Abstract:

Cryptography is used to protect data and communications. The basic tools are cryptographic primitives, whose security and efficiency are widely studied. But in real-life applications these primitives are not used individually, but combined inside complex protocols. So these cryptographic protocols have to be analysed and their security assessed in formal way.

The rise of Bitcoin has shown to the world the great potential of blockchain technologies. Satoshi Nakamoto’s breakthrough allows to build publicly verifiable and almost immutable ledgers, but sometimes privacy has to be factored in.

In this talk will be presented an original protocol that allows sensitive data to be stored on a ledger where its integrity may be publicly verified, but its privacy is preserved. The intent is to allow secure sharing of this data between authorized parties, and integrate an end-to-end one-time access system that provides full control over the usage of private data.

The security analysis considers various internal and external adversaries, and proves the security reducing the attacks to the solution of Diffie-Hellman problems.

Supervisor:

Massimiliano Sala