Learning module 4: Digital Signatures

Description

Digital signatures are the extension of paper signatures to the digital realm that is made possible thanks to the development of asymmetric cryptography. Like real signatures, they are a way to prove one's identity and to certify the origin of a message.

Learning Module 4 describes the properties and technical requirements necessary for the implementation of digital signatures and the mathematical prerequisites. The generic characteristics of a digital signature algorithms are then presented and specific algorithms that are commonly used in blockchain systems implementation are discussed in detail. Privacy preserving digital signature algorithms are discussed, focusing on their use in the cryptocurrency space and concepts of anonymity and pseudonymity of transaction on a blockchain are presented. Security of digital signatures and possible attack schemes are considered and an in-depth analysis of one possible attack vector is analyzed in a lab. The last part of the module discusses the future of digital signatures, presenting novel algorithms designed to be resistant to present and foreseen threats linked to the advent of quantum computers.

Dependencies

This learning module has the following prerequisites:

- Encryption techniques (LM2)

Learning Objectives

- To explain basic properties that a digital signature algorithm must satisfy.
- To present the digital signature algorithms that are most widely used in blockchain-based systems
- To present privacy-preserving digital signature algorithms.
- To discuss anonymity and pseudonymity features of blockchain systems.
- To present attacks and security issues related to digital signature algorithms.
- To present beyond state-of-the-art development related to digital signature algorithms.
- To present use cases of digital signatures in blockchain-based systems.

Learning Outcomes

- **Understand** fundamental properties of digital signature algorithms.
- **Understand** details of the most used digital signature algorithms
- **Acquire** technical skills related to the use of digital signatures.
- **Understand** the workings of privacy preserving digital signature algorithms.
- **Recite** possible attacks on commonly used digital signature algorithms.

Syllabus

1. Signature definitions, properties, and requests
2. Preliminaries
   - 2.1. Elliptic Curves
   - 2.2. Lab: the bitcoin-core/secp256k1 library
3. Digital signature algorithms
   - 3.1. Introduction
   - 3.2. DSA
   - 3.3. ECDSA
   - 3.4. Schnorr signatures
   - 3.5. Lab: implementation and analysis of Schnorr signatures
4. Ring signatures
   - 4.1. Properties
   - 4.2. The role of ring signatures in the Monero blockchain
   - 4.3. Lab: implementing ring signatures
5. Anonymity and pseudonymity in blockchain transactions
6. Security and Attacks
   - 6.1. Overview of security problems and attacks
   - 6.2. Lab: specific attack on Schnorr signatures
7. The Future of Digital Signatures: Lattices, hash signatures, and threshold signatures
8. Use cases