Postgraduate Studentships Queen's Doctoral Training Programme on Secure Connected Intelligent Design and Manufacturing

School of Electronics, Electrical Engineering and Computer Science

PhD Studentship 2020/21

Proposed Project Title: DTP: Hardware-based authentication for Industrial IoT

Principal Supervisor:
Prof. Maire O'Neill
Dr. Chongyan Gu
Prof. Paul Maropoulos

Contact Details:
QUB Address: ECIT, Queen's Road, Belfast, BT3 9DT
Tele No: 028 9097 1722
E-Mail: m.oneill@ecit.qub.ac.uk; c.gu@qub.ac.uk

Research Area
Hardware security

Proposal open to other School (indicate area of Interest)

Mechanical Engineering, Maths & Physics

Degree linked to ELE (delete as appropriate)

This project is part of the Queen's Doctoral Training Programme in Secure Connected Intelligent Design and Manufacturing. Many of today's industrial approaches require transformative changes to ensure long term societal, economic and environmental resilience and sustainability. PhD projects in this programme explore the potential of emerging digital technologies, such as artificial intelligence, robotics, and the Internet of Things, to transform the way we design, manufacture and operate products and services.

The programme offers a bespoke research and training programme that aims to develop students into cross-disciplinary, industry-conscious thinkers and leaders who will influence the roadmaps of future advanced manufacturing technologies and their applications. They will have a balanced understanding of ICT (security, communications and data analytics) in the context of their application to Advanced Manufacturing and High Value Design.

Project Description:

The Internet of Things (IoT), enabling smart devices and machines widely and intelligently connected, has led to the development of smart factories. The development of Industry 4.0 reduces production downtime, optimizes manufacturing system efficiency and improves product design. However, the move to industrial IoT devices and machine-to-machine communication poses serious security and privacy issues as there is not direct control over the connected devices. This opens up new attack vectors for hackers to exploit including the threat of malicious or tampered devices. Attacks have already been demonstrated against network-connected light bulbs [1], automation devices [2] and smart car systems [3]. The globalisation of the IIoT device manufacturing process had led to a significant increase in the potential for malicious access, modification and counterfeiting of devices. It is crucial for innovative manufacturing systems to be securely designed and built.

Silicon physical unclonable functions (PUFs), which exploit manufacturing variations of silicon chips, offer a promising mechanism that can be used in many security, protection and digital rights management applications. Such a primitive has a number of desirable properties from a security perspective, such as the ability to provide a low-cost unique identifier for an integrated circuit (IC) or to provide a variability aware circuit that returns a device specific response to an input challenge. This gives it an advantage over current state-of-art alternatives such as secure non-volatile memory (NVM) or trusted platform modules (TPMs). No special manufacturing processes are required to integrate a PUF into a design. This lowers the overall cost of the security for the IC enabling the PUF to be utilised as a hardware root of trust for all security or identity related operations on the device.

However, PUF based authentication/identification schemes are vulnerable to a number of security attacks including machine learning based modelling attacks and physical cloning attacks [4]. The aim of this project is to develop a secure PUF design, which can deliver a corner stone for building unforgeable devices. A low-cost secure PUF-based authentication/identification scheme will lead to a step change in meeting the stringent security requirements of a number of key areas of the digital economy such as Industry 4.0, IoT, and the hardware supply chain.

Objectives:

1. To study the state-of-the-art in PUFs.
2. To investigate the vulnerabilities of different PUF designs and the countermeasures for machine learning based modelling attacks.
3. To explore a fundamental frame work for a theoretical model of PUF.
4. To develop low-cost modelling attack resistant PUF designs.
5. To implement the PUF design developed in 4 on an FPGA/ASIC.
6. To evaluate the output performance of the design developed in 4.

Academic Requirements:

A minimum 2.1 honours degree or equivalent in Computer Science or Electrical and Electronic Engineering or relevant degree is required.

GENERAL INFORMATION

This 3.5 year PhD studentship, potentially funded by the Department for Employment and Learning (DfE), commences on 1 October 2020.

Eligibility for both fees and maintenance (approximately £15,000) depends on the applicants being either an ordinary UK resident or those EU residents who have lived permanently in the UK for the 3 years immediately preceding the start of the studentship. Non UK residents who hold EU residency may also apply but if successful may receive fees only.

Applicants should apply electronically through the Queen's online application portal at: https://dap.qub.ac.uk/portal/

Further information available at: https://www.qub.ac.uk/schools/eeecs/Research/PhDStudy/

Closing date for applications: 15 March 2020