Abstract:
Most approaches to confidentiality in the literature are based on the idea of restricting the flow of information between different security levels. However, there might be cases when one needs to control these flows instead of merely restricting them. Suppose a piece of code is downloaded from an untrusted source to be executed on a local (trusted) host. Furthermore, this code is assumed to implement an agent of a cryptographic protocol. The agent implementation will access local secret information and transmit it, under encryption, over untrusted media. In other words, the program needs to establish a flow of information from a higher level of security (secret data in the local host) to a lower one (data over the untrusted communication media).
Suppose now that the protocol is known to preserve confidentiality. One might then be tempted to try proving that the downloaded code actually implements its part in this protocol. However, usual notions of refinement are inappropriate for this task, since they are known not to preserve confidentiality.
This talk reports on current work aimed at providing a definition of confidentiality that is relative to a specification, and can cope with information downgrading. It is based on the following publications:

