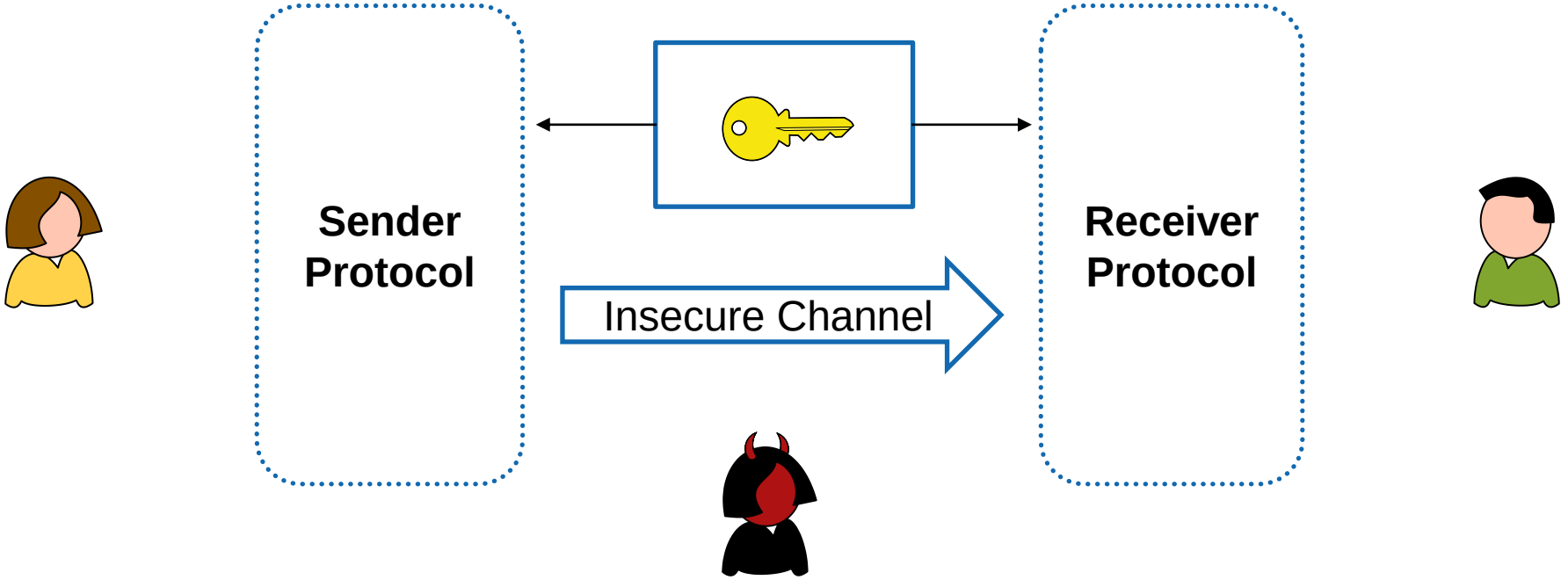
ETH zürich

Robust Authenticated Encryption and the Limits of Symmetric Cryptography

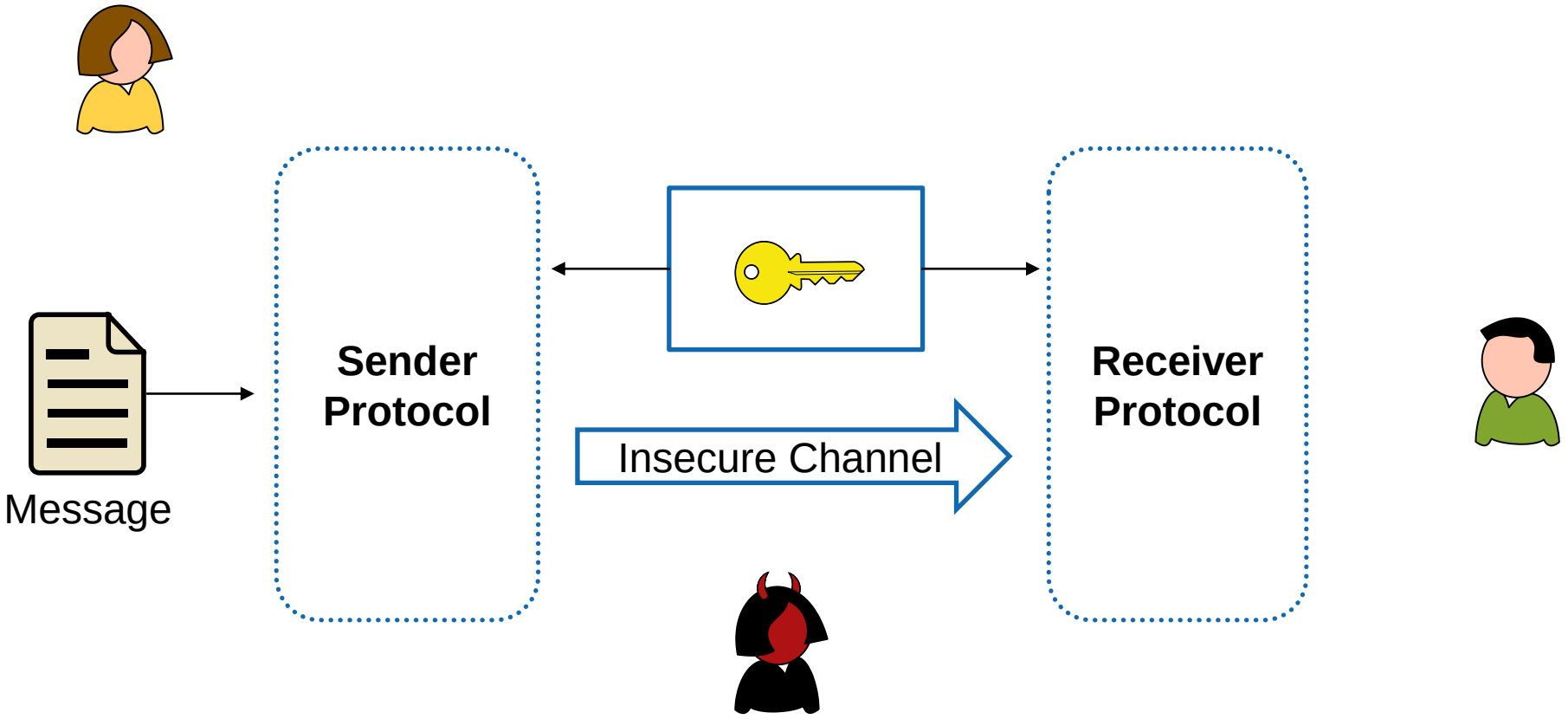
Christian Badertscher[1], Christian Matt[1], Ueli Maurer[1],
Phil Rogaway[2], Björn Tackmann[3]

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

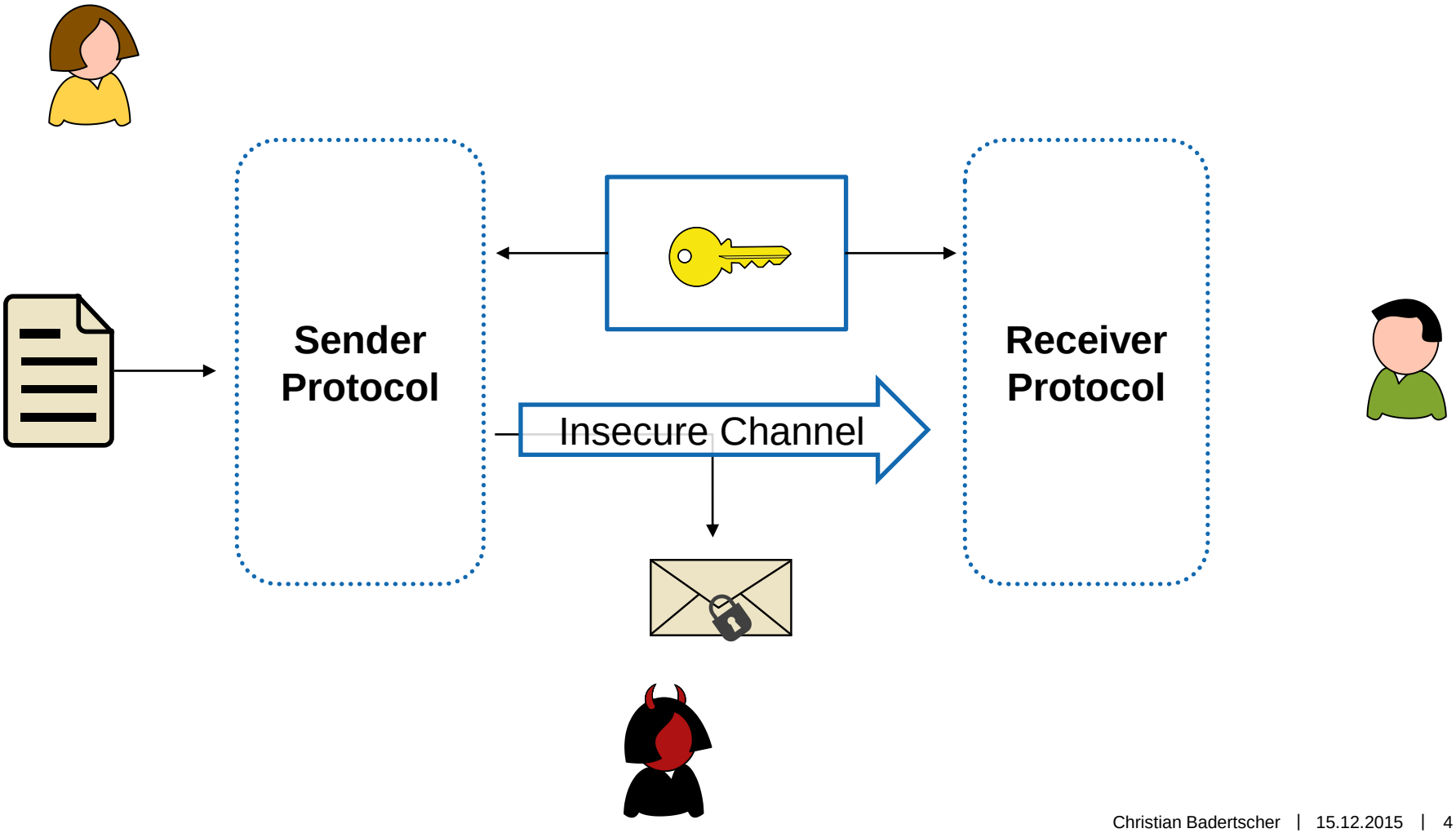
Protecting Communication



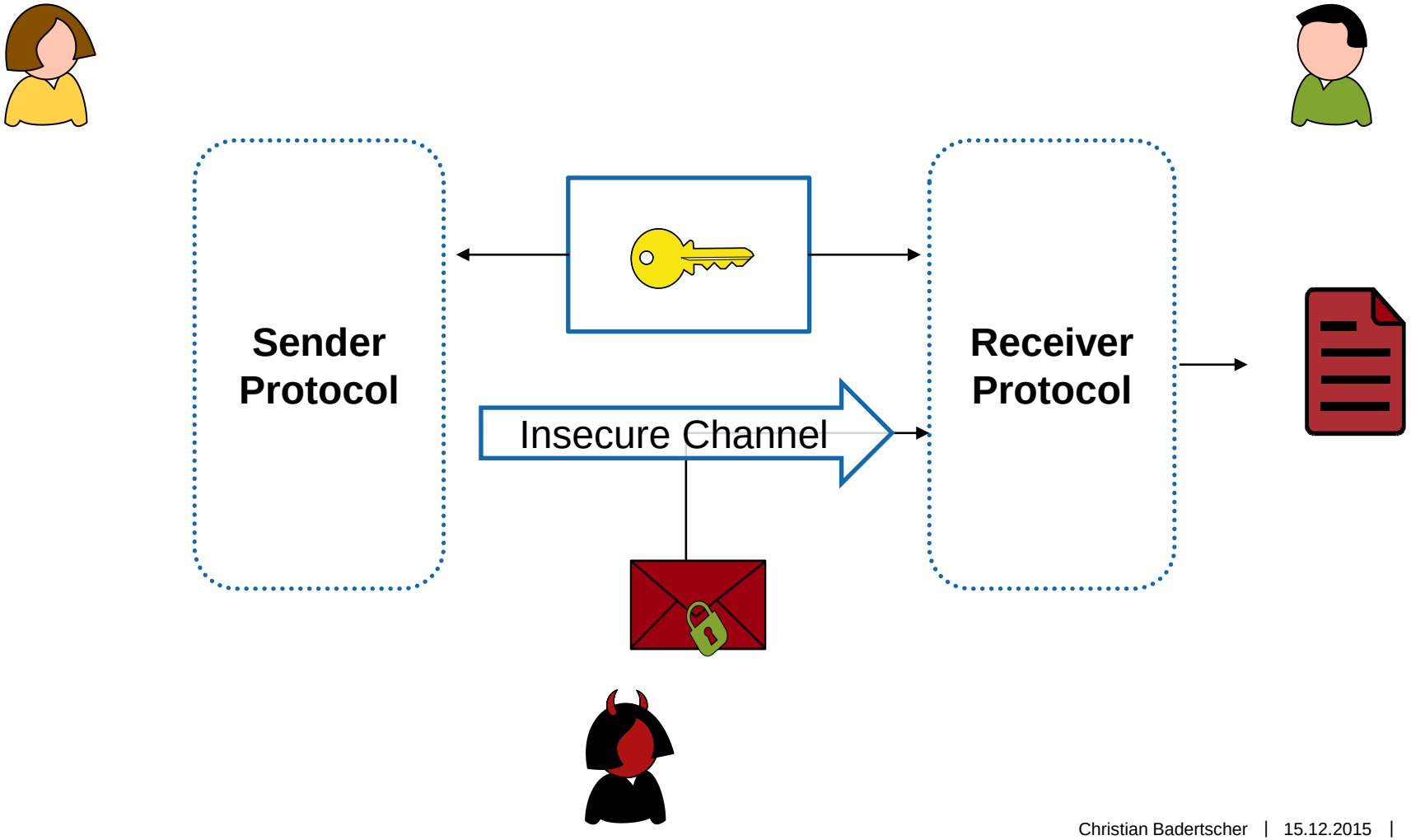
Protecting Communication



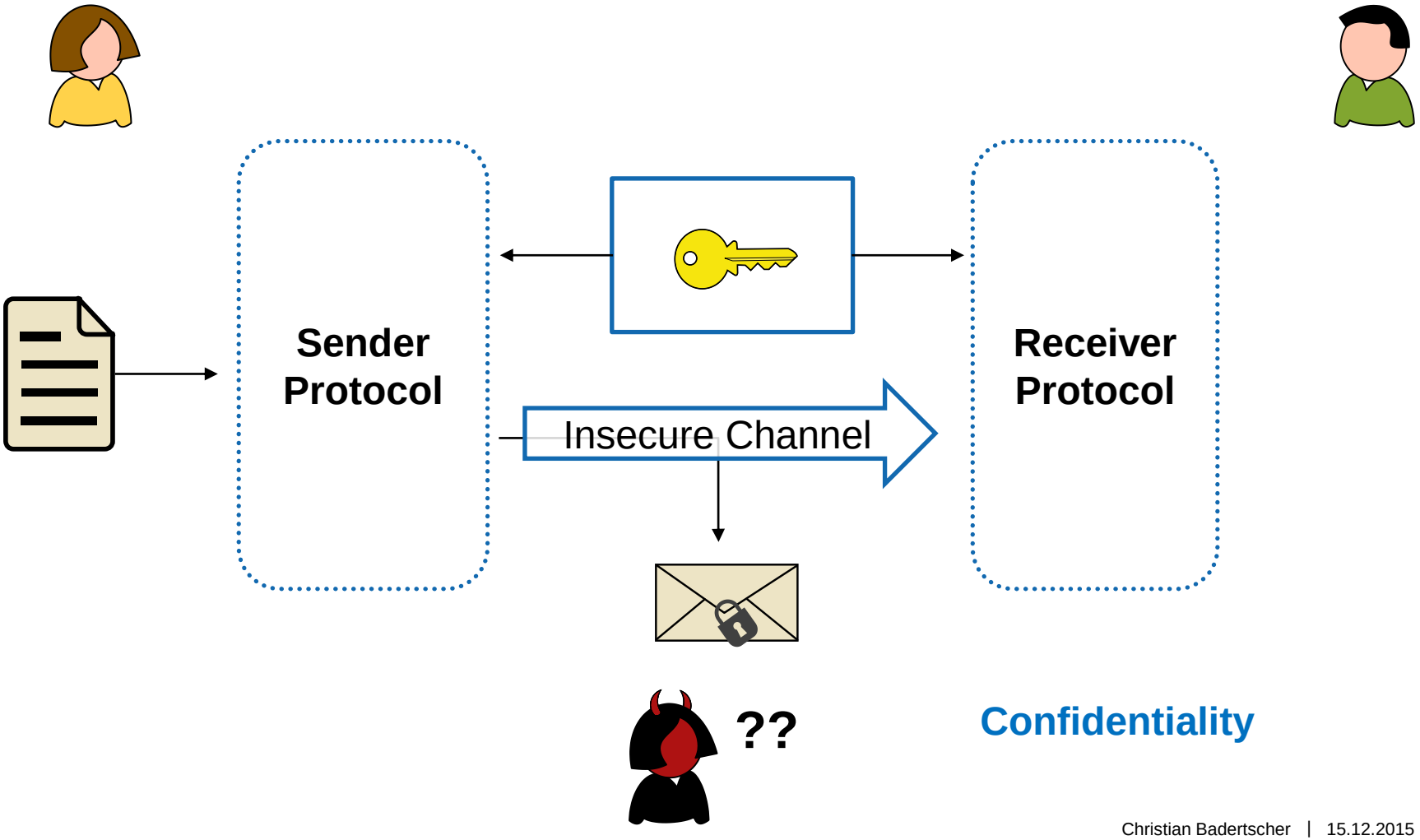
Protecting Communication



Protecting Communication

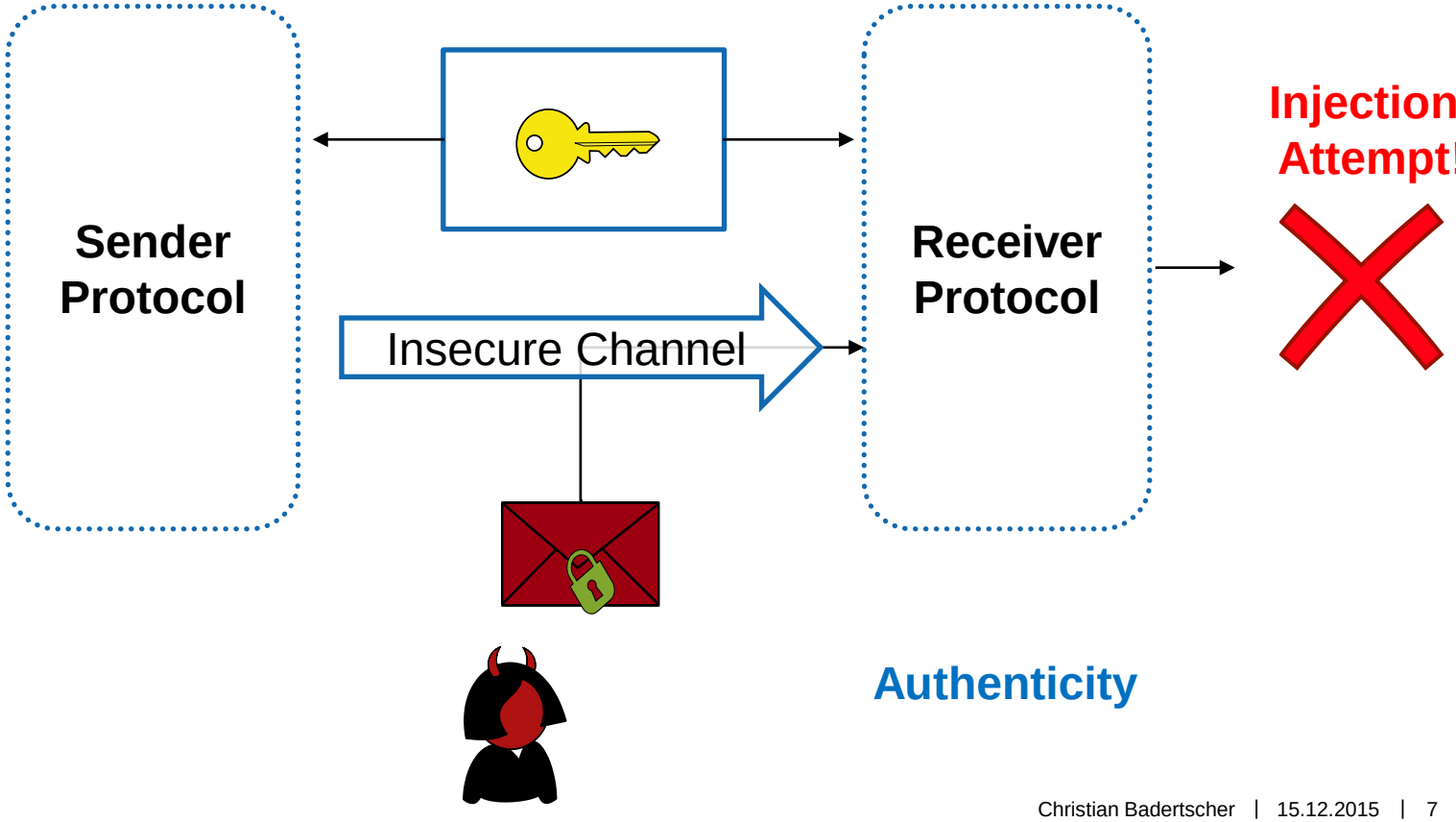


Protecting Communication



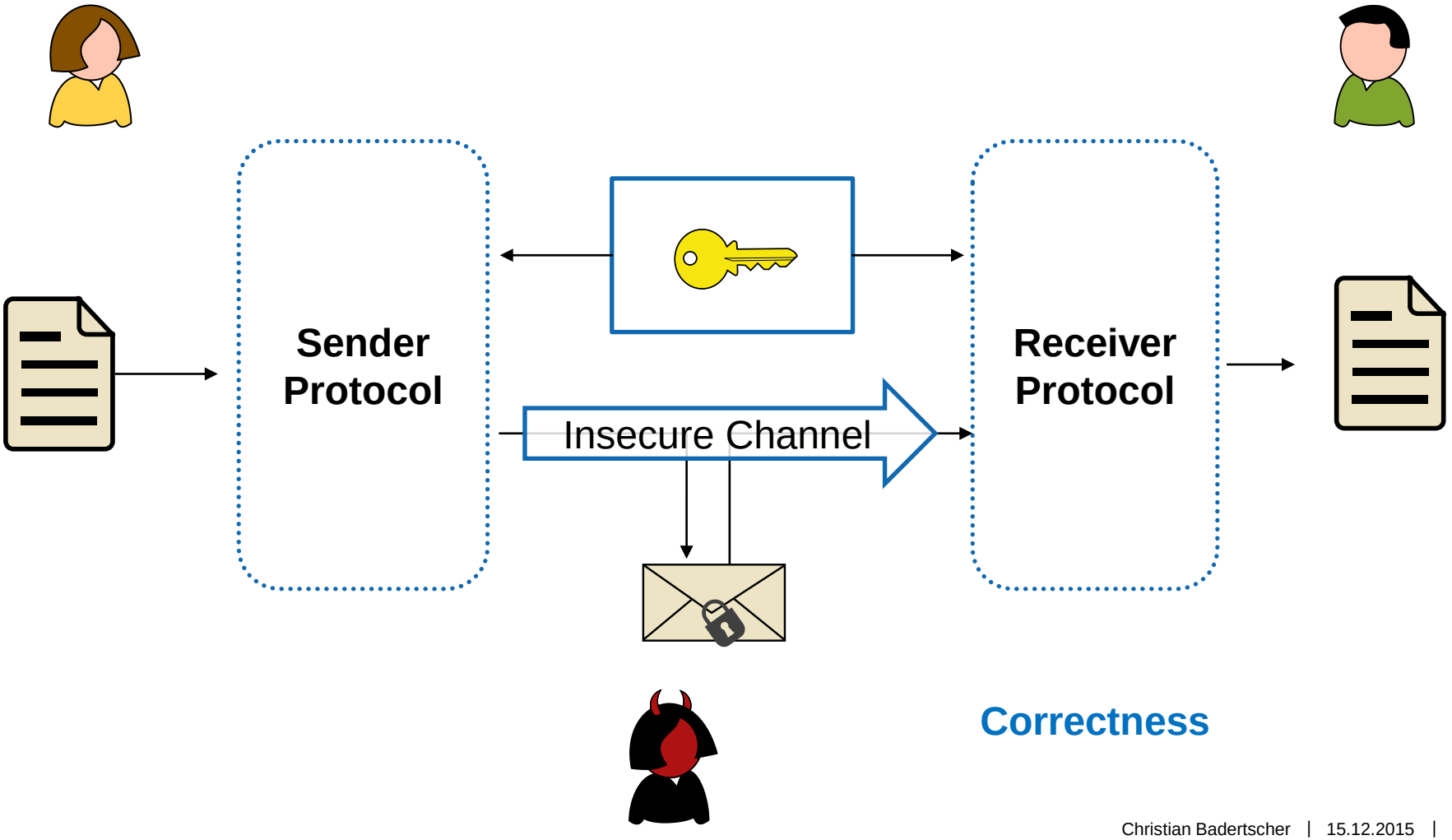
Confidentiality

Protecting Communication



Authenticity

Protecting Communication

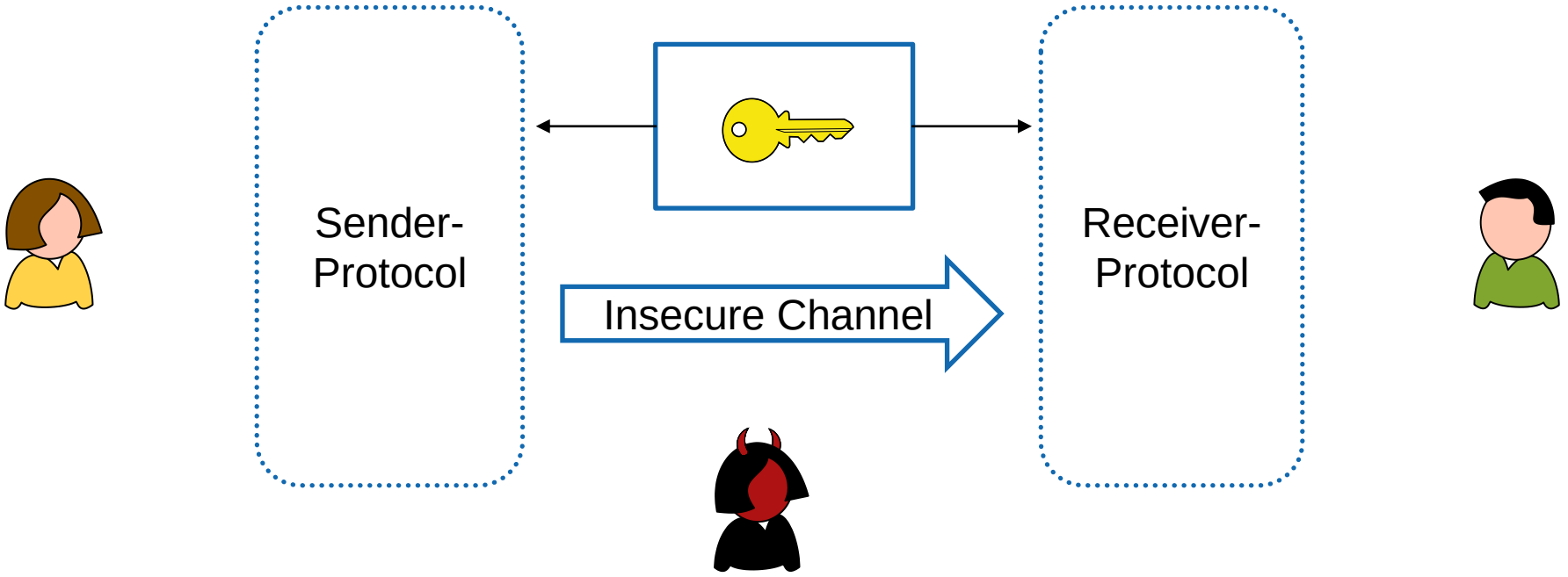


Correctness

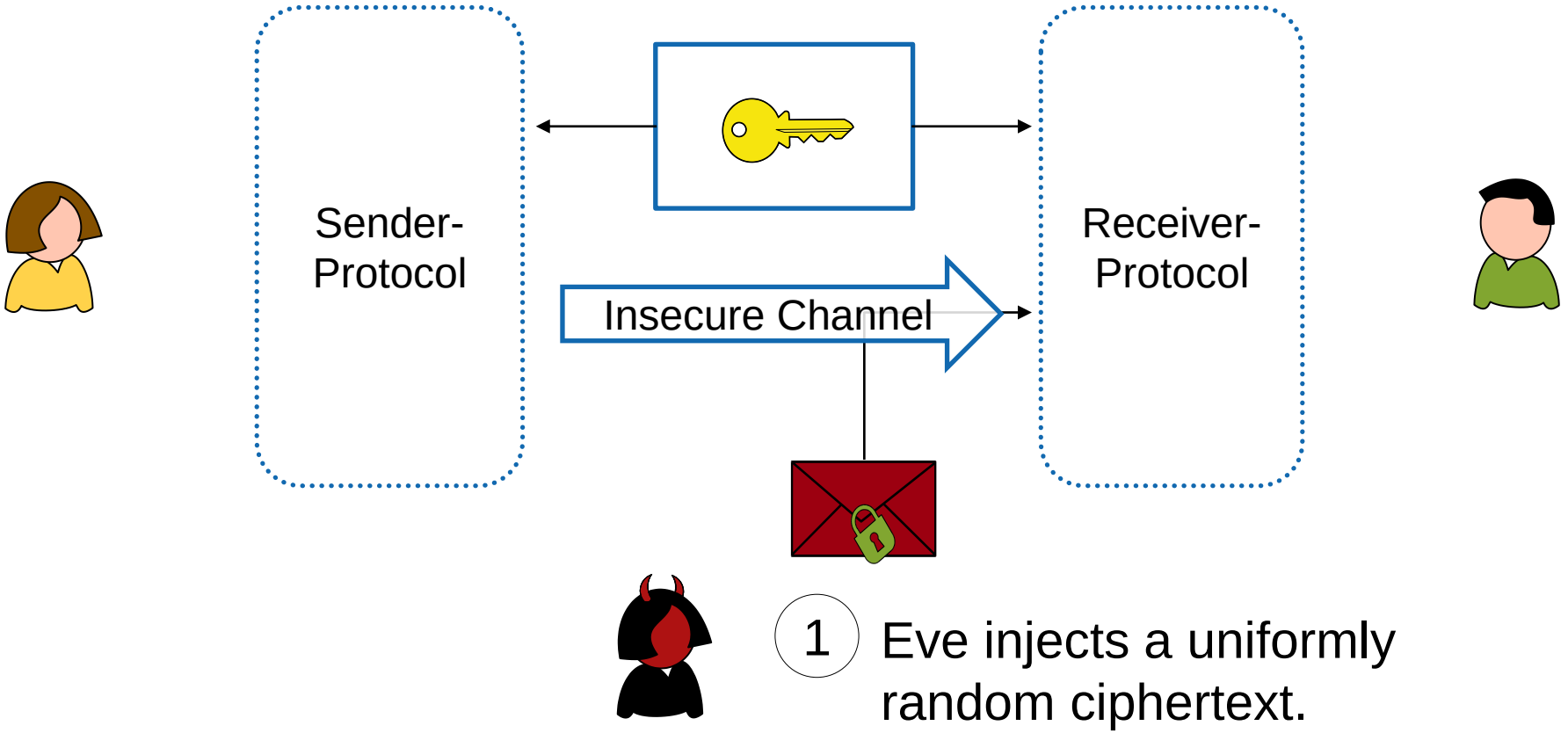
Roadmap

- **Fundamental limitations** of protecting communication in the **private key setting**?
- **Best schemes** within those limits?

A General Problem in the Real World

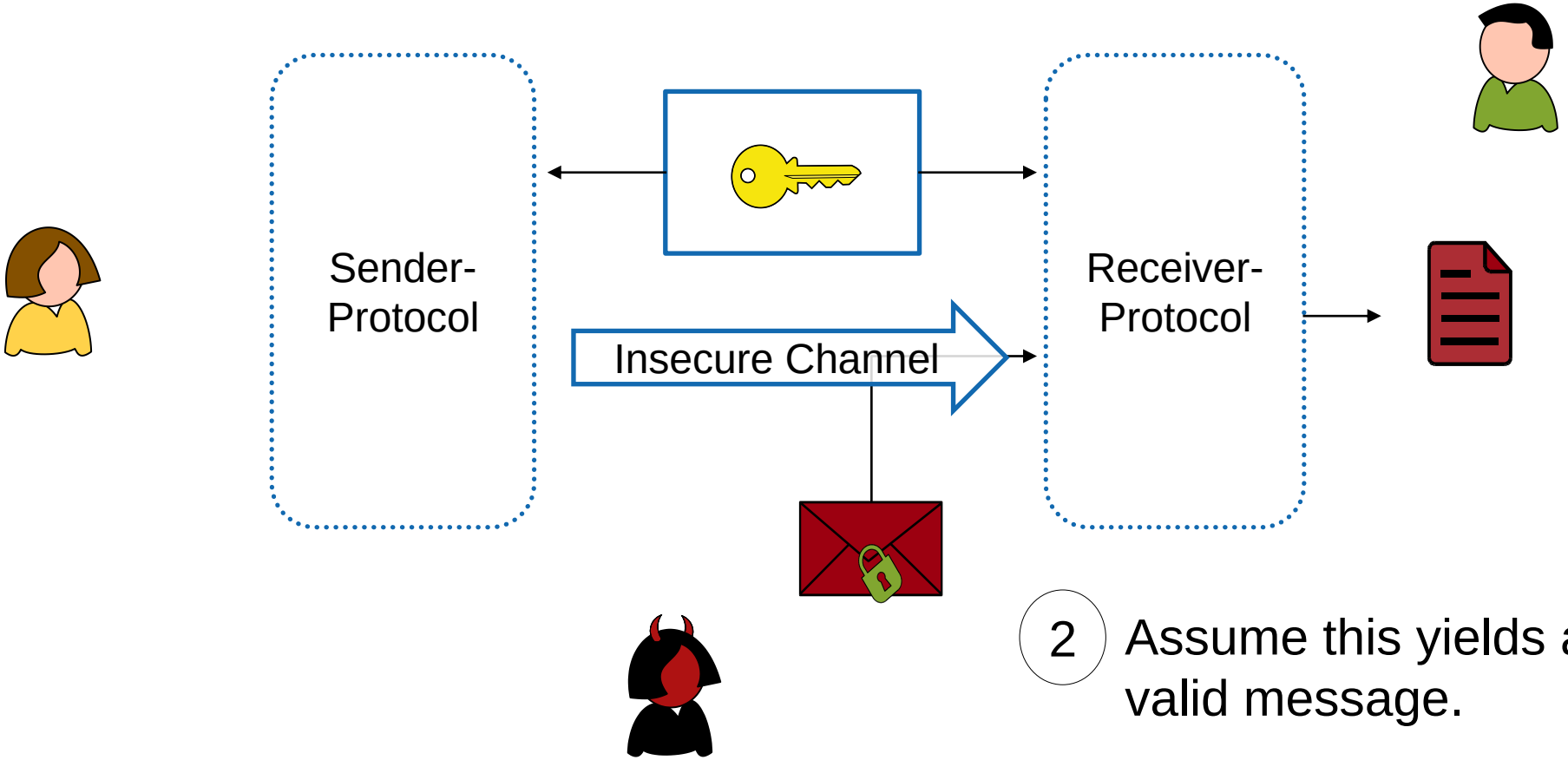


A General Problem in the Real World



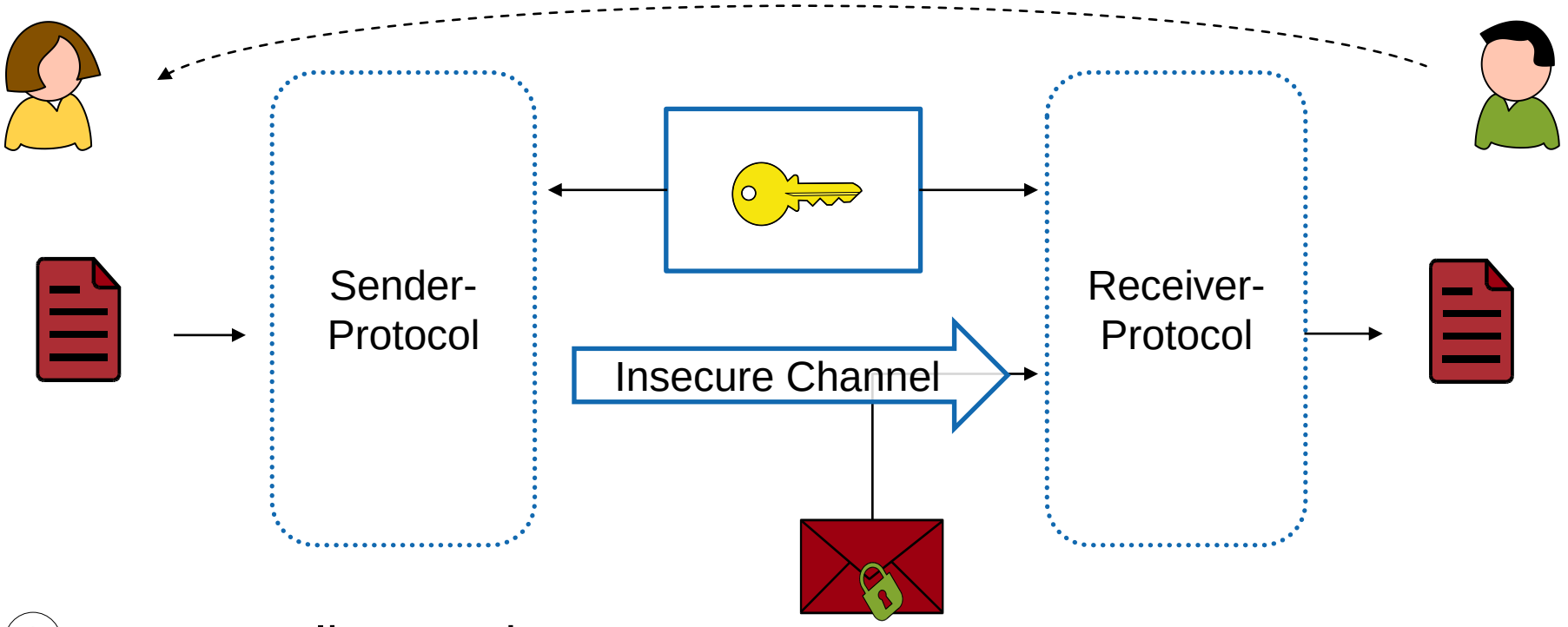
1 Eve injects a uniformly random ciphertext.

A General Problem in the Real World



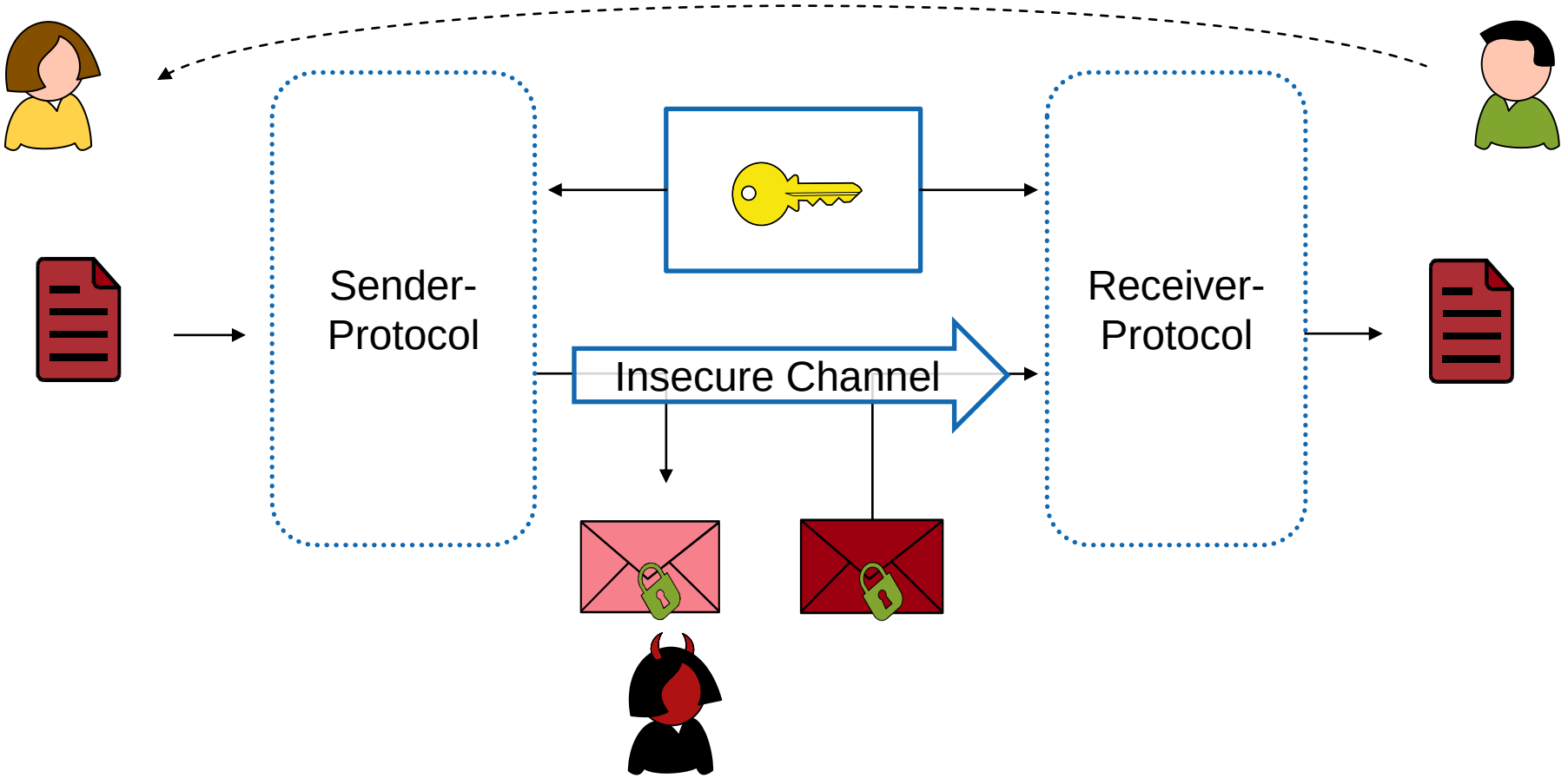
2 Assume this yields a valid message.

A General Problem in the Real World

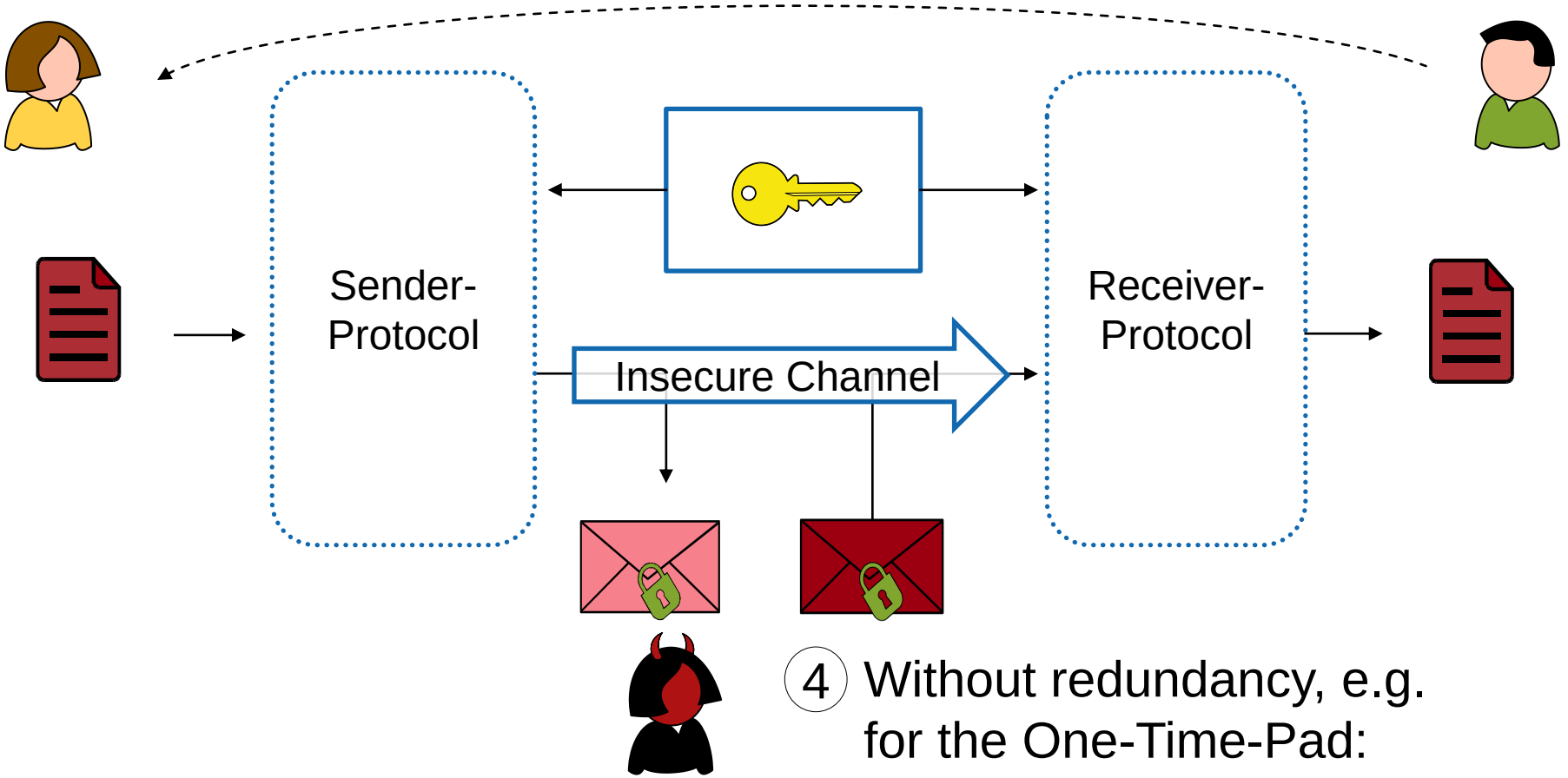


3 Assume Alice sends the message that Bob decrypted before.

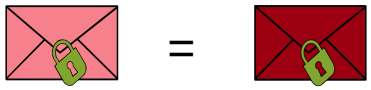
A General Problem in the Real World



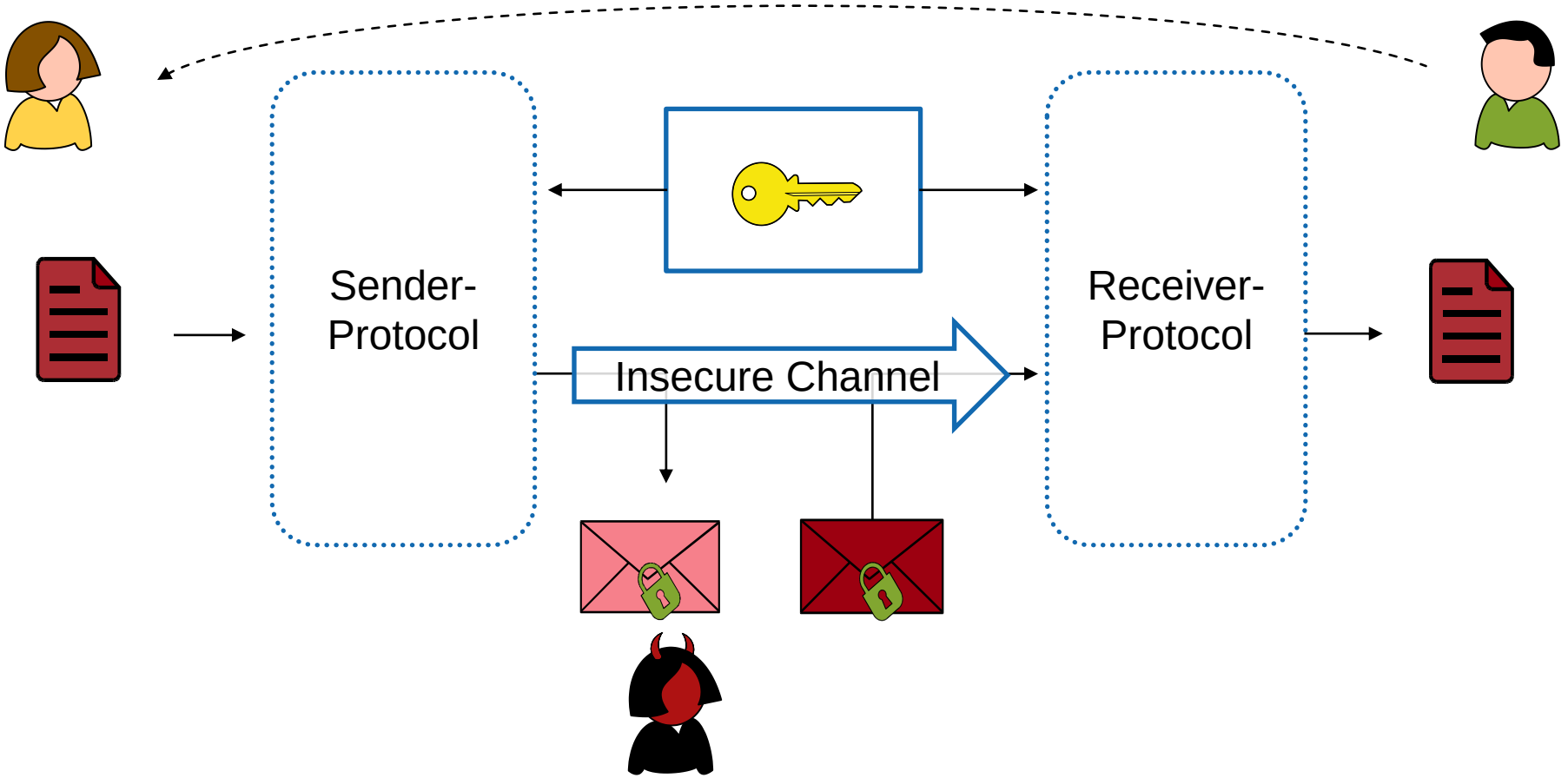
A General Problem in the Real World



4 Without redundancy, e.g. for the One-Time-Pad:

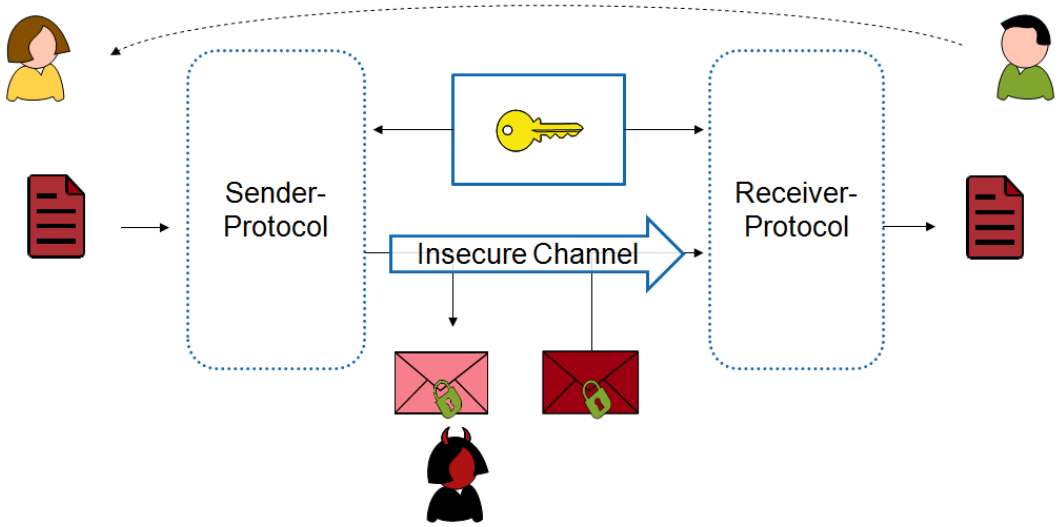


A General Problem in the Real World



Eve learns more than the length of the message.

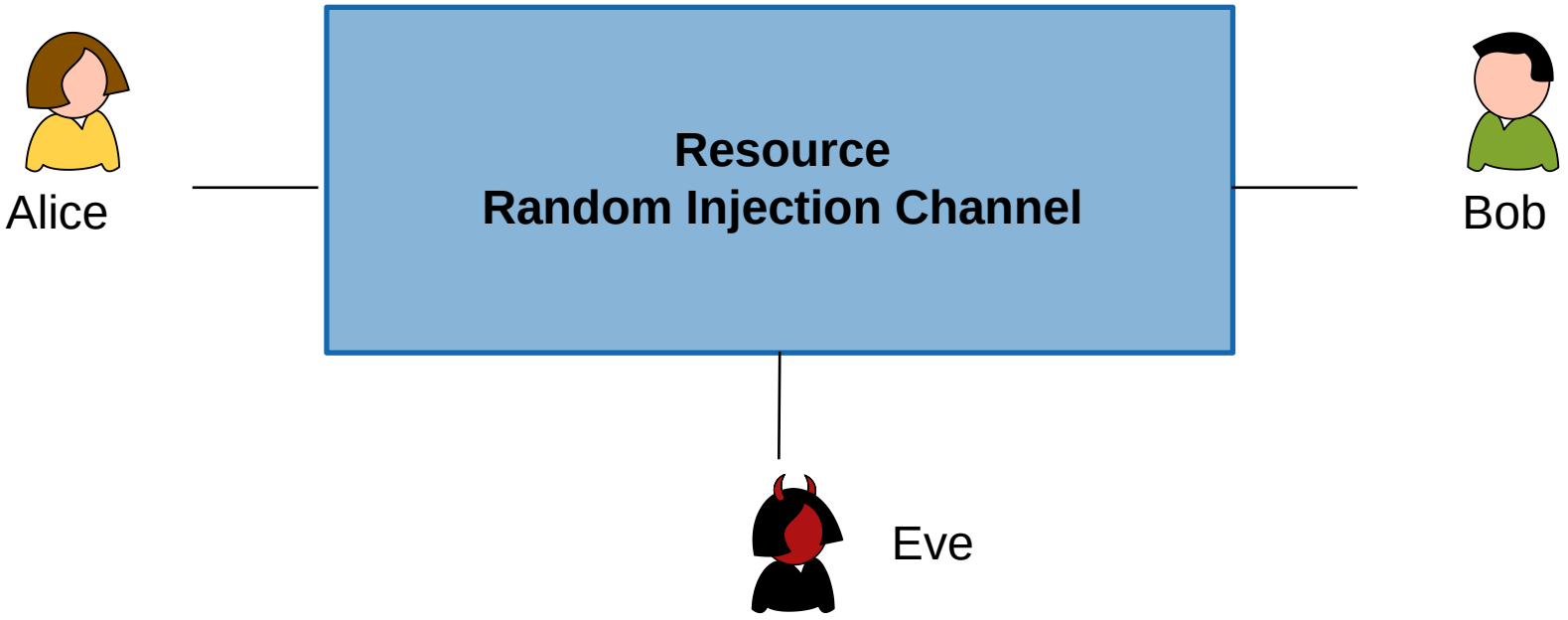
A General Problem in the Real World



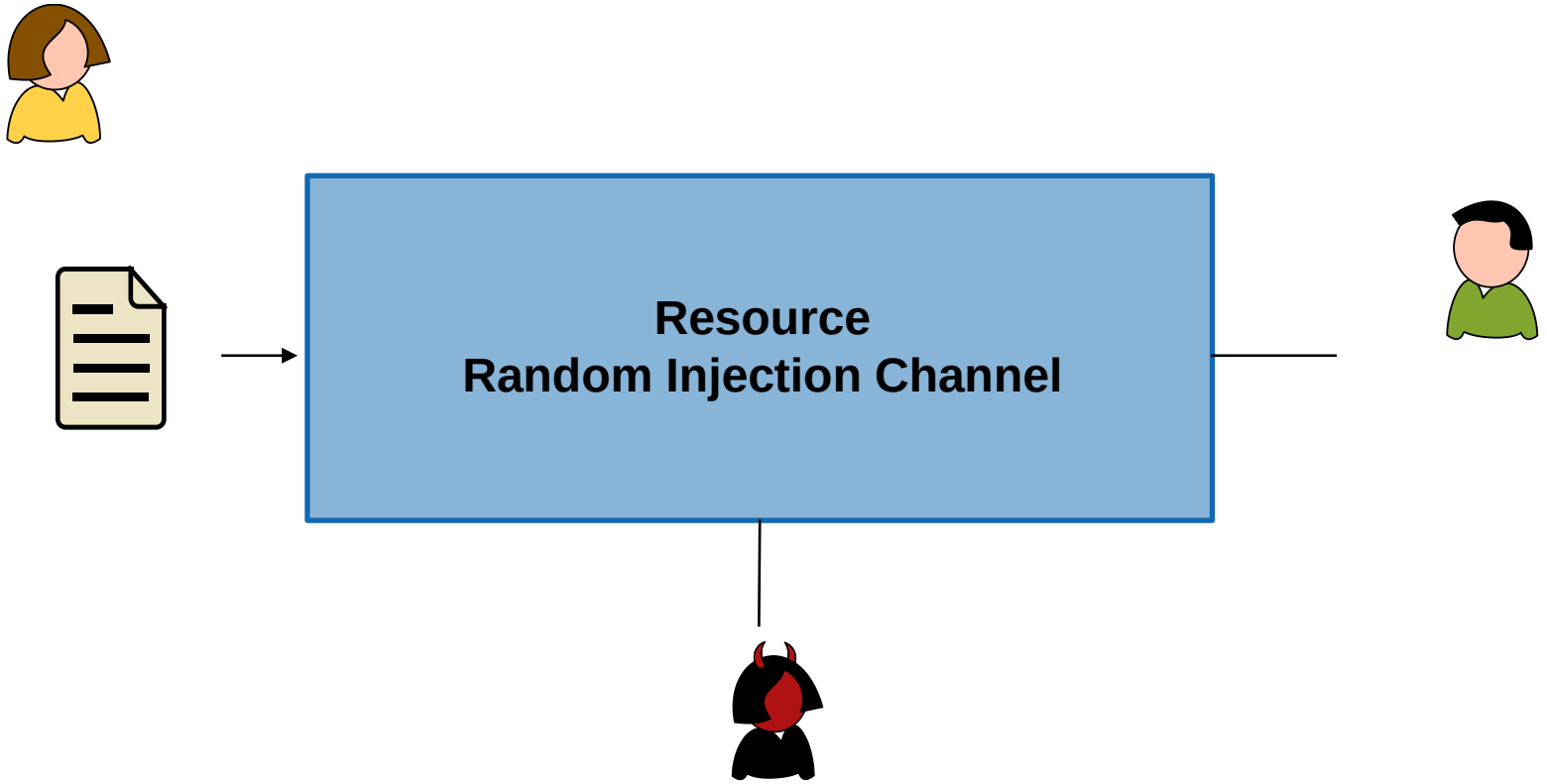
Observation: For any correct protocol that maps ℓ-bit messages to $\ell+\lambda$-bit ciphertexts (and vice-versa):

$$\Pr\left[\text{is a valid message} \wedge = \right] \geq \frac{1}{2^{\lambda}}$$

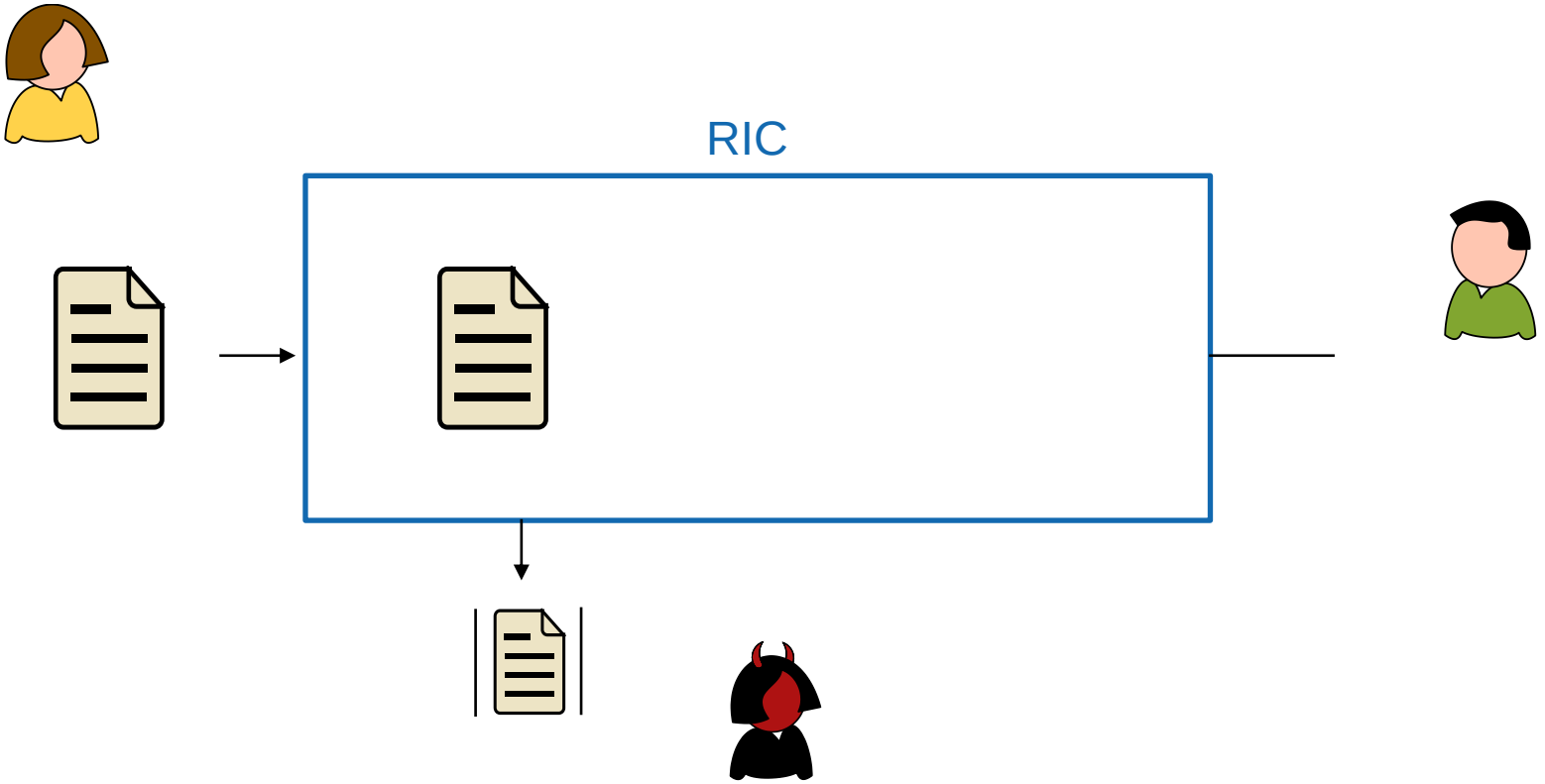
Random Injection Channel



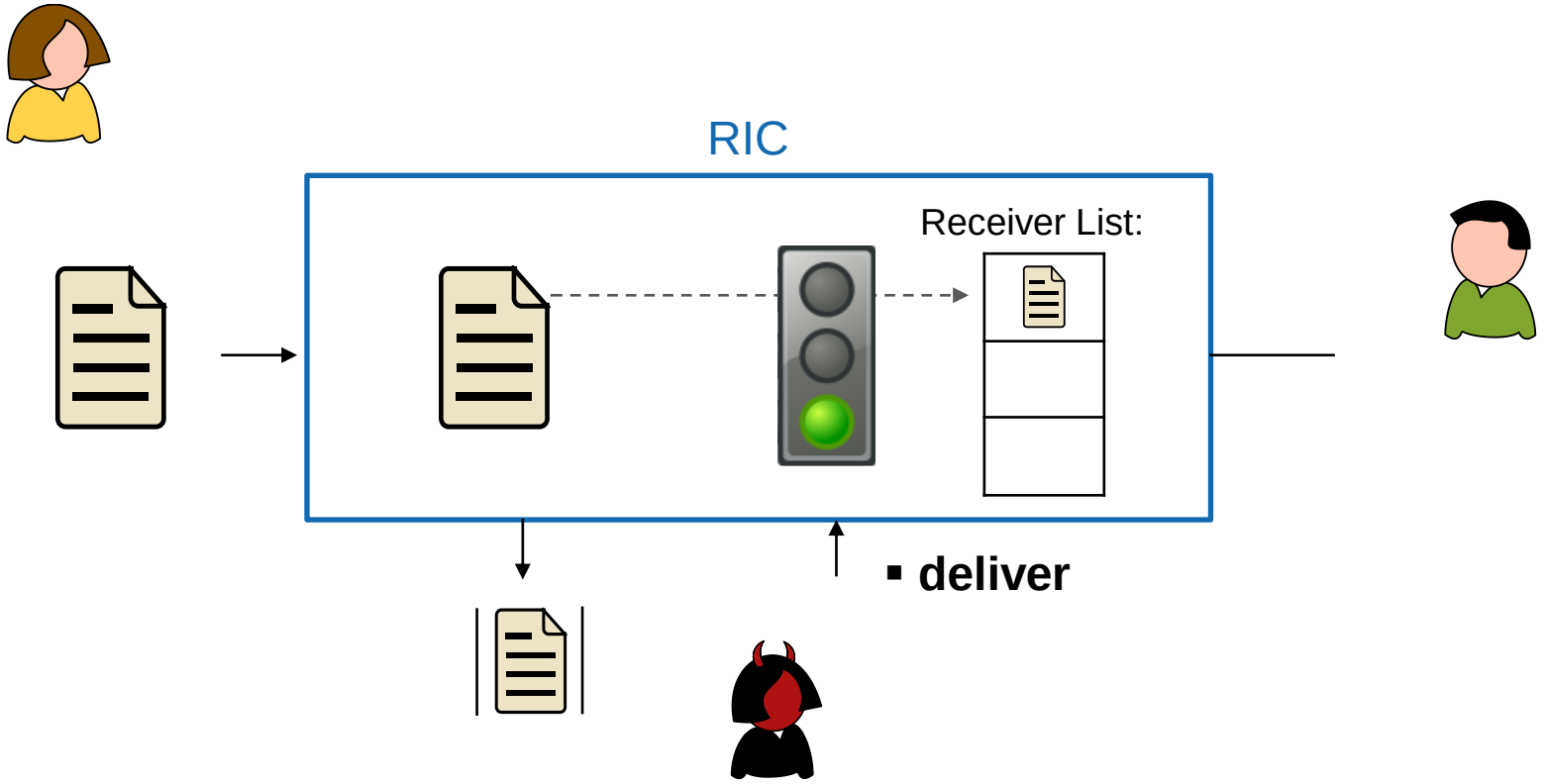
Random Injection Channel



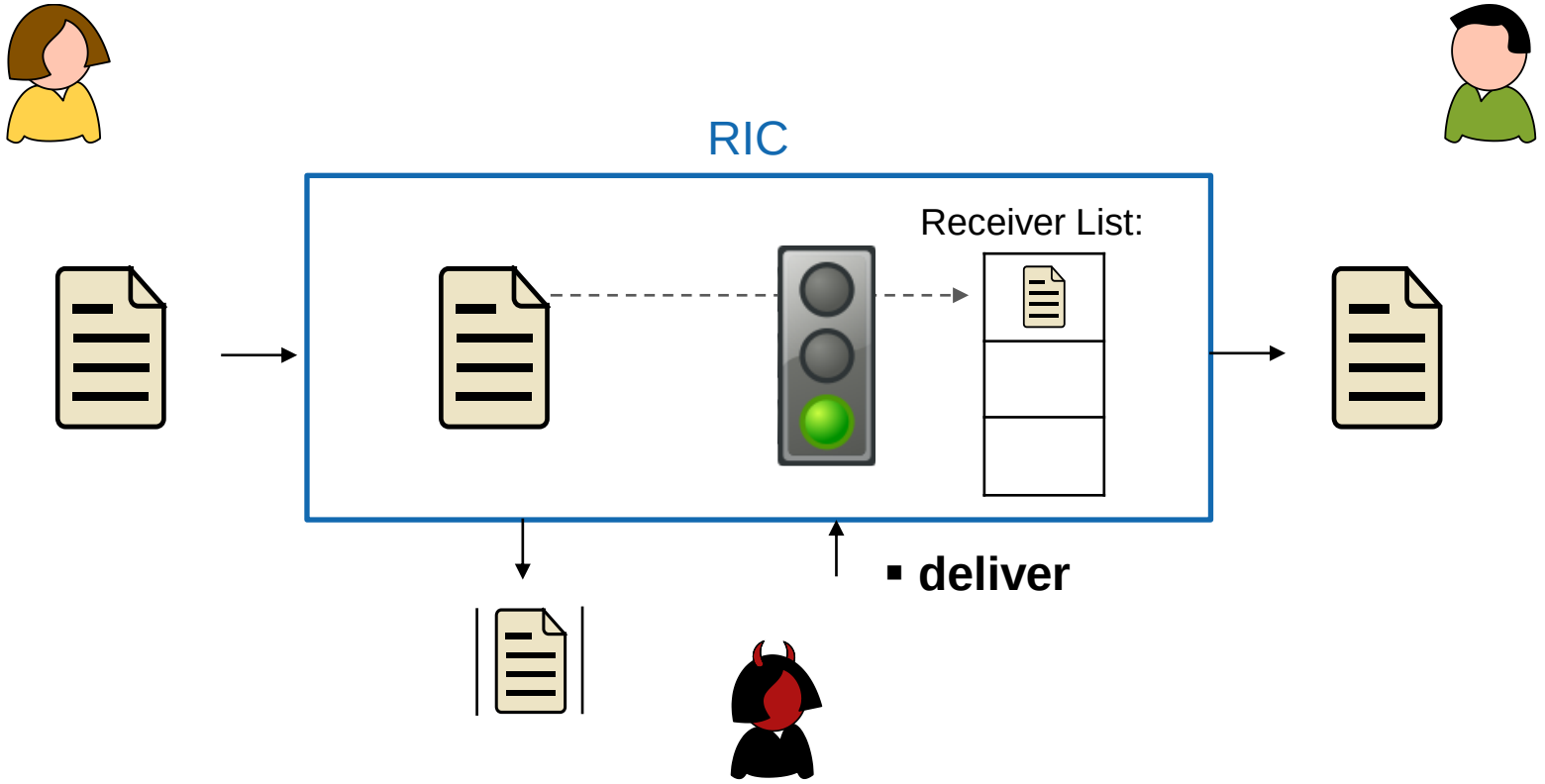
Random Injection Channel



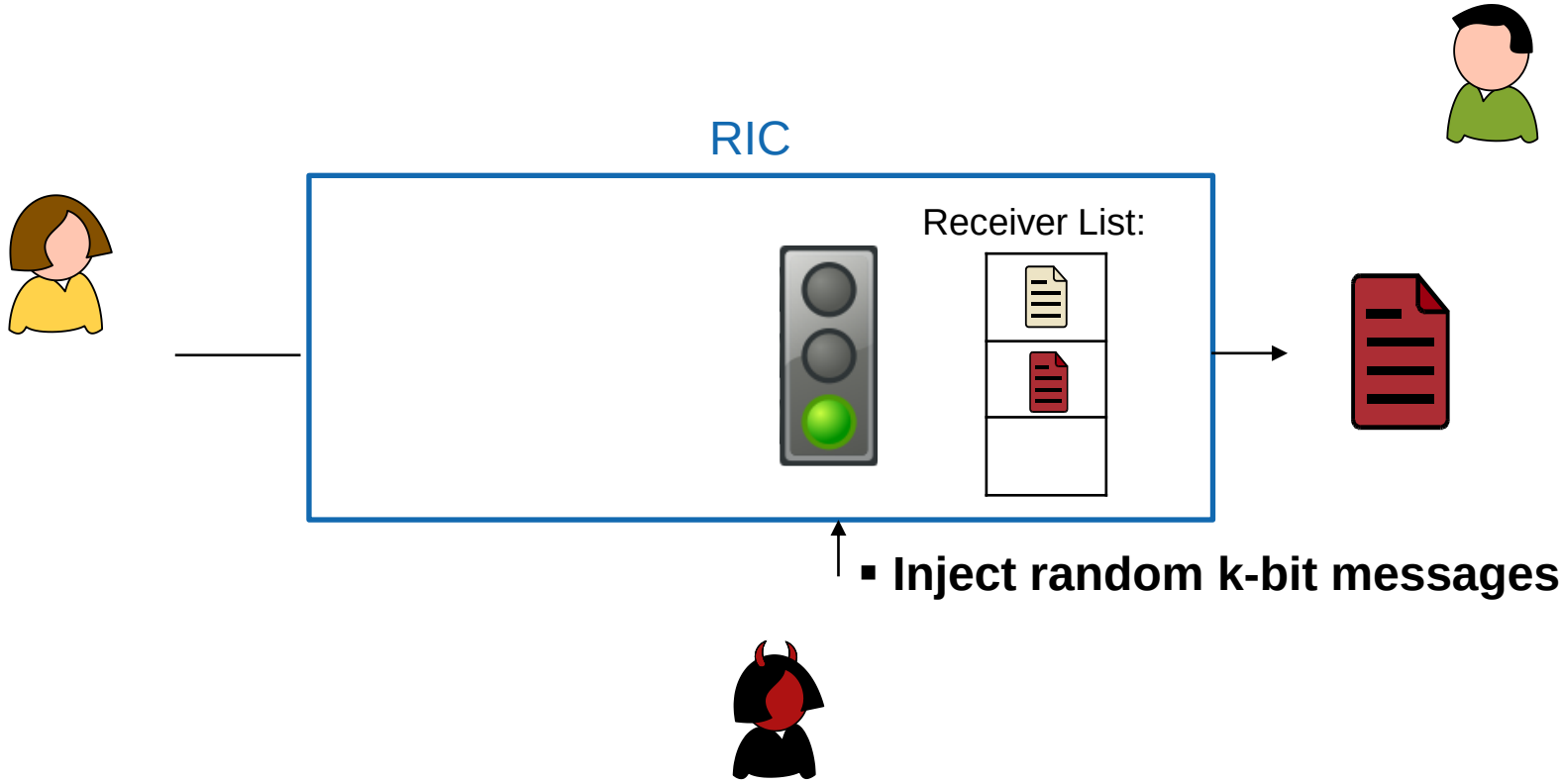
Random Injection Channel



Random Injection Channel

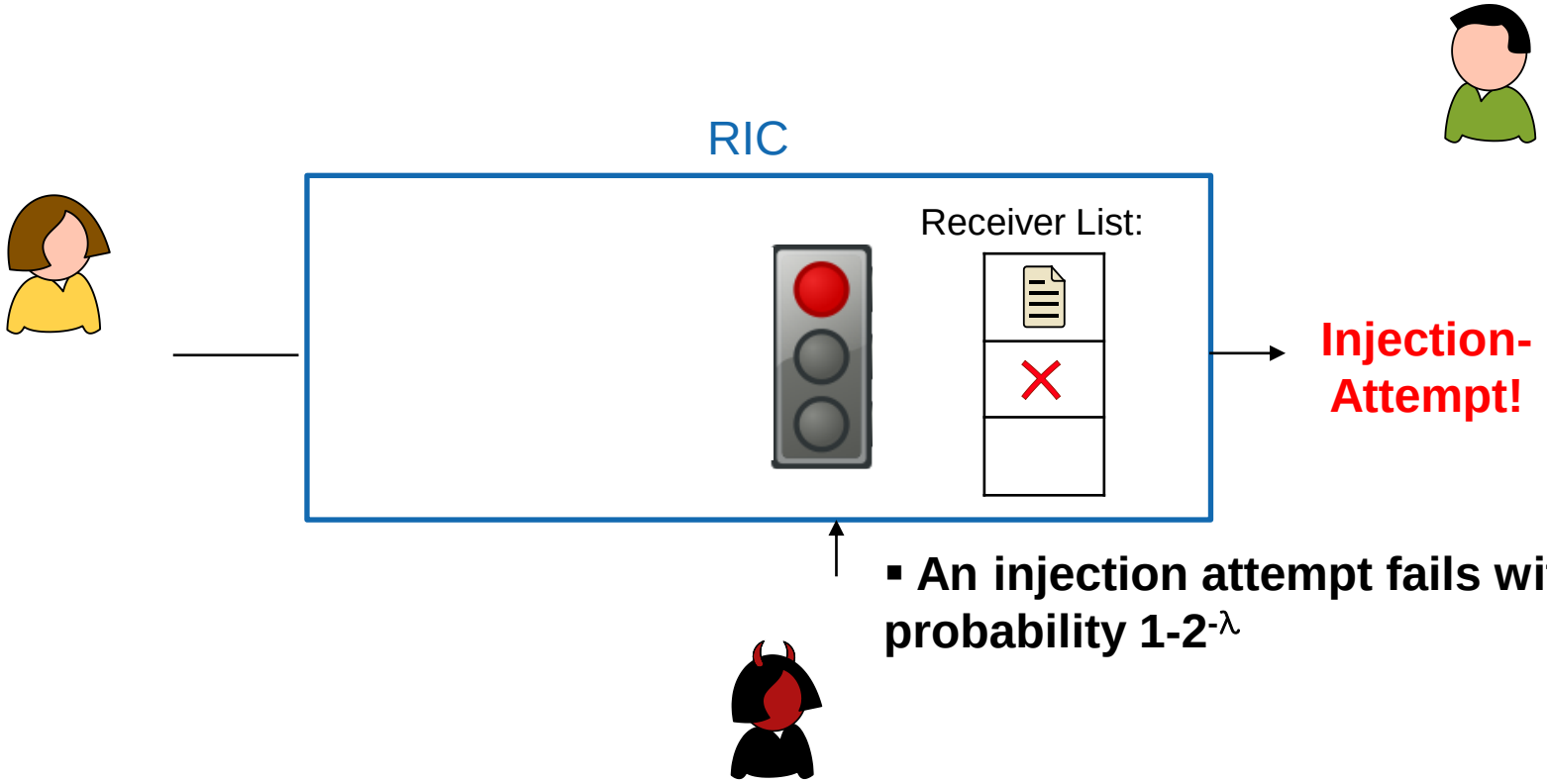


Random Injection Channel



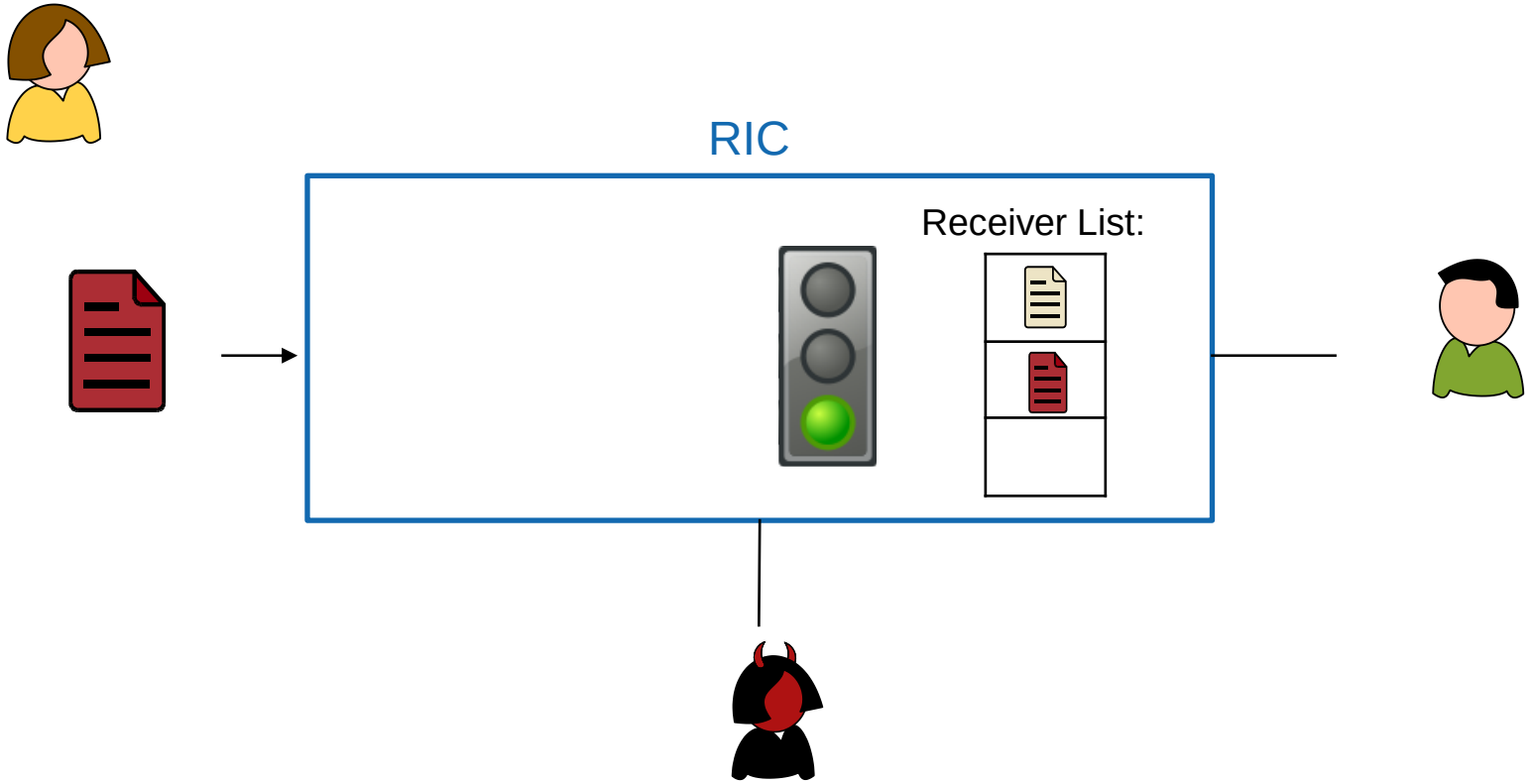
The channel is not fully authenticated.

Random Injection Channel

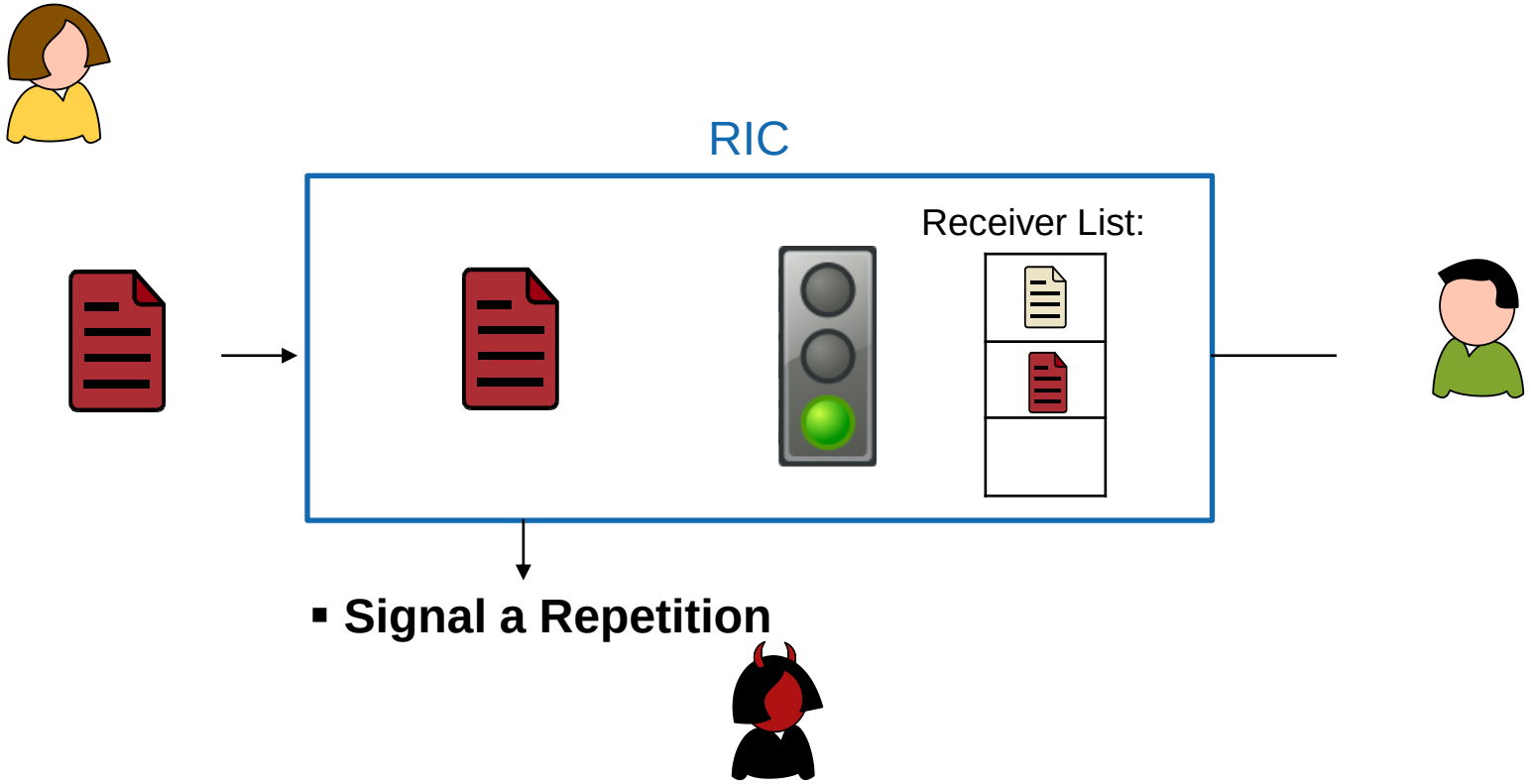


- **An injection attempt fails with probability $1-2^{-\lambda}$**

Random Injection Channel



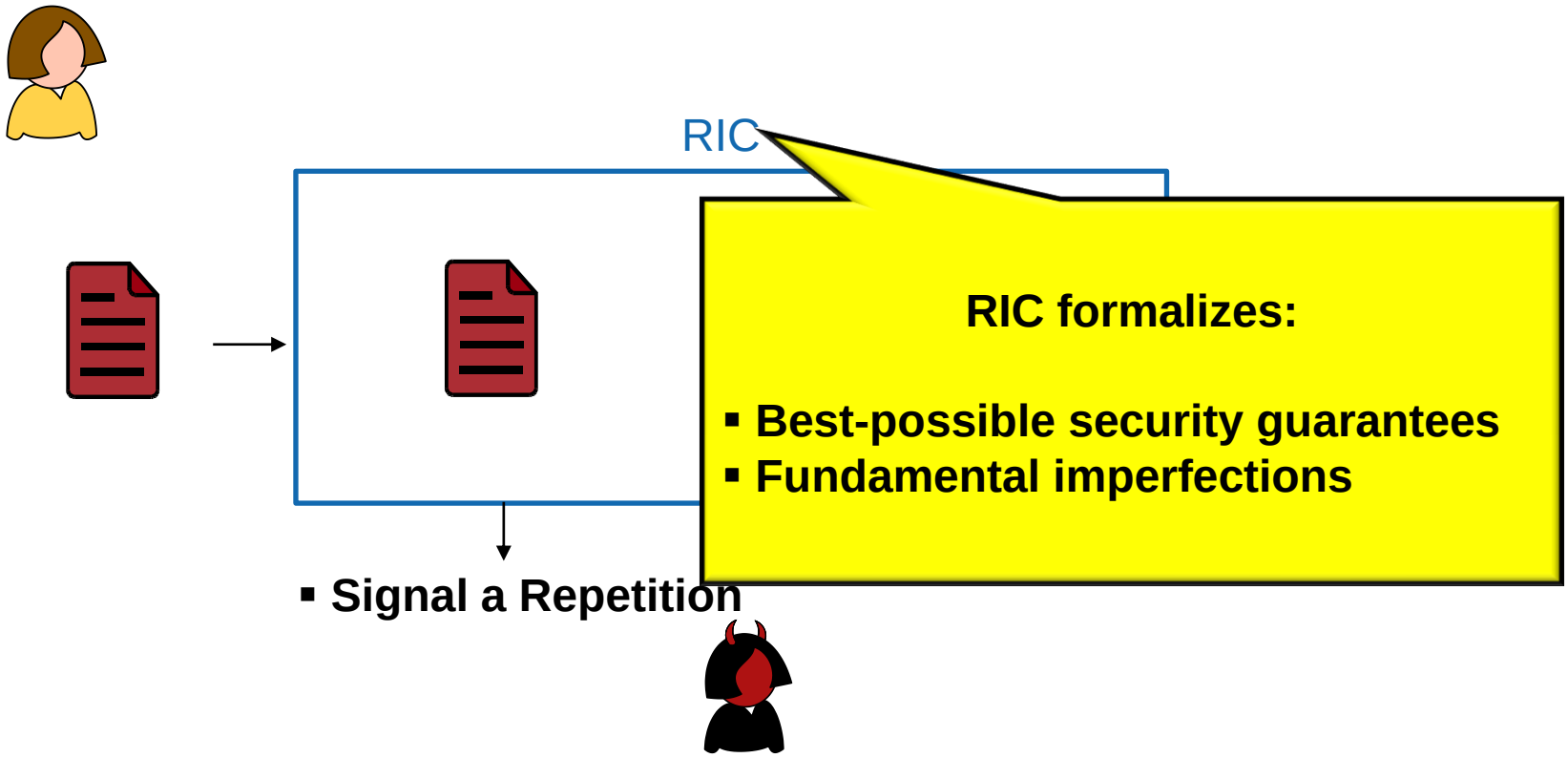
Random Injection Channel



- **Signal a Repetition**

The channel is not fully confidential.

Random Injection Channel

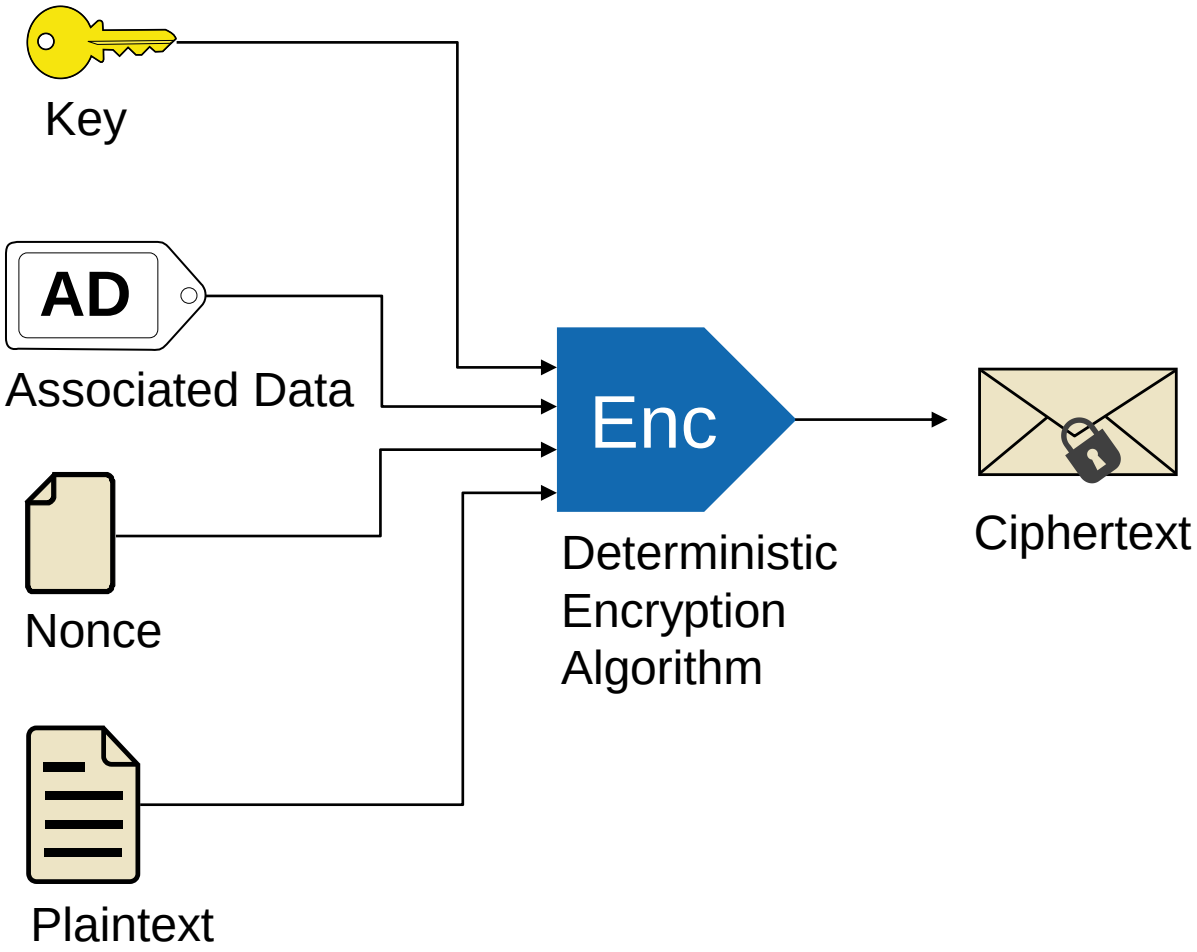


The channel is not fully confidential.

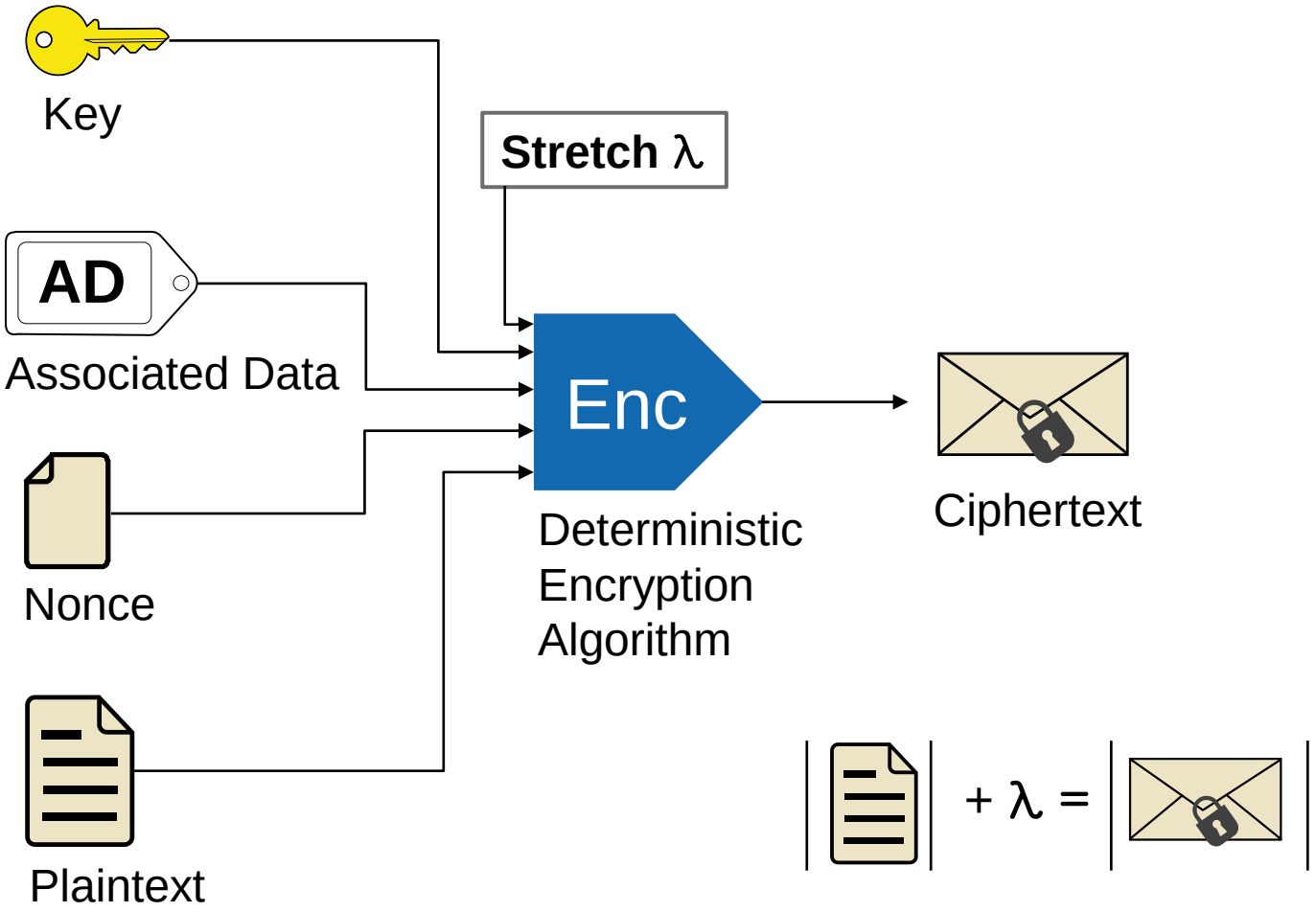
Roadmap

- **Fundamental limitations** of protecting communication in the **private key setting**?
- **Best schemes** within those limits?
  - Robust Authenticated-Encryption Schemes [HKR15].

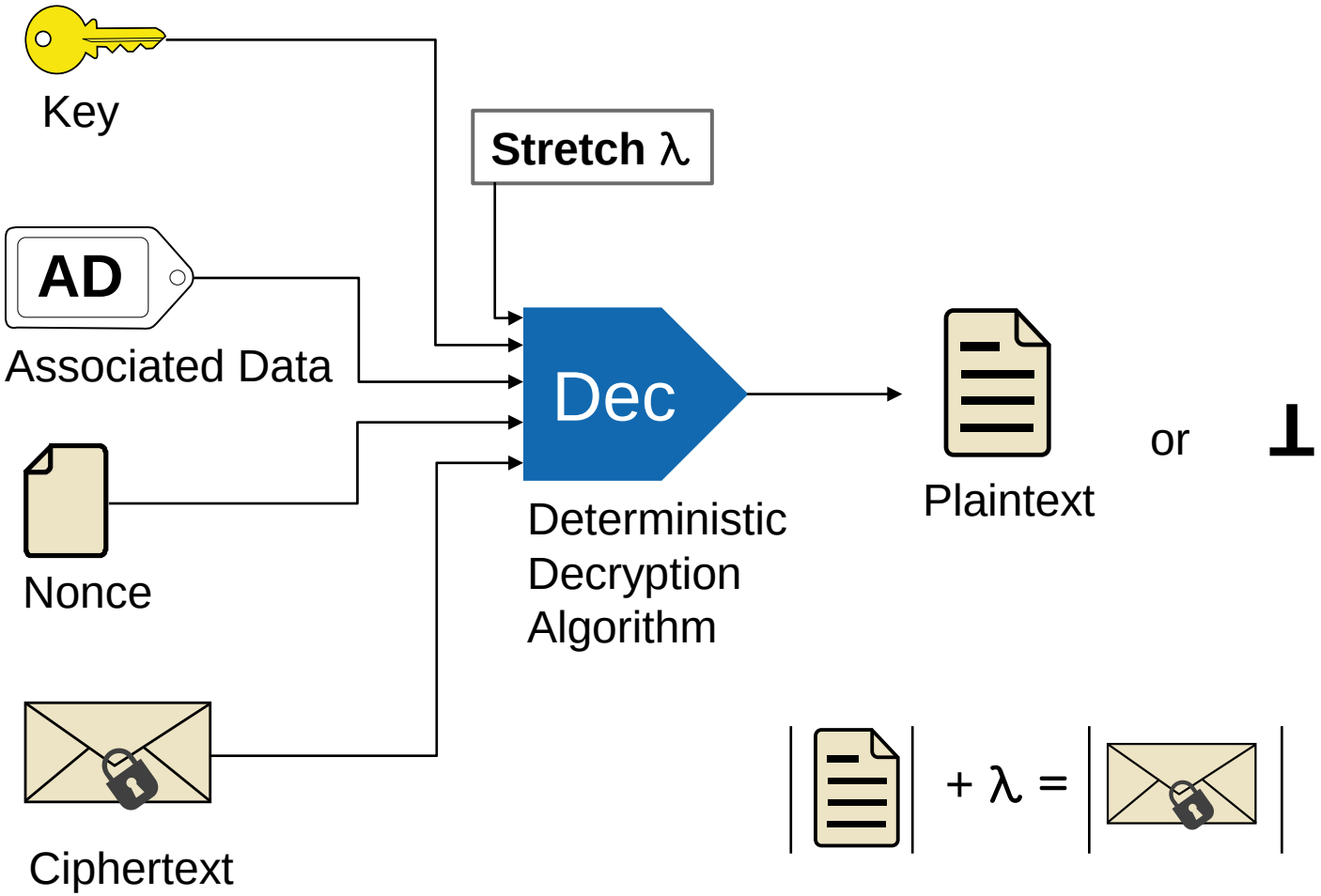
Robust Authenticated Encryption



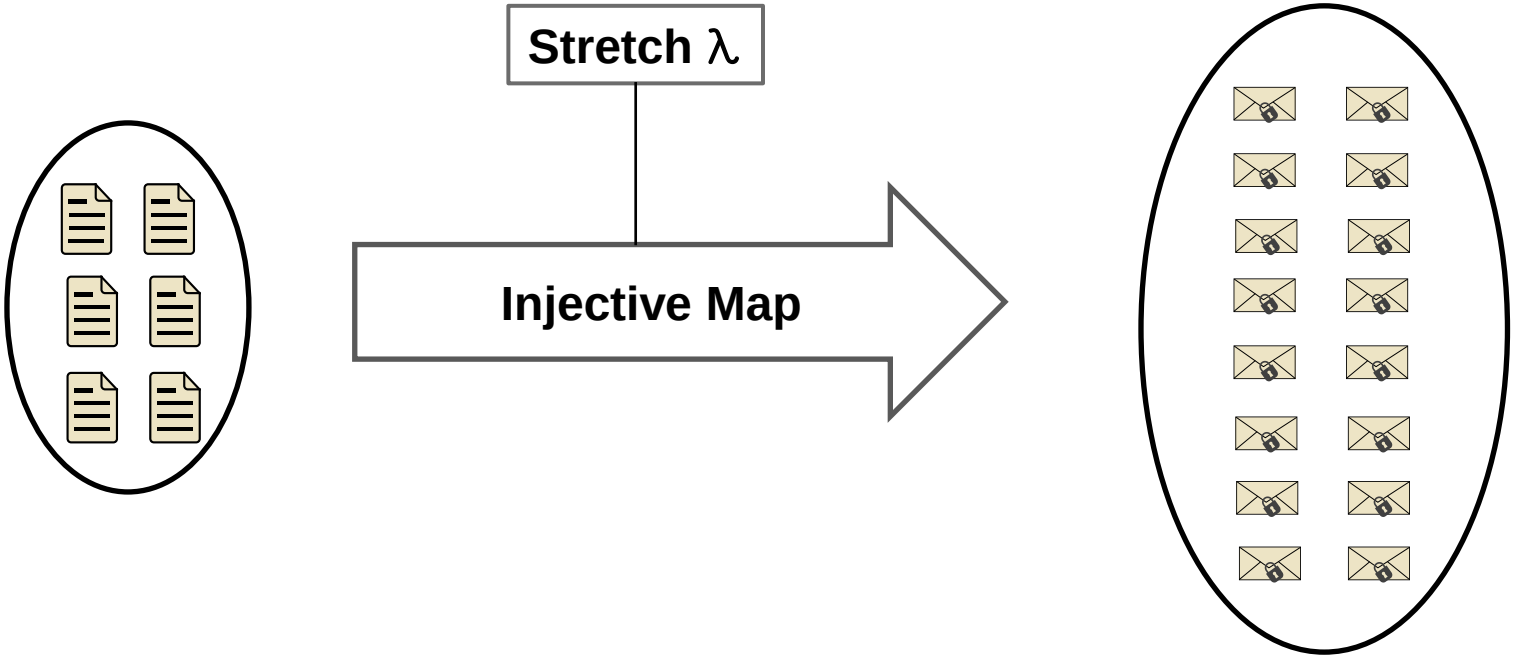
Robust Authenticated Encryption



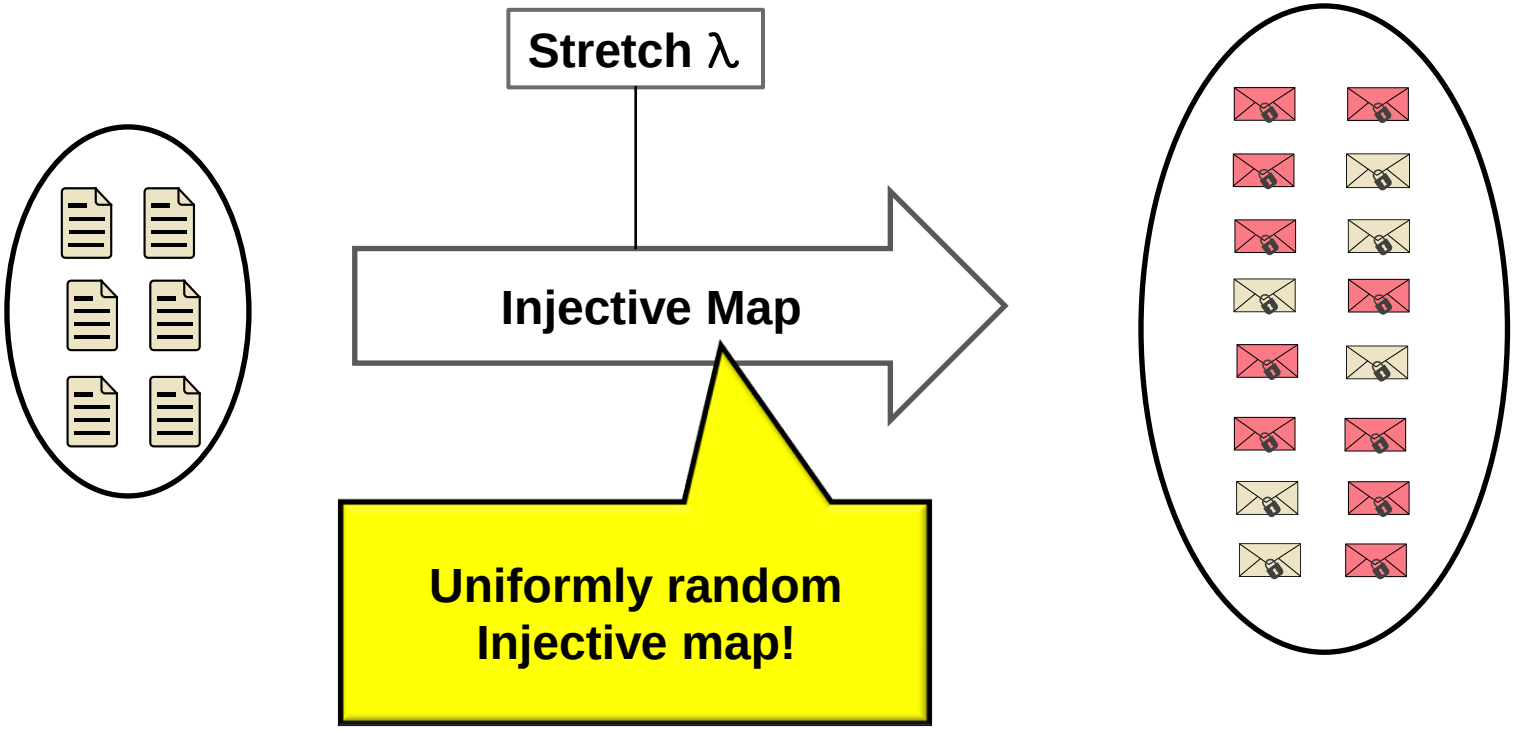
Robust Authenticated Encryption



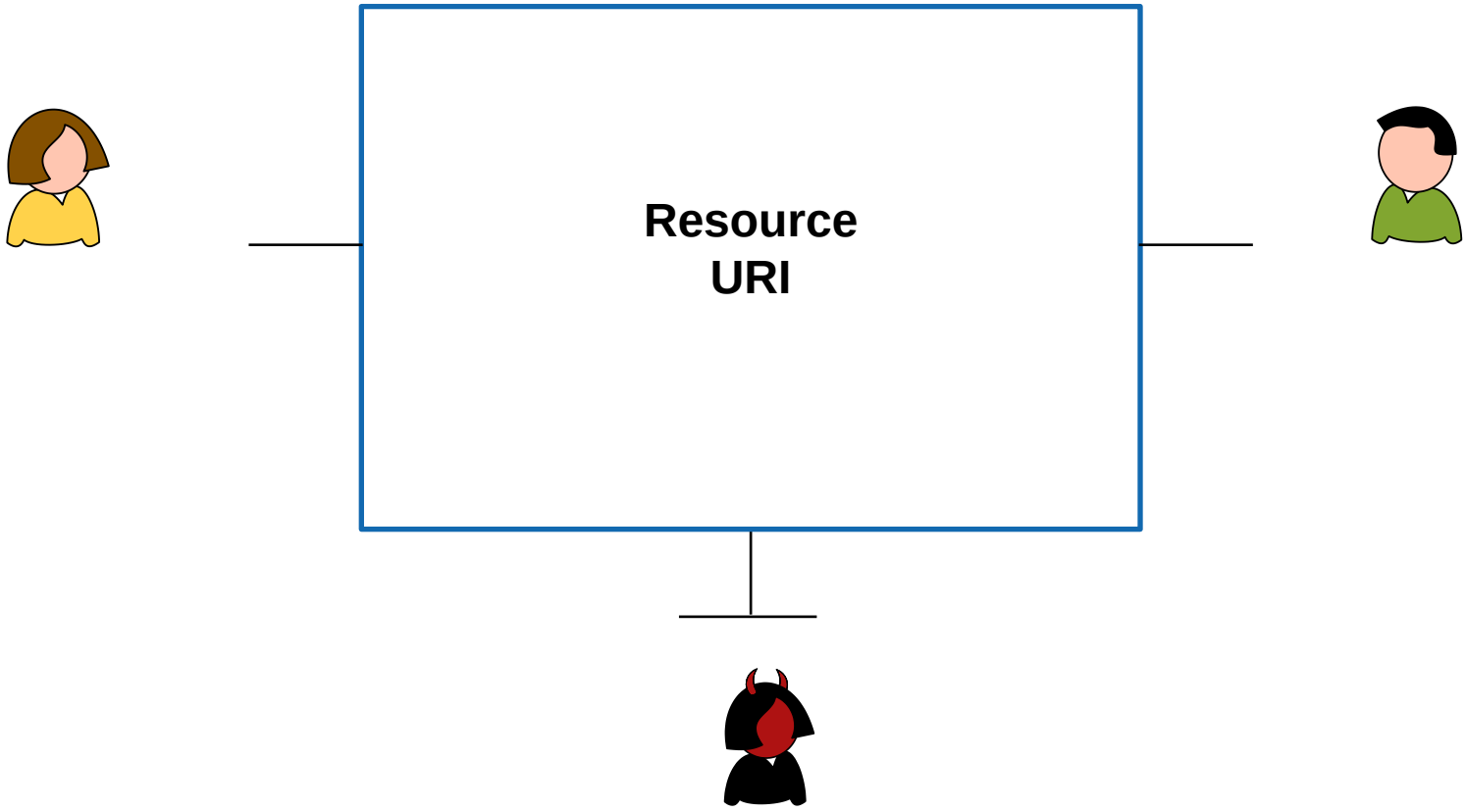
Security of RAE – The idea



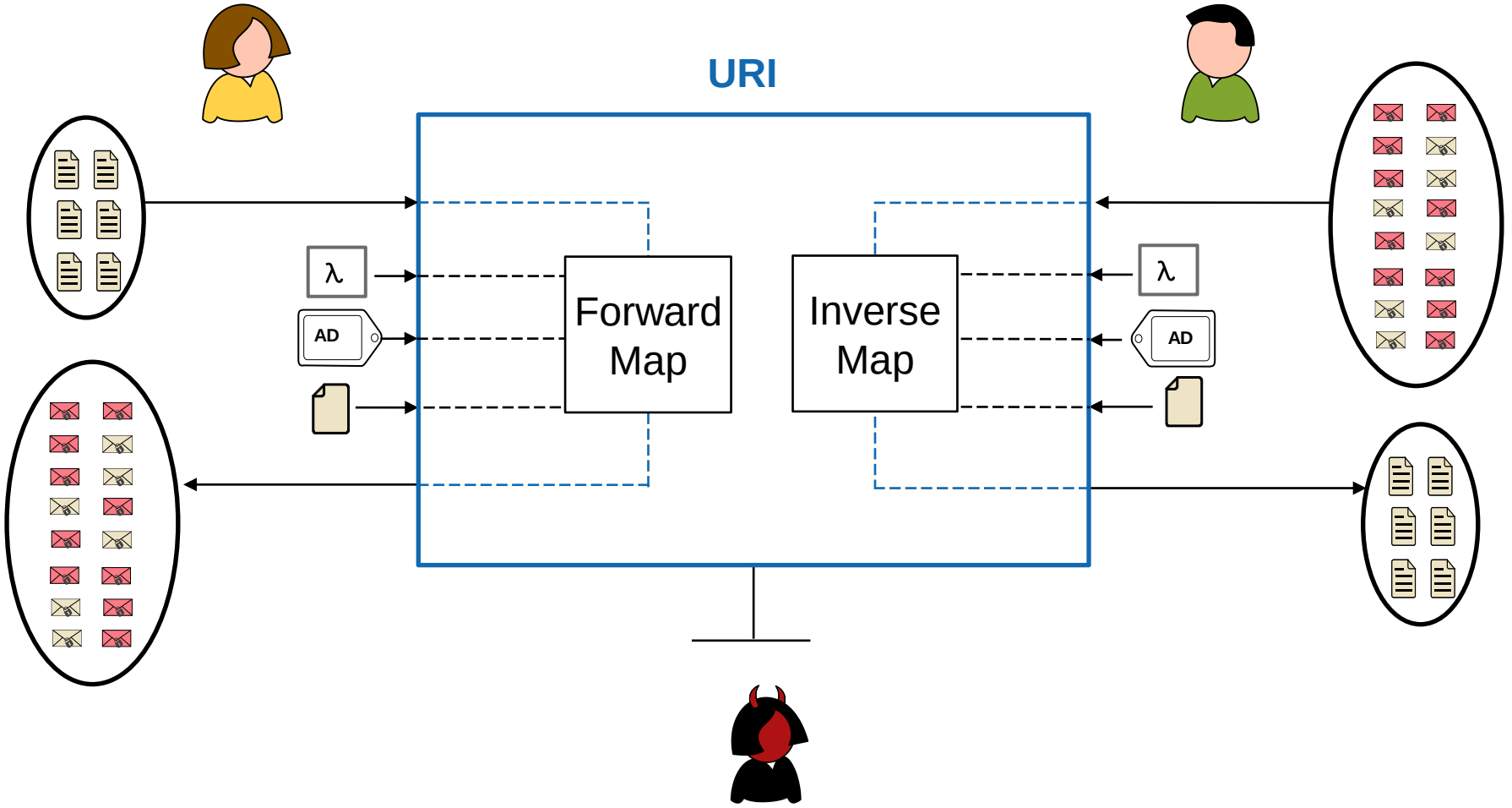
Security of RAE – The idea



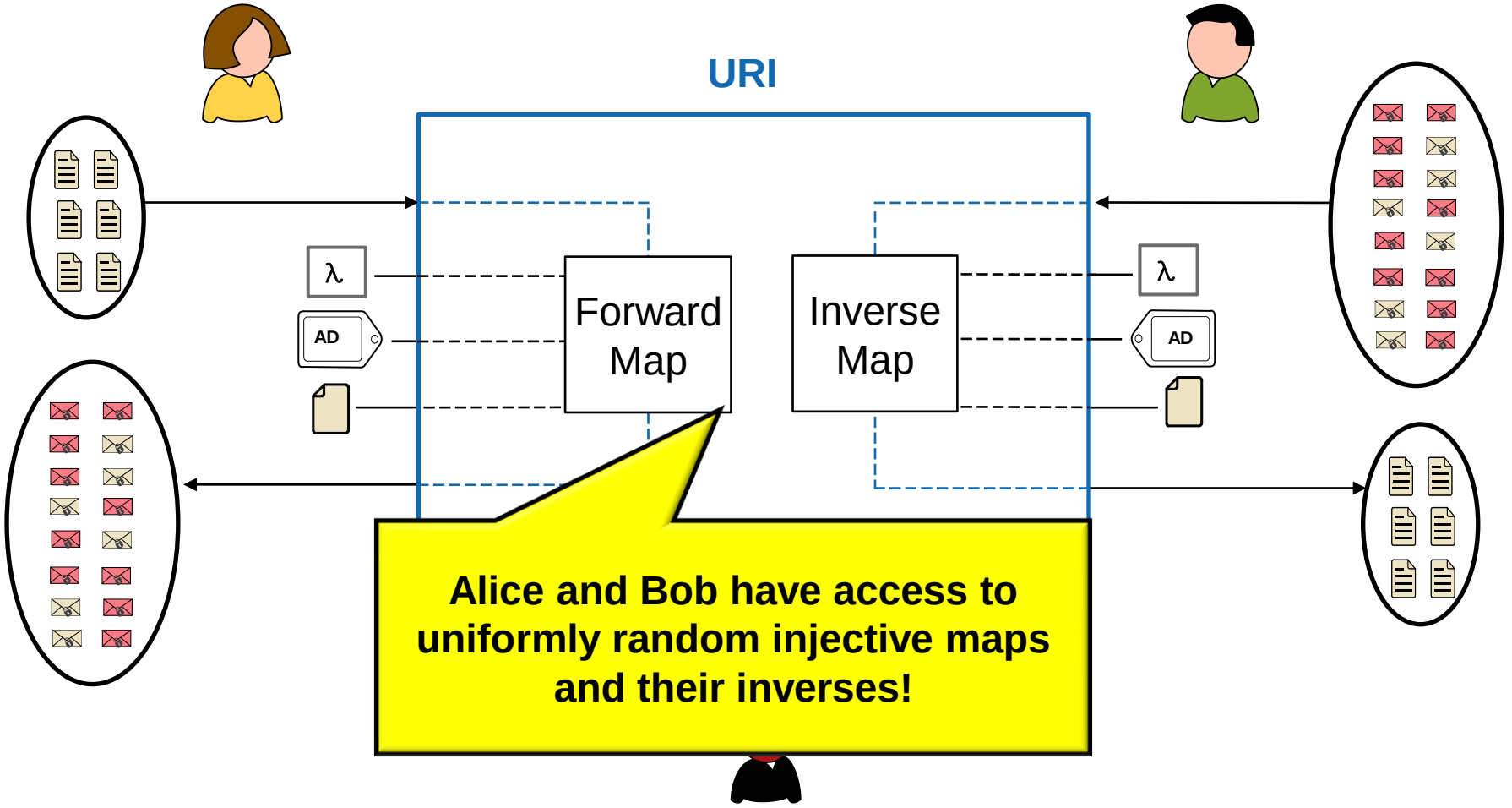
Security of RAE



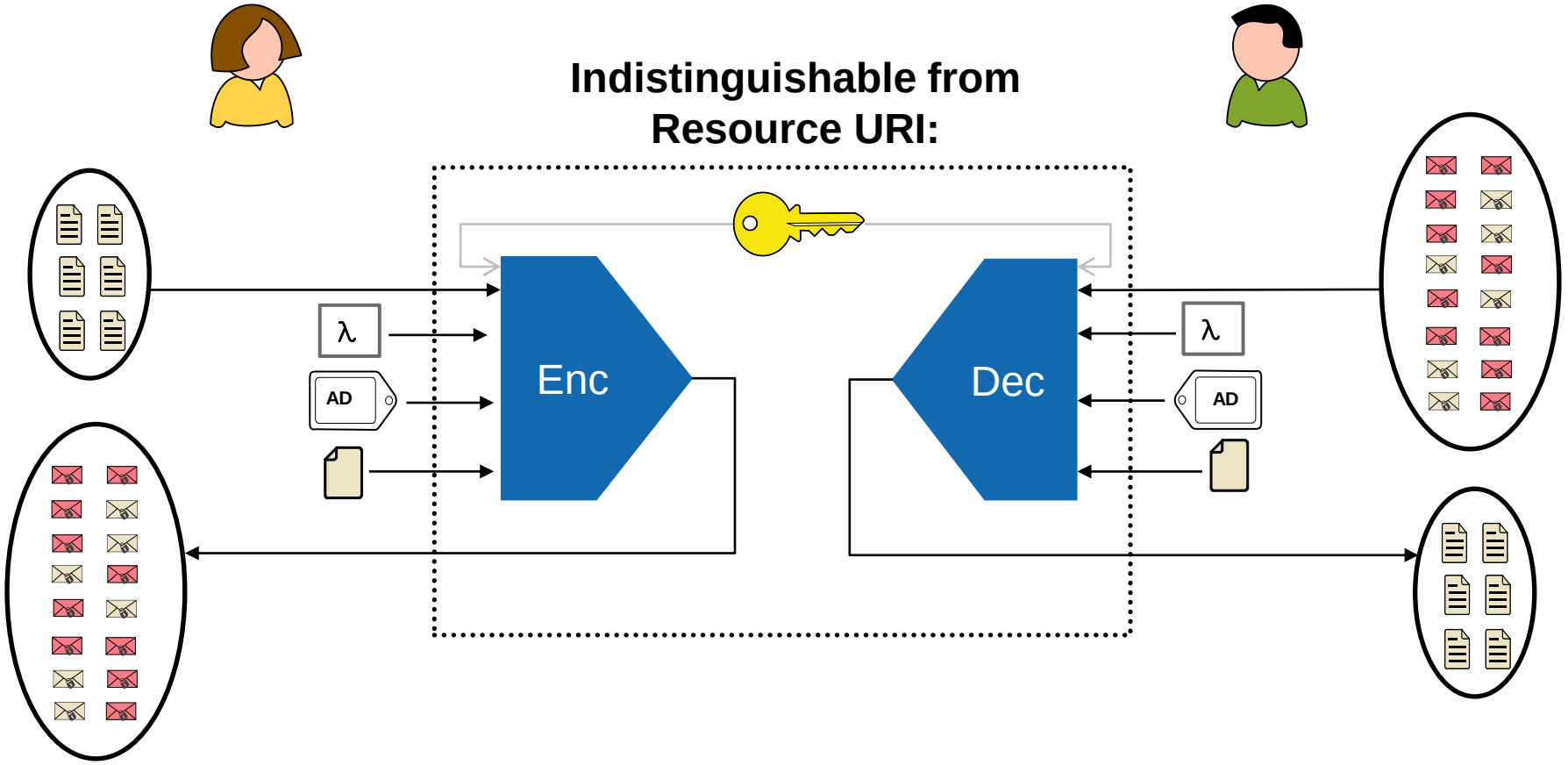
Security of RAE



Security of RAE



Security of RAE



RIC from Uniformly Random Injective Maps

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

The real world:

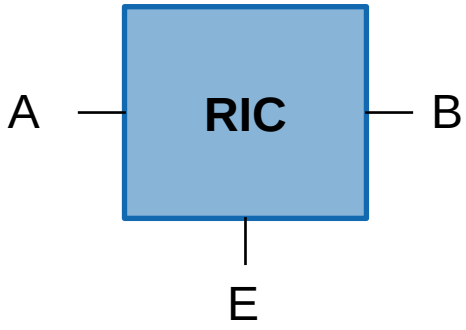
The idealized world:

RIC from Uniformly Random Injective Maps

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

The real world:

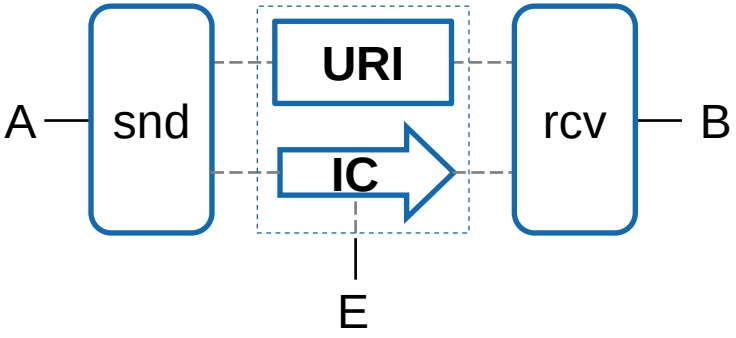
The idealized world:



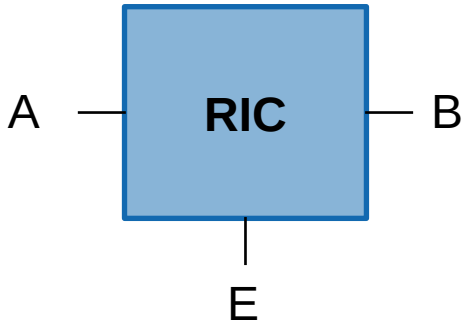
RIC from Uniformly Random Injective Maps

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

The real world:



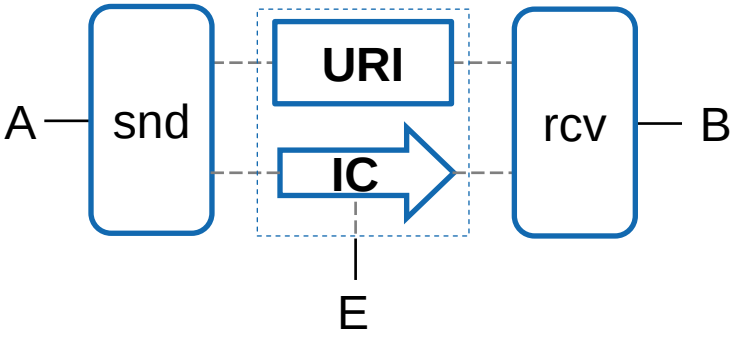
The idealized world:



RIC from Uniformly Random Injective Maps

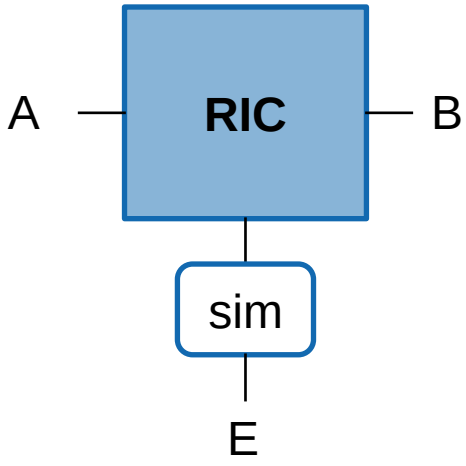
- The construction notion of constructive cryptography [MR11, Mau11]:

The real world:



=

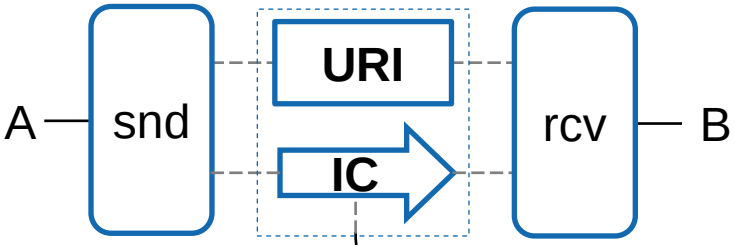
The idealized world:



RIC from Uniformly Random Injective Maps

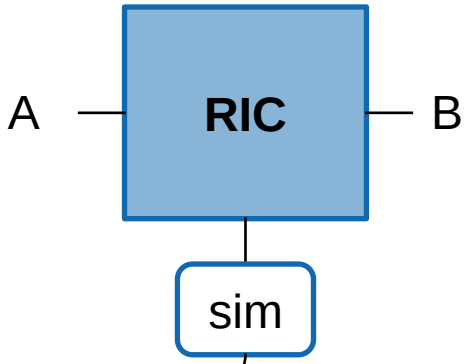
- The construction notion of constructive cryptography [MR11, Mau11]:

The real world:



=

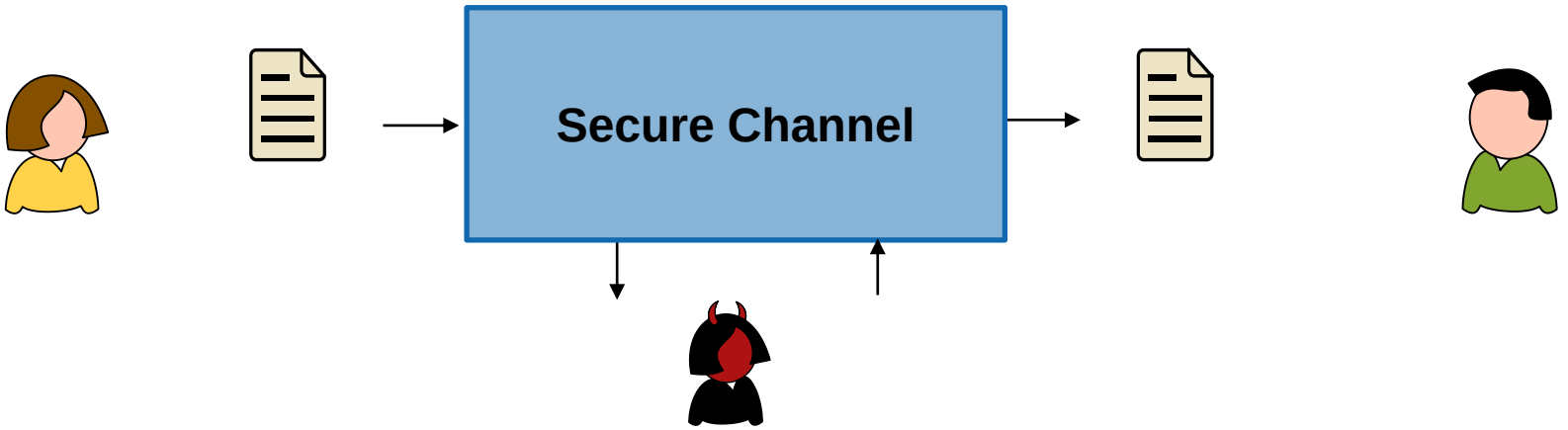
The idealized world:



Adversarial influence is the same
in both worlds

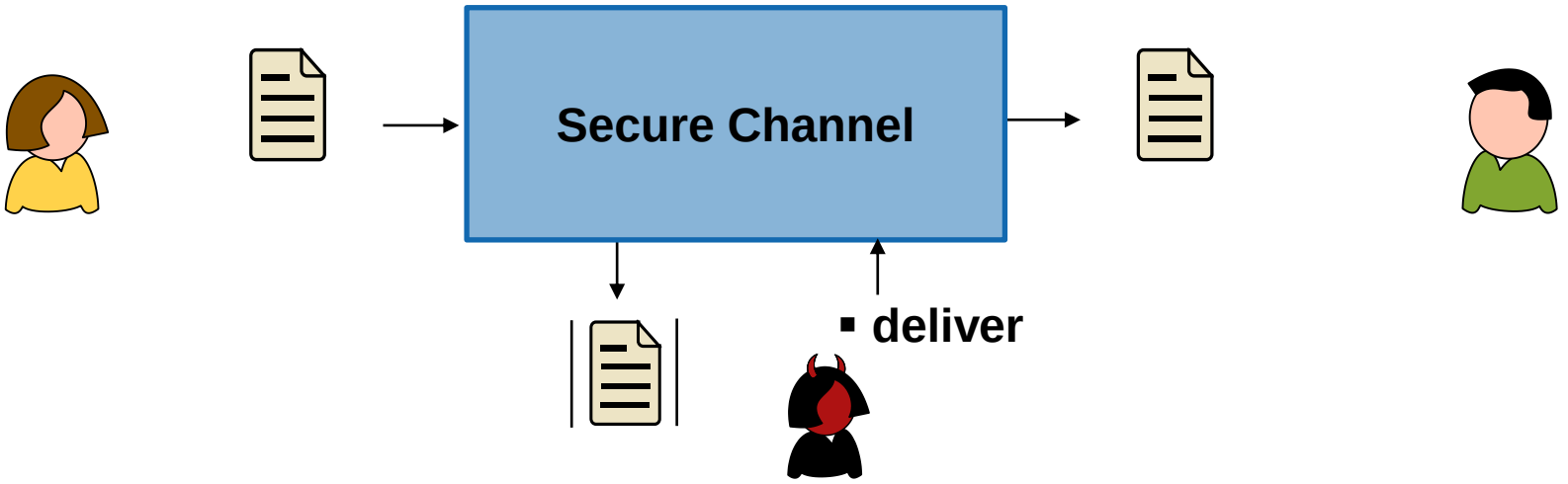
RIC: Corollaries

1.) For large ciphertext expansion, all bad events „vanish“:



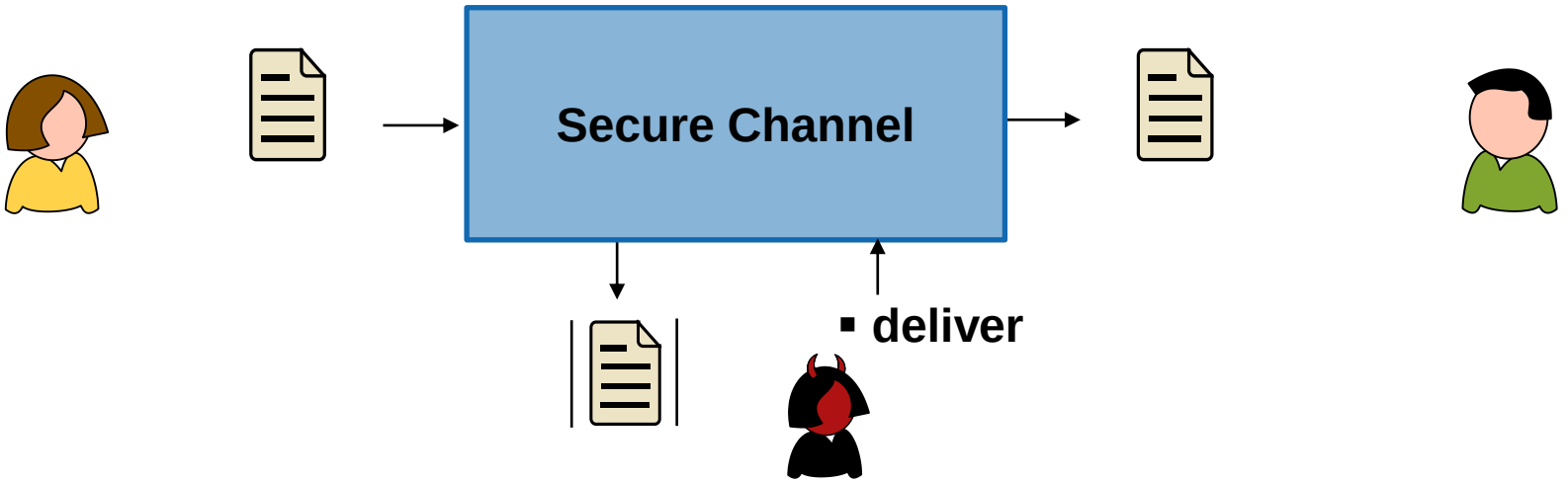
RIC: Corollaries

1.) For large ciphertext expansion, all bad events „vanish“:



RIC: Corollaries

1.) For large ciphertext expansion, all bad events „vanish“:

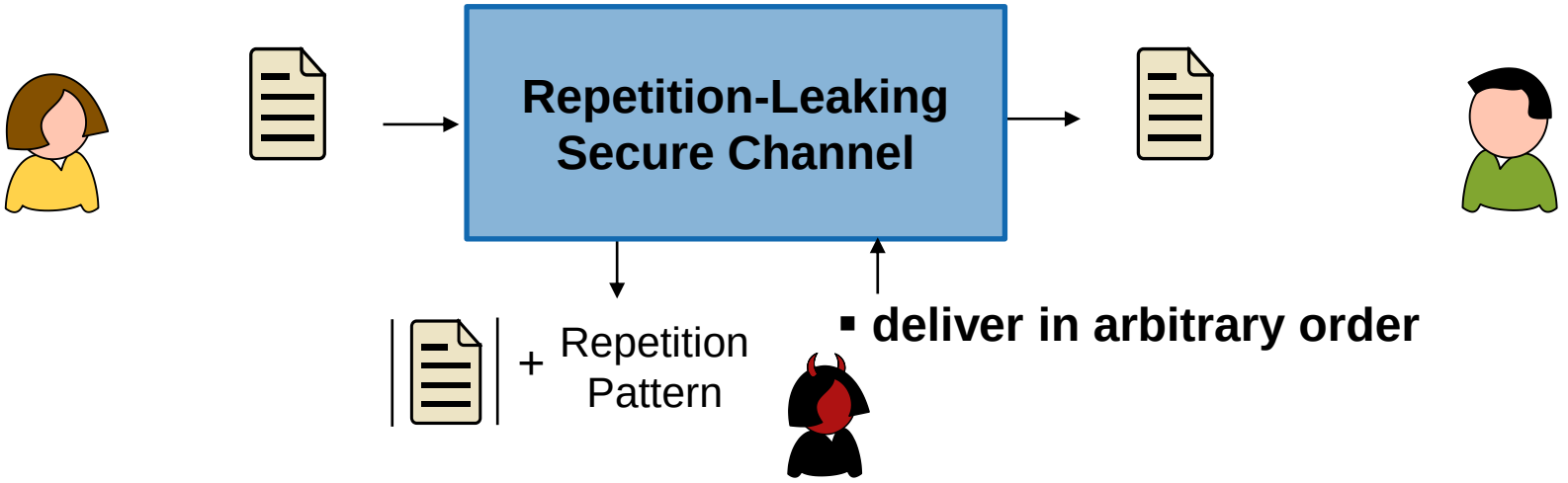


2.) Checking redundancy in messages increases authenticity.

Our proof directly implies the validity of the corresponding claim in [HKR15].

Also in the paper...

- Analysis of Nonce-Reuse Misuse-Case of RAE:



Summary

- Random injection channels provably capture the best-possible security guarantees achievable by symmetric schemes.

- Robust authenticated encryption schemes can be used to construct such channels.

- Our approach further allows to formally prove claims about RAE and its misuse-cases.

Contact information and credits

ETH Zurich

Department of Computer Science

Universitätsstrasse 6

8092 Zurich

References:

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

[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/