THEME: Cybersecurity: Technology and Ethics

PROJECT: Privacy-preserving functional cryptography

Lead Supervisor: Dr Ciara Rafferty

Supervisory Team: Dr Ciara Rafferty

Primary Location: CSIT

This PhD will investigate the technological development of functional cryptography from a privacy perspective, taking into account legal and ethical concerns.

Functional cryptography is a term describing advanced cryptographic primitives that offer extended functionalities in comparison to traditional encryption schemes and other cryptosystems. Cryptographers are developing a series of techniques that offer fine-grained access control and/or secure computation or communication within groups. These advanced methods are still being improved upon, and further research is necessary. Moreover, any such technologies often claim to be *privacy-preserving* solutions. Can we harness technology to provide privacy by default, to aid user privacy, and enable secure communications?

Despite recent advances, the impact on user privacy, secure communications and computations is yet to be fully explored. Furthermore, what ethical, legal and commercial considerations need to be made to ensure and increase online security and privacy, whilst enabling communication and computation services?

This PhD has the following core objectives:

- Investigate the state of the art in advanced cryptographic primitives and privacy-preserving technologies, particularly functional cryptography
- Analysis of privacy provisions made by promising functional and other advanced cryptographic techniques
- Consideration of practical, legal and ethical considerations, and evaluation against current privacy-preserving approaches
- Analysis of the most suitable technological solutions, and proposal for improvements to user privacy and performance.

Primary Academic Discipline: Data Security