Panelist: Mike Burmester

Mike Burmester
Royal Holloway, University of London,
Egham, Surrey,
U.K.
email: m.burmester@rhbnc.ac.uk

Statement:

Several cryptographic models provide adequate means for proving the security of protocols.

Discussion:

Cryptography is concerned with scenarios in which faults occur under the control of a malicious adversary. There are several cryptographic models which can be used to prove the security of protocols in such a scenario. These models depend on the power of the adversary. If the adversary has unlimited resources then the model is based on information theory and we have unconditional security.

If the adversary has limited resources (polynomially bounded), then the model is based, either on pseudorandomness and we have proven security, or the security is reduced to a problem which is (believed to be) intractable.

The strength of the cryptographic approach lies, essentially, in its flexibility.

Depending on the security requirements and the model, we can use appropriate cryptographic attributes such as zero-knowledge or indistinguishability, as a tool to design secure protocols. We will discuss practical network protocols whose security can be proved in an appropriate cryptographic model.