

IT Security for Citizens

Gert Læssøe Mikkelsen

Department of Computer Science
Aarhus University

March 24, 2009

Introduction

Digital Signatures in Practice



Sign
→



Introduction

Digital Signatures in Practice



Sign
→

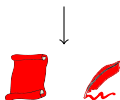
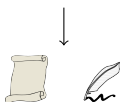


Introduction

Digital Signatures in Practice



Sign →



Introduction

Digital Signatures in Practice



Sign
→



Introduction

Digital Signatures in Practice



Sign
→

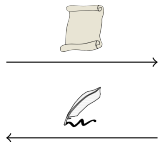


Introduction

Digital Signatures in Practice

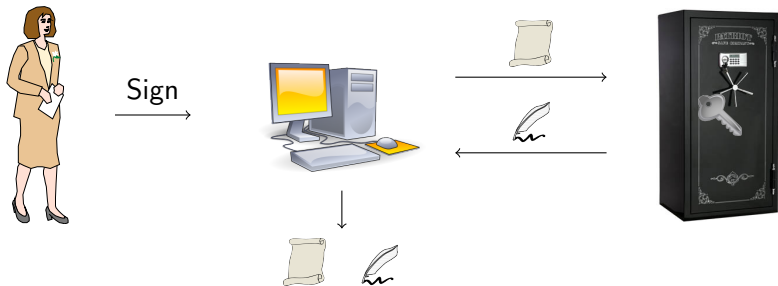


Sign
→



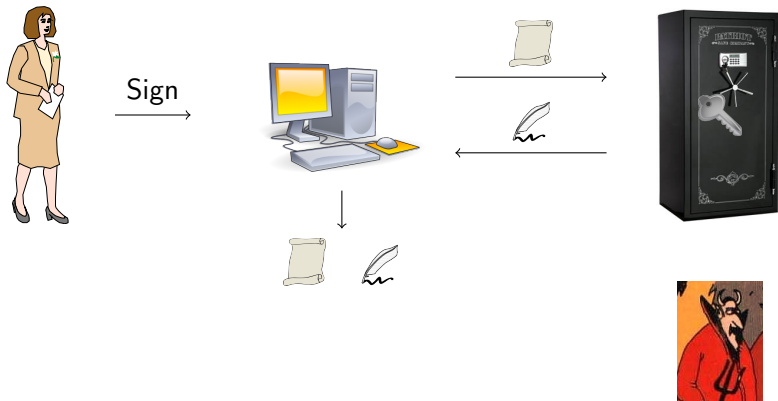
Introduction

Digital Signatures in Practice



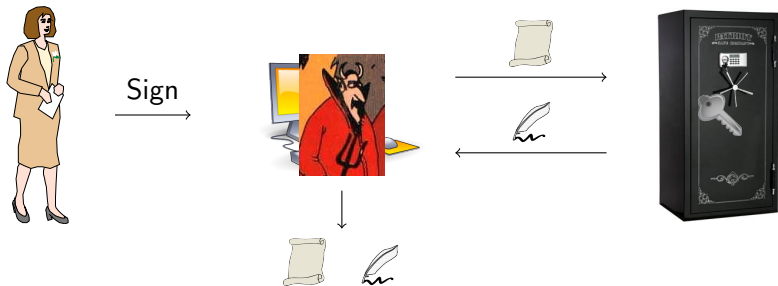
Introduction

Digital Signatures in Practice



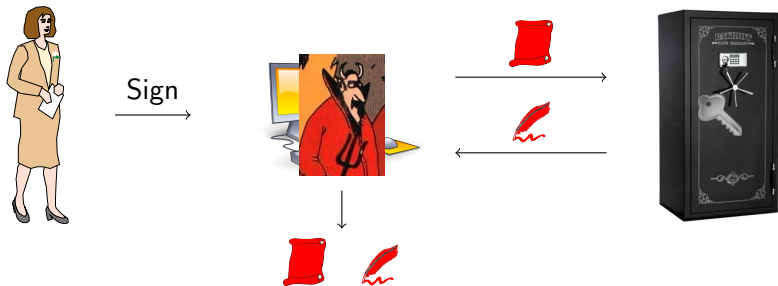
Introduction

Digital Signatures in Practice

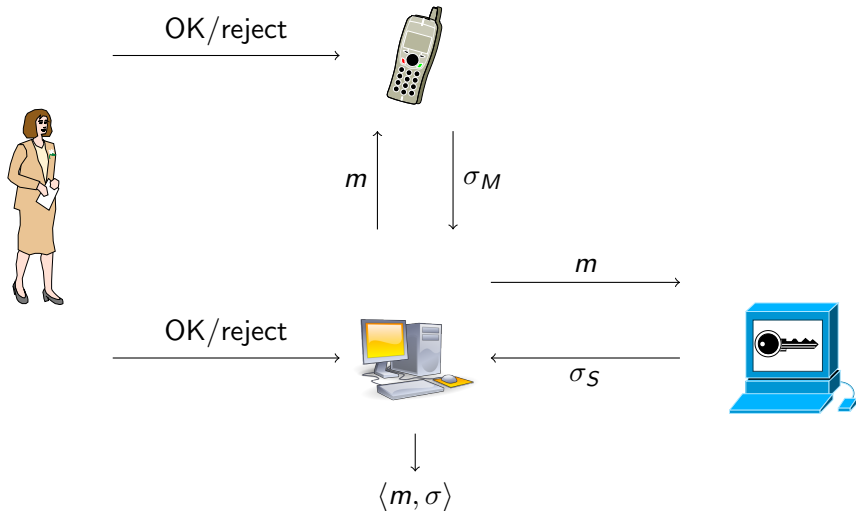


Introduction

Digital Signatures in Practice



Overview of the Protocol



Players in the protocol

- U : Incorruptible human user.
- T : Terminal used during signature issuing.
- M : Mobile device, with low computational power.
- S : A server.

The adversary \mathcal{A} may corrupt at most one of $\{T, M, S\}$

Players in the protocol

- U : Incorruptible human user.
- T : Terminal used during signature issuing.
- M : Mobile device, with low computational power.
- S : A server.

The adversary \mathcal{A} may corrupt at most one of $\{T, M, S\}$

Ingredients

- Standard RSA signatures: $sig(m) = m^d \pmod{N}$

Players in the protocol

- U : Incorruptable human user.
- T : Terminal used during signature issuing.
- M : Mobile device, with low computational power.
- S : A server.

The adversary \mathcal{A} may corrupt at most one of $\{T, M, S\}$

Ingredients

- Standard RSA signatures: $\text{sig}(m) = m^d \pmod N$
- Additive secret sharing:

$$\begin{aligned}d &= d_1 + d_2 \\ \text{sig}(m) &= m^d \pmod N = m^{d_1} m^{d_2} \pmod N\end{aligned}$$

Protocol π_{M-SIG} signature generation



pwd



$\{d_M\}$



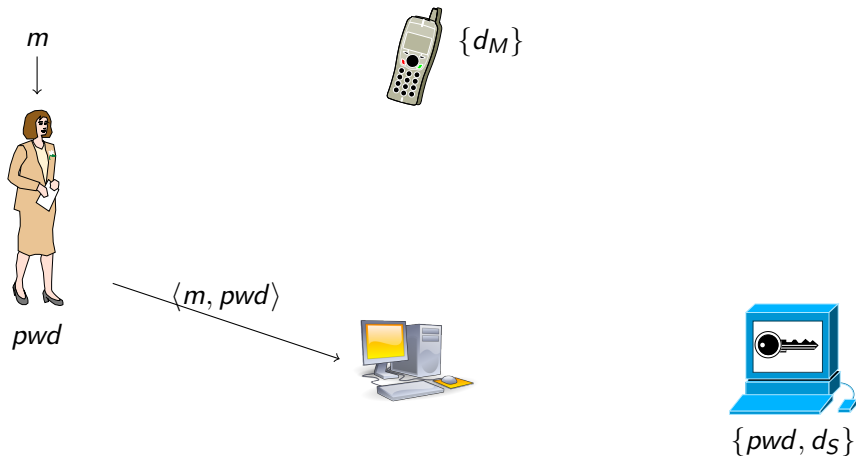
$\{pwd, d_S\}$

Protocol π_{M-SIG} signature generation

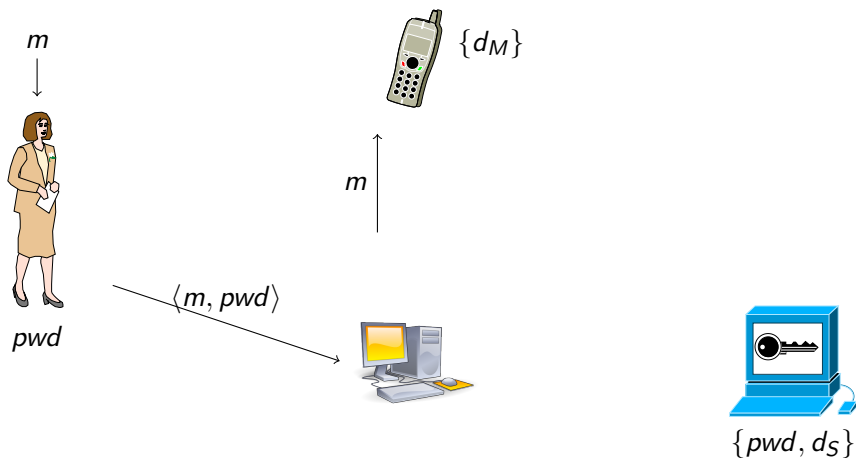


$\{pwd, d_S\}$

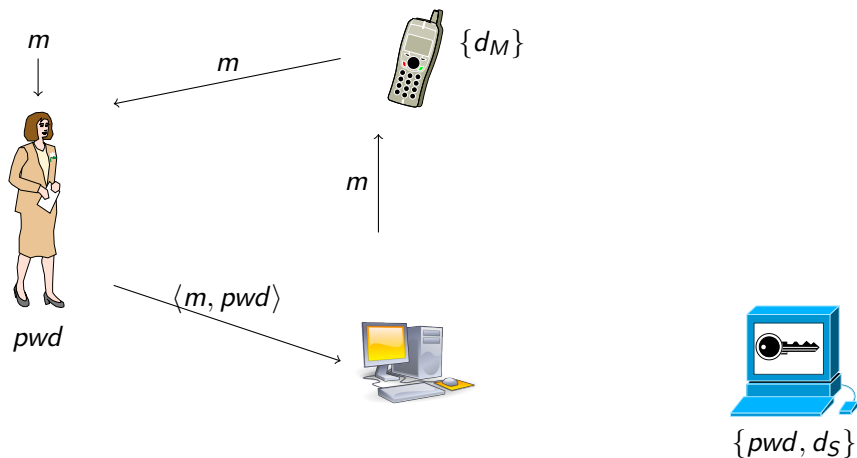
Protocol π_{M-SIG} signature generation



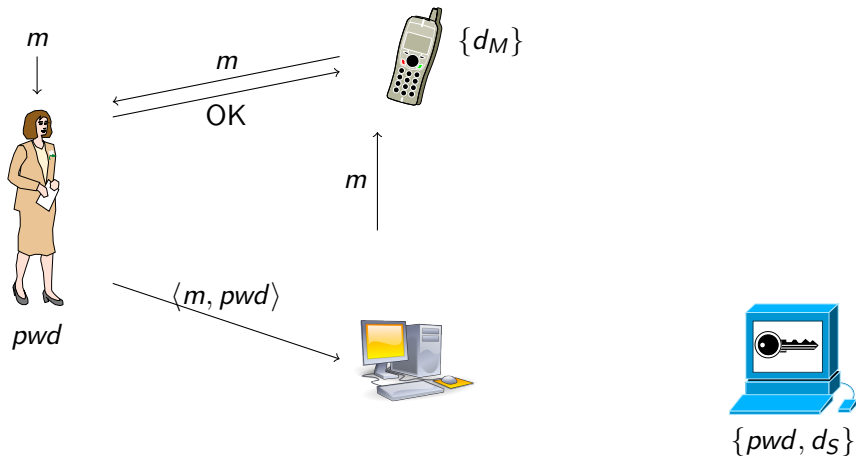
Protocol π_{M-SIG} signature generation



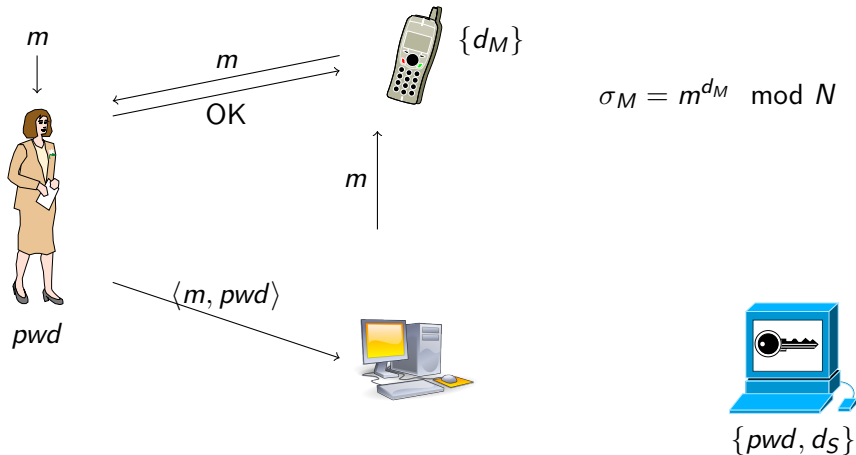
Protocol π_{M-SIG} signature generation



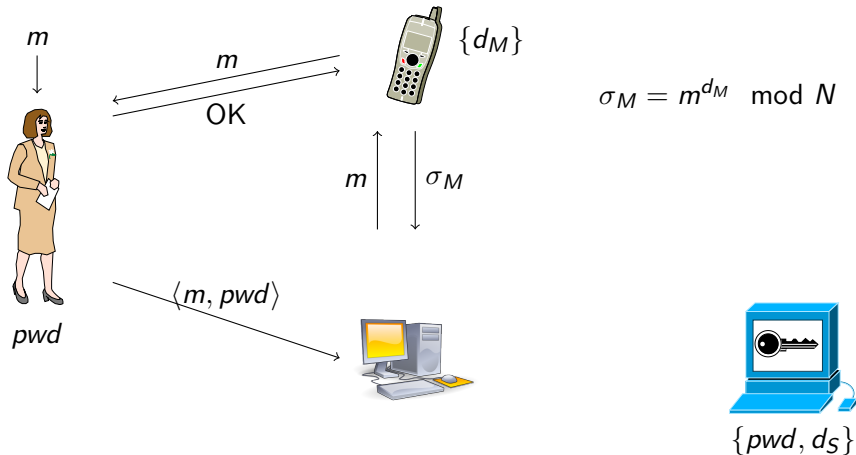
Protocol π_{M-SIG} signature generation



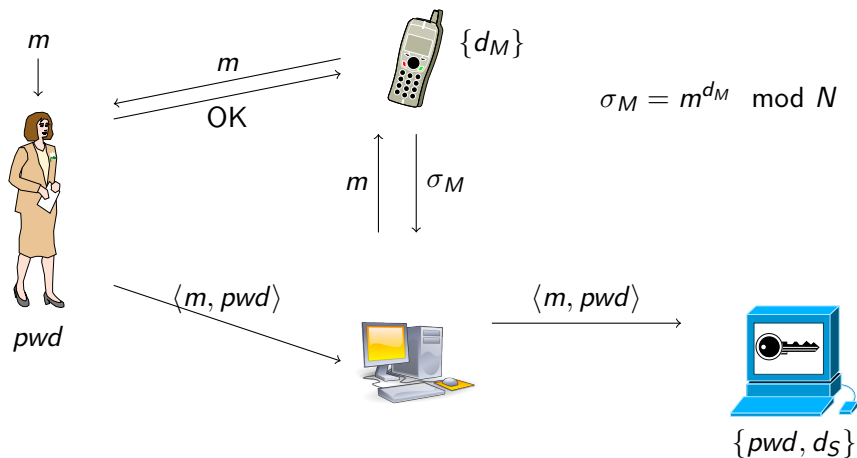
Protocol π_{M-SIG} signature generation



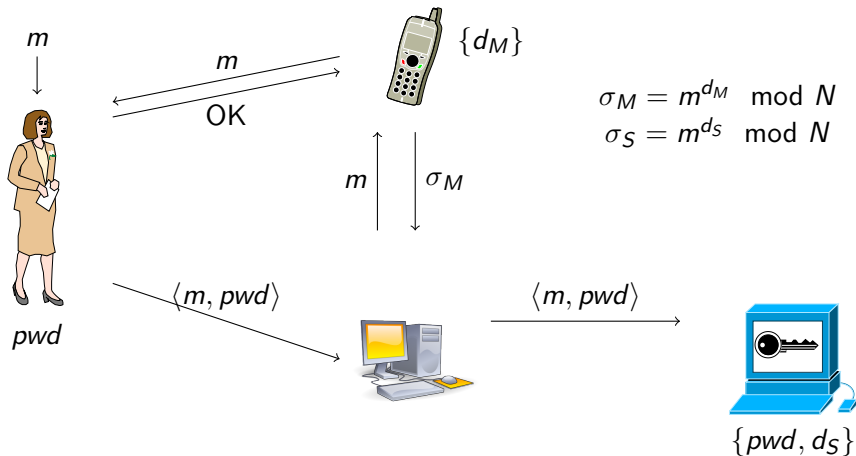
Protocol π_{M-SIG} signature generation



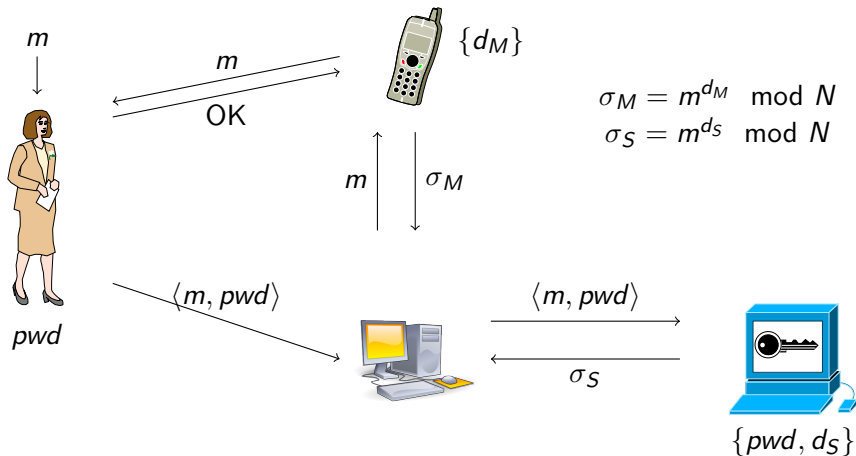
Protocol π_{M-SIG} signature generation



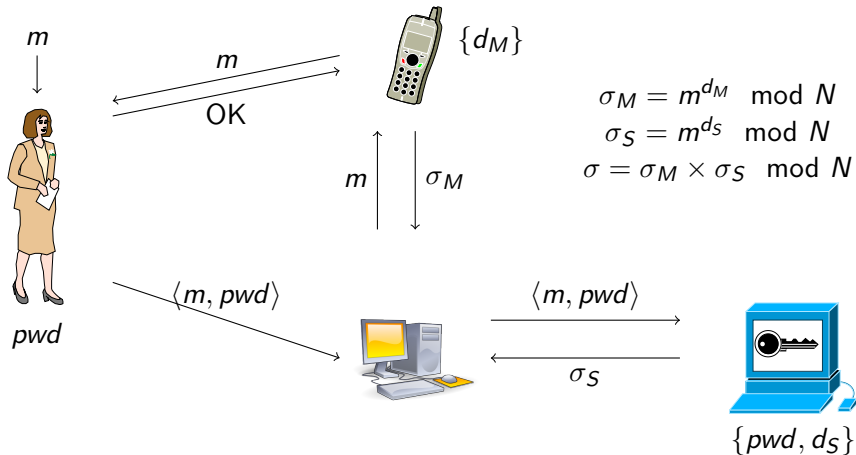
Protocol π_{M-SIG} signature generation



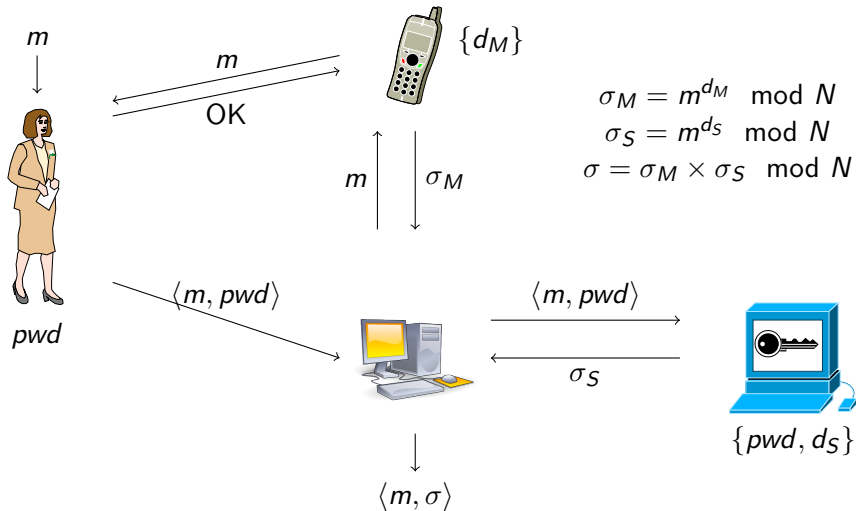
Protocol π_{M-SIG} signature generation



Protocol π_{M-SIG} signature generation



Protocol π_{M-SIG} signature generation



Prototype implementation

Current Status

Prototype implementation

Current Status

- The protocol part for issuing signatures.

Prototype implementation

Current Status

- The protocol part for issuing signatures.
- Is working in the Danish OCES PKI.

Prototype implementation

Current Status

- The protocol part for issuing signatures.
- Is working in the Danish OCES PKI.
- Trick: Outsourcing improves the protocol in practice.