Securing Low Power DES Crypto-Chip against PA-FI Side Channel Attack

Behnam Ghavami, Hossien Pedram

Computer Engineering Department, Amirkabir University of Technology
(Tehran Polytechnic) 424 Hafez Ave, Tehran 15785, Iran
E-mail: {ghavami, pedram}@ce.aut.ac.ir

Abstract

It has shown that balanced QDI asynchronous circuits possess considerable inherent countermeasure against side channel attacks. Due to the hardware redundancy of previous balanced-gate designs, there are many faults making a balanced-gate imbalanced without causing logical errors. This vulnerability increases the possibility of new attack based on the combination of fault and power attacks. In this paper, we present an asynchronous approach to implement a Data Encryption Standard (DSA) crypto-chip which is resistant to DPA-FI attack. Furthermore, by using asynchronous methodology and suggesting a restructuring on the conditional statements at the high-level description of the DES circuit, results in a huge optimization in power consumption. This implementation shows a 1.8 times energy consumption improvement over the synchronous implementation using the same TSMC 0.18µm technology.

1. Introduction

Widely use of the secure hardware systems has recently increased research interests in cryptanalysis leading to countermeasures solutions. During the past decade, there have been extensive researches to enhance the security of cryptosystems [1]. Although cryptographic algorithms have been designed to withstand rigorous cryptanalysis attacks, they are vulnerable to the attacks which analyze the physical characteristics of the hardware. Several attacks have been developed that exploit the physical properties of implementation and information leaked through side channels[3][4][6].

When a cryptographic module performs encryption or decryption, side channel parameters such as power dissipation, electromagnetic radiation or time operation correlate with the processed data. This information can be useful to find the secret key of the crypto-systems.

Efficient methods for performing power analyzing and fault analyzing attacks have been developed to statistically evaluate the side channels and extract useful information [3].

Differential Power Analysis (DPA), one of the well-known types of side-channel attacks, is based on the fact that logic operations in standard static CMOS have power characteristics depending on the input data. By using this attack the key of an unprotected ASIC AES implementation was found in less than three minutes [3] which shows the weakness of the unprotected security hardware modules.

Another side-channel attack is Differential Fault Attack (DFA) that uses the information obtained from an incorrectly functioning hardware to find the secret key. DFA attack was first proposed in [6] against of hardware implementation of DES algorithm. Faults can be injected into a device even in the presence of tamper resistance packaging by introducing the device to elevated levels of radiation or temperature, atypical clock rate or incorrect voltage [7].

Several solutions have been proposed to resistance against DPA and DFA attacks. One of the most effective countermeasures against power analysis attacks is based on the use of specially designed balanced gates where the power consumption is equal for all data and all transitions of the gate. Several balanced gates recently have been presented (e.g SABL [8] and BSDT [9]). Most of proposed fault attack countermeasures were based on the addition of redundancy to the hardware, usually in the form of error-detecting codes, to detect errors in the logical level (i.e. [10]).

It has recently become clear that if asynchronous circuits were implemented correctly they would have several convenient features for a secure hardware design [11][12]. Since the clock signal is eliminated in asynchronous circuits, they are resistant to the fault injection in clock. Clock elimination attenuates electromagnetic radiation leading to much increased complexity in these types of attacks. In addition power consumption in the dual rail QDI asynchronous circuits is independent of input data [12], so these circuits are countermeasure to power attacks. Symmetry in the data
processing circuits to assure independence of the power consumption from input values, and exploiting the propagating alarm signals to defend chip against fault injection are design aspects mentioned to increase the resistance to attacks. The asynchronous approach to increase the security of crypto-chips is based on power balancing of QDI logic cells. The analysis of three different QDI DES architectures and design styles demonstrated how properties of a dual-rail encoding and four-phase handshake protocol can significantly improve the countermeasure against DPA attacks [11].

Balanced asynchronous circuits are effective countermeasures for their respective attacks if the side-channels are considered separately. Joint consideration of power and fault side channels attacks can raise several practical security limitations for the approaches. In other words, balanced QDI circuits are vulnerable to a new hybrid attack, when power and fault attacks are considered together [2].

All the currently known balanced QDI circuits require hardware redundancy to ensure balanced computations. Weaknesses in the present balanced cells exist due to the redundancy of the cells. There exist many internal transistor level faults which will not affect the Boolean function of the cell and can not be detected by traditional testing methods; however these can affect the balanced behavior of the cell [2].

One of the main issues to design Crypto systems is the power reduction, especially for portable systems as smart cards which requires new methods in design architectures and implementation of Crypto Systems. Asynchronous circuits gain popularity due to their potential advantages such low power consumption. Most of the asynchronous benefits are due to the elimination of the global clock by employing local message passing as the main synchronization method [16].

In this paper, we present a customized template for secure asynchronous hardware implementation of DES crypto-chip. Also we introduce an efficient methodology to reduce power consumption in asynchronous DES crypto-chip based on restructuring on the conditional statements in a high-level description of the circuit specification.

The rest of the paper is as follows: In section 2, we present asynchronous circuit design methodology, especially synthesis of QDI circuits with AsyncTool synthesis tool. Vulnerability of the existing library cells to DPA attacks is shown in section 3. The proposed cell library design approach is described in section 4. Section 5 draws the power optimization method in outline and the DES implementation. Finally, the conclusion is presented in section 6.

2. Asynchronous Circuit Design

Asynchronous circuits represent a class of circuits that are not controlled by a global clock but rely on exchanging local request and acknowledge signaling for the purpose of synchronization. In fact, an asynchronous circuit is composed of individual modules which communicate with each other by means of point-to-point communication channels. Therefore, a given module becomes active when it senses the presence of an incoming data. It then performs the computation and sends the result via output channels. Communications through channels are controlled by handshake protocols [16].

An asynchronous circuit is called delay-insensitive if it preserves its functionality independent of the delays of gates and wires [16]. It has been shown that the range of the circuits that can be implemented completely delay-insensitive is very limited [19]. Therefore, some timing assumptions exist in different design styles that must be hold to ensure the correctness of the circuit. Different asynchronous techniques distinguish themselves in the choice of the compromises to the delay-insensitivity.

Quasi delay-insensitive (QDI) circuits are like delay-insensitive circuits with a weak timing constraint: isochronic forks. In an isochronic fork, the difference between the delays through the branches must be less than minimum gate delay. QDI implementations appear to be the most appropriate class of asynchronous circuits that can be synthesized automatically from any large high-level behavior specifications. This is because of the week timing constraint that can be easily managed in this design style. Return to zero handshaking protocol with dual-rail data encoding that switch the output from data to spacer and back is the most common QDI implementation form. The most efficient QDI implementations are based on per-charge logic which makes it easy to incorporate existing dynamic domino style balanced power structures in the QDI templates [9].

The encodings of the channels can be in a variety of ways. Return to zero handshaking protocol with dual-rail data encoding that switches the output from data to spacer and back is the most common QDI implementation form. We use a dual rail encoding. The data channel contains a valid data (token) when exactly one of 2 wires is high. When the two wires are lowered the channel contains no valid data and is called to be neutral (Figure 1).
One of the major protocols used in asynchronous circuits is four phase protocol. In the sequence of four phase protocol a receive action consists of four steps. (1) Wait for input to become valid: [L]. (2) Acknowledge the sender after the computation performed L^ack. (3) Wait for inputs to become neutral [~L]. (4) And lower the acknowledgement signal. A send action consists of four phases: (1) send a valid output R.(2) wait for acknowledge [R^ack]. (3) Make the output neutral ~R.(4) wait for acknowledge to lower [~R^ack].

Figure 2 shows a four phase handshake sequence.

2.1 AsyncTool: A QDI asynchronous synthesis tool

AsyncTool (also known as Persi) is an asynchronous synthesis tool developed for automatic synthesis of QDI asynchronous circuits [13]. The structure of AsyncTool is based on the design flow shown in figure 3 which can be considered as the following three individual portions: QDI synthesis, layout synthesis, and simulation at various levels. The simulation flow is intended to verify the correctness of the synthesized circuit at all levels of abstraction.

CSP is a well-known language for description of concurrent systems which is accepted as a good description language for asynchronous systems. AsyncTool uses Verilog-CSP [14], an extension of the standard Verilog supporting asynchronous communications as the hardware description language for all levels of abstractions except the netlist which uses standard Verilog. The input of AsyncTool is a Verilog description of a circuit that will be converted to a netlist of standard-cell elements through several steps of QDI synthesis flow. The two major steps in AsyncTool synthesis are Decomposition and Template Synthesizer (TSYN). In the following subsections we briefly describe the functionalities of these two stages.

2.1.1 Decomposition

Our synthesis approach is based on the pre-design asynchronous four-phased dual rail templates. Each template can be considered as a simple pipeline stage. The most renowned form of these templates is named pre-charge full buffer (PCFB) [15] (Figure 4). A PCFB reads its data from input ports performs the computations and writes the results to the output ports. It can have multiple inputs and outputs, have conditional inputs and outputs and hold states. The circuit is similar to pre-charge domino-logic style circuits in synchronous designs except that instead of a global pre-charge signal local pre-charge signals are generated. The QDI timing constraint (i.e. isochoric fork) is local to each template. Figure 4 represents a PCFB buffer used in AsyncTool synthesis tool.

The high-level Verilog-CSP description of even very simple practical circuits can not directly be converted to PCFB. The intention of Decomposition stage is to decompose the original description into a collection of smaller interacting processes. These processes are compatible to predefined templates and are synthesized in the next stages of QDI synthesis flow.

2.1.2 TSYN

Template Synthesizer [17], as the final stage of QDI synthesis flow, receives a Verilog-CSP source code containing a number of PCFB-compatible modules and
optionally a top-level netlist and generates a netlist of standard-cell elements with dual-rail ports that can be used for creating final layout. The output of TSYN can be simulated in standard Verilog simulators by using the behavioural description of standard-cell library elements.

3. DPA attack and vulnerability of existing PCFB template

DPA attacks use statistical techniques to determine the secret keys by observing the power consumption of crypto devices [3]. Usually in a typical attack, an attacker samples power consumption of the target device to build the power traces using high-speed analog-to-digital converter can be used to create these power traces. The measured power traces are compared with the predicted power consumptions. To make a prediction a guess on the secret key is used. Several statistical and mathematical techniques are available to correlate the predictions and measurements. Based on these analyses the secret key can be found. Figure 5 shows the DPA platform.

Initially, our cell library was designed to get the highest performance of the system. The circuits which synthesized with current cell library have the potential of being attacked by power analysis but it is not possible to perform a fault attack in this cell because an injected fault will cause the system to go to deadlock. That is, the faults prevent or stop the necessary four phase handshake protocol between each gate, which leads to stalling the communication between dependent downstream gates and prevents any further data processing. Figure 4 shows the transistor level circuit of a PCFB buffer.

The circuit which synthesized with current cell library is venerable to power attacks. The HSPICE simulation of an imbalanced PCFB buffer’s consumed power is shown in Figure 6. The upper curve is the power consumption of PCFB template when all of the input bits are one. The other one is the power consumption of it when all the inputs are zero.

It is clear that the power consumption behavior of the current template depends on the input data. Kulikowski and etc. showed that how one can incorporate a balanced system design in the QDI asynchronous pipelines [2]. The authors also mentioned the possibility of a hybrid fault and power attack to a system. In this kind of attack (DPA-FI) a fault is injected to the system that changes the balanced behavior of the system without affects the functionality of system which in turn would not be detected by traditional voltage level testing and reliability measurement methods. In the next section we will change the traditional PCFB template to make if invulnerable to this hybrid attack.

4. Cell customization and security benefits

We balanced the PCFB buffers by adding redundancy to the unbalanced parts of template -The input validity checking circuit, the output validity checker and the pull-down computation logic(parts 1 to 3 in figure 8 respectively). Figure 8 shows how we
made these balancing in a PCFB Buffer gate. We balanced the PDFB buffer by using two identical NOR gates and a C_Element in input and output validity checker. The C_Element [16] output changes when both of its inputs have the same value and their values are opposite of the C_Element current value. If a fault is injected in the proposed balancing circuits as previously mentioned, the circuit creates deadlock (then activates an alarm signal). Figure 7.a shows the previous method for balancing the power consumption which is demonstrated as the standard NOR gate here. Figure 7.b is our method that uses a C_Element in addition to the previous balancing redundancy. In our method, when the output must be charged to one and when the circuit is fault free, both of the pull-up network branches will charge the inputs of the C_Element so that the output of the C_Element will be charged to one. But if a fault injected to one of the pull-up network branches, the C_Element will not be charged to the new value. In this manner, we will be able to discover the attacker's injected fault in the logic level and avoid any hybrid Fault Analysis-Deferential Power Attack (FI-DPA [2]).

Figure 7. Previous balanced NOR gate [8] (a); Our proposed balanced NOR gate for input validity checker (b)

Figure 8. The Balanced PCFB 1-bit buffer

Figure 9 shows the computational network of balanced PCFB XOR gate. The circuit is completely symmetric with respect to the input signals so it is obvious that the power consumption behavior of the circuit is independent of the input data. The circuit goes to a deadlock state in the case of a fault injects to the template. Here a C_Element helps us to find the intended unbalancing of the circuit. If a fault is injected to the balancing circuit the C_Element gate does not change its state because its inputs are not the same. So, the normal operating cycle of the circuit will not happen and the circuit will go to the deadlock state. The power consumption behavior of the circuit is completely input independent and hence it is resistant to power attacks.

Figure 9. The balanced computation section of a 2-bit PCFB-XOR gate

5. DES implementation and Power optimization

Among various asynchronous synthesis methods, Data Driven Decomposition [19] shows a higher capability to generate high performance and low power systems. Our synthesis tool uses this methodology. In the decomposition phase, the high-level sequential specification of the circuit is broken into a set of communicating modules that are individually synthesized at lower levels. The inter module communications mapped out during this step, consume the bulk of energy by extra circuitry as data must be not only sent, but also validated and acknowledged [19].

Since decomposing forms the general structure of the system as the main synthesis step, it largely affects on the energy of the final circuit.

The Verilog-CSP [14] hardware description language was used to describe the asynchronous Data Encryption Standard (DES) algorithm -56 bit key, 64 bit data-. We optimize the high-level description of the DES crypto-processor utilizing conditional structures to reduce handshaking overheads in the final decomposed circuit which consequently leads to the power reduction. As shown in Figure 10, after decomposition, a conditional variable in the high-level
description is distributed over the broken blocks; all the inputs, outputs and the middle blocks which compute the results between inputs and outputs must handshake with conditional variable block. As mentioned in [18] handshaking is the main source of power consumption for the QDI asynchronous circuit. Therefore a huge optimization in power consumption can be resulted with removing extra handshaking.

Consider the following piece of Verilog-CSP code for DES specification:

```verilog
define compare=0
begin
  body statements;
end
```

To preserve the functionality of the generated circuit, it is required that none of the fine grain processes of the body statement will generate an output value when the condition is not true. One way to achieve this goal is that all these processes receive the condition variable. Consider the if statement of the code, due to the nature of decomposition algorithm, the process which is corresponding to generate the value of condition variable must sent the value to all the processes generated from the decomposition of the body statement.

Being aware of the synchronization mechanism of asynchronous circuits, conditional activation of the body statement can be done by conditional writing on and reading from its input and output ports. So it is necessary to apply condition on the input and output channels of the body statement which eliminates the need of distributing the conditional variable to all of the processes of the body statement so the number of extra handshake communications can be reduced considerably. It leads to effective reduction on power consumption of the circuit.

When we eliminate extra handshaking, all computations inside the conditional block are removed and will be added to a new block which computes the results unconditionally. This optimization method acts as shown in Figure 11.

As shown in Figure 11, some of the extra conditional applications have eliminated from the computation section using the validity check circuitry with the corresponding power overheads.

In order to evaluate the asynchronous design, also a synchronous version of this algorithm was designed. By using Synopsys commercially available tools, the synchronous Verilog code was synthesized. For both implementations TSMC 0.18µm technology was used.

Our approach proved lower power consumption of the asynchronous implementation compared to an existing synchronous one. Furthermore, in comparing the one stage of DES implementation after Optimization and before it, the energy reduces up to %19 (Table 1). Note that in the synchronous case there is no side channel attack protection, and if there was, it would result in a significant power overhead.

| Table 1. The energy consumption of one stage of DES encryption portion which simulated using SPICE |
|---|---|---|
| synchronous | Secure Asynchronous | Low Power/Secure Asynchronous |
| Energy(J) | 54.9 E-13 | 36.3 E-13 | 30.5 E-13 |
We simulate the DES implementations with the proposed cell-library using SPICE. Results show that the power consumption is totally input independent. Figure 12 shows the power simulations for two different inputs.

![Figure 12. Power consumption by Sbox module in secure asynchronous DES with two different inputs](image)

6. Conclusions

This paper presented an asynchronous approach to design and implement a secure and low power DES crypto-chip. At first, some of the library cells of the AsyncTool asynchronous synthesis tool were customized to make power consumption of the cells will become independent of inputs. A self testable template to resolve the faults that make the balance PCFB template imbalanced was presented that makes the DPA/FI attacks to the proposed library cells are not improbable. At last, we present a power optimization method which employs the conditional restructuring in the high-level description of the circuit.

Results show that this new implementation has more resistance to multiple side-channel attacks compared with synchronous solutions. Also this new approach proved lower power consumption of the asynchronous design.

7. References


