Symmetric Security Review

Rohit Musti

CUNY - Hunter College

March 2, 2022

Outline

One Time Pad: Encryption

```
def encrypt(key, message):
    cipher_text = ""
    if len(key) != len(message):
      print("error, key is not the same length as the message'
      print("key length:", len(key))
      print("message length:", len(message))

    for i in range(len(key)):
      cipher_text += f"{key[i] != message[i]}"

    return cipher_text
```

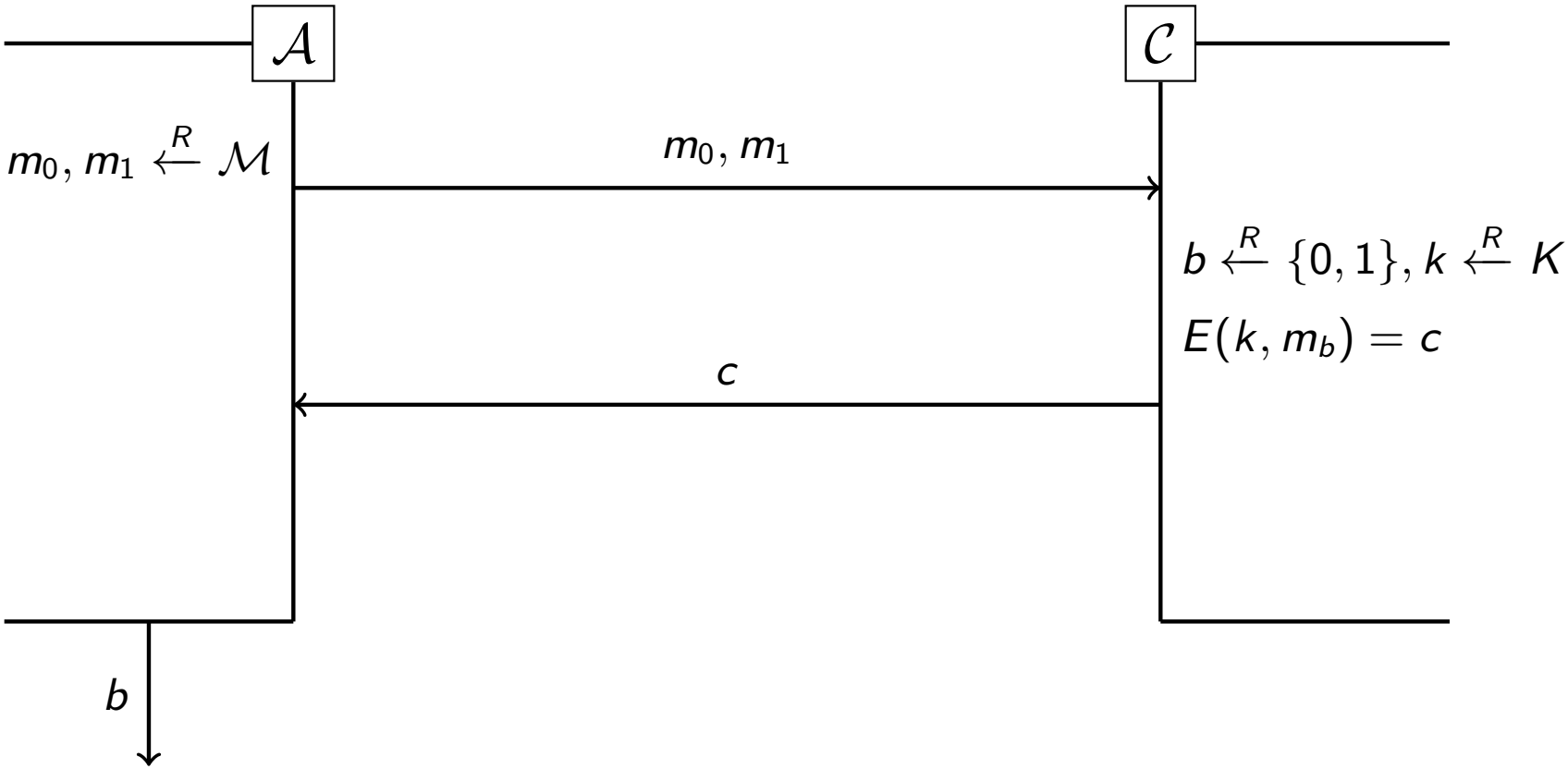
One Time Pad: Decryption

```
def decrypt(key, cipher_text):
    message = ""
    if len(key) != len(cipher_text):
      print("error, key is not the same length as the cipherte
      print("key length:", len(key))
      print("cipher_text length:", len(cipher_text))

    for i in range(len(key)):
      message += f"{key[i] != cipher_text[i]}"

    return message
```

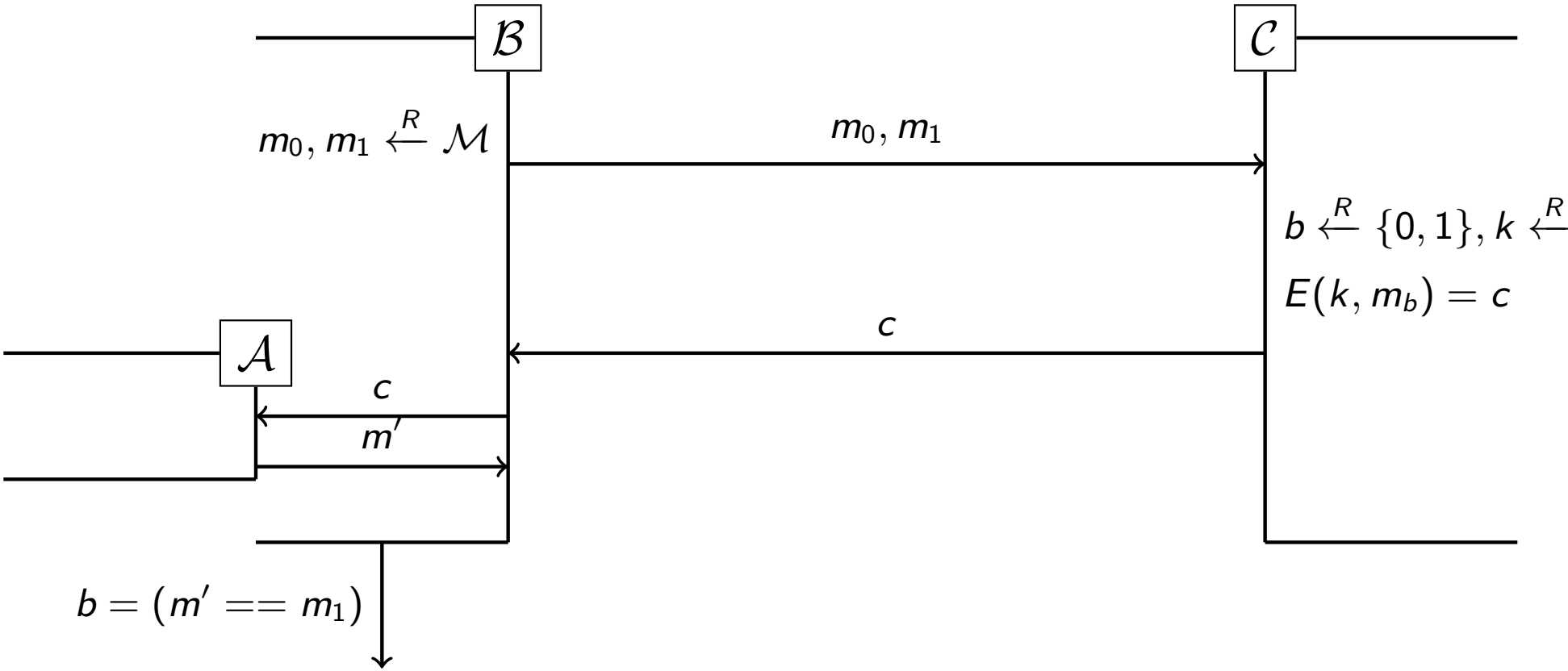
One Time Pad: Decryption

- Encrypt example
- Decrypt example
- Correctness walk through
- Is this a Shannon Cipher?
- Security eaknesses in this example?

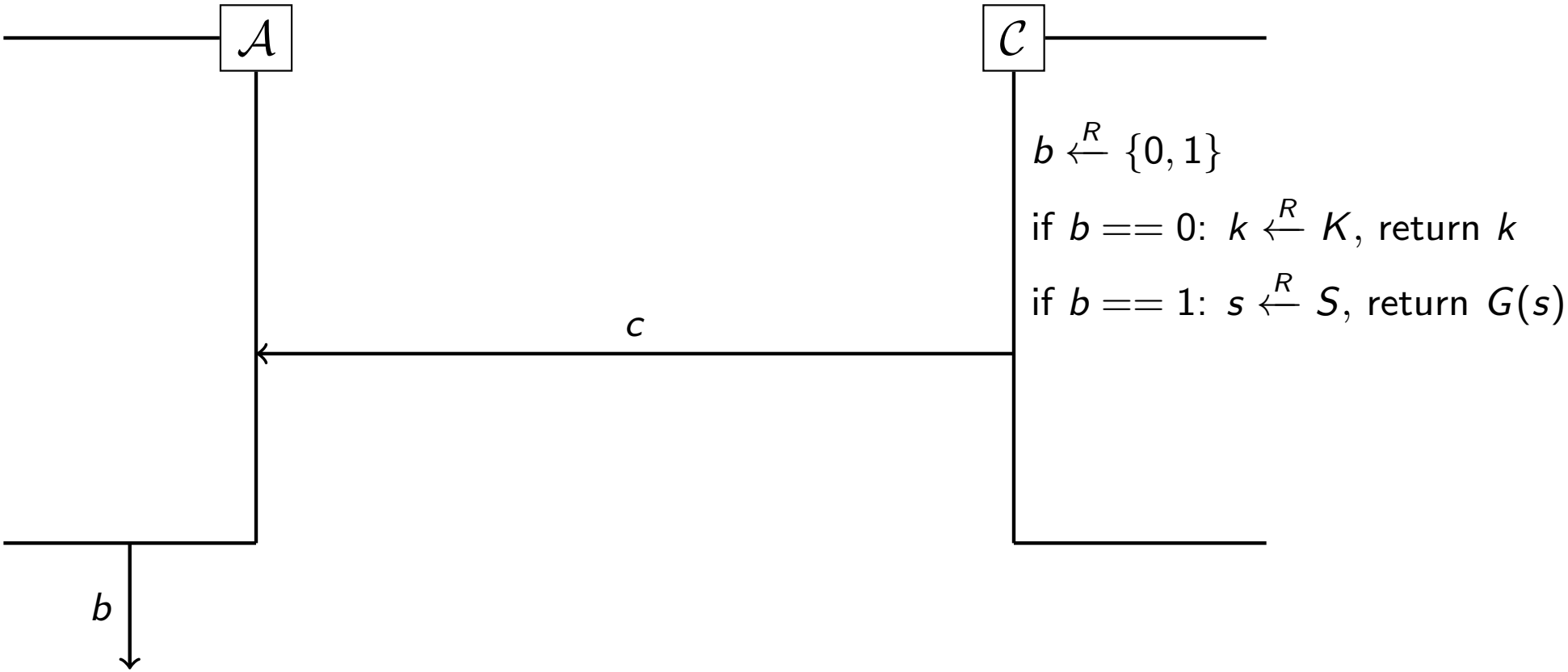
Semantic Security



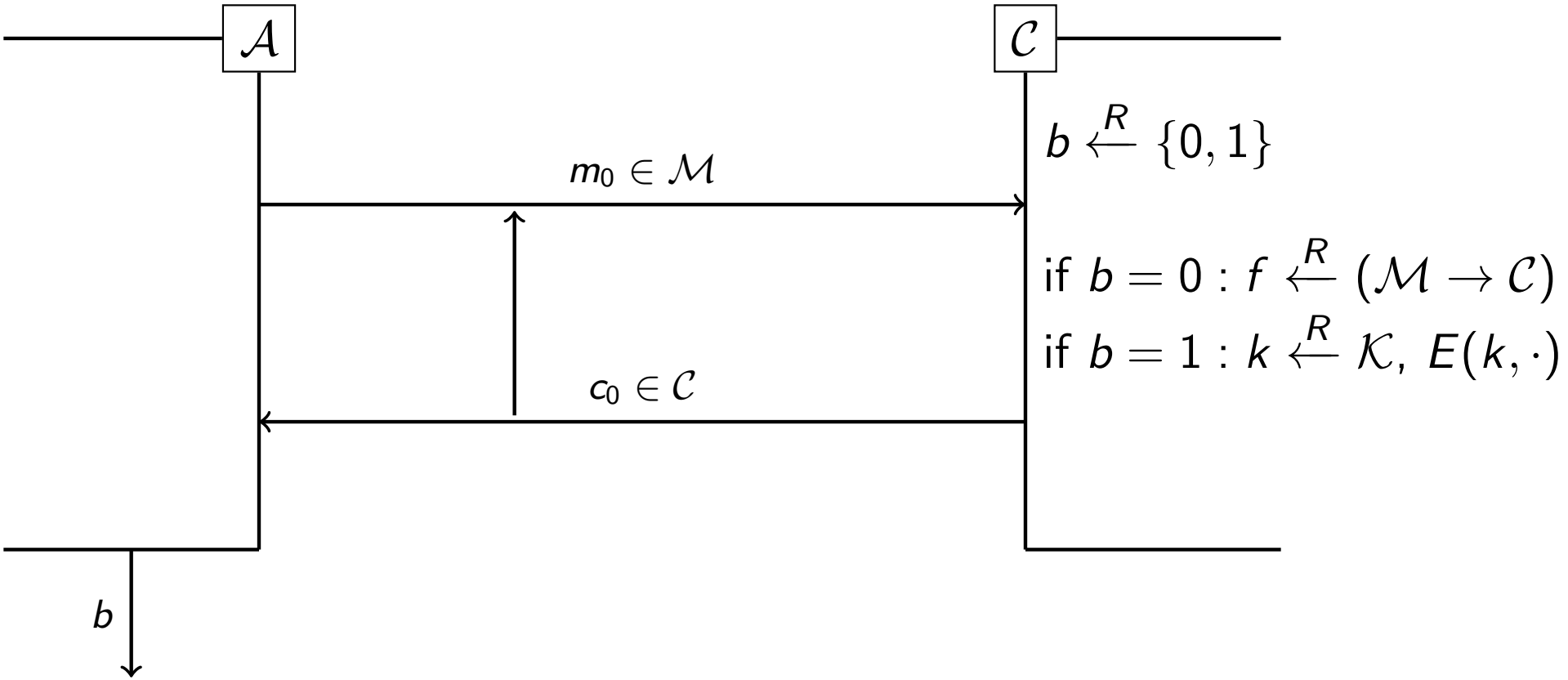
Semantic Security → Message Recovery Game



PRG Security Game

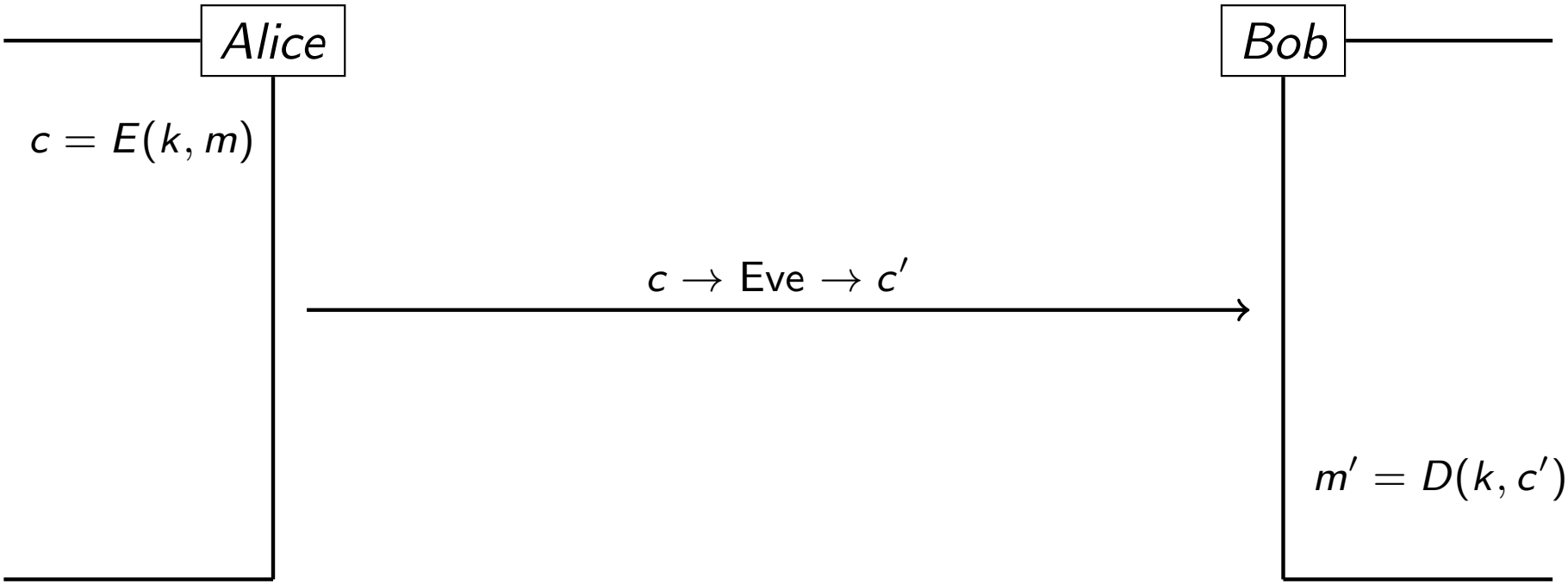


PRF Security Game: Chosen Plaintext Attack

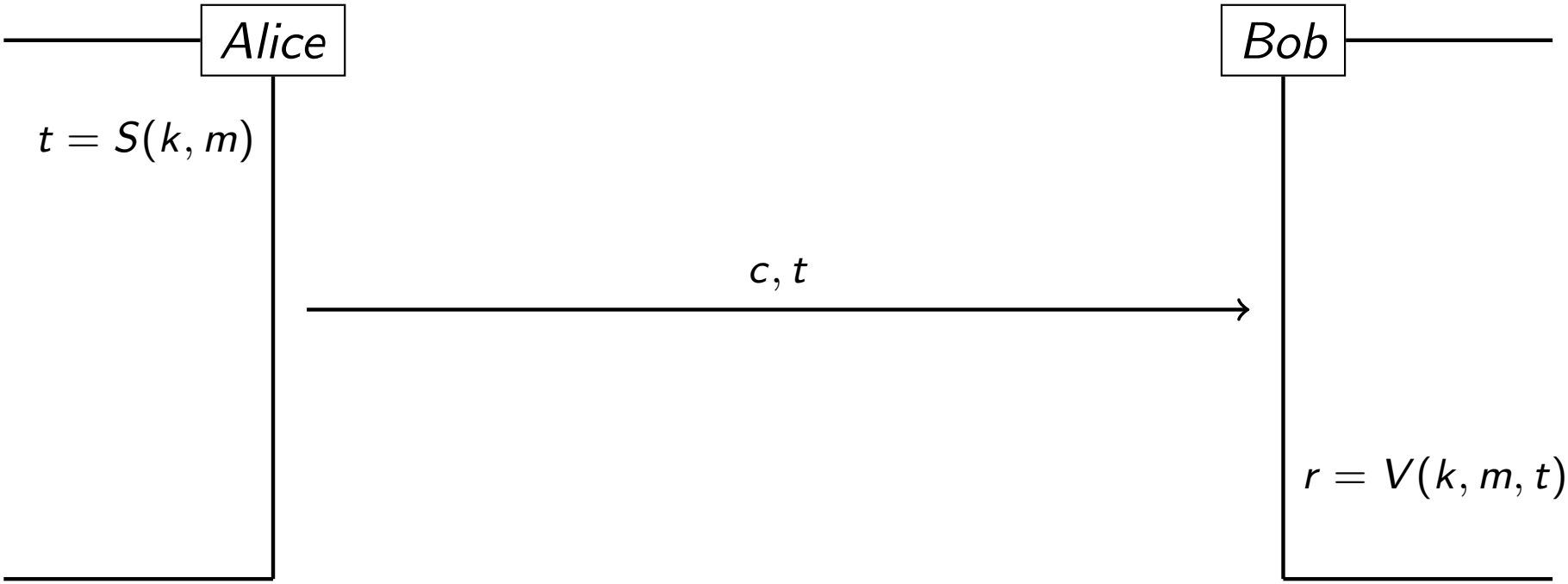


Man in the Middle Attack

Let $\mathcal{E} = (E, D)$ be a cipher secure against chosen plaintext attacks

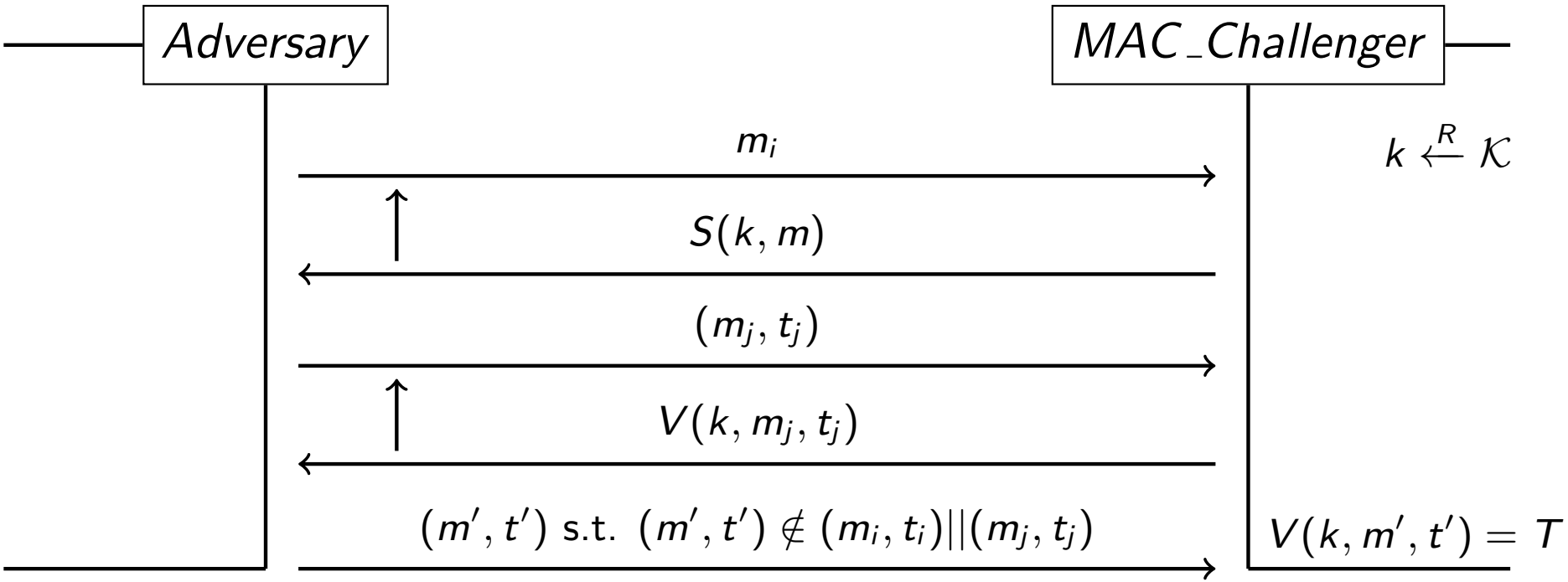


MAC Visualized



MAC Attack Game

$$V(k, m, t) = S(k, m) == t$$



Cipher Text Integrity Game