RTL Description of the above article is simulated and synthesized using Xilinx14.4 (ISE-Simulator), various results are shown below, figure4 and figure5 shows the simulation output result before and after applying attacker model.

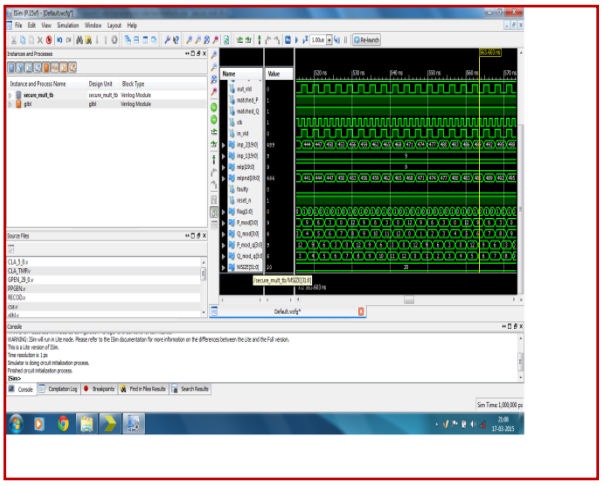

Figure4. Simulation output before attacker model

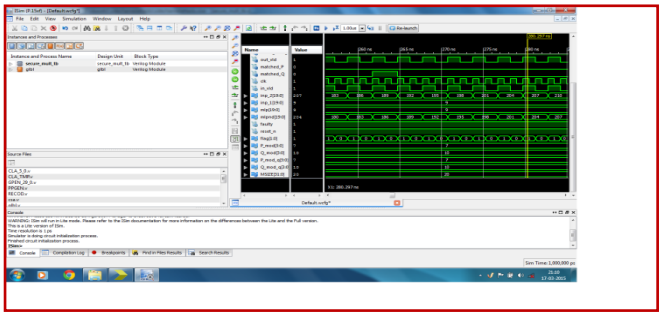

Figure5. Simulation output after attacker model

The synthesis results of proposed model are shown in figure6 and the summary of synthesis report is listed in the table2.

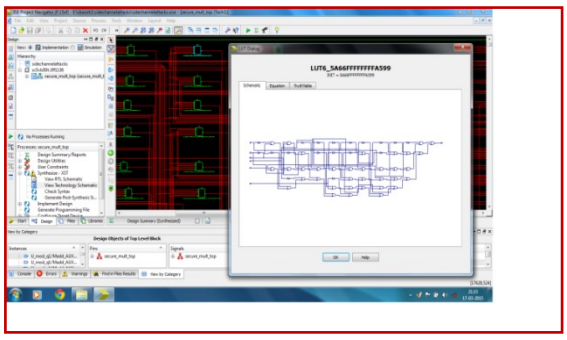

Figure6. Synthesized output

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 05, May 2015
Available at http://internationaljournalofresearch.org

The Synthesized report is summarized in the following Table.

TABLE 2
SUMMARY OF SYNTHESIS REPORT

Sno	Parameter	Quantification
1	Target Device	xc5vlx50t-2-ff1136
2	Slice Logic utilization	< 9%
3	Slice logic distribution	92%
4	IO utilization	47%
5	Specific feature factor	3%
6	Total logic delay	57.827 nS
7	Total offset delay	57.827 nS
8	Total path delay	5.401 nS
9	Real time compilation	1140.00 S
10	Total memory usage	351276 Kb

III. CONCLUSION

This paper analyzes the complete VLSI Hardware modeling side channel attacks on modern processors for cryptographic applications; this paper has realized with Xilinx tools along with Virtex -5 FPGA such designs are suggested to exhibits a competitive performance with current work.

ACKNOWLEDGMENT

We would like to thank Dr.V.THRIMURTHULU, for his outstanding support and also we would like to especially express gratitude EDUPLUS-IERC team for their technical advices.

REFERENCES

[1] John L. Hennessy and David A.Patterson, "Memory Hierarchy Design," in *Computer Architecture, A Quantitative Approach,* 5" ed. Morgan Kaufmann, 2011, ch. 2, sec. 2, pp. 78-95

[2] N. Lawson, "Side-Channel Attacks on Cryptographic Software", *IEEE Security & Privacy,* vol. 7, no. *6,* pp.65 -68 2009

[3] G. Bertoni, V. Zaccaria, L. Breveglieri, M. Monchiero and G. alermo, "AES Power Attack Based on Induced Cache Miss and Countermeasure", Proc. of the International Conference on Information Technology: Coding and Computing (ITCC05), 2005

[4] J. Daemen and V. Rijmen, "The Design of Rijndael: AES - The Advanced Encryption Standard," Springer, 2002. ISBN 3-540-42580-2. (238pp.)

[5] Yinqian Zhang, A. Juels, A. Oprea, and M.K.Reiter."Home Alone Coresidency Detection in the Cloud via Side-Channel Analysis," In security and Privacy (SP) ,2011 IEEE Symposium on, pages 313 -328, May 2011.

AUTHORS

DENESH KUMAR MUKKU received his B.Tech Degree in Electronics & Communication Engineering from Chadalawada Ramanamma Engineering College Tirupati (A.P),India, in the year2011. Currently pursuing his M.Tech Degree in VLSI SYSTEM DESIGN at Chadalawada Ramanamma Engineering College, Tirupati (A.P),India ..His area of research includes in vlsi modelling of side channel attacks on modern proce **ssor.**

G.DILLIRANI is currently working as Assistant Professor in the Dept of Electronics &Communication Engineering at Chadalawada Ramanamma Engineering College Tirupati, India .She has 6 years of teaching experience .Her's extensive education includes B.Tech from SIET Puttur,from JNTU Hyderabad University,plus M.tech in SIET Puttur ,A.P,India. She is making research in the field of Biomedical Signal Processing.

DR.V.THRIMURTHULU M.E., Ph.D., MIETE., MISTE Professor & Head of ECE Dept. He received his Graduation in Electronics & Communication Engineering AMIETE in 1994 from Institute of Electronics & Telecommunication Engineering, New Delhi, Post Graduation in Engineering M.E specialization in Microwaves and Radar Engineering in the year Feb, 2003, from University College of Engineering, Osmania University, Hyderabad., and his Doctorate in philosophy Ph.D from central University, in the year 2012. He has done his research work on Ad-Hoc Networks.