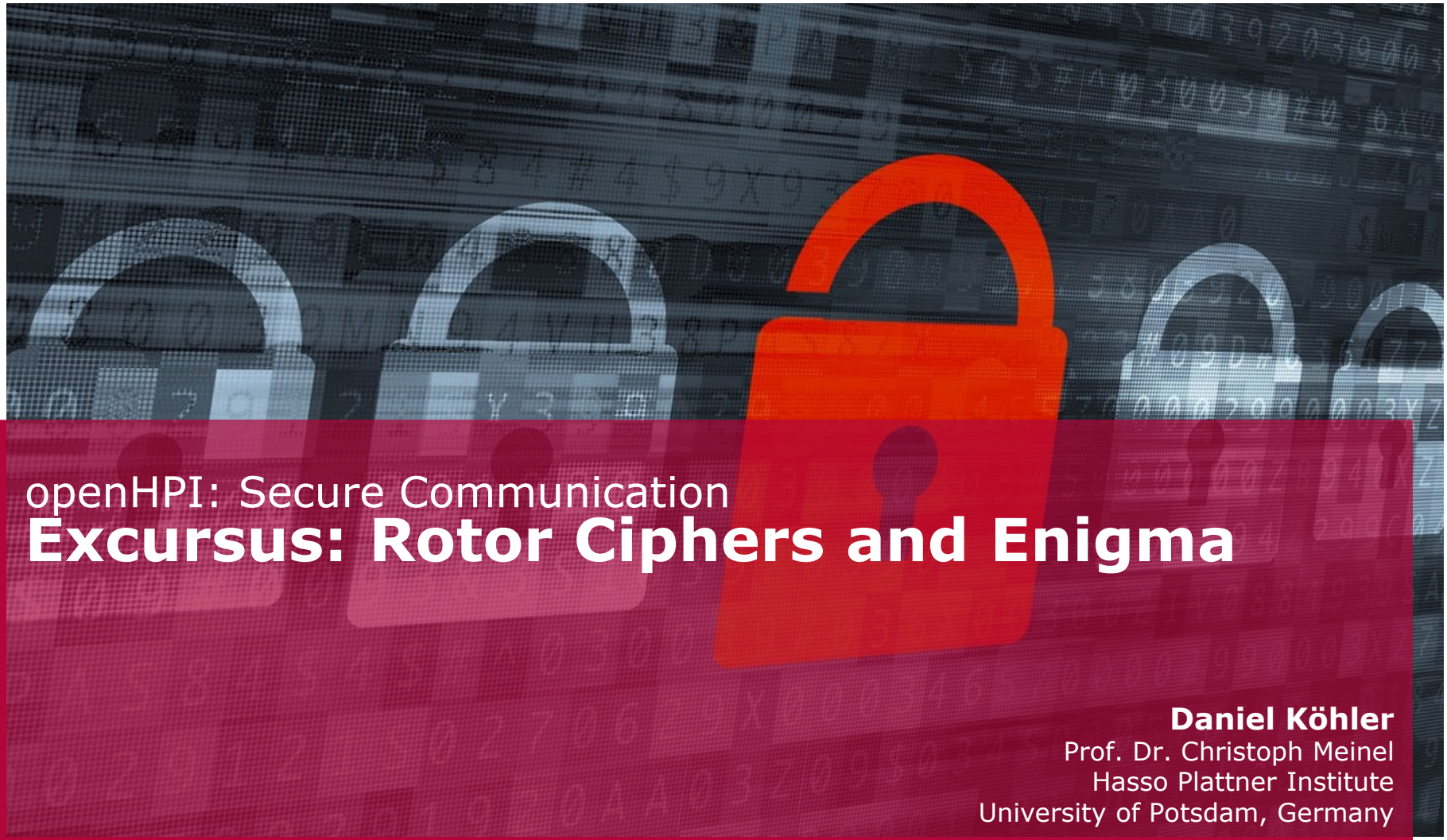

openHPI: Secure Communication

Excursus: Rotor Ciphers and Enigma

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

Rotor Ciphers
Historical Background

Historical facts:

- In the 1st World War, radio messages were encrypted with an improved version of the Vigenère cipher
- Around 1918, the rotor ciphers became independently invented by at least four different inventors
- The most famous representative of the rotor ciphers was the **Enigma** encryption machine used by the German Wehrmacht in the Second World War.

Rotor Ciphers
Function Principle (1/2)

Basic idea of the rotor ciphers (1/2):

- Electromechanical construction:
  - Rotor 1 rotates one position after each letter
  - After one full rotation, next rotor moves one position further
- Rotor ciphers are therefore **polyalphabetic substitution ciphers**:
  - Each letter is encoded according to a different scheme until the last rotor has completed its rotation

Rotor Ciphers
Function Principle (2/2)

Basic idea of the rotor ciphers (2/2):

- Code is only repeated after the last rotor has made a full turn, i.e. after 26^n with n = number of rotors
- Key of a rotor cipher: **Initial position of the rotors**
- Number of keys: 26^n e.g. 26^3 for n = 3 : 17,576
- Number of keys can be drastically increased by replacing the rotors e.g. choose 3 from 5 rotors

$$\binom{5}{3} 3! \times 26^3 = 60 \times 26^3 > 1{,}000{,}000$$

Rotor Ciphers
Example: Enigma (1/3)

Enigma:

- Inventor (1918): Arthur Scherbius
  - Patented in 1926
  - Enigma means "secret" in Greek
- First equipped with three rotors, later a fourth rotor was added
- Behind the last rotor there was still an immovable rotor, the **Reflector**
  - Was used to make sure that a letter from the original text would not correspond to the same letter in the ciphertext

Rotor Ciphers
Example: Enigma (2/3)

History of cryptanalysis of the Enigma (1/2):

- One of the most exciting stories in cryptography ever
- Was of strategic importance for the course and duration of the **Second World War** ...
- Was operated under the strictest secrecy (until 1974!) under industrial conditions (7,000 employees) in a shielded campus - Bletchley Park near London - to decode German radio messages
- Dealing with the Enigma's cryptanalysis has greatly advanced the development of the first computers

Rotor Ciphers
Example: Enigma (3/3)

History of cryptanalysis of the Enigma (2/2):

Errors on the German side during use and espionage helped the cryptanalysts, e.g:

- Consistent news items, fixed formats
- Weather forecasts: Sending the same messages with different keys (rotor positions)
- Looting of valid codebooks, rotors, enigmas
  (e.g. looting of a submarine in 1941 including Enigma and valid key book)
- "*Design weakness*": use of the reflector