ISSN 2394-3777 (Print)

ISSN 2394-3785 (Online)

Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 7, March 2018

Securing Embedded processor using gating and memory splitting Topology

R.Nithyalakshmi[1],P.Pavadharani[2],M.Priyadharshini[3],R.Renuga[4],M.Bhakyalakshmi[5]

Assistant Professor, Department of ECE, Bharathiyar Institute of Engineering For Women,Deviyakurichi,Tamilnadu,India[1]

UG Scholar,Department of ECE, Bharathiyar Institute of Engineering For Women,Deviyakurichi,Tamilnadu,India[2,3,4,5]

ABSTRACT

Power consumption has risen to one of the much sought after field of research in VLSI design. The clock gating technique that has been proposed is based on the relationship between the triggering transition of the clock and the present and the next state function of the flip flop. Power has been calculated by implementing the clock gated benchmark circuits. It has been found that the power reduces although there is an area trade off. From the experimental results shown above, the dynamic power is reduced by cutting off the idle cycles of the flip flop and splitting the memory by disabling the clock input. The proposed model can be made compatible with other optimization techniques for further reduction of power and also for the reduction in number of components.

1.INTRODUCTION

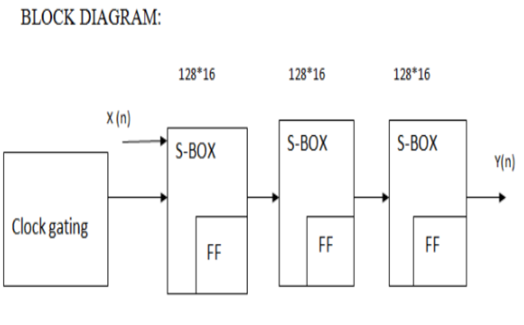
Embedding security into devices is not a straightforward process. First the type of security functionality to embed into the device must be determined. This is often a challenge since specifying security requirements largely depends upon attack or threat models, which may not be fully known at the time.

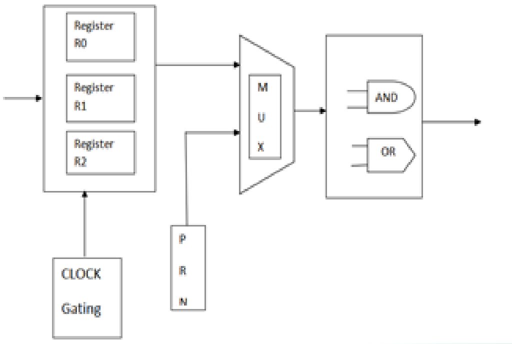
Designers must also ensure that their implementations are secure, since this is typically the focus of attacks. Unlike other constraints such as energy, performance, and cost, which can be verified and quantified, the verification of security is often not possible (apart from functionality).In general, the security cannot be quantified nor can it be readily verified due to the possibility of unforeseen future attacks. From a security point of view, a complete understanding of the device from the

1

process level and up is necessary in order to verify that the security and its implementation are sound. This section will discuss attacks and the need for

BASIC BLOCK DIAGRAM





S-BOX DIAGRAM

2.ADVANCED ENCRYPTION STANDARD (AES)

Rijndael algorithm is symmetric block cipher that can process data blocks

security in some interesting embedded systems.General-purpose CPUs are generally designed for high performance supporting full programmability and supporting a wide range of workloads. This is unlike embedded systems which generally utilize processors and/or devices embedded in specific systems that are highly constrained.

of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits, which is specified,however, they are not adopted by this standard.The algorithm specified will be referred to as “the AES algorithm”. The algorithm may be used with the three different key lengths indicated above, and therefore these different “flavors” may be referred to as “AES-128”, “AES-192” and “AES-256” [86].This specification includes the following sections:

1. Mathematical properties that is useful in understanding the algorithm.

2. Algorithm specification, covering the key expansion, encryption, and decryption routines. Implementation issues, such as key length support, keying restrictions, and additional block/key/round sizes.

All byte values in the AES algorithm will be presented as the concatenation of its individual bit values (0 or 1) between braces in the order {b7, b6, b5, b4, b3, b2, b1, b0}.

3.CLOCK GATING

Clock gating is a popular technique used in many synchronous circuits for

2

reducing dynamic power dissipation. clock gating saves power by adding more logic to a circuit to prune the clock tree. Pruning the clock disables portions of the circuitry so that the flip flops in them do not have to switch states. Switching states consumes power.

When not being switched, the switching power consumption goes to zero and only leakage currents are incurredin Gate based clock gating.

Design of Clock Gated D Flip Flop

The flip flop that is most commonly used for the designing of any circuit is the D flip flop as it has a simple function. The input that is fed as the input to the D flip flop appears as the output after the edge of the clock is triggered. It is used commonly in many circuits as a memory element because it ensures that the inputs S and R are never equal to one at the same time. For. This is the principle on which the following design has been described. When the present and next state of the D flip flop is observed, it is noticed that when two continuous inputs are identical, the D flip flop gives the same value as output. The clock gated D flip flop. The clock cycle that is fed into the D flip flop when the output does not vary is termed as idle clock cycles. The number of cycles in the derived clock is less than that of the original clock Waveform for gated D flip flop,Power Analysis of D Flip Flop is obtained from Xilinx too l,We adapt VHDL technique for its Configuration,. Due to the reduce in the number of cycles of the derived clock, the power consumed by the clock gated D flip flop is reduced by 29.74% compared to original D flip flop.

4.MEMORY SPLITTING:

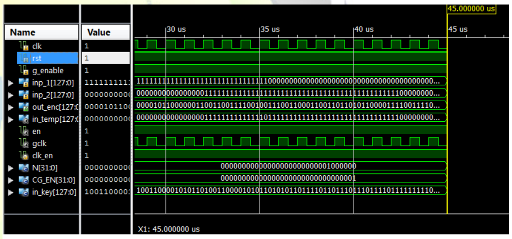
A critical component in the design of secure processors is memory encryption which provides protection for the privacy of code and data stored in off-chip memory. The overhead of the Recently hardware counter-based one-time pad encryption techniqueshave been proposed to reduce this overhead.

Our experiments show that the proposed technique reduces average execution time overhead of memory encryption for low-end (medium-end) embedded processor with 0 KB (32 KB) L1 cache from 60% (13.1%), with single counter, to 12.5% (2.1%) by additionally using only 8 hardware counter-registers.Currently, the high-end processors operate at 3–4 GHz frequency whereas even the fastest off-chip memory operates at just around 600 MHz [1–6].The idea of memory hierarchy comes from observing two common characteristics of the memory accesses in the wide range of programs, namely temporal locality and spatial locality.

In typical computer systems, more than four levels of the memory hierarchy are widely adopted, Recent work has shown that side channel attacks pose a serious threat to cryptosystems implemented in embedded devices and a memory at the higher level is realized as a smaller and faster memory than those of the lower levelsdescribes typical arrangement of the memory hierarchy.

5.RESULT AND ANALYSIS

This proposed system was developed to encrypt the data in secure manner using clock gattingtechnology.The upcoming signal values which are developed by the Xilinx was implemented. The processor is highly secured by generating the duplicate keys. AES algorithm is used to masking the input data and duplicate keys generated and the waveform are generated in Xilinx.



Name	Value
clk	1
rst	1
g_enable	1
inp_1[127:0]	111111111
inp_2[127:0]	000000000
out_enc[127:0	000010110
in_temp[127:0	000000000
en	1
gclk	1
clk_en	1
N[31:0]	000000000
CG_EN[31:0]	000000000
in_key[127:0]	100110000

6.CONCLUSION

The data is secured by combining it with duplicate keys generated by pattern recognition number. By this topology the data cannot be able to hack. It provides high security to the processor.

REFERENCES

[1] J.E.Thorton,"parallel operation in the CDC6600," in AFIPS proc.FJCC,1964,pp.33-40.

[2] S.Mangard, E.Oswald, and T.Popp,power analysis attack-Revealing the secrets of smartcard.Springer,2007.

[3] P.C.Kocher, J.Jaffe, and B. Jun,"Differential power analysis," in advances in cryptology, 1999, pp.388-397.

[4]K.Tiri,D.Hwang,a.Hodjat,B-C.Lai,S. Yang, P.Schaumont ,and I.Verbauwhede,"Prototype IC with WDDL and differential routing- DPA resistance assessment," in proceeding of the 2005 cryptographic hardware and embedded systems workshop, 2005,pp.354-365.

4