# The Charles Phelps Taft Research Center and the Department of Mathematical Sciences Taft Lecture Series 2016

# Peter Ryan

## University of Luxembourg

**Thursday, September 8, 2016**
**4 pm**
**Taft Research Center,**
**Edwards I, Suite 1110**
**University of Cincinnati**
***Reception at 3:30 pm***

## Modeling & Analysis of Security Protocols

Protocols are ubiquitous and govern the way people and things interact, from elementary particles to nation states. With the rise of the internet and the information age, security protocols permeate society, albeit largely invisible. They enable people who are located on opposite sides of the planet to communicate securely and to establish trust relationships. They enable internet banking and shopping, social networking and perhaps eventually internet voting. The invention of public key (PK) cryptography in the ‘60s gave rise to a vast new landscape of such protocols. More recently, the rise of quantum technologies threatens the foundations of much of PK cryptography whilst also opening up new vistas of its own: quantum cryptography.

Understanding and analyzing such protocols, both classical and quantum, presents immense challenges. We need to show that they guarantee extremely subtle properties even in a hostile, malicious environment.

In this lecture, I will attempt to provide a broad overview of the nature of security protocols and the approaches to modeling and analyzing them.

UNIVERSITY OF Cincinnati