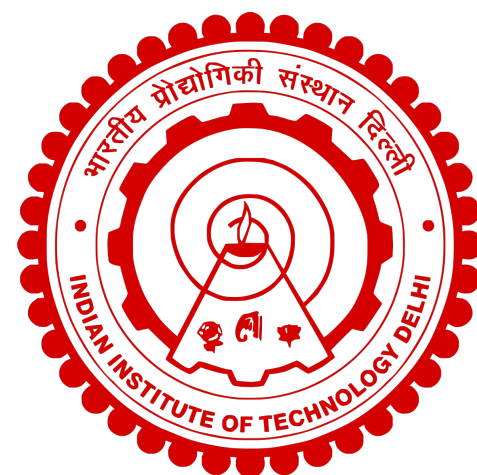


Non-Committing Identity Based Encryption: Constructions and Applications

Maresh Sreekumar Rajasree

CISPA Helmholtz

PKC 2025



Joint work with Rishab Goyal (UW-Madison), Fuyuki Kitagawa (NTT Japan), Venkata Koppula (IITD), Ryo Nishimaki (NTT Japan) and Takashi Yamakawa (NTT Japan)

Standard Security : Definition

[Goldwasser-Micali'84]

Standard Security : Definition



[Goldwasser-Micali'84]

Standard Security : Definition



Challenger



[Goldwasser-Micali'84]

Adversary

Standard Security : Definition



Challenger

$(sk, pk) \leftarrow Setup()$



[Goldwasser-Micali'84]

Adversary

Standard Security : Definition



Challenger

$(sk, pk) \leftarrow Setup()$



Adversary

[Goldwasser-Micali'84]

pk



Standard Security : Definition



Challenger

$(sk, pk) \leftarrow Setup()$



Adversary

[Goldwasser-Micali'84]

pk

m_0, m_1

Standard Security : Definition



Challenger

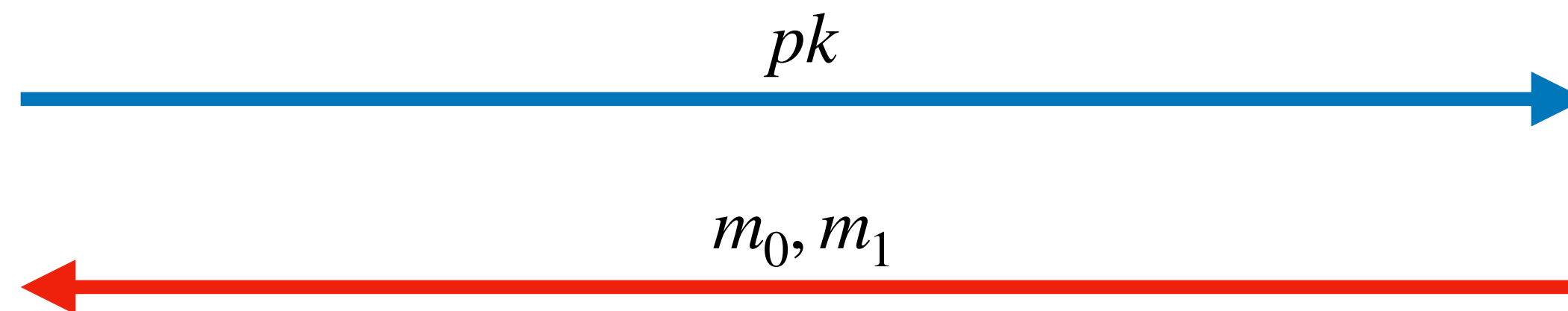
$(sk, pk) \leftarrow Setup()$

$b \leftarrow \{0,1\}$



Adversary

[Goldwasser-Micali'84]



Standard Security : Definition



Challenger

$(sk, pk) \leftarrow Setup()$



Adversary

[Goldwasser-Micali'84]

pk

m_0, m_1

$b \leftarrow \{0,1\}$

$c \leftarrow Enc(pk, m_b)$

Standard Security : Definition



Challenger

$(sk, pk) \leftarrow Setup()$



Adversary

[Goldwasser-Micali'84]

pk

m_0, m_1

$b \leftarrow \{0,1\}$

$c \leftarrow Enc(pk, m_b)$

c

Standard Security : Definition



Challenger

$(sk, pk) \leftarrow Setup()$



Adversary

[Goldwasser-Micali'84]

pk

m_0, m_1

$b \leftarrow \{0,1\}$

$c \leftarrow Enc(pk, m_b)$

c

$b' \in \{0,1\}$

Standard Security : Definition



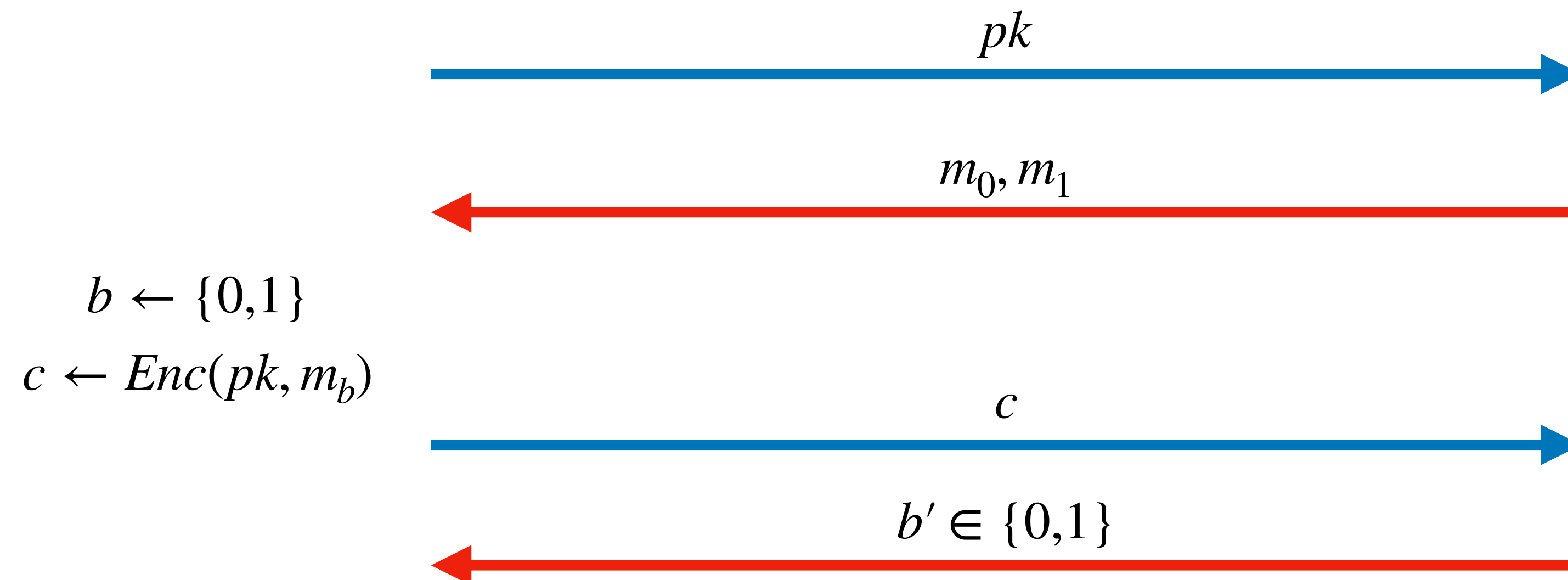
Challenger

$(sk, pk) \leftarrow Setup()$



Adversary

[Goldwasser-Micali'84]



Adversary wins if $b = b'$

Incompressible Cryptography

[Dziembowski'06, Guan-Wichs-Zhandry'22]

Incompressible Cryptography

[Dziembowski'06,Guan-Wichs-Zhandry'22]

- Security is lost if adversary has **entire ciphertext** and **entire secret key** due to **correctness**.

Incompressible Cryptography

[Dziembowski'06,Guan-Wichs-Zhandry'22]

- Security is lost if adversary has **entire ciphertext** and **entire secret key** due to **correctness**.
- Dziembowski'06 and Guan-Wichs-Zhandry'22 proposed incompressible security model

Incompressible Cryptography

[Dziembowski'06,Guan-Wichs-Zhandry'22]

- Security is lost if adversary has **entire ciphertext** and **entire secret key** due to **correctness**.
- Dziembowski'06 and Guan-Wichs-Zhandry'22 proposed incompressible security model
 - Make ciphertext large so that long-term storage is expensive.

Incompressible Cryptography

[Dziembowski'06,Guan-Wichs-Zhandry'22]

- Security is lost if adversary has **entire ciphertext** and **entire secret key** due to **correctness**.
- Dziembowski'06 and Guan-Wichs-Zhandry'22 proposed incompressible security model
 - Make ciphertext large so that long-term storage is expensive.
 - Adversary gets a challenge ciphertext ct^* for m_0, m_1 and then it has to compress/reduce its storage which contains ct^* .

Incompressible Cryptography

[Dziembowski'06, Guan-Wichs-Zhandry'22]

- Security is lost if adversary has **entire ciphertext** and **entire secret key** due to **correctness**.
- Dziembowski'06 and Guan-Wichs-Zhandry'22 proposed incompressible security model
 - Make ciphertext large so that long-term storage is expensive.
 - Adversary gets a challenge ciphertext ct^* for m_0, m_1 and then it has to compress/reduce its storage which contains ct^* .
 - After which it receives sk , but still should not be able to distinguish.

Incompressible PKE Security

[Guan-Wichs-Zhandry'22]

Incompressible PKE Security

[Guan-Wichs-Zhandry'22]



Incompressible PKE Security

[Guan-Wichs-Zhandry'22]



Challenger



Adversary 1

Incompressible PKE Security

[Guan-Wichs-Zhandry'22]



Challenger

$(pk, sk) \leftarrow \text{Setup}()$



Adversary 1

Incompressible PKE Security

[Guan-Wichs-Zhandry'22]



Challenger



Adversary 1

$(pk, sk) \leftarrow Setup()$

mpk



Incompressible PKE Security

[Guan-Wichs-Zhandry'22]



Challenger



Adversary 1

$(pk, sk) \leftarrow Setup()$

mpk

m_0, m_1

Incompressible PKE Security

[Guan-Wichs-Zhandry'22]



Challenger



Adversary 1

$(pk, sk) \leftarrow Setup()$

mpk

m_0, m_1

$b \leftarrow \{0,1\}$

$c \leftarrow Enc(pk, m_b)$

Incompressible PKE Security

[Guan-Wichs-Zhandry'22]



Challenger



Adversary 1

$(pk, sk) \leftarrow Setup()$

mpk

m_0, m_1

$b \leftarrow \{0,1\}$

$c \leftarrow Enc(pk, m_b)$

c

Incompressible PKE Security

[Guan-Wichs-Zhandry'22]



Challenger



Adversary 1

$(pk, sk) \leftarrow Setup()$

mpk

m_0, m_1

$b \leftarrow \{0,1\}$

c

$c \leftarrow Enc(pk, m_b)$

$state$

Incompressible PKE Security

[Guan-Wichs-Zhandry'22]



Challenger



Adversary 1

$(pk, sk) \leftarrow Setup()$

mpk

m_0, m_1

$b \leftarrow \{0,1\}$

$c \leftarrow Enc(pk, m_b)$

c

$state$

$|state| \leq S$

Incompressible PKE Security

[Guan-Wichs-Zhandry'22]



Challenger



Adversary 1

$(pk, sk) \leftarrow Setup()$

mpk

m_0, m_1

$b \leftarrow \{0,1\}$

$c \leftarrow Enc(pk, m_b)$

c

$state$

$|state| \leq S$



Adversary 2

Incompressible PKE Security

[Guan-Wichs-Zhandry'22]



Challenger



Adversary 1

$(pk, sk) \leftarrow Setup()$

mpk

m_0, m_1

$b \leftarrow \{0,1\}$

$c \leftarrow Enc(pk, m_b)$

c

$state$

$|state| \leq S$

$pk, sk, state$

Adversary 2



Incompressible PKE Security

[Guan-Wichs-Zhandry'22]



Challenger



Adversary 1

$(pk, sk) \leftarrow Setup()$

mpk

m_0, m_1

$b \leftarrow \{0,1\}$

$c \leftarrow Enc(pk, m_b)$

c

$state$

$|state| \leq S$

$pk, sk, state$

$b' \in \{0,1\}$

Adversary 2



Incompressible PKE Security

[Guan-Wichs-Zhandry'22]



Challenger



Adversary 1

$(pk, sk) \leftarrow Setup()$

mpk

m_0, m_1

$b \leftarrow \{0,1\}$

$c \leftarrow Enc(pk, m_b)$

c

$state$

$|state| \leq S$



Adversary 2

$pk, sk, state$

$b' \in \{0,1\}$

Adversaries win if $b = b'$

Prior works

Prior works

Dziembowski'06

Introduced and constructed the first Incompressible SKE.

Prior works

Dziembowski'06

Introduced and constructed the first Incompressible SKE.

Guan-Wichs-Zhandry'22

Extended the notion to Incompressible PKE and provided constructions from regulars PKE (poor rate) and iO (rate-1).

Prior works

Dziembowski'06

Introduced and constructed the first Incompressible SKE.

Guan-Wichs-Zhandry'22

Extended the notion to Incompressible PKE and provided constructions from regulars PKE (poor rate) and iO (rate-1).

Branco-Döttling-Dujmovic'23

Constructed CCA-Incompressible PKE (rate-1) from standard assumptions.

Prior works

Dziembowski'06

Introduced and constructed the first Incompressible SKE.

Guan-Wichs-Zhandry'22

Extended the notion to Incompressible PKE and provided constructions from regulars PKE (poor rate) and iO (rate-1).

Branco-Döttling-Dujmovic'23

Constructed CCA-Incompressible PKE (rate-1) from standard assumptions.

Guan-Wichs-Zhandry'23

Extended the notion to Multi-user Incompressible PKE setting.

Prior works

Dziembowski'06

Introduced and constructed the first Incompressible SKE.

Guan-Wichs-Zhandry'22

Extended the notion to Incompressible PKE and provided constructions from regulars PKE (poor rate) and iO (rate-1).

Branco-Döttling-Dujmovic'23

Constructed CCA-Incompressible PKE (rate-1) from standard assumptions.

Guan-Wichs-Zhandry'23

Extended the notion to Multi-user Incompressible PKE setting.

**Bhushan-Goyal-Koppula-
Narayanan-Prabhakaran-
Rajasree'24**

Extended the notion to leakage-resilience.

Prior works

Dziembowski'06

Introduced and constructed the first Incompressible SKE.

Guan-Wichs-Zhandry'22

Extended the notion to Incompressible PKE and provided constructions from regulars PKE (poor rate) and iO (rate-1).

Branco-Döttling-Dujmovic'23

Constructed CCA-Incompressible PKE (rate-1) from standard assumptions.

Guan-Wichs-Zhandry'23

Extended the notion to Multi-user Incompressible PKE setting.

Bhushan-Goyal-Koppula-
Narayanan-Prabhakaran-
Rajasree'24

Extended the notion to leakage-resilience.

Goyal-Koppula-**Rajasree**-
Verma'25

Extended the notion to FE, ABE and **IBE**

Incompressible PKE from NCE

Incompressible PKE from NCE

Non-Committing Encryption

Incompressible PKE from NCE

Non-Committing Encryption

+

Incompressible PKE from NCE

Non-Committing Encryption

+

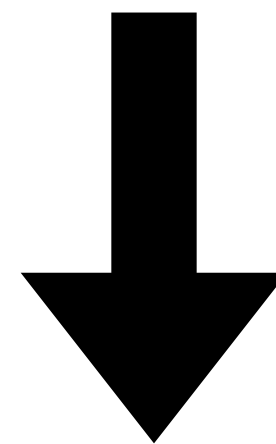
Incompressible SKE

Incompressible PKE from NCE

Non-Committing Encryption

+

Incompressible SKE

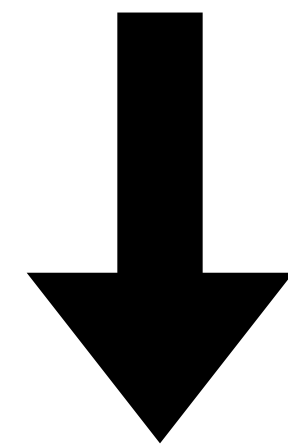


Incompressible PKE from NCE

Non-Committing Encryption

+

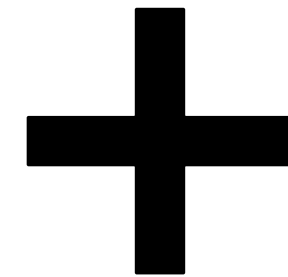
Incompressible SKE



Incompressible PKE

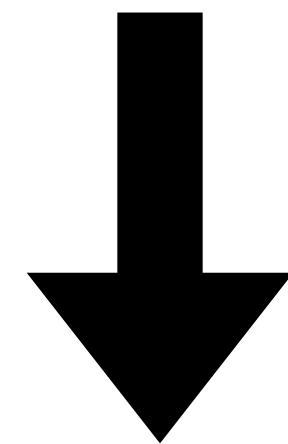
Incompressible PKE from NCE

Non-Committing Encryption



Incompressible SKE

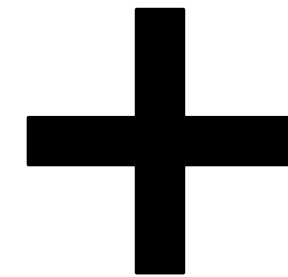
Can be build from OWF



Incompressible PKE

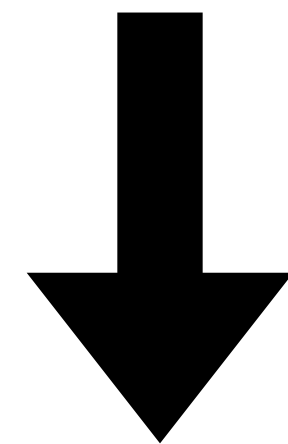
Incompressible PKE from NCE

Non-Committing Encryption



Incompressible SKE

Can be build from OWF



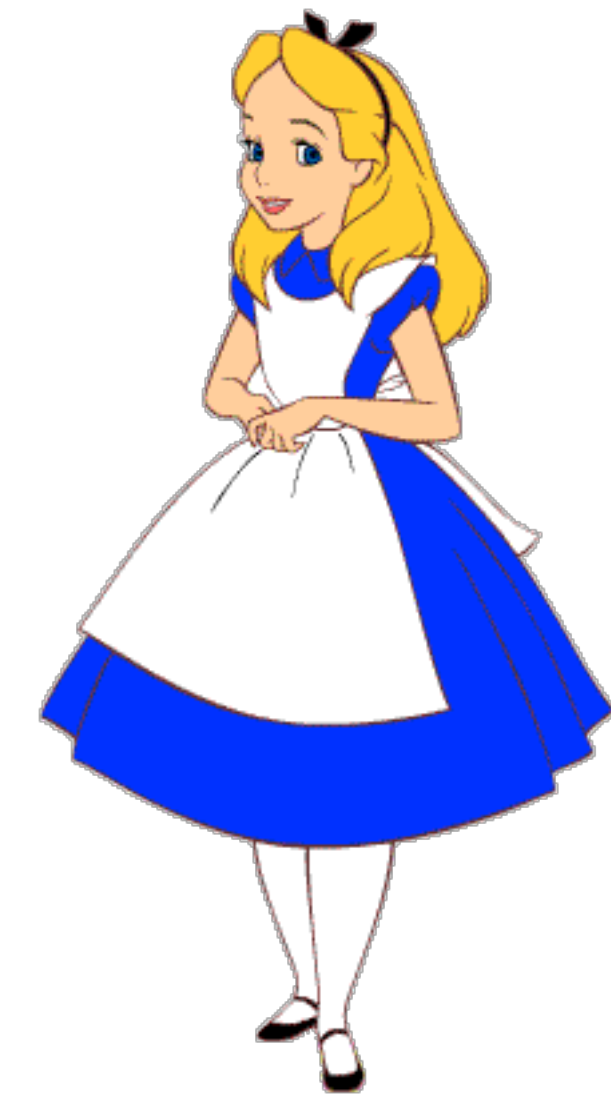
Incompressible PKE

Non-Committing Encryption (NCE)

[CFGN'96]

Non-Committing Encryption (NCE)

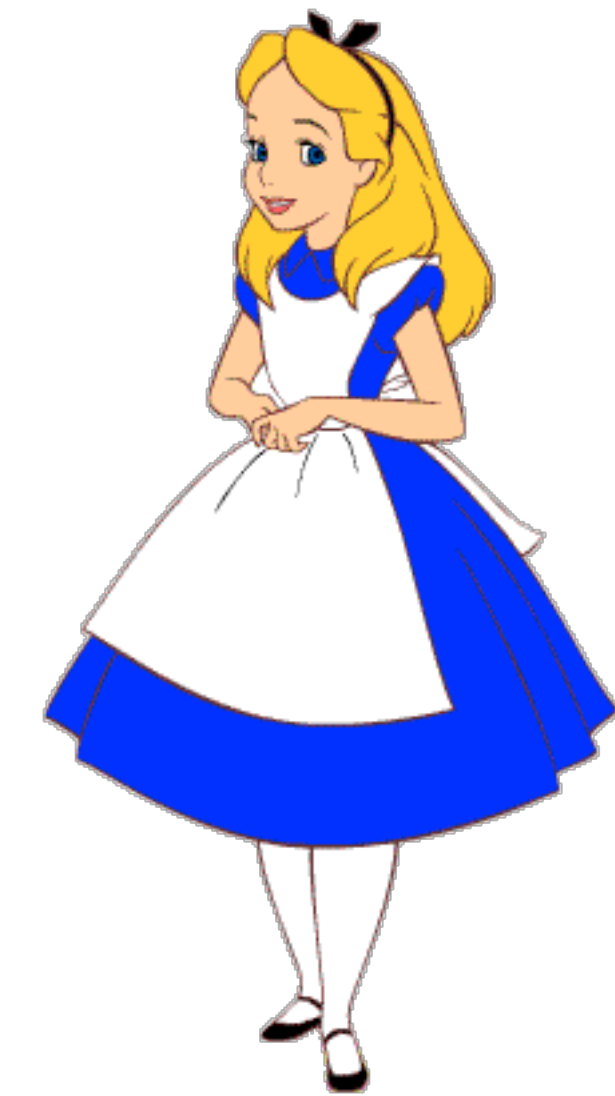
[CFGN'96]



Non-Committing Encryption (NCE)

[CFGN'96]

pk

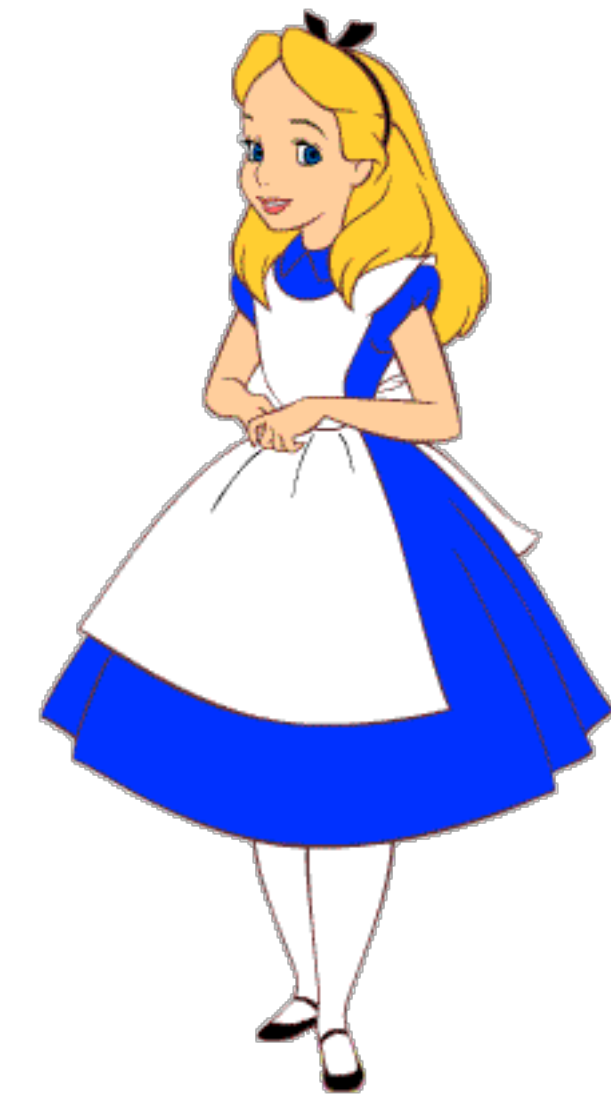


Non-Committing Encryption (NCE)

[CFGN'96]

pk

sk



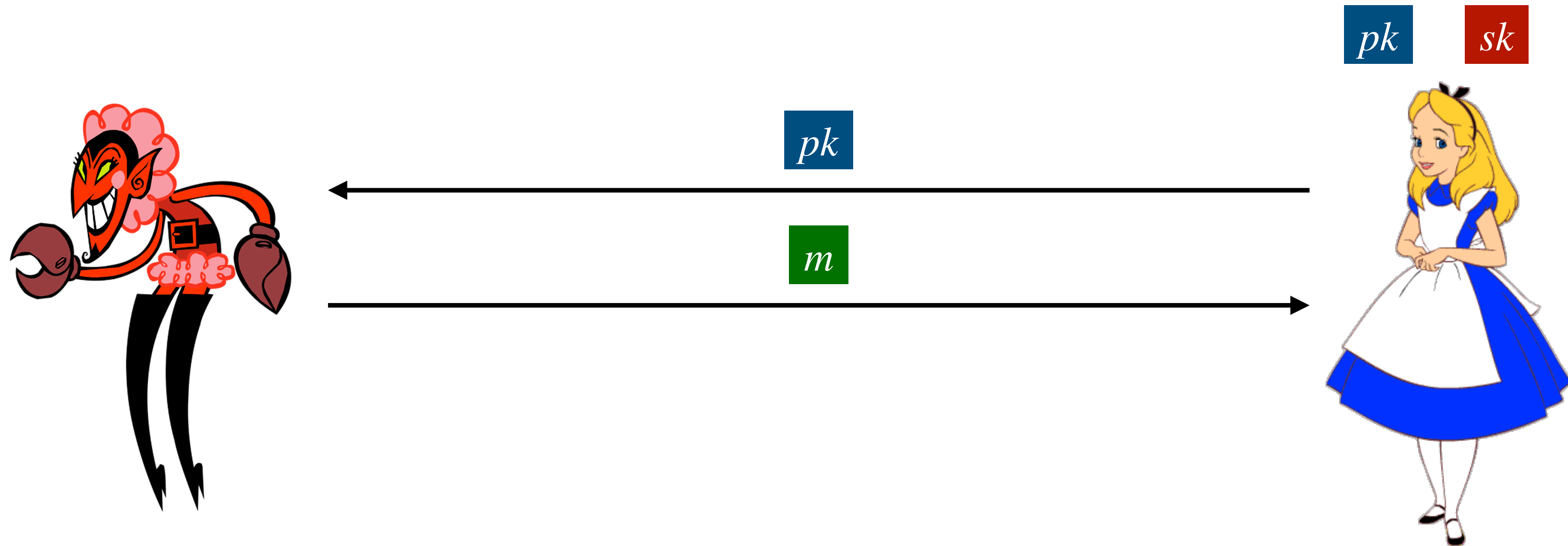
Non-Committing Encryption (NCE)

[CFGN'96]



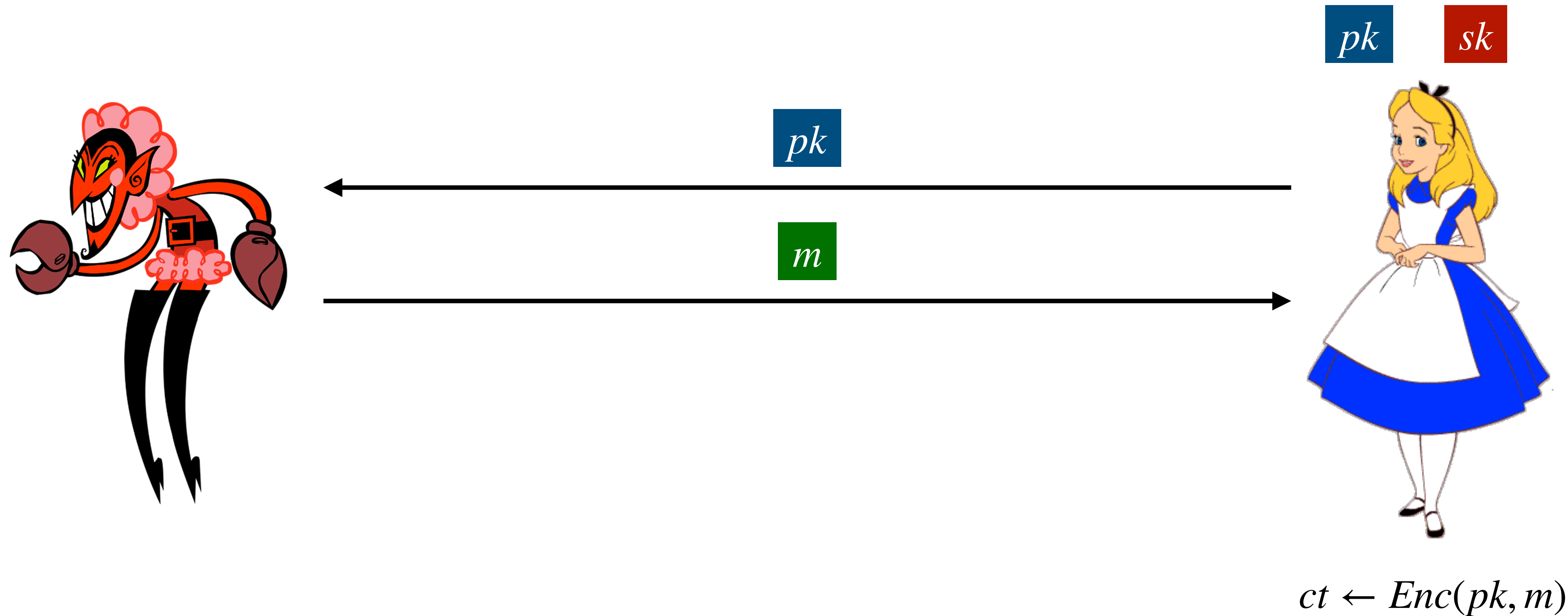
Non-Committing Encryption (NCE)

[CFGN'96]



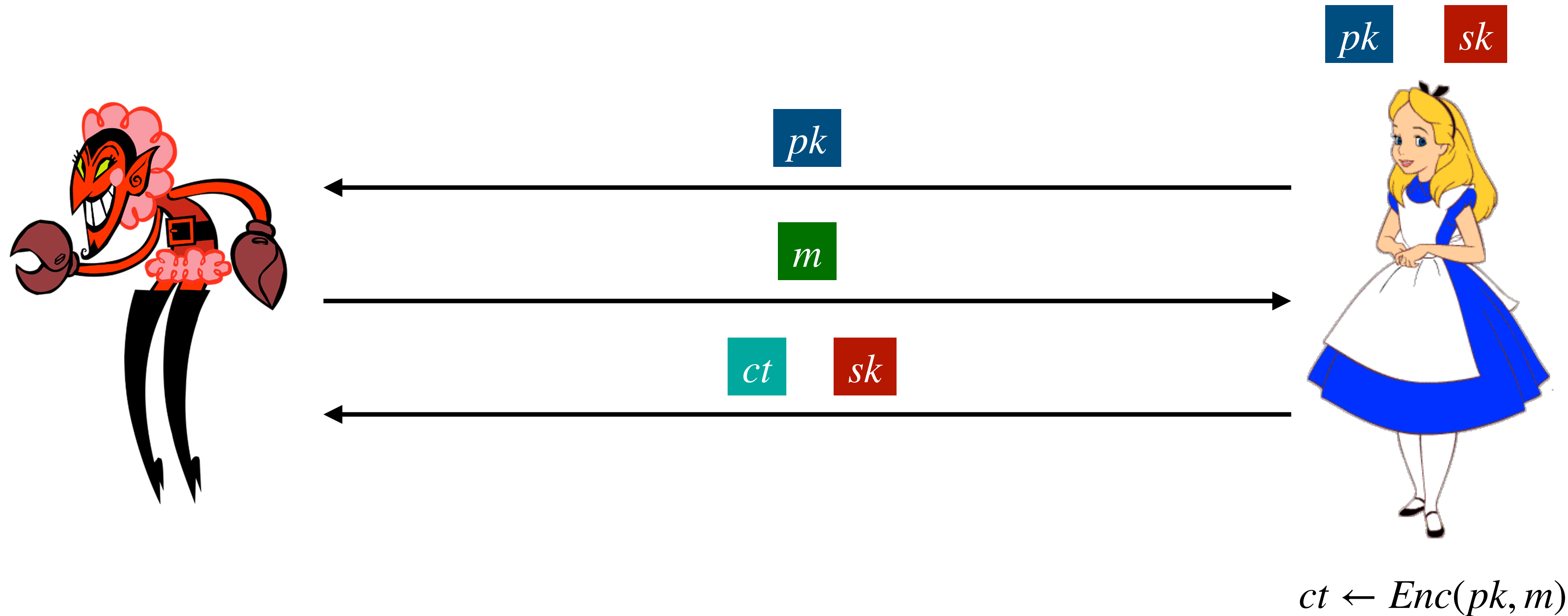
Non-Committing Encryption (NCE)

[CFGN'96]



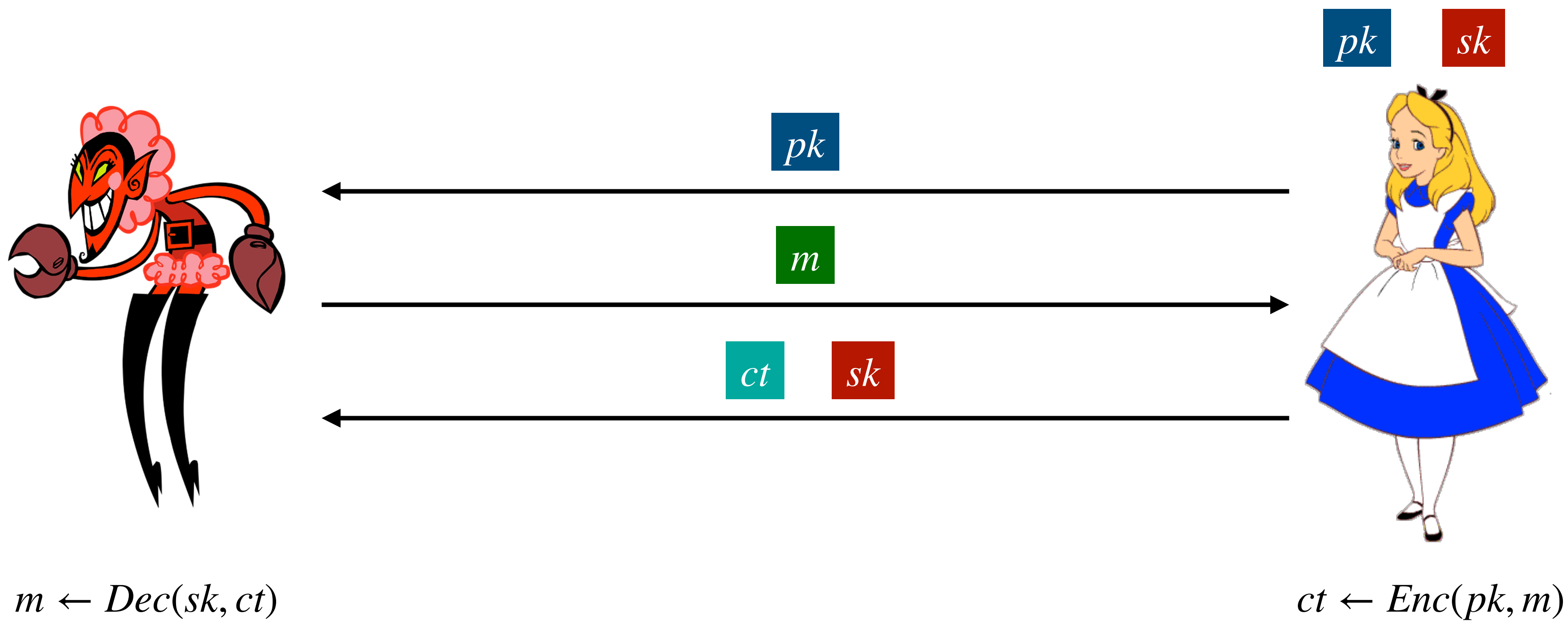
Non-Committing Encryption (NCE)

[CFGN'96]



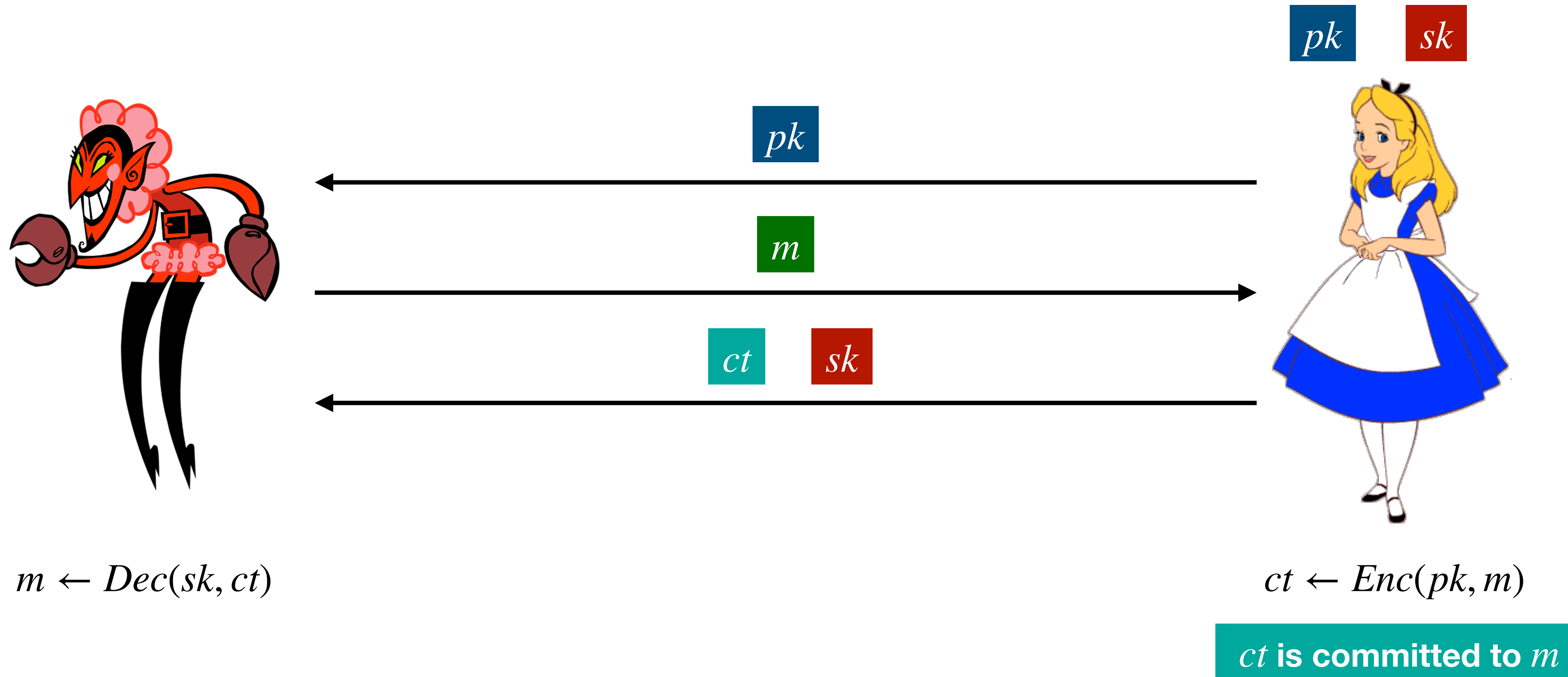
Non-Committing Encryption (NCE)

[CFGN'96]



Non-Committing Encryption (NCE)

[CFGN'96]

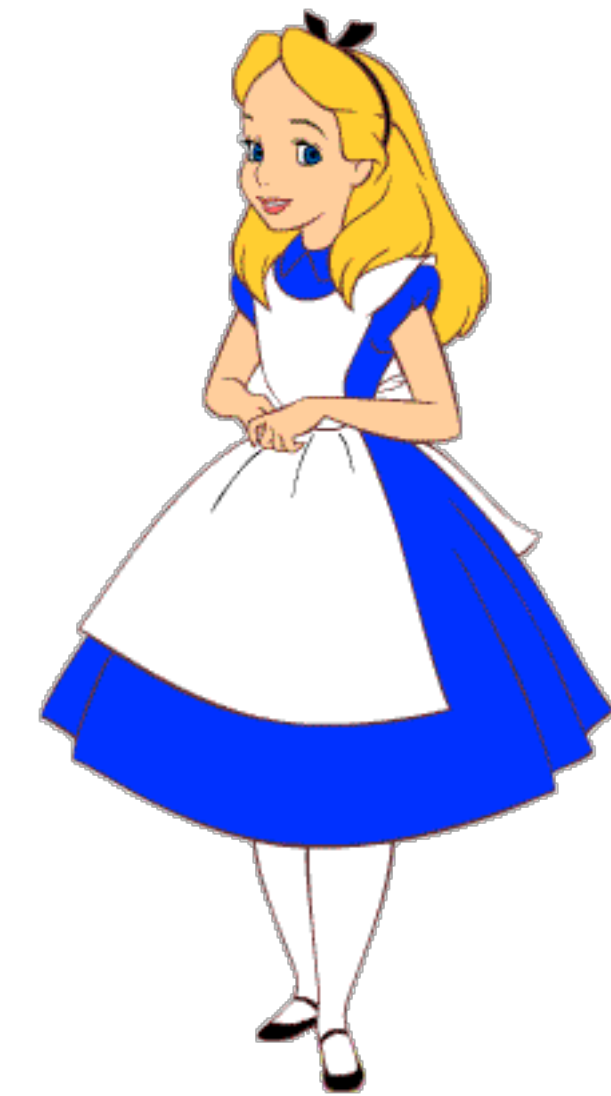


Non-Committing Encryption (NCE)

[CFGN'96]

Non-Committing Encryption (NCE)

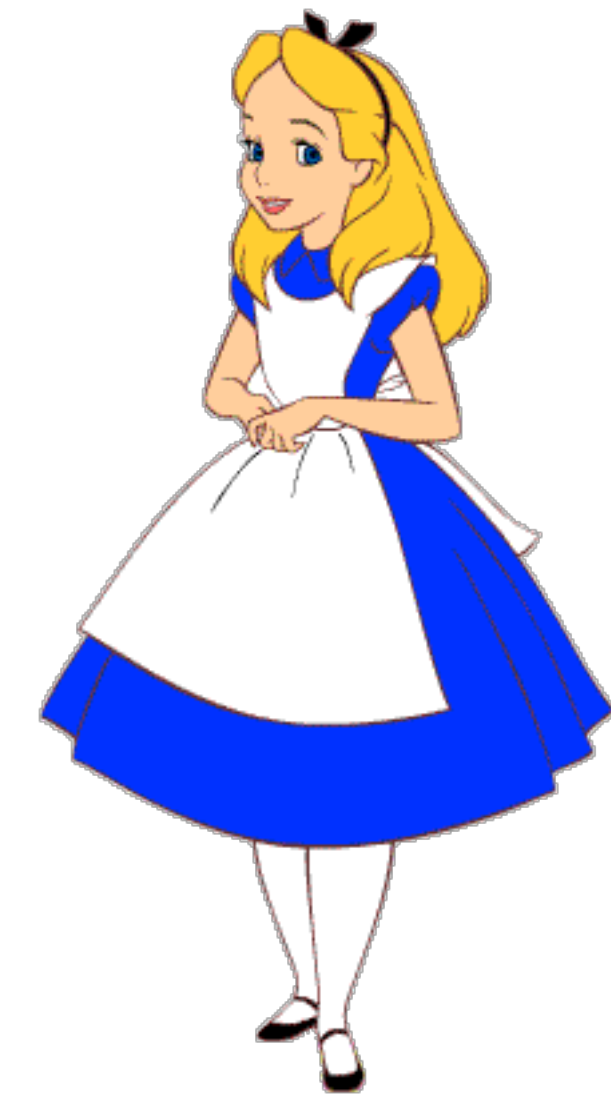
[CFGN'96]



Non-Committing Encryption (NCE)

[CFGN'96]

pk

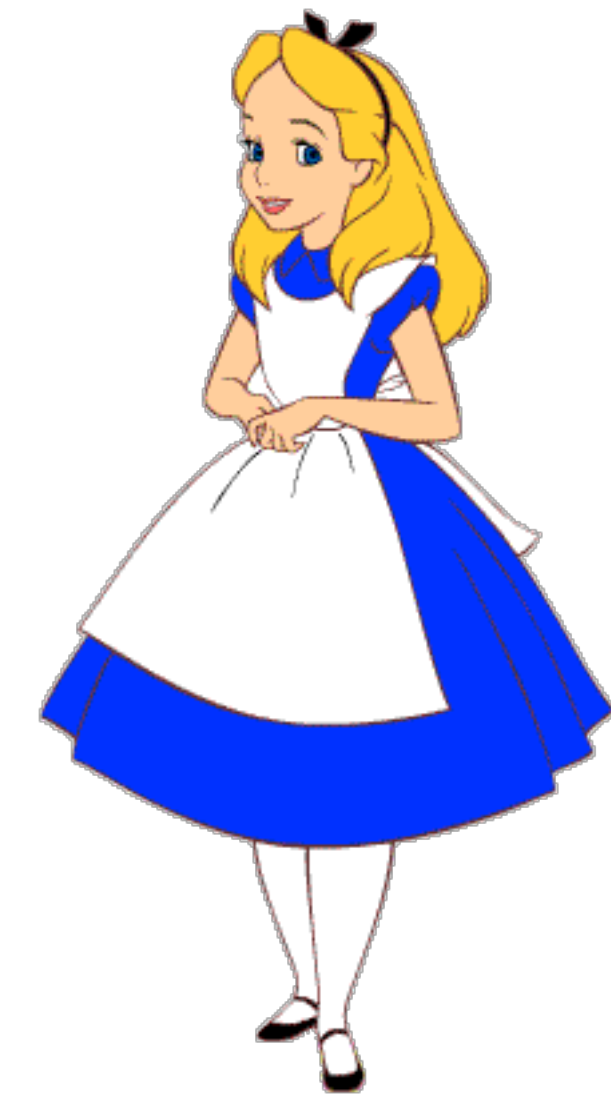


Non-Committing Encryption (NCE)

[CFGN'96]

pk

ct



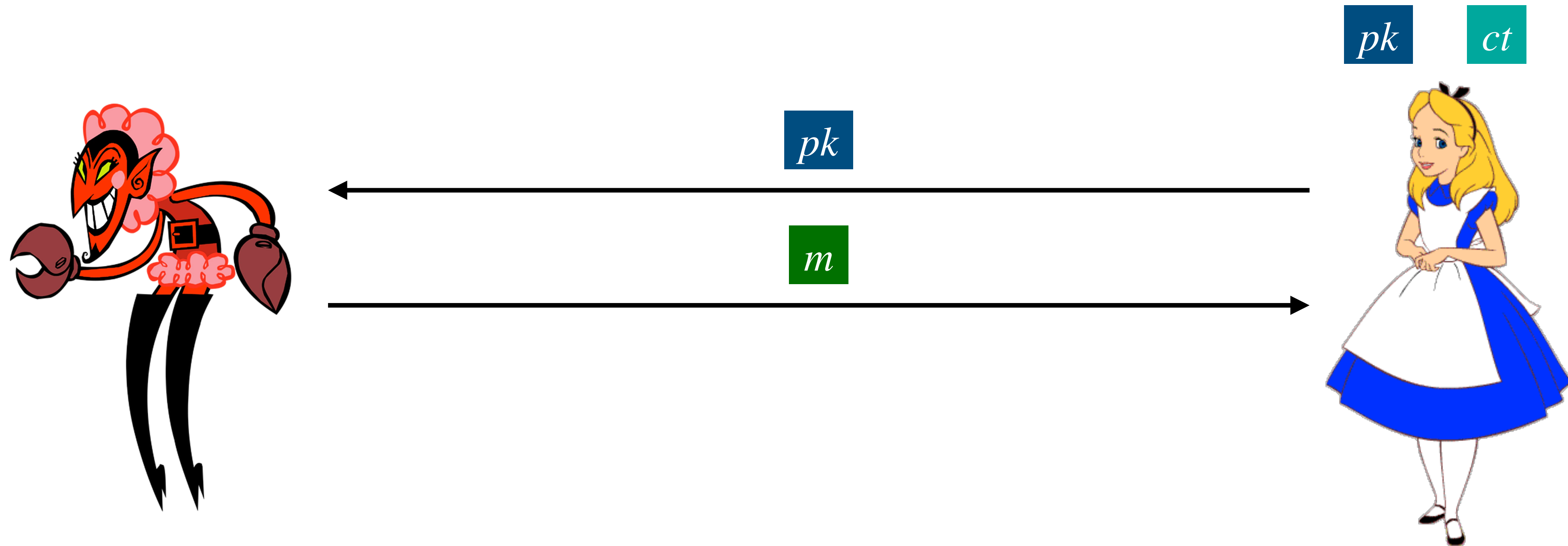
Non-Committing Encryption (NCE)

[CFGN'96]



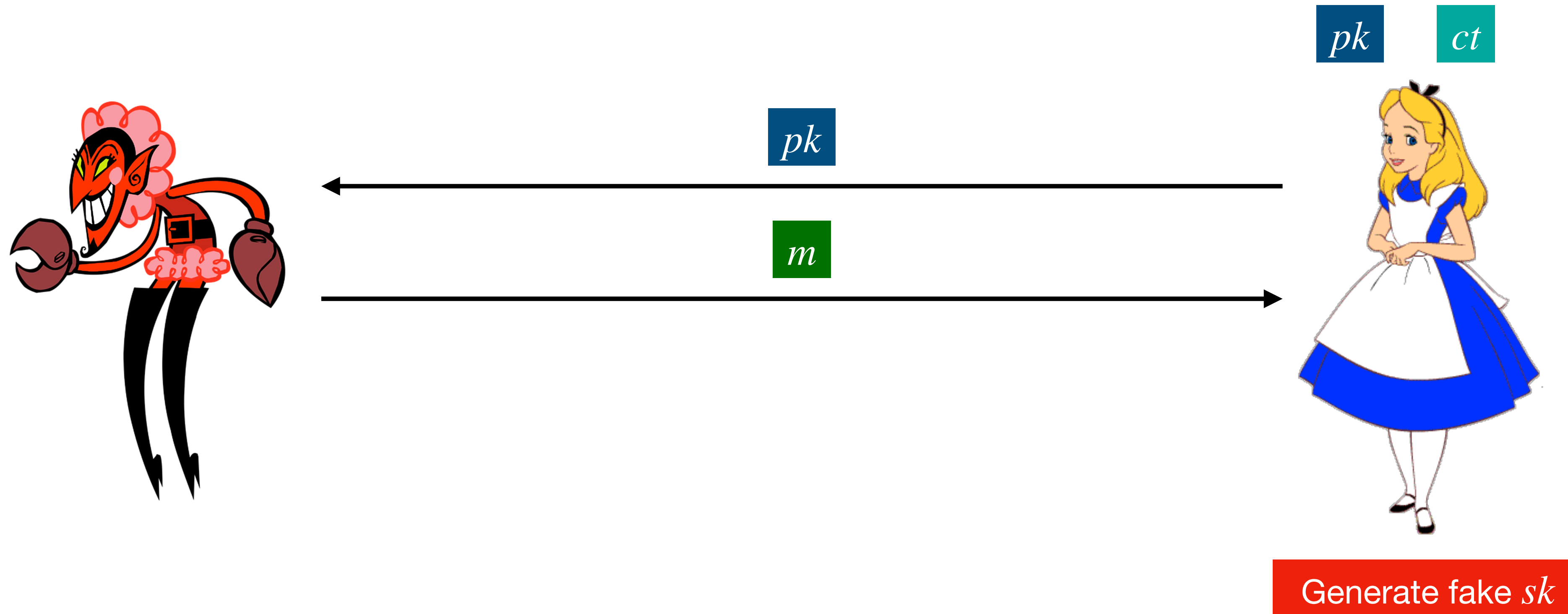
Non-Committing Encryption (NCE)

[CFGN'96]



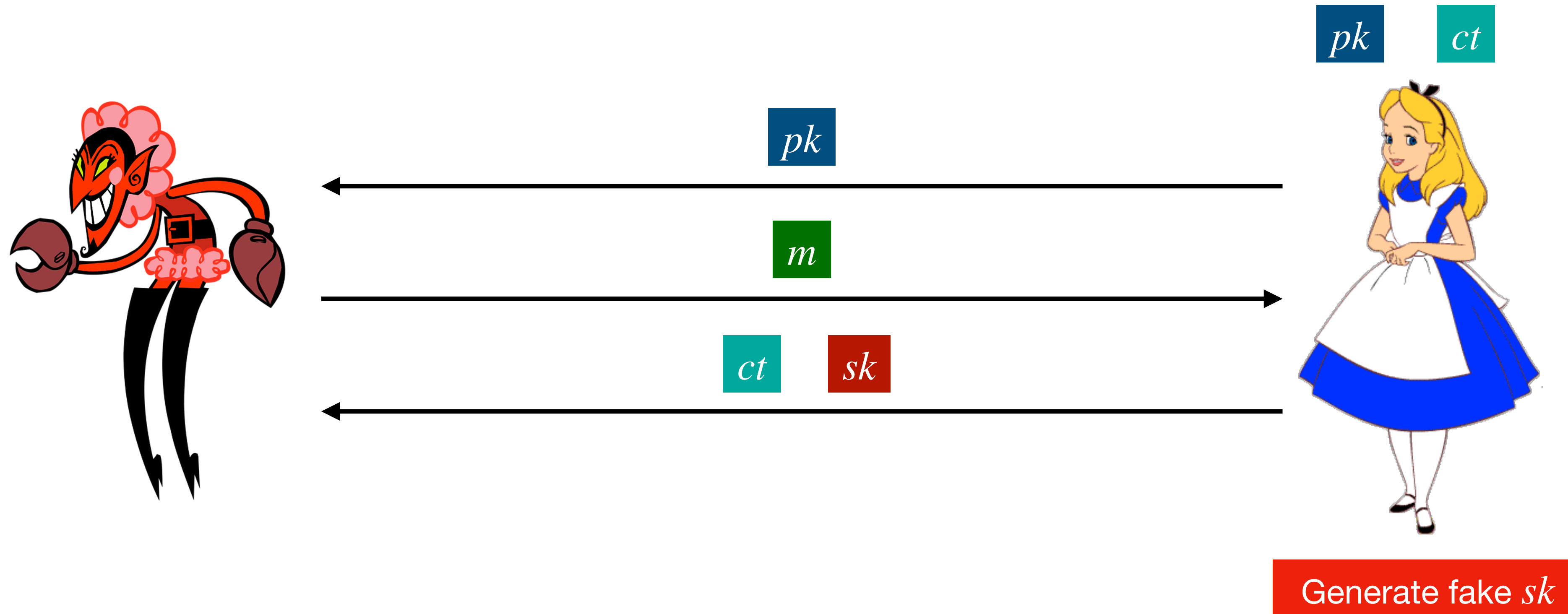
Non-Committing Encryption (NCE)

[CFGN'96]



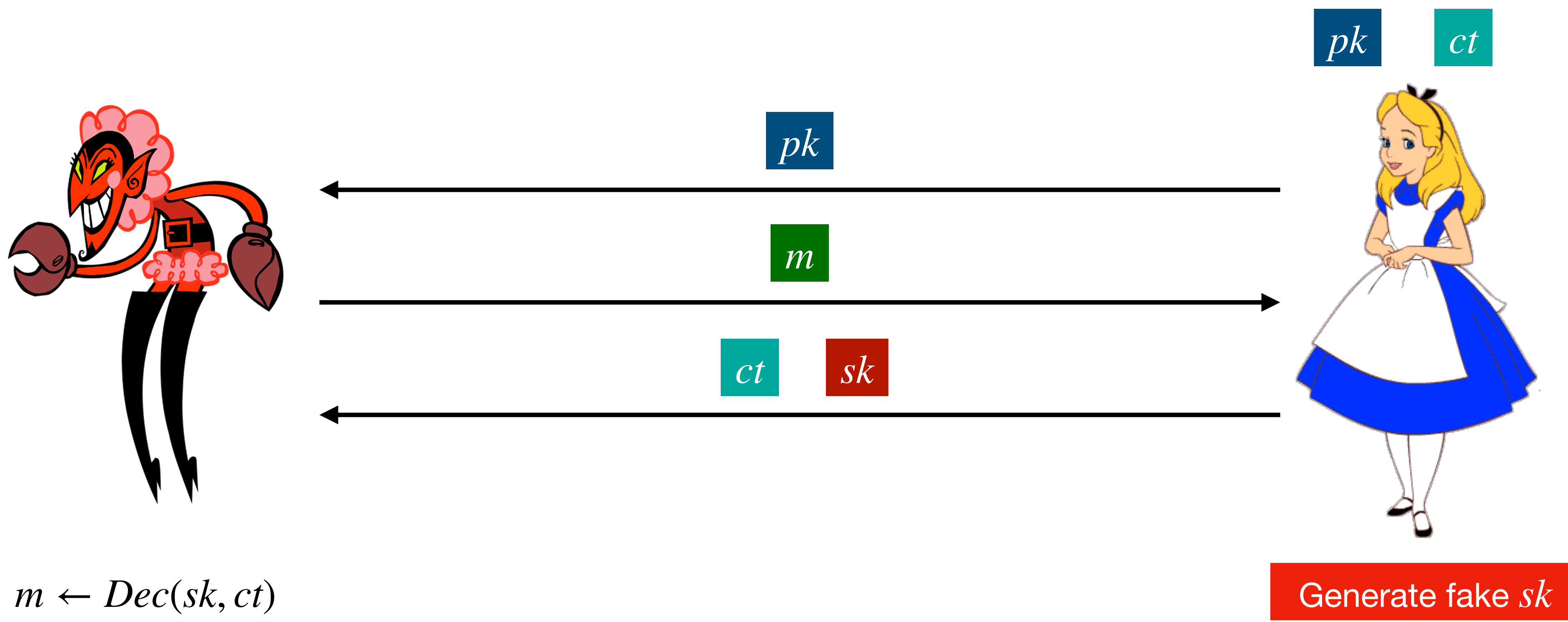
Non-Committing Encryption (NCE)

[CFGN'96]



Non-Committing Encryption (NCE)

[CFGN'96]



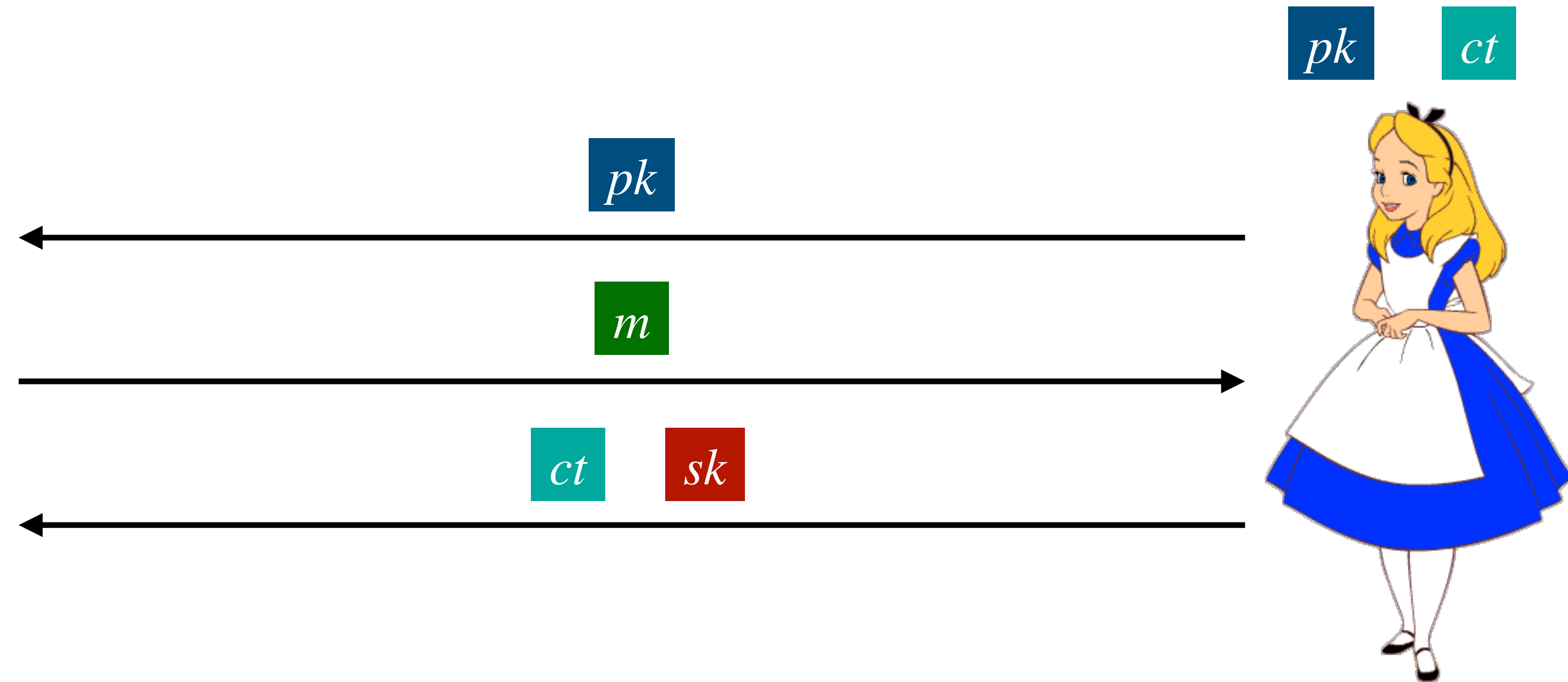
Non-Committing Encryption (NCE)

[CFGN'96]



$$m \leftarrow \text{Dec}(sk, ct)$$

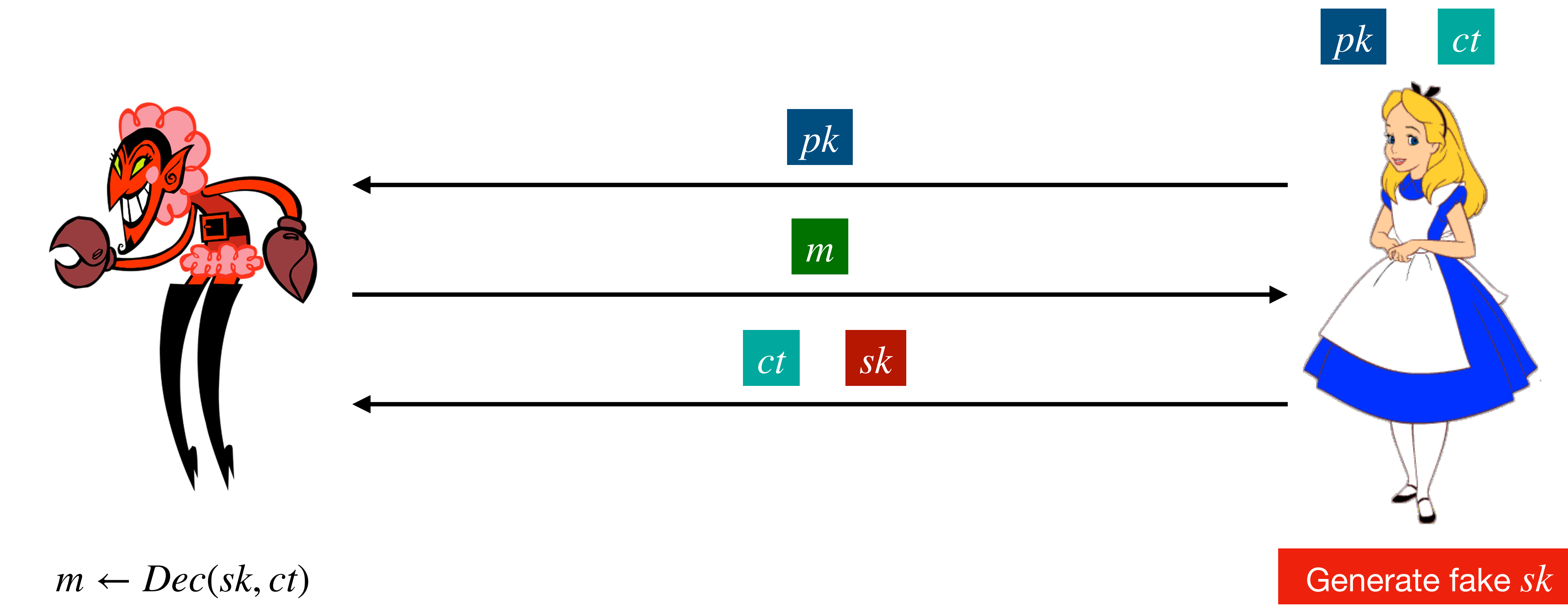
Adaptivity in MPC



Generate fake sk

Non-Committing Encryption (NCE)

[CFGN'96]

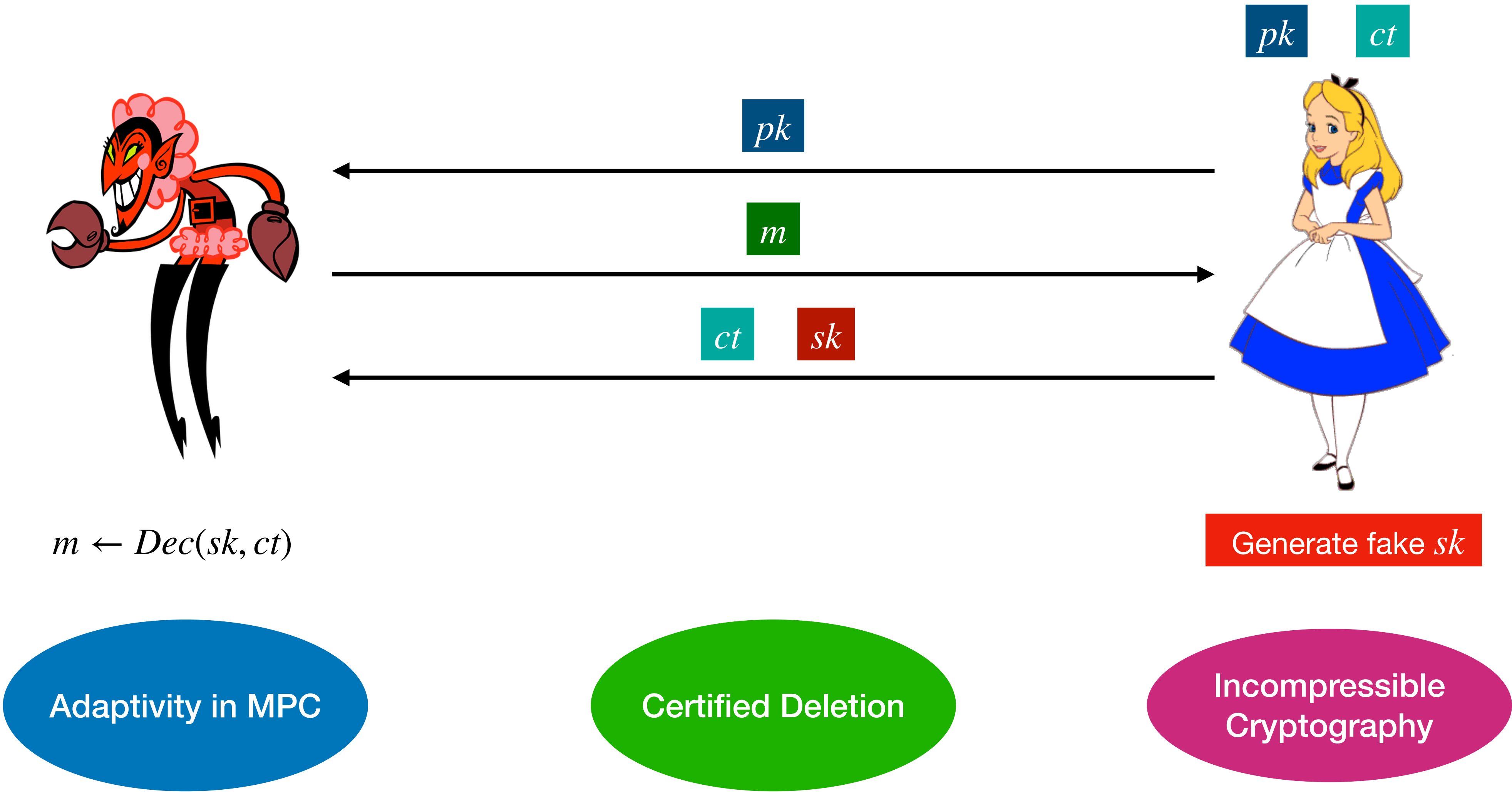


Adaptivity in MPC

Certified Deletion

Non-Committing Encryption (NCE)

[CFGN'96]



Receiver NCE Syntax

Receiver NCE Syntax

$Setup(\lambda) \rightarrow$ public key pk , secret key sk

Receiver NCE Syntax

$Setup(\lambda) \rightarrow$ public key pk , secret key sk

$Enc(pk, m) \rightarrow$ ciphertext ct

Receiver NCE Syntax

$Setup(\lambda) \rightarrow$ public key pk , secret key sk

$Enc(pk, m) \rightarrow$ ciphertext ct

$Dec(sk, ct) \rightarrow m / \perp$

Receiver NCE Syntax

$Setup(\lambda) \rightarrow$ public key pk , secret key sk

$Enc(pk, m) \rightarrow$ ciphertext ct

$Dec(sk, ct) \rightarrow m / \perp$

$Sim_1(\lambda) \rightarrow$ fake public key pk^* , fake ciphertext

Receiver NCE Syntax

$Setup(\lambda) \rightarrow$ public key pk , secret key sk

$Enc(pk, m) \rightarrow$ ciphertext ct

$Dec(sk, ct) \rightarrow m / \perp$

$Sim_1(\lambda) \rightarrow$ fake public key pk^* , fake ciphertext ct^*

$Sim_2(m) \rightarrow$ fake secret key sk^*

Receiver NCE Syntax

$Setup(\lambda) \rightarrow$ public key pk , secret key sk

$Enc(pk, m) \rightarrow$ ciphertext ct

$Dec(sk, ct) \rightarrow m / \perp$

Security

$$\underbrace{\{pk, sk, ct_m\}}_{Real} \approx_c \underbrace{\{pk^*, sk^*, ct^*\}}_{Simulated}$$

$Sim_1(\lambda) \rightarrow$ fake public key pk^* , fake ciphertext ct^*

$Sim_2(m) \rightarrow$ fake secret key sk^*

Identity Based Encryption

[Shamir'85]

Identity Based Encryption

[Shamir'85]

- Generalisation of PKE.

Identity Based Encryption

[Shamir'85]

- Generalisation of PKE.
- n users in the system each with a **distinct identity**. **Secret keys** are associated with **identity id**

Identity Based Encryption

[Shamir'85]

- Generalisation of PKE.
- n users in the system each with a **distinct identity**. **Secret keys** are associated with **identity id**
- To encrypt a message m , a master public key mpk is used along with id .

Identity Based Encryption

[Shamir'85]

- Generalisation of PKE.
- n users in the system each with a **distinct identity**. **Secret keys** are associated with **identity id**
- To encrypt a message m , a master public key mpk is used along with id .
- Adversary gets a challenge ciphertext ct^* for m_0, m_1 encrypted under the identity id^* and then it has to distinguish it.

Identity Based Encryption

[Shamir'85]

- Generalisation of PKE.
- n users in the system each with a **distinct identity**. **Secret keys** are associated with **identity id**
- To encrypt a message m , a master public key mpk is used along with id .
 - Adversary gets a challenge ciphertext ct^* for m_0, m_1 encrypted under the identity id^* and then it has to distinguish it.
 - Also obtains multiple sk_{id} where $id \neq id^*$.

(RNC)-IBE Syntax

(RNC)-IBE Syntax

$Setup(\lambda) \rightarrow$ master public key mpk , master secret key msk

(RNC)-IBE Syntax

$Setup(\lambda) \rightarrow$ master public key mpk , master secret key msk

$Enc(mpk, id, m) \rightarrow$ Ciphertext ct

(RNC)-IBE Syntax

$Setup(\lambda) \rightarrow$ master public key mpk , master secret key msk

$Enc(mpk, id, m) \rightarrow$ Ciphertext ct

$KeyGen(msk, id) \rightarrow$ Secret key sk_{id}

(RNC)-IBE Syntax

$Setup(\lambda) \rightarrow$ master public key mpk , master secret key msk

$Enc(mpk, id, m) \rightarrow$ Ciphertext ct

$KeyGen(msk, id) \rightarrow$ Secret key sk_{id}

$Dec(sk_{id}, ct) \rightarrow m$

(RNC)-IBE Syntax

$Setup(\lambda) \rightarrow$ master public key mpk , master secret key msk

$Enc(mpk, id, m) \rightarrow$ Ciphertext ct

$KeyGen(msk, id) \rightarrow$ Secret key sk_{id}

$Dec(sk_{id}, ct) \rightarrow m$

$Sim_1(\lambda) \rightarrow$ fake master public key mpk^* , fake ciphertext ct^*

(RNC)-IBE Syntax

$Setup(\lambda) \rightarrow$ master public key mpk , master secret key msk

$Enc(mpk, id, m) \rightarrow$ Ciphertext ct

$KeyGen(msk, id) \rightarrow$ Secret key sk_{id}

$Dec(sk_{id}, ct) \rightarrow m$

$Sim_1(\lambda) \rightarrow$ fake master public key mpk^* , fake ciphertext ct^*

$Sim_2(id) \rightarrow$ Fake secret key sk_{id}

(RNC)-IBE Syntax

$Setup(\lambda) \rightarrow$ master public key mpk , master secret key msk

$Enc(mpk, id, m) \rightarrow$ Ciphertext ct

$KeyGen(msk, id) \rightarrow$ Secret key sk_{id}

$Dec(sk_{id}, ct) \rightarrow m$

$Sim_1(\lambda) \rightarrow$ fake master public key mpk^* , fake ciphertext ct^*

$Sim_2(id) \rightarrow$ Fake secret key sk_{id}

$Sim_3(m) \rightarrow$ Fake master secret key msk^*

Prior works*

Prior works*

**Canetti-Feige-Goldreich-
Naor'96**

Introduced NCE to design adaptively secure multiparty computation protocols.

Prior works*

**Canetti-Feige-Goldreich-
Naor'96**

Introduced NCE to design adaptively secure multiparty computation protocols.

**Bea'97,DN'00,CDMW'09,HOR
'15,HORR'15,CPR17,YKT'19**

Constructions from various assumptions.

Prior works*

**Canetti-Feige-Goldreich-
Naor'96**

Introduced NCE to design adaptively secure multiparty computation protocols.

**Bea'97, DN'00, CDMW'09, HOR
'15, HORR'15, CPR17, YKT'19**

Constructions from various assumptions.

**Brakerski-Branco-Döttling-
Garg-Malavolta'20
Yoshida-Kitagawa-Xagawa-
Tanaka'20**

Rate-1 NCE

Prior works*

**Canetti-Feige-Goldreich-
Naor'96**

Introduced NCE to design adaptively secure multiparty computation protocols.

**Bea'97, DN'00, CDMW'09, HOR
'15, HORR'15, CPR17, YKT'19**

Constructions from various assumptions.

**Brakerski-Branco-Döttling-
Garg-Malavolta'20
Yoshida-Kitagawa-Xagawa-
Tanaka'20**

Rate-1 NCE

Reveals randomness used during setup and encryption algorithm.

Prior works*

Canetti-Feige-Goldreich-
Naor'96

Introduced NCE to design adaptively secure multiparty computation protocols.

Bea'97, DN'00, CDMW'09, HOR
'15, HORR'15, CPR17, YKT'19

Constructions from various assumptions.

Brakerski-Branco-Döttling-
Garg-Malavolta'20
Yoshida-Kitagawa-Xagawa-
Tanaka'20

Rate-1 NCE

Hiroka-Morimae-Nishimaki-
Yamakawa'21

Introduced **identity based non-committing encryption** to build certified IBE with certified deletion.

Reveals randomness used during setup and encryption algorithm.

RNC-IBE Security

[Hiroka-Morimae-Nishimaki-Yamakawa'21]

RNC-IBE Security

[Hiroka-Morimae-Nishimaki-Yamakawa'21]



RNC-IBE Security

[Hiroka-Morimae-Nishimaki-Yamakawa'21]



Challenger



Adversary

RNC-IBE Security

[Hiroka-Morimae-Nishimaki-Yamakawa'21]



Challenger

$(mpk, msk) \leftarrow Setup(\lambda)$



Adversary

RNC-IBE Security

[Hiroka-Morimae-Nishimaki-Yamakawa'21]



Challenger



Adversary

$(mpk, msk) \leftarrow \text{Setup}(\lambda)$

mpk



RNC-IBE Security

[Hiroka-Morimae-Nishimaki-Yamakawa'21]



Challenger



Adversary

$(mpk, msk) \leftarrow \text{Setup}(\lambda)$

mpk

id

$\text{KeyGen}(msk, id)$

RNC-IBE Security

[Hiroka-Morimae-Nishimaki-Yamakawa'21]

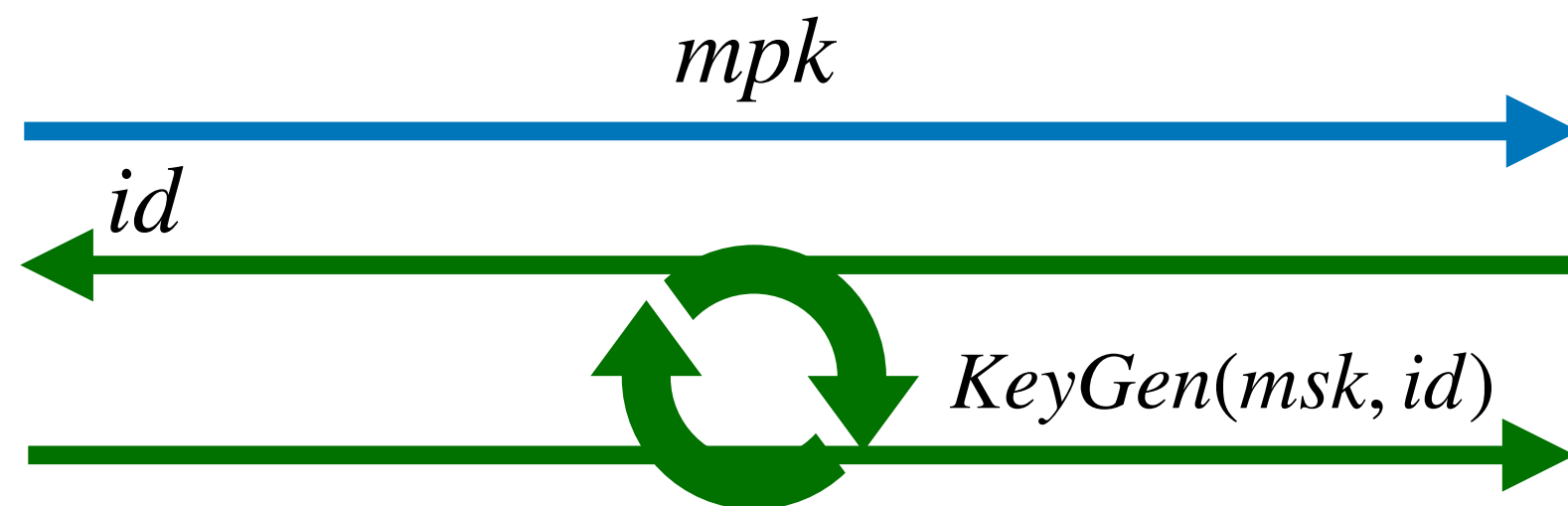


Challenger



Adversary

$(mpk, msk) \leftarrow \text{Setup}(\lambda)$



RNC-IBE Security

[Hiroka-Morimae-Nishimaki-Yamakawa'21]

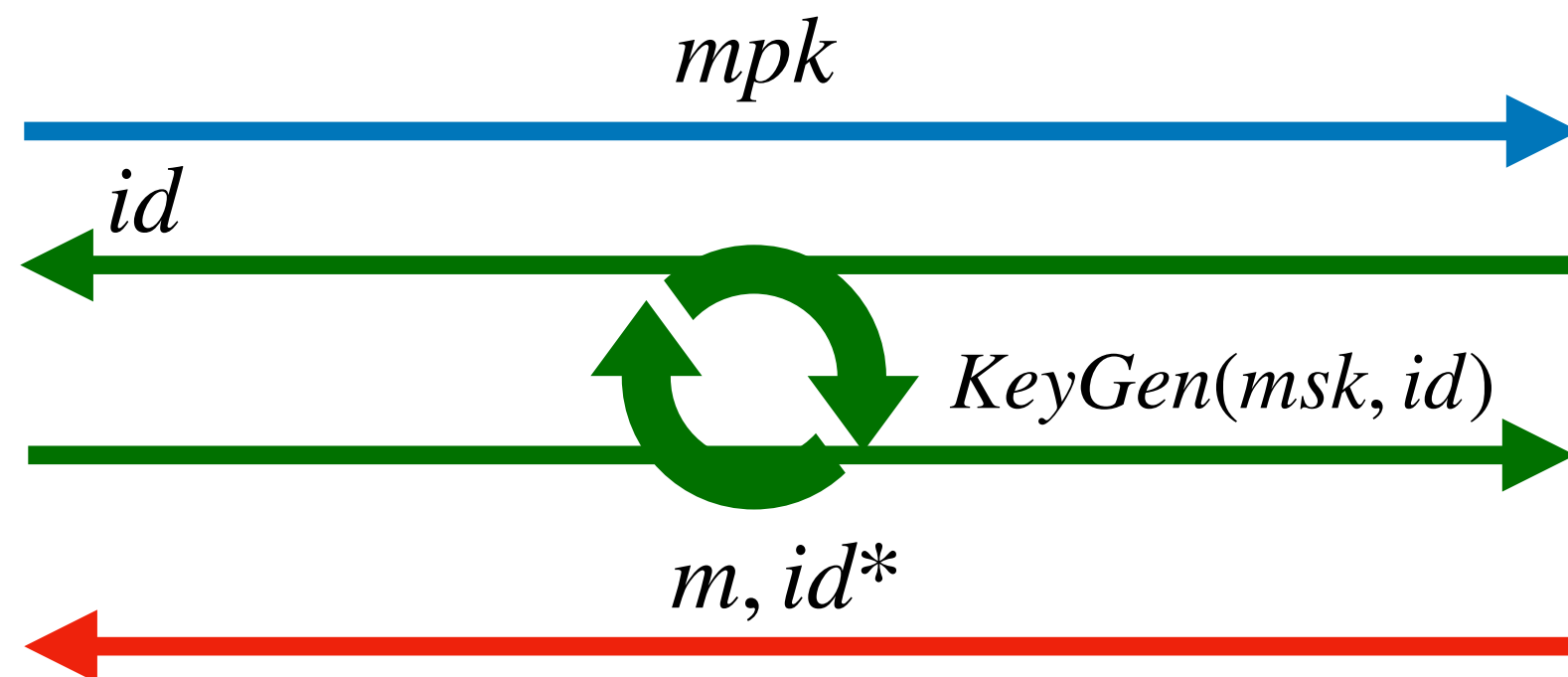


Challenger



Adversary

$(mpk, msk) \leftarrow \text{Setup}(\lambda)$



RNC-IBE Security

[Hiroka-Morimae-Nishimaki-Yamakawa'21]

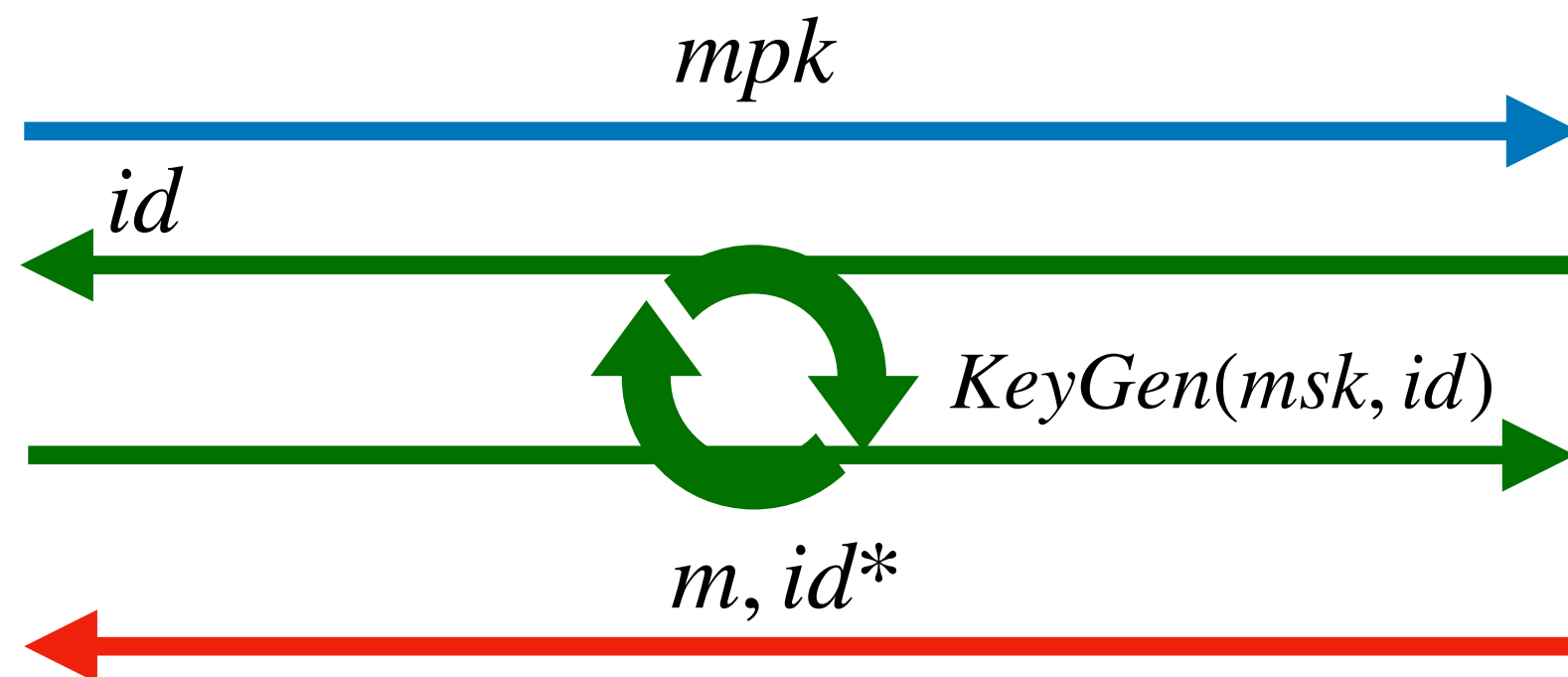


Challenger



Adversary

$(mpk, msk) \leftarrow Setup(\lambda)$



$b = 0$
 $ct \leftarrow Enc(mpk, id^*, m)$

RNC-IBE Security

[Hiroka-Morimae-Nishimaki-Yamakawa'21]



Challenger



Adversary

$(mpk, msk) \leftarrow Setup(\lambda)$

mpk

id

$KeyGen(msk, id)$

m, id^*

$b = 0$

$ct \leftarrow Enc(mpk, id^*, m)$

ct, msk

RNC-IBE Security

[Hiroka-Morimae-Nishimaki-Yamakawa'21]



Challenger



Adversary

$(mpk, msk) \leftarrow Setup(\lambda)$

mpk

id

$KeyGen(msk, id)$

m, id^*

$b = 0$

$ct \leftarrow Enc(mpk, id^*, m)$

ct, msk

$b' \in \{0,1\}$

RNC-IBE Security

[Hiroka-Morimae-Nishimaki-Yamakawa'21]

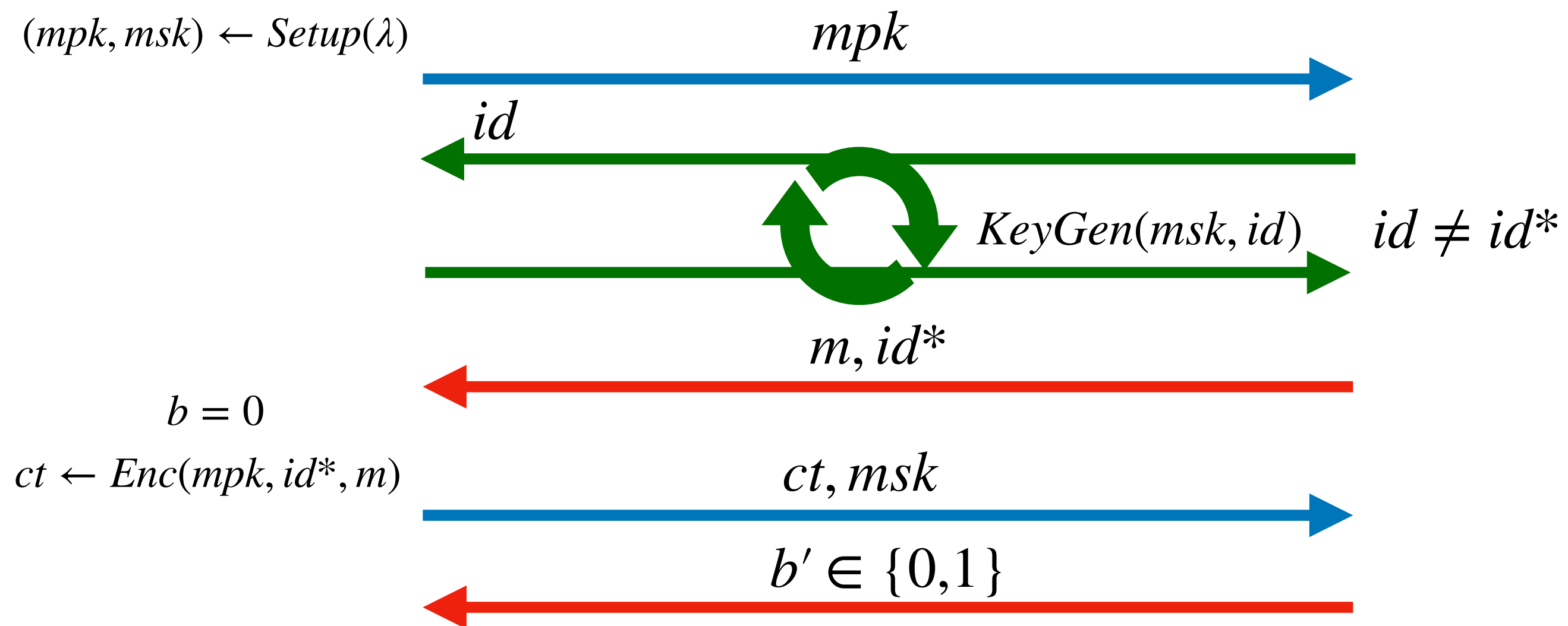


Challenger



Adversary

$(mpk, msk) \leftarrow Setup(\lambda)$



RNC-IBE Security

[Hiroka-Morimae-Nishimaki-Yamakawa'21]



Challenger

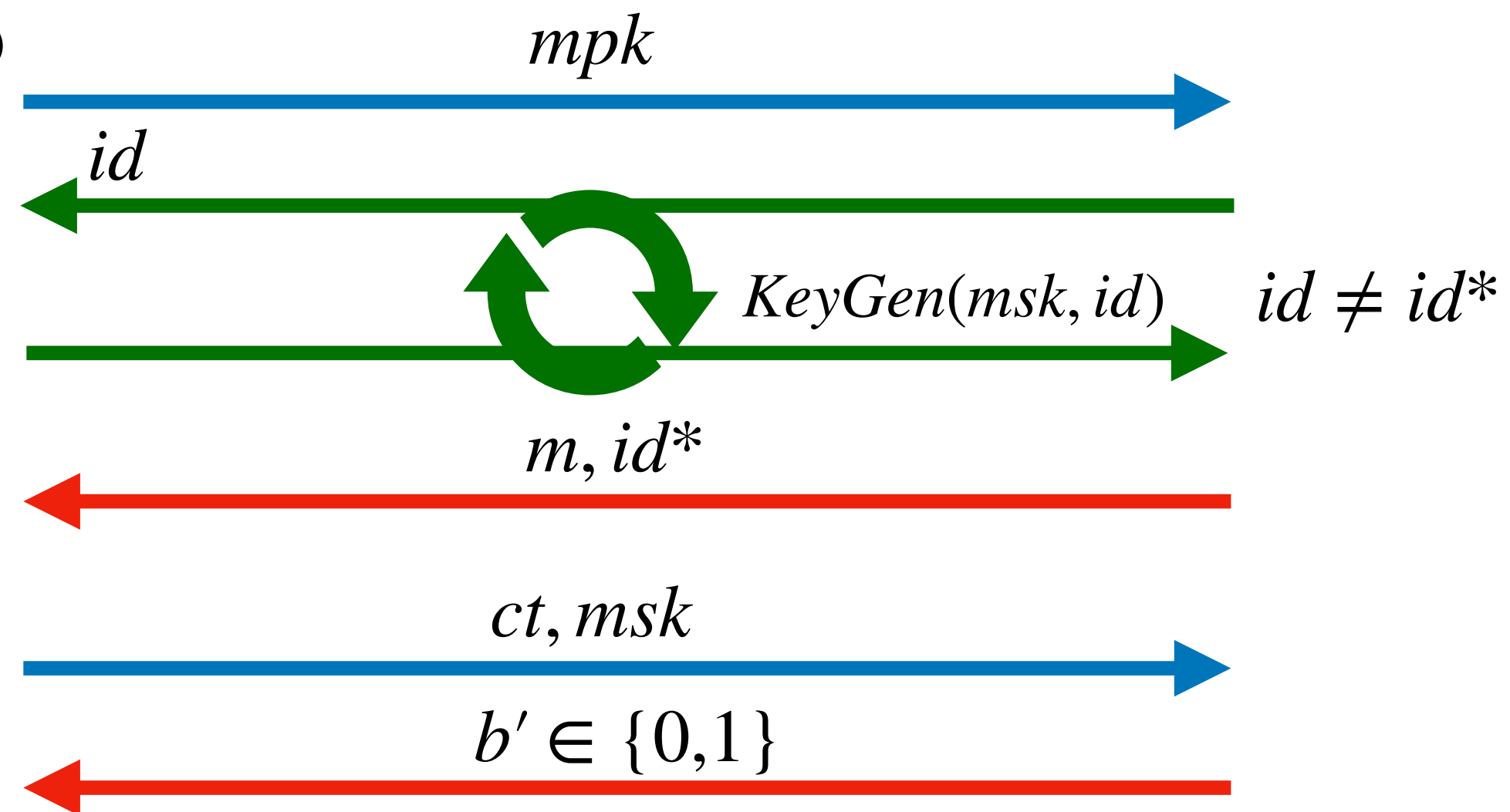


Adversary



Simulator

$(mpk, msk) \leftarrow Setup(\lambda)$



RNC-IBE Security

[Hiroka-Morimae-Nishimaki-Yamakawa'21]



Challenger



Adversary



Simulator

$(mpk, msk) \leftarrow Setup(\lambda)$

mpk

id

$KeyGen(msk, id)$

$id \neq id^*$

m, id^*

$b = 0$

$ct \leftarrow Enc(mpk, id^*, m)$

ct, msk

$b' \in \{0,1\}$

$(mpk, ct) \leftarrow Sim_1(\lambda)$

RNC-IBE Security

[Hiroka-Morimae-Nishimaki-Yamakawa'21]



Challenger



Adversary



Simulator

$(mpk, msk) \leftarrow Setup(\lambda)$

mpk

id

$KeyGen(msk, id)$

$id \neq id^*$

m, id^*

$b = 0$

$ct \leftarrow Enc(mpk, id^*, m)$

ct, msk

$b' \in \{0, 1\}$

$(mpk, ct) \leftarrow Sim_1(\lambda)$

RNC-IBE Security

[Hiroka-Morimae-Nishimaki-Yamakawa'21]



Challenger



Adversary



Simulator

$(mpk, msk) \leftarrow Setup(\lambda)$

mpk

id

$KeyGen(msk, id)$

$id \neq id^*$

m, id^*

$b = 0$

$ct \leftarrow Enc(mpk, id^*, m)$

ct, msk

$b' \in \{0, 1\}$

mpk

$(mpk, ct) \leftarrow Sim_1(\lambda)$

RNC-IBE Security

[Hiroka-Morimae-Nishimaki-Yamakawa'21]



Challenger



Adversary

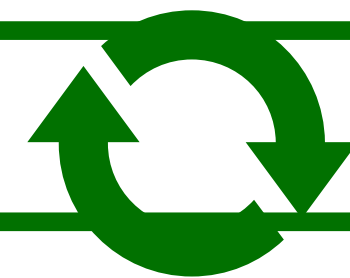


Simulator

$(mpk, msk) \leftarrow Setup(\lambda)$

mpk

id



$KeyGen(msk, id)$

$id \neq id^*$

m, id^*

$b = 0$

$ct \leftarrow Enc(mpk, id^*, m)$

ct, msk

$b' \in \{0, 1\}$

mpk

$(mpk, ct) \leftarrow Sim_1(\lambda)$

id

$Sim_2(id)$

RNC-IBE Security

[Hiroka-Morimae-Nishimaki-Yamakawa'21]



Challenger



Adversary



Simulator

$(mpk, msk) \leftarrow Setup(\lambda)$

mpk

id



m, id^*

$b = 0$

$ct \leftarrow Enc(mpk, id^*, m)$

ct, msk

$b' \in \{0,1\}$

mpk

id



$(mpk, ct) \leftarrow Sim_1(\lambda)$

RNC-IBE Security

[Hiroka-Morimae-Nishimaki-Yamakawa'21]



Challenger

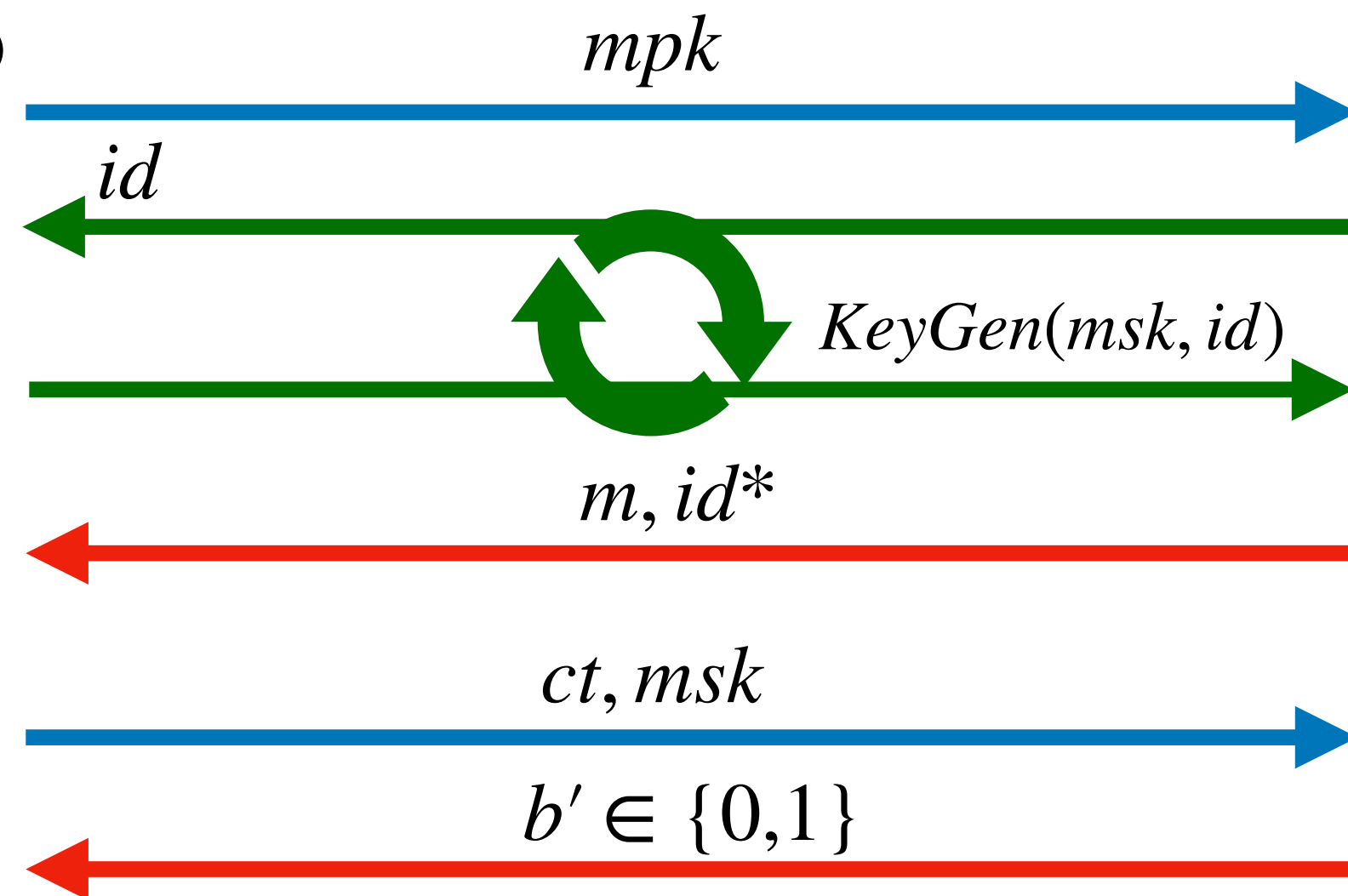


Adversary

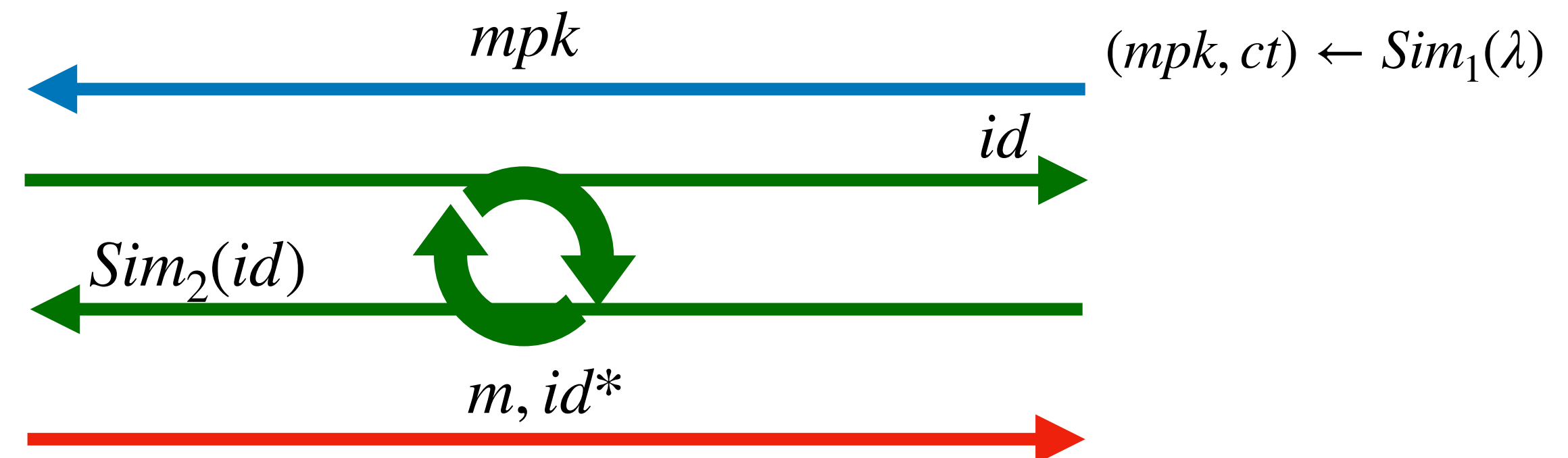


Simulator

$(mpk, msk) \leftarrow Setup(\lambda)$



$id \neq id^*$



$(mpk, ct) \leftarrow Sim_1(\lambda)$

RNC-IBE Security

[Hiroka-Morimae-Nishimaki-Yamakawa'21]



Challenger

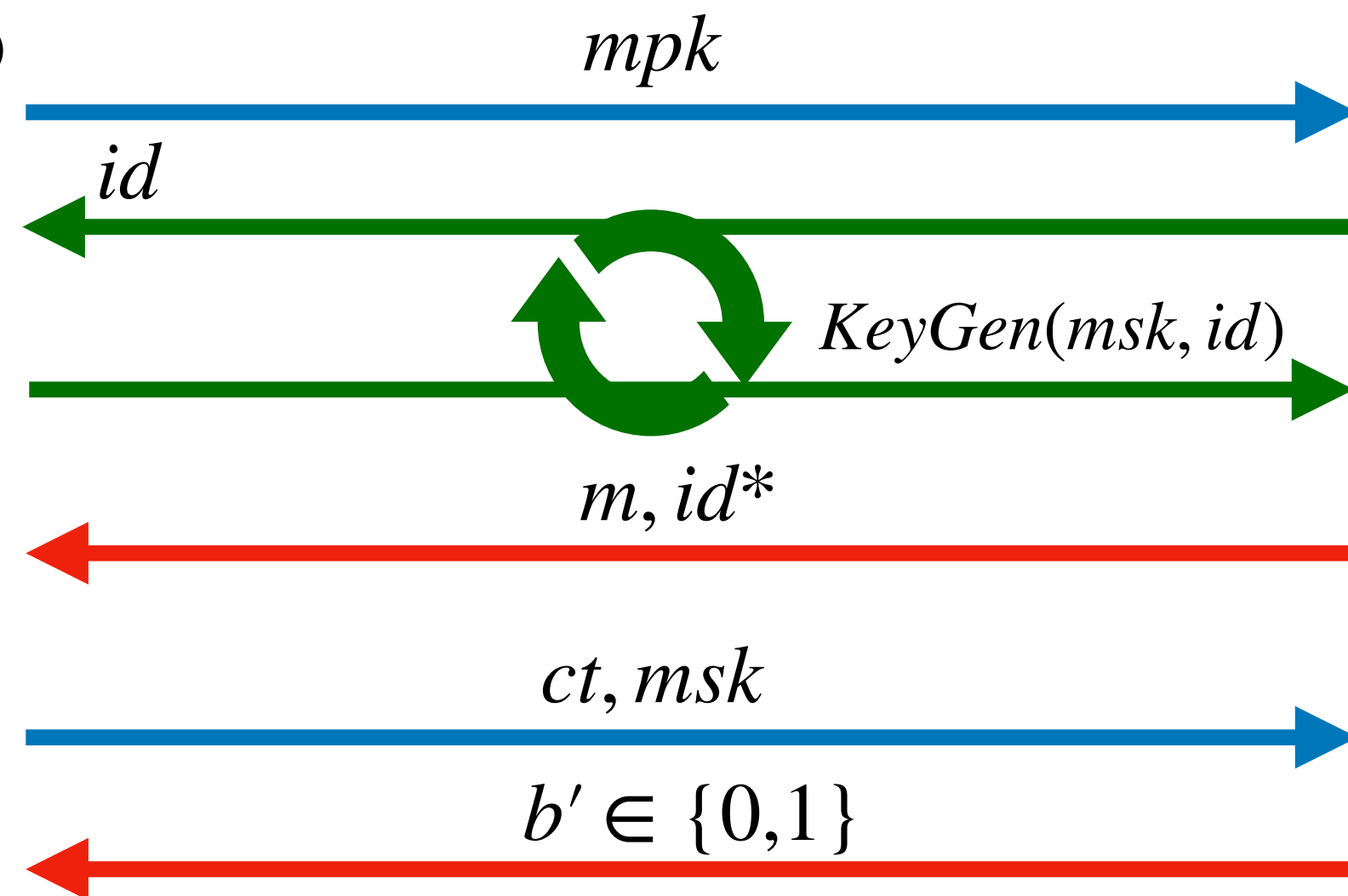


Adversary

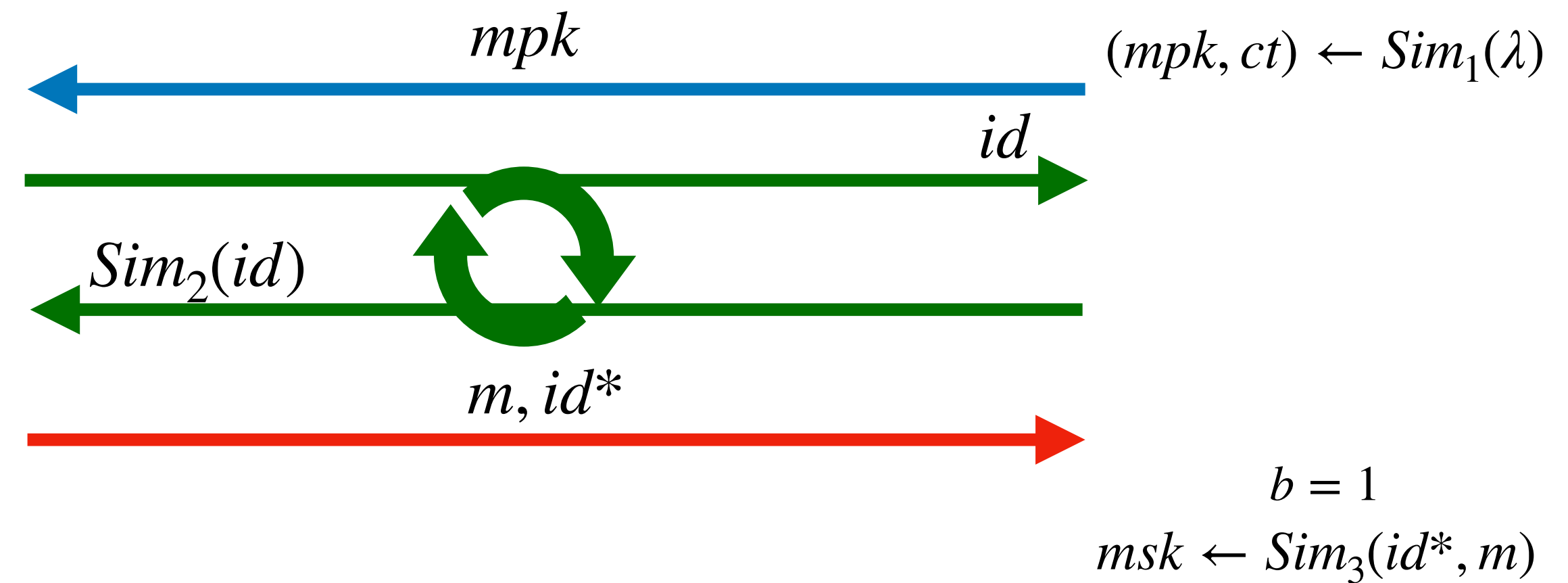


Simulator

$(mpk, msk) \leftarrow Setup(\lambda)$



$id \neq id^*$



RNC-IBE Security

[Hiroka-Morimae-Nishimaki-Yamakawa'21]



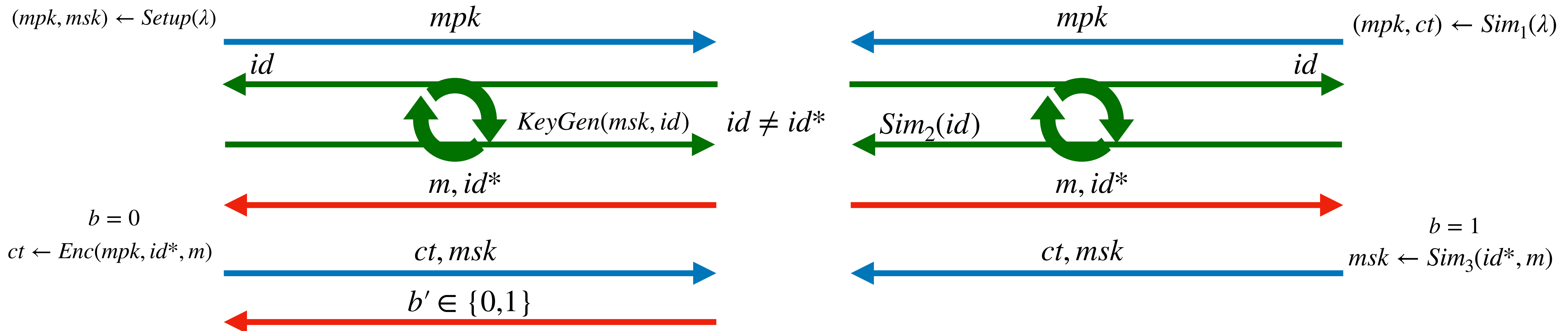
Challenger



Adversary



Simulator



RNC-IBE Security

[Hiroka-Morimae-Nishimaki-Yamakawa'21]



Challenger

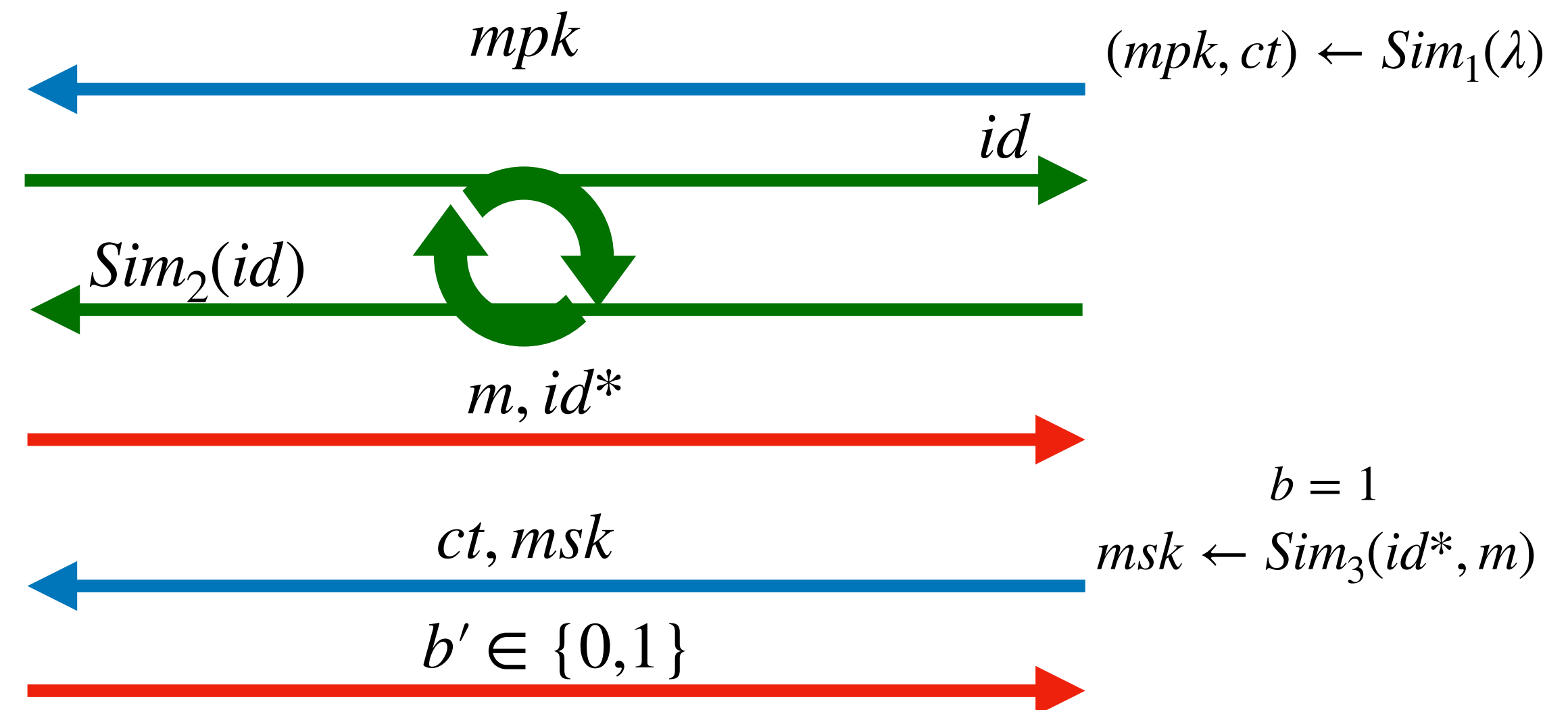
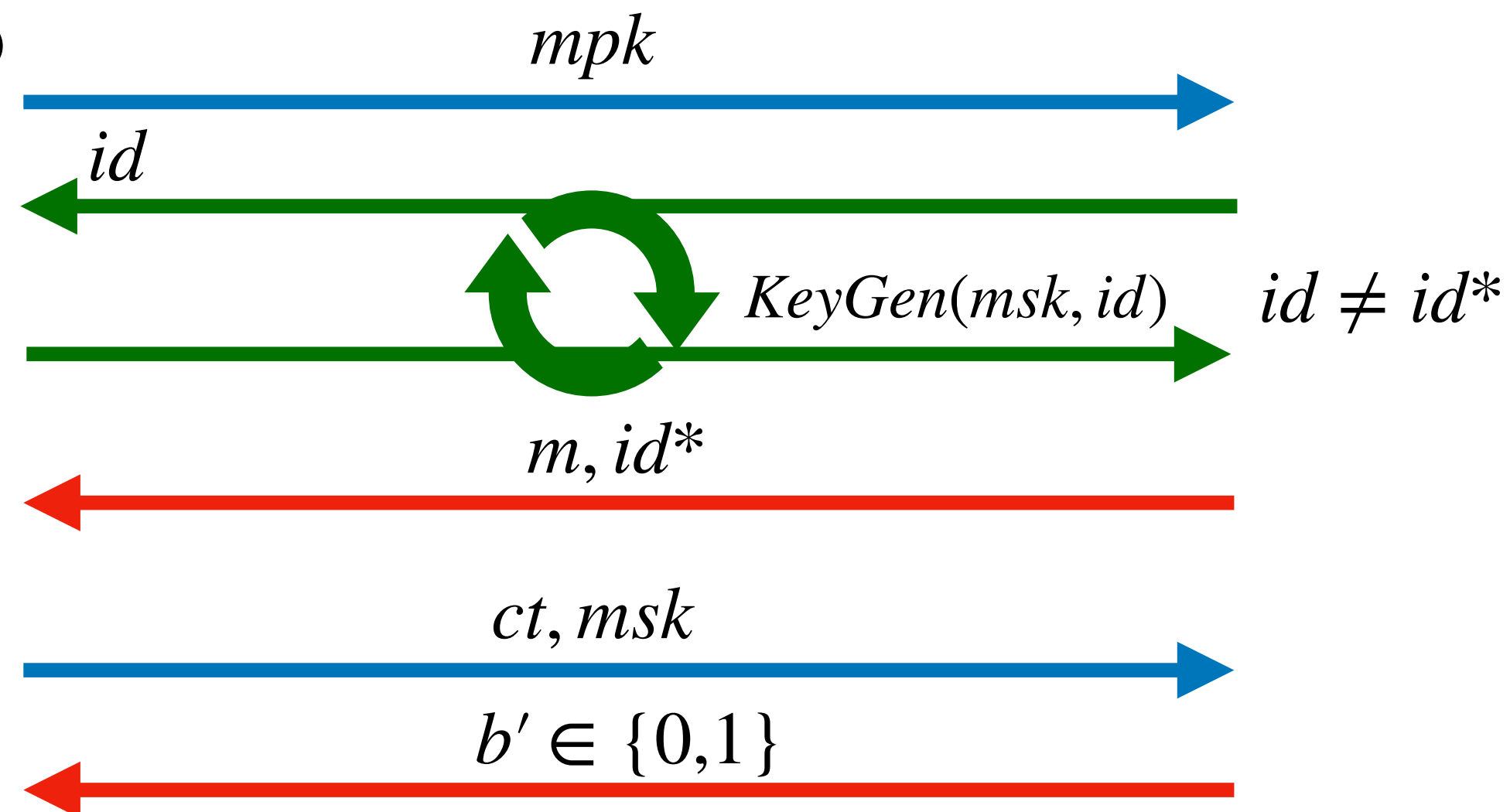


Adversary



Simulator

$(mpk, msk) \leftarrow Setup(\lambda)$



RNC-IBE Security

[Hiroka-Morimae-Nishimaki-Yamakawa'21]



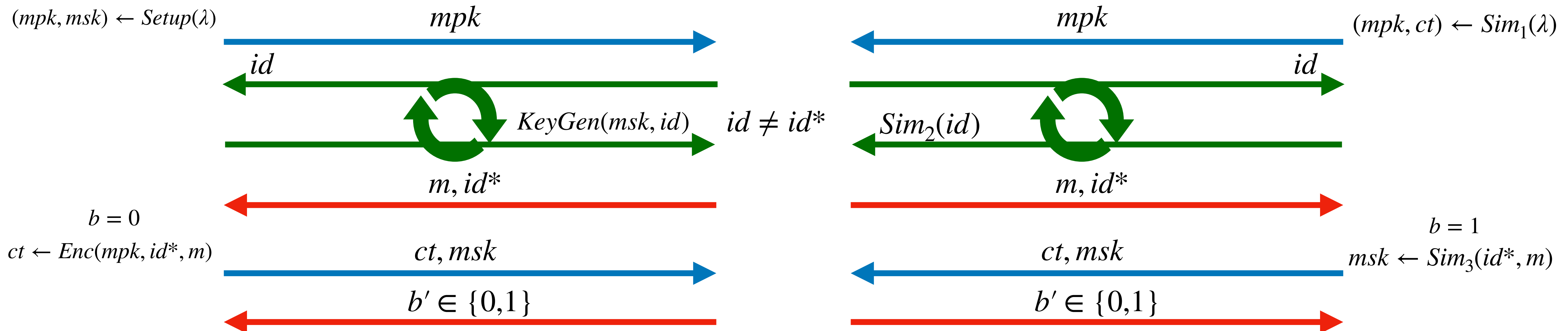
Challenger



Adversary



Simulator



Adversary wins if $b = b'$

This work

This work

**Can we build RNC-IBE from standard
assumptions*?**

This work

Can we build RNC-IBE from standard assumptions*?

Prior work used indistinguishable obfuscation.

Our Results

Our Results

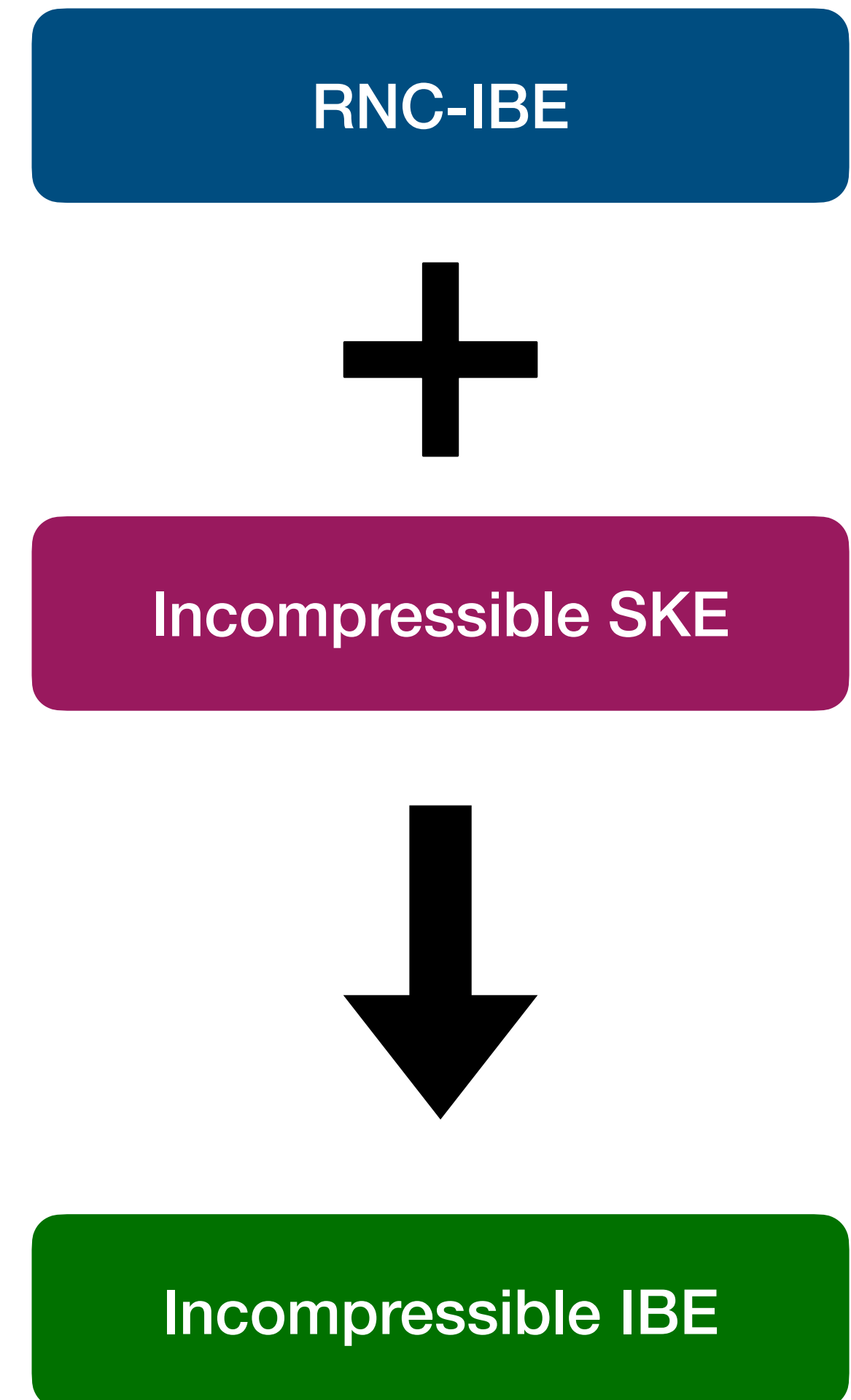
- **Rate-1** RNC-IBE from **bilinear pairings**.

Our Results

- **Rate-1** RNC-IBE from **bilinear pairings**.
- **Rate-1** strong incompressible IBE from **bilinear pairings** and **LWE** (or **DCR**)

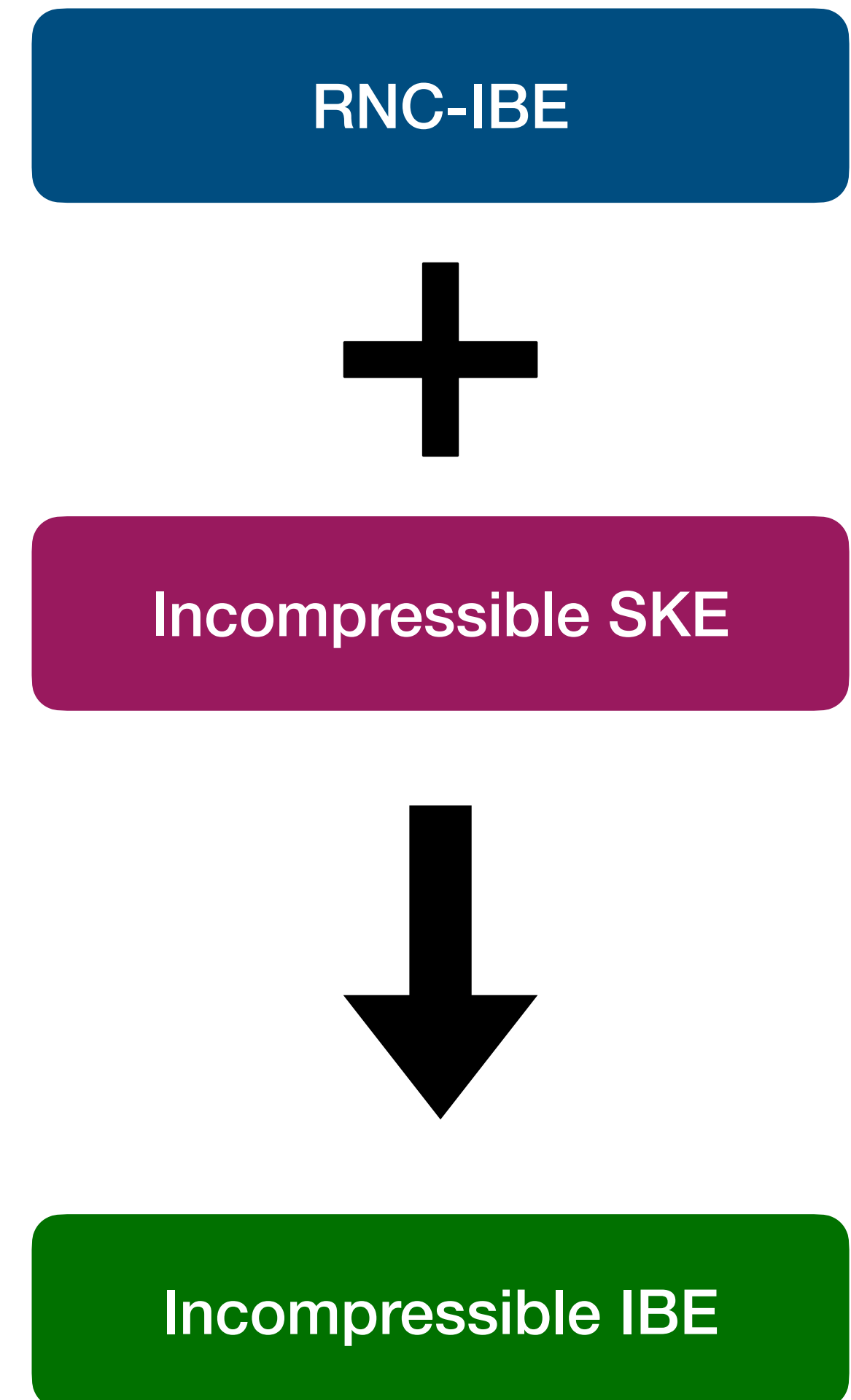
Our Results

- **Rate-1** RNC-IBE from **bilinear pairings**.
- **Rate-1** strong incompressible IBE from **bilinear pairings** and **LWE** (or **DCR**)



Our Results

- **Rate-1** RNC-IBE from **bilinear pairings**.
- **Rate-1** strong incompressible IBE from **bilinear pairings** and **LWE** (or **DCR**)
- RNC-IBE for **polynomially bounded identity space** from **DDH**, **LWE**.



Bilinear Pairings

Bilinear Pairings

$e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ where $\mathbb{G}_i$ is a prime order group

Bilinear Pairings

$e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ where $\mathbb{G}_i$ is a prime order group

$g_1, g_2, e(g_1, g_2)$ are generators of $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$

Bilinear Pairings

$e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ where $\mathbb{G}_i$ is a prime order group

$g_1, g_2, e(g_1, g_2)$ are generators of $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$

$$e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$$

Bilinear Pairings

$e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ where $\mathbb{G}_i$ is a prime order group

$g_1, g_2, e(g_1, g_2)$ are generators of $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$

$$e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$$

$[a]_b$ denotes g_b^a

Construction

Construction

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

Construction

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

Setup $\rightarrow$

Construction

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

$$Setup \rightarrow MSK = ($$

Construction

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

$$Setup \rightarrow MSK = (\quad k \leftarrow \mathbb{Z}_p^2 \quad)$$

Construction

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

$$\begin{aligned} Setup \rightarrow MSK &= (\quad k \leftarrow \mathbb{Z}_p^2 \quad) \\ MPK &= (\end{aligned}$$

Construction

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

$$\begin{aligned} Setup \rightarrow MSK &= (\quad k \leftarrow \mathbb{Z}_p^2 \quad) \\ MPK &= (\quad [a^T k]_T \quad) \end{aligned}$$

Construction

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

$$\begin{aligned} Setup \rightarrow MSK &= (\quad k \leftarrow \mathbb{Z}_p^2 \quad) \\ MPK &= (\quad [a^T k]_T \quad) \end{aligned}$$

$$KeyGen(id) \rightarrow ($$

Construction

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

$$\begin{aligned} \text{Setup} \rightarrow MSK &= (\quad k \leftarrow \mathbb{Z}_p^2 \quad) \\ MPK &= (\quad [a^T k]_T \quad) \end{aligned}$$

$$\text{KeyGen}(id) \rightarrow (\quad [sb]_2 \quad),$$

Construction

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

$$Setup \rightarrow MSK = (\quad k \leftarrow \mathbb{Z}_p^2 \quad)$$

$$MPK = (\quad [a^T k]_T \quad)$$

$$KeyGen(id) \rightarrow (\quad [sb]_2 \quad , \quad [k + s(W_1 + id \cdot W_2)^T b]_2 \quad)$$

Construction

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

$$Setup \rightarrow MSK = (\quad k \leftarrow \mathbb{Z}_p^2 \quad)$$

$$MPK = (\quad [a^T k]_T \quad)$$

$$KeyGen(id) \rightarrow (\quad [sb]_2 \quad , \quad [k + s(W_1 + id \cdot W_2)^T b]_2 \quad)$$

$$Enc(MPK, id, m \in \mathbb{G}_T) \rightarrow$$

Construction

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

$$Setup \rightarrow MSK = (\quad k \leftarrow \mathbb{Z}_p^2 \quad)$$

$$MPK = (\quad [a^T k]_T \quad)$$

$$KeyGen(id) \rightarrow (\quad [sb]_2 \quad , \quad [k + s(W_1 + id \cdot W_2)^T b]_2 \quad)$$

$$Enc(MPK, id, m \in \mathbb{G}_T) \rightarrow ($$

Construction

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

$$Setup \rightarrow MSK = (\quad k \leftarrow \mathbb{Z}_p^2 \quad)$$

$$MPK = (\quad [a^T k]_T \quad)$$

$$KeyGen(id) \rightarrow (\quad [sb]_2 \quad , \quad [k + s(W_1 + id \cdot W_2)^T b]_2 \quad)$$

$$Enc(MPK, id, m \in \mathbb{G}_T) \rightarrow (\quad [ra]_1 \quad ,$$

Construction

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

$$Setup \rightarrow MSK = (\quad k \leftarrow \mathbb{Z}_p^2 \quad)$$

$$MPK = (\quad [a^T k]_T \quad)$$

$$KeyGen(id) \rightarrow (\quad [sb]_2 \quad , \quad [k + s(W_1 + id \cdot W_2)^T b]_2 \quad)$$

$$Enc(MPK, id, m \in \mathbb{G}_T) \rightarrow (\quad [ra]_1 \quad , \quad [r(W_1 + id \cdot W_2)a]_1 \quad ,$$

Construction

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

$$\begin{aligned} Setup &\rightarrow MSK = (\quad k \leftarrow \mathbb{Z}_p^2 \quad) \\ MPK &= (\quad [a^T k]_T \quad) \end{aligned}$$

$$KeyGen(id) \rightarrow (\quad [sb]_2 \quad , \quad [k + s(W_1 + id \cdot W_2)^T b]_2 \quad)$$

$$Enc(MPK, id, m \in \mathbb{G}_T) \rightarrow (\quad [ra]_1 \quad , \quad [r(W_1 + id \cdot W_2)a]_1 \quad , \quad [ra^T k]_T \cdot m \quad)$$

Construction

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

$$\text{Setup} \rightarrow \text{MSK} = (\quad k \leftarrow \mathbb{Z}_p^2 \quad)$$
$$\text{MPK} = (\quad [a^T k]_T \quad)$$

$$\text{KeyGen}(id) \rightarrow (\quad [sb]_2 \quad , \quad [k + s(W_1 + id \cdot W_2)^T b]_2 \quad)$$

$$\text{Enc}(\text{MPK}, id, m \in \mathbb{G}_T) \rightarrow (\quad [ra]_1 \quad , \quad [r(W_1 + id \cdot W_2)a]_1 \quad , \quad [ra^T k]_T \cdot m \quad)$$

$$\text{Dec}(sk_{id}, ct) \rightarrow$$

Construction

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

$$\begin{aligned} \text{Setup} \rightarrow MSK &= (\quad k \leftarrow \mathbb{Z}_p^2 \quad) \\ MPK &= (\quad [a^T k]_T \quad) \end{aligned}$$

$$\text{KeyGen}(id) \rightarrow (\quad [sb]_2 \quad , \quad [k + s(W_1 + id \cdot W_2)^T b]_2 \quad)$$

$$\text{Enc}(MPK, id, m \in \mathbb{G}_T) \rightarrow (\quad [ra]_1 \quad , \quad [r(W_1 + id \cdot W_2)a]_1 \quad , \quad [ra^T k]_T \cdot m \quad)$$

$$\text{Dec}(sk_{id}, ct) \rightarrow [ra^T k]_T \cdot m$$

Construction

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

$$\begin{aligned} Setup &\rightarrow MSK = (\quad k \leftarrow \mathbb{Z}_p^2 \quad) \\ MPK &= (\quad [a^T k]_T \quad) \end{aligned}$$

$$KeyGen(id) \rightarrow (\quad [sb]_2 \quad , \quad [k + s(W_1 + id \cdot W_2)^T b]_2 \quad)$$

$$Enc(MPK, id, m \in \mathbb{G}_T) \rightarrow (\quad [ra]_1 \quad , \quad [r(W_1 + id \cdot W_2)a]_1 \quad , \quad [ra^T k]_T \cdot m \quad)$$

$$Dec(sk_{id}, ct) \rightarrow [ra^T k]_T \cdot m \times$$

Construction

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

$$\text{Setup} \rightarrow \text{MSK} = (\quad k \leftarrow \mathbb{Z}_p^2 \quad)$$
$$\text{MPK} = (\quad [a^T k]_T \quad)$$

$$\text{KeyGen}(id) \rightarrow (\quad [sb]_2 \quad , \quad [k + s(W_1 + id \cdot W_2)^T b]_2 \quad)$$

$$\text{Enc}(\text{MPK}, id, m \in \mathbb{G}_T) \rightarrow (\quad [ra]_1 \quad , \quad [r(W_1 + id \cdot W_2)a]_1 \quad , \quad [ra^T k]_T \cdot m \quad)$$

$$\text{Dec}(sk_{id}, ct) \rightarrow \quad [ra^T k]_T \cdot m \quad \times e \left(\quad [r(W_1 + id \cdot W_2)a]_1 \quad , \quad [sb]_2 \quad \right)$$

Construction

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

$$\text{Setup} \rightarrow \text{MSK} = (k \leftarrow \mathbb{Z}_p^2) \\ \text{MPK} = ([a^T k]_T)$$

$$\text{KeyGen}(id) \rightarrow ([sb]_2, [k + s(W_1 + id \cdot W_2)^T b]_2)$$

$$\text{Enc}(\text{MPK}, id, m \in \mathbb{G}_T) \rightarrow ([ra]_1, [r(W_1 + id \cdot W_2)a]_1, [ra^T k]_T \cdot m)$$

$$\text{Dec}(sk_{id}, ct) \rightarrow \frac{[ra^T k]_T \cdot m}{[r(W_1 + id \cdot W_2)a]_1, [sb]_2}$$

Construction

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

$$\text{Setup} \rightarrow \text{MSK} = (k \leftarrow \mathbb{Z}_p^2)$$

$$\text{MPK} = ([a^T k]_T)$$

$$\text{KeyGen}(id) \rightarrow ([sb]_2, [k + s(W_1 + id \cdot W_2)^T b]_2)$$

$$\text{Enc}(\text{MPK}, id, m \in \mathbb{G}_T) \rightarrow ([ra]_1, [r(W_1 + id \cdot W_2)a]_1, [ra^T k]_T \cdot m)$$

$$\text{Dec}(sk_{id}, ct) \rightarrow \frac{[ra^T k]_T \cdot m \times e([r(W_1 + id \cdot W_2)a]_1, [sb]_2)}{e([ra]_1, [k + s(W_1 + id \cdot W_2)^T b]_2)}$$

Simulation

Simulation

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

Simulation

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

$$Sim_1(id^*) \rightarrow$$

Simulation

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

$$Sim_1(id^*) \rightarrow MPK = ($$

Simulation

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

$$Sim_1(id^*) \rightarrow MPK = (\text{[redacted]})$$

Simulation

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

$$Sim_1(id^*) \rightarrow MPK = (\text{[redacted]}) \text{ where } k_1 \leftarrow \mathbb{Z}_p$$

Simulation

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

$$Sim_1(id^*) \rightarrow MPK = (\text{[redacted]}) \text{ where } k_1 \leftarrow \mathbb{Z}_p$$
$$ct = ($$

Simulation

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

$$Sim_1(id^*) \rightarrow MPK = (\text{[redacted]}) \text{ where } k_1 \leftarrow \mathbb{Z}_p$$
$$ct = (\text{[redacted]},$$

Simulation

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

$$Sim_1(id^*) \rightarrow MPK = ([k_1]_T) \text{ where } k_1 \leftarrow \mathbb{Z}_p$$

$$ct = ([u]_1, [(W_1 + id^* \cdot W_2)u]_1),$$

Simulation

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

$$\begin{aligned} \text{Sim}_1(id^*) &\rightarrow MPK = (\text{[redacted]}) \text{ where } k_1 \leftarrow \mathbb{Z}_p \\ ct &= (\text{[redacted]}, \text{[redacted]}, \text{[redacted]}) \end{aligned}$$

Simulation

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

$$Sim_1(id^*) \rightarrow MPK = (\text{[redacted]}) \text{ where } k_1 \leftarrow \mathbb{Z}_p$$

$$ct = (\text{[redacted]}, \text{[redacted]}, \text{[redacted]})$$

$$Sim_2(id) \rightarrow ($$

Simulation

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

$$\begin{aligned} Sim_1(id^*) &\rightarrow MPK = (\text{[blue box containing } [k_1]_T \text{]}) \text{ where } k_1 \leftarrow \mathbb{Z}_p \\ ct &= (\text{[purple box containing } [u]_1 \text{]}, \text{[purple box containing } [(W_1 + id^* \cdot W_2)u]_1 \text{]}, \text{[black box containing } [r]_T \text{]}) \end{aligned}$$

$$Sim_2(id) \rightarrow (\text{[green box containing } [sb]_2 \text{]},$$

Simulation

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

$$Sim_1(id^*) \rightarrow MPK = ([k_1]_T) \text{ where } k_1 \leftarrow \mathbb{Z}_p$$

$$ct = ([u]_1, [(W_1 + id^* \cdot W_2)u]_1, [r]_T)$$

$$Sim_2(id) \rightarrow ([sb]_2, [\frac{k_1 a}{|a|^2} + s(W_1 + id \cdot W_2)^T b + wa^T]_2)$$

Simulation

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

$$Sim_1(id^*) \rightarrow MPK = ([k_1]_T) \text{ where } k_1 \leftarrow \mathbb{Z}_p$$

$$ct = ([u]_1, [(W_1 + id^* \cdot W_2)u]_1, [r]_T)$$

$$Sim_2(id) \rightarrow ([sb]_2, [\frac{k_1 a}{|a|^2} + s(W_1 + id \cdot W_2)^T b + wa^T]_2)$$

k_2 is not used anywhere

Simulation

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

$$Sim_1(id^*) \rightarrow MPK = ([k_1]_T) \text{ where } k_1 \leftarrow \mathbb{Z}_p$$

$$ct = ([u]_1, [(W_1 + id^* \cdot W_2)u]_1, [r]_T)$$

$$Sim_2(id) \rightarrow ([sb]_2, [\frac{k_1 a}{|a|^2} + s(W_1 + id \cdot W_2)^T b + wa^T]_2)$$

k_2 is not used anywhere

$$Sim_3(m) \rightarrow$$

Simulation

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

$$Sim_1(id^*) \rightarrow MPK = ([k_1]_T) \text{ where } k_1 \leftarrow \mathbb{Z}_p$$

$$ct = ([u]_1, [(W_1 + id^* \cdot W_2)u]_1, [r]_T)$$

$$Sim_2(id) \rightarrow ([sb]_2, [\frac{k_1 a}{|a|^2} + s(W_1 + id \cdot W_2)^T b + wa^T]_2)$$

k_2 is not used anywhere

$$Sim_3(m) \rightarrow \text{Set } k_2 = \frac{\frac{r}{m} - u_1 k_1}{u_2} \text{ where } u = u_1 a + u_2 a^\top$$

Simulation

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

$$Sim_1(id^*) \rightarrow MPK = ([k_1]_T) \text{ where } k_1 \leftarrow \mathbb{Z}_p$$

$$ct = ([u]_1, [(W_1 + id^* \cdot W_2)u]_1, [r]_T)$$

$$Sim_2(id) \rightarrow ([sb]_2, [\frac{k_1 a}{|a|^2} + s(W_1 + id \cdot W_2)^T b + wa^T]_2)$$

k_2 is not used anywhere

$$Sim_3(m) \rightarrow \text{Set } k_2 = \frac{\frac{r}{m} - u_1 k_1}{u_2} \text{ where } u = u_1 a + u_2 a^\top$$

$$MSK = ($$

Simulation

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

$$Sim_1(id^*) \rightarrow MPK = ([k_1]_T) \text{ where } k_1 \leftarrow \mathbb{Z}_p$$

$$ct = ([u]_1, [(W_1 + id^* \cdot W_2)u]_1, [r]_T)$$

$$Sim_2(id) \rightarrow ([sb]_2, [\frac{k_1 a}{|a|^2} + s(W_1 + id \cdot W_2)^T b + wa^T]_2)$$

k_2 is not used anywhere

$$Sim_3(m) \rightarrow \text{Set } k_2 = \frac{\frac{r}{m} - u_1 k_1}{u_2} \text{ where } u = u_1 a + u_2 a^\top$$

$$MSK = (k = \frac{k_1}{|a|^2} a + \frac{k_2}{|a^\top|^2} a^\top)$$

Simulation

$$pp = ([a]_1, [b]_2, [W_1 a]_1, [W_2 a]_1, [W_1^T b]_2, [W_2^T b]_2) \text{ where } a, b \leftarrow \mathbb{Z}_p^2, W_i \leftarrow \mathbb{Z}_p^{2 \times 2}$$

$$Sim_1(id^*) \rightarrow MPK = (\text{[blue box: } [k_1]_T \text{]}) \text{ where } k_1 \leftarrow \mathbb{Z}_p$$

$$ct = (\text{[purple box: } [u]_1 \text{]}, \text{[purple box: } [(W_1 + id^* \cdot W_2)u]_1 \text{]}, \text{[black box: } [r]_T \text{]})$$


DDH

$$Sim_2(id) \rightarrow (\text{[green box: } [sb]_2 \text{]}, \text{[green box: } [\frac{k_1 a}{|a|^2} + s(W_1 + id \cdot W_2)^T b + wa^T]_2 \text{]})$$

k_2 is not used anywhere

$$Sim_3(m) \rightarrow \text{Set } k_2 = \frac{\frac{r}{m} - u_1 k_1}{u_2} \text{ where } u = u_1 a + u_2 a^\top$$

$$MSK = (k = \frac{k_1}{|a|^2} a + \frac{k_2}{|a^\top|^2} a^\top)$$

Incomp IBE from RNC-IBE

Incomp IBE from RNC-IBE

1. RNC-IBE

Incomp IBE from RNC-IBE

1. RNC-IBE
2. Incompressible SKE scheme

Incomp IBE from RNC-IBE

1. RNC-IBE
2. Incompressible SKE scheme

Setup →

Incomp IBE from RNC-IBE

1. RNC-IBE
2. Incompressible SKE scheme

$Setup \rightarrow MPK = ($

Incomp IBE from RNC-IBE

1. RNC-IBE
2. Incompressible SKE scheme

$$\textit{Setup} \rightarrow \textit{MPK} = (\textit{RNCIBE.MPK})$$

Incomp IBE from RNC-IBE

1. RNC-IBE
2. Incompressible SKE scheme

$$\textit{Setup} \rightarrow \textit{MPK} = (\textit{RNCIBE.MPK})$$

$$\textit{MSK} = ($$

Incomp IBE from RNC-IBE

1. RNC-IBE
2. Incompressible SKE scheme

$$\textit{Setup} \rightarrow \textit{MPK} = (\textit{RNCIBE.MPK})$$

$$\textit{MSK} = (\textit{RNCIBE.MSK})$$

Incomp IBE from RNC-IBE

1. RNC-IBE
2. Incompressible SKE scheme

$$Setup \rightarrow MPK = (\text{RNCIBE.MPK})$$

$$MSK = (\text{RNCIBE.MSK})$$

$$KeyGen(id) \rightarrow$$

Incomp IBE from RNC-IBE

1. RNC-IBE
2. Incompressible SKE scheme

$$\textit{Setup} \rightarrow \textit{MPK} = (\textit{RNCIBE.MPK})$$

$$\textit{MSK} = (\textit{RNCIBE.MSK})$$

$$\textit{KeyGen}(id) \rightarrow \textit{RNCIBE.KeyGen}($$

Incomp IBE from RNC-IBE

1. RNC-IBE
2. Incompressible SKE scheme

$$\textit{Setup} \rightarrow \textit{MPK} = (\textit{RNCIBE.MPK})$$

$$\textit{MSK} = (\textit{RNCIBE.MSK})$$

$$\textit{KeyGen}(id) \rightarrow \textit{RNCIBE.KeyGen}(\textit{RNCIBE.MPK},$$

Incomp IBE from RNC-IBE

1. RNC-IBE
2. Incompressible SKE scheme

$$\textit{Setup} \rightarrow \textit{MPK} = (\textit{RNCIBE.MPK})$$

$$\textit{MSK} = (\textit{RNCIBE.MSK})$$

$$\textit{KeyGen}(id) \rightarrow \textit{RNCIBE.KeyGen}(\textit{RNCIBE.MPK}, id)$$

Incomp IBE from RNC-IBE

1. RNC-IBE
2. Incompressible SKE scheme

$$Setup \rightarrow MPK = (\text{RNCIBE.MPK})$$

$$MSK = (\text{RNCIBE.MSK})$$

$$KeyGen(id) \rightarrow \text{RNCIBE.KeyGen}(\text{RNCIBE.MPK}, id)$$

$$Enc(id, m) \rightarrow$$

Incomp IBE from RNC-IBE

1. RNC-IBE
2. Incompressible SKE scheme

$$Setup \rightarrow MPK = (\text{RNCIBE.MPK})$$

$$MSK = (\text{RNCIBE.MSK})$$

$$KeyGen(id) \rightarrow \text{RNCIBE.KeyGen}(\text{RNCIBE.MPK}, id)$$

$$Enc(id, m) \rightarrow \text{IncompSKE.Enc}($$

Incomp IBE from RNC-IBE

1. RNC-IBE
2. Incompressible SKE scheme

$$Setup \rightarrow MPK = (\text{RNCIBE.MPK})$$

$$MSK = (\text{RNCIBE.MSK})$$

$$KeyGen(id) \rightarrow \text{RNCIBE.KeyGen}(\text{RNCIBE.MPK}, id)$$

$$Enc(id, m) \rightarrow \text{IncompSKE.Enc}(\text{incompSK},$$

Incomp IBE from RNC-IBE

1. RNC-IBE
2. Incompressible SKE scheme

$$Setup \rightarrow MPK = (\text{RNCIBE.MPK})$$

$$MSK = (\text{RNCIBE.MSK})$$

$$KeyGen(id) \rightarrow \text{RNCIBE} . KeyGen(\text{RNCIBE.MPK}, id)$$

$$Enc(id, m) \rightarrow \text{IncompSKE} . Enc(\text{incompSK}, m)$$

Incomp IBE from RNC-IBE

1. RNC-IBE
2. Incompressible SKE scheme

$$Setup \rightarrow MPK = (\text{RNCIBE.MPK})$$

$$MSK = (\text{RNCIBE.MSK})$$

$$KeyGen(id) \rightarrow \text{RNCIBE.KeyGen}(\text{RNCIBE.MPK}, id)$$

$$Enc(id, m) \rightarrow \text{IncompSKE.Enc}(\text{incompSK}, m)$$

$$\text{RNCIBE.Enc}($$

Incomp IBE from RNC-IBE

1. RNC-IBE
2. Incompressible SKE scheme

$$Setup \rightarrow MPK = (\text{RNCIBE.MPK})$$

$$MSK = (\text{RNCIBE.MSK})$$

$$KeyGen(id) \rightarrow \text{RNCIBE.KeyGen}(\text{RNCIBE.MPK}, id)$$

$$Enc(id, m) \rightarrow \text{IncompSKE.Enc}(\text{incompSK}, m)$$

$$\text{RNCIBE.Enc}(\text{RNCIBE.MPK},$$

Incomp IBE from RNC-IBE

1. RNC-IBE
2. Incompressible SKE scheme

$$Setup \rightarrow MPK = (\text{RNCIBE.MPK})$$

$$MSK = (\text{RNCIBE.MSK})$$

$$KeyGen(id) \rightarrow \text{RNCIBE.KeyGen}(\text{RNCIBE.MPK}, id)$$

$$Enc(id, m) \rightarrow \text{IncompSKE.Enc}(\text{incompSK}, m)$$

$$\text{RNCIBE.Enc}(\text{RNCIBE.MPK}, id ,$$

Incomp IBE from RNC-IBE

1. RNC-IBE
2. Incompressible SKE scheme

$$Setup \rightarrow MPK = (\text{RNCIBE.MPK})$$

$$MSK = (\text{RNCIBE.MSK})$$

$$KeyGen(id) \rightarrow \text{RNCIBE} . KeyGen(\text{RNCIBE.MPK}, id)$$

$$Enc(id, m) \rightarrow \text{IncompSKE} . Enc(\text{incompSK}, m)$$

$$\text{RNCIBE} . Enc(\text{RNCIBE.MPK}, id, \text{incompSK})$$

Incomp IBE from RNC-IBE

1. RNC-IBE
2. Incompressible SKE scheme

$$Setup \rightarrow MPK = (\text{RNCIBE.MPK})$$

$$MSK = (\text{RNCIBE.MSK})$$

$$KeyGen(id) \rightarrow \text{RNCIBE.KeyGen}(\text{RNCIBE.MPK}, id)$$

$$Enc(id, m) \rightarrow \text{IncompSKE.Enc}(\text{incompSK}, m)$$

Hybrid encryption  $\text{RNCIBE.Enc}(\text{RNCIBE.MPK}, id, \text{incompSK})$

Future Directions

Future Directions

1. RNC-IBE from LWE and other assumptions.

Future Directions

1. RNC-IBE from LWE and other assumptions.
2. **Full** NC-IBE from standard assumptions.

Future Directions

1. RNC-IBE from LWE and other assumptions.
2. **Full** NC-IBE from standard assumptions.
3. ~~Rate-1 RNC-ABE from bilinear pairings.~~

Future Directions

1. RNC-IBE from LWE and other assumptions.
2. **Full** NC-IBE from standard assumptions.
3. ~~Rate-1 RNC-ABE from bilinear pairings.~~
4. Strong incompressible IBE and ABE from other standard assumptions.



Thank You

<https://mahe94.github.io>