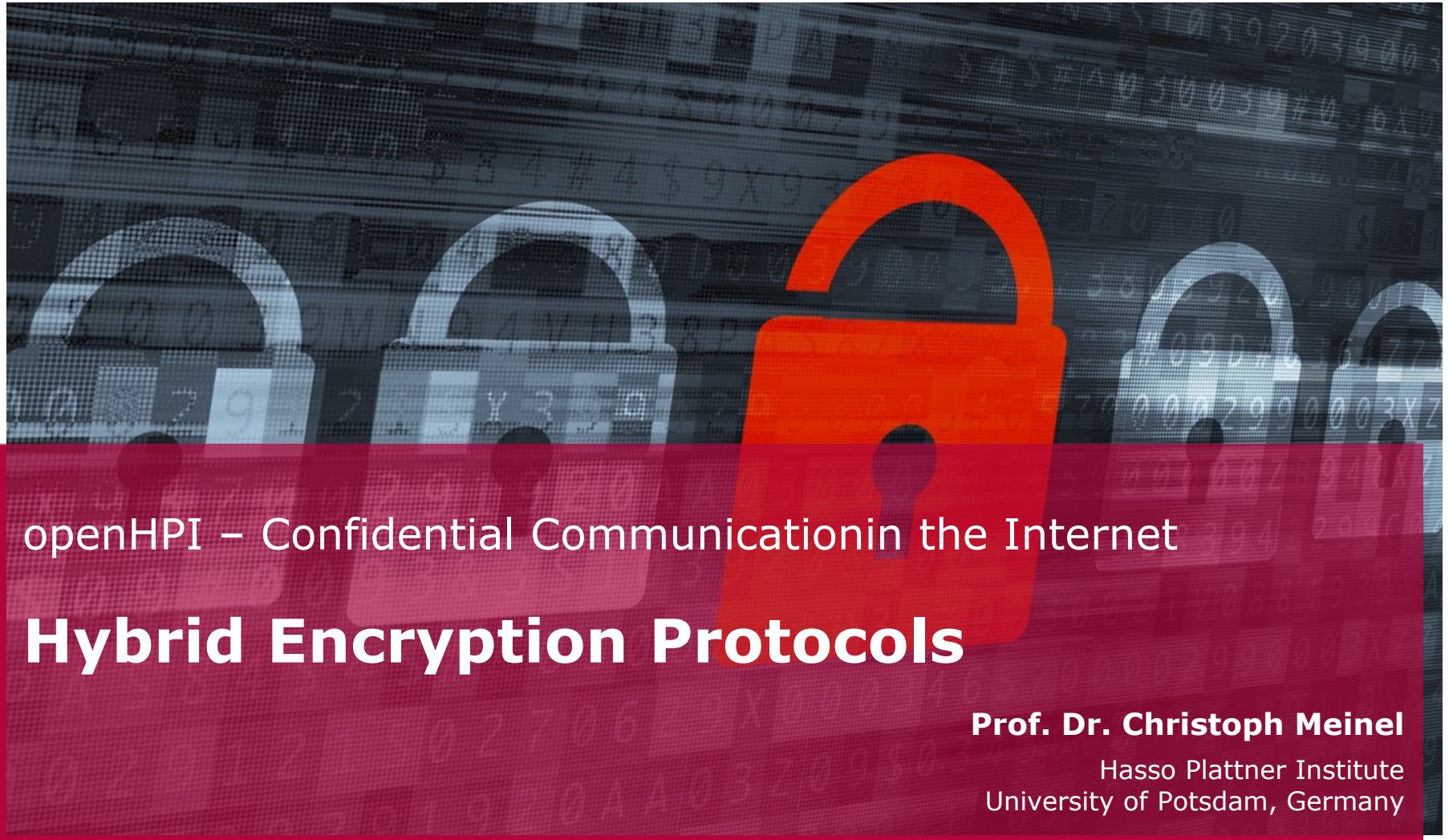

openHPI – Confidential Communicationin the Internet

Hybrid Encryption Protocols

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

Hybrid Encryption Protocols (1/4)

The idea of hybrid encryption protocols is the combine the advantages of the symmetric and asymmetric encryption methods and to avoid their disadvantages

Basic protocol (1/2):

- Alice and Bob agree on a **symmetric cryptosystem** to encrypt the actual message
- Alice generates a **secret session key** for the agreed symmetric cryptosystem
- Alice and Bob agree on a **asymmetric cryptosystem** to **exchange the session key**
- Alice takes the **public key of Bob** to **encrypt** the **session key** with the **public key of Bob** and the agreed **asymmetric cryptosystem**
- …

Hybrid Encryption Protocols (2/4)

Basic protocol (2/2):

- ...
- Alice **encrypts the actual message** with the agreed **symmetric cryptosystem** and the chosen **session key**
- Alice sends Bob the **(asymmetrically) encrypted session key** and the **(symmetrically) encrypted message**
- Bob **decrypts the session key** with **his private key** and the agreed asymmetric cryptosystem
- Bob **decrypts the ciphertext** with the agreed **symmetric cryptosystem** and the retrieved **session key**

Hybrid Encryption Protocols (3/4)

Advantages:

- Secure **secure exchange of the secret key** for the symmetrical encryptions – **solution of the key exchange problem** of symmetric encryptions
- High computational effort of asymmetric encryption is limited to the encryption of short session keys
- Even very long messages can be efficiently encrypted / decrypted with the symmetric encryption method
- Validity period of the session key in the common communication can easily be adapted to security requirements

Hybrid Encryption Protocols (4/4)

Problems:

- **Arrangements (PKI) are needed** to ensure that the correct public keys are used
  - Arrangements needed to use correct **cryptographic algorithms**

Application on the Internet:

- Asymmetric RSA is predominantly used for key exchange together with symmetric TripleDES, IDEA, AES (formerly DES)