This year my research was aimed at improving the security of an AES-128 design when defending against a CPA attack. To do this my approach was to evaluation the protection WDDL provides to an AES core which is being attacked. Data was collected for protecting different stages of the algorithm.

A fully protected AES core using WDDL with a precharge phase took on average 70,440 power traces to uncover the encryption key. This is a 46x increase in security when compared to the basic AES core which took 1526 power traces to break. The down side of implementing this type of protection is a steep increase in area. The fully protected AES core used 18,618 LUTs and when compared to the basic AES design, which had 2055 LUTs, this is a 9x increase in area.

This increase in area highlights one of the main issues with security in embedded systems. Although there are some defenses that can be implemented that defend against side channel attacks, the expense of area is often too much for the device. As stated earlier, these embedded systems are usually application specific and made as small and efficient as possible. This means an increase in size, like the one witnessed in the data, would mean an increase in size of the device which is not always an option.