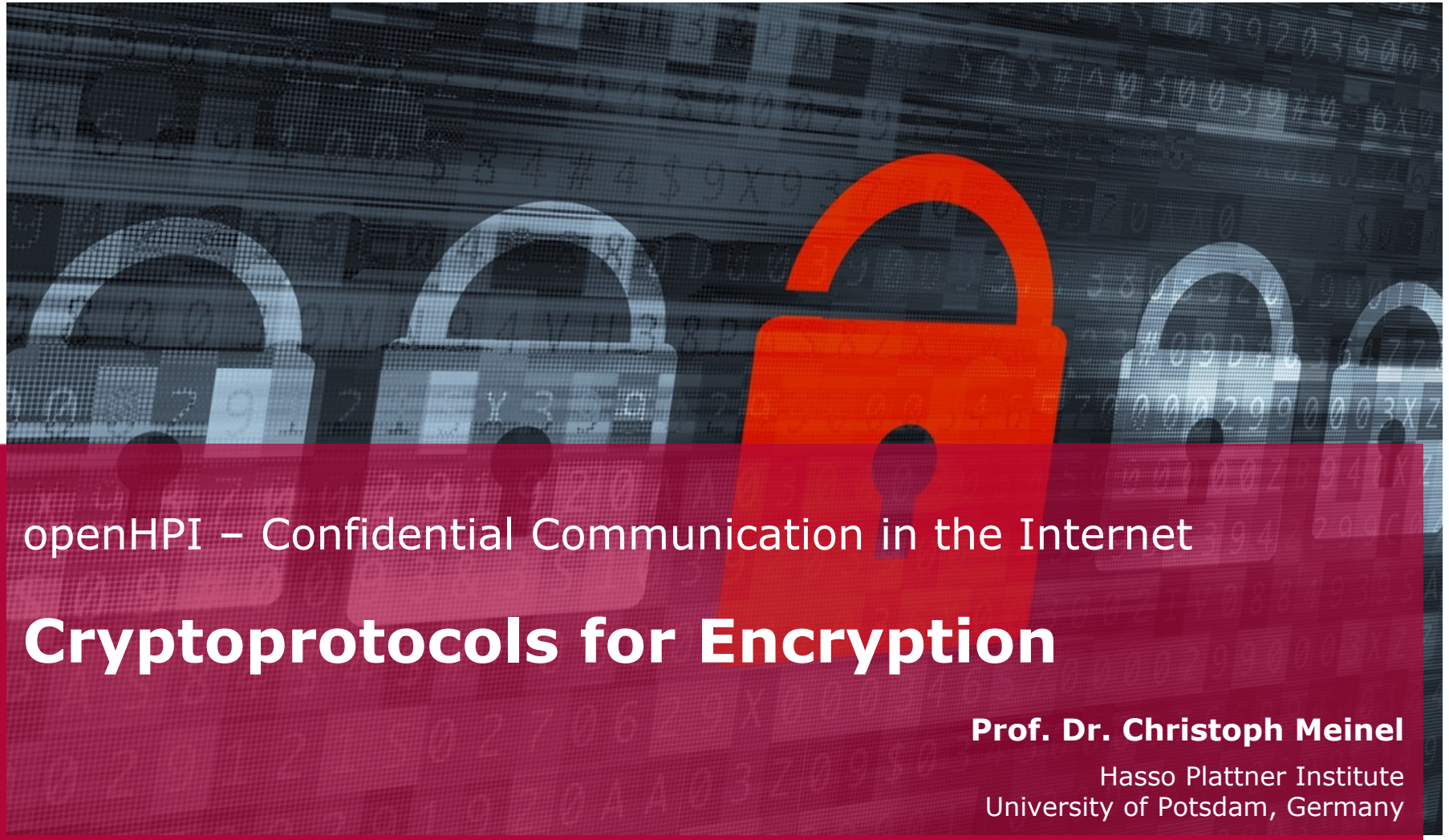


openHPI – Confidential Communication in the Internet

Cryptoprotocols for Encryption

Prof. Dr. Christoph Meinel
Hasso Plattner Institute
University of Potsdam, Germany

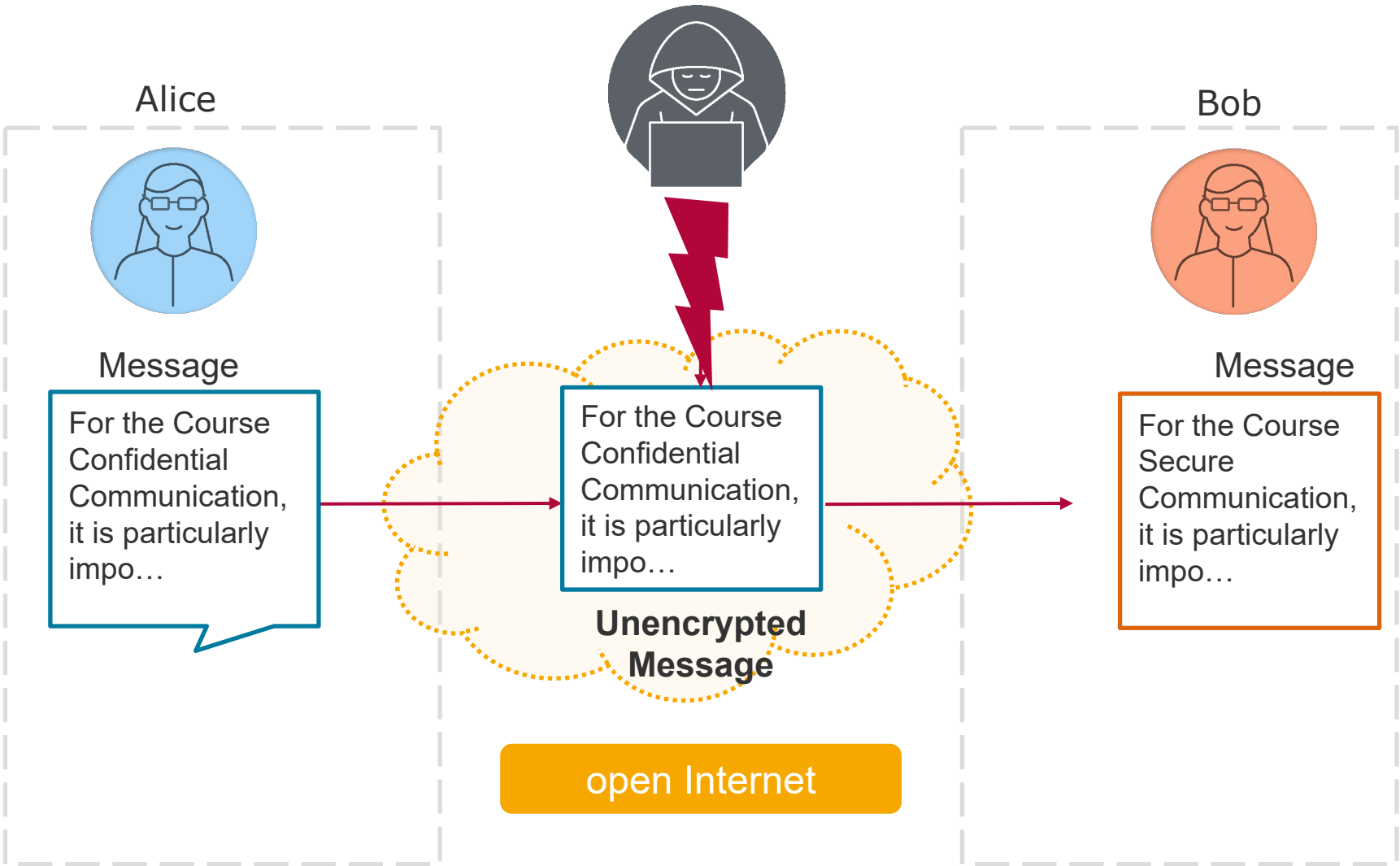
Reminder:
Basic Scheme of Encryption Protocols

–Cryptoprotocols for **encryption** are used to transmit confidential messages over insecure communication channels, like the open Internet

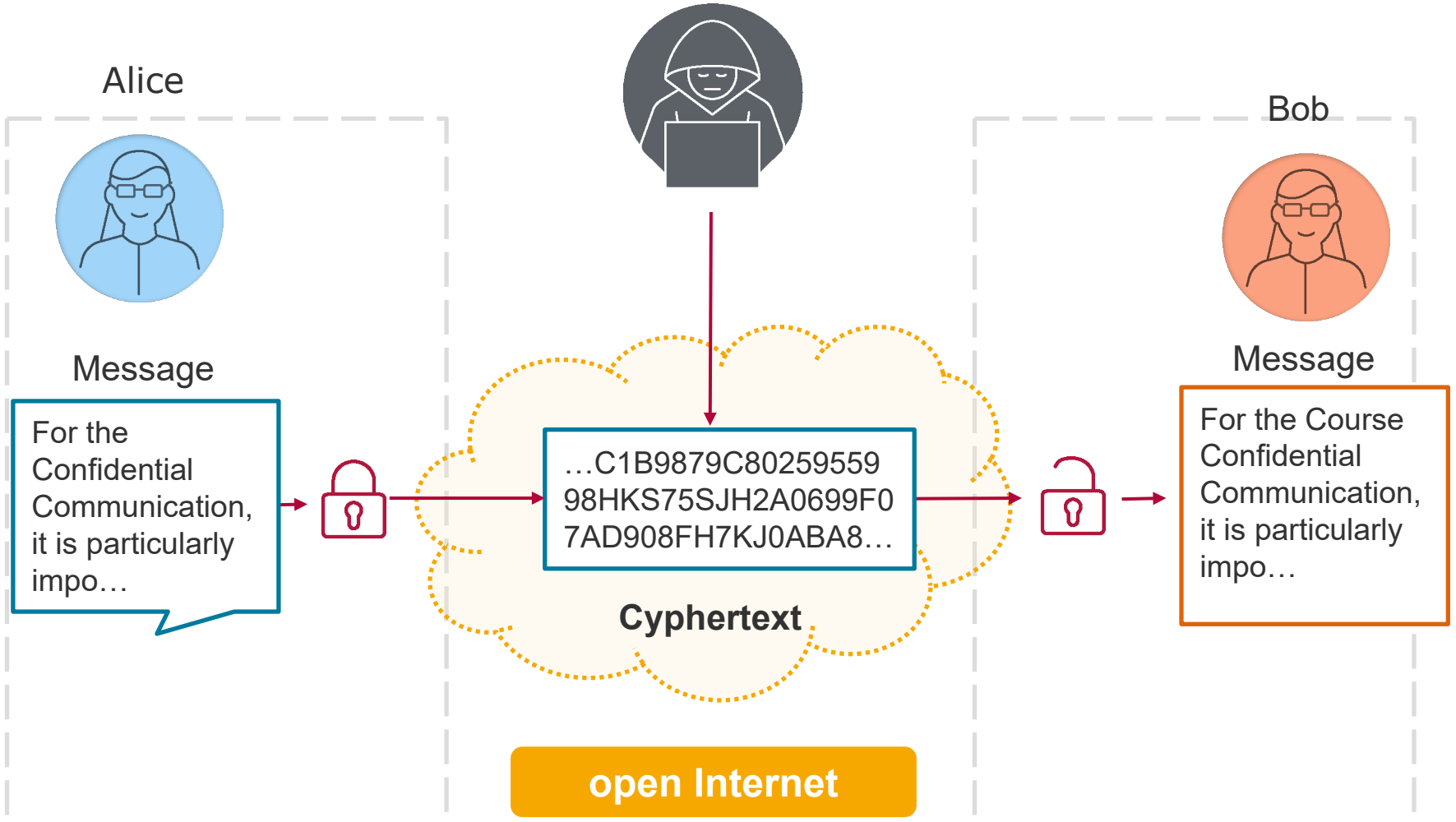
Basic protocol:

- Alice and Bob arrange a **cryptosystem**
- Alice and Bob agree on the **key(**s) to be used
- Alice **encrypts** her message with the encryption function of the agreed cryptosystem and the agreed key
- Alice sends the **ciphertext** over the insecure communication channel
- Bob **decrypts** the ciphertext with the decryption function of the agreed upon cryptosystem and the agreed upon key

Sending an Unencrypted Message



Sending an Encrypted Message



Reminder:
Symmetric Encryption Protocols (1/2)

Basic protocol:

- Alice and Bob arrange a **symmetric cryptosystem**
- Alice and Bob agree on a **common key**
- Alice **encrypts** her message with the agreed symmetric encryption function and the common key
- Alice sends the ciphertext over the insecure communication channel
- Bob **decrypts** the ciphertext with the agreed decryption function and the common key

Reminder: **Symmetric Encryption Protocols** (2/2)

Advantages:

- Symmetric encryption and decryption algorithms can be calculated very efficiently
- Clear situation for cryptanalysis
- ...

Main problem:

- Arrangement and/or exchange of the common secret key

Reminder:
Asymmetric Encryption Protocols (1/2)

Basic protocol:

- Alice and Bob arrange **asymmetric cryptosystem**
- Alice takes the **public key of Bob**
- Alice **encrypts** her message with the agreed encryption function and the public key from Bob
- Alice sends the ciphertext over the insecure communication channel
- Bob **decrypts** the ciphertext with the agreed decryption function and **his private key**

Reminder:
Asymmetric Encryption Protocols (1/2)

Advantages:

- No need to exchange the **secret key**

Problems:

- Asymmetric encryption and decryption is computationally very expensive
- Precautions are necessary to ensure the use of the correct public keys