Security Notions for Bidirectional Channels

Giorgia Azzurra Marson   Bertram Poettering

FSE 2017
Tokyo, Japan

RUHR
UNIVERSITÄT
BOCHUM
RUB

hgi
Horst Görtz Institut
für IT-Sicherheit

Outline

Secure channels and how they are modeled

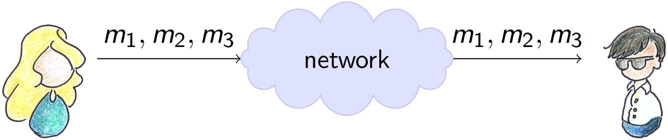
Security notions for bidirectional channels

Analysis of bidirectional channel design

Communication channels

- setting: two-party communication over the Internet
- goal: deliver messages and preserve sending order
- how to achieve this: TCP/IP

Good, if there are only Alice and Bob (idealized world)



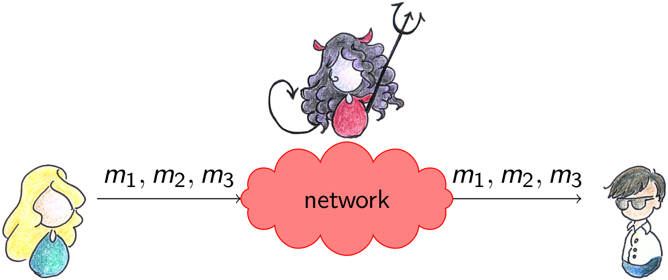
m_1, m_2, m_3

network

m_1, m_2, m_3

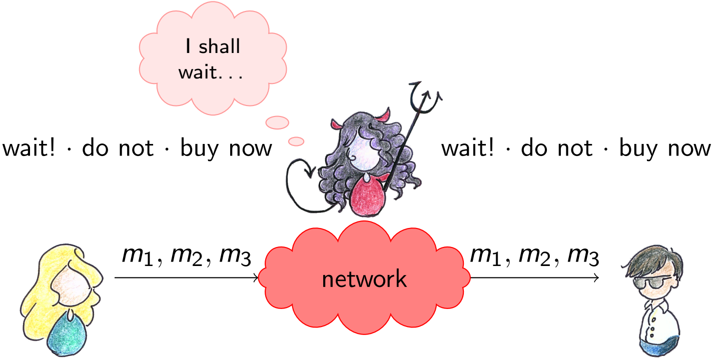
Cryptographic channels (a.k.a. secure channels)

- setting: two-party communication over the Internet
- goal: **protect** communication from adversaries



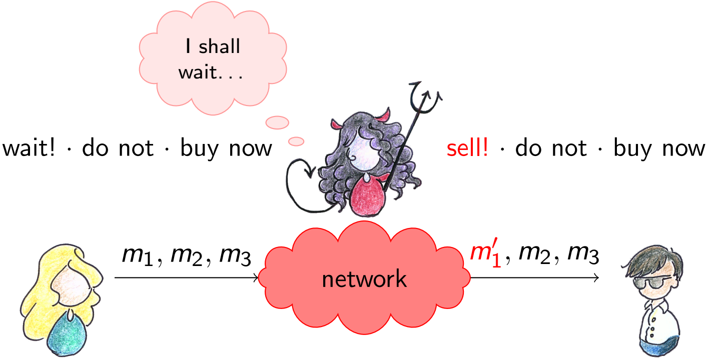
Cryptographic channels (a.k.a. secure channels)

- setting: two-party communication over the Internet
- goal: **protect** communication from adversaries
- security (informally): prevent eavesdropping



Cryptographic channels (a.k.a. secure channels)

- setting: two-party communication over the Internet
- goal: **protect** communication from adversaries
- security (informally): prevent eavesdropping and manipulation



I shall wait. . .

wait! · do not · buy now

sell! · do not · buy now

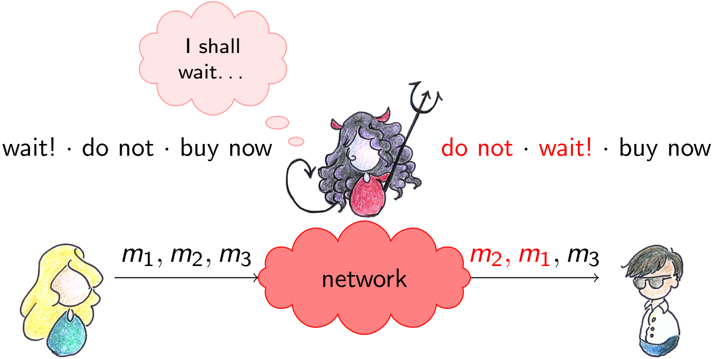
m_1, m_2, m_3

network

m'_1, m_2, m_3

Cryptographic channels (a.k.a. secure channels)

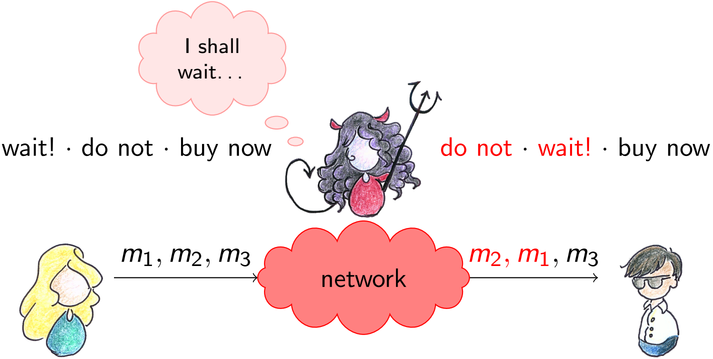
- setting: two-party communication over the Internet
- goal: **protect** communication from adversaries
- security (informally): prevent eavesdropping and manipulation



Cryptographic channels (a.k.a. secure channels)

- setting: two-party communication over the Internet
- goal: **protect** communication from adversaries
- security (informally): prevent eavesdropping and manipulation

make real world close to idealized world



I shall wait. . .

wait! · do not · buy now

do not · wait! · buy now

m_1, m_2, m_3

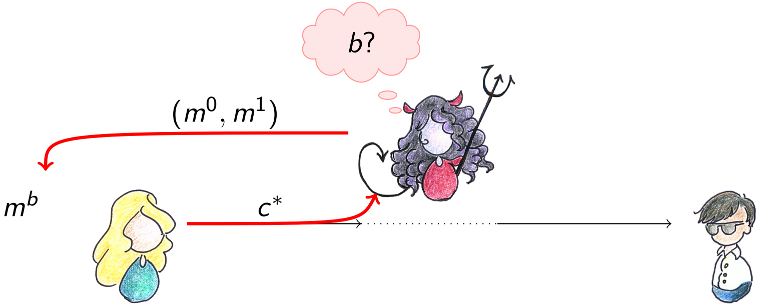
network

m_2, m_1, m_3

Modeling channel security [BKN'02]

Confidentiality

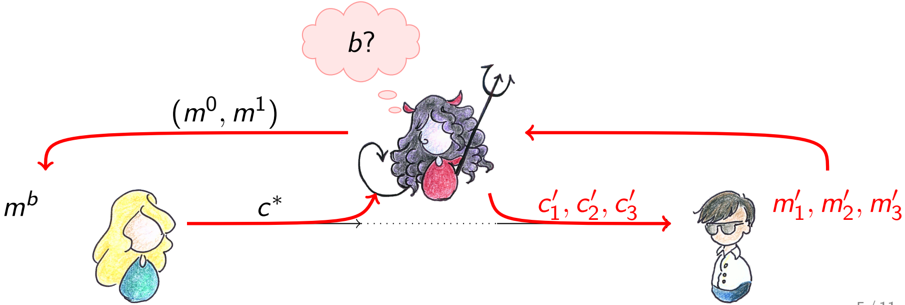
- intuitively: ciphertext hides plaintext
- formally: **IND-CPA** (a.k.a. 'passive')



Modeling channel security [BKN'02]

Confidentiality

- intuitively: ciphertext hides plaintext
- formally: **IND-CPA** (a.k.a. 'passive') and **IND-CCA** (a.k.a. 'active')



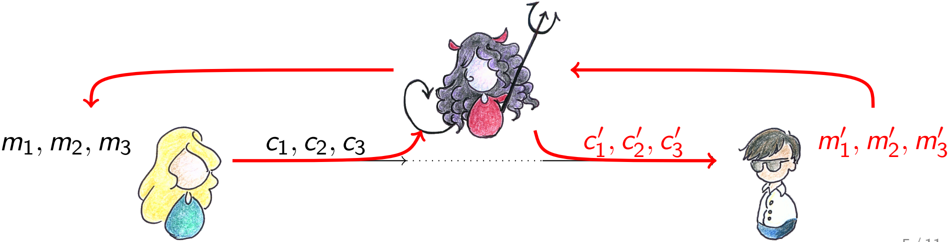
Modeling channel security [BKN'02]

Confidentiality

- intuitively: ciphertext hides plaintext
- formally: **IND-CPA** (a.k.a. 'passive') and **IND-CCA** (a.k.a. 'active')

Integrity

- intuitively: manipulations are detected
- formally: **INT-PTXT**



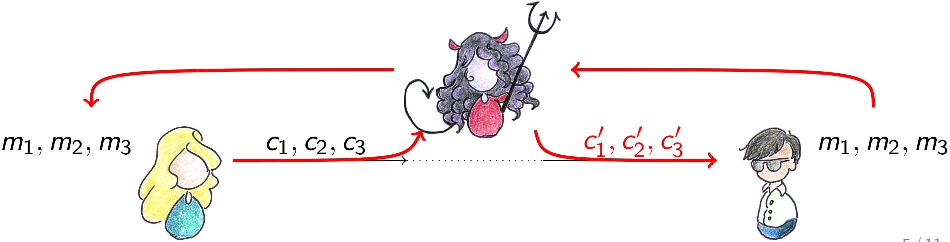
Modeling channel security [BKN'02]

Confidentiality

- intuitively: ciphertext hides plaintext
- formally: **IND-CPA** (a.k.a. 'passive') and **IND-CCA** (a.k.a. 'active')

Integrity

- intuitively: manipulations are detected
- formally: **INT-PTXT** and **INT-CTXT**



Modeling channel security [BKN'02]

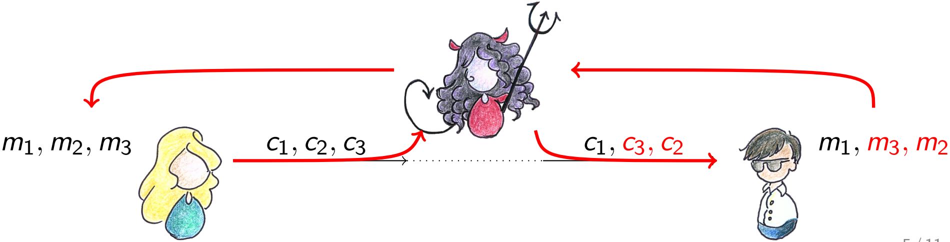
Confidentiality

- intuitively: ciphertext hides plaintext
- formally: **IND-CPA** (a.k.a. 'passive') and **IND-CCA** (a.k.a. 'active')

Integrity

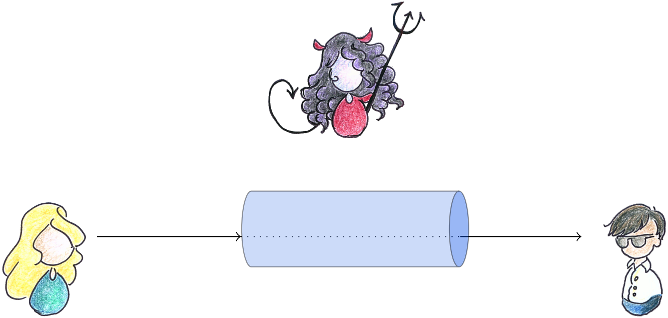
- intuitively: manipulations are detected
- formally: **INT-PTXT** and **INT-CTXT**

both incorporate replay and reordering protection



Cryptographic channels in theory: state of the art

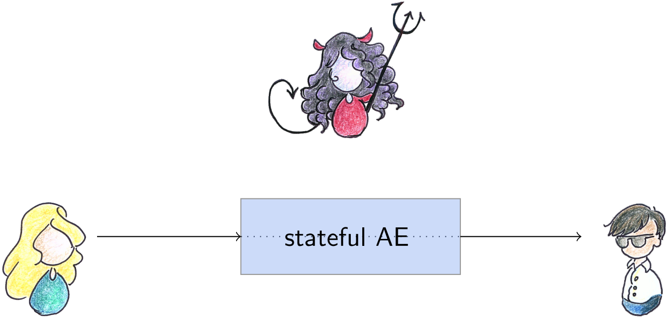
- channel security: IND-CPA + **INT-CTXT** ($\Longrightarrow$ **IND-CCA**)
- also called 'stateful authenticated encryption' (stateful AE)
- introduced to analyze (and prove) SSH channel security [BKN02]
- reference model to analyse TLS [JKSS12,KPW13,. . .]



Cryptographic channels in theory: state of the art

- channel security: IND-CPA + **INT-CTXT** ($\Longrightarrow$ **IND-CCA**)
- also called ‘stateful authenticated encryption’ (stateful AE)
- introduced to analyze (and prove) SSH channel security [BKN02]
- reference model to analyse TLS [JKSS12,KPW13,. . .]

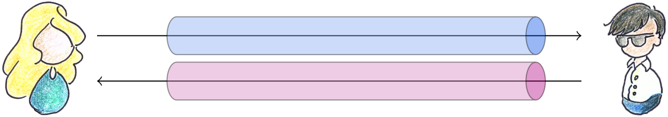
stateful AE considered good abstraction of a secure channel



Channels are used for bidirectional communication

- prior work: 'Sender → Receiver' communication
- practice: channels protect bidirectional communication
- standard approach employs two independent unidirectional channels

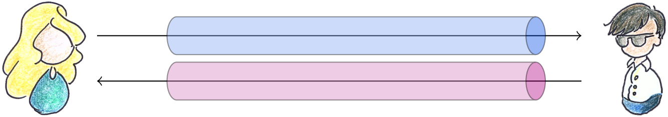
canonic composition of unidirectional channels



Channels are used for bidirectional communication

- prior work: ‘Sender → Receiver’ communication
- practice: channels protect bidirectional communication
- standard approach employs two independent unidirectional channels
- does this yield a secure bidirectional channel?
- folklore: unidirectional security ⟹ bidirectional security

canonic composition of unidirectional channels



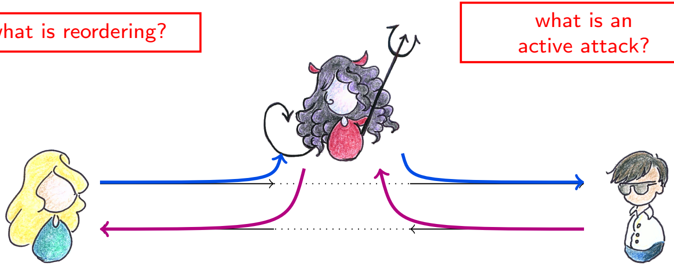
Channels are used for bidirectional communication

- prior work: ‘Sender → Receiver’ communication
- practice: channels protect bidirectional communication
- standard approach employs two independent unidirectional channels
- does this yield a secure bidirectional channel?
- folklore: unidirectional security $\Longrightarrow$ bidirectional security

what does it mean
‘bidirectional security’?

what is reordering?

what is an
active attack?



Our contribution in a nutshell

Defining bidirectional security

- confidentiality: IND-2-CPA, IND-2-CCA
- integrity: INT-2-PTXT, INT-2-CTXT
- notions reflect that → and ← are not independent of each other

Our contribution in a nutshell

Defining bidirectional security

- confidentiality: IND-2-CPA, IND-2-CCA
- integrity: INT-2-PTXT, INT-2-CTXT
- notions reflect that → and ← are not independent of each other

Relations among notions

- INT-2-CTXT $\Longrightarrow$ INT-2-PTXT
- IND-2-CCA $\Longrightarrow$ IND-2-CPA
- INT-2-CTXT + IND-2-CPA $\Longrightarrow$ IND-2-CCA

Our contribution in a nutshell

Defining bidirectional security

- confidentiality: IND-2-CPA, IND-2-CCA
- integrity: INT-2-PTXT, INT-2-CTXT
- notions reflect that → and ← are not independent of each other

Relations among notions

- INT-2-CTXT $\Longrightarrow$ INT-2-PTXT
- IND-2-CCA $\Longrightarrow$ IND-2-CPA
- INT-2-CTXT + IND-2-CPA $\Longrightarrow$ IND-2-CCA

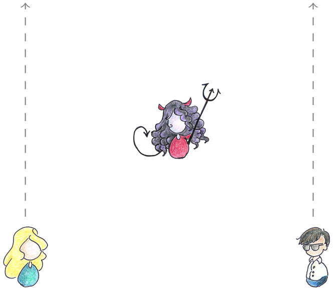
Analysis of the canonic composition

- question: can security be lifted from unidirectional components?
- our results question common belief…

Active attacks in a bidirectional setting

active ≈ deviation from honest behavior

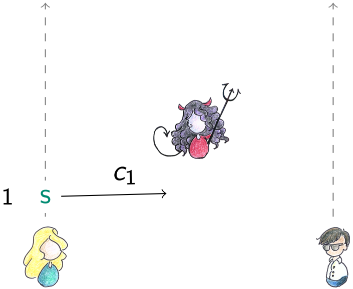
manipulation of ciphertexts or of their order (akin to unidirectional setting)



Active attacks in a bidirectional setting

active ≈ deviation from honest behavior

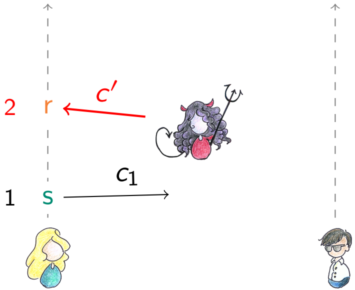
manipulation of ciphertexts or of their order (akin to unidirectional setting)



Active attacks in a bidirectional setting

active ≈ deviation from honest behavior

manipulation of ciphertexts or of their order (akin to unidirectional setting)



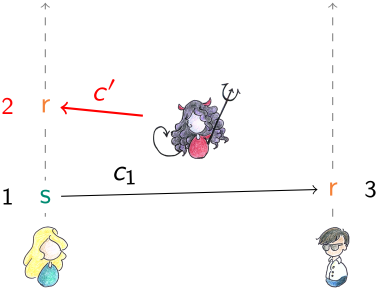
Active attacks in a bidirectional setting

active ≈ deviation from honest behavior

manipulation of ciphertexts or of their order (akin to unidirectional setting)

Our model additionally allows to express that:

- 'passive' query may chronologically follow 'active' query (concurrency)



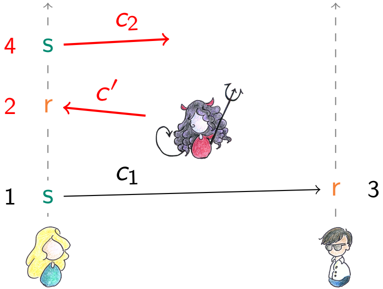
Active attacks in a bidirectional setting

active ≈ deviation from honest behavior

manipulation of ciphertexts or of their order (akin to unidirectional setting)

Our model additionally allows to express that:

- ‘passive’ query may chronologically follow ‘active’ query (concurrency)



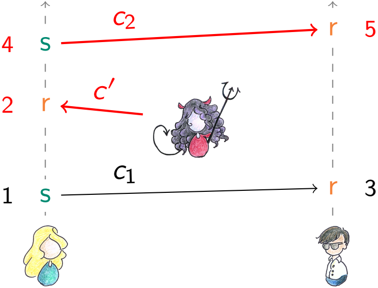
Active attacks in a bidirectional setting

active ≈ deviation from honest behavior

manipulation of ciphertexts or of their order (akin to unidirectional setting)

Our model additionally allows to express that:

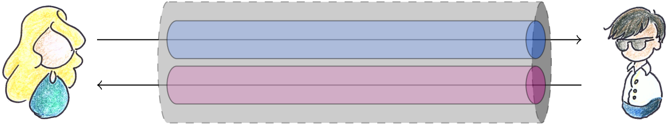
- 'passive' query may chronologically follow 'active' query (concurrency)
- active attack on ← may influence security of →



Bidirectional security of the canonic composition

Generic analysis: can security be lifted from unidirectional components?

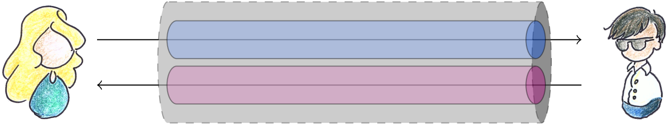
- INT-PTXT + INT-PTXT $\Longrightarrow$ INT-2-PTXT
- INT-CTXT + INT-CTXT $\Longrightarrow$ INT-2-CTXT
- IND-CPA + IND-CPA $\Longrightarrow$ INT-2-CPA



Bidirectional security of the canonic composition

Generic analysis: can security be lifted from unidirectional components?

- INT-PTXT + INT-PTXT $\Longrightarrow$ INT-2-PTXT
- INT-CTXT + INT-CTXT $\Longrightarrow$ INT-2-CTXT
- IND-CPA + IND-CPA $\Longrightarrow$ INT-2-CPA
- IND-CCA + IND-CCA $\not\Longrightarrow$ INT-2-CCA



Bidirectional security of the canonic composition

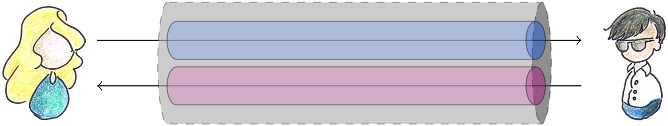
Generic analysis: can security be lifted from unidirectional components?

- INT-PTXT + INT-PTXT $\Longrightarrow$ INT-2-PTXT
- INT-CTXT + INT-CTXT $\Longrightarrow$ INT-2-CTXT
- IND-CPA + IND-CPA $\Longrightarrow$ INT-2-CPA

  $\}\Longrightarrow$ IND-2-CCA
- IND-CCA + IND-CCA $\not\Longrightarrow$ INT-2-CCA

Bidirectional security of TLS and SSH (the good news)

- TLS and SSH channel offer stateful AE security [K01,BKN02,PRS11]
  Encode-then-E&M for SSH, CBC-based M-then-E for TLS
- our result: they also offer **IND-2-CCA** and **INT-2-CTXT** security



Summary

This work

- formalize security notions for bidirectional channels
- analyze ‘canonic composition’
- confirm security of (crypto core of) TLS and SSH channels

Summary

This work

- formalize security notions for bidirectional channels
- analyze ‘canonic composition’
- confirm security of (crypto core of) TLS and SSH channels

Future work & open questions

- channel security in a multi-party setting (work in progress)
- bidirectional security of real TLS and SSH (beyond crypto core)

Summary

This work

- formalize security notions for bidirectional channels
- analyze ‘canonic composition’
- confirm security of (crypto core of) TLS and SSH channels

Future work & open questions

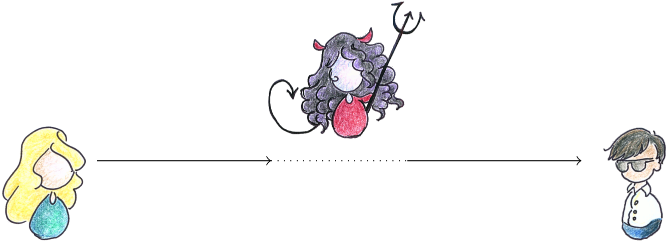
- channel security in a multi-party setting (work in progress)
- bidirectional security of real TLS and SSH (beyond crypto core)

Thank you!

Defining bidirectional confidentiality (IND-2-CCA)

```
**Send** $(u, m^0, m^1)$
    $c^* \leftarrow \mathrm{Send}(\mathrm{st}_u, m^b)$
    if $h_u = \mathrm{True}$
        $C_u[s_u] \leftarrow c^*$
        $s_u \leftarrow s_u + 1$
    Return $c^*$
```

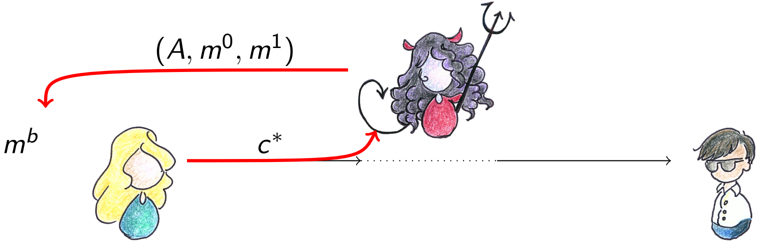
```
**Recv** $(u, c)$
    $m \leftarrow \mathrm{Recv}(\mathrm{st}_u, c)$
    if $r_u < s_v$ and $c = C_v[r_u]$
        $r_u \leftarrow r_u + 1$
    else
        $h_u \leftarrow \mathrm{False}$
    Return $h_u ? \diamond : m$
```



Defining bidirectional confidentiality (IND-2-CCA)

```
Send $(u, m^0, m^1)$
    $c^* \leftarrow \mathrm{Send}(\mathrm{st}_u, m^b)$
    if $h_u = \mathrm{True}$
        $C_u[s_u] \leftarrow c^*$
        $s_u \leftarrow s_u + 1$
    Return $c^*$
```

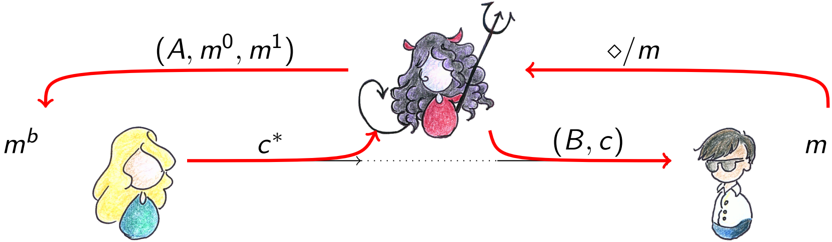
```
Recv $(u, c)$
    $m \leftarrow \mathrm{Recv}(\mathrm{st}_u, c)$
    if $r_u < s_v$ and $c = C_v[r_u]$
        $r_u \leftarrow r_u + 1$
    else
        $h_u \leftarrow \mathrm{False}$
    Return $h_u ? \diamond : m$
```



Defining bidirectional confidentiality (IND-2-CCA)

```
Send $(u, m^0, m^1)$
    $c^* \leftarrow \mathrm{Send}(\mathrm{st}_u, m^b)$
    if $h_u = \mathrm{True}$
        $C_u[s_u] \leftarrow c^*$
        $s_u \leftarrow s_u + 1$
    Return $c^*$
```

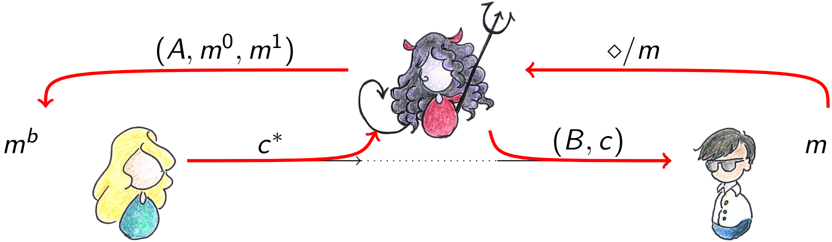
```
Recv $(u, c)$
    $m \leftarrow \mathrm{Recv}(\mathrm{st}_u, c)$
    if $r_u < s_v$ and $c = C_v[r_u]$
        $r_u \leftarrow r_u + 1$
    else
        $h_u \leftarrow \mathrm{False}$
    Return $h_u ? \diamond : m$
```



Defining bidirectional confidentiality (IND-2-CCA)

```
**Send** $(u, m^0, m^1)$
    $c^* \leftarrow \text{Send}(\text{st}_u, m^b)$
    if $h_u = \text{True}$
        $C_u[s_u] \leftarrow c^*$
        $s_u \leftarrow s_u + 1$
    Return $c^*$
```

```
**Recv** $(u, c)$
    $m \leftarrow \text{Recv}(\text{st}_u, c)$
    if $r_u < s_v$ and $c = C_v[r_u]$
        $r_u \leftarrow r_u + 1$
    else
        $h_u \leftarrow \text{False}$
    Return $h_u ? \diamond : m$
```



(A, m^0, m^1)

$\diamond / m$

m^b

c^*

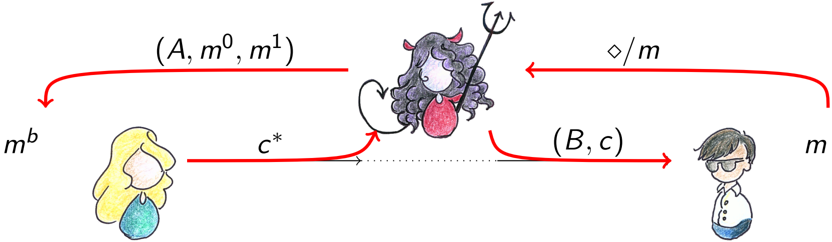
(B, c)

m

Defining bidirectional confidentiality (IND-2-CCA)

```
**Send** $(u, m^0, m^1)$
    $c^* \leftarrow \text{Send}(\text{st}_u, m^b)$
    if $h_u = \text{True}$
        $C_u[s_u] \leftarrow c^*$
        $s_u \leftarrow s_u + 1$
    Return $c^*$
```

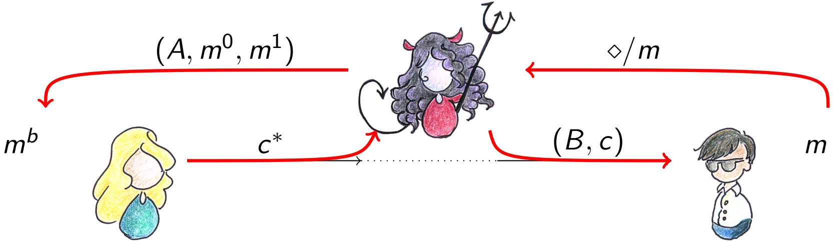
```
**Recv** $(u, c)$
    $m \leftarrow \text{Recv}(\text{st}_u, c)$
    if $r_u < s_v$ and $c = C_v[r_u]$
        $r_u \leftarrow r_u + 1$
    else
        $h_u \leftarrow \text{False}$
    Return $h_u ? \diamond : m$
```



Defining bidirectional confidentiality (IND-2-CCA)

```
**Send** $(u, m^0, m^1)$
    $c^* \leftarrow \text{Send}(\text{st}_u, m^b)$
    if $h_u = \text{True}$
        $C_u[s_u] \leftarrow c^*$
        $s_u \leftarrow s_u + 1$
    Return $c^*$
```

```
**Recv** $(u, c)$
    $m \leftarrow \text{Recv}(\text{st}_u, c)$
    if $r_u < s_v$ and $c = C_v[r_u]$
        $r_u \leftarrow r_u + 1$
    else
        $h_u \leftarrow \text{False}$
    Return $h_u ? \diamond : m$
```


(A, m^0, m^1)
$\diamond / m$
m^b
c^*
(B, c)
m