Fall 2021

Using a Light-Based Power Source to Defeat Power Analysis Attacks

Remus Valentin Tumac
Southern Methodist University, remus.tumac@gmail.com

USING A LIGHT-BASED POWER SOURCE TO DEFEAT POWER ANALYSIS ATTACKS

Approved by:

Jennifer Dworak
Department of Electrical and Computer Engineering
Thesis Committee Chairperson

Gary Evans
Department of Electrical and Computer Engineering

Scott McWilliams
Department of Electrical and Computer Engineering

Frank Coyle
Department of Computer Science

USING A LIGHT-BASED POWER SOURCE TO DEFEAT POWER ANALYSIS ATTACKS

A Thesis Presented to the Graduate Faculty of the

Bobby B. Lyle School of Engineering

Southern Methodist University

in

Partial Fulfillment of the Requirements

for the degree of

Master of Science

with a

Major in Computer Science

by

Remus Valentin Tumac

B.S., Computer Science, Southern Methodist University

December 18, 2021

ACKNOWLEDGMENTS

First, I would like to express my sincere gratitude to my advisor, Dr. Jennifer Dworak. Her guidance and encouragement throughout this project have been invaluable. I would like to thank Dr. Gary Evans and Scott McWilliams for their assistance with the experiment designs.

I would also like to thank my parents, Romulus and Niculina, and my siblings, Adriana and Alisia, for their support and patience throughout the course of this project.

A special thank you goes to Joshua Whittington-Manning for his constant support, encouragement, and lighting design expertise which proved critical in troubleshooting some of the laser experiments.

Last, and most importantly, all glory to God!

Tumac, Remus Valentin B.S., Computer Science, Southern Methodist University, 2019

Using a Light-Based Power Source to Defeat Power Analysis Attacks

Advisor: Jennifer Dworak

Master of Science conferred December 18, 2021

Thesis completed November 1, 2021

Power analysis attacks exploit the correlation between the information processed by an electronic system and the power consumption of the system. By powering an electronic system with an optical power source, we can prevent meaningful information from being leaked to the power pins and captured in power traces. The relatively constant current draw of the optical power source hides any variability in the power consumption of the target system caused by the logic gates' switching activity of the system as observed at the power pins. This thesis will provide evidence to show that using an optical power source should make it impossible for an attacker to extract meaningful information from the power trace of the monitored system, as measured at the power pins.

TABLE OF CONTENTS

LIST OF FIGURES

Figure Page

LIST OF TABLES

Table Page

This thesis is dedicated to my parents, Romulus and Niculina, who have deeply inspired me through their sacrificial love for my siblings and me.

Chapter 1

Introduction

1.1 Encryption

Cryptography is widely used in order to protect valuable information. Most cryptographic algorithms utilize a secret key in order to encrypt plaintext and to decrypt ciphertext. The purpose of the key is to allow only authorised access to the protected information. When using modern cryptographic algorithms, extracting the plaintext from ciphertext is impossible without knowing the key.

The naive method of obtaining a cryptographic key is a brute force attack. System designers can guard against this attack by increasing the length of the key. The AES-128 encryption standard uses a key length of 128 bits. AES-128 has $2^{128} = 3.4028 \times 10^{38}$ number of possible key combinations. If we wanted to brute force a key of this length, assuming we are able to check 10 billion keys every second, it would take over 10^{21} years to find the key [1].

1.2 Side Channel Analysis

A cryptographic algorithm implemented on a hardware device can leak information through side channels. Side channel analysis (SCA) is the analysis of data leaked by a device on a side channel such as: power, timing, photon emission, or electromagnetic radiation. Kocher was the first to introduce the idea of using the timing between different steps of an encryption algorithm [2], or the power consumed by a hardware implementation of an encryption algorithm [3] in order to reveal additional information about the encryption key. SCA attack methods allow the extraction of the cryptographic key significantly faster when compared to a brute force attack.

Typical cryptanalysis methods use a black box model, while side channel attacks make use of a grey box model. With a black box model, the attacker can only see the plaintext

input and the ciphertext output of the encryption system. The attacker cannot see the internal variables of the system. On the other hand, with a grey box model the attacker can see some of the internal variables and use that towards their advantage [4].

1.3 Exploring Solutions to Power Analysis Attacks

Using a long encryption key and a robust encryption algorithm is not sufficient for ensuring an adequate level of security. When it comes to hardware implementation of an encryption algorithm, system designers must give special attention to potential leakage of information via side channels.

The focus of our research is to explore the use of an optical power source to hide the information leaked by a system through variations in power consumption as observed through a power trace [5]. We will perform power analysis attacks on unprotected systems and systems protected by an optical power source. Finally, we will assess the effectiveness of using an optical power source as a power analysis attack countermeasure.

Chapter 2

Background

2.1 Simple Power Analysis

Simple power analysis (SPA) involves direct interpretation of the distinct characteristics of a power trace. For example, Fig. 2.1 shows the second and third round of a DES encryption operation [3]. SPA could reveal the state of a system at a particular point in time. This information can be extremely valuable to an adversary trying to extract protected information from the system.

2.2 Differential Power Analysis

Differential power analysis (DPA) was first introduced by Kocher [3] and formalized by Messerges [6]. DPA makes use of statistical functions in order to extract information that would have been otherwise overpowered by measurement error or noise in the system. The statistical analysis of power traces is typically tailored to the algorithm being attacked. The use of statistical tools is necessary because the variations in power consumption observed are

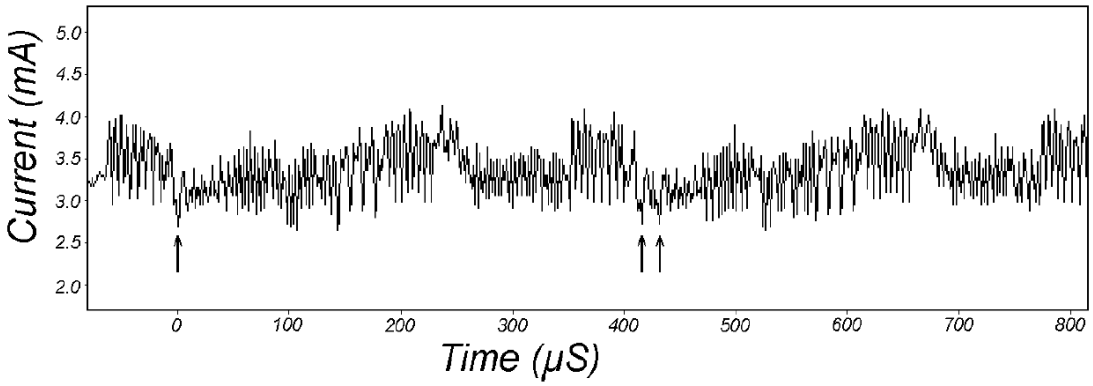

Figure 2.1: SPA power trace showing DES rounds 2 and 3 [3]

relatively small, and they are typically caused by the values manipulated by the algorithm [3].

Since the original paper by Kocher [3], other statistical functions have been proposed that yield better results in practice [7]. Despite correlation power analysis with a leakage model (CPA) [7] being a more effective attack than DPA, the authors of the paper conclude that countermeasures for DPA are just as effective against CPA.

2.3 Countermeasures for Power Analysis Attacks

The goal of any countermeasure is to make the power consumption of the target hardware independent from the information processed by the same hardware. Published research shows two main approaches to preventing power analysis attacks: hiding and masking. The hiding countermeasure works by altering or removing the link between the power consumption and the data being processed. While focused more on protecting cryptographic systems, masking relies on randomization of the intermediate values of a cryptographic algorithm. Masking tries to create a power consumption that is independent of the intermediate values while still executing on hardware with data-dependent power consumption [8].

Multiple masking and hiding countermeasures have been proposed so far. Unfortunately, most of them fail to completely remove the dependency between the information processed and the observed power consumption of the device processing the information. For example, most masking schemes can be attacked through higher-order DPA attacks [8, 9]. Other countermeasures e.g. [10–15], have similar effectiveness against power analysis attacks.

Tiri and Verbauwhede [10] introduced Wave Dynamics Differential Logic (WDDL), which is part of the Dual-rail with Precharge Logic (DPL) family of countermeasures against power analysis attacks. DPL countermeasures aim to balance the power consumption of the system at the logic cell level. One challenge with such approach is balancing the capacitance and resistance of the wires connecting the logic cells [8]. While testing the effectiveness of WDDL, the authors of [10] were able to recover 11 bytes from a 16 byte encryption key. Moreover, [16] showed that WDDL is vulnerable to power analysis attacks when no place and route constraints are used. Other countermeasures in the DPL family have been proposed [17,18], but just as WDDL are susceptible to imbalance in capacitance and resistance of wiring [8], and early propagation of data [19].

Current flattening is another technique that has been proposed as a countermeasure against power analysis attacks. Its goal is to maintain a constant current draw for the target device. Consequently, this countermeasure should remove the dependency between the data and the current consumed by the target device as measured at the power pins. [11] introduces a current flattening countermeasure which could be implemented in the same die as the microcontroller processing the sensitive information. In testing, researchers in [11] showed increased resistance to power analysis attacks but sensitive information was still leaked on the power side channel.

Since the introduction of power analysis attacks, significant advances in protective measures against it have been made. In spite of that, the dependency between the secret information processed by a system and the power consumption of the system has not been completely removed at the power pins. Thus, some information could still leak and compromise the system. Using a light-based power source addresses all of these issues by completely removing the dependency between the power consumption of the secure system as seen at the power pins and the secret information processed by the system. Due to the nature of our proposed countermeasure, an optical power source would be successful in preventing a power analysis attack even in special circumstances created by aging, environmental change, or fault injection attacks.

Chapter 3

Proposed Approach

3.1 Goal of Experiment

The experiment was designed to show that powering a secure system with the use of an optical power source linked with an optical detector removes the dependency between the power consumption of the secure system from the standpoint of the power pins and the information processed by the secure system. This approach was initially proposed in patent application [5], and according to the inventors it should be a highly effective way to protect the secure system against power analysis attacks.

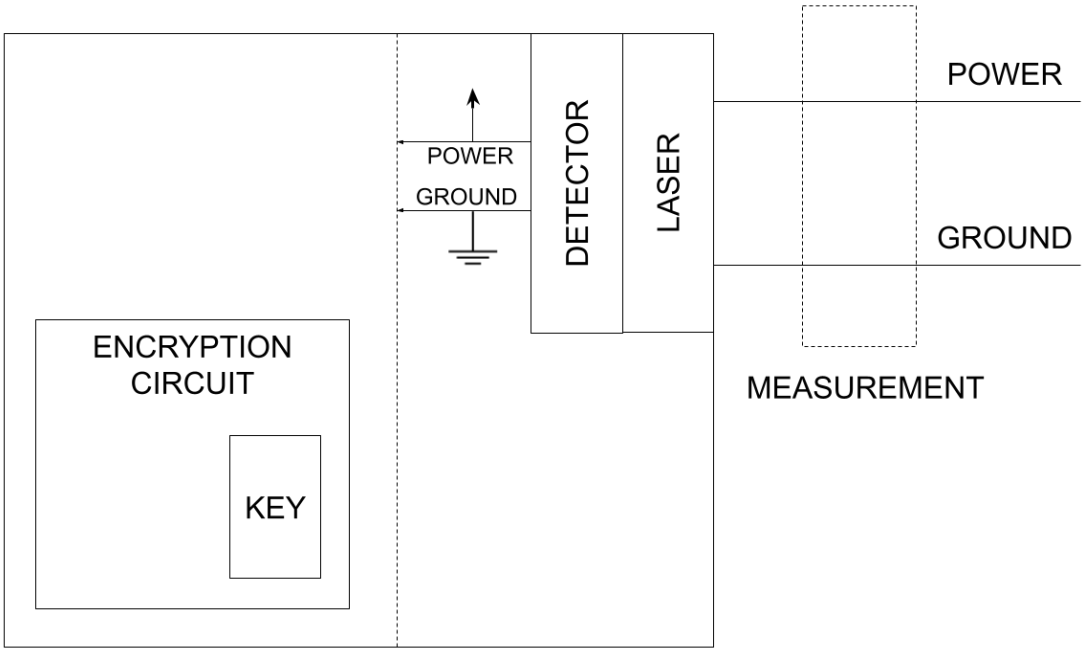

Figure 3.1: Optical source powered circuit [5]

The inventors of [5] describe the approach shown in Fig. 3.1, where an optical power source (laser) is linked to an optical detector. The detector converts the optical energy into electrical energy that powers the secure circuit. Measurements by a device at the main power lines should yield no information about the secret key [5]. This is true if the switching activity caused by the secure circuit while handling the secret information is not correlated with the observed variations in the power consumption of the optical power source. Protecting against power analysis attacks by reducing this correlations is known as hiding [8].

3.2 Proposed Control Experiment with Conventional Power Source

In order to show if the insertion of an optical power source between a conventional power source and the device removes the dependency between the data processed by the system and the observed power consumption of the system, we compared power traces from a system powered by a conventional DC power source and a system powered by an optical power source. In the control experiment, we collected power traces from a system powered by a DC power supply as shown in Fig. 3.2. The power traces were collected by measuring the voltage across a known resistor wired in series with the DC power supply and the device under test (DUT). A programmable device (FPGA board, Arduino) was used as the DUT, which was to be the target of simple and differential power analysis attacks.

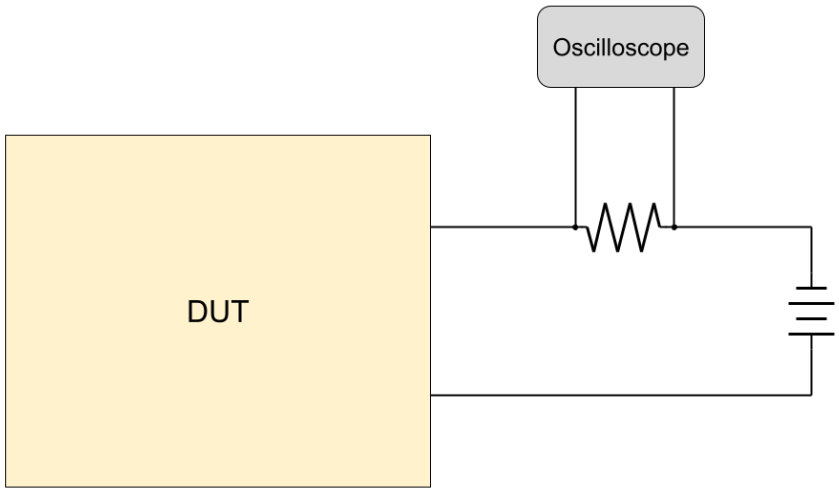

Figure 3.2: Device under test (DUT) powered by DC power supply

The choice of a programmable board was made because it allowed us to easily change the digital logic that was subjected to power analysis attacks. While there are multiple countermeasures that can be implemented in digital logic to make power analysis attacks difficult or impossible to perform, our goal is to show that even without any other countermeasures implemented, using an optical power source is a very effective way to stop power analysis attacks at the power pins.

3.3 Proposed Experiment with Optical Power Source

3.3.1 Using a Laser as a Power Source

To achieve our experimental goal, we replicated the setup outlined in Fig. 3.1, which was proposed in patent [5]. This section builds on top of the control experiments described in Section 3.2. The main difference is the addition of a laser and a detector (Fig. 3.3). The laser will provide optical energy to the detector, which will convert the optical energy into electrical energy. The electrical energy will then be used to power the DUT. Power traces will be collected by measuring the voltage across a known resistor wired in series with the DC power supply and the laser.

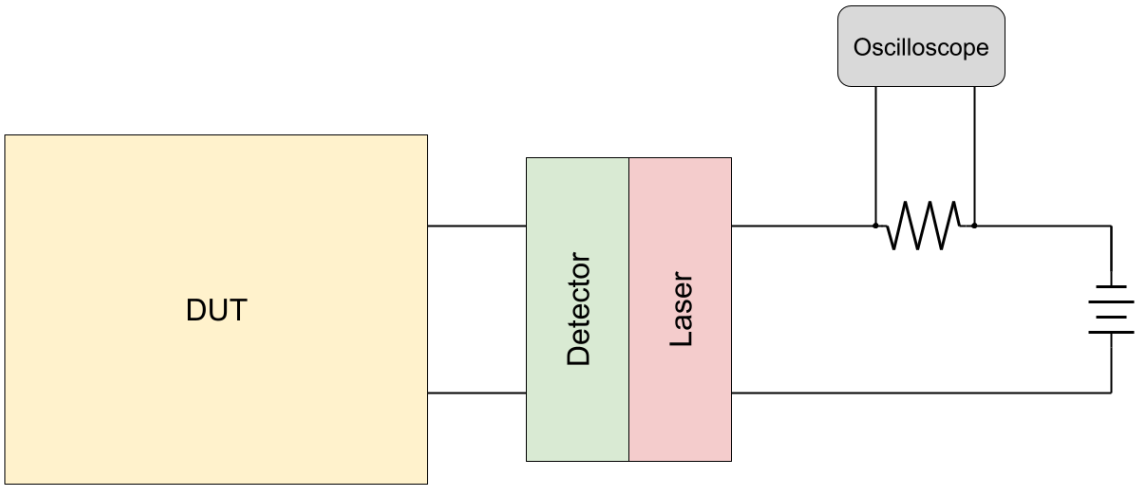

Figure 3.3: DUT powered by an optical power source

The purpose of the DC power supply in this circuit is only to power the laser. We are treating the laser, detector, and DUT as one system that is the target of a power analysis attack. The assumption is that the attacker would not have access to power lines inside this system, and they can only monitor the power going in and out of the system. In a commercial product, the detector could be embedded inside the silicon die of the protected circuit. Thus, an attacker would not be able to gain access to power lines inside the system without physically damaging the protected circuit [5].

3.3.2 Using Sunlight as a Power Source

In this additional experiment, we are replacing the laser as a power source with the optical energy we can capture from external power sources available in the environment. It is not uncommon to see calculators powered by ambient light. Our simple setup for this experiment is shown in Fig. 3.4, and it consists of our IXOLAR SLMD481H08L optical detector wired in series with the Digilent Basys 2 FPGA board. The optical detector presents a surface area of 3,840 mm^2 with a 22% efficiency in converting energy from sunlight to electricity. Assuming a solar irradiance of 1,000 W/m^2, our optical detector should produce 1.1 W of power when in direct sunlight.

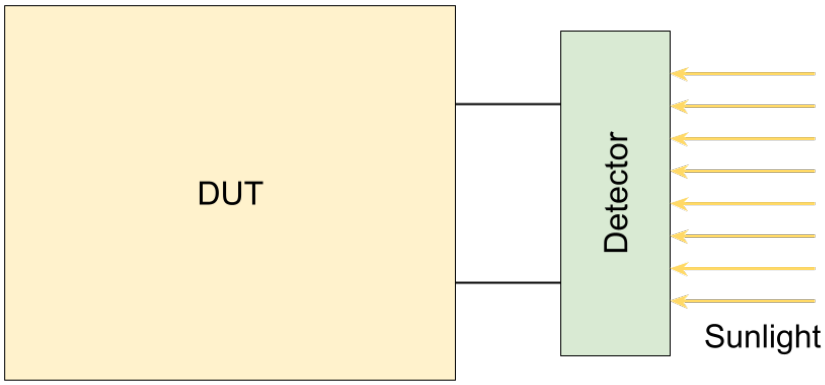

Figure 3.4: DUT powered by light received from the sun

3.4 Collecting Power Traces

Power analysis attacks make use of power traces in order to extract secret information from the device under attack [3]. Depending on the target system and attack strategy, an attacker might need to use one or more traces in order to extract the desired information. Power traces can be collected with any voltage or current measuring device that desirably can sample at a frequency that is at least twice the frequency of the signal being measured.

Oscilloscopes provide an easy way to collect thousands of voltage measurements per second. While being designed to take voltage measurements, there are multiple ways to adapt an oscilloscope to take current measurements. An expensive solution would use a current probe, or a differential probe. As an alternative, we can collect power information by measuring the voltage across a known resistor. With the use of Ohm's Law, we can divide the voltage measurements by the known resistance of the shunt resistor in order to obtain current measurements.

When using an oscilloscope, one must consider the potential of creating a ground loop. The ground clip of the oscilloscope is usually connected to earth ground. If the ground clip is connected to a device under test that is also connected to earth ground, there is the possibility of creating a ground loop. A ground loop can introduce noise into the measurements and cause damage to the equipment [20]. We avoided creating a ground loop by powering the target system with a power supply that uses an isolation transformer. To further reduce the potential of creating a ground loop, we used two battery powered laptops. One laptop was used to control the DUT (only for the experiments using Arduino board). A second laptop was used to download the power traces from the oscilloscope.

Chapter 4

Experiment Setup and Results

4.1 Control Experiment for Simple Power Analysis Attack

4.1.1 Setup

For the Simple Power Analysis control experiment, we used a FPGA board, a DC power supply, and a shunt resistor (Fig. 3.2). The power traces were collected across the shunt resistor with an oscilloscope. It is worth noting that we have set up this stage of the experiment with two different FPGA boards: Digilent Basys 2 representing target device 1 (Fig. 4.1), and Altera MAX 10 representing target device 2 (Fig. 4.2). Table 4.1 lists the exact hardware used with both targets.

For the experiment using target 1 in Fig. 4.1, we have soldered the 1.1 Ω shunt resistor directly onto the FPGA main ground pin. The leads of the 5V DC power supply were connected to the positive pin of the FPGA board and the far end of the shunt resistor. Soldering the shunt resistor to the FPGA board allows us to capture high frequency signals that would have otherwise been lost with a breadboard connection. In the target device 2

Table 4.1: Hardware equipment used in SPA attack control experiment

Hardware Equipment	Brand and Model
Target device 1	Digilent Basys 2
Target device 2	Altera MAX 10 FPGA Development Kit 10M50DAF
Oscilloscope	Keysight InfiniiVision DSO-X 2022A
Voltage probe	Tek P6109
DC power supply	HP E3631A
Shunt resistor for target 1	1.1 Ω
Shunt resistor for target 2	2.1 Ω

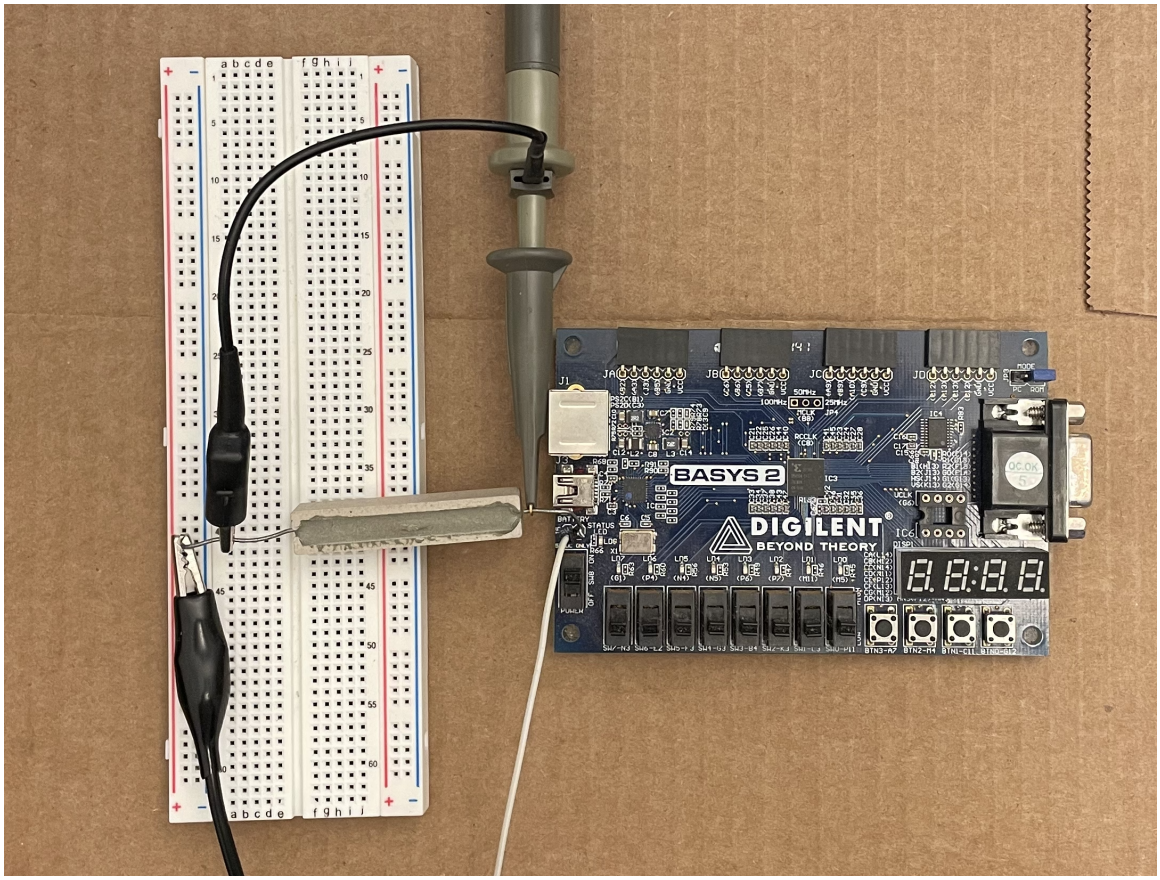

Figure 4.1: SPA control experiment with Digilent Basys 2 FPGA board

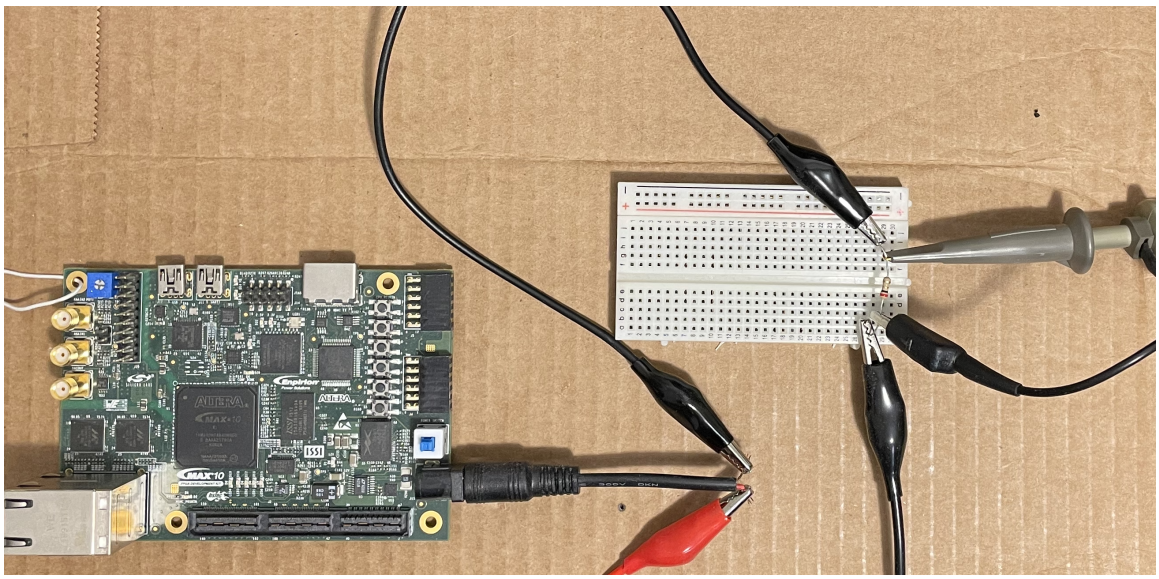

Figure 4.2: SPA control experiment with Altera MAX 10 FPGA board

experiment (Fig. 4.2), we used alligator clips to wire the shunt resistor in series with the FPGA board and the DC power supply. We did not solder the shunt resistor onto target device 2 due to concerns of damaging the device.

The FPGA boards were programmed with a simple 4 bit counter being driven by a clock divider at a 3 Hz rate. The content of the counter register was mapped to the on-board LEDs. We based the counter Verilog implementation on Example 8 found in [21].

4.1.2 Data analysis

Sampling the voltage across the shunt resistor at 5 kSa/s allowed us to extract very detailed information about the state of the LEDs representing the state of the counter. With the use of the power trace and the knowledge that the counter increments from 0 to 15, we were able to determine every state of the counter from the Basys 2 FPGA board power trace in Fig. 4.3. While the signal is noiser, we can see a similar trend in the power trace from the Altera FPGA board in Fig. 4.4. The easiest values to identify are 0 and 15. This is because the power consumption is the lowest when the counter is at 0, and all the LEDs are off. On the other hand, the power consumption peaks when the counter is at 15, and all 4 LEDs are on. If the counter always increments by one, we can determine all the intermediary values between 0 and 15. If the order of the numbers is not sequential, the probability of correctly guessing intermediate values between 0 and 15 is still very high.

Given $x_1 \in S_m$, $x_2 \in S_n$, where $m \neq n$, and m,n represent the number of 1s required for the binary representation of any element in their respective set S, we can easily distinguish between the power trace for value x_1 and the power trace for value x_2. For our 4 bit counter experiment, the sets are $S_0 = \{0\}$, $S_1 = \{1, 2, 4, 8\}$, $S_2 = \{3, 5, 6, 9, 10, 12\}$, $S_3 = \{7, 11, 13, 14\}$, $S_4 = \{15\}$. Assuming power traces for 4-bit unique values $x_1, \ldots, x_{16}$, the probability of correctly associating x with its power trace is determined by the cardinality of the set S to which x belongs. If $x \in S_1$, or $x \in S_3$, the probability is $1/4$. If $x \in S_2$, then the probability is $1/6$. These probabilities can further be increased if the attacker accounts for the fact that every LED consumes a slightly different amount of power due to the random differences in the characteristics of the LEDs introduced during manufacturing. Such differences will likely be hard to observe within one power trace, and thus will likely

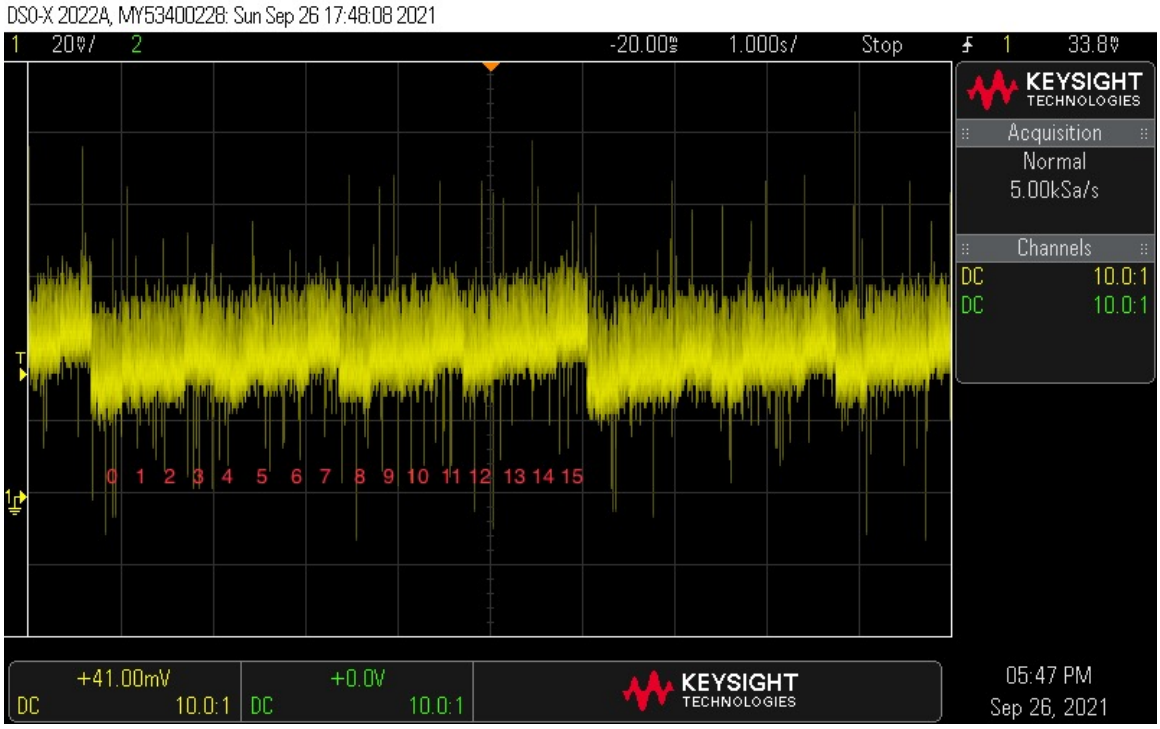

Figure 4.3: SPA power trace from Digilent Basys 2 FPGA board

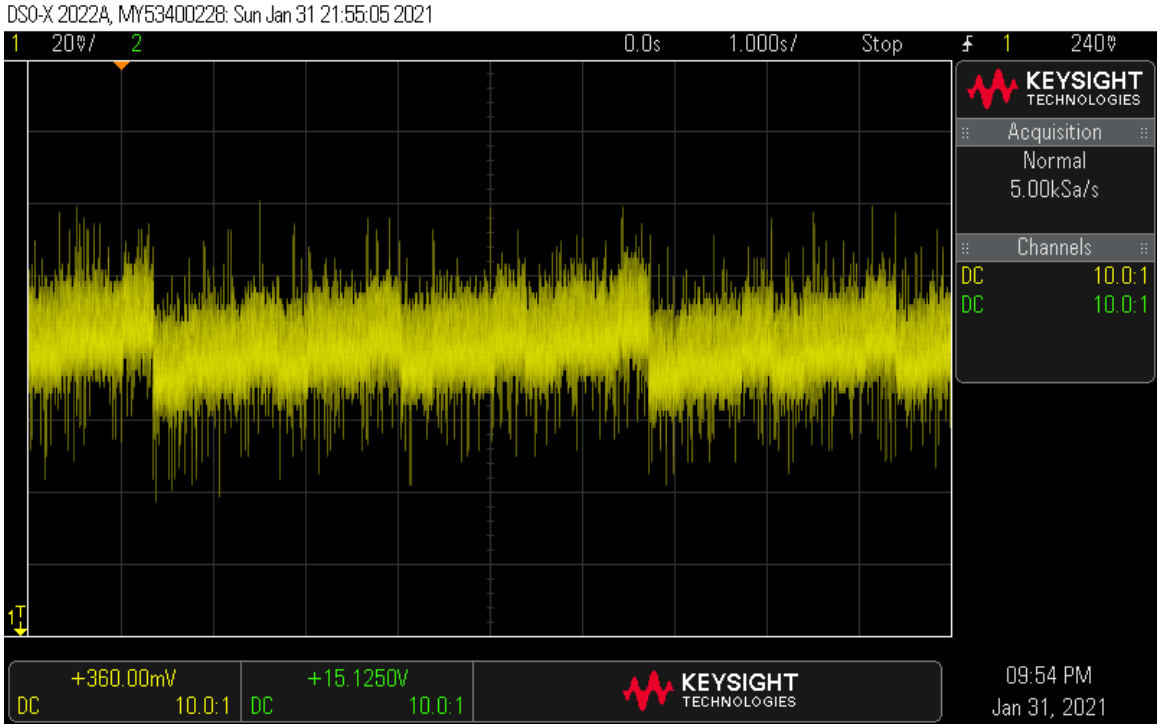

Figure 4.4: SPA power trace from Altera MAX 10 FPGA board

require using a more complex attack than SPA.

In a real attack scenario, the attacker could determine the state of the counter just by looking at the on-board LEDs. Despite that, this experiment can still show the potential effectiveness of using an optical power supply as demonstrated through SPA attack in Sec. 4.3. We have attempted more complex setups with our FPGA boards that do not utilize the on-board LEDs, but we were not able to collect any meaningful power traces. As discussed in [22], the reason for our lack of success could be due to decoupling capacitors, and other modules that run concurrently on the FPGA board that contribute to the overall power consumption.

4.2 Control Experiment for Differential Power Analysis Attack

4.2.1 Setup

The setup of the control experiment for the DPA attack follows the diagram in Fig. 3.2, and requires an Arduino, a DC power supply, and a shunt resistor. The power traces were collected across the shunt resistor with an oscilloscope. Table 4.2 shows a list of the exact hardware used in this experiment.

The Arduino was programmed to perform AES ECB encryption on plaintext sent via a serial connection. The implementation was based on the source code used for the Piece of SCAke challenge at the Riscure 2016 CTF event [23]. Fig. 4.5 shows a picture of our control experiment setup. A 1.1 Ω resistor was soldered directly onto the Arduino ground pin. The leads of the 5V DC power supply were connected to the Vin pin and the far end

Table 4.2: Hardware equipment used in DPA attack control experiment

Hardware Equipment	Brand and Model
Target device	Arduino Nano ATmega238P/CH340
Oscilloscope	Keysight InfiniiVision DSO-X 2022A
Voltage probe	Tek P6109
DC power supply	HP E3631A
Shunt resistor	1.1 Ω

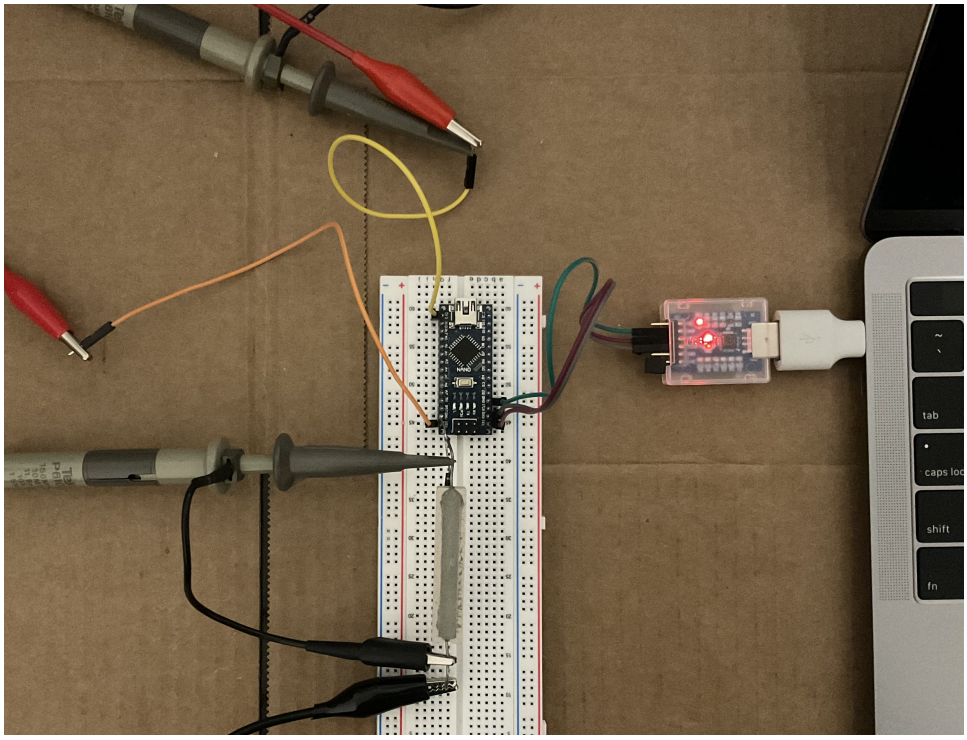

Figure 4.5: DPA control experiment with Arduino Nano

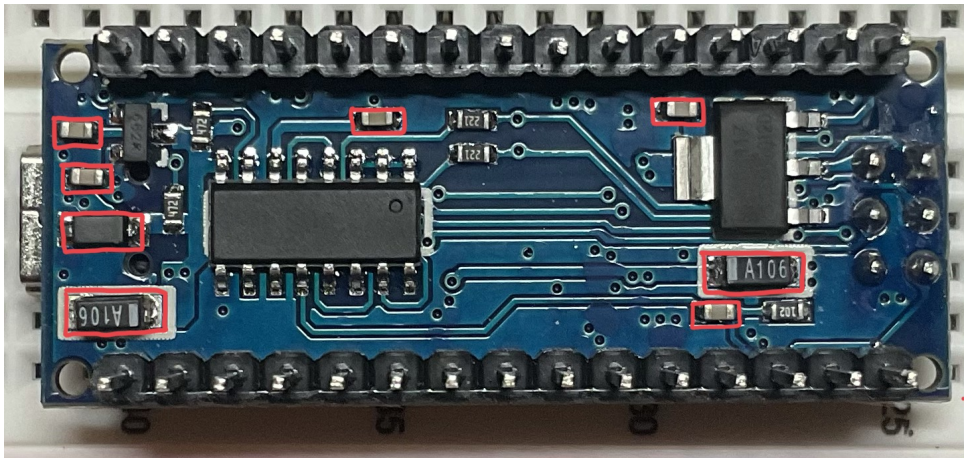

Figure 4.6: Eight decoupling capacitors removed from Arduino Nano (outlined in red)

of the 1.1 Ω resistor. The oscilloscope probe collecting the power traces was sampling the voltage potential between the two ends of the resistor. A second oscilloscope probe was used to capture the trigger on Arduino digital pin 13. The trigger digital signal went high at the beginning of the encryption operation and stayed high throughout the encryption operation. This signal was used to align the power traces in order to give the DPA attack a higher chance of success.

As with the FPGA board, decoupling capacitors on the Arduino board prevented us from being able to see the desired information in the power traces. To be able to successfully execute a DPA attack, we had to remove decoupling capacitors from the back of the Arduino Nano (Fig. 4.6) as suggested in [24–26].

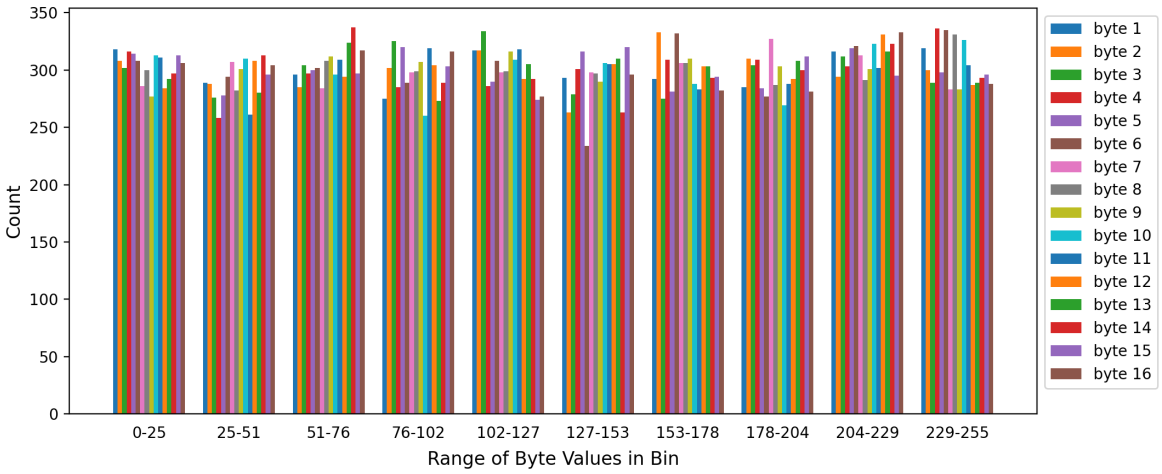

Figure 4.7: Distribution of byte values in the input data set consisting of 3,000 16-byte plaintext strings

To execute the DPA attack, we used 3,000 power traces generated by 3,000 unique plaintext inputs sent from the computer to the Arduino board via a serial connection. The plaintext data set used to generate the power traces is constructed of 3,000 strings, each

16 bytes in size. The value of each byte position within the 16 bytes strings is relatively uniformly distributed between the values of 0 and 255. The histogram in graph Fig. 4.7 splits the 0-255 range of possible values into 10 bins. For each bin, the graph displays the number of occurrences in which the value of the byte falls within the range of values of the bin. If we add all the occurrences of any one byte across all 10 bins, we get a total of 3,000. For example, byte 1 represents the first byte in all 3,000 strings. Thus, adding all occurrences of byte 1 across all bins will give a total sum of 3,000.

A second computer was used to control the oscilloscope and download the power traces in real time. Once all the power traces were collected, we used the Jlsca library [27] to correlate the power traces with the plaintext and ciphertext in order to find the encryption key. The Jlsca library is a toolbox written in Julia that provides the computational part of the DPA attack.

4.2.2 Data analysis

The presented setup allowed us to successfully execute the DPA attack. All 16 bytes of the encryption key ($0x74$, $0x51$, $0x23$, $0x75$, $0xf0$, $0x12$, $0xea$, $0xab$, $0xea$, $0xf6$, $0x95$, $0x5f$, $0x58$, $0x2a$, $0x03$, $0xf7$) were correctly determined within 1,700 traces. This is confirmed by the key rank evolution graph in Fig. 4.8.

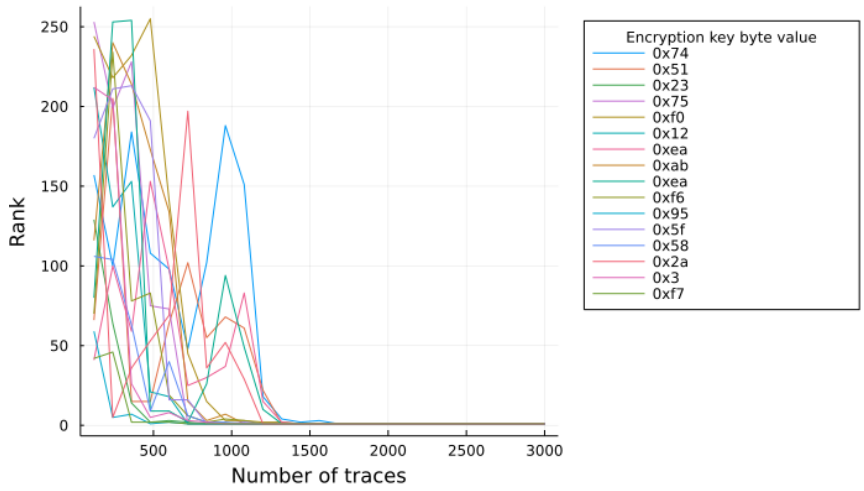

Figure 4.8: Rank evolution of each byte of the encryption key in the DPA control experiment

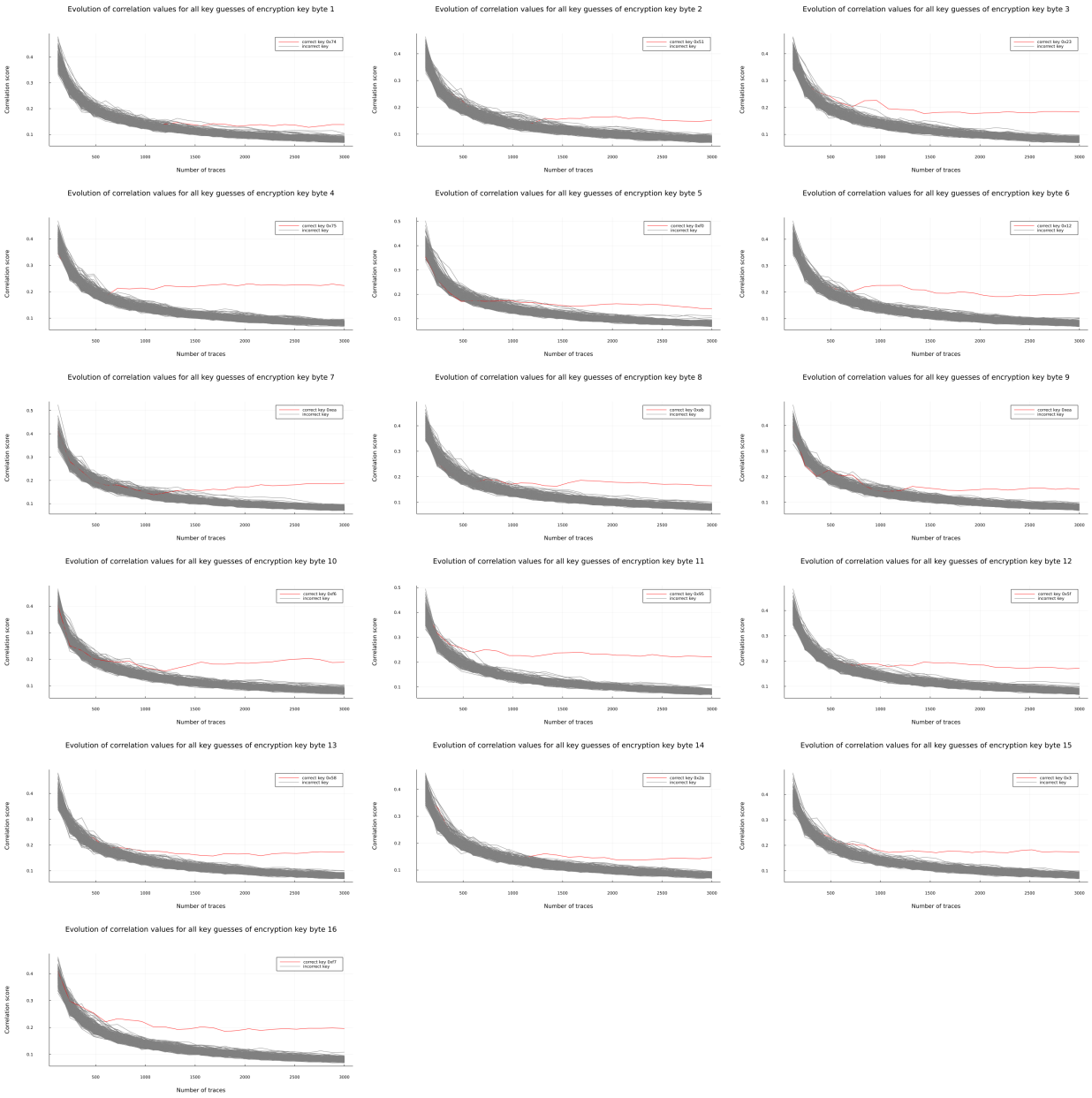

Figure 4.9: Evolution of correlation values for all guesses of the encryption key in the DPA control experiment (correct encryption key guess shown in red)

The key rank evolution graph shows the rank of each byte of the encryption key changing as the CPA algorithm processes more traces. The rank is determined by the correlation coefficient between the modeled power consumption and the actual power consumption.

The guess with the highest correlation score has a rank of 1 and the guess with the lowest correlation score has a rank of 256. Note how in Fig. 4.8, the byte values of the actual encryption key reach a rank of 1 after 1,700 traces.

After processing all traces, the attack algorithm selects the byte values with a rank of 1 as the final key guess. In this experiment, the final key guess is the encryption key. These results are further confirmed by the graphs of the correlation values in Fig. 4.9 which show the correlation values of the correct key guess (shown in red) being well separated from the correlation values of the incorrect key guesses (shown in gray).

4.3 Simple Power Analysis Attack on Laser Powered System

4.3.1 Setup

Our setup for the SPA attack on a laser powered system follows the diagram in Fig. 3.3 and requires a FPGA board, a laser, a detector, a DC power supply, and a shunt resistor. The power trace was collected across the shunt resistor with an oscilloscope. Table 4.3 lists the exact hardware used in this experiment.

Fig. 4.10 displays the setup of the SPA attack on the laser powered FPGA. A 1.1 Ω resistor was soldered directly onto the laser diode ground pin. The leads of the DC power supply were connected to the positive pin of the laser diode and the far end of the 1.1 Ω resistor. The oscilloscope probe collecting the power traces was sampling the voltage

Table 4.3: Hardware equipment used in SPA attack on laser powered system

Hardware Equipment	Brand and Model
Target device	Digilent Basys 2
Oscilloscope	Keysight InfiniiVision DSO-X 2022A
Voltage probe	Tek P6109
DC power supply	HP E3631A
Laser	975nm 8W Fiber Coupled
Optical detector	IXOLAR SLMD481H08L
Optical detector	IXOLAR SM351K09L
Shunt resistor	1.1 Ω

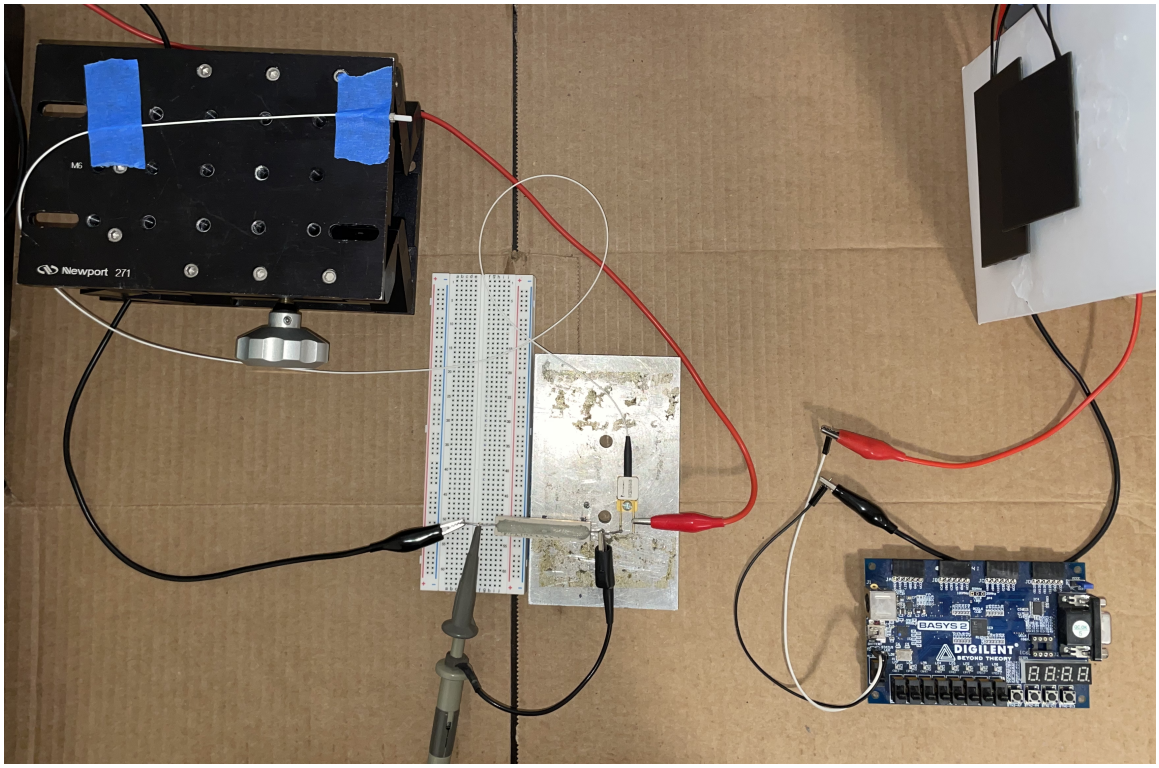

Figure 4.10: Setup of SPA attack on laser powered Basys 2 FPGA board

potential between the two ends of the resistor.

We chose the Basys 2 FPGA board as the target for our SPA attack. In the control experiment in Sec. 4.1, we saw that traces from the Basys 2 FPGA board contained less noise than the traces from the Altera FPGA board. Another determining factor for picking the Basys 2 board was its lower power requirements of only 4V 35mA. On the other hand, the Altera board requires 12V 225mA.

4.3.2 Data analysis

The power trace collected during the SPA attack (Fig. 4.11) shows no information about the counter running on the FPGA board. The laser successfully hid the fluctuations in the power consumption caused by the LEDs being driven by the 4-bit counter. Consequently, we cannot determine the state of the counter from the power trace.

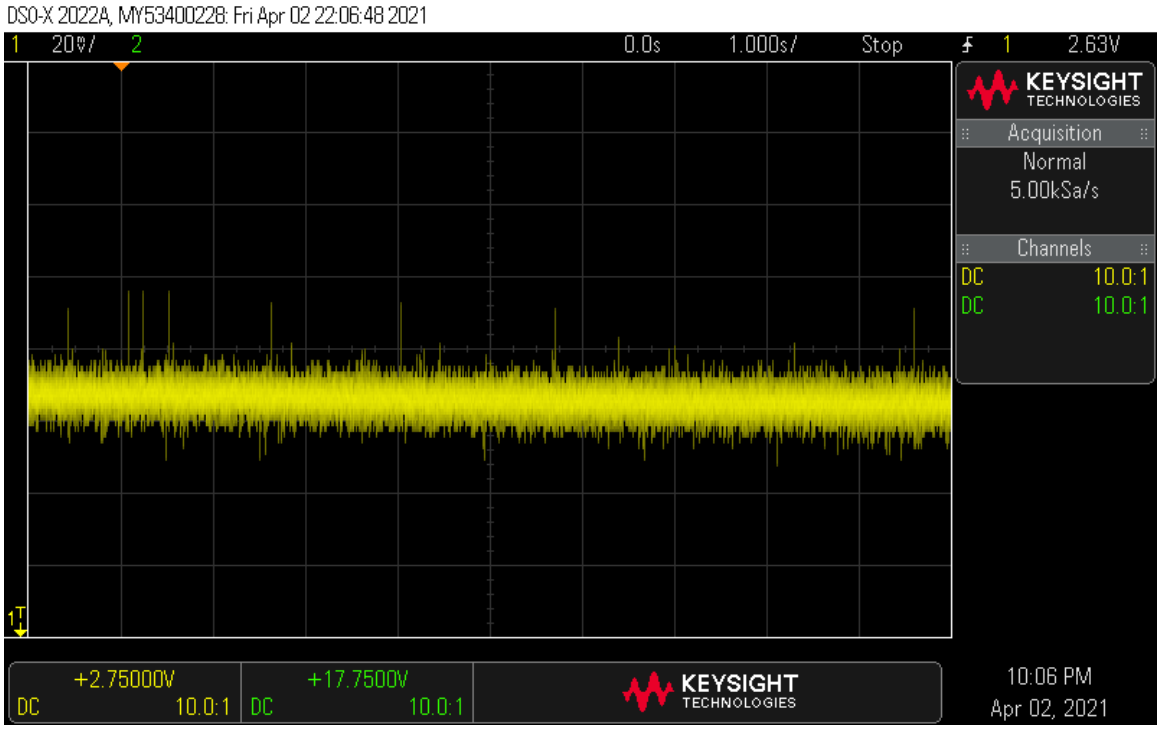

Figure 4.11: SPA attack on Digilent Basys 2 FPGA powered by laser

4.4 Differential Power Analysis Attack on Laser Powered System

4.4.1 Setup

The setup of the DPA attack on a laser powered system follows Fig. 3.3 and requires an Arduino board, a laser, a detector, a DC power supply, and a shunt resistor. The power traces were collected across the shunt resistor with an oscilloscope. Table 4.4 shows a list of the exact hardware used in this experiment.

Fig. 4.12 displays the setup of the DPA attack on the laser powered Arduino. A 1.1 Ω resistor was soldered directly onto the laser diode ground pin. The leads of the DC power supply were connected to the positive pin of the laser diode and the far end of the 1.1 Ω resistor. The oscilloscope probe collecting the power traces was sampling the voltage potential between the two ends of the resistor. A second oscilloscope probe was used to capture the trigger on Arduino digital pin 13.

Table 4.4: Hardware equipment used in DPA attack laser powered system

Hardware Equipment	Brand and Model
Target device	Arduino Nano ATmega238P/CH340
Oscilloscope	Keysight InfiniiVision DSO-X 2022A
Voltage probe	Tek P6109
DC power supply	HP E3631A
Laser	975nm 8W Fiber Coupled
Optical detector	IXOLAR SLMD481H08L
Shunt resistor	1.1 Ω

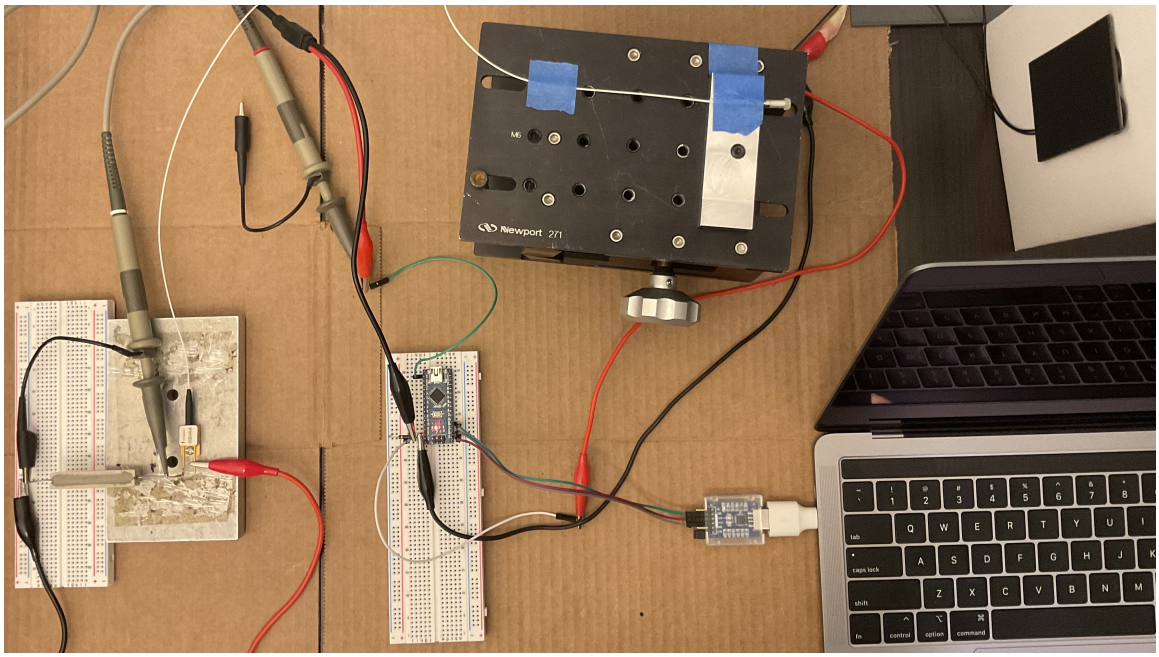

Figure 4.12: Setup of DPA attack on laser powered Arduino board

4.4.2 Data analysis

We collected 10,000 traces capturing the power information during the encryption of 10,000 unique plaintext inputs. The plaintext data set used to generate the power traces is constructed of 10,000 strings, each 16 bytes in size. The distribution of the byte values across all 10,000 samples is shown in Fig. 4.13.

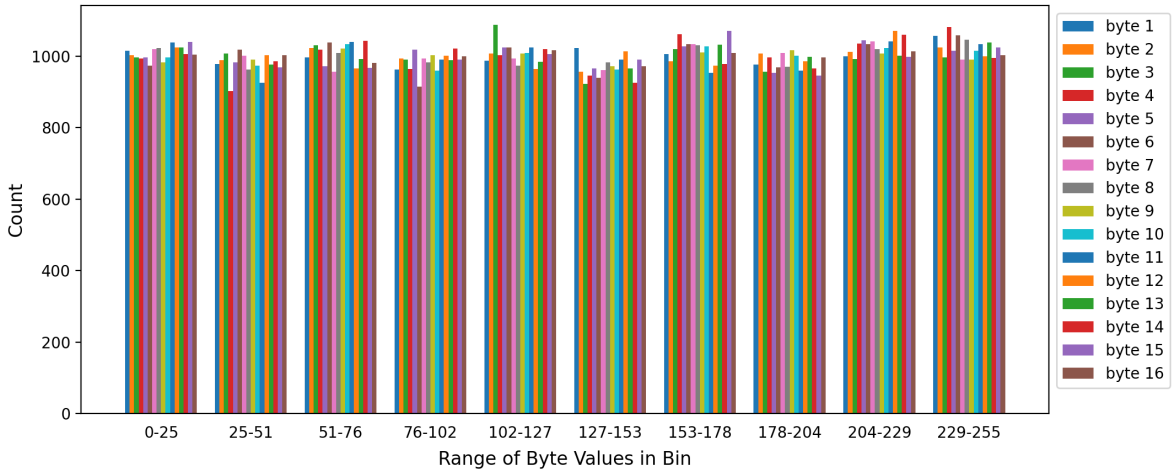

Figure 4.13: Distribution of byte values in 10,000 plaintext strings that form the plaintext input set

During this attack, we were not able to recover any of the 16 bytes of the encryption key. The key rank evolution graph in Fig. 4.14 shows the rank of the encryption key bytes not converging down to rank 1 even after 10,000 traces. In the control experiment, all the key bytes were found within 1,700 traces. The graphs of the correlation values in Fig. 4.15 display the correlation values of the correct encryption key guess (shown in red) not separating from the correlation values of the incorrect key guesses (shown in gray). We can conclude that the laser was successful in decoupling the power consumption measured at the power pins of the target system from the data processed by the target system for this DPA attack.

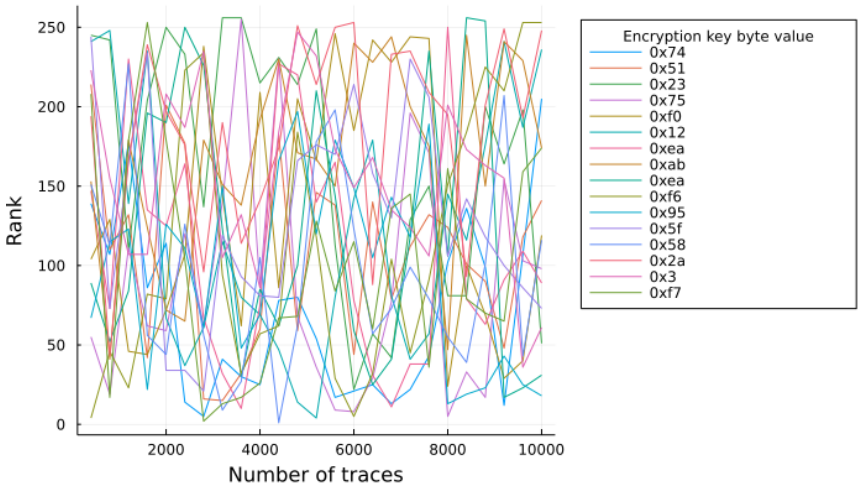

Figure 4.14: Rank evolution of each byte of the encryption key in the DPA attack on the laser powered system

4.5 Power Analysis Attack on Sunlight Powered System

We were also able to power the Basys 2 board with power captured from sunlight as shown in Fig. 3.4. The system was designed specifically to not allow the collection of power traces measuring the variation in power consumption of the system. Because this method of protection is successful in stopping attackers from collecting power traces, it is also successful in preventing power analysis attacks.

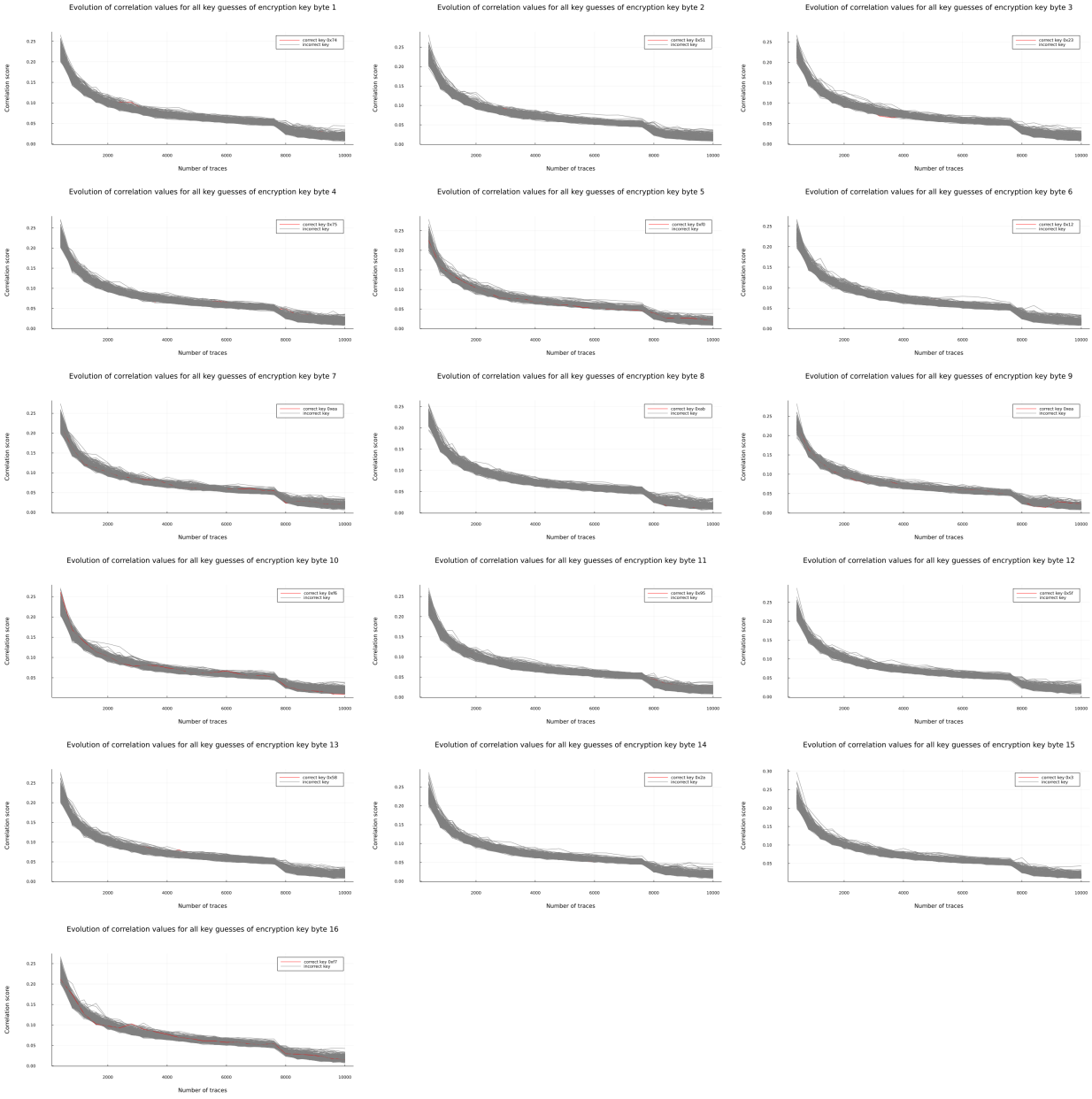

Figure 4.15: Evolution of correlation values for all guesses of the encryption key in the DPA attack on the laser powered system (correct encryption key guess shown in red)

Chapter 5

Conclusion and Future Work

Using a light-based power source is a very effective method for creating a system with data-independent power consumption at the power pins. We were able to show the effectiveness of using a laser power source as a countermeasure against SPA and DPA attacks. Using a laser power source prevented us from identifying the state of the LEDs in the SPA attack. In the case of the DPA attack, it prevented us from finding any of the encryption key bytes even after 10,000 traces.

The effectiveness of this method comes at the price of increased power consumption. Further research can focus on increasing the power efficiency of the system. Improvements can also be made on reducing the size of the laser/detector system, and embedding the detector within the chip die for additional security. Appropriate protection from EM side channel attacks will also need to be developed.

BIBLIOGRAPHY

[1] C. O'Flynn. Introduction to Side-Channel Power Analysis (SCA, DPA). YouTube. [Online]. Available: https://youtu.be/OlX-p4AGhWs 1

[2] P. C. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," in *Advances in Cryptology — CRYPTO '96*, N. Koblitz, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996, pp. 104–113. 1

[3] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," in *Advances in Cryptology — CRYPTO' 99*, M. Wiener, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 388–397. 1, 3, 4, 10

[4] A. C. Kunming, "Comparison of side channel analysis measurement setups," Master's thesis, Eindhoven University of Technology, Aug. 2015. 2

[5] J. L. Dworak, G. A. Evans, P. Gui, and S. McWilliams, "Powering an Electronic System with an Optical Source to Defeat Power Analysis Attacks," U.S. Patent Application 20 200 136 346, April 30, 2020. 2, 6, 7, 8, 9

[6] T. Messerges, E. Dabbish, and R. Sloan, "Investigations of power analysis attacks on smartcards," *USENIX Workshop on Smartcard Technology*, 1999. 3

[7] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *Cryptographic Hardware and Embedded Systems - CHES 2004*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 16–29. 4

[8] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. Boston, MA: Springer, 2007. 4, 7

[9] S. D. Putra, A. S. Ahmad, S. Sutikno, and Y. Kurniawan, "Attacking aes-masking encryption device with correlation power analysis," *International Journal of Communication Networks and Information Security*, vol. 10, no. 2, pp. 397–402, 2018. 4

[10] K. Tiri and I. Verbauwhede, "A digital design flow for secure integrated circuits," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 25, no. 7, pp. 1197–1208, 2006. 4

[11] R. Muresan and S. Gregori, "Protection circuit against differential power analysis attacks for smart cards," *IEEE Transactions on Computers*, vol. 57, no. 11, pp. 1540–1549, 2008. 4, 5

[12] W. Yu and S. Köse, "Charge-withheld converter-reshuffling: A countermeasure against power analysis attacks," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 63, no. 5, pp. 438–442, 2016. 4

[13] W. Yu, O. A. Uzun, and S. Köse, "Leveraging on-chip voltage regulators as a countermeasure against side-channel attacks," in *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, 2015, pp. 1–6. 4

[14] W.-G. Ho, N. K. Z. Lwin, N. A. Kyaw, J.-S. Ng, J. Chen, K.-S. Chong, B.-H. Gwee, and J. S. Chang, "A dpa-resistant asynchronous-logic noc router with dual-supply-voltage-scaling for multicore cryptographic applications," in *2020 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2020, pp. 1–5. 4

[15] K. Baddam and M. Zwolinski, "Evaluation of dynamic voltage and frequency scaling as a differential power analysis countermeasure," in *20th International Conference on VLSI Design held jointly with 6th International Conference on Embedded Systems (VLSID'07)*, 2007, pp. 854–862. 4

[16] L. Sauvage, S. Guilley, J.-L. Danger, Y. Mathieu, and M. Nassar, "Successful attack on an fpga-based wddl des cryptoprocessor without place and route constraints," in *2009 Design, Automation Test in Europe Conference Exhibition*, 2009, pp. 640–645. 4

[17] S. Mane, M. Taha, and P. Schaumont, "Efficient and side-channel-secure block cipher implementation with custom instructions on fpga," in *22nd International Conference on Field Programmable Logic and Applications (FPL)*, 2012, pp. 20–25. 4

[18] V. Lomné, T. Ordas, P. Maurine, L. Torres, M. Robert, R. Soares, and N. Calazans, "Triple rail logic robustness against dpa," in *2008 International Conference on Reconfigurable Computing and FPGAs*, 2008, pp. 415–420. 4

[19] V. Sundaresan, S. Rammohan, and R. Vemuri, "Defense against side-channel power analysis attacks on microelectronic systems," in *2008 IEEE National Aerospace and Electronics Conference*, 2008, pp. 144–150. 4

[20] T. Reyes, "How to measure current with an oscilloscope," Feb 28, 2019. [Online]. Available: https://github.com/saleae/gitbook-articles/blob/master/oscilloscopes/how-to-measure-current-with-an-oscilloscope.md 10

[21] R. E. Haskell and D. M. Hanna, *Introduction to Digital Design Using Digilent FPGA Boards*. Rochester Hills, MI: LBE Books, 2009. 13

[22] S. Sun, Z. Yan, J. Zambreno, and S. Sun, "Demonstrable differential power analysis attacks on real-world fpga-based embedded systems," *Integrated Computer Aided Engineering*, vol. 16, no. 2, pp. 119–130, 2009. 15

[23] "Rhme-2016," https://github.com/Riscure/Rhme-2016, Riscure, 2016. 15

[24] N. Oberli, "Rhme2 writeup," https://www.balda.ch/posts/2017/Mar/01/rhme2-writeup, 2017. 17

[25] "Sca 100 - piece of scake,"
https://github.com/gijsh/rhme2_writeups/blob/master/sca/README.md,
HydraBus, 2017. 17

[26] "Rsa power analysis side-channel attack - rhme2,"
https://www.youtube.com/watch?v=bFfyROX7V0s&feature=youtu.be, LiveOverflow,
2017. 17

[27] I. Kizhvatov and C. Breunesse, "Rhme2 piece of scake challenge,"
https://github.com/ikizhvatov/jlsca-tutorials/blob/master/rhme2-pieceofscake.ipynb,
2020. 18