ELE2742 / ENG1467 - PUC-Rio, 2019.1

Lecture 1: Introduction

DATE

Lecturer: Yi-Fan Tseng *Scribe: Yi-Fan Tseng*

Digital signature is an important topic in asymmetric cryptography (public key cryptography), which is a mathematical scheme for verifying the authenticity of digital messages. In a digital signature scheme, a *signer* is able to generate a digital signature for a message of her choice using her private key, and a *verifier* is able to verify the validity of a signature using signer's public key.

We show several common reasons for applying digital signature.

- Authentication: Since the private key used to sign a message is bounded to a specific user, the validity of a digital signature implies that the message was sent by that user.
- Integrity: For a digital signature, any change to the signed message will invalidate the signature. Besides, the security of a digital signature scheme makes sure that there is no efficient way to modify a message and its signature to produce a new message with a valid signature.
- Non-Repudiation: Because the private key used for generating a digital signature is kept secret by the signer, she cannot deny having signed the message.

In this course, we will introduce the following contents.

- Mathematical Background: The preliminaries that will be used through the entire course
- One-Time Signature: The most simple signature scheme, which can only be used for one-time
- RSA/Rabin/ElGamal/Schnorr Signature: Commonly-used signature schemes
- Blind Signature: The signed message is hidden from the signer
- Designated Verifier Signature: The signer is able to make the signature to be verified only by a designated verifier
- Ring/Group Signature: The identity of the signer is hidden from the verifier
- Proxy Signature: A proxy is able to generate a valid signature on behalf of the original signer
- Identity-Based Signature: Using identity as the public key
- Certificateless Signature: The combination of public-key-based signature and identity-based signature
- Security Proof: The technique to prove the security for a signature scheme