Workshop
Post quantum cryptography for travel documents and 5G

*Dipartimento di Matematica e Fisica*
*Largo San Leonardo Murialdo 1*

**March 11, 2020**
**Aula M3**

*Chair Prof. Massimiliano Sala* Università degli Studi di Trento

2:30 – 2:45 p.m.
**Opening**

Giulio Codogni, Università Tor Vergata

2:45 – 3:45 p.m.
**Chris Mitchell,** Royal Holloway, University of London
Quantum computing – What will be the real impact on 5G security?

3:45 – 4:15 p.m.
**break**

4:15 – 4:30 p.m.
**Andrea De Maria,** Head of the research unit of the “Poligrafico dello Stato”

4:30 – 5:30 p.m.
**Gaëtan Pradel,** INCERT Luxembourg
Post-Quantum Certificates for Electronic Travel Documents

5:30 – 6:00 p.m.
**Questions and Discussion**
ABSTRACTS:

**Chris Mitchel**  
*Quantum computing – What will be the real impact on 5G security?*

As has been widely discussed, if and when large-scale general-purpose quantum computers are constructed, the effect on currently used cryptography will be very significant – all asymmetric algorithms based on factoring large integers or discrete logarithms (include elliptic curve) will be rendered insecure for practically feasible key lengths. Also, all symmetric algorithms will in effect have their key length halved; i.e., with the aid of a quantum computer, a k-bit key could be ‘brute-forced’ in of the order of $2^{k/2}$ computations, so a 128-bit key will offer roughly the same level of security as a 64-bit key does today. In this context it is clearly vital to consider what the impact will be in practice. For algorithms solely used for verifying data integrity of transmitted data, there will no significant problems, as long as new ‘secure’ algorithms are introduced by the time quantum computing is available. However, the significance for encryption and key establishment algorithms is potentially catastrophic. If ciphertext is intercepted and stored, then it could be decrypted if and when the encryption algorithm is broken; i.e. data whose secrecy is of long-term significance is being made vulnerable right now through the use of algorithms which are quantum-unsafe. These widely discussed facts mean that it is imperative that we carefully examine current uses of cryptography to understand what needs to be done and when. In this talk I will use a case study of the current 5G security provisions as the basis for a more general discussion of the quantum security problem. References will also be made to other widely used security schemes, such as SSL/TLS and the EMV payment security system. Conclusions will be drawn about what algorithms need changing and when, on the assumption that quantum computing will eventually become a reality.

**Gaëtan Pradel**  
*Post-Quantum Certificates for Electronic Travel Documents*

Public key cryptosystems play a crucial role in the security of widely used communication protocols and in the protection of data. However, the foreseen emergence of quantum computers will break the security of most of the asymmetric cryptographic techniques used today, including those used to verify the authenticity of electronic travel documents. The security of international borders would thus be jeopardised in a quantum scenario. To overcome the threat to current asymmetric cryptography, post-quantum cryptography aims to provide practical mechanisms which are resilient to attacks using quantum computers. In this paper, we investigate the practicality of employing post-quantum digital signatures to ensure the authenticity of an electronic travel document.

We created a special-purpose public key infrastructure based on these techniques and give performance results for both creation and verification of certificates. This is the first important step towards specifying the next generation of electronic travel documents, as well as providing a valuable use case test for post-quantum techniques.