Embedded systems are application specific computers made to perform specific functionalities and are used in nearly every aspect of our lives. They are responsible for a wide variety of applications, from automatic braking in a car to withdrawing money from an ATM. These systems are normally small devices with limited processing power, usually just enough to perform the functions required of it. Because of this type of design, embedded systems are often limited in the amount of security they can provide. They normally employ encryption algorithms to secure data being processed on them but these encryption algorithms need to be as lightweight as possible, and sometimes this creates a security vulnerability.

These encryption algorithms are used to mask the data being processed inside the device. In certain applications of embedded systems, medical devices for example, the information being processed by the device may be sensitive and could be targeted by an outside attacker. Encryption algorithms, such as Advanced Encryption Standard (AES), have been shown to be resistant to cryptanalysis and therefore are mathematically secure for encrypting data. The problem when working with embedded systems is that an attacker can perform what is called a side channel attack to get around these encryption algorithms.

Side channel attacks target the hardware implementation of the encryption algorithm rather than the mathematical properties of the algorithm. These attacks target the electrical characteristics of the device and can infer certain properties of the device’s current state and the data being processed. One type of side channel attack is power analysis. Different amounts of power is consumed depending on if the bit value being processed is a 1 or a 0. This means the total power being consumed by a device is related to the data being processed by it. Using this fact, attackers have the ability to capture numerous power traces, perform statistical analysis on them, and decipher specific bit values of the data being processed by the device. If this type of attack is done when the device is running an encryption algorithm, the attacker has the ability to decipher bit values of the encryption key used to encrypt the data. If the attacker can extract all the bits of the key, then they obtain the ability to decrypt all the data being encrypted by the device.

My research was aimed at defending against these side channel attacks. More specifically, I be focused on implementing the AES encryption algorithm in a way that is resistant to a side channel power analysis attack. My hypothesis was, if each gate in the design consumes a constant power consumption for every evaluation, the device as a whole will have a constant power consumption independent of the data being processed. To examine this hypothesis I worked with the idea of Wave Dynamic Differential Logic (WDDL). This type of logic adds a complement gate to every true gate in the design. With this type of design, when the true gate outputs a value, the complement gate will always output the opposite value. Another aspect of WDDL I be implemented was a precharge phase. This precharge phase initializes the outputs of every gate in the design to 0. Therefore, when these gates are being evaluated, they will all be starting with the same initial value as their output. This will ensure that, between the true gate and its complement, there is only one transition of 0 to 1 regardless of the values being evaluated. If applied to every gate in the design, the result will be a constant power consumption for the device and will in turn make the implementation resistant to power analysis [1].

My modified AES core was implemented on a Field Programmable Gate Array (FPGA). A FPGA is a programmable device used to mimic the functionality of an integrated circuit (IC). It implements programmable hardware, which is done by using lookup tables (LUTs). These tables take in specific inputs and depending on how they are programmed, produce specific outputs. The ability for a designer to program the hardware on an FPGA makes it much more flexible than an IC and ideal for use in embedded systems.

To quantify the security of an AES core, I used the ChipWhisperer platform to conduct power analysis attacks on it. The ChipWhisperer platform allows a user to easily attack an encryption design programmed onto an FPGA. The ChipWhisperer software program collects power traces and then analyzes them to extract the keys of the encryption algorithm [2]. The metric I used to compare the security of different AES core designs is the average number of power traces needed to uncover the encryption key. Also I wanted to examine the impact of area these designs when implemented. To quantify this I recorded the number of LUTs in each design.

The results of my research showed the WDDL defense was effective in increasing the number of power traces needed to break the AES algorithm. When implementing a fully WDDL protected AES core, when compared to the baseline AES with no added defense, there was a 4538% increase in security. The downside of this is a 806% increase in area and a decrease in the clock rate by 50%. These results show the effectiveness of this design in terms of security but also highlights the issue of implementing this type of protection on space limited devices such as many embedded systems.

Section II gives background information about encryption algorithms, power analysis attacks, and several defences against theses attacks. Section III goes in depth on the research methods used throughout this year. Section IV displays the results of my research. The paper concludes with Section V.