

Digital Signatures

Rohit Musti

CUNY - Hunter College

April 6, 2022

Table of Contents

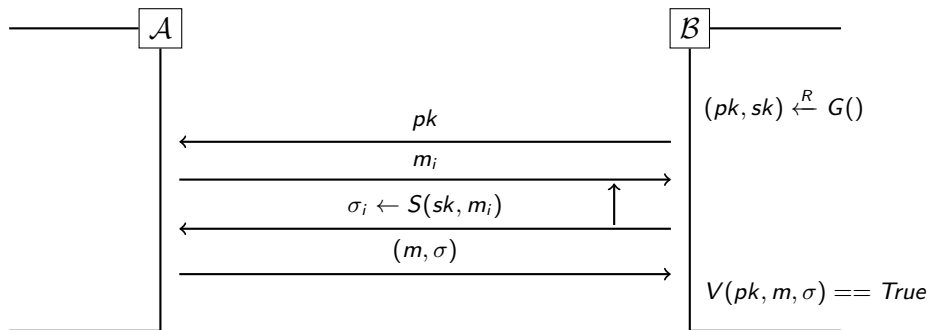
- 1 Overview
- 2 Trapdoor Construction of Digital Signatures
- 3 Legality of Digital Signatures

1 Overview

Example Use Case

- Let's pretend you are a software company
- Occasionally, you will distribute updates to your software
- Customers will need a way to verify that the software is really from the company without sharing a secret key with every single customer
- Enter digital signatures!

Digital Signatures Attack Game



Non-Repudiation

- 1 Non-Repudiation: there is no way to deny that the signature was not produced by someone with access to the secret key
- 2 This sounds legally useful right? Unfortunately not, it is very easy for someone to claim the public key isn't theirs or their secret key was exposed/leaked/stolen by a hacker.
- 3 Even more maliciously, Alice could have leaked her key right after or before sending a signature

Limits

- ① Binding Signatures: Easy for a signer to issue multiple yet contradicting signed messages
- ② Duplicate Keys: Given a signature σ for a public key pk , could I generate a pk', sk', m that produces $\sigma' == \sigma$
- ③ Future HW Question: Is there an easy way to get around duplicate keys attacks???

2 Trapdoor Construction of Digital Signatures

Construction

$$S(sk, m) = y \leftarrow H(m), \sigma \leftarrow I(sk, y)$$

$$V(pk, m, \sigma) = y \leftarrow F(pk, \sigma), y == H(m)$$

Security

- In order to prove security we must model the hash function as a random oracle
- This means that y is essentially a random point in the space, and there is no way for an attacker to forge its signature
- Without this hashing, an attacker could trivially generate secure signatures! Future HW question: How???

3 Legality of Digital Signatures

US

- In 2000, Congress passed a law known as E-signatures
- The goal was to facilitate the use of digital signatures over interstate commerce
- all sales of goods over \$500 require a signatures
- a US digital signature must contain three elements
 - 1 a symbol or sound
 - 2 attached or logically associated digital record
 - 3 made with the intent to sign the record
- did they succeed? qualifying signature examples: name typed, digitized picture of signature, pin to identify the recipient, mouse click, a sound, a cryptographic digital signature

UN

- UN adopted digital signature requirements in a 2005 convention
- additional requirements including identify the signer and is reliable (basically a mouse click still qualifies if you can prove who clicked and establish a clear intention behind the click)