FPGA Implementation of DES and Side Channel Attacks

ECE 6095 Hardware Security
University of Connecticut

Jeffrey Urban Jordan Cote

Dr. Tehranipoor

Spring 2010

Abstract

A DES encryption core is implemented on a Xilinx Spartan 3 FPGA with minimal supporting logic to update input data and keys. The host Digilent PCB evaluation board was modified to facilitate a simple power analysis attack. This attack succeeded in identifying DES rounds and exposed differences between power consumption in subsequent encryptions for each round. Additional DES processes and noise were introduced to make an attack more difficult. One implementation succeeded in making the simple power analysis trace have a more consistently random appearance, which should make simple power analysis more difficult. A second succeeded in making the trace have a more consistent appearance, which should make differential power analysis more difficult. A third implementation combined elements of the previous two.

Contents

1 Introduction

FPGAs are a popular platform for cryptoprocessors. Their speed, which comes largely from parallelability, and reconfigurable nature makes them a natural choice. With a parallel architecture, power analysis is usually more difficult since many things can be happening at one time. This decreases the amount of entropy through the power supply side channel. In this paper, we show that simple power analysis is viable for a DES encryption algorithm which uses parallelism.

We also present several methods to counteract SPA on DES. We compare those power traces to that of the unmodified code. The rest of the paper is organized as follows. First, we review the DES algorithm. We then describe the process of implementing it on FPGA. Our experimental setup is described, including modifications, analysis equipment and experimental methods. Finally, results are presented and analyzed.

2 DES Algorithm

Data Encryption Standard (DES) is a symmetric key block cipher. The block size is 64 bits, although the key length is only 56 bits long. The algorithm is structured as a Feistal cipher, which has the characteristic of splitting the input block in half and alternating the purpose of each half between rounds. There are 16 rounds in total, all of which are identical except for their key schedule (which determines what bits of the key are used) and constants. In addition, there is a permutation at the beginning and end of block processing.

In each round, one half of the data is run through a special function whose output is XOR'ed with the other half of the data. This function is designed to provide the acclaimed "confusion and diffusion" via substitution and expansion permutation operations. The expansion operation generates 48 bits from the 32 bit input. A portion of the key (depending on the round) is applied to the 48 bits with an XOR operation. For the substitution eight reducing lookup tables are applied to the portions of input so that 32 bits are produced in the end. These substitutions are non-linear from a functional standpoint. Finally, there is another permutation operation that shuffles the bits.

The input of the next round is such that the half of input that did not go through the "confusion and diffusion" process will do so in the next round. While DES used to be considered the standard, it has been replaced by AES (soon to be replaced itself). It is now considered insecure, and can be broken in less than a day's time. If it is used, it is applied three times. This is called Triple DES.

3 FPGA Implementation

An FPGA DES implementation was needed as the attack target. A suitable VHDL DES core was found on *Opencores.org*. The core is distributed as free software under the GNU LGPL. Standard inputs and outputs are used. Inputs include 64 bit data and keys, DES start enable and a decipher option, clock and reset. Outputs include 64 bit data and a data-ready pulse.

The original plan for implementing the core was to interface the board to communicate with a computer to receive and return values to allow an automated DPA attack. With uncertainty regarding equipment availability and project complexity, the project was refocused on SPA for a more realistic project scope.

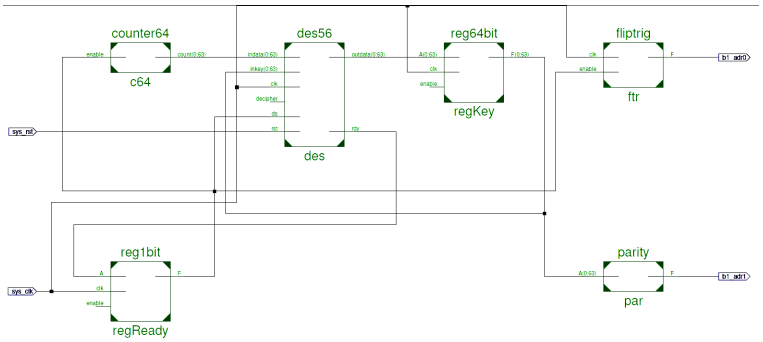


Figure 1: RTL schematic of Simple DES implementation

Although the core was capable of both encryption and decryption, it was outfitted solely for encryption. This was decided because the two operations are very similar.

The LCD on the Spartan 3E starter board was used to verify correct operation of the DES core. This was decided due to complexity of non-attack related coding related to serial communication and ethernet communication. There was also a lack of sample code that was obtainable without special licensing for these purposes. The LCD core was built using the Picoblaze 8-bit virtual processor. Code was available in its assembly language which included some LCD functionality. This code was modified to suit our purposes which included changes to pipe input from the DES core. Encryptions from known values were computed and shown on the LCD. The output was then verified by an existing software implementation[UNS].

4 Implementation for SPA Attack

Because of the nature of the algorithm being that each round needs the input from the last, it is inheriently sequential to some degree. This provided our attack point. However, excess noise in the power trace would make SPA difficult. Optimizing the attack required minimizing chip components and eliminating excess switching during the DES encryption, while ensuring that no integral DES encryption circuits would be eliminated or left dormant by the Xilinx synthesis or mapping process.

A few components were added to support the DES core and exercise its inputs with a wide distribution of values. Settings to prevent logic trimming were unsuccessful unless the logic was eventually connected to an output pin. The additional components performed operations following the end of one DES encryption and before the next so they did not interfere with the DES power trace.

To prevent automatic trimming of components by Xilinx, the core needed to be fully exercised. A 64 bit counter was connected to the DES data input and incremented between each encryption. To minimize noise during power analysis, supporting logic was active only between encryptions. The DES core restarts itself after supporting logic has completed. The DES as implemented starts a 16 cycle encryption every 18 cycles, with the first cycle setting up the encryption and the last cycle preparing values for the next encryption. A 64 bit register, enabled upon data-ready, saves the DES data, which is recycled back to the DES key input to iterate through key values without a direct relationship to the input values from the counter. Changing input and key values not only prevented trimming of core logic, it also would create fluctuations in the power traces based on key differences.

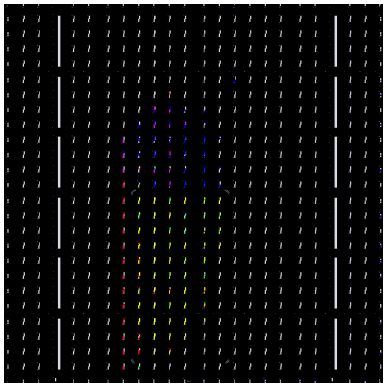


Figure 2: FPGA layout

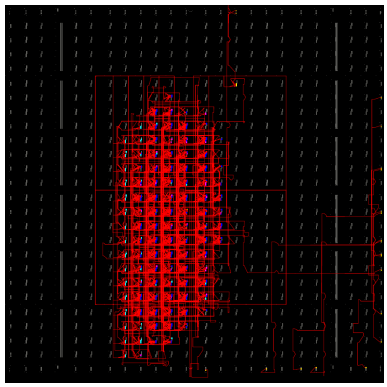


Figure 3: FPGA interconnects

To trigger the test oscilloscope, the data-ready signal was initially routed directly to output pin b1_adr0. The scope could not be adjusted for the $20ns$ ($50MHz$) single pulse to serve as a trigger. The circuit was modified by adding a one bit register than inverts the stored value upon data-ready. This formed a 36 clock cycle ($720ns$) trigger cycle that was recognizable by the scope. Because the trigger alternation is activated by changes in the data-ready output of the DES core, switching of the trigger is an indication of continued operation of the DES core encryption process.

Despite defining settings to prevent trimming of unused logic, Xilinx ISE removed entire components as well as additional internal signals and logic to simplify the circuit unless these elements were actually tied to an output. To preserve the complete DES encryption circuit, a parity check enabled upon dataready was added to the DES data register. The parity value was routed to external pin b1_adr1 to prevent logic trimming. The layout of the FPGA components is shown in Figure 1. Yellow indicates the DES core, red - the 64 bit counter, blue - the parity generator, green - the 64 bit data register.

5 Software and Hardware

- Software:
  - Xilinx ISE 11.1 - Coding of VHDL design files
  - ModelSim XE III 6.4b - Simulation & verification
- Demonstration Unit
  - Digilent Spartan 3E evaluation board
- Test Unit
  - Modified Digilent Spartan 3 evaluation board
  - All 19 decoupling capacitors - removed from V_{int}
  - V_{int} $1.2V$ DC / DC converter disconnected from power and ground
  - V_{int} tapped for direct $1.2V$ DC voltage input (through external resistor)
  - Power supply cord clipped to allow direct $5V$ DC voltage input
- Measurement Tools

– Tektronix TDS 3032 $300MHz$ Digital Phosphor Oscilloscope
– 2 standard (non differential) $100MHz$ voltage probes
– GW GPC-1850D Voltage generator
– Protoboard PB-103
– 1.6Ω resistor

The Tektronix oscilloscope was the fastest available in the UConn senior design lab with $300MHz$ bandwidth. This approaches the bandwidth of scopes used in prior literature at $500MHz$ and compares favorably with the board clock frequency of $50MHz$. All other available scopes were similar models (TDS 3012) with lower bandwidth at $100MHz$. This scope did not offer any recording capabilities beyond the ability to save the display as an image or save the interpolated points from a single trace across the display as 500 sample points.

6 Modifications

To aid power analysis of the Digilent Spartan 3 evaluation board, modifications were made to reduce the level of noise affecting the FPGA from external sources and allow control and more direct access to the internal voltage supply. These modifications follow similar modifications from the literature [SrQP04].

Filtering capacitors were first removed from the voltage network supplying the FPGA internal logic. The FPGA internal voltage source schematics were traced using the Digilent Specifications Manual[Dig09]. A filtering capacitor was identified at the output of the 1.2V DC / DC voltage converter that supplies the internal logic. 18 decoupling capacitors were identified alongside the FPGA on the internal logic (V_{int}) power network from the $1.2V$ source. Each is a surface mount component connecting V_{int} to FPGA ground. All 19 of these capacitors were removed to reduce high frequency filtering of the signal. Bit files were loaded onto the board to confirm trouble-free programming and operation of other programs.

The 5V power source was modified to reduce the introduction of external noise onto the PCB. The wall plug transformer was removed from the power cord to allow direct connection of the $5V$ power input to a $5V$ voltage generator to provide a cleaner power signal.

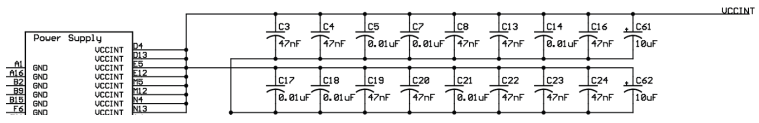


Figure 4: PCB schematic part showing removed capacitors

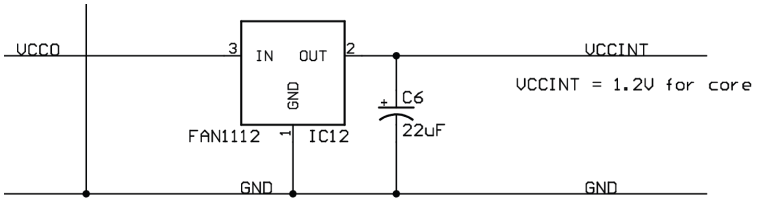


Figure 5: PCB schematic part showing C6 (removed) and IC12 DC converter (disconnected)

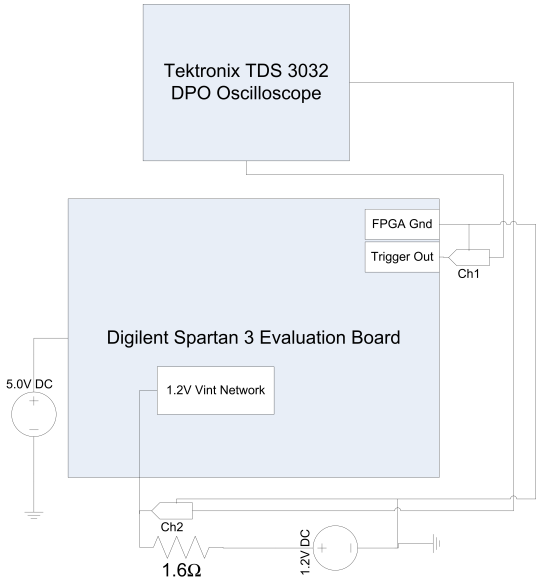


Figure 6: Experimental setup for SPA

Next, the built-in $1.2V$ supply on the PCB was disconnected and replaced with an external $1.2V$ source. The Digilent evaluation board includes transistor based DC / DC converters that step voltage down from $5V$ main supply to $3.3V$, then $2.5V$, then $1.2V$ for V_{int}. After removing the Vint capacitors, and before disconnecting the final converter, the converter's transistor switching was clearly visible on the oscilloscope. This final step down converter from $2.5V$ to $1.2V$ (component IC12) was disconnected from $2.5V$ and gnd, leaving Vint isolated from the other PCB voltage supply networks. An external power supply was then routed through an open through-hole on the V_{int} network.

To aid measurement of fluctuations on the stripped Vint network, a resistor was selected and connected near the board, in series with the $1.2V$ external source. Xilinx power analyzer predicted power consumption on V_{int} of $19.72mW$ at $1.2V$, with $7.43mW$ dynamic power and $12.29mW$ quiescent. Based on this prediction, a 2Ω resistor was specified for an approximate $33mV$ voltage drop across the resistor including $12mV$ swing for logic fluctuations. 1.6Ω was the closest available value and was used. An input voltage range was not specified for V_{int} in the Spartan 3 manual, so the voltage source was set at $1.2V$ to avoid any chance of overvolting the chip and correct operation was confirmed at the reduced voltage.

7 Experimental Setup

In the attack test setup, a $1.6/Omega$ resistor was installed between the $1.2V$ power source from the voltage generator and the internal circuitry of the FPGA. The voltage on the FPGA side of the resistor (at the Vint input) was measured with respect to FPGA ground as an AC signal, filtered of low frequency elements below approximately $100kHz$ (according to scope on-screen prompts). This replicates the signal of a classic power analysis attack, but does not match the classic setup.

To perform a classic power analysis attack, the differential voltage is measured across a resistor between the power supply and internal logic circuitry of the FPGA. This setup was not achieved using the standard probes available in the lab, due to ground loops introduced between the scope and voltage generator. When

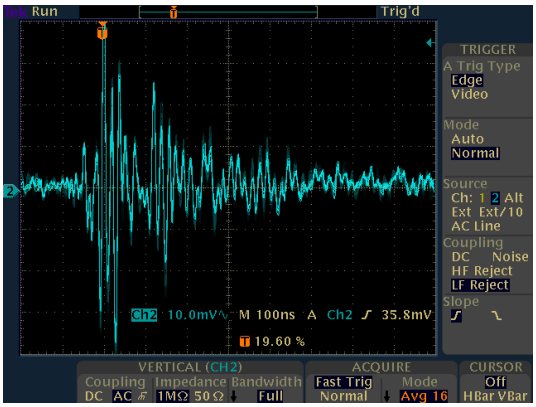


Figure 7: SPA power trace of $200\mu s$ oscillation

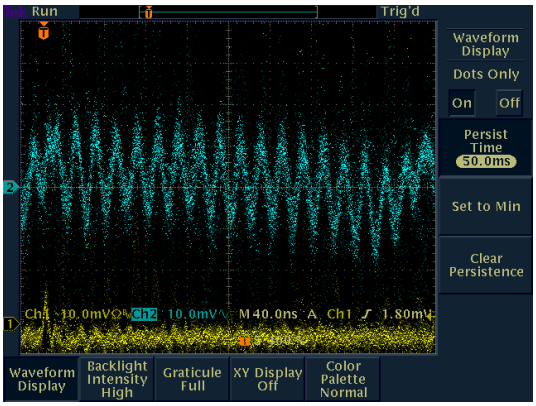


Figure 8: SPA persistance trace of one encryption

the probe ground was connected to the power circuit, the internal logic lost power and reset upon disconnection. An attempt was made to use two probes for a calculated differential value, however triggering on the third probe 'trigger' input was not successful due to different specifications on the input and / or an inability to visualize the input trace. A proper differential measurement across the resistor could be obtained by floating both $5V$ and $1.2V$ power inputs, if the scope can detect the trigger pulse as an AC signal without a solid ground connection. Alternatively, differential probes could be sourced.

8 Simple Power Analysis of DES on FPGA

Before the data-ready trigger was successfully implemented, triggering was attempted from the Vint power trace itself. A large excitation and decaying oscillation was evident and repeated approximately every $200\mu s(Fig.7)$. It is not clear what may be the cause of this oscillation. Bit files from other designs had similar patterns with the same rate of repetition, but each was unique and more complicated designs have messier patterns.

The data-ready trigger signal was successfully used, but did not perform as expected. In DC capture mode, the signal alternated between values with amplitude around $20mV$ - significantly lower than the expected $3.3V$ swing for a board I/O port. The trigger signal carried enough noise that consistent triggering was not possible on the transition itself (in either direction). The voltage overshoot upon transition as detected in AC mode was used for a consistent trigger. It is not clear why the detected signal was so much lower than expected.

With the data-ready alternating trigger successfully recognized, the resulting scope traces of Vint looked somewhat random until the scope was changed to persistence mode, when a repeating pattern became clear, correlated to the trigger repetition. The pattern consisted of 18 $20ns$ pulses with the first two pulses clearly different from the others. These corresponded to the 16 sequential rounds of the DES encryption preceded by two cycles dedicated to setting up the encryption (as in Fig. 8 and 9a). This pattern was compared to patterns from two other bit files whose traces formed distinctly different patterns.

After changing from persistence mode to average-16 mode, the trace was well defined. Areas of inconsistency were identified in the power trace by fluctuations in the shape of the waveform. While lower frequency

noise elements may be responsible for these fluctuations, they may instead represent differences in power consumption dependent on key and input values.

9 Defenses against Simple Power Analysis

Efforts to prevent this type of attack were also implemented. The first attempt was a randomized algorithm that either did a heavy computation on a clock cycle or did not. The randomness was derived from a modulus operation on a persisting variable that changed every clock. This effort had minimal impact on the power trace, however, since the multiplications that were being carried out were just not as power consuming as the combinatorial logic of the DES algorithm.

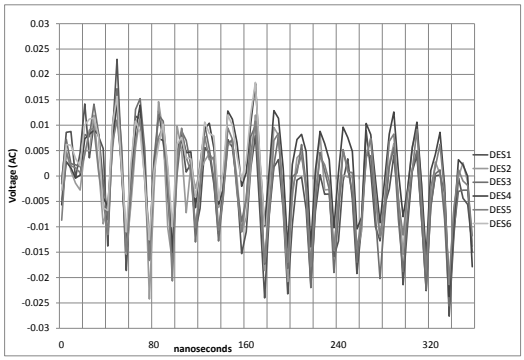
To ensure that enough switching would be done to be noticeable, a separate DES process was run concurrently using the same key and input values. This was done in several ways. One approach was to use an inverted clock for the other DES algorithm. In this case, there would be a DES operation triggered on both clock rise and fall. This indeed helped smooth out the power trace so that the rounds were less visible. There was actually an even more noticeable power difference at the beginning of the DES process, since there was twice as much logic (and power) involved.

Figure 9 shows SPA traces for the Simple DES and for DES with each of the three implemented defense mechanisms. On each graph, six consecutive encryptions using incremented values and different keys are superimposed for comparison. Each trace is composed of two $20ns$ setup cycles followed by the 16 DES rounds of the primary DES core. The patterns in these graphs are based on discrete time domain recordings that are difficult to visualize in real time on the oscilloscope. Updated and persistence views change to quickly to identify individual encryption traces. Views averaged over multiple samples give a more consistent appearance between different mechanisms despite differences in individual traces.

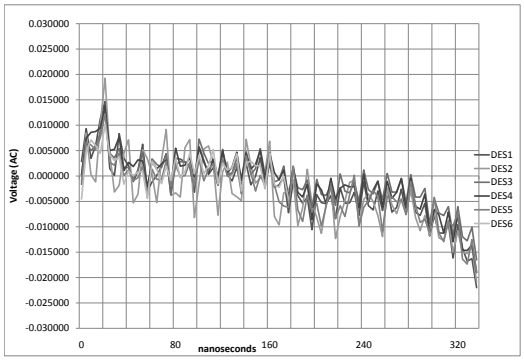
The Simple DES trace (Fig. 9a) has a consistent and clearly identifiable overall pattern with peak height and shape variations that may be useful to determine the encryption key. The extra inverted clock DES trace (Fig. 9b) exhibits a pattern that appears more random and with smaller amplitude fluctuations. This obscures the signal to make SPA more difficult, but the differences may be valuable for a DPA attack. The extra DES with $\frac{1}{3}^{rd}$ clock (Fig. 9c) slightly obscures the setup cycles and exhibits a more consistent appearance and amplitude of each DES round. Since the attacker should not have access to a trigger specific to the primary DES, it will be more difficult to determine the actual DES start cycles. The greater consistency in amplitude and appearance of each round should make a DPA attack more difficult. The extra DES with $\frac{1}{3}^{rd}$ inverted clock (Fig. 9d) exhibits a combination of properties from the two previous mechanisms. It is neither as random as (9b), nor as consistent as (9c), however it may offer a combination of the advantages of the prior two mechanisms.

We then used a divided clock for the second DES algorithm, so that its clock was $\frac{1}{3}^{rd}$ the speed of the main clock. This offset the beginning times of the two DES algorithms and further obfuscated the power trace. A trigger was generated by only the primary DES algorithm under attack. Combining this method with the inverted clock yielded the best results.

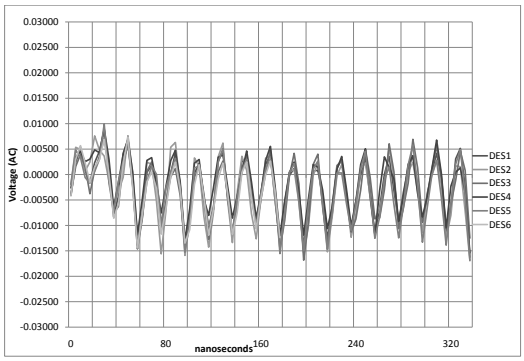
To determine capacitance effect in reducing the signal, $10\mu F$ and $100\mu F$ capacitors were each connected inside of the 1.6Ω resistor between V_{int} and chip ground (through port B1). There was no visible difference in traces. A network tuned to the internal clock frequency may be an effective countermeasure.



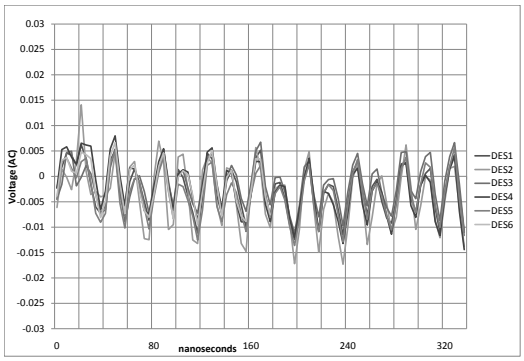
(a) Original DES



(b) Extra DES, inverted clock



(c) Extra DES: $\frac{1}{3}^{rd}$ clock



(d) Extra DES: $\frac{1}{3}^{rd}$ inverted clock

Figure 9: Consecutive DES encryptions superimposed (with varying SPA defenses)

10 Attempted Electromotive Force Analysis of FPGA

Before modifying the Spartan 3 board, a simple EMF attack was attempted, based on a setup in [DMOPV07]. The paper was not clear regarding the details of the test setup beyond those of the scope and loop antenna. In the paper, the scope was rated at $500Mhz$ and the antenna was formed of a simple wire loop around the FPGA package. Our setup was based on that setup, using a $1mm$ diameter solid copper wire formed into an open loop and connected to the $300MHz$ lab scope with one end of the loop attached to the probe and the other to the probe ground.

Using this setup, we were not able to detect any difference between samples taken at the chip and at other locations. Higher amplitude signals were found with this setup than with the probe directly connected to its ground, so the antenna succeeded in picking up some signals from the lab environment. This crude

antenna was not tuned to the circuit.

11 Input / Output Considerations

The assignment specified I/O communications with the board over the JTAG connection. Unfortunately, this was not possible with the components at hand. The Digilent Spartan3 JTAG cable is not compatible with Xilinx ISE, requiring Digilent Adept software for communications[Dig09]. The Spartan 3 board does not support the EPP communication protocol required to send data upstream to the Adept software. The communication options were not available when connecting to the board. As an alternative, RS232 I/O was considered and initially explored before implementing DES on the Spartan 3E board with 16 digit hexadecimal output to the LCD display. I/O connections would aid a DPA attack, but would not be a necessity since the series of values can be preselected and the series of keys calculated.

12 Digital Clock Management Considerations

Use of the Spartan 3 on-chip digital clock managers (DCMs) was considered to generate a slower clock cycle to allow more separation between the power traces of subsequent logic cycles. While the DCMs are on chip, they are powered by a 2.5V source, not Vint which supplies the internal logic (confirm and include specific voltage line names). Difficulties in implementing DCMs prevented their use. Despite their simplicity in implementation, DCM operation was not operational besides a default half-speed clock output. For more realistic conditions, a slower clock was not used in final testing.

References

[Dig09] Digilent, Inc., Pullman, WA. *Adept Application User's Manual*, March 2009.

[Dil04] Inc. Diligent. S3 board schematic, December 2004.

[DMOPV07] E. De Mulder, S. B. Örs, B. Preneel, and I. Verbauwhede. Differential power and electromagnetic attacks on a fpga implementation of elliptic curve cryptosystems. *Comput. Electr. Eng.*, 33(5-6), 2007.

[SrQP04] François-Xavier Standaert, Siddika Berna Örs, Jean-Jacques Quisquater, and Bart Preneel. Power analysis attacks against fpga implementations of the des. In *In Proceedings of Field Programmable Logic and Application*, pages 84–94. Springer-Verlag, 2004.

[UNS] UNSW. Des calculator. http://www.unsw.adfa.edu.au/ lpb/src/DEScalc/DEScalc.html.