Dottorato in Matematica
30° ciclo
SEMINARIO DI DOTTORATO

Giovedì 19 ottobre 2017- ore 12.00
(Aula Seminari “-1” – Dipartimento di Matematica)

Riccardo Longo
(Dottorando Università di Trento)

On the Security of the Blockchain Bix Protocol and Certificates

Abstract

The BIX protocol is a blockchain-based protocol that allows distribution of certificates linking a subject with his public key, hence providing a service similar to that of a PKI but without the need of a CA.

After an introduction on proofs of security, the BIX protocol will be presented, then its security will be analysed in a formal way. Once the formal security assumptions will be identified, some attack scenarios against the BIX protocol will be presented, and finally, theorems that these attacks are not feasible under our previously established assumptions will be provided, with a sketch of their proofs.

Relatore:
Massimiliano Sala