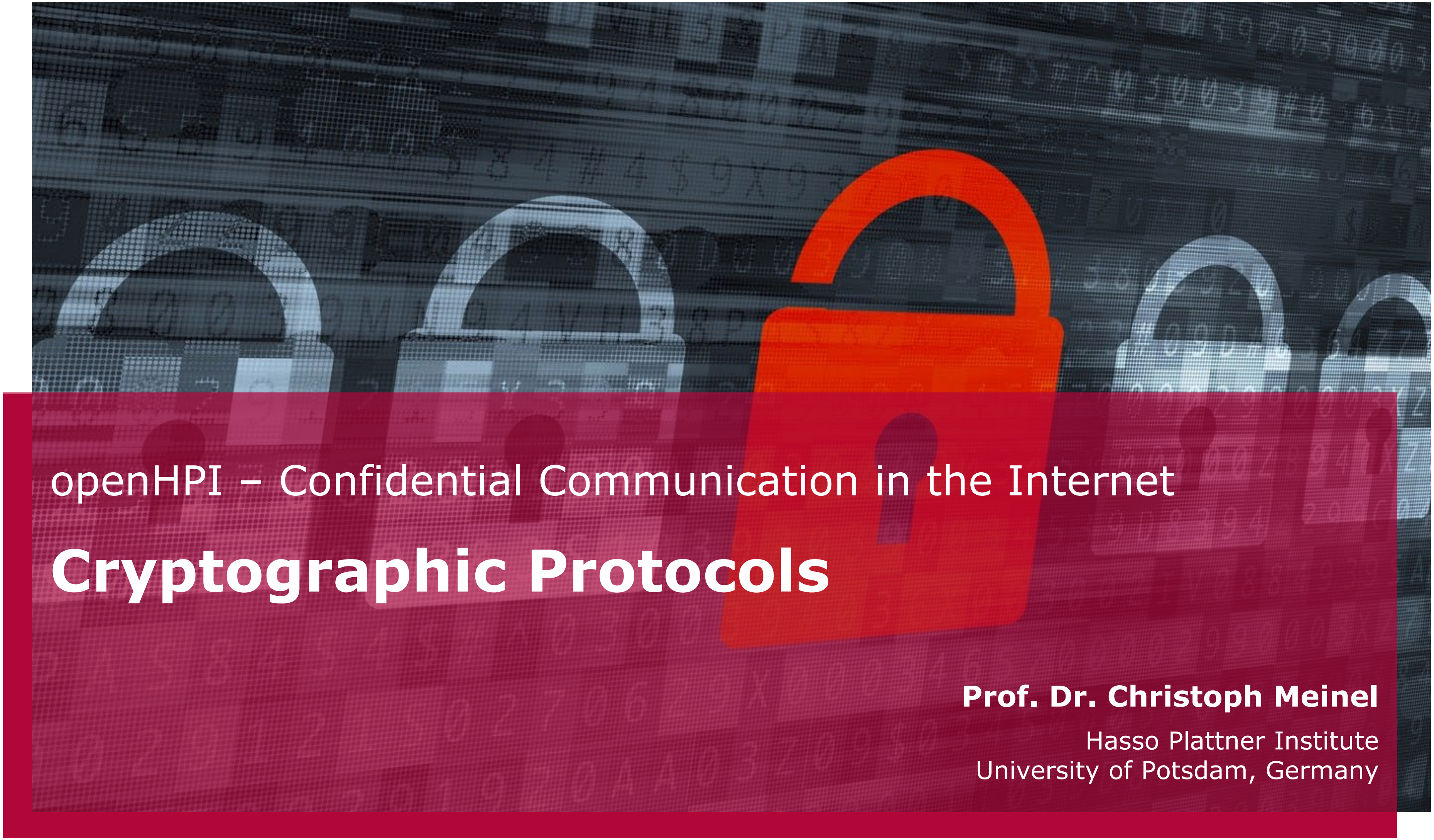


openHPI – Confidential Communication in the Internet

Cryptographic Protocols

Prof. Dr. Christoph Meinel

Hasso Plattner Institute
University of Potsdam, Germany

Cryptographic Protocols (1/2)

A **cryptographic protocol, shortly cryptoprotocol** is defined as

- an established sequence of actions
- for two or more participants
- to **ensure one or more security goals**, e.g.
  - □ securing **confidentiality**
  - □ ensuring **integrity**
  - □ …

A **cryptoprotocol** is based on a **cryptosystem** with a **crypto procedure**/**algorithm** on the middle

Cryptographic Protocols (1/2)

Typical participants of a cryptoprotocol:

Alice

- First communication partner and initiator of the communication in a cryptoprotocol

Bob

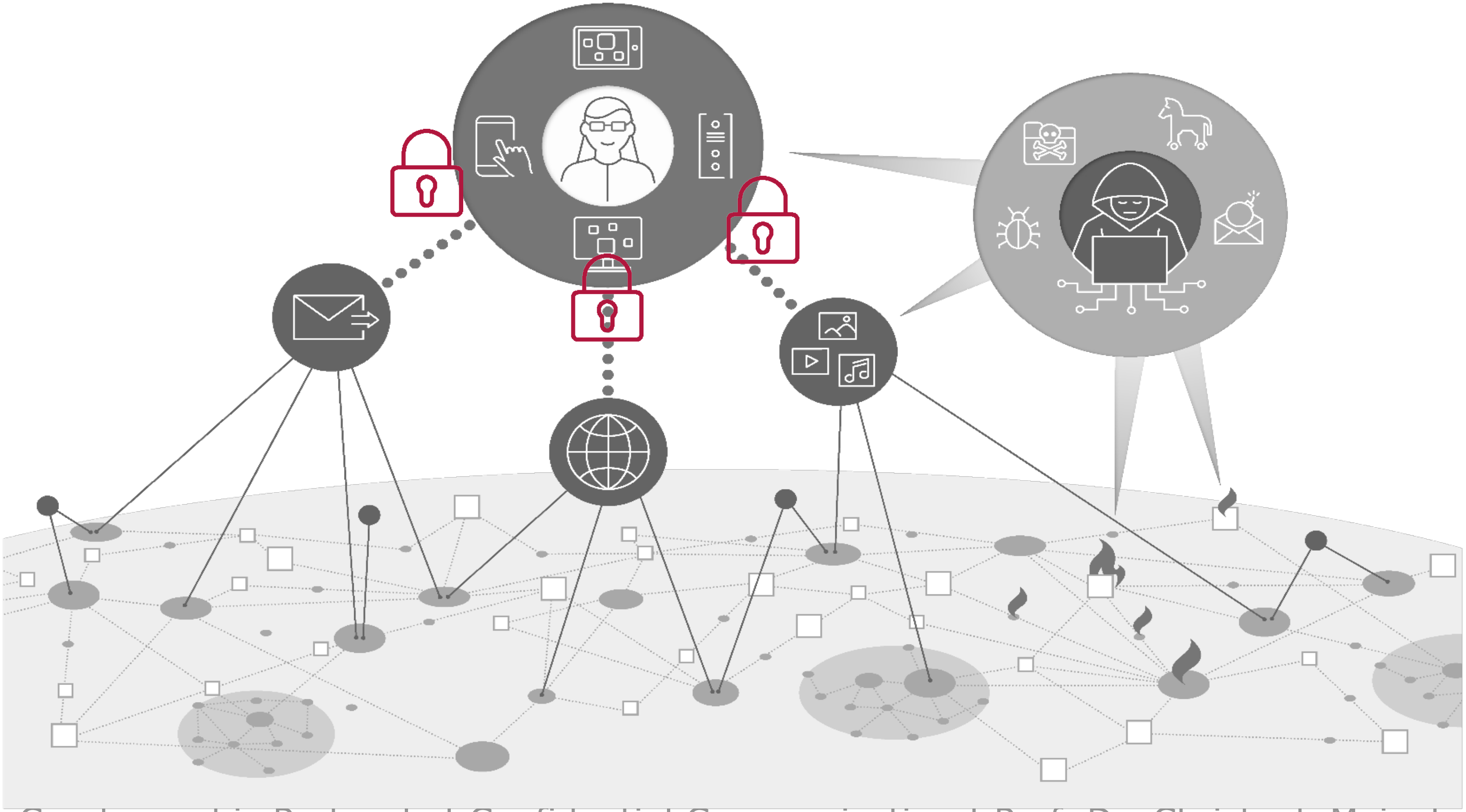
- Second communication partner in a cryptoprotocol

Mallory

- Bad guy with unlimited (computationally) abilities
  - when listening to a communication channel
  - when manipulating the tapped data and
  - when forwarding fake messages
  - ...

Cryptographic Protocol for …
Encryption (1/2)

Target: Ensuring the **confidentiality** of information to prevent spying on secrets e.g. when it is transmitted over the Internet



Cryptographic Protocol for … **Encryption** (2/2)

Preliminary remarks:

- We have already discussed symmetric and asymmetric procedures for encryption …
- General problem with symmetrical procedures:
  - **Sscure key exchange is very difficult**
- Gereral problem with asymmetrical procedures:
  - passing on the public key is safe
  - **but**: Asymmetric methods are only suitable for small data volumes due to the **enormous computing time**

Idea: Hybrid encryption process

- Use of asymmetric procedures for the key exchange
- Use of symmetric procedures for the data exchange

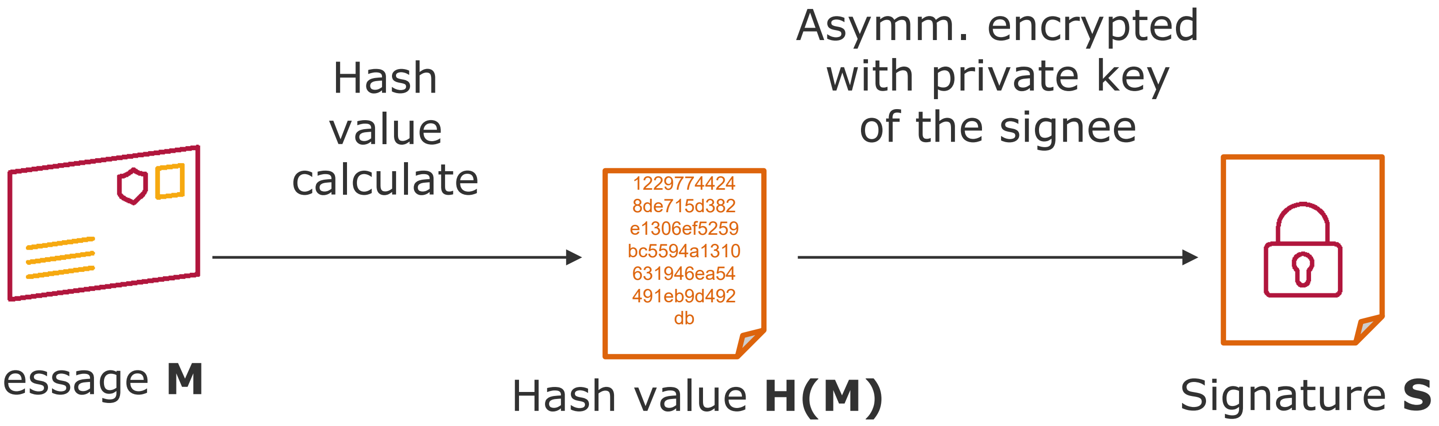
Cryptographic Protocol for …
Digital Signatures (1/2)

Digital signatures are cryptoprotocols that ensure

- securing the **identity of the author/sender** and
- **integrity** of the **content**

No manipulation possible neither of the sender nor of the content

Process of the Digital Signature:



Hash value calculate

Asymm. encrypted with private key of the signee

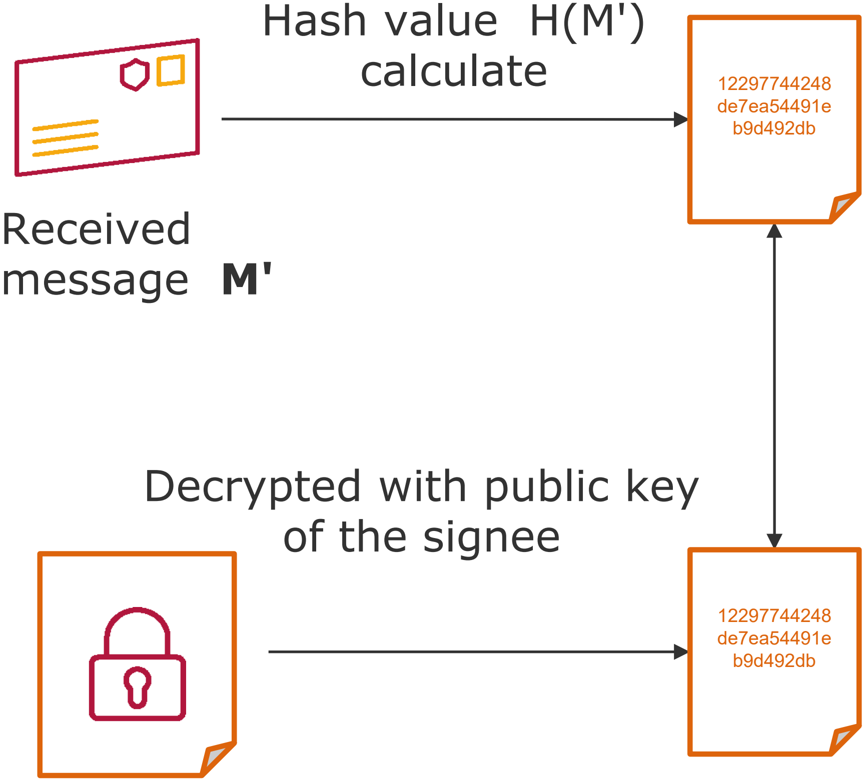
Message **M**

Hash value **H(M)**

Signature **S**

Cryptographic Protocol for …
Digital Signatures (2/2)

Verification:



Hash value H(M')
calculate

12297744248
de7ea54491e
b9d492db

Received
message **M'**

Decrypted with public key
of the signee

12297744248
de7ea54491e
b9d492db

Signature **s**

Hash value **H(M')**

If **H(M') = H(M)**,

then **M‵ = M** applies

Hash value **H(M)**