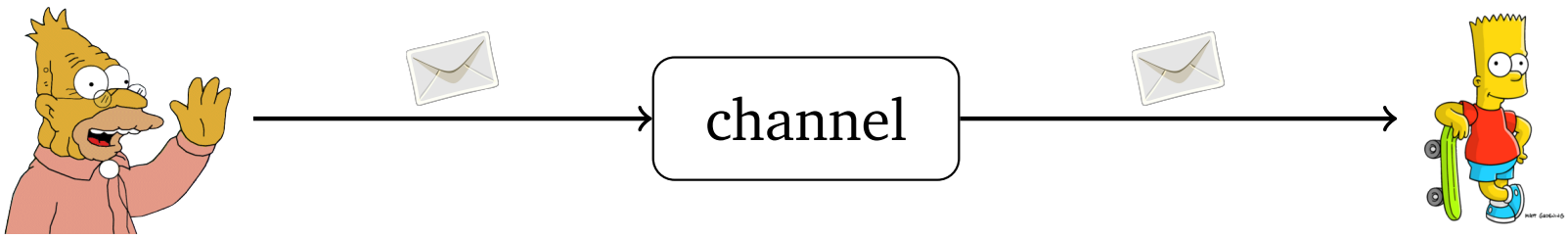
Formalizing the Malleability of Encryption

Ueli Maurer and Björn Tackmann, ETH Zürich.

Eurocrypt Rump Session, June 1st, 2010.

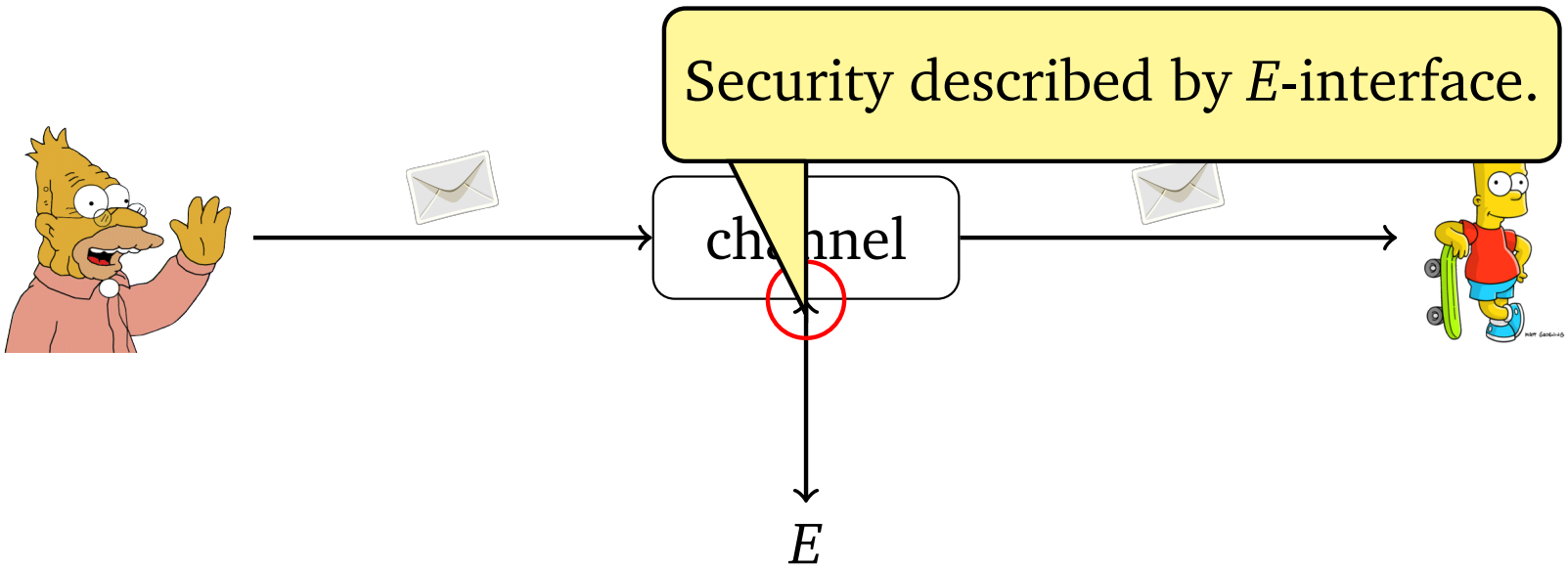
Formalizing Secure Communication

Communication between two entities as a system:

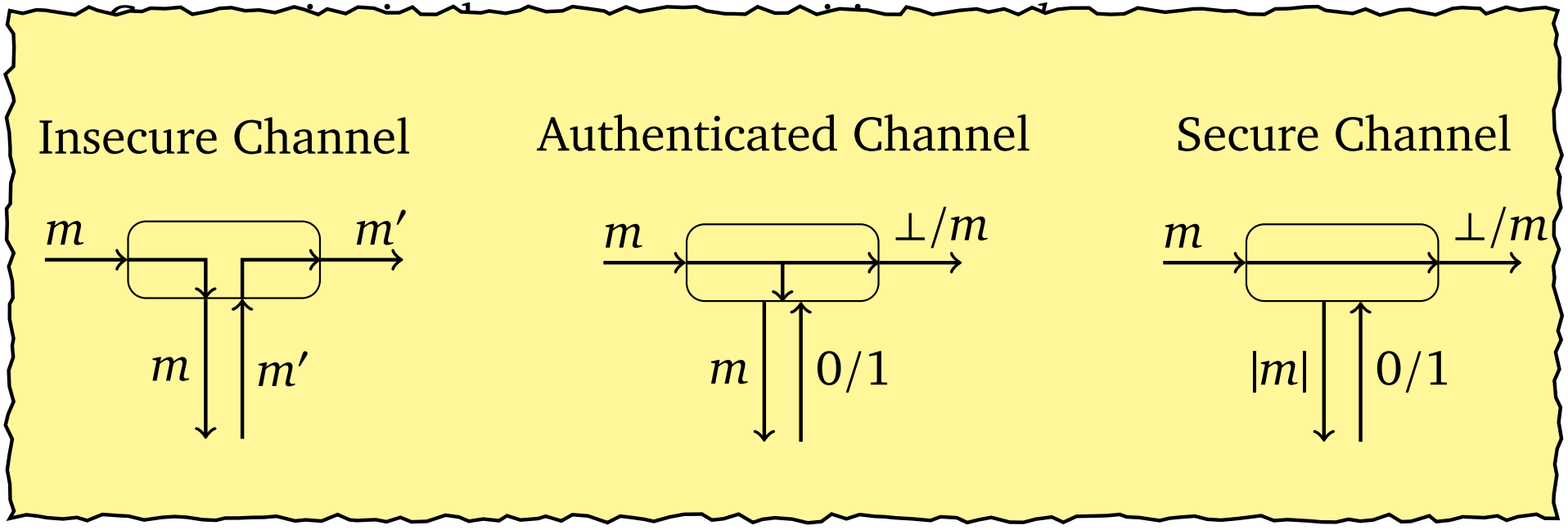


Formalizing Secure Communication

Communication between two entities as a *three-party* system:

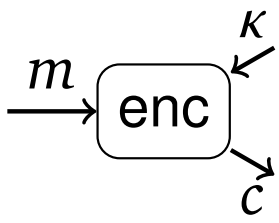


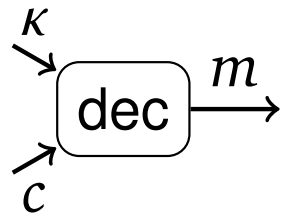
Formalizing Secure Communication



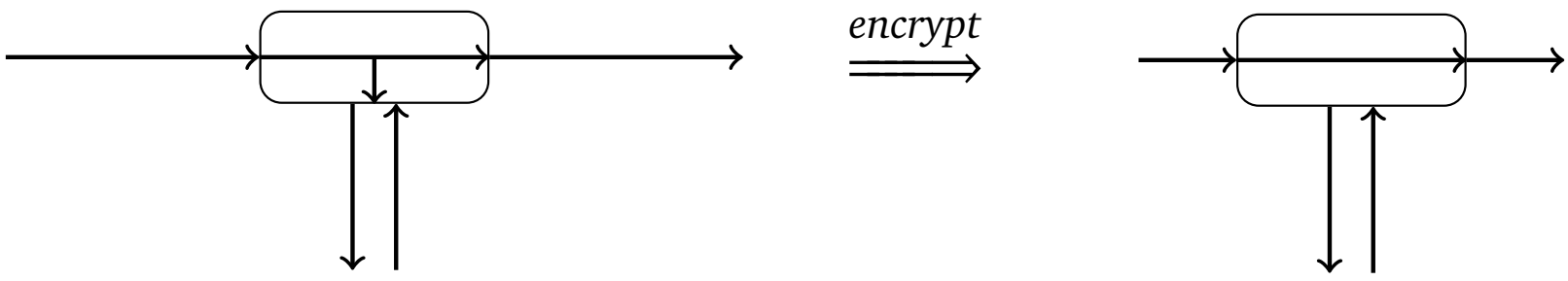
Protocols: Constructing "More Secure" Channels

Example (Encryption):



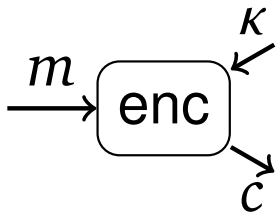


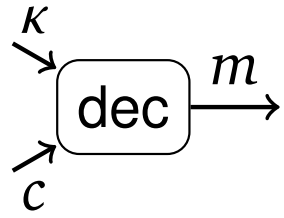
Constructing a **secure** from an **authenticated channel**:



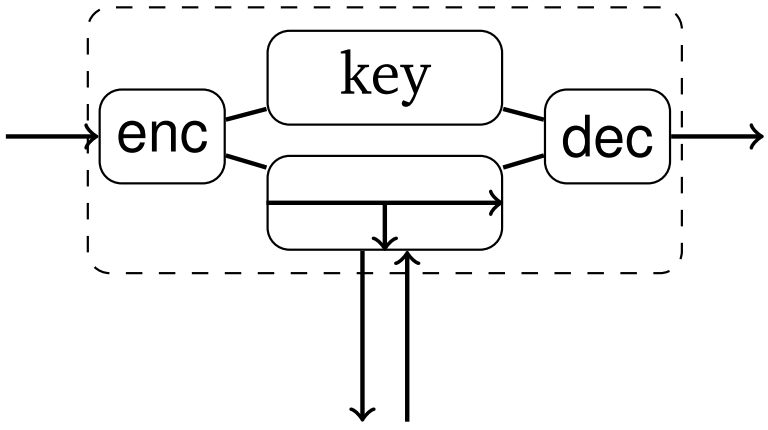
Protocols: Constructing "More Secure" Channels

Example (Encryption):

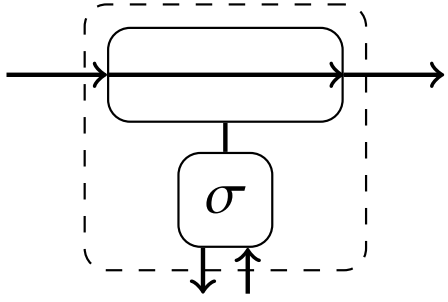




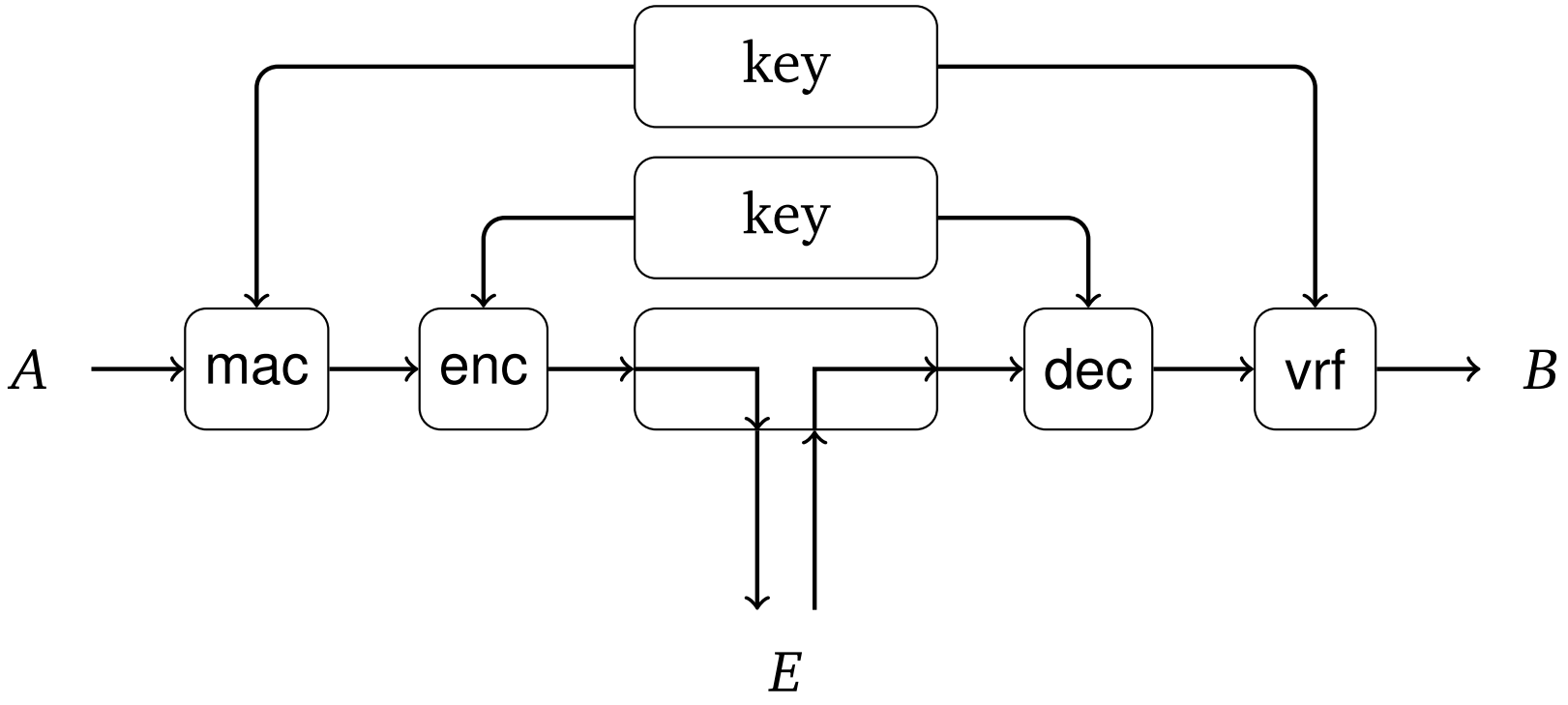
Constructing a **secure** from an **authenticated channel**:



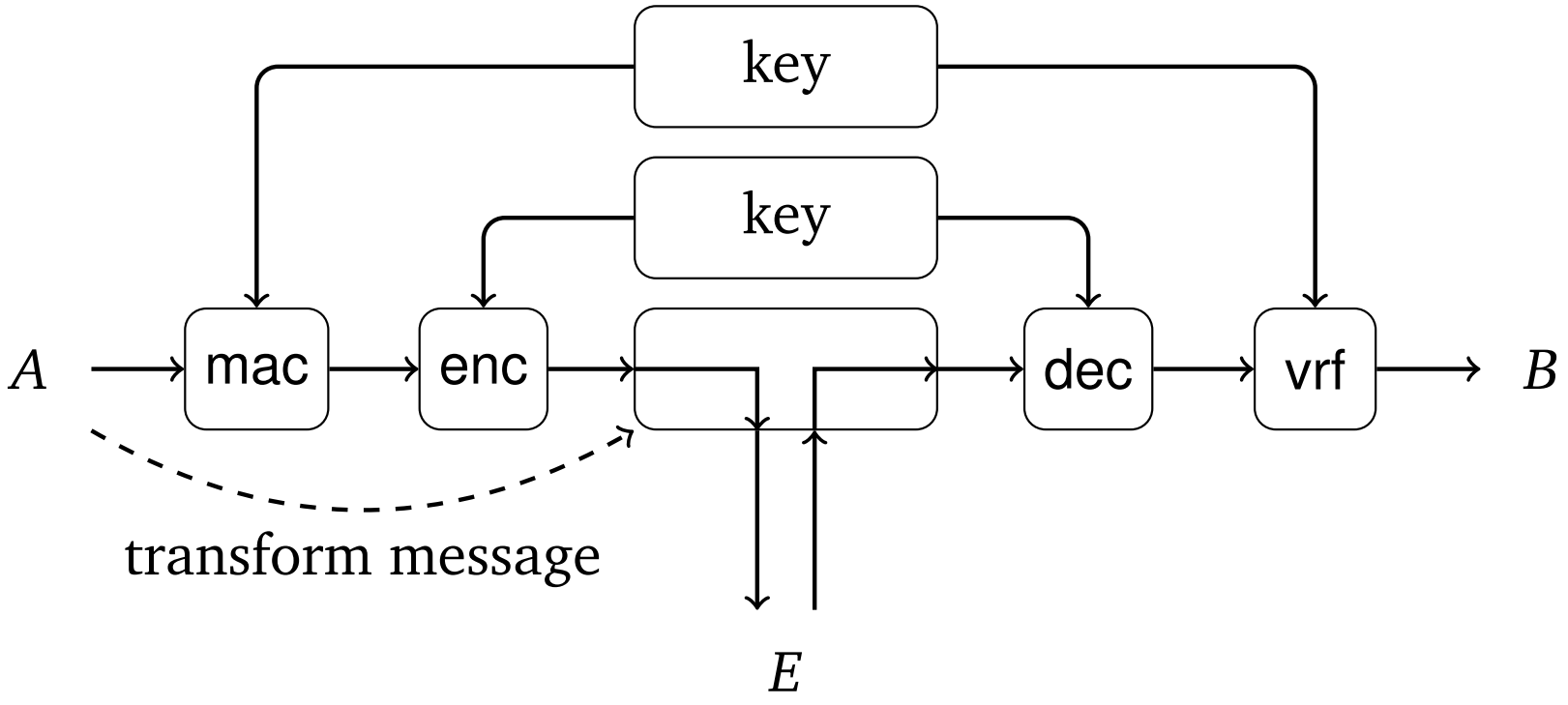
≈



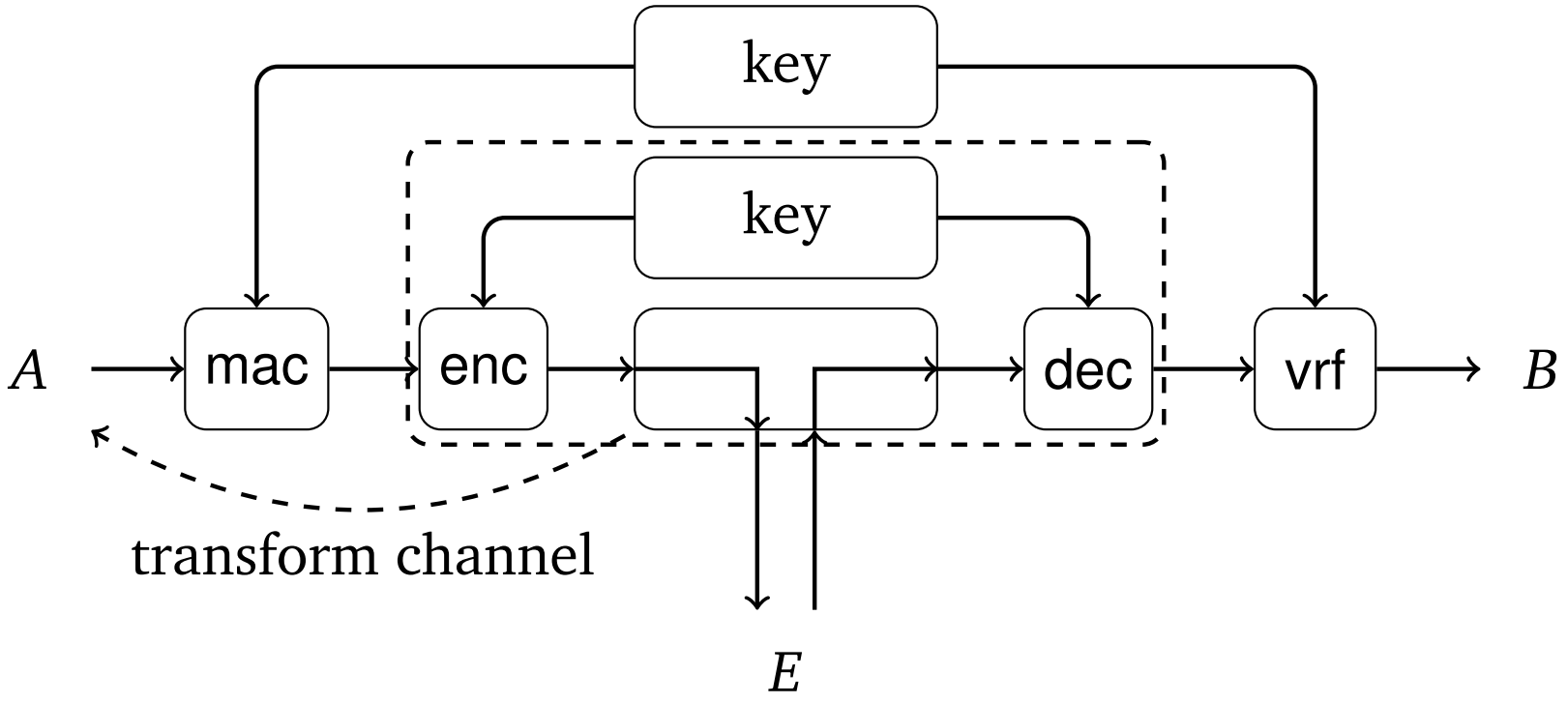
Malleability and Authenticate-then-Encrypt



Malleability and Authenticate-then-Encrypt

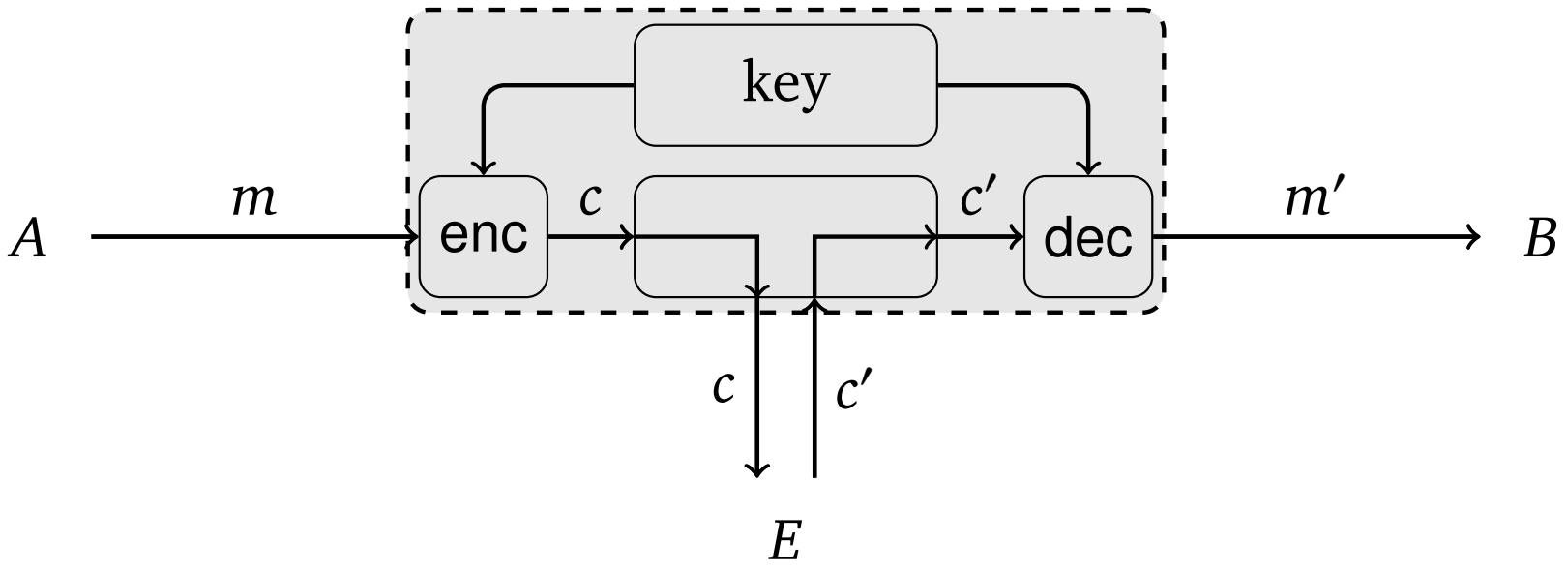


Malleability and Authenticate-then-Encrypt



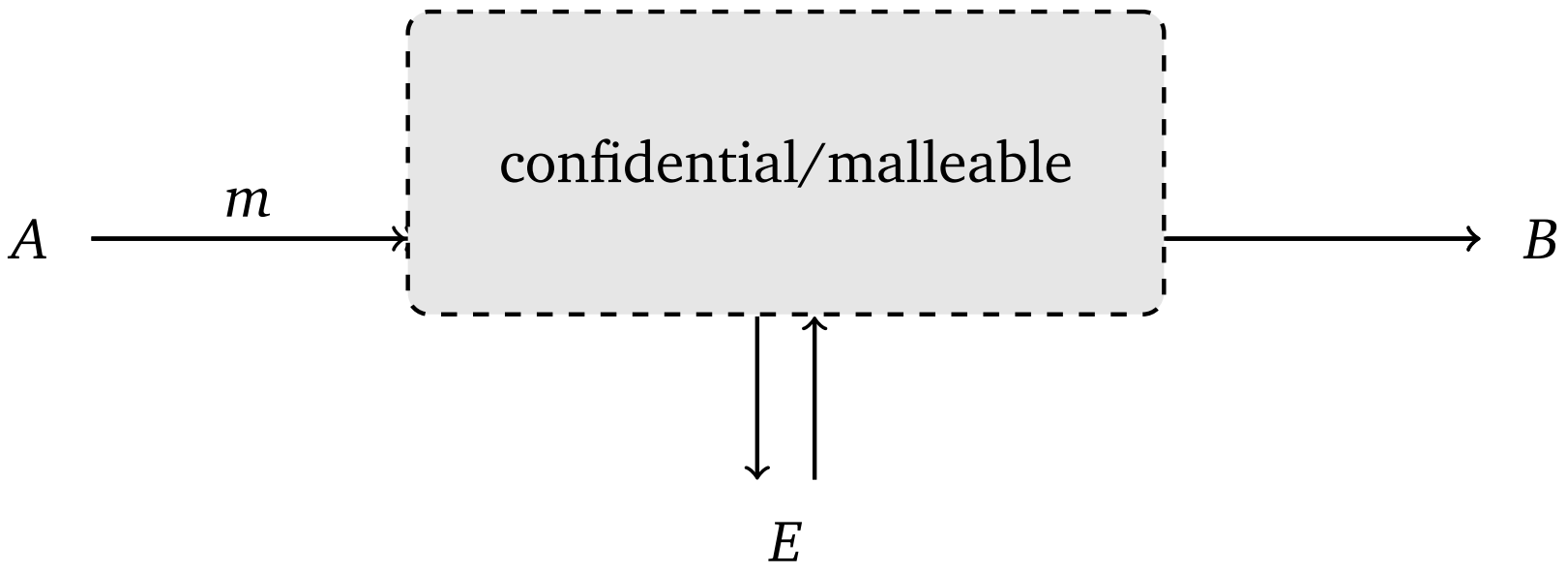
- Encryption directly applied to the insecure channel.

Malleability and Authenticate-then-Encrypt



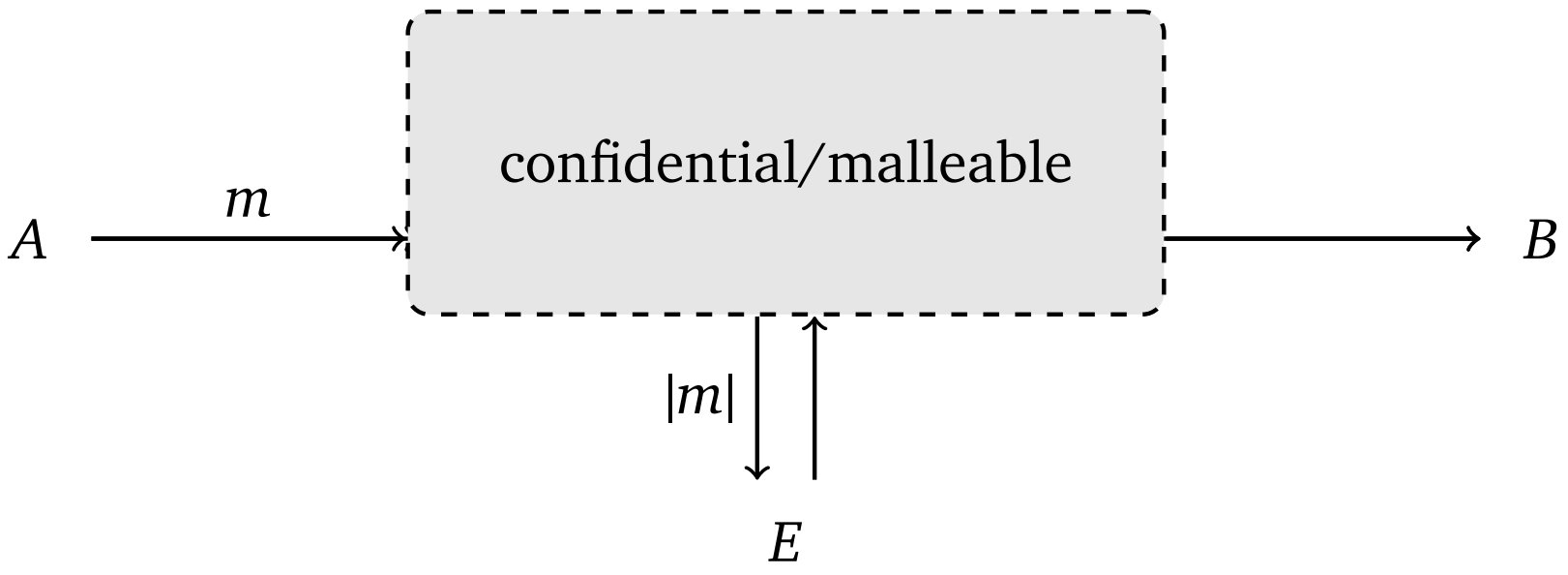
- Encryption directly applied to the insecure channel.

Malleability and Authenticate-then-Encrypt



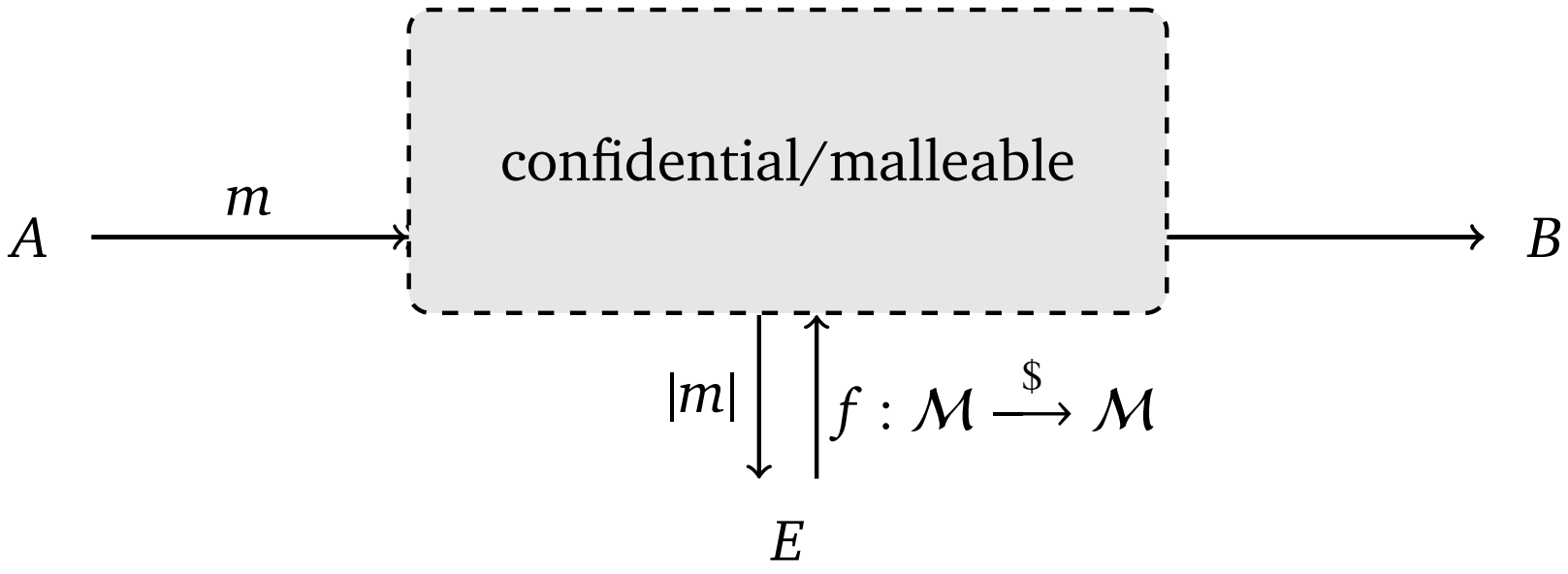
- Encryption directly applied to the insecure channel.

Malleability and Authenticate-then-Encrypt



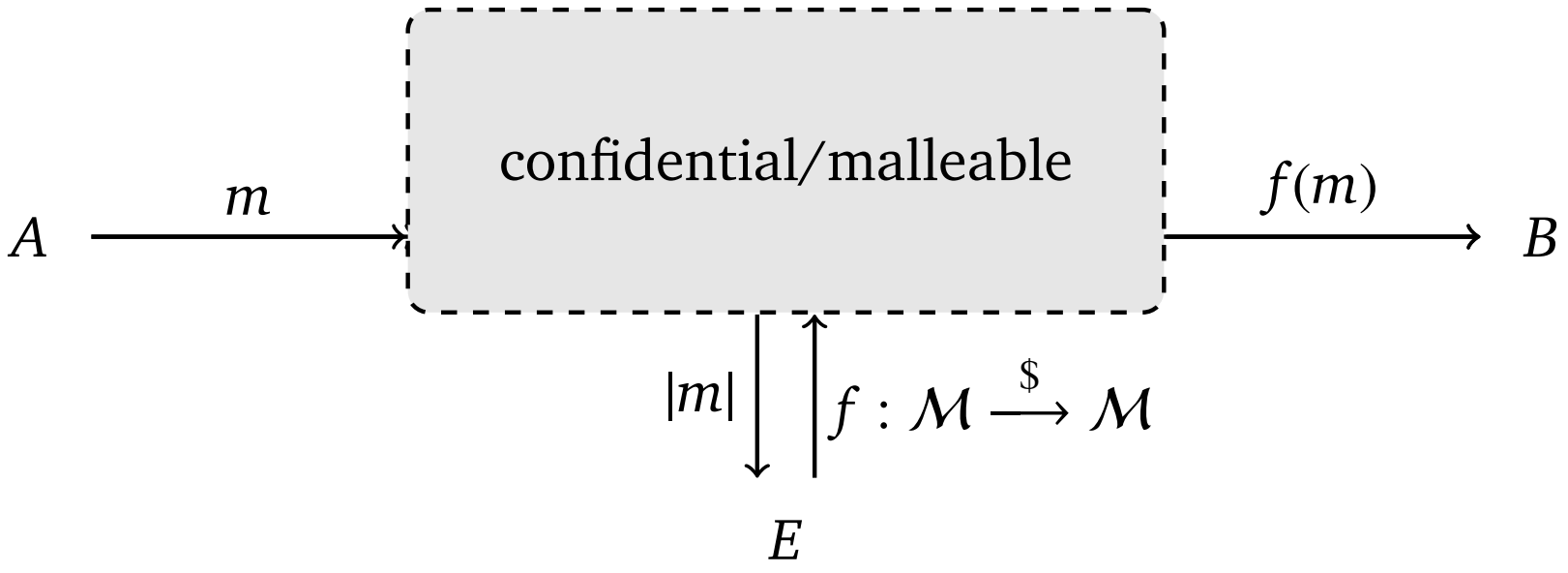
- Encryption directly applied to the insecure channel.

Malleability and Authenticate-then-Encrypt



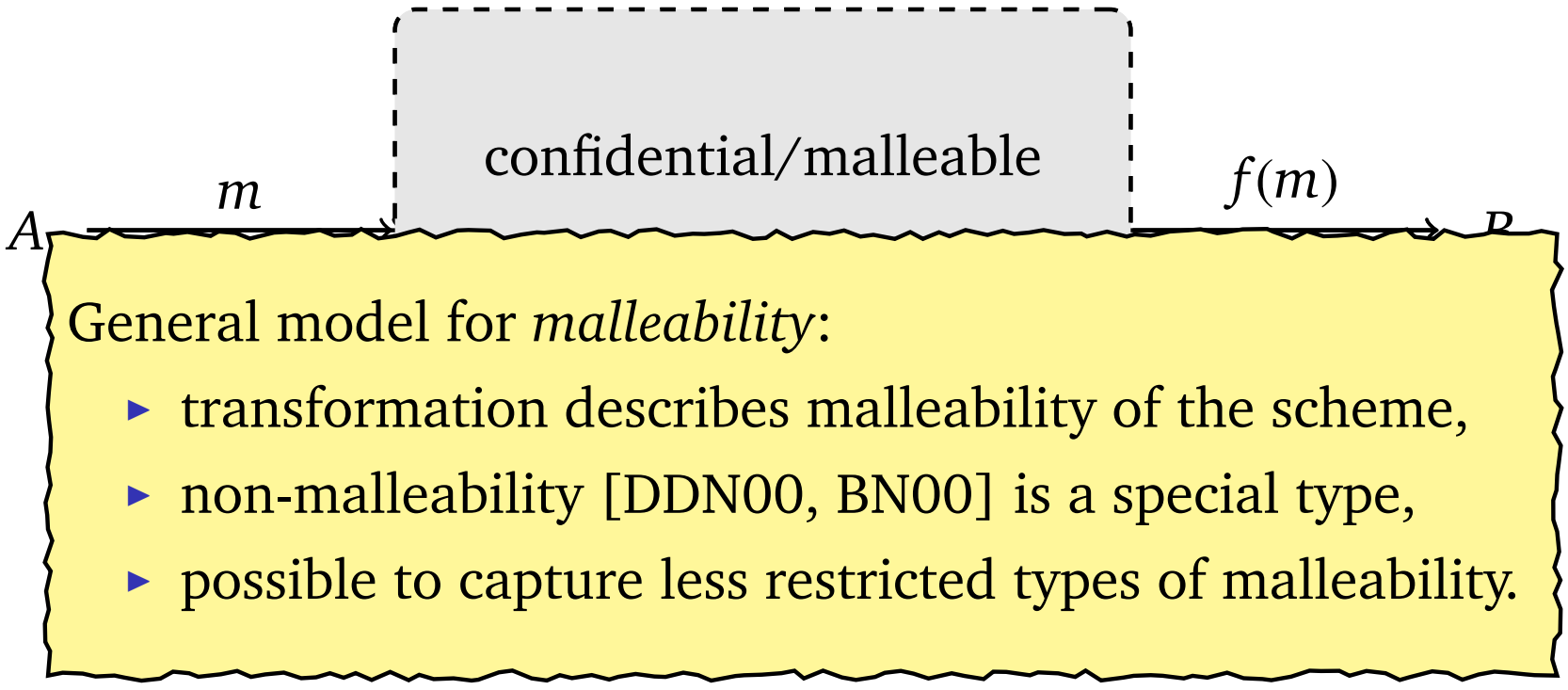
- Encryption directly applied to the insecure channel.

Malleability and Authenticate-then-Encrypt



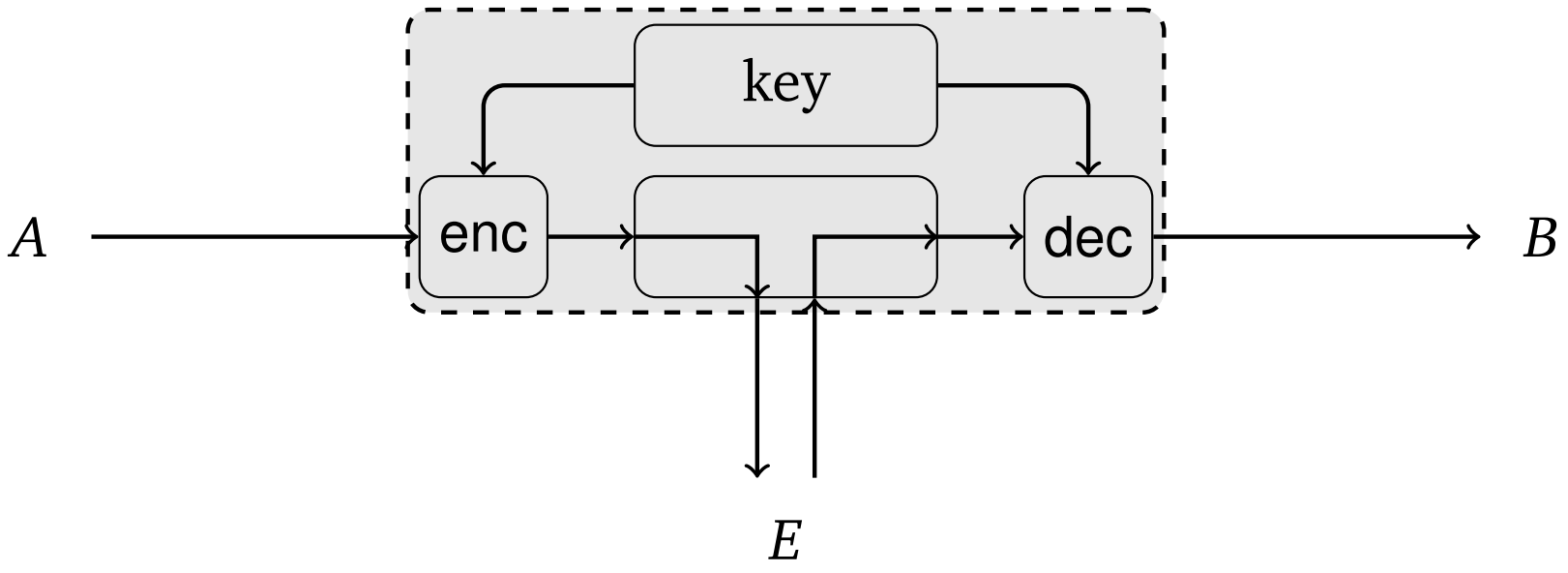
- Encryption directly applied to the insecure channel.

Malleability and Authenticate-then-Encrypt



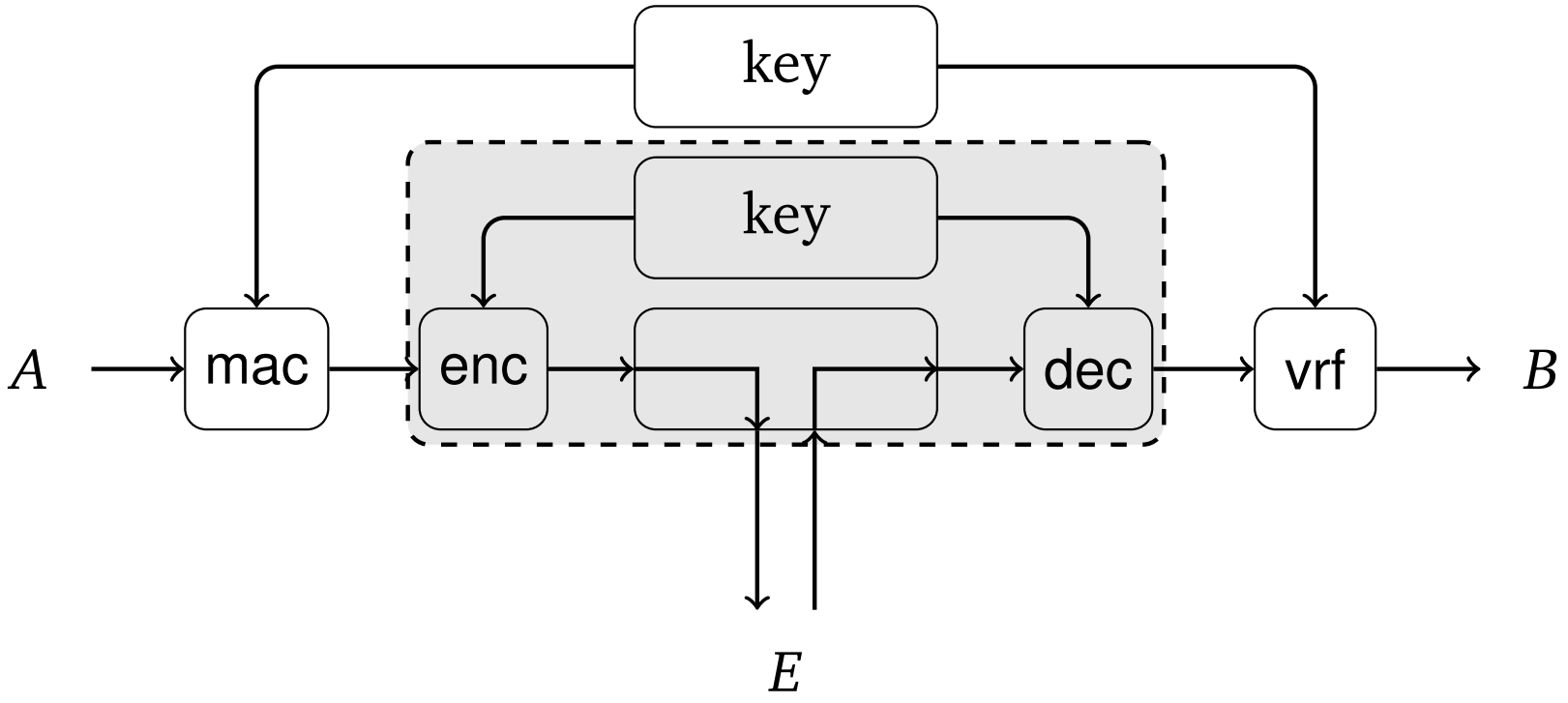
- Encryption directly applied to the insecure channel.

Malleability and Authenticate-then-Encrypt



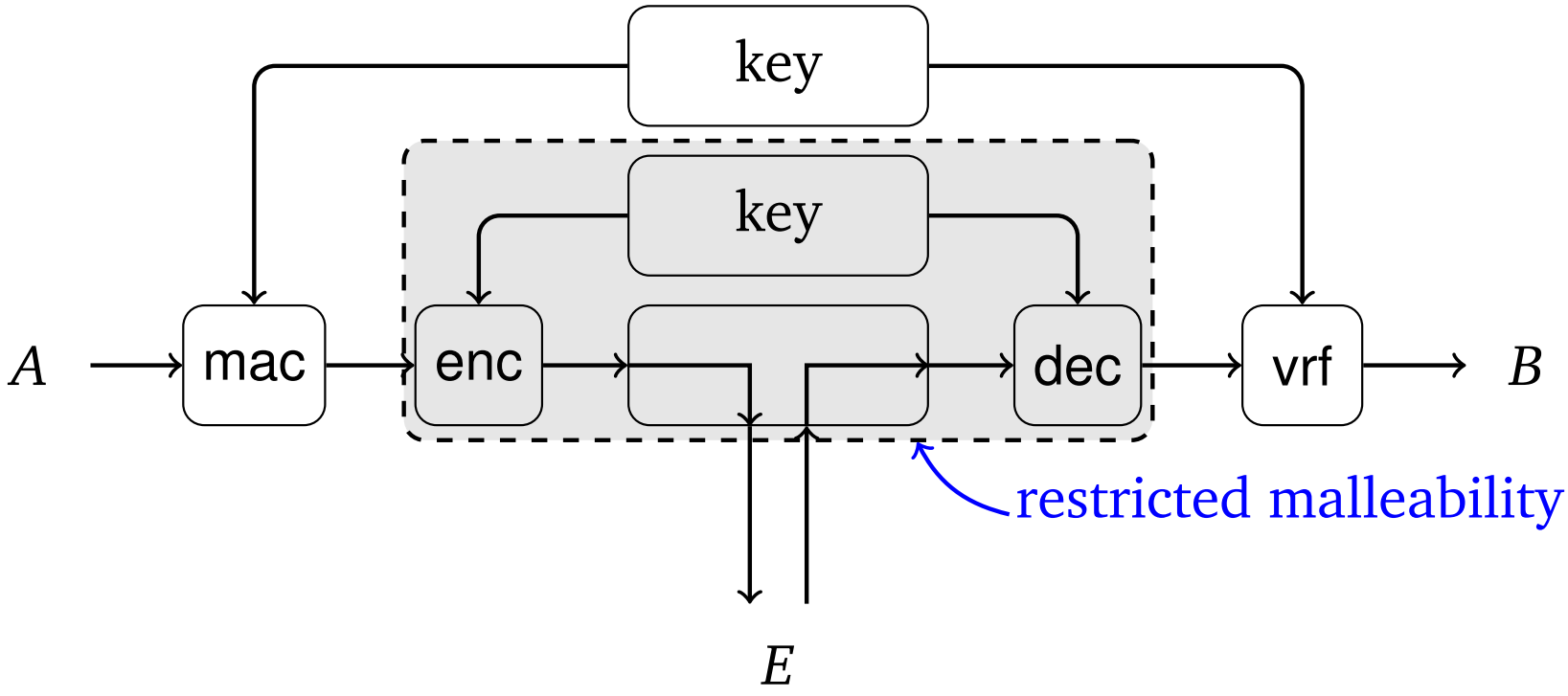
- Encryption directly applied to the insecure channel.

Malleability and Authenticate-then-Encrypt



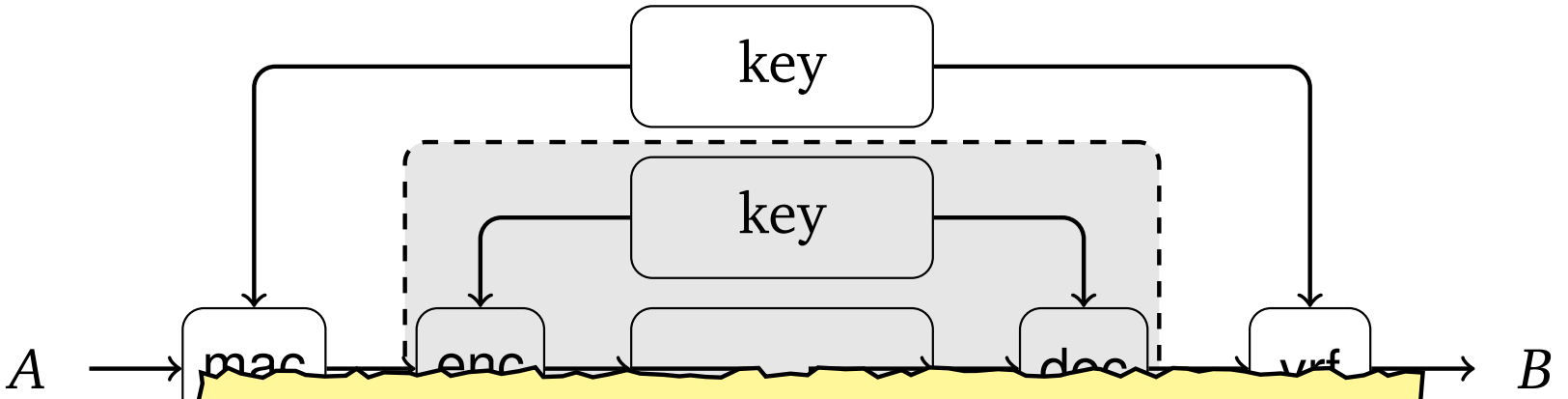
- Encryption directly applied to the insecure channel.

Malleability and Authenticate-then-Encrypt



- Encryption directly applied to the insecure channel.
- Describe explicit restriction on the malleability.
- Generic proof for AtE with such schemes.
- Schemes from TLS are sufficient.

Malleability and Authenticate-then-Encrypt



Previous view [BN00, Kra01]:

- AtE **not** "generically" secure!

Our analysis suggests a different view:

- AtE **is** "generically" secure, but
- stricter security notion for encryption.

- Encr
- Describe explicit restriction on the malleability.
- Generic proof for AtE with such schemes.
- Schemes from TLS are sufficient.

Thanks!