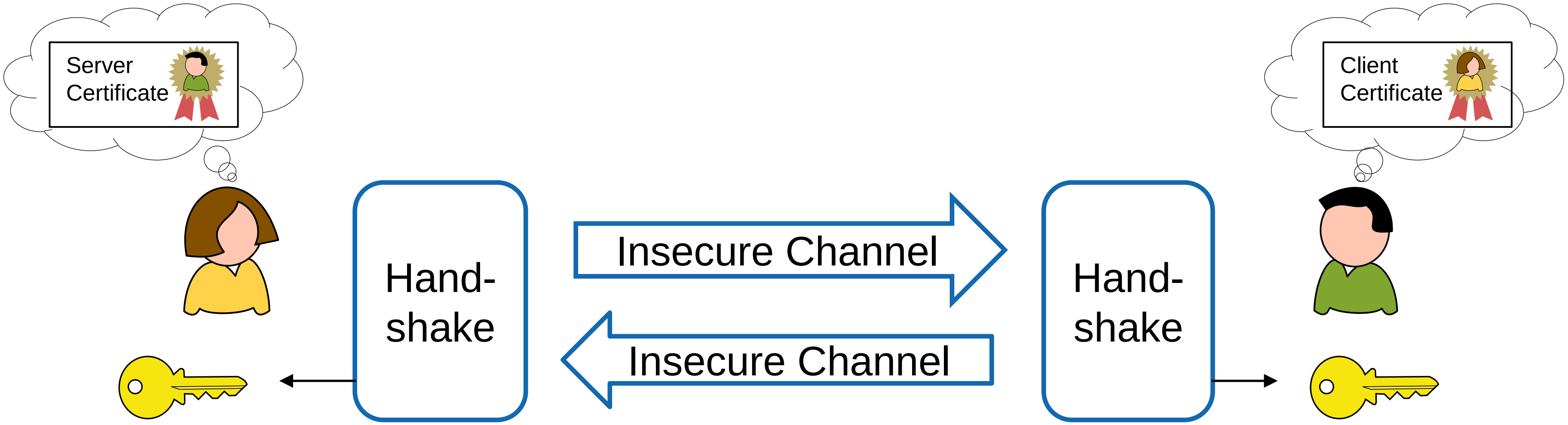
Augmented Secure Channels and the Goal of the TLS 1.3 Record Layer

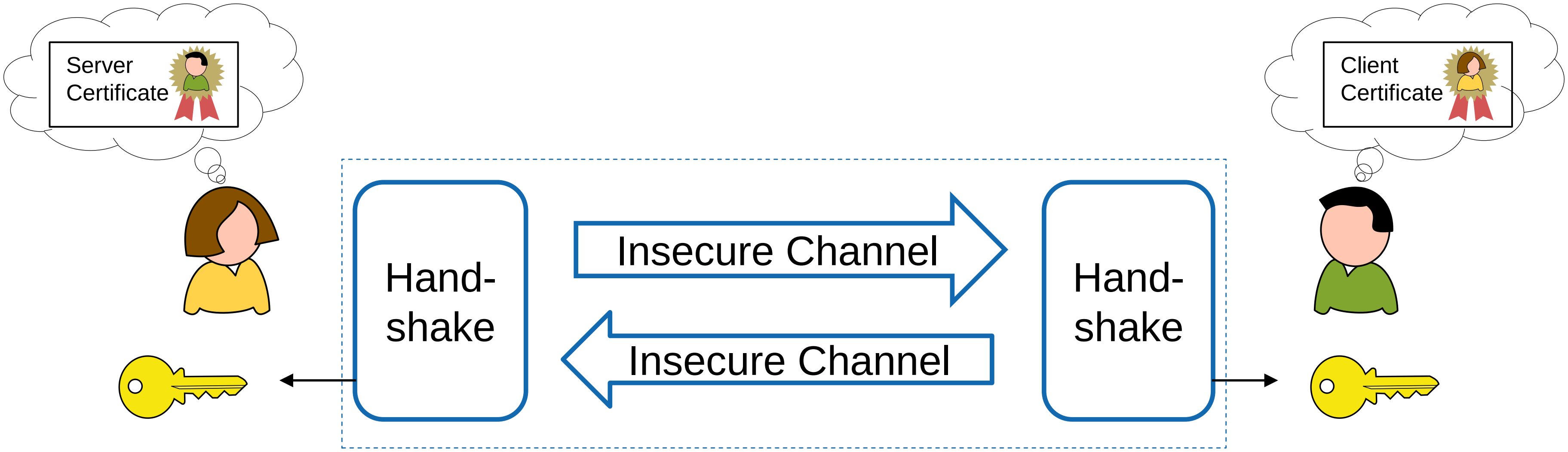
Christian Badertscher[1], Christian Matt[1], Ueli Maurer[1],
Phil Rogaway[2], Björn Tackmann[3]

[1]ETH Zurich, [2]UC Davis, [3]UC San Diego

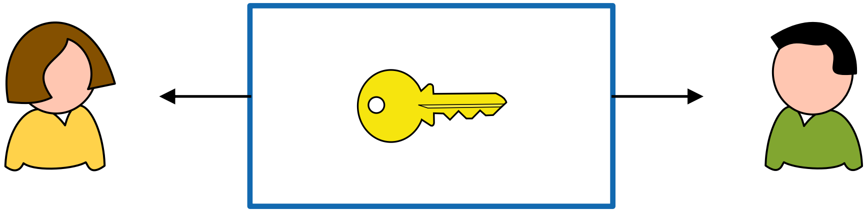
The Handshake of TLS 1.3



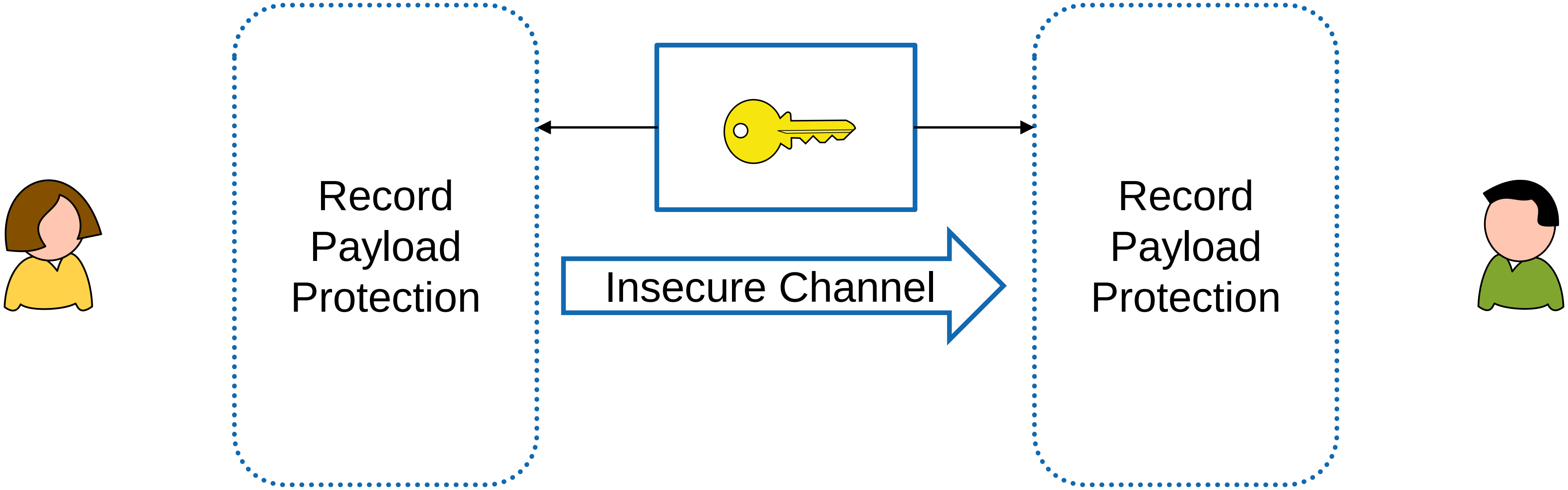
The Handshake of TLS 1.3



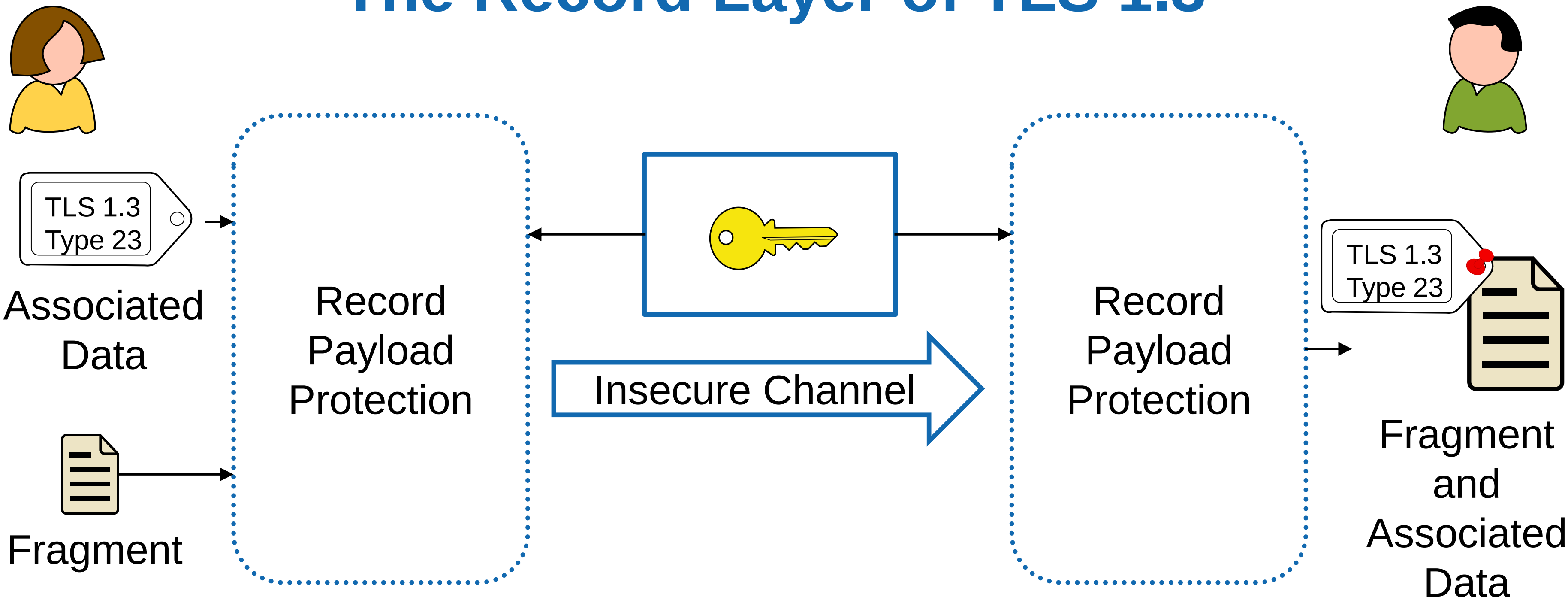
Ideal abstraction of the handshake [DFG15, KMO14]:
A shared key resource



The Record Layer of TLS 1.3



The Record Layer of TLS 1.3



TLS 1.3 Type 23

Associated Data

Fragment

Record Payload Protection

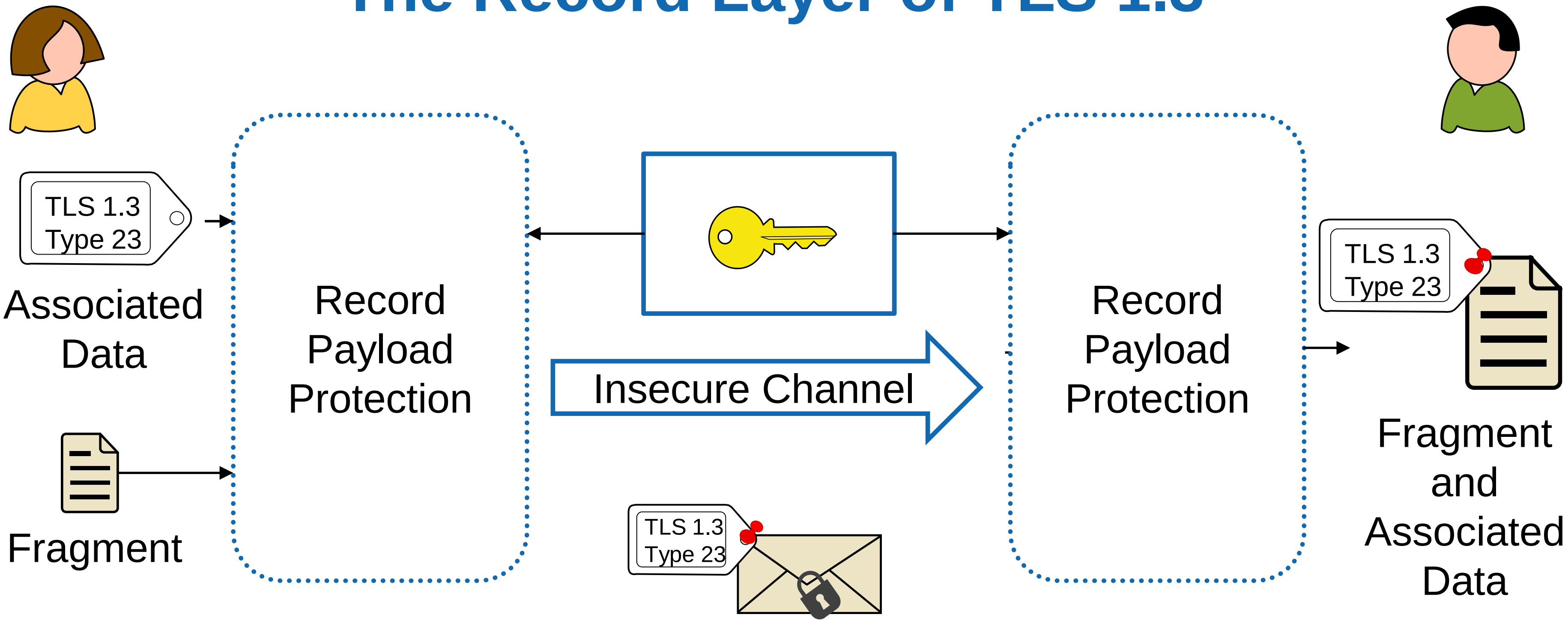
Insecure Channel

Record Payload Protection

TLS 1.3 Type 23

Fragment and Associated Data

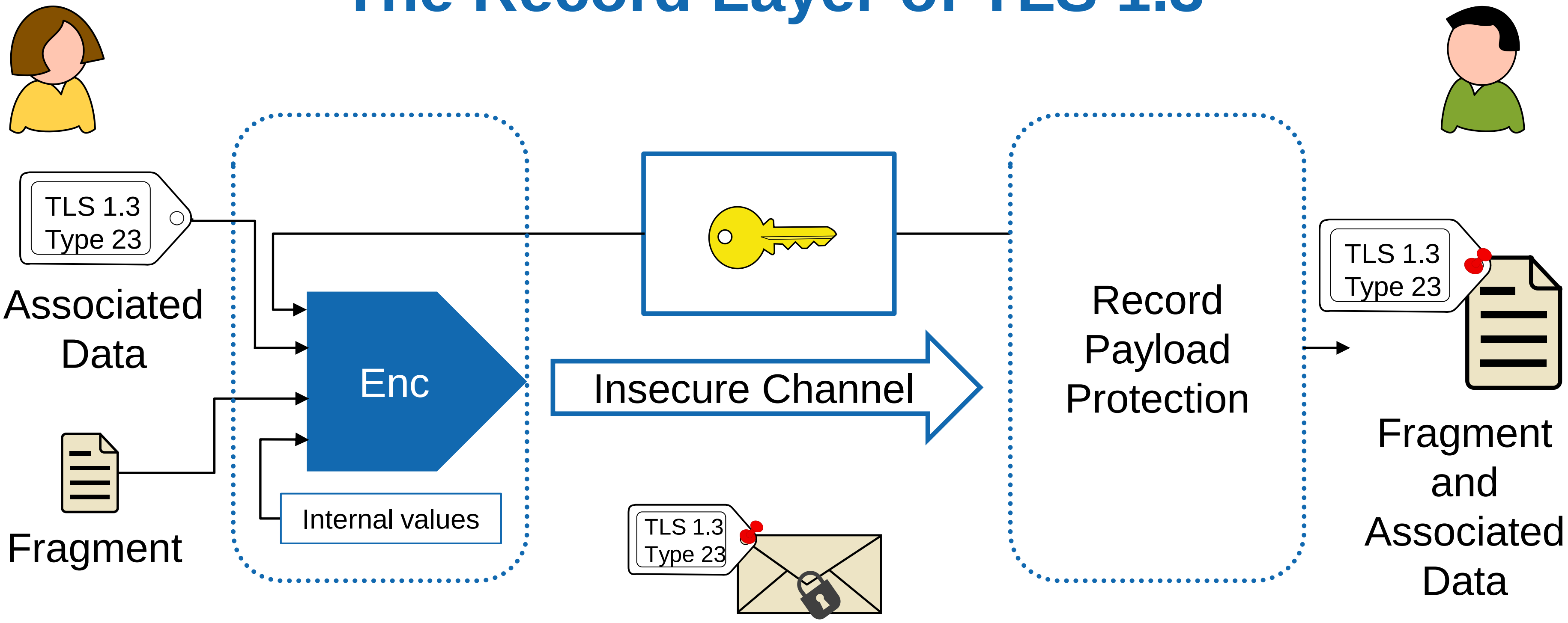
The Record Layer of TLS 1.3



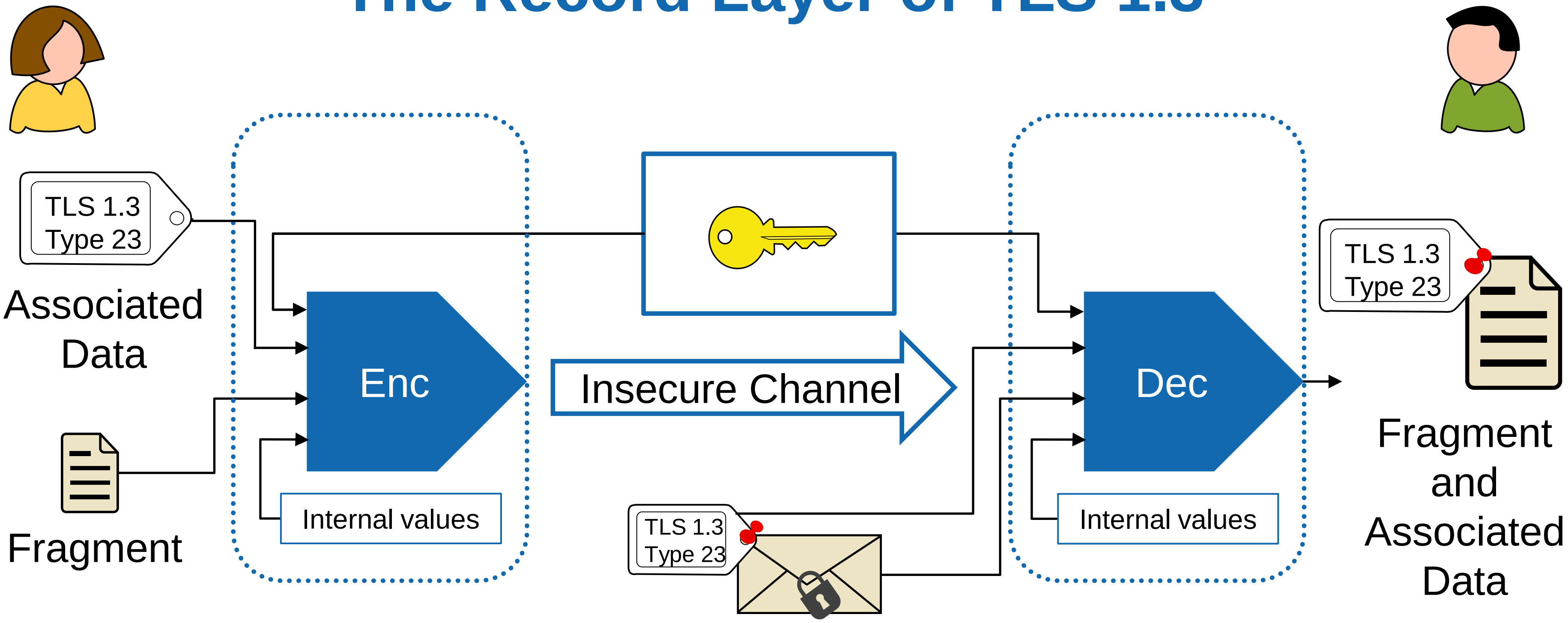
Structure of transmitted packets:

- Non-private header
- Private payload
- Both parts are authentic

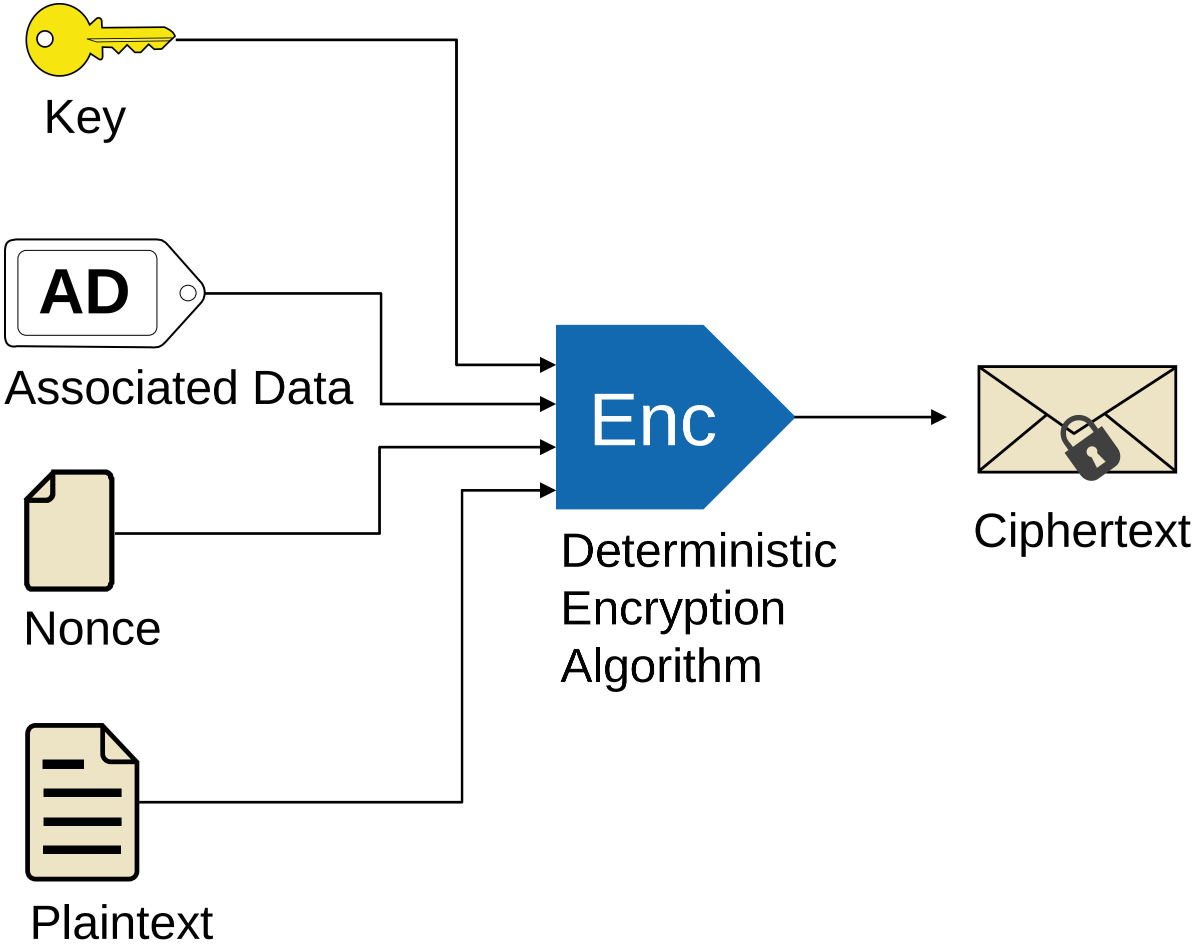
The Record Layer of TLS 1.3



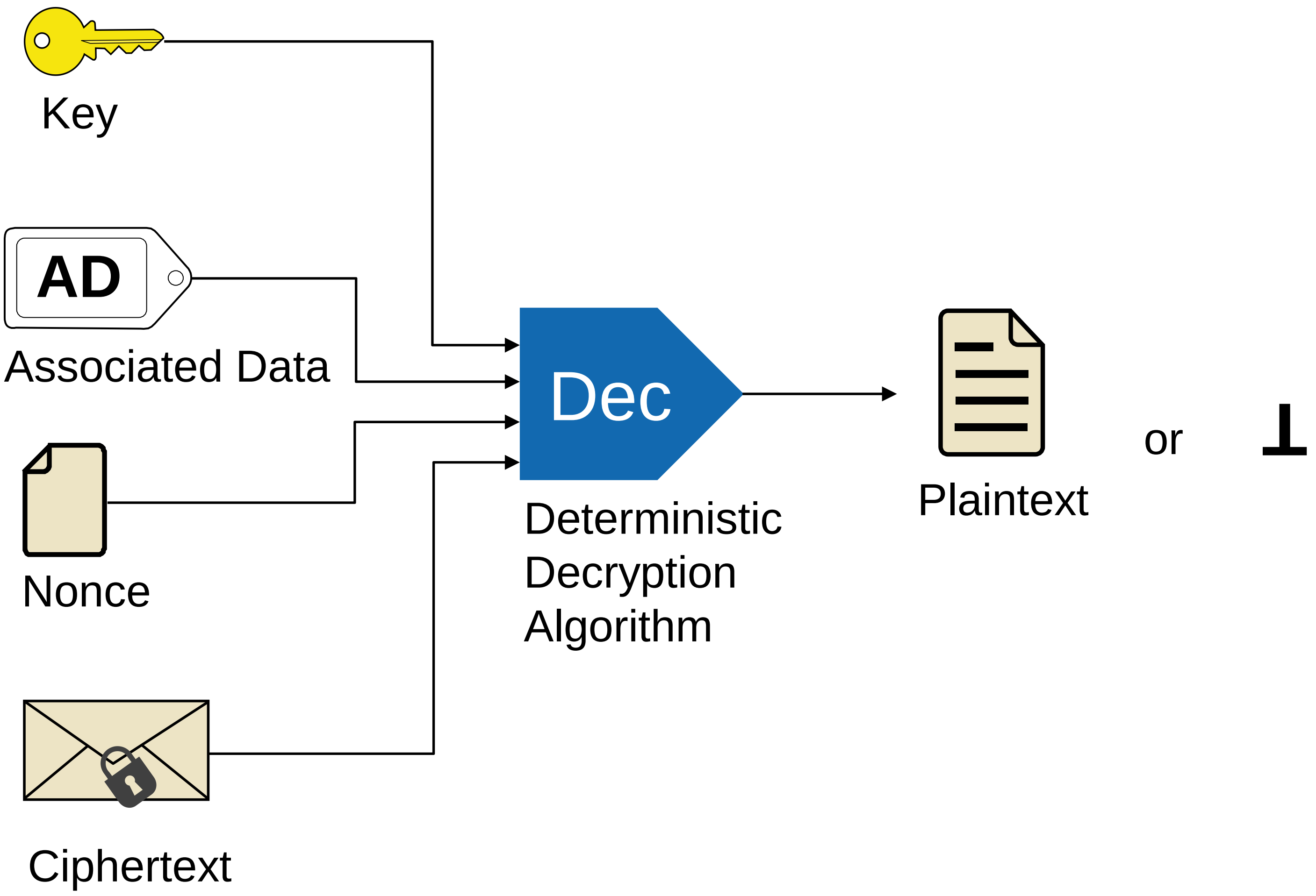
The Record Layer of TLS 1.3



Authenticated Encryption with Associated Data



Authenticated Encryption with Associated Data



Key

AD

Associated Data

Nonce

Ciphertext

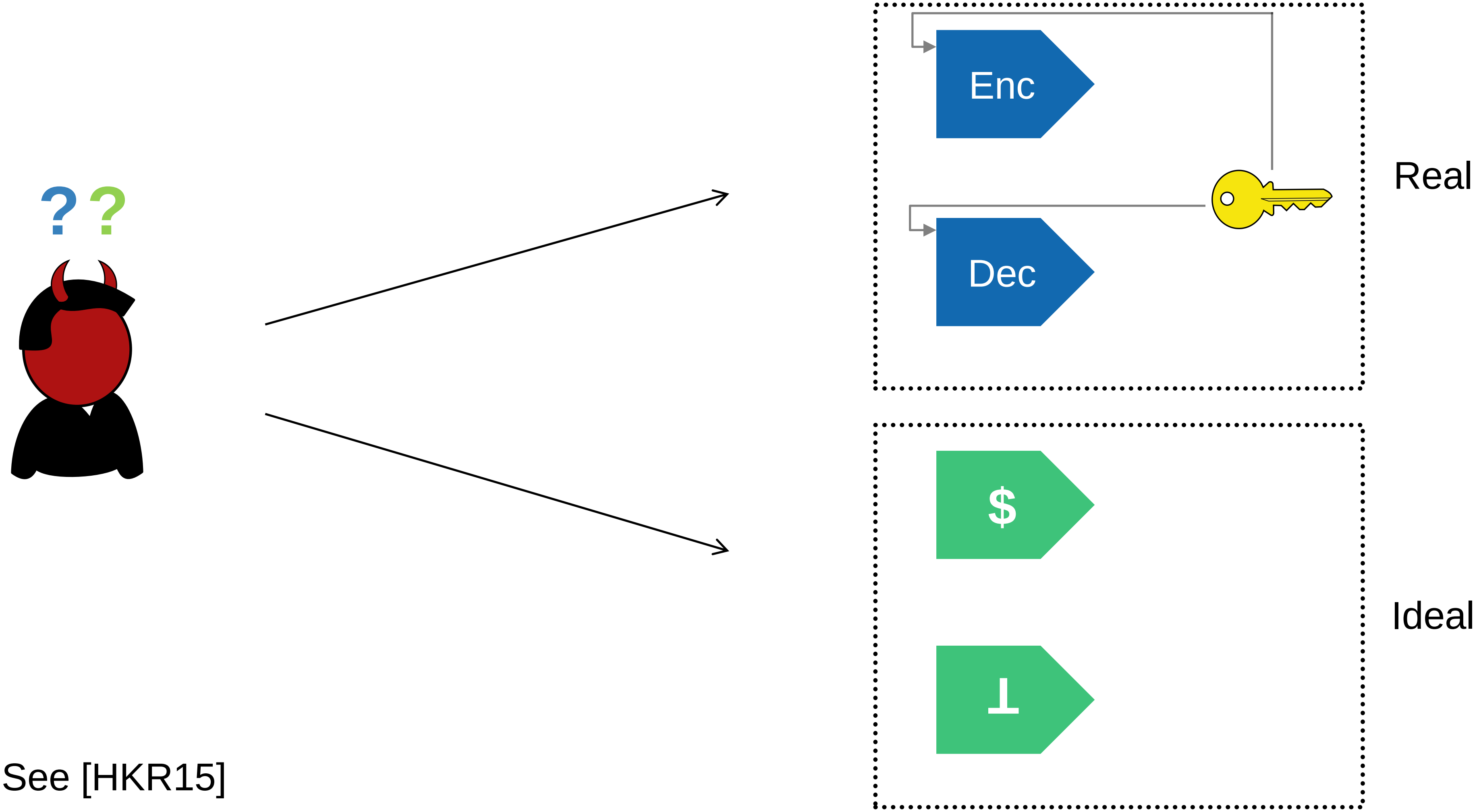
Dec

Deterministic Decryption Algorithm

Plaintext

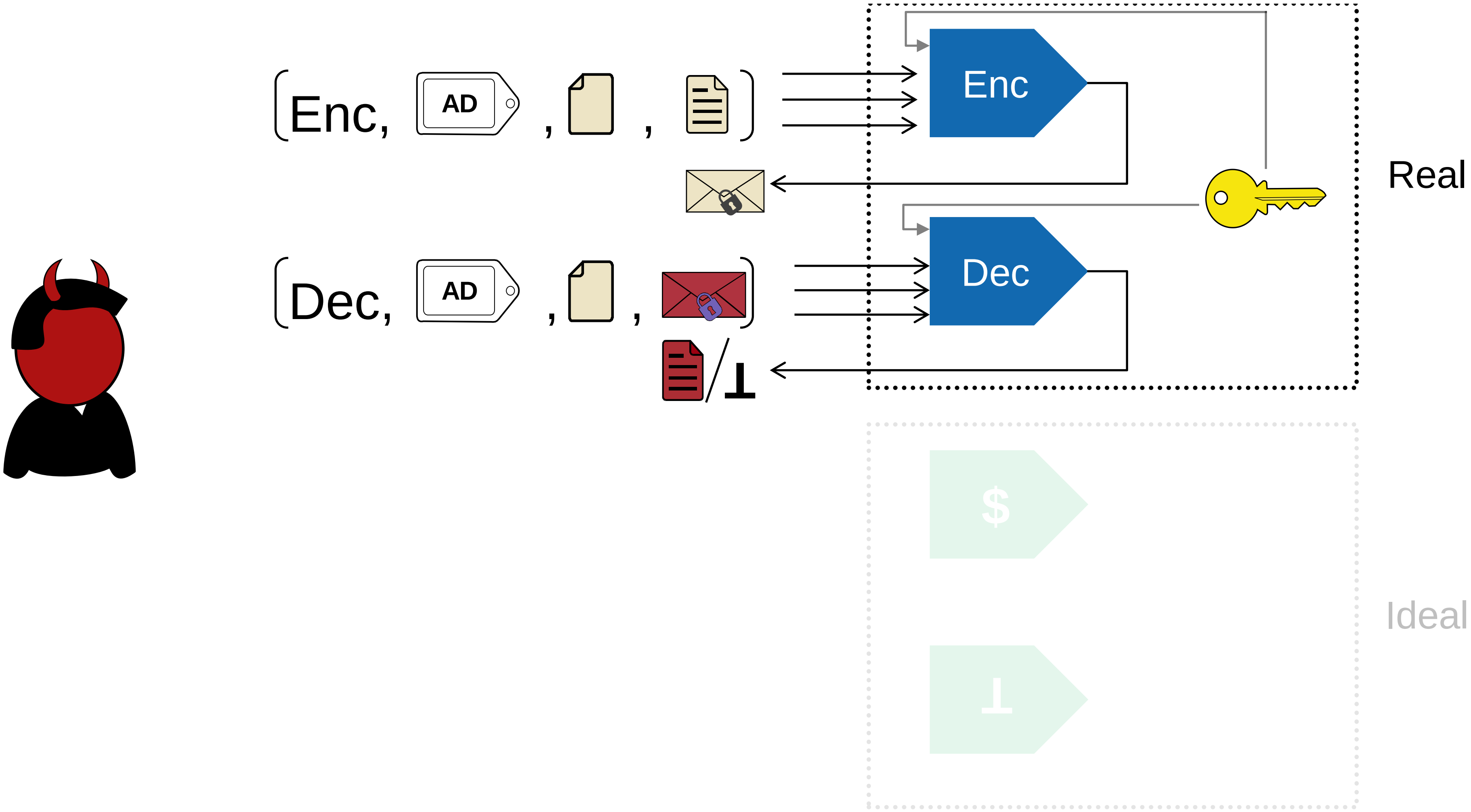
or $\perp$

AEAD Security Game

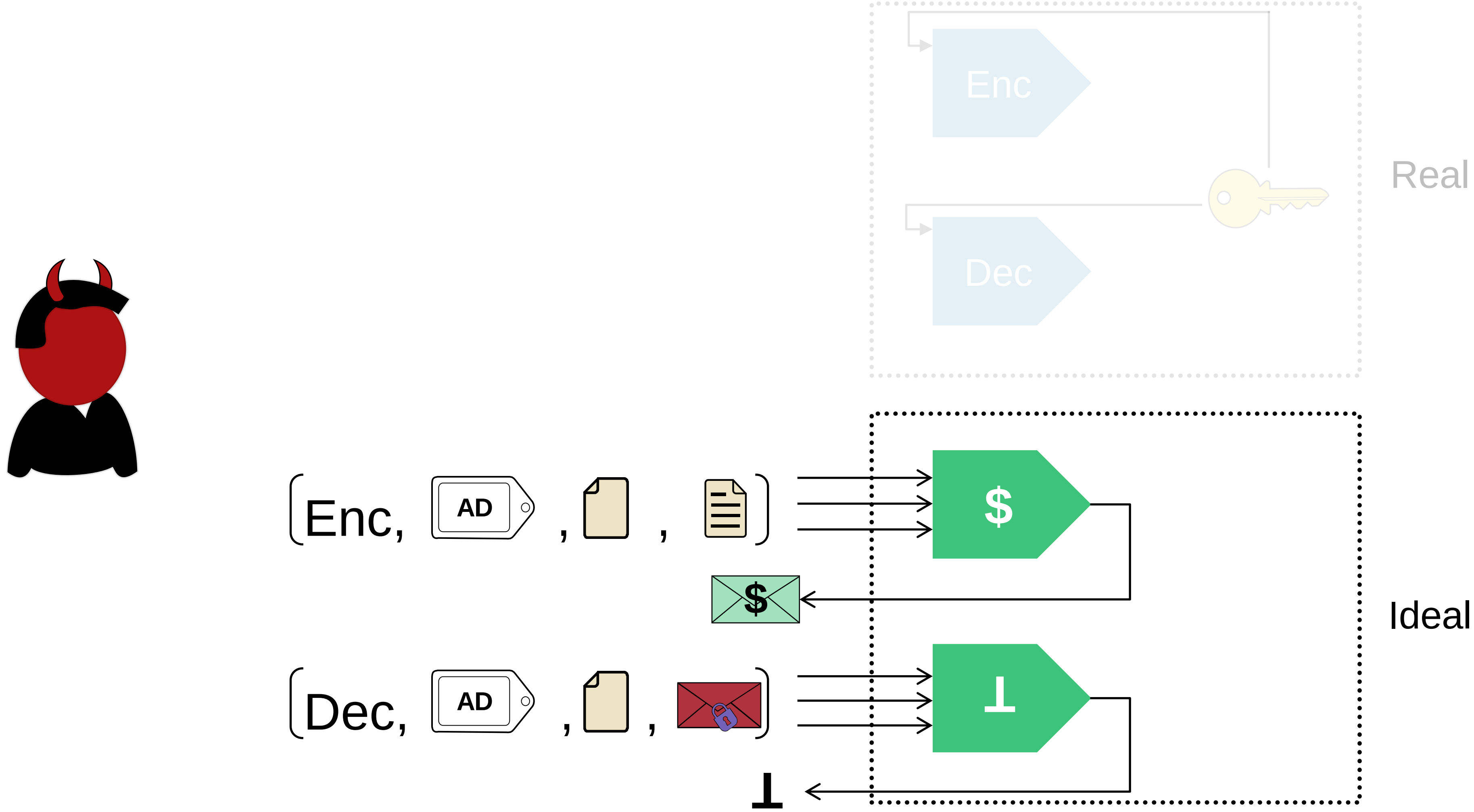


See [HKR15]

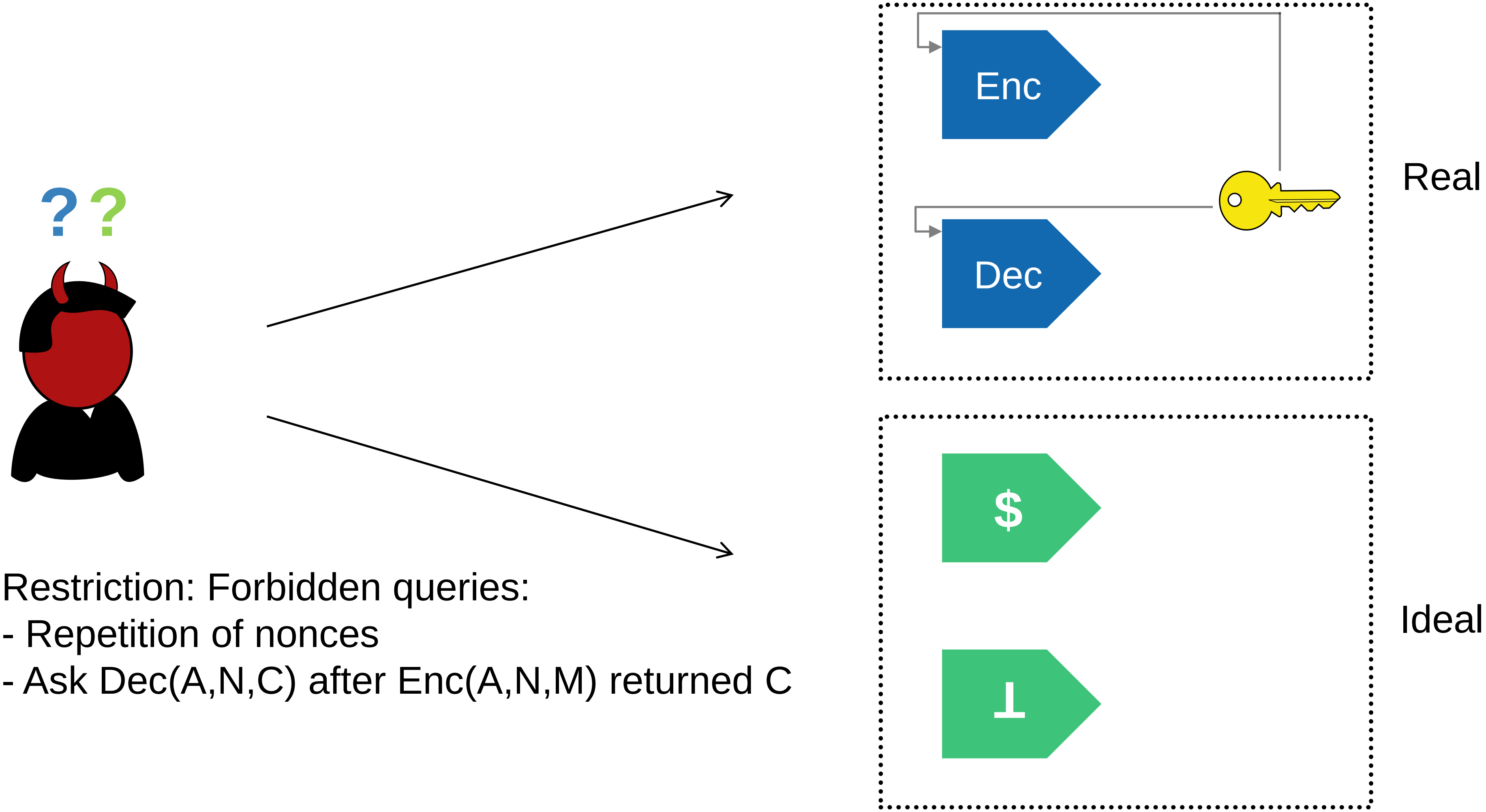
AEAD Security Game



AEAD Security Game



AEAD Security Game

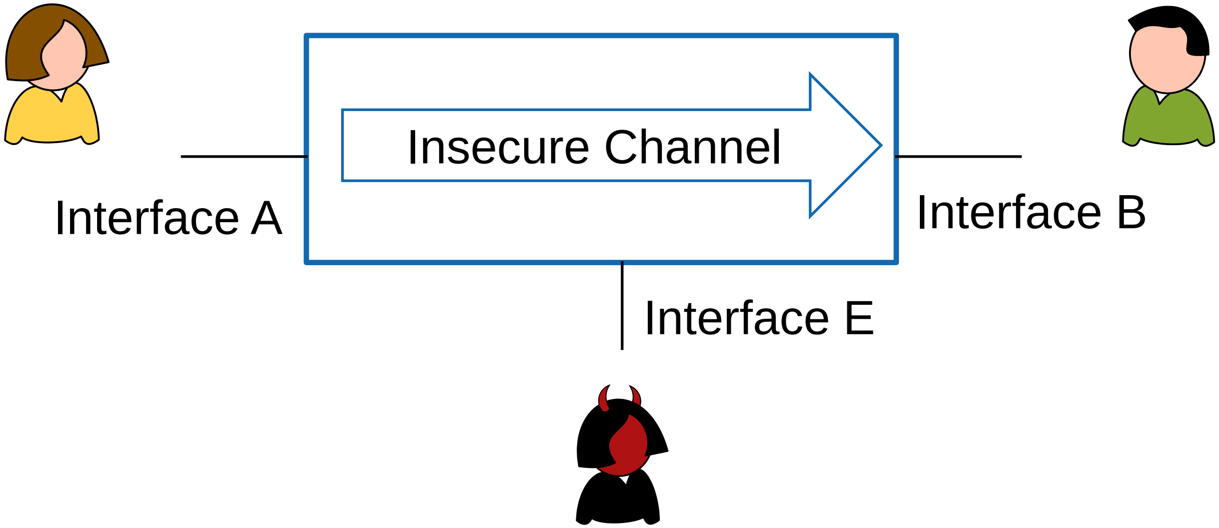


Restriction: Forbidden queries:
- Repetition of nonces
- Ask Dec(A,N,C) after Enc(A,N,M) returned C

Roadmap

- We formulate application-centric security guarantees of AEAD
- We derive a method to judge the security of TLS proposals
- This method can be used to improve existing proposals

Modeling Communication



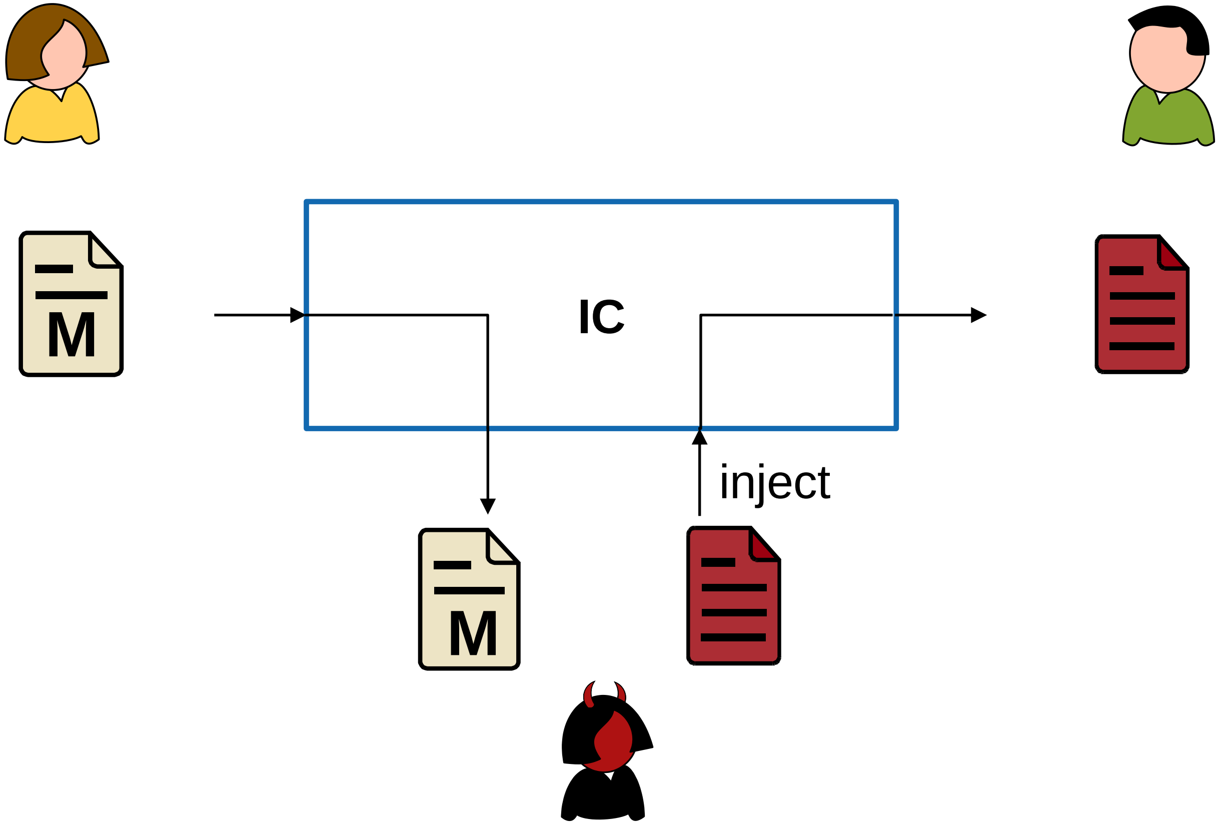
Insecure Channel

Interface A

Interface B

Interface E

Modeling Communication



What Features should a Secure Channel have?

What Features should a Secure Channel have?

Structure of Packets:

- Header and payload part
  - Header: Version number, type information; Payload: message fragments

What Features should a Secure Channel have?

Structure of Packets:

- Header and payload part
  - Header: Version number, type information; Payload: message fragments

Security requirements:

- Payload is confidential
- Entire packet is authenticated
- Each packet is bound to a certain context
  - E.g.: Version number of the protocol

What Features should a Secure Channel have?

Structure of Packets:

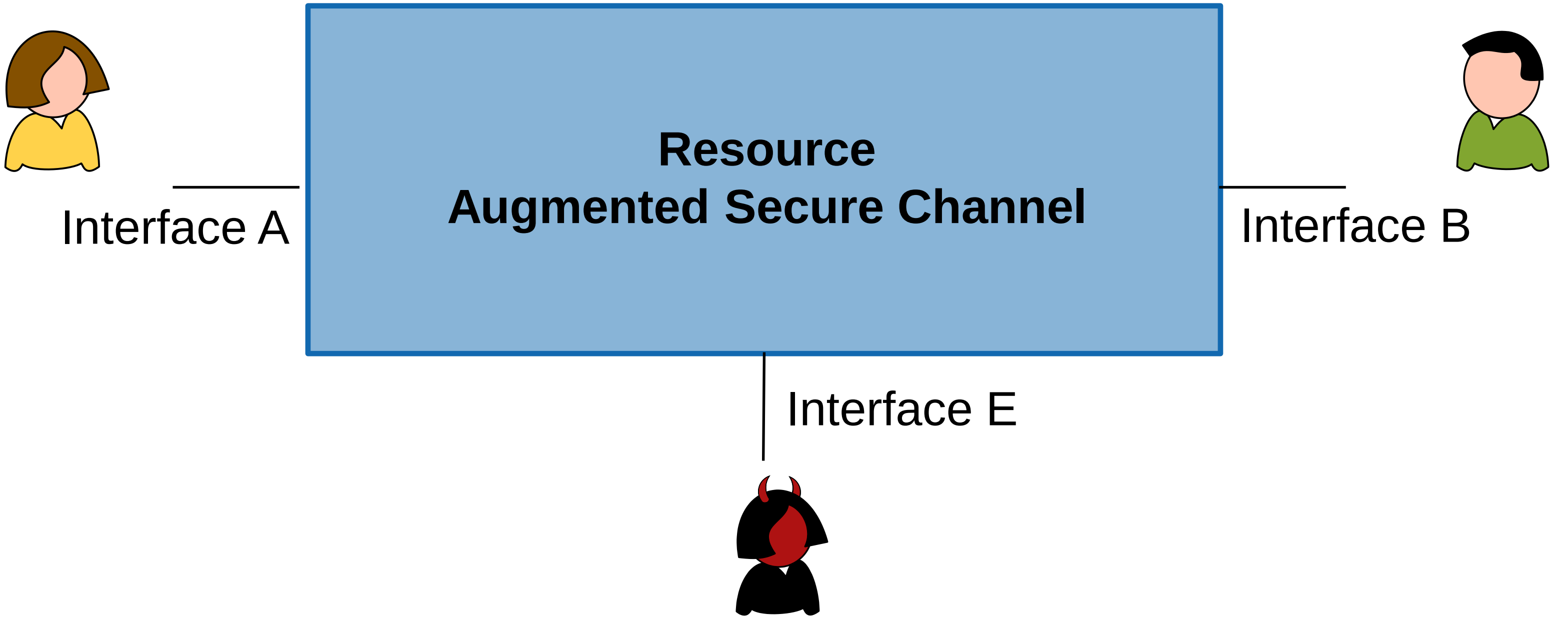
- Header and payload part
  - Header: Version number, type information; Payload: message fragments

Security requirements:

- Payload is confidential
- Entire packet is authenticated
- Each packet is bound to a certain context
  - E.g.: Version number of the protocol

Let us model this as an idealized channel resource!

Augmented Secure Channel



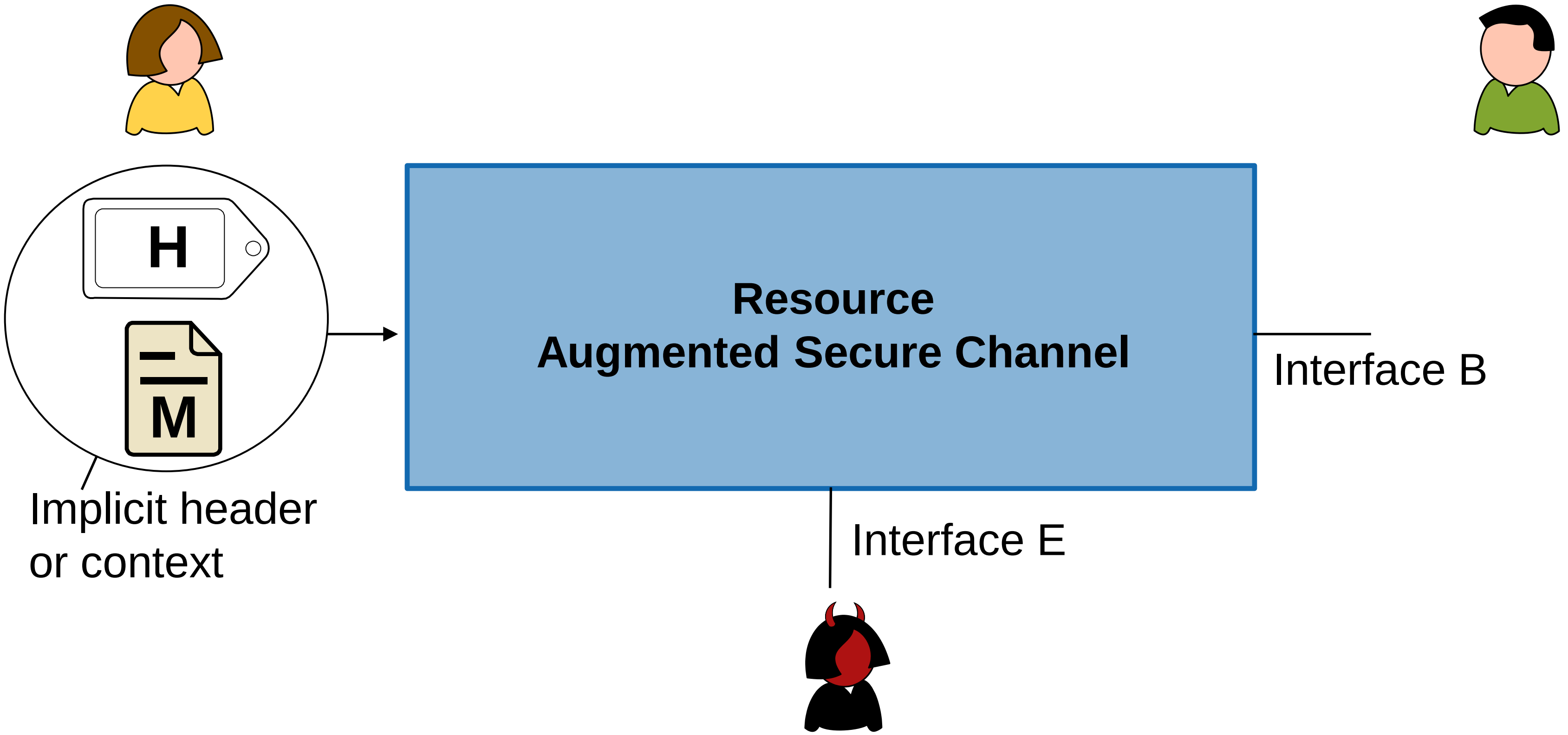
Resource
Augmented Secure Channel

Interface A

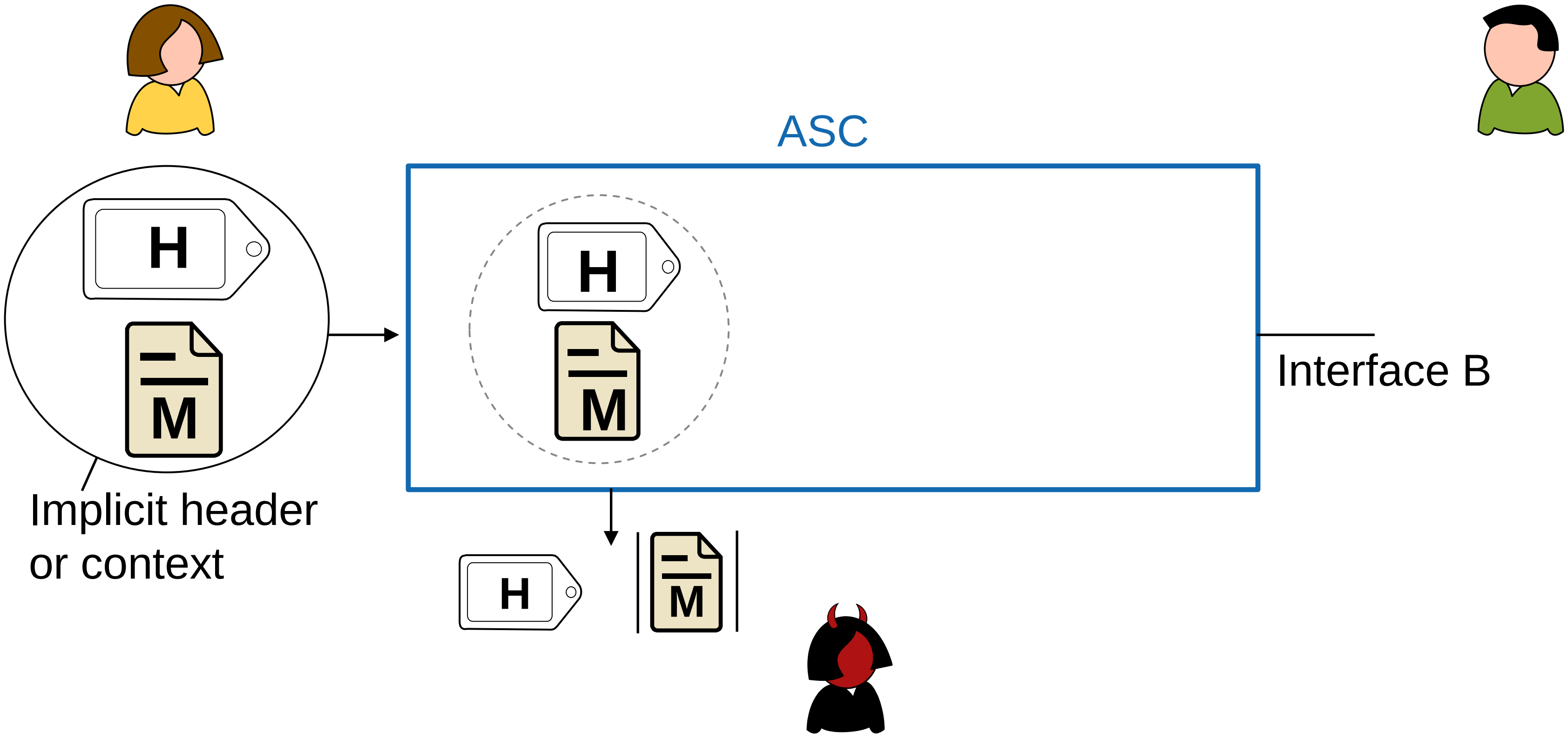
Interface B

Interface E

Augmented Secure Channel



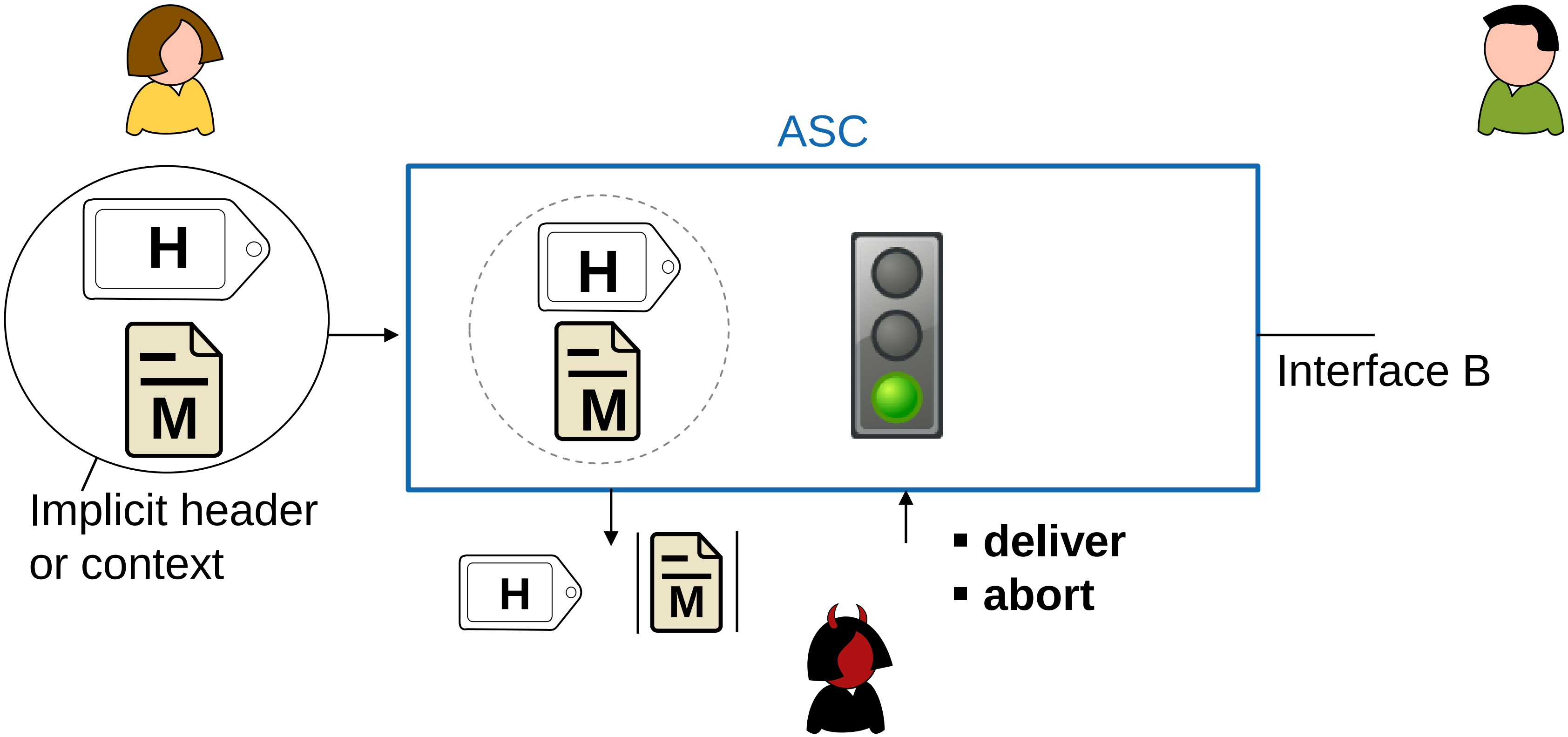
Augmented Secure Channel



Interface B

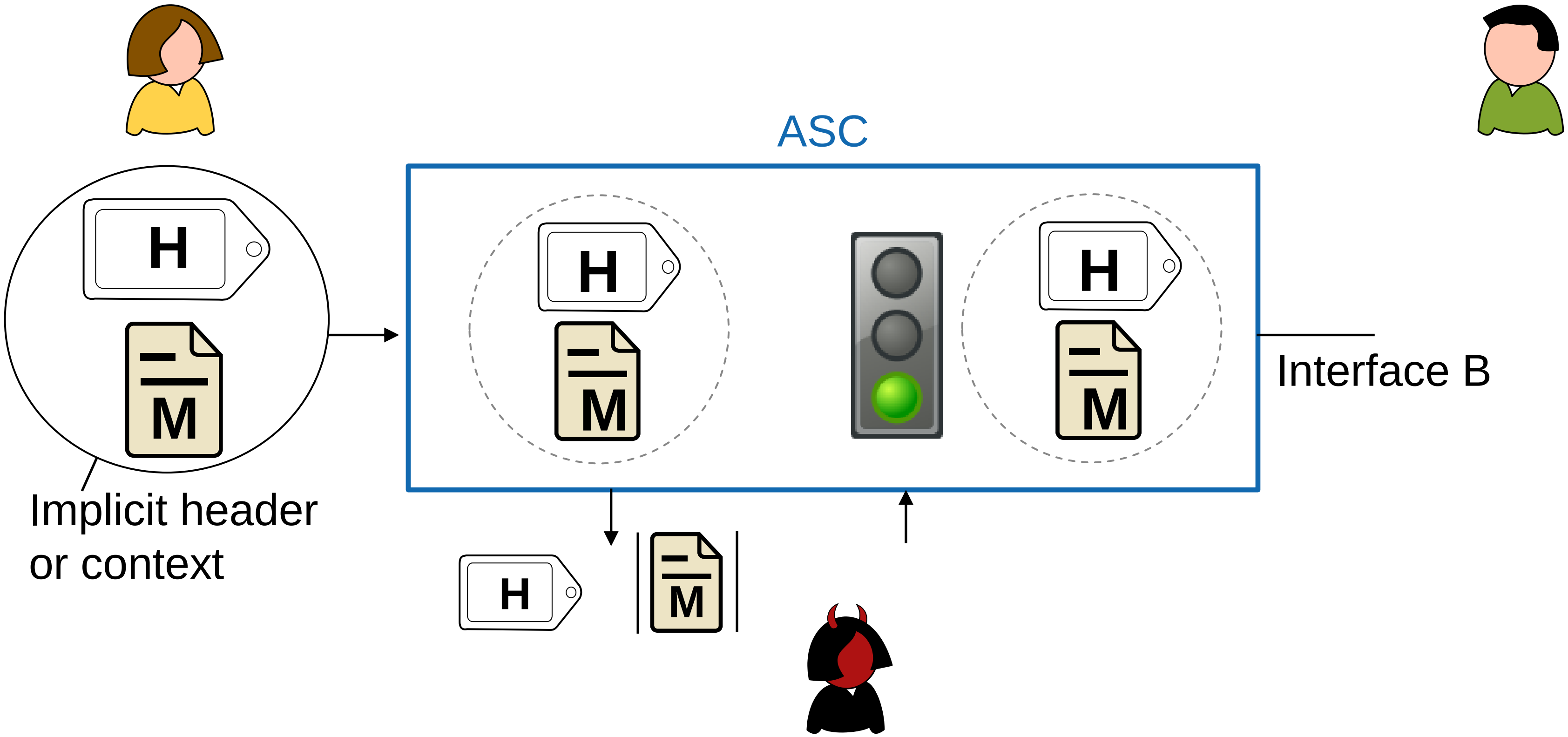
Implicit header or context

Augmented Secure Channel

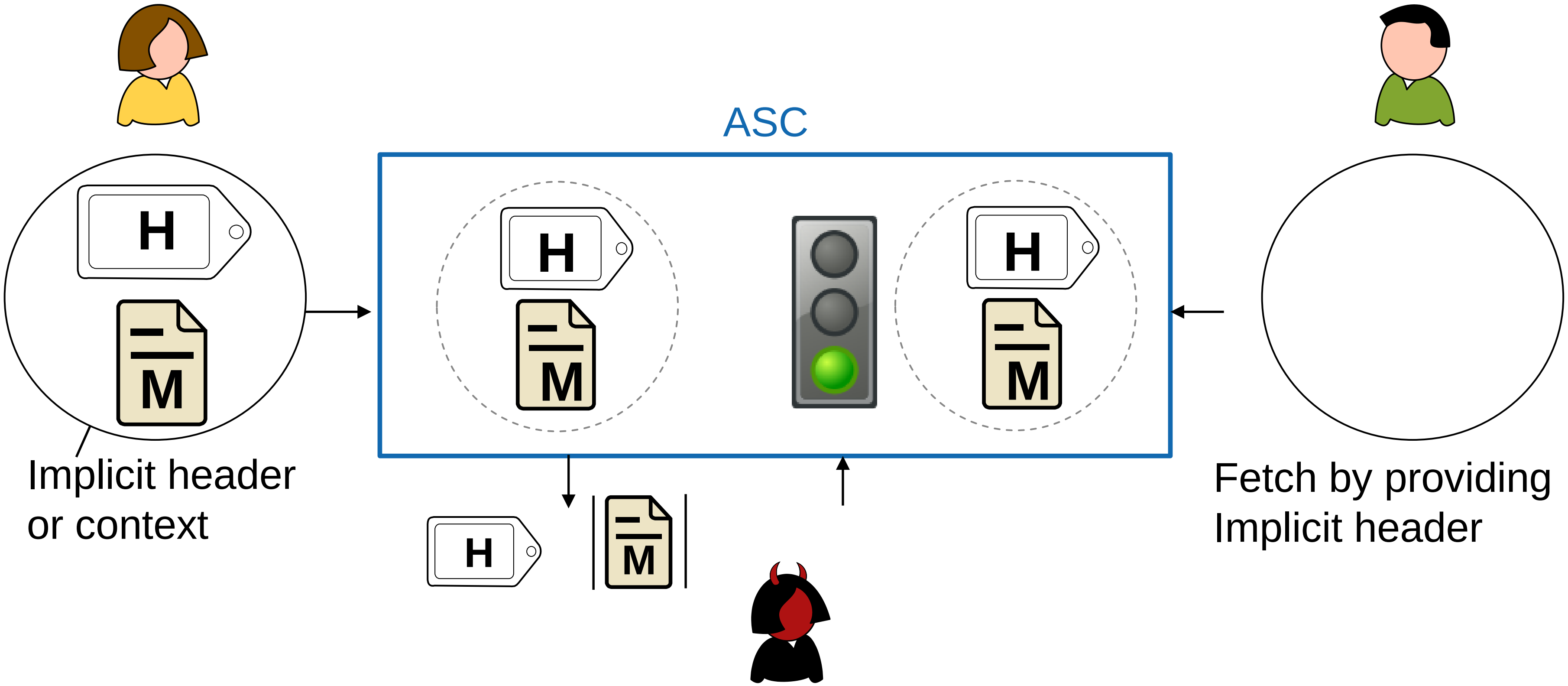


- **deliver**
- **abort**

Augmented Secure Channel



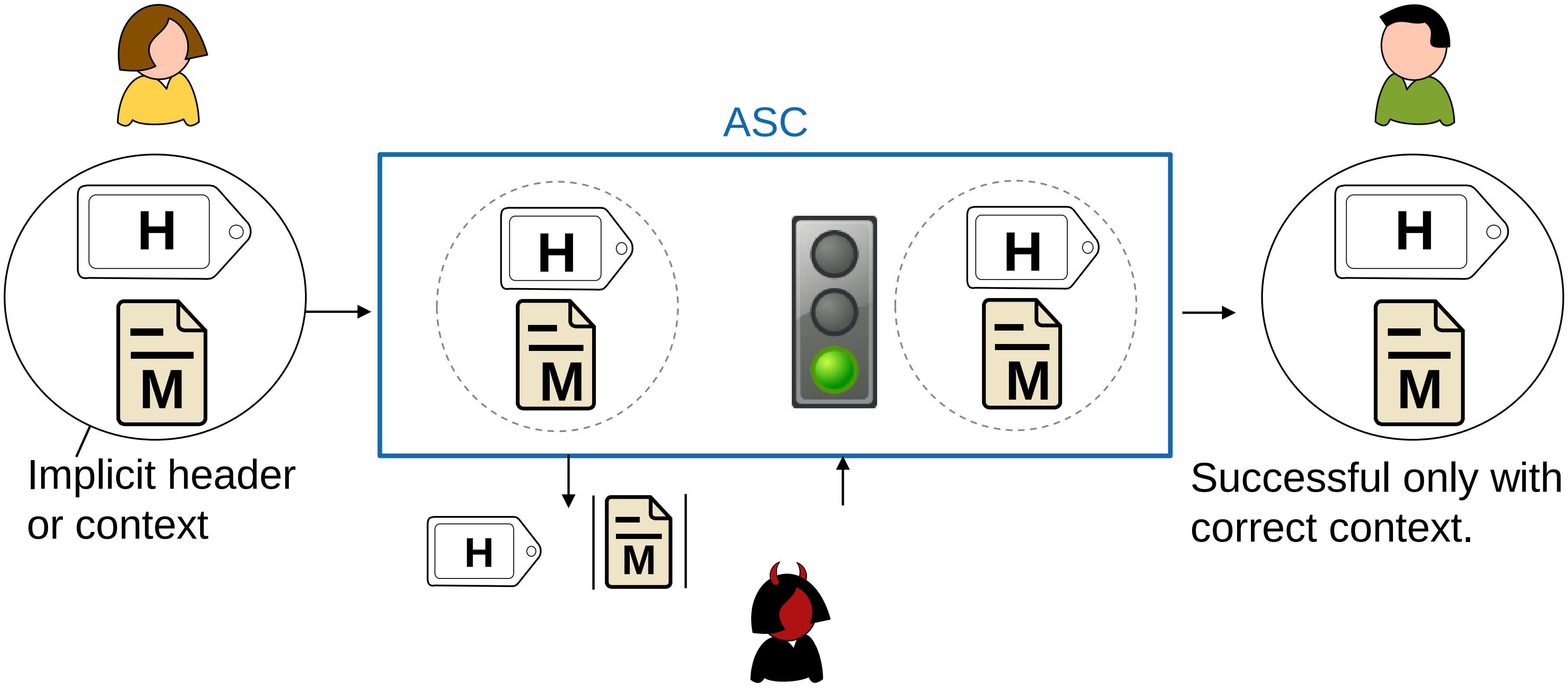
Augmented Secure Channel



Implicit header or context

Fetch by providing Implicit header

Augmented Secure Channel



Implicit header or context

Successful only with correct context.

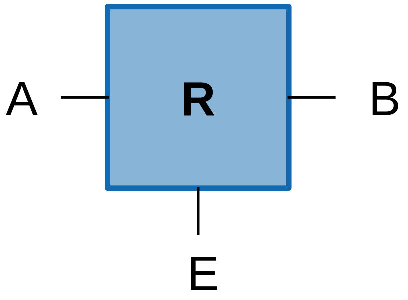
Constructing the Augmented Secure Channel

- The construction notion of constructive cryptography [MR11, Mau11]:

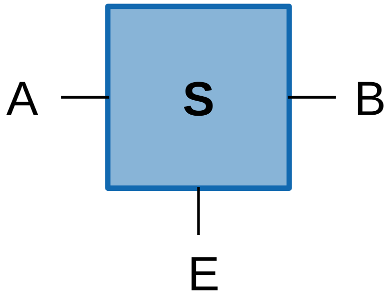
Constructing the Augmented Secure Channel

- The construction notion of constructive cryptography [MR11, Mau11]:

The real world:

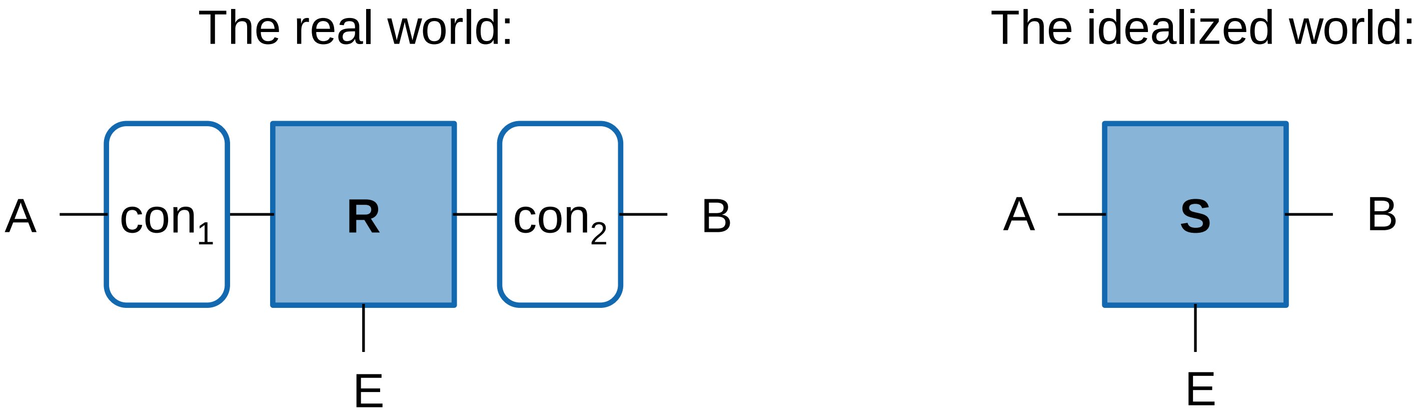


The idealized world:



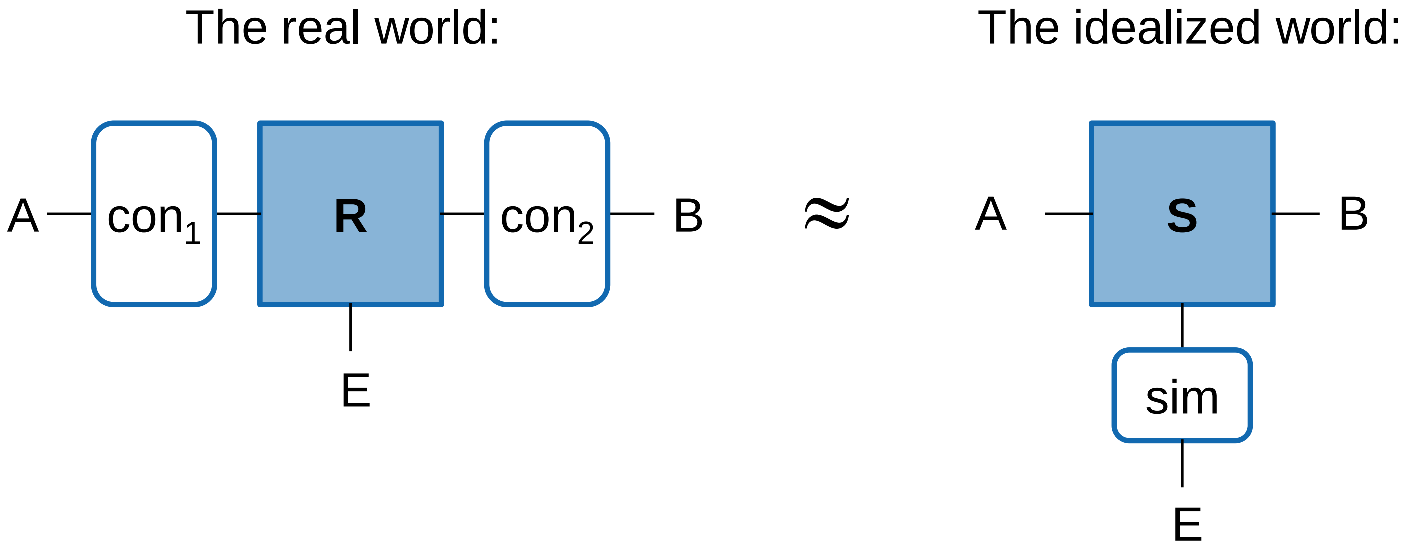
Constructing the Augmented Secure Channel

- The construction notion of constructive cryptography [MR11, Mau11]:



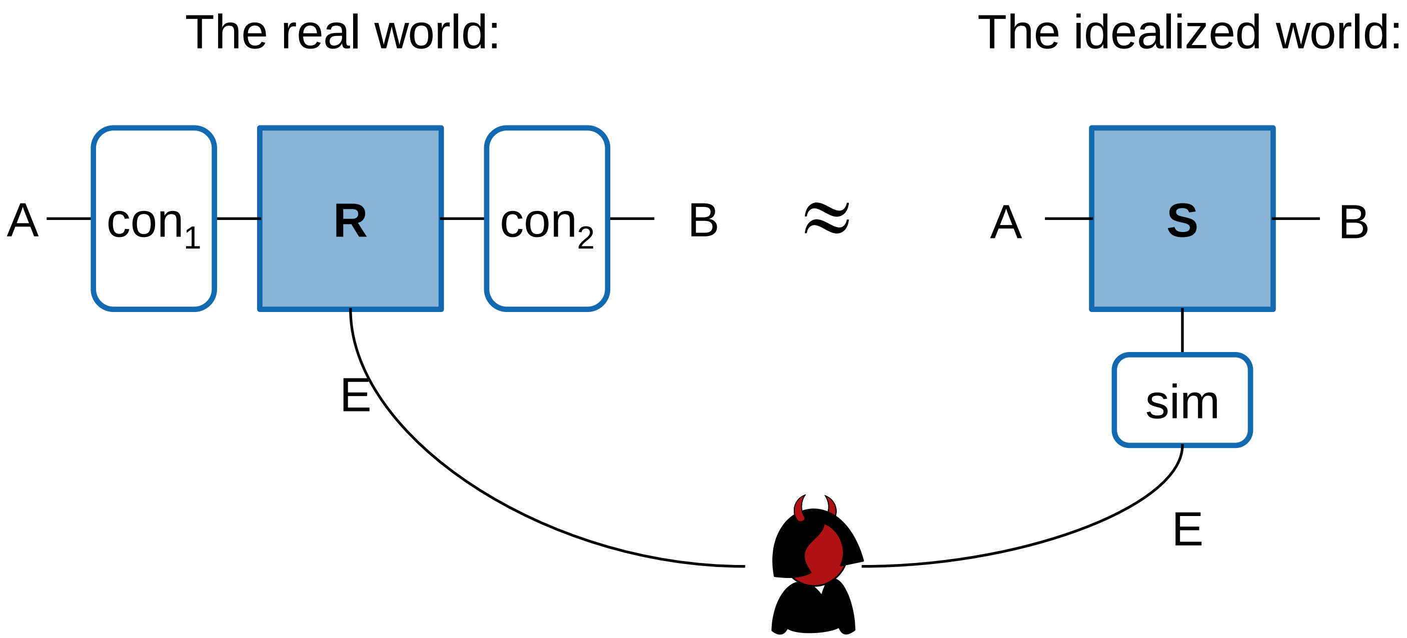
Constructing the Augmented Secure Channel

- The construction notion of constructive cryptography [MR11, Mau11]:



Constructing the Augmented Secure Channel

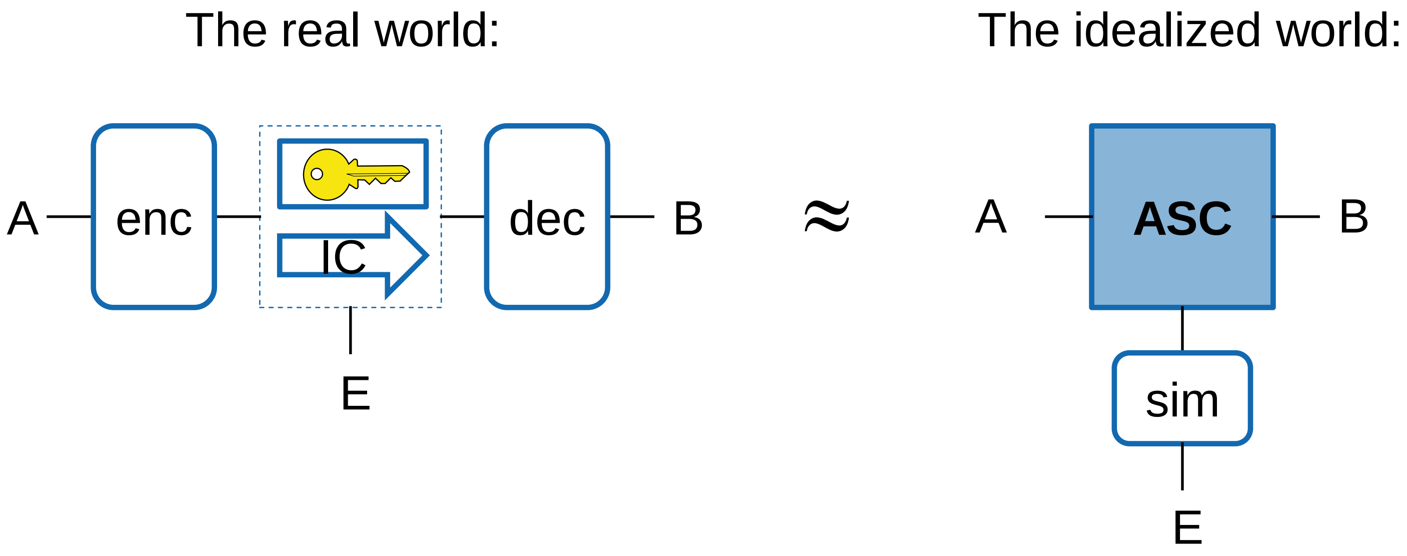
- The construction notion of constructive cryptography [MR11, Mau11]:



Adversarial influence is essentially the same
in both worlds

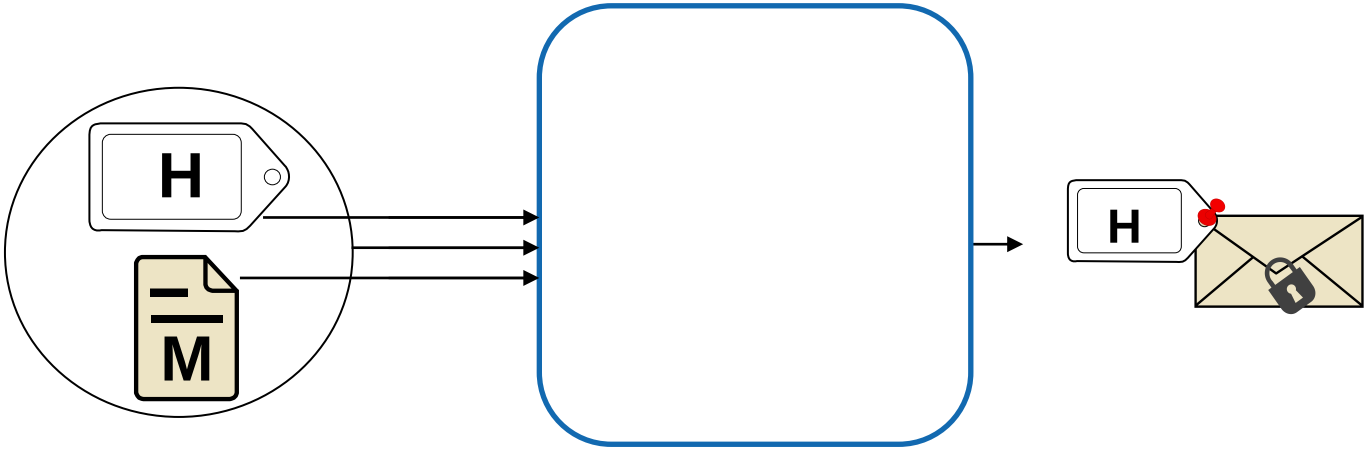
Constructing the Augmented Secure Channel

Theorem: *Resource ASC can be constructed from a shared key and an insecure channel using a secure AEAD scheme:*



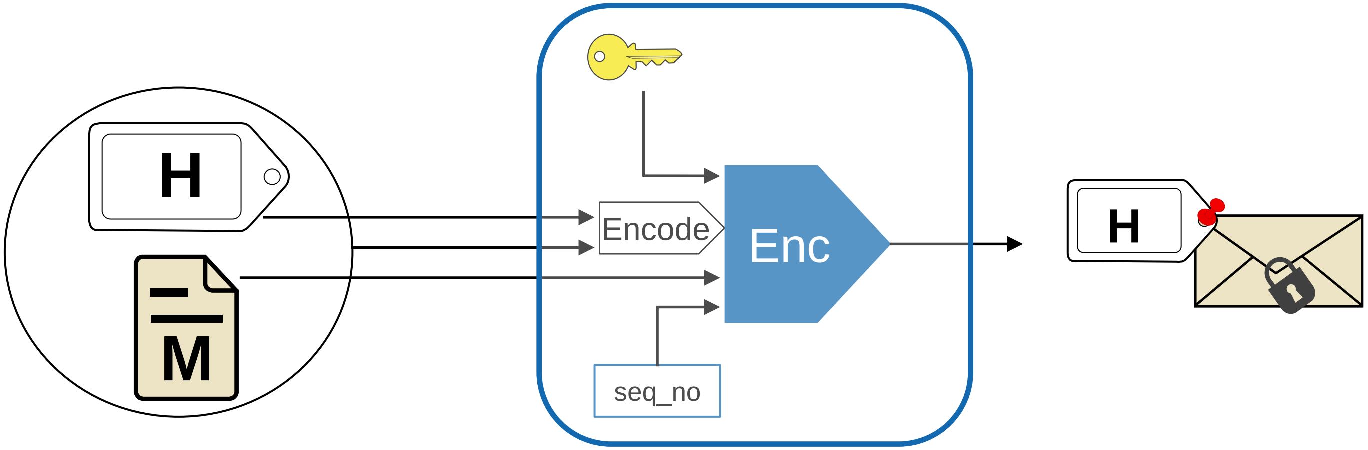
Details on the Construction

Converter of Alice:



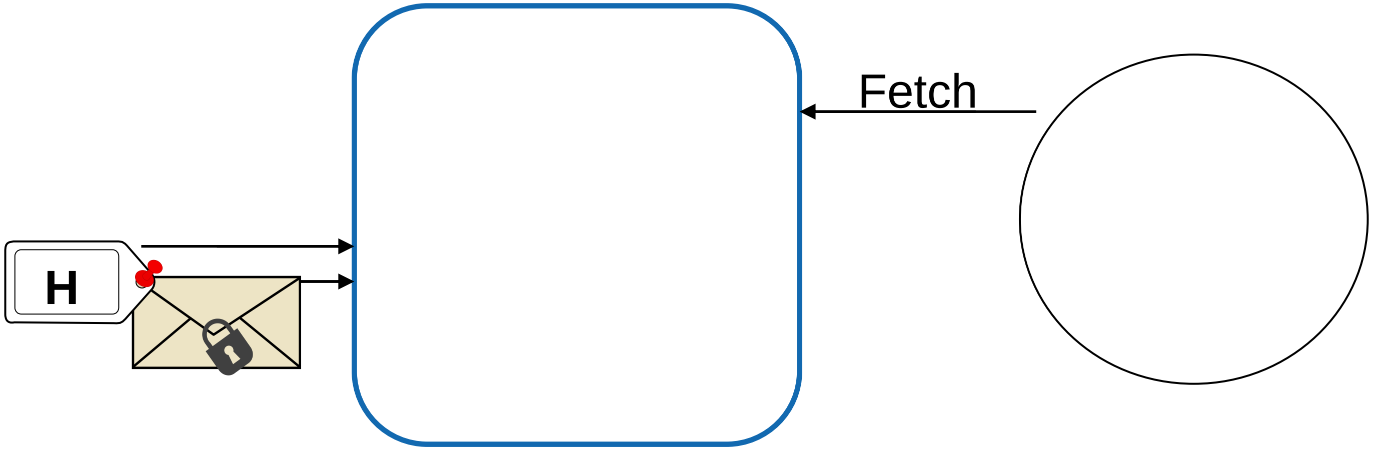
Details on the Construction

Converter of Alice:



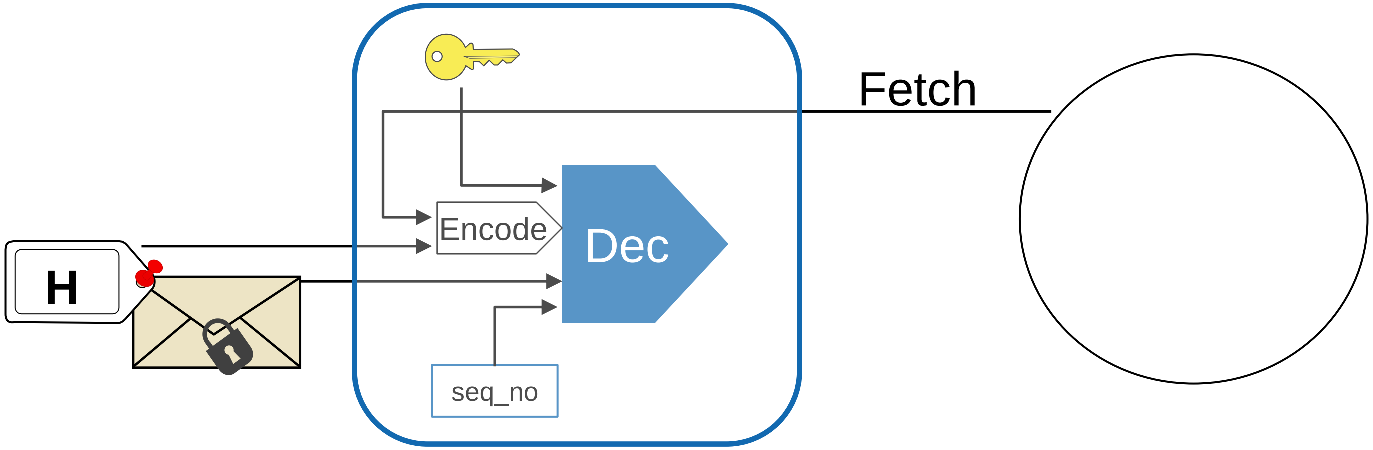
Details on the Construction

Converter of Bob:



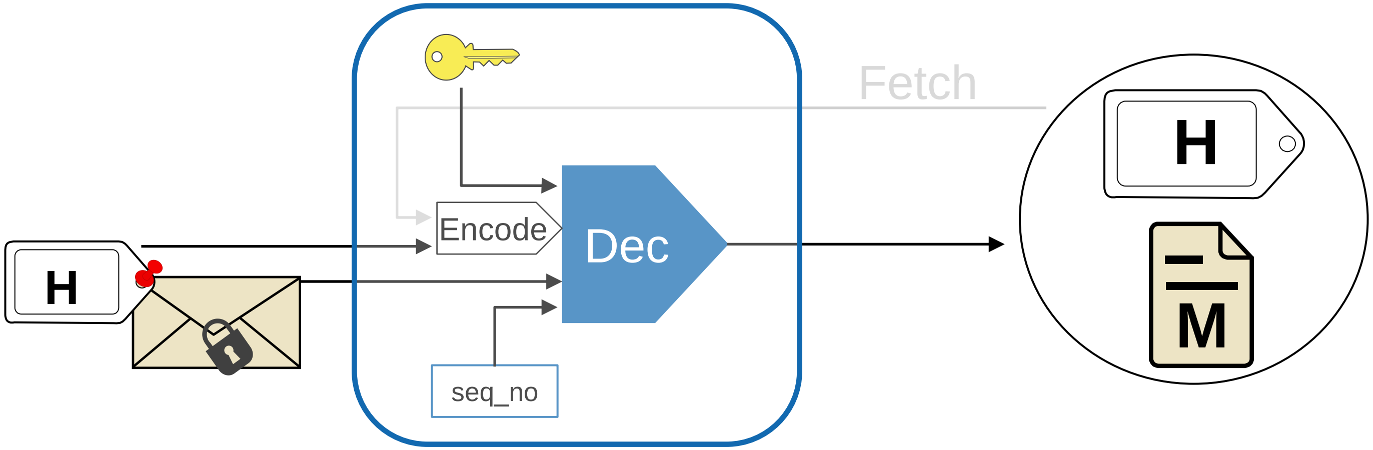
Details on the Construction

Converter of Bob:



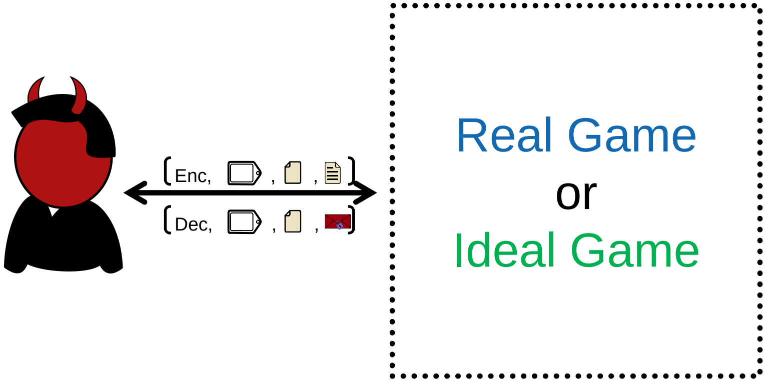
Details on the Construction

Converter of Bob:



Details on the Construction

Proof Idea: Problem of distinguishing the AEAD games reduces to the problem of distinguishing the real and ideal worlds:



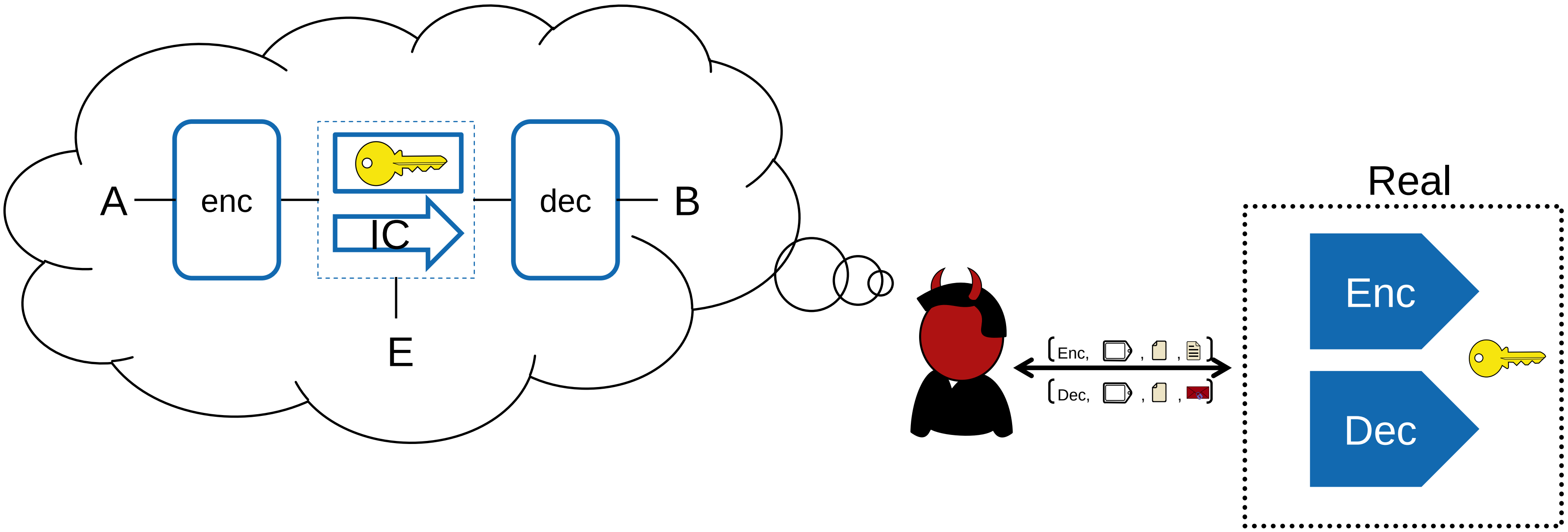
Real Game

or

Ideal Game

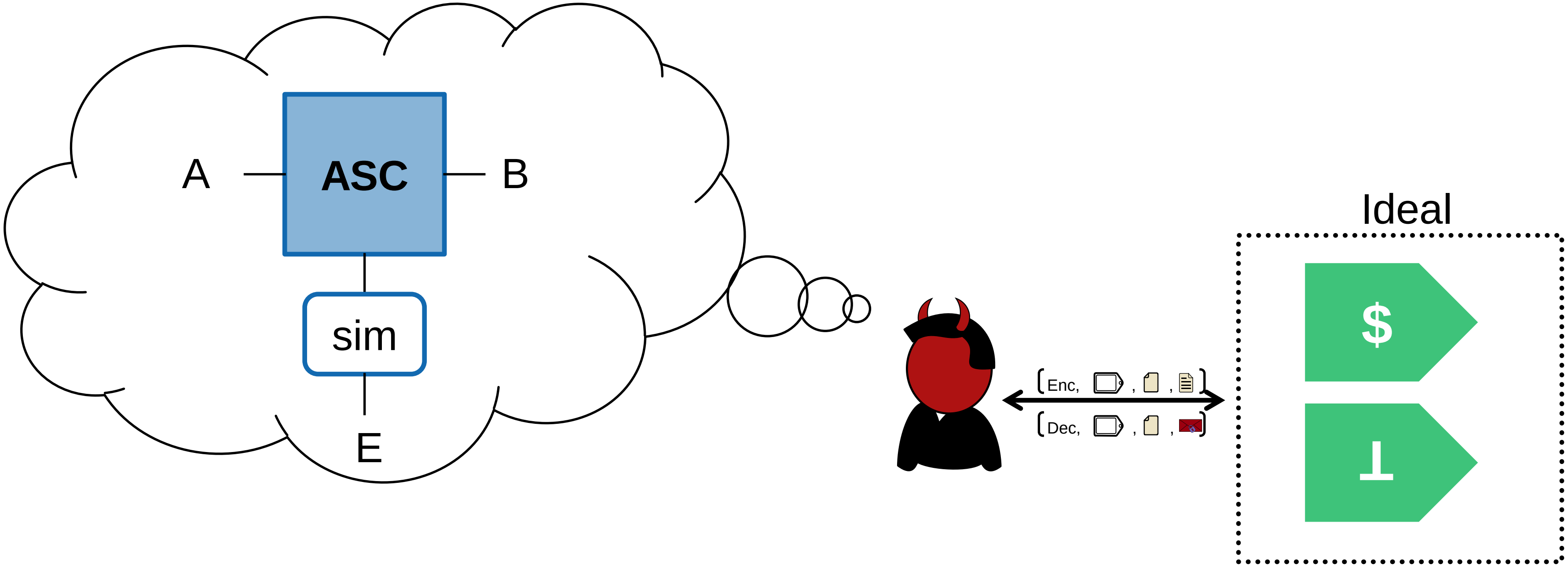
Details on the Construction

Proof Idea: Problem of distinguishing the AEAD games reduces to the problem of distinguishing the real and ideal worlds:



Details on the Construction

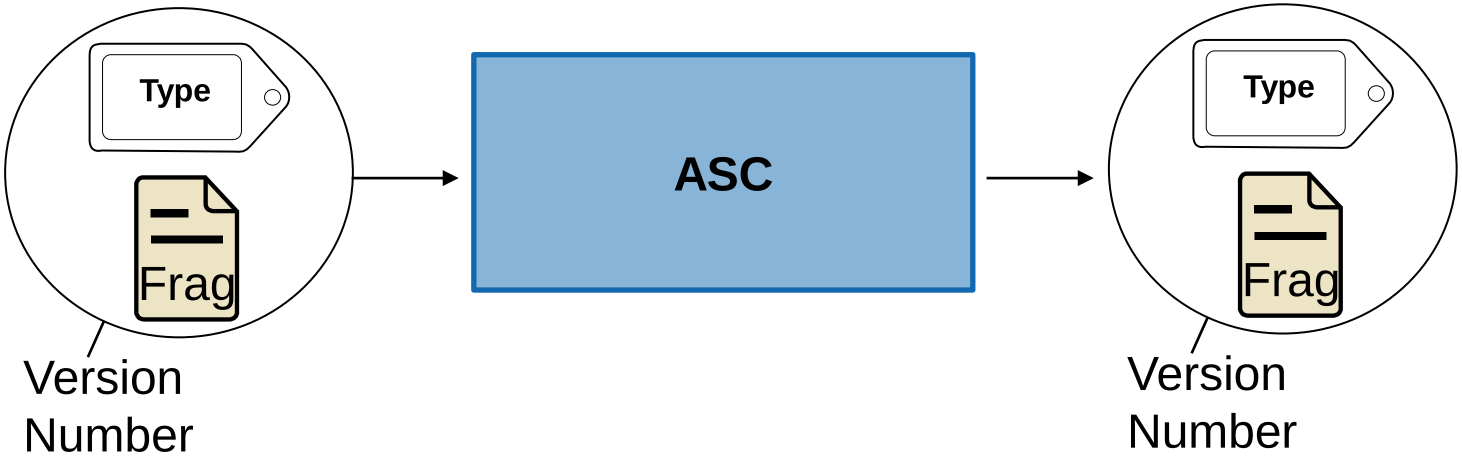
Proof Idea: Problem of distinguishing the AEAD games reduces to the problem of distinguishing the real and ideal worlds:



Application of ASC: Sound Design of Practical Protocols

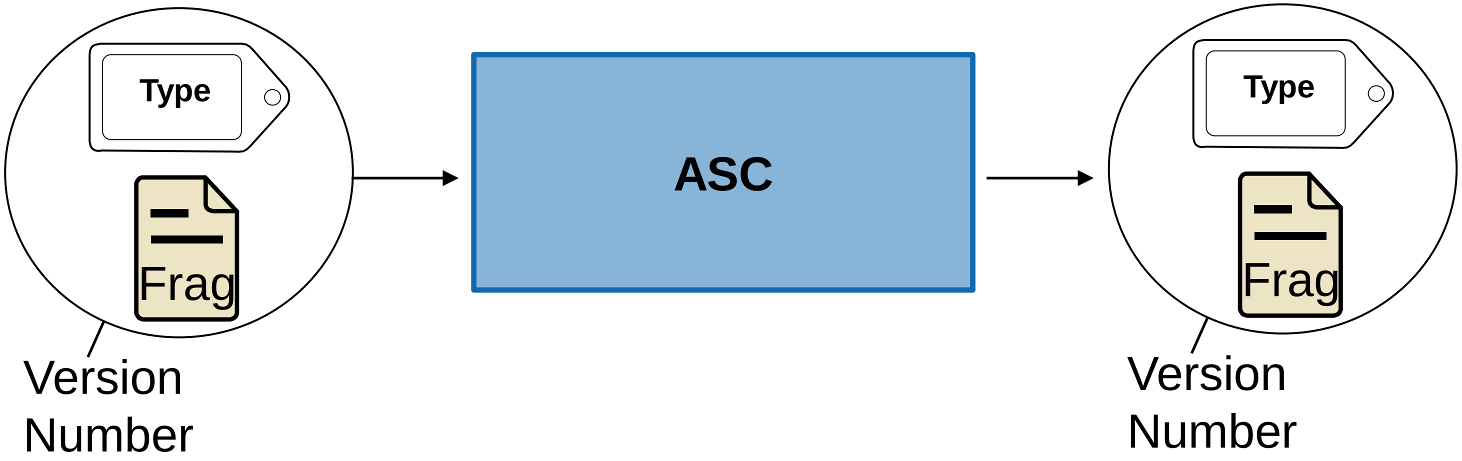
Application of ASC: Sound Design of Practical Protocols

Example: Re-Modelling the TLS 1.3 Record Layer:



Application of ASC: Sound Design of Practical Protocols

Example: Re-Modeling the TLS 1.3 Record Layer:



Our model gives insights into current proposals:

1. The nonce needs no randomness.
2. The sequence number need not be part of the AD.
3. The version number can be part of the implicit header.

Summary

Augmented Secure Channels…

- capture the application semantics of AEAD.
- allow easy security checks of existing protocols.
- allow to develop sound communication protocols in a modular way.

Contact information and credits

ETH Zurich
Department of Computer Science
Universitätsstrasse 6
8092 Zurich

References:

[DFG15]: B. Dowling, M. Fischlin, F. Günther, D. Stebila. A Cryptographic Analysis of the TLS 1.3 Handshake Protocol Candidates. CCS 2015.

[HKR15]: V.T. Hoang, T. Krovetz, P. Rogaway. Robust Authenticated Encryption – AEZ and the Problem that it solves. Eurocrypt 2015.

[KMO14]: M. Kohlweiss, U. Maurer, C. Onete, B. Tackmann, D. Venturi. (De-)Constructing TLS. Cryptology ePrint Archive, Report 2014/020.

[MR11]: U. Maurer, R. Renner. Abstract Cryptography. ICS 2011.

[Mau11]: U. Maurer. Constructive Cryptography – A New Paradigm for Security Definitions and Proofs. TOSCA 2011.

Images: https://openclipart.org/