Title:	**AES Asynchronous Hardware Implementation Analysis**
Company:	**Qualcomm**
Location:	**Cork, Ireland**
How to apply:	Email aahogan@qti.qualcomm.com

Project Overview:

The **Advanced Encryption Standard (AES**) is a widely used technique for encryption of electronic data. AES has been an established standard from the U.S. National Institute of Standards and Technology (NIST) since 2001.

Many methods can be used to implement AES including specialized, CPU instruction sets and hardware accelerators. Hardware accelerators can provide significant performance benefits in terms of speed due to their highly specialized implementation. However, these implementations can also have security vulnerabilities to attack via (for example) side channel analysis. More recently, asynchronous design techniques have shown promise in being robust to many power analysis attacks as these circuits are not reliant on a core clock.

The successful applicant will design and compare AES accelerator hardware in Verilog using (1) the traditional synchronous logic approach and (2) the newer asynchronous logic approach. The student will work to complete the following:

- Design of AES using (1) synchronous and (2) asynchronous design techniques
- Detailed technical comparison of (1) and (2) focusing on:
    - Performance (data throughput per clock)
    - Area (gate count)
    - Power consumption
    - Security resilience against side channel analysis
    - Security resilience against glitching attacks